1 Table of Contents

Table of Contents

1.1 Revision History

DATE	VERSION	EDITOR	CHANGES
17 Mar 2024	0.1	Ariya Parsamanesh	Initial creation
21 Mar 2024	0.2	Ariya Parsamanesh	Added the authentication proxy section

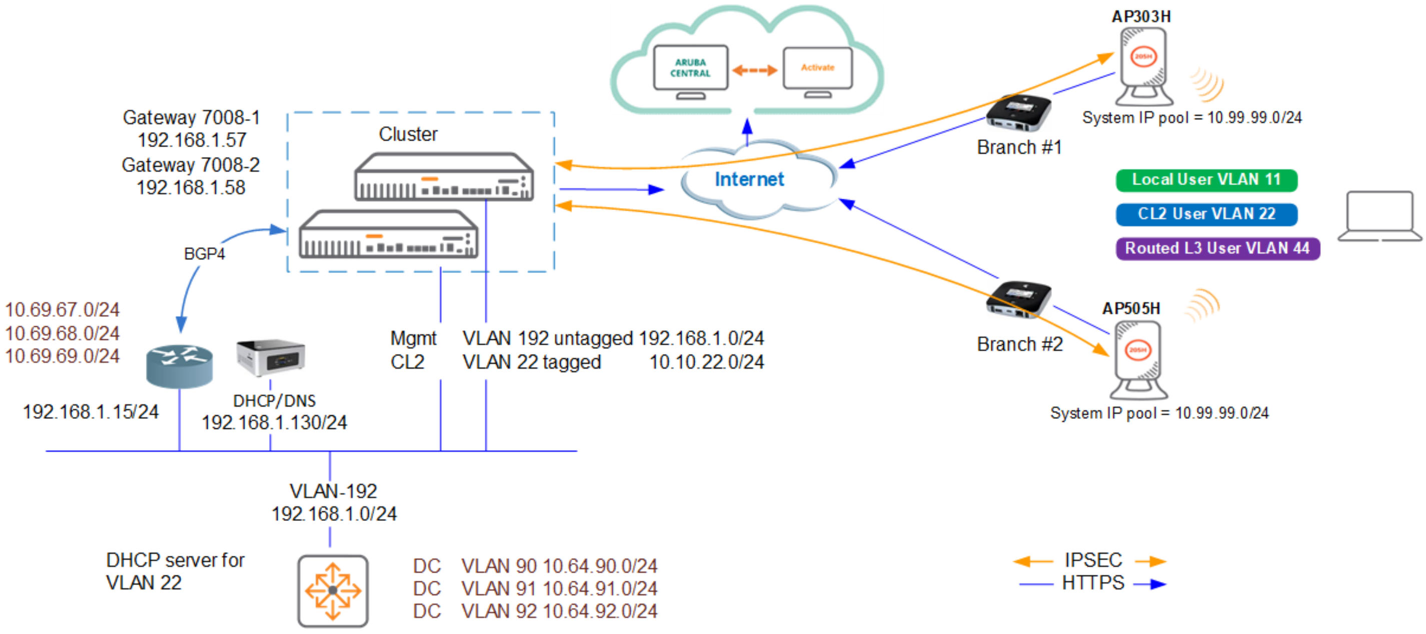
2 Microbranch with AOS10

AOS 10.x enables APs in remote sites to use most of the SD-WAN features and be managed by Aruba Central. For Micro Branch deployments, AOS 10.x currently supports deployment of a single AP as a Micro Branch AP in remote sites. The AOS 10.x enables these APs to form orchestrated IPsec tunnels to the Gateway cluster.

Microbranch APs support

- Orchestrated tunnels and routes (hub & spoke)
- VPNC Clustering
- PBR for local breakout (incl. 1st packet classification)
- Gateway Like WAN Monitoring
- Cloud Security Orchestration (Aruba AXIS, ZScaler, etc)

The topology that we'll be deploying is as shown below.



This is a 5x parts microbranch series. The aim here is to provide the starting point to put together a solution that include the AOS10 APs as microbranch, two VPNCs that are clustered along with Aruba Central to configure and monitor the solution.

- Part1 – Solution overview, basic configuration and testing of VPNC and AOS10 AP
- Part2 – Centralised L2 forwarding mode with authentication and policy-based routing
- Part3 – NATed Layer 3 forwarding mode with centralised authentication proxy
- Part4 – Routed Layer 3 forwarding mode with centralised authentication proxy
- Part5 – Overlay Route Orchestrator, route summarisation, BGP routes redistribution and monitoring

2.1 Things you need

- Two AOS10 APs running 10.4.0.2 or later
- AOS10 VPNCs running 10.4.0.2 or later
- Aruba Central account with eval licenses.
- LAN switch
- Operational Internet link

2.2 IP Addressing

This tables shows the IP addressing, subnets and routes that we'll be using.

	System IP Pool	Local VLAN (SNAT)	Centralised L2	Routed L3 (shared Pool)	Configured Routes
	Used for Tunnel-inner-ip	VLAN11	VLAN22	VLAN44	
Microbranch1	10.99.99.7/32	10.11.11.1/24		10.44.44.81/28	
Microbranch2	10.99.99.4/32	10.11.11.1/24		10.44.44.17/28	
DC DHCP server			10.10.22.1/24		
VPNC 1	192.168.1.57/24				
VPNC 2	192.168.1.58/24				
VPNC – static routes					10.64.90.0/24 10.64.91.0/24 10.64.92.0/24
VPNC – BGP routes					10.69.67.0/24 10.69.68.0/24 10.69.69.0/24

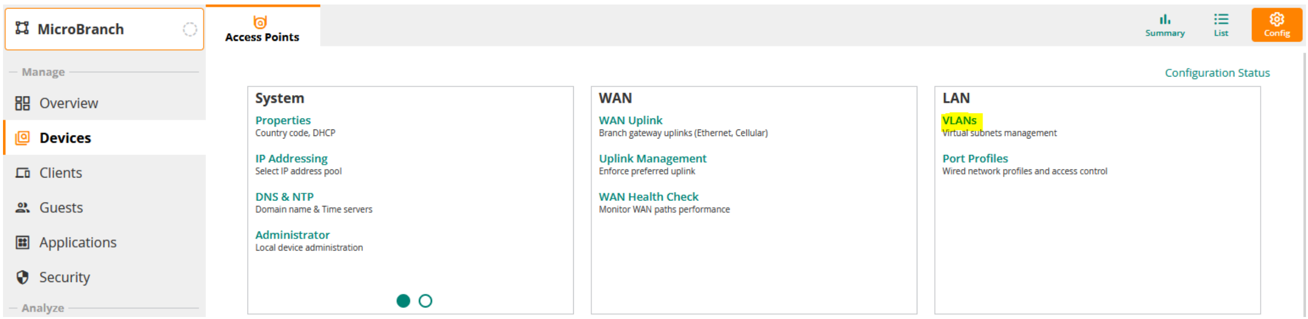
3 Microbranch NATed L3 Configuration

In this section we'll configure a simple local VLAN 11 that will use for "br-local" SSID. In this mode

- DHCP service for the VLAN is performed by the DHCP server in the AP.
- The client will not have connectivity to the DC routes. As the Local subnet is not known to the VPNCs.
- Client traffic to Internet is source NATed with the AP's uplink IP address.
- The forwarding mode will be NATed L3, and this VLAN11 is not advertised to VPNC clusters by ORO.
- This mode is suitable for the case where we don't want the user subnets to be visible to DC and the traffic only needs to be initiated from a branch.
- For authentication you can use the VPNC cluster for RADIUS proxy, otherwise you can configure your authentication server and use the local subnet to reach it.

3.1 NATed VLAN Configuration

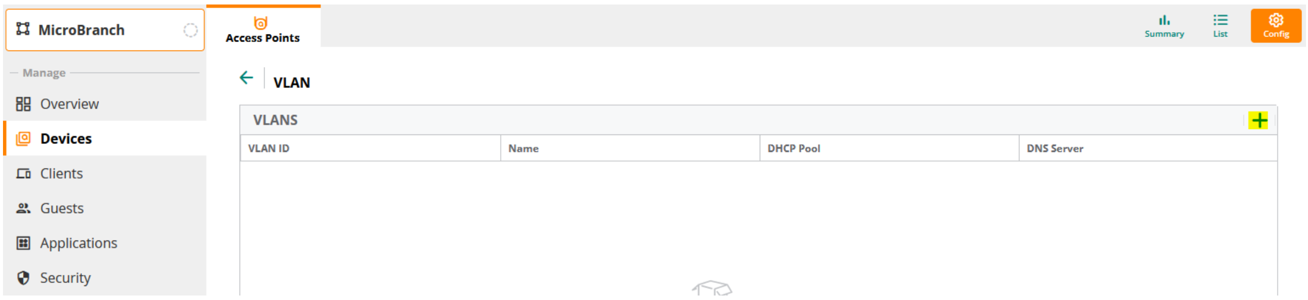
From the group level we'll select the microbranch group and then VLANs.



System
Properties
Country code, DHCP
IP Addressing
Select IP address pool
DNS & NTP
Domain name & Time servers
Administrator
Local device administration

WAN
WAN Uplink
Branch gateway uplinks (Ethernet, Cellular)
Uplink Management
Enforce preferred uplink
WAN Health Check
Monitor WAN paths performance

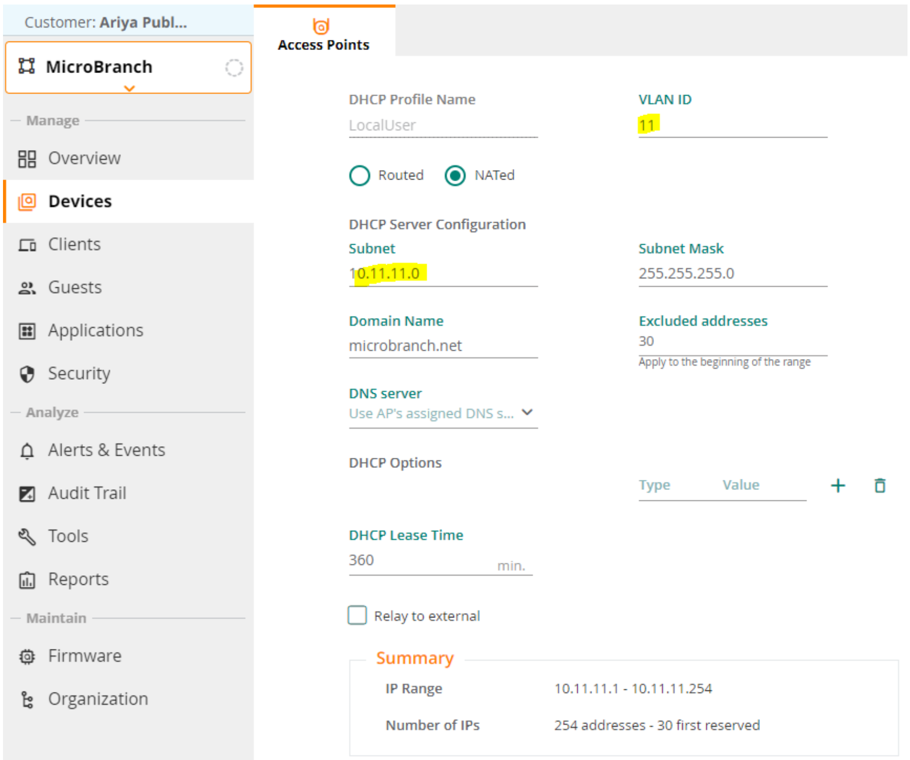
LAN
VLANs
Virtual subnets management
Port Profiles
Wired network profiles and access control



VLAN

VLANS

VLAN ID	Name	DHCP Pool	DNS Server



DHCP Profile Name
LocalUser

VLAN ID
11

○ Routed ● NATed

DHCP Server Configuration

Subnet
10.11.11.0

Subnet Mask
255.255.255.0

Domain Name
microbranch.net

Excluded addresses
30
Apply to the beginning of the range

DNS server
Use AP's assigned DNS s...

DHCP Options
Type Value +

DHCP Lease Time
360 min.

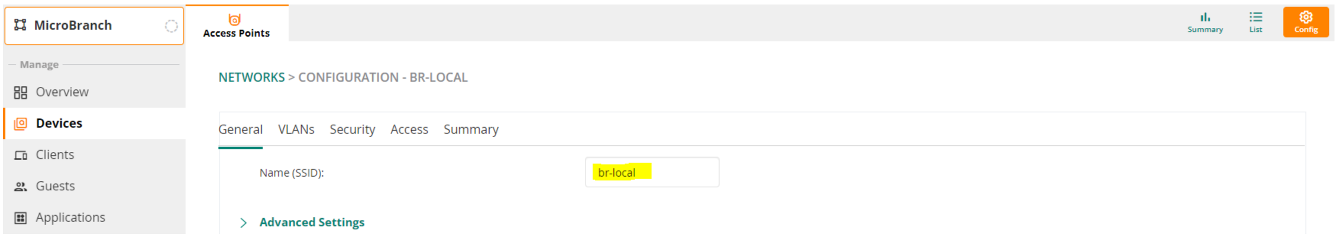
□ Relay to external

Summary

IP Range	10.11.11.1 - 10.11.11.254
Number of IPs	254 addresses - 30 first reserved

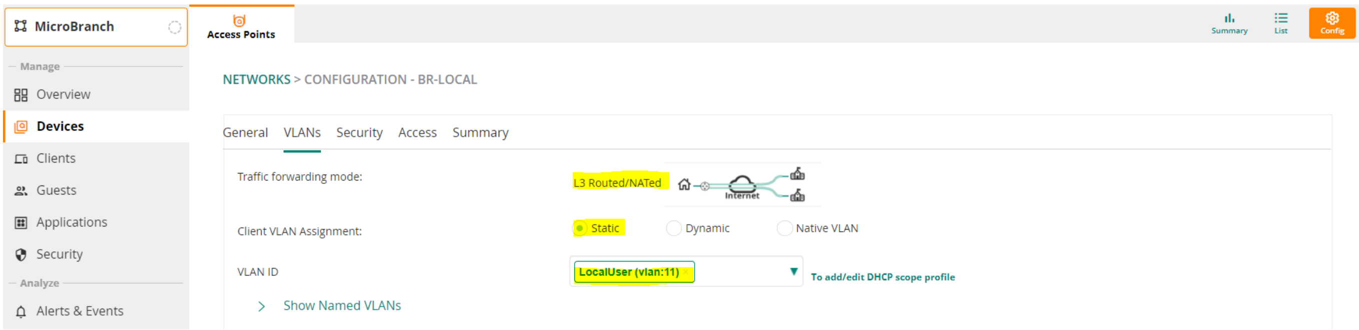
3.2 Local WLAN Configuration

We'll start with local VLAN 11 configuration and then with the WLAN.



NETWORKS > CONFIGURATION - BR-LOCAL

Name (SSID): br-local

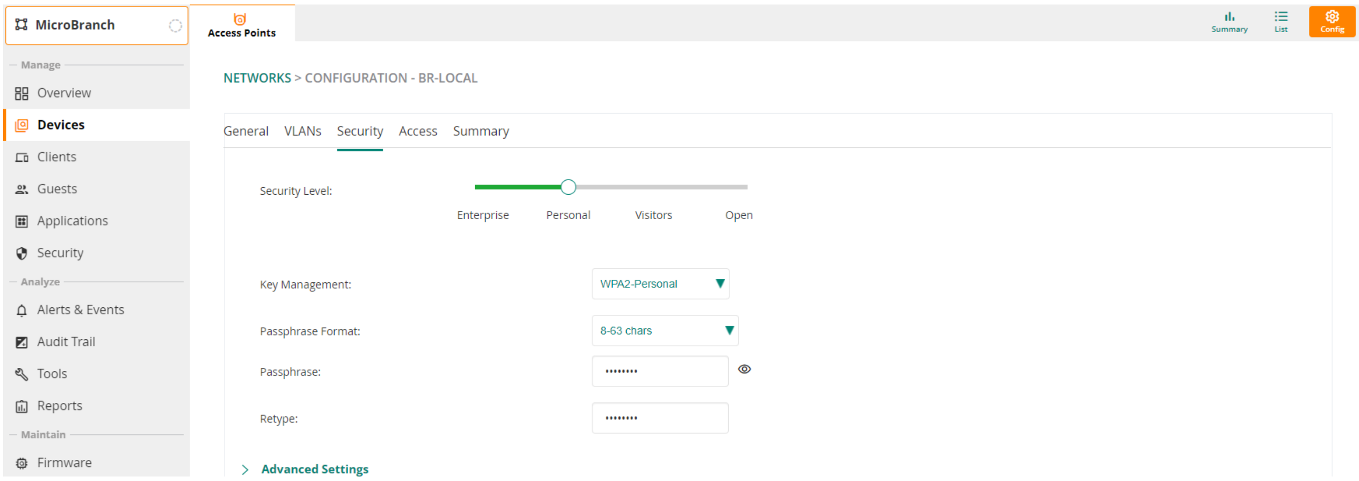


NETWORKS > CONFIGURATION - BR-LOCAL

Traffic forwarding mode: L3 Routed/NATed

Client VLAN Assignment: ● Static ○ Dynamic ○ Native VLAN

VLAN ID: LocalUser (vlan:11)



NETWORKS > CONFIGURATION - BR-LOCAL

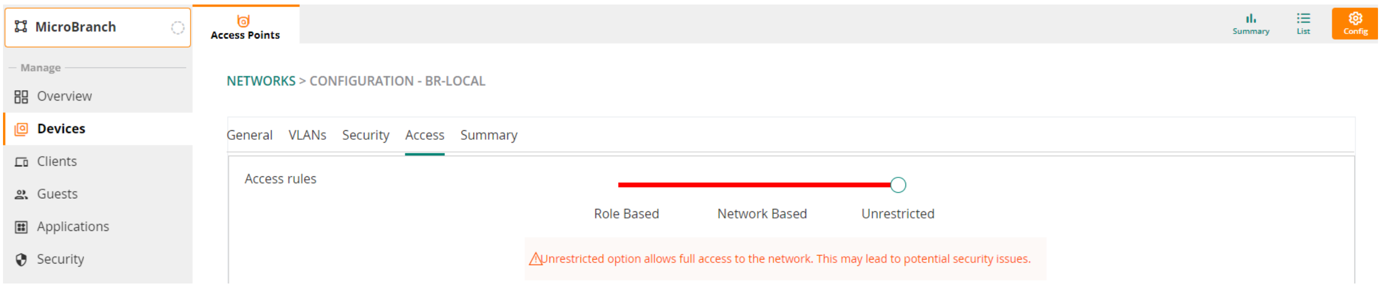
Security Level: Personal

Key Management: WPA2-Personal

Passphrase Format: 8-63 chars

Passphrase: ••••••••

Retype: ••••••••



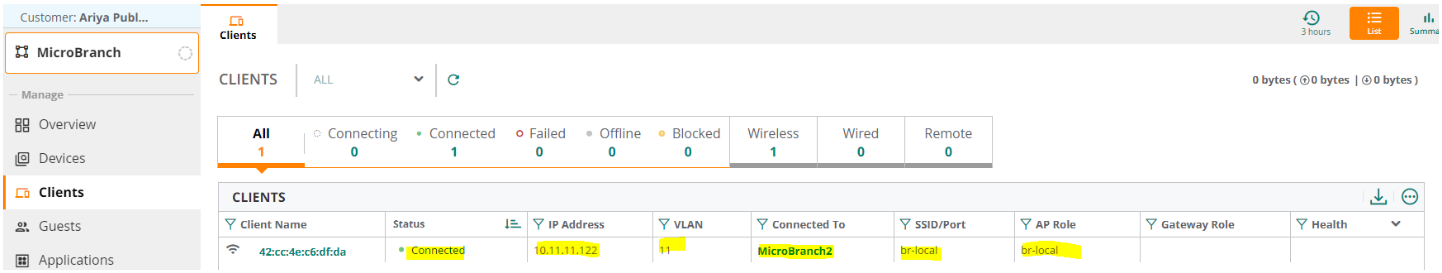
NETWORKS > CONFIGURATION - BR-LOCAL

Access rules: Unrestricted

⚠Unrestricted option allows full access to the network. This may lead to potential security issues.

3.3 NATed L3 SSID Testing

Now save it and we are ready to test it out by getting a client to connect to br-local SSID.



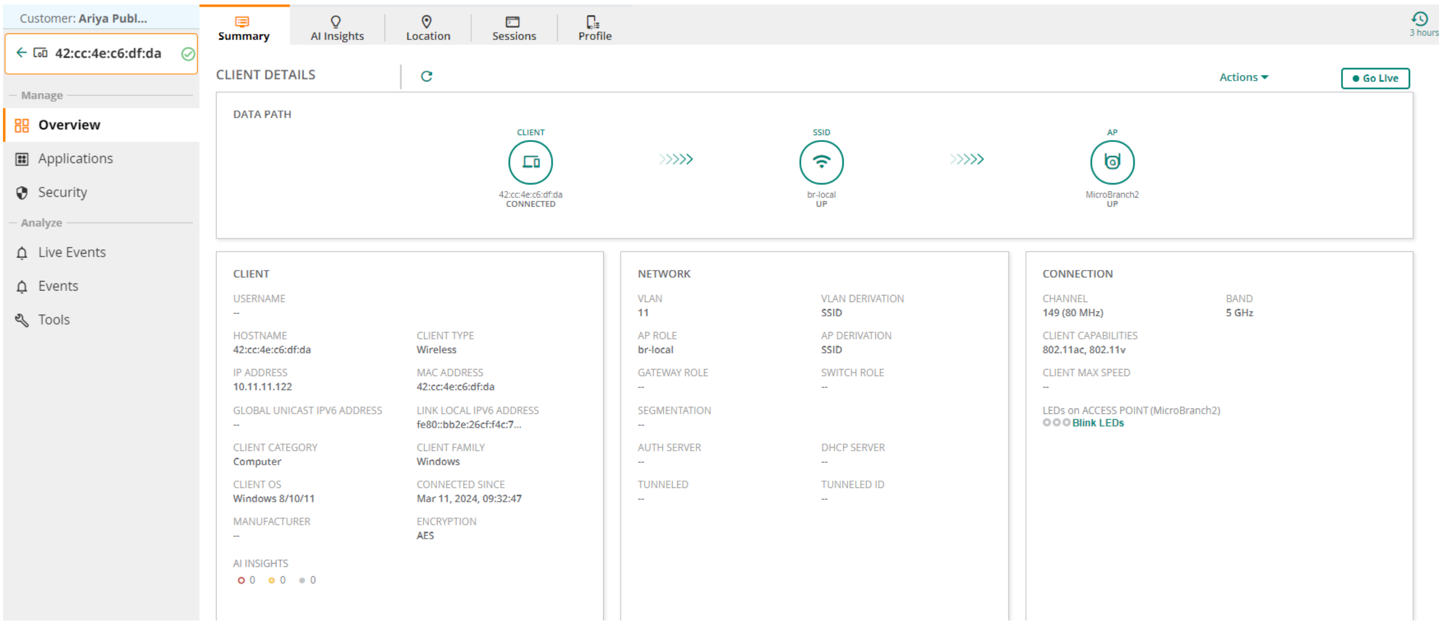
CLIENTS ALL

0 bytes (0 bytes | 0 bytes)

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

CLIENTS

Client Name	Status	IP Address	VLAN	Connected To	SSID/Port	AP Role	Gateway Role	Health
42:cc:4e:c6:df:da	Connected	10.11.11.122	11	MicroBranch2	br-local	br-local		



CLIENT DETAILS

DATA PATH

42:cc:4e:c6:df:da CONNECTED → br-local UP → MicroBranch2 UP

CLIENT

USERNAME: --

HOSTNAME: 42:cc:4e:c6:df:da

CLIENT TYPE: Wireless

IP ADDRESS: 10.11.11.122

MAC ADDRESS: 42:cc:4e:c6:df:da

GLOBAL UNICAST IPV6 ADDRESS: --

LINK LOCAL IPV6 ADDRESS: fe80::bb2e:26cf:f4c:7...

CLIENT CATEGORY: Computer

CLIENT FAMILY: Windows

CLIENT OS: Windows 8/10/11

CONNECTED SINCE: Mar 11, 2024, 09:32:47

MANUFACTURER: --

ENCRYPTION: AES

AI INSIGHTS: 0 0 0

NETWORK

VLAN: 11

VLAN DERIVATION: SSID

AP ROLE: br-local

AP DERIVATION: SSID

GATEWAY ROLE: --

SWITCH ROLE: --

SEGMENTATION: --

AUTH SERVER: --

DHCP SERVER: --

TUNNELED: --

TUNNELED ID: --

CONNECTION

CHANNEL: 149 (80 MHz)

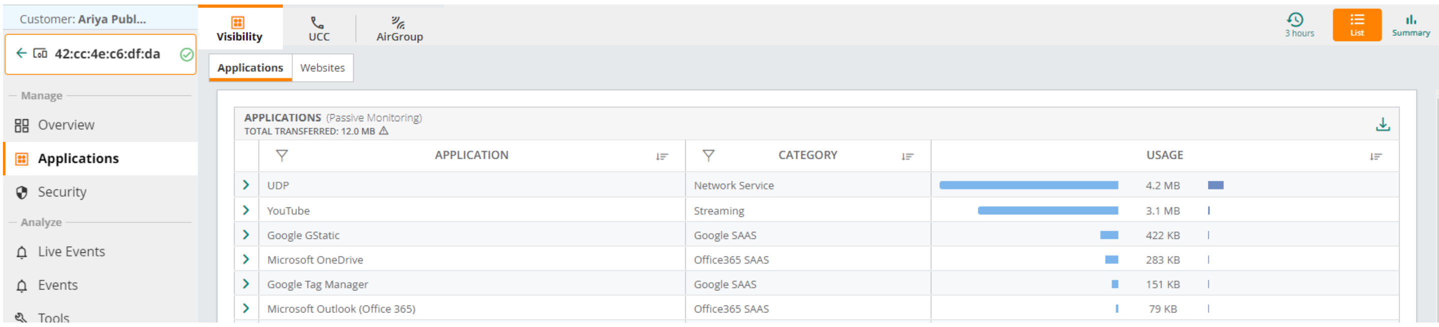
BAND: 5 GHz

CLIENT CAPABILITIES: 802.11ac, 802.11v

CLIENT MAX SPEED: --

LEDs on ACCESS POINT (MicroBranch2)

Checking the applications that the user is accessing.



APPLICATIONS (Passive Monitoring)
TOTAL TRANSFERRED: 12.0 MB

APPLICATION	CATEGORY	USAGE
UDP	Network Service	4.2 MB
YouTube	Streaming	3.1 MB
Google GStatic	Google SAAS	422 KB
Microsoft OneDrive	Office365 SAAS	283 KB
Google Tag Manager	Google SAAS	151 KB
Microsoft Outlook (Office 365)	Office365 SAAS	79 KB

```
MicroBranch2# sh clients

Client List
-----------
Name  IP Address    MAC Address        OS     ESSID     Access Point  Channel  Type  
Role       IPv6 Address              Signal(dB)  Speed (Mbps)
----  ----------    -----------        --     -----     ------------  -------  ----  ---
-      ------------               ----------  ------------
      10.11.11.122  42:cc:4e:c6:df:da  Win 10  br-local  MicroBranch2  149E     AC    br-
local  fe80::bb2e:26cf:f4c:7b95  43(good)    780(good)
Number of Clients   :1
Info timestamp      :559

MicroBranch2#
```

Note that DC bound traffic from a NATed L3 mode client will be source NATed from the AP's inner IP. This means that you cannot initiate a session from DC to that subnet.

```
MicroBranch2# sh ip int b
Interface                         IP Address / IP Netmask       Admin  Protocol
br0                              169.254.1.1 / 255.255.0.0       up     up
br0.11                            10.11.11.1 / 255.255.255.0     up     up
br0.3333                         172.31.98.1 / 255.255.254.0     up     up
br0.4092                      10.224.254.157 / 255.255.255.128   up     up

MicroBranch2#
```

Now from the client we'll ping www.hp.com and check the datapath session to see if it is getting source NATed.

Here are the flags

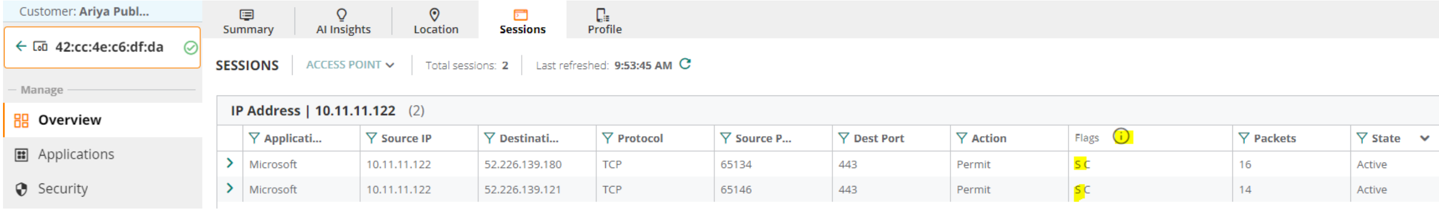
```
Flags: A - Application Firewall Inspect
       C - client, D - deny, E - Media Deep Inspect
       F - fast age, G - media signal, H - high prio
       I - Deep inspect, L - ALG session, M - mirror, N - dest NAT
       O - Session is programmed through SDN/Openflow controller
       P - set prio, R - redirect, S - src NAT,
       T - set ToS, U - Locally destined, V - VOIP
       X - Http/https redirect for dpi denied session
       Y - no syn
       a - rtp analysis, h - Https redirect error page
       i - in offload flow, m - media mon
       p - Session is marked as permanent
       s - media signal
       d - DPI cache hit
       f - FIB init pending in session
RAP Flags: 0 - Q0, 1 - Q1, 2 - Q2, r - redirect to conductor
           t - time based, i - in flow, l - local redirect
Flow Offload Denylist Flags: O - Openflow, E - Default, U - User os unknown, T - Tunnel
                             R - L3 route
```

And here is the session table for it, where we see a bunch of S flags

```
MicroBranch2# sh datapath session | incl 11.122
10.11.11.122      192.168.2.1      17    49860 53     0     0     0    0    dev40        50    2        70    FSCId   E
10.11.11.122      20.69.137.228    6     65145 443    0     0     0    4    dev40        2c1   16       2a67  SCid
10.11.11.122      184.50.237.185   1     70    2048   0     0     0    1    dev40        4f    1        3c    FSCI
10.11.11.122      184.50.237.185   1     71    2048   0     0     0    0    dev40        45    1        3c    FSCI
10.11.11.122      184.50.237.185   1     72    2048   0     0     0    0    dev40        3a    1        3c    FSCI
10.11.11.122      184.50.237.185   1     73    2048   0     0     0    0    dev40        30    1        3c    FSCI
10.11.11.122      52.226.139.180   6     65134 443    0     0     0    12   dev40        76e   d        c19   SCid
10.11.11.122      52.226.139.121   6     65146 443    0     0     0    4    dev40        2b9   e        a46   Sci

MicroBranch2#
```

Here is how you can check it from Aruba Central.



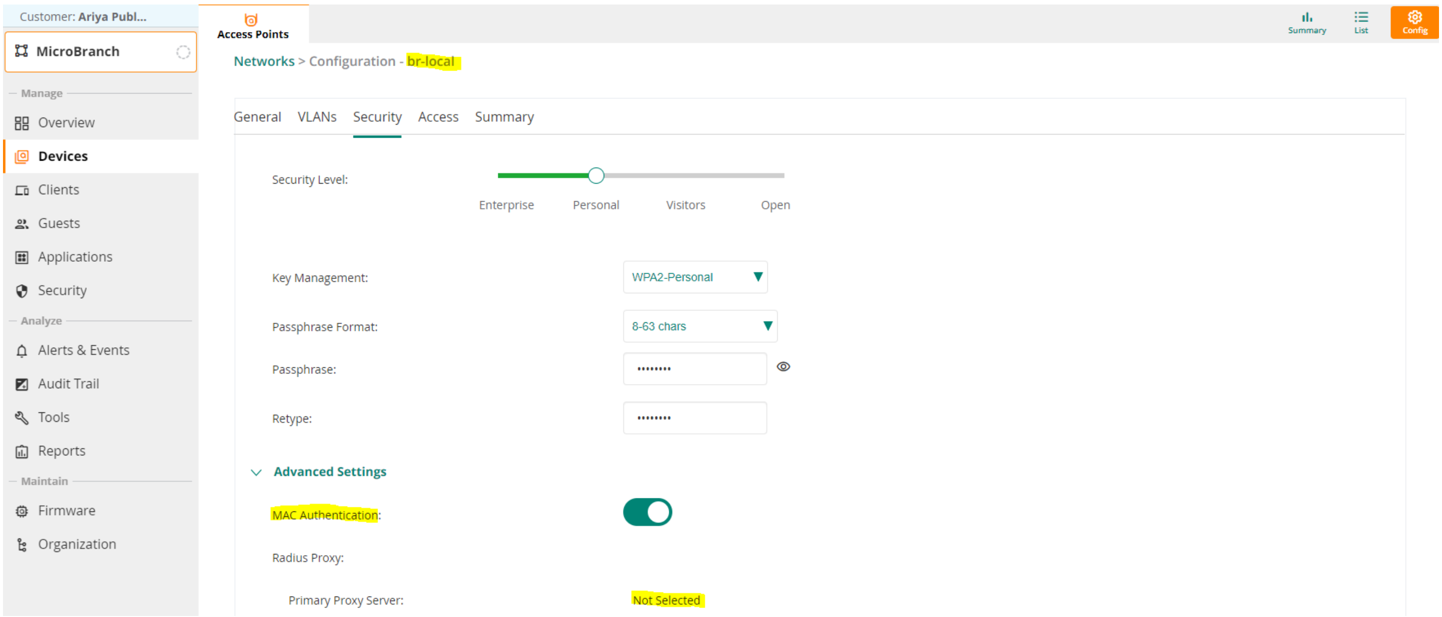
SESSIONS Total sessions: 2 Last refreshed: 9:53:45 AM

IP Address | 10.11.11.122 (2)

Applicati...	Source IP	Destinati...	Protocol	Source P...	Dest Port	Action	Flags	Packets	State
Microsoft	10.11.11.122	52.226.139.180	TCP	65134	443	Permit	S C	16	Active
Microsoft	10.11.11.122	52.226.139.121	TCP	65146	443	Permit	S C	14	Active

3.4 NATed L3 With Authentication Proxy

Here we have added a MAC auth to our PSK based SSID just to demonstrate what happens during the authentication process. When you want to use authentication, you have a choice to use the VPNCs as radius proxy. You can choose this option only when you create a new WLAN and not when you want to modify an existing RL3 type wlan as shown below, where we have selected MAC auth for existing NATed L3 WLAN.



Networks > Configuration - br-local

Security Level: Enterprise Personal Visitors Open

Key Management: WPA2-Personal

Passphrase Format: 8-63 chars

Passphrase: ••••••••

Retype: ••••••••

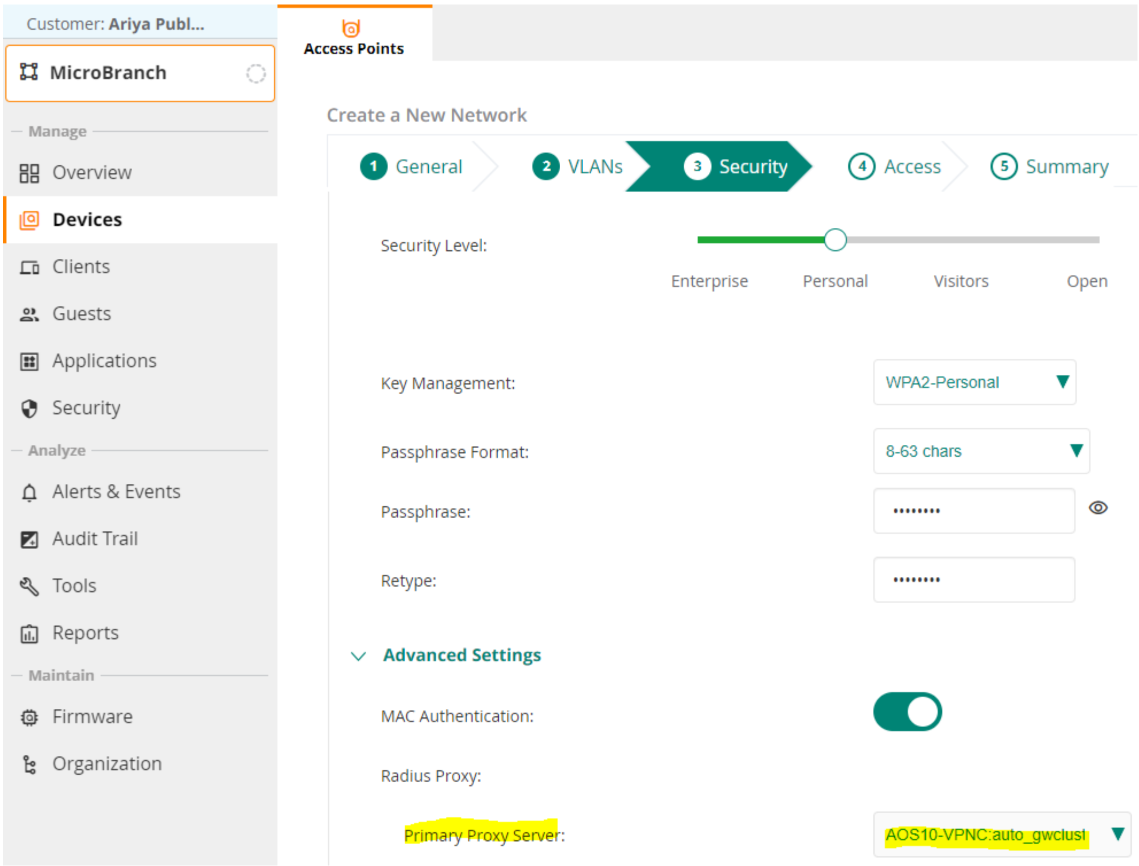
Advanced Settings

MAC Authentication:

Radius Proxy:

Primary Proxy Server: Not Selected

If you want to use the feature, you must select proxy server option when you create a WLAN as shown below.



Create a New Network

Security Level: Enterprise Personal Visitors Open

Key Management: WPA2-Personal

Passphrase Format: 8-63 chars

Passphrase: ••••••••

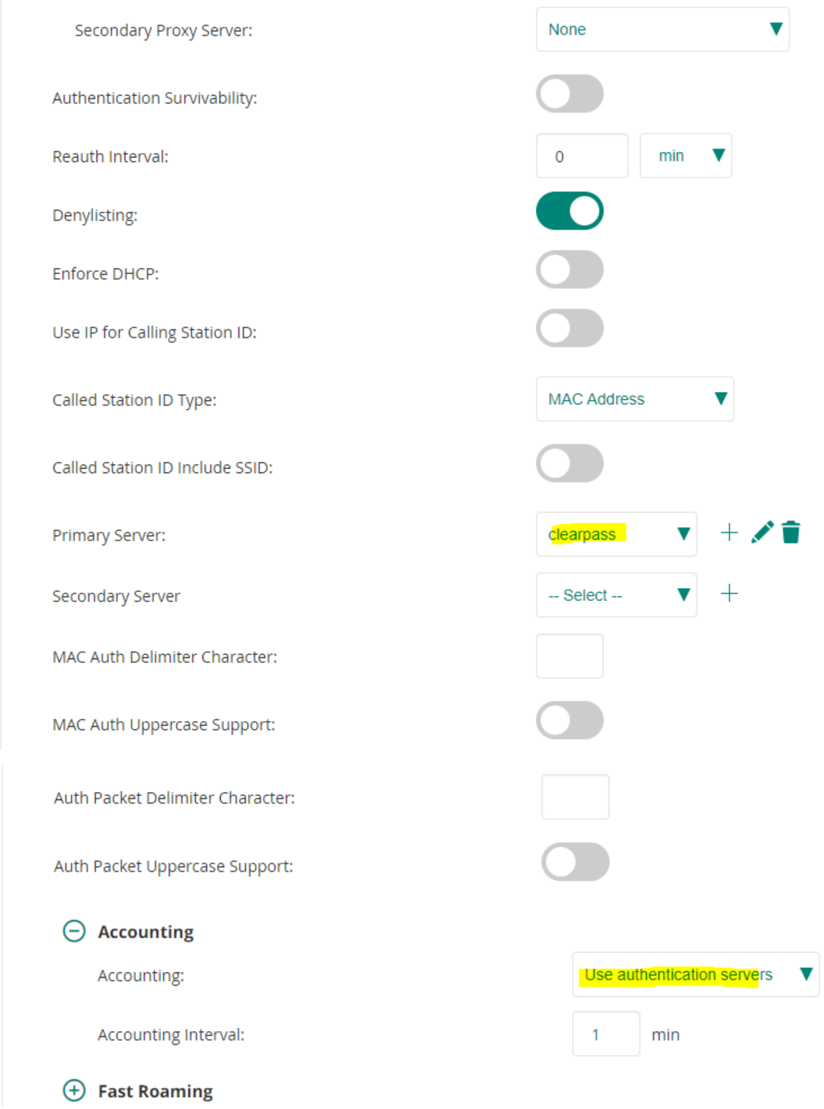
Retype: ••••••••

Advanced Settings

MAC Authentication:

Radius Proxy:

Primary Proxy Server: AOS10-VPNC:auto_gwclust



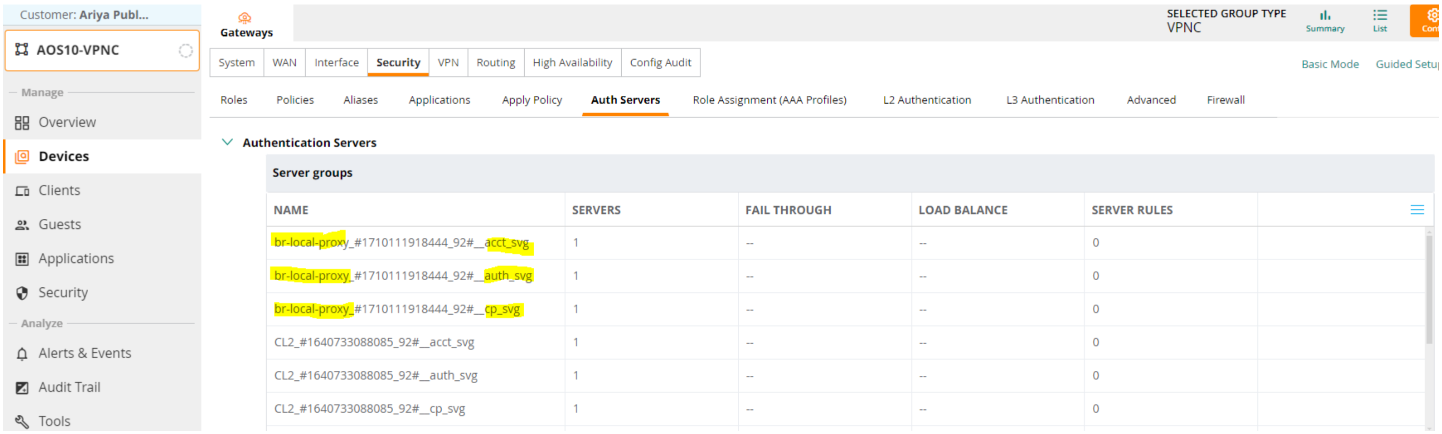
Secondary Proxy Server:	None ▼
Authentication Survivability:	○
Reauth Interval:	0 min ▼
Denylisting:	●
Enforce DHCP:	○
Use IP for Calling Station ID:	○
Called Station ID Type:	MAC Address ▼
Called Station ID Include SSID:	○
Primary Server:	clearpass ▼
Secondary Server	-- Select -- ▼
MAC Auth Delimiter Character:	
MAC Auth Uppercase Support:	○
Auth Packet Delimiter Character:	
Auth Packet Uppercase Support:	○

Accounting

Accounting:	Use authentication servers ▼
Accounting Interval:	1 min

Fast Roaming

Here I have created a new SSID called br-local-proxy and I have enabled MAC auth for it with VPNC as authentication proxy. Once we have configured this new SSID, the radius-proxy info gets pushed to VPNC cluster as seen below.

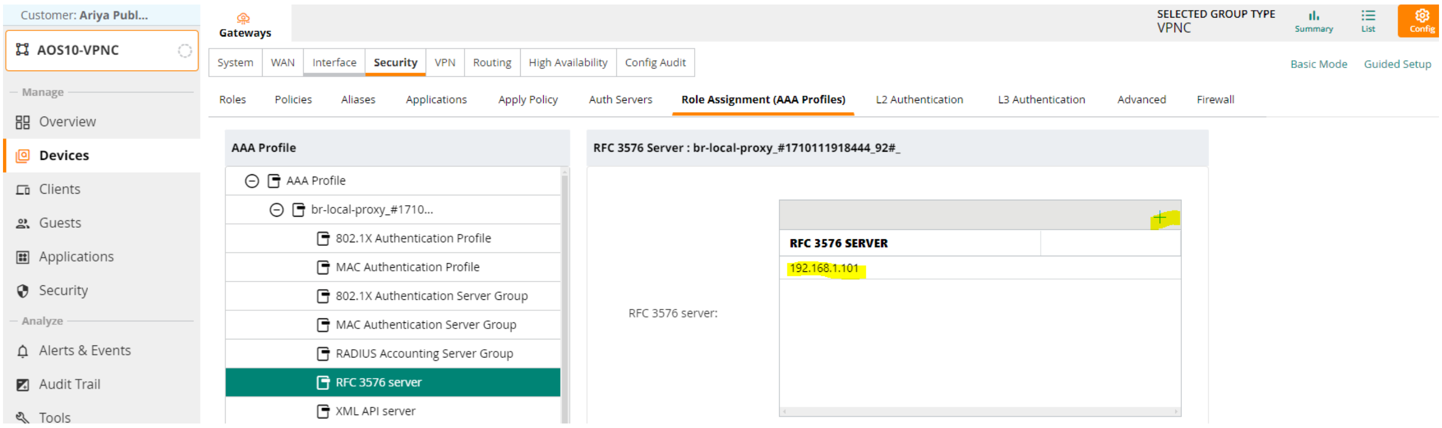


Authentication Servers

Server groups

NAME	SERVERS	FAIL THROUGH	LOAD BALANCE	SERVER RULES
br-local-proxy_#1710111918444_92#__acct_svg	1	--	--	0
br-local-proxy_#1710111918444_92#__auth_svg	1	--	--	0
br-local-proxy_#1710111918444_92#__cp_svg	1	--	--	0
CL2_#1640733088085_92#__acct_svg	1	--	--	0
CL2_#1640733088085_92#__auth_svg	1	--	--	0
CL2_#1640733088085_92#__cp_svg	1	--	--	0

Also check the Role assignment (AAA Profile) and add the CoA server manually like we did in CL2 section.

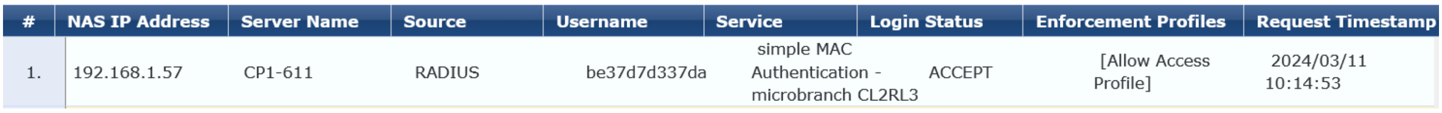


RFC 3576 Server : br-local-proxy_#1710111918444_92#_

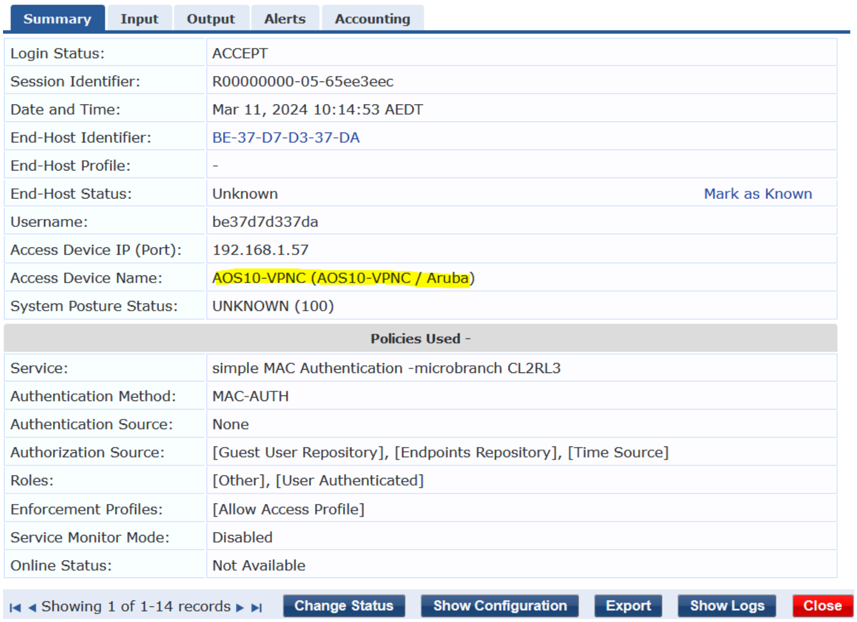
RFC 3576 server:

RFC 3576 SERVER	
192.168.1.101	

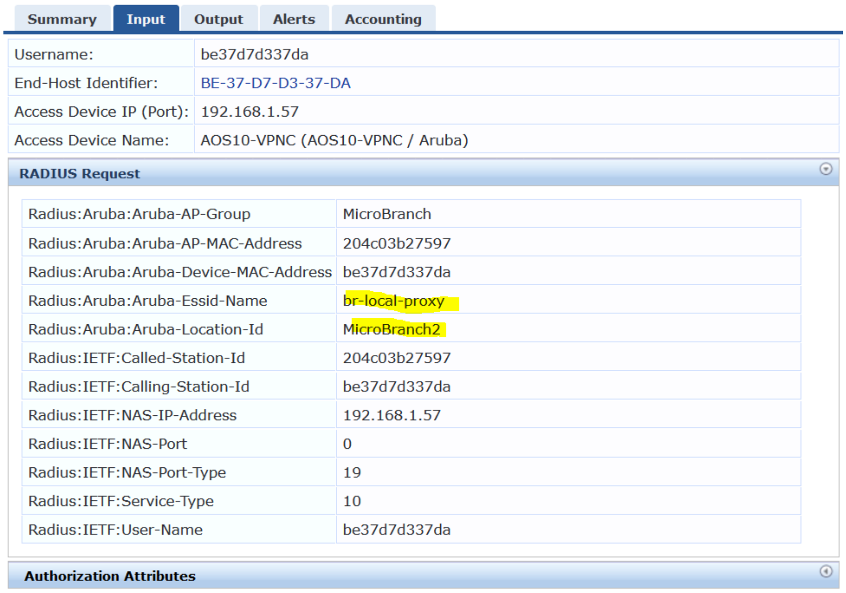
Now we are all set, I’ll connect a laptop to br-local-proxy ssid and check the access tracker on ClearPass.



#	NAS IP Address	Server Name	Source	Username	Service	Login Status	Enforcement Profiles	Request Timestamp
1.	192.168.1.57	CP1-611	RADIUS	be37d7d337da	simple MAC Authentication - microbranch CL2RL3	ACCEPT	[Allow Access Profile]	2024/03/11 10:14:53



Login Status:	ACCEPT
Session Identifier:	R00000000-05-65ee3eec
Date and Time:	Mar 11, 2024 10:14:53 AEDT
End-Host Identifier:	BE-37-D7-D3-37-DA
End-Host Profile:	-
End-Host Status:	Unknown Mark as Known
Username:	be37d7d337da
Access Device IP (Port):	192.168.1.57
Access Device Name:	AOS10-VPNC (AOS10-VPNC / Aruba)
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	simple MAC Authentication -microbranch CL2RL3
Authentication Method:	MAC-AUTH
Authentication Source:	None
Authorization Source:	[Guest User Repository], [Endpoints Repository], [Time Source]
Roles:	[Other], [User Authenticated]
Enforcement Profiles:	[Allow Access Profile]
Service Monitor Mode:	Disabled
Online Status:	Not Available



Username:	be37d7d337da
End-Host Identifier:	BE-37-D7-D3-37-DA
Access Device IP (Port):	192.168.1.57
Access Device Name:	AOS10-VPNC (AOS10-VPNC / Aruba)

RADIUS Request

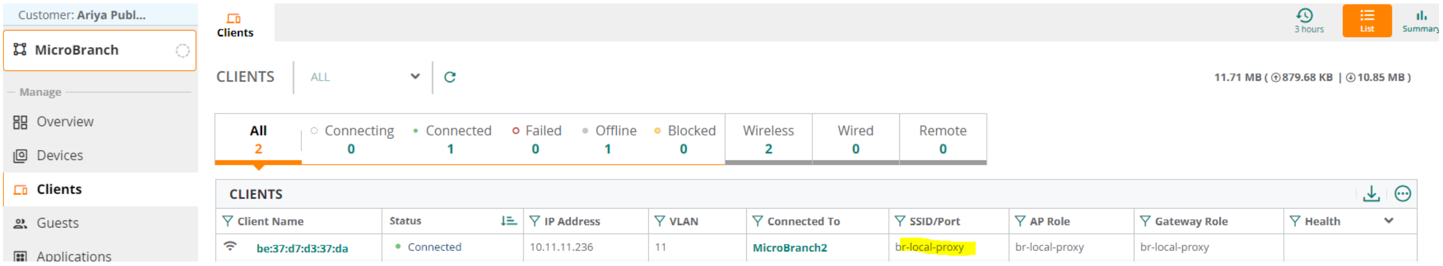
Radius:Aruba:Aruba-AP-Group	MicroBranch
Radius:Aruba:Aruba-AP-MAC-Address	204c03b27597
Radius:Aruba:Aruba-Device-MAC-Address	be37d7d337da
Radius:Aruba:Aruba-Essid-Name	br-local-proxy
Radius:Aruba:Aruba-Location-Id	MicroBranch2
Radius:IETF:Called-Station-Id	204c03b27597
Radius:IETF:Calling-Station-Id	be37d7d337da
Radius:IETF:NAS-IP-Address	192.168.1.57
Radius:IETF:NAS-Port	0
Radius:IETF:NAS-Port-Type	19
Radius:IETF:Service-Type	10
Radius:IETF:User-Name	be37d7d337da

Authorization Attributes

```
MicroBranch2# sh clients

Client List
-----------
Name          IP Address    MAC Address        OS      ESSID           Access Point
Channel  Type  Role            IPv6 Address               Signal(dB)   Speed (Mbps)
----          ----------    -----------        --      -----           ------------  ----
---  ----  ----              ------------               ----------  ------------
be37d7d337da  10.11.11.236  be:37:d7:d3:37:da  Win 10  br-local-proxy  MicroBranch2  1
GN     br-local-proxy  fe80::cf8a:a5cf:1095:5bbf  53(good)     144(good)
Number of Clients    :1
Info timestamp       :3240

MicroBranch2#
```



11.71 MB (⊕879.68 KB | ⊕10.85 MB)

All	Connecting	Connected	Failed	Offline	Blocked	Wireless	Wired	Remote
2	0	1	0	1	0	2	0	0

CLIENTS

Client Name	Status	IP Address	VLAN	Connected To	SSID/Port	AP Role	Gateway Role	Health
be:37:d7:d3:37:da	Connected	10.11.11.236	11	MicroBranch2	br-local-proxy	br-local-proxy	br-local-proxy	