1 Table of Contents

1 Table of Contents 1
1.1 Revision History 1
2 Dynamic Segmentation for HPE Mist AP with ClearPass 2
2.1 Things you need 2
3 Mist AP Configuration 3
3.1 RF and WLAN Templates 3
3.2 User Labels 7
3.3 WxLAN Policy 8
4 ClearPass Configuration 10
4.1 NAD configuration 10
4.2 RADIUS Dictionaries 10
4.3 ClearPass Service 11
4.4 RADIUS Enforcement Profiles 13
4.5 Enforcement Profile for CoA 14
4.6 ClearPass Guest 15
5 Verification and Testing 17
5.1 HPE Mist Dashboard 17
5.2 ClearPass Access Tracker 19
5.3 Customised Captive Portal Redirect 21

1.1 Revision History

DATE	VERSION	EDITOR	CHANGES
09 Nov 2026	0.1	Ariya Parsamanesh	Initial creation
19 Nov 2026	0.2	Ariya Parsamanesh	Added the validation section

2 Dynamic Segmentation with HPE Mist AP and ClearPass

Many organisations already use ClearPass as their centralised authentication and policy platform across their wired and wireless networks. This TechNote demonstrates how organisations deploying Mist APs can continue to use ClearPass for **802.1X authentication, policy enforcement, and dynamic network segmentation**, extending their existing ClearPass policies and operational model into the Mist wireless environment.

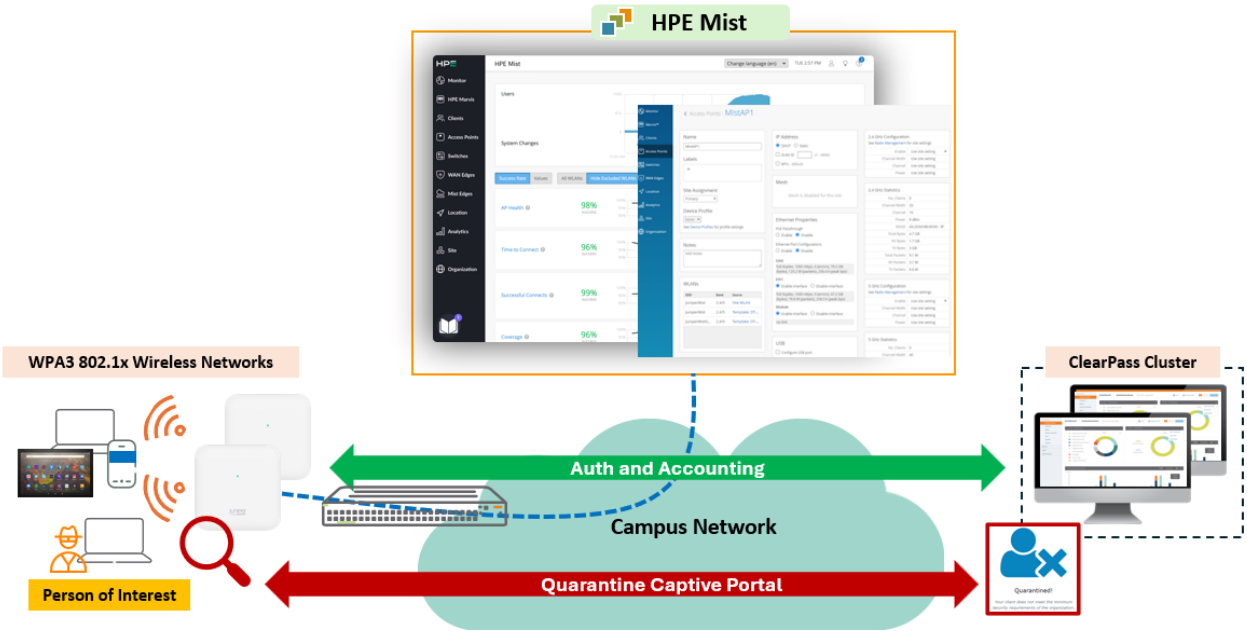
The solution uses 802.1X to authenticate wireless users. ClearPass makes the policy decision and returns RADIUS attributes that place each user in the right VLAN. It will return Aruba-User-Role vendor-specific attribute (VSA), which lets us apply granular resource restrictions. Along the way, I'll show how HPE Mist's WxLAN policies can replace legacy ACLs and firewall rules with something much simpler to manage.

This allows a single WLAN to support different users and access requirements while ClearPass centrally determines the level of network access each authenticated session should receive.

The TechNote then shows dynamic authorization using RADIUS Change of Authorization (CoA), including how administrators can trigger a CoA directly from Access Tracker.

Finally, it demonstrates a use case to identify people of interest when they connect and automatically quarantines them with a redirection to a customised captive portal.

These use cases rest on one idea: authentication is only the start of the access-control lifecycle. A user's access may need to change after they've connected. RADIUS Change of Authorisation (CoA) lets ClearPass modify an active session on the fly, which is what makes quarantine, remediation and other changes in access possible.



This TechNote is also the starting point for a series of ClearPass and Mist integration guides, with each solution building on the capabilities introduced previously. Together, the series will demonstrate how ClearPass can provide more than authentication for HPE Mist wireless networks.

2.1 Things you need

- Mist AP that are already claimed and visible in HPE Mist platform
- Operational DHCP/DNS services and LAN switch to provide Poe for the AP
- LAN switch configured for minimum of 4x VLANs
- ClearPass version 6.11.16 with operational Active Directory integration.

3 Mist AP Configuration

Before I start the configuration, here's the plan. The table below shows each VLAN, the AD user group that maps to it, the Aruba-User-Role VSA that ClearPass returns after a successful authentication, and the matching HPE Mist label.

VLAN Id	Description VLAN	IP Subnet	AD user group	ClearPass VSA Aruba-User-Role	HPE Mist Labels
30	Mgmt. for AP	10.10.30.0/24	N/A	N/A	N/A
11	Staff	10.10.11.0/24	Staff	Staff	Staff
12	Student	10.10.12.0/24	Student	Student	Student
12	Contractor	10.10.12.0/24	Contractor	Contractor	Contractor
13	Quarantine	10.10.13.0/24	N/A	q-redirect	Quarantine

Based on the above VLAN information, I am assuming that the LAN switch (I am using a CX 6200 switch) is configured with the needed VLANs for various user groups. For completeness, below is my LAN switch configuration that shows the AP port is a trunk with native VLAN 30 (AP management) and that the user VLANs are tagged.

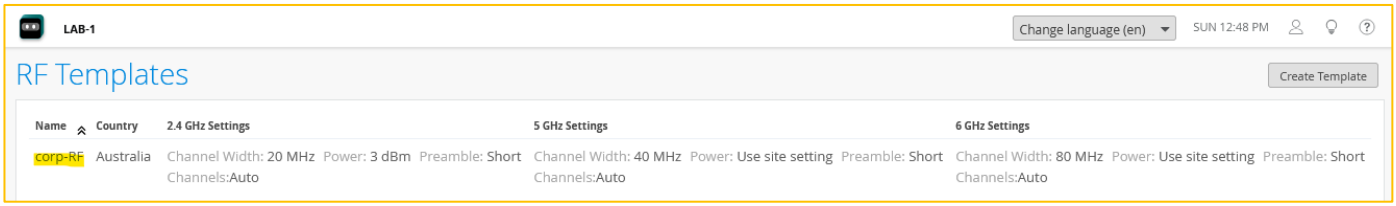
```
Access switch# sh run int 1/1/3
interface 1/1/3
    description HPE Mist AP
    no shutdown
    no routing
    vlan trunk native 30
    vlan trunk allowed 10-13,30
    exit

Access switch#
```

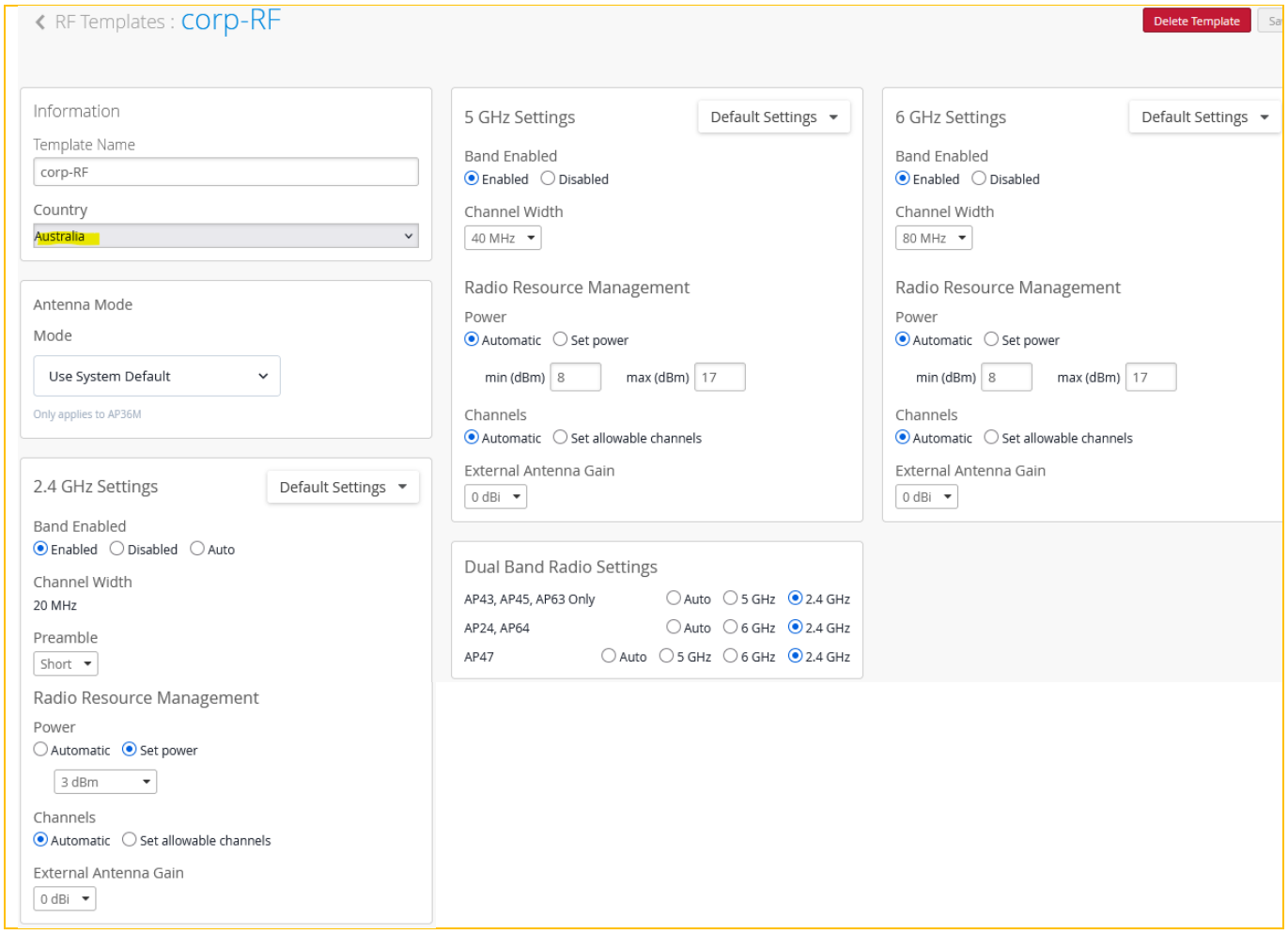
3.1 RF and WLAN Templates

I'm starting the HPE Mist configuration with an RF template at the global level, so every AP in my account gets the same radio settings. An RF template is a reusable set of radio configuration settings that you can apply across an organisation, a site or a group of APs, which keeps things consistent as you scale.

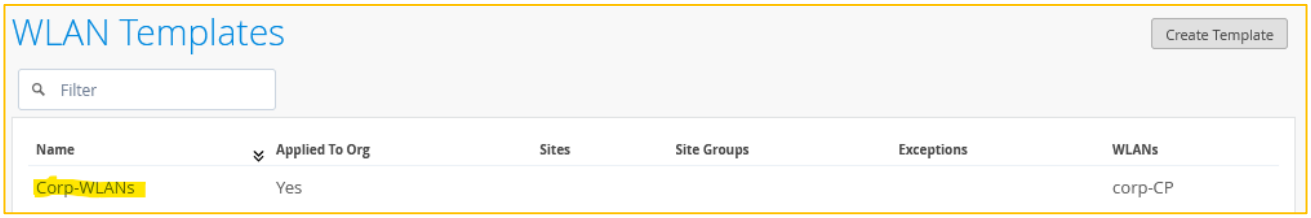
Navigate to Organisation » RF Template and create a new template. Here's mine.



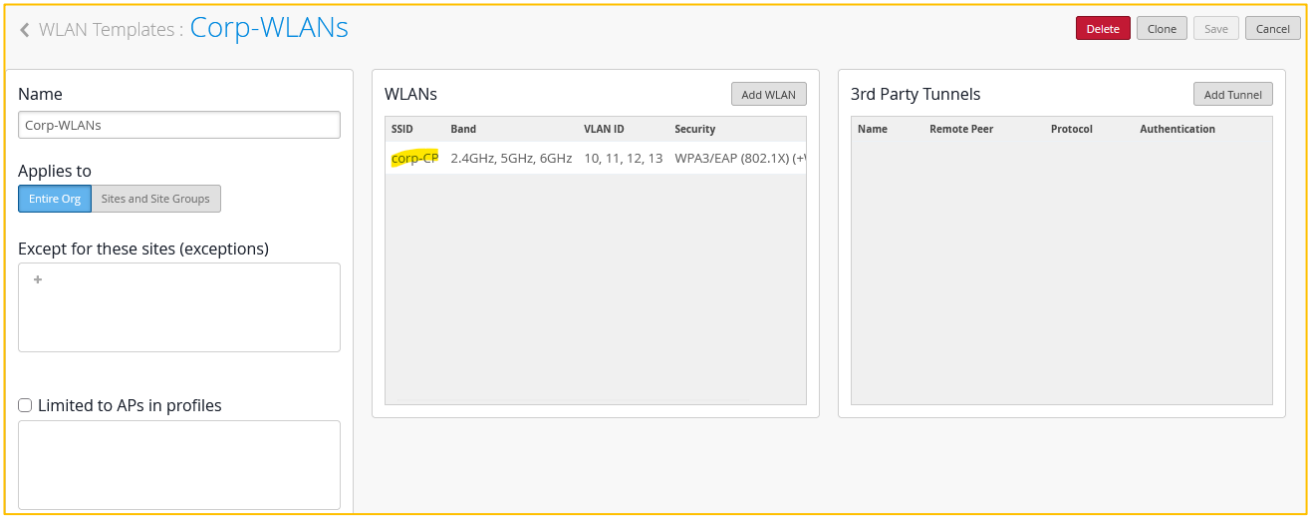
Clicking on "corp-RF" shows the details. I've left everything at its default except two things: the country is set to Australia, which sets the regulatory domain, and I've lowered the 2.4 GHz transmit power under Radio Resource Management because this is a lab.



Next, we'll configure the WLAN by creating our first WLAN template. Navigate to Organisation » WLAN Template and create a new one. I've already created a template called Corp-WLANs, which contains a single WLAN.



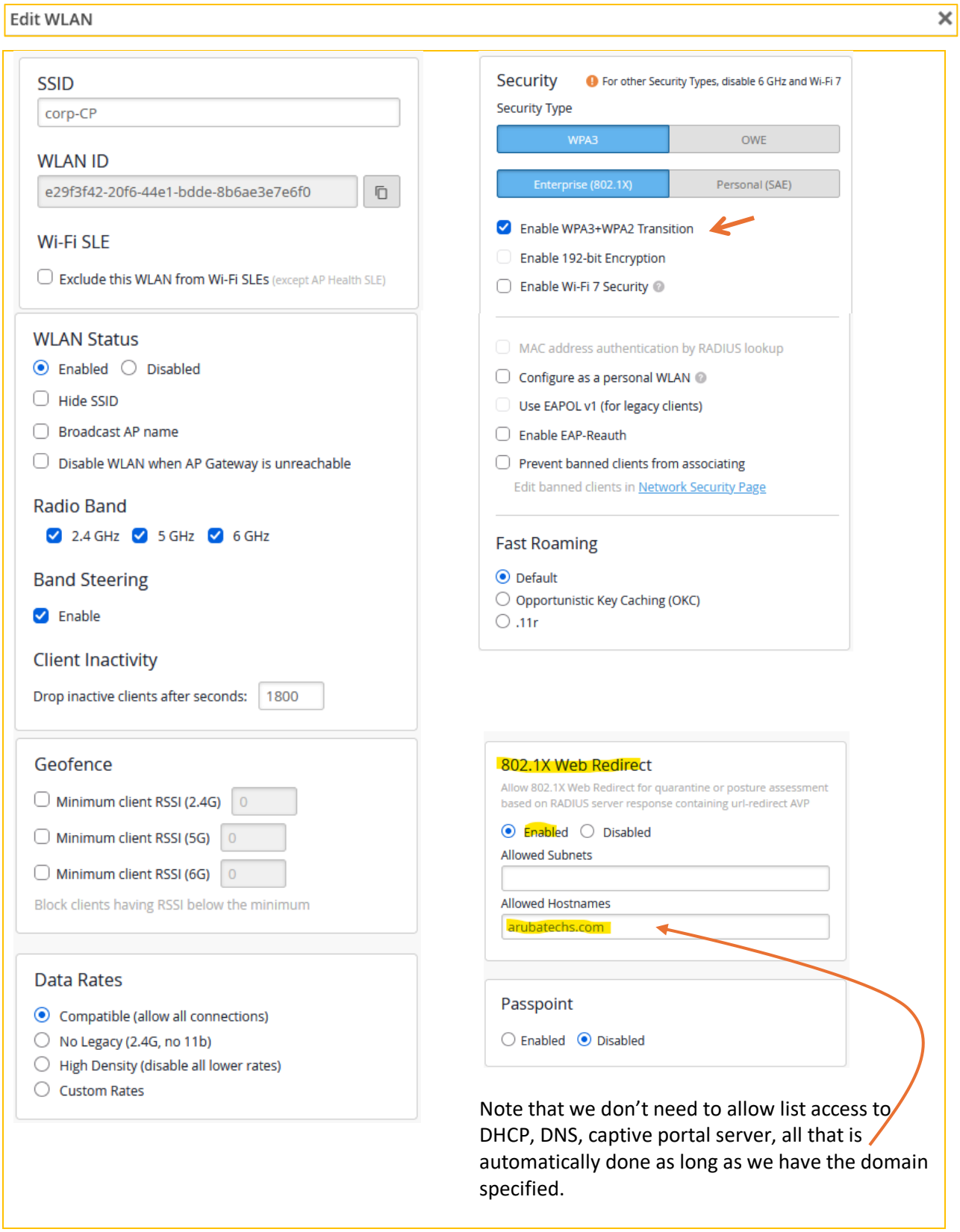
After clicking on the name of the template, you should see the WLANs that are configured, and you can add new WLANs by clicking on the "Add WLAN" button.

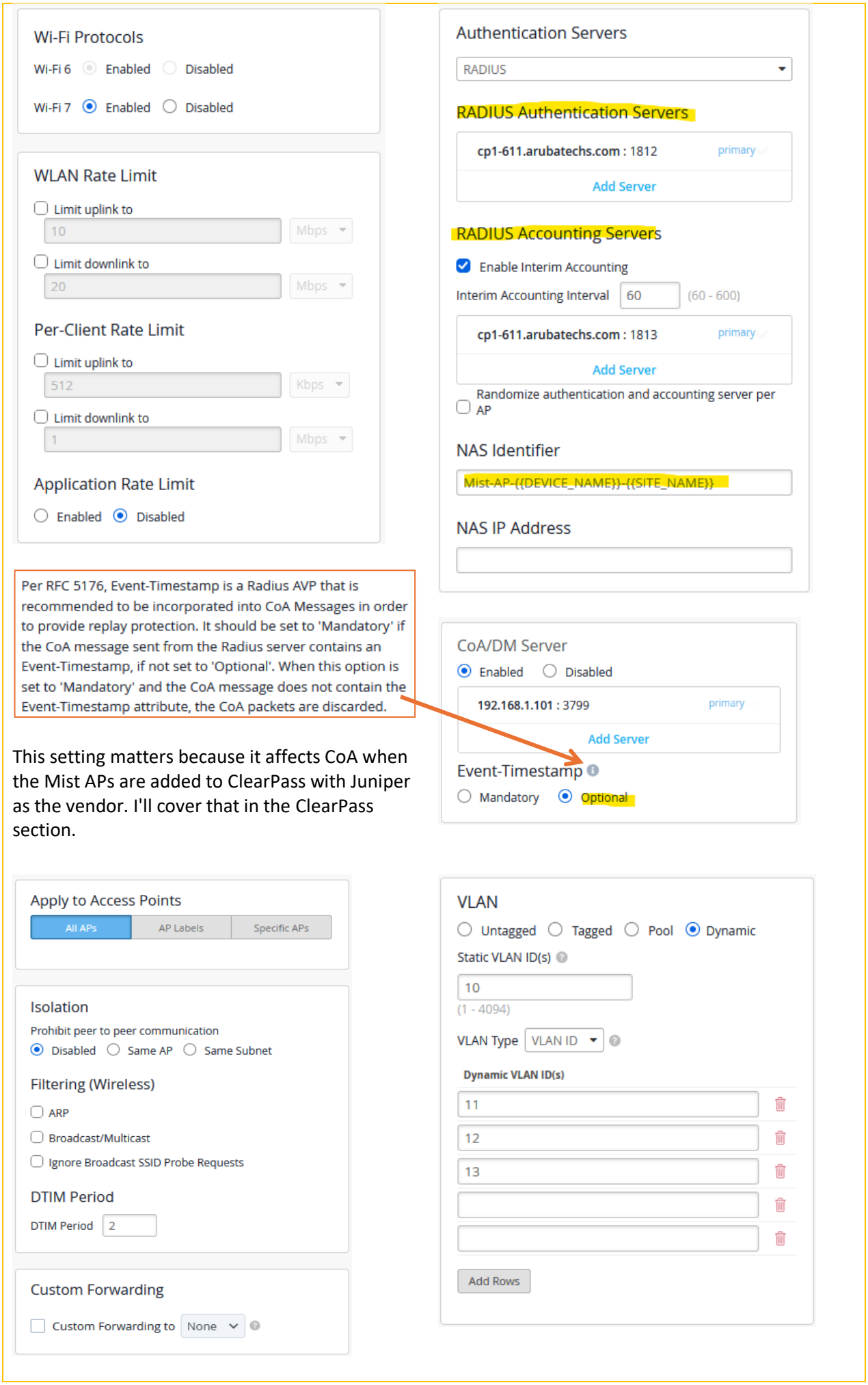


I've already configured a WLAN called "corp-CP". Here are the settings for 802.1X authentication with ClearPass as the policy manager. I've highlighted two areas. The first is security: I'm using WPA3 for 802.1X, in transition mode so that devices without WPA3 support can still connect.

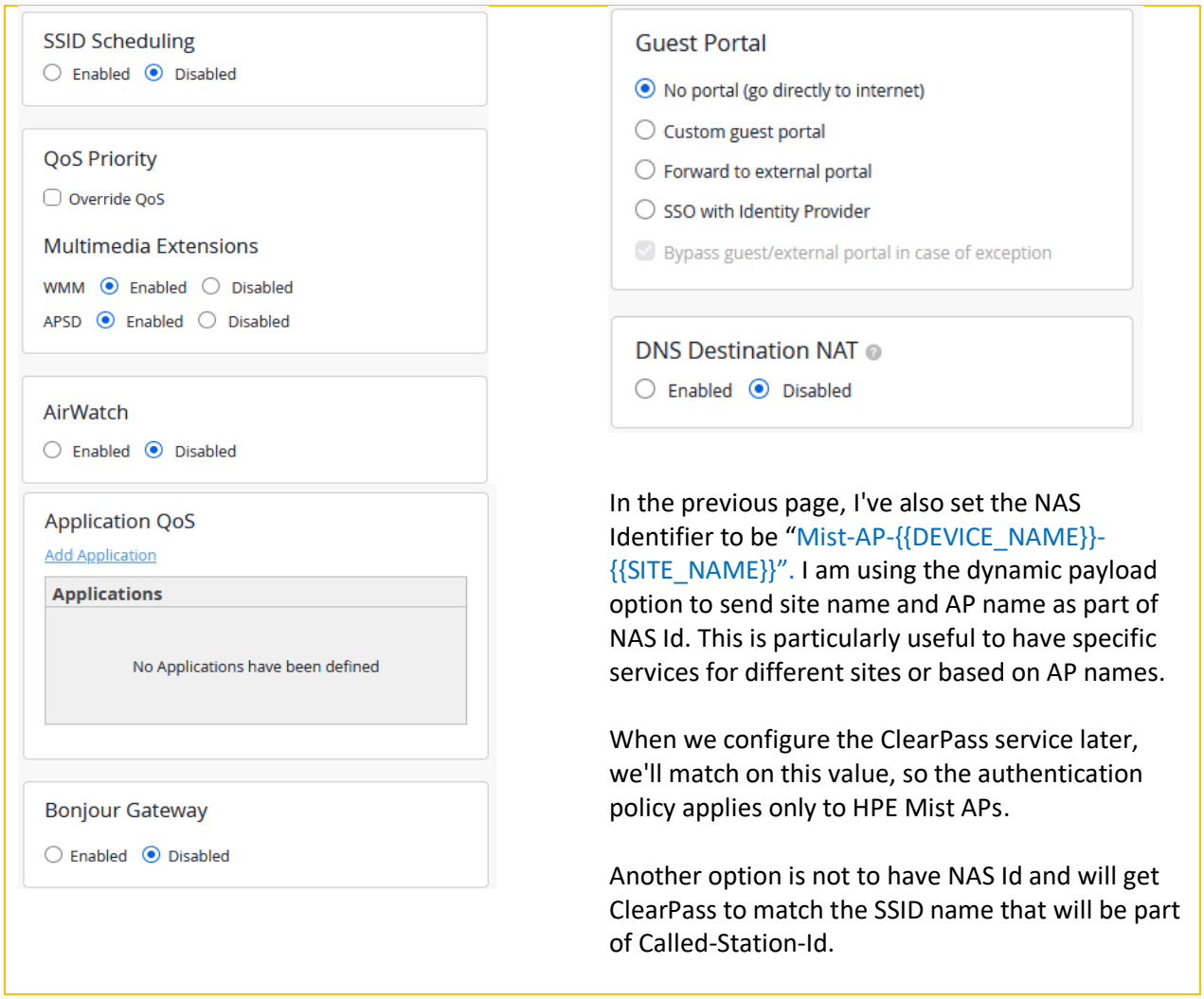
The second area is the 802.1X Web Redirect feature, which redirects the client based on a url-redirect AAA attribute in the RADIUS server's response.

When a client authenticates via 802.1X, ClearPass can return an ACCESS-ACCEPT message with a url-redirect attribute. This places the client into a limited, quarantined state where their network traffic is restricted.





This setting matters because it affects CoA when the Mist APs are added to ClearPass with Juniper as the vendor. I'll cover that in the ClearPass section.

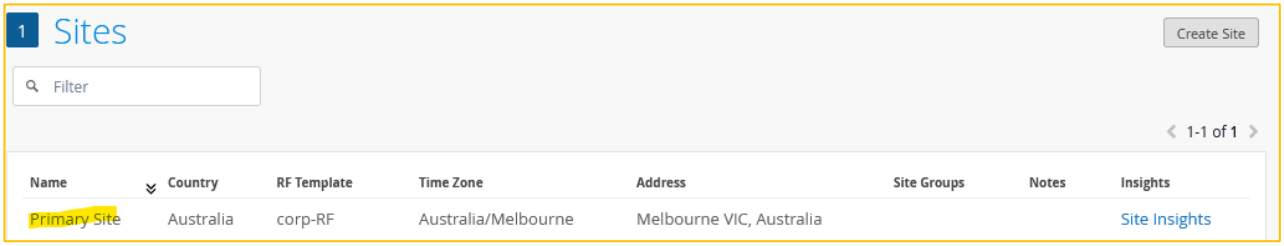


In the previous page, I've also set the NAS Identifier to be "Mist-AP-{{DEVICE_NAME}}-{{SITE_NAME}}". I am using the dynamic payload option to send site name and AP name as part of NAS Id. This is particularly useful to have specific services for different sites or based on AP names.

When we configure the ClearPass service later, we'll match on this value, so the authentication policy applies only to HPE Mist APs.

Another option is not to have NAS Id and will get ClearPass to match the SSID name that will be part of Called-Station-Id.

Now that RF and WLAN templates configuration is done and before we go to the next section, we need to assign the RF template to our site, by navigating to Organisation » Site Configuration and add your site.

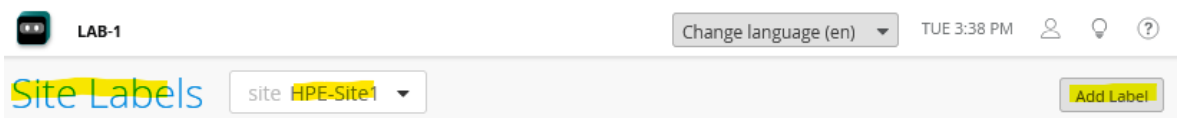


Here is the place where in addition to assigning the RF template, you can have per site setting for AP firmware policy, webhooks, site variables, Marvis mini behaviours, location services, etc. I will rename the site to HPE-Site1 by clicking on the site name.

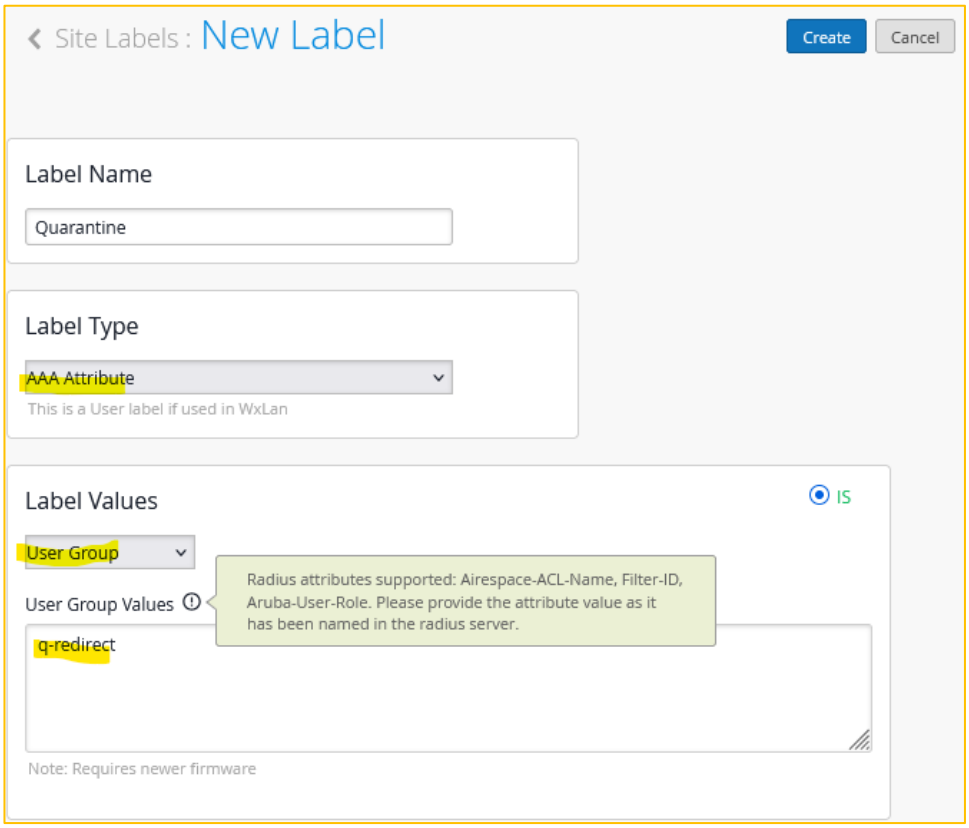
3.2 User Labels

To build access policies for the wireless network, we first need to create labels. HPE Mist uses labels to group and identify users and resources, and you can then use them in a WxLAN policy to allow or deny access.

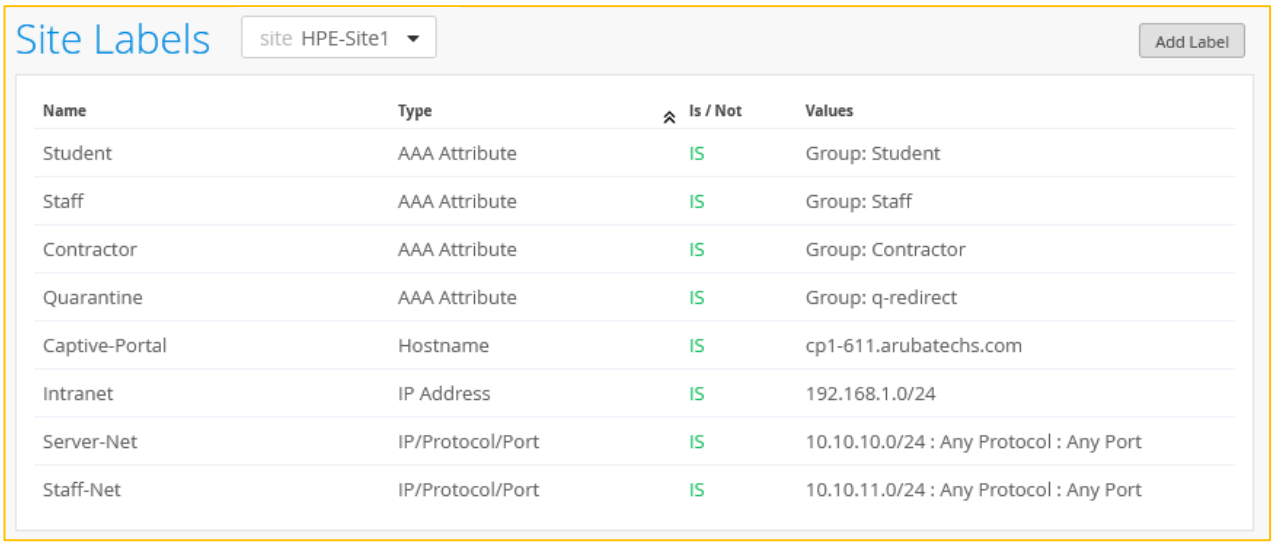
You can create your labels both at organisation and site levels. Here I am creating it at site level and starting with AAA attribute label type. Navigate to Site » Wireless » Labels



I'm creating a label called "Quarantine", which, as the name suggests, I'll use to quarantine users and devices. The label type is AAA attribute, meaning the value comes back from ClearPass. For this type you can match on either Radius Username or User Group. I'm using User Group.



The key point is that HPE Mist understands several vendor-specific RADIUS attributes. The one we care about is Aruba-User-Role. ClearPass will send the value q-redirect, and the label value here must match it exactly. Here are the other labels I created for the WxLAN policy. It is important if you are already using enforcement profiles with Aruba-User-Role, this was you can reuse them here as well.



Name	Type	Is / Not	Values
Student	AAA Attribute	IS	Group: Student
Staff	AAA Attribute	IS	Group: Staff
Contractor	AAA Attribute	IS	Group: Contractor
Quarantine	AAA Attribute	IS	Group: q-redirect
Captive-Portal	Hostname	IS	cp1-611.arubatechs.com
Intranet	IP Address	IS	192.168.1.0/24
Server-Net	IP/Protocol/Port	IS	10.10.10.0/24 : Any Protocol : Any Port
Staff-Net	IP/Protocol/Port	IS	10.10.11.0/24 : Any Protocol : Any Port

3.3 WxLAN Policy

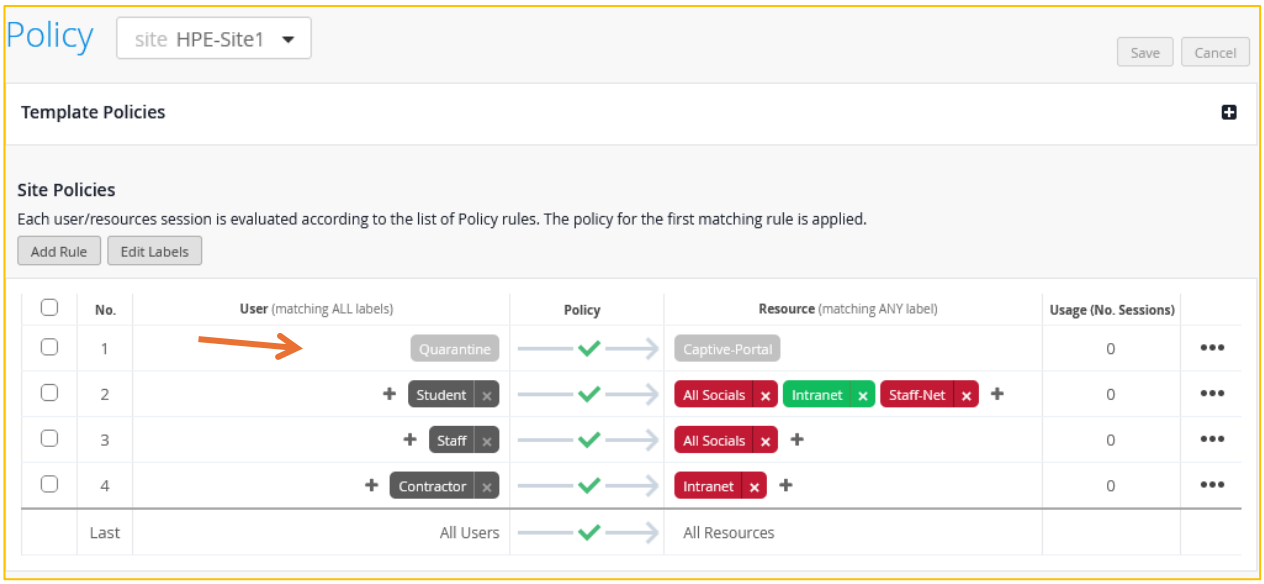
WxLAN policies control what wireless clients can access, and you can configure them in three places, depending on your use case:

1. Organisation level for a specific WLAN template – here you can choose to apply the policy to the entire organisation or select number of Sites or Site Groups. Organization » Wireless » WLAN Templates » <name of your template> (under Policies)

   Once a user is authenticated and, on the network, the WxLAN policy dictates what internal resources, subnets, or external applications they are allowed or denied access to

2. Site level for specific sites by navigating to Site » Wireless » Policy
3. Organisation level » Access » Auth Policies – used generally when you have Mist Access Assurance subscriptions

I'm configuring the policy at the site level. Some resources can be added directly in a rule's "add resource" option without creating a label first. My policy is deliberately simple. For example, the “Student” label can't reach social networks or Staff-Net, but it can reach the Intranet.



The first rule is disabled, which is why it's greyed out. I left it in to show that you don't need a dedicated rule to allow list the custom captive portal. Now for each rule, operator is set to allow but you can get the resources to be either allowed or denied.

Now here are some notes on the operation of these rules.

For rules that contain only allow resources, the user can access just those resources and everything else is denied.

For rules that contain only deny resources, the user is blocked from just those resources and everything else is allowed.

This brings us to the rule that consists of few allow and few deny resources, in this case user is only allowed to access resources is allowed while everything else is denied.

If you mix organisation-level and site-level policies, the organisation-level policies are processed first. Site-level policies are evaluated only for traffic that doesn't match an organisation-level rule, and they can reference site-level labels only.

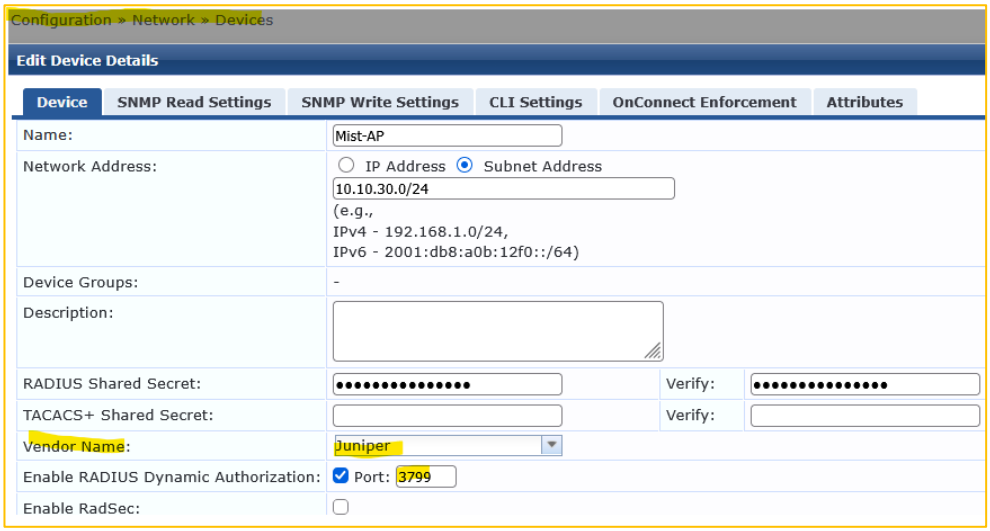
Also, you cannot use the labels created at the global level at the site levels.

4 ClearPass Configuration

This section covers the ClearPass configuration for HPE Mist APs doing 802.1X authentication. I'll walk through the RADIUS attributes we can use and build a customised captive portal for quarantined devices. I'm assuming ClearPass has already joined Active Directory and is fully operational.

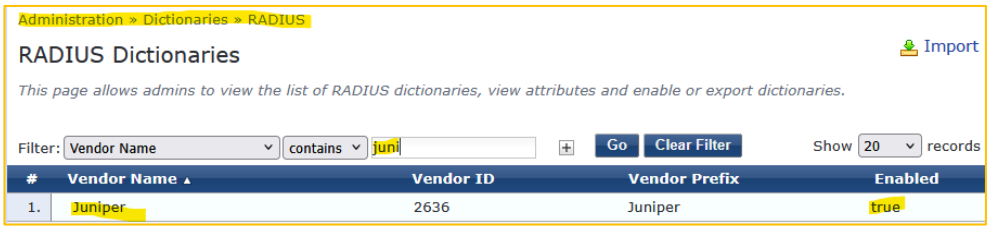
4.1 NAD configuration

First, we'll add the HPE Mist APs to ClearPass as network devices (NADs). Picking the right vendor matters here. I've selected Juniper, and the dynamic authorisation port (3799) matches what I configured in HPE Mist.

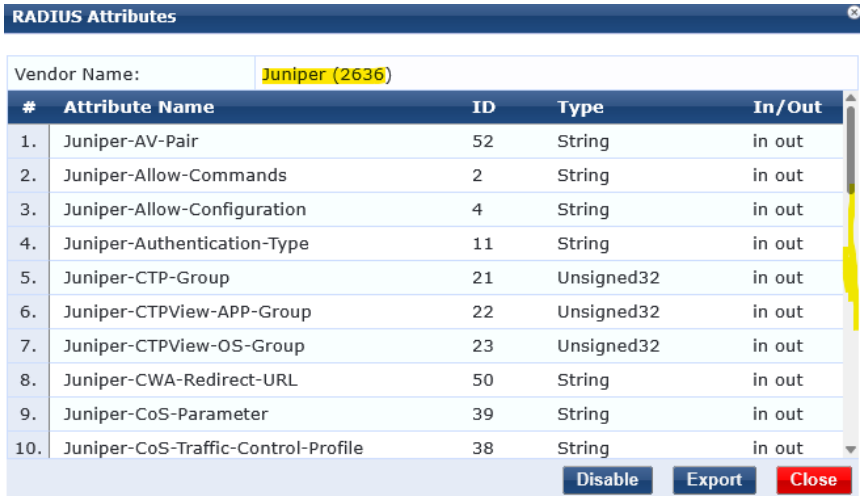


4.2 RADIUS Dictionaries

Many vendor RADIUS dictionaries are disabled by default. Go to Administration » Dictionaries » RADIUS to see them. There are over 100, so search for Juniper and make sure its dictionary is enabled.

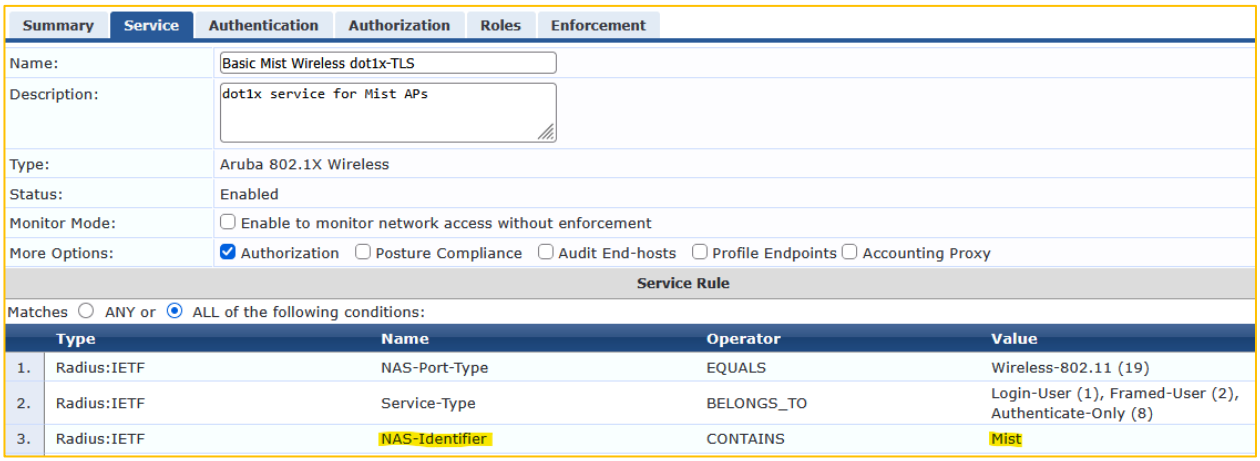


You can click on it to see the details of the attributes as well.



4.3 ClearPass Service

With the NADs added and the dictionary enabled, we can configure the service. The first job is to give it a unique match condition. Remember that we set the NAS Identifier in HPE Mist, so here we match on that value. This guarantees the service handles only wireless authentications from HPE Mist APs.



Summary | Service | Authentication | Authorization | Roles | Enforcement

Name:	Basic Mist Wireless dot1x-TLS
Description:	dot1x service for Mist APs
Type:	Aruba 802.1X Wireless
Status:	Enabled
Monitor Mode:	Enable to monitor network access without enforcement
More Options:	Authorization, Posture Compliance, Audit End-hosts, Profile Endpoints, Accounting Proxy

Service Rule

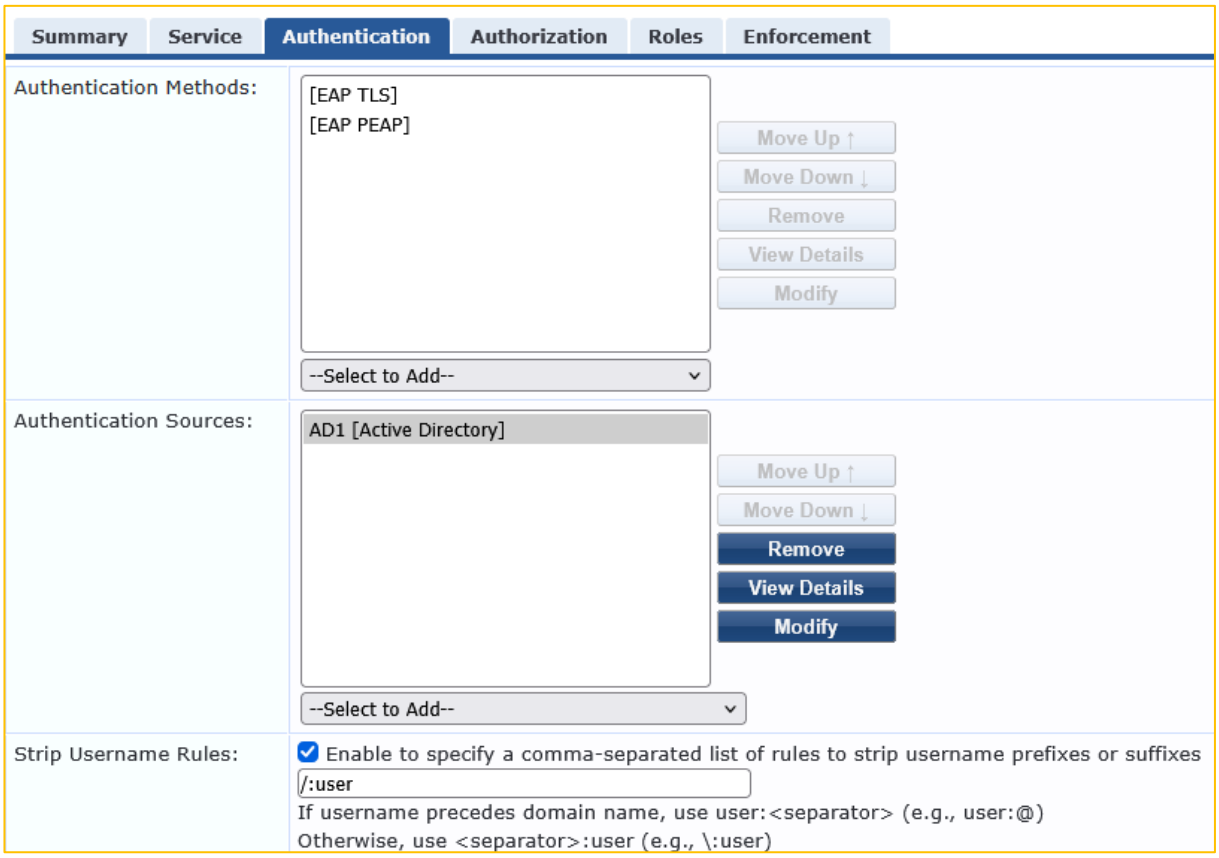
Matches ANY or ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)
3.	Radius:IETF	NAS-Identifier	CONTAINS	Mist

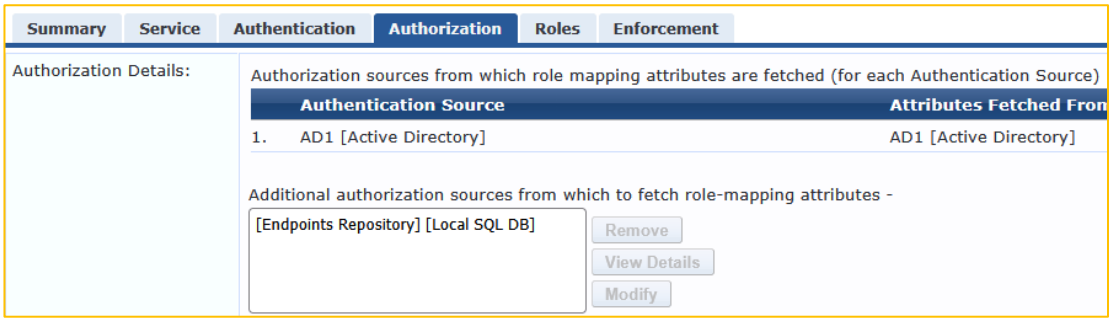
The next item is authentication methods and here for some of my devices, I am using mainly EAP-PEAP for simplicity and the fact that this is a lab setup and is completely isolated environment.

In a real deployment, avoid EAP-PEAP where you can. Clients often don't validate the server's identity properly, which leaves PEAP-MSCHAPv2 open to credential theft. Microsoft recommends moving Wi-Fi and VPN connections to certificate-based EAP-TLS, and I'd suggest starting with EAP-TLS wherever possible.

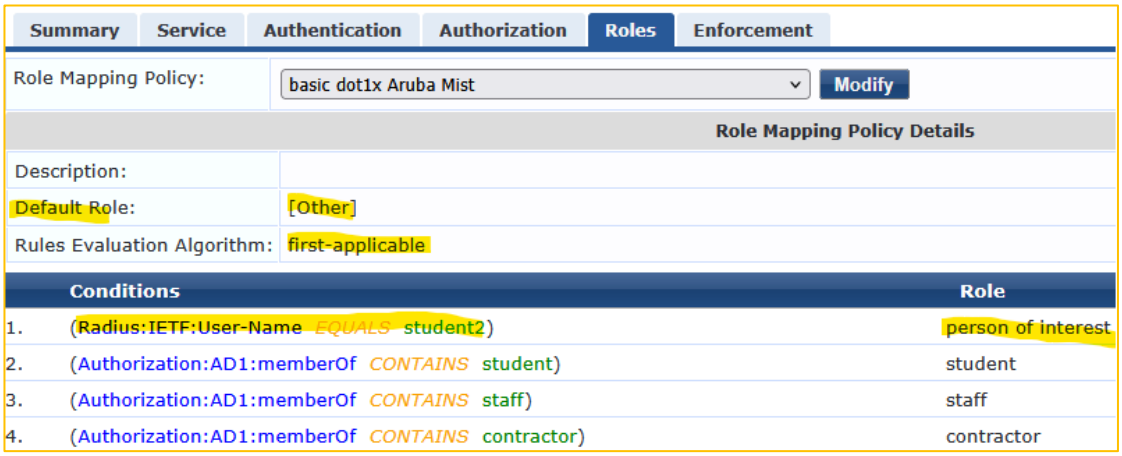
I am also using Active Directory as my authentication source.



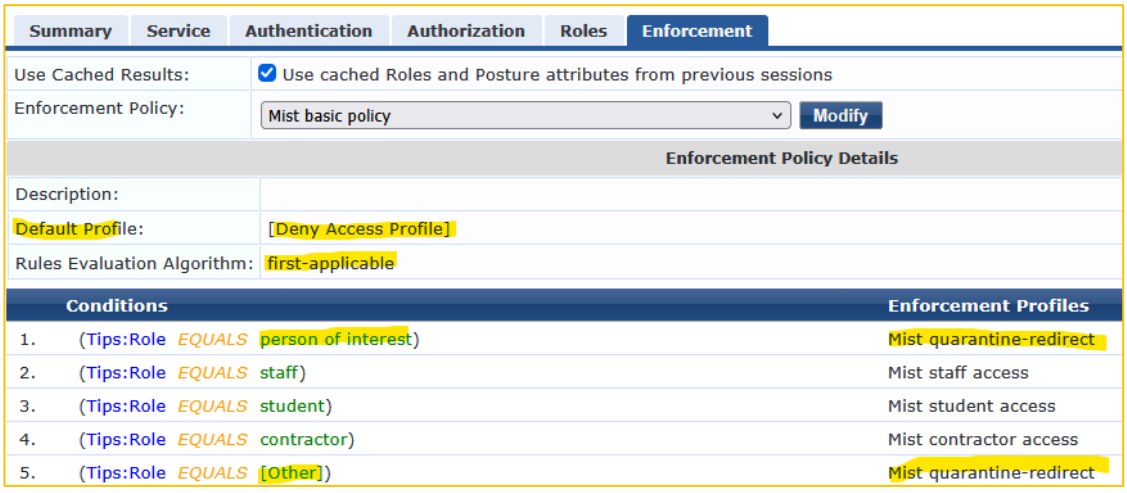
For authorisation, I'm using Active Directory plus ClearPass's Endpoint Repository. The Endpoint Repository lets policies evaluate stored device metadata, custom attributes and profiling data when making dynamic policy decisions.



Here's my deliberately simple role mapping policy, which I created earlier. It assigns logical roles to a user or device after authentication, based on contextual attributes, and I'll use those roles in the enforcement policy. As well as matching AD user groups, it checks for the username "student2" and assigns that user the "person of interest" role.



On the enforcement policy tab, you can see that I'm using the roles assigned in the role mapping policy. The default profile is [Deny Access Profile], so if nothing matches, ClearPass sends a RADIUS Reject.



The logic is simple: each role triggers its own enforcement profile. For example, a user in the Staff AD group gets the Staff role from the role mapping policy, which matches the "Mist staff access" enforcement profile, and that profile is applied.

Now look at the first condition. In the role mapping policy, anyone who authenticates as student2 gets the "person of interest" role. Here in the enforcement policy, that role triggers the "Mist quarantine-redirect" enforcement profile.

4.4 RADIUS Enforcement Profiles

Enforcement profiles are how ClearPass sends RADIUS attributes back to the HPE Mist APs. In HPE Mist, WxLAN role assignment and VLAN assignment are handled separately. If the profile returns only the Aruba-User-Role VSA, the user lands in the WLAN's default VLAN. That's because Mist uses Aruba-User-Role purely as an AAA attribute match for granular resource and WxLAN policies, not for VLAN assignment.

This is because HPE Mist APs use the Aruba-User-Role RADIUS attribute as an AAA attribute match condition to assign granular network resources and firewall/WxLAN policies and not used for VLAN assignments.

To get dynamic VLAN assignment in HPE Mist, I add three IETF standard attributes alongside Aruba-User-Role: Tunnel-Type, Tunnel-Medium-Type and Tunnel-Private-Group-Id. Remember that in the HPE Mist WLAN config we already set VLAN assignment to "Dynamic" with a default VLAN ID and a list of allowed dynamic VLAN IDs. Here are the enforcement profiles, starting with "Mist staff access".

Enforcement Profiles - Mist staff access

Summary | Profile | Attributes

Profile:

Name:	Mist staff access
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	Staff
2.	Radius:IETF	Tunnel-Medium-Type	=	IEEE-802 (6)
3.	Radius:IETF	Tunnel-Type	=	VLAN (13)
4.	Radius:IETF	Tunnel-Private-Group-Id	=	11

Enforcement Profiles - Mist student access

Summary | Profile | Attributes

Profile:

Name:	Mist student access
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	Student
2.	Radius:IETF	Tunnel-Medium-Type	=	IEEE-802 (6)
3.	Radius:IETF	Tunnel-Type	=	VLAN (13)
4.	Radius:IETF	Tunnel-Private-Group-Id	=	12

Enforcement Profiles - Mist contractor access

Summary | Profile | Attributes

Profile:

Name:	Mist contractor access
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	Contractor
2.	Radius:IETF	Tunnel-Medium-Type	=	IEEE-802 (6)
3.	Radius:IETF	Tunnel-Type	=	VLAN (13)
4.	Radius:IETF	Tunnel-Private-Group-Id	=	12

Note that we can get away by just using Aruba-User-Role and Tunnel-Private-Group-Id.

This is because HPE Mist automatically infers Tunnel-Type and Tunnel-Medium-Type when only Tunnel-Private-Group-ID is present.

I prefer the four-attribute approach shown above because it doesn't rely on implicit behaviour. A future HPE Mist AP firmware update that tightens RFC compliance could break dynamic VLAN assignment if Tunnel-Type and Tunnel-Medium-Type are missing.

The final Enforcement profile called "**Mist quarantine-redirect**", in which I want to send the relevant attributes to quarantine a user/device and to also have a customised quarantine captive portal for it. This approach is quite useful in various scenarios like posture assessment.

Enforcement Profiles - Mist quarantine-redirect

Summary | Profile | Attributes

Profile:

Name:	Mist quarantine-redirect
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	q-redirect
2.	Radius:IETF	Tunnel-Medium-Type	=	IEEE-802 (6)
3.	Radius:IETF	Tunnel-Type	=	VLAN (13)
4.	Radius:IETF	Tunnel-Private-Group-Id	=	13
5.	Radius:IETF	Session-Timeout	=	300
6.	Radius:Cisco	Cisco-AVPair	=	url-redirect=https://cp1-611.arubatechs.com/guest/quarantined_blocked.php

This profile uses two extra attributes. Session-Timeout is set to 300 seconds, so the device re-authenticates every five minutes. URL-Redirect points to the customised quarantine captive portal. It's the same AAA attribute that HPE Mist uses for the "802.1X Web Redirect" feature we configured earlier. The exact details of the url-redirect will be covered in ClearPass Guest section when we configure the quarantine page.

4.5 Enforcement Profile for CoA

CoA is quite important in any NAC or authentication infrastructure because it turns classic RADIUS from a one-time authentication into a live, real-time control system for active network sessions. So, this way ClearPass can send a CoA based on an interesting event that occurs.

When you add the HPE Mist APs to ClearPass with Juniper as the vendor, ClearPass automatically associates the default [Juniper Terminate Session] dynamic RADIUS attributes with their authentication sessions.

Remember that when we configured the “corp-CP” WLAN in HPE Mist, we set Event-Timestamp as optional under the CoA server. Per RFC 5176, the Event-Timestamp attribute protects CoA messages against replay. If we had set it to Mandatory, HPE Mist would discard any CoA message that doesn't include it.

Now by default ClearPass does not include Event-Timestamp RADIUS AVP in the default terminate session for Juniper as a vendor. You can navigate to Configuration » Enforcement » Profiles and try to edit Enforcement Profile - [Juniper Terminate Session], but unfortunately, you cannot edit any default or system profiles.

But we can copy it and create our own CoA profile. Here I have copied the default [Juniper Terminate Session] and named it as “Juniper_CoA” and added the Event-Timestamp attribute to it.

```
Radius:IETF Event-Timestamp    =      %{Authorization:[TimeSource]:Now}
```

Here is the default enforcement profile.

Enforcement Profiles - [Juniper Terminate Session]

Summary | Profile | Attributes

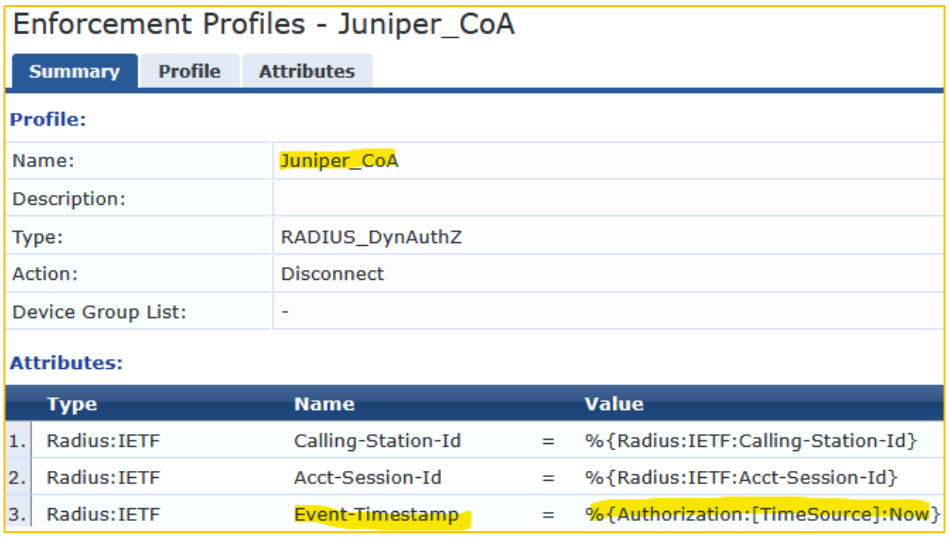
Profile:

Name:	[Juniper Terminate Session]
Description:	System-defined profile to disconnect user (Juniper)
Type:	RADIUS_DynAuthZ
Action:	Disconnect
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:IETF	Calling-Station-Id	=	%{Radius:IETF:Calling-Station-Id}
2.	Radius:IETF	Acct-Session-Id	=	%{Radius:IETF:Acct-Session-Id}

And this one is the one we created by copy the previous one and adding the third RADIUS attribute.



Enforcement Profiles - Juniper_CoA

Summary | Profile | Attributes

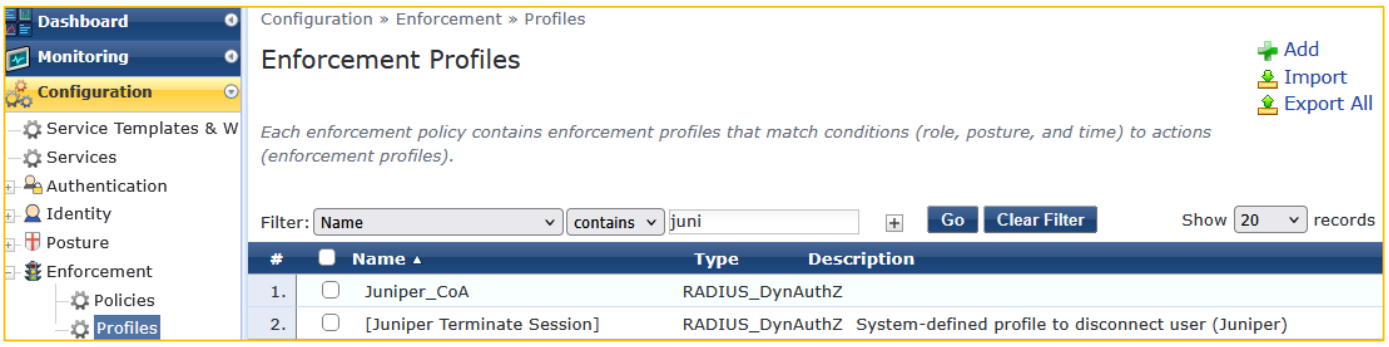
Profile:

Name:	Juniper_CoA
Description:	
Type:	RADIUS_DynAuthZ
Action:	Disconnect
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:IETF	Calling-Station-Id	=	%{Radius:IETF:Calling-Station-Id}
2.	Radius:IETF	Acct-Session-Id	=	%{Radius:IETF:Acct-Session-Id}
3.	Radius:IETF	Event-Timestamp	=	%{Authorization:[TimeSource]:Now}

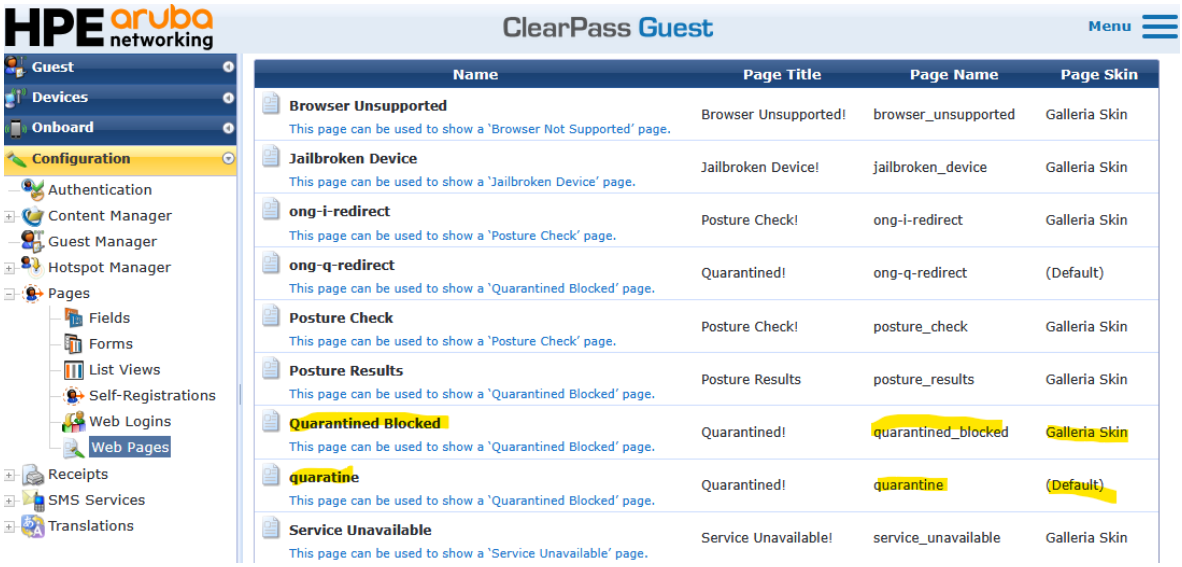
Once I save the new profile, it appears in the list. In the Verification and Testing section, we'll use the Mist quarantine-redirect and Juniper_CoA profiles and watch how they behave.



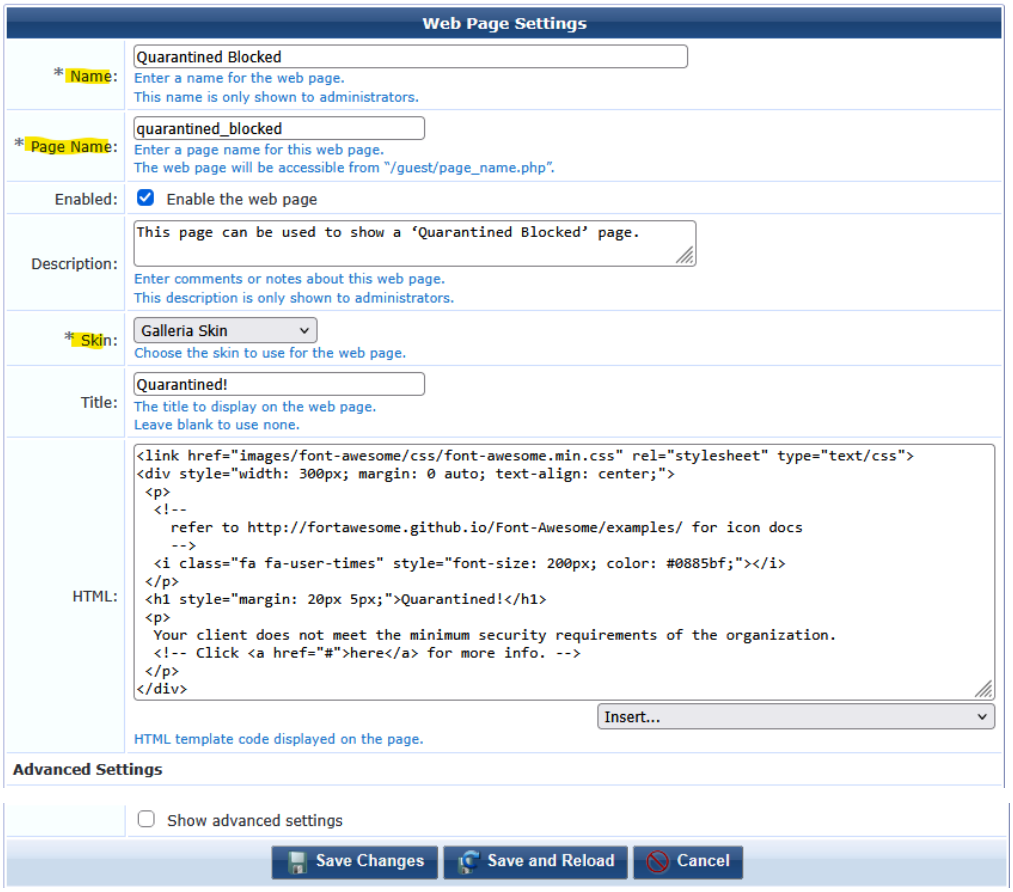
4.6 ClearPass Guest

The last piece of the solution is a customised captive portal page for quarantined devices. Use the menu button at the top right of the ClearPass dashboard to open the Guest section, then go to Home » Configuration » Pages » Web Pages.

ClearPass includes a default page called "quarantine", but I made a copy, renamed it "Quarantined Blocked", and changed the skin and page name. The page name becomes part of the URL that the RADIUS url-redirect attribute points to.

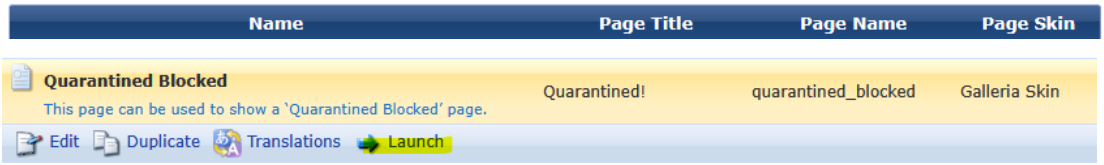


Here is my Quarantined Blocked page. Page name is part of what is referenced in the RADIUS url-redirect AVP.

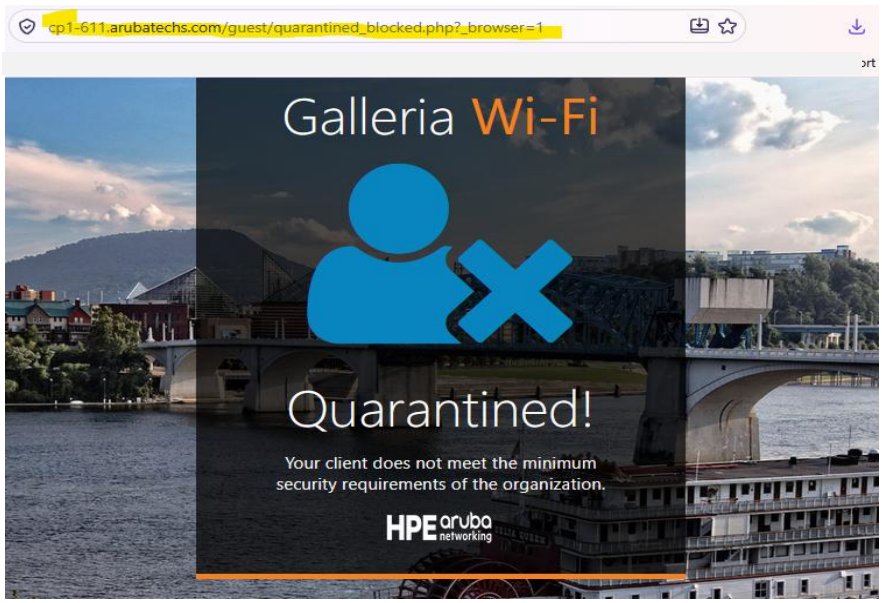


The complete URL is https://cp1-611.arubatechs.com/guest/quarantined_blocked.php

You can test it directly from ClearPass guest



And you get the following screenshot.

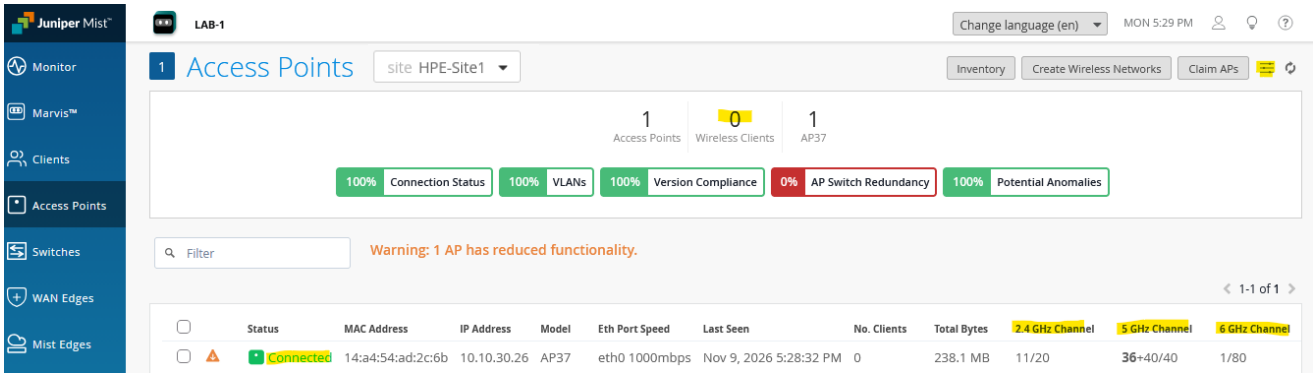


5 Verification and Testing

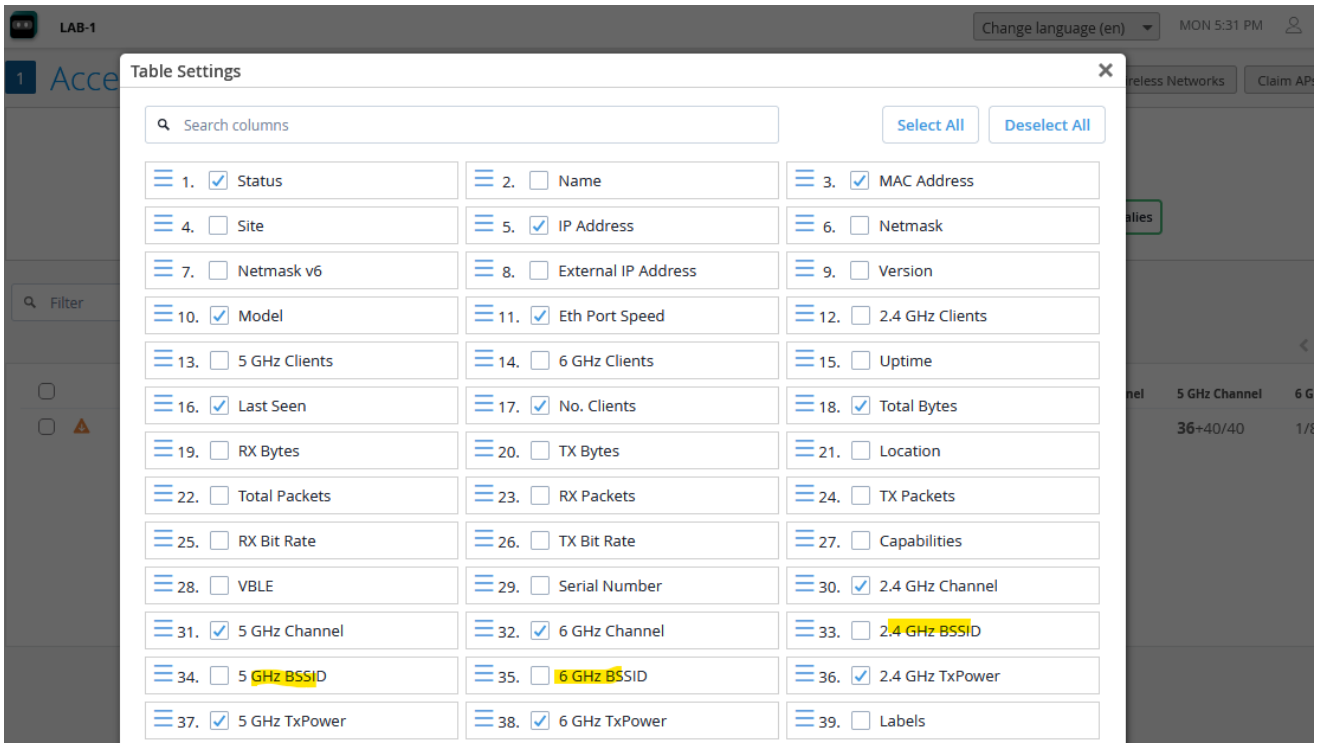
In this section we'll validate our configuration and go through client testing.

5.1 HPE Mist Dashboard

First, let's run some basic checks. In the HPE Mist dashboard, confirm that the AP status shows as Connected



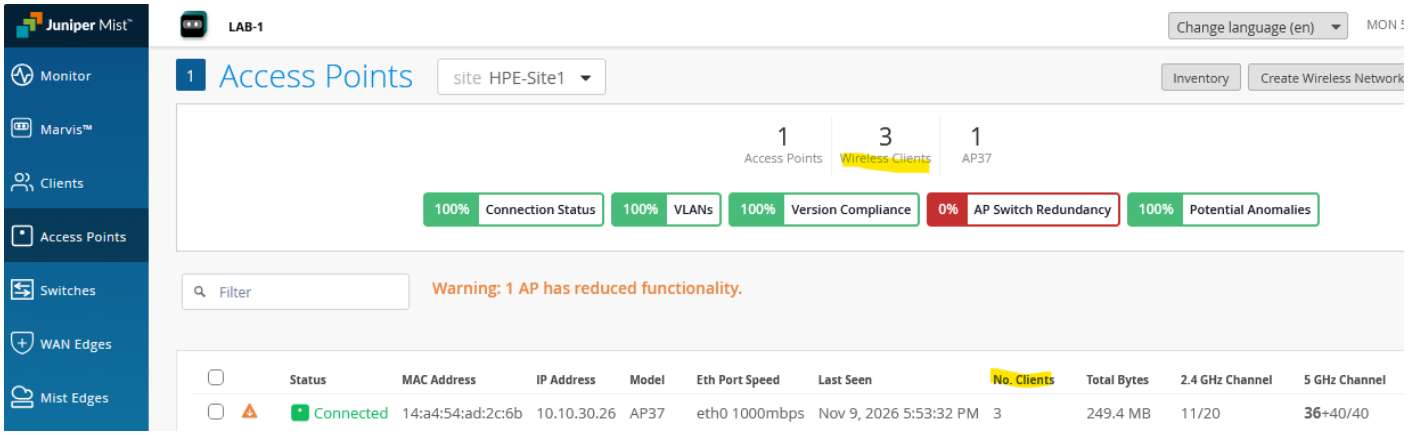
You can click on it and see if the WLANs we configured are present or click on the column setting at top right to add BSSID for various RF bands



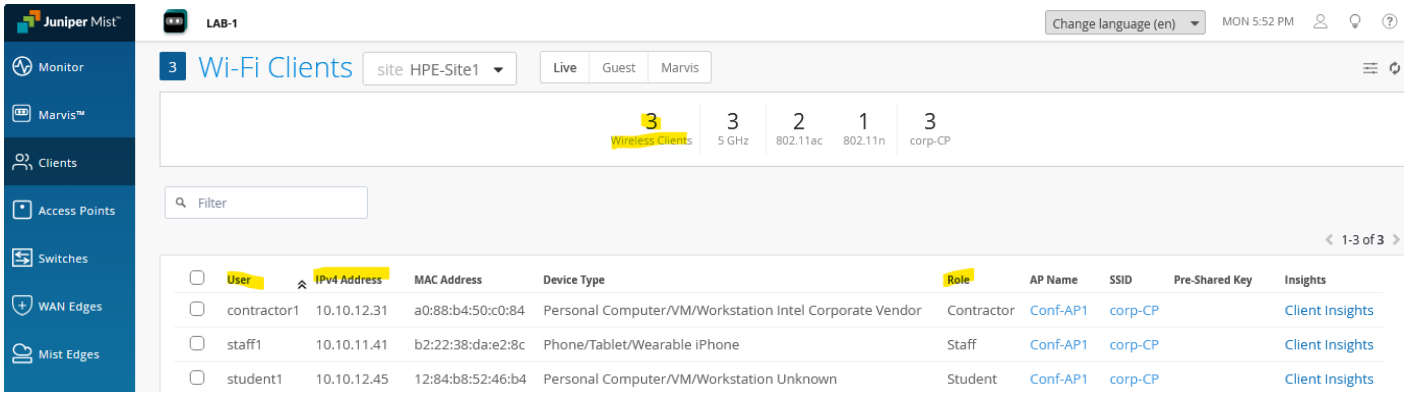
Next we get wireless clients to connect to the corp-CP WLAN. We have the following users that after authentication should be placed in the following roles and VLANs.

Username	Role	VLAN Id	IP Subnet
staff1	Staff	11	10.10.11.0/24
contractor1	Contractor	12	10.10.12.0/24
student1	Student	12	10.10.12.0/24
student2	Quarantine	13	10.10.13.0/24

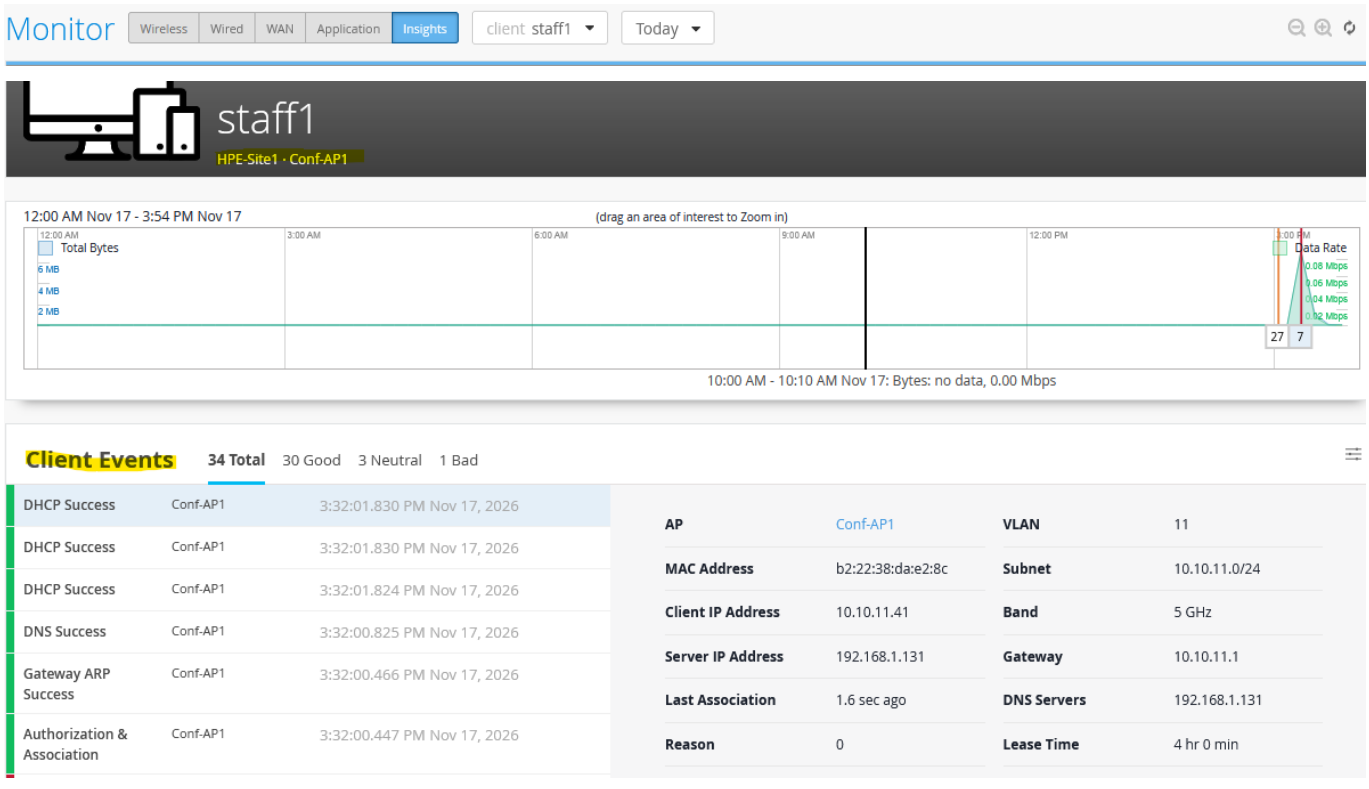
I'll start by connecting staff1, contractor1 and student1 to the WLAN. After a few minutes, they should appear in the HPE Mist dashboard. Under Access Points, we can see them listed.



Similarly, you should see the Wi-Fi clients under Clients » Wi-Fi Clients

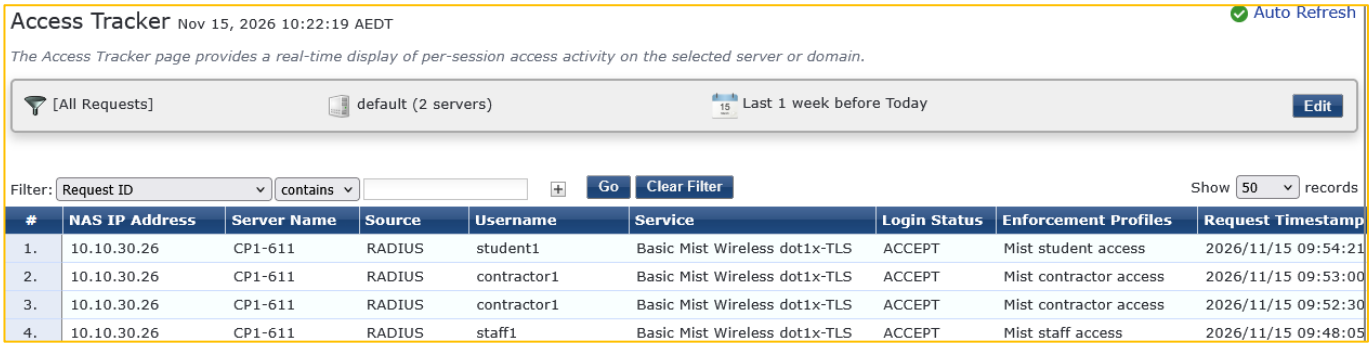


Also, by clicking on Client Insight, you get more info on specific clients. Here is the one for staff1 where we can check the client events



5.2 ClearPass Access Tracker

Here we'll first let's check the access tracker by navigating to Monitoring » Live Monitoring » Access Tracker



Access Tracker Nov 15, 2026 10:22:19 AEDT — Auto Refresh

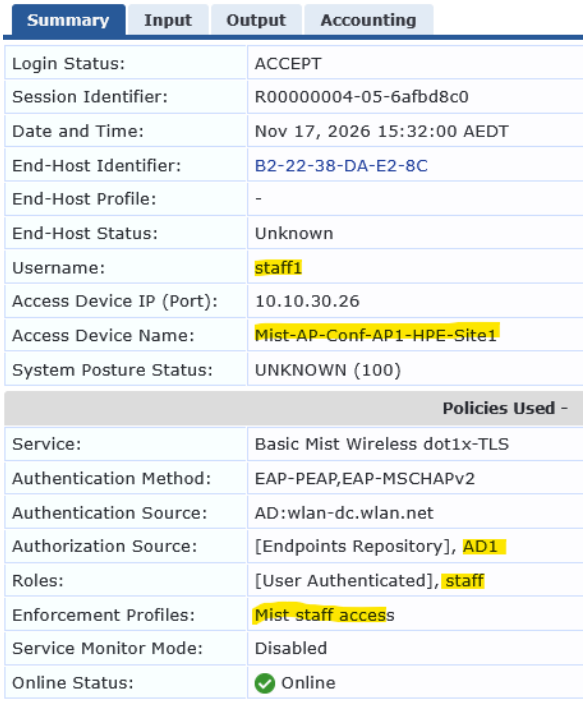
The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.

[All Requests] | default (2 servers) | Last 1 week before Today | Edit

Filter: Request ID | contains | Go | Clear Filter | Show 50 records

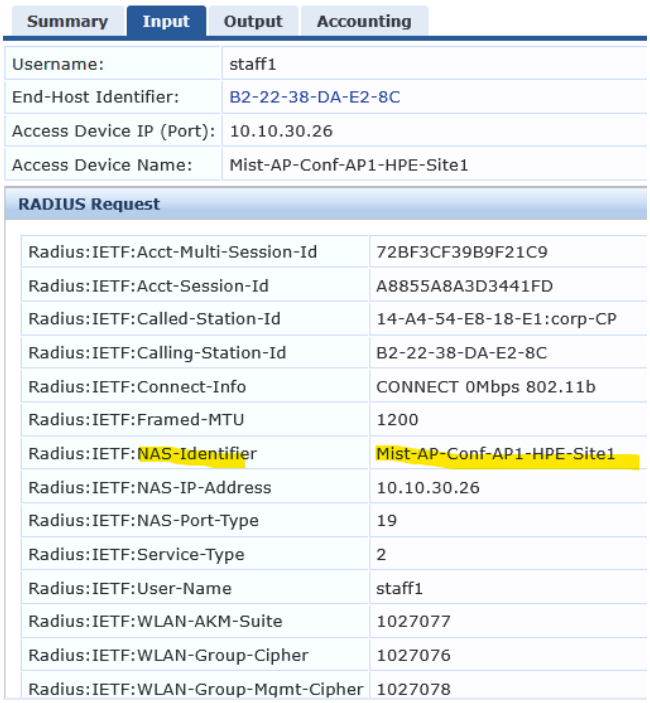
#	NAS IP Address	Server Name	Source	Username	Service	Login Status	Enforcement Profiles	Request Timestamp
1.	10.10.30.26	CP1-611	RADIUS	student1	Basic Mist Wireless dot1x-TLS	ACCEPT	Mist student access	2026/11/15 09:54:21
2.	10.10.30.26	CP1-611	RADIUS	contractor1	Basic Mist Wireless dot1x-TLS	ACCEPT	Mist contractor access	2026/11/15 09:53:00
3.	10.10.30.26	CP1-611	RADIUS	contractor1	Basic Mist Wireless dot1x-TLS	ACCEPT	Mist contractor access	2026/11/15 09:52:30
4.	10.10.30.26	CP1-611	RADIUS	staff1	Basic Mist Wireless dot1x-TLS	ACCEPT	Mist staff access	2026/11/15 09:48:05

As seen above there are four sessions and session #4 is for staff1.



Summary | Input | Output | Accounting

Login Status:	ACCEPT
Session Identifier:	R00000004-05-6afbd8c0
Date and Time:	Nov 17, 2026 15:32:00 AEDT
End-Host Identifier:	B2-22-38-DA-E2-8C
End-Host Profile:	-
End-Host Status:	Unknown
Username:	staff1
Access Device IP (Port):	10.10.30.26
Access Device Name:	Mist-AP-Conf-AP1-HPE-Site1
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	Basic Mist Wireless dot1x-TLS
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2
Authentication Source:	AD:wlan-dc.wlan.net
Authorization Source:	[Endpoints Repository], AD1
Roles:	[User Authenticated], staff
Enforcement Profiles:	Mist staff access
Service Monitor Mode:	Disabled
Online Status:	Online



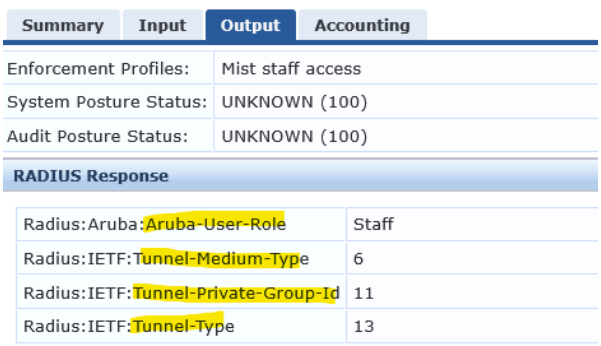
Summary | Input | Output | Accounting

Username:	staff1
End-Host Identifier:	B2-22-38-DA-E2-8C
Access Device IP (Port):	10.10.30.26
Access Device Name:	Mist-AP-Conf-AP1-HPE-Site1

RADIUS Request

Radius:IETF:Acct-Multi-Session-Id	72BF3CF39B9F21C9
Radius:IETF:Acct-Session-Id	A8855A8A3D3441FD
Radius:IETF:Called-Station-Id	14-A4-54-E8-18-E1:corp-CP
Radius:IETF:Calling-Station-Id	B2-22-38-DA-E2-8C
Radius:IETF:Connect-Info	CONNECT 0Mbps 802.11b
Radius:IETF:Framed-MTU	1200
Radius:IETF:NAS-Identifier	Mist-AP-Conf-AP1-HPE-Site1
Radius:IETF:NAS-IP-Address	10.10.30.26
Radius:IETF:NAS-Port-Type	19
Radius:IETF:Service-Type	2
Radius:IETF:User-Name	staff1
Radius:IETF:WLAN-AKM-Suite	1027077
Radius:IETF:WLAN-Group-Cipher	1027076
Radius:IETF:WLAN-Group-Mgmt-Cipher	1027078

Note that we used NAS-Identifier to match ClearPass service, however we could also use Called-Station-Id as it contains "corp-CP" which is the name of the SSID.

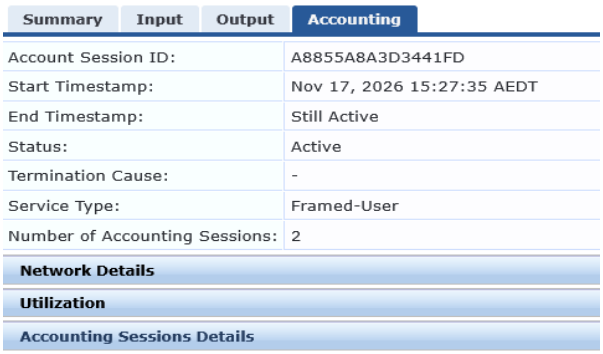


Summary | Input | Output | Accounting

Enforcement Profiles:	Mist staff access
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

Radius:Aruba:Aruba-User-Role	Staff
Radius:IETF:Tunnel-Medium-Type	6
Radius:IETF:Tunnel-Private-Group-Id	11
Radius:IETF:Tunnel-Type	13



Summary | Input | Output | Accounting

Account Session ID:	A8855A8A3D3441FD
Start Timestamp:	Nov 17, 2026 15:27:35 AEDT
End Timestamp:	Still Active
Status:	Active
Termination Cause:	-
Service Type:	Framed-User
Number of Accounting Sessions:	2

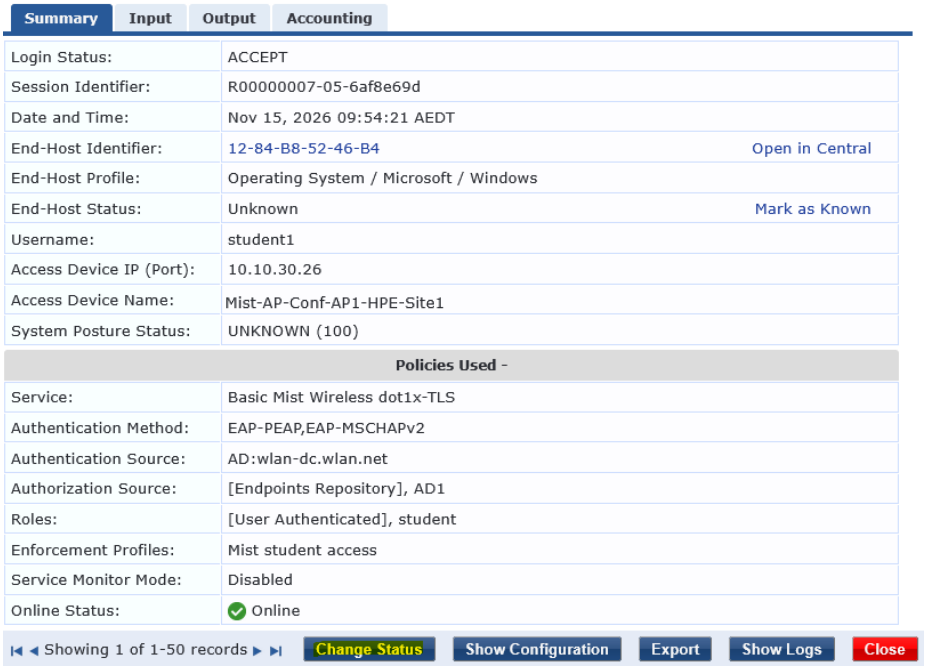
Network Details

Utilization

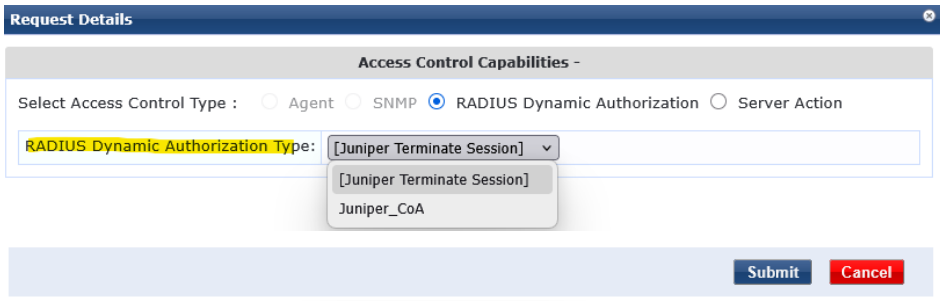
Accounting Sessions Details

The main parts are highlighted, and we also see that RADIUS accounting is working as well. It displays the number of accounting sessions too.

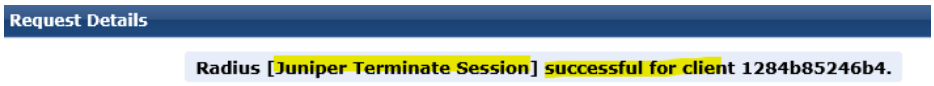
Now one way to quickly test CoA is to use "change status" button in access tracker. Below I have displayed the RADIUS session for Student1, right at the bottom, you can see the "Change Status" button.



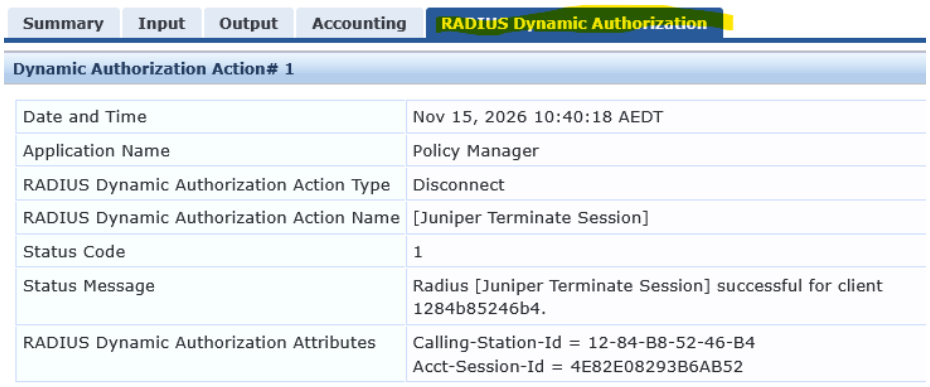
Clicking on the “Change Status” button brings up this display where you can choose the type of RADIUS Dynamic Authorisation type of enforcement profiles. Here we see the default one and the new one we configured.



You can choose either of them and when we submit it, you should see the confirmation as shown below.



And when we open the same session we’ll see the new dynamic authorisation tab.



You can go back to the HPE Mist and modify the WLAN template to set Event-Timestamp as Mandatory. Once you do that the default [Juniper Terminate Session] CoA in ClearPass will not work. For that you need to use “Juniper_CoA” instead.

5.3 Quarantine Captive Portal Redirect

Now I'll get student2 to connect to the corp-CP WLAN and it should get redirected to the quarantine captive portal and be on VLAN 13.

Here is the access tracker live monitoring that shows two sessions for student2.

Filter: Request ID contains Go Clear Filter Show 50 records

#	NAS IP Address	Server Name	Source	Username	Service	Login Status	Enforcement Profiles	Request Timestamp
1.	10.10.30.26	CP1-611	RADIUS	student2	Basic Mist Wireless dot1x-TLS	ACCEPT	Mist quarantine-redirect	2026/11/15 11:04:52
2.	10.10.30.26	CP1-611	RADIUS	minis-radius-user	Mist Minis	REJECT	[Deny Access Profile]	2026/11/15 11:01:02
3.	10.10.30.26	CP1-611	RADIUS	student2	Basic Mist Wireless dot1x-TLS	ACCEPT	Mist quarantine-redirect	2026/11/15 10:59:50
4.	10.10.30.26	CP1-611	RADIUS	student1	Basic Mist Wireless dot1x-TLS	ACCEPT	Mist student access	2026/11/15 10:45:26

Let's open the first session #1 and we can observe that the ClearPass role is "person of interest" that shows our role mapping policy has worked and it also matched its corresponding enforcement profile Mist quarantine-redirect.

Summary | Input | Output | Accounting

Login Status:	ACCEPT
Session Identifier:	R0000000c-05-6af8f722
Date and Time:	Nov 15, 2026 11:04:52 AEDT
End-Host Identifier:	A4-D1-D2-5F-32-52
End-Host Profile:	Tablet Endpoint / Apple / Apple iPad
End-Host Status:	Unknown
Username:	student2
Access Device IP (Port):	10.10.30.26
Access Device Name:	Mist-AP-Conf-AP1-HPE-Site1
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	Basic Mist Wireless dot1x-TLS
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2
Authentication Source:	AD:wlan-dc.wlan.net
Authorization Source:	[Endpoints Repository], AD1
Roles:	[User Authenticated], person of interest
Enforcement Profiles:	Mist quarantine-redirect
Service Monitor Mode:	Disabled
Online Status:	Online

Summary | Input | Output | Accounting

Username:	student2
End-Host Identifier:	A4-D1-D2-5F-32-52 (Tablet Endpoint / Apple / Apple iPad)
Access Device IP (Port):	10.10.30.26
Access Device Name:	Mist-AP-Conf-AP1-HPE-Site1

RADIUS Request

Authorization Attributes

Authorization:AD1:Account Expires	9223372036854775807 [30828-09-14 12:48:05 AEST]
Authorization:AD1:Department	Student
Authorization:AD1:memberOf	CN=Student,CN=Users,DC=wlan,DC=net
Authorization:AD1:Name	student2
Authorization:AD1:OfficeName	HS
Authorization:AD1:Title	Student
Authorization:AD1:UserDN	CN=student2,CN=Users,DC=wlan,DC=net

Computed Attributes

Authentication:ErrorCode	0
Authentication:Full-Username	student2
Authentication:InnerMethod	EAP-MSCHAPv2
Authentication:MacAuth	NotApplicable

Below we see the RADIUS outputs that ClearPass sent back to HPE Mist AP.

Summary | Input | Output | Accounting

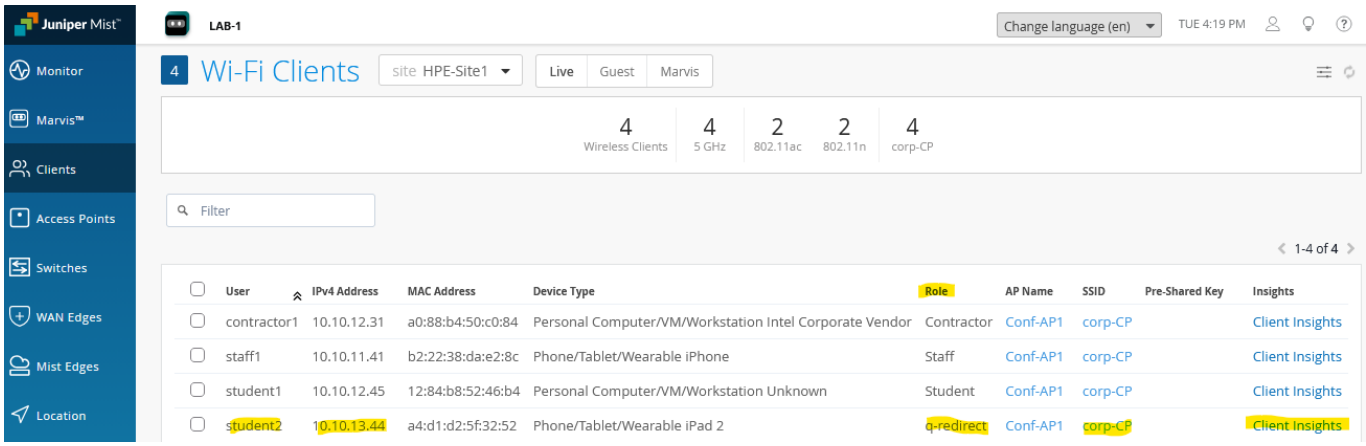
Enforcement Profiles:	Mist quarantine-redirect
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

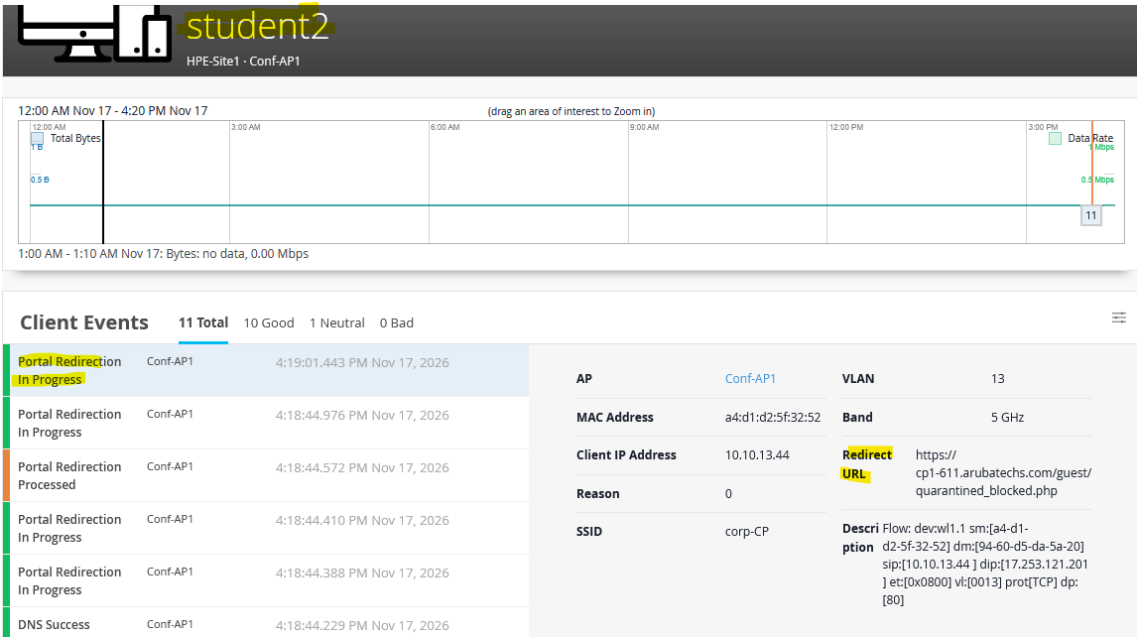
Radius:Aruba:Aruba-User-Role	q-redirect
Radius:Cisco:Cisco-AVPair	url-redirect=https://cp1-611.arubatechs.com/guest/quarantined_blocked.php
Radius:IETF:Session-Timeout	300
Radius:IETF:Tunnel-Medium-Type	6
Radius:IETF:Tunnel-Private-Group-Id	13
Radius:IETF:Tunnel-Type	13

Note that the Mist quarantine-redirect enforcement profile has a session timeout of 300 seconds, which is why we see student2 re-authenticate every five minutes.

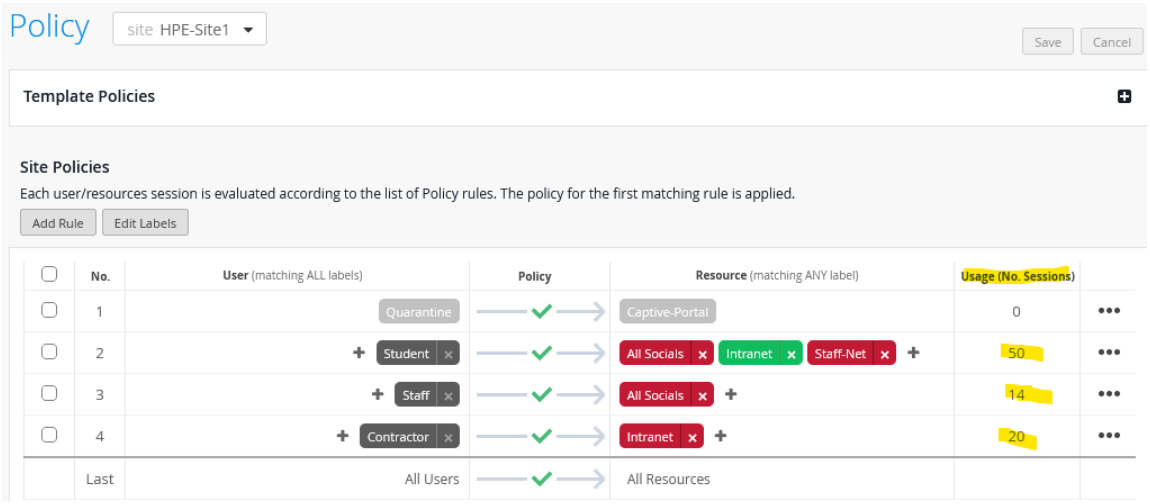
From the wireless client view, they get redirected as expected to quarantined page. Now let's check HPE Mist dashboard. Here we see that the client is on VLAN13 and the role is q-redirect which was the RADIUS aruba-user-role VSA that ClearPass sent.



Let's check the Client Insights for it where we see that Portal Redirection in progress.



Clicking on it shows the event details. Now let's check our access policies. Here we see the hits on each policy.



Also on interest is the fact that we don't have a specific policy for Captive portal as it is disabled as shown in the above screenshot. This shows that when we configured "802.1X Web Redirect" in our WLAN, that takes precedence over any policies. Even if we had enabled it the hot counts for it would be 0.