

## LiveNX TCP Flags Flow Flex Filter

The TCP flags filter matches against TCP flags contained in the standard IPFIX info element (field ID 6). Note that the flags contained in this field could be an aggregation of TCP flags contained within multiple network packets since a flow record often represents data from a collection of packets and not single network packets.

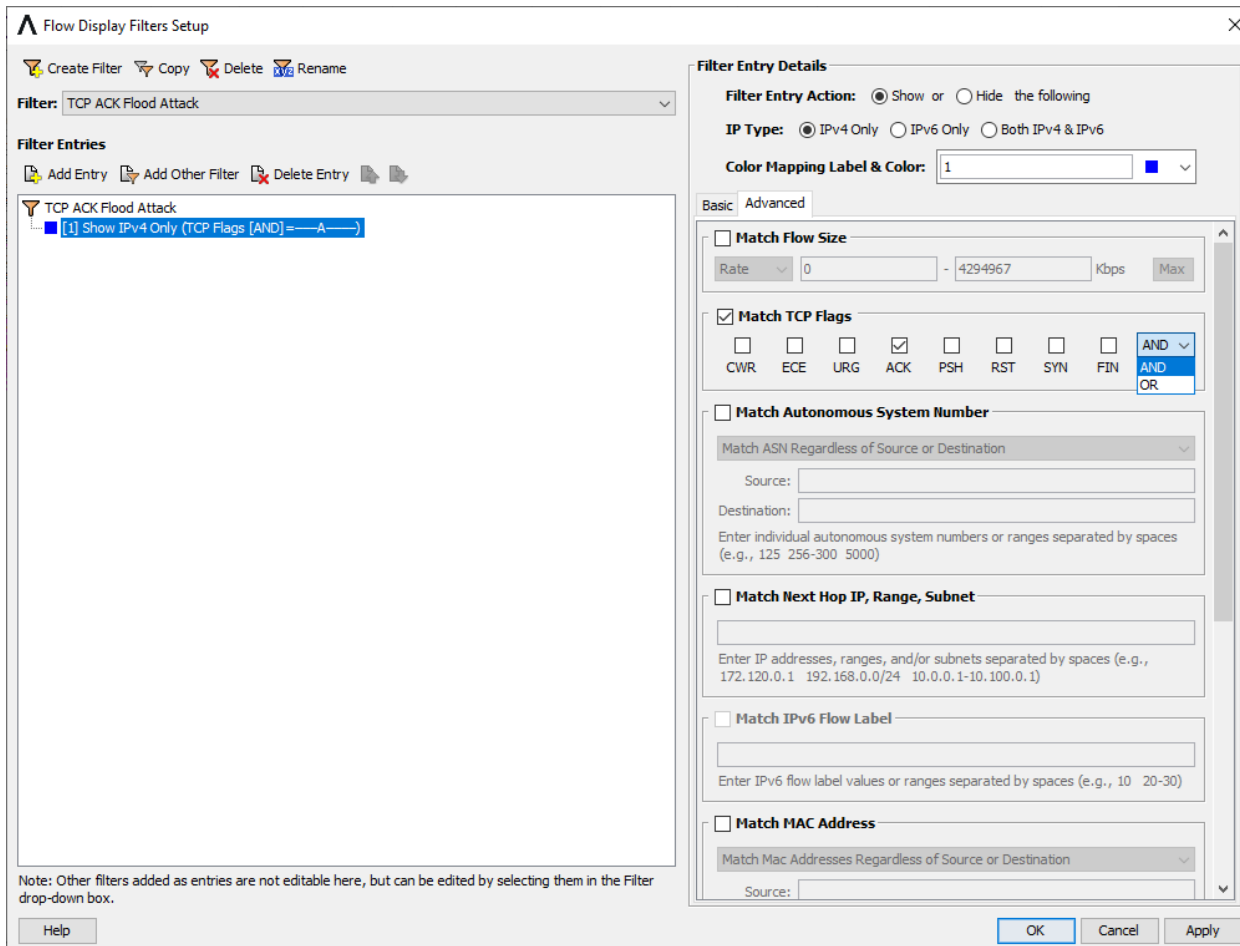
In addition to looking for particular kinds of traffic, filtering on the TCP flags might be helpful in detecting some kinds of scans or attacks.

### Display Filter

Currently, the display filter can only be created/edited on the Engineering Console. However, most reports should support selecting a display filter to use.

The Engineering Console display filters have had the ability to filter on TCP flags for quite some time. With the original implementation, there were only two kinds of matching supported.

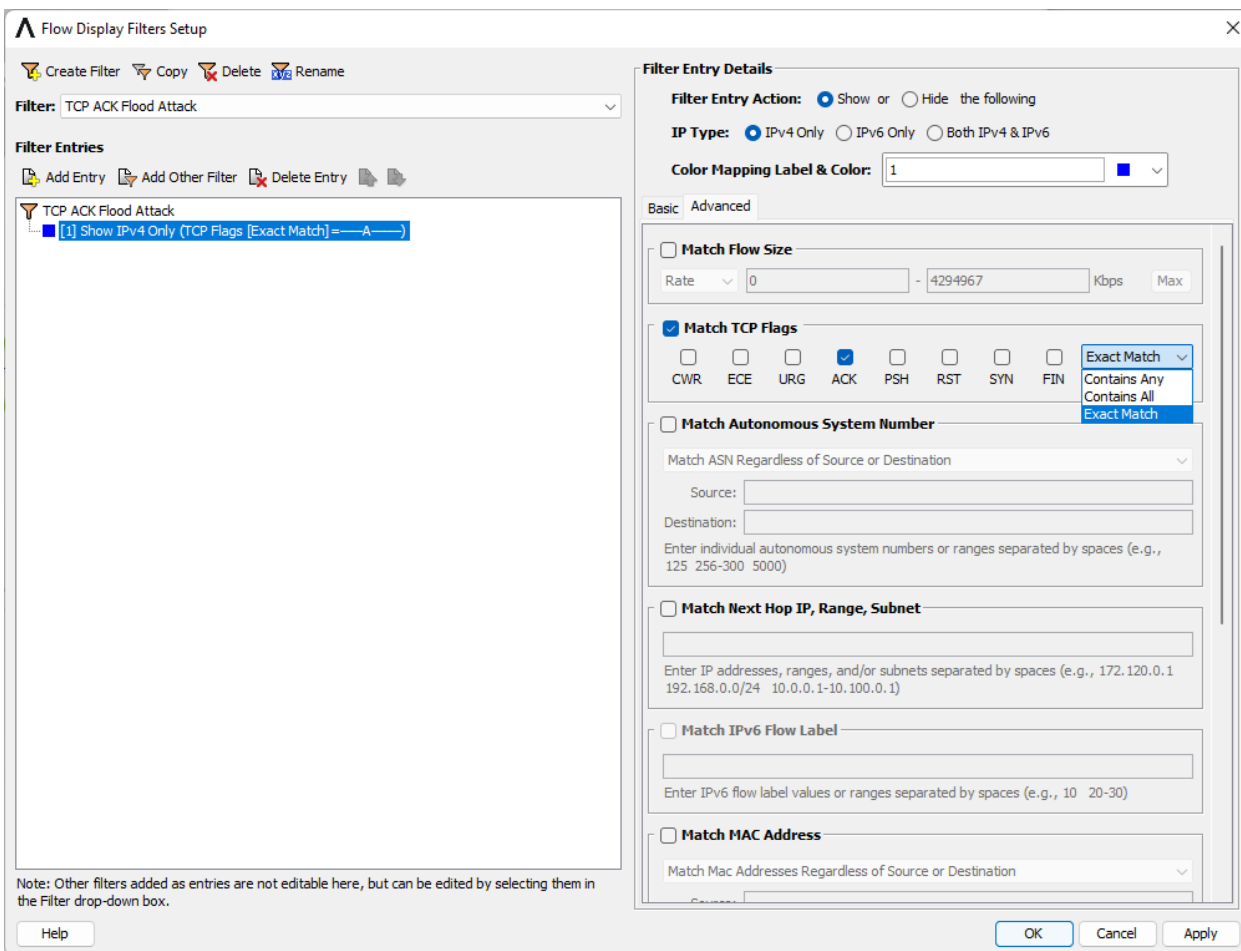
- **AND:** The TCP flags field must contain only the specified TCP flags in the filter (exact match)
- **OR:** The TCP flags field contains any of the specified TCP flags in the filter



## Improvements in 24.3.0

The behavior of the AND and OR settings might have been a little ambiguous and the wording has been changed to make this clearer. Also, another match type has been added, "contains all":

- **Exact Match** (formerly AND): The TCP flags field must contain only the specified TCP flags in the filter
  - This the only option that can match against a TCP flags field that has no TCP flags set
- **Contains Any** (formerly OR): The TCP flags field contains any of the specified TCP flags in the filter
  - If no TCP flags are specified in the filter, this filter matches everything
- **Contains All** (new): The TCP flags field contains all of the specified TCP flags in the filter, but could also contain additional flags.
  - If no TCP flags are specified in the filter, this filter returns no matches



This change to the match type will make some of the LiveNX configuration files and alerts incompatible with previous versions.

---

## Implementation

The flow flex string version of the filter will provide the similar filtering capability as the updated display filter. The following are examples of the syntax used for the new filter:

Type	Syntax	Description
Exact Match	<ul style="list-style-type: none"><li>• flow.tcpFlags=ACK,FIN</li><li>• flow.tcpFlags.cwr=false &amp; flow.tcpFlags.ece=false &amp; flow.tcpFlags.urg=false &amp; flow.tcpFlags.ack=true &amp; flow.tcpFlags.psh=false &amp; flow.tcpFlags.rst=false &amp; flow.tcpFlags.syn=false &amp; flow.tcpFlags.fin=true</li></ul>	<ul style="list-style-type: none"><li>• The TCP flags field must only contain the ACK and FIN flags.</li><li>• With the second form of the filter string all of the TCP flags must be specified.</li><li>• Drill downs on the TCP flags field will us</li></ul>
Exact Match	flow.tcpFlags=""	The TCP flags field must contain no TCP flags.
Contains Any	flow.tcpFlags.ack=true   flow.tcpFlags.fin=true	<ul style="list-style-type: none"><li>• The TCP flags field must contain the ACK or FIN flag. Note that flags set to false will be ignored when OR'ed together.</li><li>• Equivalent to the "contains any" display filter</li></ul>
Contains All	flow.tcpFlags.ack=true & flow.tcpFlags.fin=true	<ul style="list-style-type: none"><li>• The TCP flags field must contain both the ACK or FIN flags, but could contain other flags.</li><li>• Equivalent to the "contains all" display filter</li></ul>
Mixed	flow.tcpFlags.urg=false & flow.tcpFlags.ack=true & flow.tcpFlags.fin=true	<ul style="list-style-type: none"><li>• The TCP flags field must contain both the ACK or FIN flags, but could contain other flags except for the URG flag.</li><li>• The display filter does not support this type of matching</li></ul>
Mixed	flow.tcpFlags.ack= true   flow.tcpFlags.syn=true & flow.tcpFlags.fin=true	This is equivalent to flow.tcpFlags.ack= true   (flow.tcpFlags.syn=true & flow.tcpFlags.fin=true). The TCP flags field must contain either the ACK flag or both SYN and FIN flags.

The values following the equals sign should be a non-case sensitive comma delimited list (with no spaces) consisting of the three character TCP flag values:

- CWR
- ECE
- URG
- ACK
- PSH
- RST
- SYN
- FIN

Generally, this filter should be AND'ed with the "flow.protocol=TCP" filter to ensure that this filter is only applied to TCP flows.

- Note that almost all TCP flags filtering will be using the raw flow store vl because it is not a key in any long-term aggregated standard report. Currently, the only case where the long-term store might be used is with a custom report where the TCP flags field is the only key and the custom report is enabled for long-term aggregation.

- Support for this filter has not been added to the ClickHouse report filtering and there are no currently plans to do this.

Most reports do not display the "TCP Flags" field, although the TCP flags filter can be used with almost any flow report using the raw flow store v1 since most raw basic flow records contain the field. The only places the TCP flags field might be displayed are in the following:

- Top Analysis report
- Custom report with the TCP flags field added
- Engineering Console flow device view

## Related Updates

TCP flags info element can now be used as a key in a custom report.

EDIT CUSTOM REPORT
✕

1 General Settings
2 Keys and Metrics

**Keys** Q Search...

NAME	FIELD NAME	SEARCH STRING	FIELD ID	PEN
<input type="checkbox"/> Name	Field name	Search string	Field ID	PEN
<input checked="" type="checkbox"/> Protocol	protocolIdentifier	flow.protocol	4	Standard
<input type="checkbox"/> Src DSCP	ipClassOfService	flow.tos.src	5	Standard
<input checked="" type="checkbox"/> TCP Flags	tcpControlBits	flow.tcpFlags	6	Standard
<input checked="" type="checkbox"/> Src Port	sourceTransportPort	flow.port.src	7	Standard
<input checked="" type="checkbox"/> Src IP Addr	sourceIPv4Address	flow.ip.src	8	Standard
<input type="checkbox"/> Src Prefix Len	sourceIPv4PrefixLength	flow.mask.src	9	Standard
<input type="checkbox"/> In IF	ingressInterface	flow.ifidx.in	10	Standard
<input checked="" type="checkbox"/> Dst Port	destinationTransportP...	flow.port.dst	11	Standard
<input checked="" type="checkbox"/> Dst IP Addr	destinationIPv4Address	flow.ip.dst	12	Standard
<input type="checkbox"/> Dst Prefix Len	destinationIPv4Prefix...	flow.mask.dst	13	Standard
<input type="checkbox"/> Out IF	egressInterface	flow.ifidx.out	14	Standard
<input type="checkbox"/> Next Hop IP Addr	ipNextHopIPv4Address	flow.ip.nextHop	15	Standard
<input type="checkbox"/> Src AS	bgpSourceASNumber	flow.as.src	16	Standard
<input type="checkbox"/> Dst AS	bgpDestinationASNu...	flow.as.dst	17	Standard

**Metrics** Q Search...

NAME	FIELD NAME	FIELD ID	PEN
<input type="checkbox"/> In Bytes	octetDeltaCount	1	Standard
<input type="checkbox"/> In Packets	packetDeltaCount	2	Standard
<input type="checkbox"/> Total Bytes	postOctetDeltaCount	23	Standard
<input type="checkbox"/> Total Packets	postPacketDeltaCount	24	Standard
<input type="checkbox"/> Min Packet Len	minimumIpTotalLength	25	Standard
<input type="checkbox"/> Max Packet Len	maximumIpTotalLength	26	Standard
<input type="checkbox"/> Total Bytes Exported	exportedOctetTotalCo...	40	Standard
<input type="checkbox"/> Total Packets Exported	exportedMessageTotalCo...	41	Standard
<input checked="" type="checkbox"/> Total Flows	exportedFlowRecordTotalCo...	42	Standard
<input type="checkbox"/> Initiator Octets	initiatorOctets	231	Standard
<input type="checkbox"/> Responder Octets	responderOctets	232	Standard
<input type="checkbox"/> L2 Frame Delta Count	layer2FrameDeltaCount	430	Standard
<input type="checkbox"/> L2 Frame Total Count	layer2FrameTotalCount	431	Standard
<input type="checkbox"/> Ignored L2 Frame Total Count	ignoredLayer2FrameTotalCo...	433	Standard

**Preview**

Rearrange by dragging the headings below

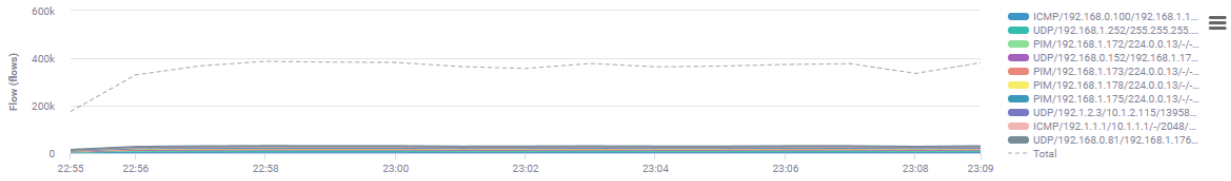
Protocol	Src IP Addr	Dst IP Addr	Src Port	Dst Port	TCP Flags	Total Flows	Average Bit Rate	Average Packet Rate
----------	-------------	-------------	----------	----------	-----------	-------------	------------------	---------------------

Cancel
Previous Step
Save

You can now drill down on the TCP flags field (where drill downs are available). Note that the drill down creates "exact match" filters.

Dynamic TCP Flags (Flow)

Interface: All Interfaces Execution Type: timeseries Sort By: FLOW Should Wait For Dns Resolution: false Device: All Devices Flow Type: basic Direction: both Display Filter: No Display Filtering Bin Duration: auto  
 Start Time: Aug 08, 2024 22:54:00 HST (GMT-10:00) End Time: Aug 08, 2024 23:09:00 HST (GMT-10:00) Business Hours: none Bin Interval: 1 minute  
 Warning: \*This report is based in part on sampled flow data, therefore it is an approximation based on incomplete data. In this report, sampled flow data are extrapolated by applying the sampling multiplier.



<< Page 182 / 200 >>

Search...

Legend	Protocol	Src IP Addr	Dst IP Addr	Src Port	Dst Port	TCP Flags	Total Flows	Average Bit Rate	Average Packet Rate
	UDP	10.2.101.146	10.131.1.24	30001	161	-	15	2.53 Kbps	1.51 pps
	TCP	10.122.71.140	10.131.101.2	2156	80	ACK FIN	15	0.15 Kbps	0.48 pps
	ICMP	172.31.43.2	172.49.50.60	-	-				0.02 pps
	ICMP	172.26.43.26	172.49.50.227	-	-				0.02 pps
	ICMP	172.31.43.2	172.49.50.63	-	-				0.02 pps
	ICMP	172.31.43.2	172.49.50.108	-	-				0.02 pps
	UDP	10.4.201.207	10.4.203.156	161	42945				0.93 pps
	ICMP	172.31.43.2	172.49.50.143	-	-				0.02 pps
	TCP	192.168.2.207	188.65.124.59	47476	443	ACK PSH			0.24 pps
	UDP	192.168.2.211	10.2.101.141	54437	5004		14	36.26 Kbps	5.15 pps

- Apply ACK FIN to Search Filter
- Apply Specific Flow to Search Filter
- Drill down on ACK FIN as Application
- Drill down on ACK FIN as Top Conversations
- Drill down on ACK FIN as Interface Bandwidth
- Drill down on ACK FIN as DSCP
- Drill down on ACK FIN as IPs and Ports
- Drill down to Specific Flow on Flow Path Analysis Story

# Auto Rotating Dashboards

In LiveNX 24.3.0, we have an ability to see multiple dashboards on a single monitor. This feature rotate or cycle through the set of desired dashboards at a fixed interval. This is supported in LiveNX when using the full screen dashboard view.

## Configuration

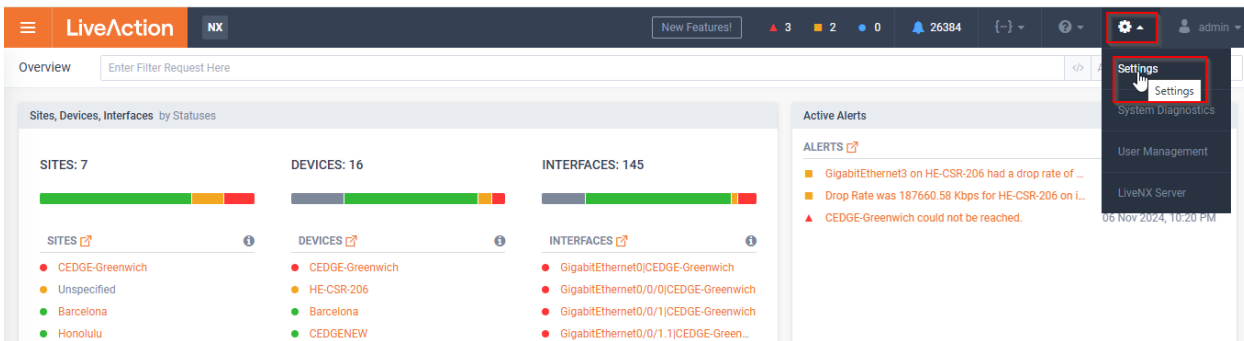
There are two aspects of configuration.

### Global auto cycle configuration interval –

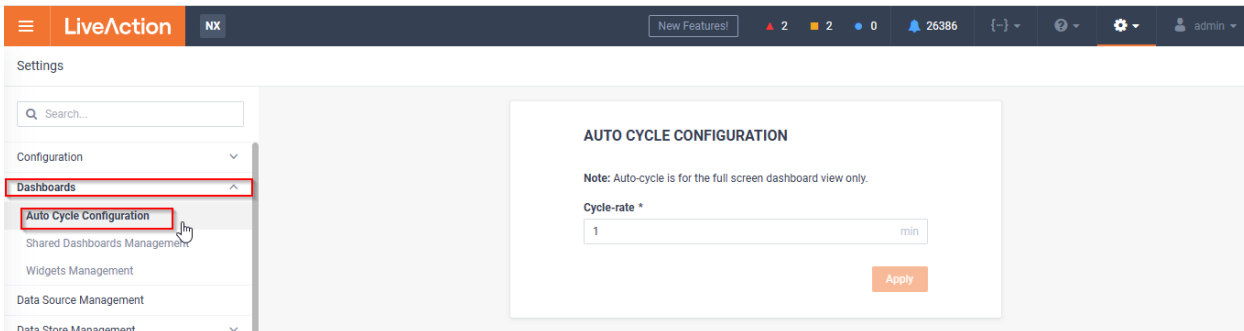
This can only be set by admins and is applied to all users. This is persisted and available for all users.

### To configure the Global Auto cycle Configuration Interval:

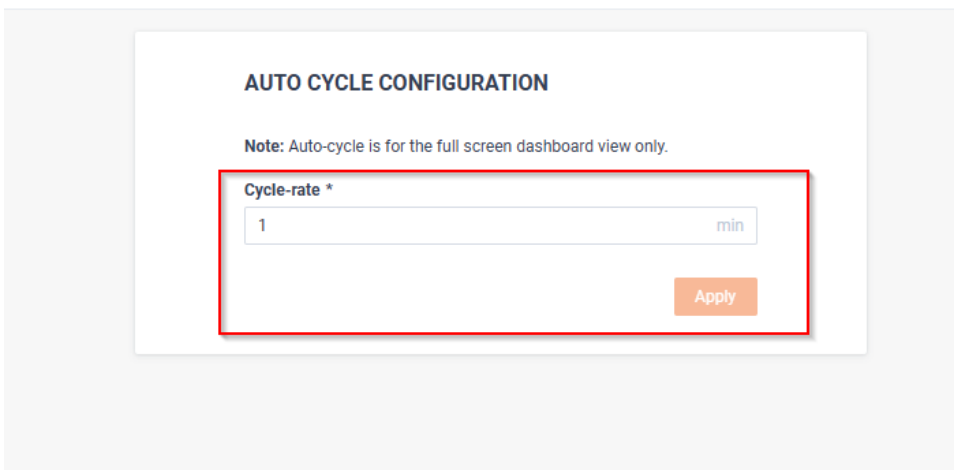
1. From LiveNX Web Click on Gear Icon and then select Settings.



2. On the settings Page Expand Dashboard Option and the select Auto Cycle Configuration.

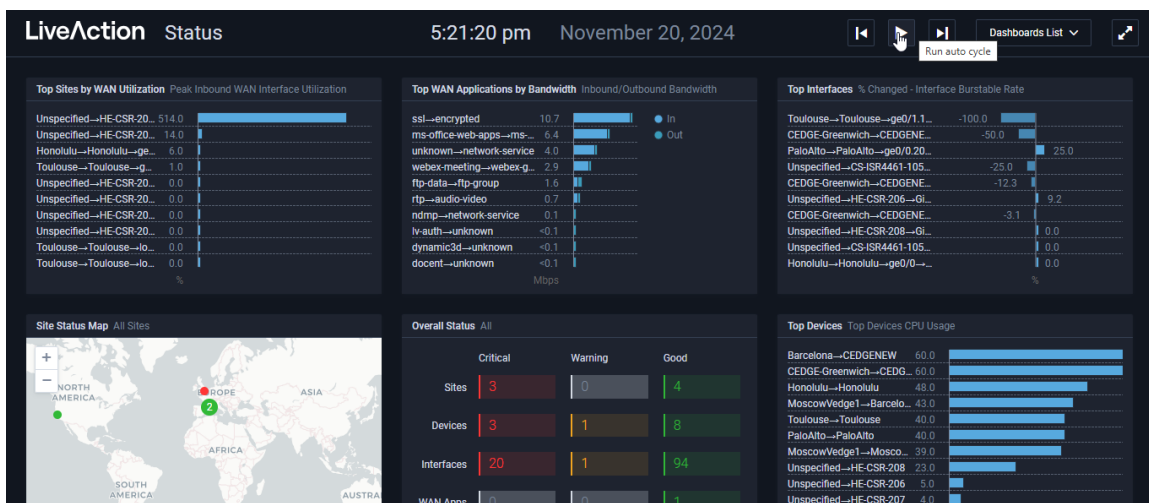
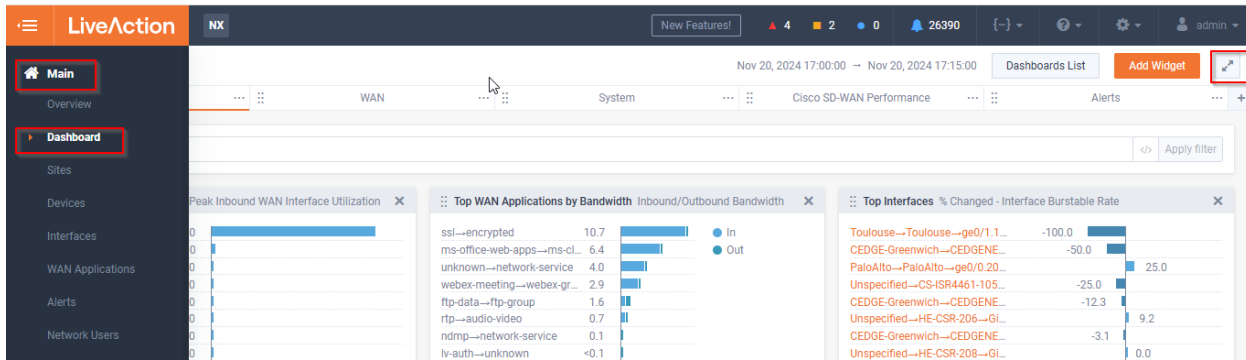


3. On The Auto Cycle configuration page you can configure the cycle rate (in minutes) for the Dashboard.



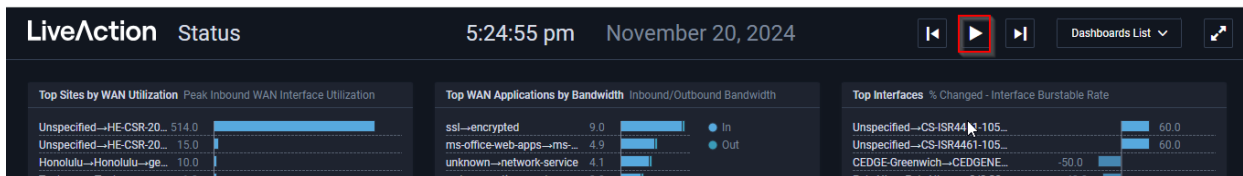
## Full Screen Dashboard

User can get the full screen dashboard on selecting the "Open FullScreen Button" available on Main > Dashboard of LiveNX web. It will open a full screen dark dashboard in new browser Tab.



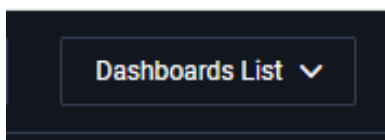
## Enabling Auto Rotation of Dashboard

On the Full Screen Dashboard you can enable the Auto rotation of the dashboards on selecting the "Run Auto Cycle Button".



## Configuration Options Available on Full Screen Dashboard

**Dashboard List:** It will list all the available Dashboard option which you can add in auto rotation feature.



**Go Back Button:** It will take you to the Previous Dashboard.



---

**Run Auto Cycle:** It will enable the auto rotation of the dashboard.



**Next Button:** It will show next Dashboard available in Dashboard List.



### **Individual dashboard options**

This allows users to choose which dashboards should be included in the rotation. This is not persisted.



# Improved Third Party Auth Login UX

Customers who use third party auth do not have local accounts for users and as such the “user name” and “password” sections are confusing since most people gravitate to that input rather than the TACACS or RADIUS buttons at the top. We have improved the login user experience to make it more intuitive.

## Logging In

The login experience has changed in the following ways:

- TACACS and RADIUS authentication buttons have been removed
- A new drop down menu to select the authentication mechanism has been added
  - Local auth, TACACS, and RADIUS can be selected if enabled
  - If TACACS and RADIUS are not enabled, then the drop down will not be visible

---

**Note** Single Sign On is intentionally left as a button because it needs to navigate to another page (IdP) to perform the authentication.

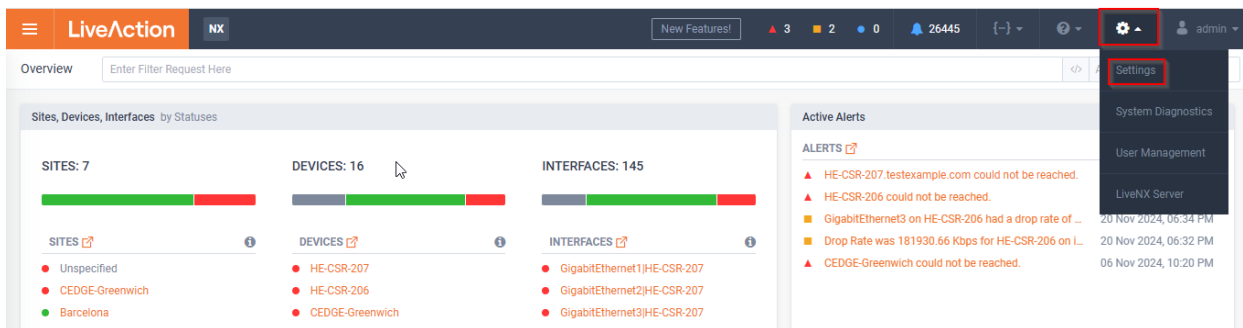
---

## Configuration

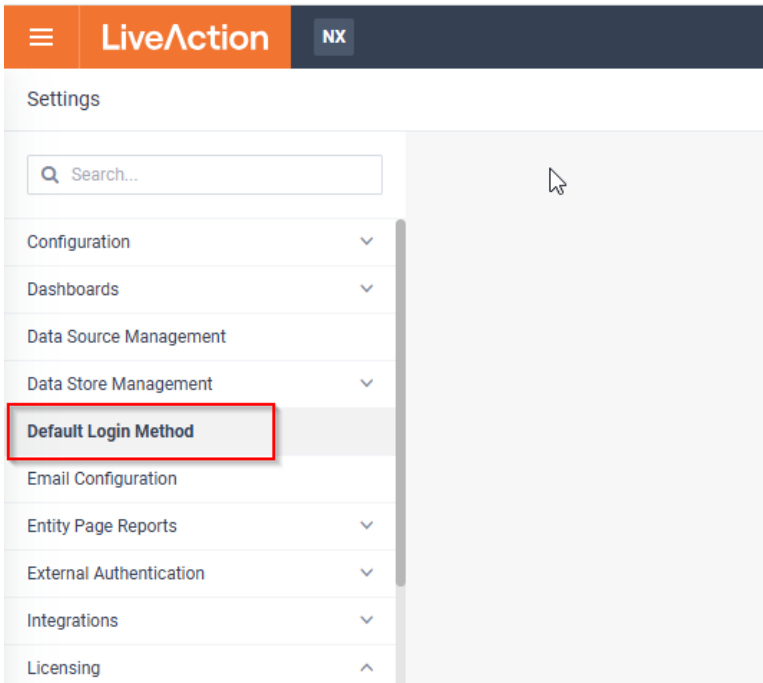
Every LiveNX deployment will have a primary authentication mechanism. Whether that is local users created via LDAP or using a third party auth mechanism like RADIUS. In order to reduce confusion, **admin users** can set the default login method via Settings ? Default Login Method.

Please find the steps below to configure the “Default Login Method”

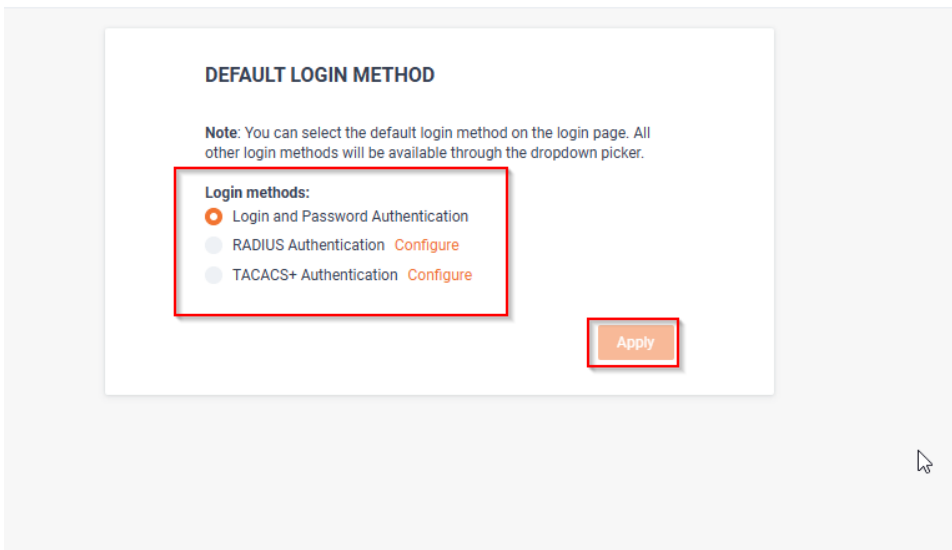
1. From LiveNX web, Select Gear icon available on Navigation bar and then select “Settings”.



2. On Settings Page, From left hand side menu options select "Default Login Method".



3. On The "Default Login Page" You can select your login method. and click Apply to make changes.



### Notable functionality

- The selected login method will be the default login method when on the landing page.
- If a selection is invalid due to the auth method being disabled (e.g., RADIUS was previously selected but has since been disabled via the RADIUS configuration), then the login method configuration will remain unchanged but the actual login page will default to "local" auth.
- Unconfigured authentication mechanisms will have a link to their respective configuration pages.

# Unlimited Dashboards

In 24.3.0 we have unbounded the number of dashboards to ensure that users do not need to juggle dashboards in order to stay within the allotted maximum of 12. This new functionality was added via a new “Dashboards List” drawer which allows users to store and manage dashboards exceeding the allotted viewable amount (12).

## Use Case

- I am an expert user who needs to create many dashboards for other users to use. Other users rely on me to manage their dashboards.
- I have many special dashboards and custom widgets that allow me to filter beyond what is available in the standard search bar. I do not have enough tabs.

## Functionality and Limitations

### Functionality

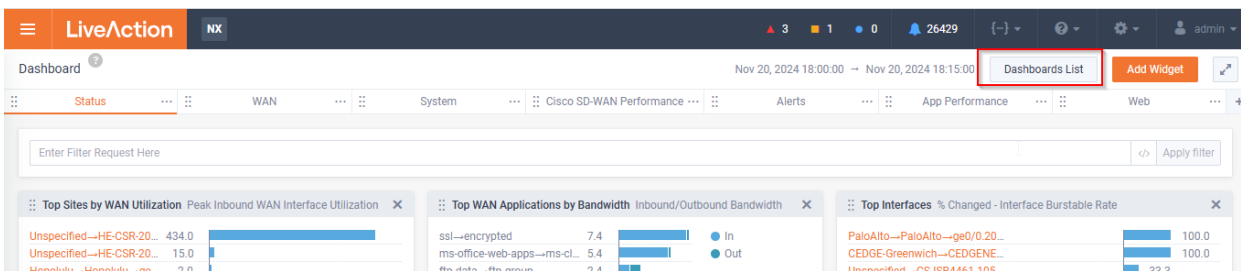
- Users can create any number of dashboards
- **Inactive** (stashed) dashboards are persisted in the dashboards list and can be shared, copied, etc
- All dashboards, active and inactive, are still tied to the user who created them
- All dashboards can be shared, deleted, or copied
- The dashboard list will show shared and imported dashboards, even if the user has not added them
  - These dashboards cannot be set to **active**, only copied. Copying them creates the dashboard and ties it to the current user.

### Limitations

- Only 12 dashboards can be **active** (viewable) at any time, similar to previous versions
- Renaming can only be done when the dashboard is **active**

## Accessing Dashboards List

The dashboard list can be accessed from the top of the dashboard page of LiveNX Web.



## Dashboard List Functionality

- **Sort by** - Sort by name, status, or selected to find the desired dashboard easier
- **Filtering** - Filter by string
- **Add** - Adds a new dashboard as active if possible. If there is no room a dashboard will be added in inactive state.
- **Duplicate** - Clones any selected dashboards and adds them to the dashboard list. All dashboards created in this manner will attempt to be activated if there is room.
- **Delete** - Deletes selected dashboards
- **Share/Unshare** - Shares/unshares the specific dashboard that is selected

The screenshot displays the LiveAction dashboard interface. The top navigation bar includes the LiveAction logo, a user profile icon for 'admin', and a notification bell with '26429' alerts. The main dashboard area is divided into several sections: 'Status' (with a filter input), 'WAN', 'System', 'Cisco SD-WAN Performance', and 'Alerts'. The 'Dashboards List' panel is open on the right, showing a search bar, a 'Sort by Status' dropdown, and buttons for 'Add', 'Duplicate', and 'Delete'. Below these are several dashboard entries, each with a checkbox, a status indicator (orange square), and a set of icons for actions (share, duplicate, delete, refresh). The entries include 'Status', 'WAN', 'System', 'Cisco SD-WAN Performance', 'Alerts', 'App Performance', 'VMware', 'Fortinet', and 'Voice/Video'. The 'Dashboards List' panel also indicates 'Active Dashboards: 8/12'.

## Caveat

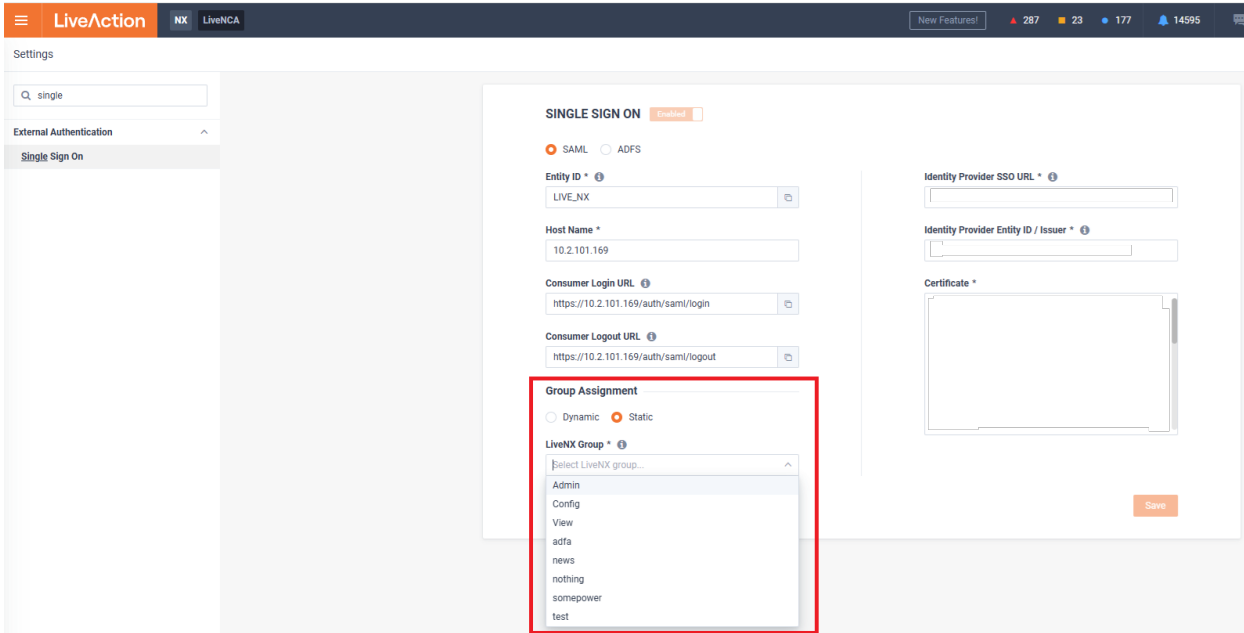
- When **adding** a dashboard, the standard default dashboard selection screen will only show up if there is an active slot. If no active slot is present the dashboard is added as inactive and the user will need to choose a default dashboard template at a later time.
- If creating more than the allowable number of dashboards, (e.g., duplicating 5 dashboards there are already 10 active dashboards) dashboards that exceed the active count limit will be set to inactive.

# SSO Static Group Assignment

Previously, dynamic authentication was introduced that allows a SAML IDP to provide role to assign to users. This behavior is a loophole to the above problem since anyone who controls the IDP could give admin access to LiveNX.

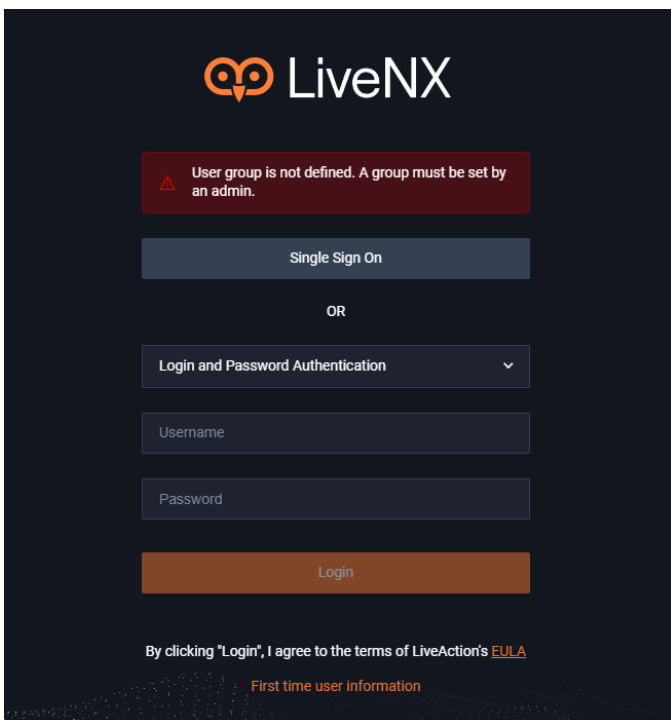
## Static SAML Group Assignment

A new **static group assignment** option has been added which if selected will assign all users who log in via SAML the specified user group.



## Edge Case

If static is selected but no user group is selected (e.g., selected user group has been deleted) then a message explaining this will be shown to users on attempted login.



# Alert Root Cause Analysis

Users want to know what an actionable analysis when something is wrong with their system. LiveNX will now send information to the platform to create a root cause analysis of what the problems could be and possible remediations.

## Supported Alerts for Root Cause Analysis

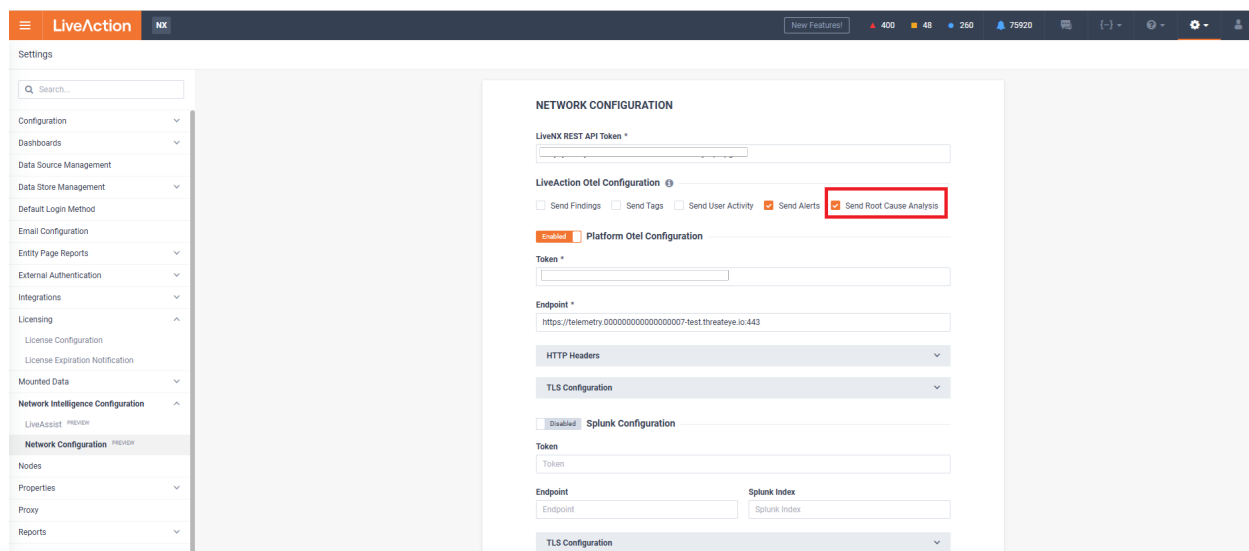
In LiveNX 24.3.0, we are targeting application performance alerts.

Alert	Version Introduced	Data Utilized
Critical Traffic Response Time	24.3.0	Flow path analysis
Voice/Video Performance - Jitter Avg	24.3.0	Flow path analysis
Voice/Video Performance - Jitter Max	24.3.0	Flow path analysis
Voice/Video Performance - Packet Loss	24.3.0	Flow path analysis
Application Performance - App Delay	24.3.0	Flow path analysis
Application Performance - Network Delay	24.3.0	Flow path analysis
Voice, Video Applications Performance	24.3.0	Flow path analysis
Low WAN Interface Utilization	24.3.0	Application report
High WAN Interface Utilization	24.3.0	Application report

## Configuration

Steps to enable and setup Alert Root Cause Analysis.

1. Configure LiveAssist - LiveAssist must be enabled for Root Cause analysis to work.
2. Ensure that the new "Send Root Cause Analysis" setting on the Settings > Network Intelligence. Go to *Setting > Network intelligence Configuration > Network Configuration*.



- Configure desired alerts to support root cause analysis. Any alert that can support root cause analysis will have a section on the alert configuration for "AI Diagnostics - Root Cause Analysis".

**Application Performance - App Delay**

LIST OF INSTANCES ADD NEW INSTANCE

1. New Alert Default Instance

INSTANCE DETAILS

For at Least: > 15 min, Automatic Resolution Time: Manual

Static
  Dynamic
  Static and Dynamic
  Static or Dynamic

**CRITICAL** ▲ Average Application Delay \*  ms

**WARNING** ■ Average Application Delay \*  ms

**INFO** ● Average Application Delay \*  ms

**AI Diagnostics**

**Basic Analysis**  
 A high level diagnostic useful for correlating various alerts together to better understand problems on the network. Information can be queried using LiveAssist.

**Root Cause Analysis**  
 Additional information will be gathered to provide guidance on the root cause and potential remediation. A synopsis will be added to alerts when available. This level of diagnostics can impact system performance and should be enabled sparingly.

**Sharing**

**Email**  
 Type Email

- Wait for alerts to be created. Once an alert is created, it can take some time for the root cause analysis to be generated. See above documentation for workflow.

## Workflow

Once a system has been properly configured, a new AI Diagnostics section will be available for alert configuration.

Alert Management LiveNX Alerts

ALERT TYPE	ENABLED	AFFECT STATUS	CATEGORY
> Application Bandwidth	✓	✓	Application
> Application Performance - App Delay	✓	✓	Application
> Application Performance - Network Delay	✓	✓	Application
> BGP Peer Connection Change	✓	✓	Network
> Cisco I WAN Path Change	✓	✓	Network
> Cisco I WAN Threshold Crossing	✓	✓	Network
> Cisco SD-WAN Performance - Jitter	✓	✓	Network
> Cisco SD-WAN Performance - Network Delay	✓	✓	Network
> Cisco SD-WAN Performance - Packet Loss	✓	✓	Network
> Cisco SD-WAN SLA Class Path Change	✓	✓	Network
> Cisco SD-WAN VManage Connectivity	✓	✓	System
> Critical Traffic Response Time	✓	✓	Application
> Device CPU Utilization	✓	✓	Device, Interface
> Device Flow Stop	✓	✓	Device, Interface
> Device Memory Utilization	✓	✓	Device, Interface
> Device Reachability	✓	✓	Device, Interface
> EIGRP Neighbor Count Decrease	✓	✓	Network
> EIGRP Neighbor Count Increase	✓	✓	Network
> Fan Tray Operational State	✓	✓	Device, Interface
> Fortinet Performance SLA - Jitter	✓	✓	Network
> Fortinet Performance SLA - Network Delay	✓	✓	Network
> Fortinet Performance SLA - Packet Loss	✓	✓	Network
> High WAN Interface Utilization	✓	✓	Device, Interface

**Application Performance - Network Delay**

LIST OF INSTANCES ADD NEW INSTANCE

1. New Alert Default Instance

INSTANCE DETAILS

For at Least: > 0 min, Automatic Resolution Time: Manual

**CRITICAL** ▲ Delay Time \*  ms

**WARNING** ■ Delay Time \*  ms

**INFO** ● Delay Time \*  ms

**AI Diagnostics**

**Basic Analysis**  
 A high level diagnostic useful for correlating various alerts together to better understand problems on the network. Information can be queried using LiveAssist.

**Root Cause Analysis**  
 Additional information will be gathered to provide guidance on the root cause and potential remediation. A synopsis will be added to alerts when available. This level of diagnostics can impact system performance and should be enabled sparingly.

**Sharing**

**Email**  
 Type Email

Cancel Save

## Notable details about alert configuration

- Basic analysis is enabled by default
- Root cause analysis is disabled by default
- Root cause analysis is only done for alerts created while root cause analysis is enabled. Enabling root cause analysis will not retroactively populate a root cause analysis for historic alerts.
- Every instance can have their own configuration. Users should try to apply as many filters as possible to alerts with root cause analysis enabled, this will ensure a smoother experience.

It is recommended that users do not enable root cause analysis for the default instance. Root cause analysis is processing intensive and should be used for as specific of a use case as possible. Applying more filters to an instance with root cause analysis will help to ensure a better experience.

## Viewing Root Cause Analysis

Any alert which should have a root cause analysis will have additional info available under the "AI diagnostics" section.

## Root Cause Analysis Pending

While LiveNX is waiting for a root cause analysis to be ready, a place holder message is added to the alert.

● **Application Performance - App Delay** ×

---

**Status & Time**

Status:

Time opened: 09 Nov 2024, 04:15 PM

Active for: 2 minutes

**Source Info**

Site: CSR

Device: HE-CSR-208

Conversation: TCP 48.10.0.11:443 to 66.1.0.11

Server Site: Internet

Client Site: Internet

Event: Report

**Description**

HE-CSR-208 had 0.00 ms application delay for the application youtube

**Details**

Application Name: youtube

Initial Average Application Flow Delay: 0.00 ms

Latest Average Application Flow Delay: 0.00 ms

Configured Threshold: 0.00 ms

AI Analysis Levels: Basic Analysis, Root Cause Analysis

**AI Diagnostics**

Summary: Root cause analysis in progress... Please check back later for the results.

**Notes**

Notes



## Root Cause Analysis Complete

Once a root cause analysis is populated, the information shown in the alert will change. As of 24.3.0, no email is sent notifying users that the root cause analysis is ready for the alert.

### ■ Voice, Video applications performance ×

---

#### Status & Time

Status: Active ▼

Time opened: 12 Nov 2024, 07:11 PM

Active for: 1 day

#### Source Info

Site: San Jose

Device: Media

Conversation: UDP 192.168.2.202:49991 to 10.2.101.141:5004

Source Site: Unspecified

Destination Site: Unspecified

#### Description

Media running application rtp-video had voice/video traffic with 15.17 ms max jitter

#### Details

Initial Packet Loss: 0.00 %

Latest Packet Loss: 0.00 %

Application: rtp-video

Packet Loss Threshold: 1.00 %

Jitter Max Threshold: 1.00 ms

Initial Jitter Max: 15.17 ms

Latest Jitter Max: 15.62 ms

AI Analysis Levels: Basic Analysis, Root Cause Analysis

#### AI Diagnostics

Summary: Analysis of the network path reveals significant packet loss and potential quality issues for media traffic.

Issues: 5 issues detected

#### Notes

Notes

## AI Diagnostic Details

- Issue:** High outbound packet loss rate of 34.2% on the Media device (10.4.202.205)  
**Recommendation:** Investigate the cause of packet loss on the Media device's outbound interface. Check for network congestion, interface errors, or misconfiguration.
- Issue:** DSCP marking set to 0 (Best Effort) for RTP video traffic  
**Recommendation:** Configure appropriate QoS policies to mark RTP video traffic with a higher priority DSCP value, such as AF41 or EF, to ensure better treatment across the network.
- Issue:** No QoS policies applied on inbound or outbound interfaces of the Media device  
**Recommendation:** Implement QoS policies on both inbound and outbound interfaces to prioritize and protect media traffic.
- Issue:** Jitter present in both directions, with maximum values of 27.578ms (inbound) and 27.878ms (outbound)  
**Recommendation:** Monitor jitter closely and consider implementing traffic shaping and prioritization to reduce jitter for improved media quality.
- Issue:** Lack of data for MOS score, network delay, and application delay  
**Recommendation:** Enable collection of these metrics to get a more comprehensive view of media quality and end-to-end performance.

## Additional Column Filter

When root cause analysis is enabled (i.e., when LiveAssist is enabled) an additional column will be present on the "View Alerts" page to filter on root cause analysis alerts. Any alert that has a completed or pending root cause analysis will show a check mark.

SEVERITY	SITE	DEVICE	DESCRIPTION	TIME OPENED	ACTIVE FOR	CATEGORY	TYPE	THIRD PARTY	AI DIAGNOSTIC...
Critical	LiveAction	MICRO-CSR-15.sd.liv...	MICRO-CSR-15.sd.livaction.com. had 511.22 ms application delay for the application cdn.vimeo.tv	12 Nov 2024, 11:37 PM	less than a mi...	Application	Application Performance - App Delay	Third Party I	
Info	LiveAction	MICRO-CSR-15.sd.liv...	MICRO-CSR-15.sd.livaction.com. had 124.00 ms application delay for the application ts01-b.clo...	12 Nov 2024, 11:33 PM	3 minutes	Application	Application Performance - App Delay		
Info	LiveAction	MICRO-CSR-15.sd.liv...	MICRO-CSR-15.sd.livaction.com. had 113.38 ms network delay for the application lida.tv	12 Nov 2024, 10:27 PM	about 1 hour	Application	Application Performance - Network Delay		✓
Info	Heaven	ASR1001.livaction.co...	Tunnel1 on ASR1001.livaction.com was over utilized at 109.22% in the Outbound direction.	12 Nov 2024, 08:17 PM	about 3 hours	Device, Interface	High WAN Interface Utilization		
Critical	PaioAlto	PaioAlto	PaioAlto to MoscowWedge1 on mpis: 0 % of packet loss (1.1.9.4 to 1.1.2.4)	12 Nov 2024, 06:16 PM	about 5 hours	Network	Cisco SD-WAN Performance - Packet Loss		
Info	LiveAction	MICRO-CSR-15.sd.liv...	MICRO-CSR-15.sd.livaction.com. had 150.33 ms application delay for the application cdn3.wowza	12 Nov 2024, 05:41 PM	about 6 hours	Application	Application Performance - App Delay		✓
Critical	PaioAlto	PaioAlto	PaioAlto to MoscowWedge1 on mpis: 0 % of packet loss (1.1.9.4 to 111.111.111.6)	12 Nov 2024, 05:23 PM	about 6 hours	Network	Cisco SD-WAN Performance - Packet Loss		
Info	Toulouse	Toulouse	Toulouse to Barcelona on mpis: 0 ms of jitter (1.1.20.4 to 1.1.4.4)	12 Nov 2024, 03:04 PM	about 9 hours	Network	Cisco SD-WAN Performance - Jitter		
Critical	LiveAction	MICRO-CSR-15.sd.liv...	MICRO-CSR-15.sd.livaction.com. had 109.57 ms network delay for the application us.tv.squared	12 Nov 2024, 02:23 PM	about 9 hours	Application	Application Performance - Network Delay		✓
Info	PaioAlto	PaioAlto	PaioAlto to Toulouse on mpis: 0 ms of jitter (1.1.9.4 to 2.2.20.4)	12 Nov 2024, 01:40 PM	about 10 hours	Network	Cisco SD-WAN Performance - Jitter		
Critical	LiveAction	MICRO-CSR-15.sd.liv...	MICRO-CSR-15.sd.livaction.com. had 112.63 ms network delay for the application granicus	12 Nov 2024, 01:21 PM	about 10 hours	Application	Application Performance - Network Delay		✓
Critical	PaioAlto	PaioAlto	PaioAlto to MoscowWedge1 on private1: 0 % of packet loss (1.1.10.4 to 111.111.111.10)	12 Nov 2024, 01:10 PM	about 10 hours	Network	Cisco SD-WAN Performance - Packet Loss		
Critical	LiveAction	MICRO-CSR-15.sd.liv...	MICRO-CSR-15.sd.livaction.com. had 121.57 ms network delay for the application a47b	12 Nov 2024, 11:26 AM	about 12 hours	Application	Application Performance - Network Delay		✓
Info	LiveAction	MICRO-CSR-15.sd.liv...	MICRO-CSR-15.sd.livaction.com. had 67.77 ms network delay for the application event.prod.bide.io	12 Nov 2024, 11:18 AM	about 12 hours	Application	Application Performance - Network Delay		✓
Critical	LiveAction	MICRO-CSR-15.sd.liv...	MICRO-CSR-15.sd.livaction.com. had 67.33 ms network delay for the application segment.prod.b...	12 Nov 2024, 11:18 AM	about 12 hours	Application	Application Performance - Network Delay		✓
Info	LiveAction	MICRO-CSR-15.sd.liv...	MICRO-CSR-15.sd.livaction.com. had 117.60 ms network delay for the application rbcu.as	12 Nov 2024, 11:17 AM	about 12 hours	Application	Application Performance - Network Delay		✓
Info	LiveAction	MICRO-CSR-15.sd.liv...	MICRO-CSR-15.sd.livaction.com. had 337.00 ms application delay for the application buffer-com	12 Nov 2024, 11:13 AM	about 12 hours	Application	Application Performance - App Delay		✓
Critical	LiveAction	MICRO-CSR-15.sd.liv...	MICRO-CSR-15.sd.livaction.com. had 194.60 ms network delay for the application adx.opera	12 Nov 2024, 11:12 AM	about 12 hours	Application	Application Performance - Network Delay		✓
Critical	LiveAction	MICRO-CSR-15.sd.liv...	MICRO-CSR-15.sd.livaction.com. had 73.00 ms network delay for the application pulseinsights	12 Nov 2024, 11:10 AM	about 12 hours	Application	Application Performance - Network Delay		✓
Critical	LiveAction	MICRO-CSR-15.sd.liv...	MICRO-CSR-15.sd.livaction.com. had 119.25 ms network delay for the application events.launch...	12 Nov 2024, 11:10 AM	about 12 hours	Application	Application Performance - Network Delay		✓
Critical	LiveAction	MICRO-CSR-15.sd.liv...	MICRO-CSR-15.sd.livaction.com. had 104.86 ms network delay for the application bs.serving-sys	12 Nov 2024, 11:10 AM	about 12 hours	Application	Application Performance - Network Delay		✓
Info	LiveAction	MICRO-CSR-15.sd.liv...	MICRO-CSR-15.sd.livaction.com. had 12.96 ms network delay for the application map.mp.nbc	12 Nov 2024, 11:10 AM	about 12 hours	Application	Application Performance - Network Delay		✓
Info	LiveAction	MICRO-CSR-15.sd.liv...	MICRO-CSR-15.sd.livaction.com. had 6.71 ms network delay for the application identity.mp.artice	12 Nov 2024, 11:10 AM	about 12 hours	Application	Application Performance - Network Delay		✓

---

## Technical details

- Root cause analysis is done on the platform
  - Data is sent from LiveNX via OTEL
  - Root cause analysis is based on flow path analysis topology data (available by clicking into the *conversation* link in an alert)
  - The OTEL process handles shutdowns and will keep it's place in processing and catch up once service restarts
  - The OTEL process polls every 1 minute
  - We poll for root cause analysis (RCA) events from LiveNX every 5 minutes. This can be configured via the property `platform.poll-interval-minutes`
  - We poll for the most recent 100k alerts that expect an RCA but have not received one
  - The platform can take up to 10 minutes to populate data into the RCA table
  - **Timeout** for API calls to platform is default 60 seconds. See "Additional Configuration" on how to modify this

## Advanced Configuration

This section is for fine tuning systems experiencing problems.

### Connection Timeouts

The LiveNX communication defaults all platform communication to **60 seconds**. This means if any query to LiveAssist takes longer than 60 seconds the request will be timed out to ensure the user is not waiting excessive amounts of time. This setting can be overwritten via *application properties*.

- `platform.connect-timeout-seconds` - default is 60 seconds
- `platform.read-timeout-seconds` - default is 60 seconds
- `platform.write-timeout-seconds` - default is 60 seconds

### Polling Interval

The root cause analysis polling interval can also be configured. This setting determines how often LiveNX polls the platform for root cause analysis.

- `platform.poll-interval-minutes` - default is 5 minutes
- Root cause analysis has to be enabled when an alert is triggered for an analysis to occur
  - Alerts created prior to the root cause analysis being enabled will not get an analysis
- Any alert triggered while root cause analysis will received an analysis
  - Disabling root cause analysis for an alert will not cancel pending analysis. This can be an issue if there are many alerts being generated as the root cause analysis may never catch up. A work around is to manually delete alerts from the database.
  - Only the most recent 100,000 alerts without a root cause analysis are polled for information. If the customer has many many alerts being created, we may never see data since we populate root cause analysis oldest to newest.

# LiveNX Security Dashboard

Users want an easy way to view their security findings. A grafana dashboard already existed but in 24.3.0 we have made it easier to navigate to it from within LiveNX.

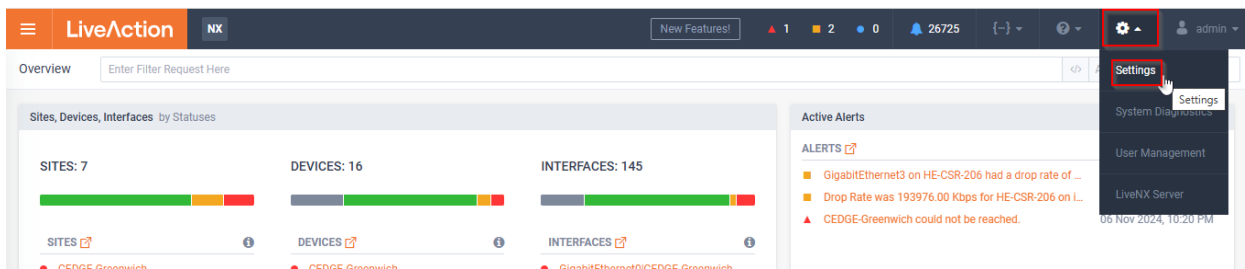
## Prerequisites

- Grafana must be enabled (should be enabled by default 24.3.0+). For enabling grafana (for LiveNX prior to 24.3.0), contact LiveAction support.
- Whoever wants to view the dashboard must be able to login to grafana.
- User with Admin role can be enable the security dashboard.

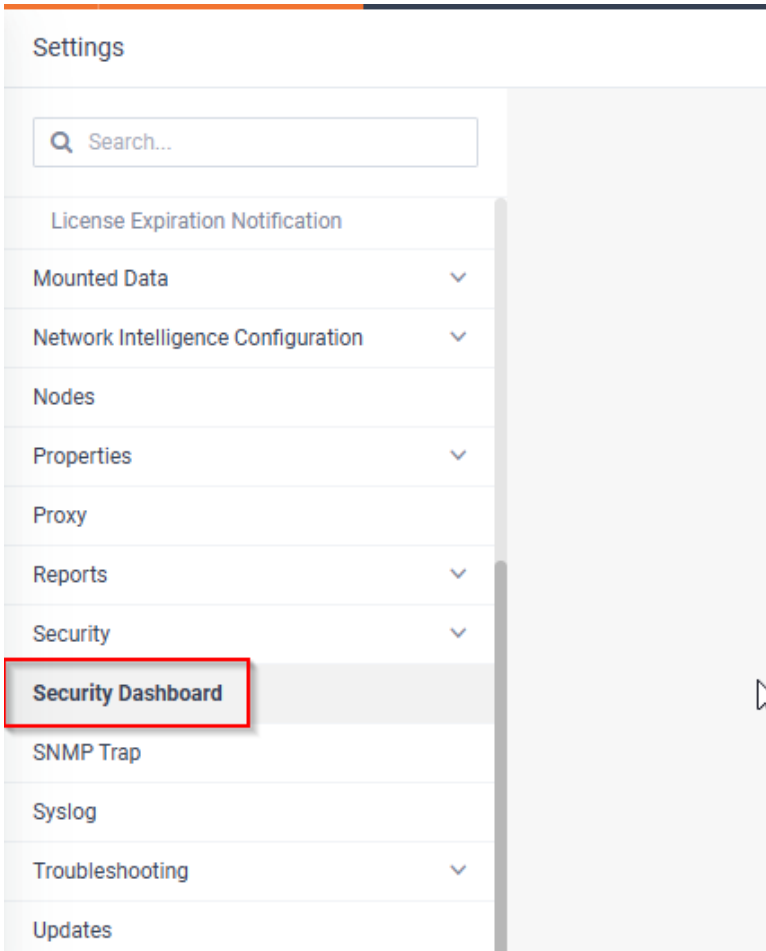
## Steps To Configure Security Dashboard

Any admin can enable the dashboard to appear for all users. Steps to configure the “Security Dashboard” are as below.

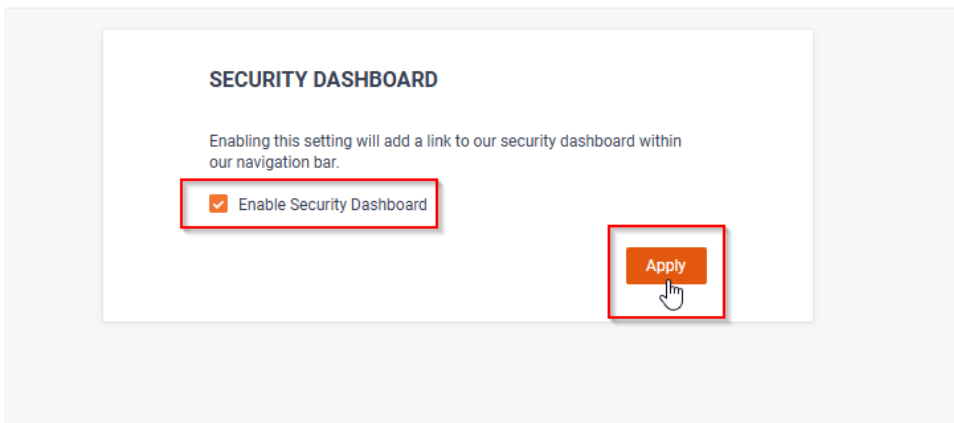
1. From LiveNX Web, select gear icon available on navigation bar and then select settings menu.



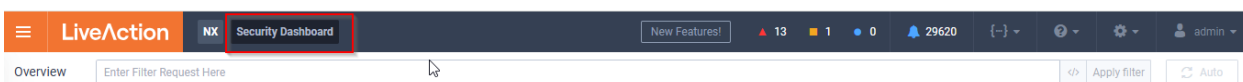
2. On the *Settings* page, find and select “Security Dashboard” option.



3. On the *Security* dashboard page, check “Enable Security Dashboard” and click **Apply**.



4. After enabling the security dashboard, a “Security Dashboard” button appears on the Navigation bar.





---

# Grafana Dashboards

## Overview

LiveNX 24.3.0 ships with Prometheus and Grafana, with dashboards to monitor aspects of the LiveNX deployment. Grafana can be accessed at <https://livenx-ip:3000/>.

## Dashboard

- Host metrics: **Monitoring / Node Exporter Full**
- Docker metrics: **Monitoring / Cadvisor exporter**
- Clickhouse metrics: **Monitoring / ClickHouse ...**
- LiveNX metrics: **Monitoring / LiveNX Performance**
- JVM: **Monitoring / JVM Micrometer**
- OpenTelemetry: **Monitoring / OpenTelemetry ...**

## Security

### Firewall Changes

Ports **3000** (grafana) and **9091** (prometheus) have been opened on the server.

Port **9091** (prometheus) has been opened on the nodes.

### Encryption and Authorization

All external communication with Prometheus and Grafana is encrypted with TLS, and authorization is required to access. Prometheus on the server collects metrics from prometheus on the nodes, and this communication is fully encrypted and authorized.

Prometheus and Grafana share TLS certificates with the LiveNX web application.

## Simplified Interface Deletion

Users often add too many interfaces and want to remove them from LiveNX. Prior to LiveNX 24.3.0, users would need to rediscover the device to select the correct interfaces. This process could take a long time, especially if attempting to modify multiple devices.

In LiveNX 24.3.0, we have resolved this issue by allow users to instantly delete interfaces without the need to go down the discovery process. The workflow is similar to deleting a device.

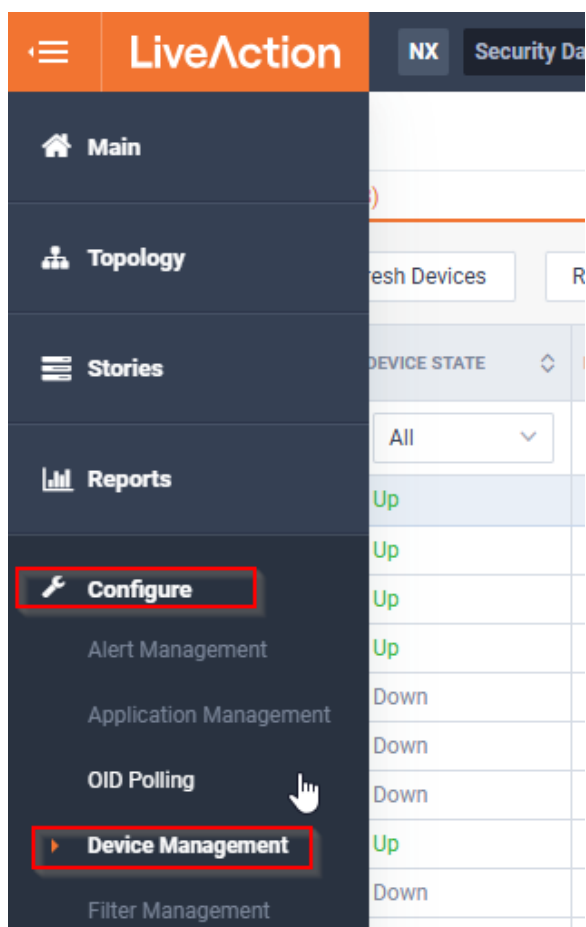
### Removing Interfaces

In LiveNX 24.3.0 interfaces can be removed / deleted by two methods which are described below.

#### From My Devices Page

To Remove the Interfaces please follow the steps below.

1. From LiveNX web go to *Configure* and then select the *Device Management* menu.





2. On the *Device Management* page, by default it will select the *My Devices* page. From this page select a device which interface you want to remove or delete from LiveNX and click the **Edit** button.

LiveAction NX Security Da

Device Management

My Devices (18)

Edit Delete Refresh Devices R

	DEVICE	DEVICE STATE
<input type="checkbox"/>	Device	All
<input checked="" type="checkbox"/>	CSR-Toul-Red	Up
<input type="checkbox"/>	CEDGEW	Up
<input type="checkbox"/>	TechSupport-310...	Up
<input type="checkbox"/>	Toulouse	Up
<input type="checkbox"/>	HE-CSR-207	Down
<input type="checkbox"/>	vbond	Down
<input type="checkbox"/>	CEdge-Greenwich	Down
<input type="checkbox"/>	CEDGEW	Up
<input type="checkbox"/>	vmanage	Down

3. After selecting the **Edit** button, the device configuration page opens. From this page select *Interfaces* tab. And from interfaces list, select the interface you want to remove. Click **Delete** and then **Apply**.

EDIT CSR-TOUL-RED

General Settings Interfaces

Add Edit Delete Search...

	NAME	SNMP INTE...	IFINDEX	IP ADDR...	SUBNET...	INPUT C...	OUTPUT...	SERVICE...	WAN/XC...	LABEL	TAGS
<input type="checkbox"/>	Name	All	Ifindex	IP Addr	Subnet	Input C	Output t	Service	A...	Label	Tags
<input type="checkbox"/>	GigabitEthernet1	✓	1								
<input type="checkbox"/>	GigabitEthernet2	✓	2					Default S...	WAN		
<input type="checkbox"/>	GigabitEthernet3	✓	3								
<input type="checkbox"/>	GigabitEthernet3.10	✓	6					Default S...	WAN		
<input type="checkbox"/>	GigabitEthernet3.20	✓	7					Default S...	WAN		
<input checked="" type="checkbox"/>	Null0	✓	5								
<input type="checkbox"/>	VoIP-Null0	✓	4								

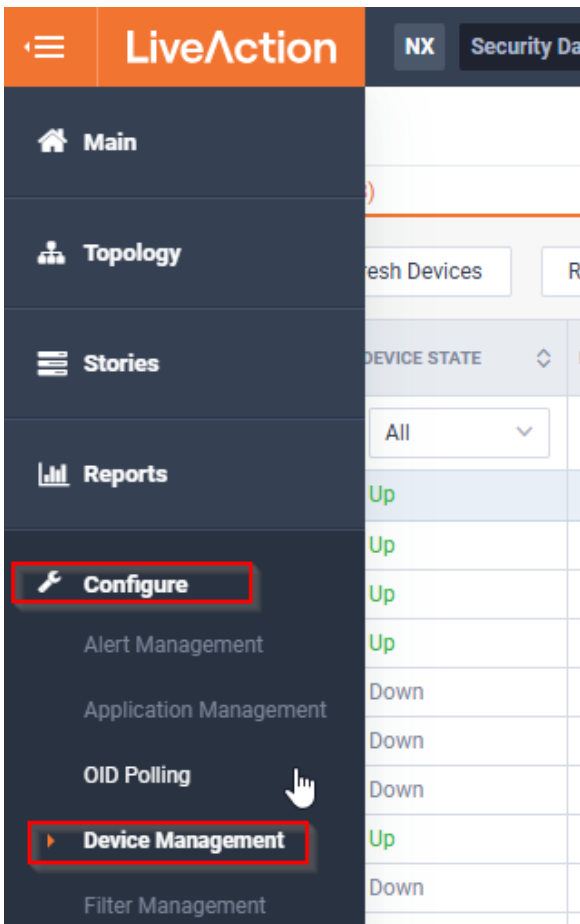
Rows: 7 / 7 Selected: 1

Cancel Apply

---

## From My Interfaces Page

1. From LiveNX web go to *Configure* and then select the *Device Management* menu.



2. On the *Device Management* page, Select the *My interfaces* tab. It will list all interfaces added in LiveNX.

3. From the *My Interfaces* page, find and select the interface which you want to delete and click the **Delete** button, and then confirm the delete.

Device Management CSV Import/Export

My Devices (18) My Interfaces (155)

	NAME	INTERFACE STATE	DEVICE	DEVICE STATE	SITE	SERVICE PR...
<input type="checkbox"/>	<input type="text" value="Name"/>	<input type="text" value="All"/>	<input type="text" value="Device"/>	<input type="text" value="All"/>	<input type="text" value="Site"/>	<input type="text" value="Service Pro"/>
<input checked="" type="checkbox"/>	GigabitEthernet1	Up	CSR-Toul-Red	Up	MoscowVed...	
<input type="checkbox"/>	GigabitEthernet2	Up	CSR-Toul-Red	Up	MoscowVed...	Default Servi...
<input type="checkbox"/>	GigabitEthernet3	Up	CSR-Toul-Red	Up	MoscowVed...	
<input type="checkbox"/>	GigabitEthernet3.10	Up	CSR-Toul-Red	Up	MoscowVed...	Default Servi...
<input type="checkbox"/>	GigabitEthernet3.20	Up	CSR-Toul-Red	Up	MoscowVed...	Default Servi...
<input type="checkbox"/>	Null0	Up	CSR-Toul-Red	Up	MoscowVed...	
<input type="checkbox"/>	VoIP-Null0	Up	CSR-Toul-Red	Up	MoscowVed...	
<input type="checkbox"/>	eth0	lin	TechSupport-31	lin		

# Dynamic Alert Thresholds

## Overview

The dynamic alert thresholds feature is a way to intelligently choose alert thresholds based on historic data. Dynamic thresholds are polled, calculated, and cached once every hour based on the filter configured by the user. The thresholds will be based on the last 30 days of data specifically looking at the current hour for the current day of the week.

## Alerts Supported as of 24.3.0

As of LiveNX 24.3.0, Application Performance - App Delay alert is supported.

## Configuration

There are four new configuration options for alert instances that support the new dynamic alert thresholds feature.

### Static

This option is akin to what users are already familiar with prior to the addition of this feature.

**Application Performance - App Delay**

**LIST OF INSTANCES** ADD NEW INSTANCE **INSTANCE DETAILS**

1. test Default Instance

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

**Instance Name \***  
test

**Alert Source \***  
Application: ms-services

**Time Window Setting:** For sites without business hours configured this setting will be ignored. Alerts can be triggered at any time of day.

**Thresholds**

**For at Least \***  min **Automatic Resolution Time \***

Static  Dynamic  Static and Dynamic  Static or Dynamic

**CRITICAL** ▲ **Average Application Delay \***  
 ms

**WARNING** ■ **Average Application Delay \***  
 ms

**INFO** ● **Average Application Delay \***  
 ms

## Dynamic

This is a new option that will calculate the threshold(s) dynamically based on historic data within the configured standard deviation.

### Application Performance - App Delay

LIST OF INSTANCES **ADD NEW INSTANCE** INSTANCE DETAILS

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

Default Instance

Instance Name \*  
test

Alert Source \*  
Application: ms-services Enter Filter Request Here

Time Window Setting: For sites without business hours configured this setting will be ignored. Alerts can be triggered at any time of day.

Thresholds

For at Least \* Automatic Resolution Time \*

> 1 min Manual

Static  Dynamic  Static and Dynamic  Static or Dynamic

CRITICAL  Standard Deviation \*  
>= 15

WARNING  Standard Deviation \*  
>= 10

INFO  Standard Deviation \*  
>= 1

Cancel Save

## Static and Dynamic

This is a new option which combines the two aforementioned options with a logical AND. This requires both thresholds to be met in order for an alert to be created.

### Application Performance - App Delay

LIST OF INSTANCES + ADD NEW INSTANCE INSTANCE DETAILS

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

Default Instance

**Instance Name \***  
test

**Alert Source \***  
Application: ms-services Enter Filter Request Here

**Time Window Setting:** For sites without business hours configured this setting will be ignored. Alerts can be triggered at any time of day.

**Thresholds**

**For at Least \***  min **Automatic Resolution Time \*** + Manual

Static  Dynamic  Static and Dynamic  Static or Dynamic

<input checked="" type="checkbox"/> CRITICAL <span>▲</span>	<b>Average Application Delay *</b> <input type="text" value="500"/> ms	AND	<b>Standard Deviation *</b> <input type="text" value="15"/> σ
<input checked="" type="checkbox"/> WARNING <span>■</span>	<b>Average Application Delay *</b> <input type="text" value="400"/> ms	AND	<b>Standard Deviation *</b> <input type="text" value="10"/> σ
<input checked="" type="checkbox"/> INFO <span>●</span>	<b>Average Application Delay *</b> <input type="text" value="0"/> ms	AND	<b>Standard Deviation *</b> <input type="text" value="1"/> σ

Cancel Save

## Static or Dynamic

This is a new option which is less restrictive than the previous option applying a logical OR to the static and dynamic thresholds. With this option, if either the static OR dynamic thresholds are met, then an alert will be created.

**Application Performance - App Delay**

LIST OF INSTANCES **ADD NEW INSTANCE** INSTANCE DETAILS

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

Default Instance

Instance Name \*  
test

Alert Source \*  
Application: ms-services Enter Filter Request Here

Time Window Setting: For sites without business hours configured this setting will be ignored. Alerts can be triggered at any time of day.

Thresholds

For at Least \* Automatic Resolution Time \*  
> 1 min Manual

Static  Dynamic  Static and Dynamic  Static or Dynamic

CRITICAL ▲ Average Application Delay \* Standard Deviation \*  
≥ 500 ms OR ≥ 15

WARNING ■ Average Application Delay \* Standard Deviation \*  
≥ 400 ms OR ≥ 10

INFO ● Average Application Delay \* Standard Deviation \*  
≥ 0 ms OR ≥ 1

Cancel Save

## Implementation Details

Thresholds are polled from Clickhouse hourly and cached in memory per instance.

## Caveats

- Dynamic config options are only available for non default instances. This restriction is for performance reasons since default instances do not require a filter.
- Since this is based on historic data in Clickhouse, dynamic thresholds may not work for the first week until there is sufficient data.

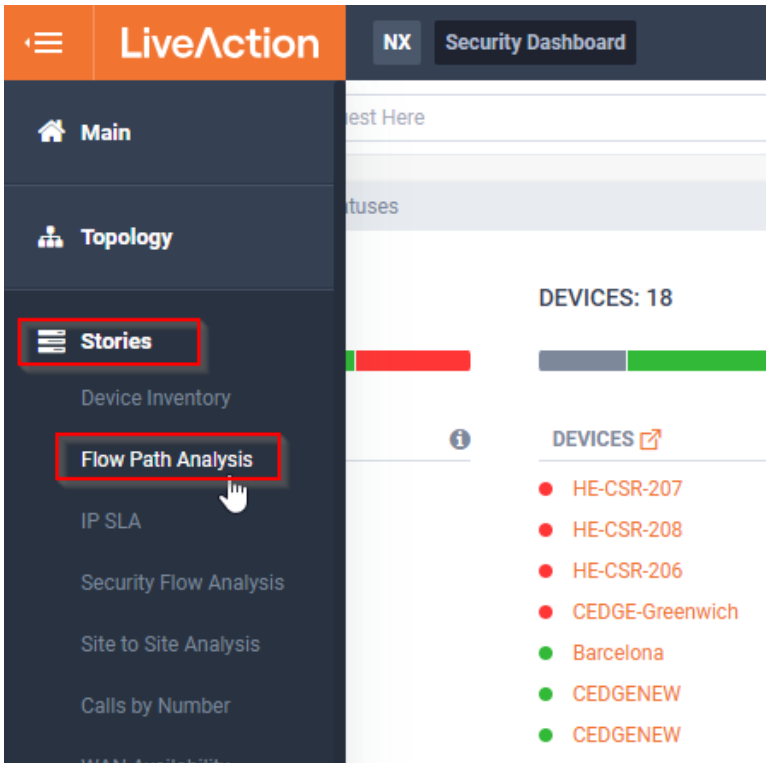
# Device Model on Flow Path Analysis

In LiveNX 24.3.0 we added an ability where user can see device model details in Flow Path Analysis report. Now user would have better understanding of what the devices in a path view are.

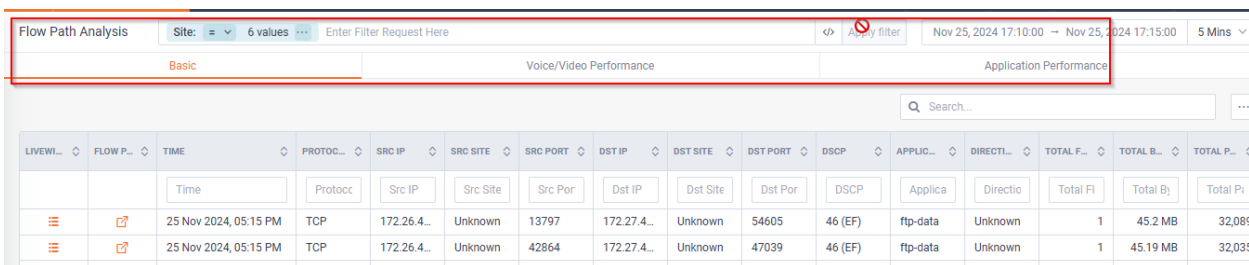
## Step To Get Flow Path Analysis

To get the flow path analysis please follow the steps below.

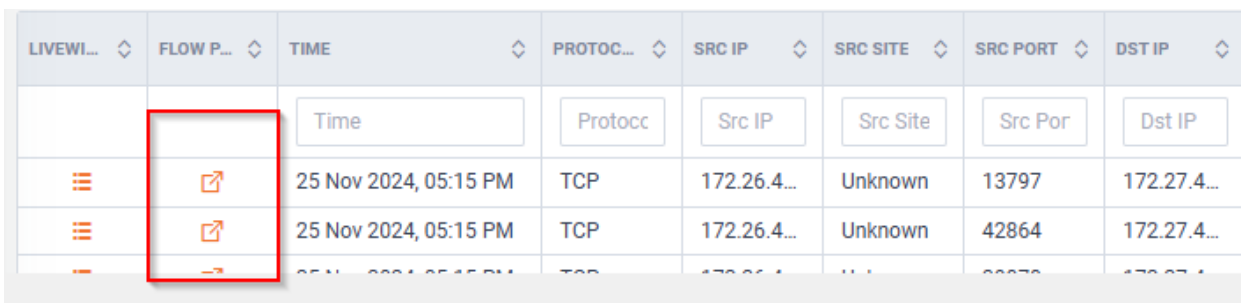
1. From LiveNX web go to Stories and select Flow Path Analysis option.



2. On Flow Path Analysis Page, Select the flow options and configure the filter to get the result.



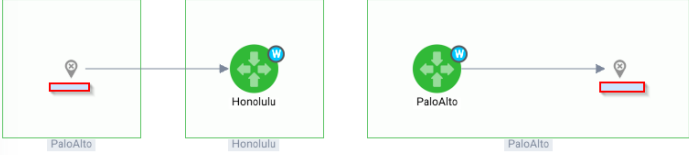
3. On the result page select the Drill down icon from Flow path Analysis column. It will open a new page in new tab.





4. On the new page user would be able to see the Flow path Analysis of the selected packet flow and the device models.

WAN Applications > PATH ICMP [redacted] Nov 25, 2024 17:15:00 - Nov 25, 2024 17:20:00



The diagram illustrates a network path analysis. It consists of three main components: a PaloAlto device on the left, a Honolulu site in the middle, and another PaloAlto device on the right. Arrows indicate the flow direction: from the left PaloAlto to Honolulu, and from Honolulu to the right PaloAlto. A second arrow points from the right PaloAlto back to the left PaloAlto, suggesting a return path. The Honolulu site is represented by a green circle with a 'W' icon. The PaloAlto devices are represented by red rectangles with a location pin icon.

**Path Flow** PaloAlto - PaloAlto

Device Name	Honolulu	PaloAlto
Device Model	vedgeCloud	vedgeCloud
Site Name	Honolulu	PaloAlto
Application	unknown	unknown
CPU Usage	42.00 %	33.00 %
Memory Usage	38.00 %	34.00 %
In Interface	Local	ge0/0.20

---

# Application Bandwidth Alert

A new alert has been added for application bandwidth. This will help users understand anomalous traffic behavior for specific applications.

## Alert

### Functionality

This alert supports our standard set of functionality, including:

- Multiple instances
- Multiple severities
- Filtering
  - Region
  - Site
  - Device
  - Interface
  - Tag
  - Application
- Contribution to status
- Auto-resolution
- "For at least" - time until alert is triggered

### Evaluation

Each incoming flow record is examined and the bandwidth is calculated using the **byte count** and the **switch times**. This allows us to calculate the bandwidth off a single flow record.

### Alert Keys

The combination of these fields are what make an alert unique. Note the granularity of an alert. This means that this alert should not be used to determine if a group of interfaces at a site are experiencing high traffic since there is no aggregation between interfaces.

- Device
- Interface
- Direction
- Application

## Example Alert

● Application Bandwidth
✕

---

### Status & Time

Status: Active

Time opened: 13 Nov 2024, 09:53 PM

Active for: less than a minute

### Source Info

Site: LiveAction

Device: MICRO-CSR-15.sd.liveaction.com.

Interface: GigabitEthernet3

Application: imrworldwide

Event: Report

### Description

imrworldwide application's bandwidth was 33.86 Kbps for MICRO-CSR-15.sd.liveaction.com. on interface GigabitEthernet3 in the Outbound direction

### Details

Application Name: imrworldwide

Direction: Outbound

Initial Application Bandwidth: 33.86 Kbps

Latest Application Bandwidth: 33.86 Kbps

Configured Threshold: 1.00 Kbps

AI Analysis Levels: Basic Analysis

### Notes

Save

## Example Report Drill Down

Report

View Options
Share
Print
Schedule
Copy
Close

---

Application Bandwidth Alert Event | Application (Flow)
✎

Device: MICRO-CSR-15 Interface: GigabitEthernet3 Display Filter: No Display Filtering Direction: outbound Flow Type: basic Execution Type: timeseries Sort By: BIT\_RATE Flex Search: flow.app="imrworldwide" Bin Duration: auto Report Data Source: auto Start Time: Nov 13, 2024 21:23:02 HST (GMT-10:00) End Time: Nov 13, 2024 22:22:02 HST (GMT-10:00) Business Hours: none Execution Data Source: flowstore\_v2 Bin Interval: 1 minute

Legend

- imrworldwide

☰

Legend	Application	Total Flows	Total Bytes	Total Packets	Average Bit Rate	Average Packet Rate
<span style="width: 10px; height: 10px; background-color: #2980b9; display: inline-block; margin-right: 5px;"></span>	imrworldwide	131	293.76 KB	1,241	0.66 Kbps	0.35 pp

---

## Caveats

- Reporting is based on 1 minute bins that average the data where as alerts are on individual flow records. This means that even though a high value is detected and alerted on, the report may never see the same peak due to the average binning.
  - It is recommended to use a "for at least" of at least 5 minutes to ensure bursty traffic does not cause alerts. By having a "for at least" of several minutes it ensures traffic is staying above the targeted threshold for a lengthy period of time which will be more visible in reporting.