DACL'S AND VLAN ASSIGNMENT

CONTENTS

REQUIREMENTS

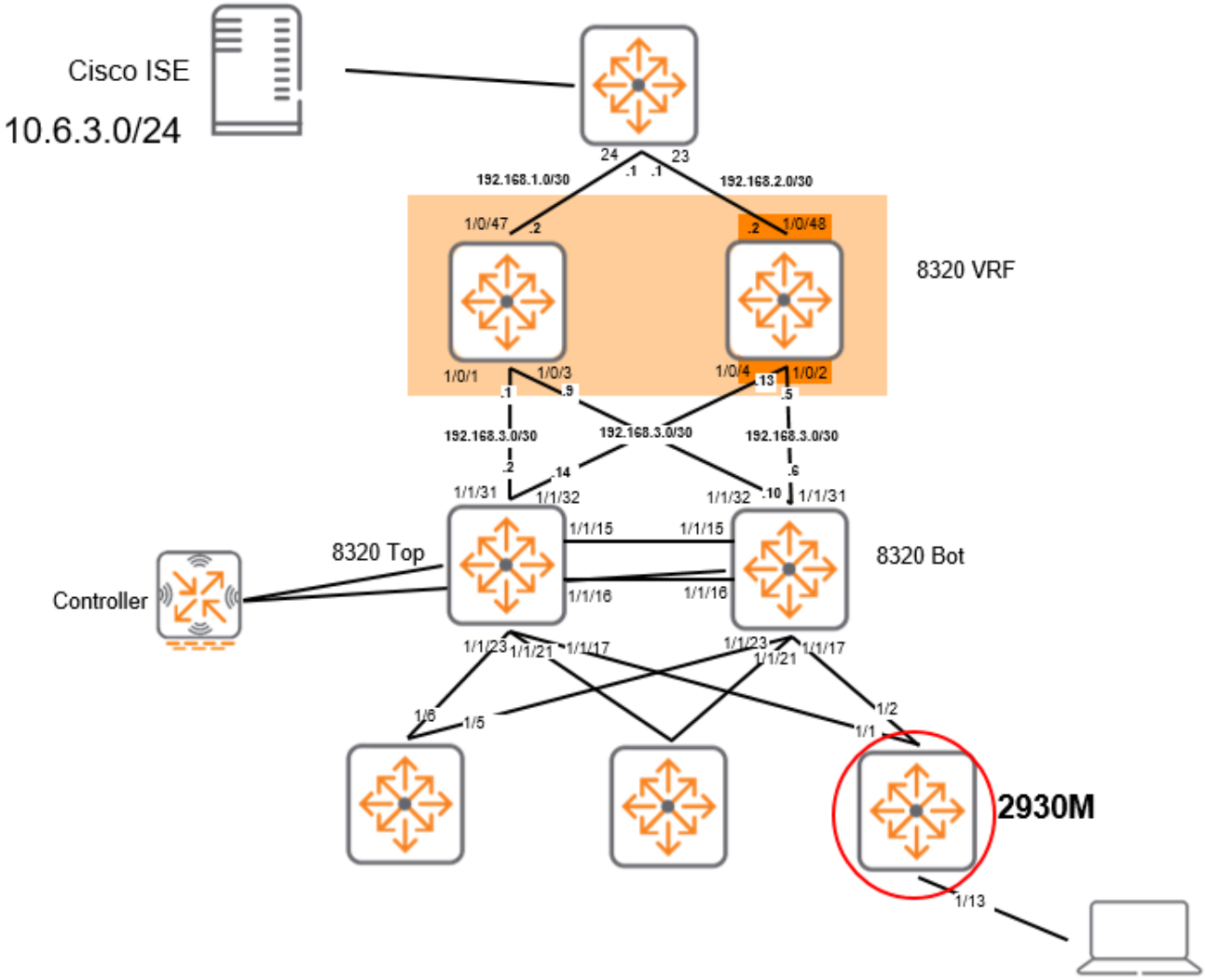
- Aruba Switch (2930M/F, 3810M, 5400)
- Cisco ISE (2.3 And Above)

OVERVIEW

This document will cover downloadable ACL's (DACL) and VLAN assignment using Cisco ISE and ArubaOS-Switch.

For this scenario, we will be creating a Mac Authentication Fallback policy within Cisco ISE to allow guest devices some network connectivity. To do this, we will also need to assign a VLAN and a DACL. This allows these guest devices to access the internet and get a DHCP address. We also need to allow the device to connect to one internal address. The 10.6.3.0/24 subnet is an internal subnet with different services sitting within the subnet such as ISE,DHCP,DNS, etc... We are going to allow the client device to access the 10.6.3.12 address on that subnet, which is a web service, for this deployment. To verify connectivity, we will just ping the address, but we will be allowing IP connectivity so web browsing will work as well.

TOPOLOGY

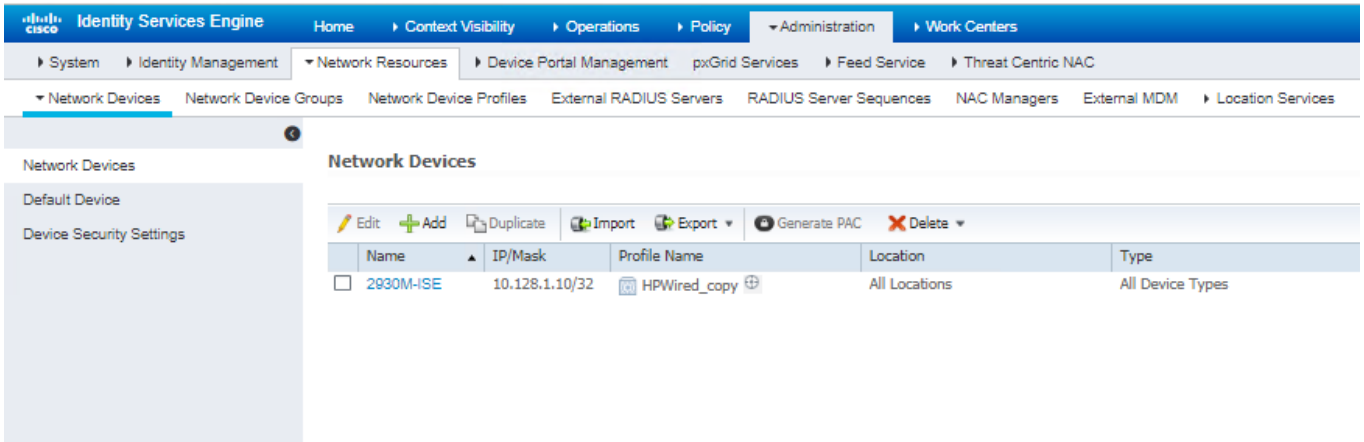

Cisco ISE
10.6.3.0/24
24
23
.1
.1
192.168.1.0/30
192.168.2.0/30
1/0/47
.2
.2
1/0/48
8320 VRF
1/0/1
1/0/3
1/0/4
1/0/2
.1
.9
.13
.5
192.168.3.0/30
192.168.3.0/30
192.168.3.0/30
.2
.14
.6
.10
1/1/31
1/1/32
1/1/32
1/1/31
1/1/15
1/1/15
8320 Top
8320 Bot
Controller
1/1/16
1/1/16
1/1/23
1/1/21
1/1/17
1/1/23
1/1/21
1/1/17
1/6
1/5
1/2
1/1
2930M
1/13

ADDING A DEVICE TO ISE

Description

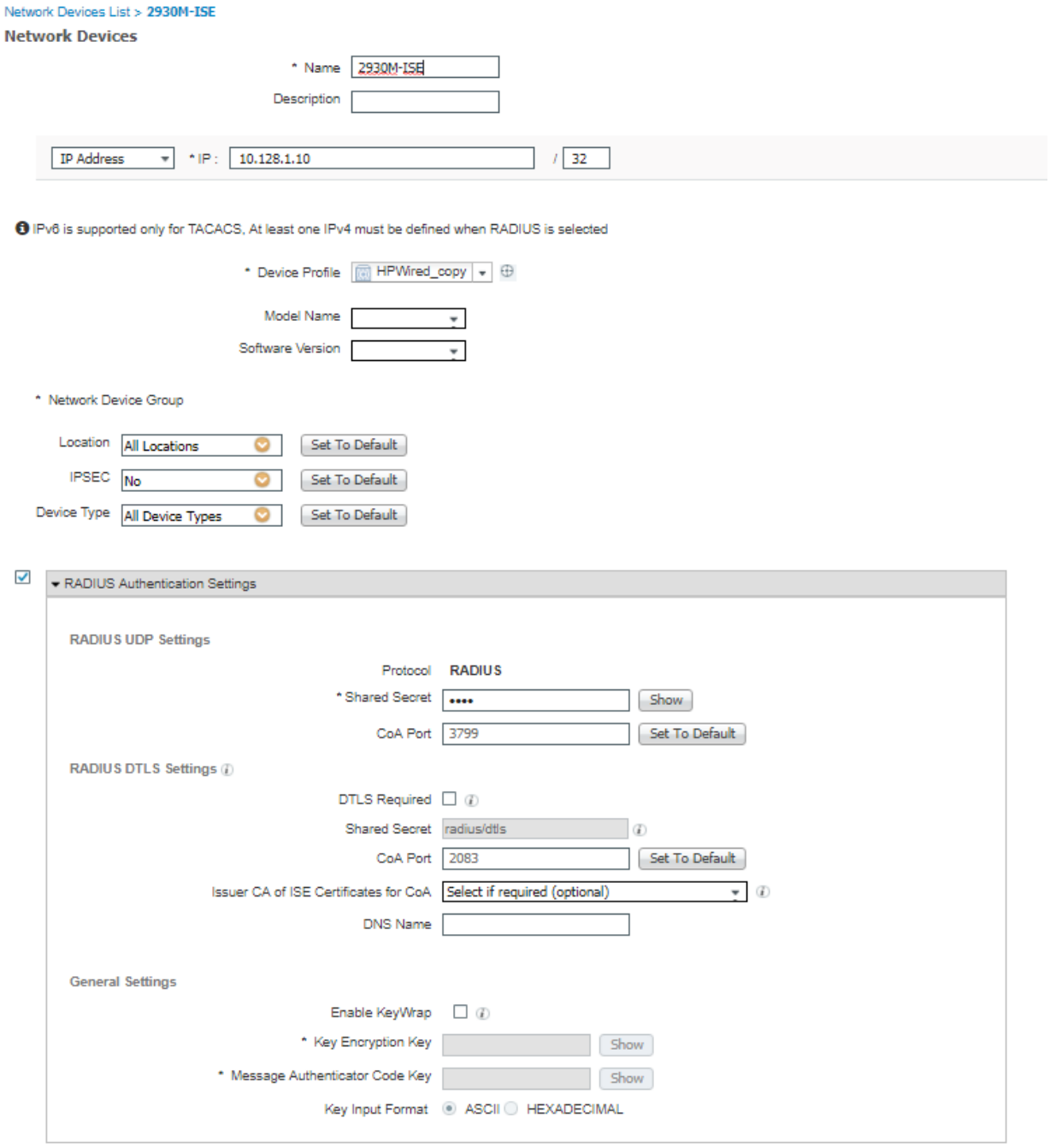
This section will go over adding a device into Cisco ISE.

Navigate to Administration> Network Devices. Click Add.



Enter the IP address, RADIUS shared secret, and model of the switch and select the proper switch profile

Note:In this example a copy of the HPWired Profile “HPWired _Copy” is being used, there is no issues using the default HPWired Profile this will work for DACL’s and Vlan Assignment as well.



Switch Configuration

Pointing the switch to ISE Server

```
radius-server host <Radius-IP> dyn-authorization
radius-server host <Radius-IP> time-window 0
radius-server key < KEY-STR>
```

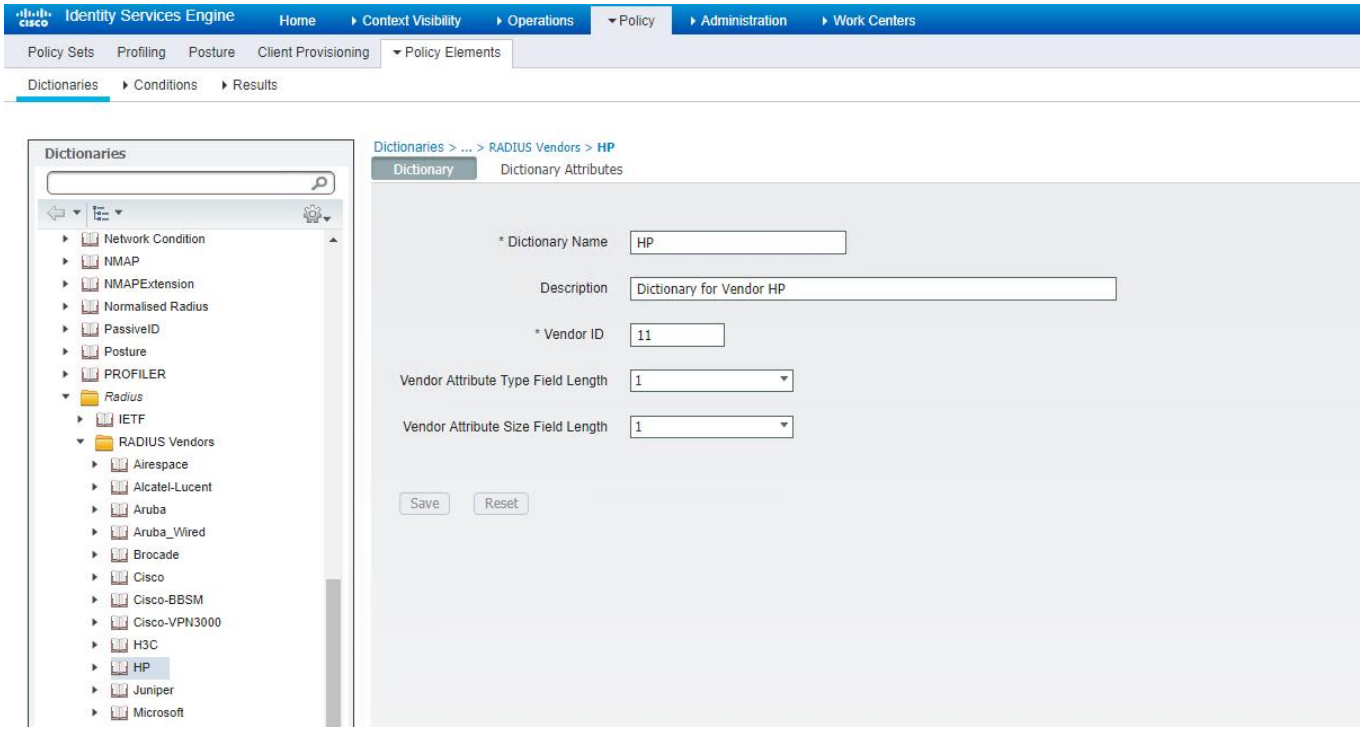
Configuring AAA on the switch for Mac Authentication as a fall back and Configuration for enabling AAA.

```
aaa authentication port-access eap-radius
aaa port-access authenticator <Ports>
aaa port-access authenticator <Ports> client-limit <Limit>
aaa port-access mac-based <Ports> addr-limit <Limit>
aaa port-access mac-based <Ports>
aaa port-access <Ports> auth-order authenticator mac-based
aaa port-access <Ports> auth-priority authenticator mac-based
aaa port-access authenticator active
```

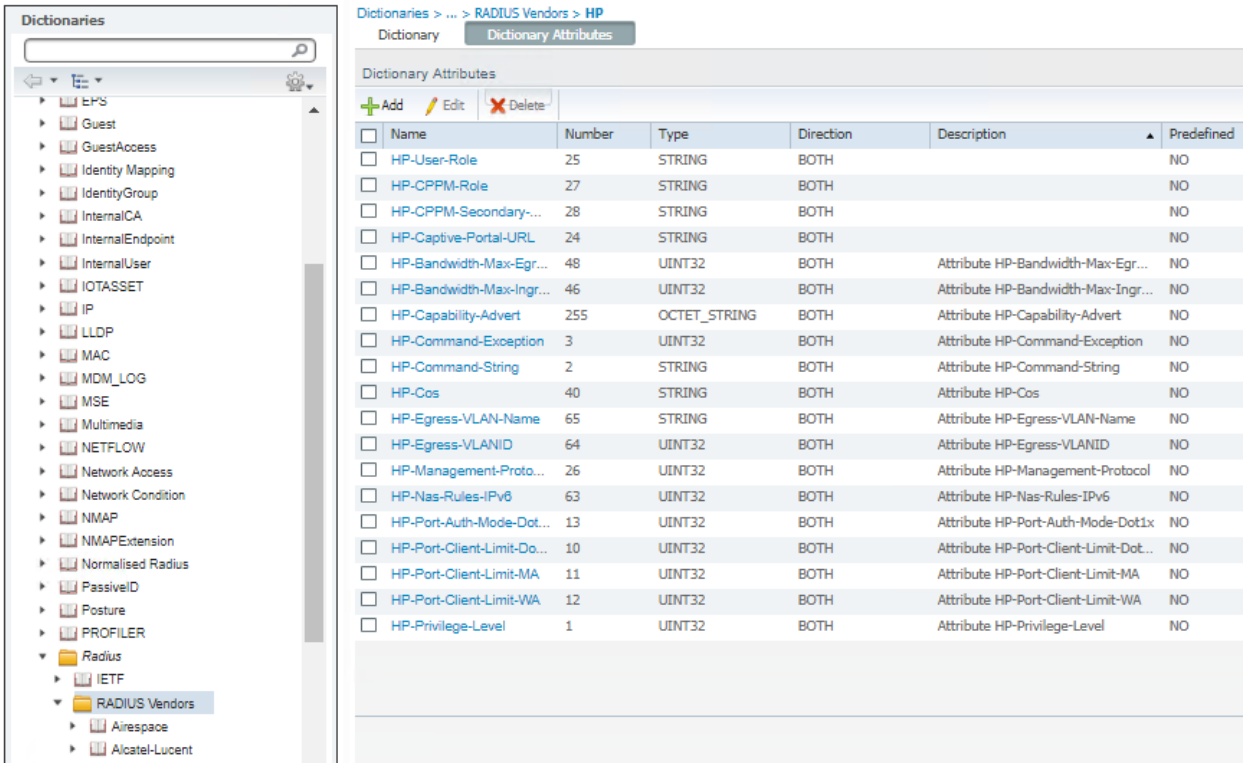
ADDING THE USER ROLE VSA TO THE HP DICTIONARY

Description

This section will guide you through how to add the HP NAS filter rule to ISE.if it is not already there.
To add the VSA, navigate to Policy>Policy Elements then click the “Radius” folder and navigate to the “HP” dictionary within the Radius Vendors Folder.

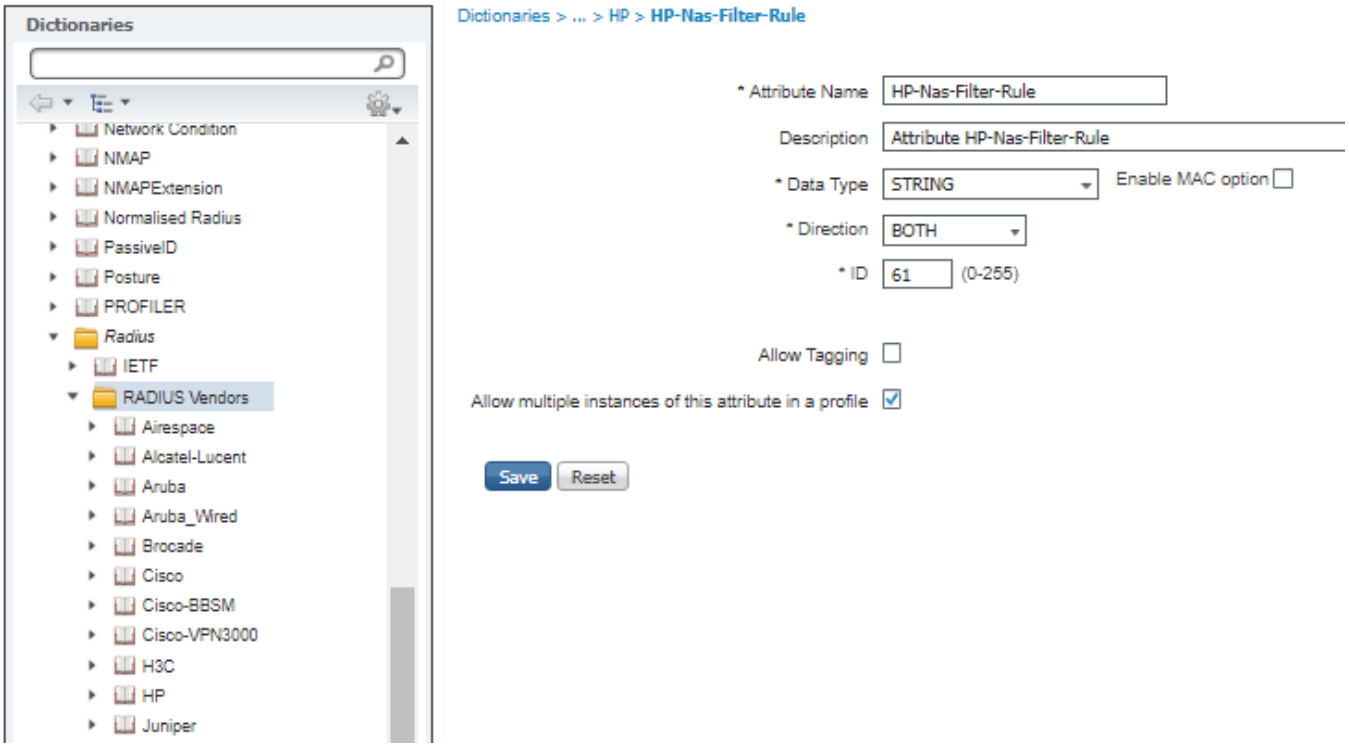


1. Click Dictionary Attributes then click add



Name	Number	Type	Direction	Description	Predefined
HP-User-Role	25	STRING	BOTH		NO
HP-CPPM-Role	27	STRING	BOTH		NO
HP-CPPM-Secondary-...	28	STRING	BOTH		NO
HP-Captive-Portal-URL	24	STRING	BOTH		NO
HP-Bandwidth-Max-Egr...	48	UINT32	BOTH	Attribute HP-Bandwidth-Max-Egr...	NO
HP-Bandwidth-Max-Ingr...	46	UINT32	BOTH	Attribute HP-Bandwidth-Max-Ingr...	NO
HP-Capability-Advert	255	OCTET_STRING	BOTH	Attribute HP-Capability-Advert	NO
HP-Command-Exception	3	UINT32	BOTH	Attribute HP-Command-Exception	NO
HP-Command-String	2	STRING	BOTH	Attribute HP-Command-String	NO
HP-Cos	40	STRING	BOTH	Attribute HP-Cos	NO
HP-Egress-VLAN-Name	65	STRING	BOTH	Attribute HP-Egress-VLAN-Name	NO
HP-Egress-VLANID	64	UINT32	BOTH	Attribute HP-Egress-VLANID	NO
HP-Management-Proto...	26	UINT32	BOTH	Attribute HP-Management-Protocol	NO
HP-Nas-Rules-IPv6	63	UINT32	BOTH	Attribute HP-Nas-Rules-IPv6	NO
HP-Port-Auth-Mode-Dot...	13	UINT32	BOTH	Attribute HP-Port-Auth-Mode-Dot1x	NO
HP-Port-Client-Limit-Do...	10	UINT32	BOTH	Attribute HP-Port-Client-Limit-Dot...	NO
HP-Port-Client-Limit-MA	11	UINT32	BOTH	Attribute HP-Port-Client-Limit-MA	NO
HP-Port-Client-Limit-WA	12	UINT32	BOTH	Attribute HP-Port-Client-Limit-WA	NO
HP-Privilege-Level	1	UINT32	BOTH	Attribute HP-Privilege-Level	NO

2. After clicking the “add dictionary attribute”, enter the information below then click Submit.
   Attribute name: “HP-Nas-Filter-Rule”
   Data type: “String”
   Direction: “Both”
   ID: “61”
   Be sure to have the “Allow Multiple Instances of this in a Profile” Box checked.

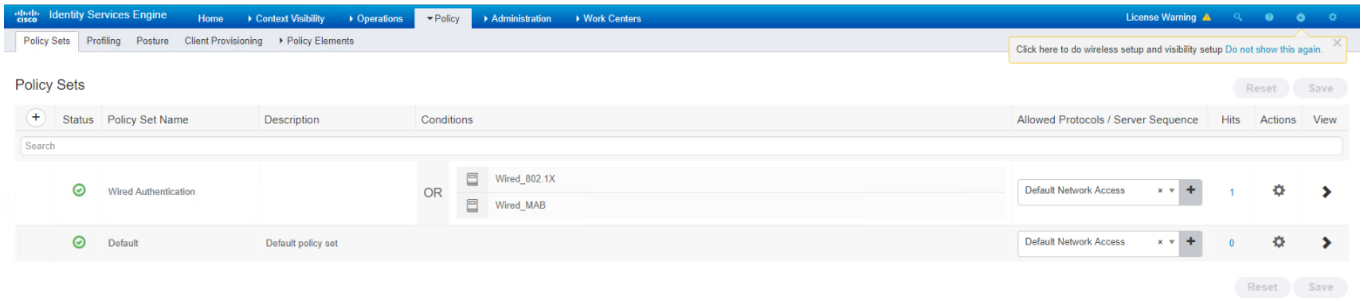


USING DACL'S AND VLAN ASSIGNMENT VSA'S

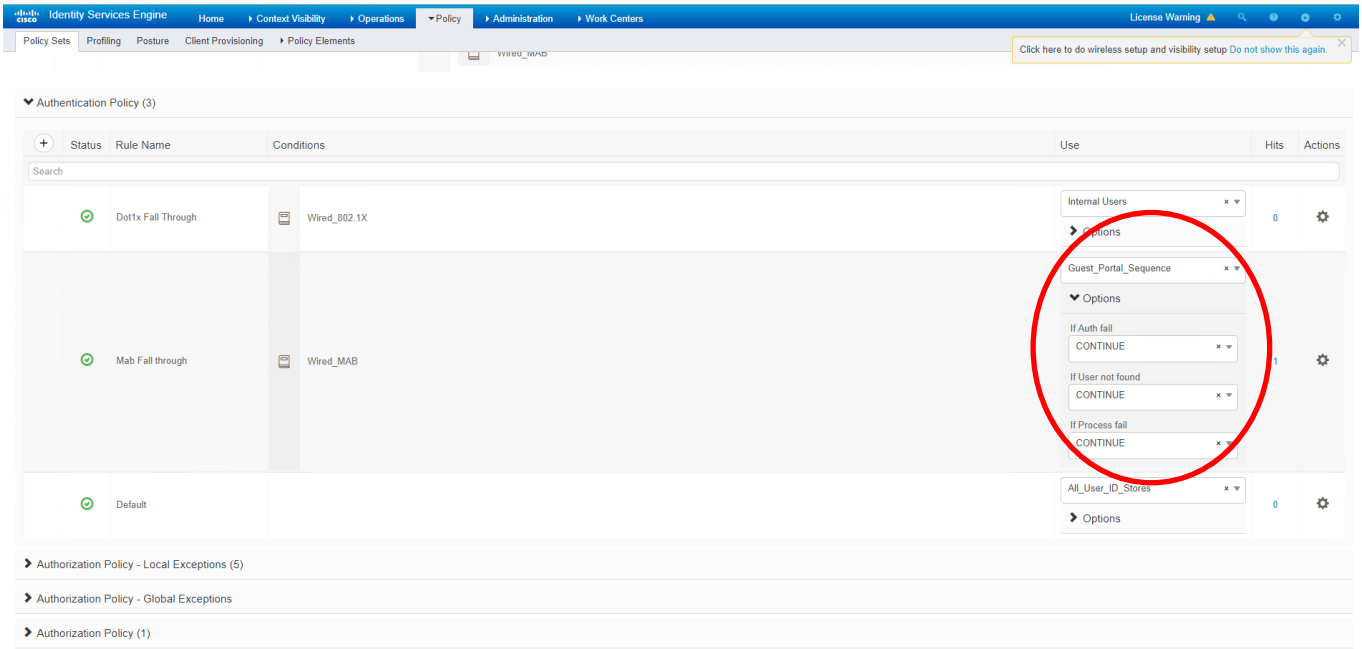
Description

This section will go over how to use the VSA in a Policy Set in ISE, however this will not cover how to create a policy set in ISE.

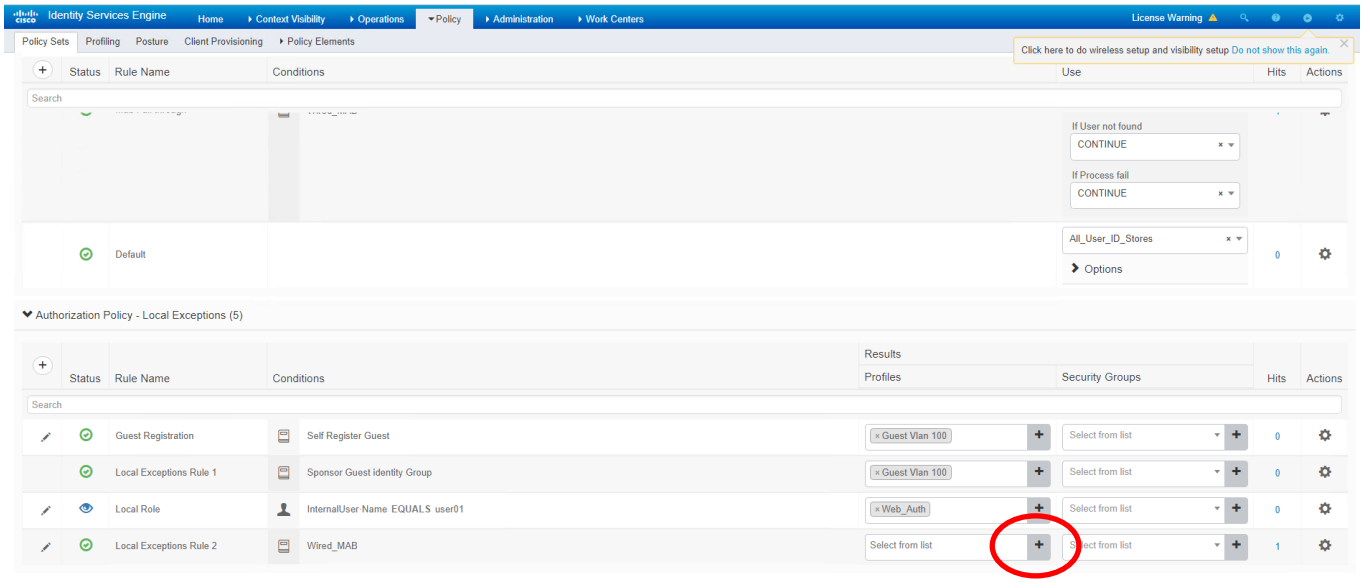
1. Now that the NAS Filter VSA is defined in ISE, it can now be used Navigate to Policy>Policy Sets and edit a policy for your environment. Click the Arrow “>” to go into the policy set .



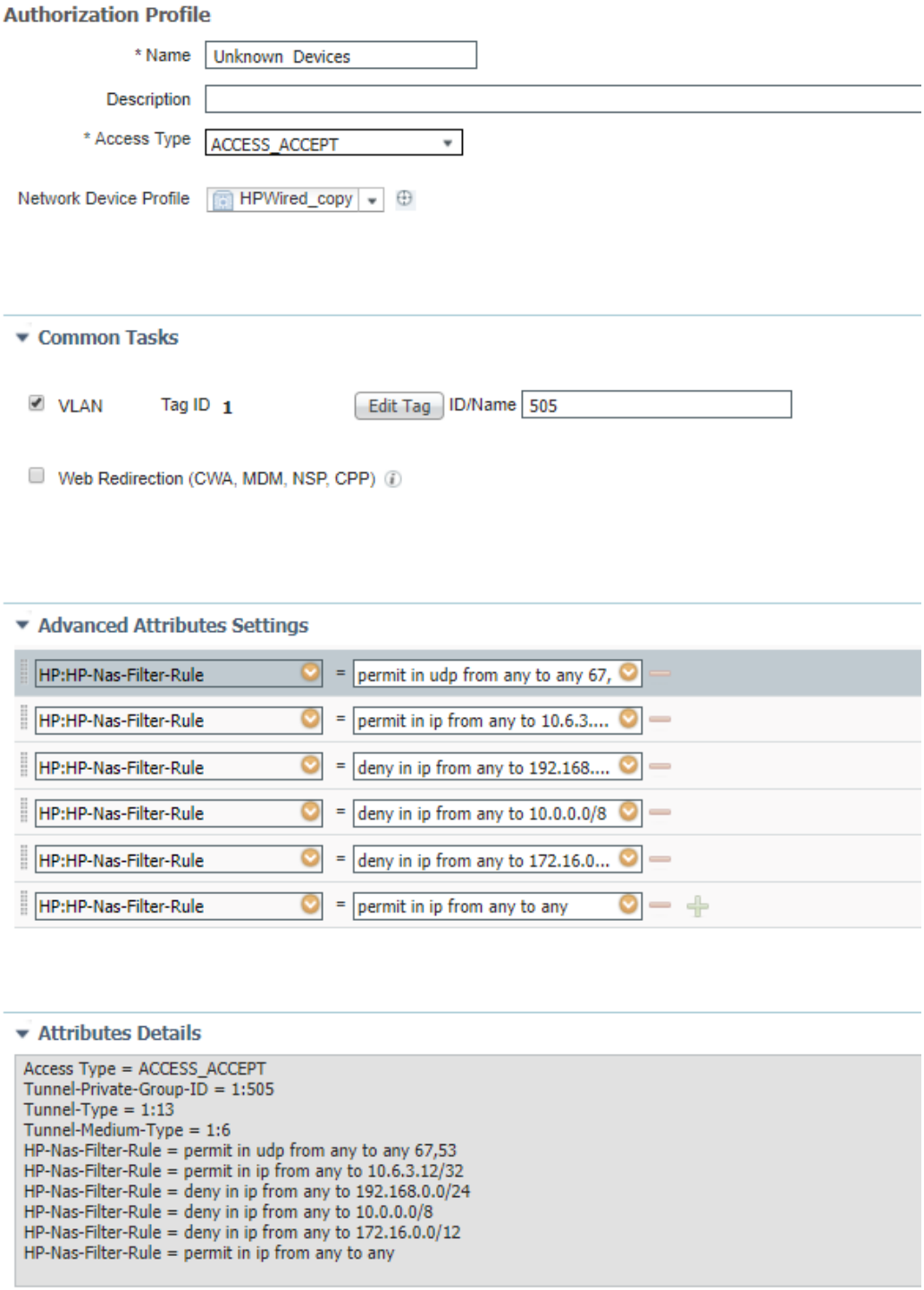
2. Under the “Policy Set”, in this example, there is a “MAB Fall Through” configured. This allows devices that are not in the ISE Authentication databases sources to have some level of network connectivity. This is done by allowing devices that have failed to authenticate against any of the data bases to continue to an authorization policy



3. Next, there needs to be an “Authorization Rule” configured that matches based on MAB. We will specify a profile for the Authorization rule, to do this ,click the “+” button to create a new authorization profile.



4. A pop up should appear and here the authorization rule can be configured. Below Is the configuration of the Authorization profile



5. Once the profile is configured, it can be selected in the “Authorization Rule” as a profile. After this is complete, the policy configuration is ready to test

VERIFICATION

1. Using the “Show Port-Access Clients Detail” command the switch will display the details of a session, it will also display the DACL that was configured in ISE.

172.16.8.5 - PuTTYNG

```
 URL              :


Client Base Details :
 Port             : 1/13                  Authentication Type : mac-based
 Client Status    : authenticated         Session Time        : 322 seconds
 Client Name      : 00-50-B6-79-BD-AC     Session Timeout     : 0 seconds
 MAC Address      : 0050b6-79bdac
 IP               : n/a

Access Policy Details :
 COS Map          : Not Defined           In Limit Kbps       : Not Set
 Untagged VLAN    : 505                   Out Limit Kbps      : Not Set
 Tagged VLANs     : No Tagged VLANs
 Port Mode        : 100FDx
 RADIUS ACL List :
    permit in udp from any to any 67,53
    permit in ip from any to 10.6.3.12/32
    deny in ip from any to 192.168.0.0/24
    deny in ip from any to 10.0.0.0/8
    deny in ip from any to 172.16.0.0/12
    permit in ip from any to any
 Auth Order       : 8021x, Mac-Auth
 Auth Priority    : 8021x, Mac-Auth
 LMA Fallback     : Disabled
```

2. The Client will not be able to ping the devices we would like as well.

Command Prompt

```
   Connection-specific DNS Suffix  . : compserver.lab
   Link-local IPv6 Address . . . . . : fe80::11ce:2ae:535c:688%18
   IPv4 Address. . . . . . . . . . . : 10.96.55.12
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.96.55.254

Tunnel adapter isatap.{D71274A1-E2B8-4E69-B602-9AE3DFDB8799}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter isatap.{62B03CFE-59FA-4DF6-B32A-51CE484D1C41}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter isatap.compserver.lab:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : compserver.lab

C:\Users\Admin>ping 10.96.55.254

Pinging 10.96.55.254 with 32 bytes of data:
Request timed out.

Ping statistics for 10.96.55.254:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
Control-C
^C
C:\Users\Admin>ping 10.6.3.12

Pinging 10.6.3.12 with 32 bytes of data:
Reply from 10.6.3.12: bytes=32 time<1ms TTL=124
Reply from 10.6.3.12: bytes=32 time<1ms TTL=124

Ping statistics for 10.6.3.12:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

3. In ISE Navigate to Operations>Radius> Live logs and you will be able to see the client's authentication. To see more detail, click the magnifying glass on one of the entries

Mar 11, 2019 08:05:15.818 PM			3	00:50:B6:79:BD:AC	00:50:B6:79:BD:AC	Unknown	Wired Authentication >> Mab ...	Wired Authentication >> Local Exc...	Unknown_Devices	
Mar 11, 2019 08:00:27.807 PM				00:50:B6:79:BD:AC	00:50:B6:79:BD:AC	Unknown	Wired Authentication >> Mab ...	Wired Authentication >> Local Exc...	Unknown_Devices	2930M-ISE
Mar 11, 2019 07:55:15.982 PM				user01	A0:CE:C8:02:A9:48	Unknown	Wired Authentication >> Dot1...	Wired Authentication >> Default	DenyAccess	2930M-ISE
Mar 11, 2019 07:45:15.815 PM				user01	A0:CE:C8:02:A9:48	Unknown	Wired Authentication >> Dot1...	Wired Authentication >> Default	DenyAccess	2930M-ISE

After clicking the magnifying glass, the results of the Radius authentication will display.

Name	Endpoint Identity Groups:Unknown
RADIUS Username	00:50:B6:79:BD:AC
NAS-Identifier	2930M-ISE
Device IP Address	10.128.1.10
Called-Station-ID	F4:03:43:DE:47:73

Result

User-Name	00-50-B6-79-BD-AC
State	ReauthSession:0a06030fujvrkNNpxXHRed7Hj_mJGPZbiamPLdyo0gx8fici15w
Class	CACS:0a06030fujvrkNNpxXHRed7Hj_mJGPZbiamPLdyo0gx8fici15w:ISE-Comp/341383157/30
Tunnel-Type	(tag=1) VLAN
Tunnel-Medium-Type	(tag=1) 802
Tunnel-Private-Group-ID	(tag=1) 505
LicenseTypes	Base license consumed
HP-Nas-Filter-Rule	permit in ip from any to any 53,67
HP-Nas-Filter-Rule	permit in ip from any to 10.6.3.12/32
HP-Nas-Filter-Rule	deny in ip from any to 192.168.0.0/24
HP-Nas-Filter-Rule	deny in ip from any to 10.0.0.0/8
HP-Nas-Filter-Rule	deny in ip from any to 172.16.0.0/12
HP-Nas-Filter-Rule	permit in ip from any to any