

## Contents

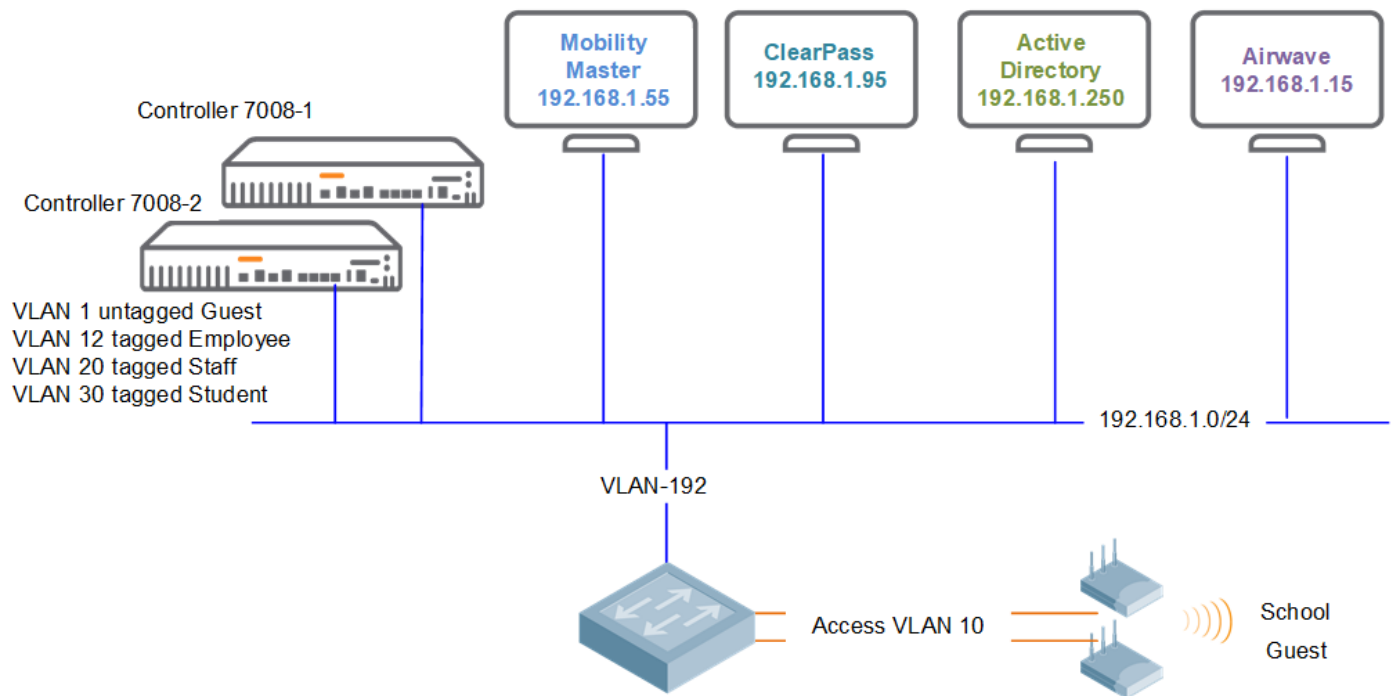
1.1	Revision History .....	1
2	Demo Topology .....	2
3	Guest Operator .....	3
3.1	ClearPass Guest Operator Configuration .....	3
4	Managed Network Dashboard .....	10

### 1.1 Revision History

DATE	VERSION	EDITOR	CHANGES
02 Feb 2021	0.1	Ariya Parsamanesh	Initial creation
15 Feb 2021	0.3	Ariya Parsamanesh	Minor modifications

## 2 Demo Topology

Here is the topology we'll be implementing. The aim here is to provide the starting point to put together a solution that include the Mobility conductor (formally known as mobility master), controllers, APs, ClearPass and Airwave.



This is the part 3 of the four parts series.

## 3 Guest Operator

In this section we'll configure a Guest operator or receptionist that can assist in creating only guest user accounts. We'll allow any user in AD user group called receptionist to be able to do this. Note that ClearPass Policy Manager has already joined the AD domain.

### 3.1 ClearPass Guest Operator Configuration

Open the Guest application by clicking the ClearPass Guest Link in the dashboard's Quick Links box for the URL redirection to ClearPass Guest.

Navigate to Home » Administration » Operator Logins » Profiles

The screenshot shows the ClearPass Guest Administration interface. On the left is a navigation menu with categories like Guest, Devices, Onboard, Configuration, and Administration. The 'Administration' menu is expanded, showing sub-items like API Services, Aruba Integrations, Check Security, Data Retention, Extensions, Import Configuration, Operator Logins (which is further expanded to show Login Configuration, Profiles, Servers, and Translation Rules), Plugin Manager, and Support. The 'Profiles' item is selected. The main content area is titled 'Operator Profiles' and contains a table listing various operator profiles. The 'Receptionist' profile is highlighted in yellow. Below the table are buttons for 'Show Details', 'Edit', 'Delete', 'Duplicate', and 'Show Usage'. At the bottom, it says '10 operator profiles' and has a 'Reload' button and a 'Show all rows' dropdown.

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.
Read-only Administrator	Operators with this profile have read-only access to the entire system.
Receptionist	Operators with this profile are limited to creating new accounts and sending receipts only, and will see the create account form on login.
Super Administrator	Default administrative profile.

For each profile that is needed, there must be a corresponding Translation Rule for operator logins to receive the correct profile. Here we'll be using "Receptionist" profile. The profile basically selects what functions are allowed.

#### Edit Operator Profile (Receptionist)

Use this form to make changes to the operator profile **Receptionist**.

The screenshot shows the 'Operator Profile Editor' form. It has two main sections: 'Basic Information' and 'Access'. The 'Basic Information' section has a '\* Name' field with 'Receptionist' entered and a 'Description' text area with the text 'Operators with this profile are limited to creating new accounts and sending receipts only, and will see the create account form on login.' The 'Access' section is titled 'Access' and has a sub-header 'These options control what operators with this profile are permitted to do.' It has an 'Enabled' checkbox which is checked. Below this is a list of 'Operator Privileges' with dropdown menus for each: Administrator (No Access), Advertising Services (No Access), API Services (No Access), Aruba Integrations (No Access), and Devices (No Access).

**Operator Profile Editor**

\* Name:  Enter a name for this operator profile.

Description:  Comments or descriptive text about the operator profile.

**Access**


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

Enabled: ☒ Allow operator logins  
If unchecked, operators with this profile will not be able to log in.

**Operator Privileges**


- Administrator:  Select operator permissions for system administration and management tasks.
- Advertising Services:  Select operator permissions for managing advertising content and services.
- API Services:  Select operator permissions for API access and management.
- Aruba Integrations:  Select operator permissions for access to Aruba integrations.
- Devices:  Select operator permissions for managing devices on a network.

Privileges:

 **Guest Manager**


Custom...

Select operator permissions for managing guest users for a network.

 **Active Sessions**


☒ No Access ☐ Read Only ☐ Full

Operators with the Active Sessions privilege may disconnect active sessions or change authorization for user accounts.

 **Active Sessions History**


☒ No Access ☐ Read Only

Operators with the Active Sessions History privilege may view the historical login access of the user accounts.

 **Change Expiration**


☒ No Access ☐ Read Only ☐ Full

Operators with this privilege may change expiration times of guest accounts.

 **Create Multiple Guest Accounts**


☒ No Access ☐ Read Only ☐ Full

Operators with this privilege may create groups of new guest accounts.

 **Create New Guest Account**


☐ No Access ☐ Read Only ☒ Full

Operators with this privilege may create individual guest accounts.

 **Edit Multiple Guest Accounts**


☐ No Access ☐ Read Only ☒ Full

Operators with this privilege may make changes to multiple guest accounts at once.

 **Export Guest Accounts**


☒ No Access ☐ Read Only

Operators with this privilege may export a list of guest accounts.

 **Full User Control**


☒ No Access ☐ Read Only ☐ Full

Operators with this privilege can change all properties of guest user accounts.

 **Import Guest Accounts**


☒ No Access ☐ Read Only ☐ Full

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

 **Manage Customization**


☒ No Access ☐ Read Only ☐ Full

Operators with this privilege may customize fields, forms and views within the application.

 **Manage Guest Accounts**


☒ No Access ☐ Read Only ☐ Full

Operators with this privilege can view a list of guest accounts.

 **Manage Print Templates**


☒ No Access ☐ Read Only ☐ Full

Operators with this privilege may manage templates used to generate guest account receipts.

 **Remove Accounts**


☒ No Access ☐ Read Only ☐ Full

Operators with this privilege may disable or remove guest accounts.

 **Reset Password**


☒ No Access ☐ Read Only ☐ Full

Operators with this privilege may reset guest account passwords.

 **Show Details**


☒ No Access ☐ Read Only ☐ Full

Operators with this privilege have the Show Details action under Manage Accounts to see all attributes for an account.

 **View Passwords**


☒ No Access ☐ Read Only

Operators with the View Passwords privilege may display the passwords for guest accounts.

 **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**


Custom...

Select operator permissions for access to SMS services.

 **Configure SMS Services**


☒ No Access ☐ Read Only ☐ Full

Operators with this privilege may configure advanced settings for SMS services.

 **Send SMS Messages**


☒ No Access ☐ Read Only ☐ Full

Operators with this privilege may send SMS messages from the application.

 **Send SMS Receipts**


☐ No Access ☐ Read Only ☒ Full

Operators with this privilege can send SMS receipt messages after creating a visitor account.

 **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

Operators with this privilege may send SMTP messages from the application.

 **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]

10 rows per page

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

\* 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.](#)

Guest Account Limit:    
 Maximum number of guests the operator can create.   
 Leave blank for no limit.

Device Account Limit:    
 Maximum number of devices the operator can create.   
 Leave blank for no limit.

**User Interface**   
 These options control the visual appearance and behavior of the application.

Skin:    
[Choose the skin to use for operators with this profile.](#)

Start Page:    
[The initial page to show this operator after logging in.](#)

Language:    
[Select the default language to use for operators with this profile.](#)

Time Zone:    
[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.

You can edit the profile based on your requirements. We have enabled “Read Only” for

- Active Sessions
- List devices
- List Guest Accounts

And full access for “Create New Guest Account”.

Now navigate to Translation rules. Home » Administration » Operator Logins » Translation Rules

Home » Administration » Operator Logins » Translation Rules

Operator Translation Rules

Use this listview to define and edit rules used to process operator attributes.

[Create new translation rule](#) [Operator Servers](#)

**Quick Help** [Create](#)

#	Name	Expression	Action	Stop
0	Map Operator Mail	mail	Assign value to operator field email	
1	Override Display Name	displayname	Assign value to operator field username	
2	RemoveAttrs	instancetype, uscreated, uschanged, objectsid, o...	Remove attribute	
3	MatchDomain	memberof contains CN=Domain Admins	Assign operator profile Super Administrator	
4	MatchAdmin	memberof contains CN=Administrators	Assign operator profile Super Administrator	
5	MatchGroup	memberof contains CN=Group Name	Assign operator profile Null Profile	
6	MatchName	cn matches /*test/	Assign operator profile Null Profile	
7	ClearPass Profile Mappings	admin_privileges	Assign value to operator field profile	

8 items [Reload](#) [Show all rows](#)

[Back to operator logins](#) [Back to administration](#) [Back to main](#)

**Quick Help** [Create](#)

#	Name	Expression	Action	Stop
0	Map Operator Mail	mail	Assign value to operator field email	
1	Override Display Name	displayname	Assign value to operator field username	
2	RemoveAttrs	instancetype, uscreated, uschanged, objectsid, o...	Remove attribute	
3	MatchDomain	memberof contains CN=Domain Admins	Assign operator profile Super Administrator	
4	MatchAdmin	memberof contains CN=Administrators	Assign operator profile Super Administrator	
5	MatchGroup	memberof contains CN=Group Name	Assign operator profile Null Profile	
6	MatchName	cn matches /*test/	Assign operator profile Null Profile	
7	ClearPass Profile Mappings	admin_privileges	Assign value to operator field profile	

[Edit](#) [Delete](#) [Duplicate](#) [Disable](#) [Move Up](#)

**Edit Translation Rule**

\* Name:    
 Enter a name for this translation rule.

Enabled: ☒ Use this rule when processing reply attributes

Attribute Name:    
 Enter the name of the attribute (e.g. memberof). Use \* for all attributes.

Matching Rule:    
 Select the matching rule to apply to the value of the attribute.

Value:    
 Enter the value to match the attribute against.

On Match:    
 Select what happens when this translation rule matches an attribute.

Operator Field:    
 Select the operator field to assign the value to.

Fallthrough: ☐ Continue translation if rule matches   
 Check this box if you want to apply multiple translation rules.

So once the receptionist user, type in their user credentials, the request should match a ClearPass Policy manager service,

- the service will check against AD user group “Receptionist”
- if the user credential and user group membership is correct then an enforcement profile will be executed to send back an attribute called “Receptionist”
- that should match a translation rule (as shown above) and the appropriate operator profile will be selected.

Now going back to ClearPass Policy manager, we’ll create the following enforcement profile

Dashboard

Monitoring

Configuration

Service Templates & Wizards

Services

Authentication

Methods

Sources

Identity

Single Sign-On (SSO)

Local Users

Endpoints

Static Host Lists

Roles

Role Mappings

Posture

Enforcement

Policies

Profiles

Network

Network Scan

Policy Simulation

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile Attributes Summary

Template:

Generic Application Enforcement

Name:

Guest Operator Login

Description:

Type:

Application

Action:

☒ Accept
 ☐ Reject
 ☐ Drop

Device Group List:

Remove View Details Modify

Profile Attributes Summary

Profile:

Template:

Generic Application Enforcement

Name:

Guest Operator Login

Description:

Type:

Application

Action:

Accept

Device Group List:

-

Attributes:

Attribute Name	Attribute Value
1. admin_privileges	= Receptionist

Profile:	Generic Application Enforcement
Name:	Guest Operator Login
Description:	
Type:	Application
Action:	Accept
Device Group List:	-

Attribute Name	Attribute Value
1. admin_privileges	= Receptionist

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
oper
Go
Clear Filter

#	Name	Type	Description
1.	Guest Operator Login	Application	
2.	[Operator Login - Admin Users]	Application	Enforcement profile for Guest admin logins
3.	[Operator Login - Local Users]	Application	Enforcement profile for Guest operator logins

Showing 1-3 of 3

Next, we’ll create a enforcement policy that will use the above enforcement profile.

Configuration » Enforcement » Policies » Edit - Ariya Guest Operator Logins

### Enforcement Policies - Ariya Guest Operator Logins

Summary Enforcement Rules

**Enforcement:**

Name: Ariya Guest Operator Logins

Description:

Enforcement Type: Application

Default Profile: [Deny Application Access Profile]

**Rules:**

Rules Evaluation Algorithm: First applicable

Conditions	Actions
1. (Authorization:Ariya AD:memberOf CONTAINS reception)	Guest Operator Login

And finally the new service that will be used to classify the authentication request.

Configuration » Services » Edit - Ariya Guest Operator Logins

### Services - Ariya Guest Operator Logins

Summary Service Authentication Roles Enforcement

Name: Ariya Guest Operator Logins

Description: Authentication Service for Guest Application

Type: Aruba Application Authentication

Status: Enabled

Monitor Mode: ☐ Enable to monitor network access without enforcement

More Options: ☐ Authorization

**Service Rule**

Matches ☐ ANY or ☒ ALL of the following conditions:

Type	Name	Operator	Value
1. Application	Name	EQUALS	Guest
2. Authentication	Type	NOT_EQUALS	SSO
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--

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: --Select-- Modify

**Role Mapping Policy Details**

Description: -

Default Role: -

Rules Evaluation Algorithm: -

Conditions	Role
------------	------

Summary Service Authentication Roles Enforcement

Use Cached Results: ☐ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: Ariya Guest Operator Logins Modify

**Enforcement Policy Details**

Description:

Default Profile: [Deny Application Access Profile]

Rules Evaluation Algorithm: first-applicable

Conditions	Enforcement Profiles
1. (Authorization:Ariya AD:memberOf CONTAINS reception)	Guest Operator Login

The last thing is to reorder the services and disable the default [guest operator logins] service.

Configuration » Services

## Services

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

Filter: Name  contains    Show  records

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

Showing 1-10 of 10

Now we'll test it out. The URL that the operators need to browse to is <https://victory.clearpass.info/guest/>  
And the user used the following credentials and authenticates successfully.



Operator Login

Username:

Password:

aruba ClearPass Guest Menu

Guest » Create Account

## Create Guest Account

✓ Last successful login from 192.168.1.128 on Sunday, 07 February 2021, 5:42 PM

i No failed attempts since last successful login

New guest account being created by reception1.

Create New Guest Account

\* Guest's Name:

Name of the guest.

\* Company Name:

Company name of the guest.

\* Email Address:

The guest's email address. This will become their username to log into the network.

Account Activation:

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

Account Expiration:

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

\* Account Role:

Role to assign to this account.

Password: 309417

Notes:

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

\* required field

[Back to guests](#)

[Back to main](#)

Now the reception user can create the guest account, the details can be emailed to the guest user as well.  
Here is the authentication session in access tracker



Dashboard
Monitoring
Live Monitoring
Access Tracker
Accounting
OnGuard Activity
Analysis & Trending
System Monitor
Profiler and Network Scan
Audit Viewer
Event Viewer
Data Filters
Blacklisted Users

Monitoring > Live Monitoring > Access Tracker

### Access Tracker

Feb 07, 2021 17:48:38 AEDT
Auto Refresh

The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.

[All Requests]
victory (192.168.1.95)
Last 1 day before Today
Edit

Filter: Request ID contains
Go Clear Filter
Show 20 records

#	Server	Source	Username	Service	Login Status	Request Timestamp
1.	192.168.1.95	Application	reception1	Ariya Guest Operator Logins	ACCEPT	2021/02/07 17:42:22
2.	192.168.1.95	RADIUS	anonymguest	GG User Authentication with MAC Caching	ACCEPT	2021/02/07 17:02:37
3.	192.168.1.95	RADIUS	a088b450c084	GG MAC Authentication	REJECT	2021/02/07 17:02:21

Request Details

Summary
Input
Output

Login Status: ACCEPT  
Session Identifier: W00000001-01-601f8bcd  
Date and Time: Feb 07, 2021 17:42:22 AEDT  
End-Host Identifier: -  
Username: reception1  
Access Device IP/Port: -  
Access Device Name: -  
System Posture Status: UNKNOWN (100)

Policies Used -

Service: Ariya Guest Operator Logins  
Authentication Method: Not applicable  
Authentication Source: Ariya AD  
Authorization Source: Ariya AD  
Roles: [User Authenticated]  
Enforcement Profiles: Guest Operator Login

Showing 1 of 1-9 records
Change Status
Show Configuration
Export
Show Logs
Close

Summary
Input
Output

Username: reception1  
End-Host Identifier: -  
Access Device IP/Port: -

Authorization Attributes

Authorization:Ariya AD:Account Expires 9223372036854775807 [30828-09-14 12:48:05 AEST]  
Authorization:Ariya AD:memberOf CN=Receptionist,CN=Users,DC=wlan,DC=net  
Authorization:Ariya AD:Name reception1  
Authorization:Ariya AD:UserDN CN=reception1,CN=Users,DC=wlan,DC=net

Computed Attributes

Summary
Input
Output

Enforcement Profiles: Guest Operator Login  
System Posture Status: UNKNOWN (100)

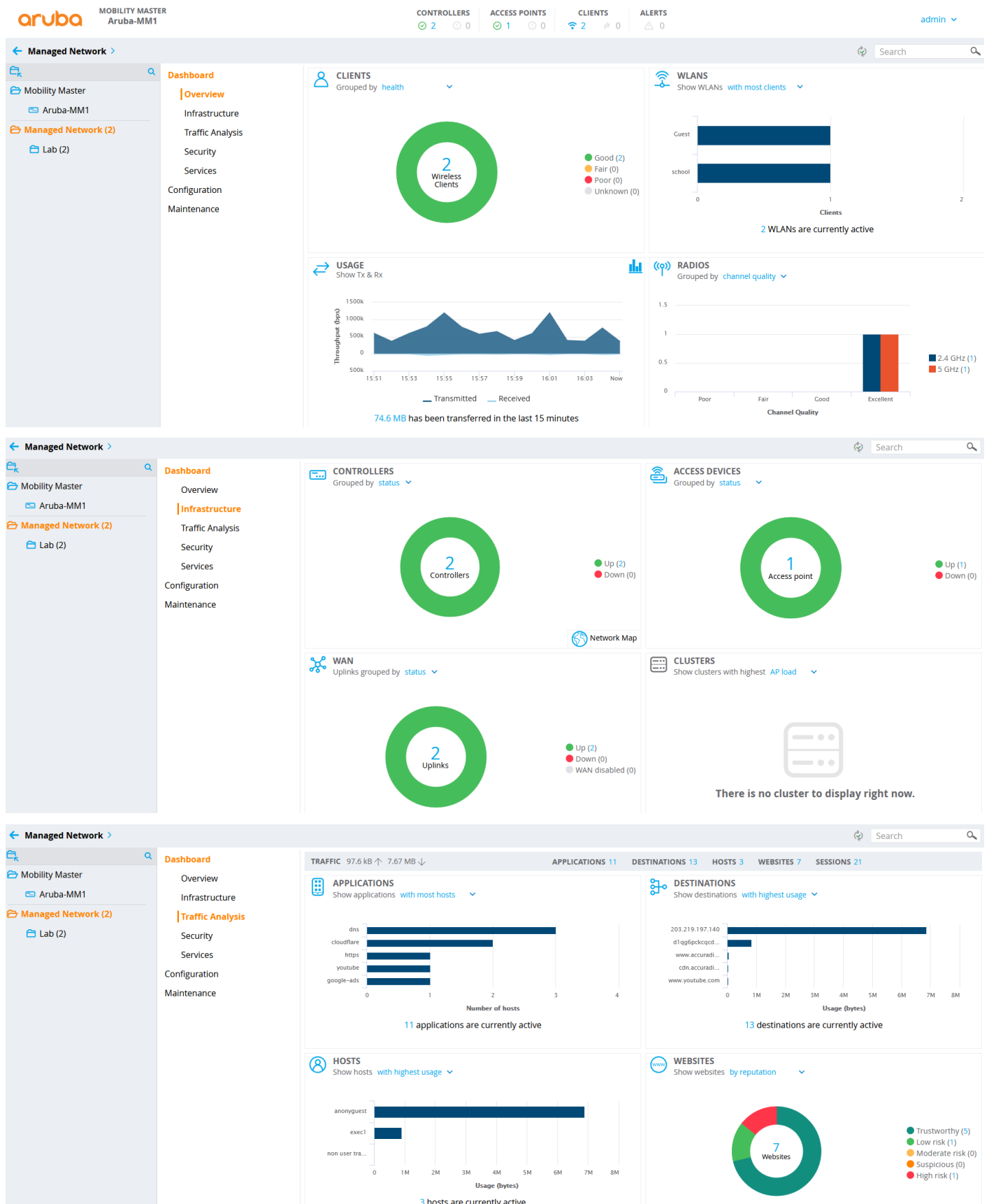
Application Response

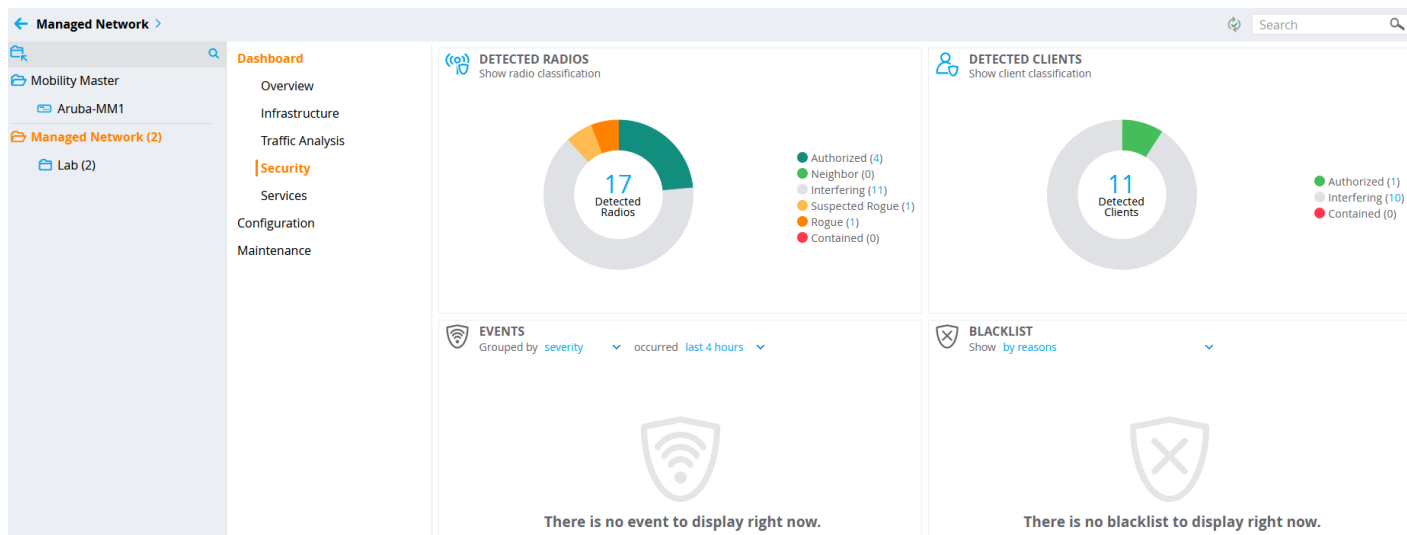
Application:admin\_privileges Receptionist

You can customise all the fields in this form which is outside the scope of this guide.

## 4 Managed Network Dashboard

This is the dashboard that you can access through MM and here we are showing the basic information that is displayed. Please refer to the user guide for the details.





Next, check part 4 of this series.