Contents

1.1 Revision History

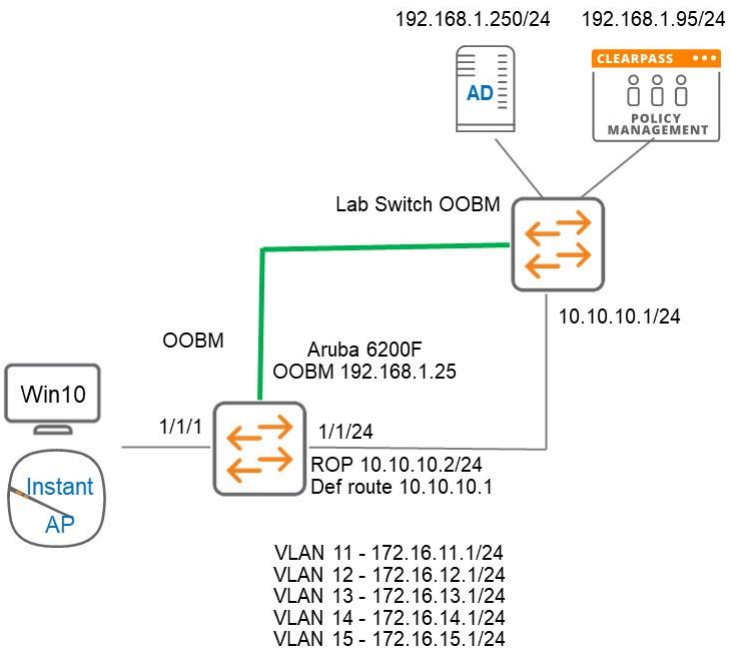
DATE	VERSION	EDITOR	CHANGES
10 Jan 2023	0.1	Ariya Parsamanesh	Initial creation

2 ClearPass Wired Enforcement for CX Switches Part 4

This is the final part of 4x parts series on Aruba CX switch wired enforcement and the main objective of this guide is to build on the first three parts. Here we'll cover downloadable user roles (DUR).

We'll use DUR for

- Wired dot1x clients
- Wired Captive portal for guests
- Wired Captive portal for AD users
- Instant APs (IAP) that use dot1x for AP authentication
- IAP profiling
- Wireless clients that connect to IAPs



2.1 Things you need

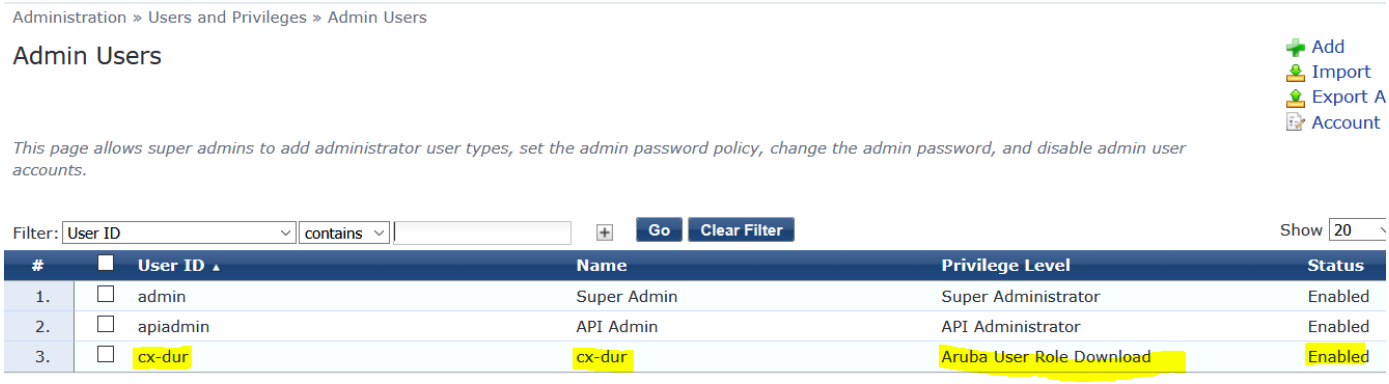
- ClearPass Policy Manager 6.9.7 (VM)
- Aruba CX switch running firmware version 10.10.1020
- Instant AP firmware version 8.11.0.1
- A wired connected laptop.

We assume the reader has gone through the first three parts of this 4x parts series.

3 Downloadable User Roles

Downloadable user roles (DUR) allows ClearPass to be the centralised policy point and send all the user roles and its related policies to the LAN switch. This means we don't have to configure the user-roles, and its policies on the LAN switches. In this example we have an AD group called Executives and they will be in their own user-role and VLAN.

First, we'll create a user credentials that the CX switch will use to download the user role from ClearPass.



Here is the corresponding switch command

```
radius-server host victory2.arubatechs.com key plaintext sdsda clearpass-username cx-dur clearpass-password ciphertext sdsds vrf mgmt.
```

Next, we need to ensure the following

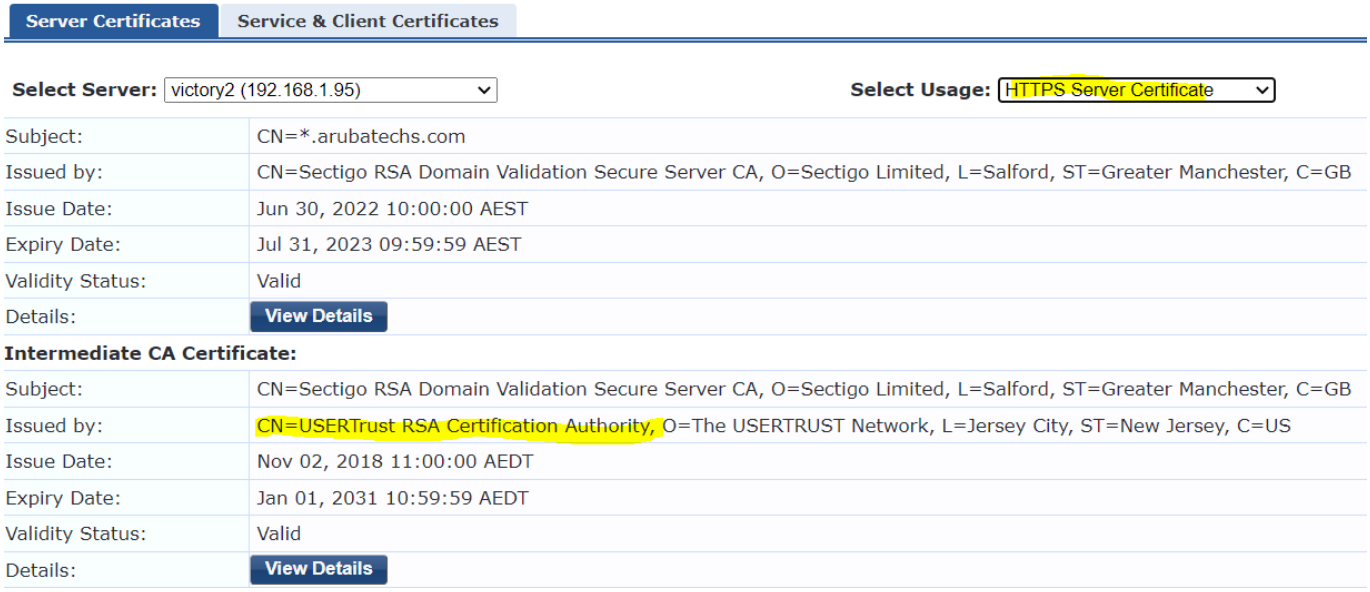
- ClearPass server should have a valid DNS entry and switch should point to the name of the server not IP
- Root certificate of the HTTPS server certificate should be installed in the switch.
- NTP should be configured
- DNS Server IP address should be configured in the switch which will resolve the Radius server IP address

```
clock timezone australia/melbourne
ntp server 216.239.35.12 iburst
ntp enable
ntp vrf mgmt.

aaa group server radius ClearPass
    server victory2.clearpass.info vrf mgmt
aaa accounting port-access start-stop interim 5 group ClearPass

radius dyn-authorization client victory2.arubatechs.com secret-key dsds vrf mgmt

ip dns server-address 192.168.1.250 vrf mgmt.
```

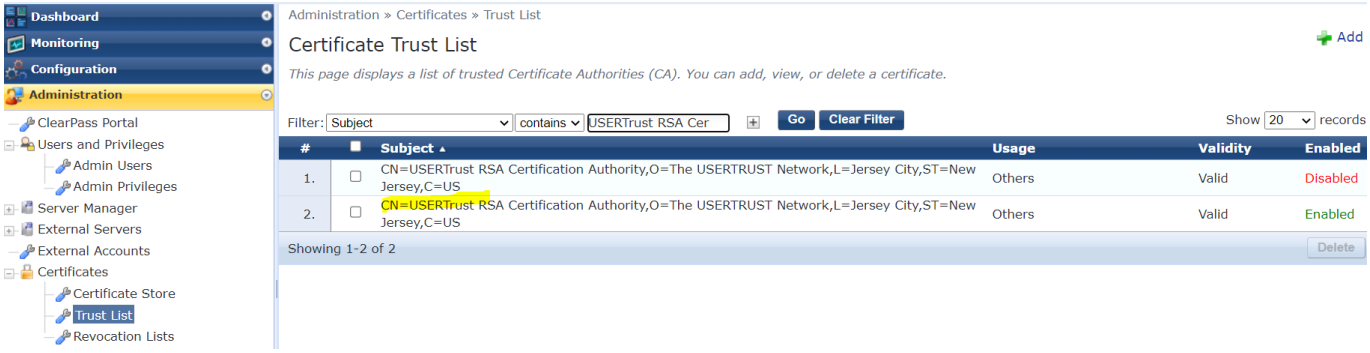
3.1 Root Certificate Configuration

As mentioned earlier we should install the Root certificate of ClearPass's HTTPS server certificate in the switch

Here we are using a wild card cert for ClearPass.



In this release of CX-switch OS, you need to manually install the root certificate. First you need to identify the root certificate. Then from ClearPass Certificate trust list we export this cert in PEM format and install it manually on the switch either by copy and paste or through TFTP.



The file that gets exported will be a CRT file which you can open in notepad. Here is the content of that file.

```
-----BEGIN CERTIFICATE-----
MIIDdTCCAl2gAwIBAgILBAAAAAABFUtaw5QwDQYJKoZIhvcNAQEFBQAwVzELMAkG
A1UEBhMCQkUxGTAXBgNVBAoTEEdsb2JhbFNpZ24gbnYtc2ExEDAOBgNVBAsTB1Jv
AbEVtQwdpf5pLGkkeB6zpxxxYu7KyJesF12KwvhHhm4qxFYxldBniYUr+WymXUad
Removed a lot of lines here 3kHMB65jUr9TU/Qr6cf9tveCX4XSQRjbgbME
HMUfpIBvFSDJ3gyICh3WZlXi/EjJKSZp4A==
-----END CERTIFICATE-----
```

Now from the CX-switch, you can use this command to paste the root certificate in. You need to ensure you copy all of the contents of the certificate including "----BEGIN" and "---END" lines.

```
6200-Lab(config)# crypto pki ta-profile USERTrust
6200-Lab(config-ta-USERTrust)# ta-certificate
Paste the certificate in PEM format below, then hit enter and ctrl-D:
6200-Lab(config-ta-cert)# -----BEGIN CERTIFICATE-----
6200-Lab(config-ta-cert)# MIIFgTCCBGmgAwIBAgIQOXJEOvkit1HX02wQ3TE1lTANBgkqhkiG9w0BAQwFADB7
6200-Lab(config-ta-cert)# Removed a lot of lines here
6200-Lab(config-ta-cert)# MQswCQYDVQQGEwJHQjEbMBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYD
6200-Lab(config-ta-cert)#
6200-Lab(config-ta-cert)# -----END CERTIFICATE-----
6200-Lab(config-ta-cert)#ctld-D

The certificate you are importing has the following attributes:
Subject: C = US, ST = New Jersey, L = Jersey City, O = The USERTRUST Network, CN = USERTrust
RSA Certification Authority
Issuer:  C = GB, ST = Greater Manchester, L = Salford, O = Comodo CA Limited, CN = AAA
Certificate Services
Serial Number: 0x3972443AF922B751D7D36C10DD313595
TA certificate import is allowed only once for a TA profile
```

```
Do you want to accept this certificate (y/n)? y
6200-Lab(config-ta-USERTrust)#
```

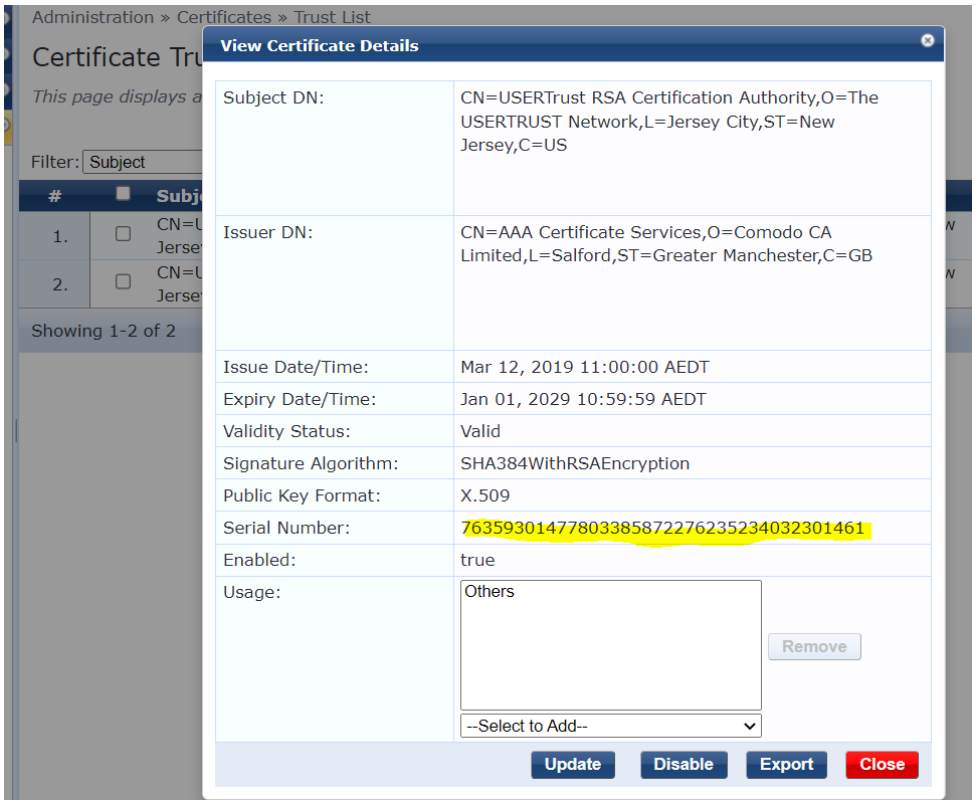
Now let's check the ta-profile to see the certificate details.

```
6200-Lab(config)# sh crypto pki ta-profile

TA Profile Name                   TA Certificate       Revocation Check
--------------------------------- -------------------- ----------------
USERTrust                         Installed, valid     disabled
```

```
6200-Lab(config)# sh crypto pki ta-profile USERTrust

  TA Profile Name    : USERTrust
  Revocation Check   : disabled
    OCSP Primary URL: Not Configured
    OCSP Secondary URL: Not Configured
    OCSP Enforcement-level: strict
    OCSP Disable Nonce: false
    OCSP VRF           : mgmt
  TA Certificate     : Installed and valid
   Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            39:72:44:3a:f9:22:b7:51:d7:d3:6c:10:dd:31:35:95
    Signature Algorithm: sha384WithRSAEncryption
        Issuer: C=GB, ST=Greater Manchester, L=Salford, O=Comodo CA Limited, CN=AAA
Certificate Services
        Validity
            Not Before: Mar 12 00:00:00 2019 GMT
            Not After : Dec 31 23:59:59 2028 GMT
        Subject: C=US, ST=New Jersey, L=Jersey City, O=The USERTRUST Network,
CN=USERTrust RSA Certification Authority
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:80:12:65:17:36:0e:c3:db:08:b3:d0:ac:57:0d:
                    76:ed:cd:27:d3:4c:ad:50:83:61:e2:aa:20:4d:09:
                    Removed a lot of lines here   2e:43:1a:4c:b4:
                    b8:0e:2b:a9:f2:4c:97:1c:07:3f:0d:52:f5:ed:ef:
                    2f:82:0f
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                keyid:A0:11:0A:23:3E:96:F1:07:EC:E2:AF:29:EF:82:A5:7F:D0:30:A4:B4

            X509v3 Subject Key Identifier:
                53:79:BF:5A:AA:2B:4A:CF:54:80:E1:D8:9B:C0:9D:F2:B2:03:66:CB
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Certificate Policies:
                Policy: X509v3 Any Policy

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://crl.comodoca.com/AAACertificateServices.crl

            Authority Information Access:
                OCSP - URI:http://ocsp.comodoca.com
```

```
    Signature Algorithm: sha384WithRSAEncryption
         18:87:51:dc:74:21:3d:9c:8a:e0:27:b7:33:d0:2e:cc:ec:f0:
         e6:cb:5e:11:de:22:6f:9b:75:8e:9e:72:fe:e4:d6:fe:aa:1f:
         Removed a lot of lines here   6f:72:3c:43:3b:c0:3f:eb:
         80:bc:6a:78:cf:b8:7f:8e:76:72:99:0c:9d:fe:d7:91:08:16:
         a1:a3:5f:95

6200-Lab#
```

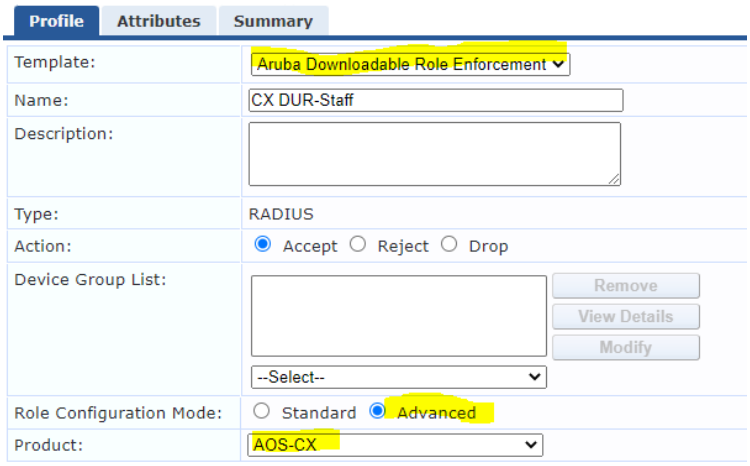
The serial number is “39:72:44:3a:f9:22:b7:51:d7:d3:6c:10:dd:31:35:95” and its decimal conversion is 76359301477803385872276235234032301461 which is same as the one we in ClearPass



Note that there is an NAE agent that does this as well, which makes it easier. You can ask your local Aruba SE for it.

3.2 ClearPass Service Configuration

We’ll create new DUR enforcement profiles for staff and students.



Here we are using the advance mode.

Enforcement Profiles

Profile | Attributes | Summary

	Type	Name		Value
1.	Radius:Aruba	Aruba-CPPM-Role	=	class ip IP-Any-Any2 10 match any any any port-access policy Staff-Pol2 10 class ip IP-Any-Any2 port-access role Staff2 description DUR-for-Staff associate policy Staff-Pol2 auth-mode client-mode client-inactivity timeout 400 trust-mode none reauth-period 3000 vlan access 11

```
class ip IP-Any-Any2
    10 match any any any

port-access policy Staff-Pol2
    10 class ip IP-Any-Any2

port-access role Staff2
    description DUR-for-Staff
    associate policy Staff-Pol2
    auth-mode client-mode
    client-inactivity timeout 400
    trust-mode none
    reauth-period 3000
    vlan access 11
```

Similarly, we'll create DUR enforcement profile for Students.

Summary | Profile | Attributes

Profile:

Name:	CX-DUR-Student
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-
Product:	AOS-CX

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-CPPM-Role	=	class ip IP-Any-Any2 10 match any any any port-access policy Student-Pol2 10 class ip IP-Any-Any2 port-access role Student2 description DUR-for-Student associate policy Student-Pol2 auth-mode client-mode client-inactivity timeout 400 trust-mode none reauth-period 3000 vlan access 12

```
class ip IP-Any-Any2
    10 match any any any

port-access policy Student-Pol2
    10 class ip IP-Any-Any2

port-access role Student2
    description DUR-for-Student
    associate policy Student-Pol2
    auth-mode client-mode
```

```
    client-inactivity timeout 400
    trust-mode none
    reauth-period 3000
    vlan access 11
```

Now I just copied the previous CX dot1x service and renamed it and then change the enforcement policy to use the new DUR enforcement profiles we created. Here is the complete DUR service.

Services

Add
Import
Export All

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

Filter: Name contains wir Go Clear Filter Show 20 records

#		Order	Name	Type	Template	Status
1.	☐	10	CX dot1x Wired	RADIUS	802.1X Wired	
2.	☐	11	CX DUR dot1x Wired	RADIUS	802.1X Wired	

Services - CX DUR dot1x Wired

Summary | Service | Authentication | Roles | Enforcement

Name:	CX DUR dot1x Wired
Description:	To authenticate users to any wired network via 802.1X.
Type:	802.1X Wired
Status:	Enabled
Monitor Mode:	☐ Enable to monitor network access without enforcement
More Options:	☐ Authorization ☐ Posture Compliance ☐ Audit End-hosts ☐ Profile Endpoints ☐ Accounting Proxy

Service Rule

Matches ○ ANY or ◉ ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	EQUALS	Ethernet (15)
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)
3.	Radius:IETF	NAS-IP-Address	EQUALS	192.168.1.25

Summary | Service | Authentication | Roles | Enforcement

Authentication Methods:	[EAP PEAP] [EAP TLS] [EAP MSCHAPv2] --Select to Add--
Authentication Sources:	[Local User Repository] [Local SQL DB] Lab-AD [Active Directory]

Move Up ↑ | Move Down ↓ | Remove | View Details | Modify

Summary | Service | Authentication | Roles | Enforcement

Use Cached Results:	☐ Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:	Wired 802.1X Wired DUR Enforcement Policy Modify

Enforcement Policy Details

Description:	
Default Profile:	CX dot1x Wired Default Profile
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Authorization:Lab-AD:memberOf *CONTAINS* Staff)	CX-DUR-Staff, [Update Endpoint Known]
2.	(Authorization:Lab-AD:memberOf *CONTAINS* Student)	CX-DUR-Student, [Update Endpoint Known]
3.	(Tips:Role *EQUALS* InstantAP)	CX-DUR-InstantAP-1x

3.3 DUR Dot1x Testing

The user staff1 connects to the LAN switch port 1/1/1 and we then see the dot1x request in access tracker.

Filter: Request ID contains Go Clear Filter

#	Server	Source	Username	Service	Login Status	Enforcement Profiles
1.	192.168.1.95	RADIUS	staff2	CX DUR dot1x Wired	ACCEPT	[Update Endpoint Known], CX-DUR-Staff

Summary | Input | Output | Accounting

Login Status:	ACCEPT
Session Identifier:	R00000041-01-63bcfe41
Date and Time:	Jan 10, 2023 16:57:22 AEDT
End-Host Identifier:	28-D2-44-52-C2-38 (Computer / Windows / Windows 10)
Username:	staff2
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 DUR dot1x Wired
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2
Authentication Source:	AD:192.168.1.250
Authorization Source:	Lab-AD
Roles:	[User Authenticated]
Enforcement Profiles:	[Update Endpoint Known], CX-DUR-Staff

Summary | Input | Output | Accounting

Enforcement Profiles:	[Update Endpoint Known], CX-DUR-Staff
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

Radius:Aruba:Aruba-CPPM-Role	CX_DUR_Staff-3020-5 class ip IP-Any-Any2 10 match any any any port-access policy Staff-Pol2 10 class ip IP-Any-Any2 port-access role Staff2 description DUR-for-Staff associate policy Staff-Pol2 auth-mode client-mode client-inactivity timeout 400 trust-mode none reauth-period 3000 vlan access 11

And we here is the output of relevant commands for verification.

```
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               CX_DUR_Staff-3020-5

6200-Lab#
```

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

Port Access Client Status Details:

Client 28:d2:44:52:c2:38, staff2
================================
  Session Details
  ---------------
    Port         : 1/1/1
    Session Time : 229s
    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, 223s ago

  Authorization Details
  ----------------------
    Role   : CX_DUR_Staff-3020-5
    Status : Applied

Role Information:

Name   : CX_DUR_Staff-3020-5
Type   : clearpass
Status: Completed
----------------------------------------------
    Reauthentication Period             : 3000 secs
    Cached Reauthentication Period      :
    Authentication Mode                 : client-mode
    Session Timeout                     :
    Client Inactivity Timeout           : 400 secs
    Description                         : DUR-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-Pol2_CX_DUR_Staff-3020-5
    Device Type                         :

Access Policy Details:
```

```
Policy Name   : Staff-Pol2_CX_DUR_Staff-3020-5
Policy Type   : Downloaded
Policy Status : Applied

SEQUENCE    CLASS                          TYPE ACTION
----------- ------------------------------ ---- ----------------------------------
10          IP-Any-Any2_CX_DUR_Staff-... ipv4 permit

Class Details:

class ip IP-Any-Any2_CX_DUR_Staff-3020-5
    10 match any any any

6200-Lab#
```

3.4 DUR with Captive Portal

Here we'll create the DUR version of the MAC auth and guest captive portal. We start with creating two advance DUR enforcement profile in ClearPass.

Enforcement Profiles - CX-DUR-Guest-CaptivePortal

Summary | Profile | Attributes

Profile:

Name:	CX-DUR-Guest-CaptivePortal
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-
Product:	AOS-CX

Attributes:

	Type	Name		Value
				class ip ClearPass2 10 match tcp any 192.168.1.95 eq 80 20 match tcp any 192.168.1.95 eq 443 class ip DHCP-DNS2 10 match udp any any eq 67 20 match udp any any eq 53 class ip ICMP2 10 match icmp any any class ip Web-Traffic2 10 match tcp any any eq 80 20 match tcp any any eq 443
1.	Radius:Aruba	Aruba-CPPM-Role	=	port-access policy cp_policy2 10 class ip DHCP-DNS2 20 class ip ICMP2 30 class ip ClearPass2 40 class ip Web-Traffic2 action redirect captive-portal aaa authentication port-access captive-portal-profile dur_user url https://victory2.arubatechs.com/guest/wired_school.php port-access role Captive-Portal2 description DUR-for-PreAuth associate captive-portal-profile dur_user associate policy cp_policy2 auth-mode client-mode client-inactivity timeout 400 trust-mode none reauth-period 3000 vlan access 13

Here is the details of the attribute value

```
class ip ClearPass2
    10 match tcp any 192.168.1.95 eq 80
    20 match tcp any 192.168.1.95 eq 443

class ip DHCP-DNS2
    10 match udp any any eq 67
    20 match udp any any eq 53
```

```
class ip ICMP2
    10 match icmp any any

class ip Web-Traffic2
    10 match tcp any any eq 80
    20 match tcp any any eq 443

port-access policy cp_policy2
    10 class ip DHCP-DNS2
    20 class ip ICMP2
    30 class ip ClearPass2
    40 class ip Web-Traffic2 action redirect captive-portal

aaa authentication port-access captive-portal-profile dur_user
    url https://victory2.arubatechs.com/guest/wired-school.php

port-access role Captive-Portal2
    description DUR-for-PreAuth
    associate captive-portal-profile dur_user
    associate policy cp_policy2
    auth-mode client-mode
    client-inactivity timeout 400
    trust-mode none
    reauth-period 3000
    vlan access 13
```

The second enforcement profile for successful MAC-auth

Enforcement Profiles - CX-DUR-MAC-Auth-Guest

Summary | Profile | Attributes

Profile:

Name:	CX-DUR-MAC-Auth-Guest
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-
Product:	AOS-CX

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-CPPM-Role	=	class ip IP-Any-Any2 10 match any any any port-access policy Guest-Pol2 10 class ip IP-Any-Any2 port-access role Guest2 description DUR-for-Guest associate policy Guest-Pol2 auth-mode client-mode client-inactivity timeout 400 trust-mode none reauth-period 3000 vlan access 14

Here is the details of the attribute value

```
class ip IP-Any-Any2
    10 match any any any

port-access policy Guest-Pol2
    10 class ip IP-Any-Any

port-access role Guest2
    description DUR-for-Guest
    associate policy Guest-Pol2
    auth-mode client-mode
    client-inactivity timeout 400
    trust-mode none
    reauth-period 3000
    vlan access 14
```

and finally, enforcement profile for AD user using the guest captive portal

Enforcement Profiles - CX-DUR-AD-Guest

Summary | Profile | Attributes

Profile:

Name:	CX-DUR-AD-Guest
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-
Product:	AOS-CX

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-CPPM-Role	=	class ip IP-Any-Any2 10 match any any any port-access policy AD-Guest-Pol2 10 class ip IP-Any-Any port-access role AD-Guest2 description DUR-for-AD-Guest associate policy AD-Guest-Pol2 auth-mode client-mode client-inactivity timeout 400 trust-mode none reauth-period 3000 vlan access 14

We'll create a new MAC auth service and we'll disable the LUR version of it.

10.	☐	10	CX dot1x Wired	RADIUS	802.1X Wired	
11.	☐	11	CX DUR dot1x Wired	RADIUS	802.1X Wired	
12.	☐	12	CX MAC Auth	RADIUS	MAC Authentication	
13.	☐	13	CX DUR MAC Auth	RADIUS	MAC Authentication	
14.	☐	14	CX GuestWebAuth	WEBAUTH	Web-based Authentication	

Showing 1-14 of 14 — Reorder | Copy | Export | Delete

Here are the details of "CX DUR MAC Auth" service.

Summary | Service | Authentication | Authorization | Roles | Enforcement | Profiler

Name:	CX DUR MAC Auth
Description:	MAC-based Authentication Service
Type:	MAC Authentication
Status:	Enabled
Monitor Mode:	☐ Enable to monitor network access without enforcement
More Options:	☑ Authorization ☐ Audit End-hosts ☑ Profile Endpoints ☐ Accounting Proxy

Service Rule

Matches ○ ANY or ◉ ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	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}

Summary | Service | Authentication | Authorization | Roles | Enforcement | Profiler

Authentication Methods: [Allow All MAC AUTH] — Move Up ↑ | Move Down ↓ | Remove | View Details | Modify — Add New Authentication Method

--Select to Add--

Authentication Sources: [Endpoints Repository] [Local SQL DB] — Move Up ↑ — Add New Authentication Source

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

Authorization Details:

Authorization sources from which role mapping attributes are fetched (for each Authentication Source)

	Authentication Source	Attributes Fetched From
1.	[Endpoints Repository] [Local SQL DB]	[Endpoints Repository] [Local SQL DB]

Additional authorization sources from which to fetch role-mapping attributes -

[Insight Repository] [Local SQL DB]
[Time Source] [Local SQL DB]
[Guest User Repository] [Local SQL DB]
[Guest Device Repository] [Local SQL DB]

Remove | View Details | Modify

Add New Authentication Source

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

Role Mapping Policy: Wired-CX MAC auth-role-mapping | Modify

Add New Role Mapping Policy

Role Mapping Policy Details

Description:	
Default Role:	[Other]
Rules Evaluation Algorithm:	evaluate-all

	Conditions	Role
1.	(Authorization:[Endpoints Repository]:Unique-Device-Count *EXISTS*) *AND* (Date:Date-Time *LESS_THAN* %{Endpoint:MAC-Auth Expiry})	[MAC Caching]
2.	(Endpoint:Guest Role ID *EQUALS* 1)	[Contractor]
3.	(Endpoint:Guest Role ID *EQUALS* 2)	[Guest]
4.	(Endpoint:Guest Role ID *EQUALS* 3)	[Employee]
5.	(Authorization:[Endpoints Repository]:Status *EQUALS* known) *OR* (Endpoint:School_secure_access *EQUALS* true)	School-Asset

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

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

Enforcement Policy: Ariya Wired-CX DUR MAC Auth | Modify

Add New Enforcement Policy

Enforcement Policy Details

Description:	
Default Profile:	CX-DUR-Guest-CaptivePortal
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Authorization:[Endpoints Repository]:Conflict *EQUALS* true)	Wired-CX-MAC-Spoof-CP
2.	(Tips:Role *EQUALS* School-Asset)	CX-DUR-CorpDev
3.	(Tips:Role *MATCHES_ALL* [MAC Caching] [Guest] [User Authenticated])	CX-DUR-MAC-Auth-Guest, CX Return-Endpoint-Username
4.	(Tips:Role *EQUALS* [MAC Caching]) *AND* (Endpoint:Guest Role ID *EQUALS* AD-User)	CX-DUR-AD-Guest, CX Return-Endpoint-Username

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

Endpoint Classification:

Select the classification(s) after which an action must be triggered -

Any Category / OS Family / Name

Remove

-- Select --

RADIUS CoA Action: [AOS-CX - Bounce Switch Port] | View Details | Modify

Add New RADIUS CoA Action

3.5 Testing DUR Guest Captive Portal with MAC Caching

Now we are ready to test. Here is the workflow for it.

- We'll get guest users connecting to interface 1/1/1 of the switch,
- There will be a MAC auth and the default enforcement profile will use "CX-DUR-Guest-CaptivePortal" to send the captive portal redirection configuration to the switch.

Here is the Access tracker

Summary | Input | Output | Accounting

Login Status:	ACCEPT
Session Identifier:	R00000005-01-63bde7dc
Date and Time:	Jan 11, 2023 09:34:04 AEDT
End-Host Identifier:	28-D2-44-52-C2-38 (Computer / Windows / Windows 10)
Username:	28d24452c238
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 DUR MAC Auth
Authentication Method:	MAC-AUTH
Authentication Source:	Local:localhost
Authorization Source:	[Guest User Repository], [Guest Device Repository], [Endpoints Repository], [Insight Repository], [Time Source]
Roles:	[Other], [User Authenticated]

Summary | **Input** | **Output** | Accounting

Enforcement Profiles:	CX-DUR-Guest-CaptivePortal
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

Radius:Aruba:Aruba-CPPM-Role	CX_DUR_Guest_CaptivePortal-3023-11 class ip ClearPass2 10 match tcp any 192.168.1.95 eq 80 20 match tcp any 192.168.1.95 eq 443 class ip DHCP-DNS2 10 match udp any any eq 67 20 match udp any any eq 53 class ip ICMP2 10 match icmp any any class ip Web-Traffic2 10 match tcp any any eq 80 20 match tcp any any eq 443

And this is what we see on the 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                  In-Progress


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 mac-auth        Success
CX_DUR_Guest_CaptivePortal-3023-7

6200-Lab#
```

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

Port Access Client Status Details:

Client 28:d2:44:52:c2:38, 28d24452c238
======================================
  Session Details
  ---------------
    Port         : 1/1/1
    Session Time : 17s
    IPv4 Address : 172.16.13.28
    IPv6 Address :
    Device Type  :

  VLAN Details
  ------------
    VLAN Group Name :
    VLANs Assigned  : 13
      Access          : 13
      Native Untagged :
      Allowed Trunk   :

  Authentication Details
  ----------------------
    Status          : mac-auth Authenticated
    Auth Precedence : dot1x - Unauthenticated, mac-auth - Authenticated
    Auth History    : mac-auth - Authenticated, 6s ago
                      dot1x - Unauthenticated, Supplicant-Timeout, 6s ago

  Authorization Details
  ----------------------
    Role   : CX_DUR_Guest_CaptivePortal-3023-9
    Status : Applied

Role Information:

Name   : CX_DUR_Guest_CaptivePortal-3023-9
Type   : clearpass
Status: Completed
----------------------------------------------
    Reauthentication Period             : 3000 secs
    Cached Reauthentication Period      :
    Authentication Mode                 : client-mode
    Session Timeout                     :
    Client Inactivity Timeout           : 400 secs
    Description                         : DUR-for-PreAuth
    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              : dur_user_CX_DUR_Guest_CaptivePortal-3023-9
    Policy                              : cp_policy2_CX_DUR_Guest_CaptivePortal-3023-9
    Device Type                         :

Captive Portal Profile Configuration
```

```
    Name                                : dur_user_CX_DUR_Guest_CaptivePortal-3023-9
    Type                                : downloaded
    URL                                 : https://victory2.arubatechs.com/guest/wired-school.php

Access Policy Details:

Policy Name   : cp_policy2_CX_DUR_Guest_CaptivePortal-3023-9
Policy Type   : Downloaded
Policy Status : Applied

SEQUENCE    CLASS                        TYPE ACTION
----------- ---------------------------- ---- ----------------------------------
10          DHCP-DNS2_CX_DUR_Guest_Ca... ipv4 permit
20          ICMP2_CX_DUR_Guest_Captiv... ipv4 permit
30          ClearPass2_CX_DUR_Guest_C... ipv4 permit
40          Web-Traffic2_CX_DUR_Guest... ipv4 redirect captive-portal

Class Details:

class ip DHCP-DNS2_CX_DUR_Guest_CaptivePortal-3023-9
    10 match udp any any eq dhcp-server
    20 match udp any any eq dns
class ip ICMP2_CX_DUR_Guest_CaptivePortal-3023-9
    10 match icmp any any
class ip ClearPass2_CX_DUR_Guest_CaptivePortal-3023-9
    10 match tcp any 192.168.1.95 eq http
    20 match tcp any 192.168.1.95 eq https
class ip Web-Traffic2_CX_DUR_Guest_CaptivePortal-3023-9
    10 match tcp any any eq http
    20 match tcp any any eq https

6200-Lab#
```

Checking the captive portal profile that was downloaded.

```
6200-Lab#  sh port-access captive-portal-profile

Captive Portal Profile Configuration

    Name                                : cp-profile
    Type                                : local
    URL                                 : https://192.168.1.95/guest/wired_guest.php

    Name                                : dur_user_CX_DUR_Guest_CaptivePortal-3023-11
    Type                                : downloaded
    URL                                 : https://victory2.arubatechs.com/guest/wired-school.php

6200-Lab#
```

As before the user will get redirected to the captive portal page and after the user uses cpuser credentials, it will see a wait for 30 sec.

And as before the WEBAUTH authentication comes in followed by a MAC auth.

#	Server	Source	Username	Service	Login Status	Enforcement Profiles	Request Timestamp
1.	192.168.1.95	RADIUS	cpuser	CX DUR MAC Auth	ACCEPT	CX-DUR-MAC-Auth-Guest, CX Return-Endpoint-Username	2023/01/11 09:37:43
2.	192.168.1.95	WEBAUTH	cpuser	CX GuestWebAuth	ACCEPT	CX-GuestMAC-Caching, CX MAC Caching Expire Post Login, [Update Endpoint Known], [AOS-CX - Bounce Switch Port]	2023/01/11 09:37:08
3.	192.168.1.95	RADIUS	28d24452c238	CX DUR MAC Auth	ACCEPT	CX-DUR-Guest-CaptivePortal	2023/01/11 09:34:04

Starting with Session #2, this authenticates the cpuser and then bounces the switch port.

Summary | Input | Output

Login Status:	ACCEPT
Session Identifier:	W00000001-01-63bde893
Date and Time:	Jan 11, 2023 09:37:08 AEDT
End-Host Identifier:	28-D2-44-52-C2-38
Username:	cpuser
Access Device IP/Port:	-
Access Device Name:	-
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	CX GuestWebAuth
Authentication Method:	Not applicable
Authentication Source:	[Guest User Repository]
Authorization Source:	[Guest User Repository], [Endpoints Repository], [Time Source]
Roles:	[Guest], [User Authenticated]
Enforcement Profiles:	CX-GuestMAC-Caching, CX MAC Caching Expire Post Login, [Update Endpoint

Summary | Input | **Output**

Enforcement Profiles:	CX-GuestMAC-Caching, CX MAC Caching Expire Post Login, [Update Endpoint Known], [AOS-CX - Bounce Switch Port]
System Posture Status:	UNKNOWN (100)

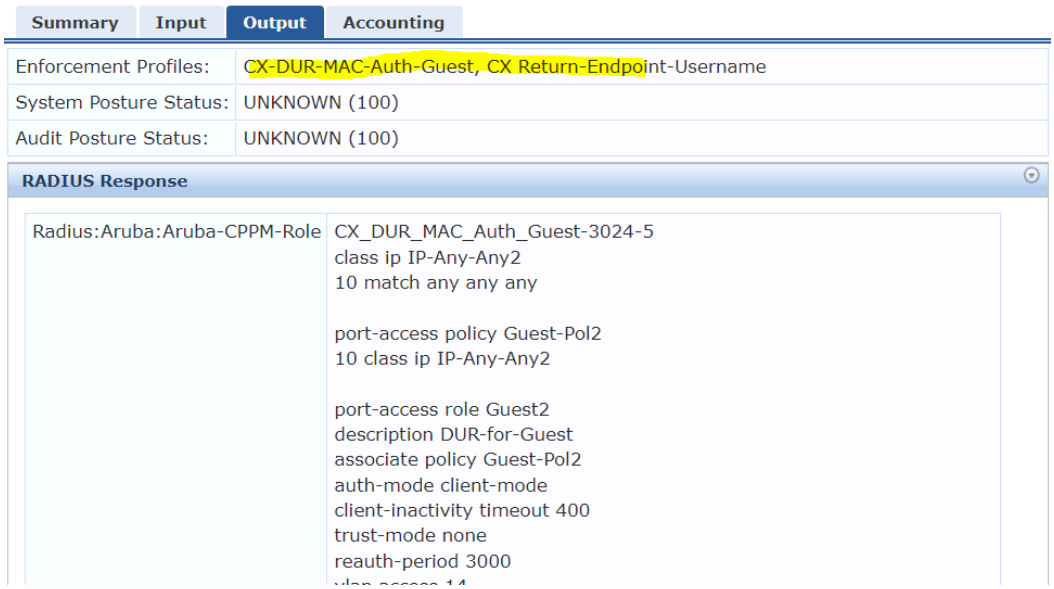
RADIUS Response

Endpoint:Guest Role ID	2
Endpoint:MAC-Auth Expiry	2023-01-12 09:19:09
Endpoint:Username	cpuser
Expire-Time-Update:GuestUser	0
Radius:Aruba:Aruba-Port-Bounce-Host	12
Radius:IETF:Calling-Station-Id	28-D2-44-52-C2-38
Radius:IETF:NAS-Identifier	6200-Lab
Radius:IETF:NAS-Port	1
Radius:IETF:User-Name	28d24452c238
Status-Update:Endpoint	Known

Lastly this will generate the third authentication (Session #1), in which the DUR of Guest user is sent to the switch.

Summary | Input | Output | Accounting

Login Status:	ACCEPT
Session Identifier:	R00000006-01-63bde8b7
Date and Time:	Jan 11, 2023 09:37:43 AEDT
End-Host Identifier:	28-D2-44-52-C2-38 (Computer / Windows / Windows 10)
Username:	cpuser
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 DUR MAC Auth
Authentication Method:	MAC-AUTH
Authentication Source:	Local:localhost
Authorization Source:	[Guest User Repository], [Guest Device Repository], [Endpoints Repository], [Insight Repository], [Time Source]
Roles:	[Guest], [MAC Caching], [User Authenticated]



And this is what we see on the LAN 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 mac-auth        Success
CX_DUR_MAC_Auth_Guest-3024-5

6200-Lab#
```

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

Port Access Client Status Details:

Client 28:d2:44:52:c2:38, cpuser
================================
  Session Details
  ---------------
    Port         : 1/1/1
    Session Time : 358s
    IPv4 Address : 172.16.14.28
    IPv6 Address :
    Device Type  :

  VLAN Details
  ------------
    VLAN Group Name :
    VLANs Assigned  : 14
      Access          : 14
      Native Untagged :
      Allowed Trunk   :

  Authentication Details
  ----------------------
    Status          : mac-auth Authenticated
    Auth Precedence : dot1x - Unauthenticated, mac-auth - Authenticated
```

```
    Auth History     : mac-auth - Authenticated, 346s ago
                       dot1x - Unauthenticated, Supplicant-Timeout, 346s ago

  Authorization Details
  ----------------------
    Role   : CX_DUR_MAC_Auth_Guest-3024-5
    Status : Applied

Role Information:

Name   : CX_DUR_MAC_Auth_Guest-3024-5
Type   : clearpass
Status: Completed
----------------------------------------------
    Reauthentication Period              : 3000 secs
    Cached Reauthentication Period       :
    Authentication Mode                  : client-mode
    Session Timeout                      :
    Client Inactivity Timeout            : 400 secs
    Description                          : DUR-for-Guest
    Gateway Zone                         :
    UBT Gateway Role                     :
    UBT Gateway Clearpass Role           :
    Access VLAN                          : 14
    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                               : Guest-Pol2_CX_DUR_MAC_Auth_Guest-3024-5
    Device Type                          :

Access Policy Details:

Policy Name   : Guest-Pol2_CX_DUR_MAC_Auth_Guest-3024-5
Policy Type   : Downloaded
Policy Status : Applied

SEQUENCE    CLASS                          TYPE ACTION
----------- ------------------------------ ---- ----------------------------------
10          IP-Any-Any2_CX_DUR_MAC_Au... ipv4 permit

Class Details:

class ip IP-Any-Any2_CX_DUR_MAC_Auth_Guest-3024-5
    10 match any any any

6200-Lab#
```

3.6 Testing DUR Guest Captive Portal for AD User

Here as we did with the LUR scenario, we'll use the guest captive portal but this time we'll login with AD credentials. In this case the workflow will be

- The user gets redirected to the guest captive portal
- The user uses AD creds to login

- Webauth service will authenticate the user against AD and updates an Endpoint attribute called “Guest Role ID” and issues a switch port bounce
- There will be a new MAC auth and the service will check for called “Guest Role ID” if it is updated and will let the AD user in without redirecting it to the captive portal.

4.	192.168.1.95	RADIUS	staff1	CX DUR MAC Auth	ACCEPT	CX-DUR-AD-Guest, CX Return-Endpoint-Username
5.	192.168.1.95	WEBAUTH	staff1	CX GuestWebAuth	ACCEPT	CX-AD-MAC-Caching, [AOS-CX - Bounce Switch Port]
6.	192.168.1.95	RADIUS	28d24452c238	CX DUR MAC Auth	ACCEPT	CX-DUR-Guest-CaptivePortal

Session #6 is the initial captive portal redirection

Session #5 is when the user uses the AD credentials (staff1) to login

Session #4 is the subsequent MAC auth

This is Session #5

Summary | Input | Output | Alerts

Login Status:	ACCEPT
Session Identifier:	W00000002-01-63bdec3b
Date and Time:	Jan 11, 2023 09:52:43 AEDT
End-Host Identifier:	28-D2-44-52-C2-38
Username:	staff1
Access Device IP/Port:	-
Access Device Name:	-
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	CX GuestWebAuth
Authentication Method:	Not applicable
Authentication Source:	Lab-AD
Authorization Source:	[Endpoints Repository], [Time Source], Lab-AD
Roles:	[User Authenticated]
Enforcement Profiles:	CX-AD-MAC-Caching, [AOS-CX - Bounce Switch Port]

Summary | Input | **Output** | Alerts

Enforcement Profiles:	CX-AD-MAC-Caching, [AOS-CX - Bounce Switch Port]
System Posture Status:	UNKNOWN (100)

RADIUS Response

Endpoint:Guest Role ID	AD-User
Endpoint:MAC-Auth Expiry	2023-01-12 09:00:00
Endpoint:Username	staff1
Radius:Aruba:Aruba-Port-Bounce-Host	12
Radius:IETF:Calling-Station-Id	28-D2-44-52-C2-38
Radius:IETF:NAS-Identifier	6200-Lab
Radius:IETF:NAS-Port	1
Radius:IETF:User-Name	28d24452c238

And the Session #4

Summary | Input | Output | Accounting

Login Status:	ACCEPT
Session Identifier:	R0000000b-01-63bdeef2
Date and Time:	Jan 11, 2023 10:04:18 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 DUR MAC Auth
Authentication Method:	MAC-AUTH
Authentication Source:	Local:localhost
Authorization Source:	[Guest User Repository], [Guest Device Repository], [Endpoints Repository], [Insight Repository], [Time Source]
Roles:	[MAC Caching], [User Authenticated]

Summary | Input | Output | Accounting

Enforcement Profiles:	CX-DUR-ADGuest, CX Return-Endpoint-Username
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

Radius:Aruba:Aruba-CPPM-Role	CX_DUR_ADGuest-3025-6 class ip IP-Any-Any2 10 match any any any port-access policy ADGuest-Pol2 10 class ip IP-Any-Any2 port-access role ADGuest2 description DUR-for-Guest associate policy ADGuest-Pol2 auth-mode client-mode client-inactivity timeout 400 trust-mode none reauth-period 3000 vlan access 14

And here is the Endpoint db for the laptop that shows the Guest Role ID

Configuration » Identity » Endpoints

Endpoints

This page auto
which it is con

Filter: MAC Ad

#	
1.	
2.	
3.	

Edit Endpoint

Endpoint | Attributes | Device Fingerprints | Policy Cache

	Attribute		Value
1.	Guest Role ID	=	AD-User
2.	MAC-Auth Expiry	=	2023-01-12 09:00:00
3.	Username	=	staff1
4.	*Click to add...*		

3.7 DUR with Instant APs – dot1x

When using DUR for Aruba Instant APs we need to first configure a DUR enforcement profile.

Enforcement Profiles - CX-DUR-InstantAP-1x

Summary | Profile | Attributes

Profile:

Name:	CX-DUR-InstantAP-1x
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-
Product:	AOS-CX

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-CPPM-Role	=	class ip IP-Any-Any2 10 match any any any port-access policy InstantAP-Pol2 10 class ip IP-Any-Any2 port-access role DUR-InstantAP-1x description DUR-for-IAPs associate policy InstantAP-Pol2 auth-mode device-mode poe-priority critical trust-mode dscp vlan trunk native 15 vlan trunk allowed 11-12

Here is the details of the attribute value

```
class ip IP-Any-Any2
    10 match any any any

port-access policy InstantAP-Pol2
    10 class ip IP-Any-Any2

port-access role DUR-InstantAP-1x
    description DUR-for-IAPs
    associate policy InstantAP-Pol2
    auth-mode device-mode
    poe-priority critical
    trust-mode dscp
    vlan trunk native 15
    vlan trunk allowed 11-12
```

Now I'll just update the enforcement policy for our DUR dot1x service.

Services - CX DUR dot1x Wired

Summary | Service | Authentication | Roles | Enforcement

Use Cached Results:	☐ Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:	Wired 802.1X Wired DUR Enforcement Policy Modify — Add New Enforcement Policy

Enforcement Policy Details

Description:	
Default Profile:	CX dot1x Wired Default Profile
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Authorization:Lab-AD:memberOf *CONTAINS* Staff)	CX-DUR-Staff, [Update Endpoint Known]
2.	(Authorization:Lab-AD:memberOf *CONTAINS* Student)	CX-DUR-Student, [Update Endpoint Known]
3.	(Tips:Role *EQUALS* InstantAP)	CX-DUR-InstantAP-1x

3.8 Testing DUR with Instant APs Dot1x

Before we connect the IAP to interface 1/1/1 of the switch, just ensure that you've configured the IAP for dot1x authentication. We covered that in part 2 of the series.

Now checking the ClearPass access tracker

Filter: Request ID contains Go Clear Filter

#	Server	Source	Username	Service	Login Status	Enforcement Profiles
1.	192.168.1.95	RADIUS	InstantAP	CX DUR dot1x Wired	ACCEPT	CX-DUR-InstantAP-1x

Summary Input Output

Login Status:	ACCEPT
Session Identifier:	R00000001-01-63bf6331
Date and Time:	Jan 12, 2023 12:32:33 AEDT
End-Host Identifier:	20-4C-03-23-A7-C0 (Access Points / Aruba / Aruba IAP)
Username:	InstantAP
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 DUR dot1x Wired
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2
Authentication Source:	Local:localhost
Authorization Source:	[Local User Repository]
Roles:	InstantAP, [User Authenticated]
Enforcement Profiles:	CX-DUR-InstantAP-1x

Summary Input Output Accounting

Enforcement Profiles:	CX-DUR-InstantAP-1x
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

Radius:Aruba:Aruba-CPPM-Role	CX_DUR_InstantAP_1x-3029-4 class ip IP-Any-Any2 10 match any any any port-access policy InstantAP-Pol2 10 class ip IP-Any-Any2 port-access role DUR-InstantAP-1x description DUR-for-IAPs associate policy InstantAP-Pol2 auth-mode device-mode poe-priority critical trust-mode dscp vlan trunk native 15 vlan trunk allowed 11-12

From the switch we can see this

```
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
--------------------------------------------------------------------------------
d 1/1/1     20:4c:03:23:a7:c0 dot1x           Success               CX_DUR_InstantAP_1x-
3029-4
```

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

Port Access Client Status Details:
```

```
Client 20:4c:03:23:a7:c0, InstantAP
===================================
  Session Details
  ---------------
    Port         : 1/1/1
    Session Time : 326s
    IPv4 Address :
    IPv6 Address :
    Device Type  :

  VLAN Details
  ------------
    VLAN Group Name :
    VLANs Assigned  : 11-12,15
      Access          :
      Native Untagged : 15
      Allowed Trunk   : 11-12

  Authentication Details
  ----------------------
    Status          : dot1x Authenticated
    Auth Precedence : dot1x - Authenticated, mac-auth - Not attempted
    Auth History    : dot1x - Authenticated, 287s ago
                      mac-auth - Authenticated, 316s ago
                      dot1x - Unauthenticated, Supplicant-Timeout, 316s ago

  Authorization Details
  ----------------------
    Role   : CX_DUR_InstantAP_1x-3029-4
    Status : Applied

Role Information:

Name  : CX_DUR_InstantAP_1x-3029-4
Type  : clearpass
Status: Completed
----------------------------------------------
    Reauthentication Period             :
    Cached Reauthentication Period      :
    Authentication Mode                 : device-mode
    Session Timeout                     :
    Client Inactivity Timeout           :
    Description                         : DUR-for-IAPs
    Gateway Zone                        :
    UBT Gateway Role                    :
    UBT Gateway Clearpass Role          :
    Access VLAN                         :
    Native VLAN                         : 15
    Allowed Trunk VLANs                 : 11-12
    Access VLAN Name                    :
    Native VLAN Name                    :
    Allowed Trunk VLAN Names            :
    VLAN Group Name                     :
    MTU                                 :
    QOS Trust Mode                      : dscp
    STP Administrative Edge Port        :
    PoE Priority                        : critical
    PVLAN Port Type                     :
    Captive Portal Profile              :
    Policy                              : InstantAP-Pol2_CX_DUR_InstantAP_1x-3029-4
    Device Type                         :

Access Policy Details:

Policy Name   : InstantAP-Pol2_CX_DUR_InstantAP_1x-3029-4
```

```
Policy Type   : Downloaded
Policy Status : Applied

SEQUENCE    CLASS                          TYPE ACTION
----------- ------------------------------ ---- ----------------------------------
10          IP-Any-Any2_CX_DUR_Instan... ipv4 permit


Class Details:

class ip IP-Any-Any2_CX_DUR_InstantAP_1x-3029-4
    10 match any any any

6200-Lab#
```

3.9 DUR with Instant APs – Profiling

Following on with the same concepts, we'll now disable supplicant dot1x authentication for IAPs and now ClearPass will profile them and based on the fact that they are Instant APs. The IAPs will be pushed into their user-role. The enforcement profile will be DUR-IAP is as shown below.

Enforcement Profiles - CX-DUR-InstantAP

Summary | Profile | Attributes

Profile:

Name:	CX-DUR-InstantAP
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-
Product:	AOS-CX

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-CPPM-Role	=	class ip IP-Any-Any2 10 match any any any port-access policy InstantAP-Pol2 10 class ip IP-Any-Any2 port-access role DUR-InstantAP description DUR-for-IAPs associate policy InstantAP-Pol2 auth-mode device-mode poe-priority critical trust-mode dscp vlan trunk native 15 vlan trunk allowed 11-12

and this needs to be reference in the MAC auth service policy

Services - CX DUR MAC Auth

Summary | Service | Authentication | Authorization | Roles | Enforcement | Profiler

Use Cached Results:	☐ Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:	Ariya Wired-CX DUR MAC Auth [Modify] Add New Enforcement Policy

Enforcement Policy Details

Description:	
Default Profile:	CX-DUR-Guest-CaptivePortal
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Authorization:[Endpoints Repository]:Conflict *EQUALS* true)	Wired-CX-MAC-Spoof-CP
2.	(Tips:Role *EQUALS* School-Asset)	CX-DUR-CorpDev
3.	(Tips:Role *MATCHES_ALL* [MAC Caching] [Guest] [User Authenticated])	CX-DUR-MAC-Auth-Guest, CX Return-Endpoint-Username
4.	(Tips:Role *EQUALS* [MAC Caching]) *AND* (Endpoint:Guest Role ID *EQUALS* AD-User)	CX-DUR-ADGuest, CX Return-Endpoint-Username
5.	(Authorization:[Endpoints Repository]:Device Name *EQUALS* Aruba IAP)	CX-DUR-InstantAP, [Update Endpoint Known]

So now our ClearPass services are as shown here.

10.	☐	10	CX dot1x Wired	RADIUS	802.1X Wired	⊖
11.	☐	11	CX DUR dot1x Wired	RADIUS	802.1X Wired	✓
12.	☐	12	CX MAC Auth	RADIUS	MAC Authentication	⊖
13.	☐	13	CX DUR MAC Auth	RADIUS	MAC Authentication	✓
14.	☐	14	CX GuestWebAuth	WEBAUTH	Web-based Authentication	✓

Once we have disabled supplicant dot1x on IAP, we need to reboot it.

3.10 Testing DUR with Instant APs – Profiling

As we described it in part 2 of the series, the workflow will be:

- when a new Instant AP connects to the wired network, the switch sends the MAC auth followed by DHCP request (using ip-helper command) to ClearPass.
- ClearPass will allow all the MAC authentication and checks the MAC vendor OUI and puts it in the Captive-portal user role.
- While in this user-role which is quite restrictive, the AP will do a DHCP request which ClearPass can see and then profiles it to be Instant AP along with AP name, etc.
- Now because we have enabled "profile endpoints" for this service, we have added a rule in the profile tab that if there is any change in the initial endpoint classification, use CoA to bounce the switch port.
- Now once ClearPass profiles the Instant AP, it'll update the endpoint category which then bounce the switch port.
- There will be a new MAC auth and this time because Instant AP has been profiles, we can match it with any attribute of the endpoint repository like device name which will be "Aruba IAP"

Ensure that you delete the IAP's entry in the Endpoint database so that ClearPass does the profiling and changes the user role.

Here are the two MAC auth entries we see in access tracker.

#	Server	Source	Username	Service	Login Status	Enforcement Profiles	
1.	192.168.1.95	RADIUS	204c0323a7c0	CX DUR MAC Auth	ACCEPT	[Update Endpoint Known], CX-DUR-InstantAP	1
2.	192.168.1.95	RADIUS	204c0323a7c0	CX DUR MAC Auth	ACCEPT	CX-DUR-Guest-CaptivePortal	1

Session#2 shows the IAP is getting Captive portal user role.

Summary | Input | Output | Accounting | RADIUS CoA | Alerts

Login Status:	ACCEPT
Session Identifier:	R00000004-01-63bf698a
Date and Time:	Jan 12, 2023 12:59:38 AEDT
End-Host Identifier:	20-4C-03-23-A7-C0 (Access Points / Aruba / Aruba IAP)
Username:	204c0323a7c0
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 DUR MAC Auth
Authentication Method:	MAC-AUTH
Authentication Source:	None
Authorization Source:	[Guest User Repository], [Guest Device Repository], [Endpoints Repository], [Insight Repository], [Time Source]
Roles:	[Other], [User Authenticated]

Summary | Input | **Output** | Accounting | RADIUS CoA | Alerts

Enforcement Profiles:	CX-DUR-Guest-CaptivePortal
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

Radius:Aruba:Aruba-CPPM-Role	CX_DUR_Guest_CaptivePortal-3023-11 class ip ClearPass2 10 match tcp any 192.168.1.95 eq 80 20 match tcp any 192.168.1.95 eq 443 class ip DHCP-DNS2 10 match udp any any eq 67 20 match udp any any eq 53 class ip ICMP2 10 match icmp any any class ip Web-Traffic2 10 match tcp any any eq 80 20 match tcp any any eq 443

Summary | Input | Output | Accounting | **RADIUS CoA** | Alerts

CoA Action# 1

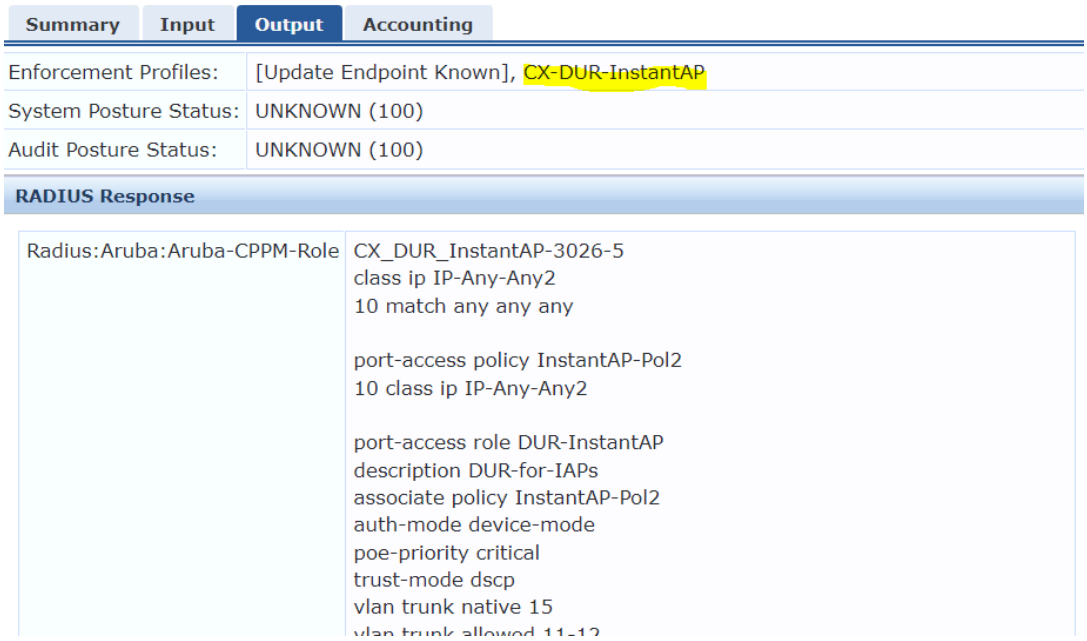
Date and Time	Jan 12, 2023 13:00:19 AEDT
Application Name	Policy Manager
RADIUS CoA Action Type	CoA
RADIUS CoA Action Name	[AOS-CX - Bounce Switch Port]
Status Code	1
Status Message	Radius [AOS-CX - Bounce Switch Port] successful for client 204c0323a7c0.
RADIUS CoA Attributes	Event-Timestamp = 1673488817 User-Name = 204c0323a7c0 Aruba-Port-Bounce-Host = 12 NAS-Identifier = 6200-Lab Calling-Station-Id = 20-4C-03-23-A7-C0 NAS-Port = 1

Then once it is profiled by ClearPass, the switch bounce will happen and the next auth request comes in. This time it will match with the 5th rule in the enforcement policy and gets the CX-DUR-InstantAP enforcement profile.

This is session #1

Summary | Input | Output | Accounting

Login Status:	ACCEPT
Session Identifier:	R00000005-01-63bf69cd
Date and Time:	Jan 12, 2023 13:00:45 AEDT
End-Host Identifier:	20-4C-03-23-A7-C0 (Access Points / Aruba / Aruba IAP)
Username:	204c0323a7c0
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 DUR MAC Auth
Authentication Method:	MAC-AUTH
Authentication Source:	None
Authorization Source:	[Guest User Repository], [Guest Device Repository], [Endpoints Repository], [Insight Repository], [Time Source]
Roles:	[Other], [User Authenticated]



Here we see the switch first showing the captive portal DUR user role and then the InstantAP DUR role

```
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     20:4c:03:23:a7:c0 mac-auth       Success
CX_DUR_Guest_CaptivePortal-3023-11

6200-Lab# sh port-access clients
No port-access clients found.
6200-Lab#
6200-Lab#
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
--------------------------------------------------------------------------------
d 1/1/1     20:4c:03:23:a7:c0 mac-auth       Success              CX_DUR_InstantAP-
3026-5

6200-Lab#
```

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

Port Access Client Status Details:

Client 20:4c:03:23:a7:c0, 204c0323a7c0
======================================
```

```
  Session Details
  ---------------
    Port         : 1/1/1
    Session Time : 563s
    IPv4 Address :
    IPv6 Address :
    Device Type  :

  VLAN Details
  ------------
    VLAN Group Name :
    VLANs Assigned  : 11-12,15
      Access          :
      Native Untagged : 15
      Allowed Trunk   : 11-12

  Authentication Details
  ----------------------
    Status          : mac-auth Authenticated
    Auth Precedence : dot1x - Unauthenticated, mac-auth - Authenticated
    Auth History    : mac-auth - Authenticated, 553s ago
                      dot1x - Unauthenticated, Supplicant-Timeout, 553s ago

  Authorization Details
  ----------------------
    Role   : CX_DUR_InstantAP-3026-5
    Status : Applied

Role Information:

Name  : CX_DUR_InstantAP-3026-5
Type  : clearpass
Status: Completed
----------------------------------------------
    Reauthentication Period             :
    Cached Reauthentication Period      :
    Authentication Mode                 : device-mode
    Session Timeout                     :
    Client Inactivity Timeout           :
    Description                         : DUR-for-IAPs
    Gateway Zone                        :
    UBT Gateway Role                    :
    UBT Gateway Clearpass Role          :
    Access VLAN                         :
    Native VLAN                         : 15
    Allowed Trunk VLANs                 : 11-12
    Access VLAN Name                    :
    Native VLAN Name                    :
    Allowed Trunk VLAN Names            :
    VLAN Group Name                     :
    MTU                                 :
    QOS Trust Mode                      : dscp
    STP Administrative Edge Port        :
    PoE Priority                        : critical
    PVLAN Port Type                     :
    Captive Portal Profile              :
    Policy                              : InstantAP-Pol2_CX_DUR_InstantAP-3026-5
    Device Type                         :

Access Policy Details:

Policy Name   : InstantAP-Pol2_CX_DUR_InstantAP-3026-5
Policy Type   : Downloaded
Policy Status : Applied

SEQUENCE    CLASS                         TYPE ACTION
```

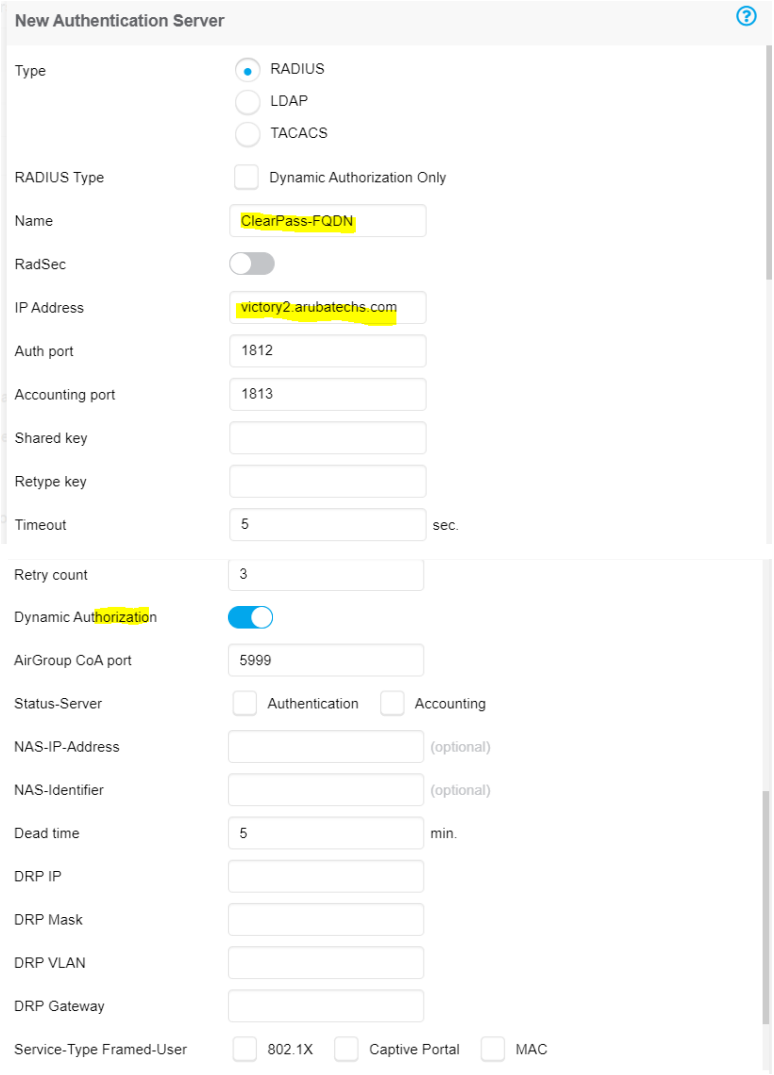
```
----------- ---------------------------- ---- ----------------------------------
10          IP-Any-Any2_CX_DUR_Instan... ipv4 permit

Class Details:

class ip IP-Any-Any2_CX_DUR_InstantAP-3026-5
    10 match any any any

6200-Lab#
```

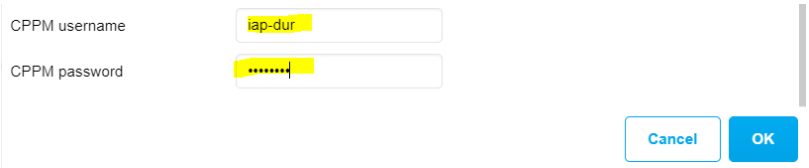
This is to check the interfaces on the CX switch.

```
6200-Lab# sh int brief
-----------------------------------------------------------------------------------------------
Port       Native  Mode   Type          Enabled Status  Reason                 Speed
Description
           VLAN                                                                 (Mb/s)
-----------------------------------------------------------------------------------------------
1/1/1      15      trunk  1GbT          yes     up                             1000     --
1/1/2      15      access 1GbT          yes     down    Waiting for link       --       --
1/1/3      1       access 1GbT          yes     down    Waiting for link       --       --
```

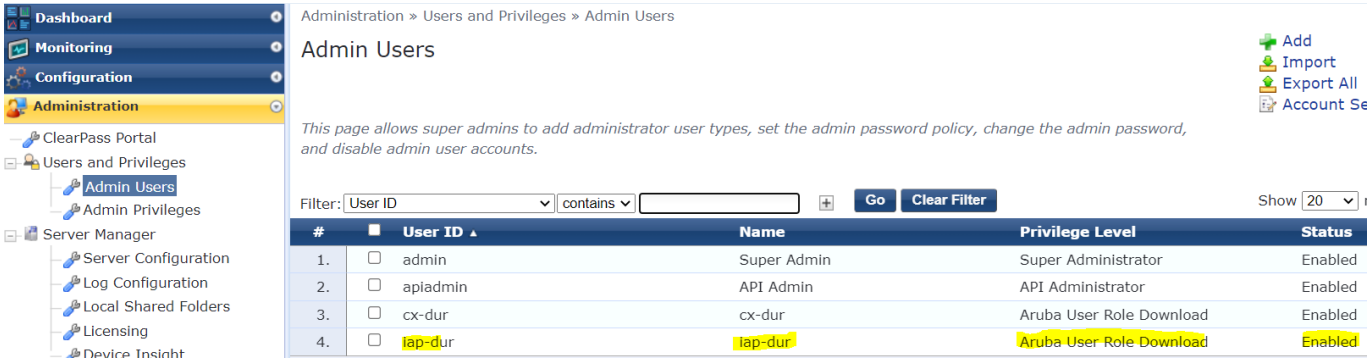
3.11 DUR for Wireless Clients for Instant APs

Like LAN switches, you can use DUR for Aruba Instant APs as well. The same concept apply here too. At first you need to configure the authentication with FQDN instead of the IP address and add the ClearPass username and password.



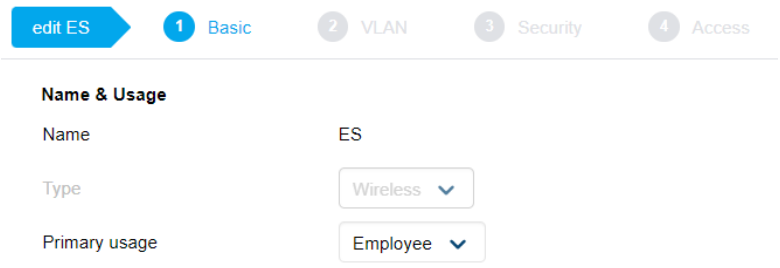


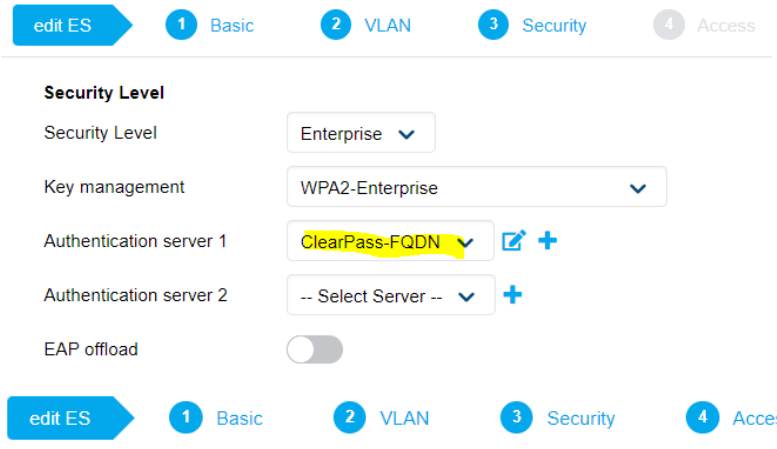
The username/password should match the user credentials configured in ClearPass.

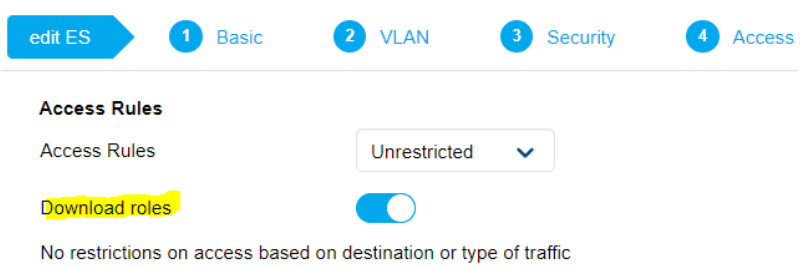


Aruba Instant can also download the root certificate for ClearPass automatically.

Next you need to configure the WLAN that will use the DURs, here we are reconfiguring Test WLAN. Here we are only highlighting the relevant changes you need to make to this WLAN.







At this point we are done with Instant AP configurations. We'll just quickly check to see if the root certificate has been downloaded.

```
20:4c:03:23:a7:a0# sh clearpassca
```

```
Default clearpass CA Certificate:
Version        :2
Serial Number :01
Issuer         :/C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate Services
Subject        :/C=GB/ST=Greater Manchester/L=Salford/O=Comodo CA Limited/CN=AAA Certificate Services
Issued On      :Jan  1 00:00:00 2004 GMT
Expires On     :Dec 31 23:59:59 2028 GMT
RSA Key size   :2048 bits
Signed Using   :RSA-SHA1

20:4c:03:23:a7:a0#
```

Next, we'll configure ClearPass by starting with enforcement profiles

Configuration » Enforcement » Profiles

Enforcement Profiles

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

Filter: Name contains dur s Go Clear Filter

#		Name	Type	Description
1.	☐	school 1xWiFi DUR Staff	RADIUS	
2.	☐	school 1xWiFi DUR Student	RADIUS	

We'll need the following enforcement profiles for our testing

Summary | Profile | Attributes

Profile:

Name:	school 1xWiFi DUR Staff
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:IETF	Session-Timeout	=	28800
2.	Radius:Aruba	Aruba-CPPM-Role	=	wlan access-rule Staff rule any any match any any any permit
3.	Radius:Aruba	Aruba-User-Vlan	=	11

Summary | Profile | Attributes

Profile:

Name:	school 1xWiFi DUR Student
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:IETF	Session-Timeout	=	28800
2.	Radius:Aruba	Aruba-CPPM-Role	=	wlan access-rule Student-DUR rule any any match udp 67 68 permit rule any any match any any any permit
3.	Radius:Aruba	Aruba-User-Vlan	=	12

And here is the service that we'll be using to reference these enforcement profiles

Services - School 802.1X WiFi

Summary | Service | Authentication | Roles | Enforcement

Use Cached Results:	☐ Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:	IAP DUR 802.1X WiFi Enforcement Policy [Modify] Add New Enforcement Policy

Enforcement Policy Details

Description:	
Default Profile:	[Deny Access Profile]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Authorization:Lab-AD:memberOf *CONTAINS* Staff)	school 1xWiFi DUR Staff, [Update Endpoint Known]
2.	(Authorization:Lab-AD:memberOf *CONTAINS* Student)	school 1xWiFi DUR Student, [Update Endpoint Known]

3.12 Testing DUR for Wireless Clients for Instant APs

Now we are ready to connect a user. Here we have staff1 connect to the "ES" SSID.

Filter: Request ID contains [ ] [+] Go Clear Filter Show

#	Server	Source	Username	Service	Login Status	Enforcement Profiles
1.	192.168.1.95	RADIUS	staff1	School 802.1X WiFi	ACCEPT	[Update Endpoint Known], school 1xWiFi DUR Staff

Summary | Input | Output | Accounting

Login Status:	ACCEPT
Session Identifier:	R00000007-01-63bf7428
Date and Time:	Jan 12, 2023 13:44:57 AEDT
End-Host Identifier:	F0-D5-BF-4B-67-11 (Computer / Windows / Windows 10)
Username:	staff1
Access Device IP/Port:	172.16.15.10
Access Device Name:	172.16.15.25
System Posture Status:	UNKNOWN (100)

Policies Used -

Service:	School 802.1X WiFi
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2
Authentication Source:	AD:192.168.1.250
Authorization Source:	Lab-AD
Roles:	[User Authenticated]
Enforcement Profiles:	[Update Endpoint Known], school 1xWiFi DUR Staff

Summary | Input | Output | Accounting

Enforcement Profiles:	[Update Endpoint Known], school 1xWiFi DUR Staff
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

Radius:Aruba:Aruba-CPPM-Role	school_1xWiFi_DUR_Staff-3030-9 wlan access-rule Staff rule any any match any any any permit
Radius:Aruba:Aruba-User-Vlan	11
Radius:IETF:Session-Timeout	28800
Status-Update:Endpoint	Known

Now checking the Instant AP's Web UI

aruba | VIRTUAL CONTROLLER | IAP-LabVC

- Dashboard
  - Overview
  - Networks
  - Access Points
  - Clients
  - Mesh Devices
- Configuration
  - Networks
  - Access Points

Wireless (1) Wired (0)

Name	IP Address	MAC address	OS	ESSID	Access Point	Channel	Type	Role
staff1	172.16.11.23	f0:d5:bf:4b:67:11	Win 10	ES	20:4c:03:23:a7:c0	52+	AN	school_1x...

Overview | AppRF

Info

Name	staff1	IPv6 Address	fe80::eac6:491f:8fa8:1aa5
IP Address	172.16.11.23	MAC address	f0:d5:bf:4b:67:11
OS	Win 10	ESSID	ES
Access Point	20:4c:03:23:a7:c0	Channel	52+
Type	AN	Role	school_1xWiFi_DUR_Staff-3030-9

RF Dashboard

Client	Signal
staff1	
Access Point	**Utilization**
20:4c:03:23:a7:c0	