

1 Table of Contents

Table of Contents

1	Table of Contents	1
1.1	Revision History	1
2	AOS10 MPSK Configuration	2
2.1	Authentication Server Configuration	2
2.2	MPSK Configuration	2
3	ClearPass Configuration	6
3.1	RADIUS Dictionary	6
3.2	Service Template	6
3.3	Enforcement Profiles.....	8
3.4	Enforcement Policy	9
3.5	Role Mapping.....	9
3.6	ClearPass Service.....	9
3.7	Operator Service.....	11
3.8	Messaging Server.....	12
4	ClearPass Guest	13
4.1	MPSK Configuration.....	13
4.2	Operator Profile	14
4.3	Form Fields	15

1.1 Revision History

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

2 AOS10 MPSK Configuration

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

2.1 Authentication Server Configuration

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

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

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

Buttons: Cancel, Save

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

Name	Type
ClearPass	RADIUS

2.2 MPSK Configuration

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

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

- General
- VLANs
- Security
- Access
- Summary

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

- NAME (SSID): ArubaMPSK
- > Advanced Settings

Buttons: Cancel, Next

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

Access Points

Switches

Gateways

WLANs

Access Points

Radios

Interfaces

Security

Services

System

Configuration Audit

List

Summary

Config

Hide Advanced

CREATE A NEW NETWORK

1 General

2 VLANs

3 Security

4 Access

5 Summary

Traffic forwarding mode:

☒ Bridge

☐ Tunnel

☐ Mixed

Client VLAN Assignment:

☒ Static

☐ Dynamic

☐ Native VLAN

VLAN ID:

22

> Show Named VLANs

Cancel

Back

Next

Access Points

Switches

Gateways

WLANs

Access Points

Radios

Interfaces

Security

Services

System

Configuration Audit

List

Summary

Config

Hide Advanced

CREATE A NEW NETWORK

1 General

2 VLANs

3 Security

4 Access

5 Summary

Security Level:

Enterprise

Personal

Captive Portal

Open

Key Management:

MPSK AES

Primary Server:

ClearPass

+

Secondary Server:

-- Select --

+

Advanced Settings

Enforce DHCP:

Use IP for Calling Station ID:

Called Station ID Type:

MAC Address

Called Station ID Include SSID:

Accounting

Accounting:

Use authentication servers

Accounting Interval:

1

min

Fast Roaming

Cancel

Back

Next

AOS10 Access Points Switches Gateways List Summary Config

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

CREATE A NEW NETWORK

1 General 2 VLANs 3 Security 4 Access 5 Summary

Access rules

Role Based Network Based Unrestricted

ROLE	ACCESS RULES FOR SELECTED ROLES
ArubaMPSK	Deny any to all destinations
CP-Guest	
Contractor	
Employee	
Executive-Bridge	
IoT1	
IoT2	

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

AOS10 Access Points Switches Gateways List Summary Config

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

CREATE A NEW NETWORK

1 General 2 VLANs 3 Security 4 Access 5 Summary

Network Summary

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

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

AOS10 Access Points Switches Gateways List Summary Config

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

SECURITY

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

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

Access Points

Switches

Gateways

WLANs

Access Points

ADD ROLE

Roles:

Cancel

OK

SECURITY

> Authentication Servers

> MPSK Local

> User For Internal Server

> Roles

Roles

+

Hide Advanced

AOS10

Access Points

Switches

Gateways

WLANs

Access Points

Radios

Interfaces

Security

Services

System

Configuration Audit

Hide Advanced

Manage

Overview

Devices

Clients

Guests

Applications

Security

Analyze

Alerts & Events

Audit Trail

Tools

Reports

Maintain

Firmware

SECURITY

> Authentication Servers

> MPSK Local

> User For Internal Server

> Roles

Roles

Role

Student-Devs

ArubaMPSK

CP-Guest

Contractor

Employee

Executive-Bridge

IoT1

IoT2

MDCV

Access Rules For Selected Roles

Allow any to all destinations

Cancel

Save Settings

3 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.

3.1 RADIUS Dictionary

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

The screenshot shows the ClearPass Policy Manager interface. On the left is a navigation menu with 'Administration' selected. The main area displays a table of RADIUS attributes. A modal window titled 'RADIUS Attributes' is open, showing a list of attributes for 'Aruba (14823)'. The attributes include Vendor Name, Vendor ID, Vendor Prefix, and Enabled status. The 'Aruba-MPSK-Passphrase' attribute is highlighted in yellow.

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

3.2 Service Template

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

The screenshot shows the ClearPass Policy Manager interface. The left navigation menu has 'Configuration' selected. The main area displays 'Service Templates & Wizards'. It includes instructions on how to configure services and a list of service templates. The 'Aruba Wireless with MPSK' template is highlighted in yellow.

Configuration » Service Templates & Wizards

Service Templates & Wizards

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

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

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

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

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

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

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

Using the Aruba Wireless with MPSK wizard.

Service Templates - Aruba Wireless with MPSK

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

[Back to Service Templates & Wizards](#)

Delete

Next →

Add Service

Cancel

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

[Back to Service Templates & Wizards](#)

Delete

Next →

Add Service

Cancel

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

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

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

[Back to Service Templates & Wizards](#)

Delete

Next →

Add Service

Cancel

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

Create a New Enforcement Policy

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

Default MPSK*:

Default Aruba User Role*:

[Back to Service Templates & Wizards](#)

Delete

Next →

Add Service

Cancel

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

Menu

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

Configuration » Services
Services

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

- Add
- Import
- Export All

3.3 Enforcement Profiles

Here are the two enforcement profiles that were created.

Configuration » Enforcement » Profiles

Enforcement Profiles

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

Filter: Name contains mpsk Go Clear Filter Show 20 records

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

Showing 1-2 of 2 Copy Export Delete

Enforcement Profile - MPSK Aruba Wireless with MPSK Default Profile

Summary Profile Attributes

Profile:

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

Attributes:

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

It also created this enforcement profile.

Enforcement Profile - Aruba User Role – Student-Devs

Note: This Enforcement Profile is created by Service Template

Summary Profile Attributes

Profile:

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

Attributes:

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

Enforcement Profiles - [Registered Device MPSK]

This is a default profile.

Summary Profile Attributes

Profile:

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

Attributes:

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

3.4 Enforcement Policy

This is the enforcement policy that got created.

Enforcement Policies - MPSK Aruba Wireless with MPSK Enforcement Policy

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

3.5 Role Mapping

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

Role Mappings - MPSK Aruba Wireless with MPSK Role Map

aruba	ClearPass Policy Manager	Menu
Dashboard	Configuration » Identity » Role Mappings » Edit - MPSK Aruba Wireless with MPSK Role Map	
Monitoring	Role Mappings - MPSK Aruba Wireless with MPSK Role Map	
Configuration	Note: This Role Mapping policy is created by Service Template	
Service Templates & Wizards	Summary	Policy Mapping Rules
Services	Policy:	
Authentication	Policy Name:	MPSK Aruba Wireless with MPSK Role Map
Identity	Description:	
Single Sign-On (SSO)	Default Role:	[Other]
Local Users	Mapping Rules:	
Endpoints	Rules Evaluation Algorithm:	Evaluate all
Static Host Lists	Conditions	Role Name
Roles	1. (Authorization:[Guest Device Repository]:Device Role ID EQUALS 3009)	Student-Devs
Role Mappings		
Posture		
Enforcement		

3.6 ClearPass Service

And here is the complete serviced that was configured.

Services

[Add](#)
[Import](#)
[Export All](#)

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

Filter: contains Show records

#	<input type="checkbox"/>	Order ▲	Name	Type	Template	Status
1.	<input type="checkbox"/>	1	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	
2.	<input type="checkbox"/>	2	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	
3.	<input type="checkbox"/>	3	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	
4.	<input type="checkbox"/>	4	Modified Aruba Device Access Service	TACACS	TACACS+ Enforcement	
5.	<input type="checkbox"/>	5	[Guest Operator Logins]	Application	Aruba Application Authentication	
6.	<input type="checkbox"/>	6	[Insight Operator Logins]	Application	Aruba Application Authentication	
7.	<input type="checkbox"/>	7	Ariya Guest Operator Logins	Application	Aruba Application Authentication	
8.	<input type="checkbox"/>	8	MM-admin-service	RADIUS	RADIUS Enforcement (Generic)	
9.	<input type="checkbox"/>	9	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	
10.	<input type="checkbox"/>	10	AA Aruba 802.1X Wireless	RADIUS	Aruba 802.1X Wireless	
11.	<input type="checkbox"/>	11	GG MAC Authentication	RADIUS	MAC Authentication	
12.	<input type="checkbox"/>	12	GG User Authentication with MAC Caching	RADIUS	RADIUS Enforcement (Generic)	
13.	<input type="checkbox"/>	13	MPSK Aruba Wireless with MPSK	RADIUS	MAC Authentication	

Summary

Service

Authentication

Roles

Enforcement

Name:

MPSK Aruba Wireless with MPSK

Description:

To authenticate devices using an Aruba MPSK.

Type:

MAC Authentication

Status:

Enabled

Monitor Mode:

☐ Enable to monitor network access without enforcement

More Options:

☐ Authorization ☐ Audit End-hosts ☐ Profile Endpoints ☐ Accounting Proxy

Service Rule

Matches ☐ ANY or ☒ ALL of the following conditions:

	Type	Name	Operator	Value	
1.	Radius:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)	
2.	Radius:IETF	Service-Type	EQUALS	Call-Check (10)	
3.	Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}	
4.	Connection	SSID	EQUALS	ArubaMPSK	
5.	Click to add...				

Summary

Service

Authentication

Roles

Enforcement

Authentication Methods:

[Allow All MAC AUTH]

Move Up ↑

Move Down ↓

Remove

View Details

Modify

--Select to Add--

Add New Authentication Method

Authentication Sources:

[Guest Device Repository] [Local SQL DB]

Move Up ↑

Move Down ↓

Remove

View Details

Modify

--Select to Add--

Add New Authentication Source

Strip Username Rules:

☐ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes

Summary

Service

Authentication

Roles

Enforcement

Role Mapping Policy:

MPSK Aruba Wireless with MPSK Role Map

Modify

Add New Role Mapping Policy

Role Mapping Policy Details

Description:

Default Role:

[Other]

Rules Evaluation Algorithm:

evaluate-all

Conditions

Role

1.

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

Student-Devs

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

3.7 Operator Service

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

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

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

Summary	Service	Authentication	Roles	Enforcement
Role Mapping Policy:	--Select-- Modify			Add New Role Mapping Policy
Role Mapping Policy Details				
Description:	-			
Default Role:	-			
Rules Evaluation Algorithm:	-			
Conditions	Role			

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

Enforcement Profiles - MPSK-Operator

Summary

Profile

Attributes

Profile:

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

Attributes:

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

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

3.8 Messaging Server

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

aruba

Dashboard

Monitoring

Configuration

Administration

ClearPass Portal

Users and Privileges

Server Manager

External Servers

SNMP Trap Receivers

Syslog Targets

Syslog Export Filters

Messaging Setup

Endpoint Context Servers

File Backup Servers

External Accounts

ClearPass Policy Manager

Administration » External Servers » Messaging Setup

Messaging

Successfully sent test email to: ariyap@hpe.com

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

SMTP Server

SMTP Settings

Server Name:smtp.gmail.com

Username:

Password:

Verify Password:

Default From Address:ariyap@hpe.com

Connection Security:StartTLS

Port:587

Connection Timeout:30 seconds

Send Test Email

Send Test SMS

Reset

Save

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

4 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.

4.1 MPSK Configuration

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

aruba ClearPass Guest Menu

Home » Administration » Aruba Integrations » MPSK Configuration

Configure MPSK

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

Configure MPSK

Auto-Configuration

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

Password Options

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

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

MPSK Example: trldjqtr Generate

Save Configuration

* required field

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

Home » Administration » Aruba Integrations » MPSK Configuration

Configure MPSK

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

Configure MPSK

Auto-Configuration

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

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

Forms

- mac_create: Add field mpsk_enable
- mac_create: Add field sponsor_email
- mac_create: Add field auto_send_smtp
- mac_create: Add field smtp_email_field
- mac_create_receipt: Add field mpsk_enable
- mac_create_receipt: Add field mpsk
- mac_edit: Add field mpsk_enable
- mac_edit: Add field mpsk_refresh
- mac_edit: Add field mpsk
- mac_edit: Add field mpsk_has_key
- mac_edit: Add field smtp_auto_send_field
- mac_edit_receipt: Add field mpsk_enable
- mac_edit_receipt: Add field mpsk
- mactrac_create: Add field mpsk_enable
- mactrac_create: Add field sponsor_email
- mactrac_create: Add field auto_send_smtp
- mactrac_create: Add field smtp_email_field
- mactrac_edit: Add field mpsk_enable
- mactrac_edit: Add field mpsk_refresh
- mactrac_edit: Add field mpsk
- mactrac_edit: Add field mpsk_has_key
- mactrac_edit: Add field smtp_auto_send_field

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

Password Options

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

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

MPSK Example: trldjqtr Generate

Save Configuration

* required field

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

4.2 Operator Profile

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

aruba

Guest

Devices

Onboard

Configuration

Administration

API Services

API Clients

API Explorer

SOAP Web Services

Aruba Integrations

Controllers

AirGroup Configuration

MPSK Configuration

Check Security

Data Retention

Extensions

Import Configuration

Operator Logins

Login Configuration

Profiles

Servers

Translation Rules

ClearPass Guest

Menu

Home » Administration » Operator Logins » Profiles

Operator Profiles

Create a new operator profile

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

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

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

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

Home » Administration » Operator Logins » Profiles

Edit Operator Profile (new)

Use this form to create a new operator profile.

Operator Profile Editor

* Name:

Students

Enter a name for this operator profile.

Description:

MPSK operator

Comments or descriptive text about the operator profile.

Access

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

Enabled:

☒ Allow operator logins

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

Operator Privileges

Administrator

No Access

Select operator permissions for system administration and management tasks.

Advertising Services

No Access

Select operator permissions for managing advertising content and services.

API Services

No Access

Select operator permissions for API access and management.

Aruba Integrations

No Access

Select operator permissions for access to Aruba integrations.

Devices

Custom...

Select operator permissions for managing devices on a network.

Create New Device

☐ No Access

☐ Read Only

☒ Full

Operators with this privilege may create individual devices.

Export Devices

☒ No Access

☐ Read Only

Operators with this privilege may export a list of devices.

Import Devices

☒ No Access

☐ Read Only

☐ Full

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

Manage Devices

☐ No Access

☐ Read Only

☒ Full

Operators with this privilege may view and manage individual devices.

Privileges:

Guest Manager
No Access

Select operator permissions for managing guest users for a network.

Hotspot Manager
No Access

Select operator permissions for managing self-provisioned guest access.

Insight
No Access

Select operator permissions for Insight application

IP Phone Services
No Access

Select operator permissions for IP phone administration and management tasks.

Onboard
No Access

Select operator permissions for managing Onboard device provisioning.

Operator Logins
No Access

Select permissions for managing local operator logins.

Pass Services
No Access

Select operator permissions for managing digital passes.

Platform
No Access

Select operator permissions for platform administration tasks.

Policy Manager
No Access

Select operator permissions for Policy Manager

SMS Services
No Access

Select operator permissions for access to SMS services.

SMTP Services
Custom...

Select operator permissions for SMTP services.

Configure SMTP Services
☒ No Access
☐ Read Only
☐ Full

Operators with this privilege may configure SMTP settings.

Send SMTP Messages
☐ No Access
☐ Read Only
☒ Full

Support Services
No Access

Select operator permissions for access to support services.

Translation Assistant
No Access

Select operator permissions for tasks related to translation.

☒ Show descriptions

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

User Roles:

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

10 rows per page

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

* Operator Filter:

No operator filter

Select the default operator filtering to apply to guest accounts.

User Account Filter:

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

Session Filter:

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

Account Limit:

0

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

User Interface

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

Skin:

(Default)

Choose the skin to use for operators with this profile.

Start Page:

(Default)

The initial page to show this operator after logging in.

Language:

Auto-detect

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

Time Zone:

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

Select the default time zone for operators with this profile.

Customization:

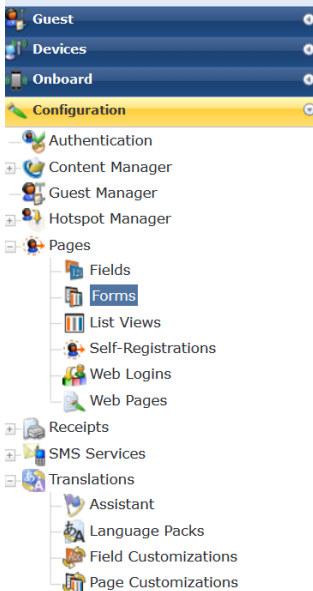
☐ Override the application's forms and views

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

Save Changes

4.3 Form Fields


The form that the users will use to register their devices is “mac_create” as seen below. You need to make sure that “sponsor_email” is enabled.




Home » Configuration » Pages » Forms

Customize Form Fields (mac_create)

Use this list view to modify the fields of the form **mac_create**.

 Quick Help

 Preview Form

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

AirGroup uses device ownership and

AirGroup uses device ownership and

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

Home » Configuration » Pages » Forms

Customize Form Field (sponsor_email)

Use this form to override the field **sponsor_email** in the form **mac_create**. [Edit Base Field](#)

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

Label After (HTML):	<div style="border: 1px solid green; height: 30px; width: 400px;"></div> <div style="border: 1px solid green; padding: 2px;">Insert...</div> <p>HTML to display after the user interface element. You can use Smarty template syntax in this field.</p>
Form Validation Properties These properties control how the value of this field is checked.	
Field Required:	<input type="checkbox"/> Field value must be supplied Select this option if the field cannot be omitted or left blank.
Initial Value:	<div style="border: 1px solid green; padding: 2px;">array ('generator' => 'GeneratorFromSession', 'generator_ar</div> <div style="border: 1px solid green; padding: 2px;">Revert</div> <p>Value to initialize this field with when the form is first displayed.</p>
* Validator:	<div style="border: 1px solid green; padding: 2px;">IsValidEmail</div> <p>The function used to validate the contents of a field.</p>
Validator Param:	<div style="border: 1px solid green; padding: 2px;">(None)</div> <p>Optional name of field whose value will be supplied as the argument to a validator.</p>
Validator Argument:	<div style="border: 1px solid green; padding: 2px;"> <pre>array ('allow' => array (</pre> </div> <p>Optional value to supply as the argument to a validator.</p>
Validation Error:	<div style="border: 1px solid green; padding: 2px;">Please enter a valid email address.</div> <p>The error message to display if the field's value fails validation and the validator does not return an error message directly.</p>
Advanced Properties These properties control conversion, display and dynamic behaviours.	
Advanced:	<input type="checkbox"/> Show advanced properties
Type Error:	<div style="border: 1px solid green; height: 20px; width: 400px;"></div> <p>The error message to display if the field's value is not supplied, has an incorrect type, or if conversion fails.</p>
<div style="border: 1px solid black; padding: 5px; display: inline-block;"> Save Changes </div>	

The initial value should be as shown below.

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

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

You also want to change the initial value of the

- “role_id” field to be “4” which is Student-Devs
- “creator_accept_terms” field to be “1” which is selected.

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

Guest
Devices
Onboard
Configuration
 Authentication
 Content Manager
 Guest Manager
 Hotspot Manager
 Pages
 Fields
 Forms
 List Views
 Self-Registrations
 Web Logins
 Web Pages
 Receipts
 SMS Services
 Translations

ClearPass Guest

Use this list view to modify the fields of the form **mac_create**.

Quick Help

Preview Form

Create New Device

* MAC Address:

MAC address of the device.

Sponsor's Email:

Email of the person sponsoring this account.

* Device Name:

Name of the device.

AirGroup:

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

Account Activation:

Now

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

Account Expiration:

1 year from now

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

* Account Role:

Student-Devs

Role to assign to this account.

Comments or notes stored with the account.

* Terms of Use:

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

Create

* required field