# **1** Table of Contents

## **Table of Contents**

1	Table of Contents	1
2	1.1 Revision History Multiple PSK Aruba Instant	.1
3	<ul> <li>2.1 Things you need</li> <li>2.2 Overall Workflow</li> <li>Instant AP Configuration</li> </ul>	.2 .2 .3
4	<ul> <li>3.1 Aruba Instant ClearPass Configuration</li> <li>3.2 Aruba Instant MPSK Configuration</li> <li>ClearPass Configuration</li> </ul>	.3 4 6
5	<ul> <li>4.1 RADIUS Dictionary</li></ul>	.6 .8 .9 .9 .9 10 12
6	<ul> <li>5.1 MPSK Configuration</li></ul>	13 14 15 18
7	<ul> <li>6.1 Device Registration</li> <li>6.2 ClearPass Access Tracker Operator Login</li> <li>6.3 Aruba Instant AP</li> <li>6.4 ClearPass Access Tracker MPSK Authentication</li> <li>6.5 Packet Capture</li> <li>Pre-populating MAC address Workflow</li> </ul>	18 20 23 25 26 28
8	<ul> <li>7.1 Aruba Instant Configuration</li> <li>7.2 ClearPass Guest</li> <li>7.3 Testing the new workflow</li> <li>Prepopulating MAC address with Self Registration</li> </ul>	28 29 30 33
	<ul> <li>8.1 Aruba Instant Configuration</li></ul>	33 33 44 45

# 1.1 Revision History

DATE	VERSION	EDITOR	CHANGES
28 April 2019	0.1	Ariya Parsamanesh	Initial creation
05 April 2019	0.2	Ariya Parsamanesh	Prepopulated MAC address workflow
17 Jul 2019	0.3	Ariya Parsamanesh	Added the Instant 8.5.0.1

# 2 Multiple PSK Aruba Instant

All the WPA2 Pre Shared Key (PSK) based Wireless LAN consist of a single passphrase. This passphrase is used by all the clients that connect to that WLAN in which its authentication is based on PSK.

Aruba Instant version 8.5.0.1 now 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. This feature requires Aruba ClearPass 6.8.x to be the authentication server.

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



### 2.1 Things you need

- Two IAPs Aruba Instant version 8.5.0.1 or later
- Aruba ClearPass version 6.8.x or later
- A Layer three switch and some WiFi clients

### 2.2 Overall Workflow

The overall workflow with MPSK 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 Instant AP Configuration**

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. Also, ensure that the RADIUS server configured for the WLAN SSID profile is ClearPass Policy Manager and lastly RADIUS accounting will be added in the upcoming release.

### 3.1 Aruba Instant ClearPass Configuration

First we need to configure ClearPass as the authentication server.



# 3.2 Aruba Instant MPSK Configuration

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

a		RTUAL InstantVC
<u>lılı</u>	Dashboard	Edit network ArubaMPSK         1         Basic         2         VLAN         3         Security         4         Access
	Overview	Name & Usage
	Networks	Name ArubaMPSK
	Access Points	Type Wireless 🗸
	Clients	Primary usage Employee 🗸
۵	Configuration	
	Networks	
<u></u>	Dashboard	Edit network ArubaMPSK         1         Basic         2         VLAN         3         Security         4         Access
	Overview	Client IP & VLAN Assignment
	Networks	Client IP assignment Virtual Controller managed
	Access Points	Network assigned
	Clients	Client VLAN assignment   Default  Static
\$	Configuration	
	Networks	
<u></u>	Dashboard	Edit network ArubaMPSK         1         Basic         2         VLAN         3         Security         4         Access
	Overview	Security Level
	Networks	Security Level Personal V
	Access Points	Key management MPSK-AES V
	Clients	Authentication server 1 ClearPass V Z +
		Authentication server 2 Select Server 🗸 🕂
÷	Configuration	Enforce DHCP
	Networks	Fast Roaming
	Access Points	802.11r
	System	802.11k
	RF	802.11v
	Security	



After the successful MPSK authentication, the MPSK passphase is cached with in the Instant Cluster and shared among the IAPs with in it. We also need to configure the right Security user role.



# 4 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.

### 4.1 RADIUS Dictionary

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

aruba	ClearPass Policy Manager									
Dashboard	📀 Last s	uccessful login from 192.168.1.	135 on Apr 26, 2019	15:42:48 AEST						
Monitoring O	No fail	ed attempts since last successf	ul login							
🖗 Configuration 🔹 💿	Administration » Dictionaries » RADIUS									
Administration 📀	RADIUS Dictionaries									
ClearPass Portal     Sers and Privileges     Modmin Users     Modmin Users	This pag	e allows admins to view the list	of RADIUS dictionari	ies, view attribute	es and enable or exp Go Clear Filter	port dictionaries.				
Server Manager	#	Vendor Name ⊾		Vend	or ID	Vendor	r Prefi			
- P Server Configuration	1.	Aruba		1482	3	Aruba				
Log Configuration     PLocal Shared Folders										
External Servers	Vene	dor Name: Aruba (	14823)							
- A External Accounts	17.	Aruba-Calea-Server-Ip	41	IPv4Address	in out					
- 🔓 Certificates	18.	Aruba-Captive-Portal-URL	43	String	in out					
- III Dictionaries	19.	Aruba-Command-String	46	String	in out					
- 🖉 RADIUS	20.	Aruba-Device-Type	12	String	in out					
– J RADIUS Dynamic Authorization Te	21.	Aruba-Essid-Name	5	String	in out					
- Jacacs + Services	22.	Aruba-Framed-IPv6-Address	11	String	in out					
- Jevice Fingerprints	23.	Aruba-Location-Id	6	String	in out					
- Dictionary Attributes	24.	Aruba-MPSK-Passphrase	44	OctetArray	in out					
- JP Applications	25.	Aruba-Mdps-Device-Iccid	17	String	in out					
Context Server Actions	26.	Aruba-Mdps-Device-Imei	16	String	in out					
Agents and Software Undates	27	Aruba-Mdne-Device-Name	10	String	in out	×				
- DonGuard Settings				Disable	Export Close	e				

## 4.2 Service Template

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

aruba	ClearPass Policy Manager	Menu
Dashboard O Monitoring O Configuration O	Configuration » Service Templates & Wizards Service Templates & Wizards • To configure service and related policies using the full wizard, click here.	
Service Templates & Wizards     Services	• Or filter by <b>service templates</b> for common use cases: All Templates	
<ul> <li>➡ Q Identity</li> <li>➡ Posture</li> </ul>	802.1X Wired To authenticate users to any wired network via 802.1X.	
Senforcement     Hetwork     Arrow Devices	802.1X Wireless           To authenticate users to any wireless network via 802.1X.	
- Device Groups - Proxy Targets - Event Sources	Aruba 802.1X Wireless To authenticate users to an Aruba wireless network via 802.1X.	
– 🙀 Network Scan – 🏠 Policy Simulation	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 dients 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.

Configuration » Service Templates & Wizards

#### Service Templates - Aruba Wireless with MPSK

General	Wireless Network Settings	Device Roles	Enforcement Details						
Name Prefix	*: MPSK								
	Description								
For wirele Device Re	ess devices that do not supp egistration. This service type	ort strong 802.1X handles the devi	authentication, Aruba MF ce authentication from an	SK allows each device to be as Aruba Mobility Controller or In	ssigned a uniquistant AP.	ue pre-shared key	/ during		
Back to S	ervice Templates & Wiza	rds		Delete	Next $\rightarrow$	Add Service	Cancel		
General	Wireless Network Settings	Device Poles	Enforcement Details				I		
Select a wi	reless controller from the	list. or create a	new one						
Select Wirel	ess Controller:	InstantVC	~						
Wireless Co	ntroller Name:	InstantVC							
Controller I	Address:	192.168.1.10							
Vendor Nam	ie:	Aruba	~						
RADIUS Sha	ared Secret:	•••••	D						
Enable RAD	IUS Dynamic Authorization:								
Dynamic Au	thorization Port:	3799							
SSID Name	:	ArubaMPSK		(Enter single or multiple cor	mma separateo	d SSIDs)			
Enable Rads	Sec:								

#### Do not select RadSec as it is not supported for MPSK.

General	Wireles	s Network Settings	Device Roles	Enforcement Details						
Define logic	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 <u>*</u> :	Students-Devs	<b>*</b>							
Device Role	2:		*							
Device Role	3:		*							
Device Role	4:		*							
Device Role	5:		T							

General Wireless Network Settings Device Roles Enforcement Details

Create a New Enforcement Po	reate a New Enforcement Policy					
Device Role	Aruba Role					
If Students-Devs	then assign Role Students-Devs					
If	then assign Role					
If	then assign Role					
If	then assign Role					
If	then assign Role					
Default MPSK ::	•••••					
Default Aruba User Role*:	Employee					
Back to Service Templates 8	& Wizards					

The default MPSK that we have configured is aruba123. You don't have to use this default MPSK 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 MPSK for the devices that fall through the logic to get contained using captive portal and restricted ACL.

ClearPass Policy Manager					
Configuration » Services Services		♣ Add ♣ Import ♣ Export All			
	<ul> <li>Added 2 Enforcement Profile(s)</li> <li>Added 1 Enforcement Policies</li> <li>Added 1 Role Mapping Policies</li> <li>Added 1 service(s)</li> </ul>				
This page shows the current list and order of services that ClearPass follows during authentication and authorization.					

### 4.3 Enforcement Profiles

Here are the two enforcement profiles that were created.

aruba				Menu <b>=</b>				
Dashboard O	Config	uration	» Enforcement » Profiles					
Monitoring O	Enfo	forcement Profiles						🚽 Add
😤 Configuration 📀	tion 📀							Export All
— Service Templates & Wizards	Service Templates & Wizards Each enforcement policy contains enforcement profiles that match conditions (role, posture, and time) to actions (enforcement profiles).						es).	
- 🛱 Services								
- 🗣 Authentication	Filter:	Name	<ul> <li>✓ contains </li> <li>✓ mpsk</li> </ul>		+	Go Clear Filter	Show 2	0 v records
- Lentity	#		Name 🛦	Туре		Description		
⊡-	1.		MPSK Aruba Wireless with MPSK Default Profile	RADIUS				
- Policies	2.		[Registered Device MPSK]	RADIUS		Returns a device's assigned MPSK that was generate Registration	d automatically	during Device
- Profiles	Showi	ng 1-2 (	of 2				Сору Ехро	Delete

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

Summary	Profile	Attributes		
Profile:				
Name:		MPSK Aru	a V	Vireless with MPSK Default Profile
Description:				
Type:		RADIUS		
Action:		Accept		
Device Group	List:	-		
Attributes:				
Туре				Name

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

#### Enforcement Profiles - Aruba User Role – Students-Devs

Summar	/ Profile	Attributes						
Profile:								
Name:		Aruba Use	r Role - Students-Devs					
Description	n:							
Type:		RADIUS						
Action:		Accept	Accept					
Device Gro	up List:	-						
Attributes	Attributes:							
Тур	e		Name		Value			
1. Radi	us:Aruba		Aruba-User-Role	=	Students-Devs			

#### **Enforcement Profiles - [Registered Device MPSK]**

This is a default profile.

Su	mmary	Profile	Attributes							
Prof	ïle:									
Name:			[Register	[Registered Device MPSK]						
Description: Returns a device's assigned MPSK that was generated automatically during Device Registration										
Туре:			RADIUS	RADIUS						
Actio	on:		Accept							
Dev	ice Group	List:	-							
Attr	ibutes:									
	Туре			Name		Value				
1.	Radius:	Aruba		Aruba-MPSK-Passphrase	=	Device's Assigned MPSK				

### 4.4 Enforcement Policy

This is the enforcement policy that got created.

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

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

### 4.5 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

Summa	ary	Policy	Mapping Rules		
Policy:					
Policy Name:		MPSK Aruba V	Wireless with MPSK Role Map		
Descripti	ion:				
Default P	Role:		[Other]		
Mapping	g Rule:	s:			
Rules Ev	aluatio	n Algorit	hm: Evaluate all		
Con	dition	s			
1. (Aut	thorizat	tion:[Gu	est Device Reposito	tory]:Device Role ID EQUALS 3008)	

# 4.6 ClearPass Service

And here is the complete serviced that was configured.

#### Services



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

Filter:	lame		✓ contains ✓	Go Clear Filter		Show 20 ~ records
#		Order 🔺	Name	Туре	Template	Status
1.		1	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	0
2.		2	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement ( Generic )	<b>S</b>
3.		3	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	<b>S</b>
4.		4	[Guest Operator Logins]	Application	Aruba Application Authentication	$\bigcirc$
5.		5	[Insight Operator Logins]	Application	Aruba Application Authentication	<b>S</b>
6.		6	Lab Aruba 802.1X Wireless	RADIUS	Aruba 802.1X Wireless	$\bigcirc$
7.		7	Ariya WiredAOS-S Dot1x	RADIUS	802.1X Wired	<b>O</b>
8.		8	Ariya Wired-AOS-S MAC Auth	RADIUS	MAC Authentication	0
9.		9	Ariya Wired-AOS-S MAC Auth-DUR	RADIUS	MAC Authentication	<b>S</b>
10.		10	Ariya Wired-AOS-S GuestWebAuth	WEBAUTH	Web-based Authentication	0
11.		11	Ariya Wired-AOS-S GuestWebAuth-DUR	WEBAUTH	Web-based Authentication	<b>S</b>
12.		12	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	<b>S</b>
13.		13	MPSK Aruba Wireless with MPSK	RADIUS	MAC Authentication	<b>O</b>
Showing	11-13	of 13			Reorder	Copy Export Delete

Su	mmary	Service	Authentication	Roles	Enforcement						
Nam	e:		MPSK Aruba Wire	less with M	MPSK						
Desc	ription:		To authentica MPSK.	te de <b>v</b> ic	es using an Ar:	uba					
Type	:		MAC Authentica	tion							
Stat	us:		Enabled								
Monitor Mode:		Enable to mo	Fnable to monitor network access without enforcement								
More	Options:		Authorization	Aud	lit End-hosts	Profile Endpoints	Accounting Proxy				
						Servi	ce Rule				
Matc	hes 🔿 Al	NY or 🔍 Al	L of the following	conditio	ns:						
	Туре			Na	ame		Operator		Value		
1.	Radius:I	IETF		NA	S-Port-Type		EQUALS		Wireless-802.11 (19)		Ť
2.	Radius:I	IETF		Se	rvice-Type		EQUALS		Call-Check (10)		Ť
3.	Connect	ion		Cli	ent-Mac-Address		EQUALS		%{Radius:IETF:User-Name}	Ē	Ť
4.	Connect	ion		SS	SID		EQUALS		ArubaMPSK		Ť
5.	Click to	add									
Su	mmary	Service	Authentication	Poles	Enforcement						
30		Service	Authentication	Roles	Emorcement	7					
Auth	entication	Methods:	[Allow All MAC A	UTH]	^	Move Up ↑			Add New Auther	ntication M	lethod
						Move Down ↓					
						Remove					
						View Details					
						Modify					
			Select to Add		~	]					
Auth	ontication	Sourcos	Found Davies D		[L] COL D.D.]	]			Add Now Author	akieskies C	
Auti	entication	i Sources.	[Guest Device Re	epository	[LOCAI SQL DB]	Move Up ↑			Add New Authe	nucation a	source
						Move Down ↓					
						Remove					
						View Details					
					~	Modify					
			Select to Add			~					
Strip	Usernam	e Rules:	Enable to spe	ecify a co	mma-separated	list of rules to strip u	isername prefixes o	or suffixes			
Su	mmary	Service	Authentication	Roles	Enforcement						
Role	Mapping	Policy:	MPSK Aruba Win	eless with	MPSK Role Map	✓ Modify			Add New Ro	le Mapping	g Policy
						Role Mappir	g Policy Details				
Des	cription:										
Defa	ult Role:		[Other]								
Rule	s Evaluati	ion Algorithn	n: evaluate-all								
	Conditi	ons					Role				
1.	(Authori	ization:[Gue	st Device Reposite	ory]:Devi	ice Role ID EQUA	ALS 3008)	Studer	nts-Devs			
SI	Immary	Service	Authentication	Roles	Enforcement						
Use	Cached Re	esults:		oles and	Posture attribute	es from previous sess	ions				
Enfo	rcement F	Policy:	MPSK Aruba Wire	less with	MPSK Enforcement	Policy × Modify			Add New En	forcement	Policy
						Enforcemen	t Policy Details				
Des	cription:										
Def	ault Profile	:	MPSK Aruba W	ireless w	ith MPSK Default	Profile					
Rule	es Evaluati	ion Algorithn	n: first-applicable	2.200 1							
	Conditi	ione	FF				Enfor	rcomont Profiles			
	(Tips:F	Role EOUAL	S Students-Devs				Enfor	reement promes			
1.	AND AND	(Authorizat	ion:[Guest Device	Reposito Reposito	ory]:Device Acco	unt Active EQUALS ( ( EXISTS )	true) Aruba Spons	a User Role - Studen sor Name - RADIUS	ts-Devs, [Registered Device MPSK], [ User-Name]	Return Dev	vice

# 4.7 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.

Sum	mary	Service	Authentication	Roles	Enforcement				
Name:	:		Guest Operator	Logins					
Descri	ption:		Authenticati application	on servio	ce for Guest	***			
Type: Aruba Application Authentication									
Status: Enabled									
Monito	r Mode:		Enable to m	onitor ne	twork access wit	thout enforcement			
More C	Options:		Authorizatio	วท					
						Servio	e Rule		
Matche	es O Al	NY or 🖲 A	LL of the followin	ig conditio	ons:				
1	l ype Applicati	le n		Nan	ne		Operator	Value	Bar an
1. 7	Authonti	ication		Type				SSO	eg u Ba m
3. (	Click to a	add		Type	,		NOT_EQUALS	550	4 <u>5</u> w
Cum		Comico	Authontication	Poloc	Enforcomont				
Authentication Sources:		Sources:	AriyaAD [Active [Local User Re [Admin User R	e Directory] pository] [L epository] [	, ocal SQL DB] Local SQL DB]	Move Up ↑ Move Down ↓ Remove View Details Modify			Add New Authentication Source
			Select to Add	1		~			
Strip l	Jsernam	ne Rules:	Enable to s	pecify a c	omma-separated	d list of rules to str	ip username prefixes o	r suffixes	
Sum	mary	Service	Authentication	Roles	Enforcement				
Role M	1apping	Policy:	Select			~ Modify			Add New Role Mapping Policy
						Role Mappir	ng Policy Details		
Descri	iption:		-						
Defau	It Role:		-						
Rules	Evaluat	ion Algorith	im: -						
	Conditi	ions		_			Role		
Sum	mary	Service	Authentication	Roles	Enforcement				
Use Ca	ached R	esults:	Use cached	l Roles an	d Posture attrib	utes from previous	s sessions		
Enforc	ement F	Policy:	Guest Operato	or Logins w	ith MPSK	✓ Modify			Add New Enforcement Policy
						Enforcemen	t Policy Details		
Descri			Enforcement	t policy	ntrolling access	to Guest applicati	on		
	ption:			r policy co	access				
Defaul	ption: It Profile	e:	[Deny Applic	ation Acc	ess Profile]				
Defaul Rules	ption: It Profile Evaluati	e: ion Algorith	[Deny Applic m: first-applical	c policy cc cation Acc ple	ess Profile]				
Defaul Rules	ption: It Profile Evaluati Conditio	e: ion Algorith <b>ons</b>	[Deny Application ]	cation Acc	æss Profile]		Enforce	ment Profiles	
Defaul Rules 1.	ption: It Profile Evaluati <b>Conditi</b> (Authe AND	e: ion Algorith ons entication:S (Authoriza	[Deny Applicat m: first-applicat ource EQUALS of tion:AriyaAD:me	ation Acc ble AriyaAD)	contains deces	dent)	Enforce MPSK-Op	<b>ment Profiles</b> perator	
Defaul Rules 1. 2.	ption: It Profile Evaluati Conditio (Authe AND (Tips:F AND	e: ion Algorith ons entication:S (Authoriza Role <i>EQUAL</i> (Authentic	[Deny Applicat m: first-applicat ource EQUALS i tion:AriyaAD:me .S [User Authen iation:Source EQ	ation Acc ble AriyaAD) mberOf ( ticated]) 20ALS [Lu	contains decess contains stud	dent) itory])	Enforce MPSK-Op [Operato	<b>ment Profiles</b> berator or Login - Local Users]	
Defaul Rules 1. 2. 3.	ption: It Profile Evaluati (Authe AND (Tips:F AND (Tips:F AND	e: ion Algorith ons entication: S (Authoriza Role EQUAL (Authontic (Authontic	[Deny Application: First-application: AriyaAD:metation: Source EQUALS of User Authentiation: Source EC	AriyaAD) mberOf ( ticated]) 20ALS [Lu ticated])	CONTAINS Stud	itory])	Enforce MPSK-Op [Operato [Operato	ment Profiles perator or Login - Local Users] or Login - Admin Users]	

#### **Enforcement Profiles - MPSK-Operator**

Su	immary	Profile	Attributes				
Prof	file:						
Name: MPSK-Operator							
Description: Enforcement profile for MPSK operator logins							
Туре	Type: Application						
Actio	on:		Accept				
Devi	ice Group	List:	-				
Attri	ibutes:						
Attribute Name Attribute Value							
1.	admin_privileges = Students						
2.	ClearPa	ss:User-E	mail-Address		=	%{Authorizat	tion:AriyaAD: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 use so the MPSK credentials can be emailed to the user.

# 4.8 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

Dashboard	Administration » External						
Monitoring •	Messaging	Messaging					
🚓 Configuration 🔹 🔹	ClearPass Messaging Setu	p guides you through configurati	on of the SMTP server for email and S	GMS notifications.			
Administration 📀	SMTP Server						
- DearPass Portal	SMTP Settings						
Admin Users	Server Name:	smtp.gmail.com		Connection Security:	StartTLS		
- Admin Privileges	Username:	and the second	]	Port:	587		
- 📲 Server Manager	Password:		]	Connection Timeout:	30 seconds		
- Jerver Configuration	Verify Password:	•••••	]				
- Jeg Configuration	Default From Address:	ariyap@aruba.com	]				
- Jocal Shared Folders							
- Coensing				Send Test	Email Send Test SMS Reset Save		
SNMP Trap Receivers	1						
- Jossi Syslog Targets							
- Josepheren Syslog Export Filters							
- A Messaging Setup							
- Definition Context Servers							
- JP File Backup Servers							
- PEXTERNAL ACCOUNTS							

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

# **5 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.

## 5.1 MPSK Configuration

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



In most of the cases "Allow generate unique WiFi passwords" is used, Here 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.

aruba		ClearPass Guest
Guest O	Home » Administration » Arub	a Integrations » MPSK Configuration
Devices 0	Configure MPSK	
Onboard O	-	
🔦 Configuration 🛛 📀	Use this form to make change	s to the configuration options for Aruba MPSK.
Administration		Configure MPSK
API Services	Auto-Configuration	
→ API Clients → API Explorer → SOAP Web Services → *** Controllers	* 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
Controllers		An Aruba MPSK will be generated for each new device that is registered. Forms • mac_create: Add field mpsk_enable • mac_create: Add field auto_send_smtp • mac_create: Add field auto_send_smtp • mac_ereate: Add field mpsk_enable • mac_edit: Add field mpsk_enable • mac_edit: Add field mpsk_refresh • mac_edit: Add field mpsk_enable • mactrac_create: Add field mpsk_enable • mactrac_create: Add field smtp_smail • mactrac_create: Add field smtp_smail • mactrac_create: Add field smtp_email_field • mactrac_edit: Add field mpsk_enable • mactrac_edit: Add field mpsk_enable • mactrac_edit: Add field mpsk_enable • mactrac_edit: Add field mpsk_refresh • mactrac_edit: Add field mpsk_has_key
		<ul> <li>mactrac_edit: Add field smtp_auto_send_field</li> <li>Device Wi-Fi passwords are sent via email receipts and valid SMTP server settings must be provided.</li> </ul>
	Password Options	
	* Random MPSK Method:	Random lowercase letters excluding vowels The method used to generate a random device MPSK.
	* Random Password Length:	8 Sumber of characters to include in randomly-generated pre-shared keys.
	* Password Complexity:	No password complexity requirement  V Password complexity to enforce for manually-entered MPSK.
	MPSK Example:	gwclrngx C Generate
		ave Configuration

Menu 📃

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

## 5.2 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.

ClearPass Guest Home » Administration » Operator Logins » Profiles Edit Operator Profile (Students) Use this form to make changes to the operator profile Students. **Operator Profile Editor** Students \* Name: a name for this operator profile. Description: Comments or descriptive text about the operator profile Access These options control what operators with this profile are permitted to do. Allow operator logins Enabled: If unchecked, operators with this profile will not be able to log in. Operator Privileges -No Access 鰠 Administrator 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 elect operator permissions for API access and manager 🖤 Aruba Integrations No Access Select operator permissions for access to Aruba integrations Custom... 🗊 Devices 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 No Access O Read Only 📩 Export Devices Operators with this privilege may export a list of devices ● No Access ○ Read Only ○ Full 🚵 Import Devices Operators with this privilege may create new devices from a data sou 📩 Manage Devices ○ No Access ○ Read Only ● Full Operators with this privilege may view and manage individual devices 覺 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 Privileges: Select operator permissions for IP phone administration and management tasks. 🗐 Onboard No Access Select operator permissions for managing Onboard device provisioning. 駒 Operator Logins No Access Select permissions for managing local operator logins 🕼 Pass Services No Access elect operator permissions for managing digital passes No Access i Platform Select operator permissions for platform administration tasks No Access 💿 Policy Manager  $\sim$ Select operator permissions for Policy Manager SMS Services No Access elect 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 O No Access O Read Only ● Full

	Support Services No Access								
	Select operator permissions for access to support services.								
	Select operator permissions for tasks related to translation								
	Show descriptions								
	Select the privileges that will be granted to this operator login.								
	Name								
	🗹 💿 ClearPass Policy Manager								
	Contractor]								
	Guest]								
User Roles:	[Employee]								
	Students								
	Students-Devs								
	10 rows per page								
	Select the visitor account roles that these operators are permitted to use								
	Seed the vision account roles that these operators are permitted to use.								
* Operator Filter:	No operator filter								
operator rater.	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.								
	0 🔹								
Account Limit:	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:	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								

## 5.3 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.

aruba	ClearPass Guest						
💐 Guest 🛛 🛛 🛛	Home » Configuration » Pages » Forms						
🚺 Devices 🔹 💿	Customize Forr	m Fields (mac_create)					
📳 Onboard 🛛 💿		· _ /					
🔦 Configuration 💿							
– 😻 Authentication	Use this list view to m	odify the fields of the form <b>mac_c</b>	create.				
🖅 🌝 Content Manager	1 Quick Help			Preview Form			
– 🕵 Guest Manager	🛆 Rank	Field	Туре	Label	Description		
	1	enabled	dropdown	Account Status:	Select an option for changing the status of this account.		
- 🌆 Fields	5	mac_auth	hidden	Is Device:			
- 🌆 Forms	5.1	mac	text	MAC Address:	MAC address of the device.		
- III List Views	10	sponsor_name	text	Sponsor's Name:	Name of the person sponsoring this account.		
- A Web Logins	10.1	sponsor_email	text	Sponsor's Email:	Email of the person sponsoring this account.		
🤤 Web Pages	20	visitor_name	text	Device Name:	Name of the device.		
∃- 🔂 Receipts	25	visitor_phone	phone	Phone Number:	The guest's phone number.		
	30	visitor_company	text	Company Name:	Company name of the guest.		
Translations	35	airgroup_device_type	dropdown	Device Type:	Select the type of your device.		
- 💛 Assistant	40	mpsk_enable	hidden	Wi-Fi Password:			
Language Packs	40.2	auto_send_smtp	hidden	Auto Email:			
Field Customizations	40.30000000000004	smtp_email_field	hidden	Email Field:			
- ustomizations					AirGroup uses device ownership and		

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:	sponsor_email ~					
Tield Mallie.	Select the field definition to attach to the form.					
Form Display Pr These properties control	Form Display Properties These properties control the user interface displayed for this field.					
Field:	Enable this field When checked, the field will be included as part of the form.					
* Rank:	10.1 Number indicating the relative ordering of user interface fields, which are displayed in order of increasing rank.					
* User Interface:	Text field The kind of user interface element to use when entering or editing this field.					
Label:	Sponsor's Email: Label for this field to display on the form.					
Description:	Email of the person sponsoring this account. Descriptive text for this field, displayed with the user-interface element.					
CSS Class:	Optional CSS class name to apply to this form field.					
CSS Style:	width: 240px; Optional CSS style text to apply to this form field.					
Placeholder:	Prompt text to display in the user interface element. Requires a HTML 5 capable browser.					
Label After:	Text to display after the user interface element.					
Label After (HTML):						
Form Validation	Properties ol how the value of this field is checked.					
Field Required:	Field value must be supplied Select this option if the field cannot be omitted or left blank.					
Initial Value:	array ( 'generator' => 'GeneratorFromSession', 'generator_ar Value to initialize this field with when the form is first displayed.					
* Validator:	IsValidEmail  The function used to validate the contents of a field.					
Validator Param:	(None) Optional name of field whose value will be supplied as the argument to a validator.					
Validator Argument:	array ( 'allow' => array ( Optional value to supply as the argument to a validator.					
Validation Error:	Please enter a valid email address. The error message to display if the field's value fails validation and the validator does not return an error message directly.					
Advanced Proper These properties control	erties ol conversion, display and dynamic behaviours.					
Advanced:	Show advanced properties					
Type Error:	The error message to display if the field's value is not supplied, has an incorrect type, or if conversion fails.					
	Save Changes					

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.

# 6 Testing

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

### 6.1 Device Registration

DQ	Cle	earPass Guest
		Operator Login
	Username:	student1
	Password:	••••••
		Log In

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.

aruba	ClearPass Guest	Menu 🗮
Devices     Create Device     Manage Devices	<ul> <li>Unified Visitor Management</li> <li>Last successful login from 192.168.1.131 on Friday, 26 April 2019, 1:51 PM</li> <li>No failed attempts since last successful login</li> </ul>	
	Devices         Manage devices.         • Create new device         • Manage devices         • Manage devices         • Manage devices         • Manage devices         • Legout	

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.

aruba		ClearPass Guest Menu
📲 Guest 🛛 🛛 🛛	ivew device beilig c	realed by students.
J Devices 💿		Create New Device
Create Device	* MAC Address:	a4:d1:d2:5f:32:52 MAC address of the device.
- Manage Multiple Device	Sponsor's Email:	ariyap@hpe.com Email of the person sponsoring this account.
	* Device Name:	My-ipad 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.
1	Account Expiration:	1 day from now Select an option for changing the expiration time of this account.
	* Account Role:	Students-Devs Role to assign to this account.
	Notes:	
	* Terms of Use:	I am the sponsor of this account and accept the terms of use
		<b>Streate</b>
	* required field	
🔦 Configuration 🛛 🛛 🛛 🛛	🖺 Back to device	IS .
🗼 Administration 🛛 💿	😭 Back to main	

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

aruba		ClearPass Guest	Menu 🗮
🖣 Guest 🛛 🛛 🛛 🛛	Home » Devices » C	reate Device	
JI Devices 📀	Finished Crea	ating Device	Create another device Manage devices
- 🛃 Create Device - 🚮 Manage Devices	The device was succ	essfully created.	
<ul> <li>Manage Multiple Device</li> </ul>		Create New Device Receipt	
	MAC Address:	A4-D1-D2-5F-32-52	
	Account Status:	Active	
	Account Activation:	Monday, 06 May 2019, 10:13 AM	
	Account Expiration:	Account will expire at Tuesday, 07 May 2019, 10:13 AM	
	Account Role:	Students-Devs	
	Registered By:	student1	
	Wi-Fi Password:	Generated	
	<ul> <li>Open print window</li> <li>Back to devices</li> <li>Back to main</li> </ul>	using template	

The credentials for the MPSK should be email automatically to the email address of the user who was registering this device. You should also be able to view the MPSK credential from "Device Registration"



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



## 6.2 ClearPass Access Tracker Operator Login

So from Access tracker we see the following two Auth Requests

Monitori	ing » Live Monitoring » Access	s Tracker				
Acces	ccess Tracker Apr 28, 2019 10:48:37 AEST					
The Acc	ess Tracker page provides a r	eal-time display of per-session	n access activity on the selec	ted server or domain.		
<b>T</b> [A	ll Requests]	poc.clearpass.info (192.16	58.1.94)	15 Last 1 day	before Today	Edit
				_		
Filter:	lequest ID 🗸 🗸	contains 🗸	Go Clear Filte	er		Show 20 v records
#	Server	Source	Username	Service	Login Status	Request Timestamp 🔹
1.	192.168.1.94	WEBAUTH	A4-D1-D2-5F-32-52	[Device Registration Disconnect]	ACCEPT	2019/04/28 10:46:38
2.	192.168.1.94	Application	student1	Guest Operator Logins	ACCEPT	2019/04/28 10:46:02

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

Summary In	put Out	tput		
Login Status:	ŀ	ACCEP	Т	
Session Identifier:	: \	w0000	00003-01-5cc4f7ca	
Date and Time:	ŀ	Apr 28	, 2019 10:46:02 AEST	
End-Host Identifie	er: -	-		
Username:	s	studen	t1	
Access Device IP/Port:		-:-		
Access Device Name:		-		
System Posture Status:		UNKNO	OWN (100)	
			Policies Used -	
Service:	(	Guest	Operator Logins	
Authentication Me	ethod: N	Not ap	plicable	
Authentication Source:		AriyaA	D	
Authorization Sou	irce:	AriyaA	D	
Roles:	[	[User /	Authenticated]	
Enforcement Profi	iles: N	MPSK-	Operator	

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

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

Enforcement Profiles: MPSK-Operator System Posture Status: UNKNOWN (100)	
System Posture Status: UNKNOWN (100)	
Audit Posture Status: UNKNOWN (100)	
Application Response	6
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 second WEBAUTH request that basically will disconnect the device if it was on the network.

Summary Input	Output
Login Status:	ACCEPT
Session Identifier:	W0000004-01-5cc4f7ee
Date and Time:	Apr 28, 2019 10:46:38 AEST
End-Host Identifier:	a4d1d25f3252
Username:	A4-D1-D2-5F-32-52
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], [Cisc

Summary	Input	Output			
Username:		A4-D1-D2-	5F-32-52		
End-Host Identifier: a4d1d25f3252		252			
Access Device	IP/Port:	-			
Computed At	tributes				$\odot$
Application:	ClearPass	:Page-Nam	e	mac_create	
Authentication:Full-Username				A4-D1-D2-5F-32-52	
Authentication:Full-Username-Normalized			ormalized	A4-D1-D2-5F-32-52	
Authentication:Posture			Unknown		
Authentication:Source			[Guest Device Repository]		
Authenticatio	on:Status	5		User	
Authentication:Username			A4-D1-D2-5F-32-52		
Authorization:Sources			[Guest Device Repository]		
Connection:	Client-Ma	c-Address		a4d1d25f3252	
Connection:Client-Mac-Address-Colon			Colon	a4:d1:d2:5f:32:52	

Summary	Input	Output				
Enforcement Profiles: [Aruba Termina Termina Session			S Wireless - Terminate Session], [Aerohive - Terminate Session], [Cisco - te Session], [H3C - Terminate Session], [Juniper Terminate Session], [Motorola - te Session], [Trapeze - Terminate Session], [ArubaOS Switching - Terminate			
System Postu	re Status:	UNKNOV	VN (100)			
Audit Posture	Status:	UNKNOV	VN (100)			
RADIUS Res	ponse		$\odot$			
Radius:IETF	-:Acct-Sess	sion-Id				
Radius:IETF	Radius:IETF:Calling-Station-Id		a4d1d25f3252			
Radius:IETF:NAS-IP-Address		ddress	192.168.1.10			
Radius:IETF:NAS-Port			0			
Radius:IETF	Service-T	уре	1			
Radius:IETF:User-Name		ne	student1			

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

Dashboard O	Monitor	ing » Event Viewer			
Monitoring 📀	Even	t Viewer			
Access Tracker      Accounting      OnGuard Activity	The Eve are log	ent Viewer provides reports about sys	tem-level events. A	All attempted upgrade, patch, and hotfix ins	tallations S
Analysis & Trending	#	Source	Level	Category	Action
Profiler and Network Scan	1.	ClearPass Updater	INFO	AV/AS Updates	Success
	2.	Policy Manager UI	INFO	Logged in	None
– 🧶 Event Viewer	3.	Admin UI	INFO	Email Successful	None
— 🌽 Data Filters	4.	Guest UI	INFO	Logged in	None
— 🥃 Blacklisted Users	5.	ClearPass Updater	INFO	AV/AS Updates	Success

#### **Event Viewer**

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

Filter:	Source	✓ contains ✓	🕀 Go Clear Filter				
#	Source		Level Category				
1.	Policy Mana	System Event Details	0				
2.	Admin UI	Course	Advain LIT				
3.	Guest UI	Source					
4.	Policy Mana	Level	INFO				
5.	ClearPass L	Category	Email Successful				
6	Admin LIT	Action	None				
0.	Admin 01	Timestamp	Apr 28, 2019 10:46:48 AEST				
7.	Guest UI	Description	From: ariyap@aruba.com				
8.	Monitor		To: ariyap@hpe.com				
9.	Policy Mana		Mail Subject: Device receipt for My-iPad (A4-D1-D2-5F-				
10.	System		32-52)				
11.	ClearPass L						
12.	ClearPass L		Close				

#### And this is the email content that was received



### 6.3 Aruba Instant AP

Now that we have the MPSK, we'll connect the device to the MPSK SSID.

	AL   InstantV	с								۹	۵	(?
Lul Dashboard	student1	192.168.1.131	a4:d1:d2:5f <mark>:32:52</mark>	ArubaMPSK	BLDG-A-ATV	<b>'1 14</b> 9	AN S	Students-D fd	14:5f94:8156:26	39	39	
Overview	Info	ent Match AppRF			F	RF Dashboard						
Access Points	Name	student1				Client	Sigr	nal	Spee	ed		
Clients	IPv6 Address	fd14:5f94:8156:2600:8	e1:313a:3231:2cf5			student1	at.					
	IP Address	192.168.1.131	MAC address	a4:d1:d2:5f:32:52		Access Point	Utilization	No	ise	Errors		
Configuration	OS		ESSID	ArubaMPSK		BLDG-A-ATV1	_	_		_		
	Access Point	BLDG-A-ATV1	Channel	149								
🔎 Maintenance	Туре	AN	Role	Students-Devs								

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

#### Nowe we'll view the details of the MPSK local cache

BLDG-A-ATV1# show ap mpskcache PPSK Cache Table \_\_\_\_\_ Role Client MAC Del Expiry Role VLAN ESSID Key \_\_\_\_\_ \_\_\_ ----\_\_\_\_ \_\_\_\_ a4:d1:d2:5f:32:52 590A1BAFA17E... No - ArubaMPSK 1 ArubaMPSK PPSK Cache Count:1 BLDG-A-ATV1#

Note that the Del column shows "No" and Expiry columns is empty. This will be the case as long as the device is in the association table of the IAP. Here is the client association table

BLDG-A-ATV1# sh ap association

The phy column shows client's operational capabilities for current association

Flags: H: Hotspot(802.11u) client, K: 802.11K client, M: VHT Mu beam formee, R: 802.11R client, W: WMM client, w: 802.11w client, V: 802.11v BSS trans capable, P: Punctured preamble, U: HE UL Mumimo, O: OWE client, S: SAE client, E: Enterprise client

PHY	Details:	HT	:	High	throughput;	20:	20MHz;	40:	40MHz;	t: turbo	o-rates	(256-QAM)	)
		VHT	:	Very	High throughput;	80:	80MHz;	160:	160MHz;	80p80:	80MHz +	- 80MHz	
		HE	:	High	Efficieny;	80:	80MHz;	160:	160MHz;	80p80:	80MHz +	- 80MHz	
		<n>ss</n>	::	<n> :</n>	spatial streams								

Association Table

Name assoc. time	bssid num assoc	Flags	mac DataReady	UAC	auth	assoc	aid	l-int	essid	vlan-id	phy
BLDG-A-ATV1	24:f2:7f:d	5:fa:d3	a4:d1:d2:5f	:32:52	У	У	1	10	ArubaMPSK	1	a-
HT-20-1ss	2m:59s	1	W	Yes	(Impli	cit)	0.0.0.0	)			

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.

```
BLDG-A-ATV1# show ap mpskcache
PPSK Cache Table
_____
                               Del Expiry Role
                                                          VLAN ESSID
Client MAC
                Key
_____
                 ___
                                ____ ____
                                             ____
                                                           _____
a4:d1:d2:5f:32:52 590A1BAFA17E... Yes <mark>16m:38s</mark> Students-Devs 1
                                                               ArubaMPSK
PPSK Cache Count:1
BLDG-A-ATV1#
BLDG-A-ATV1# show ap mpskcache
PPSK Cache Table
_____
                                                          VLAN ESSID
Client MAC
                Key
                               Del Expiry Role
_____
                 ___
                                ___
                                     _____
                                             ____
                                                           ____
                                                                ____
a4:d1:d2:5f:32:52 590A1BAFA17E... Yes
                                     15m:36s Students-Devs 1
                                                               ArubaMPSK
PPSK Cache Count:1
BLDG-A-ATV1#
```

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

```
BLDG-A-ATV1# show ap mpskcache
PPSK Cache Table
_____
Client MAC Key Del Expiry Role VLAN ESSID
_____
          ___
               ___
                    _____
                           ____
                                 ____
                                      ____
PPSK Cache Count:0
BLDG-A-ATV1#
BLDG-A-ATV1# sh ap deb auth-trace-buf 10
Auth Trace Buffer
_____
                                                                                    - 117
                                   <- a4:d1:d2:5f:32:52 24:f2:7f:d5:fa:d0
Apr 29 16:16:47 wpa2-key1
                                   -> a4:d1:d2:5f:32:52 24:f2:7f:d5:fa:d0
Apr 29 16:16:47 wpa2-key2
                                                                                    - 117
Apr 29 16:16:47 wpa2-key3
                                   <- a4:d1:d2:5f:32:52 24:f2:7f:d5:fa:d0
                                                                                    - 151
Apr 29 16:16:47 wpa2-key4
                                   -> a4:d1:d2:5f:32:52 24:f2:7f:d5:fa:d0
                                                                                       95
Apr 29 16:16:51 server out-of-service * a4:d1:d2:5f:32:52 24:f2:7f:d5:fa:d3/ClearPass
                                                                                    _
      timeout
server
Apr 29 16:17:44 mac-auth-req
                                    -> a4:d1:d2:5f:32:52 24:f2:7f:d5:fa:d3/ClearPass -
a4d1d25f3252
Apr 29 16:18:02 mac-auth-req
                                    -> a4:d1:d2:5f:32:52 24:f2:7f:d5:fa:d3/ClearPass -
a4d1d25f3252
Apr 29 16:18:04 server out-of-service * a4:d1:d2:5f:32:52 24:f2:7f:d5:fa:d3/ClearPass -
server timeout
Apr 29 16:18:21 mac-auth-req
                                    -> a4:d1:d2:5f:32:52 24:f2:7f:d5:fa:d3/ClearPass - -
a4d1d25f3252
Apr 29 16:18:22 server out-of-service * a4:d1:d2:5f:32:52 24:f2:7f:d5:fa:d3/ClearPass -
server timeout
BLDG-A-ATV1#
```

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

BLDG-A-ATV1# sh ap deb auth-trace-buf 10

Auth Trace Buffer

Apr 29 16:18:36	wpa2-key3	<-	a4:d1	:d2:5f:32:52	24:f2:7	f:d5:fa:d0	-	151
Apr 29 16:18:36	wpa2-key4	->	a4:d1	:d2:5f:32:52	24:f2:7	f:d5:fa:d0	-	95
Apr 29 16:18:40	server out-of-server	ice *	a4:d1	:d2:5f:32:52	24:f2:7	f:d5:fa:d3/ClearPass	-	-
server timeout								
Apr 29 16:23:16	mac-auth-req	->	a4:d1	:d2:5f:32:52	24:f2:7	f:d5:fa:d3/ClearPass	-	-
a4d1d25f3252	_							
Apr 29 16:23:16	mac-auth-success	<-	a4:d1	:d2:5f:32:52	24:f2:7	f:d5:fa:d3/ClearPass	-	-
success								
Apr 29 16:23:16	station-up	*	a4:d1	:d2:5f:32:52	24:f2:7	f:d5:fa:d3	-	-
wpa2 psk aes								
Apr 29 16:23:16	wpa2-key1	<-	a4:d1	:d2:5f:32:52	24:f2:7	f:d5:fa:d3	-	117
Apr 29 16:23:17	wpa2-key2	->	a4:d1	:d2:5f:32:52	24:f2:7	f:d5:fa:d3	-	117
Apr 29 16:23:17	wpa2-key3	<-	a4:d1	:d2:5f:32:52	24:f2:7	f:d5:fa:d3	-	151
Apr 29 16:23:17	wpa2-key4	->	a4:d1	:d2:5f:32:52	24:f2:7	f:d5:fa:d3	-	95
BLDG-A-ATV1#								
BLDG-A-ATV1# sho	w ap mpskcache							
PPSK Cache Table								
Client MAC	Кеу	Del	Expiry	Role	VLAN	ESSID		
a4:d1:d2:5f:32:5	2 8EFA48327CC5	No	-	Students-Dev	s 1	ArubaMPSK		
PPSK Cache Count	:1							
BLDG-A-ATV1#								

Let's check ClearPass access tracker.

\_\_\_\_\_

# 6.4 ClearPass Access Tracker MPSK Authentication

This is the Authentication request as seen from ClearPass.

Monitor	ring » Live Monitoring	» Access Tracker								
Acce	CCESS Tracker Apr 28, 2019 11:00:38 AEST									
The Ace	he Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.									
7 [/	Tall Requests [] [] poc.clearpass.i		o (192.168.1.94)	tast 1 da	ay before Today	Edit				
Filter:	Request ID	∽]contains ∽]	🛨 Go Clear	Filter		Show 20 ~ records				
Filter:	Request ID	✓ contains ✓ Source	Go Clear Username	Filter	Login Status	Show 20 v records				
Filter:	Request ID Server 192.168.1.94	Contains       Source       RADIUS	t Go Clear Username student1	Filter Service MPSK Aruba Wireless with MPSK	Login Status ACCEPT	Show 20 v records Request Timestamp v 2019/04/28 10:57:00				
Filter:	Request ID Server 192.168.1.94 192.168.1.94	✓ contains ✓ Source RADIUS WEBAUTH	Go Clear Username student1 A4-D1-D2-5F-32-52	Filter Service MPSK Aruba Wireless with MPSK [Device Registration Disconnect]	Login Status ACCEPT ACCEPT	Show         20         records           Request Timestamp •         2019/04/28 10:57:00         2019/04/28 10:46:38				

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

Summary Input C	Dutput							
Login Status:	ACCEPT							
Session Identifier:	R0000003-01-5cc4fa5c							
Date and Time:	Apr 28, 2019 10:57:00 AEST							
End-Host Identifier:	a4d1d25f3252							
Username:	student1							
Access Device IP/Port:	192.168.1.10:0 (InstantVC / Aruba)							
Access Device Name:	InstantVC							
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:	Students-Devs, [User Authenticated]							
Enforcement Profiles:	Aruba User Role - Students-Devs. [Reaistered Device MPSK]. [Return Device							

	Summary	Input	Output					
ι	Jsername:		student1					
E	nd-Host Ider	nd-Host Identifier: a4d1d25f3252						
Access Device IP/Port: 192.168.1.10:0 (InstantVC /			192.168.1.	10:0 (InstantVC / Aruba)				
	RADIUS Request							
	Radius:Arub	a:Aruba-	AP-Group	InstantVC				
	Radius:Arub	a:Aruba-	Essid-Name	ArubaMPSK				
	Radius:Arub	a:Aruba-	Location-Id	BLDG-A-ATV1				
	Radius:IETF	:Called-S	tation-Id	204c0323a7c0				
	Radius:IETF	:Calling-S	Station-Id	a4d1d25f3252				
	Radius:IETF	:NAS-Ide	ntifier	InstantVC	InstantVC			
	Radius:IETF	:NAS-IP-/	Address	192.168.1.10				
	Radius:IETF	:NAS-Por	t	0				
	Radius:IETF	:NAS-Por	t-Type	19				
	Radius:IETF	:Service-	Гуре	10				
	Cummony	Toput	Output					
	Summary	Input	Output					
	Radius:IETF	:Service-	Гуре	10				
	Radius:IETF:User-Name		me	a4d1d25f3252				
	Authorizatior	n Attribut	es			•		
			Davias Daa	- item il A	0			
	Authorizatio	n:[Guest	Device Repo	ository]:AccountStatus				
	Authorizatio	n:[Guest	Device Repo	ository]: Device Account Active	true			
	Authorization:[Guest Device Repository]:Device Account Enabled			false				

Authorization:[Guest Device Repository]:Device MPSK     ********       Authorization:[Guest Device Repository]:Device Role ID     3008       Authorization:[Guest Device Repository]:RemainingExpiration     85777       Authorization:[Guest Device Repository]:SponsorName     student1	Authorization.[Guest Device Repository].Device Account Expired	Idise
Authorization:[Guest Device Repository]:Device Role ID       3008         Authorization:[Guest Device Repository]:RemainingExpiration       85777         Authorization:[Guest Device Repository]:SponsorName       student1	Authorization: [Guest Device Repository]: Device MPSK	*****
Authorization:[Guest Device Repository]:RemainingExpiration       85777         Authorization:[Guest Device Repository]:SponsorName       student1	Authorization:[Guest Device Repository]:Device Role ID	3008
Authorization:[Guest Device Repository]:SponsorName student1	Authorization:[Guest Device Repository]:RemainingExpiration	85777
	Authorization:[Guest Device Repository]:SponsorName	student1

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

r
]

# 6.5 Packet Capture

Here we have got the packet capture using wireshark with a4:d1:d2:5f:32:52 being the MAC address of the client.

		_		
560 13.107895	Apple_5f:32:52	Broadcast	802.11	182 Probe Request, SN=2843, FN=0, Flags=C, SSID=ArubaMPSK
561 13.108373	HewlettP_d5:fa:d3	Apple_5f:32:52	802.11	264 Probe Response, SN=0, FN=0, Flags=, BI=100, SSID=ArubaMPSK
563 13.310298	Apple_5f:32:52	HewlettP_d5:fa:d3	802.11	107 Authentication, SN=2844, FN=0, Flags=C
566 13.312608	HewlettP_d5:fa:d3	Apple_5f:32:52	802.11	96 Authentication, SN=0, FN=0, Flags=, SSID=Wildcard (Broadcast)
568 13.312611	Apple_5f:32:52	HewlettP_d5:fa:d3	802.11	233 Association Request, SN=2845, FN=0, Flags=C, SSID=ArubaMPSK
570 13.312613	HewlettP_d5:fa:d3	Apple_5f:32:52	802.11	194 Association Response, SN=0, FN=0, Flags=, SSID=Wildcard (Broadcast)
576 13.377686	Apple_5f:32:52	HewlettP_d5:fa:d3	802.11	90 Null function (No data), SN=2846, FN=0, Flags=TC
582 13.551469	HewlettP_d5:fa:d3	Apple_5f:32:52	EAPOL	221 Key (Message 1 of 4)
584 13.552998	Apple_5f:32:52	HewlettP_d5:fa:d3	EAPOL	217 Key (Message 2 of 4)[Malformed Packet]
585 13.560994	HewlettP_d5:fa:d3	Apple_5f:32:52	EAPOL	255 Key (Message 3 of 4)
587 13.562625	Apple_5f:32:52	HewlettP_d5:fa:d3	EAPOL	195 Key[Malformed Packet]
590 13.867009	Apple_5f:32:52	HewlettP_d5:fa:d3	802.11	99 Action, SN=2847, FN=0, Flags=C
591 13.867290	HewlettP_d5:fa:d3	Apple_5f:32:52	802.11	102 Action, SN=25, FN=0, Flags=, SSID=Wildcard (Broadcast)[Malformed Packet]
594 13.868490	Apple_5f:32:52	IPv6mcast_16	LLC	200 I, N(R)=16, N(S)=0; DSAP NULL LSAP Group, SSAP NULL LSAP Command
595 13.868492	192.168.1.121	192.168.1.133	802.11	86 802.11 Block Ack Req, Flags=C
596 13.926893	Apple_5f:32:52	IPv6mcast_16	802.11	194 Data, SN=2559, FN=0, Flags=.pF.

Malform packet message on wireshark just indicates that wireshark dissector can't dissect the contents of the packet any further. Here we are using one IAP to do the remote pcap. But the main thing in the above screen shot is that MPSK goes through the 4-way key exchange.

#### Here is the BSS table on the Instant AP.

BLDG-A-ATV1# sh ap bss-table

Aruba AP BSS Table	e								
bss tot-t f	ess lags	port	ip	phy	type	ch/EIRP/max-EIRP	cur-cl	ap name	in-t(s)
24:f2:7f:d5:fa:d0 3d:6h:34m:31s	SG1	?/?	192.168.1.121	a-VHT	ap	149E/27.0/28.6	1	BLDG-A-ATV1	0
24:f2:7f:d5:fa:d1	Corp	?/?	192.168.1.121	a-VHT	ap	149E/27.0/28.6	0	BLDG-A-ATV1	0
3d:6n:34m:22s 24:f2:7f:d5:fa:d2 3d:6b:34m:13s	SG9 3M	?/?	192.168.1.121	a-VHT	ap	149E/27.0/28.6	0	BLDG-A-ATV1	0
24:f2:7f:d5:fa:d3	ArubaMPSK	?/?	192.168.1.121	a-VHT	ap	149E/27.0/28.6	1	BLDG-A-ATV1	0
2d:23h:10m:43s 24:f2:7f:d5:fa:c0	SG1	?/?	192.168.1.121	g-HT	ap	1/9.0/22.1	1	BLDG-A-ATV1	0
24:f2:7f:d5:fa:c1	Corp	?/?	192.168.1.121	g-HT	ap	1/9.0/22.1	0	BLDG-A-ATV1	0
3d:6h:34m:22s 24:f2:7f:d5:fa:c2	SG9	?/?	192.168.1.121	g-HT	ap	1/9.0/22.1	0	BLDG-A-ATV1	0
24:f2:7f:d5:fa:c3 2d:23h:10m:41s	ArubaMPSK	?/?	192.168.1.121	g-HT	ap	1/9.0/22.1	0	BLDG-A-ATV1	0

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

Num APs:8 Num Associations:3

Flags: K = 802.11K Enabled; W = 802.11W Enabled; 3 = WPA3 BSS; O = OWE Transition mode OWE BSS; o = OWE
Transition mode Open BSS; M = WPA3-SAE mixed mode BSS
BLDG-A-ATV1#

#### And here is the corresponding Authentication trace from IAP.

BLDG-A-ATV1# sh ap deb auth-trace-buf mac a4:d1:d2:5f:32:52 12

Auth Trace Buffer

Apr 29 14:05:46	mac-auth-req	->	a4:d1:d2:5f:32:52	24:f2:7f:d5:fa:d3/ClearPass	-	-
a4d1d25f3252						
Apr 29 14:05:46	mac-auth-success	<-	a4:d1:d2:5f:32:52	24:f2:7f:d5:fa:d3/ClearPass	-	-
success						
Apr 29 14:05:46	station-up	*	a4:d1:d2:5f:32:52	24:f2:7f:d5:fa:d3	-	-
wpa2 psk aes						
Apr 29 14:05:46	wpa2-key1	<-	a4:d1:d2:5f:32:52	24:f2:7f:d5:fa:d3	-	117
Apr 29 14:05:46	wpa2-key2	->	a4:d1:d2:5f:32:52	24:f2:7f:d5:fa:d3	-	117
Apr 29 14:05:46	wpa2-key3	<-	a4:d1:d2:5f:32:52	24:f2:7f:d5:fa:d3	-	151
Apr 29 14:05:46	wpa2-key4	->	a4:d1:d2:5f:32:52	24:f2:7f:d5:fa:d3	-	95
Apr 29 14:48:51	station-up	*	a4:d1:d2:5f:32:52	24:f2:7f:d5:fa:d3	-	-
wpa2 psk aes						
Apr 29 14:48:51	wpa2-key1	<-	a4:d1:d2:5f:32:52	24:f2:7f:d5:fa:d3	-	117
Apr 29 14:48:51	wpa2-key2	->	a4:d1:d2:5f:32:52	24:f2:7f:d5:fa:d3	-	117
Apr 29 14:48:51	wpa2-key3	<-	a4:d1:d2:5f:32:52	24:f2:7f:d5:fa:d3	-	151
Apr 29 14:48:51	wpa2-key4	->	a4:d1:d2:5f:32:52	24:f2:7f:d5:fa:d3	-	95
BLDG-A-ATV1#						

# 7 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.

## 7.1 Aruba Instant 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.

	RTUAL InstantVC		
Lul Dashboard	<ul> <li>Authentication Servers</li> <li>Users</li> </ul>		
Networks	> Roles		
Access Points	<ul> <li>Firewall Settings</li> </ul>	MPSK-Rego	
Configuration	> Inbound Firewall	Type IP or hostname	RADIUS Authentication 🗸
Networks	External Captive Portal	Port	/guest/mac_create.php 443
Access Points	Name	Use HTTPS	
System RF	DemoCP	Captive Portal failure Automatic URL Whitelisting	Deny internet V
Security	Guest-CP	Server offload Prevent frame overlay	
IDS	BYOD-CP MPSK-Rego	Use VC IP in Redirect URL	
Routing	<ul> <li>+ 2 m</li> <li>&gt; Custom Redirect Page URL</li> </ul>		Cancel

#### Then we'll reference that in our Guest WLAN.



Edit network Guest	2 VLAN 3 Security 4 Access
Client IP & VLAN Assignment Client IP assignment	<ul> <li>Virtual Controller managed</li> <li>Network assigned</li> </ul>
Client VLAN assignment	Default     Static     Dynamic
Edit network Guest	Basic   2   VLAN   3   Security   4   Access
Security Level	
Splash page type	External V
Captive portal proxy server	1
Captive portal profile	MPSK-Rego 🗸 🗹 🕇
WISPr	
MAC authentication	
Delimiter character	
Uppercase support	
Authentication server 1	ClearPass v Z +
Authentication server 2	Select Server 🗸 🕂
Reauth interval	hrs. 🗸
Accounting	Use authentication servers $\checkmark$
Accounting mode	Authentication 🗸
Accounting interval	1 min.
Blacklisting	
Enforce DHCP	
Edit network Guest	Basic 2 VLAN 3 Security 4 Access
Access Rules	
Access Rules	Network-based V
Access Rules for Guest	
Deny webcategory adult-at     Allow any to all destination	nd-pornography to all destinations
- Anon any to an destination	

## 7.2 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	ClearPass Guest							
🚑 Guest 🔹 🕻	Home » Administration » Plu	Home » Administration » Plugin Manager						
ji <sup>1</sup> Devices	MAC Authentication	MAC Authentication 6.8.0-109592 Configuration						
📳 Onboard 🔹								
🔦 Configuration 🔹	Set the configuration option	s for MAC Authentication 6.8.0-109592.						
S Administration		Configure MAC Authentication 6.8.0-109592						
API Services	* MAC Detect:	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.						
SOAP Web Services	Device Filter:	<ul> <li>Manage Accounts</li> <li>Manage Multiple Accounts</li> <li>Select which views should not display devices (user accounts with the 'mac_auth' field set).</li> </ul>						
- 💱 AirGroup Configuration	Aruba MPSK Options							
- I MPSK Configuration	* 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.						
Import Configuration	* Password Complexity:	No password complexity requirement Password complexity to enforce for manually-entered MPSK.						
Import Configuration     Import     Last Import     Son Operator Logins	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.						
- Drafiles		Save Configuration						
- 💭 Profiles - 🥏 Servers	* required field							
- 🔊 Translation Rules	Restore default configu	ration						
- C Plugin Manager	Back to plugin manager	r						

## 7.3 Testing the new workflow

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

	TUAL ROLLER InstantVC										Q
Overview	Wireless (8) Wire	ed (0)									
Networks	Name	IP Address	MAC address	os	ESSID	Access Point	Channel	Туре	Role	IPv6 Address	Signal
Access Points		192.168.1.128	84:38:38:46:a9:39	Android	SG1	BLDG-A-ATV1	36E	AC	S5-Remote	fd14:5f94:8156:26	27
Clients	DESKTOP-SOID	192.168.1.133	f0:d5:bf:4b:67:11	Win 10	SG1	BLDG-A-ATV1	36E	AC	ShiziLaptop		48
	a4d1d25f3252	192.168.1.120	a4:d1:d2:5f:32:52		Guest	BLDG-A-ATV1	36	AN	External CP	fd14:5f94:8156:26	40

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.

iPad ᅙ		1:56 PM		722		53% 🔳				
< > 🕮 📃		■ 192.168.1.94	¢	Û	+					
aruba		ClearPass Guest			Menu					
📲 Guest 🛛 🛛 🗿	Home » Devices »	Create Device								
JI Devices 💿	Create Devic	ce		💕 Ma	inage (	levices				
- 42 Create Device	Last successful login from 192.168.1.120 on Wednesday, 01 May 2019, 5:47 PM									
- Manage Multiple Device	No failed attem	ants since last successful login								
	New device being o	created by <b>student1</b> .								
		Create New Device								
	* MAC Address:	(4:d1:d2:5f:32:52) MAC address of the device.								
	Sponsor's Email:	Email: ariyap@hpe.com Email of the person sponsoring this account.								
	* Device Name:	* Device Name: Myipad Name of the device.								
	AirGroup: AirGroup uses device ownership and location information to limit the printers and Apple TVs available to network users.									
	Account Now Select an option for changing the activation time of this account.									
	Account I day from now Select an option for changing the expiration time of this account.									
	* Account Role:	Students-Devs Role to assign to this account.								
6 Configuration 0	Device Category:	SmartDevice								
Administration 0	Device Family:	Apple								
Administration 0	Device Name:	Apple iPad								

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.

iPad 중		1:56 PM	53% 💷)
< > 🕮 📃		€ 192.168.1.94	c 🕆 🗇
aruba		ClearPass Guest	Menu 🗮
🐫 Guest 🛛 🛛 🛛 🛛 🗿	Home » Devices » C	reate Device	
Devices 📀	Finished Crea	ting Device	Create another device Manage devices
- Streate Device - Streate Devices	The device was succ	essfully created.	
— 🧾 Manage Multiple Device		Create New Device Receipt	
	MAC Address:	A4-D1-D2-5F-32-52	
	Account Status:	Active	
	Account Activation:	Sunday, 05 May 2019, 2:00 PM	
	Account Expiration:	Account will expire at Monday, 06 May 2019, 2:00 PM	
	Device Category:	SmartDevice	
	Device Family:	Apple	
	Device Name:	Apple iPad	
	Device IP:	192.168.1.120	
	Account Role:	Students-Devs	
	Registered By:	student1	
	Wi-Fi Password:	Generated	
	Open print window	using template	

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

student1	192.168.1.120	a4:d1:d2:5f:32:52	iPad	ArubaMPSK	BLDG-A-A	FV1 36	AN	Students-D	fd14:5f94:8156:26	36 52
Shizzys-iPhone	192.168.1.131	b8:41:a4:74:e5:46	iPhone	SG1	BLDG-A-A	TV1 36E	AC	SG1	fd14:5f94:8156:26	32 468
Overview Clie	nt Match AppRF									
Info						RF Dashboard				
Name	student1					Client		Signal	Spe	ed
IPv6 Address	fd14:5f94:8156:2600:8	e1:313a:3231:2cf5				student1		.el	4	
IP Address	192.168.1.120	MAC addres	s <mark>a4:d</mark>	1:d2:5f:32:52		Access Point	Utiliza	tion	Noise	Errors
os	iPad	ESSID	Arub	aMPSK		BLDG-A-ATV1	_		_	_
Access Point	BLDG-A-ATV1	Channel	36							
Туре	AN	Role	Stud	ents-Devs						

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

# 8 Prepopulating MAC address with Self Registration

This is a variation on the previous workflow where we configure a self-registration page for MPSK.

### 8.1 Aruba Instant Configuration

Here we just need to change the URL redirection for Guest clients in the MPSK-Rego External Captive Portal

aruba   Vir Conti	ROLLER InstantVC			
Overview	> Authentication Servers			
Networks	> Users			
Access Points	> Roles	MPSK-Rego		
Clients	> Blacklisting	Туре	RADIUS Authentication 🗸	
	> Firewall Settings	IP or hostname	192.168.1.94	
Configuration	> Inbound Firewall	URL	/guest/mac_create_2.ph	
Networks	<ul> <li>External Captive Portal</li> </ul>	Port	443	
Access Points	External Captive Portal	Use HTTPS		
System	Name	Cantive Portal failure		
RF	default			
Security	DemoCP	Automatic URL whitelisting		
IDS	Offender	Server offload		
Bouting	BYOD-CP	Prevent frame overlay		
Routing	MPSK-Rego	Use VC IP in Redirect URL		
Tunneling	+ 🥒 🟛	Redirect URL	(optional)	
Services	> Custom Redirect Page URL			
DHCP Server				Cancel OK

The URL for redirection is "/guest/mac\_create\_2.php?\_browser=1"

### 8.2 ClearPass Guest Self Rego

We need to create a self-registration page with that name.

But before that we'll duplicate the create\_mac form by going to "Configuration » Pages » Forms"



#### Now we should have mac\_create\_2 as shown below.

(A) B		
🥵 Pages 🌆 Fields	hotspot_user Hotspot Manager form that collects customer information.	Your Details
– m Forms – m List Views	mac_create * Create a single device.	Create New Device
Self-Registrations	mac_create_2 * Create a single device.	MPSK-Registration

Now we'll create a new self-registration page.

Home » Configuration » Pages » Self-Registrations

### Self-Registrations

Self-Registration 'MPSK-Registration'

Use this list view to manage the pages used for self-registration.

1 Quick Help									
ا الم	Register Page	Skin	Parent						
Guest Self-Registration Default settings for visitor self-registration.	guest_register	(Default)	(No Parent)						
S MPSK-Registration	MPSK-Rego	(Default)	(No Parent)						
2 self-registrations 🚫 Reload			Show all rows						

Once you have created the self-registration page go to Advanced Editor to change some of the configurations.



💐 Advanced editor

I have highlighted all the fields/areas that need to be changed. First type in the

#### Customize Self-Registration (MPSK-Registration)

Use this form to make changes to the self-registration instance **MPSK-Registration**.

	Customize Self-Registration							
<b>Basic Propert</b>	ies							
Options controlling	pasic operation of self-registration.							
* Name:	MPSK-Registration							
	Enter a name to identify the self-registration instance. This is visible only to administrators.							
Description:								
	er comments about this instance of self-registration. This is visible only to administrators.							
Enabled:	Enable self-registration							
* Degister Dege	mac_create_2							
* Register Page:	Enter the base page name for the self-registration page.							
* User Databaser	🔞 ClearPass Policy Manager							
User Database:	Self provisioned guest accounts are created using this service handler.							
* Chin	(Default)							
Skin:	Choose the skin for the self-registration pages.							
	Enable bypassing the Apple Captive Network Assistant							
Prevent CNA:	The Apple Captive Network Assistant (CNA) is the pop-up browser shown when joining a network that has a captive portal.							
Advertising:	$\sqcup$ Enable Advertising Services content							
Translations:	tions: Skip automatic translation handling							
	Many fields and pages have translations available under Configuration * Translations * Page Customizations. Select this option to keep all text as default.							
Access Contro								
Controls access to th	e registration page.							
	Require operator credentials prior to registering the guest							
Authentic	tion: If checked, access to this registration page will require operator credentials.							
	The sponsor's operator profile must have the Guest Manager > Create New Guest Account privilege.							
Allowed Ar								
Allowed Ad								
	Enter the IP addresses and networks from which self-registration is permitted.							
Denied Ac	cess:							
	1							
	Enter the IP addresses and networks that are denied self-registration access.							
* Deny Beh	avior: Send HTTP 404 Not Found status $\checkmark$							
	Select the response of the system to a request that is not permitted.							
Time A								
Time Ac	cess:							
	Enter a list of time ranges during which self-registration is enabled, one per line. For example, 'weekdays 7:00 to 19:00'. Leave blank to enable registration at all times.							

The above highlighted area is need to ensure the user gets authenticated as a Guest operator.

#### Register Page UI

Options controlling the appe	arance of the self-registration page.
Title:	Self-Registration The title to display on the self-registration page.
Form Title:	Self-Registration The form title to display on the self-registration page.
Header HTML:	<pre>{nwa_cookiecheck} F Please complete the form below to gain access to the network.   Insert  HTML template code displayed before the self-registration form.</pre>
Footer HTML:	{if \$gsr_metadata.nas_login.enabled} Already have an account? <a """"""""""""""""""""""""""""""""""<="" href="" th=""></a>
Override Form:	Do not include self-registration form contents Select this option if you want to replace the HTML of the form.

Receipt Page UI Options controlling the app	earance of the guest receipt page.							
Title:	Self-Registration Receipt							
Form Title:	The form title to display on the receipt page.							
Header HTML:	The details for your guest account are shown below.							
	HTML template code displayed before the guest receipt.							
Footer HTML:	Insert v							
Override Receipt:	Do not include guest receipt contents Select this option if you want to replace the HTML of the guest receipt.							
Receipt Actions Options for delivering a rec	eipt to a self-registered guest.							
Enabled:	Enable download of guest receipt							
Print								
Enabled	Enable print window for quest receipts							
Email Delivery								
Enabled:	Always auto-send guest receipts by email							
* Email Field:	sponsor_email   The field containing the visitor account's email address.							
Subject Line:	MPSK-Receipt         Template specifying the subject line for emailed visitor account receipts.         Leave blank to use the default.         Guests: Visitor account receipt for {\$email}         Devices: Device receipt for {if \$visitor_name}{\$visitor_name} ({\$mac}){else}{\$mac}{/if}							
* Email Receipt:	Device Registration  The plain text or HTML print template to use when generating an email receipt.							
* Email Skin:	(Use Default: Use the default skin) The format in which to send email receipts.							
* Send Copies:	[(Use Default: Use 'Bcc:' if sending to a visitor) $\checkmark$ Specify when to send visitor account receipts to the recipients in the Copies To list.							
Copies To:	default An optional list of email addresses to which copies of visitor account receipts will be sent. Enter `_admin' to have the email sent to the sponsor's email address.							
Reply-To:	☐ Allow the reply-to address to be overridden If checked, the reply-to address will be overridden by the sponsor_email field. Leave unchecked to use the global from address.							
SMS Delivery	,							
Enabled:	Disable sending guest receipts by SMS $\vee$							
Sponsorship Co	onfirmation							
Enabled:	Require sponsor confirmation prior to enabling the account							
Download Pass	quest receipt as a pass for use with Apple Passbook							
	A Your pass configuration does not currently enable passes to be downloaded.							
Not Available:	<ul> <li>Ensure that a valid I Pass Certificate has been installed.</li> </ul>							

Login

Options controlling logging	in for self-registered guests.
Enabled:	Enable guest login to a Network Access Server $\ ^{\smallsetminus}$
* Vendor Settings:	Aruba Networks  Select a predefined group of settings suitable for standard network configurations.
Login Method:	Controller-initiated — Guest browser performs HTTP form submit Select how the user's network login will be handled. Server-initiated logins require the user's MAC address to be available, usually from the captive portal redirection process.
* IP Address:	securelogin.arubanetworks.com Enter the IP address or hostname of the vendor's product here.
Secure Login:	Use vendor default  V Select a security option to apply to the web login process.
Dynamic Address:	The controller will send the IP to submit credentials In multi-controller deployments, it is often required to post credentials to different addresses made available as part of the original redirection. The address above will be used whenever the parameter is not available or fails the requirements below.
Security Hash:	Do not check – login will always be permitted Select the level of checking to apply to URL parameters passed to the web login page. Use this option to detect when URL parameters have been modified by the user, for example their MAC address.
Default Destination Options for controlling the	destination dients will redirect to after login.
* Default URL:	http://www.arubanetworks.com Enter the default URL to redirect clients. Please ensure you prepend "http://" for any external domain.
Override Destination:	Force default destination for all clients     If selected, the client's default destination will be overridden regardless of its value.

# You need to enable Pre-Auth check using App Authentication.

<b>Login Form</b> Options controlling the appe	arance of the NAS login form.
Custom Form:	Provide a custom login form If selected, you must supply your own HTML login form in the Header or Footer HTML areas.
Custom Labels:	Override the default labels and error messages If selected, you will be able to alter labels and error messages for the current login form.
Pre-Auth Check:	App Authentication — check using Aruba Application Authentication < Select how the username and password should be checked before proceeding to the NAS authentication.
Terms:	Require a Terms and Conditions confirmation If checked, the user will be forced to accept a Terms and Conditions checkbox.
CAPTCHA:	None  V Select a CAPTCHA mode.
Post-Authenticatio	n iccessful pre-authentication.
Health Check:	Require a successful OnGuard health check If selected, the guest will be required to pass a health check prior to accessing the network.
Update Endpoint:	Mark the user's MAC address as a known endpoint If selected, the endpoint's attributes will also be updated with other details from the user account.

#### Login Page

g the appearance of the NAS login page.

and the two togin page.
Network Login The page title to display on the login page.
<pre>{mwa_cookiecheck}  {if \$errmsg}{mwa_icontext type=error}{\$errmsg escape} {/mwa_icontext}{7if} {mwa_text id=7980} Please login to the network using your username and password.   /mwa_text} Insert   HTML template code displayed before the login form. </pre>
Sped an account? <a """"""""""""""""""""""""""""""""""<="" href="" td=""></a>
Network Login In Progress The page title to display while logging into the NAS.
Please wait while you are logged into the network

Automatic Login Options controlling automatic	cally logging in from the receipt form.				
* Login Delay:	Image: Seconds         The time in seconds to delay while displaying the login message.				
Cloud Identity Optionally present guests wi	ith various cloud identity / social login options.				
Enabled:	Enable logins with cloud identity / social network credentials				
Self-Service Portal Options controlling details ar	nd actions a visitor has to their own account.				
Enabled:	Enable self-service portal				
Disabled Users:	Prohibit disabled users from accessing the service portal				
Silent Login:	Auto login by IP address If set, and the user has an active accounting session, they will be logged in automatically.				
Login Page					
UI Overrides:	Display fields to override UI text and labels				
Summary Page					
UI Overrides:	Display fields to override UI text and labels				
Change Password					
Change Password:	Disable the ability to change passwords				
Extend Expiration:	Extend Expiration: Extend the account's expiration time. Leave blank to use the original expiration time. Example values: 30d, +30d, or 1y.				
UI Overrides:	$\Box$ Display fields to override UI text and labels				
Reset Password					
Reset Password:	$\Box$ Disable the ability to reset passwords				
* Required Field:	(Secret Question)  The field containing a value the visitor must match prior to resetting their password.				
Match:	$\square$ Perform a case-insensitive match on the required field				
* Password Generation:	Passwords will be randomly generated $\vee$ Select the policy for reset password generation.				
UI Overrides:	Display fields to override UI text and labels				
Form Title:	The form title of the room selection page.				
	Save Changes				

Now let's double check if we have selected the correct form. Note that we should see "create\_mac\_2" as the form Self-Registration 'MPSK-Registration'



Note that we should see "create\_mac\_2" as the form

# Customize Form Fields (mac\_create\_2)

#### Use this list view to modify the fields of the form **mac\_create\_2**.

1 Quick Help	Preview Form						
🛆 Rank	Field	Туре	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	mpsk_enable	hidden	Wi-Fi Password:				
40.2	auto_send_smtp	hidden	Auto Email:				
40.30000000000004	smtp_email_field	hidden	Email Field:				
44	airgroup_enable	checkbox	AirGroup:	AirGroup uses device ownership and location information to limit the printers and Apple TVs available to network users.			
				A second device is sub-motionly			
44.5	airgroup_shared	radio	Ownership:	A personal device is automatically shared with other devices owned by the same user. A shared device has no owner, but more sharing options are available.			
45	airgroup_shared_user	text	Shared With:	Enter the usernames that will be able to use this device. Use a comma-separated list, e.g. user1,user2,user3, or blank for all users.			
46	airgroup_shared_location	multiselect	Shared Locations:	Select the locations where this device will be shared.			
47	airgroup_shared_role	multiselect	Shared Roles:	Select the user roles that will be able to use this device.			
48	airgroup_shared_group	multiselect	Shared Groups:	Select the user groups that will be able to use this device. This feature requires AOS 6.4 or later.			
49	airgroup_shared_time	textarea	Time Sharing:	Specify time-based sharing rules for this device.			
50	modify_start_time	dropdown	Account Activation:	Select an option for changing the activation time of this account.			
50	start_time	datetime	Activation Time:	Scheduled date and time at which to enable the account. If blank, the account will be enabled immediately.			
61	modify_expire_time	dropdown	Account Expiration:	Select an option for changing the expiration time of this account.			
62	expire_time	datetime	Expiration Time:	Optional date and time at which the account will expire and be deleted. If blank, the account will not expire.			
63	expire_after	dropdown	Expires After:	Amount of time before this account will expire.			
66	do_expire	dropdown	Expire Action:	Select an option for controlling the expiration of this account. Note that a logout can only occur if the NAS is RFC-3576 compliant.			

70	role_id	dropdown	Account Role:	Role to assign to this account.
81	no_password	hidden	Password Change:	If set, prevents the user from changing their own password.
85	no_portal	hidden	Portal Login:	If set, prevents the user from logging into the guest service portal.
136.1	endpoint_profile_device_category	static	Device Category:	
136.2	endpoint_profile_device_family	static	Device Family:	
136.3	endpoint_profile_device_name	static	Device Name:	
136.4	endpoint_profile_ip	static	Device IP:	
800	notes	textarea	Notes:	
900	create_time	hidden	Created:	Time the account was created.
901	remote_addr	hidden	Create Address:	This is your IP address.
902	http_user_agent	hidden	User Agent:	This is your browser's user agent string.
980	creator_accept_terms	checkbox	Terms of Use:	
990	submit	submit	Create	

Here we have disabled the Airgroup field that you had seen in the previous MPSK registration pages.

When you click on the "review Form" at the top of the page, you should see the preview as shown below. The account role will be limited to "Students-Devs"

Customize Form Fields (MPSK-Rego)

Use this list view to modify the fields of the form MPSK-Rego.

Quick Help	Preview Form
	Self-Registration
MAC Address:	MAC address of the device.
* Sponsor's Email:	Email of the person sponsoring this account.
* Device Name:	Please enter your full name.
Account Activation:	Now  Select an option for changing the activation time of this account.
Account Expiration:	Account will not expire Select an option for changing the expiration time of this account.
* Account Role:	[[Guest] → Role to assign to this account.
Notes:	
* Terms of Use:	☐ I accept the terms of use Flag indicating that the creator has accepted the terms and conditions of use.
	Register
* required field	

Once we have saved these configuration while on the self-registration page we need to edit the receipt Form.

Self-Registration 'MPSK-Registration'



Once you click on the receipt form, you'll notice that the form is called mac\_create\_2\_receipt. So you could go directly to the forms section and edit it there as well. Anyway here we want to disable the "submit" field, this will remove the "Login" button from the receipt page.

Customize Form Fields (mac\_create\_2\_receipt)

Use ti	his list	view to	modify	the	fields	of the	form	mac_	create_	2_	receipt.
--------	----------	---------	--------	-----	--------	--------	------	------	---------	----	----------

1 Quick Help			Preview F	Form		
🛆 Rank	Field	Туре	Label		Description	
10	sponsor_name	static	Sponsor's Name:	-		
15	sponsor_email	static	Sponsor's Email:	_		
20	visitor_name	static	Guest's Name:			
25	visitor_phone	phone	Phone Number:	-		
30	visitor_company	static	Company Name:	-		
40	username	static	Account Username:	-		
41	password	static	Guest Password:	-		
50	start_time	static	Activation Time:	-		
60	expire_time	static	Expiration Time:	-		
65	mpsk_enable	static	Wi-Fi Password:	-		
70	role_name	static	Account Role:	-		
75	enabled	static	Account Status:	-		
999999	submit	submit	Log In			
子 Edit	🌆 Edit Base Field	峇 Insert Before 🍃	Insert After 🔀 Disable Field			

So now when you click on the "Preview Form" you should see the below screenshot.

Customize Form Fields (mac\_create\_2\_receipt)

Use this list view to modify the fields of the form mac\_create\_2\_receipt.

1 Quick Help		Preview Form	
Se	elf-Registration Receipt		
Sponsor's Name:	sponsor_name		
Sponsor's Email:	sponsor_email		
Guest's Name:	visitor_name		
Company Name:	visitor_company		
Account Username:	臭 username		
Activation Time:	Monday, 06 May 2019, 5:28 PM		
Expiration Time:	Monday, 06 May 2019, 5:28 PM		
Wi-Fi Password:	Generated		

Once you have saved all these, you need to make a change to the Receipt templates. In our Self rego page, we were using Email Receipt = Device Registration

You can find the Device Registration template here. We need to modify it a bit.

aruba		ClearPass Guest	
🖣 Guest 🔹	Home » Configuration » Receipts » Templates	3	
Devices	Guest Manager Print Template	S	
🚺 Onboard 🔹	0		
Configuration	The print templates you have defined are list	ed below.	
– 왕 Authentication	1 Quick Help		
E- 🥶 Content Manager	△ Name	Format	Status
- Suest Manager	Account List	List	Enabled
Hotspot Manager	Certificate Expiry	Page	Enabled
- The Fields	Bevice Registration	Page	Enabled
- 🚡 Forms	Download Receipt	Plain Text	Enabled
– 🛄 List Views	Guest Account Expiry	Page	Enabled
Self-Registrations	GuestManager Receipt	Page	Enabled
Web Logins	🗟 One account per page	Page	Enabled
	SMS Receipt	Plain Text	Enabled
- 10 Jigital Pass Templates	SMS Sponsor Confirmation Alert	Plain Text	Enabled
–🙀 Email Receipt	Sponsor Device Provisioning	Wizard	Enabled
- b SMS Receipt	Sponsorship Confirmation	Wizard	Enabled
	Two-column scratch cards	2-column list	Enabled
וייק אוש Services ווייק Translations	12 print templates 🟠 Reload		Show all rows

Here is the preview of it, note the SSID name.

aruba		ClearPass Guest	;
Guest o Si Devices o	1 Quick Help		
📳 Onboard 🛛 🔍 🔍	△ Name	Format	Status
🔦 Configuration 📀	Account List	List	Enabled
- 🄧 Authentication	Certificate Expiry	Page	Enabled
⊪-🥶 Content Manager	Device Registration	Page	Enabled
- Suest Manager	📑 🚰 Edit 🔓 Duplicate 🔞 Delete 🎉	Permissions	ge 🍓 Preview
Hotspot Manager			
	Your device has and can now be Wi-Fi Network: Aruba Device Name: User Na MAC Address: 01-23-4	been successfully reg connected. ame 15-67-89-00	istered
	Device Wi Ei Instructioner		
	Device wi-Fi instructions.		
	1 Make sure your wireless adapter 01	23-45-67-89-00 is set to dynamically obtain an	IP address
	2 Connect to the wireless network: An	uba .	
	3 Wi-Fi password: a1b2c3def5		
	4 Device expires: Monday, May 13, 20	19 15:02	
🔆 Administration 🔹 💿			

We'll change it to the ArubaMPSK SSID that we have configured on Aruba Instant. You can totally customise this receipt template by editing it.

#### aruba

#### ClearPass Guest



Home » Configuration » Receipts » Templates

#### Edit Print Template (Device Registration)

You can make changes to a print template for guest account receipts here.

Templates are made up of three parts: the header, which is the first part of the printed document; the body, which is the list of user a

You ca	n use	the	following	special	variables	in	the	template:	
--------	-------	-----	-----------	---------	-----------	----	-----	-----------	--

Variable	Description	Example
	User Fields	
{\$u.username}	User account name	12345678
{\$u.password}	User account password	87654321
{\$u.enabled}	Non-zero if the guest account is enabled	1
{\$u.role_name}	Role assigned to guest account	Guest
{\$u.start_time}	Time at which the guest account will become active	1155772123
{\$u.expire_time}	Time at which the guest account will expire	1155858523
{\$u.expire_postlogin}	Lifetime of the guest account login in minutes after login	120
{\$u.visitor_name}	User's name	Susan Guest
{\$u.visitor_company}	User's company name	Acme Sprockets
{\$u.sponsor_name}	Sponsor's name	John Sponsor
{\$u.custom_field}	Custom fields attached to the account	
{\$action}	Action taken on account (create, delete or edit)	create
{\$source}	Source of account action (create_user, reset_password, etc.)	create_user
{\$result.error}	Non-zero if an error occurred while creating the guest account	0
{\$result.message}	Message related to the account creation	
{\$timestamp}	Time at which the receipt was generated	1155752000
<mark>{\$site_ssid}</mark>	SSID of the wireless LAN	Aruba
{\$site_wpa_key}	WPA key for the wireless LAN	

It uses a number of variables that are all defined in the Guest Manager. We'll change the Site SSID to ArubaMPSK.

aruba		ClearPass Guest
🔍 Guest 🔹 💿		
Devices O	Account Expiry Warning:	Notify users before their user credentials expire If checked, users will receive an email notification when their device's network credentials are due to expire.
📳 Onboard 🔹 💿	Receipt Options	
Configuration O	Site SSID:	ArubaMPSK. The SSID of the wireless LAN, if applicable. This will appear on guest account print receipts.
- 🧏 Authentication 🗈 🎯 Content Manager	Site WPA Key:	The WPA key for the wireless LAN, if applicable. This will appear on guest account print receipts.
- 🛱 Guest Manager 관 🎨 Hotspot Manager	Receipt Printing:	Require click to print Guest receipts can print simply by selecting the template in the dropdown, or by clicking a link.
🖃 😫 Pages	General Options	
- 🌇 Fields - 🛅 Forms - 🛄 List Views - 🏠 Self-Registrations - 🚰 Web Logins	Terms Of Use URL:	public/terms.html           The URL of a terms and conditions page. The URL will appear in any terms checkbox with: {nwa_global name=guest_account_terms_of_use_url}           It is recommended to upload your terms in Content Manager, where the files will be referenced with the "public/" prefix.           Alternatively, you can edit Terms and Conditions under Configuration > Pages > Web Pages.           If your site is hosted externally, be sure the proper access control lists (ACLs) are in place.           If terms are not required, it is recommended to edit the terms field on your forms to a Ut type "hidden" and an Initial Value of 1.
Web Pages  Receipts  Digital Pass Templates	Active Sessions:	Enable limiting the number of active sessions a guest account may have. Enter 0 to allow an unlimited number of sessions.
System rates templates     SMS Receipt     SMS Receipt     SMS Receipt     SMS Services     Translations	ceipt eipt s About Guest Network Access:	Insert Template code to display on the Guest Manager start page, under the "About Guest Network Access" heading. Leave blank to use the default text, or enter a hyphen ("-") to remove the default text and the heading.
		Save Configuration

Lastly you need to change the "Students" operator profile and set "Guest Manager" Access to custom and with only allowing access to "Create new Guest Accounts"



### 8.3 ClearPass Policy Manager Service

We need to modify an existing [Device Registration Disconnect] Service to match our new page.

Before it was matching mac\_create and mactrac pages

Services - [Device Registration Disconnect]

Su	mmary S	ervice	Authentication	Roles	Enforcement					
Nam	ame: [Device Registration Disconnect]									
Des	cription:		Service to disconnect all headless devices after they have registered							
Туре	e:		Web-based Au	thenticati	on					
Stat	us:		Enabled	Enabled						
Mon	itor Mode:		□ Enable to monitor network access without enforcement							
Mor	e Options:		Authorizatio	n 🗌 Pos	ture Compliance	2				
						Service Rule				
Mato	hes 🔿 ANY	or 🔍 A	ALL of the following	g conditio	ns:					٦
	Туре			Name		Operator	Value			
1.	Host			Check	Гуре	EQUALS	Authentication		1 T	
2.	Application	:ClearPa	SS	Page-I	lame	BELONGS_TO	mac_create,	actrac_create	à Ť	
з.	Click to add	d								

Now we'll add mar\_create\_2 to it as well but since we can't edit the system default service, we'll create a copy.

#### Services - Copy\_of\_[Device Registration Disconnect]

Su	nmary Se	rvice	Authentication	Roles	Enforcement				
Serv	ice:								
Nam	Name: Copy_of_[Device Registration Disconnect]								
Desc	cription: Service to disconnect all headless devices after they have registered								
Туре	:		Web-based Aut	henticatio	n				
Statu	is:	s: Enabled							
Moni	tor Mode:		Disabled						
More	Options:		-						
						Service Rule			
Match	ALL of the f	ollowing	conditions:						
	Туре			Na	ime	Operator	Value		
1.	Host			Ch	eckType	EQUALS	Authentication		
2. Application:ClearPass Page-Name BELONGS_TO mac_create,mactrac_create			mac_create,mactrac_create,mac_create_2						

### 8.4 Testing the Self Registration workflow

So now the user with the device that needs to be registered for MPSK, connects to "Guest" SSID it gets redirected to the new self-registration page we have configured.

aru		TUAL   InstantVC										Q
	Overview	Wireless (8) Wire	ed (0)									
	Networks	Name	IP Address	MAC address	OS	ESSID	Access Point	Channel	Туре	Role	IPv6 Address	Signal
	Access Points	-	192.168.1.128	84:38:38:46:a9:39	Android	SG1	BLDG-A-ATV1	36E	AC	S5-Remote	fd14:5f94:8156:26	27
	Clients	DESKTOP-SOID	192.168.1.133	f0:d5:bf:4b:67:11	Win 10	SG1	BLDG-A-ATV1	36E	AC	ShiziLaptop		48
		a4d1d25f3252	192.168.1.120	a4:d1:d2:5f:32:52		Guest	BLDG-A-ATV1	36	AN	External CP	fd14:5f94:8156:26	40

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

ar	U	b	a

ClearPass Guest

Operator Login							
Username:	student1						
Password:	Password:						
	Log In						

After successful authentication the user get redirected to the registration page.

✓ Last successful login from 192.168.1.120 on Monday, 06 May 2019, 3:32 PM

No failed attempts since last successful login

Please complete the form below to gain access to the network.

	MPSK-Registration				
* MAC Address:	A1:d1:d2:5f:32:52 MAC address of the device.				
Sponsor's Email:	ariyap@hpe.com Email of the person sponsoring this account.				
* Device Name:	MyNewDev Name of the device.				
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:	Students-Devs Role to assign to this account.				
Notes:					
* Terms of Use:	$\blacksquare$ I am the sponsor of this account and accept the terms of use				
	treate الم				
* 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. Note that there is no Login button on the receipt page as shown below.

aruba	ClearPass Guest
The details for your guest account are shown below.	
Self-Registration Receipt	

Sponsor's Name:	student1					
Sponsor's Email:	ariyap@hpe.com					
Guest's Name:	MyNewDev					
Account Username:	S A4-D1-D2-5F-32-52					
Activation Time:	Monday, 06 May 2019, 3:52 PM					
Expiration Time:	Monday, 13 May 2019, 3:52 PM					
Wi-Fi Password:	Generated					

The email that the user receives is as shown below, note that it has the correct SSID that they need to connect to.



Once they know their unique PSK, they'll connect to the MPSK SSID as shown below.

student1	192.168.1.120	a4:d1:d2:5f:32:52	iPad	ArubaMPSK	BLDG-A-AT	V1 36	AN	Students-D	fd14:5f94:8156:26	36 52
Shizzys-iPhone	192.168.1.131	b8:41:a4:74:e5:46	iPhone	SG1	BLDG-A-AT	V1 36E	AC	SG1	fd14:5f94:8156:26	32 468
Overview Clie	ent Match AppRF									
Info						RF Dashboard				
Name	student1					Client	5	Signal	Spee	d
IPv6 Address	fd14:5f94:8156:2600:8e	1:313a:3231:2cf5				student1		al.		
IP Address	192.168.1.120	MAC addres	ss <mark>a4:d1</mark>	l:d2:5f:32:52		Access Point	Utilizatio	n	Noise	Errors
OS	iPad	ESSID	Arub	aMPSK		BLDG-A-ATV1	_		_	_
OS Access Point	iPad BLDG-A-ATV1	ESSID Channel	Arub 36	aMPSK		BLDG-A-ATV1	_		_	

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

#### Here are the relevant Access tracker request IDs for the device registration.

3.	192.168.1.94	WEBAUTH	A4-D1-D2-5F-32-52	Copy_of_[Device Registration Disconnect]	ACCEPT	2019/05/06 15:52:44
4.	192.168.1.94	Application	student1	Guest Operator Logins	ACCEPT	2019/05/06 15:52:11

#### And the Event Viewer

aruba	ClearPass Policy Manager							
Dashboard O	Monitoring » Event Viewer							
Monitoring 📀	Event Viewer							
Control Contr	The Ev here.	rent Viewer provides repor	ts about system-level event	ts. All attempted upgrade, p	atch, and hotfix installations	are logged	Select Server: poc.cle	
Analysis & Trending	#	Source	Level	Category	A	ction	Timestamp 🔹	
- System Monitor	1.	Admin UI	INFO	Email Successful	N	one	May 06, 2019 15:52:55	
	2.	Guest UI	INFO	Logged in	N	one	May 06, 2019 15:52:11	
	3.	ClearPass Updater	INFO	System Event Details			S (	
— Jata Filters	4.	Admin UI	INFO	-				
– 🦉 Blacklisted Users	5.	Guest UI	INFO	Source	Admin UI			
	6.	Guest UI	INFO	Level	INFO			
	7.	Guest UI	INFO	Category	Email Successful			
	8.	ClearPass Updater	INFO	Action	None		c	
	9.	Admin UI	INFO	Timestamp	May 06, 2019 15:52:55 AE	ST		
	10.	Guest UI	INFO	Description	From: ariyap@aruba.com			
	11.	ClearPass Updater	INFO		Mail Subject: MPSK-Receip	Receipt		
	12.	ClearPass Updater	INFO				(	
	13.	ClearPass Updater	INFO					
	14.	ClearPass Updater	INFO				Close	
	4.5	Current UT	THEO	I see al in			Mary 06 2010 10:22:	

For troubleshooting you can also check the "Application Log" on the ClearPass Guest side. You should get three transactions as shown below



### Application Log

The events and messages generated by this application are logged here. For in-depth information about an event, click on it.

1 Quick Help		💎 Filter		Export
Keywords:	Enter keywords to filte	er the logs. Use `	-' to negate and qu	iotes to group keywords.
≂ Time	IP	User	Severity	Message
2019-05-06 15:52:5	5 192.168.1.120	student1	🚺 info	Guest receipt was sent to ariyap@hpe.com
2019-05-06 15:52:4	4 192.168.1.120	student1	info	Successfully created device A4-D1-D2-5F-32-52 in database MPSK: Yes Account will expire at 2019-05-13 15:52:44 Account role is Students-Devs Account sponsor is student1 Created by student1 from 192.168.1.120 User DB: ClearPass Policy Manager
2019-05-06 15:52:1	1 192.168.1.120	student1	🚺 info	Operator login: student1