LiveAction

LiveNX Alert Configuration Guide

QUICK GUIDE

ver. 24.3.0a

Overview

This document explains the alerting feature in LiveNX and serves as a guide for configuring alerts. It covers various parameters such as configuration, monitoring, and severity levels.

Introduction

LiveNX maps events from devices (routers, switches, firewalls, etc.) to alerts, which are triggered when specific criteria, such as thresholds, are met. Alerts are then displayed on the Operations Dashboard.

By mapping events to alerts, LiveNX minimizes the common issue of excessive alerts by prioritizing only those that require immediate action.

Types of Alerts in LiveNX

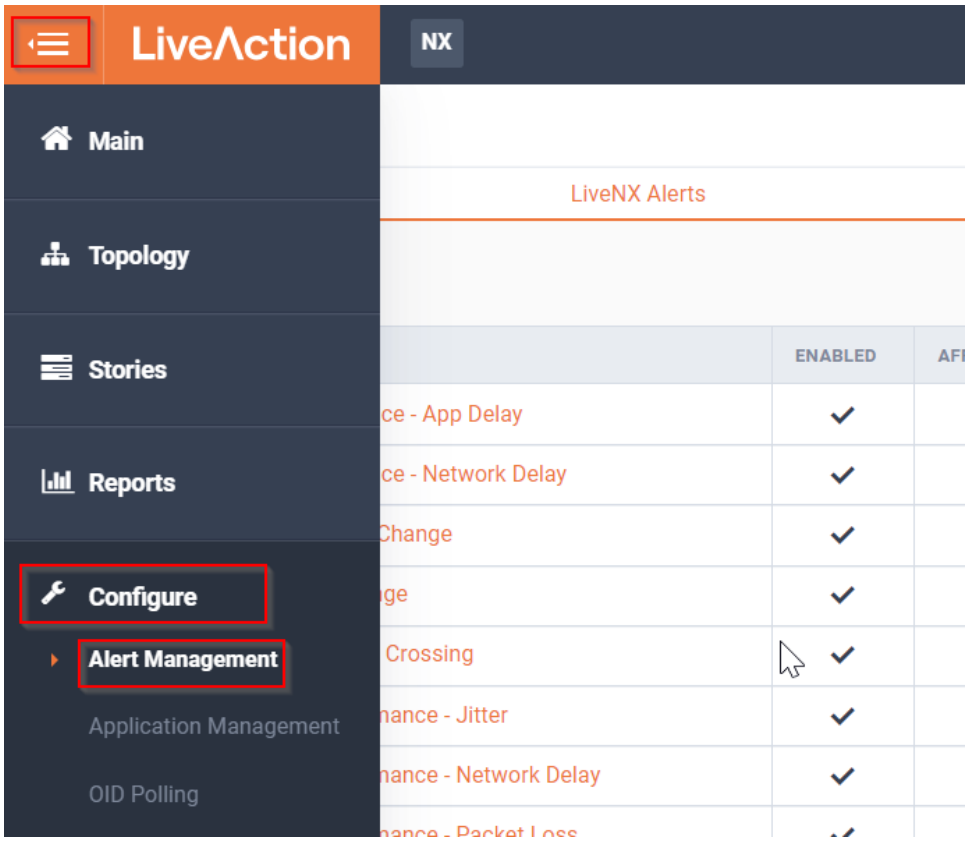
LiveNX supports two types of alerts:

1. **Single Instance Alerts**
   These alerts are global, meaning the same thresholds and sharing configurations apply to all sites, devices, and interfaces.
2. **Multi-Instance Alerts**
   Multi-instance alerts function similarly to an access list in a router or firewall. They are an ordered list of thresholds that are evaluated in a top-down manner. Each instance has an alert source filter defining the sites, devices, interfaces, etc., that it applies to.
   - When a match is found, the corresponding instance's threshold is used for the KPI measurement, and no other instances are considered.
   - If no specific instance matches, the KPI uses the default instance (if enabled).
   - Any disabled instances are ignored.

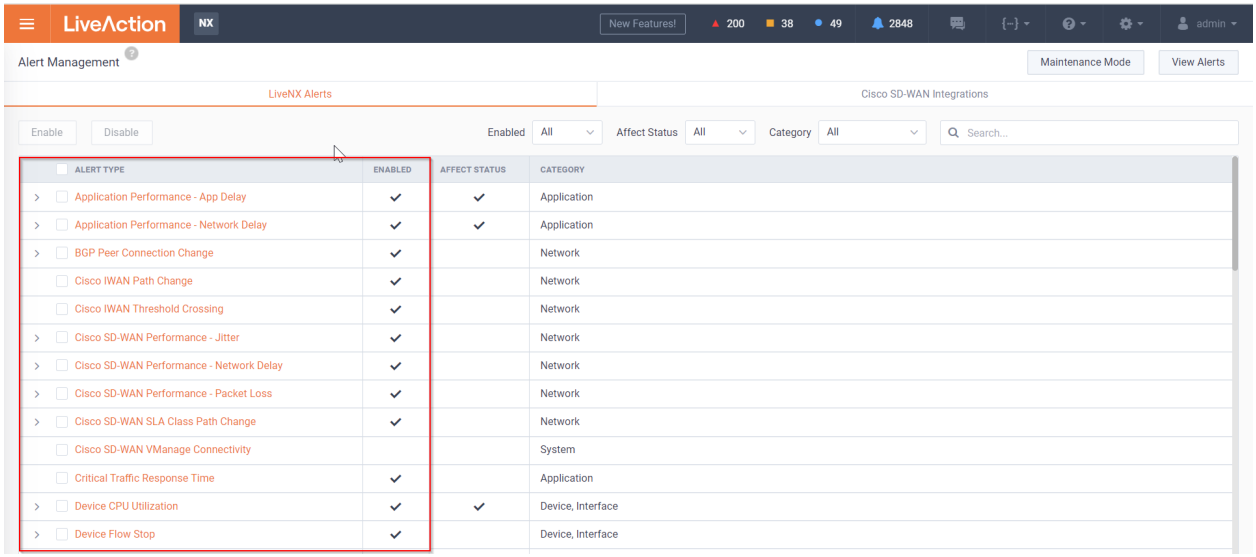
LiveNX Alert Configuration

Alerts can be configured through the **Alert Management** option under the **Configure** menu. Follow these steps:

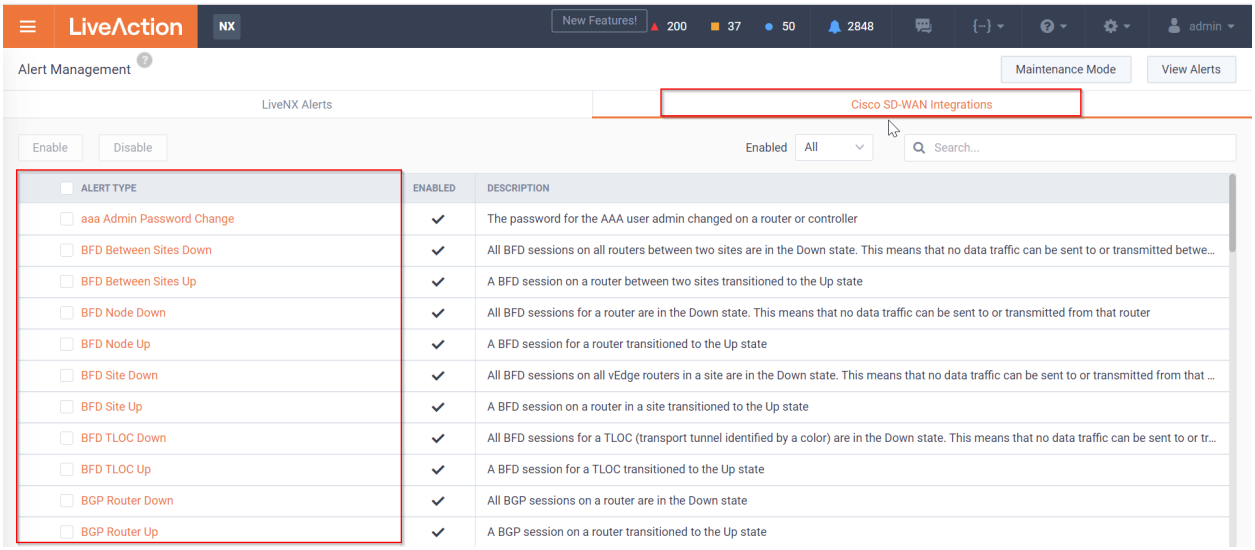
1. In the LiveNX web interface, click the **Menu** icon.
2. Navigate to **Configure > Alert Management**.



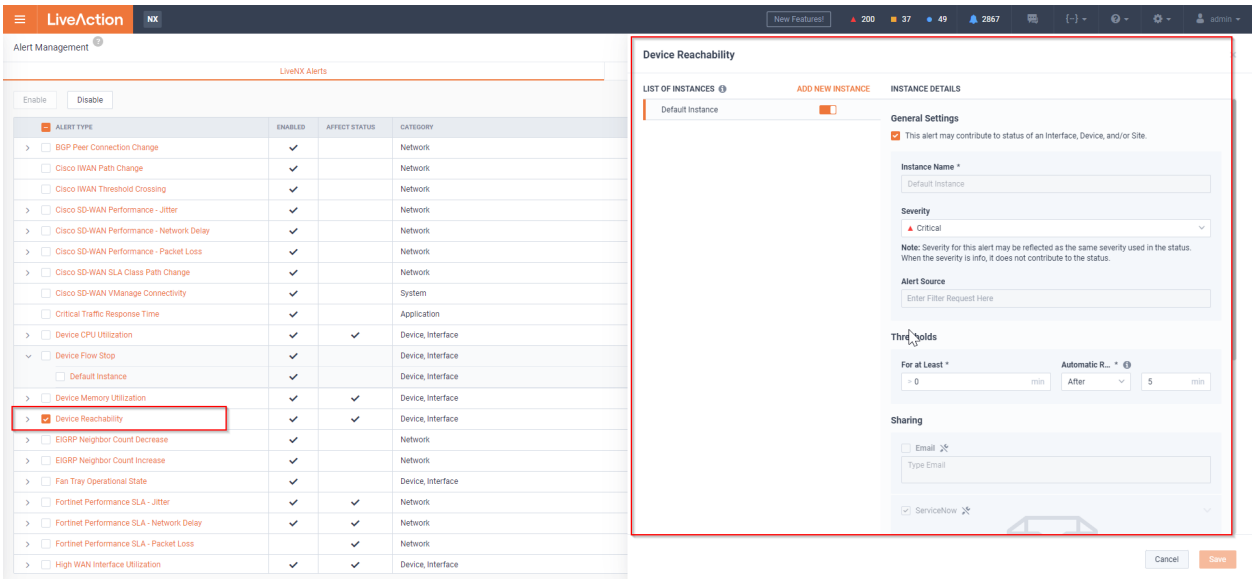
3. The **Alert Management** page provides a comprehensive list of all available alerts, along with a summary of their configurations.



4. If Cisco SD-WAN is integrated with LiveNX, a separate tab is available specifically for managing Cisco SD-WAN alerts.



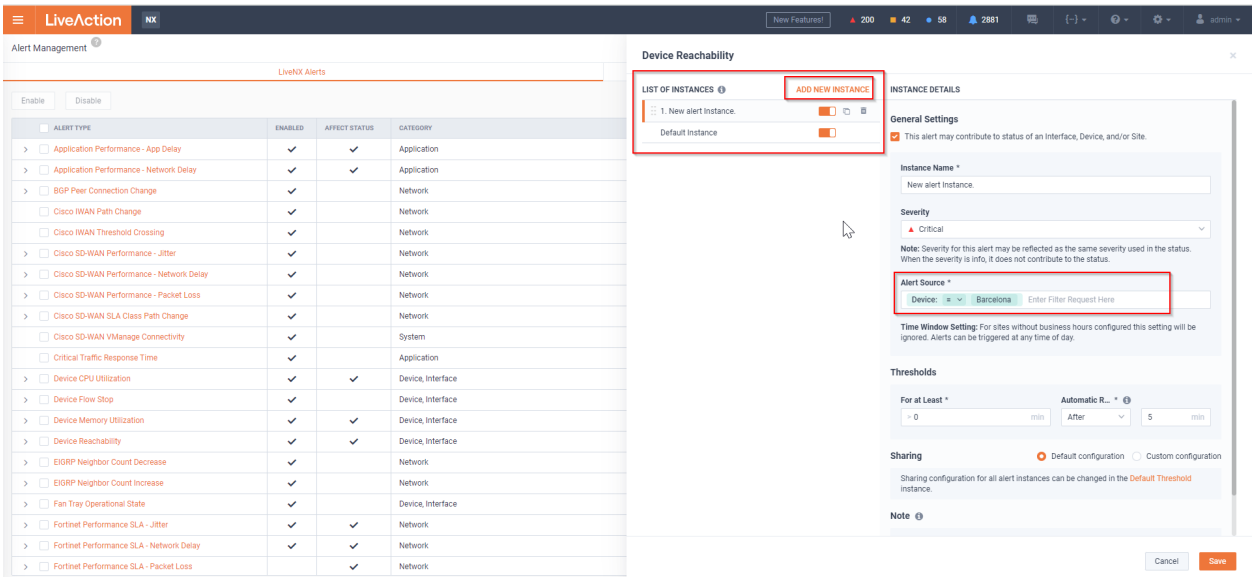
5. To configure an alert, click on its name. The configuration details will be displayed on the right side of the page.



6. On the alert configuration page, you can set up multiple variables. Here's how to use the available options:

   a. **Default Instance**: Enabling the **Default Instance** applies the alert to all devices, interfaces, sites, and/or tags. In this mode, users cannot specify individual alert sources since the configuration covers all sources. This option is best for setting uniform alert thresholds across all sources.

   b. **Add New Instance**: Adding a New Instance allows users to create multiple instances of similar alerts, each with unique variables. This is useful when configuring alerts for multiple, but not all, sources that require different alert parameters.

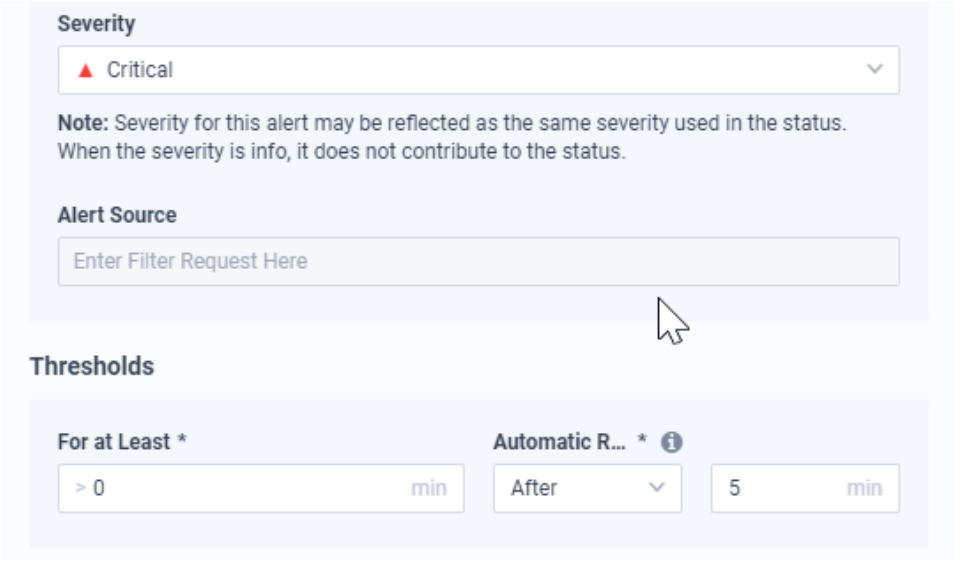


c. **Instance Name**: This field enables users to assign unique names to new alert instances for easy identification. Naming helps differentiate and manage multiple instances efficiently.

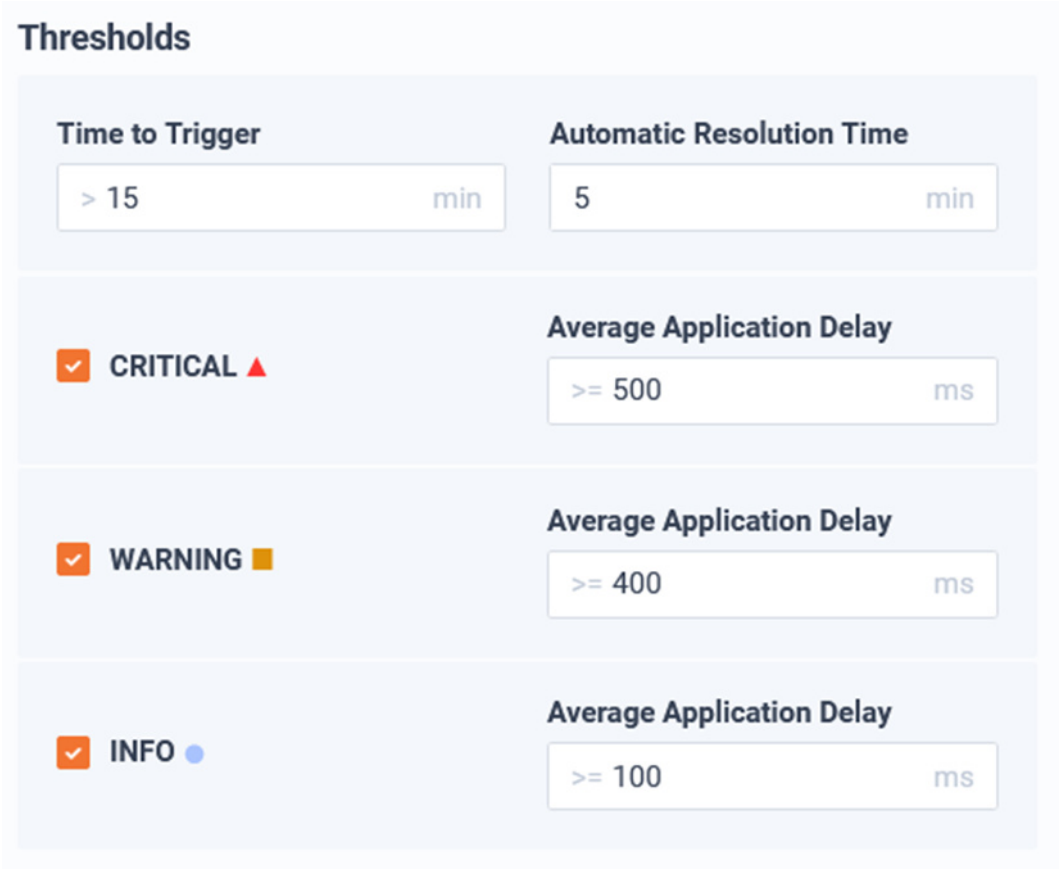
d. **Severity**: This section allows users to set the severity level of alerts. LiveNX displays severity based on configuration and offers the following levels:

   - Critical
   - Warning
   - Info

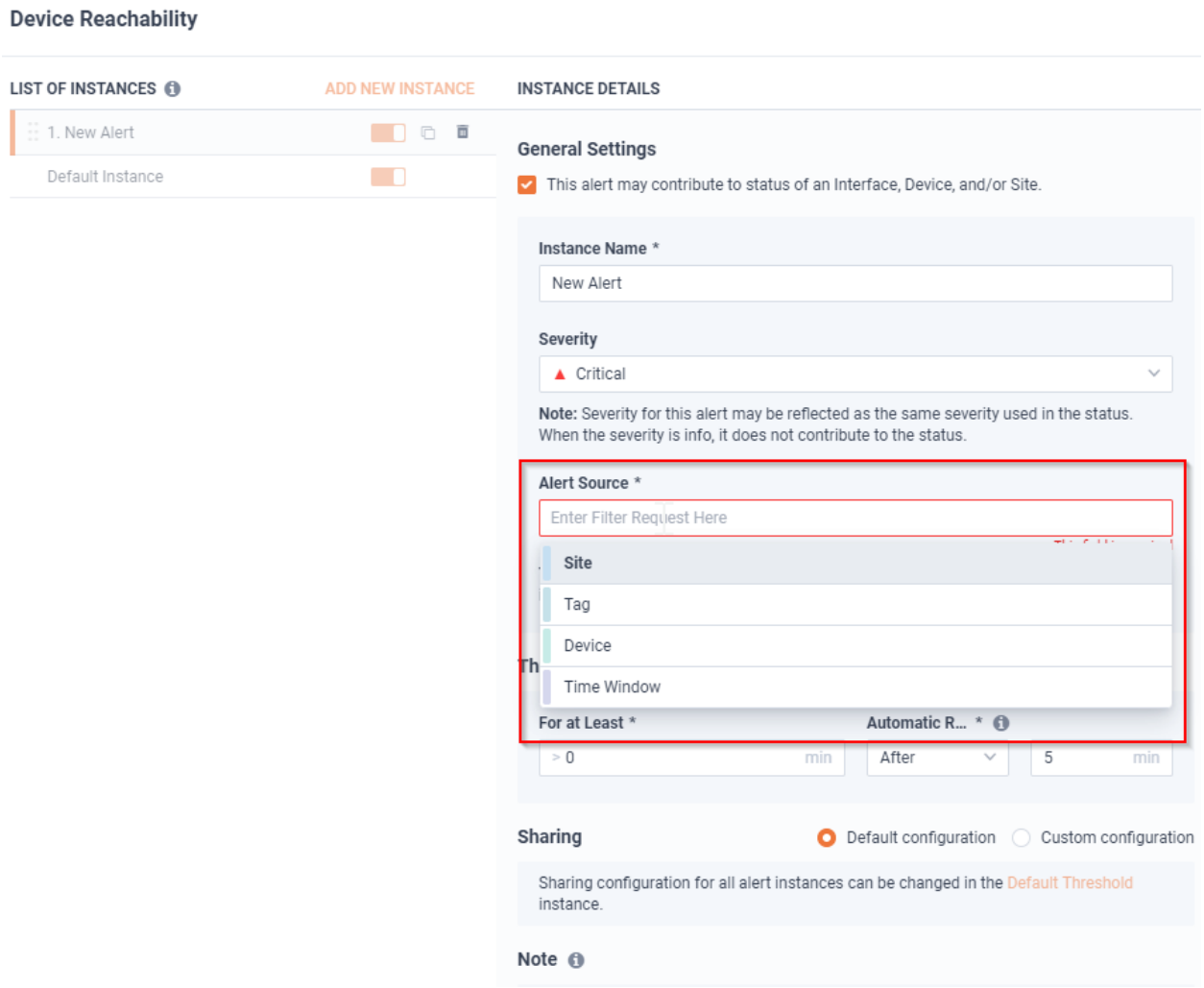
   Simple alerts have a single severity level corresponding to one threshold.



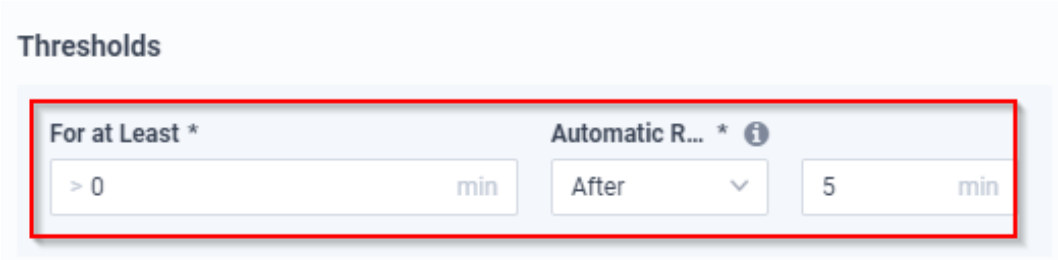
More complex alerts may support different severities, **Time to Trigger**, and **Automatic Resolution Time** for each threshold.



e. **Alert Source**: This identifies the source that triggers the alert within LiveNX. The option to specify an alert source is only available when adding a new alert instance and is not applicable to the default instance.



f. **Thresholds**: This section allows users to define both the trigger and resolution criteria for alerts based on time and conditions. It includes parameters for:
   - **For at Least**: Defines the minimum time before the alert is triggered.
   - **Automatic Resolution Time**: Specifies the time for the alert to resolve automatically after the trigger criteria are no longer met.



g. **Sharing**: LiveNX enables sharing of alert events across multiple platforms:
   - **Email**: Alerts can be sent to one or more email addresses, requiring SMTP configuration.
   - **ServiceNow**: Alerts can be forwarded as Events or Incidents via API integration, which requires ServiceNow setup in LiveNX.
   - **SNMP Trap**: Alerts can be sent to an external SNMP server for trap reception, requiring prior SNMP configuration.

- **WebUI**: Alerts are displayed in the LiveNX Operations Dashboard Notification Sidebar (enabled by default).
- **Syslog**: Alerts can be forwarded to an external Syslog server, which also needs to be configured beforehand.