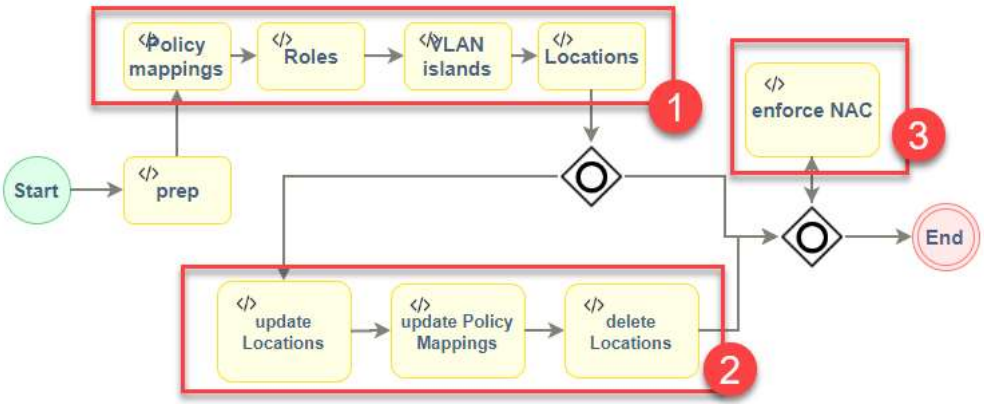
Workflow description

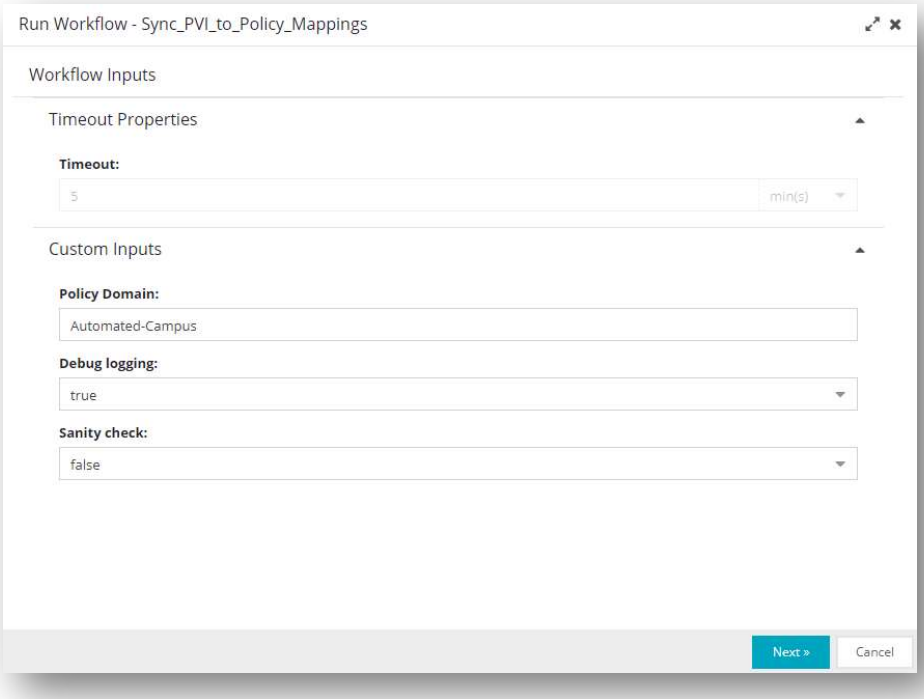
Sync Policy VLAN Islands to Policy mappings

This workflow address the need to using XIQ-SE NAC Policy based VLAN islands designed for Switch Engine (aka EXOS) for Fabric Engine (aka VSP). The Fabric Engine can't use VLAN Island it by design but Policy mappings to achieve the same. This workflow translate the VLAN Island settings to Policy Mappings.



The workflow is based on three phases. The prep activity put in place the required Python classes (common libraries) to support the code optimization in all the other activities. Phase one is reading all data. Phase two apply the changes if required. If a changed recognized, phase three takes care that the NAC engines gets enforced.

If you kick the workflow, the workflow will prompt you to provide Policy Domain. The other parameter are for test and debug propose only. The **Sanity check** will not change anything (dry run).



The workflow global variables contains two variables you adapt for your needs. First is the Engine group which get used for enforcement.

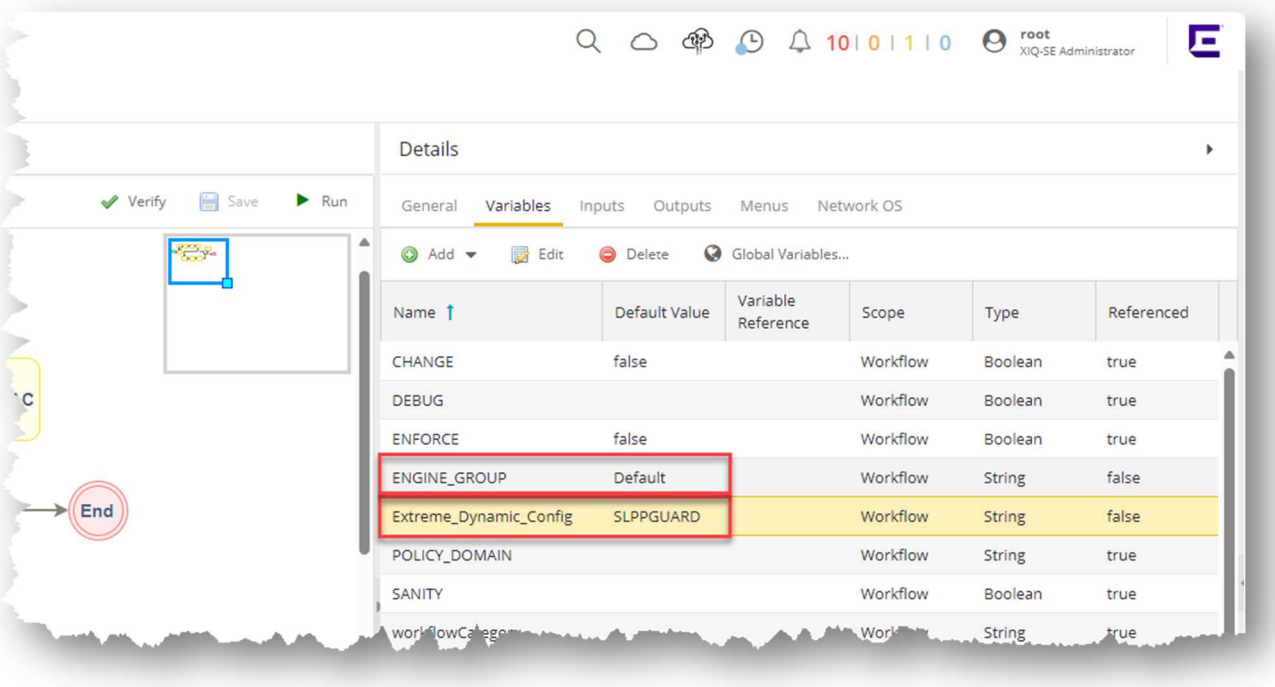
As well return attributes used for all policy mappings. The example blow shows the **SLPPGUARD** will be enabled. The used final Radius return attribute looks like this:

Extreme-Dynamic-Config=SLPPGUARD

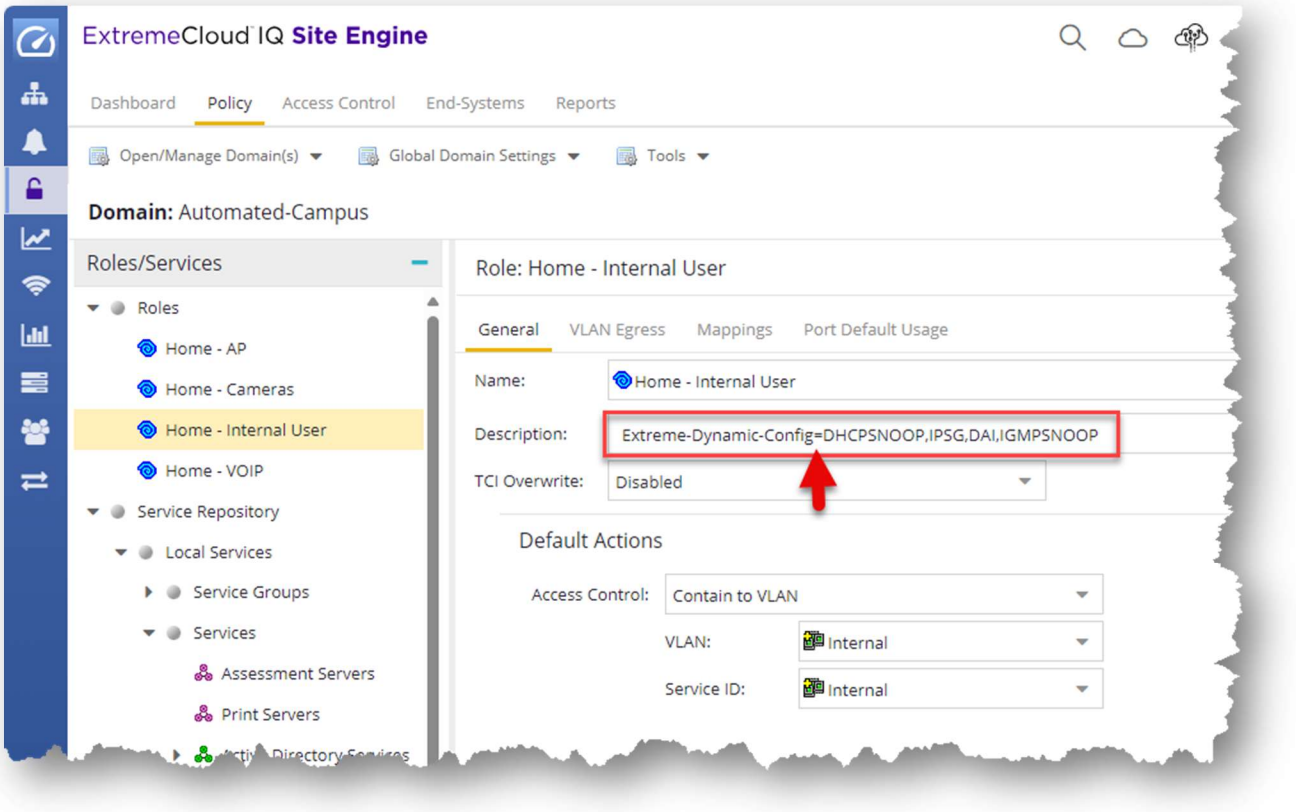
It can be also be provided a list like **SLPPGUARD,DHCPSNOOP,DAI** to enable more than one parameter. It will end up in his return attributes

Extreme-Dynamic-Config=SLPPGUARD
Extreme-Dynamic-Config=DHCPSNOOP
Extreme-Dynamic-Config=DAI

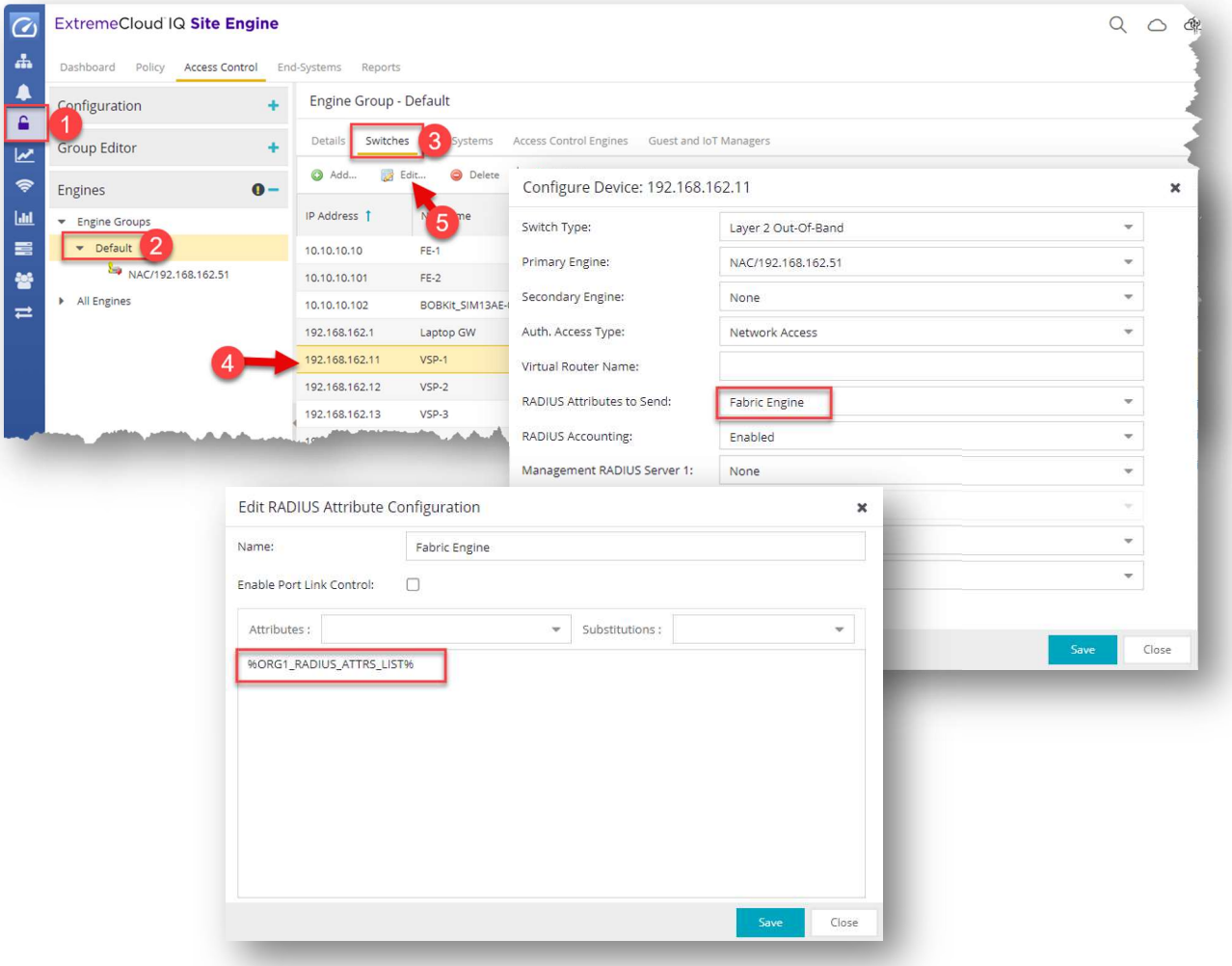
Just be aware, it applies to all policy mappings.



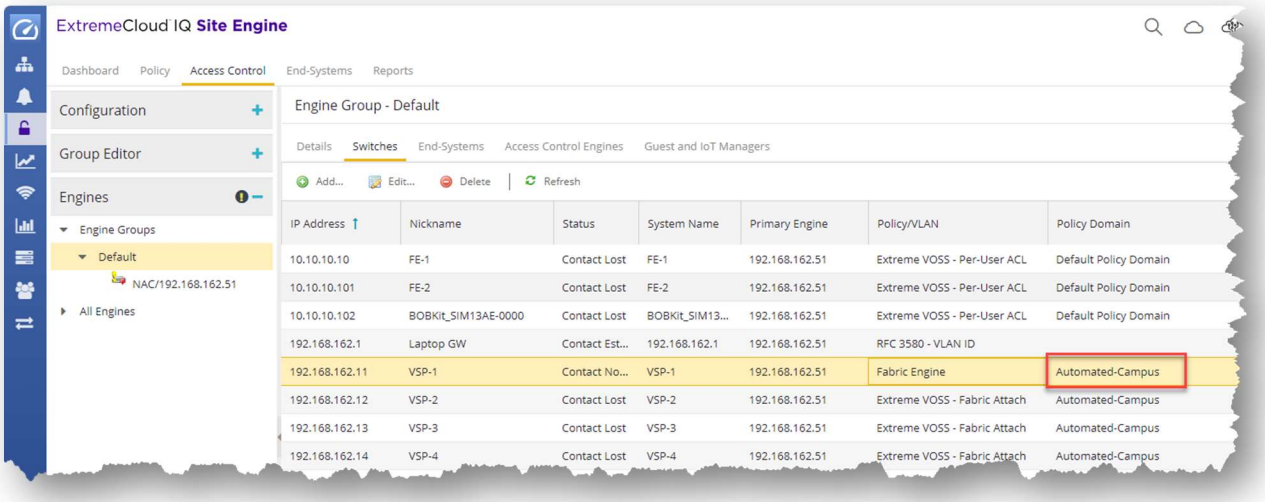
Alternative you can specify on each policy role description alternative the same settings, but specific to the role only.



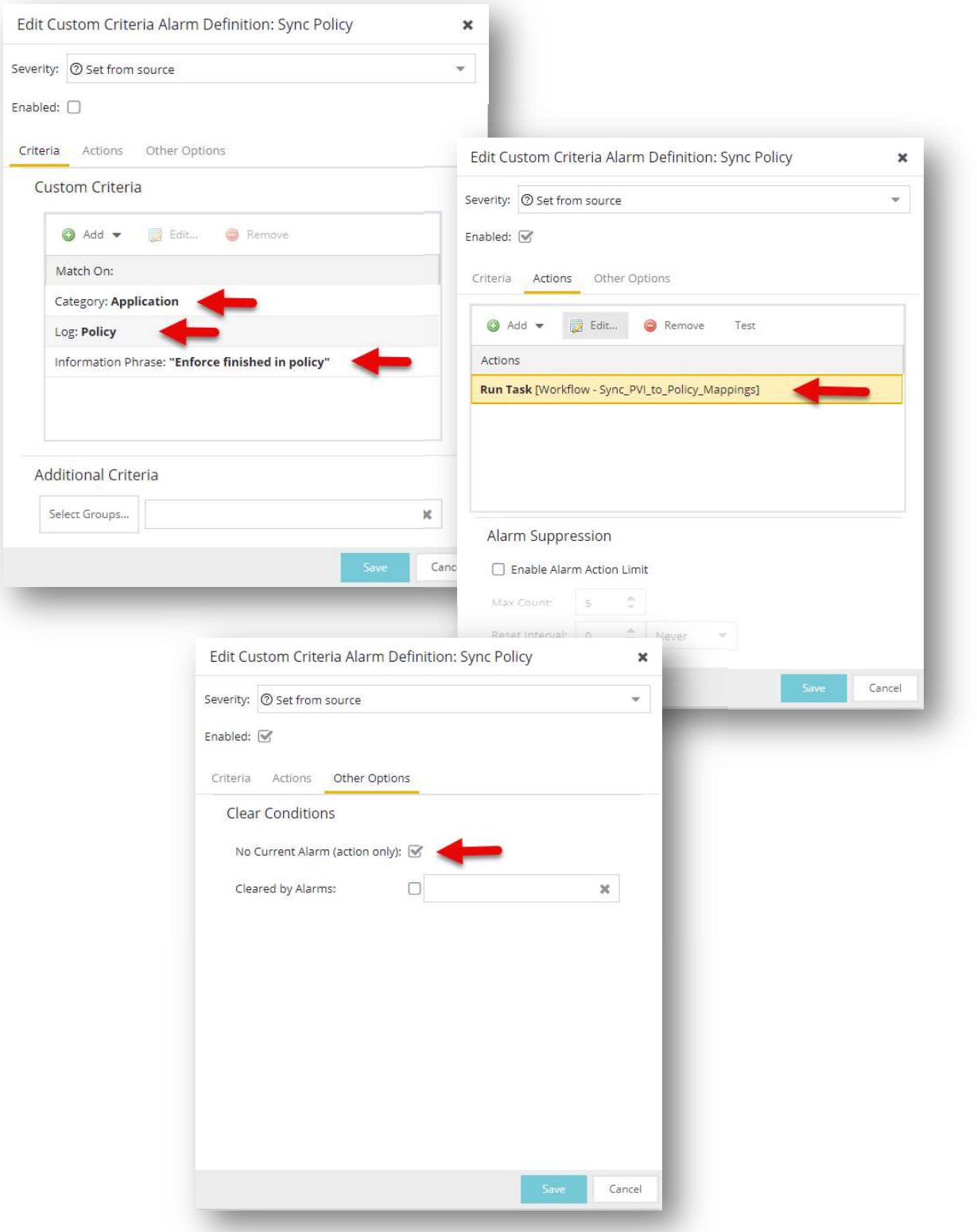
The switch setting shave to be configured like this



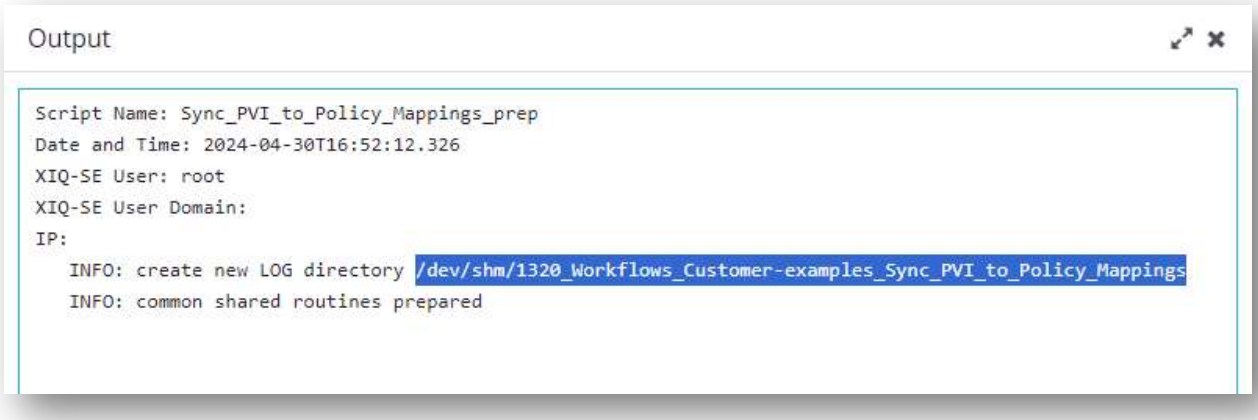
Make also sure that the right Policy domain is used.

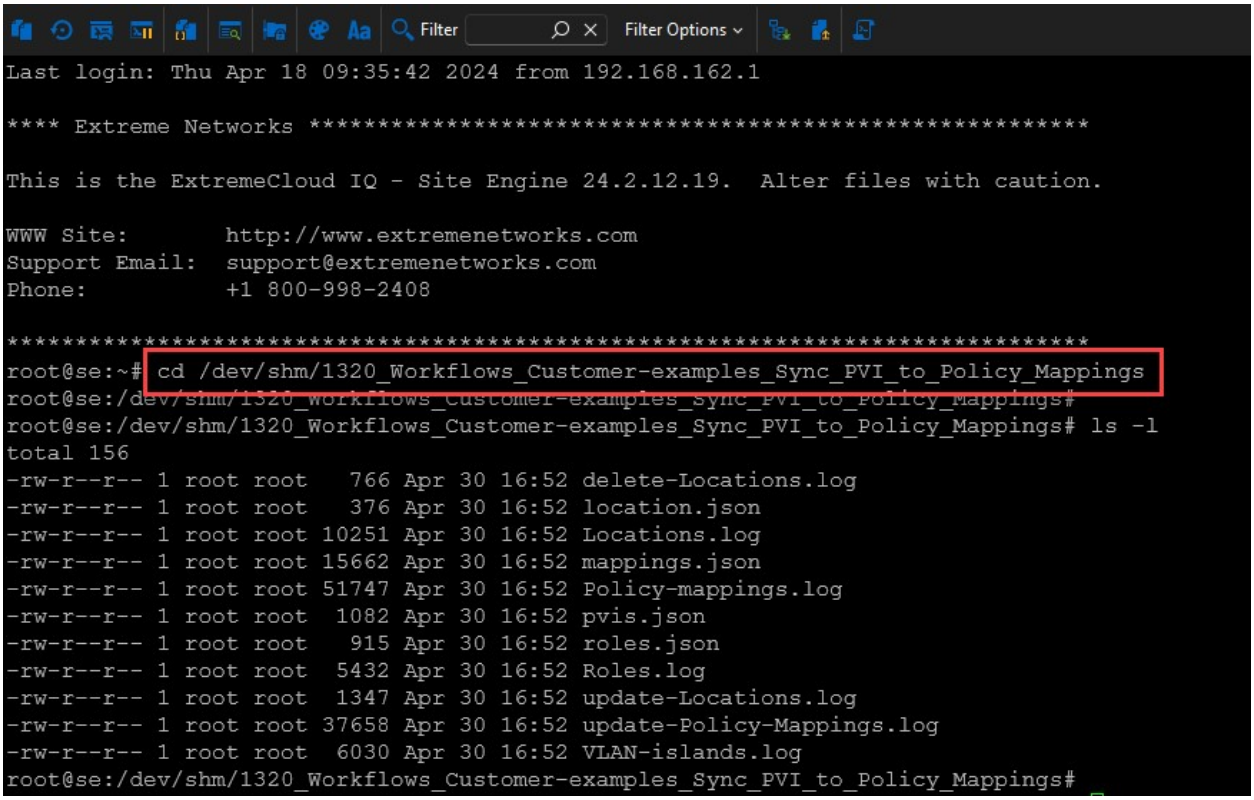


The workflow can be automatically triggered of the policy get enforced to keep in sync as best as possible the policy mappings. Just setup an alarm like this:



In case of issues, make sure you let run the workflow in DEBUG mode. The data and LOG files you will find on the file system under **/dev/shm/<Execution-ID>_<Workflow-Name>/** . The last six execution will be kept. Older ones will be wiped. In each activity you will find the detail path to the LOG file





Please note, this workflow is inspired and prototyped by **Jeff Datti**lio from **STEPCG**