LAB GUIDE

RADIUS DOT1X AUTHENTICATION

ARUBA CX SWITCHING WORKSHOP

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

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

TABLE OF CONTENTS

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

Lab Objective

This workshop will provide guidance on how to configure Radius Port-access DOT1X Authentication in AOS-CX and how to authenticate clients or devices. You will learn how to configure Radius port-access DOT1X authentication and how to configure an enforcement policy in Aruba ClearPass.

Lab Overview

IEEE 802.1X is a standard for port-based authentication. This standard provides administrators with an authentication mechanism for devices trying to access a LAN or WLAN. 802.1X defines the encapsulation of the Extensible Authentication Protocol (EAP) over IEEE 802, which is known as EAP over LAN (EAPOL).

802.1X authentication involves the following entities:

- **Supplicant:** Device that tries to access the LAN.
- **Authenticator:** A network device, such as an Ethernet switch that authenticates the supplicant.
- **Authentication Server:** Typically a host running software supporting the RADIUS and EAP protocols that provides an authentication service to the authenticator.

Until the supplicant is authenticated, the authenticator allows only EAPOL traffic through the port to which the supplicant is connected. Only after the authentication is successful, the authenticator allows normal traffic from the supplicant.

802.1X port-based authentication provides port-level security. It allows LAN access only on ports where a single 802.1X-capable client (supplicant) has entered authorized RADIUS user credentials. 802.1X authentication is recommended for applications where only one client can connect to the port at a time. Using this option, the port processes all IP traffic as if it comes from the same client.

Lab Setup

1. In EVE-NG, create the topology as shown in Figure 1.

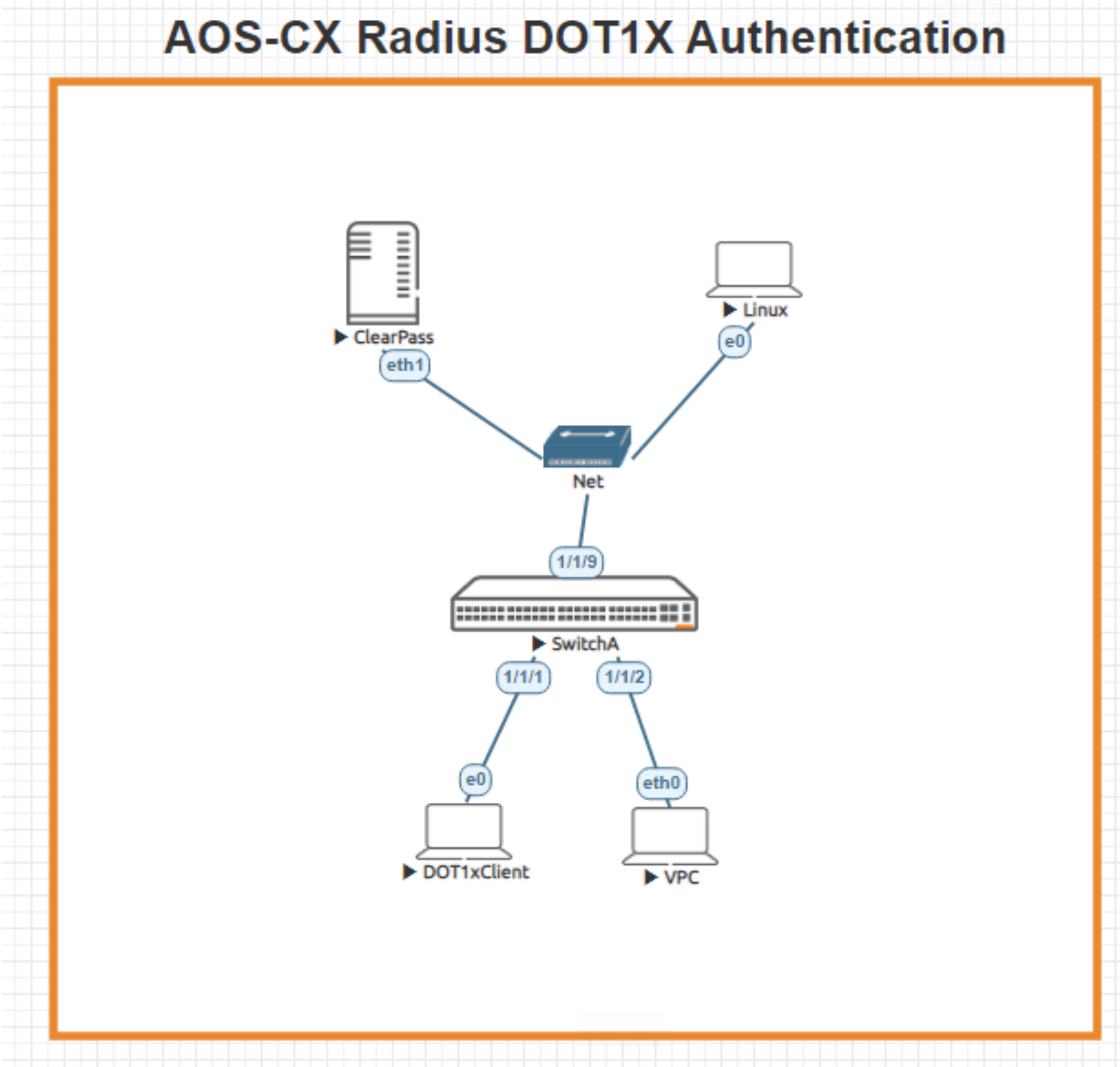


Figure 1. Example EVE-NG topology

Note: For Mac authentication please refer Radius Mac Authentication EVE-NG Lab.

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.

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)
6. Here is an example of IPs and interfaces that will be configured in this guide

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 10.10.0.250
PING 10.10.0.250 (10.10.0.250) 100(128) bytes of data.
108 bytes from 10.10.0.250: icmp_seq=1 ttl=64 time=1.36 ms
108 bytes from 10.10.0.250: icmp_seq=2 ttl=64 time=2.17 ms
108 bytes from 10.10.0.250: icmp_seq=3 ttl=64 time=1.17 ms
```

```
    108 bytes from 10.10.0.250: icmp_seq=4 ttl=64 time=1.05 ms
    108 bytes from 10.10.0.250: icmp_seq=5 ttl=64 time=1.12 ms

    --- 10.10.0.250 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. From the configuration context, enable dot1x and then enable on interface level as below:

```
SwitchA(config)# aaa authentication port-access dot1x authenticator enable

SwitchA# show running-config interface 1/1/1

interface 1/1/1

    no shutdown

    no routing

    vlan access 1

    aaa authentication port-access dot1x authenticator

        enable

    exit

SwitchA#
```

8. Configuring Local user role for dot1x client authorization.

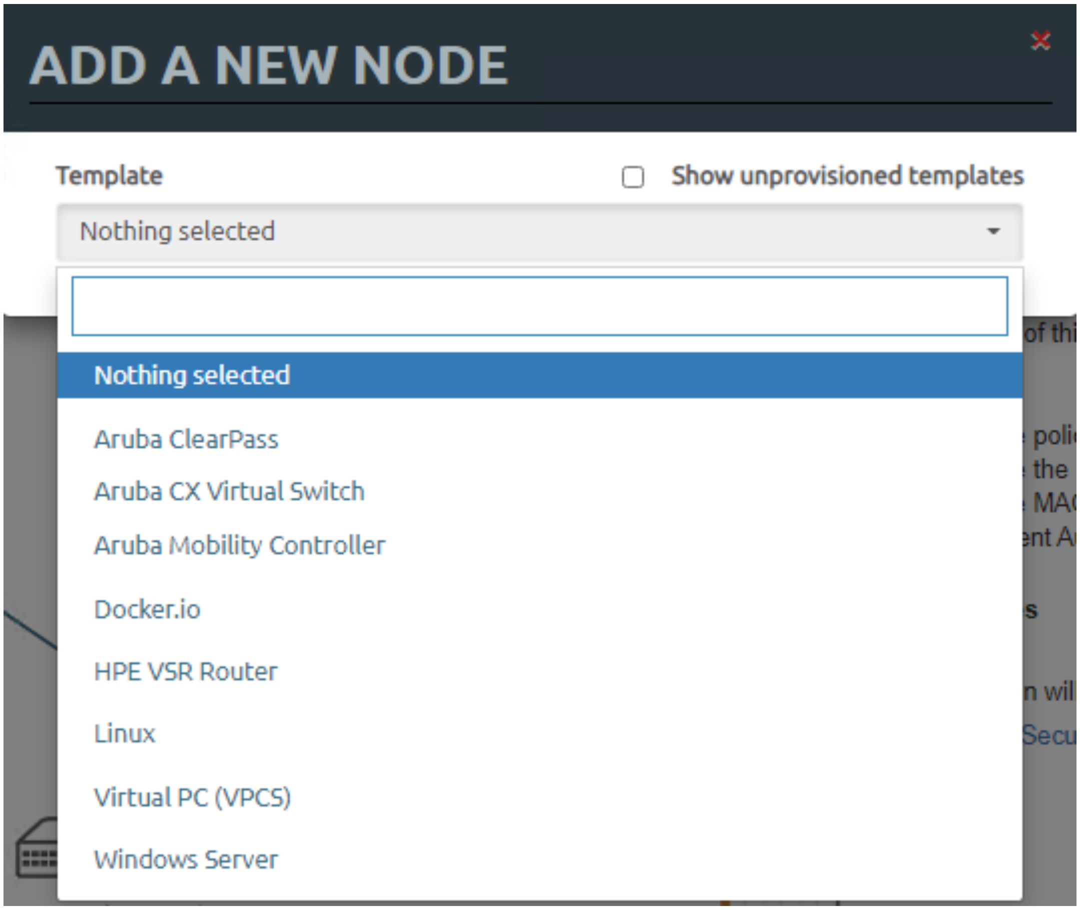
```
SwitchA#  show running-config port-access

port-access role LUR

    vlan access 10

SwitchA#
```

9. Configure Radius-server as below:

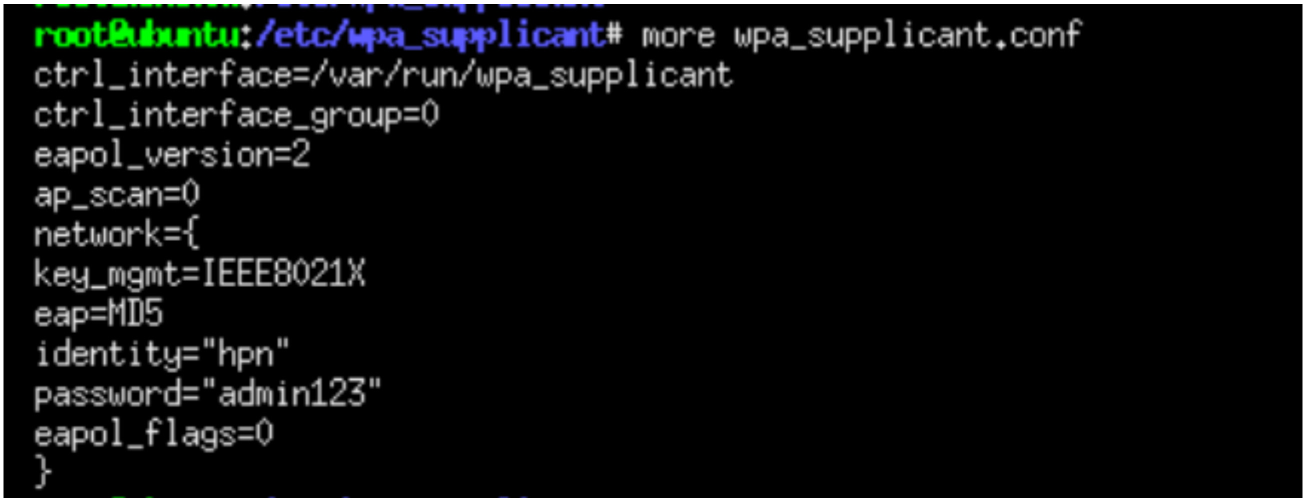
```
SwitchA(config)# radius-server host 10.10.0.250 clearpass-username admin clearpass-password
plaintext admin123 tracking-mode dead-only key plaintext admin123 tracking enable
```

Dot1x Supplicant Configuration

1. Choose Linux node from EVE-NG Node addition as below:



2. Login to linux client to below path to add dot1x supplicant as below:



```
root@ubuntu:/etc/wpa_supplicant# more wpa_supplicant.conf
ctrl_interface=/var/run/wpa_supplicant
ctrl_interface_group=0
eapol_version=2
ap_scan=0
network={
key_mgmt=IEEE8021X
eap=MD5
identity="hpn"
password="admin123"
eapol_flags=0
}
```

Note: Make sure you are logged in as root

3. Start dot1x supplicant as below as background process:

wpa_supplicant -c /etc/wpa_supplicant/wpa_supplicant.conf -D wired -i eth0 &

ClearPass Configuration

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

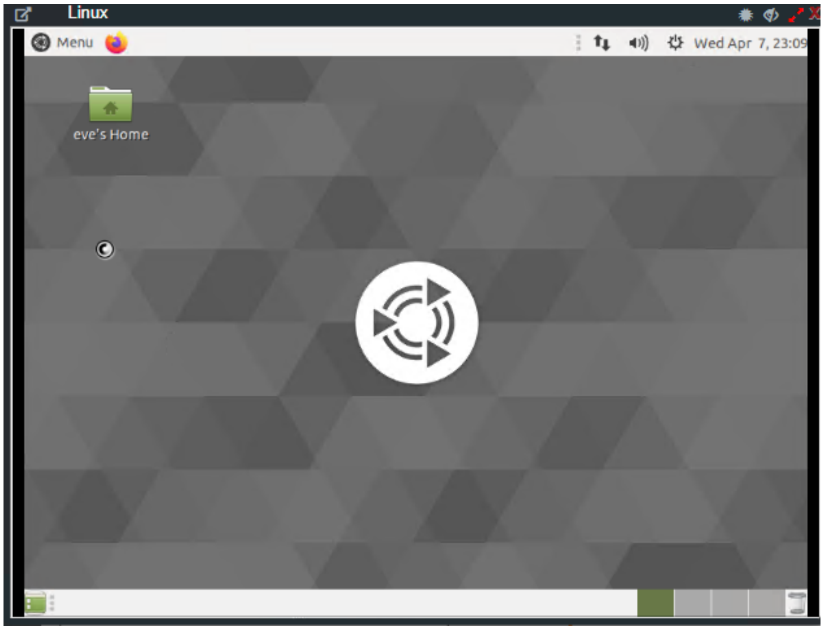


Figure 5. Ubuntu Desktop in EVE-NG

2. Open the Firefox Web Browser in the Linux window and navigate to 10.10.0.250.

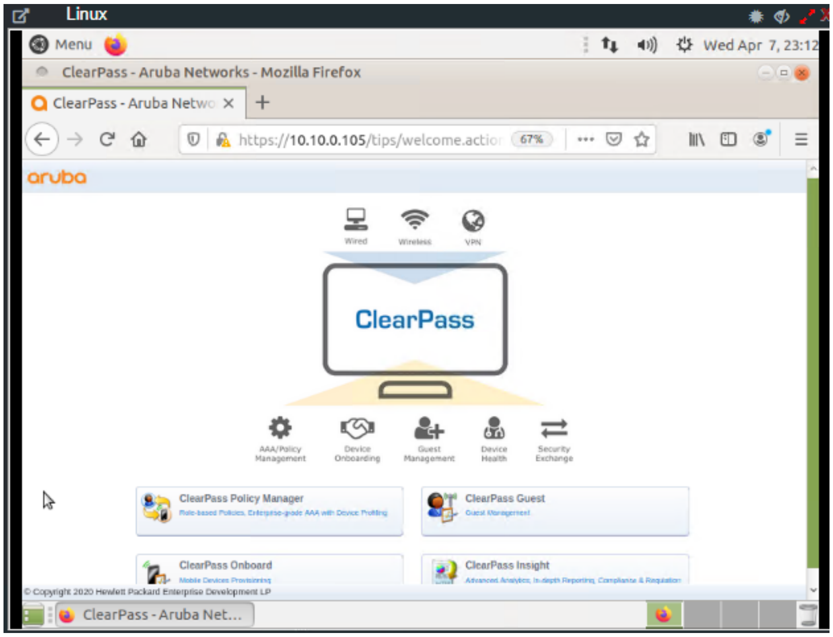
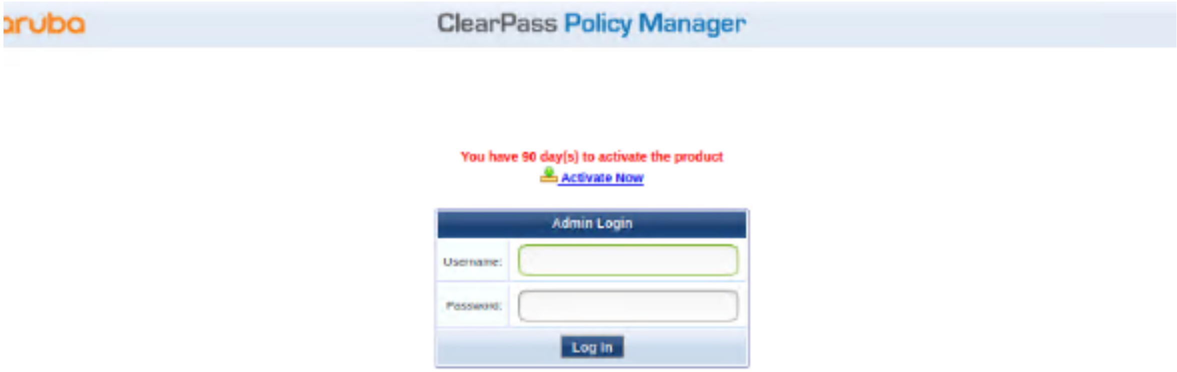

Linux
Menu
Wed Apr 7, 23:12
ClearPass - Aruba Networks - Mozilla Firefox
ClearPass - Aruba Netwo
https://10.10.0.105/tips/welcome.actio
67%
aruba
Wired
Wireless
VPN
ClearPass
AAA/Policy Management
Device Onboarding
Guest Management
Device Health
Security Exchange
ClearPass Policy Manager
Role-based Policies, 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 6. ClearPass Home Page in Ubuntu Window – EVE-NG

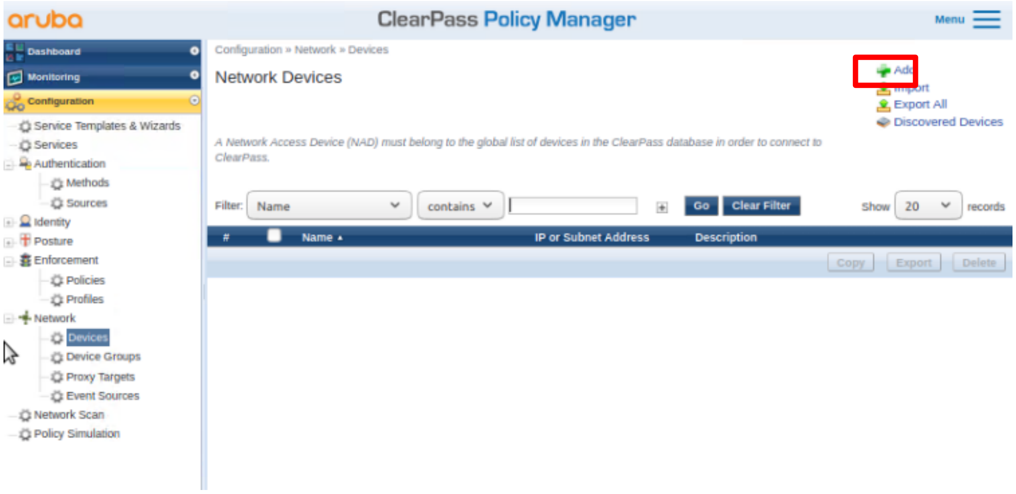
3. Click on the “ClearPass Policy Manager” Button and log into ClearPass with the following credentials, ‘admin/aruba123’.



You have 90 day(s) to activate the product

Figure 7. ClearPass Login Screen

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



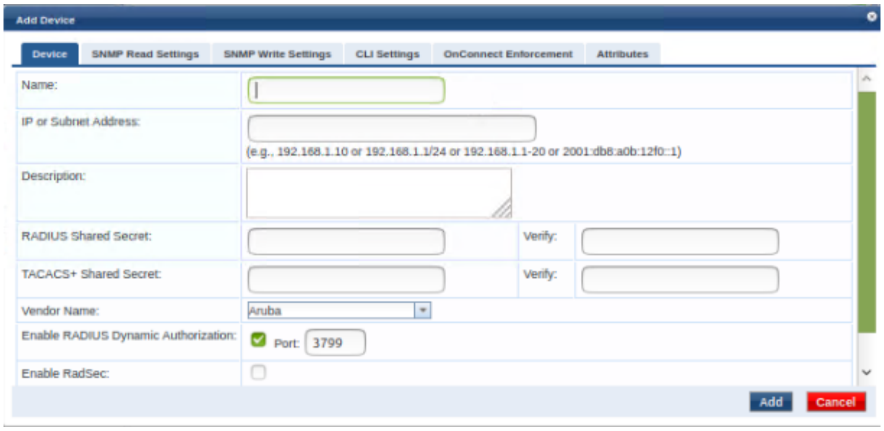
Configuration » Network » Devices

Network Devices

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

Figure 8. 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.

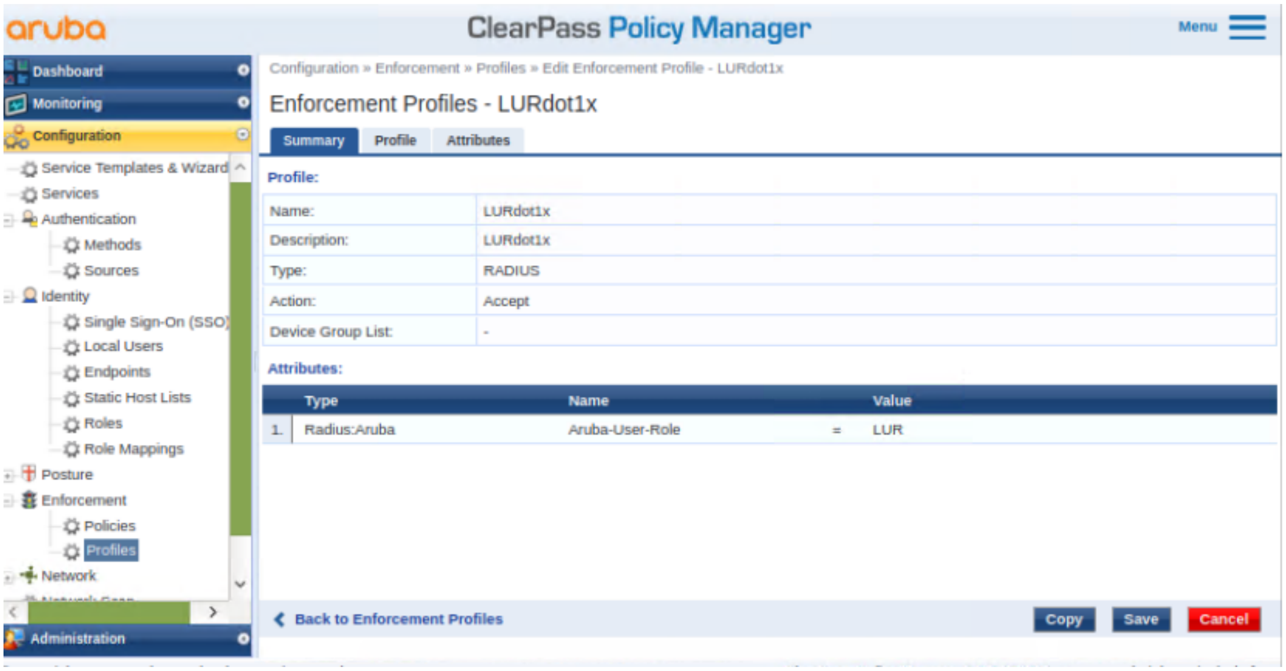


Name:			
IP or Subnet Address:	(e.g., 192.168.1.10 or 192.168.1.1/24 or 192.168.1.1-20 or 2001:db8:a0b:12f0::1)		
Description:			
RADIUS Shared Secret:		Verify:	
TACACS+ Shared Secret:		Verify:	
Vendor Name:	Aruba		
Enable RADIUS Dynamic Authorization:	☑ Port: 3799		
Enable RadSec:	□		

Figure 9. ClearPass Add Device Context

<u>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</u>

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



Configuration » Enforcement » Profiles » Edit Enforcement Profile - LURdot1x

Enforcement Profiles - LURdot1x

Profile:

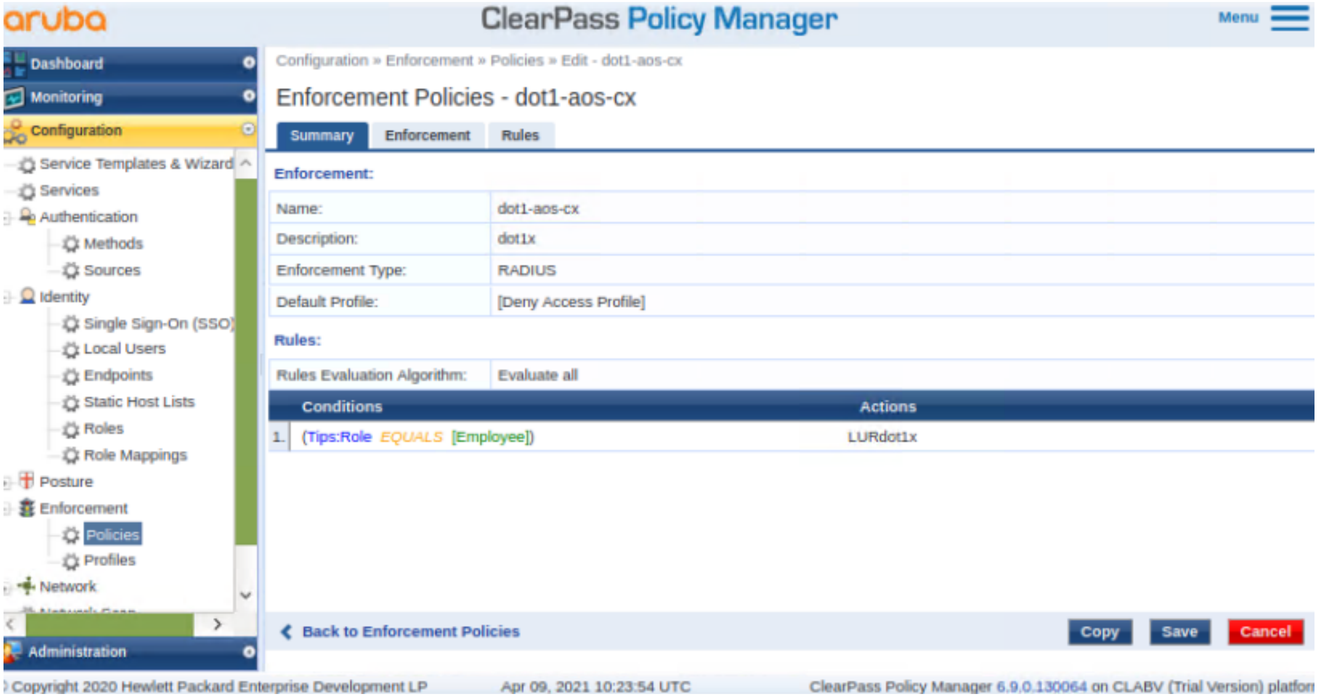
Name:	LURdot1x
Description:	LURdot1x
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	LUR

Figure 10. ClearPass Enforcement Profiles

7. Click on Configuration → Enforcement → Policies → Add.



Configuration » Enforcement » Policies » Edit - dot1-aos-cx

Enforcement Policies - dot1-aos-cx

Enforcement:

Name:	dot1-aos-cx
Description:	dot1x
Enforcement Type:	RADIUS
Default Profile:	[Deny Access Profile]

Rules:

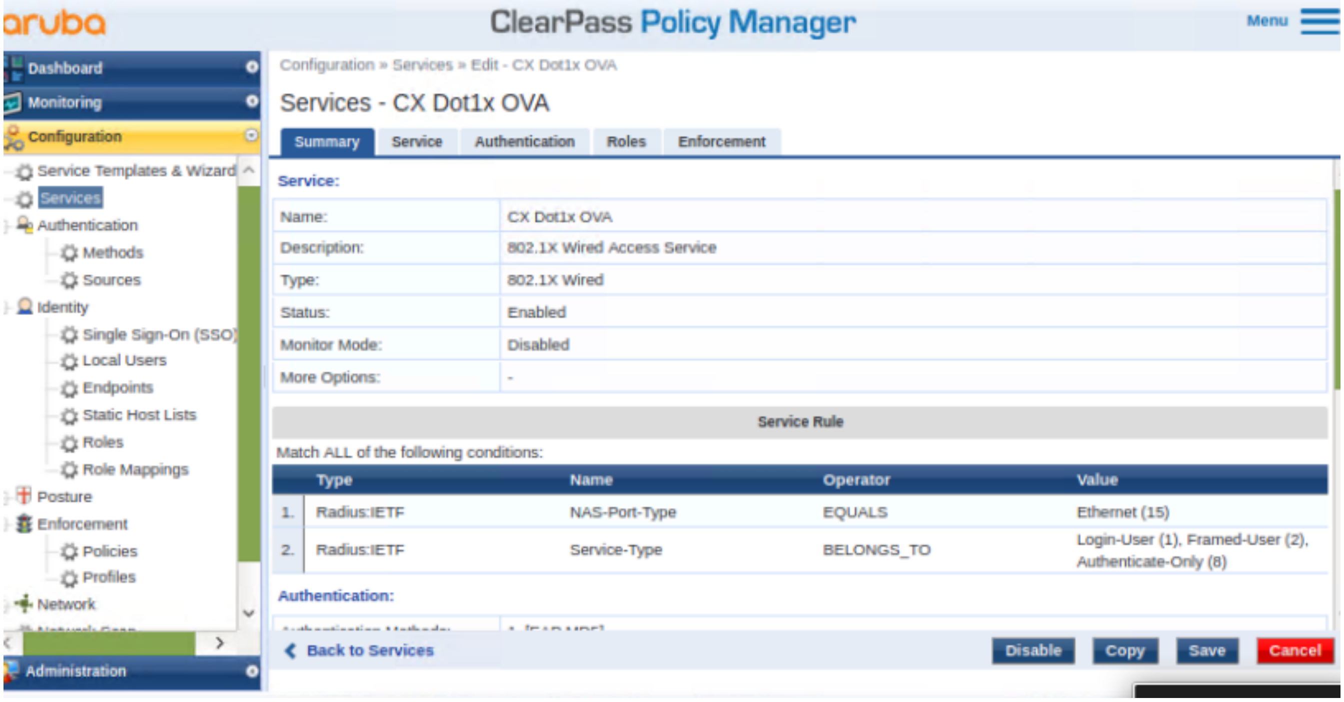
Rules Evaluation Algorithm:	Evaluate all

	Conditions	Actions
1.	(Tips:Role EQUALS [Employee])	LURdot1x

Copyright 2020 Hewlett Packard Enterprise Development LP   Apr 09, 2021 10:23:54 UTC   ClearPass Policy Manager 6.9.0.130064 on CLABV (Trial Version) platfor

Figure 11. ClearPass Services

8. In ClearPass, click on Configuration → Services, then click on “Add”.



Configuration » Services » Edit - CX Dot1x OVA

Services - CX Dot1x OVA

Service:

Name:	CX Dot1x OVA
Description:	802.1X Wired Access Service
Type:	802.1X Wired
Status:	Enabled
Monitor Mode:	Disabled
More Options:	-

Service Rule

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	EQUALS	Ethernet (15)
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)

Authentication:

Authentication Methods: 1. [EAP MD5]

Figure 11. ClearPass Services

Client Verification and Troubleshooting

1. Open the switch console and run the command “show radius-server detail”. You should see output like the following:

```
Switch-A# show radius-server detail
******* Global RADIUS Configuration *******
Shared-Secret: None
Timeout: 5
Auth-Type: pap
Retries: 1
TLS Timeout: 5
Tracking Time Interval (seconds): 60
Tracking Retries: 1
Tracking User-name: radius-tracking-user
Tracking Password: None
Number of Servers: 1
****** RADIUS Server Information ******
Server-Name              : 10.10.0.250
Auth-Port                : 1812
Accounting-Port          : 1813
VRF                      : default
TLS Enabled              : No
Shared-Secret            : AQBapfhltTYjsSH9NO5UJseS5cOG2Fv6QRKD8AIL2BgTQ2jdCAAAAC7h
fPijBaqs
Timeout                  : 5
Retries                  : 1
Auth-Type                : pap
Server-Group             : radius
Default-Priority         : 1
ClearPass-Username       : admin
ClearPass-Password       : AQBapfhltTYjsSH9NO5UJseS5cOG2Fv6QRKD8AIL2BgTQ2jdCAAAAC7h
fPijBaqs
Tracking                 : enabled
Tracking-Mode            : dead-only
Reachability-Status      : reachable, Since Thu Apr 08 06:25:40 UTC 2021
Tracking-Last-Attempted  : Thu Apr 08 06:36:15 UTC 2021
Next-Tracking-Request    : 26 seconds

Switch-A#
```

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

```
SwitchA# show port-access clients

Port Access Clients

Status codes: d device-mode

----------------------------------------------------------------------------------
  Port     MAC-Address        Onboarding     Status      Role
                              Method
----------------------------------------------------------------------------------
  1/1/1    50:06:00:05:00:00 dot1x           Success     LUR
  1/1/2    00:50:79:66:68:04 mac-auth        Success     RADIUS_1986087471

SwitchA#
```

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

```
SwitchA# show port-access clients detail

Port Access Client Status Details:

Client 50:06:00:05:00:00, hpn
============================
  Session Details
  ---------------
    Port         : 1/1/1
    Session Time : 660s
    IPv4 Address :
    IPv6 Address :

  Authentication Details
  ----------------------
```

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

  Authorization Details
  ----------------------
    Role   : LUR
    Status : Applied
Role Information:
Name  : LUR
Type  : local
----------------------------------------------
    Reauthentication Period             :
    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                         :
       Captive Portal Profile               :
       Policy                               :
```

```
Port Access Client Status Details:

Client 00:50:79:66:68:04, 005079666804
============================
  Session Details
  ---------------
    Port         : 1/1/2
    Session Time : 267s
    IPv4 Address :
    IPv6 Address :

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

  Authorization Details
  ----------------------
    Role   : RADIUS_1986087471
    Status : Applied


Role Information:

Name  : RADIUS_1986087471
Type  : radius
----------------------------------------------
    Reauthentication Period             :
    Cached Reauthentication Period      :
    Authentication Mode                 :
    Session Timeout                     :
    Client Inactivity Timeout           :
    Description                         :
    Gateway Zone                        :
    UBT Gateway Role                    :
    UBT Gateway Clearpass Role          :
    Access VLAN                         :
    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                        :
    Captive Portal Profile              :
    Policy                              :
SwitchA#
```

Appendix A – Switch Configuration

```
SwitchA# show running-config
Current configuration:
!
!Version ArubaOS-CX Virtual.10.06.0001
!export-password: default
hostname SwitchA
user admin group administrators password ciphertext AQBapZfKr36kJSLIl9H4YW1jnlLK4RS8nBX
UY9bgrl0L9s/aYgAAANpvxtgIk+LCz5cP5fY78dwfz9LETPisiE1Su6fz7f6kOFvD6J4I5dQ0aHsnCkcIHFyeDu
fOXOGCB7WPmwh/vF8q7OBr/Pdm+1uXiT6aDlQbZdvMR/86bIG3z/EUDa22ujn8
led locator on
ntp server pool.ntp.org minpoll 4 maxpoll 4 iburst
ntp enable
```

```
!
!
!
radius-server key ciphertext AQBapfhltTYjsSH9NO5UJseS5cOG2Fv6QRKD8AIL2BgTQ2jdCAAAAC7hfP
ijBaqs
!
radius-server host 10.10.0.250 retries 2 tracking enable tracking-mode dead-only clearp
ass-username admin clearpass-password ciphertext AQBapfhltTYjsSH9NO5UJseS5cOG2Fv6QRKD8A
IL2BgTQ2jdCAAAAC7hfPijBaqs
aaa authentication login default group radius
aaa authentication login ssh group radius
!
ssh server vrf mgmt
vlan 1,10
interface mgmt
    no shutdown
    ip dhcp
port-access role LUR
    vlan access 10
aaa authentication port-access dot1x authenticator
    enable
aaa authentication port-access mac-auth
    enable
interface 1/1/1
    no shutdown
    no routing
    vlan access 1
    aaa authentication port-access dot1x authenticator
        enable
interface 1/1/2
    no shutdown
    no routing
    vlan access 10
    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

!

!

!

!

!

https-server vrf mgmt
SwitchA#
```

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

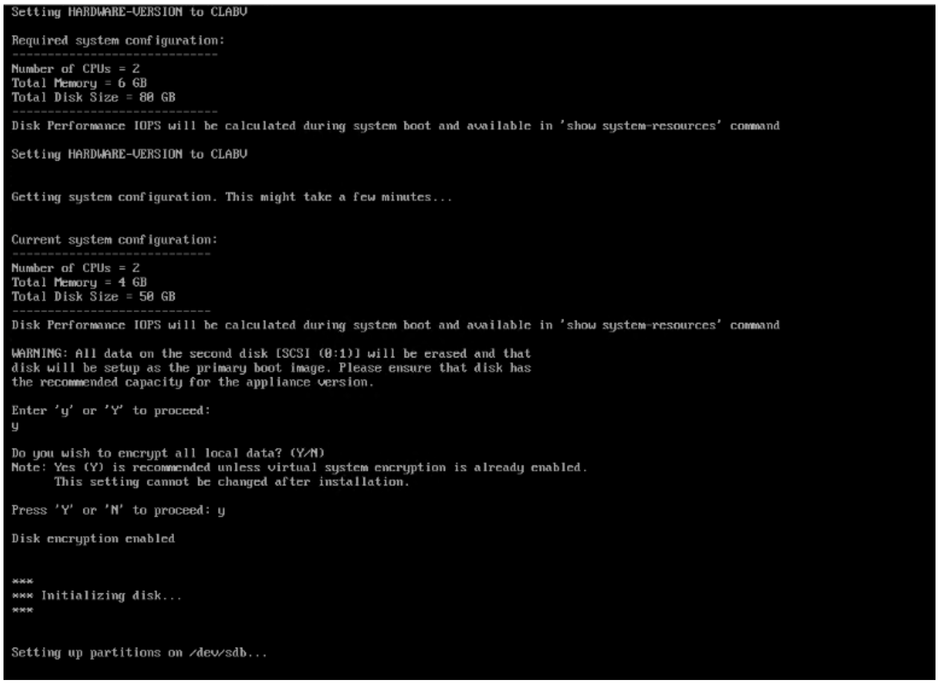
1. To first install the ClearPass OVA into the EVE-NG environment, follow the instructions at this link:

   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

2. 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.

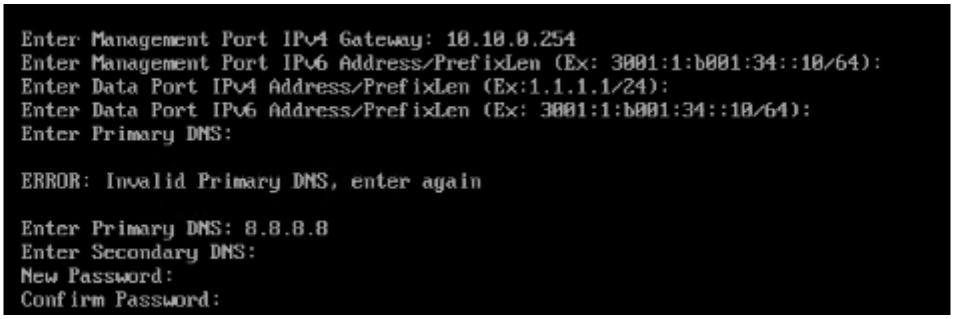


```
Setting HARDWARE-VERSION to CLABV

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 12. ClearPass Installation

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

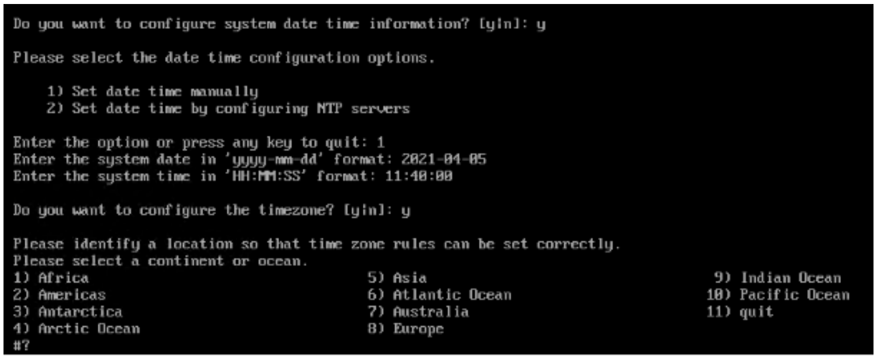
3. Once prompted, enter the IP address as “10.10.0.250”, the mask as “255.255.255.0”, the gateway as “10.10.0.254”, and the DNS as “8.8.8.8” (not needed for this exercise). Configure a new password, this lab example used “aruba123”.



```
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 13. ClearPass IP Configuration

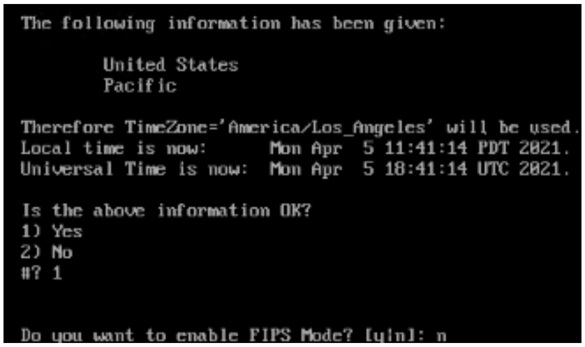
4. Configure the date and time manually as well as the time zone.



```
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 14. ClearPass Date and Time Configuration

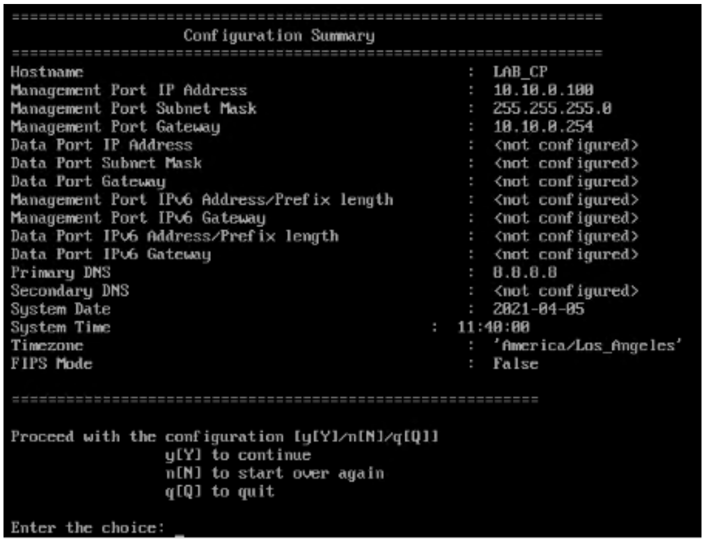
5. Confirm the correct date, time, and time zone.



```
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 15. ClearPass Date and Time Settings Confirmation

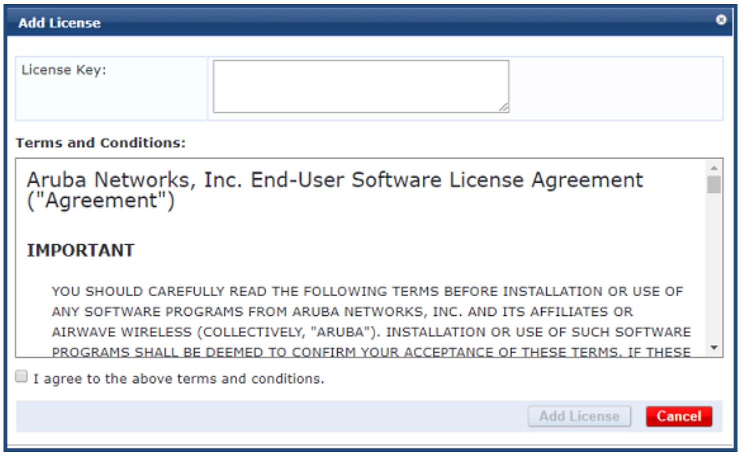
6. Confirm the configured settings are correct. Press Y to save settings.



```
================================================================
                    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 16. ClearPass Configuration Confirmation

7. 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/.



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

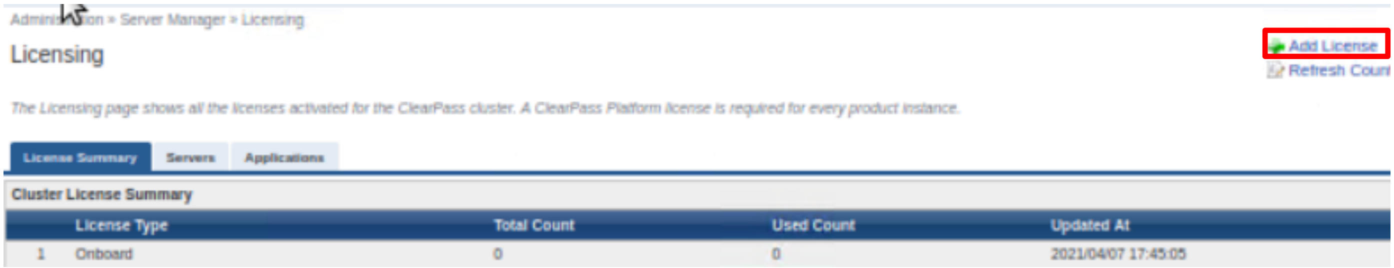
IMPORTANT

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 17. ClearPass Platform License entry

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



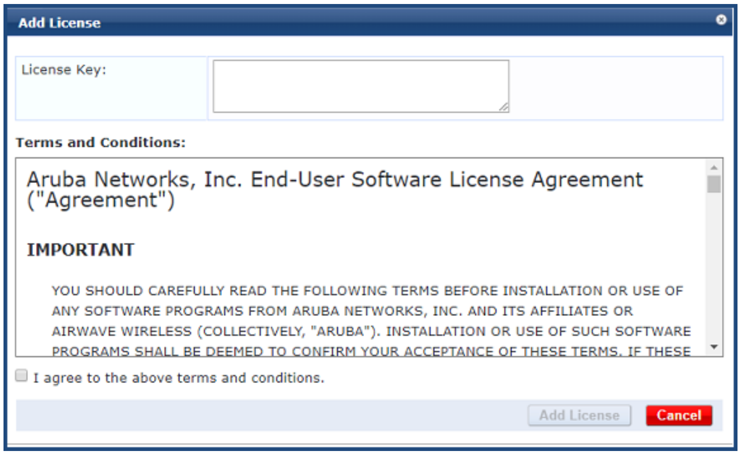
The Licensing page shows all the licenses activated for the ClearPass cluster. A ClearPass Platform license is required for every product instance.

Cluster License Summary

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

Figure 18. ClearPass Add New Server License

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



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 19. ClearPass Server license entry

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