**Configuration Guide** 

UPDATED: 1 September 2023

1 Introduction

# © 2023 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

These materials and all Progress® software products are copyrighted and all rights are reserved by Progress Software Corporation. The information in these materials is subject to change without notice, and Progress Software Corporation assumes no responsibility for any errors that may appear therein. The references in these materials to specific platforms supported are subject to change.

#1 Load Balancer in Price/Performance, 360 Central, 360 Vision, Chef, Chef (and design), Chef Habitat, Chef Infra, Code Can (and design), Compliance at Velocity, Corticon, Corticon.js, DataDirect (and design), DataDirect Cloud, DataDirect Connect, DataDirect Connect64, DataDirect XML Converters, DataDirect XQuery, DataRPM, Defrag This, Deliver More Than Expected, DevReach (and design), Driving Network Visibility, Flowmon, Inspec, Ipswitch, iMacros, K (stylized), Kemp, Kemp (and design), Kendo UI, Kinvey, LoadMaster, MessageWay, MOVEit, NativeChat, OpenEdge, Powered by Chef, Powered by Progress, Progress Software Developers Network, SequeLink, Sitefinity (and Design), Sitefinity, Sitefinity (and design), Sitefinity Insight, SpeedScript, Stylized Design (Arrow/3D Box logo), Stylized Design (C Chef logo), Stylized Design of Samurai, TeamPulse, Telerik, Telerik (and design), Test Studio, WebSpeed, WhatsConfigured, WhatsConnected, WhatsUp, and WS\_FTP are registered trademarks of Progress Software Corporation or one of its affiliates or subsidiaries in the U.S. and/or other countries.

Analytics360, AppServer, BusinessEdge, Chef Automate, Chef Compliance, Chef Desktop, Chef Workstation, Corticon Rules, Data Access, DataDirect Autonomous REST Connector, DataDirect Spy, DevCraft, Fiddler, Fiddler Classic, Fiddler Everywhere, Fiddler Jam, FiddlerCap, FiddlerCore, FiddlerScript, Hybrid Data Pipeline, iMail, InstaRelinker, JustAssembly, JustDecompile, JustMock, KendoReact, OpenAccess, PASOE, Pro2, ProDataSet, Progress Results, Progress Software, ProVision, PSE Pro, Push Jobs, SafeSpaceVR, Sitefinity Cloud, Sitefinity CMS, Sitefinity Digital Experience Cloud, Sitefinity Feather, Sitefinity Thunder, SmartBrowser, SmartComponent, SmartDataBrowser, SmartDataObjects, SmartDataView, SmartDialog, SmartFolder, SmartFrame, SmartObjects, SmartPanel, SmartQuery, SmartViewer, SmartWindow, Supermarket, SupportLink, Unite UX, and WebClient are trademarks or service marks of Progress Software Corporation and/or its subsidiaries or affiliates in the U.S. and other countries. Java is a registered trademark of Oracle and/or its affiliates. Any other marks contained herein may be trademarks of their respective owners.

Please refer to the NOTICE.txt or Release Notes – Third-Party Acknowledgements file applicable to a particular Progress product/hosted service offering release for any related required third-party acknowledgements.

#### 1 Introduction

# **Table of Contents**

1 Introduction	4
1.1 Document Purpose	4
1.2 Intended Audience	4
2 Architecture	5
3 Configure Superna Ransomware Defender	6
4 Configure Progress Flowmon Anomaly Detection System (ADS)	8
4.1 Start Data Feed	8
4.2 Create a Filter	8
4.3 Create Perspective(s)	10
4.4 Create an Email Notification	11
4.4.1 Configure the Email/ SMTP Server	11
4.4.2 Create a Notification	12
4.5 Create a Custom Script (Superna Trigger)	13
Last Updated Date	15

1 Introduction

# 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: <a href="https://support.kemptechnologies.com">https://support.kemptechnologies.com</a>.

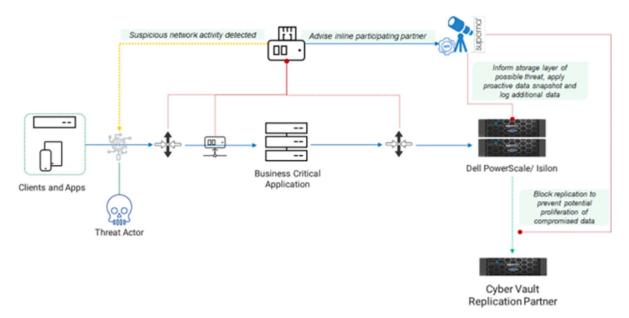
#### 1.2 Intended Audience

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

2 Architecture

# 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.



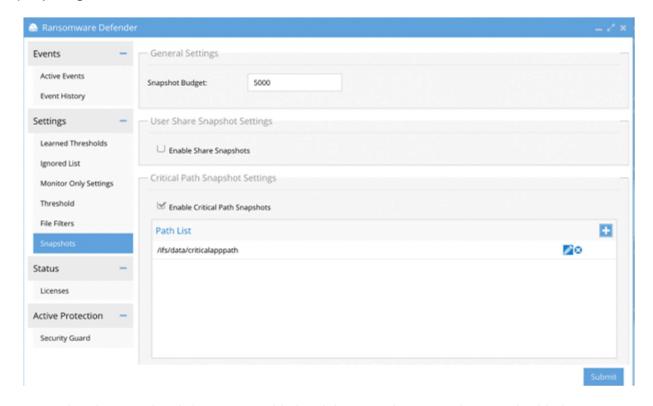
3 Configure Superna Ransomware Defender

# 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.



- 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).

3 Configure Superna Ransomware Defender

- 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 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.  \$howhride   Ust Operations   Expand Operations   alarms (v2): Raise alarms.  \$howhride   Ust Operations   Expand Operations   beand Operations   Showhride   Ust Operations   Sepand Operations   Sepand Operations   Showhride   Ust Operations   Sepand Operations   Sepand Operations   Showhride   Ust Operations   Sepand Operations   Sepand Operations   Sepand Operations   Showhride   Ust Operations   Sepand Operations   Security events (v1)   Showhride   Ust Operations   Sepand Operations   Security events   Showhride   Ust Op	eg OSS https://igls/swagger.json	igle-1sbevrp1mogkeg@q8r2usitf
A collection of utilities for programmatic interaction with Superna Byeglass  Created by Superna Support See more at http://support.superna.net Contact the developer Superna alirgap (v2): Retrieve information about AirGap policies.  alarms (v1): Retrieve information about alarms.  \$howhide   Ust Operations   Expand Operations   alarms (v2): Raise alarms.  \$howhide   Ust Operations   Expand Operations   healthcheck (v1)  \$howhide   Ust Operations   Expand Operations   healthcheck (v1)  \$howhide   Ust Operations   Expand Operations   healthcheck (v1): Startling and stopping jobs.  \$howhide   Ust Operations   howhide   how Operations   h		
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.  \$howhride   Ust Operations   Expand Operations   alarms (v2): Raise alarms.  \$howhride   Ust Operations   Expand Operations   \$howhride   Ust Operations   Expand Operations   \$howhride   Ust	eglass REST API	
See more at http://support.superna.net Contact the develope: Superna alirgap (v2): Retrieve information about AirGap policies.  showhide   Ust Operations   Expand Operations   alarms (v1): Retrieve information about alarms.  showhide   Ust Operations   Expand Operations   alarms (v2): Raise alarms.  healthcheck (v1)  showhide   Ust Operations   Expand Operations   beand Operations   showhide   Ust Operations   beand Operations   beand Operations   showhide   Ust Operations   beand Operations   beand Operations   showhide   Ust Operations   beand Oper	s for programmatic interaction with Superna Eyeglass	
alarms (v1): Retrieve information about alarms.  showhide   Ust Operations   Expand Operations	support.superna.net	
alarms (v2): Raise alarms.    Showhide   Uot Operations   Expand Operations	rieve Information about AirGap policies.	Showhilde   List Operations   Expand Operations
healthcheck (v1) Showhide   Unit Operations   Expand Operations   job (v1) : Startling and stopping jobs. Showhide   Unit Operations   Expand Operations   job (v2) : Startling and stopping jobs. Showhide   Unit Operations   Expand Operations   node (v1) : Retrieve information about managed devices, access zones, and SynclQ policies.    Showhide   Unit Operations   Expand Operations   Indicate   Unit Operations   Expand Operations   Showhide   Unit Operations   Expand Operations   Showhide   Unit Operations   Expand Opera	trieve information about alarms.	ShowHide   List Operations   Expand Operations
job (v1) : Starting and stopping jobs.   Showhride   List Operations   Expend Operations   job (v2) : Starting and stopping jobs.   Showhride   List Operations   Expend Operations   node (v1) : Retrieve information about managed devices, access zones, and SyncIQ policies.   Showhride   List Operations   Expend Operations   node (v2) : Retrieve information about configuration replication jobs on a node   Showhride   List Operations   Expend Operations   Showhride   List Operations   Expend Operations   Showhride   List Operations   Expend Operations   Inspend Operations   Showhride   List Operations   Expend Operations   Showhride   List Operations   Showhr	ise alarms.	ShowHide   List Operations   Expand Operations
job (v2) : Starting and stopping jobs.  showfride   Unt Operations   Expend Operations   Showfride   Unt Operations   Expend Operations   Showfride   Unt Operati	)	Show/Hide   List Operations   Expand Operations
node (v1) : Retrieve information about managed devices, access zones, and SyncIQ policies.    ShowNide   Ust Operations   Expand Operations	ig and stopping jobs.	ShowHide   List Operations   Expand Operations
Show/Nide   Ust Operations   Expand Operations    node (v2) : Retrieve information about configuration replication jobs on a node.  Show/Nide   Ust Operations   Expand Operations    ransomware (v1)   Show/Nide   Ust Operations   Expand Operations    ransomware (v2)   Show/Nide   Ust Operations   Expand Operations    security events (v1)   Show/Nide   Ust Operations   Expand Operations    whitelist (v1) : Retrieve Information about whitelist data for ransomware events.	ig and stopping jobs.	Show/Hide   List Operations   Expand Operations
node (v2): Retrieve information about configuration replication jobs on a node.  Showhide   Uot Operations   Expend Operations ransomware (v1)   Showhide   Uot Operations   Expend Operations ransomware (v2)   Showhide   Uot Operations   Expend Operations   Showhide   Uot Op	ieve information about managed devices, access zor	nes, and SyncIQ policies.
Showhide   Ust Operations   Expend Operations   ransomware (v1)   Showhide   Ust Operations   Expend Operations   ransomware (v2)   Showhide   Ust Operations   Expend Operations   security events (v1)   Showhide   Ust Operations   Expend Operations   whitelist (v1) : Retrieve information about whitelist data for ransomware events.		Show/Hide   List Operations   Expand Operations
ransomware (v1) Showhide   Ust Operations   Expend Operations ransomware (v2) Showhide   Ust Operations   Expend Operations security events (v1) Showhide   Ust Operations   Expend Operations whitelist (v1) : Retrieve information about whitelist data for ransomware events.	ieve information about configuration replication jobs	s on a node.
ransomware (v2) Showhide   Ust Operations   Expend Operations   Security events (v1) Showhide   Ust Operations   Expend Operations   Whitelist (v1) : Retrieve Information about whitelist data for ransomware events.		Showfilide   List Operations   Expand Operations
security events (v1) ShowNide   Use Operations   Expand Operations whitelist (v1) : Retrieve Information about whitelist data for ransomware events.	)	Showfride   List Operations   Expend Operations
whitelist (v1): Retrieve information about whitelist data for ransomware events.	0	Showfilde   List Operations   Expand Operations
	(v1)	Show/Hide   List Operations   Expand Operations
Show/Nide   List Operations   Expand Operations	letrieve information about whitelist data for ransome	ware events.
		Show/Hide   List Operations   Expand Operations

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/sera/v2/ransomware/criticalpaths' -d "{}"
```

4 Configure Progress Flowmon Anomaly Detection System (ADS)

# 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**.



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



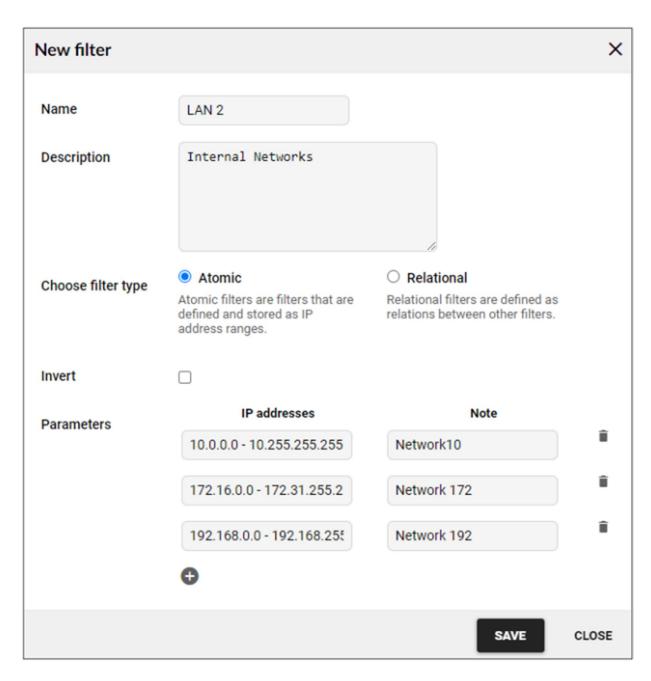
If the **Default** Data feed is not **ACTIVE**, click **Start**.

#### 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**.
- Click + NEW FILTER.

4 Configure Progress Flowmon Anomaly Detection System (ADS)



#### **EXAMPLE ONLY**

- a) Provide a Name.
- b) Select **Atomic**.
- c) Under **Parameters** add the networks that should be monitored for anomalies.

4 Configure Progress Flowmon Anomaly Detection System (ADS)

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.



#### **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 Configure Progress Flowmon Anomaly Detection System (ADS)

#### 4.4 Create an Email Notification

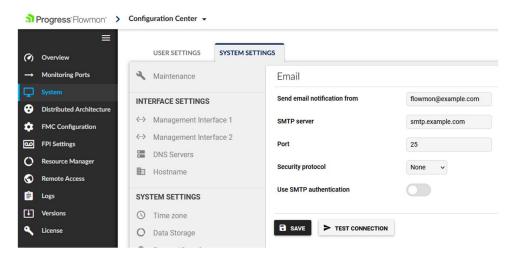
Each email notification must be bound to exactly one perspective. A notification can be in the active or inactive state. An inactive notification is defined in the system but is not being sent regularly. The option **Do not send empty reports** stops empty daily or weekly summary reports from being sent. 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.
- Go to System > System Settings > Email.

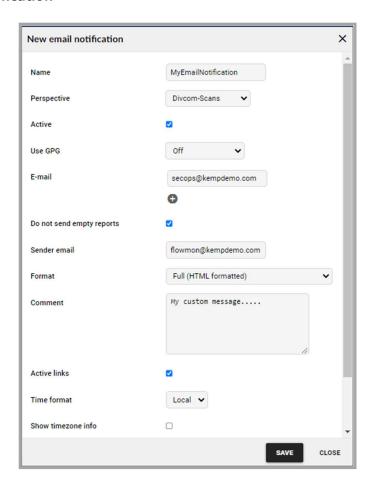


3. Provide the following:

4 Configure Progress Flowmon Anomaly Detection System (ADS)

- 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



- 1. Within the ADS Module, go to **Settings > Email notification**.
- 2. Click + NEW EMAIL NOTIFICATION.

4 Configure Progress Flowmon Anomaly Detection System (ADS)

- 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**.

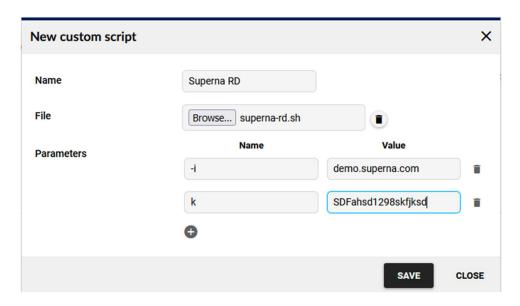
# 4.5 Create a Custom Script (Superna Trigger)

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.

4 Configure Progress Flowmon Anomaly Detection System (ADS)



- 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.

4 Configure Progress Flowmon Anomaly Detection System (ADS)

# **Last Updated Date**

This document was last updated on 1 September 2023.