Pica8 Deployment Guide

PicOS® NAC Integration with Cisco Identity Services Engine (ISE) Node

Contents

Contents

Cisco Identity Services Engine (ISE) Solution 1

PicOS Network Access Control – Secured Wired Access Solution 1

Deploying an ISE Node 1
- Requirements 2
- Use Case Overview and Topology 2

Integrating PicOS with Cisco ISE for Radius Authentication 4
- Configuring the PicOS Switch 4
- Configuring the ISE Node 5
  - Import PicOS Network Device Profile 5
  - Configure PicOS Network Device Profile 6
  - Adding a PicOS Network Device Profile 6
- Verifying the Connectivity Between the PicOS Switch and ISE Node 10

Configuring an Employee Laptop with 802.1x Supplicant 11
- Configure the PicOS Switch 11
- Configure the 802.1x Wired Access Policy for Employee Laptop 11
  - Creating User Identity Group and add Users 11
  - Create an Authorization Profile to Dynamically Assign a VLAN 13
  - Create an Authorization Profile to Dynamically assign an ACL 13
  - Create the Wired Access Policy for an Employee Laptop Running 802.1x Supplicant 14
- Configuring the Windows Supplicant on the Laptop 16
- Verifying the NAC Configuration 17

IP Phone Authentication 18
- Configuring the MAB Wired Access policy in ISE for IP Phones 18
  - Creating an IP-Phone Endpoint Identity Group and add IP Phone Mac Addresses 18
  - Create an Authorization Profile to Dynamically Assign a Voice VLAN 19
  - Create a Wired Access Policy for an IP Phone 20

Access Point Authentication 24
- Verifying the NAC Configuration 27

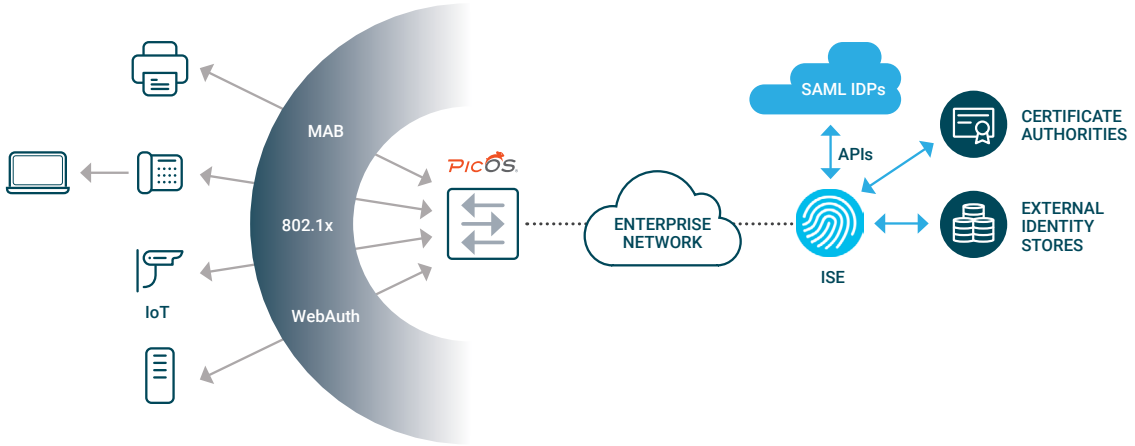
Guest Laptop Using Central Web Authentication 28
- Configuring the PicOS Switch 28
- Configuring the ISE Node With a Central Web Authentication Policy 29
- Verifying the NAC Configuration 38

Troubleshooting 42
- Check Whether the ISE Server is Reachable from the PicOS Switch 42
- Check the NAC Authentication Status of all Ports 43
- Check VLANs to Verify Dynamic VLANs Assignment to a Port 44
- Check Dynamic ACL Rules 45
- Check Downloadable ACL Rules 46
- Check Trace Logs for Radius 46

Reference 47
- PicOS 47
- ISE 47

Cisco Identity Services Engine (ISE) Solution

This document provides details on how to integrate and test the Cisco ISE NAC solution with PicOS® switches for Secured Wired Access.



ISE authenticates users and endpoints via 802.1x, Web Authentication, Mac Authentication Bypass (MAB), and other means. ISE can also query external identity sources for identity resolution and apply appropriate network policies by instructing the network devices.

PicOS Network Access Control – Secured Wired Access Solution

PicOS supports the following Secured Wired Access solutions:

- **Authentication Methods:** Following authentication methods are supported.
  - 802.1x
  - MAC Authentication Bypass (MAB or MAC-RADIUS)
  - Central Web Authentication
- **Multi-host support –** Support for multiple endpoints to be connected to the network through the same switchport
- **Policy Enforcement –** The following network policies can be enforced:
  - Dynamic VLAN Assignment (by ID and Name)
  - Dynamic Access Control List (ACL)
  - Downloadable ACL
  - CoA (Change of Authorization)
- **Server Fail VLAN –** provide limited network connectivity to users in the event of AAA server failure

Deploying an ISE Node

Please refer to the following document for deploying an ISE VM using an OVA template:
Cisco ISE Installation Guide Release 2.6

Requirements

This integration example uses the following hardware and software components for the policy infrastructure:

- A Dell N3048EP-ON switch running PicOS Release 4.1.2.2 (or later)
- An ISE node running release 2.6.0.156 patch 9 (or later)
- An employee laptop running Microsoft Windows 7 Enterprise
- A guest laptop running Mac OS
- A Cisco IP Phone
- An Aruba Access Point

Use Case Overview and Topology

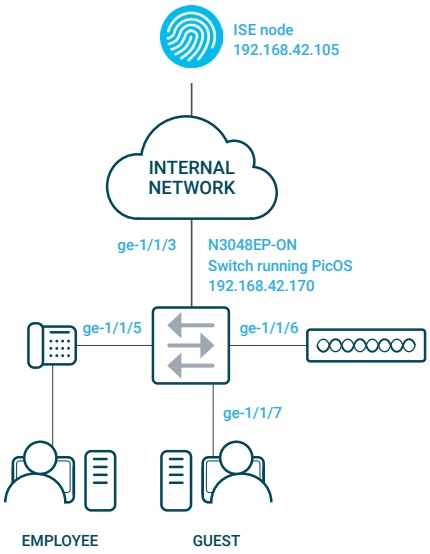
This document provides information for the following authentication uses cases.

1. **Employee laptop:** An employee laptop with 802.1x supplicant is connected to the switch either directly or behind an IP phone and will be authenticated by an 802.1x authentication method. Both dynamic VLAN and ACL policies will be applied to the port where the employee laptop is connected. In the example configuration, the ISE node is configured to authenticate 802.1X users using its local user database. If the authenticated employee is listed in the database as belonging to the Pica8 Employee group, the ISE node returns the VLAN ID 10 to the switch in a RADIUS attribute. The switch then dynamically configures the laptop access port to be in VLAN 10. The employee laptop connected behind a Cisco IP Phone is connected to port ge-1/1/5.

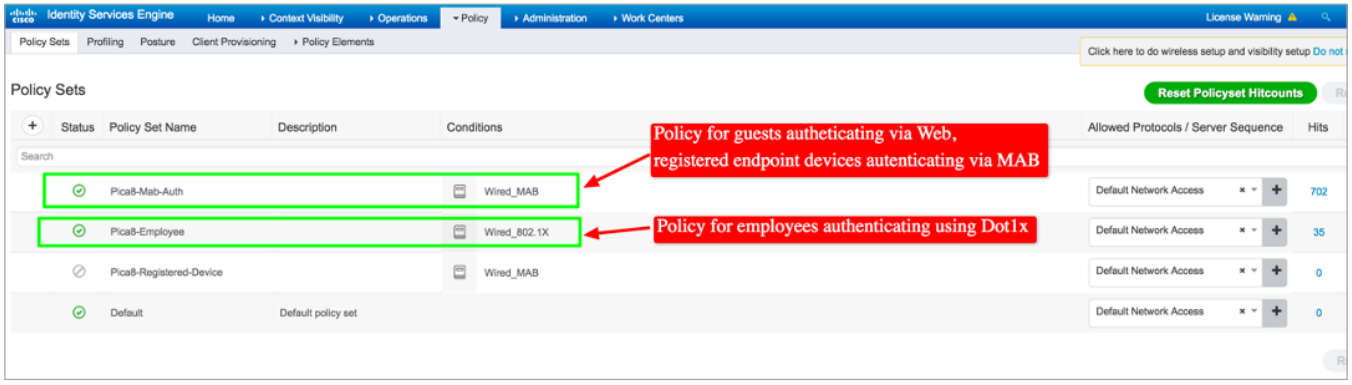
2. **IP Phone:** A Cisco IP Phone is connected to port ge-1/1/5 and gets authenticated by MAB authentication method. Dynamic Voice VLAN policy will be applied to the port where the Cisco IP phone is connected. Switch configures the port to be in VLAN 800.

3. **Registered device:** An Aruba Access Point is connected to port ge-1/1/6. We will use MAB authentication method for this endpoint. Both dynamic VLAN and Downloadable ACL policies will be applied to the port where the Access Point is connected.

4. **Guest laptop:** A guest laptop does not have 802.1x supplicant running. We will use Central Web Authentication method for this use case. The guest laptop is connected to port ge-1/1/7. Both dynamic VLAN and ACL will be applied to the port where Guest laptop is is connected.

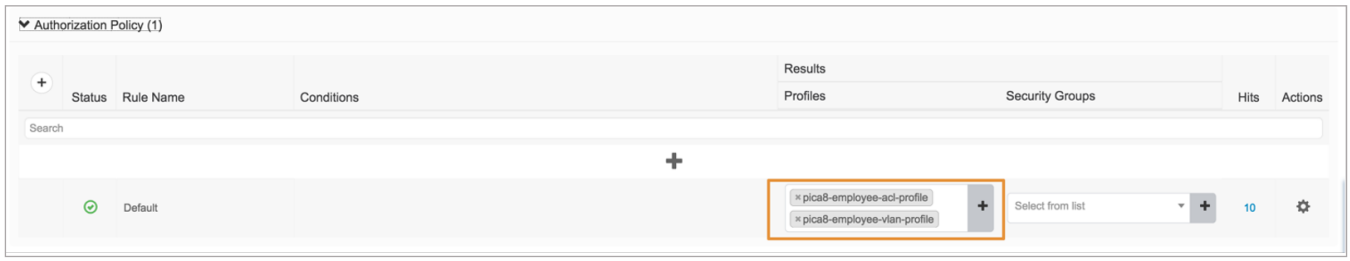


The following are high-level policies in ISE that we will use:



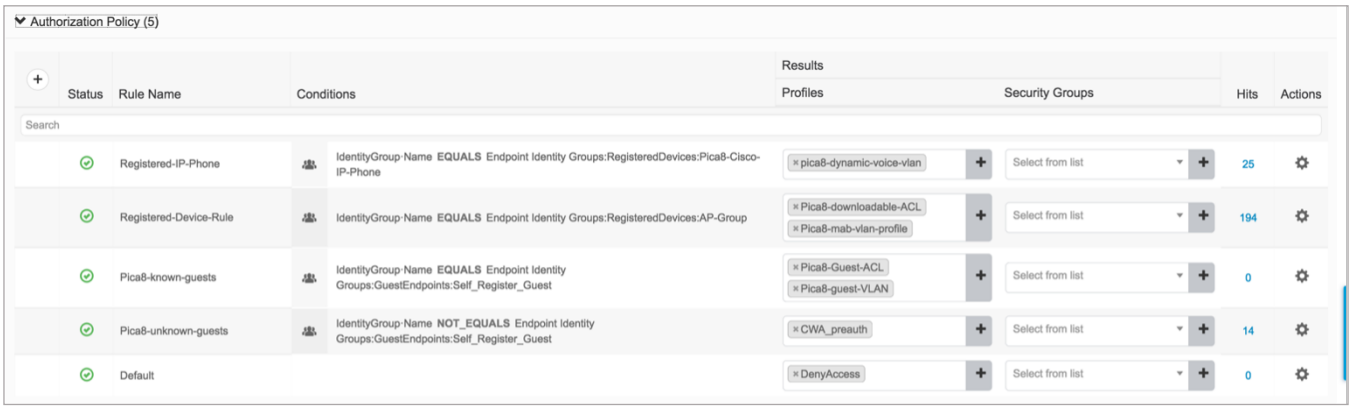
1. **Pica8-Employee Policy:** This is user based authentication and it uses an 802.1x authentication method for Employees. The following Authorization Profile is used:
   a. Default: The following policies are used for employees authenticated by an 802.1x authentication method.

For more details on the Pica8-Employee policy refer to the later sections of the document.



2. **Pica8-Mab-Auth Policy:** This is device based authentication and it uses Central Web Authentication for guests and uses Mac Authentication Bypass (MAB) for registered devices. The following Authorization Profiles are used:
   a. Registered-IP-Phone rule: This rule is used for registered Cisco IP Phones
   b. Registered-Device-Rule: This rule is used for registered AP devices
   c. Pica8-unknown-guests: This rule is used for authenticating the guest user whose laptop will not have an 802.1x supplicant.
   d. Pica8-known-guests: Once guest logins into the Guest Portal, this rule will be used for the registered guests.

For more details on the Pica8-Mab-Auth policy refer to the later sections of the document.



Authorization Policy (5)

Status	Rule Name	Conditions	Results: Profiles	Results: Security Groups	Hits	Actions
Search						
	Registered-IP-Phone	IdentityGroup·Name EQUALS Endpoint Identity Groups:RegisteredDevices:Pica8-Cisco-IP-Phone	pica8-dynamic-voice-vlan	Select from list	25	
	Registered-Device-Rule	IdentityGroup·Name EQUALS Endpoint Identity Groups:RegisteredDevices:AP-Group	Pica8-downloadable-ACL Pica8-mab-vlan-profile	Select from list	194	
	Pica8-known-guests	IdentityGroup·Name EQUALS Endpoint Identity Groups:GuestEndpoints:Self_Register_Guest	Pica8-Guest-ACL Pica8-guest-VLAN	Select from list	0	
	Pica8-unknown-guests	IdentityGroup·Name NOT_EQUALS Endpoint Identity Groups:GuestEndpoints:Self_Register_Guest	CWA_preauth	Select from list	14	
	Default		DenyAccess	Select from list	0	

Integrating PicOS with Cisco ISE for Radius Authentication

The following sections go over PicOS and Cisco ISE configurations for Radius Authentication.

Configuring the PicOS Switch

The following sections go over the basic configuration steps in a PicOS switch needed for the Radius Authentication.

1. Configure VLAN interface

```
set vlans vlan-id 10 vlan-name "vlan10"
set vlans vlan-id 10 l3-interface "vlan10"
set vlans vlan-id 800

set interface gigabit-ethernet te-1/1/3 family ethernet-switching native-vlan-id 10
set interface gigabit-ethernet te-1/1/3 family ethernet-switching port-mode "trunk"

set interface gigabit-ethernet te-1/1/5 family ethernet-switching port-mode "trunk"
set interface gigabit-ethernet te-1/1/6 family ethernet-switching port-mode "trunk"
set interface gigabit-ethernet te-1/1/7 family ethernet-switching port-mode "trunk"
```

   set l3-interface vlan-interface vlan10 address 192.168.42.170 prefix-length 24

```
set ip routing enable true
set system inband vlan-interface vlan10
```

2. Provide the RADIUS server connection information

```
set protocols dot1x aaa radius authentication server-ip 192.168.42.105 shared-key pica8pica8
```

3. Configure the access profile

```
set protocols dot1x aaa radius nas-ip 192.168.42.170
```

4. Configure a RADIUS dynamic authorization client from which the switch accepts the Change of Authorization (CoA) messages. (This is optional.)

```
set protocols dot1x aaa radius dynamic-author client 192.168.42.105 shared-key pica8pica8
```

5. Configure the interval for re-sending the authentication messages to the AAA server when the AAA server does not respond

during NAC authentication. Here retry interval is set to 3 seconds.

```
set protocols dot1x aaa radius authentication server-ip 192.168.42.105 retry-interval 3
```

6. Configure 802.1x, MAB and multiple host mode on all access ports

   The following is an example configuration for one of the access port in the PicOS switch. All ports enable the 802.1x, MAB and Web Authentication modes. Clients with 802.1x supplicant get authenticated with 802.1x while other clients get authenticated with either MAB or Central Web Authentication. Also multiple-host mode is enabled on all ports.

```
set protocols dot1x interface ge-1/1/5 auth-mode 802.1x
set protocols dot1x interface ge-1/1/5 auth-mode mac-radius
set protocols dot1x interface ge-1/1/5 auth-mode web
```

   Configure the host mode to multiple for the interface ge-1/1/5 so that we can use multiple hosts connected to the same port (Example: laptop behind an IP phone connected to the port)

```
set protocols dot1x interface ge-1/1/5 host-mode "multiple"
```

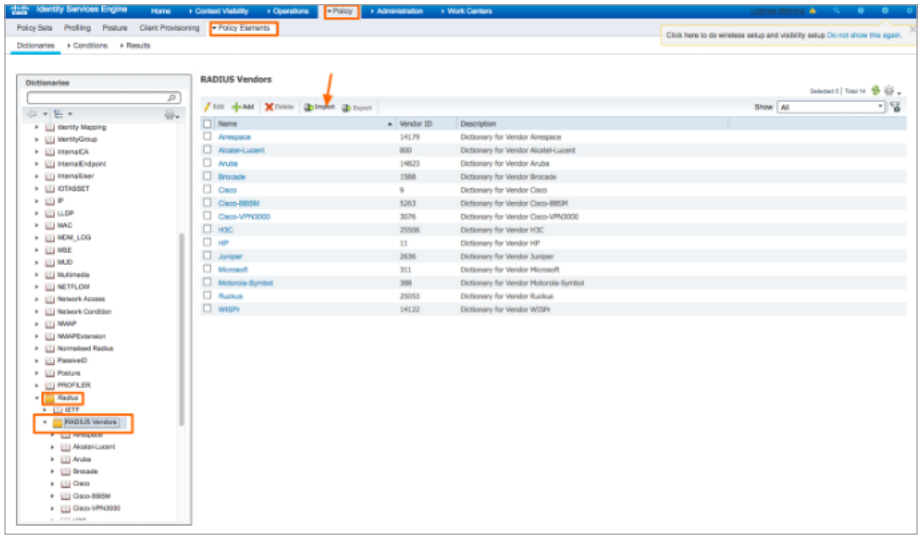
Configuring the ISE Node

The following three configuration steps are needed to configure the ISE node for RADIUS Authentication.
1. Import PicOS Network Device Profile
2. Configure PicOS Network Device Profile
3. Add a PicOS switch as ISE network device

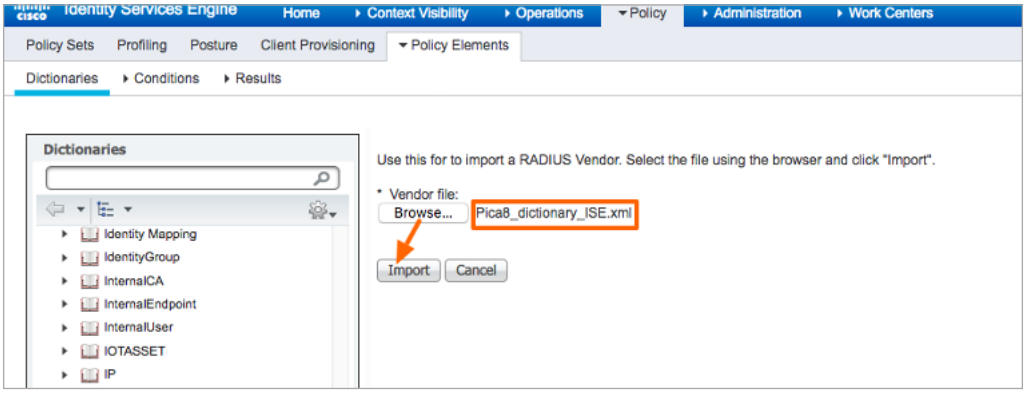
Import PicOS Network Device Profile

Cisco ISE 2.X comes with many pre-imported Network Device Profiles already on the system. The PicOS Network Device Profile is not one of these (at this time).

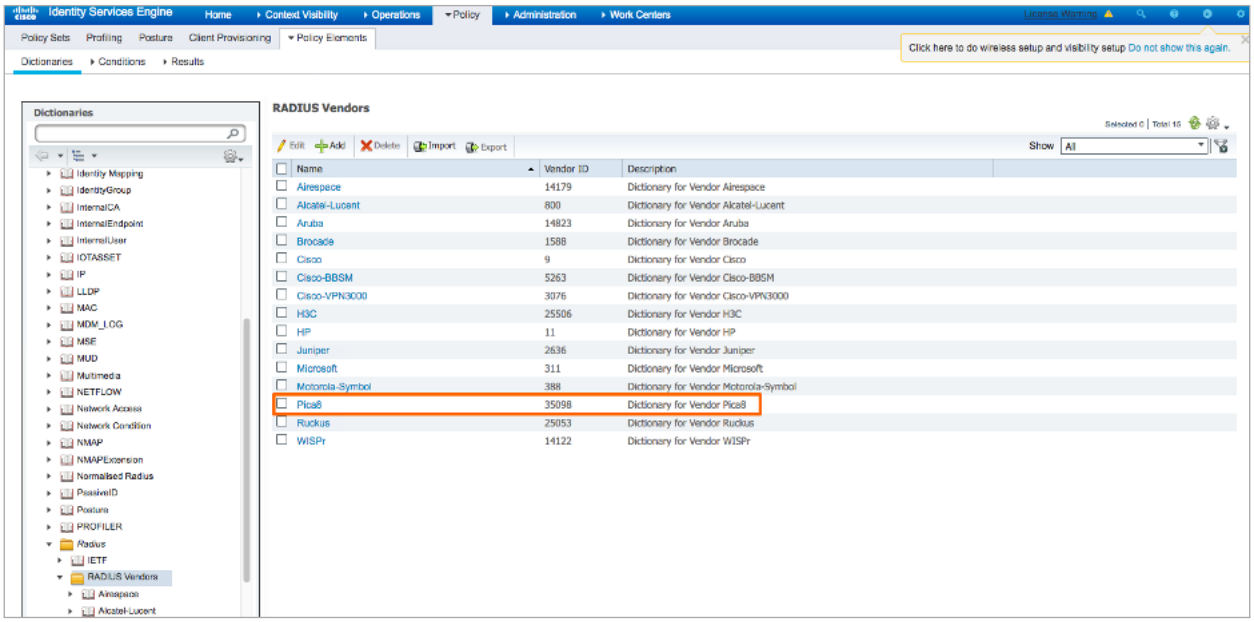
To import the PicOS Radius dictionary for ISE, navigate to **Policy->Policy Elements -> Dictionaries -> System -> Radius -> RADIUS Vendors**, and click Import at the top of the table as shown below.



Click Browse and select Pica8_dictionary_ISE.xml file.



After importing the Pica8 RADIUS dictionary, you will see Pica8 under the Radius vendors as shown below.



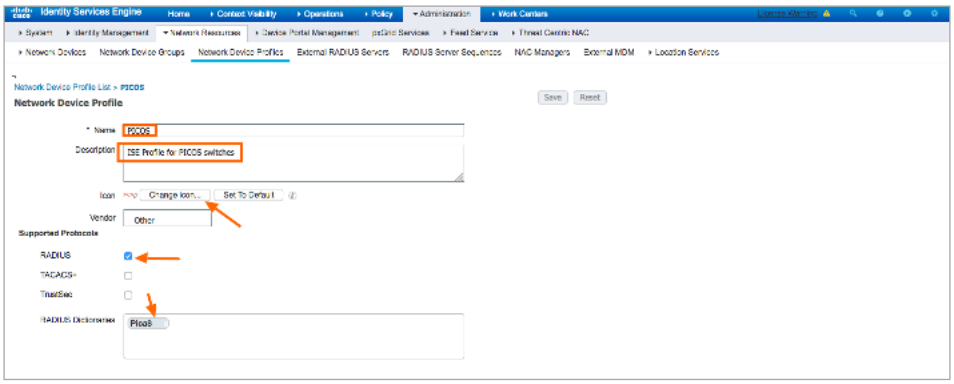
Configure PicOS Network Device Profile

To do this we will create the following Network Device Profile. PicOS – We will create a Network Device Profile called PicOS. It will cover 802.1x and MAB authentication of endpoints. PicOS switches will use this Network Device Profile.

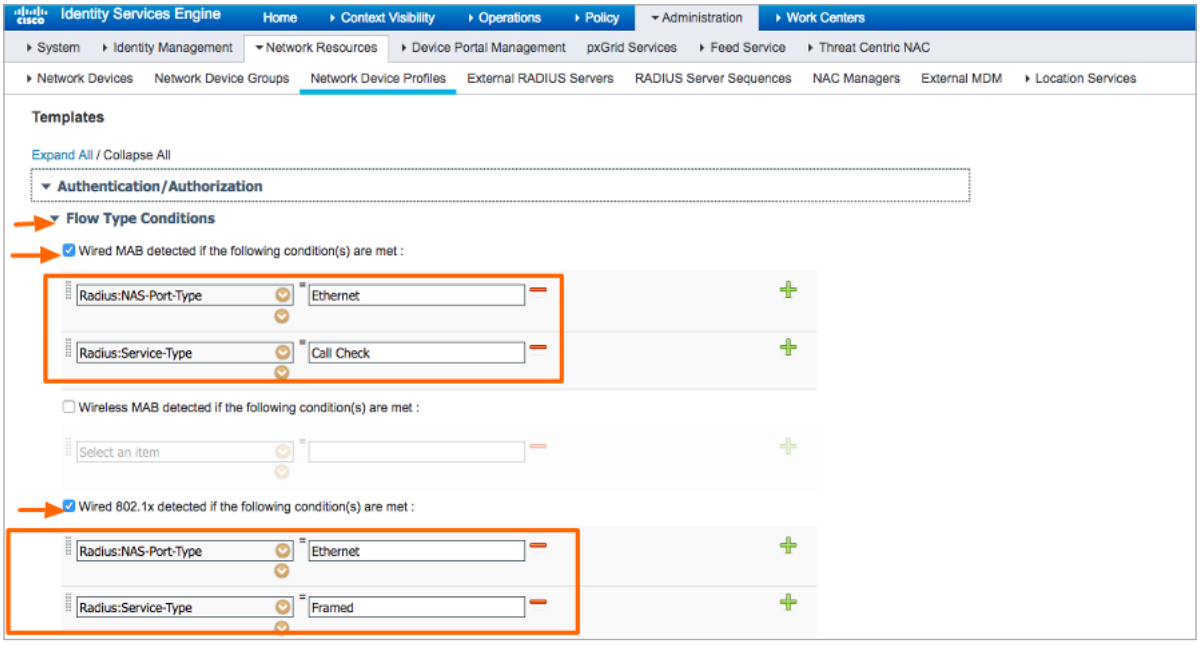
Adding a PicOS Network Device Profile

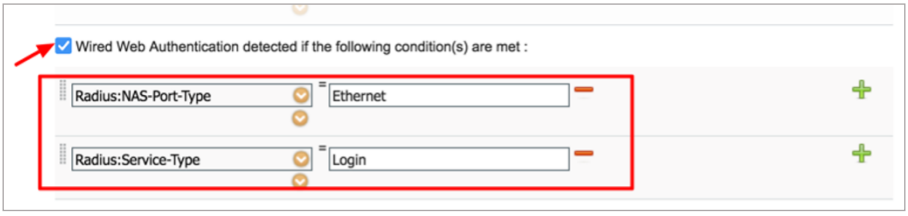
The following are the steps needed to add the PicOS Network Device Profile:

1. Navigate to Administration->Network Resources->Network Device Profiles and add click Add. Enter Name, Description, upload Pica8 icon, select RADIUS, and select Pica8 Dictionary as shown below.

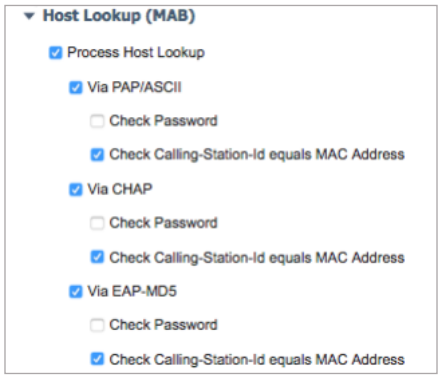


2. Expand ***Flow Type Conditions*** under the ***Authentication/Authorization*** section
   a. Select ***Wired MAB***, and enter the conditions shown below
   b. Select ***Wired 802.1x*** and enter the conditions shown below
   c. Select ***Wired Web Authentication*** and enter the conditions shown below

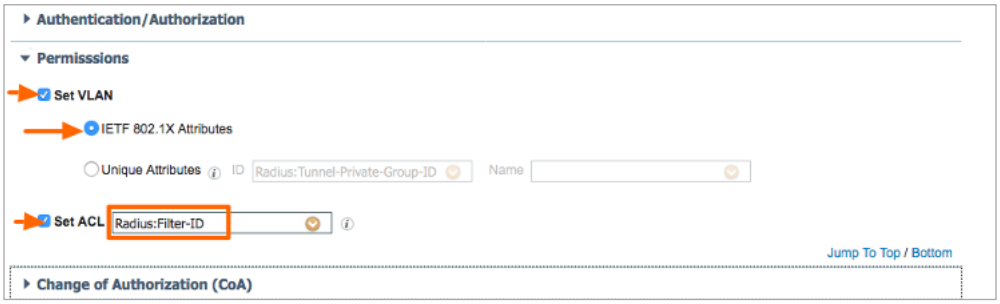




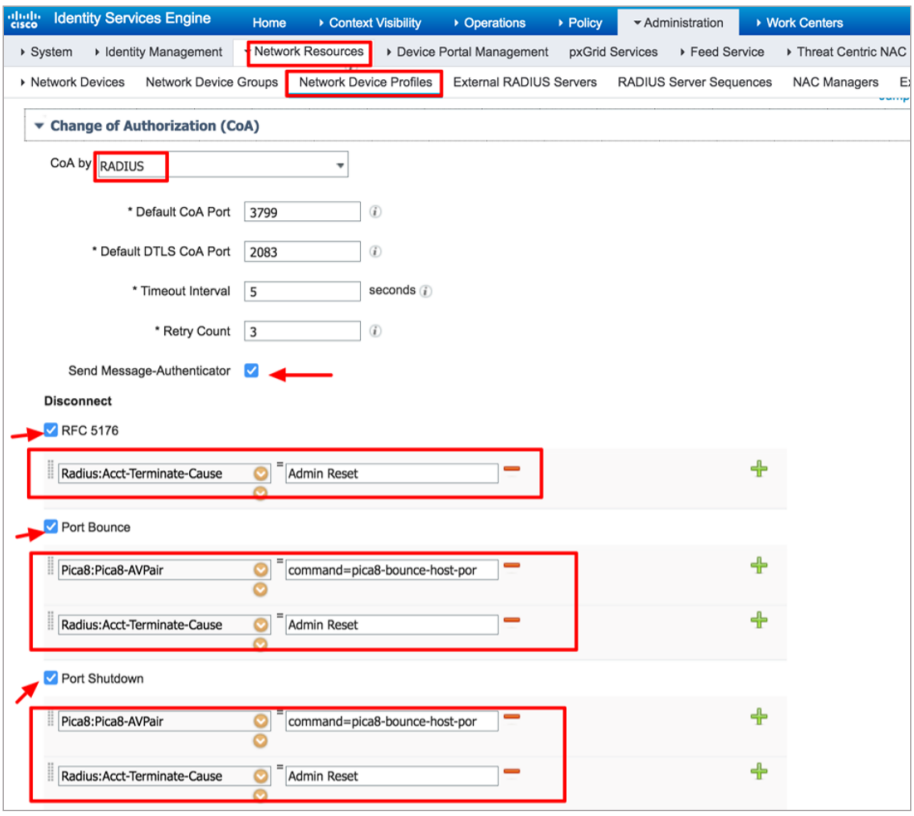
3. Set Host lookup (MAB) as shown below.



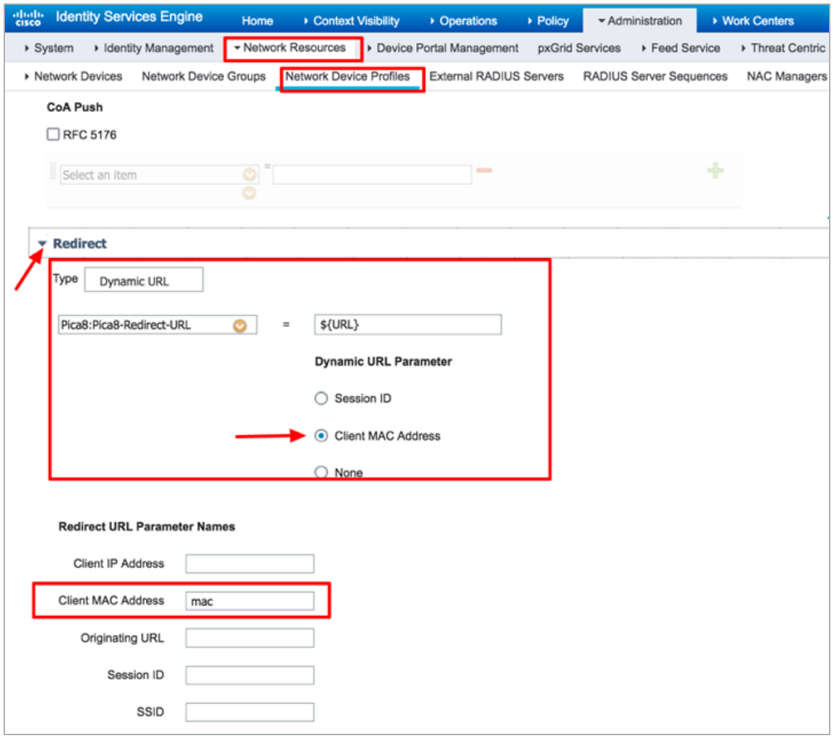
4. Expand ***Permissions***, select ***Set VLAN*** and ***IETF 802.1x Attributes***. Select Set ***ACL*** and set it to ***Radius:Filter:ID*** as shown below. This will enable the dynamic filter functionality in the NAC system.



5. Expand CoA, select Radius for CoA and set CoA parameters as shown below. This template defines how the CoA is sent to the PicOS network device.
   - **Disconnect:** Select how to send a disconnect request to these devices.
     - Select ***RFC 5176*** under Disconnect and set parameters as shown below.
   - **Port Bounce:** Select how to send a Port Bounce request to these devices.
     - Select ***Port Bounce***: Check box to terminate the session and restart the port, and enter parameters as shown below. Set the ***Pica8:Pica8-AVPair*** value is set to command=pica8-bounce-host-port
   - **Port Shutdown:** Select how to send a Port Shutdown request to these devices.
     - Select ***Port Shutdown***: Check box to terminate the session and shutdown the port and enter parameters as shown below. Set the ***Pica8:Pica8-AVPair*** value to ***command=pica8-disable-host-port***



6. Expand ***Redirect***, enter the values as shown below.



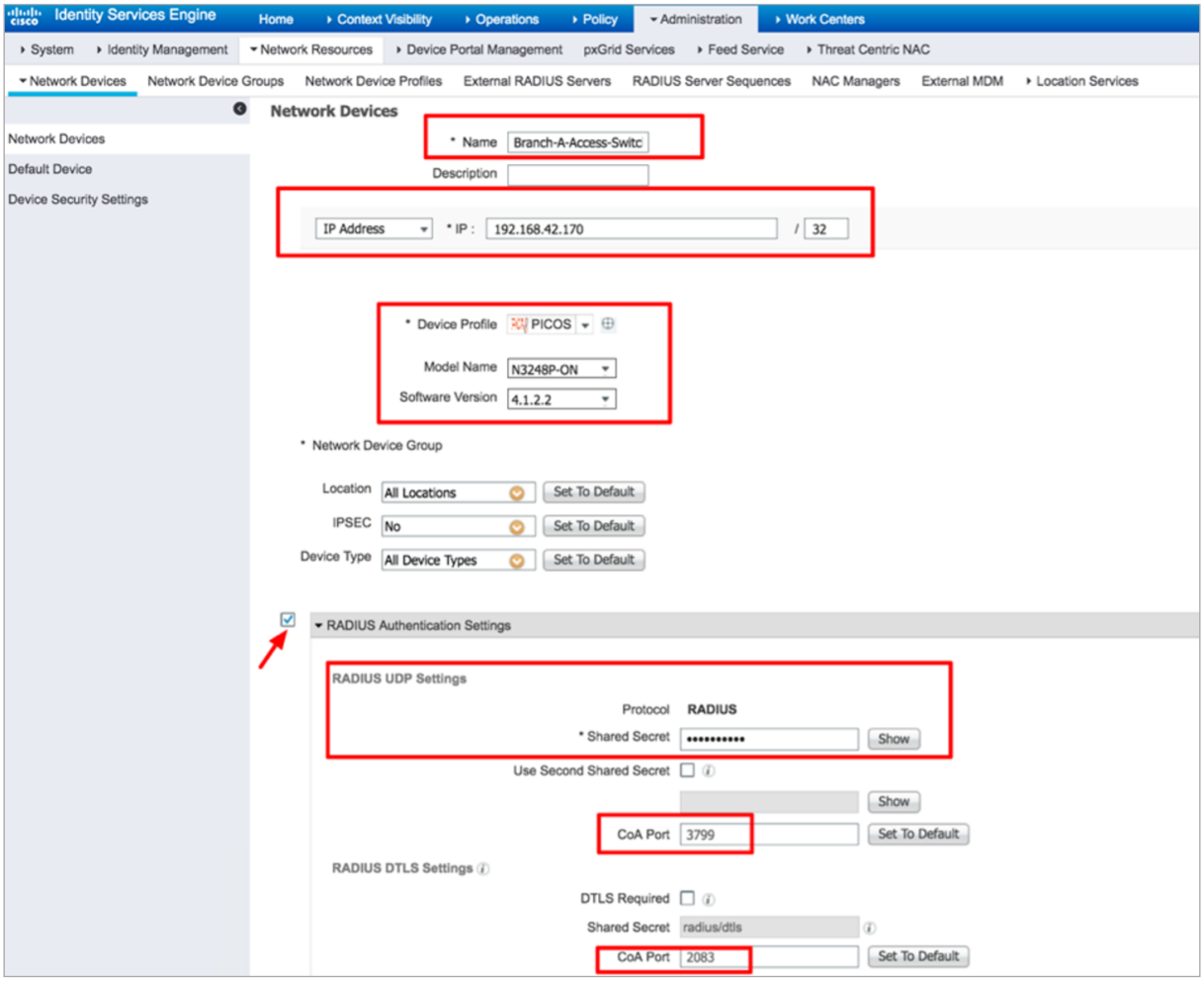
7. Lastly, click ***Submit*** to save the ***PicOS*** Network Device Profile.

Adding a PicOS switch as ISE Network Device

To add a PicOS switch to the Network Device database, navigate to ***Administration ->Network Resources->Network Devices*** and add a new device as shown below. Make sure to enter values for the following fields: ***Name, IP address, Model Name*** and ***Software version***.

Next set ***PicOS*** as the "Device Profile".

Enter the shared secret value ***pica8pica8*** as configured in the PicOS switch. Click ***Submit*** to save the Network Device configuration.



Verifying the Connectivity Between the PicOS Switch and ISE Node

Verify PicOS switch reachability to the ISE node using the following CLI command:

```
admin@P8-Access-BR-1-SW-2>  show dot1x server
Server-IP       Status   Priority  Retry-Interval  Retry-Num  Detect-Interval  Consecutive-Detect-Num
-------------  -------  --------  --------------  ---------  ---------------  ----------------------
192.168.42.105  active   ...       1   Sec(s)      3          5   Sec(s)       3
```

Configuring an Employee Laptop with 802.1x Supplicant

In this example configuration, the Cisco ISE node is configured to authenticate 802.1x users using its local user database. If the authenticated employee is listed in the database as belonging to the ***Pica8 Employee*** group, ISE returns the VLAN ID 10 to the switch in a RADIUS attribute. ISE also returns the ***mac_auth_policy_2*** dynamic ACL for employees. The switch then dynamically configures the laptop to be in VLAN 10 with ***mac_auth_policy_2*** ACL. The Cisco IP Phone is connected to port ***ge-1/1/5*** with the employee laptop connected behind the Cisco IP Phone.

This use case involves configuring the PicOS switch, configuring the ISE node, configuring the windows supplicant on the laptop, and then verifying the NAC configuration.

Configure the PicOS Switch

Configure the Dynamic ACL to be used when an employee laptop is connected to the switch.

```
set protocols dot1x filter mac_auth_policy_2 sequence 999 then action forward
```

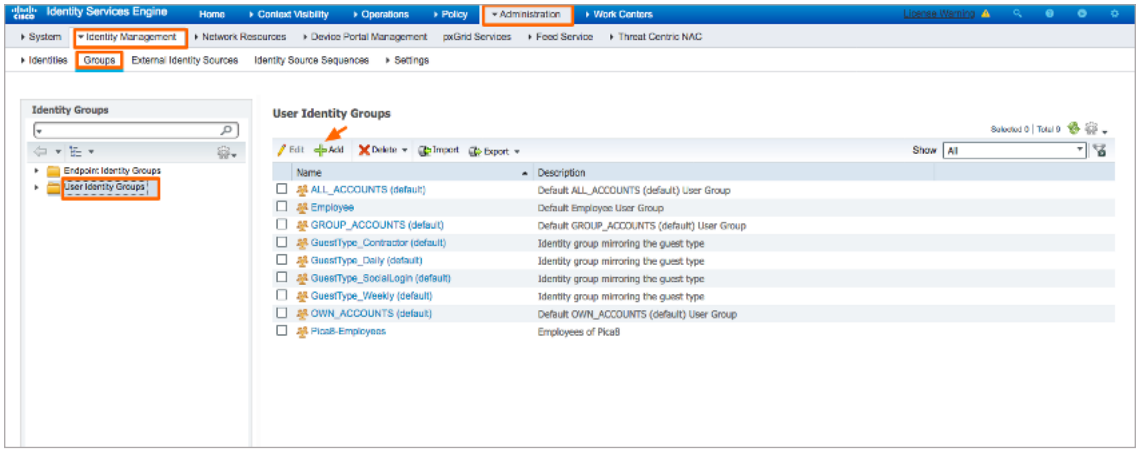
Configure the 802.1x Wired Access Policy for Employee Laptop

Configuring the 802.1x Wired Access policy in ISE for Employee laptop involves the following four steps:

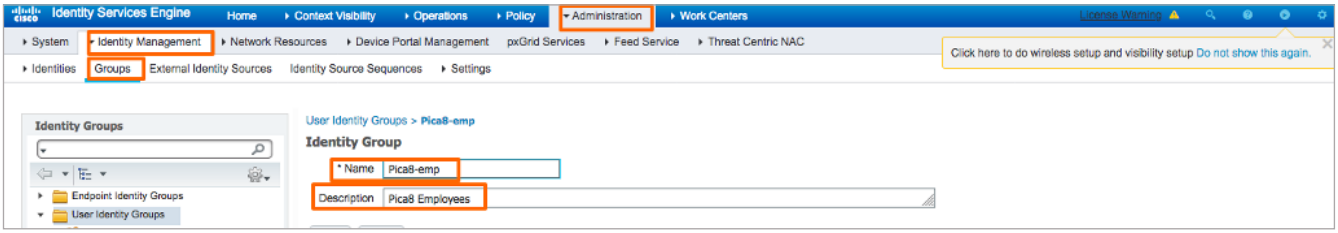
1. Create User Identity groups and integrate with AD or add local users
2. Create an Authorization Profile to dynamically assign VLAN 10 for employee laptops running 802.1x supplicant
3. Create an Authorization Profile to dynamically assign an ACL called mac_auth_policy_2 to the employee laptops that will provide full corporate network access
4. Create a Wired Access policy for Employee Laptop running 802.1x supplicant (called Pica8-Employee) that will use the above two authorization profiles

Creating User Identity Group and add Users

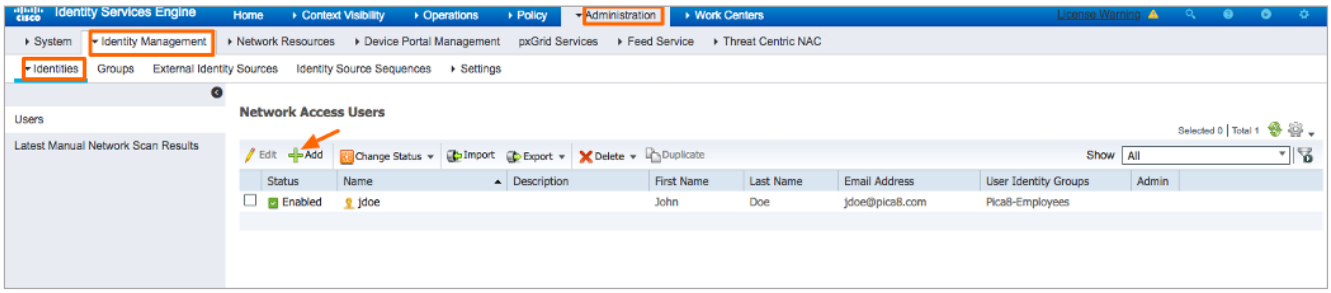
Cisco ISE allows for Active Directory integration. Here we will use local groups and users defined in ISE for this integration test. To add a group, navigate to ***Administration -> Identity Management->Groups->User Identity Groups*** and click ***+*** as shown below.



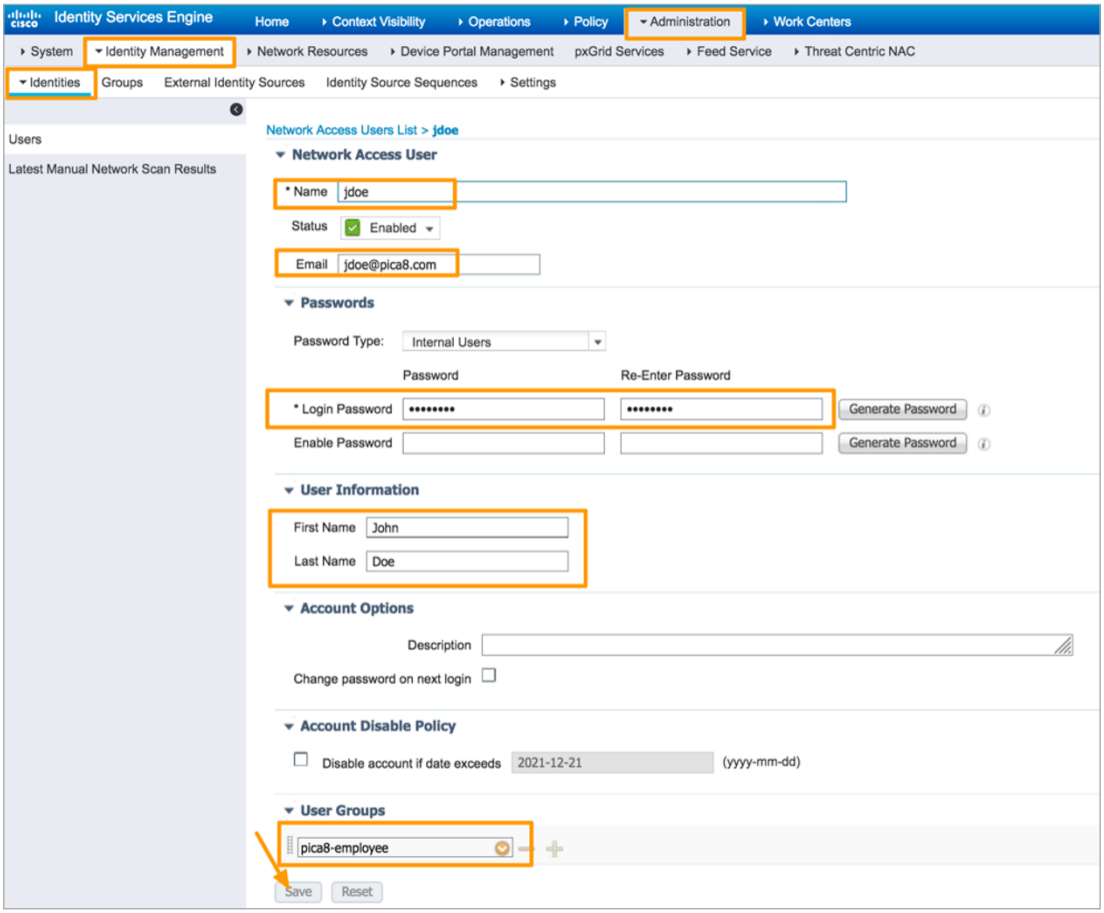
Enter ***Name*** and ***Description*** of the Group as shown below and click ***Submit***.



To add a user, navigate to ***Administration -> Identity Management->Identities*** and click ***+*** as shown below.

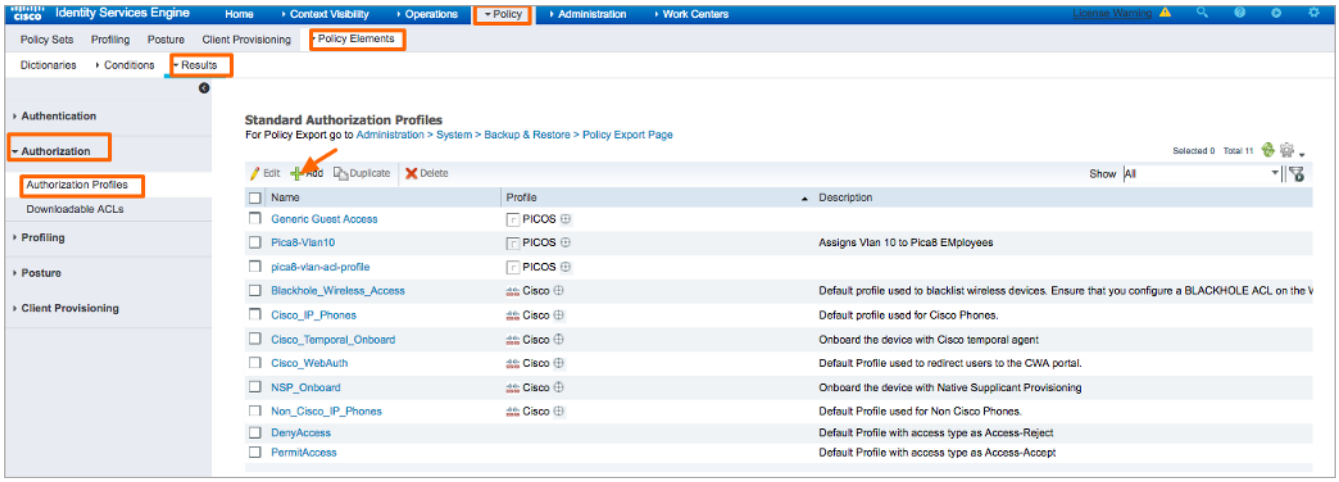


Enter ***Name, Email, Login Password*** and select ***Pica8-Employees*** *for* ***User Groups*** as shown below and click ***Submit***.
In this example we are adding ***Network Access User*** account for John Doe.

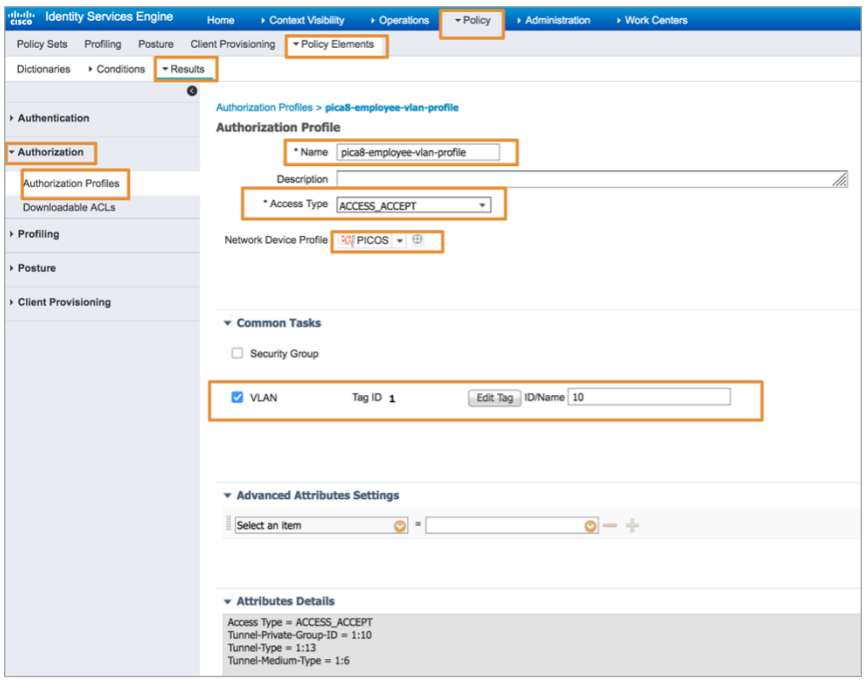


Create an Authorization Profile to Dynamically Assign a VLAN

To create the Authorization Profile, navigate to ***Policy -> Policy Elements -> Results -> Authorization -> Authorization Profiles*** and click ***+*** as shown below.



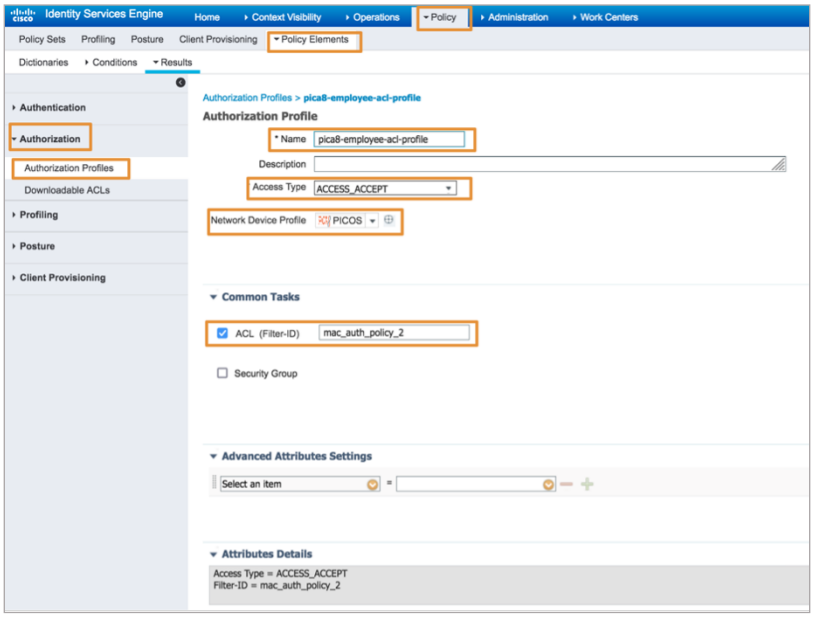
Enter ***Name, Description***, set ***Access Type to ACCESS_ACCEPT***, and set *Network Device Profile* to ***PicOS***. Check the box for ***VLAN*** and enter an attribute value that identifies a VLAN. In this example VLAN ID 10 is used. Click ***Submit***.



Create an Authorization Profile to Dynamically assign an ACL

To create an Authorization Profile, navigate to ***Policy -> Policy Elements -> Results -> Authorization -> Authorization Profiles*** and click ***+.***

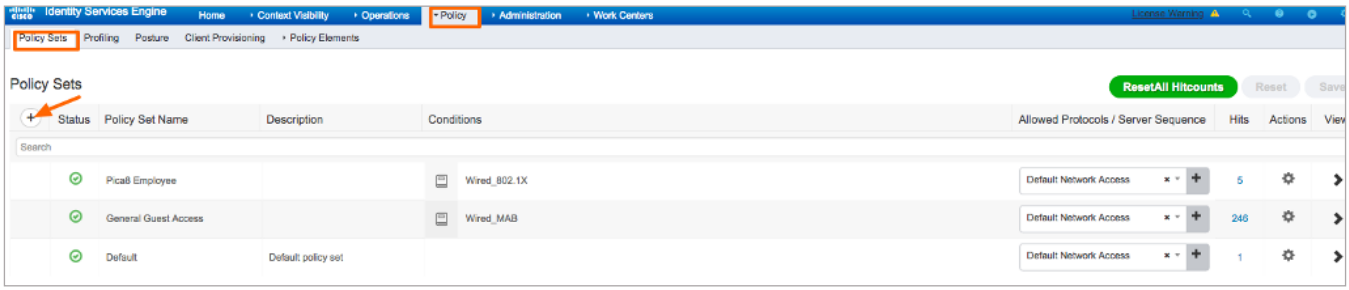
Enter ***Name, Description***, set ***Access Type to ACCESS_ACCEPT***, set ***Network Device Profile*** to ***PicOS***. Check the box for ***ACL*** and enter value for ACL. In this example mac_auth_policy_2 is used. Click *Submit*.



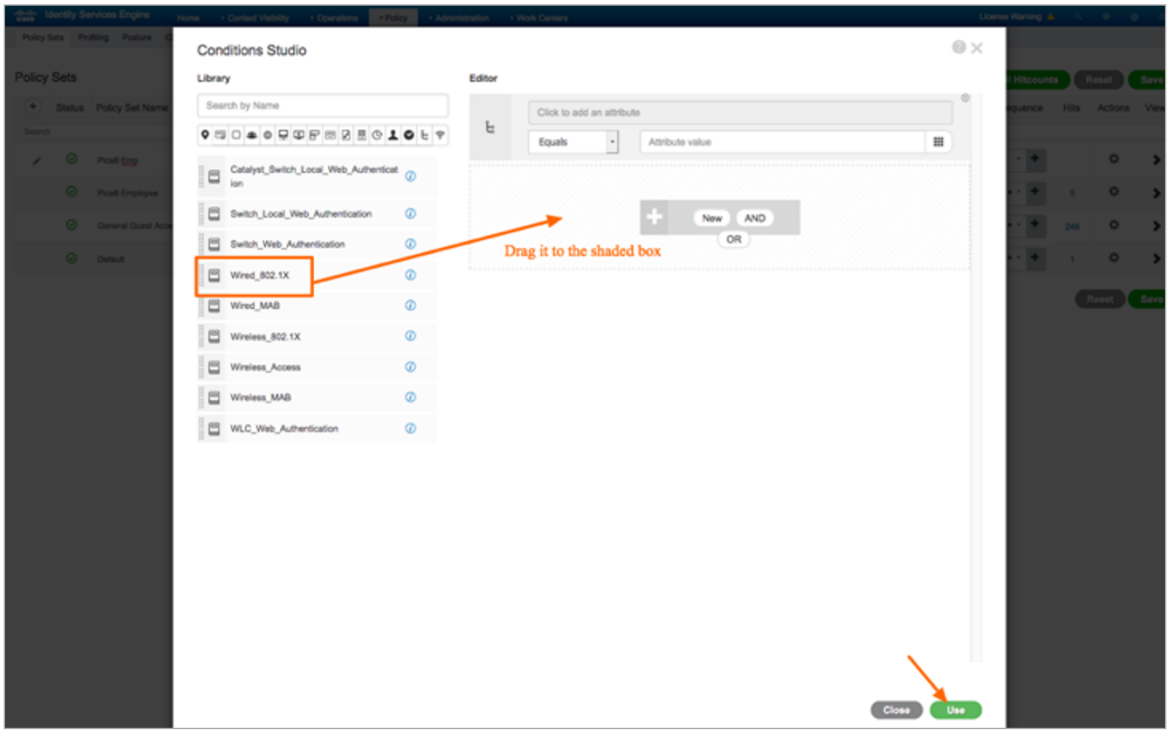
Create the Wired Access Policy for an Employee Laptop Running 802.1x Supplicant

Cisco ISE is a policy-based, network-access-control solution that offers network access policy sets, thus allowing you to manage several different network access use cases such as wireless, wired, guest, and client provisioning. Policy sets (both network access and device administration sets) enable you to logically group authentication and authorization policies within the same set. You can have several policy sets based on an area, such as policy sets based on location, access type and similar parameters.

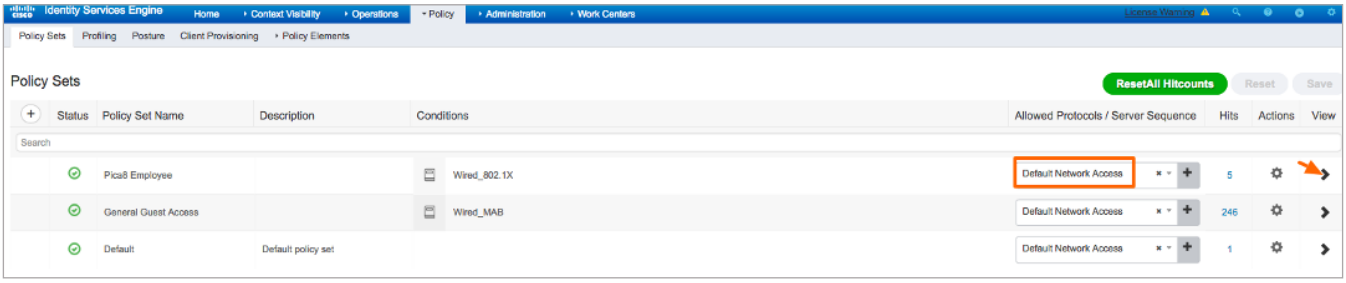
Let us create a ***Policy Set*** called ***Pica8-Employee*** to authenticate ***Wired 802.1X*** users and place the users on VLAN 10 and apply ***mac_auth_policy_2*** ACL. Navigate to ***Policy -> Policy Sets*** and click ***+*** as shown below.



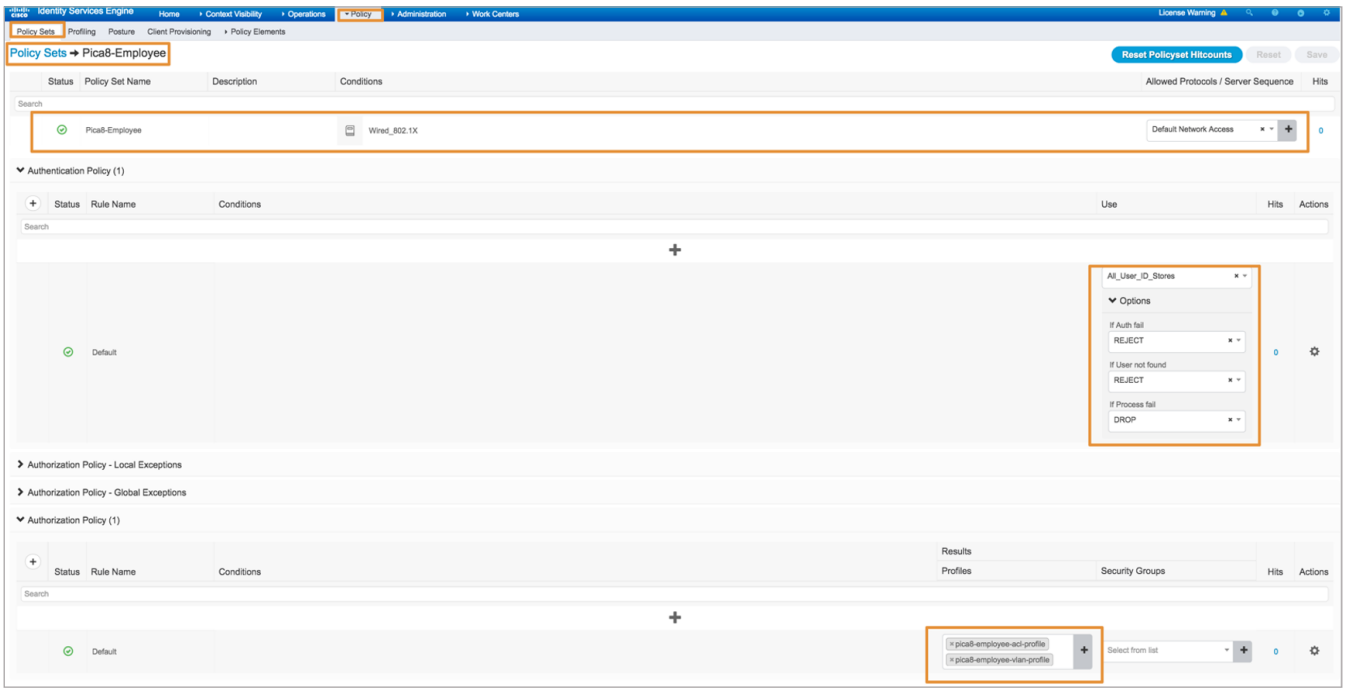
Enter ***Policy Set*** name as ***Pica8_Employees*** and click ***+*** *sign* under ***Conditions, drag Wired_MAB*** to the shaded box and click ***Use***.



Set ***Allowed Protocols*** to ***Default Network Access***, click ***Save*** and click **>** sign as shown below.



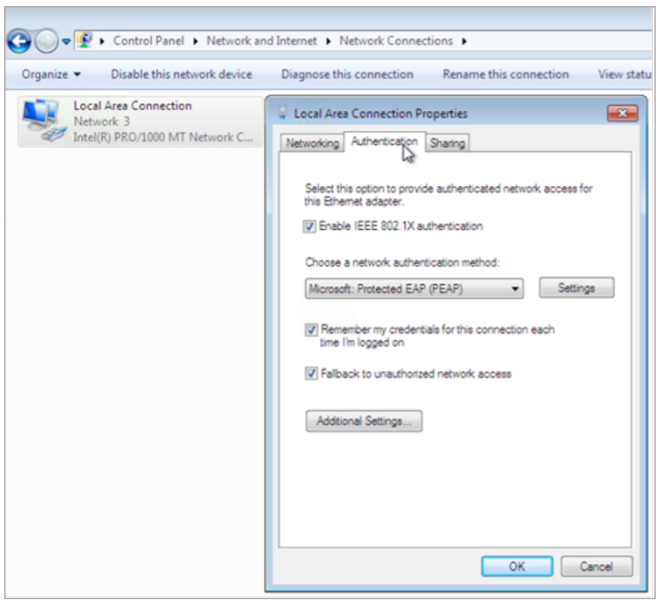
Set ***Authentication Policy Options*** as shown below. Set ***Authorization Policy*** *to* ***Pica8-employee-acl-profile*** and ***Pica8-employee-VLAN-profile*** as shown below. Click ***Save***.



Configuring the Windows Supplicant on the Laptop

On the Windows laptop enable 802.1X PEAP authentication for the Local Area Connection.

Under ***Control Panel > Network and Sharing Center > Change Adaptor Settings***, right-click ***Local Area Connection*** and then click ***Properties***. On the ***Authentication*** tab of the Local Area Connection Properties window, configure the properties as shown.



Click ***Settings*** to display the Protected EAP Properties window. In the Protected EAP Properties window, click ***Configure*** to configure the Secured password (EAP-MSCHAP v2). Set the ***Automatically use my Windows logon name and password*** check box. Credentials for the laptop are the same as the credentials stored on the ISE server.

If your ISE node is configured to use Windows Active Directory to authenticate users, you would leave this option selected.

Click ***OK***. It will trigger a login screen. Enter the user ID jdoe and password of the local user that you added to local user database on the ISE server.

Verifying the NAC Configuration

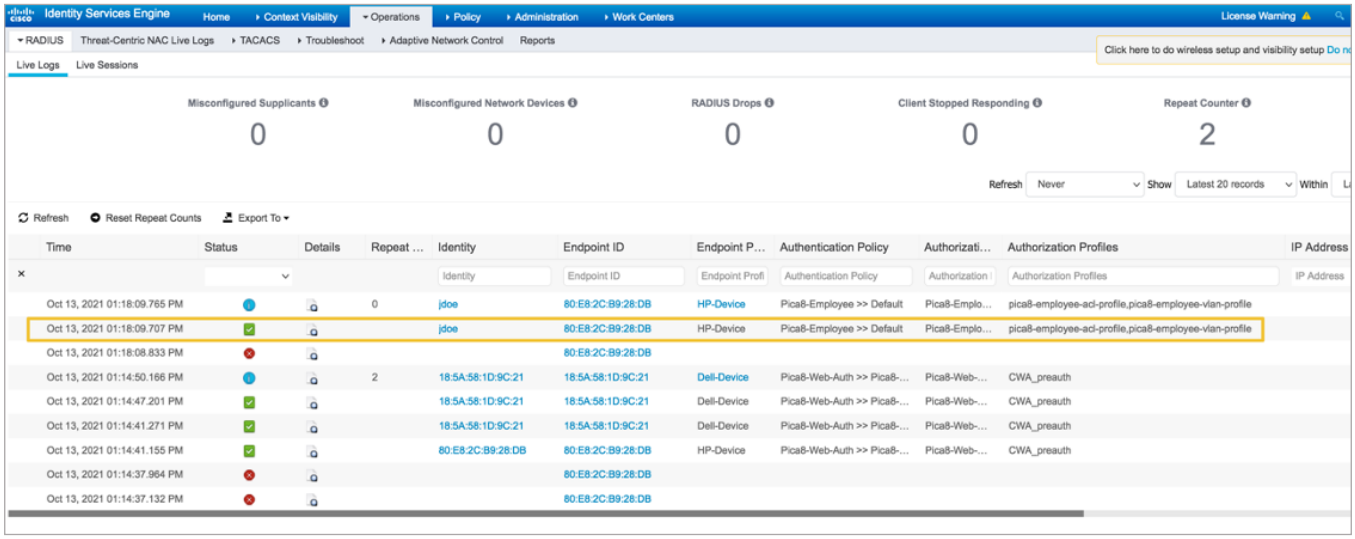
After connecting the Employee Windows laptop to the Cisco IP Phone, authenticate the user ***jdoe*** with login credentials that we configured earlier in the ISE node database. After Authentication, make sure you are able to reach www.example.com from a browser application.

On the PicOS switch run the following CLIs to verify the 802.1x NAC configuration.

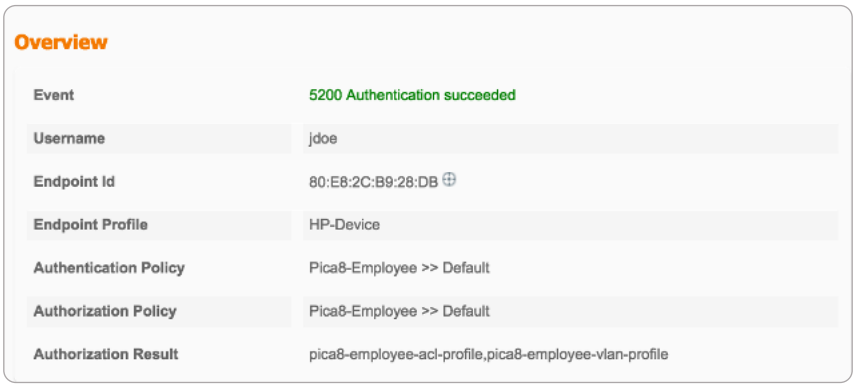
To check the 802.1x authentication run the following CLI:

```
admin@P8-Access-BR-1-SW-2> show dot1x interface gigabit-ethernet ge-1/1/5
Interface ge-1/1/5:
============================================================
  Client MAC                : 80:e8:2c:b9:28:db
  Status                    : authorized
  Success Auth Method       : Dot1x
  Last Success Time         : Wed Oct 13 13:18:25 2021
  Traffic Class             : Other
  Dynamic VLAN ID           : 10 (active)
  Dynamic Filter Name       : mac_auth_policy_2 (active)
============================================================
```

To view real-time authentication summary in ISE, navigate to ***Operations->RADIUS->Live Logs*** and click on the icon under the ***Details*** column as shown below.



Clicking the icon under the ***Details*** column opens the ***Authentication Detail Report*** in a new browser window. This report offers information about authentication status and related attributes, and authentication flow.



Overview

Event	5200 Authentication succeeded
Username	jdoe
Endpoint Id	80:E8:2C:B9:28:DB
Endpoint Profile	HP-Device
Authentication Policy	Pica8-Employee >> Default
Authorization Policy	Pica8-Employee >> Default
Authorization Result	pica8-employee-acl-profile,pica8-employee-vlan-profile

IP Phone Authentication

A Cisco ISE node is configured to authenticate IP phone Endpoint Groups with MAB authentication. Here the Cisco IP Phone is connected to port ***ge-1/1/5***, and voice VLAN 800 is configured on the PicOS switch.

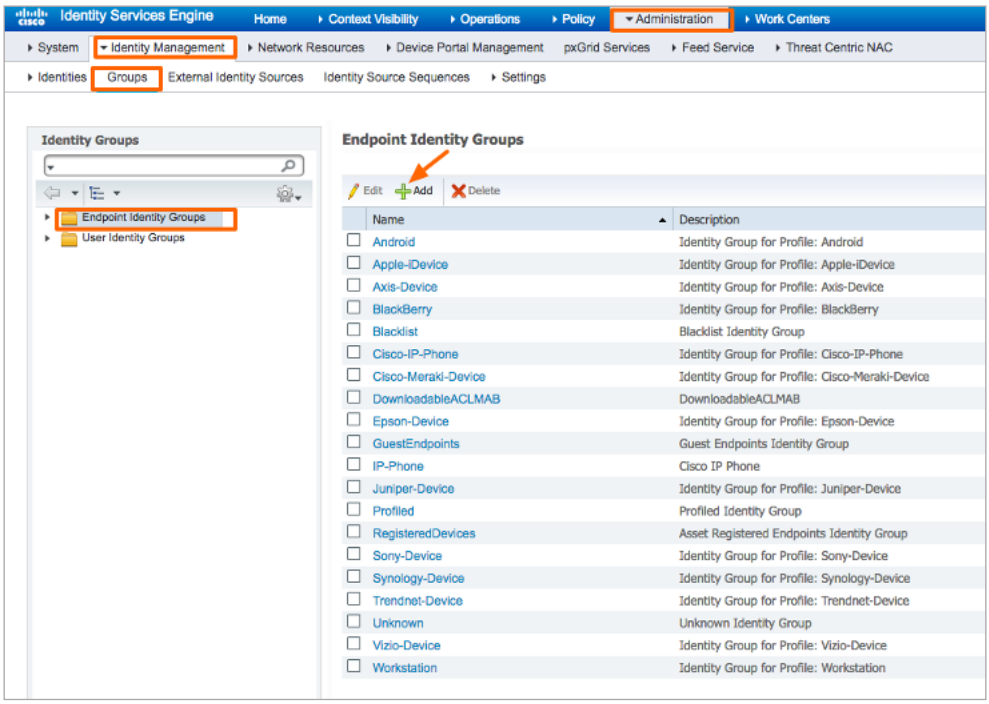
Configuring the MAB Wired Access policy in ISE for IP Phones

Configuring the MAB Wired Access Policy in ISE for IP Phones involves following three steps:

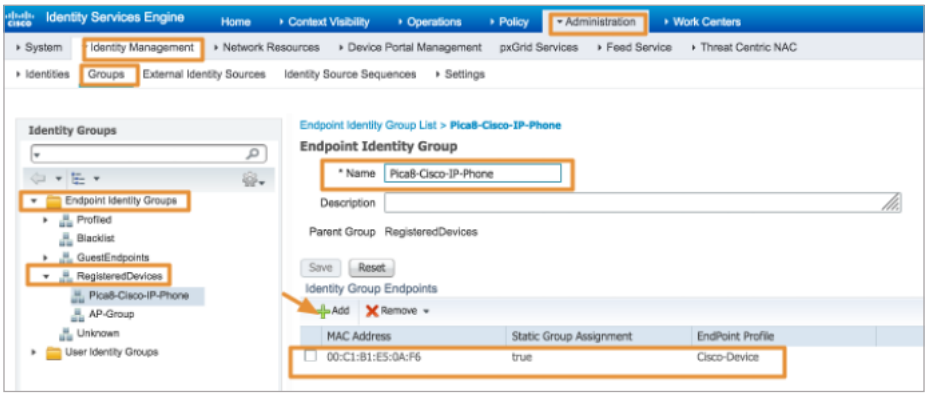
1. Create an IP-Phone Endpoint Identity Group and add IP Phone Mac addresses.
2. Create an Authorization Profile to dynamically assign voice VLAN 800 for IP Phones.
3. Create a Wired Access policy for the IP Phone that will use the above authorization profile.

Creating an IP-Phone Endpoint Identity Group and add IP Phone Mac Addresses

To create ***IP_phone*** Endpoint Identity Group , navigate to ***Administration -> Identity Management -> Groups -> Endpoint Identity Groups-> Registered Devices*** and click ***+*** as shown below.

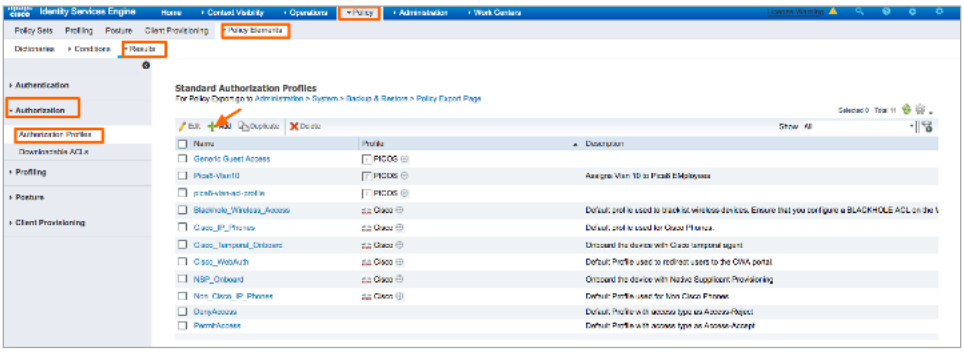


Enter ***Name, Description*** and click ***Submit***. Select Pica8-Cisco-IP-Phone Groups and click ***+*** and select the MAC address of the IP phone to add IP Phone to this Endpoint Identity Group as shown below.

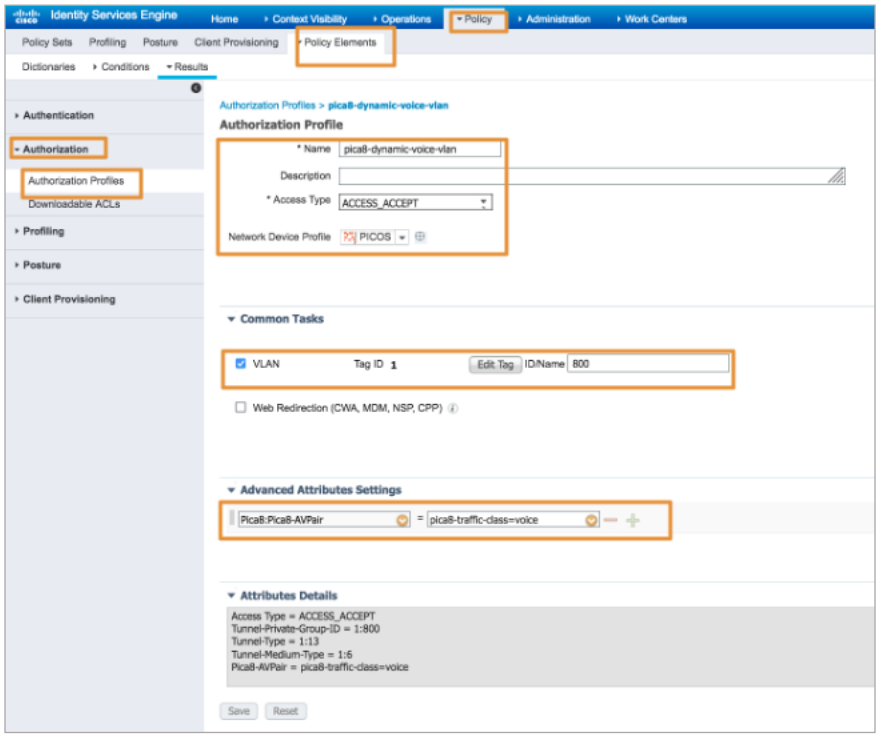


Create an Authorization Profile to Dynamically Assign a Voice VLAN

To create an Authorization Profile, navigate to ***Policy -> Policy Elements -> Results -> Authorization -> Authorization Profiles*** and click ***+*** as shown below.

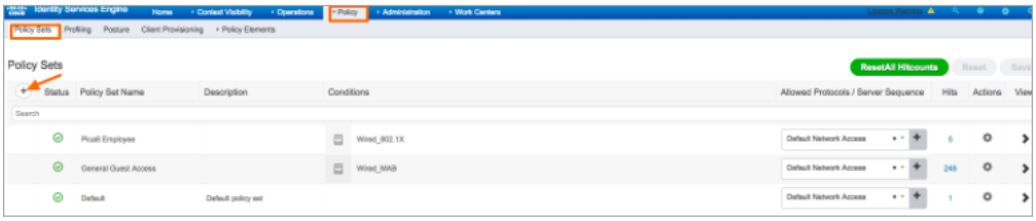


Enter ***Name, Description***, and set ***Access Type to ACCESS_ACCEPT***, then set ***Network Device Profile to PicOS***. Check the box for ***VLAN*** and enter an attribute value that identifies a VLAN. In this example VLAN ID 800 is used for Voice VLAN. Expand ***Advanced Attribute Settings*** select ***Pica8:Pica8-AVPair*** and set the value as ***pica8-traffic-class=voice***. Click ***Submit***.

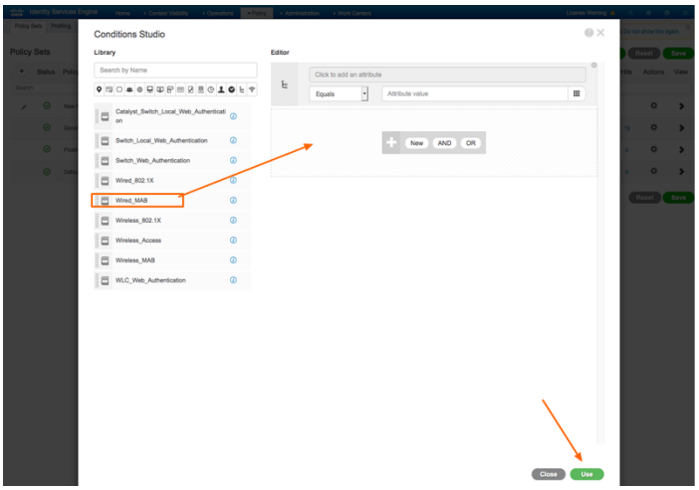


Create a Wired Access Policy for an IP Phone

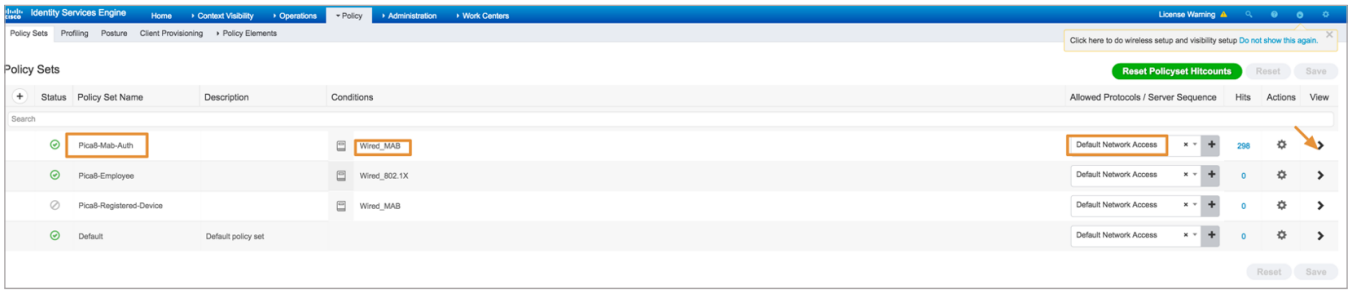
Let us create a ***Policy Set*** called ***Pica8-Mab-Auth*** to authenticate various ***Endpoint Identity Groups*** using ***MAB*** authentication. We will place the IP Phones on voice VLAN 800. Navigate to ***Policy -> Policy Sets*** and click ***+*** as shown below.



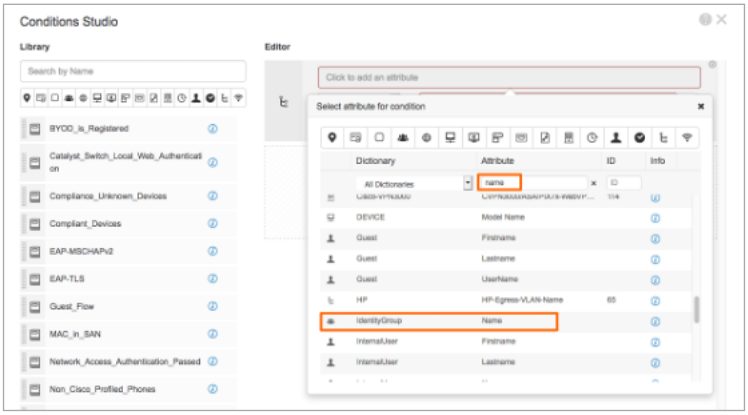
Enter the ***Policy Set*** name as ***General Access*** and click ***+*** sign under ***Conditions***, drag ***Wired_MAB*** to the shaded box and click ***Use***.



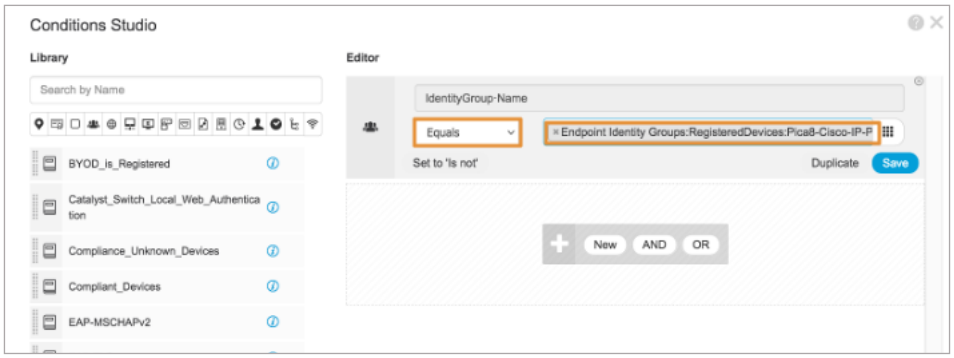
Set ***Allowed Protocols*** to ***Default Network Access***, click ***Save*** and click ***>*** sign as shown below.



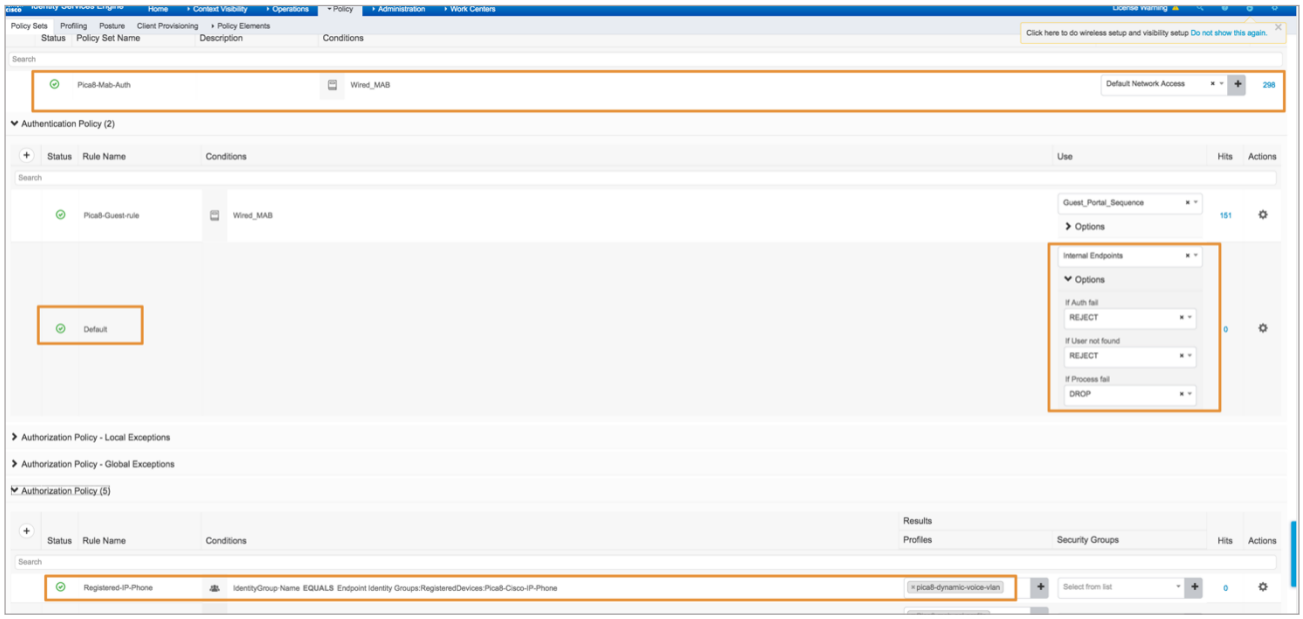
Set ***Authentication Policy Options*** as shown below. Create a new rule under ***Authorization Policy*** called ***Registered-IP-Phone***. Click ***+*** sign under ***Conditions***. In the ***Attribute*** field, search for the string ***name*** and then select the ***IdentityGroup Name*** attribute as shown below.



Select ***Endpoint Identity Groups:RegisteredDevices:Pica8-Cisco-IP--Phone*** as shown below and click ***Save***.



Set the ***Registered-IP-Phone*** rule to ***Pica8-dynamic-voice-VLAN*** Authorization profile as shown below. Click ***Save***.



Verifying the NAC Configuration

Connect the IP Phone to port ***ge-1/1/5***.

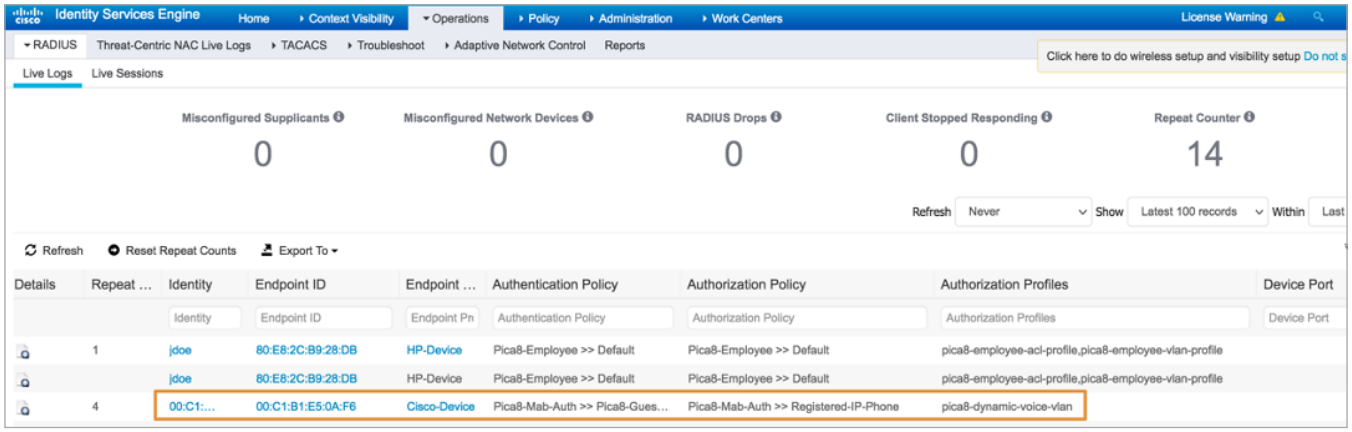
On the PicOS switch, run the following CLIs to verify the MAB Authentication for the IP Phone.

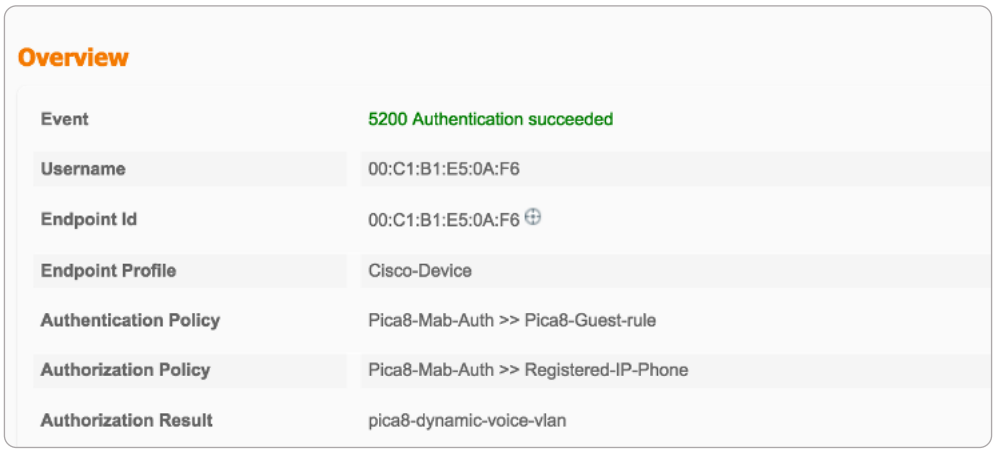
```
admin@P8-Access-BR-1-SW-2> show dot1x interface gigabit-ethernet ge-1/1/5
Interface ge-1/1/5:
============================================================
  Client MAC                : 00:c1:b1:e5:0a:f6
  Status                    : authorized
  Success Auth Method       : MAB
  Last Success Time         : Wed Oct 13 13:31:53 2021
  Traffic Class             : Voice
  Dynamic VLAN ID           : 800 (active)
============================================================
```

When Employee laptop with 802.1x supplicant is connected behind an IP phone, following is the output:

```
admin@P8-Access-BR-1-SW-2> show dot1x interface gigabit-ethernet ge-1/1/5

Interface ge-1/1/5:
============================================================
  Client MAC                : 00:c1:b1:e5:0a:f6
  Status                    : authorized
  Success Auth Method       : MAB
  Last Success Time         : Wed Oct 13 13:31:53 2021
  Traffic Class             : Voice
  Dynamic VLAN ID           : 800 (active)
============================================================
  Client MAC                : 80:e8:2c:b9:28:db
  Status                    : authorized
  Success Auth Method       : Dot1x
  Last Success Time         : Wed Oct 13 13:45:06 2021
  Traffic Class             : Other
  Dynamic VLAN ID           : 10 (active)
  Dynamic Filter Name       : mac_auth_policy_2 (active)
============================================================
```

To view a real-time authentication summary navigate to ***Operations->RADIUS->Live Logs*** and click on the icon under the ***Details*** column as shown below.





Access Point Authentication

Access Point is connected to port ***ge-1/1/6*** and authenticated using MAB.

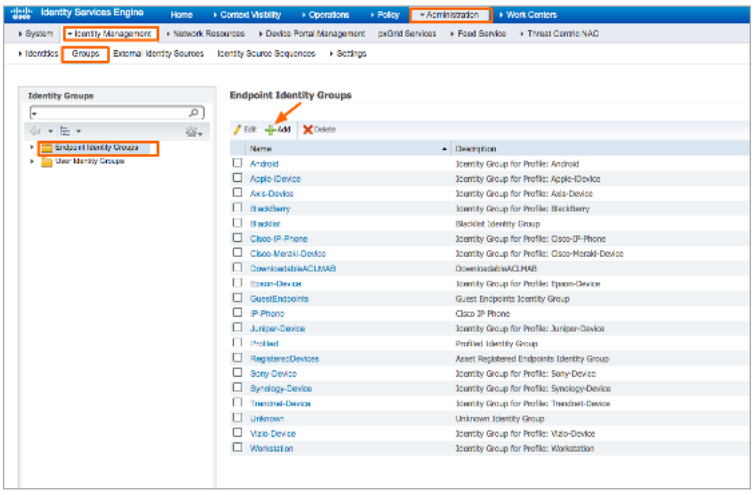
Configuring the MAB Wired Access Policy in ISE for an Access Point

Configuring the MAB Wired Access policy in ISE for Access Point involves following four steps:

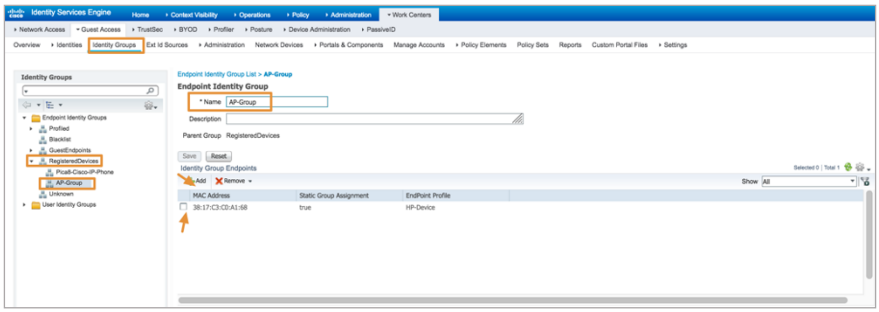
1. Create an Endpoint Identity Group for Access Points and add the Access Point Mac addresses.
2. Create an Authorization Profile to dynamically assign VLAN 10 for the Access Points.
3. Create an Authorization Profile to use downloadable ACL mac_auth_policy_3 configured in ISE.
4. Create a Wired Access policy for Access Points that will use the above two authorization profiles.

Create an Endpoint Identity Group for Access Points and add Access Point Mac Addresses

To create ***AP-Group Endpoint Identity Group***, navigate to ***Administration -> Identity Management -> Groups -> Endpoint Identity Groups->Registered Devices*** and click ***+*** as shown below.

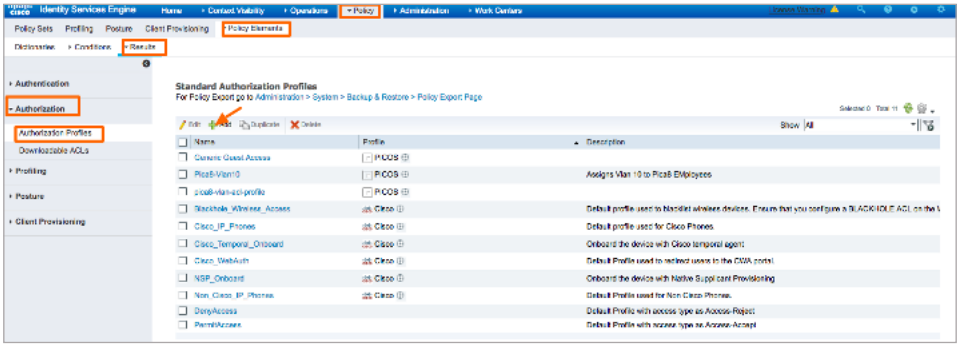


Enter ***Name and Description*** and click ***Submit***. Select ***AP-Group Endpoint Identity Groups*** and click ***+*** and select the MAC address of the Access Point to add MAC address of Access Point as shown below.

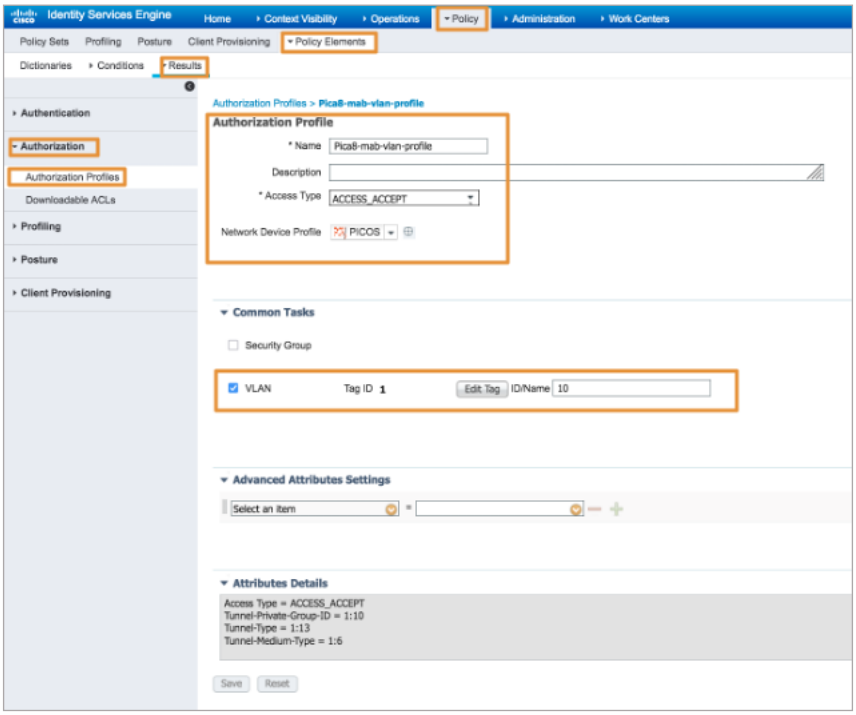


Create an Authorization Profile to Dynamically Assign a VLAN for Access Points

To create the Authorization Profile, navigate to ***Policy -> Policy Elements -> Results -> Authorization -> Authorization Profiles*** and click ***+*** as shown below.



Enter ***Name, Description***, set ***Access Type to ACCESS_ACCEPT***, and set ***Network Device Profile*** to ***PicOS***. Check the box for ***VLAN*** and enter an attribute value that identifies a VLAN. In this example VLAN ID 10 is used. Click ***Submit***.



In the above example we have added ***Pica8-mab-VLAN-profile*** for dynamically assigning a VLAN for Access Points.

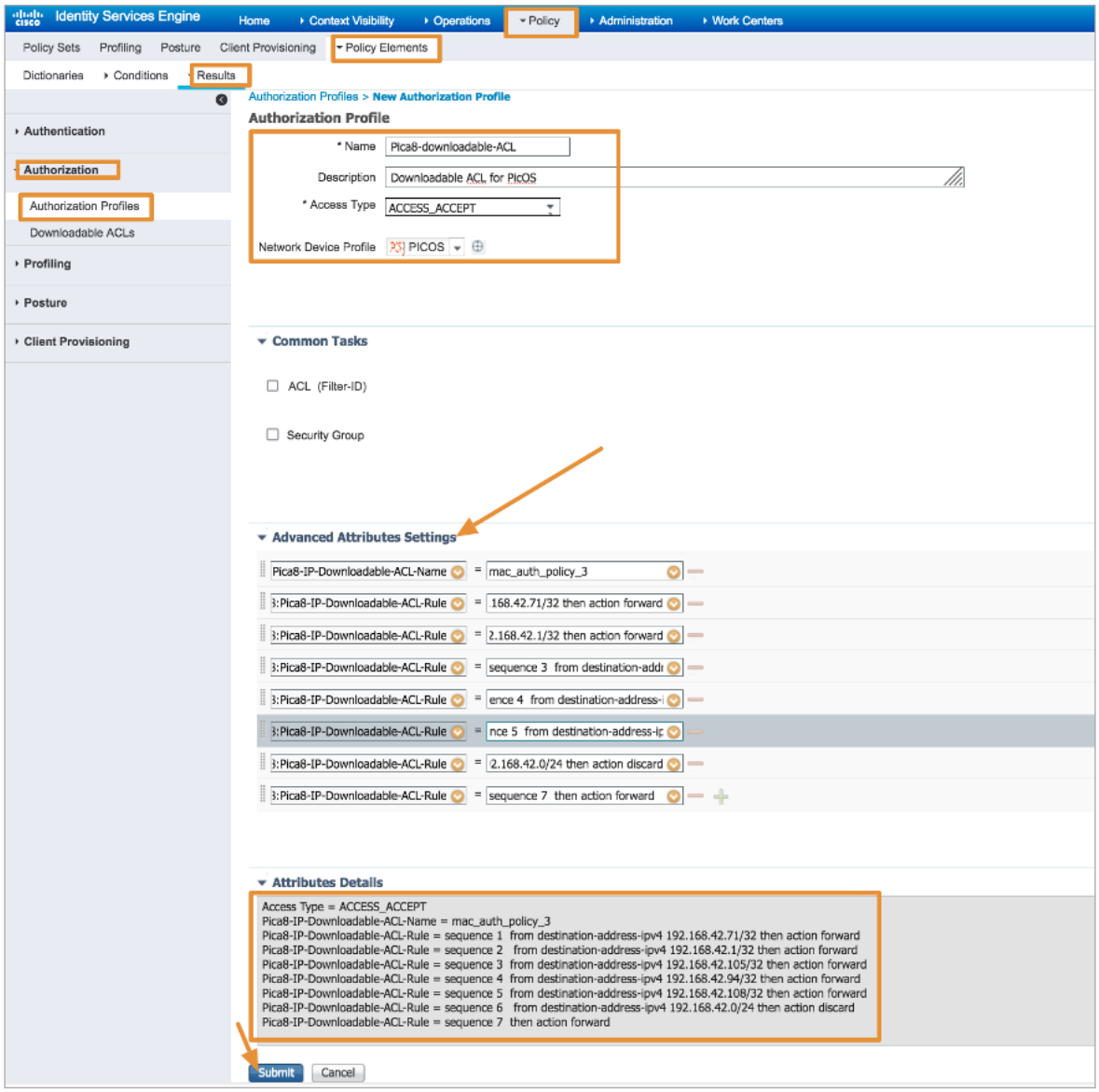
Create Authorization Profile to Use Downloadable ACL mac_auth_policy_3 Configured in ISE

To create the Authorization Profile, navigate to Policy -> Policy Elements -> Results -> Authorization -> Authorization Profiles and click + as shown below.

Enter ***Name*** as ***Pica8-Downloadable-ACL, Description***, set Access Type to ***ACCESS_ACCEPT***, then set the ***Network Device Profile*** to ***PicOS*** as shown below. Expand ***Advanced Attribute Settings*** and set the attributes shown below to download ACL from ISE:

- Select ***Pica8:Pica8-IP-Downloadable-ACL-Name attribute and set man_auth_policy_3*** as value.
- Select ***Pica8:Pica8-IP- Downloadable-ACL-Rule*** and set the rules as shown below. Click ***Submit***.

ACL rules only permit the endpoint to access a few servers in 192.168.42.0/24 network.

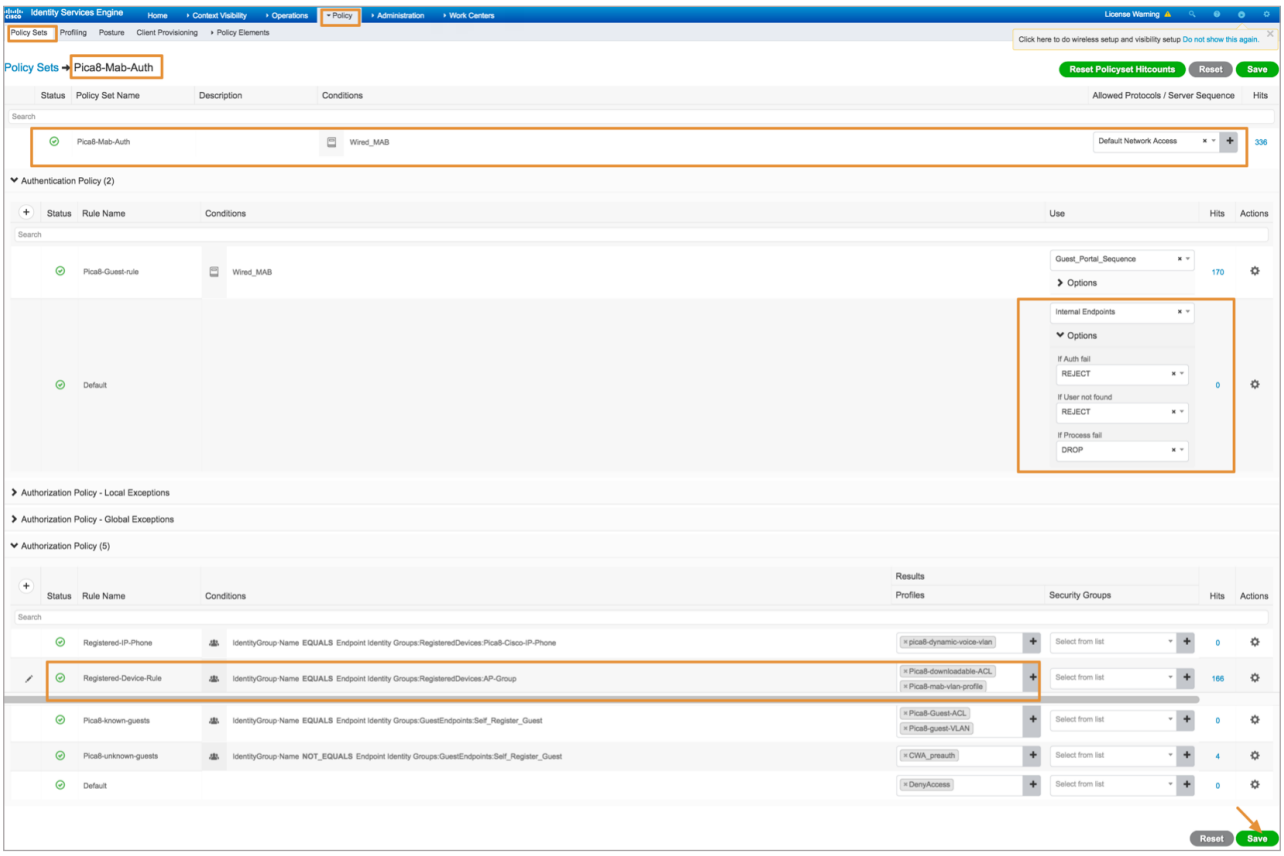


Please note: ISE and other Radius servers have threshold of 4096 bytes for size of the Access-Accept messages used by the Radius server for DACL. If your ACL size is huge, you will run into problems. For this purpose PicOS uses abbreviated downloadable ACLs. Please refer to the Downloadable ACL section in the documentation page.

Create a Wired Access Policy for the Access Point

Let us create a new rule in the ***Policy Set called Pica8-Mab-Auth*** to authenticate the Access Point, place it on VLAN 10, and use the downloadable ACL we have set up in the earlier step. Navigate to ***Policy -> Policy Sets*** and click **>** on the ***Pica8-Mab-Auth*** policy we previously created as shown below.

Create a new rule under Authorization Policy called ***Registered-Device-Rule***. Click the **+** sign under ***Conditions***. Select ***Endpoint Identity Groups:Registered Devices:AP-Group*** for ***Conditions*** as shown below and click ***Save***. Set the Authorization Policy for this rule to ***Pica8-Downloadable-ACL and Pica8-mab-VLAN-profile*** as shown below. Click ***Save***.

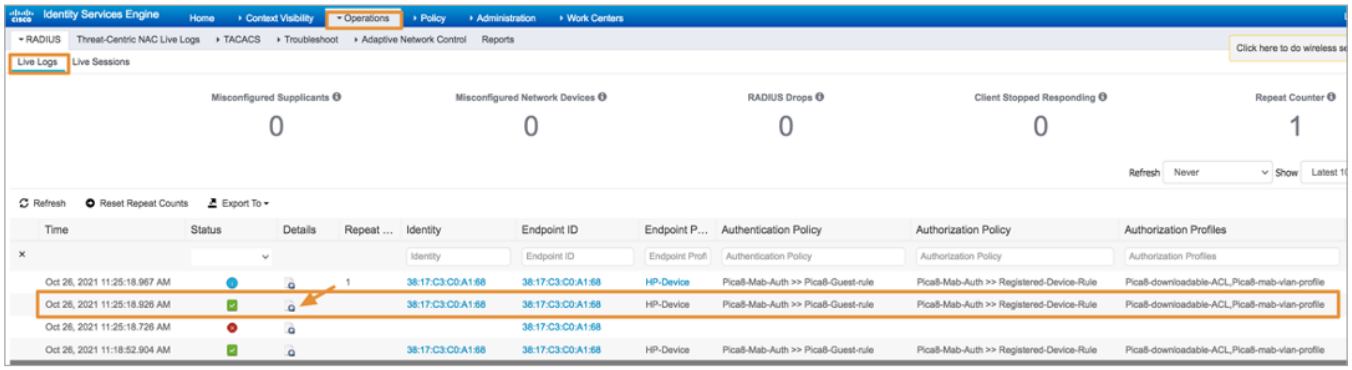


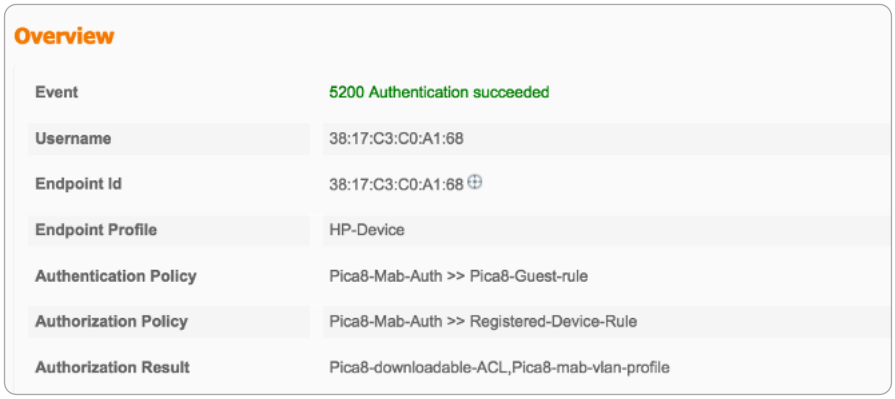
Verifying the NAC Configuration

On the PicOS switch run the following CLI to verify the MAC RADIUS authentication.

```
admin@P8-Access-BR-1-SW-2> show dot1x interface gigabit-ethernet ge-1/1/6
Interface ge-1/1/6:
============================================================
  Client MAC                  : 38:17:c3:c0:a1:68
  Status                      : authorized
  Success Auth Method         : MAB
  Last Success Time           : Tue Oct 26 11:25:34 2021
  Traffic Class               : Other
  Dynamic VLAN ID             : 10 (active)
  Downloadable Filter Name    : mac_auth_policy_3 (active)
  Downloadable Filter Rule    : sequence 1 from destination-address-ipv4 192.168.42.71/32
                                sequence 1 then action forward
                                sequence 2 from destination-address-ipv4 192.168.42.1/32
                                sequence 2 then action forward
                                sequence 3 from destination-address-ipv4 192.168.42.105/32
                                sequence 3 then action forward
                                sequence 4 from destination-address-ipv4 192.168.42.94/32
                                sequence 4 then action forward
                                sequence 5 from destination-address-ipv4 192.168.42.108/32
                                sequence 5 then action forward
                                sequence 6 from destination-address-ipv4 192.168.42.0/24
                                sequence 6 then action discard
                                sequence 7 then action forward
============================================================
```

To view a real-time authentication summary navigate to ***Operations->RADIUS->Live Logs*** and click on the icon under the ***Details*** column as shown below.





Guest Laptop Using Central Web Authentication

In this case, the switch detects that the Mac OS endpoint does not have an 802.1X supplicant. Because MAC RADIUS authentication is also enabled on the interface, the switch then attempts MAC RADIUS authentication for the detected client. We will use Central Web Authentication method for Guest laptops. The guest laptop is connected to port ge-1/1/7.

Logic for Guest laptop with Central Web Authentication is as follows: Guest laptop is not a registered device. Hence it prompts the user to login to the Guest Portal. After user successfully logins to the Guest Portal, dynamic VLAN and ACL are assigned to the port.
This use case involves configuring the PicOS switch, configure the ISE node, and verifying the NAC configuration.

Configuring the PicOS Switch

Configure the Dynamic ACL to be used when a guest laptop connects to a port. This firewall filter, which is configured on the switch, allows the guest to access the entire network except for subnet 192.168.42.0/24.

```
set protocols dot1x filter mac_auth_policy_1 sequence 4 from destination-address-ipv4
192.168.42.170/32
set protocols dot1x filter mac_auth_policy_1 sequence 4 then action “forward”
set protocols dot1x filter mac_auth_policy_1 sequence 5 from destination-address-ipv4
192.168.42.0/24
```

```
set protocols dot1x filter mac_auth_policy_1 sequence 5 then action "discard"
set protocols dot1x filter mac_auth_policy_1 sequence 6 from destination-address-ipv4
192.168.42.105/32
set protocols dot1x filter mac_auth_policy_1 sequence 6 then action "forward"
set protocols dot1x filter mac_auth_policy_1 sequence 999 then action "forward"
```

Configure ***Block VLAN***. Guest user will be put in the Block VLAN until the guest user successfully logs into the Guest Portal. Guest laptop will get an IP address in Block VLAN (192.168.44.0/24) before the user logs into the Guest Portal.

```
set protocols dot1x block-vlan-id 20
set vlans vlan-id 20 vlan-name "vlan20"
set vlans vlan-id 20 l3-interface "vlan20"
set l3-interface vlan-interface vlan20 address 192.168.44.1 prefix-length 24
```

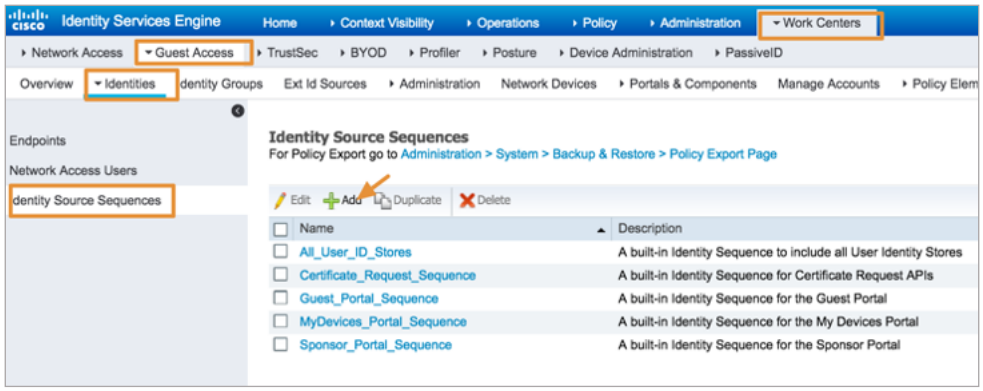
Configuring the ISE Node With a Central Web Authentication Policy

Configuring the Wired Access policy in ISE for guest laptops using Central Web Authentication (CWA) involves following eight steps:

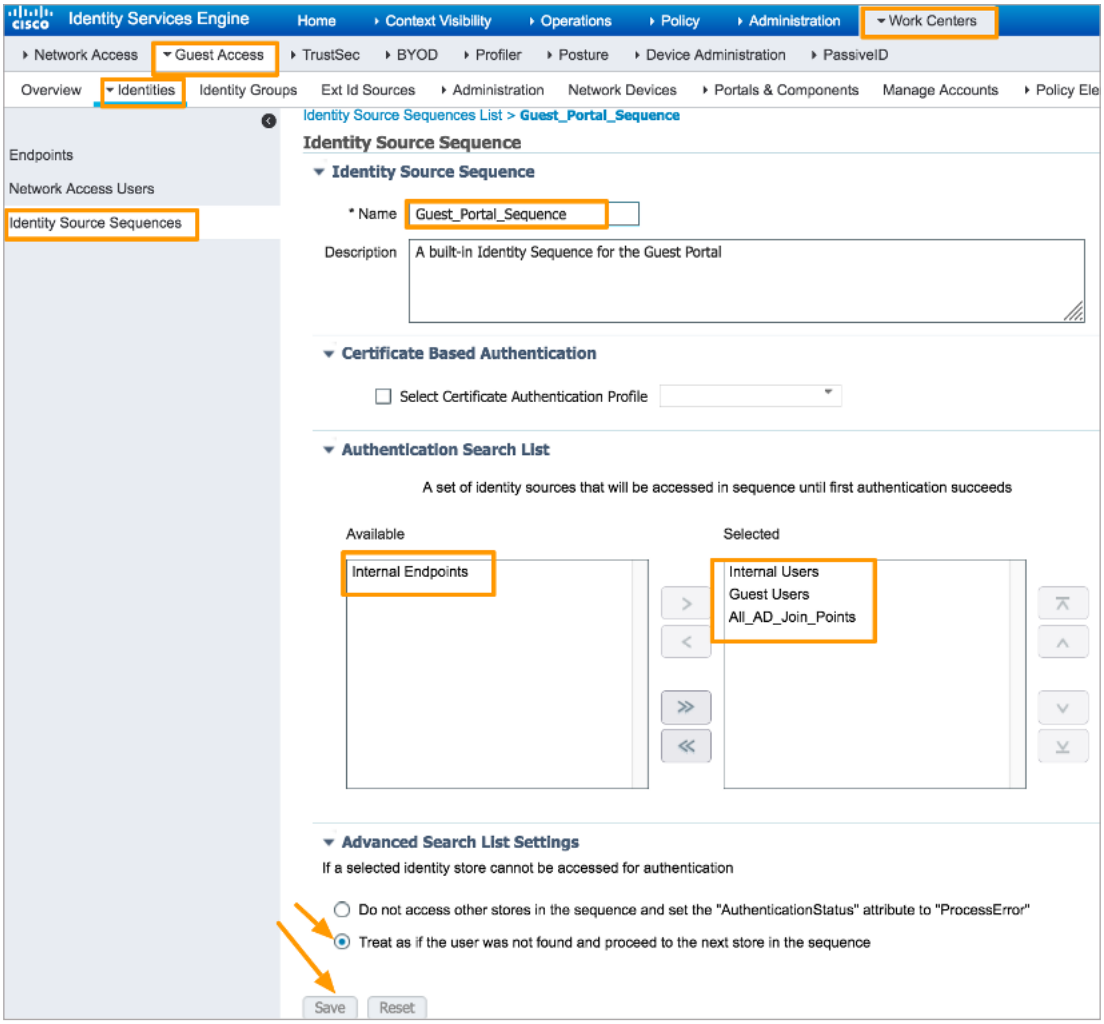
1. Create Identity Sequence for the Guest Portal
2. Create Guest Type
3. Create Self-Registered Guest Portal
4. Add a test user with login credentials in the Guest Portal
5. Create an Authorization Profile to prompt the user to login to the Guest Portal
6. Create an Authorization Profile to dynamically assign VLAN 10 for the guest laptop
7. Create an Authorization Profile to dynamically assign an ACL called mac_auth_policy_1. This firewall filter, which is configured on the switch, allows the guest to access the entire network except for subnet 192.168.42.0/24.
8. Use General Pica8-Mab-Auth policy set for guest laptop that will use the above three authorization profiles

Create Identity Sequence for the Guest Portal

To create the Guest Portal Identity Sequence , navigate to ***Work Centers -> Guest Access -> Identities -> Identity Source Sequence*** and click ***+*** as shown below.

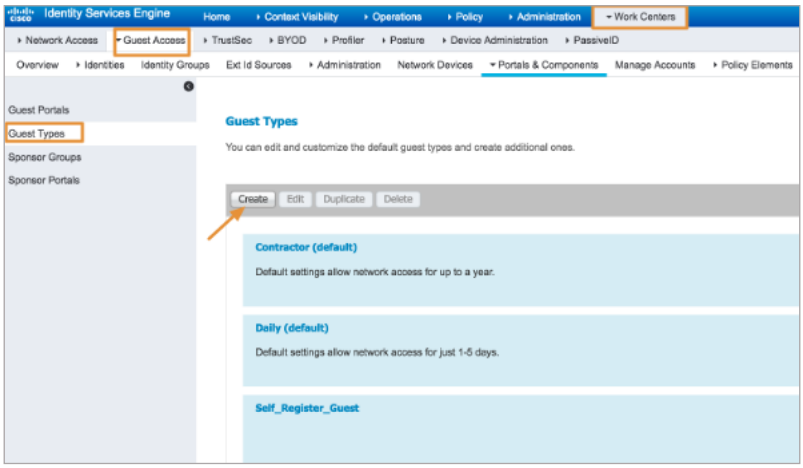


Enter ***Name*** of the sequence as ***Guest_Portal_Sequence*** and select the values for ***Authentication Search List*** as shown below and click ***Save***.



Create Guest Type

To create a new ***Guest Type***, navigate to ***Work Centers -> Guest Access -> Portals & Components-> Guest*** Types and click ***Create*** as shown below.

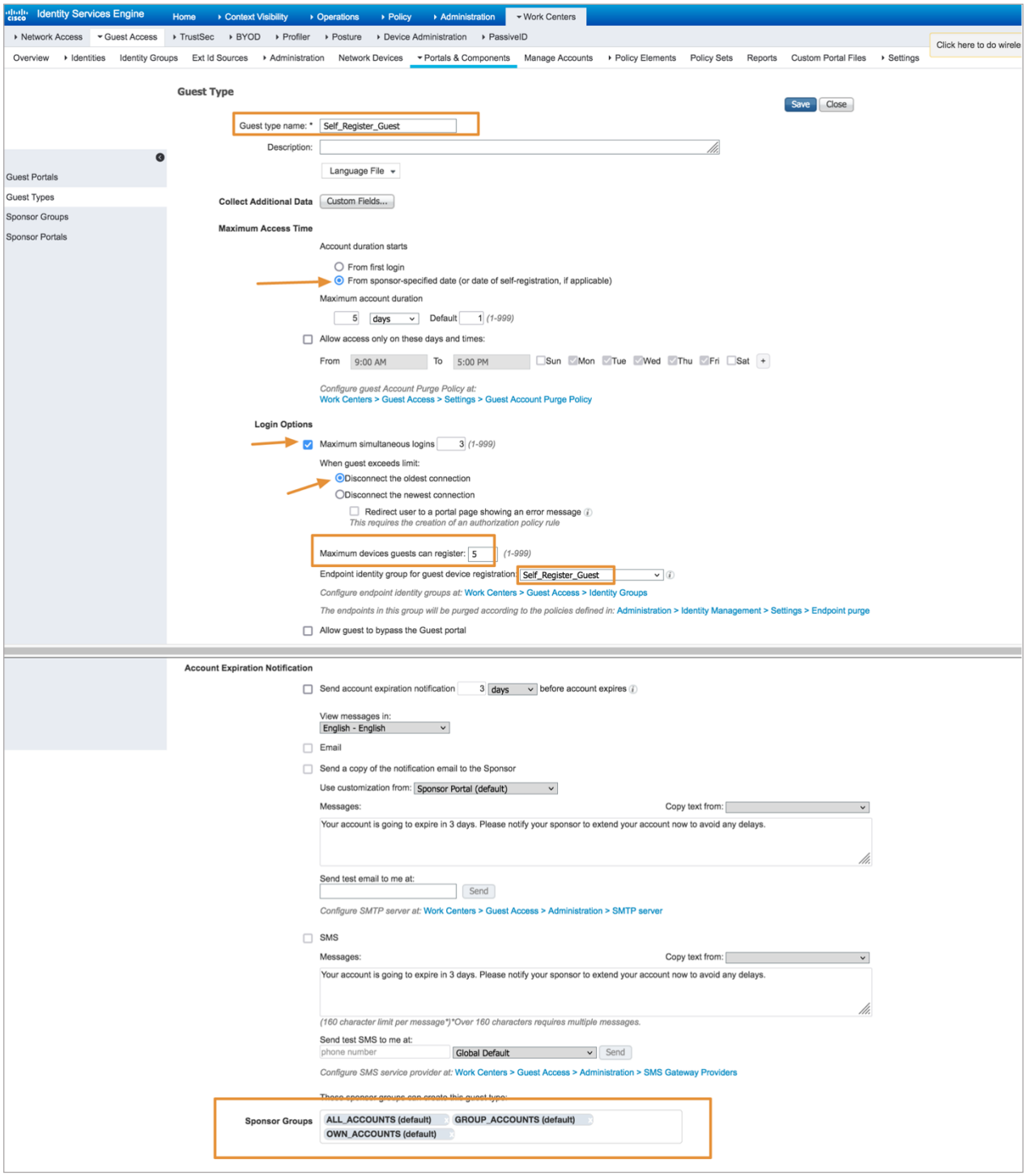


Enter ***Guest Type*** name as ***Self_Register_Guest*** and enter other values shown below including the following:

• Enter ***Self_Register_Guest*** for ***Endpoint identity group for guest device registration field***.

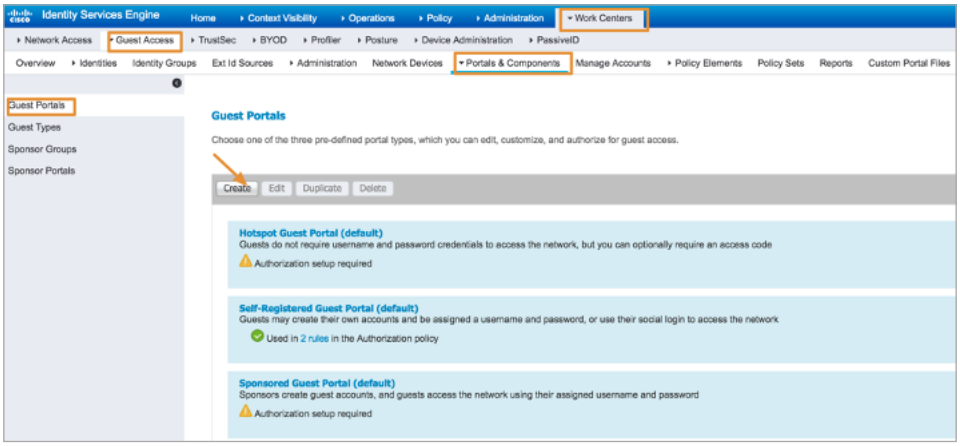
• Enter ***Sponsor Groups*** as shown below

Click ***Save***.

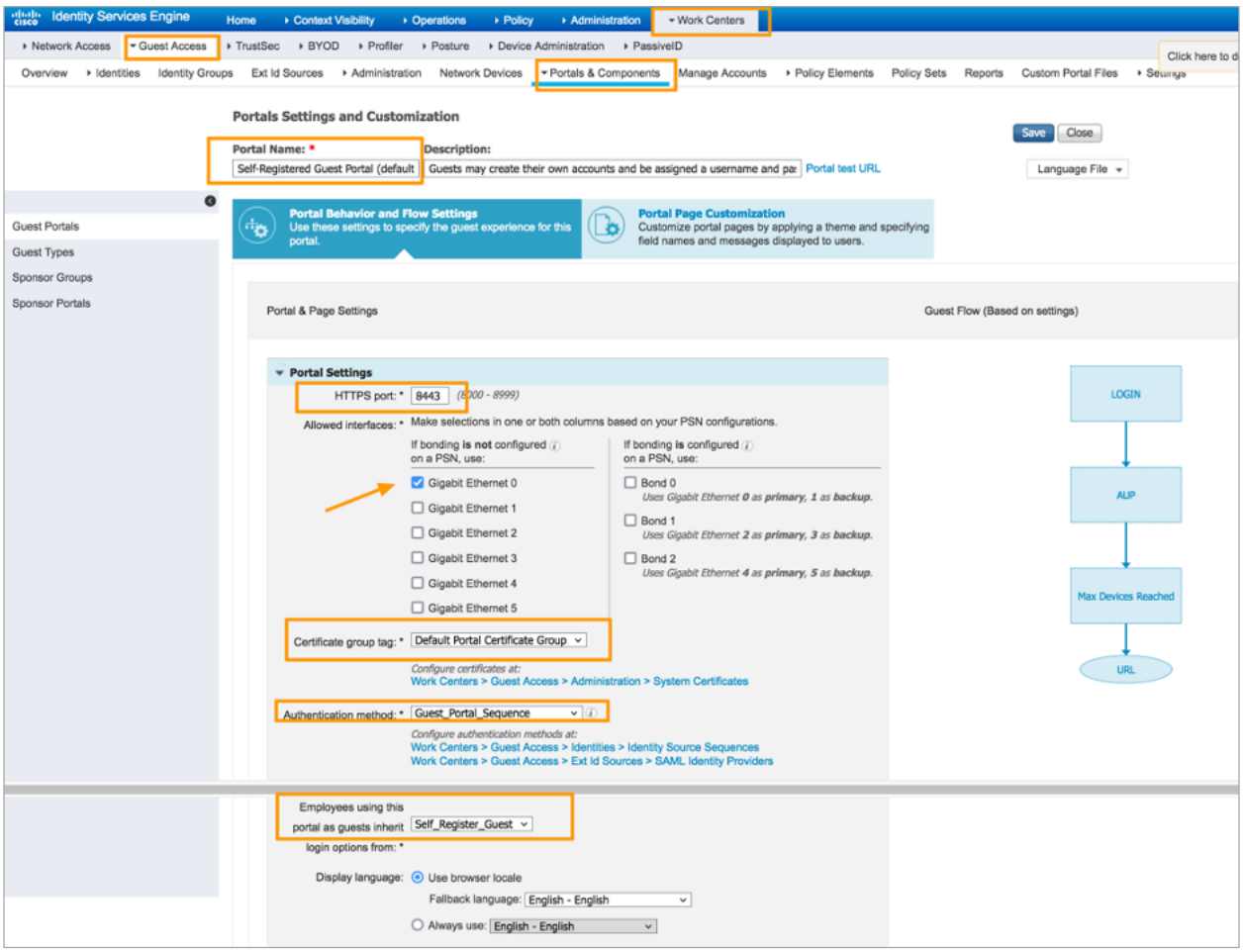


Create Self-Registered Guest Portal

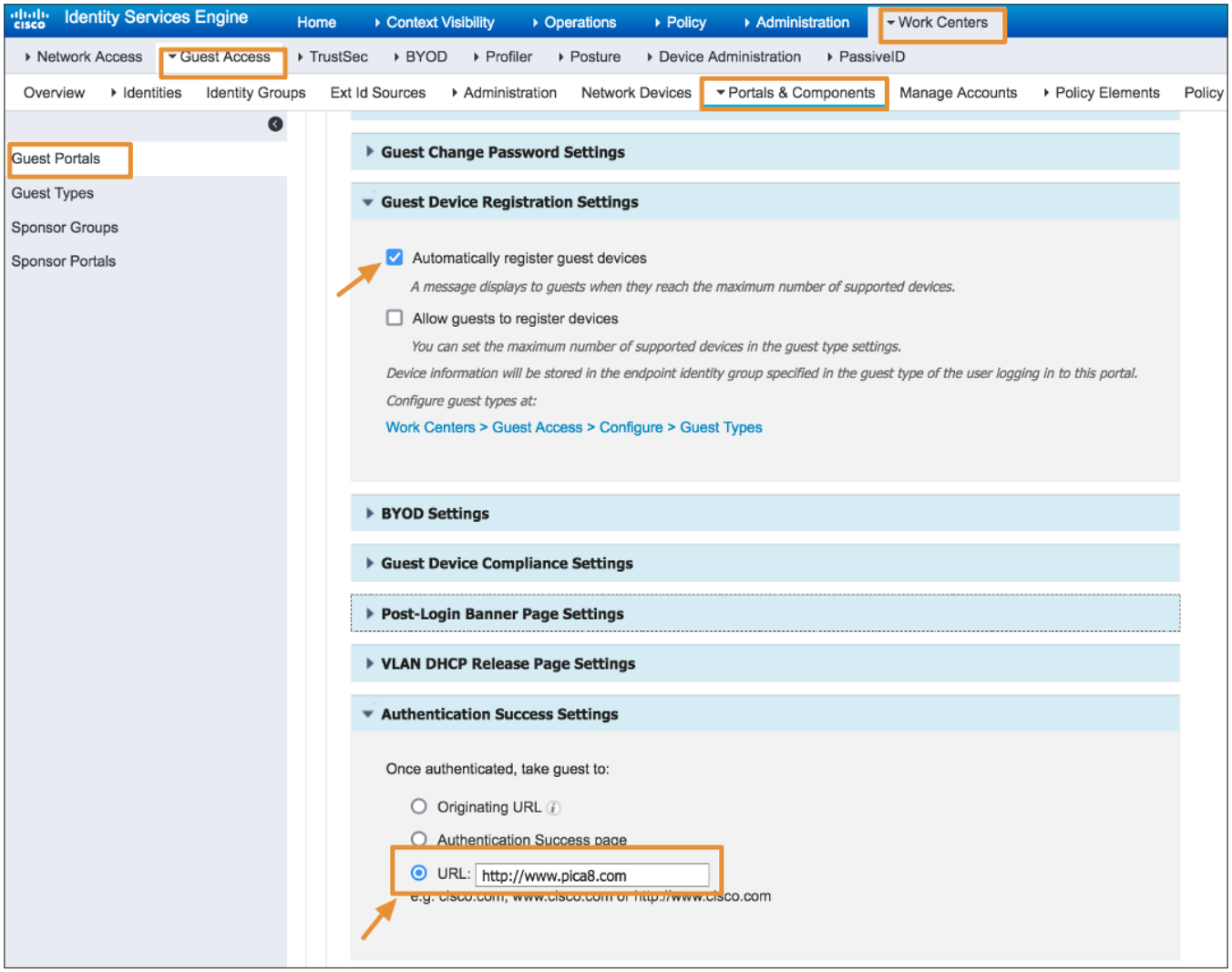
To create the Guest Portal, navigate to ***Work Centers -> Guest Access -> Portals & Components -> Guest Portals*** and click ***Create*** as shown below.



Enter ***Portal Name*** and other parameters as shown below including selecting ***Guest_Portal_Sequence*** as Authentication method.

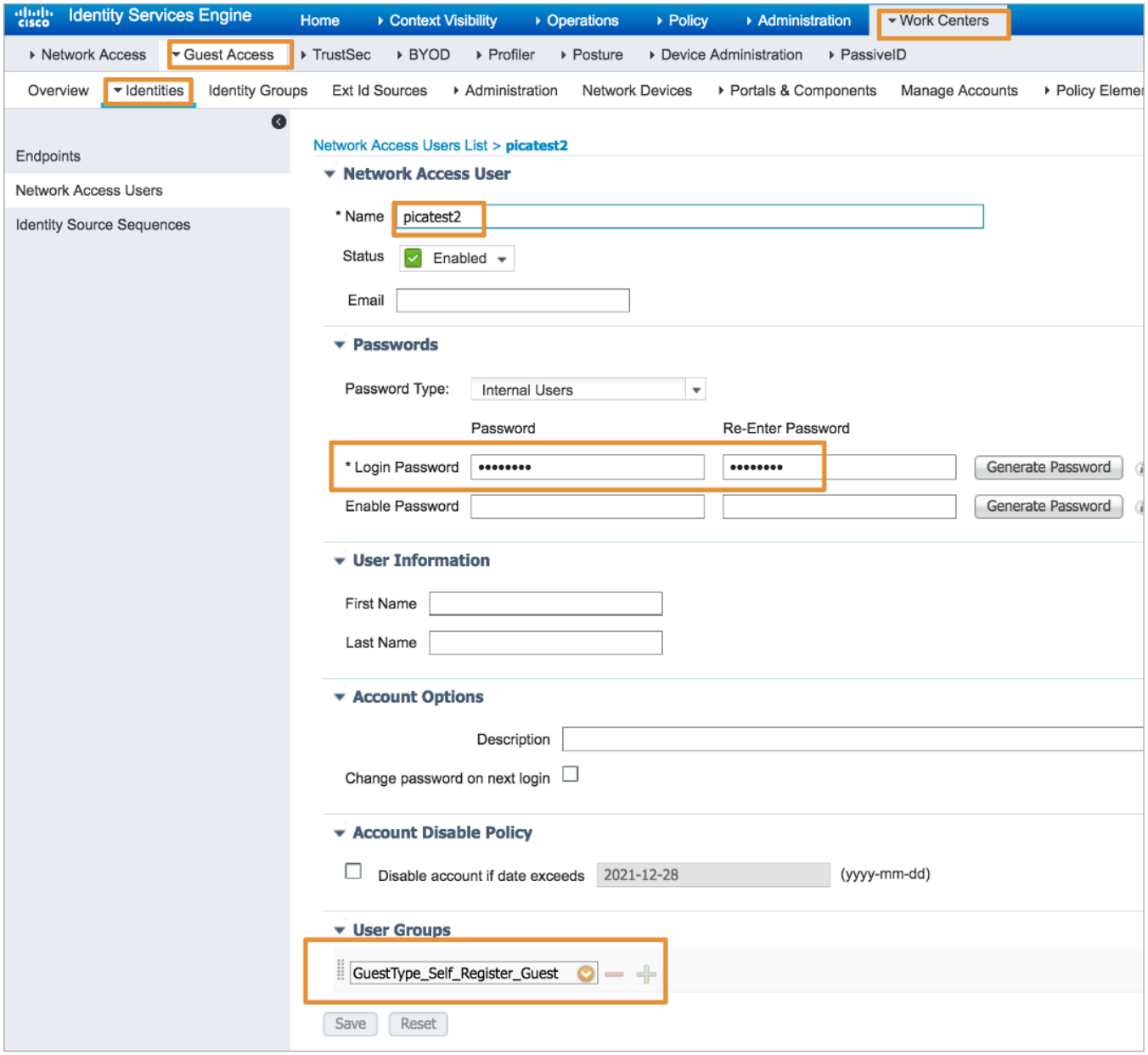


Set ***Guest Device Registration*** Settings as shown below and enter the URL you want to display after successful Guest Portal login as shown below.



Add a Test User With Login Credentials in the Guest Portal

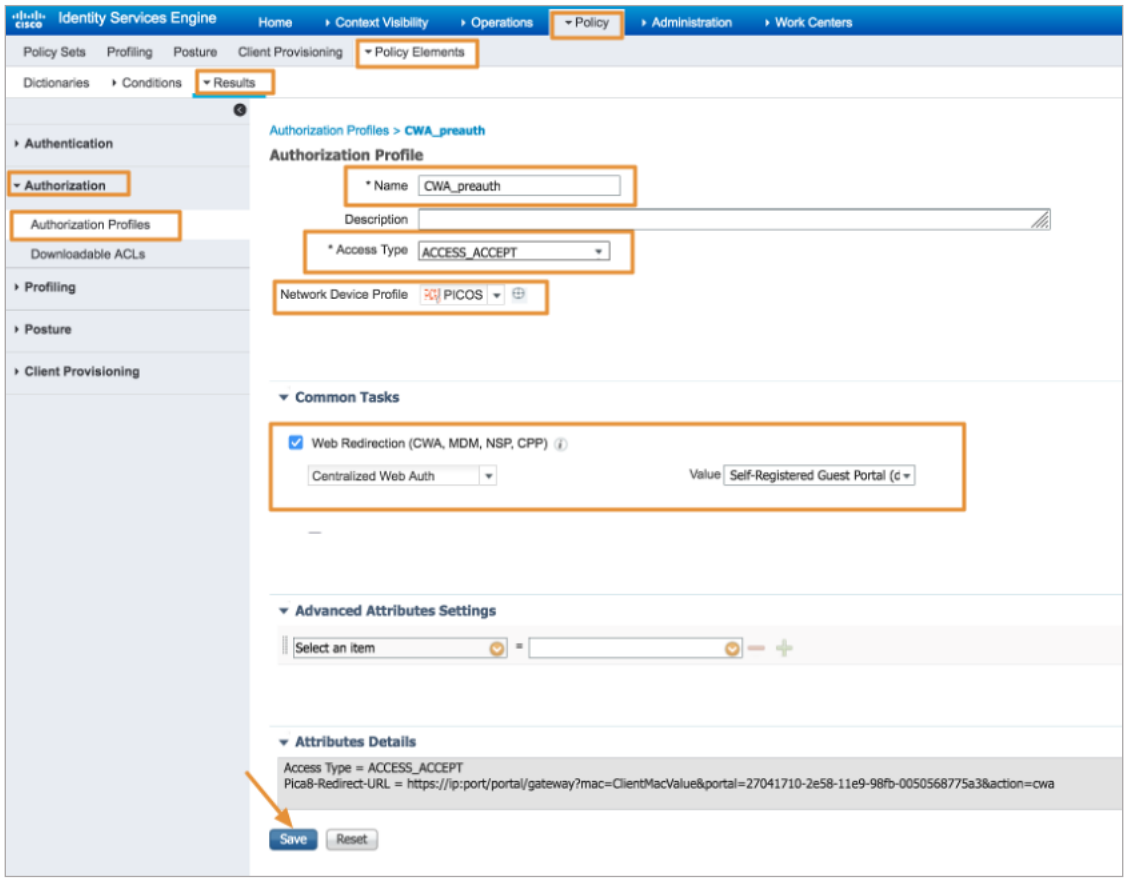
Add a test user picatest2 in the Guest Portal as shown below for GuestType_Resiter_Guest user group.



Create an Authorization Profile to Prompt the User to Login to the Guest Portal

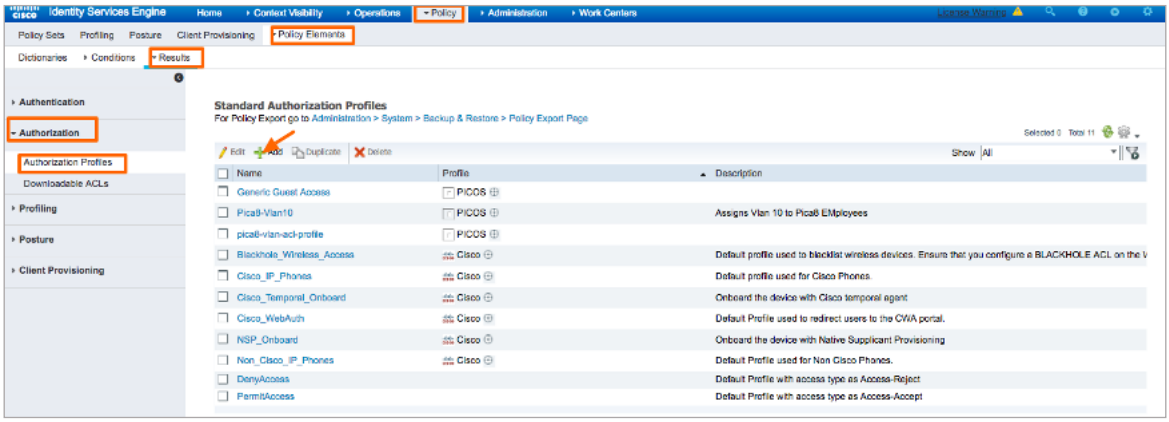
To create the Authorization Profile, navigate to ***Policy -> Policy Elements -> Results -> Authorization -> Authorization Profiles*** and click ***+*** as shown below.

Enter ***Name as CWA_preauth, Description, set Access Type to ACCESS_ACCEPT***, set ***Network Device Profile*** to ***PicOS*** as shown below. Check the box for ***Web Redirection*** and select ***Centralized Web Auth*** with value ***Self-Registered Guest Portal*** as shown below. Then click ***Submit*** or ***Save***.



Creating an Authorization Profile to Dynamically Assign VLAN for Guest Laptops

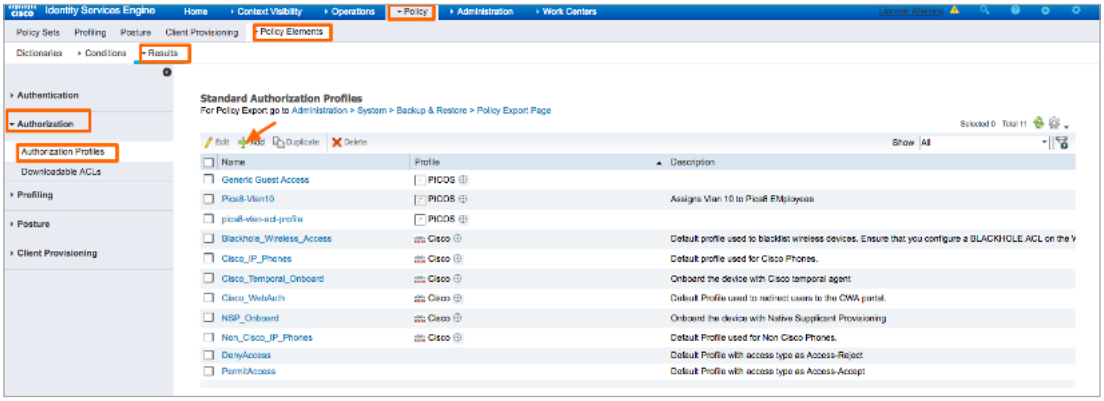
To create a Pica8-guest-VLAN Authorization Profile for guests, navigate to ***Policy -> Policy Elements -> Results -> Authorization -> Authorization Profiles*** and click ***+*** as shown below.



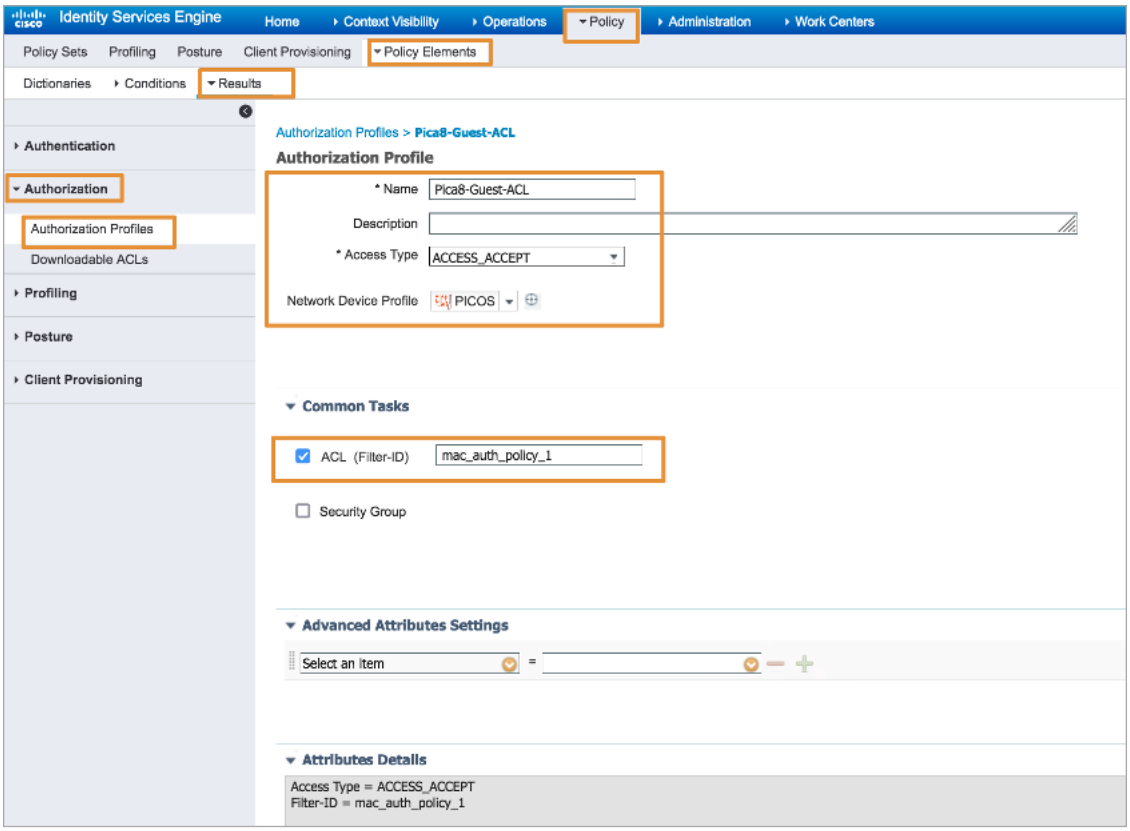
Enter ***Name*** as ***Pica8-guest-VLAN, Description***, set ***Access Type to ACCESS_ACCEPT***, set ***Network Device Profile to PicOS*** as shown below. Check the box for ***VLAN*** and enter ***10*** as value as shown below. Then click ***Submit***.

Creating an Authorization Profile to Dynamically Assign an ACL for Guest Laptops

To create a MAB Authorization Profile for guests navigate to ***Policy -> Policy Elements -> Results -> Authorization -> Authorization Profiles*** and click **+** as shown below.

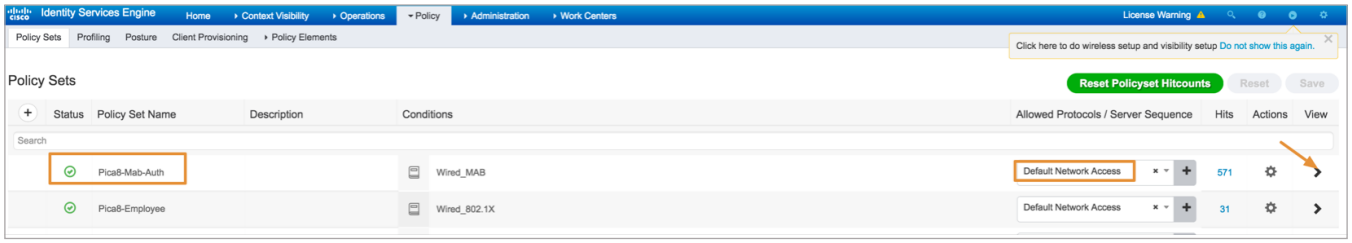


Enter Name as ***Pica8-Guest-ACL, Description***, set ***Access Type to ACCESS_ACCEPT***, and set ***Network Device Profile*** to ***PicOS*** as shown below. Check the box for ***ACL*** and enter ***mac_auth_policy_1*** as value. Click ***Submit***.



Use General Pica8-Mab-Auth Policy Set for Guest Laptop

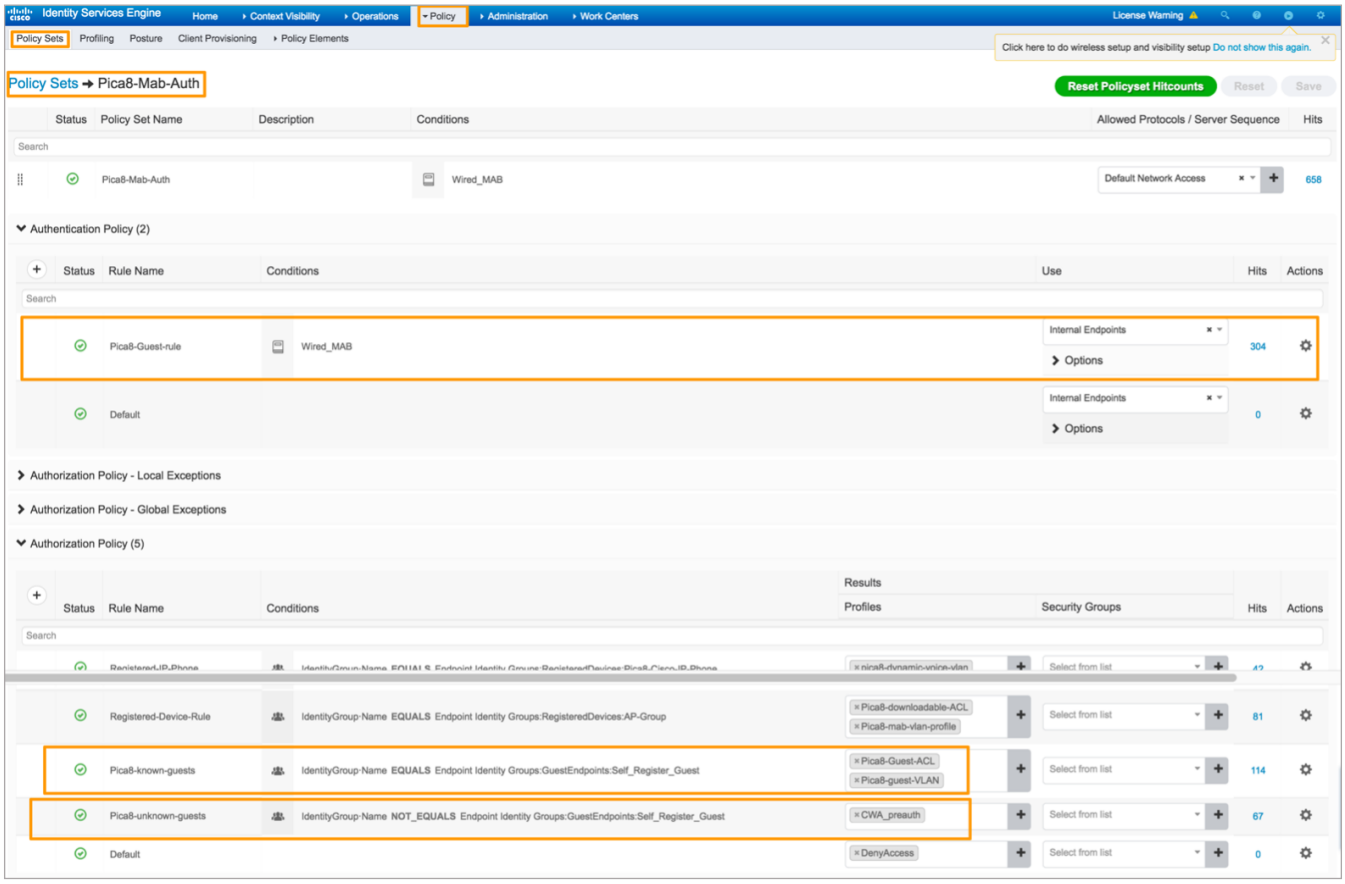
Let us use the previously created Policy Set called Pica8-Mab-Auth to authenticate guests by using Central Web Authentication method. Navigate to ***Policy -> Policy Sets*** and click > on the ***Pica8-Mab_Auth*** policy we have previously created and sign in as shown below.



Add the following policies as shown below:

- Create Pica8-Guest-rule Authentication policy using Wired-MAB and Guest_Portal_Sequence with the options shown below.
- Create Pica8-unknown-guest Authorization policy as shown below to prompt the user to login to the Guest Portal.
- Create Pica8-known-guest Authorization policy as shown to assign VLAN 10 and dynamically assign an ACL called mac_auth_policy_1 for guest laptop after guest logs successfully into the Guest profile.

Click ***Save***.



Verifying the NAC Configuration

Following verification steps are done when guest laptop is connected to port ge-1/1/7.

1. On the PicOS switch run the following CLI to verify the authentication after guest laptop is connected to port ge-1/1/7.

```
admin@P8-Access-BR-1-SW-2> show dot1x interface gigabit-ethernet ge-1/1/7
Interface ge-1/1/5:
=============================================================
Client MAC       : 00:80:8e:8a:92:76
Status           : unauthorized
=============================================================
```

At the beginning you will see guest user laptop is unauthorized.

Then guest user types in https://www.example.com in the Browser running in the laptop.

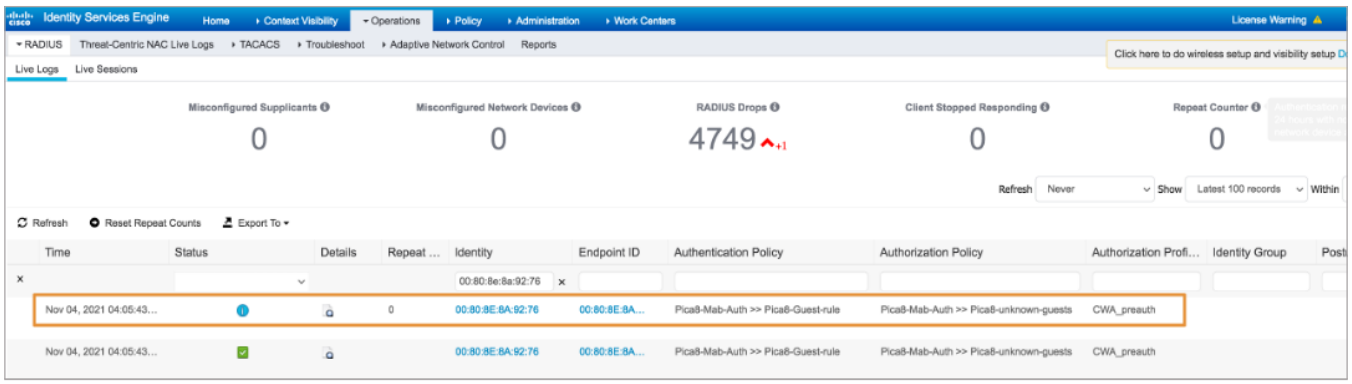
You can see Guest Registration portal URL is presented to the Endpoint Browser. On the PicOS switch run the following CLI to verify.

```
admin@P8-Access-BR-1-SW-2# run show dot1x interface gigabit-ethernet ge-1/1/7
Interface ge-1/1/7:
==============================================================
  Client MAC                : 80:e8:2c:b9:28:db
  Status                    : unauthorized
  Redirect URL              : https://ISE-26-105.pica8.com:8443/portal/gateway?mac=80-E8-2C-B9-28-
DB&portal=27041710-2e58-11e9-98fb-0050568775a3&action=cwa&token=e7c39b1e4145cbbb51638ab53c125b5f
==============================================================
```

During this time Block VLAN 20 is assigned to port ge-1/1/7. You can check using the following command.

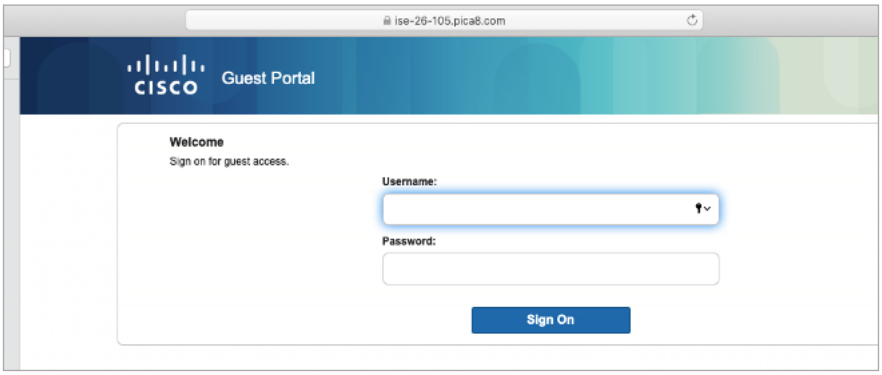
```
admin@P8-Access-BR-1-SW-2# run show vlans
VLANID  VLAN Name            Tag        Interfaces
------  ------------------   --------   -------------------------------------------------------
1       default              untagged   ge-1/1/1, xe-1/1/1, te-1/1/1, xe-1/1/2, te-1/1/2
                                        ge-1/1/2, te-1/1/3, te-1/1/4, ge-1/1/4, ge-1/1/5
                                        ge-1/1/6, ge-1/1/7, ge-1/1/8, ge-1/1/9, ge-1/1/10
                                        ge-1/1/11, ge-1/1/12, ge-1/1/13, ge-1/1/14, ge-1/1/15
                                        ge-1/1/16, ge-1/1/17, ge-1/1/18, ge-1/1/19, ge-1/1/20
                                        ge-1/1/21, ge-1/1/22, ge-1/1/23, ge-1/1/24, ge-1/1/25
                                        ge-1/1/26, ge-1/1/27, ge-1/1/28, ge-1/1/29, ge-1/1/30
                                        ge-1/1/31, ge-1/1/32, ge-1/1/33, ge-1/1/34, ge-1/1/35
                                        ge-1/1/36, ge-1/1/37, ge-1/1/38, ge-1/1/39, ge-1/1/40
                                        ge-1/1/41, ge-1/1/42, ge-1/1/43, ge-1/1/44, ge-1/1/45
                                        ge-1/1/46, ge-1/1/47, ge-1/1/48
                             tagged

10      default              untagged   ge-1/1/3, ge-1/1/6
                             tagged

20      VLAN20               untagged   ge-1/1/5, ge-1/1/6, ge-1/1/7, ge-1/1/8, ge-1/1/9
                                        ge-1/1/10, ge-1/1/11, ge-1/1/12, ge-1/1/13, ge-1/1/14
                                        ge-1/1/15, ge-1/1/16, ge-1/1/17, ge-1/1/18, ge-1/1/19
                                        ge-1/1/20, ge-1/1/21, ge-1/1/22, ge-1/1/23, ge-1/1/24
                                        ge-1/1/25, ge-1/1/26, ge-1/1/27, ge-1/1/28, ge-1/1/29
                                        ge-1/1/30, ge-1/1/31, ge-1/1/32, ge-1/1/33, ge-1/1/34
                                        ge-1/1/35, ge-1/1/36, ge-1/1/37, ge-1/1/38, ge-1/1/39
                                        ge-1/1/40, ge-1/1/41, ge-1/1/42, ge-1/1/43, ge-1/1/44
                                        ge-1/1/45, ge-1/1/46, ge-1/1/47, ge-1/1/48
                             tagged

40      VLAN40               untagged
                             tagged

800     default              untagged
                             Tagged
```

On ISE navigate to ***Operations->RADIUS->Live Logs*** and click on the icon under the ***Details*** column as shown below. You can see ***Pica8-unknown-guests*** authorization policy is triggered. This rule is used for authenticating the guest user whose laptop will not have 802.1x supplicant.



Clicking the icon under the Details column opens the ***Authentication Detail Report*** in a new browser window. This report offers information about authentication status and related attributes, and authentication flow.

On the endpoint, Guest is redirected to the Guest Registration portal as shown below. Guest enters the credentials to login to the Guest Portal.

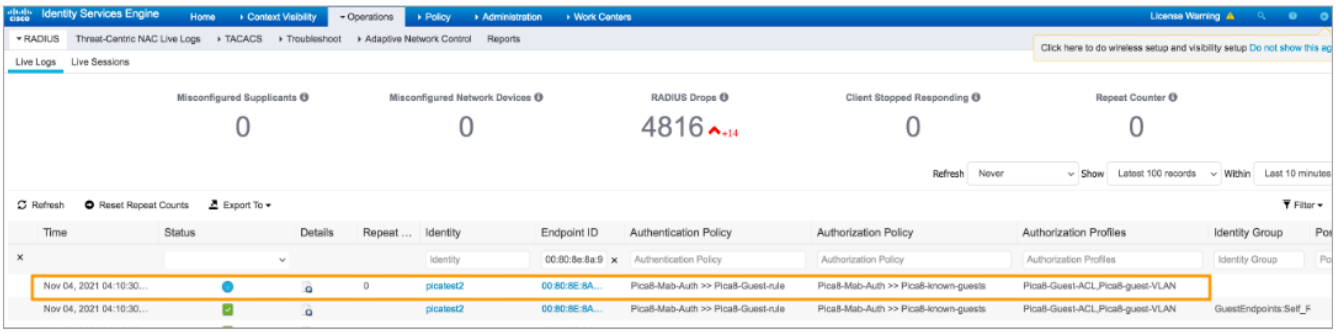


After Guest is successfully authorized, run the following CLI on the switch to verify. Here you can see VLAN 10 and ***mac_auth_policy_1 ACL*** are dynamically assigned to ***ge-1/1/7 port***.

```
admin@P8-Access-BR-1-SW-2> show dot1x interface gigabit-ethernet ge-1/1/7
Interface ge-1/1/5:
============================================================
  Client MAC                : 00:80:8e:8a:92:76
  Status                    : authorized
  Success Auth Method       : MAB
  Last Success Time         : Thu Nov  4 16:10:30 2021
  Traffic Class             : Other
  Dynamic VLAN ID           : 10 (active)
  Dynamic Filter Name       : mac_auth_policy_1 (active)
============================================================
```

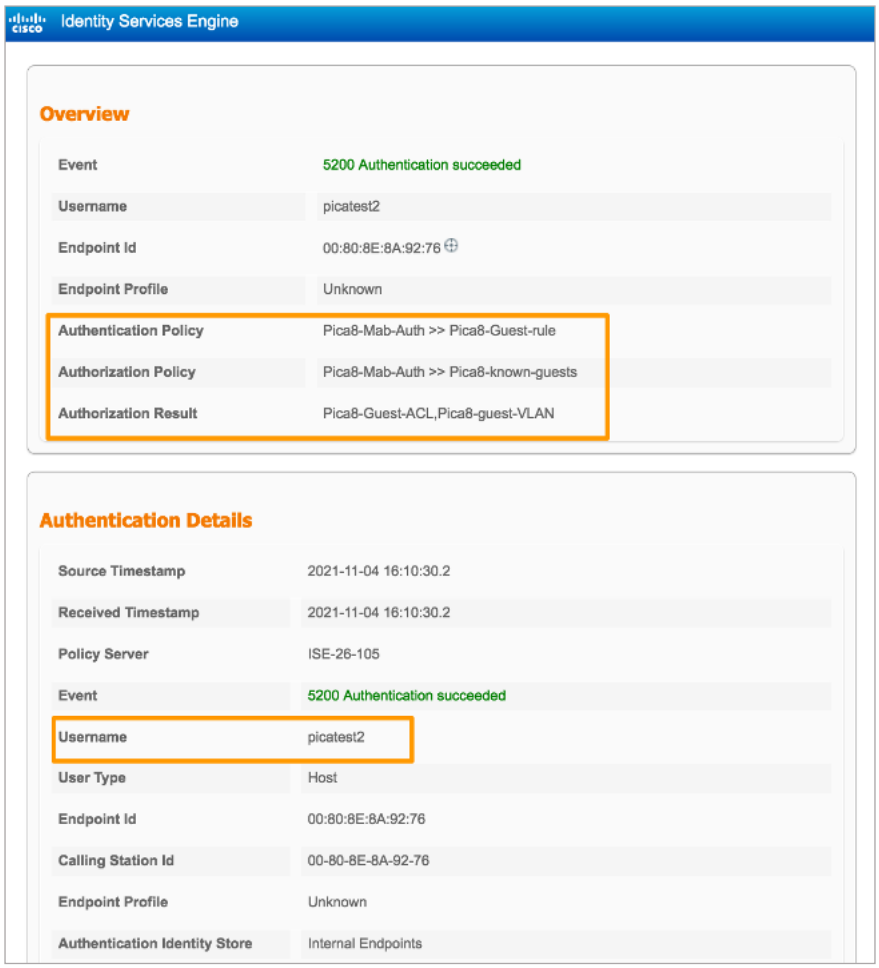
Based on the ***Authentication Success Settings*** in the ***Self-Registered Guest Portal***, guest's laptop browser displays https://www.pica8.com/ page. After this guest will be able to access the Internet.

To verify on ISE, navigate to ***Operations->RADIUS->Live Logs*** and click on the icon under the ***Details*** column as shown below.



You can see ***Pica8-known-guests*** Authorization policy was triggered after Guest successfully logged into the Guest Portal.

Clicking the icon under the Details column opens the ***Authentication Detail Report*** in a new browser window. This report offers information about authentication status and related attributes, and authentication flow. You can see ***Pica8-guest-VLAN*** and ***Pica8-Guest-ACL*** (Dynamic ACL) are assigned to the port where guest laptop is connected.



Now guest laptop has network access to access the Internet. From the Guest Mac laptop browser make sure you are able to reach www.example.com.

Troubleshooting

This section lists recommended commands for troubleshooting the NAC feature.

Check Whether the ISE Server is Reachable from the PicOS Switch

Verify reachability between ClearPass server and PicOS switch by using the following CLI command:

```
admin@P8-Access-BR-1-SW-2# run show dot1x server
Server-IP        Status       Priority  Retry-Interval  Retry-Num  Detect-Interval  Consecutive-Detect-Num
---------------  -----------  --------  --------------  ---------  ---------------  ----------------------
192.168.42.105   active       ...       1   Sec(s)      3          5   Sec(s)       3
```

Check the NAC Authentication Status of all Ports

Check NAC authentication status for all ports using the following command.

```
admin@P8-Access-BR-1-SW-2> show dot1x interface
Interface 802.1x  MAC-RADIUS  WEB     HOST-MODE  CLIENT-MAC        CLIENT-STATUS
--------------------------------------------------------------------------------

<output suppressed>
ge-1/1/5  enable  enable      enable  multiple   00:c1:b1:e5:0a:f6 authorized
                                                 80:e8:2c:b9:28:db authorized
ge-1/1/6  enable  enable      enable  multiple   38:17:c3:c0:a1:68 authorized
ge-1/1/7  enable  enable      enable  multiple
ge-1/1/8  enable  enable      enable  multiple
ge-1/1/9  enable  enable      enable  multiple
```

Check the NAC Configuration

To list NAC configuration use the following command.

```
admin@P8-Access-BR-1-SW-2# show all protocols dot1x | display set
    <output suppressed>
set protocols dot1x interface ge-1/1/5 host-mode "multiple"
set protocols dot1x interface ge-1/1/5 auth-mode 802.1x
set protocols dot1x interface ge-1/1/5 auth-mode mac-radius
set protocols dot1x interface ge-1/1/5 auth-mode web
set protocols dot1x interface ge-1/1/5 recovery-timeout 3600
set protocols dot1x interface ge-1/1/5 session-timeout 3600
set protocols dot1x interface ge-1/1/6 host-mode "multiple"
set protocols dot1x interface ge-1/1/6 auth-mode 802.1x
set protocols dot1x interface ge-1/1/6 auth-mode mac-radius
set protocols dot1x interface ge-1/1/6 auth-mode web
set protocols dot1x interface ge-1/1/6 recovery-timeout 3600
set protocols dot1x interface ge-1/1/6 session-timeout 3600
set protocols dot1x interface ge-1/1/7 host-mode "multiple"
set protocols dot1x interface ge-1/1/7 auth-mode 802.1x
set protocols dot1x interface ge-1/1/7 auth-mode mac-radius
set protocols dot1x interface ge-1/1/7 auth-mode web
set protocols dot1x interface ge-1/1/7 recovery-timeout 3600
set protocols dot1x interface ge-1/1/7 session-timeout 3600
set protocols dot1x interface ge-1/1/8 host-mode "multiple"
set protocols dot1x session-timeout 36000
set protocols dot1x block-vlan-id 20
set protocols dot1x aaa radius authentication server-ip 192.168.42.105 shared-key
"cGljYThwaWNhOA=="
set protocols dot1x aaa radius authentication server-ip 192.168.42.105 retry-interval 1
set protocols dot1x aaa radius authentication server-ip 192.168.42.105 retry-num 3
set protocols dot1x aaa radius authentication server-ip 192.168.42.105 detect-interval 5
set protocols dot1x aaa radius authentication server-ip 192.168.42.105 consecutive-detect-num 3
set protocols dot1x aaa radius dynamic-author client 192.168.42.105 shared-key "cGljYThwaWNhOA=="
set protocols dot1x aaa radius nas-ip 192.168.42.170
set protocols dot1x filter mac_auth_policy_1 description ""
set protocols dot1x filter mac_auth_policy_1 sequence 4 description ""
```

```
set protocols dot1x filter mac_auth_policy_1 sequence 4 from destination-address-ipv4
192.168.42.170/32
set protocols dot1x filter mac_auth_policy_1 sequence 4 then action “forward”
set protocols dot1x filter mac_auth_policy_1 sequence 5 description “”
set protocols dot1x filter mac_auth_policy_1 sequence 5 from destination-address-ipv4
192.168.42.0/24
set protocols dot1x filter mac_auth_policy_1 sequence 5 then action “discard”
set protocols dot1x filter mac_auth_policy_1 sequence 6 description “”
set protocols dot1x filter mac_auth_policy_1 sequence 6 from destination-address-ipv4
192.168.42.105/32
set protocols dot1x filter mac_auth_policy_1 sequence 6 then action “forward”
set protocols dot1x filter mac_auth_policy_1 sequence 999 description “”
set protocols dot1x filter mac_auth_policy_1 sequence 999 then action “forward”
set protocols dot1x filter mac_auth_policy_2 description “”
set protocols dot1x filter mac_auth_policy_2 sequence 999 description “”
set protocols dot1x filter mac_auth_policy_2 sequence 999 then action “forward”
set protocols dot1x traceoptions flag configuration disable false
```

Check VLANs to Verify Dynamic VLANs Assignment to a Port

Check VLANs dynamically assigned for access ports using the following command.

```
admin@P8-Access-BR-1-SW-2# run show vlans
VLANID  VLAN Name            Tag        Interfaces
------  ------------------   --------   -------------------------------------------------------
1       default              untagged   ge-1/1/1, xe-1/1/1, te-1/1/1, xe-1/1/2, te-1/1/2
                                        ge-1/1/2, te-1/1/3, te-1/1/4, ge-1/1/4, ge-1/1/5
                                        ge-1/1/6, ge-1/1/7, ge-1/1/8, ge-1/1/9, ge-1/1/10
                                        ge-1/1/11, ge-1/1/12, ge-1/1/13, ge-1/1/14, ge-1/1/15
                                        ge-1/1/16, ge-1/1/17, ge-1/1/18, ge-1/1/19, ge-1/1/20
                                        ge-1/1/21, ge-1/1/22, ge-1/1/23, ge-1/1/24, ge-1/1/25
                                        ge-1/1/26, ge-1/1/27, ge-1/1/28, ge-1/1/29, ge-1/1/30
                                        ge-1/1/31, ge-1/1/32, ge-1/1/33, ge-1/1/34, ge-1/1/35
                                        ge-1/1/36, ge-1/1/37, ge-1/1/38, ge-1/1/39, ge-1/1/40
                                        ge-1/1/41, ge-1/1/42, ge-1/1/43, ge-1/1/44, ge-1/1/45
                                        ge-1/1/46, ge-1/1/47, ge-1/1/48
                             tagged

10      default              untagged   ge-1/1/3, ge-1/1/5, ge-1/1/6
                             tagged

20      VLAN20               untagged   ge-1/1/5, ge-1/1/6, ge-1/1/7, ge-1/1/8, ge-1/1/9
                                        ge-1/1/10, ge-1/1/11, ge-1/1/12, ge-1/1/13, ge-1/1/14
                                        ge-1/1/15, ge-1/1/16, ge-1/1/17, ge-1/1/18, ge-1/1/19
                                        ge-1/1/20, ge-1/1/21, ge-1/1/22, ge-1/1/23, ge-1/1/24
                                        ge-1/1/25, ge-1/1/26, ge-1/1/27, ge-1/1/28, ge-1/1/29
                                        ge-1/1/30, ge-1/1/31, ge-1/1/32, ge-1/1/33, ge-1/1/34
                                        ge-1/1/35, ge-1/1/36, ge-1/1/37, ge-1/1/38, ge-1/1/39
                                        ge-1/1/40, ge-1/1/41, ge-1/1/42, ge-1/1/43, ge-1/1/44
                                        ge-1/1/45, ge-1/1/46, ge-1/1/47, ge-1/1/48
                             tagged
```

```
40      VLAN40              untagged
                            tagged

800     default             untagged
                            tagged      ge-1/1/5
```

Check Dynamic ACL Rules

Check dynamic ACL rules and counters using the following command.

```
admin@P8-Access-BR-1-SW-2> show dot1x dynamic filter
==========================================================================
Filter: mac_auth_policy_1
    Description     :
    --------------------------------------------------------------------
    Sequence        : 4
    Description     :
    Match counter   : 0 packets
    Match Condition : Destination IPv4Net  : 192.168.42.170/32
    Action          : Forward
    --------------------------------------------------------------------
    Sequence        : 5
    Description     :
    Match counter   : 0 packets
    Match Condition : Destination IPv4Net  : 192.168.42.0/24
    Action          : Discard
    --------------------------------------------------------------------
    Sequence        : 6
    Description     :
    Match counter   : 0 packets
    Match Condition : Destination IPv4Net  : 192.168.42.105/32
    Action          : Forward
    --------------------------------------------------------------------
    Sequence        : 999
    Description     :
    Match counter   : 0 packets
    Match Condition :
    Action          : Forward
==========================================================================
Filter: mac_auth_policy_2
    Description     :
    --------------------------------------------------------------------
    Sequence        : 999
    Description     :
    Match counter   : 184547 packets
    Match Condition :
    Action          : Forward
    --------------------------------------------------------------------
    Applied Clients : ge-1/1/5     80:e8:2c:b9:28:db
```

Check Downloadable ACL Rules

Check downloadable ACL rules and counters using the following command.

```
admin@P8-Access-BR-1-SW-2> show dot1x downloadable filter
-----------------------------------------------------------
Downloadable Filter Name : mac_auth_policy_3
Applied Interface        : ge-1/1/6
Applied Client MAC       : 38:17:c3:c0:a1:68
Downloadable Filter Rule : sequence 1 from destination-address-ipv4 192.168.42.71/32
                           sequence 1 then action forward
                           sequence 2 from destination-address-ipv4 192.168.42.1/32
                           sequence 2 then action forward
                           sequence 3 from destination-address-ipv4 192.168.42.105/32
                           sequence 3 then action forward
                           sequence 4 from destination-address-ipv4 192.168.42.94/32
                           sequence 4 then action forward
                           sequence 5 from destination-address-ipv4 192.168.42.108/32
                           sequence 5 then action forward
                           sequence 6 from destination-address-ipv4 192.168.42.0/24
                           sequence 6 then action discard
                           sequence 7 then action forward
Downloadable Rule Counter: sequence 1          match counter: 1 packets
                           sequence 2          match counter: 0 packets
                           sequence 3          match counter: 0 packets
                           sequence 4          match counter: 0 packets
                           sequence 5          match counter: 0 packets
                           sequence 6          match counter: 0 packets
                           sequence 7          match counter: 903 packets
```

Check Trace Logs for Radius

First enable Trace Logs for RADIUS module using the following command:
set protocols dot1x traceoptions flag all disable false

Check the Trace Logs for Radius by using the following PicOS command:

```
admin@P8-Access-BR-1-SW-2# run show log last-rows 100 | match DOT1x
Oct 26 2021 15:38:04 P8-Access-BR-1-SW-2  local0.debug : [dot1x]
Dmac:80:e8:2c:b9:28:db,Smac:18:5a:58:1d:9c:21
Oct 26 2021 15:38:04 P8-Access-BR-1-SW-2  local0.debug : [dot1x]Dmac:01:80:c2:00:00:03,Smac:80:e8:
2c:b9:28:db
Oct 26 2021 15:38:04 P8-Access-BR-1-SW-2  local0.debug : [dot1x]
Dmac:80:e8:2c:b9:28:db,Smac:18:5a:58:1d:9c:21
Oct 26 2021 15:38:04 P8-Access-BR-1-SW-2  local0.debug : [dot1x]send_add_smac_VLAN_port_filter,
mac:80:e8:2c:b9:28:db
Oct 26 2021 15:38:04 P8-Access-BR-1-SW-2  local0.debug : [dot1x]Add dynamic filter
rule,ifname:ge-1/1/5 mac 80:e8:2c:b9:28:db
Oct 26 2021 15:38:04 P8-Access-BR-1-SW-2  local0.debug : [dot1x]send add filter,
mac:80:e8:2c:b9:28:db
Oct 26 2021 15:38:04 P8-Access-BR-1-SW-2  local0.debug : [dot1x]rule action accept
```

```
Oct 26 2021 15:38:04 P8-Access-BR-1-SW-2  local0.debug : [dot1x]rule flag 1, priority 31769
Oct 26 2021 15:38:04 P8-Access-BR-1-SW-2  local0.debug : [dot1x]send add filter,
mac:80:e8:2c:b9:28:db
Oct 26 2021 15:38:04 P8-Access-BR-1-SW-2  local0.debug : [dot1x]Get transaction id 61377169
Oct 26 2021 15:38:04 P8-Access-BR-1-SW-2  local0.debug : [dot1x]Set hw port to dynamic VLAN
cb,ifname:ge-1/1/5 VLAN:10 tid:61377169
Oct 26 2021 15:38:04 P8-Access-BR-1-SW-2  local0.debug : [dot1x]Free transaction id 61377169
Oct 26 2021 15:38:04 P8-Access-BR-1-SW-2  local0.debug : [dot1x]Mac 80:e8:2c:b9:28:db,VLAN 10,type
dynamic, learn event
Oct 26 2021 15:38:20 P8-Access-BR-1-SW-2  local0.debug : [dot1x]Dmac:00:c1:b1:e5:0a:f6,Smac:18:5a:
58:1d:9c:21
Oct 26 2021 15:39:00 P8-Access-BR-1-SW-2  local0.debug : [dot1x]Get transaction id 62186051
Oct 26 2021 15:39:00 P8-Access-BR-1-SW-2  local0.debug : [dot1x]Free transaction id 62186051
Oct 26 2021 15:46:49 P8-Access-BR-1-SW-2  local0.debug : [dot1x]Mac 00:c1:b1:e5:0a:f6,VLAN 1,type
dynamic, age event
Oct 26 2021 15:46:49 P8-Access-BR-1-SW-2  local0.debug : [dot1x]Mac 80:e8:2c:b9:28:db,VLAN 1,type
dynamic, age event
Oct 26 2021 15:58:24 P8-Access-BR-1-SW-2  local0.debug : [dot1x]Mac 38:17:c3:c0:a1:68,VLAN 1,type
dynamic, learn event
```

Reference

PicOS

The following are reference materials related to PicOS:

- PicOS version 4.1.3 NAC Configuration Guide
- Configuring Dynamic and Downloadable ACLs for Cisco ISE
- Abbreviated downloadable ACLs

ISE

The following are reference materials related to Cisco ISE:

- Cisco ISE Installation Guide Release 2.6
- ISE 2.6 Admin Guide
- Cisco Identity Services Engine Ordering Guide

Copyright ©2022 Pica8 Software Inc. All Rights Reserved.