Flowmon ADS and Superna Ransomware Defender

Configuration Guide

UPDATED: 1 September 2023

Table of Contents

1 Introduction

By integrating network detection with storage layer defense, organizations can gain an upper hand on mitigating threat actors by providing early warning, detection, and remediation of ransomware attempts. Ransomware Defender's combined solution with Progress Flowmon means that business critical business data is protected and enterprise recovery objective targets can be met and exceeded. This guide provides the necessary configuration steps to enable the Progress Flowmon and Superna Ransomware Defender integration.

1.1 Document Purpose

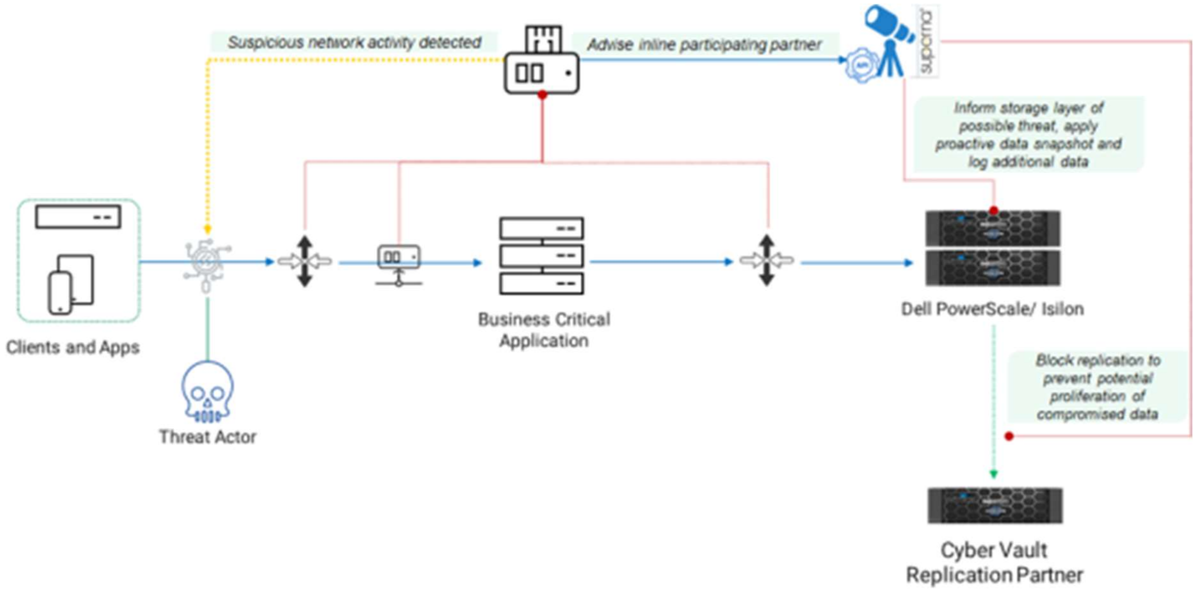
This document provides the recommended settings used when integrating Progress Flowmon (Anomaly Detection System) ADS and Superna Ransomware Defender to secure storage in the enterprise. The Progress Support team is available to provide solutions for scenarios not explicitly defined. The Support site can be found at: https://support.kemptechnologies.com.

1.2 Intended Audience

Anyone who is interested in configuring Progress Flowmon ADS and Superna Ransomware Defender.

2 Architecture

The deployment consists of a Progress Flowmon Collector with the ADS module, a Progress Flowmon Probe, Superna Ransomware Defender with the Smart AirGap Application Programming Interface (API) feature license, and (in this example) Dell PowerScale/Isilon.

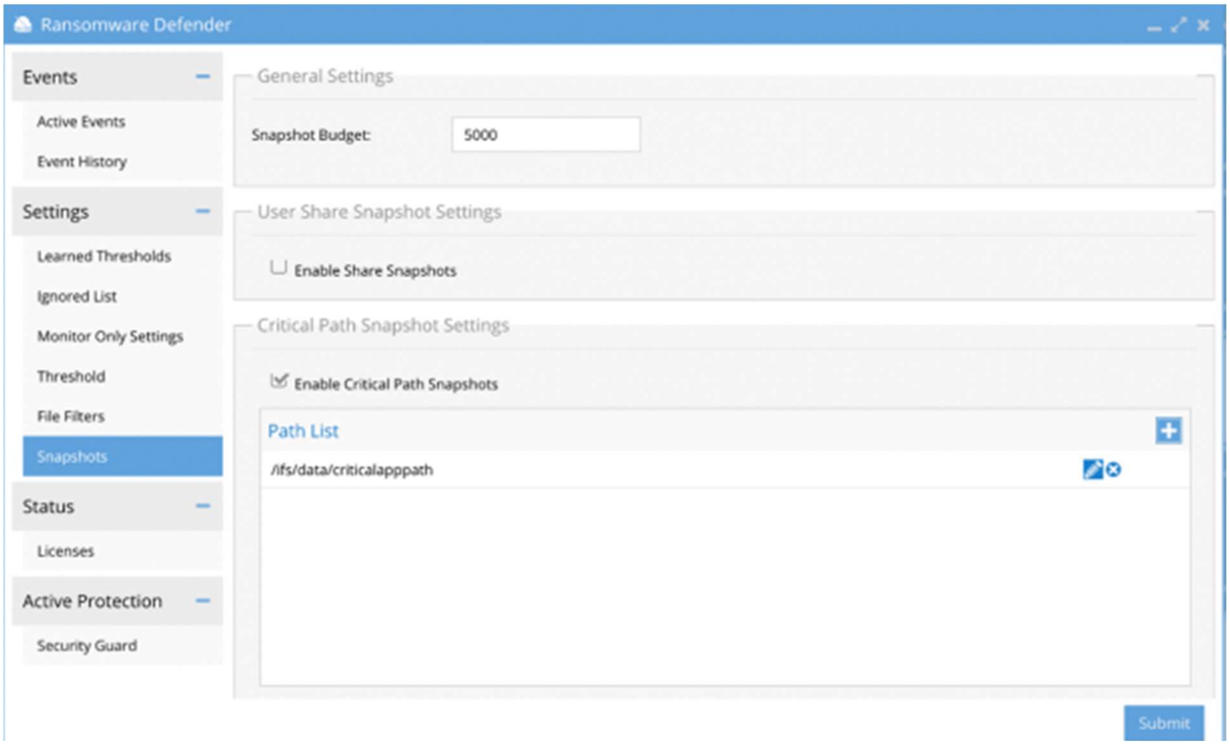

Suspicious network activity detected
Advise inline participating partner
superna
Inform storage layer of possible threat, apply proactive data snapshot and log additional data
Clients and Apps
Business Critical Application
Dell PowerScale/ Isilon
Threat Actor
Block replication to prevent potential proliferation of compromised data
Cyber Vault Replication Partner

3 Configure Superna Ransomware Defender

Defaults allow one snapshot request per hour and a four-hours expiry on snapshots. These values can be changed.

Follow these steps to configure the Superna Randomware Defender:

1. Apply the Smart Airgap API following license key apply procedures to activate the external API for 3rd party integration.



Snapshot Budget: 5000

□ Enable Share Snapshots

☑ Enable Critical Path Snapshots

Path List

/ifs/data/criticalapppath

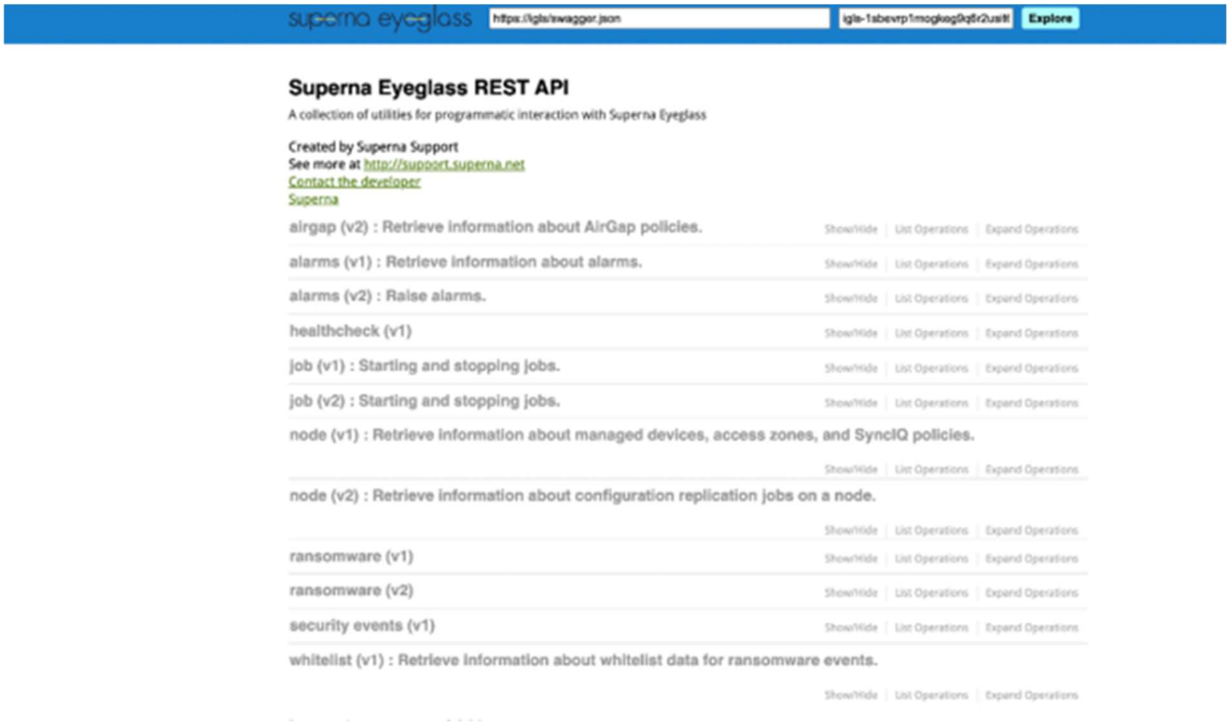
2. Ensure that the critical path feature is enabled and that SMB share snapshots are disabled.

3. Log in to the Superna Eyeglass Virtual Machine (VM).

4. Using the API explorer to build the cURL command with an authentication token to integrate with the Intrusion Detection System (IDS) or Intrusion Protection System (IPS) system that will used to integrate with Ransomware Defender.

5. Open the Eyeglass main menu and select **Eyeglass REST API**. Generate a new API token and provide a name, for example, **smartairgap**. Copy the API token and click **API Explorer**.

6. Click **Ransomware Defender API** and select the critical path route. Click **Generate** to produce a cURL command to request that critical paths get a snapshot applied.


superna eyeglass
https://igls/swagger.json
igls-1abevrp1mogkog9q6r2usit
Explore
Show/Hide | List Operations | Expand Operations

Superna Eyeglass REST API

A collection of utilities for programmatic interaction with Superna Eyeglass

Created by Superna Support
See more at http://support.superna.net
Contact the developer
Superna

airgap (v2) : Retrieve information about AirGap policies.

alarms (v1) : Retrieve information about alarms.

alarms (v2) : Raise alarms.

healthcheck (v1)

job (v1) : Starting and stopping jobs.

job (v2) : Starting and stopping jobs.

node (v1) : Retrieve information about managed devices, access zones, and SyncIQ policies.

node (v2) : Retrieve information about configuration replication jobs on a node.

ransomware (v1)

ransomware (v2)

security events (v1)

whitelist (v1) : Retrieve information about whitelist data for ransomware events.

7. The following is an example cURL command that is integrated into network security devices:

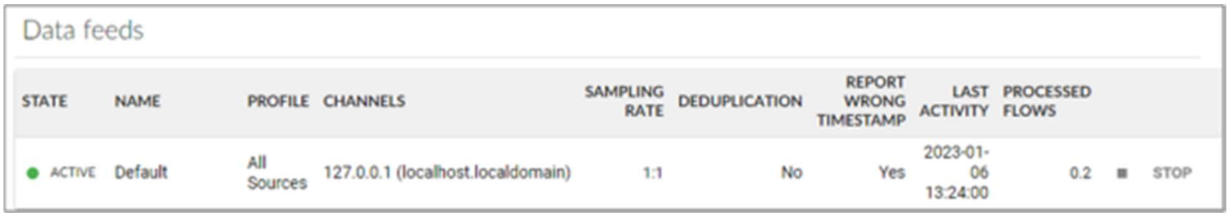
```
curl -k -X POST --header 'Content-Type: application/json' --header 'Accept:
application/json' --header 'api_key: <APIKey>'
'https://x.x.x.x/sera/v2/ransomware/criticalpaths' -d "{}"
```

4 Configure Progress Flowmon Anomaly Detection System (ADS)

Refer to the following sections for step-by-step instructions on how to configure ADS.

4.1 Start Data Feed

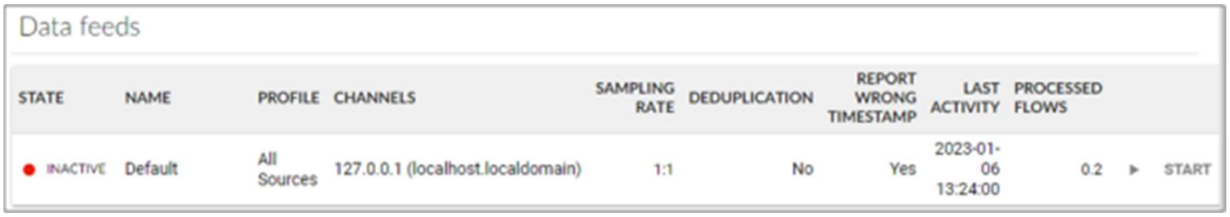
Within the ADS module, go to **Settings > Data feeds**.



Data feeds

STATE	NAME	PROFILE	CHANNELS	SAMPLING RATE	DEDUPLICATION	REPORT WRONG TIMESTAMP	LAST ACTIVITY	PROCESSED FLOWS		
● ACTIVE	Default	All Sources	127.0.0.1 (localhost.localdomain)	1:1	No	Yes	2023-01-06 13:24:00	0.2	■	STOP

If the **Default** Data Feed is active there is no action to be taken.



Data feeds

STATE	NAME	PROFILE	CHANNELS	SAMPLING RATE	DEDUPLICATION	REPORT WRONG TIMESTAMP	LAST ACTIVITY	PROCESSED FLOWS		
● INACTIVE	Default	All Sources	127.0.0.1 (localhost.localdomain)	1:1	No	Yes	2023-01-06 13:24:00	0.2	▶	START

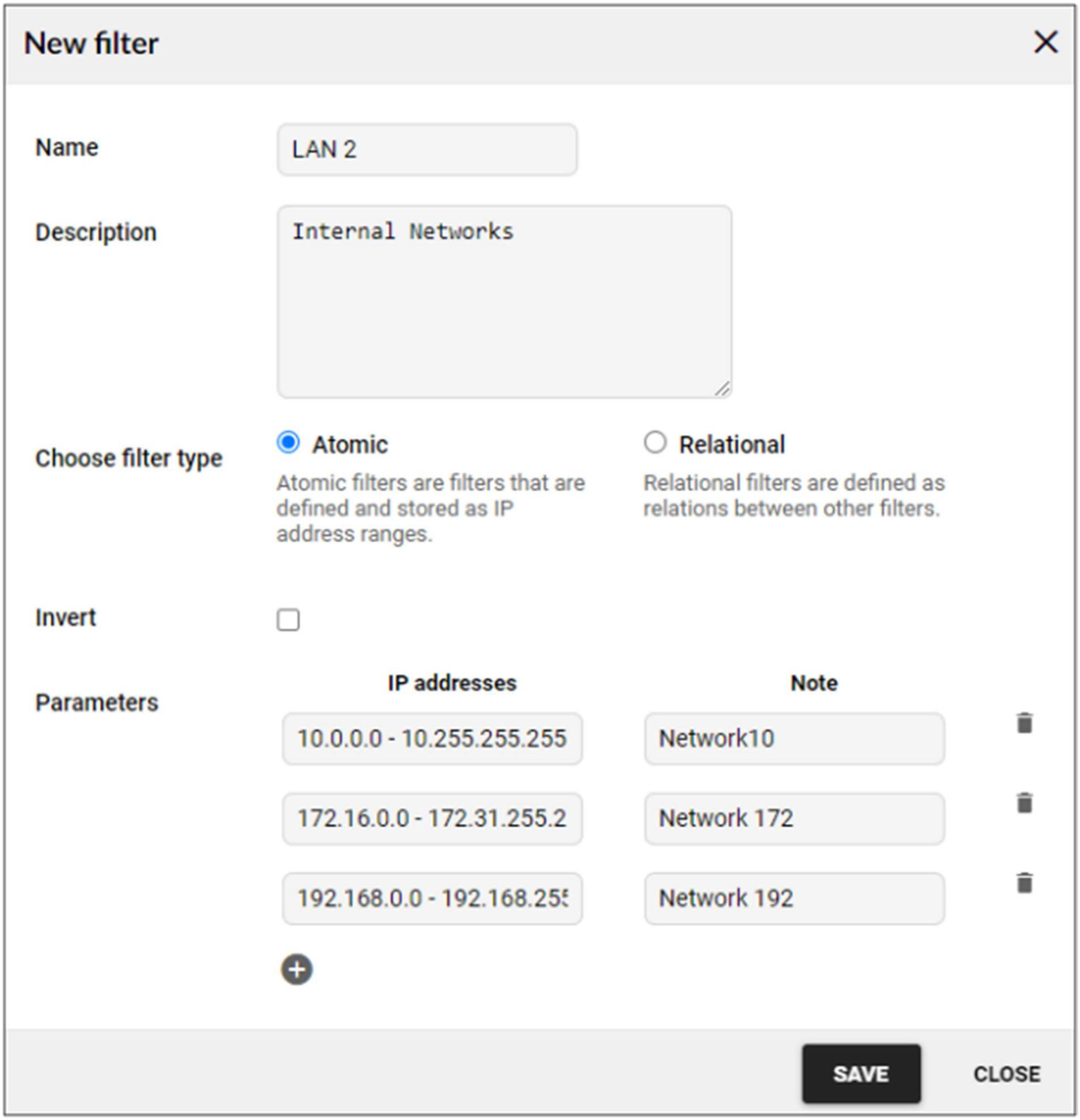
If the **Default** Data feed is not **ACTIVE**, click **Start**.

4.2 Create a Filter

Filters are used when creating a Perspective. The filter identifies what networks require monitoring for anomalies.

1. Within the ADS Module, go to **Settings > Processing > Filters**.

2. Click **+ NEW FILTER**.



New filter

Name: LAN 2

Description: Internal Networks

Choose filter type

● Atomic
Atomic filters are filters that are defined and stored as IP address ranges.

○ Relational
Relational filters are defined as relations between other filters.

Invert □

Parameters

IP addresses	Note
10.0.0.0 - 10.255.255.255	Network10
172.16.0.0 - 172.31.255.2	Network 172
192.168.0.0 - 192.168.25!	Network 192

EXAMPLE ONLY

a) Provide a **Name**.

b) Select **Atomic**.

c) Under **Parameters** add the networks that should be monitored for anomalies.

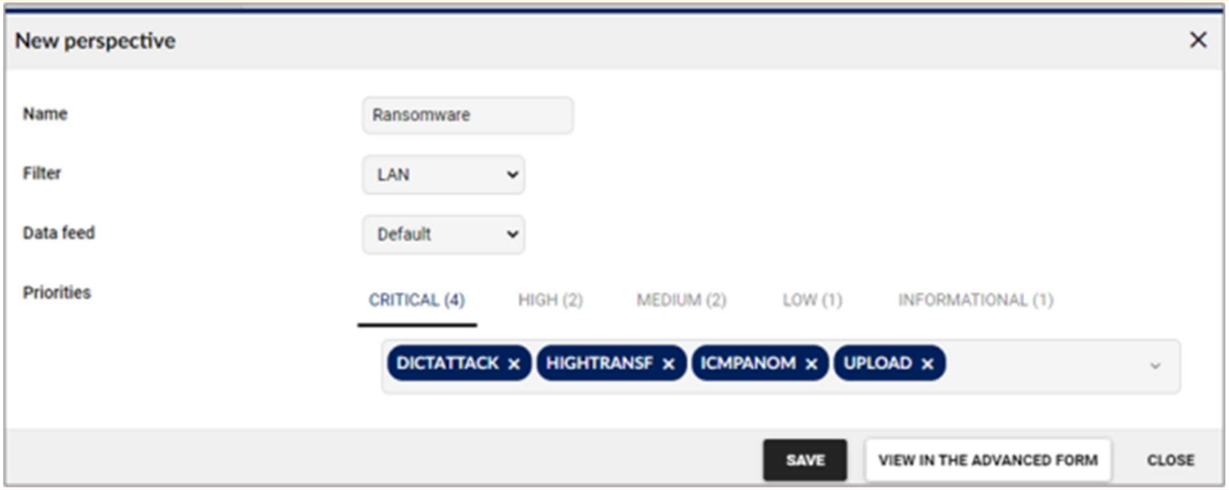
d) Click **SAVE**.

4.3 Create Perspective(s)

You can create one or more Perspectives to identify anomalies on the network.

This document provides an **example only**. In production, you must identify what traffic your organization would like to enable alerts and triggers on.

1. Within the ADS module, go to **Settings > Processing > Perspectives**.
2. Click **+ NEW PERSPECTIVE**.



New perspective

Name: Ransomware

Filter: LAN

Data feed: Default

Priorities: CRITICAL (4) | HIGH (2) | MEDIUM (2) | LOW (1) | INFORMATIONAL (1)

DICTATTACK × HIGHTRANSF × ICMPANOM × UPLOAD ×

EXAMPLE ONLY

a) Provide a **Name**.

b) Select the relevant **Filter**.

c) Select the relevant **Data feed**.

d) Select the priority (**Critical**, **High**, **Medium**, **Low**, and **Informational**) and add the relevant items to each priority.

e) Click **SAVE**.

4.4 Create an Email Notification

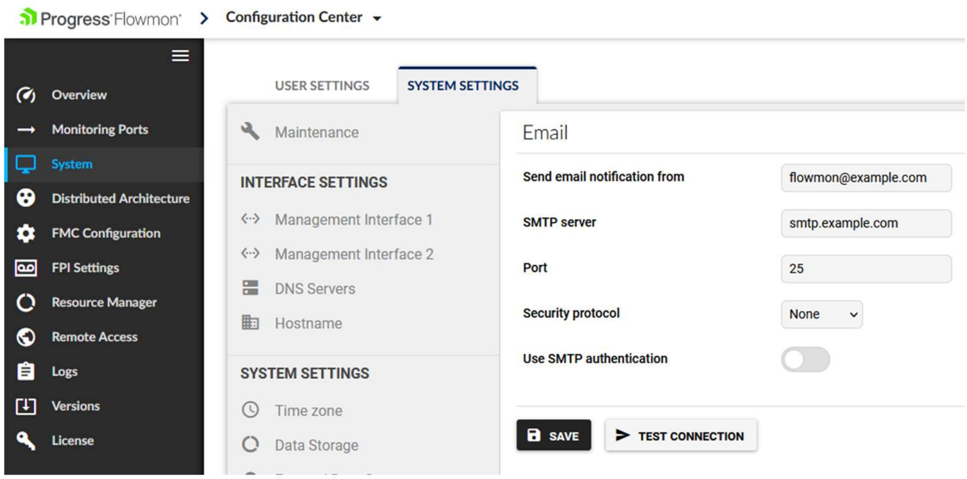
Each email notification must be bound to exactly one perspective. A notification can be in the active or inactive state. An inactive notification is defined in the system but is not being sent regularly. The option **Do not send empty reports** stops empty daily or weekly summary reports from being sent. Immediate reports, one-hour, and six-hour summaries are never sent empty to avoid spamming mailboxes. There is also an option called **Minimal priority to be reported** where you can specify the minimum priority of events to report. Reports are sent per the following rules:

- **CRITICAL:** report immediately after processing of the flow data (a blank report is never sent)
- **HIGH:** report in hourly summaries
- **MEDIUM:** report in six-hours summaries
- **LOW:** report in daily summaries
- **INFORMATION:** report in weekly summaries

4.4.1 Configure the Email/ SMTP Server

An SMTP server must be provided within the Flowmon Configuration Center prior to creating the Email notification.

1. Launch the Flowmon **Configuration Center**.
2. Go to **System > System Settings > Email**.



Email

Send email notification from: flowmon@example.com

SMTP server: smtp.example.com

Port: 25

Security protocol: None

Use SMTP authentication: ○

3. Provide the following:

a) In the **Send email notification from** text box, specify the email address to send emails from.

b) Enter an IP address or Fully Qualified Domain Name (FQDN) for the **SMTP server**.

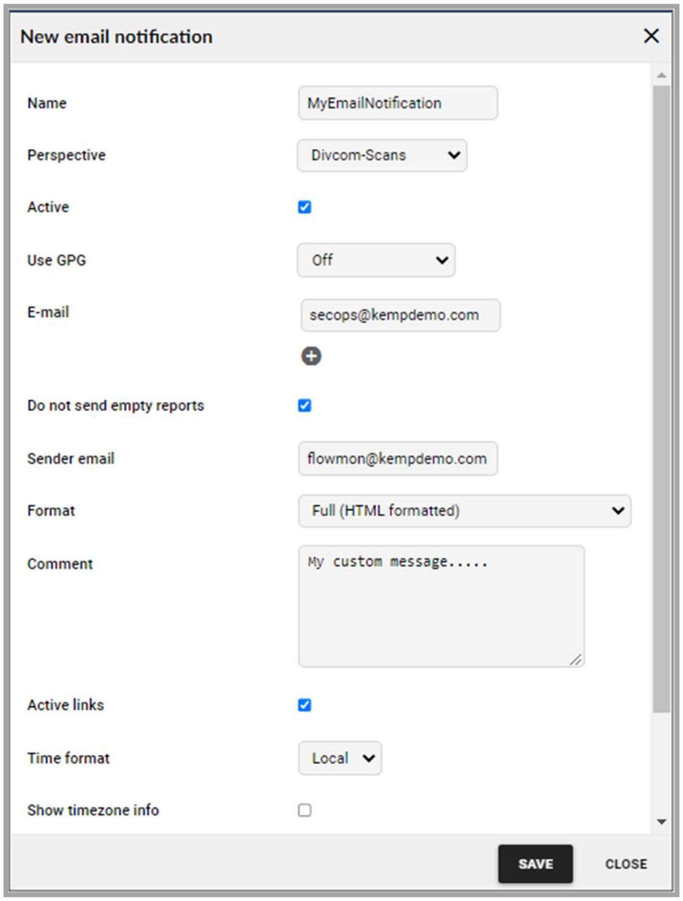
c) Enter the SMTP **Port**.

d) Provide the **Security protocol** (optional).

e) Select whether to **Use SMTP authentication** (optional).

f) Click **SAVE**.

4.4.2 Create a Notification



New email notification

Name	MyEmailNotification
Perspective	Divcom-Scans
Active	☑
Use GPG	Off
E-mail	secops@kempdemo.com
Do not send empty reports	☑
Sender email	flowmon@kempdemo.com
Format	Full (HTML formatted)
Comment	My custom message.....
Active links	☑
Time format	Local
Show timezone info	☐

1. Within the ADS Module, go to **Settings > Email notification**.

2. Click **+ NEW EMAIL NOTIFICATION**.

3. Provide a **Name**.
4. Select the relevant **Perspective**.
5. Select the **Active** checkbox to enable the notification.
6. Select the **Use GPG** setting (optional).
7. Enter an email address to send the notifications to.

    a) Click **+** to add additional addresses (optional).

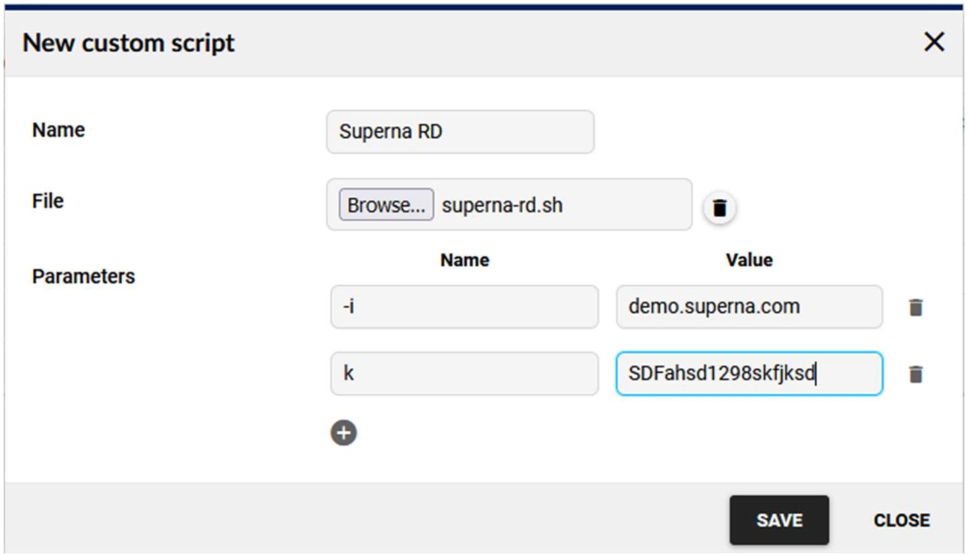
8. Enable or disable the **Do not send empty reports** check box.
9. Provide a **Sender email** address.
10. Select the **Format** to use.
11. Provide a custom **Comment** (optional and dependent on **Format** used).
12. Ensure the **Active links** checkbox is enabled.
13. Select **Time format**.
14. Select the **Minimal priority to be reported** based on the selections within the Perspective.
15. Click **SAVE**.

4.5 Create a Custom Script (Superna Trigger)

In Flowmon ADS, custom scripts are used to automate actions when activities are needed based on the configured Perspective. Each custom script must be bound to exactly one Perspective. A script can be in the active or inactive state.

You can use the script provided by us which accepts the parameters for IP addresses/hostname of Superna Ransomware Defender and API key.

1. Within the ADS Module, go to **Settings > System Settings > Custom scripts**.
2. Click **+ NEW CUSTOM SCRIPT**.
3. Provide a **Name** for the script.
4. Under **File**, click **Choose file** and select the custom script to trigger Superna Ransomware Defender actions.



New custom script

Name: Superna RD

File: superna-rd.sh

Parameters

Name	Value
-i	demo.superna.com
k	SDFahsd1298skfjksd

5. Click **SAVE**.

6. Within the ADS Module, go to **Settings > Processing > Custom scripts**.

7. Click **+ NEW CUSTOM SCRIPT ACTION**.

8. Provide a **Name** for the action.

9. Select the **Perspective**.

10. Tick the box to make the action **Active**.

11. Set the **Minimum priority to be reported**.

12. Click **SAVE**.

Last Updated Date

This document was last updated on 1 September 2023.