1 Table of Contents

Table of Contents

1.1 Revision History

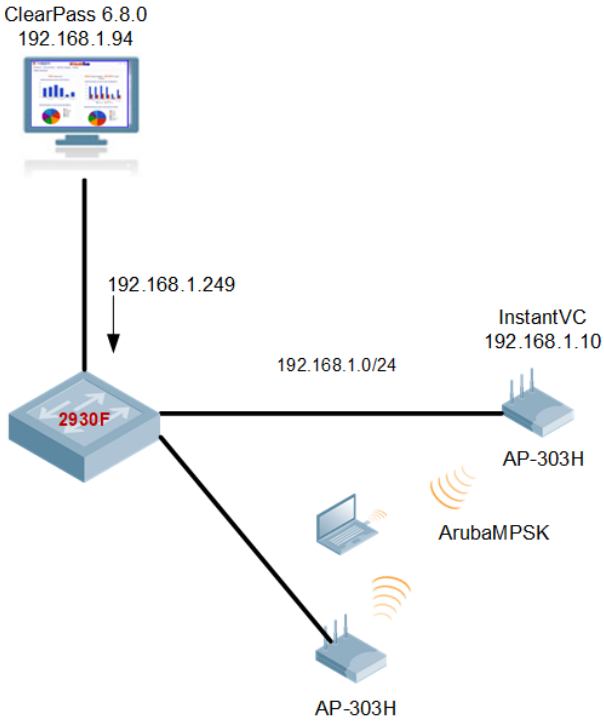
DATE	VERSION	EDITOR	CHANGES
28 April 2019	0.1	Ariya Parsamanesh	Initial creation
05 April 2019	0.2	Ariya Parsamanesh	Prepopulated MAC address workflow
17 Jul 2019	0.3	Ariya Parsamanesh	Added the Instant 8.5.0.1

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

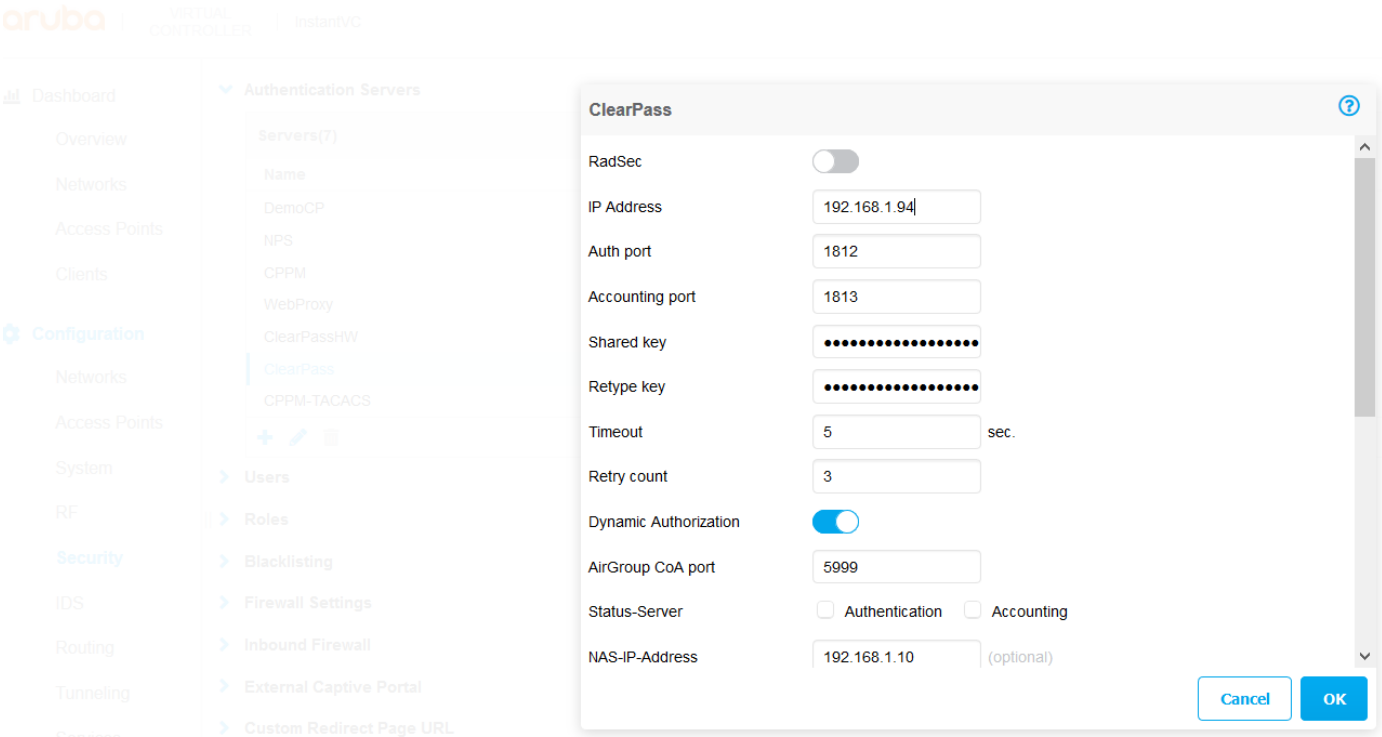
- Before connecting a device to a MPSK based SSID, the user registers the device on a ClearPass Policy Manager guest-registration or device-registration webpage
- The user receives a device-specific or group-specific MPSK passphrase through the email
- The user then connects their device with their unique 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.

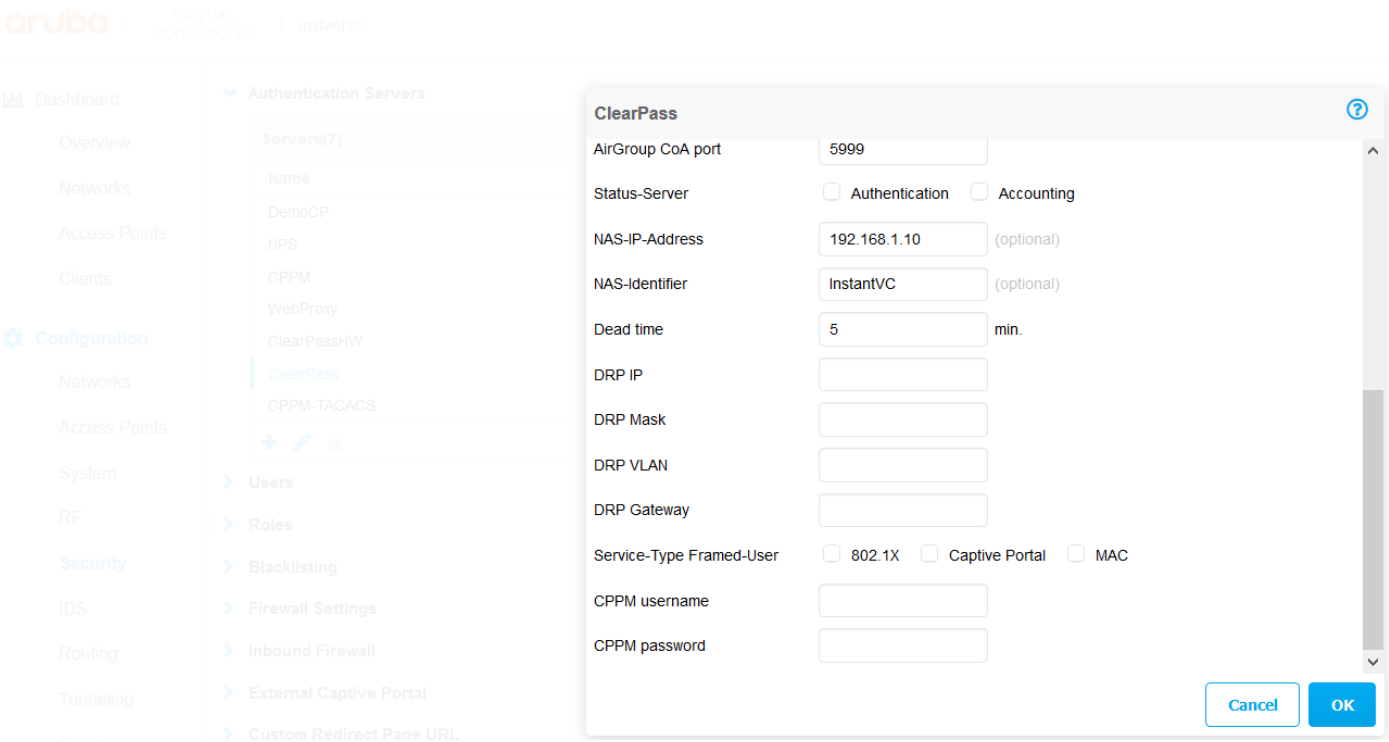
3 Instant AP Configuration

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

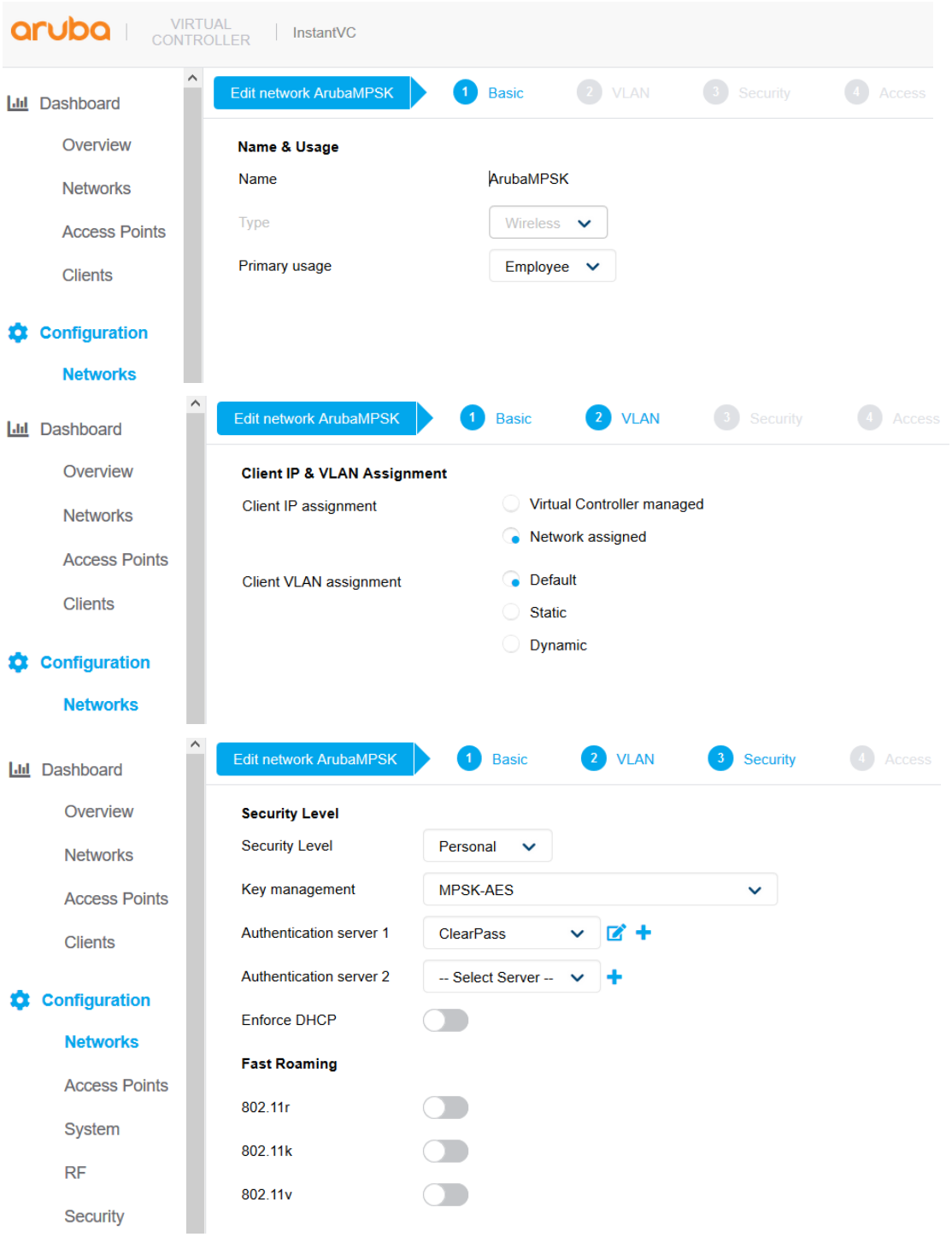
First we need to configure ClearPass as the authentication server.

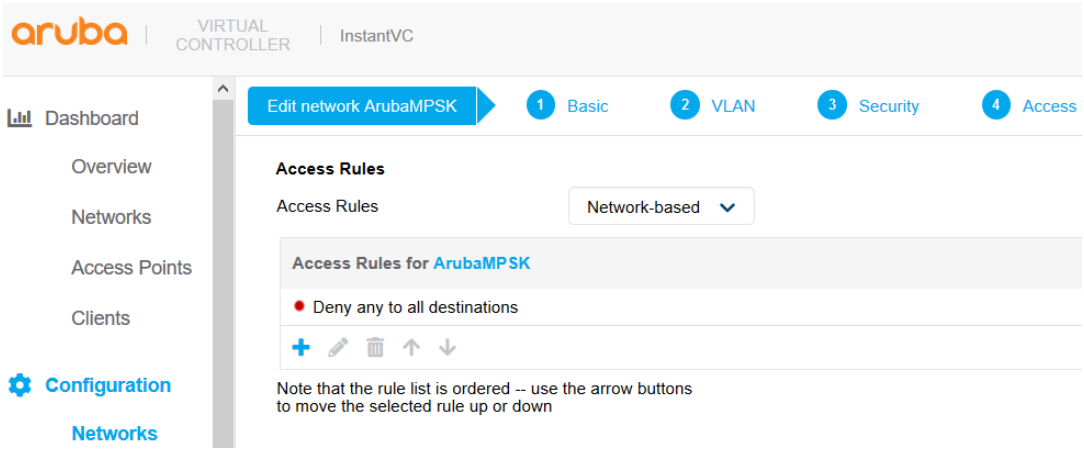




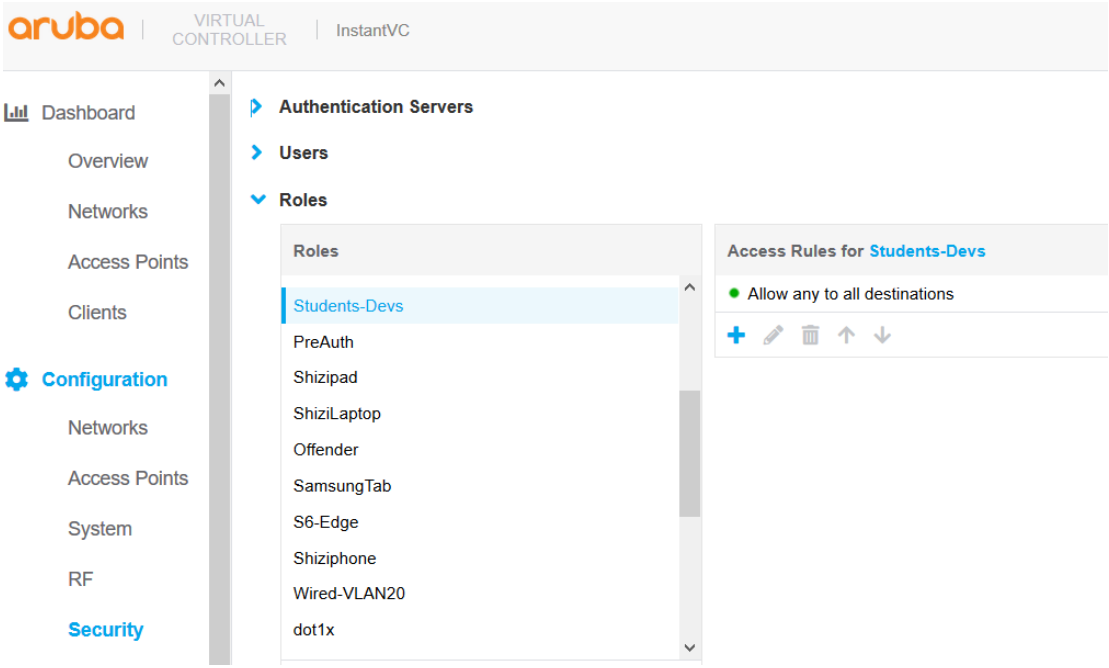
3.2 Aruba Instant MPSK Configuration

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





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.

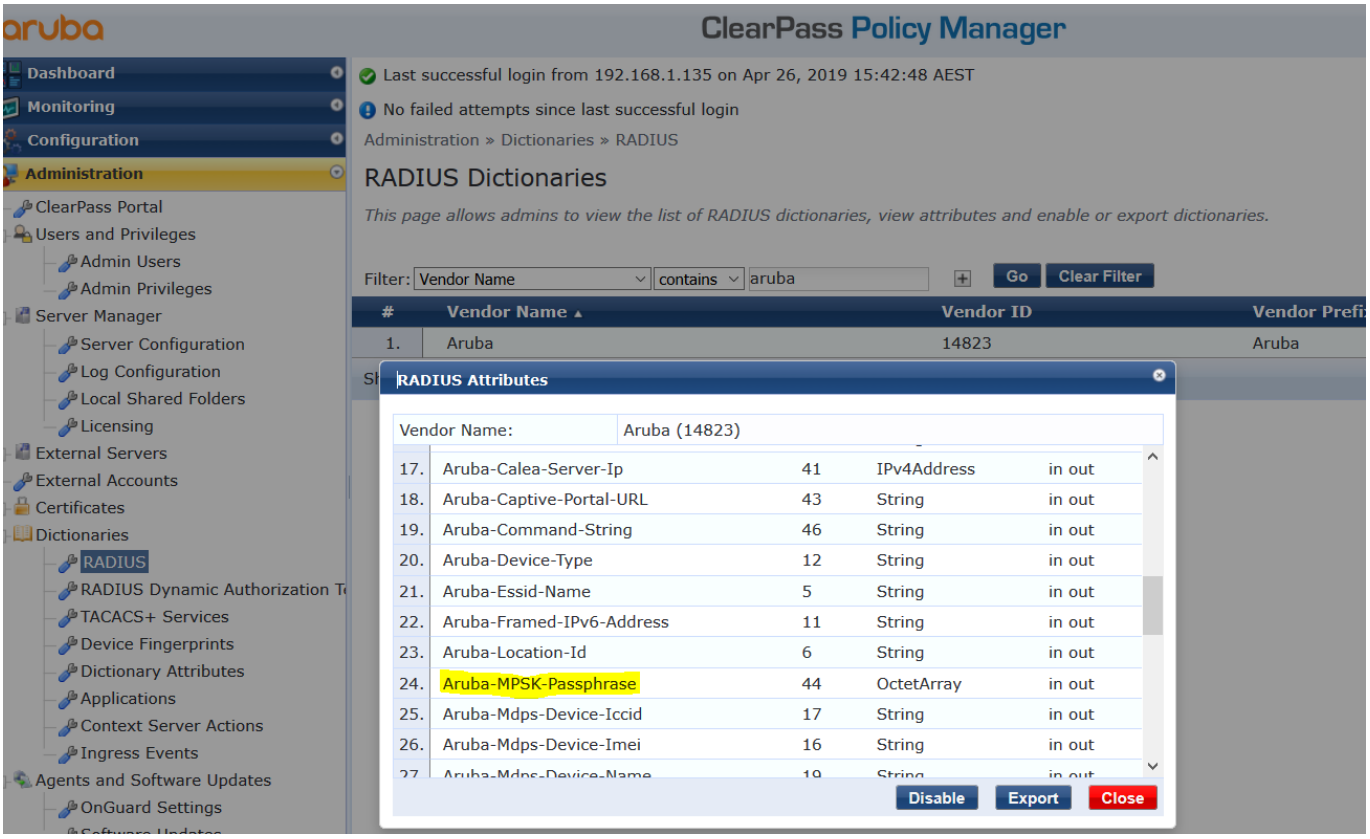


4 ClearPass Configuration

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.

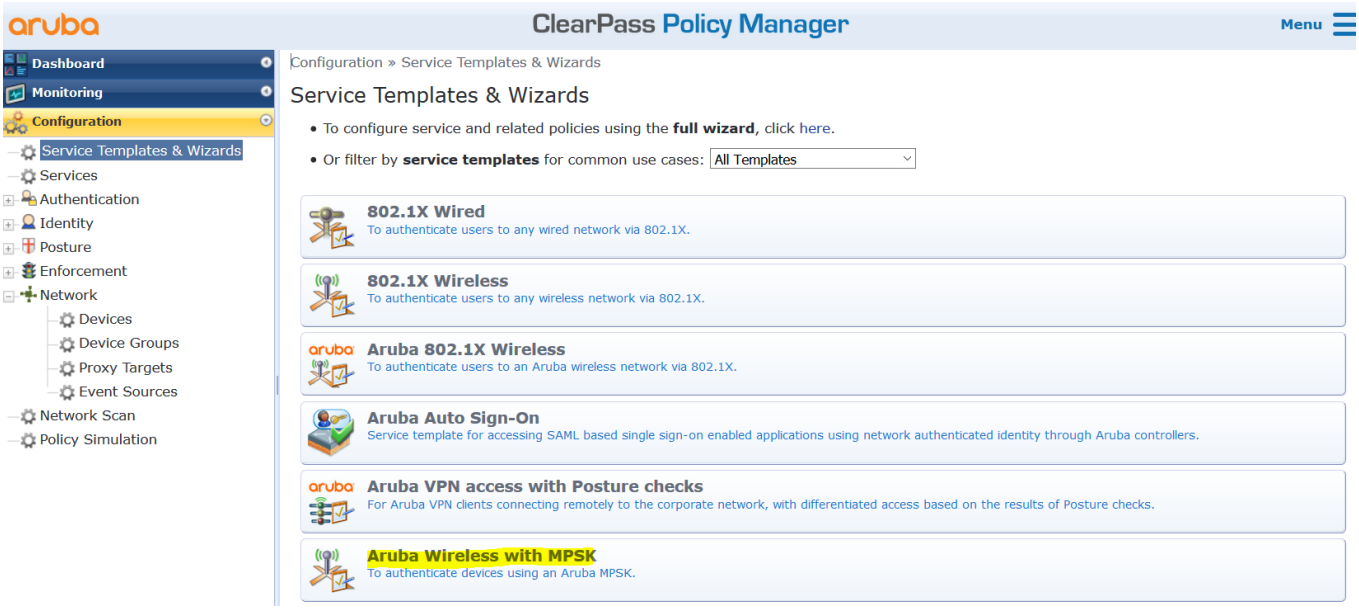
4.1 RADIUS Dictionary

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

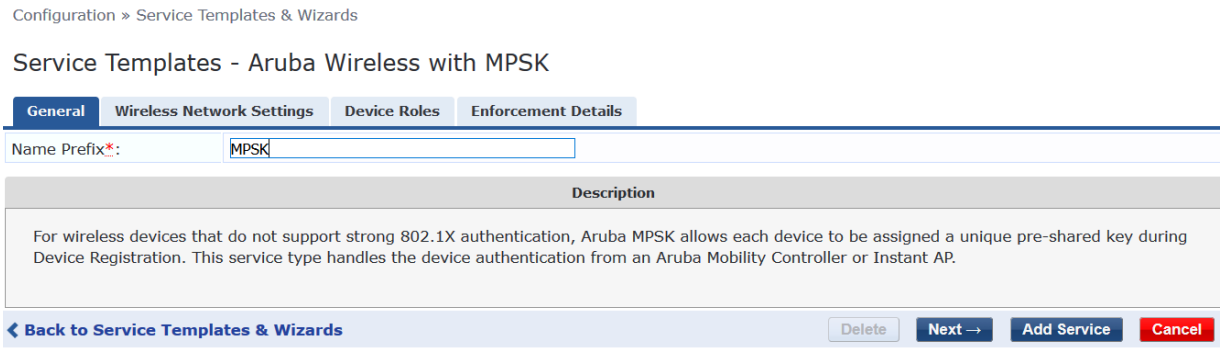


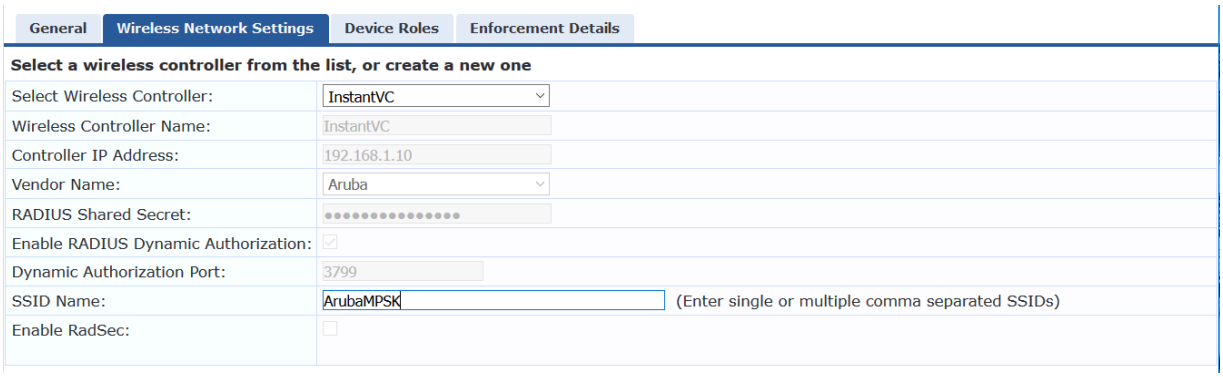
4.2 Service Template

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

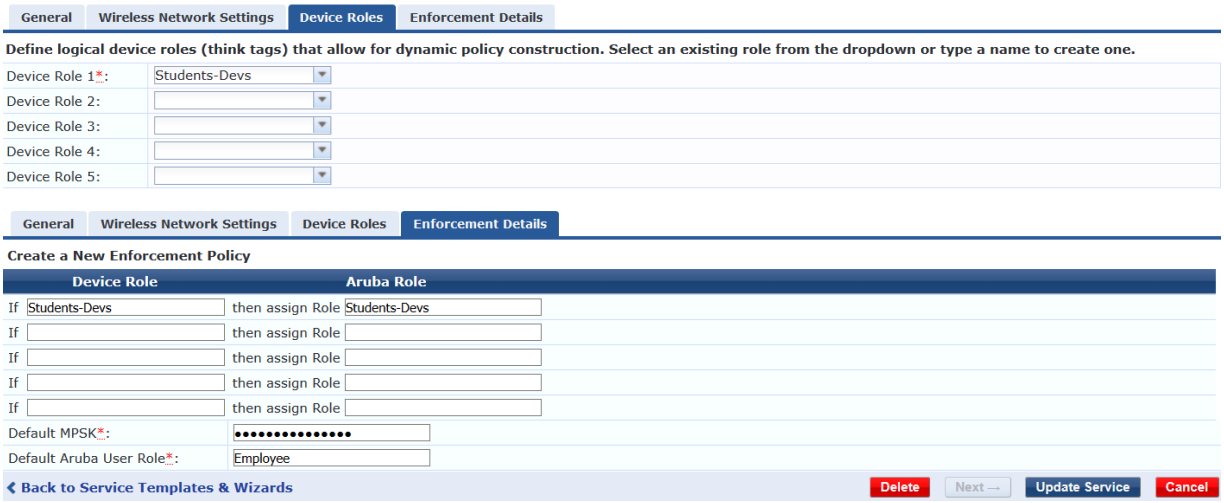


Using the Aruba Wireless with MPSK wizard.





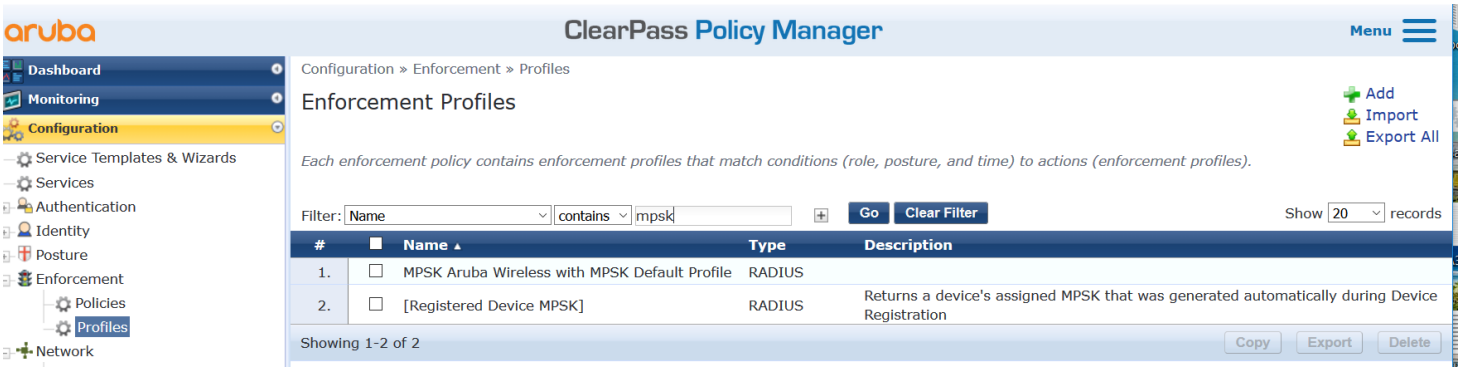
Do not select RadSec as it is not supported for MPSK.



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.

4.3 Enforcement Profiles

Here are the two enforcement profiles that were created.



Enforcement Profiles - MPSK Aruba Wireless with MPSK Default Profile

Summary | Profile | Attributes

Profile:

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

Attributes:

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

Enforcement Profiles - Aruba User Role – Students-Devs

Summary | Profile | Attributes

Profile:

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

Attributes:

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

Enforcement Profiles - [Registered Device MPSK]

This is a default profile.

Summary | Profile | Attributes

Profile:

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

Attributes:

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

4.4 Enforcement Policy

This is the enforcement policy that got created.

Enforcement Policies - MPSK Aruba Wireless with MPSK Enforcement Policy

Summary | Enforcement | Rules

Enforcement:

Name:	MPSK Aruba Wireless with MPSK Enforcement Policy
Description:	
Enforcement Type:	RADIUS
Default Profile:	MPSK Aruba Wireless with MPSK Default Profile

Rules:

Rules Evaluation Algorithm:	First applicable

	Conditions	Actions
1.	(Tips:Role *EQUALS* 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

Summary | Policy | Mapping Rules

Policy:

Policy Name:	MPSK Aruba Wireless with MPSK Role Map
Description:	
Default Role:	[Other]

Mapping Rules:

Rules Evaluation Algorithm:	Evaluate all

	Conditions	Role Name
1.	(Authorization:[Guest Device Repository]:Device Role ID *EQUALS* 3008)	Students-Devs

4.6 ClearPass Service

And here is the complete serviced that was configured.

Services

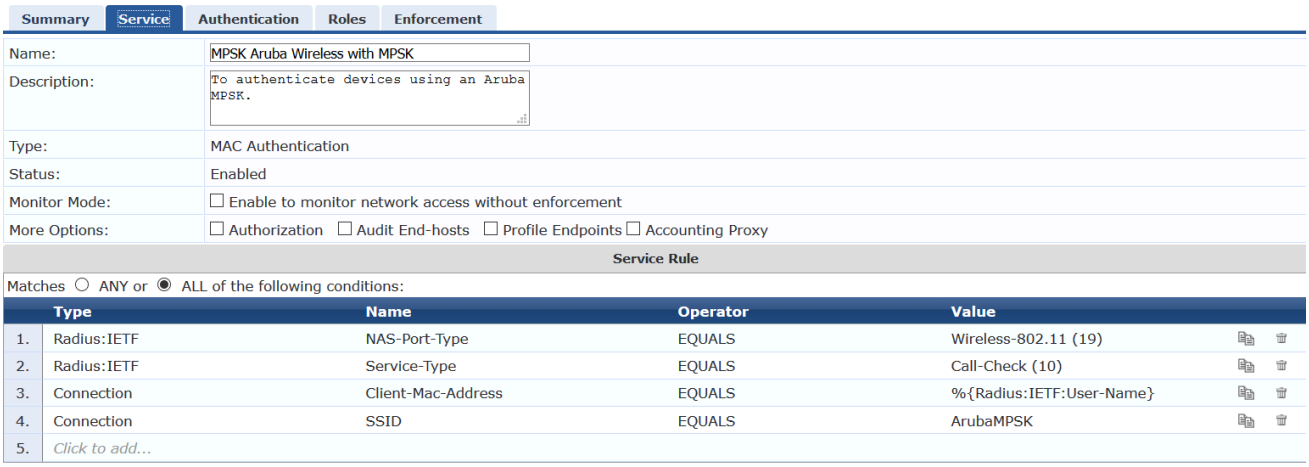
Add | Import | Export All

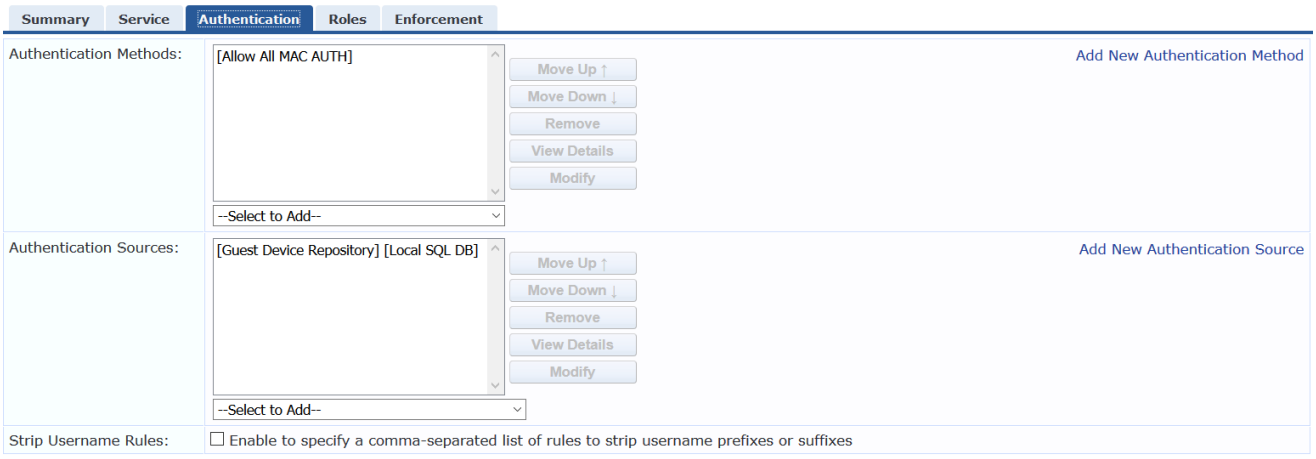
This page shows the current list and order of services that ClearPass follows during authentication and authorization.

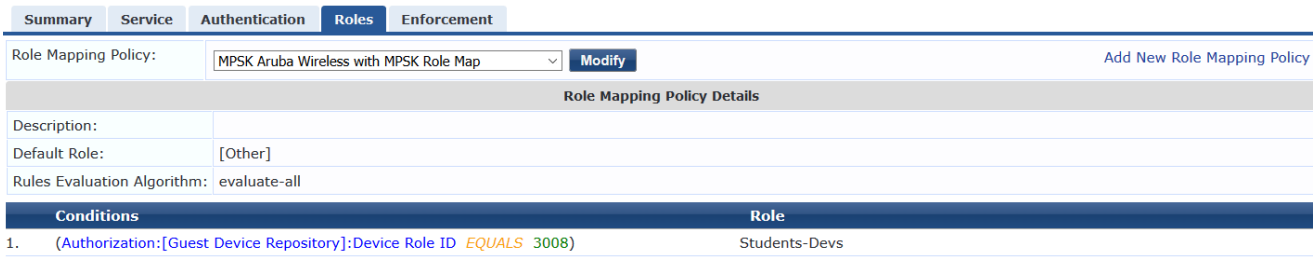
Filter: Name | contains | Go | Clear Filter | Show 20 records

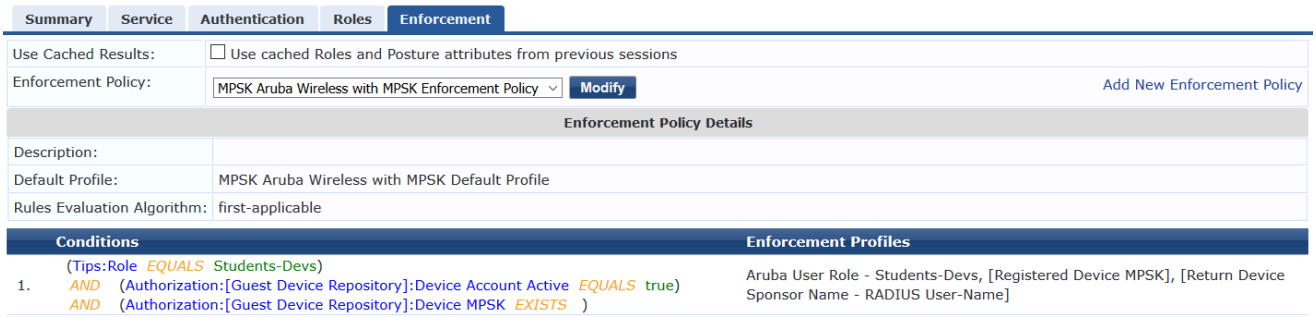
#	Order	Name	Type	Template	Status
1.	1	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	
2.	2	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	
3.	3	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	
4.	4	[Guest Operator Logins]	Application	Aruba Application Authentication	
5.	5	[Insight Operator Logins]	Application	Aruba Application Authentication	
6.	6	Lab Aruba 802.1X Wireless	RADIUS	Aruba 802.1X Wireless	
7.	7	Ariya WiredAOS-S Dot1x	RADIUS	802.1X Wired	
8.	8	Ariya Wired-AOS-S MAC Auth	RADIUS	MAC Authentication	
9.	9	Ariya Wired-AOS-S MAC Auth-DUR	RADIUS	MAC Authentication	
10.	10	Ariya Wired-AOS-S GuestWebAuth	WEBAUTH	Web-based Authentication	
11.	11	Ariya Wired-AOS-S GuestWebAuth-DUR	WEBAUTH	Web-based Authentication	
12.	12	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	
13.	13	MPSK Aruba Wireless with MPSK	RADIUS	MAC Authentication	

Showing 1-13 of 13 | Reorder | Copy | Export | Delete





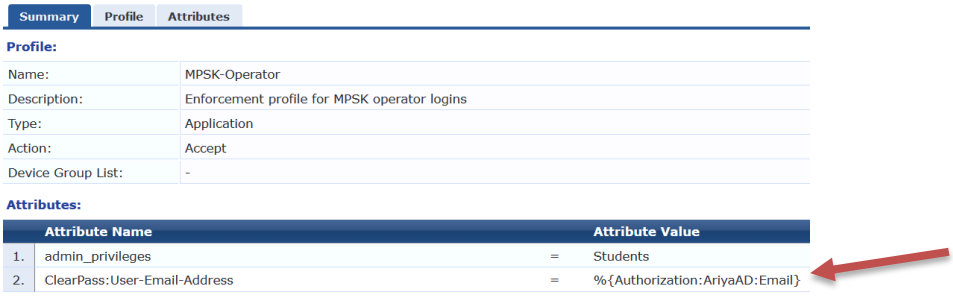




4.7 Operator Service

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.

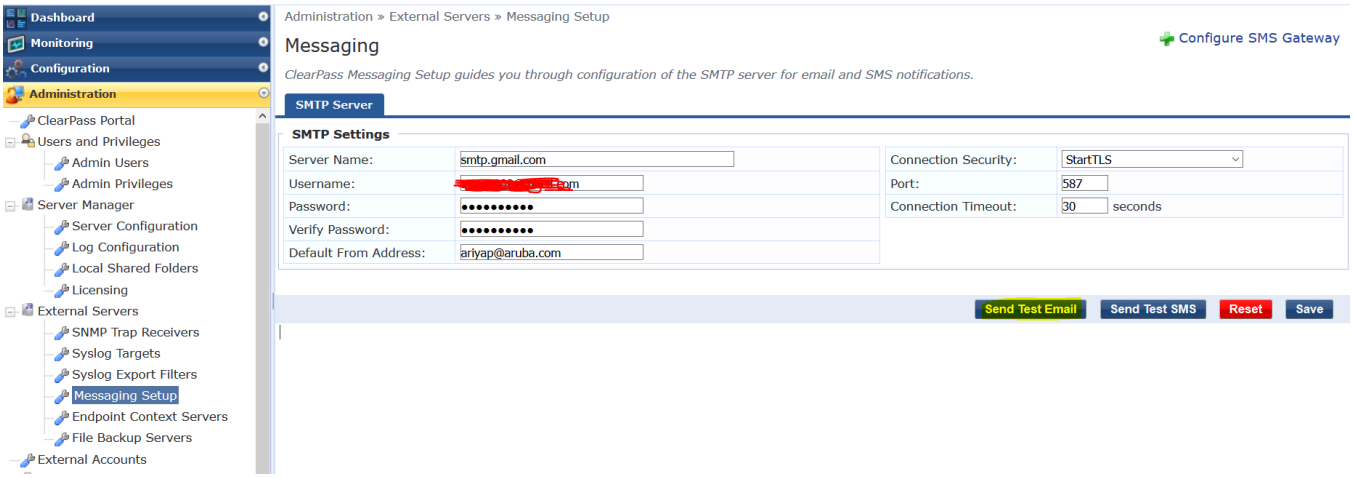
Enforcement Profiles - MPSK-Operator



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



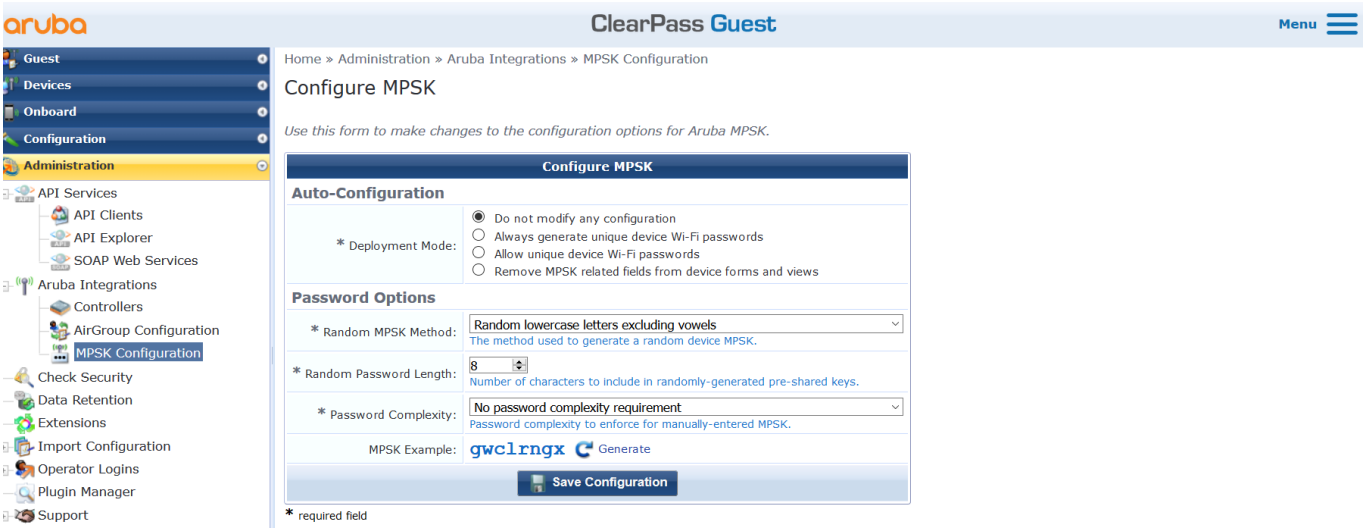
You can also send the test email by clicking on the "Send Test Email" button ensuring that all is good.

5 ClearPass Guest

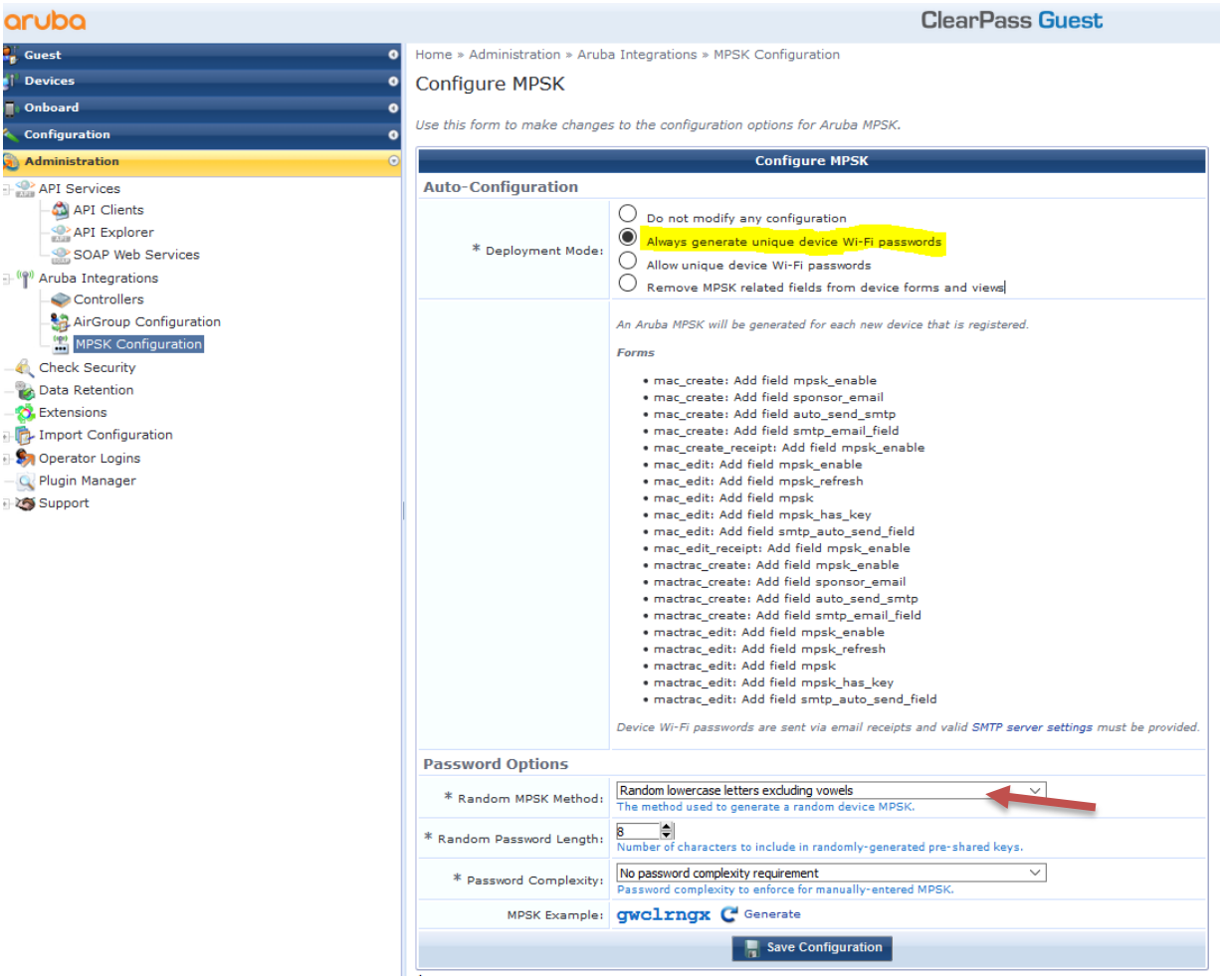
Here we'll cover the ClearPass Guest configurations that are needed. You can configure the method, complexity, and length of the MPSK passwords, and whether they will be generated or user-created.

5.1 MPSK Configuration

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



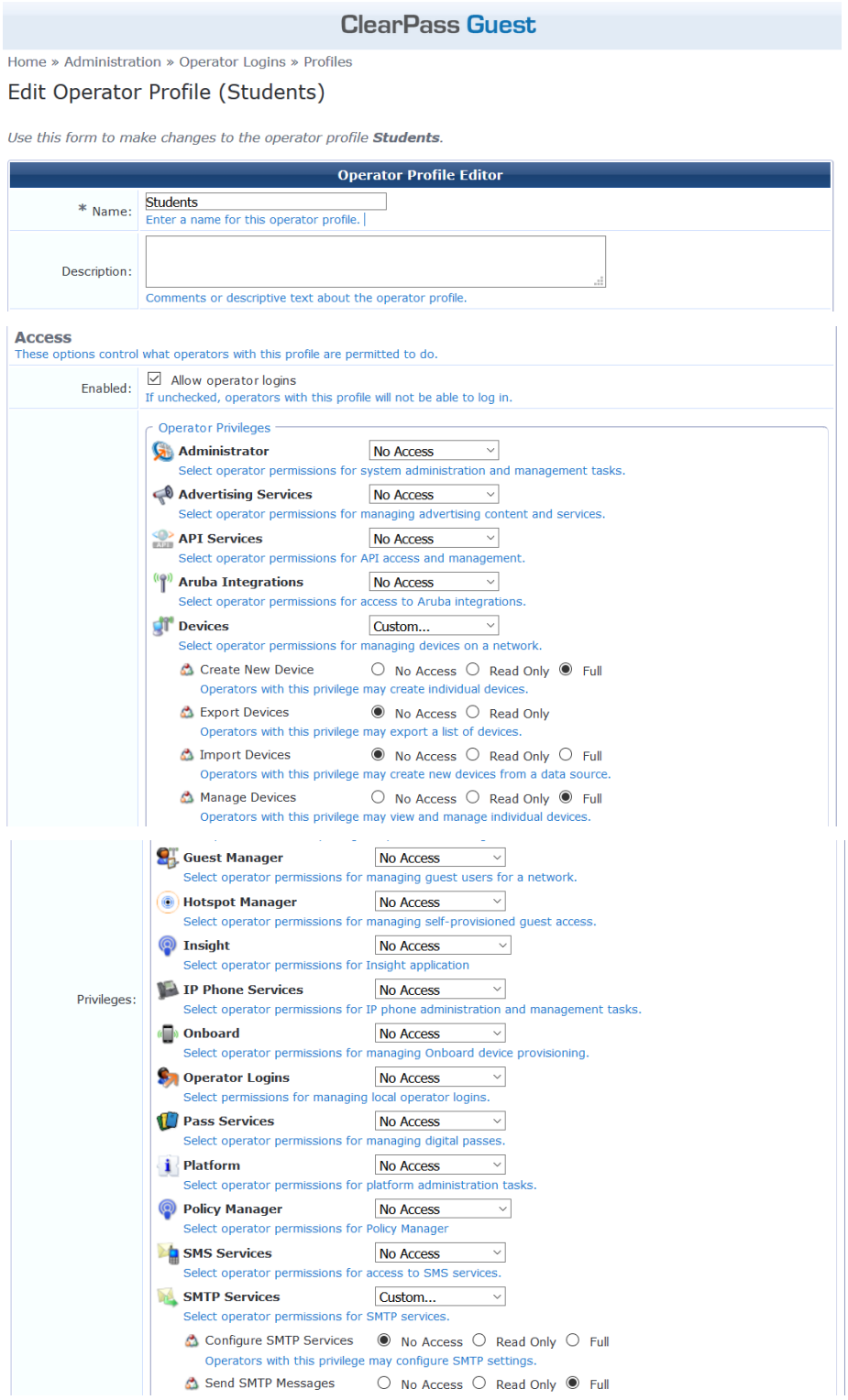
In most of the cases "Allow generate unique WiFi passwords" is used, Here WiFi password is referred to MPSK. This mode creates unique PSK for the user since most of the users don't know if they need it or not or can easily get confused. The next option "allow unique device WiFi passwords" provides a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

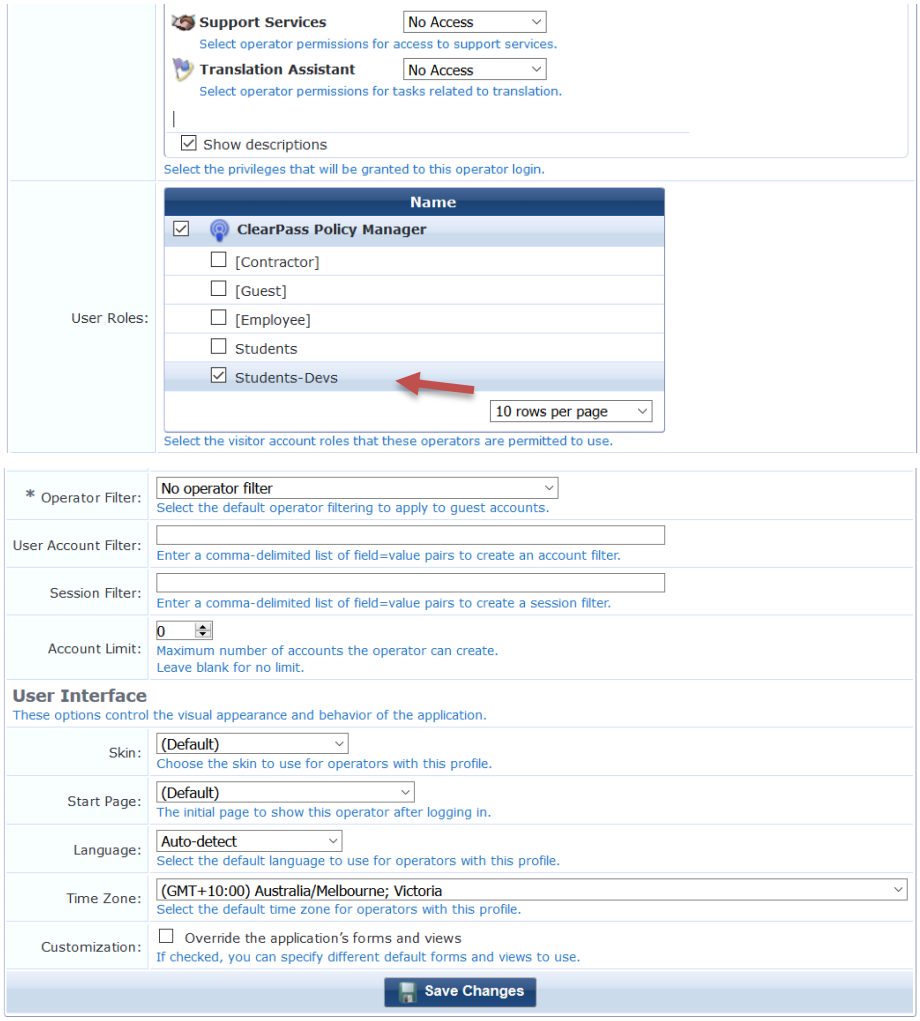


As seen above you can also choose the MPSK complexity and length but by default is minimum 8 and uses lowercase letters excluding vowels.

5.2 Operator Profile

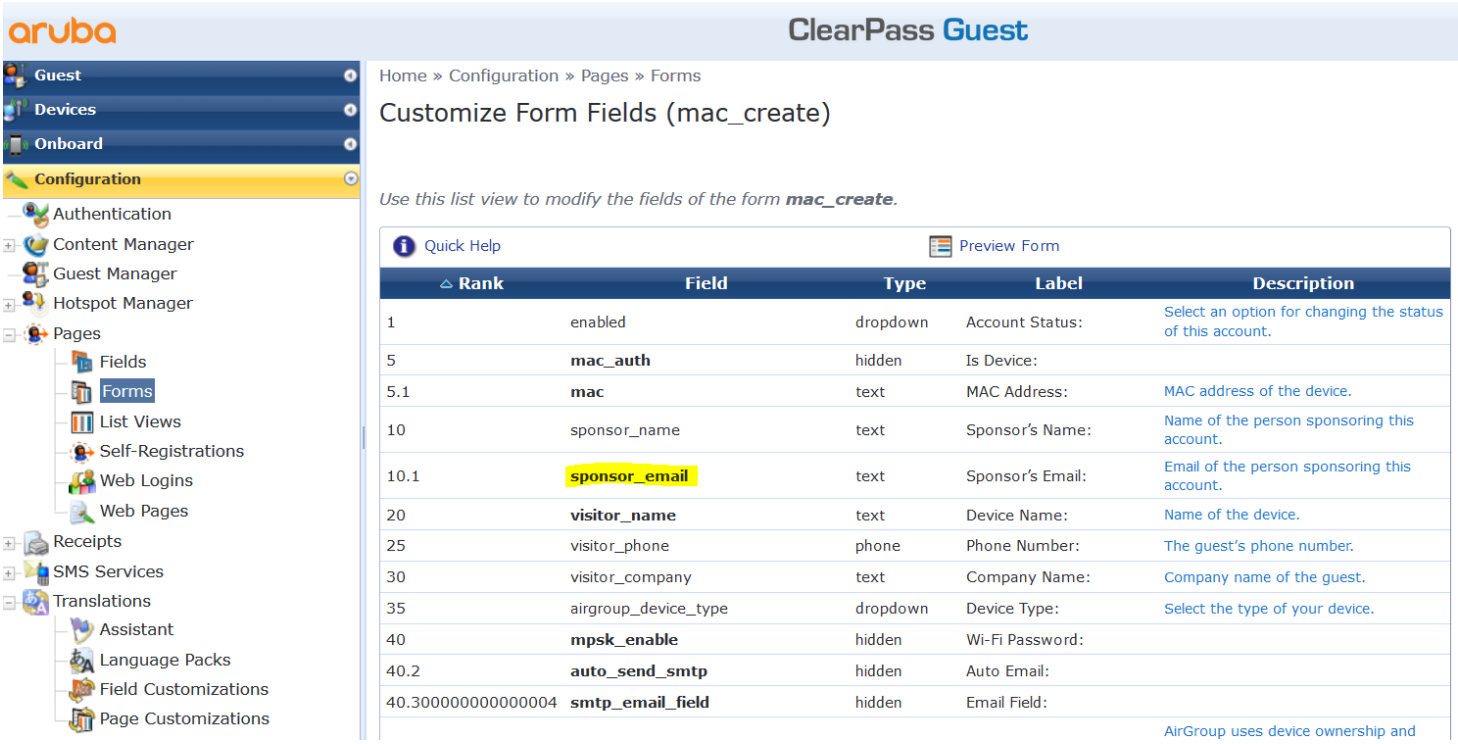
Operator profiles are used for a user who is able to log in to ClearPass Guest. You can have different operator profile with different level of access. Here we need one for the students to be able to login and register their devices.





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.



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

The initial value should be as shown below.

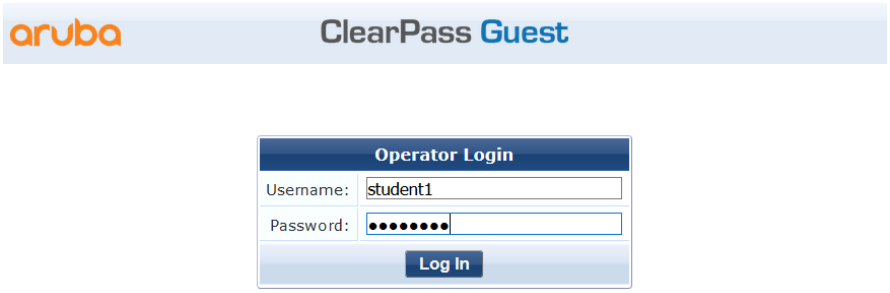
```
array (  'generator' => 'GeneratorFromSession',  'generator_args' =>   array (    0 =>
'userauth_user',    1 => 'User-Email-Address',  ),)
```

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.

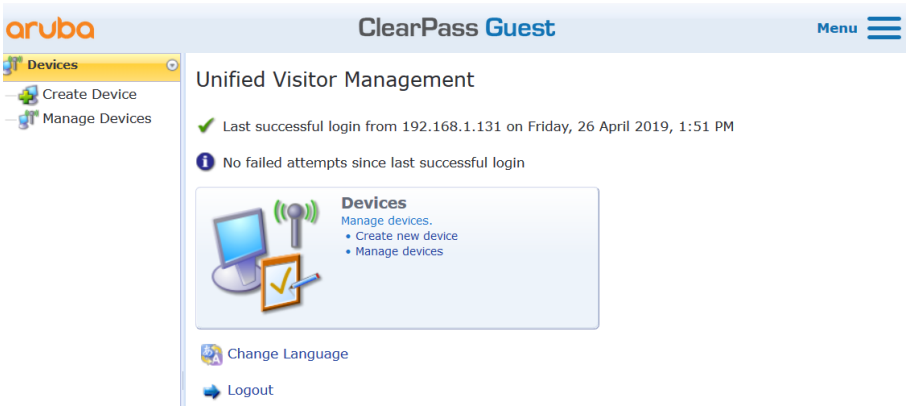
6 Testing

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”

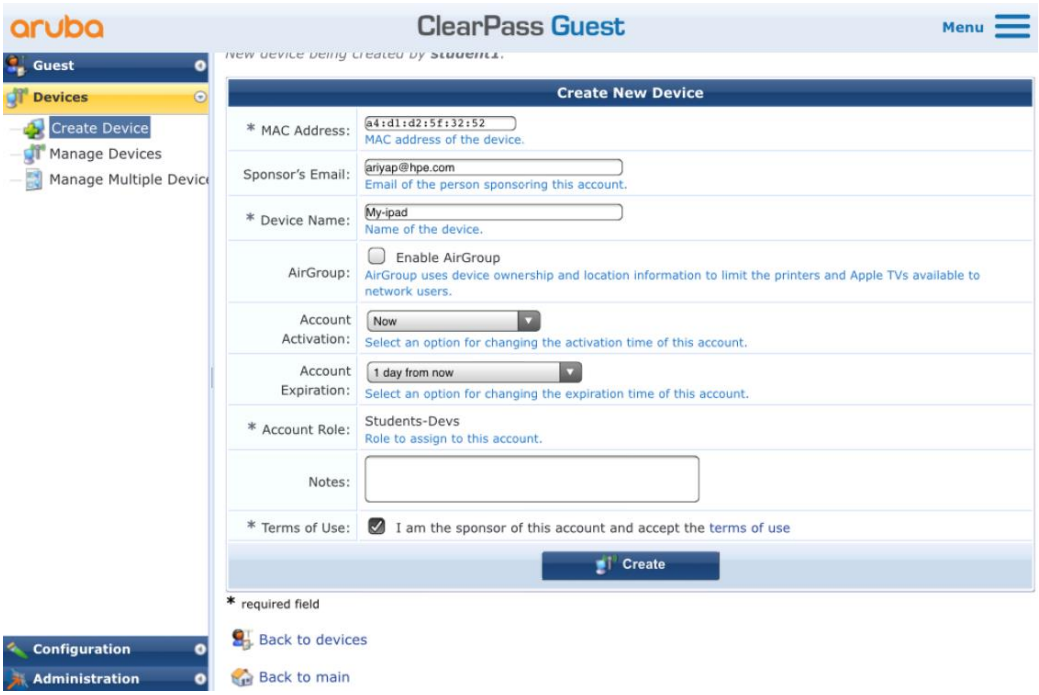
6.1 Device Registration



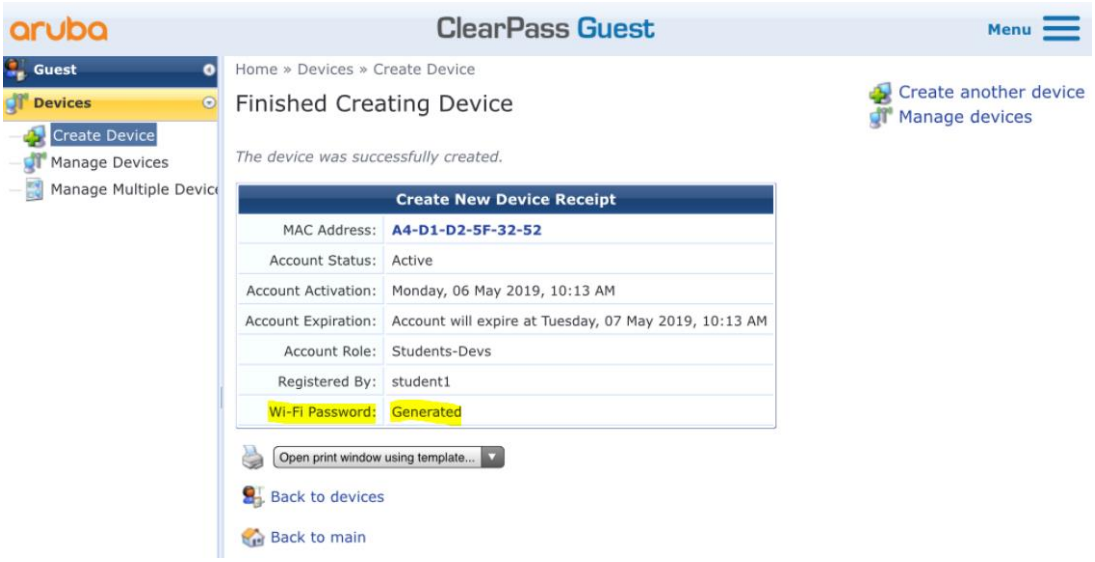
Upon successful login, the user will see this page. This is a default page and you can customise it like you would with any Guest Weblogin page.



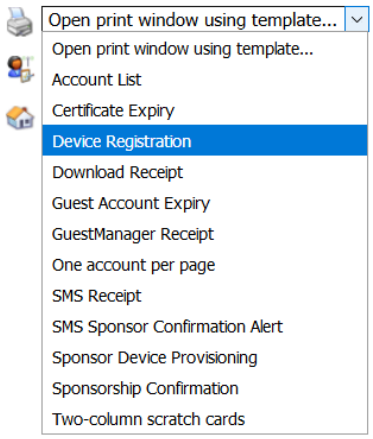
I’ll add the MAC address of my device, give it a name and choose the account expiry. Remember that account expiry can also be customised to reduce the options and you can also remove “Airgroup” field from this form.



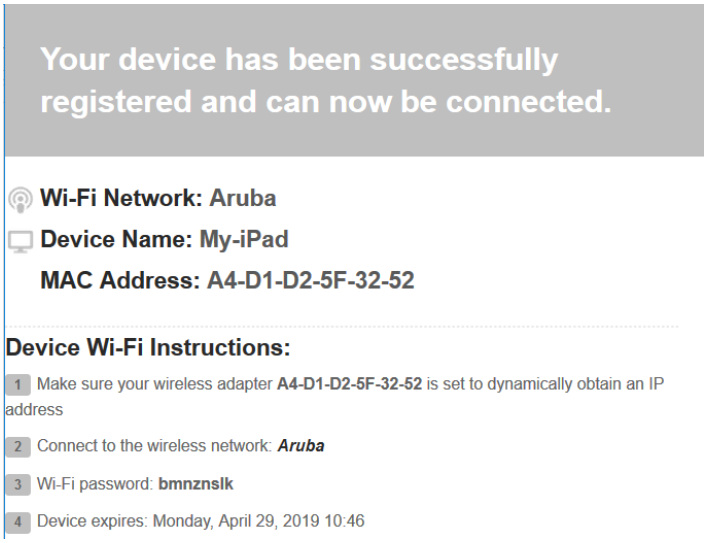
Once I have clicked on the “Create” button, I get the following screen.



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”

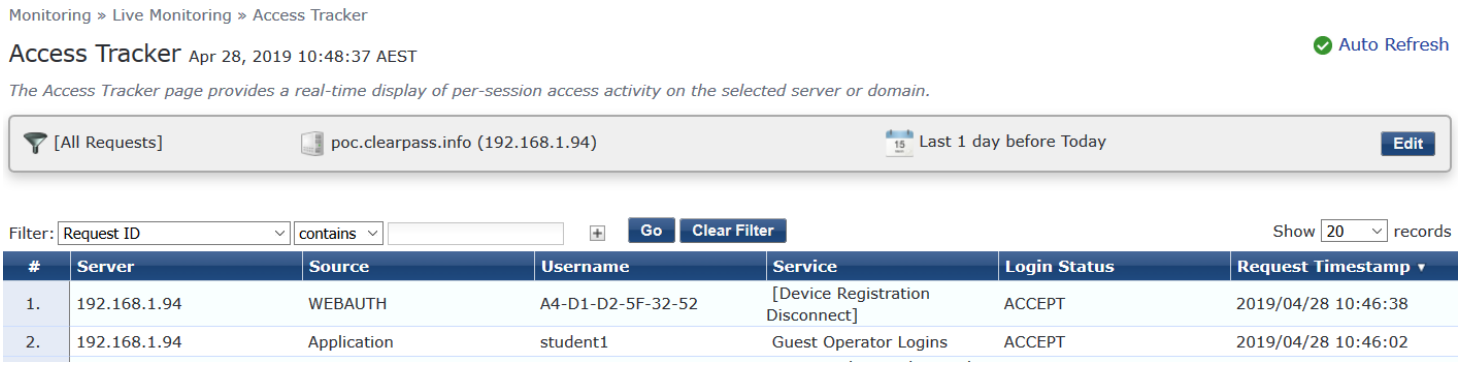


Choosing it will pop a new browser window as shown below.



6.2 ClearPass Access Tracker Operator Login

So from Access tracker we see the following two Auth Requests



#	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 | Input | Output

Login Status:	ACCEPT
Session Identifier:	W00000003-01-5cc4f7ca
Date and Time:	Apr 28, 2019 10:46:02 AEST
End-Host Identifier:	-
Username:	student1
Access Device IP/Port:	-:-
Access Device Name:	-
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	Guest Operator Logins
Authentication Method:	Not applicable
Authentication Source:	AriyaAD
Authorization Source:	AriyaAD
Roles:	[User Authenticated]
Enforcement Profiles:	MPSK-Operator

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

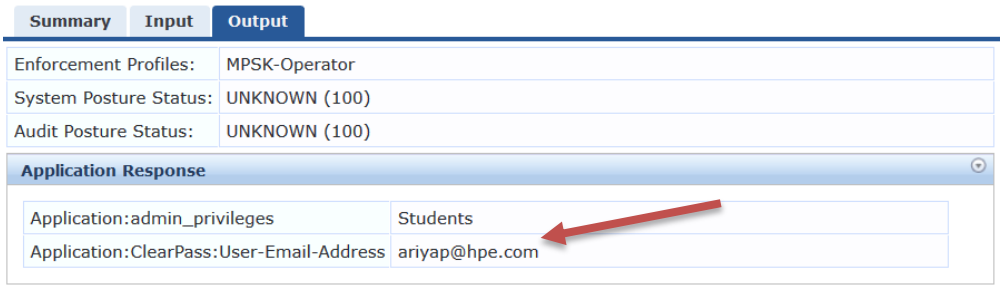
Summary | Input | Output

Username:	student1
End-Host Identifier:	-
Access Device IP/Port:	-:-

Authorization Attributes

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

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



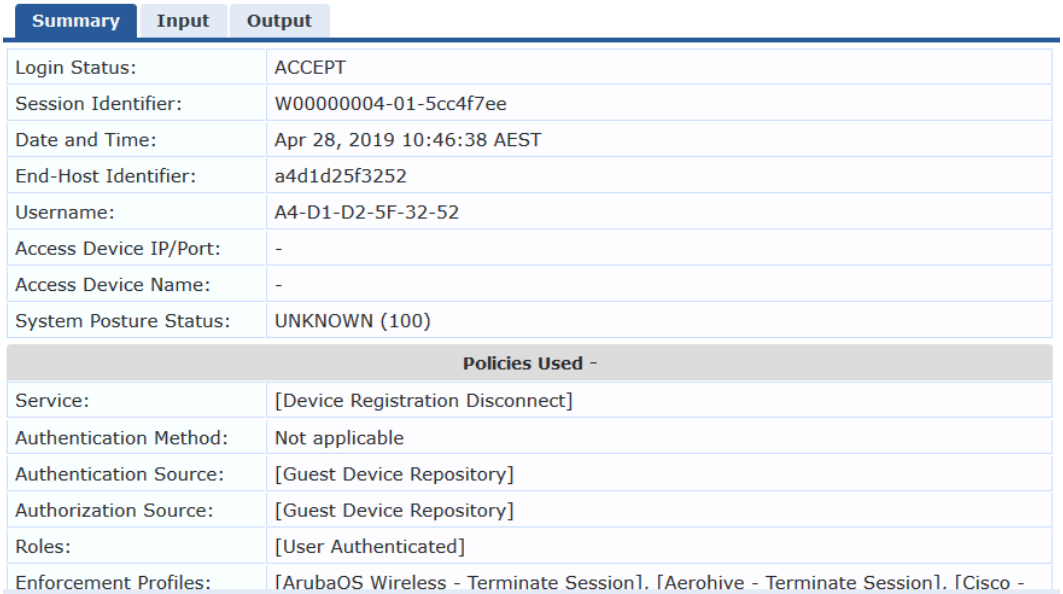
Summary | Input | Output

Enforcement Profiles:	MPSK-Operator
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

Application Response

Application:admin_privileges	Students
Application:ClearPass:User-Email-Address	ariyap@hpe.com

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

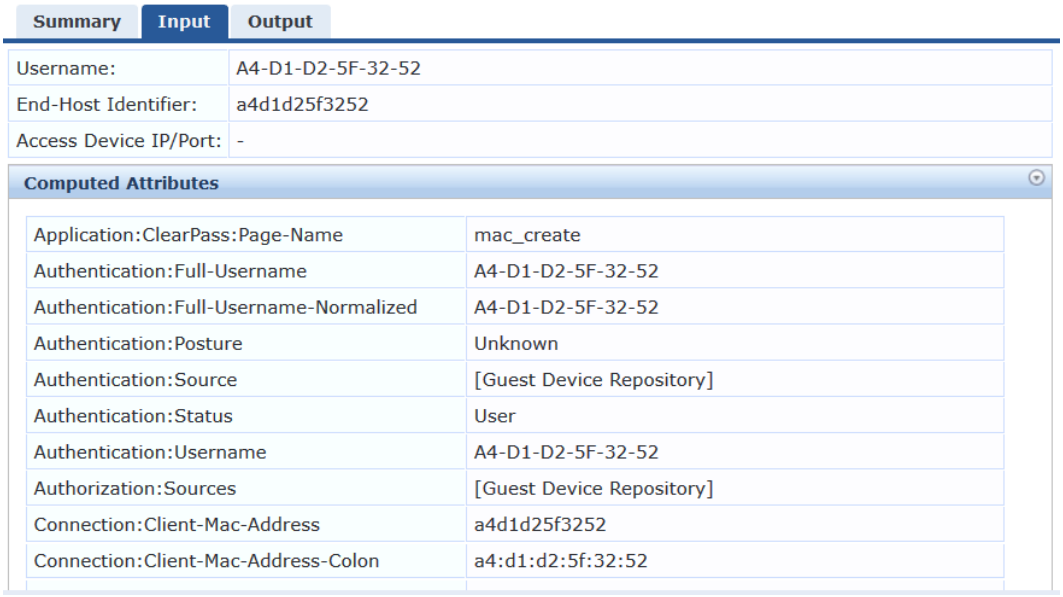


Summary | Input | Output

Login Status:	ACCEPT
Session Identifier:	W00000004-01-5cc4f7ee
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], [Cisco -



Summary | Input | Output

Username:	A4-D1-D2-5F-32-52
End-Host Identifier:	a4d1d25f3252
Access Device IP/Port:	-

Computed Attributes

Application:ClearPass:Page-Name	mac_create
Authentication:Full-Username	A4-D1-D2-5F-32-52
Authentication:Full-Username-Normalized	A4-D1-D2-5F-32-52
Authentication:Posture	Unknown
Authentication:Source	[Guest Device Repository]
Authentication:Status	User
Authentication:Username	A4-D1-D2-5F-32-52
Authorization:Sources	[Guest Device Repository]
Connection:Client-Mac-Address	a4d1d25f3252
Connection:Client-Mac-Address-Colon	a4:d1:d2:5f:32:52

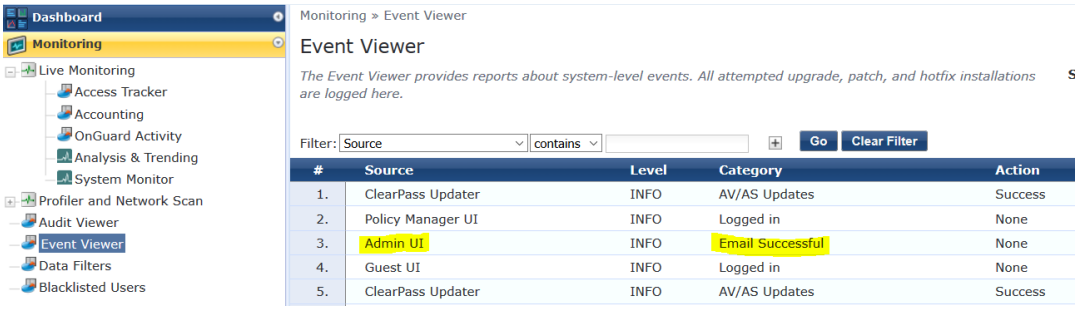
Summary | Input | Output

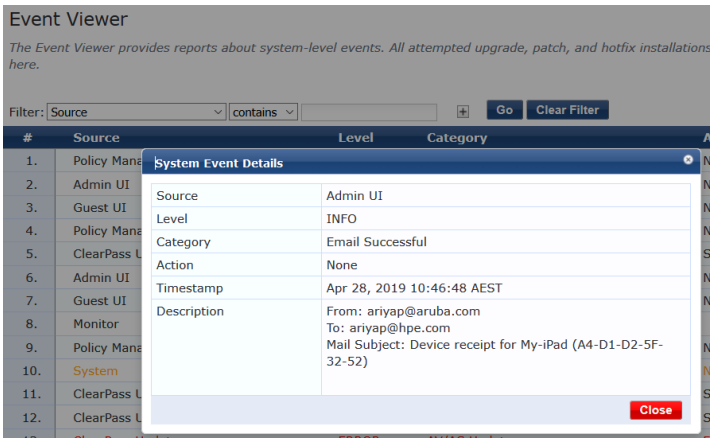
Enforcement Profiles:	[ArubaOS Wireless - Terminate Session], [Aerohive - Terminate Session], [Cisco - Terminate Session], [H3C - Terminate Session], [Juniper Terminate Session], [Motorola - Terminate Session], [Trapeze - Terminate Session], [ArubaOS Switching - Terminate Session]
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

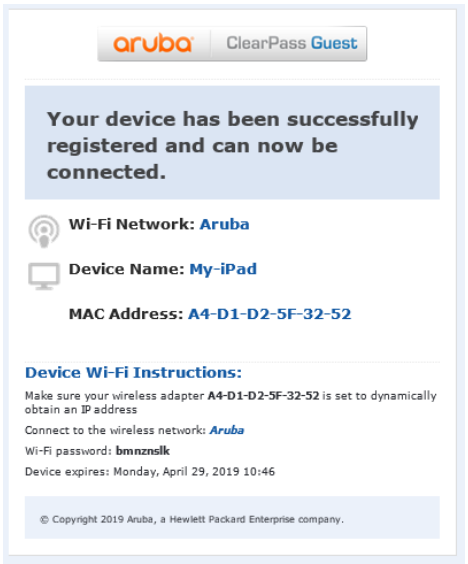
Radius:IETF:Acct-Session-Id	
Radius:IETF:Calling-Station-Id	a4d1d25f3252
Radius:IETF:NAS-IP-Address	192.168.1.10
Radius:IETF:NAS-Port	0
Radius:IETF:Service-Type	1
Radius:IETF:User-Name	student1

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



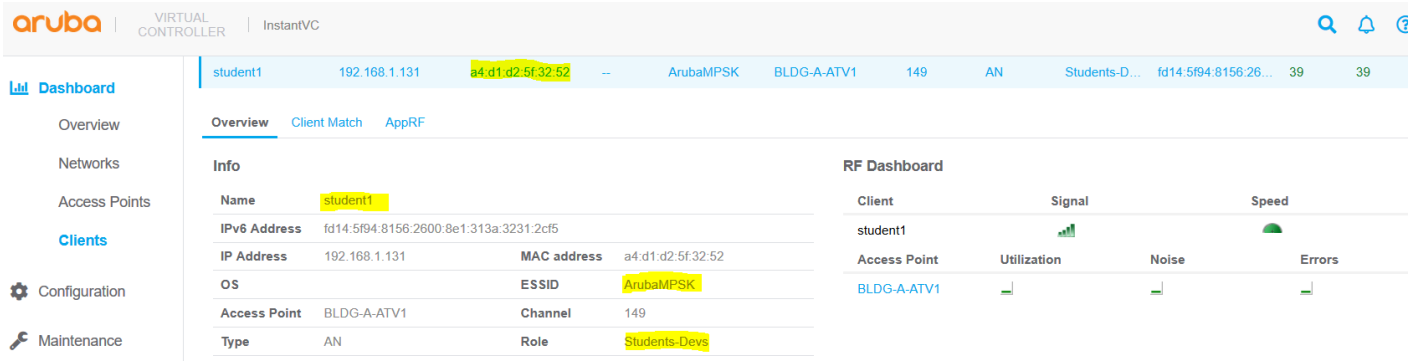


And this is the email content that was received



6.3 Aruba Instant AP

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



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

```
BLDG-A-ATV1# show ap debug auth-trace-buf mac a4:d1:d2:5f:32:52

Auth Trace Buffer
-----------------

Apr 28 10:52:55  mac-auth-req          ->  a4:d1:d2:5f:32:52  24:f2:7f:d5:fa:d3/ClearPass  -  -    a4d1d25f3252
Apr 28 10:52:55  mac-auth-success      <-  a4:d1:d2:5f:32:52  24:f2:7f:d5:fa:d3/ClearPass  -  -    success
Apr 28 10:52:55  station-up            *   a4:d1:d2:5f:32:52  24:f2:7f:d5:fa:d3            -  -    wpa2 psk aes
Apr 28 10:52:55  wpa2-key1            <-  a4:d1:d2:5f:32:52  24:f2:7f:d5:fa:d3            -  117
Apr 28 10:52:56  wpa2-key2            ->  a4:d1:d2:5f:32:52  24:f2:7f:d5:fa:d3            -  117
Apr 28 10:52:56  wpa2-key3            <-  a4:d1:d2:5f:32:52  24:f2:7f:d5:fa:d3            -  151
Apr 28 10:52:56  wpa2-key4            ->  a4:d1:d2:5f:32:52  24:f2:7f:d5:fa:d3            -  95
BLDG-A-ATV1#
```

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

```
BLDG-A-ATV1# show ap mpskcache

PPSK Cache Table
----------------
Client MAC          Key              Del  Expiry  Role        VLAN  ESSID
----------          ---              ---  ------  ----        ----  -----
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 Mu-
mimo, O: OWE client, S: SAE client, E: Enterprise client

PHY Details: HT   : High throughput;      20: 20MHz;  40: 40MHz; t: turbo-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> spatial streams

Association Table
-----------------
Name          bssid              mac               auth  assoc  aid  l-int  essid      vlan-id  phy
assoc. time   num assoc  Flags   DataReady      UAC
----          -----              ---               ----  -----  ---  -----  -----      -------  ---
-----------   ---------  -----   ---------      ---
BLDG-A-ATV1   24:f2:7f:d5:fa:d3  a4:d1:d2:5f:32:52  y     y      1    10     ArubaMPSK  1        a-
HT-20-1ss       2m:59s       1          W      Yes (Implicit)  0.0.0.0
```

```
BLDG-A-ATV1  24:f2:7f:d5:fa:d0  b8:41:a4:74:e5:46  y     y      1    20     SG1        1        a-
VHT-80sgi-1ss  17h:38m:11s  1          WV     Yes (Implicit)  0.0.0.0
Num Clients:2
BLDG-A-ATV1#
```

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
----------------
Client MAC         Key              Del  Expiry   Role           VLAN  ESSID
----------         ---              ---  ------   ----           ----  -----
a4:d1:d2:5f:32:52  590A1BAFA17E...  Yes  16m:38s  Students-Devs  1     ArubaMPSK
PPSK Cache Count:1
BLDG-A-ATV1#
BLDG-A-ATV1# show ap mpskcache

PPSK Cache Table
----------------
Client MAC         Key              Del  Expiry   Role           VLAN  ESSID
----------         ---              ---  ------   ----           ----  -----
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
-----------------

Apr 29 16:16:47  wpa2-key1             <-  a4:d1:d2:5f:32:52  24:f2:7f:d5:fa:d0            -  117
Apr 29 16:16:47  wpa2-key2             ->  a4:d1:d2:5f:32:52  24:f2:7f:d5:fa:d0            -  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  -  -
server timeout
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.

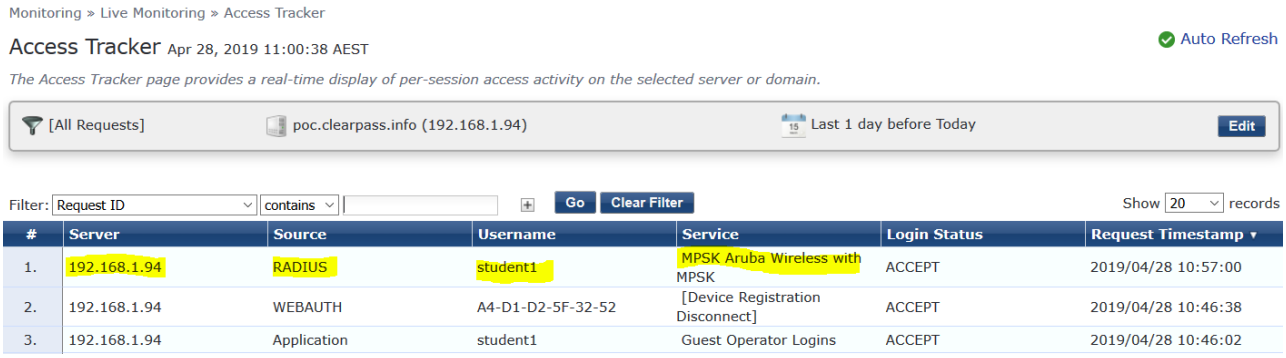
```
BLDG-A-ATV1# sh ap deb auth-trace-buf 10

Auth Trace Buffer
```

```
-----------------

Apr 29 16:18:36  wpa2-key3             <-  a4:d1:d2:5f:32:52  24:f2:7f:d5:fa:d0            -  151
Apr 29 16:18:36  wpa2-key4             ->  a4:d1:d2:5f:32:52  24:f2:7f:d5:fa:d0            -  95
Apr 29 16:18:40  server out-of-service  *   a4:d1:d2:5f:32:52  24:f2:7f:d5:fa:d3/ClearPass  -  -
server timeout
Apr 29 16:23:16  mac-auth-req          ->  a4:d1:d2:5f:32:52  24:f2:7f:d5:fa:d3/ClearPass  -  -
a4d1d25f3252
Apr 29 16:23:16  mac-auth-success      <-  a4:d1:d2:5f:32:52  24:f2:7f:d5:fa:d3/ClearPass  -  -
success
Apr 29 16:23:16  station-up            *   a4:d1:d2:5f:32:52  24:f2:7f:d5:fa:d3            -  -
wpa2 psk aes
Apr 29 16:23:16  wpa2-key1             <-  a4:d1:d2:5f:32:52  24:f2:7f:d5:fa:d3            -  117
Apr 29 16:23:17  wpa2-key2             ->  a4:d1:d2:5f:32:52  24:f2:7f:d5:fa:d3            -  117
Apr 29 16:23:17  wpa2-key3             <-  a4:d1:d2:5f:32:52  24:f2:7f:d5:fa:d3            -  151
Apr 29 16:23:17  wpa2-key4             ->  a4:d1:d2:5f:32:52  24:f2:7f:d5:fa:d3            -  95
BLDG-A-ATV1#
BLDG-A-ATV1# show ap mpskcache

PPSK Cache Table
----------------
Client MAC         Key              Del  Expiry  Role           VLAN  ESSID
----------         ---              ---  ------  ----           ----  -----
a4:d1:d2:5f:32:52  8EFA48327CC5...  No   -       Students-Devs  1     ArubaMPSK
PPSK Cache Count:1
BLDG-A-ATV1#
```

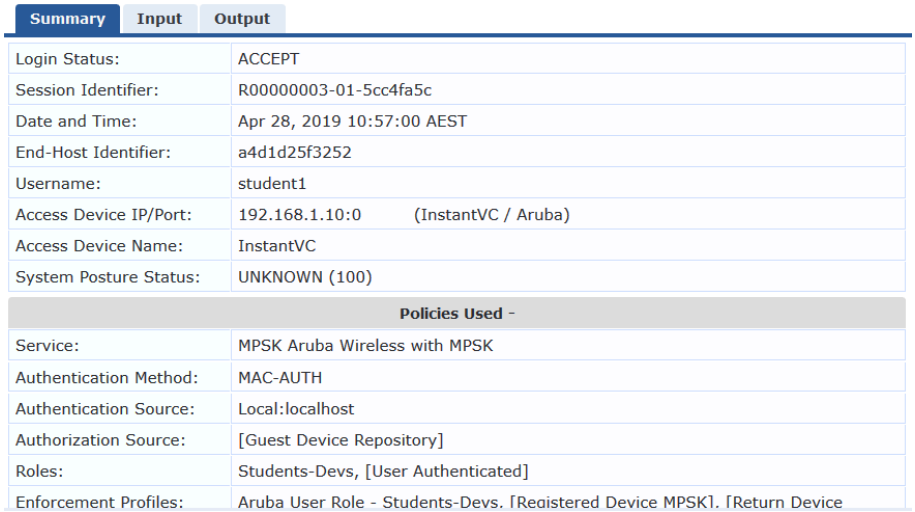
Let's check ClearPass access tracker.

6.4 ClearPass Access Tracker MPSK Authentication

This is the Authentication request as seen from ClearPass.



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



Summary | Input | Output

Username:	student1
End-Host Identifier:	a4d1d25f3252
Access Device IP/Port:	192.168.1.10:0 (InstantVC / Aruba)

RADIUS Request

Radius:Aruba:Aruba-AP-Group	InstantVC
Radius:Aruba:Aruba-Essid-Name	ArubaMPSK
Radius:Aruba:Aruba-Location-Id	BLDG-A-ATV1
Radius:IETF:Called-Station-Id	204c0323a7c0
Radius:IETF:Calling-Station-Id	a4d1d25f3252
Radius:IETF:NAS-Identifier	InstantVC
Radius:IETF:NAS-IP-Address	192.168.1.10
Radius:IETF:NAS-Port	0
Radius:IETF:NAS-Port-Type	19
Radius:IETF:Service-Type	10

Summary | Input | Output

Radius:IETF:Service-Type	10
Radius:IETF:User-Name	a4d1d25f3252

Authorization Attributes

Authorization:[Guest Device Repository]:AccountStatus	0
Authorization:[Guest Device Repository]:Device Account Active	true
Authorization:[Guest Device Repository]:Device Account Enabled	true
Authorization:[Guest Device Repository]:Device Account Expired	false
Authorization:[Guest Device Repository]:Device MPSK	**********
Authorization:[Guest Device Repository]:Device Role ID	3008
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.

Summary | Input | Output

Enforcement Profiles:	Aruba User Role - Students-Devs, [Registered Device MPSK], [Return Device Sponsor Name - RADIUS User-Name]
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

Radius:Aruba:Aruba-MPSK-Passphrase	**********
Radius:Aruba:Aruba-User-Role	Students-Devs
Radius:IETF:User-Name	student1

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=.p....F.

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
------------------
bss                ess         port  ip              phy    type  ch/EIRP/max-EIRP  cur-cl  ap name      in-t(s)
tot-t           flags
---                ---         ----  --              ---    ----  ----------------  ------  -------      -------  -
----            -----
24:f2:7f:d5:fa:d0  SG1         ?/?   192.168.1.121   a-VHT  ap    149E/27.0/28.6    1       BLDG-A-ATV1  0
3d:6h:34m:31s
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:6h:34m:22s
24:f2:7f:d5:fa:d2  SG9         ?/?   192.168.1.121   a-VHT  ap    149E/27.0/28.6    0       BLDG-A-ATV1  0
3d:6h:34m:13s   W3M
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
3d:6h:34m:31s
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
3d:6h:34m:13s   W3M
24:f2:7f:d5:fa:c3  ArubaMPSK   ?/?   192.168.1.121   g-HT   ap    1/9.0/22.1        0       BLDG-A-ATV1  0
2d:23h:10m:41s

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#
```

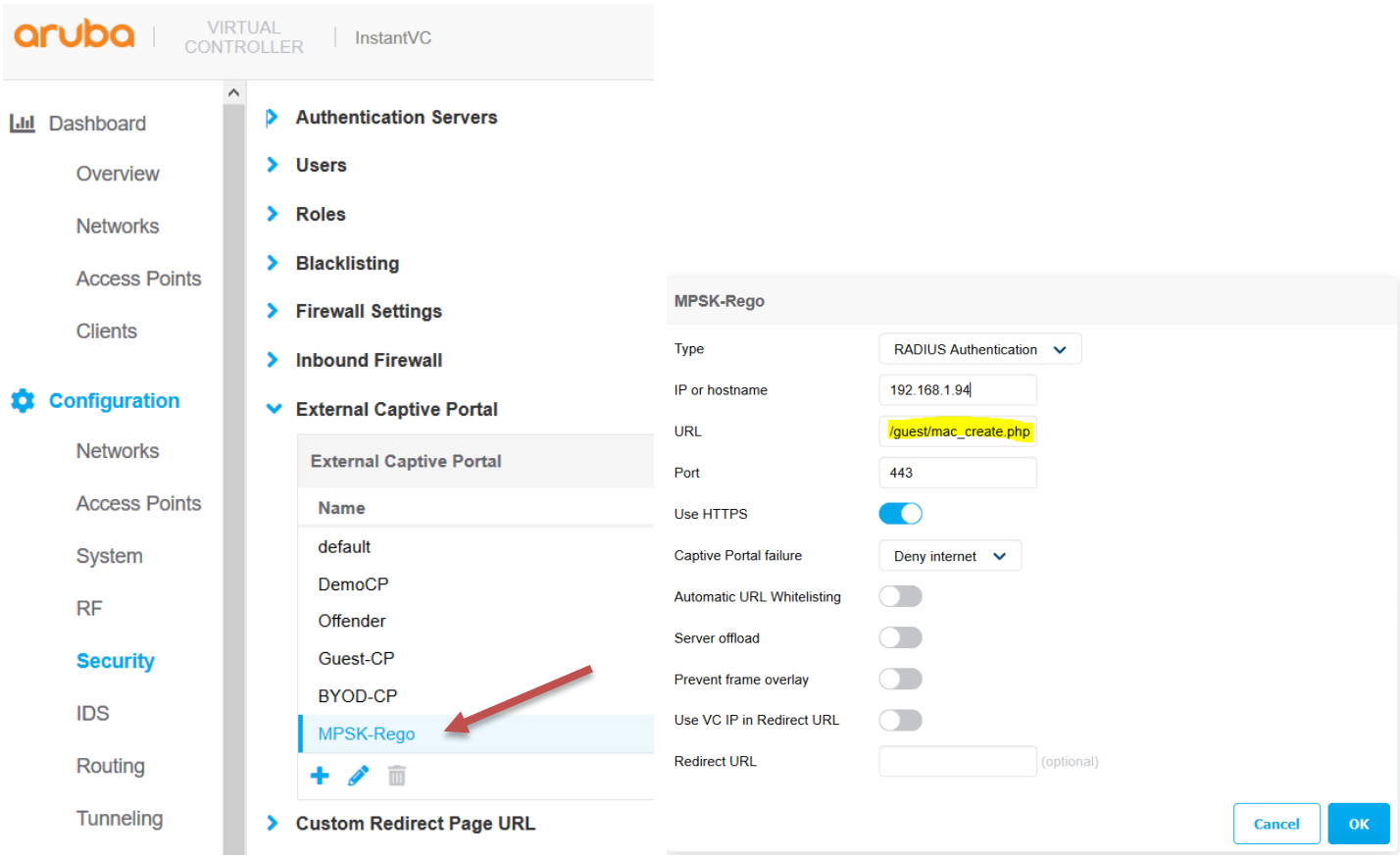
7 Pre-populating MAC address Workflow

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.

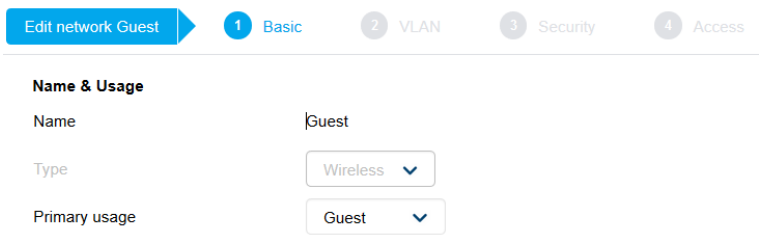
An easier workflow would be to get the user login to ClearPass Guest with their device that needs registration, and we pre-populate the MAC address field with the MAC address of the device.

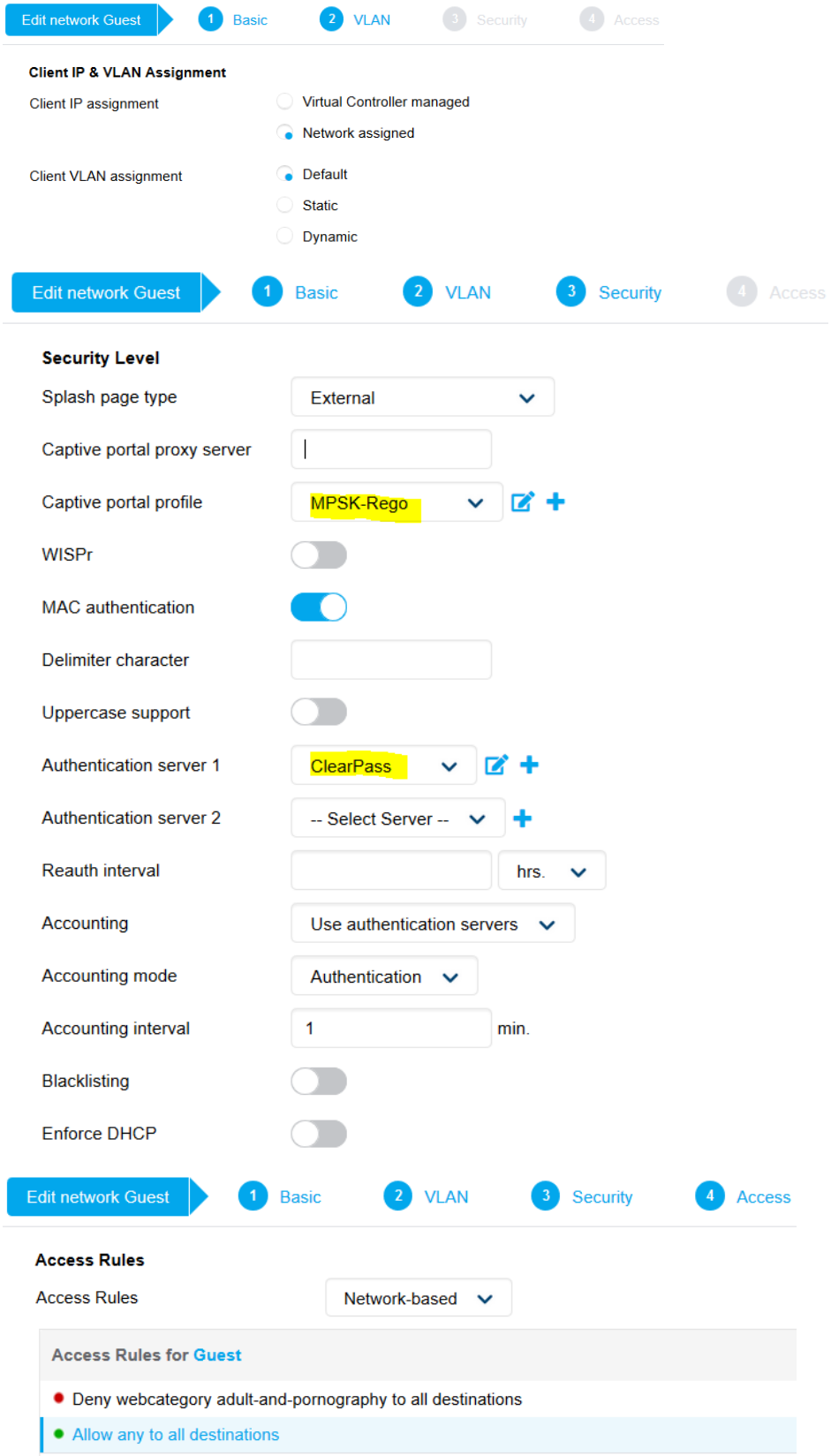
7.1 Aruba Instant Configuration

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.



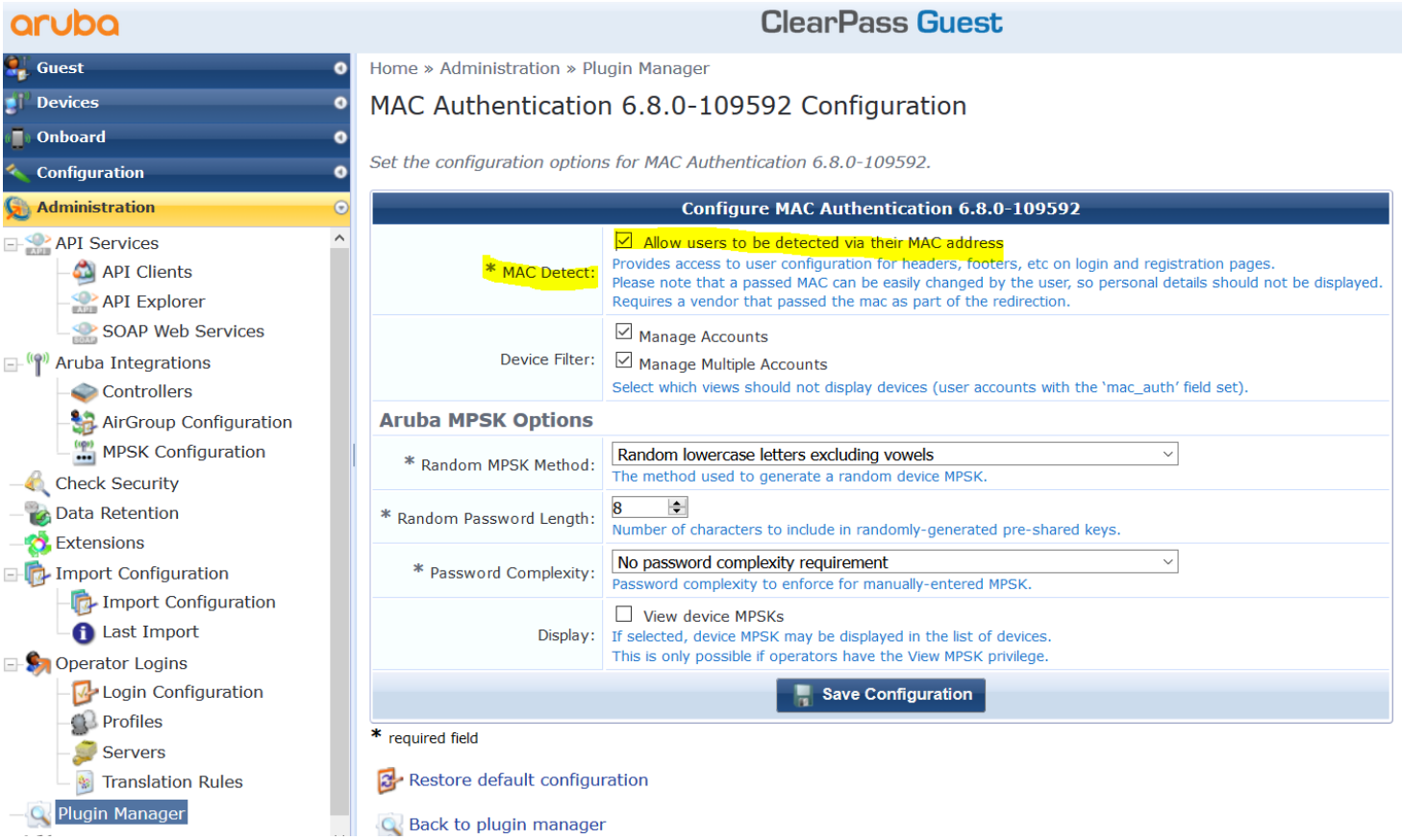
Then we’ll reference that in our Guest WLAN.





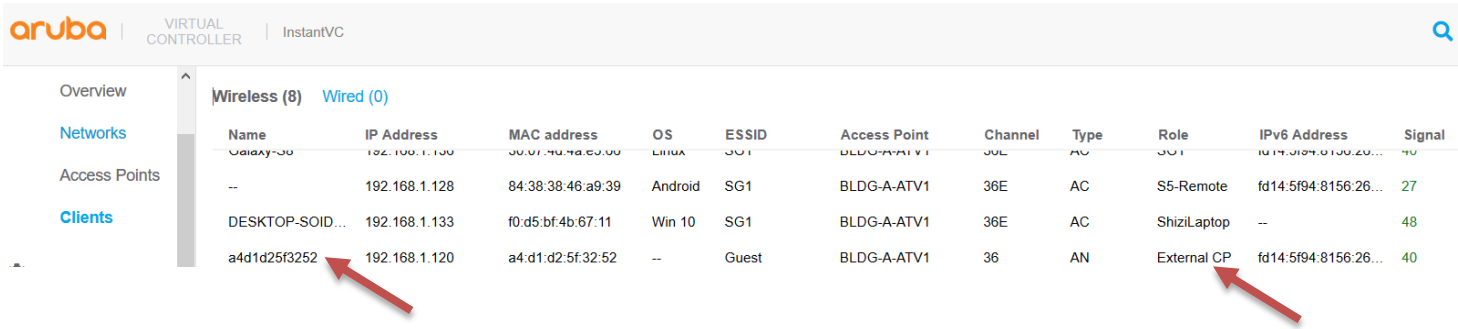
7.2 ClearPass Guest

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.

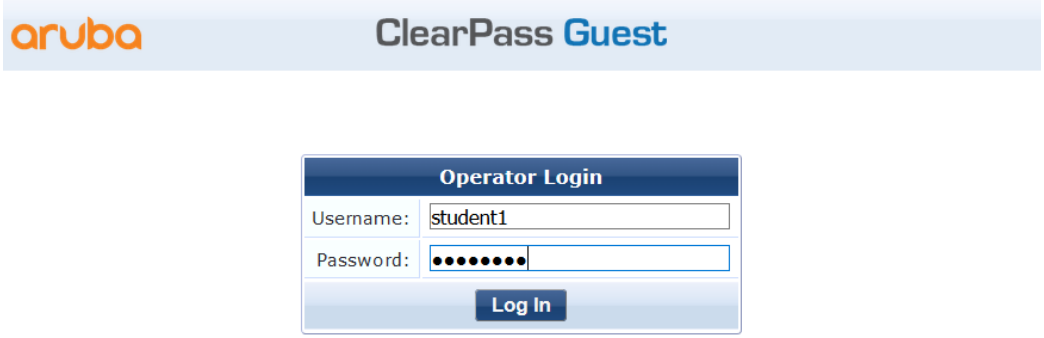


7.3 Testing the new workflow

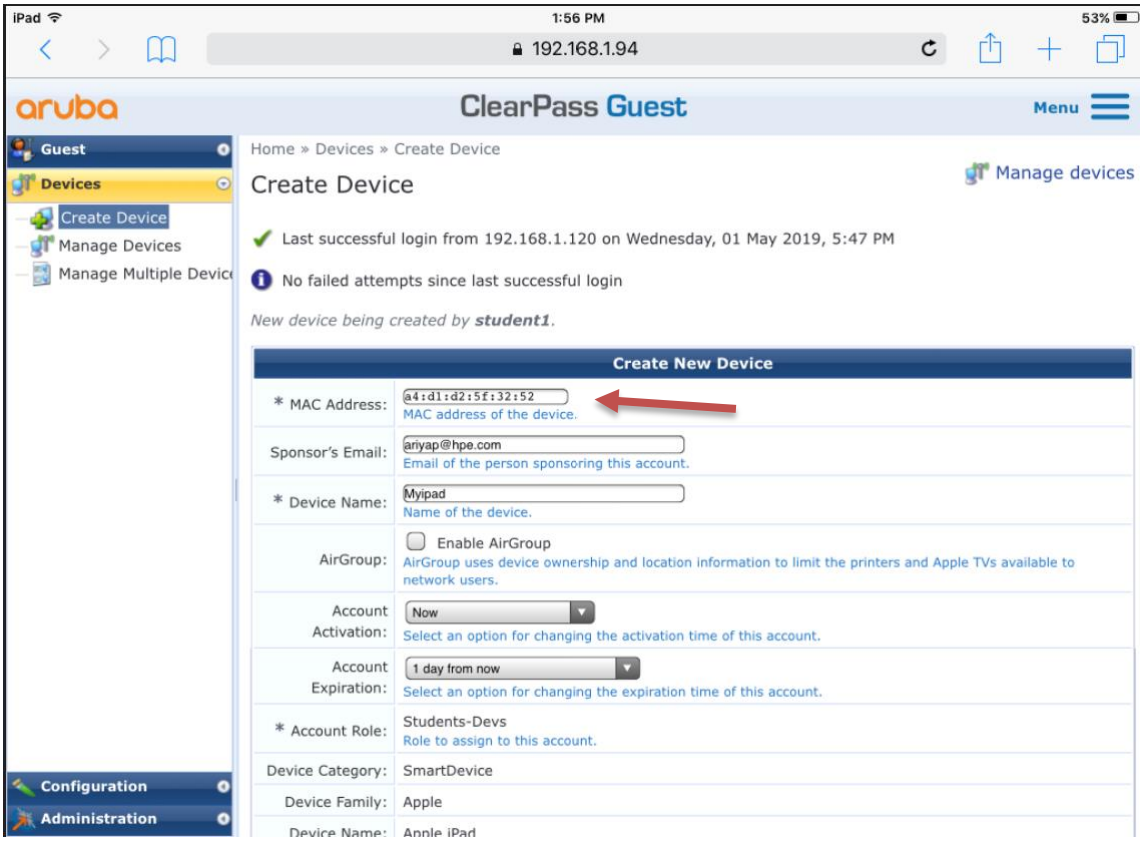
So now the user with the device that needs to be registered for MPSK, connects to "Guest" SSID it gets redirected to "/guest/mac_create.php"



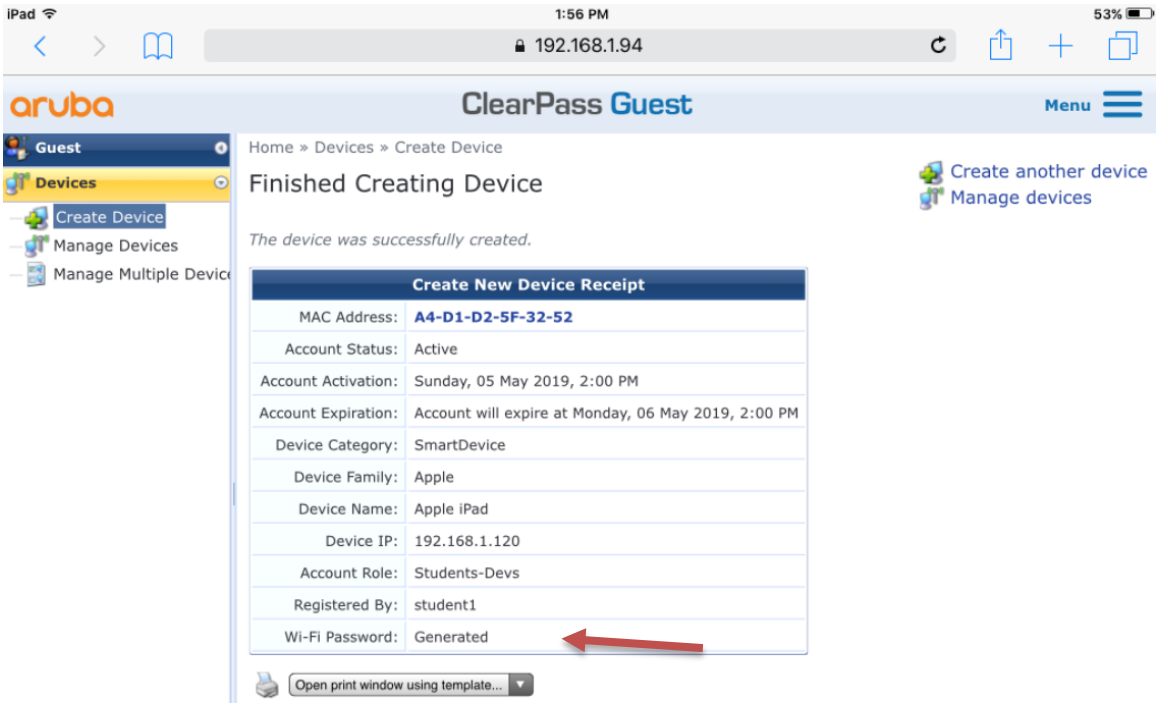
As before the user is prompted for credentials that gets authenticated against AD.



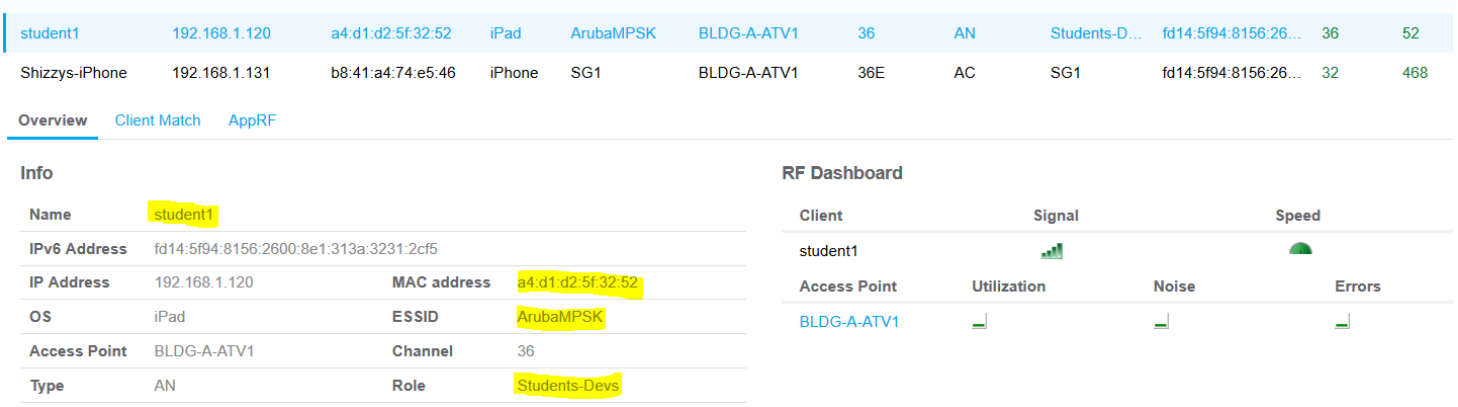
After successful authentication the user get redirected to Create_Device page.



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.



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



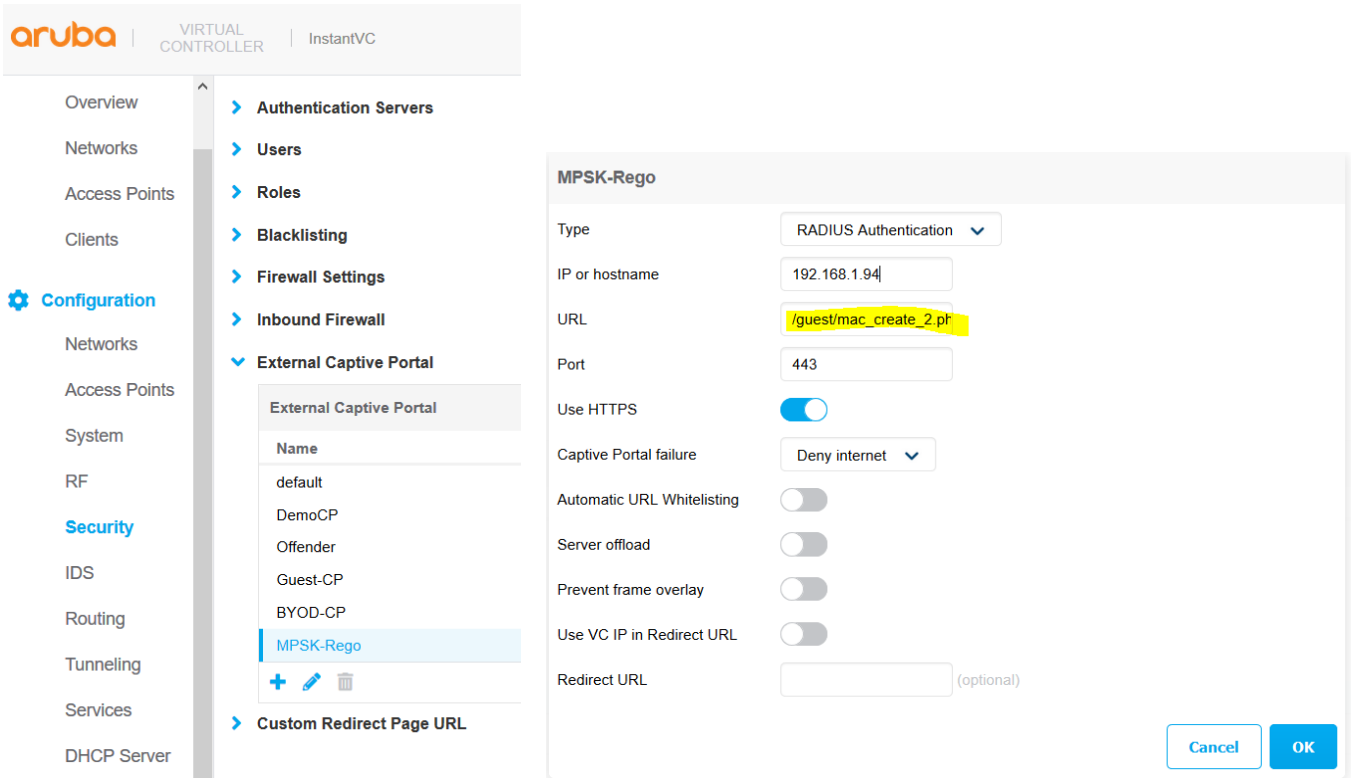
You should note that I have assumed that the standard Guest authentication services are already configured on ClearPass Policy Manager.

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

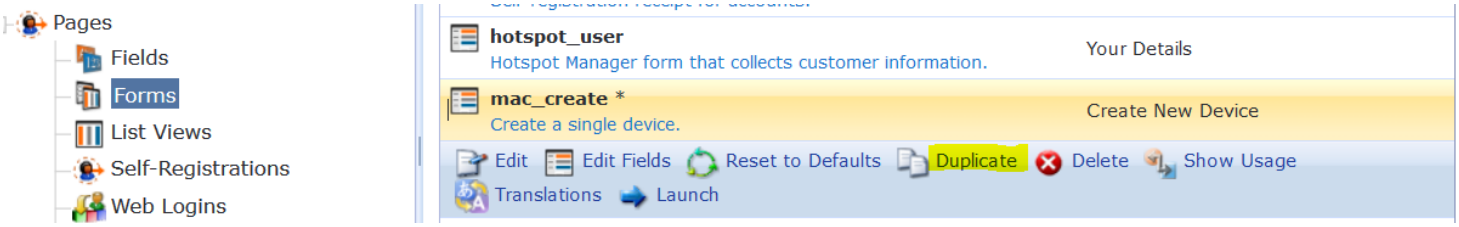


The URL for redirection is "/guest/mac_create_2.php?_browser=1"

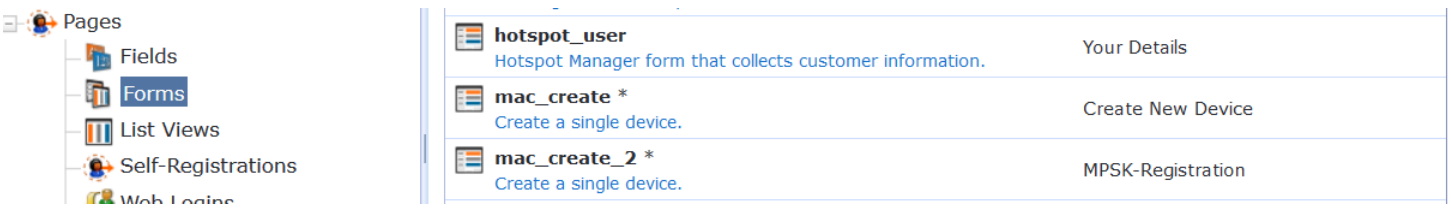
8.2 ClearPass Guest Self Rego

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.



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

Home » Configuration » Pages » Self-Registrations

Self-Registrations

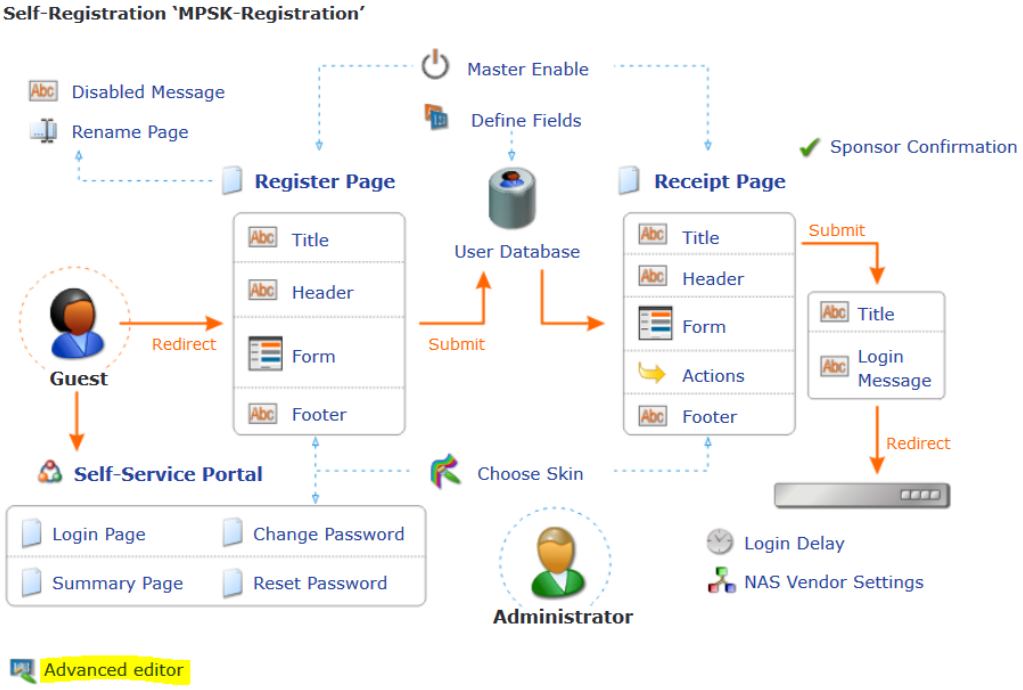
Use this list view to manage the pages used for self-registration.

Quick Help

Name	Register Page	Skin	Parent
Guest Self-Registration Default settings for visitor self-registration.	guest_register	*(Default)*	*(No Parent)*
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.



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

Home » Configuration » Pages » Self-Registrations

Customize Self-Registration (MPSK-Registration)

Back to self-regist

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

Customize Self-Registration

Basic Properties

Options controlling basic operation of self-registration.

* Name:	MPSK-Registration Enter a name to identify the self-registration instance. This is visible only to administrators.
Description:	Enter comments about this instance of self-registration. This is visible only to administrators.
Enabled:	☑ Enable self-registration
* Register Page:	mac_create_2 Enter the base page name for the self-registration page.
* User Database:	ClearPass Policy Manager Self provisioned guest accounts are created using this service handler.
* Skin:	(Default) Choose the skin for the self-registration pages.
Prevent CNA:	☐ Enable bypassing the Apple Captive Network Assistant The Apple Captive Network Assistant (CNA) is the pop-up browser shown when joining a network that has a captive portal. Note that this option may not work with all vendors, depending on how the captive portal is implemented.
Advertising:	☐ Enable Advertising Services content
Translations:	☐ 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 Control

Controls access to the registration page.

Authentication:	☑ Require operator credentials prior to registering the guest 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 Access:	Enter the IP addresses and networks from which self-registration is permitted.
Denied Access:	Enter the IP addresses and networks that are denied self-registration access.
* Deny Behavior:	Send HTTP 404 Not Found status Select the response of the system to a request that is not permitted.
Time Access:	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 appearance 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:	`{nwa_cookiecheck}`
	`<p>`
	`  Please complete the form below to gain access to the network.`
	`</p>`
	Insert...
	HTML template code displayed before the self-registration form.

Footer HTML:	`{if $gsr_metadata.nas_login.enabled}<p>`
	`  Already have an account?  <a href="`
	`{$gsr_metadata.register_page|rawurlencode}_login.php">Sign In</a>`
	`</p>{/if}`
	Insert...
	HTML template code displayed after the self-registration form.

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 appearance of the guest receipt page.

Title: Self-Registration Receipt
The title to display on the guest receipt page.

Form Title: Self-Registration Receipt
The form title to display on the receipt page.

Header HTML:
```
<p>
    The details for your guest account are shown below.
</p>
```
Insert...
HTML template code displayed before the guest receipt.

Footer HTML:
Insert...
HTML template code displayed after the guest receipt.

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 receipt to a self-registered guest.

Download

Enabled: ☐ Enable download of guest receipt

Print

Enabled: ☐ Enable print window for guest 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)
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

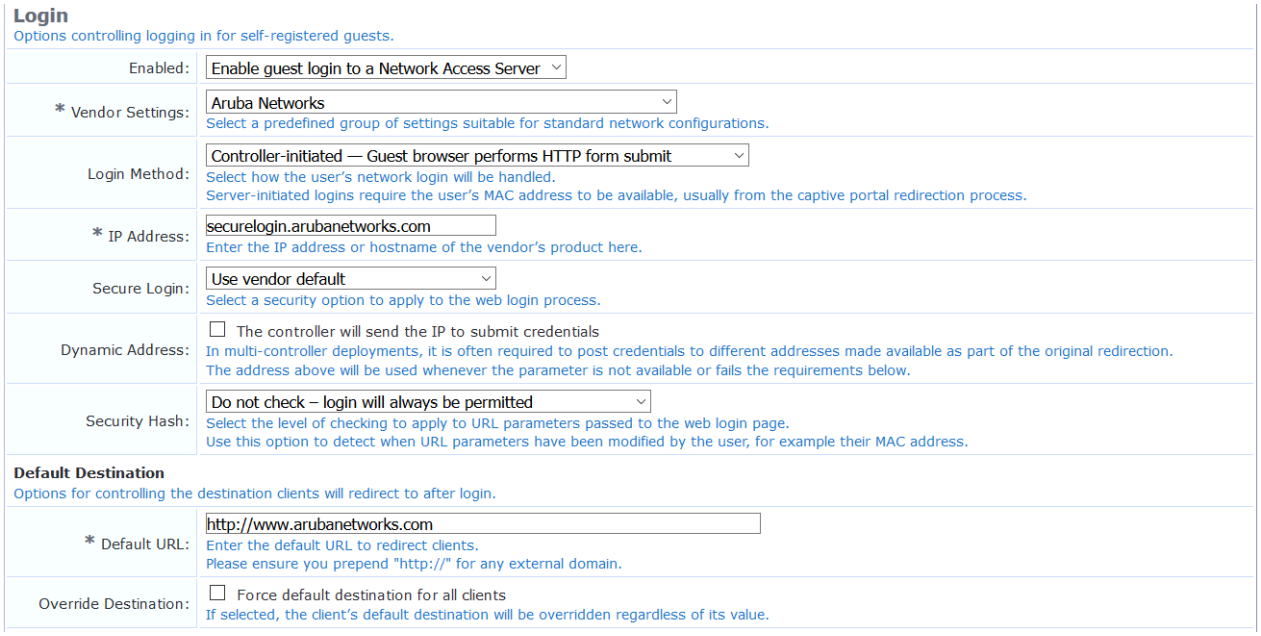
Sponsorship Confirmation

Enabled: ☐ Require sponsor confirmation prior to enabling the account

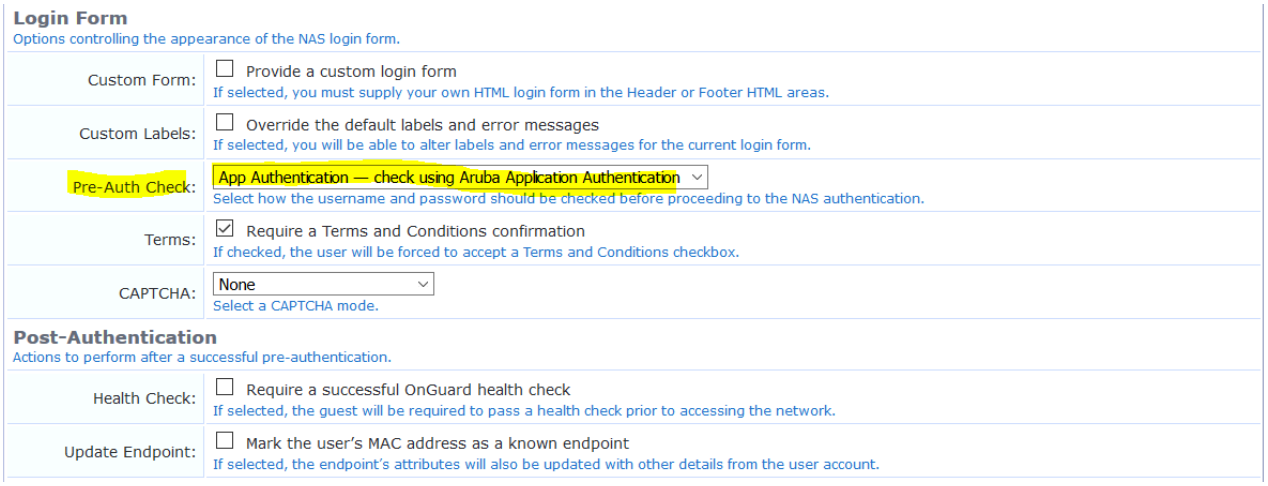
Download Pass

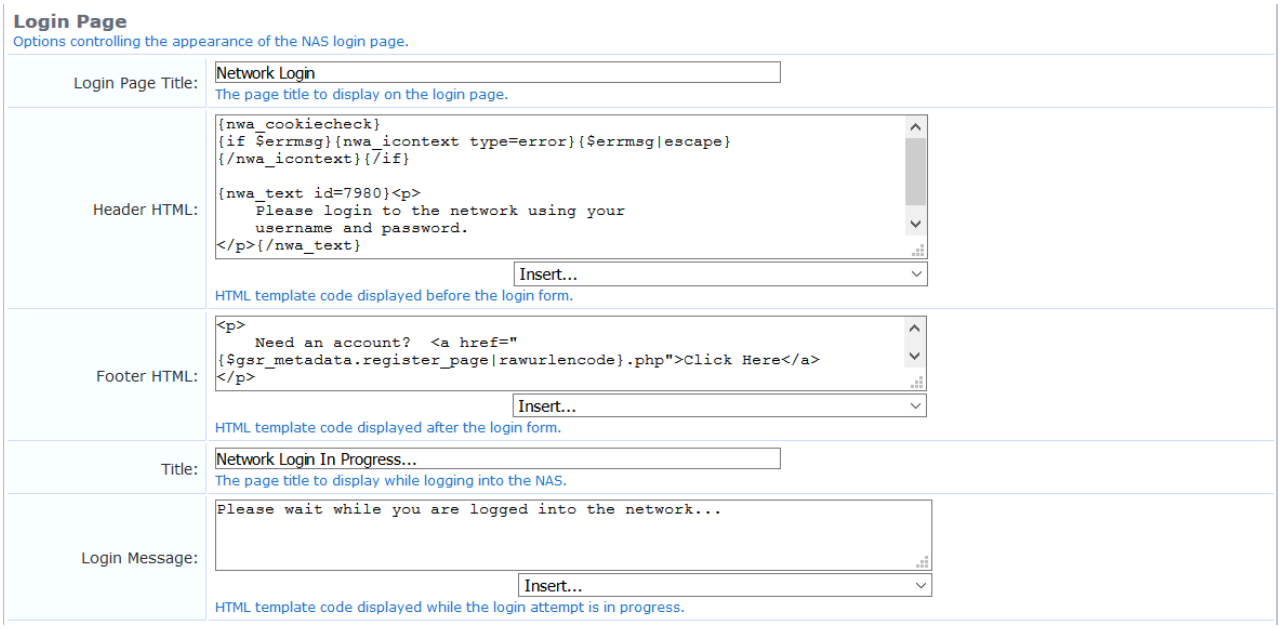
Options for downloading a guest receipt as a pass for use with Apple Passbook.

Not Available: Your pass configuration does not currently enable passes to be downloaded.
Ensure that a valid Pass Certificate has been installed.



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





Automatic Login
Options controlling automatically logging in from the receipt form.

* Login Delay:	0 seconds The time in seconds to delay while displaying the login message.

Cloud Identity
Optionally present guests with various cloud identity / social login options.

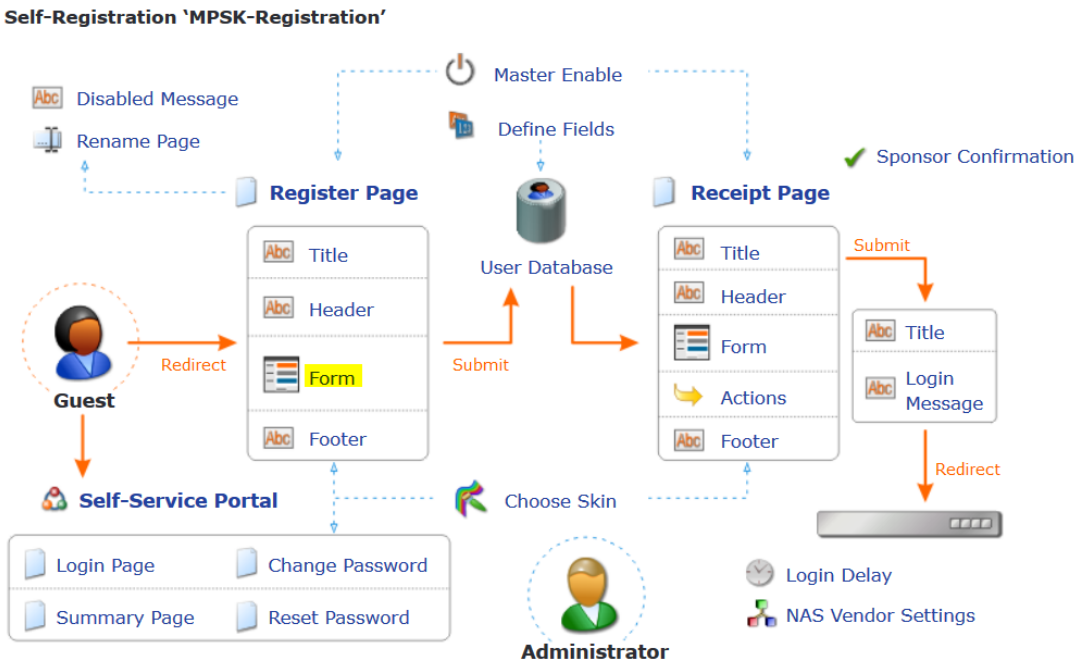
Enabled:	☐ Enable logins with cloud identity / social network credentials

Self-Service Portal
Options controlling details and 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 the account's expiration time. Leave blank to use the original expiration time. Example values: 30d, +30d, or 1y.
UI Overrides:	☐ Display fields to override UI text and labels
Reset Password	
Reset Password:	☐ 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:	☐ Perform a case-insensitive match on the required field
* Password Generation:	Passwords will be randomly generated 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



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**.*

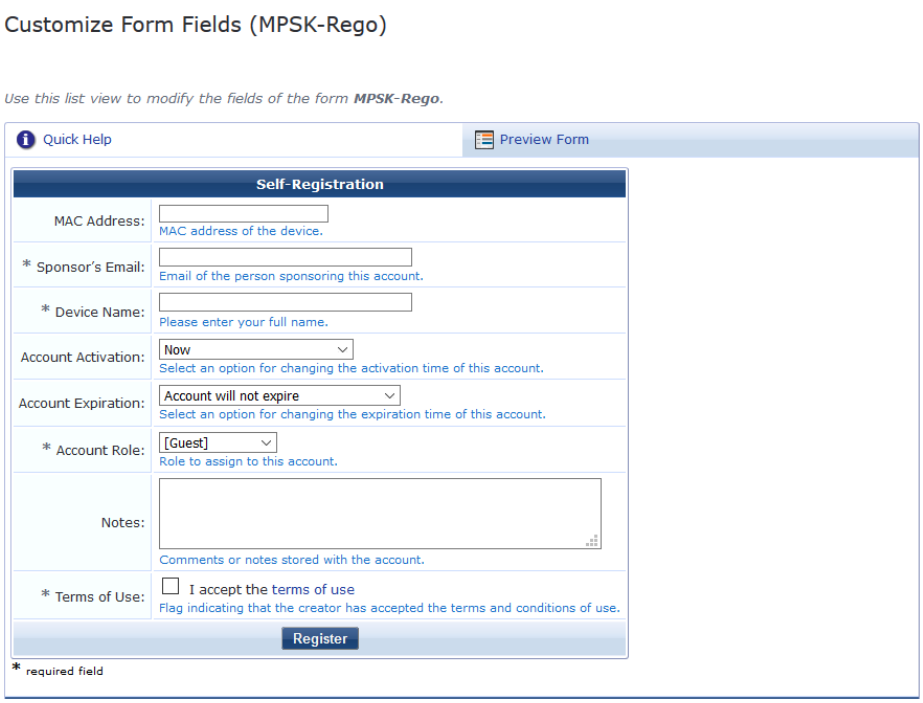
Quick Help | Preview Form

Rank	Field	Type	Label	Description
1	enabled	dropdown	Account Status:	Select an option for changing the status of this account.
5	**mac_auth**	hidden	Is Device:	
5.1	**mac**	text	MAC Address:	MAC address of the device.
10	sponsor_name	text	Sponsor's Name:	Name of the person sponsoring this account.
10.1	**sponsor_email**	text	Sponsor's Email:	Email of the person sponsoring this account.
20	**visitor_name**	text	Device Name:	Name of the device.
25	visitor_phone	phone	Phone Number:	The guest's phone number.
30	visitor_company	text	Company Name:	Company name of the guest.
35	airgroup_device_type	dropdown	Device Type:	Select the type of your device.
40	**mpsk_enable**	hidden	Wi-Fi Password:	
40.2	**auto_send_smtp**	hidden	Auto Email:	
40.300000000000004	**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.
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.

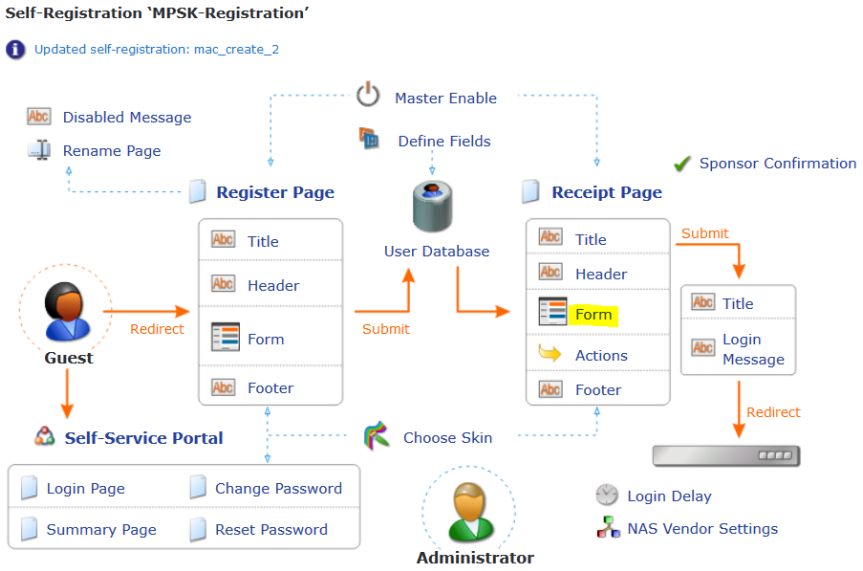
70	**role_id**	dropdown	Account Role:	Role to assign to this account.
81	**no_password**	hidden	Password Change:	If set, prevents the user from changing their own password.
85	**no_portal**	hidden	Portal Login:	If set, prevents the user from logging into the guest service portal.
136.1	**endpoint_profile_device_category**	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.

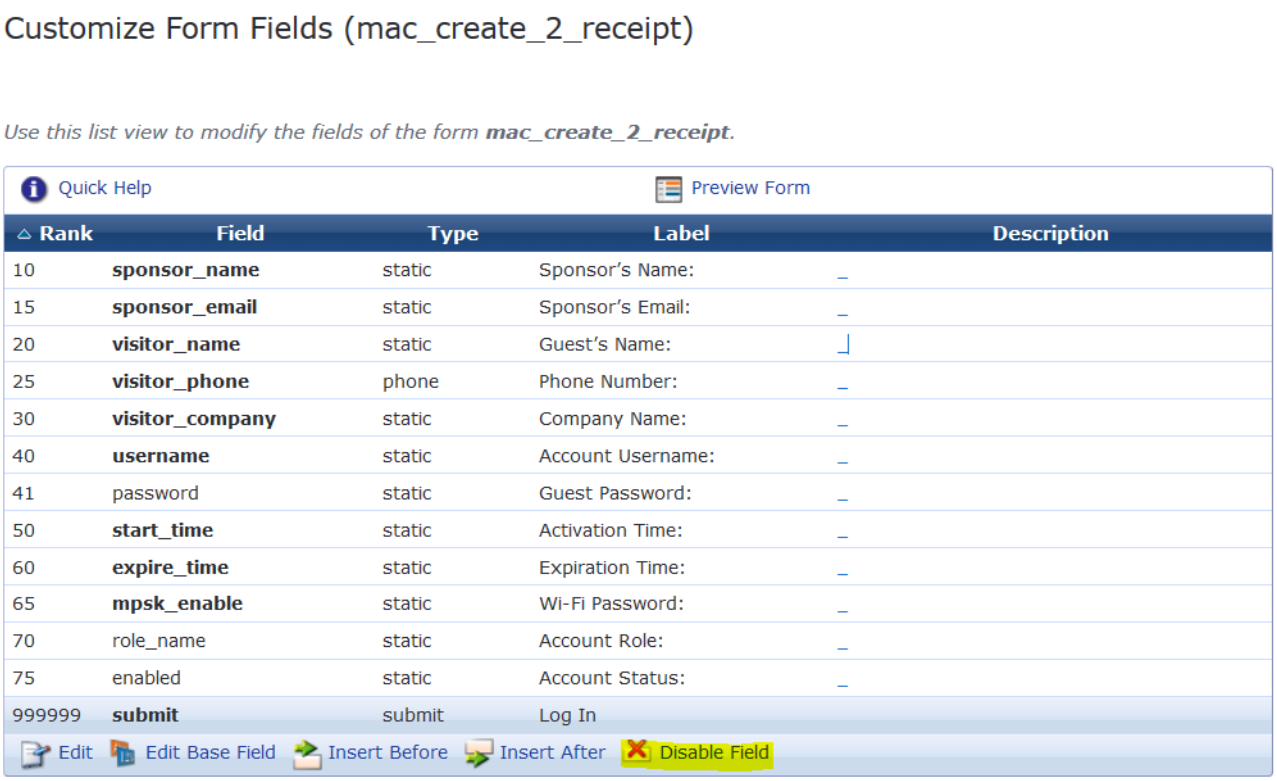
When you click on the "review Form" at the top of the page, you should see the preview as shown below. The account role will be limited to "Students-Devs"



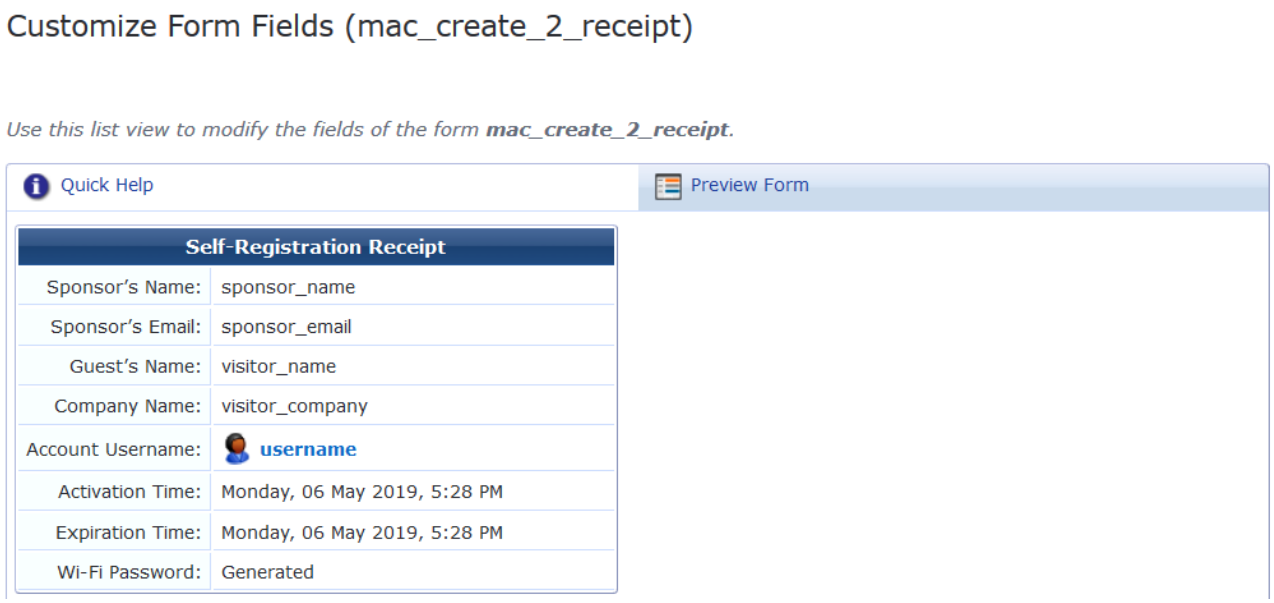
Once we have saved these configuration while on the self-registration page we need to edit the receipt Form.



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.



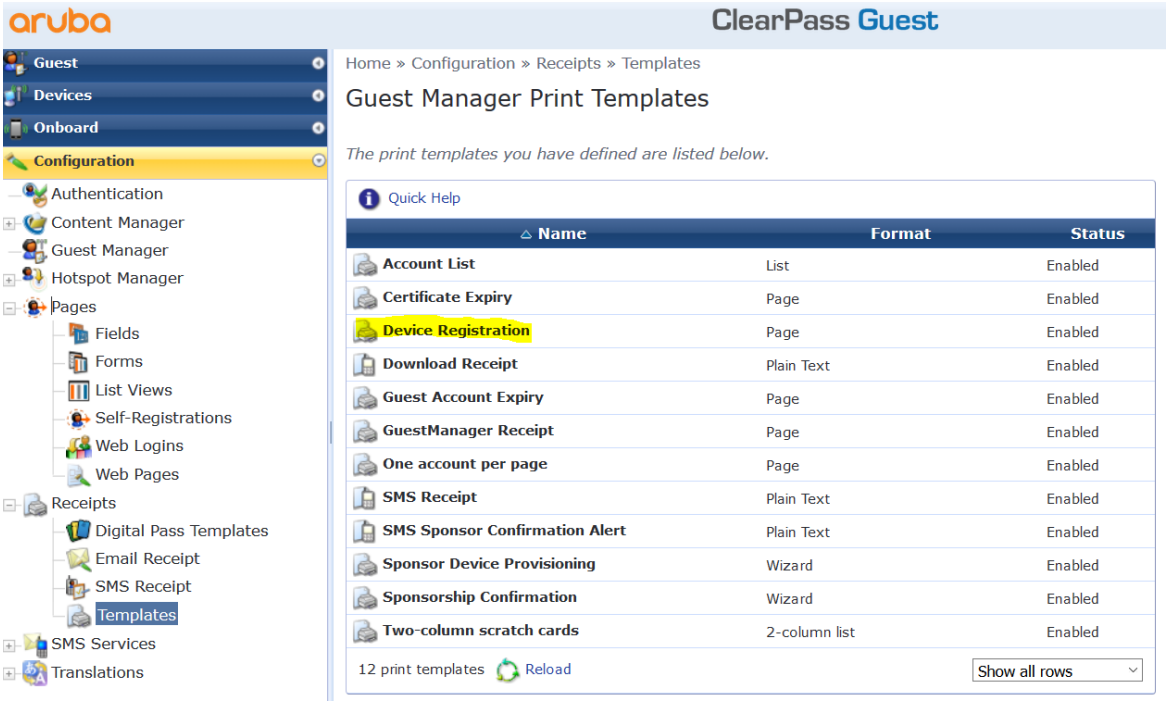
So now when you click on the "Preview Form" you should see the below screenshot.



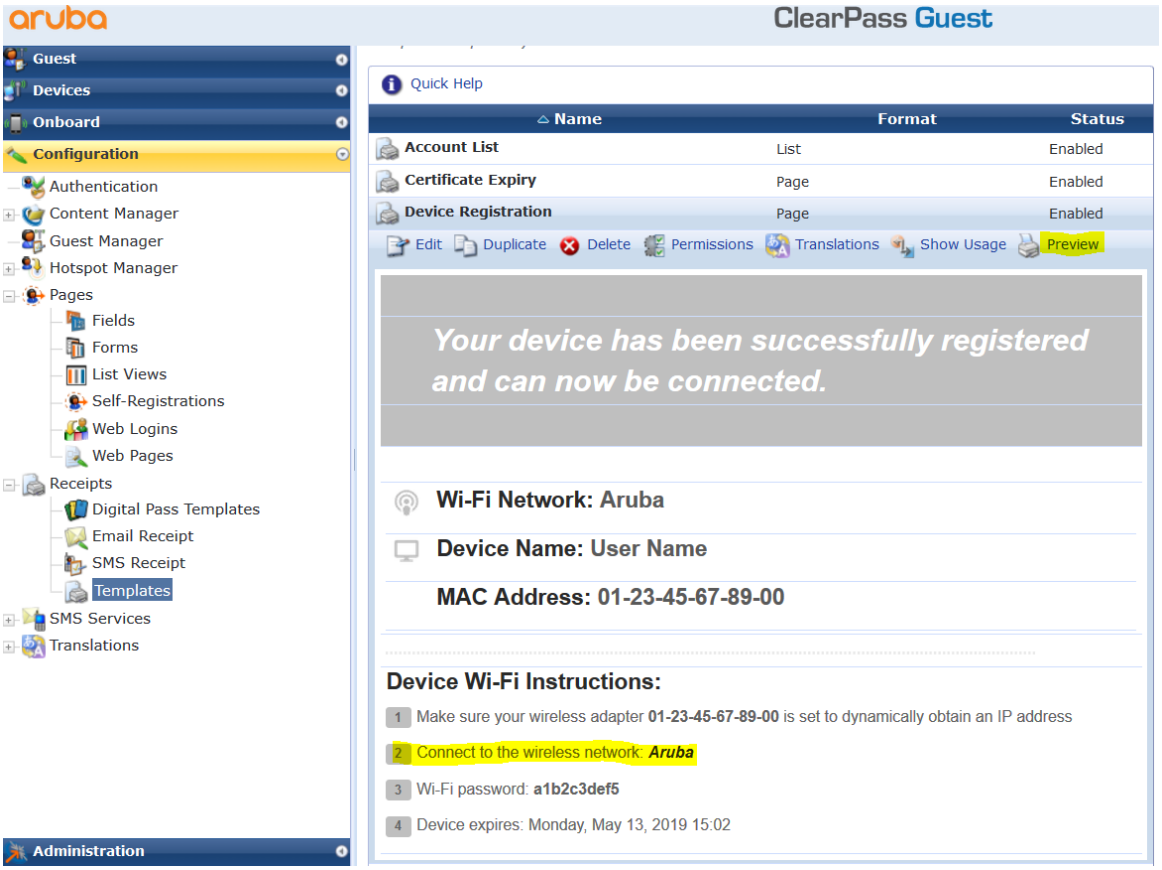
Once you have saved all these, you need to make a change to the Receipt templates. In our Self rego page, we were using

Email Receipt = Device Registration

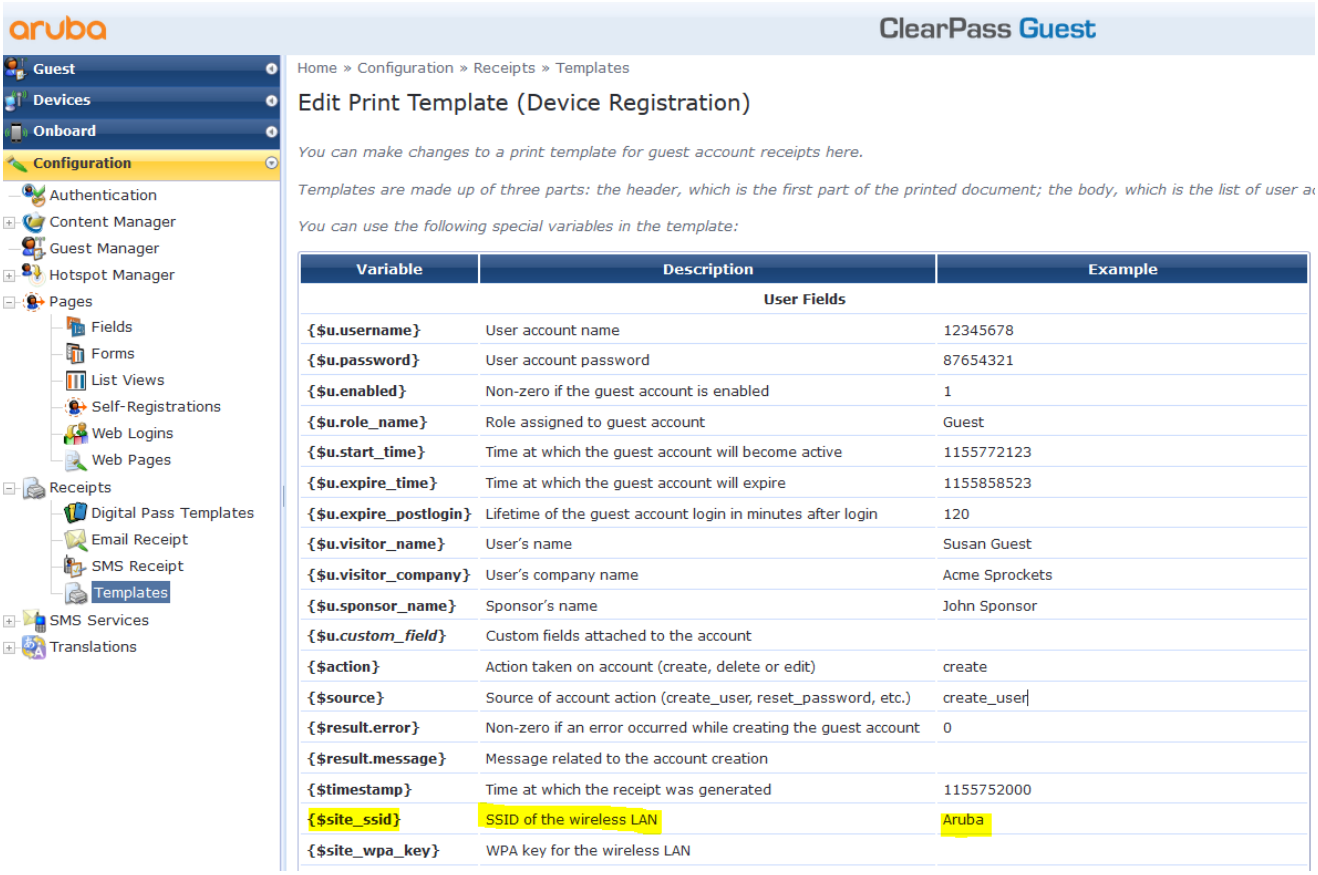
You can find the Device Registration template here. We need to modify it a bit.



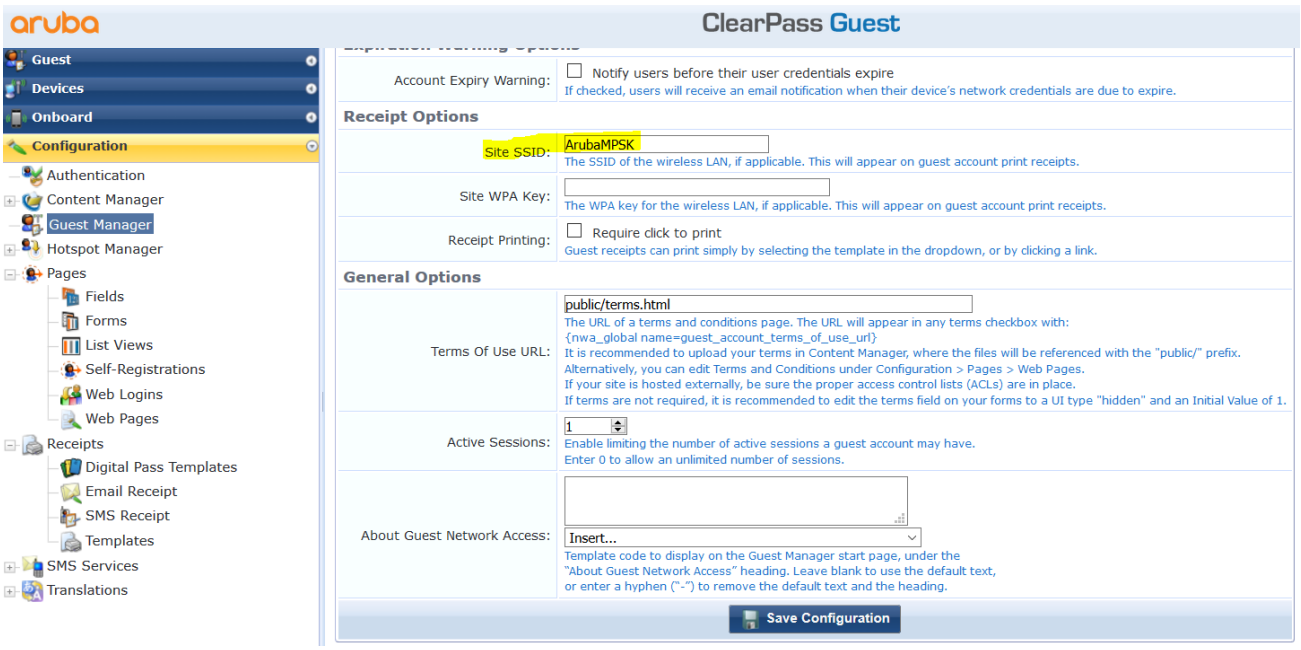
Here is the preview of it, note the SSID name.



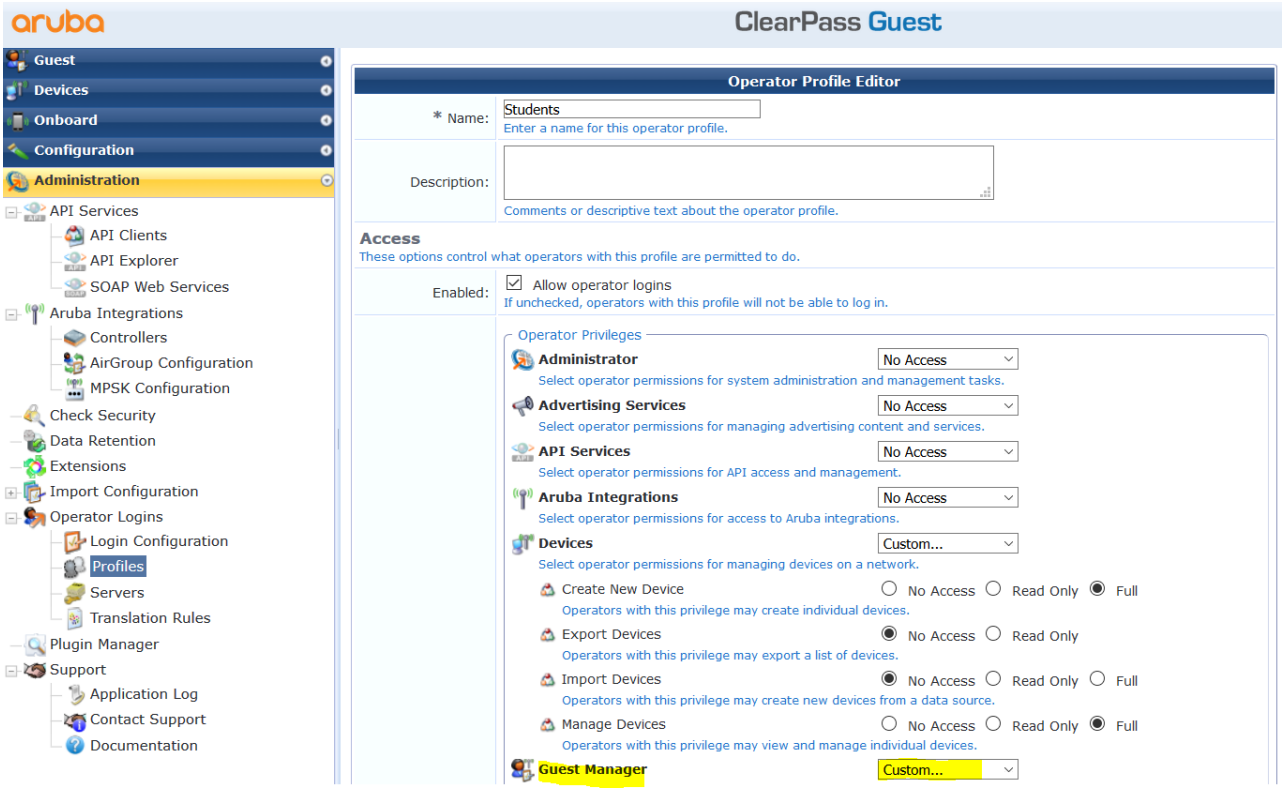
We'll change it to the ArubaMPSK SSID that we have configured on Aruba Instant. You can totally customise this receipt template by editing it.



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



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]

Summary | Service | Authentication | Roles | Enforcement

Name:	[Device Registration Disconnect]
Description:	Service to disconnect all headless devices after they have registered
Type:	Web-based Authentication
Status:	Enabled
Monitor Mode:	☐ Enable to monitor network access without enforcement
More Options:	☐ Authorization ☐ Posture Compliance

Service Rule

Matches ○ ANY or ◉ ALL of the following conditions:

	Type	Name	Operator	Value
1.	Host	CheckType	EQUALS	Authentication
2.	Application:ClearPass	Page-Name	BELONGS_TO	mac_create,mactrac_create
3.	*Click to add...*			

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]

Summary | Service | Authentication | Roles | Enforcement

Service:

Name:	Copy_of_[Device Registration Disconnect]
Description:	Service to disconnect all headless devices after they have registered
Type:	Web-based Authentication
Status:	Enabled
Monitor Mode:	Disabled
More Options:	-

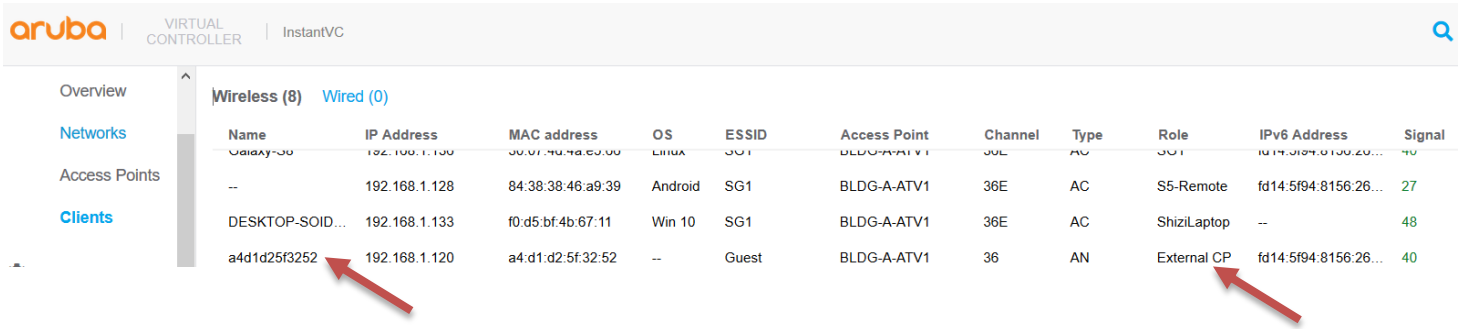
Service Rule

Match ALL of the following conditions:

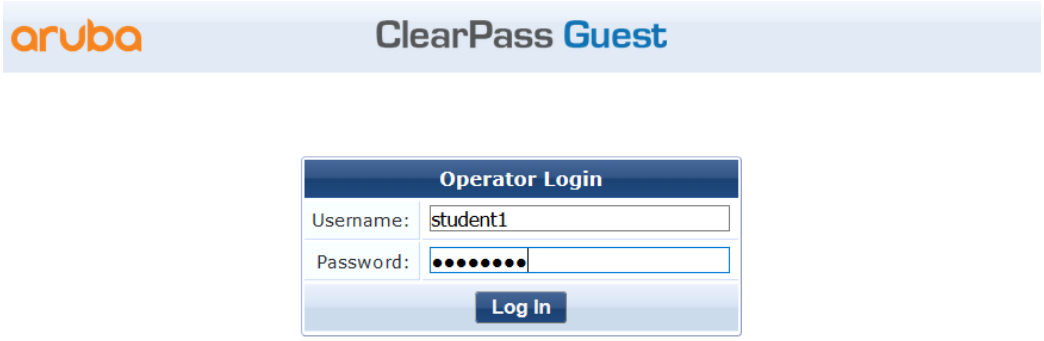
	Type	Name	Operator	Value
1.	Host	CheckType	EQUALS	Authentication
2.	Application:ClearPass	Page-Name	BELONGS_TO	mac_create,mactrac_create,mac_create_2

8.4 Testing the Self Registration workflow

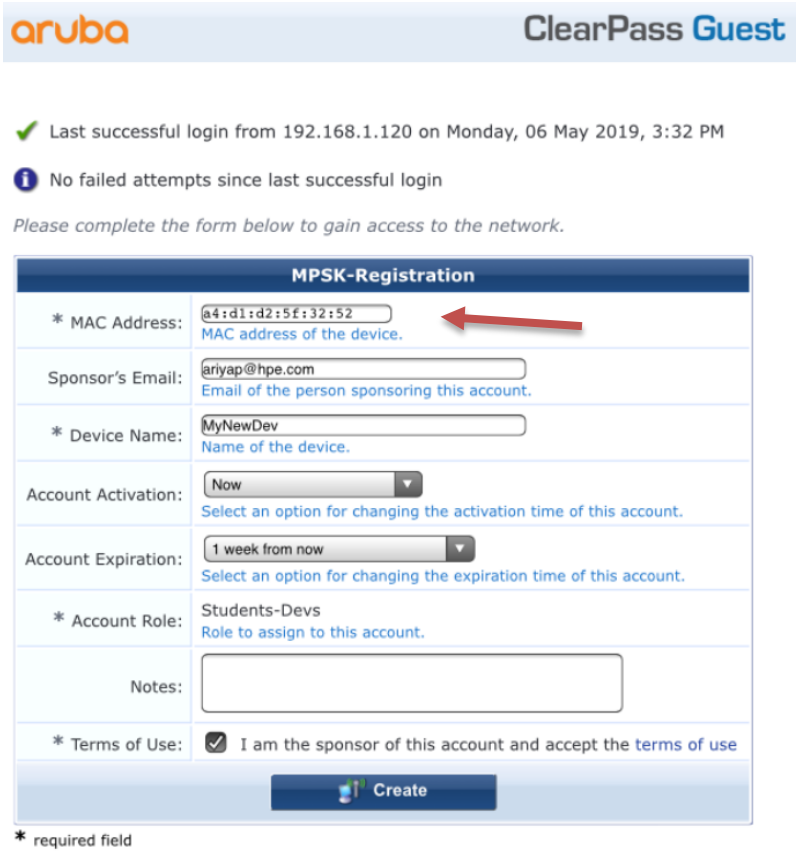
So now the user with the device that needs to be registered for MPSK, connects to “Guest” SSID it gets redirected to the new self-registration page we have configured.



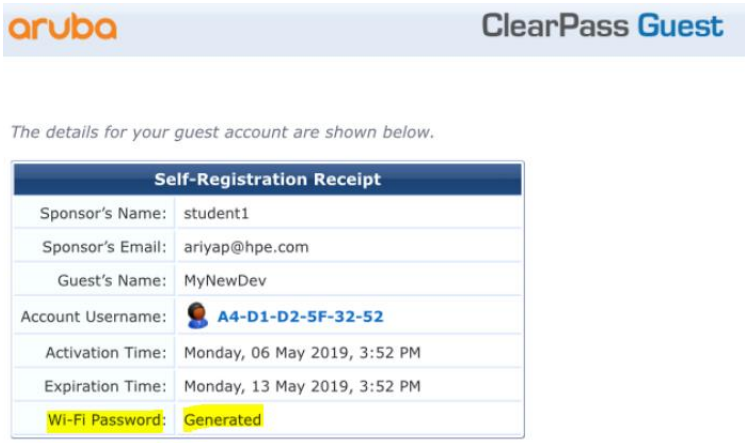
As before the user is prompted for credentials that gets authenticated against AD.



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

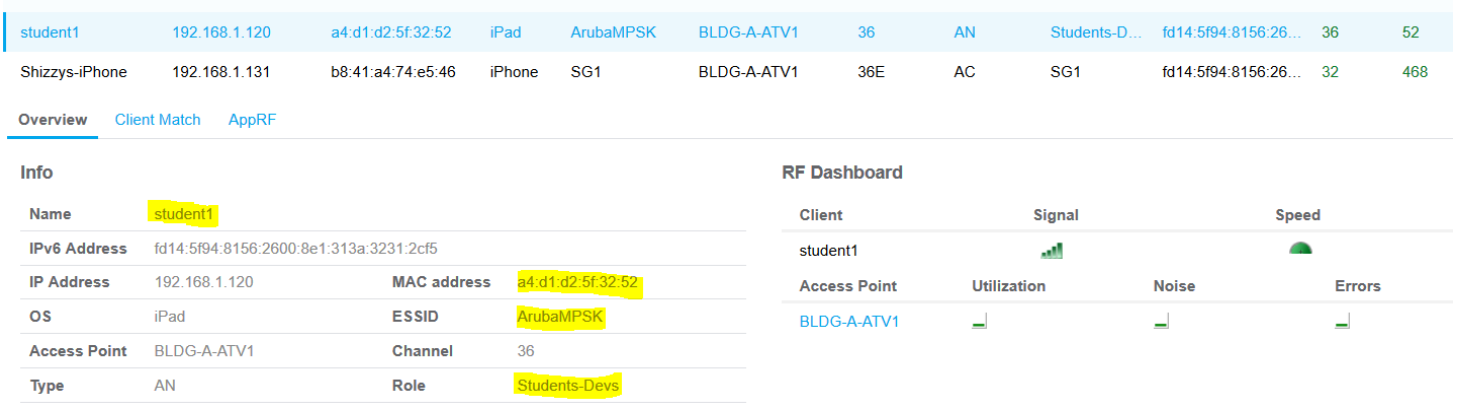


Note that the MAC address gets automatically populated. Once the user registers the device as before, they see the receipt and gets an email address with the MPSK password. Note that there is no Login button on the receipt page as shown below.



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.

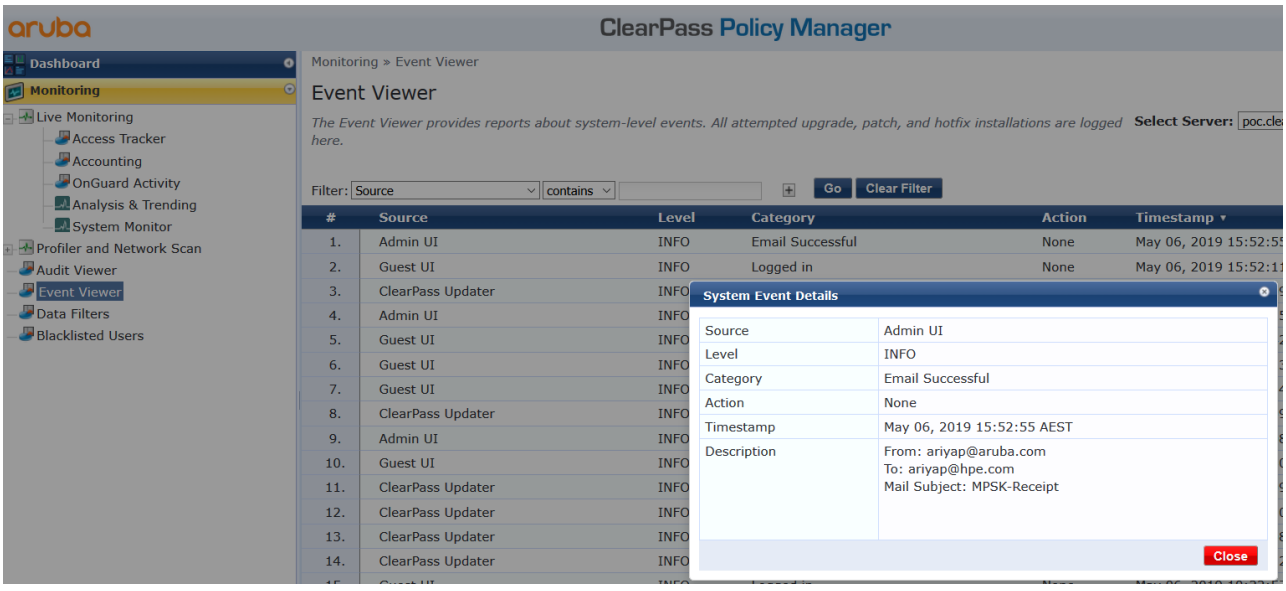


You should note that I have assumed that the standard Guest authentication services are already configured on ClearPass Policy Manager.

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



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