

## Contents

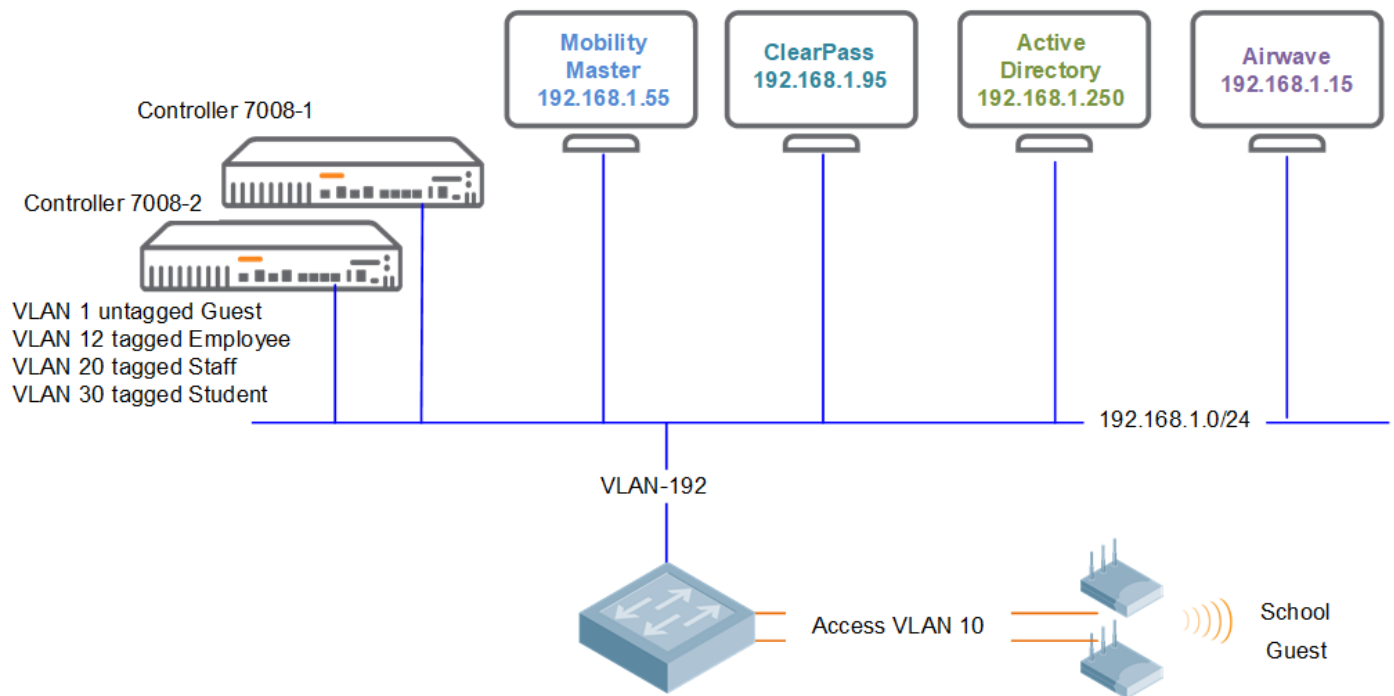
1.1	Revision History .....	1
2	Demo Topology .....	2
7	Guest Access Configuration .....	3
7.1	MM Guest Wireless Configuration .....	3
7.2	ClearPass Guest policy Configuration .....	6
7.3	ClearPass Guest Portal Configuration .....	11
7.4	Guest Testing.....	15
7.5	Captive Portal Server Certificate for MD.....	20
7.6	General Operation .....	23
8	Guest Access with Terms of use .....	24
9	Guest Operator .....	30
9.1	ClearPass Guest Operator Configuration .....	30
10	Managed Network Dashboard .....	37

### 1.1 Revision History

DATE	VERSION	EDITOR	CHANGES
02 Feb 2021	0.1	Ariya Parsamanesh	Initial creation
11 Feb 2021	0.2	Ariya Parsamanesh	Added section 9-10
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 2 of the three parts series.

# 7 Guest Access Configuration

Here we'll start with MM configuration followed by ClearPass.

## 7.1 MM Guest Wireless Configuration

We'll go through the Tasks wizard

Managed Network > Lab

Mobility Master

Managed Network (2)

Lab (2)

7008-1

7008-2

Dashboard

Configuration

WLANs

Roles & Policies

Access Points

AP Groups

Authentication

Services

Interfaces

Controllers

System

Tasks

New WLAN

General

VLANs

Security

Access

Name (SSID):

Guest

Primary usage:

☐ Employee

☒ Guest

Broadcast on:

All APs

Forwarding mode:

Tunnel

New WLAN

General

VLANs

Security

Access

VLAN:

1

[Show VLAN details](#)

New WLAN

General

VLANs

Security

Access

ClearPass or other external Captive Portal

Internal Captive Portal with authentication

Internal Captive Portal with email registration

Internal Captive Portal, no auth or registration

No Captive Portal

Captive Portal Options:

ClearPass

Auth servers:

+

Host addressing:

☒ IPv4

☐ IPv6

Host:

victory.clearpass.info

Page:

/guest/school.php

Redirect URL:

http://www.network:

Use purple wi-fi:

☐

New WLAN

General

VLANs

Security

Access

Default role:

Guest-guest-logon

So, once you deploy the configurations, the wizard created an authentication server group.

Managed Network > Lab >

Dashboard

Configuration

- WLANs
- Roles & Policies
- Access Points
- AP Groups
- Authentication**
- Services
- Interfaces
- Controllers
- System
- Tasks

Auth Servers

Server Groups 4

NAME	SERVICES	FAIL THROUGH	LOAD BALANCE	SERVICES RULES
default	2	--	--	1
internal	1	--	--	1
school_dot1_svg	1	--	--	1
<b>Guest_dot1_svg</b>	<b>1</b>	<b>--</b>	<b>--</b>	<b>0</b>

+

Server Group > Guest\_dot1\_svg

Servers

NAME	TYPE	IP ADDRESS	TRIM FQDN	MATCH RULES
ClearPass	RADIUS	192.168.1.95	--	0

Options

Server Rules

Drag rows to re-order

It also created an AAA profile with initial user role as “Guest-guest-logon”. This user role will only provide access to DHCP, DNS and redirection to ClearPass

Managed Network > Lab >

Dashboard

Configuration

- WLANs
- Roles & Policies
- Access Points
- AP Groups
- Authentication**
- Services
- Interfaces
- Controllers
- System
- Tasks
- Redundancy
- IoT
- Maintenance

Auth Servers

AAA Profiles

L2 Authentication

L3 Authentication

User Rules

Advanced

AAA Profiles

- AAA
- Guest\_aaa\_prof**
- 802.1X Authentication
- 802.1X Authentication Server Group
- MAC Authentication
- MAC Authentication Server Group
- RADIUS Accounting Server Group
- RFC 3576 server
- XML API server
- NoAuthAAAProfile
- default
- default-dot1x
- default-dot1x-psk
- default-lap-aaa-prof...

AAA Profile: Guest\_aaa\_prof

Initial role: Guest-guest-logon

MAC Authentication Default Role: guest

802.1X Authentication Default Role: guest

Download Role from CPPM: ☐

Set username from dhcp option 12: ☐

L2 Authentication Fail Through: ☐

Multiple Server Accounting: ☐

User idle timeout: seconds

Max IPv4 for wireless user: 2

RADIUS Roaming Accounting: ☐

RADIUS Interim Accounting: ☐

RADIUS Acct-Session-Id In Access-Request: ☐

User derivation rules: -None-

Now because we want to also enable MAC caching for the guest users, we need to add a MAC Authentication profile along with Auth server and accounting server groups for it. The aim of this workflow is that a new guest user gets redirected to captive portal on ClearPass and will use username/password or accepts term and conditions and gets in. Then for a specific period of time, if the same guest users disconnects and reconnects, will not get the captive portal again and will be MAC authenticated.

Managed Network > Lab >

Dashboard

Configuration

- WLANs
- Roles & Policies
- Access Points
- AP Groups
- Authentication**
- Services
- Interfaces
- Controllers
- System
- Tasks

Auth Servers

AAA Profiles

L2 Authentication

L3 Authentication

User Rules

Advanced

AAA Profiles

- AAA
- Guest\_aaa\_prof
- 802.1X Authentication
- 802.1X Authentication Server Group
- MAC Authentication**
- MAC Authentication Server Group
- RADIUS Accounting Server Group
- RFC 3576 server
- XML API server
- NoAuthAAAProfile

MAC Authentication Profile: default

MAC Authentication Profile: default

Delimiter: none

Case: lower

Max Authentication failures: 0

Reauthentication: ☐

Reauthentication Interval: 86400 sec

Use Server provided Reauthentication Interval: ☐

Managed Network > Lab >

Dashboard

Configuration

- WLANs
- Roles & Policies
- Access Points
- AP Groups
- Authentication
- Services
- Interfaces
- Controllers
- System
- Tasks

Auth Servers AAA Profiles L2 Authentication L3 Authentication User Rules Advanced

AAA Profiles

- AAA
- Guest\_aaa\_prof
- 802.1X Authentication
- 802.1X Authentication Server Group
- MAC Authentication
- MAC Authentication Server Group
- RADIUS Accounting Server Group
- RFC 3576 server
- XML API server

Server Group: Guest\_dot1\_svg

Server Group: Guest\_dot1\_svg

Fail Through: ☐

Load Balance: ☐

Managed Network > Lab >

Dashboard

Configuration

- WLANs
- Roles & Policies
- Access Points
- AP Groups
- Authentication
- Services
- Interfaces
- Controllers
- System
- Tasks

Auth Servers AAA Profiles L2 Authentication L3 Authentication User Rules Advanced

AAA Profiles

- AAA
- Guest\_aaa\_prof
- 802.1X Authentication
- 802.1X Authentication Server Group
- MAC Authentication
- MAC Authentication Server Group
- RADIUS Accounting Server Group
- RFC 3576 server
- XML API server

Server Group: Guest\_dot1\_svg

Server Group: Guest\_dot1\_svg

Fail Through: ☐

Load Balance: ☐

Managed Network > Lab >

Dashboard

Configuration

- WLANs
- Roles & Policies
- Access Points
- AP Groups
- Authentication
- Services
- Interfaces
- Controllers
- System
- Tasks

Auth Servers AAA Profiles L2 Authentication L3 Authentication User Rules Advanced

AAA Profiles

- AAA
- Guest\_aaa\_prof
- 802.1X Authentication
- 802.1X Authentication Server Group
- MAC Authentication
- MAC Authentication Server Group
- RADIUS Accounting Server Group
- RFC 3576 server
- XML API server

RFC 3576 Server

RFC 3576 SERVER

192.168.1.95

RFC 3576 server:

+

Next, we'll do some fine tuning on Captive portal profile that was created by the wizard. We'll reduce the redirect pause to 1 sec and uncheck "logout popup window"

Managed Network > Lab >

Dashboard

Configuration

- WLANs
- Roles & Policies
- Access Points
- AP Groups
- Authentication
- Services
- Interfaces
- Controllers
- System
- Tasks
- Redundancy
- IoT
- Maintenance

Auth Servers AAA Profiles L2 Authentication L3 Authentication User Rules Advanced

L3 Authentication

- Captive Portal Authentication
- Guest\_cppm\_prof
- Server Group
- default
- Stateful Kerberos Authentication
- Stateful NTLM Authentication
- VIA Authentication
- VIA Connection
- VIA Web Authentication
- VPN Authentication
- WISPr Authentication

Captive Portal Authentication Profile: Guest\_cppm\_prof

Default Role: guest

Default Guest Role: guest

Redirect Pause: 1 sec

User Login: ☒

Guest Login: ☐

Logout popup window: ☐

Use HTTP for authentication: ☐

Logon wait minimum wait: 5 sec

Logon wait maximum wait: 10 sec

logon wait CPU utilization threshold: 60 %

Max Authentication failures: 0

Lastly, note that we have not use a publicly signed HTTPS server certificate for the controllers and hence the redirection of a web page will issue a warning on the client's web browser. In all deployment it is highly recommended to have a public cert for the controllers as well as ClearPass nodes.

## 7.2 ClearPass Guest policy Configuration

We'll go through the guest confirmation needed on ClearPass. There are two part to it, one is the web pages that the client redirects to and the other is the policy service we need to create. We'll start with the policy service.

Here we are using the following template. This creates 2x services one is MAC authentication and the second one is Guest redirection to captive portal page.

The screenshot shows the Aruba ClearPass Policy Manager web interface. On the left is a navigation sidebar with categories: Dashboard, Monitoring, Configuration (selected), and Administration. Under Configuration, there are links for Service Templates & Wizards, Services, Authentication, Identity, Posture, Enforcement, and Network. The main content area is titled 'ClearPass Policy Manager' and lists several service templates: Device MAC Authentication, EDUROAM service, Encrypted Wireless Access via 802.1X Public PEAP method, Guest Access, Guest Access - Web Login, Guest Authentication with MAC Caching (highlighted in yellow), OAuth2 API User Access, Onboard, and Onboard Services Only. Each template has a brief description of its function.

Configuration » Service Templates & Wizards

### Service Templates - Guest Authentication with MAC Caching

General Wireless Network Settings **MAC Caching Settings** Posture Settings Access Restrictions

Name Prefix\*: GG

**Description**

Users first login via captive portal and their MAC addresses are cached. Subsequent logins will use MAC authentication and bypass the captive portal. Network access can be restricted based on day of the week, bandwidth limit or number of unique devices used by the User. The cache lifetime of the MAC address can vary according to the user's role (Guest, Employee or Contractor) and after that the user will have to re-authenticate via captive portal. Posture checks can be enabled, optionally, to validate the client device for antivirus, anti-spyware, firewall status. These results will determine the enforcement for the device.

◀ Back to Service Templates & Wizards Delete Next → Add Service Cancel

General Wireless Network Settings **MAC Caching Settings** Posture Settings Access Restrictions

Select NAD Client: MD-1

Wireless SSID\*: Guest

◀ Back to Service Templates & Wizards Delete Next → Add Service Cancel

General Wireless Network Settings **MAC Caching Settings** Posture Settings Access Restrictions

**Enter MAC Caching duration for the users. After this time expires, users will have to re-authenticate via captive portal**

Cache duration for Employee: One Month

Cache duration for Guest: One Day

Cache duration for Contractor: One Week

◀ Back to Service Templates & Wizards Delete Next → Add Service Cancel

General
Wireless Network Settings
MAC Caching Settings
Posture Settings
Access Restrictions

**Enable Posture Checks to perform health checks after authentication.**

Enable Posture Checks: ☐ [Configure Guest Web Login page](#)

Back to Service Templates & Wizards
Delete
Next →
Add Service
Cancel

General
Wireless Network Settings
MAC Caching Settings
Posture Settings
Access Restrictions

- Enforcement Type applies to the Captive Portal Access, Employee Access, Guest Access, and Contractor Access fields.
- Captive Portal Access is used for unauthenticated users and after the MAC caching duration has expired.
- At least one of Employee, Guest, and Contractor Access must be provided.

Enforcement Type*:	Aruba Role Enforcement
Captive Portal Access*:	Guest-guest-logout
Days allowed for access*:	<input checked="" type="checkbox"/> Monday <input checked="" type="checkbox"/> Tuesday <input checked="" type="checkbox"/> Wednesday <input checked="" type="checkbox"/> Thursday <input checked="" type="checkbox"/> Friday <input checked="" type="checkbox"/> Saturday <input checked="" type="checkbox"/> Sunday
Maximum number of devices allowed per user*:	5
Maximum bandwidth allowed per user*:	0 MB (For unlimited bandwidth, set value to 0)
Employee Access:	Employee-Guest
Guest Access:	Guest
Contractor Access:	Contractor

Back to Service Templates & Wizards
Delete
Next →
Add Service
Cancel

Services

Add
Import
Export All

- Added 15 Enforcement Profile(s)
- Added 2 Enforcement Policies
- Added 2 Role Mapping Policies
- Added 2 service(s)

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.	<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	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	
7.	<input type="checkbox"/> 7	AA Aruba 802.1X Wireless	RADIUS	Aruba 802.1X Wireless	
8.	<input type="checkbox"/> 8	GG MAC Authentication	RADIUS	MAC Authentication	
9.	<input type="checkbox"/> 9	GG User Authentication with MAC Caching	RADIUS	RADIUS Enforcement ( Generic )	

We'll look at the **MAC authentication service**

Services - GG MAC Authentication

Note: This Service is created by Service Template

Summary
Service
Authentication
Authorization
Roles
Enforcement

Name:	GG MAC Authentication
Description:	MAC Authentication bypass for captive portal users
Type:	MAC Authentication
Status:	Enabled
Monitor Mode:	<input type="checkbox"/> Enable to monitor network access without enforcement
More Options:	<input checked="" type="checkbox"/> Authorization <input type="checkbox"/> Audit End-hosts <input type="checkbox"/> Profile Endpoints <input type="checkbox"/> Accounting Proxy

Service Rule

Matches ☐ ANY or ☒ ALL of the following conditions:

Type	Name	Operator	Value
1. Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}
2. Radius:Aruba	Aruba-Essid-Name	EQUALS	Guest
3.	Click to add...		

SummaryServiceAuthenticationAuthorizationRolesEnforcement

Authentication Methods:

[Allow All MAC AUTH]

Move Up ↑

Move Down ↓

Remove

View Details

Modify

--Select to Add--

Add New Authentication Method

Authentication Sources:

[Endpoints Repository] [Local SQL DB]

Move Up ↑

Move Down ↓

Remove

View Details

Modify

--Select to Add--

Add New Authentication Source

SummaryServiceAuthenticationAuthorizationRolesEnforcement

Authorization Details:

Authorization sources from which role mapping attributes are fetched (for each Authentication Source)

Authentication Source	Attributes Fetched From
1. [Endpoints Repository] [Local SQL DB]	[Endpoints Repository] [Local SQL DB]

Additional authorization sources from which to fetch role-mapping attributes -

[Time Source] [Local SQL DB]

[Guest User Repository] [Local SQL DB]

Remove

View Details

Modify

--Select to Add--

Add New Authentication Source

SummaryServiceAuthenticationAuthorizationRolesEnforcement

Role Mapping Policy:

GG MAC Authentication Role Mapping

Modify

Add New Role Mapping Policy

Role Mapping Policy Details

Description:

Default Role:

Rules Evaluation Algorithm:

[Other]

evaluate-all

Conditions	Role
(Authorization:[Endpoints Repository]:Unique-Device-Count EXISTS ) AND (Authorization:[Time Source]:Now DT LESS_THAN %{Endpoint:MAC-Auth Expiry})	[MAC Caching]
AND (Authorization:[Guest User Repository]:AccountExpired EQUALS false) AND (Authorization:[Guest User Repository]:AccountEnabled EQUALS true)	
2. (Endpoint:Guest Role ID EQUALS 1)	[Contractor]
3. (Endpoint:Guest Role ID EQUALS 2)	[Guest]
4. (Endpoint:Guest Role ID EQUALS 3)	[Employee]

SummaryServiceAuthenticationAuthorizationRolesEnforcement

Use Cached Results:

☐ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy:

GG MAC Authentication Enforcement Policy

Modify

Add New Enforcement Policy

Enforcement Policy Details

Description:

Default Profile:

Rules Evaluation Algorithm:

[Deny Access Profile]

first-applicable

Conditions	Enforcement Profiles
(Tips:Role MATCHES_ALL [MAC Caching] 1. [Guest] [User Authenticated])	[Allow Access Profile], GG Guest Device Profile
(Tips:Role MATCHES_ALL [MAC Caching] 2. [Employee] [User Authenticated])	[Allow Access Profile], GG Employee Device Profile
(Tips:Role MATCHES_ALL [MAC Caching] 3. [Contractor] [User Authenticated])	[Allow Access Profile], GG Contractor Device Profile
(Tips:Role MATCHES_ANY [Guest] 4. [Contractor] [Employee])	[Allow Access Profile], GG Captive Portal Profile

[← Back to Services](#)

Disable

Copy

Save

Cancel

8 | Page



And here are the enforcement profiles that are used here.

Summary	Profile	Attributes
---------	---------	------------

**Profile:**

Name:	GG Guest Device Profile
Description:	Role/VLAN enforcement for Guest
Type:	RADIUS
Action:	Accept
Device Group List:	-

**Attributes:**

Type	Name	Value
1. Radius:Aruba	Aruba-User-Role	= Guest
2. Radius:IETF	User-Name	= %{Endpoint:Username}

Summary	Profile	Attributes
---------	---------	------------

**Profile:**

Name:	GG Employee Device Profile
Description:	Role/VLAN enforcement for Employee
Type:	RADIUS
Action:	Accept
Device Group List:	-

**Attributes:**

Type	Name	Value
1. Radius:Aruba	Aruba-User-Role	= Employee-Guest
2. Radius:IETF	User-Name	= %{Endpoint:Username}

Summary	Profile	Attributes
---------	---------	------------

**Profile:**

Name:	GG Contractor Device Profile
Description:	Role/VLAN enforcement for Contractor
Type:	RADIUS
Action:	Accept
Device Group List:	-

**Attributes:**

Type	Name	Value
1. Radius:Aruba	Aruba-User-Role	= Contractor
2. Radius:IETF	User-Name	= %{Endpoint:Username}

Summary	Profile	Attributes
---------	---------	------------

**Profile:**

Name:	GG Captive Portal Profile
Description:	Captive Portal Role/VLAN enforcement
Type:	RADIUS
Action:	Accept
Device Group List:	-

**Attributes:**

Type	Name	Value
1. Radius:Aruba	Aruba-User-Role	= Guest-guest-logout

Next, we'll look at the **User Authentication with MAC caching service**

Services - GG User Authentication with MAC Caching

Note: This Service is created by Service Template

Summary	Service	Authentication	Authorization	Roles	Enforcement
---------	---------	----------------	---------------	-------	-------------

Name: GG User Authentication with MAC Caching

Description: Captive Portal authentication with MAC Caching

Type: RADIUS Enforcement ( Generic )

Status: Enabled

Monitor Mode: ☐ Enable to monitor network access without enforcement

More Options: ☒ Authorization ☐ Posture Compliance ☐ Audit End-hosts ☐ Profile Endpoints ☐ Accounting Proxy

Service Rule

Matches ☐ ANY or ☒ ALL of the following conditions:

Type	Name	Operator	Value
1. Radius:IETF	Calling-Station-Id	EXISTS	
2. Connection	Client-Mac-Address	NOT_EQUALS	%{Radius:IETF:User-Name}
3. Radius:Aruba	Aruba-Essid-Name	EQUALS	Guest
Click to add...			

Summary	Service	Authentication	Authorization	Roles	Enforcement
Authentication Methods:					
		<div> [PAP]  [MSCHAP]  [CHAP] </div> <div> Move Up ↑  Move Down ↓  Remove  View Details  Modify </div>		Add New Authentication Method	
		--Select to Add--			
Authentication Sources:					
		<div> [Guest User Repository] [Local SQL DB] </div> <div> Move Up ↑  Move Down ↓  Remove  View Details  Modify </div>		Add New Authentication Source	
		--Select to Add--			

Summary	Service	Authentication	Authorization	Roles	Enforcement				
Authorization Details:									
Authorization sources from which role mapping attributes are fetched (for each Authentication Source)									
		<table border="1"> <thead> <tr> <th>Authentication Source</th> <th>Attributes Fetched From</th> </tr> </thead> <tbody> <tr> <td>1. [Guest User Repository] [Local SQL DB]</td> <td>[Guest User Repository] [Local SQL DB]</td> </tr> </tbody> </table>				Authentication Source	Attributes Fetched From	1. [Guest User Repository] [Local SQL DB]	[Guest User Repository] [Local SQL DB]
Authentication Source	Attributes Fetched From								
1. [Guest User Repository] [Local SQL DB]	[Guest User Repository] [Local SQL DB]								
Additional authorization sources from which to fetch role-mapping attributes -									
		<div> [Endpoints Repository] [Local SQL DB]  [Time Source] [Local SQL DB] </div> <div> Remove  View Details  Modify </div>		Add New Authentication Source					
		--Select to Add--							

Summary	Service	Authentication	Authorization	Roles	Enforcement								
Role Mapping Policy:													
		GG User Authentication with MAC Caching Role Mapping		Modify									
Add New Role Mapping Policy													
Role Mapping Policy Details													
Description:													
Default Role: [Other]													
Rules Evaluation Algorithm: evaluate-all													
<table border="1"> <thead> <tr> <th>Conditions</th> <th>Role</th> </tr> </thead> <tbody> <tr> <td>1. (GuestUser:Role ID EQUALS 1)</td> <td>[Contractor]</td> </tr> <tr> <td>2. (GuestUser:Role ID EQUALS 2)</td> <td>[Guest]</td> </tr> <tr> <td>3. (GuestUser:Role ID EQUALS 3)</td> <td>[Employee]</td> </tr> </tbody> </table>						Conditions	Role	1. (GuestUser:Role ID EQUALS 1)	[Contractor]	2. (GuestUser:Role ID EQUALS 2)	[Guest]	3. (GuestUser:Role ID EQUALS 3)	[Employee]
Conditions	Role												
1. (GuestUser:Role ID EQUALS 1)	[Contractor]												
2. (GuestUser:Role ID EQUALS 2)	[Guest]												
3. (GuestUser:Role ID EQUALS 3)	[Employee]												

Summary	Service	Authentication	Authorization	Roles	Enforcement										
Use Cached Results: <input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions															
Enforcement Policy:															
		GG User Authentication with MAC Caching Enforcement Policy		Modify											
Add New Enforcement Policy															
Enforcement Policy Details															
Description:															
Default Profile: [Allow Access Profile]															
Rules Evaluation Algorithm: first-applicable															
<table border="1"> <thead> <tr> <th>Conditions</th> <th>Enforcement Profiles</th> </tr> </thead> <tbody> <tr> <td>1. (Authorization:[Endpoints Repository]:Unique-Device-Count GREATER_THAN 5)</td> <td>[Deny Access Profile]</td> </tr> <tr> <td>2. (Tips:Role EQUALS [Employee]) AND (Date:Day-of-Week BELONGS_TO Monday,Tuesday,Wednesday,Thursday,Friday,Saturday,Sunday)</td> <td>GG MAC Caching Session Timeout, GG MAC Caching Bandwidth Limit, GG MAC Caching Session Limit, GG Employee MAC Caching, [Update Endpoint Known], GG MAC Caching Do Expire, GG MAC Caching Expire Post Login, GG Employee Profile</td> </tr> <tr> <td>3. (Tips:Role EQUALS [Contractor]) AND (Date:Day-of-Week BELONGS_TO Monday,Tuesday,Wednesday,Thursday,Friday,Saturday,Sunday)</td> <td>GG MAC Caching Session Timeout, GG MAC Caching Bandwidth Limit, GG MAC Caching Session Limit, GG Contractor MAC Caching, [Update Endpoint Known], GG MAC Caching Do Expire, GG MAC Caching Expire Post Login, GG Contractor Profile</td> </tr> <tr> <td>4. (Tips:Role EQUALS [Guest]) AND (Date:Day-of-Week BELONGS_TO Monday,Tuesday,Wednesday,Thursday,Friday,Saturday,Sunday)</td> <td>GG MAC Caching Session Timeout, GG MAC Caching Bandwidth Limit, GG MAC Caching Session Limit, GG Guest MAC Caching, [Update Endpoint Known], GG MAC Caching Do Expire, GG MAC Caching Expire Post Login, GG Guest Profile</td> </tr> </tbody> </table>						Conditions	Enforcement Profiles	1. (Authorization:[Endpoints Repository]:Unique-Device-Count GREATER_THAN 5)	[Deny Access Profile]	2. (Tips:Role EQUALS [Employee]) AND (Date:Day-of-Week BELONGS_TO Monday,Tuesday,Wednesday,Thursday,Friday,Saturday,Sunday)	GG MAC Caching Session Timeout, GG MAC Caching Bandwidth Limit, GG MAC Caching Session Limit, GG Employee MAC Caching, [Update Endpoint Known], GG MAC Caching Do Expire, GG MAC Caching Expire Post Login, GG Employee Profile	3. (Tips:Role EQUALS [Contractor]) AND (Date:Day-of-Week BELONGS_TO Monday,Tuesday,Wednesday,Thursday,Friday,Saturday,Sunday)	GG MAC Caching Session Timeout, GG MAC Caching Bandwidth Limit, GG MAC Caching Session Limit, GG Contractor MAC Caching, [Update Endpoint Known], GG MAC Caching Do Expire, GG MAC Caching Expire Post Login, GG Contractor Profile	4. (Tips:Role EQUALS [Guest]) AND (Date:Day-of-Week BELONGS_TO Monday,Tuesday,Wednesday,Thursday,Friday,Saturday,Sunday)	GG MAC Caching Session Timeout, GG MAC Caching Bandwidth Limit, GG MAC Caching Session Limit, GG Guest MAC Caching, [Update Endpoint Known], GG MAC Caching Do Expire, GG MAC Caching Expire Post Login, GG Guest Profile
Conditions	Enforcement Profiles														
1. (Authorization:[Endpoints Repository]:Unique-Device-Count GREATER_THAN 5)	[Deny Access Profile]														
2. (Tips:Role EQUALS [Employee]) AND (Date:Day-of-Week BELONGS_TO Monday,Tuesday,Wednesday,Thursday,Friday,Saturday,Sunday)	GG MAC Caching Session Timeout, GG MAC Caching Bandwidth Limit, GG MAC Caching Session Limit, GG Employee MAC Caching, [Update Endpoint Known], GG MAC Caching Do Expire, GG MAC Caching Expire Post Login, GG Employee Profile														
3. (Tips:Role EQUALS [Contractor]) AND (Date:Day-of-Week BELONGS_TO Monday,Tuesday,Wednesday,Thursday,Friday,Saturday,Sunday)	GG MAC Caching Session Timeout, GG MAC Caching Bandwidth Limit, GG MAC Caching Session Limit, GG Contractor MAC Caching, [Update Endpoint Known], GG MAC Caching Do Expire, GG MAC Caching Expire Post Login, GG Contractor Profile														
4. (Tips:Role EQUALS [Guest]) AND (Date:Day-of-Week BELONGS_TO Monday,Tuesday,Wednesday,Thursday,Friday,Saturday,Sunday)	GG MAC Caching Session Timeout, GG MAC Caching Bandwidth Limit, GG MAC Caching Session Limit, GG Guest MAC Caching, [Update Endpoint Known], GG MAC Caching Do Expire, GG MAC Caching Expire Post Login, GG Guest Profile														

## The enforcement profiles

Summary	Profile	Attributes
Profile:		
Name:	GG Employee Profile	
Description:	Role/VLAN enforcement for Employee	
Type:	RADIUS	
Action:	Accept	
Device Group List:	-	
Attributes:		
Type	Name	Value
1. Radius:Aruba	Aruba-User-Role	= Employee-Guest

Summary	Profile	Attributes
<b>Profile:</b>		
Name:	GG Guest Profile	
Description:	Role/VLAN enforcement for Guest	
Type:	RADIUS	
Action:	Accept	
Device Group List:	-	

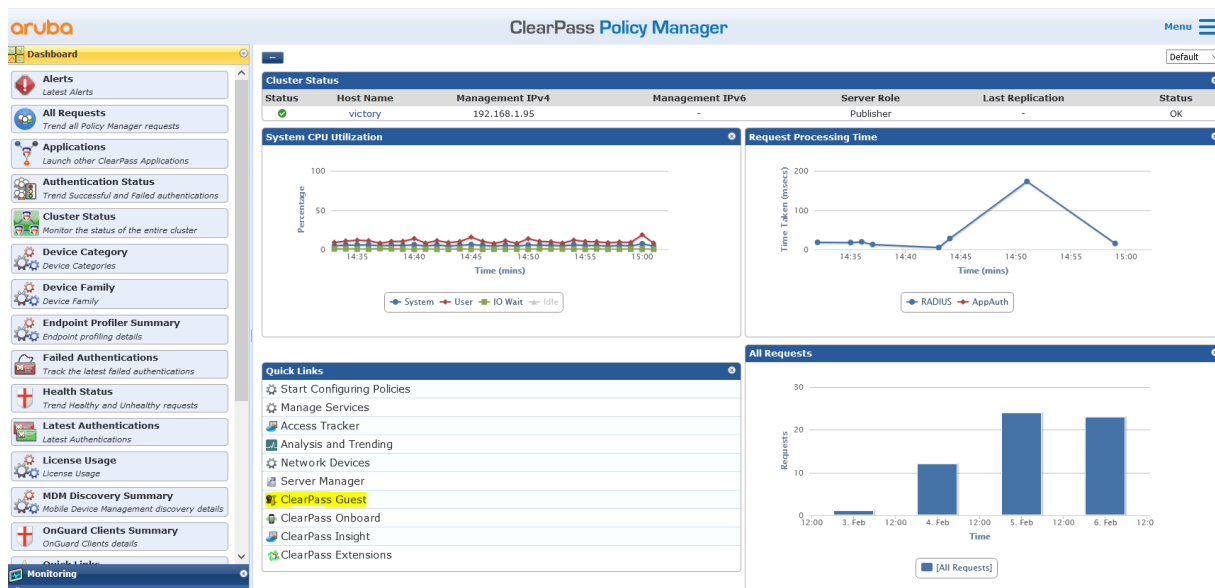
<b>Attributes:</b>				
Type	Name			Value
1. Radius:Aruba	Aruba-User-Role	=		Guest

Summary	Profile	Attributes
<b>Profile:</b>		
Name:	GG Contractor Profile	
Description:	Role/VLAN enforcement for Contractor	
Type:	RADIUS	
Action:	Accept	
Device Group List:	-	

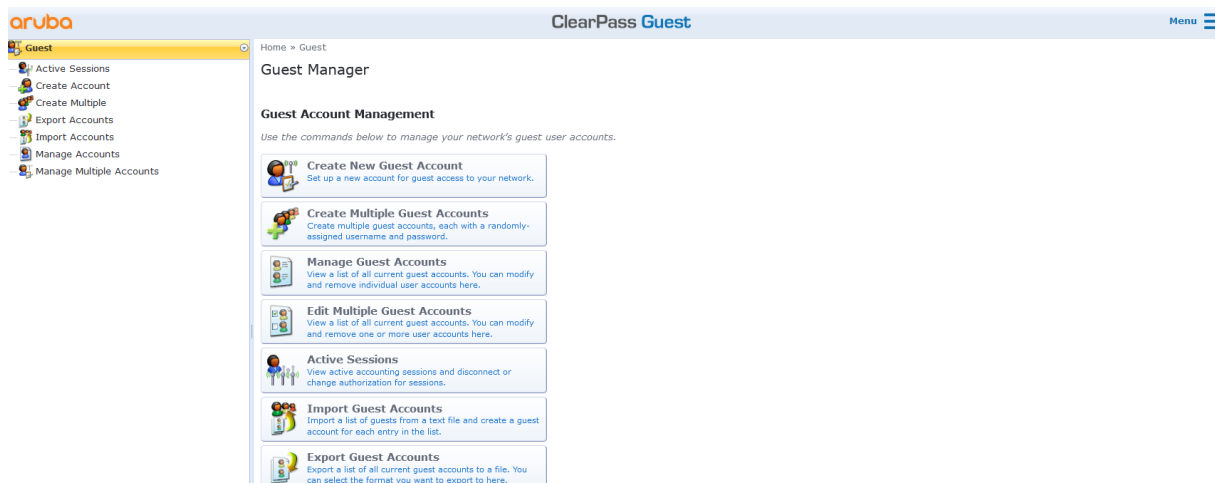
<b>Attributes:</b>				
Type	Name			Value
1. Radius:Aruba	Aruba-User-Role	=		Contractor

## 7.3 ClearPass Guest Portal Configuration

Here we'll configure the captive portal pages.



First we'll create a guest user called cpguser with no expiration on the account.



**aruba** ClearPass Guest

Home » Guest » Create Account

### Create Guest Account

*New guest account being created by admin.*

Create New Guest Account	
* Guest's Name:	<input type="text" value="cpguser"/> <small>Name of the guest.</small>
* Company Name:	<input type="text" value="cpguser"/> <small>Company name of the guest.</small>
* Email Address:	<input type="text" value="cpguser@aa.com"/> <small>The guest's email address. This will become their username to log into the network.</small>
Account Activation:	<input type="button" value="Now"/> <small>Select an option for changing the activation time of this account.</small>
Account Expiration:	<input type="button" value="Account will not expire"/> <small>Select an option for changing the expiration time of this account.</small>
* Account Role:	<input type="button" value="[Guest]"/> <small>Role to assign to this account.</small>
Password:	<b>234726</b>
Notes:	<div></div>
* Terms of Use:	<input checked="" type="checkbox"/> I am the sponsor of this account and accept the terms of use
<input type="button" value="Create"/>	

\* Required field

Once created we'll modify it to change the username and password

**aruba** ClearPass Guest

Home » Guest » Manage Accounts

### Manage Guest Accounts

*The following table shows the guest accounts that have been created. Click an account to modify it.*

Quick Help		Create	More Options	
Filter: <input type="text"/>				
Username	Role	State	Activation	Expiration
cpguser	[Guest]	Active	23 hours ago	No expiry
<input type="button" value="Reset password"/> <input type="button" value="Change expiration"/> <input type="button" value="Remove"/> <input type="button" value="Edit"/> <input type="button" value="Sessions"/> <input type="button" value="Print"/> <input type="button" value="Show Details"/>				
Refresh		1		Showing 1 - 1 of 1 20 rows per page
<input type="button" value="Back to guests"/> <input type="button" value="Back to main"/>				

**aruba** ClearPass Guest

Home » Guest » Manage Accounts

### Manage Guest Accounts

*The following table shows the guest accounts that have been created. Click an account to modify it.*

Quick Help		Create	More Options	
Filter: <input type="text"/>				
Username	Role	State	Activation	Expiration
cpguser	[Guest]	Active	23 hours ago	No expiry
<input type="button" value="Reset password"/> <input type="button" value="Change expiration"/> <input type="button" value="Remove"/> <input type="button" value="Edit"/> <input type="button" value="Sessions"/> <input type="button" value="Print"/> <input type="button" value="Show Details"/>				

*To update the properties of this guest account, use the form below:*

Edit Account	
* Guest's Name:	<input type="text" value="cpguser"/> <small>Name of the guest.</small>
* Username:	<input type="text" value="cpguser"/> <small>Name of the account.</small>
Account Activation:	<input type="button" value="(No changes: Account is active)"/> <small>Select an option for changing the activation time of this account.</small>
Account Expiration:	<input type="button" value="(No changes: Account will not expire)"/> <small>Select an option for changing the expiration time of this account.</small>
Account Lifetime:	<input type="button" value="N/A"/> <small>The amount of time after the first login before the account will expire and be deleted.</small>
Total Allowed Usage:	<input type="button" value="(No changes)"/> <small>Select an option for changing the allowed usage time of this account.</small>
Account Role:	<input type="button" value="(No changes: [Guest])"/> <small>Role to assign to this account.</small>
* Password:	<input type="button" value="Type in a new password"/> <small>Select an option for editing the guest account's password.</small>
New password:	<input type="password" value="••••••"/> <small>Type in a new password to assign to the guest account.</small>
Confirm Password:	<input type="password" value="••••••"/> <small>Repeat the new password for the guest account.</small>
Session Limit:	<input type="text" value="0"/> <small>The number of simultaneous sessions allowed for this account. Type 0 for unlimited use.</small>
Notes:	<div></div>
<input type="button" value="Update Account"/>	

Next we'll create a weblogin page, note that the page name will be in the redirection URL, also if you are using public certificate on the controllers, you need to change `securelogin.arubanetworks.com`. We'll cover this later.

Guest

Devices

Onboard

Configuration

Authentication

Content Manager

Private Files

Public Files

Guest Manager

Hotspot Manager

Pages

Fields

Forms

List Views

Self-Registrations

Web Logins

Web Pages

Receipts

SMS Services

Translations

Home » Configuration » Pages » Web Logins

Web Login (school)

Use this form to make changes to the Web Login *school*.

Web Login Editor

\* Name:

school

Enter a name for this web login page.

Page Name:

school

Enter a page name for this web login.  
The web login will be accessible from "/guest/page\_name.php".

Description:

Comments or descriptive text about the web login.

\* Vendor Settings:

Aruba

Select a predefined group of settings suitable for standard network configurations.

Login Method:

Controller-initiated — Guest browser performs HTTP form submit

Select how the user's network login will be handled.  
Server-initiated logins require the user's MAC address to be available, usually from the captive portal redirection process.

\* Address:

securelogin.arubanetworks.com

Enter the IP address or hostname of the vendor's product here.

Secure Login:

Use vendor default

Select a security option to apply to the web login process.

Dynamic Address:

☐ The controller will send the IP to submit credentials

In multi-controller deployments, it is often required to post credentials to different addresses made available as part of the original redirection.  
The address above will be used whenever the parameter is not available or fails the requirements below.

Page Redirect

Options for specifying parameters passed in the initial redirect.

Security Hash:

Do not check — login will always be permitted

Select the level of checking to apply to URL parameters passed to the web login page.  
Use this option to detect when URL parameters have been modified by the user, for example their MAC address.

Login Form

Options for specifying the behaviour and content of the login form.

Authentication:

Credentials — Require a username and password

Select the authentication requirement.  
Access Code requires a single code (username) to be entered.  
Anonymous allows a blank form requiring just the terms or a Log In button. A pre-existing account is required.  
Auto is similar to anonymous but the page is automatically submitted.  
Access Code and Anonymous require the account to have the Username Authentication field set.

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.

Custom Form:

☐ Provide a custom login form

If selected, you must supply your own HTML login form in the Header or Footer HTML areas.

Custom Labels:

☐ Override the default labels and error messages

If selected, you will be able to alter labels and error messages for the current login form.

\* Pre-Auth Check:

None — no extra checks will be made

Select how the username and password should be checked before proceeding to the NAS authentication.

Terms:

☒ Require a Terms and Conditions confirmation

If checked, the user will be forced to accept a Terms and Conditions checkbox.

CAPTCHA:

None

Select a CAPTCHA mode.

Default Destination

Options for controlling the destination clients will redirect to after login.

\* Default URL:

Enter the default URL to redirect clients.  
Please ensure you prepend "http://" for any external domain.

Override Destination:

☐ Force default destination for all clients

If selected, the client's default destination will be overridden regardless of its value.

**Login Page**  
Options for controlling the look and feel of the login page.

\* Skin: Galleria Skin 3  
Choose the skin to use when this web login page is displayed.

Title:   
The title to display on the web login page.  
Leave blank to use the default (Login).

Header HTML: 

```
{nwa_cookiecheck}
{if $errmsg}{nwaicontext type=error}{$errmsg|escape}{/nwaicontext}{/if}

{nwa_text id=7980}<p>
Please login to the network using your
username and password.
</p>/nwa_text}

```

Insert...  
HTML template code displayed before the login form.

Footer HTML: 

```
{nwa_text id=7979}<p>
Contact a staff member if you are experiencing
difficulty logging in.
</p>/nwa_text}

```

Insert...  
HTML template code displayed after the login form.

Login Message: 

```
{nwa_text id=7978}<p>
Logging in, please wait...
</p>/nwa_text}

```

Insert...  
HTML template code displayed while the login attempt is in progress.

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

#### Advertising Services

Enable advertising content on the login page.

Advertising: ☐ Enable Advertising Services content

#### Cloud Identity

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

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

#### Multi-Factor Authentication

Require a secondary factor when authenticating.

Provider: No multi-factor authentication

#### Network Login Access

Controls access to the login page.

Allowed Access:

Enter the IP addresses and networks from which logins are permitted.

Denied Access:

Enter the IP addresses and networks that are denied login access.

\* Deny Behavior: Send HTTP 404 Not Found status

Select the response of the system to a request that is not permitted.

#### Post-Authentication

Actions to perform after a successful pre-authentication.

Health Check: ☐ Require a successful OnGuard health check  
If selected, the guest will be required to pass a health check prior to accessing the network.

Update Endpoint: ☐ Mark the user's MAC address as a known endpoint  
If selected, the endpoint's attributes will also be updated with other details from the user account.

Save Changes Save and Reload

**aruba** **ClearPass Guest** Menu

Home » Configuration » Pages » Web Logins

**Web Logins** Create a new web login page

Many NAS devices support Web-based authentication for visitors.

By defining a web login page on the ClearPass Guest you are able to provide a customized graphical login page for visitors accessing the network through these NAS devices.

Use this list view to define new web login pages, and to make changes to existing web login pages.

Onboard device provisioning pages are now managed from the Web Login tab within provisioning settings

Name	Page Title	Page Name	Page Skin
school		school	Galleria Skin 3
Edit  Duplicate  Delete  Translations  Launch			

1 web login Reload Show all rows

Back to pages  
Back to configuration  
Back to main

You can test the page as well, when you'll click on the launch a tab will open and you'll see the captive portal note the URL which in this case is [https://victory.clearpass.info/guest/school.php?\\_browser=1](https://victory.clearpass.info/guest/school.php?_browser=1)

The "guest/school.php" is used in the URL redirection which we configured in MM

Now go to content manager and upload your terms and condition page.

**aruba** ClearPass Guest

Home » Configuration » Content Manager » Public Files

### Public Files

Use this list view to manage the content items stored on this ClearPass Guest.

These files are public and will be accessible via HTTP/HTTPS under /guest/public.

Currently showing directory: **Root Directory**.

Name	Owner	Type	Date Modified	Size
advertising-campaigns-blue.png		image/png	2021-02-06 11:14	24.0 KB
advertising-campaigns-orange.png		image/png	2021-02-06 11:14	25.1 KB
advertising-campaigns-steel.jpg		image/jpeg	2021-02-06 11:14	26.7 KB
advertising-services-blue-728x90.png		image/png	2021-02-06 11:14	25.3 KB
advertising-services-orange-728x90.png		image/png	2021-02-06 11:14	25.3 KB
advertising-services-steel-728x90.jpg		image/jpeg	2021-02-06 11:14	24.2 KB
<b>terms.html</b>	admin	text/html	2021-02-06 11:14	2.9 KB

Quick Help | Upload New Content | Download New Content | Create New Directory

Properties | Delete | Rename | Download | View Content | Quick View | Edit

#### School Guest Wireless Access Acceptable Use Policy

This Policy is a guide to the acceptable use of the School Guest Wireless network facilities and services.

Any individual connected to the Guest Wireless Network in order to use it directly or to connect to any other network(s), must comply with this policy, the stated purposes and Acceptable Use policies of any other network(s) or host(s) used, and all applicable laws, rules, and regulations.

School MAKES NO REPRESENTATIONS OR WARRANTIES CONCERNING THE AVAILABILITY OR SECURITY OF THE GUEST WIRELESS NETWORK, AND ALL USE IS PROVIDED ON AN AS-IS BASIS. BY USING THE GUEST WIRELESS NETWORK YOU AGREE TO DEFEND, INDEMNIFY, AND HOLD HARMLESS School FOR ANY LOSSES OR DAMAGES THAT MAY RESULT FROM YOUR USE OF THE GUEST WIRELESS NETWORK.

School takes no responsibility and assumes no liability for any content uploaded, shared, transmitted, or downloaded by you or any third party, or for anything you may encounter or any data that may be lost or compromised while connected to the Guest Wireless Network.

## 7.4 Guest Testing

Now we'll get a test device to connect to Guest SSID, it gets automatically redirected to guest page in ClearPass but the browser will issue a warning

**Login to network**

You must log in to this network before you can access the Internet.

[Open Network Login Page](#) [Advanced...](#)

Web sites prove their identity via certificates, which are issued by certificate authorities.

Firefox is backed by the non-profit Mozilla, which administers a completely open certificate authority (CA) store. The CA store helps ensure that certificate authorities are following best practices for user security.

Firefox uses the Mozilla CA store to verify that a connection is secure, rather than certificates supplied by the user's operating system. So, if an antivirus program or a network is intercepting a connection with a security certificate issued by a CA that is not in the Mozilla CA store, the connection is considered unsafe.

Error code: **MOZILLA\_PKIX\_ERROR\_MITM\_DETECTED**

[View Certificate](#)

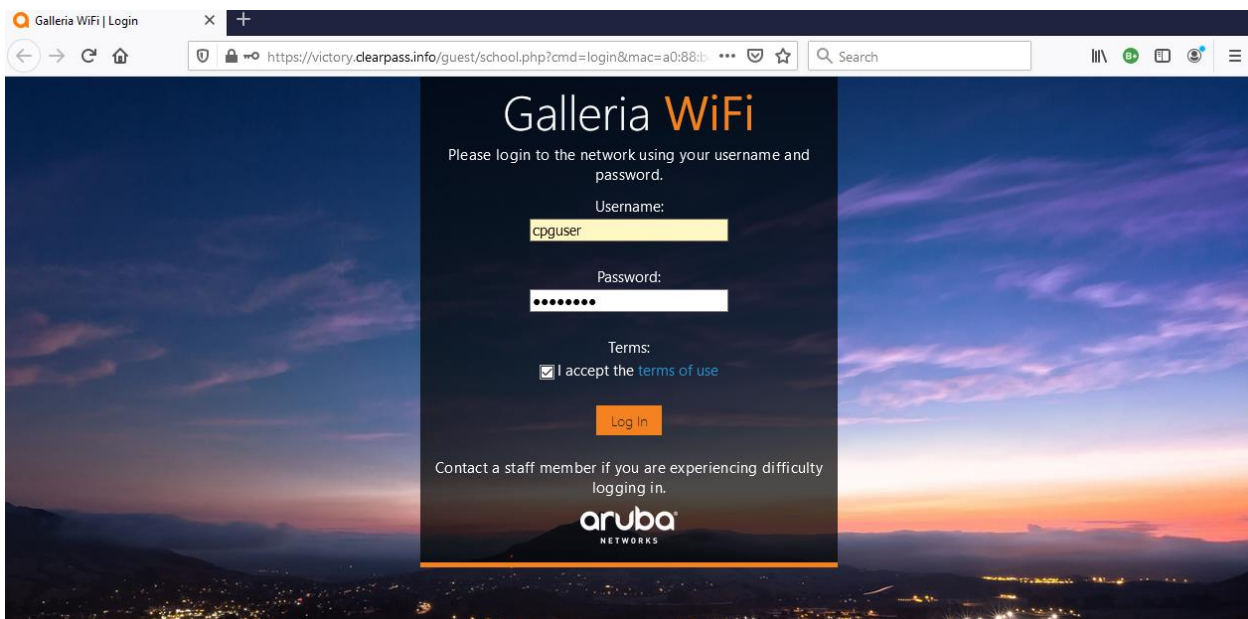
[Go Back \(Recommended\)](#) [Accept the Risk and Continue](#)

We'll have a look at the certificate, and we'll see it is the default captive portal certificate which is on the controller.

## Certificate

securelogin.arubanetworks.com	
<b>Subject Name</b>	
Common Name	securelogin.arubanetworks.com
Organisation	Aruba Networks
Country	US
<b>Issuer Name</b>	
Common Name	Aruba7008-CNDRJSP06J
Organisation	Aruba Networks
Country	US
<b>Validity</b>	
Not Before	1/1/2016, 11:00:00 AM (Australian Eastern Daylight Time)
Not After	1/26/2051, 11:08:30 PM (Australian Eastern Daylight Time)

We'll accept this and carry on, but for all deployments you need to have a public server certificate for your controllers. Once we accept the certificate, we'll get redirected to the captive portal page on ClearPass



Before we login with our guest credentials, we'll look at the MM dashboard and see the user is in guest-login role with minimum access.

**aruba** MOBILITY MASTER Aruba-MM1

CONTROLLERS 2 ACCESS POINTS 1 CLIENTS 1 ALERTS 0

admin

Managed Network

Dashboard

Overview

Infrastructure

Traffic Analysis

Security

1 Client

2 WLANs

19.4 MB

2 Radios

Wireless Clients 1

NAME	IP ADDRESS	HEALTH	BAND	ROLE	SNR	USAGE	WLAN	CONNECTE...
192.168.1.123	192.168.1.123	Good	5 GHz	Guest-guest-logon	44 dB	-	Guest	20:4c:03:5c:05:6e



Then we'll check the access tracker and see that we have a failed MAC authentication.

The screenshot shows the Aruba Access Tracker interface. The left sidebar lists various monitoring tools. The main panel displays the 'Access Tracker' for February 06, 2021, at 14:46:43 AEDT. It shows a table of requests with the following data:

#	Server	Source	Username	Service	Login Status	Request Timestamp
1.	192.168.1.95	RADIUS	a088b450c084	GG MAC Authentication	REJECT	2021/02/06 14:43:48

The first screenshot shows the 'Request Details' for the failed authentication. The 'Summary' tab is selected, showing the following information:

- Login Status: **REJECT**
- Session Identifier: R00000012-01-601e1074
- Date and Time: Feb 06, 2021 14:43:48 AEDT
- End-Host Identifier: A0-88-B4-50-C0-84 (Computer / Windows / Windows)
- Username: a088b450c084
- Access Device IP/Port: 192.168.1.57 (MD-1 / Aruba)
- Access Device Name: 7008-1
- System Posture Status: UNKNOWN (100)

The 'Policies Used' section shows:

- Service: GG MAC Authentication
- Authentication Method: MAC-AUTH
- Authentication Source: None
- Authorization Source: [Guest User Repository], [Endpoints Repository], [Time Source]
- Roles: [Other], [User Authenticated]
- Enforcement Profiles: [Deny Access Profile]

The second screenshot shows the 'Request Details' for the same request, but with the 'Output' tab selected. It displays the following information:

- Enforcement Profiles: [Deny Access Profile]
- System Posture Status: UNKNOWN (100)
- Audit Posture Status: UNKNOWN (100)

This is normal as this MAC address has not been seen before and hence the failed MAC authentication.

Now when the user performs the login process with cpguser credentials, the following will be seen.

The screenshot shows the Aruba securelogin page. The browser address bar displays 'https://securelogin.arubanetworks.com/cgi-bin/login'. The page content includes the following text:

**Authentication successful**

In 1 seconds you will be automatically redirected to <http://www.arubanetworks.com>.

Click [here](#) to go there directly.

Click [here](#) to bookmark this page.

logout

And then redirected to the page that was configured on the AAA profile on the MM

The screenshot shows the Aruba website homepage. The header includes the Aruba logo and navigation links: Products, Solutions, Services, Support, Resources, Partners, and TRY CENTRAL. The main content area features a large image of three students smiling and looking at a tablet. The text on the page reads:

# What defines the Edge?

It's where big ideas are born. Where action happens.

DEFINE YOUR EDGE

The MM dashboard and access tracker show that the user role is now "guest".

aruba MOBILITY MASTER Aruba-MM1

CONTROLLERS 2 ACCESS POINTS 1 CLIENTS 1 ALERTS 0

admin

Managed Network

Dashboard Overview

Infrastructure Traffic Analysis Security

1 Client 2 WLANs 19.6 MB 2 Radios

Wireless Clients 1

NAME	IP ADDRESS	HEALTH	BAND	ROLE	SNR	USAGE	WLAN	CONNECTE...
cpguser	192.168.1.123	Good	5 GHz	guest	44 dB	32.6 kB	Guest	20:4c:03:5c:05:6e

And the access tracker shows a successful authentication that matches with “GG User Authentication with MAC Caching” policy.

Monitoring » Live Monitoring » Access Tracker

Access Tracker Feb 06, 2021 14:52:26 AEDT

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

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

Filter: Request ID contains Go Clear Filter Show 20 records

#	Server	Source	Username	Service	Login Status	Request Timestamp
1.	192.168.1.95	RADIUS	cpguser	GG User Authentication with MAC Caching	ACCEPT	2021/02/06 14:51:23
2.	192.168.1.95	RADIUS	a088b450c084	GG MAC Authentication	REJECT	2021/02/06 14:43:48

Request Details

Summary Input Output Accounting

Login Status: ACCEPT

Session Identifier: R00000013-01-601e123b

Date and Time: Feb 06, 2021 14:51:23 AEDT

End-Host Identifier: A0-88-B4-50-C0-84 (Computer / Windows / Windows)

Username: cpguser

Access Device IP/Port: 192.168.1.57 (MD-1 / Aruba)

Access Device Name: 7008-1

System Posture Status: UNKNOWN (100)

Policies Used -

Service: GG User Authentication with MAC Caching

Authentication Method: PAP

Authentication Source: Local:localhost

Authorization Source: [Guest User Repository], [Endpoints Repository], [Time Source]

Roles: [Guest], [User Authenticated]

Enforcement Profiles: GG MAC Cachina Bandwidth Limit. GG MAC Cachina Session Limit. GG Guest MAC

Showing 1 of 1-20 records Change Status Show Configuration Export Show Logs Close

Summary Input Output Accounting

Post Login, GG MAC Caching Session Timeout, GG Guest Profile

System Posture Status: UNKNOWN (100)

Audit Posture Status: UNKNOWN (100)

RADIUS Response

Bandwidth-Check:Allowed-Limit	0
Bandwidth-Check:Check-Type	Today
Bandwidth-Check:Limit-Units	MB
Endpoint:Guest Role ID	2
Endpoint:MAC-Auth Expiry	2021-02-07 14:00:00
Endpoint:Username	cpguser
Expire-Time-Update:GuestUser	0
Expiry-Check:Expiry-Action	0
Post-Auth-Check:Action	Disconnect
Post-Auth-Check:Action	Disconnect and Block Access
Radius:Aruba:Aruba-User-Role	Guest

Showing 1 of 1-20 records Change Status Show Configuration Export Show Logs Close

Also note that one of the post authentication actions were to update the endpoint repository status for that MAC address to be “known”.



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 06, 2021 14:59:48 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	RADIUS	cpguser	GG MAC Authentication	ACCEPT	2021/02/06 14:59:42
2.	192.168.1.95	RADIUS	cpguser	GG User Authentication with MAC Caching	ACCEPT	2021/02/06 14:51:23
3.	192.168.1.95	RADIUS	a088b450c084	GG MAC Authentication	REJECT	2021/02/06 14:43:48

Looking at the details of that session

Request Details

Summary

Input

Output

Accounting

Login Status:

ACCEPT

Session Identifier:

R00000014-01-601e142e

Date and Time:

Feb 06, 2021 14:59:42 AEDT

End-Host Identifier:

A0-88-B4-50-C0-84 (Computer / Windows / Windows)

Username:

cpguser

Access Device IP/Port:

192.168.1.57 (MD-1 / Aruba)

Access Device Name:

7008-1

System Posture Status:

UNKNOWN (100)

Policies Used -

Service:

GG MAC Authentication

Authentication Method:

MAC-AUTH

Authentication Source:

Local:localhost

Authorization Source:

[Guest User Repository], [Endpoints Repository], [Time Source]

Roles:

[Guest], [MAC Caching], [User Authenticated]

Enforcement Profiles:

[Allow Access Profile], GG Guest Device Profile

Request Details

Summary

Input

Output

Accounting

Enforcement Profiles:

[Allow Access Profile], GG Guest Device Profile

System Posture Status:

UNKNOWN (100)

Audit Posture Status:

UNKNOWN (100)

RADIUS Response

Radius:Aruba:Aruba-User-Role

Guest

Radius:IETF:User-Name

cpguser

## 7.5 Captive Portal Server Certificate for MD

Here we'll upload a wild card public certificate to every MD which then can be used for Captive portal server certificate.

aruba

MOBILITY MASTER

Aruba-MM1

CONTROLLERS

1

ACCESS POINTS

0

CLIENTS

0

ALERTS

0

admin

Managed Network > Lab > 7008-1

Version 8.5.0.7

Dashboard

Configuration

WLANs

Roles & Policies

Access Points

AP Groups

Authentication

Services

Interfaces

Controller

System

Tasks

Redundancy

Maintenance

General

Admin

AirWave

CPSec

Certificates

SNMP

Logging

Profiles

More

Import Certificates

Import Certificates

NAME	TYPE	FILENAME	REFERENCES	EXPIRED
master-ssh-pub-cert	PublicCert	master-ssh-pub-cert	--	No

New Certificate

Certificate name:

CP-server-cert

Certificate filename:

clearpass.info-contr

Browse

Optional passphrase:

.....

Retype passphrase:

.....

Certificate format:

PEM

Certificate type:

ServerCert

Once it is submitted.

Managed Network > Lab > 7008-1 Version 8.6.0.7

Dashboard

Configuration

WLANs

Roles & Policies

Access Points

AP Groups

Authentication

Services

Interfaces

Controller

System

Tasks

Redundancy

Maintenance

General Admin AirWave CPsec Certificates SNMP Logging Profiles More

NAME	TYPE	FILENAME	REFERENCES	EXPIRED
master-ssh-pub-cert	PublicCert	master-ssh-pub-cert	--	No
CP-server-cert	ServerCert	clearpass.info-controller...	--	No

+

Certificate > CP-server-cert General Details

This certificate is intended for the following purpose(s):

- All issuance policies
- Ensures the identity of a remote computer

Issued to: \*.clearpass.info

Issued by: AlphaSSL CA - SHA256 - G2

Valid from: Nov 2, 2020 23:05:51 GMT

Valid to: Dec 4, 2021 23:05:51 GMT

Managed Network > Lab > 7008-1 Version 8.6.0.7

Dashboard

Configuration

WLANs

Roles & Policies

Access Points

AP Groups

Authentication

Services

Interfaces

Controller

System

Tasks

Redundancy

Maintenance

General Admin AirWave CPsec Certificates SNMP Logging Profiles More

Import Certificates

NAME	TYPE	FILENAME	REFERENCES	EXPIRED
master-ssh-pub-cert	PublicCert	master-ssh-pub-cert	--	No
CP-server-cert	ServerCert	clearpass.info-controller.pem	--	No

+

Certificate > CP-server-cert General Details

Version: 3 (0x2)

Serial number: 14155746B177D8AC839BC421

Signature algorithm: sha256WithRSAEncryption

Issuer: AlphaSSL CA - SHA256 - G2

Valid from: Nov 2, 2020 23:05:51 GMT

Valid to: Dec 4, 2021 23:05:51 GMT

Subject: \*.clearpass.info

Public key: rsaEncryption (2048 bit)

Key usage: Digital Signature, Key Encipherment

Thumbprint algorithm: SHA1

Thumbprint: 39:63:DF:EA:69:4E:3B:C2:CC:6A:85:B9:D8:06:47:57:BF:47:B6:CC

Now you need to assign it as Captive Portal certificate.

Managed Network > Lab > 7008-1 Version 8.6.0.7

Dashboard

Configuration

WLANs

Roles & Policies

Access Points

AP Groups

Authentication

Services

Interfaces

Controller

System

Tasks

Redundancy

Maintenance

General Admin AirWave CPsec Certificates SNMP Logging Profiles More

> Spanning Tree

> LACP

> Capacity Threshold

> Phone Home

> General

CAPTIVE PORTAL CERTIFICATE

Server certificate: CP-server-cert

IDP SERVER CERTIFICATE

Server certificate: default

CONFIGURE SSL/TLS PROTOCOL

SSL protocol: ☐ TLSv1 ☐ TLSv1.1 ☒ TLSv1.2

Checking it from the CLI

(7008-1) #show crypto pki serverCert

Certificates of All Nodes

Name	Expired
CP-server-cert	No

(7008-1) #show crypto pki serverCert CP-server-cert

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

14:15:57:46:b1:77:d8:ac:83:9b:c4:21

Signature Algorithm: sha256WithRSAEncryption

Issuer: C=BE, O=GlobalSign nv-sa, CN=AlphaSSL CA - SHA256 - G2

Validity

Not Before: Nov 2 23:05:51 2020 GMT

Not After : Dec 4 23:05:51 2021 GMT

Subject: CN=\*.clearpass.info

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Modulus:

00:c9:a2:fe:62:3a:4d:1a:51:51:60:fc:50:e6:c3:  
61:25:4c:27:b5:50:93:44:62:47:33:9d:da:30:39:  
ee:ee:df:46:37:31:1d:35:b3:99:04:3e:c5:df:63:  
c3:bd:50:72:9f:93:14:9d:70:f7:ae:fb:d5:01:76:  
22:46:c2:b5:0e:f1:b0:a2:be:c2:41:43:e9:82:bc:  
b2:9c:eb:f2:ee:cb:e8:0e:57:52:ac:47:01:db:75:  
51:3b:68:9c:a2:19:57:03:69:db:b1:dd:60:d7:55:  
c3:ec:1b:e1:80:50:93:1b:92:45:6e:5c:2c:44:fb:  
5a:55:09:1b:00:d2:63:e3:64:2e:ac:13:24:65:1b:  
6a:3b:ad:ea:a2:46:04:cf:44:f1:81:42:fc:29:14:  
ca:f1:77:94:d5:48:a9:ec:a7:7e:73:6b:96:a6:35:  
4e:81:2b:4b:5f:ca:1f:b1:d0:f0:dc:11:fa:b8:e6:  
08:bc:20:dd:74:57:1e:3f:17:15:77:29:b0:02:52:  
c2:c1:58:ca:4c:ee:e1:fa:fe:30:a5:5a:e0:7f:e9:  
c0:14:03:e1:78:51:40:12:7c:53:56:c2:7b:a1:44:  
83:16:dc:d4:f0:ce:b8:c3:23:e8:b7:c1:a1:71:8b:  
a5:45:fd:07:0a:58:19:41:96:0f:b2:05:c6:66:a0:  
3f:91

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Key Usage: critical

Digital Signature, Key Encipherment

Authority Information Access:

CA Issuers - URI:<http://secure2.alphassl.com/cacert/gsalphasha2g2r1.crt>

OCSP - URI:<http://ocsp2.globalsign.com/gsalphasha2g2>

X509v3 Certificate Policies:

Policy: 1.3.6.1.4.1.4146.1.10.10

CPS: <https://www.globalsign.com/repository/>

Policy: 2.23.140.1.2.1

X509v3 Basic Constraints:

CA:FALSE

X509v3 CRL Distribution Points:

Full Name:

URI:<http://crl2.alphassl.com/gs/gsalphasha2g2.crl>

X509v3 Subject Alternative Name:

DNS:\*.clearpass.info, DNS:clearpass.info

```

X509v3 Extended Key Usage:
    TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Authority Key Identifier:
    keyid:F5:CD:D5:3C:08:50:F9:6A:4F:3A:B7:97:DA:56:83:E6:69:D2:68:F7

X509v3 Subject Key Identifier:
    A3:ED:1B:14:AE:B1:5E:1B:1F:8E:DD:D0:64:5F:E9:5D:3D:08:F7:D9
1.3.6.1.4.1.11129.2.4.2:
    .....u.oSv.1.1.....Q..w.....).....7.....u.5.Z.....F0D.
.{...+.C.9.S.~sK...[.....n.iy..%... {...4.Tw..)Q%p7..eT.4....).O._.....0.[.Eg.)..6.
=....OU...CX-o..y..58.|..Im.....F0D.
Signature Algorithm: sha256WithRSAEncryption
b5:4f:45:1e:e7:23:42:20:c3:86:4e:97:27:85:db:5b:09:5b:
ef:29:a9:00:72:4f:34:15:ec:75:e5:45:05:b8:2d:ef:55:76:
e9:03:7b:46:6a:88:e5:67:b4:3b:19:f6:3a:41:61:d8:49:3e:
23:90:08:a9:60:9f:17:ad:b0:d5:8b:99:ea:07:58:a0:ea:9f:
13:73:64:0f:25:2d:9d:48:4d:f6:46:08:55:c3:f4:43:cc:6d:
71:bd:e6:39:76:4b:ae:1c:7c:88:57:f5:4d:27:a3:b8:e0:db:
8b:9b:39:b4:76:17:c8:16:a9:cf:07:36:b7:ee:b8:fd:88:bb:
a5:9b:4f:ae:32:a9:bf:6d:16:48:c0:47:cd:aa:b6:ac:b2:6a:
8d:60:25:26:02:38:a2:b9:68:c9:4d:a5:3d:59:0a:01:ca:fc:
4c:ae:8a:68:51:3e:2f:87:a9:1a:f6:8a:ef:7e:24:63:ae:99:
03:02:eb:03:97:db:20:fb:34:a7:aa:85:01:4d:de:e3:6c:bc:
e8:6a:7d:22:e6:c4:32:b2:f6:72:05:b0:5e:68:1e:c3:af:7a:
44:68:ac:c4:a7:e2:04:f9:7e:6b:e2:68:82:c3:6d:71:89:52:
57:41:43:8d:7a:f8:83:e7:2f:08:2f:c8:32:27:69:97:d6:d8:
62:8e:c7:58

(7008-1) #

```

## 7.6 General Operation

So now when the wildcard cert is imported as captive portal cert for Controllers, it will replace the asterisk “\*” in the CN of the cert with “**captiveportal-login**”.

So in ClearPass Guest weblogin or self-registration page instead of using [securelogin.arubanetworks.com](https://securelogin.arubanetworks.com), now we should be using “**captiveportal-login.clearpass.info**”.

The screenshot shows the Aruba ClearPass Guest Web Login Editor interface. The left sidebar contains navigation links for Guest, Devices, Onboard, Configuration, Authentication, Content Manager, Guest Manager, Hotspot Manager, Pages, Receipts, SMS Services, and Translations. The main content area displays the 'Web Login (school)' configuration page. The 'Web Login Editor' form includes the following fields:

- \* Name:** school
- Page Name:** school
- Description:** (empty text area)
- \* Vendor Settings:** Aruba
- Login Method:** Controller-initiated — Guest browser performs HTTP form submit
- \* Address:** captiveportal-login.clearpass.info
- Secure Login:** Use vendor default

Now with all this in place, the users should not see any browser warning for the initial redirection to the captive portal page.



## 8 Guest Access with Terms of use

This objective here is to have an anonymous weblogin for guests to just accept the terms of use.

Create a new web login with the following:

- Authentication: Anonymous – Do not require a username or password
- Auto-Generate: Checked
- Terms: Checked
- Anonymous User: Choose a unique username of your choice. It will not be visible outside the account list. Say you chose “cpguser”
- Pre-Auth Check: Local — match a local account

Guest

Devices

Onboard

Configuration

Authentication

Content Manager

Private Files

Public Files

Guest Manager

Hotspot Manager

Pages

Fields

Forms

List Views

Self-Registrations

Web Logins

Web Pages

Receipts

SMS Services

Translations

Home » Configuration » Pages » Web Logins

Web Login (Fancy Terms and Conditions Only)

Use this form to make changes to the Web Login *Fancy Terms and Conditions Only*.

Web Login Editor

\* Name:

Fancy Terms and Conditions Only

Enter a name for this web login page.

Page Name:

t\_and\_1

Enter a page name for this web login.  
The web login will be accessible from "/guest/page\_name.php".

Description:

Comments or descriptive text about the web login.

\* Vendor Settings:

Aruba

Select a predefined group of settings suitable for standard network configurations.

Login Method:

Controller-initiated — Guest browser performs HTTP form submit

Select how the user's network login will be handled.  
Server-initiated logins require the user's MAC address to be available, usually from the captive portal redirection process.

\* Address:

captiveportal-login.clearpass.info

Enter the IP address or hostname of the vendor's product here.

Secure Login:

Use vendor default

Select a security option to apply to the web login process.

Dynamic Address:

☐ The controller will send the IP to submit credentials

In multi-controller deployments, it is often required to post credentials to different addresses made available as part of the original redirection. The address above will be used whenever the parameter is not available or fails the requirements below.

Page Redirect

Options for specifying parameters passed in the initial redirect.

Security Hash:

Do not check — login will always be permitted

Select the level of checking to apply to URL parameters passed to the web login page.  
Use this option to detect when URL parameters have been modified by the user, for example their MAC address.

Login Form

Options for specifying the behaviour and content of the login form.

Authentication:

Anonymous — Do not require a username or password

Select the authentication requirement.  
Access Code requires a single code (username) to be entered.  
Anonymous allows a blank form requiring just the terms or a Log In button. A pre-existing account is required.  
Auto is similar to anonymous but the page is automatically submitted.  
Access Code and Anonymous require the account to have the Username Authentication field set.

Auto-Generate:

☒ Create a new anonymous account

The account will be created without a session limit or expiration time, and with the Guest role (ID 2).  
Enter a value for 'Anonymous User' to use a specific username, or leave blank to randomly generate a username.

\* Anonymous User:

anonyguser

The account to use for anonymous authentication.  
The password will be visible within the HTML.  
It is recommended to increase the account Session Limit to the number of guests you wish to support.

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.

Custom Form:

☒ Provide a custom login form

If selected, you must supply your own HTML login form in the Header or Footer HTML areas.

Custom Labels:

☐ Override the default labels and error messages

If selected, you will be able to alter labels and error messages for the current login form.

\* Pre-Auth Check:

Local — match a local account

Select how the username and password should be checked before proceeding to the NAS authentication.

Terms:

☒ Require a Terms and Conditions confirmation

If checked, the user will be forced to accept a Terms and Conditions checkbox.

CAPTCHA:

None

Select a CAPTCHA mode.



<b>Default Destination</b> Options for controlling the destination clients will redirect to after login.	
* Default URL:	<input type="text"/> Enter the default URL to redirect clients. Please ensure you prepend "http://" for any external domain.
Override Destination:	<input type="checkbox"/> Force default destination for all clients If selected, the client's default destination will be overridden regardless of its value.
<b>Login Page</b> Options for controlling the look and feel of the login page.	
* Skin:	<b>ClearPass Guest Skin</b> Choose the skin to use when this web login page is displayed.
Title:	<input type="text"/> The title to display on the web login page. Leave blank to use the default (Login).
Header HTML:	<pre>{nwa_cookiecheck} {if \$errmsg}{nwa_icontext type=error}{\$errmsg escape}/{/nwa_icontext}{/if}  &lt;head&gt; &lt;title&gt;Public wireless Internet access&lt;/title&gt; &lt;/head&gt; &lt;body&gt;  &lt;div align="center" width="100%"&gt; &lt;form method="POST" accept-charset="UTF-8" enctype="application/x-www-form-urlencoded" novalidate="novalidate"&gt; {if \$radius weblogin.username auth == 'anonymous'}&lt;div style="display:none;"&gt;{/if}</pre> <input type="button" value="Insert..."/>
HTML template code displayed before the login form.	
Footer HTML:	<pre>{nwa_text id=7979}&lt;p&gt; Contact a staff member if you are experiencing difficulty logging in. &lt;/p&gt;{/nwa_text}</pre> <input type="button" value="Insert..."/>
HTML template code displayed after the login form.	
Footer HTML:	<pre>{nwa_text id=7979}&lt;p&gt; Contact a staff member if you are experiencing difficulty logging in. &lt;/p&gt;{/nwa_text}</pre> <input type="button" value="Insert..."/>
HTML template code displayed after the login form.	
Login Message:	<pre>{nwa_text id=7978}&lt;p&gt; Logging in, please wait... &lt;/p&gt;{/nwa_text}</pre> <input type="button" value="Insert..."/>
HTML template code displayed while the login attempt is in progress.	
* Login Delay:	<input type="text" value="0"/> The time in seconds to delay while displaying the login message.
<b>Advertising Services</b> Enable advertising content on the login page.	
Advertising:	<input type="checkbox"/> Enable Advertising Services content
<b>Cloud Identity</b> Optionally present guests with various cloud identity / social login options.	
Enabled:	<input type="checkbox"/> Enable logins with cloud identity / social network credentials
<b>Multi-Factor Authentication</b> Require a secondary factor when authenticating.	
Provider:	<b>No multi-factor authentication</b>
<b>Network Login Access</b> Controls access to the login page.	
Allowed Access:	<input type="text"/> Enter the IP addresses and networks from which logins are permitted.
Denied Access:	<input type="text"/> Enter the IP addresses and networks that are denied login access.
* Deny Behavior:	<b>Send HTTP 404 Not Found status</b> Select the response of the system to a request that is not permitted.
<b>Post-Authentication</b> Actions to perform after a successful pre-authentication.	
Health Check:	<input type="checkbox"/> Require a successful OnGuard health check If selected, the guest will be required to pass a health check prior to accessing the network.
Update Endpoint:	<input type="checkbox"/> Mark the user's MAC address as a known endpoint If selected, the endpoint's attributes will also be updated with other details from the user account.
<input type="button" value="Save Changes"/> <input type="button" value="Save and Reload"/>	

Here is the HTML code in the header section.

```
{nwa_cookiecheck}
{if $errmsg}{nwa_icontext type=error}{$errmsg|escape}/{/nwa_icontext}{/if}

<head>
<title>Public wireless Internet access</title>
</head>
<body>

<div align="center" width="100%">
<form method="POST" accept-charset="UTF-8" enctype="application/x-www-form-urlencoded"
novalidate="novalidate">
```

```

{if $radius_weblogin.username_auth == 'anonymous'}<div style="display:none;">{/if}

<p>
<label for="username">Username:</label><br />
<input type="text" style="width: 200px;" autocapitalize="off" autocorrect="off"
spellcheck="false" id="username" name="username" value="{ $username|escape}"><br />
{if $username_error}<span class="nwaError">{ $username_error|escape}</span><br />{/if}
</p>

{if $radius_weblogin.username_auth == 'username'}<div style="display:none;">{/if}

<p>
<label for="password">Password:</label><br />
<input type="password" style="width: 200px;" id="password" name="password"><br />
{if $password_error}<span class="nwaError">{ $password_error|escape}</span><br />{/if}
</p>

{if $radius_weblogin.username_auth}</div>{/if}

<p>
{if $url_error}<span class="nwaError">{ $url_error|escape}</span><br />{/if}
</p>

{if $radius_weblogin.login_terms_require}

<pre style="width:800px;height:520px;white-space:pre-wrap">
<B>Company X</B><br/>Guest Wireless Access Acceptable Use Policy

This Policy is a guide to the acceptable use of the Company X Guest Wireless network
facilities and services.

Any individual connected to the Guest Wireless Network in order to use it directly or
to connect to any other network(s), must comply with this policy, the stated purposes
and Acceptable Use policies of any other network(s) or host(s) used, and all applicable
laws, rules, and regulations.

COMPANY C MAKES NO REPRESENTATIONS OR WARRANTIES CONCERNING THE AVAILABILITY OR
SECURITY OF THE GUEST WIRELESS NETWORK, AND ALL USE IS PROVIDED ON AN AS-IS BASIS. BY
USING THE GUEST WIRELESS NETWORK YOU AGREE TO DEFEND, INDEMNIFY, AND HOLD HARMLESS
COMPANY C FOR ANY LOSSES OR DAMAGES THAT MAY RESULT FROM YOUR USE OF THE GUEST WIRELESS
NETWORK.

Company C takes no responsibility and assumes no liability for any content uploaded,
shared, transmitted, or downloaded by you or any third party, or for anything you may
encounter or any data that may be lost or compromised while connected to the Guest
Wireless Network.

Company C reserves the right to disconnect any user at any time and for any reason. The
Guest Wireless Network is provided as a courtesy to allow our guests access to the
internet. Users will not be given access to the Company X intranet or permission to
install any software on our computers.

</pre>
<BR><label for="visitor_accept_terms"><input type="checkbox"
name="visitor_accept_terms" id="visitor_accept_terms" />I Accept</label></br />
{if $visitor_accept_terms_error}<span
class="nwaError">{ $visitor_accept_terms_error|escape}</span><br />{/if}
</p>
{/if}
<p>
<input type="submit" style="width: 200px;" id="submit" name="submit" value="Log in">
</form>
</div>
</body>

```

And this is how it looks.

**Company X**  
Guest Wireless Access Acceptable Use Policy

This Policy is a guide to the acceptable use of the Company X Guest Wireless network facilities and services.

Any individual connected to the Guest Wireless Network in order to use it directly or to connect to any other network(s), must comply with this policy, the stated purposes and Acceptable Use policies of any other network(s) or host(s) used, and all applicable laws, rules, and regulations.

COMPANY C MAKES NO REPRESENTATIONS OR WARRANTIES CONCERNING THE AVAILABILITY OR SECURITY OF THE GUEST WIRELESS NETWORK, AND ALL USE IS PROVIDED ON AN AS-IS BASIS. BY USING THE GUEST WIRELESS NETWORK YOU AGREE TO DEFEND, INDEMNIFY, AND HOLD HARMLESS COMPANY C FOR ANY LOSSES OR DAMAGES THAT MAY RESULT FROM YOUR USE OF THE GUEST WIRELESS NETWORK.

Company C takes no responsibility and assumes no liability for any content uploaded, shared, transmitted, or downloaded by you or any third party, or for anything you may encounter or any data that may be lost or compromised while connected to the Guest Wireless Network.

Company C reserves the right to disconnect any user at any time and for any reason. The Guest Wireless Network is provided as a courtesy to allow our guests access to the internet. Users will not be given access to the Company X intranet or permission to install any software on our computers.

☐ I Accept[Log in](#)

Contact a staff member if you are experiencing difficulty logging in.

Now checking the guest account, we see the new account for anonymous guest users that was automatically generated.

**aruba**

ClearPass Guest

**Guest**

- Active Sessions
- Create Account
- Create Multiple
- Export Accounts
- Import Accounts
- Manage Accounts**
- Manage Multiple Accounts

Home » Guest » Manage Accounts

**Manage Guest Accounts**

The following table shows the guest accounts that have been created. Click an account to modify it.

**Quick Help**

**Create**

**More Options**

Filter:

Username	Role	State	Activation	Expiration
<b>anonyguest</b>	[Guest]	Active	2 minutes ago	No expiry
<b>cpguser</b>	[Guest]	Active	2 days ago	No expiry

**Refresh**

Showing 1 – 2 of 2

20 rows per page

To use this captive portal page, we'll create a new controller captive portal profile so that it is pointing to this URL and then assign it in the initial user-role guest-login.

**aruba**

MOBILITY MASTER  
Aruba-MM1

**CONTROLLERS**  
1 0

**ACCESS POINTS**  
1 0

**CLIENTS**  
0 0

**ALERTS**  
0

Managed Network > Lab >

**Dashboard**

**Configuration**

**WLANs**

**Roles & Policies**

**Access Points**

**AP Groups**

**Authentication**

**Services**

**Interfaces**

**Controllers**

**System**

**Tasks**

**Redundancy**

**IoT**

**Maintenance**

**Auth Servers**

**AAA Profiles**

**L2 Authentication**

**L3 Authentication**

**User Rules**

**Advanced**

**L3 Authentication**

**Captive Portal Authentication Profile: New Profile**

**Captive Portal Authentication Profile:** **+**

**Guest\_cppm\_prof**

**default**

**Stateful Kerberos Authentication**

**Stateful NTLM Authentication**

**VIA Authentication**

**VIA Connection**

**VIA Web Authentication**

**VPN Authentication**

**WISPr Authentication**

L3 Authentication		Captive Portal Authentication Profile: New Profile	
Captive Portal Authentication		Profile name:	guest_terms_CP_Prof
Guest_cppm_prof		Default Role:	guest
default		Default Guest Role:	guest
Stateful Kerberos Authentication		Redirect Pause:	1 sec
Stateful NTLM Authentication		User Login:	<input checked="" type="checkbox"/>
VIA Authentication		Guest Login:	<input type="checkbox"/>
VIA Connection		Logout popup window:	<input type="checkbox"/>
VIA Web Authentication		Use HTTP for authentication:	<input type="checkbox"/>
VPN Authentication		Logon wait minimum wait:	5 sec
WISPr Authentication		Logon wait maximum wait:	10 sec
		logon wait CPU utilization threshold:	60 %
		Max Authentication failures:	0
		Show FQDN:	<input type="checkbox"/>
		Authentication Protocol:	PAP
		Login page:	victory.clearpass.info

The login page is “https://victory.clearpass.info/guest/t\_and\_1.php?”

L3 Authentication		Server Group: Guest_dot1_svg	
Captive Portal Authentication		Server Group:	Guest_dot1_svg
Guest_cppm_prof		Fail Through:	<input type="checkbox"/>
Guest_terms_CP_Prof		Load Balance:	<input type="checkbox"/>
Server Group			
default			
Stateful Kerberos Authentication			
Stateful NTLM Authentication			
VIA Authentication			
VIA Connection			
VIA Web Authentication			
VPN Authentication			
WISPr Authentication			

Now changing the guest-logout role to point to the new created captive portal profile.

Managed Network > Lab

Dashboard

Configuration

- WLANs
- Roles & Policies
- Access Points
- AP Groups
- Authentication
- Services
- Interfaces
- Controllers
- System
- Tasks
- Redundancy
- IoT
- Maintenance

Roles Policies Applications Aliases

Guest-guest-logout 28 Rules

Staff 2 Rules

Student 2 Rules

+

Guest-guest-logout Policies Bandwidth Captive Portal More [Show Basic View](#)

> Network

> VPN

> Authentication

IDP profile: -None-

Stateful NTLM profile: -None-

Stateful Kerberos profile: -None-

WISPr profile: -None-

Captive portal profile: Guest\_terms\_CP\_Prof

Captive portal check for accounting: ☒

Now when a client connects to the guest WLAN network, it will use the T&Cs weblogin and after the user accepts the terms, they get access to the network.

MOBILITY MASTER  
Aruba-MM1

CONTROLLERS

ACCESS POINTS

CLIENTS

ALERTS

admin

Managed Network

Dashboard

Overview

Infrastructure

Traffic Analysis

Security

Services

1 Client

2 WLANs

3.95 MB

2 Radios

Wireless Clients 1

NAME	IP ADDRESS	HEALTH	BAND	ROLE	SNR	USAGE	WLAN	CONNECTED TO
anonyguest	192.168.1.123	Good	5 GHz	guest	44 dB	-	Guest	20:4c:03:5c:05:6e

And this is what we see in access tracker.

Access Tracker

Feb 07, 2021 17:06:35 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	RADIUS	anonyguest	GG User Authentication with MAC Caching	ACCEPT	2021/02/07 17:02:37
2.	192.168.1.95	RADIUS	a088b450c084	GG MAC Authentication	REJECT	2021/02/07 17:02:21

## 9 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.

### 9.1 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 indicates '10 operator profiles' and a 'Reload' button.

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: 'Description' and 'Access'. The 'Description' section has a text area for the profile name (currently 'Receptionist') and a larger text area for the description (currently '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 contains a checkbox for 'Enabled' (checked) and a list of operator privileges. Each privilege has a dropdown menu set to 'No Access'.

Operator Privileges	Access
Administrator	No Access
Advertising Services	No Access
API Services	No Access
Aruba Integrations	No Access
Devices	No Access

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"/> <b>ClearPass Policy Manager</b>
<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

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

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

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

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

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

[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

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.	<input checked="" type="checkbox"/>	Guest Operator Login	Application	
2.	<input type="checkbox"/>	[Operator Login - Admin Users]	Application	Enforcement profile for Guest admin logins
3.	<input type="checkbox"/>	[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.

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

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

#	<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	<b>[Guest Operator Logins]</b>	Application	Aruba Application Authentication	
5.	<input type="checkbox"/>	5	[Insight Operator Logins]	Application	Aruba Application Authentication	
6.	<input type="checkbox"/>	6	<b>Anya Guest Operator Logins</b>	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

Home » 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)

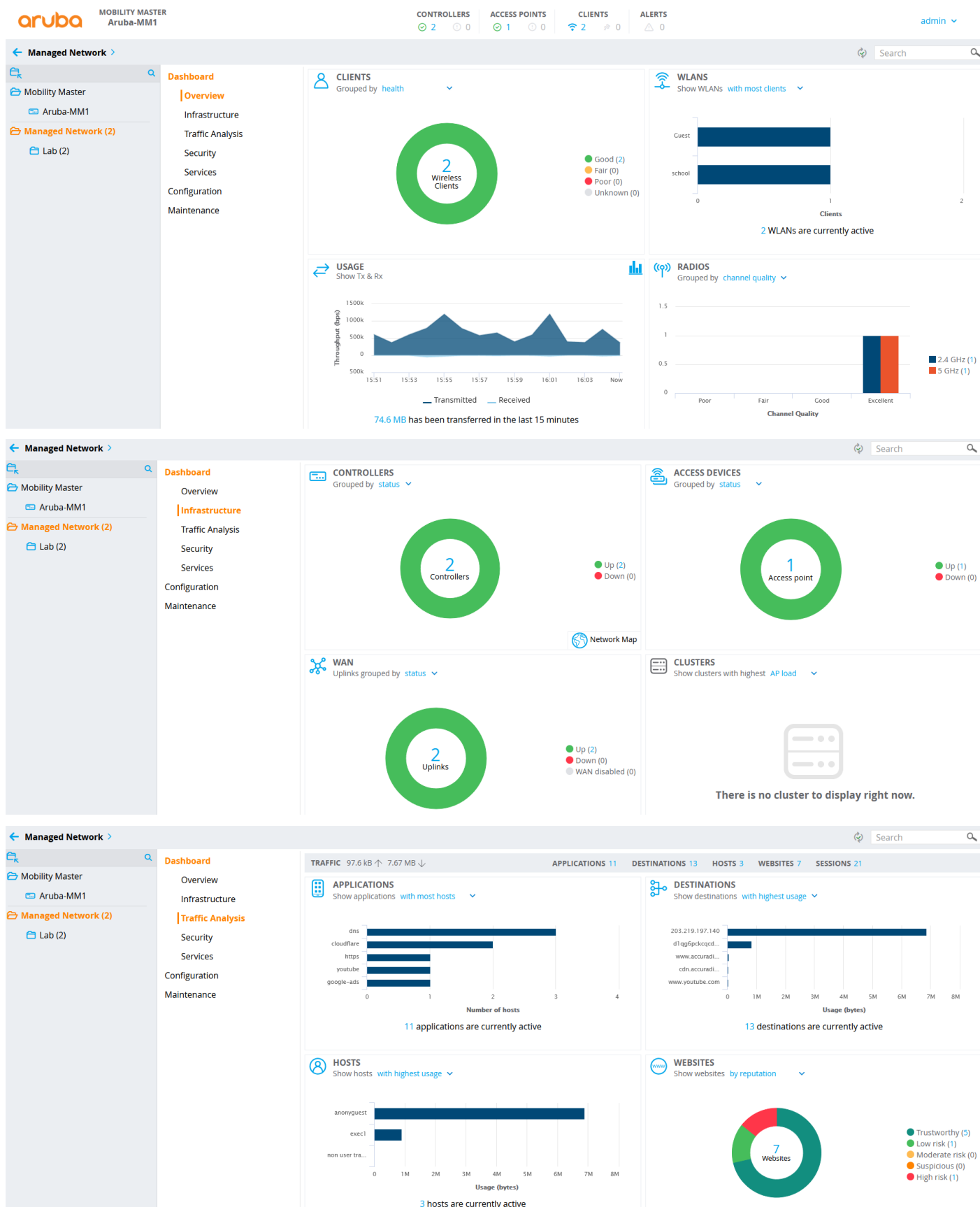
Application Response

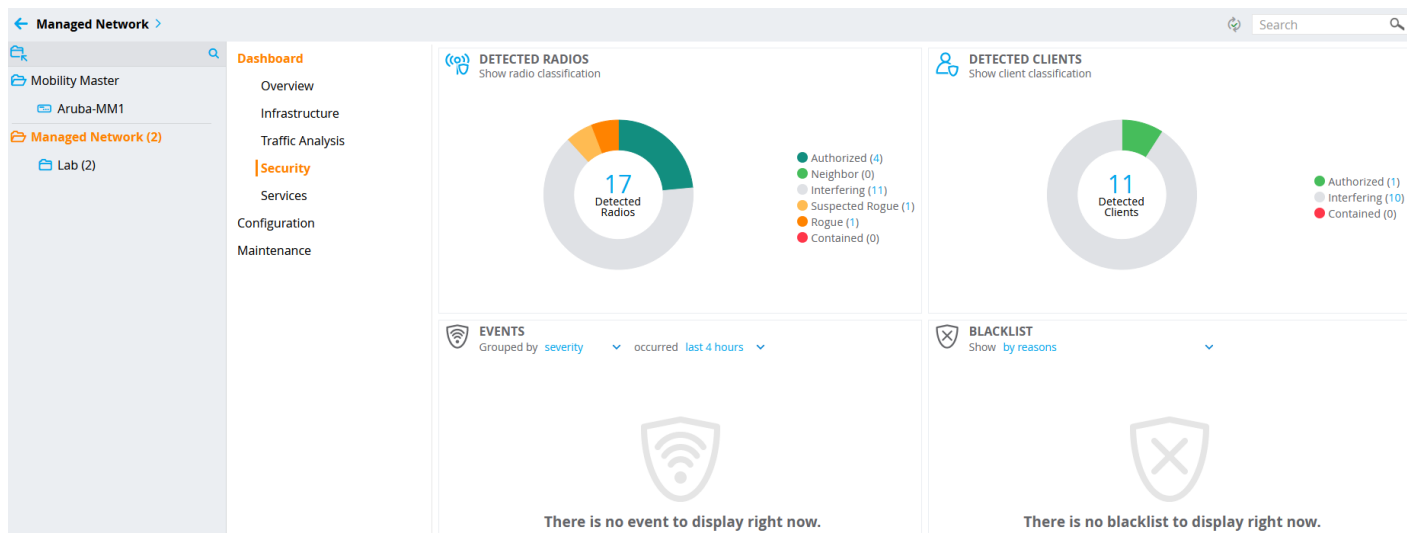
Application:admin\_privileges Receptionist

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

# 10 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 3 of this document.