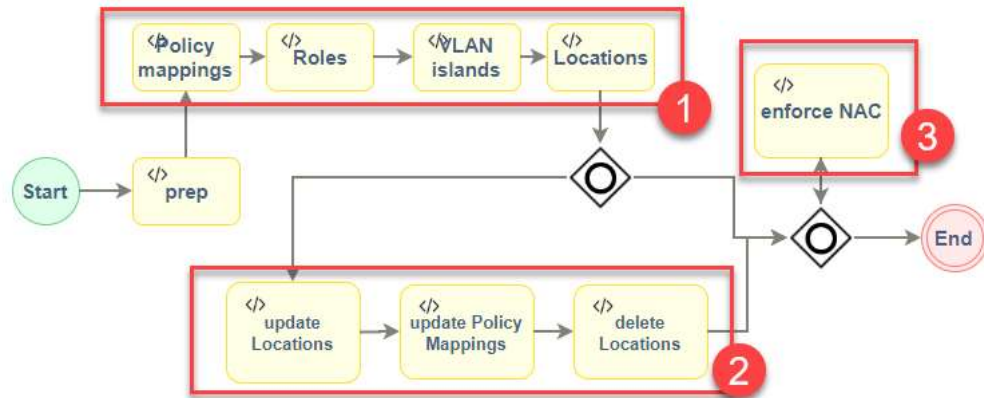


Workflow description

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

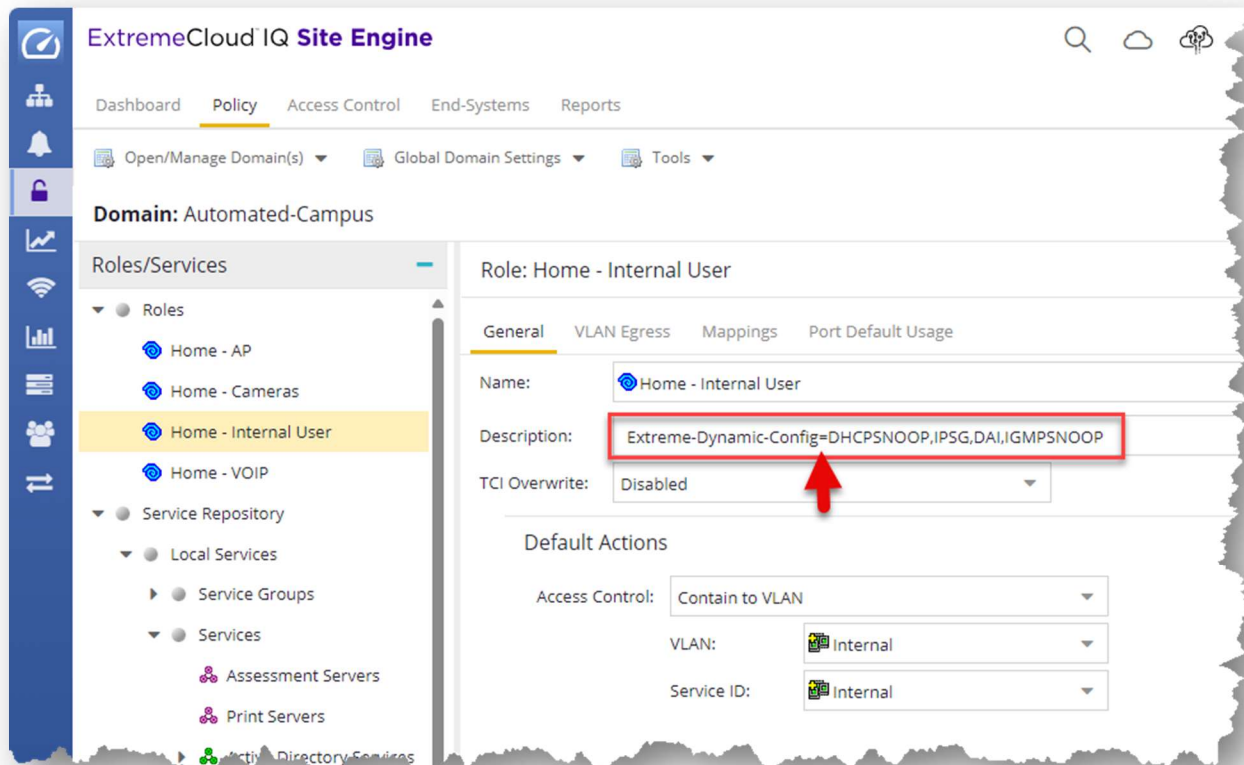
Extreme-Dynamic-Config=DAI

Just be aware, it applies to all policy mappings.

The screenshot shows the 'Variables' tab in the XIQ-SE Administrator interface. 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 (1), and the 'Engines' section is expanded, showing the 'Default' engine group (2). The 'Switches' tab is selected in the main panel (3). A table lists switches, with 'VSP-1' at IP 192.168.162.11 highlighted (4). The 'Configure Device' dialog for 192.168.162.11 is open, showing 'Switch Type' as 'Layer 2 Out-Of-Band' and 'RADIUS Attributes to Send' as 'Fabric Engine' (5). Below this, the 'Edit RADIUS Attribute Configuration' dialog is shown with 'Name' as 'Fabric Engine' and 'Attributes' set to '%ORG1_RADIUS_ATTRS_LIST%'.

Make also sure that the right Policy domain is used.

The screenshot shows the ExtremeCloud IQ Site Engine interface with the 'Switches' tab selected. A table lists switches and their configurations. The 'VSP-1' switch at IP 192.168.162.11 is highlighted, showing its configuration: 'Contact No...', 'VSP-1', '192.168.162.51', 'Fabric Engine', and 'Automated-Campus' (Policy Domain).

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...		192.168.162.51	RFC 3580 - VLAN ID	
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.

Criteria Tab: The 'Match On:' section is configured with the following values:

- Category: **Application** (indicated by a red arrow)
- Type: **Event** (indicated by a red arrow)
- Information Phrase: **"Automated-Campus"** (indicated by a red arrow)

Actions Tab: The 'Run Task' action is selected, specifically the workflow **[Workflow - Sync_PVI_to_Policy_Mappings]** (indicated by a red arrow).

Other Options Tab: The 'Clear Conditions' section is configured with the following values:

- No Current Alarm (action only): ☒ (indicated by a red arrow)
- Cleared by Alarms: ☐ (with a text input field and a clear button 'X')

The dialog box also includes a 'Severity' dropdown set to 'Set from source', an 'Enabled' checkbox checked, and 'Alarm Suppression' options (Enable Alarm Action Limit, Max Count: 5, Reset Interval: 0, Never).

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
```