Workflow description

Sync Policy VLAN Islands to Policy mappings

Credits: this workflow was inspired and prototyped by **Jeff Dattilio** at **STEPCG**.

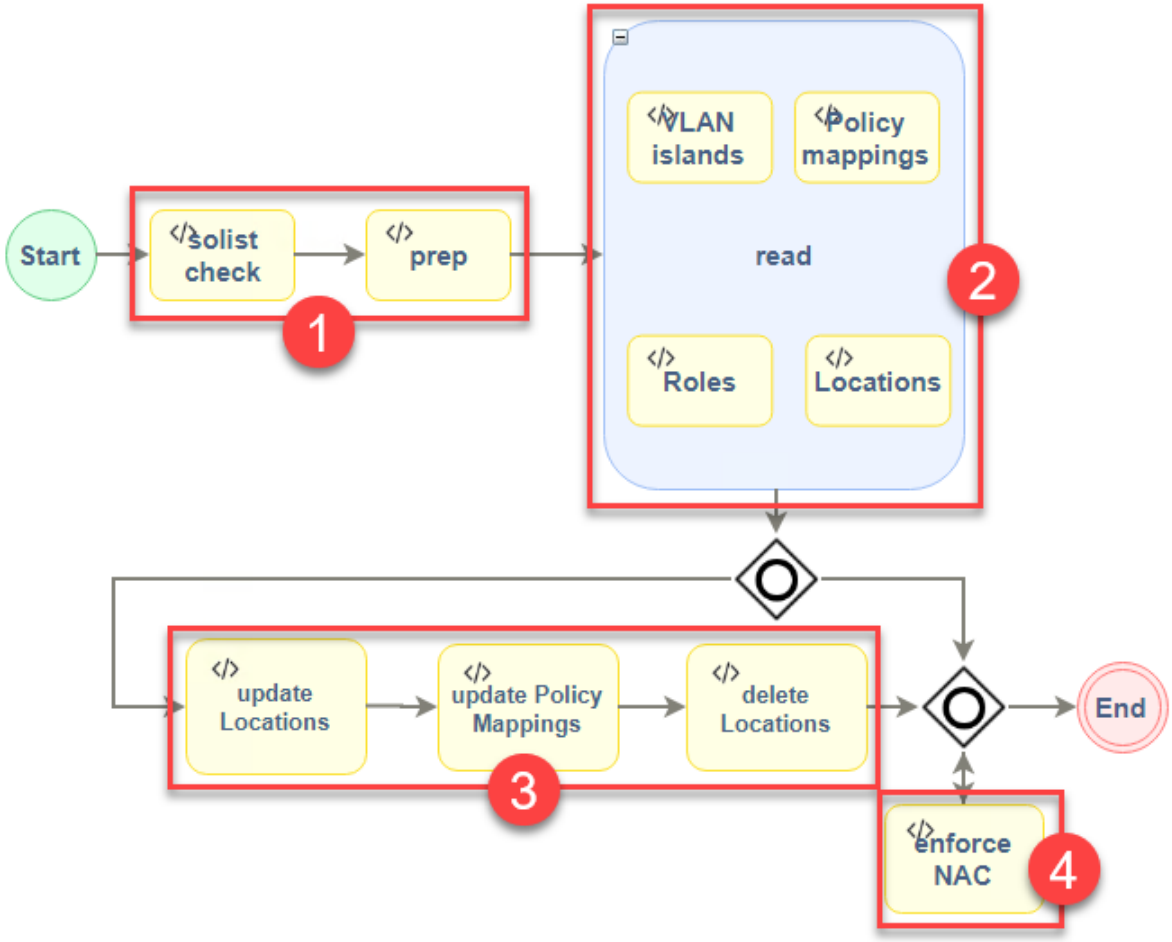
This workflow addresses the need to use XIQ-SE NAC Policy-based VLAN islands with Fabric Engine (aka VSP).

The native XIQ-SE VLAN Island functionality only caters for Policy roles applied to Switch Engine (aka EXOS), where the VLAN Islands are resolved during the Policy Enforce action, and each and every Switch Engine switch in the Policy domain gets the Policy Roles pre-pushed with the appropriate VLANs based on the VLAN Island topology. When a user is authenticated, the Control Engine RADIUS server simply returns a filter-id RADIUS VSA with the applicable Policy role name.

But with Fabric Engine, when a Policy is enforced, each role only has one VLAN/I-SID binding enforced, not to the switch but to the Control Engines, and there is no logic here for handling VLAN Islands. When a user is authenticated, the Control Engine RADIUS server returns a single VLAN/I-SID binding, which has no correlation with the VLAN Island configuration. The Policy VLAN Island user interface can still be configured, just that it will not work as expected when an end-station is authenticated on a Fabric Engine switch.

This workflow examines the Policy VLAN Island configuration and translates it into equivalent Access Control Policy Mappings to achieve the same desired outcome of the Policy VLAN Island configuration. The user can now configure Policy VLAN Island as before, and have these operate as expected not only with Switch Engine but also with Fabric Engine access switches.

Sync Policy VLAN Islands to Policy mappings



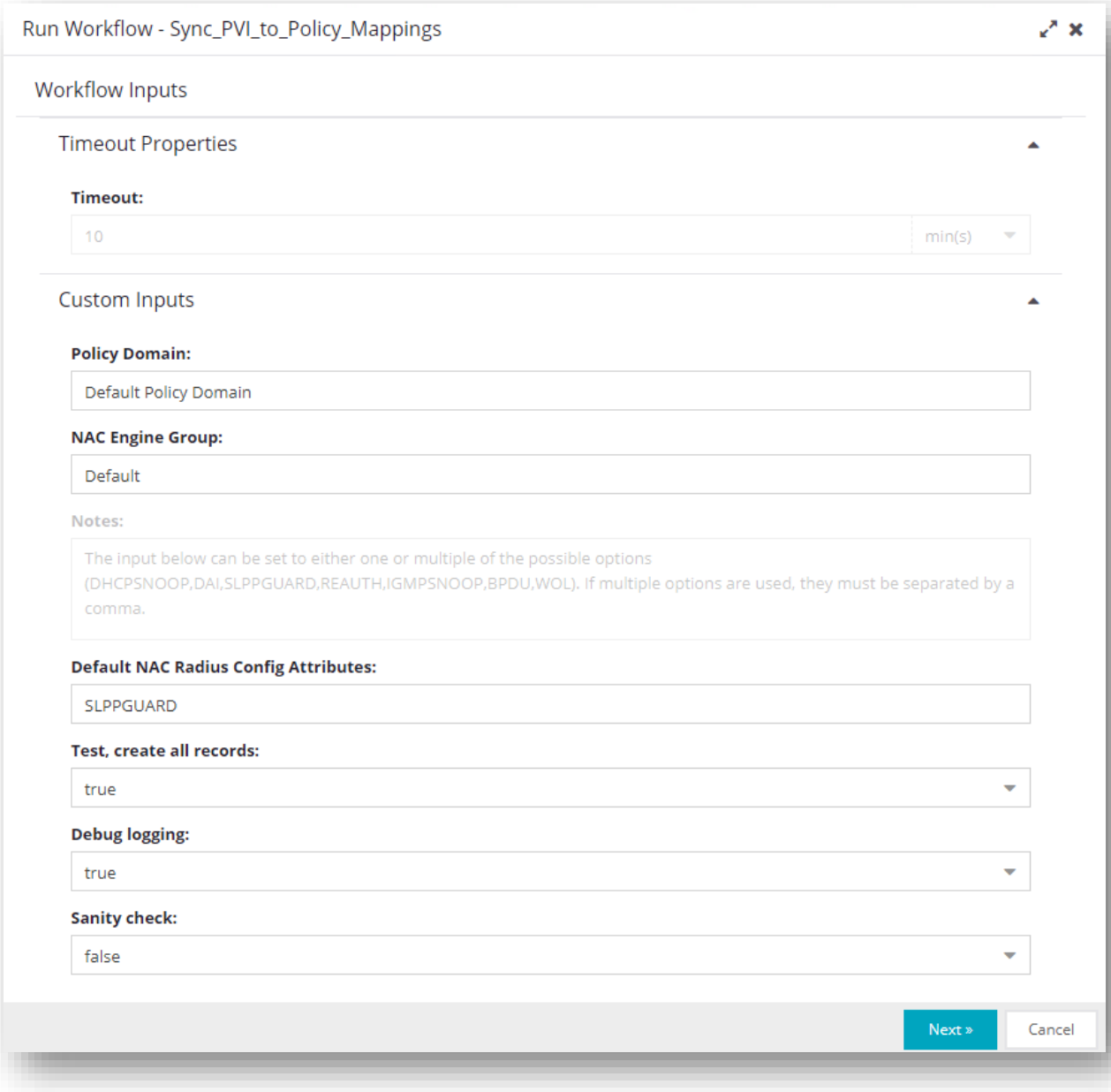
The workflow consists of four phases. The first phase involves preparing the necessary Python classes (common libraries) to support code optimisation throughout the subsequent activities. Phase two focuses on reading data from various modules. In phase three, any required changes are applied. Finally, in phase four, if any changes are made, the NAC engines are enforced to ensure changes are activated immediately.

When launching the workflow manually, it prompts for the Policy Domain, NAC Engine group, and default Radius attributes. The other parameters are intended solely for testing and debugging. The sanity check will not make any changes (dry run).

The NAC Engine Group can be empty to enforce all, or a single NAC engine or a comma-separated list of NAC engines.

The same inputs can also be saved on the workflow itself under the Inputs tab.

Sync Policy VLAN Islands to Policy mappings



The Default NAC RADIUS Config Attributes input is used for all policy role mappings. In the example shown, **SLPPGUARD** will always be activated. Thus, the final RADIUS return attributes will include this:

Extreme-Dynamic-Config=SLPPGUARD

The same input box can, however, also accept a comma-separated list of attributes, such as SLPPGUARD,DHCPSNOOP,DAI, to enable multiple parameters. In this case, the return attributes will include this:

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

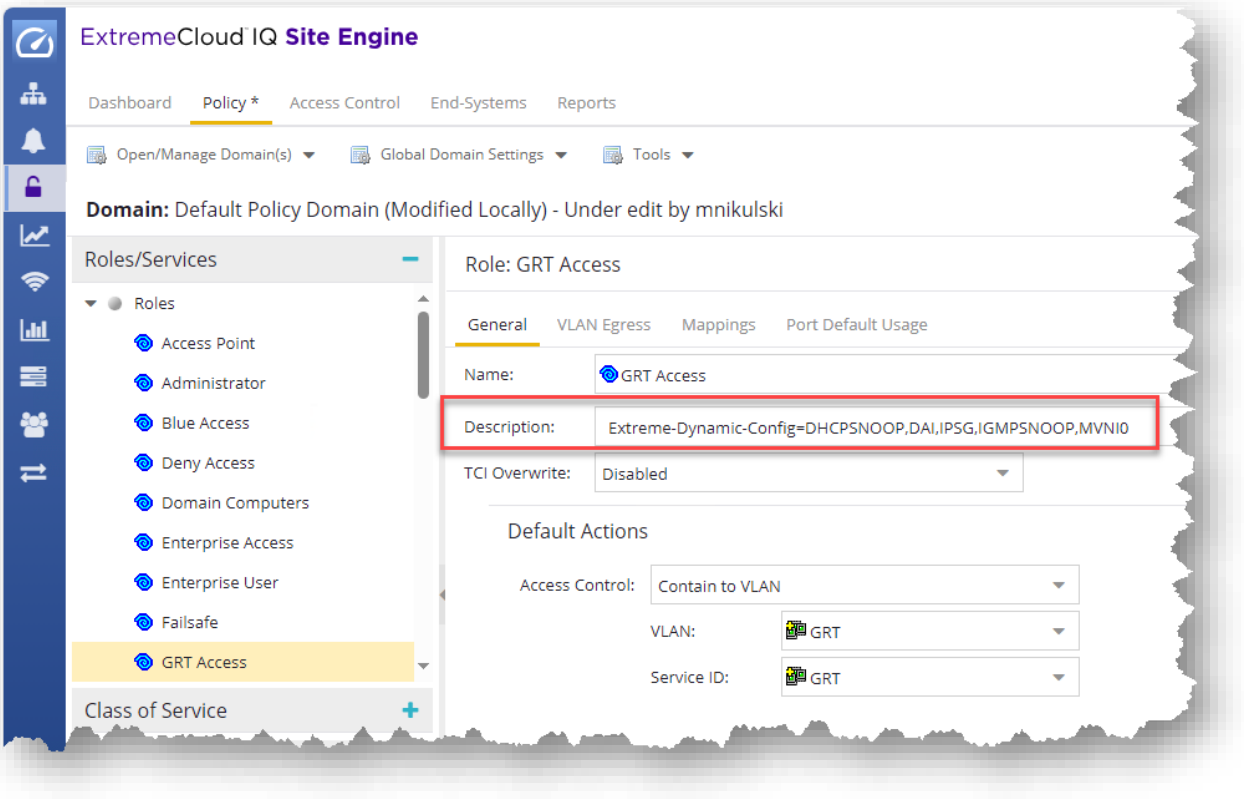
Sync Policy VLAN Islands to Policy mappings
However, entering these attributes in the workflow's input will result in these RADIUS attributes being sent for all Policy Role mappings.

If a policy role should not be synchronised, use the keyword **NO-SYNC** in the description. This keyword has the highest precedence compared to other keywords.

If **TEST creates all records** equal **true**, everything gets created, even if there is no switch assigned to a VLAN Island topology (location). If this parameter is **false**, it will only create what is in use and delete what is no longer in use.

Where it makes more sense to set the return RADIUS attributes at the Policy Role level, the workflow augments the use of the Policy Role Description field, which can now be used to convey the same selection of RADIUS attributes specifically for the single Policy Role.

The global and role-specific attributes will ultimately be combined once the workflow creates or updates the final Policy Mappings.



The possible attribute keywords accepted are:

SLPPGUARD, REAUTH ,BPDU ,WOL ,DHCPSNOOP ,DAI ,IPSG ,IGMPSNOOP ,MVNI<I-SID> ,PVLAN<SecVID>

Note that a couple of these keywords are not actual RADIUS VSAs but provide a way to control how the workflow will encode the Extreme-Dynamic-Client-Assignments VSA, which is always sent. These are:

Sync Policy VLAN Islands to Policy mappings

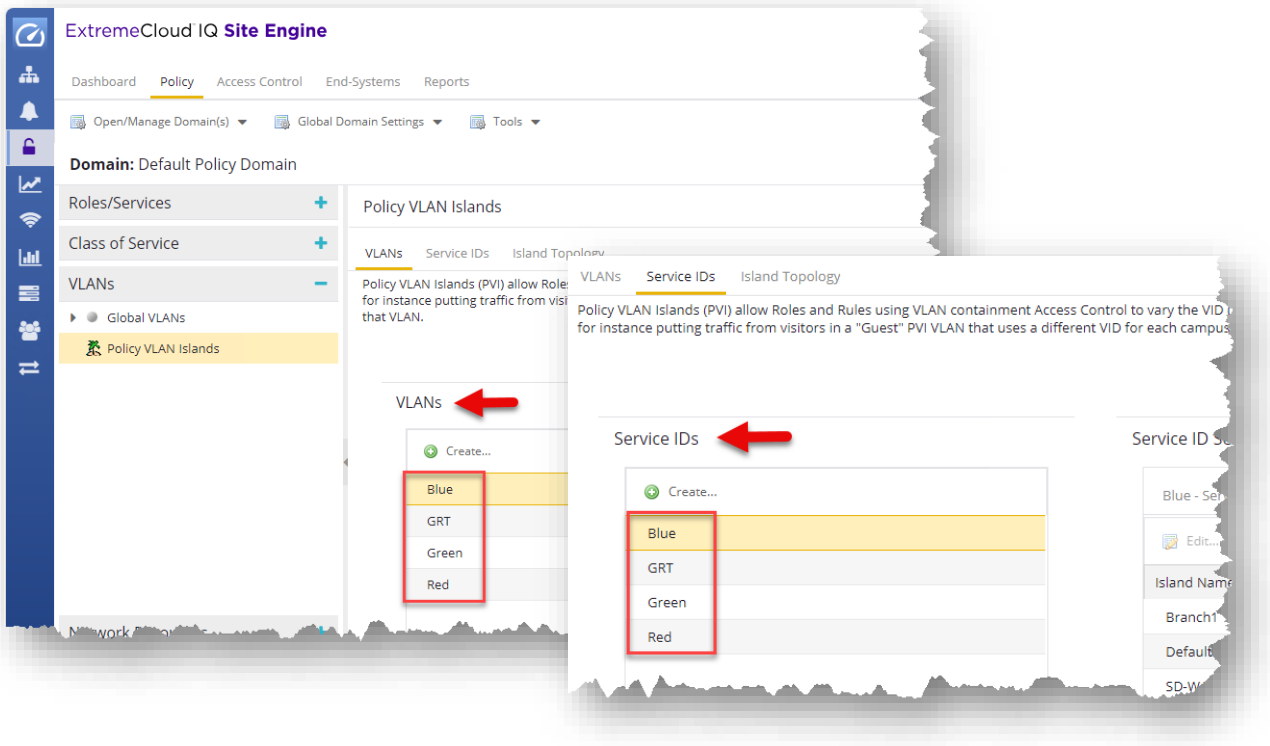
- **MVNI<I-SID>:** This enables Multicast support on the L3 I-SID context provided as <I-SID>. This will result in “mvni=<I-SID>” being added to the Extreme-Dynamic-Client-Assignments VSA. Use 0 for GRT context, and a non-zero value for VRF L3VSN IPVPN context.

- **PVLAN<SecVID>:** This will result in the Extreme-Dynamic-Client-Assignments VSA going out with “create=pvlan” and “sv=<SecVID>”, in addition to “pv=<PriVID>” which is also always added when the “create=” switch is present. The end result is that a PrivateVLAN (ETREE) service will be created on the Fabric Engine access switch.

The **DHCPSNOOP, DAI, IPSG, IGMPSNOOP, MVNI<I-SID>, PVLAN<SecVID>** keywords will all result in the Extreme-Dynamic-Client-Assignments VSA creating a platform VLAN on the switch in addition to the switch-UNI binding on the port where the end-station is authorised.

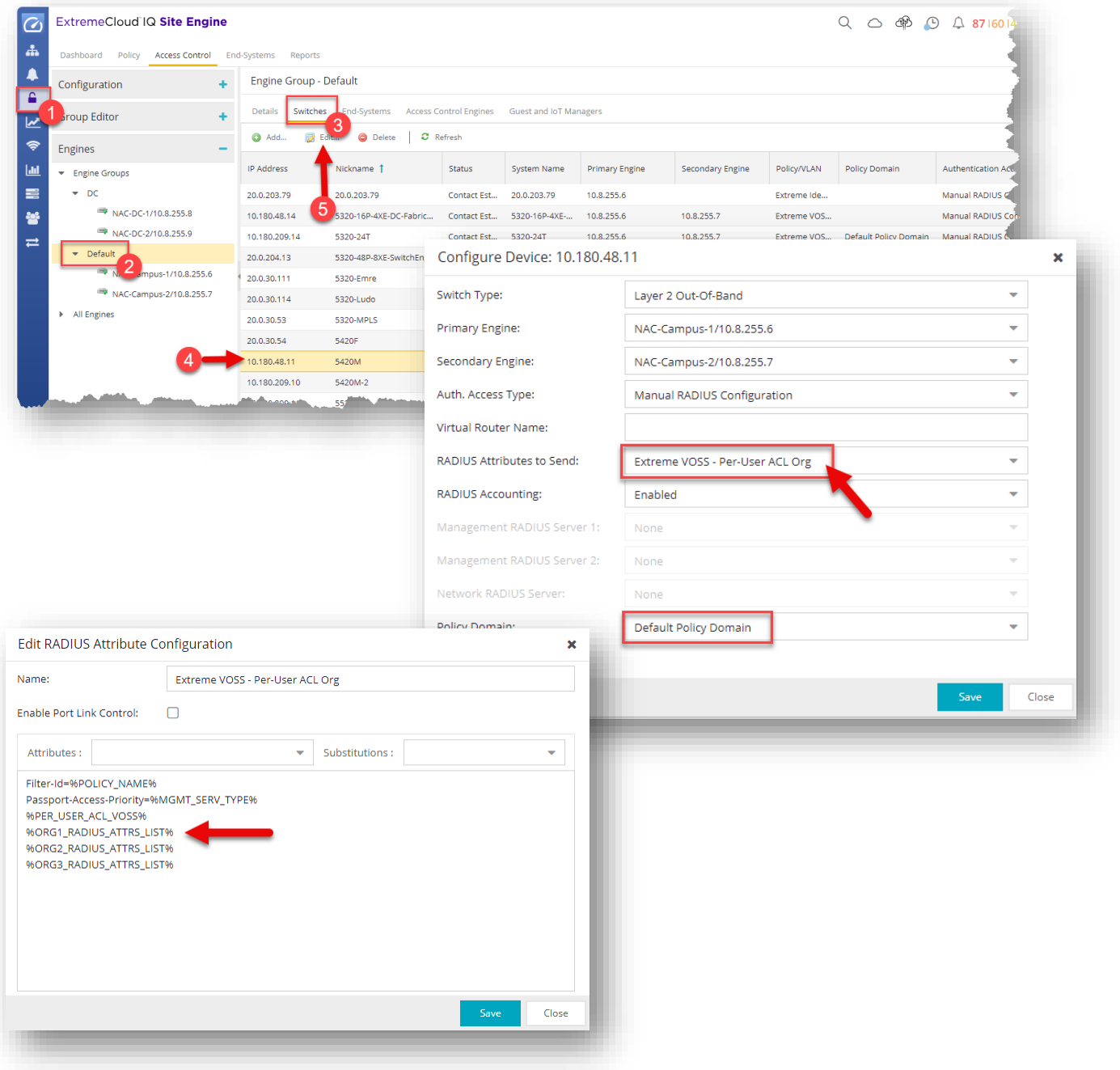
Whereas if none of those keywords is present, the Extreme-Dynamic-Client-Assignments VSA will be sent without the “create” option, and only a switch-UNI binding will be created on the port where the end-station is authorised.

Please note that it is very important to use the same VLAN and I-SID (Service ID) name. Otherwise, the workflow will result in an error during updating the policy mappings (key error)



Sync Policy VLAN Islands to Policy mappings

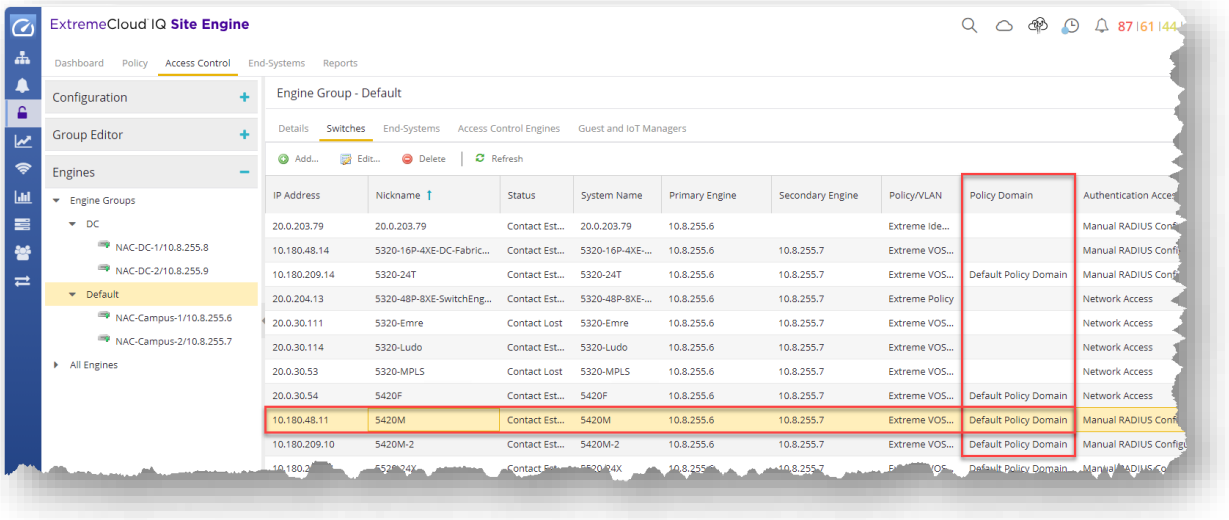
The workflow will always create the RADIUS VSA attributes in the **Organization 1** field of the Policy Mapping profile. It is therefore important to make sure that the switch RADIUS attribute template includes %ORG1_RADIUS_ATTRS_LIST%



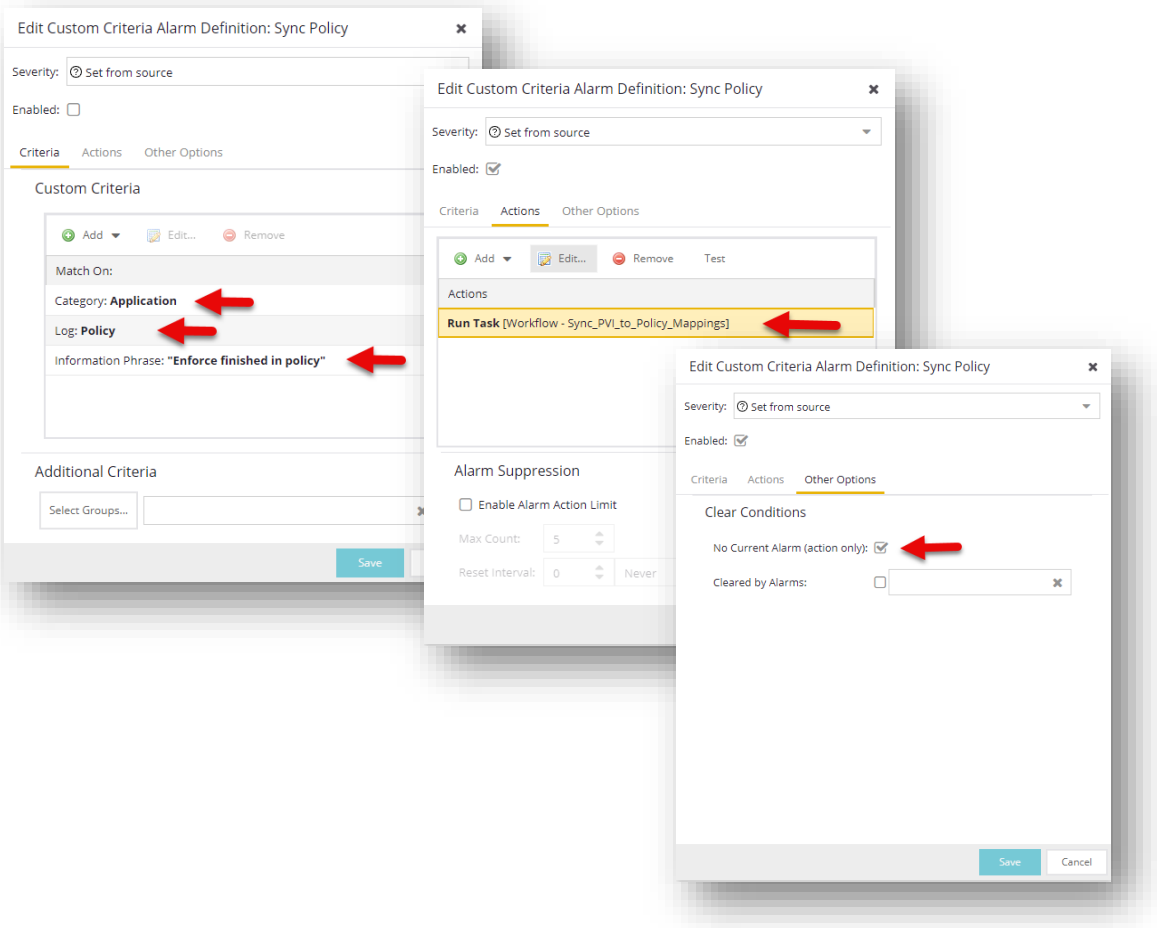
To manually add other RADIUS return attributes besides the ones automatically produced by this workflow, %ORG2_RADIUS_ATTRS_LIST% and %ORG3_RADIUS_ATTRS_LIST% can also be added in the RADIUS template.

Sync Policy VLAN Islands to Policy mappings

It is also important to make sure the switch is assigned to the correct Policy Domain under Access Control.

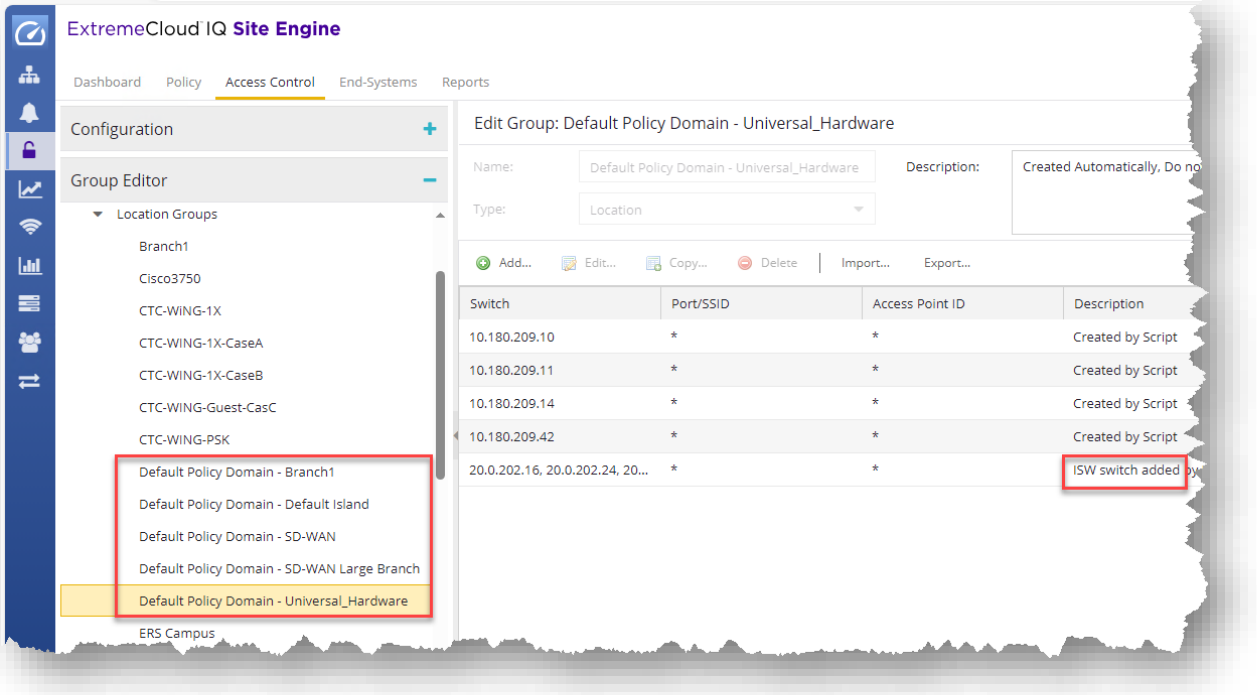


To seamlessly integrate the workflow with how the user normally operates the Policy Domain, it can be setup to be automatically run whenever the user clicks on the Policy Enforce button. To do so setup an alarm as follows:

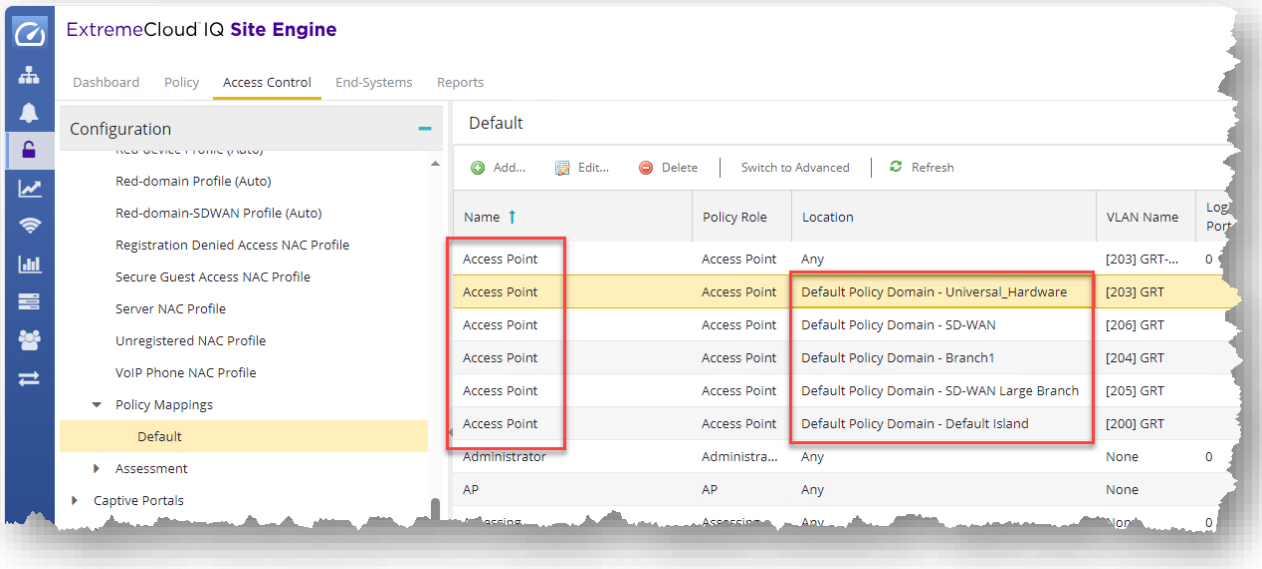


Sync Policy VLAN Islands to Policy mappings

Here are more details on the profiles the workflow will create. One is the location group, which uses the policy domain name concatenated with a hyphen, followed by the VLAN Island topology name. The group and switch entry descriptions are labelled with “Created by Script”. If, however, an entry has a different label description, as shown, then the workflow will leave those entries untouched.

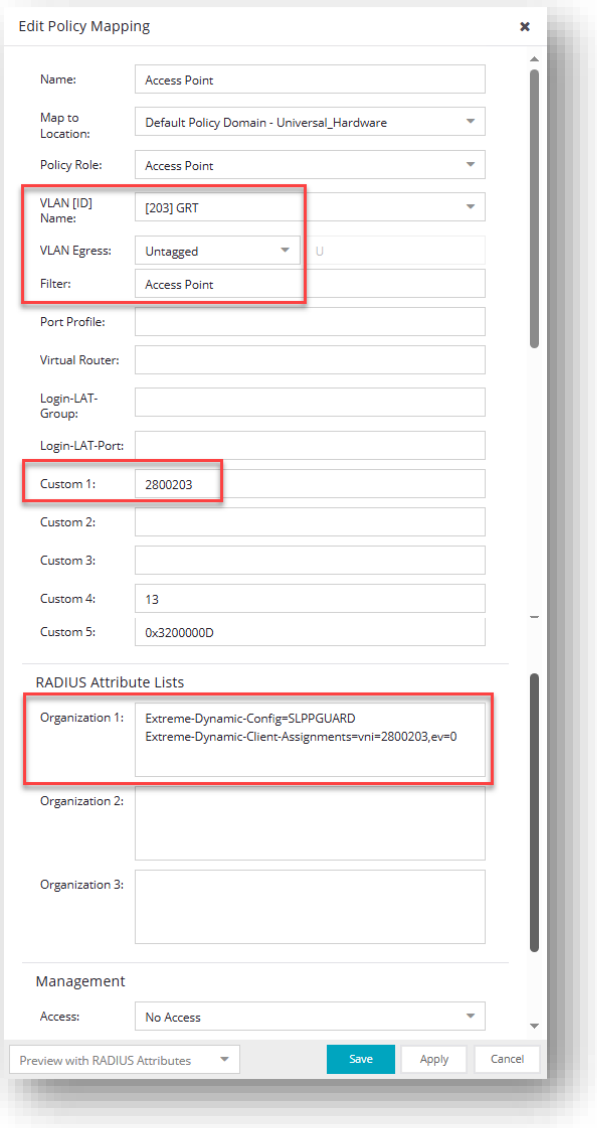


The other profiles created by the workflow are the Access Control Policy Mappings. These profiles will be created multiple times, each referencing a different Location Group profile to match each Policy VLAN Island profile. The screenshot below shows this for the “Access Point” profile.

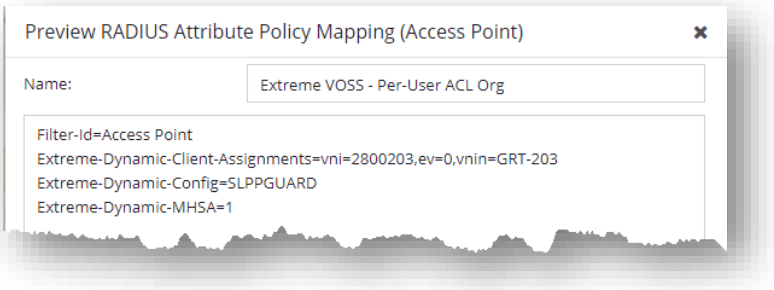


Sync Policy VLAN Islands to Policy mappings

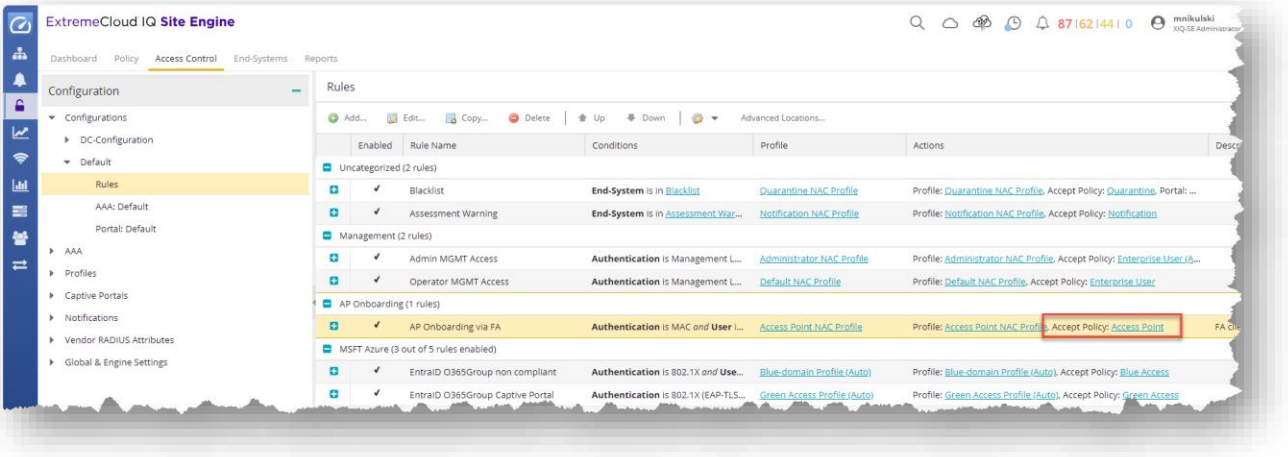
Each policy mapping will be automatically populated with the required RADIUS attributes to match the desired Policy VLAN island topology. The populated fields are the VLAN-ID, VLAN Name, Filter Name, Custom1 and Organization 1 box.



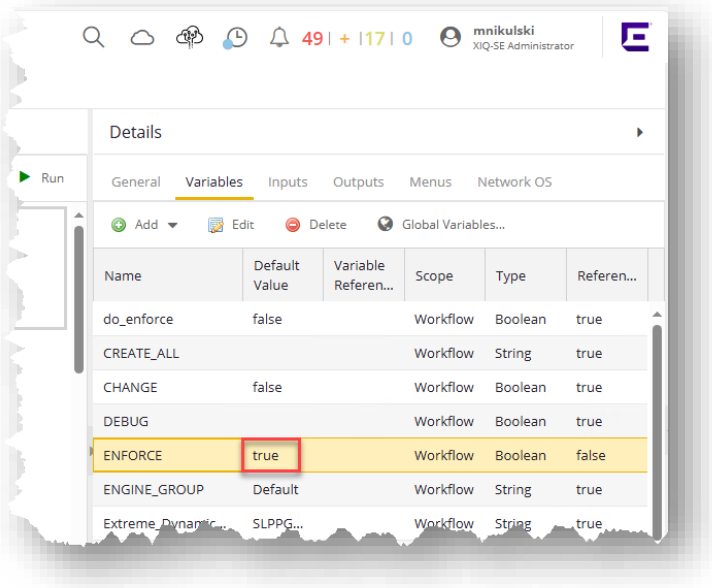
Using the preview option on the above window, the Radius attributes as they will be sent can be previewed.



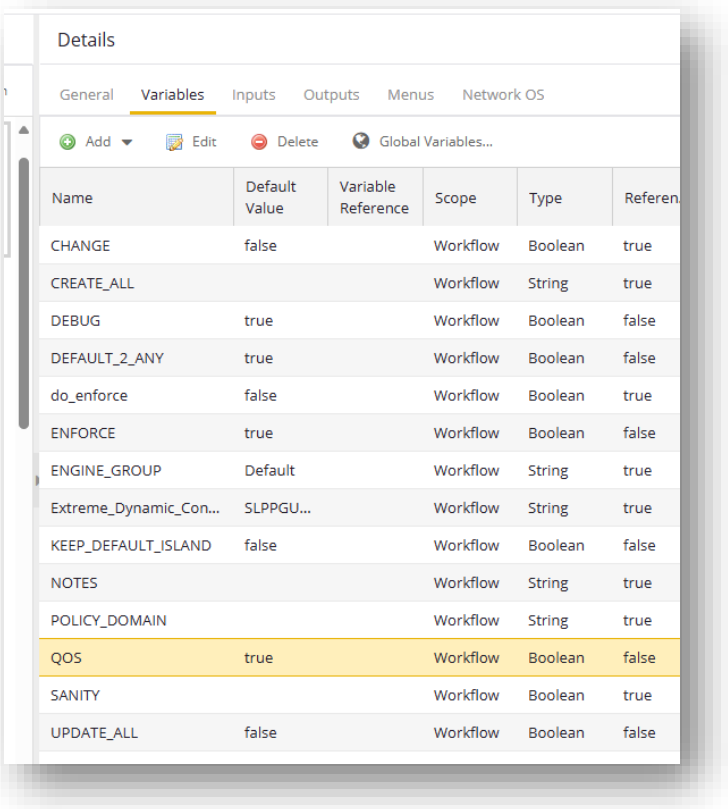
Sync Policy VLAN Islands to Policy mappings
As always, ensure that the relevant Access Control rules are using the desired Access Policy profiles created by the workflow.



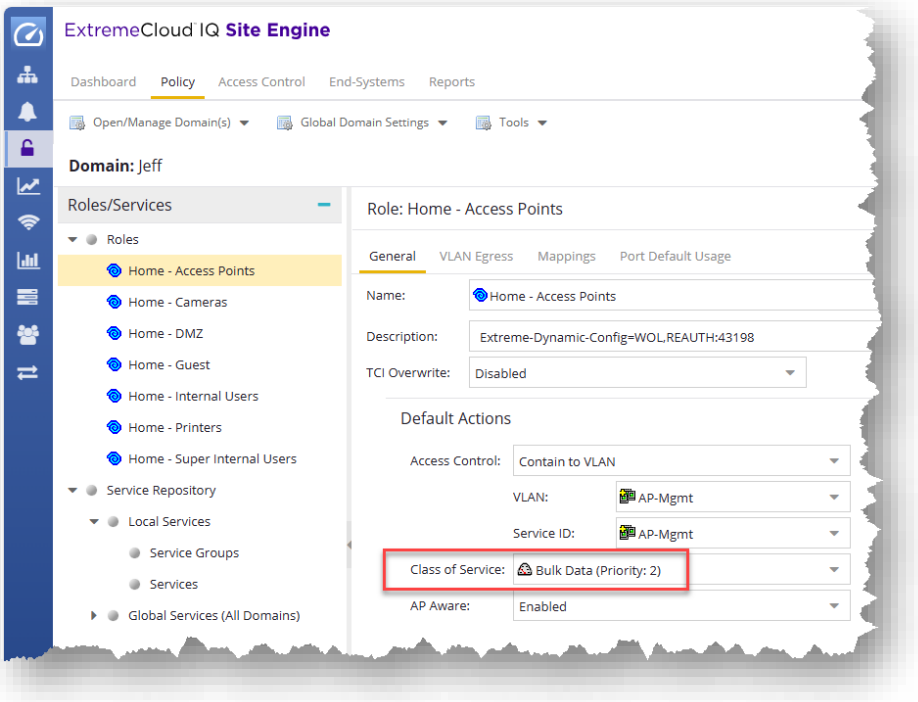
In case you don't like to enforce the changes to the NAC engines you can simply disable enforcement changing this flag to **false**.



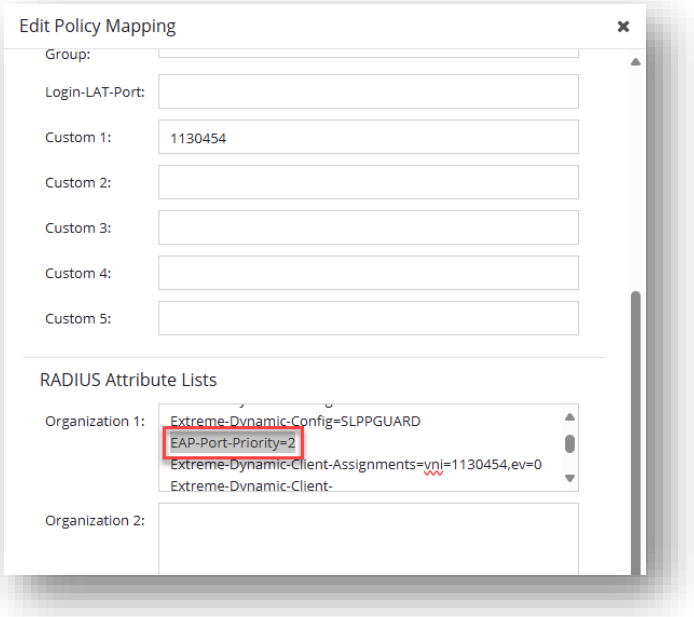
Sync Policy VLAN Islands to Policy mappings
The QOS support can be controlled by this flag.



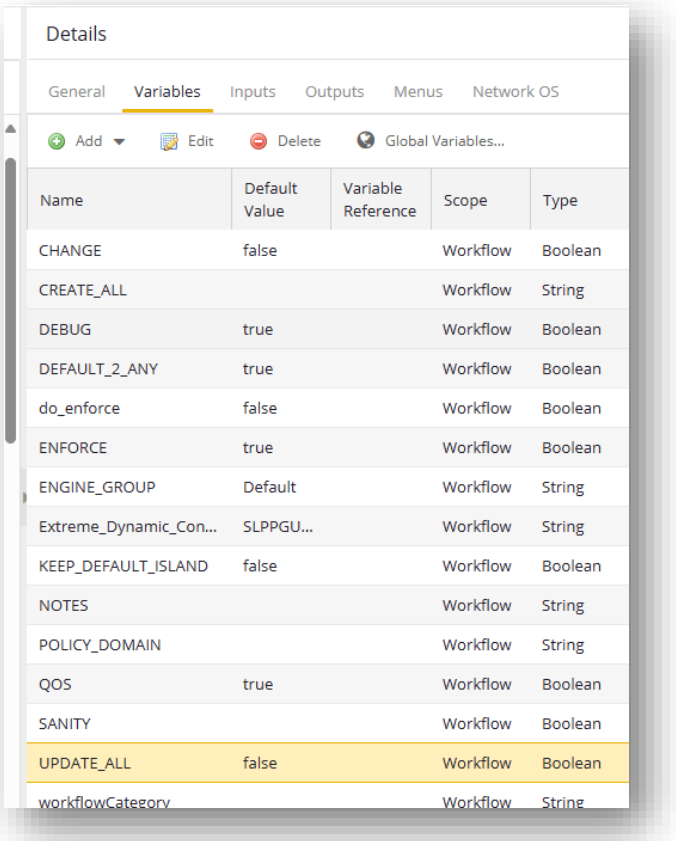
If it's **true,** then it will copy this QOS date like this



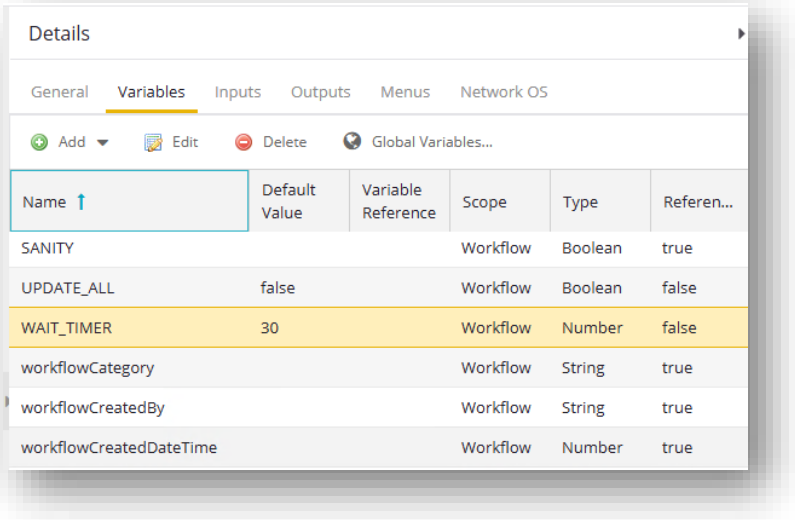
Sync Policy VLAN Islands to Policy mappings



For some test reason, it can be useful to enforce all updates even if no delta is recognised. The flag **UPDATE_ALL** must be set to **true**.

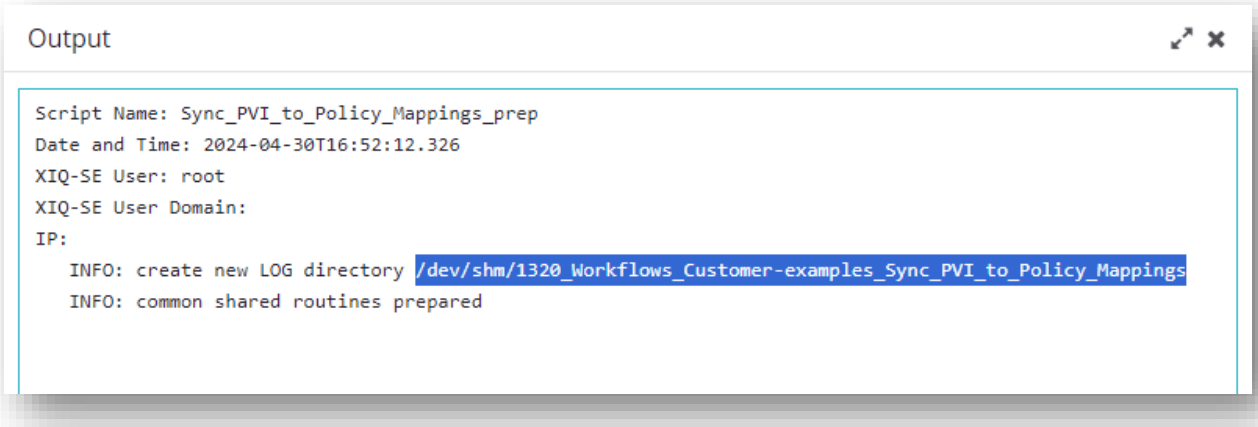


If Workflow runs more than once, the later executed Workflows wait in the queue until the prior Workflow finishes or the timeout is reached. This allows better parallel onboarding of new switches. A variable called 'WAIT_TIMER' in minutes determines the wait time. By default, it is 30 minutes. In large and complex environments, it may be necessary to extend this timer.

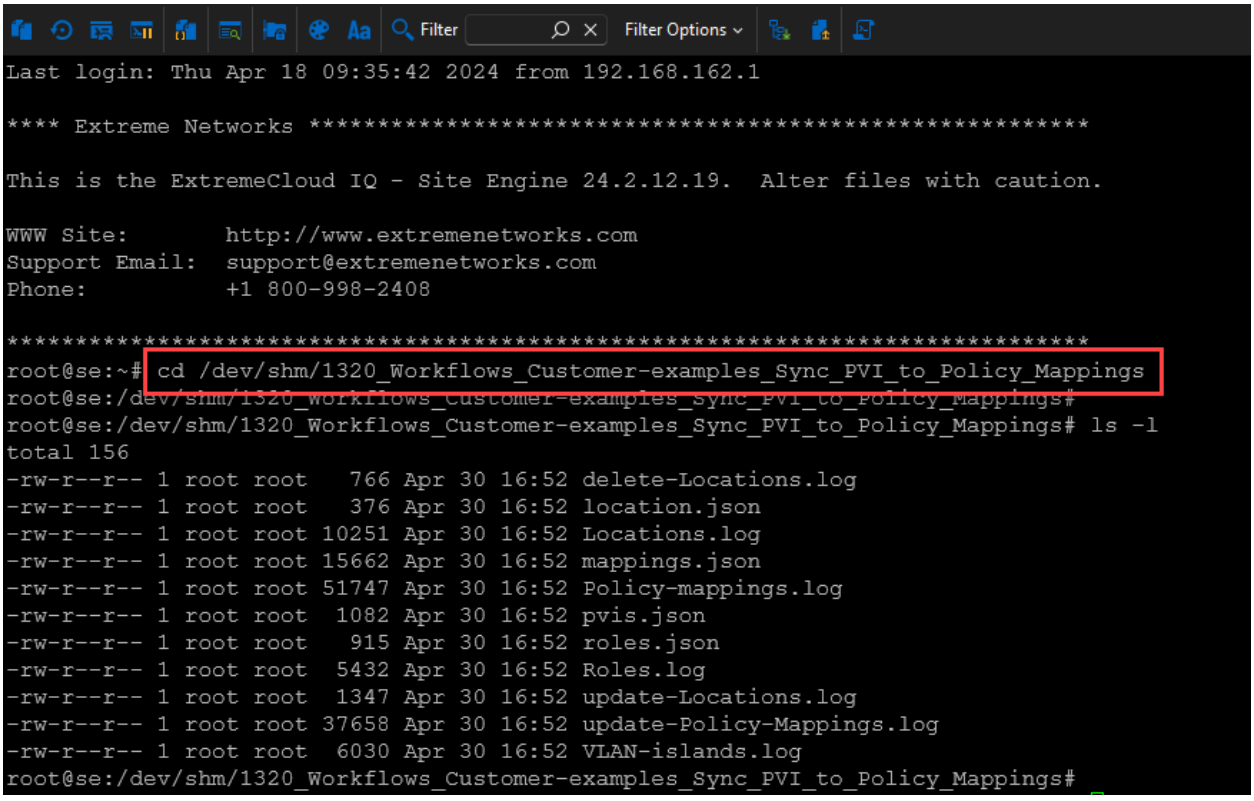


Troubleshooting

Finally, before reporting an issue, please ensure that the workflow is configured for **DEBUG** mode. The data and debug LOG files can then be found on the XIQ-SE file system under **/dev/shm/<Execution-ID>_<Workflow-Name>/** . Note that only the last six execution debug logs will be held. The actual path can also be found in each workflow activity log.



When SSH-ing XIQ-SE, the following log files should be present in the folder.



Please include all log files when reporting an issue.