WEB REDIRECTION WITH CISCO ISE

CONTENTS

REQUIREMENTS

- ArubaOS-Switch (2930M/F, 3810M, 5400R) 16.08 and Above
- Cisco ISE (2.3 And Above)

OVERVIEW

This document will cover Web Redirection with Cisco ISE.

For this scenario, we will be creating a Mac Authentication Fallback policy within Cisco ISE to allow guest devices some network connectivity. This network connectivity will only allow users access to Cisco ISE to register their device . Once the Client is registered, we only want that client to have basic internet access so we will configure a second role to allow for this to work. This same concept can be used for BYOD and a Sponsor Portal with Cisco ISE.

ARUBA SWITCH CONFIGURATION

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 port-access authenticator <Ports>
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
aaa authentication port-access eap-radius
aaa authentication captive-portal enable
aaa authorization user-role enable
```

Web Redirection User Role Configuration

Redirection Policy and Class map Configuration

```
class ipv4 "DNS"
     10 match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 53
   exit
class ipv4 "DHCP"
     10 match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 67
   exit
class ipv4 "WEB-TRAFFIC"
     10 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 80
     20 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 443
   exit
class ipv4 "CLEARPASS-WEB"
     30 match tcp 0.0.0.0 255.255.255.255 10.6.3.15 0.0.0.0 eq 80
     40 match tcp 0.0.0.0 255.255.255.255 10.6.3.15 0.0.0.0 eq 443
     50 match tcp 0.0.0.0 255.255.255.255 10.6.3.15 0.0.0.0 eq 8443
policy user "ISE-REDIRECT"
     10 class ipv4 "DNS" action permit
     20 class ipv4 "DHCP" action permit
     30 class ipv4 "CLEARPASS-WEB" action permit
     40 class ipv4 "WEB-TRAFFIC" action redirect captive-portal
```

User Role Configuration for web redirection User-Role

```
aaa authorization user-role name "ISE-CAP-PORTAL"
   captive-portal-profile "use-radius-vsa"
   policy "ISE-REDIRECT"
   vlan-id 505
   Exit
```

Guest User Role Configuration

User Role Configuration for web redirection User-Role

```
class ipv4 "BLOCK_INTERNAL"
     10 match ip 0.0.0.0 255.255.255.255 10.0.0.0 0.255.255.255
     20 match ip 0.0.0.0 255.255.255.255 192.168.0.0 0.0.255.255
     30 match ip 0.0.0.0 255.255.255.255 172.16.0.0 0.15.255.255
   Exit
class ipv4 "GUEST_ACCESS"
     40 match ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
   Exit
policy user "GUEST_ACCESS"
     10 class ipv4 "BLOCK_INTERNAL" action deny
     20 class ipv4 "GUEST_ACCESS" action permit
   Exit
```

User Role Configuration for CoA to guest Access

```
aaa authorization user-role name "Guest_Access"
   policy "GUEST_ACCESS"
   vlan-id 100
   Exit
```

ADDING VSA TO THE HP DICTIONARY

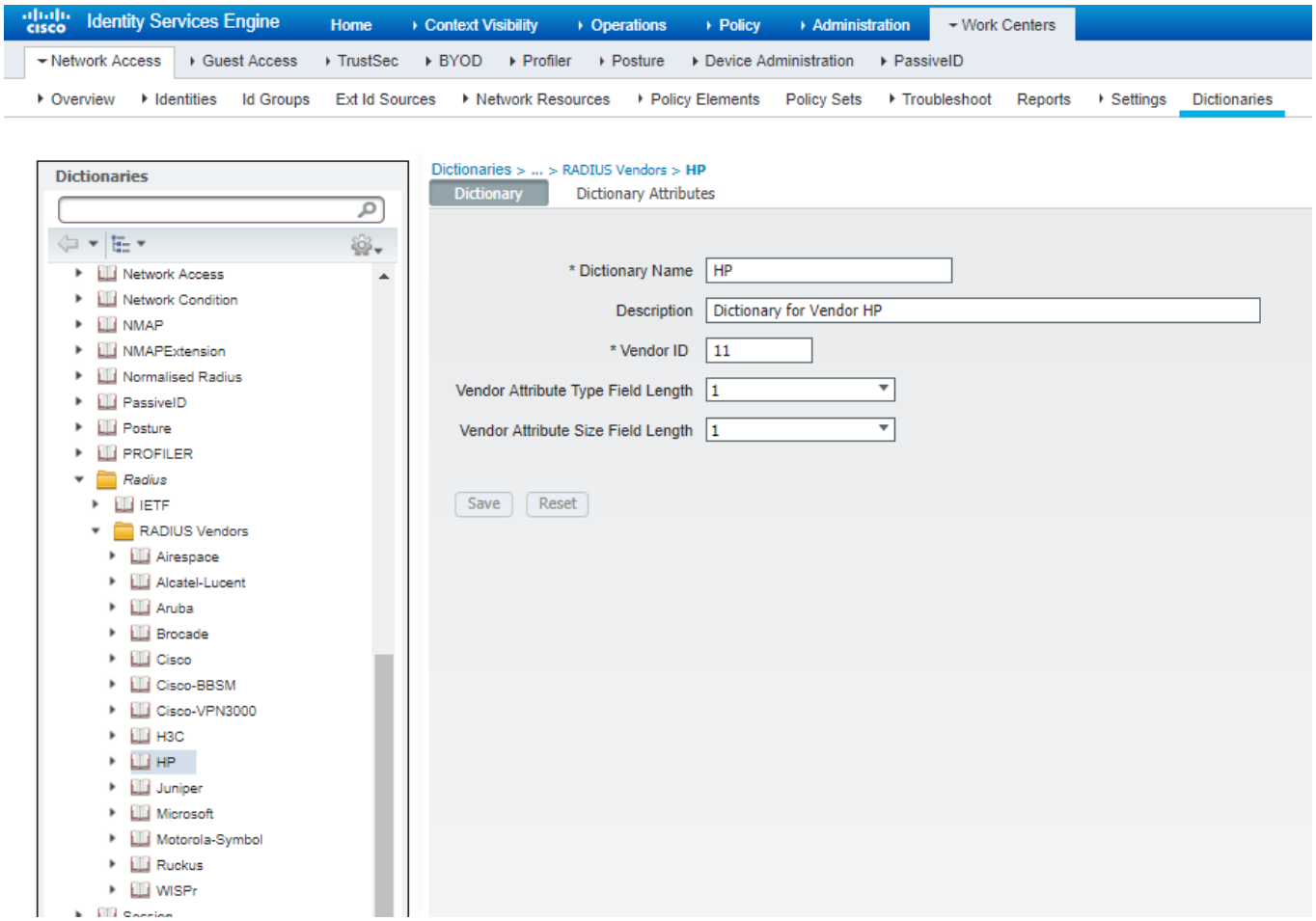
Description

Cisco ISE does not have all the VSA's that are needed by default so in order to use web redirection with Cisco ISE the VSA's need to be added.

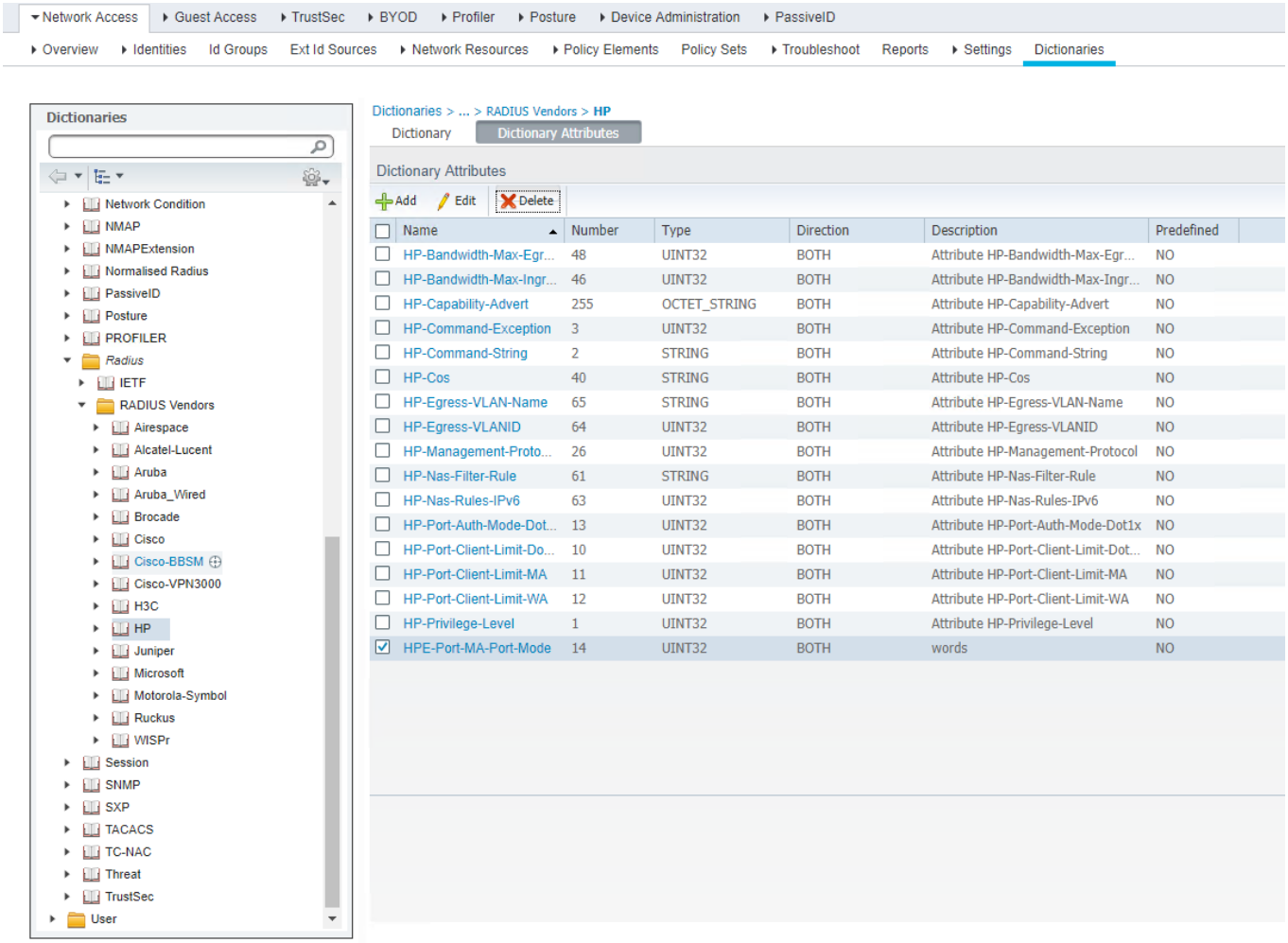
1. Navigate to "Work Centers> Network Access> Dictionaries"

   From this page go to

   "System> Radius > HP"



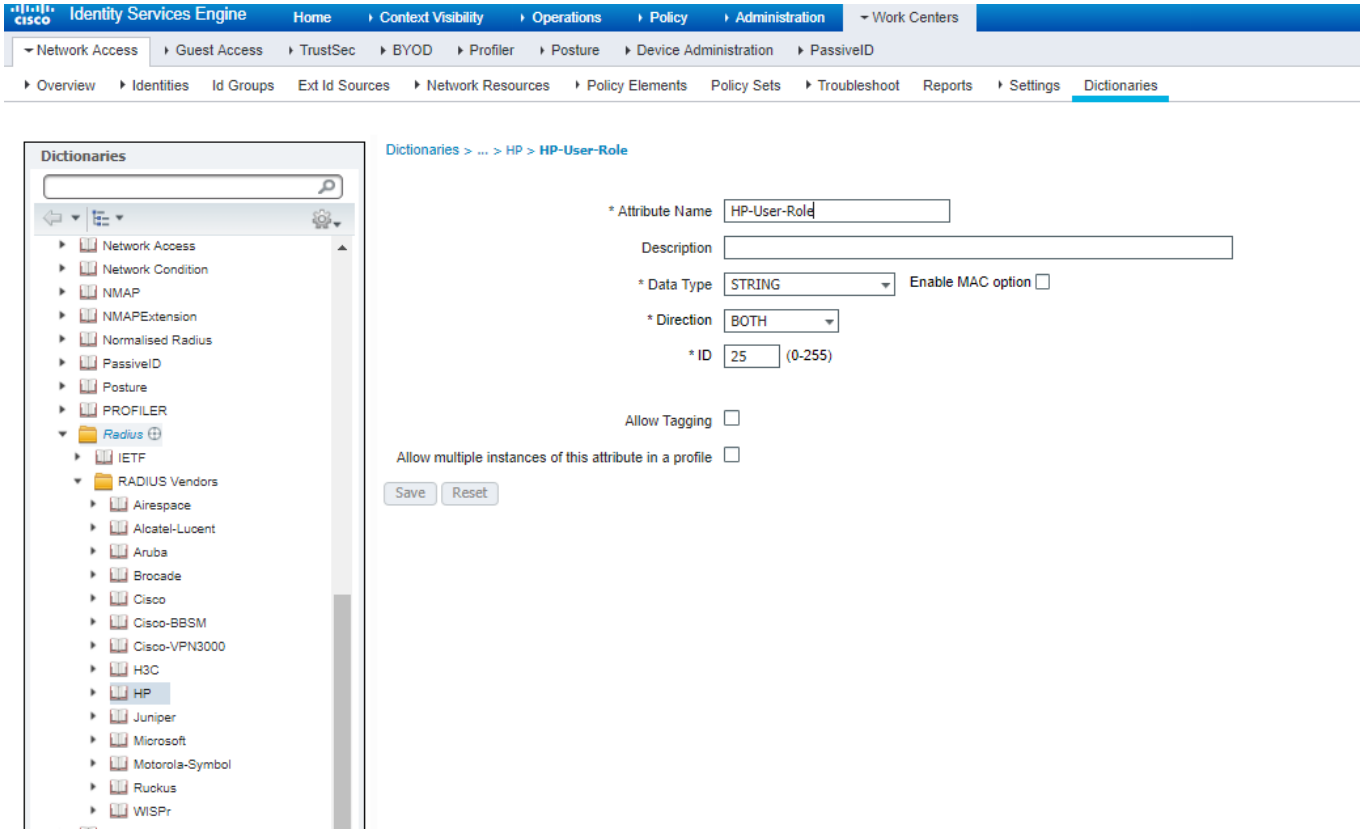
2. Click Dictionary Attributes then click “+Add”



3. A New Page will appear enter the Attribute information below

Attribute Name: “HP-User-Role”
Data type: “String”
Direction: “Both”
ID: “25”

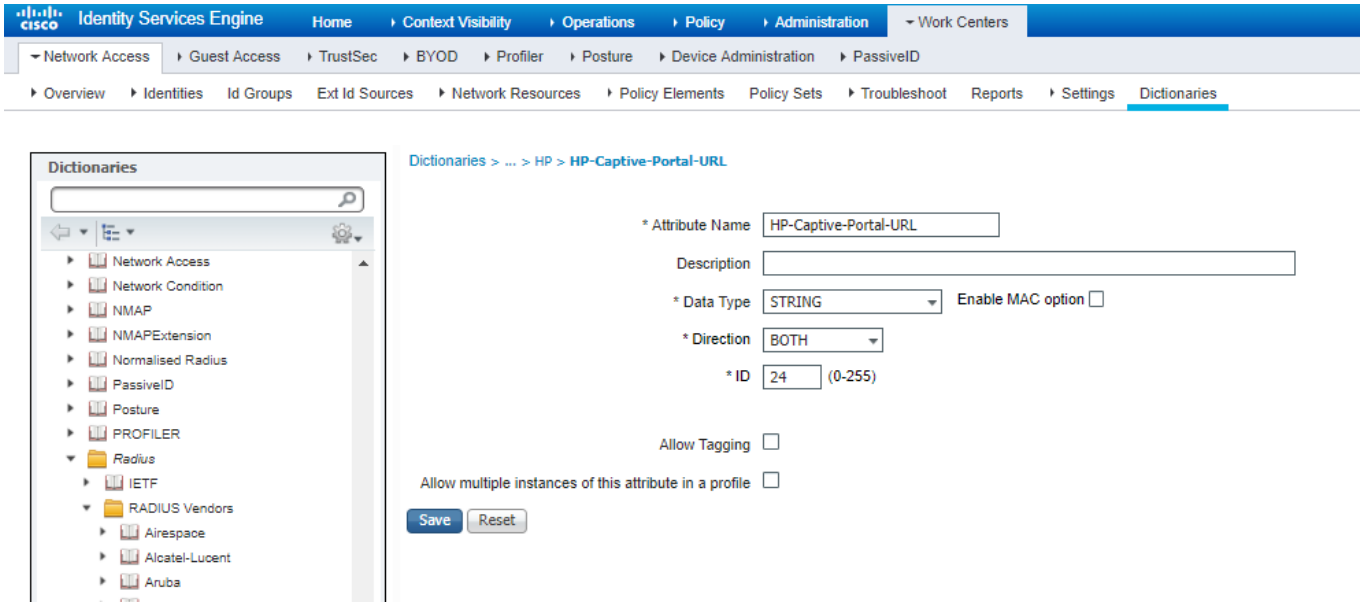
Click Save



The Captive Portal VSA has to be added Click “+Add”

Attribute Name: “HP-Captive-Portal-URL”
Data type: “String”
Direction: “Both”
ID: “24”

Click Save



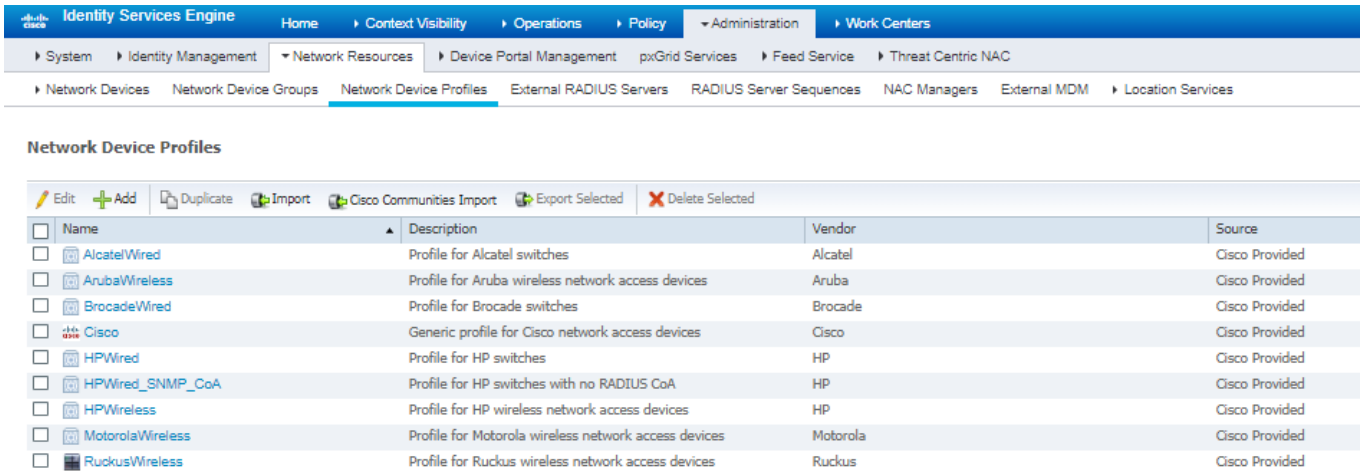
There should now be two New VSA’s in Cisco ISE that can be used.

CREATING A NETWORK DEVICE PROFILE

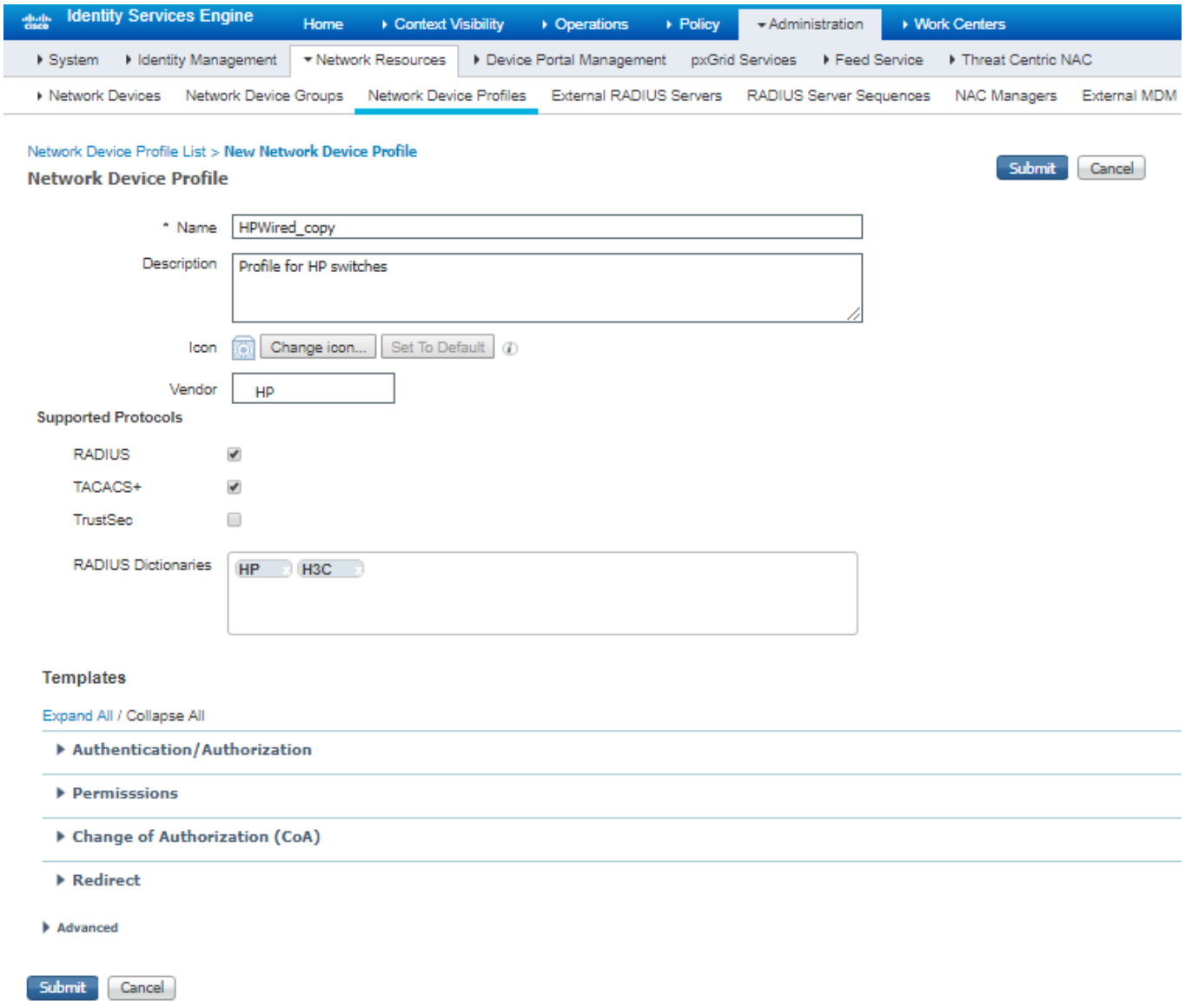
Description

Since Cisco ISE does not have the Captive portal VSA, we have to allow it to be used by the network profile. Cisco ISE does not let you edit existing profiles so we must create a copy of the existing “HP Wired” Profile so that it can be edited to use the captive portal VSA that was just created.

1. Navigate to “Administration>Network Resources> Network Device Profiles



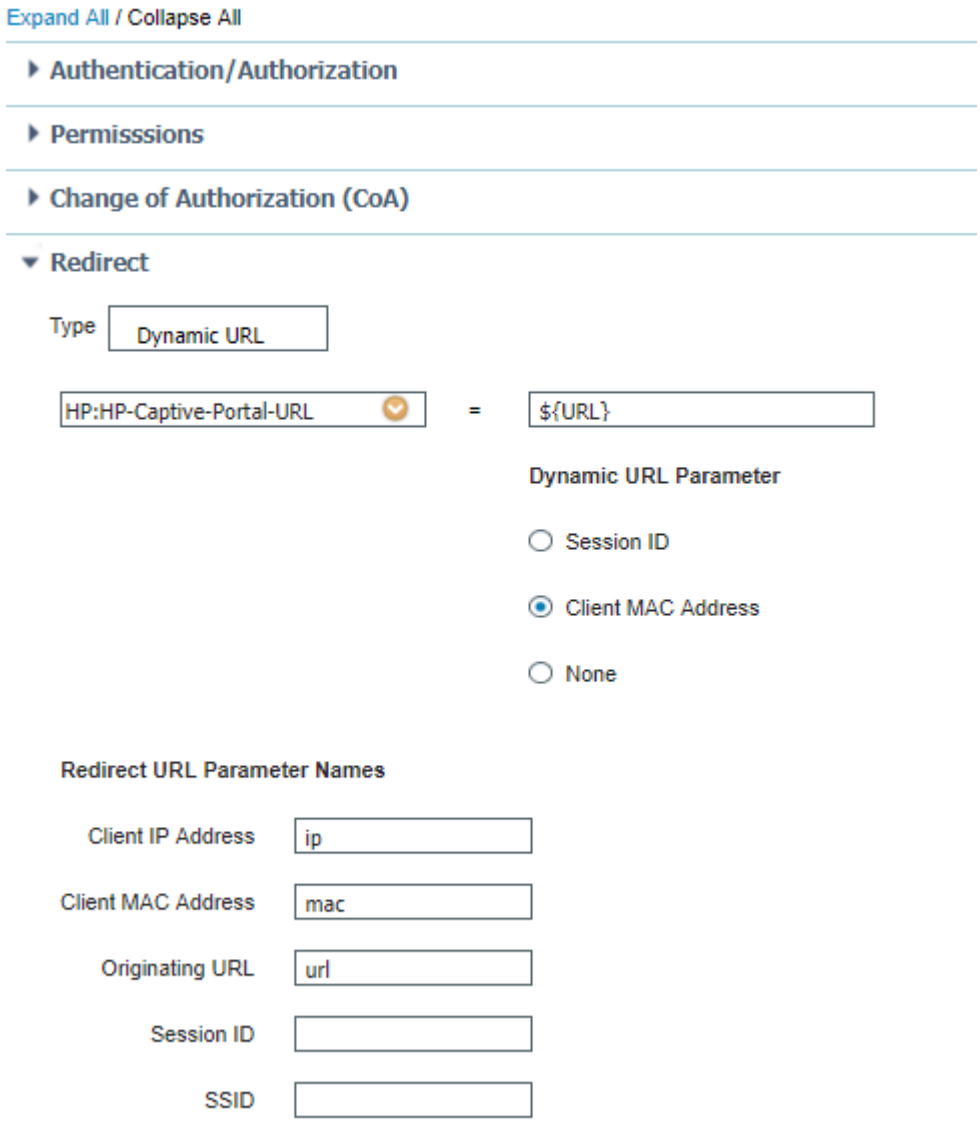
2. Select the “HP Wired” Profile then click Duplicate, it will automatically pull up the configuration of the New Profile.



3. Click the Redirect Dropdown, Select “Dynamic URL” in the drop down box select the “HP-Captive-Portal-URL” VSA that we created earlier in this document

Next check the “Client MAC Address” and Enter the following information below

Client IP Address: ip
Client MAC Address: mac
Originating URL: url



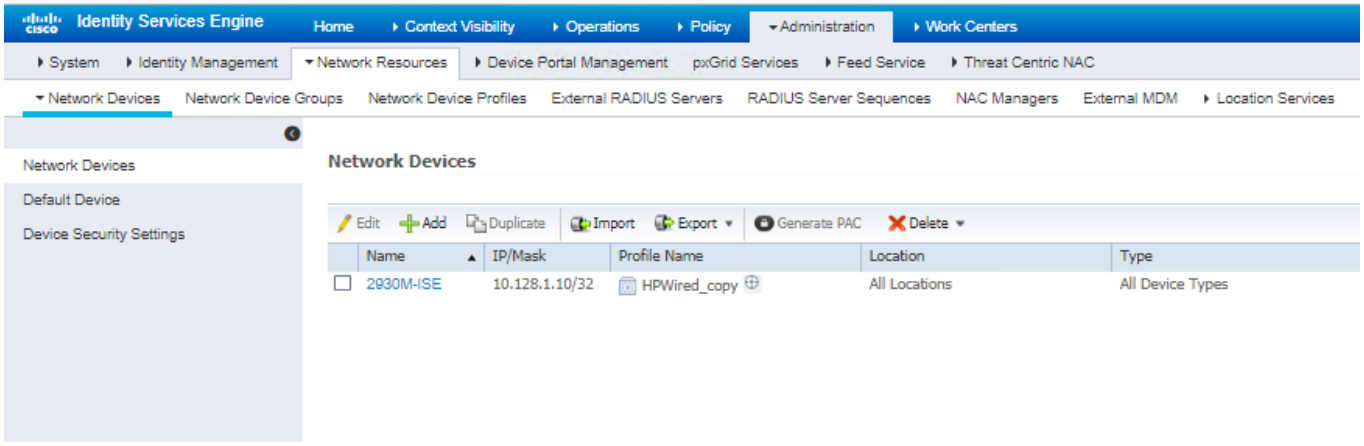
Click Save

ADDING A SWITCH TO ISE

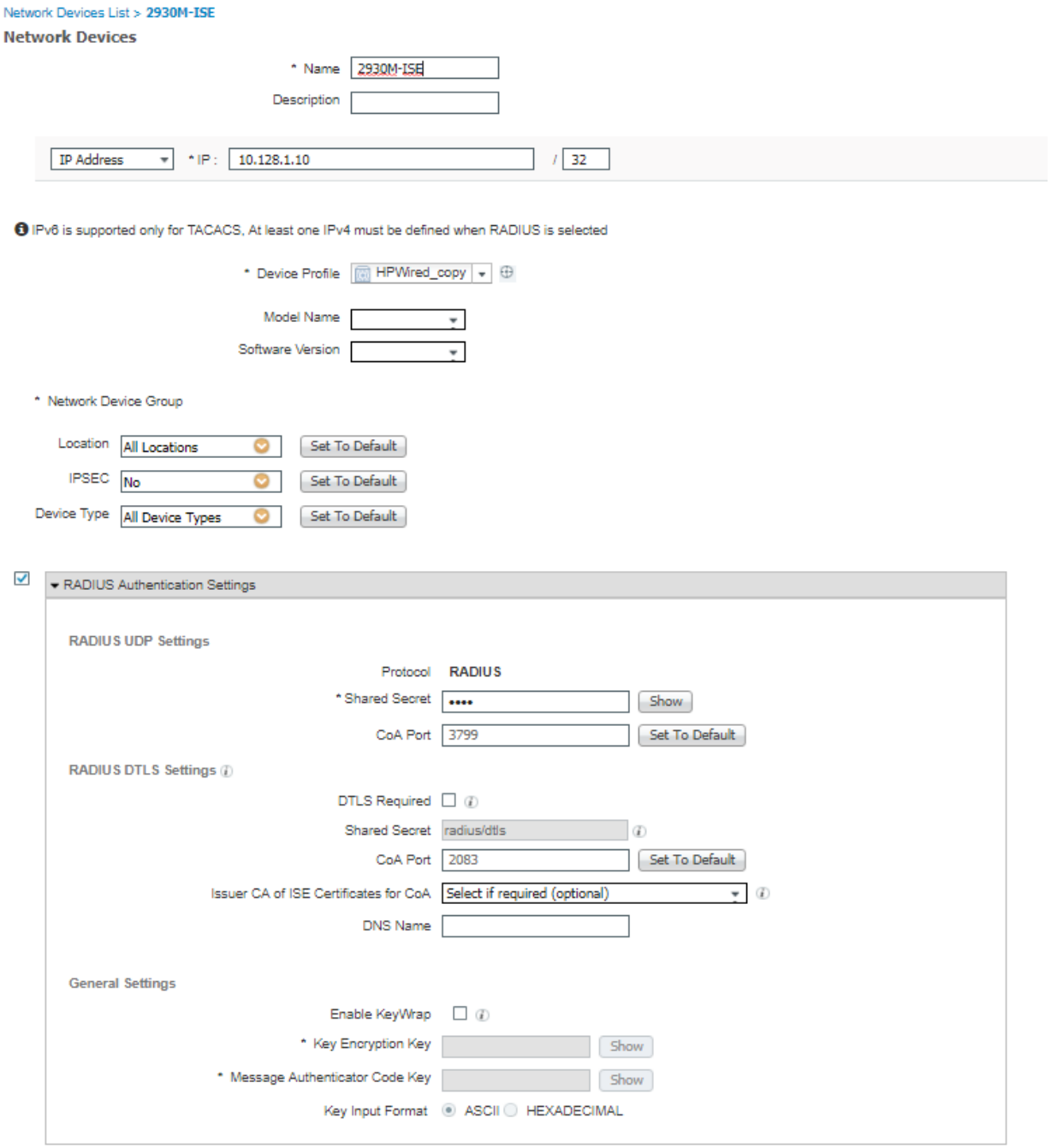
Description

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

1. Navigate to Administration> Network Devices. Click Add.



2. Enter the IP address, RADIUS shared secret, and model of the switch and select the “HPWired_copy” switch profile. If the switch is already added to ISE then just edit the device and select the “HPWired_copy” Profile



GUEST PORTAL SETTINGS

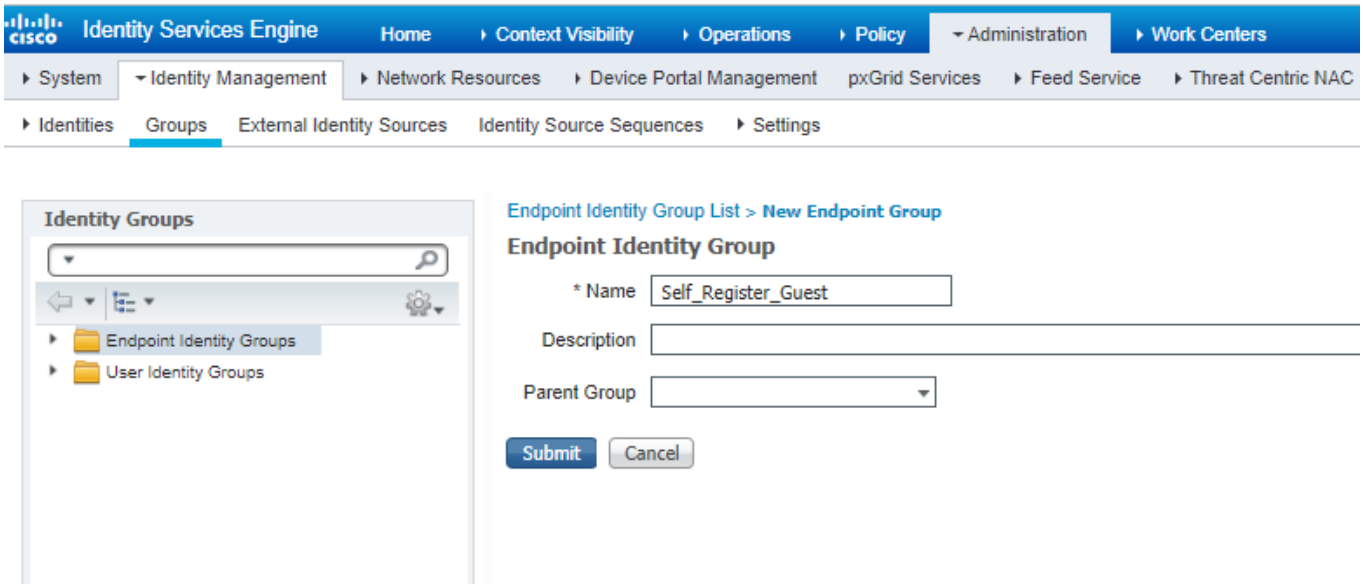
Description

Before editing the Guest portal there needs to be an Identity group for the self-registered users so that devices that register don't have to re-register every single time the move offices or sites.

1. To do this navigate to

"Administration> Groups>Endpoint Identity Groups"

Click "+ Add" and name the group and Click Save

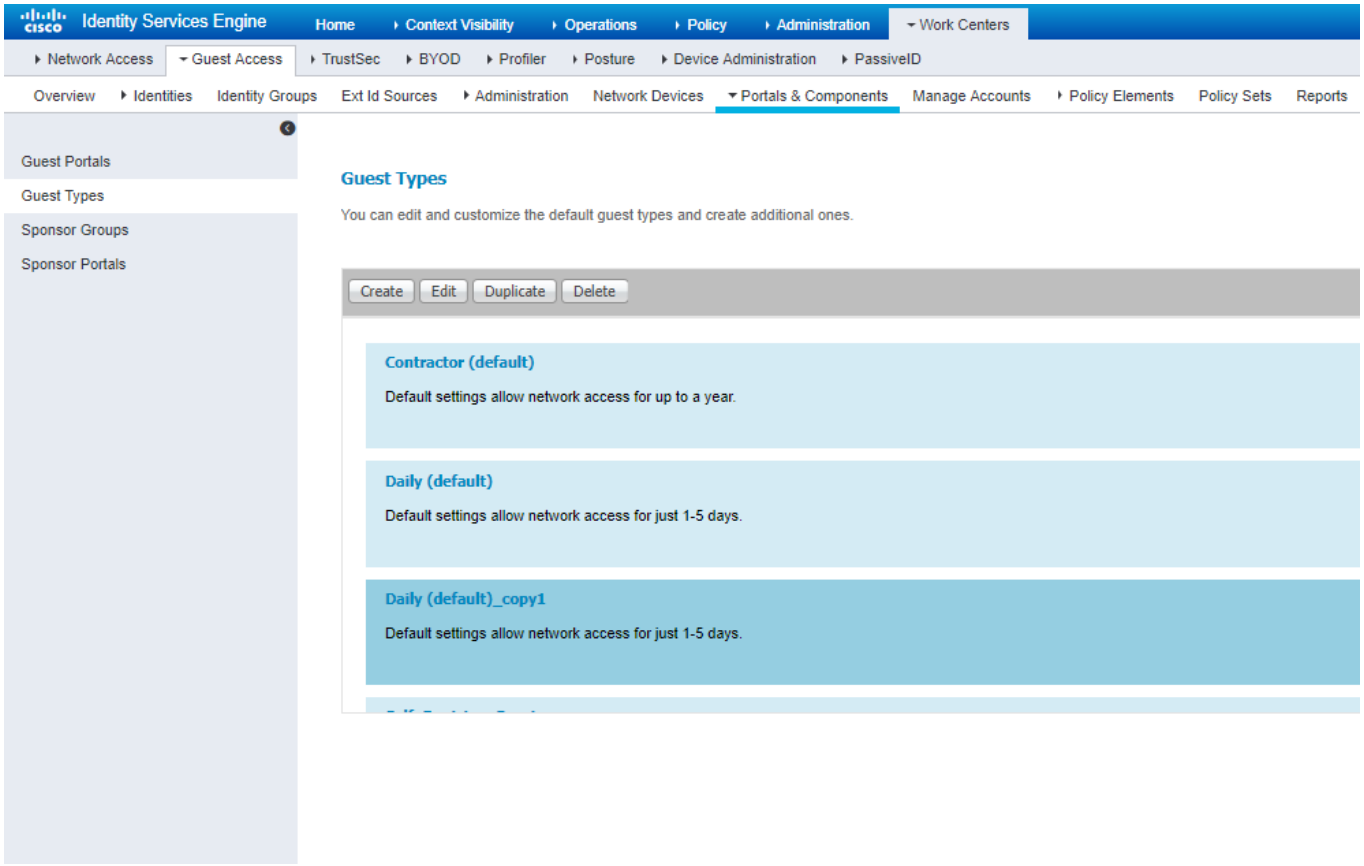


2. Edit the Guest Portal Settings

Navigate to

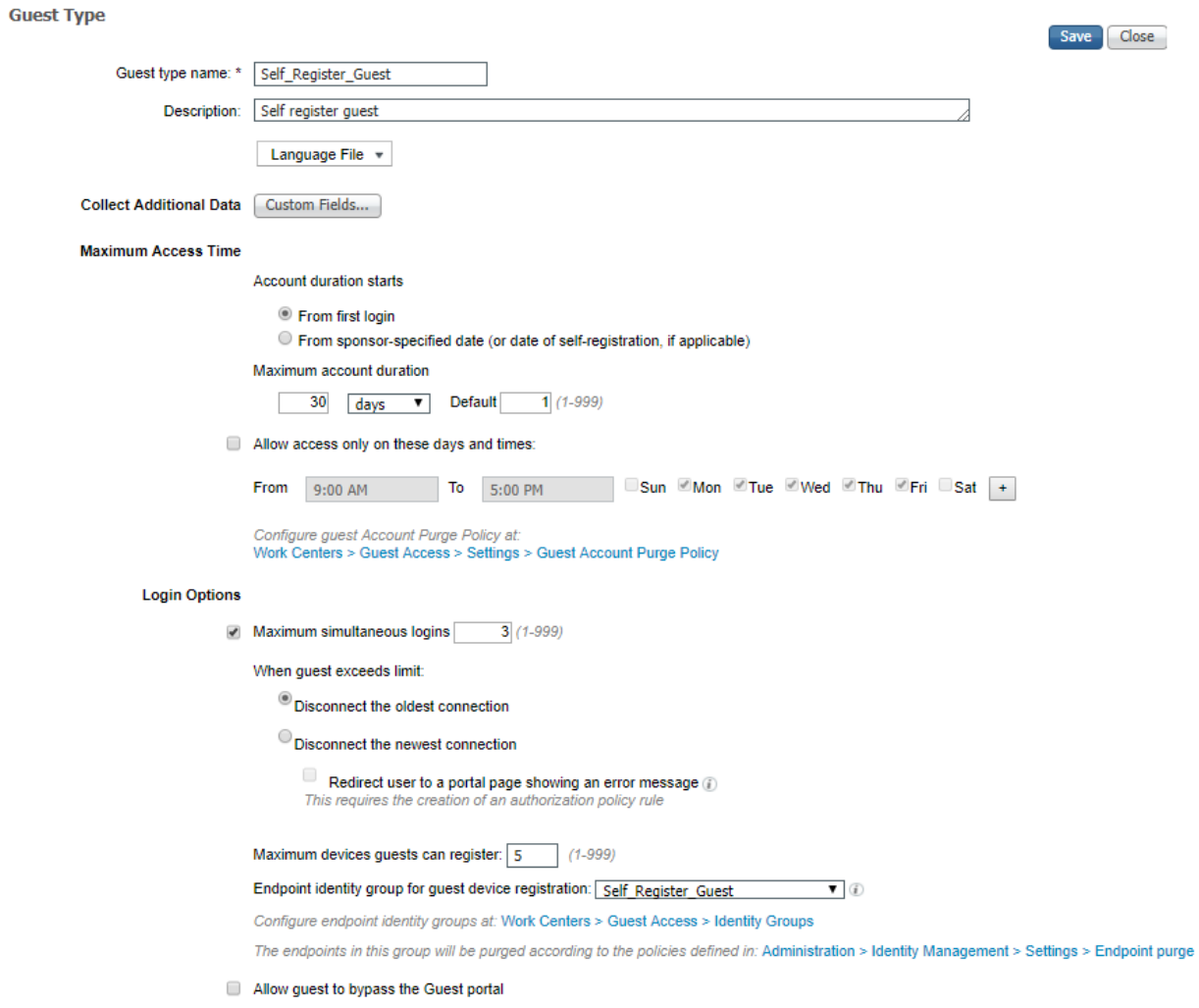
“Work Centers>Guest Access>Portals & Components.

Select Guest Types Duplicate the “Daily (Default)”



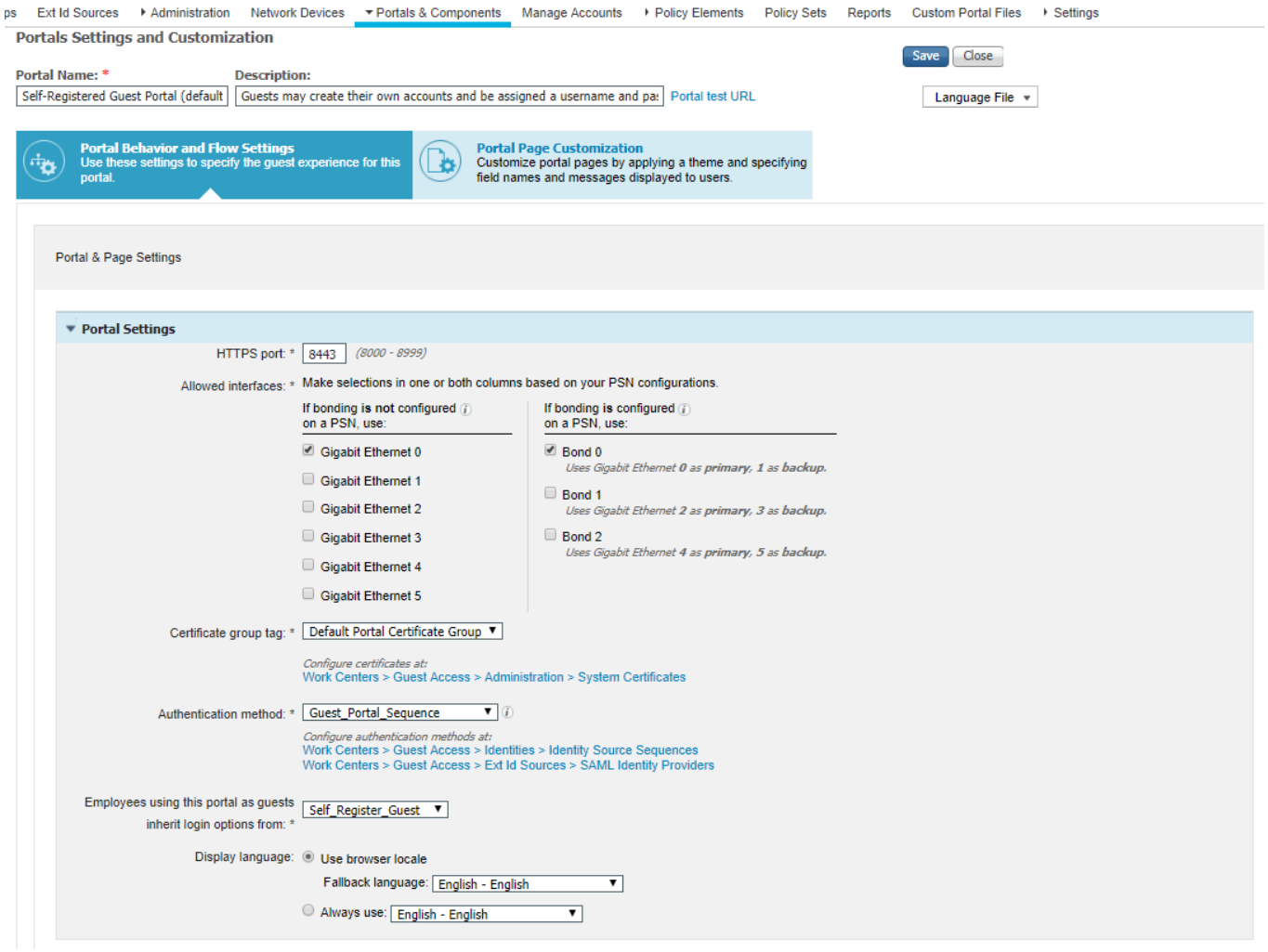
3. Select the “Daily (Default) Copy1” Guest type and Edit the Guest type.

Change the Guest type name and change the endpoint Identity group to the Self_Register_Guest group that was created before. Edit any other settings that are needed

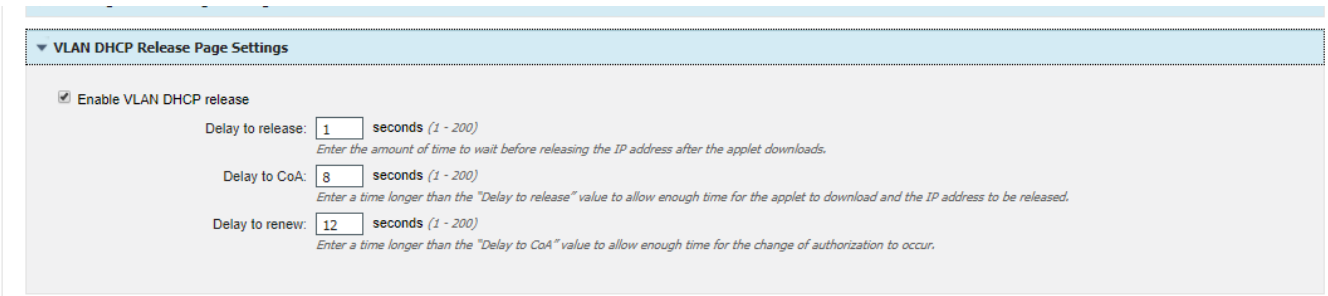


4. Edit the Guest portal Edit the “Self-Registered Guest Portal (default)” or Duplicate this portal.

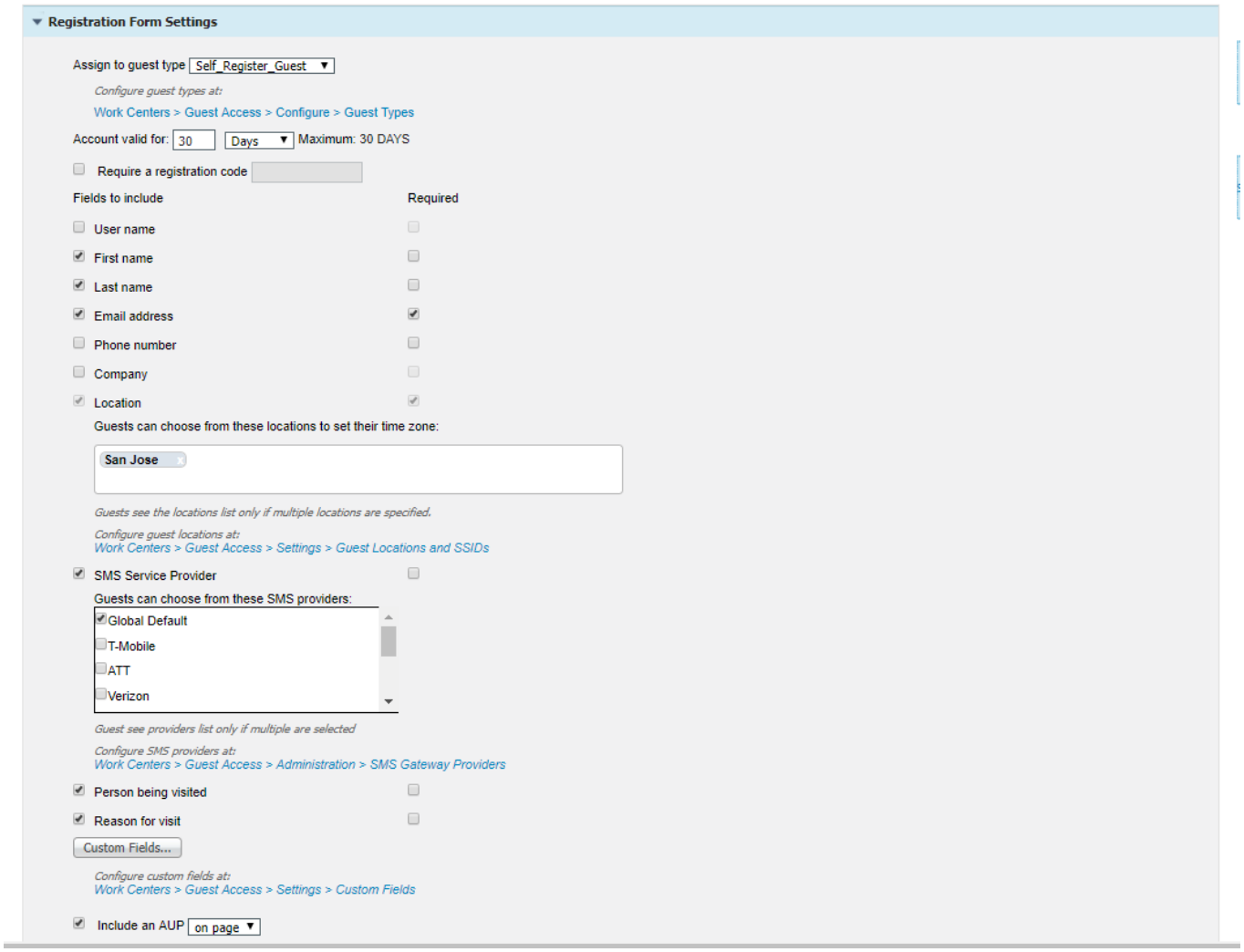
In the portal settings change the “employees using this portal as guest inherit login options” to the Self_Register_Guest. This will allow internal user to just gain internet access quickly.



5. Enable Vlan DHCP Release this will make CoA work more smoothly.



6. In the registration from edit it to fit the needs of your deployment. Click Save



WEB REDIRECTION POLICY

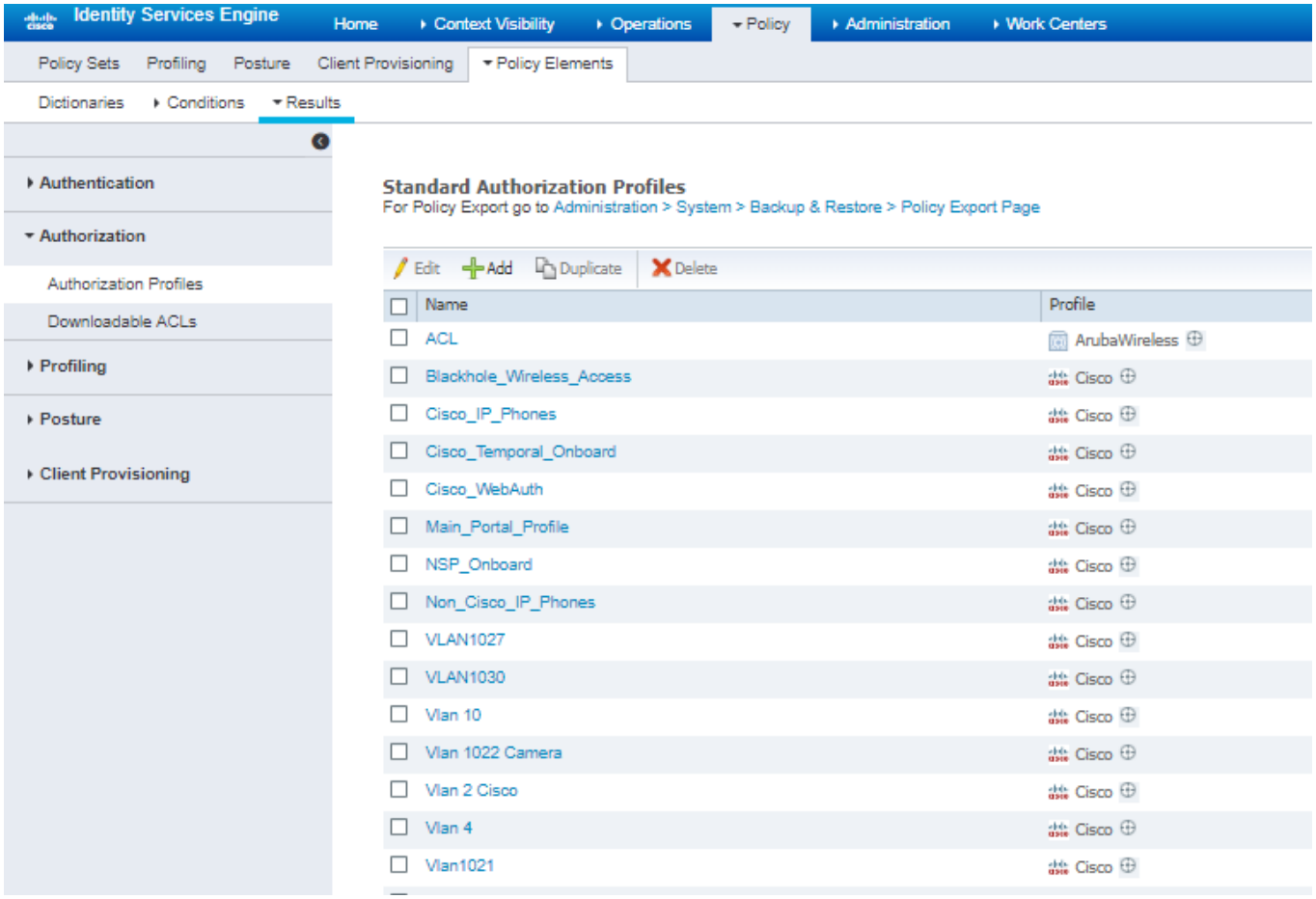
Description

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. There needs to be two authorization profiles created so configure more than one authorization profile

Navigate to “Policy>Policy Elements>Results

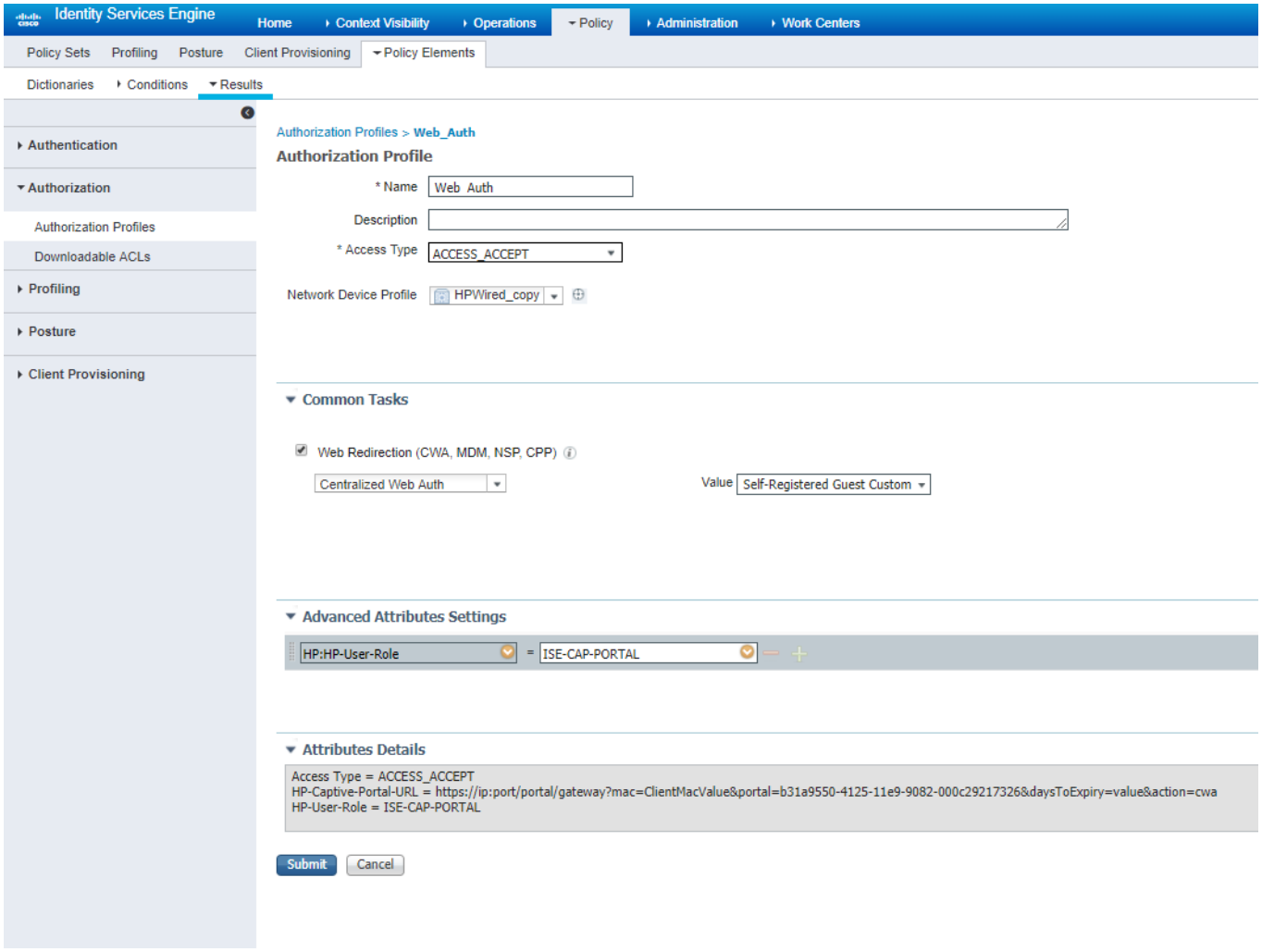
And Select Authorization > Authorization profiles



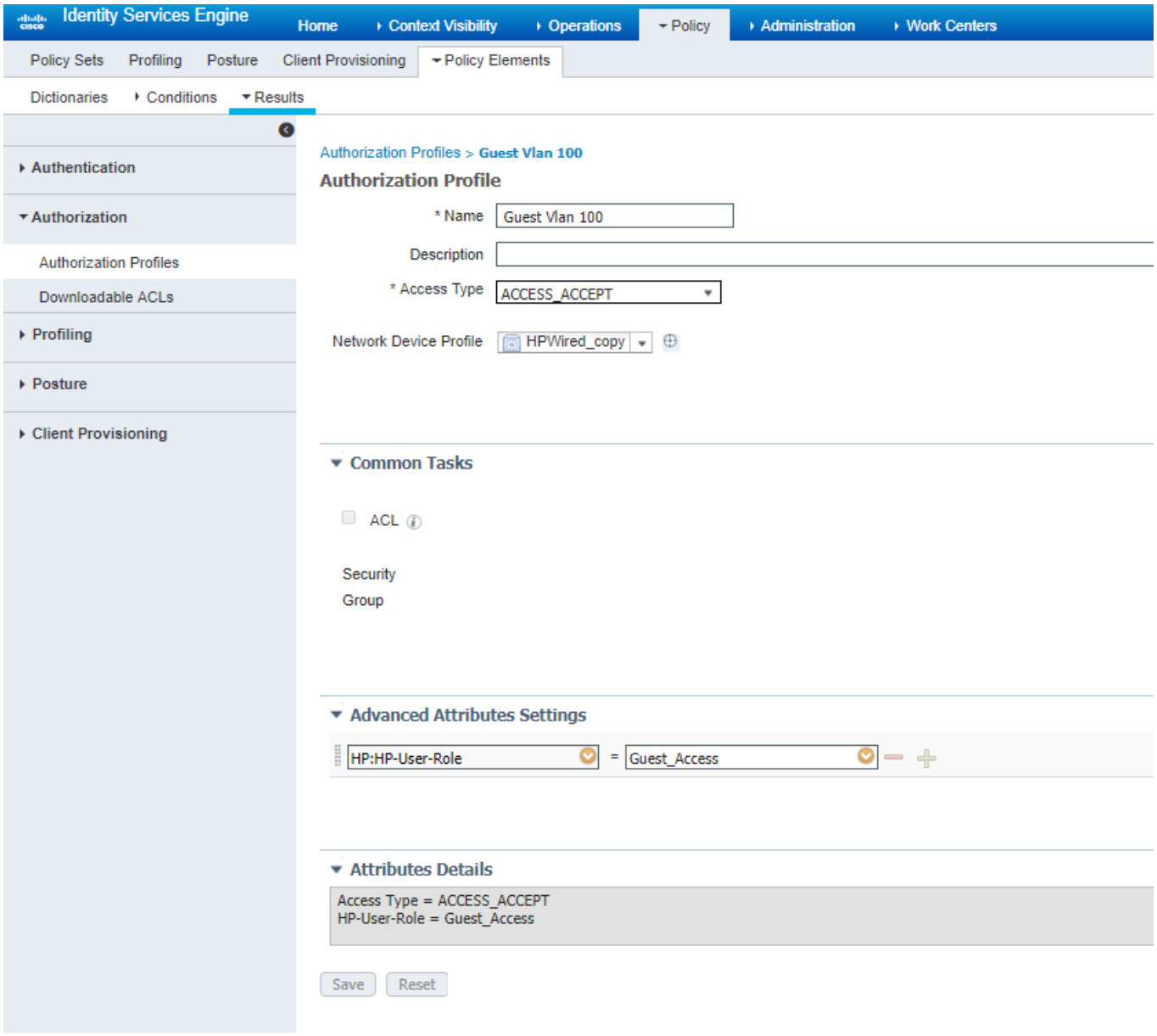
2. Click Add , Check the “Web Redirection box”

Select “Centralized Web Auth” from the Drop down then Select the Guest Portal that was configured with the settings configured before.

Then Click Advanced attributes and select the HP-User-Role and enter in the captive portal user-role that was configured on the switch before in this case it will be “ISE-CAP-PORTAL”.



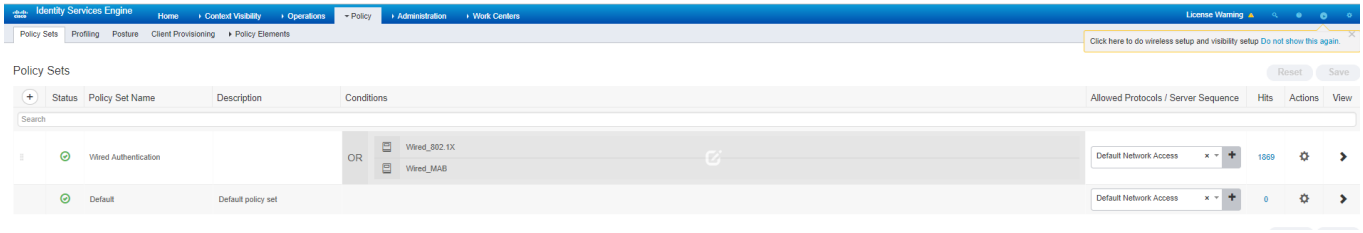
3. The guest user role authorization profile has to be created. Click add again Name the Authorization profile then Click Advanced Attributes to add the “HP-User-Role” VSA and Enter the “Guest_Access” user role that was configured on the switch. Then Click “Save”



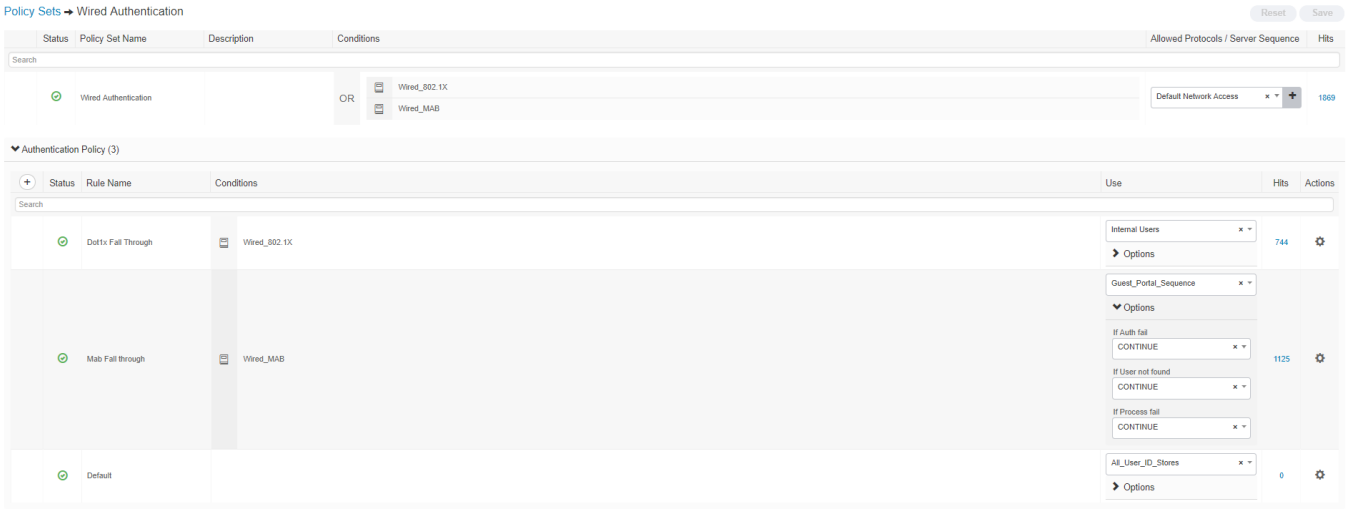
4. To create the Policy Navigate to

“Policy>Policy Sets”

In this case there is a Wired Authentication Rule to Catch all Dot1x and Mac Auth



5. Then create an authentication rule for Mac Auth Bypass so if the mac of the device cannot authenticate it will continue on to an authorization profile

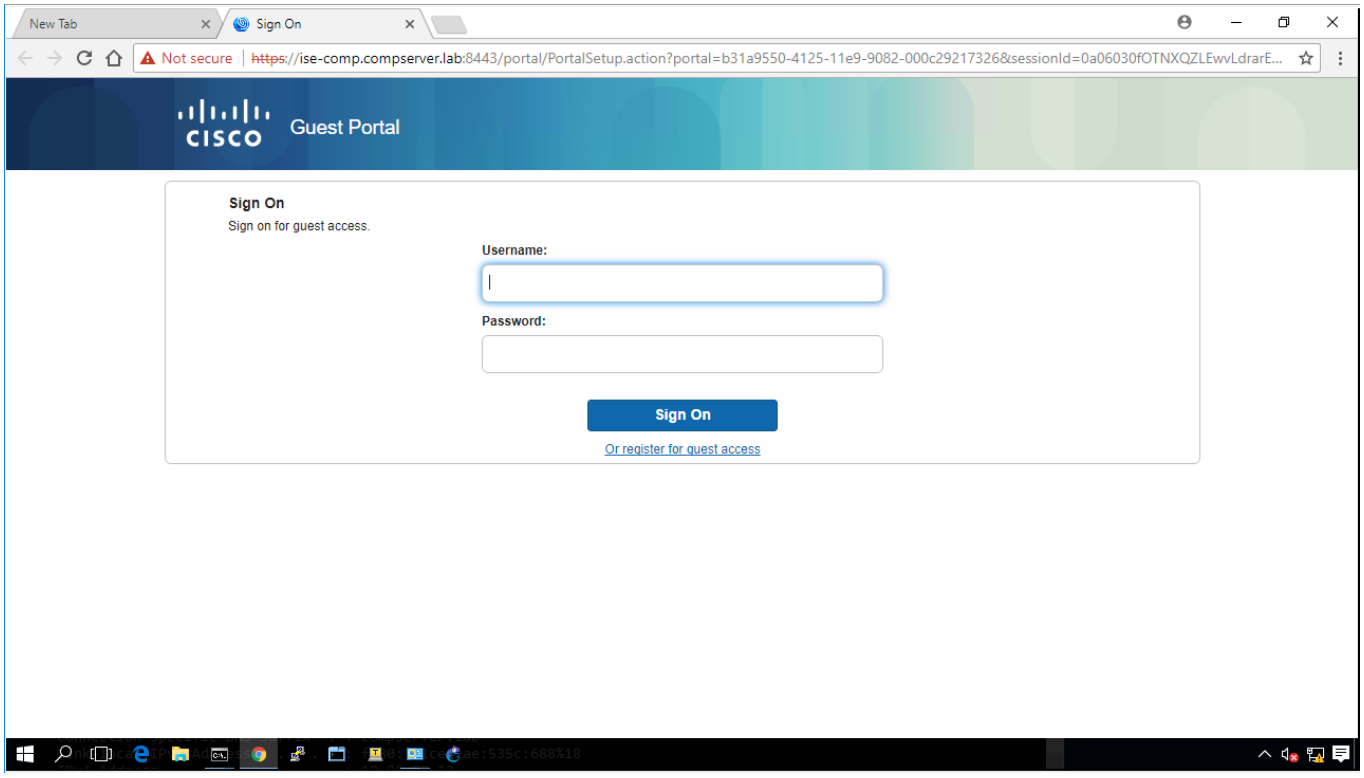


6. Create two Authorization rules one rule for devices that have registered, this rule will match authenticated devices that have already registered and have been placed into the endpoint Identity Group that was created earlier in this document. Then select the authorization profile which will be the Guest Vlan 100 profile that was configured as the result to pass devices that match this condition.

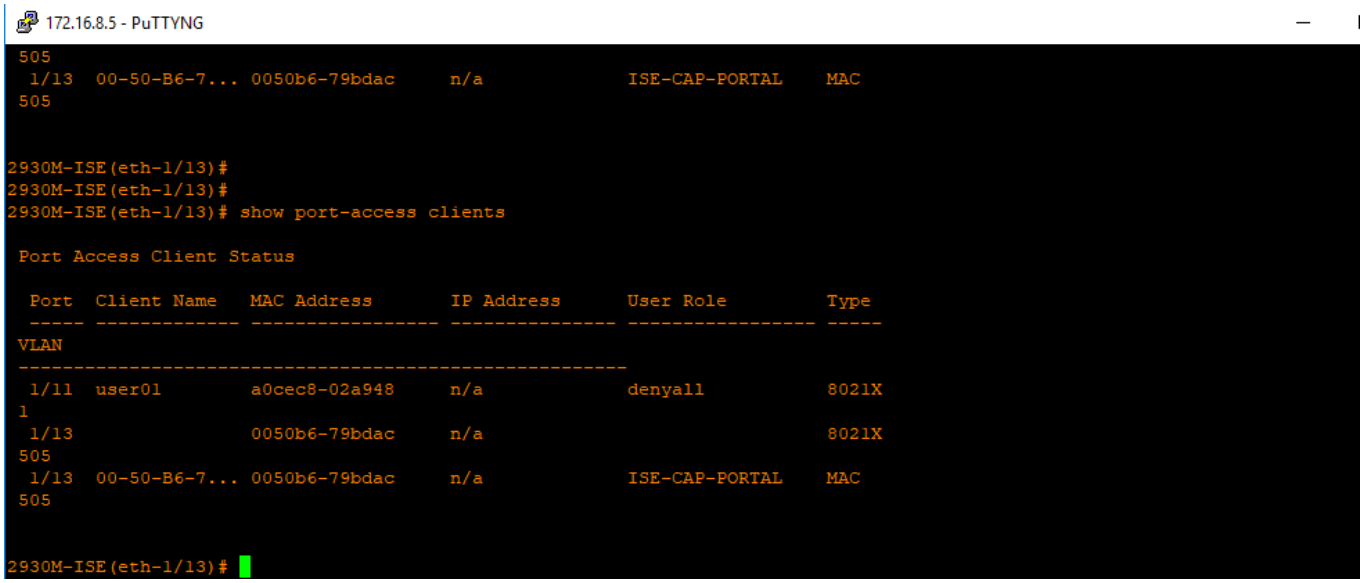
7. The second rule to create will be the last authorization rule which will match any devices doing Mac Auth and pass them the Web_Auth Profile that was configured before which will redirect the client to ISE

VERIFICATION

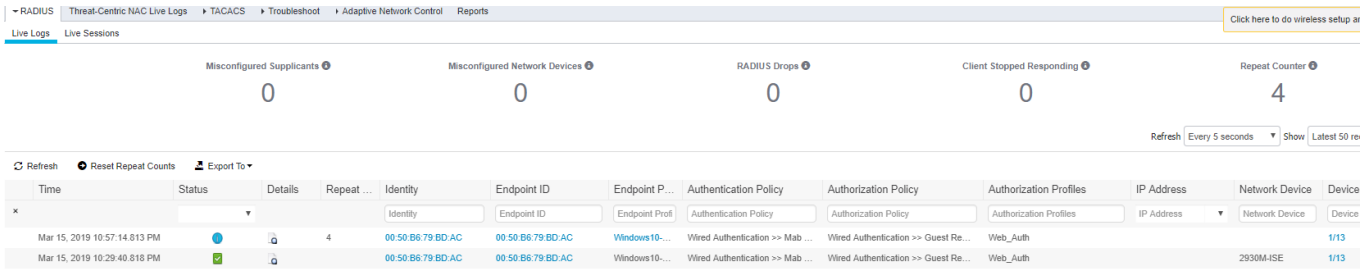
The Client will get redirected to the proper web portal



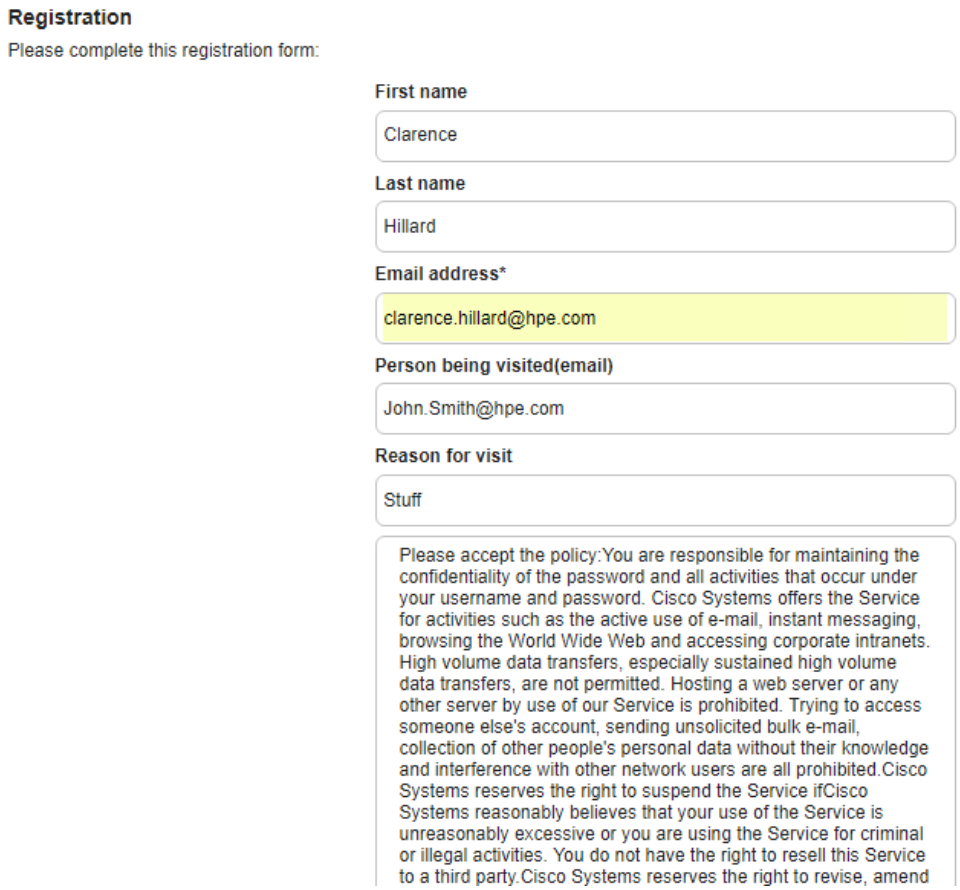
The Switch will apply the proper User Role



ISE will show the proper Log



Now that the client can get to the web portal create an account and make sure the client can will get CoA properly



Account Created

Use the following information to sign on to the network.

Username: clarence.hillard@hpe.com
Password: 7495
First name: Clarence
Last name: Hillard
Email: clarence.hillard@hpe.com
Location: San Jose

Print

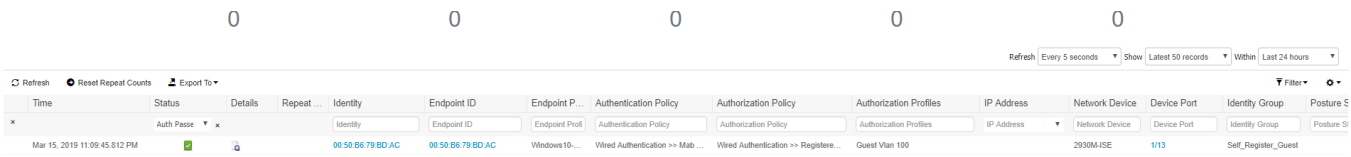
Sign On

Check the Switch

172.16.8.5 - PuTTYNG

```
1
 1/13               0050b6-79bdac     n/a                              8021X
100
 1/13  00-50-B6-7... 0050b6-79bdac     n/a              Guest_Access    MAC
100


2930M-ISE(eth-1/13)# show port-access clients

Port Access Client Status

 Port  Client Name   MAC Address       IP Address      User Role       Type
 ----- ------------- ----------------- --------------- --------------- -----
VLAN
-------------------------------------------------------
 1/11  user01        a0cec8-02a948     n/a             denyall         8021X
1
 1/13               0050b6-79bdac     n/a                              8021X
100
 1/13  00-50-B6-7... 0050b6-79bdac     n/a              Guest_Access    MAC
100


2930M-ISE(eth-1/13)#
```

Check Cisco ISE



TIPS

If the Client Is not getting sent to the guest VLAN after registering, a port bounce VSA can be used as well to force the client back through the authentication process.

Make sure DNS is configured for the ISE server it will use its domain name to pass to the client.