A picture containing text

Description automatically generated

# XIQ-SE JAMF ES Group

# Sync Workflows

Table of Contents

[Introduction 3](#_Toc198130798)

[Add JAMF Credentials to XIQ-SE 3](#_Toc198130799)

[Installing the JAMF ES Group Sync Workflow 5](#_Toc198130800)

[Running the JAMF ES Group Sync Workflow 6](#_Toc198130801)

[Advanced Setup for the JAMF ES Group Sync Workflow 8](#_Toc198130802)

Introduction

This document provides instructions for installing and using the JAMF ES Group Sync Workflows within XIQ-SE. The solution consists of two separate workflows:

* **JAMF\_Computer\_Sync**: Queries the JAMF API to retrieve records for Mac laptops.
* **JAMF\_Mobile\_Sync**: Queries the JAMF API to retrieve records for iOS devices.

Each workflow extracts the MAC addresses from the respective JAMF device records. Simultaneously, they perform Northbound Interface (NBI) queries to obtain the current list of MAC addresses associated with their corresponding End-System (ES) Groups in XIQ-SE.

⚠️ **Important:** Each workflow must be mapped to a **separate ES Group** in XIQ-SE. This is necessary to prevent the two workflows from overwriting each other's data during synchronization.

The script compares the MAC address lists from JAMF and XIQ-SE and automatically updates the appropriate ES Group by adding or removing MAC addresses, ensuring each group reflects the accurate set of devices registered in JAMF.

Add JAMF Credentials to XIQ-SE

To perform the necessary API call and retrieve device data, each Workflow must first generate an API token. This is accomplished by submitting JAMF credentials to the /v1/auth/token endpoint. For enhanced security, these JAMF credentials can be securely stored within the Site Engine Profiles.

* Go to **Administration** on the left
* Select **CLI Credentials** in the bottom pane
* Select **Add**

A screenshot of a computer

AI-generated content may be incorrect.

* A screenshot of a computer login box

  AI-generated content may be incorrect.Enter a description
* JAMF username
* JAMF password

Note: leave the type as SSH, you do not need to enter anything for the Enable or Configuration password

* Select **Add** in the top pane to create the Profile

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

* Give the **profile** the name JAMF\_API
* For CLI Credentials, select the **CLI Credentials** you just created.

Installing the JAMF ES Group Sync Workflows

The JAMF ES Group Sync Workflows can be imported into a XIQ-SE appliance.

* Go to the **Tasks** tab on the left
* Select the **Workflows** tab
* Select either the **Workflows** folder or a **subfolder**
* Click the **gear** on the bottom and select **import**

Graphical user interface, application, Teams

Description automatically generated

* Choose **Select Files** and locate the **.xwf** file
* Click **Import**

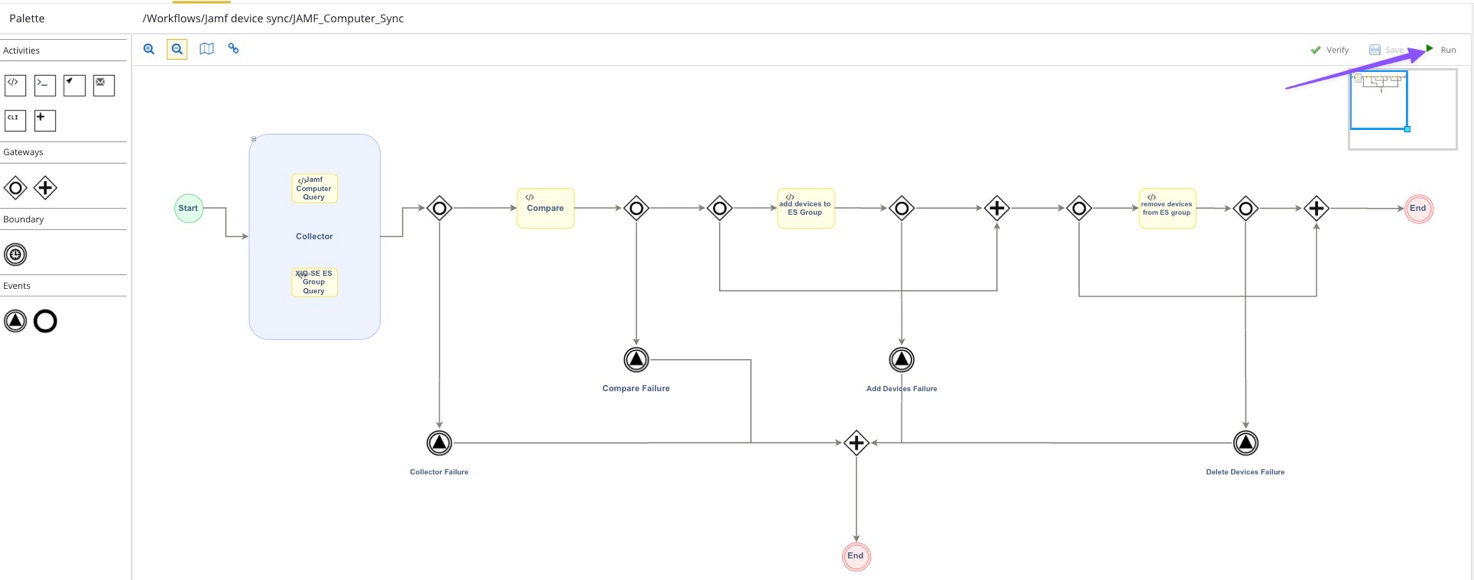
Graphical user interface, application, Teams

Description automatically generated

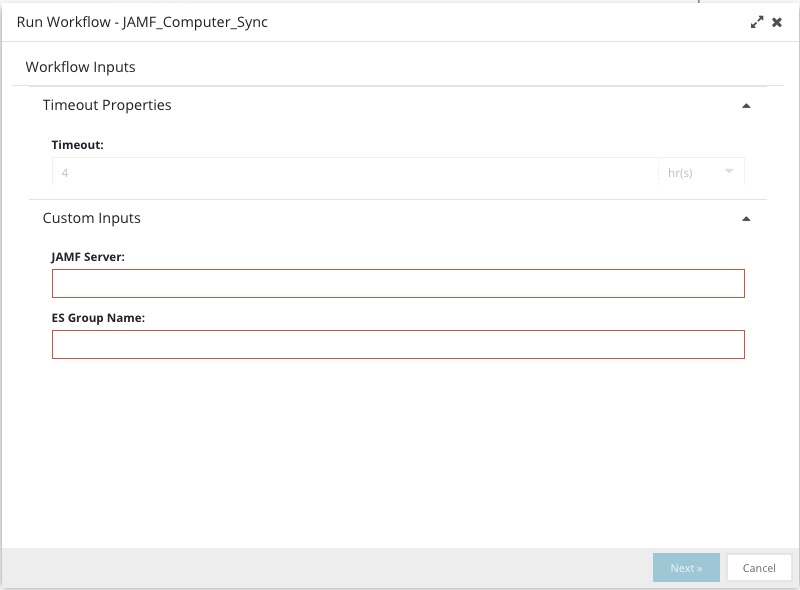
* Repeat for both Workflows

Running the JAMF ES Group Sync Workflows

Each workflow can be run by clicking **run** in the workflow window. The workflows function the same way.

Running the Workflow

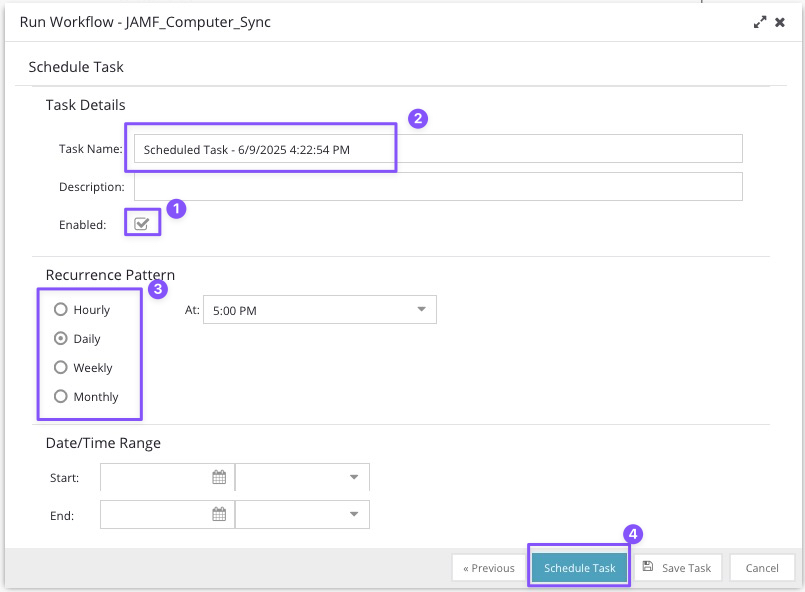
* Enter the JAMF server name (your organization name), and the name of the End-Systems Group you would like to sync.



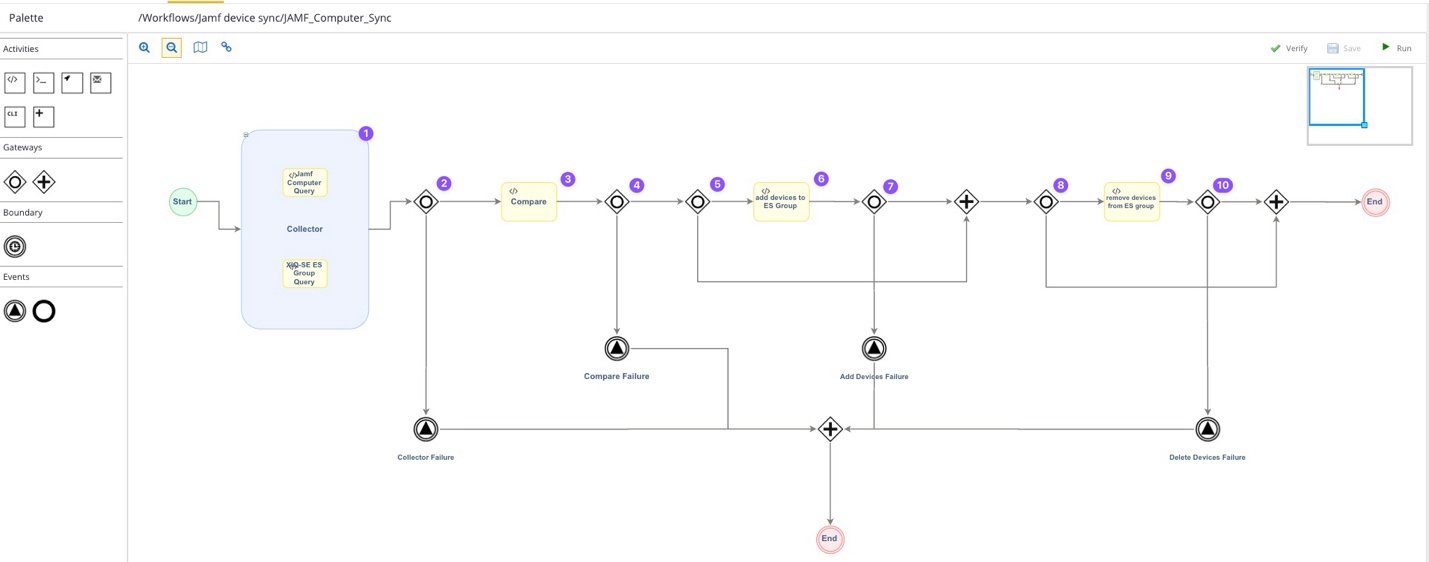
You can also create a schedule for the workflow to run. You can save it as a task and schedule the workflow to run.

Scheduling a Task

1. Select Enable for Schedule Task
2. Name the Schedule Task
3. Set the frequency you want the workflow to run. You could run hourly or Daily
4. Click Schedule Task



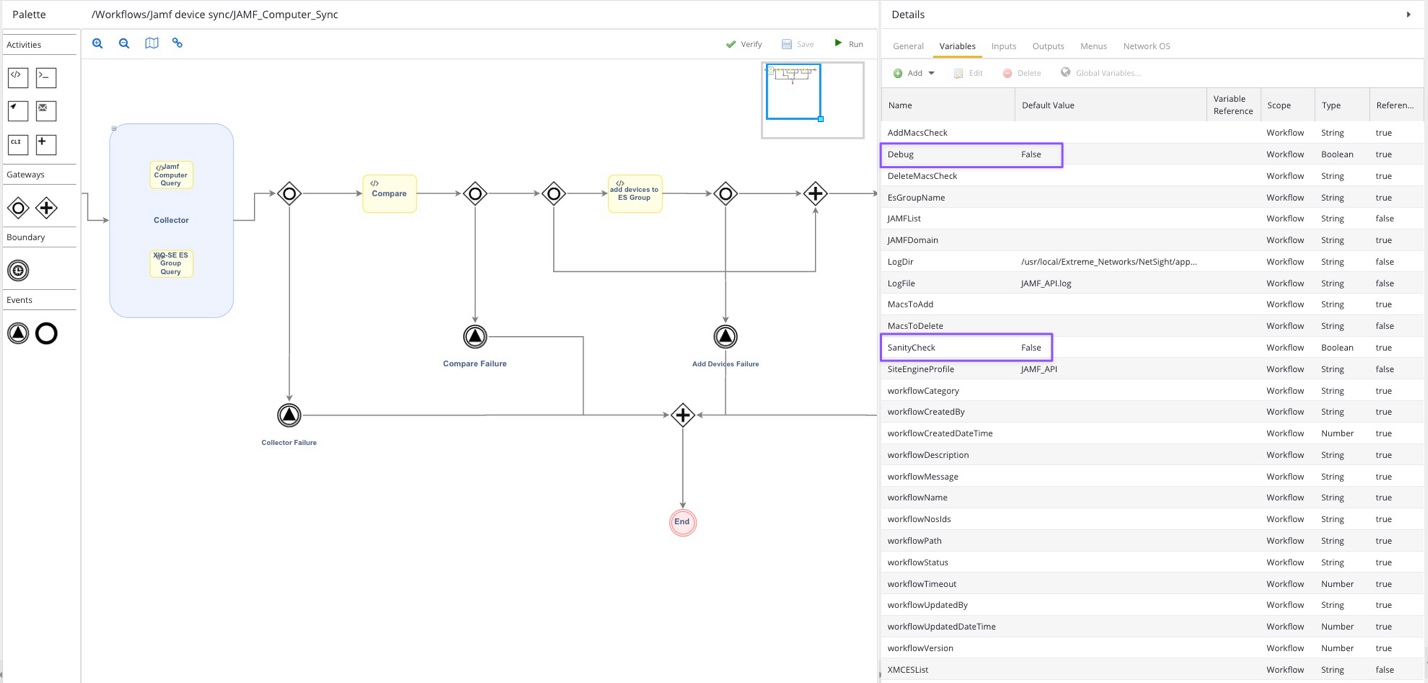
How the Workflows work

****

1. **Collector** – The first section consists of 2 scripts that run simultaneously.
   * **Jamf <Computer or Mobile> Sync** – Using the Jamf Pro API, this script collects the MAC addresses of Mac Computers or Mobile devices from JAMF and saves the list to the **JAMFList** variable.
   * **XIQ-SE ES Group Query** – Using the NBI Query, this script will collect the MAC addresses in the End-Systems group from Control and saves the list to the **XMCESList** variable.
2. Gateway – If either Collector scripts fail, the Collector Failure Alert will occur, and the workflow will end.
3. **Compare** – This script will load and compare the **JAMFList** and **XMCESList** variables. This script will look for MAC addresses that need to be added or removed from the ES Group.
   * If MAC addresses need to be added to the ES Group, the **AddMacsCheck** variable is set to true, and the addresses to be added are put in the **MacsToAdd** variable.
   * If MAC addresses need to be removed from the ES Group, the **DeleteMacsCheck** is set to true, and the addresses to be removed are put in the **MacsToDelete** variable.
4. Gateway – If the Compare script fails, the Compare Failure Alert will occur, and the workflow will end.
5. Gateway – If the **AddMacsCheck** variable is set to true by the add devices to ES Group script will run; otherwise, the Workflow will bypass the script and proceed to step 8.
6. **Add devices to ES Group** – This script will add all devices in the MacsToAdd variable to the ES Group.
7. Gateway – If the add devices to ES Group script fails, the Add Devices Failure Alert will occur, and the workflow will end.
8. Gateway – If the **DeleteMacsCheck** variable is set to true by the remove devices to ES Group script will run; otherwise, the Workflow will bypass the script.
9. **Remove devices from ES Group** – This script will remove all devices in the MacsToDelete variable from the ES Group.
10. Gateway – If the remove devices from ES Group script fails, the Delete Devices Failure Alert will occur, and the workflow will end.

Testing the JAMF ES Group Sync Workflows

The **Debug** and **SanityCheck** variables help test and troubleshoot the JAMF ES Group Sync Workflows in XIQ-SE. When Debug is on, the scripts print extra details, like API results and logs, to help spot issues or check the process. The SanityCheck variable, when enabled, stops the workflows from changing MAC addresses in XIQ-SE ES Groups and instead shows the JSON data that would be sent, letting you review changes safely. Together, they make testing and fixing the workflows easier and safer.



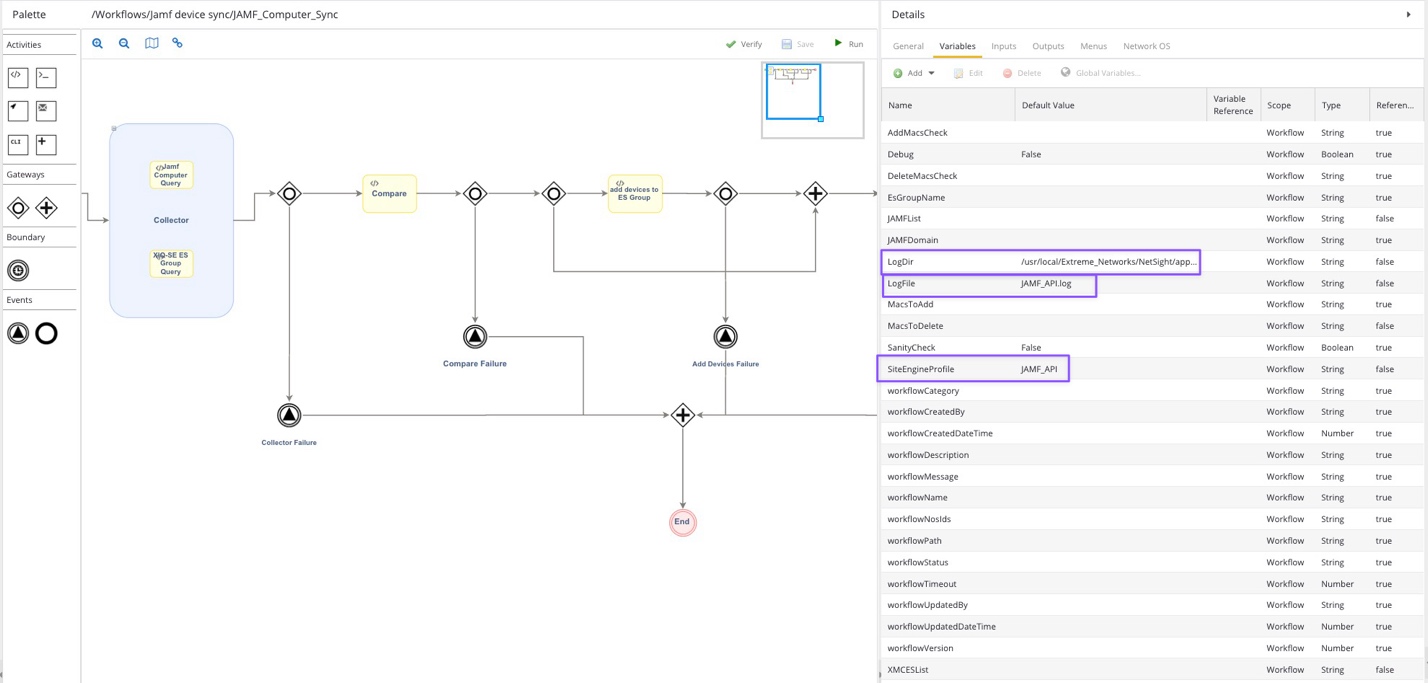
Advanced Setup for the JAMF ES Group Sync Workflows

The Workflow will save any changes to the ES Group in a log file. These 2 Variables can be changed to change the location of the log file.

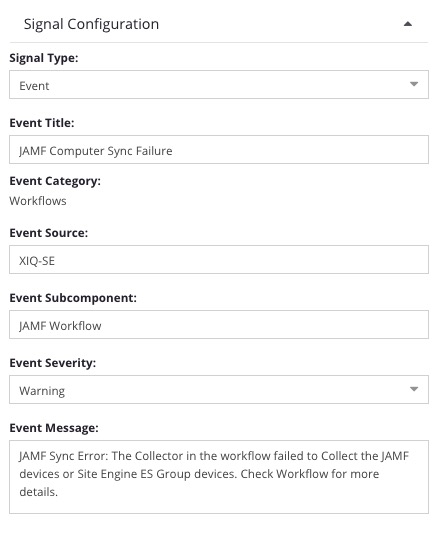
1. LogDir ==> /usr/local/Extreme\_Networks/NetSight/appdata/logs/scripting/JAMF\_Sync
2. LogFile ==> JAMF\_API.log

You can also change the name of the Site Engine Profile to be used.

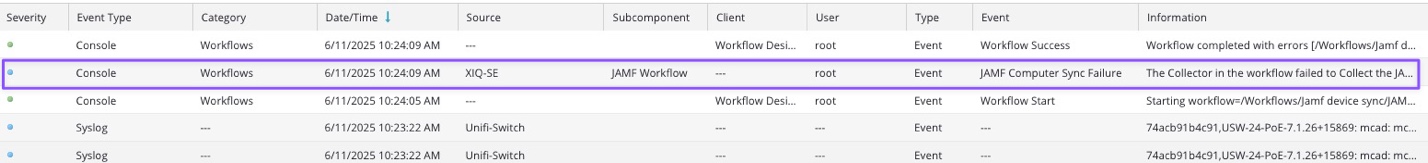
* SiteEngineProfile==> JAMF\_API



Alerting

If there are failures in any of the scripts in the workflow an alert should be created. The Event Title will either be “JAMF Computer Sync Failure” or “JAMF Mobile Sync Failure”

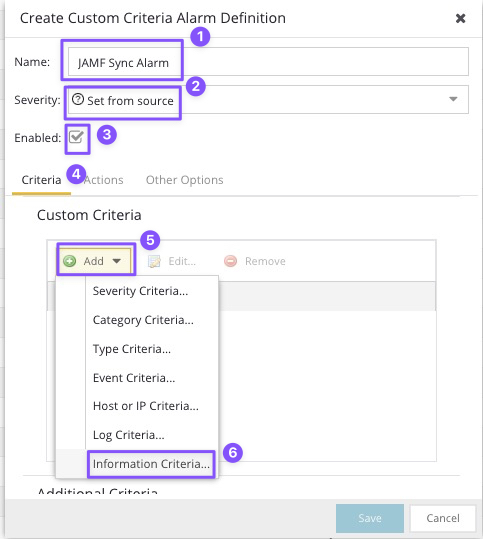
The Event Sources is set to XIQ-SE and Event Subcomponent is ‘JAMF Workflow’

The Event message will identify which script had the issue. Each event starts with “JAMF Sync Error: “

Building an Alarm from the Event

Under Alarm configuration, you can add a Custom Criteria Alarm.A screenshot of a computer

Description automatically generated

In this window you will want to

1. name the alarm
2. set the severty
   1. The Workflow will set the Severity to “Warning” but can be overwritten here.
3. check the box to enable the alarm
4. Add a Custom Criteria to search the Information Critera.

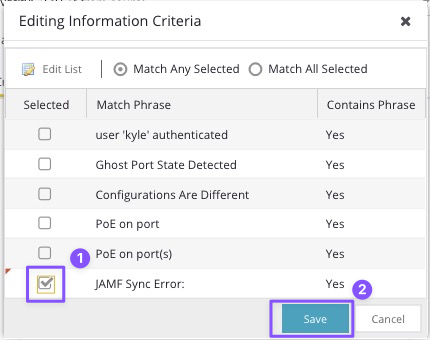
A screenshot of a computer

Description automatically generated

This will open a window, select the Edit List button.

A screenshot of a computer

AI-generated content may be incorrect.Here you can add the Phrase “JAMF Sync Error:” This is included in each message of the Events.

After you’ve added that to the list. Scroll down and check that Phrase and click Save.

A screenshot of a computer

AI-generated content may be incorrect.Then Back in the Alarm Definition select Actions. This will let you configure the Alarm to email a group when this Alarm is triggered.

A screenshot of a email action

Description automatically generatedYou will then have the Alarm showing under Alarm Configuration.