Aruba Wireless and ClearPass 6 Integration Guide

Technical Note

Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. Includes software from Litech Systems Design. The IF-MAP client library copyright 2011 Infoblox, Inc. All rights reserved. This product includes software developed by Lars Fenneberg et al. The Open Source code used can be found at this site::

http://www.arubanetworks.com/open_source

Legal Notice

The use of Aruba Networks, Inc. switching platforms and software, by all individuals or corporations, to terminate other vendors' VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Aruba Networks, Inc. from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of those vendors.

Warranty

This hardware product is protected by the standard Aruba warranty of one year parts/labor. For more information, refer to the ARUBACARE SERVICE AND SUPPORT TERMS AND CONDITIONS.

Altering this device (such as painting it) voids the warranty.

www.arubanetworks.com
1344 Crossman Avenue
Sunnyvale, California 94089
Phone: 408.227.4500
Fax 408.227.4550

Table of Contents

1. Aruba Wireless and ClearPass 6.0.1 Integration Guide

Purpose

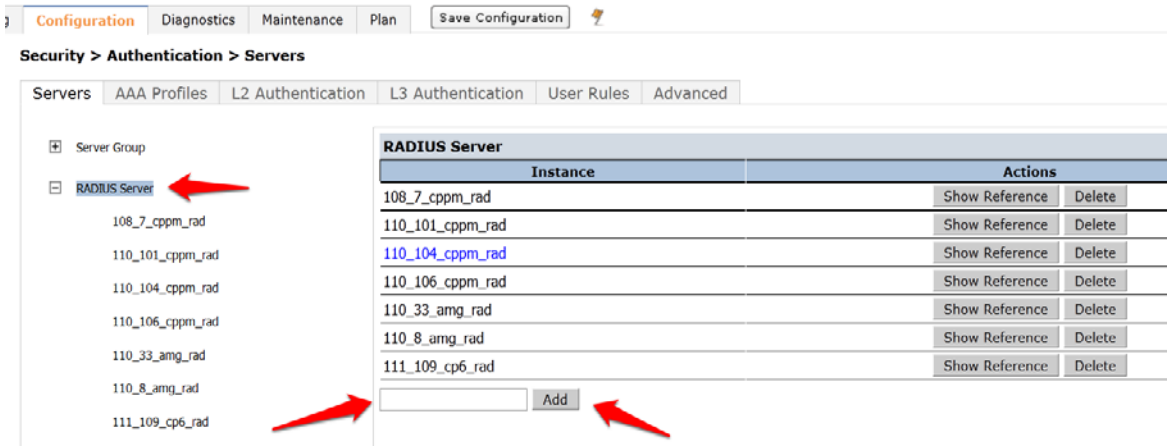
The purpose of this document is to provide instructions for integrating Aruba Networks Wireless Hardware with ClearPass 6.0.1. This will include basic topics for 802.1x, RADIUS, and Guest integration in an environment using an Aruba Networks WLAN Solution.

Assumptions

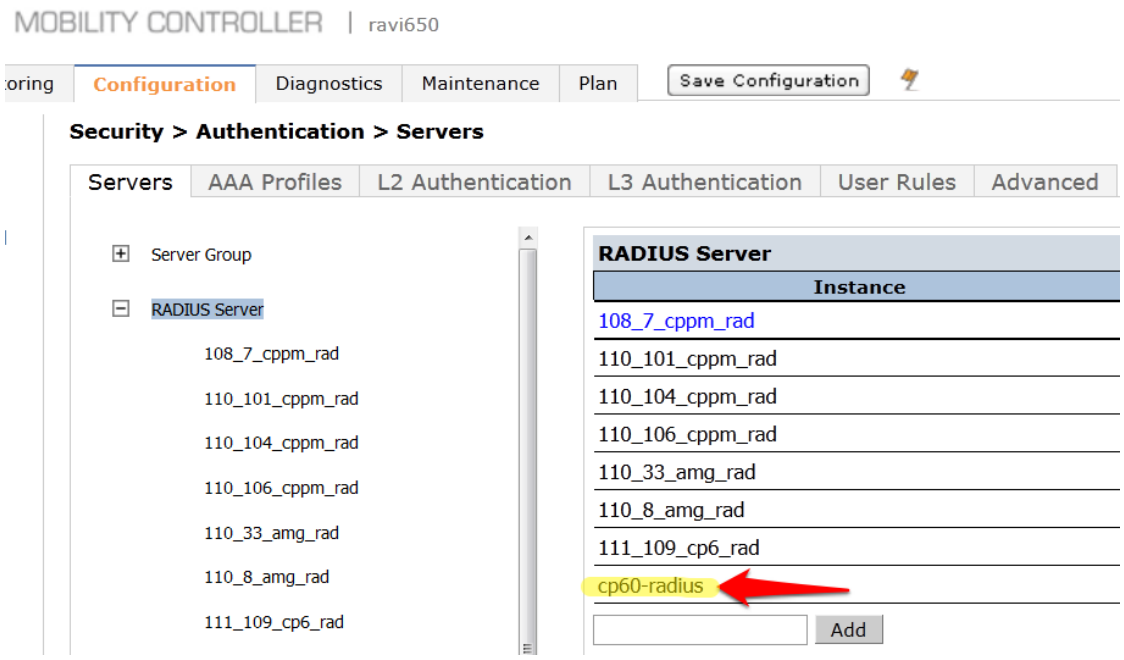
1. Aruba Networks wireless controller is setup and running the latest code.
2. At least one access point is provisioned on the controller for testing.
3. 802.1x SSID is already configured.
4. Guest SSID with Captive Portal is already configured.
5. DHCP and DNS are appropriately configured.
6. ClearPass 6.0.1 server (VM or Physical Appliance) initial setup is complete. This includes network settings, time and date, and system name.
7. Aruba Wireless controller can communicate with ClearPass 6.0.1.
8. The Guest SSID VLAN can communicate with ClearPass 6.0.1.
9. All systems are appropriately licensed.
10. Only one interface is configured on ClearPass.

Step 1: AOS Controller Configuration

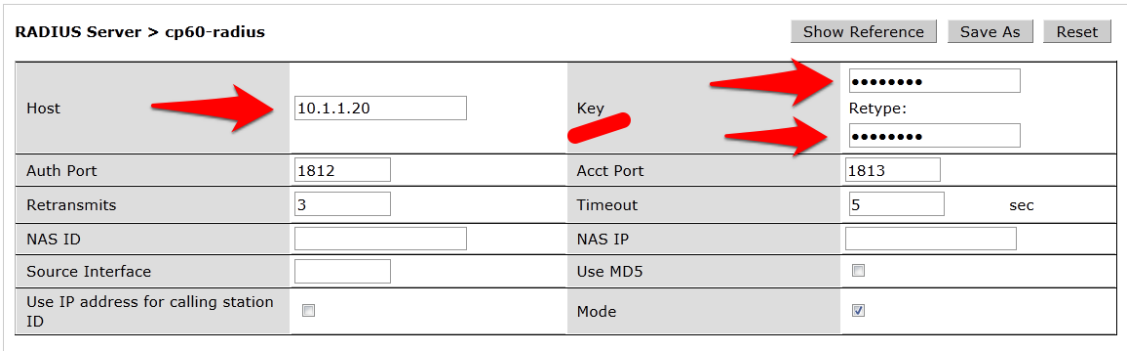
Login to the controller GUI as an admin user. Navigate to **Configuration->Security->Authentication->Servers tab**. Click on **RADIUS Server** and create a new RADIUS server by entering the new RADIUS server reference name in the empty Add box and clicking **Add**.



Click on the new server name that shows up in the RADIUS Server list on that page:



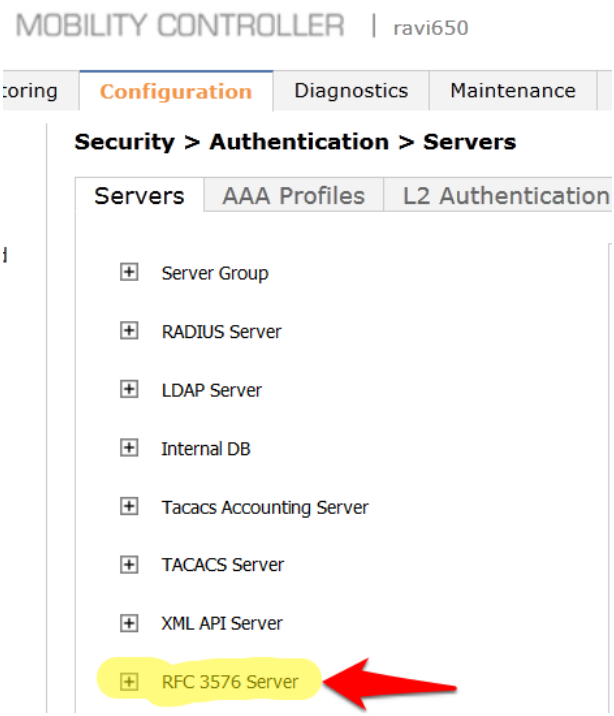
Enter the IP address for ClearPass in the **Host** field. Enter aruba123 for the **key**. Click **Apply** at the bottom of the page to save these configuration settings.



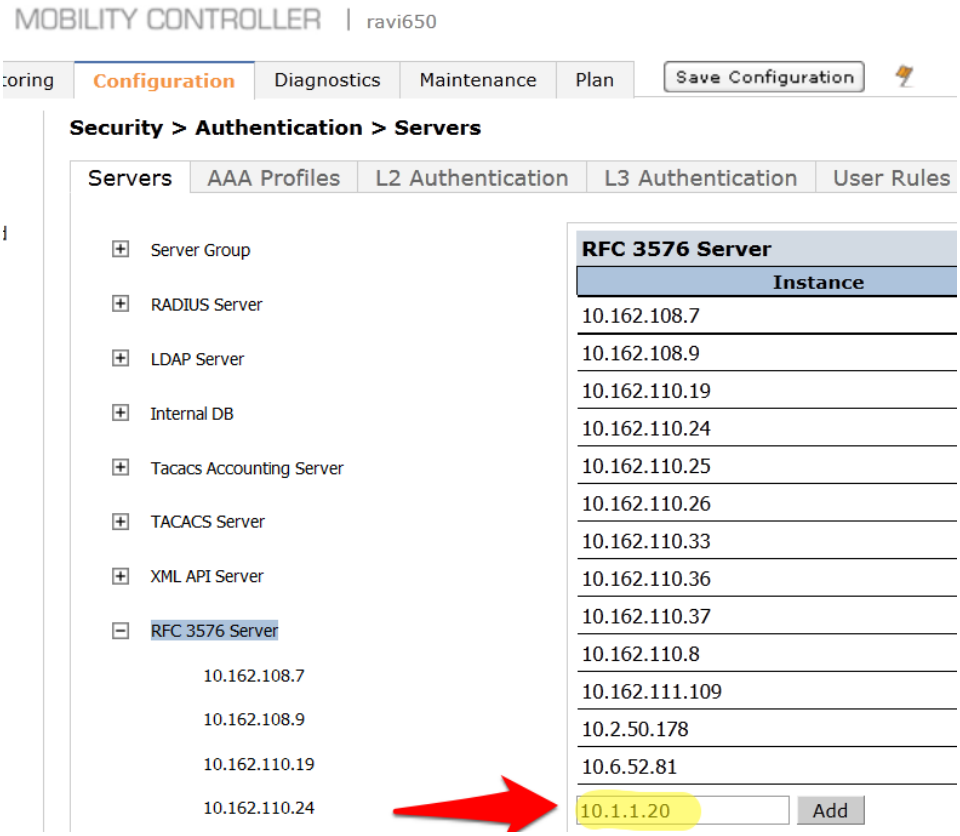
Step 2: Adding a RFC 3576 Server

The next step is to add an RFC 3576 server entry for ClearPass.

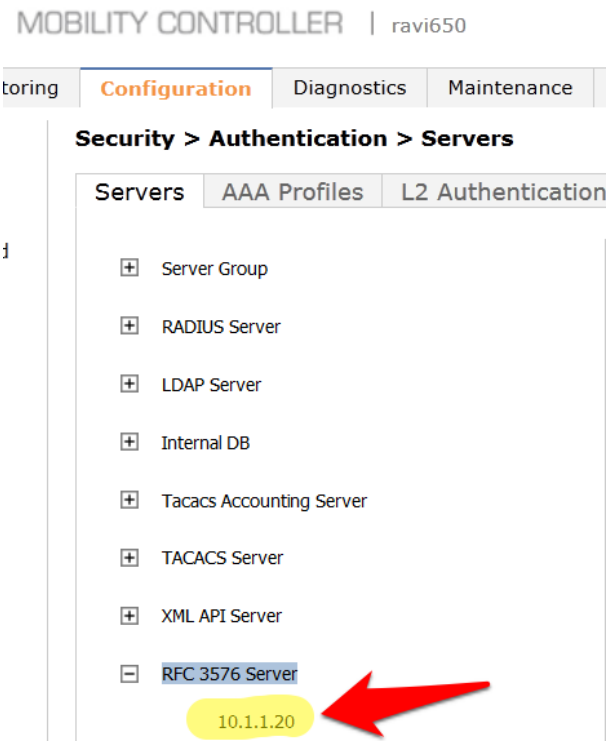
Click on **RFC 3576 Server.**



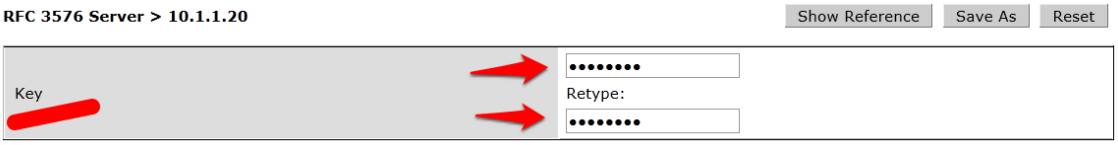
Enter the **IP address** of ClearPass in the entry box and click **Add**.



Click on the IP address of ClearPass that appears in the left column under RFC 3576 Server.



You will be presented with a screen in the right column that looks like this:

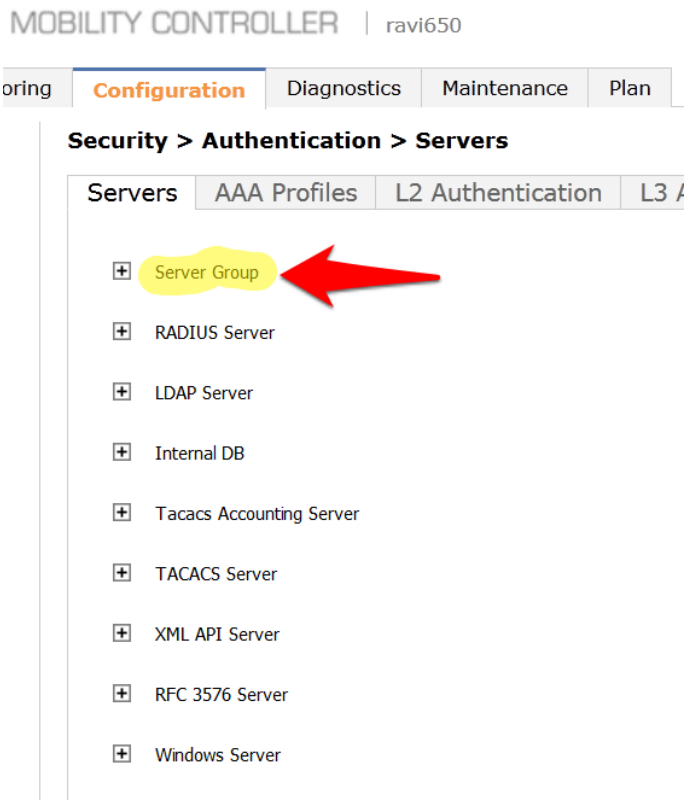


1. You **MUST** enter the RADIUS shared key into the key boxes. Enter aruba123 in both boxes and click **Apply** at the bottom of the page to save the changes.

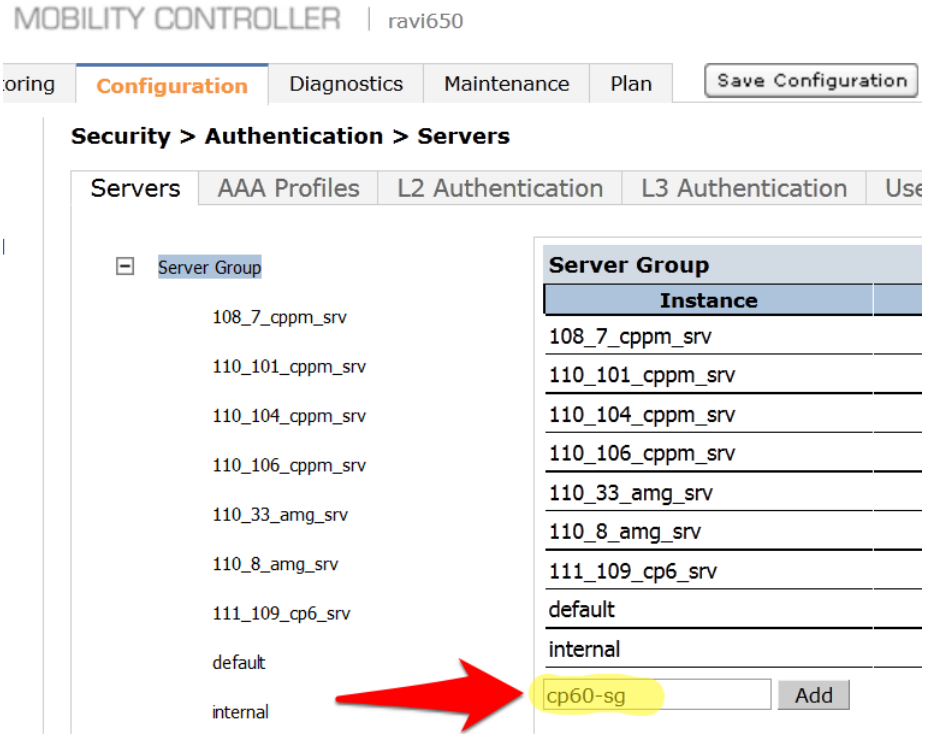
Note: This step is extremely important!

Step 3: Creating a new Server Group for ClearPass

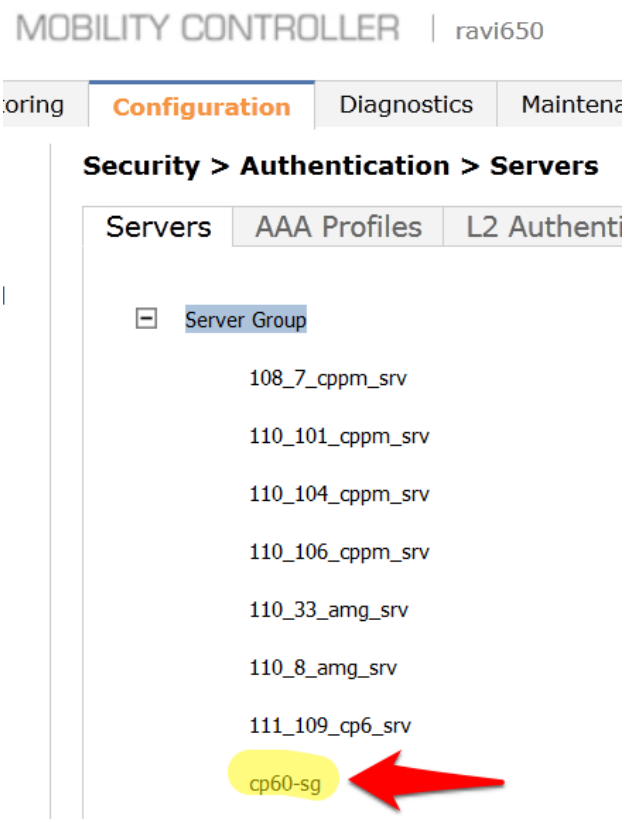
The next step is to create a new Server Group for ClearPass. Click on Server Group.



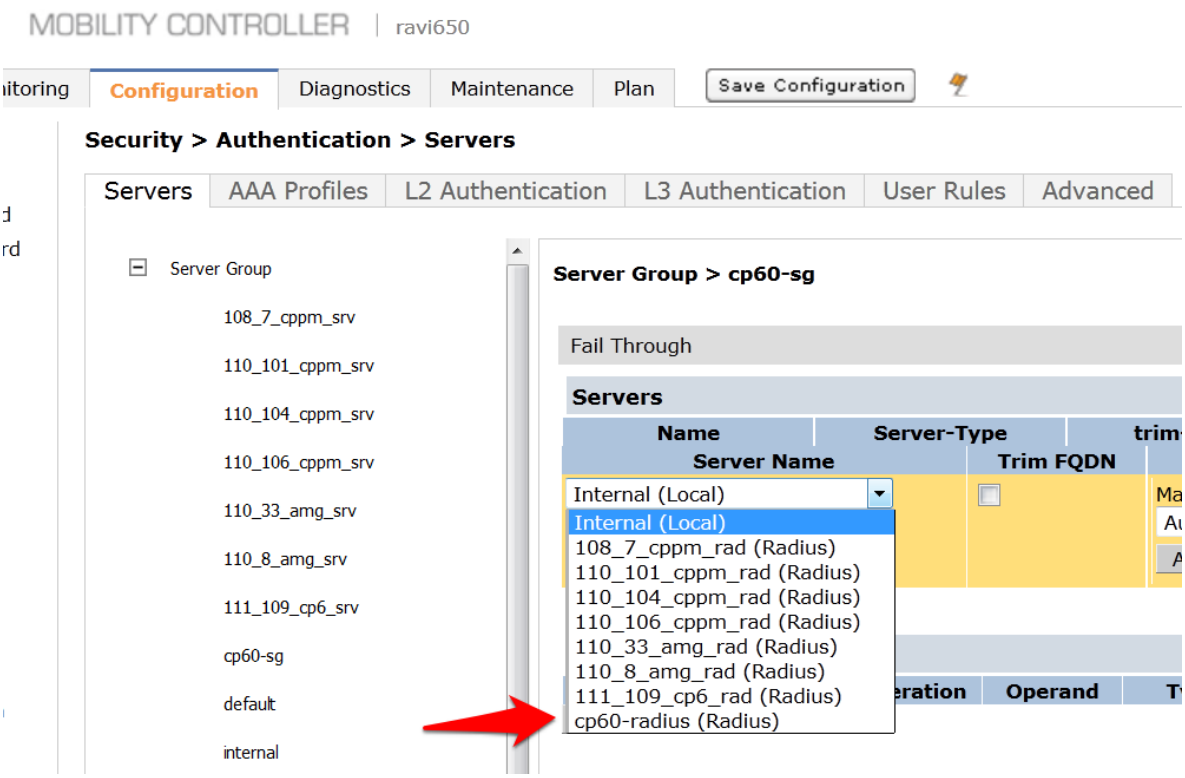
Enter the a reference name for your ClearPass Server Group in the empty box and click **Add**.



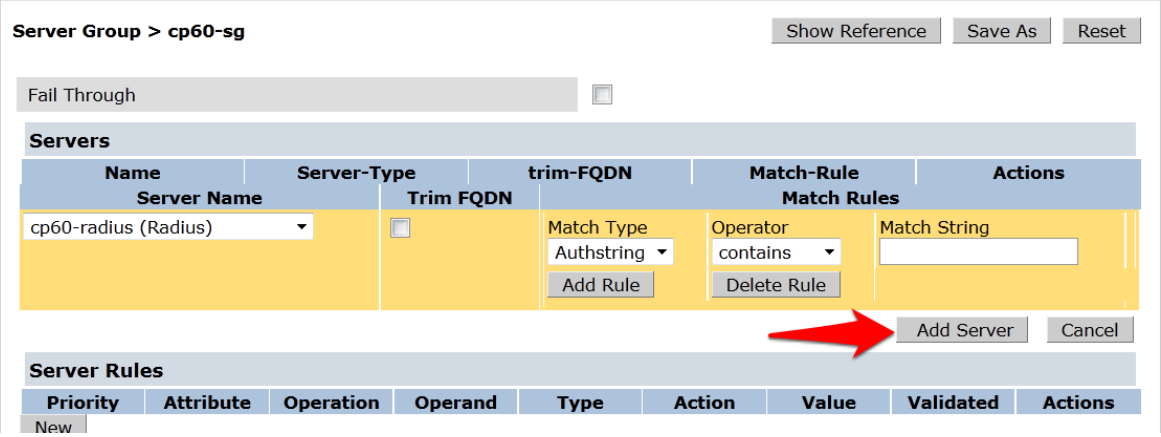
Select the newly created Server Group on the right under Server Group:



Click **New** and select the ClearPass RADIUS server from the previous step.



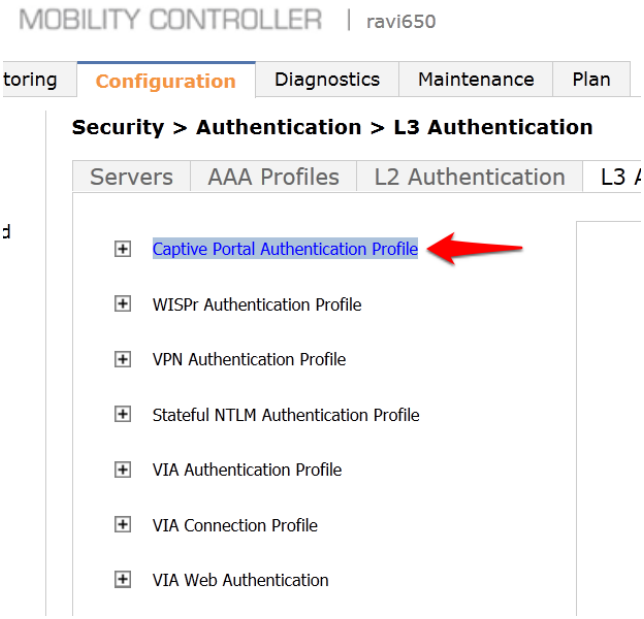
2. Click **Add Server**. Click **Apply** at the bottom of the page to save the changes.



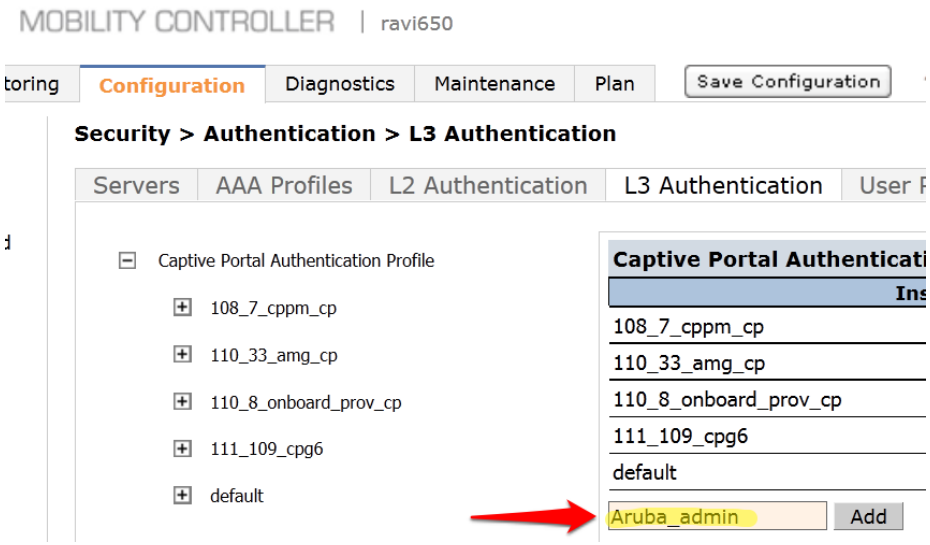
Captive Portal profile

Click on the **L3 Authentication tab**.

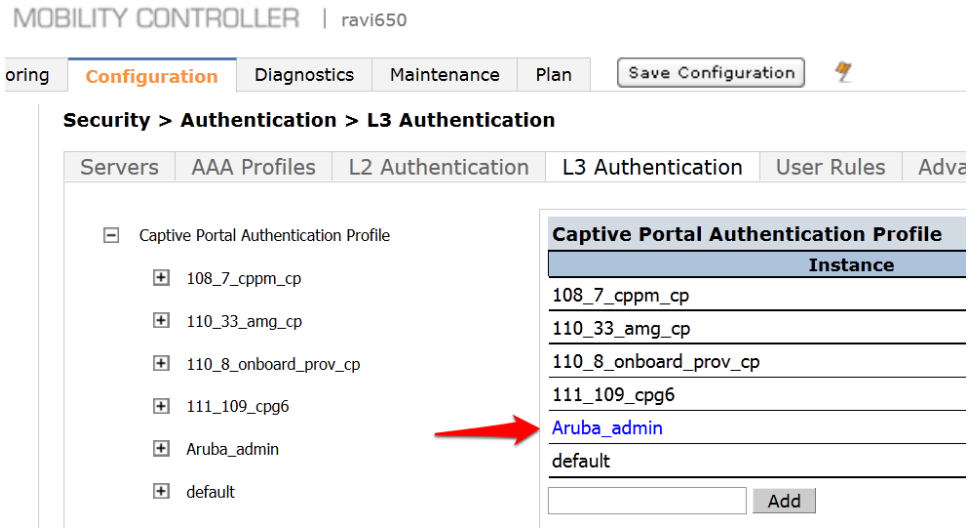
Click on **Captive Portal Authentication Profile**.



Enter a new Captive Portal profile name in the empty box and click **Add**.

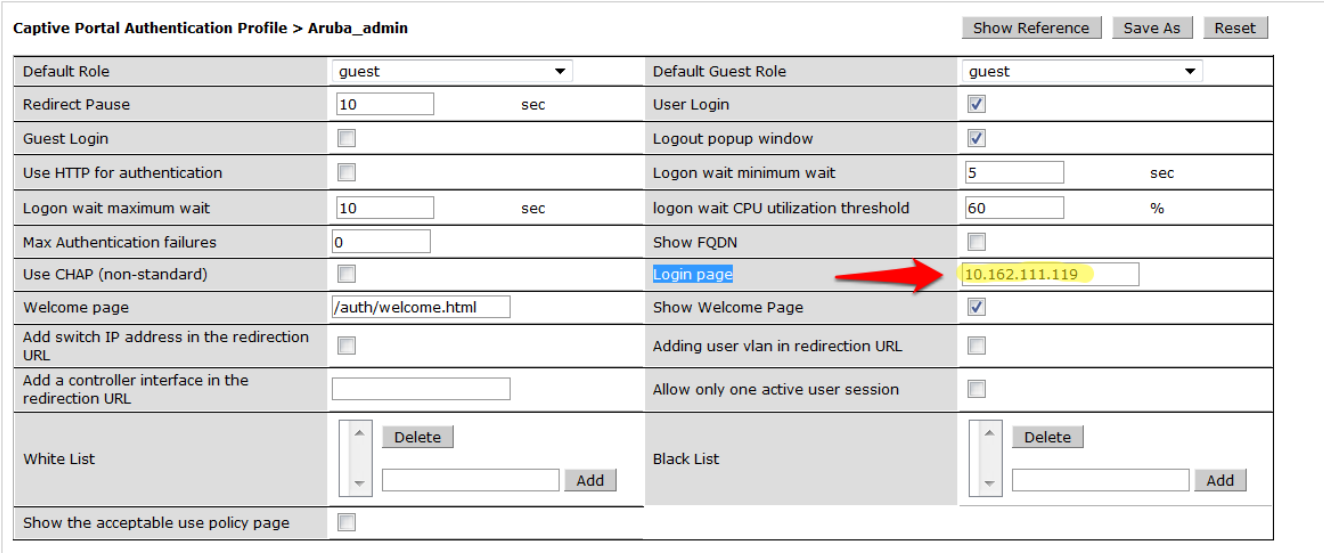


Select the newly created **Captive Portal Authentication Profile** under **Captive Portal Authentication Profile** on the right.



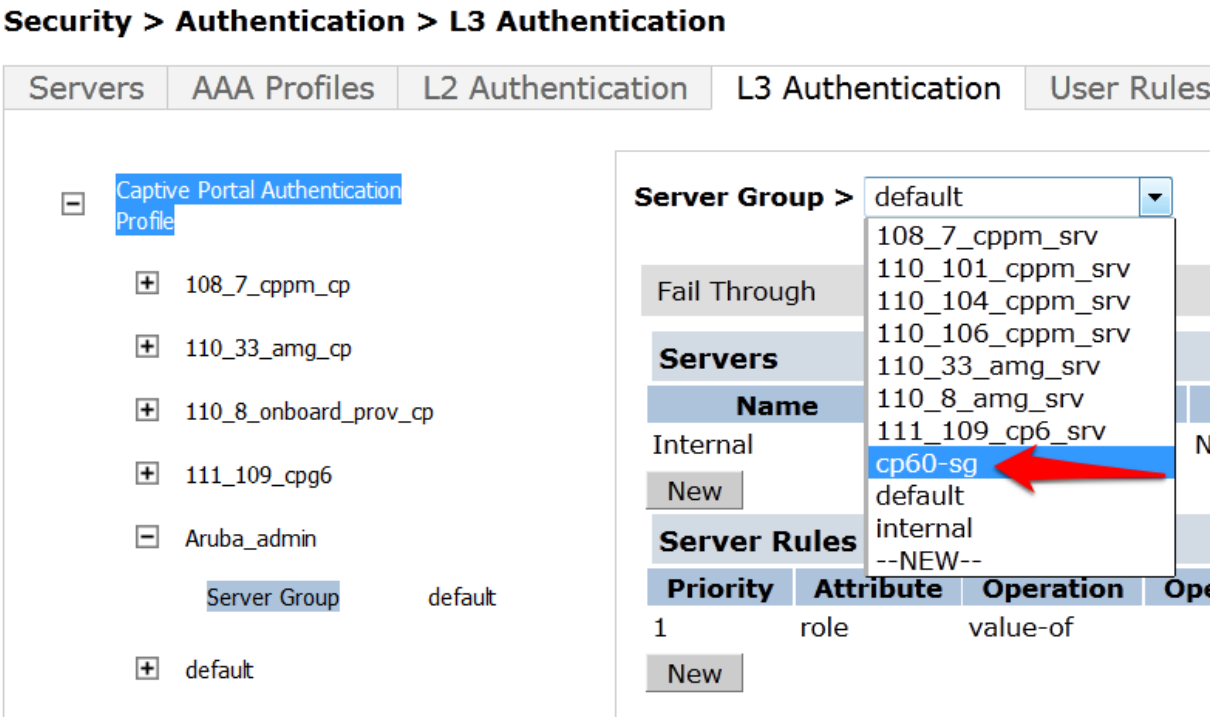
There are two things we need to change on this profile.

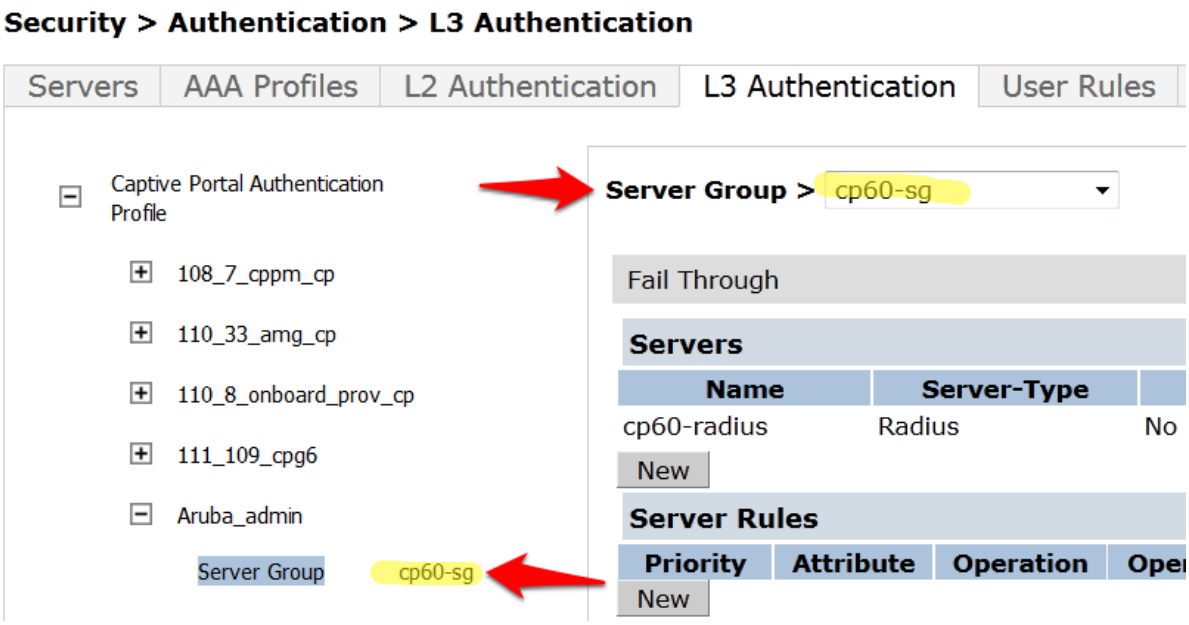
3. Change the **Login page** to http://10.1.1.20/guest/guest_register_login.php (replacing the 10.1.1.20 with the IP address of your ClearPass 6.0.1 server.



Click **Apply** at the bottom to save the changes.

4. Click on **Server Group** under the **Captive Portal Authentication Profile** and change the **Server Group** from **default** to the Server Group that you created for ClearPass in the previous steps and click **Apply** at the bottom of the page to save the changes.

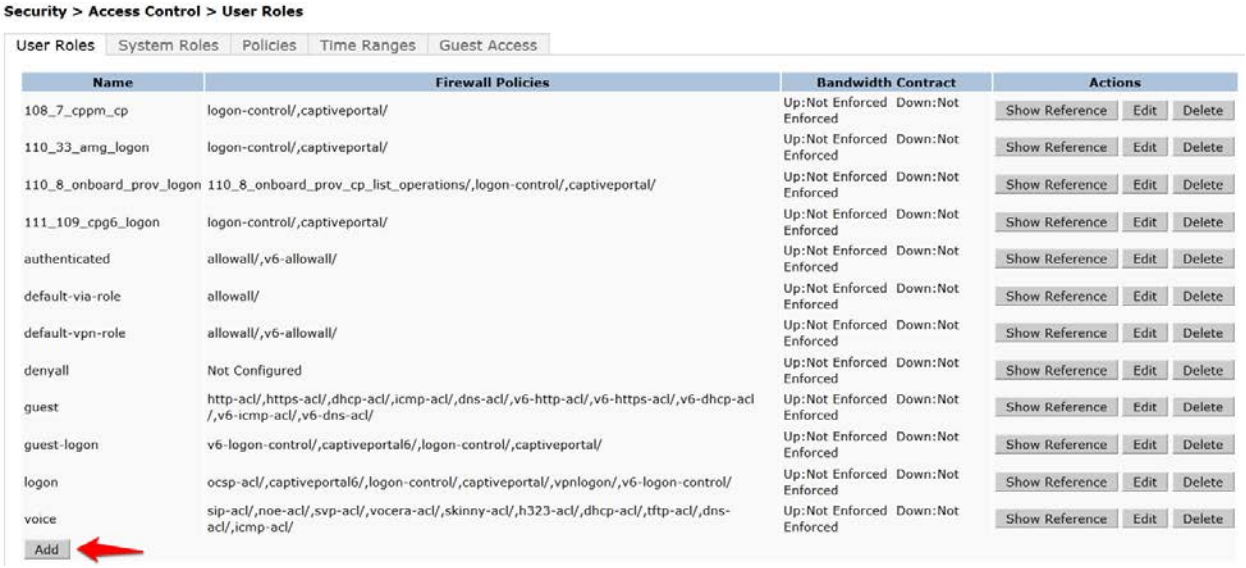




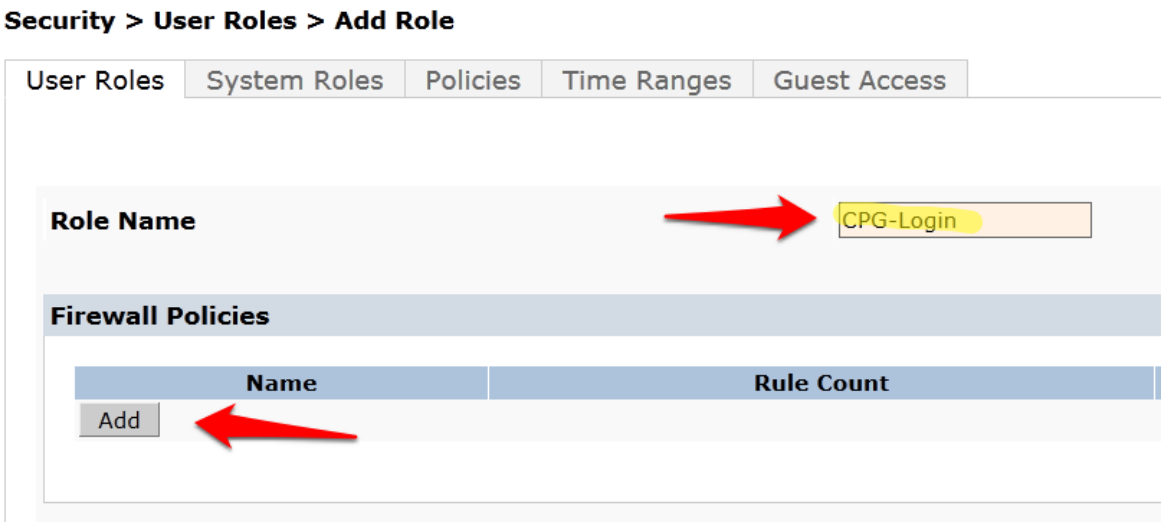
Create a Captive Portal role

Now we need to create our Captive Portal role, which is the role that clients will receive when they connect to the Guest SSID.

Navigate to **Configuration->Security->Access Control->User Roles** tab. Click **Add** to create a new User Role.

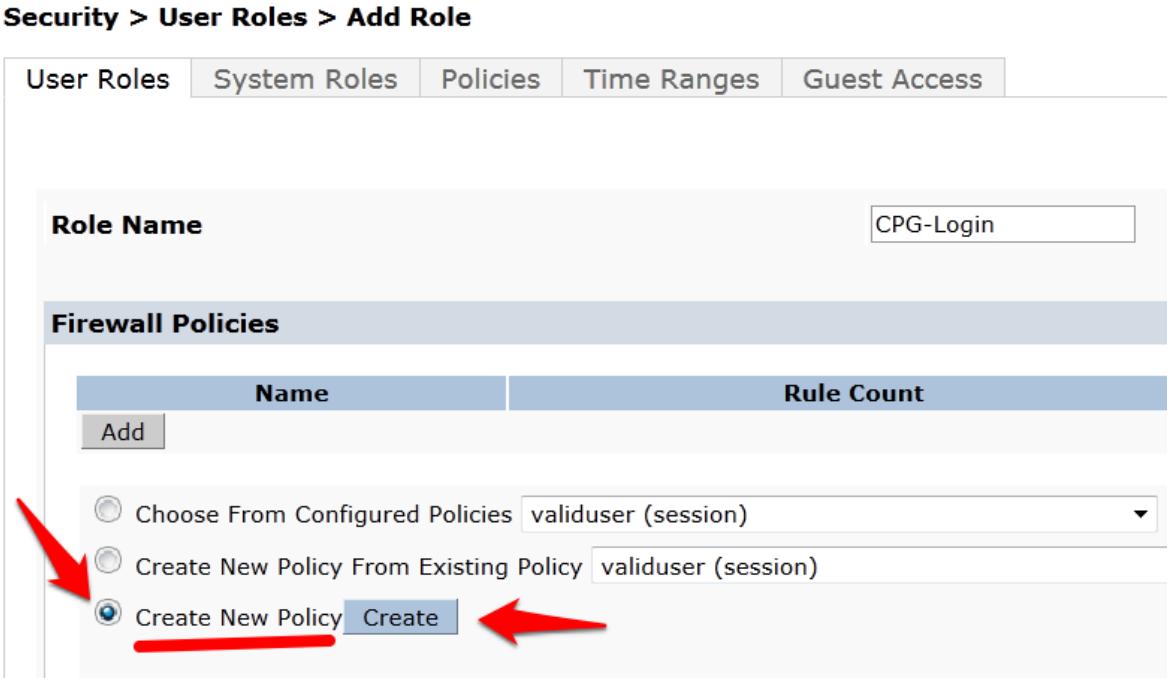


Enter a name like “CPG-Login” for the Role Name under **Firewall Policies**, Click **Add**.



For the first policy, it is essentially important that we add an ACL that will allow our Guest user to access ClearPass 6.0.1, which is where the Captive Portal webpage will be hosted.

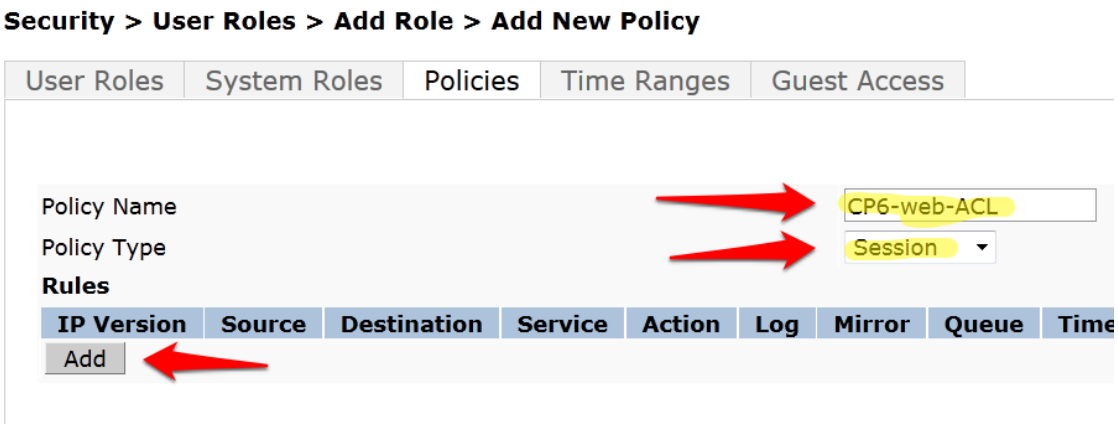
Choose the radio button for **Create New Policy**, and click the **Create** button:



Enter and select the following information:

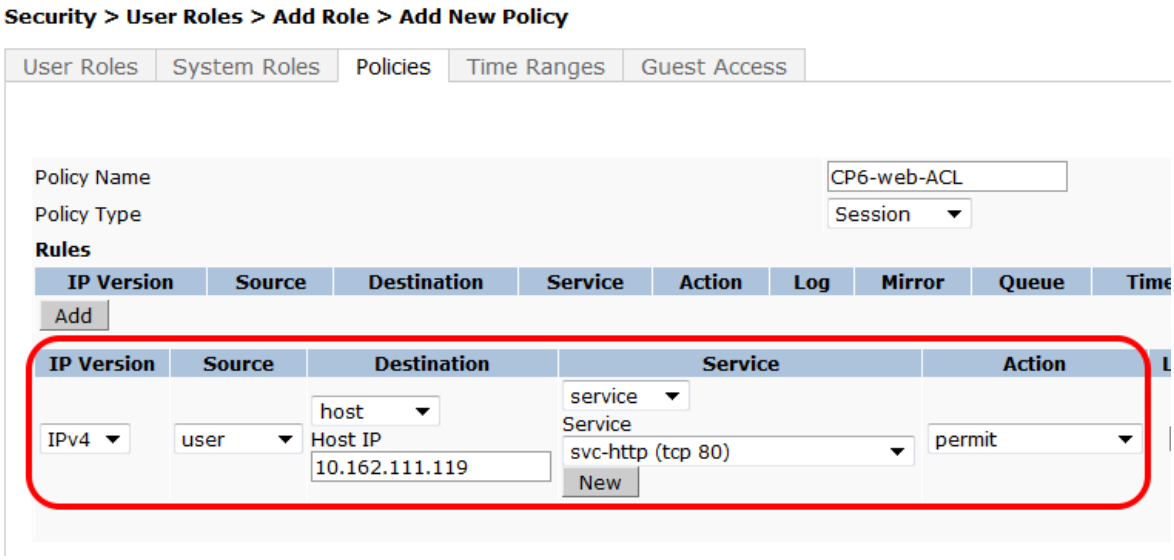
- **Policy Name**: "CP6-web-ACL"
- **Policy Type**: "Session"

Click **Add**.

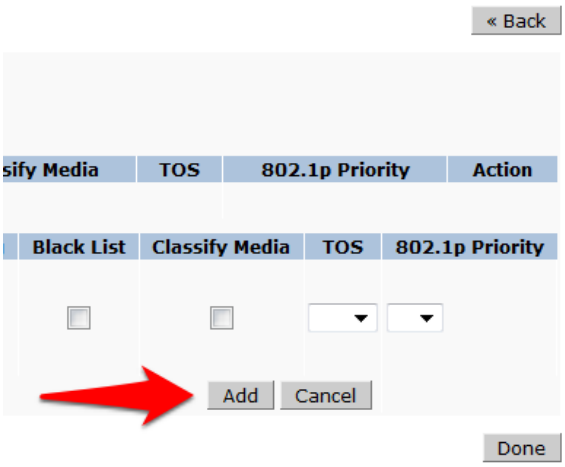


Select and enter the following information for the first line of the ACL:

- **IP Version**: “IPv4”
- **Source**: “User”
- **Destination**: host
  - **Host IP**: (the IP address of your ClearPass server)
- **Service**: “service”
  - **Service**: “svc-http (tcp 80)”
- **Action**: “permit”

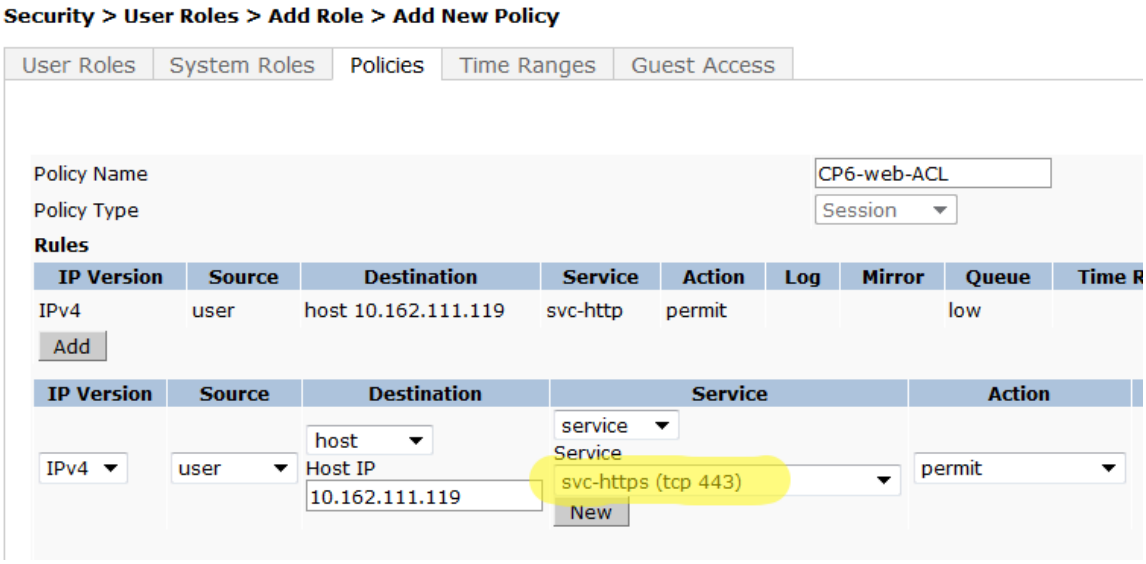


Click **Add** at the far right underneath this rule.

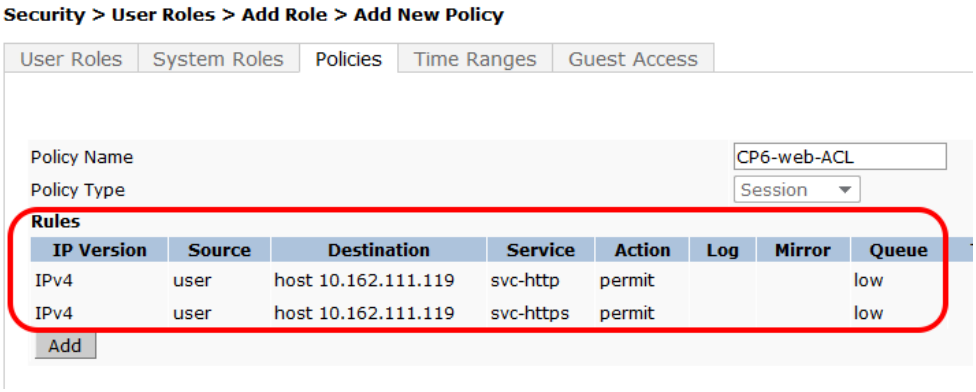


Click **Add** again to add another line to this ACL, identical to the previous line except:

Choose **Service**: "svc-https (tcp 443)"

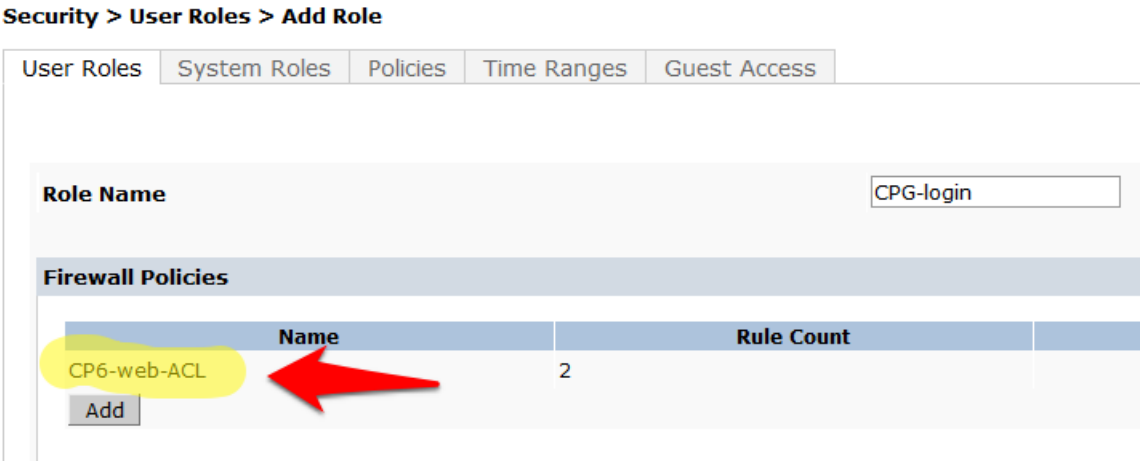


Click **Add** at the far right underneath this rule.



Click **Done**

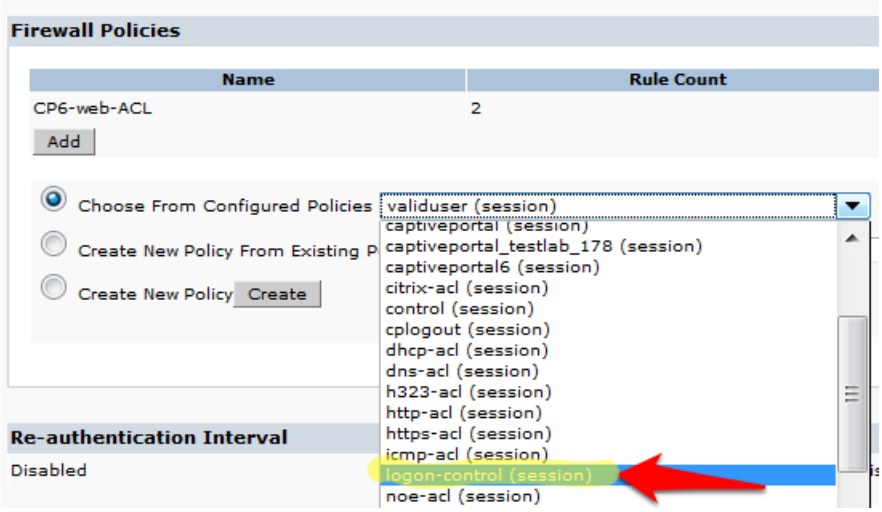
You will be brought back to the Add Role page where you were creating your CPG-Login User Role.



Step 4: Pre-configured Firewall Policies

The Firewall Policy that you just created has been added to the list. Now we need to add two more pre-configured Firewall Policies.

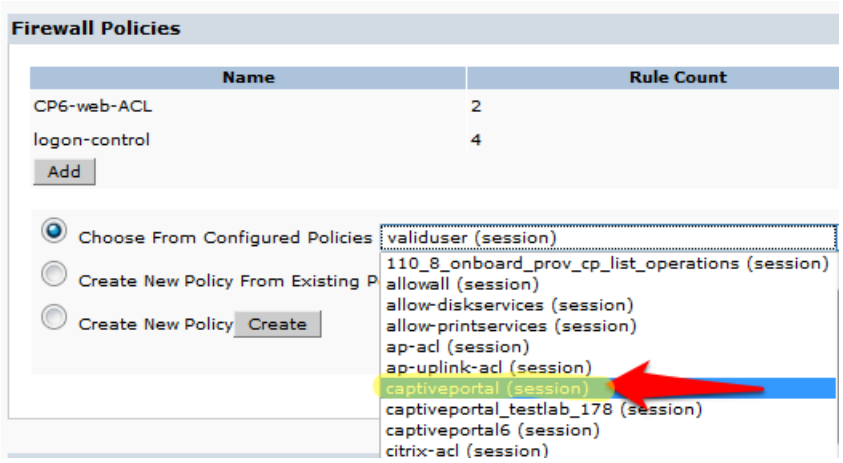
Click **Add** under **Firewall Policies**. Select the radio button for “Choose From Configured Policies” and select the policy called “logon-control (session)”.



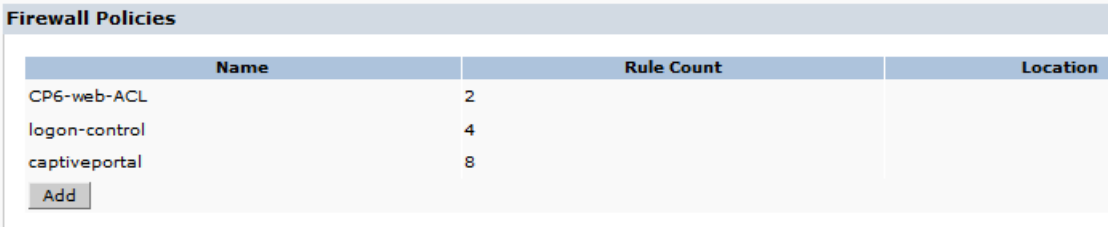
Click **Done** in the **Firewall Policies** section.

Click **Add** again in the **Firewall Policies** section.

Select the radio button for “Choose From Configured Policies” and select the policy called “captiveportal (session)”.



Click **Done** in the **Firewall Policies** section. Your Firewall Policy should look like this:



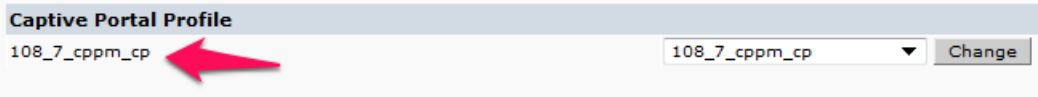
NOTE: The Firewall policy order **MUST** place "captive portal" at the **bottom** of the list!

Scroll down this page to the **Captive Portal Profile** section.

Select the previously configured Captive Portal Profile from the drop-down list.

Click the **Change** button.

Verify that the "Not Assigned" has changed to the name of your Captive Portal Profile.



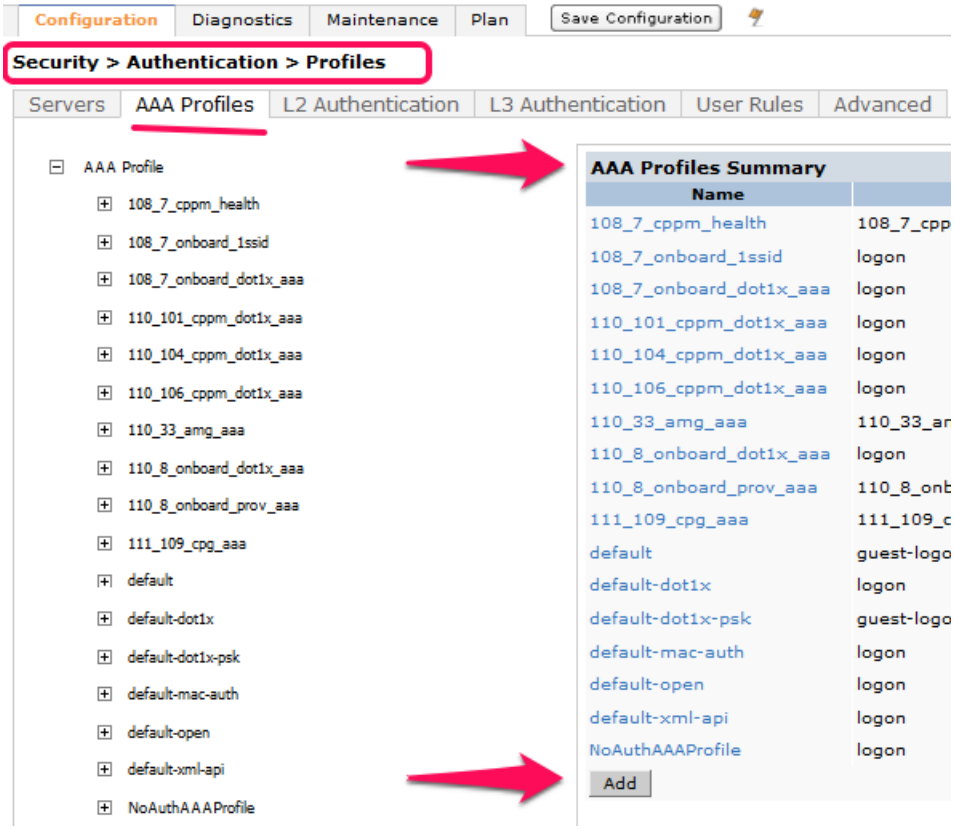
Click **Apply** at the bottom of the page to save the newly created User Role.

Step 5: Creating AAA Profiles for the ClearPass Guest and 802.1x SSID

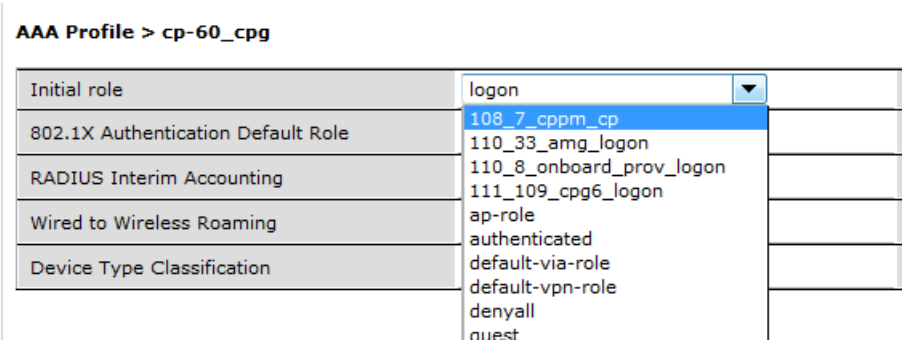
The next step is to create AAA Profiles for the ClearPass Guest and 802.1x SSID.

Navigate to **Configuration->Security->Authentication->AAA Profiles tab**.

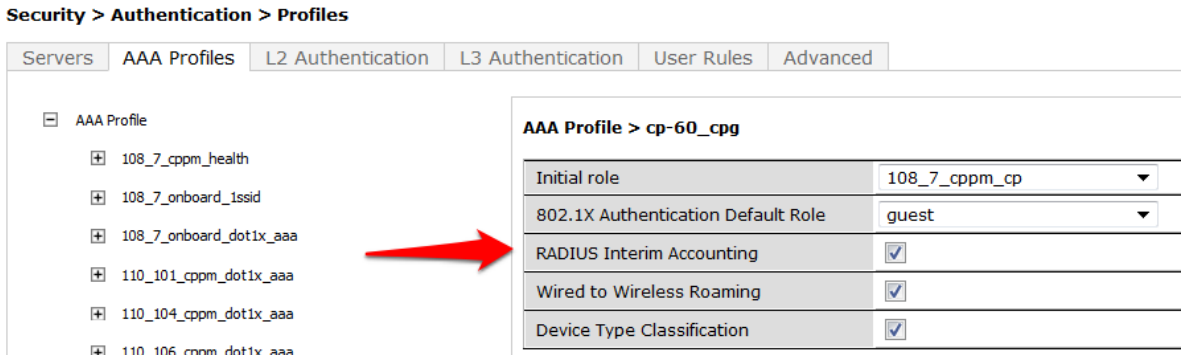
Click **Add**, enter a name for the ClearPass Guest Profile, and then click **Add** again.



Now in the left column, click on the new profile that you just created. Change the Initial role to the role that you created in the previous step.



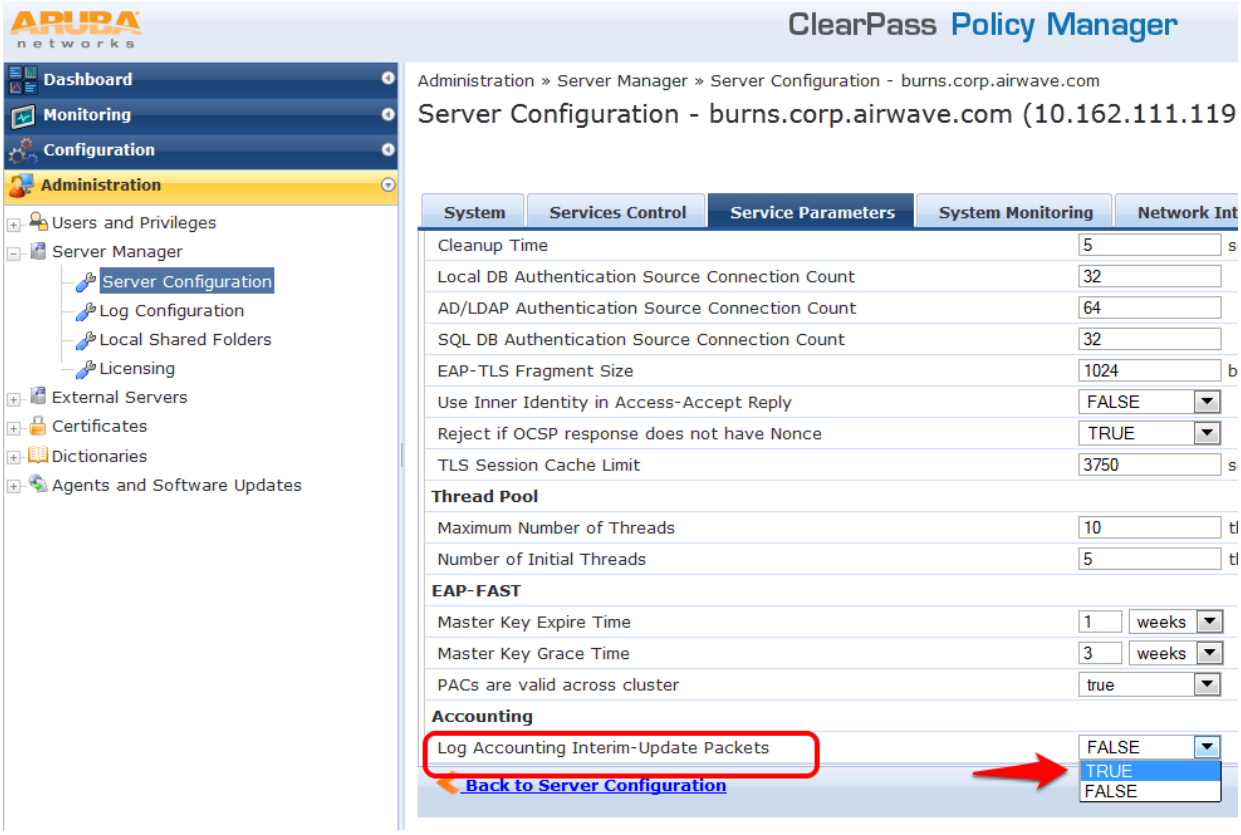
Tech Tip: On this page you will see an option for "RADIUS Interim Accounting". This should be checked <u>if you want live utilization updates in ClearPass</u>, usually used to control guest users based on Bandwidth Utilization.



This also needs to be enabled on ClearPass.

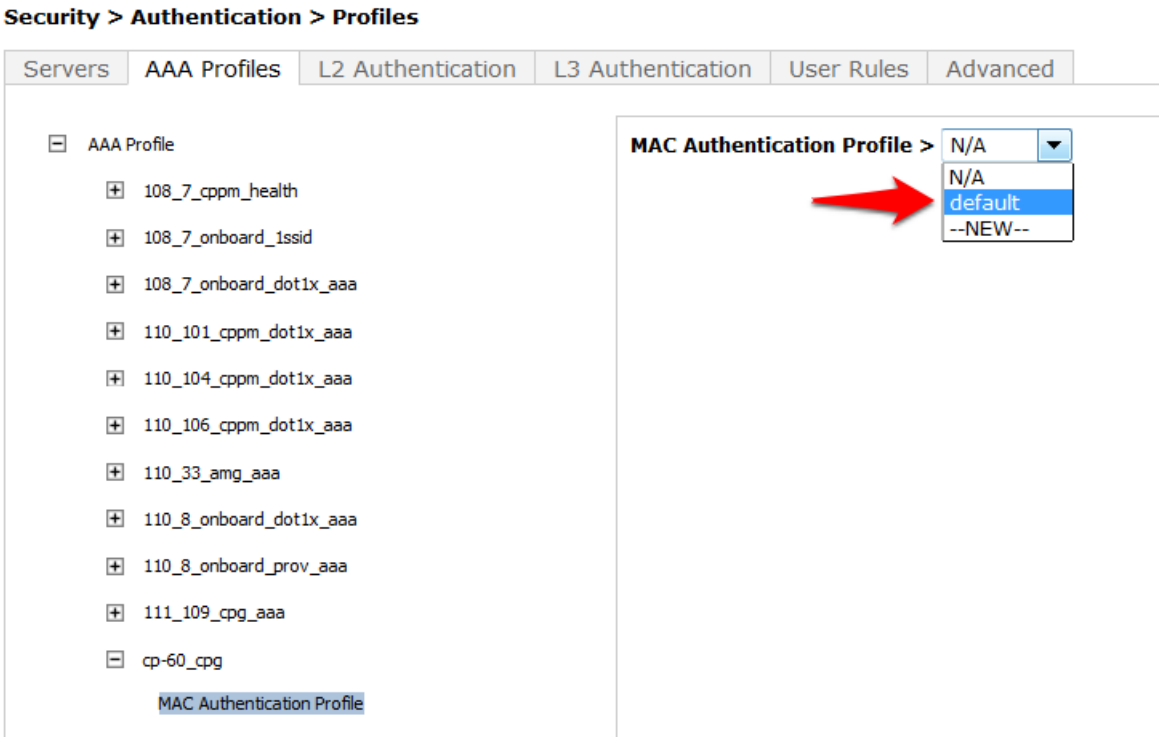
In ClearPass Policy Manager, navigate to:

Administration->Server Manager->Server Configuration->Select Server->Service Parameters->RADIUS Server->Log Accounting Interim-Update Packets="TRUE".

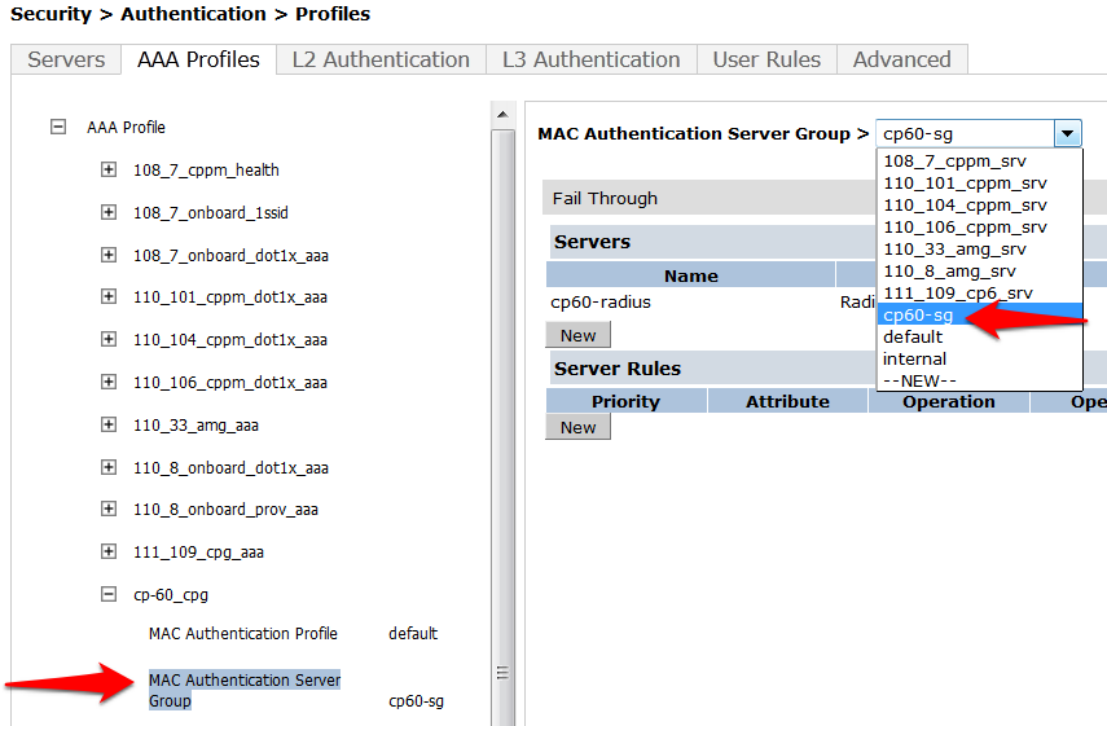


Set the subsections of the profile as described below, clicking **Apply** after each change:

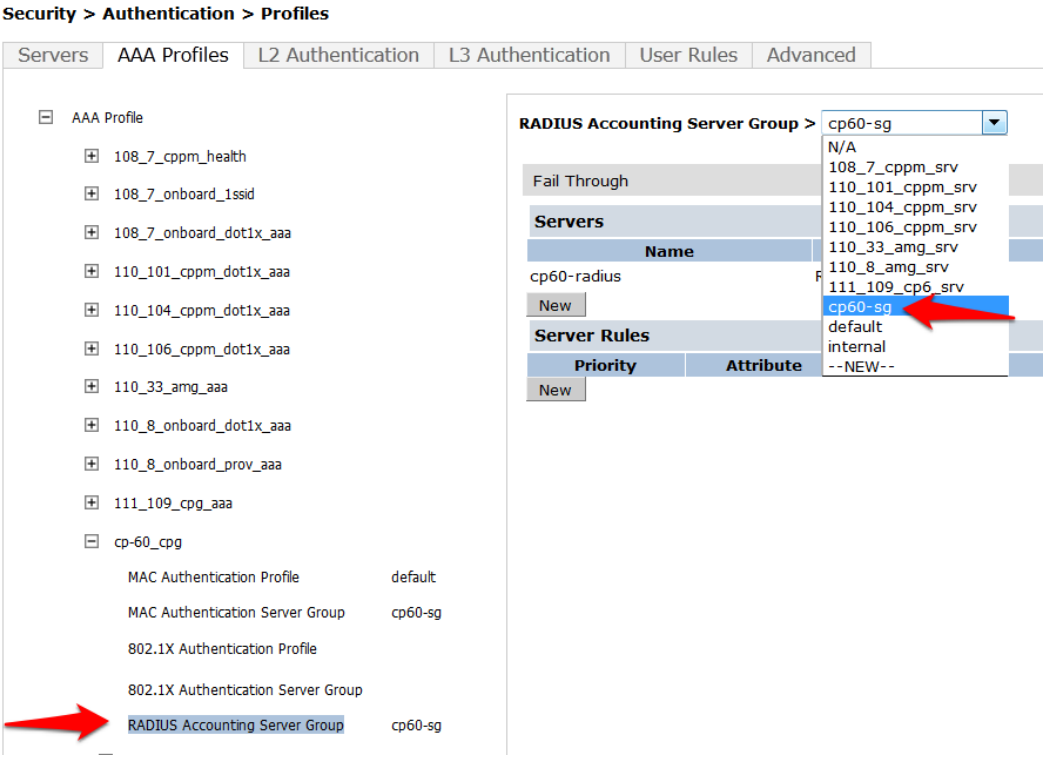
MAC Authentication Profile: "default"



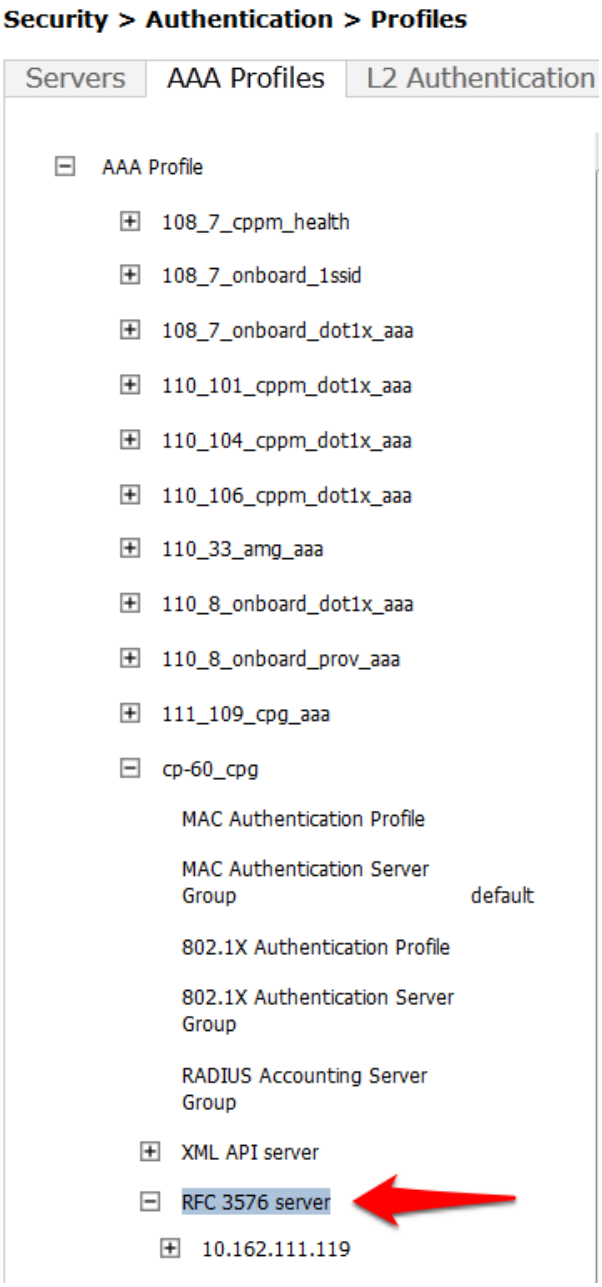
MAC Authentication Server Group: (*Your ClearPass 6.0.1 Server Group*)



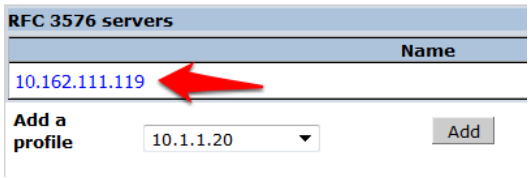
RADIUS Accounting Server Group: (*Your ClearPass 6.0.1 Server Group*)



Click on **RFC 3576** for this AAA Profile.



From the **Add a profile** list, select the IP address of your ClearPass server and click the **Add** button.



Click **Apply** to save these settings.

Repeat Creating AAA Profiles for the ClearPass Guest and 802.1x SSID, page 19, to create the AAA Profile for the 802.1x SSID. The only difference is that this AAA Profile will have 802.1x settings but no MAC Authentication Profile. See example below:

AAA Profile

cp60-AAA

cp60-dot1x-aaa

MAC Authentication Profile

MAC Authentication Server Group default

802.1X Authentication Profile default

802.1X Authentication Server Group cp60-sg

RADIUS Accounting Server Group

XML API server

RFC 3576 server

10.162.110.103

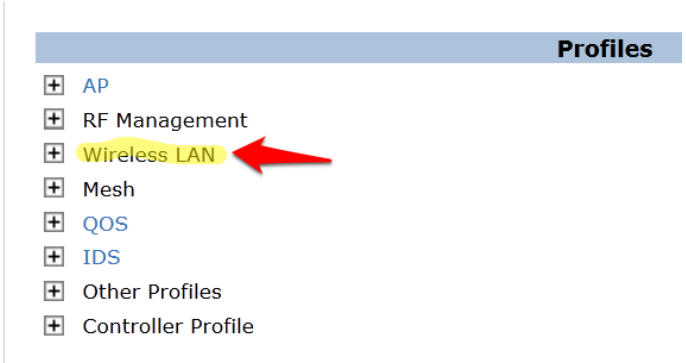
Step 6: Associating a 802.1x SSID and Guest SSID with AAA Profiles

The next step is to associate our 802.1x SSID and Guest SSID with the AAA Profiles we just created.

Navigate to **Configuration->Advanced Services->All Profiles**.

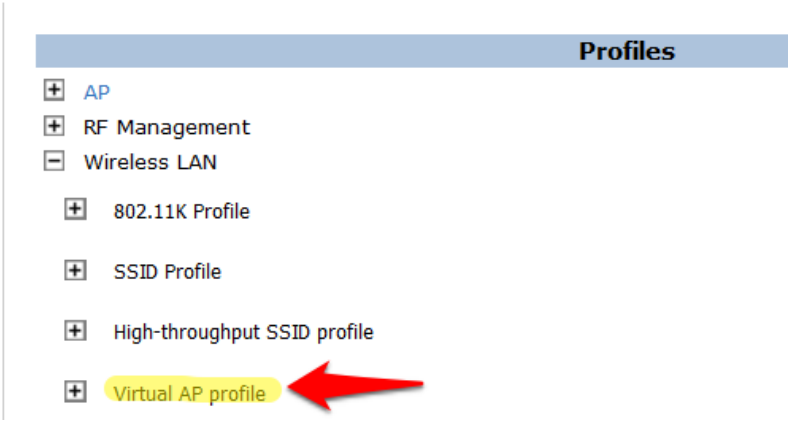
Expand the **Wireless LAN** section.

Advanced Services > All Profile Management

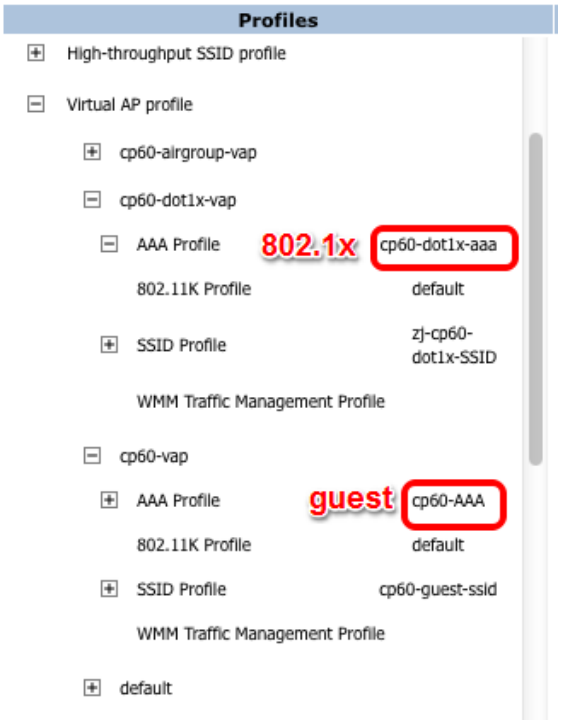


Expand the **Virtual AP profile** and locate your Guest and 802.1x SSID profiles.

Advanced Services > All Profile Management



Modify each Virtual AP profile to use the appropriate AAA Profile that you created in the previous section.



Make sure to click **Apply** after each change.

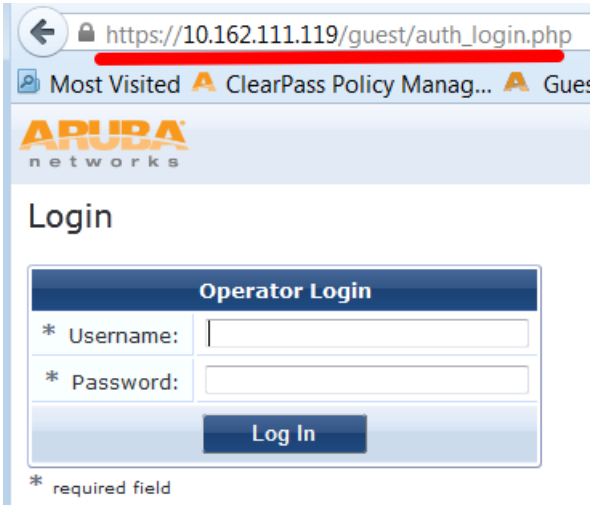
Click the **Save Configuration** button at the top of the page once the changes are completed.

Step 7: ClearPass Guest Setup

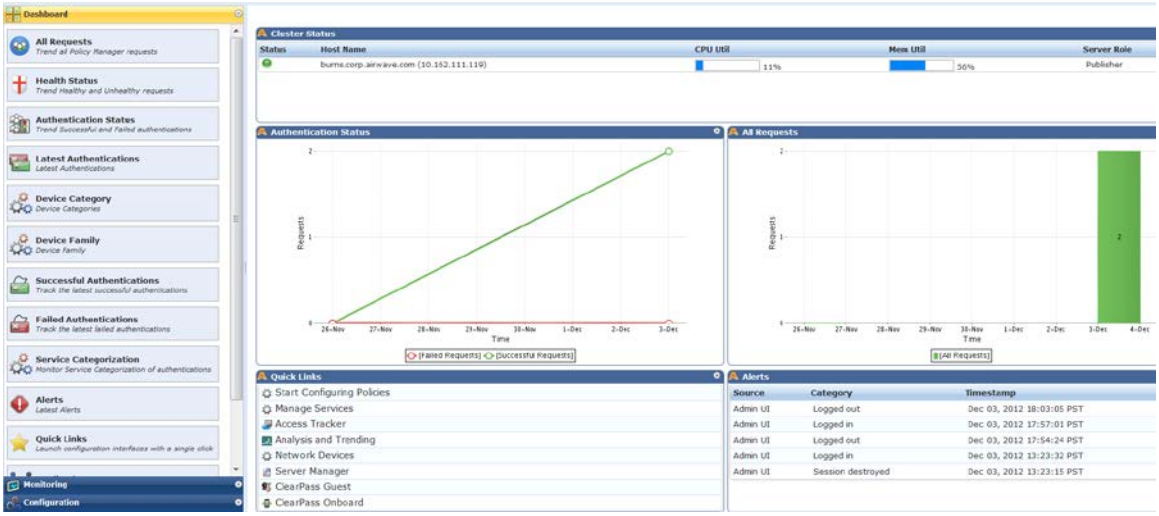
In this step we will configure basic Guest Registration and Login.

Basic Guest Registration and Login configuration

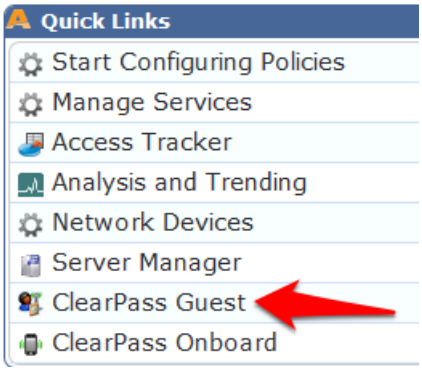
Log into ClearPass Policy Manager (https://your-cp-ip-here/tips).



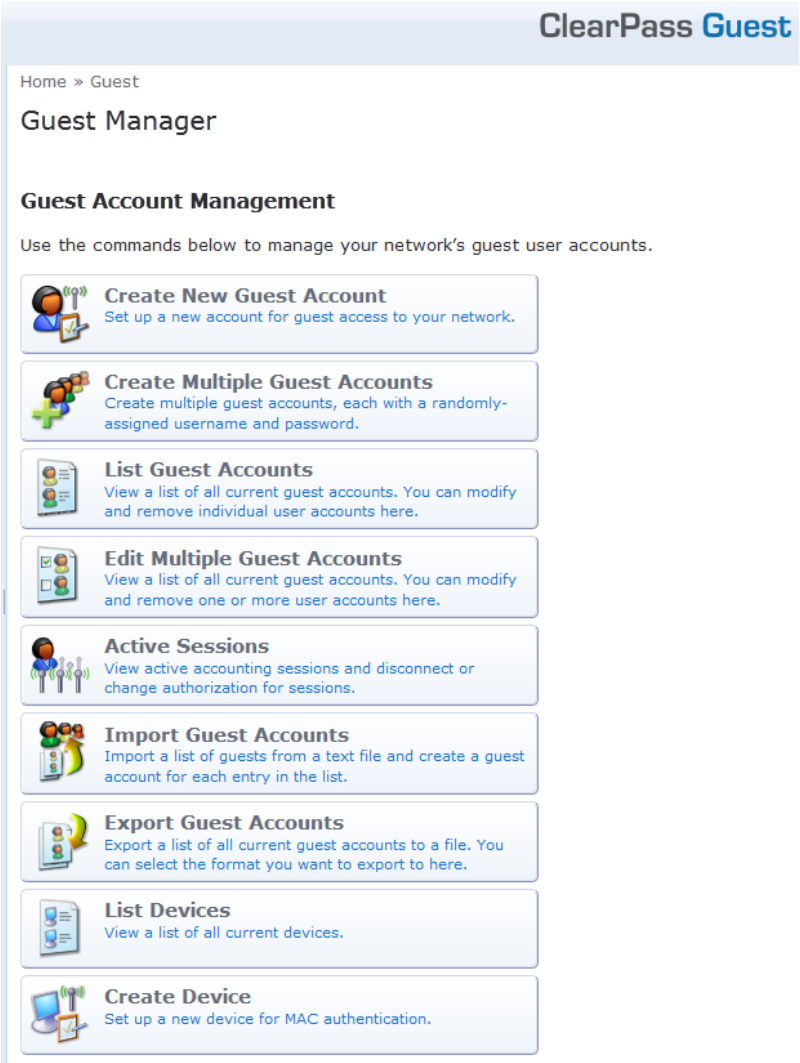
After you login, you will see the ClearPass Policy Manager Dashboard.



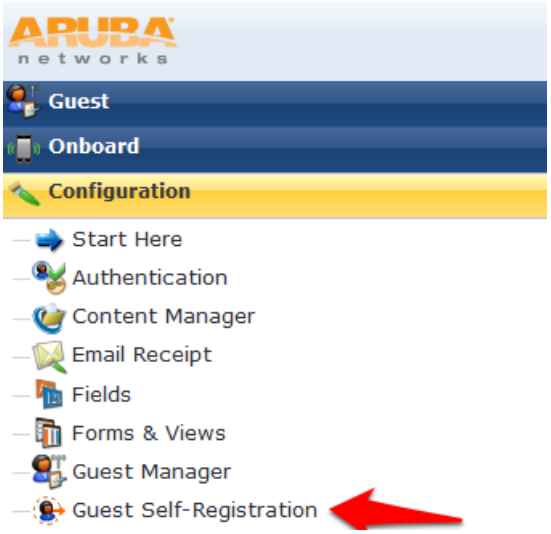
One of the Dashboard objects is Quick Links. Click on the quick link for ClearPass Guest



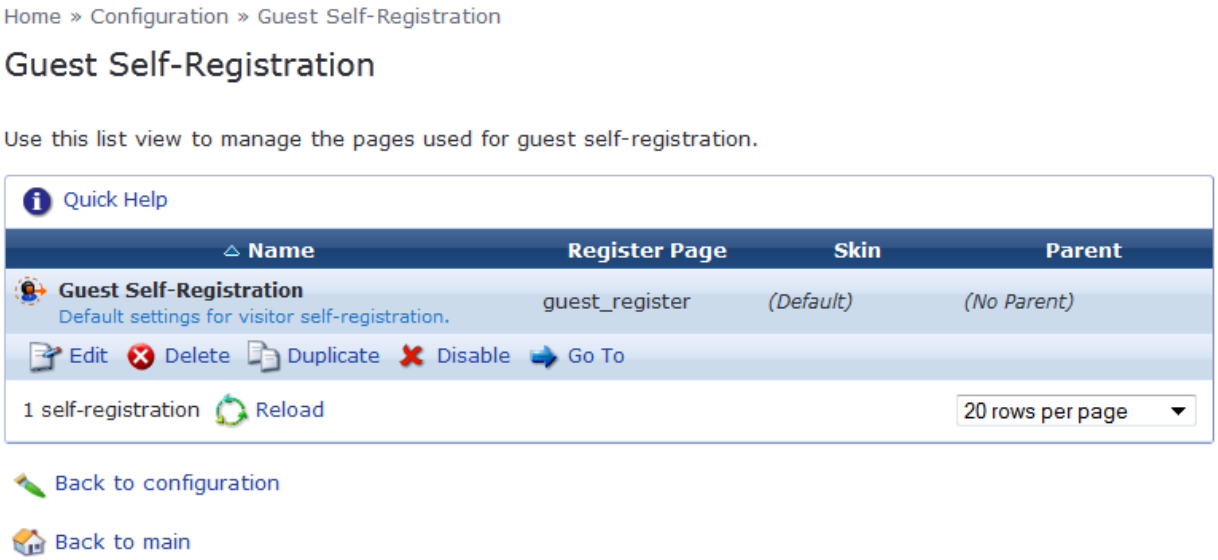
Clicking this link will automatically log you into the ClearPass Guest administration page. Alternatively you could enter the url for the Guest page (https://your-cp-ip-here/guest).



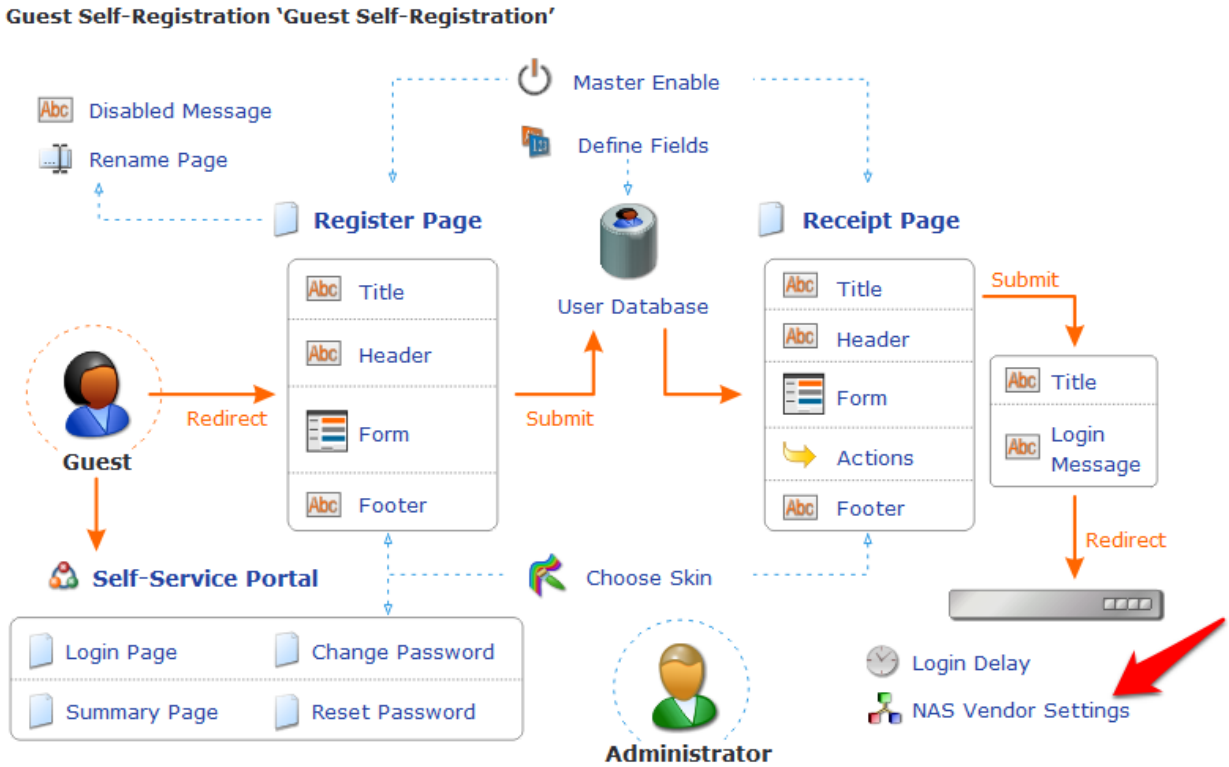
Navigate to **Configuration->Guest Self-Registration**.



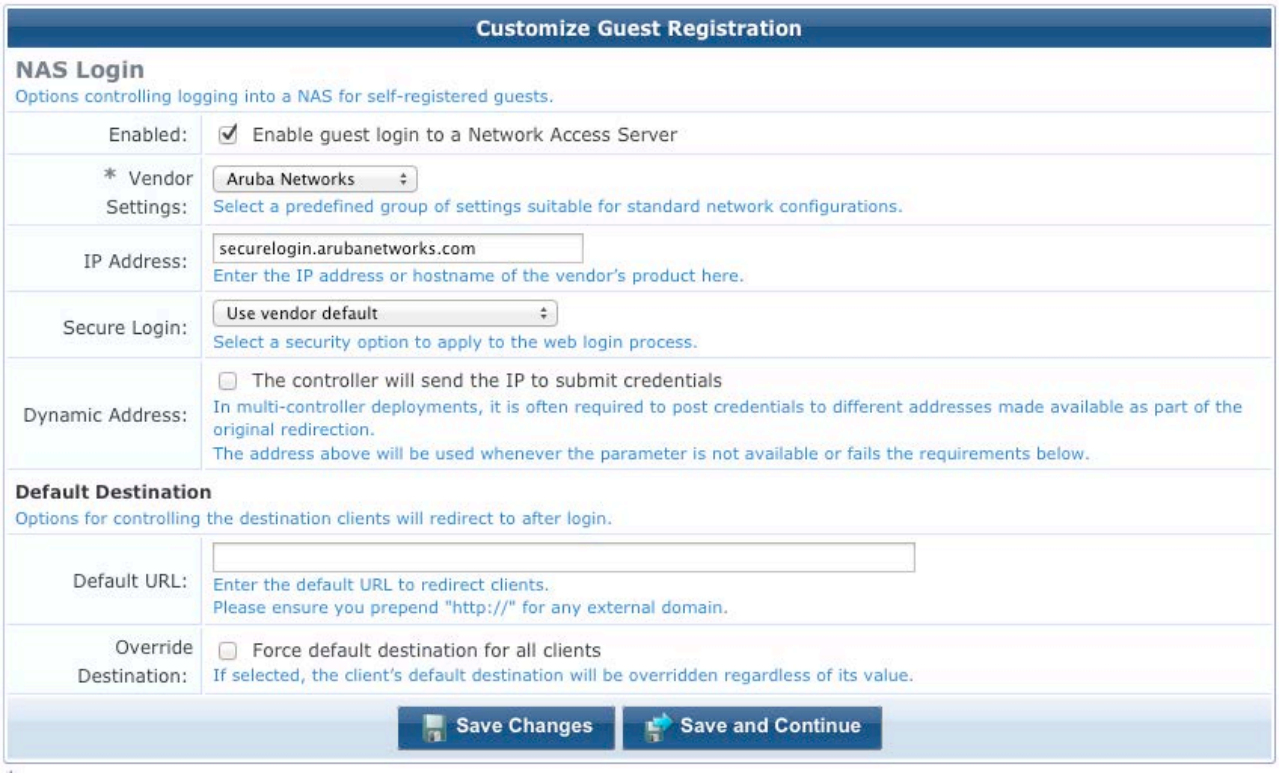
Click on the preconfigured **Guest Self-Registration** profile. This will reveal several options. Click **Edit**.



In this guest registration profile, it is necessary to enable web login. Click **NAS Vendor Settings** from the edit diagram:



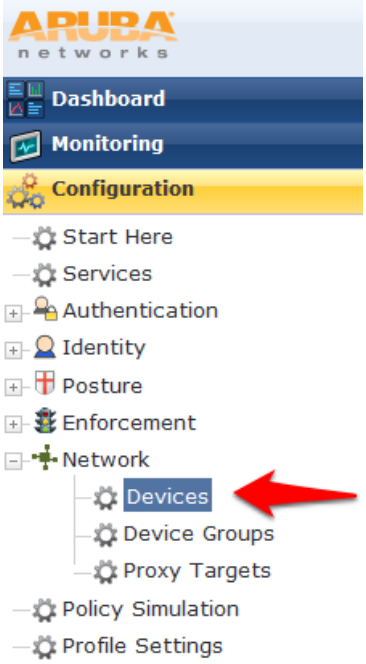
On the **NAS Login** settings page, check the checkbox to "Enable guest login to a Network Access Server." It will prepopulate the settings with Aruba Networks NAS settings.



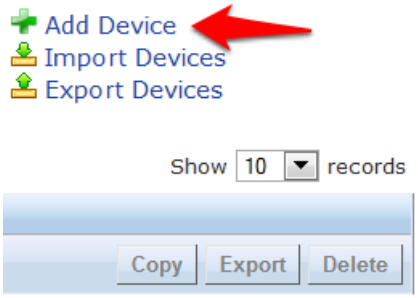
Click **Save Changes.**

2. ClearPass Policy Manager Setup

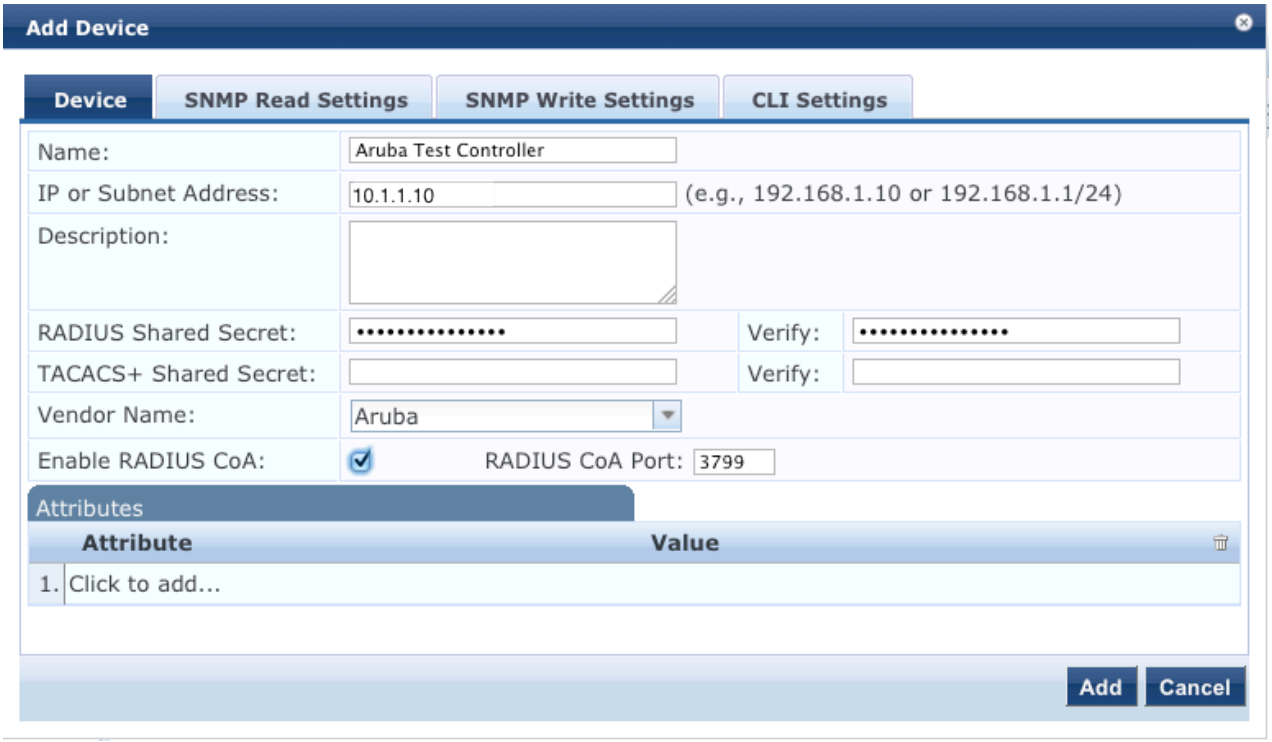
In ClearPass Policy Manager, navigate to **Configuration->Network->Devices**.



Click **Add Device** in the top right corner of the page.

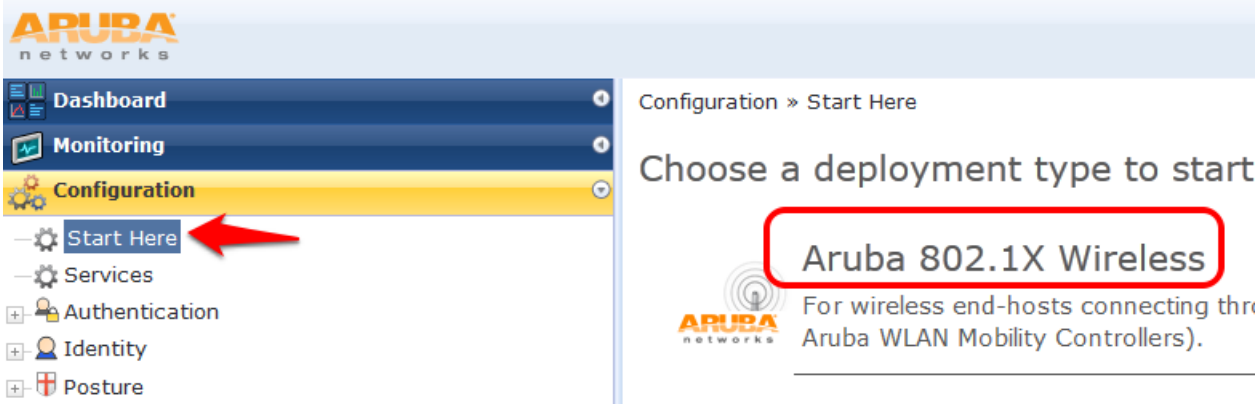


Enter a **Name** and the **IP or Subnet address** for your Wireless Controller. For the RADIUS Shared Secret, enter aruba123 (the same shared secret we used in the Controller setup for RADIUS and RFC 3576). Select “Aruba” as the **Vendor Name**, and check the box to “**Enable RADIUS CoA:**”

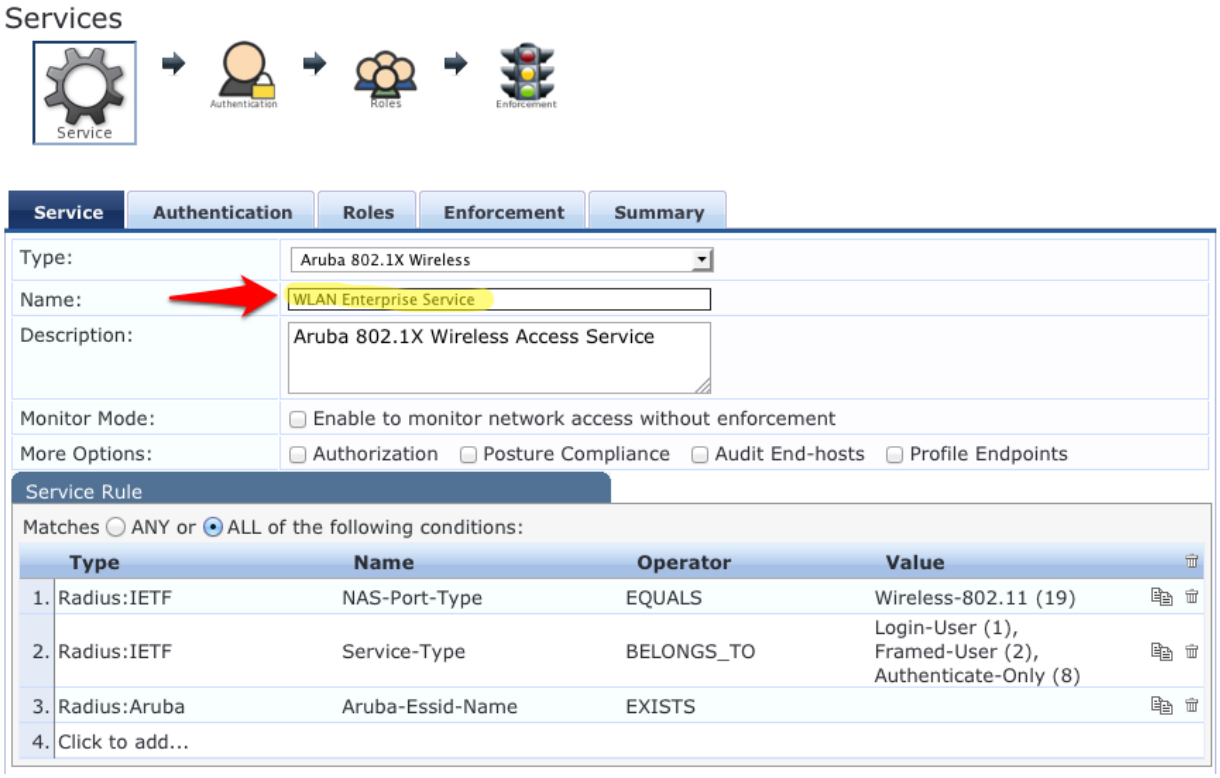


Click **Add**.

Navigate to **Configuration->Start Here** and select Aruba 802.1X Wireless.

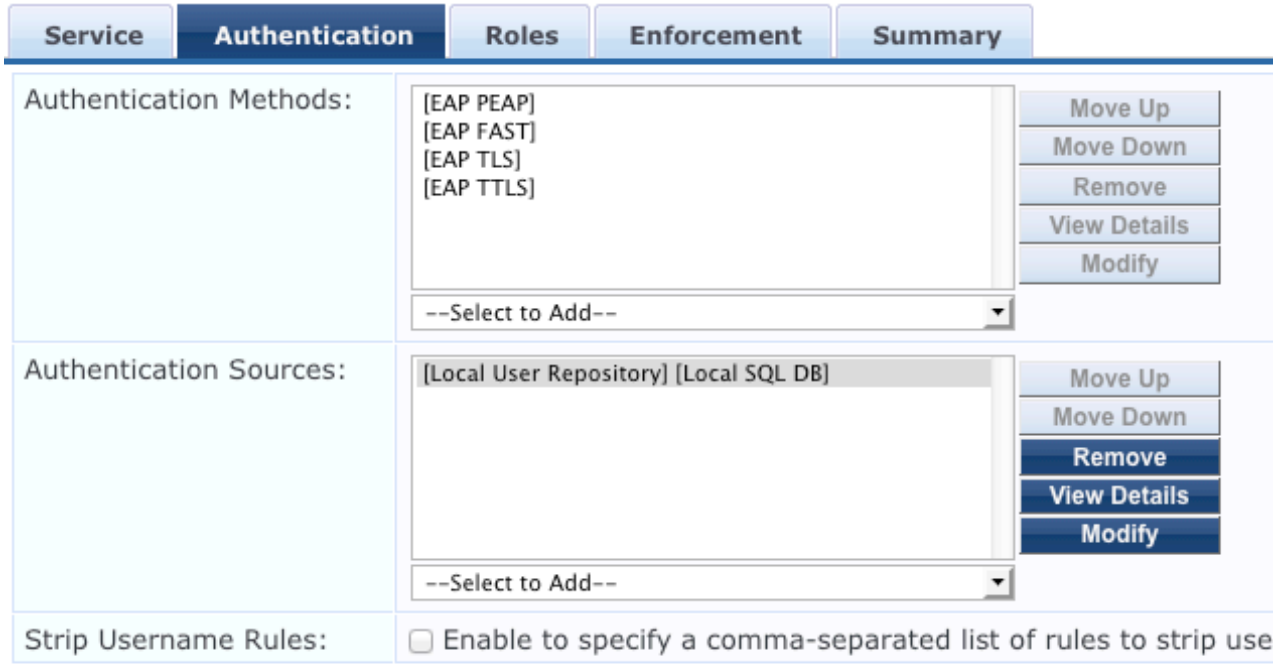


Give the service a name such as “WLAN Enterprise Service”.



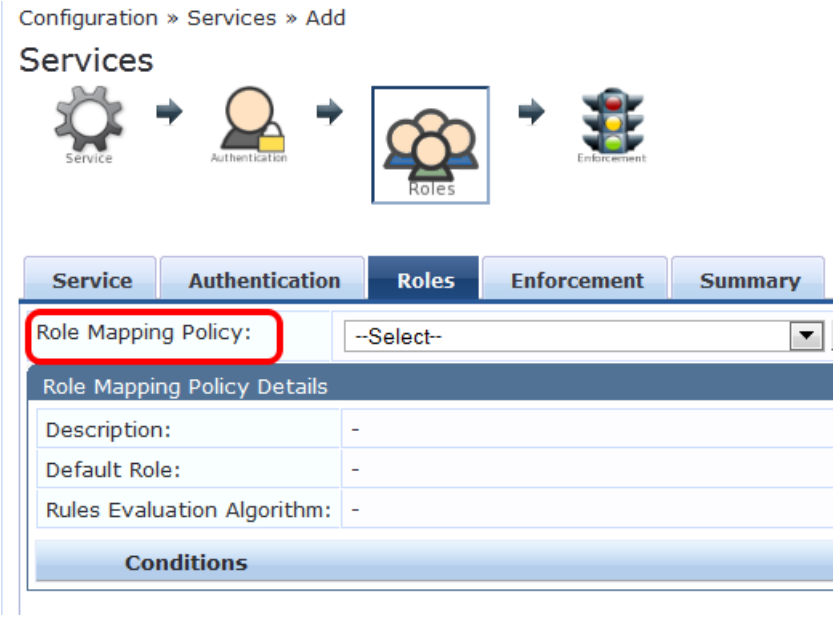
Click **Next**.

On the **Authentication** tab, Click the “Select to Add” down arrow and choose “[Local User Repository] [Local SQL DB]” as the “Authentication Sources”.

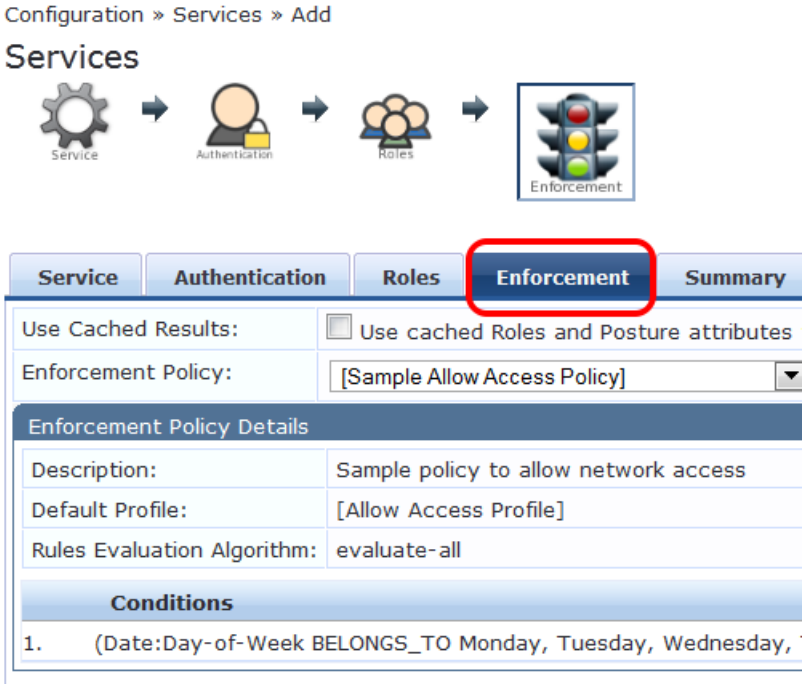


Click **Next**.

For initial testing, **Role mapping Policy** <u>will not</u> be used. Click **Next** on the **Roles** tab at the bottom right corner of the page to continue.



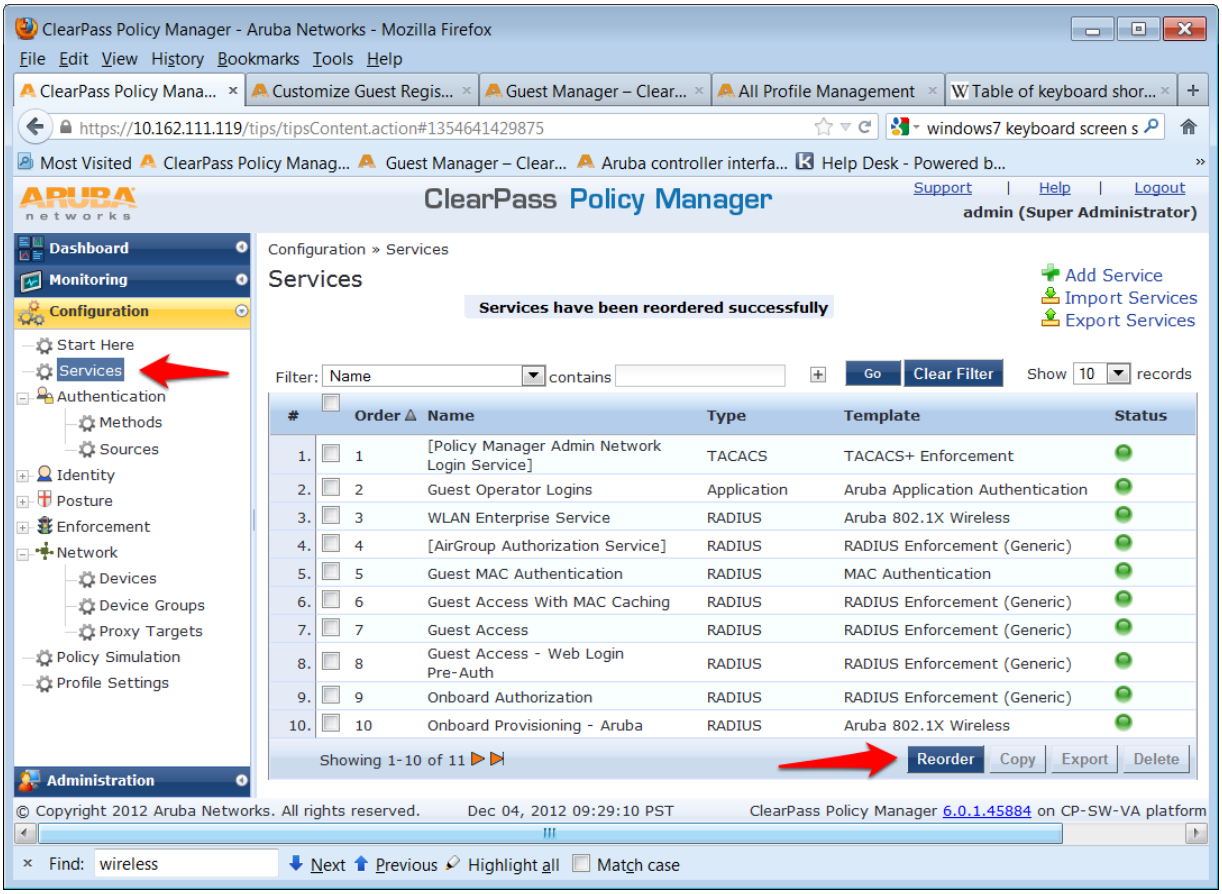
On the **Enforcement tab**, no changes are necessary. Click **Next** at the bottom right corner of the page to continue.



Review the summary and click **Save**.

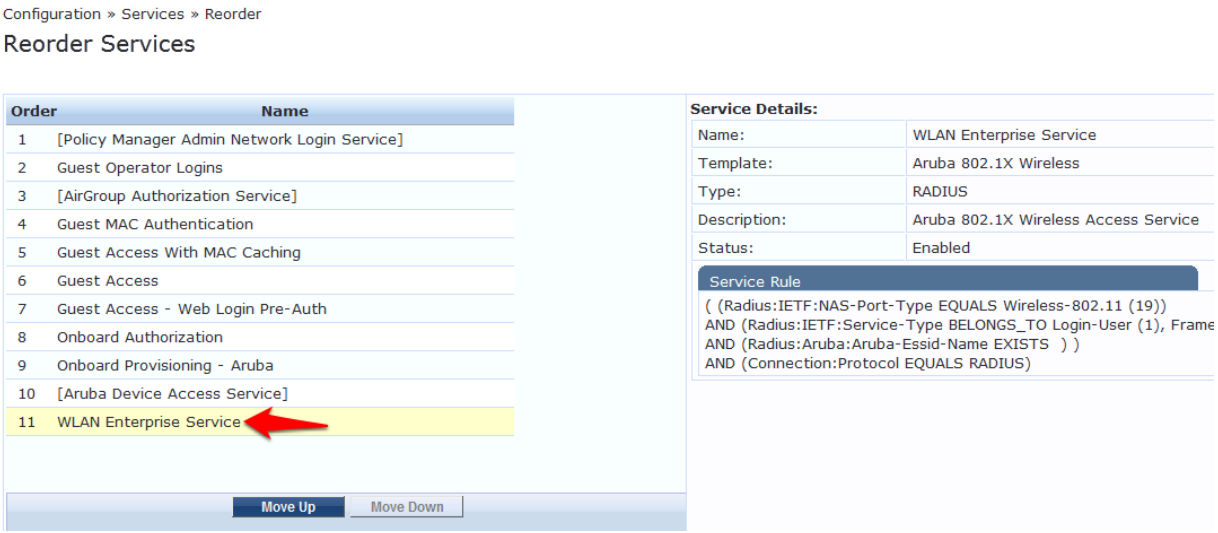
Important! You must move the WLAN Enterprise Service above any generic RADIUS services that are not filtering via service rules. ClearPass 6.0.1 does not ship with any generic RADIUS services that have no service rules.

Navigate to **Configuration->Services** and select **Reorder** to move "WLAN Enterprise Service" above ANY generic RADIUS services that are not filtering via service rules.



Select ”WLAN Enterprise Service” and click on the **Move up** button to position ” above ANY generic RADIUS services that <u>are not</u> filtering via service rules.

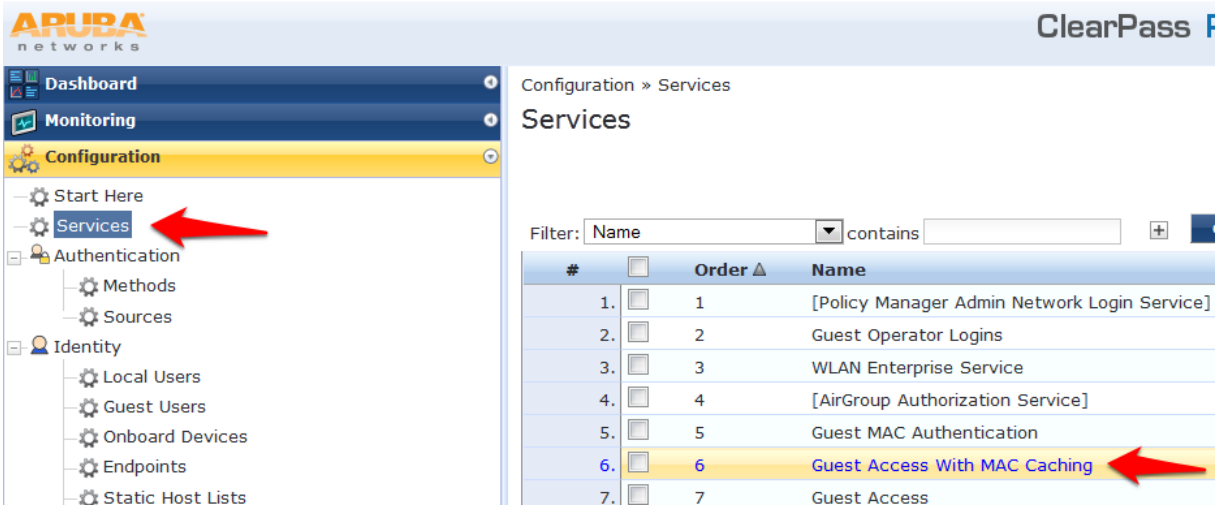
Note: Do <u>NOT</u> move any services you create ABOVE the initial services that are installed with ClearPass Policy Manager. **IF** you add a service and move it ABOVE the initial services installed your newly created service **could** intercept RADIUS requests that “Guest Mac authentication”, which is Mac caching, or Onboarding, and AirGroup.



If you are running the beta version of 6.0, you may not have the Guest MAC Authentication services. If this is the case, please <u>download</u> the non-beta version of 6.0, as it will include these services by default.

Guest SSID Login service configuration

To configure the Guest SSID Login service, navigate to **Configuration->Services**. Click on “Guest Access With MAC Caching.”

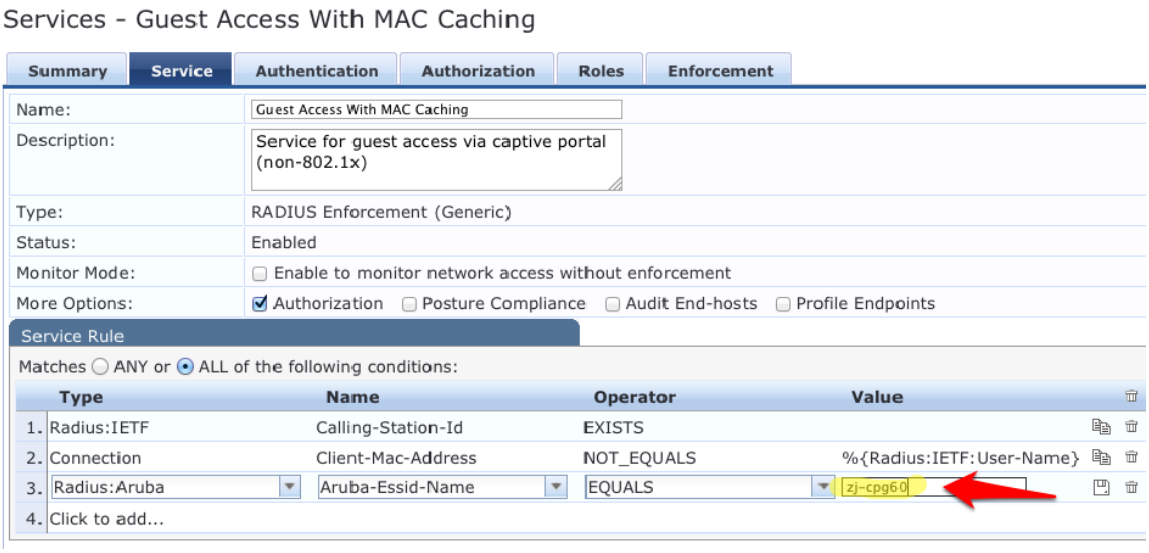


Click on the **Service tab**.

In order to get this service to respond to the guest SSID, click the “Radius:Aruba, Aruba-Essid-Name, EQUALS, Guest SSID Name” row under **Service Rule** sub-tab to modify.

Replace the “Guest SSID Name” with the actual guest SSID used on the controller.

In the example below, the guest SSID is “zj-cpg60.”



Click **Save** to register the modifications to the service.

Repeat those steps for the “Guest MAC Authentication” service:

Services - Guest MAC Authentication

Summary | Service | Authentication | Authorization | Roles | Enforcement

Name:	Guest MAC Authentication
Description:	Service performing authentication for cached MAC entries for guest accounts
Type:	MAC Authentication
Status:	Enabled
Monitor Mode:	Enable to monitor network access without enforcement
More Options:	Authorization Audit End-hosts Profile Endpoints

Service Rule

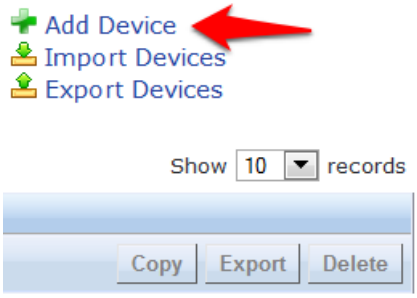
Matches ANY or ALL of the following conditions:

	Type	Name	Operator	Value
1.	Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}
2.	Radius:Aruba	Aruba-Essid-Name	EQUALS	zj-cpg60
3.	Click to add...			

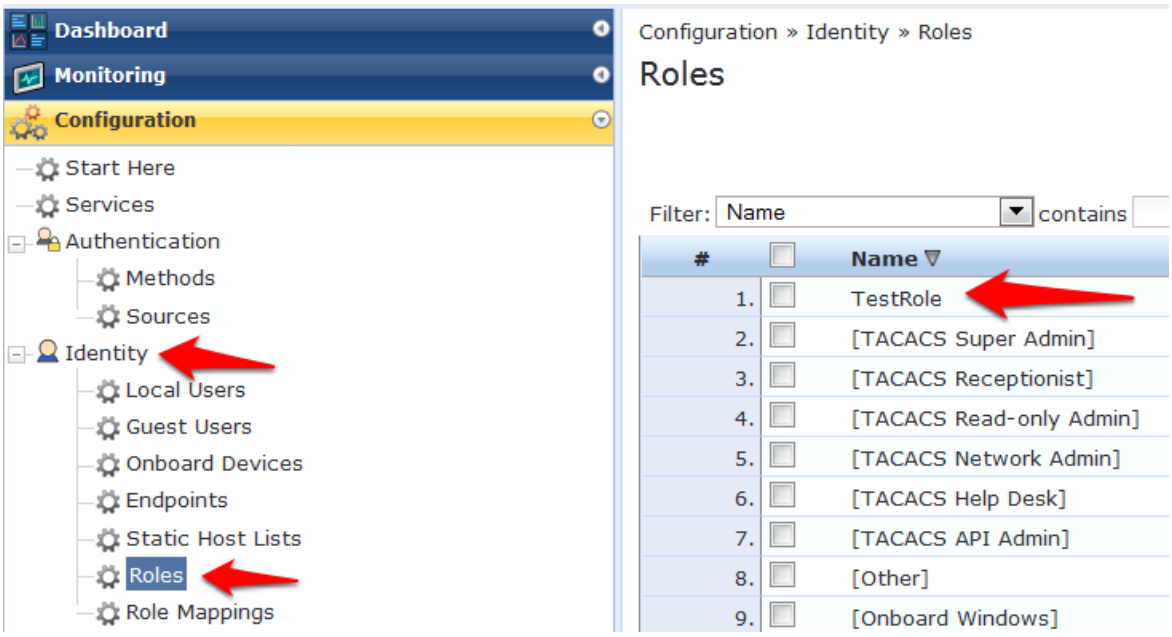
The next step is to add a User Role. Even though no role mapping is in use in the WLAN Enterprise Service, a user role must be created for any local user account added into the Local User Repository.

Navigate to **Configuration->Identity->Roles**

Click **Add Device** in the top right corner of the page.

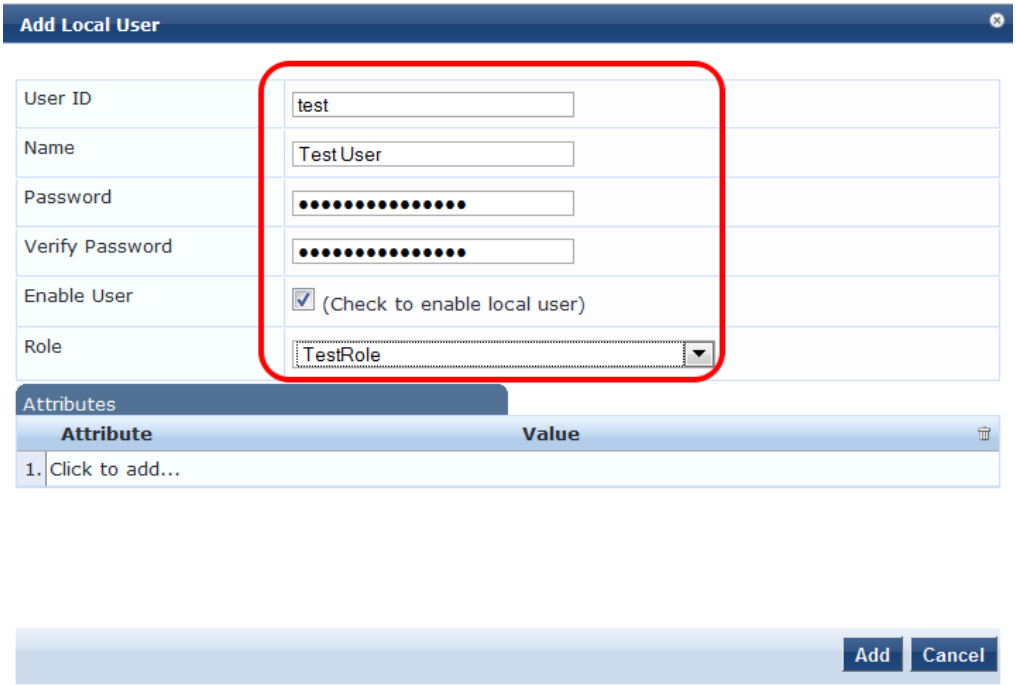


Enter “TestRole” as the name, and click **Save**.



Navigate to **Configuration->Identity->Local Users**. Click **Add User**. Enter the following information:

- User ID: test
- Name: Test User
- Password: test123
- Verify Password: test123
- Enable User: *checked*
- Role: TestRole



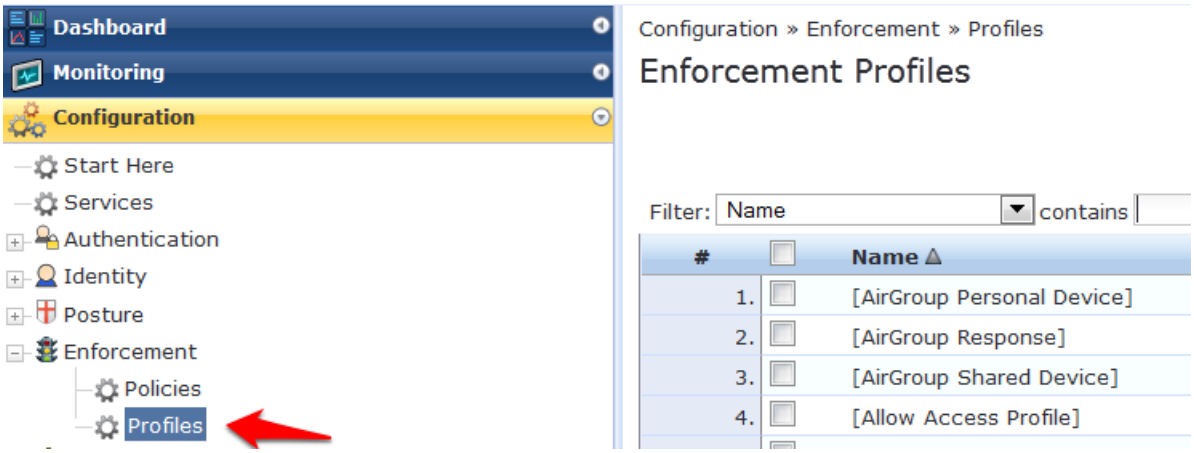
Click **Add.**

3. Testing the 802.1x and Guest SSID

At this point testing of the 802.1x and Guest SSID could commence. However, when 802.1x is tested with the Test User account, the user will authenticate but receive the guest role on the controller. This is because an Aruba User Role is not being passed back for the Test User. When the controller receives the RADIUS Accept from a successful authentication, the controller will give the client the default 802.1x role set in the AAA Profile.

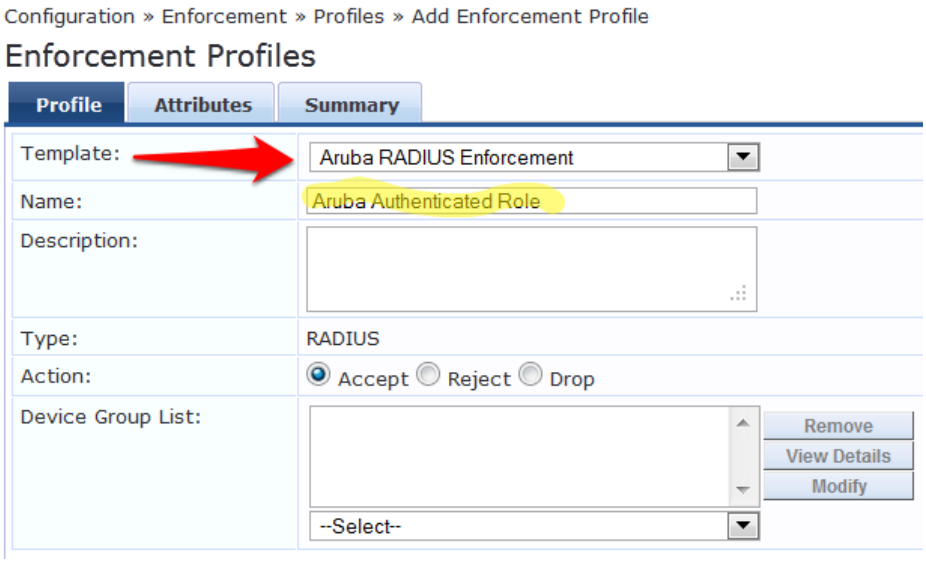
In order to pass back an Aruba User Role, an Enforcement Profile must be built and the Sample Allow Access Policy must be modified to send this Enforcement Profile.

Navigate to **Configuration->Enforcement->Profiles**.



Click **Add Enforcement Policy** in the top right corner of the page.

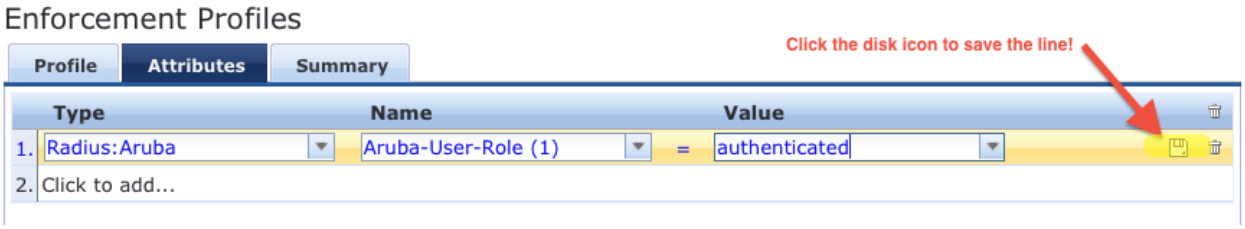
Give it a name like "Aruba Authenticated Role". Make sure the Template selected is Aruba RADIUS Enforcement:



Click **Next**.

Click on “Enter role here” and enter “authenticated” as the role to be passed back. Then click on the disk icon  to save the line.

Click **Save.**

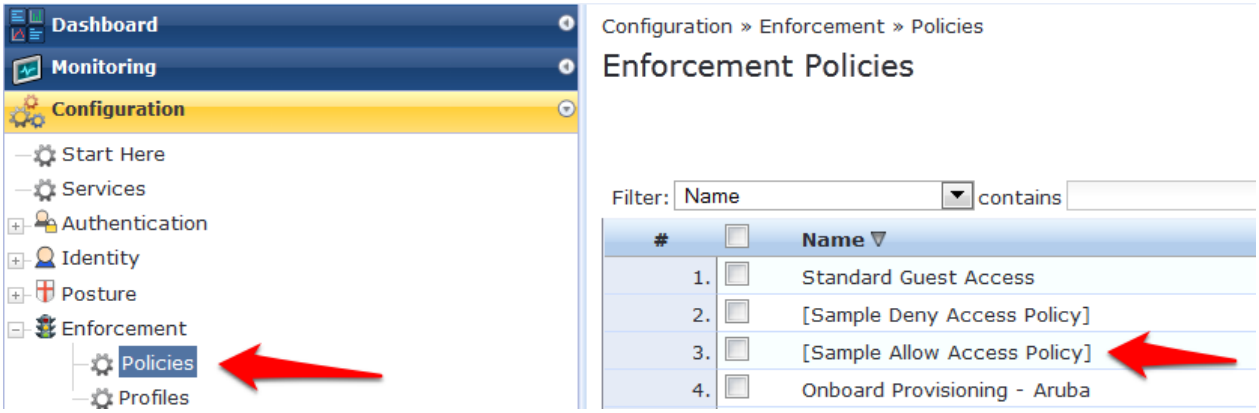


Tech Tip: Get used to clicking that disk icon. Whenever you edit a line like this, click the disk icon to save the line, or else your change may not get saved.

Click **Next**.

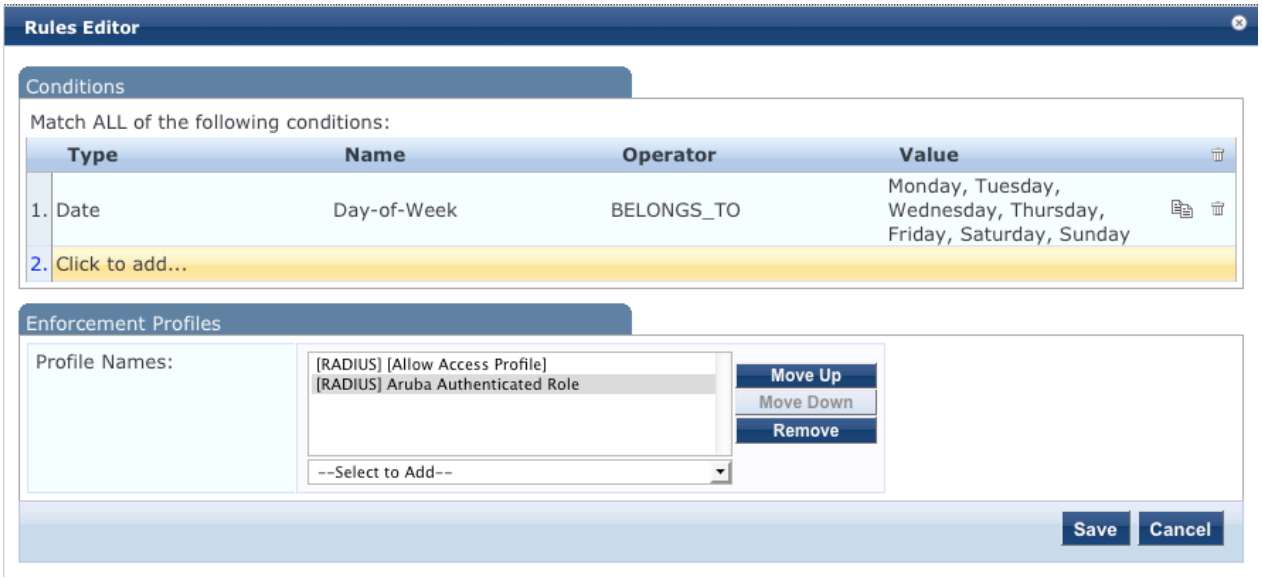
Click **Save**.

Navigate to **Configuration->Enforcement->Policies**. Click on the “Sample Allow Access Policy” to edit.



Click on the **Rules** tab. Click on the only Condition in the list to highlight it, and click **Edit Rule**.

Select the “Aruba Authenticated Profile” from the “—Select to Add—“ drop down menu to the list of Enforcement Profiles that will be executed when a user successfully authenticates:



Click **Save** the the **Rules Editor** window.

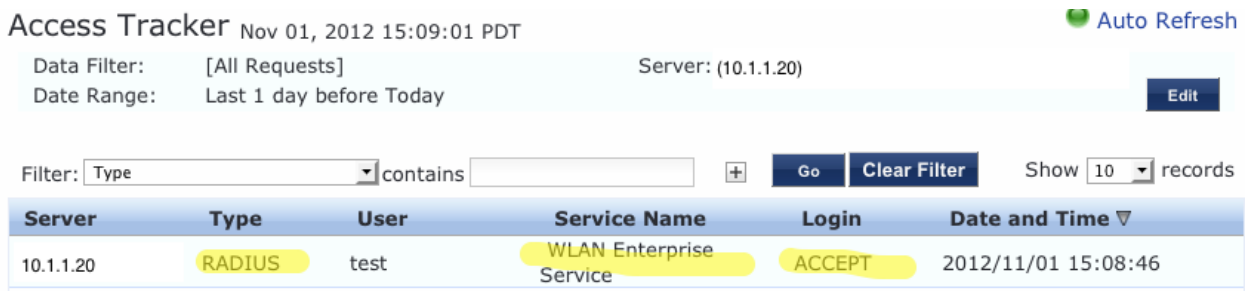
Click **Save** in the lower right corner of the page.

Step 8: Test the 802.1x SSID

Connect to the 802.1x SSID, and login with the local user account (NOT the guest account) created in the ClearPass Policy Manager setup.

Navigate to **Monitoring->Live Monitoring->Access Tracker**.

A RADIUS ACCEPT for the WLAN Enterprise Service server should be visible.

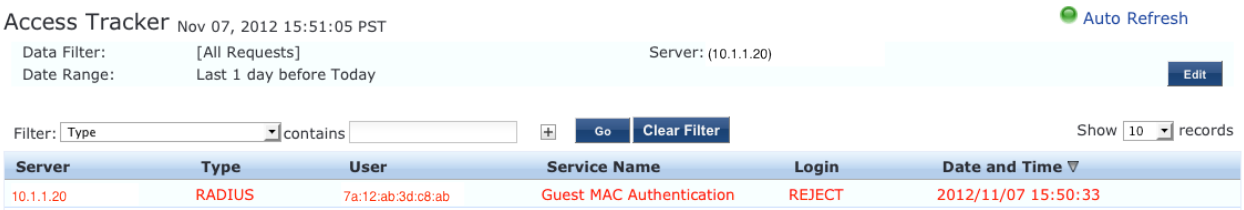


Step 9: Testing the Guest SSID

At this point, both the 802.1x SSID and the Guest SSID can be tested. Start by testing the Guest SSID.

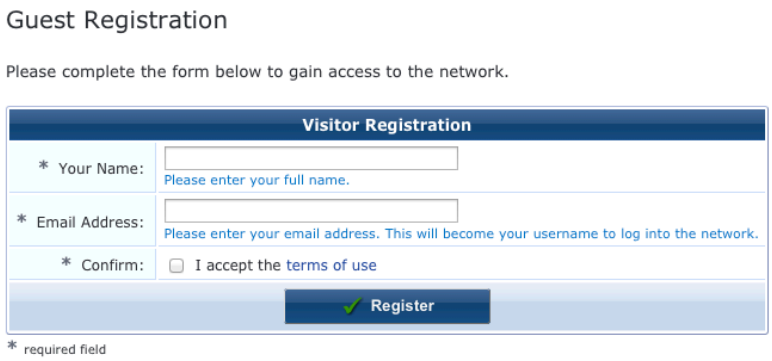
In ClearPass Policy Manager navigate to **Monitoring->Live Monitoring->Access Tracker**.

When your device first connects to the Guest SSID you will notice a MAC Auth REJECT. This is for the MAC Caching on the Guest SSID.



Open up a web browser on your device that just connected. It should redirect you to the Guest Login page. Select "Click Here" after **Need an account?**

You will be then be presented with the Guest Account Creation page.



Enter the information (Email Address will become the guest username), check the box to accept the terms of use, and click Register.

You will then be presented with the Guest Registration Receipt that shows the guest username and password.

Clicking "Log In" will automatically submit these credentials to the wireless controller's internal captive portal, which will in turn create a RADIUS request with the Authentication Method PAP. This request will hit the Guest SSID Login Service that was created in ClearPass Policy Manager in the previous step.

After logging in on the test device, return to Access Tracker in ClearPass Policy Manager.

Notice the RADIUS ACCEPT entry for test@test.com:

Filter: Type contains Go Clear Filter Show 10 records

Server	Type	User	Service Name	Login	Date and Time
10.1.1.20	RADIUS	test@test.com	Guest Access With MAC Caching	ACCEPT	2012/11/07 15:52:34
10.1.1.20	RADIUS	7a:12:ab:3d:c8:ab	Guest MAC Authentication	REJECT	2012/11/07 15:50:33

STOP! Wait 3 minutes before proceeding to the next step. For MAC Caching, the service queries the Insight Database. Information is pushed to the Insight Database every 3 minutes.

Testing the MAC Caching

The next steps test the MAC Caching.

1. SSH to your controller and run the "show user-table | include test@test.com" in order to find the MAC address of the test device.
2. Disable the wireless on the test device and run the "aaa user delete mac 00:aa:22:bb:44:cc" command where "00:aa:22:bb:44:cc" is the MAC address returned from the show user-table command.
3. Re-enable the wireless on the test device. Now in Access Tracker you will see a successful MAC authentication.

Filter: Type contains Go Clear Filter Show 10 records

Server	Type	User	Service Name	Login	Date and Time
10.1.1.20	RADIUS	7a:12:ab:3d:c8:ab	Guest MAC Authentication	ACCEPT	2012/11/07 15:57:55
10.1.1.20	RADIUS	test@test.com	Guest Access With MAC Caching	ACCEPT	2012/11/07 15:52:34
10.1.1.20	RADIUS	7a:12:ab:3d:c8:ab	Guest MAC Authentication	REJECT	2012/11/07 15:50:33

Advanced Features

Controller Management Login Authentication with ClearPass Policy Manager

In ClearPass Policy Manager, navigate to **Configuration->Identity->Roles**.

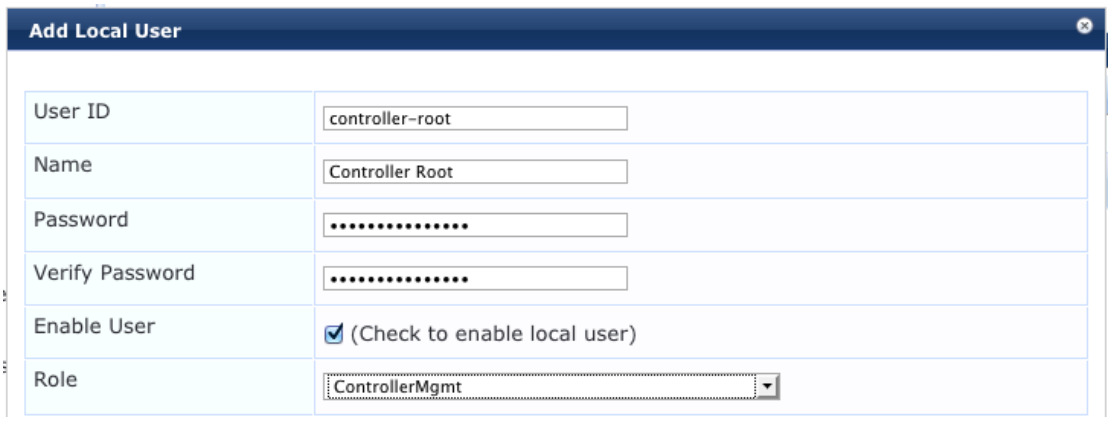
Click **Add Roles**.

Create a new role called “ControllerMgmt.”

Navigate to **Configuration->Identity->Local Users**.

Click **Add User**.

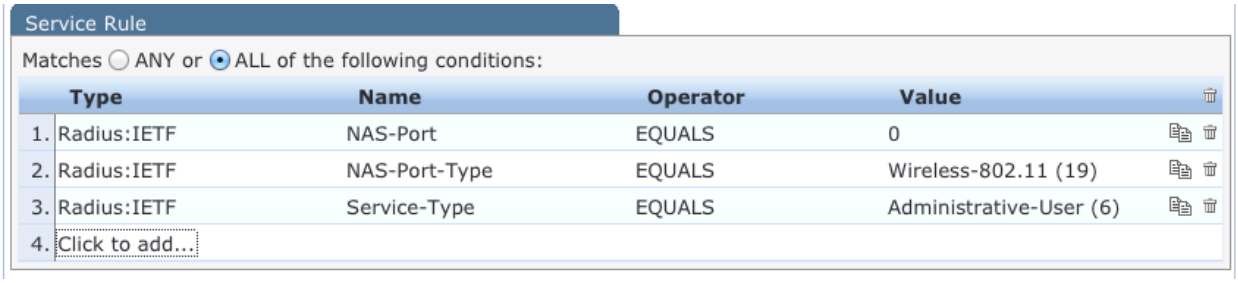
Enter the information in the image below, using whatever you want for the password (this will be the login and password for managing the controller):



Click **Add** to save this user account.

Navigate to **Configuration->Start Here**.

Click on RADIUS Enforcement (Generic). Give the service a name such as “Aruba Controller Management Login.” Add the Service Rules in the image below:

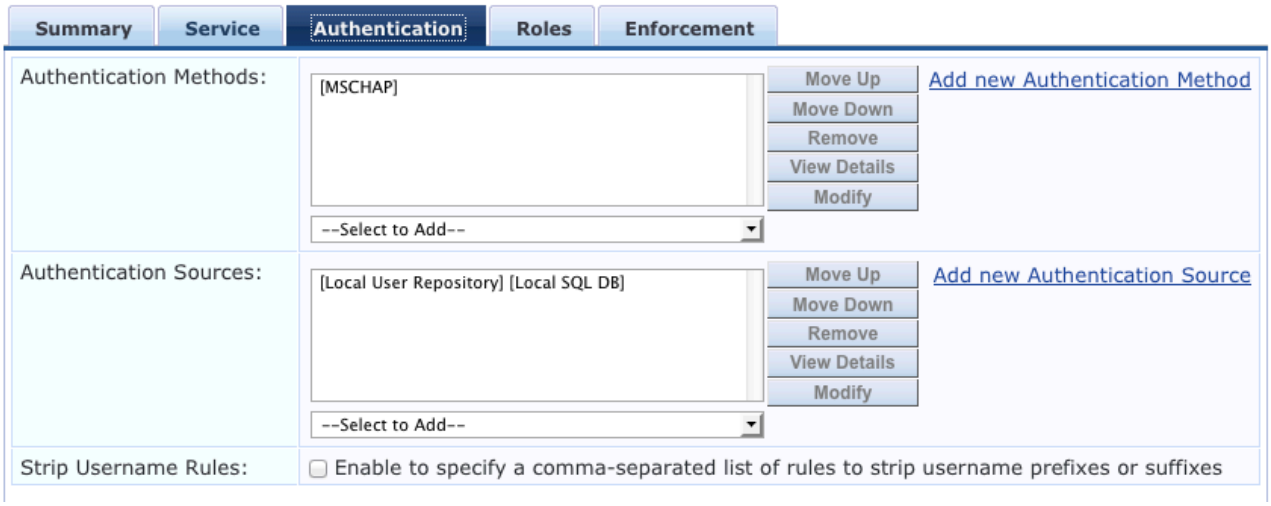


Remember to click the disk at the end of each line in order to save the line.

Click **Next**.

For “Authentication Methods”, Click the “Select to Add” down arrow and choose “[MACHAP].”

For “Authentication Sources,” Click the “Select to Add” down arrow and choose [Local User Repository] [Local SQL DB]

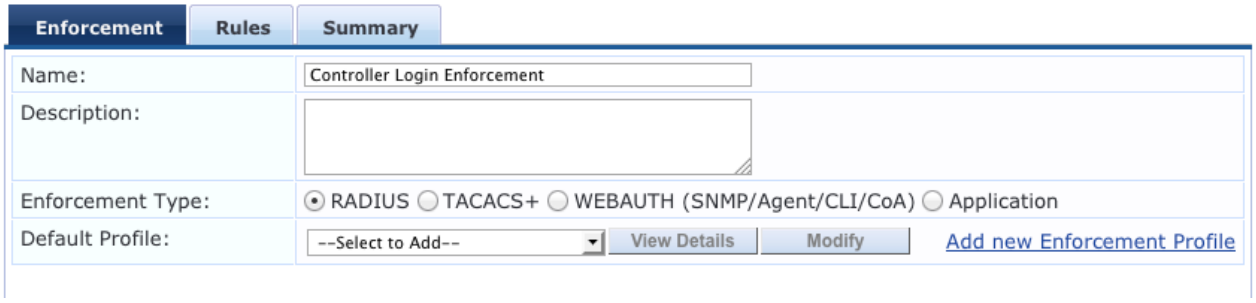


Click **Next**.

Tech Tip: You could use a Role Mapping Policy, but it is not required. It would be required if the Authentication source was Active Directory, in which case you would create a Role Mapping rule that would look for Authorization: SomeADServer:MemberOf:Contains:IT-Admins; Role Name: ControllerMgmt.

Click **Next.**

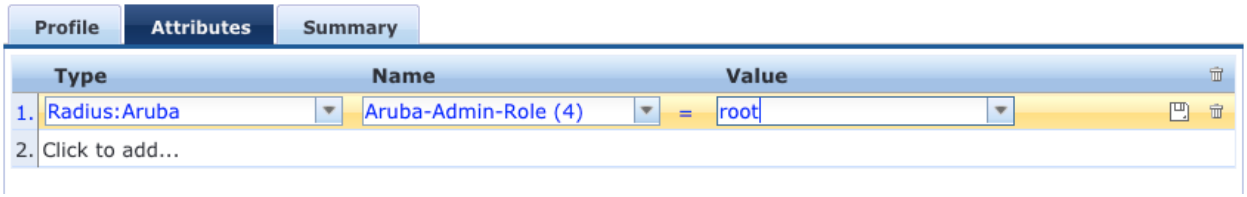
On the **Enforcement** tab, Click **Add new Enforcement Policy**. Give the new Enforcement Policy a name like "Controller Login Enforcement."



Click **Add new Enforcement Profile**. Use the Aruba RADIUS Enforcement template. Enter a name for the Enforcement Profile such as "Aruba MGMT Root User."

Click **Next**. Match the Attribute to the following image

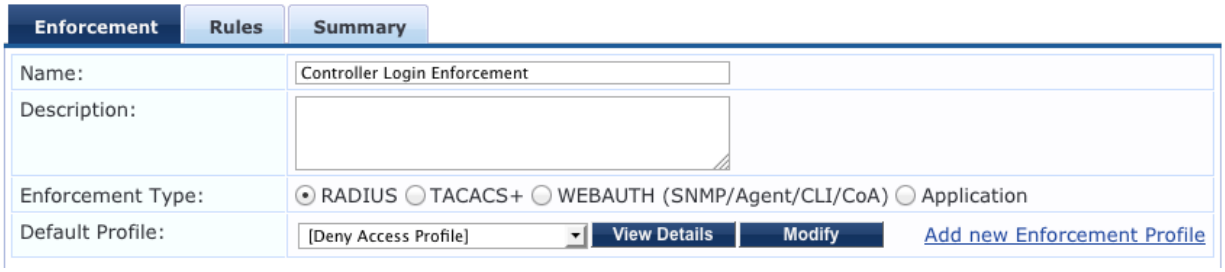
(**Note:** "Aruba-User-Role" is changed to "Aruba-Admin-Role"):



Remember to click the Save Disk at the end of the line.

Click **Next**.

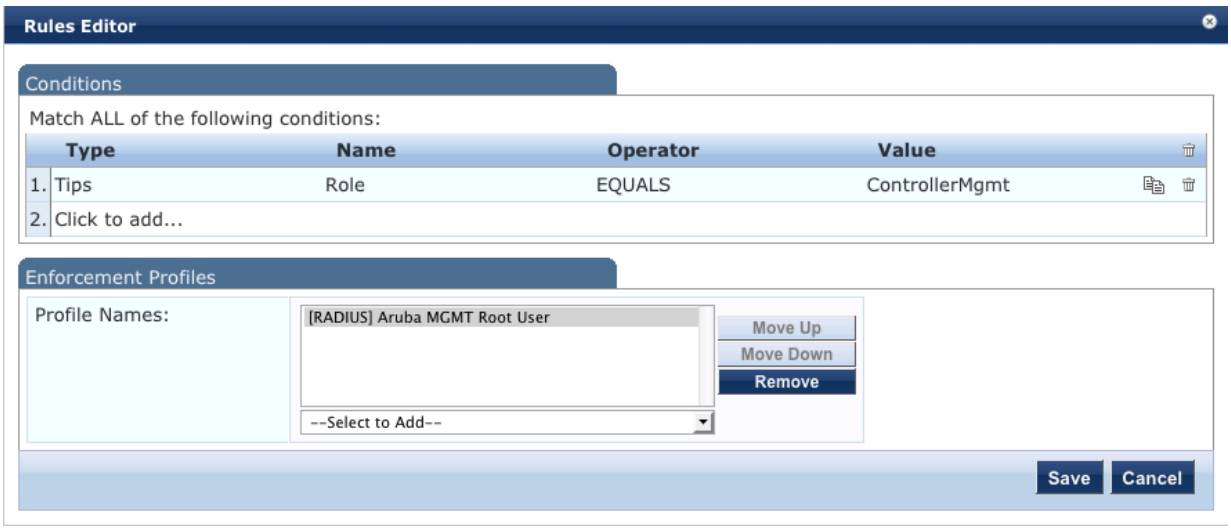
Click **Save**. This will return you to the Enforcement Policy creation. Change the **Default Profile** to “Deny Access Profile.”



Click **Next**.

On the **Rules** tab, click **Add Rule**.

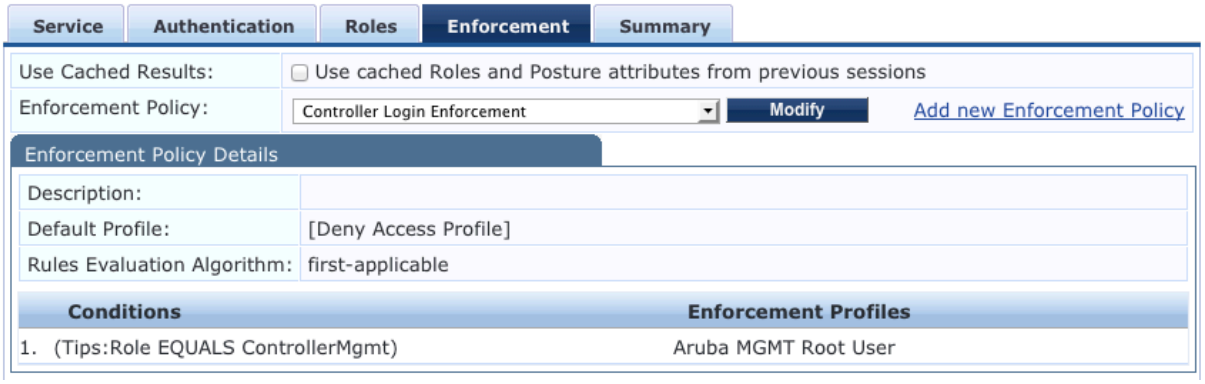
Enter the Rule **Conditions** and **Enforcement Profiles** as shown in the image below:



Click **Save**. Click **Next**.

Click **Save** to log the Enforcement Policy.

The newly created Enforcement Policy should automatically be selected for the Service in the Service creation flow.



Click **Next**.

Click **Save**.

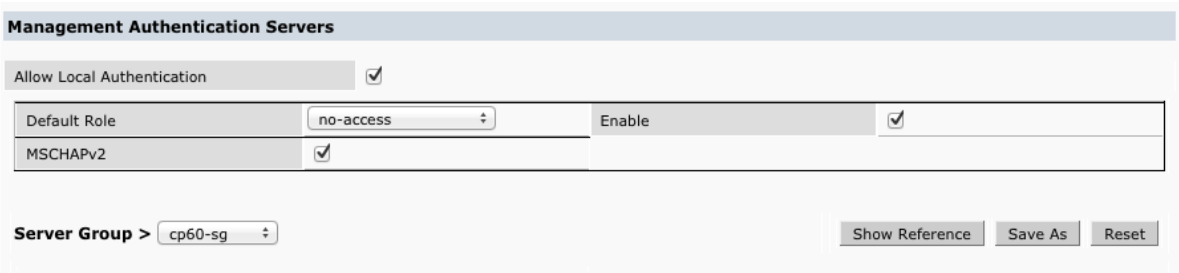
Note: Reorder the service so that it is **above** the Guest – MAC caching generic service.

Click **Save**.

Login to the wireless controller GUI.

Navigate to **Configuration->Management->Administration**.

1. Change Default Role to “no-access.”
2. Check the checkbox for **Enable**.
3. Check the checkbox for **MSCHAPv2**.
4. Change the **Server Group** to the ClearPass Policy Manager server group created earlier in this document.

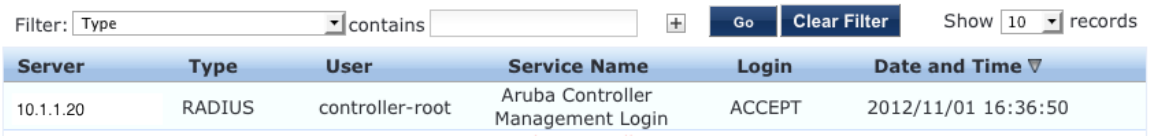


Important! Leave the **Allow Local Authentication** box checked. If this box is unchecked and there is a problem with the Management Authentication configuration, you will not be able to login to the controller if **Allow Local Authentication** is unchecked.

Click **Appl**y to save these settings.

Logout of the controller and test login with the controller-root test user created earlier.

In Access Tracker you should see the RADIUS ACCEPT for the controller-root test user:



Troubleshooting

Problem:

MAC Caching is not working.

Solution:

Check the Endpoints Repository (Identity->Endpoints) for the device in question. Click on the device and verify that the device status is set to Known. If it is not, verify that the correct controller-ip vlan has been set on the wireless controller.

Problem:

During creation of Enforcement Policy, an error appears when trying to save: Name contains special characters…

Solution:

Creation of the Enforcement Policy has timed out. Click Cancel, then create the Enforcement Policy again.