LAB GUIDE

Local User Roles in AOS-CX

!!IMPORTANT!!

THIS GUIDE ASSUMES THAT THE AOS-CX SWITCH SIMULATOR HAS BEEN INSTALLED AND WORKS IN GNS3 OR EVE-NG. PLEASE REFER TO GNS3/EVE-NG INITIAL SETUP LABS IF REQUIRED.

AT THIS TIME, EVE-NG DOES NOT SUPPORT EXPORTING/IMPORTING AOS-CX STARTUP-CONFIG. THE LAB USER SHOULD COPY/PASTE THE AOS-CX NODE CONFIGURATION FROM THE LAB GUIDE AS DESCRIBED IN THE LAB GUIDE IF REQUIRED.

TABLE OF CONTENTS

Lab Objective

This workshop will provide guidance on how to configure Local User Roles in AOS-CX and how to authenticate clients or devices to use user roles. You will learn how to configure local user roles and how to configure an enforcement policy in ClearPass.

Lab Overview

User Roles

Aruba CX switches provides the ability to simplify the burden of configuration, grouping policies and port attributes into a “role” that can be referenced by many device or user types.

Roles can be configured locally on the switch using a Local User Role (LUR) or on ClearPass Policy Manager, using a downloadable user role (DUR). Roles that are configured locally can be assigned via any RADIUS server, using the Aruba-User-Role VSA. When using DUR, the ClearPass Aruba-CPPM-Role VSA (or using the “standard” option in the enforcement policy UI) is used in combination with HTTPS to transfer the role to the switch.

A role at a minimum will dictate what VLAN is to be assigned (trunk or access) and if the traffic is locally switched, or if tunneled back to an Aruba Mobility Gateway. Optionally, a role can also assign a policy (ACL/QOS), reauthentication timers, and a captive portal redirect. The same CLI syntax is used if it is pre-defined on a switch (local roles) or downloaded from ClearPass, it must exist on the switch before it can be applied to a user/device. The switch still needs the CLI commands to parse and apply to the user or device.

Lab Network Layout

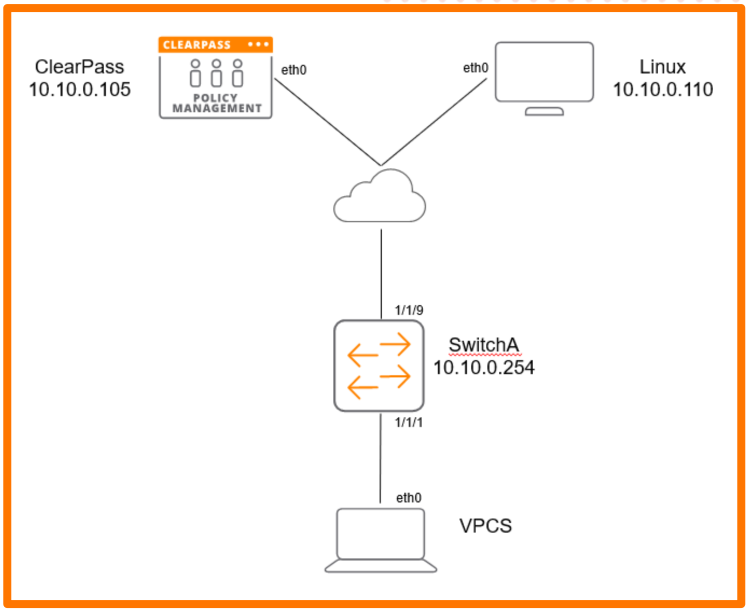


Figure 1. Lab topology and addresses

If using an external ClearPass, the topology would look like the example in Figure 2.

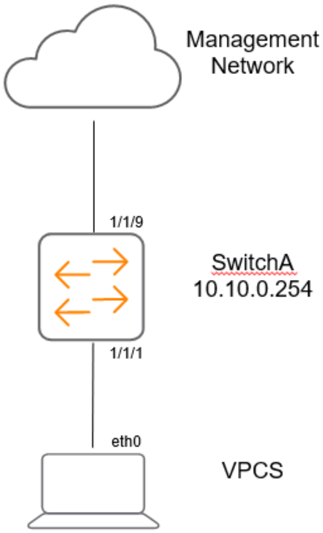


Figure 2. Example EVE-NG topology – external ClearPass

Lab Tasks

Task 1 - Lab setup

Note:

There are various ways to install a RADIUS server in EVE-NG. As this is an Aruba lab, ClearPass Policy Manager will be used. ***Refer to Appendix B*** to explore how to install ClearPass within EVE-NG, else you can point your EVE-NG instance and switch to the same network as the ClearPass server for RADIUS authentication. ClearPass will need to be accessible from a web browser to configure the enforcement policy if accessing outside of EVE-NG.

1. In GNS3/EVE-NG, create the topology as shown in Figure 1.
2. A Windows or Linux desktop will need to be pre-installed into EVE-NG to access ClearPass and configure. For the purposes of this lab, a customized EVE-NG Ubuntu server distribution was installed. Instructions on how to do this for EVE-NG environments can be found here:

   https://www.eve-ng.net/index.php/documentation/howtos/howto-create-own-linux-host-image/
3. Start the devices
4. Open the switch console and log in with the user “admin” and no password
5. Change the password when prompted to the desired new password (ex: admin)

Task 2 – Switch Configuration

1. Change the switch hostname to SwitchA as shown in the topology

```
switch# configure
switch(config)# hostname SwitchA
SwitchA(config)#
```

2. On the switch, bring up the required uplink port.

```
SwitchA# configure
SwitchA (config)# int 1/1/9
SwitchA (config-if)# no shut
SwitchA (config-if)# no routing
```

3. Bring up the client port.

```
SwitchA# configure
SwitchA (config)# int 1/1/1
SwitchA (config-if)# no shut
SwitchA (config-if)# no routing
```

4. Configure the VLAN and gateway IP address that will be used for connectivity.

```
vlan 10
interface vlan 10
ip address 10.10.0.254/24
```

5. Configure the uplink port to be able to access the connectivity VLAN.

```
interface 1/1/9
no shutdown
no routing
```

```
vlan access 10
```

6. Validate the switch has connectivity to ClearPass.

```
Switch-A# ping 10.10.0.105
PING 10.10.0.105 (10.10.0.105) 100(128) bytes of data.
108 bytes from 10.10.0.105: icmp_seq=1 ttl=64 time=1.36 ms
108 bytes from 10.10.0.105: icmp_seq=2 ttl=64 time=2.17 ms
108 bytes from 10.10.0.105: icmp_seq=3 ttl=64 time=1.17 ms
108 bytes from 10.10.0.105: icmp_seq=4 ttl=64 time=1.05 ms
108 bytes from 10.10.0.105: icmp_seq=5 ttl=64 time=1.12 ms

--- 10.10.0.105 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 1.055/1.379/2.175/0.411 ms
```

7. Configure the RADIUS server.

```
SwitchA(config)#radius-server host 10.10.0.105 key plaintext admin
```

8. From the configuration context, configure a local role on the switch using the `port-access role` command.

```
Switch-A(config)#
port-access role User1
poe-priority low
reauth-period 60
vlan access 10
```

Note: Ensure to add “`vlan access 10`” to test the client connectivity.

Optional: Add in other user role attributes for additional practice

```
Switch-A(config)# port-access role User1
Switch-A(config-pa-role)#
  associate              Associate captive-portal-profile or policy with this
                         role.
  auth-mode              Configure authentication mode for this Role.
  cached-reauth-period   Configure cached re-authentication period in the role.
  client-inactivity      Configure client inactivity monitor mode for this Role.
  description            Description for this Role.
  end                    End current mode and change to enable mode.
  exit                   Exit current mode and change to previous mode
  gateway-zone           Configure gateway parameters for the Role.
  list                   Print command list
  mtu                    Configure MTU for this Role.
  no                     Negate a command or set its defaults
  poe-priority           Configure POE priority for this Role.
  reauth-period          Configure reauth period for this Role.
  session-timeout        Configure session timeout for this Role.
  show                   Show running system information
  stp-admin-edge-port    Configure to enable administrative spanning-tree edge
                         port.
  trust-mode             Configure trust mode for this Role.
  vlan                   Configure VLAN mode for this Role.
```

Task 3 – ClearPass Configuration

1. If running ClearPass from within the EVE-NG lab, open the Linux instance, log in using the credentials created in the Lab Setup Step 2 (default credentials - eve/eve).

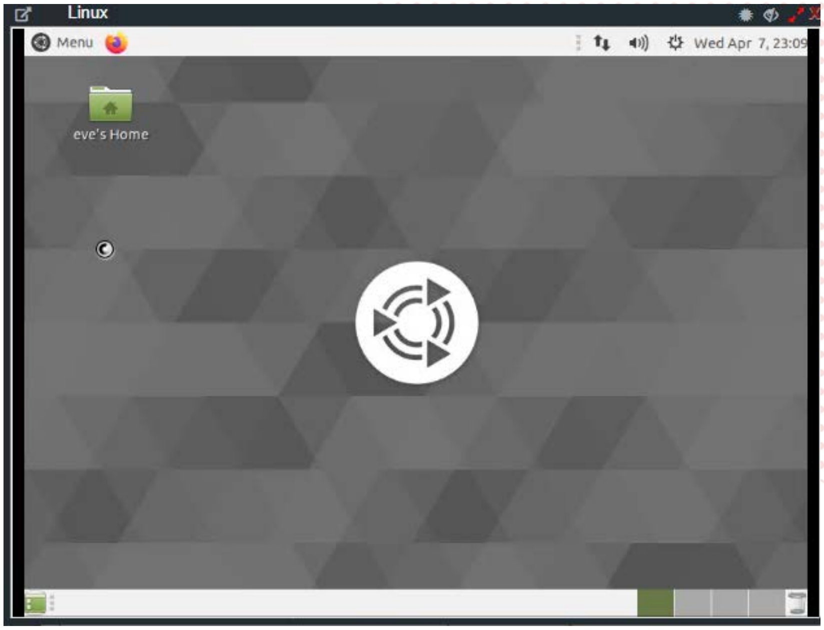


Figure 3. Ubuntu Desktop in EVE-NG

2. Open the Firefox Web Browser in the Linux window and navigate to 10.10.0.105.

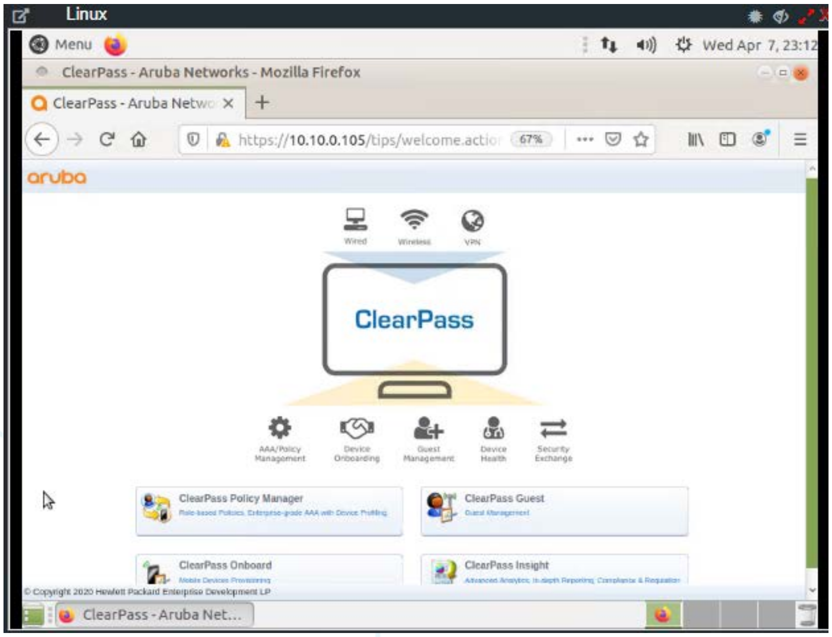
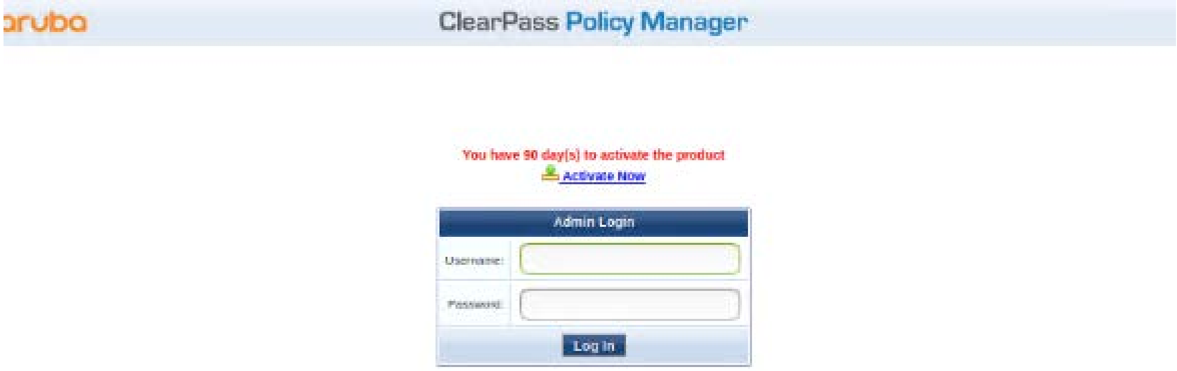

Linux
Menu
Wed Apr 7, 23:12
ClearPass - Aruba Networks - Mozilla Firefox
ClearPass - Aruba Netwo
https://10.10.0.105/tips/welcome.actio
67%
aruba
Wired
Wireless
VPN
ClearPass
AAA/Policy Management
Device Onboarding
Guest Management
Device Health
Security Exchange
ClearPass Policy Manager
Role-based Policies, Enterprise-grade AAA with Device Profiling
ClearPass Guest
Guest Management
ClearPass Onboard
Mobile Devices Provisioning
ClearPass Insight
Advanced Analytics, In-depth Reporting, Compliance & Regulation
© Copyright 2020 Hewlett Packard Enterprise Development LP
ClearPass - Aruba Net...

Figure 4. ClearPass Home Page in Ubuntu Window – EVE-NG

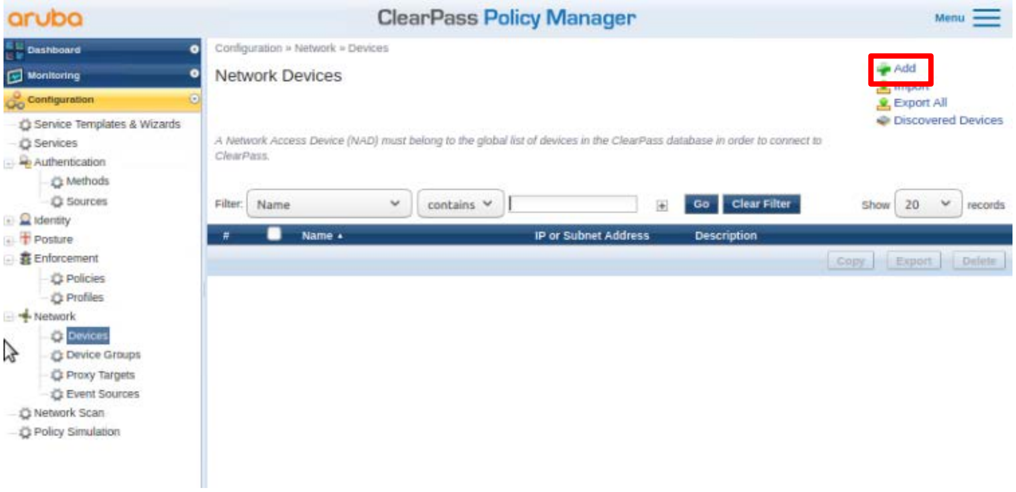
3. Click on the “ClearPass Policy Manager” Button and log into ClearPass with the following credentials, ‘admin/aruba123’.



You have 90 day(s) to activate the product

Figure 5. ClearPass Login Screen

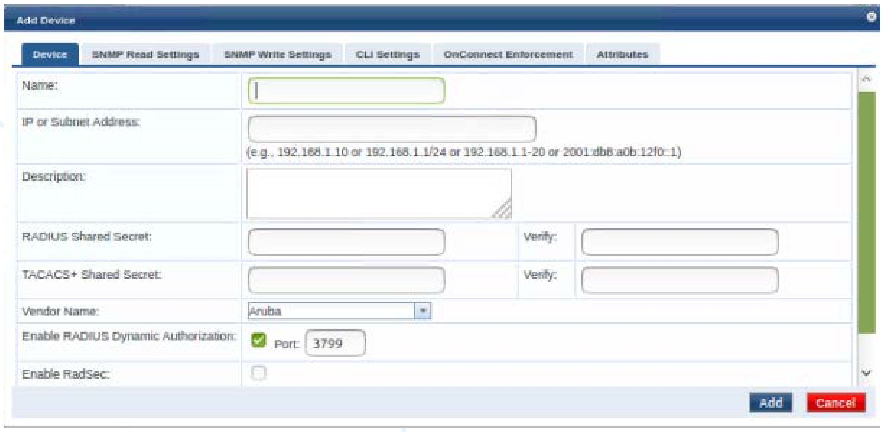
4. Navigate to “Configuration → Network → Devices” and click on Devices, then click on “Add”



A Network Access Device (NAD) must belong to the global list of devices in the ClearPass database in order to connect to ClearPass.

Figure 6. ClearPass Devices window

5. Enter the name of the Switch that will be identified as the authenticating device in ClearPass then enter the RADIUS key and confirm it.



(e.g., 192.168.1.10 or 192.168.1.1/24 or 192.168.1.1-20 or 2001:db8:a0b:12f0::1)

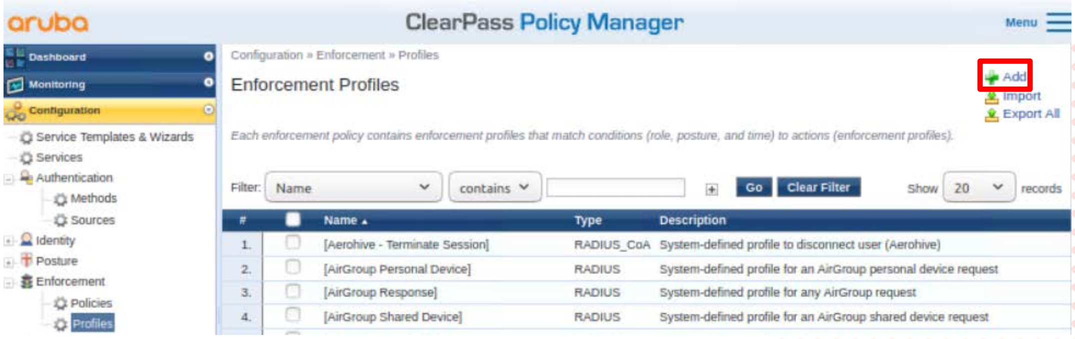
Vendor Name: Aruba

Enable RADIUS Dynamic Authorization: ☑ Port: 3799

Figure 7. ClearPass Add Device Context

Note: The following steps are used to create a ClearPass Enforcement Policy for the purposes of this lab. For best practices in creating ClearPass enforcement policies in production environments, please refer to the ClearPass Policy Manager Documentation - https://www.arubanetworks.com/techdocs/ClearPass/6.9/PolicyManager/Content/home.htm. Also note that this is using MAC Authentication. 802.1x can also be used but for the purposes of this lab.

6. Click on Configuration → Enforcement → Profiles → Add.



Configuration » Enforcement » Profiles

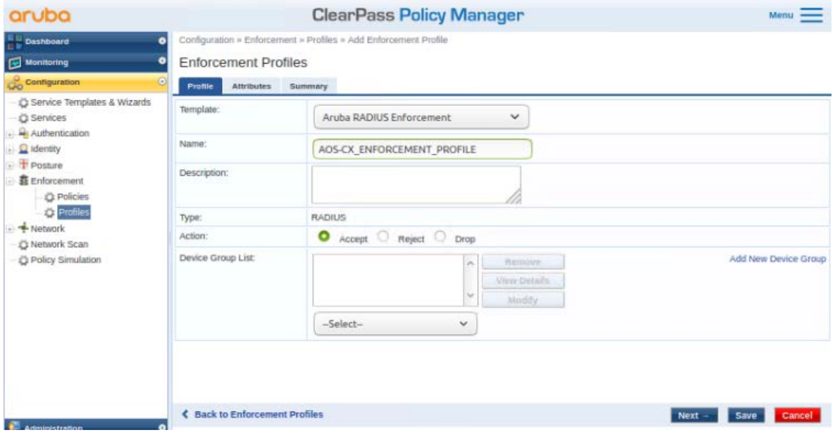
Enforcement Profiles

Each enforcement policy contains enforcement profiles that match conditions (role, posture, and time) to actions (enforcement profiles).

#		Name ▲	Type	Description
1.	□	[Aerohive - Terminate Session]	RADIUS_CoA	System-defined profile to disconnect user (Aerohive)
2.	□	[AirGroup Personal Device]	RADIUS	System-defined profile for an AirGroup personal device request
3.	□	[AirGroup Response]	RADIUS	System-defined profile for any AirGroup request
4.	□	[AirGroup Shared Device]	RADIUS	System-defined profile for an AirGroup shared device request

Figure 8. ClearPass Enforcement Profiles

7. Select the template "Aruba RADIUS Enforcement" and give the new profile a name (Ex: AOS-CX_ENFORCEMENT_PROFILE). Click Next.



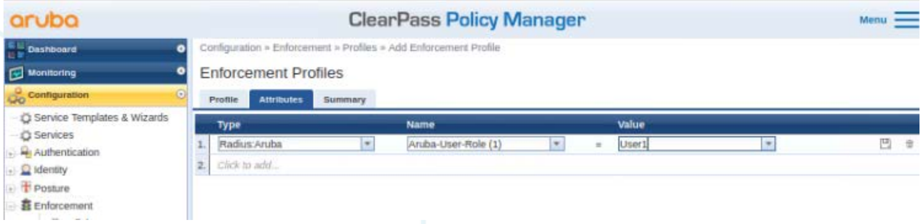
Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Template:	Aruba RADIUS Enforcement
Name:	AOS-CX_ENFORCEMENT_PROFILE
Description:	
Type:	RADIUS
Action:	● Accept ○ Reject ○ Drop
Device Group List:	--Select--

Figure 9. ClearPass Enforcement Profile creation

8. Select as type "Radius:Aruba", Name "Aruba-User-Role", and value as the value created in the switch setup, "User1". Click the "Save" icon (floppy disk). Click Save.



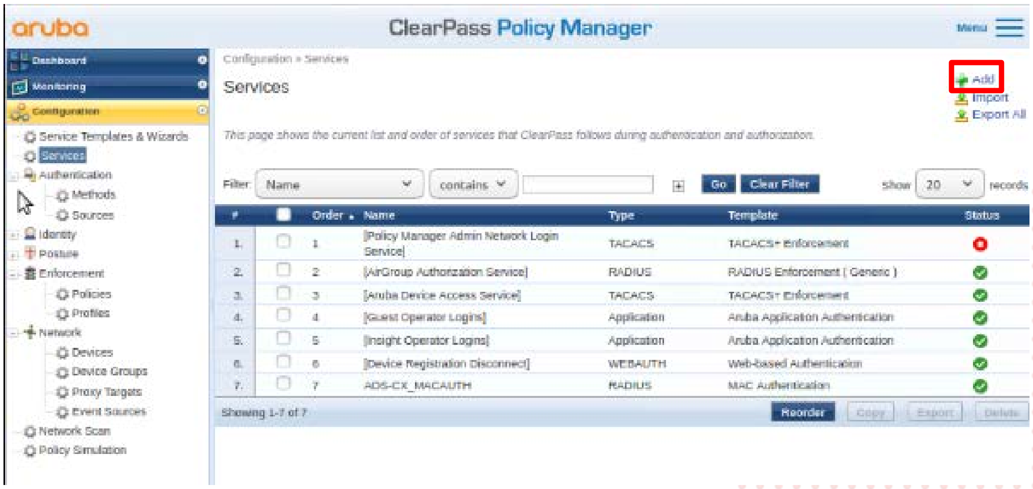
Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role (1)	=	User1
2.	Click to add...			

Figure 10. Aruba User Role Attribute creation

9. In ClearPass, click on Configuration → Services, then click on "Add".



Services

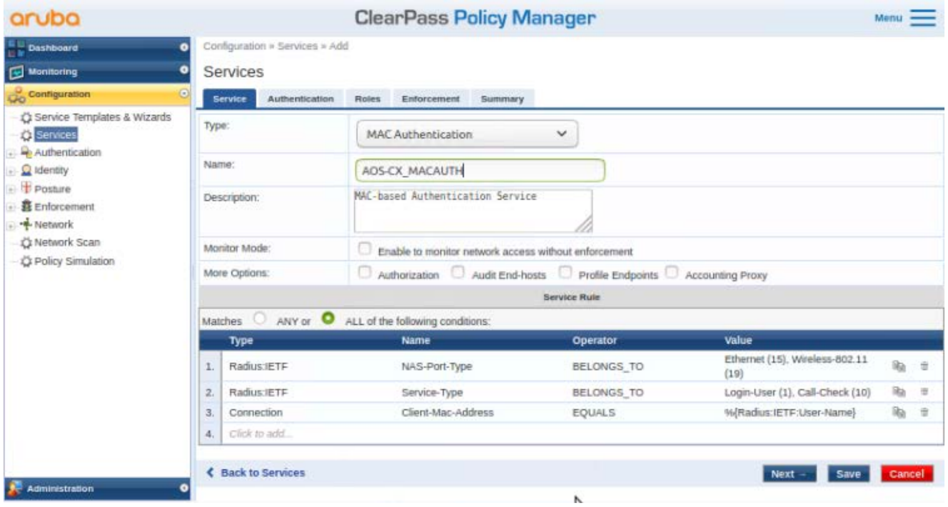
This page shows the current list and order of services that ClearPass follows during authentication and authorization.

#	□	Order ▲	Name	Type	Template	Status
1.	□	1	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	🔴
2.	□	2	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	✓
3.	□	3	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	✓
4.	□	4	[Guest Operator Logins]	Application	Aruba Application Authentication	✓
5.	□	5	[Insight Operator Logins]	Application	Aruba Application Authentication	✓
6.	□	6	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	✓
7.	□	7	AOS-CX_MACAUTH	RADIUS	MAC Authentication	✓

Showing 1-7 of 7

Figure 11. ClearPass Services

10. Select "MAC Authentication" from the drop down and give it a name (Ex: AOS-CX_MACAUTH). Click "Next".



Services

Type: MAC Authentication

Name: AOS-CX_MACAUTH

Description: MAC-based Authentication Service

Monitor Mode: □ Enable to monitor network access without enforcement

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

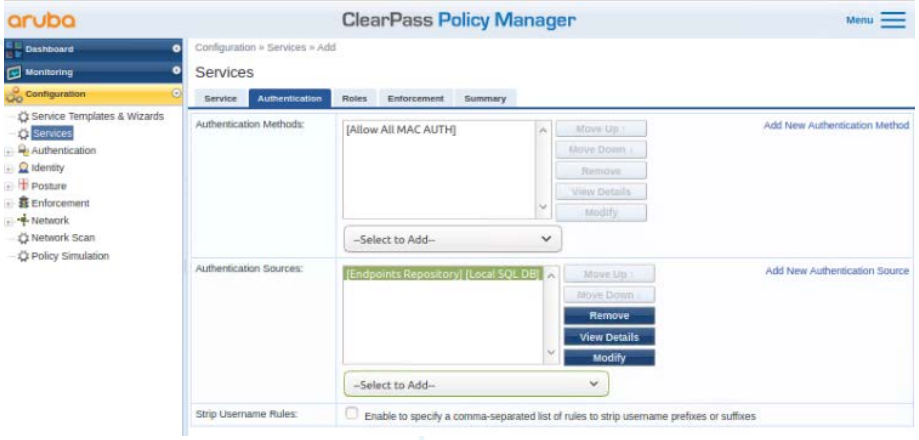
Service Rule

Matches ○ ANY or ● ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	BELONGS_TO	Ethernet (15), Wireless-802.11 (19)
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Call-Check (10)
3.	Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}
4.	Click to add...			

Figure 12. ClearPass MAC Authentication Service

11. Select "Endpoints Repository" from the "Authentication Sources" dropdown, then click "Next". Click "Next" again to skip the configuration of roles (not needed for this lab).



Services

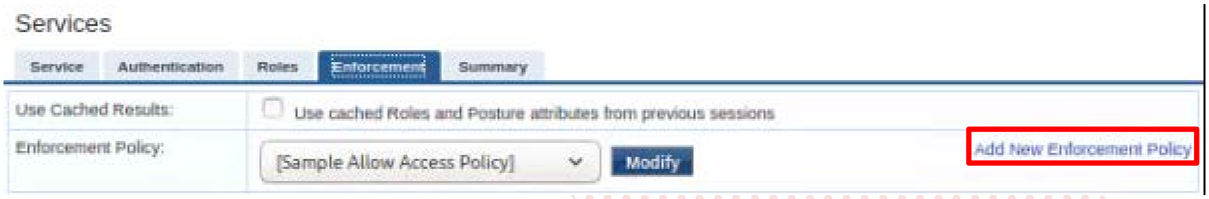
Authentication Methods: [Allow All MAC AUTH]
--Select to Add--

Authentication Sources: [Endpoints Repository] [Local SQL DB]
--Select to Add--

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

Figure 13. ClearPass MAC Authentication Sources

12. From the “Enforcement” tab, click on “Add New Enforcement Policy”.

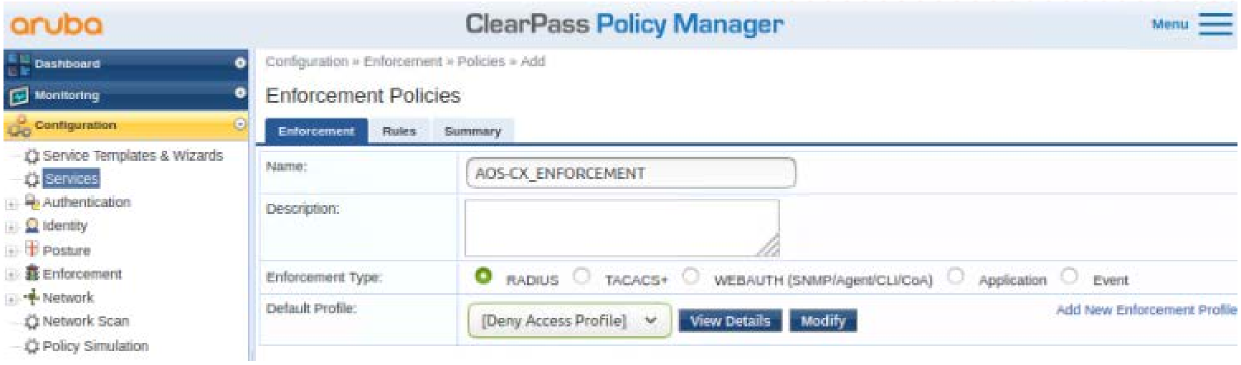


Use Cached Results: □ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: [Sample Allow Access Policy]

Figure 14. ClearPass Enforcement Policy

13. Give the new Enforcement Policy a name (Ex: AOS-CX_ENFORCEMENT) and select “Deny Access Profile” as the default profile. Click “Next”.



Name: AOS-CX_ENFORCEMENT

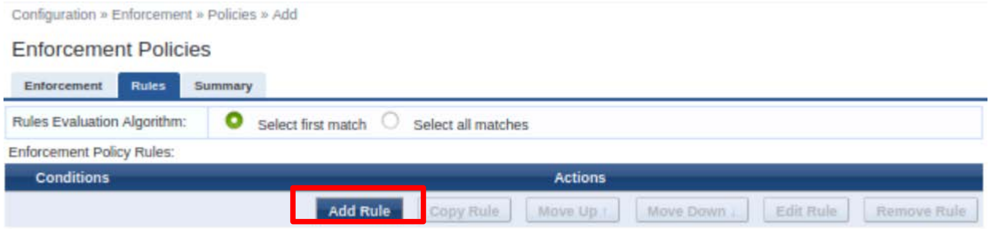
Description:

Enforcement Type: ● RADIUS ○ TACACS+ ○ WEBAUTH (SNMP/Agent/CLI/CoA) ○ Application ○ Event

Default Profile: [Deny Access Profile]

Figure 15. Adding a new Enforcement Policy

14. Click on “Add Rule”.

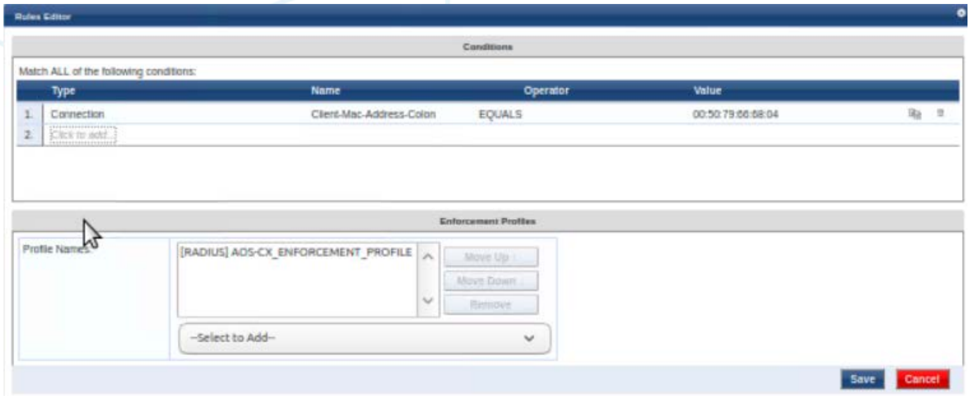


Rules Evaluation Algorithm: ● Select first match ○ Select all matches

Enforcement Policy Rules:

Figure 16. Adding a new Enforcement Policy

15. For the purposes of this lab, we will match on the client’s MAC address, this is the MAC address that was copied from the switch configuration. Enter the Type: Connection, Name: Client-Mac-Address-Colon, Operator: EQUALS, and Value as the client MAC Address previously retrieved. Click “Save” when finished.



Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Connection	Client-Mac-Address-Colon	EQUALS	00:50:79:66:68:04
2.	Click to add...			

Profile Names: [RADIUS] AOS-CX_ENFORCEMENT_PROFILE

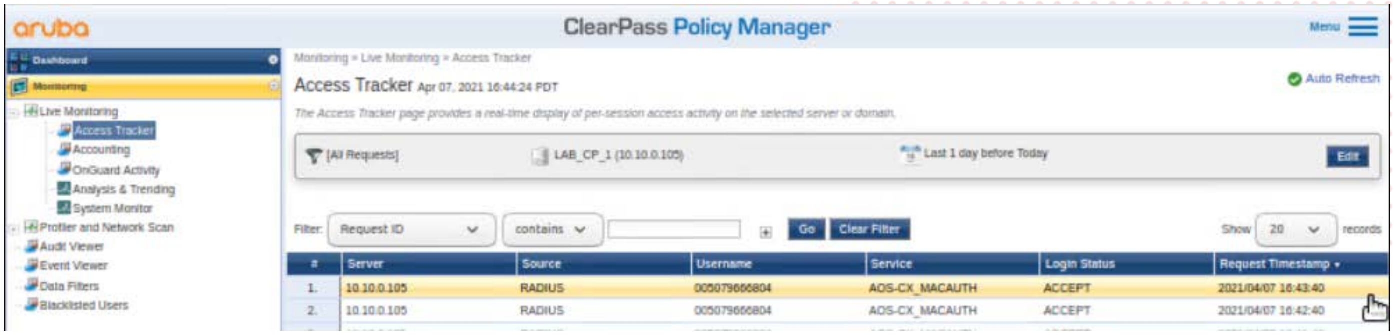
Figure 17. Adding a rule to an enforcement policy

Task 4 – Client Verification and Troubleshooting

1. Open the switch console and run the command “show port-access clients”. You should see output like the following:

```
Switch-A# show port-acc clients

Port Access Clients

Status codes: d device-mode

---------------------------------------------------------------------------------
  Port      MAC-Address       Onboarding     Status      Role
                              Method
---------------------------------------------------------------------------------
  1/1/1     00:50:79:66:68:04 mac-auth       Success     User1
```

Note: If there is no client showing, check the access tracker in ClearPass to see if the authentication is successful. You can find that in Monitoring → Access Tracker. A successful authentication should appear as in Figure 15.



Access Tracker Apr 07, 2021 16:44:24 PDT

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

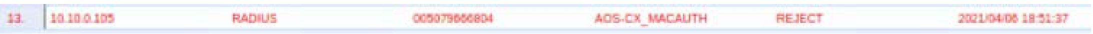
[All Requests] LAB_CP_1 (10.10.0.105) Last 1 day before Today

Filter: Request ID contains Show 20 records

#	Server	Source	Username	Service	Login Status	Request Timestamp ▾
1.	10.10.0.105	RADIUS	005079666804	AOS-CX_MACAUTH	ACCEPT	2021/04/07 16:43:40
2.	10.10.0.105	RADIUS	005079666804	AOS-CX_MACAUTH	ACCEPT	2021/04/07 16:42:40

Figure 18. Successful Authentication in ClearPass Access Tracker

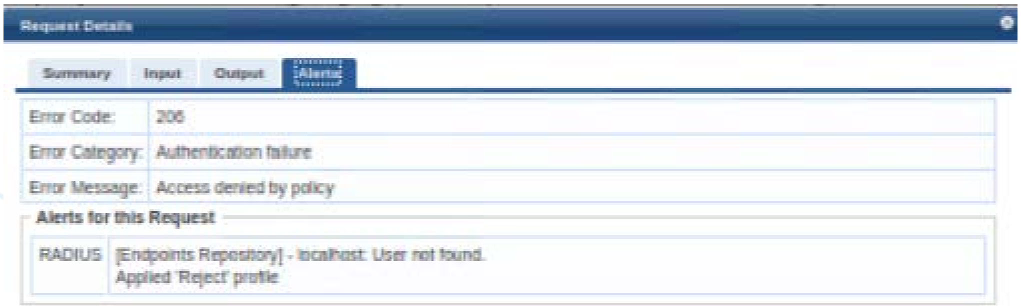
If the authentication were NOT successful, it would appear as a red line.



13.	10.10.0.105	RADIUS	005079666804	AOS-CX_MACAUTH	REJECT	2021/04/06 18:51:37

Figure 19. Unsuccessful Authentication in ClearPass Access Tracker

Click on the line and click on “Alerts” in the resulting window to see the reason why it was rejected.



Error Code:	206
Error Category:	Authentication failure
Error Message:	Access denied by policy

Alerts for this Request

RADIUS	[Endpoints Repository] - localhost: User not found. Applied 'Reject' profile

Figure 20. Unsuccessful Authentication in ClearPass Access Tracker

Also ensure that the user role name on the switch matches what is in the Aruba-User-Role attribute configured in Step 15.

2. Run the command “show port-access role local”, this gives the details of the local user role that was previously configured.

```
Switch-A# show port-access role local

Role Information:

Name  : User1
Type  : local
----------------------------------------------
    Reauthentication Period             : 60 secs
    Cached Reauthentication Period      :
    Authentication Mode                 :
    Session Timeout                     :
    Client Inactivity Timeout           :
    Description                         :
    Gateway Zone                        :
    UBT Gateway Role                    :
    UBT Gateway Clearpass Role          :
    Access VLAN                         : 10
    Native VLAN                         :
    Allowed Trunk VLANs                 :
    Access VLAN Name                    :
    Native VLAN Name                    :
    Allowed Trunk VLAN Names            :
    VLAN Group Name                     :
    MTU                                 :
    QOS Trust Mode                      :
    STP Administrative Edge Port        :
    PoE Priority                        : low
    Captive Portal Profile              :
    Policy                              :
```

3. Run the command “show port-access clients interface 1/1/1 detail”. This gives authentication information on the interface as well as for the role that is applied to the interface.

```
Switch-A# show port-access clients interface 1/1/1 detail

Port Access Client Status Details:

Client 00:50:79:66:68:04, 005079666804
============================
  Session Details
  ---------------
    Port         : 1/1/2
    Session Time : 20s
    IPv4 Address :
    IPv6 Address :

  Authentication Details
  ----------------------
    Status          : mac-auth Authenticated
    Auth Precedence : dot1x - Not attempted, mac-auth - Authenticated

  Authorization Details
  ----------------------
    Role   : User1
    Status : Applied
Role Information:

Name   : User1
Type   : local
----------------------------------------------
    Reauthentication Period             : 60 secs
    Cached Reauthentication Period      :
    Authentication Mode                 :
    Session Timeout                     :
    Client Inactivity Timeout           :
    Description                         :
    Gateway Zone                        :
    UBT Gateway Role                    :
    UBT Gateway Clearpass Role          :
    Access VLAN                         : 10
    Native VLAN                         :
    Allowed Trunk VLANs                 :
    Access VLAN Name                    :
    Native VLAN Name                    :
    Allowed Trunk VLAN Names            :
    VLAN Group Name                     :
    MTU                                 :
    QOS Trust Mode                      :
    STP Administrative Edge Port        :
    PoE Priority                        : low
    Captive Portal Profile              :
    Policy                  :
```

You have completed the lab!

Appendix A – Completed Switch Configuration

SwitchA

```
Current configuration:
!
!Version ArubaOS-CX Virtual.10.06.0001
!export-password: default
hostname Switch-A
user admin group administrators password ciphertext
AQBapeNXXNcbKueh7HOeVthlTeWJz2scUeBv2FMPzj8hb4M0YgAAAB2jfPUflzf3jizRA32/IFkQuGSBlGIYz3alDexN9nM
Ql63VOuT7X+a+YLFLEQ9zMzRsWRJxgr1hS0gnRwyxoOxki0UimxZq
ba1AULPG7RxhtCs2v26SOCsQVQhgV2zqIaql
led locator on
ntp server pool.ntp.org minpoll 4 maxpoll 4 iburst
ntp enable
!
!
!
!
radius-server host 10.10.0.105 key ciphertext
AQBapdAz4irjSK61Zg/CFArsNYWKbn1LObqDD/v9SH1eMQ6ABQAAADY26liu
!
radius dyn-authorization enable
ssh server vrf mgmt
debug portaccess all
vlan 1,10
```

```
interface mgmt
    no shutdown
    ip dhcp
port-access role User1
    poe-priority low
    reauth-period 60
    vlan access 10
aaa authentication port-access mac-auth
    enable
interface 1/1/1
    no shutdown
    no routing
    vlan access 1
    aaa authentication port-access client-limit 5
    aaa authentication port-access mac-auth
        enable
interface 1/1/2
    no shutdown
    no routing
    vlan access 1
    aaa authentication port-access client-limit 5
    aaa authentication port-access mac-auth
        enable
interface 1/1/9
    no shutdown
    no routing
    vlan access 10
interface vlan 10
    ip address 10.10.0.254/24
!
!
!
!
!
ip source-interface radius 10.10.0.254
https-server vrf mgmt
```

Appendix B – EVE-NG ClearPass Installation

Pre-Requisites:

- An Aruba Support Port account will be required to download the ClearPass OVA as well as EVAL licenses.

Steps

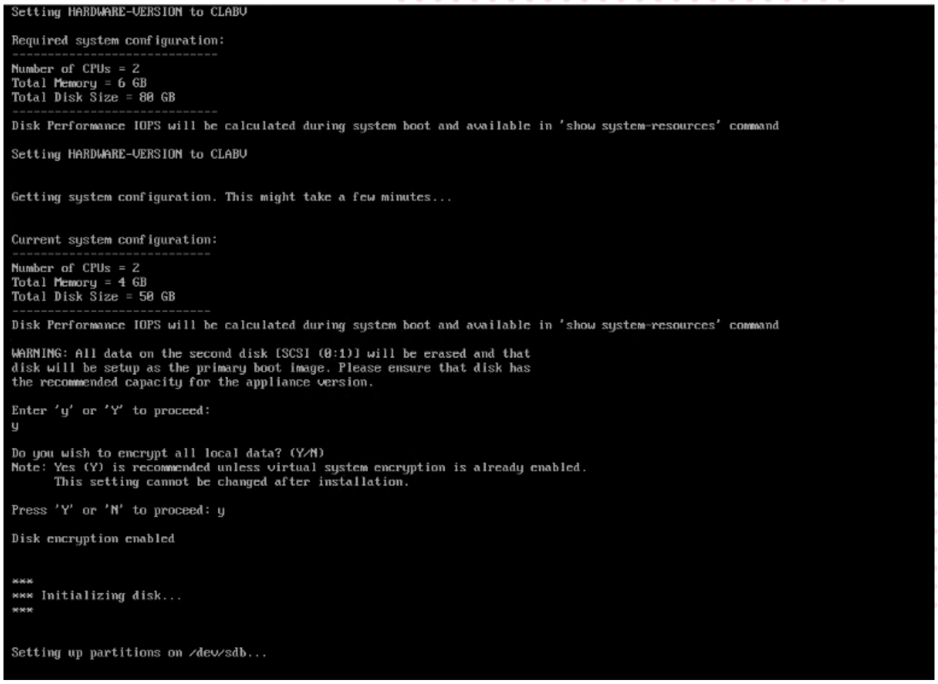
4. To first install the ClearPass OVA into the EVE-NG environment, follow the instructions at this link:

   https://www.eve-ng.net/index.php/documentation/howtos/howto-add-aruba-clearpass/

   This lab uses the latest ClearPass OVA v. 6.9.0, which can be downloaded from the Aruba Support Portal:

   https://asp.arubanetworks.com/downloads

5. Once installed, and the node is created in the EVE-NG lab file, follow the configuration steps for ClearPass. First login to ClearPass using the default credentials (appadmin/eTIPS123). Once entered, the configuration process will begin.

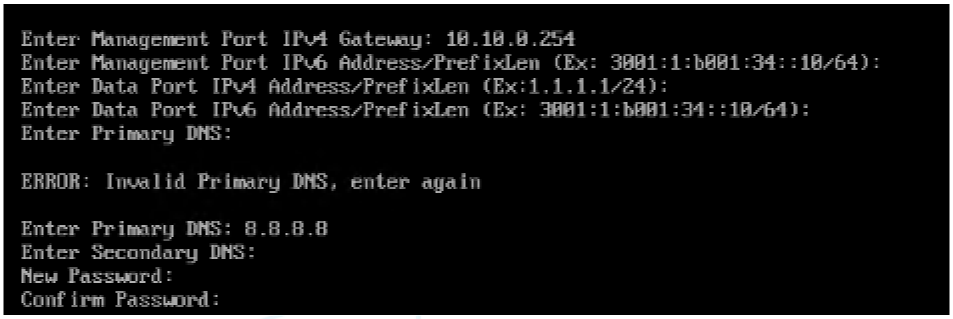


```
Setting HARDWARE-VERSION to CLABV

Required system configuration:
-----------------------------
Number of CPUs = 2
Total Memory = 6 GB
Total Disk Size = 80 GB
-----------------------------
Disk Performance IOPS will be calculated during system boot and available in 'show system-resources' command

Setting HARDWARE-VERSION to CLABV


Getting system configuration. This might take a few minutes...


Current system configuration:
----------------------------
Number of CPUs = 2
Total Memory = 4 GB
Total Disk Size = 50 GB
----------------------------
Disk Performance IOPS will be calculated during system boot and available in 'show system-resources' command

WARNING: All data on the second disk [SCSI (0:1)] will be erased and that
disk will be setup as the primary boot image. Please ensure that disk has
the recommended capacity for the appliance version.

Enter 'y' or 'Y' to proceed:
y

Do you wish to encrypt all local data? (Y/N)
Note: Yes (Y) is recommended unless virtual system encryption is already enabled.
      This setting cannot be changed after installation.

Press 'Y' or 'N' to proceed: y

Disk encryption enabled


***
*** Initializing disk...
***


Setting up partitions on /dev/sdb...
```

Figure 21. ClearPass Installation

Select the CLABV installation, click “Y” to proceed and “Y” to encrypt data.

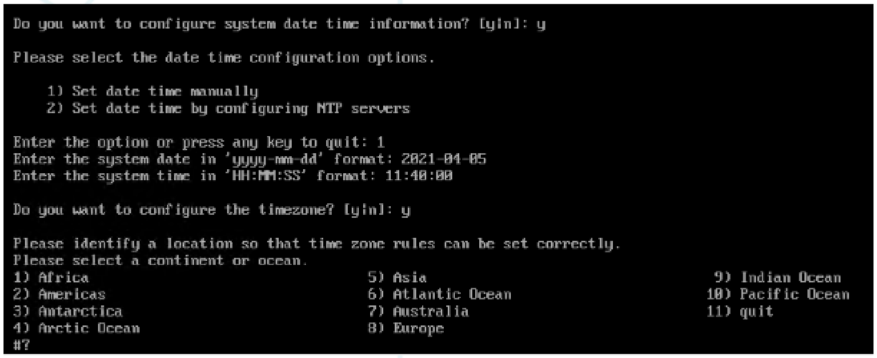
6. Once prompted, enter the IP address as “10.10.0.105”, the mask as “255.255.255.0”, the gateway as “10.10.0.254”, and the DNS as “8.8.8.8” (not needed for this exercise). Configure a new password, this lab example used “aruba123”.



```
Enter Management Port IPv4 Gateway: 10.10.0.254
Enter Management Port IPv6 Address/PrefixLen (Ex: 3001:1:b001:34::10/64):
Enter Data Port IPv4 Address/PrefixLen (Ex:1.1.1.1/24):
Enter Data Port IPv6 Address/PrefixLen (Ex: 3001:1:b001:34::10/64):
Enter Primary DNS:

ERROR: Invalid Primary DNS, enter again

Enter Primary DNS: 8.8.8.8
Enter Secondary DNS:
New Password:
Confirm Password:
```

Figure 22. ClearPass IP Configuration

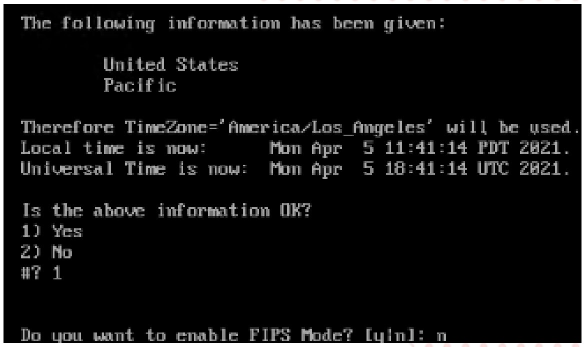
7. Configure the date and time manually as well as the time zone.



```
Do you want to configure system date time information? [y|n]: y

Please select the date time configuration options.

    1) Set date time manually
    2) Set date time by configuring NTP servers

Enter the option or press any key to quit: 1
Enter the system date in 'yyyy-mm-dd' format: 2021-04-05
Enter the system time in 'HH:MM:SS' format: 11:40:00

Do you want to configure the timezone? [y|n]: y

Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa                                  5) Asia                                    9) Indian Ocean
2) Americas                                6) Atlantic Ocean                         10) Pacific Ocean
3) Antarctica                              7) Australia                              11) quit
4) Arctic Ocean                            8) Europe
#?
```

Figure 23. ClearPass Date and Time Configuration

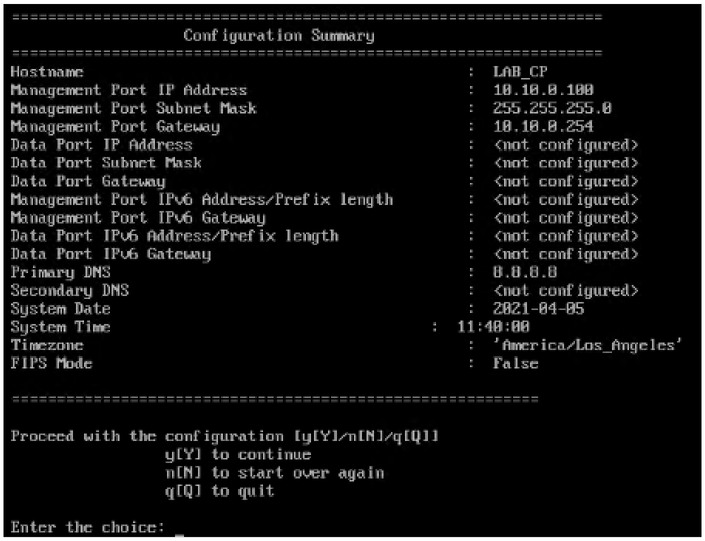
8. Confirm the correct date, time, and time zone.



```
The following information has been given:

        United States
        Pacific

Therefore TimeZone='America/Los_Angeles' will be used.
Local time is now:      Mon Apr  5 11:41:14 PDT 2021.
Universal Time is now:  Mon Apr  5 18:41:14 UTC 2021.

Is the above information OK?
1) Yes
2) No
#? 1


Do you want to enable FIPS Mode? [y|n]: n
```

Figure 24. ClearPass Date and Time Settings Confirmation

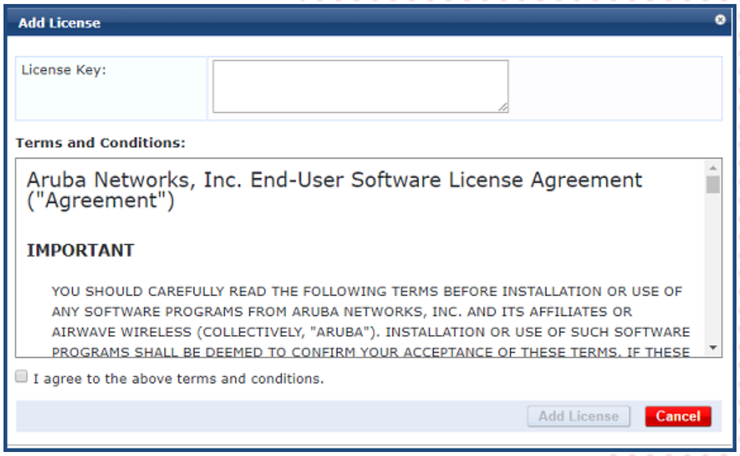
9. Confirm the configured settings are correct. Press Y to save settings.



```
=================================================================
                   Configuration Summary
=================================================================
Hostname                                          :  LAB_CP
Management Port IP Address                        :  10.10.0.100
Management Port Subnet Mask                       :  255.255.255.0
Management Port Gateway                           :  10.10.0.254
Data Port IP Address                              :  <not configured>
Data Port Subnet Mask                             :  <not configured>
Data Port Gateway                                 :  <not configured>
Management Port IPv6 Address/Prefix length        :  <not configured>
Management Port IPv6 Gateway                      :  <not configured>
Data Port IPv6 Address/Prefix length              :  <not configured>
Data Port IPv6 Gateway                            :  <not configured>
Primary DNS                                       :  8.8.8.8
Secondary DNS                                     :  <not configured>
System Date                                       :  2021-04-05
System Time                                   :  11:40:00
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: _
```

Figure 25. ClearPass Configuration Confirmation

10. ClearPass will then reboot and will then allow the user to log in to add licenses. Enter the platform license key retrieved from the Aruba Support Portal Licensing Management System - https://lms.arubanetworks.com/.



Add License

License Key:

Terms and Conditions:

Aruba Networks, Inc. End-User Software License Agreement ("Agreement")

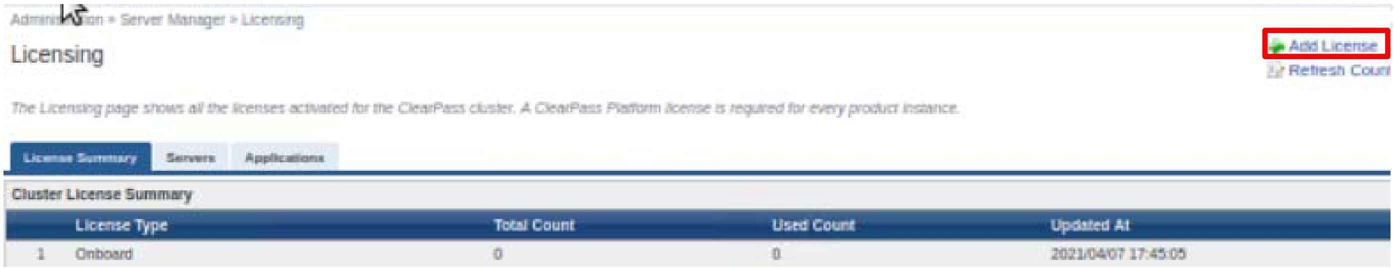
IMPORTANT

YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS BEFORE INSTALLATION OR USE OF ANY SOFTWARE PROGRAMS FROM ARUBA NETWORKS, INC. AND ITS AFFILIATES OR AIRWAVE WIRELESS (COLLECTIVELY, "ARUBA"). INSTALLATION OR USE OF SUCH SOFTWARE PROGRAMS SHALL BE DEEMED TO CONFIRM YOUR ACCEPTANCE OF THESE TERMS. IF THESE

☐ I agree to the above terms and conditions.

Figure 26. ClearPass Platform License entry

11. Once logged into ClearPass, enter the licensing section (Administration → Server Manager → Licensing). Click on "Add License".



Administration » Server Manager » Licensing

Licensing

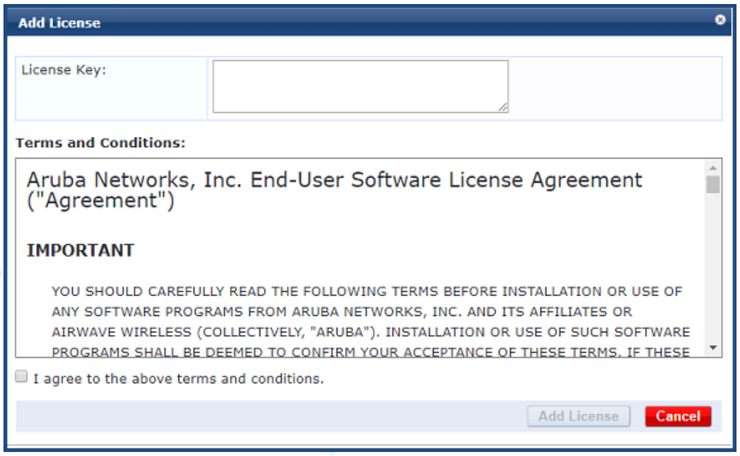
The Licensing page shows all the licenses activated for the ClearPass cluster. A ClearPass Platform license is required for every product instance.

Cluster License Summary

	License Type	Total Count	Used Count	Updated At
1	Onboard	0	0	2021/04/07 17:45:05

Figure 27. ClearPass Add New Server License

12. Add the new license and agree to the terms and conditions. ClearPass will then be ready to configure for authentication.



Add License

License Key:

Terms and Conditions:

Aruba Networks, Inc. End-User Software License Agreement ("Agreement")

IMPORTANT

YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS BEFORE INSTALLATION OR USE OF ANY SOFTWARE PROGRAMS FROM ARUBA NETWORKS, INC. AND ITS AFFILIATES OR AIRWAVE WIRELESS (COLLECTIVELY, "ARUBA"). INSTALLATION OR USE OF SUCH SOFTWARE PROGRAMS SHALL BE DEEMED TO CONFIRM YOUR ACCEPTANCE OF THESE TERMS. IF THESE

☐ I agree to the above terms and conditions.

Figure 28. ClearPass Server license entry

a Hewlett Packard
Enterprise company

www.arubanetworks.com

3333 Scott Blvd. Santa Clara, CA 95054
1.844.472.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | info@arubanetworks.com