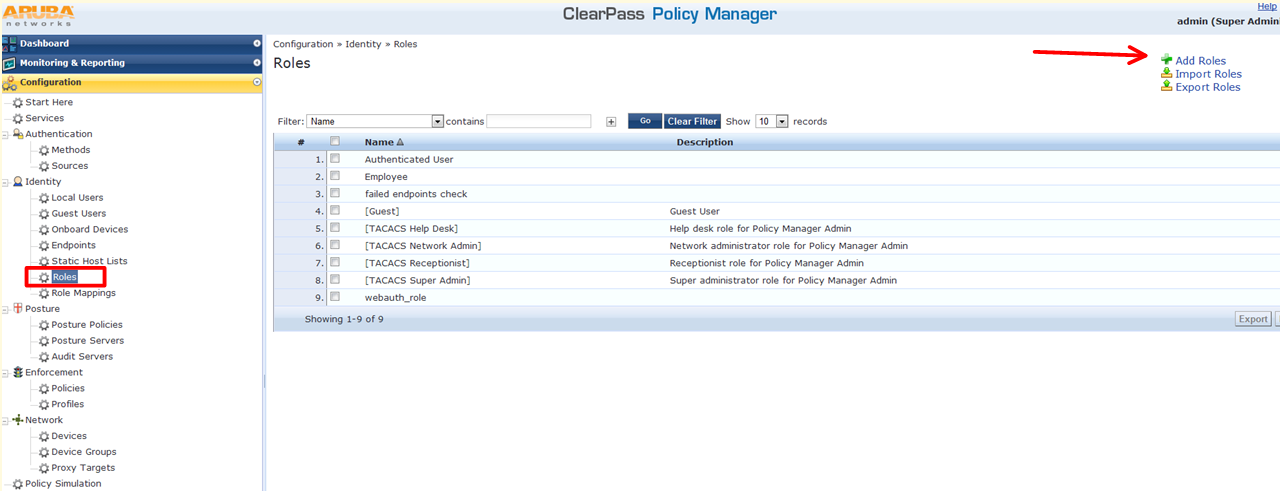
**Placing users in Controller Roles based off of AD Groups with CPPM**

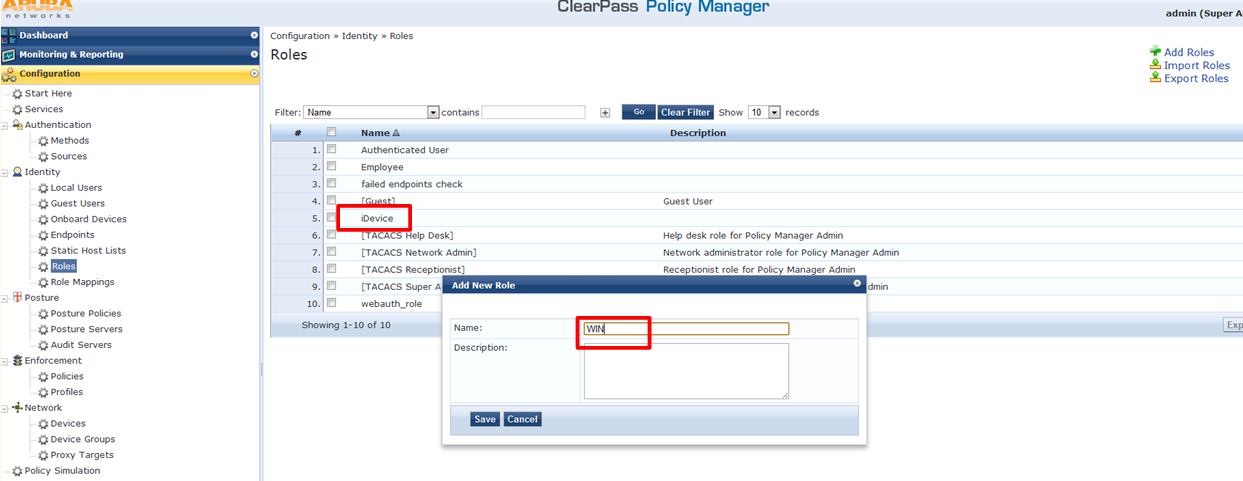
To start we need to make a couple of things that we will apply in the Services configuration. First we will make the Roles for the devices and then we will make the Enforcement Profiles.

In this example I already have CPPM tied into AD and running a wireless 802.1x service. There are other documents that explain how to do that if you need them.

**Roles**



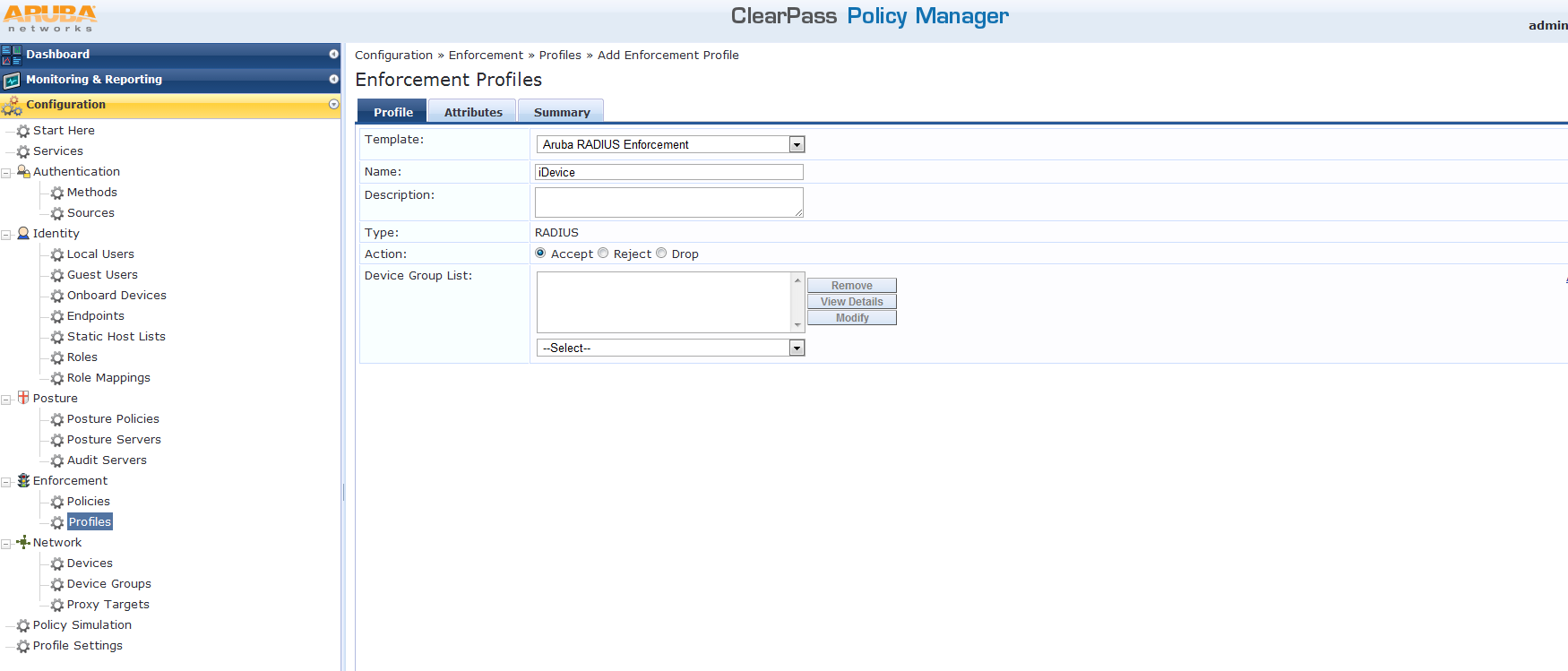
Give the Roles a name



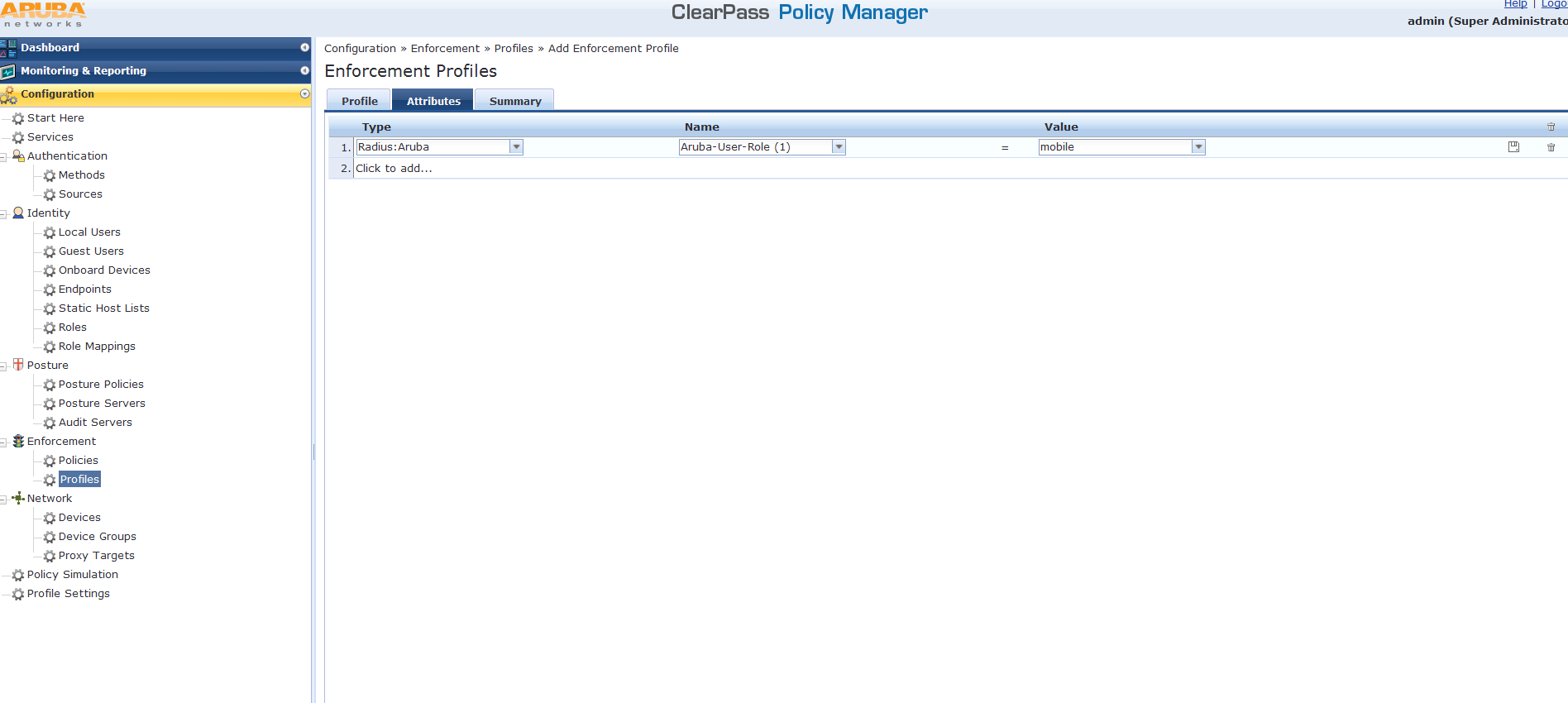
**Enforcement Profiles**

Make an Enforcement Profile for each AD Group you want to place in a different Aruba Firewall Role. From the Template you can also assign a VLAN if you would rather.

Give it a name.



In the Attributes tab enter a Value that matches the Aruba Controller Firewall User Role.

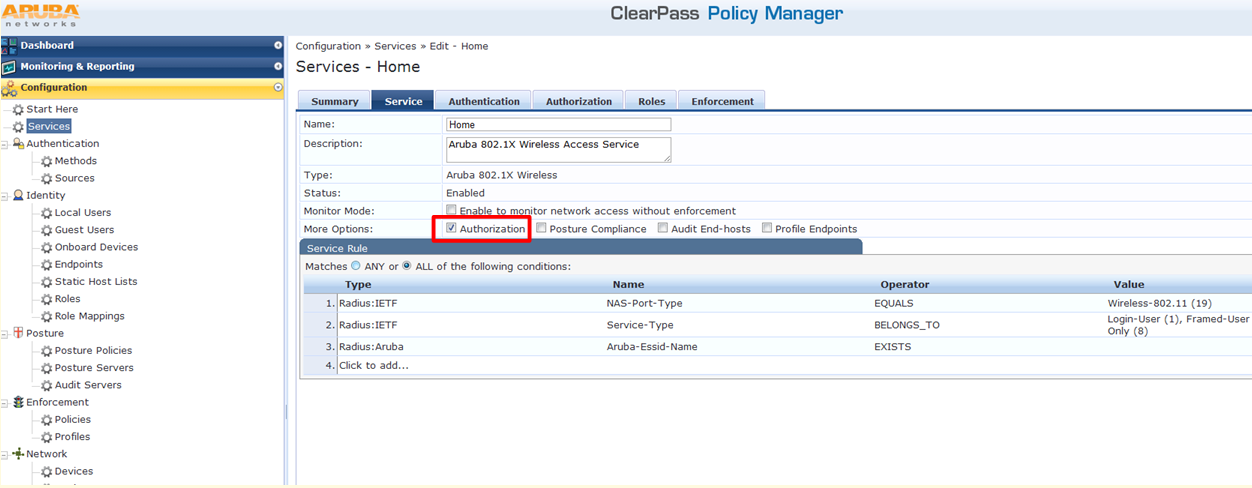


Save it and repeat for each AD Group you want to match.

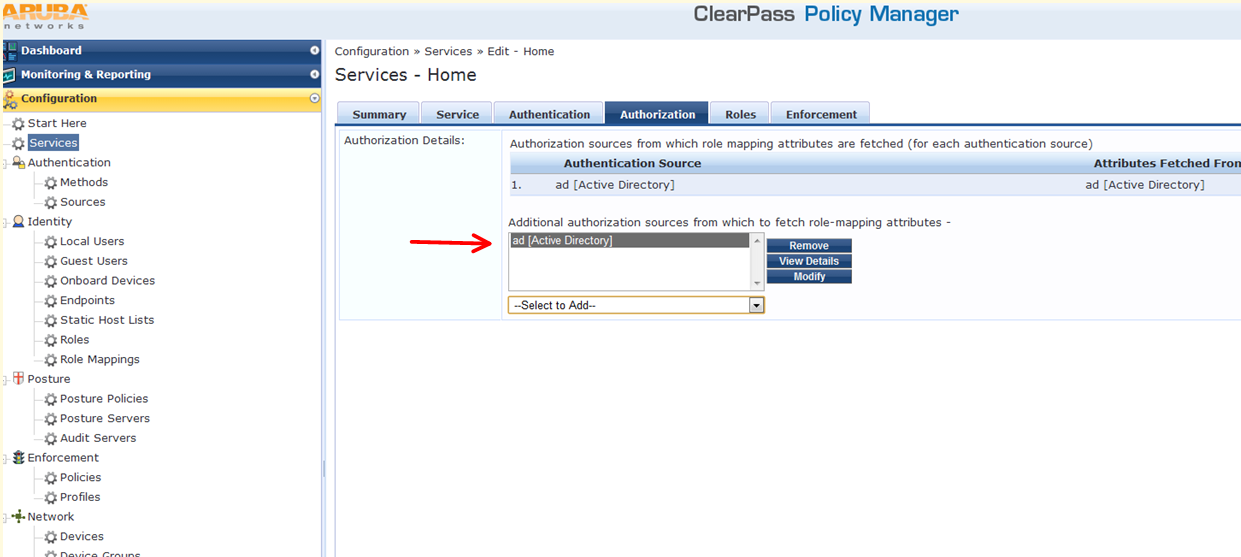
**Services**

In the Service you are using for PEAP, check the Authorization box. This will add a new tab at the top.

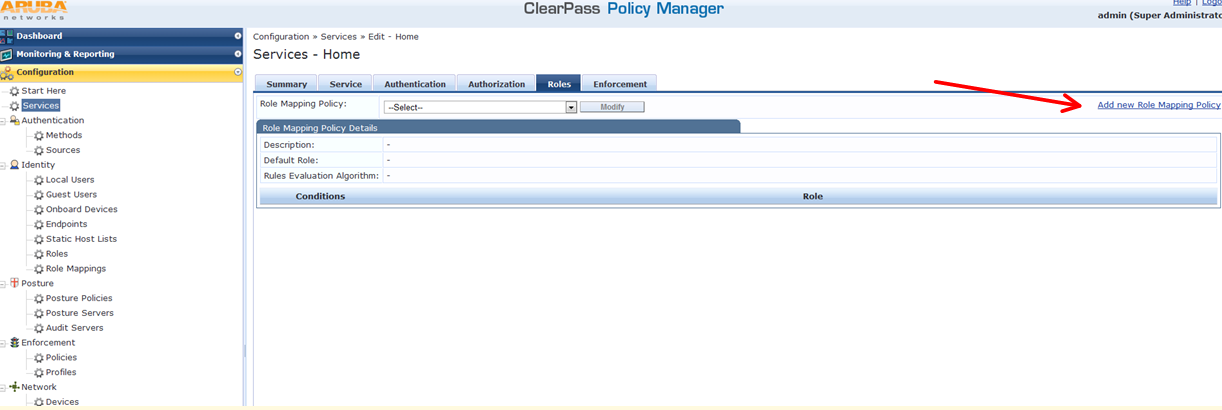
Note: if you don't already have a Service configured for PEAP go to Start Here and walk through the wizard.



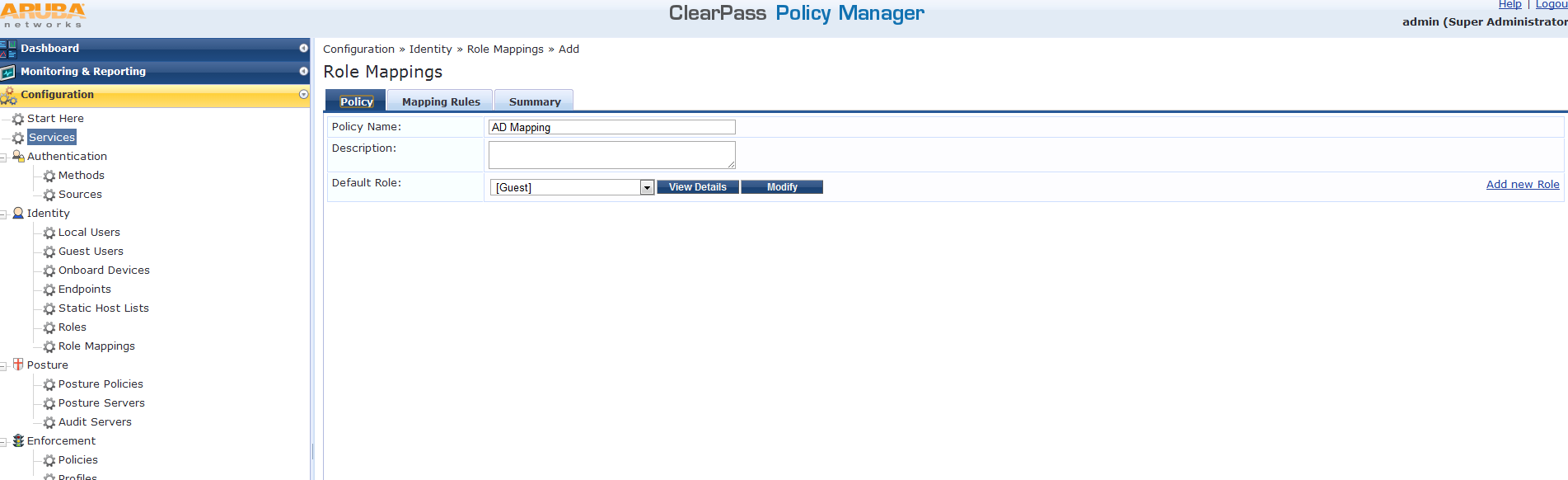
Add your AD server to the additional sources.



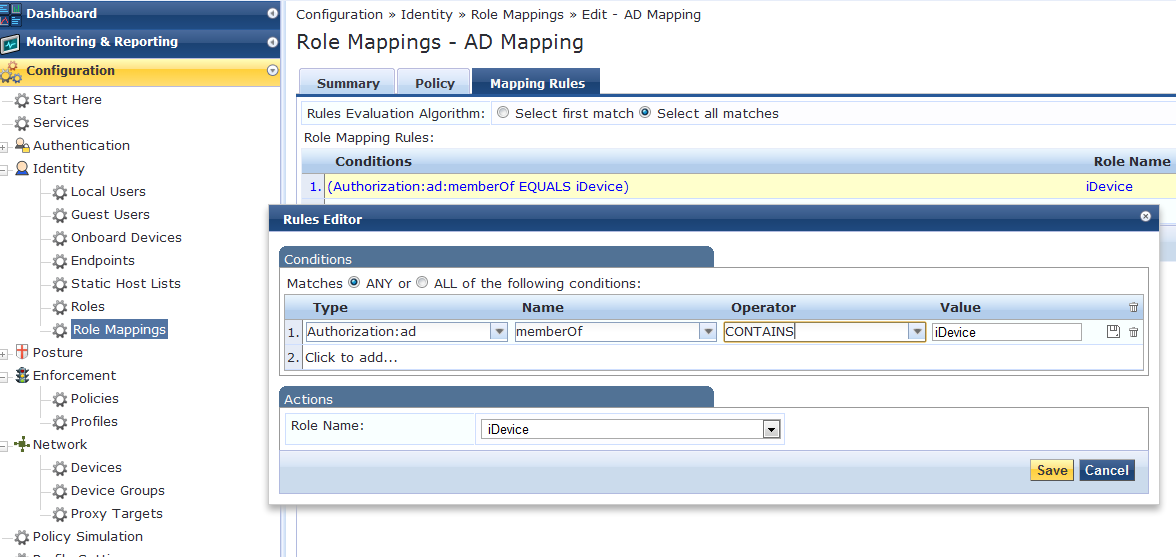
Under the Roles tab you will need to add a new Role Mapping Policy. This is what is going to look for the group coming from AD.



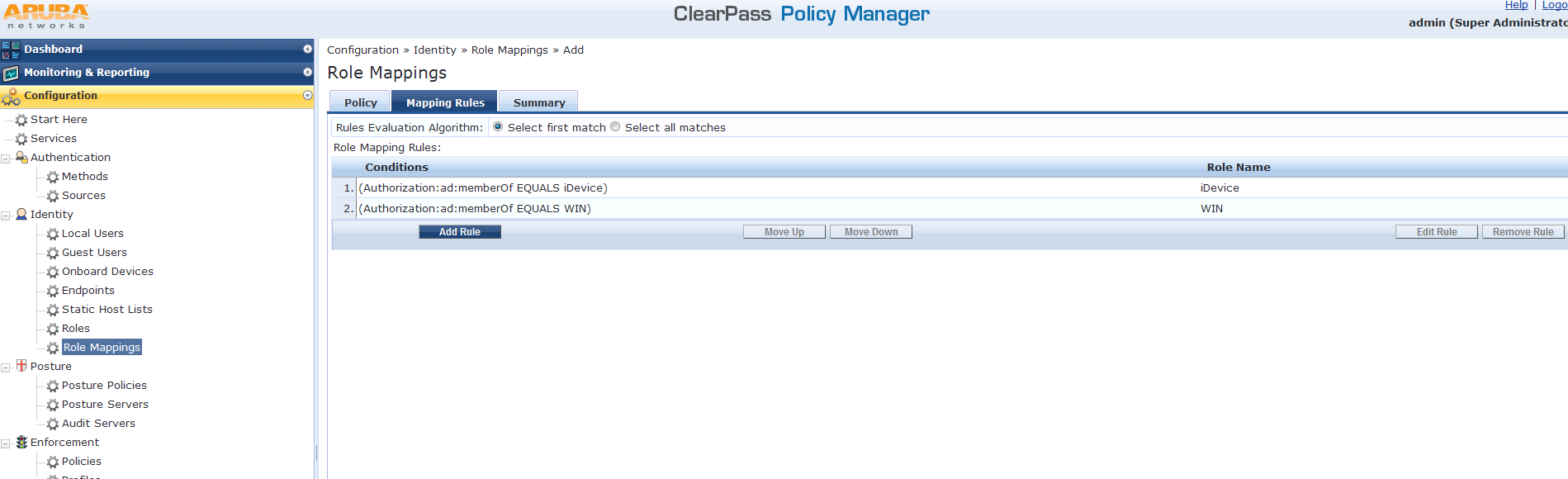
Give it a name. The Default Role is going to be which role they are in if they don't match any of the Rules we are about to write.



Add a Rule for each AD Group you want to match. The Operator will be contains if the user is in more than one AD Group.

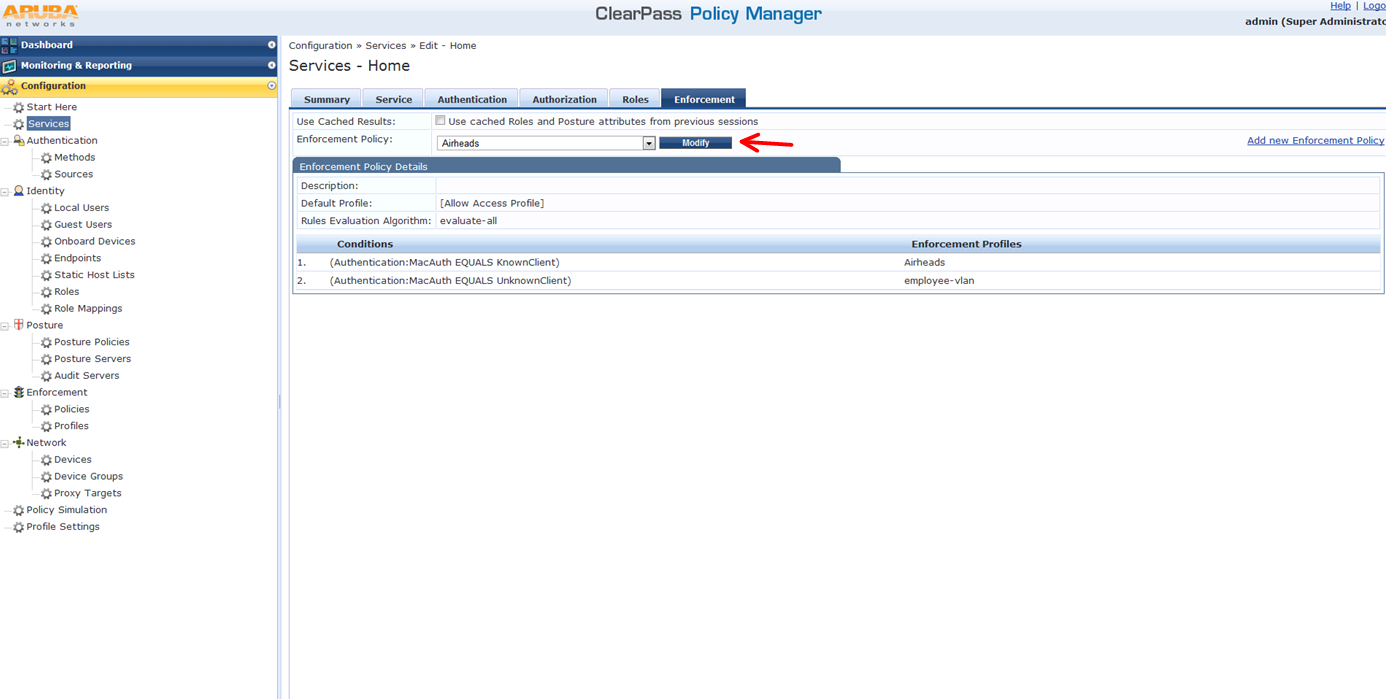


Here is what they both look like

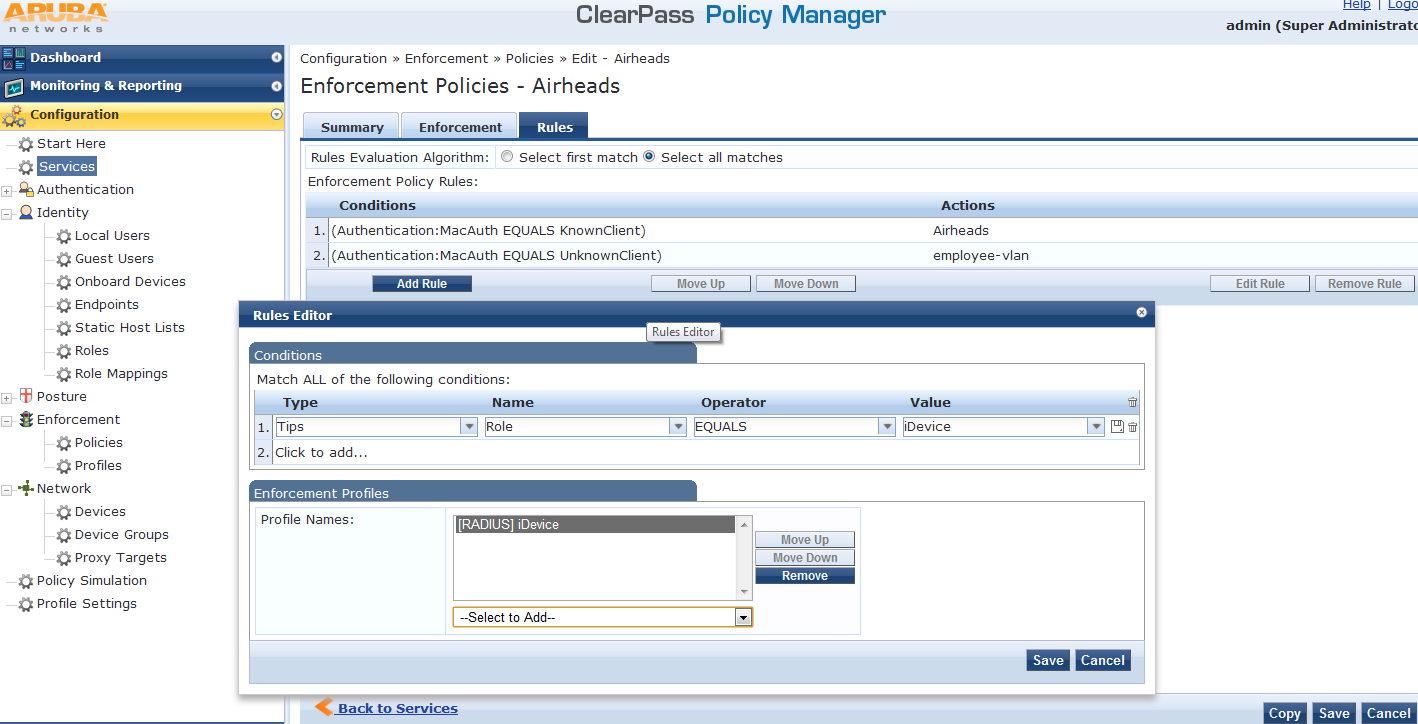


Now that we have the inbound rules written for what to watch for we will write the outbound rule that will send attributes to the Aruba controller. This is done in the Enforcement tab.

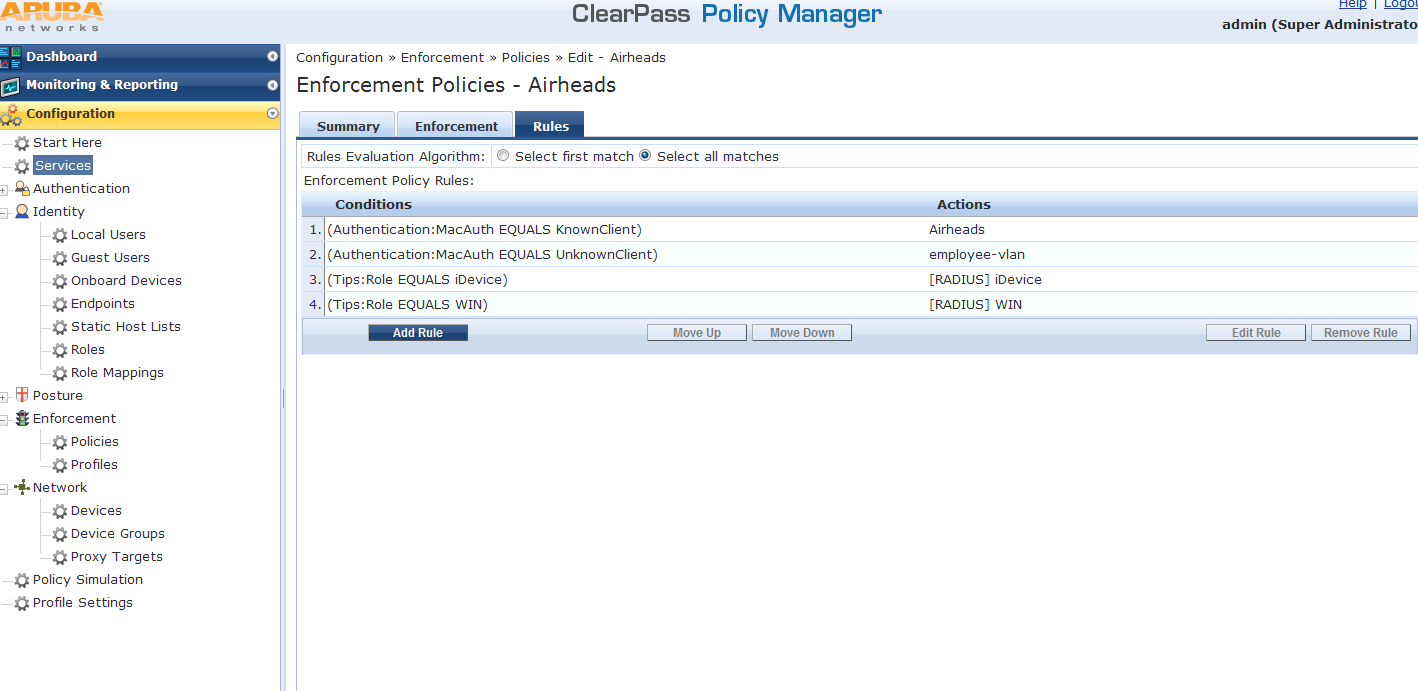
I already have an Enforcement policy that is doing MAC Auth that I will Modify. If you don't already have one you can add a new one on the right.



The rule to match the value I set in role mapping looks like this : (Tips:Role EQUALS iDevice) and then you tie in the Enforcement Profile that we made when we started.



Here is a summary of the two new rules we created. You might need to reorder them and change the Rules Evaluation Algorithm to meet your goals.



**Test**

To verify your user is being placed in the correct role view an authentication in Access Tracker. Under the Policies Used you will see what Roles were used

