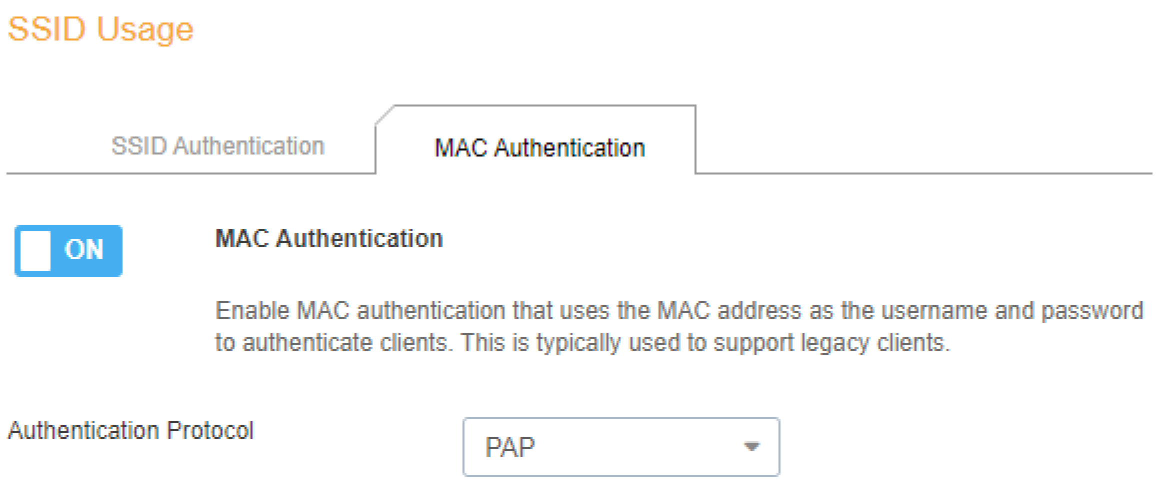
Create a new Network Policy in EIQ.
Create a new SSID with Open as the Auth-Type. (Or Preferred)

Enable MAC-Auth



SSID Usage

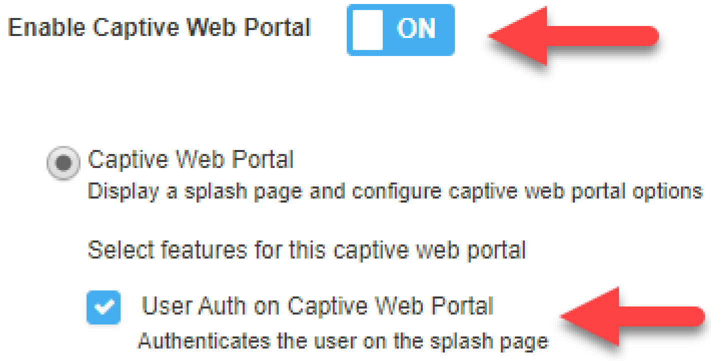
SSID Authentication | MAC Authentication

ON **MAC Authentication**

Enable MAC authentication that uses the MAC address as the username and password to authenticate clients. This is typically used to support legacy clients.

Authentication Protocol: PAP

Enable CWP.



Enable Captive Web Portal ON

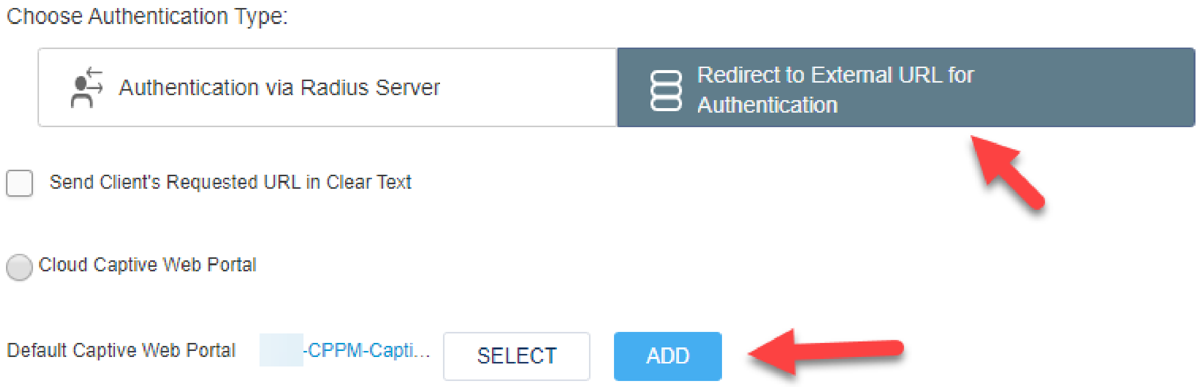
● Captive Web Portal
Display a splash page and configure captive web portal options

Select features for this captive web portal

☑ User Auth on Captive Web Portal
Authenticates the user on the splash page

Set CWP Authentication type as "Redirect to External URL for Authentication"

Click "Add" to create a new CWP profile.



Choose Authentication Type:

Authentication via Radius Server | Redirect to External URL for Authentication

☐ Send Client's Requested URL in Clear Text

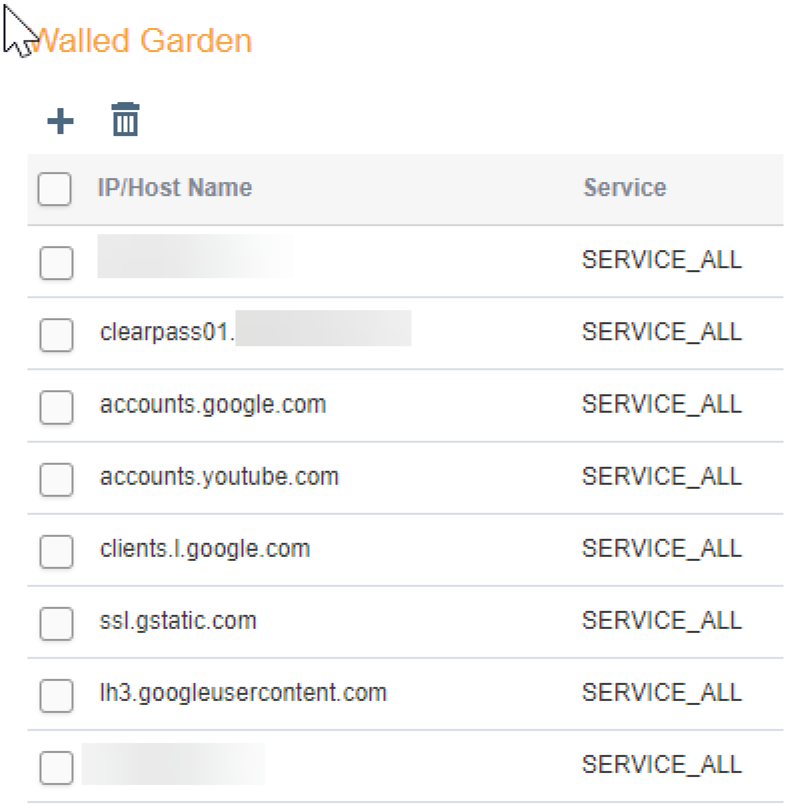
○ Cloud Captive Web Portal

Default Captive Web Portal -CPPM-Capti... SELECT ADD

For the Login URL input the CPPM URL for the Web Login page. Ie. https://clearpass.domain.com/guest/webLogin.php

Password Encryption: None
Authentication Method: PAP
Success/Failure Pages: On/Off. (Customer Preference)

Walled Garden:
*NOTE: These are the servers that the client needs access to for a successful authentication when in the "Pre-Auth" state. Ie. Clearpass. So add your Clearpass server(s) here. If you're using Social logins, as in this example, you need to add the relevant servers for Google authentication as well. In this scenario, we're using Gsuite. So, I've added those servers to the list. You can find a list with most providers from the Aruba Github. Link
**NOTE: SERVICE_ALL is not required, and should be locked down to what is required. WEB only is probably preferred.

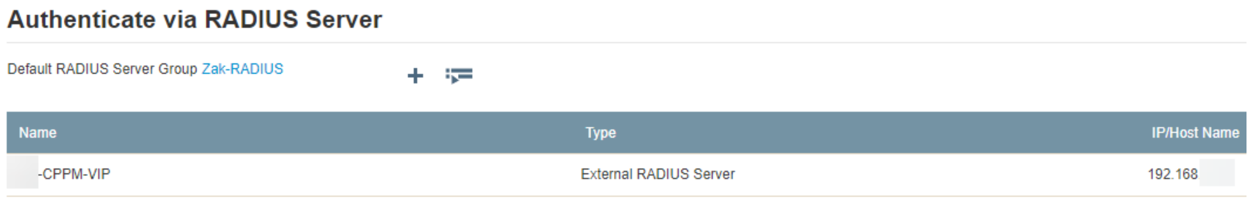


Walled Garden

☐	IP/Host Name	Service
☐	[redacted]	SERVICE_ALL
☐	clearpass01.[redacted]	SERVICE_ALL
☐	accounts.google.com	SERVICE_ALL
☐	accounts.youtube.com	SERVICE_ALL
☐	clients.l.google.com	SERVICE_ALL
☐	ssl.gstatic.com	SERVICE_ALL
☐	lh3.googleusercontent.com	SERVICE_ALL
☐	[redacted]	SERVICE_ALL

Save.

Add your Clearpass server(s) as RADIUS server(s).



Authenticate via RADIUS Server

Default RADIUS Server Group Zak-RADIUS

Name	Type	IP/Host Name
[redacted]-CPPM-VIP	External RADIUS Server	192.168[redacted]

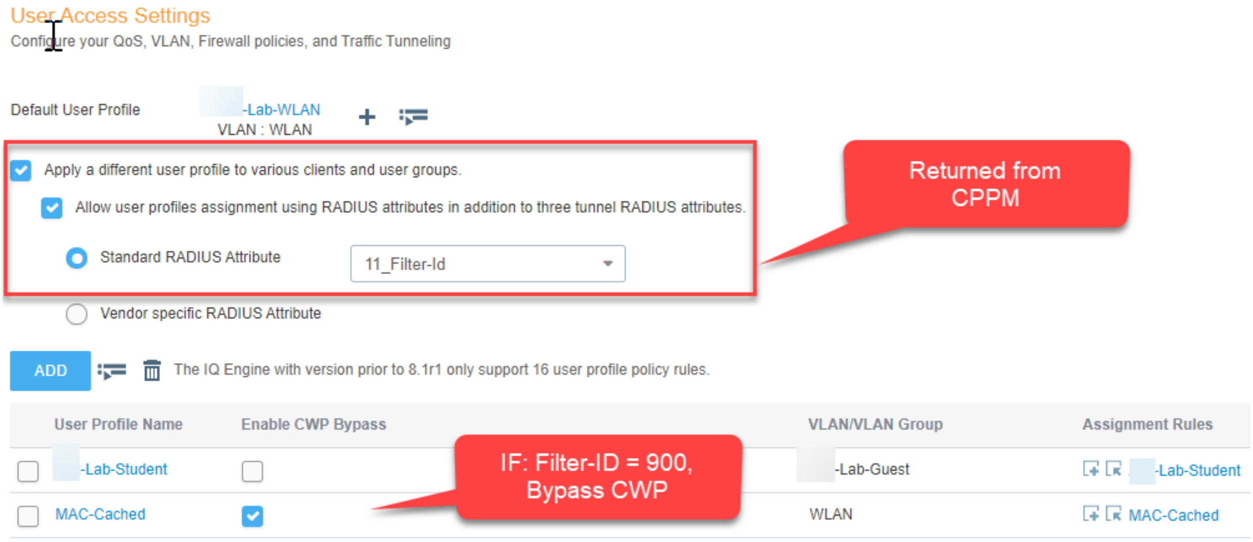
Next is perhaps the most important part. You need to define your User Profiles for different VLANs and permissions. This will also determine what to do with MAC-Cached clients.
Below I have define two user profiles. One is for MAC-Cached users, the other is for non-MAC-Cached users.

I setup two rules based on the RADIUS attribute Filter-ID to determine when a user receives either UP 1 or UP 2.

IF: CPPM returns Filter-Id 900, the user is considered MAC-Cached, and bypasses the Captive Portal. (VLAN 2)

- Filter-Id is returned by the corresponding CPPM service handling MAC-Auth from EIQ. (The user is MAC-Cached)

IF: CPPM returns Filter-Id 2, the user is considered new/expired and is required to login again. (VLAN 2)



User Access Settings

Configure your QoS, VLAN, Firewall policies, and Traffic Tunneling

Default User Profile [redacted]-Lab-WLAN
VLAN : WLAN

☑ Apply a different user profile to various clients and user groups.

☑ Allow user profiles assignment using RADIUS attributes in addition to three tunnel RADIUS attributes.

● Standard RADIUS Attribute: 11_Filter-Id

○ Vendor specific RADIUS Attribute

Returned from CPPM

ADD

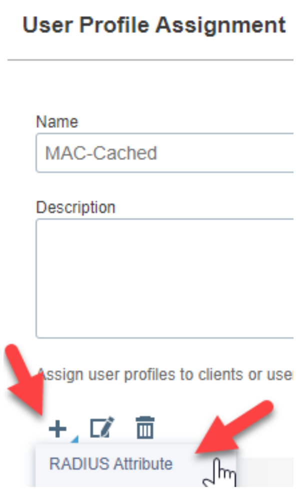
The IQ Engine with version prior to 8.1r1 only support 16 user profile policy rules.

	User Profile Name	Enable CWP Bypass	VLAN/VLAN Group	Assignment Rules
□	[redacted]-Lab-Student	□	[redacted]-Lab-Guest	[redacted]-Lab-Student
□	MAC-Cached	☑	WLAN	MAC-Cached

IF: Filter-ID = 900, Bypass CWP

*NOTE: Make sure you tick the "Enable CWP Bypass" checkbox.

Creating the User Profile Assignment rules.

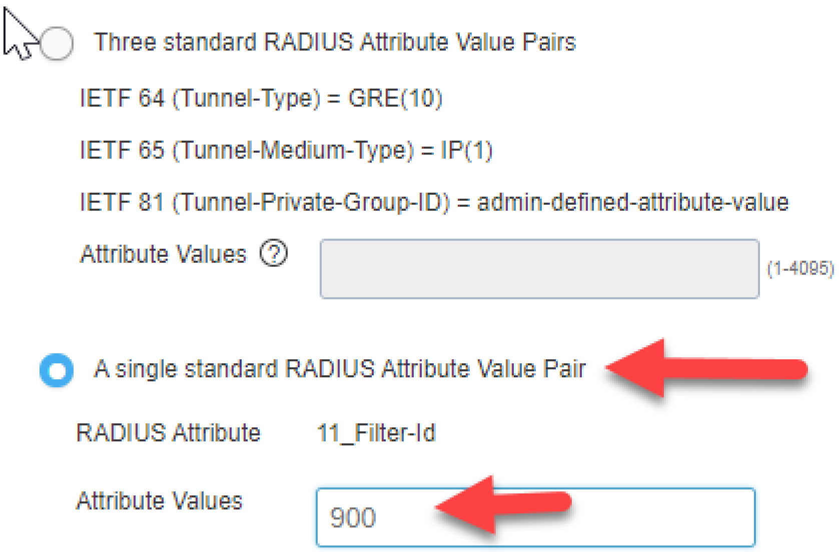


User Profile Assignment

Name: MAC-Cached

Description:

Assign user profiles to clients or use



○ Three standard RADIUS Attribute Value Pairs

IETF 64 (Tunnel-Type) = GRE(10)

IETF 65 (Tunnel-Medium-Type) = IP(1)

IETF 81 (Tunnel-Private-Group-ID) = admin-defined-attribute-value

Attribute Values: (1-4095)

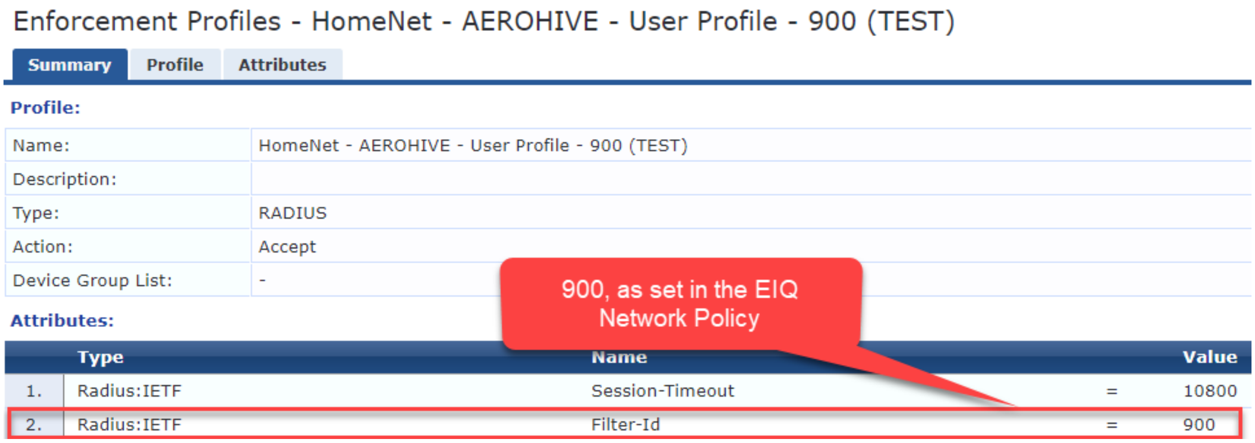
● A single standard RADIUS Attribute Value Pair

RADIUS Attribute: 11_Filter-Id

Attribute Values: 900

This tells the AP that if CPPM returns a RADIUS:IETF Filter-ID = 900. Then assign this User Profile, which bypasses the Captive Portal. (MAC-Cache)

I won't go into the configuration too deep on the Clearpass side since MAC-Caching is well-documented. You should have two services as typical. One for User Authentication, and one for MAC Authentication. Here is the profile that needs to be passed back in your MAC-AUTH policy to allow MAC-Caching.



Enforcement Profiles - HomeNet - AEROHIVE - User Profile - 900 (TEST)

Profile:

Name:	HomeNet - AEROHIVE - User Profile - 900 (TEST)
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:IETF	Session-Timeout	=	10800
2.	Radius:IETF	Filter-Id	=	900

900, as set in the EIQ Network Policy

*NOTE: If you pass back any attributes that do not assign an User Profile that has CWP Bypass enabled, then the user will get the Captive Portal. This is regardless of VLAN, firewall settings, etc.

**NOTE: NAS Vendor settings seem to be debated on how to configure. I have seen many articles explaining how to set this manually (in the CWP settings under Advanced Configuration -> Network Settings -> Customize), but it seems dependent on firmware version. In my lab with one AP running firmware 8.4r7, the correct IP for NAS-IP is: 198.18.34.1 (RFC 5735). This would be set in your NAS Vendor Settings of the Web Login configuration in Clearpass Guest. I have not had a chance to test this at scale, however. I was able to find this IP based on the redirection URL upon connecting to the SSID.

***NOTE: I have disabled HTTPS authentication in the Web Login page settings. To provide maximum security this should probably be configured. However, I have not tested this workflow.