Infoblox NetMRI with Cisco ACS 5.x for TACACS+.
Comments: Adam Obszynski <**aobszynski@infoblox.com**>

For Cisco ACS 5.x (VM or HW Appliance based) you need to use IE or Safari. Firefox and Chrome tend to not render all policy editor fields on web GUI.

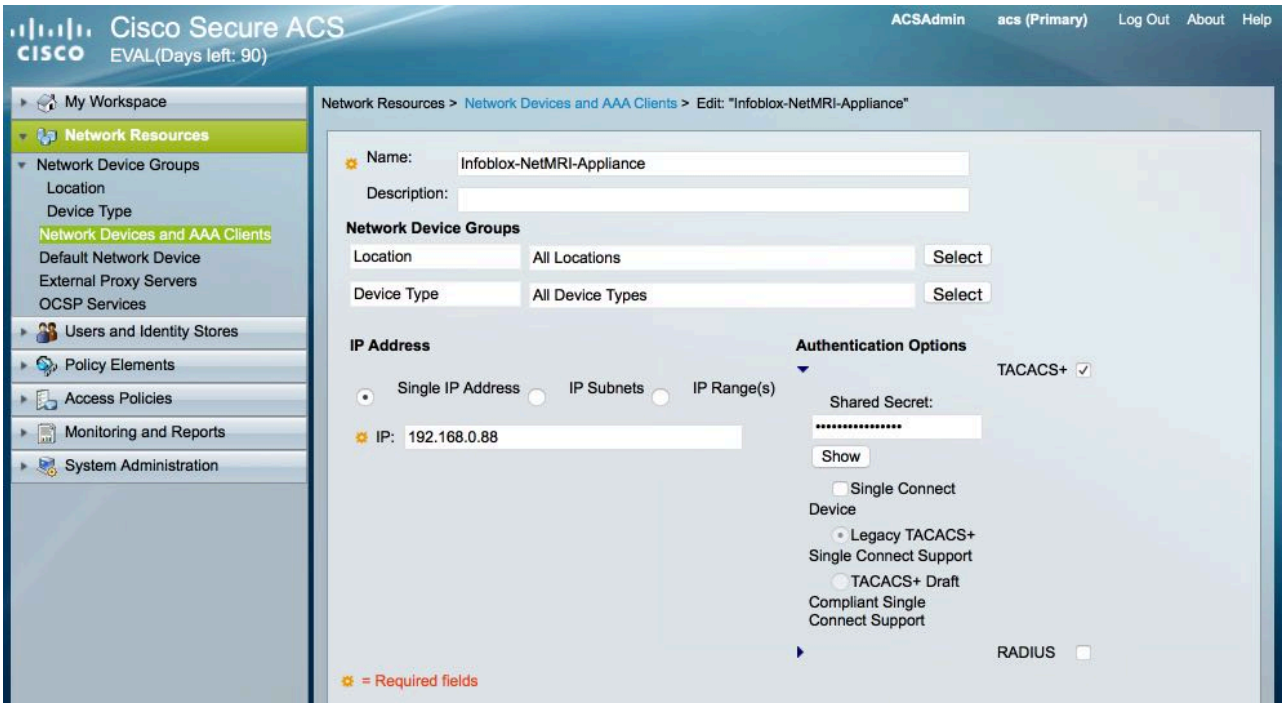
Settings on ACS environment can vary between different environments. But ACS admin who uses the system on daily basis will know how to use mentioned here directions.

AUTHENTICATION

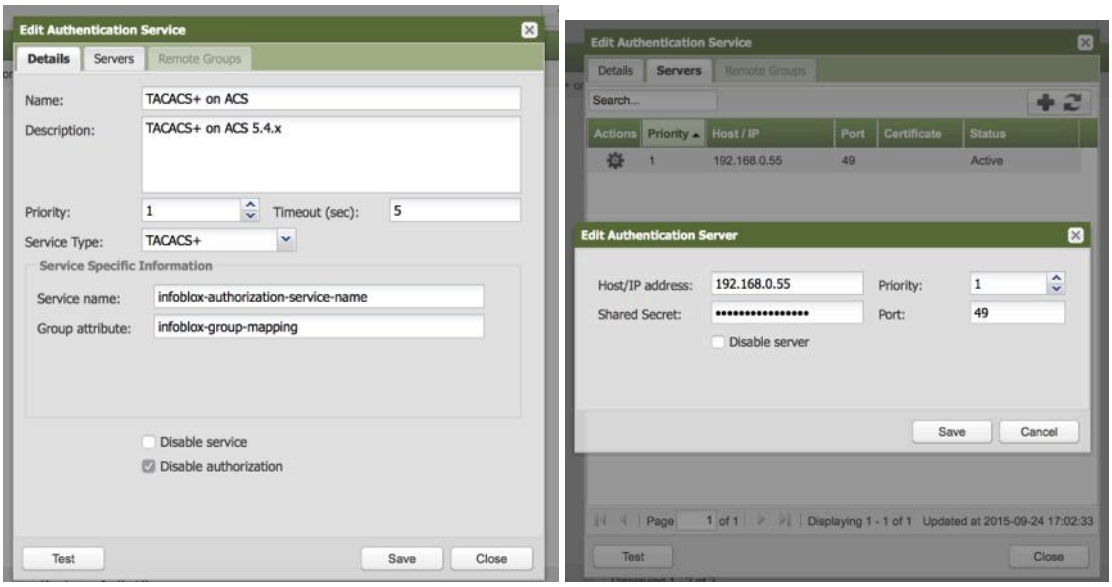
To simply authenticate users You need to define NetMRI IP as TACACS+ enabled device and define shared password that will match on both sides – NetMRI and ACS.

In ACS GUI go to
Network Resources > Network Devices and AAA Clients and click **Create**

Enter NAME and Single IP Address fields. Be sure that TACACS+ is checked and Shared Secret is same as on NetMRI.



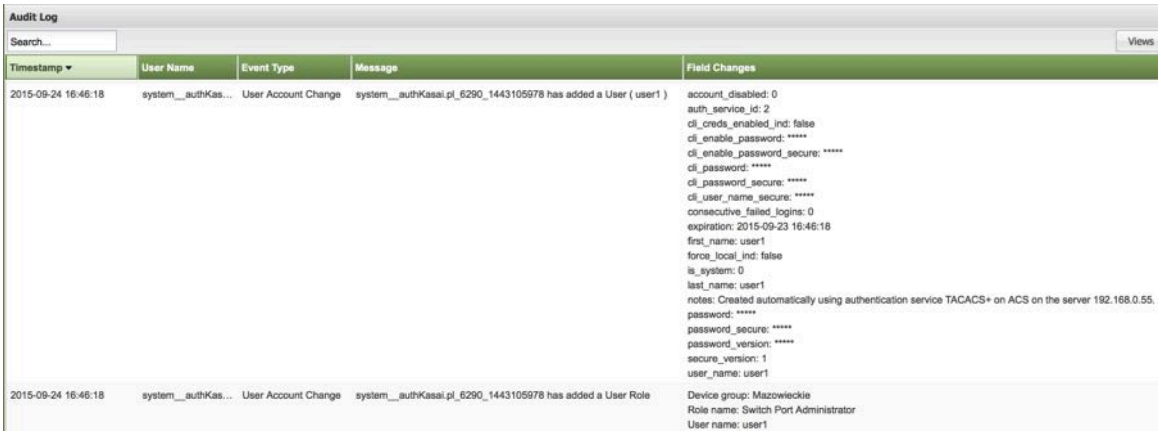
On Infoblox NetMRI side you need to have TACACS+ server defined and Authentication DISABLED until you want to use it (next paragraph).
Service name and Group attribute will be important for authorization settings – enter anything you want.



Test button gives you option to test credentials and confirm if TACACS+ works correctly.

AUTHORIZATION

Adding authorization to the NetMRI configuration will allow you to have automatic user creation after successful authentication if user group will be matched. Sample audit log bellow.



On NetMRI side you need to uncheck “Disable authorization” in TACACS+ settings window. Then define “Service name” as infoblox and “Group attribute” to value that will be used inside ACS settings. In example below I’m using “infoblox-group-mapping”.

After saving this settings “Remote Groups” tab will become active.
Define group/role mapping you want to achive.

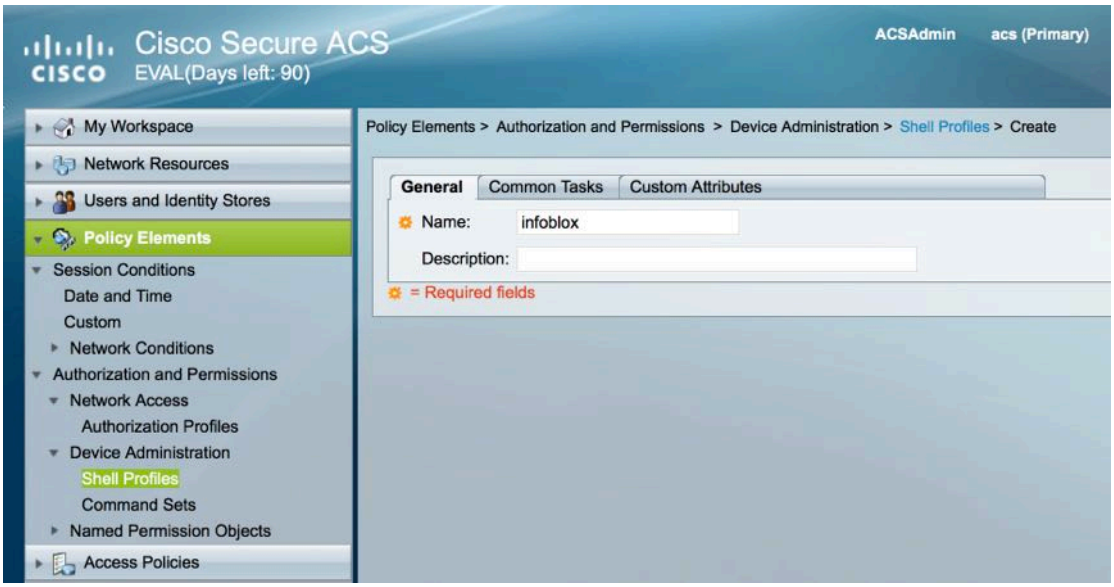
In my example:

Remote group called BLOXERS2 is created on ACS to authorize user into group SPM Admin. Important thing to remember is that you need first enter Remote Group name and Save. Only then you will be able to add NA Roles to entered Remote Group.

Now time for ACS side.

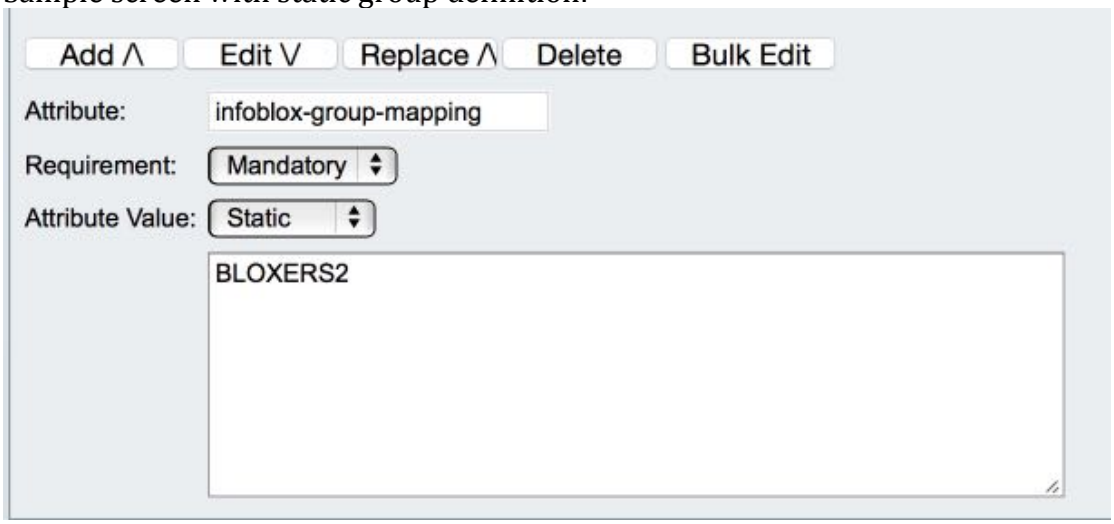
Go to **Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles**, then Create

In General/Name enter profile name ie. “infoblox”.



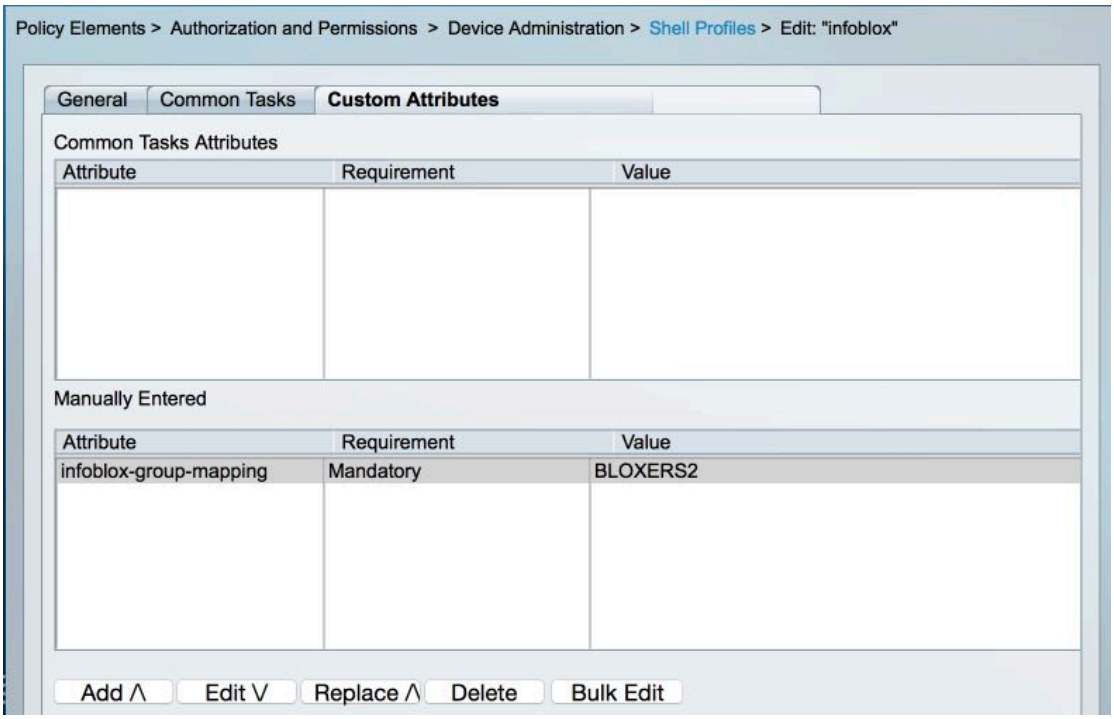
Then in Customer Attributes tab define attribute that will define group mapping. In my example there is static definition. When ACS is using external MS Active Directory you can use Dynamic settings for Attribute Value to use Group from AD structure.

Sample screen with static group definition:



Please remember to add value by clicking “Add /\” button, then Save.

Final view:

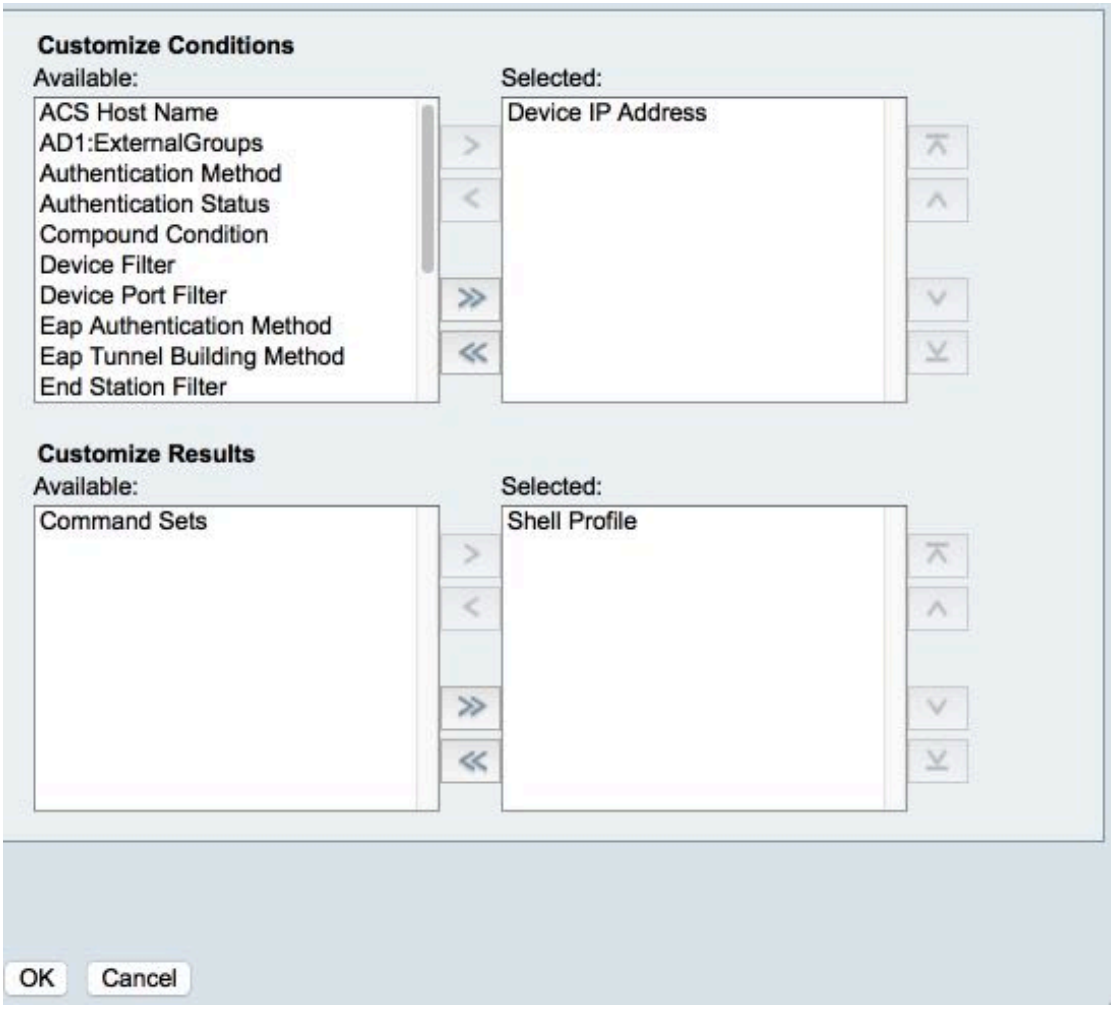


From that point setting may be different for each customer. Data provided below is from simplified LAB environment.

Go to **Access Policies > Access Services > Service Selection Rules**
Select Single checkbox and select **Default Device Admin** from drop down menu.

Go to **Access Policies > Access Services > Default Device Admin > Authorization**

Click "**CUSTOMIZE**" button and check/add Device IP Address and Shell Profile are available for selection. Close windows by using OK button.

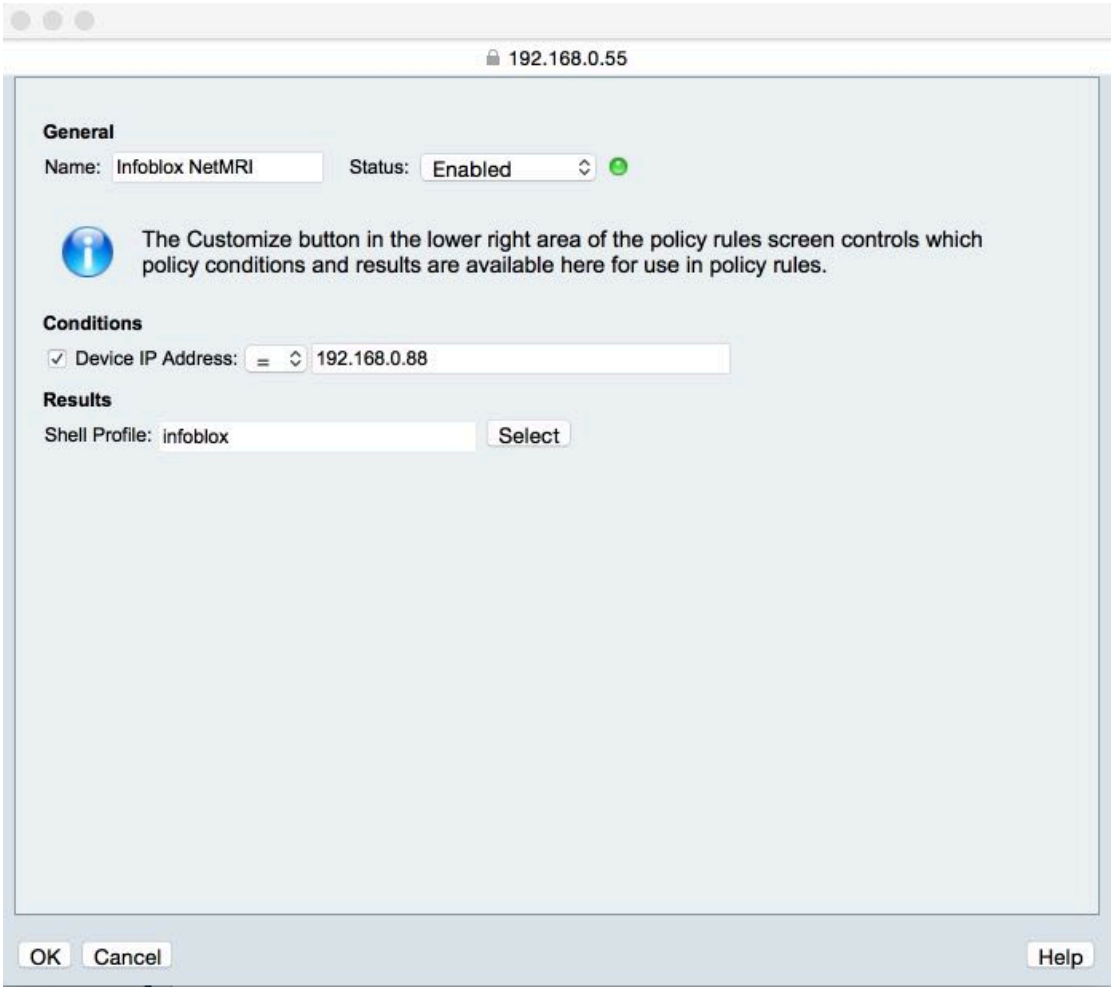


Then click **Create**.

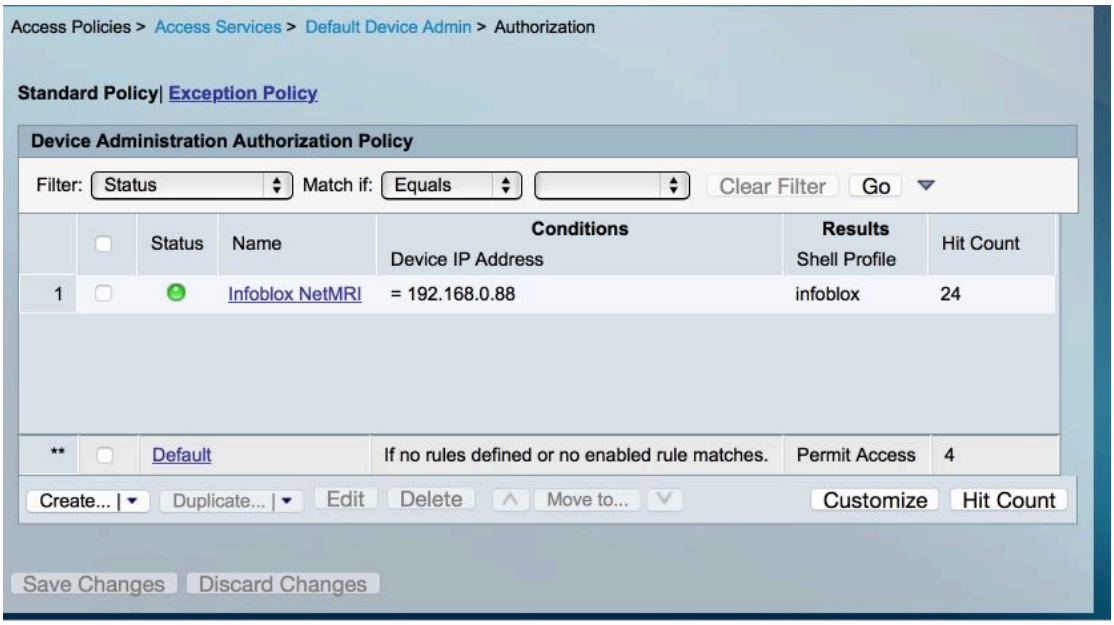
WARNING: In unsupported browser Create button will be greyed out! For me Windows-IE and MAC-Safari worked fine. Firefox & Chrome didn't.

Under **General**, name the new rule ie. Infoblox NetMRI and ensure that it is enabled.
Under **Conditions**, select the checkbox next to **Device IP Address**, and type the IP address of the NetMRI appliance (in my case 192.168.0.88)

Under **Results**, click the **Select** button, located next to the **Shell Profile** field, and select one you created earlier (in my case infoblox), and click OK.
Click OK to close the window.



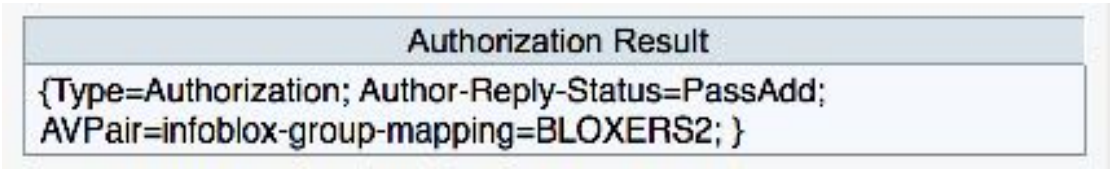
Click Save Changes, located at the bottom of the page.



On ACS you can check if ACS auth. works in Monitoring and Reports menu. Then on Dashboard of Viewer window look for “Authentications - TACACS – Today” Report.

To get details about what Authorization data was sent to NetMRI you need to expand tree view Reports -> Catalog -> AAA Protocol and select TACACS_Authorization report.

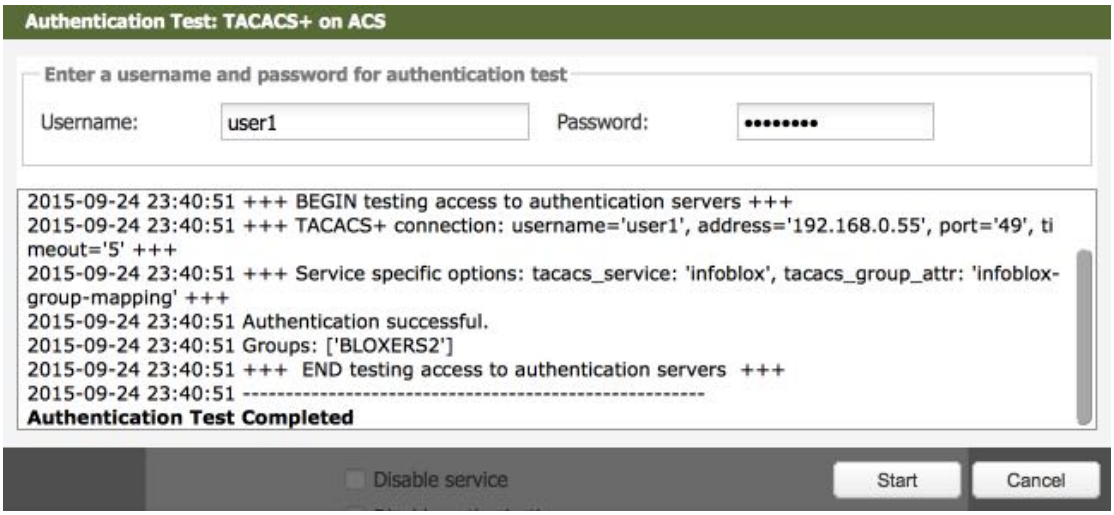
In the right upper part of user session you will see result with mapping:



Finally time to test it on NetMRI.

Go to Settings -> Authentication Services and edit TACACS+ profile you created already.

Using TEST button you can confirm final mapping working fine:



Well DONE!