



---

Pica8 Deployment Guide

---

# **PicOS<sup>®</sup> NAC Integration with Cisco Identity Services Engine (ISE) Node**

---

# Contents

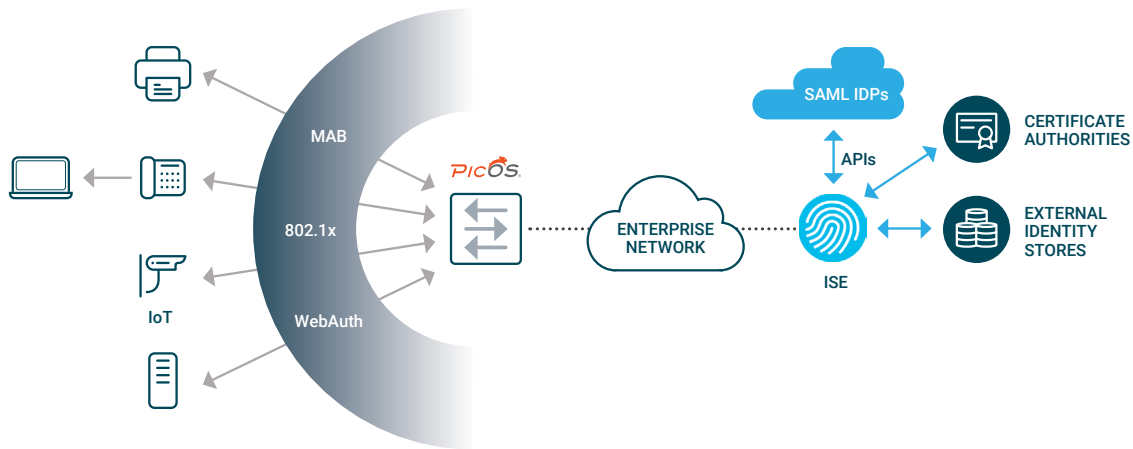
---

## Contents

<b>Cisco Identity Services Engine (ISE) Solution</b>	<b>1</b>
<b>PicOS Network Access Control – Secured Wired Access Solution</b>	<b>1</b>
<b>Deploying an ISE Node</b>	<b>1</b>
Requirements	2
Use Case Overview and Topology	2
<b>Integrating PicOS with Cisco ISE for Radius Authentication</b>	<b>4</b>
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
<b>Configuring an Employee Laptop with 802.1x Supplicant</b>	<b>11</b>
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
<b>IP Phone Authentication</b>	<b>18</b>
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
<b>Access Point Authentication</b>	<b>24</b>
Verifying the NAC Configuration	27
<b>Guest Laptop Using Central Web Authentication</b>	<b>28</b>
Configuring the PicOS Switch	28
Configuring the ISE Node With a Central Web Authentication Policy	29
Verifying the NAC Configuration	38
<b>Troubleshooting</b>	<b>42</b>
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
<b>Reference</b>	<b>47</b>
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

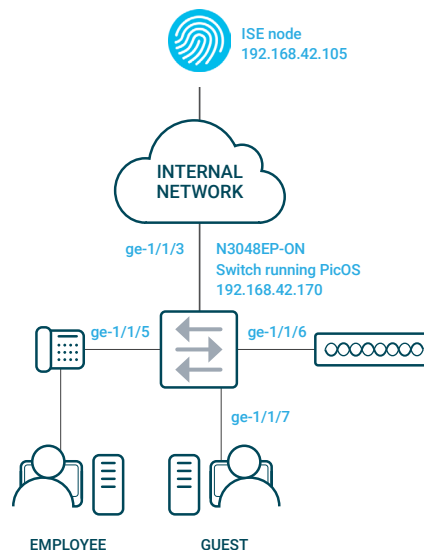
This integration example uses the following hardware and software components for the policy infrastructure:

- 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 use 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 connected.







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

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Pica8-Mab-Auth		Wired_MAB	Default Network Access	702
✓	Pica8-Employee		Wired_802.1X	Default Network Access	35
✓	Pica8-Registered-Device		Wired_MAB	Default Network Access	0
✓	Default	Default policy set		Default Network Access	0

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.

Status	Rule Name	Conditions	Results	Security Groups	Hits	Actions
✓	Default		<div>pica8-employee-acl-profile pica8-employee-vlan-profile</div>	Select from list	10	

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 logs 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.



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

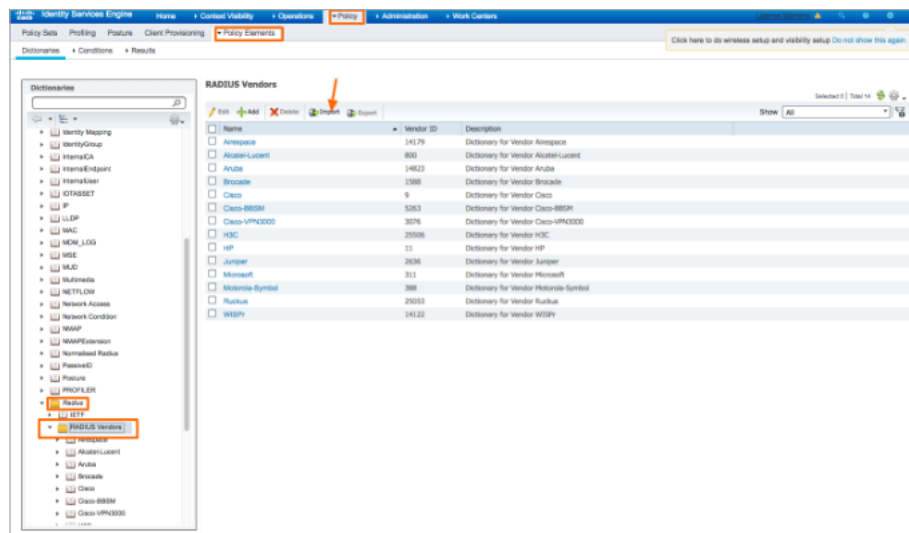
The following three configuration steps are needed to configure the ISE node for RADIUS Authentication.

1. Import PicOS Network Device Profile
2. Configure PicOS Network Device Profile
3. Add a PicOS switch as ISE network device

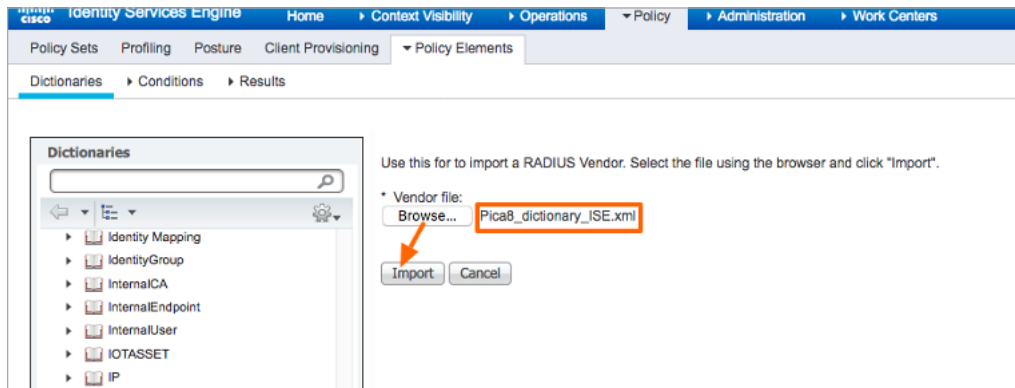
### Import PicOS Network Device Profile

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).

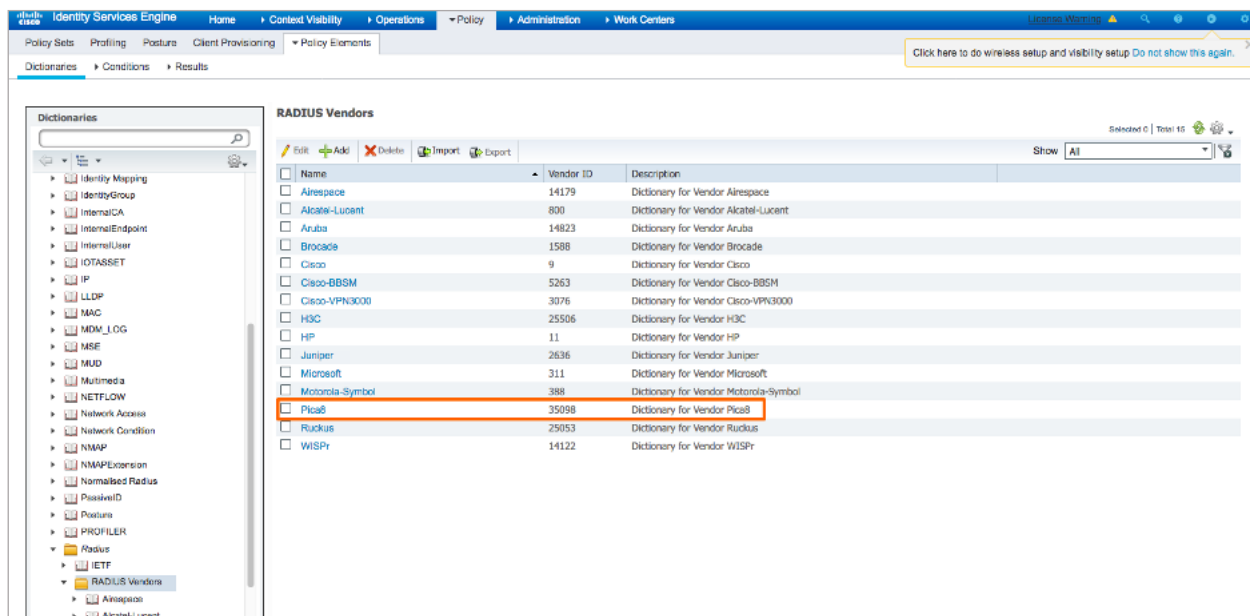
To import the PicOS Radius dictionary for ISE, navigate to **Policy->Policy Elements -> Dictionaries -> System -> Radius -> RADIUS Vendors**, and click Import at the top of the table as shown below.



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.



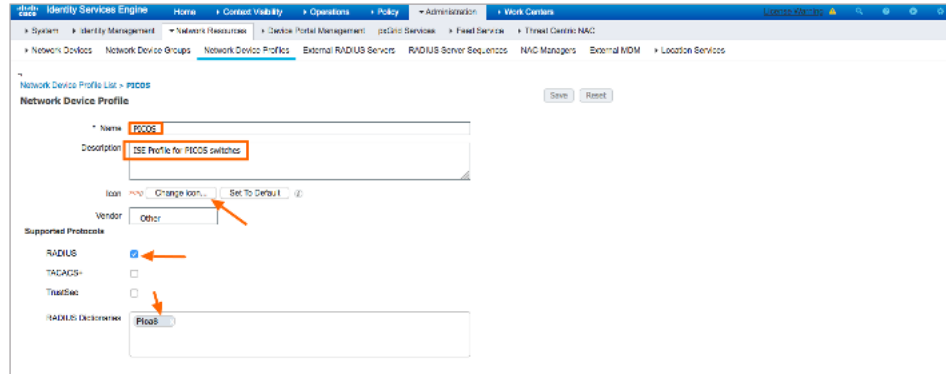
## Configure PicOS Network Device Profile

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.



Network Device Profile List > PICO8

Network Device Profile

Name: PICO8

Description: ISE Profile for PICO8 switches

Icon: Change icon... Set To Default

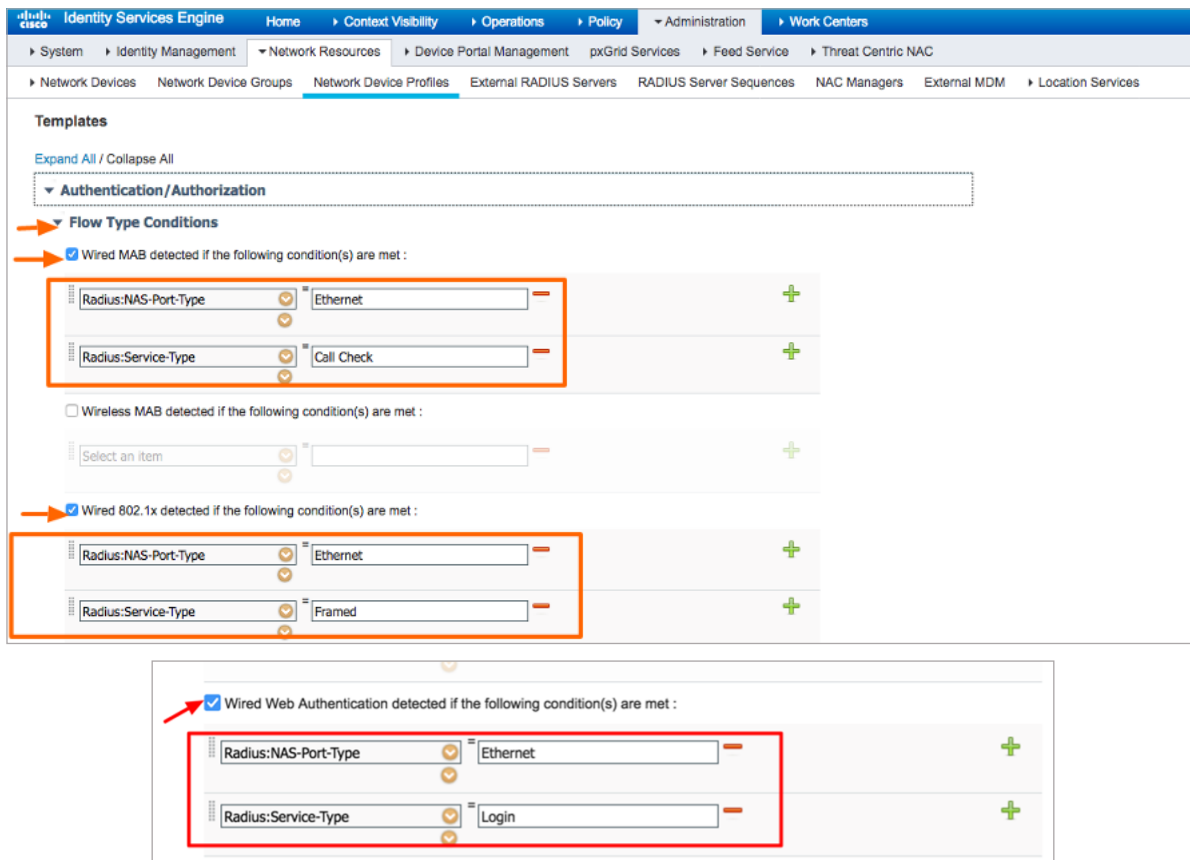
Vendor: Other

Supported Protocols:

- ☒ RADIUS
- ☐ TACACS+
- ☐ TruSecure

RADIUS Authentication: Pico8

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



Identity Services Engine

Home > Context Visibility > Operations > Policy > Administration > Work Centers

System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Centric NAC

Network Devices > Network Device Groups > Network Device Profiles > External RADIUS Servers > RADIUS Server Sequences > NAC Managers > External MDM > Location Services

Templates

Expand All / Collapse All

Authentication/Authorization

Flow Type Conditions

Wired MAB detected if the following condition(s) are met :

- Radius:NAS-Port-Type = Ethernet
- Radius:Service-Type = Call Check

Wireless MAB detected if the following condition(s) are met :

- Select an item

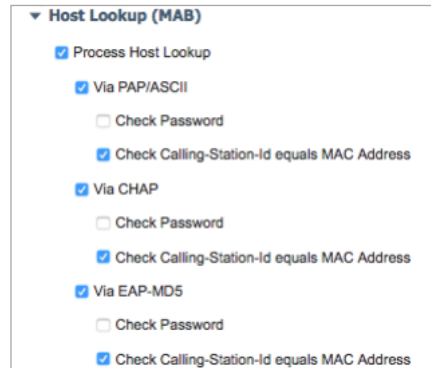
Wired 802.1x detected if the following condition(s) are met :

- Radius:NAS-Port-Type = Ethernet
- Radius:Service-Type = Framed

Wired Web Authentication detected if the following condition(s) are met :

- Radius:NAS-Port-Type = Ethernet
- Radius:Service-Type = Login

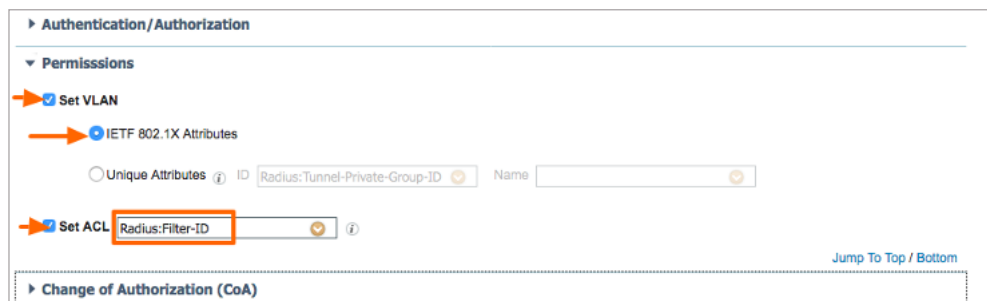
3. Set Host lookup (MAB) as shown below.



**Host Lookup (MAB)**

- ☒ Process Host Lookup
  - ☒ Via PAP/ASCII
    - ☐ Check Password
    - ☒ Check Calling-Station-Id equals MAC Address
  - ☒ Via CHAP
    - ☐ Check Password
    - ☒ Check Calling-Station-Id equals MAC Address
  - ☒ Via EAP-MD5
    - ☐ Check Password
    - ☒ Check Calling-Station-Id equals MAC Address

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.



**Authentication/Authorization**

**Permissions**

- ☒ Set VLAN
  - ☒ IETF 802.1X Attributes
    - ☐ Unique Attributes
      - ID: Radius:Tunnel-Private-Group-ID
      - Name:
- ☒ Set ACL
  - Radius:Filter-ID

[Jump To Top / Bottom](#)

**Change of Authorization (CoA)**

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**

**Identity Services Engine** Home Context Visibility Operations Policy Administration Work Centers

System Identity Management **Network Resources** Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Network Devices Network Device Groups **Network Device Profiles** External RADIUS Servers RADIUS Server Sequences NAC Managers

**Change of Authorization (CoA)**

CoA by **RADIUS**

\* Default CoA Port 3799

\* Default DTLS CoA Port 2083

\* Timeout Interval 5 seconds

\* Retry Count 3

Send Message-Authenticator ☒

**Disconnect**

☒ RFC 5176

**RADIUS:Acct-Terminate-Cause** = Admin Reset

☒ Port Bounce

**Pica8:Pica8-AVPair** = command=pica8-bounce-host-por

**RADIUS:Acct-Terminate-Cause** = Admin Reset

☒ Port Shutdown

**Pica8:Pica8-AVPair** = command=pica8-bounce-host-por

**RADIUS:Acct-Terminate-Cause** = Admin Reset

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

**Identity Services Engine** Home Context Visibility Operations Policy Administration Work Centers

System Identity Management **Network Resources** Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Network Devices Network Device Groups **Network Device Profiles** External RADIUS Servers RADIUS Server Sequences NAC Managers

**CoA Push**

☐ RFC 5176

Select an Item

**Redirect**

Type Dynamic URL

**Pica8:Pica8-Redirect-URL** = \${URL}

**Dynamic URL Parameter**

☐ Session ID

☒ Client MAC Address

☐ None

**Redirect URL Parameter Names**

Client IP Address

**Client MAC Address** mac

Originating URL

Session ID

SSID



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.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface for adding a new network device. The page is titled "Network Devices" and includes a sidebar with navigation options like "System", "Identity Management", "Network Resources", "Device Portal Management", "pxGrid Services", "Feed Service", and "Threat Centric NAC". The main content area is divided into sections for "Network Devices", "Default Device", and "Device Security Settings". The "Network Devices" section is active, showing a form to add a new device. The form includes fields for "Name" (Branch-A-Access-Sw), "IP Address" (192.168.42.170), "Device Profile" (PICOS), "Model Name" (N3248P-ON), and "Software Version" (4.1.2.2). Below these are "Network Device Group" settings for Location, IPSEC, and Device Type. The "RADIUS Authentication Settings" section is expanded, showing "RADIUS UDP Settings" with Protocol set to RADIUS, Shared Secret set to pica8pica8, and CoA Port set to 3799. The "RADIUS DTLS Settings" section is also visible, with DTLS Required set to false and CoA Port set to 2083. A red arrow points to the "RADIUS Authentication Settings" section.

### 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
```

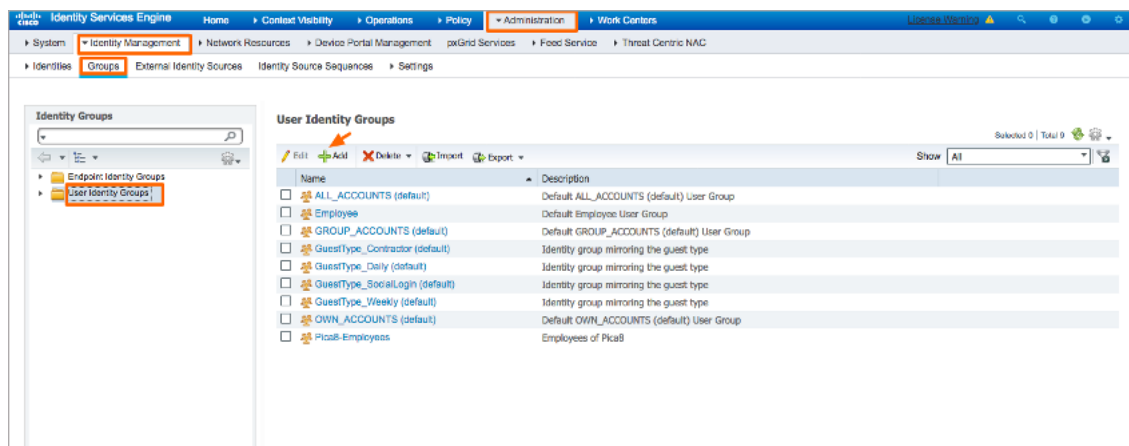
### Configure the 802.1x Wired Access Policy for Employee Laptop

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

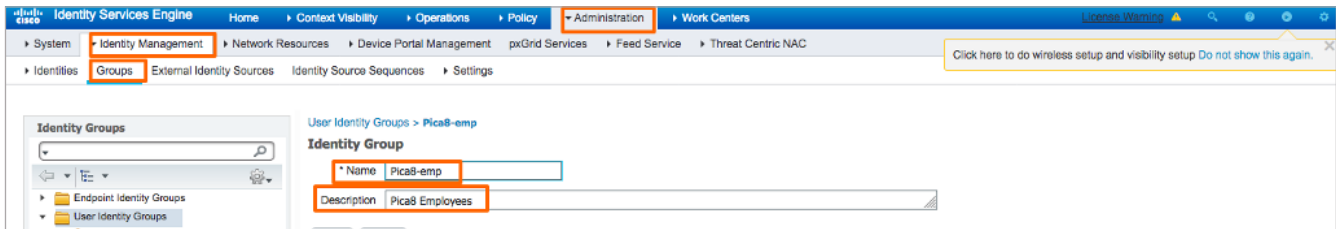
1. Create User Identity groups and integrate with AD or add local users
2. Create an Authorization Profile to dynamically assign VLAN 10 for employee laptops running 802.1x supplicant
3. Create an Authorization Profile to dynamically assign an ACL called mac\_auth\_policy\_2 to the employee laptops that 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.

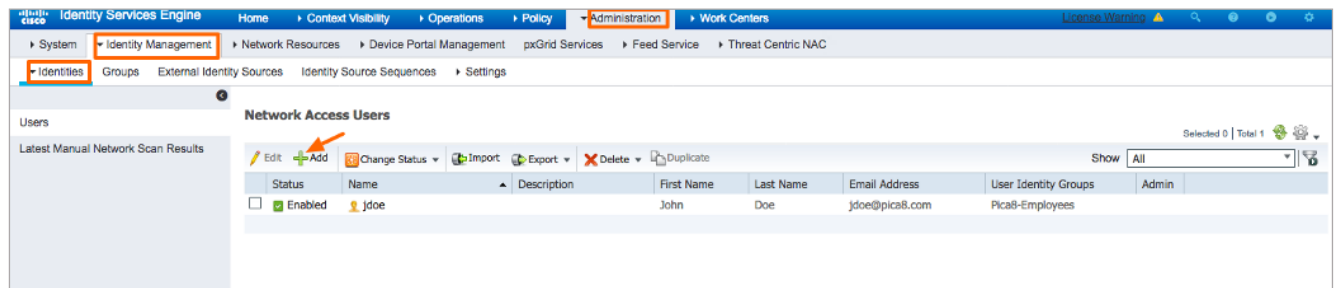


Enter **Name** and **Description** of the Group as shown below and click **Submit**.



The screenshot shows the 'Administration' tab in the Identity Services Engine. Under 'Identity Management', the 'Identities' section is selected, and the 'Groups' sub-section is active. The 'Identity Group' configuration for 'Pica8-emp' is displayed. The 'Name' field is set to 'Pica8-emp' and the 'Description' field is set to 'Pica8 Employees'.

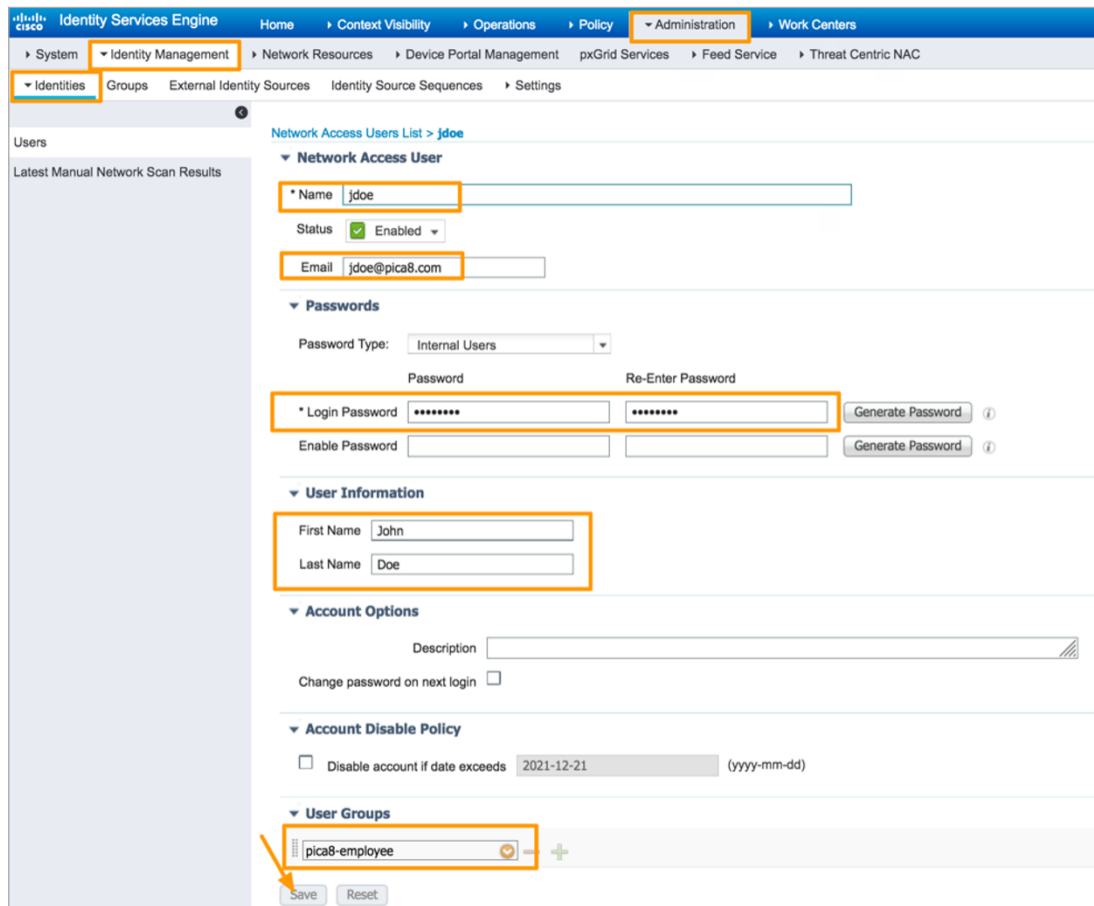
To add a user, navigate to **Administration -> Identity Management->Identities** and click **+** as shown below.



The screenshot shows the 'Administration' tab in the Identity Services Engine. Under 'Identity Management', the 'Identities' section is selected, and the 'Groups' sub-section is active. The 'Network Access Users' list is displayed, showing a table with columns: Status, Name, Description, First Name, Last Name, Email Address, User Identity Groups, and Admin. A red arrow points to the 'Add' button in the top left corner of the table.

Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
<input checked="" type="checkbox"/> Enabled	jdoe		John	Doe	jdoe@pica8.com	Pica8-Employees	Admin

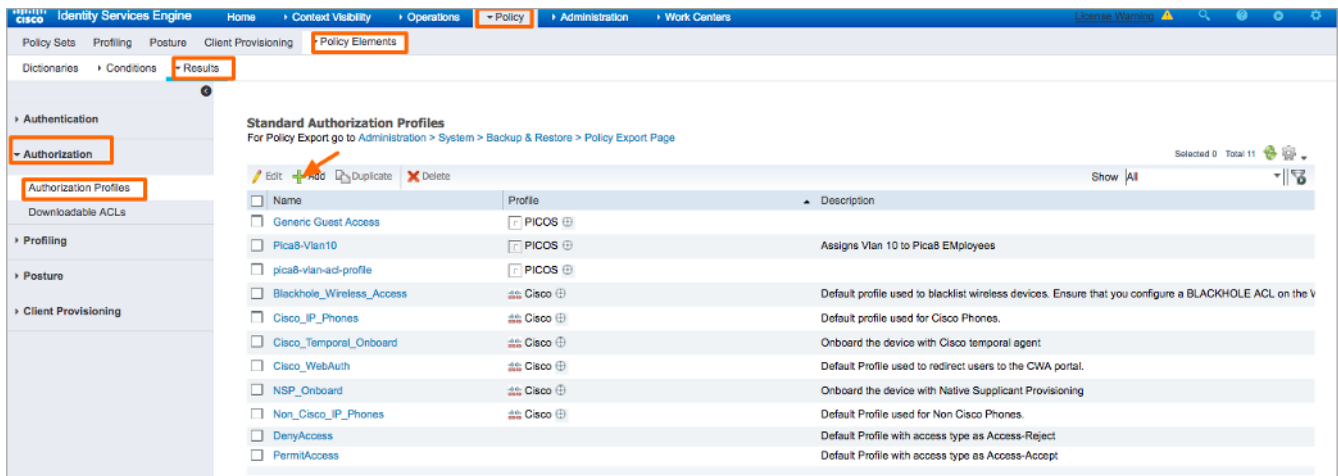
Enter **Name**, **Email**, **Login Password** and select **Pica8-Employees** for **User Groups** as shown below and click **Submit**. In this example we are adding **Network Access User** account for John Doe.



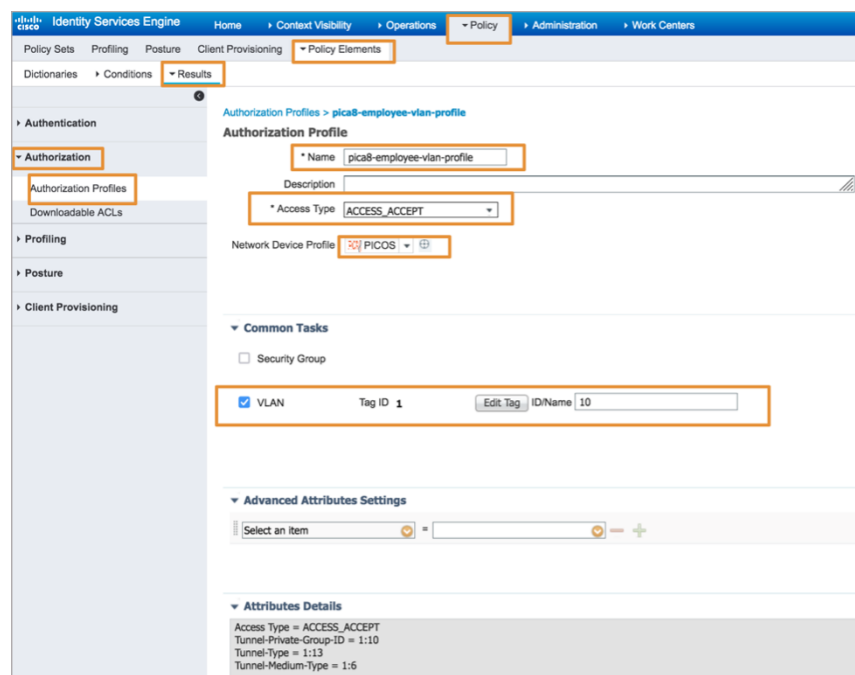
The screenshot shows the 'Administration' tab in the Identity Services Engine. Under 'Identity Management', the 'Identities' section is selected, and the 'Groups' sub-section is active. The 'Network Access Users List > jdoe' page is displayed, showing the configuration form for a new user. The form includes fields for Name, Status, Email, Passwords, User Information, Account Options, Account Disable Policy, and User Groups. The 'Name' field is set to 'jdoe', the 'Status' is 'Enabled', the 'Email' is 'jdoe@pica8.com', the 'Login Password' is '\*\*\*\*\*', the 'First Name' is 'John', and the 'Last Name' is 'Doe'. The 'User Groups' section shows 'pica8-employee' selected.

## 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**.

The screenshot shows the 'Policy Elements' configuration page in Cisco ISE. The 'Authorization Profile' section is active, showing the following configuration:

- Name:** pica8-employee-ad-profile
- Description:** (empty)
- Access Type:** ACCESS\_ACCEPT
- Network Device Profile:** PICOS
- Common Tasks:**
  - ☒ **ACL (Filter-ID):** mac\_auth\_policy\_2
  - ☐ **Security Group:** (empty)
- Advanced Attributes Settings:** (empty)
- Attributes Details:**
  - Access Type = ACCESS\_ACCEPT
  - Filter-ID = mac\_auth\_policy\_2

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

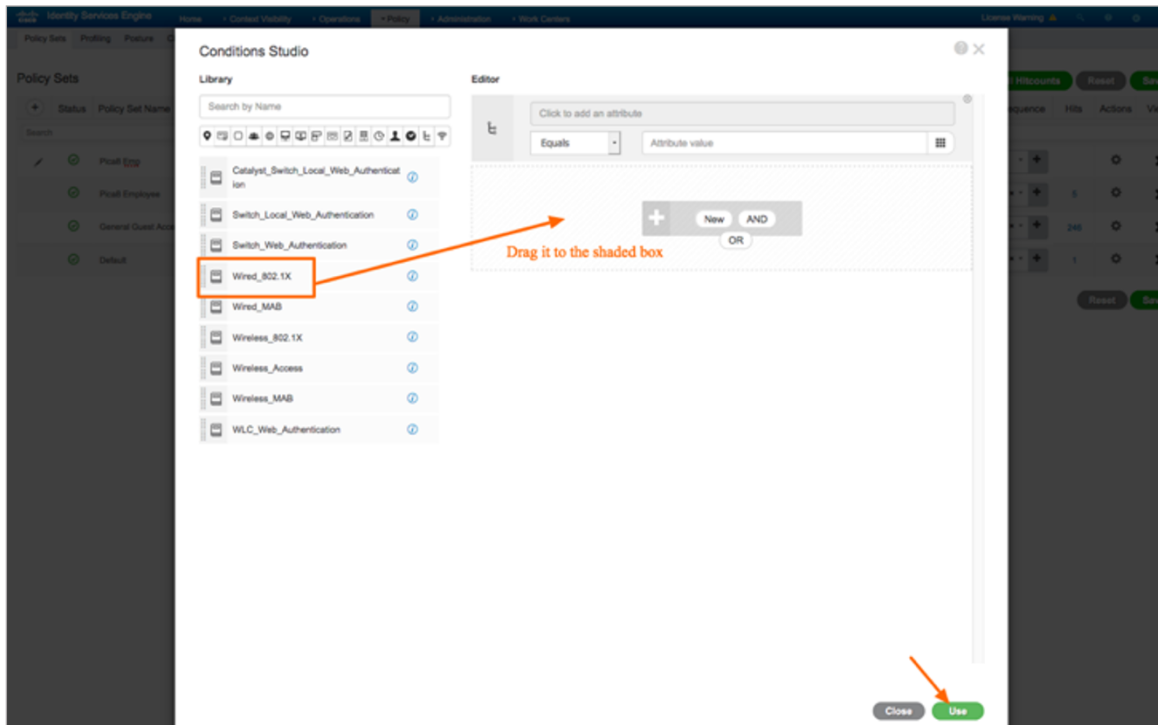
Cisco ISE is a policy-based, network-access-control solution that offers network access policy sets, thus allowing you to manage several different network access use cases such as wireless, wired, guest, and client provisioning. Policy sets (both network access and device administration sets) enable 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.

The screenshot shows the 'Policy Sets' configuration page in Cisco ISE. The 'Policy Sets' section is active, showing a table of existing policy sets:

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	Pica8 Employee		Wired_802.1X	Default Network Access	5	⚙️	➡️
✓	General Guest Access		Wired_MAB	Default Network Access	246	⚙️	➡️
✓	Default	Default policy set		Default Network Access	1	⚙️	➡️

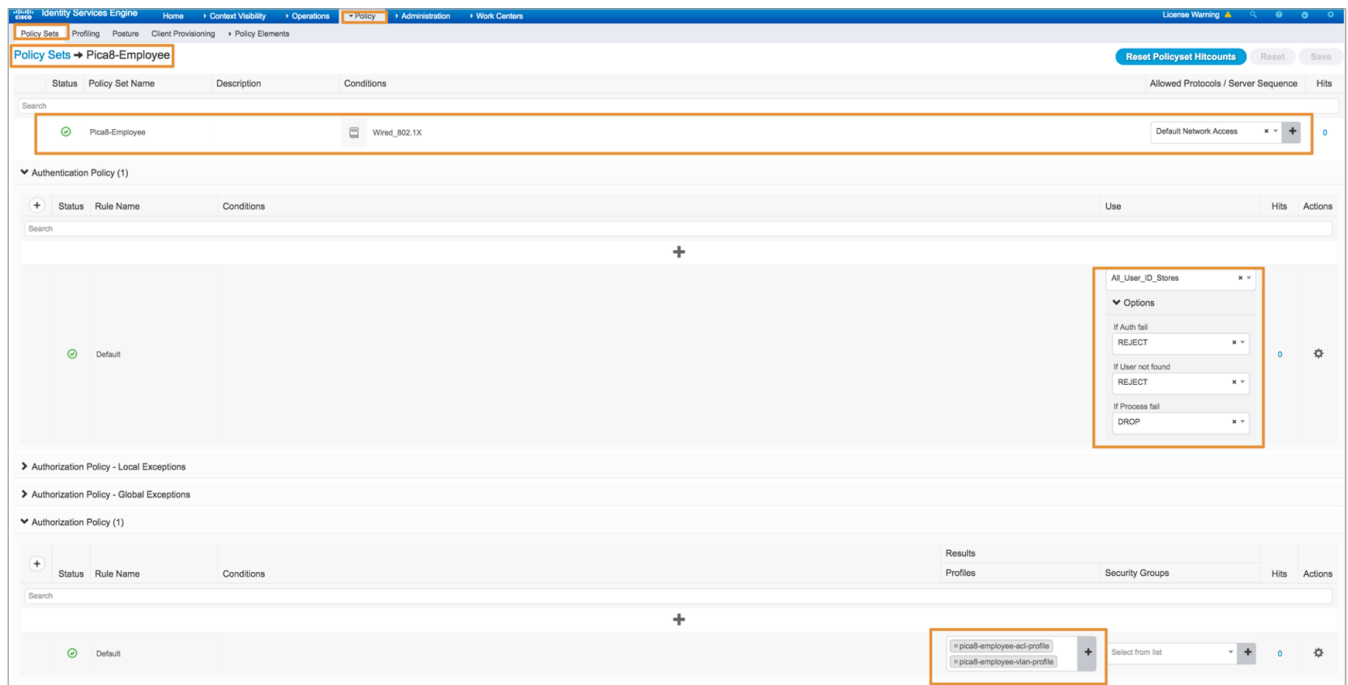
Enter **Policy Set** name as **Pica8\_Employees** and click **+** sign under **Conditions**, drag **Wired\_MAB** to the shaded box and click **Use**.



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

Identity Services Engine							License Warning		
Policy Sets							ResetAll Hitcounts		
Policy Sets							Reset		
Policy Sets							Save		
Policy Sets							Allowed Protocols / Server Sequence		
Policy Sets							Hits		
Policy Sets							Actions		
Policy Sets							View		
Policy Sets									
Pica8 Employee							Default Network Access	5	
General Guest Access							Default Network Access	246	
Default							Default Network Access	1	

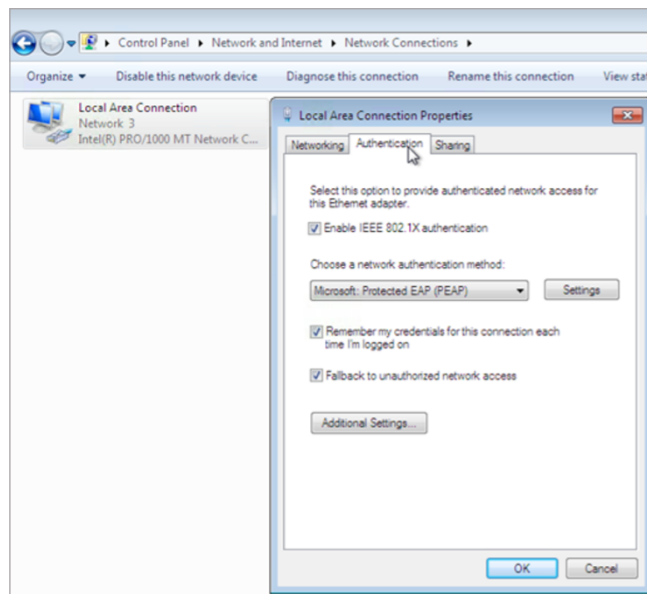
Set **Authentication Policy Options** as shown below. Set **Authorization Policy** to **Pica8-employee-acl-profile** and **Pica8-employee-VLAN-profile** as shown below. Click **Save**.



## 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.

Time	Status	Details	Repeat	Identity	Endpoint ID	Endpoint P...	Authentication Policy	Authorizati...	Authorization Profiles	IP Address
Oct 13, 2021 01:18:09.765 PM	Success		0	jdoe	80:E8:2C:B9:28:DB	HP-Device	Pica8-Employee >> Default	Pica8-Empl...	pica8-employee-ad-profile,pica8-employee-vlan-profile	
Oct 13, 2021 01:18:09.707 PM	Success			jdoe	80:E8:2C:B9:28:DB	HP-Device	Pica8-Employee >> Default	Pica8-Empl...	pica8-employee-ad-profile,pica8-employee-vlan-profile	
Oct 13, 2021 01:18:08.833 PM	Failure				80:E8:2C:B9:28:DB					
Oct 13, 2021 01:14:50.166 PM	Failure		2	18:5A:58:1D:9C:21	18:5A:58:1D:9C:21	Dell-Device	Pica8-Web-Auth >> Pica8...	Pica8-Web...	CWA_preauth	
Oct 13, 2021 01:14:47.201 PM	Success			18:5A:58:1D:9C:21	18:5A:58:1D:9C:21	Dell-Device	Pica8-Web-Auth >> Pica8...	Pica8-Web...	CWA_preauth	
Oct 13, 2021 01:14:41.271 PM	Success			18:5A:58:1D:9C:21	18:5A:58:1D:9C:21	Dell-Device	Pica8-Web-Auth >> Pica8...	Pica8-Web...	CWA_preauth	
Oct 13, 2021 01:14:41.155 PM	Success			80:E8:2C:B9:28:DB	80:E8:2C:B9:28:DB	HP-Device	Pica8-Web-Auth >> Pica8...	Pica8-Web...	CWA_preauth	
Oct 13, 2021 01:14:37.964 PM	Failure				80:E8:2C:B9:28:DB					
Oct 13, 2021 01:14:37.132 PM	Failure				80:E8:2C:B9:28:DB					



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

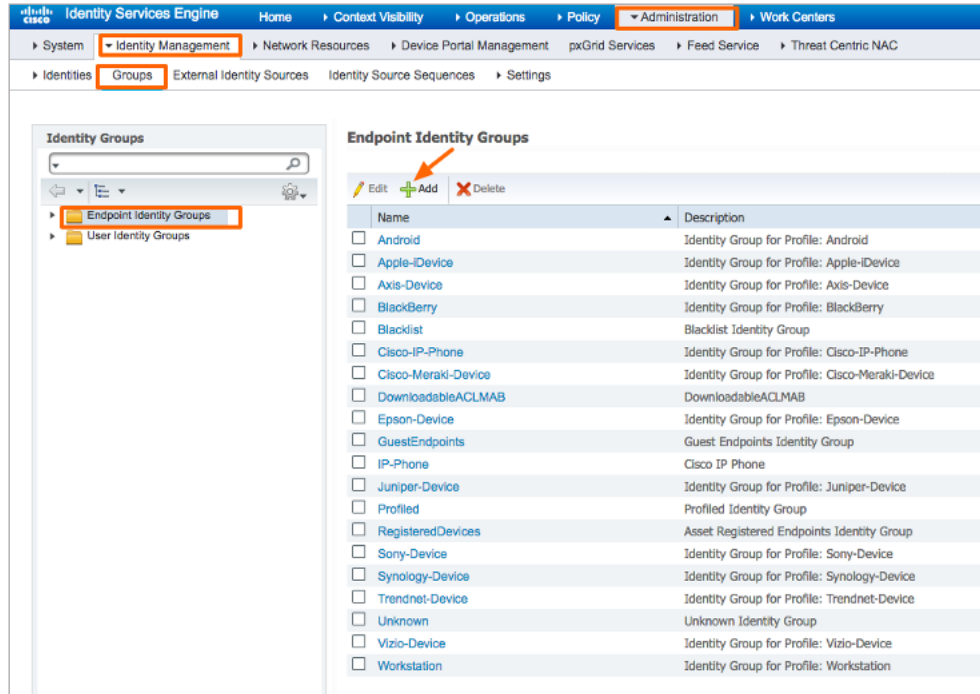
Configuring the MAB Wired Access Policy in ISE for IP Phones involves following three steps:

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.

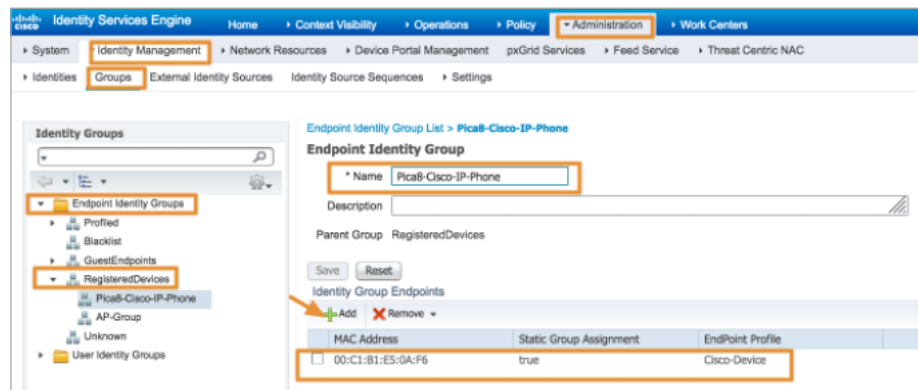
#### Creating an IP-Phone Endpoint Identity Group and add IP Phone Mac Addresses

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



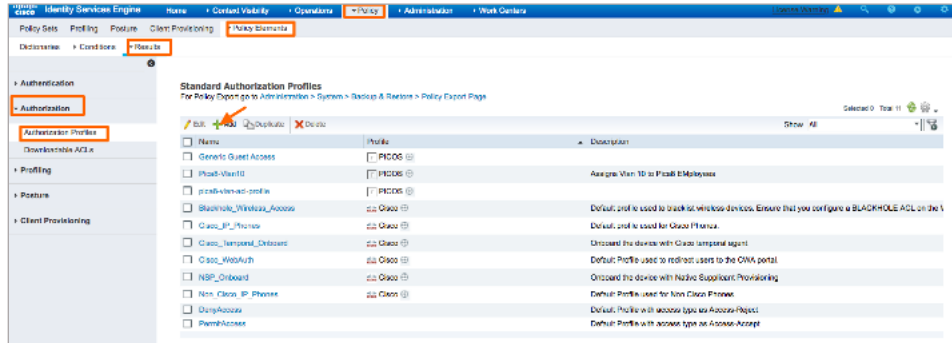


Enter **Name**, **Description** and click **Submit**. Select Pica8-Cisco-IP-Phone Groups and click **+** and select the MAC address of the IP phone to add IP Phone to this Endpoint Identity Group as shown below.

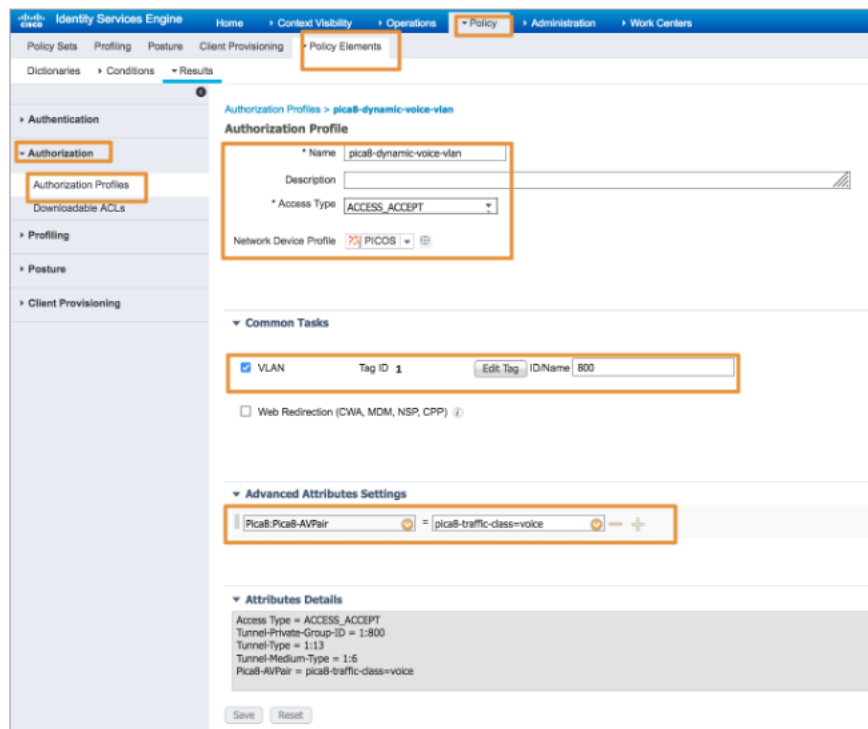


### Create an Authorization Profile to Dynamically Assign a Voice VLAN

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

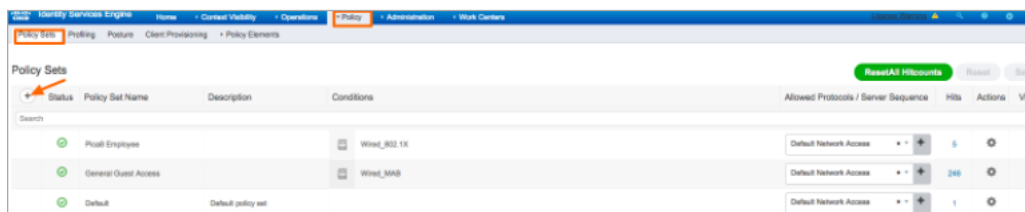


Enter **Name**, **Description**, and set **Access Type** to **ACCESS\_ACCEPT**, then set **Network Device Profile** to **PicoS**. Check the box for **VLAN** and enter an attribute value that identifies a VLAN. In this example VLAN ID 800 is used for Voice VLAN. Expand **Advanced Attribute Settings**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

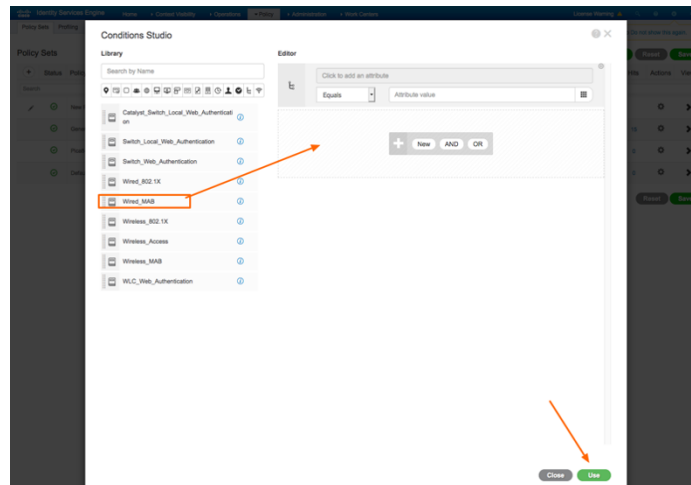


## Create a Wired Access Policy for an IP Phone

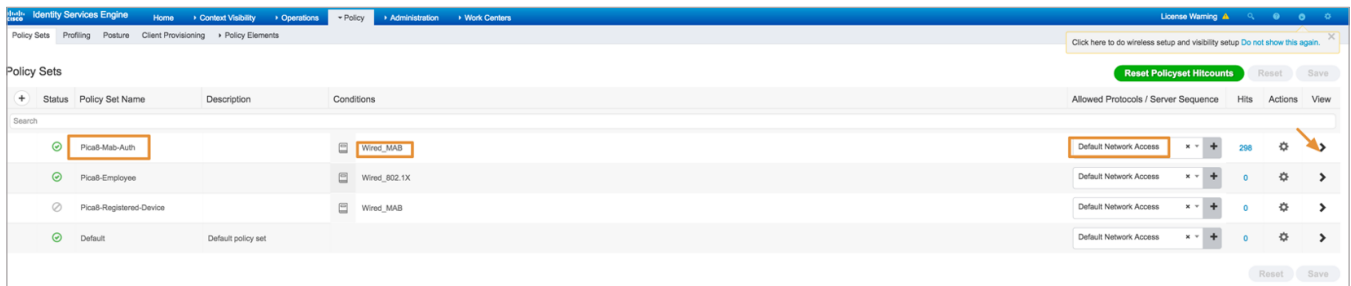
Let us create a **Policy Set** called **Pica8-Mab-Auth** to authenticate various **Endpoint Identity Groups** using **MAB** authentication. We will place the IP Phones on voice VLAN 800. Navigate to **Policy -> Policy Sets** and click **+** as shown below.



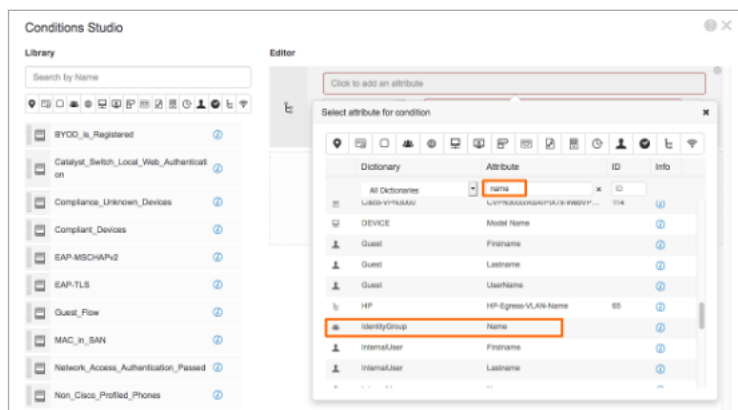
Enter the **Policy Set** name as **General Access** and click **+** sign under **Conditions**, drag **Wired\_MAB** to the shaded box and click **Use**.



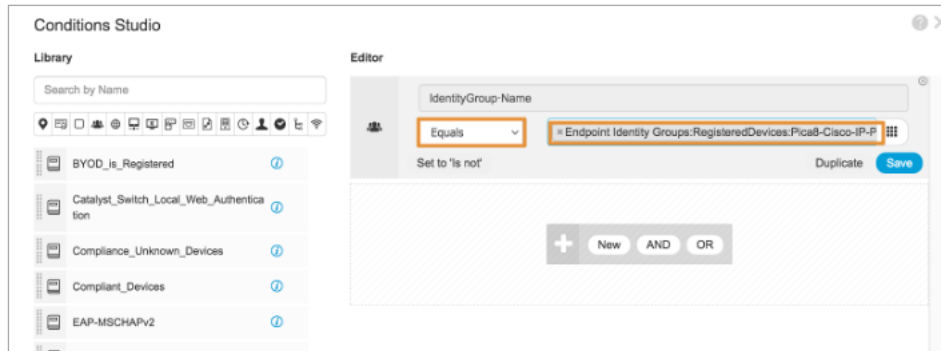
Set **Allowed Protocols** to **Default Network Access**, click **Save** and click **>** sign as shown below.



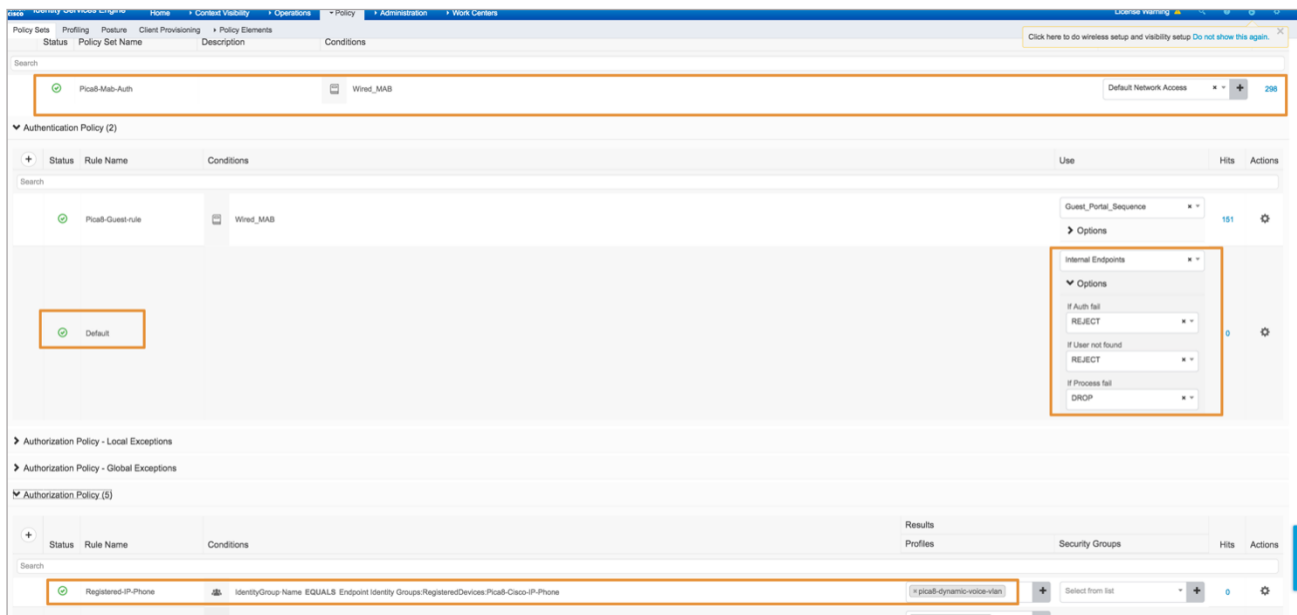
Set **Authentication Policy Options** as shown below. Create a new rule under **Authorization Policy** called **Registered-IP-Phone**. Click **+** sign under **Conditions**. In the **Attribute** field, search for the string **name** and then select the **IdentityGroup Name** attribute as shown below.



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.

Cisco Identity Services Engine									
Home > Context Visibility > Operations > Policy > Administration > Work Centers									
License Warning									
RADIUS > Threat-Centric NAC Live Logs > TACACS > Troubleshoot > Adaptive Network Control > Reports									
Click here to do wireless setup and visibility setup Do not s									
Live Logs Live Sessions									
Misconfigured Supplicants 0 Misconfigured Network Devices 0 RADIUS Drops 0 Client Stopped Responding 0 Repeat Counter 14									
Refresh Never Show Latest 100 records Within Last									
Refresh Reset Repeat Counts Export To									
Details	Repeat ...	Identity	Endpoint ID	Endpoint ...	Authentication Policy	Authorization Policy	Authorization Profiles		Device Port
		Identity	Endpoint ID	Endpoint Ph	Authentication Policy	Authorization Policy	Authorization Profiles		Device Port
	1	jdoe	80:E8:2C:B9:28:DB	HP-Device	Pica8-Employee >> Default	Pica8-Employee >> Default	pica8-employee-acl-profile,pica8-employee-vlan-profile		
		jdoe	80:E8:2C:B9:28:DB	HP-Device	Pica8-Employee >> Default	Pica8-Employee >> Default	pica8-employee-acl-profile,pica8-employee-vlan-profile		
	4	00:C1:...	00:C1:B1:E5:0A:F6	Cisco-Device	Pica8-Mab-Auth >> Pica8-Gues...	Pica8-Mab-Auth >> Registered-IP-Phone	pica8-dynamic-voice-vlan		

## Overview

Event	5200 Authentication succeeded
Username	00:C1:B1:E5:0A:F6
Endpoint Id	00:C1:B1:E5:0A:F6
Endpoint Profile	Cisco-Device
Authentication Policy	Pica8-Mab-Auth >> Pica8-Guest-rule
Authorization Policy	Pica8-Mab-Auth >> Registered-IP-Phone
Authorization Result	pica8-dynamic-voice-vlan

## Access Point Authentication

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

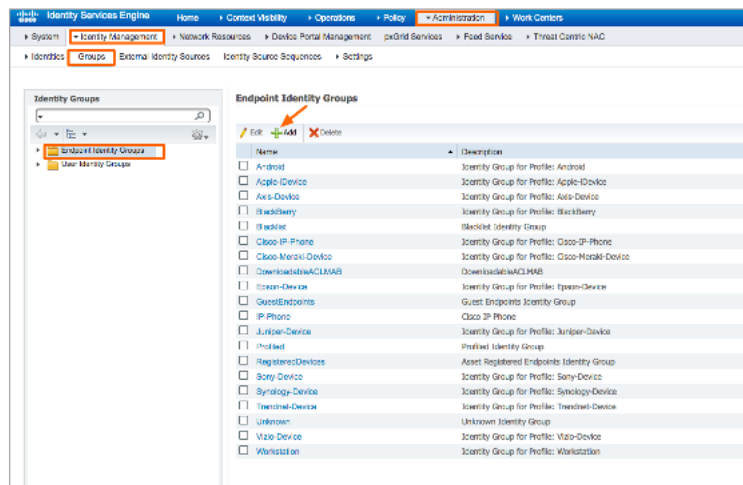
### Configuring the MAB Wired Access Policy in ISE for an Access Point

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

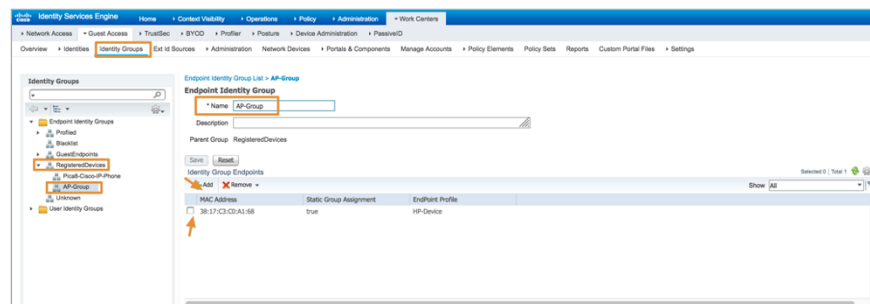
1. Create an Endpoint Identity Group for Access Points and add the Access Point Mac addresses.
2. Create an Authorization Profile to dynamically assign VLAN 10 for the Access Points.
3. Create an Authorization Profile to use downloadable ACL mac\_auth\_policy\_3 configured in ISE.
4. Create a Wired Access 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.

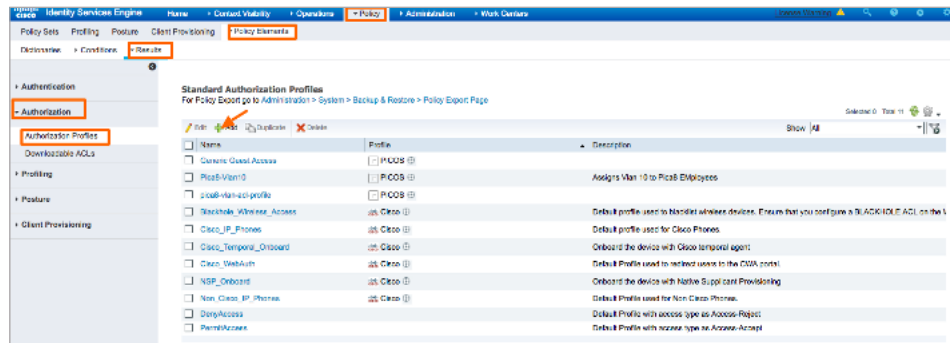


Enter **Name and Description** and click **Submit**. Select **AP-Group Endpoint Identity Groups** and click **+** and select the MAC address of the Access Point to add MAC address of Access Point as shown below.

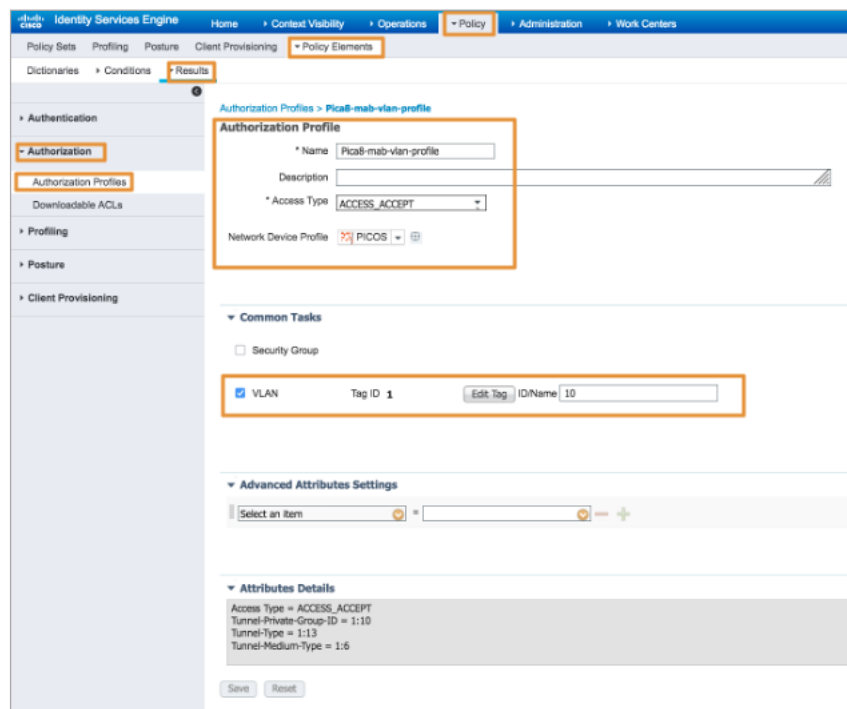


### Create an Authorization Profile to Dynamically Assign a VLAN for Access Points

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.

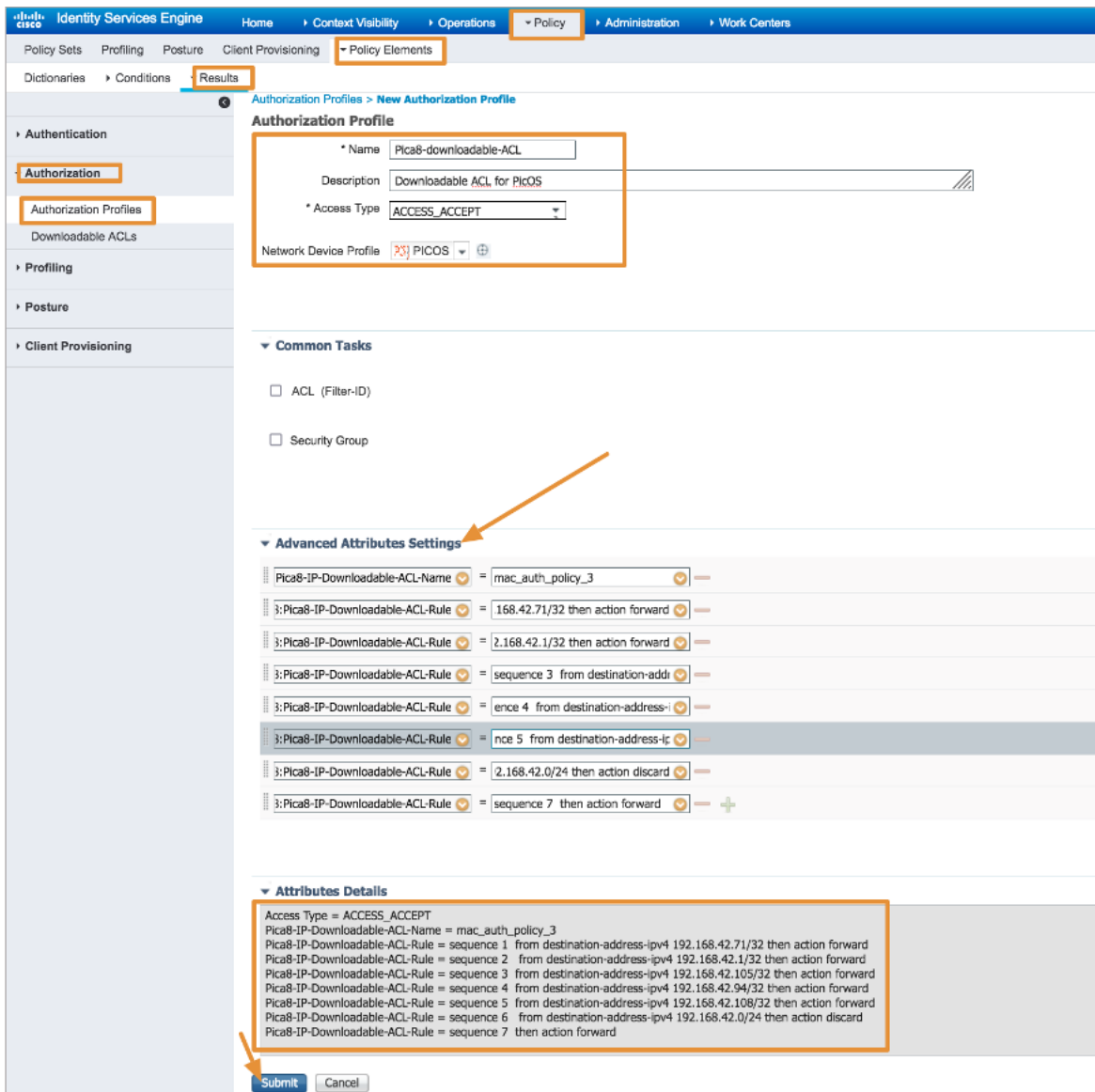
### Create Authorization Profile to Use Downloadable ACL mac\_auth\_policy\_3 Configured in ISE

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.



**Authorization Profile**

Name: Pica8-downloadable-ACL

Description: Downloadable ACL for PicoS

Access Type: ACCESS\_ACCEPT

Network Device Profile: PICO S

**Common Tasks**

☐ ACL (Filter-ID)

☐ Security Group

**Advanced Attributes Settings**

Pica8-IP-Downloadable-ACL-Name = mac\_auth\_policy\_3

3:Pica8-IP-Downloadable-ACL-Rule = 168.42.71/32 then action forward

3:Pica8-IP-Downloadable-ACL-Rule = 2.168.42.1/32 then action forward

3:Pica8-IP-Downloadable-ACL-Rule = sequence 3 from destination-address

3:Pica8-IP-Downloadable-ACL-Rule = ence 4 from destination-address-i

3:Pica8-IP-Downloadable-ACL-Rule = nce 5 from destination-address-l

3:Pica8-IP-Downloadable-ACL-Rule = 2.168.42.0/24 then action discard

3:Pica8-IP-Downloadable-ACL-Rule = sequence 7 then action forward

**Attributes Details**

Access Type = ACCESS\_ACCEPT

Pica8-IP-Downloadable-ACL-Name = mac\_auth\_policy\_3

Pica8-IP-Downloadable-ACL-Rule = sequence 1 from destination-address-ipv4 192.168.42.71/32 then action forward

Pica8-IP-Downloadable-ACL-Rule = sequence 2 from destination-address-ipv4 192.168.42.1/32 then action forward

Pica8-IP-Downloadable-ACL-Rule = sequence 3 from destination-address-ipv4 192.168.42.105/32 then action forward

Pica8-IP-Downloadable-ACL-Rule = sequence 4 from destination-address-ipv4 192.168.42.94/32 then action forward

Pica8-IP-Downloadable-ACL-Rule = sequence 5 from destination-address-ipv4 192.168.42.108/32 then action forward

Pica8-IP-Downloadable-ACL-Rule = sequence 6 from destination-address-ipv4 192.168.42.0/24 then action discard

Pica8-IP-Downloadable-ACL-Rule = sequence 7 then action forward

**Submit** **Cancel**

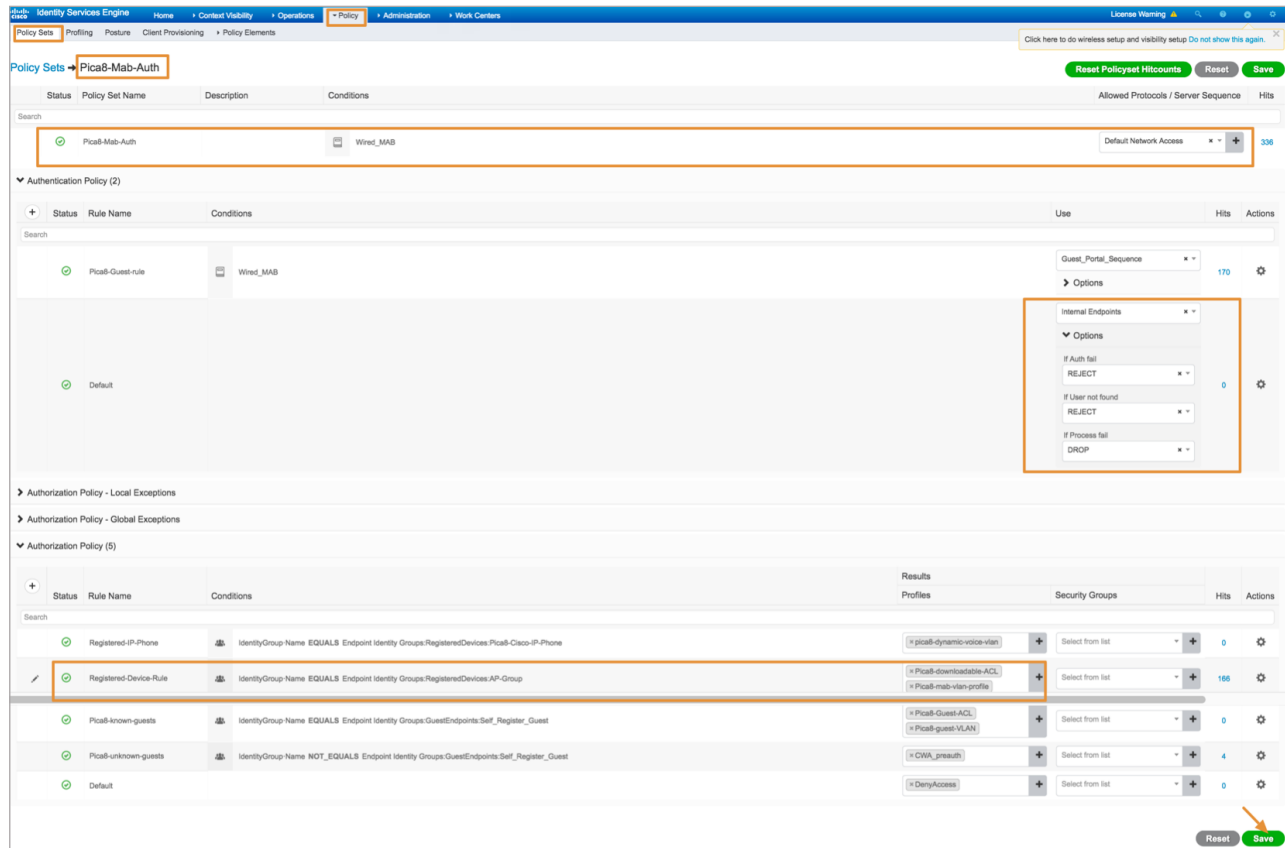
Please note: ISE and other Radius servers have threshold of 4096 bytes for size of the Access-Accept messages used by the Radius server for DACL. If your ACL size is huge, you will run into problems. For this purpose PicoS uses abbreviated downloadable ACLs. Please refer to the [Downloadable ACL](#)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

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authentication Policy	Authorization Policy	Authorization Profiles
Oct 26, 2021 11:25:18.967 AM			1	38:17:C3:C0:A1:68	38:17:C3:C0:A1:68	HP-Device	Pica8-Mab-Auth >> Pica8-Guest-rule	Pica8-Mab-Auth >> Registered-Device-Rule	Pica8-downloadable-ACL,Pica8-mab-vlan-profile
Oct 26, 2021 11:25:18.928 AM				38:17:C3:C0:A1:68	38:17:C3:C0:A1:68	HP-Device	Pica8-Mab-Auth >> Pica8-Guest-rule	Pica8-Mab-Auth >> Registered-Device-Rule	Pica8-downloadable-ACL,Pica8-mab-vlan-profile
Oct 26, 2021 11:25:18.728 AM				38:17:C3:C0:A1:68	38:17:C3:C0:A1:68	HP-Device	Pica8-Mab-Auth >> Pica8-Guest-rule	Pica8-Mab-Auth >> Registered-Device-Rule	Pica8-downloadable-ACL,Pica8-mab-vlan-profile
Oct 26, 2021 11:18:52.904 AM				38:17:C3:C0:A1:68	38:17:C3:C0:A1:68	HP-Device	Pica8-Mab-Auth >> Pica8-Guest-rule	Pica8-Mab-Auth >> Registered-Device-Rule	Pica8-downloadable-ACL,Pica8-mab-vlan-profile

### Overview

Event	5200 Authentication succeeded
Username	38:17:C3:C0:A1:68
Endpoint Id	38:17:C3:C0:A1:68 ⓘ
Endpoint Profile	HP-Device
Authentication Policy	Pica8-Mab-Auth >> Pica8-Guest-rule
Authorization Policy	Pica8-Mab-Auth >> Registered-Device-Rule
Authorization Result	Pica8-downloadable-ACL,Pica8-mab-vlan-profile

## 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 logs in 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
```

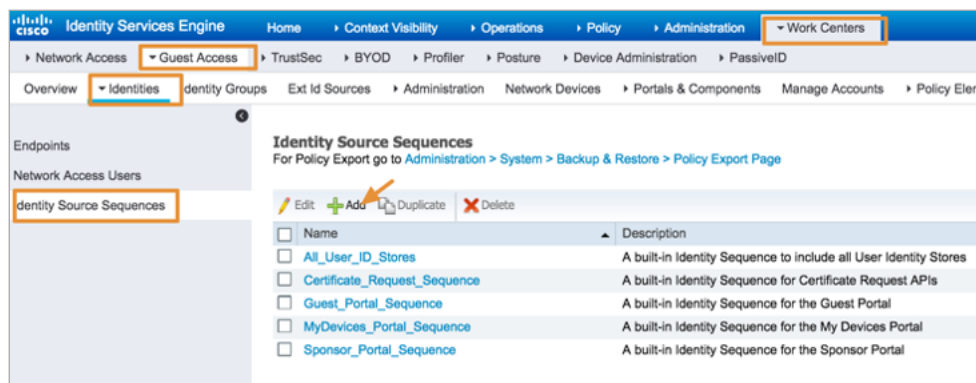
## Configuring the ISE Node With a Central Web Authentication Policy

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**.

**Guest Type**

Guest type name: **Self\_Register\_Guest**

Description:

Language File

Collect Additional Data: Custom Fields...

Maximum Access Time

Account duration starts

☐ From first login

☒ From sponsor-specified date (or date of self-registration, if applicable)

Maximum account duration

5 days Default: 1 (1-999)

☐ Allow access only on these days and times:

From 9:00 AM To 5:00 PM ☐ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☐ Sat

Configure guest Account Purge Policy at:  
[Work Centers > Guest Access > Settings > Guest Account Purge Policy](#)

Login Options

☒ Maximum simultaneous logins 3 (1-999)

When guest exceeds limit:

☒ Disconnect the oldest connection

☐ Disconnect the newest connection

☐ Redirect user to a portal page showing an error message (i)  
This requires the creation of an authorization policy rule

Maximum devices guests can register: 5 (1-999)

Endpoint identity group for guest device registration: **Self\_Register\_Guest** (i)

Configure endpoint identity groups at: [Work Centers > Guest Access > Identity Groups](#)

The endpoints in this group will be purged according to the policies defined in: [Administration > Identity Management > Settings > Endpoint purge](#)

☐ Allow guest to bypass the Guest portal

Account Expiration Notification

☐ Send account expiration notification 3 days before account expires (i)

View messages in:  
English - English

☐ Email

☐ Send a copy of the notification email to the Sponsor

Use customization from: **Sponsor Portal (default)**

Messages: Copy text from:

Your account is going to expire in 3 days. Please notify your sponsor to extend your account now to avoid any delays.

Send test email to me at: Send

Configure SMTP server at: [Work Centers > Guest Access > Administration > SMTP server](#)

☐ SMS

Messages: Copy text from:

Your account is going to expire in 3 days. Please notify your sponsor to extend your account now to avoid any delays.

(160 character limit per message)\*Over 160 characters requires multiple messages.

Send test SMS to me at: phone number Global Default Send

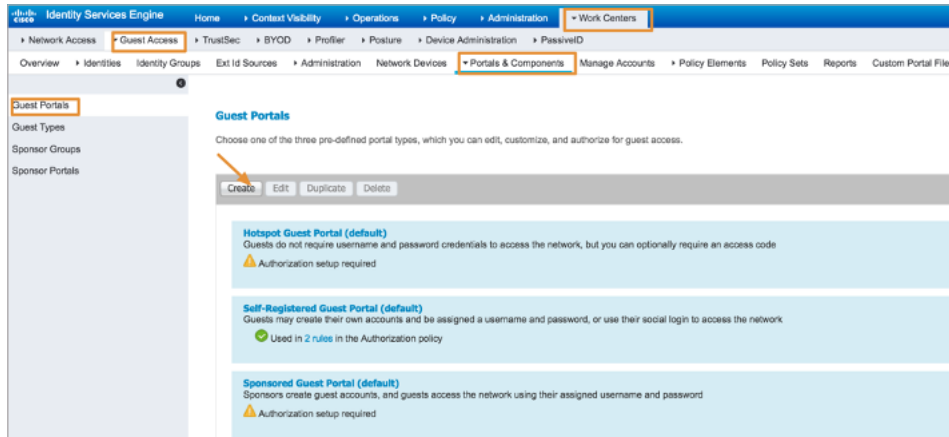
Configure SMS service provider at: [Work Centers > Guest Access > Administration > SMS Gateway Providers](#)

These sponsor groups can create this guest type:

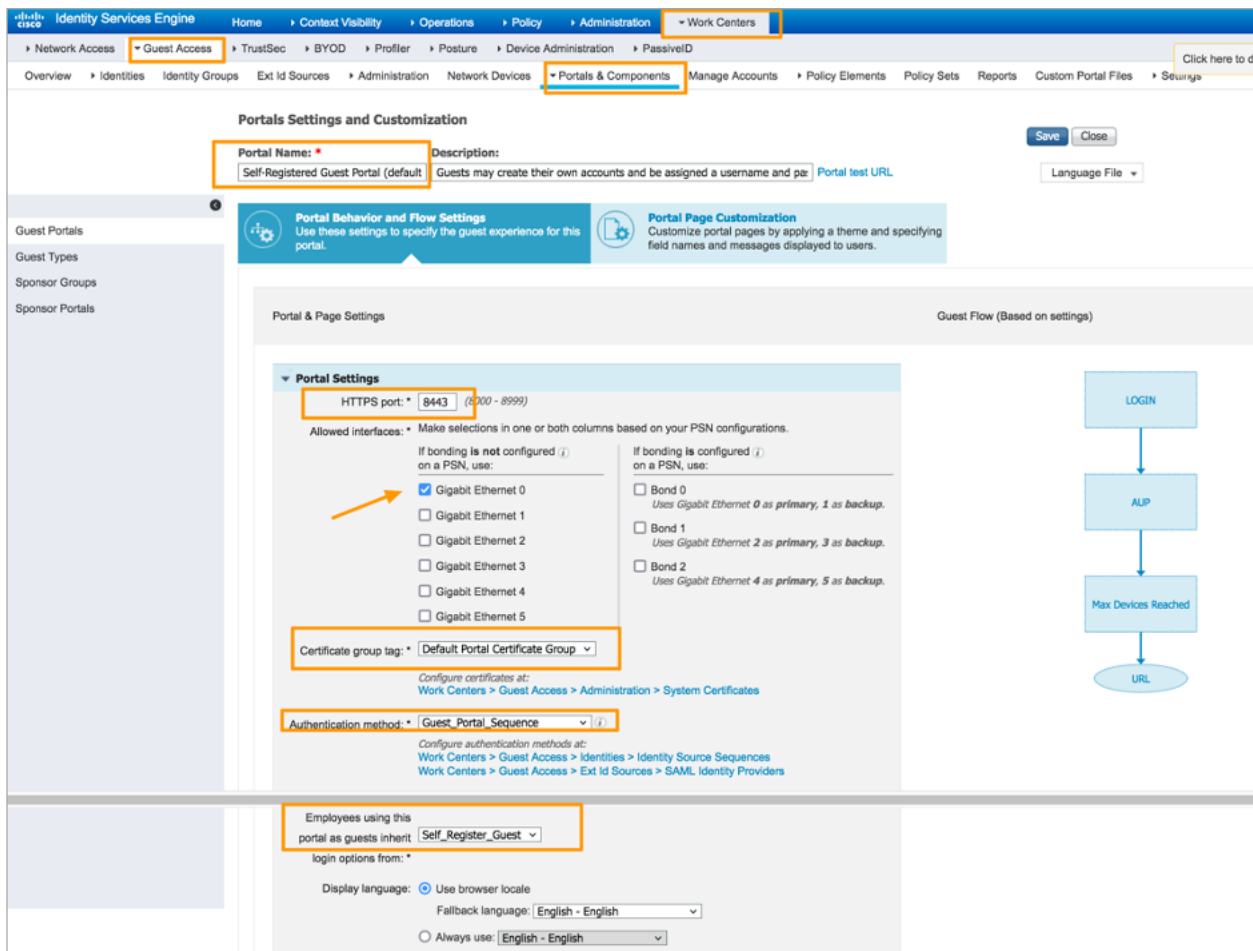
Sponsor Groups: **ALL\_ACCOUNTS (default)** **GROUP\_ACCOUNTS (default)** **OWN\_ACCOUNTS (default)**

## Create Self-Registered Guest Portal

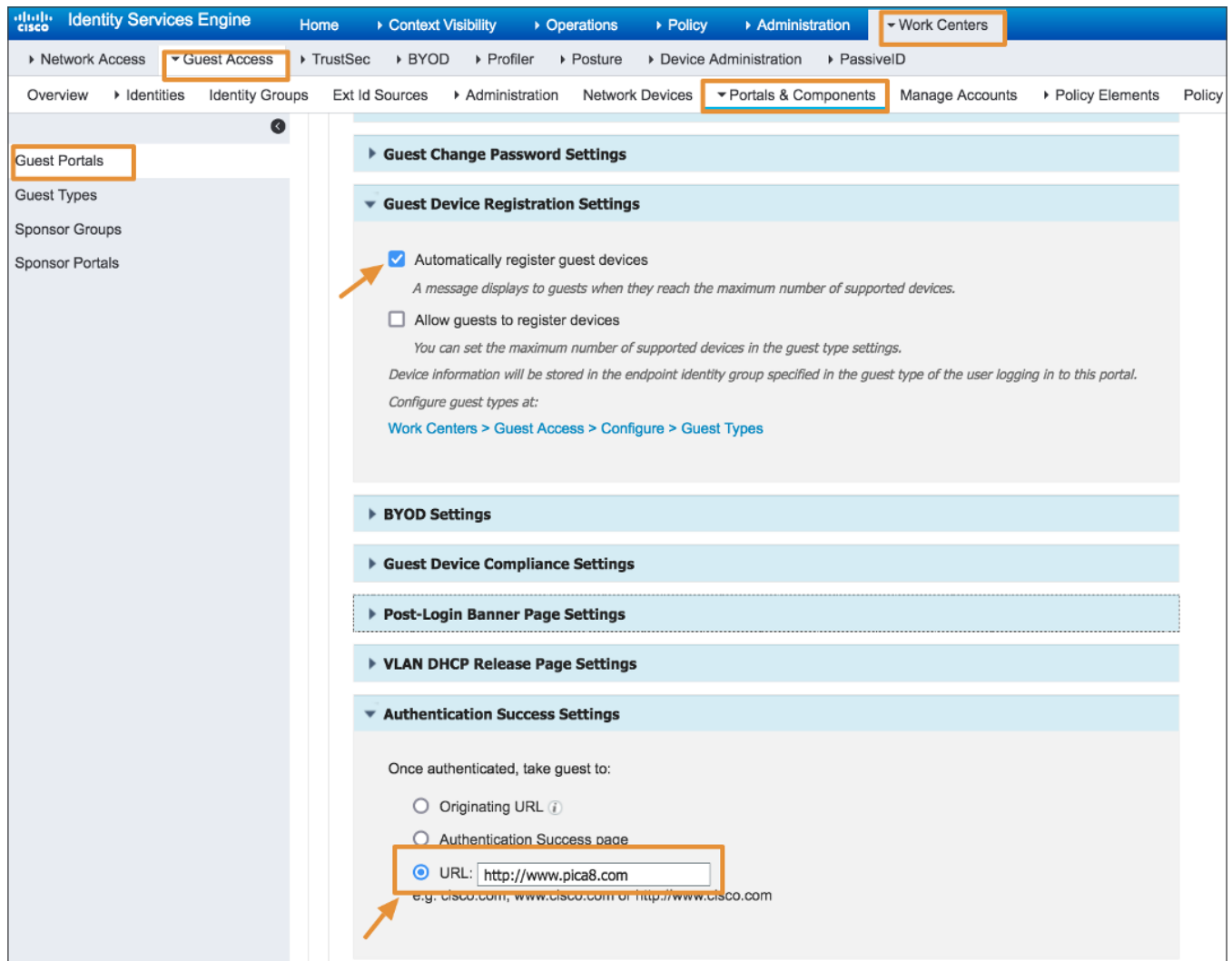
To create the Guest Portal, navigate to **Work Centers** -> **Guest Access** -> **Portals & Components** -> **Guest Portals** and click **Create** as shown below.



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.

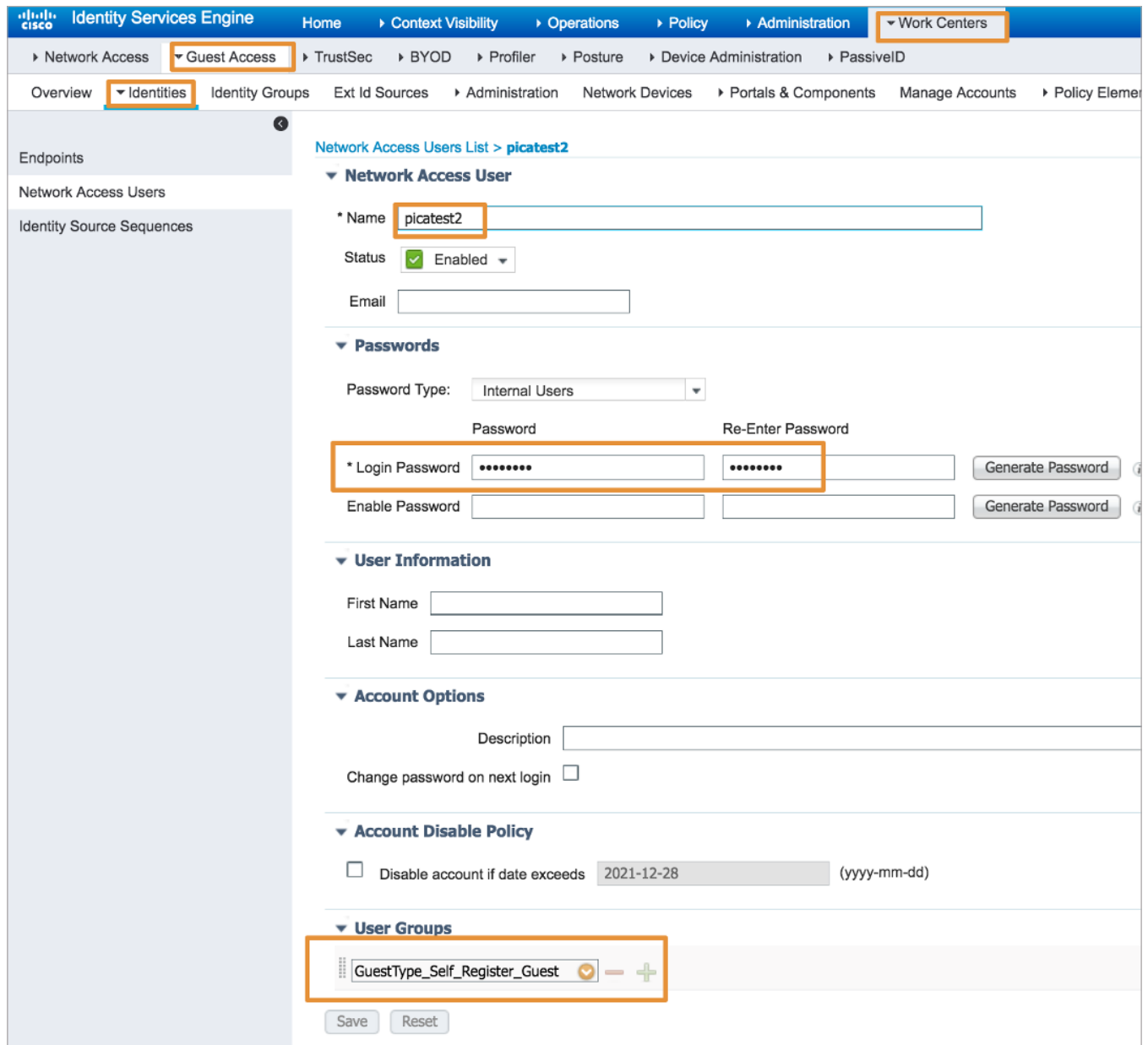


The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The top navigation bar includes tabs for Home, Context Visibility, Operations, Policy, Administration, and Work Centers. The left sidebar shows the configuration tree with 'Guest Access' expanded, and 'Guest Portals' selected. The main content area displays the 'Guest Device Registration Settings' for a specific portal. The settings include:

- Guest Change Password Settings**
- Guest Device Registration Settings**
  - ☒ Automatically register guest devices. A message displays to guests when they reach the maximum number of supported devices.
  - ☐ Allow guests to register devices. You can set the maximum number of supported devices in the guest type settings. Device information will be stored in the endpoint identity group specified in the guest type of the user logging in to this portal. Configure guest types at: [Work Centers > Guest Access > Configure > Guest Types](#)
- BYOD Settings**
- Guest Device Compliance Settings**
- Post-Login Banner Page Settings**
- VLAN DHCP Release Page Settings**
- Authentication Success Settings**
  - Once authenticated, take guest to:
    - ☐ Originating URL
    - ☐ Authentication Success page
    - ☒ URL:  (e.g. cisco.com, www.cisco.com or http://www.cisco.com)

### 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.



**Identity Services Engine**

Home > Context Visibility > Operations > Policy > Administration > **Work Centers**

Network Access > **Guest Access** > TrustSec > BYOD > Profiler > Posture > Device Administration > PassiveID

Overview > **Identities** > Identity Groups > Ext Id Sources > Administration > Network Devices > Portals & Components > Manage Accounts > Policy Elements

Endpoints

Network Access Users

Identity Source Sequences

**Network Access Users List > picatest2**

**Network Access User**

\* Name:

Status: ☒ Enabled

Email:

**Passwords**

Password Type:

Password:  Re-Enter Password:

\* Login Password:

Enable Password:

**User Information**

First Name:

Last Name:

**Account Options**

Description:

Change password on next login: ☐

**Account Disable Policy**

☐ Disable account if date exceeds:  (yyyy-mm-dd)

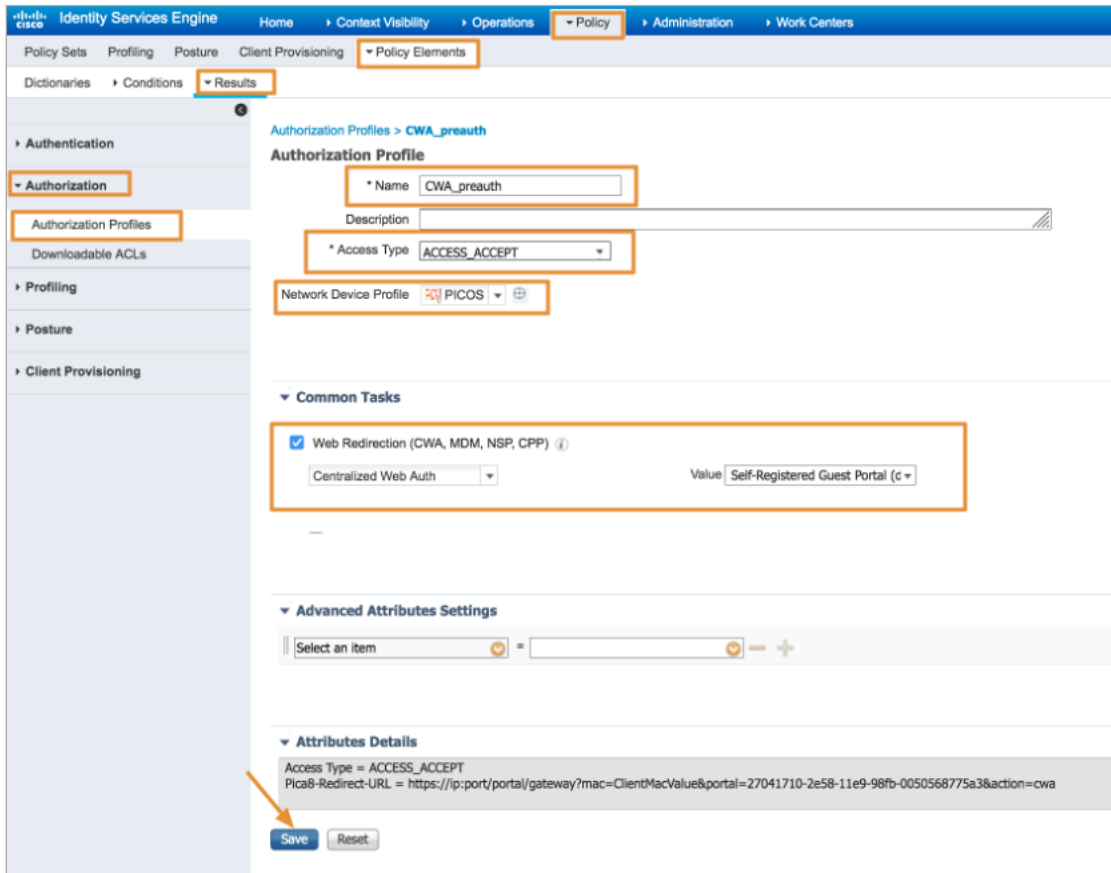
**User Groups**

### 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.

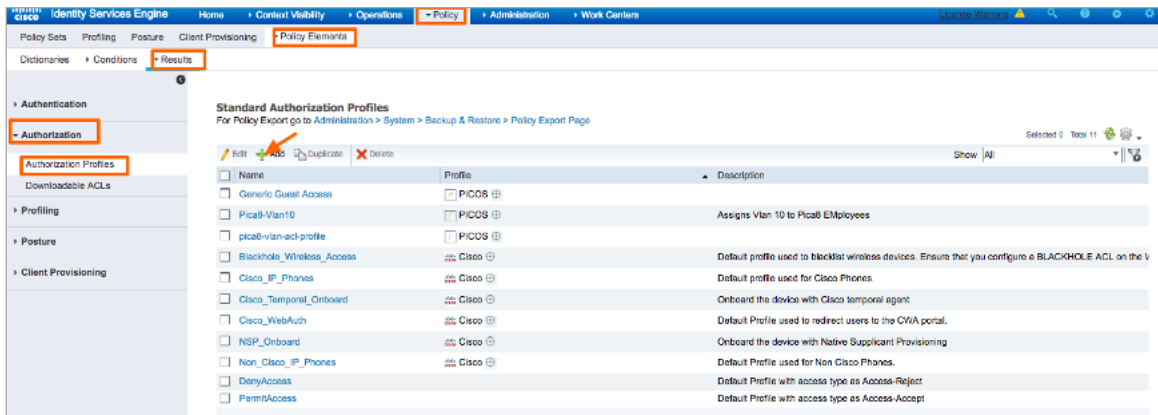
Enter **Name** as **CWA\_preauth**, **Description**, set **Access Type** to **ACCESS\_ACCEPT**, set **Network Device Profile** to **PicOS** as shown below. Check the box for **Web Redirection** and select **Centralized Web Auth** with value **Self-Registered Guest Portal** as shown below. Then click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





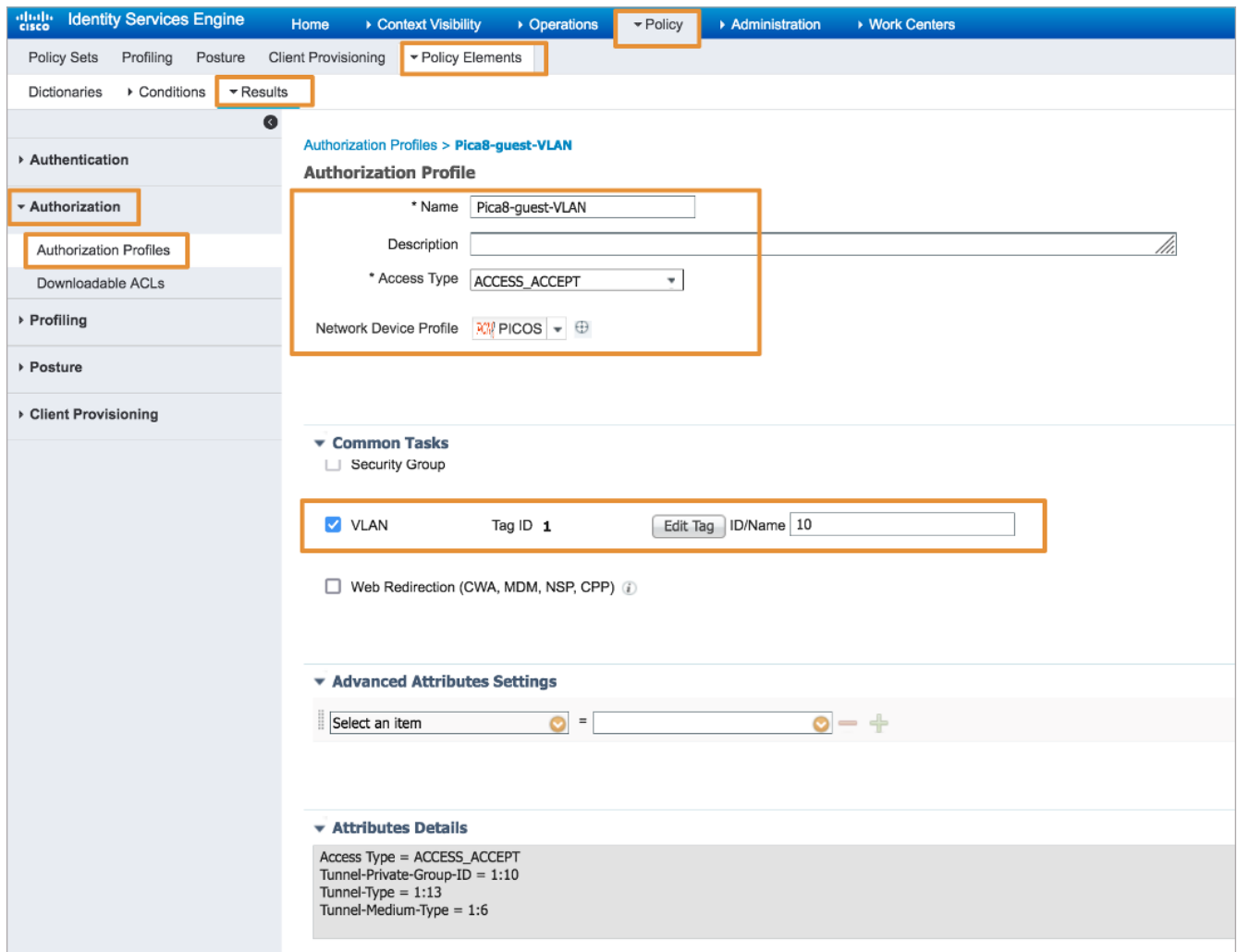
## Creating an Authorization Profile to Dynamically Assign VLAN for Guest Laptops

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



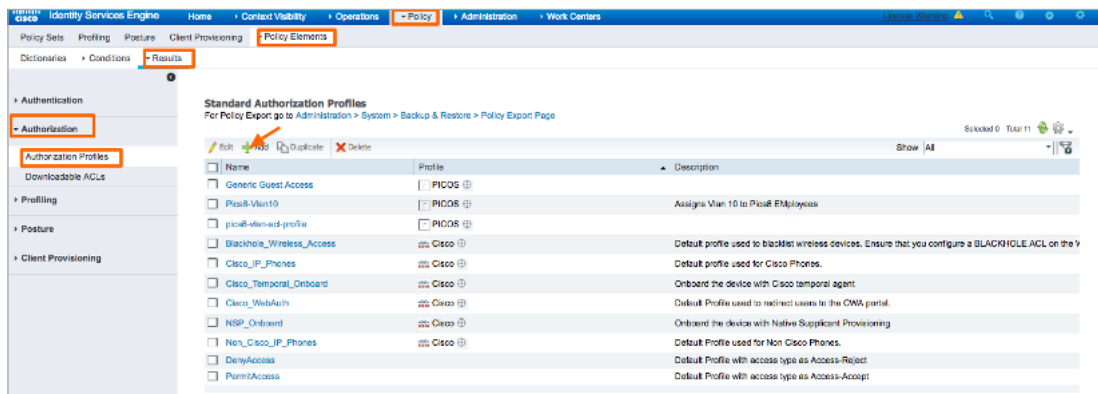
Name	Profile	Description
Generic Guest Access	PICOS	
Pica8-Vlan10	PICOS	Assigns Vlan 10 to Pica8 Employees
pica8-vlan-acl-profile	PICOS	
Blackhole_Wireless_Access	Cisco	Default profile used to blacklist wireless devices. Ensure that you configure a BLACKHOLE ACL on the V
Cisco_IP_Phones	Cisco	Default profile used for Cisco Phones
Cisco_Temporal_Onboard	Cisco	Onboard the device with Cisco temporal agent
Cisco_WebAuth	Cisco	Default Profile used to redirect users to the CWA portal.
NSP_Onboard	Cisco	Onboard the device with Native Supplicant Provisioning
Non_Cisco_IP_Phones	Cisco	Default Profile used for Non Cisco Phones.
DenyAccess		Default Profile with access type as Access-Reject
PermitAccess		Default Profile with access type as Access-Accept

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.



Name	Profile	Description
Generic Guest Access	PICO8	
Pica8-Vlan10	PICO8	Assigns Vlan 10 to Pico8 Employees
pica8-vlan-ed-profile	PICO8	
Blackhole_Wireless_Access	Cisco	Default profile used to blacklist wireless devices. Ensure that you configure a BLACKHOLE ACL on the y
Cisco_IP_Phones	Cisco	Default profile used for Cisco Phones.
Cisco_Temporal_Onboard	Cisco	Onboard the device with Cisco temporal agent.
Cisco_WebAuth	Cisco	Default Profile used to redirect users to the CWA portal.
NSP_Onboard	Cisco	Onboard the device with Native Supplicant Provisioning
Non_Cisco_IP_Phones	Cisco	Default Profile used for Non Cisco Phones.
DenyAccess		Default Profile with access type as Access-Reject
PermAccess		Default Profile with access type as Access-Accept



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**.

The screenshot shows the Cisco Identity Services Engine (ISE) Policy configuration page. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The left sidebar shows the navigation menu with 'Policy Elements' selected. Under 'Policy Elements', 'Results' is selected. The main content area shows the 'Authorization Profiles > Pica8-Guest-ACL' configuration. The 'Authorization Profile' section has the following fields: Name (Pica8-Guest-ACL), Description (empty), Access Type (ACCESS\_ACCEPT), and Network Device Profile (PICOS). Below this, the 'Common Tasks' section has a checkbox for 'ACL (Filter-ID)' which is checked, and the value 'mac\_auth\_policy\_1' is entered. The 'Advanced Attributes Settings' section shows a dropdown for 'Select an Item' with an equals sign and a plus sign. The 'Attributes Details' section shows 'Access Type = ACCESS\_ACCEPT' and 'Filter-ID = mac\_auth\_policy\_1'.

### 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.

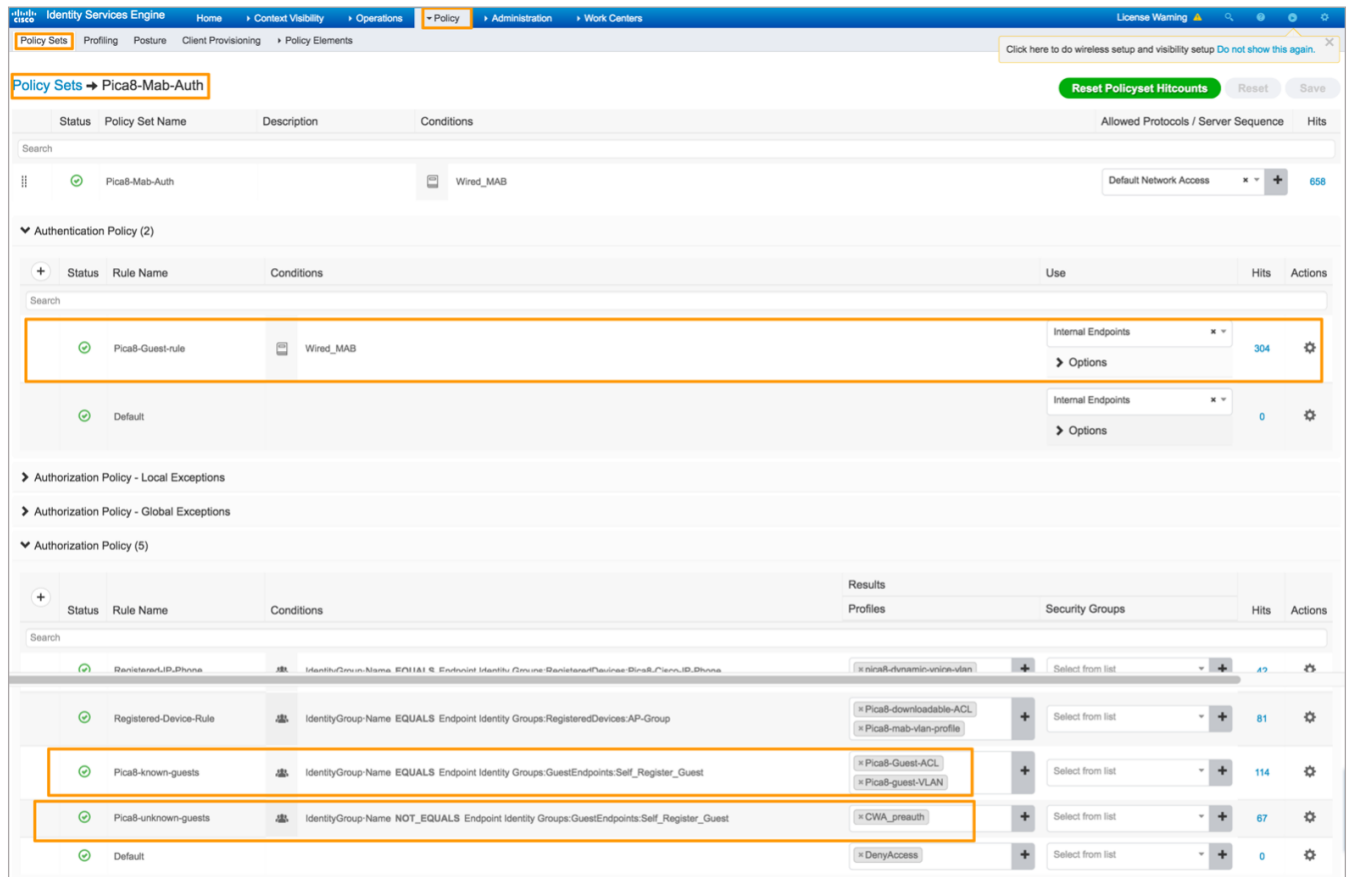
The screenshot shows the Cisco Identity Services Engine (ISE) Policy Sets configuration page. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The left sidebar shows the navigation menu with 'Policy Sets' selected. The main content area shows a table of Policy Sets. The table has columns: Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, Hits, Actions, and View. The table contains two rows: Pica8-Mab-Auth and Pica8-Employee. The Pica8-Mab-Auth row is highlighted. The 'Allowed Protocols / Server Sequence' column shows 'Default Network Access' with a plus sign and a minus sign. The 'Hits' column shows '571'. The 'Actions' column shows a gear icon and a right arrow icon. The 'View' column shows a right arrow icon.

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	Pica8-Mab-Auth		Wired_MAB	Default Network Access	571	⚙️ ➡️	➡️
✓	Pica8-Employee		Wired_802.1X	Default Network Access	31	⚙️ ➡️	➡️

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**.



The screenshot shows the Cisco Identity Services Engine (ISE) Policy configuration page. The 'Policy Sets' configuration for 'Pica8-Mab-Auth' is displayed. The page includes a table of policy sets and a detailed view of the 'Authentication Policy (2)' and 'Authorization Policy (5)'. The 'Pica8-Guest-rule' and 'Pica8-known-guests' rules are highlighted with orange boxes.

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Pica8-Mab-Auth		Wired_MAB	Default Network Access	668

**Authentication Policy (2)**

Status	Rule Name	Conditions	Use	Hits	Actions
✓	Pica8-Guest-rule	Wired_MAB	Internal Endpoints	304	Options
✓	Default		Internal Endpoints	0	Options

**Authorization Policy (5)**

Status	Rule Name	Conditions	Results	Security Groups	Hits	Actions
✓	Registered-Device-Rule	IdentityGroup-Name EQUALS Endpoint Identity Groups:RegisteredDevices:AP-Group	Pica8-downloadable-ACL Pica8-mab-vlan-profile	Select from list	81	Options
✓	Pica8-known-guests	IdentityGroup-Name EQUALS Endpoint Identity Groups:GuestEndpoints:Self_Register_Guest	Pica8-Guest-ACL Pica8-guest-VLAN	Select from list	114	Options
✓	Pica8-unknown-guests	IdentityGroup-Name NOT_EQUALS Endpoint Identity Groups:GuestEndpoints:Self_Register_Guest	CWA_preauth	Select from list	67	Options
✓	Default		DenyAccess	Select from list	0	Options

## 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.

Identity Services Engine										
<a href="#">Home</a> <a href="#">Context Visibility</a> <a href="#">Operations</a> <a href="#">Policy</a> <a href="#">Administration</a> <a href="#">Work Centers</a>										
<a href="#">RADIUS</a> <a href="#">Threat-Centric NAC Live Logs</a> <a href="#">TACACS</a> <a href="#">Troubleshoot</a> <a href="#">Adaptive Network Control</a> <a href="#">Reports</a>										
<a href="#">Live Logs</a> <a href="#">Live Sessions</a>										
<div> Misconfigured Supplicants 0 Misconfigured Network Devices 0 RADIUS Drops 4749 Client Stopped Responding 0 Repeat Counter 0 </div>										
Refresh Reset Repeat Counts Export To										
Time	Status	Details	Repeat ...	Identity	Endpoint ID	Authentication Policy	Authorization Policy	Authorization Prof...	Identity Group	Post
Nov 04, 2021 04:05:43...			0	00:80:8E:8A:92:76	00:80:8E:8A...	Pica8-Mab-Auth >> Pica8-Guest-rule	Pica8-Mab-Auth >> Pica8-unknown-guests	CWA_preauth		
Nov 04, 2021 04:05:43...				00:80:8E:8A:92:76	00:80:8E:8A...	Pica8-Mab-Auth >> Pica8-Guest-rule	Pica8-Mab-Auth >> Pica8-unknown-guests	CWA_preauth		

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.

Identity Services Engine

Overview

Event

5200 Authentication succeeded

Username

00:80:8E:8A:92:76

Endpoint Id

00:80:8E:8A:92:76

Endpoint Profile

Authentication Policy

Pica8-Mab-Auth >> Pica8-Guest-rule

Authorization Policy

Pica8-Mab-Auth >> Pica8-unknown-guests

Authorization Result

CWA\_preauth

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

ise-26-105.pica8.com

Guest Portal

Welcome

Sign on for guest access.

Username:

Password:

Sign On



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.

Time	Status	Details	Repeat	Identity	Endpoint ID	Authentication Policy	Authorization Policy	Authorization Profiles	Identity Group	Policy
Nov 04, 2021 04:10:30...	Success	Details icon	0	pica8test2	00:80:8e:8a:92:76	Pica8-Mab-Auth >> Pica8-Guest-rule	Pica8-Mab-Auth >> Pica8-known-guests	Pica8-Guest-ACL,Pica8-guest-VLAN		
Nov 04, 2021 04:10:30...	Success	Details icon	0	pica8test2	00:80:8e:8a:92:76	Pica8-Mab-Auth >> Pica8-Guest-rule	Pica8-Mab-Auth >> Pica8-known-guests	Pica8-Guest-ACL,Pica8-guest-VLAN		GuestEndpoints:Self_F

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.

Cisco
Identity Services Engine

### Overview

Event	5200 Authentication succeeded
Username	picatest2
Endpoint Id	00:80:8E:8A:92:76
Endpoint Profile	Unknown
Authentication Policy	Pica8-Mab-Auth >> Pica8-Guest-rule
Authorization Policy	Pica8-Mab-Auth >> Pica8-known-guests
Authorization Result	Pica8-Guest-ACL,Pica8-guest-VLAN

### Authentication Details

Source Timestamp	2021-11-04 16:10:30.2
Received Timestamp	2021-11-04 16:10:30.2
Policy Server	ISE-26-105
Event	5200 Authentication succeeded
Username	picatest2
User Type	Host
Endpoint Id	00:80:8E:8A:92:76
Calling Station Id	00-80-8E-8A-92-76
Endpoint Profile	Unknown
Authentication Identity Store	Internal Endpoints

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](http://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