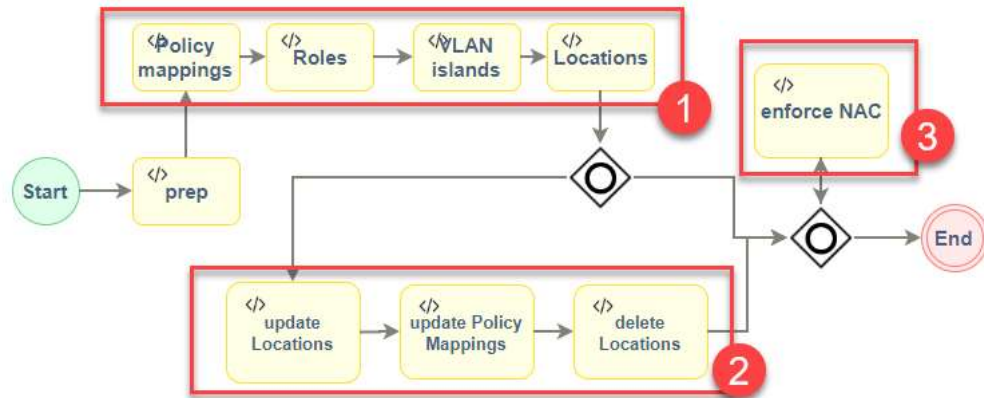


Workflow description

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).

Run Workflow - Sync_PVI_to_Policy_Mappings

Workflow Inputs

Timeout Properties

Timeout: 5 min(s)

Custom Inputs

Policy Domain: Automated-Campus

Debug logging: true

Sanity check: false

Next » Cancel

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

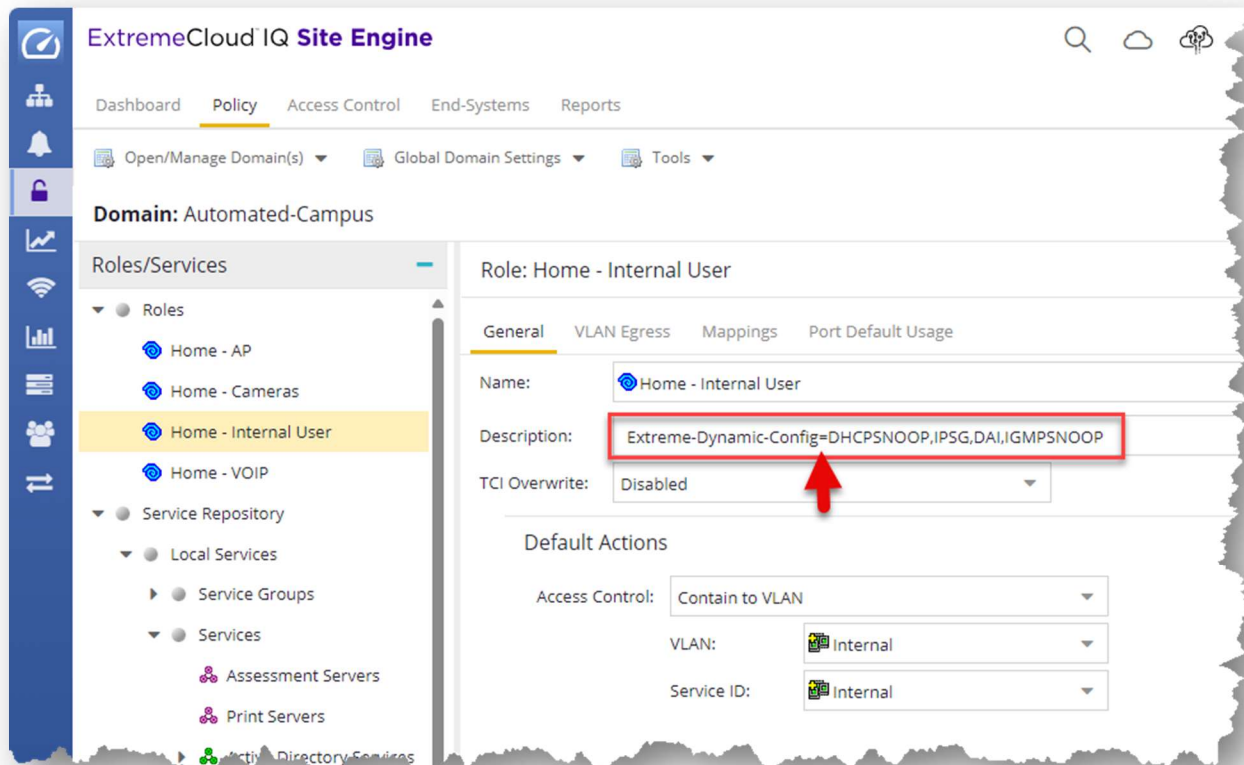
Extreme-Dynamic-Config=DAI

Just be aware, it applies to all policy mappings.

The screenshot shows the 'Variables' tab in the XIQ-SE Administrator. The table lists the following variables:

Name	Default Value	Variable Reference	Scope	Type	Referenced
CHANGE	false		Workflow	Boolean	true
DEBUG			Workflow	Boolean	true
ENFORCE	false		Workflow	Boolean	true
ENGINE_GROUP	Default		Workflow	String	false
Extreme_Dynamic_Config	SLPPGUARD		Workflow	String	false
POLICY_DOMAIN			Workflow	String	true
SANITY			Workflow	Boolean	true
workflowCategory			Workflow	String	true

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

The screenshot shows the ExtremeCloud IQ Site Engine interface. On the left sidebar, the 'Configuration' tab is selected, and the 'Engines' section is expanded, showing the 'Default' engine group. The 'Switches' tab is selected in the main panel. A table lists switches with their IP addresses and names. The switch '192.168.162.11 VSP-1' is highlighted. A red arrow points to the 'Edit...' button for this switch. A second window, 'Configure Device: 192.168.162.11', is open, showing configuration details for the selected switch. The 'Switch Type' is 'Layer 2 Out-Of-Band', 'Primary Engine' is 'NAC/192.168.162.51', 'Auth. Access Type' is 'Network Access', 'RADIUS Attributes to Send' is 'Fabric Engine', 'RADIUS Accounting' is 'Enabled', and 'Management RADIUS Server 1' is 'None'. A third window, 'Edit RADIUS Attribute Configuration', is open, showing the 'Fabric Engine' attribute configuration. The 'Attributes' field is set to '%ORG1_RADIUS_ATTRS_LIST%'. The 'Save' button is highlighted in the bottom right of the 'Edit RADIUS Attribute Configuration' window.

ExtremeCloud IQ Site Engine

Dashboard Policy Access Control End-Systems Reports

Configuration Group Editor Engines

Engine Groups

Default

NAC/192.168.162.51

All Engines

Engine Group - Default

Details Switches Systems Access Control Engines Guest and IoT Managers

Add... Edit... Delete

IP Address Nickname

10.10.10.10 FE-1

10.10.10.101 FE-2

10.10.10.102 BOBKit_SIM13AE-

192.168.162.1 Laptop GW

192.168.162.11 VSP-1

192.168.162.12 VSP-2

192.168.162.13 VSP-3

Configure Device: 192.168.162.11

Switch Type: Layer 2 Out-Of-Band

Primary Engine: NAC/192.168.162.51

Secondary Engine: None

Auth. Access Type: Network Access

Virtual Router Name:

RADIUS Attributes to Send: Fabric Engine

RADIUS Accounting: Enabled

Management RADIUS Server 1: None

Edit RADIUS Attribute Configuration

Name: Fabric Engine

Enable Port Link Control: ☐

Attributes: Substitutions:

%ORG1_RADIUS_ATTRS_LIST%

Save Close

Make also sure that the right Policy domain is used.

The screenshot shows the ExtremeCloud IQ Site Engine interface. On the left sidebar, the 'Configuration' tab is selected, and the 'Engines' section is expanded, showing the 'Default' engine group. The 'Switches' tab is selected in the main panel. A table lists switches with their IP addresses, nicknames, status, system names, primary engines, policy/VLAN, and policy domain. The switch '192.168.162.11 VSP-1' is highlighted, and its policy domain is 'Automated-Campus'.

ExtremeCloud IQ Site Engine

Dashboard Policy Access Control End-Systems Reports

Configuration Group Editor Engines

Engine Groups

Default

NAC/192.168.162.51

All Engines

Engine Group - Default

Details Switches End-Systems Access Control Engines Guest and IoT Managers

Add... Edit... Delete Refresh

IP Address	Nickname	Status	System Name	Primary Engine	Policy/VLAN	Policy Domain
10.10.10.10	FE-1	Contact Lost	FE-1	192.168.162.51	Extreme VOSS - Per-User ACL	Default Policy Domain
10.10.10.101	FE-2	Contact Lost	FE-2	192.168.162.51	Extreme VOSS - Per-User ACL	Default Policy Domain
10.10.10.102	BOBKit_SIM13AE-0000	Contact Lost	BOBKit_SIM13...	192.168.162.51	Extreme VOSS - Per-User ACL	Default Policy Domain
192.168.162.1	Laptop GW	Contact Est...	192.168.162.1	192.168.162.51	RFC 3580 - VLAN ID	Default Policy Domain
192.168.162.11	VSP-1	Contact No...	VSP-1	192.168.162.51	Fabric Engine	Automated-Campus
192.168.162.12	VSP-2	Contact Lost	VSP-2	192.168.162.51	Extreme VOSS - Fabric Attach	Automated-Campus
192.168.162.13	VSP-3	Contact Lost	VSP-3	192.168.162.51	Extreme VOSS - Fabric Attach	Automated-Campus
192.168.162.14	VSP-4	Contact Lost	VSP-4	192.168.162.51	Extreme VOSS - Fabric Attach	Automated-Campus

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:

The image displays three overlapping screenshots of the 'Edit Custom Criteria Alarm Definition: Sync Policy' dialog box, illustrating the configuration steps for an alarm.

Top Left Screenshot (Criteria Tab):

- Severity: Set from source
- Enabled: ☐
- Custom Criteria:
 - Match On:
 - Category: **Application** (highlighted with a red arrow)
 - Log: **Policy** (highlighted with a red arrow)
 - Information Phrase: **"Enforce finished in policy"** (highlighted with a red arrow)
- Additional Criteria: Select Groups... (text box)
- Buttons: Save, Cancel

Top Right Screenshot (Actions Tab):

- Severity: Set from source
- Enabled: ☒
- Actions:
 - Run Task [Workflow - Sync_PVL_to_Policy_Mappings] (highlighted with a red arrow)
- Alarm Suppression:
 - Enable Alarm Action Limit: ☐
 - Max Count: 5
 - Reset Interval: 0, Never
- Buttons: Save, Cancel

Bottom Screenshot (Other Options Tab):

- Severity: Set from source
- Enabled: ☒
- Clear Conditions:
 - No Current Alarm (action only): ☒ (highlighted with a red arrow)
 - Cleared by Alarms: ☐ (text box)
- Buttons: Save, Cancel

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

```
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
```

```
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 note, this workflow is inspired and prototyped by **Jeff Dattilio** from **STEPCG**