# Contents

	1.1	Revision History	1
2	Clea	rPass Wired Enforcement for CX Switches Part 4	2
	2.1	Things you need	2
3	Dow	nloadable User Roles	3
	3.1	Root Certificate Configuration	3
	3.2	ClearPass Service Configuration	6
	3.3	DUR Dot1x Testing	8
	3.4	DUR with Captive Portal	11
	3.5	Testing DUR Guest Captive Portal with MAC Caching	14
	3.6	Testing DUR Guest Captive Portal for AD User	20
	3.7	DUR with Instant APs – dot1x	22
	3.8	Testing DUR with Instant APs Dot1x	23
	3.9	DUR with Instant APs – Profiling	26
	3.10	Testing DUR with Instant APs – Profiling	27
	3.11	DUR for Wireless Clients for Instant APs	31
	3.12	Testing DUR for Wireless Clients for Instant APs	34

# **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.

Administration » Users and Privileges » Admin Users	
Admin Users	<ul> <li>♣ Add</li> <li>▲ Import</li> <li>▲ Export A</li> <li>➡ Account</li> </ul>
This page allows super admins to add administrator user types, set the admin password policy, change the admin password, and disable admin user accounts.	

Filter:	User ID	<ul> <li>✓ contains </li> </ul>	+ Go Clear Filter		Show 20
#		User ID 🔺	Name	Privilege Level	Status
1.		admin	Super Admin	Super Administrator	Enabled
2.		apiadmin	API Admin	API Administrator	Enabled
3.		<mark>cx-dur</mark>	cx-dur	Aruba User Role Download	Enabled

#### Here is the corresponding switch command

```
radius-server host victory2.arubatechs.com key plaintext sdsda clearpass-username <mark>cx-</mark>
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.



Service & Client Certificates

Select Server: victory2 (	192.168.1.95)
Subject:	CN=*.arubatechs.com
Issued by:	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB
Issue Date:	Jun 30, 2022 10:00:00 AEST
Expiry Date:	Jul 31, 2023 09:59:59 AEST
Validity Status:	Valid
Details:	View Details
Intermediate CA Certifi	cate:
Subject:	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB
Issued by:	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US
Issue Date:	Nov 02, 2018 11:00:00 AEDT
Expiry Date:	Jan 01, 2031 10:59:59 AEDT
Validity Status:	Valid
Details:	View Details

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.

Dashboard O Administration » Certificates » Trust List								
🖾 Monitoring 🔹 💿	Monitoring • Certificate Trust List					🛉 Add		
😤 Configuration 🔹 💿	This p	This page displays a list of trusted Certificate Authorities (CA). You can add, view, or delete a certificate.						
🔐 Administration 📀								
— 🎤 ClearPass Portal	Filter:	Subject	t 🗸 🗸 contains 🗸 USERTrust RSA Cer 🕢 🛨 🛛 Go 🛛 Clear Filter		Show 20	✓ records		
Users and Privileges	#		Subject 🔺	Usage	Validity	Enabled		
- 🌽 Admin Users 🌽 Admin Privileges	1.		CN=USERTrust RSA Certification Authority,O=The USERTRUST Network,L=Jersey City,ST=New Jersey,C=US	Others	Valid	Disabled		
Gerver Manager     External Servers	2.		CN=USERTrust RSA Certification Authority,O=The USERTRUST Network,L=Jersey City,ST=New Jersey,C=US	Others	Valid	Enabled		
- PExternal Accounts	Showi	ng 1-2	of 2			Delete		
🖃 🖶 Certificates								
- 🌽 Certificate Store								
– 🧀 Trust List								
Revocation Lists								

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
AlUEBhMCQkUxGTAXBgNVBAoTEEdsb2JhbFNpZ24gbnYtc2ExEDAOBgNVBAsTB1Jv
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)# MIIFgTCCBGmgAwIBAgIQOXJEOvkit1HX02wQ3TE11TANBgkqhkiG9w0BAQwFADB7
6200-Lab(config-ta-cert) # Removed a lot of lines here
6200-Lab(config-ta-cert)# MQswCQYDVQQGEwJHQjEbMBkGA1UECAwSR3J1YXRlciBNYW5jaGVzdGVyMRAwDgYD
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 USERTrust TA Profile Name : USERTrust TA Profile Name : USERTrus Revocation Check : disabled OCSP Primary URL: Not Configured OCSP Secondary URL: Not Configured OCSP Enforcement-level: strict OCSP Disable Nonce: false : mgmt OCSP VRF 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

Administration » Cer	ficates » Trust List						
Certificate Tru	View Certificate Details	•					
This page displays a Filter: Subject # Subj	Subject DN:	CN=USERTrust RSA Certification Authority,O=The USERTRUST Network,L=Jersey City,ST=New Jersey,C=US					
1.     CN=U Jerse       2.     CN=U Derse       Showing 1-2 of 2	Issuer DN:	CN=AAA Certificate Services,O=Comodo CA Limited,L=Salford,ST=Greater Manchester,C=GB					
	Issue Date/Time:	Mar 12, 2019 11:00:00 AEDT					
	Expiry Date/Time:	Jan 01, 2029 10:59:59 AEDT					
	Validity Status:	Valid					
	Signature Algorithm:	SHA384WithRSAEncryption					
	Public Key Format:	X.509					
	Serial Number:	76359301477803385872276235234032301461					
	Enabled:	true					
	Usage:	Others       Remove      Select to Add					
		Update Disable Export Close					

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.

Profile Attributes	Summary		
Template:	Aruba Downloadable Role Enforcement 🗸		
Name:	CX DUR-Staff		
Description:			
Туре:	RADIUS		
Action:	● Accept ○ Reject ○ Drop		
Device Group List:	Remove		
	View Details		
	Modify		
	Select V		
Role Configuration Mode:	O Standard O Advanced		
Product:	AOS-CX		

#### Here we are using the advance mode.



#### **Enforcement Profiles**

Profile		Attributes	Summary		
	Туре			Name	Value
1.	Radius	:Aruba		Aruba-CPPM-Role	<pre>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</pre>

```
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.

Sı	ummary Profile A	ttributes		
Pro	file:			
Nan	ie:	CX-DUR-Student		
Des	cription:			
тур	9:	RADIUS		
Acti	on:	Accept		
Dev	ice Group List:	-		
Proc	luct:	AOS-CX		
Attr	ibutes:			
	Туре	Name		Value
				class ip IP-Any-Any2 10 match any any any
				port-access policy Student-Pol2 10 class ip IP-Any-Any2
1.	Radius:Aruba	Aruba-CPPM-Role	=	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
clā	ass ip IP-An 10 match a	y-Any2 ny any any		
poi	rt-access po 10 class i	licy Student-Pol2 o IP-Any-Any2		
poi	rt-access ro descriptio associate auth-mode	le Student2 n DUR-for-Student policy Student-Pol2 client-mode		



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



Filter:	Name		✓ contains ✓ wir	+	Go Clear Filter		Show 20 🗸 records
#		Order 🛦	Name		Туре	Template	Status
1.		10	CX dot1x Wired		RADIUS	802.1X Wired	0
2.		11	CX DUR dot1x Wired		RADIUS	802.1X Wired	

#### Services - CX DUR dot1x Wired

Summary Servi	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  $\bigcirc$  ANY or  $\odot$  ALL of the following conditions:

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

#### Summary Service Authentication Roles Enforcement

		_			
Authenticatio	n Methods:	[EAP PEAP] [EAP TLS] [EAP MSCHAPv	2]	Move Up ↑ Move Down ↓ Remove View Details Modify	
Authenticatio	n Sources:	[Local User Rep Lab-AD [Active [	ository] [Local SQL DB] )irectory]	Move Up ↑	]
Summary	Service	Authentication	Roles Enforcemen	t	
Use Cached R	esults:	Use cached	Roles and Posture attrib	utes from previous s	sessions
Enforcement I	Policy:	Wired 802.1X W	/ired DUR Enforcement Po	licy 🗸 Modify	
				Enforcement I	Policy Details
Description:					
Default Profile	e:	CX dot1x Wire	ed Default Profile		
Rules Evaluat	ion Algorith	m: first-applicable	e		
Conditi	ions				Enforcement Profiles
1. (Autho	orization:La	b-AD:memberOf	CONTAINS Staff)		CX-DUR-Staff, [Update Endpoint Known]
2. (Autho	orization:La	b-AD:memberOf (	CONTAINS Student)		CX-DUR-Student, [Update Endpoint Known
3. (Tips:F	Role EQUAL	S 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.



🜪 Add

🛓 Import 🛓 Export All

Filter:	Request ID		✓ contains ✓		+	Go	Clear Filter		
#	Server	Source	Username	Service				Login Status	Enforcement Profiles
1.	192.168.1.95	RADIUS	staff2	CX DUR dot1	x Wire	d		ACCEPT	[Update Endpoint Known], CX-DUR- Staff

Summary	Input	Output	Accounting			
Login Status:		ACCER	т			
Session Identi	fier:	R0000	0041-01-63bc	fe41		
Date and Time	e:	Jan 10	), 2023 16:57:	22 AEDT		
End-Host Iden	tifier:	28-D2	2-44-52-C2-38 (Computer / Windows / Windows 10)			
Username:		staff2				
Access Device IP/Port: 192.			68.1.25:1 (CX-	SW1 / Aruba)		
Access Device Name: 6200			Lab			
System Posture Status: UNK			OWN (100)			
				Policies Used -		
Service:		CX DU	IR dot1x Wired			
Authentication Method: EAP		EAP-P	EAP,EAP-MSCH	APv2		
Authentication Source: AD			2.168.1.250			
Authorization Source: Lab			D			
Roles: [U		[User	ser Authenticated]			
Enforcement Profiles: [U			te Endpoint Kn	own], <mark>CX-DUR-Staff</mark>		
Summary	Input	Output	Accounting			
Enforcement P	Profiles:	[Update	Endpoint Know	n], CX-DUR-Staff		
System Postur	re Status:	UNKNOW	N (100)			
Audit Posture	Status:	UNKNOW	N (100)			
RADIUS Resp	onse	1		(		
Radius:Aruba:Aruba-CPPM-Role		CX_DUR_Staf class ip IP-An 10 match any port-access p 10 class ip IP port-access ro description Dr associate poli auth-mode cli client-inactivit trust-mode nor reauth-period	if-3020-5 y-Any2 y any any olicy Staff-Pol2 -Any-Any2 ole Staff2 UR-for-Staff cy Staff-Pol2 lent-mode ty timeout 400 one 2000			

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

c 1/1/1	28:d2:44:52:c2:38	dotlx	Success	CX_DUR_Staff=3020=5			
	-	Method					
Port Device Type	MAC-Address	Onboarding	Status	Role			
Status Code	Status Codes: d device-mode, c client-mode, m multi-domain						
Port Access Clients							
6200-Lab# sh port-access clients							

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: 11Access: 11
     Native Untagged :
     Allowed Trunk :
 Authentication Details
  _____
   Status : dotlx 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
                                    : Staff-Pol2 CX DUR Staff-3020-5
   Policy
   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

Summ	nary Profile	Attributes		
Profile:	:			
Name:		CX-DUR-G	Guest-CaptivePortal	
Descript	tion:			
Type:		RADIUS		
Action:		Accept		
Device	Group List:	-		
Product	t:	AOS-CX		
Attributes:				
Т	уре		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. R	ladius:Aruba		Aruba-CPPM-Role	<ul> <li>port-access policy cp_policy2</li> <li>10 class ip DHCP-DNS2</li> <li>20 class ip ICMP2</li> <li>30 class ip ClearPass2</li> <li>40 class ip Web-Traffic2 action redirect captive-portal</li> <li>aaa authentication port-access captive-portal-profile dur_user</li> <li>url https://victory2.arubatechs.com/guest/wired_school.php</li> <li>port-access role Captive-Portal2</li> <li>description DUR-for-PreAuth</li> <li>associate captive-portal-profile dur_user</li> <li>associate captive-portal-profile dur_user</li></ul>

#### 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-M
Description:		
Type:		RADIUS
Action:		Accept
Device Group L	.ist:	-
Product:		AOS-CX
Attributes:		

	Туре	Name	Value
1.	Radius:Aruba	Aruba-CPPM-Role =	value         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

Su	mmary Profile	Attributes					
Prof	Profile:						
Nam	e:	CX-DUR-AD-Guest					
Desc	ription:						
Туре	:	RADIUS					
Actio	on:	Accept					
Devi	ce Group List:	-					
Prod	uct:	AOS-CX					
Attri	butes:						
	Туре	Name	Value				
1.	Radius:Aruba	Aruba-CPPM-Role	<ul> <li>class ip IP-Any-Any2</li> <li>10 match any any any</li> <li>port-access policy AD-Guest-Pol2</li> <li>10 class ip IP-Any-Any</li> <li>port-access role AD-Guest2</li> <li>description DUR-for-AD-Guest</li> <li>associate policy AD-Guest-Pol2</li> <li>auth-mode client-mode</li> <li>client-inactivity timeout 400</li> <li>trust-mode none</li> <li>reauth-period 3000</li> <li>vlan access 14</li> </ul>				

### 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	0	
11.	□ 11	CX DUR dot1x Wired	RADIUS	802.1X Wired		
12.	□ 12	CX MAC Auth	RADIUS	MAC Authentication	0	
13.	13	CX DUR MAC Auth	RADIUS	MAC Authentication		
14.	□ 14	CX GuestWebAuth	WEBAUTH	Web-based Authentication	<b>S</b>	
Showing 1-14 of 14 Copy Export Delete						

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

Theres	Haddies of Air of the following conditions.									
	Туре	Name	Operator	Value						
1.	Radius:IETF	NAS-Port-Type	BELONGS_TO	Ethernet (15), Wireless-802.11 (19)		Ť				
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Call-Check (10)		Ť				
3.	Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}		Ť				

Summary	Service	Authentication	Authorization	Roles	Enforcement	Profiler	
Authentication	n Methods:	[Allow All MAC #	UTH]		Move Up↑ Move Down↓ Remove View Details	] ] ]	Add New Authentication Method
Authentication	n Sources:	Select to Add-	sitory] [Local SQL D	<b>v</b>	Move Up ↑	]	Add New Authentication Source



Summary	Service	Authentication	Authorization	Roles	Enforcement	Profiler		
Authorization	Details:	Authorization	sources from which	h role ma	pping attributes	are fetched	(for each Authentication Source)	
		Authen	tication Source				Attributes Fetched From	
		1. [Endpoir	nts Repository] [Lo	cal SQL [	DB]		[Endpoints Repository] [Local SQL DB]	
		Additional auth	horization sources	from whi	ch to fetch role-n	napping attr	ibutes -	Add New Authentication Source
		[Insight Reposite [Time Source] [L	oryj [Local SQL DB] Local SQL DB]		Remove			Add New Authentication Source
		[Guest User Re	pository] [Local SQL I	DB]	View Details			
		[Guest Device F	Repositoryj [Local SQ	LDBJ	Modify			
Summary	Service	Authentication	Authorization	Roles	Enforcement	Profiler		
Role Mapping	Policy:	Wired-CX MAC	auth-role-mapping	~	Modify			Add New Role Mapping Policy
					Role Mappin	g Policy De	tails	
Description:								
Default Role:		[Other]						
Rules Evaluat	tion Algorithn	n: evaluate-all						
Condit	ions						Role	
1. (Author	rization:[End	points Repository	/]:Unique-Device-C	Count EX	ISTS )		[MAC Caching]	
2. (Endpo	int:Guest Rol	In FOUALS 1	%{Enupoint:MA	C-Auth E	xpiry})		[Contractor]	
3. (Endpo	int:Guest Rol	e ID EOUALS 2	)				[Guest]	
4. (Endpo	int:Guest Rol	e ID EQUALS 3	)				[Employee]	
5. (Author	rization:[End	points Repository	/]:Status EQUALS	known)			School-Asset	
	(Endpoint.Se	.nooi_secure_dec		/				
Summary	Service	Authentication	Authorization	Roles	Enforcement	Profiler		
Use Cached F	Results:	□ Use cached	Roles and Posture	attribute	s from previous s	essions		
Enforcement	Policy:	Ariya Wired-CX	DUR MAC Auth		✓ Modify			Add New Enforcement Policy
					Enforcemer	t Policy De	ails	
Description:								
Default Profil	e:	CX-DUR-Gues	st-CaptivePortal					
Rules Evaluat	tion Algorithn	n: first-applicabl	le					
Condit	ions						Enforcement Profiles	
1. (Auth	orization:[En	dpoints Reposito	ry]:Conflict EOUA	LS true)			Wired-CX-MAC-Spoof-CP	
2. (Tips:	Role EOUAL	S School-Asset)		,			CX-DUR-CorpDev	
· · ·			a china l					
(Tips:	Role MATCH	ES_ALL [MAC CO	aching]					
(Tips: 3. [Guest]	Role MATCH	1)	achingj				CX-DUR-MAC-Auth-Guest, CX Return-Endpoi	int-Username
(Tips: 3. [Guest] [User A (Tips:	Role <i>MATCH</i>                   	]) S [MAC Caching]	])				CX-DUR-MAC-Auth-Guest, CX Return-Endpoint	int-Username
(Tips: 3. [Guest] [User A 4. (Tips: AND	Role <i>MATCH</i> withenticated Role <i>EQUAL</i> (Endpoint:0	]) S [MAC Caching] Guest Role ID EC	]) QUALS AD-User)				CX-DUR-MAC-Auth-Guest, CX Return-Endpoi	int-Username rname
(Tips: 3. [Guest] [User A 4. (Tips: AND Summary	Role MATCH authenticated Role EQUALS (Endpoint: Service	]) S [MAC Caching] Guest Role ID EC Authentication	]) 2 <i>UALS</i> AD-User) Authorization	Roles	Enforcement	Profiler	CX-DUR-MAC-Auth-Guest, CX Return-Endpoint-Use	int-Username rname
(Tips: 3. [Guest] [User A 4. (Tips: AND Summary Endpoint Class	Role MATCH uthenticated Role EQUALS (Endpoint: Service ssification:	]) S [MAC Caching] Guest Role ID EC Authentication Select the class	]) QUALS AD-User) Authorization ssification(s) after	Roles which an	Enforcement action must be t	Profiler riggered -	CX-DUR-MAC-Auth-Guest, CX Return-Endpoint-Use	int-Username mame
(Tips: 3. [Guest] [User A 4. (Tips: AND Summary Endpoint Class	Role MATCH uthenticated Role EQUALS (Endpoint:0 Service ssification:	]) S [MAC Caching] Guest Role ID EC Authentication Select the class Any Category /	)) QUALS AD-User) Authorization ssification(s) after OS Family / Name	Roles which an	Enforcement action must be t	Profiler	CX-DUR-MAC-Auth-Guest, CX Return-Endpoin CX-DUR-AD-Guest, CX Return-Endpoint-Use	int-Username rname
(Tips: 3. [Guest] [User A 4. (Tips: AND Summary Endpoint Class	Role MATCH uthenticated Role EQUALS (Endpoint:C Service ssification:	]) S [MAC Caching] Guest Role ID EC Authentication Select the class Any Category /	) QUALS AD-User) Authorization ssification(s) after OS Family / Name	Roles which an	Enforcement action must be t Remove	Profiler riggered -	CX-DUR-MAC-Auth-Guest, CX Return-Endpoint-Use	int-Username rname
(Tips: 3. [Guest] [User A 4. (Tips: AND Summary Endpoint Class	Role MATCH authenticated Role EQUALS (Endpoint: Service ssification:	]) S [MAC Caching: Guest Role ID EC Authentication Select the clas Any Category /	)) QUALS AD-User) Authorization ssification(s) after OS Family / Name	Roles which an	Enforcement action must be t Remove	Profiler riggered -	CX-DUR-MAC-Auth-Guest, CX Return-Endpoint-Use	int-Username
(Tips: 3. [Guest] [User A 4. (Tips: AND Summary Endpoint Class	Role MATCH uthenticated Role EQUAL: (Endpoint: Service ssification:	S [MAC Caching: Guest Role ID EC     Authentication     Select the clas     Any Category /	)) QUALS AD-User) Authorization ssification(s) after OS Family / Name	Roles which an	Enforcement action must be t Remove	Profiler riggered -	CX-DUR-MAC-Auth-Guest, CX Return-Endpoint-Use	int-Username

# 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:		ACCE	PT				
Session Ident	tifier:	R000	00005-01-63bd	e7dc			
Date and Tim	ne:	Jan 1	1, 2023 09:34:	04 AEDT			
End-Host Ide	ntifier:	28-D	2-44-52-C2-38	(Computer / Windows / W	/indows 10)		
Username: Access Device IP/Port: Access Device Name:		28d2	28d24452c238				
		192.3	168.1.25:1 (CX-	SW1 / Aruba)			
Access Device	e Name:	6200	-Lab				
System Postu	ire Status	: UNKI	NOWN (100)				
				Policies Used -			
Service:		CX D	UR MAC Auth				
Authenticatio	n Method	MAC	AUTH				
Authenticatio	n Source:	Local	:localhost				
Authorization	Source:	[Gue [Insig	st User Reposito ght Repository],	ory], [Guest Device Reposite [Time Source]	ory], [Endpoints Repository],		
Roles:		[Othe	er], [User Authe	nticated]			
Cummany	Toput	Quitout	Accounting				
Summary	Input	ουτρατ	Accounting				
Enforcement I	Profiles:	CX-DUR-	Guest-CaptiveP	ortal			
System Postu	re Status:	UNKNOW	/N (100)				
Audit Posture	Status:	UNKNOW	/N (100)			0	
RADIUS Resp	oonse					()	
RADIUS Response		CPPM-Role	CX_DUR_Gues class ip ClearP 10 match tcp a 20 match tcp a class ip DHCP- 10 match udp 20 match udp class ip ICMP2 10 match icmp class ip Web-T 10 match tcp a 20 match tcp a	t_CaptivePortal-3023-11 ass2 any 192.168.1.95 eq 80 any 192.168.1.95 eq 443 DNS2 any any eq 67 any any eq 53 o any any raffic2 any any eq 80 per en es 442			
6200. Tob	# ch	ort o		onta			
	# SII [	Jore-a	cess cll	enus			
Port Acc	ess Cl	lients					
Status Co	odes:	d dev:	ice-mode,	c client-mode,	m multi-domain		
Port	 MA(		 288	Onboarding	Status		

ole 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 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 \_\_\_\_\_ : 3000 secs Reauthentication Period Cached Reauthentication Period Authentication Mode : : client-mode Session Timeout : : 400 secs Client Inactivity Timeout : DUR-for-PreAuth Description Gateway Zone UBT Gateway Role UBT Gateway Clearpass Role : : 13 Access VLAN Native VLAN : Allowed Trunk VLANs Access VLAN Name Native VLAN Name : Allowed Trunk VLAN Names VLAN Group Name MTU QOS Trust Mode STP Administrative Edge Port : PoE Priority PVLAN Port Type : dur\_user\_CX\_DUR\_Guest\_CaptivePortal-3023-9 Captive Portal Profile 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 Poli	cy Details:
Policy Name	: cp_policy2_CX_DUR_Guest_CaptivePortal-3023-9
Policy Type	: <mark>Downloaded</mark>
Policy State	us : 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 Detai	ls:
class ip DH	CP-DNS2_CX_DUR_Guest_CaptivePortal-3023-9
10 matcl	h udp any any eq dhcp-server
20 matcl	h udp any any eq dns
class ip ICI	MP2_CX_DUR_Guest_CaptivePortal-3023-9
10 matcl	h icmp any any
class ip Cle	earPass2_CX_DUR_Guest_CaptivePortal-3023-9
10 matcl	h tcp any 192.168.1.95 eq http
20 matcl	h tcp any 192.168.1.95 eq https
class ip We	b-Traffic2_CX_DUR_Guest_CaptivePortal-3023-9
10 matcl	h tcp any any eq http
20 matcl	h 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

: 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	l 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:	W0000000	-01-63bde893		
Date and Time:	Jan 11, 202	3 09:37:08 AEDT		
End-Host Identifier:	28-D2-44-5	2-C2-38		
Username:	<mark>cpuser</mark>			
Access Device IP/Port:	-			
Access Device Name:	-			
System Posture Status	UNKNOWN	(100)		
		Policies Used -		
Service:	CX GuestWe	ebAuth		
Authentication Method:	Not applical	ble		
Authentication Source: [Guest User		Repository]		
Authorization Source: [Guest User		Repository], [Endpoints Repository], [Time Source]		
Roles: [Guest], [Us		ser Authenticated]		
Enforcement Profiles:	CX-GuestM/	AC-Caching, CX MAC Caching Expire Post Login, [Update Endpoint		
Summary Input	Output			
Summary Input Enforcement Profiles:	Output CX-GuestMAC-C [AOS-CX - Bour	aching, CX MAC Caching Expire Post Login, [Update Endpoint Known], ice Switch Port]		
SummaryInputEnforcementProfiles:SystemPostureStatus:	Output CX-GuestMAC-C [AOS-CX - Bour UNKNOWN (100	aching, CX MAC Caching Expire Post Login, [Update Endpoint Known], ice Switch Port] ))		
SummaryInputEnforcement Profiles:System Posture Status:RADIUS Response	Output CX-GuestMAC-C [AOS-CX - Bour UNKNOWN (100	aching, CX MAC Caching Expire Post Login, [Update Endpoint Known], ace Switch Port] ) )		
SummaryInputEnforcement Profiles:System Posture Status:RADIUS ResponseEndpoint:Guest Role I	Output CX-GuestMAC-C [AOS-CX - Bour UNKNOWN (100	aching, CX MAC Caching Expire Post Login, [Update Endpoint Known], ace Switch Port] D) 2		
Summary     Input       Enforcement Profiles:       System Posture Status:       RADIUS Response       Endpoint:Guest Role I       Endpoint:MAC-Auth E>	Output CX-GuestMAC-C [AOS-CX - Bour UNKNOWN (100 D cpiry	aching, CX MAC Caching Expire Post Login, [Update Endpoint Known], ice Switch Port]		
Summary     Input       Enforcement     Profiles:       System     Posture       Status:     RADIUS Response       Endpoint:Guest     Role I       Endpoint:MAC-Auth Exployed     Endpoint:Username	Output CX-GuestMAC-C [AOS-CX - Bour UNKNOWN (100 D cpiry	aching, CX MAC Caching Expire Post Login, [Update Endpoint Known], ace Switch Port] a) 2 2 2023-01-12 09:19:09 cpuser		
SummaryInputEnforcementProfiles:SystemPostureStatus:Status:RADIUSResponseEndpoint:GuestRole IEndpoint:MAC-AuthExplore-Time-Update:GExplore-Time-Update:G	Output CX-GuestMAC-C [AOS-CX - Bour UNKNOWN (100 D cpiry uestUser	aching, CX MAC Caching Expire Post Login, [Update Endpoint Known], ace Switch Port]		
Summary     Input       Enforcement Profiles:       System Posture Status:       RADIUS Response       Endpoint:Guest Role I       Endpoint:MAC-Auth Exemption:MAC-Auth Exemption:Username       Expire-Time-Update:G       Radius:Aruba:Aruba:Aruba	Output CX-GuestMAC-C [AOS-CX - Bour UNKNOWN (100 D cpiry uestUser ort-Bounce-Host	2 2023-01-12 09:19:09 cpuser 0 12		
SummaryInputEnforcementProfiles:SystemPostureSystemPostureRADIUSResponseEndpoint:GuestEndpoint:MAC-AuthEndpoint:UsernameExpire-Time-Update:GuestRadius:Aruba-PRadius:IETF:Calling-St	Output CX-GuestMAC-C [AOS-CX - Bour UNKNOWN (100 D cpiry uestUser ort-Bounce-Host ration-Id	aching, CX MAC Caching Expire Post Login, [Update Endpoint Known], ice Switch Port] 0) 2 2 2023-01-12 09:19:09 cpuser 0 12 28-D2-44-52-C2-38		
Summary     Input       Enforcement     Profiles:       System     Posture       Status:     Status:       RADIUS     Response       Endpoint:Guest     Role I       Endpoint:MAC-Auth     Explore-Time-Update:G       Radius:Aruba:Aruba-P       Radius:IETF:Calling-Si       Radius:IETF:NAS-Idem	Output CX-GuestMAC-C [AOS-CX - Bour UNKNOWN (100 D cpiry uestUser ort-Bounce-Host cation-Id tifier	aching, CX MAC Caching Expire Post Login, [Update Endpoint Known], ice Switch Port]  2 2 2 2023-01-12 09:19:09 cpuser 0 12 28-D2-44-52-C2-38 6200-Lab		
Summary       Input         Enforcement Profiles:         System Posture Status:         RADIUS Response         Endpoint:Guest Role I         Endpoint:MAC-Auth Exployint:Username         Expire-Time-Update:G         Radius:Aruba:Aruba-P         Radius:IETF:Calling-St         Radius:IETF:NAS-Ident         Radius:IETF:NAS-Port	Output CX-GuestMAC-C [AOS-CX - Bour UNKNOWN (100 D cpiry uestUser ort-Bounce-Host cation-Id tifier	aching, CX MAC Caching Expire Post Login, [Update Endpoint Known], ice Switch Port] ) 2 2023-01-12 09:19:09 cpuser 0 12 28-D2-44-52-C2-38 6200-Lab 1		
SummaryInputEnforcementForfiles:SystemPostureSystemPostureRADIUSResponseEndpoint:MAC-AuthEndpoint:MAC-AuthEndpoint:UsernameExpire-Time-Update:GRadius:Aruba-PRadius:IETF:Radius:IETF:NAS-IdenRadius:Radius:IETF:NAS-PortRadius:Radius:IETF:NAS-PortRadius:Radius:IETF:NAS-PortRadius:Radius:IETF:User-NameNameRadius:IETF:StateNameRadius:IETF:NAS-PortRadius:Radius:IETF:User-NameNameRadius:IETF:User-NameNameRadius:IETF:User-Name <t< td=""><td>Output CX-GuestMAC-C [AOS-CX - Bour UNKNOWN (100 D cpiry uestUser ort-Bounce-Host cation-Id tifier</td><td>aching, CX MAC Caching Expire Post Login, [Update Endpoint Known], ice Switch Port]</td></t<>	Output CX-GuestMAC-C [AOS-CX - Bour UNKNOWN (100 D cpiry uestUser ort-Bounce-Host cation-Id tifier	aching, CX MAC Caching Expire Post Login, [Update Endpoint Known], ice Switch Port]		

# 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:		ACCE	T				
Session Identif	fier:	R0000	)0006-01-63bde8b7				
Date and Time	:	Jan 11	1, 2023 09:37:43 AEDT				
End-Host Identifier:		28-D2	28-D2-44-52-C2-38 (Computer / Windows / Windows 10)				
Username:		-cpuse	F				
Access Device	IP/Port:	192.1	68.1.25:1 (CX-SW1 / Aruba)				
Access Device	Name:	6200-	Lab				
System Postur	e Status:	UNKN	OWN (100)				
			Policies Used -				
Service:		CX DU	JR MAC Auth				
Authentication	Method:	MAC-A	AUTH				
Authentication	Source:	Local:	localhost				
Authorization S	Source:	[Gues [Insig	t User Repository], [Guest Device Repository], [Endpoints Repository], ht Repository], [Time Source]				
Roles:		[Gues	t], [MAC Caching], [User Authenticated]				



Summary Inp	out Outp	ut	Accounting	
Enforcement Profil	es: CX-D	UR-N	MAC-Auth-Guest, CX Return-Endpoint-Username	
System Posture St	atus: UNKI	NOW	N (100)	
Audit Posture State	us: UNKI	NOW	N (100)	
RADIUS Response				
Radius:Aruba:Ar	uba-CPPM-f	Role	CX_DUR_MAC_Auth_Guest-3024-5 class ip IP-Any-Any2 10 match 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	

#### And this is what we see on the LAN switch

6200-Lab# sh	port-access clie	ents		
Port Access C	lients			
Status Codes:	d device-mode,	c client-mode,	m multi-domain	
Port MA Device Type	C-Address	Onboarding Method	Status	Role
c 1/1/1 28 CX_DUR_MAC_Au	:d2:44:52:c2:38 th_Guest-3024-5	mac-auth	Success	
6200-Lab#				
6200-Lab# sh	port-access clie lient Status Det	ents detail		
Client 28:d2:	44:52:c2:38, cpi	iser		
Session Det Port Session T IPv4 Addr IPv6 Addr Device Ty	ails  : 1/1/1 ime : 358s ess : 172.16.14 ess : pe :	.28		
VLAN Detail  VLAN Grou VLANs Ass Access Native	s - p Name : igned : 14 : 14 Untagged :			



Allowed Trunk :

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 \_\_\_\_\_ Cached Reauthentication Period : 3000 secs Authentication Mode : client Reauthentication Period : 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:		ACCE	PT		
	Session Ident	ifier:	W000	00002-01	-63bdec3b	
	Date and Time	e:	Jan 1	1, 2023 0	9:52:43 AEDT	
	End-Host Ider	ntifier:	28-D2	2-44-52-0	2-38	
	Username:		staff1			
	Access Device	e IP/Port:	-			
	Access Device	Name:	-			
	System Postu	re Status:	UNKN	OWN (10	0)	
					Policies Used -	
	Service:		CX G	lestWebA	uth	
	Authentication	n Method:	Not a	pplicable		
	Authentication	n Source:	Lab-A	D		
	Authorization	Source:	[Endp	oints Rep	ository], [Time Source], Lab-AD	
	Roles:		[User	Authentic	ated]	
	Enforcement I	Profiles:	CX-A	D-MAC-Ca	ching, [AOS-CX - Bounce Switch Port]	
	Summary	Input	Output	Alerts		
E	Enforcement Pr	rofiles:	CX-AD-MA	C-Caching	J, [AOS-CX - Bounce Switch Port]	
\$	System Posture	e Status:	UNKNOW	(100)		
	RADIUS Respo	onse				۲
	Endpoint:Gue	est Role IL	<b>)</b>	AD		
	Endpoint:MAG	C-Auth Ex	piry	202	23-01-12 09:00:00	
	Endpoint:Use	ername		sta	11	
	Radius:Aruba		ort-Bounce	-Host 12	D2 44 52 62 20	
	Radius:IETF:	Calling-Su	ation-id	28-	-D2-44-52-C2-38	
	Radius IETE	NAS-Iuen	uner	1	JU-LAU	
	Radius IETE	User-Nam	٩	28/	124452c238	
	Naulus.ILTF.	03er-Indill	0	200	1277326230	

#### And the Session #4



_	Summary	Input	Output	Accounting					
Login Status: ACCE				PT					
Session Identifier: R000			R0000	000000b-01-63bdeef2					
Date and Time: Jan 1				an 11, 2023 10:04:18 AEDT					
End-Host Identifier: 28-E			28-D2	2-44-52-C2-38	(Computer / Windows / Windows 10)				
	Username:		staff1						
	Access Device	e IP/Port:	192.1	68.1.25:1 (CX-	SW1 / Aruba)				
	Access Device	e Name:	6200-	Lab					
	System Postu	re Status:	UNKN	OWN (100)					
					Policies Used -				
	Service:		CX DI	JR MAC Auth					
	Authenticatio	n Method:	MAC-	AUTH					
	Authentication	n Source:	Local:	localhost					
Authorization Source: [Gue [Insig Roles: [MAC			[Gues [Insig	Guest User Repository], [Guest Device Repository], [Endpoints Repository], Insight Repository], [Time Source]					
			[MAC	MAC Caching], [User Authenticated]					
	C	Turnut	Output	Accounting					
	Summary	Input	Ουτρυτ	Accounting					
E	Inforcement F	Profiles:	CX-DUR-	ADGuest, CX R	eturn-Endpoint-Username				
S	System Postur	re Status:	UNKNOW	OWN (100)					
F	Audit Posture	Status:	UNKNOW	/N (100)					
	RADIUS Resp	onse							
	Radius:Arub	a:Aruba-C	CPPM-Role	CX_DUR_ADG class ip IP-Am 10 match any port-access por 10 class ip IP- port-access ro description DU associate politi auth-mode cli	Guest-3025-6 y-Any2 any any olicy ADGuest-Pol2 -Any-Any2 ole ADGuest2 JR-for-Guest cy ADGuest-Pol2 ent-mode				

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

Configura	Configuration » Identity » Endpoints								
Endpoi	ints								
		Edi	t Endpoint						8
This page which it is	auto 5 coni	I	Endpoint	Attributes	Device Fingerprints	Poli	cy Cache		
			Attribut	te			Value		
Filter: MA	C Add	1.	Guest Ro	ole ID		=	AD-User	Ēþ	Ť
#	•	2.	MAC-Aut	h Expiry		=	2023-01-12 09:00:00	Ē	Ť
1.		з.	Usernam	пе		=	staff1	Ē	Ť
2.		4.	Click to a	add					
3.			1						

# **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:

	Туре	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 F	lesults:	Use cached F	oles and	Posture attribute	es from previous sessions	
Enforcement Policy:		Wired 802.1X W	ired DUR E	Enforcement Policy	y ✔ Modify Add New Enforcement Policy	
				Enfor	orcement Policy Details	
Description:						
Default Profil	e:	CX dot1x Wire	CX dot1x Wired Default Profile			
Rules Evaluat	ion Algorithr	n: first-applicable				
Conditi	ons				Enforcement Profiles	
1. (Authorization:Lab-AD:memberOf CONTAL			ONTAINS	Staff)	CX-DUR-Staff, [Update Endpoint Known]	
2. (Authorization:Lab-AD:memberOf CONTAINS			ONTAINS	Student)	CX-DUR-Student, [Update Endpoint Known]	
3. (Tips:F	Role <mark>EQUALS</mark>	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 ✓	<b>⊕</b> 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 (	Dutput		
Login Status:	ACCEPT		
Session Identifier:	R0000001-01-63bf6331		
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:	antAP, [User Authenticated]		
Enforcement Profiles:	CX-DUR-InstantAP-1x		
Summary Input 0	Accounting		
Enforcement Profiles: C	X-DUR-InstantAP-1x		
System Posture Status: U	INKNOWN (100)		
Audit Posture Status: U	INKNOWN (100)		
RADIUS Response	$\odot$		
Radius:Aruba:Aruba-CPF	PM-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       5		

### From the switch we can see this

6200-Lab# s	sh port-access clie	ents		
Port Access	s Clients			
Status Code	es: d device-mode,	c client-mode,	m multi-domain	
Port Device Type	MAC-Address	Onboarding Method	Status	Role
d 1/1/1 3029-4	20:4c:03:23:a7:c0	dot1x	Success	CX_DUR_InstantAP_1x-

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

Port Access Client Status Details:



```
Client 20:4c:03:23:a7:c0, InstantAP
_____
 Session Details
 _____
         : 1/1/1
   Port
   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
                                  : DUR-for-IAPs
   Description
   Gateway Zone
   UBT Gateway Role
   UBT Gateway Clearpass Role
   Access VLAN
                                   : 15
   Native VLAN
                                   : 11-12
   Allowed Trunk VLANs
   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
                                   :
                                  : InstantAP-Pol2 CX DUR InstantAP 1x-3029-4
   Policy
   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

S	ummary Pro	file Attributes				
Pro	file:					
Nar	ne:	CX-DUR-I	nstantAP			
Des	cription:					
Тур	e:	RADIUS				
Acti	on:	Accept				
Dev	rice Group List:	-				
Pro	duct:	AOS-CX				
Att	ributes:					
	Туре		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 F	Results:	Use cached F	Roles and Posture	attributes	from previous s	sessions
Enforcement	Policy:	Ariya Wired-CX	DUR MAC Auth	```	Modify	Add New Enforcement Policy
				Enfor	cement Policy De	etails
Description:						
Default Profil	e:	CX-DUR-Guest	-CaptivePortal			
Rules Evaluat	ion Algorith	m: first-applicable	9			
Conditi	ons					Enforcement Profiles
1. (Autho	prization:[En	dpoints Repository	/]:Conflict EQUAL	S true)		Wired-CX-MAC-Spoof-CP
2. (Tips:	Role EQUAL	School-Asset)				CX-DUR-CorpDev
(Tips:Role MATCHES_ALL [MAC Caching] 3. [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. (Autho	5. (Authorization:[Endpoints Repository]: Device Name EQUALS Aruba IAP)				ruba 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	0
11.	11	CX DUR dot1x Wired	RADIUS	802.1X Wired	<b>O</b>
12.	12	CX MAC Auth	RADIUS	MAC Authentication	0
13.	13	CX DUR MAC Auth	RADIUS	MAC Authentication	
14.	□ 14	CX GuestWebAuth	WEBAUTH	Web-based Authentication	<b>S</b>

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 Captiveportal 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

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

Summary Input O	utput Accounting RADIUS CoA Alerts				
Login Status:	ACCEPT				
Session Identifier:	R0000004-01-63bf698a				
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-CaptiveP	ortal		
System Posture Status:	UNKNOW	'N (100)			
Audit Posture Status:	UNKNOW	'N (100)			
RADIUS Response					۲
Radius:Aruba:Aruba-C	PPM-Role	CX_DUR_Gues class ip ClearP 10 match tcp a 20 match tcp a class ip DHCP- 10 match udp 20 match udp class ip ICMP2 10 match icmp class ip Web-T 10 match tcp a 20 match tcp a	st_CaptivePortal- bass2 any 192.168.1.9 any 192.168.1.9 DNS2 any any eq 67 any any eq 53 b any any eq 53 c any any eq 80 any any eq 80 any any eq 443	3023-11 5 eq 80 5 eq 443	

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

RADIUS CoA

Alerts

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 5<sup>th</sup> rule in the enforcement policy and gets the CX-DUR-InstantAP enforcement profile.

#### This is session #1

Summary Input Output Accounting

Summary Input	Output	Accounting			
Login Status:	ACCE	рт			
Session Identifier:	R0000	R0000005-01-63bf69cd			
Date and Time:	Jan 12	Jan 12, 2023 13:00:45 AEDT			
End-Host Identifier:	20-40	20-4C-03-23-A7-C0 (Access Points / Aruba / Aruba IAP)			
Username:	204c0	204c0323a7c0			
Access Device IP/Port:	192.1	68.1.25:1 (CX-	SW1 / Aruba)		
Access Device Name:	6200-	6200-Lab			
System Posture Status:	UNKN	UNKNOWN (100)			
			Policies Used -		
Service:	CX DL	JR MAC Auth			
Authentication Method:	MAC-A	AUTH			
Authentication Source:	None				
Authorization Source:	[Gues [Insig	t User Reposito ht Repository],	ory], [Guest Device Repository], [Endpoints Repository], [Time Source]		
Roles:	[Othe	r], [User Authe	nticated]		



Summary	Input	Output	Accounting						
Enforcement	Profiles:	[Update	e Endpoint Known], <mark>CX-DUR-InstantAP</mark>						
System Postu	tem Posture Status: UNK		WN (100)						
Audit Posture	Status:	UNKNOW	NOWN (100)						
RADIUS Resp	oonse								
Radius:Arub	oa:Aruba-C	CPPM-Role	CX_DUR_Insta class ip IP-Any 10 match any port-access po 10 class ip IP- port-access ro description DU associate polic auth-mode de poe-priority cr trust-mode ds vlan trunk atc	antAP-3026-5 /-Any2 any any vicy InstantAP-Pol2 Any-Any2 le DUR-InstantAP IR-for-IAPs ty InstantAP-Pol2 vice-mode itical cp ive 15 wood 11-12					

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

5200-Lab# sh port-access clients									
Port Access Clients									
Status Codes: d device-mode,	c client-mode,	m multi-domain							
Port MAC-Address Device Type	Onboarding Method	Status	Role						
c 1/1/1 20:4c:03:23:a7:c0 CX_DUR_Guest_CaptivePortal-30	mac-auth )23-11	Success							
6200-Lab# sh port-access clie No port-access clients found 6200-Lab# 6200-Lab# 6200-Lab# sh port-access clie	ents ents								
Port Access clients									
Status Codes: d device-mode,	c client-mode,	m multi-domain							
Port MAC-Address Device Type	Onboarding Method	Status	Role						
d 1/1/1 20:4c:03:23:a7:c0 mac-auth <mark>Success CX_DUR_InstantAP</mark> - 3026-5									
6200-Lab#									
6200-Lab# sh port-access clie Port Access Client Status Det	ents de cails:								
Client 20:4c:03:23:a7:c0, 204	lient 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
   Reauthentication Period
   Session Timeout
   Client Inactivity Timeout
   Description
                                    : DUR-for-IAPs
   Gateway Zone
   UBT Gateway Role
   UBT Gateway Clearpass Role
   Access VLAN
   Native VLAN: 15Allowed Trunk VLANs: 11-12
   Native VLAN
   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
                                     : InstantAP-Pol2 CX DUR InstantAP-3026-5
   Policy
   Device Type
Access Policy Details:
Policy Name : InstantAP-Pol2_CX_DUR_InstantAP-3026-5
Policy Type : Downloaded
Policy Status : Applied
SEQUENCE CLASS
                                      TYPE ACTION
                                                                        30 | Page
aruba
```

```
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 b	prief								
Port Descriptio	Native	Mode	Туре	Enabled	Status	Reason			Speed	
	VLAN								(Mb/s)	
1/1/1	15	trunk	1GbT	yes	up				1000	
1/1/2	15	access	1GbT	yes	down	Waiting #	for 1	link		
1/1/3	1	access	1GbT	yes	down	Waiting #	for 1	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.

New Authentication Serve	r		?
Туре	RADIUS     LDAP     TACACS		
RADIUS Type	Dynamic Authorization	Only	
Name	ClearPass-FQDN		
RadSec			
IP Address	victory2.arubatechs.com		
Auth port	1812		
Accounting port	1813		
Shared key			
Retype key			
Timeout	5	sec.	
Retry count	3		
Dynamic Aut <mark>horizatio</mark> n			
AirGroup CoA port	5999		
Status-Server	Authentication	Accounting	
NAS-IP-Address		(optional)	
NAS-Identifier		(optional)	- 1
Dead time	5	min.	
DRP IP			
DRP Mask			
DRP VLAN			
DRP Gateway			
Service-Type Framed-User	802.1X Captive	Portal MAC	



CPPINI username	lap-dur	
CPPM password		

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

Dashboard	Admin	nistration » Users and Privile	eges » Admin Users					
Monitoring	Adm	Admin Users						
🖧 Configuration 🔹 🤇	D							
🛃 Administration 🛛 🔇								
ClearPass Portal Users and Privileges  Admin Users  Admin Privileges	This p and di Filter:	This page allows super admins to add administrator user types, set the admin password policy, change the admin password, and disable admin user accounts.  Filter: User ID  Contains  Go Clear Filter						
🖃 🖉 Server Manager	#	User ID 🔺	Name	Privilege Level	Status			
- Jerver Configuration	1.	admin	Super Admin	Super Administrator	Enabled			
– <i>b</i> Log Configuration	2.	apiadmin	API Admin	API Administrator	Enabled			
- & Local Shared Folders	3.	C cx-dur	cx-dur	Aruba User Role Download	Enabled			
Licensing	4.	🗆 lap-dur	iap-dur	Aruba User Role Download	Enabled			

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.

edit ES 1 Basic	2 VLAN		
Name & Usage			
Name	ES		
Туре	Wireless 🗸	•	
Primary usage	Employee	~	
edit ES 1 Basic	2 VLAN	3 Security	
Security Level			
Security Level	Enterprise 🗸		
Key management	WPA2-Enterprise		~
Authentication server 1	ClearPass-FQDN	<mark>y</mark> 🗹 🕇	
Authentication server 2	Select Server	<b>→</b> +	
EAP offload			
edit ES 1 Basic	2 VLAN	3 Security	4 Access
Access Rules			
Access Rules	Unrestrict	ed 🗸	
Download roles			

No restrictions on access based on destination or type of traffic

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 clearp	pass 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 🔺	Туре	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
I	Profile:		
	Name:		school 1x
	Description:		
	Type:		RADIUS
	Action:		Accept
	Device Group	List:	-

#### Attributes:

	Туре	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 1x
Description:		
Туре:		RADIUS
Action:		Accept
Device Group	List:	-
Attailantaa		

#### Attributes:

	Туре	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



Serv	vices	- Schoo	ol 802.1X Wil	-i		
Sum	mary	Service	Authentication	Roles	Enforcement	
Use Ca	ached R	lesults:	Use cached	Roles and	Posture attribut	tes from previous sessions
Enforcement Policy:			IAP DUR 802.1	K WiFi Enfo	prcement Policy	Modify     Add New Enforcement Policy
					Enf	orcement Policy Details
Descri	ption:					
Defaul	t Profile	e:	[Deny Access	Profile]		
Rules I	Evaluat	ion Algorith	m: first-applicable	е		
C	Conditi	ons				Enforcement Profiles
1.	(Autho	rization:Lal	o-AD:memberOf C	ONTAINS	Staff)	school 1xWiFi DUR Staff, [Update Endpoint Known]
2. (Authorization:Lab-			o-AD:memberOf C	ONTAINS	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	<b>~</b>	🕂 Go Cle	ear Filter	Shov
#	Server	Source	Username	Service	Login Status	Enforcem	ent Profiles
1.	192.168.1.9	5 RADIUS	s <mark>taff1</mark>	School 802.1X WiFi	ACCEPT	[Update Er <mark>Staff</mark>	ndpoint Known], <mark>school 1xWiFi DUR</mark>
Sumr	nary Input	Output	Accounting				
Login S	itatus:	ACCE	PT				
Session	Identifier:	R000	00007-01-63bf74	28			
Date ar	nd Time:	Jan 1	2, 2023 13:44:57	AEDT			
End-Ho	st Identifier:	F0-D5	5-BF-4B-67-11 (	Computer / Windows / Wind	ows 10)		
Userna	me:	staff1					
Access	Device IP/Port:	172.1	6.15.10				
Access	Device Name:	172.1	6.15.25				
System	Posture Status	: UNKN	IOWN (100)				
			Po	licies Used -			
Service	:	Schoo	ol 802.1X WiFi				
Authen	tication Method	EAP-F	PEAP, EAP-MSCHAP	v2			
Authen	tication Source:	AD:19	92.168.1.250				
Authori	zation Source:	Lab-A	D				
Roles:		[User	Authenticated]				
Enforce	ement Profiles:	[Upda	ate Endpoint Know	vn], <mark>school 1xWiFi DUR Staff</mark>			
Summ	any Input	Output	Accounting				
Enforce	ment Profiles:	[Update B	Endpoint Known],	school 1xWiFi DUR Staff			=
System	Posture Status:	UNKNOW	N (100)				
Audit Po	osture Status:	UNKNOW	N (100)				
RADIU	S Response					۲	
Radius:Aruba:Aruba-CPPM-Role school_1xV wlan acces rule any ar			school_1xWiFi_D wlan access-rule rule any any mat	UR_Staff-3030-9 Staff ch any any any permit			
Radius:Aruba:Aruba-User-Vlan 11		11					
Radiu	s:IETF:Session-	Timeout	28800				
01.1	s-Undate Endpo	int	Known				



