**Rogue Containment From AMP to Aruba Controllers:**

1. The Rogue containment works only for Cisco WLC and Aruba Controllers. RAPIDS > setup page > Containment Options is self explanatory. Select Manage Rogue AP containment to yes.
2. If the controllers are in Manage mode, not to worry about the second option here.
3. If the controllers are in Monitor mode, make sure Manage rogue AP containment in monitor mode is selected ‘yes’. For Aruba Controllers, if WMS offload is enabled, no need to worry about this option here. If WMS offload is not enabled, make sure to select the option. (You need to have telnet/ssh to Controller)



1. From RAPIDS > List select a rogue AP and set the RAPIDS classification to contained:



1. After you make sure that AMP is able to push the containment by checking the RAPIDS list where the RAPIDS classification would be ‘contained’ and on the controller run the below command to check the list of Rogues and see if the rogue class is contained.

# show wms ap list

The class should be contained.

1. On the Aruba controller make sure the Rogue Containment option is selected under Configuration > AP Group > IDS > IDS Profile > IDS unauthorized Device profile



1. a. For wireless containment, select the IDS profile > IDS General Profile in use and set the wireless containment to deauth only

b. For wired containment only select the wireless containment to ‘None’, check wired containment and check wired containment of AP’s adj Macs as well to ensure proper wired containment.



1. To test, try to connect a user to the Rogue and see if the user is getting connected.