Contents

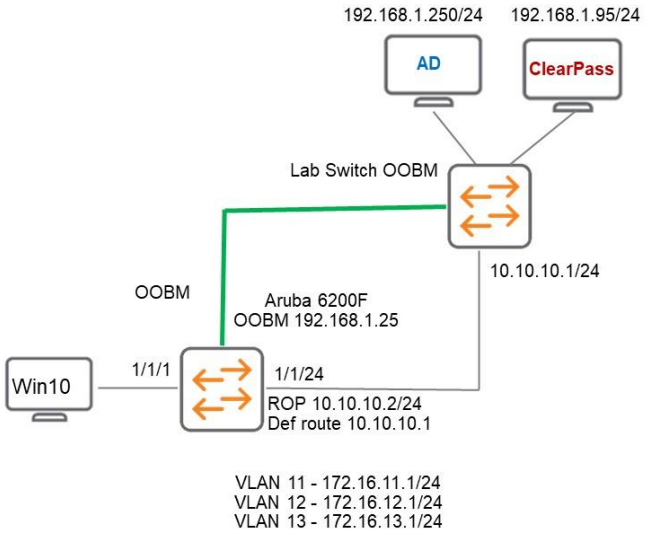
1.1 Revision History

DATE	VERSION	EDITOR	CHANGES
06 Jan 2023	0.1	Ariya Parsamanesh	Initial creation

2 ClearPass Wired Enforcement for CX Switches

This is the first part of 6x part series on Aruba CX switch wired enforcement.

The main objective of this guide is for easy/quick demo of ClearPass Policy Manager (CPPM) wired dot1x, MAC authentication, Guest Captive portal using local user roles for Aruba CX switches.



2.1 Things you need

- ClearPass Policy Manager 6.9.7 (VM)
- Aruba CX switch running firmware version 10.10.1020
- A laptop that can do dot1x authentication.
    - Staff user will be in Staff role (VLAN 11)
    - Student user will be in Student role (VLAN 12)
    - Guest pre-auth user will be in Captive-Portal role (VLAN 13)
    - Guest user will be in Guest role (VLAN 14)

2.2 Demo/PoC Assumptions

- ClearPass has join the AD domain with an AD user account.
- DNS, DHCP and NTP are in place and configured

2.3 Demonstration Goals

Demonstrating the wired enforcement using Local user roles for

- Wired dot1x authentication

3 Aruba CX Switch Configuration

Here we cover the Aruba 6200F switch configuration.

3.1 VLAN and DHCP configuration

Here we are enabling couple of VLANs and IP routing along with DHCP services.

```
allow-unsupported-transceiver
cli-session
    timeout 0
!
aruba-central
    disable
ssh server vrf default
ssh server vrf mgmt
!
vlan 1
vlan 11
    name staff-vlan
vlan 12
    name student-vlan
vlan 13
    name IoT-vlan
!
interface mgmt
    no shutdown
    ip static 192.168.1.25/24
    default-gateway 192.168.1.249
!
interface vlan 11
    ip address 172.16.11.1/24
    ip helper-address 192.168.1.95
interface vlan 12
    ip address 172.16.12.1/24
    ip helper-address 192.168.1.95
interface vlan 13
    ip address 172.16.13.1/24
    ip helper-address 192.168.1.95
interface vlan 14
    ip address 172.16.14.1/24
    ip helper-address 192.168.1.95

ip route 0.0.0.0/0 10.10.10.1
ip dns server-address 192.168.1.130 vrf mgmt
https-server vrf default
https-server vrf mgmt
```

Here is the DHCP server configuration

```
dhcp-server vrf default
    pool Staff-11
        range 172.16.11.20 172.16.11.29
        default-router 172.16.11.1
        dns-server 192.168.1.130
        lease 00:04:00
        exit
    pool Student-12
        range 172.16.12.20 172.16.12.29
        default-router 172.16.12.1
        dns-server 192.168.1.130
        lease 00:04:00
        exit
    pool IoT-13
```

```
        range 172.16.13.20 172.16.13.29
        default-router 172.16.13.1
        dns-server 192.168.1.130
        lease 00:04:00
        exit
     pool Guest-14
        range 172.16.14.20 172.16.14.29
        default-router 172.16.14.1
        dns-server 192.168.1.130
        lease 00:04:00
        exit
    enable
```

3.2 Client IP tracking Configuration

You need to enable Client tracking at global and as well as at VLAN level.

```
client track ip
!
vlan 1
!
vlan 11
    name staff-vlan
    client track ip
!
vlan 12
    name student-vlan
    client track ip
!
vlan 13
    name IoT-vlan
    client track ip
!
vlan 14
    name Guest-vlan
    client track ip
```

3.3 Policy and User Role Configuration

These “policy user” commands create a context that may be used to classify the policy. The actions are specific to policy user which are redirect, permit and deny.

```
class ip DHCP-DNS
    10 match udp any any eq dhcp-server
    20 match udp any any eq dns
!
class ip ICMP
    10 match icmp any any
!
class ip ClearPass
    10 match tcp any 192.168.1.95 eq http
    20 match tcp any 192.168.1.95 eq https
!
class ip IP-Any-Any
    10 match any any any
!
class ip Web-Traffic
    10 match tcp any any eq 443
    20 match tcp any any eq 80
!
```

```
port-access policy Staff-Pol
    10 class ip IP-Any-Any
!
```

```
port-access policy Student-Pol
    10 class ip IP-Any-Any
!
port-access policy AD-Guest-Pol
    10 class ip IP-Any-Any
!
port-access policy Guest-Pol
    10 class ip IP-Any-Any
!
port-access policy cp-policy
    10 class ip DHCP-DNS
    20 class ip ICMP
    30 class ip ClearPass
    40 class ip Web-Traffic action redirect captive-portal
!
```

Here are the local user roles that are configured.

```
aaa authentication port-access captive-portal-profile cp-profile
    url https://192.168.1.95/guest/wired_guest.php

port-access role Critical-Role
    vlan access 13
!
port-access role Staff
    description LUR-for-Staff
    associate policy Staff-Pol
    client-inactivity timeout 400
    reauth-period 3000
    trust-mode none
    auth-mode client-mode
    vlan access 11
!
port-access role Student
    description LUR-for-Student
    associate policy Student-Pol
    client-inactivity timeout 400
    reauth-period 3000
    trust-mode none
    auth-mode client-mode
    vlan access 12
!
port-access role Guest
    description LUR-for-Guest
    associate policy Guest-Pol
    auth-mode client-mode
    client-inactivity timeout 400
    trust-mode none
    reauth-period 3000
    vlan access 14

port-access role AD-Guest
    description LUR-for-AD-Guest
    associate policy AD-Guest-Pol
    auth-mode client-mode
    client-inactivity timeout 400
    trust-mode none
    reauth-period 3000
    vlan access 11

port-access role Captive-Portal
    description LUR-for-PreAuth
    associate captive-portal-profile cp-profile
    associate policy cp-policy
    auth-mode client-mode
```

```
    client-inactivity timeout 400
    trust-mode none
    reauth-period 3000
    vlan access 13
!
```

Auth-mode provides two options,

1. Client mode provides the ability in which all clients connecting to the port are sent for authentication. The maximum number of clients allowed to connect to the port is limited by the client limit value configured with the aaa authentication port-access client-limit command.
2. Device mode provides the ability that only the first client connecting to the port is sent for authentication. Once this client is authenticated, the port is considered as open and all subsequent clients trying to connect on that port are not sent for authentication

3.4 Authentication and CoA Configuration

```
radius-server host 192.168.1.95 key plaintext aruba tracking enable vrf mgmt
radius-server tracking interval 3600
radius-server tracking user-name radius-tracking-user password plaintext aruba

aaa group server radius ClearPass
    server 192.168.1.95 vrf mgmt

aaa authentication port-access dot1x authenticator radius server-group ClearPass
aaa authentication port-access dot1x authenticator enable

aaa authentication port-access mac-auth radius server-group ClearPass
aaa authentication port-access mac-auth enable

aaa accounting port-access start-stop interim 5 group ClearPass

radius dyn-authorization enable
radius dyn-authorization client 192.168.1.95 secret-key plaintext aruba vrf mgmt
```

We have enabled server tracking for the RADIUS server. Tracked servers are probed at the start of each server tracking interval to check if they are reachable.

```
6200-Lab# sh radius-server detail
******* Global RADIUS Configuration *******

Shared-Secret: None
Timeout: 5
Auth-Type: pap
Retries: 1
TLS Timeout: 5
Tracking Time Interval (seconds): 3600
Tracking Retries: 1
Tracking User-name: radius-tracking-user
Tracking Password: AQBapbX19aZW8eeI5JeQd7xMIk/kpE+oSLCOOsFDjhDNw7w9BQAAADv+iScp
Status-Server Time Interval (seconds): 300
Number of Servers: 2
AAA Server Status Trap: Disabled

****** RADIUS Server Information ******
Server-Name              : 192.168.1.95
Auth-Port                : 1812
Accounting-Port          : 1813
VRF                      : mgmt
TLS Enabled              : No
Shared-Secret            : AQBapW+n5wXvRjwhsN7HPPnsuW5qu4LA9EhvLTzOVe48vu1ZBQAAAPuyKM8A
Timeout                  : 5
```

```
Retries                  : 1
Auth-Type                : pap
Server-Group             : ClearPass
Group-Priority           : 1
ClearPass-Username       :
ClearPass-Password       : None
Tracking                 : enabled
Tracking-Mode            : any
Reachability-Status      : reachable, Since Thu Jan 05 12:26:19 AEDT 2023
Tracking-Last-Attempted  : Thu Jan 05 13:16:15 AEDT 2023
Next-Tracking-Request    : 3461 seconds

Server-Name              : 192.168.1.95
Auth-Port                : 1812
Accounting-Port          : 1813
VRF                      : default
TLS Enabled              : No
Shared-Secret            : AQBapUbJYn0Jrvzkduvl Gi+R1GD3X0+j3K6OrF8fvIRELzoIBQAAAMf9s4I3
Timeout                  : 5
Retries                  : 1
Auth-Type                : pap
Server-Group             : radius
Default-Priority         : 1
ClearPass-Username       :
ClearPass-Password       : None
Tracking                 : disabled
Tracking-Mode            : any
Reachability-Status      : unknown
Tracking-Last-Attempted  : N/A
Next-Tracking-Request    : N/A

6200-Lab#
```

Showing AAA accounting server

```
6200-Lab# sh aaa accounting port-access
AAA Accounting Port Access
==========================
  Radius Accounting Enabled        : yes
  Radius Server Group              : ClearPass
  Local Accounting Enabled         : no
  Accounting Mode                  : start-stop
  Interim Update Enabled           : yes
  Interim Interval                 : 5 minutes
  Interim Update on-reauth Enabled : no

6200-Lab#
```

Showing CoA status

```
6200-Lab# sh radius dyn-authorization
Status and Counters - RADIUS Dynamic Authorization Information

  RADIUS Dynamic Authorization                  : Enabled
  RADIUS Dynamic Authorization UDP Port         : 3799
  Invalid Client Addresses in CoA Requests      : 0
  Invalid Client Addresses in Disconnect Requests: 0

Dynamic Authorization Client Information
========================================

IP Address          : 192.168.1.95
VRF                 : mgmt
TLS Enabled         : No
Replay Protection   : Disabled
Time Window         : 300
Disconnect Requests : 0
Disconnect ACKs     : 0
Disconnect NAKs     : 0
CoA Requests        : 0
CoA ACKs            : 0
```

```
CoA NAKs            : 0
Shared-Secret       : AQBapbac1AdbyjwzITI2Dsztl5k2mZYPuMv3t9OAuSW+9TIKBQAAAHYQWZJs
6200-Lab#
```

You can use the following commands to check if your RADIUS server is working.

```
6200-Lab# sh radius-server statistics
  accounting      RADIUS server accounting statistics
  authentication  RADIUS server authentication statistics

6200-Lab# sh radius-server statistics authentication
 Server Name     : 192.168.1.95
 Auth-Port       : 1812
 Accounting-Port : 1813
 VRF             : default
 TLS Enabled     : No

  Authentication Statistics
  -------------------------
    Round Trip Time                          : 0
    Pending Requests                         : 0
    Timeouts                                 : 4
    Bad Authenticators                       : 0
    Packets Dropped                          : 0
    Access Requests                          : 5
    Access challenge                         : 0
    Access Accepts                           : 0
    Access Rejects                           : 0
    Access Response Malformed                : 0
    Access Retransmits                       : 2
    Tracking Requests                        : 3
    Tracking Responses                       : 0
    Unknown Response Code                    : 0
 Server Name     : 192.168.1.95
 Auth-Port       : 1812
 Accounting-Port : 1813
 VRF             : mgmt
 TLS Enabled     : No

  Authentication Statistics
  -------------------------
    Round Trip Time                          : 0
    Pending Requests                         : 0
    Timeouts                                 : 0
    Bad Authenticators                       : 0
    Packets Dropped                          : 0
    Access Requests                          : 0
    Access challenge                         : 0
    Access Accepts                           : 0
    Access Rejects                           : 0
    Access Response Malformed                : 0
    Access Retransmits                       : 0
    Tracking Requests                        : 0
    Tracking Responses                       : 0
    Unknown Response Code                    : 0

6200-Lab#
```

```
6200-Lab# sh radius-server statistics accounting
 Server Name     : 192.168.1.95
 Auth-Port       : 1812
 Accounting-Port : 1813
 VRF             : default
 TLS Enabled     : No
```

```
  Accounting Statistics
  ------------------------
    Round Trip Time               : 0
    Pending Requests              : 0
    Timeouts                      : 0
    Bad Authenticators            : 0
    Packets Dropped               : 0
    Accounting Requests           : 0
    Accounting Responses          : 0
    Accounting Response Malformed : 0
    Accounting Retransmits        : 0
    Unknown Response Code         : 0
 Server Name     : 192.168.1.95
 Auth-Port       : 1812
 Accounting-Port : 1813
 VRF             : mgmt
 TLS Enabled     : No

  Accounting Statistics
  ------------------------
    Round Trip Time               : 0
    Pending Requests              : 0
    Timeouts                      : 0
    Bad Authenticators            : 0
    Packets Dropped               : 0
    Accounting Requests           : 0
    Accounting Responses          : 0
    Accounting Response Malformed : 0
    Accounting Retransmits        : 0
    Unknown Response Code         : 0
6200-Lab#
```

3.5 Interface Configuration

Here we are using interface 1/1/1 for testing and connecting our wired client.

```
interface 1/1/1
    no shutdown
    no routing
    vlan access 1
    loop-protect
    spanning-tree port-type admin-edge

    aaa authentication port-access allow-cdp-bpdu
    aaa authentication port-access allow-lldp-bpdu
    aaa authentication port-access client-limit 2
    aaa authentication port-access critical-role Critical-Role
    aaa authentication port-access dot1x authenticator
        max-eapol-requests 1
        max-retries 1
        enable
    aaa authentication port-access mac-auth
        enable

    client track ip enable
    client track ip update-interval 60
```

3.6 NTP Configuration

Its always a good practise to have this configured.

```
clock timezone australia/melbourne
radius-server tracking interval 3600
ntp server 192.168.1.130 iburst
ntp server 216.239.35.12 iburst
```

```
ntp server pool.ntp.org minpoll 4 maxpoll 4 iburst
ntp enable
ntp vrf mgmt
```

You can check the status of NTP with these commands.

```
6200-Lab# sh ntp associations
-------------------------------------------------------------------------
 ID            NAME          REMOTE          REF-ID ST LAST POLL REACH
-------------------------------------------------------------------------
+ 1   192.168.1.130   192.168.1.130   180.150.12.46  2   93  128    37
+ 2  time.cloudflar   162.159.200.1      10.47.8.71  3    9   16   377
* 3  time4.google.c   216.239.35.12          .GOOG.  1  122  128     3
-------------------------------------------------------------------------
6200-Lab#
```

```
6200-Lab# sh ntp server
-----------------------------------------------------
           NTP SERVER KEYID MINPOLL MAXPOLL OPTION VER
-----------------------------------------------------
        192.168.1.130    --       6      10 iburst   4
        216.239.35.12    --       6      10 iburst   4 prefer(auto)
pool.ntp.org(default)    --       4       4 iburst   4
-----------------------------------------------------
6200-Lab#

6200-Lab# sh ntp status
NTP Status Information

NTP                          : Enabled
NTP DHCP                     : Enabled
NTP Authentication           : Disabled
NTP Server Connections       : Using the mgmt VRF

System time                  : Thu Jan  5 10:38:45 AEDT 2023
NTP uptime                   : 1 hours, 12 minutes, 20 seconds

NTP Synchronization Information

NTP Server                   : 216.239.35.12 at stratum 1
Poll interval                : 64 seconds
Time accuracy                : Within 0.005351 seconds
Reference time               : Thu Jan  5 2023 10:37:53.967 as per
Australia/Melbourne
6200-Lab#
```

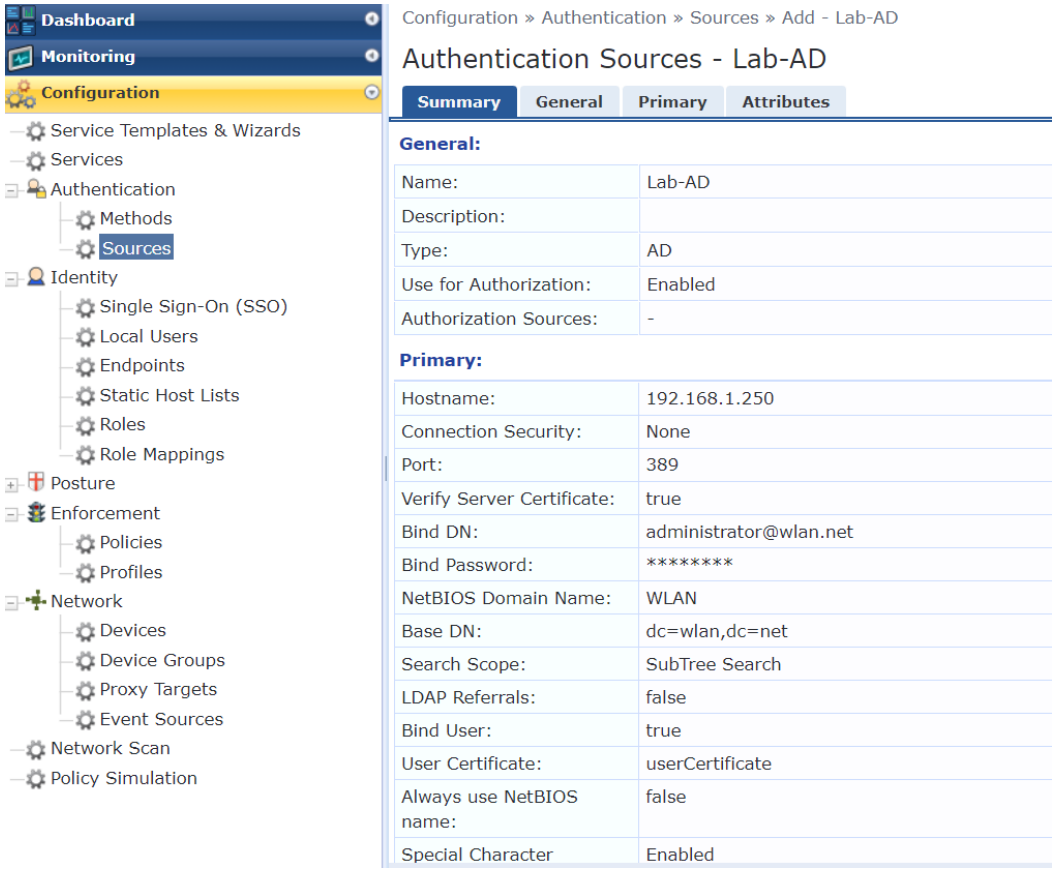
4 ClearPass LUR dot1x Auth Configuration

In this section we'll be exploring the local user role approach for CX switches to provide differentiated access based on AD user group memberships.

Note that ClearPass has already joined the Lab AD domain and its corresponding authentication source configured.

4.1 Authentication Sources

You need to add the AD domain as an authentication source so CPPM can authenticate against it.



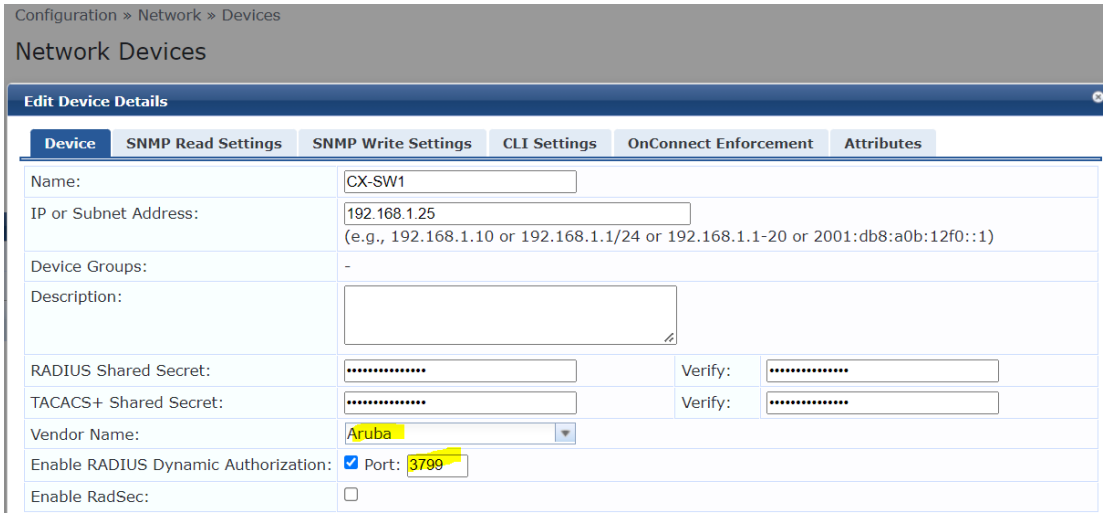
Summary | General | Primary | Attributes

Specify filter queries used to fetch authentication and authorization attributes

	Filter Name	Attribute Name	Alias Name	Enabled As
1.	Authentication	dn	UserDN	-
		department	Department	-
		title	Title	-
		company	company	-
		memberOf	memberOf	-
		telephoneNumber	Phone	-
		mail	Email	-
		displayName	Name	-
		accountExpires	Account Expires	-
2.	Group	cn	Groups	-
3.	Machine	dNSHostName	HostName	-
		operatingSystem	OperatingSystem	-
		operatingSystemServicePack	OSServicePack	-
4.	Onboard Device Owner	memberOf	Onboard memberOf	-
5.	Onboard Device Owner Group	cn	Onboard Groups	-

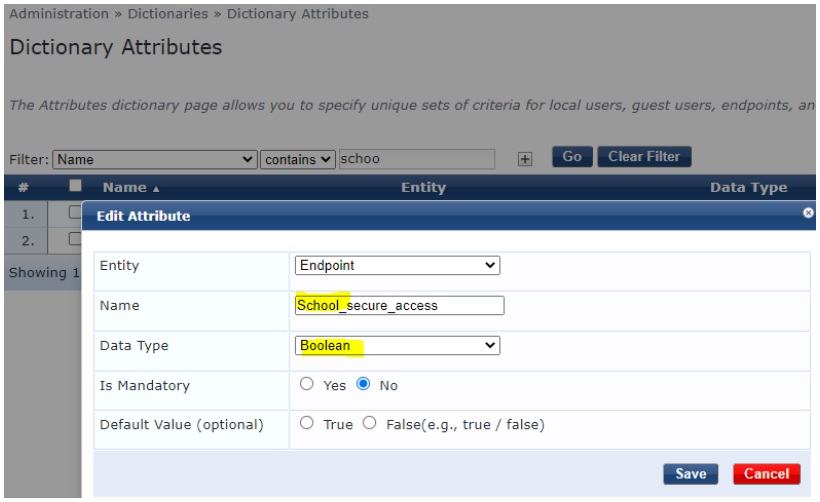
4.2 Adding Network Access Device

Here we need to add the Aruba CX switch to ClearPass as a NAD. Note that vendor name is Aruba.



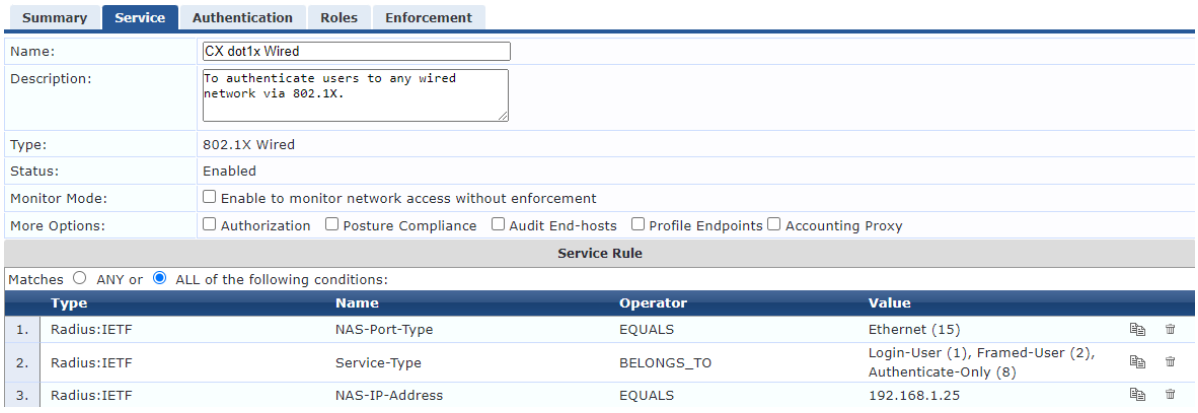
4.3 Endpoint Dictionary Attribute

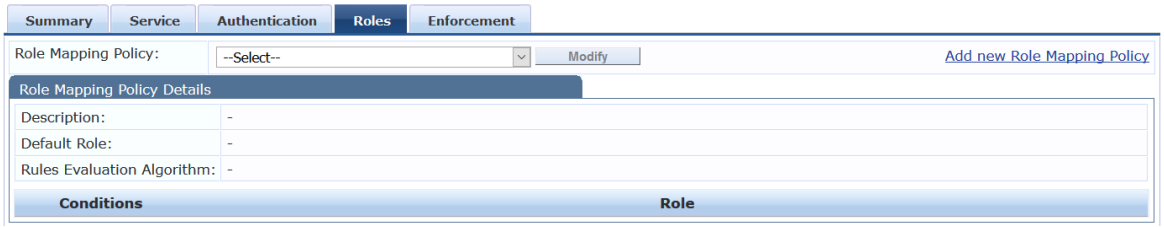
Here we'll create an attribute "School_secure_access" in the endpoint DB so that we can track devices that go through dot1x authentication and then based on that we could have a policy rule to deny access for them to join Guest network.



4.4 Services – CX dot1x Wired with Local User Role

For dot1x authentication with Local User Role (LUR) we need the following service.





The default role here is deny all, but you could have an enforcement profile to send back say a guest user role.

4.5 Enforcement Profiles

Here are the enforcemet profiles used.

Summary | Profile | Attributes

Profile:

Name:	CX dot1x Wired Staff
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	Staff
2.	Radius:IETF	Session-Timeout	=	28800
3.	Radius:IETF	User-Name	=	%{Radius:IETF:User-Name}

Summary | Profile | Attributes

Profile:

Name:	CX dot1x Wired Student
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	Student
2.	Radius:IETF	Session-Timeout	=	28800
3.	Radius:IETF	User-Name	=	%{Radius:IETF:User-Name}

Summary | Profile | Attributes

Profile:

Name:	CX Update Endpoint sec-access
Description:	System-defined profile to change Endpoint's status to Known
Type:	Post_Authentication
Action:	
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Endpoint	School_secure_access	=	true

4.6 Service for RADIUS Server Tracking

This is for successfully matching the RADIUS server tracking username that we configured on the switch. Remember we had configured this command on the switch

```
radius-server tracking user-name radius-tracking-user password plaintext aruba
```

Summary | Service | Authentication | Roles | Enforcement

Name:	Aruba switch RADIUS-Tracking
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	User-Name	EQUALS	radius-tracking-user
2.	Radius:IETF	NAS-IP-Address	EQUALS	192.168.1.25

Summary | Service | Authentication | Roles | Enforcement

Authentication Methods: [PAP] — Move Up ↑ | Move Down ↓ | Remove | View Details | Modify

--Select to Add--

Authentication Sources: [Local User Repository] [Local SQL DB] — Move Up ↑

Summary | Service | Authentication | Roles | Enforcement

Use Cached Results:	☐ Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:	[Sample Allow Access Policy] Modify

Enforcement Policy Details

Description:	Sample policy to allow network access
Default Profile:	[Allow Access Profile]
Rules Evaluation Algorithm:	evaluate-all

	Conditions	Enforcement Profiles
1.	(Date:Day-of-Week *BELONGS_TO* Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday)	[Allow Access Profile]

Next, we'll configure a local user for radius-tracking.

Configuration » Identity » Local Users

Local Users

ClearPass Policy Manager lists all local users in the Local Users page.

Filter: User ID contains Go Clear Filter

#		User ID ▲	Name	Role
1.	☐	InstantAP	InstantAP	InstantAP
2.	☐	radius-tracking-user	radius-tracking-user	[Employee]

Now when the CX switch sends out PAP auth to check the reachability of if RADIUS server, the auth request will be successful. See below

Summary | Input | Output

Login Status:	ACCEPT
Session Identifier:	R00000048-01-63b7bc22
Date and Time:	Jan 06, 2023 17:13:54 AEDT
End-Host Identifier:	-
Username:	radius-tracking-user
Access Device IP/Port:	192.168.1.25 (CX-SW1 / Aruba)
Access Device Name:	6200-Lab
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	Aruba switch RADIUS-Tracking
Authentication Method:	PAP
Authentication Source:	Local:localhost
Authorization Source:	[Local User Repository]
Roles:	[Employee], [User Authenticated]
Enforcement Profiles:	[Allow Access Profile]

Summary | **Input** | Output

Username:	radius-tracking-user	
End-Host Identifier:	-	
Access Device IP/Port:	192.168.1.25	(CX-SW1 / Aruba)

RADIUS Request

Radius:IETF:NAS-Identifier	6200-Lab
Radius:IETF:NAS-IP-Address	192.168.1.25
Radius:IETF:NAS-IPv6-Address	fd14:5f94:8156:2600:bed7:a5ff:fec0:e5c1
Radius:IETF:User-Name	radius-tracking-user

Computed Attributes

Authentication:Full-Username	radius-tracking-user
Authentication:Full-Username-Normalized	radius-tracking-user
Authentication:MacAuth	NotApplicable
Authentication:OuterMethod	PAP
Authentication:Posture	Unknown
Authentication:Source	[Local User Repository]
Authentication:Status	User
Authentication:Username	radius-tracking-user
Authorization:Sources	[Local User Repository]
Connection:Dest-IP-Address	192.168.1.95
Connection:Dest-Port	1812
Connection:NAD-IP-Address	192.168.1.25
Connection:Protocol	RADIUS
Connection:Src-IP-Address	192.168.1.25
Connection:Src-Port	60163

Summary | Input | **Output**

Enforcement Profiles:	[Allow Access Profile]
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

4.7 Testing Dot1x with LUR

Now we are ready for our wired dot1x testing, here is our user table for reference.

AD-Group membership	Enforcement Profile	Aruba-User-Role	VLAN
Staff	CX dot1x Wired Staff	Staff	11
Students	CX dot1x Wired Student	Students	12

Before we start let's have a look at configured user-roles.

```
6200-Lab# sh port-access role

Role Information:
Attributes overridden by RADIUS are prefixed by '*'.

Name   : Critical-Role
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                         : 13
    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                        :
    PVLAN Port Type                     :
    Captive Portal Profile              :
    Policy                              :
    Device Type                         :

Name   : Staff
Type   : local
-----------------------------------------------
    Reauthentication Period             : 3000 secs
    Cached Reauthentication Period      :
    Authentication Mode                 : client-mode
    Session Timeout                     :
    Client Inactivity Timeout           : 400 secs
    Description                         : LUR-for-Staff
    Gateway Zone                        :
    UBT Gateway Role                    :
    UBT Gateway Clearpass Role          :
    Access VLAN                         : 11
    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                        :
    PVLAN Port Type                     :
    Captive Portal Profile              :
    Policy                              : Staff-Pol
    Device Type                         :

Name   : Student
Type   : local
-----------------------------------------------
    Reauthentication Period             : 3000 secs
    Cached Reauthentication Period      :
    Authentication Mode                 : client-mode
    Session Timeout                     :
    Client Inactivity Timeout           : 400 secs
    Description                         : LUR-for-Student
    Gateway Zone                        :
    UBT Gateway Role                    :
    UBT Gateway Clearpass Role          :
    Access VLAN                         : 12
    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                        :
    PVLAN Port Type                     :
    Captive Portal Profile              :
    Policy                              : Student-Pol
    Device Type                         :

6200-Lab#
```

We'll now connect a laptop to port 1 of the switch and start testing the dot1x PEAP authentication. This is the staff member authenticating

Filter: Request ID contains Go Clear Filter Show 50 records

#	Server	Source	Username	Service	Login Status	Request Timestamp
1.	192.168.1.95	RADIUS	staff1	CX dot1x Wired	ACCEPT	2023/01/05 16:06:01
2.	192.168.1.95	RADIUS	radius-tracking-user	Aruba switch RADIUS-Tracking	ACCEPT	2023/01/05 16:01:37
3.	192.168.1.95	RADIUS	radius-tracking-user	Aruba switch RADIUS-Tracking	ACCEPT	2023/01/05 15:55:30

Session #1 shows the successful dot1x authentication, but the other two sessions are result of radius tracking that we configured on the switch.

Summary | Input | Output | Accounting

Login Status:	ACCEPT
Session Identifier:	R0000000e-01-63b65ab8
Date and Time:	Jan 05, 2023 16:06:01 AEDT
End-Host Identifier:	28-D2-44-52-C2-38 (Computer / Windows / Windows 10)
Username:	staff1
Access Device IP/Port:	192.168.1.25:1 (CX-SW1 / Aruba)
Access Device Name:	6200-Lab
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	CX dot1x Wired
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2
Authentication Source:	AD:192.168.1.250
Authorization Source:	Lab-AD
Roles:	[User Authenticated]
Enforcement Profiles:	CX Update Endpoint sec-access, CX dot1x Wired Staff

Summary | Input | Output | Accounting

RADIUS Request

Radius:IETF:Called-Station-Id	BC-D7-A5-C0-E5-C0
Radius:IETF:Calling-Station-Id	28-D2-44-52-C2-38
Radius:IETF:Framed-MTU	768
Radius:IETF:NAS-Identifier	6200-Lab
Radius:IETF:NAS-IP-Address	192.168.1.25
Radius:IETF:NAS-IPv6-Address	fd14:5f94:8156:2600:bed7:a5ff:fec0:e5c1
Radius:IETF:NAS-Port	1
Radius:IETF:NAS-Port-Id	1/1/1
Radius:IETF:NAS-Port-Type	15
Radius:IETF:Service-Type	2
Radius:IETF:User-Name	staff1

Authorization Attributes

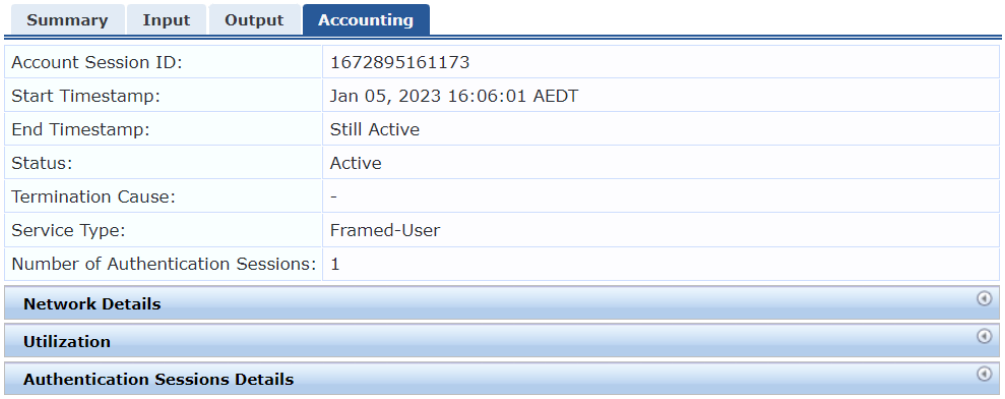
Authorization:Lab-AD:Account Expires	9223372036854775807 [30828-09-14 12:48:05 AEST]
Authorization:Lab-AD:Department	Staff
Authorization:Lab-AD:memberOf	CN=Administrators,CN=Builtin,DC=wlan,DC=net, CN=Staff,CN=Users,DC=wlan,DC=net
Authorization:Lab-AD:Name	staff1
Authorization:Lab-AD:Title	Teacher
Authorization:Lab-AD:UserDN	CN=staff1,CN=Users,DC=wlan,DC=net

Summary | Input | Output | Accounting

Enforcement Profiles:	CX Update Endpoint sec-access, CX dot1x Wired Staff
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

Endpoint:School_secure_access	true
Radius:Aruba:Aruba-User-Role	Staff
Radius:IETF:Session-Timeout	28800
Radius:IETF:User-Name	staff1



Now looking at the some of the show commands on the CX switch

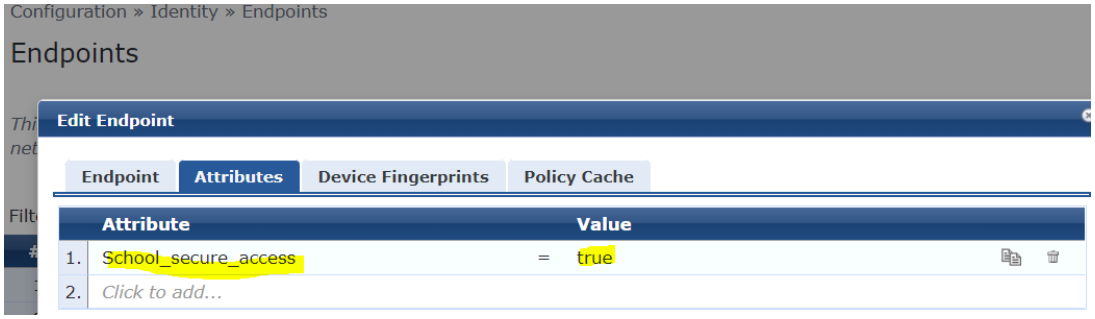
```
6200-Lab# sh port-access clients

Port Access Clients

Status Codes: d device-mode, c client-mode, m multi-domain

-------------------------------------------------------------------------------------------------------
  Port     MAC-Address       Onboarding     Status               Role
Device Type
                             Method
-------------------------------------------------------------------------------------------------------
c 1/1/1    28:d2:44:52:c2:38 dot1x          Success              Staff

6200-Lab#
```

```
6200-Lab# sh port-access clients detail

Port Access Client Status Details:

Client 28:d2:44:52:c2:38, staff1
================================
  Session Details
  ---------------
    Port         : 1/1/1
    Session Time : 895s
    IPv4 Address : 172.16.11.28
    IPv6 Address :
    Device Type  :

  VLAN Details
  ------------
    VLAN Group Name :
    VLANs Assigned  : 11
      Access          : 11
      Native Untagged :
      Allowed Trunk   :

  Authentication Details
  ----------------------
    Status          : dot1x Authenticated
    Auth Precedence : dot1x - Authenticated, mac-auth - Not attempted
    Auth History    : dot1x - Authenticated, 890s ago

  Authorization Details
  ---------------------
    Role   : Staff
    Status : Applied

Role Information:

Name   : Staff
Type   : local
```

```
-------------------------------------------
    Reauthentication Period             : 3000 secs
    Cached Reauthentication Period      :
    Authentication Mode                 : client-mode
    Session Timeout                     :
    Client Inactivity Timeout           : 400 secs
    Description                         : LUR-for-Staff
    Gateway Zone                        :
    UBT Gateway Role                    :
    UBT Gateway Clearpass Role          :
    Access VLAN                         : 11
    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                        :
    PVLAN Port Type                     :
    Captive Portal Profile              :
    Policy                              : Staff-Pol
    Device Type                         :

Access Policy Details:

Policy Name   : Staff-Pol
Policy Type   : Local
Policy Status : Applied

SEQUENCE    CLASS                         TYPE ACTION
----------- ----------------------------- ---- ----------------------------------
10          IP-Any-Any                    ipv4 permit

Class Details:

class ip IP-Any-Any
    10 match any any any

6200-Lab#
```

```
6200-Lab# sh client ip

 MAC Address               Interface        VLAN             IP Address
 ------------------------------------------------------------------------------
 28:d2:44:52:c2:38         1/1/1            11               172.16.11.28

6200-Lab#
```

Lastly, we'll check the endpoint attribute that we updated as part of the enforcement policy.



Looking at Session #2

Summary | Input | Output

Login Status:	ACCEPT
Session Identifier:	R0000000d-01-63b659b1
Date and Time:	Jan 05, 2023 16:01:37 AEDT
End-Host Identifier:	-
Username:	radius-tracking-user
Access Device IP/Port:	192.168.1.25 (CX-SW1 / Aruba)
Access Device Name:	6200-Lab
System Posture Status:	UNKNOWN (100)

Policies Used -

Service:	Aruba switch RADIUS-Tracking
Authentication Method:	PAP
Authentication Source:	Local:localhost
Authorization Source:	[Local User Repository]
Roles:	[Employee], [User Authenticated]
Enforcement Profiles:	[Allow Access Profile]

Summary | Input | Output

Username:	radius-tracking-user	
End-Host Identifier:	-	
Access Device IP/Port:	192.168.1.25	(CX-SW1 / Aruba)

RADIUS Request

Radius:IETF:NAS-Identifier	6200-Lab
Radius:IETF:NAS-IP-Address	192.168.1.25
Radius:IETF:NAS-IPv6-Address	fd14:5f94:8156:2600:bed7:a5ff:fec0:e5c1
Radius:IETF:User-Name	radius-tracking-user

Computed Attributes

Authentication:ErrorCode	0
Authentication:Full-Username	radius-tracking-user
Authentication:Full-Username-Normalized	radius-tracking-user
Authentication:MacAuth	NotApplicable
Authentication:OuterMethod	PAP
Authentication:Posture	Unknown
Authentication:Source	[Local User Repository]
Authentication:Status	User
Authentication:Username	radius-tracking-user
Authorization:Sources	[Local User Repository]
Connection:Dest-IP-Address	192.168.1.95
Connection:Dest-Port	1812
Connection:NAD-IP-Address	192.168.1.25
Connection:Protocol	RADIUS

Summary | Input | Output

Enforcement Profiles:	[Allow Access Profile]
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

Now we'll login with student1 credentials who is not in the Student user group, after successful authentication it will be put into a different VLAN along with different policy.

Access Tracker Jan 05, 2023 16:27:14 AEDT

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

[All Requests] victory2 (192.168.1.95) Last 1 day before Today

Filter: Request ID contains Go Clear Filter

#	Server	Source	Username	Service	Login Status
1.	192.168.1.95	RADIUS	student1	CX dot1x Wired	ACCEPT

Summary | Input | Output | Accounting

Login Status:	ACCEPT
Session Identifier:	R00000013-01-63b65f7e
Date and Time:	Jan 05, 2023 16:26:22 AEDT
End-Host Identifier:	28-D2-44-52-C2-38 (Computer / Windows / Windows 10)
Username:	student1
Access Device IP/Port:	192.168.1.25:1 (CX-SW1 / Aruba)
Access Device Name:	6200-Lab
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	CX dot1x Wired
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2
Authentication Source:	AD:192.168.1.250
Authorization Source:	Lab-AD
Roles:	[User Authenticated]
Enforcement Profiles:	CX Update Endpoint sec-access, CX dot1x Wired Student

Summary | Input | **Output** | Accounting

Enforcement Profiles:	CX Update Endpoint sec-access, CX dot1x Wired Student
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

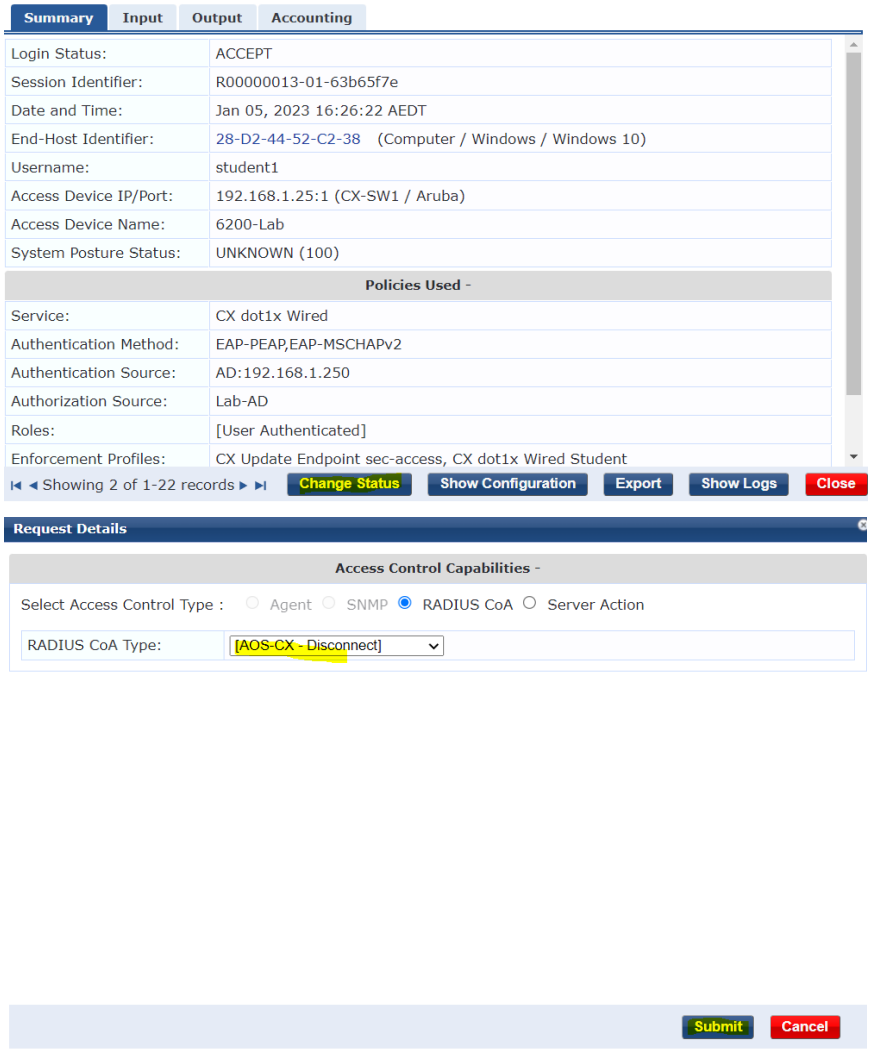
RADIUS Response

Endpoint:School_secure_access	true
Radius:Aruba:Aruba-User-Role	Student
Radius:IETF:Session-Timeout	28800
Radius:IETF:User-Name	student1

```
6200-Lab# sh port-access clients

Port Access Clients

Status Codes: d device-mode, c client-mode, m multi-domain

------------------------------------------------------------------------------
  Port     MAC-Address       Onboarding     Status               Role
Device Type
                           Method
------------------------------------------------------------------------------
c 1/1/1    28:d2:44:52:c2:38 dot1x          Success              Student

6200-Lab#
```

```
6200-Lab# sh client ip

 MAC Address               Interface        VLAN             IP Address
 ------------------------------------------------------------------------
 28:d2:44:52:c2:38         1/1/1            12               172.16.12.28

6200-Lab#
```

Lastly, we'll test the CoA




```
6200-Lab# sh radius dyn-authorization
Status and Counters - RADIUS Dynamic Authorization Information

  RADIUS Dynamic Authorization                    : Enabled
  RADIUS Dynamic Authorization UDP Port           : 3799
  Invalid Client Addresses in CoA Requests        : 0
  Invalid Client Addresses in Disconnect Requests: 0

Dynamic Authorization Client Information
========================================

IP Address           : 192.168.1.95
VRF                  : mgmt
TLS Enabled          : No
Replay Protection    : Disabled
Time Window          : 300
Disconnect Requests  : 2
Disconnect ACKs      : 2
Disconnect NAKs      : 0
CoA Requests         : 0
CoA ACKs             : 0
CoA NAKs             : 0
Shared-Secret        : AQBapcxIKpxsuGo4y8/1/o0mApzzTGrciXUTqFlh5jbvhcS/BQAAADRR1eg1
6200-Lab#
```