

Workflow description

Sync Policy VLAN Islands to Policy mappings

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

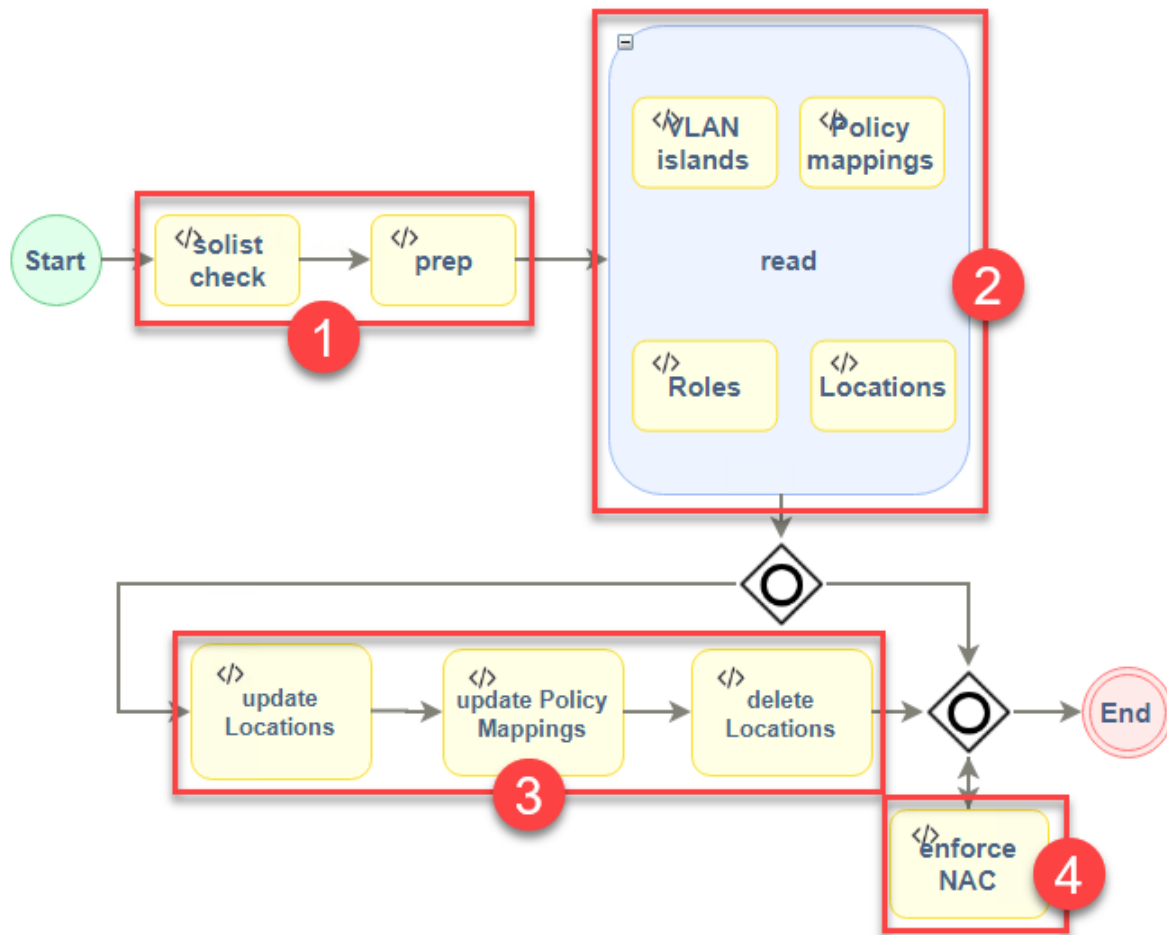
This workflow addresses the need to use XIQ-SE NAC Policy based VLAN islands with Fabric Engine (aka VSP).

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,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 take a comma separated list of attributes, like **SLPPGUARD,DHCP Snooping,DAI**, so as to enable more than one parameter. In this case the return attributes will include this:

Extreme-Dynamic-Config=SLPPGUARD

Extreme-Dynamic-Config=DHCP Snooping

Extreme-Dynamic-Config=DAI

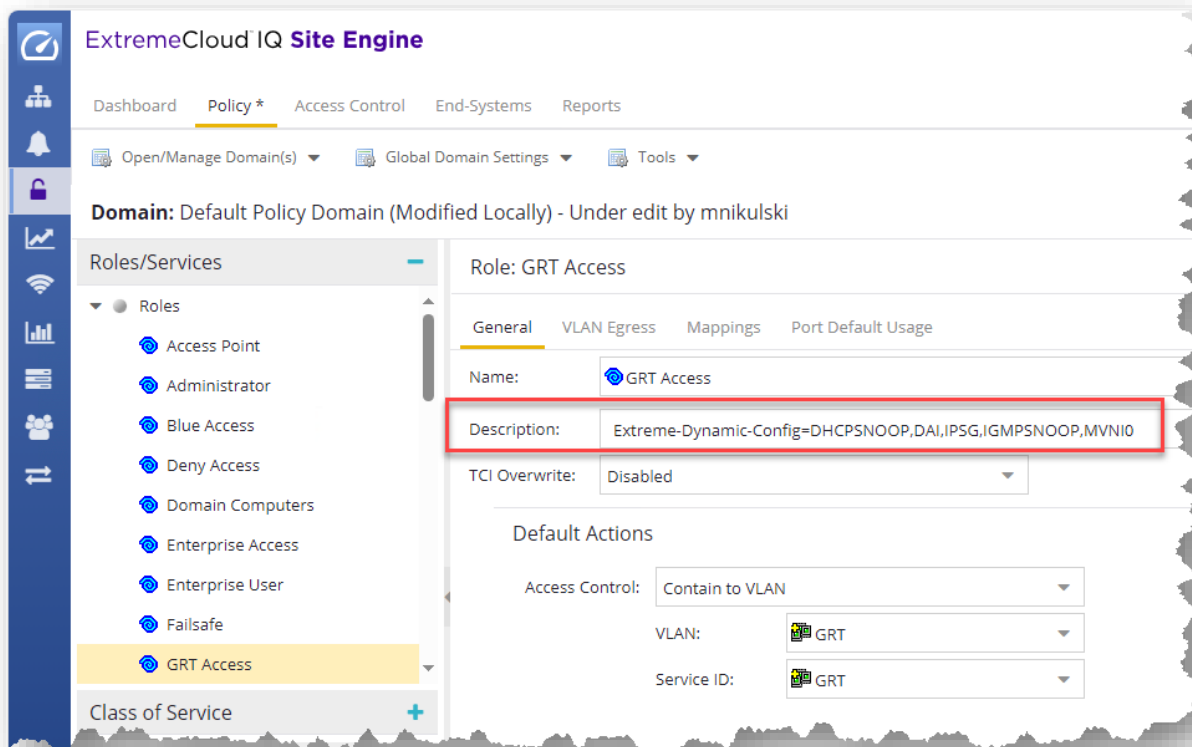
Sync Policy VLAN Islands to Policy mappings

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

If **TEST creates all records** equal **true** everything gets created even if no switch is assigned to a VLAN Island topology (location). If this parameter is **false**, it will only create what is used and delete what is not used anymore.

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 together once the final Policy Mappings are created or updated by the workflow.



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:

- **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.

Sync Policy VLAN Islands to Policy mappings

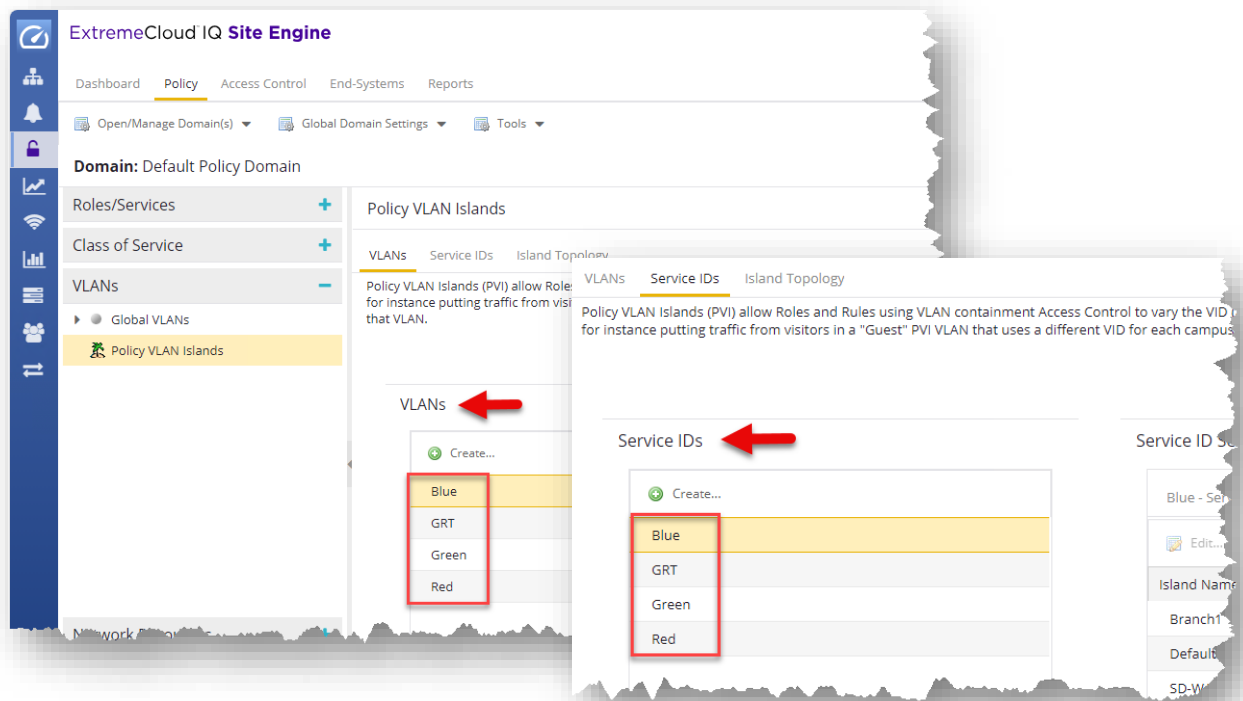
- **PVLAN<SecVID>**: This will result in the Extreme-Dynamic-Client-Assignments VSA going out with “create=pvlan” and “sv=<SecVID>”, in addition to “pv=<PriVID>” which is also always added when the “create=” switch is present. The end result is that a PrivateVLAN (ETREE) service will be created on the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

Sync Policy VLAN Islands to Policy mappings

The **DHCP Snoop**, **DAI**, **IPSG**, **IGMP Snoop**, **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 authorized.

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 authorized.

Please note, It is very important is to use the same VLAN and I-SID (Service ID) name. Otherwise the workflow will result in a 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 must include %ORG1_RADIUS_ATTRS_LIST%

The screenshot displays the ExtremeCloud IQ Site Engine interface. The left sidebar shows the 'Configuration' menu with 'Engine Group Editor' and 'Engines' options. The 'Engines' section is expanded, showing 'Engine Groups' and 'All Engines'. The 'Default' engine group is selected, and the 'Switches' tab is active. A table lists switches, with '10.180.48.11' selected. The 'Configure Device: 10.180.48.11' dialog is open, showing configuration details for the switch. The 'RADIUS Attributes to Send' dropdown is set to 'Extreme VOSS - Per-User ACL Org'. The 'Edit RADIUS Attribute Configuration' dialog is also open, showing the 'Name' field set to 'Extreme VOSS - Per-User ACL Org' and the 'Attributes' field containing the following template:

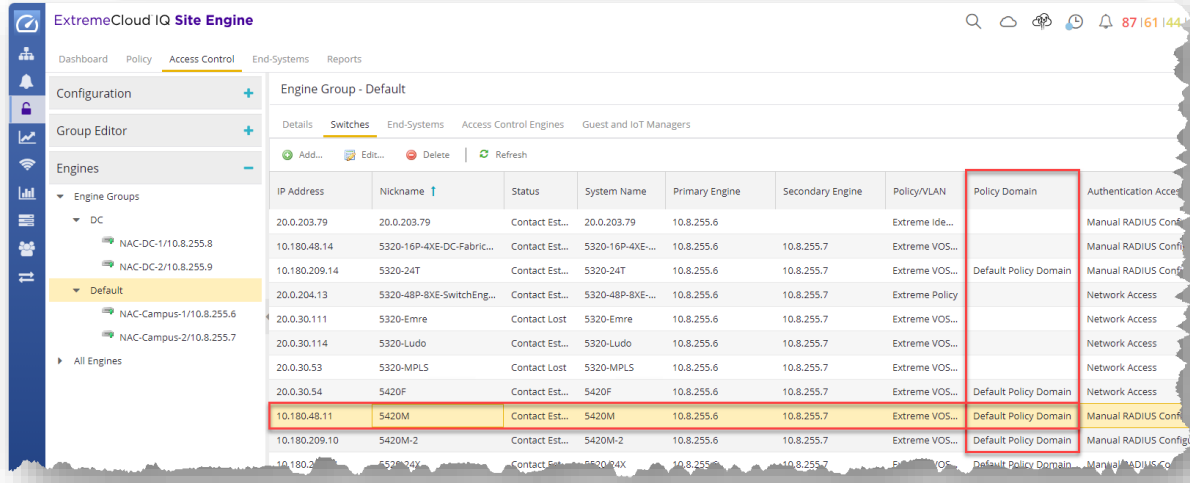
```
Filter-id=%POLICY_NAME%
Passport-Access-Priority=%MGMT_SERV_TYPE%
%PER_USER_ACL_VOSS%
%ORG1_RADIUS_ATTRS_LIST%
%ORG2_RADIUS_ATTRS_LIST%
%ORG3_RADIUS_ATTRS_LIST%
```

Red arrows indicate the workflow steps: 1. Select 'Engine Group Editor', 2. Select 'Default' engine group, 3. Select 'Switches' tab, 4. Select the switch '10.180.48.11', 5. Select the 'Extreme VOSS - Per-User ACL Org' RADIUS attribute template.

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.

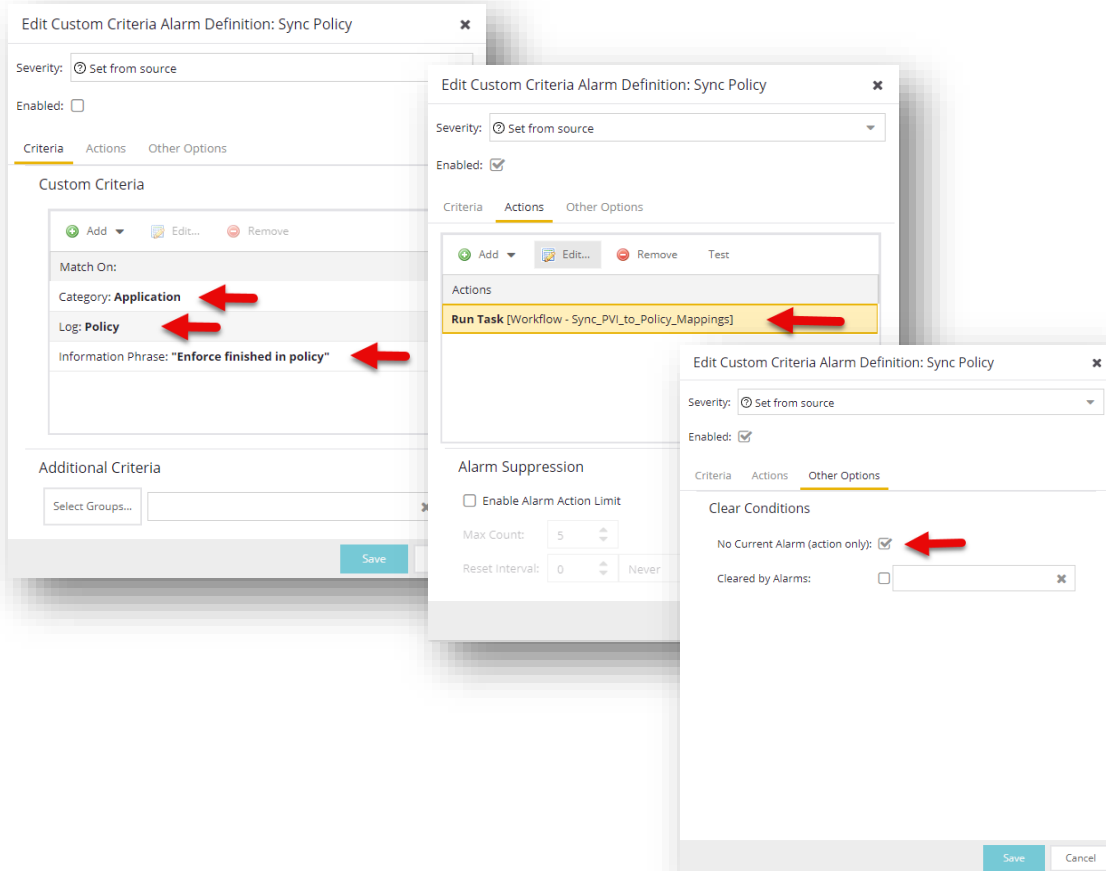
Sync Policy VLAN Islands to Policy mappings

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...		Manual RADIUS Conf...
10.180.48.14	5320-16P-4XE-Fabric...	Contact Est...	5320-16P-4XE...	10.8.255.6	10.8.255.7	Extreme VOS...		Manual RADIUS Conf...
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 Conf...
20.0.204.13	5320-48P-8XE-SwitchEng...	Contact Est...	5320-48P-8XE...	10.8.255.6	10.8.255.7	Extreme Policy		Network Access
20.0.30.111	5320-Emre	Contact Lost	5320-Emre	10.8.255.6	10.8.255.7	Extreme VOS...		Network Access
20.0.30.114	5320-Ludo	Contact Est...	5320-Ludo	10.8.255.6	10.8.255.7	Extreme VOS...		Network Access
20.0.30.53	5320-MPLS	Contact Lost	5320-MPLS	10.8.255.6	10.8.255.7	Extreme VOS...		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 Conf...
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 Conf...
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 Conf...

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**

Log: **Policy**

Information Phrase: **"Enforce finished in policy"**

Additional Criteria

Select Groups...

Save

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]

Alarm Suppression

☐ Enable Alarm Action Limit

Max Count: 5

Reset Interval: 0 Never

Edit Custom Criteria Alarm Definition: Sync Policy

Severity: ☐ Set from source

Enabled: ☒

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

Clear Conditions

No Current Alarm (action only): ☒

Cleared by Alarms: ☐ [X]

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. The 'Access Control' tab is selected. In the left sidebar, the 'Group Editor' is open, showing a list of 'Location Groups'. The group 'Default Policy Domain - Universal_Hardware' is highlighted. The main panel shows the 'Edit Group' details for this group. The 'Name' is 'Default Policy Domain - Universal_Hardware' and the 'Description' is 'Created Automatically, Do not...'. Below this, there is a table of switches with columns: Switch, Port/SSID, Access Point ID, and Description. The table contains five entries, all with descriptions 'Created by Script'. The last entry, '20.0.202.16, 20.0.202.24, 20...', has a description 'ISW switch added by...'. A red box highlights the 'Description' column for the last entry.

Switch	Port/SSID	Access Point ID	Description
10.180.209.10	*	*	Created by Script
10.180.209.11	*	*	Created by Script
10.180.209.14	*	*	Created by Script
10.180.209.42	*	*	Created by Script
20.0.202.16, 20.0.202.24, 20...	*	*	ISW switch added by...

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

The screenshot shows the 'ExtremeCloud IQ Site Engine' interface. The 'Access Control' tab is selected. In the left sidebar, the 'Policy Mappings' section is open, and the 'Default' mapping is highlighted. The main panel shows the 'Default' policy mapping details. The 'Name' is 'Access Point', the 'Policy Role' is 'Access Point', and the 'Location' is 'Default Policy Domain - Universal_Hardware'. Below this, there is a table of policy mappings with columns: Name, Policy Role, Location, VLAN Name, and Log Port. The table contains six entries, all with 'Access Point' as the Name and 'Access Point' as the Policy Role. The 'Location' column contains different values: 'Any', 'Default Policy Domain - Universal_Hardware', 'Default Policy Domain - SD-WAN', 'Default Policy Domain - Branch1', 'Default Policy Domain - SD-WAN Large Branch', and 'Default Policy Domain - Default Island'. The 'VLAN Name' column contains values like '[203] GRT...', '[203] GRT', '[206] GRT', '[204] GRT', '[205] GRT', and '[200] GRT'. The 'Log Port' column contains values like '0', '0', '0', '0', '0', and '0'. A red box highlights the 'Location' column for the first five entries.

Name	Policy Role	Location	VLAN Name	Log Port
Access Point	Access Point	Any	[203] GRT...	0
Access Point	Access Point	Default Policy Domain - Universal_Hardware	[203] GRT	0
Access Point	Access Point	Default Policy Domain - SD-WAN	[206] GRT	0
Access Point	Access Point	Default Policy Domain - Branch1	[204] GRT	0
Access Point	Access Point	Default Policy Domain - SD-WAN Large Branch	[205] GRT	0
Access Point	Access Point	Default Policy Domain - Default Island	[200] GRT	0
Administrator	Administra...	Any	None	0
AP	AP	Any	None	0
Access Point	Access Point	Any	None	0

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, Custom1 and Organization 1 box.

The screenshot shows the 'Edit Policy Mapping' window with the following configuration:

- Name: Access Point
- Map to Location: Default Policy Domain - Universal_Hardware
- Policy Role: Access Point
- VLAN [ID] Name: [203] GRT
- VLAN Egress: Untagged
- Filter:
- Login-LAT-Port:
- Custom 1: 2800203
- Custom 2:
- Custom 3:
- Custom 4:

RADIUS Attribute Lists

- Organization 1: Extreme-Dynamic-Config=SLPPGUARD
Extreme-Dynamic-MHSA=1
Extreme-Dynamic-Client-Assignments=vni=2800203,ev=0,vnin=GRT-203
- Organization 2:
- Organization 3:

Management

- Access: No Access

Buttons at the bottom: Preview with RADIUS Attributes, Save, Apply, Cancel. A 'Show Advanced' link is also present.

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

Preview RADIUS Attribute Policy Mapping (Access Point)

Name:

Filter-Id=Access Point
Extreme-Dynamic-Client-Assignments=vni=2800203,ev=0,vnin=GRT-203
Extreme-Dynamic-Config=SLPPGUARD
Extreme-Dynamic-MHSA=1

As always, ensure that the relevant Access Control rules are using the desired Access Policy profiles created by the workflow.

ExtremeCloud IQ Site Engine

Dashboard Policy Access Control End-Systems Reports

Configuration

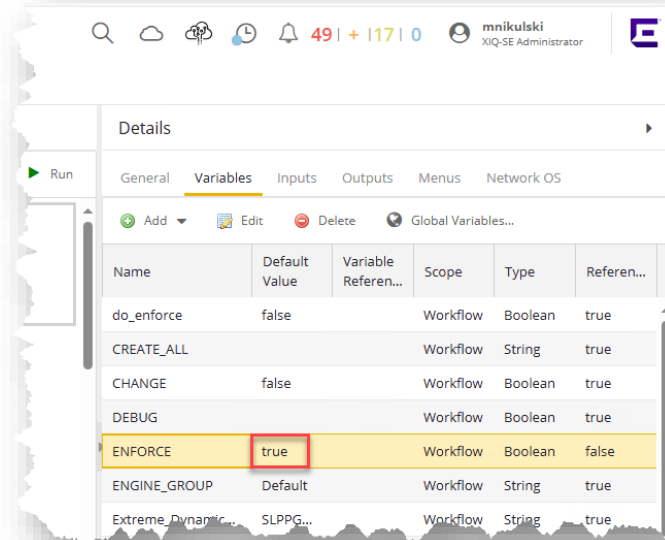
- Configurations
 - DC-Configuration
 - Default
 - Rules**
 - AAA: Default
 - Portal: Default
 - Profiles
 - Captive Portals
 - Notifications
 - Vendor RADIUS Attributes
 - Global & Engine Settings

Rules

Enabled	Rule Name	Conditions	Profile	Actions	Description
Uncategorized (2 rules)					
<input checked="" type="checkbox"/>	Blacklist	End-System is in Blacklist	Quarantine NAC Profile	Profile: Quarantine NAC Profile , Accept Policy: Quarantine , Portal: ...	
<input checked="" type="checkbox"/>	Assessment Warning	End-System is in Assessment War...	Notification NAC Profile	Profile: Notification NAC Profile , Accept Policy: Notification	
Management (2 rules)					
<input checked="" type="checkbox"/>	Admin MGMT Access	Authentication is Management L...	Administrator NAC Profile	Profile: Administrator NAC Profile , Accept Policy: Enterprise User (A...	
<input checked="" type="checkbox"/>	Operator MGMT Access	Authentication is Management L...	Default NAC Profile	Profile: Default NAC Profile , Accept Policy: Enterprise User	
AP Onboarding (1 rules)					
<input checked="" type="checkbox"/>	AP Onboarding via FA	Authentication is MAC and User L...	Access Point NAC Profile	Profile: Access Point NAC Profile , Accept Policy: Access Point	FA On...
MSFT Azure (3 out of 5 rules enabled)					
<input checked="" type="checkbox"/>	EntraID O365Group non compliant	Authentication is 802.1X and Use...	Blue-domain Profile (Auto)	Profile: Blue-domain Profile (Auto) , Accept Policy: Blue Access	
<input checked="" type="checkbox"/>	EntraID 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**.

Sync Policy VLAN Islands to Policy mappings



The screenshot shows a web-based interface for managing variables. At the top, there is a navigation bar with a search icon, a cloud icon, a gear icon, a clock icon, a bell icon, and a user profile for 'mnikulski XIQ-SE Administrator'. Below the navigation bar, there is a 'Details' section with tabs for 'General', 'Variables', 'Inputs', 'Outputs', 'Menus', and 'Network OS'. The 'Variables' tab is selected. Below the tabs, there is a table with columns: 'Name', 'Default Value', 'Variable Referen...', 'Scope', 'Type', and 'Referen...'. The table contains several rows of variables. The 'ENFORCE' row is highlighted in yellow, and its 'true' value in the 'Default Value' column is enclosed in a red box.

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

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 the each workflow activity log.

```
Output

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.