

# 1 Table of Contents

---

## Table of Contents

1	Table of Contents .....	1
1.1	Revision History .....	1
2	Multiple PSK Aruba Instant .....	2
2.1	Things you need .....	2
2.2	Overall Workflow.....	2
3	AOS10 MPSK Local.....	3
3.1	WLAN Configuration .....	3
3.2	MPSK Local Testing .....	7
4	AOS10 MPSK Configuration .....	9
4.1	Authentication Server Configuration .....	9
4.2	MPSK Configuration.....	9
5	ClearPass Configuration.....	13
5.1	RADIUS Dictionary .....	13
5.2	Service Template .....	13
5.3	Enforcement Profiles.....	15
5.4	Enforcement Policy .....	16
5.5	Role Mapping.....	16
5.6	ClearPass Service.....	16
5.7	Operator Service.....	18
5.8	Messaging Server.....	19
6	ClearPass Guest .....	20
6.1	MPSK Configuration.....	20
6.2	Operator Profile .....	21
6.3	Form Fields .....	22
7	Testing .....	25
7.1	Device Registration .....	25
7.2	ClearPass Access Tracker Operator Login .....	27
7.3	ClearPass Access Tracker MPSK Authentication .....	29
7.4	Aruba Central Clients Monitoring .....	30
8	Pre-populating MAC address Workflow.....	34
8.1	Aruba Central Configuration .....	34
8.2	ClearPass Guest.....	36
8.3	Testing the new workflow.....	37

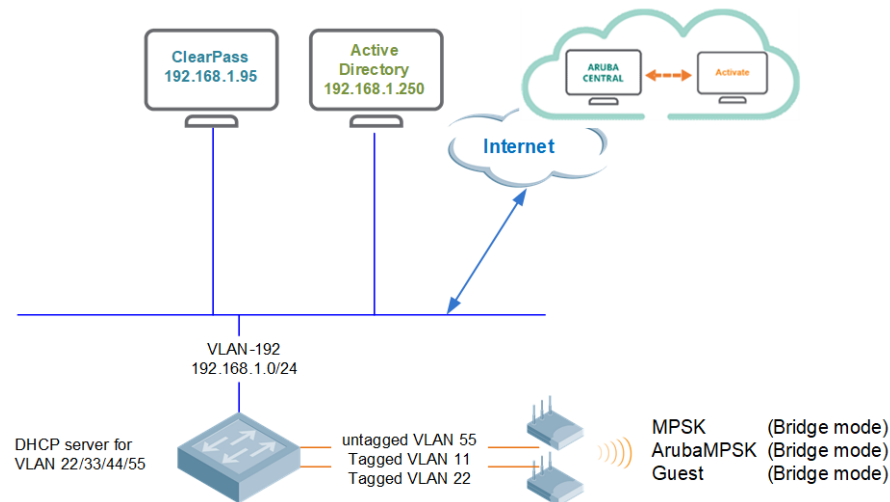
## 1.1 Revision History

DATE	VERSION	EDITOR	CHANGES
24 Jul 2021	0.1	Ariya Parsamanesh	Initial creation
04 Sep 2021	0.2	Ariya Parsamanesh	Added the ClearPass workflow

## 2 Multiple PSK Aruba Instant

Aruba AOS10 supports multiple PSKs (MPSK) for the same SSID. This means that each client connected to the PSK based SSID will have its own unique PSK that is not shared with the rest of the clients. You can use this feature with ClearPass which will be more scalable. You can also use it in local mode without having ClearPass which is called MPSK-Local.

It should be noted that MPSK solution was designed for the headless devices like IoTs, printers, TVs, etc. and not designed for laptops, tablets and mobile devices that support secure authentication using dot1x supplicants.



### 2.1 Things you need

- Two AOS10 APs running 10.2.0.2 or later
- Aruba ClearPass version 6.8.x or later (here we are using 6.9.5)
- A Layer three switch and some WiFi clients

### 2.2 Overall Workflow

The overall workflow with MPSK Local is as follows

- Configure MPSK Local profile for the group of APs with the passphrase value and user role. You can use the user role and then assign VLANs, BW contracts, etc.
- Use WLAN SSID configuration wizard, to create the SSID profile with MPSK Local as the opmode.
- The IoT1 with their own <password1> will connect and will be put in VLAN X
- The IoT2 with their own <password2> will connect to the same SSID and will be put in VLAN Y

The overall workflow with MPSK with ClearPass solution is as follows

- Before connecting a device to a MPSK based SSID, the user registers the device on a ClearPass Policy Manager guest-registration or device-registration webpage
- The user receives a device-specific or group-specific MPSK passphrase through the email
- The user then connects their device with their unique PSK to the MPSK based SSID
- The Instant AP performs MAC authentication of the client device against the ClearPass Policy Manager server
- On successful MAC authentication, the ClearPass Policy Manager returns Access-Accept with the VSA containing the encrypted passphrase
- The Instant AP generates a PSK from the passphrase and performs 4-way key exchange.

## 3 AOS10 MPSK Local

When multiple PSK is enabled on the WLAN SSID profile, make sure that MAC authentication is not configured for RADIUS authentication. Multiple PSK and MAC authentication are mutually exclusive and follows a special procedure which does not require enabling MAC authentication in the WLAN SSID manually.

The MPSK Local operating mode allows to configure 24 pre-shared keys per SSID without external RADIUS server like ClearPass. These local PSKs serve as an extension of the base pre-shared key functionality. MPSK Local operating mode is supported on the SSID profile. MPSK Local works only with wpa2-psk-aes encryption and not with any other PSK-based encryption.

### 3.1 WLAN Configuration

Before we start with the WLA configuration we need to configure the passphrases for MPSK local profiles. For that we need to go to the security tab in the AP configuration.

The screenshot displays the AOS10 configuration interface. The left sidebar shows the navigation menu with 'Security' selected. The main panel shows the 'Security' tab for 'Access Points'. Under 'Authentication Servers', 'MPSK Local' is expanded. A table titled 'MPSK Local Passphrase' is shown with columns 'Name' and 'Role'. The table is currently empty, and a warning message states: '\* MPSK local passphrase table should not be empty'. The 'Name' field is highlighted in yellow. The 'IoT-Group' field is also visible. The 'test' value is entered in the 'Name' field. The 'Role' field is empty. The 'Cancel' and 'OK' buttons are at the bottom.

Name	Role
test	

Access Points

Switches

Gateways

WLANs

Access Points

SECURITY

> Authentication

> MPSPK Local

MPSPK Local

Name

IoT-Group

test

MPSPK LOCAL PASSPHRASE

Name :

iot1

Passphrase :

.....

Retype Passphrase :

.....

Role :

IoT1

Cancel

OK

Access Points

Switches

Gateways

WLANs

Access Points

SECURITY

> Authentication

> MPSPK Local

MPSPK Local

Name

IoT-Group

test

MPSPK LOCAL

Name :

IoT-Group

MPSPK Local Passphrase

Name

Role

iot1

IoT1

Cancel

OK

Access Points

Switches

Gateways

WLANs

Access Points

SECURITY

> Authentication

> MPSPK Local

MPSPK Local

Name

IoT-Group

test

MPSPK LOCAL PASSPHRASE

Name :

iot2

Passphrase :

.....

Retype Passphrase :

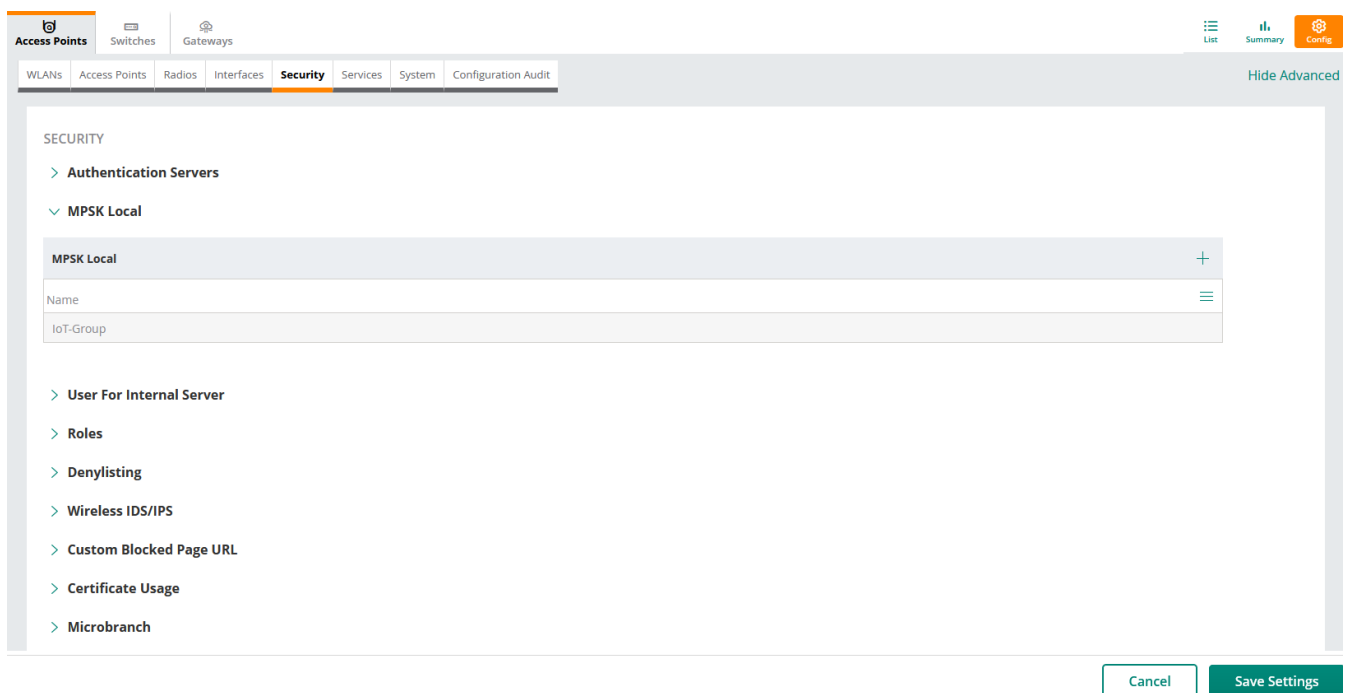
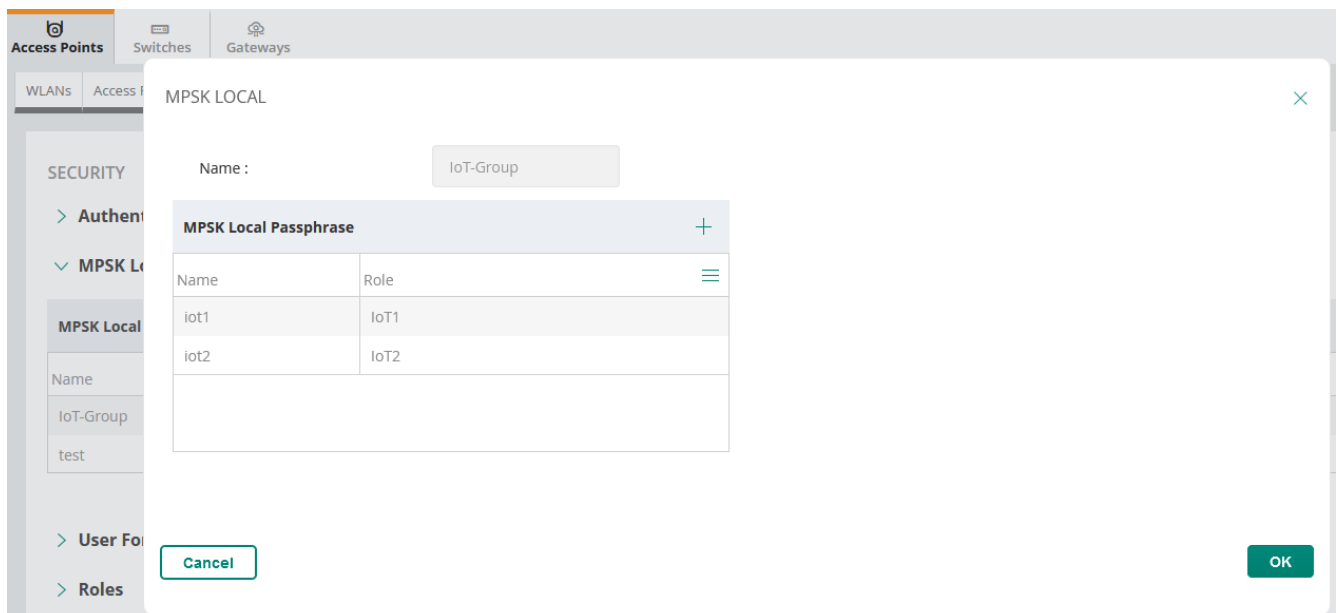
.....

Role :

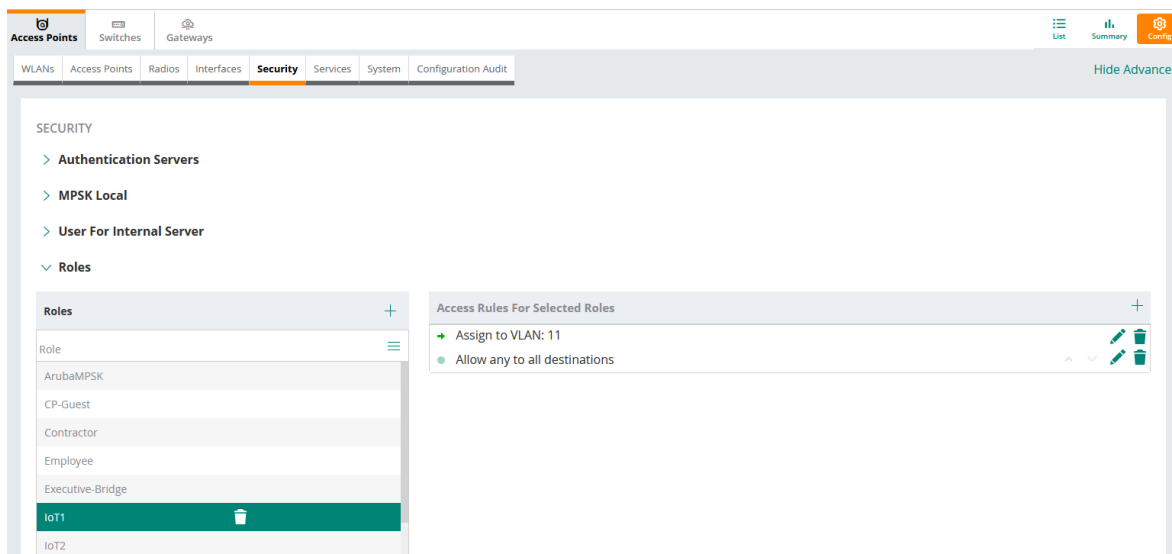
IoT2

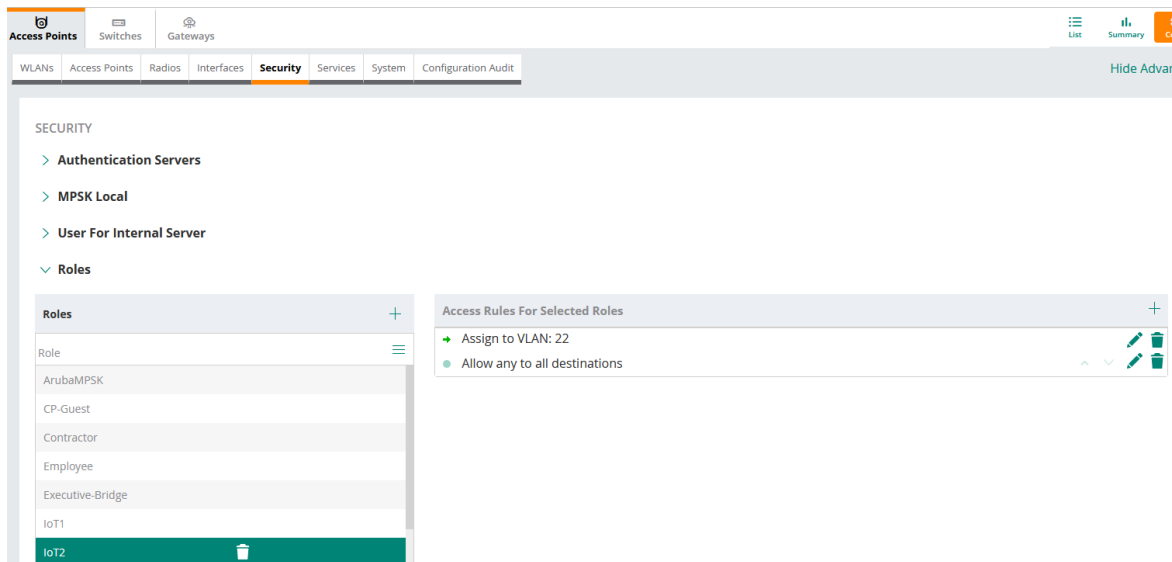
Cancel

OK

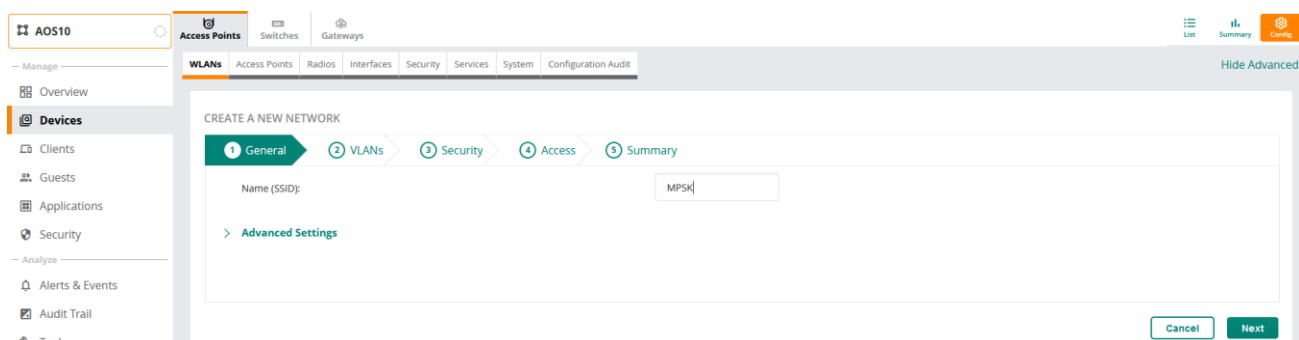


Finally, we'll put the above user roles in diff VLANs.

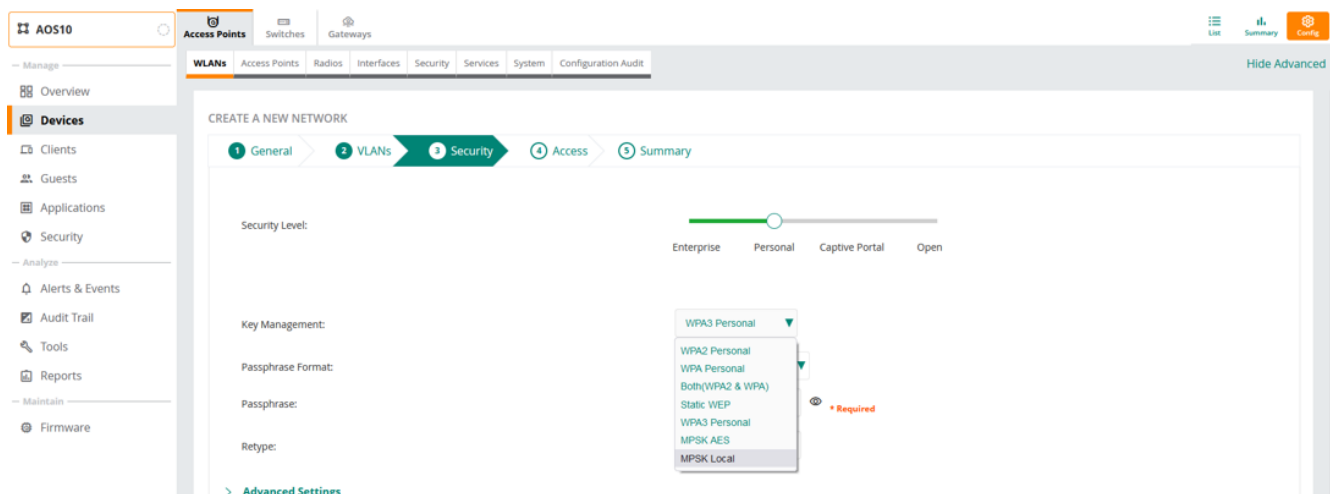
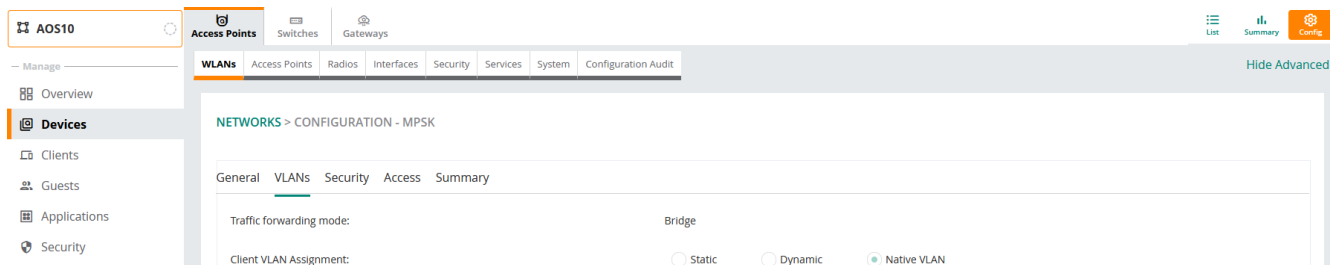


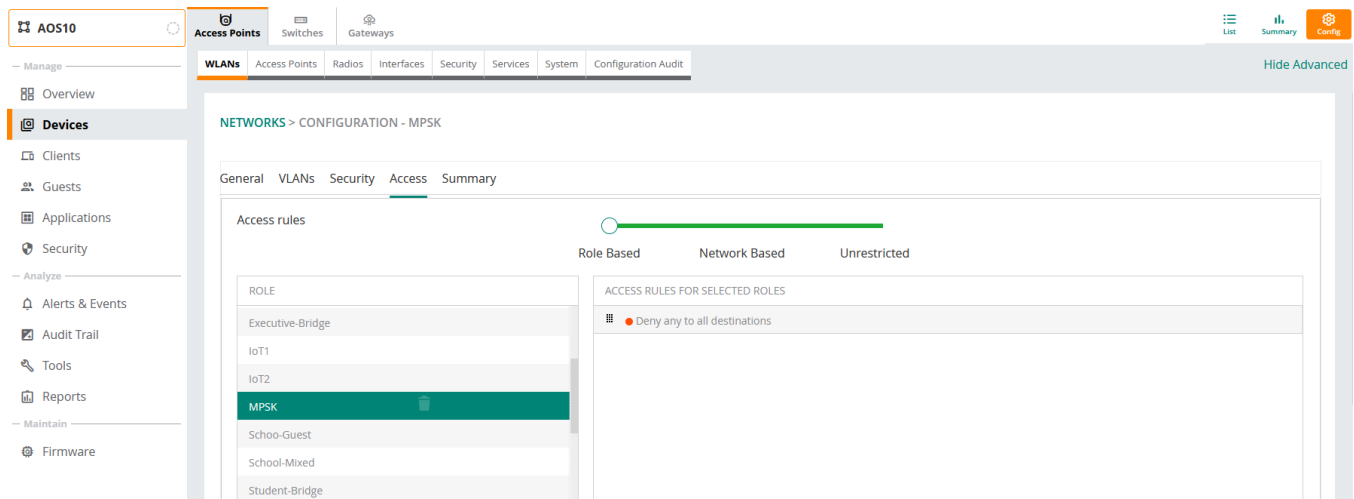
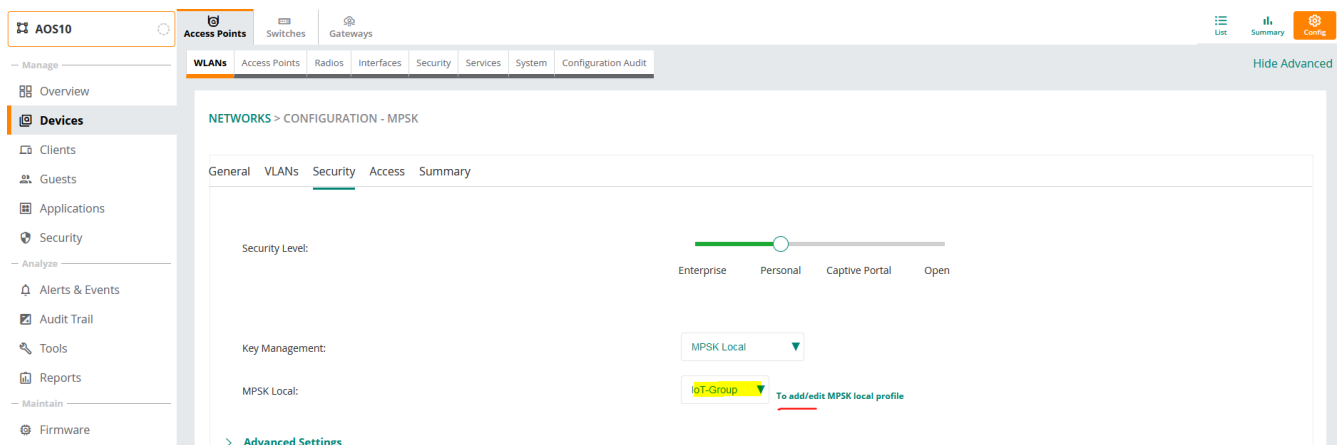


Now we can configure MPSK based WLAN



Note that you can configure MPSK local with tunnel mode as well here we are using bridge mode.



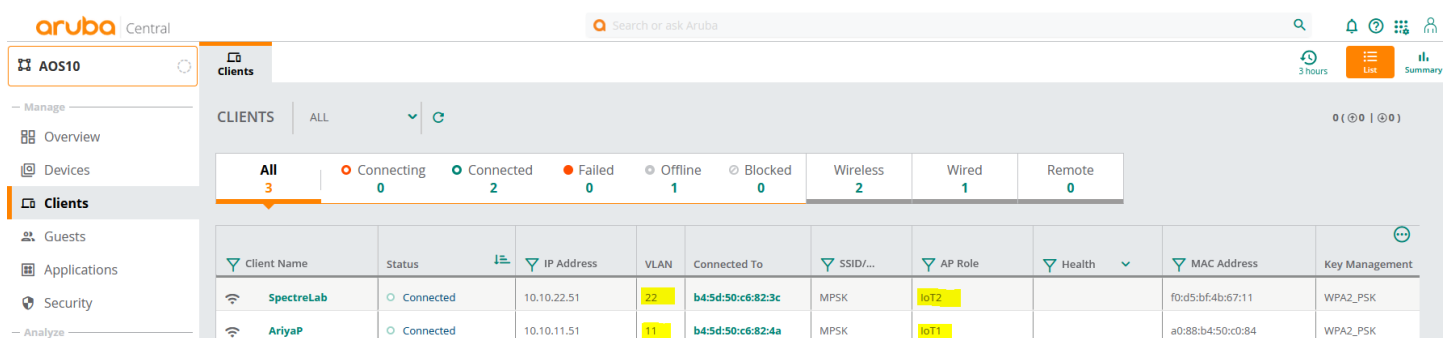


Note that we are denying access here, so the logic is that if the devices are in IoT1 or IoT2 user role, then they'll be in VLAN 11 and 22 respectively, any other device will be denied.

## 3.2 MPSK Local Testing

So now we'll test our MPSK Local with the two devices that we have.

- lot1 user role with <password1> will be in VLAN 11
- lot2 user role with <password2> will be in VLAN 22



← AriyaP

Summary

AI Insights

Location

Sessions

Manage

Overview

Applications

Analyze

Live Events

Events

Tools

CLIENT DETAILS

DATA PATH

CLIENT

AriyaP

CONNECTED

SSID

MPSK

UP

AP

b4:5d:50:c6:82:4a

UP

SWITCH

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

UP

CLIENT

USERNAME

...

HOSTNAME

AriyaP

IP ADDRESS

10.10.11.51

GLOBAL UNICAST IPV6 ADDRESS

...

CLIENT OS

Win10

MANUFACTURER

Intel Corporate

AI INSIGHTS

0 0 0 0

CLIENT TYPE

Wireless

MAC ADDRESS

a0:88:b4:50:c0:84

LINK LOCAL IPV6 ADDRESS

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

CONNECTED SINCE

Jul 19, 2021, 12:14:29

LAST SEEN

...

ENCRIPTION

AES

NETWORK

VLAN

11

AP ROLE

IoT1

GATEWAY ROLE

...

SEGMENTATION

...

AUTH SERVER

...

TUNNELED

...

VLAN DERIVATION

User Role

AP DERIVATION

...

SWITCH ROLE

...

DHCP SERVER

10.10.11.1

TUNNELED ID

...

CONNECTION

CHANNEL

11 (20 MHz)

BAND

2.4 GHz

CLIENT CAPABILITIES

802.11gn

CLIENT MAX SPEED

288 Mbps

LEDs on ACCESS POINT (b4:5d:50:c6:82:4a)

0 0 0 Blink LEDs

← AriyaP

Events

Manage

Overview

Applications

Analyze

Live Events

Events

Tools

EVENTS

2

CLICK HERE FOR ADVANCED FILTERING

EVENTS (2)

Download

Refresh

← SpectreLab

Summary

AI Insights

Location

Sessions

Manage

Overview

Applications

Analyze

Live Events

Events

Tools

CLIENT DETAILS

DATA PATH

CLIENT

SpectreLab

CONNECTED

SSID

MPSK

UP

AP

b4:5d:50:c6:82:3c

UP

SWITCH

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

UP

CLIENT

USERNAME

...

HOSTNAME

SpectreLab

IP ADDRESS

10.10.22.51

GLOBAL UNICAST IPV6 ADDRESS

...

CLIENT OS

Win10

MANUFACTURER

Intel Corporate

AI INSIGHTS

0 0 0 0

CLIENT TYPE

Wireless

MAC ADDRESS

f0:d5:bf:4b:67:11

LINK LOCAL IPV6 ADDRESS

fe80:ce86b:ceb9:86c6...

CONNECTED SINCE

Jul 19, 2021, 12:16:43

ENCRIPTION

AES

NETWORK

VLAN

22

AP ROLE

IoT2

GATEWAY ROLE

...

SEGMENTATION

...

AUTH SERVER

...

TUNNELED

...

VLAN DERIVATION

User Role

AP DERIVATION

...

SWITCH ROLE

...

DHCP SERVER

10.10.22.1

TUNNELED ID

...

CONNECTION

CHANNEL

6 (20 MHz)

BAND

2.4 GHz

CLIENT CAPABILITIES

802.11gn, 802.11v

CLIENT MAX SPEED

288 Mbps

LEDs on ACCESS POINT (b4:5d:50:c6:82:3c)

0 0 0 Blink LEDs



## 4 AOS10 MPSK Configuration

Now we'll configure the SSID to be MPSK instead of MPSK-Local.

### 4.1 Authentication Server Configuration

First, we need to configure ClearPass as the authentication server.

The screenshot shows the AOS10 configuration interface. The left sidebar has 'AOS10' selected. The main panel is under 'Access Points' > 'Security'. The 'NEW SERVER' dialog is open, showing the following fields:

- Server Type: RADIUS
- Name: ClearPass
- IP Address: 192.168.1.95
- Shared Key: (masked with dots)
- Retype Key: (masked with dots)
- Timeout: 30 sec
- Auth Port: 1812
- NAS IP Address: optional
- NAS Identifier: optional
- Retry Count: 3
- Service Type Framed User: ☐ MAC/Captive Portal
- Dynamic Authorization: ☐
- Query Status of RADIUS Servers(RFC 5997): ☐
- Authentication: ☐
- Accounting: ☐
- Accounting Port: 1813

Buttons: Cancel, Save

The screenshot shows the AOS10 configuration interface. The left sidebar has 'AOS10' selected. The main panel is under 'Access Points' > 'Security'. The 'Authentication Servers' table is visible, showing the following entry:

Name	Type
ClearPass	RADIUS

### 4.2 MPSK Configuration

Here we'll start with the MPSK configuration by adding a new WLAN.

The screenshot shows the AOS10 configuration interface. The left sidebar has 'AOS10' selected. The main panel is under 'WLANs'. The 'CREATE A NEW NETWORK' wizard is open, showing the following steps:

- General
- VLANs
- Security
- Access
- Summary

The 'General' step is active, showing the following fields:

- NAME (SSID): ArubaMPSK
- > Advanced Settings

Buttons: Cancel, Next

Again, like the previous configuration, this can be bridged or tunneled, here we'll use bridge mode.

Access Points

Switches

Gateways

WLANs

Access Points

Radios

Interfaces

Security

Services

System

Configuration Audit

ListSummaryConfig

Hide Advanced

CREATE A NEW NETWORK

1 General

2 VLANs

3 Security

4 Access

5 Summary

Traffic forwarding mode:

☒ Bridge

☐ Tunnel

☐ Mixed

Client VLAN Assignment:

☒ Static

☐ Dynamic

☐ Native VLAN

VLAN ID:

22

> Show Named VLANs

Cancel

Back

Next

Access Points

Switches

Gateways

WLANs

Access Points

Radios

Interfaces

Security

Services

System

Configuration Audit

ListSummaryConfig

Hide Advanced

CREATE A NEW NETWORK

1 General

2 VLANs

3 Security

4 Access

5 Summary

Security Level:

Enterprise

Personal

Captive Portal

Open

Key Management:

MPSK AES

Primary Server:

ClearPass

+

Secondary Server:

-- Select --

+

Advanced Settings

Enforce DHCP:

Use IP for Calling Station ID:

Called Station ID Type:

MAC Address

Called Station ID Include SSID:

Accounting

Accounting:

Use authentication servers

Accounting Interval:

1

min

Fast Roaming

Cancel

Back

Next

**AOS10** Access Points Switches Gateways List Summary Config

WLANs Access Points Radios Interfaces Security Services System Configuration Audit Hide Advanced

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
ArubaMPSK	Deny any to all destinations
CP-Guest	
Contractor	
Employee	
Executive-Bridge	
IoT1	
IoT2	

+ Add Role 15 Role(s) + Add Rule 1 Rule(s)

**AOS10** Access Points Switches Gateways List Summary Config

WLANs Access Points Radios Interfaces Security Services System Configuration Audit Hide Advanced

CREATE A NEW NETWORK

1 General 2 VLANs 3 Security 4 Access 5 Summary

Network Summary

General		Security	
ESSID	ArubaMPSK	Security Level	Personal
Multicast Optimization	Disabled	Auth Server 1	ClearPass
Band	all	Key Management	MPSK AES
DTIM Interval	1 beacons	MAC Authentication	Disabled
Primary Usage	employee	<b>VLANs</b>	
Inactivity Timeout	1000 secs	Traffic forwarding mode	Bridge
Dynamic Multicast OPT	Disabled	Client VLAN Assignment	Static
Content Filtering	Disabled	VLAN	22
Airtime	unlimited	<b>Access</b>	
Hide SSID	Disabled	Role Assignments For Authenticated Users	Disabled
Broadcast filtering	arp	ENFORCE MAC AUTH ONLY ROLE	Disabled
Transmit Rates (legacy Only)	2.4 GHz Min: 1Mbps Max: 54Mbps	ASSIGN PRE-AUTHENTICATION ROLE	Disabled

After the successful MPSK authentication, the MPSK passphrase is cached with in the APs. We also need to configure the right Security user role.

**AOS10** Access Points Switches Gateways List Summary Config

WLANs Access Points Radios Interfaces Security Services System Configuration Audit Hide Advanced

SECURITY

- > Authentication Servers
- > MPSK Local
- > User For Internal Server
- > Roles

Roles	Access Rules For Selected Roles
Role	Deny any to all destinations
ArubaMPSK	
CP-Guest	
Contractor	
Employee	

Access Points

Switches

Gateways

WLANs

Access Points

ADD ROLE

Roles: Student-Devs

Cancel

OK

SECURITY

> Authentication Servers

> MPSK Local

> User For Internal Server

> Roles

Roles

AOS10

Access Points

Switches

Gateways

WLANs

Access Points

Radios

Interfaces

Security

Services

System

Configuration Audit

Hide Advanced

Manage

Overview

Devices

Clients

Guests

Applications

Security

Analyze

Alerts & Events

Audit Trail

Tools

Reports

Maintain

Firmware

SECURITY

> Authentication Servers

> MPSK Local

> User For Internal Server

> Roles

Roles

Role

Student-Devs

ArubaMPSK

CP-Guest

Contractor

Employee

Executive-Bridge

IoT1

IoT2

MDCV

Access Rules For Selected Roles

Allow any to all destinations

Cancel

Save Settings

## 5 ClearPass Configuration

In this section we'll go through the ClearPass configuration needed for the MPSK solution. Remember you need ClearPass 6.8.x or later. MPSK passphrase requires MAC authentication against a ClearPass Policy Manager server and the only encryption type that is support with MPSK is wpa2-psk-aes.

### 5.1 RADIUS Dictionary

ClearPass 6.8 brought a new Aruba RADIUS VSA called Aruba-MPSK-Passphrase. This VSA is used with the unique PSK for the client.

The screenshot shows the ClearPass Policy Manager interface. On the left is a navigation menu with 'Administration' selected. The main area displays a table of RADIUS attributes. A modal window titled 'RADIUS Attributes' is open, showing a list of attributes for 'Aruba (14823)'. The attributes include Vendor Name, Aruba-CPM-Rule, Aruba-Calea-Server-IP, Aruba-Captive-Portal-URL, Aruba-Command-String, Aruba-Device-Type, Aruba-Essid-Name, Aruba-Framed-IPv6-Address, Aruba-Gateway-Zone, Aruba-Location-Id, Aruba-MPSK-Passphrase (highlighted), and Aruba-Mdps-Device-Iccid. At the bottom of the modal are 'Disable', 'Export', and 'Close' buttons.

#	Vendor Name	Vendor ID	Vendor Prefix	Enabled
1.	3com	43	3com	false
2.	GPP		GPP	false
3.	cc		cc	false
4.	cme		cme	false
5.	DSL-Forum		DSL-Forum	false
6.	dva		dva	false
7.	erohive		erohive	false
8.	irespace		irespace	false
9.	lcatel		lcatel	false
10.	lcatel-Lucent-Enterprise		lcatel-Lucent-Enterprise	true
11.	lcatel-Lucent-Service-Router		lcatel-Lucent-Service-Router	false
12.	lteon		lteon	false
13.	lvarion		lvarion	false
14.	PC		PC	false
15.	aruba		aruba	true
16.	scend		scend	false
17.	Avenda	25427	Avenda	true

### 5.2 Service Template

We will start with the Service template to build it out.

The screenshot shows the 'Service Templates & Wizards' page in the ClearPass Policy Manager. The left navigation menu has 'Configuration' selected. The main area shows a list of service templates. The 'Aruba Wireless with MPSK' template is highlighted.

Configuration » Service Templates & Wizards

Service Templates & Wizards

- To configure service and related policies using the **full wizard**, click [here](#).
- Or filter by **service templates** for common use cases:

**802.1X Wired**  
To authenticate users to any wired network via 802.1X.

**802.1X Wireless**  
To authenticate users to any wireless network via 802.1X.

**Aruba 802.1X Wireless**  
To authenticate users to an Aruba wireless network via 802.1X.

**Aruba Auto Sign-On**  
Service template for accessing SAML based single sign-on enabled applications using network authenticated identity through Aruba controllers.

**Aruba VPN access with Posture checks**  
For Aruba VPN clients connecting remotely to the corporate network, with differentiated access based on the results of Posture checks.

**Aruba Wireless with MPSK**  
To authenticate devices using an Aruba MPSK.

Using the Aruba Wireless with MPSK wizard.

## Service Templates - Aruba Wireless with MPK

General	Wireless Network Settings	Device Roles	Enforcement Details
Name Prefix*: <input type="text" value="MPK"/>			
<p align="center"><b>Description</b></p> <p>For wireless devices that do not support strong 802.1X authentication, Aruba MPK allows each device to be assigned a unique pre-shared key during Device Registration. This service type handles the device authentication from an Aruba Mobility Controller or Instant AP.</p>			

[Back to Service Templates & Wizards](#)

Delete

Next →

Add Service

Cancel

General	Wireless Network Settings	Device Roles	Enforcement Details
Select NAD Client: <input type="text" value="AOS10-APs"/>			
SSID Name: <input type="text" value="ArubaMPK"/> (Enter single or multiple comma separated SSIDs)			

[Back to Service Templates & Wizards](#)

Delete

Next →

Add Service

Cancel

General	Wireless Network Settings	Device Roles	Enforcement Details
---------	---------------------------	--------------	---------------------

**Define logical device roles (think tags) that allow for dynamic policy construction. Select an existing role from the dropdown or type a name to create one.**

Device Role 1*:	<input type="text" value="Student-Devs"/>
Device Role 2:	<input type="text"/>
Device Role 3:	<input type="text"/>
Device Role 4:	<input type="text"/>
Device Role 5:	<input type="text"/>
Device Role 6:	<input type="text"/>
Device Role 7:	<input type="text"/>
Device Role 8:	<input type="text"/>
Device Role 9:	<input type="text"/>
Device Role 10:	<input type="text"/>

[Back to Service Templates & Wizards](#)

Delete

Next →

Add Service

Cancel

General	Wireless Network Settings	Device Roles	Enforcement Details
---------	---------------------------	--------------	---------------------

## Create a New Enforcement Policy

Device Role	Aruba Role
If <input type="text" value="Student-Devs"/>	then assign Role <input type="text" value="Student-Devs"/>
If <input type="text"/>	then assign Role <input type="text"/>
If <input type="text"/>	then assign Role <input type="text"/>
If <input type="text"/>	then assign Role <input type="text"/>
If <input type="text"/>	then assign Role <input type="text"/>
If <input type="text"/>	then assign Role <input type="text"/>
If <input type="text"/>	then assign Role <input type="text"/>
If <input type="text"/>	then assign Role <input type="text"/>
If <input type="text"/>	then assign Role <input type="text"/>
If <input type="text"/>	then assign Role <input type="text"/>

Default MPK\*:

Default Aruba User Role\*:

[Back to Service Templates & Wizards](#)

Delete

Next →

Add Service

Cancel

The default MPK that we have configured is aruba123. You don't have to use this default MPK and just put some random value in that case. There are not that many use cases where you want to give out a default value. But if you want to use it, the aim is to provide a default MPK for the devices that fall through the logic to get contained using captive portal and restricted ACL.

ClearPass Policy Manager

Menu

- Dashboard
- Monitoring
- Configuration
  - Service Templates & Wizards
  - Services
  - Authentication
  - Identity
  - Posture

Configuration » Services  
Services

- Added 2 Enforcement Profile(s)
- Added 1 Enforcement Policies
- Added 1 Roles
- Added 1 Role Mapping Policies
- Added 1 service(s)

- Add
- Import
- Export All

## 5.3 Enforcement Profiles

Here are the two enforcement profiles that were created.

aruba ClearPass Policy Manager

Configuration » Enforcement » Profiles

Enforcement Profiles

Each enforcement policy contains enforcement profiles that match conditions (role, posture, and time) to actions (enforcement profiles).

Filter: Name contains mpsk Go Clear Filter

Show 20 records

#	Name	Type	Description
1.	MPSK Aruba Wireless with MPSK Default Profile	RADIUS	
2.	[Registered Device MPSK]	RADIUS	Returns a device's assigned MPSK that was generated automatically during Device Registration

Showing 1-2 of 2

Copy Export Delete

### Enforcement Profile - MPSK Aruba Wireless with MPSK Default Profile

Summary Profile Attributes

**Profile:**

Name:	MPSK Aruba Wireless with MPSK Default Profile
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

**Attributes:**

Type	Name	Value
1. Radius:Aruba	Aruba-User-Role	= Employee
2. Radius:Aruba	Aruba-MPSK-Passphrase	= aruba123

It also created this enforcement profile.

### Enforcement Profile - Aruba User Role – Student-Devs

Note: This Enforcement Profile is created by Service Template

Summary Profile Attributes

**Profile:**

Name:	Aruba User Role - Student-Devs
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

**Attributes:**

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

### Enforcement Profiles - [Registered Device MPSK]

This is a default profile.

Summary Profile Attributes

**Profile:**

Name:	[Registered Device MPSK]
Description:	Returns a device's assigned MPSK that was generated automatically during Device Registration
Type:	RADIUS
Action:	Accept
Device Group List:	-

**Attributes:**

Type	Name	Value
1. Radius:Aruba	Aruba-MPSK-Passphrase	= Device's Assigned MPSK

## 5.4 Enforcement Policy

This is the enforcement policy that got created.

### Enforcement Policies - MPSK Aruba Wireless with MPSK Enforcement Policy

Summary	Enforcement	Rules
Enforcement:		
Name:	MPSK Aruba Wireless with MPSK Enforcement Policy	
Description:		
Enforcement Type:	RADIUS	
Default Profile:	MPSK Aruba Wireless with MPSK Default Profile	
Rules:		
Rules Evaluation Algorithm:	First applicable	
Conditions		Actions
1.	(Tips:Role EQUALS Student-Devs) AND (Authorization:[Guest Device Repository]:Device Account Active EQUALS true) AND (Authorization:[Guest Device Repository]:Device MPSK EXISTS )	Aruba User Role - Student-Devs, [Registered Device MPSK], [Return Device Sponsor Name - RADIUS User-Name]

## 5.5 Role Mapping

And lastly this is the role mapping that got created. Generally, with previous ClearPass version you had to manually create the various roles that you wanted to make use of in ClearPass guest, but now with version 6.8 this service template does it automatically.

### Role Mappings - MPSK Aruba Wireless with MPSK Role Map

aruba

Dashboard

Monitoring

Configuration

Service Templates & Wizards

Services

Authentication

Identity

- Single Sign-On (SSO)
- Local Users
- Endpoints
- Static Host Lists
- Roles
- Role Mappings

Posture

ClearPass Policy Manager

Menu

Configuration » Identity » Role Mappings » Edit - MPSK Aruba Wireless with MPSK Role Map

Role Mappings - MPSK Aruba Wireless with MPSK Role Map

Note: This Role Mapping policy is created by Service Template

Summary

Policy

Mapping Rules

Policy:

Policy Name:

MPSK Aruba Wireless with MPSK Role Map

Description:

Default Role:

[Other]

Mapping Rules:

Rules Evaluation Algorithm:

Evaluate all

Conditions

Role Name

1. (Authorization:[Guest Device Repository]:Device Role ID EQUALS 3009)

Student-Devs

## 5.6 ClearPass Service


And here is the complete serviced that was configured.



## Services

 Add  
 Import  
 Export All

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

Filter:  contains     Show  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	Modified Aruba Device Access Service	TACACS	TACACS+ Enforcement	
5.	<input type="checkbox"/>	5	[Guest Operator Logins]	Application	Aruba Application Authentication	
6.	<input type="checkbox"/>	6	[Insight Operator Logins]	Application	Aruba Application Authentication	
7.	<input type="checkbox"/>	7	Ariya Guest Operator Logins	Application	Aruba Application Authentication	
8.	<input type="checkbox"/>	8	MM-admin-service	RADIUS	RADIUS Enforcement ( Generic )	
9.	<input type="checkbox"/>	9	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	
10.	<input type="checkbox"/>	10	AA Aruba 802.1X Wireless	RADIUS	Aruba 802.1X Wireless	
11.	<input type="checkbox"/>	11	GG MAC Authentication	RADIUS	MAC Authentication	
12.	<input type="checkbox"/>	12	GG User Authentication with MAC Caching	RADIUS	RADIUS Enforcement ( Generic )	
13.	<input type="checkbox"/>	13	MPSK Aruba Wireless with MPSK	RADIUS	MAC Authentication	

Summary	Service	Authentication	Roles	Enforcement
Name:		<input type="text" value="MPSK Aruba Wireless with MPSK"/>		
Description:		<div>To authenticate devices using an Aruba MPSK.</div>		
Type:		MAC Authentication		
Status:		Enabled		
Monitor Mode:		<input type="checkbox"/> Enable to monitor network access without enforcement		
More Options:		<input type="checkbox"/> Authorization <input type="checkbox"/> Audit End-hosts <input type="checkbox"/> Profile Endpoints <input type="checkbox"/> Accounting Proxy		
Service Rule				
Matches <input type="radio"/> ANY or <input checked="" type="radio"/> 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	EQUALS	Call-Check (10)	
3. Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}	
4. Connection	SSID	EQUALS	ArubaMPSK	
5. <a href="#">Click to add...</a>				

Summary	Service	Authentication	Roles	Enforcement
Authentication Methods:		<div><div>[Allow All MAC AUTH]</div><div><div>Move Up </div><div>Move Down </div><div>Remove</div><div>View Details</div><div>Modify</div></div><div>--Select to Add--</div></div> <div>Add New Authentication Method</div>		
Authentication Sources:		<div><div>[Guest Device Repository] [Local SQL DB]</div><div><div>Move Up </div><div>Move Down </div><div>Remove</div><div>View Details</div><div>Modify</div></div><div>--Select to Add--</div></div> <div>Add New Authentication Source</div>		
Strip Username Rules:		<input type="checkbox"/> Enable to specify a comma-separated list of rules to strip username prefixes or suffixes		

Summary	Service	Authentication	Roles	Enforcement
Role Mapping Policy:		<div><input type="text" value="MPSK Aruba Wireless with MPSK Role Map"/> <input type="button" value="Modify"/></div> <div>Add New Role Mapping Policy</div>		
Role Mapping Policy Details				
Description:				
Default Role:		[Other]		
Rules Evaluation Algorithm:		evaluate-all		
Conditions	Role			
1.	(Authorization:[Guest Device Repository]:Device Role ID EQUALS 3009)			Student-Devs

Summary	Service	Authentication	Roles	Enforcement
Use Cached Results:	<input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions			
Enforcement Policy:	MPSK Aruba Wireless with MPSK Enforcement Policy <a href="#">Modify</a>			<a href="#">Add New Enforcement Policy</a>
Enforcement Policy Details				
Description:				
Default Profile:	MPSK Aruba Wireless with MPSK Default Profile			
Rules Evaluation Algorithm:	first-applicable			
Conditions		Enforcement Profiles		
1. (Tips:Role <b>EQUALS</b> Student-Devs) <b>AND</b> (Authorization:[Guest Device Repository]:Device Account Active <b>EQUALS</b> true) <b>AND</b> (Authorization:[Guest Device Repository]:Device MPSK <b>EXISTS</b> )		Aruba User Role - Student-Devs, [Registered Device MPSK], [Return Device Sponsor Name - RADIUS User-Name]		

## 5.7 Operator Service

We also need to create an operator service so that the users can register their devices after they login to ClearPass Guest. Here we are using AD as the authentication source.

Summary	Service	Authentication	Roles	Enforcement
Name:	Ariya Guest Operator Logins			
Description:	Authentication Service for Guest Application			
Type:	Aruba Application Authentication			
Status:	Enabled			
Monitor Mode:	<input type="checkbox"/> Enable to monitor network access without enforcement			
More Options:	<input type="checkbox"/> Authorization			
Service Rule				
Matches <input type="radio"/> ANY or <input checked="" type="radio"/> ALL of the following conditions:				
Type	Name	Operator	Value	
1. Application	Name	EQUALS	Guest	<a href="#">Copy</a> <a href="#">Delete</a>
2. Authentication	Type	NOT_EQUALS	SSO	<a href="#">Copy</a> <a href="#">Delete</a>
3. <a href="#">Click to add...</a>				

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

Summary	Service	Authentication	Roles	Enforcement
Role Mapping Policy:	--Select-- <a href="#">Modify</a>			<a href="#">Add New Role Mapping Policy</a>
Role Mapping Policy Details				
Description:	-			
Default Role:	-			
Rules Evaluation Algorithm:	-			
Conditions		Role		

Summary	Service	Authentication	Roles	Enforcement
Use Cached Results:	<input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions			
Enforcement Policy:	Ariya MPSK Operator Logins <a href="#">Modify</a>			<a href="#">Add New Enforcement Policy</a>
Enforcement Policy Details				
Description:				
Default Profile:	[Deny Application Access Profile]			
Rules Evaluation Algorithm:	first-applicable			
Conditions		Enforcement Profiles		
1. (Authorization:Ariya AD:memberOf <b>CONTAINS</b> Student)		MPSK Operator		

### Enforcement Profiles - MPSK-Operator

Summary

Profile

Attributes

Profile:

Name:	MPSK Operator
Description:	
Type:	Application
Action:	Accept
Device Group List:	-

Attributes:

Attribute Name		Attribute Value	
1.	admin_privileges	=	Students
2.	ClearPass:User-Email-Address	=	%{Authorization:Ariya AD:Email}

The important bit here is the Attributes we are sending back to ClearPass Guest application authentication. The first one is “Students” which is the name of the operator profile we will configure in ClearPass Guest. The second attribute is the email address of the user so the MPSK credentials can be emailed to the user.

## 5.8 Messaging Server

Part of the MPSK workflow is for ClearPass to email the credentials to the person who is registering their devices. For that we need to configure SMTP relay server. Here I am using a gmail account

aruba

Dashboard

Monitoring

Configuration

Administration

ClearPass Portal

Users and Privileges

Server Manager

External Servers

SNMP Trap Receivers

Syslog Targets

Syslog Export Filters

Messaging Setup

Endpoint Context Servers

File Backup Servers

External Accounts

ClearPass Policy Manager

Menu

Administration » External Servers » Messaging Setup

Messaging

Successfully sent test email to: ariyap@hpe.com

ClearPass Messaging Setup guides you through configuration of the SMTP server for email and SMS notifications.

SMTP Server

SMTP Settings

Server Name:smtp.gmail.com

Username:

Password:

Verify Password:

Default From Address:ariyap@hpe.com

Connection Security:StartTLS

Port:587

Connection Timeout:30 seconds

Send Test Email

Send Test SMS

Reset

Save

You can also send the test email by clicking on the “Send Test Email” button ensuring that all is good.

## 6 ClearPass Guest

Here we'll cover the ClearPass Guest configurations that are needed. You can configure the method, complexity, and length of the MPSK passwords, and whether they will be generated, or user created.

### 6.1 MPSK Configuration

There is a new MPSK configuration that you can find under Administration -> Aruba Integrations

aruba ClearPass Guest Menu

Home » Administration » Aruba Integrations » MPSK Configuration

Configure MPSK

Use this form to make changes to the configuration options for Aruba MPSK.

**Configure MPSK**

**Auto-Configuration**

\* Deployment Mode: ☒ Do not modify any configuration  
☐ Always generate unique device Wi-Fi passwords  
☐ Allow unique device Wi-Fi passwords  
☐ Remove MPSK related fields from device forms and views

**Password Options**

\* Random MPSK Method: Random lowercase letters excluding vowels  
The method used to generate a random device MPSK.

\* Random Password Length: 8  
Number of characters to include in randomly-generated pre-shared keys.

MPSK Example: trldjqtr Generate

Save Configuration

\* required field

In most of the cases “Allow generate unique WiFi passwords” is used, where WiFi password is referred to MPSK. This mode creates unique PSK for the user since most of the users don't know if they need it or not or can easily get confused. The next option “allow unique device WiFi passwords” provides a checkbox in the mac\_create form for the user to select it.

Home » Administration » Aruba Integrations » MPSK Configuration

#### Configure MPSK

Use this form to make changes to the configuration options for Aruba MPSK.

**Configure MPSK**

**Auto-Configuration**

\* Deployment Mode: ☒ Always generate unique device Wi-Fi passwords  
☐ Do not modify any configuration  
☐ Allow unique device Wi-Fi passwords  
☐ Remove MPSK related fields from device forms and views

An Aruba MPSK will be generated for each new device that is registered.

**Forms**

- mac\_create: Add field mpsk\_enable
- mac\_create: Add field sponsor\_email
- mac\_create: Add field auto\_send\_smtp
- mac\_create: Add field smtp\_email\_field
- mac\_create\_receipt: Add field mpsk\_enable
- mac\_create\_receipt: Add field mpsk
- mac\_edit: Add field mpsk\_enable
- mac\_edit: Add field mpsk\_refresh
- mac\_edit: Add field mpsk
- mac\_edit: Add field mpsk\_has\_key
- mac\_edit: Add field smtp\_auto\_send\_field
- mac\_edit\_receipt: Add field mpsk\_enable
- mac\_edit\_receipt: Add field mpsk
- mactrac\_create: Add field mpsk\_enable
- mactrac\_create: Add field sponsor\_email
- mactrac\_create: Add field auto\_send\_smtp
- mactrac\_create: Add field smtp\_email\_field
- mactrac\_edit: Add field mpsk\_enable
- mactrac\_edit: Add field mpsk\_refresh
- mactrac\_edit: Add field mpsk
- mactrac\_edit: Add field mpsk\_has\_key
- mactrac\_edit: Add field smtp\_auto\_send\_field

Device Wi-Fi passwords are sent via email receipts and valid SMTP server settings must be provided.

**Password Options**

\* Random MPSK Method: Random lowercase letters excluding vowels  
The method used to generate a random device MPSK.

\* Random Password Length: 8  
Number of characters to include in randomly-generated pre-shared keys.

MPSK Example: trldjqtr Generate

Save Configuration

\* required field

As seen above you can also choose the MPSPK complexity and length but by default is minimum 8 and uses lowercase letters excluding vowels.

## 6.2 Operator Profile

Operator profiles are used for a user who is able to log in to ClearPass Guest. You can have different operator profile with different level of access. Here we need one for the students to be able to login and register their devices.

aruba

Guest

Devices

Onboard

Configuration

Administration

API Services

API Clients

API Explorer

SOAP Web Services

Aruba Integrations

Controllers

AirGroup Configuration

MPSK Configuration

Check Security

Data Retention

Extensions

Import Configuration

Operator Logins

Login Configuration

Profiles

Servers

Translation Rules

ClearPass Guest

Menu

Home » Administration » Operator Logins » Profiles

Operator Profiles

Create a new operator profile

ClearPass Guest supports role-based access control through the use of operator profiles. Each operator using the server is assigned a profile, which determines the actions that the operator may perform, as well as global settings such as the look and feel of the user interface.

Some operator profile settings may be overridden in the operator's account settings. These customized settings will take precedence over the default values defined in the operator profile.

Use this list view to define new operator profiles, and to make changes to existing operator profiles.

Name	Description
API Guest Operator	Operators with this profile can use the API to manage guest accounts.
BYOD Operator	Operators with this profile can view and manage their own provisioned devices.
Device Registration	Operators with this profile can self-provision their devices, for use with MAC authentication and AirGroup sharing.
Help Desk	Operators with this profile can troubleshoot problems reported by end users.
Network Administrator	Operators with this profile can view and configure network-related settings.
Null Profile	Default profile with no permissions.
Operations and Marketing	Operators with this profile can configure guest workflows, manage print templates and control other application customization options.

Home » Administration » Operator Logins » Profiles

Edit Operator Profile (new)

Use this form to create a new operator profile.

Operator Profile Editor

\* Name:

Students

Enter a name for this operator profile.

Description:

MPSK operator

Comments or descriptive text about the operator profile.

Access

These options control what operators with this profile are permitted to do.

Enabled:

☒ Allow operator logins

If unchecked, operators with this profile will not be able to log in.

Operator Privileges

Administrator

No Access

Select operator permissions for system administration and management tasks.

Advertising Services

No Access

Select operator permissions for managing advertising content and services.

API Services

No Access

Select operator permissions for API access and management.

Aruba Integrations

No Access

Select operator permissions for access to Aruba integrations.

Devices

Custom...

Select operator permissions for managing devices on a network.

Create New Device

☐ No Access ☐ Read Only ☒ Full

Operators with this privilege may create individual devices.

Export Devices

☒ No Access ☐ Read Only

Operators with this privilege may export a list of devices.

Import Devices

☒ No Access ☐ Read Only ☐ Full

Operators with this privilege may create new devices from a data source.

Manage Devices

☐ No Access ☐ Read Only ☒ Full

Operators with this privilege may view and manage individual devices.

Privileges:

**Guest Manager**
No Access

Select operator permissions for managing guest users for a network.

**Hotspot Manager**
No Access

Select operator permissions for managing self-provisioned guest access.

**Insight**
No Access

Select operator permissions for Insight application

**IP Phone Services**
No Access

Select operator permissions for IP phone administration and management tasks.

**Onboard**
No Access

Select operator permissions for managing Onboard device provisioning.

**Operator Logins**
No Access

Select permissions for managing local operator logins.

**Pass Services**
No Access

Select operator permissions for managing digital passes.

**Platform**
No Access

Select operator permissions for platform administration tasks.

**Policy Manager**
No Access

Select operator permissions for Policy Manager

**SMS Services**
No Access

Select operator permissions for access to SMS services.

**SMTP Services**
Custom...

Select operator permissions for SMTP services.

Configure SMTP Services
☒ No Access
☐ Read Only
☐ Full

Operators with this privilege may configure SMTP settings.

Send SMTP Messages
☐ No Access
☐ Read Only
☒ Full

**Support Services**
No Access

Select operator permissions for access to support services.

**Translation Assistant**
No Access

Select operator permissions for tasks related to translation.

☒ Show descriptions

Select the privileges that will be granted to this operator login.

User Roles:

Name
<input checked="" type="checkbox"/> ClearPass Policy Manager
<input type="checkbox"/> [Contractor]
<input type="checkbox"/> [Guest]
<input type="checkbox"/> [Employee]
<input checked="" type="checkbox"/> Student-Devs

10 rows per page

Select the visitor account roles that these operators are permitted to use.

\* Operator Filter:

No operator filter

Select the default operator filtering to apply to guest accounts.

User Account Filter:

Enter a comma-delimited list of field=value pairs to create an account filter.

Session Filter:

Enter a comma-delimited list of field=value pairs to create a session filter.

Account Limit:

0

Maximum number of accounts the operator can create.  
Leave blank for no limit.

User Interface

These options control the visual appearance and behavior of the application.

Skin:

(Default)

Choose the skin to use for operators with this profile.

Start Page:

(Default)

The initial page to show this operator after logging in.

Language:

Auto-detect

Select the default language to use for operators with this profile.

Time Zone:

(GMT+10:00) Australia/Melbourne; Victoria

Select the default time zone for operators with this profile.

Customization:

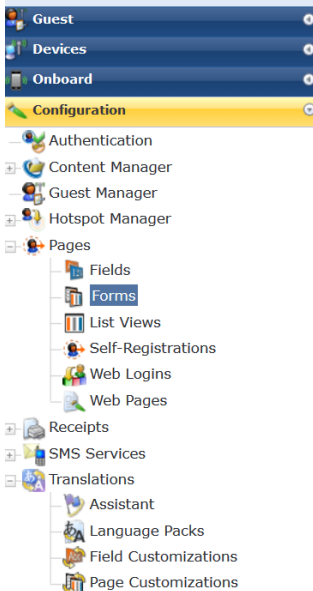
☐ Override the application's forms and views

If checked, you can specify different default forms and views to use.

Save Changes

## 6.3 Form Fields

The form that the users will use to register their devices is “mac\_create” as seen below. You need to make sure that “sponsor\_email” is enabled.



Home » Configuration » Pages » Forms

## Customize Form Fields (mac\_create)

Use this list view to modify the fields of the form **mac\_create**.

Quick Help		Preview Form			
Rank	Field	Type	Label	Description	
1	enabled	dropdown	Account Status:	Select an option for changing the status of this account.	
5	mac_auth	hidden	Is Device:		
5.1	mac	text	MAC Address:	MAC address of the device.	
10	sponsor_name	text	Sponsor's Name:	Name of the person sponsoring this account.	
10.1	sponsor_email	text	Sponsor's Email:	Email of the person sponsoring this account.	
20	visitor_name	text	Device Name:	Name of the device.	
25	visitor_phone	phone	Phone Number:	The guest's phone number.	
30	visitor_company	text	Company Name:	Company name of the guest.	
35	airgroup_device_type	dropdown	Device Type:	Select the type of your device.	
40	mppsk_enable	hidden	Wi-Fi Password:		
40.2	auto_send_smtp	hidden	Auto Email:		
40.3000000000000004	smtp_email_field	hidden	Email Field:		

AirGroup uses device ownership and

You need to further edit that field and add a value to the "Initial value"

Home » Configuration » Pages » Forms

## Customize Form Field (sponsor\_email)

Use this form to override the field **sponsor\_email** in the form **mac\_create**. [Edit Base Field](#)

Form Field Editor	
* Field Name:	<input type="text" value="sponsor_email"/> Select the field definition to attach to the form.
<b>Form Display Properties</b>	
These properties control the user interface displayed for this field.	
Field:	<input checked="" type="checkbox"/> Enable this field When checked, the field will be included as part of the form.
* Rank:	<input type="text" value="10.1"/> Number indicating the relative ordering of user interface fields, which are displayed in order of increasing rank.
* User Interface:	<input type="text" value="Text field"/> The kind of user interface element to use when entering or editing this field.
Label:	<input type="text" value="Sponsor's Email:"/> Label for this field to display on the form.
Description:	<input type="text" value="Email of the person sponsoring this account."/> Descriptive text for this field, displayed with the user-interface element.
CSS Class:	<input type="text"/> Optional CSS class name to apply to this form field.
CSS Style:	<input type="text" value="width: 240px;"/> Optional CSS style text to apply to this form field.
Placeholder:	<input type="text"/> Prompt text to display in the user interface element. Requires a HTML 5 capable browser.
Label After:	<input type="text"/> Text to display after the user interface element.

Label After (HTML):	<div style="border: 1px solid green; height: 30px; width: 100%;"></div> <div style="border: 1px solid green; padding: 2px;">Insert...</div> <p>HTML to display after the user interface element. You can use Smarty template syntax in this field.</p>
<b>Form Validation Properties</b> These properties control how the value of this field is checked.	
Field Required:	<input type="checkbox"/> <div style="border: 1px solid green; padding: 2px;">Field value must be supplied</div> Select this option if the field cannot be omitted or left blank.
Initial Value:	<div style="border: 1px solid green; padding: 2px;">array ( 'generator' =&gt; 'GeneratorFromSession', 'generator_ar</div> <div style="float: right; text-align: right;">Revert</div> <p>Value to initialize this field with when the form is first displayed.</p>
* Validator:	<div style="border: 1px solid green; padding: 2px;">IsValidEmail</div> <p>The function used to validate the contents of a field.</p>
Validator Param:	<div style="border: 1px solid green; padding: 2px;">(None)</div> <p>Optional name of field whose value will be supplied as the argument to a validator.</p>
Validator Argument:	<div style="border: 1px solid green; padding: 2px;"> <pre>array (   'allow' =&gt;     array (</pre> </div> <p>Optional value to supply as the argument to a validator.</p>
Validation Error:	<div style="border: 1px solid green; padding: 2px;">Please enter a valid email address.</div> <p>The error message to display if the field's value fails validation and the validator does not return an error message directly.</p>
<b>Advanced Properties</b> These properties control conversion, display and dynamic behaviours.	
Advanced:	<input type="checkbox"/> <div style="border: 1px solid green; padding: 2px;">Show advanced properties</div>
Type Error:	<div style="border: 1px solid green; height: 20px; width: 100%;"></div> <p>The error message to display if the field's value is not supplied, has an incorrect type, or if conversion fails.</p>
<div style="background-color: #4f81bd; color: white; padding: 5px 10px; display: inline-block;">Save Changes</div>	

The initial value should be as shown below.

```
array ( 'generator' => 'GeneratorFromSession', 'generator_args' => array ( 0 => 'userauth_user', 1 => 'User-Email-Address', ), )
```

The above will populate the sponsor email field with the email attribute of the user who is registering the device. Remember that “MPSK-Operator” enforcement profile is sending the “%{Authorization:AriyaAD:Email} to Aruba Guest application.

You also want to change the initial value of the

- “role\_id” field to be “4” which is Student-Devs
- “creator\_accept\_terms” field to be “1” which is selected

And finally, you might want to disable “airgroup” field. Once you have saved it you can click on the preview of the form to double check it as shown below.

Guest

Devices

Onboard

Configuration

Authentication

Content Manager

Guest Manager

Hotspot Manager

Pages

Fields

Forms

List Views

Self-Registrations

Web Logins

Web Pages

Receipts

SMS Services

Translations

Administration

ClearPass Guest

Use this list view to modify the fields of the form **mac\_create**.

Quick Help
Preview Form

Create New Device

\* MAC Address:

Sponsor's Email:

\* Device Name:

AirGroup: ☐ Enable AirGroup  
AirGroup uses device ownership and location information to limit the printers and Apple TVs available to network users.

Account Activation: 

Now

Account Expiration: 

1 year from now

\* Account Role: 

Student-Devs

Notes:

\* Terms of Use: ☒ I am the sponsor of this account and accept the terms of use  
Flag indicating that the creator has accepted the terms and conditions of use.

Create

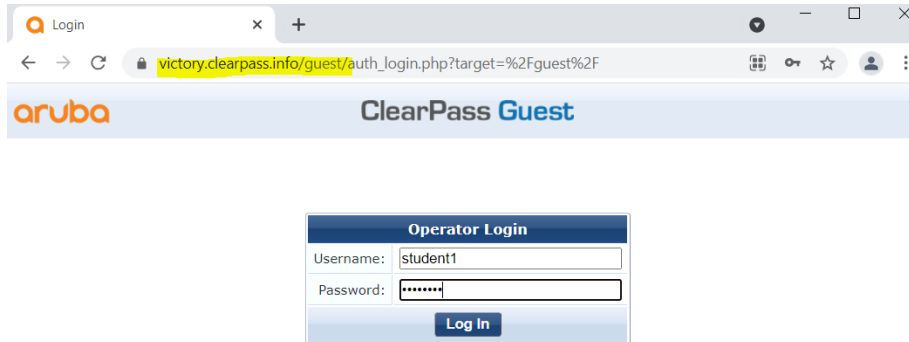


## 7 Testing

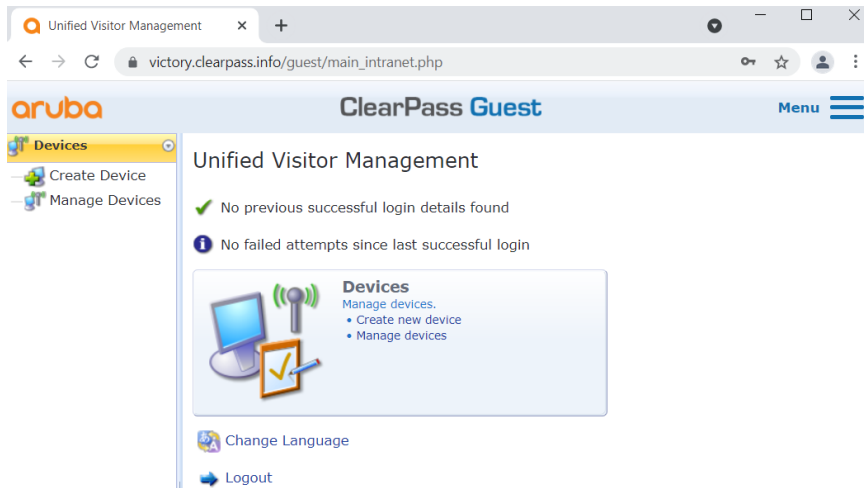
So now when the user who is in “Students” AD user group login to ClearPass Guest for device registration, its authentication request should match the “Guest Operator Logins”

### 7.1 Device Registration

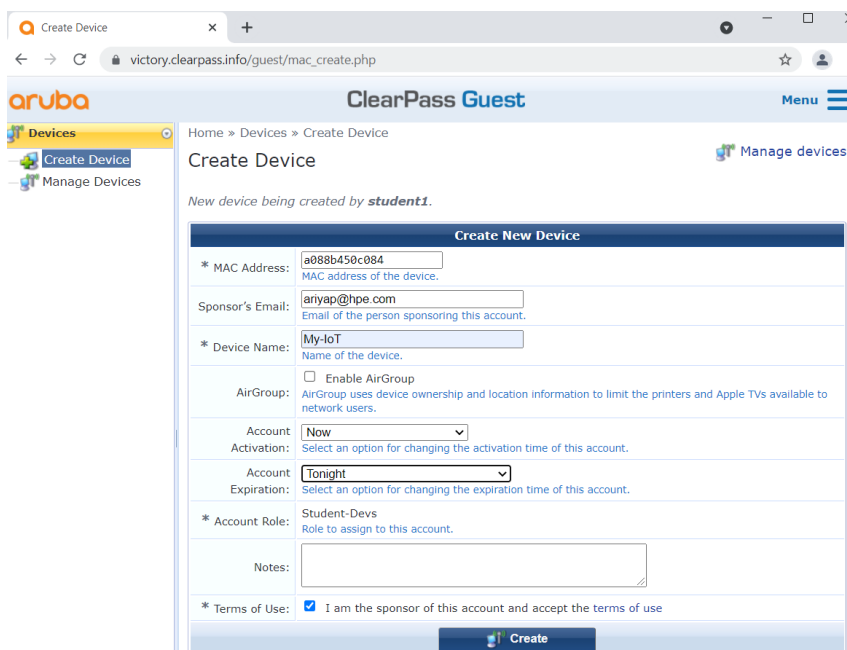
So now when the user is instructed to go to the ClearPass guest URL to login,



Upon successful login, the user will see this page. This is a default page and you can customise it like you would with any Guest Weblogin page.



I’ll add the MAC address of my device, give it a name, and choose the account expiry. Remember that account expiry can also be customised to reduce the options and you can also remove “Airgroup” field from this form.



Once I have clicked on the “Create” button, I get the following screen.

aruba ClearPass Guest Menu

Home » Devices » Create Device

Create Device Manage Devices

Create another device Manage devices

The device was successfully created.

Create New Device Receipt	
MAC Address:	A0-88-B4-50-C0-84
Account Status:	Active
Account Activation:	Saturday, 17 July 2021, 4:50 PM
Account Expiration:	Account will expire at Saturday, 17 July 2021, 11:59 PM
Account Role:	Student-Devs
Registered By:	student1
Wi-Fi Password:	lbxwtwnwz

Open print window using template... ▾

Back to devices

Back to main

The credentials for the MPSK should also be email automatically to the email address of the user who was registering this device. Here is the sample email that was sent.

Device receipt for My-IoT (A0-88-B4-50-C0-84)

Aruba ClearPass Guest

**Your device has been successfully registered and can now be connected.**

**Wi-Fi Network:** Aruba

**Device Name:** My-IoT

**MAC Address:** A0-88-B4-50-C0-84

**Device Wi-Fi Instructions:**

Make sure your wireless adapter A0-88-B4-50-C0-84 is set to dynamically obtain an IP address

Connect to the wireless network: Aruba

Wi-Fi password: lbxwtwnwz

Device expires: Saturday, July 17, 2021 23:59

© Copyright 2021 Aruba, a Hewlett Packard Enterprise company.

You should also be able to view the MPSK credential from “Device Registration”

Open print window using template... ▾

Open print window using template...

Account List

Certificate Expiry

**Device Registration**

Download Receipt

Guest Account Expiry

GuestManager Receipt

One account per page

SMS Receipt

SMS Sponsor Confirmation Alert

Sponsor Device Provisioning

Sponsorship Confirmation

Two-column scratch cards

Choosing it will pop a new browser window as shown below.

**Your device has been successfully registered and can now be connected.**

**Wi-Fi Network: Aruba**

**Device Name: My-IoT**

**MAC Address: A0-88-B4-50-C0-84**

**Device Wi-Fi Instructions:**

- 1 Make sure your wireless adapter **A0-88-B4-50-C0-84** is set to dynamically obtain an IP address
- 2 Connect to the wireless network: **Aruba**
- 3 Wi-Fi password: **lbxwtwz**
- 4 Device expires: Saturday, July 17, 2021 23:59

Menu

Create another device

Manage devices

## 7.2 ClearPass Access Tracker Operator Login

So, from Access tracker we see the following two Auth Requests

**aruba**

Dashboard

Monitoring

Live Monitoring

Access Tracker

Accounting

OnGuard Activity

Analysis & Trending

System Monitor

Profiler and Network Scan

Audit Viewer

Event Viewer

Data Filters

Blacklisted Users

**ClearPass Policy Manager**

Monitoring » Live Monitoring » Access Tracker

**Access Tracker** Jul 17, 2021 16:28:30 AEST

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

#	Server	Source	Username	Service	Login Status	Request Timestamp
1.	192.168.1.95	WEBAUTH	B4-5D-50-C6-82-4A	[Device Registration Disconnect]	ACCEPT	2021/07/17 16:07:04
2.	192.168.1.95	Application	student1	Ariya Guest Operator Logins	ACCEPT	2021/07/17 16:03:22

The Request ID #2 is when the student1 login to ClearPass Guest for device registration.

Request Details

Summary

Input

Output

Login Status: ACCEPT

Session Identifier: W00000002-01-60f272aa

Date and Time: Jul 17, 2021 16:03:22 AEST

End-Host Identifier: -

Username: student1

Access Device IP/Port: -

Access Device Name: -

System Posture Status: UNKNOWN (100)

**Policies Used -**

Service: Ariya Guest Operator Logins

Authentication Method: Not applicable

Authentication Source: Ariya AD

Authorization Source: Ariya AD

Roles: Student, [User Authenticated]

Enforcement Profiles: MPSK Operator

Showing 2 of 1-3 records

Change Status

Show Configuration

Export

Show Logs

Close

While checking the "Input" tab for Authorization attributes, we see the email address of the user

Summary

Input

Output

Username: student1

End-Host Identifier: -

Access Device IP/Port: -

**Authorization Attributes**

Authorization:Ariya AD:Account Expires	9223372036854775807 [30828-09-14 12:48:05 AEST]
Authorization:Ariya AD:Email	ariyap@hpe.com
Authorization:Ariya AD:memberOf	CN=Student,CN=Users,DC=wlan,DC=net
Authorization:Ariya AD:Name	student1
Authorization:Ariya AD:Nested Groups	Student
Authorization:Ariya AD:UserDN	CN=student1,CN=Users,DC=wlan,DC=net

**Computed Attributes**

And we are passing that to ClearPass Guest along with the operator profile name.

Summary	Input	Output
Enforcement Profiles:	MPSK Operator	
System Posture Status:	UNKNOWN (100)	
Application Response		
Application:admin_privileges	Students	
Application:ClearPass:User-Email-Address	ariyap@hpe.com	

When we clicked on the “Create” button for device registration, it will generate the WEBAUTH request that basically will disconnect the device if it was on the network.

Request Details

Summary	Input	Output
Login Status:	ACCEPT	
Session Identifier:	W00000003-01-60f27387	
Date and Time:	Jul 17, 2021 16:07:04 AEST	
End-Host Identifier:	B4-5D-50-C6-82-4A	
Username:	B4-5D-50-C6-82-4A	
Access Device IP/Port:	-	
Access Device Name:	-	
System Posture Status:	UNKNOWN (100)	
Policies Used -		
Service:	[Device Registration Disconnect]	
Authentication Method:	Not applicable	
Authentication Source:	[Guest Device Repository]	
Authorization Source:	[Guest Device Repository]	
Roles:	[User Authenticated]	
Enforcement Profiles:	[ArubaOS Wireless - Terminate Session], [Aerohive - Terminate Session], [Cisco -	
Summary	Input	Output
Username:	B4-5D-50-C6-82-4A	
End-Host Identifier:	B4-5D-50-C6-82-4A	
Access Device IP/Port:	-	
Computed Attributes		
Application:ClearPass:Page-Name	mac_create	
Authentication:Full-Username	B4-5D-50-C6-82-4A	
Authentication:Full-Username-Normalized	B4-5D-50-C6-82-4A	
Authentication:Posture	Unknown	
Authentication:Source	[Guest Device Repository]	
Authentication:Status	User	
Authentication:Username	B4-5D-50-C6-82-4A	
Authorization:Sources	[Guest Device Repository]	
Connection:Client-Mac-Address	b45d50c6824a	
Connection:Client-Mac-Address-Colon	b4:5d:50:c6:82:4a	
Connection:Client-Mac-Address-Not	b45d50c6824a	
Summary	Input	Output
Enforcement Profiles:	[ArubaOS Wireless - Terminate Session], [Aerohive - Terminate Session], [Cisco - Terminate Session], [H3C - Terminate Session], [Juniper Terminate Session], [Motorola - Terminate Session], [Trapeze - Terminate Session], [ArubaOS Switching - Terminate Session], [AOS-CX - Disconnect]	
System Posture Status:	UNKNOWN (100)	
RADIUS Response		
Radius:IETF:Acct-Session-Id		
Radius:IETF:Calling-Station-Id	a088b450c084	
Radius:IETF:NAS-Identifier		
Radius:IETF:NAS-IP-Address	10.10.55.10	
Radius:IETF:NAS-Port	0	
Radius:IETF:Service-Type	1	
Radius:IETF:User-Name	a088b450c084	

Now we should also check the Event Viewer to see if the email was sent to the user.

aruba ClearPass Policy Manager

Monitoring » Event Viewer

Event Viewer

The Event Viewer provides reports about system-level events. All attempted upgrade, patch, and hotfix installations are logged here.

Select Server: victory (192.168.1.95)

Filter: Source contains Go Clear Filter Show 20 records

#	Source	Level	Category	Action	Timestamp
1.	Admin UI	INFO	Email Successful	None	Jul 17, 2021 16:07:16 AEST
2.	Guest UI	INFO	Logged in	None	Jul 17, 2021 16:03:22 AEST
3.	ClearPass Updater	INFO	AV/AS Updates	Success	Jul 17, 2021 15:56:14 AEST

aruba ClearPass Policy Manager

Monitoring » Event Viewer

Event Viewer

The Event Viewer provides reports about system-level events. All attempted upgrade, patch, and hotfix installations are logged here.

Filter: Source contains Go Clear Filter

#	Source	Level	Category	Action	Timestamp
1.	Admin UI	INFO	Email Successful	None	Jul 17, 2021 16:07:16 AEST
2.	Guest UI	INFO	Logged in	None	Jul 17, 2021 16:03:22 AEST
3.	ClearPass Updater	INFO	AV/AS Updates	Success	Jul 17, 2021 15:56:14 AEST

System Event Details

Source	Admin UI
Level	INFO
Category	Email Successful
Action	None
Timestamp	Jul 17, 2021 16:07:16 AEST
Description	From: ariyap@hpe.com To: ariyap@hpe.com Mail Subject: Device receipt for My-IoT (B4-5D-50-C6-82-4A)

Close

## 7.3 ClearPass Access Tracker MPSK Authentication

This is the Authentication request as seen from ClearPass.

ClearPass Policy Manager

Monitoring » Live Monitoring » Access Tracker

Access Tracker Jul 17, 2021 16:57:27 AEST

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 Edit

Filter: Request ID contains Go Clear Filter Show 20 records

#	Server	Source	Username	Service	Login Status	Request Timestamp
1.	192.168.1.95	RADIUS	student1	MPSK Aruba Wireless with MPSK	ACCEPT	2021/07/17 16:56:03
2.	192.168.1.95	WEBAUTH	A0-88-B4-50-C0-84	[Device Registration Disconnect]	ACCEPT	2021/07/17 16:50:35
3.	192.168.1.95	Application	student1	Ariya Guest Operator Logins	ACCEPT	2021/07/17 16:48:39

Here is the full detail of the access tracker tabs for this request.

Request Details

Summary Input Output Accounting

Login Status:	ACCEPT
Session Identifier:	R00000003-01-60f280cc
Date and Time:	Jul 17, 2021 17:03:40 AEST
End-Host Identifier:	A0-88-B4-50-C0-84
Username:	student1
Access Device IP/Port:	10.10.55.10
Access Device Name:	AOS10-APs
System Posture Status:	UNKNOWN (100)

Policies Used -

Service:	MPSK Aruba Wireless with MPSK
Authentication Method:	MAC-AUTH
Authentication Source:	Local:localhost
Authorization Source:	[Guest Device Repository]
Roles:	Student-Devs, [User Authenticated]
Enforcement Profiles:	Aruba User Role - Student-Devs, [Registered Device MPSK], [Return Device]

Summary	Input	Output	Accounting
Username:	student1		
End-Host Identifier:	A0-88-B4-50-C0-84		
Access Device IP/Port:	10.10.55.10		
RADIUS Request			
Radius:Aruba:Aruba-AP-Group	AOS10		
Radius:Aruba:Aruba-Essid-Name	ArubaMPSK		
Radius:Aruba:Aruba-Location-Id	b4:5d:50:c6:82:4a		
Radius:IETF:Called-Station-Id	b45d50c6824a		
Radius:IETF:Calling-Station-Id	a088b450c084		
Radius:IETF:NAS-IP-Address	10.10.55.10		
Radius:IETF:NAS-Port	0		
Radius:IETF:NAS-Port-Type	19		
Radius:IETF:Service-Type	10		
Radius:IETF:User-Name	a088b450c084		

Summary	Input	Output	Accounting
Username:	student1		
End-Host Identifier:	A0-88-B4-50-C0-84		
Access Device IP/Port:	10.10.55.10		
RADIUS Request			
Authorization Attributes			
Authorization:[Guest Device Repository]:AccountStatus	0		
Authorization:[Guest Device Repository]:Device Account Active	true		
Authorization:[Guest Device Repository]:Device Account Enabled	true		
Authorization:[Guest Device Repository]:Device Account Expired	false		
Authorization:[Guest Device Repository]:Device MPSK	*****		
Authorization:[Guest Device Repository]:Device Role ID	3009		
Authorization:[Guest Device Repository]:RemainingExpiration	24919		
Authorization:[Guest Device Repository]:SponsorName	student1		

And most importantly ClearPass sends back the MPSK, username and user role to Aruba APs.

Summary	Input	Output	Accounting
Enforcement Profiles:	Aruba User Role - Student-Devs, [Registered Device MPSK], [Return Device Sponsor Name - RADIUS User-Name]		
System Posture Status:	UNKNOWN (100)		
Audit Posture Status:	UNKNOWN (100)		
RADIUS Response			
Radius:Aruba:Aruba-MPSK-Passphrase	*****		
Radius:Aruba:Aruba-User-Role	Student-Devs		
Radius:IETF:User-Name	student1		

## 7.4 Aruba Central Clients Monitoring

Here are the Aruba Central clients view.

aruba

Central

Search or ask Aruba

3 hours

List

Summary

Global

Manage

Overview

Devices

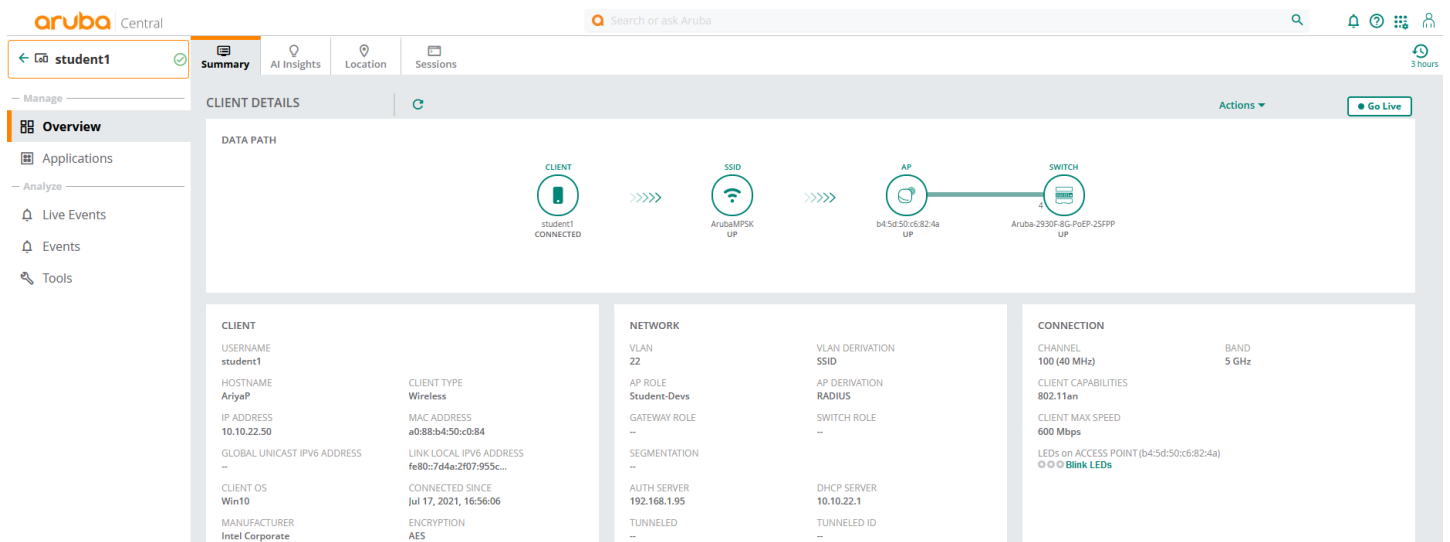
Clients

CLIENTS

ALL

0 (00 | 00)

Client Name	Status	IP Address	VLAN	Connected To	SSID/P...	AP Role	Health	MAC Address	Key Management
student1	Connected	10.10.22.50	22	b4:5d:50:c6:82:4a	ArubaMPSK	Student-Devs	Good	a0:88:b4:50:c0:84	WPA2_PSK



As it can be seen above the device connected successfully. We'll check the authentication buffer as well.

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

Client List
-----
Name      IP Address  MAC Address  OS      ESSID      Access Point  Channel  Type  Role
IPv6 Address  Signal      Speed (mbps)
-----
student1  10.10.22.50  a0:88:b4:50:c0:84  Win 10  ArubaMPSK  b4:5d:50:c6:82:4a  100+    AN    Student-Devs
fe80::7d4a:2f07:955c:cd4f  43(good)  108(ok)
Number of Clients : 1
Info timestamp : 22476
b4:5d:50:c6:82:4a# sh ap debug auth-trace-buf mac a0:88:b4:50:c0:84

Auth Trace Buffer
-----
Jul 17 17:04:12 mac-auth-req -> a0:88:b4:50:c0:84 b4:5d:50:e8:24:b4/ClearPass - - a088b450c084
Jul 17 17:04:12 mac-auth-success <- a0:88:b4:50:c0:84 b4:5d:50:e8:24:b4/ClearPass - - success
Jul 17 17:04:12 station-up * a0:88:b4:50:c0:84 b4:5d:50:e8:24:b4 - - wpa2 psk aes
Jul 17 17:04:12 wpa2-key1 <- a0:88:b4:50:c0:84 b4:5d:50:e8:24:b4 - 117
Jul 17 17:04:13 wpa2-key2 -> a0:88:b4:50:c0:84 b4:5d:50:e8:24:b4 - 119
Jul 17 17:04:13 wpa2-key3 <- a0:88:b4:50:c0:84 b4:5d:50:e8:24:b4 - 151
Jul 17 17:04:13 wpa2-key4 -> a0:88:b4:50:c0:84 b4:5d:50:e8:24:b4 - 95
Jul 17 17:04:13 rad-acct-start -> a0:88:b4:50:c0:84 b4:5d:50:e8:24:b4/ClearPass - -
Jul 17 17:04:29 rad-acct-int-update -> a0:88:b4:50:c0:84 b4:5d:50:e8:24:b4 - -
Jul 17 17:05:29 rad-acct-int-update -> a0:88:b4:50:c0:84 b4:5d:50:e8:24:b4 - -
Jul 17 17:06:30 rad-acct-int-update -> a0:88:b4:50:c0:84 b4:5d:50:e8:24:b4 - -
Jul 17 17:07:30 rad-acct-int-update -> a0:88:b4:50:c0:84 b4:5d:50:e8:24:b4 - -
Jul 17 17:08:30 rad-acct-int-update -> a0:88:b4:50:c0:84 b4:5d:50:e8:24:b4 - -
Jul 17 17:09:30 rad-acct-int-update -> a0:88:b4:50:c0:84 b4:5d:50:e8:24:b4 - -
Jul 17 17:10:30 rad-acct-int-update -> a0:88:b4:50:c0:84 b4:5d:50:e8:24:b4 - -
b4:5d:50:c6:82:4a#
```

Now we'll view the details of the MPSK local cache

```
b4:5d:50:c6:82:4a# show ap mpskcache

PPSK Cache Table
-----
Client MAC      Key      Del  Expiry  Role      VLAN  ESSID
Seqno IP
-----
a0:88:b4:50:c0:84 (6): b8 b0 5d 26 5e 62 ... No - Student-Devs 22 ArubaMPSK
22234 10.10.22.50
PPSK Cache Count: 1
b4:5d:50:c6:82:4a#
```

Note that the Del column shows “No” and Expiry columns is empty. This will be the case if the device is in the association table of the IAP.

Now I have disconnected the device. As soon as the client is removed from this table, you’ll see the Del= Yes and the expiry time is set to 16:40 min.

```
b4:5d:50:c6:82:4a# show ap mpskcache

PPSK Cache Table
-----
Client MAC      Key          Del  Expiry  Role          VLAN  ESSID
Seqno  IP
-----
-----
a0:88:b4:50:c0:84  (6): b8 b0 5d 26 5e 62 ... Yes  16m:40s  Student-Devs  22
ArubaMPSK  22234  10.10.22.50
PPSK Cache Count:1
b4:5d:50:c6:82:4a#
b4:5d:50:c6:82:4a# show ap mpskcache

PPSK Cache Table
-----
Client MAC      Key          Del  Expiry  Role          VLAN  ESSID
Seqno  IP
-----
-----
a0:88:b4:50:c0:84  (6): b8 b0 5d 26 5e 62 ... Yes  13m:49s  Student-Devs  22
ArubaMPSK  22234  10.10.22.50
PPSK Cache Count:1
b4:5d:50:c6:82:4a#
```

When the MPSK local cache is available all MPSK authentication will be successful even if ClearPass is not reachable. However, when the Expiry time runs out and ClearPass is not available the MPSK clients can’t authenticate, see below

```
b4:5d:50:c6:82:4a# show ap mpskcache

PPSK Cache Table
-----
Client MAC      Key          Del  Expiry  Role          VLAN  ESSID  Seqno  IP
-----
-----
PPSK Cache Count:0
b4:5d:50:c6:82:4a#

b4:5d:50:c6:82:4a# sh ap debug auth-trace-buf 10

Auth Trace Buffer
-----
Jul 17 18:19:01 mac-auth-req          -> a0:88:b4:50:c0:84 b4:5d:50:e8:24:b4/ClearPass - -
a088b450c084
Jul 17 18:19:21 rad-status-server      * 00:00:00:00:00:01 00:00:00:00:00:01/ClearPass - -
Jul 17 18:19:21 server out-of-service * a0:88:b4:50:c0:84 b4:5d:50:e8:24:b4/ClearPass - -
server timeout
Jul 17 18:19:41 server out-of-service * b4:5d:50:c6:82:4a 00:00:00:00:00:01/ClearPass - -
server timeout
b4:5d:50:c6:82:4a#
```

And when we reconnect the ClearPass to the network like before, all MPSK authentication will get through.

```
b4:5d:50:c6:82:4a# sh ap debug auth-trace-buf 20

Auth Trace Buffer
-----
Jul 17 18:19:01 mac-auth-req          -> a0:88:b4:50:c0:84 b4:5d:50:e8:24:b4/ClearPass - -
a088b450c084
Jul 17 18:19:21 rad-status-server      * 00:00:00:00:00:01 00:00:00:00:00:01/ClearPass - -
```



```

Jul 17 18:19:21 server out-of-service * a0:88:b4:50:c0:84 b4:5d:50:e8:24:b4/ClearPass - -
server timeout
Jul 17 18:19:41 server out-of-service * b4:5d:50:c6:82:4a 00:00:00:00:00:01/ClearPass - -
server timeout
Jul 17 18:30:34 mac-auth-req -> a0:88:b4:50:c0:84 b4:5d:50:e8:24:b4/ClearPass - -
a088b450c084
Jul 17 18:30:34 mac-auth-success <- a0:88:b4:50:c0:84 b4:5d:50:e8:24:b4/ClearPass - -
success
Jul 17 18:30:34 station-up * a0:88:b4:50:c0:84 b4:5d:50:e8:24:b4 - -
wpa2 psk aes
Jul 17 18:30:34 wpa2-key1 <- a0:88:b4:50:c0:84 b4:5d:50:e8:24:b4 - 117
Jul 17 18:30:34 wpa2-key2 -> a0:88:b4:50:c0:84 b4:5d:50:e8:24:b4 - 119
Jul 17 18:30:34 wpa2-key3 <- a0:88:b4:50:c0:84 b4:5d:50:e8:24:b4 - 151
Jul 17 18:30:34 wpa2-key4 -> a0:88:b4:50:c0:84 b4:5d:50:e8:24:b4 - 95
Jul 17 18:30:34 rad-acct-start -> a0:88:b4:50:c0:84 b4:5d:50:e8:24:b4/ClearPass - -
Jul 17 18:30:42 rad-acct-int-update -> a0:88:b4:50:c0:84 b4:5d:50:e8:24:b4 - -
b4:5d:50:c6:82:4a#

b4:5d:50:c6:82:4a# show ap mpskcache

PPSK Cache Table
-----
Client MAC      Key              Del  Expiry  Role          VLAN  ESSID          Seqno
IP
-----
-
a0:88:b4:50:c0:84 (6): b8 b0 5d 26 5e 62 ... No - Student-Devs 22 ArubaMPSK 22235
10.10.22.50
PPSK Cache Count:1
b4:5d:50:c6:82:4a#

```

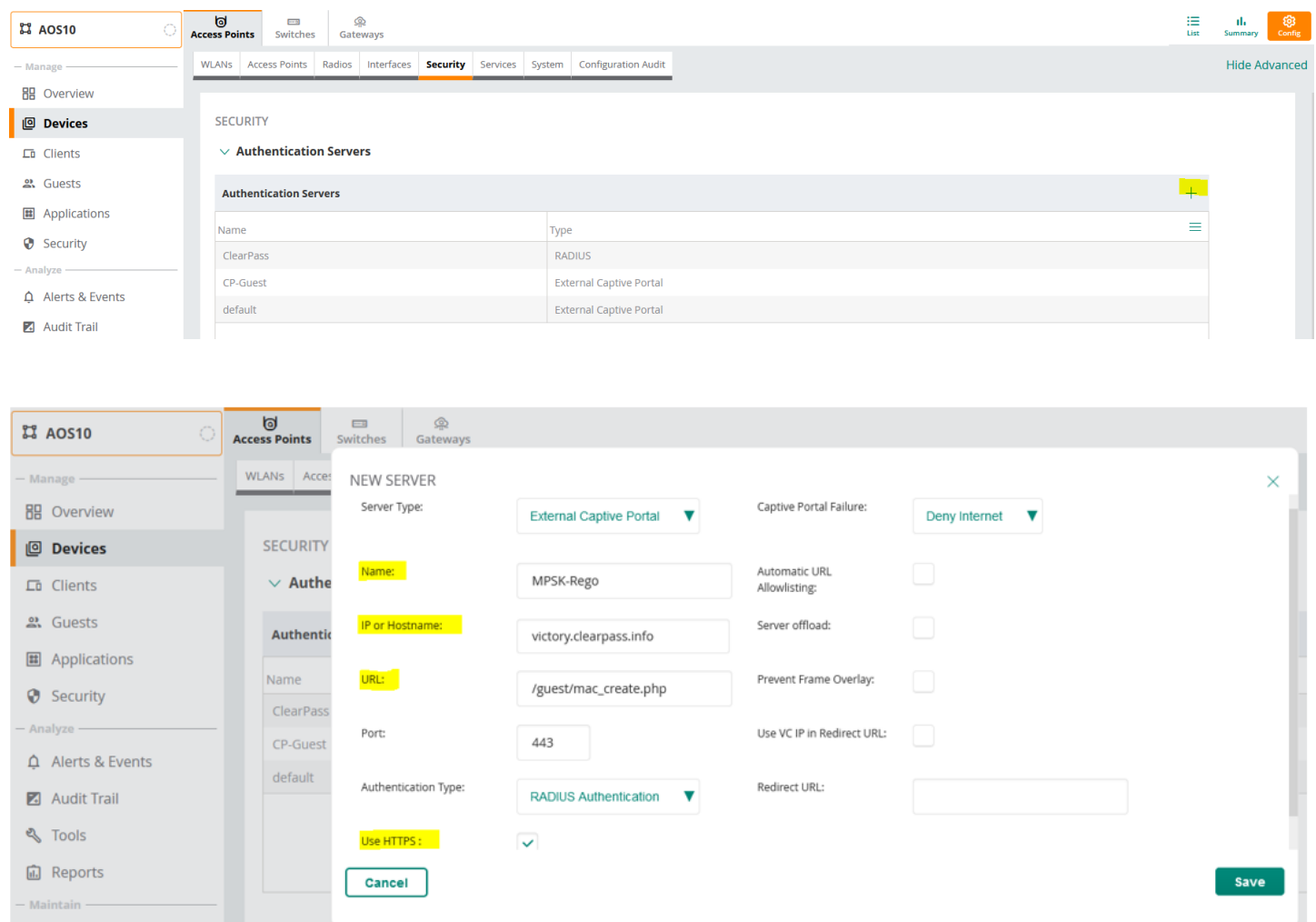
## 8 Pre-populating MAC address Workflow

In the previous workflow when the users who want to register their devices for MPSK, had to login to ClearPass Guest then they would be prompted for a MAC address of their device that they want to register. This could be problematic for the users since most of them may not even know what the MAC address is and where to get it.

An easier workflow would be to get the user login to ClearPass Guest with their device that needs registration, and we pre-populate the MAC address field with the MAC address of the device.

### 8.1 Aruba Central Configuration

For this workflow, we need to configure a Captive portal profile that redirects the user to Device Registration page. The external captive portal profile we have configured here is “MPSK-Rego” and URL is “/guest/mac\_create.php” as seen below.



The screenshot displays the Aruba Central configuration interface. On the left, a sidebar menu includes 'Manage' (Overview, Devices, Clients, Guests, Applications, Security, Alerts & Events, Audit Trail) and 'Analyze' (Tools, Reports, Maintain). The main panel is titled 'AOS10' and shows the 'Security' tab under 'Access Points'. The 'Authentication Servers' section is active, showing a table with three entries: 'ClearPass' (RADIUS), 'CP-Guest' (External Captive Portal), and 'default' (External Captive Portal). A 'NEW SERVER' modal is open, showing configuration for an 'External Captive Portal' server named 'MPSK-Rego'. The modal includes fields for 'Name', 'IP or Hostname' (victory.clearpass.info), 'URL' (/guest/mac\_create.php), 'Port' (443), 'Authentication Type' (RADIUS Authentication), 'Captive Portal Failure' (Deny Internet), 'Automatic URL Allowlisting' (unchecked), 'Server offload' (unchecked), 'Prevent Frame Overlay' (unchecked), 'Use VC IP in Redirect URL' (unchecked), and 'Redirect URL' (empty). The 'Use HTTPS' checkbox is checked. 'Cancel' and 'Save' buttons are at the bottom.

Name	Type
ClearPass	RADIUS
CP-Guest	External Captive Portal
default	External Captive Portal

Field	Value
Server Type	External Captive Portal
Name	MPSK-Rego
IP or Hostname	victory.clearpass.info
URL	/guest/mac_create.php
Port	443
Authentication Type	RADIUS Authentication
Captive Portal Failure	Deny Internet
Automatic URL Allowlisting	<input type="checkbox"/>
Server offload	<input type="checkbox"/>
Prevent Frame Overlay	<input type="checkbox"/>
Use VC IP in Redirect URL	<input type="checkbox"/>
Redirect URL	
Use HTTPS	<input checked="" type="checkbox"/>

Then we'll reference that in our Guest-MPSK-Rego WLAN.

AOS10

Access Points

Switches

Gateways

WLANs

Access Points

Radios

Interfaces

Security

Services

System

Configuration Audit

Hide Advanced

1 General

2 VLANs

3 Security

4 Access

5 Summary

Name (SSID):

Guest-MPSK-Rego

> Advanced Settings

Again, here you can make it tunnel mode as well, but we'll stick to bridge mode.

AOS10

Access Points

Switches

Gateways

WLANs

Access Points

Radios

Interfaces

Security

Services

System

Configuration Audit

Hide Advanced

1 General

2 VLANs

3 Security

4 Access

5 Summary

Traffic forwarding mode:

☒ Bridge

☐ Tunnel

☐ Mixed

Client VLAN Assignment:

☐ Static

☐ Dynamic

☒ Native VLAN

AOS10

Access Points

Switches

Gateways

WLANs

Access Points

Radios

Interfaces

Security

Services

System

Configuration Audit

Hide Advanced

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:

MPSK-Rego

Primary Server:

ClearPass

Secondary Server:

-- Select --

Encryption:

☐

Key Management:

Enhanced Open

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

Hide Advanced

CREATE A NEW NETWORK

1 General

2 VLANs

3 Security

4 Access

5 Summary

Access rules

Role Based

Network Based

Unrestricted

ROLE

Guest-MPSK-Rego

ArubaMPSK

CP-Guest

Contractor

Employee

Executive-Bridge

IoT1

ACCESS RULES FOR SELECTED ROLES

Allow any on server 192.168.1.95/255.2...

+ Add Role

17 Role(s)

+ Add Rule

1 Rule(s)

ROLE ASSIGNMENT RULES

Default role: Guest-MPSK-Rego

+ ADD ROLE ASSIGNMENT

1 Role(s)

ASSIGN PRE-AUTHENTICATION ROLE:

☒

Guest-MPSK-Rego

## 8.2 ClearPass Guest

We just need to ensure that MAC detect is enabled as shown below. You need to go to Administrator-> Plugin manager and enabled it and save the changes.

aruba

Guest

Devices

Onboard

Configuration

Administration

API Services

API Clients

API Explorer

SOAP Web Services

Aruba Integrations

Controllers

AirGroup Configurati

MPSK Configuration

Check Security

Data Retention

Extensions

Import Configuration

Operator Logins

Plugin Manager

Support

ClearPass Guest

Menu

Hotspot Manager

Enable visitors to self-provision their own network accounts.

6.9.6

Enabled

Configuration

About

LDAP Sponsor Lookup

Performs an LDAP lookup of a particular field to continue the registration process.

6.9.6

Enabled

Configuration

About

MAC Authentication

Create and manage MAC-based device authentication for a network.

6.9.6

Enabled

Configuration

About

Pages

Provides customizable web pages.

6.9.6

Enabled

Configuration

About

Pass Services

Provides services to create, download and manage passes.

6.9.6

Enabled

Configuration

About

Platform Services

Provides platform support and administration functions.

6.9.6

Enabled

Configuration

About

SMS Services

Send visitor account receipts to mobile phones as SMS messages.

6.9.6

Enabled

Configuration

About

**aruba** ClearPass Guest Menu

Home » Administration » Plugin Manager

## MAC Authentication 6.9.6-131326 Configuration

Set the configuration options for MAC Authentication 6.9.6-131326.

**Guest**

**Devices**

**Onboard**

**Configuration**

**Administration**

API Services

API Clients

API Explorer

SOAP Web Services

Aruba Integrations

Controllers

AirGroup Configuration

MPSK Configuration

Check Security

Data Retention

Extensions

Import Configuration

Operator Logins

**Plugin Manager**

Support

### Configure MAC Authentication 6.9.6-131326

☒ Allow users to be detected via their MAC address  
Provides access to user configuration for headers, footers, etc on login and registration pages. Please note that a passed MAC can be easily changed by the user, so personal details should not be displayed. Requires a vendor that passed the mac as part of the redirection.

**\* MAC Detect:**

Device Filter:

☒ Manage Accounts

☒ Manage Multiple Accounts  
Select which views should not display devices (user accounts with the 'mac\_auth' field set).

### Aruba MPSK Options

\* Random MPSK Method: Random lowercase letters excluding vowels  
The method used to generate a random device MPSK.

\* Random Password Length: 8  
Number of characters to include in randomly-generated pre-shared keys.

Display: ☐ View device MPSKs  
If selected, device MPSK may be displayed in the list of devices. This is only possible if operators have the View MPSK privilege.

**Save Configuration**

\* required field

## 8.3 Testing the new workflow

So now the user with the device that needs to be registered for MPSK, connects to “Guest-MPSK-Rego” SSID it gets redirected to “/guest/mac\_create.php”

**aruba** Central

Search or ask Aruba

**AOS10**

Manage

Overview

Devices

**Clients**

Guests

Applications

Security

**CLIENTS** ALL

4.57 GB ( 136.09 MB | 4.44 GB )

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

Client Name	Status	IP Address	VLAN	Connected To	SSID/...	AP Role	Health	MAC Address	Key Manag
AriyaP	Connecting	10.10.55.12	1	b4:5d:50:c6:82:4a	Guest-MPSK-R...	Guest-MPSK-Rego		a0:88:b4:50:c0:84	NONE

As before the user is prompted for credentials that gets authenticated against AD.

**aruba** ClearPass Guest

### Operator Login

Username: student1

Password: ••••••

**Log In**

After successful authentication the user get redirected to Create\_Device page.

**aruba** ClearPass Guest

✓ Last successful login from 192.168.1.121 on Saturday, 17 July 2021, 4:48 PM

❗ No failed attempts since last successful login

New device being created by student1.

### Create New Device

\* MAC Address: a0:88:b4:50:c0:84  
MAC address of the device.

Sponsor's Email: ariyap@hpe.com  
Email of the person sponsoring this account.

\* Device Name: MyIoT  
Name of the device.

AirGroup: ☐ Enable AirGroup  
AirGroup uses device ownership and location information to limit the printers and Apple TVs available to network users.

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

Account Expiration: 1 week from now  
Select an option for changing the expiration time of this account.

\* Account Role: Student-Devs  
Role to assign to this account.

Notes:

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

**Create**

\* required field

Note that the MAC address gets automatically populated. Once the user registers the device as before, they see the receipt and gets an email address with the MPSK password.

**Finished Creating Device**

The device was successfully created.

Create New Device Receipt	
MAC Address:	A0-88-B4-50-C0-84
Account Status:	Active
Account Activation:	Tuesday, 20 July 2021, 11:56 AM
Account Expiration:	Account will expire at Tuesday, 27 July 2021, 11:56 AM
Account Role:	Student-Devs
Registered By:	student1
Wi-Fi Password:	jfcnwxmh

Open print window using template...

[Back to devices](#)

[Back to main](#)

Here is the email that will also receive

To: Parsamanesh, Ariya

Tue 20/07/2021 11:56 AM

If there are problems with how this message is displayed, click here to view it in a web browser.

**Aruba ClearPass Guest**

**Your device has been successfully registered and can now be connected.**

**Wi-Fi Network: Aruba**

**Device Name: MyIoT**

**MAC Address: A0-88-B4-50-C0-84**

**Device Wi-Fi Instructions:**

Make sure your wireless adapter A0-88-B4-50-C0-84 is set to dynamically obtain an IP address

Connect to the wireless network: **Aruba**

Wi-Fi password: **jfcnwxmh**

Device expires: Tuesday, July 27, 2021 11:56

© Copyright 2021 Aruba, a Hewlett Packard Enterprise company.

Once they know the password, they'll connect to the MPSK SSID as shown below.

**CLIENTS** | ALL

4.57 GB ( @ 136.09 MB | @ 4.44 GB )

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

Client Name	Status	IP Address	VLAN	Connected To	SSID/...	AP Role	Health	MAC Address	Key Manag
student1	Connected	10.10.22.50	22	b4:5d:50:c6:82:4a	ArubaMPSK	Student-Devs		a0:88:b4:50:c0:84	WPA2_PSK

You should note that I have assumed that the standard Guest authentication services are already configured on ClearPass Policy Manager.