LAB GUIDE

RADIUS MAC 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 Mac Authentication in AOS-CX and how to authenticate clients or devices. You will learn how to configure Radius port-access mac authentication and how to configure an enforcement policy in Aruba ClearPass.

Lab Overview

MAC authentication relies on a RADIUS server to authenticate clients. This technique simplifies access security management by using a master database on a single server to control client access. Up to three RADIUS servers can be used for backup in case access to the primary server fails. It also means that the same credentials can be used for authentication, regardless of which switch, or switch port is the current access point into the LAN.

MAC authentication grants access to a secure network by authenticating devices. When a device connects to the switch, either by direct link or through the network, the switch forwards the device MAC address to the RADIUS server for authentication. The RADIUS server uses the device MAC address as the username and password, and grants or denies network access in the same way that it does for clients capable of interactive logons. The process does not use a client device configuration or a logon session. MAC authentication is well suited for clients not capable of providing interactive logons, such as telephones, printers, and wireless access points. Also, because most RADIUS servers allow for authentication to depend on the source switch and port through which the client connects to the network, you can use MAC authentication to lock a particular device to a specific switch and port.

Lab Setup

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

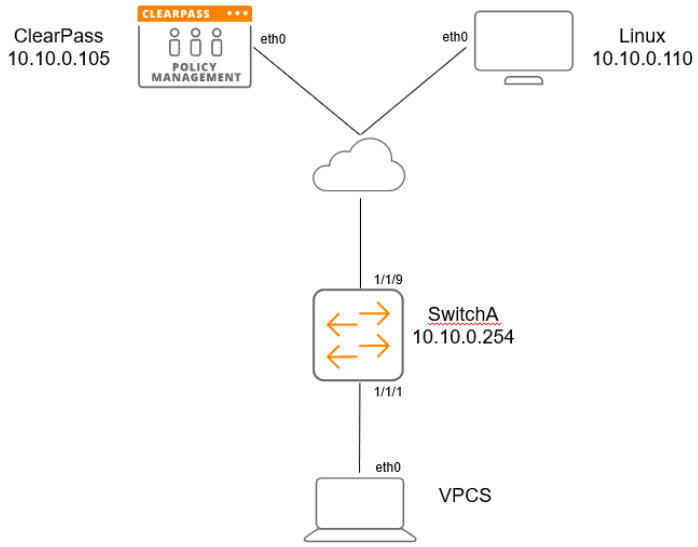


Figure 1. Example EVE-NG topology

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

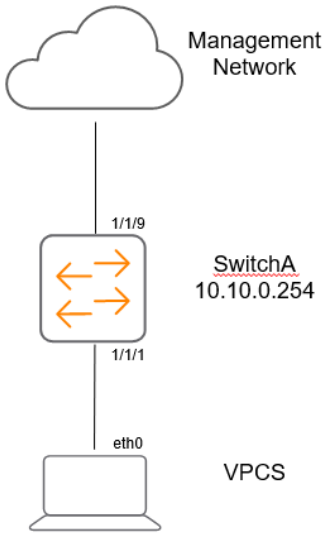


Figure 2. Example EVE-NG topology – no ClearPass

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

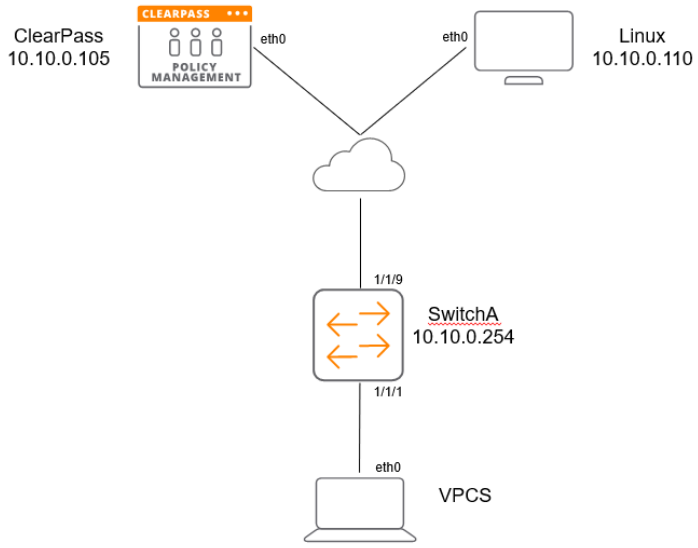


Figure 3. Lab interface and IP details

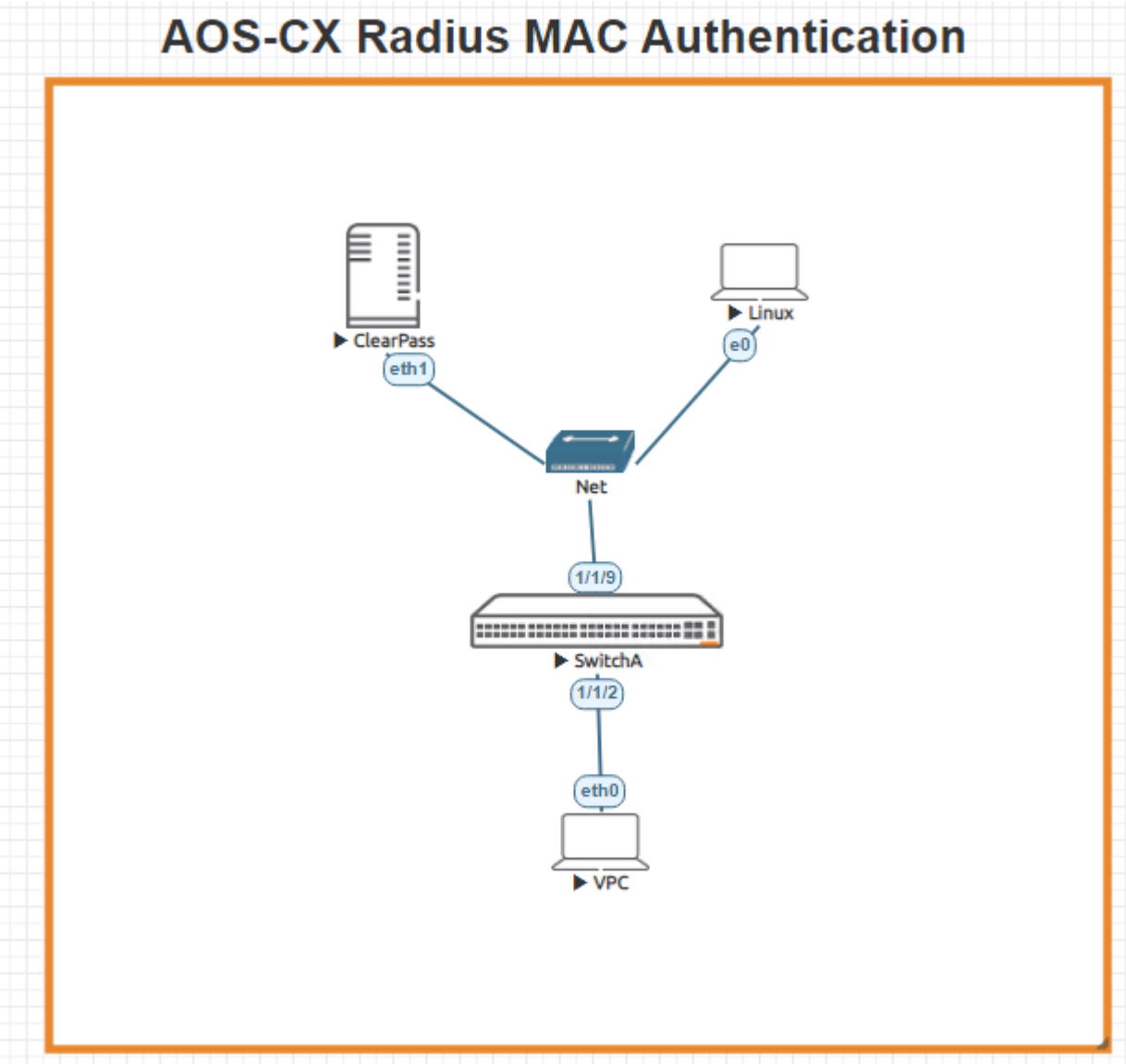


Figure 4. EVE-NG Radius Mac Authentication Topology

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

```
Switch-A(config)# aaa authentication port-access mac-auth enable
Switch-A(config-if)# interface 1/1/1
Switch-A(config-if)# no shutdown
Switch-A(config-if)#   no routing
Switch-A(config-if)#   vlan access 10
Switch-A(config-if)#    aaa authentication port-access mac-auth enable
Switch-A(config-if)#    end
```

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

- Verify client mac is learned on connected port.

```
Switch-A# show mac-address-table detail
MAC age-time             : 300 seconds
Number of MAC addresses : 2
MAC Address          VLAN     Type                      Port       Age        Denied
never_ageout
```

```
--------------------------------------------------------------------------------
50:09:00:01:00:00    10        dynamic                 1/1/8       300         false   false
00:50:79:66:68:04    10        port-access-security    1/1/1       300         false   false
Switch-A#
```

8. 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
```

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).

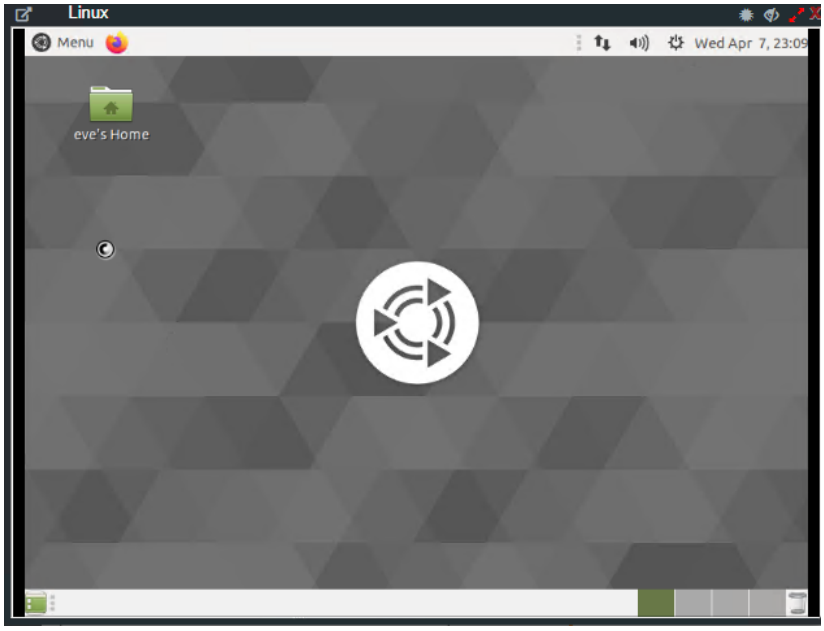


Figure 5. Ubuntu Desktop in EVE-NG

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

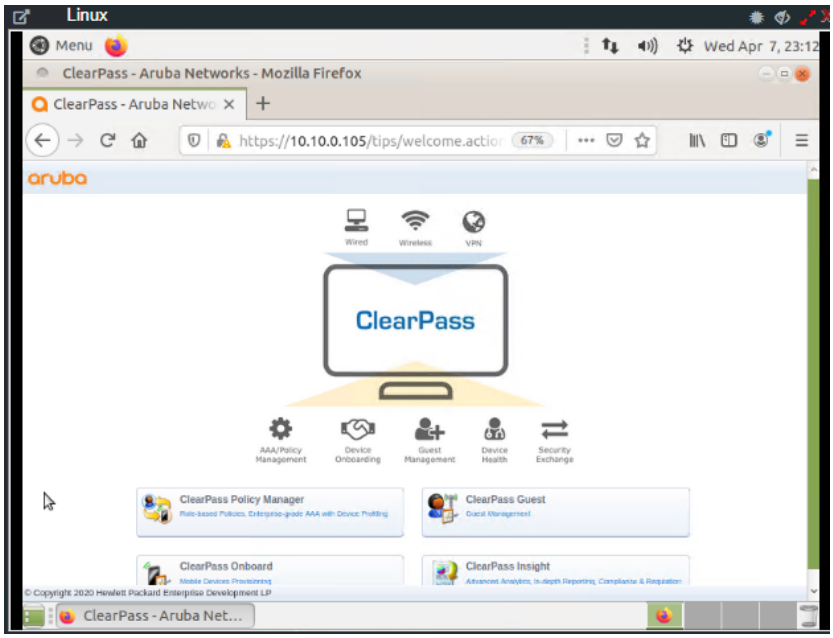


Figure 6. ClearPass Home Page in Ubuntu Window – EVE-NG

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

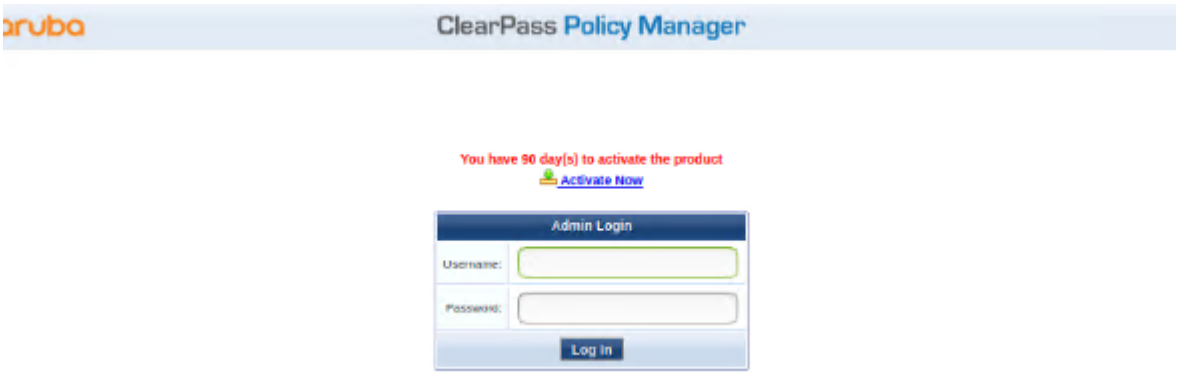


Figure 7. ClearPass Login Screen

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

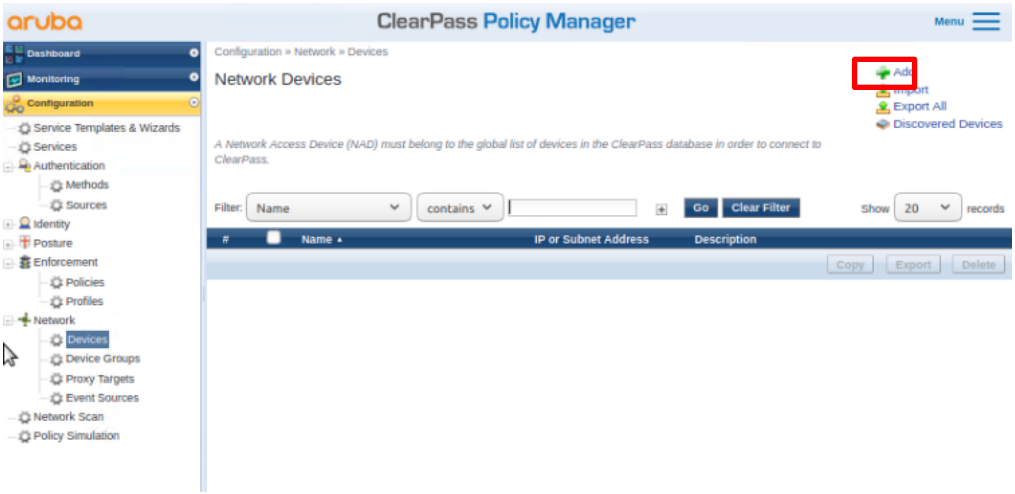


Figure 8. ClearPass Devices window

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.

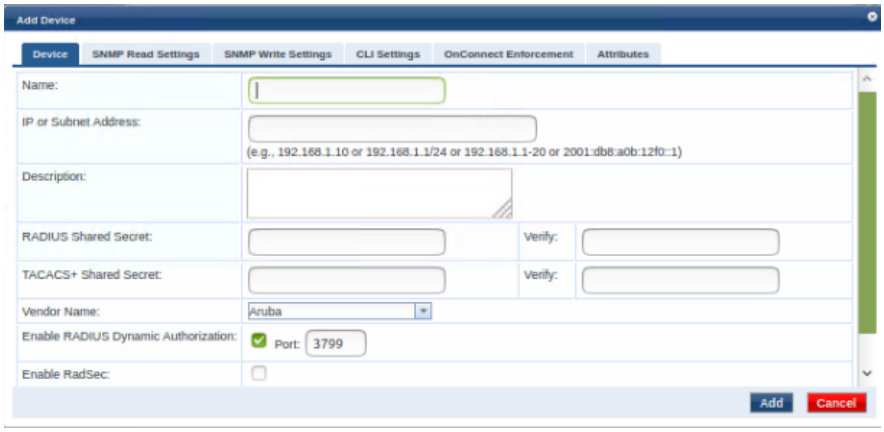


Figure 9. ClearPass Add Device Context

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

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

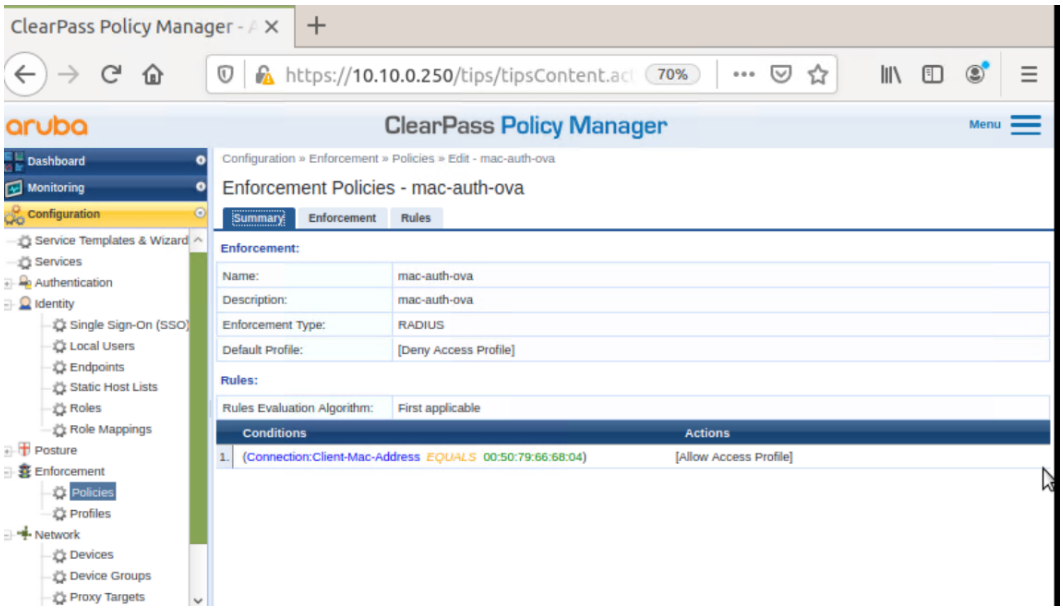


Figure 10. ClearPass Enforcement Profiles

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

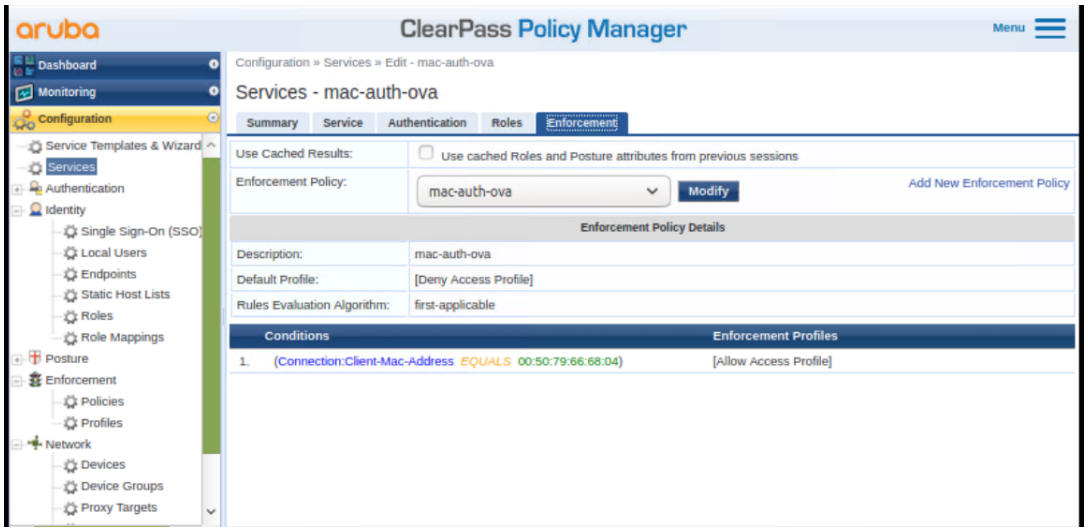


Figure 11. ClearPass Services

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:

```
Switch-A# show port-access 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     RADIUS_1986087471
```

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

```
Switch-A # show port-access clients detail
Port Access Client Status Details:
Client 00:50:79:66:68:04, 005079666804
==============================
  Session Details
  ---------------
    Port         : 1/1/1
    Session Time : 43s
    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:
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                              :
Switch-A#
```

Appendix A – Switch Configuration

```
Switch-A# show running-config
Current configuration:
!
!Version ArubaOS-CX Virtual.10.06.0001
!export-password: default
hostname Switch-A
```

```
user admin group administrators password ciphertext
AQBapWEFlF5u34QibFTrfv5vpW7Rd3ciSjqfJyZlbLyC1vqpYgAAAC8hwTJk8+S7hoA5LSal8Y9oUTbXs06yyMJMwyjAL7huM
n+HS5y8j4+nqnImGLzjaEgt/f0hvC2DR2d7
G9MzKZ0f+v8XE0sPrHEHlTq+0PtJks3dbLWbUS0zI6Gblx7MG3/K
led locator on
radius-server tracking interval 60
vrf vrf1
ntp server pool.ntp.org minpoll 4 maxpoll 4 iburst
ntp enable
!
!
!
!
tacacs-server host 10.10.0.254 key ciphertext
AQBapfhltTYjsSH9NO5UJseS5cOG2Fv6QRKD8AIL2BgTQ2jdCAAAAC7hfPijBaqs tracking enable
!
radius-server host 10.10.0.250 key ciphertext
AQBapfhltTYjsSH9NO5UJseS5cOG2Fv6QRKD8AIL2BgTQ2jdCAAAAC7hfPijBaqs tracking enable tracking-mode
dead-only clearpass-username admin clearpas
s-password ciphertext AQBapfhltTYjsSH9NO5UJseS5cOG2Fv6QRKD8AIL2BgTQ2jdCAAAAC7hfPijBaqs
!
ssh server vrf default
ssh server vrf mgmt
debug tacacs all
vlan 1,10
interface mgmt
    no shutdown
    ip dhcp
aaa authentication port-access mac-auth
    enable
interface 1/1/1
    no shutdown
    no routing
    vlan access 10
    aaa authentication port-access mac-auth
        cached-reauth
        cached-reauth-period 100
        reauth
        reauth-period 2
       enable
interface 1/1/8
    no shutdown
    no routing
    vlan access 10
interface vlan 10
    ip address 10.10.0.254/24
!
https-server vrf default
https-server vrf mgmt
Switch-A#
```

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.

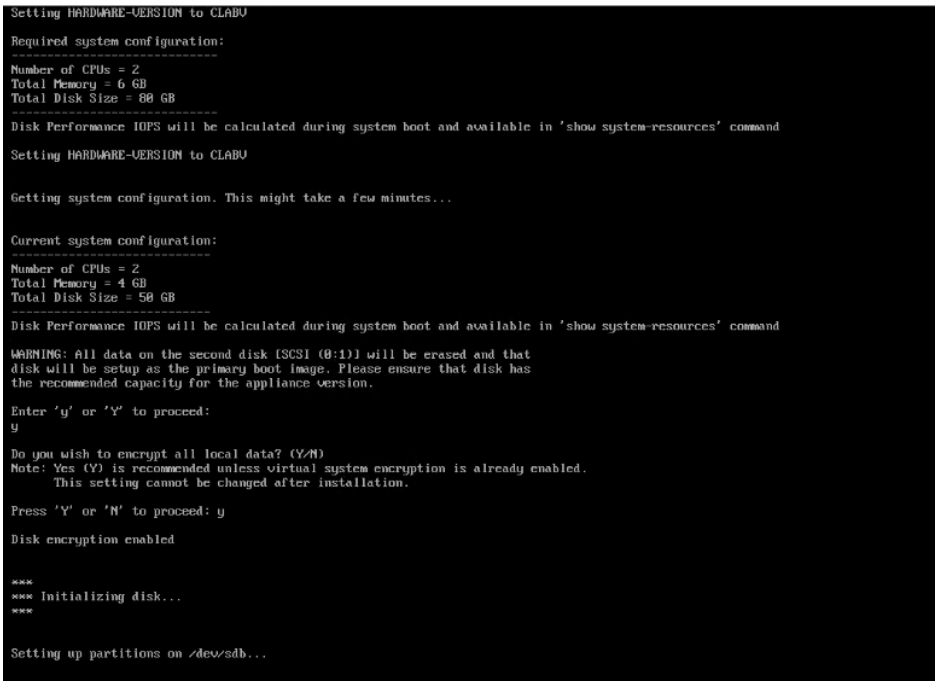
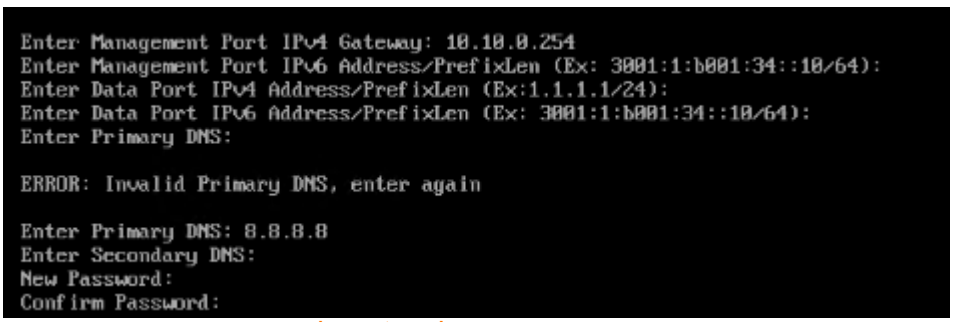


Figure 12. ClearPass Installation

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

3. Once prompted, enter the IP address as “10.10.0.105”, 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”.

Figure 13. ClearPass IP Configuration

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

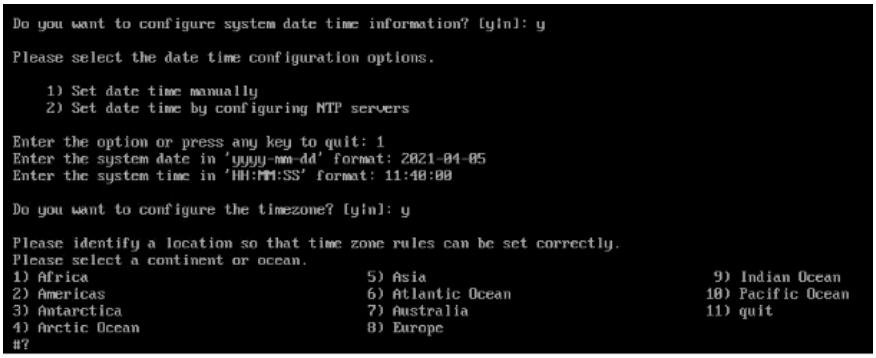


Figure 14. ClearPass Date and Time Configuration

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

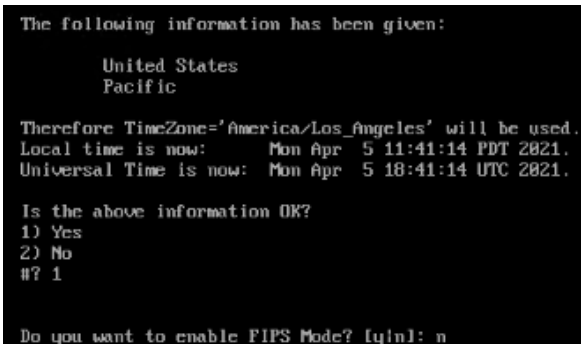


Figure 15. ClearPass Date and Time Settings Confirmation

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

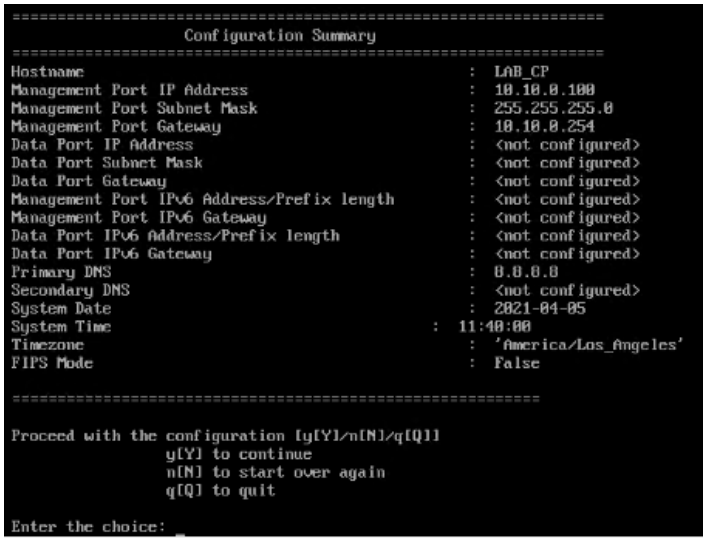


Figure 16. ClearPass Configuration Confirmation

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/.

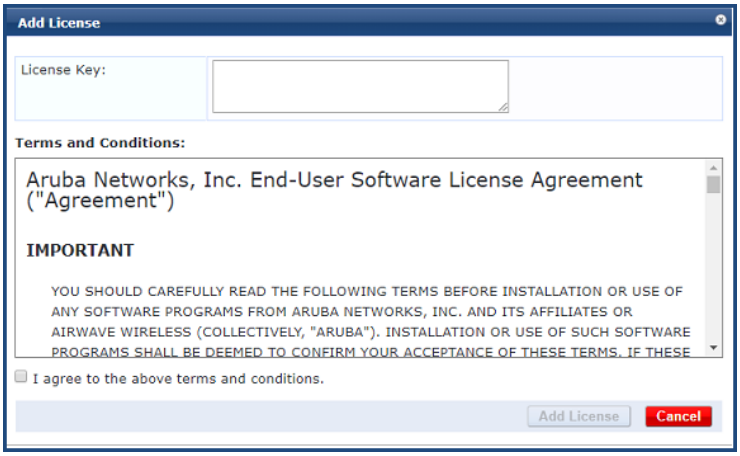


Figure 17. ClearPass Platform License entry

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

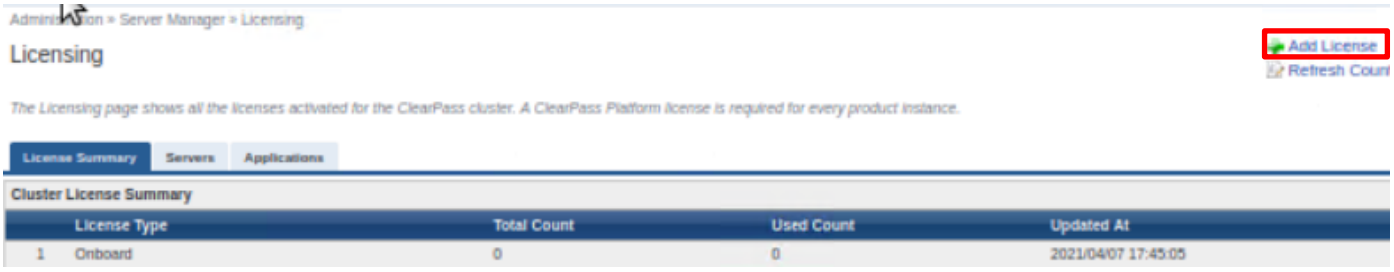


Figure 18. ClearPass Add New Server License

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

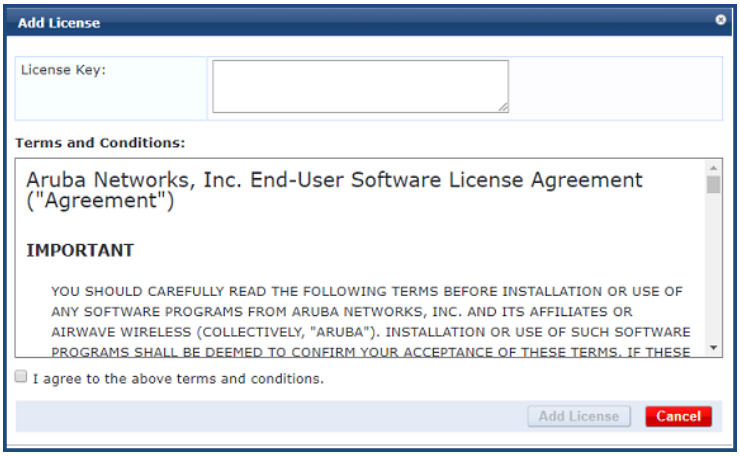


Figure 19. ClearPass Server license entry

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