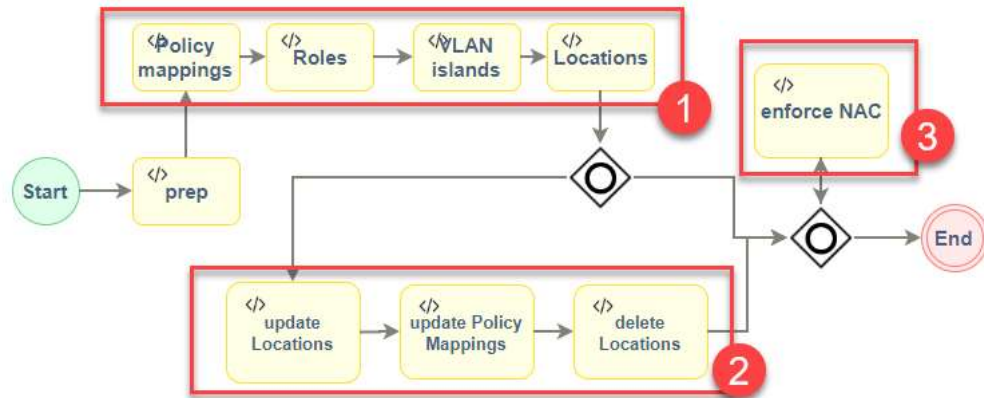


## Workflow description

### 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**

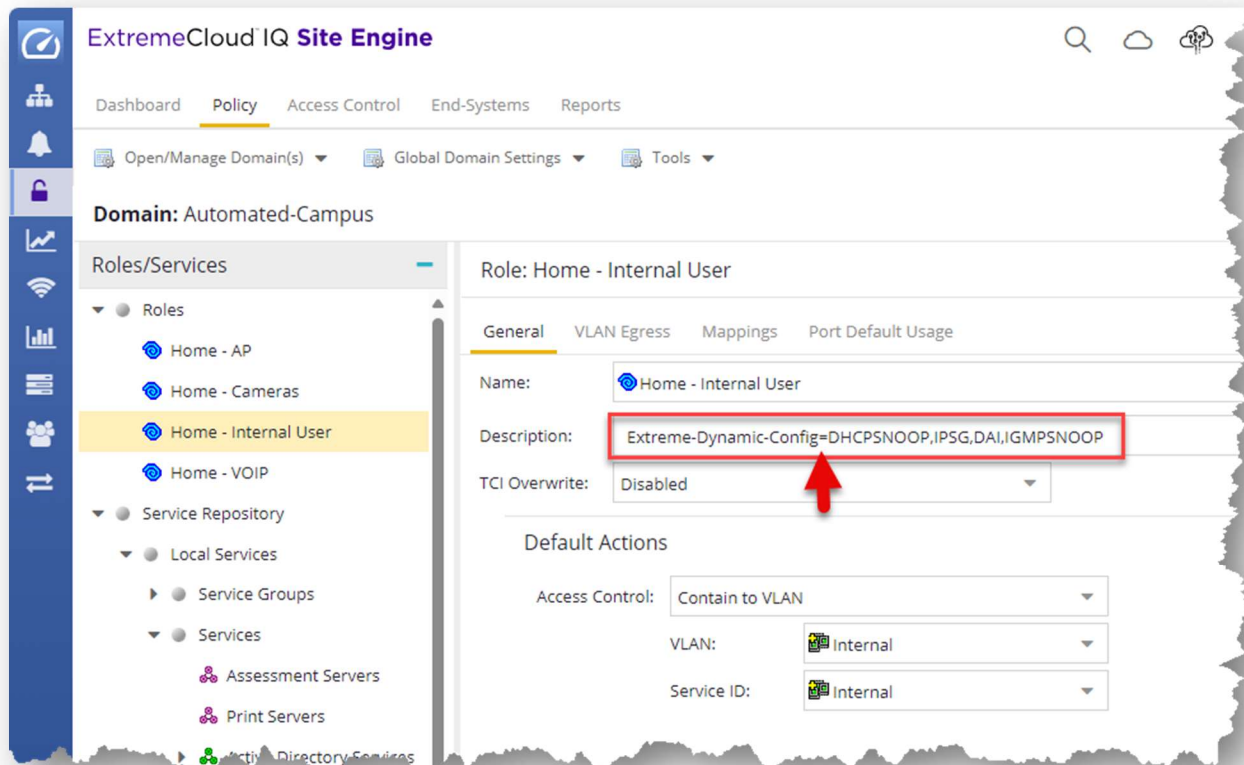
**Extreme-Dynamic-Config=DAI**

Just be aware, it applies to all policy mappings.

The screenshot shows the 'Variables' tab in the XIQ-SE Administrator. The table lists various workflow variables. The 'Extreme\_Dynamic\_Config' variable is highlighted with a red box, indicating its default value is 'SLPPGUARD'.

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. The left sidebar has a lock icon highlighted with a red circle and the number 1. The 'Engines' section is expanded, and 'Default' is selected with a red circle and the number 2. The 'Switches' tab is active, and the 'VSP-1' switch is highlighted with a red circle and the number 4. A red arrow points from the 'VSP-1' switch to the 'Configure Device: 192.168.162.11' dialog box. The 'Switches' tab is also highlighted with a red circle and the number 3. The 'Configure Device' dialog box shows the 'Switch Type' as 'Layer 2 Out-Of-Band', 'Primary Engine' as 'NAC/192.168.162.51', 'Secondary Engine' as 'None', 'Auth. Access Type' as 'Network Access', 'Virtual Router Name' as empty, 'RADIUS Attributes to Send' as 'Fabric Engine' (highlighted with a red box), 'RADIUS Accounting' as 'Enabled', and 'Management RADIUS Server 1' as 'None'. Below the dialog box, the 'Edit RADIUS Attribute Configuration' dialog box is open, showing the 'Name' as 'Fabric Engine', 'Enable Port Link Control' as unchecked, and 'Attributes' as '%ORG1\_RADIUS\_ATTRS\_LIST%' (highlighted with a red box). The 'Substitutions' field is empty.

ExtremeCloud IQ Site Engine

Dashboard Policy Access Control End-Systems Reports

Configuration +

Group Editor +

Engines

Engine Groups

Default 2

NAC/192.168.162.51

All Engines

Engine Group - Default

Details Switches 3 Systems Access Control Engines Guest and IoT Managers

Add... Edit... Delete

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. The left sidebar has a lock icon highlighted with a red circle and the number 1. The 'Engines' section is expanded, and 'Default' is selected with a red circle and the number 2. The 'Switches' tab is active, and the 'VSP-1' switch is highlighted with a red circle and the number 4. The 'Configure Device: 192.168.162.11' dialog box is open, showing the 'Switch Type' as 'Layer 2 Out-Of-Band', 'Primary Engine' as 'NAC/192.168.162.51', 'Secondary Engine' as 'None', 'Auth. Access Type' as 'Network Access', 'Virtual Router Name' as empty, 'RADIUS Attributes to Send' as 'Fabric Engine' (highlighted with a red box), 'RADIUS Accounting' as 'Enabled', and 'Management RADIUS Server 1' as 'None'. Below the dialog box, the 'Edit RADIUS Attribute Configuration' dialog box is open, showing the 'Name' as 'Fabric Engine', 'Enable Port Link Control' as unchecked, and 'Attributes' as '%ORG1\_RADIUS\_ATTRS\_LIST%' (highlighted with a red box). The 'Substitutions' field is empty.

ExtremeCloud IQ Site Engine

Dashboard Policy Access Control End-Systems Reports

Configuration +

Group Editor +

Engines

Engine Groups

Default 2

NAC/192.168.162.51

All Engines

Engine Group - Default

Details Switches 3 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...		192.168.162.51	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

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
```