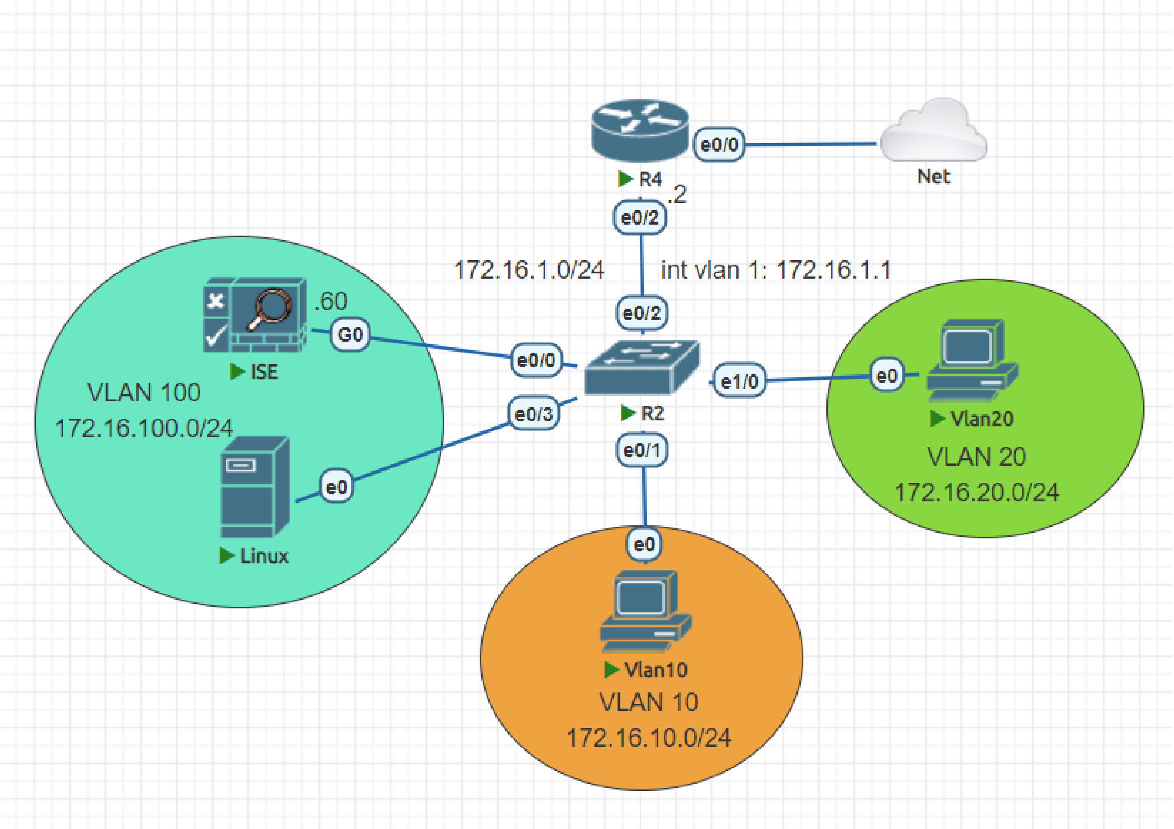
LAB – Cấu hình Cisco Profiling

Sơ đồ LAB



Mô tả:

Sơ đồ Lab gồm 1 router, 1 switch layer 3, 1 cisco ISE đóng vai trò là server radius và 3 PC được đấu nối như hình.

Trên sơ đồ này, học viên sẽ thực tập cấu hình chức năng cisco profiling để giúp phân loại các thiết bị khi kết nối vào mạng.

Yêu cầu:

1. Học viên thực hiện đấu nối các thiết bị và đặt địa chỉ IP(trừ các PC trong vlan 10,20 và 100) cũng như các hostname của các thiết bị được chỉ ra mô hình.
2. Sau khi thiết lập xong mô hình, học viên tiến hành ip address dhcp trên cổng e0/0 của router, cấu hình nat theo kiểu PAT đảm bảo mọi địa chỉ có thể đi internet. Cấu hình dhcp trên router để cấp ip cho các vlan 1, 10, 20 và 100.
3. Trên switch cấu hình các vlan 10, 20 và 100 đặt tên lần lượt là: window10, window20 và window100. Sau đó cấu hình SVI, ip cho vlan 1 là 172.16.1.1/24, vlan 10 là 172.16.10.1/24, vlan 20 là 172.16.20.1/24 và vlan 100 là 172.16.100.1/24.

4. Cấu hình các thông tin cho cisco ise như ip và gateway, cấu hình dhcp cho PC trong vlan 100. Bắt đầu cấu hình xác thực 802.1x kết hợp mab và phân quyền đảm bảo các PC trong các vlan 10, 20 và 100 có thể vào mạng được.
5. Cấu hình chức năng profiling sao cho nếu pc là thiết bị microsoft và thuộc các endpoints group thì tự động đổi phân quyền cho thiết bị đó.

Thực hiện:

Bước 1: Kết nối và cấu hình cơ bản:

Học viên thực hiện kết nối thiết bị và cấu hình cơ bản trên các thiết bị theo yêu cầu đặt ra.

Bước 2: Cấu hình nat, dhcp trên router:

Học viên thực hiện cấu hình trên router theo yêu cầu đã đặt ra.

Bước 3: Cấu hình vlan và SVI trên switch:

Học viên thực hiện cấu hình trên switch theo yêu cầu đặt ra.

Bước 4: Cấu hình 802.1x, mab và phân quyền:

Cấu hình đặt ip và gateway cho cisco ise:

```
CiscoISE/admin(config)# interface gigabitEthernet 0

CiscoISE/admin(config-GigabitEthernet)# ip address 172.16.100.60
255.255.255.0

CiscoISE/admin(config-GigabitEthernet)# exit

CiscoISE/admin(config)# ip default-gateway 172.16.100.1
```

Cấu hình bật xác thực 802.1x trên switch:

```
SW1(config)#aaa new-model

SW1(config)#aaa authentication dot1x default group ISE-RADIUS local

SW1(config)#aaa authorization network default group ISE-RADIUS local

SW1(config)#dot1x system-auth-control

SW1(config)#exit
```

Cấu hình thông tin radius server trên switch:

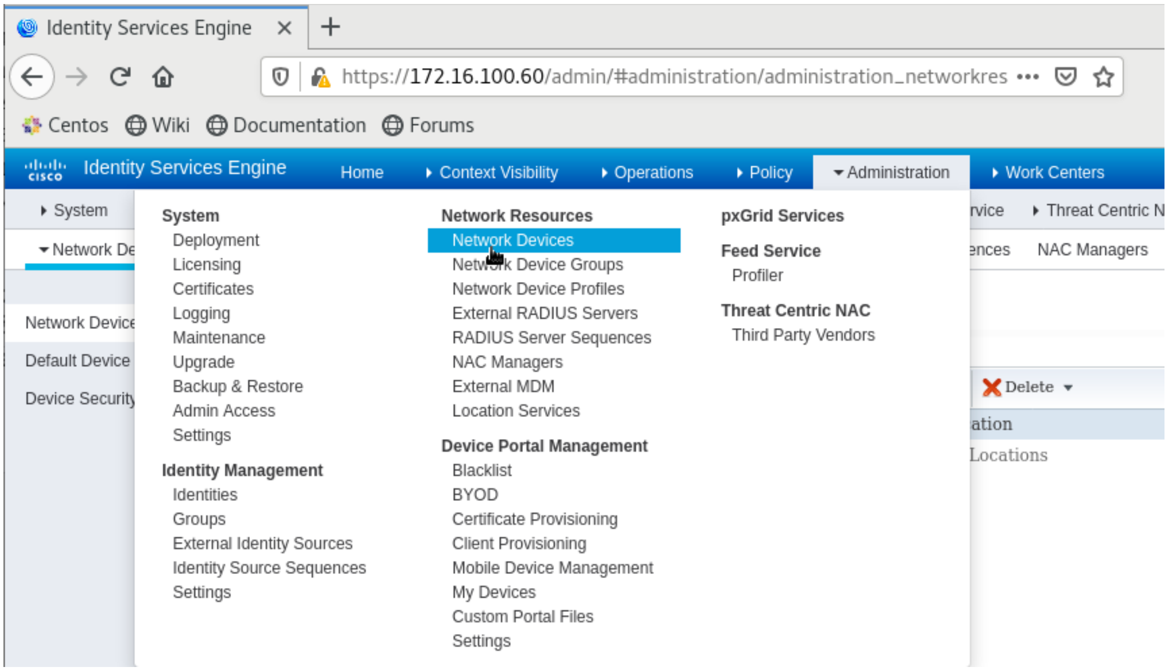
```
SW1(config)#radius server ise-radius

SW1(config-radius-server)#address ipv4 172.16.100.60

SW1(config-radius-server)#key VnPro123

SW1(config-radius-server)#exit

SW1(config)#aaa group server radius ISE-RADIUS

SW1(config-sg-radius)#server name ise-radius
```

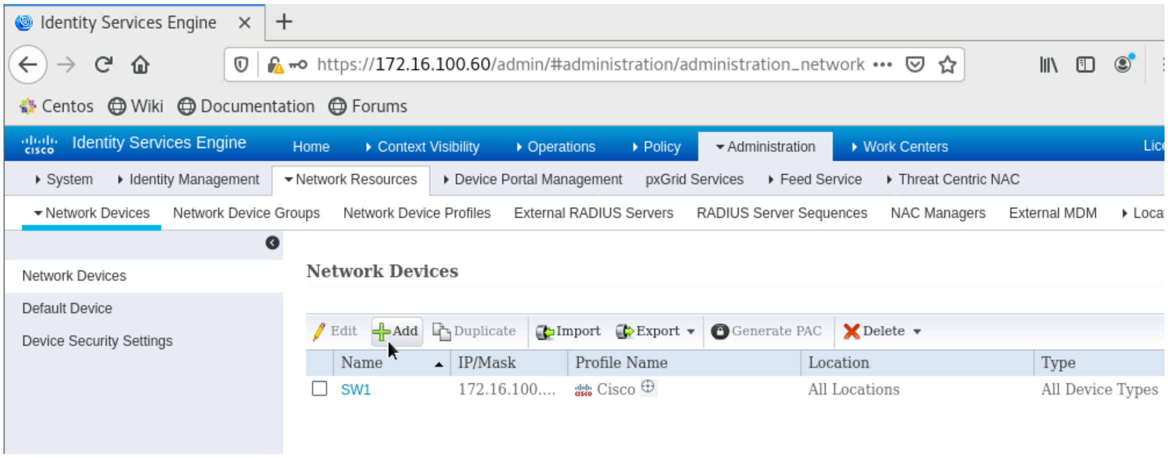
```
SW1(config-sg-radius)#exit
```

Cấu hình bật 802.1x và mab trên interface e0/1 và e1/0:

```
SW1(config)#interface range e0/1, e1/0
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#ip device tracking maximum 1
SW1(config-if-range)#authentication host-mode multi-auth
SW1(config-if-range)#authentication order mab dot1x
SW1(config-if-range)# authentication priority dot1x mab
SW1(config-if-range)#authentication port-control auto
SW1(config-if-range)#authentication periodic
SW1(config-if-range)#authentication timer reauthenticate server
SW1(config-if-range)#mab
SW1(config-if-range)#dot1x pae authenticator
SW1(config-if-range)#dot1x timeout tx-period 10
SW1(config-if-range)#spanning-tree portfast
```

Mở PC Linux vào web và gõ địa chỉ cisco ise 172.16.100.60 sau đó cấu hình network devices để có thể trao đổi với switch Administration->Network Devices->Add:

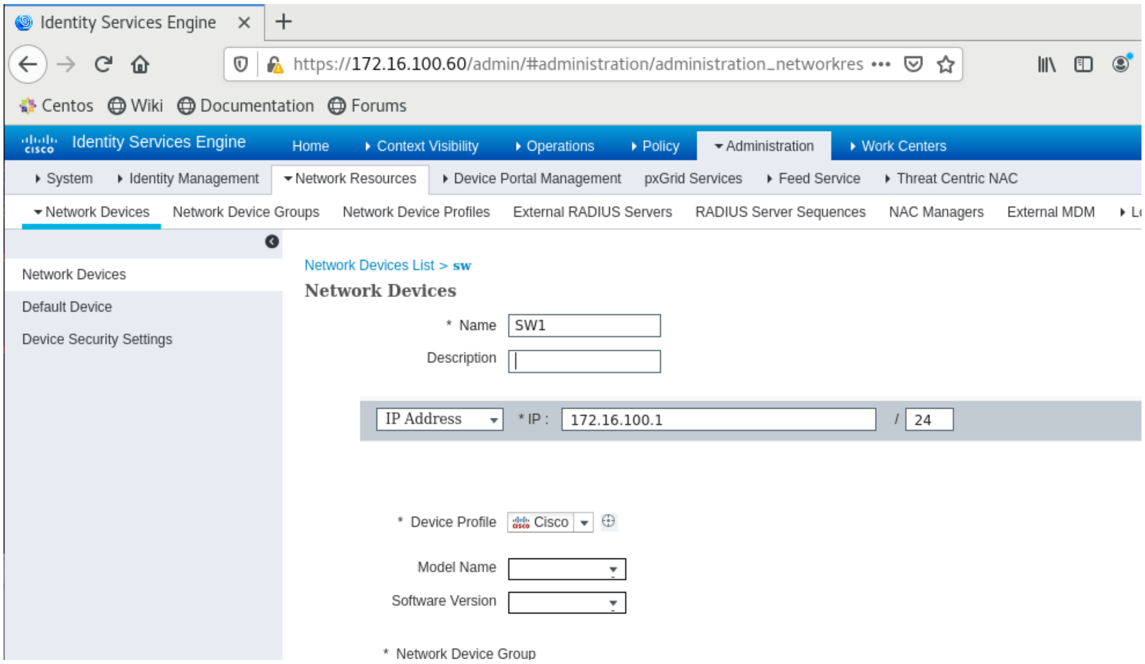




Network Devices

	Name	IP/Mask	Profile Name	Location	Type
□	SW1	172.16.100....	Cisco	All Locations	All Device Types

Cấu hình các thông số như hình rồi nhấn submit:



Network Devices List > sw

Network Devices

* Name: SW1

Description:

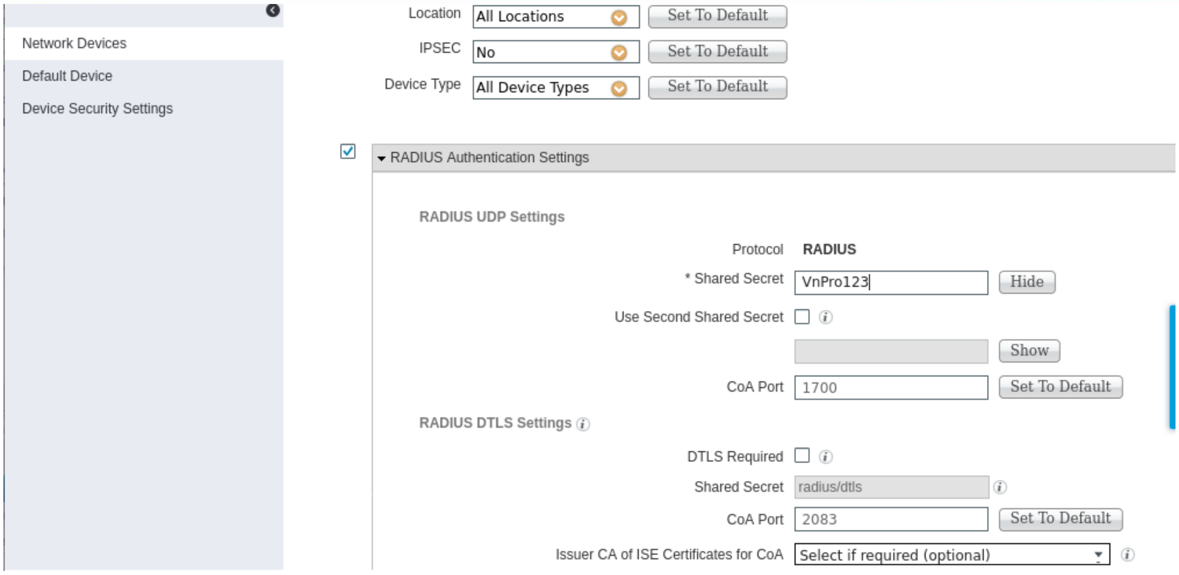
IP Address * IP : 172.16.100.1 / 24

* Device Profile: Cisco

Model Name:

Software Version:

* Network Device Group



Location: All Locations [Set To Default]
IPSEC: No [Set To Default]
Device Type: All Device Types [Set To Default]

☑ RADIUS Authentication Settings

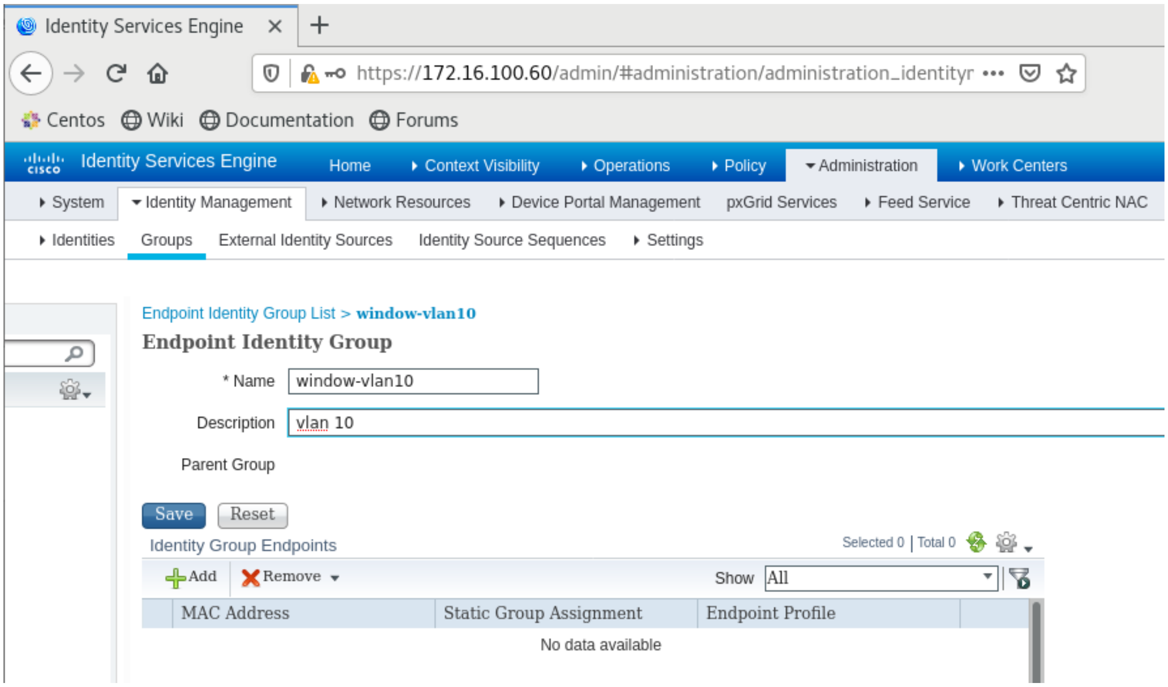
RADIUS UDP Settings

Protocol: RADIUS
* Shared Secret: VnPro123 [Hide]
Use Second Shared Secret: □
[Show]
CoA Port: 1700 [Set To Default]

RADIUS DTLS Settings

DTLS Required: □
Shared Secret: radius/dtls
CoA Port: 2083 [Set To Default]
Issuer CA of ISE Certificates for CoA: Select if required (optional)

Cấu hình tạo ra các endpoint groups window10, window20 và window100 trên cisco ise Administration->Groups->Endpoint Identity Groups->Add:



Endpoint Identity Group List > window-vlan10

Endpoint Identity Group

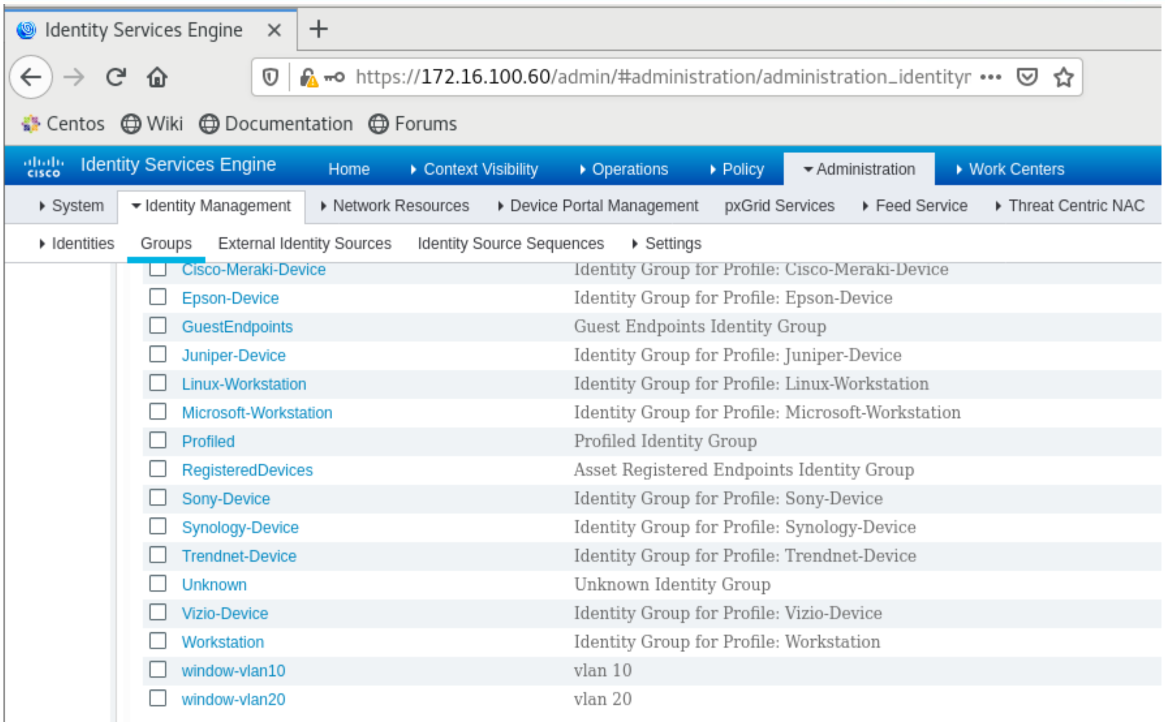
* Name: window-vlan10
Description: vlan 10
Parent Group:

[Save] [Reset]

Identity Group Endpoints — Selected 0 | Total 0

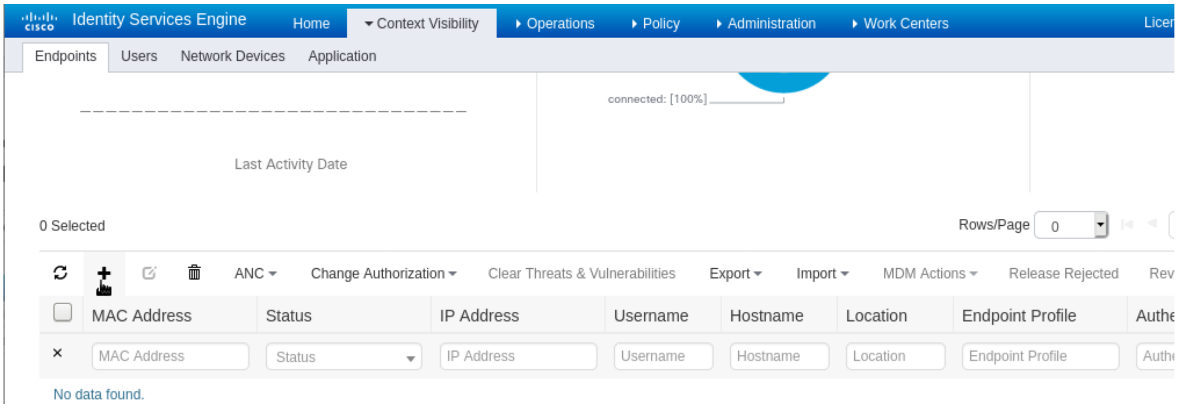
MAC Address	Static Group Assignment	Endpoint Profile
No data available		

Làm tương tự cho window20 và window100



□	Cisco-Meraki-Device	Identity Group for Profile: Cisco-Meraki-Device
□	Epson-Device	Identity Group for Profile: Epson-Device
□	GuestEndpoints	Guest Endpoints Identity Group
□	Juniper-Device	Identity Group for Profile: Juniper-Device
□	Linux-Workstation	Identity Group for Profile: Linux-Workstation
□	Microsoft-Workstation	Identity Group for Profile: Microsoft-Workstation
□	Profiled	Profiled Identity Group
□	RegisteredDevices	Asset Registered Endpoints Identity Group
□	Sony-Device	Identity Group for Profile: Sony-Device
□	Synology-Device	Identity Group for Profile: Synology-Device
□	Trendnet-Device	Identity Group for Profile: Trendnet-Device
□	Unknown	Unknown Identity Group
□	Vizio-Device	Identity Group for Profile: Vizio-Device
□	Workstation	Identity Group for Profile: Workstation
□	window-vlan10	vlan 10
□	window-vlan20	vlan 20

Cấu hình thêm các địa chỉ mac của endpoints theo từng group, pc trong vlan 10 vào group window10 và pc trong vlan 20 vào group window20 Context Visibility->Endpoints->+

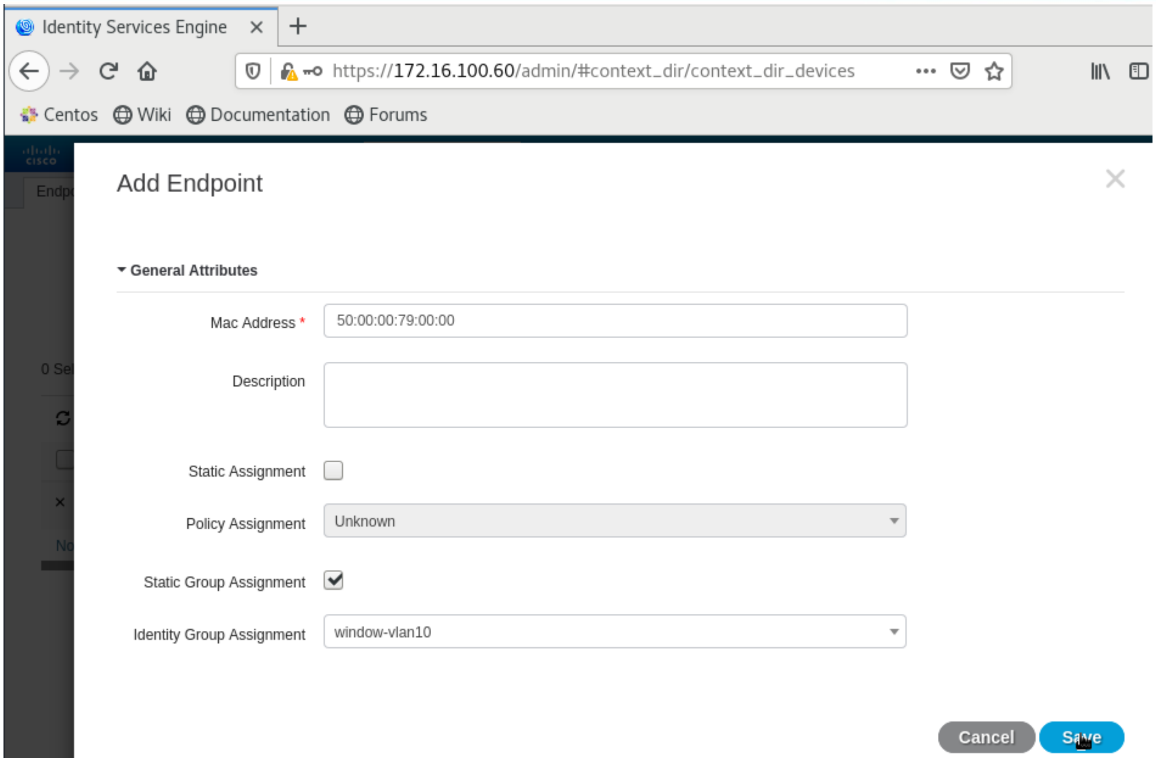


0 Selected

Rows/Page 0

□	MAC Address	Status	IP Address	Username	Hostname	Location	Endpoint Profile	Authe
×	MAC Address	Status	IP Address	Username	Hostname	Location	Endpoint Profile	Authe

No data found.


Identity Services Engine
https://172.16.100.60/admin/#context_dir/context_dir_devices
Centos
Wiki
Documentation
Forums

Add Endpoint

General Attributes

Mac Address * 50:00:00:79:00:00

Description

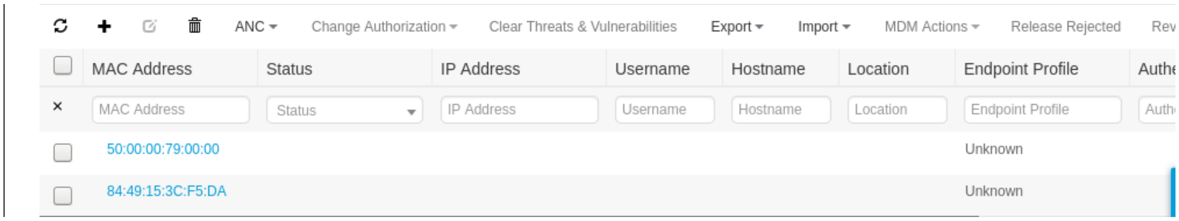
Static Assignment ☐

Policy Assignment Unknown

Static Group Assignment ☑

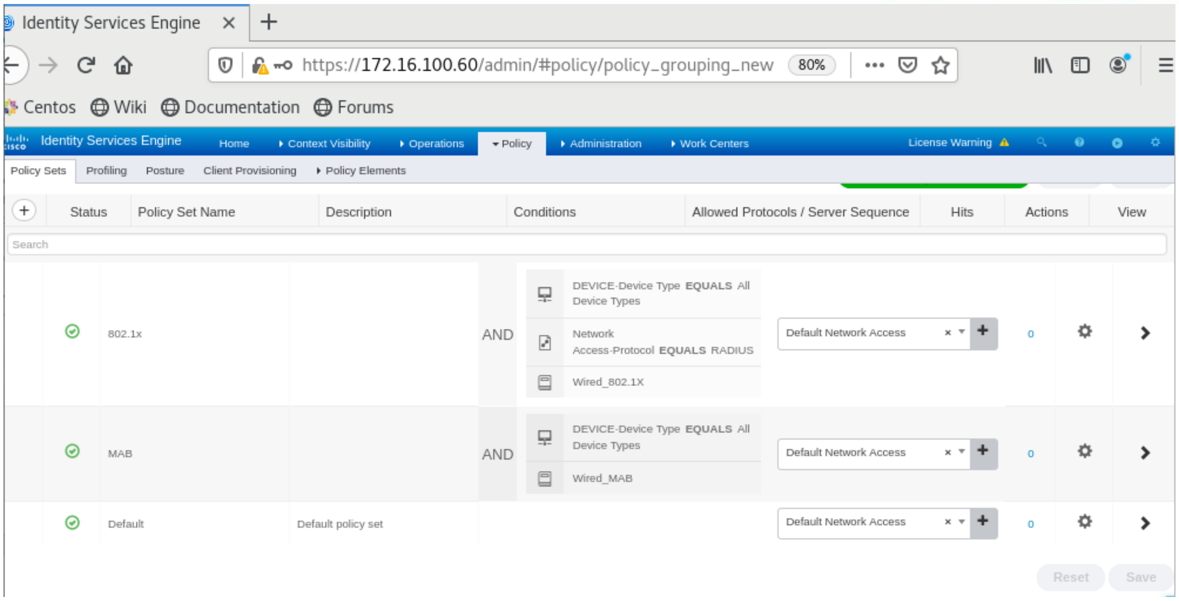
Identity Group Assignment window-vlan10

Làm tương tự cho pc trong vlan 20



	MAC Address	Status	IP Address	Username	Hostname	Location	Endpoint Profile	Authe
☐	50:00:00:79:00:00						Unknown	
☐	84:49:15:3C:F5:DA						Unknown	

Tạo policy để xác thực MAB Policy->Policy Sets:

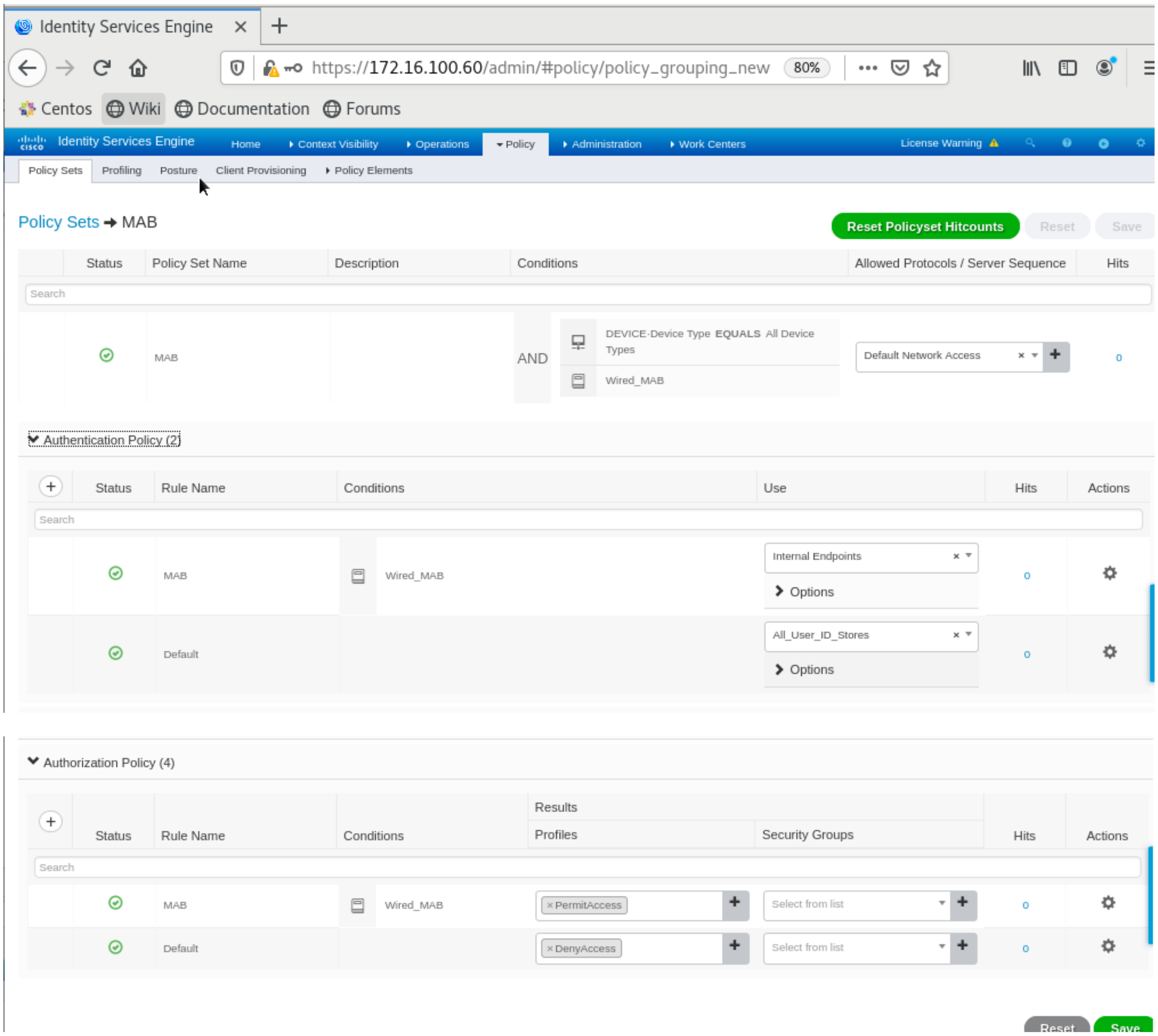


Identity Services Engine

https://172.16.100.60/admin/#policy/policy_grouping_new 80%

Centos Wiki Documentation Forums

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	802.1x		AND DEVICE·Device Type EQUALS All Device Types Network Access·Protocol EQUALS RADIUS Wired_802.1X	Default Network Access	0	⚙	›
✓	MAB		AND DEVICE·Device Type EQUALS All Device Types Wired_MAB	Default Network Access	0	⚙	›
✓	Default	Default policy set		Default Network Access	0	⚙	›



Identity Services Engine

https://172.16.100.60/admin/#policy/policy_grouping_new 80%

Centos Wiki Documentation Forums

Policy Sets → MAB

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	MAB		AND DEVICE·Device Type EQUALS All Device Types Wired_MAB	Default Network Access	0

Authentication Policy (2)

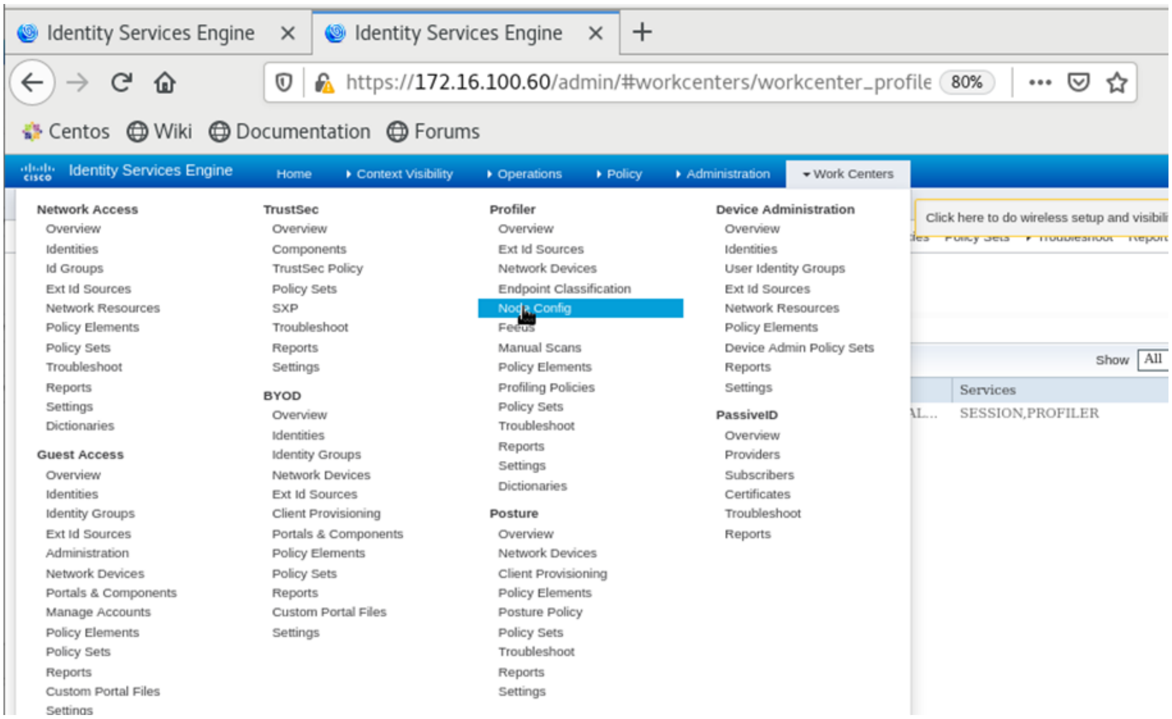
Status	Rule Name	Conditions	Use	Hits	Actions
✓	MAB	Wired_MAB	Internal Endpoints Options	0	⚙
✓	Default		All_User_ID_Stores Options	0	⚙

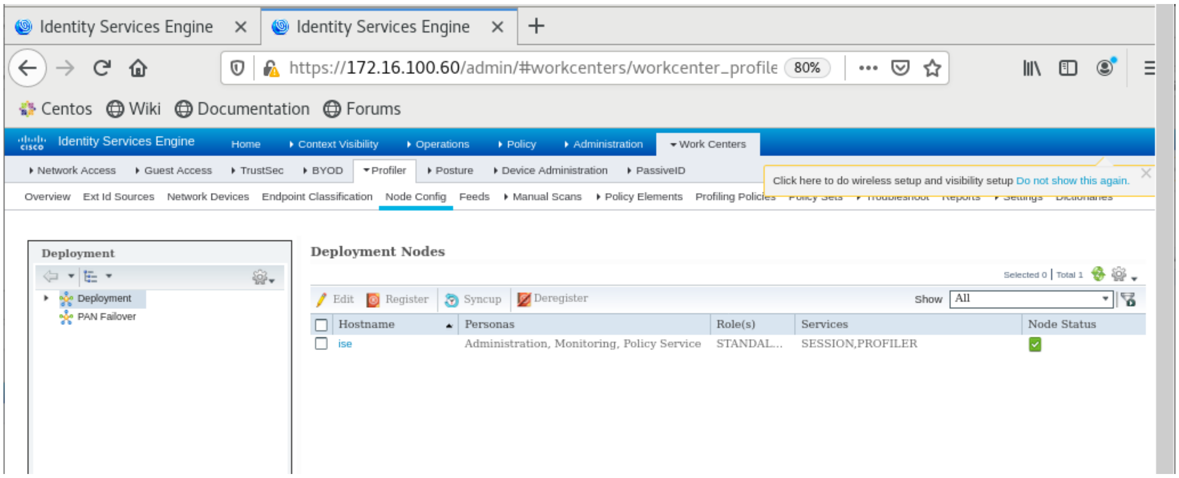
Authorization Policy (4)

			Results			
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	MAB	Wired_MAB	PermitAccess	Select from list	0	⚙
✓	Default		DenyAccess	Select from list	0	⚙

Bước 5: Cấu hình chức năng profiling:

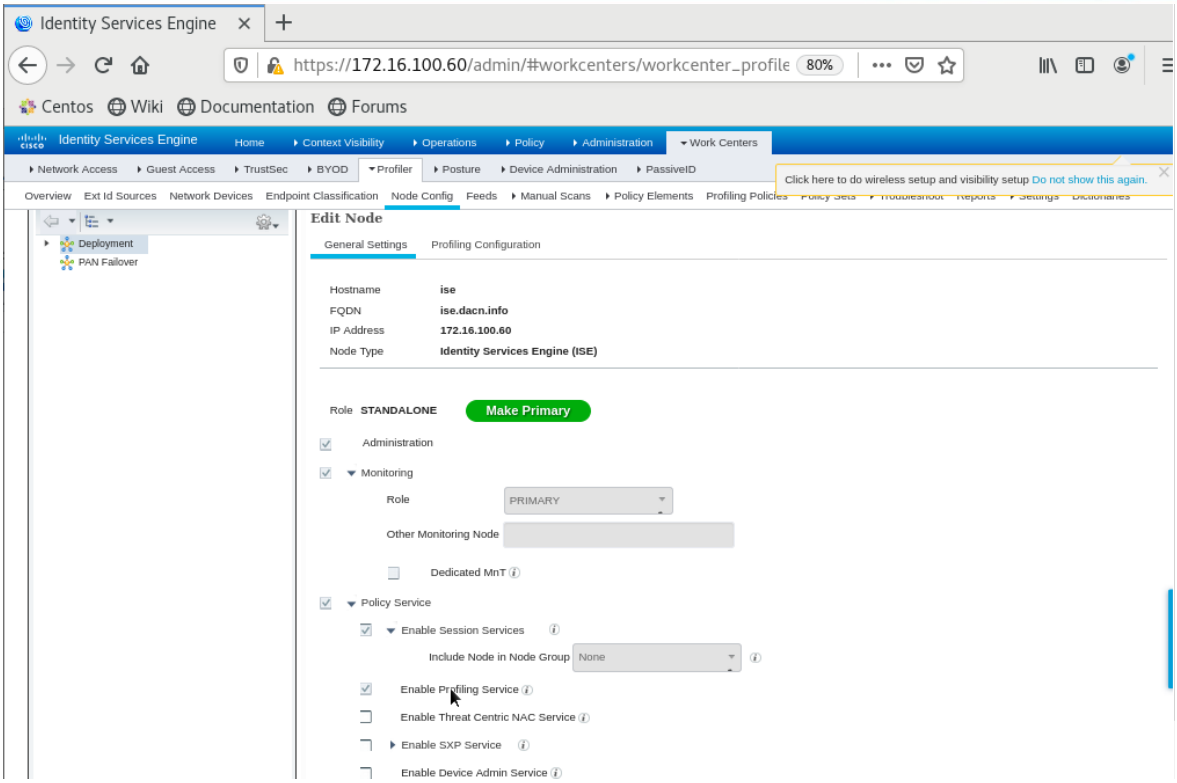
Bật chức năng profiling Work Centers->Node Config->ise->General Settings





Deployment Nodes

□	Hostname	Personas	Role(s)	Services	Node Status
□	ise	Administration, Monitoring, Policy Service	STANDAL...	SESSION,PROFILER	✓


Identity Services Engine
https://172.16.100.60/admin/#workcenters/workcenter_profile 80%
Centos Wiki Documentation Forums
Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers
Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID
Overview Ext Id Sources Network Devices Endpoint Classification Node Config Feeds Manual Scans Policy Elements Profiling Policies
Click here to do wireless setup and visibility setup Do not show this again.
Deployment
PAN Failover
Make Primary

Edit Node

General Settings | Profiling Configuration

Hostname ise
FQDN ise.dacn.info
IP Address 172.16.100.60
Node Type Identity Services Engine (ISE)

Role STANDALONE

☑ Administration

☑ Monitoring

Role PRIMARY

Other Monitoring Node

□ Dedicated MnT

☑ Policy Service

☑ Enable Session Services

Include Node in Node Group None

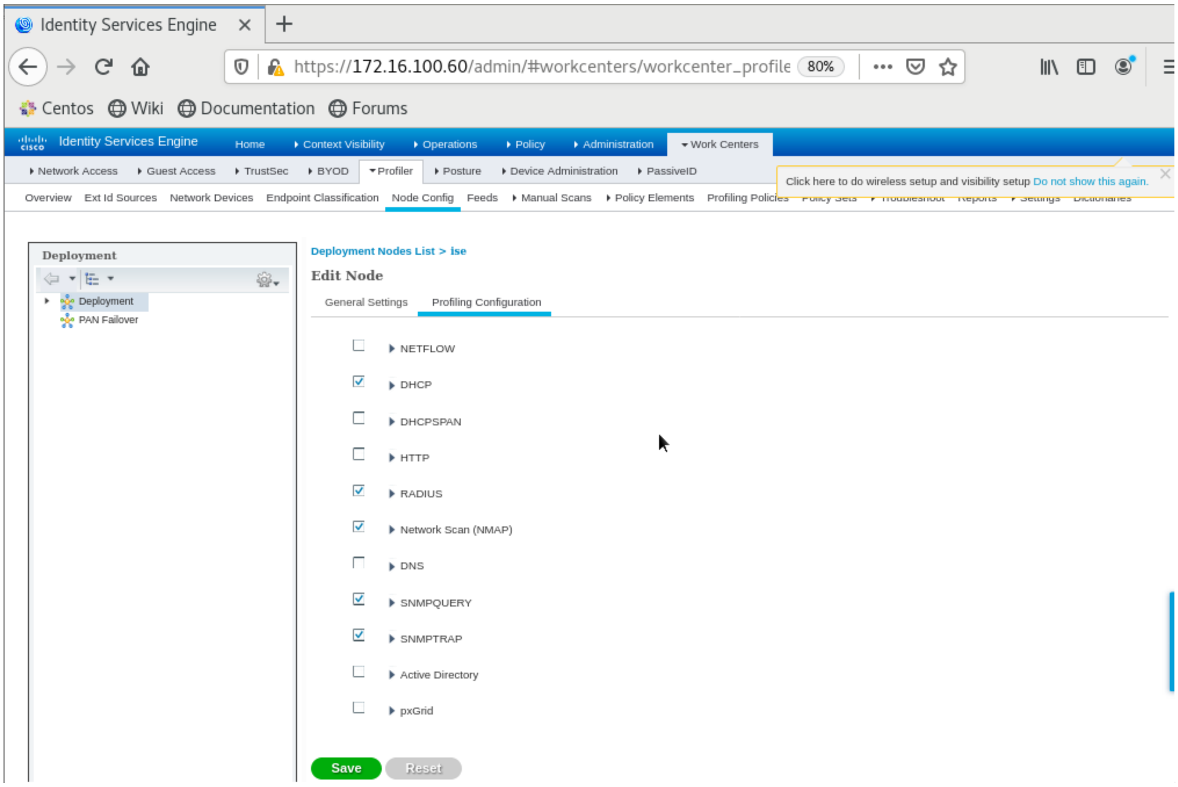
☑ Enable Profiling Service

□ Enable Threat Centric NAC Service

□ Enable SXP Service

□ Enable Device Admin Service

Chọn các thuộc tính mà cisco ise sẽ sử dụng khi phân loại thiết bị Work Centers->Node Config->ise->Profiling Configuration


Identity Services Engine
https://172.16.100.60/admin/#workcenters/workcenter_profile 80%
Centos Wiki Documentation Forums
Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers
Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID
Overview Ext Id Sources Network Devices Endpoint Classification Node Config Feeds Manual Scans Policy Elements Profiling Policies
Click here to do wireless setup and visibility setup Do not show this again.
Deployment
Deployment
PAN Failover
Save
Reset

Deployment Nodes List > ise

Edit Node

General Settings | Profiling Configuration

□ NETFLOW

☑ DHCP

□ DHCPSPAN

□ HTTP

☑ RADIUS

☑ Network Scan (NMAP)

□ DNS

☑ SNMPQUERY

☑ SNMPTRAP

□ Active Directory

□ pxGrid

Cấu hình trên SW1 để gửi các thông tin về cisco ISE:

Radius:

```
SW1(config)#aaa accounting dot1x default start-stop group ISE-RADIUS
```

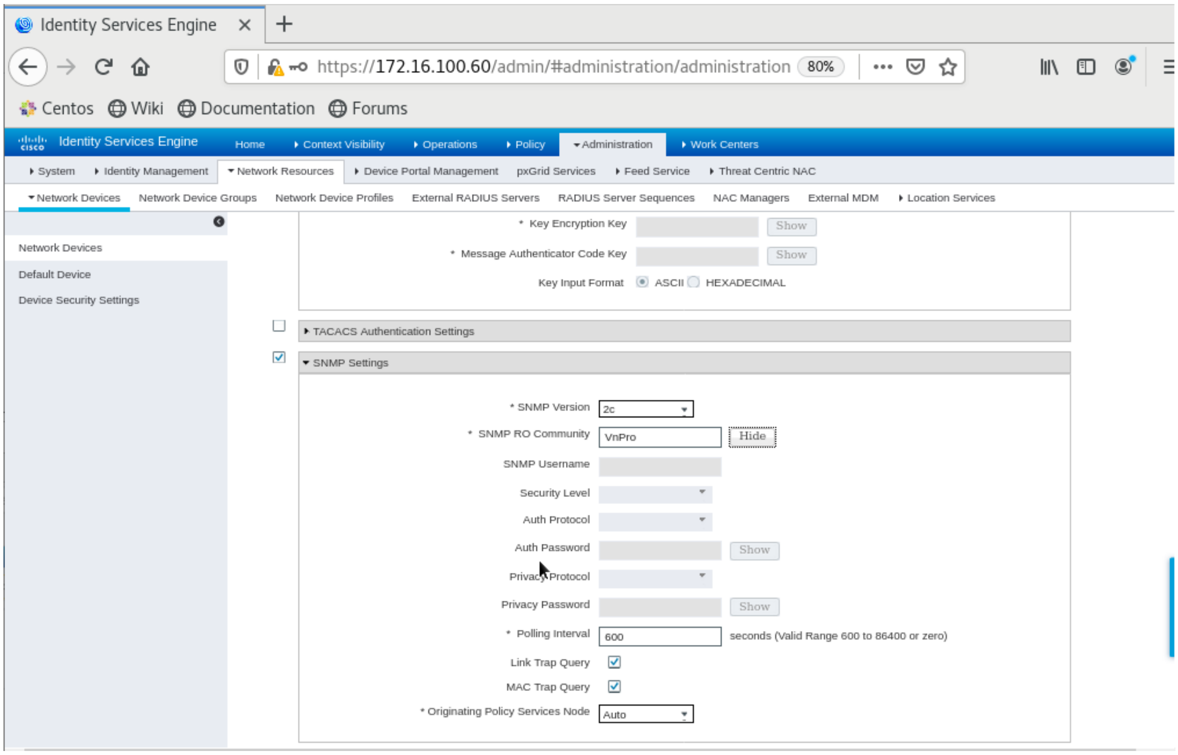
DHCP:

```
SW1(config)#int range vlan 1,vlan 10, vlan 20,vlan 100

SW1(config-if-range)#ip helper-address 172.16.100.60
```

SNMP:

```
SW1(config)#snmp-server community VnPro RO

SW1(config)#snmp-server trap-source Vlan1

SW1(config)#snmp-server source-interface informs Vlan1

SW1(config)#snmp-server enable traps snmp authentication linkdown linkup
coldstart warmstart

SW1(config)#snmp-server host 172.16.100.60 version 2c VnPro  snmp
```

Cấu hình SNMP trên cisco ise Administration->Network Devices->SW1



* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ● ASCII ○ HEXADECIMAL

□ TACACS Authentication Settings

☑ SNMP Settings

* SNMP Version: 2c

* SNMP RO Community: VnPro

SNMP Username

Security Level

Auth Protocol

Auth Password

Privacy Protocol

Privacy Password

* Polling Interval: 600 seconds (Valid Range 600 to 86400 or zero)

Link Trap Query ☑

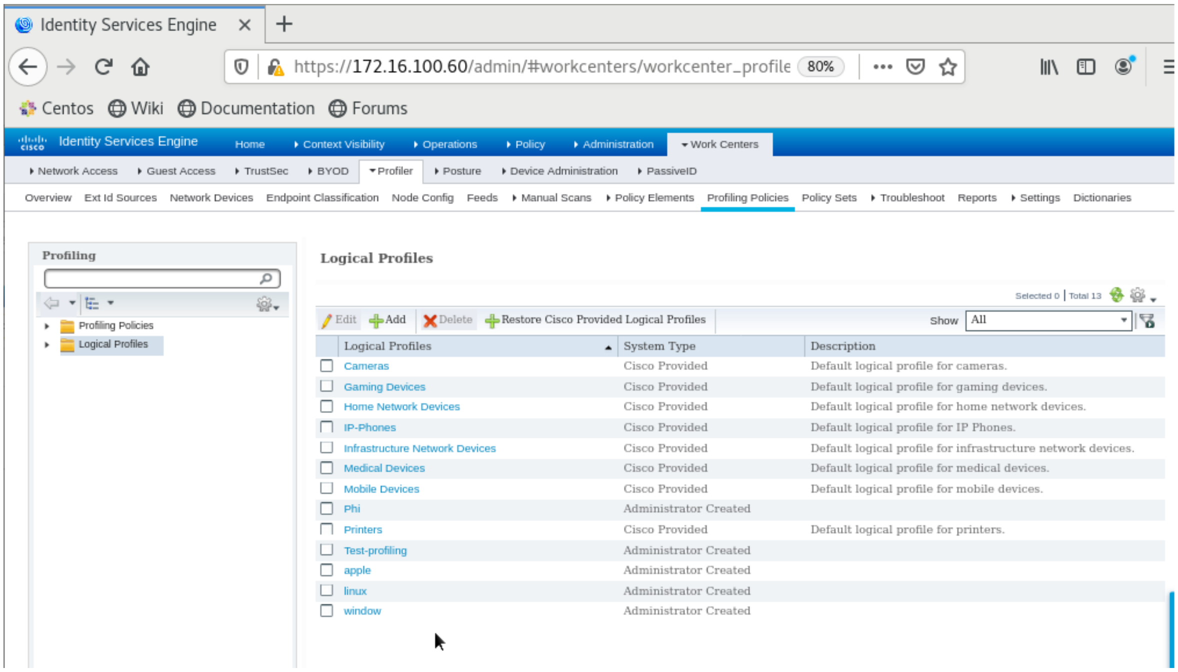
MAC Trap Query ☑

* Originating Policy Services Node: Auto

<u>Lưu ý:</u> Cisco ISE đã hỗ trợ cho chúng ta rất nhiều policy để detect ra thiết bị bằng cách lấy các thông tin như: hostname, OS, MAC… thông qua các giao thức SNMP, DHCP, NMAP, RADIUS... Nếu muốn tự customs các policy có thể vào mục Work Centers->Policy Elements->Profiler Conditions. Sau khi có được các policy thì cần phải thêm profling policy tại Work

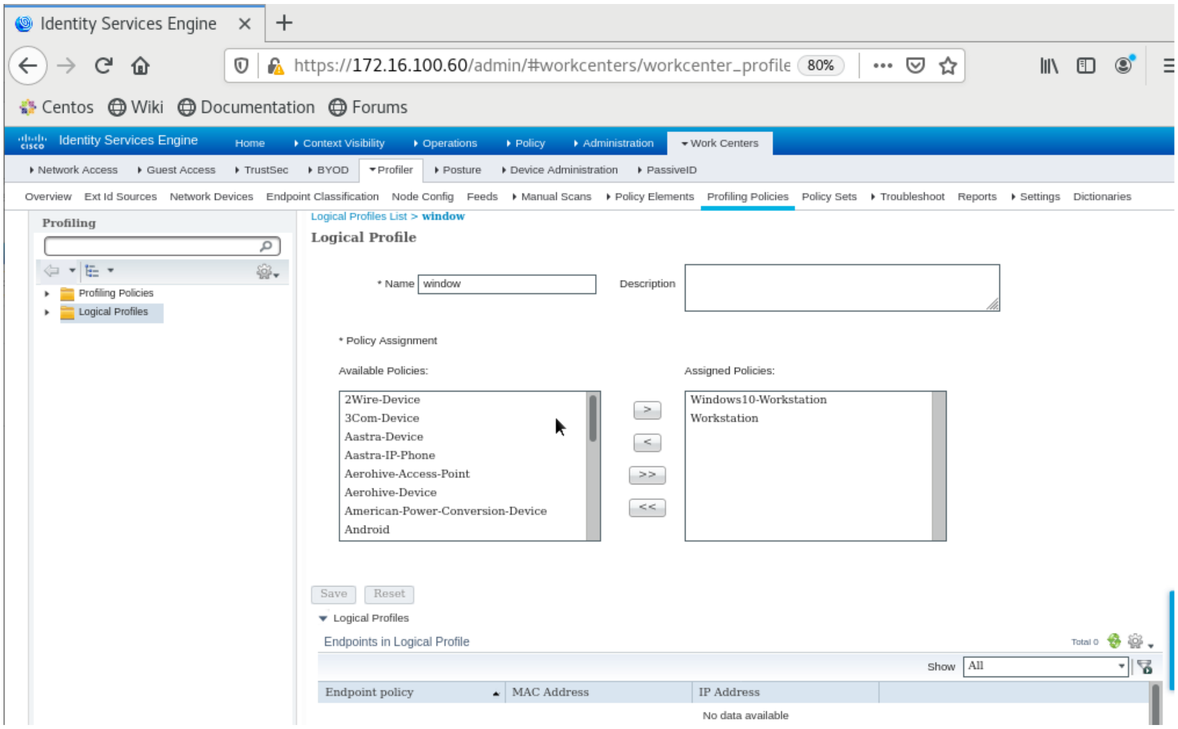
Centers->Profiling Policies->Profiling Policies. Ở bài này ta sẽ sử dụng các policy có sẵn trên cisco ISE.

Tạo các Logical Profiles để xác định thiết bị Work Centers->Profiling Policies->Logical Profiles->Add


Identity Services Engine
https://172.16.100.60/admin/#workcenters/workcenter_profile 80%
Centos Wiki Documentation Forums
Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers
Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID
Overview Ext Id Sources Network Devices Endpoint Classification Node Config Feeds Manual Scans Policy Elements Profiling Policies Policy Sets Troubleshoot Reports Settings Dictionaries
Profiling
Profiling Policies
Logical Profiles
Selected 0 | Total 13
Edit Add Delete Restore Cisco Provided Logical Profiles
Show All

Logical Profiles

Logical Profiles	System Type	Description
Cameras	Cisco Provided	Default logical profile for cameras.
Gaming Devices	Cisco Provided	Default logical profile for gaming devices.
Home Network Devices	Cisco Provided	Default logical profile for home network devices.
IP-Phones	Cisco Provided	Default logical profile for IP Phones.
Infrastructure Network Devices	Cisco Provided	Default logical profile for infrastructure network devices.
Medical Devices	Cisco Provided	Default logical profile for medical devices.
Mobile Devices	Cisco Provided	Default logical profile for mobile devices.
Phi	Administrator Created	
Printers	Cisco Provided	Default logical profile for printers.
Test-profiling	Administrator Created	
apple	Administrator Created	
linux	Administrator Created	
window	Administrator Created	


Identity Services Engine
https://172.16.100.60/admin/#workcenters/workcenter_profile 80%
Centos Wiki Documentation Forums
Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers
Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID
Overview Ext Id Sources Network Devices Endpoint Classification Node Config Feeds Manual Scans Policy Elements Profiling Policies Policy Sets Troubleshoot Reports Settings Dictionaries
Profiling
Profiling Policies
Logical Profiles
>
&lt;
>>
&lt;&lt;
Save Reset
Total 0
Show All

Logical Profiles List > window

Logical Profile

* Name: window
Description:

* Policy Assignment

Available Policies:
2Wire-Device
3Com-Device
Aastra-Device
Aastra-IP-Phone
Aerohive-Access-Point
Aerohive-Device
American-Power-Conversion-Device
Android

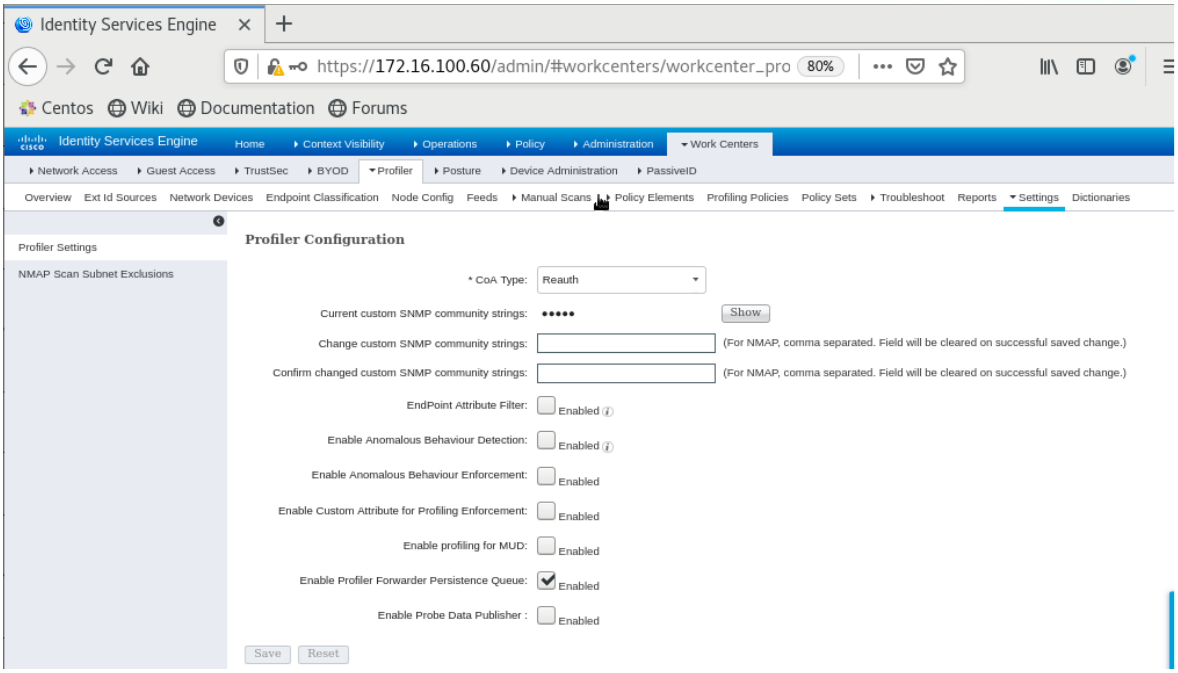
Assigned Policies:
Windows10-Workstation
Workstation

Logical Profiles

Endpoints in Logical Profile

Endpoint policy	MAC Address	IP Address
No data available		

Điều chỉnh CoA thành Reauth để phân quyền lại thiết bị khi phân loại được thiết bị đó Work Centers->Settings->Profiler Settings


Identity Services Engine
https://172.16.100.60/admin/#workcenters/workcenter_pro 80%
Centos Wiki Documentation Forums
Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers
Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID
Overview Ext Id Sources Network Devices Endpoint Classification Node Config Feeds Manual Scans Policy Elements Profiling Policies Policy Sets Troubleshoot Reports Settings Dictionaries
Profiler Settings
NMAP Scan Subnet Exclusions

Profiler Configuration

* CoA Type: Reauth

Current custom SNMP community strings: ••••• Show

Change custom SNMP community strings: (For NMAP, comma separated. Field will be cleared on successful saved change.)

Confirm changed custom SNMP community strings: (For NMAP, comma separated. Field will be cleared on successful saved change.)

EndPoint Attribute Filter: □ Enabled

Enable Anomalous Behaviour Detection: □ Enabled

Enable Anomalous Behaviour Enforcement: □ Enabled

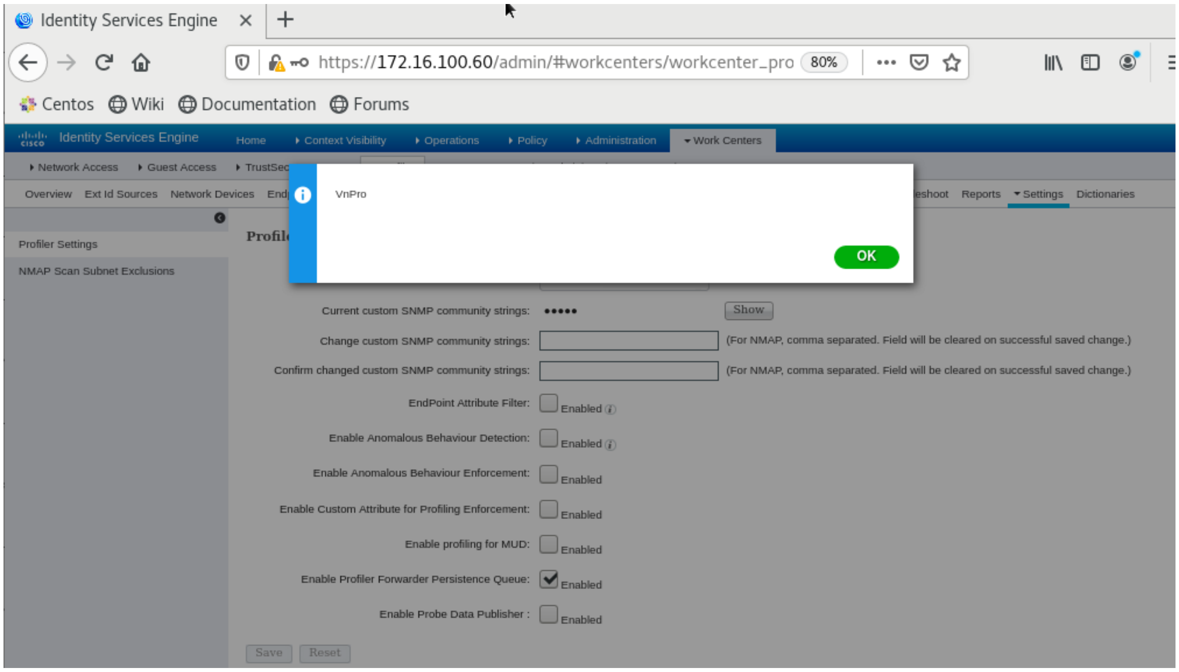
Enable Custom Attribute for Profiling Enforcement: □ Enabled

Enable profiling for MUD: □ Enabled

Enable Profiler Forwarder Persistence Queue: ☑ Enabled

Enable Probe Data Publisher : □ Enabled

Thay đổi SNMP string thành VnPro


Identity Services Engine
https://172.16.100.60/admin/#workcenters/workcenter_pro 80%
Centos Wiki Documentation Forums
Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers
Network Access Guest Access TrustSec
Overview Ext Id Sources Network Devices End
Troubleshoot Reports Settings Dictionaries
Profiler Settings
NMAP Scan Subnet Exclusions

VnPro

Current custom SNMP community strings: ••••• Show

Change custom SNMP community strings: (For NMAP, comma separated. Field will be cleared on successful saved change.)

Confirm changed custom SNMP community strings: (For NMAP, comma separated. Field will be cleared on successful saved change.)

EndPoint Attribute Filter: □ Enabled

Enable Anomalous Behaviour Detection: □ Enabled

Enable Anomalous Behaviour Enforcement: □ Enabled

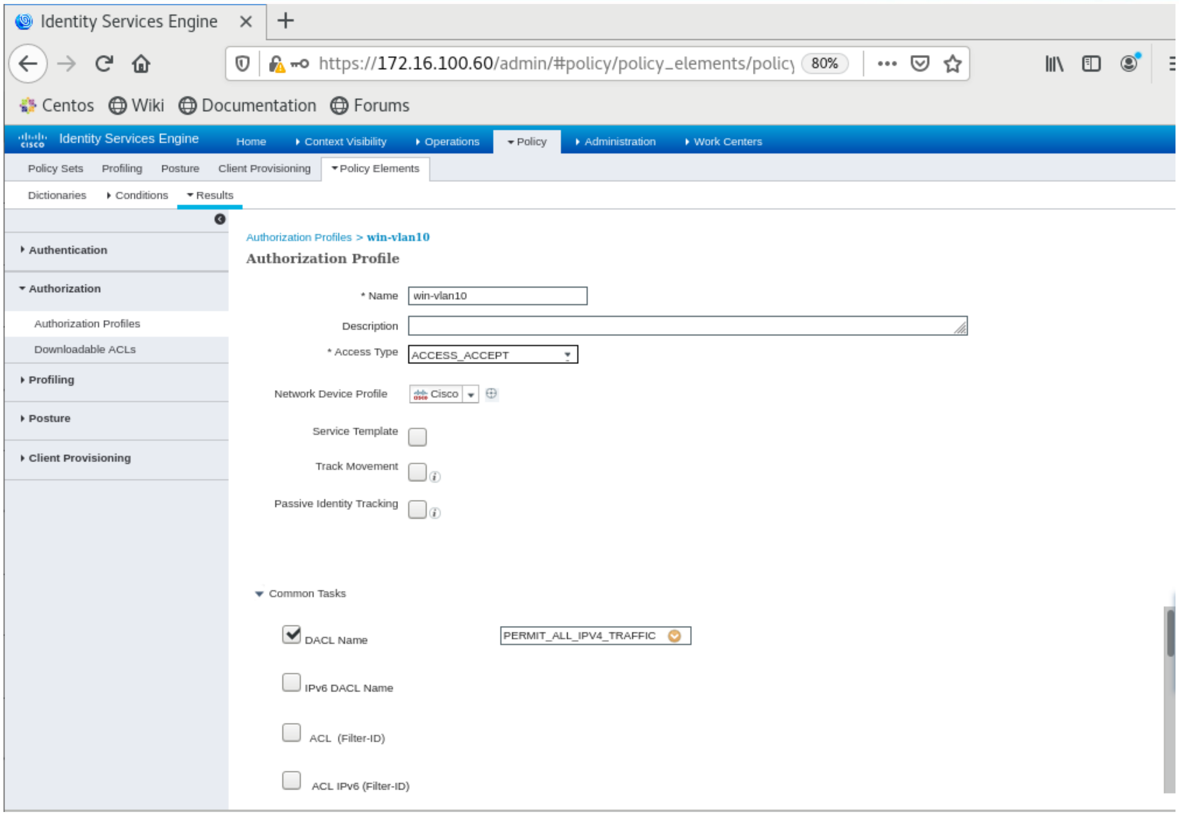
Enable Custom Attribute for Profiling Enforcement: □ Enabled

Enable profiling for MUD: □ Enabled

Enable Profiler Forwarder Persistence Queue: ☑ Enabled

Enable Probe Data Publisher : □ Enabled

Tạo Authorization profile cho vlan 10 và vlan 20 Policy->Results->Authorization->Authorization Profiles->Add



Authorization Profiles > win-vlan10

Authorization Profile

* Name: win-vlan10

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

Passive Identity Tracking □

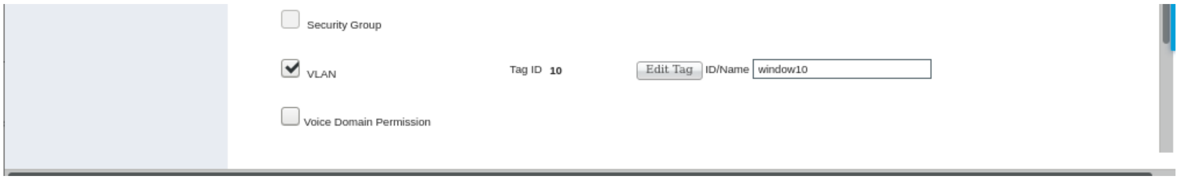
Common Tasks

☑ DACL Name: PERMIT_ALL_IPV4_TRAFFIC

□ IPv6 DACL Name

□ ACL (Filter-ID)

□ ACL IPv6 (Filter-ID)

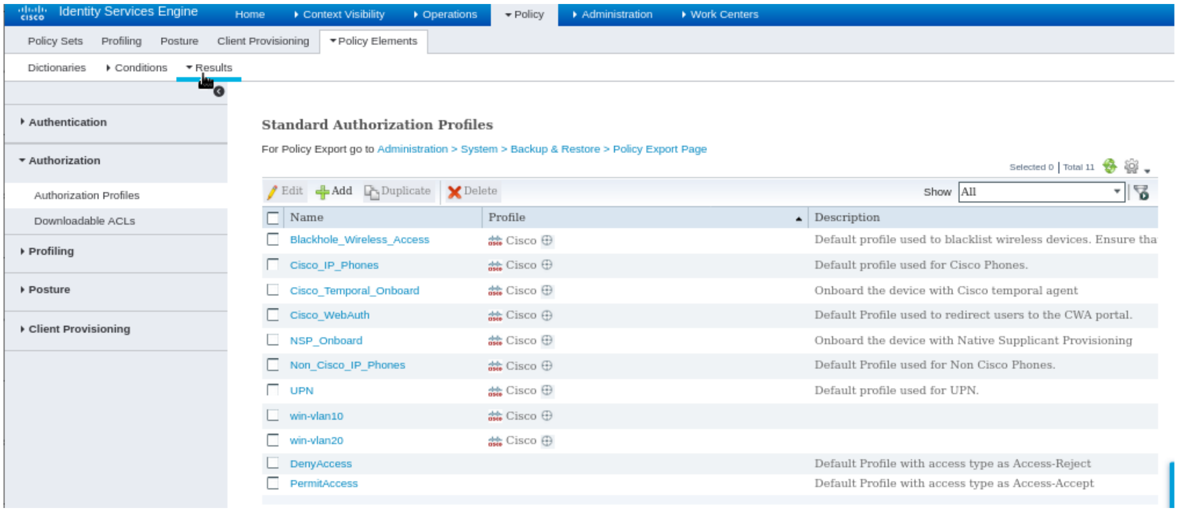


□ Security Group

☑ VLAN Tag ID 10 Edit Tag ID/Name: window10

□ Voice Domain Permission

Làm tương tự cho vlan 20

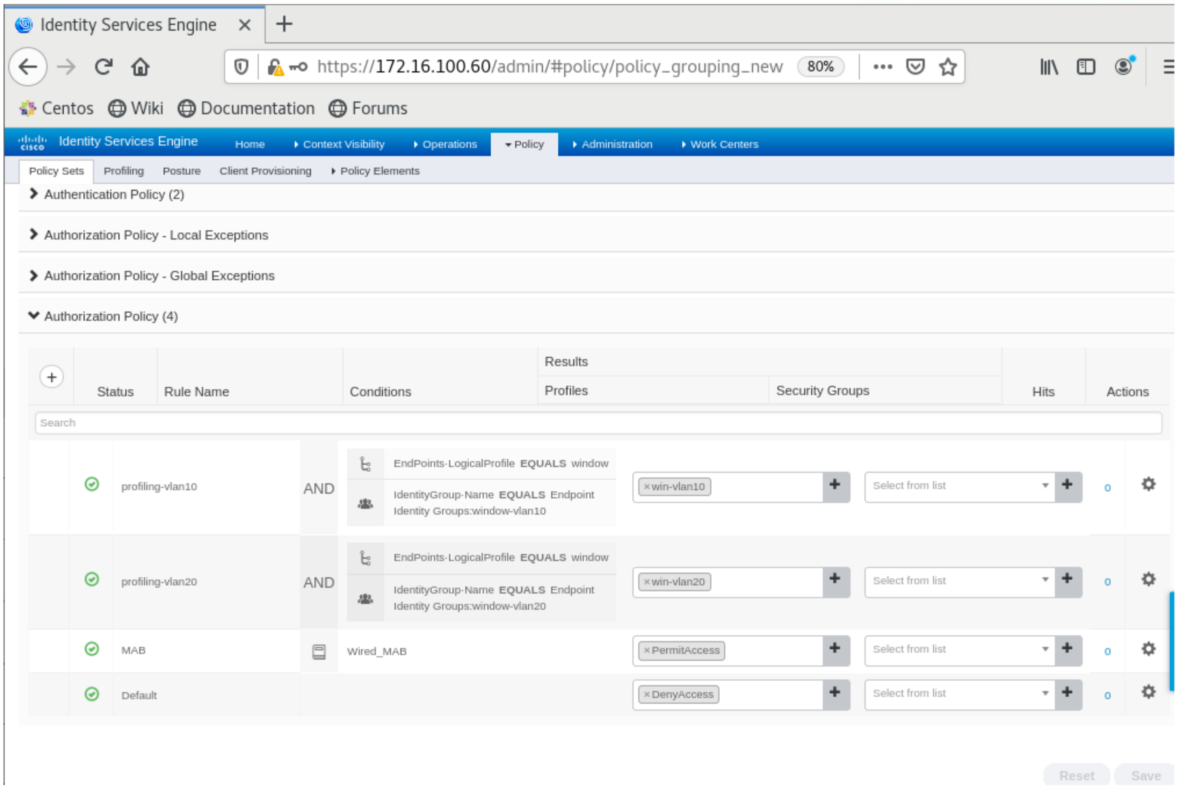


Standard Authorization Profiles

For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Name	Profile	Description
Blackhole_Wireless_Access	Cisco	Default profile used to blacklist wireless devices. Ensure tha
Cisco_IP_Phones	Cisco	Default profile used for Cisco Phones.
Cisco_Temporal_Onboard	Cisco	Onboard the device with Cisco temporal agent
Cisco_WebAuth	Cisco	Default Profile used to redirect users to the CWA portal.
NSP_Onboard	Cisco	Onboard the device with Native Supplicant Provisioning
Non_Cisco_IP_Phones	Cisco	Default Profile used for Non Cisco Phones.
UPN	Cisco	Default profile used for UPN.
win-vlan10	Cisco	
win-vlan20	Cisco	
DenyAccess		Default Profile with access type as Access-Reject
PermitAccess		Default Profile with access type as Access-Accept

Thay đổi lại authorization cho MAB



Status	Rule Name	Conditions		Results: Profiles	Results: Security Groups	Hits	Actions
✓	profiling-vlan10	AND	EndPoints·LogicalProfile **EQUALS** window IdentityGroup·Name **EQUALS** Endpoint Identity Groups:window-vlan10	× win-vlan10	Select from list	0	⚙
✓	profiling-vlan20	AND	EndPoints·LogicalProfile **EQUALS** window IdentityGroup·Name **EQUALS** Endpoint Identity Groups:window-vlan20	× win-vlan20	Select from list	0	⚙
✓	MAB		Wired_MAB	× PermitAccess	Select from list	0	⚙
✓	Default			× DenyAccess	Select from list	0	⚙

Kiểm Tra:

Kiểm tra phần MAB:

```
SW1#show mab all
MAB details for Ethernet0/1
-------------------------------------
Mac-Auth-Bypass           = Enabled

MAB details for Ethernet1/0
-------------------------------------
Mac-Auth-Bypass           = Enabled

SW1#show mab all ?
  details  Show MAB details for all interfaces
  summary  Show MAB summary for all interfaces
  |        Output modifiers
  <cr>
```

```
SW1#show mab all details
MAB details for Ethernet0/1
-------------------------------------
Mac-Auth-Bypass           = Enabled


MAB Client List Is Empty


MAB details for Ethernet1/0
-------------------------------------
Mac-Auth-Bypass           = Enabled


MAB Client List Is Empty
```

Kiểm tra phần 802.1x:

```
SW1#show dot1x all details
Sysauthcontrol             Disabled
Dot1x Protocol Version            3


Dot1x Info for Ethernet0/1
-----------------------------------
PAE                       = AUTHENTICATOR
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 10


Dot1x Authenticator Client List Empty


Port Status               = AUTHORIZED
Dot1x Info for Ethernet1/0
-----------------------------------
PAE                       = AUTHENTICATOR
```

```
QuietPeriod                = 60
ServerTimeout              = 0
SuppTimeout                = 30
ReAuthMax                  = 2

MaxReq                     = 2
TxPeriod                   = 10

Dot1x Authenticator Client List Empty

Port Status                = AUTHORIZED
```

Kiểm tra thông tin radius server:

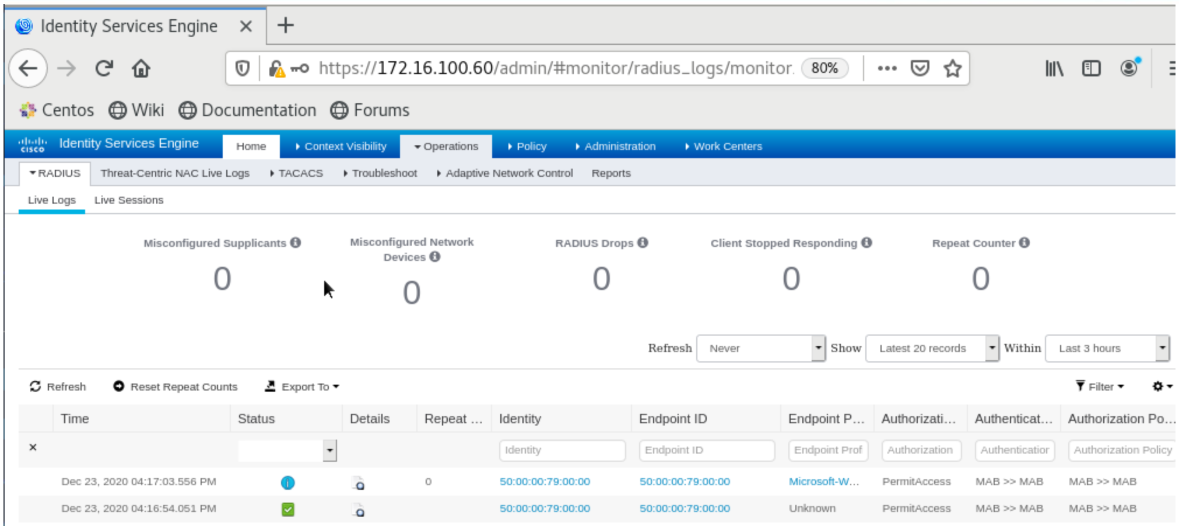
```
SW1#show radius server-group all
Server group radius
    Sharecount = 1  sg_unconfigured = FALSE
    Type = standard  Memlocks = 1
    Server(172.16.100.60:1645,1646) Transactions:
    Authen: 0   Author: 0       Acct: 0
    Server_auto_test_enabled: FALSE
     Keywrap enabled: FALSE
Server group ISE-RADIUS
    Sharecount = 1  sg_unconfigured = FALSE
    Type = standard  Memlocks = 1
    Server(172.16.100.60:1645,1646) Transactions:
    Authen: 11  Author: 1       Acct: 13
    Server_auto_test_enabled: FALSE
     Keywrap enabled: FALSE
```

Kiểm tra authetication sessions:

```
SW1#show authentication sessions

Interface    Identifier     Method  Domain  Status Fg Session ID
Et1/0        8449.153c.f5da N/A     DATA    Auth
AC1001010000001300777CF1
```

```
Et0/1        5000.0079.0000 N/A      DATA    Auth
AC10010100000014007B5B3C


Session count = 2


Key to Session Events Blocked Status Flags:


  A - Applying Policy (multi-line status for details)

  D - Awaiting Deletion

  F - Final Removal in progress

  I - Awaiting IIF ID allocation

  N - Waiting for AAA to come up

  P - Pushed Session

  R - Removing User Profile (multi-line status for details)

  U - Applying User Profile (multi-line status for details)

  X - Unknown Blocker


SW1#show vlan br


VLAN Name                             Status    Ports

---- -------------------------------- --------- ------------------------

1    default                          active    Et1/1, Et1/2, Et1/3

10   window10                         active    Et0/1

20   window20                         active    Et1/0

100  window100                        active    Et0/0, Et0/3

1002 fddi-default                     act/unsup

1003 token-ring-default               act/unsup

1004 fddinet-default                  act/unsup

1005 trnet-default                    act/unsup
```

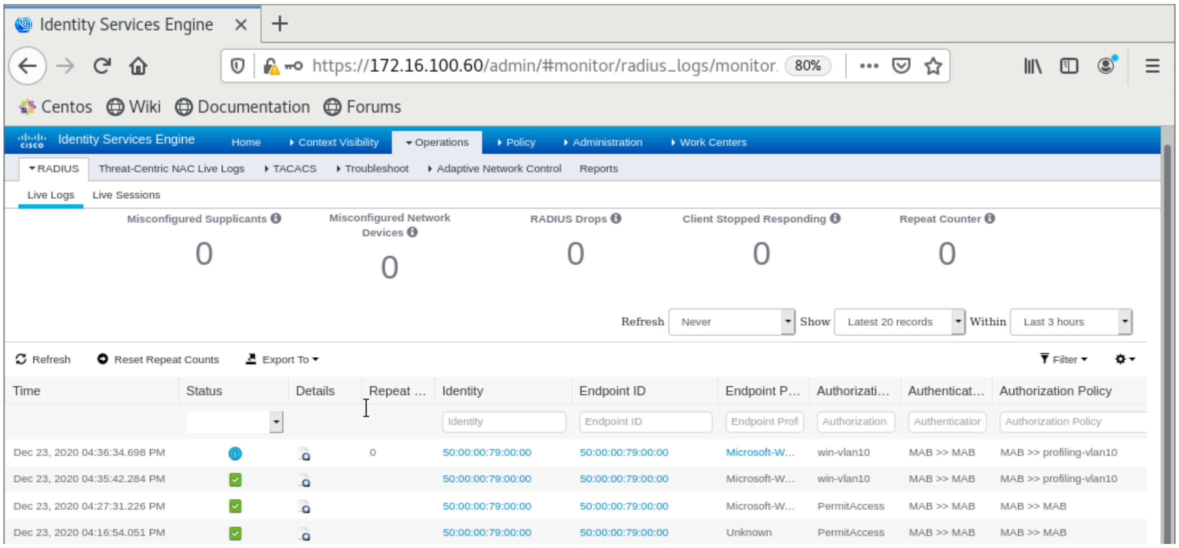
Ta thấy author profiles thay đổi từ MAB sang profiling-vlan10



Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	0	0	0

Refresh Never Show Latest 20 records Within Last 3 hours

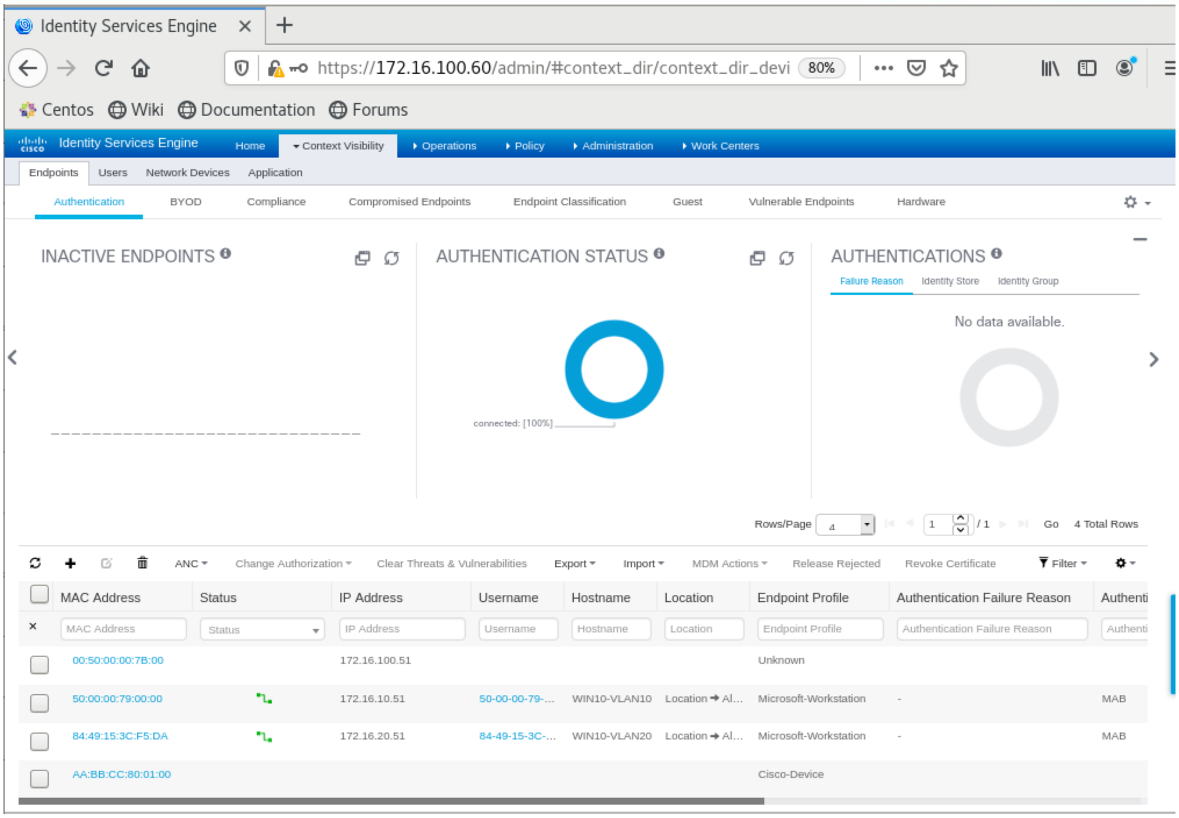
Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authorizati...	Authenticat...	Authorization Po...
Dec 23, 2020 04:17:03.556 PM	●		0	50:00:00:79:00:00	50:00:00:79:00:00	Microsoft-W...	PermitAccess	MAB >> MAB	MAB >> MAB
Dec 23, 2020 04:16:54.051 PM	✓			50:00:00:79:00:00	50:00:00:79:00:00	Unknown	PermitAccess	MAB >> MAB	MAB >> MAB



Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	0	0	0

Refresh Never Show Latest 20 records Within Last 3 hours

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authorizati...	Authenticat...	Authorization Policy
Dec 23, 2020 04:36:34.698 PM	●		0	50:00:00:79:00:00	50:00:00:79:00:00	Microsoft-W...	win-vlan10	MAB >> MAB	MAB >> profiling-vlan10
Dec 23, 2020 04:35:42.284 PM	✓			50:00:00:79:00:00	50:00:00:79:00:00	Microsoft-W...	win-vlan10	MAB >> MAB	MAB >> profiling-vlan10
Dec 23, 2020 04:27:31.226 PM	✓			50:00:00:79:00:00	50:00:00:79:00:00	Microsoft-W...	PermitAccess	MAB >> MAB	MAB >> MAB
Dec 23, 2020 04:16:54.051 PM	✓			50:00:00:79:00:00	50:00:00:79:00:00	Unknown	PermitAccess	MAB >> MAB	MAB >> MAB



MAC Address	Status	IP Address	Username	Hostname	Location	Endpoint Profile	Authentication Failure Reason	Authenti
00:50:00:00:7B:00		172.16.100.51				Unknown		
50:00:00:79:00:00		172.16.10.51	50-00-00-79-...	WIN10-VLAN10	Location ➔ Al...	Microsoft-Workstation	-	MAB
84:49:15:3C:F5:DA		172.16.20.51	84-49-15-3C-...	WIN10-VLAN20	Location ➔ Al...	Microsoft-Workstation	-	MAB
AA:BB:CC:80:01:00						Cisco-Device		

Cấu hình đầy đủ:

Router:

```
ip dhcp excluded-address 172.16.1.1 172.16.1.50

ip dhcp excluded-address 172.16.10.1 172.16.10.50

ip dhcp excluded-address 172.16.100.1 172.16.100.50

ip dhcp excluded-address 172.16.20.1 172.16.20.50

!

ip dhcp pool vlan1

 network 172.16.1.0 255.255.255.0

 default-router 172.16.1.1

 dns-server 8.8.8.8 8.8.4.4

!

ip dhcp pool vlan10

 network 172.16.10.0 255.255.255.0

 default-router 172.16.10.1

 dns-server 8.8.8.8 8.8.4.4

!
```

```
ip dhcp pool vlan100
 network 172.16.100.0 255.255.255.0
 dns-server 8.8.8.8 8.8.4.4
 default-router 172.16.100.1
!
ip dhcp pool vlan20
 network 172.16.20.0 255.255.255.0
 default-router 172.16.20.1
 dns-server 8.8.8.8 8.8.4.4
!
interface Ethernet0/0
 ip address dhcp
 ip nat outside
 ip virtual-reassembly in
!
interface Ethernet0/2
 ip address 172.16.1.2 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
!
ip nat inside source list 1 interface Ethernet0/0 overload
ip route 172.16.0.0 255.255.0.0 172.16.1.1
!
access-list 1 permit any
```

SW1:

```
hostname SW1
!
aaa new-model
!
aaa group server radius ISE-RADIUS
 server name ise-radius
!
aaa authentication dot1x default group ISE-RADIUS local
aaa authorization network default group ISE-RADIUS local
aaa accounting dot1x default start-stop group ISE-RADIUS
!
interface Ethernet0/0
 switchport access vlan 100
!
interface Ethernet0/1
 switchport mode access
 authentication host-mode multi-auth
 authentication order mab dot1x
 authentication priority dot1x mab
 authentication port-control auto
 authentication periodic
 authentication timer reauthenticate server
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 10
 spanning-tree portfast edge
!
interface Ethernet0/3
 switchport access vlan 100
!
interface Ethernet1/0
 switchport mode access
 authentication host-mode multi-auth
 authentication order mab dot1x
 authentication priority dot1x mab
 authentication port-control auto
 authentication periodic
 authentication timer reauthenticate server
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 10
 spanning-tree portfast edge
```

```
!
interface Vlan1
 ip address 172.16.1.1 255.255.255.0
 ip helper-address 172.16.100.60
 ip helper-address 172.16.1.2
!
interface Vlan10
 ip address 172.16.10.1 255.255.255.0
 ip helper-address 172.16.100.60
 ip helper-address 172.16.1.2
!
interface Vlan20
 ip address 172.16.20.1 255.255.255.0
 ip helper-address 172.16.100.60
 ip helper-address 172.16.1.2
!
interface Vlan100
 ip address 172.16.100.1 255.255.255.0
 ip helper-address 172.16.100.60
 ip helper-address 172.16.1.2
!
ip route 0.0.0.0 0.0.0.0 172.16.1.2
!
snmp-server community VnPro RO
snmp-server trap-source Vlan1
snmp-server source-interface informs Vlan1
snmp-server enable traps snmp authentication linkdown linkup coldstart
warmstart
snmp-server host 172.16.100.60 version 2c VnPro  snmp
!
radius server ise-radius
 address ipv4 172.16.100.60 auth-port 1645 acct-port 1646
 key VnPro123
```