Contents

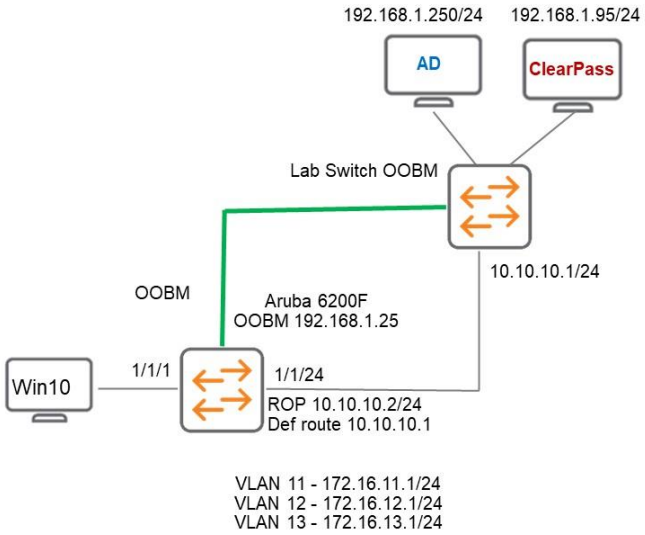
1.1 Revision History

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

2 ClearPass Wired Enforcement for CX Switches Part 2

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

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



2.1 Things you need

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

2.2 Demo/PoC Assumptions

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

2.3 Demonstration Goals

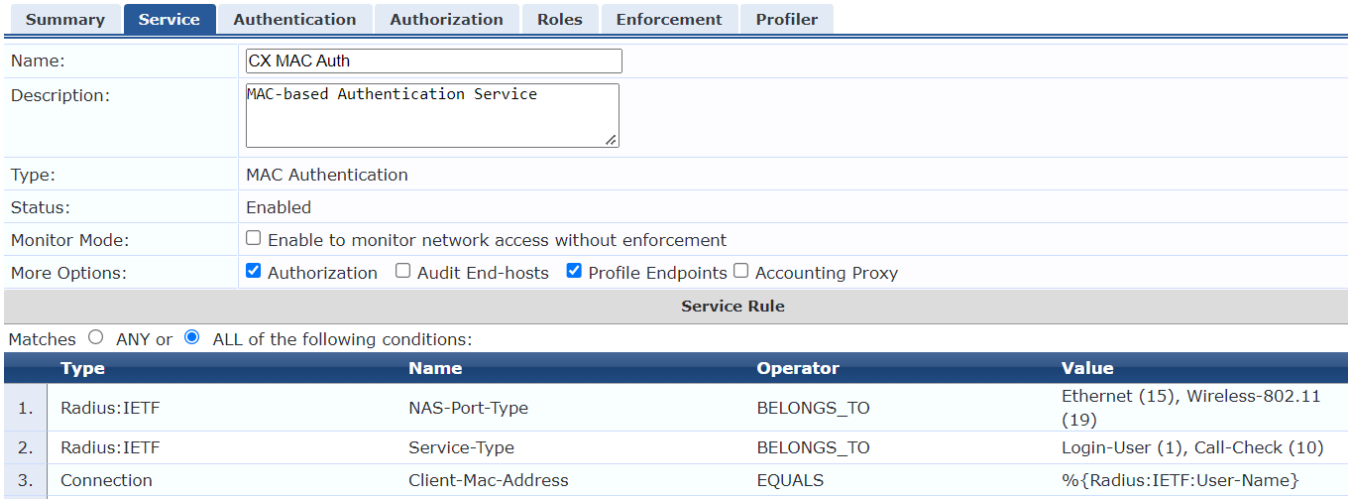
Demonstrating the wired enforcement using Local user roles for

- Wired MAC authentication
- MAC authentication and MAC caching with automatic captive portal redirection
- AD user having access to Guest portal on temporary basis.

3 ClearPass LUR MAC Auth Configuration

3.1 Services - CX MAC Auth with Local User Role

Here we configure the MAC Auth service to go with guest captive portal so when the authenticated users reconnect, they should not get prompted for the captive portal again.



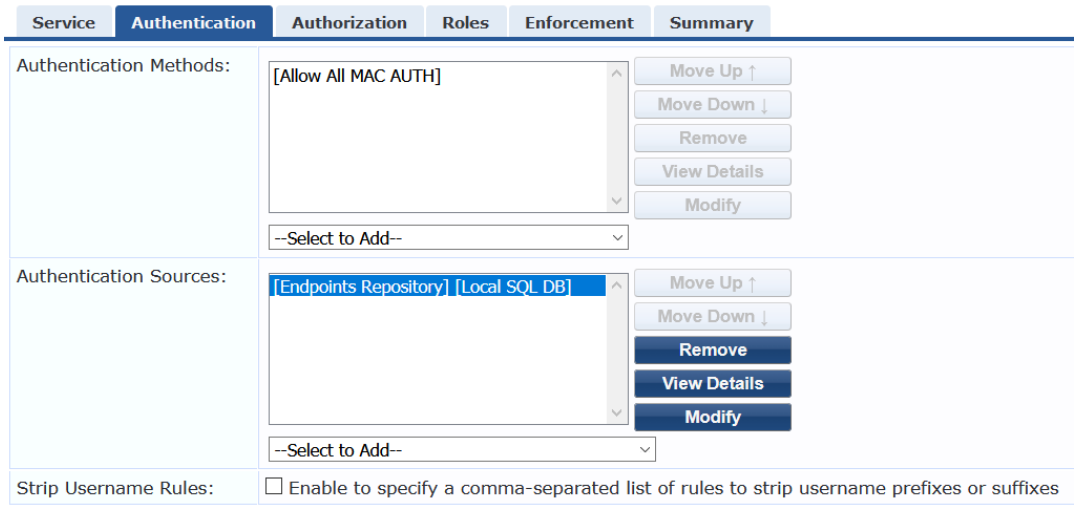
Summary | Service | Authentication | Authorization | Roles | Enforcement | Profiler

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

Service Rule

Matches ○ ANY or ◉ ALL of the following conditions:

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

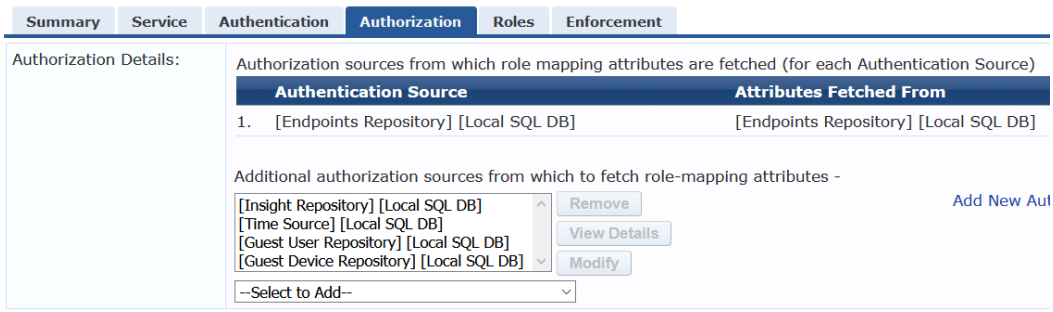


Service | Authentication | Authorization | Roles | Enforcement | Summary

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

Authentication Sources: [Endpoints Repository] [Local SQL DB] — Move Up ↑ | Move Down ↓ | Remove | View Details | Modify — --Select to Add--

Strip Username Rules: ☐ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes



Summary | Service | Authentication | Authorization | Roles | Enforcement

Authorization Details:

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

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

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

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

Remove | View Details | Modify | Add New Aut

--Select to Add--

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

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

Role Mapping Policy Details

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

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

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

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

Enforcement Policy: Wired-CX MAC Auth [Modify] Add New Enforcement Policy

Enforcement Policy Details

Description:	
Default Profile:	Wired-CX-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)	Wired-CX-CorpDev
3.	(Tips:Role *MATCHES_ALL* [MAC Caching] [Guest] [User Authenticated])	Wired-CX-MAC-Auth Guest, CX Return-Endpoint-Username
4.	(Tips:Role *EQUALS* [MAC Caching]) *AND* (Endpoint:Guest Role ID *EQUALS* AD-User)	Wired-CX-AD-Guest, CX Return-Endpoint-Username
5.	(Authorization:[Endpoints Repository]:Device Name *EQUALS* Aruba IAP)	CX Wired Instant-AP

For time being we won't cover the first two rules as it will be covered later.

3.2 Enforcement Profiles

Here are the enforcement profiles that were referenced in the enforcement policy "Wired-CX MAC Auth" that were used in the MAC auth service.

- Wired-CX-CorpDev

Summary | **Profile** | **Attributes**

Profile:

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

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	Corp-Dev
2.	Radius:IETF	Session-Timeout	=	28800

- Wired-CX-MAC-Auth Guest

Summary | Profile | Attributes

Profile:

Name:	Wired-CX-MAC-Auth Guest
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	Guest
2.	Radius:IETF	Session-Timeout	=	28800

- Wired-CX-AD-Guest

Summary | Profile | Attributes

Profile:

Name:	Wired-CX-AD-Guest
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	AD-Guest
2.	Radius:IETF	Session-Timeout	=	28800

- CX Return-Endpoint-Username

Summary | Profile | Attributes

Profile:

Name:	CX Return-Endpoint-Username
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:IETF	User-Name	=	%{Endpoint:Username}

The above enforcement profile is used to send back the username to the Aruba switch so that when you use show commands you can see the username as well.

- Wired-CX-Guest CaptivePortal

Summary | Profile | Attributes

Profile:

Name:	Wired-CX-Guest CaptivePortal
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	Captive-Portal
2.	Radius:Aruba	Aruba-Captive-Portal-URL	=	https://192.168.1.95/guest/wired_guest.php
3.	Radius:IETF	Session-Timeout	=	600

Note that the above highlighted attribute will not work with LUR.

We can't use a local/downloaded user role with other RADIUS attributes. That's why we need to remove it ansd then add it to the captive-portal profile in the local role on the CX switch.

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

```
port-access policy cp-policy
    10 class ip DHCP-DNS
    20 class ip ICMP
    30 class ip ClearPass
    40 class ip Web-Traffic action redirect captive-portal
```

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

```
port-access role Captive-Portal
    description LUR-for-PreAuth
    associate captive-portal-profile cp-profile
    associate policy cp-policy
    auth-mode client-mode
    client-inactivity timeout 400
    trust-mode none
    reauth-period 3000
    vlan access 13
```

The enforcement profile should look like this, which will pass "Captive-Portal" as a user role, the rest is configured on the switch.

Summary | **Profile** | **Attributes**

Profile:

Name:	Wired-CX-Guest CaptivePortal
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

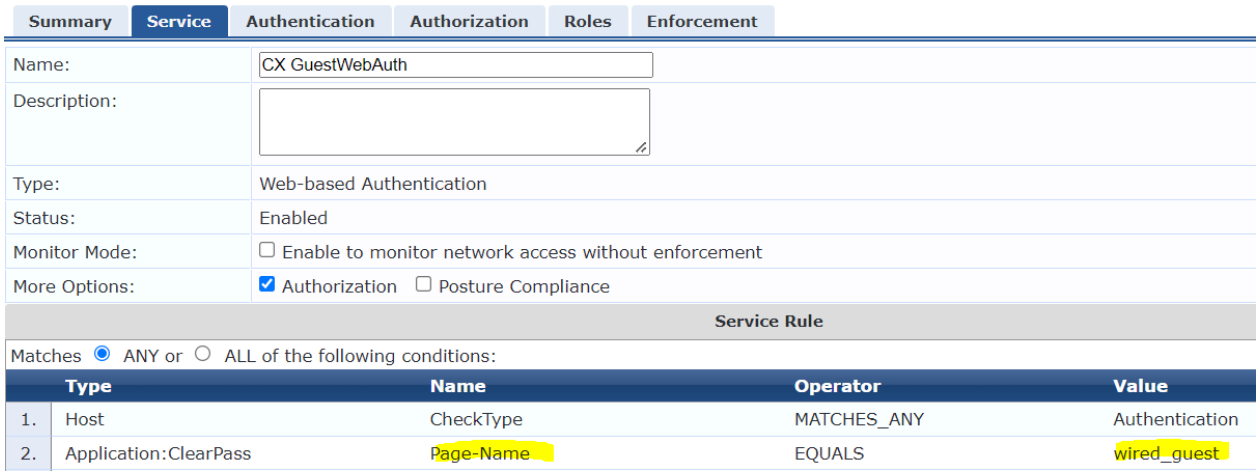
Attributes:

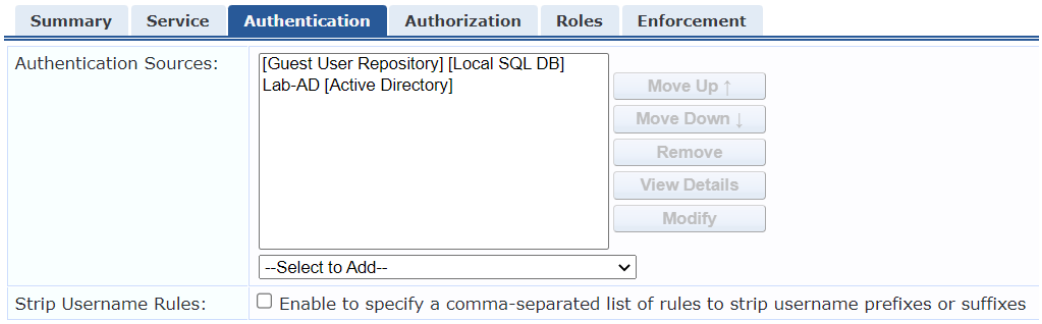
	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	Captive-Portal
2.	Radius:IETF	Session-Timeout	=	600

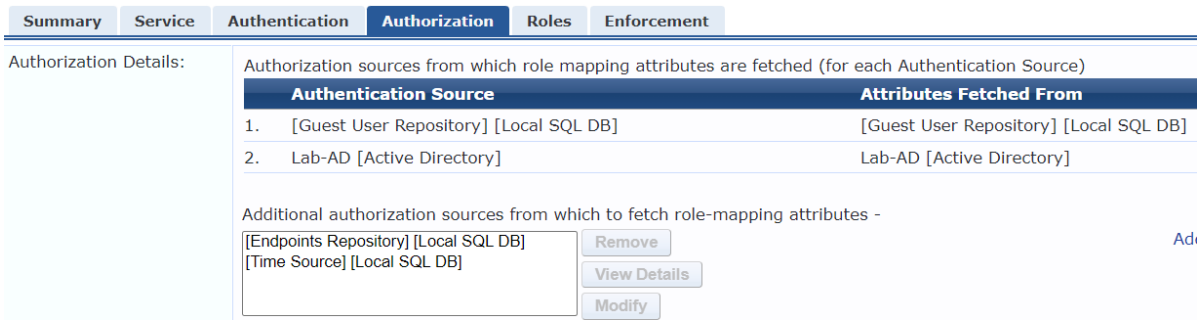
3.3 Services –CX GuestWebAuth

We use server-initiated workflow for Aruba switches. This also makes the enforcement policy for the WEBAUTH quite simple. The main aim here is to update the endpoint database with some attributes that will be used for subsequent MAC authentications and then bounce the port to trigger a re-authentication event and perhaps VLAN change and for the client to request a new IP address.

If a VLAN change is not required, a Terminate Session disconnect message can be used instead of a Bounce-Switch-Port.







No role mapping used here.

3.4 Enforcement Profiles

- Enforcement Profiles - CX-GuestMAC-Caching

Summary | Profile | Attributes

Profile:

Name:	CX-GuestMAC-Caching
Description:	
Type:	Post_Authentication
Action:	
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Endpoint	Username	=	%{Authentication:Username}
2.	Endpoint	Guest Role ID	=	%{GuestUser:Role ID}
3.	Endpoint	MAC-Auth Expiry	=	%{Authorization:[Guest User Repository]:ExpireTime}

Now we need an enforcement profile for the AD users. Since captive portal-based access should only be temporary for employees, an expiration of one day will be used via [Time Source] which is a pre-built authentication source.

- Enforcement Profiles - CX-AD-MAC-Caching

Summary | Profile | Attributes

Profile:

Name:	CX-AD-MAC-Caching
Description:	
Type:	Post_Authentication
Action:	
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Endpoint	Username	=	%{Authentication:Username}
2.	Endpoint	Guest Role ID	=	AD-User
3.	Endpoint	MAC-Auth Expiry	=	%{Authorization:[Time Source]:One Day DT}

Since the above is a Post_Authentication profile, we'll write three attributes into the endpoint database.

1. the name if the user
2. the guest role ID which will be AD-User
3. and the expiry time which will be 1 day

- Enforcement Profiles - CX MAC Caching Expire Post Login

Summary | Profile | Attributes

Profile:

Name:	CX MAC Caching Expire Post Login
Description:	
Type:	Post_Authentication
Action:	
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Expire-Time-Update	GuestUser	=	%{GuestUser:expire_postlogin}

- Enforcement Profiles - [Update Endpoint Known]

Summary | Profile | Attributes

Profile:

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

Attributes:

	Type	Name		Value
1.	Status-Update	Endpoint	=	Known

- Enforcement Profiles - [AOS-CX Bounce Host-Port]

Summary | Profile | Attributes

Profile:

Name:	[AOS-CX - Bounce Switch Port]
Description:	System-defined profile to bounce the switch port on AOS-CX switches.
Type:	RADIUS_CoA
Action:	CoA
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:IETF	Calling-Station-Id	=	%{Radius:IETF:Calling-Station-Id}
2.	Radius:IETF	NAS-Port	=	%{Radius:IETF:NAS-Port}
3.	Radius:IETF	NAS-Identifier	=	%{Radius:IETF:NAS-Identifier}
4.	Radius:IETF	User-Name	=	%{Radius:IETF:User-Name}
5.	Radius:IETF	Event-Timestamp	=	%{Radius:IETF:Event-Timestamp}
6.	Radius:Aruba	Aruba-Port-Bounce-Host	=	12

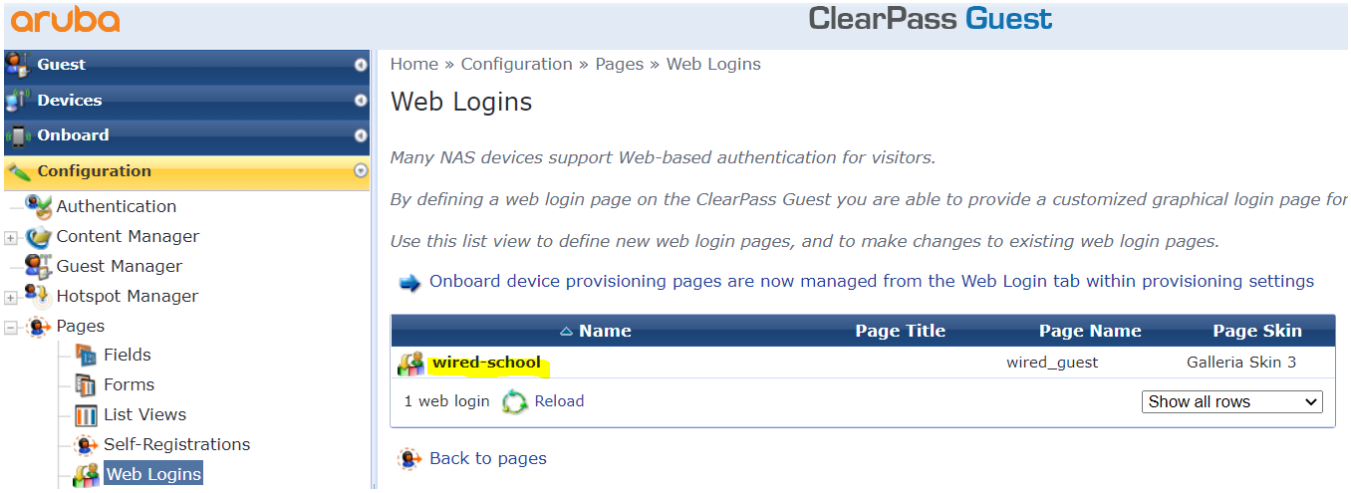
Note that any enforcement profiles/policies/services/role-mapping that are in square brackets [] are system default and you don't have to create them.

3.5 ClearPass Guest Splash Page

Remember that we configured the redirection URL on the switch

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

This URL should match the weblogin page "wired_guest.php"



The only relevant settings on the weblogin page are the NAS Vendor Settings and the Login Delay.

Under NAS Vendor Settings, be sure the Vendor Settings are set to Hewlett Packard Enterprise. This will tell Guest to use a server-initiated login and which will craft a WEBAUTH request which is handled by the service we previously created.

Web Login Editor

* Name:	wired-school Enter a name for this web login page.
Page Name:	wired_guest Enter a page name for this web login. The web login will be accessible from "/guest/page_name.php".
Description:	Comments or descriptive text about the web login.
* Vendor Settings:	Hewlett Packard Enterprise Select a predefined group of settings suitable for standard network configurations.

Page Redirect
Options for specifying parameters passed in the initial redirect.

Security Hash:	Do not check – login will always be permitted Select the level of checking to apply to URL parameters passed to the web login page. Use this option to detect when URL parameters have been modified by the user, for example their MAC address.

Login Form
Options for specifying the behaviour and content of the login form.

Authentication:	Credentials – Require a username and password Select the authentication requirement. Access Code requires a single code (username) to be entered. Anonymous allows a blank form requiring just the terms or a Log In button. A pre-existing account is required. Auto is similar to anonymous but the page is automatically submitted. Access Code and Anonymous require the account to have the Username Authentication field set.
Prevent CNA:	☑ Enable bypassing the Apple Captive Network Assistant The Apple Captive Network Assistant (CNA) is the pop-up browser shown when joining a network that has a captive portal. Note that this option may not work with all vendors, depending on how the captive portal is implemented.
Custom Form:	☐ Provide a custom login form If selected, you must supply your own HTML login form in the Header or Footer HTML areas.
Custom Labels:	☐ Override the default labels and error messages If selected, you will be able to alter labels and error messages for the current login form.
* Pre-Auth Check:	None — no extra checks will be made Select how the username and password should be checked before proceeding to the NAS authentication.
Terms:	☐ Require a Terms and Conditions confirmation If checked, the user will be forced to accept a Terms and Conditions checkbox.
CAPTCHA:	None Select a CAPTCHA mode.

Default Destination
Options for controlling the destination clients will redirect to after login.

* Default URL:	http://192.168.1.250 Enter the default URL to redirect clients. Please ensure you prepend "http://" for any external domain.
Override Destination:	☑ Force default destination for all clients If selected, the client's default destination will be overridden regardless of its value.

Login Page
Options for controlling the look and feel of the login page.

* Skin:	Galleria Skin 3 Choose the skin to use when this web login page is displayed.
Title:	The title to display on the web login page. Leave blank to use the default (Login).

Header HTML:	`{nwa_cookiecheck}`
	`{if $errmsg}{nwa_icontext type=error}{$errmsg|escape}`
	`{/nwa_icontext}{/if}`
	
	`{nwa_text id=7980}<p>`
	`Please login to the network using your`
	`username and password.`
	`</p>{/nwa_text}`
	Insert...
	HTML template code displayed before the login form.

Footer HTML:	`{nwa_text id=7979}<p>`
	`Contact a staff member if you are experiencing`
	`difficulty logging in.`
	`</p>{/nwa_text}`
	Insert...
	HTML template code displayed after the login form.

Login Message:	`<p>`
	`Logging in, please wait... <span id="refresh"></span>`
	`</p>`
	Insert...
	HTML template code displayed while the login attempt is in progress.

* Login Delay:	30 The time in seconds to delay while displaying the login message.

4 Testing Captive Portal with MAC Auth

Here we are testing the following scenario

1. new guest / temporary AD user connects to a switch port 1
    a. there will be a MAC auth and "Captive-Portal" user role will be sent to the switch which will put the laptop in VLAN 13
    b. the user's browser gets redirected to the captive portal page on ClearPass
    c. the user enters the credential (cpguser) and click on the login button
    d. the user will see 30sec delay countdown on the web page.
    e. there will be a WEB-Auth and certain attributes gets written to the endpoint database
    f. because we are using bounce switch port, after around 12 sec, the switch port will be bounced
    g. there will be a MAC auth and this time based on the rules, a particular user-role will be sent to the switch
2. temporary AD user using the captive portal to login. The workflow should be the same. The Captive Portal user role will be sent to the switch.

4.1 Guest User with Captive Portal with MAC Auth

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

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

Role Information:

Name   : AD-Guest
Type   : local
------------------------------------------------
    Reauthentication Period             : 3000 secs
    Cached Reauthentication Period      :
    Authentication Mode                 : client-mode
    Session Timeout                     :
    Client Inactivity Timeout           : 400 secs
    Description                         : LUR-for-AD-Guest
    Gateway Zone                        :
    UBT Gateway Role                    :
    UBT Gateway Clearpass Role          :
    Access VLAN                         : 11
    Native VLAN                         :
    Allowed Trunk VLANs                 :
    Access VLAN Name                    :
    Native VLAN Name                    :
    Allowed Trunk VLAN Names            :
    VLAN Group Name                     :
    MTU                                 :
    QOS Trust Mode                      :
    STP Administrative Edge Port        :
    PoE Priority                        :
    PVLAN Port Type                     :
    Captive Portal Profile              :
    Policy                              : AD-Guest-Pol
    Device Type                         :

Name   : Captive-Portal
Type   : local
------------------------------------------------
    Reauthentication Period             : 3000 secs
```

```
    Cached Reauthentication Period      :
    Authentication Mode                 : client-mode
    Session Timeout                     :
    Client Inactivity Timeout           : 400 secs
    Description                         : LUR-for-PreAuth
    Gateway Zone                        :
    UBT Gateway Role                    :
    UBT Gateway Clearpass Role          :
    Access VLAN                         : 13
    Native VLAN                         :
    Allowed Trunk VLANs                 :
    Access VLAN Name                    :
    Native VLAN Name                    :
    Allowed Trunk VLAN Names            :
    VLAN Group Name                     :
    MTU                                 :
    QOS Trust Mode                      :
    STP Administrative Edge Port        :
    PoE Priority                        :
    PVLAN Port Type                     :
    Captive Portal Profile              : cp-user
    Policy                              : cp-policy
    Device Type                         :

Name   : Guest
Type   : local
-----------------------------------------------
    Reauthentication Period             : 3000 secs
    Cached Reauthentication Period      :
    Authentication Mode                 : client-mode
    Session Timeout                     :
    Client Inactivity Timeout           : 400 secs
    Description                         : LUR-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-Pol
    Device Type                         :

6200-Lab#
6200-Lab# sh port-access clients
No port-access clients found.

6200-Lab#
```

So now if we connect a non dot1x capable device to the same switch port, we see the MAC authentication happening along with Captive portal redirection. We are using the same laptop without enabling dot1x.

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

Port Access Clients

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

```
--------------------------------------------------------------------------------------------------------
  Port     MAC-Address       Onboarding     Status              Role
Device Type
                             Method
--------------------------------------------------------------------------------------------------------
c 1/1/1    28:d2:44:52:c2:38               In-Progress

6200-Lab# show 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             Captive-Portal

6200-Lab#
```

```
6200-Lab# sh client ip

 MAC Address                Interface        VLAN              IP Address
 ---------------------------------------------------------------------------
 28:d2:44:52:c2:38          1/1/1            13                172.16.13.28

6200-Lab#
```

Now checking access tracker.

Summary | Input | Output | Accounting

Session Identifier:	R00000030-01-63b7a6a2
Date and Time:	Jan 06, 2023 15:42:10 AEDT
End-Host Identifier:	28-D2-44-52-C2-38 (Computer / Windows / Windows 10)
Username:	28d24452c238
Access Device IP/Port:	192.168.1.25:1 (CX-SW1 / Aruba)
Access Device Name:	6200-Lab
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	CX 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]
Enforcement Profiles:	Wired-CX-Guest CaptivePortal

Summary | Input | **Output** | Accounting

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

RADIUS Response

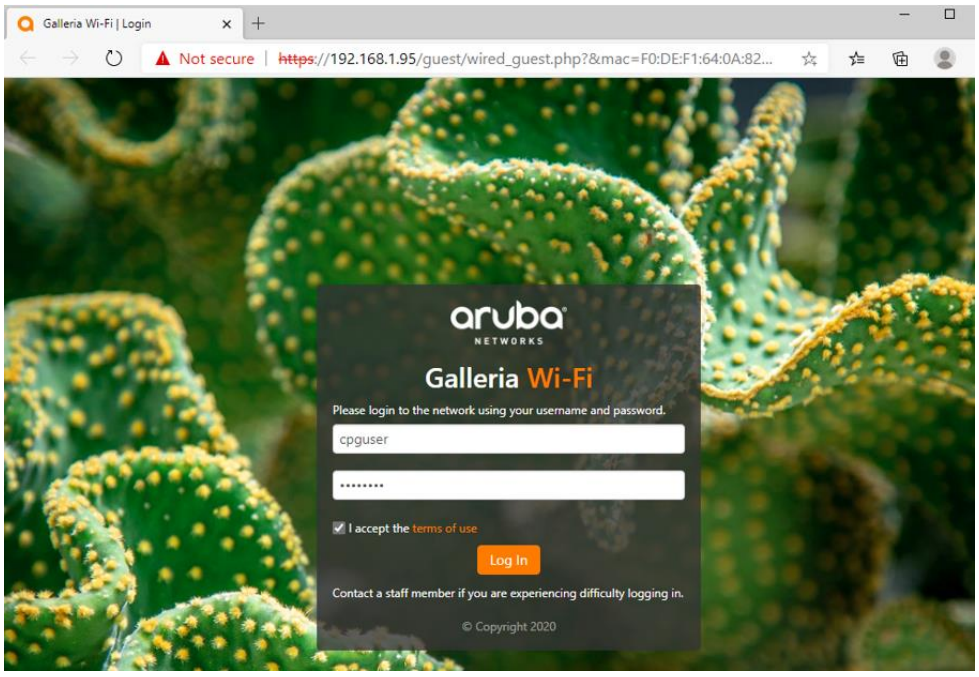
Radius:Aruba:Aruba-User-Role	Captive-Portal
Radius:IETF:Session-Timeout	600

Here we see the client details.

```
6200-Lab# show port-access clients det

Port Access Client Status Details:

Client 28:d2:44:52:c2:38, 28d24452c238
======================================
  Session Details
  ---------------
    Port         : 1/1/1
    Session Time : 257s
    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, 246s ago
                      dot1x - Unauthenticated, Supplicant-Timeout, 246s ago

  Authorization Details
  ---------------------
    Role   : Captive-Portal
    Status : Applied

Role Information:

Name  : Captive-Portal
Type  : local
---------------------------------------------
    Reauthentication Period             : 3000 secs
    Cached Reauthentication Period      :
    Authentication Mode                 : client-mode
    Session Timeout                     :
    Client Inactivity Timeout           : 400 secs
    Description                         : LUR-for-PreAuth
    Gateway Zone                        :
    UBT Gateway Role                    :
    UBT Gateway Clearpass Role          :
    Access VLAN                         : 13
    Native VLAN                         :
    Allowed Trunk VLANs                 :
    Access VLAN Name                    :
    Native VLAN Name                    :
    Allowed Trunk VLAN Names            :
    VLAN Group Name                     :
    MTU                                 :
    QOS Trust Mode                      :
    STP Administrative Edge Port        :
    PoE Priority                        :
    PVLAN Port Type                     :
    Captive Portal Profile              : cp-profile
    Policy                              : cp-policy
    Device Type                         :
```

```
Captive Portal Profile Configuration

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

Access Policy Details:

Policy Name   : cp-policy
Policy Type   : Local
Policy Status : Applied

SEQUENCE    CLASS                          TYPE ACTION
----------- ------------------------------ ---- ----------------------------------
10          DHCP-DNS                       ipv4 permit
20          ICMP                           ipv4 permit
30          ClearPass                      ipv4 permit
40          Web-Traffic                    ipv4 redirect captive-portal

Class Details:

class ip DHCP-DNS
    10 match udp any any eq dhcp-server
    20 match udp any any eq dns
class ip ICMP
    10 match icmp any any
class ip ClearPass
    10 match tcp any 192.168.1.95 eq http
    20 match tcp any 192.168.1.95 eq https
class ip Web-Traffic
    10 match tcp any any eq http
    20 match tcp any any eq https

6200-Lab#
```

Now the guest user will start its web browser and in our example will browse to http://airwave.mylab.com gets redirected to Captive portal and uses “cpguser” guest account to login as shown below:



At this stage we should see a WEB-Auth session in ClearPass Access tracker (session #2) below.

#	Server	Source	Username	Service	Login Status	Enforcement Profiles	Request Timestamp
1.	192.168.1.95	RADIUS	cpuser	CX MAC Auth	ACCEPT	Wired-CX-MAC-Auth Guest, CX Return-Endpoint-Username	2023/01/06 15:58:44
2.	192.168.1.95	WEBAUTH	cpuser	CX GuestWebAuth	ACCEPT	CX-GuestMAC-Caching, CX MAC Caching Expire Post Login, [Update Endpoint Known], [AOS-CX - Bounce Switch Port]	2023/01/06 15:58:11

Session #2

Summary | Input | Output

Login Status:	ACCEPT
Session Identifier:	W00000003-01-63b7aa63
Date and Time:	Jan 06, 2023 15:58:11 AEDT
End-Host Identifier:	28-D2-44-52-C2-38
Username:	cpuser
Access Device IP/Port:	-
Access Device Name:	-
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	CX GuestWebAuth
Authentication Method:	Not applicable
Authentication Source:	[Guest User Repository]
Authorization Source:	[Guest User Repository], [Endpoints Repository], [Time Source]
Roles:	[Guest], [User Authenticated]
Enforcement Profiles:	CX-GuestMAC-Caching, CX MAC Caching Expire Post Login, [Update Endpoint

Summary | **Input** | Output

Username:	cpuser
End-Host Identifier:	28-D2-44-52-C2-38
Access Device IP/Port:	-

Authorization Attributes

Authorization:[Guest User Repository]:ExpireTime	2023-01-07 15:51:18
Authorization:[Guest User Repository]:RemainingExpiration	85987
Authorization:[Guest User Repository]:SponsorName	admin

Computed Attributes

Application:ClearPass:Page-Name	wired_guest
Application:WebLoginURL:ip	172.16.13.28
Application:WebLoginURL:mac	28:D2:44:52:C2:38
Application:WebLoginURL:timestamp	2304132817
Application:WebLoginURL:url	http://www.msftconnecttest.com/redirect
Authentication:Full-Username	cpuser
Authentication:Full-Username-Normalized	cpuser
Authentication:Posture	Unknown
Authentication:Source	[Guest User Repository]
Authentication:Status	User
Authentication:Username	cpuser
Authorization:Sources	[Guest User Repository], [Endpoints Repository], [Time Source]
Connection:Client-IP-Address	172.16.13.28

Summary | Input | Output

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

RADIUS Response

Endpoint:Guest Role ID	2
Endpoint:MAC-Auth Expiry	2023-01-07 15:51:18
Endpoint:Username	cpuser
Expire-Time-Update:GuestUser	0
Radius:Aruba:Aruba-Port-Bounce-Host	12
Radius:IETF:Calling-Station-Id	28-D2-44-52-C2-38
Radius:IETF:NAS-Identifier	6200-Lab
Radius:IETF:NAS-Port	1
Radius:IETF:User-Name	28d24452c238
Status-Update:Endpoint	Known

The guest user will now see on the browser, the 30 sec countdown starts. The endpoint database will be updated with guest expire time, username and status being known.

Configuration » Identity » Endpoints

Endpoints

Add
Import
Export

This page automatically lists all discovered, ingested or authenticated endpoints. An endpoint is a device that communicates back and forth with a network to which it is connected (e.g. Desktops, Laptops, Smartphones, Tablets, Servers, Workstations, Internet-of-things (IoT) devices).

Filter: MAC Address | contains | 38 | Go | Clear Filter | Show 20

#	MAC Address	Hostname	Device Category	Device OS Family	Status	Profiled
1.	28-D2-44-52-C2-38	t440s-ssd	Computer	Windows	Known	Yes

Endpoint | Attributes | Device Fingerprints

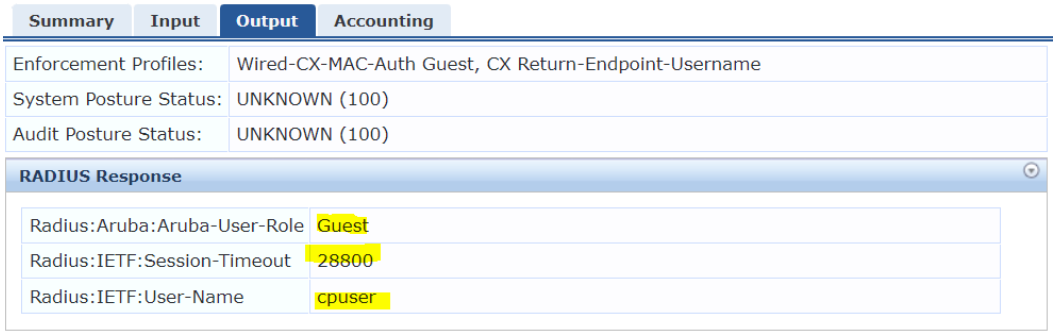
	Attribute		Value
1.	Guest Role ID	=	2
2.	MAC-Auth Expiry	=	2023-01-07 15:51:18
3.	Username	=	cpuser

Last thing that happens in Session #2 is that there will be a port bounce and then we see a RADIUS MAC auth request come in with the correct username

Summary | Input | Output | Accounting

Login Status:	ACCEPT
Session Identifier:	R00000036-01-63b7aa84
Date and Time:	Jan 06, 2023 16:03:44 AEDT
End-Host Identifier:	28-D2-44-52-C2-38 (Computer / Windows / Windows 10)
Username:	cpuser
Access Device IP/Port:	192.168.1.25:1 (CX-SW1 / Aruba)
Access Device Name:	6200-Lab
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	CX MAC Auth
Authentication Method:	MAC-AUTH
Authentication Source:	Local:localhost
Authorization Source:	[Guest User Repository], [Guest Device Repository], [Endpoints Repository], [Insight Repository], [Time Source]
Roles:	[Guest], [MAC Caching], [User Authenticated]

You should note that the role is [MAC Caching] which will indicate that our mac caching rule is working.



And we see the user role changes to Guest.

```
6200-Lab# show 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              Guest

6200-Lab# sh client ip

 MAC Address               Interface        VLAN             IP Address
 ------------------------------------------------------------------------------
 28:d2:44:52:c2:38         1/1/1            14               172.16.14.28

6200-Lab#
```

```
6200-Lab# show aaa authentication port-access interface all client-status

Port Access Client Status Details

Client 28:d2:44:52:c2:38, cpuser
================================
  Session Details
  ---------------
    Port         : 1/1/1
    Session Time : 1260s
    IPv4 Address : 172.16.14.28
    IPv6 Address :
    Device Type  :

  Authentication Details
  ----------------------
    Status          : mac-auth Authenticated
    Auth Precedence : dot1x - Unauthenticated, mac-auth - Authenticated
    Auth History    : mac-auth - Authenticated, 1249s ago
                      dot1x - Unauthenticated, Supplicant-Timeout, 1249s ago

  Authorization Details
  ---------------------
    Role   : Guest
    Status : Applied

6200-Lab#
```

Finally, the user will be redirected to the forced web page that we configured in weblogin page.

4.2 AD User with Captive Portal with MAC Auth

Now we'll test the temporary AD user using the captive portal to login. Since we are using the same laptop for this test, we'll delete its entry from the endpoint database and start new.

Here we'll use exec1 AD user. The workflow should be the same. The Captive Portal user role will be sent to the switch.

So here are the three authentication requests.

#	Server	Source	Username	Service	Login Status	Enforcement Profiles	Request Timestamp
1.	192.168.1.95	RADIUS	exec1	CX MAC Auth	ACCEPT	Wired-CX-AD-Guest, CX Return-Endpoint-Username	2023/01/06 16:23:50
2.	192.168.1.95	WEBAUTH	exec1	CX GuestWebAuth	ACCEPT	CX-AD-MAC-Caching, [AOS-CX - Bounce Switch Port]	2023/01/06 16:23:17
3.	192.168.1.95	RADIUS	28d24452c238	CX MAC Auth	ACCEPT	Wired-CX-Guest CaptivePortal	2023/01/06 16:23:05

Starting from Session #3, the first MAC auth is accepted and send the Captive-Portal user role to the switch.

Summary | Input | Output | Accounting | RADIUS CoA

Login Status:	ACCEPT
Session Identifier:	R0000003c-01-63b7b038
Date and Time:	Jan 06, 2023 16:23:05 AEDT
End-Host Identifier:	28-D2-44-52-C2-38 (Computer / Windows / Windows 10)
Username:	28d24452c238
Access Device IP/Port:	192.168.1.25:1 (CX-SW1 / Aruba)
Access Device Name:	6200-Lab
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	CX 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]

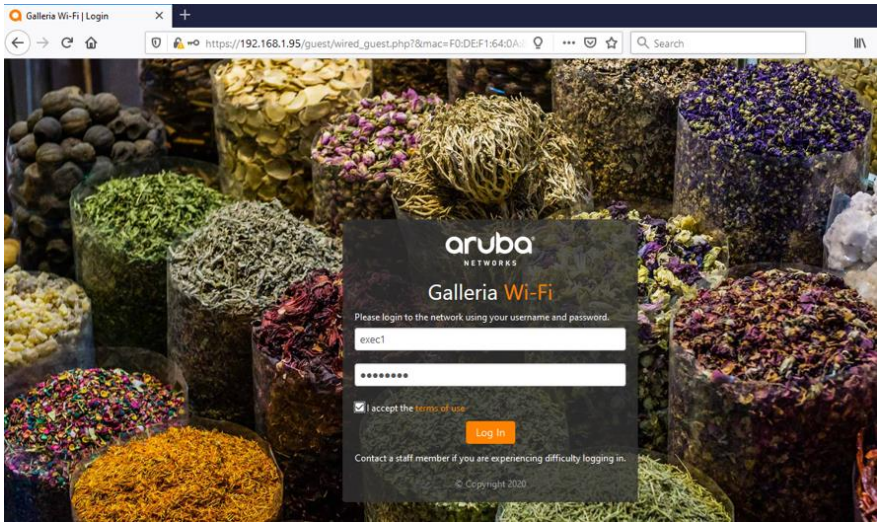
Summary	Input	Output	Accounting	RADIUS CoA

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

RADIUS Response

Radius:Aruba:Aruba-User-Role	Captive-Portal
Radius:IETF:Session-Timeout	600

The user uses exec1 credentials.



There will be a WEB-Auth request. (session #2)

Summary	Input	Output	Alerts

Login Status:	ACCEPT
Session Identifier:	W00000004-01-63b7b045
Date and Time:	Jan 06, 2023 16:23:17 AEDT
End-Host Identifier:	28-D2-44-52-C2-38
Username:	exec1
Access Device IP/Port:	-
Access Device Name:	-
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	CX GuestWebAuth
Authentication Method:	Not applicable
Authentication Source:	Lab-AD
Authorization Source:	[Endpoints Repository], [Time Source], Lab-AD
Roles:	[User Authenticated]
Enforcement Profiles:	CX-AD-MAC-Caching, [AOS-CX - Bounce Switch Port]

Summary | Input | Output | Alerts

Username:	exec1
End-Host Identifier:	28-D2-44-52-C2-38
Access Device IP/Port:	-

Authorization Attributes

Computed Attributes

Application:ClearPass:Page-Name	wired_guest
Application:WebLoginURL:ip	172.16.13.28
Application:WebLoginURL:mac	28:D2:44:52:C2:38
Application:WebLoginURL:timestamp	2304134589
Application:WebLoginURL:url	http://11.2.1.1/
Authentication:Full-Username	exec1
Authentication:Full-Username-Normalized	exec1
Authentication:Posture	Unknown
Authentication:Source	Lab-AD

Summary | Input | Output | Alerts

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

RADIUS Response

Endpoint:Guest Role ID	AD-User
Endpoint:MAC-Auth Expiry	2023-01-07 16:00:00
Endpoint:Username	exec1
Radius:Aruba:Aruba-Port-Bounce-Host	12
Radius:IETF:Calling-Station-Id	28-D2-44-52-C2-38
Radius:IETF:NAS-Identifier	6200-Lab
Radius:IETF:NAS-Port	1
Radius:IETF:User-Name	28d24452c238

Now the endpoint database entry will be slightly different. Remember that for the AD user we are adding the guest role ID and expire time of one day.

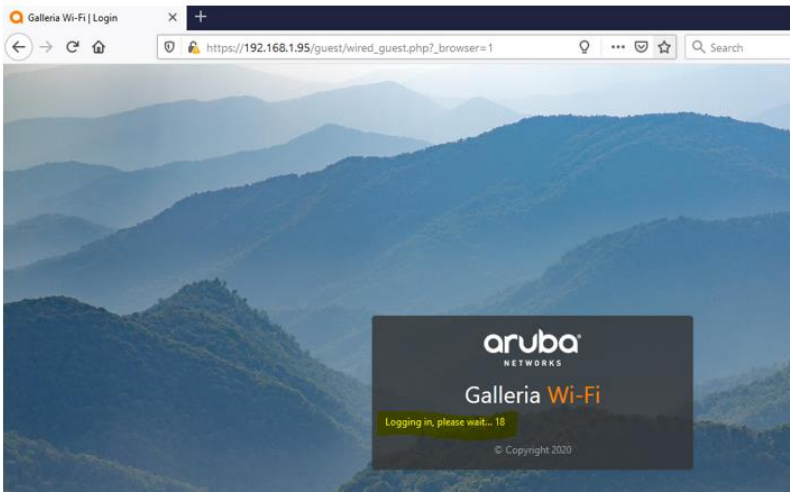
Endpoint | Attributes | Device Fingerprints

MAC Address	28-D2-44-52-C2-38	IP Address	172.16.14.28
Description		Static IP	FALSE
		Hostname	t440s-ssd
		Device Category	Computer
Status	○ Known client ◉ Unknown client ○ Disabled client	Device OS Family	Windows
		Device Name	Windows 10
MAC Vendor	LCFC(HeFei) Electronics Technology co., ltd	Added At	Jan 06, 2023 16:22:19 AEDT
Added by	Policy Manager	Profiled by	Policy Manager
Online Status	Online	Last Profiled At	Jan 06, 2023 16:23:49 AEDT
Connection Type	Wired		
Switch IP	192.168.1.25		
Switch Port	1/1/1		
School_Asset	○ Yes ◉ No		

Endpoint | Attributes | Device Fingerprints | Policy Cache

	Attribute		Value
1.	Guest Role ID	=	AD-User
2.	MAC-Auth Expiry	=	2023-01-07 16:00:00
3.	Username	=	exec1
4.	*Click to add...*		

There will be a port bounce.



The final MAC auth request comes in. (session #1)

Summary	Input	Output	Accounting

Login Status:	ACCEPT
Session Identifier:	R0000003d-01-63b7b066
Date and Time:	Jan 06, 2023 16:23:50 AEDT
End-Host Identifier:	28-D2-44-52-C2-38 (Computer / Windows / Windows 10)
Username:	exec1
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 MAC Auth
Authentication Method:	MAC-AUTH
Authentication Source:	None
Authorization Source:	[Guest User Repository], [Guest Device Repository], [Endpoints Repository], [Insight Repository], [Time Source]
Roles:	[MAC Caching], [User Authenticated]

Summary	Input	Output	Accounting

Enforcement Profiles:	Wired-CX-AD-Guest, CX Return-Endpoint-Username
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response	
Radius:Aruba:Aruba-User-Role	AD-Guest
Radius:IETF:Session-Timeout	28800
Radius:IETF:User-Name	exec1

Now on the CX switch we check a few things.

```
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              AD-Guest

6200-Lab# sh client ip

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

6200-Lab#
```

```
6200-Lab# show aaa authentication port-access interface all client-status

Port Access Client Status Details

Client 28:d2:44:52:c2:38, exec1
==============================
  Session Details
  ---------------
    Port         : 1/1/1
    Session Time : 595s
    IPv4 Address : 172.16.11.28
    IPv6 Address :
    Device Type  :

  Authentication Details
  ----------------------
    Status          : mac-auth Authenticated
    Auth Precedence : dot1x - Unauthenticated, mac-auth - Authenticated
    Auth History    : mac-auth - Authenticated, 584s ago
                      dot1x - Unauthenticated, Supplicant-Timeout, 585s ago

  Authorization Details
  ---------------------
    Role   : AD-Guest
    Status : Applied

6200-Lab#
```