

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

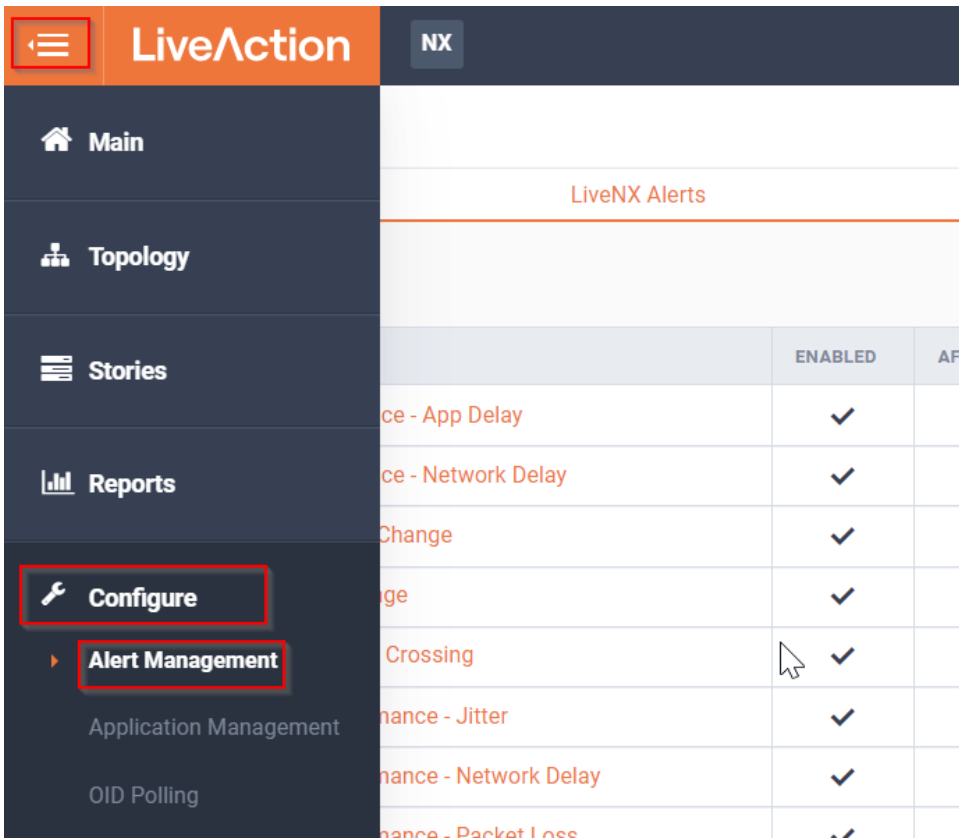
Multi-instance alerts function similarly to an access list in a router or firewall. They are an ordered list of thresholds that are evaluated in a top-down manner. Each instance has an alert source filter defining the sites, devices, interfaces, etc., that it applies to.

- 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.

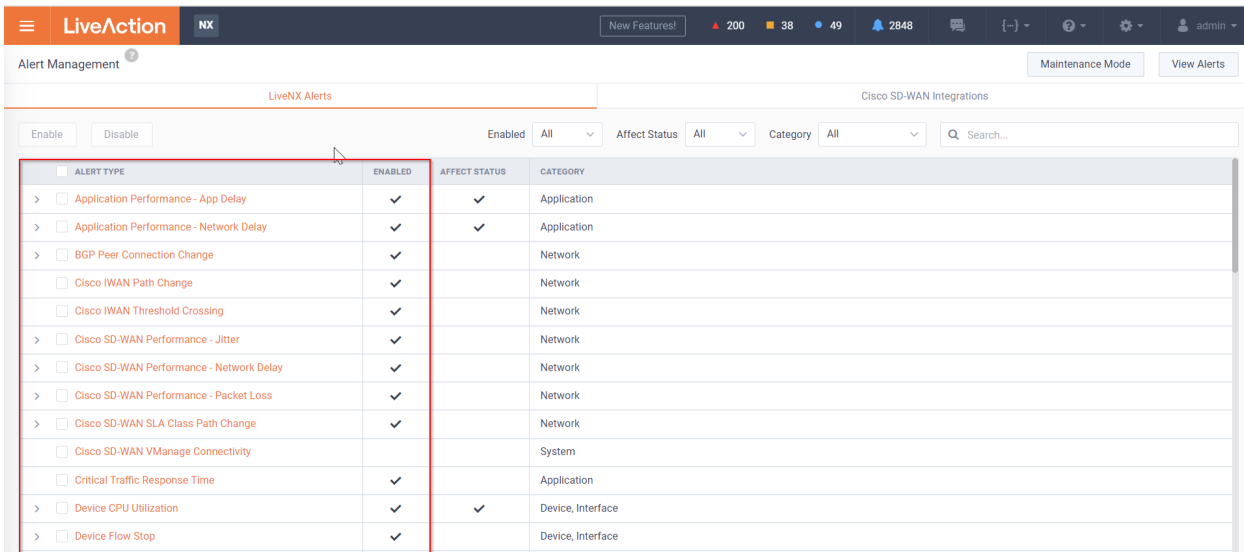
LiveNX Alert Configuration

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.

The screenshot shows the LiveAction Alert Management interface. At the top, there's a navigation bar with 'LiveAction' and 'NX' logos, and a status bar with 'New Features!', '200', '37', '50', '2848', and 'admin'. Below this, the 'Alert Management' section is visible, with 'LiveNX Alerts' and 'Cisco SD-WAN Integrations' tabs. A search bar and 'Enable/Disable' buttons are present. A table lists various alert types, with a red box highlighting the 'ALERT TYPE' column. The table has columns for 'ENABLED' and 'DESCRIPTION'.

ALERT TYPE	ENABLED	DESCRIPTION
<input type="checkbox"/> aaa Admin Password Change	✓	The password for the AAA user admin changed on a router or controller
<input type="checkbox"/> BFD Between Sites Down	✓	All BFD sessions on all routers between two sites are in the Down state. This means that no data traffic can be sent to or transmitted betwe...
<input type="checkbox"/> BFD Between Sites Up	✓	A BFD session on a router between two sites transitioned to the Up state
<input type="checkbox"/> BFD Node Down	✓	All BFD sessions for a router are in the Down state. This means that no data traffic can be sent to or transmitted from that router
<input type="checkbox"/> BFD Node Up	✓	A BFD session for a router transitioned to the Up state
<input type="checkbox"/> BFD Site Down	✓	All BFD sessions on all vEdge routers in a site are in the Down state. This means that no data traffic can be sent to or transmitted from that ...
<input type="checkbox"/> BFD Site Up	✓	A BFD session on a router in a site transitioned to the Up state
<input type="checkbox"/> BFD TLOC Down	✓	All BFD sessions for a TLOC (transport tunnel identified by a color) are in the Down state. This means that no data traffic can be sent to or tr...
<input type="checkbox"/> BFD TLOC Up	✓	A BFD session for a TLOC transitioned to the Up state
<input type="checkbox"/> BGP Router Down	✓	All BGP sessions on a router are in the Down state
<input type="checkbox"/> BGP Router Up	✓	A BGP session on a router transitioned to the Up state

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

The screenshot shows the LiveAction Alert Management interface with the 'Device Reachability' alert configuration page open. The left sidebar shows a list of alerts, with 'Device Reachability' highlighted. The main content area shows the configuration details for this alert, including 'General Settings', 'Thresholds', and 'Sharing' sections. A red box highlights the configuration details on the right side.

Device Reachability

LIST OF INSTANCES: Default Instance (checked)

General Settings

- This alert may contribute to status of an Interface, Device, and/or Site.
- Instance Name: Default Instance
- Severity: Critical
- Note: Severity for this alert may be reflected as the same severity used in the status. When the severity is info, it does not contribute to the status.
- Alert Source: Enter Filter Request Here

Thresholds

For at Least: 0 min, Automatic R...: After 5 min

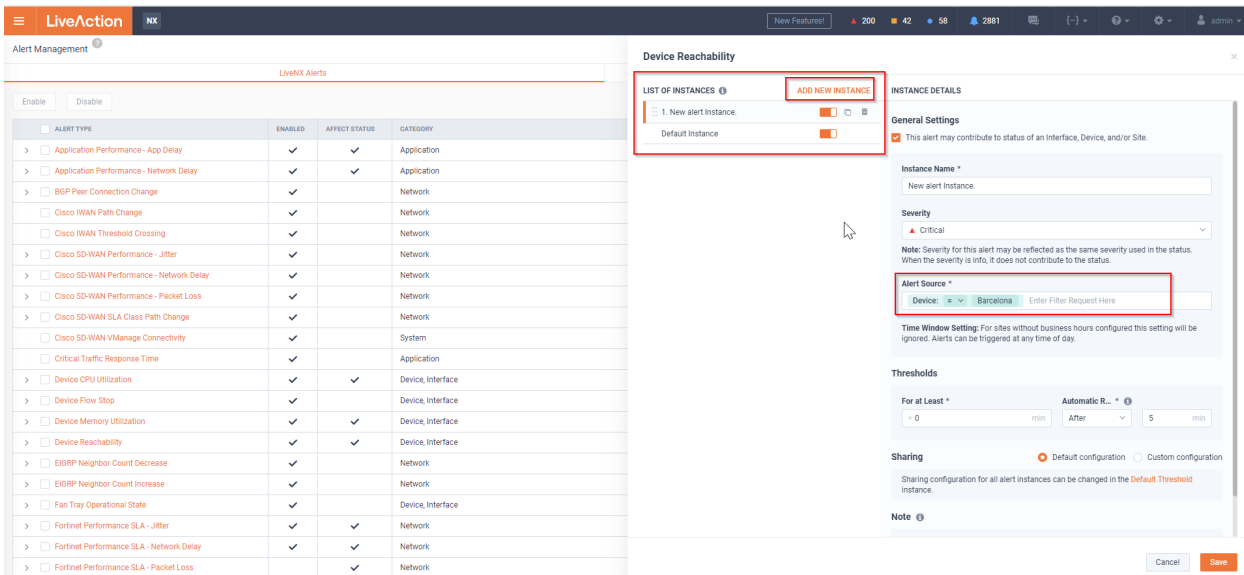
Sharing

- Email
- Type Email
- ServiceNow

Buttons: Cancel, Save

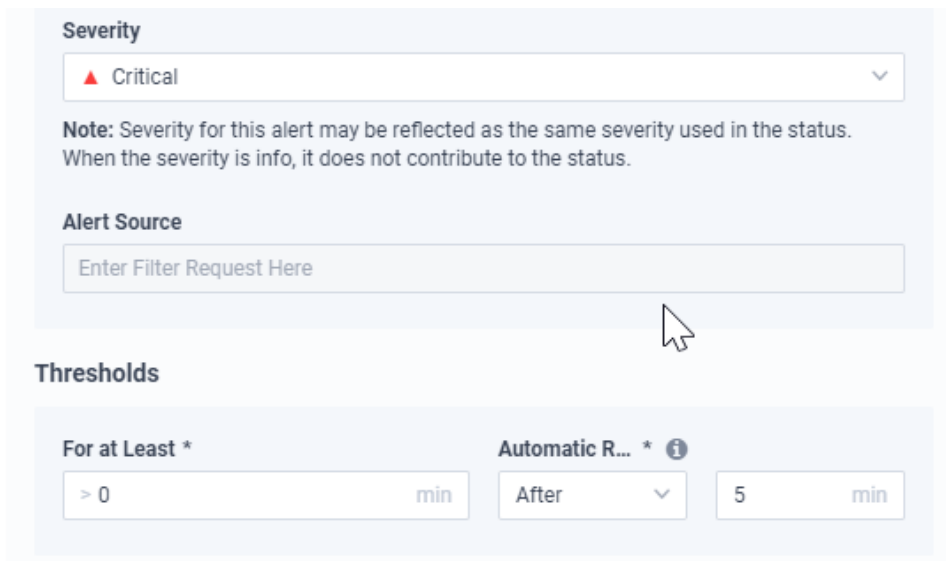
6. On the alert configuration page, you can set up multiple variables. Here's how to use the available options:

- 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.
- 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.

Thresholds

Time to Trigger	Automatic Resolution Time
> 15 min	5 min
<input checked="" type="checkbox"/> CRITICAL ▲	Average Application Delay
	>= 500 ms
<input checked="" type="checkbox"/> WARNING ■	Average Application Delay
	>= 400 ms
<input checked="" type="checkbox"/> INFO ●	Average Application Delay
	>= 100 ms

- 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.

Device Reachability

LIST OF INSTANCES ⓘ ADD NEW INSTANCE INSTANCE DETAILS

1. New Alert 🔴 📄 🗑️

Default Instance 🔴

General Settings

This alert may contribute to status of an Interface, Device, and/or Site.

Instance Name *

Severity
▲ Critical ▼

Note: Severity for this alert may be reflected as the same severity used in the status. When the severity is info, it does not contribute to the status.

Alert Source *

- Site
- Tag
- Device
- Time Window

For at Least * **Automatic R... *** ⓘ

> 0 min After 5 min

Sharing Default configuration Custom configuration

Sharing configuration for all alert instances can be changed in the [Default Threshold](#) instance.

Note ⓘ

- 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.

Thresholds

For at Least * **Automatic R... *** ⓘ

> 0 min After 5 min

- 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.

Sharing

Email

×
Type email

ServiceNow ^

Default ServiceNow settings set on **Global settings** page. You can override individual settings below.

Category

 ▼

Subcategory

 ▼

Add value to override

 ▼

SNMP trap ⌘

Web UI

Syslog