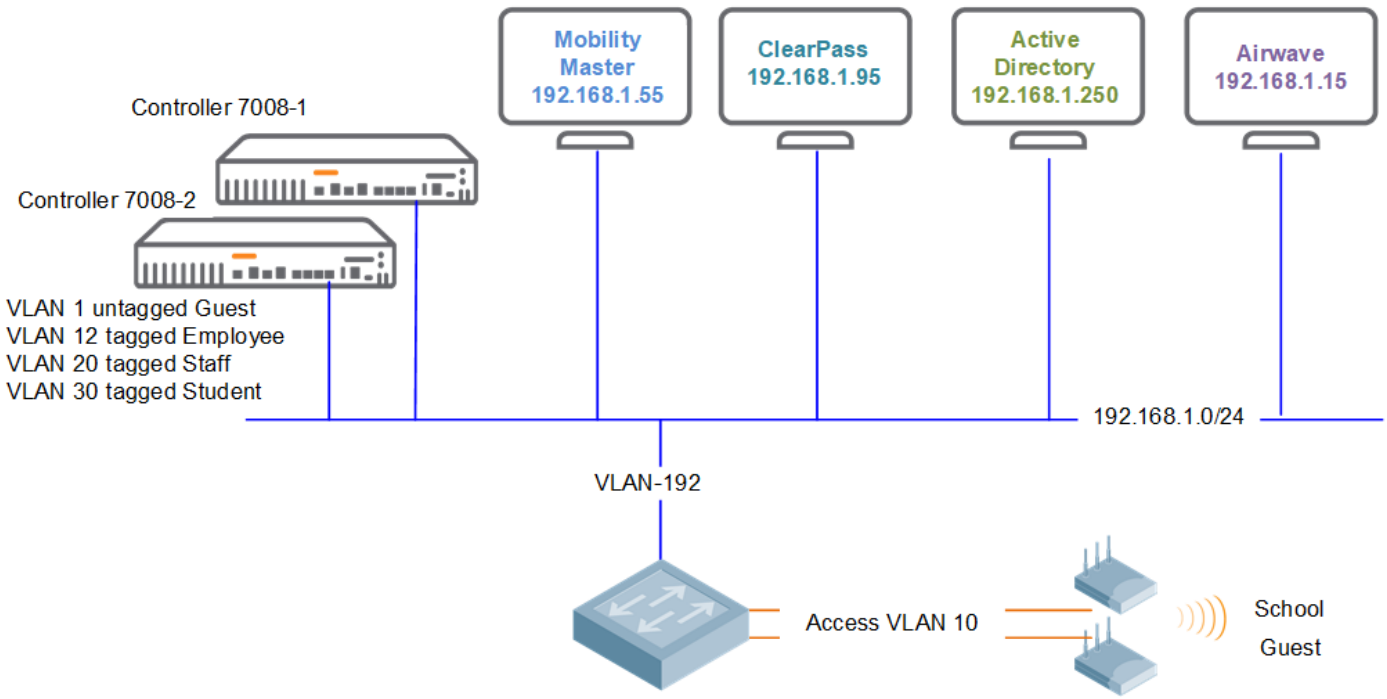
Contents

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.



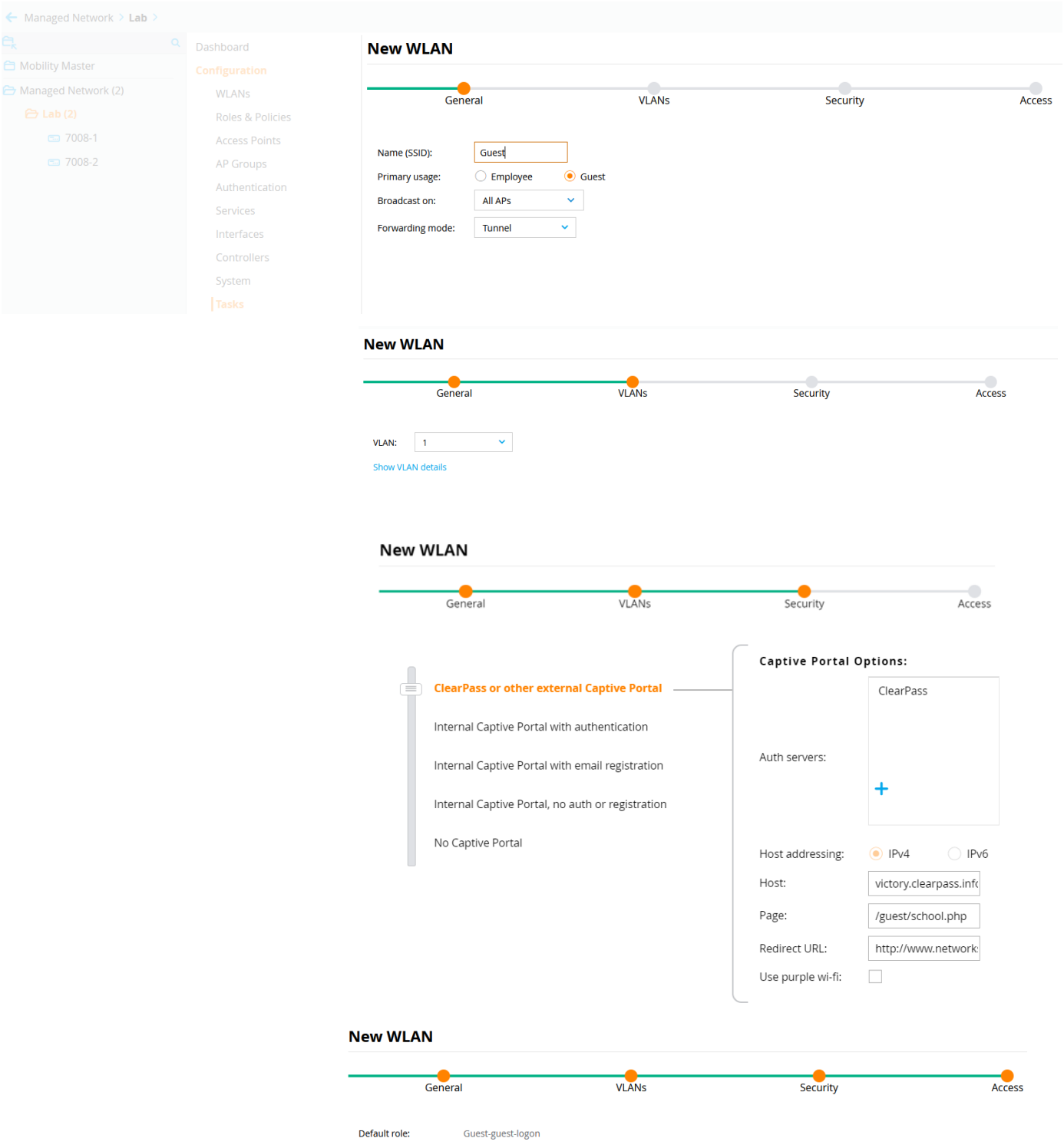
This is the part 2 of the three parts series.

7 Guest Access Configuration

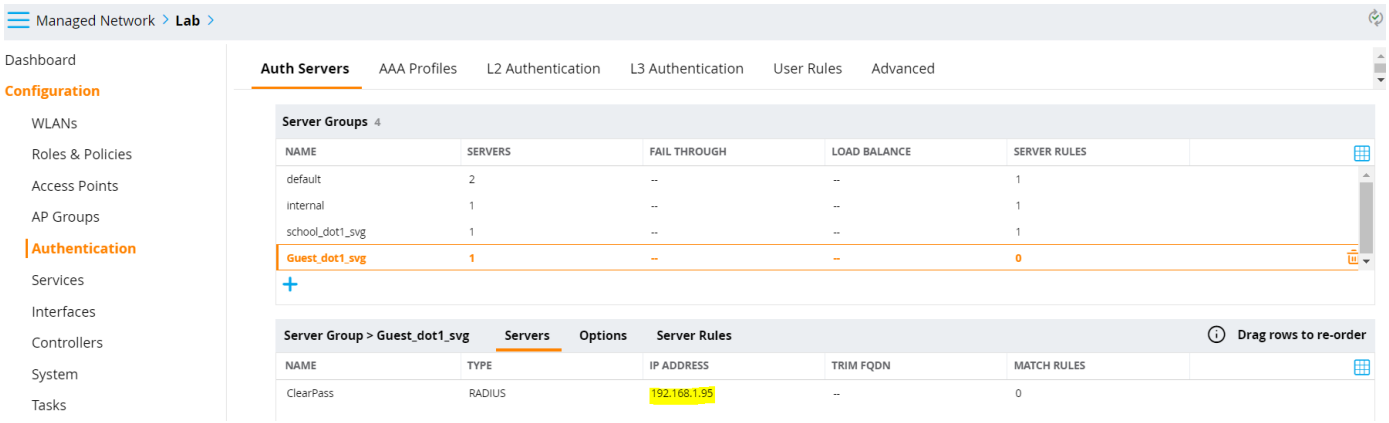
Here we'll start with MM configuration followed by ClearPass.

7.1 MM Guest Wireless Configuration

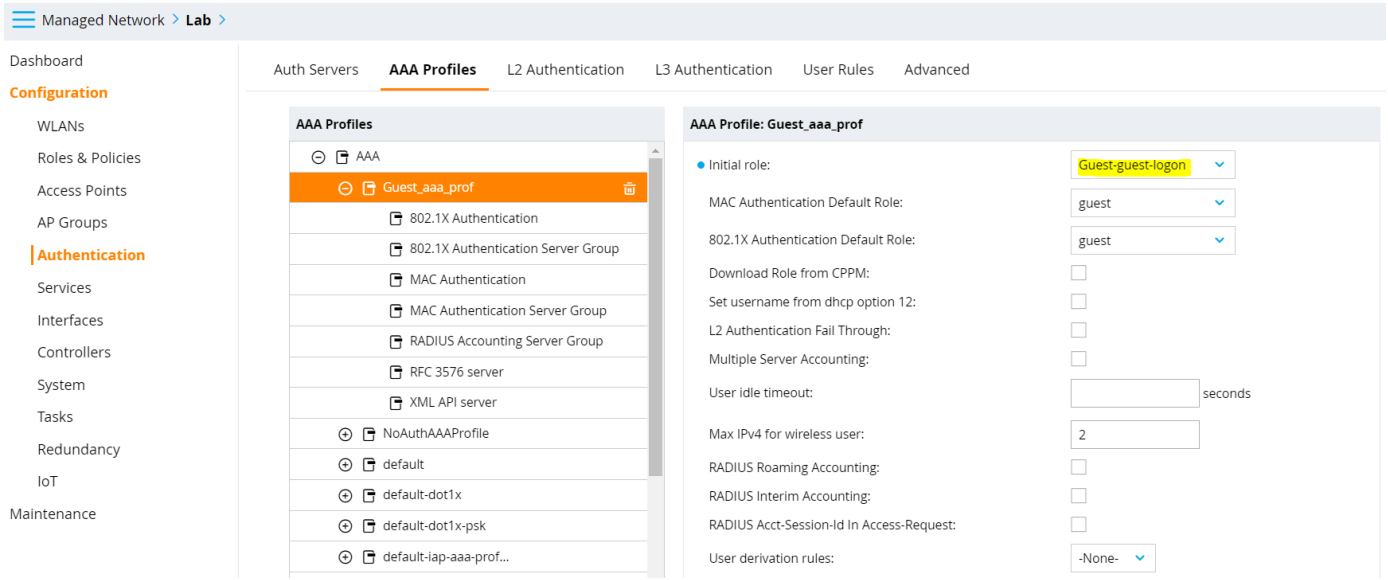
We'll go through the Tasks wizard



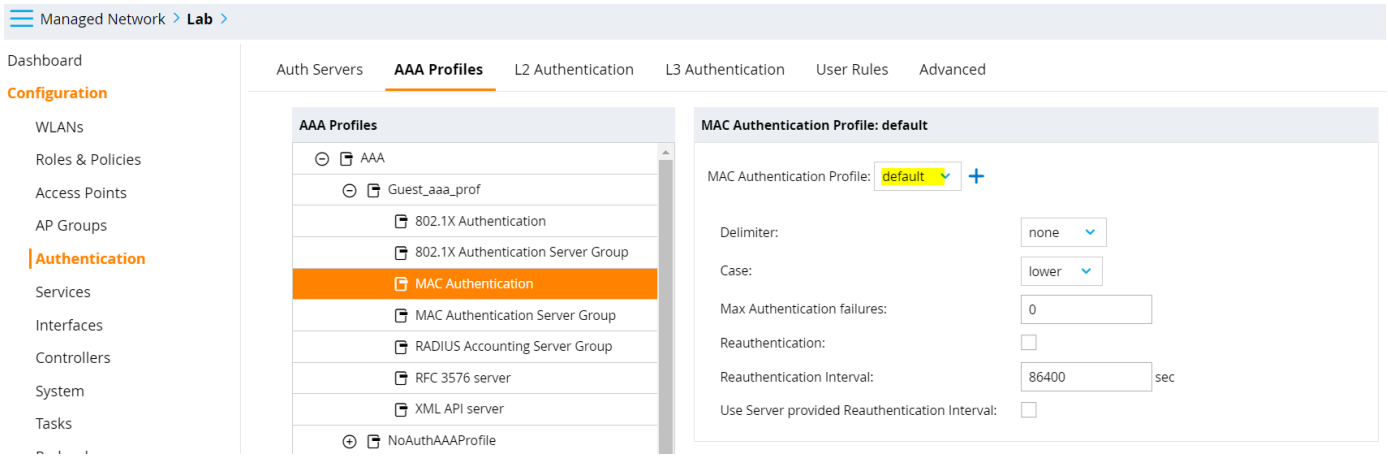
So, once you deploy the configurations, the wizard created a authentication server group.

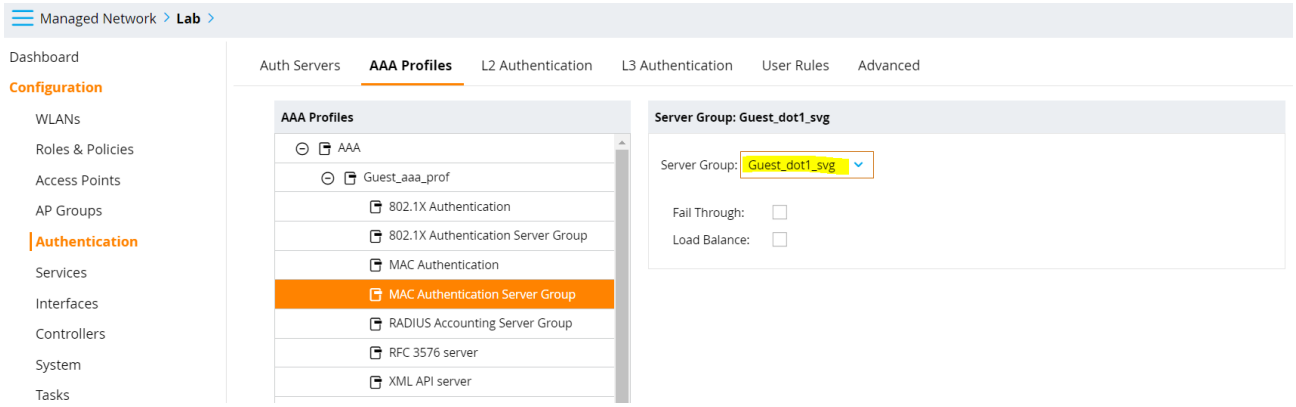


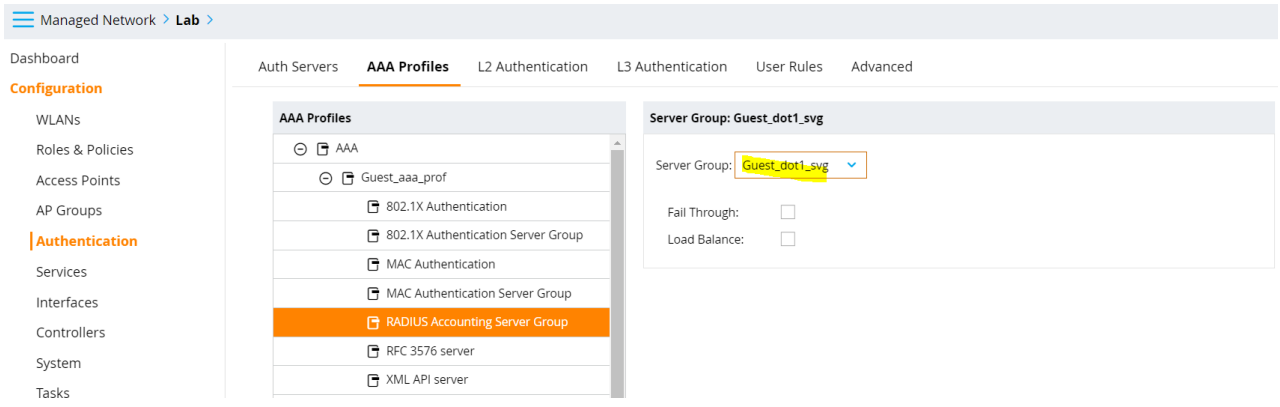
It also created an AAA profile with initial user role as “Guest-guest-logon”. This user role will only provide access to DHCP, DNS and redirection to ClearPass

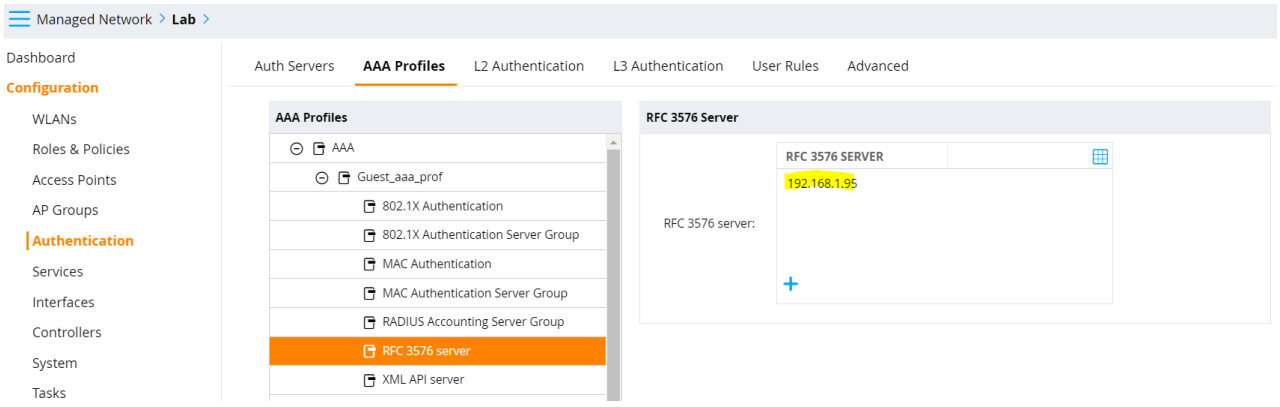


Now because we want to also enable MAC caching for the guest users, we need to add a MAC Authentication profile along with Auth server and accounting server groups for it. The aim of this workflow is that a new guest user gets redirected to captive portal on ClearPass and will use username/password or 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.

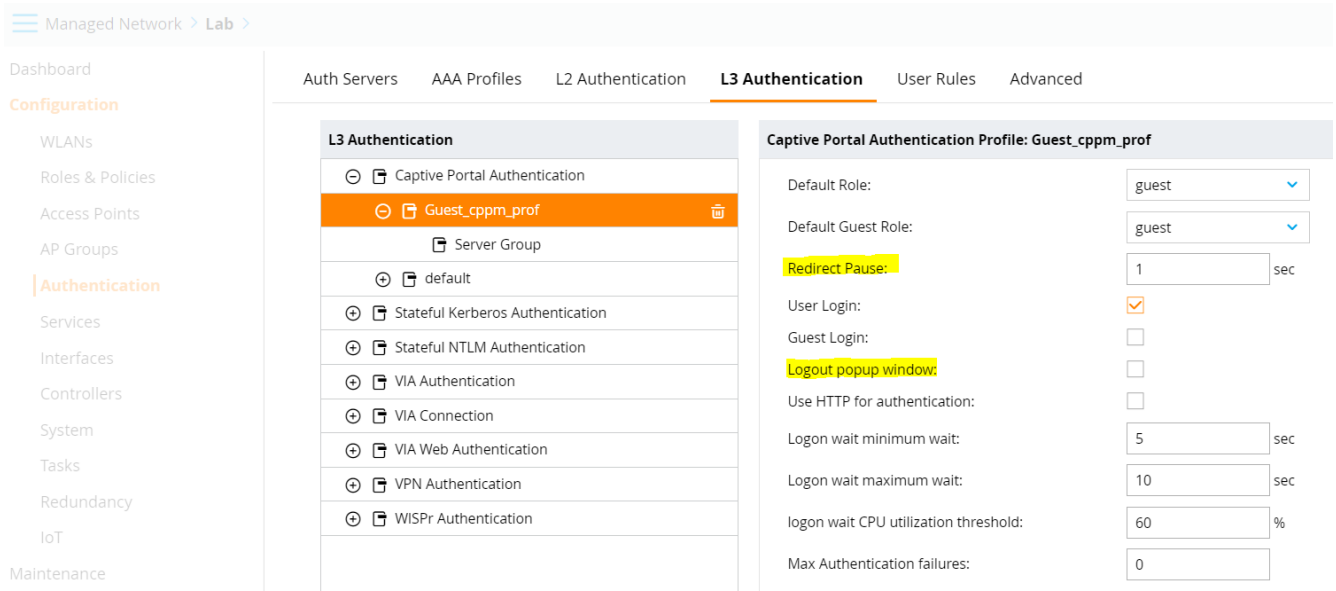








Next, we'll do some fine tuning on Captive portal profile that was created by the wizard. We'll reduce the redirect pause to 1 sec fand uncheck "logout popup window"

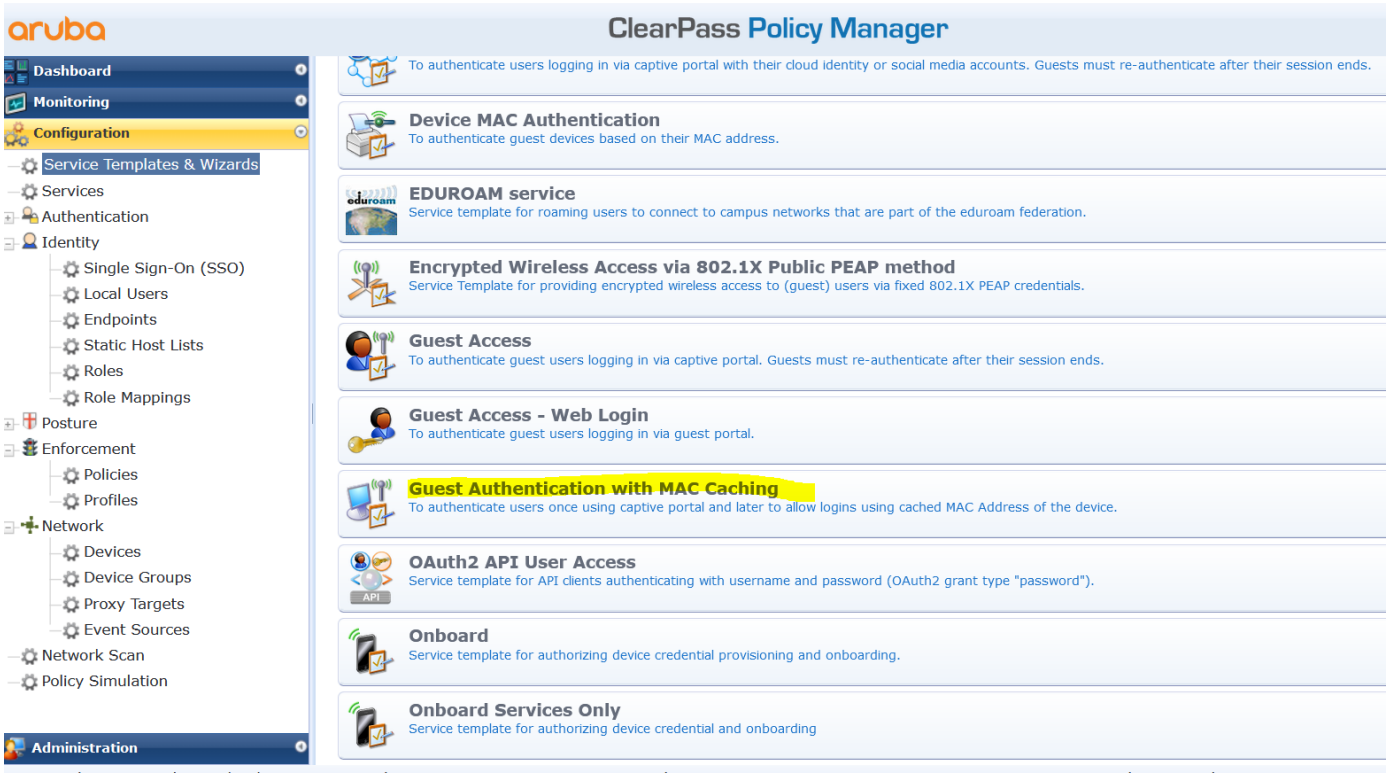


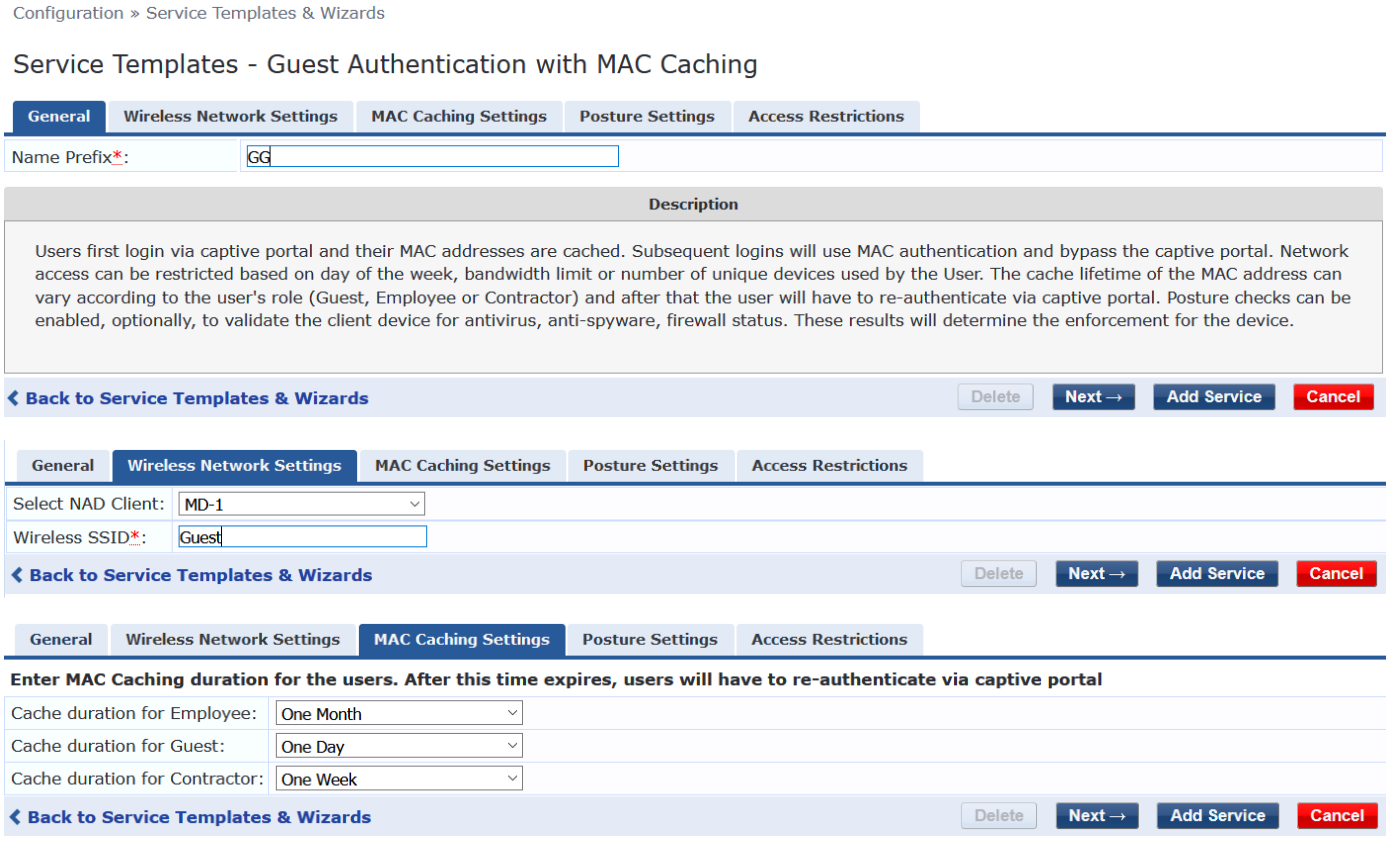
Lastly, note that we have not use a publicly signed HTTPS server certificate for the controllers and hence the redirection of a web page will issue a warning on the client's web browser. In all deployment it is highly recommended to have a public cert for the controllers as well as ClearPass nodes.

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.





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-logon
Days allowed for access*:	☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ 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.	☐	1	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	●
2.	☐	2	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	✓
3.	☐	3	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	✓
4.	☐	4	[Guest Operator Logins]	Application	Aruba Application Authentication	✓
5.	☐	5	[Insight Operator Logins]	Application	Aruba Application Authentication	✓
6.	☐	6	[Device Registration Disconnect]	WEBAUTH	Web-based Authentication	✓
7.	☐	7	AA Aruba 802.1X Wireless	RADIUS	Aruba 802.1X Wireless	✓
8.	☐	8	GG MAC Authentication	RADIUS	MAC Authentication	✓
9.	☐	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:	☐ Enable to monitor network access without enforcement
More Options:	☑ Authorization ☐ Audit End-hosts ☐ Profile Endpoints ☐ Accounting Proxy

Service Rule

Matches ○ ANY or ◉ ALL of the following conditions:

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

Summary | Service | **Authentication** | Authorization | Roles | Enforcement

Authentication Methods: [Allow All MAC AUTH] — Move Up ↑ | Move Down ↓ | Remove | View Details | Modify — Add New Authentication Method

--Select to Add--

Authentication Sources: [Endpoints Repository] [Local SQL DB] — Move Up ↑ | Move Down ↓ | Remove | View Details | Modify — 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)

	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 — Add New Authentication Source

--Select to Add--

Summary | Service | Authentication | Authorization | **Roles** | Enforcement

Role Mapping Policy: GG MAC Authentication Role Mapping — Modify — Add New Role Mapping Policy

Role Mapping Policy Details

Description:	
Default Role:	[Other]
Rules Evaluation Algorithm:	evaluate-all

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

Summary | Service | Authentication | Authorization | Roles | **Enforcement**

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:	[Deny Access Profile]
Rules Evaluation Algorithm:	first-applicable

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

Back to Services — Disable | Copy | Save | Cancel

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-logon

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

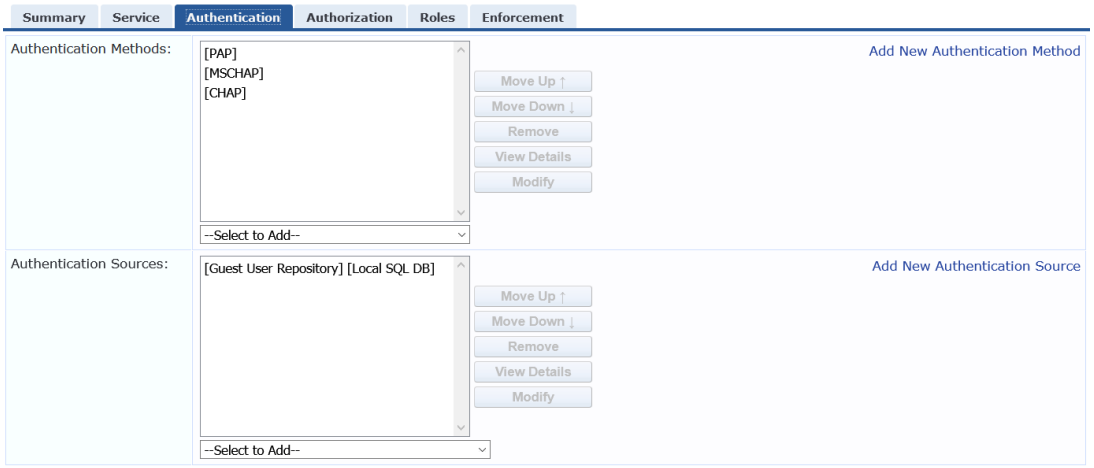
Summary | Service | Authentication | Authorization | Roles | Enforcement

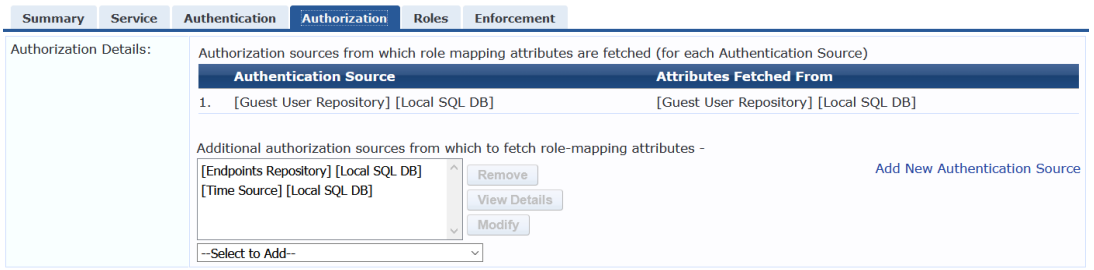
Name:	GG User Authentication with MAC Caching
Description:	Captive Portal authentication with MAC Caching
Type:	RADIUS Enforcement (Generic)
Status:	Enabled
Monitor Mode:	☐ Enable to monitor network access without enforcement
More Options:	☑ Authorization ☐ Posture Compliance ☐ Audit End-hosts ☐ Profile Endpoints ☐ Accounting Proxy

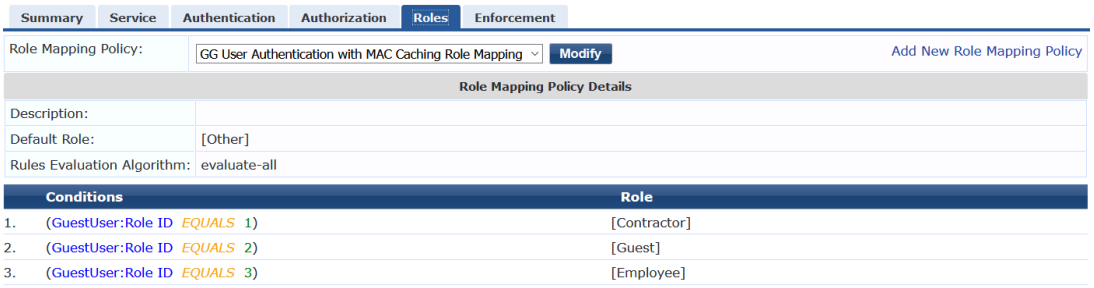
Service Rule

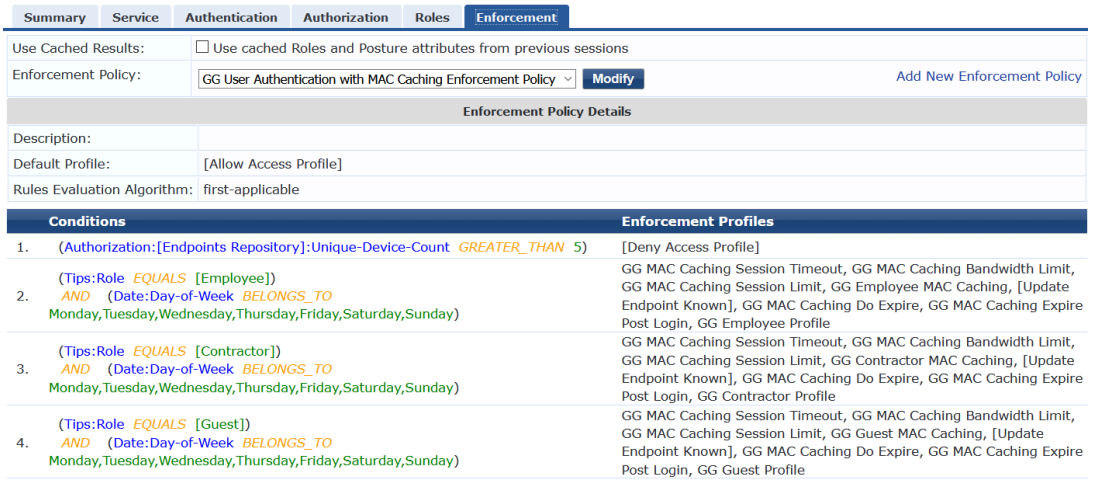
Matches ○ ANY or ◉ ALL of the following conditions:

	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
4.	Click to add...			

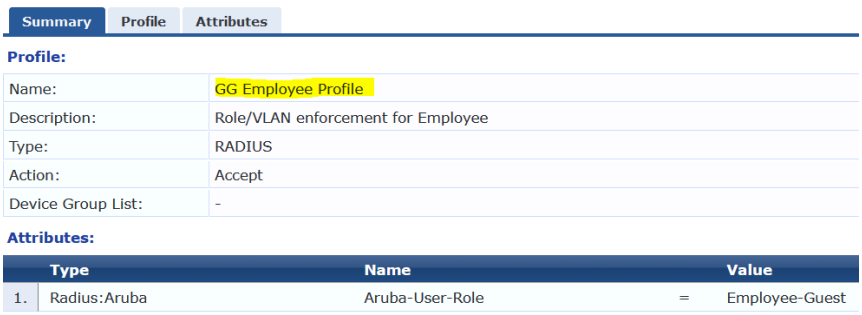








The enforcement profiles



Summary | Profile | Attributes

Profile:

Name:	GG Guest 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

Summary | Profile | Attributes

Profile:

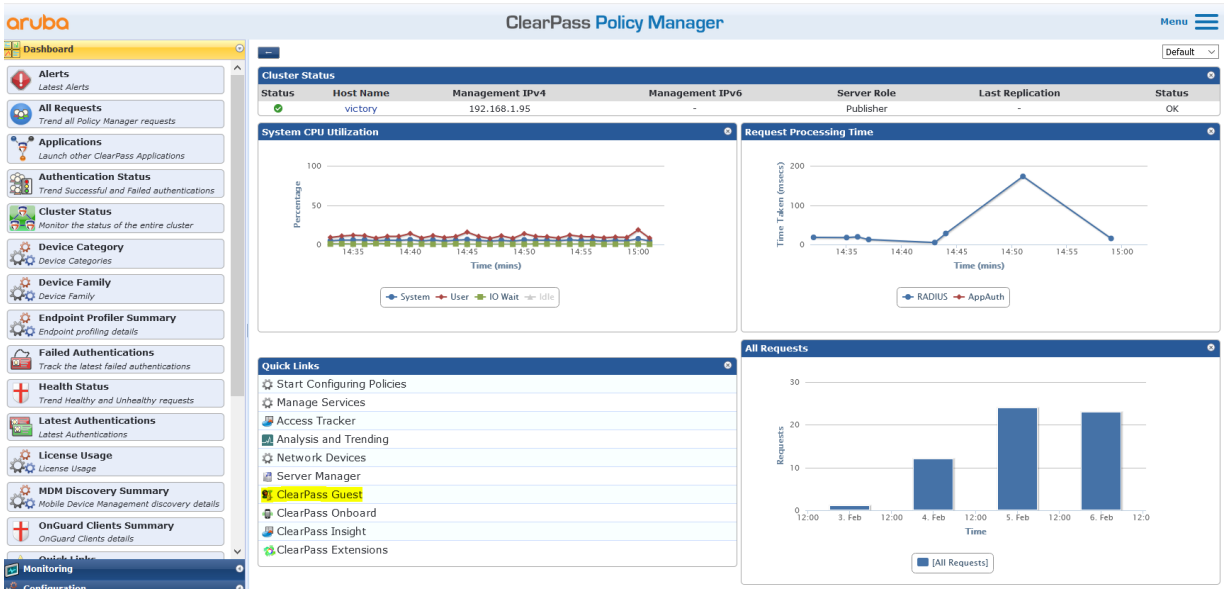
Name:	GG Contractor Profile
Description:	Role/VLAN enforcement for Contractor
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

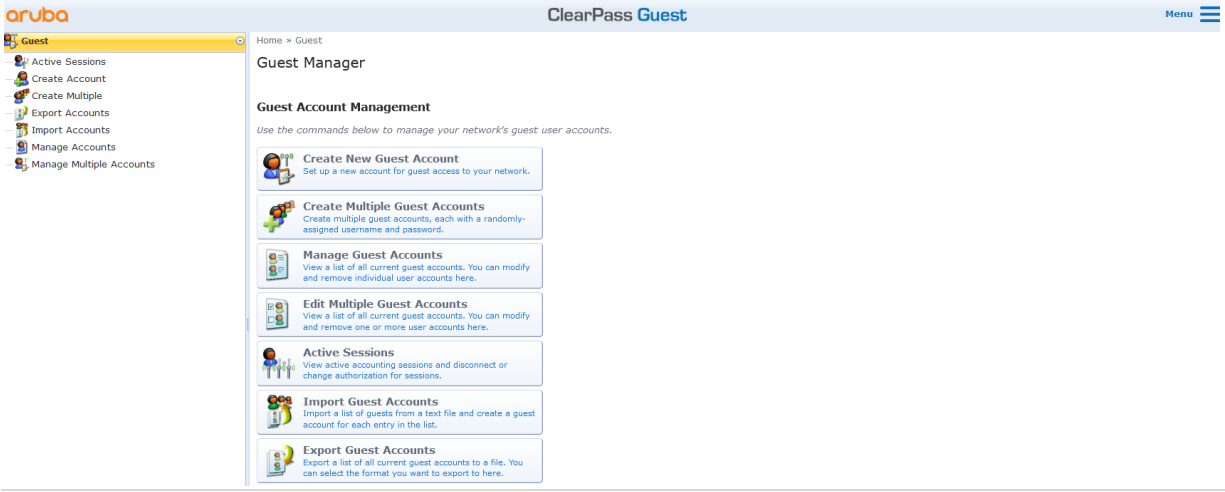
	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	Contractor

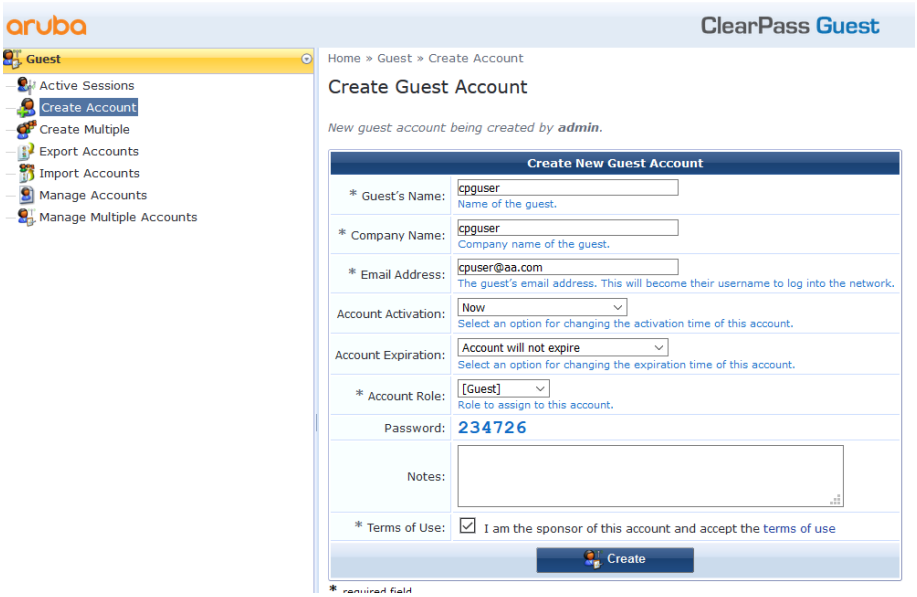
7.3 ClearPass Guest Portal Configuration

Here we'll configure the captive portal pages.

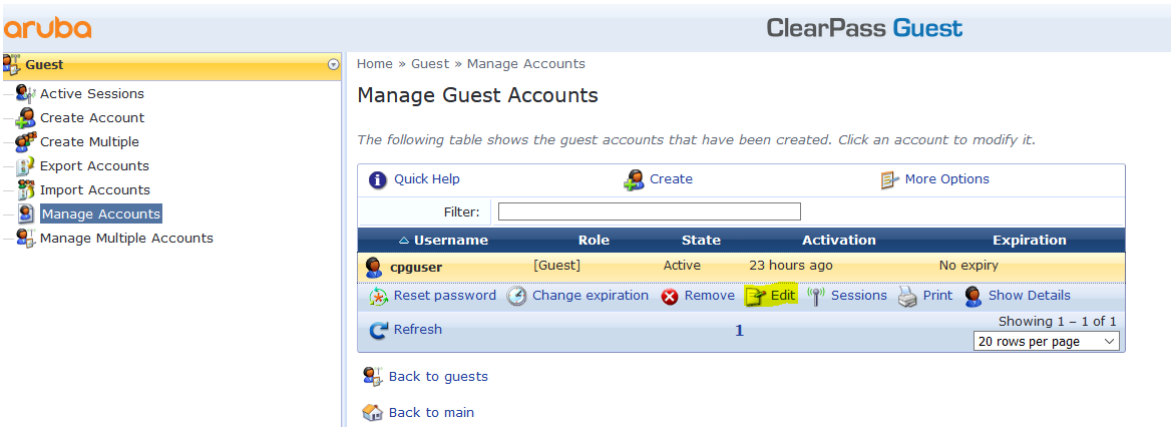


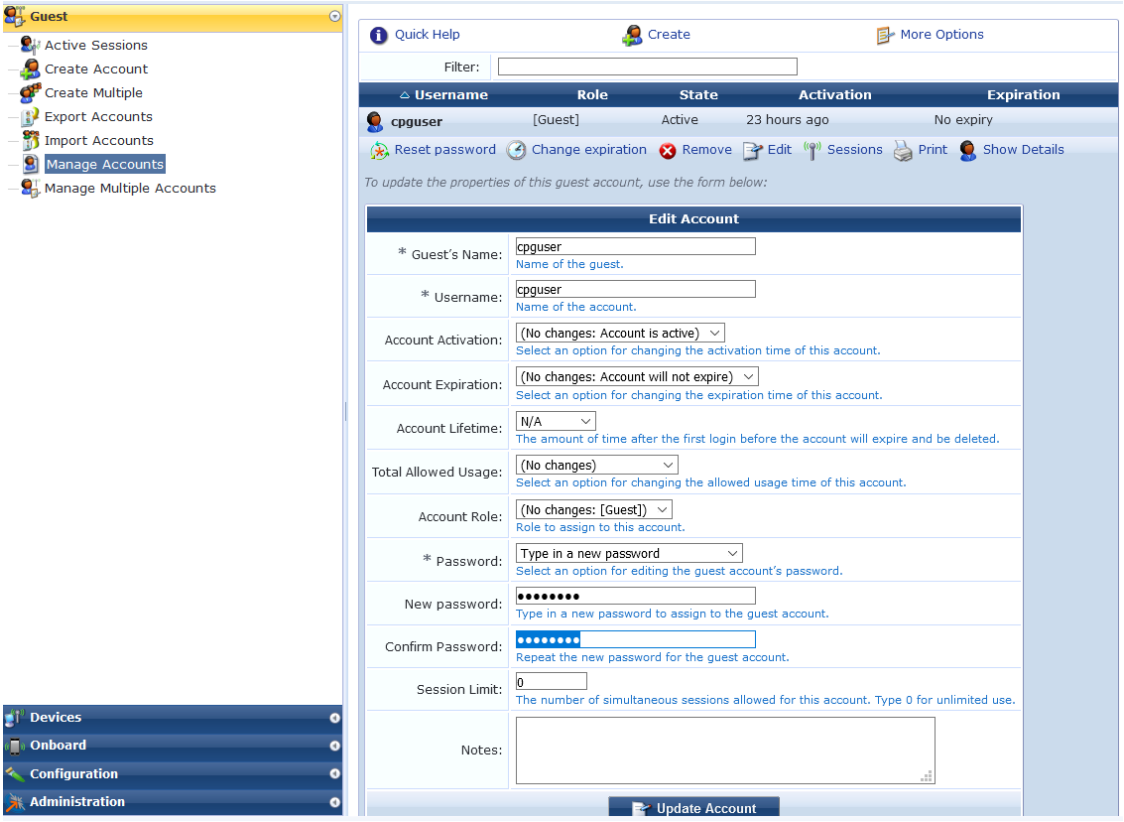
First we'll create a guest user called cpguser with no expiration on the account.



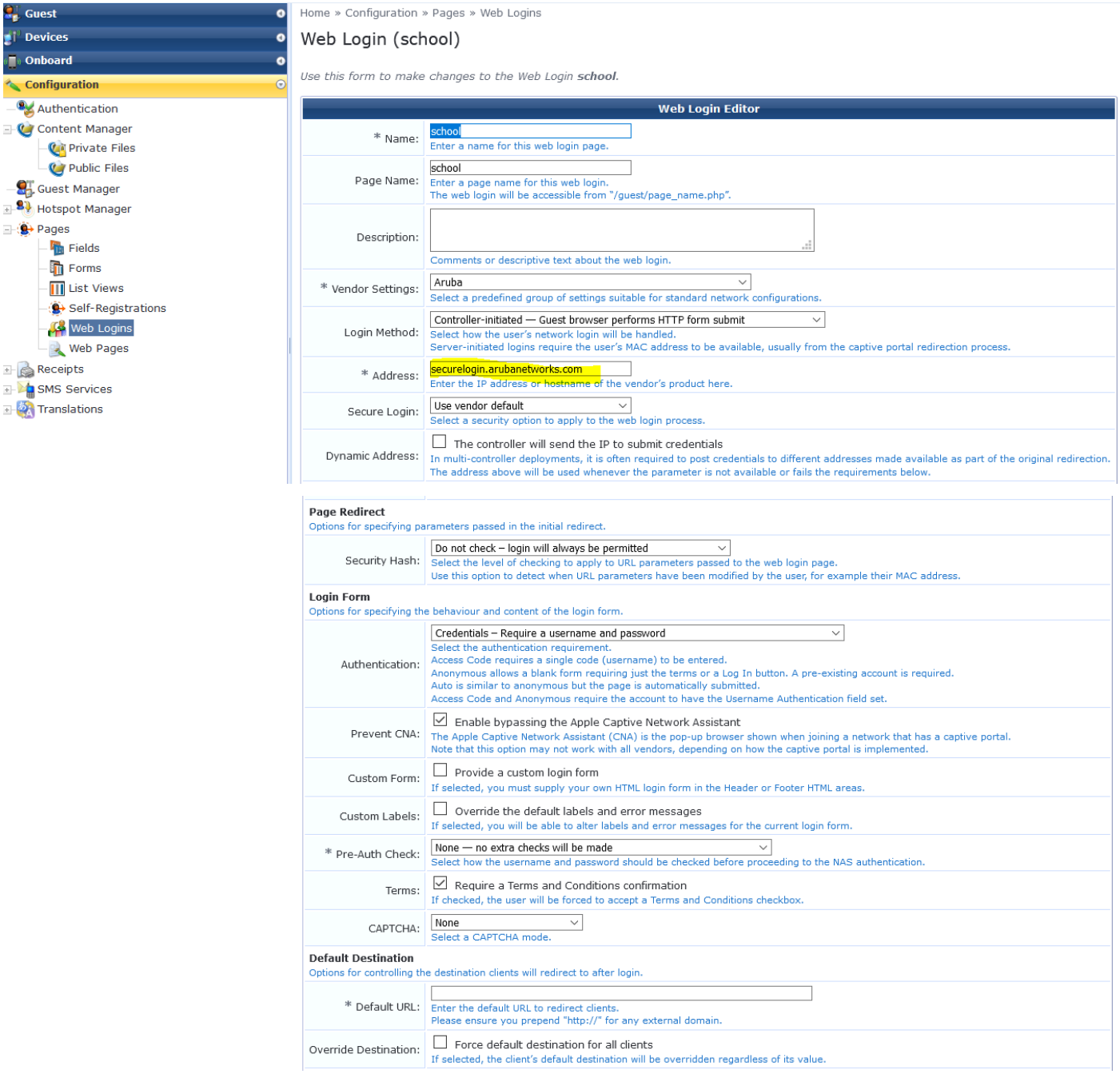


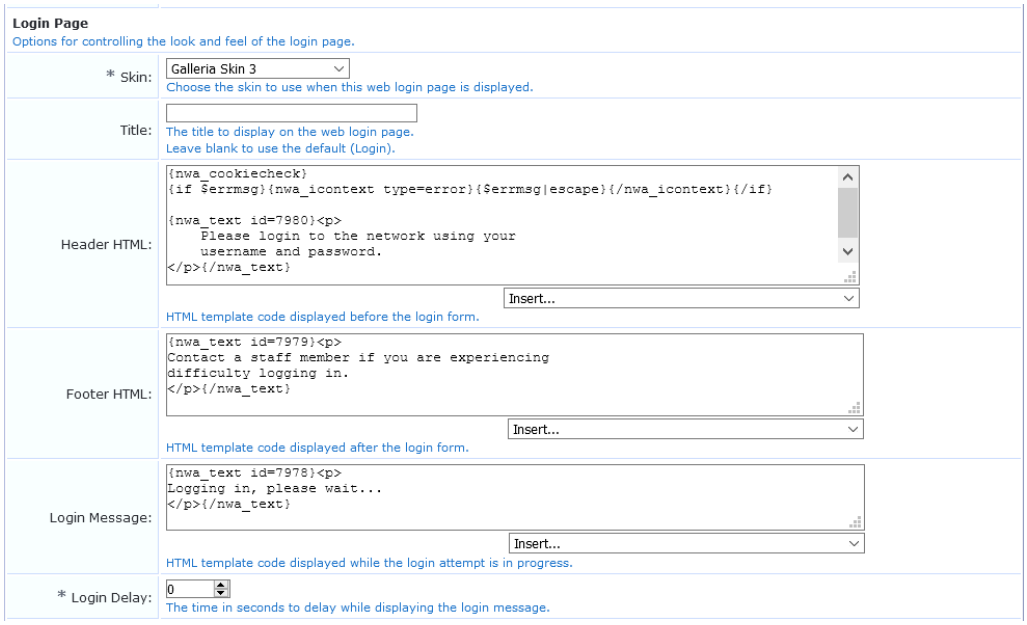
Once created we'll modify it to change the username and password

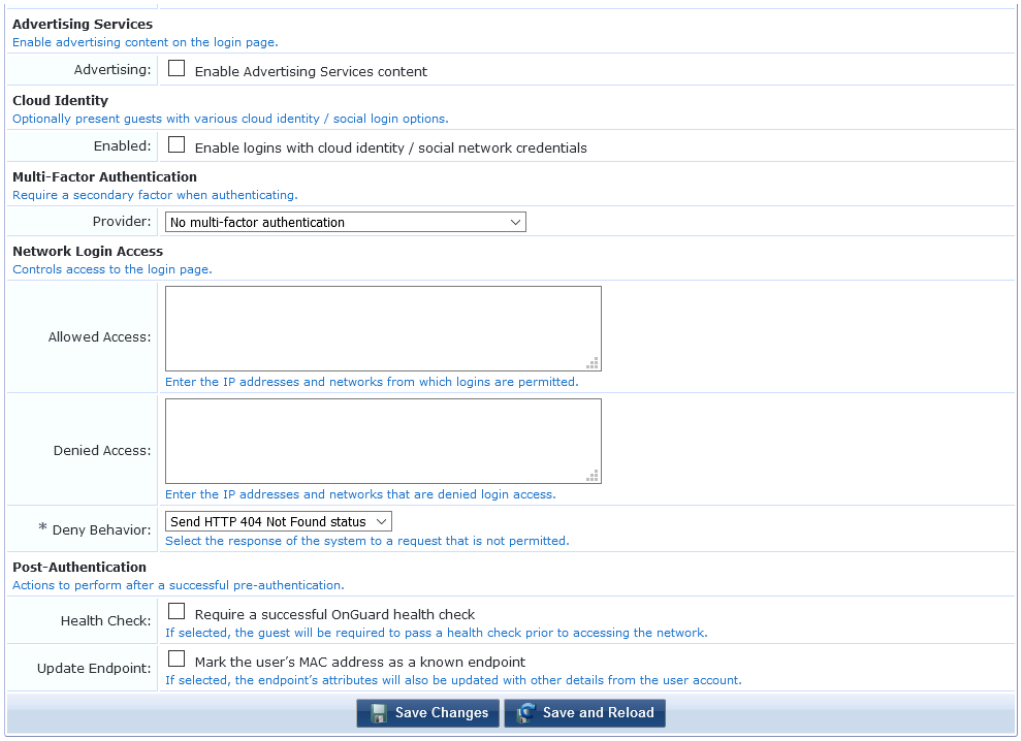


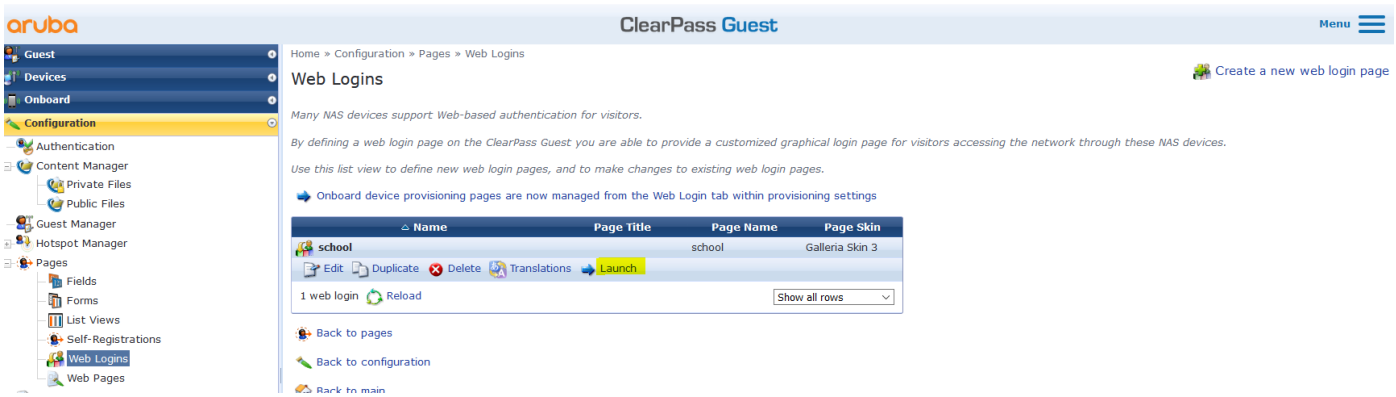


Next we'll create a weblogin page, note that the page name will be in the redirection URL, also if you are using public certificate on the controllers, you need to change securelogin.arubanetworks.com. We'll cover this later.





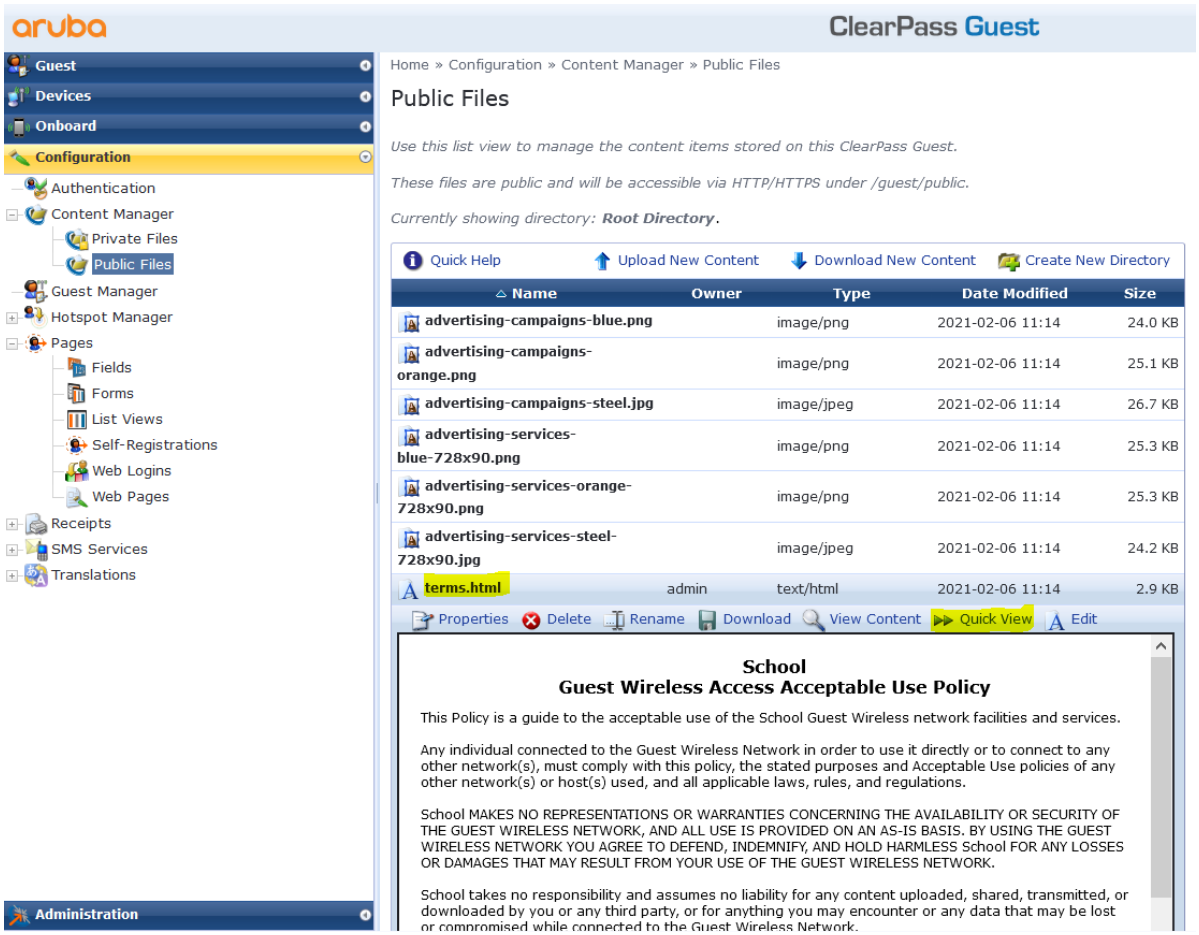




You can test the page as well, when you'll click on the launch a tab will open and you'll see the captive portal note the URL which in this case is https://victory.clearpass.info/guest/school.php?_browser=1

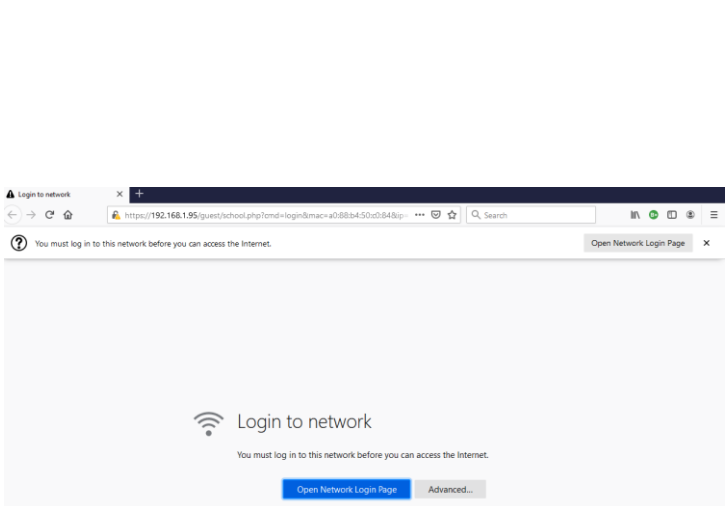
The "guest/school.php" is used in the URL redirection which we configured in MM

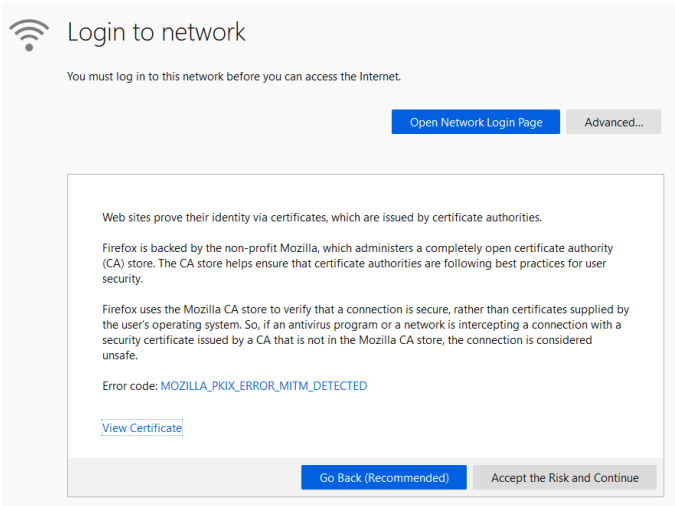
Now go to content manager and upload your terms and condition page.



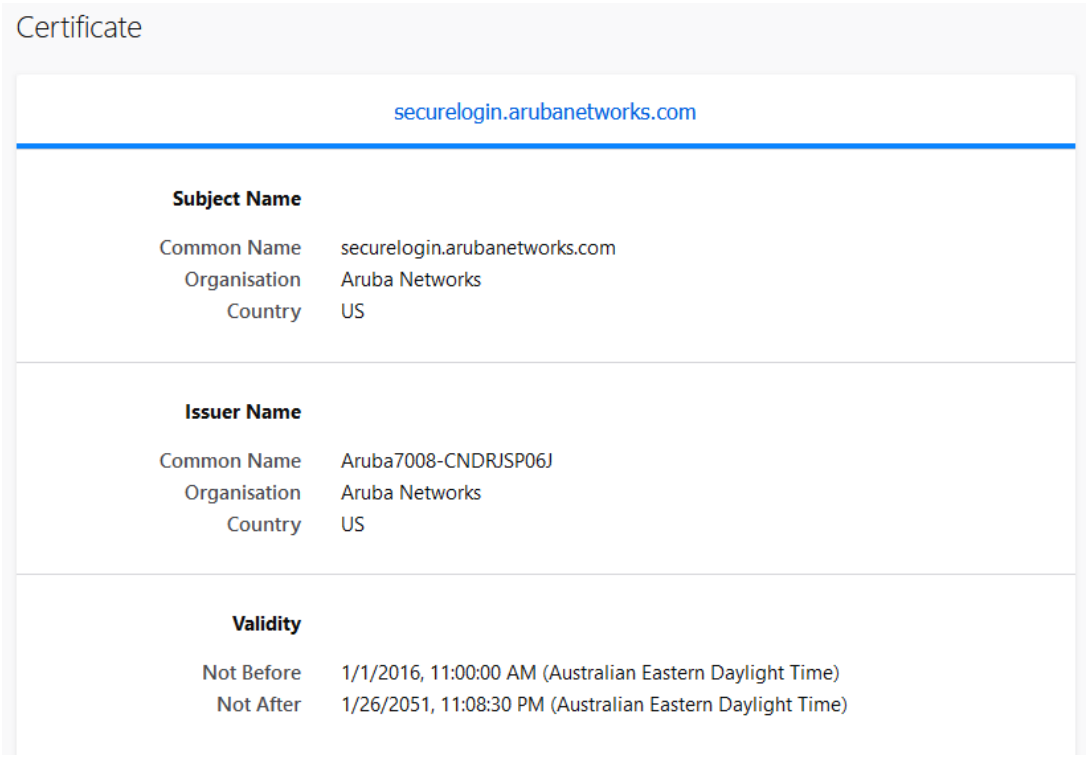
7.4 Guest Testing

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

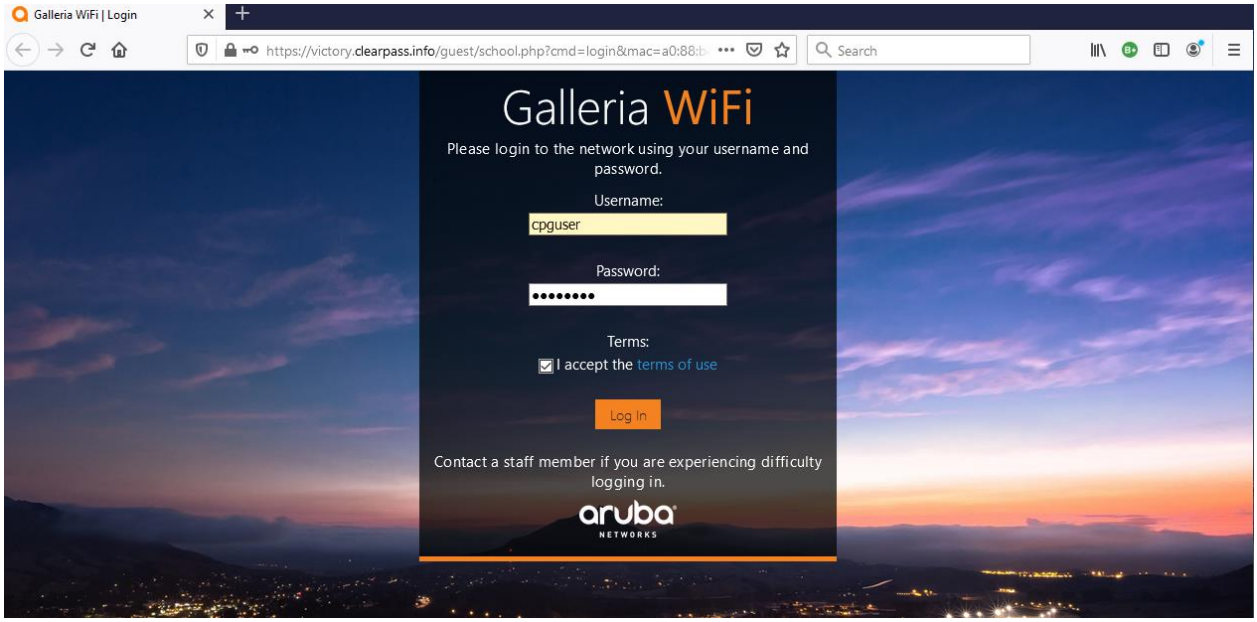




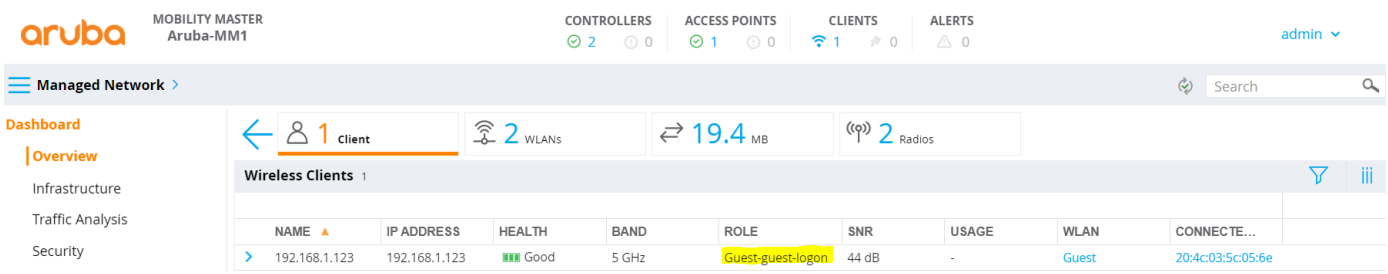
We'll have a look at the certificate, and we'll see it is the default captive portal certificate which is on the controller.



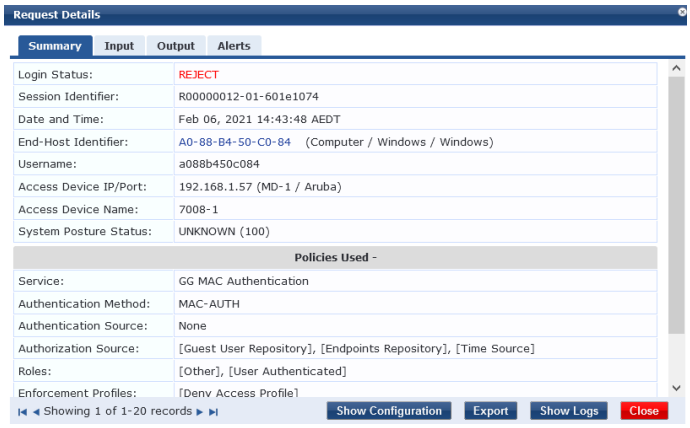
We'll accept this and carry on, but for all deployments you need to have a public server certificate for your controllers. Once we accept the certificate, we'll get redirected to the captive portal page on ClearPass

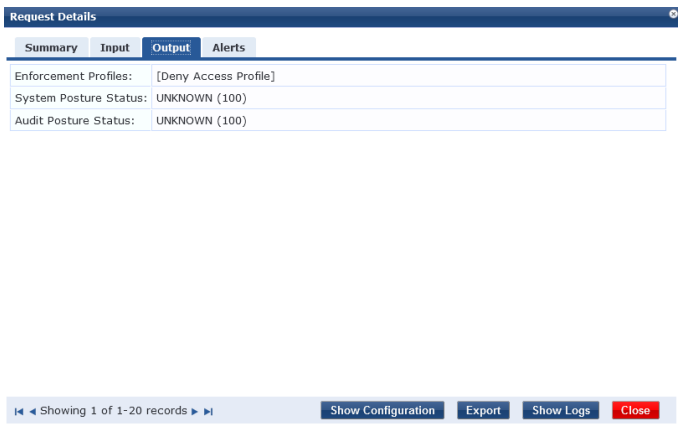


Before we login with our guest credentials, we'll look at the MM dashboard and see the user is in guest-login role with minimum access.



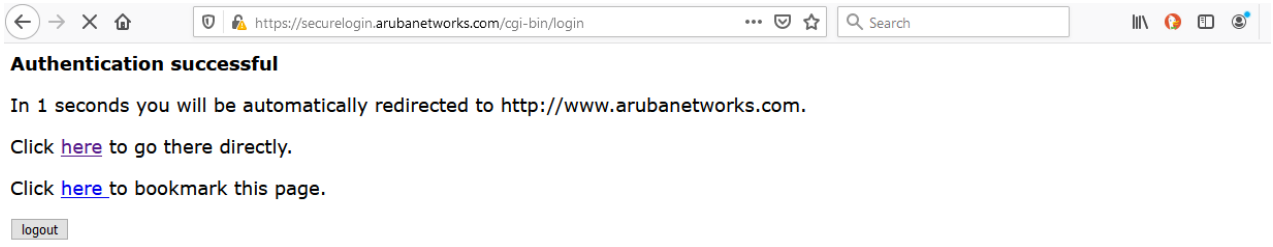
Then we'll check the access tracker and see that we have a failed MAC authentication.



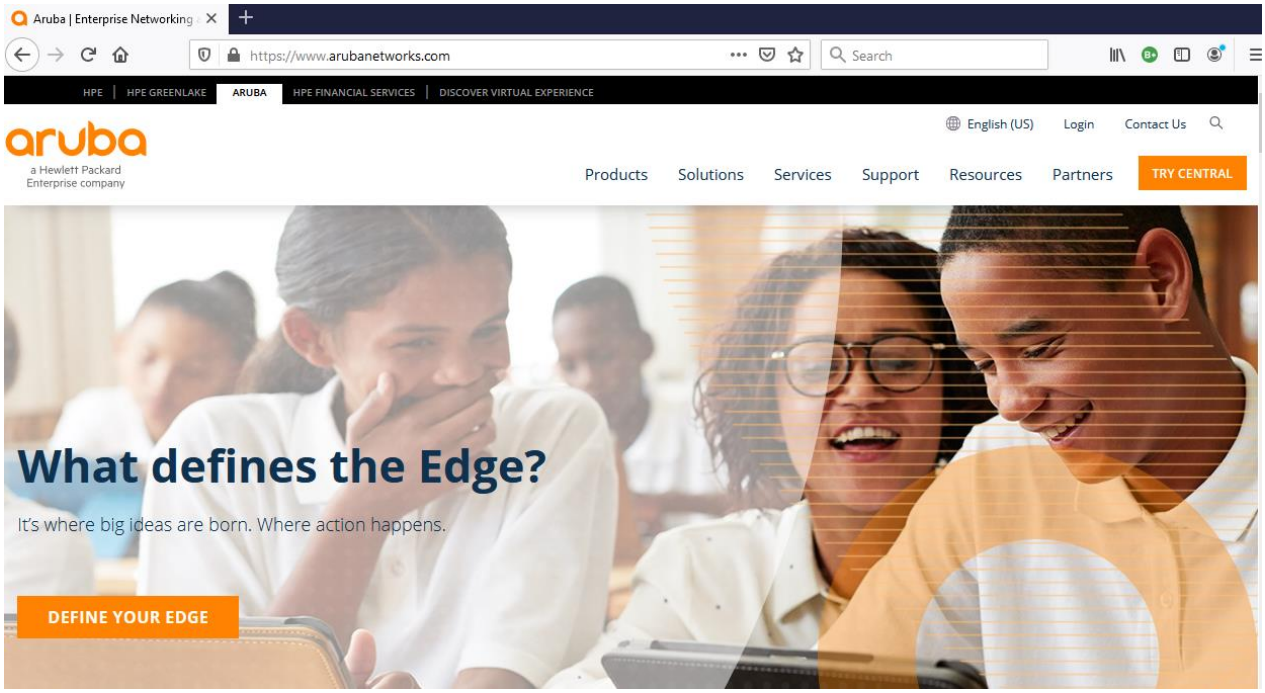


This is normal as this MAC address has not been seen before and hence the failed MAC authentication.

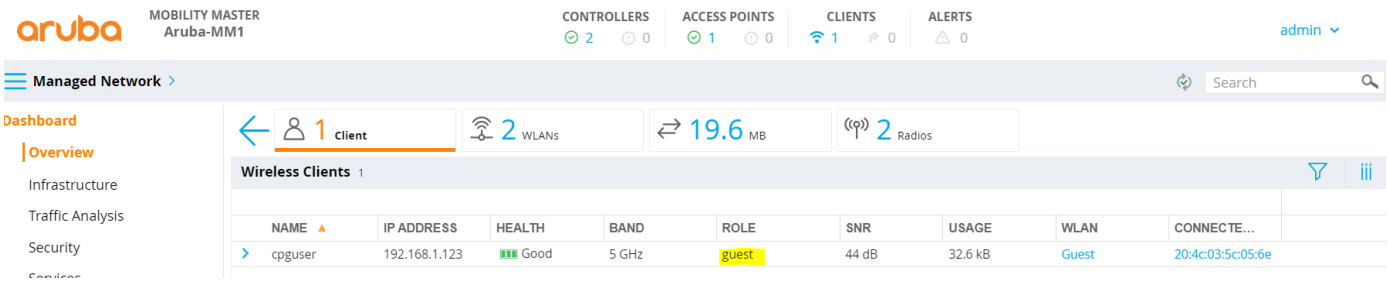
Now when the user performs the login process with cpguser credentials, the following will be seen.



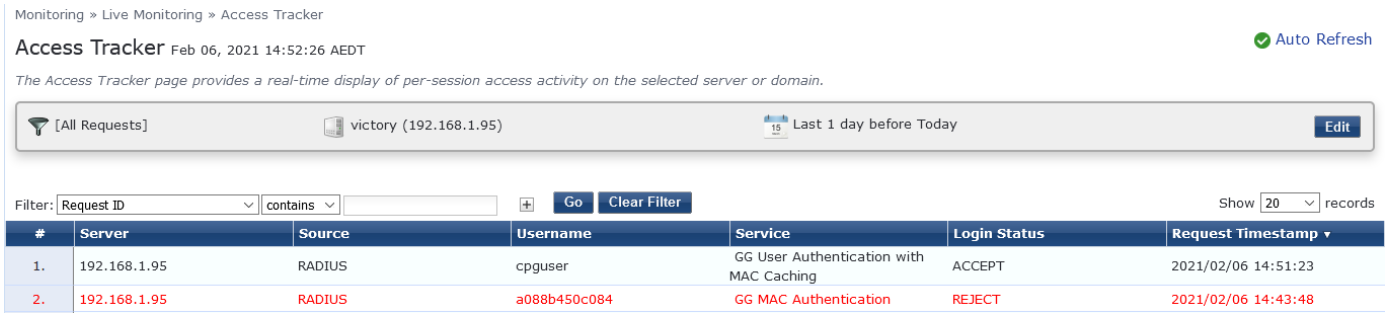
And then redirected to the page that was configured on the AAA profile on the MM

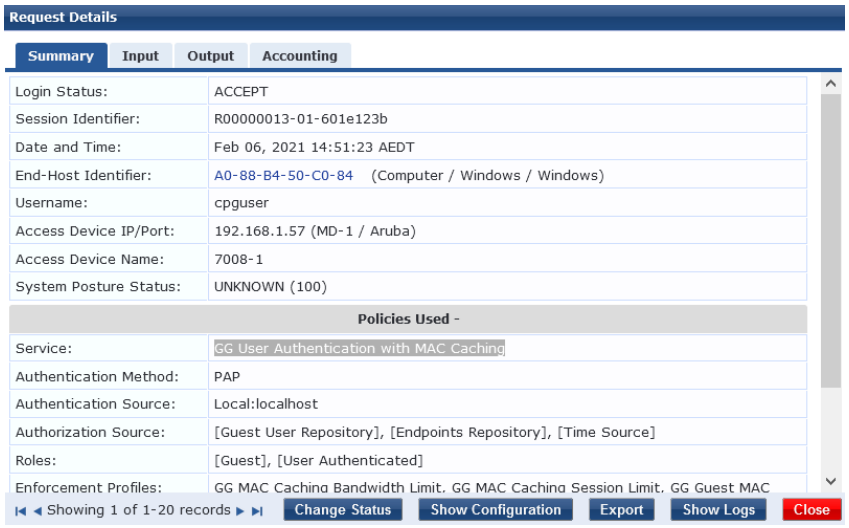


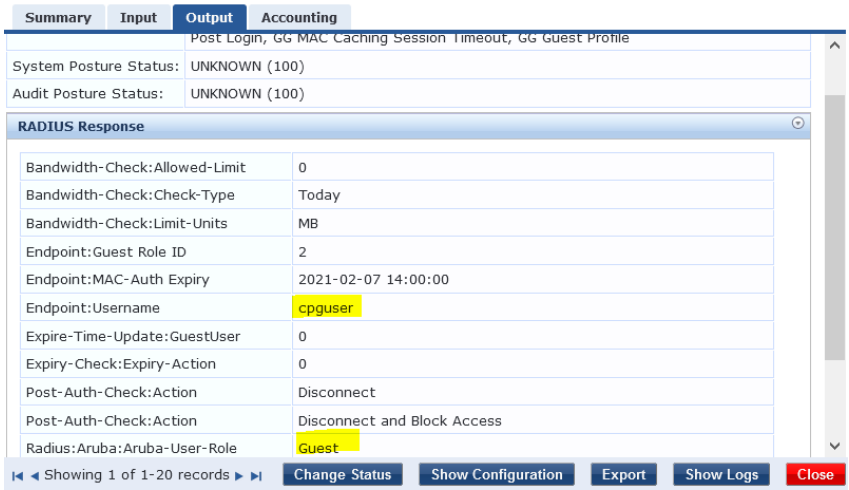
The MM dashboard and access tracker show that the user role is now "guest".



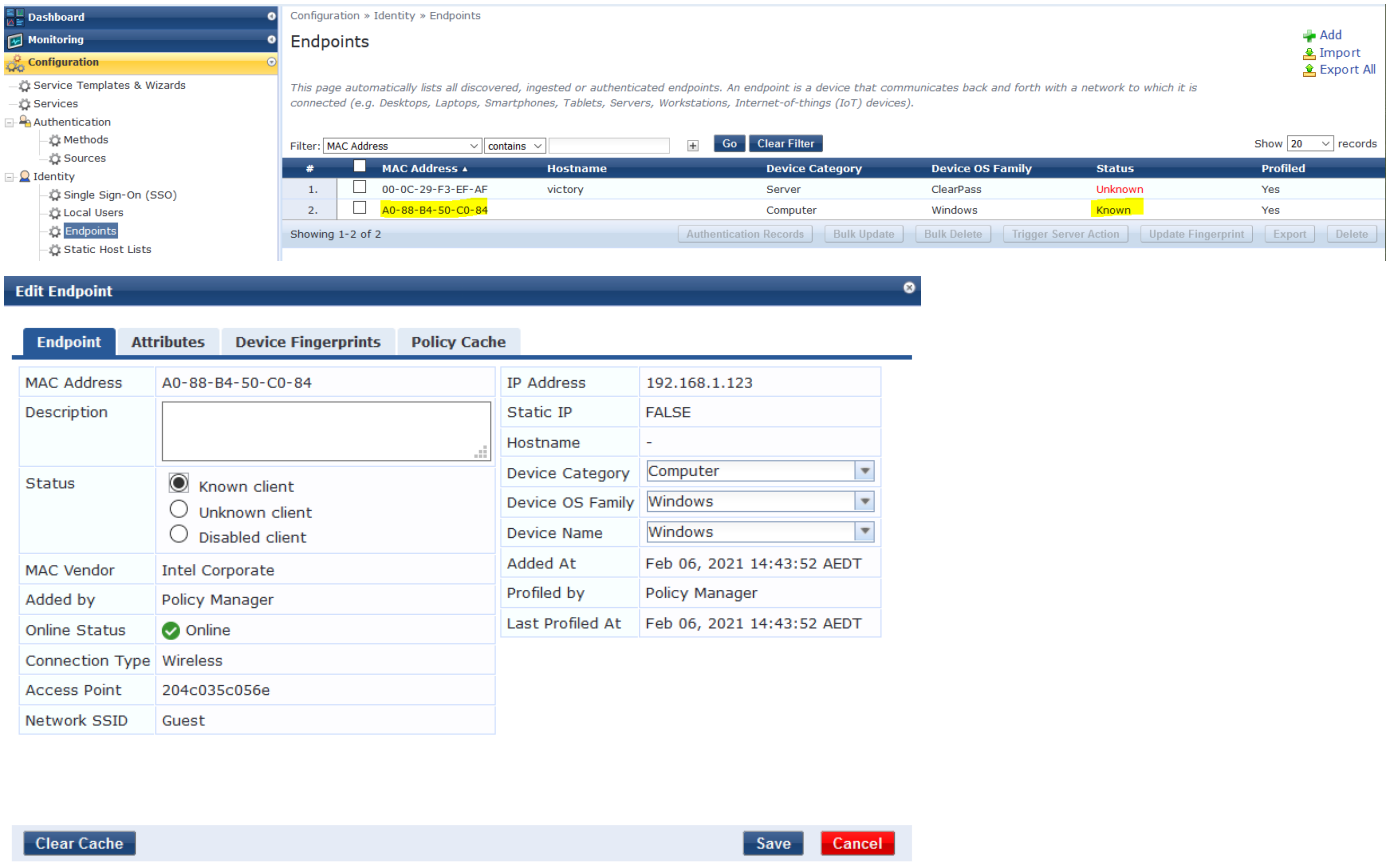
And the access tracker shows a successful authentication that matches with “GG User Authentication with MAC Caching” policy.



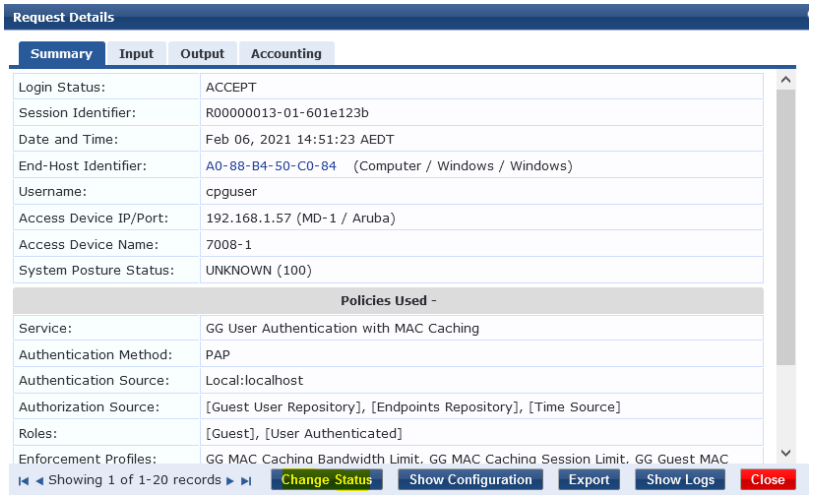


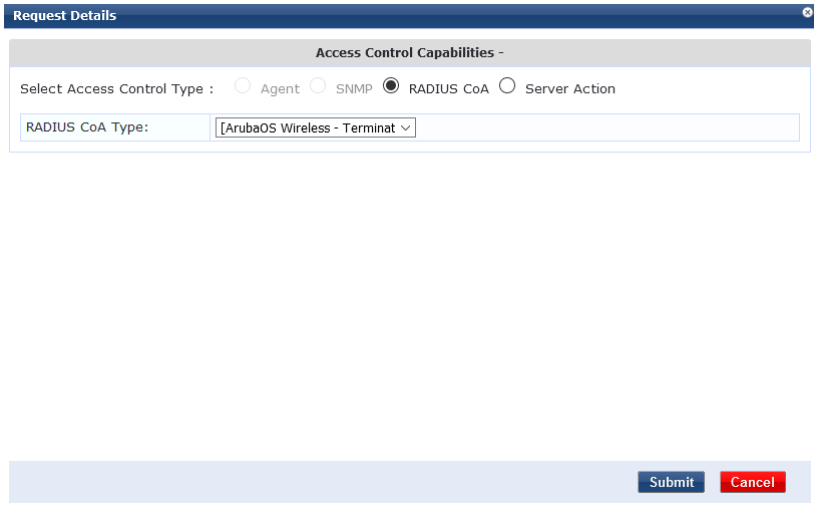


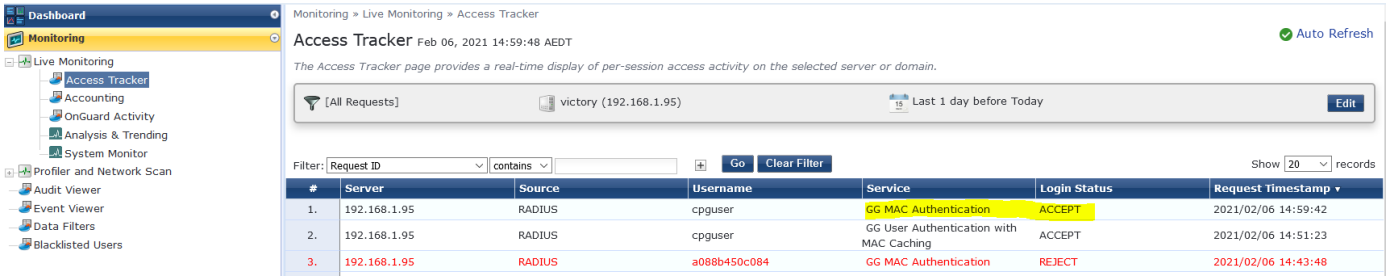
Also note that one of the post authentication actions were to update the endpoint repository status for that MAC address to be “known”.



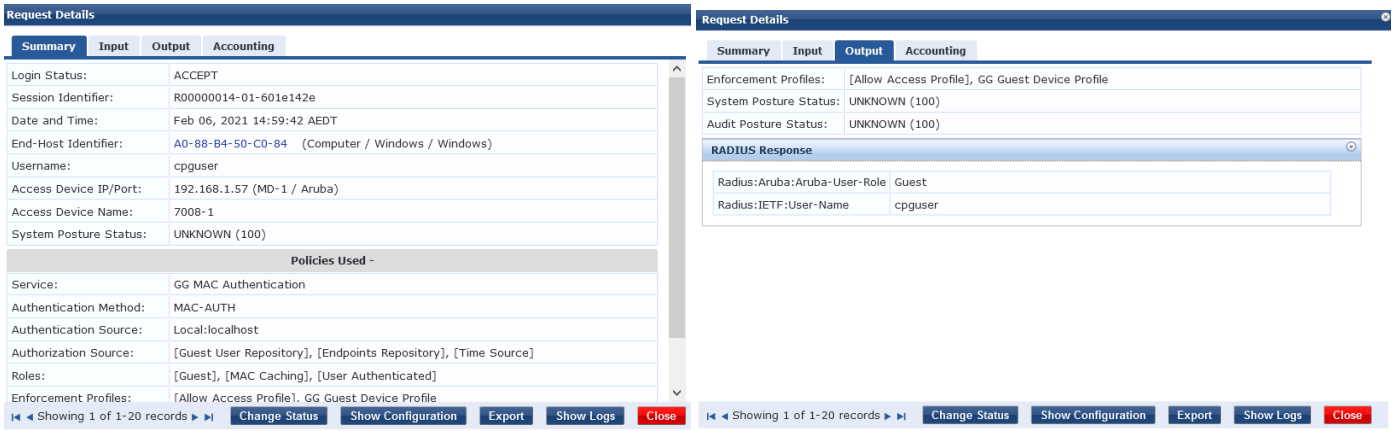
Now because the status of this endpoint is known the next time this client connects it will not be redirected to the captive portal until its allotted time has expired. So now if we disconnect the client, we should see it will successfully MAC auths.





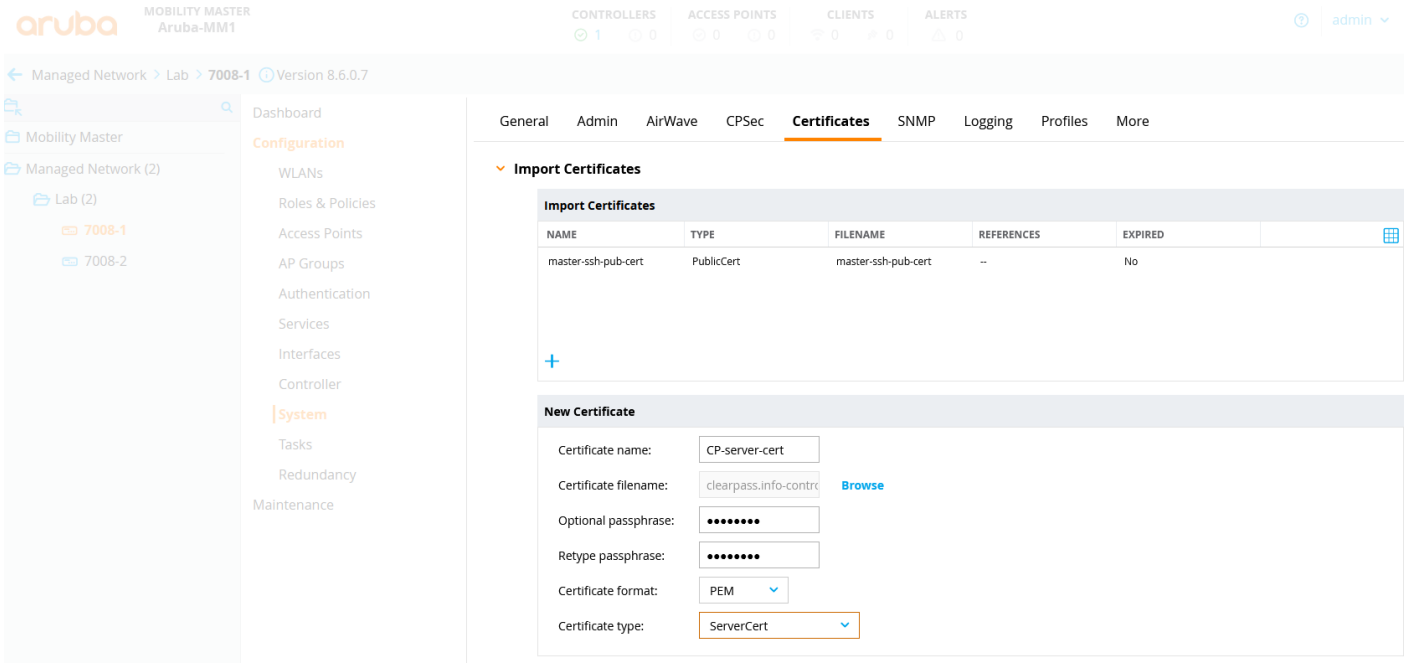


Looking at the details of that session

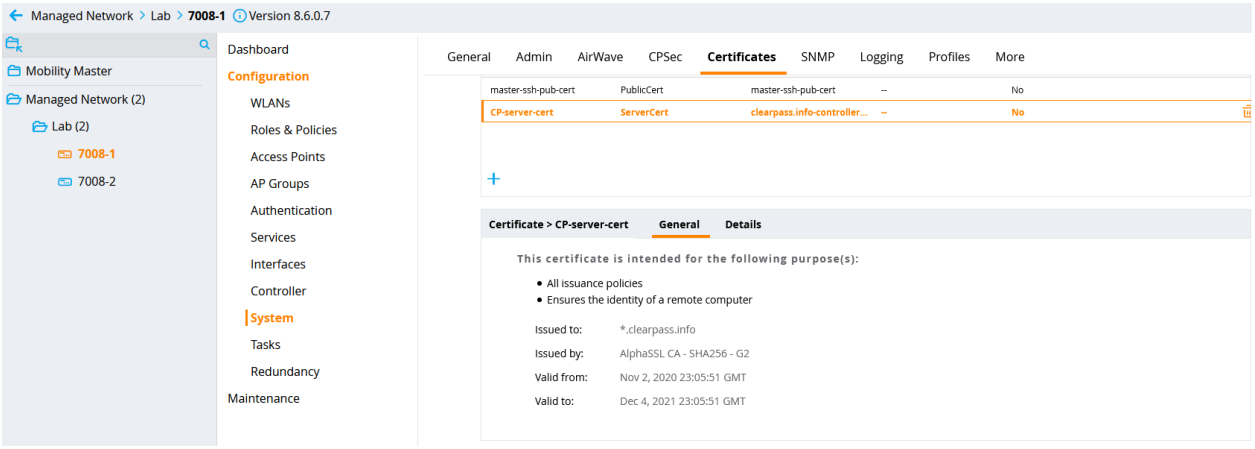


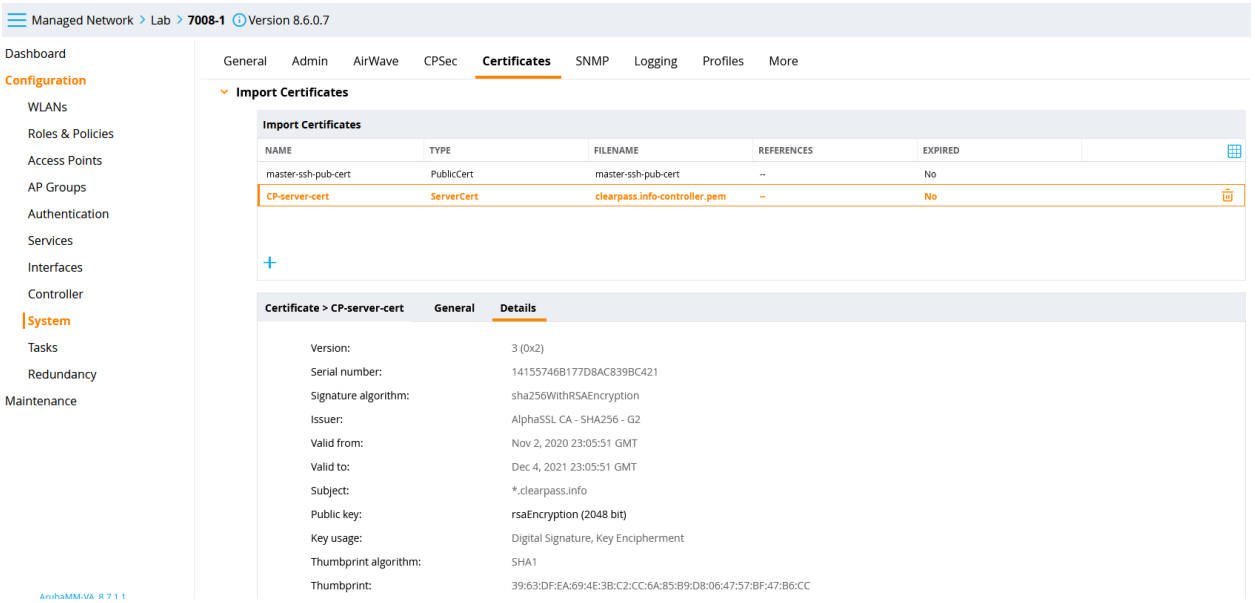
7.5 Captive Portal Server Certificate for MD

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

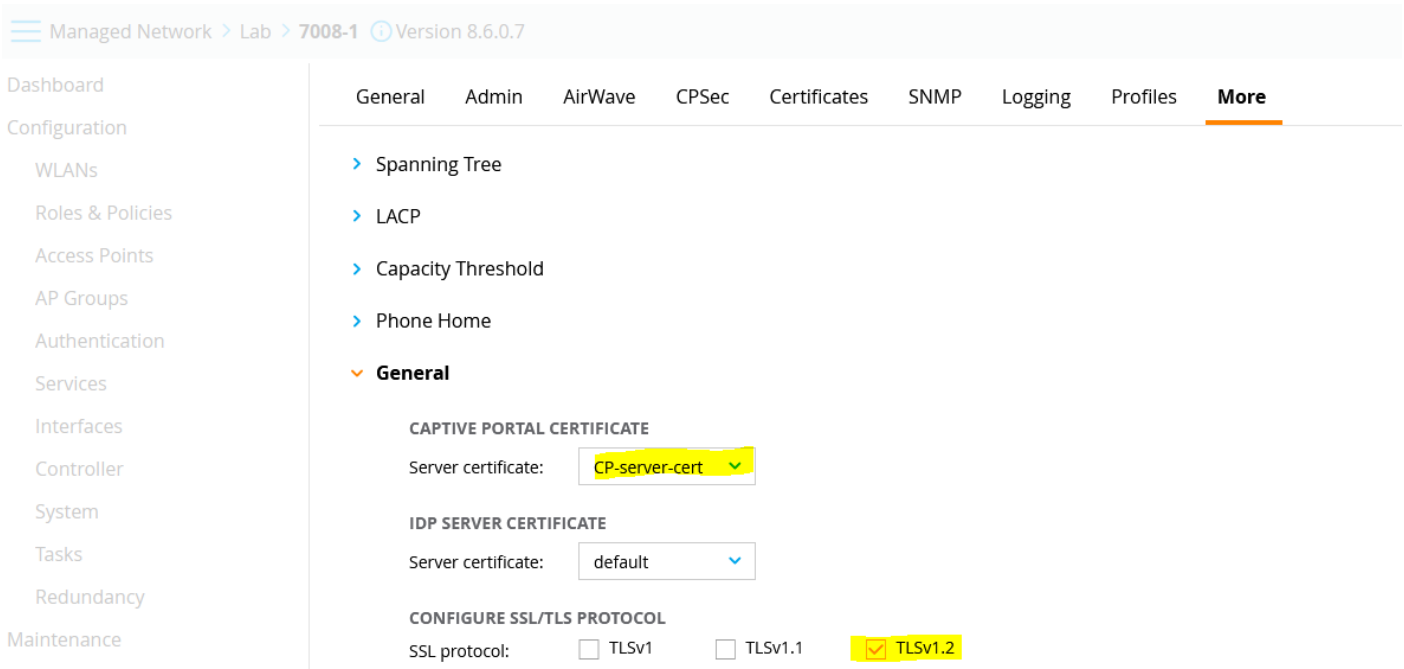


Once it is submitted.





Now you need to assign it as Captive Portal certificate.



Checking it from the CLI

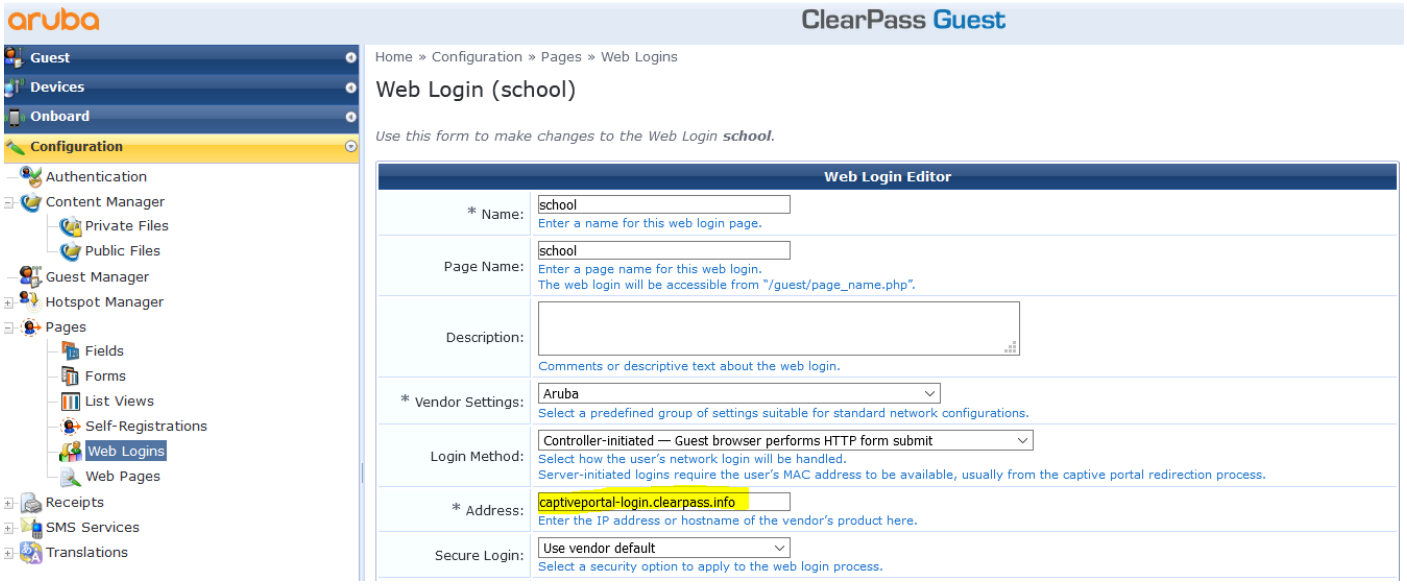
```
(7008-1) #show crypto pki serverCert

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, now we should be using "captiveportal-login.clearpass.info".



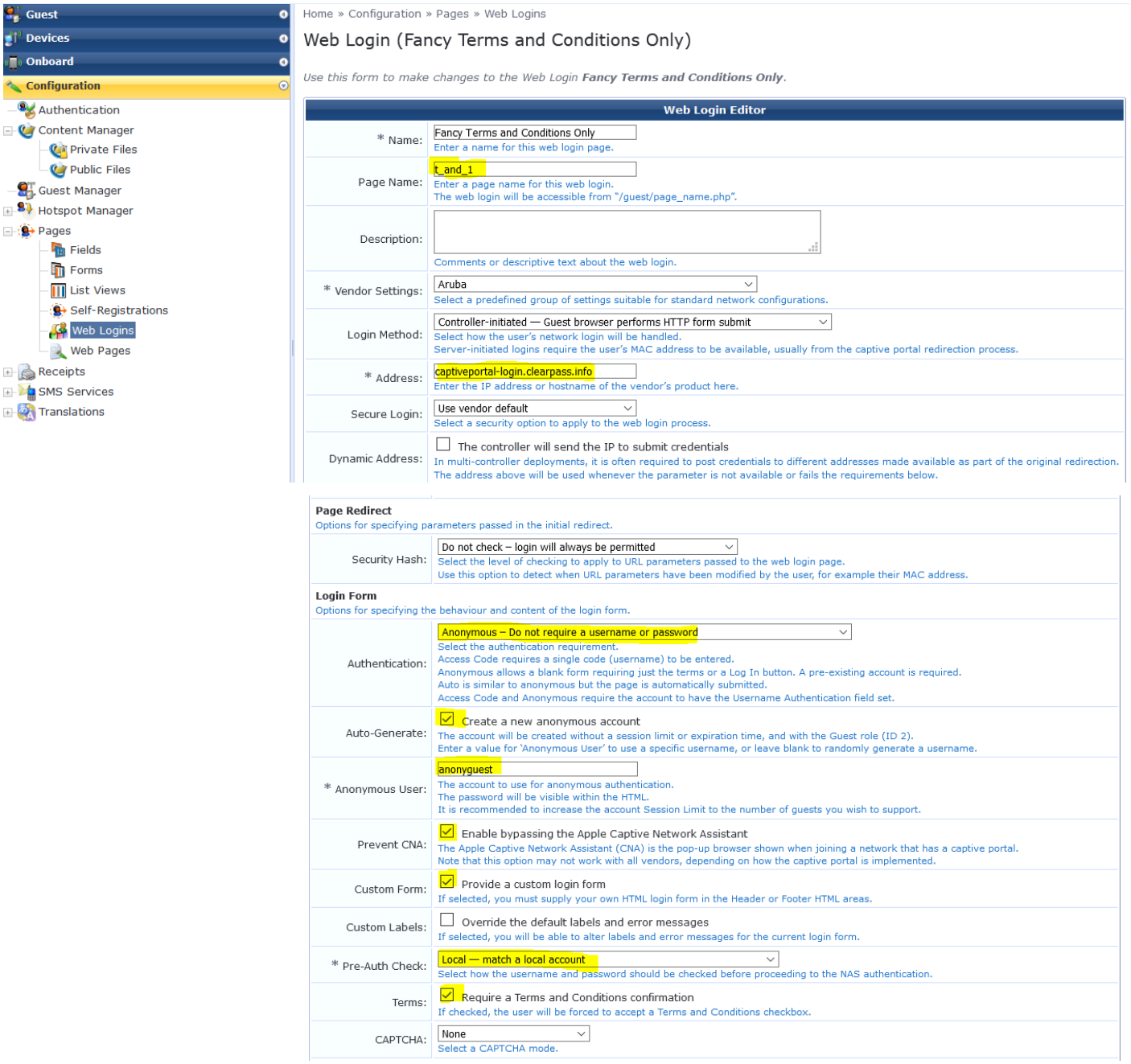
Now with all this in place, the users should not see any browser warning for the initial redirection to the captive portal page.

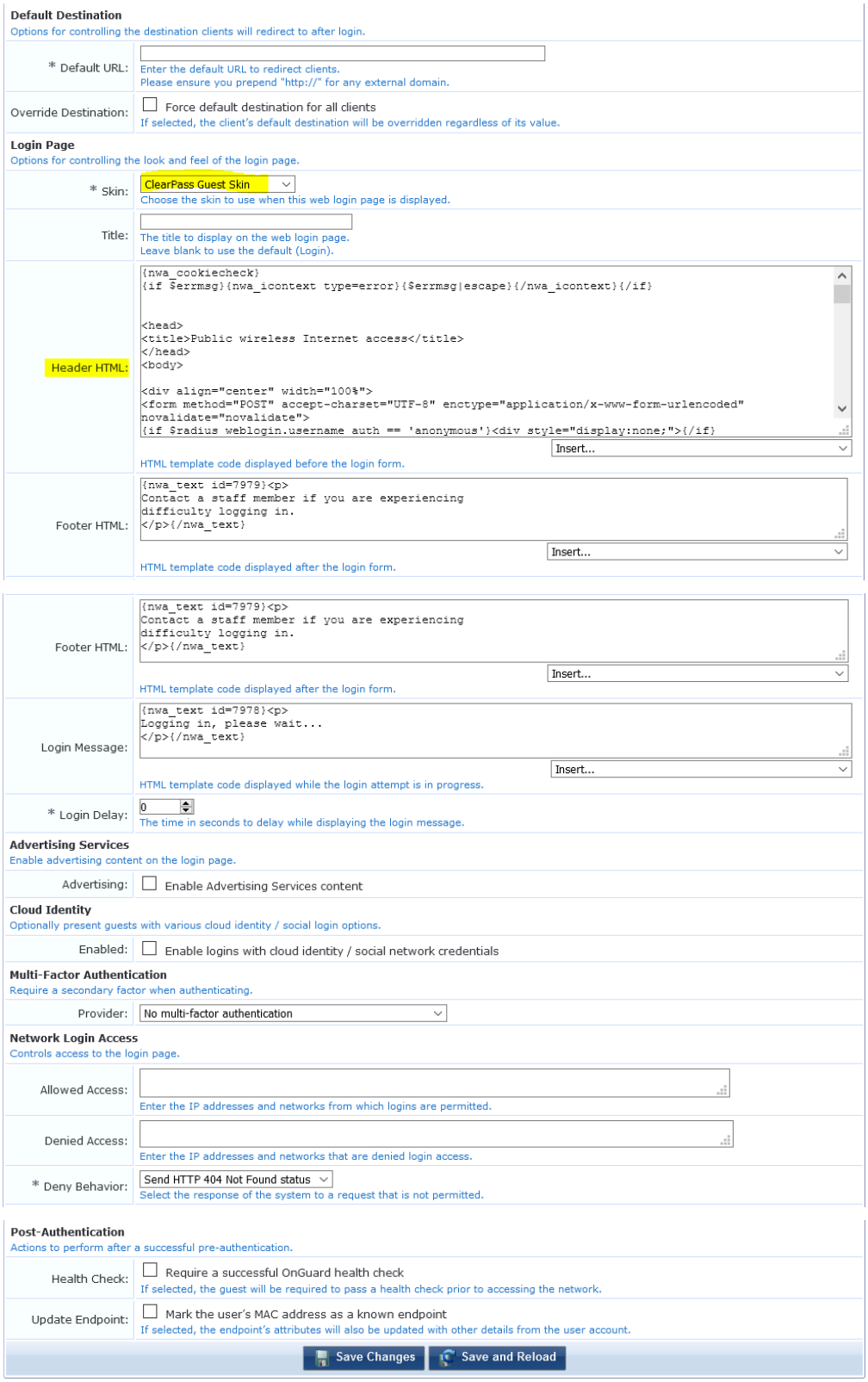
8 Guest Access with Terms of use

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



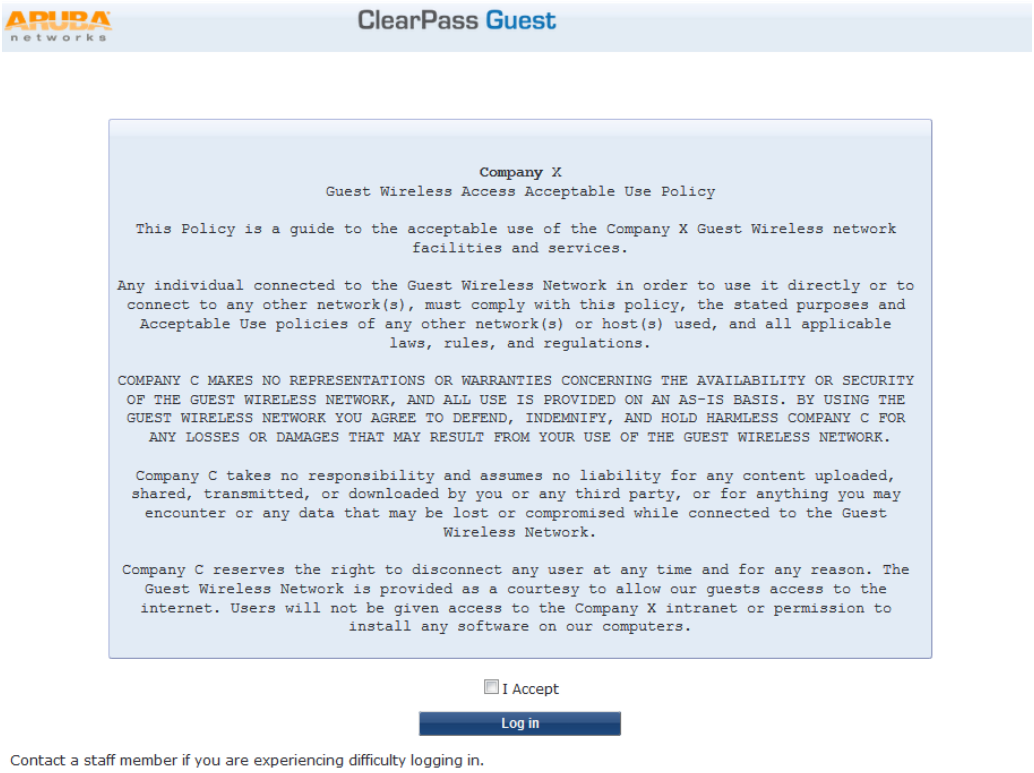


Here is the HTML code in the header section.

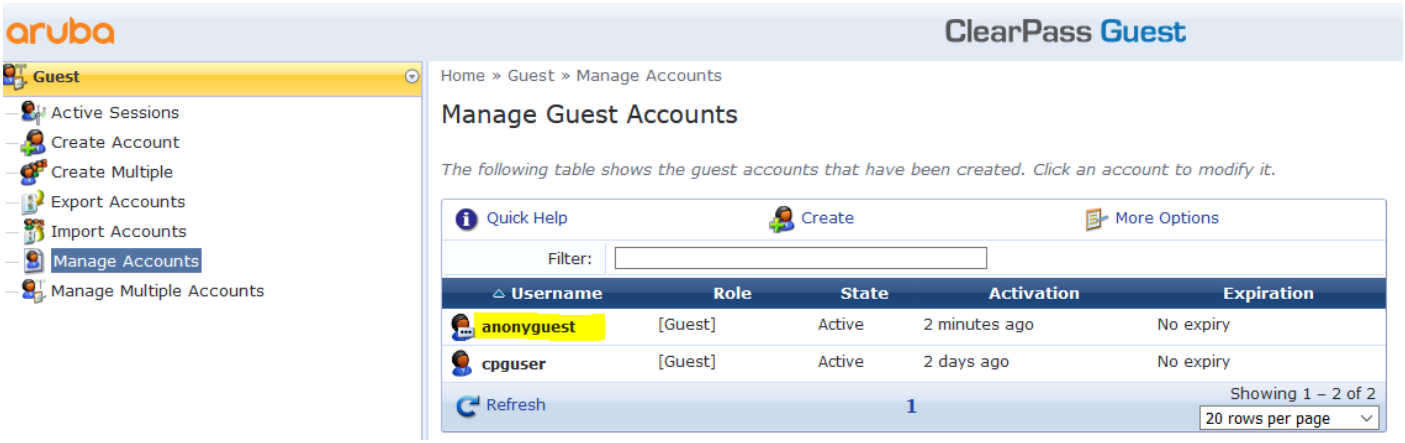
```
{nwa_cookiecheck}
{if $errmsg}{nwa_icontext type=error}{$errmsg|escape}{/nwa_icontext}{/if}

<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>
```

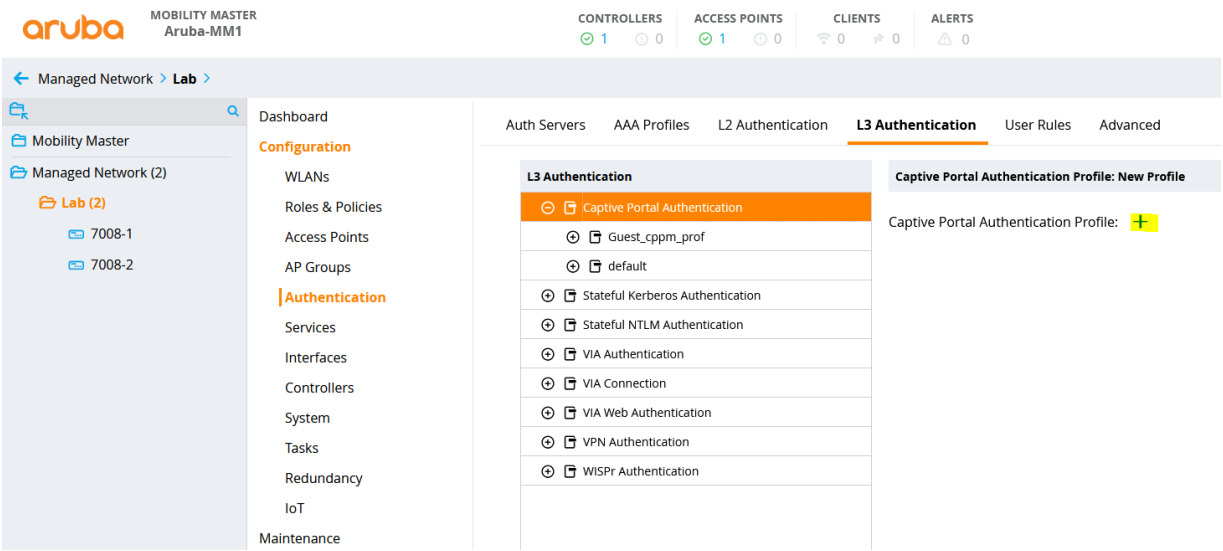
And this is how it looks.

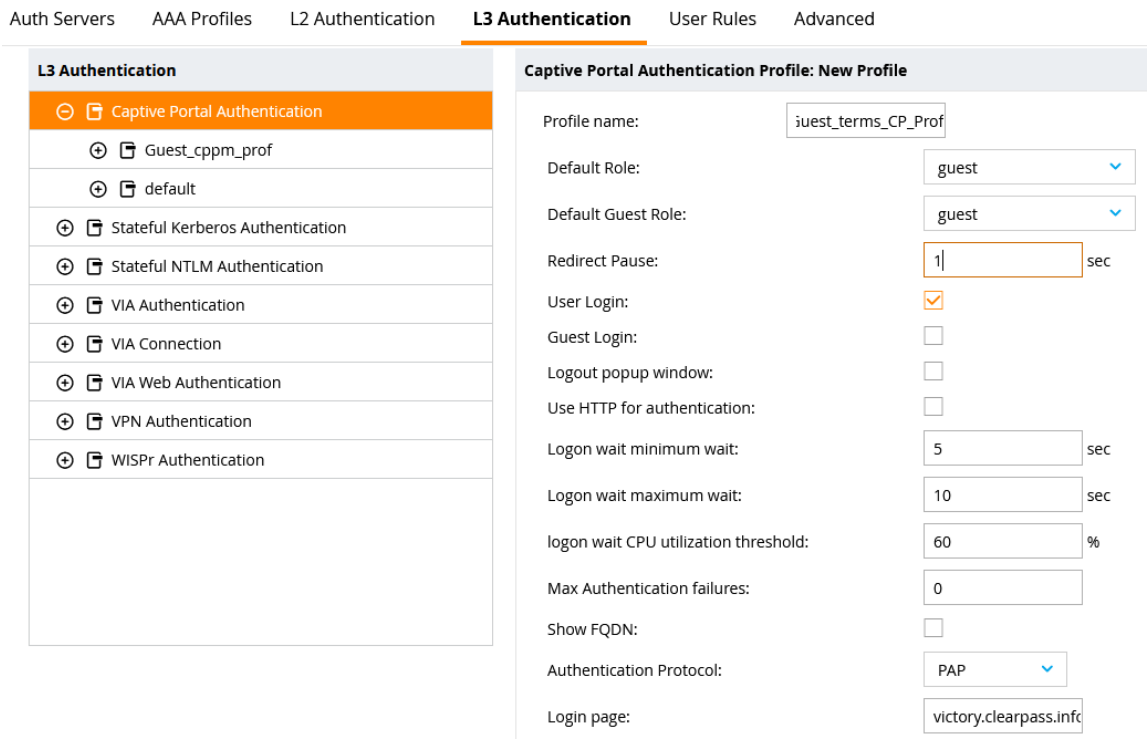


Now checking the guest account, we see the new account for anonymous guest users that was automatically generated.

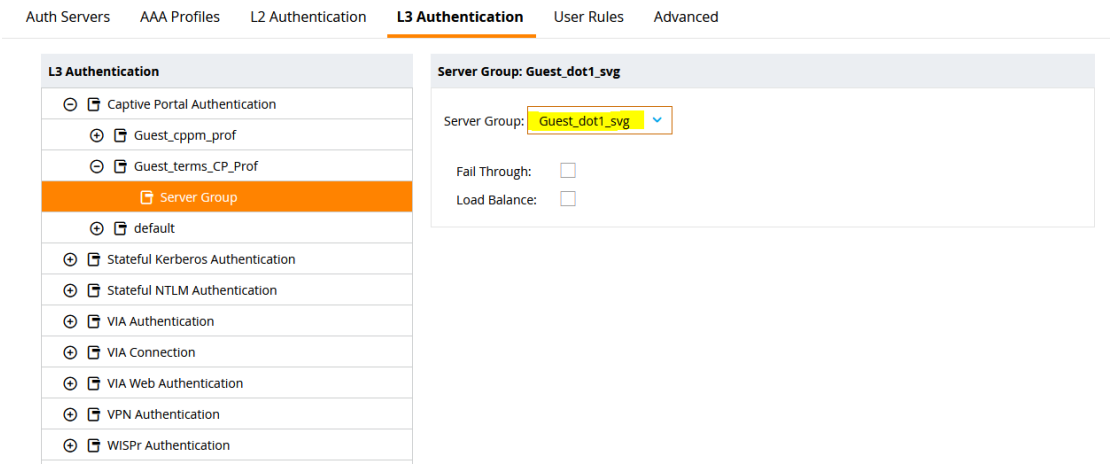


To use this captive portal page, we'll create a new controller captive portal profile so that it is pointing to this URL and then assign it in the initial user-role guest-logon.

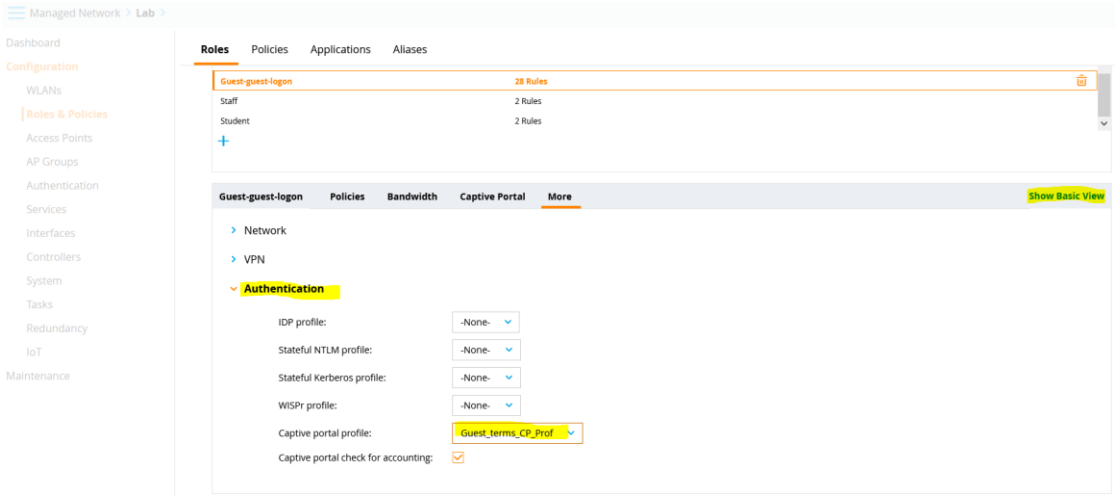




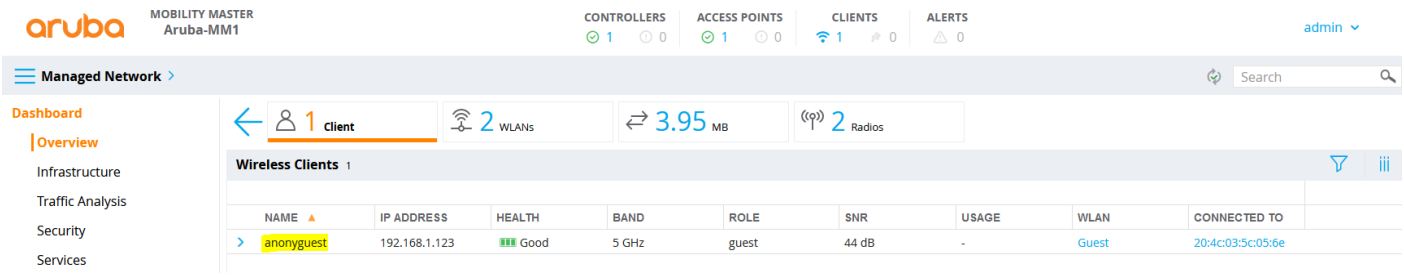
The login page is "https://victory.clearpass.info/guest/t_and_1.php? "



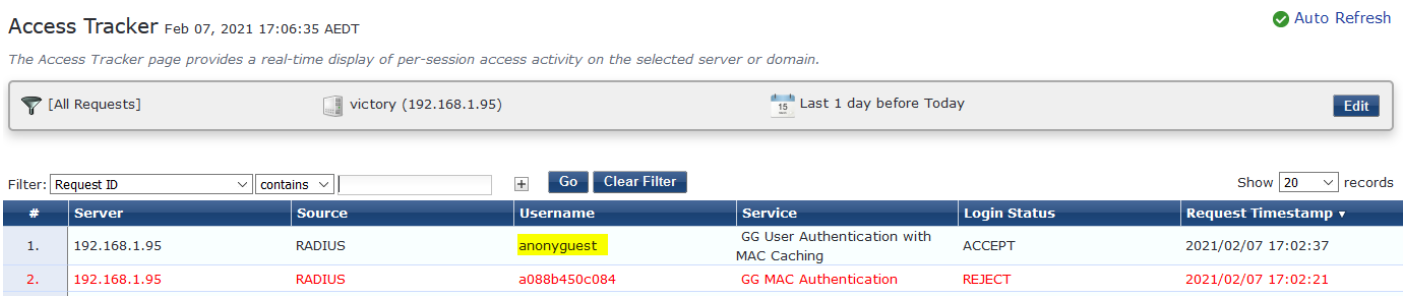
Now changing the guest-logon role to point to the new created captive portal profile.



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.



And this is what we see in access tracker.



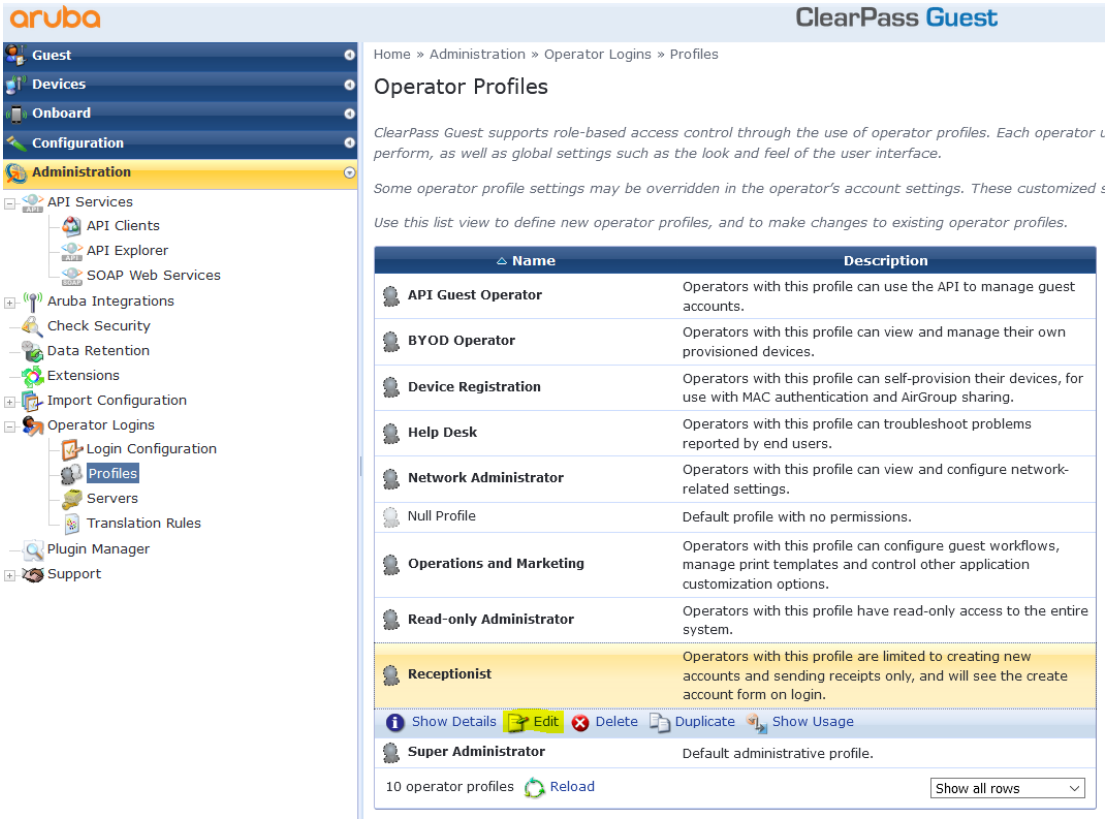
9 Guest Operator

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.

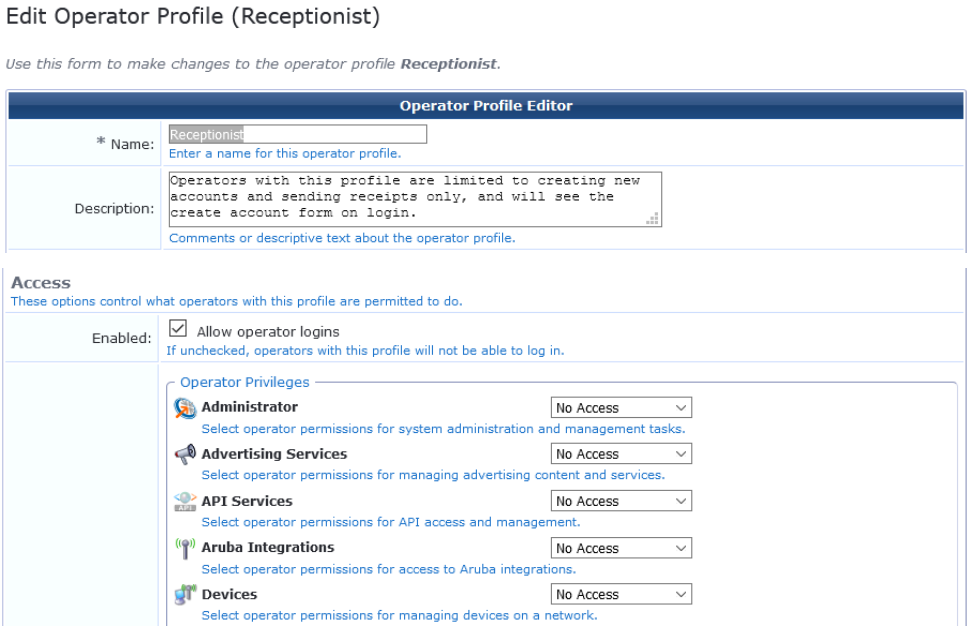
9.1 ClearPass Guest Operator Configuration

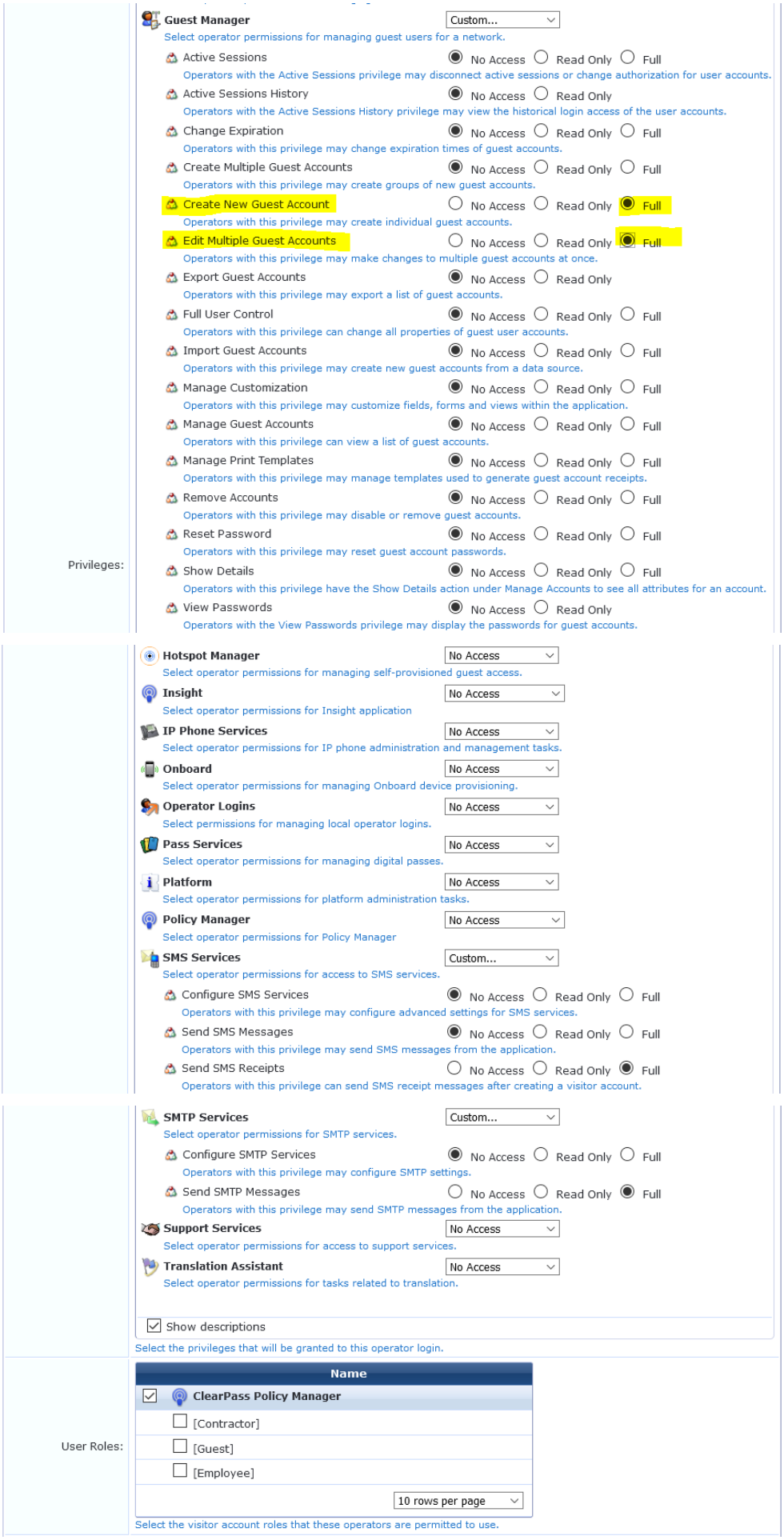
Open the Guest application by clicking the ClearPass Guest Link in the dashboard's Quick Links box for the URL redirection to ClearPass Guest.

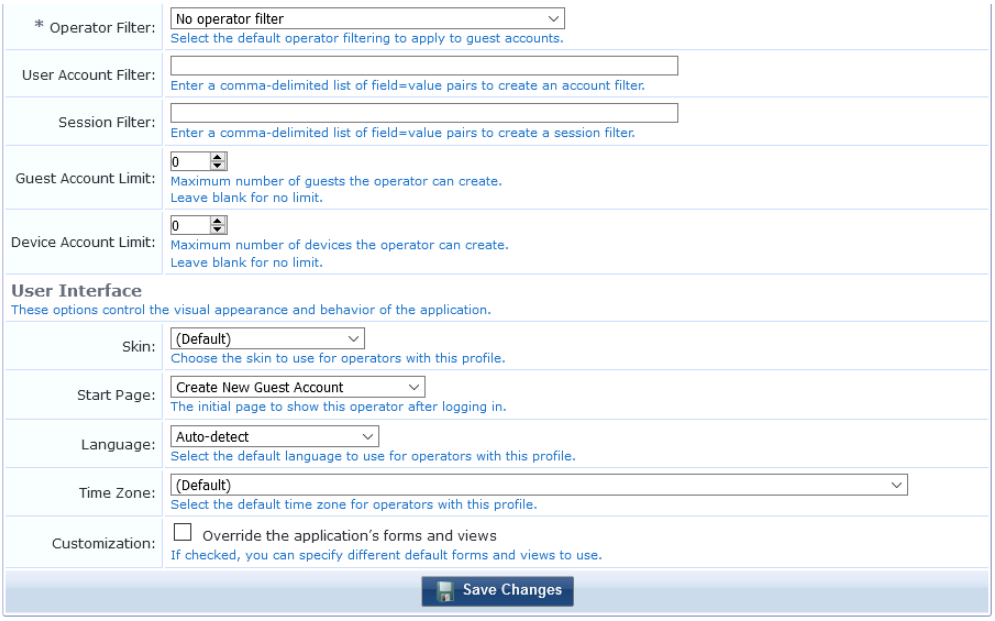
Navigate to Home » Administration » Operator Logins » Profiles



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.




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
ClearPass Policy Manager
[Contractor]
[Guest]
[Employee]
10 rows per page
Select the visitor account roles that these operators are permitted to use.

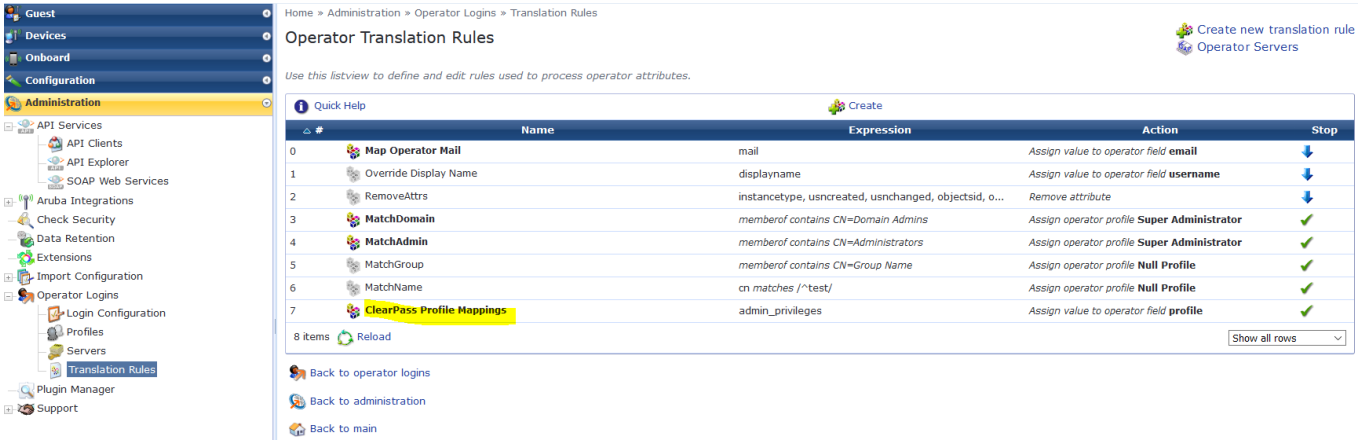


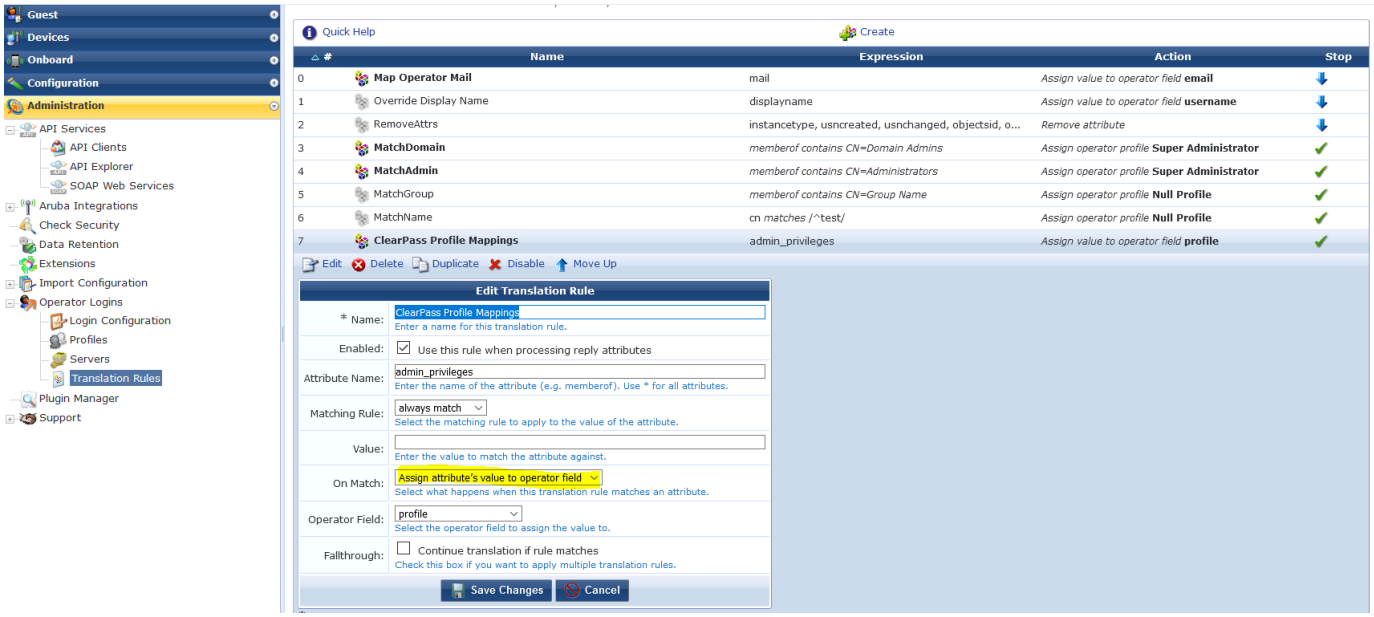
You can edit the profile based on your requirements. We have enabled "Read Only" for

- 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

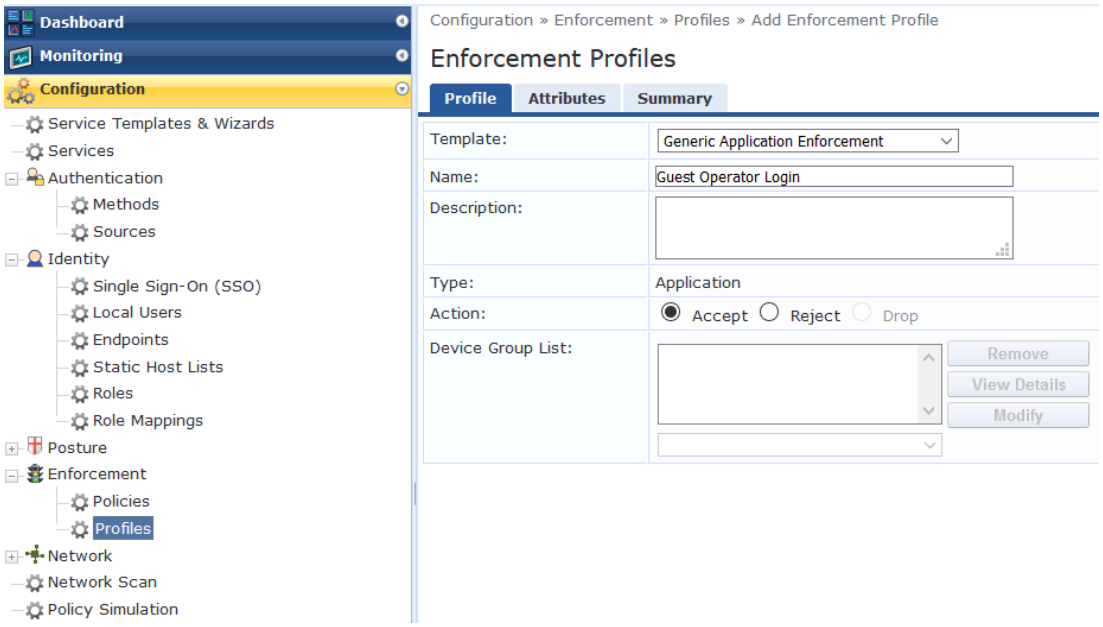


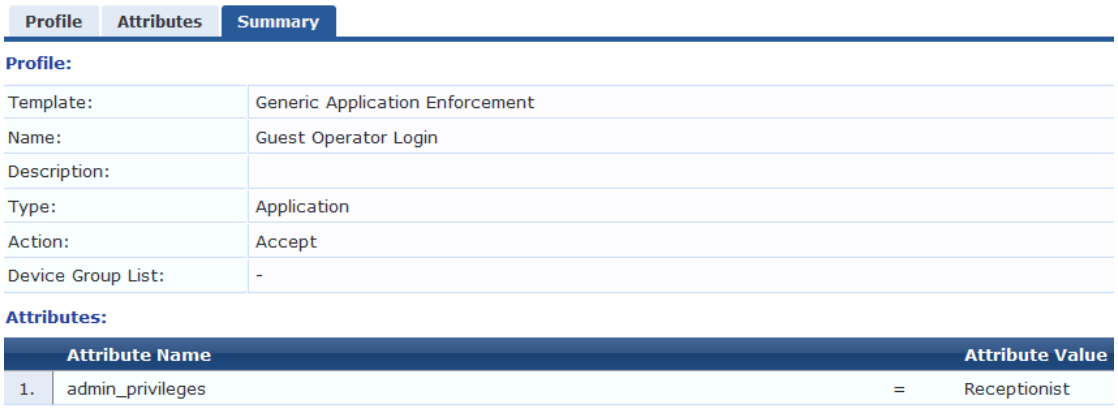


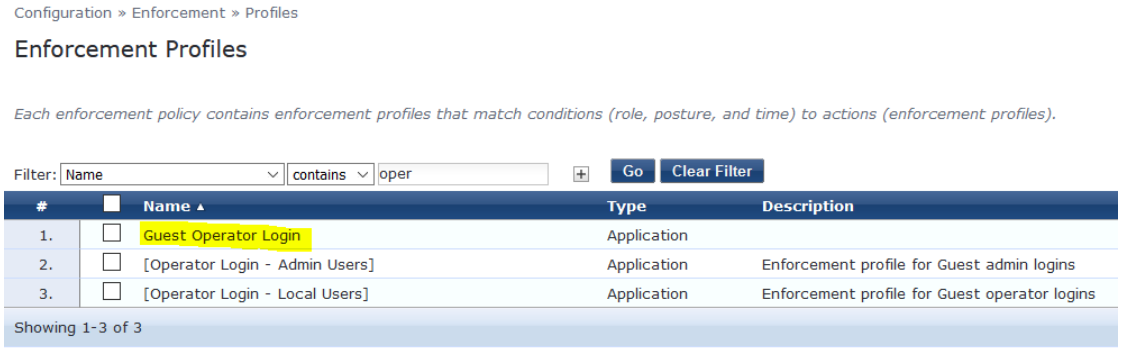
So once the receptionist user, type in their user credentials, the request should match a ClearPass Policy manager service,

- 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.

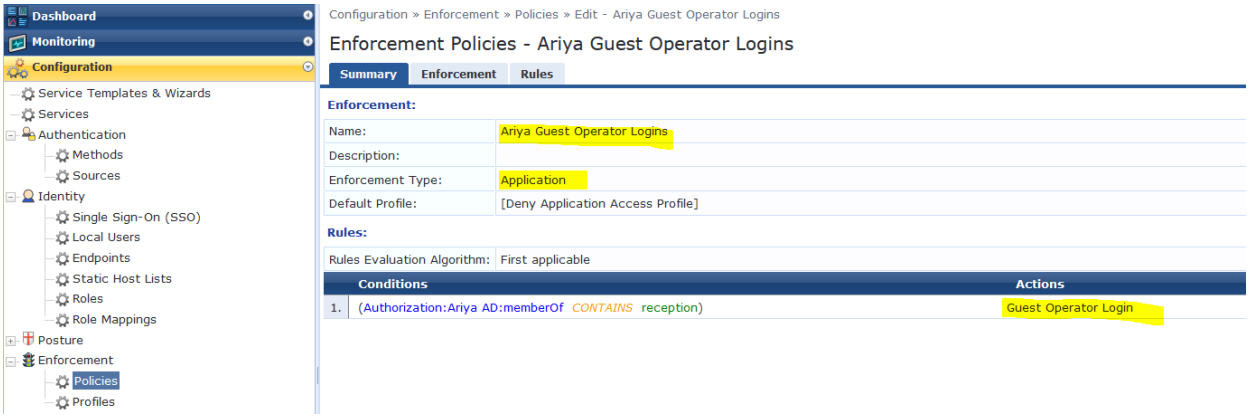
Now going back to ClearPass Policy manager, we’ll create the following enfocemenet profile



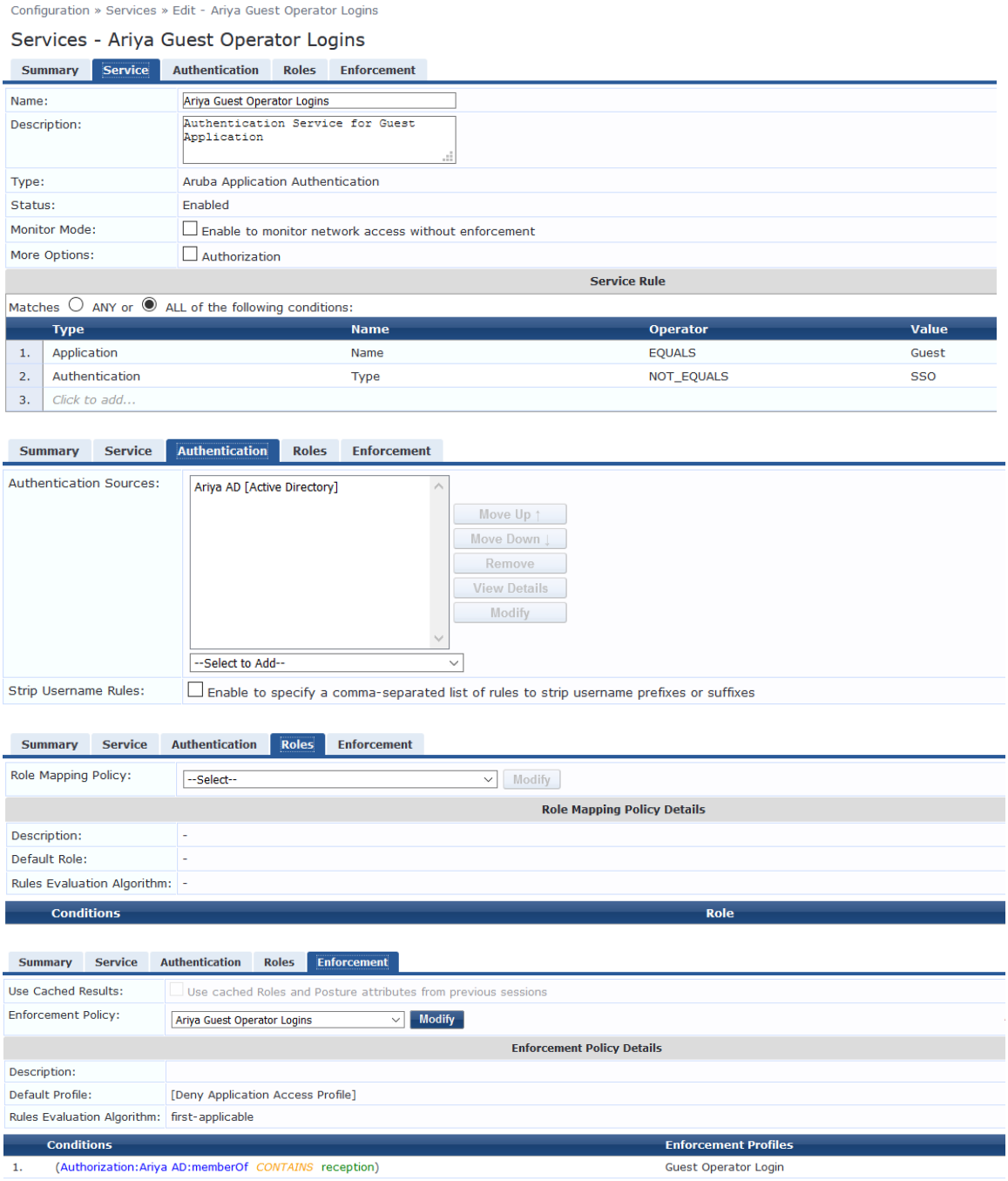




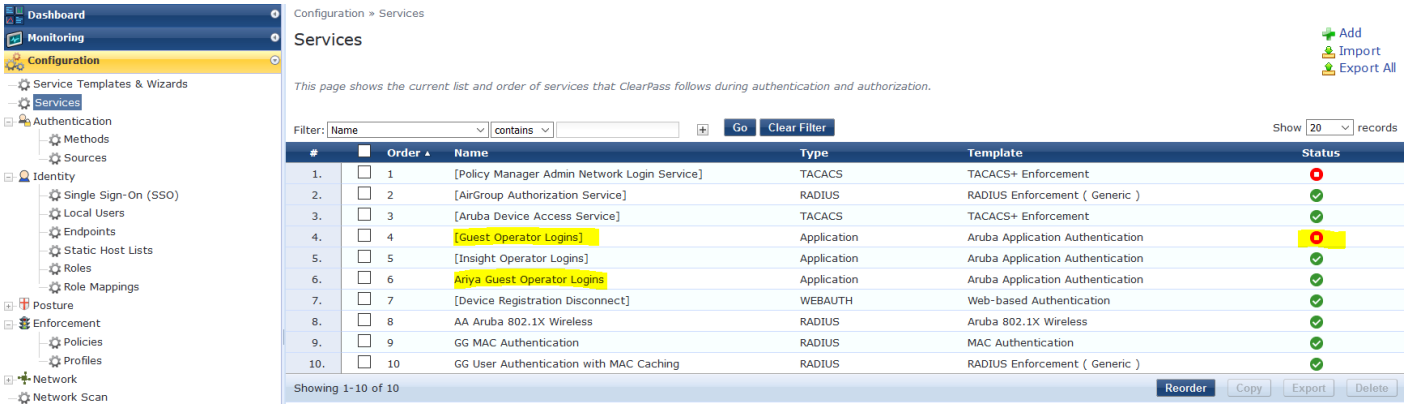
Next, we’ll create a enforcement policy that will use the above enforcement profile.



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

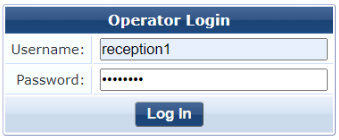


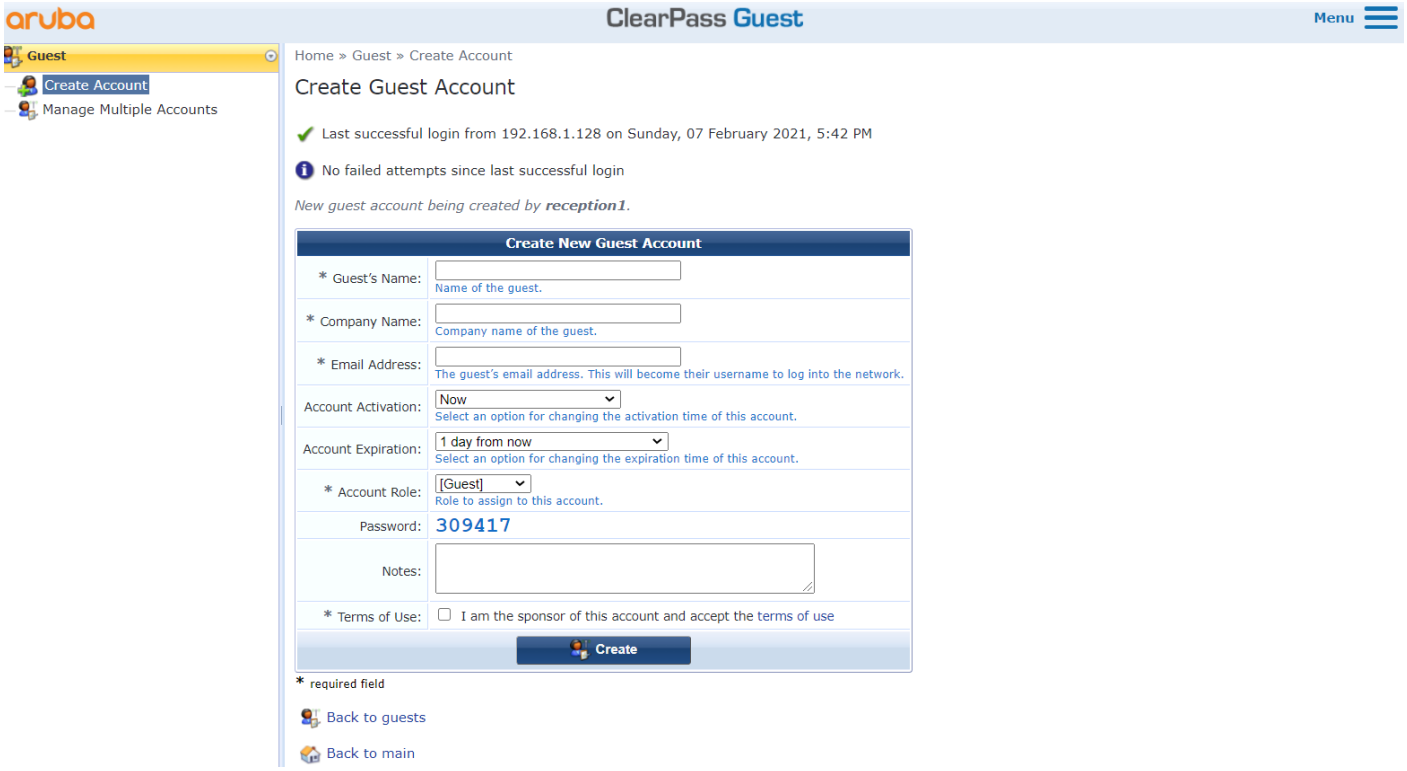
The last thing is to reorder the services and disable the default [guest operator logins] service.



Now we'll test it out. The URL that the operators need to browse to is https://victory.clearpass.info/guest/

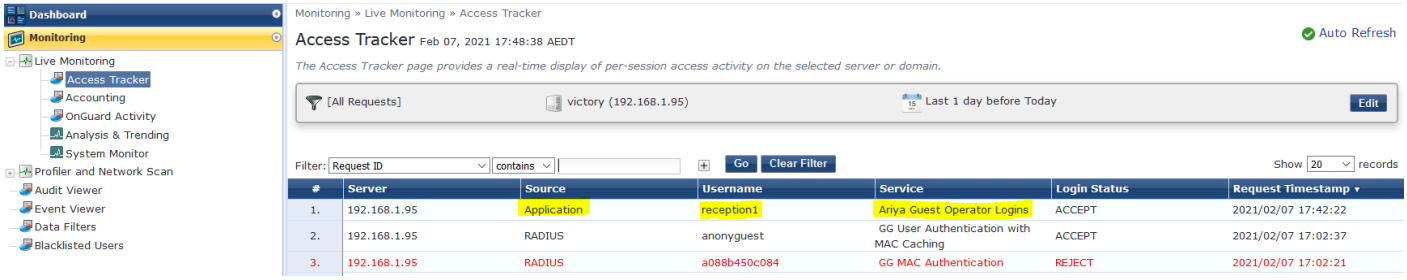
And the user used the following credentials and authenticates successfully.

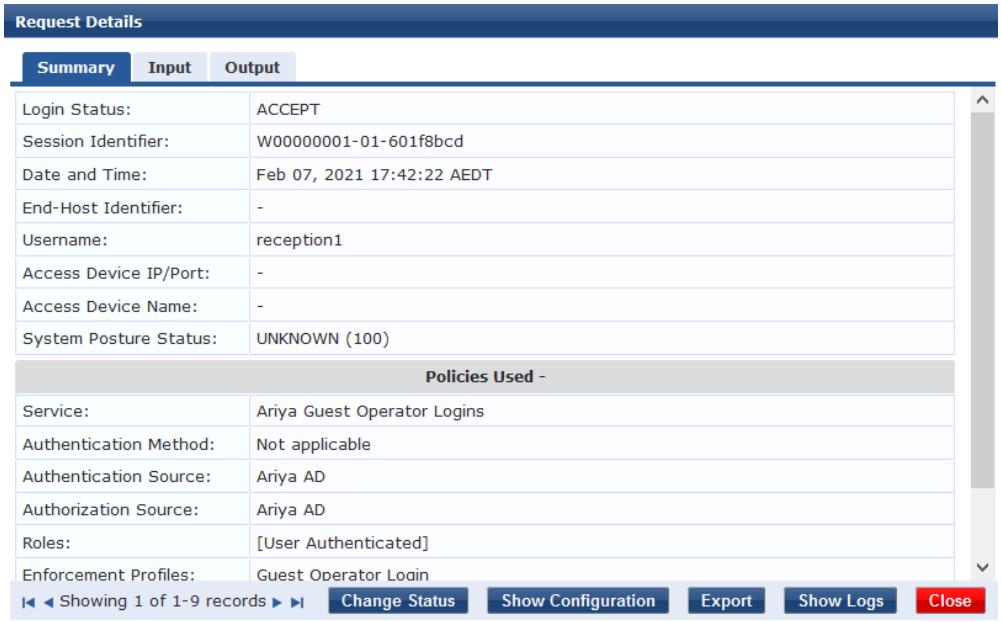


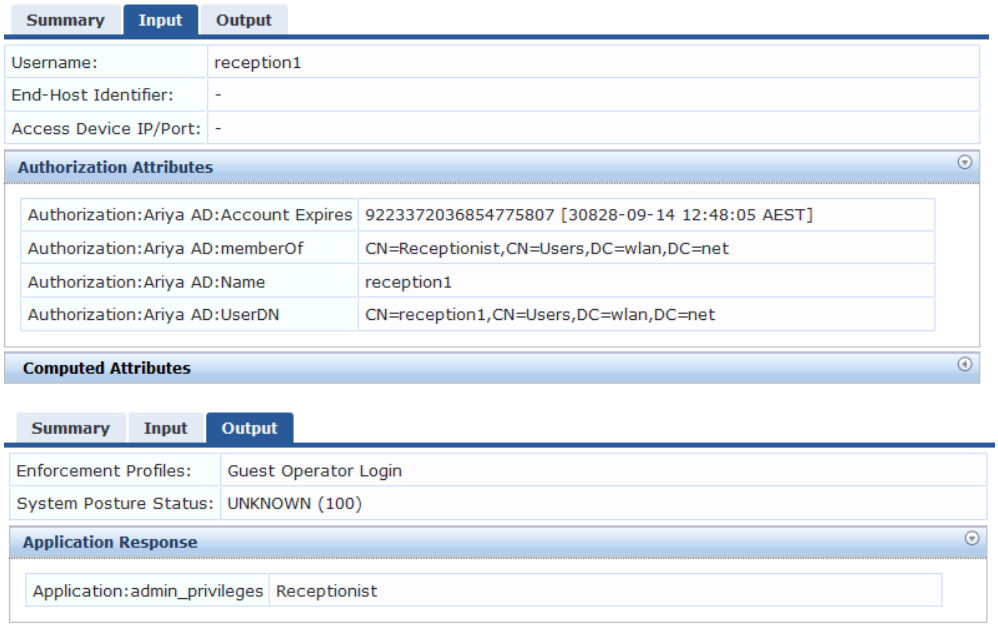


Now the reception user can create the guest account, the details can be emailed to the guest user as well.

Here is the authentication session in access tracker



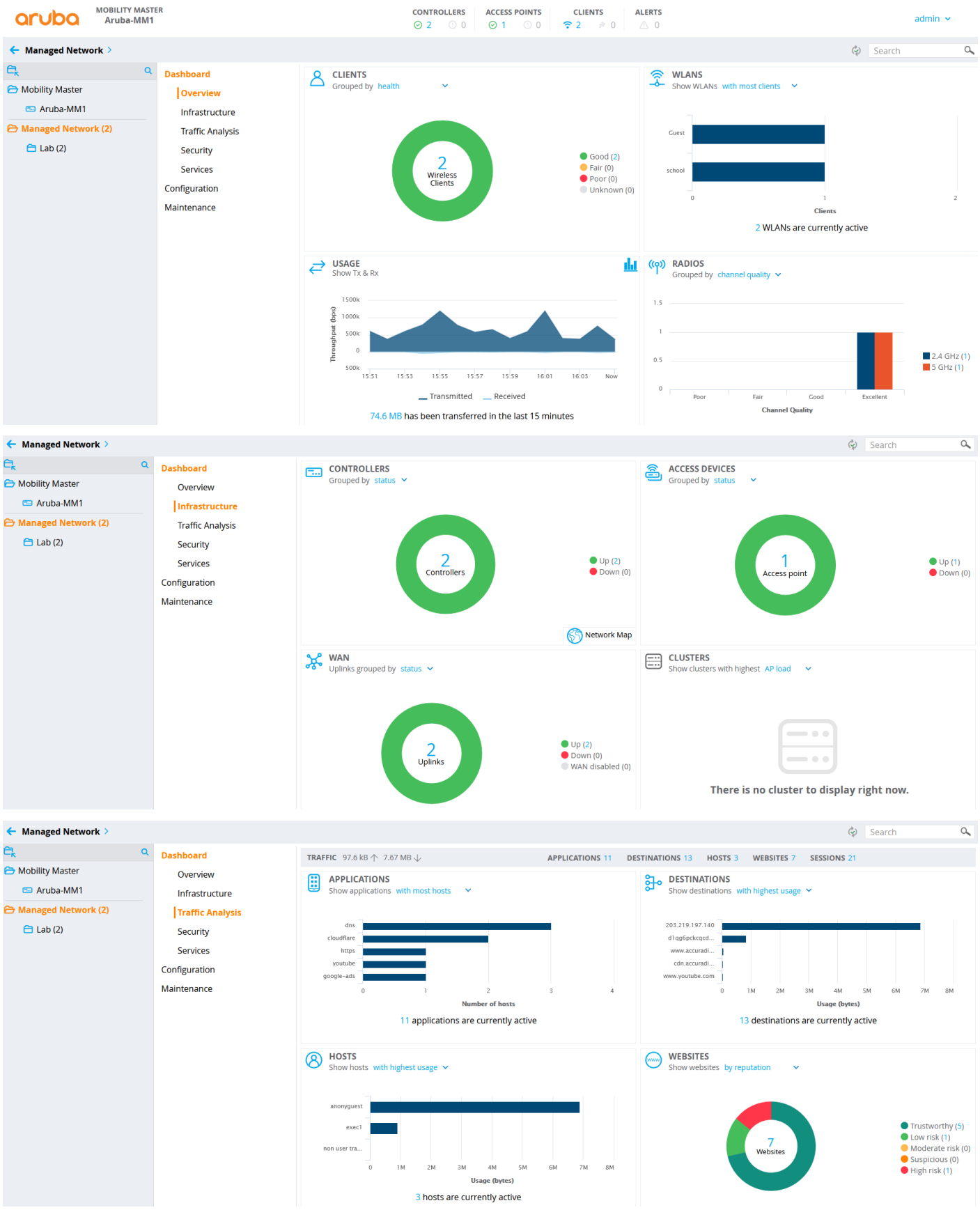


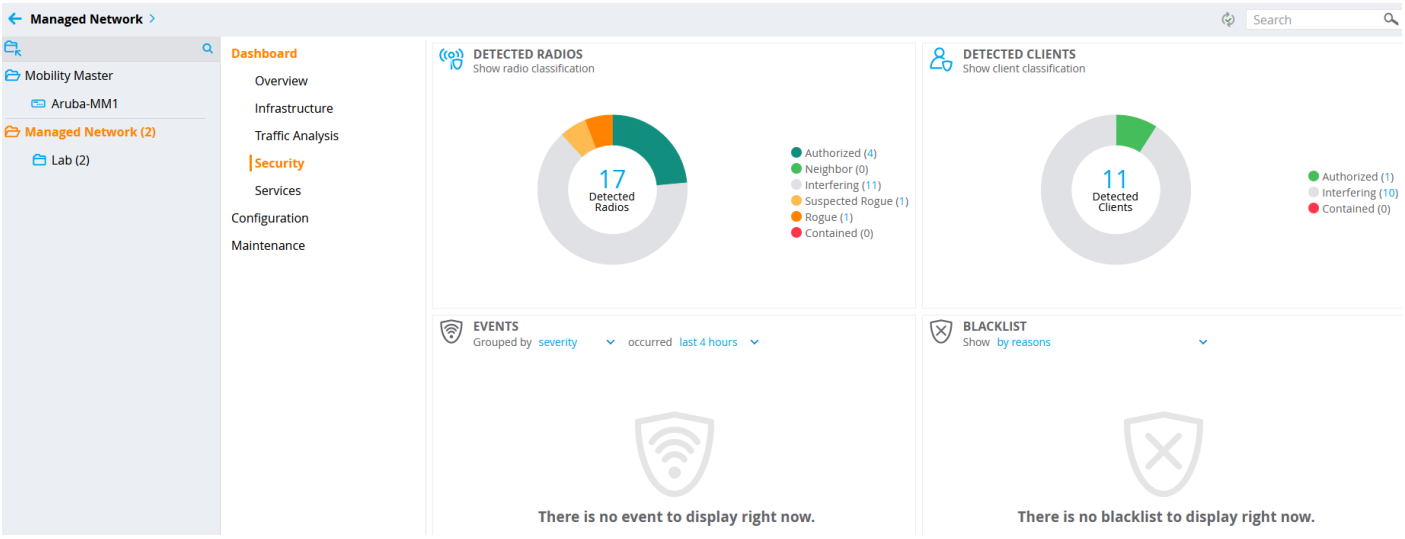


You can customise all the fields in this form which is outside the scope of this guide.

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.