

Contents

1.1	Revision History	1
2	Demo Topology	2
3	Aruba Central Account	3
4	Aruba Central Configuration	6
4.1	LAN Switch Configuration	6
4.2	Gateway Configuration	7
4.3	AP Configuration.....	12
4.4	Assigning Static IP addresses for APs.....	14
4.5	Firmware Upgrade	14
4.6	Gateway Cluster	17
4.7	Monitoring Gateway Cluster	17
5	ClearPass Initial Configuration	20
5.1	Joining AD Domain.....	21
5.2	ClearPass dot1x Service	22
5.3	NAD Configuration.....	24
6	WLAN Configuration.....	25
6.1	Tunnelled Wireless Configuration	25
6.2	Wireless dot1x Testing.....	27
7	RF Monitoring	31
8	Guest Access Configuration	37
8.1	Guest Wireless Configuration.....	37
8.2	ClearPass Guest policy Configuration	41
8.3	ClearPass Guest Portal Configuration	46
8.4	Guest Testing.....	50

1.1 Revision History

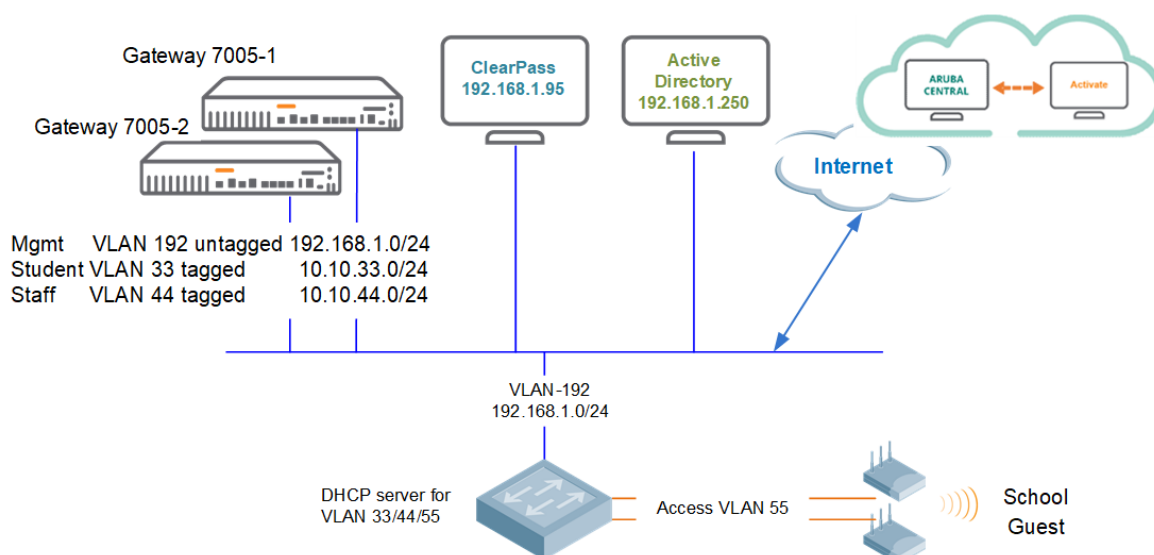
DATE	VERSION	EDITOR	CHANGES
15 Mar 2021	0.1	Ariya Parsamanesh	Initial creation
22 May 2021	0.2	Ariya Parsamanesh	Added the ClearPass guest operator login
04 Jul 2021	0.3	Ariya Parsamanesh	Added the Monitoring section

2 Demo Topology

The aim here is to provide the starting point to put together a solution that include the AOS10 APs, two gateways, ClearPass and obviously Aruba Central.

Note that APs in AOS10 support bridged, tunnelled and mix mode wireless LANs (WLAN) however in this technote we'll be deploying tunnelled mode WLANs. We'll also demonstrate the gateway clustering with AOS10.

This type of deployment is particularly useful when all the buildings in a school/college campus have L3 IP demarcation and are routed to various part of the campus.



With AOS10, the campus architecture consists of two layers:

1. **The infrastructure layer** consists of a WLAN setup which can be either a campus setup or a branch setup. The campus setup can consist only of access points (APs) or APs combined with gateway clusters. In case of a branch setup, the infrastructure layer includes an AP. Here we have combined the Instant APs and Campus APs into just APs, and you bridge, or tunnel user traffic based on the configuration on the APs.
2. **The cloud management layer** consists of Aruba Central which is a cloud management SaaS platform. The Network Operations app is one of the Aruba apps which is a part of Aruba Central and this app helps to create the SSID profiles for the different WLAN campus and branch setups.



As you can see in the above diagram, the classic components that would normally run on mobility master or instant APs are now run as services in Aruba Central. I am talking about Airmatch, Roaming, clientmatch, etc.

Here we'll not go to the details of the architecture for that please refer to this link

https://www.arubanetworks.com/techdocs/AOS10X_OLH/Content/overview/architecture-overview.htm

3 Aruba Central Account

You need an Aruba Central account with appropriate licenses for APs and gateways. You can sign up for a 90 days trial from this link

<https://www.arubanetworks.com/products/network-management-operations/central/eval/>


Once you login to your Central account you need to add your devices (APs and Gateways) to the device inventory

ACCOUNT HOME

Manage your Network Inventory, Subscriptions, and User Access. Use any of the following apps to make Aruba work better for you.

APPS

90 DAYS LEFT



Network Operations
Manage your wired, wireless, and WAN infrastructure

LAUNCH

GLOBAL SETTINGS

USERS AND ROLES
Manage user access

KEY MANAGEMENT
Manage your subscription keys

DEVICE INVENTORY
Manage the Devices in your Inventory

LICENSE ASSIGNMENT
Assign Licenses to Devices

AUDIT TRAIL
View audit-trail logs

SINGLE SIGN ON
Create and manage SAML Profiles

API GATEWAY
Access API Gateway and manage access tokens

WEBHOOKS
Manage Webhook end points

Here I have already added my APs.

Account Home > Device Inventory

If the devices associated with your account are not automatically discovered and are not displayed in your inventory, you can add devices manually by clicking the ADD DEVICES text.

You can also add your devices using the Aruba Central mobile app and they will automatically appear in your inventory.

All 15

Access Points 2

Switches 5

Serial N...	MAC Address	Part
CNCO...	B4:5D:50:...	IAP-324...
CNCO...	B4:5D:50:...	IAP-324...

Add Devices Import via CSV Download s

ADD DEVICES

SERIAL NUMBER

MAC ADDRESS

SERIAL NUMBER

MAC ADDRESS

SERIAL NUMBER

MAC ADDRESS

SERIAL NUMBER

MAC ADDRESS

SERIAL NUMBER

MAC ADDRESS

Add more devices Done

Custo...

Assign...

HPE Aruba

Foundation

HPE Aruba

Foundation

You do the same for the gateways as well. Then you need to assign the licenses to the devices, for this from Account home you need to go to “License Assignment”

GLOBAL SETTINGS

USERS AND ROLES
Manage user access

KEY MANAGEMENT
Manage your subscription keys

DEVICE INVENTORY
Manage the Devices in your Inventory

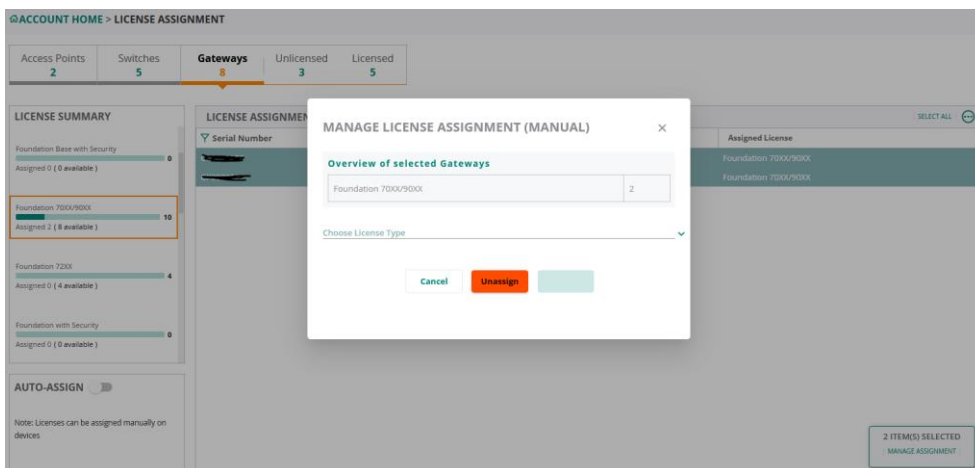
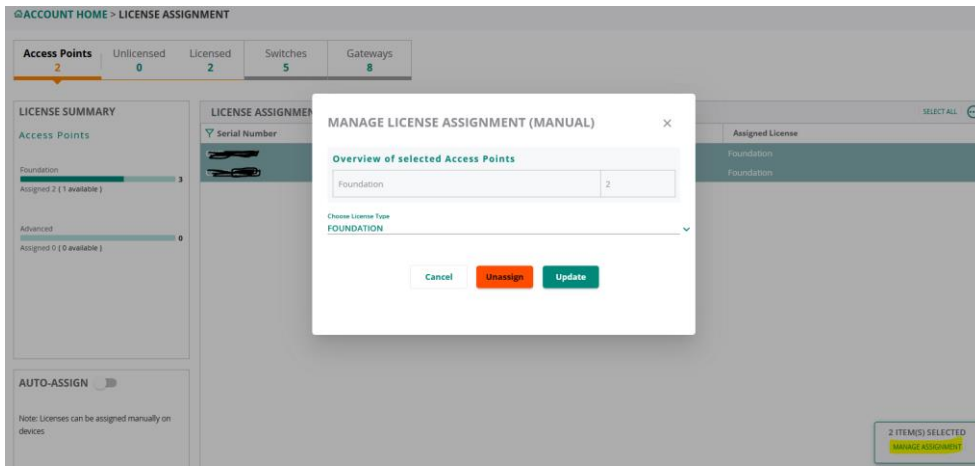
LICENSE ASSIGNMENT
Assign Licenses to Devices

AUDIT TRAIL
View audit-trail logs

SINGLE SIGN ON
Create and manage SAML Profiles

API GATEWAY
Access API Gateway and manage access tokens

WEBHOOKS
Manage Webhook end points



Now, we'll go the network operations App in Aruba Central.

ACCOUNT HOME

Manage your Network Inventory, Subscriptions, and User Access. Use any of the following apps to make Aruba work better for you.

APPS

EVALUATION 413 DAYS LEFT

Network Operations

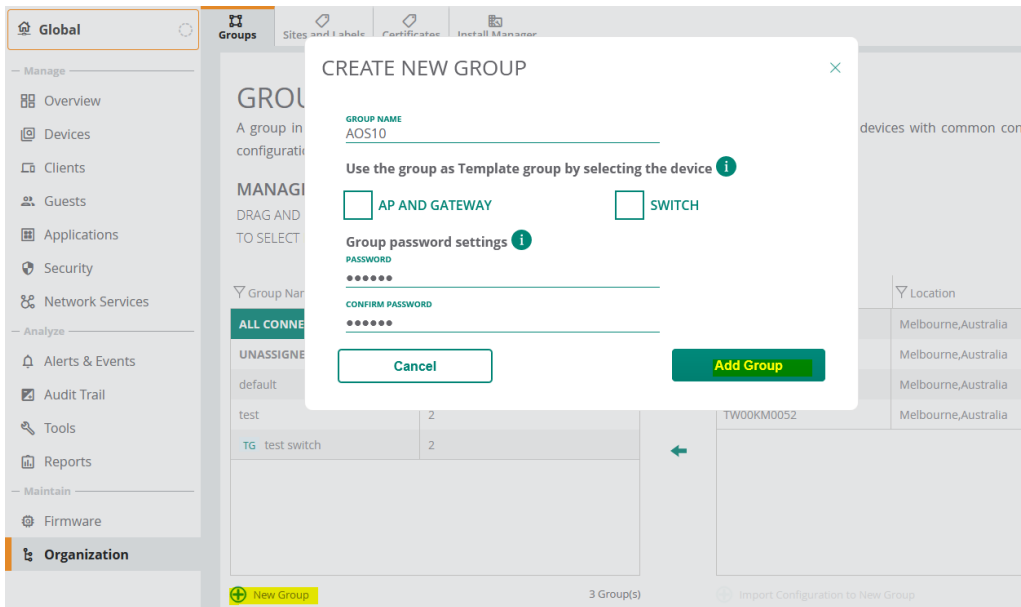
Manage your wired, wireless, and WAN infrastructure

LAUNCH

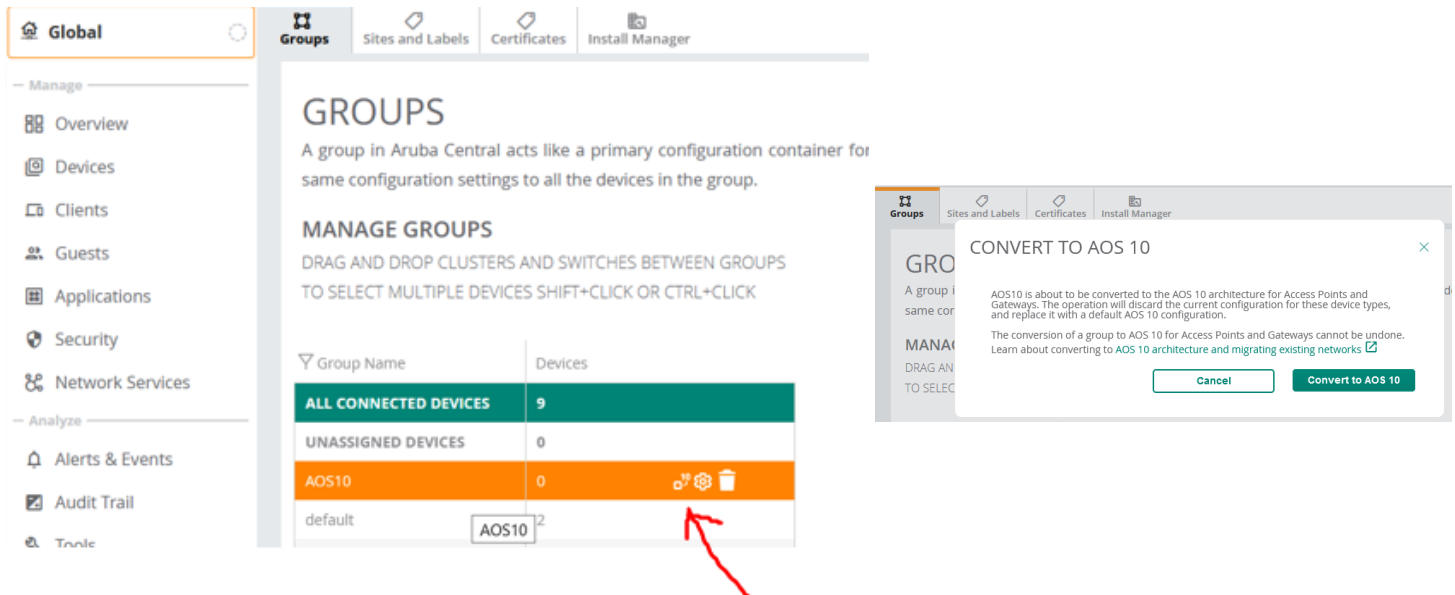
GLOBAL SETTINGS

USERS AND ROLES Manage user access	KEY MANAGEMENT Manage your subscription keys	DEVICE INVENTORY Manage the Devices in your inventory	LICENSE ASSIGNMENT Assign Licenses to Devices
AUDIT TRAIL View audit-trail logs	SINGLE SIGN ON Create and manage SAML Profiles	API GATEWAY Access API Gateway and manage access tokens	WEBHOOKS Manage Webhook end points

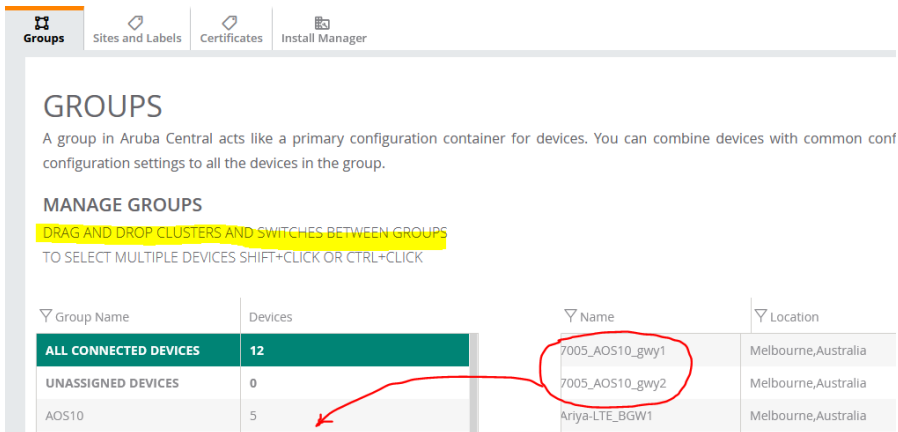
Here we'll create a group and move the devices into it. The groups are used for device configurations.



Then you need to convert the group to AOS10.



Once the group is converted, you can then drag and drop the devices from the right hand side table.

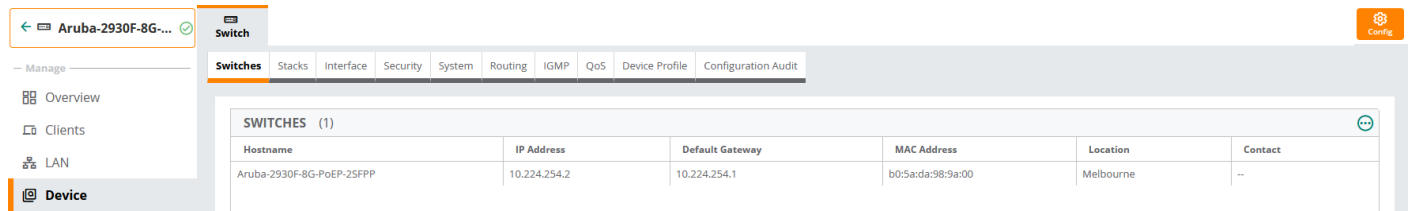


4 Aruba Central Configuration

For this demo, I have also added Aruba 2930F switch to Aruba Central's AOS10 group. We'll start with the configuration of the LAN switch to which we'll connect the APs and the gateways.

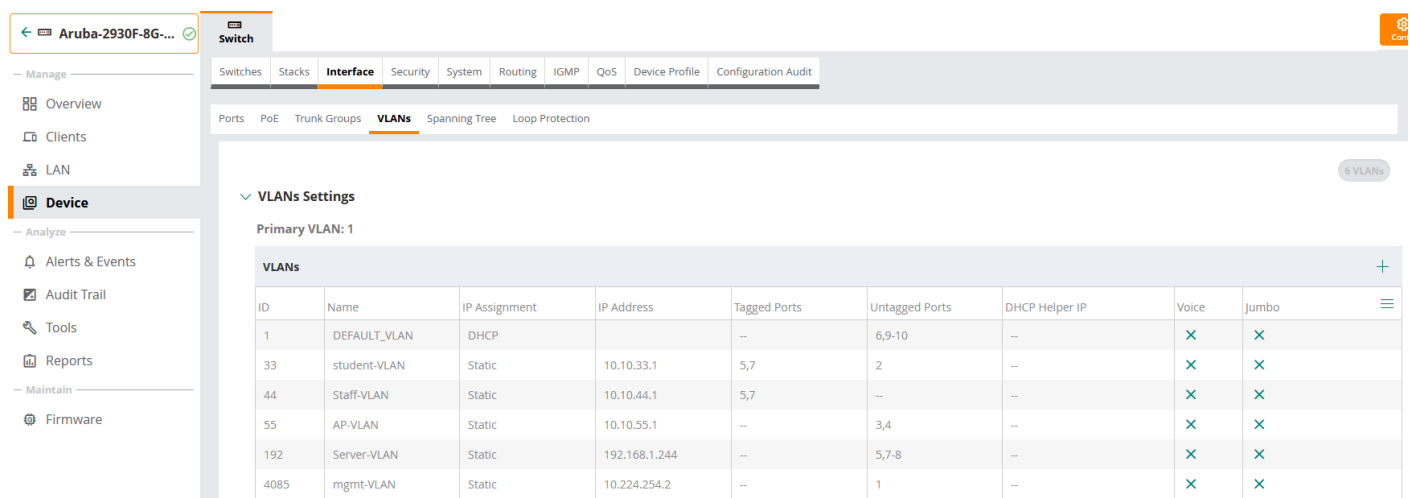
4.1 LAN Switch Configuration

We won't go deep in this section as the focus here is AOS 10 demo. Take a note of the VLANs that are configured.



Switches (1)

Hostname	IP Address	Default Gateway	MAC Address	Location	Contact
Aruba-2930F-8G-PoEP-25FPP	10.224.254.2	10.224.254.1	b0:5a:da:98:9a:00	Melbourne	--



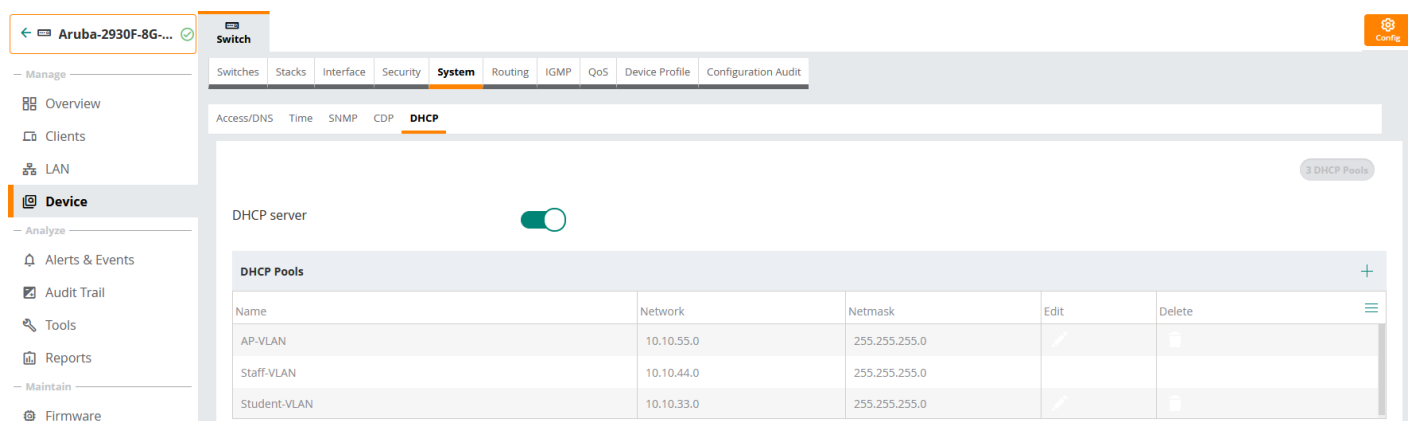
VLANs Settings

Primary VLAN: 1

ID	Name	IP Assignment	IP Address	Tagged Ports	Untagged Ports	DHCP Helper IP	Voice	Jumbo
1	DEFAULT_VLAN	DHCP		--	6,9-10	--	✗	✗
33	student-VLAN	Static	10.10.33.1	5,7	2	--	✗	✗
44	Staff-VLAN	Static	10.10.44.1	5,7	--	--	✗	✗
55	AP-VLAN	Static	10.10.55.1	--	3,4	--	✗	✗
192	Server-VLAN	Static	192.168.1.244	--	5,7-8	--	✗	✗
4085	mgmt-VLAN	Static	10.224.254.2	--	1	--	✗	✗

As the names suggests, APs are connected to AP-VLAN, gateways and ClearPass are connected to Server VLAN.

The gateways are connected to port 5 and 7 that are configured for VLAN trunking. DHCP for AP, staff, and student VLANs are configured on the switch.



DHCP server

DHCP Pools

Name	Network	Netmask	Edit	Delete
AP-VLAN	10.10.55.0	255.255.255.0		
Staff-VLAN	10.10.44.0	255.255.255.0		
Student-VLAN	10.10.33.0	255.255.255.0		

```
dhcp-server pool "AP-VLAN"
  default-router "10.10.55.1"
  dns-server "10.224.254.1"
  lease 00:08:00
  network 10.10.55.0 255.255.255.0
  range 10.10.55.10 10.10.55.19
  exit
dhcp-server pool "Staff-VLAN"
```

```

default-router "10.10.44.1"
dns-server "1.1.1.1"
lease 00:04:00
network 10.10.44.0 255.255.255.0
range 10.10.44.50 10.10.44.59
exit
dhcp-server pool "Student-VLAN"
default-router "10.10.33.1"
dns-server "1.1.1.1"
lease 00:04:00
network 10.10.33.0 255.255.255.0
range 10.10.33.50 10.10.33.59
exit
dhcp-server enable

Aruba-2930F-8G-PoEP-2SFPP#

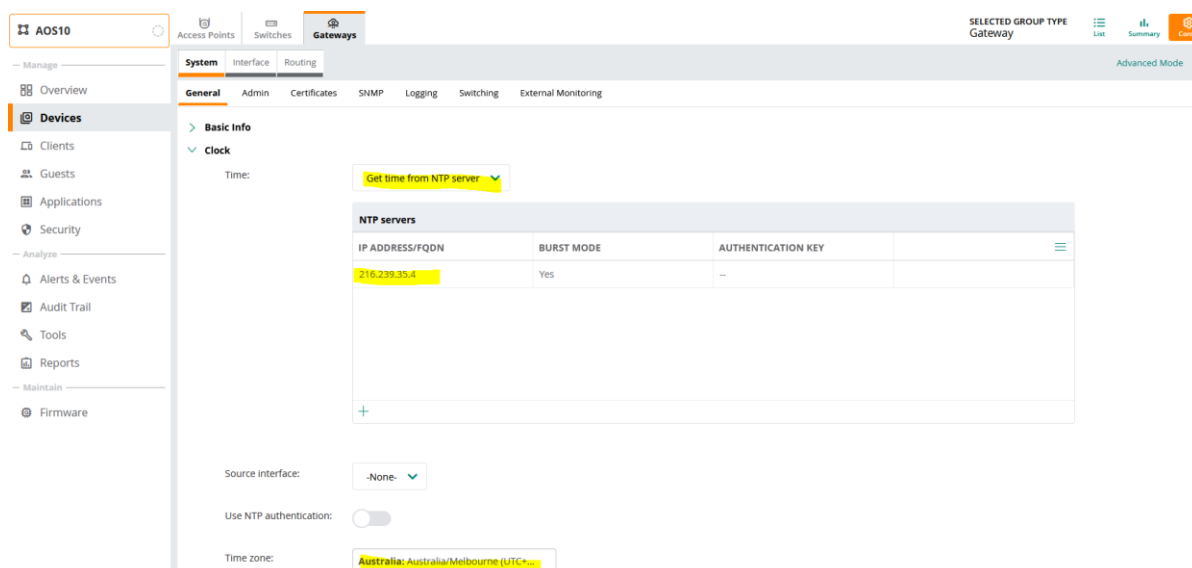
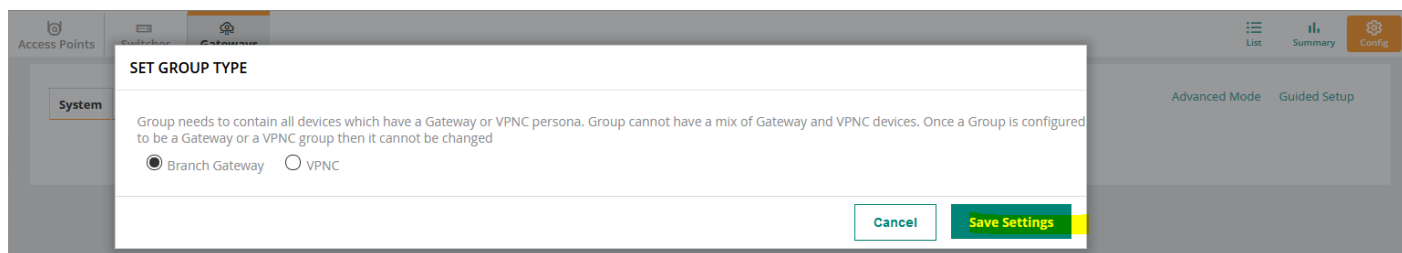
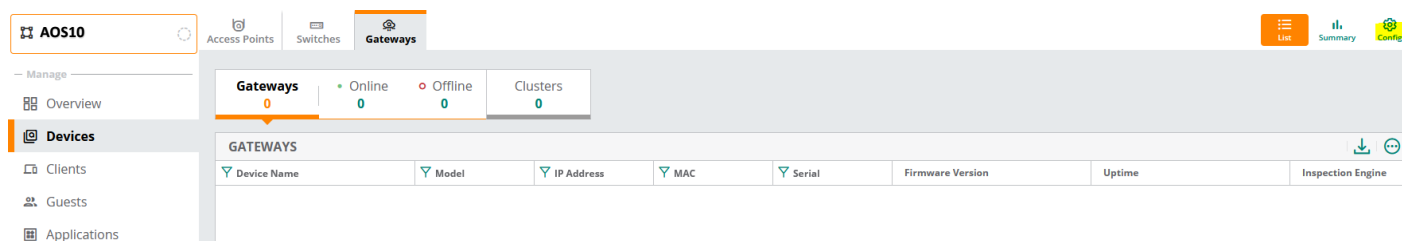
```

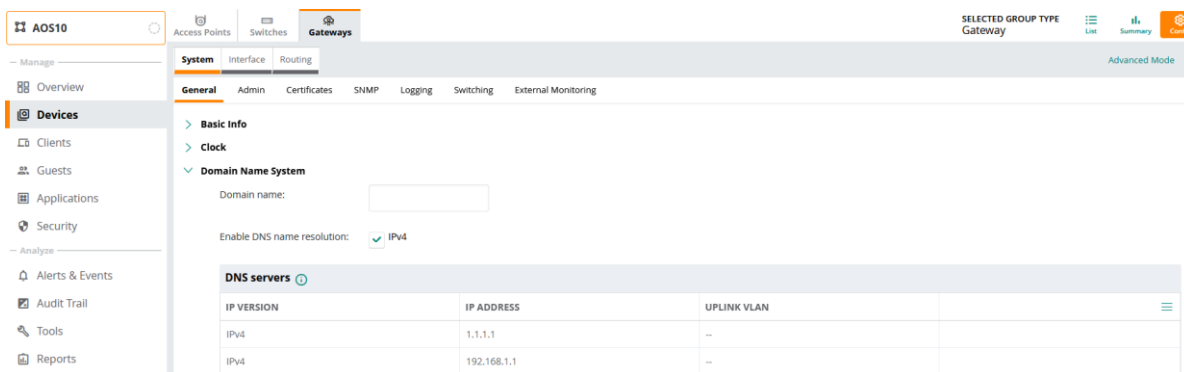
4.2 Gateway Configuration

Note that with AOS 10, Gateways are not mandatory. They are required if you want to tunnel user traffic to a central location particularly useful for scenarios that you need L2 roaming between APs in different subnets.

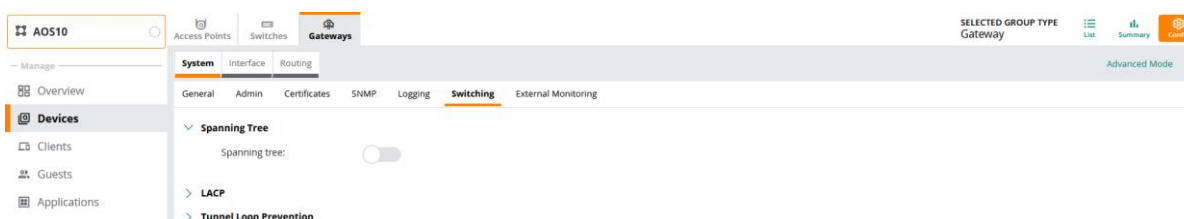
We'll start the configuration at group level before powering up the gateways. This is to minimise the reboots and some potential network issues especially when it comes to changing IP address and loosing connectivity.

We'll be using Aruba 7005 gateways which have 4x ports.

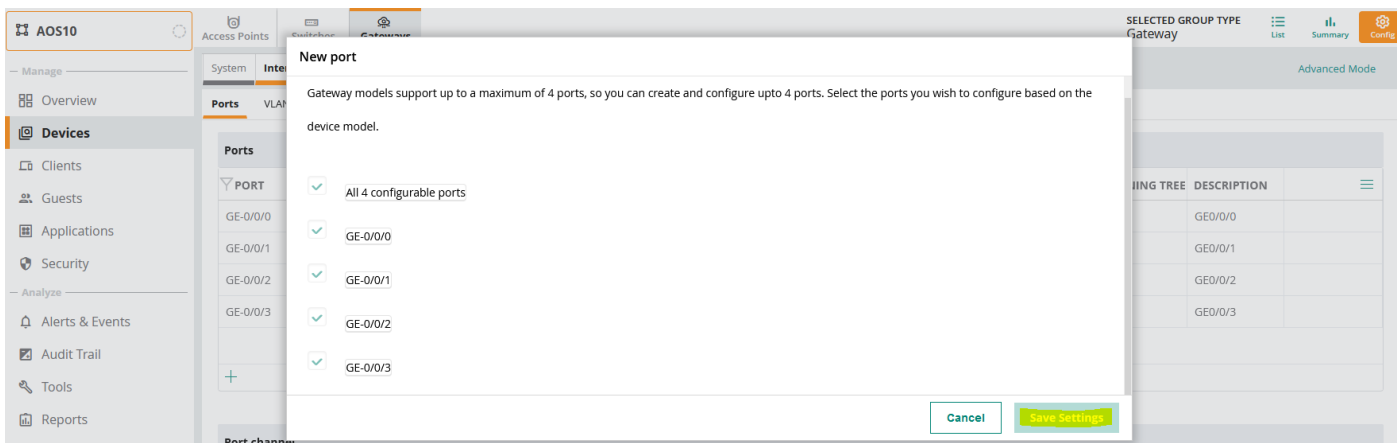




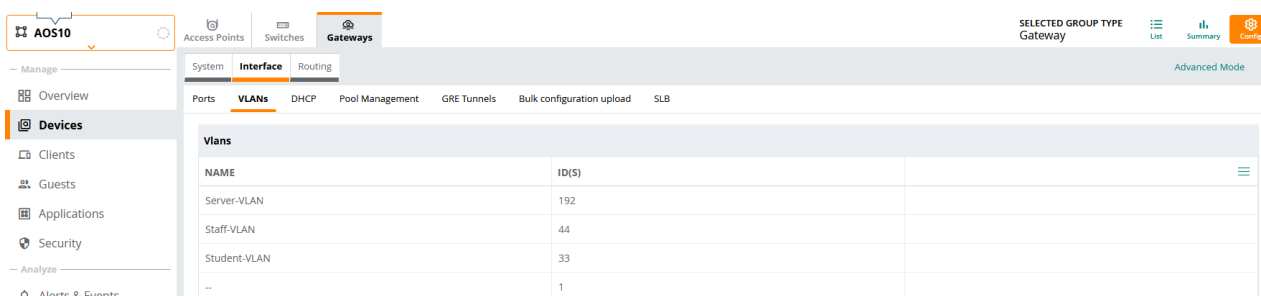
Disabling spanning tree



Adding the relevant ports for Aruba 7005 gateway.



I am planning to use interface 0/0/0 as my gateway uplink. This port needs to be in trunk mode and here we'll add the relevant VLANs.



Adding the VLANs to appropriate ports.

AOS10 | Access Points | Switches | **Gateways** | SELECTED GROUP TYPE: Gateway | List | Summary | Config

System | **Interface** | Routing | Advanced Mode

Ports | VLANs | DHCP | Pool Management | GRE Tunnels | Bulk configuration upload | SLB

PORT	TYPE	ADMIN STATE	POLICY	MODE	NATIVE VLAN	ACCESS VLAN	TRUNK VLANs	TRUSTED VLANs	SPANNING TREE	DESCRIPTION
GE-0/0/0	--	Enabled	Not-defined	trunk	192	--	33,44,192	33,44,192	✓	GE0/0/0
GE-0/0/1	--	Enabled	Not-defined	access	--	1	--	--	✓	GE0/0/1
GE-0/0/2	--	Enabled	Not-defined	access	--	1	--	1-4094	✓	GE0/0/2
GE-0/0/3	--	Enabled	Not-defined	access	--	1	--	1-4094	✓	GE0/0/3

GE-0/0/0


Type: LAN

Admin state: ☒

Speed: auto Mbps

Duplex: auto

Poe: ☐

Trust: ☒ 

Policy: Not-defined

Mode: Trunk

Native VLAN: 192

Allowed VLANs: 33,44,192

Description: GE0/0/0

Jumbo MTU: ☐

Port monitoring: -None-

Adding the default route

AOS10 | Access Points | Switches | **Gateways** | SELECTED GROUP TYPE: Gateway | List | Summary | Config

System | Interface | **Routing** | WAN | Security | VPN | High Availability | Config Audit | Basic Mode

IP Routes | Policy-Based Routing | NextHop Configuration | RIP | OSPF | BGP | Overlay Routing

> IP Routes

Static Default Gateway

DEFAULT GATEWAY	COST
192.168.1.1	1

Adding the user roles by going to “security tab”

AOS10 | Access Points | Switches | **Gateways** | SELECTED GROUP TYPE: Gateway | List | Summary | Config

System | Interface | **Security** | Roles | Policy-Based Routing | High Availability | Config Audit | Basic Mode

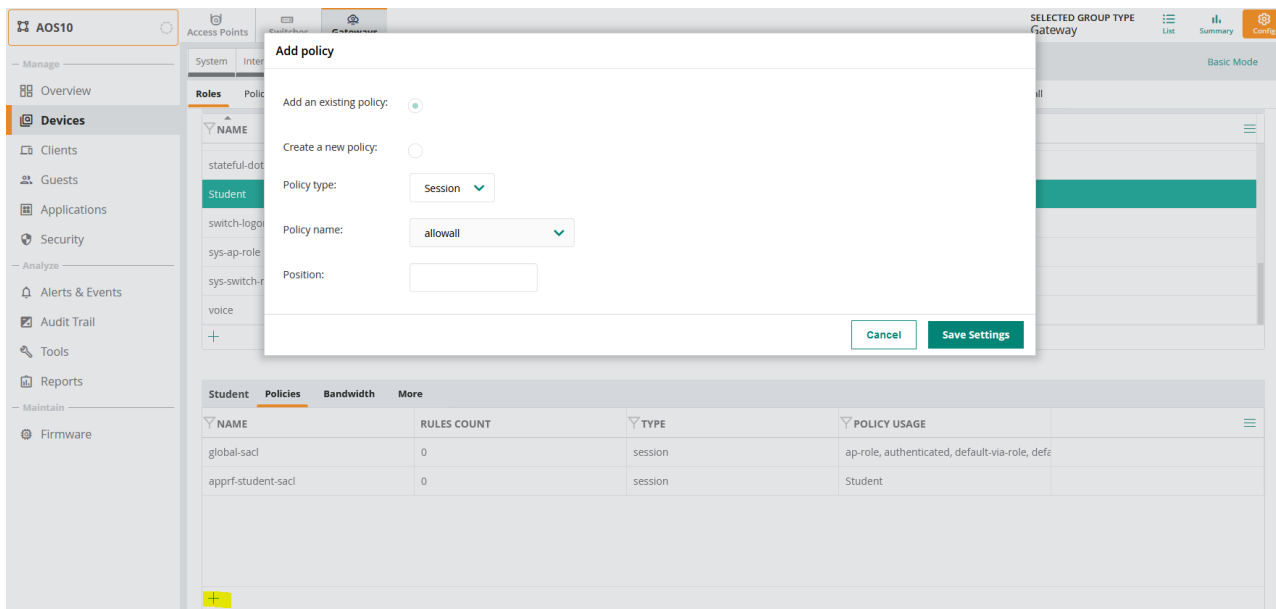
Roles | Policy-Based Routing

New role

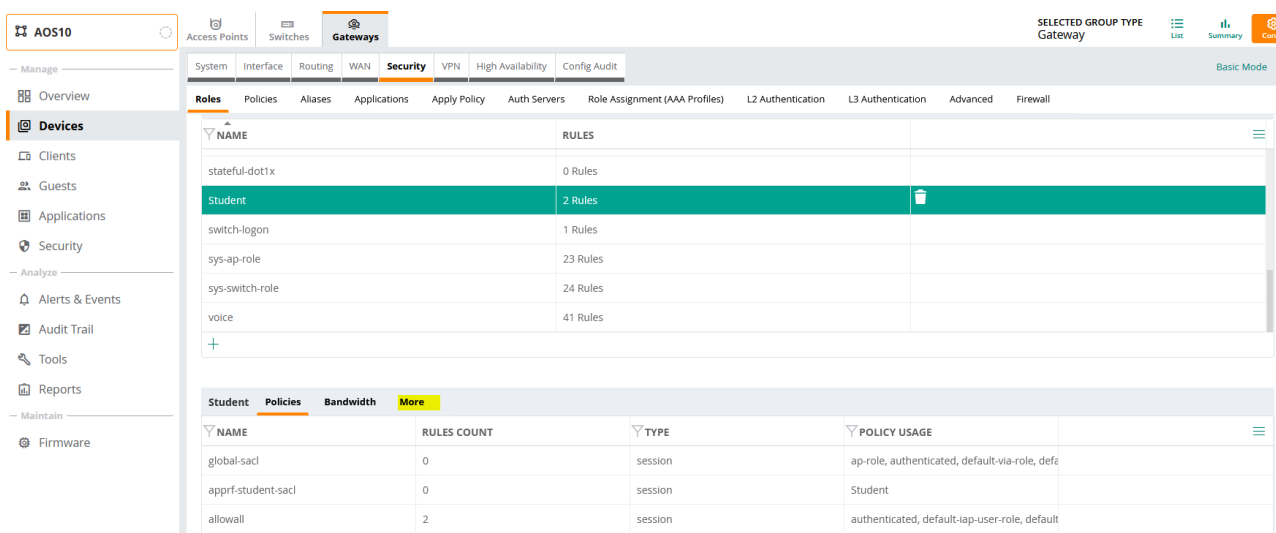
Name: Student

Cancel | Save Settings

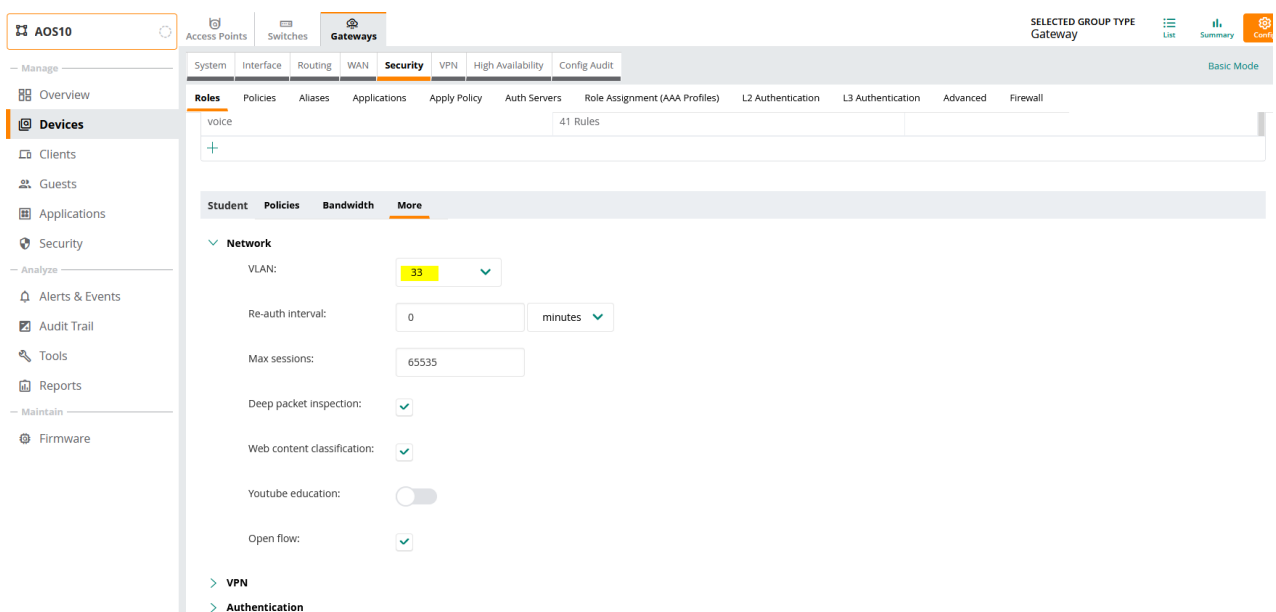
NAME	Rules
ap-role	35 Rules
authenticated	4 Rules
default-iap-user-role	2 Rules
default-via-role	3 Rules
default-vpn-role	4 Rules
guest	11 Rules



Here we'll add the allow-all policy.



Next, we'll assign a VLAN to this role.



We'll create a new user role staff and as before, we'll add a allow-all policy and assign VLAN 44 to it.

The screenshot shows the AOS10 configuration interface. The left sidebar has a 'Manage' section with 'Overview' and 'Devices'. The 'Devices' section is expanded, showing 'Clients', 'Guests', 'Applications', 'Security', 'Alerts & Events', 'Audit Trail', 'Tools', and 'Reports'. The main panel is titled 'Gateways' and has tabs for 'System', 'Interface', 'Routing', 'WAN', 'Security', 'VPN', 'High Availability', and 'Config Audit'. The 'Security' tab is selected, and the 'Auth Servers' sub-tab is active. A table titled 'Roles' is displayed with the following data:

NAME	RULES
guest-login	27 Rules
login	32 Rules
school	1 Rules
Staff	2 Rules
stateful-dot1x	0 Rules
student	2 Rules

We'll configure the authentication server and RFC3576 for RADIUS CoA

The screenshot shows the 'New server' dialog box in the AOS10 configuration interface. The dialog has the following fields:

- Name: ClearPass-GW
- IP address / hostname: 192.168.1.95
- Type: Radius

There are 'Cancel' and 'Save Settings' buttons at the bottom right of the dialog.

Then once saved, click on it to set the RADIUS secret key

The screenshot shows the 'Auth Servers' configuration page in the AOS10 configuration interface. The 'Auth Servers' sub-tab is selected under the 'Security' tab. The 'Server options' section is displayed with the following fields:

- Name: ClearPass-GW
- IP address / hostname: 192.168.1.95
- Secure radius: ☐
- Auth port: 1812
- Acct port: 1813
- Shared key: [Redacted]
- Retype key: [Redacted]
- Timeout: 5

And finally add a rfc3576 server for CoA.

Access Points

System WAN

Roles Policies

NA

+

New server

IP address: 192.168.1.95

Key:

Retype key:

Type: RFC 3576

Cancel Save Settings

All servers

NAME	TYPE	IP ADDRESS / HOSTNAME	SERVER GROUP
ClearPass1	Radius	192.168.1.95	--

+

Note that they are not assigned to any authentication server groups.

Manage

Overview

Devices

Clients

Guests

Applications

Security

Analyze

Alerts & Events

Audit Trail

Tools

Reports

Maintain

Firmware

System WAN Interface Security VPN Routing High Availability Config Audit

Roles Policies Aliases Applications Apply Policy Auth Servers Role Assignment (AAA Profiles) L2 Authentication L3 Authentication Advanced Firewall

NAME	SERVICES	FAIL THROUGH	LOAD BALANCE	SERVER RULES
No data to display				

+

All servers

NAME	TYPE	IP ADDRESS / HOSTNAME	SERVER GROUP
ClearPass1	Radius	192.168.1.95	--
--	RFC 3576	192.168.1.95	--

4.3 AP Configuration

Here we'll go through the AP configuration. As always, we'll do the bulk of configuration at the group level.

AOS10

Access Points Switches Gateways

WLANs Access Points Radios Interfaces Security Services System Configuration Audit

Hide Advance

SYSTEM

General

Set Country code for group : AU - Australia

Timezone : Melbourne UTC+10

The selected country observes Daylight Savings Time

Preferred Band : 5 GHz

NTP Server : 216.239.35.4

DHCP Option 82 XML :

Login Session Timeout: 5

Console Access:

Console Access :	<input checked="" type="checkbox"/>
WebUI Access :	<input checked="" type="checkbox"/>
Telnet Server :	<input type="checkbox"/>
LED Display :	<input checked="" type="checkbox"/>
Deny Inter User Bridging :	<input type="checkbox"/>
Deny Local Routing :	<input type="checkbox"/>
Mobility Access Switch Integration :	<input type="checkbox"/>
URL Visibility:	<input checked="" type="checkbox"/>
Restrict uplink port to specified VLANs:	<input type="checkbox"/>
VOIP QOS Trust:	<input type="checkbox"/>

- > Administrator
- > Mesh
- > Time-Based Services
- > Enterprise Domains
- > Logging
- > SNMP
- > Proxy
- > IPM

AOS10

Manage

Overview

Devices

Clients

Guests

Applications

Security

Access Points

Switches

Gateways

WLANs

Access Points

Radios

Interfaces

Security

Services

System

Configuration Audit

3 hours

List

Summary

Config

Hide Advance

SECURITY

Authentication Servers

Authentication Servers

Name

Type

NEW SERVER

Server Type:

RADIUS

Name:

ClearPass

Radsec:

☐

IP Address:

192.168.1.95

Auth Port:

1812

Shared Key:

NAS IP Address:

optional

Retype Key:

NAS Identifier:

optional

Timeout :

5

sec

Retry Count:

3

Service Type Framed User :

☐ MAC/Captive Portal

Query Status of RADIUS Servers(RFC 5997):

☐ Authentication

Dynamic Authorization:

☐

Accounting Port:

1813

Accounting:

☐

Cancel

Save

As we did with gateways, we'll create various user roles here as well.

AOS10

Manage

Overview

Devices

Clients

Guests

Applications

Security

Analyze

Alerts & Events

Audit Trail

Tools

Reports

Maintain

Firmware

Access Points

Switches

Gateways

WLANs

Access Points

Radios

Interfaces

Security

Services

System

Configuration Audit

List

Summary

Config

Hide Advanced

SECURITY

Authentication Servers

MPSK Local

User For Internal Server

Roles

Roles

Role

Staff

Student

default_wired_port_profile

school

wired-SetMeUp

Access Rules For Selected Roles

Allow any to all destinations

This is in case we want to change from tunnel mode to bridge mode for user traffic, otherwise we don't need these roles here.

4.4 Assigning Static IP addresses for APs

In most of the cases you'll go with DHCP based IP addresses, but in case you need to assign static IP addresses, it is done as shown below.

The screenshot shows the Aruba Central AOS10 interface. The 'Access Points' tab is selected, displaying a summary of 2 access points. Below the summary, a table lists the access points:

Device Name	Status	IP Address	Model	Firmware Version	Group	Uptime
b4:5d:50:c6:82:3c	Offline	10.10.55.10	AP-324	10.2.0.1_79907	AOS10	-
b4:5d:50:c6:82:4a	Online	10.10.55.11	AP-324	10.2.0.1_79907	AOS10	4 Hours 42 Minutes 18 Seconds

The screenshot shows the 'Configuration Audit' tab for the access point b4:5d:50:c6:82:3c. It displays a table with the following information:

Name	Status	IP Address	WLANs	Radio Profile	Type
b4:5d:50:c6:82:3c	Down	10.10.55.10	All SSIDs selected	default	AP-324

The screenshot shows the 'Configuration Audit' tab for the access point b4:5d:50:c6:82:3c, specifically the 'SYSTEM' configuration section. The fields are as follows:

- Name: b4:5d:50:c6:82:3c
- IP Address For Access Point: ☐ Get IP Address from DHCP server, ☒ Static
- IP Address: Invalid IP Address
- Netmask: Invalid Netmask
- Default Gateway: Invalid IP Address
- DNS Server:
- Domain Name:
- LACP Mode:

4.5 Firmware Upgrade

We'll now connect the APs that we previously added to Aruba Central inventory that are running Instant software to the network. The network must have Internet access. Ensure that the APs are in factory default mode to get rid of any previous configuration. When they are powered up, they will get DHCP IP address and with a valid DNS and will then contact Central and will end up in AOS10 group that we created before.

For the gateways ensure they are factory default and running the SD-branch image 8.6.0.4-2.2.x.x or better. Again, like the APs, once the gateways are powered up they can use DHCP to get their IP addresses and will then contact Aruba Central, but we'll go through the full setup without DHCP.

Auto-provisioning is in progress. It requires DHCP and Activate servers
Choose one of the following options to override or debug auto-provisioning...

```
'enable-debug' : Enable auto-provisioning debug logs
```

```
'disable-debug'      : Disable auto-provisioning debug logs
'mini-setup'         : Start mini setup dialog. Provides minimal customization and
requires DHCP server
'full-setup'         : Start full setup dialog. Provides full customization
'static-activate'    : Provides customization for static or PPPOE ip assignment.
Uses activate for master information
```

Enter Option (partial string is acceptable): **full-setup**

Are you sure that you want to stop auto-provisioning and start full setup dialog?
(yes/no): yes

```
***** Welcome to the Aruba7005 setup dialog *****
This dialog will help you to set the basic configuration for the switch.
These settings, except for the Country Code, can later be changed from the
Command Line Interface or Graphical User Interface.
```

```
Commands: <Enter> Submit input or use [default value], <ctrl-I> Help
<ctrl-B> Back, <ctrl-F> Forward, <ctrl-A> Line begin, <ctrl-E> Line end
<ctrl-D> Delete, <BackSpace> Delete back, <ctrl-K> Delete to end of line
<ctrl-P> Previous question <ctrl-X> Restart beginning <ctrl-R> Reload box
```

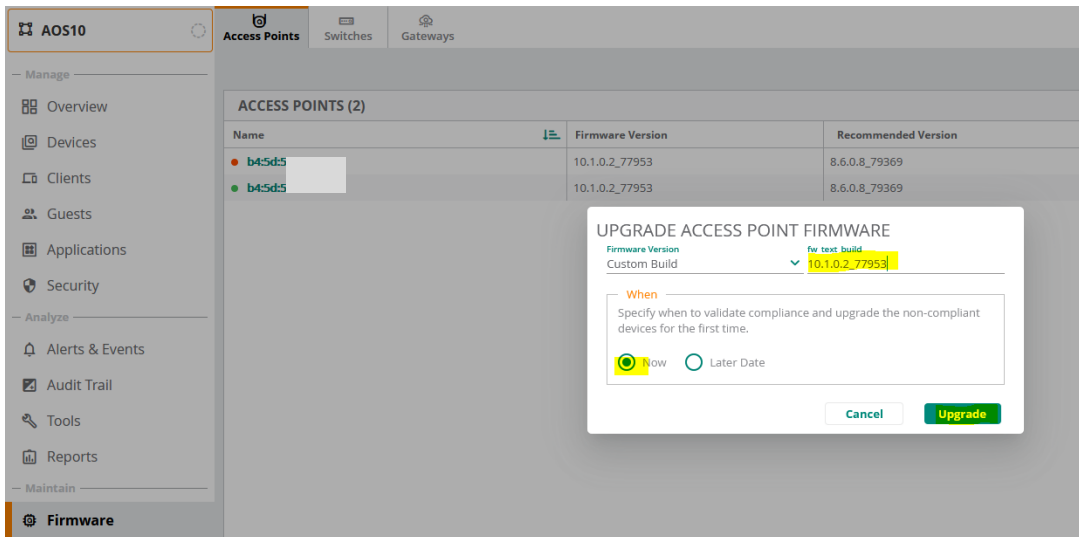
```
Enter System name [Aruba7005]: 7005-1
Enter Switch Role (standalone|md) [md]:
Enter IP type to terminate IPsec tunnel (ipv4|ipv6) [ipv4]:
Enter Master switch IP address/FQDN or ACP IP address/FQDN: device-
apacsouth.central.arubanetworks.com
Enter Master switch type(MM|ACP) ACP
Enter Uplink Vlan ID [1]:192
Enter Uplink port [GE 0/0/0]:
Enter Uplink port mode (access|trunk) [access]:
Enter Uplink Vlan IP assignment method (dhcp|static|pppoe) [static]:
Enter Uplink Vlan Static IP address [172.16.0.254]: 192.168.1.243
Enter Uplink Vlan Static IP netmask [255.255.255.0]:
Enter IP default gateway [none]: 192.168.1.1
Enter DNS IP address [none]: 192.168.1.1
Do you wish to configure IPV6 address on vlan (yes|no) [yes]: no
Do you want to configure dynamic port-channel (yes|no) [no]:
Enter Country code (ISO-3166), <ctrl-I> for supported list: AU
You have chosen Country code AU for Australia (yes|no)? : yes
Enter the controller's IANA Time zone [America/Los_Angeles]: Australia/Melbourne
Enter Time in UTC [12:53:36]:
Enter Date (MM/DD/YYYY) [12/3/2021]:
Do you want to create admin account (yes|no) [yes]:
Enter Password for admin login (up to 32 chars): *****
Re-type Password for admin login: *****
```

<omitted the other lines>

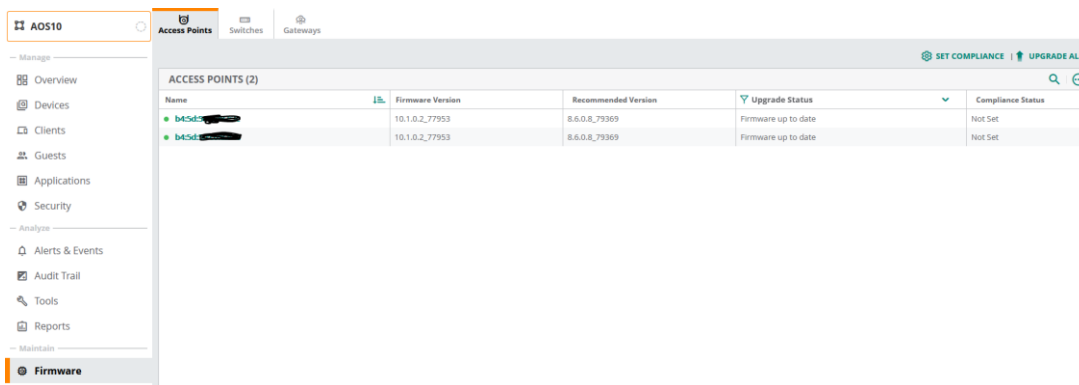
System will now restart!

```
[12:55:07]:Starting rebootme
[12:55:07]:Shutdown processing started
```

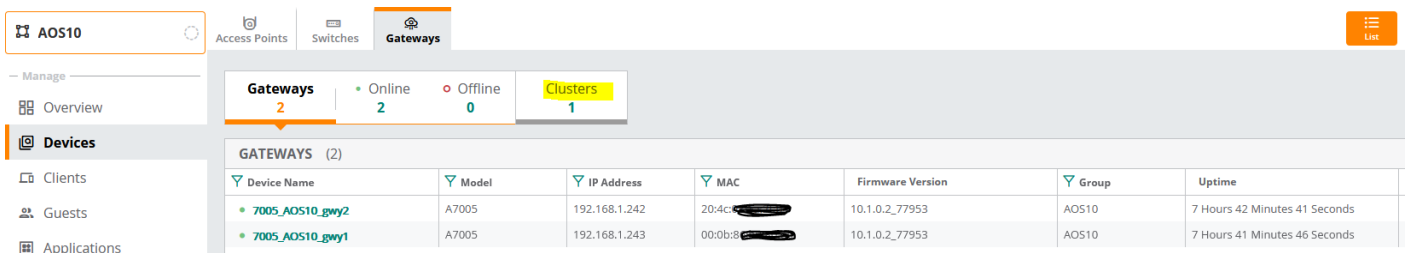
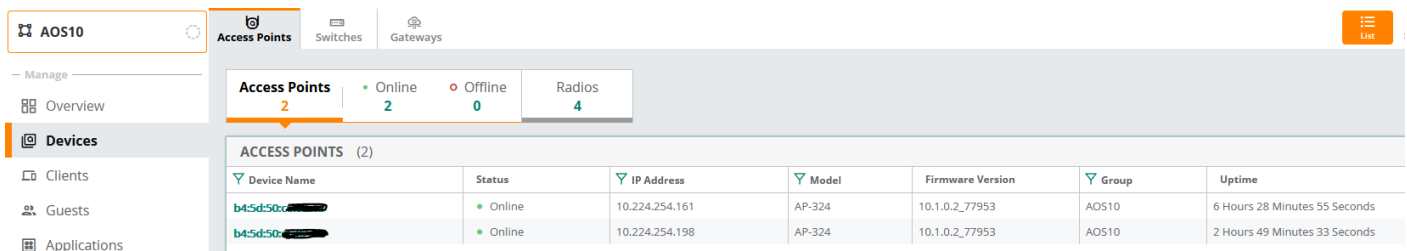
Once the APs and gateways are online in Aruba Central, we'll upgrade them to AOS10 image. In the next release SD-branch and AOS10 firmware will merge. I have already upgraded my APs, but this is how you can do it.



We'll use the same firmware version for the gateways as well.



Here we'll check to see if the APs and gateways are online with the correct firmware



Notice that there is one gateway cluster. The cluster will automatically be formed between gateways on the network using their system IP addresses.

4.6 Gateway Cluster

Cluster is a combination of multiple MDs working together to provide high availability to all the clients and ensure service continuity when a failover occurs. The gateways need not be identical and can be either L2- connected or L3- connected with a mixed configuration. In case of failover, the client SSO works for the L2- connected managed devices and the clients are de-authenticated for L3-connected managed devices in a cluster.

The aims of clustering are

- seamless Campus Roaming: When a client roams between APs of different managed devices within a large L2 domain, the client retains the same subnet and IP address to ensure seamless roaming. The clients remain anchored to a single managed device in a cluster throughout their roaming area which makes their roaming experience seamless because their L2 or L3 information and sessions remain on the same managed device.
- Hitless Client Failover: When a managed device fails, all the users fail over to their standby managed device seamlessly without any disruption to their wireless connectivity or existing high-value sessions.
- Client and AP Load Balancing: When there is excessive workload among the managed devices, the client and AP load is evenly balanced among the cluster members. Both clients and APs are load balanced seamlessly.

4.7 Monitoring Gateway Cluster

Here is how to check the gateway cluster

Name	Group	AP Tunnel	Clients	Model	Site	Version	Hitless Failover	Max Gateway Failover
auto_gwcluster_178_0 (2)	AOS10	4	2	A7005		10.1.0.2_77953	POSSIBLE	1

Gateway Name	AP Tunnel	Clients	Model	Site	Version	MAC Address	IP Address
7005_AOS10_gwy1	2	1	A7005		10.1.0.2_77953	00:0b:86:b8:80:d0	192.168.1.243
7005_AOS10_gwy2	2	1	A7005		10.1.0.2_77953	20:4c:03:1a:2fb4	192.168.1.242

CLUSTER INFO

CLUSTER NAME	CLUSTER CLIENT CAPACITY	VLAN MISMATCH	CURRENT LEADER VERSION
auto_gwcluster_178_0	4096	Yes	10.1.0.2_77953
MAX GATEWAY FAILURE WITHSTAND COUNT	SITE		
1	-		

CLIENT CAPACITY

7005_AOS10_GWY1: 100% (Active)

7005_AOS10_GWY2: 100% (Active)

Gateway Name	IP Address	Status	Client Capacity (Active Standby)	Model	Role	Version
7005_AOS10_gwy1	192.168.1.243	Up	1 (0 1)	A7005	Member	10.1.0.2_77953
7005_AOS10_gwy2	192.168.1.242	Up	1 (1 0)	A7005	Leader	10.1.0.2_77953

GATEWAY PEER DETAIL (2)

Type	IP Address	Status	Role	VLAN Mismatch
SELF	192.168.1.243	-	Member	-
PEER	192.168.1.242	Connected	Leader	1

auto_gwcluster_1...

Summary Gateways Tunnels

Manage

Overview

Analyze

Alerts & Events

Audit Trail

GATEWAY CLUSTER DETAILS

TUNNEL DOWN - SUMMARY

AP Name	IP Address	Last Connected	Last Key Recd By AP	Last Key Recd By Gateway	Reason	Gateway Name
No data to display right now						

GATEWAYS | 7005_AOS10_GWY1

TUNNEL DETAILS

AP Name	IP Address	SSID	Status	Uptime	Last Key Recd By Gateway	Last Key Recd By AP
b45d-50c6-823c	10.224.254.198	school	Up	15 Mins 41 Secs	15 Mins: 47 Secs ago	
b45d-50c6-824a	10.224.254.161	school	Up	15 Mins 42 Secs	15 Mins: 47 Secs ago	

Here is the CLI command to check the operation of the cluster.

```
(7005_AOS10_gwy1) #show lc-cluster group-membership

Cluster Enabled, Profile Name = "auto_gwcluster_178_0"
Heartbeat Threshold = 900 msec
Cluster Info Table
-----
Type IPv4 Address      Priority Connection-Type STATUS
-----
self   192.168.1.243       128      N/A CONNECTED (Member)
peer   192.168.1.242       128      L2-Connected CONNECTED (Leader)

(7005_AOS10_gwy1) #show lc-cluster load distribution client

Cluster Load Distribution for Clients
-----
Type IPv4 Address      Active Clients Standby Clients
-----
self   192.168.1.243       0            1
peer   192.168.1.242       1            0
Total: Active Clients 1 Standby Clients 1

(7005_AOS10_gwy1) #
(7005_AOS10_gwy1) #show lc-cluster load distribution ap

Cluster Load Distribution for APs
-----
Type IPv4 Address      Active APs      Standby APs
-----
self   192.168.1.243       1              1
peer   192.168.1.242       1              1
Total: Active APs 2 Standby APs 2

(7005_AOS10_gwy1) #
```

Now checking the second gateway. Note we have 1x client and 2x APs that are connected.

```
(7005_AOS10_gwy2) #show lc-cluster group-membership

Cluster Enabled, Profile Name = "auto_gwcluster_178_0"
Heartbeat Threshold = 900 msec
Cluster Info Table
-----
Type IPv4 Address      Priority Connection-Type STATUS
-----
peer   192.168.1.243       128      L2-Connected CONNECTED (Member)
self   192.168.1.242       128      N/A CONNECTED (Leader)

(7005_AOS10_gwy2) #
(7005_AOS10_gwy2) #
(7005_AOS10_gwy2) #show lc-cluster load distribution client
```

Cluster Load Distribution for Clients

```
-----
Type IPv4 Address      Active Clients Standby Clients
-----
peer   192.168.1.243          0             1
self   192.168.1.242          1             0
Total: Active Clients 1 Standby Clients 1
```

(7005_AOS10_gwy2) #

(7005_AOS10_gwy2) #show lc-cluster load distribution ap

Cluster Load Distribution for APs

```
-----
Type IPv4 Address      Active APs      Standby APs
-----
peer   192.168.1.243          1             1
self   192.168.1.242          1             1
Total: Active APs 2 Standby APs 2
```

(7005_AOS10_gwy2) #

5 ClearPass Initial Configuration

Here we'll do the basic ClearPass configuration and join it to the AD domain along with creation of dot1x service policy. We'll start with NTP and time zone.

Administration » Server Manager » Server Configuration

Server Configuration

Change Cluster Password
Cluster-Wide Parameters
Clear Machine Authentication Cache
Make Subscriber
Manage Policy Manager Zones
NetEvents Targets
Set Date & Time
Virtual IP Settings

Publisher Server: victory [192.168.1.95]

#	Server Name	Management Port	Data Port	Zone	Cluster Sync	Last Sync Time
1.	victory	(IPv4) 192.168.1.95	-	default	Enabled	-

Showing 1-1 of 1

Collect Logs Back Up Restore Cleanup Shutdown Reboot

Change Date and Time

This will change Date & Time for all nodes in the cluster:

Date & Time

Time Zone on Publisher

☒ Synchronize time with NTP server

Primary Server:

NTP Server	<input type="text" value="216.239.35.4"/>
Key ID	<input type="text"/>
Key Value	<input type="text"/>
Algorithm	<input type="text"/>

Secondary Server (1):

NTP Server	<input type="text"/>
Key ID	<input type="text"/>
Key Value	<input type="text"/>
Algorithm	<input type="text"/>

WARNING: After command execution, Policy Manager services will be restarted. This may take a few minutes.

Save

Cancel

Change Date and Time

This will change Date & Time for all nodes in the cluster:

Date & Time

Time Zone on Publisher

To change the time zone, select your area from the list below:

<input type="text" value="Africa/Abidjan"/>
Africa/Accra
Africa/Addis_Ababa
Africa/Algiers
Africa/Asmara
Africa/Asmera
Africa/Bamako
Africa/Bangui
Africa/Banjul
Africa/Bissau

Current time zone: Australia/Melbourne(GMT +11:00)

WARNING: After command execution, Policy Manager services will be restarted. This may take a few minutes.

Save

Cancel

Administration » Server Manager » Server Configuration - victory

Server Configuration - victory (192.168.1.95)

System Services Control Service Parameters System Monitoring Network FIPS

Hostname:

FQDN:

Policy Manager Zone: Manage Policy

Enable Performance Monitoring Display: ☒ Enable this server for performance monitoring display

Insight Setting: ☒ Enable Insight ☐ Enable as Insight Master Current Master: -

Enable Ingress Events Processing: ☐ Enable Ingress Events processing on this server

Master Server in Zone:

Span Port:

	IPv4	IPv6	Action
Management Port	IP Address	192.168.1.95	Configure
	Subnet Mask	255.255.255.0	
	Default Gateway	192.168.1.249	
Data/External Port	IP Address		Configure
	Subnet Mask		
	Default Gateway		
DNS Settings	Primary	192.168.1.250	Configure
	Secondary	192.168.1.130	
	Tertiary		
	DNS Caching	Disabled	

AD Domains:

5.1 Joining AD Domain

Configure the IP addresses and the rest as per your Lab setup but ensure you have the IP address of your domain controller as the primary DNS. CPPM needs to join the AD domain, in order to authenticate against it. Make sure the clock time for AD and CPPM are almost in sync. It is best to use NTP. If they are not in sync, then CPPM will not be able to join the domain. When you click on the “join domain” button, you need to provide the FQDN of the DC and that’s why you need the DNS entry to resolve the name of your domain controller.

Policy Manager Zone: default [Manage Policy Manager Zones](#)

Enable Prof... **Join AD Domain**

Enter the FQDN of the controller and the short (NETBIOS) name for the domain:

Domain Controller: wlan-dc.wlan.net

NetBIOS Name: WLAN

In case of a controller name conflict

- ☒ Use specified Domain Controller
- ☐ Use Domain Controller returned by DNS query
- ☐ Fail on conflict

☒ Use default domain admin user [Administrator]

Username: []

Password: []

Save **Cancel**

AD Domains: Policy Manager is not part of any domain. Join to domain here. **Join AD Domain**

Join AD Domain

Adding host to AD domain

Adding host to AD domain...

INFO - Fetched REALM 'WLAN.NET' from domain FQDN 'wlan-dc.wlan.net'

INFO - Fetched the NETBIOS name 'WLAN'

INFO - Creating domain directories for 'WLAN'

INFO - Using Administrator as the WLAN-DC's username

Enter Administrator's password:

Using short domain name -- WLAN

Joined 'CP63LAB' to dns domain 'wlan.net'

INFO - Creating service scripts for 'WLAN'

Starting cpass-domain-server_WLAN: [OK]

Close

Join AD Domain

Added host to the domain

INFO - Creating service scripts for 'WLAN'

Starting cpass-domain-server_WLAN: [OK]

INFO - updating domain configuration files

Stopping cpass-domain-server_WLAN: [OK]

[OK]

Starting cpass-domain-server_WLAN: [OK]

Stopping cpass-sysmon-server: [OK]

Starting cpass-sysmon-server: [OK]

Stopping cpass-radius-server: [OK]

Starting cpass-radius-server: [OK]

INFO - CP63Lab joined the domain WLAN.NET

Close

Now we need to add the AD as authentication source

Dashboard

Monitoring

Configuration

- Service Templates & Wizards
- Services
- Authentication
 - Methods
 - Sources**
- Identity
 - Single Sign-On (SSO)
 - Local Users
 - Endpoints
 - Static Host Lists
 - Roles
 - Role Mappings
- Posture
- Enforcement
- Network
 - Network Scan
 - Policy Simulation

Configuration » Authentication » Sources » Add - Ariya AD

Authentication Sources - Ariya AD

Summary **General** **Primary** **Attributes**

Name: Ariya AD

Description: []

Type: Active Directory

Use for Authorization: ☒ Enable to use this Authentication Source to also fetch role mapping attributes

Authorization Sources: [] **Remove** **View Details**

-- Select --

Server Timeout: 10 seconds

Cache Timeout: 36000 seconds

Backup Servers Priority: [] **Move Up ↑** **Move Down ↓** **Add Backup** **Remove**

Dashboard

Monitoring

Configuration

Service Templates & Wizards

Services

Authentication

Methods

Sources

Identity

Single Sign-On (SSO)

Local Users

Endpoints

Static Host Lists

Roles

Role Mappings

Posture

Enforcement

Network

Network Scan

Policy Simulation

Configuration » Authentication » Sources » Add - Ariya AD

Authentication Sources - Ariya AD

SummaryGeneralPrimaryAttributes

Connection Details

Hostname:192.168.1.250

Connection Security:None

Port:389 (For secure connection, use 636)

Verify Server Certificate:☒ Enable to verify Server Certificate for secure connection

Bind DN:administrator@wlan.net (e.g. administrator@example.com OR cn=administrator,cn=users,dc=example,dc=com)

Bind Password:••••••••

NetBIOS Domain Name:WLAN

Base DN:dc=wlan,dc=net Search Base Dn

Search Scope:SubTree Search

LDAP Referrals:☐ Follow referrals

Bind User:☒ Allow bind using user password

User Certificate:userCertificate

Always use NetBIOS name:☐ Enable to always use NetBIOS name instead of the domain part in username for authentication

Special Character Handling for LDAP Query:☒ Enabled ☐ Disabled

Dashboard

Monitoring

Configuration

Service Templates & Wizards

Services

Authentication

Methods

Sources

Identity

Single Sign-On (SSO)

Local Users

Endpoints

Static Host Lists

Roles

Role Mappings

Posture

Enforcement

Network

Network Scan

Policy Simulation

Configuration » Authentication » Sources » Add - Ariya AD

Authentication Sources - Ariya AD

SummaryGeneralPrimaryAttributes

Specify filter queries used to fetch authentication and authorization attributes

	Filter Name	Attribute Name	Alias Name	Enabled As
1.		dn	UserDN	-
		department	Department	-
		title	Title	-
		company	company	-
	Authentication	memberOf	memberOf	-
		telephoneNumber	Phone	-
		mail	Email	-
		displayName	Name	-
		accountExpires	Account Expires	-
2.	Group	cn	Groups	-
3.		dNSHostName	HostName	-
	Machine	operatingSystem	OperatingSystem	-
		operatingSystemServicePack	OSServicePack	-
4.	Onboard Device Owner	memberOf	Onboard memberOf	-
5.	Onboard Device Owner Group	cn	Onboard Groups	-

5.2 ClearPass dot1x Service

Here we create a dot1x service for wireless access.

aruba

ClearPass Policy Manager

Menu

Dashboard

Monitoring

Configuration

Service Templates & Wizards

Services

Authentication

Methods

Sources

Identity

Single Sign-On (SSO)

Local Users

Endpoints

Static Host Lists

Roles

Role Mappings

Posture

Configuration » Services

Services

Add

Import

Export All

This page shows the current list and order of services that ClearPass follows during authentication and authorization.

Filter: (Name) contains Go Clear Filter Show 20 records

#	Order	Name	Type	Template	Status
1.	<input type="checkbox"/>	1 [Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	
2.	<input type="checkbox"/>	2 [AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	
3.	<input type="checkbox"/>	3 [Aruba Device Access Service]	TACACS	TACACS+ Enforcement	
4.	<input type="checkbox"/>	4 [Guest Operator Logins]	Application	Aruba Application Authentication	
5.	<input type="checkbox"/>	5 [Insight Operator Logins]	Application	Aruba Application Authentication	
6.	<input type="checkbox"/>	6 [Device Registration Disconnect]	WEBAUTH	Web-based Authentication	
7.	<input type="checkbox"/>	7 AA Aruba 802.1X Wireless	RADIUS	Aruba 802.1X Wireless	

Summary

Service

Authentication

Roles

Enforcement

Name:AA Aruba 802.1X Wireless

Description:To authenticate users to an Aruba Wireless network via 802.1X.

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:Aruba	Aruba-Essid-Name	EQUALS	school
4.	Click to add...		

“school” is the name of the SSID

Summary	Service	Authentication	Roles	Enforcement
Authentication Methods: <div> <div>[EAP PEAP] [EAP TLS]</div> <div> Move Up ↑ Move Down ↓ Remove View Details Modify </div> </div> <div>--Select to Add--</div>				
Authentication Sources: <div> <div>Ariya AD [Active Directory]</div> <div> Move Up ↑ Move Down ↓ Remove View Details Modify </div> </div> <div>--Select to Add--</div>				
Strip Username Rules: <input type="checkbox"/> Enable to specify a comma-separated list of rules to strip username prefixes or suffixes				
Service Certificate: <div>--Select to Add--</div>				

Summary	Service	Authentication	Roles	Enforcement								
Role Mapping Policy: <div>--Select--</div> Modify Add New Role Mapping Policy												
Role Mapping Policy Details												
Description: -												
Default Role: -												
Rules Evaluation Algorithm: -												
<table border="1"> <thead> <tr> <th>Conditions</th> <th>Role</th> </tr> </thead> <tbody> <tr><td> </td><td> </td></tr> <tr><td> </td><td> </td></tr> <tr><td> </td><td> </td></tr> </tbody> </table>					Conditions	Role						
Conditions	Role											

Summary	Service	Authentication	Roles	Enforcement										
Use Cached Results: <input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions														
Enforcement Policy: <div>AA Aruba 802.1X Wireless Enforcement Policy</div> Modify Add New Enforcement Policy														
Enforcement Policy Details														
Description: -														
Default Profile: AA Aruba 802.1X Wireless Default Profile														
Rules Evaluation Algorithm: first-applicable														
<table border="1"> <thead> <tr> <th>Conditions</th> <th>Enforcement Profiles</th> </tr> </thead> <tbody> <tr> <td>1. (Authorization:Ariya AD:memberOf CONTAINS Staff)</td> <td>AA-Aruba 802.1X Wireless Staff Profile, AA Aruba 802.1X Wireless Update Endpoint Location</td> </tr> <tr> <td>2. (Authorization:Ariya AD:memberOf CONTAINS Student)</td> <td>AA-Aruba 802.1X Wireless Student Profile, AA Aruba 802.1X Wireless Update Endpoint Location</td> </tr> <tr> <td>3. (Tips:Role EQUALS [Machine Authenticated]) AND (Authorization:Ariya AD:memberOf CONTAINS Staff)</td> <td>AA-Aruba 802.1X Wireless Staff Profile, [Update Endpoint Known]</td> </tr> <tr> <td>4. (Tips:Role EQUALS [Machine Authenticated]) AND (Authorization:Ariya AD:memberOf CONTAINS Student)</td> <td>AA-Aruba 802.1X Wireless Student Profile, [Update Endpoint Known]</td> </tr> </tbody> </table>					Conditions	Enforcement Profiles	1. (Authorization:Ariya AD:memberOf CONTAINS Staff)	AA-Aruba 802.1X Wireless Staff Profile, AA Aruba 802.1X Wireless Update Endpoint Location	2. (Authorization:Ariya AD:memberOf CONTAINS Student)	AA-Aruba 802.1X Wireless Student Profile, AA Aruba 802.1X Wireless Update Endpoint Location	3. (Tips:Role EQUALS [Machine Authenticated]) AND (Authorization:Ariya AD:memberOf CONTAINS Staff)	AA-Aruba 802.1X Wireless Staff Profile, [Update Endpoint Known]	4. (Tips:Role EQUALS [Machine Authenticated]) AND (Authorization:Ariya AD:memberOf CONTAINS Student)	AA-Aruba 802.1X Wireless Student Profile, [Update Endpoint Known]
Conditions	Enforcement Profiles													
1. (Authorization:Ariya AD:memberOf CONTAINS Staff)	AA-Aruba 802.1X Wireless Staff Profile, AA Aruba 802.1X Wireless Update Endpoint Location													
2. (Authorization:Ariya AD:memberOf CONTAINS Student)	AA-Aruba 802.1X Wireless Student Profile, AA Aruba 802.1X Wireless Update Endpoint Location													
3. (Tips:Role EQUALS [Machine Authenticated]) AND (Authorization:Ariya AD:memberOf CONTAINS Staff)	AA-Aruba 802.1X Wireless Staff Profile, [Update Endpoint Known]													
4. (Tips:Role EQUALS [Machine Authenticated]) AND (Authorization:Ariya AD:memberOf CONTAINS Student)	AA-Aruba 802.1X Wireless Student Profile, [Update Endpoint Known]													

And here are the enforcement profiles that are being used in the enforcement policy

- AA Aruba 802.1X Wireless Default Profile RADIUS
- AA-Aruba 802.1X Wireless Staff Profile RADIUS
- AA-Aruba 802.1X Wireless Student Profile RADIUS
- AA Aruba 802.1X Wireless Update Endpoint Location Post_Authentication

Enforcement Profiles - AA Aruba 802.1X Wireless Default Profile

Note: This Enforcement Profile is created by Service Template

Summary	Profile	Attributes
Profile:		
Name:	AA Aruba 802.1X Wireless Default Profile	
Description:		
Type:	RADIUS	
Action:	Accept	
Device Group List:	-	
Attributes:		
Type	Name	Value
1. Radius:Aruba	Aruba-User-Role	= Employee

Enforcement Profiles - AA-Aruba 802.1X Wireless Staff Profile

Note: This Enforcement Profile is created by Service Template

Summary Profile Attributes

Profile:

Name:	AA-Aruba 802.1X Wireless Staff Profile
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

Type	Name	Value
1. Radius:Aruba	Aruba-User-Role	= Staff

Enforcement Profiles - AA-Aruba 802.1X Wireless Student Profile

Note: This Enforcement Profile is created by Service Template

Summary Profile Attributes

Profile:

Name:	AA-Aruba 802.1X Wireless Student Profile
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

Type	Name	Value
1. Radius:Aruba	Aruba-User-Role	= Student

Enforcement Profiles - AA Aruba 802.1X Wireless Update Endpoint Location

Note: This Enforcement Profile is created by Service Template

Summary Profile Attributes

Profile:

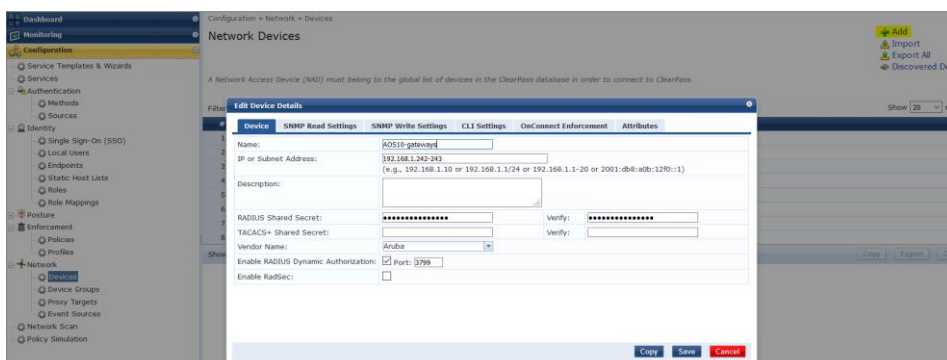
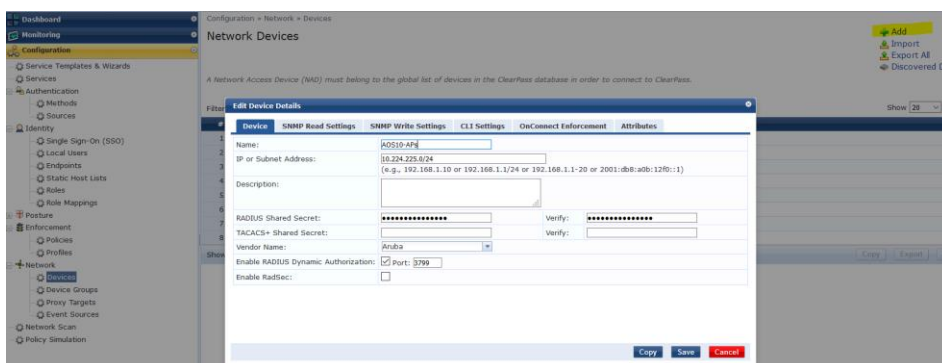
Name:	AA Aruba 802.1X Wireless Update Endpoint Location
Description:	
Type:	Post_Authentication
Action:	
Device Group List:	-

Attributes:

Type	Name	Value
1. Endpoint	Last Known Location	= %{Radius:IETF:NAS-IP-Address};%{Radius:Aruba:Aruba-Location-Id}

5.3 NAD Configuration

Here we are adding Network Access Devices (NAD). This will be the AOS10 APs and gateways. Note that you need to either add the AP IP addresses individually or just add their subnet as I have done here.



6 WLAN Configuration

Here we'll configure the AOS10 APs to broadcast a tunnelled SSID. This is done at the group level.

6.1 Tunnelled Wireless Configuration

The screenshot shows the AOS10 configuration interface. On the left, there is a sidebar with 'Manage' and 'Analyze' sections. The 'Manage' section includes 'Overview', 'Devices', 'Clients', 'Guests', 'Applications', 'Security', 'Alerts & Events', 'Audit Trail', and 'Tools'. The 'Analyze' section includes 'Alerts & Events', 'Audit Trail', and 'Tools'. The main content area is titled 'Wireless SSIDs' and contains a table with columns: DISPLAY NAME, OPMODE, ACCESS_TYPE, VLAN FORWARDING MODE, and ACTIONS. The table is empty, and a 'No data to display' message is shown. Below the table, there is a '+ Add SSID' button. The top navigation bar includes 'Access Points', 'Switches', and 'Gateways' tabs. The bottom navigation bar includes 'WLANs', 'Access Points', 'Radios', 'Interfaces', 'Security', 'Services', 'System', and 'Configuration Audit' tabs. The 'WLANs' tab is selected.

You can choose the cluster from the menu. Also note that the VLAN IDs are being displayed from the gateways.

The screenshot shows the AOS10 configuration interface with the 'CREATE A NEW NETWORK' wizard. The wizard has five steps: 1. General, 2. VLANs, 3. Security, 4. Access, and 5. Summary. The 'VLANs' step is currently selected. The 'Traffic forwarding mode' is set to 'Tunnel'. The 'Primary Gateway Cluster' is set to 'AOS10_auto_gwcluster_178-0'. The 'Secondary Gateway Cluster' is set to 'None'. The 'Client VLAN Assignment' is set to 'Static'. The 'VLAN ID' is set to '192'. The 'Show Named VLANs' link is visible. The bottom navigation bar includes 'WLANs', 'Access Points', 'Radios', 'Interfaces', 'Security', 'Services', 'System', and 'Configuration Audit' tabs. The 'WLANs' tab is selected.

Select the authentication server that we had configured on the gateways. It gets automatically populated using the drop down menu. Note that this is not the RADIUS server that we configured in the AP group but rather from the gateway group. Next select Accounting from the advance Setting section

The first screenshot shows the 'Advanced Settings' section for a configuration. The 'Accounting' section is highlighted, and the 'Use authentication servers' dropdown menu is set to 'Use authentication servers'.

The second screenshot shows the 'Advanced Settings' section for a configuration. The 'Accounting' section is highlighted, and the 'Use authentication servers' dropdown menu is set to 'Use authentication servers'. The 'Accounting Interval' is set to 1 min.

The screenshot shows the 'Access rules' section for a specific configuration. The 'Role Based' tab is selected, and the 'school' role is listed. The 'Access rules for selected roles' section shows a rule that allows access to all destinations.

And save the configuration.

The screenshot shows a success message dialog box with the text 'SUCCESS' and 'school is configured Successfully'. The 'OK' button is visible.

6.2 Wireless dot1x Testing

First, we'll check the gateway authentication server configuration, the highlighted lines were pushed from the AP's tunnel configuration.

The screenshot shows the Aruba NetworkOS Gateway configuration interface. The left sidebar contains navigation options like Overview, Devices, Clients, Guests, Applications, Security, Alerts & Events, Audit Trail, Tools, Reports, and Firmware. The main content area is titled 'Authentication Servers' and contains two tables.

Server groups table:

NAME	SERVERS	FAIL THROUGH	LOAD BALANCE	SERVER RULES
school_#1615532079504_41#_acct_svg	1	--	--	0
school_#1615532079504_41#_auth_svg	1	--	--	0
school_#1615532079504_41#_cp_svg	1	--	--	0

All servers table:

NAME	TYPE	IP ADDRESS / HOSTNAME	SERVER GROUP
ClearPass-GW	Radius	192.168.1.95	school_#1615532079504_41#_acct_svg
--	RFC 3576	192.168.1.95	--

Now we'll get a laptop to connect to "school" SSID with staff1 user credentials and check ClearPass access tracker

The screenshot shows the ClearPass Policy Manager Access Tracker interface. The left sidebar contains navigation options like Dashboard, Monitoring, Live Monitoring, Access Tracker, Accounting, OnGuard Activity, Analysis & Trending, System Monitor, Profiler and Network Scan, Audit Viewer, and Event Viewer. The main content area is titled 'Access Tracker' and shows a table of access requests.

Access Tracker Table:

#	Server	Source	Username	Service	Login Status	Request Timestamp
1.	192.168.1.95	RADIUS	staff1	AA Aruba 802.1X Wireless	ACCEPT	2021/03/12 17:58:39

Note that 192.168.1.242 is the IP address of the gateway-1 and 10.224.254.161 is the IP address of the AP.

The screenshot shows the ClearPass Policy Manager Request Details interface. The left sidebar contains navigation options like Summary, Input, Output, and Accounting. The main content area is titled 'Request Details' and shows a table of session information.

Request Details Table:

Field	Value
Login Status:	ACCEPT
Session Identifier:	R00000006-01-604b111f
Date and Time:	Mar 12, 2021 17:58:39 AEDT
End-Host Identifier:	A0-88-B4-50-C0-84 (Computer / Windows / Windows)
Username:	staff1
Access Device IP/Port:	192.168.1.242
Access Device Name:	10.224.254.161
System Posture Status:	UNKNOWN (100)

Policies Used -

Field	Value
Service:	AA Aruba 802.1X Wireless
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2
Authentication Source:	AD:192.168.1.250
Authorization Source:	Ariya AD
Roles:	[User Authenticated]
Enforcement Profiles:	AA Aruba 802.1X Wireless Update Endpoint Location, AA-Aruba 802.1X Wireless

Showing 1 of 1-7 records. Buttons: Change Status, Show Configuration, Export, Show Logs, Close.

Request Details	
Summary	Input
Enforcement Profiles:	AA Aruba 802.1X Wireless Update Endpoint Location, AA-Aruba 802.1X Wireless Staff Profile
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)
RADIUS Response	
Endpoint: Last Known Location	192.168.1.242:b4:5d:50:c6:82:4a
Radius: Aruba:Aruba-User-Role	Staff

◀ Showing 1 of 1-7 records ▶ | [Change Status](#) [Show Configuration](#) [Export](#) [Show Logs](#) [Close](#)

And we also have the accounting tab, which indicates RADIUS accounting is working

Request Details	
Summary	Input
Account Session ID:	B45D50E824B0-A088B450C084-604B111F-EA565
Start Timestamp:	Mar 12, 2021 17:58:39 AEDT
End Timestamp:	Still Active
Status:	Active
Termination Cause:	-
Service Type:	-
Number of Authentication Sessions:	1
Network Details	
Utilization	
Authentication Sessions Details	

◀ Showing 1 of 1-7 records ▶ | [Change Status](#) [Show Configuration](#) [Export](#) [Show Logs](#) [Close](#)

Lastly, we need to test if CoA is working, click on the “change status” to terminate the session

Request Details	
Access Control Capabilities -	
Select Access Control Type :	<input type="radio"/> Agent <input type="radio"/> SNMP <input checked="" type="radio"/> RADIUS CoA <input type="radio"/> Server Action
RADIUS CoA Type:	[ArubaOS Wireless - Terminat ▼]

[Submit](#) [Cancel](#)

Request Details	
Radius [ArubaOS Wireless - Terminate Session] successful for client a088b450c084.	
Summary	Input
Account Session ID:	B45D50E824B0-A088B450C084-604B111F-EA565
Start Timestamp:	Mar 12, 2021 17:58:39 AEDT
End Timestamp:	Still Active
Status:	Active
Termination Cause:	-
Service Type:	-
Number of Authentication Sessions:	1
Network Details	
Utilization	
Authentication Sessions Details	

Showing 1 of 1-7 records
Change Status
Show Configuration
Export
Show Logs
Close

Now looking at Aruba Central pages.

AOS10

Manage

Overview

Devices

Clients

Guests

Applications

Security

Clients

244.08 MB (8.04 MB | 236.05 MB)

All 1

Connecting 0

Connected 1

Failed 0

Offline 0

Blocked 0

Wireless 1

Wired 0

Remote 0

Client Name	Status	IP Address	VLAN	Connected To	Gateway Role	SSID/Port	Health	Usage
staff1	Connected	10.10.44.50	44	b45d50:c6:824a	Staff	school		244.08 MB

staff1

Manage

Overview

Applications

Live Events

Events

Tools

Summary

AI Insights

Location

Sessions

CLIENT DETAILS

DATA PATH

CLIENT

staff1

CONNECTED

SSID

school

UP

AP

b45d50:c6:824a

UP

SWITCH

Aruba-2930F-8G-PoEP-25PPP

UP

GATEWAY

7005_AOS10_gwy2

UP

CLIENT

USERNAME

staff1

HOSTNAME

AryaP

IP ADDRESS

10.10.44.50

GLOBAL UNICAST IPV6 ADDRESS

CLIENT OS

Win10

MANUFACTURER

Intel Corporate

AI INSIGHTS

0 0 0 0

CLIENT TYPE

Wireless

MAC ADDRESS

a088b450:c084

LINK LOCAL IPV6 ADDRESS

fe80::7d4a:2f07:955c:...

CONNECTED SINCE

Mar 12, 2021, 17:58:41

ENCRYPTION

AES

NETWORK

VLAN

44

AP ROLE

Staff

GATEWAY ROLE

Staff

SEGMENTATION

AUTH SERVER

192.168.1.242

TUNNELED

VLAN DERIVATION

VSA

AP DERIVATION

RADIUS

SWITCH ROLE

DHCP SERVER

10.10.44.1

TUNNELED ID

CONNECTION

CHANNEL

149 (40 MHz)

BAND

5 GHz

CLIENT CAPABILITIES

802.11an

CLIENT MAX SPEED

600 Mbps

LEDs on ACCESS POINT (b45d50:c6:824a)

0 0 0 Blink LEDs

staff1

Manage

Overview

Applications

Live Events

Events

Tools

Visibility

Applications

Websites

APPLICATIONS

Passive Monitoring

Total Transferred: 1.4 GB

APPLICATION	CATEGORY	USAGE	SENT	RECEIVED
YouTube	Streaming	1.3 GB (93.21%)	28.0 MB	1.3 GB
TCP	Network Service	19.9 MB (1.40%)	386 KB	19.5 MB
Microsoft	Office365 SAAS	2.2 MB (0.16%)	309 KB	1.9 MB
HTTPS	Web	959 KB (0.07%)	101 KB	858 KB
Google Ads	Google SAAS	355 KB (0.02%)	72 KB	284 KB
Mozilla	Web	319 KB (0.02%)	57 KB	262 KB
Google Generic	Google SAAS	212 KB (0.01%)	110 KB	102 KB
Microsoft OneDrive	sharepoint_onedrive_saas	163 KB (0.01%)	12 KB	151 KB
Netbios Name Service	Network Service	76 KB (0.01%)	76 KB	0 B
Bing.com	Web	51 KB (0.00%)	7 KB	44 KB
Microsoft Azure	Office365 SAAS	47 KB (0.00%)	3 KB	43 KB
SOAP	Network Service	42 KB (0.00%)	42 KB	0 B
Microsoft Office 365	Office365 SAAS	35 KB (0.00%)	4 KB	31 KB
Server Message Block	Network Service	13 KB (0.00%)	13 KB	0 B
Unclassified	Unclassified	72.3 MB (5.08%)	798 KB	71.5 MB

Clicking on the gateway symbol takes us to the gateway that is terminating the user traffic



Summary Routing Sessions AI Insights

Overview

WAN LAN Device Clients Applications Security

DEVICE

NAME	SERIAL NUMBER	MODEL	MAC ADDRESS	SYSTEM IP ADDRESS	PUBLIC IP ADDRESS
7005_AOS10_gwy2	CP0031855	A7005	20:4c:03:1a:2fb4	192.168.1.242	203.63.103.176
FIRMWARE VERSION	POE (DRAW/MAx)	REDUNDANCY PEER	GROUP NAME	SITE	LABELS
10.1.0.2.77953	--	--	AOS10	--	--
UPTIME	4G/LTE MODEM STATUS	4G/LTE MODEM TYPE	NTP SERVER	CONFIG SYNC STATUS	LAST REBOOT REASON
9 hours 53 minutes	--	--	time2.google.com(Synchronized)	Update Successful	POE Power Cycle
CLUSTER NAME	auto_gwcluster_178_0				

Summary Routing Sessions AI Insights

Overview

WAN LAN Device Clients Applications Security

CLIENTS

244.08 MB (@ 8.04 MB | @ 236.05 MB)

All	Connecting	Connected	Failed	Offline	Blocked	Wireless	Wired	Remote
1	0	1	0	0	0	1	0	0

Client Name	Status	Gateway Name	Gateway Role	IP Address	Port	VLAN	Usage
staff1	Connected	7005_AOS10_gwy2	Staff	10.10.44.50	Tunneled	44	244.08 MB

Now we'll run a few CLI commands.

```
b4:5d:50:c6:82:4a# sh ap bss-table

Aruba AP BSS Table
-----
bss      ess      port  ip      phy  type  ch/EIRP/max-EIRP  cur-cl  ap name      in-t(s)  tot-t  --
flags
---
b4:5d:50:e8:24:b0  school  ???  10.224.254.161  a-VHT  ap  36E/15.0/21.5  1  b4:5d:50:c6:82:4a  0  1h:2m:16s
b4:5d:50:e8:24:b1  Guest  ???  10.224.254.161  a-VHT  ap  36E/15.0/21.5  1  b4:5d:50:c6:82:4a  0  4m:29s  o
b4:5d:50:e8:24:b2  _owetm_Guest2874425900  ???  10.224.254.161  a-VHT  ap  36E/15.0/21.5  0  b4:5d:50:c6:82:4a  0  4m:28s  WO
b4:5d:50:e8:24:a0  school  ???  10.224.254.161  g-HT  ap  3/7.5/21.5  0  b4:5d:50:c6:82:4a  0  1h:2m:15s
b4:5d:50:e8:24:a1  Guest  ???  10.224.254.161  g-HT  ap  3/7.5/21.5  0  b4:5d:50:c6:82:4a  0  4m:29s  o
b4:5d:50:e8:24:a2  _owetm_Guest2874425900  ???  10.224.254.161  g-HT  ap  3/7.5/21.5  0  b4:5d:50:c6:82:4a  0  4m:28s  WO

Channel followed by "*" indicates channel selected due to unsupported configured channel.
"Spectrum" followed by "^" indicates Local Spectrum Override in effect.

Num APs:6
Num Associations:2

Flags:      K = 802.11K Enabled; W = 802.11W Enabled; 3 = WPA3 BSS; O = Enhanced-open BSS with transition mode; o = Enhanced-open transition mode open BSS; M = WPA3-SAE mixed mode BSS; E = Enhanced-open BSS without transition mode; m = Agile Multiband (MBO) BSS; c = MBO Cellular Data Capable BSS; I = Imminent VAP Down; T = Individual TWT Enabled; t = Broadcast TWT Enabled
b4:5d:50:c6:82:4a#
```

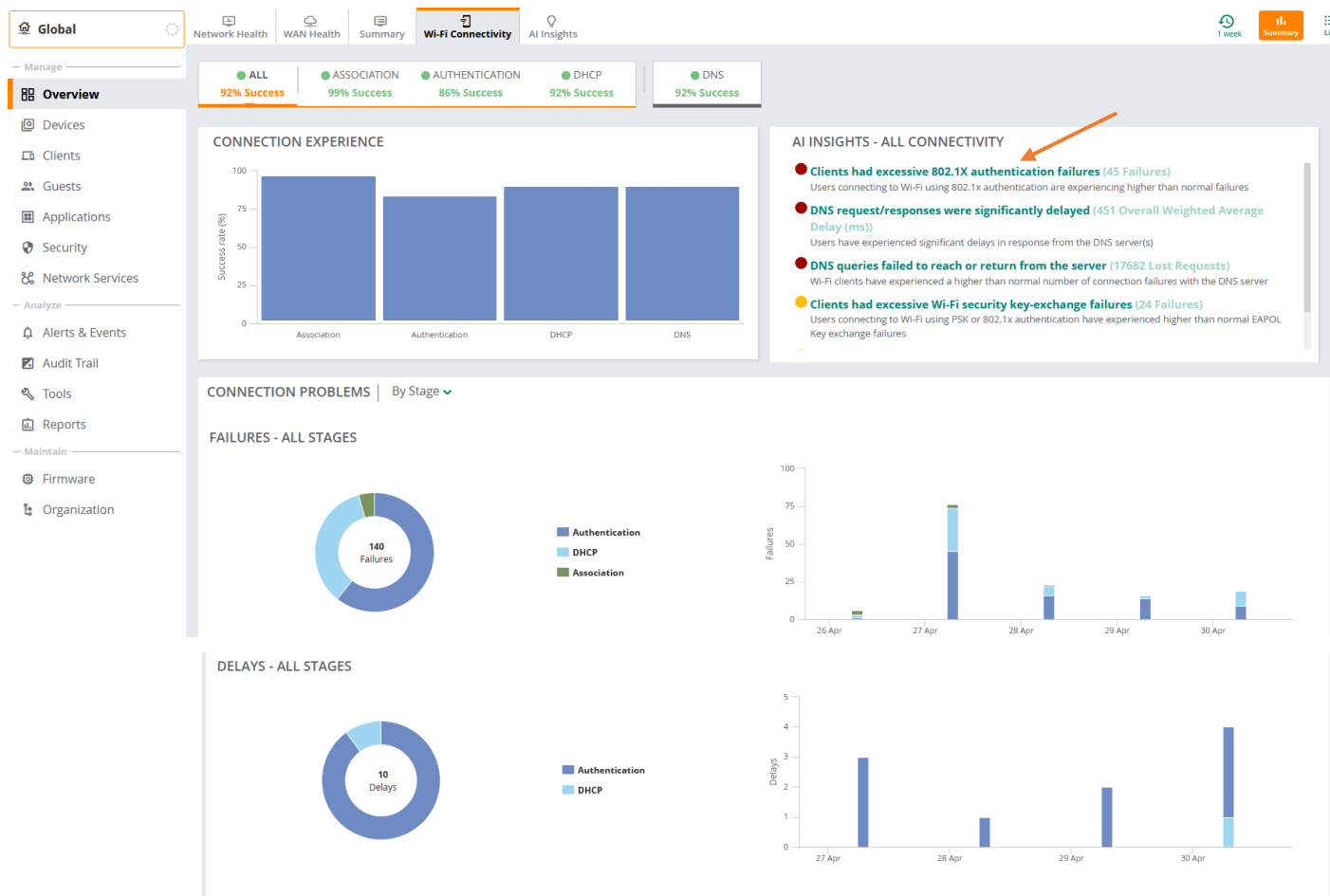
checking the IPSEC tunnels from the AP

```
b4:5d:50:c6:82:4a# sh ata endpoint

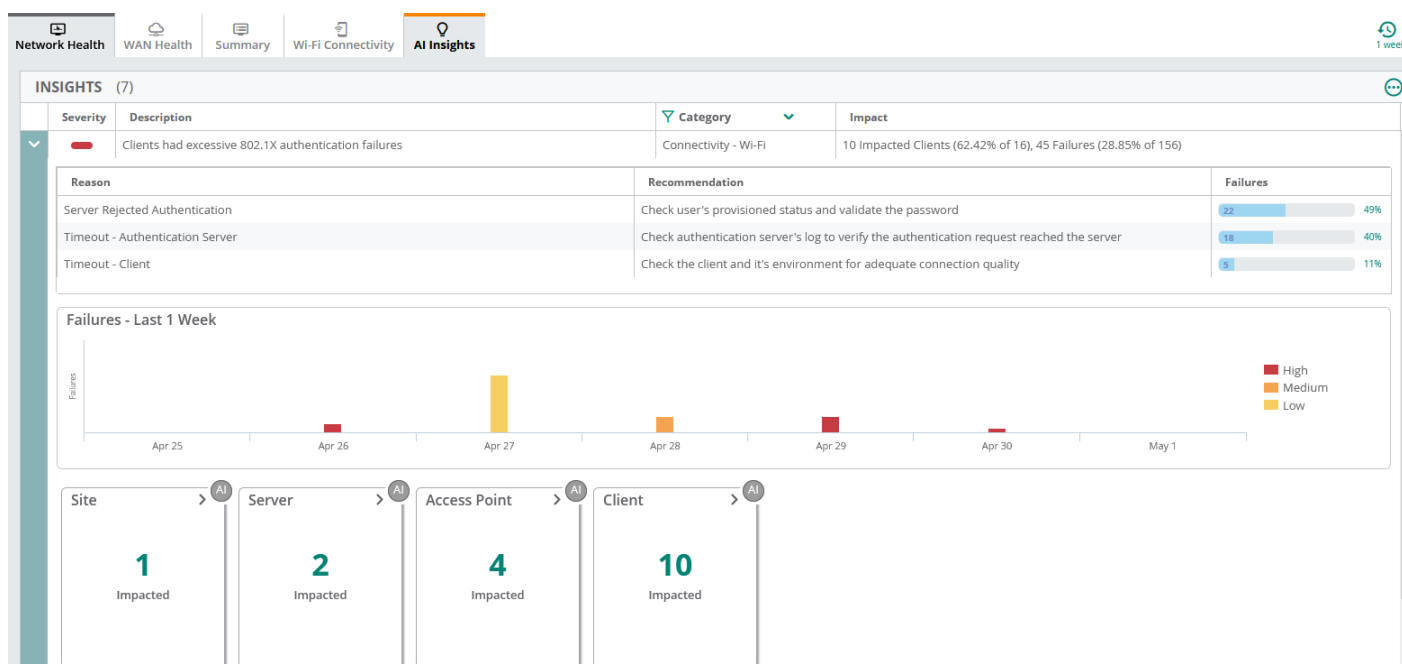
ATA Endpoint Status
-----
UUID      IP ADDR  STATE  TUN DEV  TUN SPI(OUT/IN)  PORT(SRC/DST)  VALID TIME(s)  TUNNEL TYPE
GRE VLANs  HBT(Jiff/Missed/Sent/Rcv)  INNER IP  UP TIME(s)
-----
522d59ab-05d0-43b6-ab49-177e49fb7bb0  192.168.1.242  SM STATE_CONNECTED  tun0  1ad1b900/c6d09100  4500/4500  125781  GRE
1,33,44,192,4094  3999/0/3808/3808  10.224.254.161  2021-03-13 08:28:59
5bb2c1da-f402-4afa-af39-c09d4aafa946  192.168.1.243  SM STATE_CONNECTED  tun1  92607100/969f6100  4500/4500  125783  GRE
1,33,44,192,4094  3999/0/3807/3807  10.224.254.161  2021-03-13 08:29:01
Total Endpoints Count: 2
b4:5d:50:c6:82:4a#
```

7 RF Monitoring

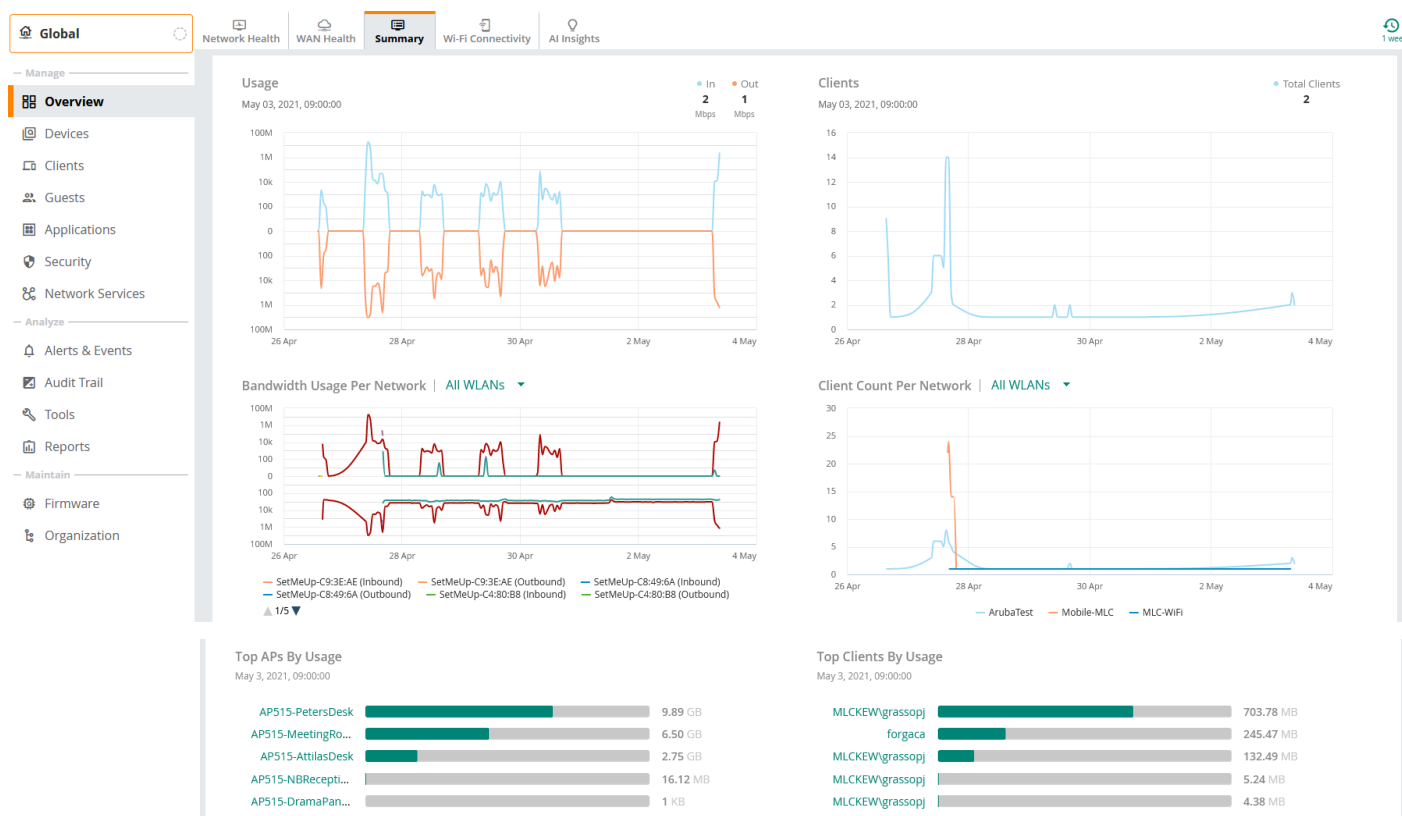
Here we'll just touch on some of the RF mgmt. info that are available in Central. To start with at the global level, you can check the WiFi connectivity and then drill down on any specifics, like AI insights, associations, authentication , etc.



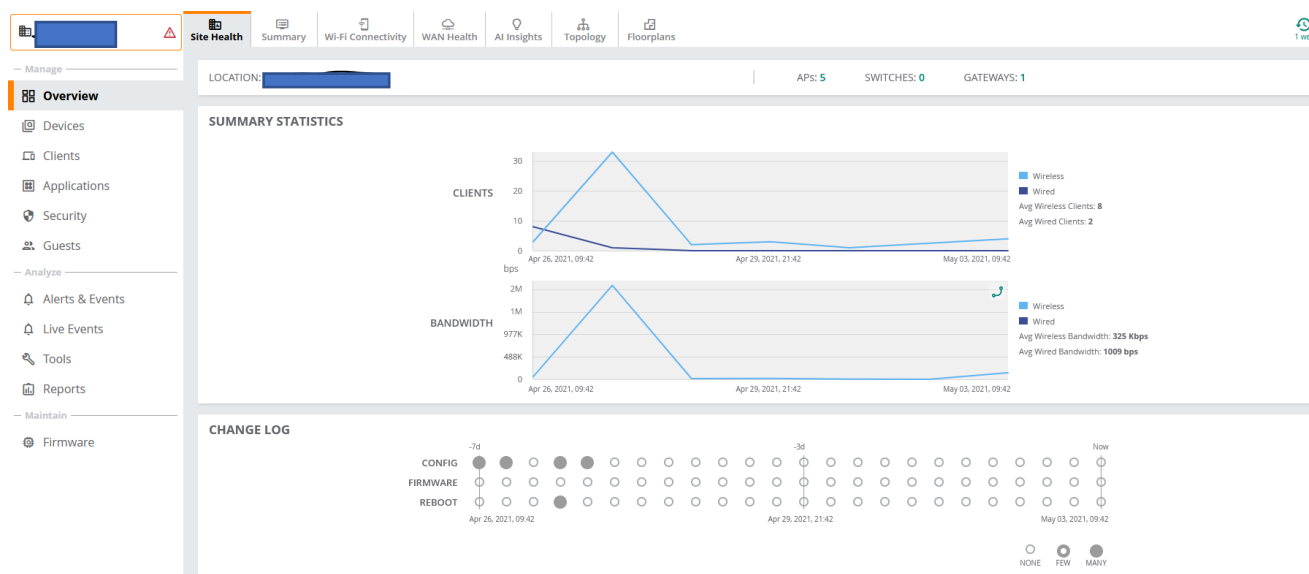
Clicking on “clients had excessive 802.1x failures”



Next, we can check the usage summary



We can then go to the Site level and see some of the stats



<div> <div>Access Points</div> <div>Switches</div> <div>Gateways</div> </div> <div> <div>Access Points</div> <div>Switches</div> <div>Gateways</div> </div>	<div> <div>Access Points</div> <div>Switches</div> <div>Gateways</div> </div> <div> <div>Access Points</div> <div>Switches</div> <div>Gateways</div> </div>
---	---

The figure displays three screenshots of the Aruba Central interface, focusing on network configuration and monitoring for Access Points (APs).

Top Screenshot: Summary and Radio Details

The interface shows a summary of 5 Access Points and 10 Radios. The 'RADIO' table lists details for 5 radios:

Access Point	Radio MAC Address	Band	Bandwidth	Channel	Utilization (%)	Channel Changes	Power (dBm)	Power Changes	Noise floor (dBm)
AP515-AtlasDesk	d0:15:a6:04:96:a0	2.4 GHz	20 MHz	11	26	26	7	3	-98
AP515-DramaPanelR-	bc:9f:e4:c8:7f:80	2.4 GHz	-	-	-	33	-	7	-
AP515-MeetingRoom	9c:8c:d8:13:1d:20	2.4 GHz	20 MHz	11	21	37	7	4	-98
AP515-NBRReception	bc:9f:e4:c8:0b:90	2.4 GHz	20 MHz	1	16	31	7	5	-98
AP515-PetersDesk	9c:8c:d8:13:ea:e0	2.4 GHz	20 MHz	6	21	47	7	6	-96

Middle Screenshot: Summary and Radio Details

The interface shows a summary of 5 Access Points and 5 Radios. The 'RADIO' table lists details for 5 radios:

Access Point	Radio MAC Address	Band	Bandwidth	Channel	Utilization (%)	Channel Changes	Power (dBm)	Power Changes	Noise floor (dBm)
AP515-AtlasDesk	d0:15:a6:04:96:b0	5 GHz	80 MHz	48	3	2	15	4	-98
AP515-DramaPanelR-	bc:9f:e4:c8:7f:80	5 GHz	-	-	-	1	-	2	-
AP515-MeetingRoom	9c:8c:d8:13:1d:30	5 GHz	80 MHz	108	3	5	15	2	-98
AP515-NBRReception	bc:9f:e4:c8:0b:90	5 GHz	80 MHz	157	5	4	15	3	-98
AP515-PetersDesk	9c:8c:d8:13:ea:f0	5 GHz	80 MHz	52	3	4	15	4	-98

Bottom Screenshot: Channel Distribution and Changes

The interface shows a 'CHANNEL DISTRIBUTION' chart for 5 GHz and 2.4 GHz bands. The chart displays the number of radios using each channel, with a color scale from Low (light blue) to High (dark blue).

5 GHz Channel Distribution:

Channel	Number of Radios
36	1
40	1
44	1
48	1
52	1
56	1
60	1
64	1
100	1
104	1
108	1
112	1
116	1
120	1
124	1
128	1
132	1
136	1
140	1
144	1
149	1
153	1
157	1
161	1
165	1
169	1

2.4 GHz Channel Distribution:

Channel	Number of Radios
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	1
9	1
10	1
11	1
12	1
13	1
14	1

Channel Changes and Power Changes (Last 1 Week):

The interface shows two donut charts comparing 'AirMatch' (dark blue) and 'Config' (light blue) changes over the last week.

- Channel Changes:** 16 Channel changes in the last 1 Week (AirMatch).
- Power Changes:** 3 Power changes in the last 1 Week (AirMatch).

[illegible]

CHANNEL CHANGES (10)					
Event Time	Reason	From Channel	To Channel	Band	Access Point
Apr 28, 2021, 05:00	Algorithm Assigned	149E	157E	5 GHz	AP515-NBReception
Apr 28, 2021, 05:00	Algorithm Assigned	112E	108E	5 GHz	AP515-MeetingRoom
Apr 28, 2021, 05:00	Algorithm Assigned	40E	48E	5 GHz	AP515-AttilasDesk
Apr 28, 2021, 05:00	Algorithm Assigned	60E	52E	5 GHz	AP515-PetersDesk
Apr 26, 2021, 18:30	Algorithm Assigned	108E	112E	5 GHz	AP515-MeetingRoom
Apr 26, 2021, 18:30	Algorithm Assigned	153E	149E	5 GHz	AP515-NBReception
Apr 26, 2021, 18:30	Algorithm Assigned	36E	40E	5 GHz	AP515-AttilasDesk
Apr 26, 2021, 18:30	Algorithm Assigned	64E	60E	5 GHz	AP515-PetersDesk
Apr 26, 2021, 18:15	Algorithm Assigned	100E	108E	5 GHz	AP515-MeetingRoom
Apr 26, 2021, 18:15	Algorithm Assigned	36E	153E	5 GHz	AP515-NBReception

Next, we can have a look at the Live view, for that we'll choose a specific AP.

Global

Access Points

Switches

Gateways

Manage

Overview

Devices

Clients

Guests

Applications

Security

Network Services

Access Points

Online 4

Offline 1

Radios 10

ACCESS POINTS (5)

Device Name	Status	IP Address	Model
AP515-DramaPanelRoom	Offline	10.16.136.201	AP-515
AP515-NBReception	Online	10.2.136.12	AP-515
AP515-MeetingRoom	Online	10.2.136.11	AP-515
AP515-PetersDesk	Online	10.2.136.10	AP-515
AP515-AttilasDesk	Online	10.2.136.13	AP-515

AP515-AttilasDesk

Summary

AI Insights

Floor Plan

Performance

RF

Manage

Overview

Device

Clients

Security

Analyze

Live Events

Alerts & Events

Audit Trail

Tools

Maintain

Firmware

DEVICE

AP MODEL

AP-515

COUNTRY CODE

AU

MAC

d0:15:aa:00:00:00

SERIAL NUMBER

000000000000

UPTIME

5 Days 22 Hours 30 Minutes

LAST REBOOT REASON

AP reload

FIRMWARE VERSION

10.2.0.1_79907

CONFIGURATION STATUS

Synchronized

Last Config Changed on Apr 28, 2021, 03:51

BAND SELECTION

Dual Band

POWER DRAW

13.16 W

POWER NEGOTIATION

802.3 at

GROUP

AOS10-Group

LABELS

-

LEDs on ACCESS POINT

●●●Blink LED

NETWORK

ETH0

Up

SPEED (Mbps) / DUPLEX

1000 / Full

VLAN

Trunk (all)

LLDP Details

ETH1

Down

SPEED (Mbps) / DUPLEX

-

VLAN

-

CURRENT UPLINK

Ethernet (br0)

UPLINK CONNECTED TO

-

IP ADDRESS

10.2.136.13 (DHCP)

PUBLIC IP ADDRESS

203.1.203.51

DNS NAME SERVERS

10.99.64.202

DEFAULT GATEWAY

10.2.136.1 (DHCP)

NTP SERVER

10.250.136.1

Manage

Actions

Go Live

Overview

Device

Clients

Security

Analyze

Live Events

Alerts & Events

Audit Trail

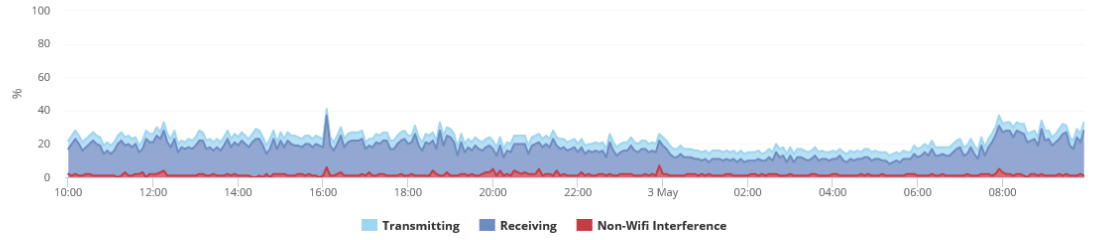
Tools

Maintain

Firmware

RADIO 2.4 GHz RADIO 5 GHz

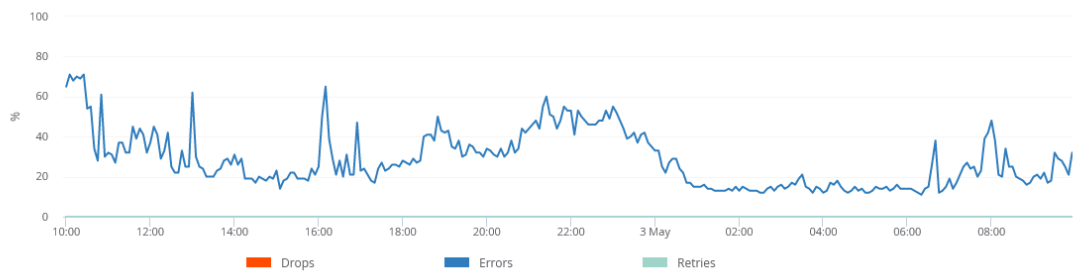
CHANNEL UTILIZATION



NOISE FLOOR

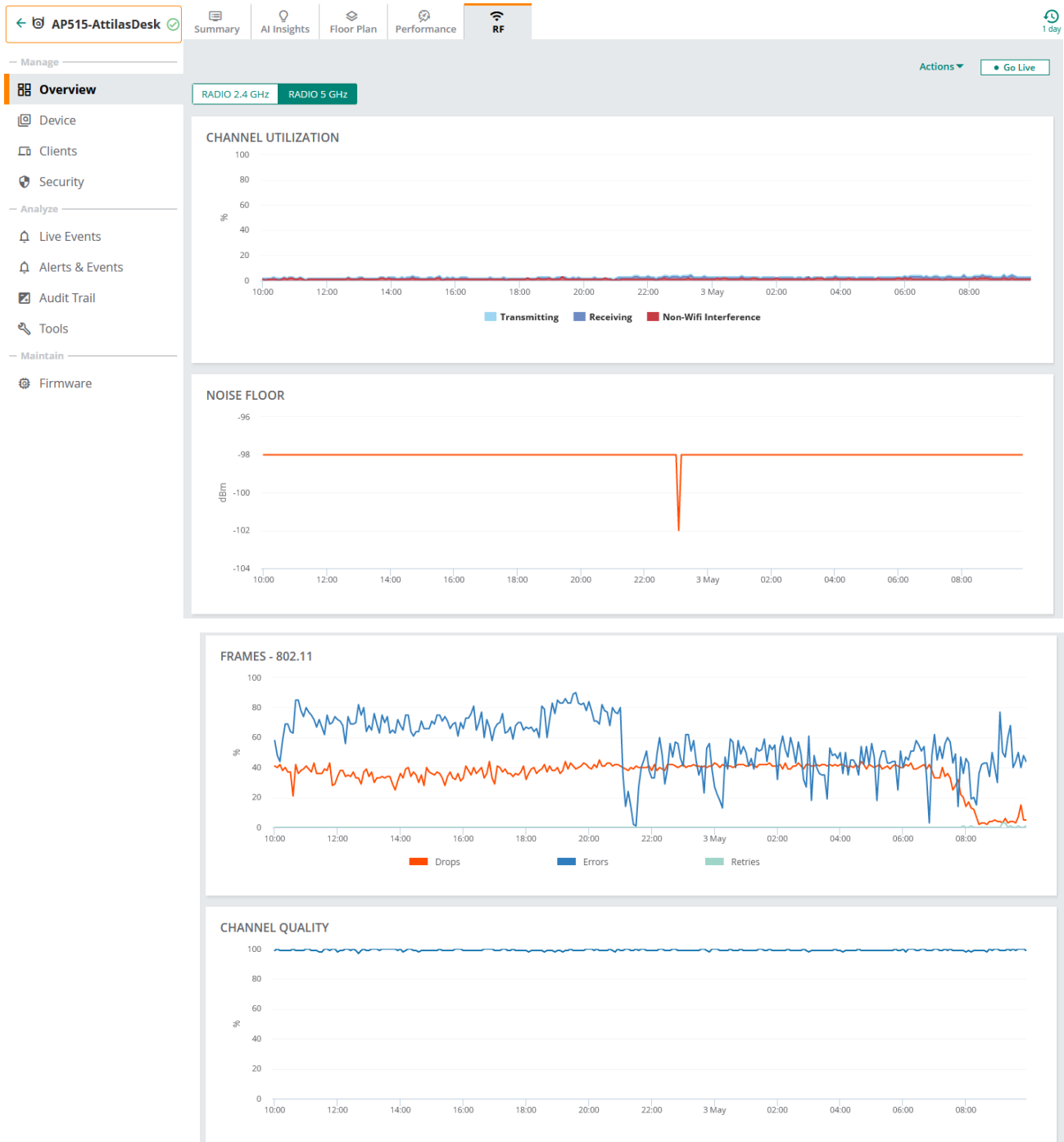


FRAMES - 802.11

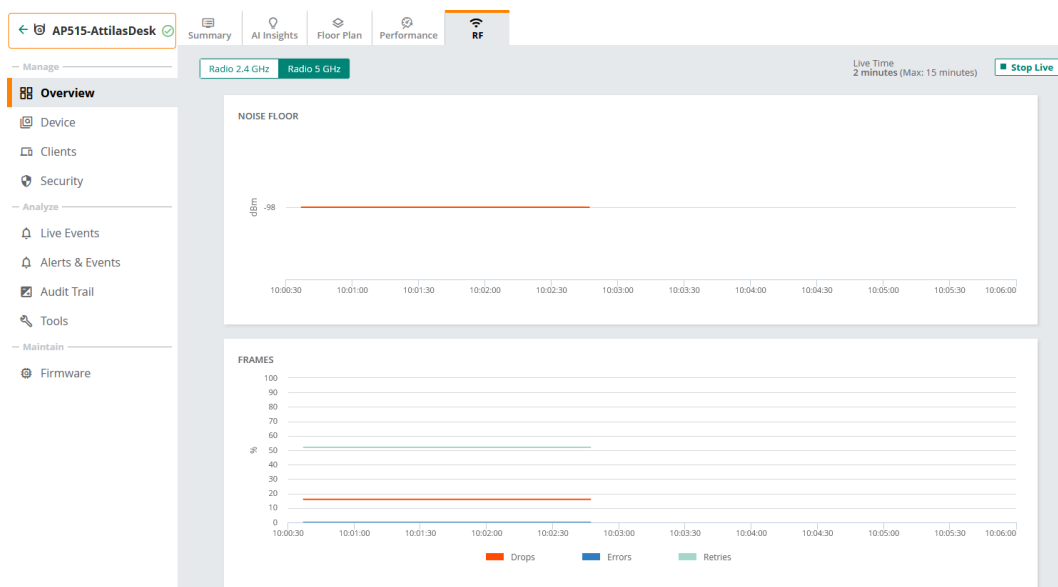


CHANNEL QUALITY





Now you can click on go live to get real-time view of the RF counter for 15min.



8 Guest Access Configuration

Here we'll start with AP configuration followed by ClearPass.

8.1 Guest Wireless Configuration

The Guest WLAN will be tunnelled to the gateways, for this scenario all the configuration will take place on the AP group.

The screenshot shows the AOS10 configuration interface. The left sidebar has a 'Manage' section with 'Overview' and 'Devices' (selected), and an 'Analyze' section with 'Alerts & Events', 'Audit Trail', 'Tools', 'Reports', and 'Maintain' with 'Firmware'. The top navigation bar includes 'Access Points', 'Switches', and 'Gateways'. The main content area is titled 'CREATE A NEW NETWORK' and has a progress bar with five steps: 1 General (active), 2 VLANs, 3 Security, 4 Access, and 5 Summary. The 'General' tab contains a 'Name (SSID):' field with the value 'Schoo-Guest'. Below this is an 'Advanced Settings' section with expandable options: 'Broadcast/Multicast', 'Transmit Rates (Legacy Only)', 'Bandwidth Control', 'WiFi Multimedia', 'Miscellaneous', and 'Time Range Profiles'. At the bottom right are 'Cancel' and 'Next' buttons.

The screenshot shows the AOS10 configuration interface with the 'VLANs' tab selected. The progress bar now highlights step 2 'VLANs'. The 'Traffic forwarding mode:' section has three radio buttons: 'Bridge', 'Tunnel' (selected), and 'Mixed'. The 'Primary Gateway Cluster:' dropdown is set to 'AOS10.auto_gwcluster_178_0'. The 'Secondary Gateway Cluster:' dropdown is set to 'None'. The 'Client VLAN Assignment:' section has two radio buttons: 'Static' (selected) and 'Dynamic'. The 'VLAN ID:' dropdown is set to '192'. A link '> Show Named VLANs' is present. At the bottom right are 'Cancel', 'Back', and 'Next' buttons.

The screenshot shows the AOS10 configuration interface with the 'Security' tab selected. The progress bar now highlights step 3 'Security'. The 'Security Level:' section features a slider with four positions: 'Enterprise', 'Personal', 'Captive Portal' (selected), and 'Open'. The 'Splash Page' section includes a 'Captive Portal Type:' dropdown set to 'External' and a 'Captive Portal Profile:' dropdown set to '-- Select --' with a yellow plus icon. A red error message 'This field is mandatory.' is displayed below the profile dropdown. At the bottom right are 'Cancel', 'Back', and 'Next' buttons.

AOS10

Access Points

Switches

Gateways

Manage

Overview

Devices

Clients

Guests

Applications

Security

Analyze

Alerts & Events

Audit Trail

Tools

Reports

Maintain

Firmware

WLANs

Access Points

Switches

Gateways

EXTERNAL CAPTIVE PORTAL-NEW

Name:

CP-Guest

Authentication Type:

RADIUS Authentication

IP or Hostname:

victory.clearpass.info

URL:

/guest/school.php

Port:

443

Use HTTPS:

☒

Captive Portal Failure:

Deny Internet

Server offload:

☐

Cancel

OK

AOS10

Access Points

Switches

Gateways

Manage

Overview

Devices

Clients

Guests

Applications

Security

Analyze

Alerts & Events

Audit Trail

Tools

Reports

Maintain

Firmware

WLANs

Access Points

Radios

Interfaces

Security

Services

System

Configuration Audit

1 General

2 VLANs

3 Security

4 Access

5 Summary

Security Level:

Enterprise

Personal

Captive Portal

Open

Splash Page

Captive Portal Type:

External

Captive Portal Profile:

CP-Guest

Primary Server:

ClearPass-GW

Secondary Server:

-- Select --

Encryption:

☐

Key Management:

Open

Advanced Settings

Advanced Settings

Captive Portal Proxy Server IP:

Captive Portal Proxy Server Port:

MAC Authentication:

Use IP for Calling Station ID:

Delimiter Character:

Called Station ID Type:

Reauth Interval:

Denylisting:

Max Authentication Failures:

Enforce DHCP: ☐

WPA3 Transition: ☒

Called Station ID Include SSID: ☐

Uppercase Support: ☐

☒ Accounting

Accounting:

Accounting Interval: min

☒ Disable if uplink type is

In the above we have also enabled MAC auth and RADIUS accounting. MAC auth is enabled because we want to also enable MAC caching for the guest users.

AOS10

Access Points

WLANs

CREATE A NEW NETWORK

1 General **2 VLANs** **3 Security** **4 Access** **5 Summary**

Access rules

Role Based ☒ Network Based ☐ Unrestricted ☐

ROLE	ACCESS RULES FOR SELECTED ROLES
Schoo-Guest	Allow any to all destinations
school	
CP-Guest	

ROLE ASSIGNMENT RULES

Default role: Schoo-Guest

ADD ROLE ASSIGNMENT 1 Role(s)

ASSIGN PRE-AUTHENTICATION ROLE: ☒ CP-Guest

ENFORCE MAC AUTH ONLY ROLE: ☐

aruba Central

AOS10

Access Points

WLANs

SUCCESS

Schoo-Guest is Configured Successfully

Now we have our Guest SSID configured.

Lastly note that we have not use a publicly signed HTTPS server certificate for the controllers and hence the redirection of a web page will issue a warning on the client's web browser. In all deployment you need to have a public cert for the controllers as well as ClearPass nodes.

8.2 ClearPass Guest policy Configuration

We'll go through the guest confirmation needed on ClearPass. There are two part to it, one is the web pages that the client redirects to and the other is the policy service we need to create. We'll start with the policy service. Here we are using the following template. This creates 2x services one is MAC authentication and the second one is Guest redirection to captive portal page.

The screenshot shows the Aruba ClearPass Policy Manager web interface. On the left is a navigation menu with sections: Dashboard, Monitoring, Configuration (selected), and Administration. Under Configuration, 'Service Templates & Wizards' is selected. The main area displays a list of service templates:

- Device MAC Authentication**: To authenticate guest devices based on their MAC address.
- EDUROAM service**: Service template for roaming users to connect to campus networks that are part of the eduroam federation.
- Encrypted Wireless Access via 802.1X Public PEAP method**: Service Template for providing encrypted wireless access to (guest) users via fixed 802.1X PEAP credentials.
- Guest Access**: To authenticate guest users logging in via captive portal. Guests must re-authenticate after their session ends.
- Guest Access - Web Login**: To authenticate guest users logging in via guest portal.
- Guest Authentication with MAC Caching** (highlighted): To authenticate users once using captive portal and later to allow logins using cached MAC Address of the device.
- OAuth2 API User Access**: Service template for API clients authenticating with username and password (OAuth2 grant type "password").
- Onboard**: Service template for authorizing device credential provisioning and onboarding.
- Onboard Services Only**: Service template for authorizing device credential and onboarding.

Configuration » Service Templates & Wizards

Service Templates - Guest Authentication with MAC Caching

General	Wireless Network Settings	MAC Caching Settings	Posture Settings	Access Restrictions
Name Prefix*: GG				
Description				
Users first login via captive portal and their MAC addresses are cached. Subsequent logins will use MAC authentication and bypass the captive portal. Network access can be restricted based on day of the week, bandwidth limit or number of unique devices used by the User. The cache lifetime of the MAC address can vary according to the user's role (Guest, Employee or Contractor) and after that the user will have to re-authenticate via captive portal. Posture checks can be enabled, optionally, to validate the client device for antivirus, anti-spyware, firewall status. These results will determine the enforcement for the device.				
Back to Service Templates & Wizards Delete Next → Add Service Cancel				

General	Wireless Network Settings	MAC Caching Settings	Posture Settings	Access Restrictions
Select NAD Client: MD-1				
Wireless SSID*: Guest				
Back to Service Templates & Wizards Delete Next → Add Service Cancel				

General	Wireless Network Settings	MAC Caching Settings	Posture Settings	Access Restrictions
Enter MAC Caching duration for the users. After this time expires, users will have to re-authenticate via captive portal				
Cache duration for Employee: One Month				
Cache duration for Guest: One Day				
Cache duration for Contractor: One Week				
Back to Service Templates & Wizards Delete Next → Add Service Cancel				

General
Wireless Network Settings
MAC Caching Settings
Posture Settings
Access Restrictions

Enable Posture Checks to perform health checks after authentication.

Enable Posture Checks:
☐
Configure Guest Web Login page

Back to Service Templates & Wizards
Delete
Next →
Add Service
Cancel

General
Wireless Network Settings
MAC Caching Settings
Posture Settings
Access Restrictions

- Enforcement Type applies to the Captive Portal Access, Employee Access, Guest Access, and Contractor Access fields.
- Captive Portal Access is used for unauthenticated users and after the MAC caching duration has expired.
- At least one of Employee, Guest, and Contractor Access must be provided.

Enforcement Type*:Aruba Role Enforcement

Captive Portal Access*:GuestCaptivePortal

Days allowed for access*:☒ Monday ☒ Tuesday ☒ Wednesday ☒ Thursday ☒ Friday ☒ Saturday ☒ Sunday

Maximum number of devices allowed per user*:5

Maximum bandwidth allowed per user*:0 MB (For unlimited bandwidth, set value to 0)

Employee Access:Employee-Guest

Guest Access:Guest

Contractor Access:Contractor

Back to Service Templates & Wizards
Delete
Next →
Add Service
Cancel

Services

Add
Import
Export All

- Added 15 Enforcement Profile(s)
- Added 2 Enforcement Policies
- Added 2 Role Mapping Policies
- Added 2 service(s)

This page shows the current list and order of services that ClearPass follows during authentication and authorization.

Filter: Name contains + Go Clear Filter Show 20 records

#	Order	Name	Type	Template	Status
1.	<input type="checkbox"/> 1	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	
2.	<input type="checkbox"/> 2	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	
3.	<input type="checkbox"/> 3	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	
4.	<input type="checkbox"/> 4	[Guest Operator Logins]	Application	Aruba Application Authentication	
5.	<input type="checkbox"/> 5	[Insight Operator Logins]	Application	Aruba Application Authentication	
6.	<input type="checkbox"/> 6	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	
7.	<input type="checkbox"/> 7	AA Aruba 802.1X Wireless	RADIUS	Aruba 802.1X Wireless	
8.	<input type="checkbox"/> 8	GG MAC Authentication	RADIUS	MAC Authentication	
9.	<input type="checkbox"/> 9	GG User Authentication with MAC Caching	RADIUS	RADIUS Enforcement (Generic)	

We'll look at the MAC authentication service

Services - GG MAC Authentication

Note: This Service is created by Service Template

Summary
Service
Authentication
Authorization
Roles
Enforcement

Name:GG MAC Authentication

Description:MAC Authentication bypass for captive portal users

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. Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}
2. Radius:Aruba	Aruba-Essid-Name	BEGINS_WITH	Guest
3.	Click to add...		

SummaryServiceAuthenticationAuthorizationRolesEnforcement

Authentication Methods:

[Allow All MAC AUTH]

Move Up ↑

Move Down ↓

Remove

View Details

Modify

--Select to Add--

Add New Authentication Method

Authentication Sources:

[Endpoints Repository] [Local SQL DB]

Move Up ↑

Move Down ↓

Remove

View Details

Modify

--Select to Add--

Add New Authentication Source

SummaryServiceAuthenticationAuthorizationRolesEnforcement

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 -

[Time Source] [Local SQL DB]

Remove

View Details

Modify

--Select to Add--

Add New Authentication Source

SummaryServiceAuthenticationAuthorizationRolesEnforcement

Role Mapping Policy:

GG MAC Authentication Role Mapping

Modify

Add New Role Mapping Policy

Role Mapping Policy Details

Description:

Default Role:

Rules Evaluation Algorithm:

evaluate-all

Conditions	Role
(Authorization:[Endpoints Repository]:Unique-Device-Count EXISTS) AND (Authorization:[Time Source]:Now DT LESS_THAN %{Endpoint:MAC-Auth Expiry}) AND (Authorization:[Guest User Repository]:AccountExpired EQUALS false) AND (Authorization:[Guest User Repository]:AccountEnabled EQUALS true)	[MAC Caching]
(Endpoint:Guest Role ID EQUALS 1)	[Contractor]
(Endpoint:Guest Role ID EQUALS 2)	[Guest]
(Endpoint:Guest Role ID EQUALS 3)	[Employee]

SummaryServiceAuthenticationAuthorizationRolesEnforcement

Use Cached Results:

☐ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy:

GG MAC Authentication Enforcement Policy

Modify

Add New Enforcement Policy

Enforcement Policy Details

Description:

Default Profile:

Rules Evaluation Algorithm:

first-applicable

Conditions	Enforcement Profiles
(Tips:Role MATCHES_ALL [MAC Caching]) [Guest] [User Authenticated])	[Allow Access Profile], GG Guest Device Profile
(Tips:Role MATCHES_ALL [MAC Caching]) [Employee] [User Authenticated])	[Allow Access Profile], GG Employee Device Profile
(Tips:Role MATCHES_ALL [MAC Caching]) [Contractor] [User Authenticated])	[Allow Access Profile], GG Contractor Device Profile
(Tips:Role MATCHES_ANY [Guest]) [Contractor] [Employee])	[Allow Access Profile], GG Captive Portal Profile

Back to Services

Disable

Copy

Save

Cancel

And here are the enforcement profiles that are used here

43 | Page

Profile:

Name:

GG Guest Device Profile

Description:

Role/VLAN enforcement for Guest

Type:

RADIUS

Action:

Accept

Device Group List:

-

Attributes:

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

Profile:

Name:

GG Employee Device Profile

Description:

Role/VLAN enforcement for Employee

Type:

RADIUS

Action:

Accept

Device Group List:

-

Attributes:

Type	Name	Value
1. Radius:Aruba	Aruba-User-Role	= Employee-Guest
2. Radius:IETF	User-Name	= %{Endpoint:Username}

Profile:

Name:

GG Contractor Device Profile

Description:

Role/VLAN enforcement for Contractor

Type:

RADIUS

Action:

Accept

Device Group List:

-

Attributes:

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

Profile:

Name:

GG Captive Portal Profile

Description:

Captive Portal Role/VLAN enforcement

Type:

RADIUS

Action:

Accept

Device Group List:

-

Attributes:

Type	Name	Value
1. Radius:Aruba	Aruba-User-Role	= Guest-guest-logon

We'll look at the User Authentication with MAC caching service

Services - GG User Authentication with MAC Caching

Summary

Service

Authentication

Authorization

Roles

Enforcement

Name:

GG User Authentication with MAC Caching

Description:

Captive Portal authentication with MAC Caching

Type:

RADIUS Enforcement (Generic)

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	Calling-Station-Id	EXISTS	
2. Connection	Client-Mac-Address	NOT_EQUALS	%{Radius:IETF:User-Name}
3. Radius:Aruba	Aruba-Essid-Name	BEGINS_WITH	Guest
4.	Click to add...		

SummaryServiceAuthenticationAuthorizationRolesEnforcement

Authentication Methods:

[PAP]
[MSCHAP]
[CHAP]

Move Up ↑

Move Down ↓

Remove

View Details

Modify

Add New Authentication Method

Authentication Sources:

[Guest User Repository] [Local SQL DB]

Move Up ↑

Move Down ↓

Remove

View Details

Modify

Add New Authentication Source

SummaryServiceAuthenticationAuthorizationRolesEnforcement

Authorization Details:

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

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

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

[Endpoints Repository] [Local SQL DB]
[Time Source] [Local SQL DB]

Remove

View Details

Modify

Add New Authentication Source

SummaryServiceAuthenticationAuthorizationRolesEnforcement

Role Mapping Policy:

GG User Authentication with MAC Caching Role Mapping

Modify

Add New Role Mapping Policy

Role Mapping Policy Details

Description:

Default Role:

Rules Evaluation Algorithm:

[Other]

evaluate-all

Conditions	Role
1. (GuestUser:Role ID EQUALS 1)	[Contractor]
2. (GuestUser:Role ID EQUALS 2)	[Guest]
3. (GuestUser:Role ID EQUALS 3)	[Employee]

SummaryServiceAuthenticationAuthorizationRolesEnforcement

Use Cached Results:

☐ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy:

GG User Authentication with MAC Caching Enforcement Policy

Modify

Add New Enforcement Policy

Enforcement Policy Details

Description:

Default Profile:

Rules Evaluation Algorithm:

[Allow Access Profile]

first-applicable

Conditions	Enforcement Profiles
1. (Authorization:[Endpoints Repository]:Unique-Device-Count GREATER_THAN 5)	[Deny Access Profile]
2. (Tips:Role EQUALS [Employee]) AND (Date:Day-of-Week BELONGS_TO Monday,Tuesday,Wednesday,Thursday,Friday,Saturday,Sunday)	GG MAC Caching Session Timeout, GG MAC Caching Bandwidth Limit, GG MAC Caching Session Limit, GG Employee MAC Caching, [Update Endpoint Known], GG MAC Caching Do Expire, GG MAC Caching Expire Post Login, GG Employee Profile
3. (Tips:Role EQUALS [Contractor]) AND (Date:Day-of-Week BELONGS_TO Monday,Tuesday,Wednesday,Thursday,Friday,Saturday,Sunday)	GG MAC Caching Session Timeout, GG MAC Caching Bandwidth Limit, GG MAC Caching Session Limit, GG Contractor MAC Caching, [Update Endpoint Known], GG MAC Caching Do Expire, GG MAC Caching Expire Post Login, GG Contractor Profile
4. (Tips:Role EQUALS [Guest]) AND (Date:Day-of-Week BELONGS_TO Monday,Tuesday,Wednesday,Thursday,Friday,Saturday,Sunday)	GG MAC Caching Session Timeout, GG MAC Caching Bandwidth Limit, GG MAC Caching Session Limit, GG Guest MAC Caching, [Update Endpoint Known], GG MAC Caching Do Expire, GG MAC Caching Expire Post Login, GG Guest Profile

The enforcement profiles

45 | Page

Profile:

Name:	GG Employee Profile
Description:	Role/VLAN enforcement for Employee
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

Type	Name	Value
1. Radius:Aruba	Aruba-User-Role	= Employee-Guest

Profile:

Name:	GG Guest Profile
Description:	Role/VLAN enforcement for Guest
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

Type	Name	Value
1. Radius:Aruba	Aruba-User-Role	= Guest

Profile:

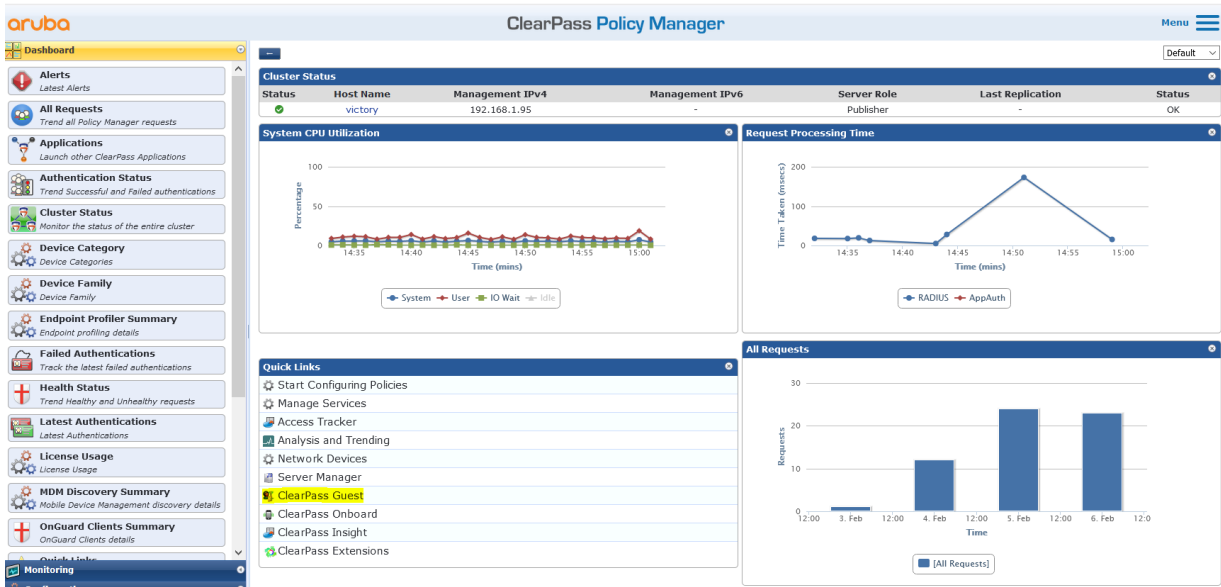
Name:	GG Contractor Profile
Description:	Role/VLAN enforcement for Contractor
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

Type	Name	Value
1. Radius:Aruba	Aruba-User-Role	= Contractor

8.3 ClearPass Guest Portal Configuration

Here we'll configure the portal pages.



Now we'll create a guest user called cpghuser with no expiration on the account.

aruba ClearPass Guest

Home » Guest

Guest Manager

Guest Account Management

Use the commands below to manage your network's guest user accounts.

- Create New Guest Account**
Set up a new account for guest access to your network.
- Create Multiple Guest Accounts**
Create multiple guest accounts, each with a randomly-assigned username and password.
- Manage Guest Accounts**
View a list of all current guest accounts. You can modify and remove individual user accounts here.
- Edit Multiple Guest Accounts**
View a list of all current guest accounts. You can modify and remove one or more user accounts here.
- Active Sessions**
View active accounting sessions and disconnect or change authorization for sessions.
- Import Guest Accounts**
Import a list of guests from a text file and create a guest account for each entry in the list.
- Export Guest Accounts**
Export a list of all current guest accounts to a file. You can select the format you want to export to here.

aruba ClearPass Guest

Home » Guest » Create Account

Create Guest Account

New guest account being created by admin.

Create New Guest Account

* Guest's Name:
Name of the guest.

* Company Name:
Company name of the guest.

* Email Address:
The guest's email address. This will become their username to log into the network.

Account Activation:
Select an option for changing the activation time of this account.

Account Expiration:
Select an option for changing the expiration time of this account.

* Account Role:
Role to assign to this account.

Password:

Notes:

* Terms of Use: ☒ I am the sponsor of this account and accept the terms of use

* required field

Once created we'll modify it to change the username and password

aruba ClearPass Guest

Home » Guest » Manage Accounts

Manage Guest Accounts

The following table shows the guest accounts that have been created. Click an account to modify it.

Filter:

Username	Role	State	Activation	Expiration
cpguser	[Guest]	Active	23 hours ago	No expiry
<input type="button" value="Reset password"/> <input type="button" value="Change expiration"/> <input type="button" value="Remove"/> <input type="button" value="Edit"/> <input type="button" value="Sessions"/> <input type="button" value="Print"/> <input type="button" value="Show Details"/>				
Refresh			1	Showing 1 - 1 of 1

Guest

- Active Sessions
- Create Account
- Create Multiple
- Export Accounts
- Import Accounts
- Manage Accounts
- Manage Multiple Accounts

Quick Help
Create
More Options

Filter:

Username	Role	State	Activation	Expiration
cpguser	[Guest]	Active	23 hours ago	No expiry

Reset password
Change expiration
Remove
Edit
Sessions
Print
Show Details

To update the properties of this guest account, use the form below:

Edit Account

* Guest's Name: cpguser
Name of the guest.

* Username: cpguser
Name of the account.

Account Activation: (No changes: Account is active)
Select an option for changing the activation time of this account.

Account Expiration: (No changes: Account will not expire)
Select an option for changing the expiration time of this account.

Account Lifetime: N/A
The amount of time after the first login before the account will expire and be deleted.

Total Allowed Usage: (No changes)
Select an option for changing the allowed usage time of this account.

Account Role: (No changes: [Guest])
Role to assign to this account.

* Password: Type in a new password
Select an option for editing the guest account's password.

New password:
Type in a new password to assign to the guest account.

Confirm Password:
Repeat the new password for the guest account.

Session Limit: 0
The number of simultaneous sessions allowed for this account. Type 0 for unlimited use.

Notes:

Update Account

Next we'll create a weblogin page, note that the page name will be in the redirection URL, also `securelogin.hpe.com` will need to change to CN in the server certificate on Aruba controller.

Guest
Devices
Onboard
Configuration

- Authentication
- Content Manager
 - Private Files
 - Public Files
- Guest Manager
- Hotspot Manager
- Pages
 - Fields
 - Forms
 - List Views
 - Self-Registrations
 - Web Logins
 - Web Pages
- Receipts
- SMS Services
- Translations

Home » Configuration » Pages » Web Logins

Web Login (school)

Use this form to make changes to the Web Login school.

Web Login Editor

* Name: school
Enter a name for this web login page.

Page Name: school
Enter a page name for this web login.
The web login will be accessible from "/guest/page_name.php".

Description: for AOS-10
Comments or descriptive text about the web login.

* Vendor Settings: Aruba
Select a predefined group of settings suitable for standard network configurations.

Login Method: Controller-initiated — Guest browser performs HTTP form submit
Select how the user's network login will be handled.
Server-initiated logins require the user's MAC address to be available, usually from the captive portal redirection process.

* Address: securelogin.hpe.com
Enter the IP address or hostname of the vendor's product here.

Secure Login: Use vendor default
Select a security option to apply to the web login process.

Dynamic Address: ☐ The controller will send the IP to submit credentials
In multi-controller deployments, it is often required to post credentials to different addresses made available as part of the original redirection.
The address above will be used whenever the parameter is not available or fails the requirements below.

Page Redirect Options for specifying parameters passed in the initial redirect.	
Security Hash:	<div>Do not check – login will always be permitted</div> <div>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.</div>
Login Form Options for specifying the behaviour and content of the login form.	
Authentication:	<div>Credentials – Require a username and password</div> <div>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.</div>
Prevent CNA:	<input checked="" type="checkbox"/> 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:	<input type="checkbox"/> Provide a custom login form If selected, you must supply your own HTML login form in the Header or Footer HTML areas.
Custom Labels:	<input type="checkbox"/> 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:	<div>None — no extra checks will be made</div> <div>Select how the username and password should be checked before proceeding to the NAS authentication.</div>
Terms:	<input checked="" type="checkbox"/> Require a Terms and Conditions confirmation If checked, the user will be forced to accept a Terms and Conditions checkbox.
CAPTCHA:	<div>None</div> <div>Select a CAPTCHA mode.</div>
Default Destination Options for controlling the destination clients will redirect to after login.	
* Default URL:	<div></div> <div>Enter the default URL to redirect clients. Please ensure you prepend "http://" for any external domain.</div>
Override Destination:	<input type="checkbox"/> 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:	<div>Galleria Skin 3</div> <div>Choose the skin to use when this web login page is displayed.</div>
Title:	<div></div> <div>The title to display on the web login page. Leave blank to use the default (Login).</div>
Header HTML:	<div> <pre>{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}</pre> </div> <div>HTML template code displayed before the login form.</div>
Footer HTML:	<div> <pre>{nwa_text id=7979}<p> Contact a staff member if you are experiencing difficulty logging in. </p>{/nwa_text}</pre> </div> <div>HTML template code displayed after the login form.</div>
Login Message:	<div> <pre>{nwa_text id=7978}<p> Logging in, please wait... </p>{/nwa_text}</pre> </div> <div>HTML template code displayed while the login attempt is in progress.</div>
* Login Delay:	<div>0</div> <div>The time in seconds to delay while displaying the login message.</div>
Advertising Services Enable advertising content on the login page.	
Advertising:	<input type="checkbox"/> Enable Advertising Services content
Cloud Identity Optionally present guests with various cloud identity / social login options.	
Enabled:	<input type="checkbox"/> Enable logins with cloud identity / social network credentials
Multi-Factor Authentication Require a secondary factor when authenticating.	
Provider:	<div>No multi-factor authentication</div>
Network Login Access Controls access to the login page.	
Allowed Access:	<div></div> <div>Enter the IP addresses and networks from which logins are permitted.</div>
Denied Access:	<div></div> <div>Enter the IP addresses and networks that are denied login access.</div>
* Deny Behavior:	<div>Send HTTP 404 Not Found status</div> <div>Select the response of the system to a request that is not permitted.</div>
Post-Authentication Actions to perform after a successful pre-authentication.	
Health Check:	<input type="checkbox"/> Require a successful OnGuard health check If selected, the guest will be required to pass a health check prior to accessing the network.
Update Endpoint:	<input type="checkbox"/> Mark the user's MAC address as a known endpoint If selected, the endpoint's attributes will also be updated with other details from the user account.
<div>Save Changes</div> <div>Save and Reload</div>	

aruba ClearPass Guest

Home » Configuration » Pages » Web Logins

Web Logins

Create a new web login page

Many NAS devices support Web-based authentication for visitors.

By defining a web login page on the ClearPass Guest you are able to provide a customized graphical login page for visitors accessing the network through these NAS devices.

Use this list view to define new web login pages, and to make changes to existing web login pages.

Onboard device provisioning pages are now managed from the Web Login tab within provisioning settings

Name	Page Title	Page Name	Page Skin
school		school	Galleria Skin 3

1 web login

Back to pages

Back to configuration

Back to main

You can test the page as well, when you'll click on the launch a tab will open and you'll see the captive portal note the URL which in this case is <https://victory.clearpass.info/guest/school.php? browser=1>

The "guest/school.php" is used in the URL redirection which we configured in MM

Now go to content manager and upload your terms and condition page.

aruba ClearPass Guest

Home » Configuration » Content Manager » Public Files

Public Files

Use this list view to manage the content items stored on this ClearPass Guest.

These files are public and will be accessible via HTTP/HTTPS under /guest/public.

Currently showing directory: Root Directory.

Name	Owner	Type	Date Modified	Size
advertising-campaigns-blue.png		image/png	2021-02-06 11:14	24.0 KB
advertising-campaigns-orange.png		image/png	2021-02-06 11:14	25.1 KB
advertising-campaigns-steel.jpg		image/jpeg	2021-02-06 11:14	26.7 KB
advertising-services-blue-728x90.png		image/png	2021-02-06 11:14	25.3 KB
advertising-services-orange-728x90.png		image/png	2021-02-06 11:14	25.3 KB
advertising-services-steel-728x90.jpg		image/jpeg	2021-02-06 11:14	24.2 KB
terms.html	admin	text/html	2021-02-06 11:14	2.9 KB

Quick Help Upload New Content Download New Content Create New Directory

Properties Delete Rename Download View Content Quick View Edit

School

Guest Wireless Access Acceptable Use Policy

This Policy is a guide to the acceptable use of the School Guest Wireless network facilities and services.

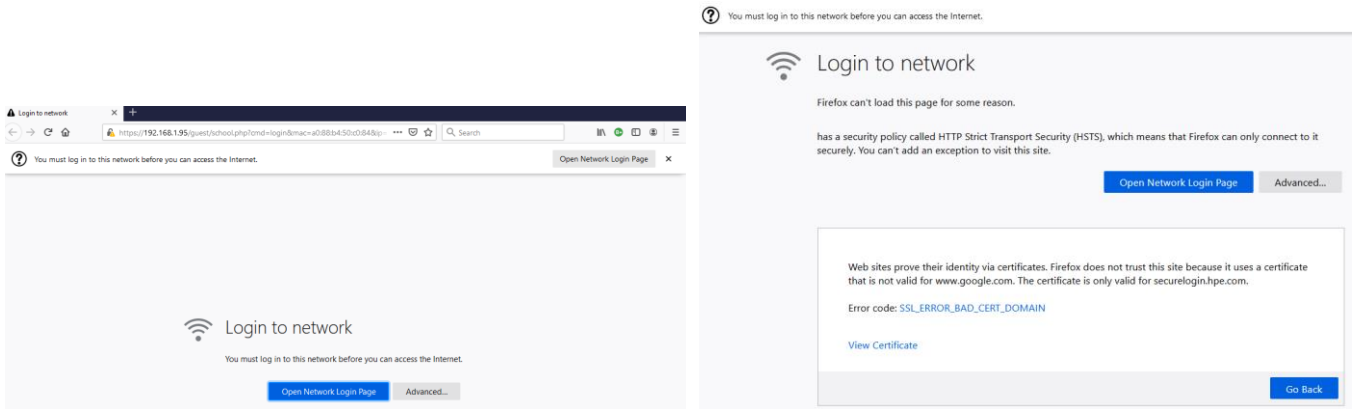
Any individual connected to the Guest Wireless Network in order to use it directly or to connect to any other network(s), must comply with this policy, the stated purposes and Acceptable Use policies of any other network(s) or host(s) used, and all applicable laws, rules, and regulations.

School MAKES NO REPRESENTATIONS OR WARRANTIES CONCERNING THE AVAILABILITY OR SECURITY OF THE GUEST WIRELESS NETWORK, AND ALL USE IS PROVIDED ON AN AS-IS BASIS. BY USING THE GUEST WIRELESS NETWORK YOU AGREE TO DEFEND, INDEMNIFY, AND HOLD HARMLESS School FOR ANY LOSSES OR DAMAGES THAT MAY RESULT FROM YOUR USE OF THE GUEST WIRELESS NETWORK.

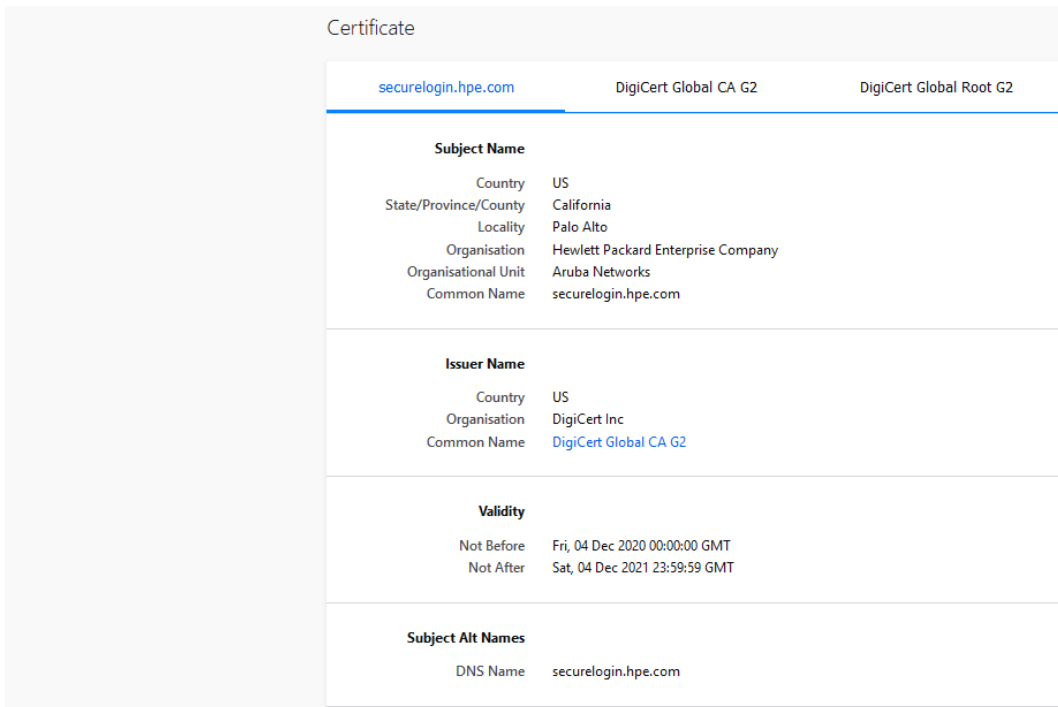
School takes no responsibility and assumes no liability for any content uploaded, shared, transmitted, or downloaded by you or any third party, or for anything you may encounter or any data that may be lost or compromised while connected to the Guest Wireless Network.

8.4 Guest Testing

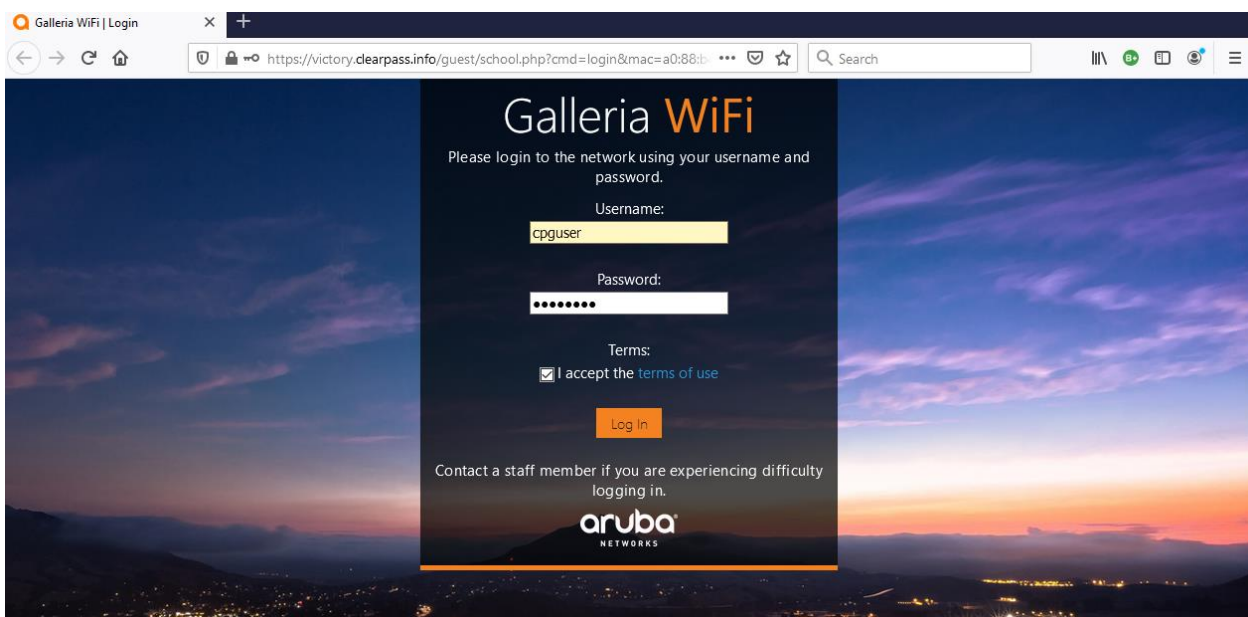
Now we'll get a test device to connect to Guest SSID, it gets automatically redirected to guest page in ClearPass but the browser will issue a warning



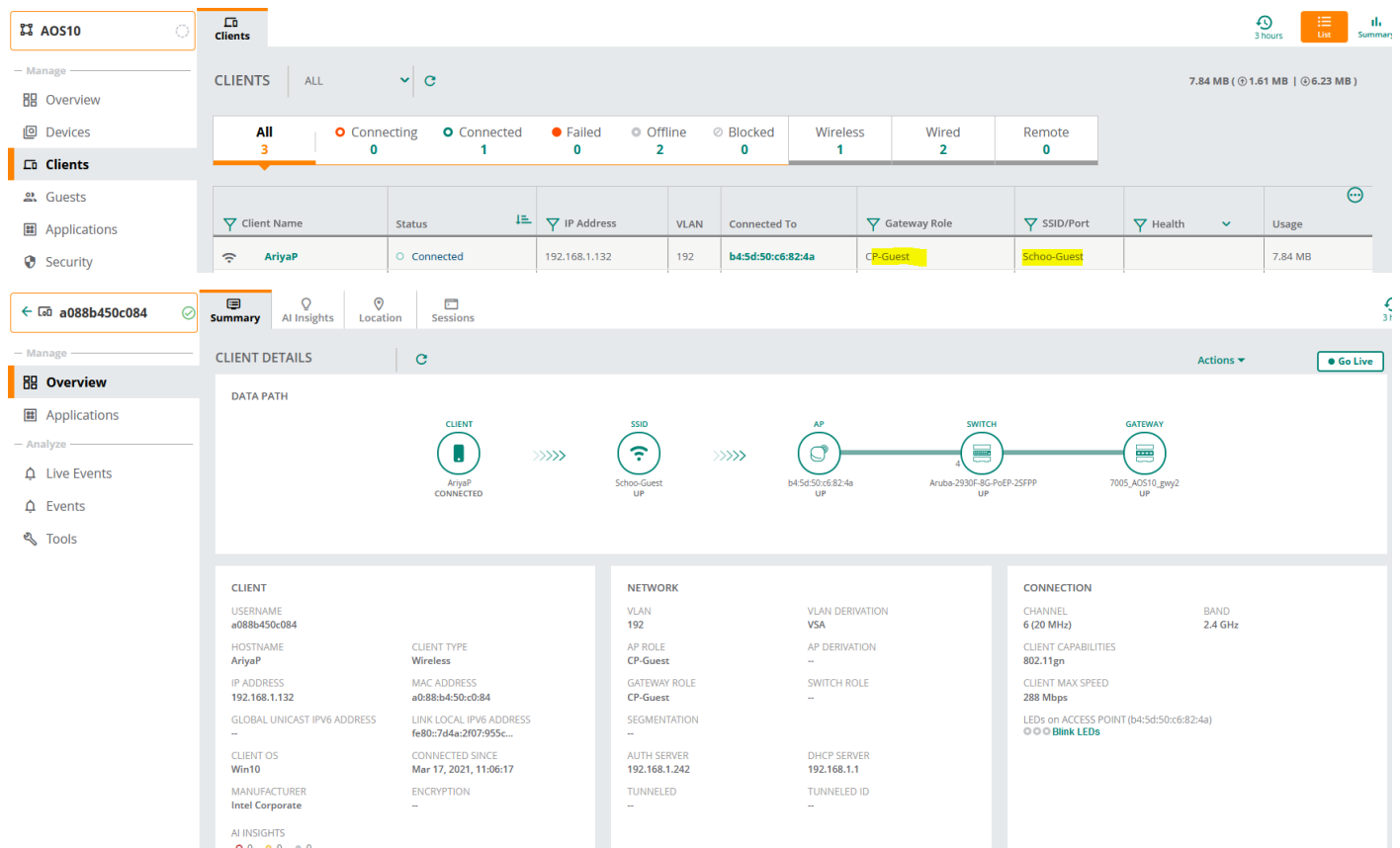
We'll have a look at the certificate, and we'll see it is the default captive portal certificate which is on the controller.



We'll accept this and carry on, but for all deployments you need to have a public server certificate for your controllers. Once we accept the certificate, we'll get redirected to the captive portal page on ClearPass



Before we login with our guest credentials, we'll look at the MM dashboard and see the user is in guest-login role with minimum access.

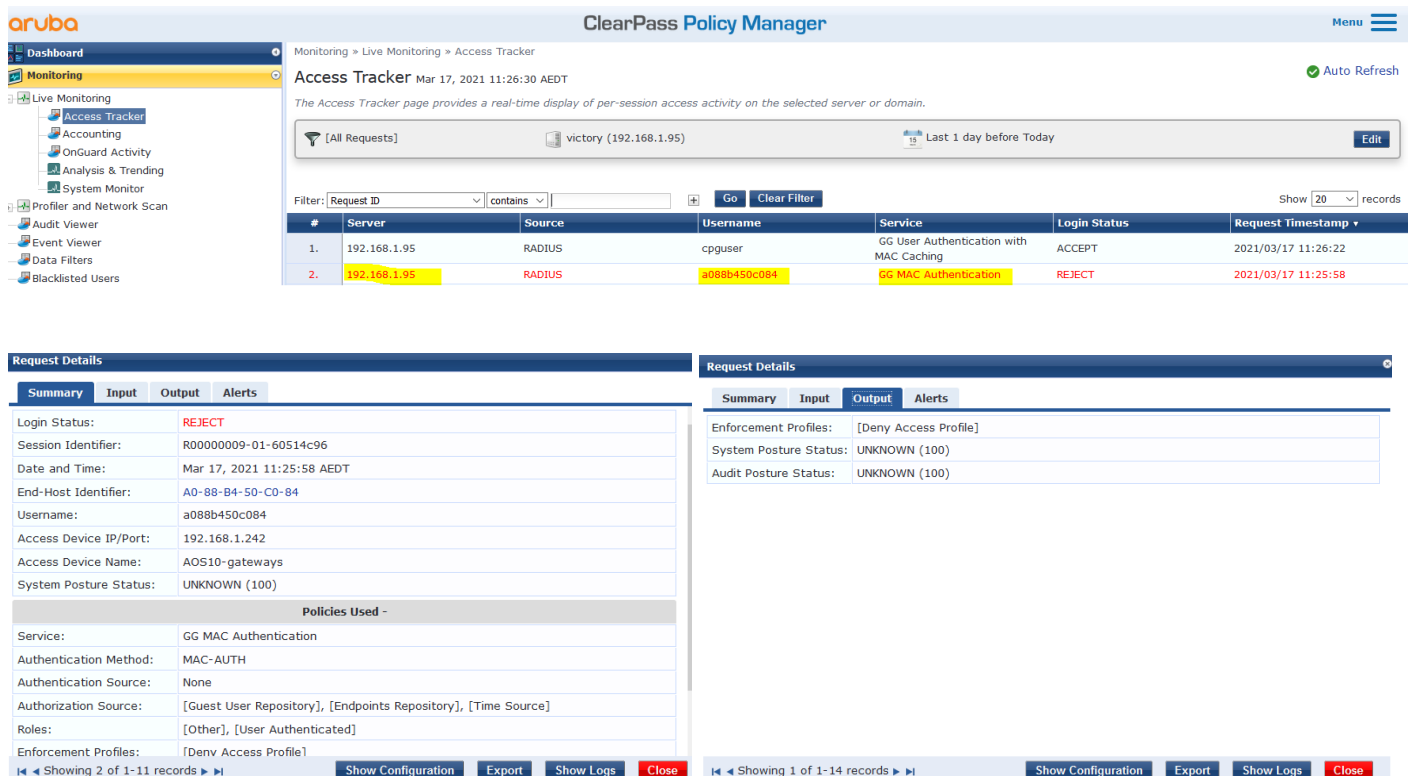


The screenshot shows the Aruba MM (Management Monitor) dashboard. The left sidebar has a 'Clients' section with a search bar containing 'AOS10'. The main area displays a 'CLIENTS' table with columns for Client Name, Status, IP Address, VLAN, Connected To, Gateway Role, SSID/Port, Health, and Usage. The table shows one client, 'AriyaP', with status 'Connected', IP '192.168.1.132', and gateway role 'CP-Guest'. Below the table, the 'CLIENT DETAILS' section shows a data path diagram and detailed client information.

Client Name	Status	IP Address	VLAN	Connected To	Gateway Role	SSID/Port	Health	Usage
AriyaP	Connected	192.168.1.132	192	b4:5d:50:c6:82:4a	CP-Guest	Schoo-Guest		7.84 MB

CLIENT		NETWORK		CONNECTION	
USERNAME	a088b450c084	VLAN	192	CHANNEL	6 (20 MHz)
HOSTNAME	AriyaP	AP ROLE	CP-Guest	CLIENT CAPABILITIES	802.11gn
IP ADDRESS	192.168.1.132	GATEWAY ROLE	CP-Guest	CLIENT MAX SPEED	288 Mbps
GLOBAL UNICAST IPV6 ADDRESS	--	SEGMENTATION	--	LEDs on ACCESS POINT (b4:5d:50:c6:82:4a)	LEDs on Blink LEDs
CLIENT OS	Win10	AUTH SERVER	192.168.1.242		
MANUFACTURER	Intel Corporate	TUNNELED	--		

Then we'll check the access tracker and see that we have a failed MAC authentication.



The screenshot shows the ClearPass Policy Manager 'Access Tracker' page. It displays a table of access requests. The second request is highlighted, showing a failed MAC authentication attempt for the user 'a088b450c084' on the server '192.168.1.95'.

#	Server	Source	Username	Service	Login Status	Request Timestamp
1.	192.168.1.95	RADIUS	cpguser	GG User Authentication with MAC Caching	ACCEPT	2021/03/17 11:26:22
2.	192.168.1.95	RADIUS	a088b450c084	GG MAC Authentication	REJECT	2021/03/17 11:25:58

Request Details	
Login Status:	REJECT
Session Identifier:	R00000009-01-60514c96
Date and Time:	Mar 17, 2021 11:25:58 AEDT
End-Host Identifier:	A0-88-B4-50-C0-84
Username:	a088b450c084
Access Device IP/Port:	192.168.1.242
Access Device Name:	AOS10-gateways
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	GG MAC Authentication
Authentication Method:	MAC-AUTH
Authentication Source:	None
Authorization Source:	[Guest User Repository], [Endpoints Repository], [Time Source]
Roles:	[Other], [User Authenticated]
Enforcement Profiles:	[Denv Access Profile]

This is normal as this MAC address has not been seen before.

It should be noted that the redirection happens from the AP not the gateways

```
b4:5d:50:c6:82:4a# sh client
```


Client List

```

-----
Name  IP Address  MAC Address  OS  ESSID  Access Point  Channel  Type  Role  IPv6
Address Signal  Speed (mbps)
-----
--
Number of Clients      :0
Info timestamp         :8460
b4:5d:50:c6:82:4a#
b4:5d:50:c6:82:4a#
b4:5d:50:c6:82:4a# sh client

```

Client List

```

-----
Name          IP Address      MAC Address      OS      ESSID      Access Point
Channel  Type  Role      IPv6 Address      Signal      Speed (mbps)
-----
a088b450c084  192.168.1.132  a0:88:b4:50:c0:84  Win 10  Schoo-Guest  b4:5d:50:c6:82:4a
6          GN      CP-Guest  fe80::7d4a:2f07:955c:cd4f  54(good)  72(ok)

```

```

Number of Clients      :1
Info timestamp         :9155

b4:5d:50:c6:82:4a#
b4:5d:50:c6:82:4a# sh external-captive-portal

```

External Captive Portal

```

-----
Name          Server          Port  Url          Auth Text          Redirect Url
Server Fail Through  Disable Auto Whitelist  Use HTTPs  Server Offload  Prevent Frame
Overlay  In Use  Redirect Mode  Switch IP
-----
default    localhost      80    /            Authenticated
Disable          Enable          Yes      No      Disable
No      Yes      No
CP-Guest  victory.clearpass.info  443    /guest/school.php
http://www.arubanetworks.com  Disable          Enable          Yes
No      Disable          Yes      Yes      No

```

```

b4:5d:50:c6:82:4a# sh external-captive-portal CP-Guest

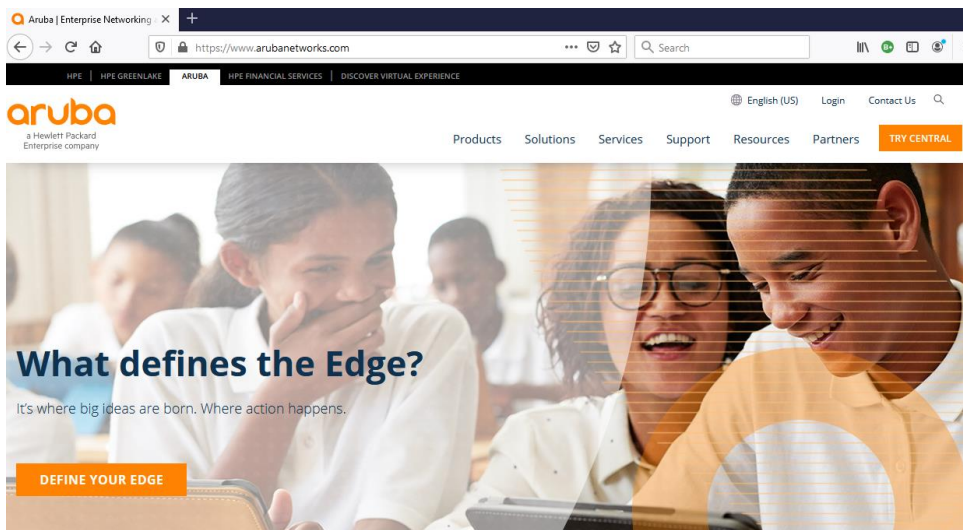
```

```

Name          :CP-Guest
Server        :victory.clearpass.info
Port          :443
Url           :/guest/school.php
Auth Text     :
Redirect Url   :http://www.arubanetworks.com
Server Fail Throuth :Disable
Disable Auto Whitelist :Enable
Use HTTPs     :Yes
Server Offload :No
Prevent Frame Overlay :Disable
In Used       :Yes
Redirect Mode  :Yes
Switch IP     :No
b4:5d:50:c6:82:4a#

```

Now when the user performs a successful the login (we are using username cpguser) process, they will be redirected to the "redirect URL" that we specified.



Now let's look at the Client dashboard and access tracker, note that the user role is now "guest".

Client Name	Status	IP Address	VLAN	Connected To	Gateway Role	SSID/Port	Health	Usage
cpguser	Connected	192.168.1.132	192	b4:5d:50:c6:82:4a	guest	Schoo-Guest	Good	8.31 MB

And the access tracker shows a successful authentication that matches with "GG User Authentication with MAC Caching" policy.

#	Server	Source	Username	Service	Login Status	Request Timestamp
1.	192.168.1.95	RADIUS	cpguser	GG User Authentication with MAC Caching	ACCEPT	2021/03/17 11:26:22
2.	192.168.1.95	RADIUS	a088b450c084	GG MAC Authentication	REJECT	2021/03/17 11:25:58

Request Details	
Summary	Input / Output / Accounting
Login Status:	ACCEPT
Session Identifier:	R0000000a-01-60514cae
Date and Time:	Mar 17, 2021 11:26:22 AEDT
End-Host Identifier:	A0-88-B4-50-C0-84
Username:	cpguser
Access Device IP/Port:	192.168.1.242
Access Device Name:	AOS10-gateways
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	GG User Authentication with MAC Caching
Authentication Method:	PAP
Authentication Source:	Local:localhost
Authorization Source:	[Guest User Repository], [Endpoints Repository], [Time Source]
Roles:	[Guest], [User Authenticated]
Enforcement Profiles:	GG MAC Caching Bandwidth Limit, GG MAC Caching Session Limit, GG Guest MAC

Request Details

Summary Input Output Accounting

Audit Posture Status: UNKNOWN (100)

RADIUS Response

Bandwidth-Check:Allowed-Limit	0
Bandwidth-Check:Check-Type	Today
Bandwidth-Check:Limit-Units	MB
Endpoint:Guest Role ID	2
Endpoint:MAC-Auth Expiry	2021-03-18 11:00:00
Endpoint:Username	cpguser
Expire-Time-Update:GuestUser	0
Expiry-Check:Expiry-Action	0
Post-Auth-Check:Action	Disconnect
Post-Auth-Check:Action	Disconnect and Block Access
Radius:Aruba:Aruba-User-Role	Guest
Radius:IETF:Session-Timeout	0

Showing 1 of 1-11 records

Change Status Show Configuration Export Show Logs Close

Also note that one of the post authentication actions were to update the endpoint repository status for that MAC address to be known.

Dashboard Monitoring Configuration

Configuration > Identity > Endpoints

Endpoints

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 Go Clear Filter

Show 20 records

#	MAC Address	Hostname	Device Category	Device OS Family	Status	Profiled
1.	00-0C-29-F3-EF-AF	victory	Server	ClearPass	Unknown	Yes
2.	A0-88-B4-50-C0-84		Computer	Windows	Known	Yes

Showing 1-2 of 2

Authentication Records Bulk Update Bulk Delete Trigger Server Action Update Fingerprint Export Delete

Now because the status of this endpoint is known the next time, this client connects it will not be redirected to the captive portal until its allotted time has expired. So now if we disconnect the client, we should see it will successfully MAC auths. This uses RADIUS CoA. We can do that directly from the access tracker.

Request Details

Summary Input Output Accounting

Login Status: ACCEPT

Session Identifier: R0000000a-01-60514cae

Date and Time: Mar 17, 2021 11:26:22 AEDT

End-Host Identifier: A0-88-B4-50-C0-84

Username: cpguser

Access Device IP/Port: 192.168.1.242

Access Device Name: AOS10-gateways

System Posture Status: UNKNOWN (100)

Policies Used -

Service: GG User Authentication with MAC Caching

Authentication Method: PAP

Authentication Source: Local:localhost

Authorization Source: [Guest User Repository], [Endpoints Repository], [Time Source]

Roles: [Guest], [User Authenticated]

Enforcement Profiles: GG MAC Caching Bandwidth Limit. GG MAC Caching Session Limit. GG Guest MAC

Showing 1 of 1-11 records

Change Status Show Configuration Export Show Logs Close

Request Details

Access Control Capabilities -

Select Access Control Type : Agent SNMP RADIUS CoA Server Action

RADIUS CoA Type: [ArubaOS Wireless - Terminat

Submit Cancel

Request Details

Radius [ArubaOS Wireless - Terminate Session] successful for client a088b450c084

Summary Input Output Accounting

Login Status: ACCEPT

Session Identifier: R0000000a-01-60514cae

Date and Time: Mar 17, 2021 11:26:22 AEDT

End-Host Identifier: A0-88-B4-50-C0-84

Username: cpguser

Access Device IP/Port: 192.168.1.242

Access Device Name: AOS10-gateways

System Posture Status: UNKNOWN (100)

Policies Used -

Service: GG User Authentication with MAC Caching

Authentication Method: PAP

Authentication Source: Local:localhost

Authorization Source: [Guest User Repository], [Endpoints Repository], [Time Source]

Roles: [Guest], [User Authenticated]

Enforcement Profiles: GG MAC Caching Bandwidth Limit. GG MAC Caching Session Limit. GG Guest MAC

Showing 1 of 1-11 records

Change Status Show Configuration Export Show Logs Close

aruba ClearPass Policy Manager

Monitoring » Live Monitoring » Access Tracker

Access Tracker Mar 17, 2021 11:33:25 AEDT

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

[All Requests] victory (192.168.1.95) Last 1 day before Today

Filter: Request ID contains Go Clear Filter Show 20 records

#	Server	Source	Username	Service	Login Status	Request Timestamp
1.	192.168.1.95	RADIUS	cpguser	GG MAC Authentication	ACCEPT	2021/03/17 11:33:04
2.	192.168.1.95	RADIUS	cpguser	GG User Authentication with MAC Caching	ACCEPT	2021/03/17 11:26:22
3.	192.168.1.95	RADIUS	a088b450c084	GG MAC Authentication	REJECT	2021/03/17 11:25:58

Looking at the details of that session

Request Details

Summary Input Output Accounting

Login Status: ACCEPT
Session Identifier: R0000000b-01-60514e40
Date and Time: Mar 17, 2021 11:33:04 AEDT
End-Host Identifier: A0-88-B4-50-C0-84
Username: cpguser
Access Device IP/Port: 192.168.1.242
Access Device Name: AOS10-gateways
System Posture Status: UNKNOWN (100)

Policies Used -

Service: GG MAC Authentication
Authentication Method: MAC-AUTH
Authentication Source: Local:localhost
Authorization Source: [Guest User Repository], [Endpoints Repository], [Time Source]
Roles: [Guest], [MAC Caching], [User Authenticated]
Enforcement Profiles: [Allow Access Profile], GG Guest Device Profile

Request Details

Summary Input Output Accounting

Enforcement Profiles: [Allow Access Profile], GG Guest Device Profile
System Posture Status: UNKNOWN (100)
Audit Posture Status: UNKNOWN (100)

RADIUS Response

Radius:Aruba:Aruba-User-Role Guest
Radius:IETF:User-Name cpguser

Showing 1 of 1-12 records Change Status Show Configuration Export Show Logs Close

Here we can see the user in the gateway's user table using tunnel forwarding mode and in guest user role.

```
(7005_AOS10_gwy2) #show user
This operation can take a while depending on number of users. Please be patient ....

Users
-----
IP           MAC           Name           Role           Age(d:h:m)   Auth   VPN link
Connected To Roaming   Essid/Bssid/Phy Profile
mode Type   Host Name  User Type
-----
192.168.1.132 a0:88:b4:50:c0:84 a088b450c084 guest 00:00:03 MAC
b4:5d:50:c6:82:4a Wireless Schoo-Guest Schoo-Guest_#1615938135060_41# dtunnel
Win 10 WIRELESS

User Entries: 1/1
Curr/Cum Alloc:1/6 Free:0/5 Dyn:1 AllocErr:0 FreeErr:0
(7005_AOS10_gwy2) #
```