WLC Access via RADIUS (ISE)

11 Sunday May 2014

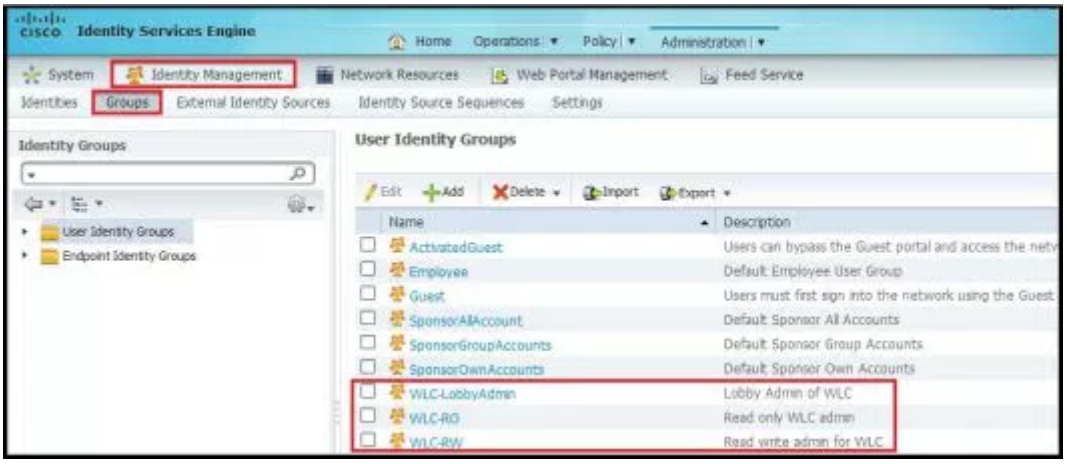
Posted by nayarasi in ISE, WLC Management

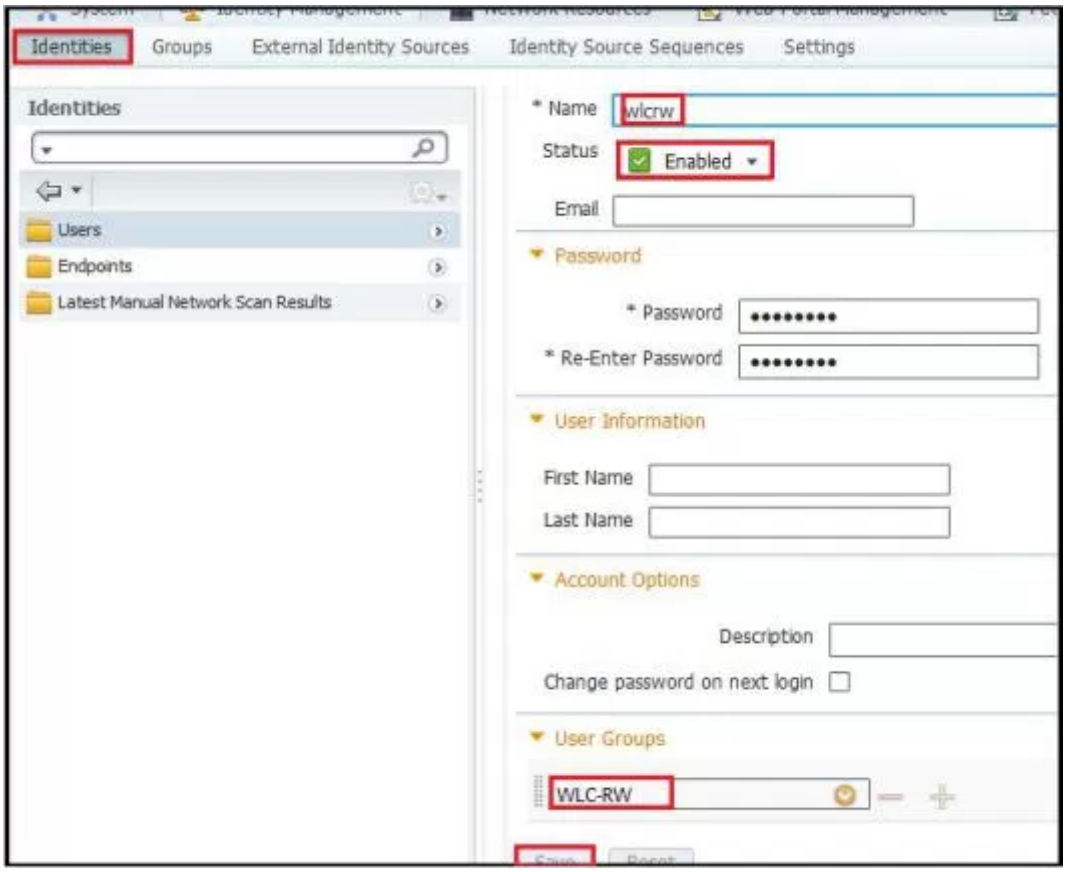
≈ 14 Comments

Tags
ISE, WLC access via RADIUS

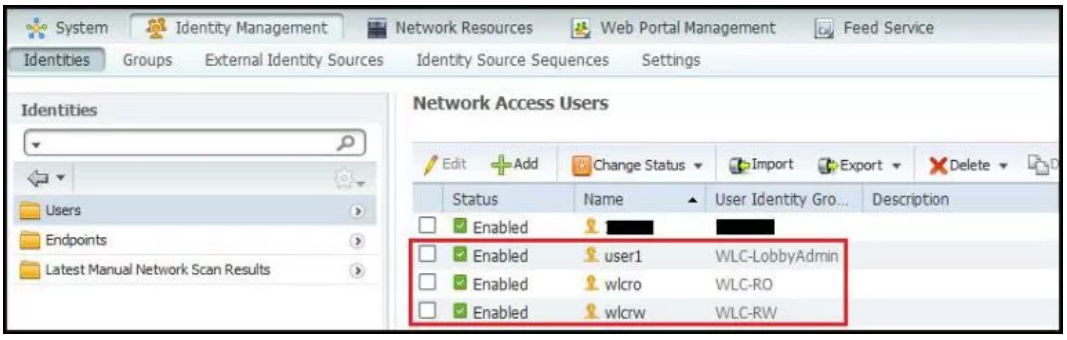
In this post we will see how to control access to a WLC using a RADIUS server. I have used Cisco ISE (Identity Service Engine)a s RADIUS server in this post.

I have created 3 user group (WLC-RW,WLC-RO & WLC-LobbyAdmin) and created 3 users (wlcrw,wlcro & user1). Each user assign for respective User Group as shown below.

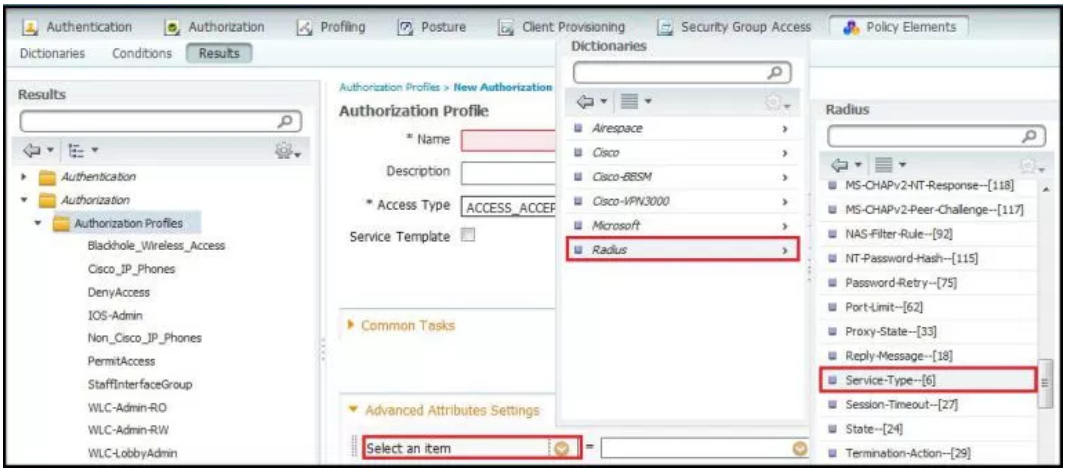




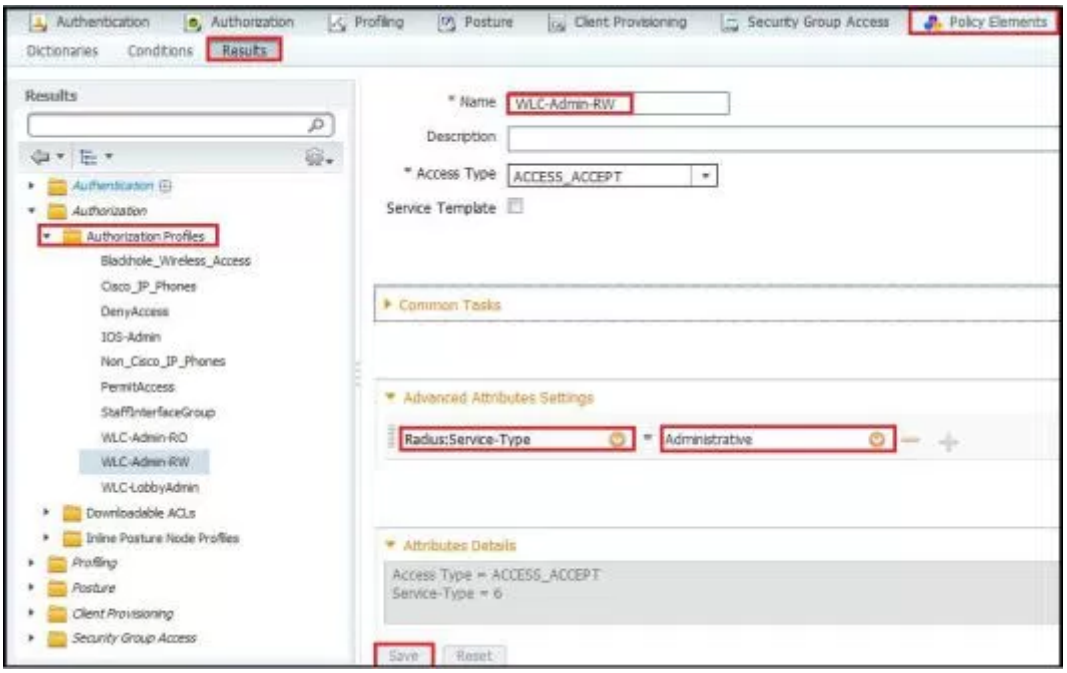
Below shows the 3 users with their respective Group.



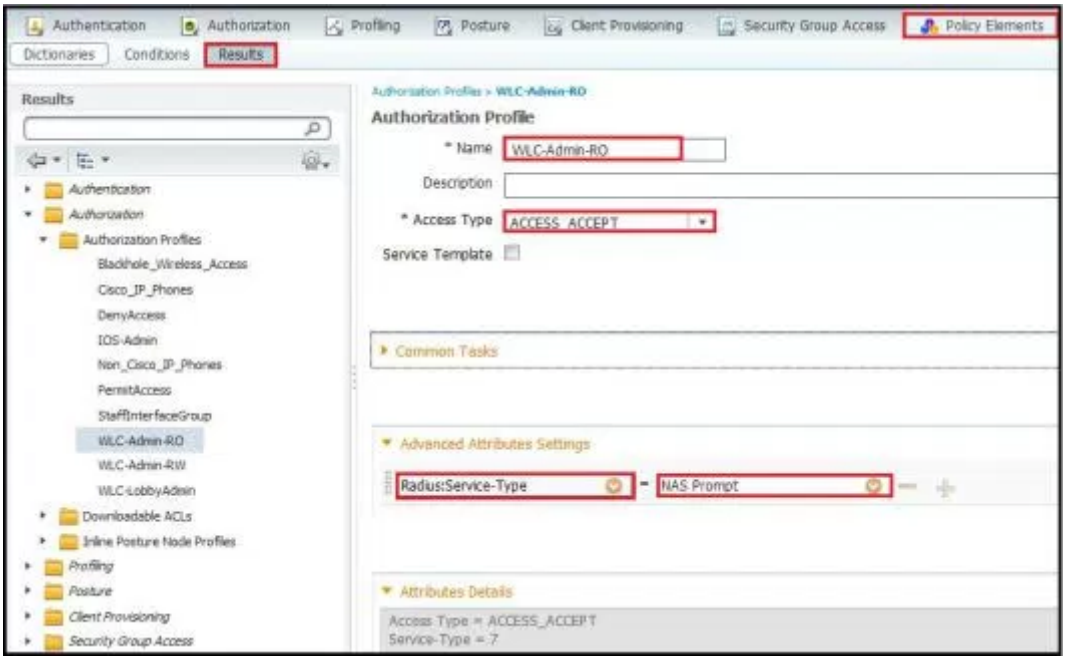
Now you can create 3 different “Authorization Profiles” under “Policy->Policy Elements -> Results” section with different RADIUS attribute values. For full administrative access you have to choose”Service-Type” Radius Attribute setting to “Administrative“. For the Read-Only user this setting should be set to “NAS-prompt” where as for Lobby Ambassador it should be set to “Callback Administrative ”



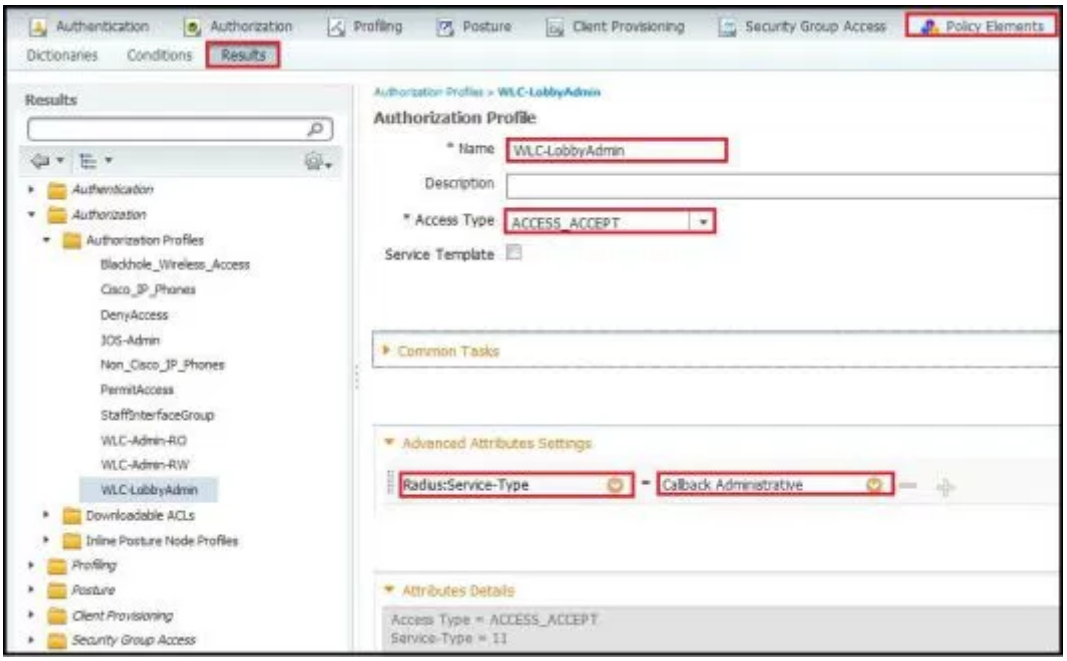
Below shows the created “WLC-Admin-RW” profile with “Service-Type” RADIUS setting to “Administrative”



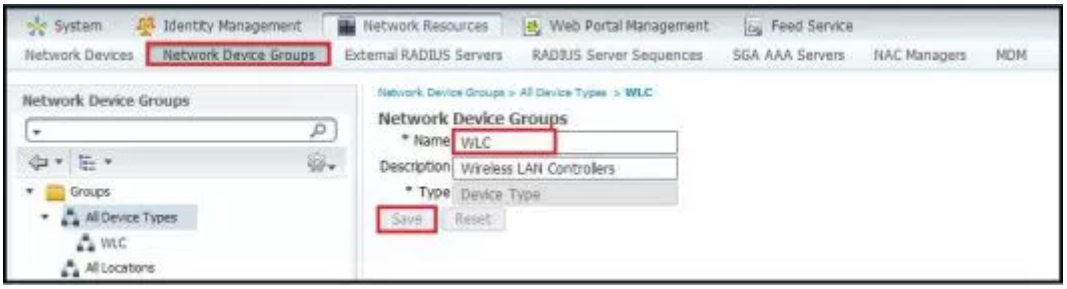
Here is the Authorization profile created for Read-Only user.



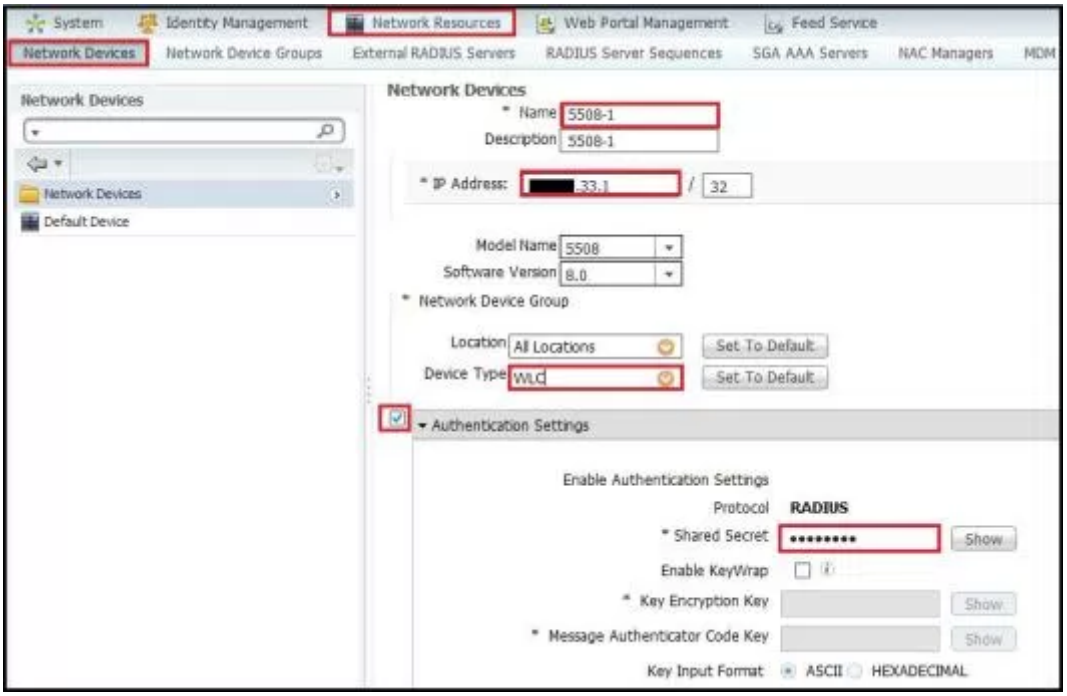
Here is the Authorization profile created for Lobby Ambassador user.



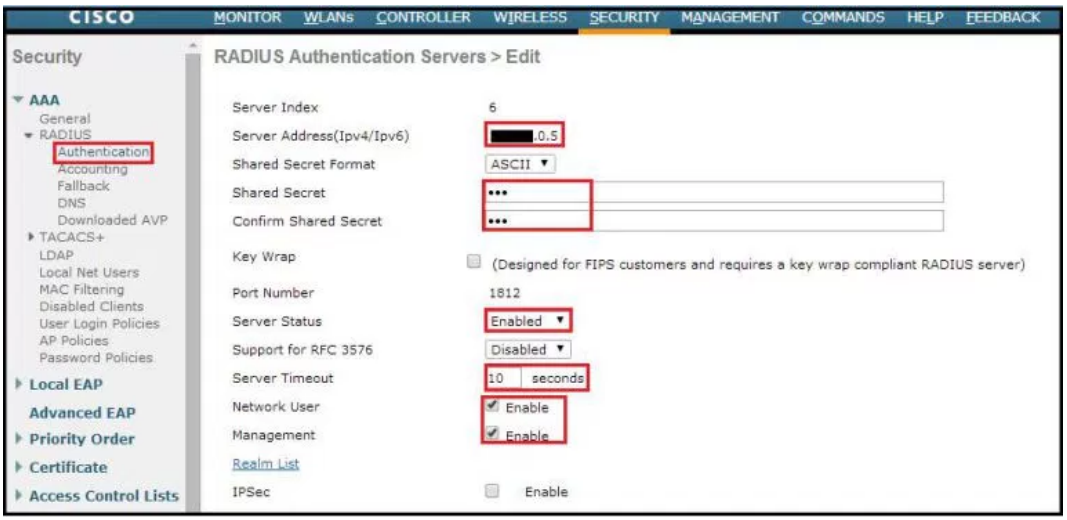
Let's add a 5508 controller onto ISE as managed network device. I have created a WLC "Device Type" group to better control similar type of devices.



You have to use same "Shared Secret" when configuring RADIUS server on WLC as well.

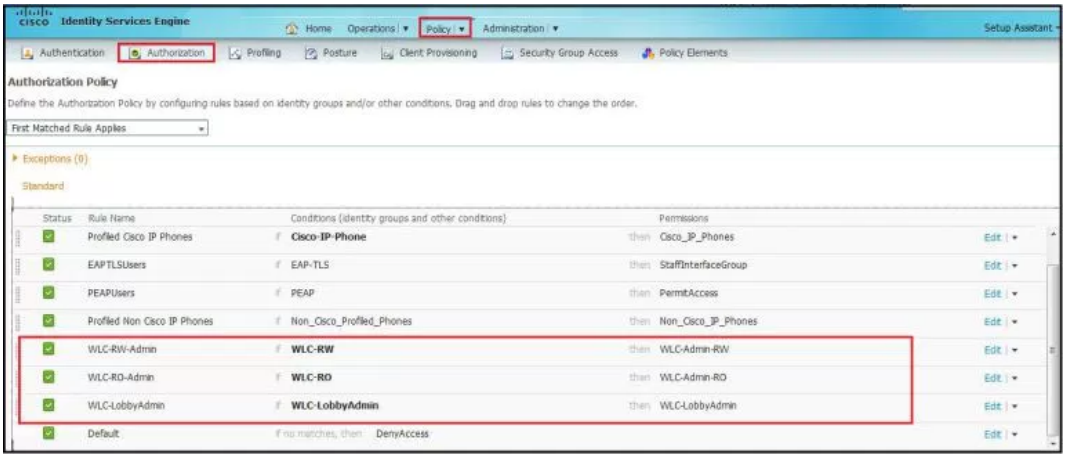


Here is the WLC RADIUS Server configuration Settings, You have to remember to tick "Management User" option here.



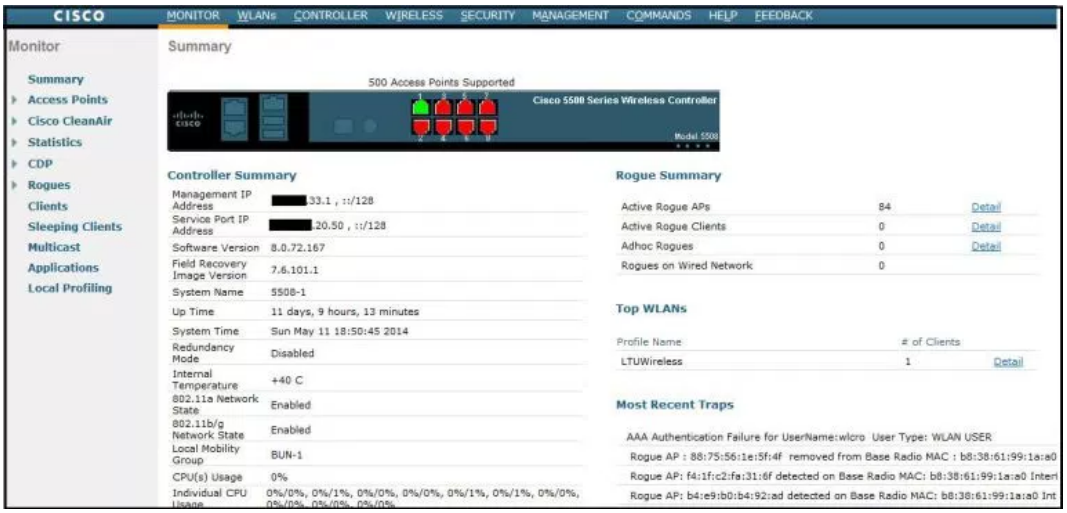
Then I have create a simple "Authentication Policy" to use "Internal User". Since default policy also to point to "Internal Users" this step may be optional.

Finally you need to create a "Authorization Policy" for each type of use case selecting the different "Authorization Profiles" you created.



Now it is ready to test. If you access the WLC via "https://wlc-mgt-ip" URL & when prompt, if you enter user1 (WLC Lobby Admin user) credential you will see something like this.

If you use "wlcro" Read-Only user credentials you will see a output like below. It is very similar to full WLC access view, but if you try to modify some changes using this credential it should prompt user does not have sufficient privileges.



Here is the output when I try to disable a SSID using this login.

If you use "wlcrw" credential you will have the full administrative access of the WLC.

Remember that this will applicable for any AireOS WLC (5508, 2504, WiSM2,etc) & not applicable for Next Gen IOS based WLC (5760,3850,3650). For those IOS based controllers you can restrict device CLI access (Privilege level 15 for full access, Privilege Level 1 for minimum access) via RADIUS. I do not see a way of controlling WLC access (https://device-mgt-ip/wireless) via RADIUS.

PS: Thanks to Gaith Alrawi (CCIE#23006 Sec, Wireless) for helping me on this topic.

Related Posts

1. WLC access via TACACS
2. WLC access via RADIUS (ACS 5.2)

thoughts on "WLC Access via RADIUS (ISE)"

1. *said:*Zusugi

   June 6, 2014 at 11:29 pm

   Very useful and works fine. Thank you for a good article!

   REPLY

   - ***said:*nayarasi**

     August 1, 2014 at 3:19 pm