



Pica8 Deployment Guide

PicOS[®] NAC Integration with Aruba ClearPass Policy Manager

Contents

Aruba ClearPass Policy Manager NAC Solution	1
PicOS Network Access Control – Secured Wired Access Solution	1
Solution Overview and Topology	1
Aruba ClearPass NAC Solution	3
Install ClearPass Server and Setup System Configuration	3
Deploying an Aruba ClearPass Policy Manager	4
Requirements	4
Integrating PicOS with ClearPass Policy Manager for Radius Authentication	5
Configuring the PicOS Switch	5
Configuring the ClearPass Policy Manager	6
Import PicOS RADIUS Dictionary	6
Add a PicOS Network Device and Group	7
Add a Test User	8
Employee Laptop Authentication	9
Configure the 802.1x Wired Access Policy for Employee Laptop	9
Configure Dynamic VLAN Enforcement Profile	9
Configure Downloadable ACL Enforcement Profile	10
Create an Enforcement Policy to Assign Dynamic VLAN and DACL	11
Create a Service for Employee 802.1X Authentication	12
Configuring the Windows Supplciant on the Laptop	16
Verify the NAC Configuration	17
IP Phone Authentication	19
Configuring the MAB Wired Access Policy in ClearPass Policy Manager for IP Phones	19
Creating Static Host Lists for IP Phones and Adding IP Phone’s MAC Address to the Static Host Lists Table	19
Configure Dynamic VLAN Enforcement Profile for IP Phone	20
Create an Enforcement Policy to Assign Dynamic Voice VLAN and ACL to the IP Phones Device Group	21
Create a Service for MAB Authentication of IP Phone Devices	22
Verifying the NAC Configuration	24
Multi-host Authentication	25
IoT Device Authentication	25
Configuring the MAB Wired Access Policy in ClearPass Policy Manager for an IoT Device	25
Creating Static Host Lists for IoT Devices and Add IoT Device’s MAC Address to the Static Host Lists Table	25
Configure Dynamic VLAN Enforcement Profile	26
Configure Dynamic ACL Enforcement Profile	27
Create an Enforcement Policy to Assign Dynamic VLAN and ACL	28
Create a Service for MAB Authentication of IoT Device	30
Verifying the NAC Configuration	31

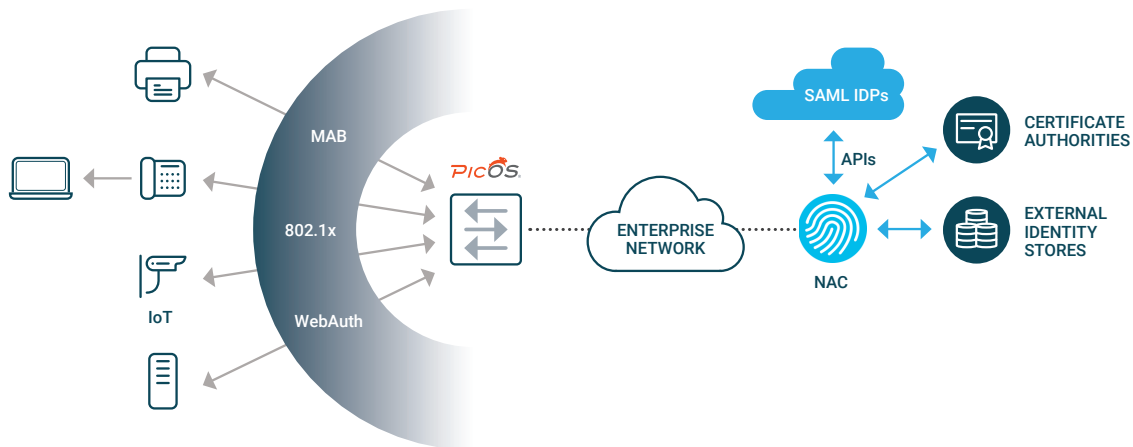
Contents – cont'd

Guest Laptop Using MAB and Central Web Authentication	32
Configuring the PicOS Switch	32
Configuring Aruba ClearPass Guest Portal	33
Set up the Guest User Account	33
Configure the Guest Access Login Page	34
Configure the ClearPass Policy Manager	35
Verifying the NAC Configuration	43
Troubleshooting	48
Check Whether the ClearPass Server is Reachable from the PicOS Switch	48
Check the NAC Authentication Status of all Ports	48
Check the NAC Configuration	48
Check VLANs to Verify Dynamic VLANs Assignment to a Port	49
Check Dynamic ACL Rules	50
Check Downloadable ACL Rules	51
Check Trace Logs for Radius	51
Reference	52
PicOS	52
ClearPass	52



Aruba ClearPass Policy Manager NAC Solution

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



ClearPass authenticates users and endpoints via 802.1x, Web Authentication, Mac Authentication Bypass (MAB), and other means.

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.

Solution Overview and Topology

Secured Wired Access solution consists of authenticating the following use cases:

1. User Based Authentication: Employee laptops will have 802.1x supplicant. We will use 802.1x authentication for Employees.

2. Device Based Authentication: We will use MAB (MAC Address Bypass) Authentication for authenticating devices. Following example use cases for authenticating devices are covered in this document.

- a. Group of IP Phones
- b. Group of IoT Devices
- c. Contractor laptops which are not running 802.1x supplicant. Details on logic for this device is given in Guest Laptop using MAB and Central Web Authentication section

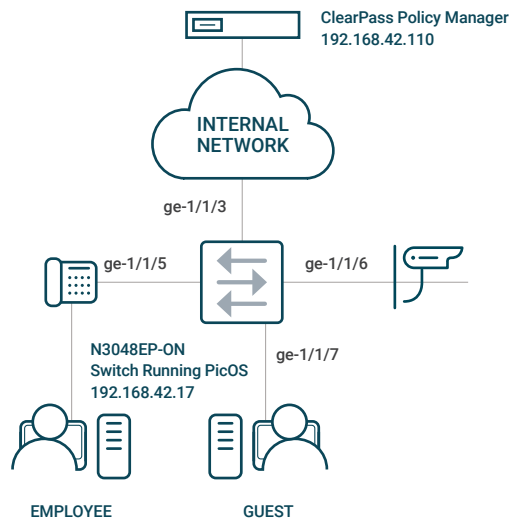
3. Multi-host Authentication: This case includes more than one device connected to a switch port. Following is one of the example use cases: Employee laptop connected behind an IP Phone and IP Phone is connected to the switch.

RADIUS server is configured with the following Secured Access Policies. Once the user or device is authenticated using RADIUS server, the following secured access techniques are assigned to the port as per Policy settings in RADIUS server.

- 1. Dynamic VLAN
- 2. Either Dynamic or Downloadable ACL

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 DACL (Downloadable ACL) policies will be applied to the port where the employee laptop is connected. The employee laptop connected behind a Cisco IP Phone is connected to port ge-1/1/5.
- 2. Registered 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 IoT device: An IoT device 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 MAB and 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.





Aruba ClearPass NAC Solution

This document provides details on how to install, integrate and test the Aruba ClearPass NAC solution with PicOS switches.

Install ClearPass Server and Setup System Configuration

The following steps will install ClearPass Radius Server and setup the system configuration:

1. Install VM: Install Virtual Appliance. Follow the section “Using VMware vSphere Web Client to Install ClearPass on a Virtual Machine” in 6.8 ClearPass Getting Started Guide.
2. Log in: Login with following credentials: appadmin/eTIPS123. This initiates the Policy Manager Configuration wizard.
3. Configure the ClearPass hardware appliance: Follow the prompts, replacing the placeholder entries in the following:

- Hostname
- Management Port IP Address
- Management Port Subnet Mask
- Management Port Gateway
- Data Port IP Address
- Data Port Subnet Mask

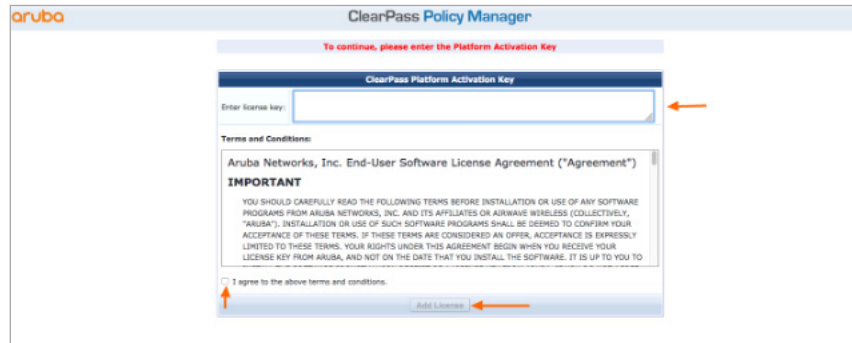
- Data Port Gateway
- Primary DNS
- Secondary DNS

```
=====
                        Configuration Summary
=====
Hostname                : ClearPassNac100
Management Port IP Address : 192.168.42.101
Management Port Subnet Mask : 255.255.255.0
Management Port Gateway   : 192.168.42.1
Data Port IP Address       : <not configured>
Data Port Subnet Mask      : <not configured>
Data Port Gateway         : <not configured>
Primary DNS                : 192.168.42.71
Secondary DNS              : 8.8.8.8
System Date               : 2019-10-22
System Time               : 15:45:00
Timezone                  : 'America/Los_Angeles'
FIPS Mode                 : False
=====

Proceed with the configuration [y[Y]/n[N]/q[Q]]
    y[Y] to continue
    n[N] to start over again
    q[Q] to quit

Enter the choice: _
```

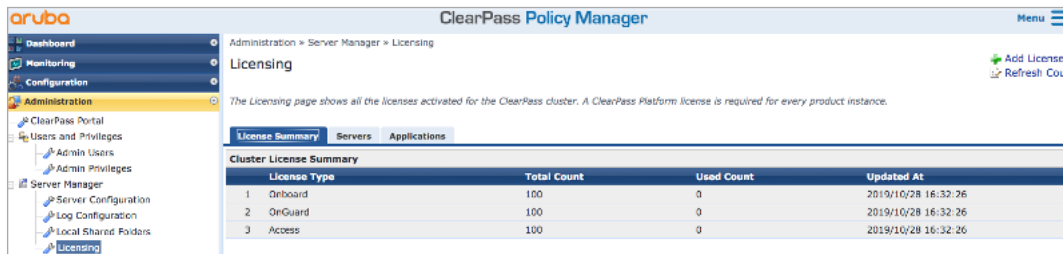
4. **Configure the system date and time and apply the configuration.**
Follow the prompts to configure the system date and time. Press **Y** to apply the configuration.
5. **Activating ClearPass License:** To activate ClearPass Policy Manager and apply the ClearPass license, go to the following <https://x.x.x.x/tips/>, where **x.x.x.x** is the IP address of the management interface defined for the ClearPass server. Click on the *Policy Manager* tab.
Make sure the **I agree to the above terms and conditions** checkbox is enabled. Enter license key text box, enter your ClearPass license key and click Add License.



Upon successfully entering the license key, the **Admin Login** screen appears with a message indicating that you have 90 days to activate the product and a link to activate the product.

Click **Online Activation -> Activate Now** to activate the license over the Internet with Aruba License Activation servers.

Click **Administration->Server Manager->Licensing** to make sure you have the following type of licenses installed and activated: Onboard, OnGuard and Access. These Licenses are needed for adding a **service** functionality.



Deploying an Aruba ClearPass Policy Manager

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)
- ClearPass appliance running release 6.8 (or later)
- An employee laptop running Microsoft Windows 7 Enterprise



- A guest laptop running Mac OS
- A Cisco IP Phone
- An Aruba Access Point

Integrating PicOS with ClearPass Policy Manager for Radius Authentication

The following sections go over PicOS and ClearPass Policy Manager 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 192.168.42.110 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 192.168.42.110 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 192.168.42.110 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"
```

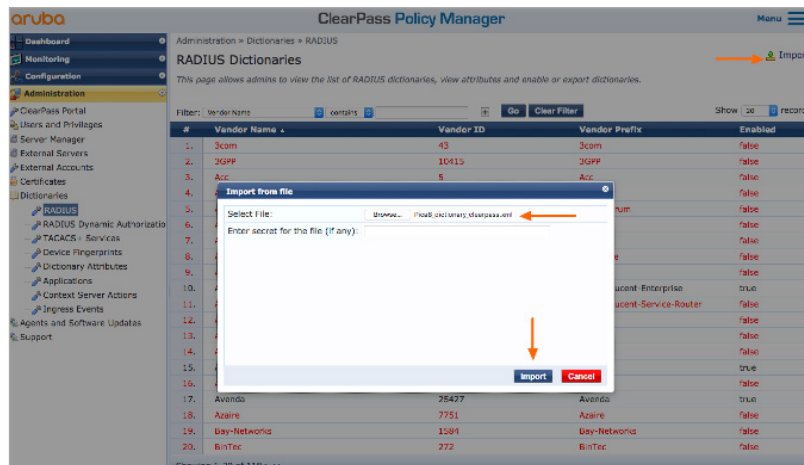
Configuring the ClearPass Policy Manager

The following three configuration steps are needed to configure the ClearPass Policy Manager for RADIUS Authentication.

1. Import PicOS RADIUS Dictionary
2. Add PicOS Network Device and Group
3. Add a Test User

Import PicOS RADIUS Dictionary

Navigate to **Administration -> Dictionaries -> RADIUS** and import **Pica8 RADIUS Dictionary** as shown below.



To verify **Pica8 RADIUS dictionary** is imported successfully, enter **Pica8** in contains field and click **Go** as shown below.



Add a PicOS Network Device and Group

The following are configuration steps using the ClearPass UI:

Click on **Configuration->Network->Devices->Add**. Fill out device name, IP address, vendor name and Radius secret key and click **Add** to save the settings to ClearPass database as shown below.

Verify PicOS switch reachability to the RADIUS server with the following CLI command:

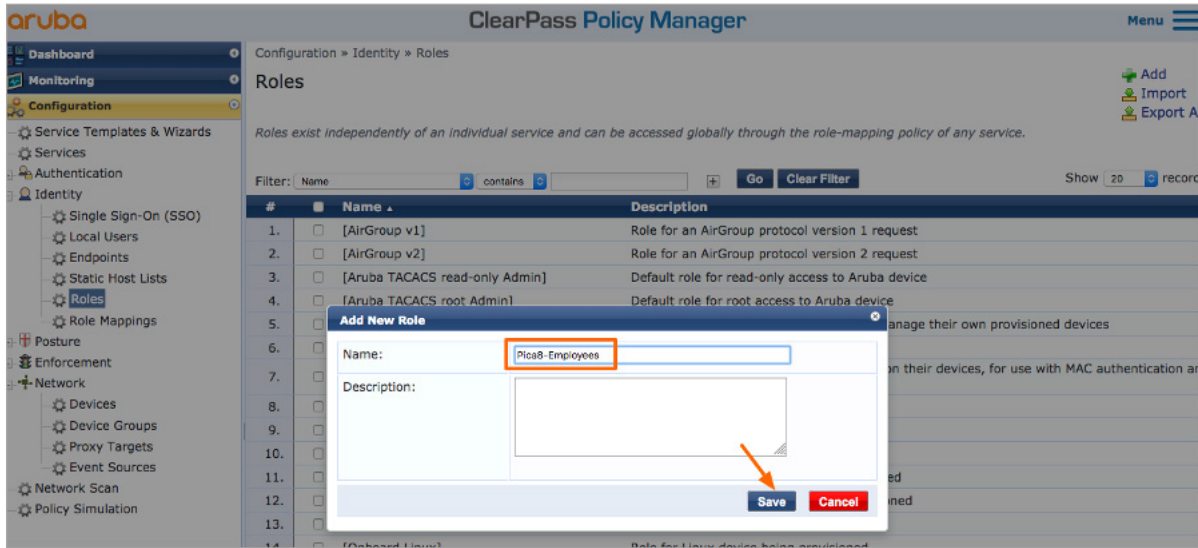
```
admin@P8-Access-BR-1-SW-2> show dot1x server
Server-IP          Status          Priority  Retry-Interval  Retry-Num  Detect-Interval  Consecutive-
-----          -
Detect-Num
-----
-----
192.168.42.110    active          ...      3 Sec(s)        3          5 Sec(s)        3
```

Add a new device group called **PICOS-Switches** by clicking on **Configuration->Network->Device Groups->Add**. Add the device you created in the previous step as shown below and click **Save**.

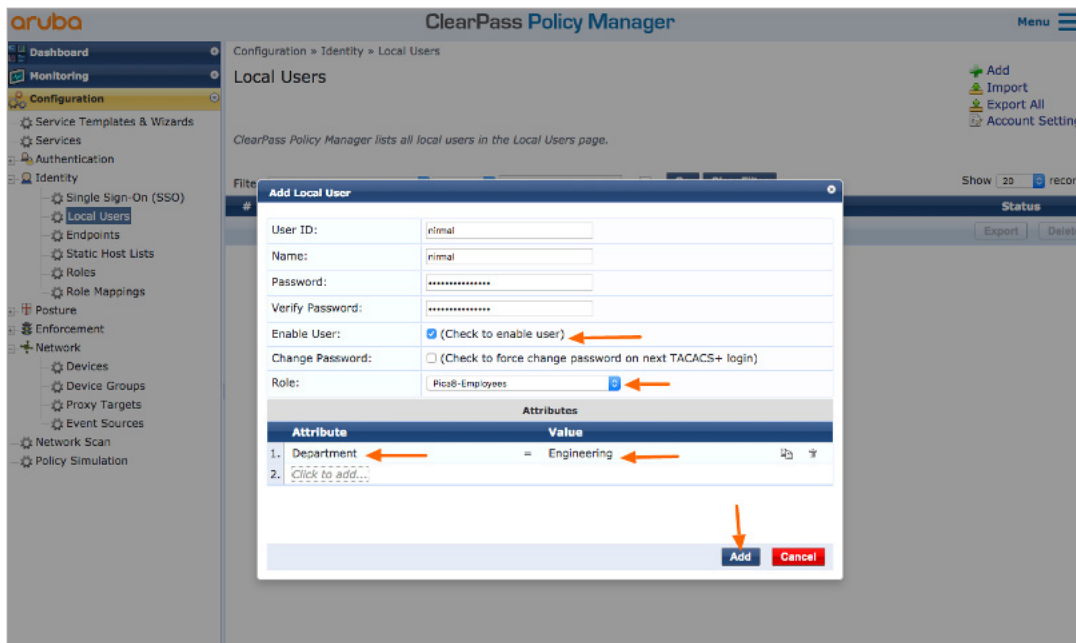
Add a Test User

You can integrate your Active Directory with ClearPass. For testing purpose we will add a local Test User in the ClearPass Policy Manager as follows:

Add a role to ClearPass by clicking on the **Configuration->Identity->Roles->Add** menu as shown below, enter the new role name and click **Save**.



To add a new user, click on **Configuration->Identity->Local Users**, select the role Pica8-Employees, enter name of the department as shown below and then click **Add**.



Employee Laptop Authentication

In this example configuration, the ClearPass Policy Manager 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, ClearPass Policy Manager returns the VLAN ID 10 to the switch in a RADIUS attribute. ClearPass Policy Manager also returns the Pica8-Downloadable-ACL ACL for employees. The switch then dynamically configures the laptop to be in VLAN 10 with Pica8-Downloadable-ACL. The Cisco IP Phone is connected to port ge-1/1/5 and the employee laptop with 802.1x supplicant is connected behind the Cisco IP Phone.

This use case involves configuring the ClearPass Policy Manager, configuring the windows supplicant on the laptop, and then verifying the NAC configuration.

Configure the 802.1x Wired Access Policy for Employee Laptop

Configuring and testing the 802.1x Wired Access policy in ClearPass Policy manager for the Employee laptop involves the following five steps:

1. Configure Dynamic VLAN enforcement profile
2. Configure Downloadable ACL (DACL) enforcement profile
3. Create an enforcement policy to assign dynamic VLAN and DACL to the employee laptop after 802.1x authentication.
4. Create a Service for Employee 802.1X Authentication
5. Create a Wired Access policy for Employee Laptop running 802.1x supplicant (called Pica8-Employee) that will use the above two authorization profiles

Configure Dynamic VLAN Enforcement Profile

This profile defines the RADIUS attributes for specifying VLAN 10. These RADIUS attributes are sent to the switch when a user who belongs to the Engineering department authenticates using 802.1X, enabling the switch to dynamically assign VLAN 10 to the access port.

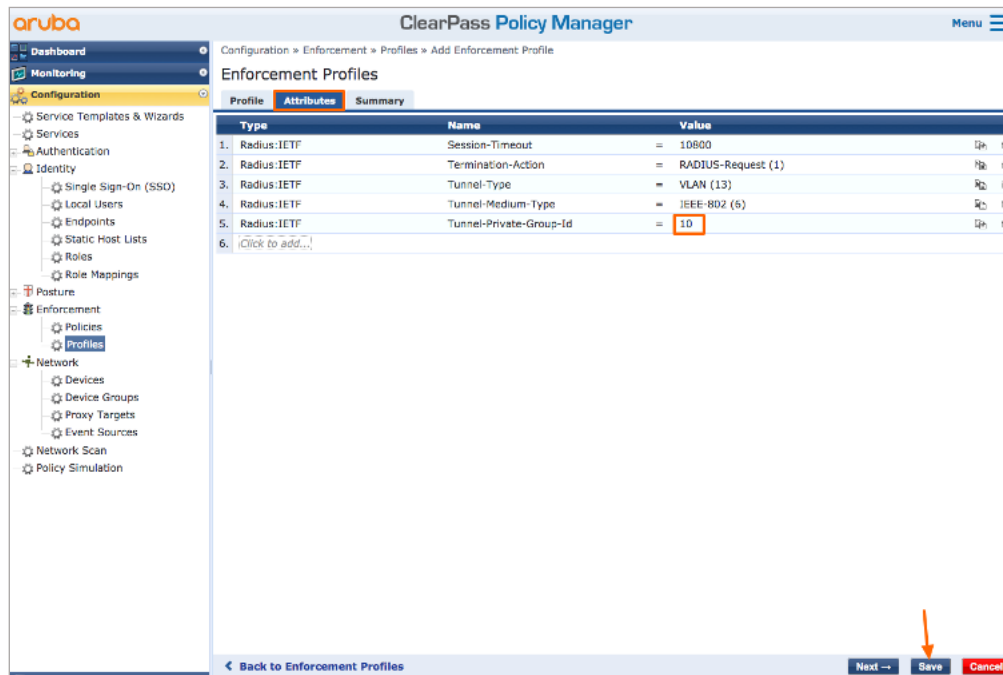
To add an enforcement profile, click on **Configuration->Enforcement->Profiles->Add** to add a new enforcement profile. On the Profile tab, choose **VLAN Enforcement** template, enter the VLAN name and select a Pica8-Switches device group as shown below and click **Next**.

The screenshot shows the Aruba ClearPass Policy Manager web interface. The breadcrumb navigation is Configuration » Enforcement » Profiles » Add Enforcement Profile. The main heading is 'Enforcement Profiles'. The 'Profile' tab is active, showing the following configuration fields:

- Template: VLAN Enforcement
- Name: 802.1X-VLAN
- Description: 802.1X VLAN
- Type: RADIUS
- Action: Accept Reject Drop
- Device Group List: Pica8-Switches

Buttons for 'Remove', 'View Details', and 'Modify' are visible next to the Device Group List. The left sidebar shows the navigation tree with 'Profiles' highlighted under 'Enforcement'.

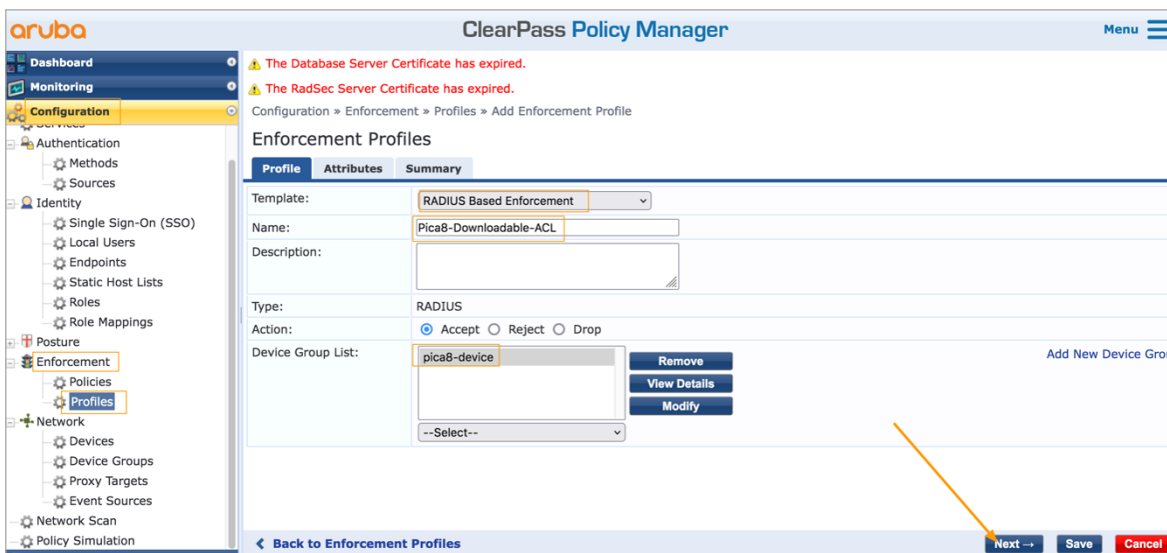
On the **Attributes** tab, fill the VLAN number you want to dynamically assign as shown below and click **Save**.



Configure Downloadable ACL Enforcement Profile

This profile defines the RADIUS attributes for specifying a downloadable ACL called Pica8-Downloadable-ACL. These RADIUS attributes are sent to the switch when a user who belongs to the Engineering department authenticates using 802.1X, enabling the switch to download Pica8-Downloadable-ACL to the access port.

To add a enforcement profile, click on **Configuration->Enforcement->Profiles->Add** to add a new enforcement profile. On the Profile tab, choose **Radius Based Enforcement** template, enter the Download ACL name and select a **Pica8-Switches** device group as shown below and click **Next**.



On the **Attributes** tab fill the Downloadable ACL you want to download to the access port as shown below and click **Save**.

Configuration » Enforcement » Profiles » Edit Enforcement Profile - Pica8-Downloadable-ACL

Enforcement Profiles - Pica8-Downloadable-ACL

Summary Profile **Attributes**

Type	Name	Value
1. Radius:Pica8	Pica8-IP-Downloadable-ACL-Name	= Pica8-Downloadable-ACL
2. Radius:Pica8	Pica8-IP-Downloadable-ACL-Rule	= seq 10 from destination-address-ipv4 192.168.42.71/32 then action forward
3. Radius:Pica8	Pica8-IP-Downloadable-ACL-Rule	= seq 20 from destination-address-ipv4 192.168.42.1/32 then action forward
4. Radius:Pica8	Pica8-IP-Downloadable-ACL-Rule	= seq 30 from destination-address-ipv4 192.168.42.110/32 then action forward
5. Radius:Pica8	Pica8-IP-Downloadable-ACL-Rule	= seq 40 from destination-address-ipv4 192.168.42.94/32 then action forward
6. Radius:Pica8	Pica8-IP-Downloadable-ACL-Rule	= seq 50 from destination-address-ipv4 192.168.42.108/32 then action forward
7. Radius:Pica8	Pica8-IP-Downloadable-ACL-Rule	= seq 60 from destination-address-ipv4 192.168.42.0/24 then action discard
8. Radius:Pica8	Pica8-IP-Downloadable-ACL-Rule	= seq 70 then action forward
9.	Click to add...	

Back to Enforcement Profiles Copy Save Cancel

Create an Enforcement Policy to Assign Dynamic VLAN and DACL

To add an enforcement policy, click on **Configuration->Enforcement->Policies** and click **Add**. Enter a **Name**, select **SE-LAB-VLAN** profile and click **Rules** tab as shown below.

Configuration » Enforcement » Policies » Edit - SE-LAB-Employee-Policy

Enforcement Policies - SE-LAB-Employee-Policy

Summary **Enforcement** Rules

Name: SE-LAB-Employee-Policy

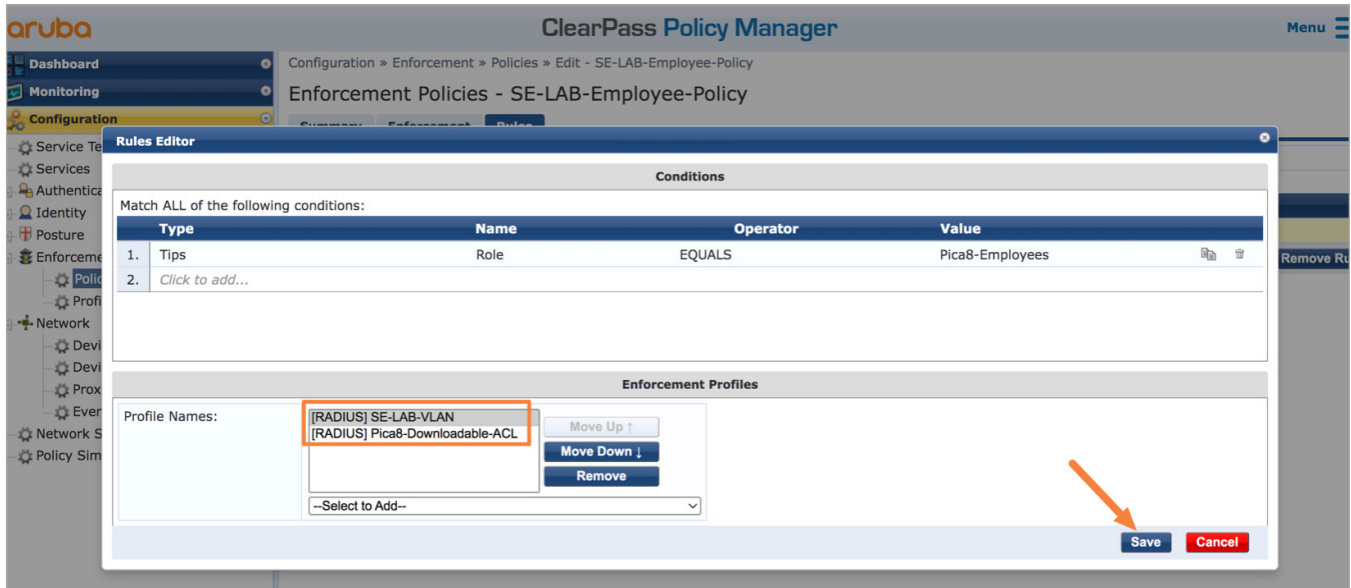
Description: SE-LAB-Employee-Policy

Enforcement Type: RADIUS

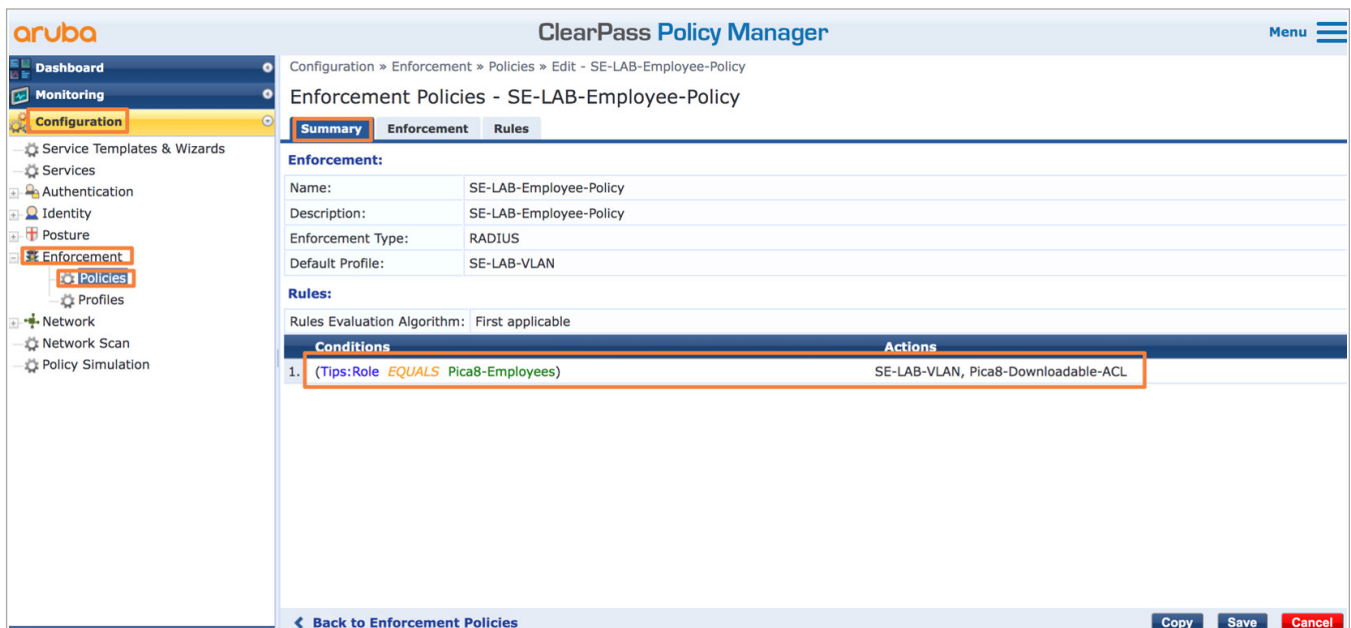
Default Profile: SE-LAB-VLAN View Details Modify Add New Enforcement Profile

Back to Enforcement Policies Copy Save Cancel

Click **Add Rule** and select the values as shown below for a new rule and select **SE-LAB-VLAN** and **Pica8-Downloadable-ACL** profiles and click **Save** in the **Rule** tab as shown below.



Click **Configuration->Enforcement->Policies-> SE-LAB-Employee-Policy** to view the newly created policy as shown below.



Create a Service for Employee 802.1X Authentication

Add 802.1x service called Pica8-Dot1x by clicking **Configuration -> Services** and click **Add**. Enter a **Name** and **Description** and select **options** and configure eight **conditions** shown below.

Configuration » Services » Edit - Pica8-Dot1x

Services - Pica8-Dot1x

Summary **Service** Authentication Roles Enforcement Audit Profiler

Name: Pica8-Dot1x

Description: 802.1X Wired Access Service

Type: 802.1X Wired

Status: Enabled

Monitor Mode: Enable to monitor network access without enforcement

More Options: Authorization Posture Compliance Audit End-hosts Profile Endpoints Accounting Proxy

Service Rule

Matches ANY or ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	EQUALS	Ethernet (15)
2.	Radius:IETF	Service-Type	EQUALS	Framed-User (2)
3.	Radius:IETF	NAS-IP-Address	EXISTS	
4.	Radius:IETF	Framed-MTU	EXISTS	
5.	Radius:IETF	Called-Station-Id	EXISTS	
5.	Radius:IETF	Calling-Station-Id	EXISTS	

Select **Authentication** tab and select six **authentication modes** in the same order shown below. Also select **Authentication Sources** as shown below.

Configuration » Services » Add

Services

Service **Authentication** Authorization Roles Enforcement Audit Profiler Summary

Authentication Methods:

- [EAP MD5]
- [EAP PEAP]
- [EAP FAST]
- [EAP TLS]
- [EAP TTLS]
- [EAP MSCHAPv2]

Authentication Sources:

- [Local User Repository] [Local SQL DB]

Strip Username Rules: Enable to specify a comma-separated list of rules to strip username prefixes or suffixes

Service Certificate: Select to Add

Click on the **Roles** tab and create a **Policy** and **Conditions** shown below and click **Save**.

aruba ClearPass Policy Manager

Configuration » Identity » Role Mappings » Add

Role Mappings

Role mapping policy has not been saved

Policy Mapping Rules Summary

Policy:

Policy Name: Pica8 Employee Policy
 Description: Pica8 Employee Policy
 Default Role: Pica8-Employees

Mapping Rules:

Rules Evaluation Algorithm: First applicable

Conditions	Role Name
1. (Authentication:Username EQUALS nirma)	Pica8-Employees

← Back to Services Next → Save Cancel

Go back to **Roles** tab and make sure **Pica8 Employee Policy** is selected. Following is summary of enforcement for Pica8-Dot1x service.

aruba ClearPass Policy Manager

Configuration » Services » Edit - Pica8-Dot1x

Services - Pica8-Dot1x

Summary Service Authentication Roles Enforcement Audit Profiler

Use Cached Results: Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: SE-LAB-Employee-Policy Modify Add New Enforcement Policy

Enforcement Policy Details

Description: SE-LAB-Employee-Policy
 Default Profile: SE-LAB-VLAN
 Rules Evaluation Algorithm: first-applicable

Conditions	Enforcement Profiles
1. (Tips:Role EQUALS Pica8-Employees)	SE-LAB-VLAN, Pica8-Downloadable-ACL

aruba ClearPass Policy Manager

Configuration » Services » Add

Services

Role mapping policy "Pica8 Employee Policy" added

Service Authentication Roles Enforcement Audit Profiler Summary

Role Mapping Policy: Pica8 Employee Policy Modify Add New Role Mapping Policy

Role Mapping Policy Details

Description: Pica8 Employee Policy
 Default Role: Pica8-Employees
 Rules Evaluation Algorithm: first-applicable

Conditions	Role
1. (Authentication:Username EQUALS nirmal)	Pica8-Employees

[Back to Services](#) Next → Save Cancel

Click **Audit** tab and select the **Audit Trigger** conditions and **Action after audit** as shown below:

aruba ClearPass Policy Manager

Configuration » Services » Edit - Pica8 Dot1x

Services - Pica8 Dot1x

Summary Service Authentication Roles Enforcement Audit Profiler

Audit Server: (Nmap Audit) View Details Modify Add New Audit Server

Audit Trigger Conditions:

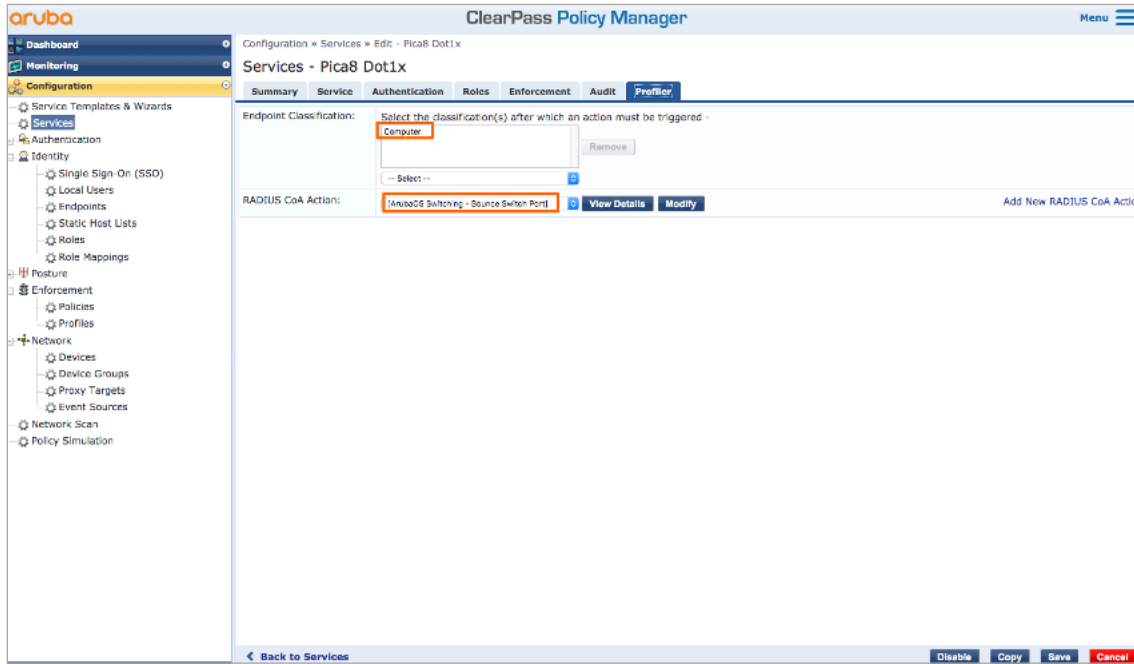
- Always
- When posture is not available
- For MAC authentication request

Action after audit:

- No Action
- Do SNMP bounce
- Trigger RADIUS CoA action

[Back to Services](#) Disable Copy Save Cancel

Click **Profiler** tab and select the **Endpoint Classification** and **RADIUS CoA Action** as shown below and click **Save** to save the newly added service.

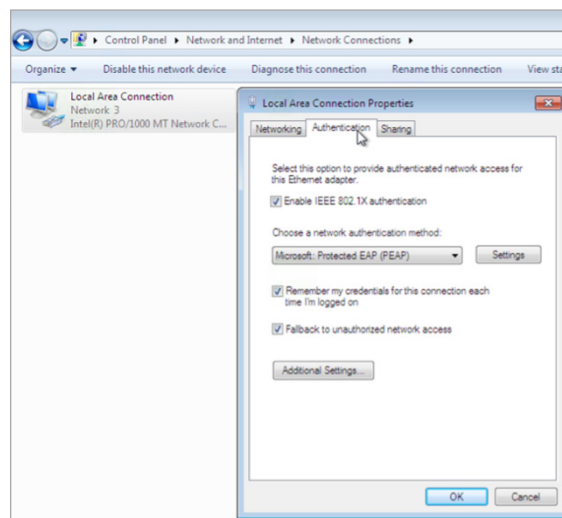


Configuring the Windows Supplicant on the Laptop

This configuration example does not use the Windows Active Directory credentials for user authentication. Instead, it uses the credentials of the local user defined on the Aruba ClearPass server.

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 Secured password (EAP-MSCHAP v2). Clear the **Automatically use my Windows logon name and password** check box.

If your Aruba ClearPass server is configured to use Windows Active Directory to authenticate users, you would leave this option selected.

Click **OK**. It will trigger login screen. Enter the user ID (nirmal) and password of the local user that you added to local user database on the Aruba ClearPass server

Verify the NAC Configuration

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

To check the communication between the PicOS switch and ClearPass run the following CLI:

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

When the Employee Laptop is connected to port ge-1/1/5, first you will see unauthorized status as shown below. User will be prompted to enter the login credentials in the Employee Laptop.

```
admin@P8-Access-BR-1-SW-2# run show dot1x interface gigabit-ethernet ge-1/1/5
Interface ge-1/1/5:
=====
Client MAC      : 80:e8:2c:b9:28:db
Status          : unauthorized
=====
```

After user successfully logs into the laptop, you will see the following the 802.1x authentication status on the switch for port ge-1/1/5:

```
admin@P8-Access-BR-1-SW-2# run 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 : Tue Mar 8 14:50:10 2022
Traffic Class   : Other
Dynamic VLAN ID : 10 (active)
Downloadable Filter Name : Pica8-Downloadable-ACL (active)
Downloadable Filter Rule : sequence 10 from destination-address-ipv4 192.168.42.71/32
                        : sequence 10 then action forward
                        : sequence 20 from destination-address-ipv4 192.168.42.1/32
                        : sequence 20 then action forward
```



```

sequence 30 from destination-address-ipv4 192.168.42.110/32
sequence 30 then action forward
sequence 40 from destination-address-ipv4 192.168.42.94/32
sequence 40 then action forward
sequence 50 from destination-address-ipv4 192.168.42.108/32
sequence 50 then action forward
sequence 60 from destination-address-ipv4 192.168.42.0/24
sequence 60 then action discard
sequence 70 then action forward

```

On the ClearPass Policy Manager UI, click **Monitoring -> Access Tracker** and click on the request entry to see the details as shown below.

ClearPass Policy Manager

Monitoring » Live Monitoring » Access Tracker

Access Tracker Mar 08, 2022 14:51:51 PST

The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.

[All Requests] C1000 (192.168.42.110) Last 6 days before Today

Filter: Host MAC Address contains [] Go Clear Filter Show 1000

#	Server	Source	Username	Service	Login Status	Request Time
1.	192.168.42.110	RADIUS	pica8	Pica8-Dot1x	ACCEPT	2022/03/08 14:4
2.	192.168.42.110	RADIUS	pica8	Pica8-Dot1x	ACCEPT	2022/03/08 14:4
3.	192.168.42.110	RADIUS	pica8	Pica8-Dot1x	ACCEPT	2022/03/08 14:4
4.	192.168.42.110	RADIUS	pica8	Pica8-Dot1x	ACCEPT	2022/03/07 21:2
5.	192.168.42.110	RADIUS	pica8	Pica8-Dot1x	ACCEPT	2022/03/07 18:2
6.	192.168.42.110	RADIUS	pica8	Pica8-Dot1x	ACCEPT	2022/03/07 15:2
7.	192.168.42.110	RADIUS	pica8	Pica8-Dot1x	ACCEPT	2022/03/07 15:2

ClearPass Policy Manager

Monitoring » Live Monitoring » Access Tracker

Access Tracker Mar 08, 2022 15:23:47 PST

Request Details

Summary Input Output Alerts

Login Status: ACCEPT

Session Identifier: R00000005-01-6227dd85

Date and Time: Mar 08, 2022 14:49:41 PST

End-Host Identifier: 80-E8-2C-B9-28-DB

Username: pica8

Access Device IP/Port: 192.168.42.170:5 (P8-Access-BR-1-SW-2 / Pica8)

Access Device Name: P8-Access-BR-1-SW-2

System Posture Status: UNKNOWN (100)

Policies Used -

Service: Pica8-Dot1x

Authentication Method: EAP-PEAP,EAP-MSCHAPv2

Authentication Source: Local:localhost

Authorization Source: [Local User Repository]

Roles: Pica8-Employees, [User Authenticated]

Enforcement Profiles: SE-LAB-VLAN, Pica8-Downloadable-ACL

Showing 1 of 16 records



To verify the RADIUS attributes sent by the switch to Aruba ClearPass for a particular request, click the request and then click the **Input** tab in the Request Details window.

Request Details			
Summary	Input	Output	Alerts
Username:	pica8		
End-Host Identifier:	80-E8-2C-B9-28-DB		
Access Device IP/Port:	192.168.42.170:5 (P8-Access-BR-1-SW-2 / Pica8)		
RADIUS Request			
Radius:IETF:Called-Station-Id	18-5A-58-1D-9C-21		
Radius:IETF:Calling-Station-Id	80-E8-2C-B9-28-DB		
Radius:IETF:Framed-MTU	768		
Radius:IETF:NAS-IP-Address	192.168.42.170		
Radius:IETF:NAS-Port	5		
Radius:IETF:NAS-Port-Type	15		
Radius:IETF:Service-Type	2		
Radius:IETF:User-Name	pica8		
Computed Attributes			
Endpoint Attributes			
Showing 1 of 1-6 records			
Change Status		Show Configuration	
Export		Show Logs	
Close			

From the Employee Windows laptop browser make sure you are able to reach www.example.com.

IP Phone Authentication

ClearPass Policy Manager is configured to authenticate IP phone Endpoint Groups with MAB authentication. Cisco IP Phone is connected to port ge-1/1/5. Voice VLAN 800 gets dynamically assigned to the IP Phone.

Configuring the MAB Wired Access Policy in ClearPass Policy Manager for IP Phones

Configuring the MAB Wired Access Policy in ClearPass Policy Manager for IP Involves Following Four Steps:

1. Create Static Host List for IP Phones and add IP Phone device MAC address to the Static Host Lists table
2. Configure Dynamic VLAN enforcement profile for IP Phones
3. Create an enforcement policy to assign dynamic Voice VLAN and ACL to the IP Phones device group after MAB authentication
4. Create a Service for MAB Authentication of IP Phone devices

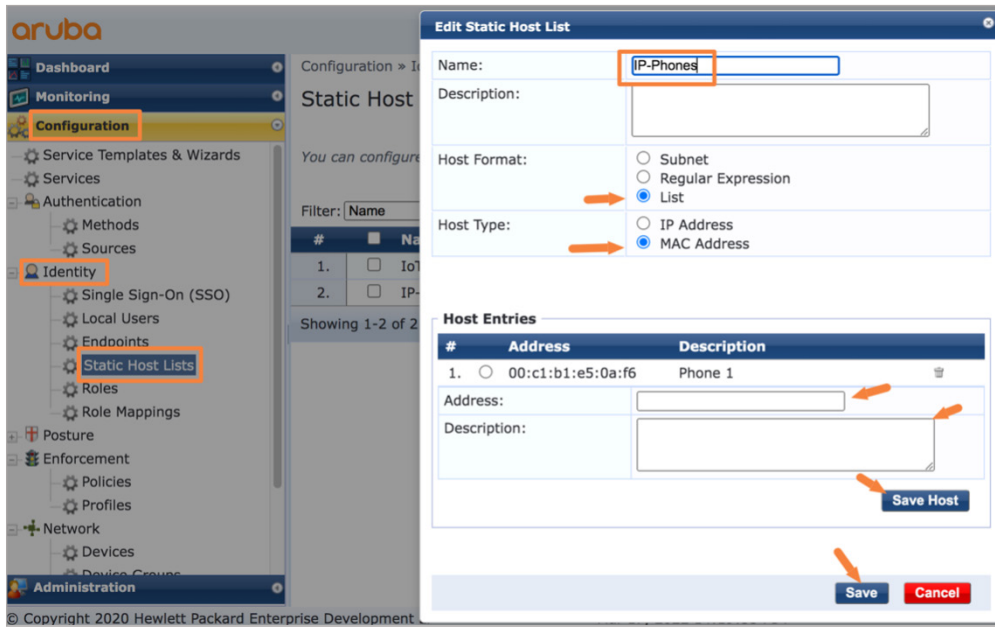
Creating Static Host Lists for IP Phones and Adding IP Phone's MAC Address to the Static Host Lists Table

Connect the IoT device to port ge-1/1/6. Run the following command in the PicOS switch to identify the MAC address of the first IP Phone device.

```
admin@P8-Access-BR-1-SW-2# run show dot1x interface gigabit-ethernet ge-1/1/5
Interface ge-1/1/5:
```

```
Client MAC           : 00:c1:b1:e5:0a:f6
Status              : unauthorized
```

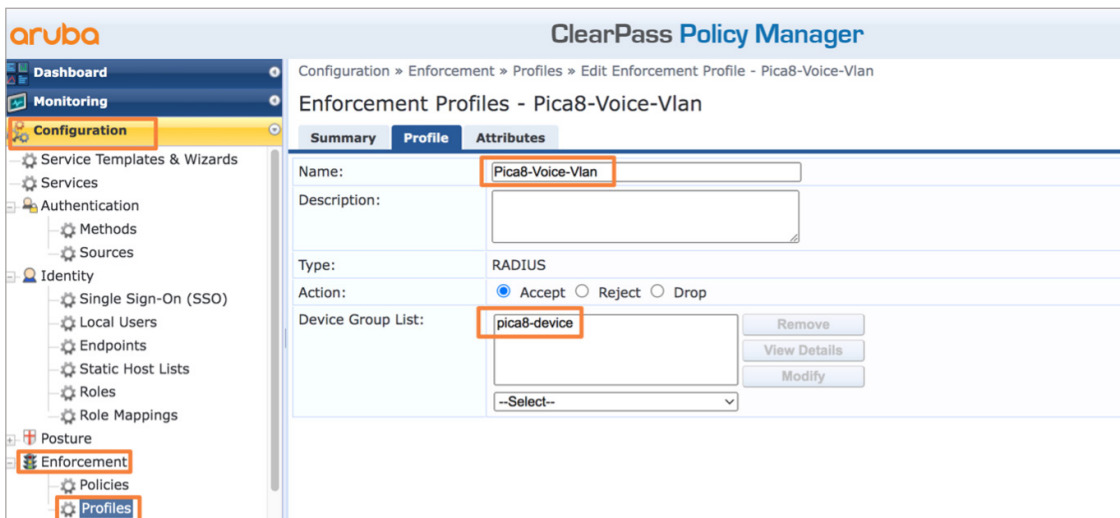
To create Static Hosts List (SHL) for IP Phones and adding IP Phone's Mac address to the SHL, navigate **Configuration -> Identity -> Static Host Lists** and click **+ Add**. Enter **Name**, select **List Host Format**, select **MAC Address**, enter the **MAC Address** of the first IP Phone device to this group list, enter **Description**, click **Save Host** and click **Save** as shown below.



Configure Dynamic VLAN Enforcement Profile for IP Phone

This profile defines the RADIUS attributes for specifying Voice VLAN 800. These RADIUS attributes are sent to the switch when an IP Phone device gets authenticated using MAB, enabling the switch to dynamically assign Voice VLAN 800 to the access port.

To add an enforcement profile, click on **Configuration->Enforcement->Profiles->Add** to add a new enforcement profile. On the Profile tab, choose **VLAN Enforcement** template, enter the VLAN name and select a Pica8-Switches device group as shown below and click **Next**.



On the **Attributes** tab fill the VLAN number you want to dynamically assign for Voice VLAN, add Pica8-AVPair attribute with value pica8-traffic-class=voice as shown below and click **Save**.

ClearPass Policy Manager

Configuration » Enforcement » Profiles » Edit Enforcement Profile - Pica8-Voice-Vlan

Enforcement Profiles - Pica8-Voice-Vlan

Type	Name	Value
1. RADIUS:IETF	Session-Timeout	= 10800
2. RADIUS:IETF	Termination-Action	= RADIUS-Request (1)
3. RADIUS:IETF	Tunnel-Type	= VLAN (13)
4. RADIUS:IETF	Tunnel-Medium-Type	= IEEE-802 (6)
5. RADIUS:IETF	Tunnel-Private-Group-Id	= 800
6. RADIUS:Pica8	Pica8-AVPair	= pica8-traffic-class=voice
7.	Click to add...	

← Back to Enforcement Profiles

Copy Save Cancel

Create an Enforcement Policy to Assign Dynamic Voice VLAN and ACL to the IP Phones Device Group

To add an enforcement policy, click on **Configuration->Enforcement->Policies** and click **Add**. Enter a Name, select Pica8-Voice-Vlan profile and click **Rules** tab as shown below.

ClearPass Policy Manager

Configuration » Enforcement » Policies » Edit - Pica8-IP-Phone-Policy

Enforcement Policies - Pica8-IP-Phone-Policy

Summary Enforcement Rules

Name: Pica8-IP-Phone-Policy

Description:

Enforcement Type: RADIUS

Default Profile: Pica8-Voice-Vlan View Details Modify

Add New Enforcement Profile

Click **Add Rule** and select the values as shown below for a new condition for IP Phones and then select **Pica8-Voice-Vlan** enforcement profiles and click **Save** in the **Rule** tab as shown below.

Configuration » Enforcement » Policies » Edit - Pica8-MAC-Auth-Policy

Enforcement Policies - Pica8-MAC-Auth-Policy

Summary Enforcement **Rules**

Rules Evaluation Algorithm: Select first match Select all matches

Enforcement Policy Rules:

Conditions	Actions
1. (Authentication:Source EQUALS IP Phones)	Pica8-Voice-Vlan
2. (Authentication:Source EQUALS IoT device)	SE-LAB-VLAN, Pica8-Dynamic-ACL
3. (Authentication:MacAuth EQUALS KnownClient)	SE-LAB-VLAN, Pica8-Dynamic-ACL
4. (Authentication:MacAuth EQUALS UnknownClient)	Guest_Access_Portal_Profile

Buttons: Add Rule, Copy Rule, Move Up ↑, Move Down ↓, Edit Rule, Remove Rule

Summary of the Policy is shown below:

Configuration » Enforcement » Policies » Edit - Pica8-MAC-Auth-Policy

Enforcement Policies - Pica8-MAC-Auth-Policy

Summary **Enforcement** Rules

Enforcement:

Name:	Pica8-MAC-Auth-Policy
Description:	
Enforcement Type:	RADIUS
Default Profile:	[Deny Access Profile]

Rules:

Rules Evaluation Algorithm: First applicable

Conditions	Actions
1. (Authentication:Source EQUALS IP Phones)	Pica8-Voice-Vlan

Create a Service for MAB Authentication of IP Phone Devices

Add a service called Pica8-MAB by clicking **Configuration -> Services** and click **Add**. Enter a **Name** and **Description** and select **options** and configure eight **conditions** shown below.

ClearPass Policy Manager

Configuration » Services » Edit - Pica8-MAB

Services - Pica8-MAB

Summary Service **Authentication** Authorization Roles Enforcement

Description: MAC-based Authentication Service

Type: MAC Authentication

Status: Enabled

Monitor Mode: Enable to monitor network access without enforcement

More Options: Authorization Audit End-hosts Profile Endpoints Accounting Proxy

Service Rule

Matches ANY or ALL of the following conditions:

Type	Name	Operator	Value
1. Radius:IETF	NAS-Port-Type	EQUALS	Ethernet (15)
2. Radius:IETF	Service-Type	EQUALS	Call-Check (10)
3. Radius:IETF	NAS-IP-Address	EXISTS	
4. Radius:IETF	Framed-MTU	EXISTS	
5. Radius:IETF	Called-Station-Id	EXISTS	
6. Radius:IETF	Calling-Station-Id	EXISTS	
7. Radius:IETF	NAS-Port	EXISTS	
8. Radius:IETF	User-Name	EXISTS	

Select **Authentication** tab and select Authentication Methods as shown below. Also select **Authentication Sources** as shown below:

ClearPass Policy Manager

Configuration » Services » Edit - Pica8-MAB

Services - Pica8-MAB

Summary Service **Authentication** Authorization Roles Enforcement

Authentication Methods: [Allow All MAC AUTH] Add New Authentication Method

Authentication Sources: [Endpoints Repository] [Local SQL DB] [IP Phones (Static Host List)] [IoT device (Static Host List)] Add New Authentication Source

Strip Username Rules: Enable to specify a comma-separated list of rules to strip username prefixes or suffixes

On the Enforcement tab, select **Pica8-Mac-Auth-Policy** and a new **Condition** for IP Phones as shown below and click **Save**.

ClearPass Policy Manager

Configuration » Services » Edit - Pica8-MAB

Services - Pica8-MAB

Summary Service Authentication Authorization Roles **Enforcement**

Use Cached Results: Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: Pica8-MAC-Auth-Policy Add New Enforcement Policy

Enforcement Policy Details

Description:

Default Profile: [Deny Access Profile]

Rules Evaluation Algorithm: first-applicable

Conditions	Enforcement Profiles
1. [Authentication:Source EQUALS IP Phones]	Pica8-Voice-Vlan

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)
=====
```

The screenshot shows the Aruba ClearPass Policy Manager interface. The left sidebar contains navigation options like Dashboard, Monitoring, Accounting, and System Monitor. The main area displays the 'Access Tracker' page for server C1000 (192.168.42.110) on Mar 18, 2022. A table lists access requests, with two rows highlighted in orange:

#	Server	Source	Username	Service	Login Status	Request Timestamp
1.	192.168.42.110	RADIUS	38:17:c3:c0:a1:68	Pica8-MAB	ACCEPT	2022/03/16 15:07:39
2.	192.168.42.110	RADIUS	00:c1:b1:e5:0a:f6	Pica8-MAB	ACCEPT	2022/03/16 15:07:35

To check the RADIUS attributes sent by Aruba ClearPass Policy Manager to the switch for IP Phone, click the **Output** tab shown below:

The screenshot shows the 'Request Details' window with the 'Output' tab selected. It displays enforcement profiles and a list of RADIUS response attributes. Two attributes are highlighted with orange boxes:

- Radius:IETF:Tunnel-Private-Group-Id: 800
- Radius:Pica8:Pica8-AVPair: pica8-traffic-class=voice



Multi-host Authentication

An employee laptop is connected behind Cisco IP Phone and Cisco IP Phone is connected to port ge-1/1/5 of the switch. To check authentication of multiple hosts connected to the same port, execute the following command in the switch:

```
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_1 (active)
=====
```

Dynamic Voice VLAN 800 is assigned to the IP Phone and Dynamic VLAN 10 and Dynamic ACL mac_auth_policy_1 are assigned to the Employee laptop.

IoT Device Authentication

IoT device is connected to port ge-1/1/6 and authenticated using MAB. After authentication VLAN 10 and mac_auth_policy_1 ACL are dynamically assigned to the IoT device.

Configuring the MAB Wired Access Policy in ClearPass Policy Manager for an IoT Device

Configuring the MAB Wired Access policy in ClearPass Policy Manager for IoT devices involves following four steps:

1. Create Static Host Lists for IoT devices and add IoT device MAC address to the Static Host Lists table
2. Configure Dynamic VLAN enforcement profile
3. Configure Dynamic ACL enforcement profile
4. Create an enforcement policy to assign dynamic VLAN and ACL to the IoT device after MAB authentication
5. Create a Service for MAB Authentication of IoT device

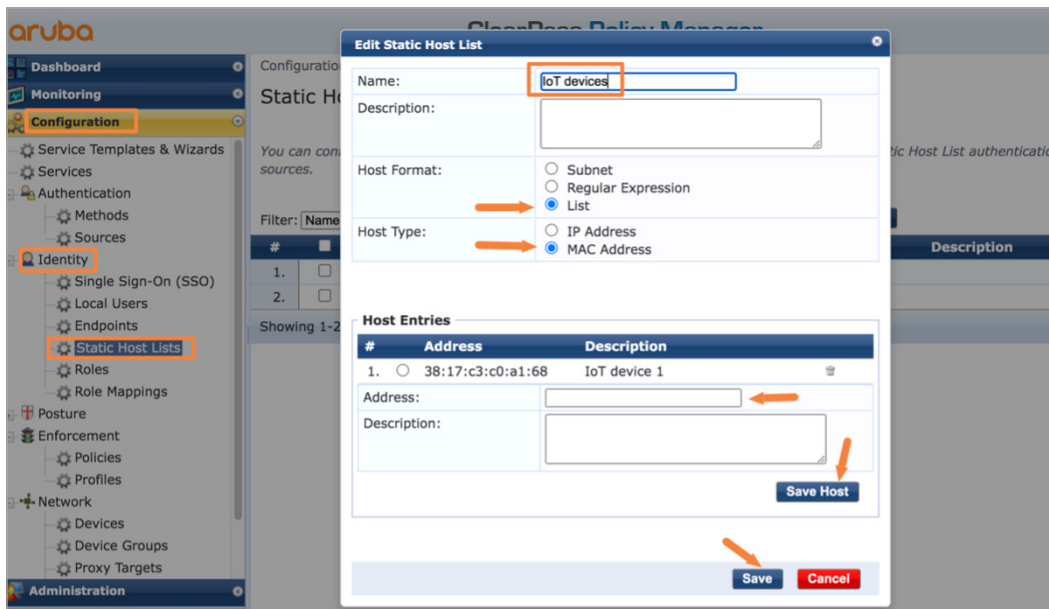
Creating Static Host Lists for IoT Devices and Add IoT Device's MAC Address to the Static Host Lists Table

Connect the IoT device to port ge-1/1/6. Run the following command in the PicOS switch to identify the MAC address of the IoT device.


```
admin@P8-Access-BR-1-SW-2# run show dot1x interface gigabit-ethernet ge-1/1/6
Interface ge-1/1/6:
```

```
=====
Client MAC           : 38:17:c3:c0:a1:68
Status               : unauthorized
```

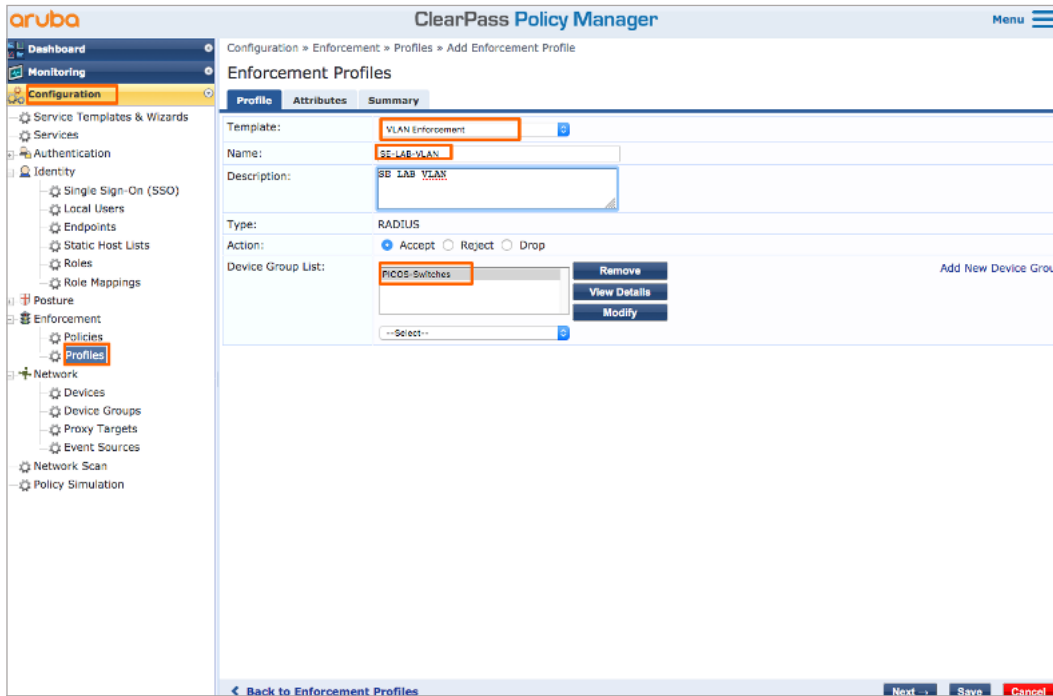
To create Static Hosts List (SHL) for IoT devices and add IoT device's Mac address to the SHL, navigate **Configuration -> Identity -> Static Host Lists** and click **+ Add**. Enter **Name**, select **List Host Format**, select **MAC Address**, enter the MAC Address of the first IoT device to this group list, enter **Description**, click **Save Host** and click **Save** as shown below.



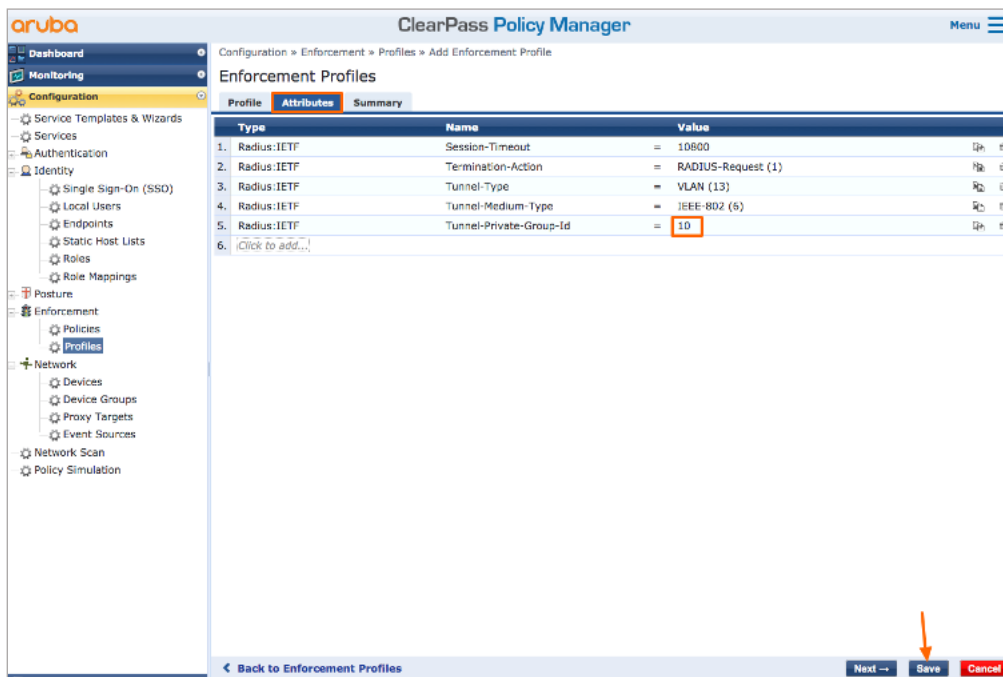
Configure Dynamic VLAN Enforcement Profile

This profile defines the RADIUS attributes for specifying VLAN 10. These RADIUS attributes are sent to the switch when a user who belongs to the Engineering department authenticates using 802.1X, enabling the switch to dynamically assign VLAN 10 to the access port.

To add a enforcement profile, click on **Configuration->Enforcement->Profiles->Add** to add a new enforcement profile. On the Profile tab, choose **VLAN Enforcement** template, enter the VLAN name and select a Pica8-Switches device group as shown below and click **Next**.



On the **Attributes** tab fill the VLAN number you want to dynamically assign as shown below and click **Save**.

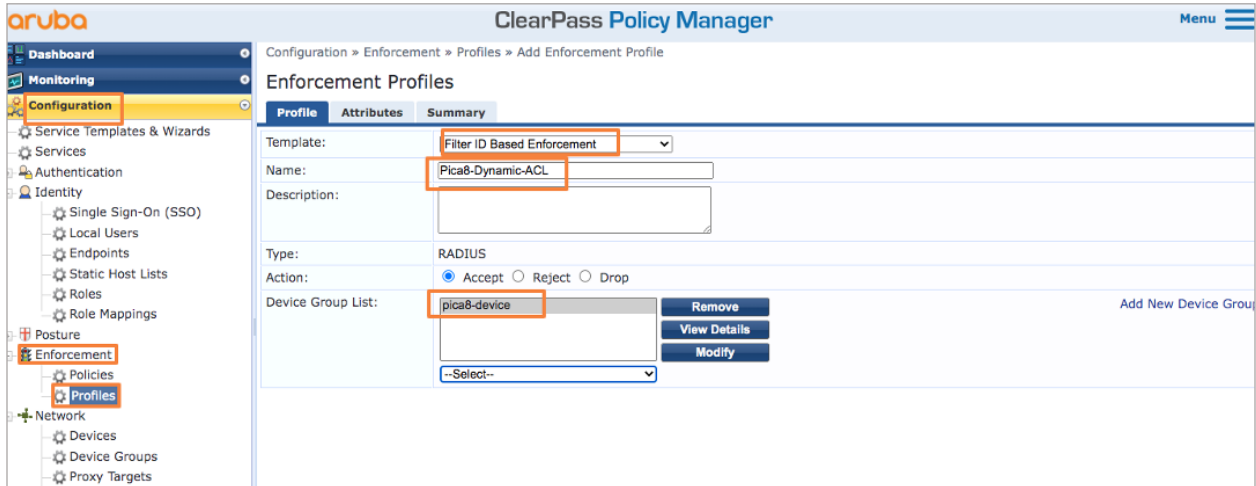


Configure Dynamic ACL Enforcement Profile

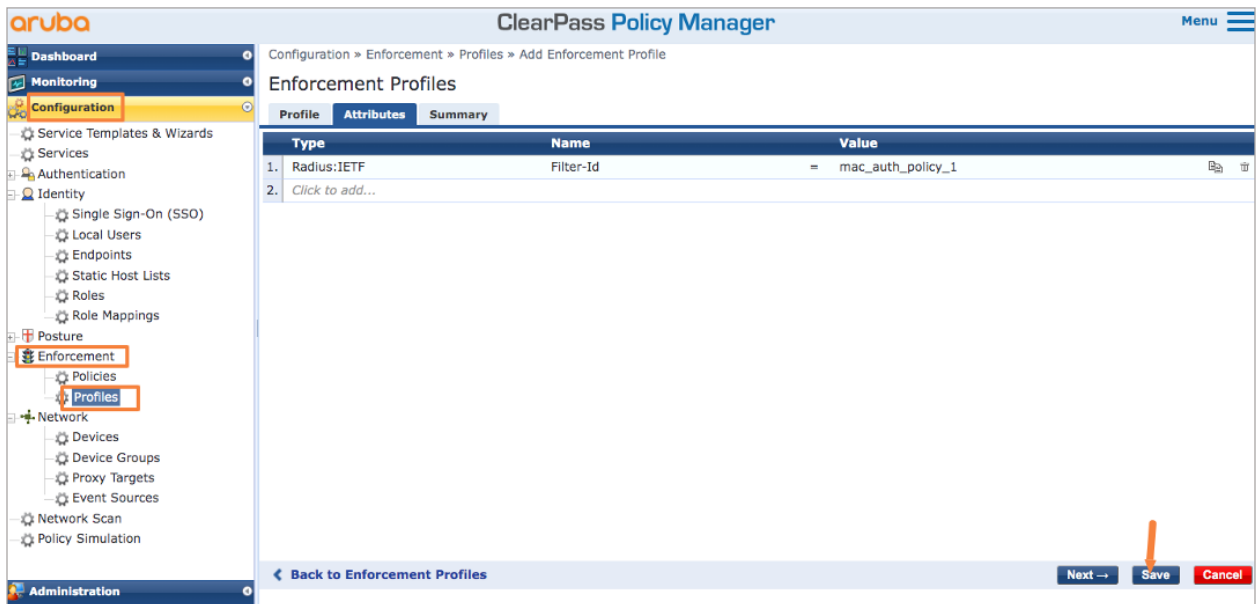
This profile defines the RADIUS attributes for specifying a dynamic ACL called Pica8-Dynamic-ACL.

To add a enforcement profile, click on **Configuration->Enforcement->Profiles->Add** to add a new enforcement profile.

On the Profile tab, choose **Filter ID based Enforcement** template, enter the Dynamic ACL name and select a **Pica8-device** device group as shown below and click **Next**.



Enter **mac_auth_policy_1** as **Filter-id** value and click **Save**.



Create an Enforcement Policy to Assign Dynamic VLAN and ACL

To add an enforcement policy, click on **Configuration->Enforcement->Policies** and click **Add**. Enter a **Name**, select **Default Access Profile** profile and click **Rules** tab as shown below.

ClearPass Policy Manager

Configuration » Enforcement » Policies » Edit - Pica8-MAC-Auth-Policy

Enforcement Policies - Pica8-MAC-Auth-Policy

Summary Enforcement Rules

Name: Pica8-MAC-Auth-Policy

Description:

Enforcement Type: RADIUS

Default Profile: [Deny Access Profile] [View Details](#) [Modify](#)

Click **Add Rule** and select the values as shown below for a new condition for IoT devices and then select **SE-LAB-VLAN** and **Pica8-Dynamic-ACL** enforcement profiles and click **Save** in the **Rule** tab as shown below.

ClearPass Policy Manager

Configuration » Enforcement » Policies » Edit - Pica8-MAC-Auth-Policy

Enforcement Policies - Pica8-MAC-Auth-Policy

Summary Enforcement Rules

Rules Evaluation Algorithm: Select first match Select all matches

Enforcement Policy Rules:

Conditions	Actions
1. (Authentication:Source EQUALS IP Phones)	Pica8-Voice-Vlan
2. (Authentication:Source EQUALS IoT device)	SE-LAB-VLAN, Pica8-Dynamic-ACL
3. (Authentication:MacAuth EQUALS KnownClient)	SE-LAB-VLAN, Pica8-Dynamic-ACL
4. (Authentication:MacAuth EQUALS UnknownClient)	Guest_Access_Portal_Profile

[Add Rule](#) [Copy Rule](#) [Move Up ↑](#) [Move Down ↓](#) [Edit Rule](#) [Remove Rule](#)

Summary of the Policy is shown below:

ClearPass Policy Manager

Configuration » Enforcement » Policies » Edit - Pica8-MAC-Auth-Policy

Enforcement Policies - Pica8-MAC-Auth-Policy

Summary Enforcement Rules

Enforcement:

Name: Pica8-MAC-Auth-Policy

Description:

Enforcement Type: RADIUS

Default Profile: [Deny Access Profile]

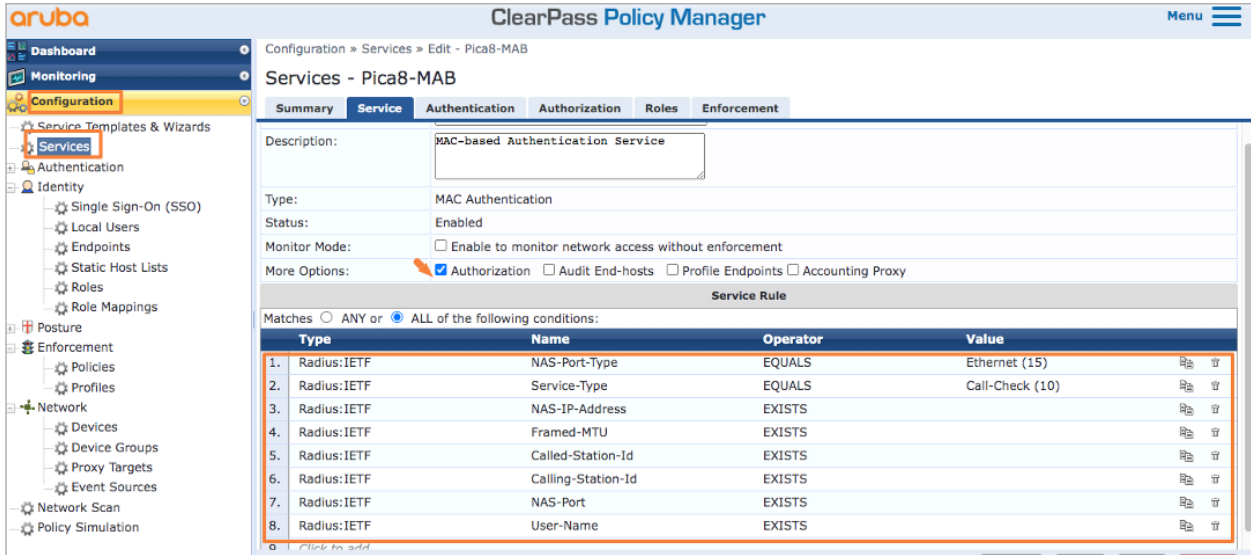
Rules:

Rules Evaluation Algorithm: First applicable

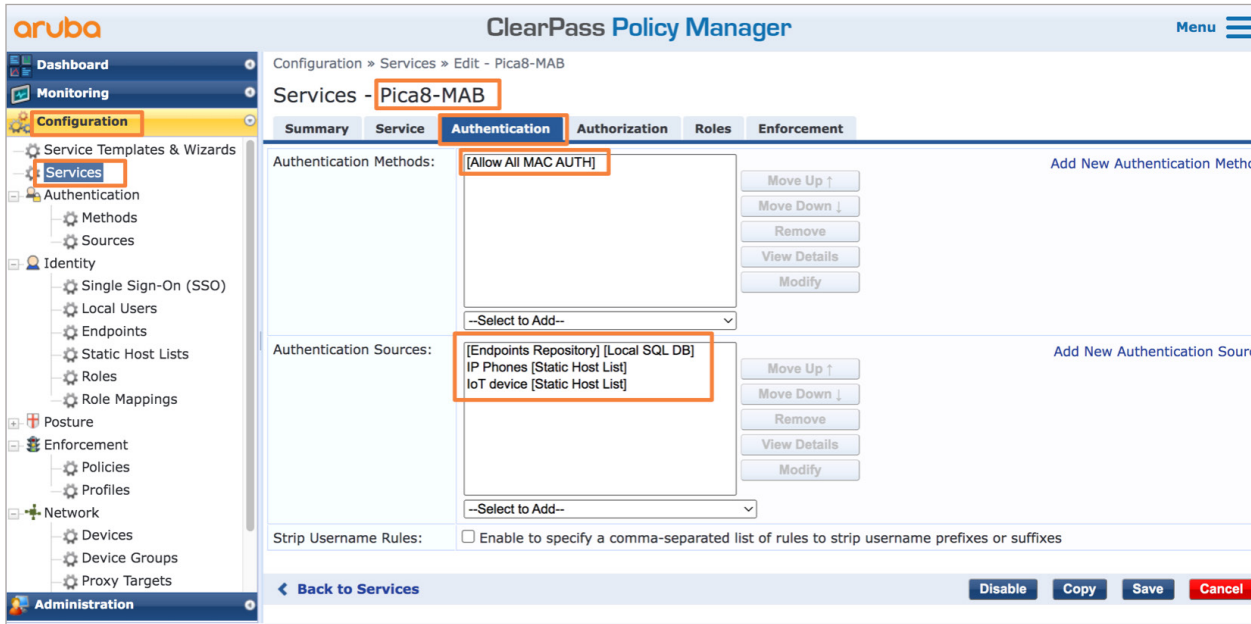
Conditions	Actions
1. (Authentication:MacAuth EQUALS KnownClient)	SE-LAB-VLAN, Pica8-Dynamic-ACL

Create a Service for MAB Authentication of IoT Device

Add a service called Pica8-MAB by clicking **Configuration -> Services** and click **Add**. Enter a **Name** and **Description** and select **options** and configure eight **conditions** shown below.



Select **Authentication** tab and select Authentication Methods as shown below. Also select **Authentication Sources** as shown below.



On the **Enforcement** tab, select **Pica8-Mac-Auth-Policy** as shown below, add a new condition for IoT device and click **Save** as shown below.

Configuration » Services » Edit - Pica8-MAB

Services - Pica8-MAB

Summary Service Authentication Authorization Roles **Enforcement**

Use Cached Results: Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: **Pica8-MAC-Auth-Policy** [Modify](#) [Add New Enforc](#)

Enforcement Policy Details

Description:

Default Profile: [Deny Access Profile]

Rules Evaluation Algorithm: first-applicable

Conditions	Enforcement Profiles
1. (Authentication:Source EQUALS IP Phones)	Pica8-Voice-Vlan
2. (Authentication:Source EQUALS IoT device)	SE-LAB-VLAN, Pica8-Dynamic-ACL

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# run 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    : Wed Mar 9 13:33:50 2022
Traffic Class        : Other
Dynamic VLAN ID      : 10 (active)
Dynamic Filter Name   : mac_auth_policy_1 (active)
=====
```

On the ClearPass Policy Manager UI, click **Monitoring -> Access Tracker** and click on the request entry to see the details as shown below.

Monitoring » Live Monitoring » Access Tracker

Access Tracker Mar 09, 2022 13:29:56 PST Auto Refresh

The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.

[All Requests] C1000 (192.168.42.110) Last 3 days before Today [Edit](#)

Filter: Host MAC Address contains 38:17:c3:c0:a1:68 [Go](#) [Clear Filter](#) Show 1000 records

#	Server	Source	Username	Service	Login Status	Request Timestamp
1.	192.168.42.110	RADIUS	38:17:c3:c0:a1:68	Pica8-MAB	ACCEPT	2022/03/09 13:27:22

To check the **Enforcement Profiles** used by Aruba ClearPass Policy Manager for the IoT device click the **Summary** tab shown below:

Request Details		
Summary	Input	Output
Login Status:	ACCEPT	
Session Identifier:	R00000013-01-62291bba	
Date and Time:	Mar 09, 2022 13:27:22 PST	
End-Host Identifier:	38-17-C3-C0-A1-68	
Username:	38:17:c3:c0:a1:68	
Access Device IP/Port:	192.168.42.170:6 (P8-Access-BR-1-SW-2 / Pica8)	
Access Device Name:	P8-Access-BR-1-SW-2	
System Posture Status:	UNKNOWN (100)	
Policies Used -		
Service:	Pica8-MAB	
Authentication Method:	MAC-AUTH	
Authentication Source:	Local:localhost	
Authorization Source:	[Endpoints Repository]	
Roles:	[User Authenticated]	
Enforcement Profiles:	SE-LAB-VLAN, Pica8-Dynamic-ACL	

◀ ◀ Showing 1 of 1-5 records ▶ ▶
 [Change Status](#)
 [Show Configuration](#)
 [Export](#)
 [Show Logs](#)
 [Close](#)

Guest Laptop Using MAB and Central Web Authentication

In this case, the switch detects that the Mac OS endpoint does not have an 802.1X supplicant. The guest laptop is connected to port ge-1/1/7.

Logic for Guest laptop authentication is as follows:

1. MAB Authentication detects Guest laptop device is not a registered device. The default rule for unknown device redirects the user to the Guest Portal with URL <https://www.clearpass.com/guest/weblogin.php/2?&mac=<MAC Address of unknown device>>
2. Guest or contractor logs into the Guest Portal. This part is handled by Central Web Authentication. After successful authentication, RADIUS server marks the device as Known Device and sends the following RADIUS attribute which bounces the port in which Guest Laptop is connected. Radius Attribute is sent as follows: Pica8-AVPair with value command=pica8-bounce-host-port
3. MAB Authentication detects Guest laptop device is a known device and it assigns a Dynamic VLAN (SE-LAB-VLAN), and Dynamic ACL (Pica8-Dynamic-ACL) to the device.

This use case involves configuring the PicOS switch, configure the ClearPass Guest Portal, configure the ClearPass Policy Manager, 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
  192.168.42.110/32
set protocols dot1x filter mac_auth_policy_1 sequence 6 then action "forward"
set protocols dot1x filter mac_auth_policy_1 sequence 7 from destination-address-ipv4
  192.168.42.1/32
set protocols dot1x filter mac_auth_policy_1 sequence 7 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 "vlan0"
set vlans vlan-id 20 l3-interface "vlan20"
set l3-interface vlan-interface vlan20 address 192.168.44.1 prefix-length 24

```

Configuring Aruba ClearPass Guest Portal

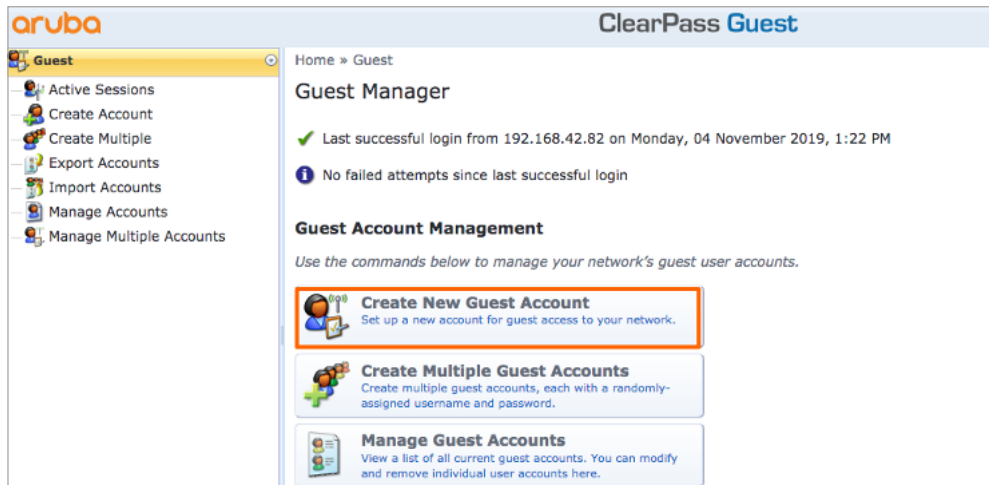
We will use the ClearPass Guest Portal for the Guest authentication. The following are the main steps for configuring ClearPass Guest:

- Set up the guest user account
- Configure the guest login page

Log in to ClearPass Guest. For example: <https://192.168.42.110/guest-with-credentials-admin/pica8pica8>

Set up the Guest User Account

Click **Create New Guest Account**



Provide the details for the guest user account, as shown below. Make sure to note the password, which is automatically generated. Click **Create**.

aruba ClearPass Guest

Home » Guest » Create Account

Create Guest Account

New guest account being created by *admin*.

Create New Guest Account

* Guest's Name: Name of the guest.

* Company Name: Company name of the guest.

* Email Address: The guest's email address. This will become their username to log into the network.

Account Activation: Select an option for changing the activation time of this account.

Account Expiration: Select an option for changing the expiration time of this account.

* Account Role: Role to assign to this account.

Password:

Notes:

* Terms of Use: I am the sponsor of this account and accept the terms of use

* required field

[Back to guests](#)

[Back to main](#)

Configure the Guest Access Login Page

Select **Configuration -> Pages -> Web Logins** and click **Create a new web login page**.

aruba ClearPass Guest

Home » Configuration » Pages » Web Logins

Web Logins

Many NAS devices support Web-based authentication for visitors.

By defining a web login page on the ClearPass Guest you are able to provide a customized graphical login page for visitors accessing the network through these NAS devices.

Use this list view to define new web login pages, and to make changes to existing web login pages.

Onboard device provisioning pages are now managed from the Web Login tab within provisioning settings

Name	Page Title	Page Name	Page Skin
There are no web login pages to display.			
0 web logins <input type="button" value="Reload"/> <input type="button" value="Show all rows"/>			

[Back to pages](#)

[Back to configuration](#)

[Back to main](#)

In the **Web Login** Editor, provide a name for the Web login page you are creating, specify the login page name as it appears in the URL, and set Login Method to **Server-Initiated – Change of authorization (RFC 3576) sent to controller** as shown below. In the **Login Form** section of the Web Login page, set **Pre-Auth Check** to **None – no extra checks will be made** as shown below.

Set **Login Delay** to 20 seconds. In the **Default Destination** section, enter a default URL, as shown below, to which the guest gets redirected after successful authentication. In this example, the guest is redirected to the Pica8 home page after authentication.

Default Destination	
Options for controlling the destination clients will redirect to after login.	
* Default URL:	<input type="text" value="http://pica8.com"/> Enter the default URL to redirect clients. Please ensure you prepend "http://" for any external domain.
Override Destination:	<input checked="" type="checkbox"/> Force default destination for all clients If selected, the client's default destination will be overridden regardless of its value.

Click **Save Changes**.

Configure the ClearPass Policy Manager

Following table provides summary of profile, policy, service names and sequence of operation configured for this use case.

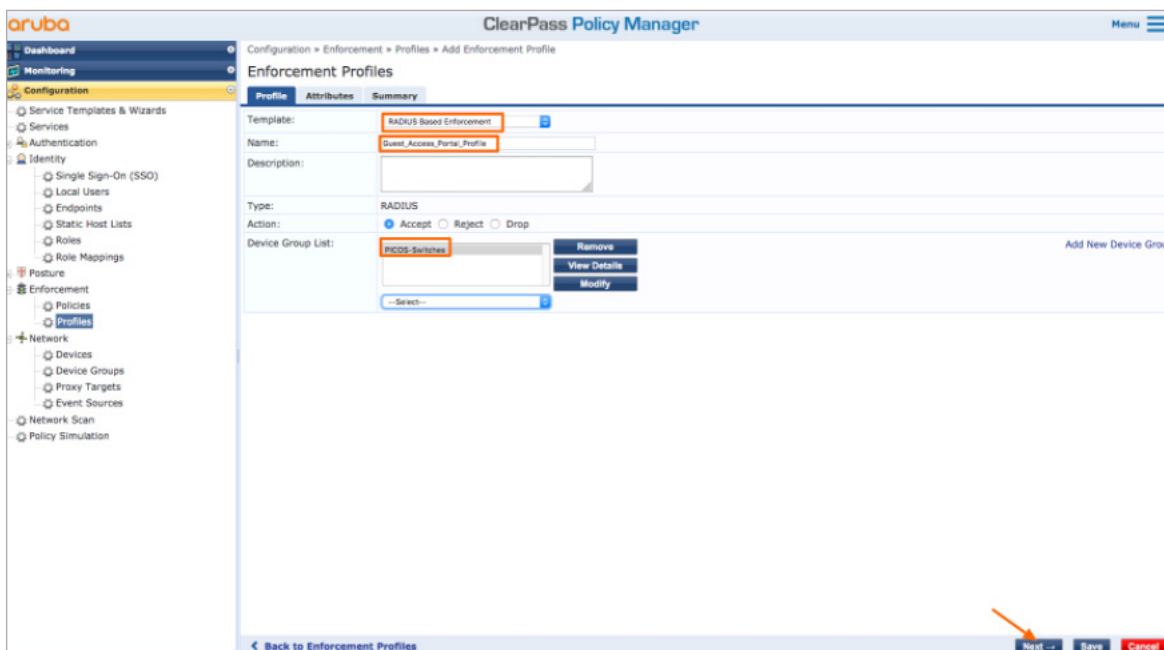
Sequence of Operation	Service Name	Service Type	Policy Name	Profile Name	Client Type	Operation
1	Pica8-MAB	MAB	Pica8-Mac-Auth-Policy	Guest_Access_Portal_Profile	UnknownClient	Redirects the guest to ClearPass Guest login page for CWA. Puts the guest in Block VLAN
2	Guest_Web_Auth_Service	CWA	Guest_Auth_Enforcement_Policy	Pica8-CoA-Bounce-Port	UnknownClient	After Guest enters credentials, Web authentication Guest becomes KnownClient
3	Pica8-MAB	MAB	Pica8-Mac-Auth-Policy	SE-LAB-VLAN, Pica8-Dynamic-ACL	KnownClient	Put the guest in VLAN10 and applies dynamic ACL

The following are configuration steps using ClearPass UI:

1. Follow **Add device and group**, and **Configure a Vlan enforcement profile and policy** sections from 802.1x which are common for this use case as well.
2. **Configure the MAC RADIUS authentication enforcement profile.**

This profile provides the switch with the address of the redirect URL for Aruba ClearPass Guest login page. Select **Configuration->Enforcement->Profiles**, click **Add**.

On the Profile tab, set Template to **RADIUS Based Enforcement** and type the profile name, **Guest_Access_Portal_Profile** in the Name field, **PICOSwitches** in the Device Group List and click **Next** as shown below.



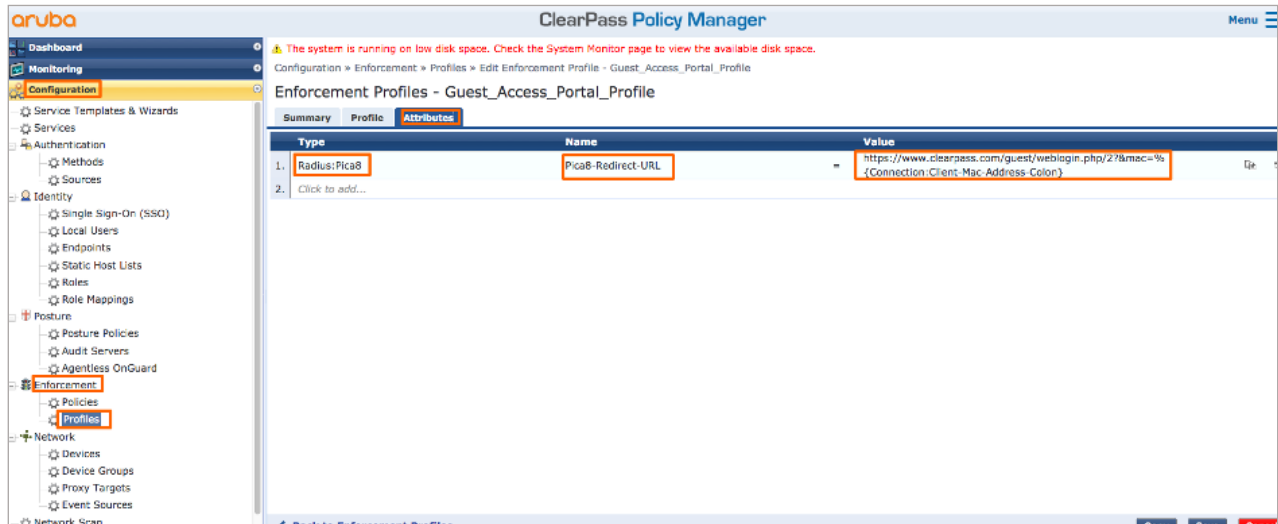


On the Attributes tab, configure the following attributes:

Set **Radius:Pica8** attribute type with **PICA8-Redirect-URL** name and value set to the following: **<https://www.clearpass.com/guest/weblogin.php/2?&mac=%{Connection:Client-Mac-Address-Colon}>**

This URL goes to the Aruba ClearPass Guest server. It also passes the MAC address of the endpoint to ClearPass Guest as shown below.

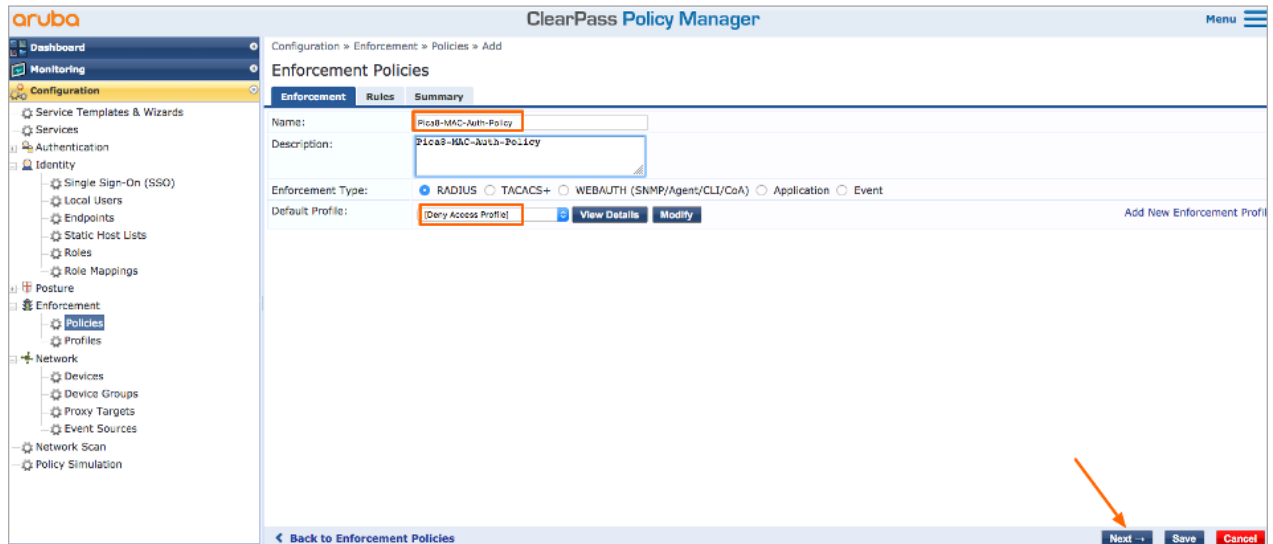
Click **Save**.



3. Configure the MAC RADIUS authentication enforcement policy.

The MAC RADIUS policy tells Aruba ClearPass to apply the **Deny Access Profile** to all endpoints undergoing MAC RADIUS authentication that are not already known to ClearPass—that is, are not in the endpoint repository.

Select **Configuration->Enforcement->Policies**, click **Add**. On the Enforcement tab, type the name of policy as **Pica8-MAC-Auth-Policy** and set the Default Profile to **Deny Access Profile** as shown below and click **Next**.



On the Rules tab, click **Add Rule** and add the rule shown. Enter the rules as shown below (includes previously configured rules for IP Phones and IoT devices) and Click **Save**.

Configuration » Enforcement » Policies » Edit - Pica8-MAC-Auth-Policy

Enforcement Policies - Pica8-MAC-Auth-Policy

Summary Enforcement **Rules**

Rules Evaluation Algorithm: Select first match Select all matches

Enforcement Policy Rules:

Conditions	Actions
1. (Authentication:Source EQUALS IP Phones)	Pica8-Voice-Vlan
2. (Authentication:Source EQUALS IoT device)	SE-LAB-VLAN, Pica8-Dynamic-ACL
3. (Authentication:MacAuth EQUALS KnownClient)	SE-LAB-VLAN, Pica8-Dynamic-ACL
4. (Authentication:MacAuth EQUALS UnknownClient)	Guest_Access_Portal_Profile

Buttons: Add Rule, Copy Rule, Move Up ↑, Move Down ↓, Edit Rule, Remove Rule

Bottom buttons: Copy, **Save**, Cancel

4. Configure the MAC Radius authentication service.

Pica8-MAB is a simple service for handling unknown client types only. We will create a new Radius Mac Authentication service that will handle both known and unknown client types.

Configuration » Services

Services

This page shows the current list and order of services that ClearPass follows during authentication and authorization.

Filter: Name contains [] Go Clear Filter Show 20 records

#	Order	Name	Type	Template	Status
1.	<input type="checkbox"/>	7 Pica8-MAB	RADIUS	MAC Authentication	✓
2.	<input type="checkbox"/>	8 Pica8-Dot1x	RADIUS	802.1X Wired	✓
3.	<input type="checkbox"/>	11 Guest_Web_Auth_Service	WEBAUTH	Web-based Authentication	✓
4.	<input type="checkbox"/>	1 [Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	⊘
5.	<input type="checkbox"/>	2 [AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	⊘

Select **Configuration** -> **Services**, click **Add**. On the **Service** tab, fill out the fields as shown below.

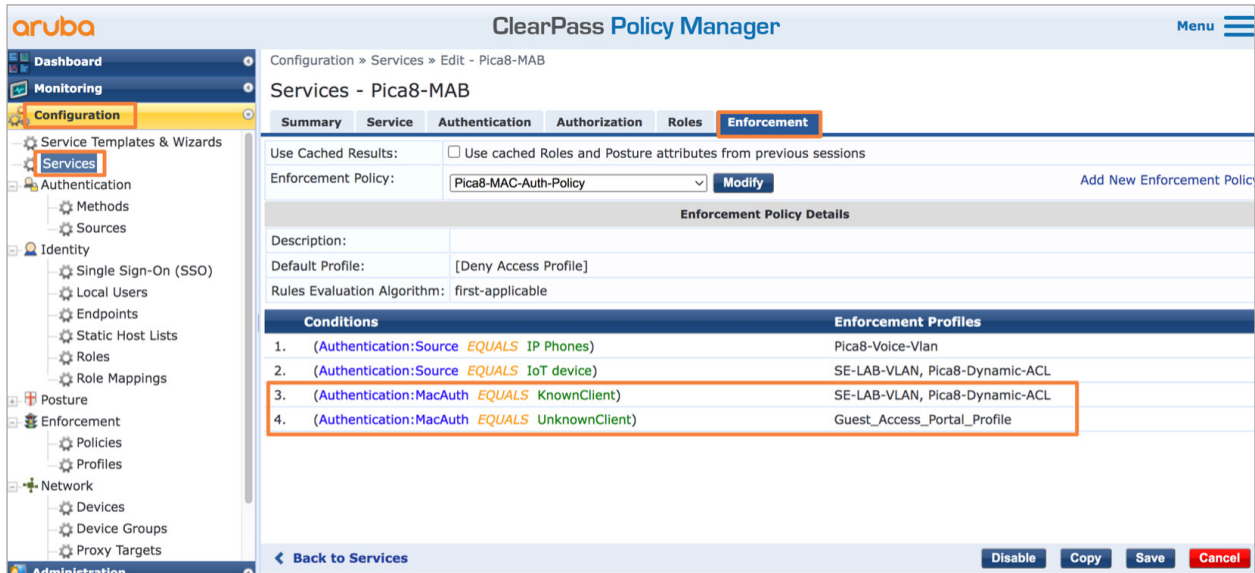
The screenshot shows the 'Services - Pica8-MAB' configuration page in the 'Service' tab. The 'Name' field is 'Pica8-MAB' and the 'Description' is 'MAC-based Authentication Service'. The 'Type' is 'MAC Authentication' and the 'Status' is 'Enabled'. The 'Monitor Mode' has an option to 'Enable to monitor network access without enforcement' which is unchecked. Under 'More Options', 'Authorization' is checked, while 'Audit End-hosts', 'Profile Endpoints', and 'Accounting Proxy' are unchecked. The 'Service Rule' section shows a table with 8 conditions:

Type	Name	Operator	Value
1. Radius:IETF	NAS-Port-Type	EQUALS	Ethernet (15)
2. Radius:IETF	Service-Type	EQUALS	Call-Check (10)
3. Radius:IETF	NAS-IP-Address	EXISTS	
4. Radius:IETF	Framed-MTU	EXISTS	
5. Radius:IETF	Called-Station-Id	EXISTS	
6. Radius:IETF	Calling-Station-Id	EXISTS	
7. Radius:IETF	NAS-Port	EXISTS	
8. Radius:IETF	User-Name	EXISTS	

On the **Authentication** tab, set **Authentication Sources** as shown below. It includes all Authentication sources for MAB namely IP Phone devices, IoT devices and contractor devices.

The screenshot shows the 'Services - Pica8-MAB' configuration page in the 'Authentication' tab. The 'Authentication Methods' section contains '(Allow All MAC AUTH)'. The 'Authentication Sources' section contains a list of sources: '[Endpoints Repository] [Local SQL DB]', 'IP Phones [Static Host List]', and 'IoT device [Static Host List]'. The 'Strip Username Rules' checkbox is unchecked.

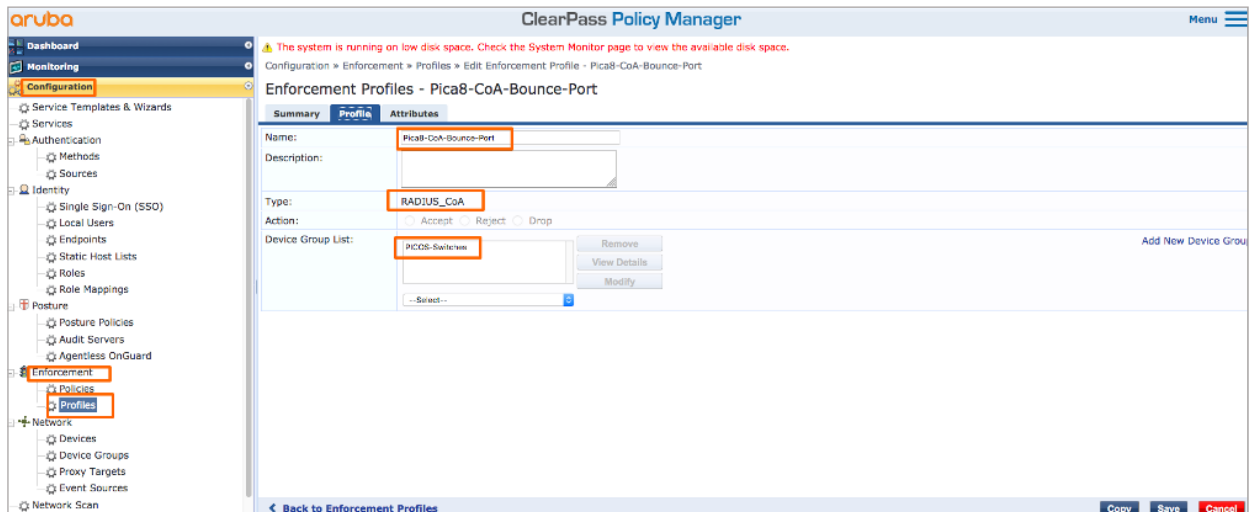
On the **Enforcement** tab, set **Enforcement Policy** to **Pica8-MAC-Auth-Policy**. It includes rules 3 and 4 shown below for Central Web Authentication (CWA) and rule 1 for IP Phone devices and rule 2 for IoT devices. Click **Save**.



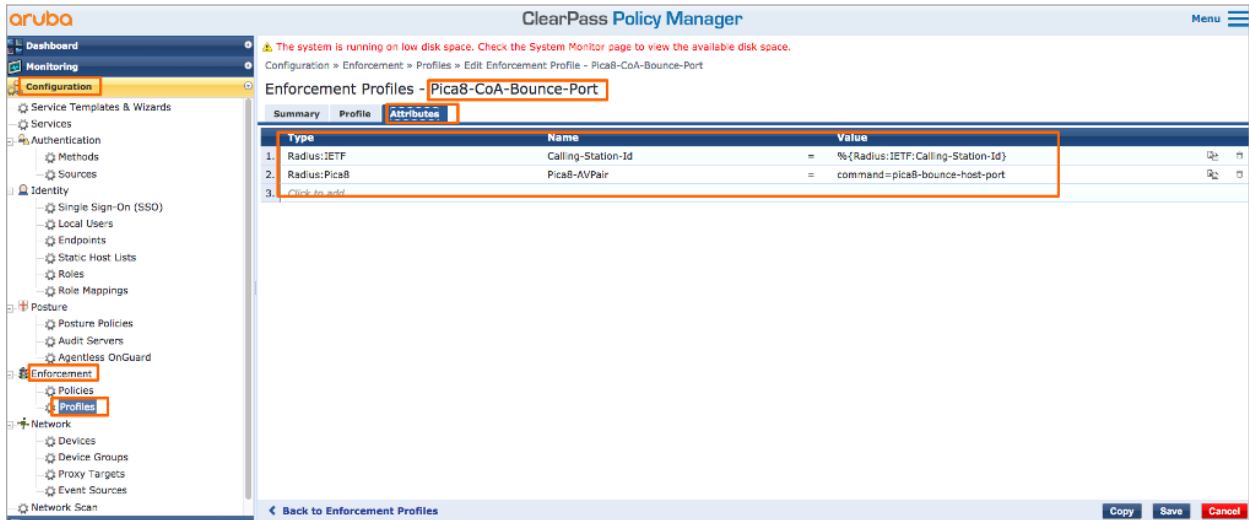
5. Configure the Central Web Authentication enforcement profile.

This profile is configured as a RADIUS Change of Authorization (CoA) profile. It tells Aruba ClearPass to send a RADIUS CoA to the switch.

Select **Configuration->Enforcement->Profiles**, click Add to add a new profile as **Pica8-CoA-Bounce-Port** as shown below. Select template **Radius Dynamic Authorization** and select **PICOSwitches** Devices Group List.



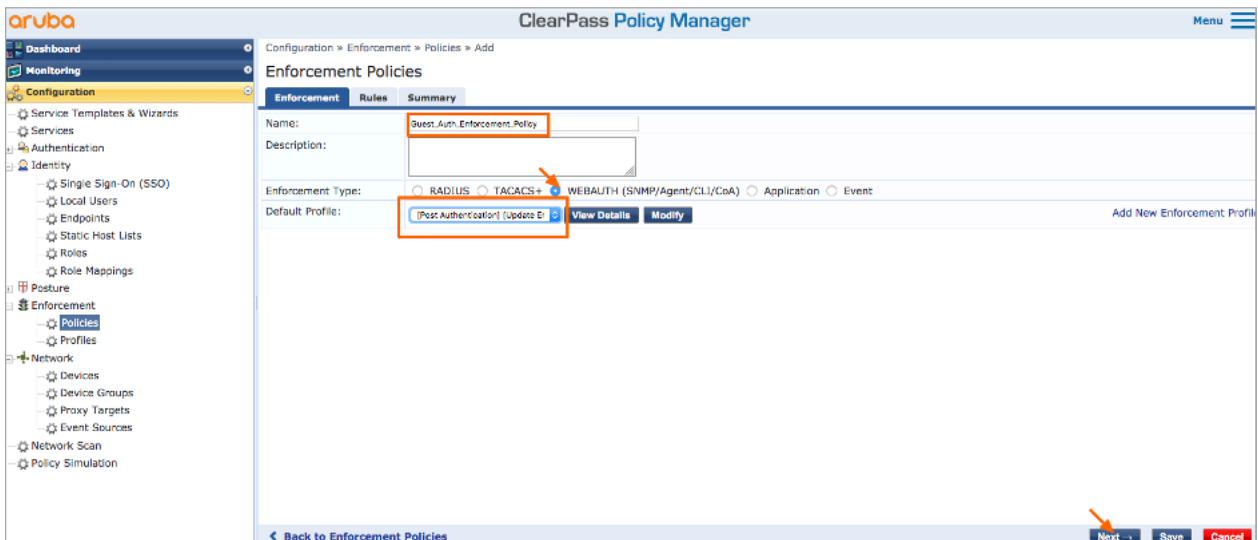
On the **Attributes** tab, enter the attributes as shown below and click **Save**.



6. Configure the Web authentication enforcement policy.

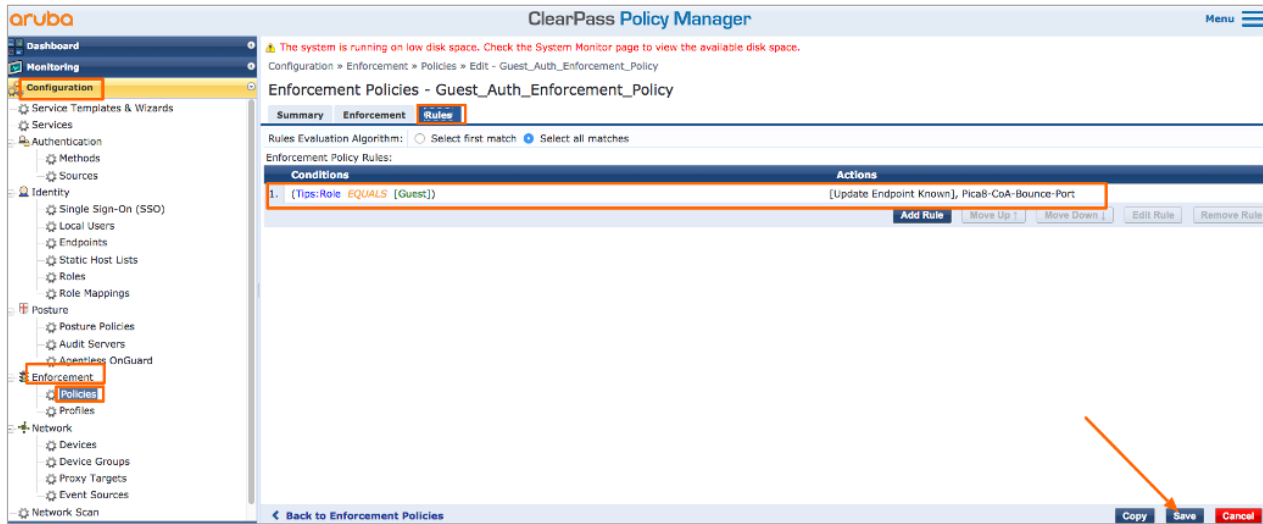
This policy takes effect after the guest is redirected to the Aruba ClearPass Guest and ClearPass Guest authenticates the guest. It tells Aruba ClearPass to add the endpoint to the endpoint repository and marks its status as a known client. It also sends the **Pica8-CoA-Bounce-Port COA** message to the port.

Select **Configuration->Enforcement->Policies**, click **Add**. On the **Enforcement** tab, type the name of the policy as **Guest Auth Enforcement Policy** and set Default Profile to **[Post Authentication][Update Endpoint Known]**. This is a predefined profile that results in the endpoint being added as a known endpoint in the endpoint repository.



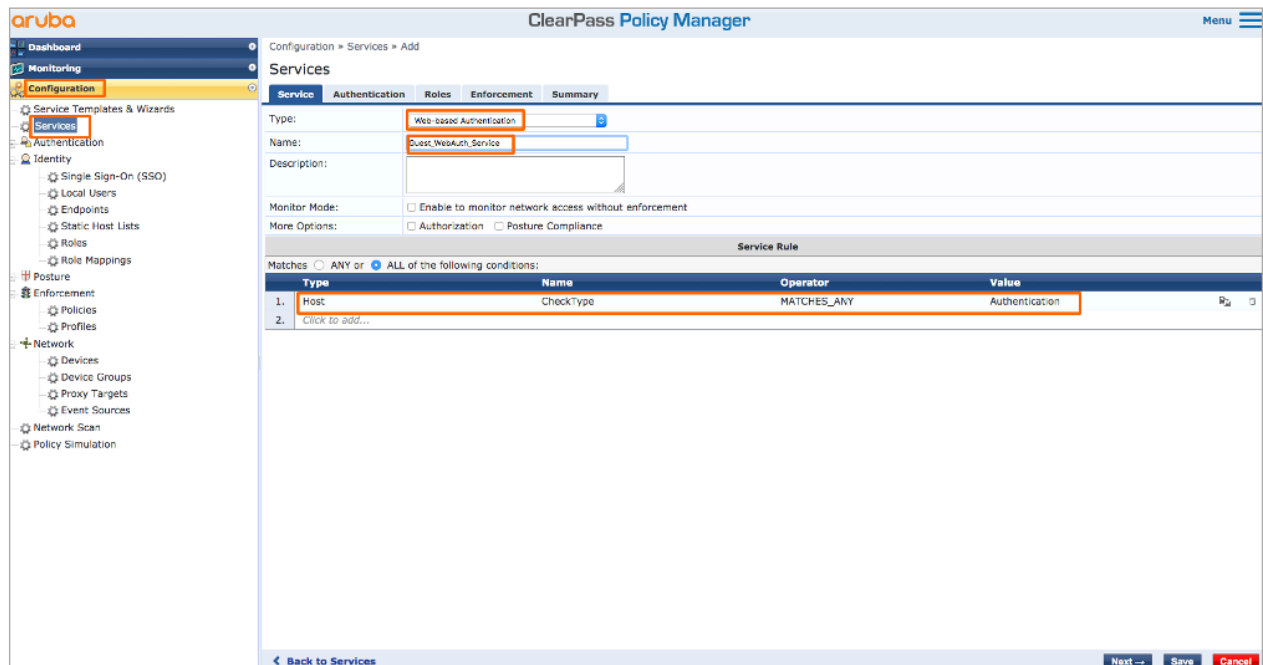
On the **Rules** tab, click **Add Rule** and add the rule shown below.

This rule tells Aruba ClearPass to apply the **Pica8-CoA-Bounce-Port** enforcement profile to any endpoint. Click **Save** as shown below.

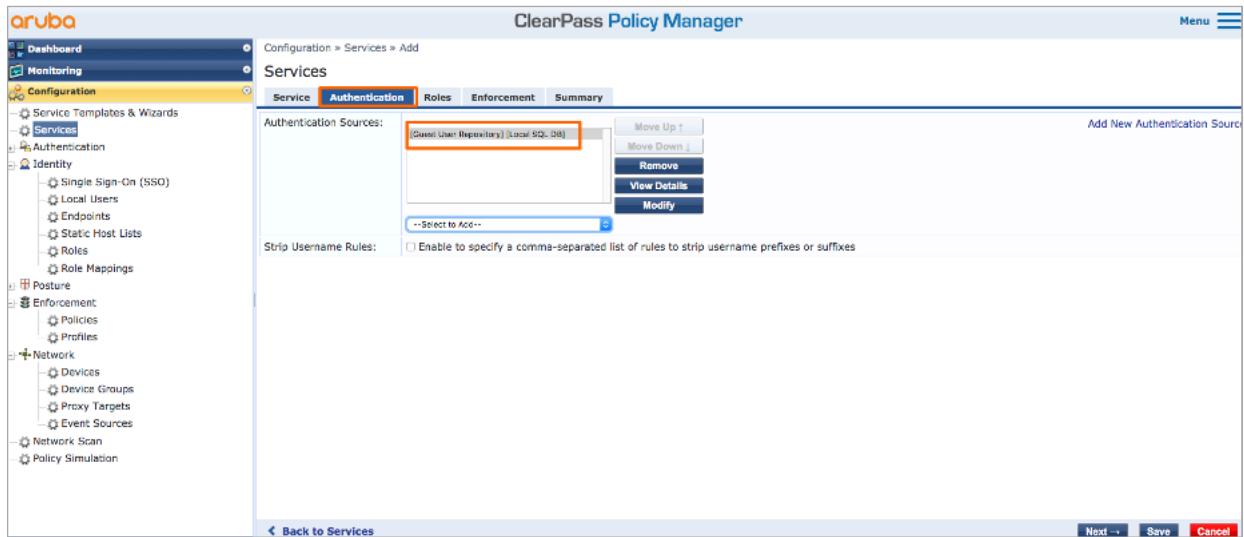


7. Configure the Web-based authentication service.

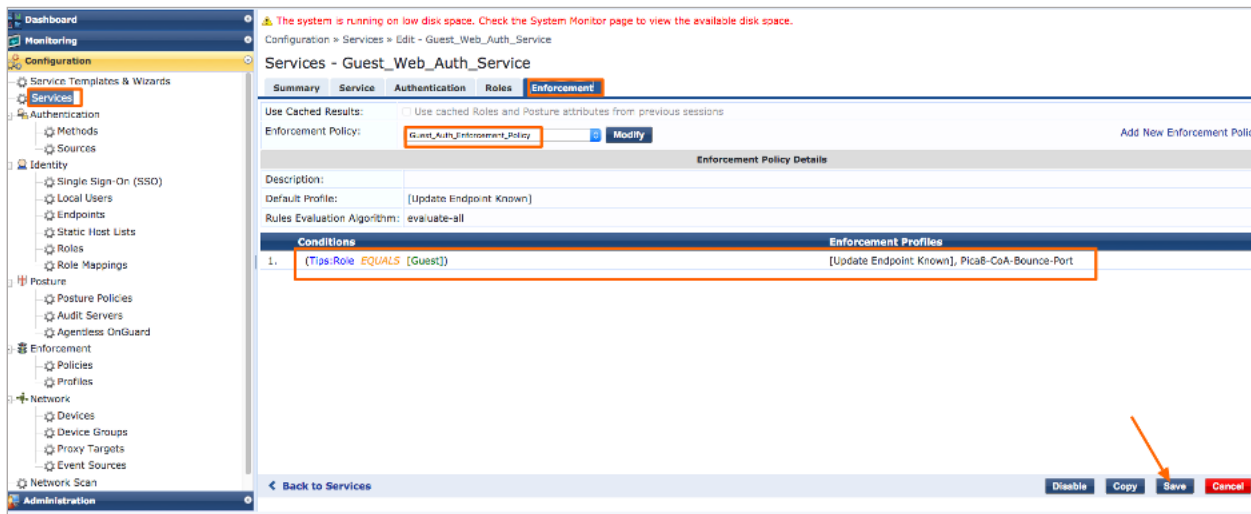
Select **Configuration -> Services**, click **Add**. On the **Service** tab, fill out the fields as shown below. Select **Web-based Authentication service** type. It allows Web-based authentication requests from any client. Fill our Service Name as **Guest_Web_Auth_Service**.



On the **Authentication** tab, set **Authentication Sources** to **[Guest User Repository][Local SQL DB]** as shown below.



On the **Enforcement** tab, set **Enforcement Policy** to **Guest_Auth_Enforcement_Policy**. Click **Save**.



Verifying the NAC Configuration

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

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# run show dot1x interface gigabit-ethernet ge-1/1/7
Interface ge-1/1/7:
```

```
=====
Client MAC           : 10:9a:dd:43:06:02
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.

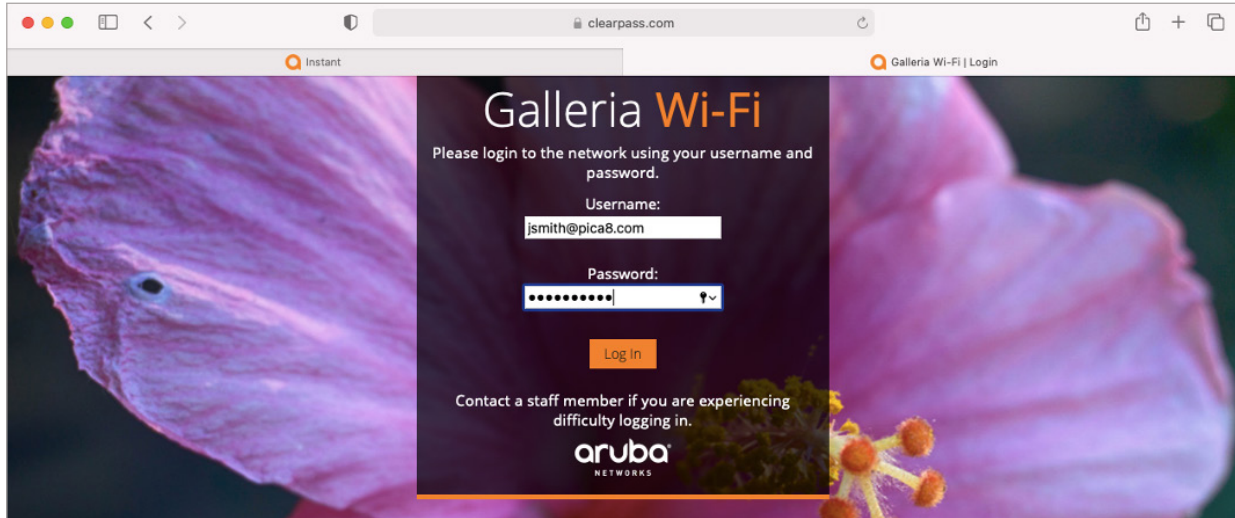
You can see Guest Registration portal URL is presented to the Endpoint Browser. On the PicOS switch run the following CLI to verify.

```
admin@P8-Access-BR-1-SW-2# run show dot1x interface gigabit-ethernet ge-1/1/7
Interface ge-1/1/7:
=====
Client MAC           : 10:9a:dd:43:06:02
Status               : unauthorized
Redirect URL         : https://www.clearpass.com/guest/weblogin.
                     php/2?&mac=10:9a:dd:43:06:02
=====
```

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

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



On the ClearPass Policy Manager UI, click **Monitoring -> Access Tracker** and click on the request entry to see the details as shown below.

#	Server	Source	Username	Service	Login Status	Request Timestamp
1.	192.168.42.110	RADIUS	10:9a:dd:43:06:02	Pica8-MAB	ACCEPT	2022/03/11 14:13:48
2.	192.168.42.110	WEBAUTH	jsmith@pica8.com	Guest_Web_Auth_Service	ACCEPT	2022/03/11 14:13:35
3.	192.168.42.110	RADIUS	10:9a:dd:43:06:02	Pica8-MAB	ACCEPT	2022/03/11 14:10:57
4.	192.168.42.110	RADIUS	10:9a:dd:43:06:02	Pica8-MAB	ACCEPT	2022/03/11 14:03:57
5.	192.168.42.110	RADIUS	38:17:c3:c0:a1:68	Pica8-MAB	ACCEPT	2022/03/09 13:27:22
6.	192.168.42.110	RADIUS	38:17:c3:c0:a1:68	Pica8-MAB	ACCEPT	2022/03/09 12:01:42
7.	192.168.42.110	RADIUS	38:17:c3:c0:a1:68	Pica8-MAB	ACCEPT	2022/03/09 11:49:22
8.	192.168.42.110	RADIUS	38:17:c3:c0:a1:68	Pica8-MAB	ACCEPT	2022/03/09 11:42:22
9.	192.168.42.110	RADIUS	38:17:c3:c0:a1:68	Pica8-MAB	ACCEPT	2022/03/09 11:36:54
10.	192.168.42.110	RADIUS	00:c1:b1:e5:0a:f6	Pica8-MAB	ACCEPT	2022/03/09 10:48:29
11.	192.168.42.110	RADIUS	00:c1:b1:e5:0a:f6	Pica8-MAB	ACCEPT	2022/03/09 10:46:54

In ClearPass Policy Manager double click on second log to see the details of Guest_Web_auth_Service as shown below:

Request Details ✕

Summary
Input
Output

Login Status:	ACCEPT
Session Identifier:	W00000001-01-622bc98c
Date and Time:	Mar 11, 2022 14:13:35 PST
End-Host Identifier:	109add430602
Username:	jsmith@pica8.com
Access Device IP/Port:	-
Access Device Name:	-
System Posture Status:	UNKNOWN (100)

Policies Used -

Service:	Guest_Web_Auth_Service
Authentication Method:	Not applicable
Authentication Source:	[Guest User Repository]
Authorization Source:	[Guest User Repository]
Roles:	[Guest], [User Authenticated]
Enforcement Profiles:	[Update Endpoint Known], Pica8-CoA-Bounce-Port

◀ Showing 2 of 1-4 records ▶

Change Status
Show Configuration
Export
Show Logs
Close

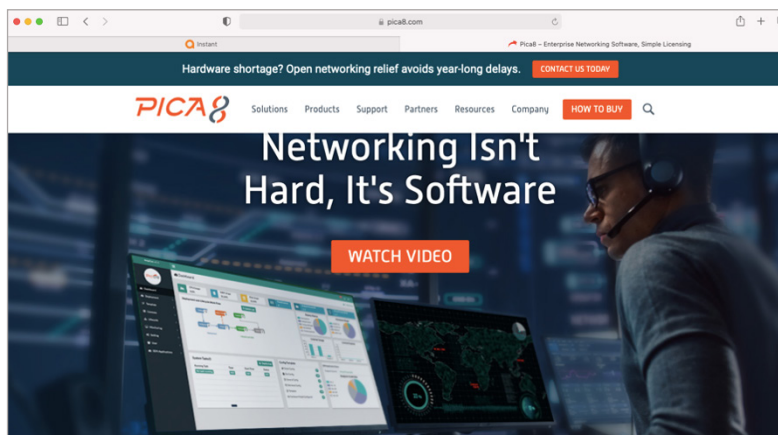
After Guest is successfully authorized, run the following CLI on the switch to verify. Here you can see VLAN 10 and mac_auth_policy_1 ACL are dynamically assigned to ge-1/1/7 port.

```
admin@P8-Access-BR-1-SW-2# run show dot1x interface gigabit-ethernet ge-1/1/7
Interface ge-1/1/7:
=====
Client MAC           : 10:9a:dd:43:06:02
Status               : authorized
Success Auth Method  : MAB
Last Success Time    : Fri Mar 11 14:20:17 2022
Traffic Class        : Other
Dynamic VLAN ID      : 10 (active)
Dynamic Filter Name   : mac_auth_policy_1 (active)
=====
```

In ClearPass Policy Manager double click on second log to see the details of Pica8_MAB as shown below:

Request Details		
Summary	Input	Output
Login Status:	ACCEPT	
Session Identifier:	R00000016-01-622bc99c	
Date and Time:	Mar 11, 2022 14:13:48 PST	
End-Host Identifier:	10-9A-DD-43-06-02	
Username:	10:9a:dd:43:06:02	
Access Device IP/Port:	192.168.42.170:7 (P8-Access-BR-1-SW-2 / Pica8)	
Access Device Name:	P8-Access-BR-1-SW-2	
System Posture Status:	UNKNOWN (100)	
Policies Used -		
Service:	Pica8-MAB	
Authentication Method:	MAC-AUTH	
Authentication Source:	Local:localhost	
Authorization Source:	[Endpoints Repository]	
Roles:	[User Authenticated]	
Enforcement Profiles:	SE-LAB-VLAN, Pica8-Dynamic-ACL	
Showing 1 of 1-4 records Change Status Show Configuration Export Show Logs Close		

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.



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 ClearPass 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 Detect-Num	Status	Priority	Retry-Interval	Retry-Num	Detect-Interval	Consecutive-
192.168.42.110	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
<i><output suppressed></i>						
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 192.168.42.110 shared-key
    "cGljYThwaWNhOA=="
set protocols dot1x aaa radius authentication server-ip 192.168.42.1110 retry-interval 1
set protocols dot1x aaa radius authentication server-ip 192.168.42.110 retry-num 3
set protocols dot1x aaa radius authentication server-ip 192.168.42.110 detect-interval 5
set protocols dot1x aaa radius authentication server-ip 192.168.42.110 consecutive-detect-num 3
set protocols dot1x aaa radius dynamic-author client 192.168.42.110 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
    192.168.42.110/32
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 : 192.168.42.110/32
  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 192.168.42.110/32  
                        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](#)

ClearPass

The following lists reference materials related to ClearPass:

- [6.8 ClearPass Getting Started Guide](#)
- [6.8 ClearPass Deployment Guide](#)