Contents

1.1 Revision History

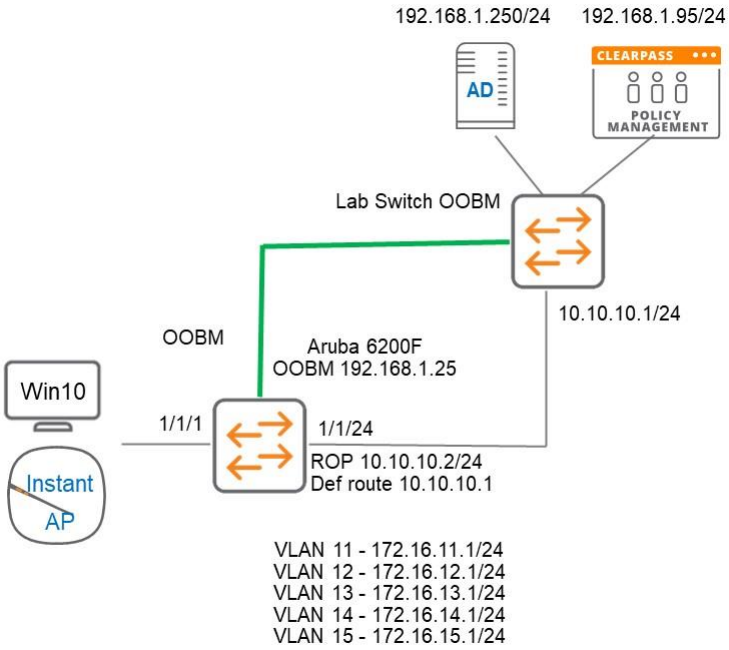
DATE	VERSION	EDITOR	CHANGES
10 Jan 2023	0.1	Ariya Parsamanesh	Initial creation

2 ClearPass Wired Enforcement for CX Switches Part 6

This is the final part of 6x parts series on Aruba CX switch wired enforcement and the main objective of this guide is to build on the first four parts. Here we'll cover downloadable user roles (DUR).

We'll use DUR for

- 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 five parts of this 6x parts series.

3 Downloadable User Roles for IAPs

3.1 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

3.2 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] S

#	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#
```

3.3 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.

3.4 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
2.	192.168.1.95	RADIUS	204c0323a7c0	CX DUR MAC Auth	ACCEPT	CX-DUR-Guest-CaptivePortal

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]

Summary | Input | Output | Accounting

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

RADIUS Response

Radius:Aruba:Aruba-CPPM-Role	CX_DUR_InstantAP-3026-5 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

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
```

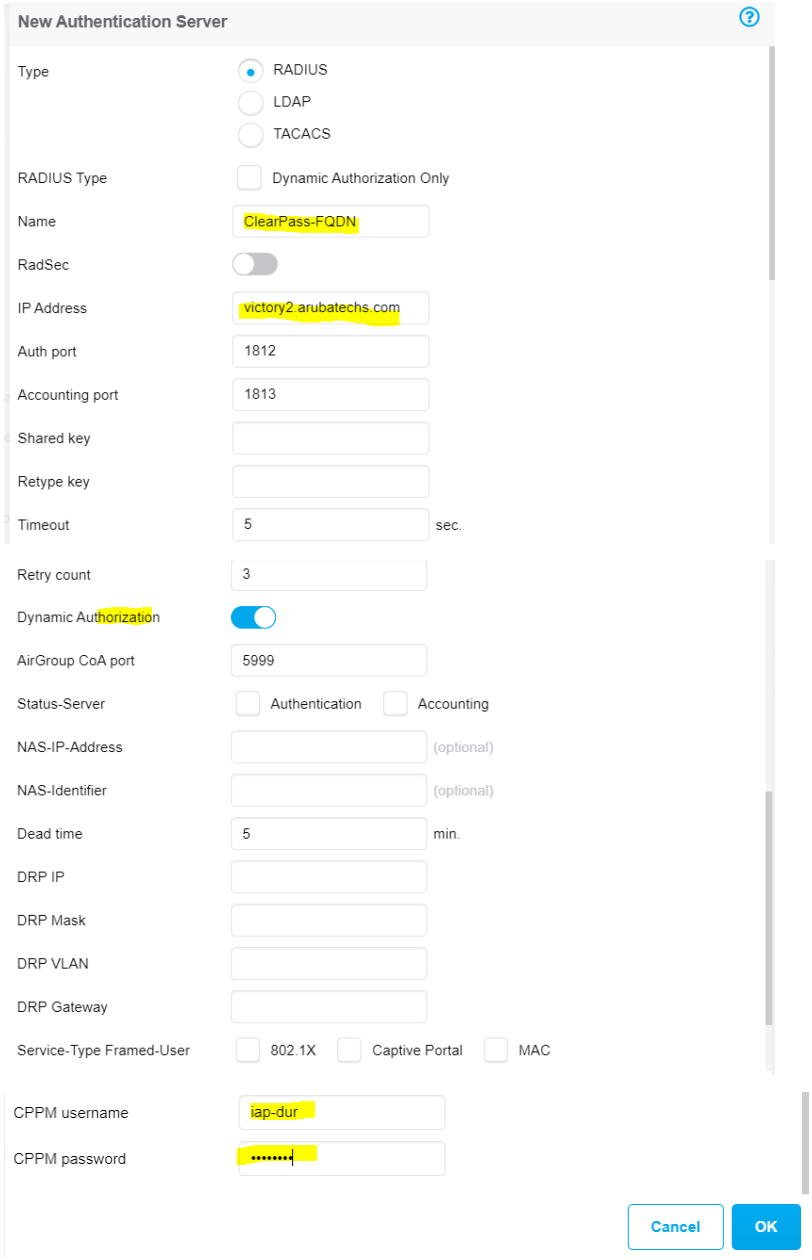
```
  Authorization Details
  ---------------------
    Role   : CX_DUR_InstantAP-3026-5
    Status : Applied

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.

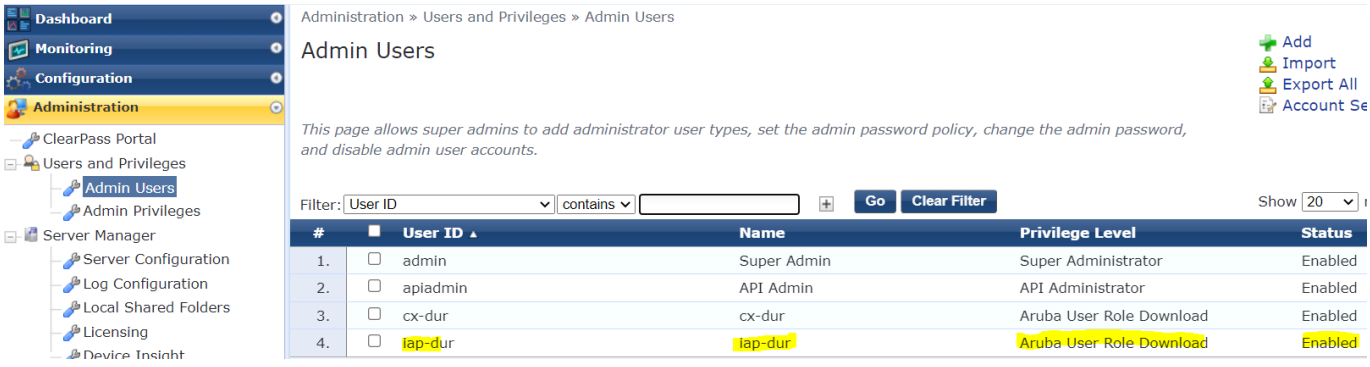
```
6200-Lab# sh int brief
-------------------------------------------------------------------------------------------
Port      Native  Mode   Type          Enabled Status  Reason                Speed
Description
          VLAN                                                               (Mb/s)
-------------------------------------------------------------------------------------------
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      --      --
```

3.5 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.

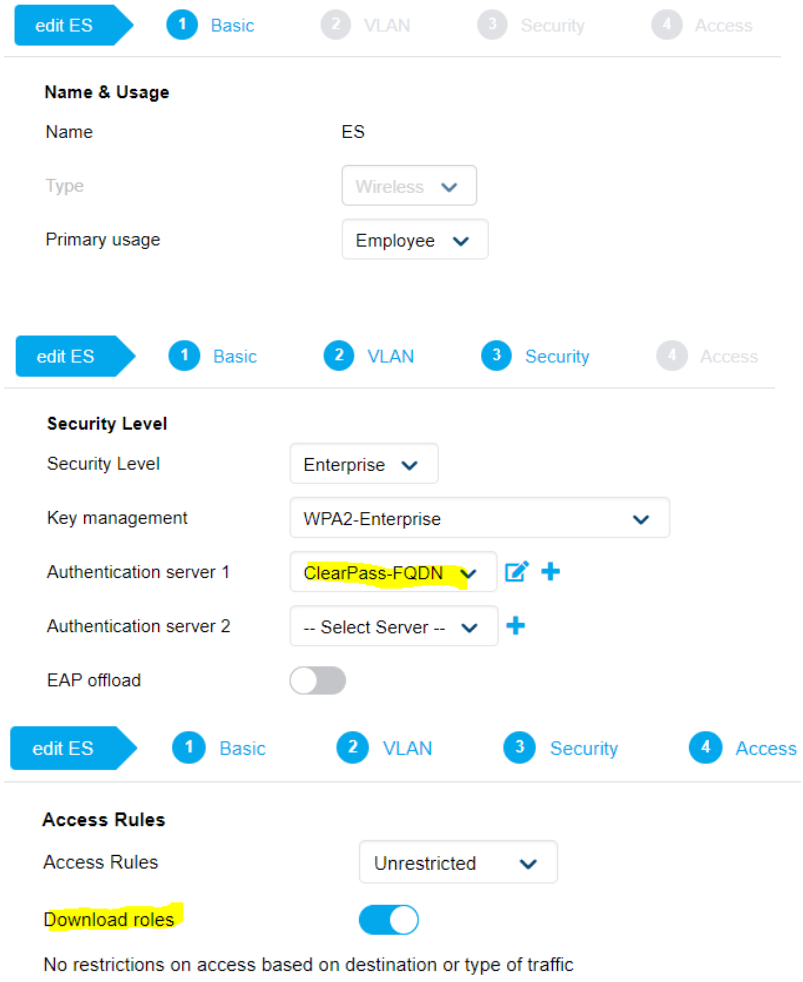


The username/password should match the user credentials configured in ClearPass.



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

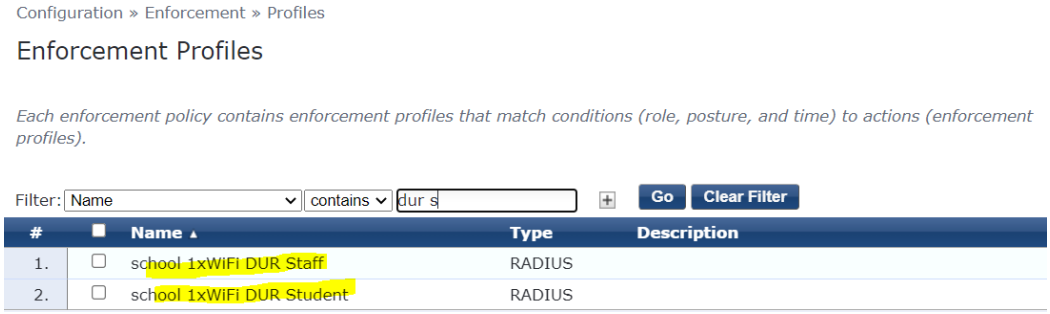
Next you need to configure the WLAN that will use the DURs, here we are reconfiguring Test WLAN. Here we are only highlighting the relevant changes you need to make to this WLAN.



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



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]

3.6 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