

## Workflow description

### **Sync Policy VLAN Islands to Policy mappings**

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

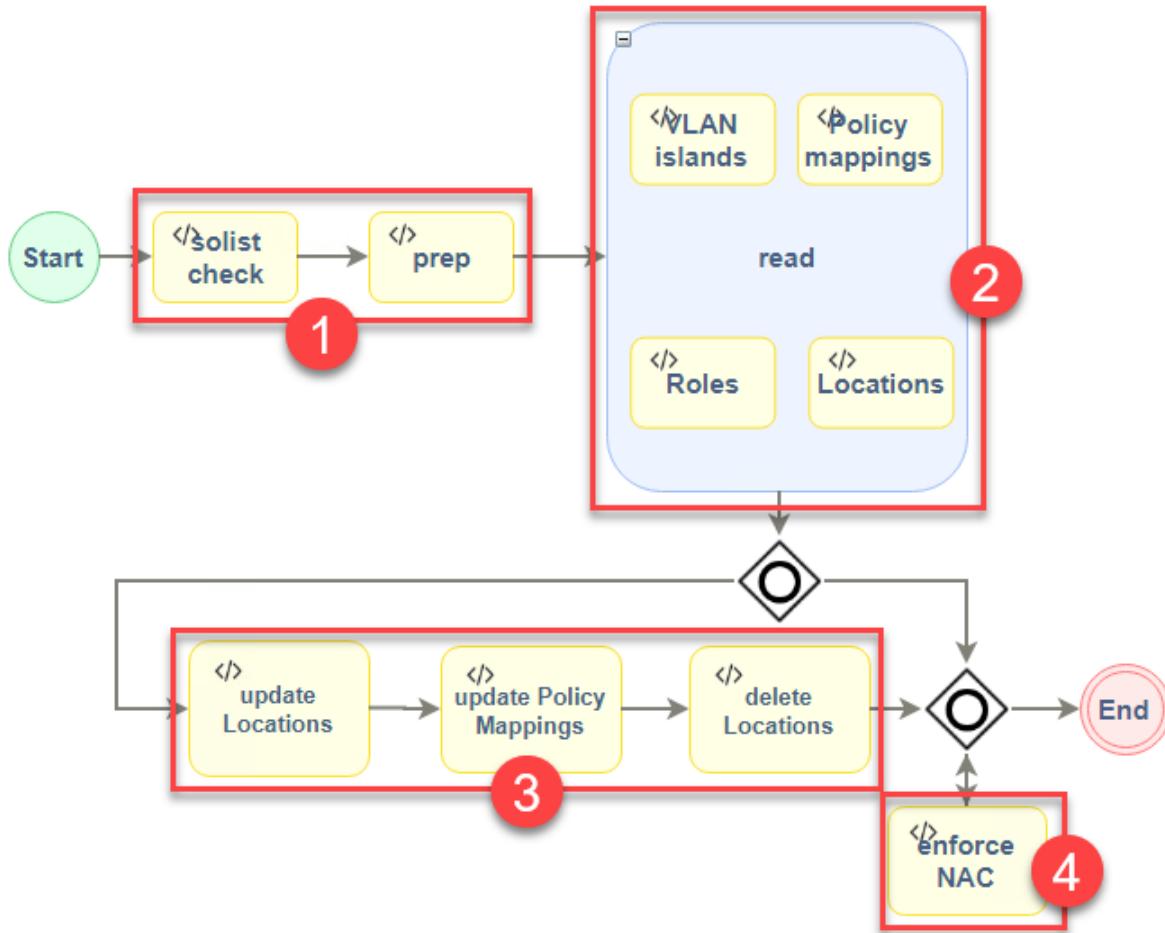
This workflow addresses the need to use XIQ-SE NAC Policy based VLAN islands with Fabric Engine (aka VSP).

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 optimization 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 were made, the NAC engines are enforced to ensure changes are activated immediately.

When launching the workflow manually, it will prompt for the Policy Domain, NAC Engine group and default Radius attributes. The other parameters are intended for testing and debugging purposes only. 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 separate 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

Run Workflow - Sync\_PVI\_to\_Policy\_Mappings

Workflow Inputs

Timeout Properties

**Timeout:**  
10 min(s)

Custom Inputs

**Policy Domain:**  
Default Policy Domain

**NAC Engine Group:**  
Default

Notes:  
The input below can be set to either one or multiple of the possible options (DHCP Snooping, DAI, SLPPGUARD, REAUTH, IGMP Snooping, BPDU Guard, WOL). If multiple options are used, they must be separated by a comma.

**Default NAC Radius Config Attributes:**  
SLPPGUARD

**Test, create all records:**  
true

**Debug logging:**  
true

**Sanity check:**  
false

**Next »** **Cancel**

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,DHCP Snooping,DAI, to enable multiple parameters. In this case, the return attributes will include this:

### **Extreme-Dynamic-Config=SLPPGUARD**

**Extreme-Dynamic-Config=DHCP Snooping**

**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 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 final Policy Mappings are created or updated by the workflow.

The screenshot shows the ExtremeCloud IQ Site Engine interface. On the left, a vertical sidebar lists icons for Dashboard, Policy (selected), Access Control, End-Systems, and Reports. Below these are icons for Open/Manage Domain(s), Global Domain Settings, and Tools. The main content area is titled 'Domain: Default Policy Domain (Modified Locally) - Under edit by mnikulski'. A sidebar on the left under 'Roles/Services' shows a list of roles, with 'GRT Access' highlighted in yellow. The main panel shows the configuration for 'Role: GRT Access'. The 'General' tab is selected. The 'Name' field contains 'GRT Access'. The 'Description' field contains the value 'Extreme-Dynamic-Config=DHCP Snooping,Dai,Ipsg,IGMP Snooping,Mvnio', which is highlighted with a red box. The 'TCI Overwrite' dropdown is set to 'Disabled'. In the 'Default Actions' section, 'Access Control' is set to 'Contain to VLAN', 'VLAN' is set to 'GRT', and 'Service ID' is set to 'GRT'.

The possible attribute keywords accepted are:

**SLPPGUARD, REAUTH ,BPDU ,WOL ,DHCP Snooping ,DAI ,IPSG ,IGMP Snooping ,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, then the Extreme-Dynamic-Client-Assignments VSA will be sent without the “create” option and thus 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)

The screenshot shows the ExtremeCloud IQ Site Engine interface under the 'Policy' tab. On the left, there's a sidebar with icons for Dashboard, Policy, Access Control, End-Systems, and Reports. The main area is titled 'Domain: Default Policy Domain'. It shows 'Policy VLAN Islands' and has tabs for 'VLANS', 'Service IDs', and 'Island Topology'. The 'VLANS' tab is active, displaying a list of VLANs: Blue, GRT, Green, and Red. A red arrow points to this list. Below it, another red arrow points to the 'Service IDs' tab, which also lists the same four VLAN names: Blue, GRT, Green, and Red. The right side of the screen shows a detailed view of the 'Blue' entry, including fields for Island Name (Branch1), Default, and SD-WAN.

## 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 must include `%ORG1_RADIUS_ATTRS_LIST%`

The screenshot shows the ExtremeCloud IQ Site Engine interface with the following steps highlighted:

- Access Control tab selected.
- Engine Groups section, Default group selected.
- Switches tab selected.
- Switch 10.180.48.11 selected.
- Configure Device dialog for 10.180.48.11, showing the RADIUS Attributes to Send field set to "Extreme VOSS - Per-User ACL Org".

**Edit RADIUS Attribute Configuration** dialog (bottom left):
 

- Name: Extreme VOSS - Per-User ACL Org
- Enable Port Link Control:
- Attributes: Filter-Id=%POLICY\_NAME%  
Passport-Access-Priority=%MGMT\_SERV\_TYPE%  
%PER\_USER\_ACL\_VOSS%  
**%ORG1\_RADIUS\_ATTRS\_LIST%** (highlighted with a red arrow)
- Substitutions:

**Configure Device: 10.180.48.11** dialog (top right):
 

- Switch Type: Layer 2 Out-Of-Band
- Primary Engine: NAC-Campus-1/10.8.255.6
- Secondary Engine: NAC-Campus-2/10.8.255.7
- Auth. Access Type: Manual RADIUS Configuration
- RADIUS Attributes to Send: Extreme VOSS - Per-User ACL Org (highlighted with a red box)
- RADIUS Accounting: Enabled
- Management RADIUS Server 1: None
- Management RADIUS Server 2: None
- Network RADIUS Server: None
- Policy Domain: Default Policy Domain (highlighted with a red box)

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.

IP Address	Nickname	Status	System Name	Primary Engine	Secondary Engine	Policy/VLAN	Policy Domain	Authentication Access
20.0.203.79	20.0.203.79	Contact Est...	20.0.203.79	10.8.255.6		Extreme Ide...	Default Policy Domain	Manual RADIUS Config
10.180.48.14	5320-16P-4XE-DC-Fabric...	Contact Est...	5320-16P-4XE...	10.8.255.6	10.8.255.7	Extreme VOS...	Default Policy Domain	Manual RADIUS Config
10.180.209.14	5320-24T	Contact Est...	5320-24T	10.8.255.6	10.8.255.7	Extreme VOS...	Default Policy Domain	Manual RADIUS Config
20.0.204.13	5320-48P-8XE-SwitchEng...	Contact Est...	5320-48P-8XE...	10.8.255.6	10.8.255.7	Extreme Policy	Default Policy Domain	Network Access
20.0.30.111	5320-Emre	Contact Lost	5320-Emre	10.8.255.6	10.8.255.7	Extreme VOS...	Default Policy Domain	Network Access
20.0.30.114	5320-Ludo	Contact Est...	5320-Ludo...	10.8.255.6	10.8.255.7	Extreme VOS...	Default Policy Domain	Network Access
20.0.30.53	5320-MPLS	Contact Lost	5320-MPLS	10.8.255.6	10.8.255.7	Extreme VOS...	Default Policy Domain	Network Access
20.0.30.54	5420F	Contact Est...	5420F	10.8.255.6	10.8.255.7	Extreme VOS...	Default Policy Domain	Network Access
10.180.48.11	5420M	Contact Est...	5420M	10.8.255.6	10.8.255.7	Extreme VOS...	Default Policy Domain	Manual RADIUS Config
10.180.209.10	5420M-2	Contact Est...	5420M-2	10.8.255.6	10.8.255.7	Extreme VOS...	Default Policy Domain	Manual RADIUS Config
10.180.209.10	5520-24X	Contact Est...	5520-24X	10.8.255.6	10.8.255.7	Extreme VOS...	Default Policy Domain	Manual RADIUS Config

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:

**Edit Custom Criteria Alarm Definition: Sync Policy**

Severity:  Set from source

Enabled:

**Criteria** **Actions** **Other Options**

**Custom Criteria**

Match On:

Category: Application (arrow)

Log: Policy (arrow)

Information Phrase: "Enforce finished in policy" (arrow)

**Additional Criteria**

Select Groups...

**Edit Custom Criteria Alarm Definition: Sync Policy**

Severity:  Set from source

Enabled:

**Criteria** **Actions** **Other Options**

**Actions**

Run Task [Workflow - Sync\_PVI\_to\_Policy\_Mappings] (arrow)

**Edit Custom Criteria Alarm Definition: Sync Policy**

Severity:  Set from source

Enabled:

**Criteria** **Actions** **Other Options**

**Alarm Suppression**

Enable Alarm Action Limit

Max Count: 5

Reset Interval: 0 Never

**Clear Conditions**

No Current Alarm (action only):  (arrow)

Cleared by Alarms:

**Save** **Cancel**

## 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 separator and the VLAN Island topology name. The group and switch entry description 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.

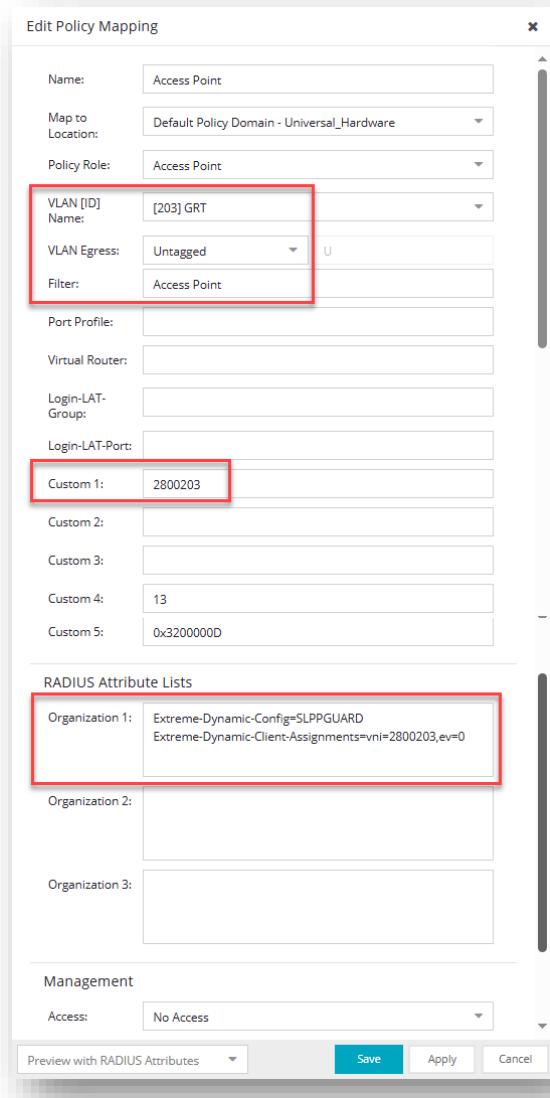
The screenshot shows the ExtremeCloud IQ Site Engine interface under the Access Control tab. In the left sidebar, 'Configuration' is selected. Under 'Group Editor', 'Location Groups' is expanded, showing a list of groups including 'Branch1', 'Cisco3750', 'CTC-WING-1X', 'CTC-WING-1X-CaseA', 'CTC-WING-1X-CaseB', 'CTC-WING-Guest-CasC', 'CTC-WING-PSK', and several 'Default Policy Domain' entries. A red box highlights the 'Default Policy Domain - Universal\_Hardware' entry. To the right, the 'Edit Group' panel shows the group's name and type, and a table listing switches with their descriptions. A red box highlights the entry for '20.0.202.16, 20.0.202.24, 20...' which has a description of 'ISW switch added'.

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.

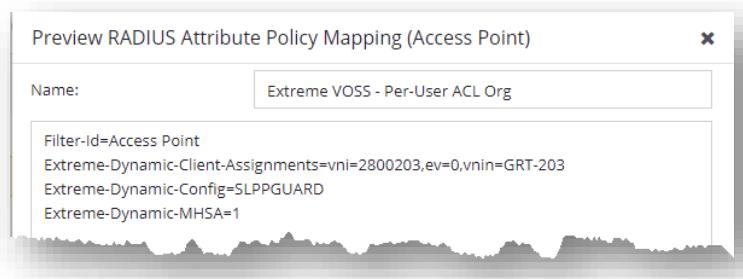
The screenshot shows the ExtremeCloud IQ Site Engine interface under the Access Control tab. In the left sidebar, 'Policy Mappings' is selected, with 'Default' highlighted. The main area displays a table of policy mappings. A red box highlights the first row under the 'Access Point' column, which has a different description ('Default Policy Domain - Universal\_Hardware') than the other rows.

## 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.

Enabled	Rule Name	Conditions	Profile	Actions
✓	Blacklist	End-System is in Blacklist	Quarantine NAC Profile	Profile: Quarantine NAC Profile, Accept Policy: Quarantine, Portal: ...
✓	Assessment Warning	End-System is in Assessment War...	Notification NAC Profile	Profile: Notification NAC Profile, Accept Policy: Notification
Management (2 rules)				
✓	Admin MGMT Access	Authentication is Management L...	Administrator NAC Profile	Profile: Administrator NAC Profile, Accept Policy: Enterprise User, A...
✓	Operator MGMT Access	Authentication is Management L...	Default NAC Profile	Profile: Default NAC Profile, Accept Policy: Enterprise User
AP Onboarding (1 rule)				
✓	AP Onboarding via FA	Authentication is MAC and User ...	Access Point NAC Profile	Profile: Access Point NAC Profile, Accept Policy: Access Point
MSFT Azure (3 out of 5 rules enabled)				
✓	EnrollID O365Group non compliant	Authentication is 802.1X and Use...	Blue-domain Profile (Auto)	Profile: Blue-domain Profile (Auto), Accept Policy: Blue Access
✓	EnrollID O365Group Captive Portal	Authentication is 802.1X (EAP-TLS...	Green Access Profile (Auto)	Profile: Green Access Profile (Auto), Accept Policy: Green Access

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

Name	Default Value	Variable Referen...	Scope	Type	Referen...
do_enforce	false		Workflow	Boolean	true
CREATE_ALL			Workflow	String	true
CHANGE	false		Workflow	Boolean	true
DEBUG			Workflow	Boolean	true
ENFORCE	true		Workflow	Boolean	false
ENGINE_GROUP	Default		Workflow	String	true
Extreme_Dynamic...	SLPPG...		Workflow	String	true

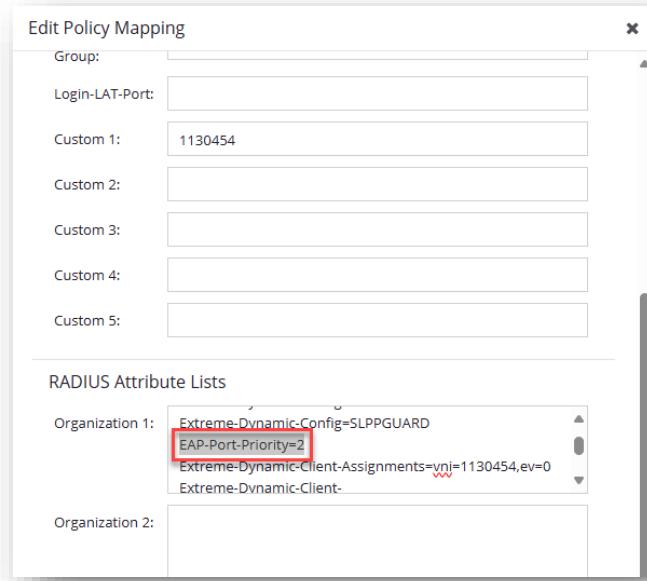
Sync Policy VLAN Islands to Policy mappings  
The QOS support can be controlled by this flag.

Details					
General Variables Inputs Outputs Menus Network OS					
Name	Default Value	Variable Reference	Scope	Type	Referenc...
CHANGE	false		Workflow	Boolean	true
CREATE_ALL			Workflow	String	true
DEBUG	true		Workflow	Boolean	false
DEFAULT_2_ANY	true		Workflow	Boolean	false
do_enforce	false		Workflow	Boolean	true
ENFORCE	true		Workflow	Boolean	false
ENGINE_GROUP	Default		Workflow	String	true
Extreme_Dynamic_Con...	SLPPGU...		Workflow	String	true
KEEP_DEFAULT_ISLAND	false		Workflow	Boolean	false
NOTES			Workflow	String	true
POLICY_DOMAIN			Workflow	String	true
QOS	true		Workflow	Boolean	false
SANITY			Workflow	Boolean	true
UPDATE_ALL	false		Workflow	Boolean	false

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

The screenshot shows the 'ExtremeCloud IQ Site Engine' interface. The left sidebar has a dark blue theme with icons for dashboard, policy, access control, end-systems, and reports. The 'Policy' tab is selected. The main area shows a 'Domain: Jeff' configuration. On the left, under 'Roles/Services', there is a tree view with 'Roles' expanded, showing 'Home - Access Points' selected. To the right, the 'Role: Home - Access Points' configuration page is displayed. It includes tabs for General, VLAN Egress, Mappings, and Port Default Usage. Under 'General', the 'Name' is 'Home - Access Points', 'Description' is 'Extreme-Dynamic-Config=WOL.REAUTH:43198', and 'TCI Overwrite' is 'Disabled'. Under 'Default Actions', 'Access Control' is set to 'Contain to VLAN', 'VLAN' is 'AP-Mgmt', 'Service ID' is 'AP-Mgmt', and 'Class of Service' is 'Bulk Data (Priority: 2)', which is highlighted with a red box. 'AP Aware' is set to 'Enabled'.

## 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**.

Details				
General Variables Inputs Outputs Menus Network OS				
<a href="#">Add</a> <a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Global Variables...</a>				
Name	Default Value	Variable Reference	Scope	Type
CHANGE	false		Workflow	Boolean
CREATE_ALL			Workflow	String
DEBUG	true		Workflow	Boolean
DEFAULT_2_ANY	true		Workflow	Boolean
do_enforce	false		Workflow	Boolean
ENFORCE	true		Workflow	Boolean
ENGINE_GROUP	Default		Workflow	String
Extreme_Dynamic_Con...	SLPPGU...		Workflow	String
KEEP_DEFAULT_ISLAND	false		Workflow	Boolean
NOTES			Workflow	String
POLICY_DOMAIN			Workflow	String
QOS	true		Workflow	Boolean
SANITY			Workflow	Boolean
UPDATE_ALL	false		Workflow	Boolean
workflowCategory			Workflow	String

## Sync Policy VLAN Islands to Policy mappings

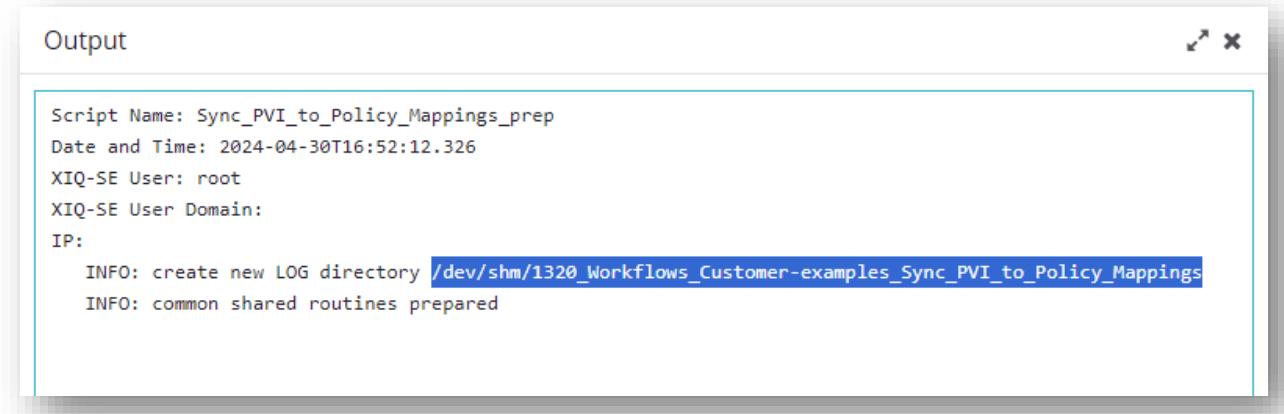
If Workflow runs more than once, the later executed Workflows wait in the queue until the prior Workflow finishes or the timeout is reached. This allows better parallel onboarding of new switches. A variable called 'WAIT\_TIMER' in minutes determines the wait time. By default, it is 30 minutes. In large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

Details					
General	Variables	Inputs	Outputs	Menus	Network OS
		Add	Edit	Delete	Global Variables...
Name ↑	Default Value	Variable Reference	Scope	Type	Referen...
SANITY		Workflow	Boolean	true	
UPDATE_ALL	false	Workflow	Boolean	false	
WAIT_TIMER	30	Workflow	Number	false	
workflowCategory		Workflow	String	true	
workflowCreatedBy		Workflow	String	true	
workflowCreatedDateTime		Workflow	Number	true	

## Sync Policy VLAN Islands to Policy mappings

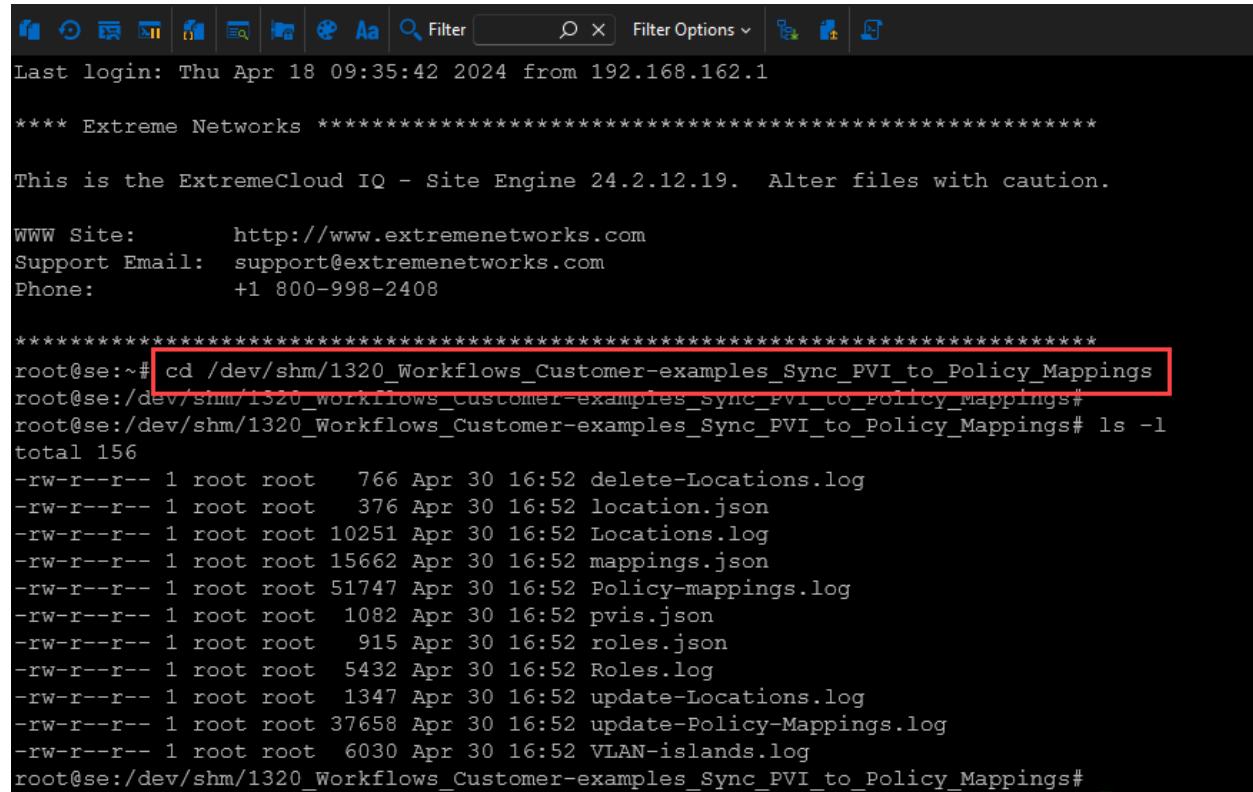
### Troubleshooting

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.



```
Script Name: Sync_PVI_to_Policy_Mappings_prep
Date and Time: 2024-04-30T16:52:12.326
XIQ-SE User: root
XIQ-SE User Domain:
IP:
INFO: create new LOG directory /dev/shm/1320_Workflows_Customer-examples_Sync_PVI_to_Policy_Mappings
INFO: common shared routines prepared
```

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



```
Last login: Thu Apr 18 09:35:42 2024 from 192.168.162.1
**** Extreme Networks ****
This is the ExtremeCloud IQ - Site Engine 24.2.12.19. Alter files with caution.

WWW Site: http://www.extremenetworks.com
Support Email: support@extremenetworks.com
Phone: +1 800-998-2408

*****
root@se:~# cd /dev/shm/1320_Workflows_Customer-examples_Sync_PVI_to_Policy_Mappings
root@se:/dev/shm/1320_Workflows_Customer-examples_Sync_PVI_to_Policy_Mappings#
root@se:/dev/shm/1320_Workflows_Customer-examples_Sync_PVI_to_Policy_Mappings# ls -l
total 156
-rw-r--r-- 1 root root    766 Apr 30 16:52 delete-Locations.log
-rw-r--r-- 1 root root   376 Apr 30 16:52 location.json
-rw-r--r-- 1 root root 10251 Apr 30 16:52 Locations.log
-rw-r--r-- 1 root root 15662 Apr 30 16:52 mappings.json
-rw-r--r-- 1 root root 51747 Apr 30 16:52 Policy-mappings.log
-rw-r--r-- 1 root root  1082 Apr 30 16:52 pvis.json
-rw-r--r-- 1 root root   915 Apr 30 16:52 roles.json
-rw-r--r-- 1 root root  5432 Apr 30 16:52 Roles.log
-rw-r--r-- 1 root root 1347 Apr 30 16:52 update-Locations.log
-rw-r--r-- 1 root root 37658 Apr 30 16:52 update-Policy-Mappings.log
-rw-r--r-- 1 root root  6030 Apr 30 16:52 VLAN-islands.log
root@se:/dev/shm/1320_Workflows_Customer-examples_Sync_PVI_to_Policy_Mappings#
```

Please include all log files when reporting an issue.