

LiveAction®

# LiveNX

## Operations Dashboard

---

User Guide



LiveAction, Inc.  
960 San Antonio Road, Ste. 200  
Palo Alto, CA 94303, USA  
+1 (888) 881-1116  
<https://www.liveaction.com>

Copyright © 2021 LiveAction, Inc.  
All rights reserved

20211124-LNXU\_215a

# Contents

<b>Chapter 1</b>	<b>Introduction</b> .....	<b>1</b>
	Overview.....	2
	Overview Page.....	2
	Status Bar .....	2
	Navigation Bar .....	10
<b>Chapter 2</b>	<b>Main</b> .....	<b>11</b>
	Main .....	12
	Overview.....	12
	Dashboard.....	14
	Sites .....	25
	Devices.....	33
	Interfaces .....	42
	WAN Applications.....	47
	Alerts.....	49
	Network Users.....	56
<b>Chapter 3</b>	<b>Topology</b> .....	<b>59</b>
	Geo Topology .....	60
	Logical Topology .....	72
<b>Chapter 4</b>	<b>Stories</b> .....	<b>84</b>
	Stories.....	85
	Device Inventory .....	85
	Flow Path Analysis.....	86
	IP SLA .....	89
	SD Access Traffic Assessment .....	91
	Security Flow Analysis.....	93
	Site to Site Analysis.....	94
	Calls by Number .....	99
	WAN Availability.....	102
	WAN Capacity Planning .....	103
	WAN Utilization .....	106
<b>Chapter 5</b>	<b>Reports</b> .....	<b>109</b>
	Reports.....	110
	List of Reports.....	110
	List of Report Parameters .....	116
	View Reports .....	117
	Custom Reports.....	135
	View Schedule.....	140
<b>Chapter 6</b>	<b>LiveNA</b> .....	<b>148</b>
	LiveNA .....	149
	Predictions.....	153

## Introduction

### In this chapter:

<i>Overview</i> .....	2
<i>Overview Page</i> .....	2
<i>Status Bar</i> .....	2
<i>Navigation Bar</i> .....	10



## Overview

LiveNX is an intelligent, action-oriented Network Operations and Management software that provides real-time visualizations, deep monitoring, and troubleshooting of multi-vendor network devices, with an easy-to-use graphical user interface.

LiveNX delivers its network and application monitoring capabilities via two User Interfaces. The Operations Dashboard delivered via Web technologies is the primary interface and is built for Day 2 network operations. It is designed to be used by Operations Engineers, Tier 1, 2 Technical Support Engineers, and advanced users such as Networking Administrators and Network Architects. The Engineering Console is delivered via a thick-client and is built for configurations (e.g., QoS policies) and caters to Network Engineers and Architects who want to perform deeper troubleshooting tasks. This User Guide is built for users of the Operations Dashboard. For the User Guide built for users of the Engineering Console, please refer to our complete documentation at <https://docs.liveaction.com/LiveNX>.

When accessing the LiveNX Operations Dashboard, the default page presented after successful login is the Overview page. At the top of this page is a status bar. This will be present on all other LiveNX pages.

## Overview Page

The *Overview Page* shows status for *Sites*, *Devices*, and *Interfaces*. It also shows *Active Alerts*. Users can drill down using these links to explore further.

The screenshot displays the LiveNX Overview page. At the top, there is a navigation bar with the LiveAction logo and a status bar showing 273 alerts, 12 devices, and 4 interfaces. Below the navigation bar, the main content area is divided into two sections: 'Sites, Devices, Interfaces by Status' and 'Active Alerts'.

**Sites, Devices, Interfaces by Status:**

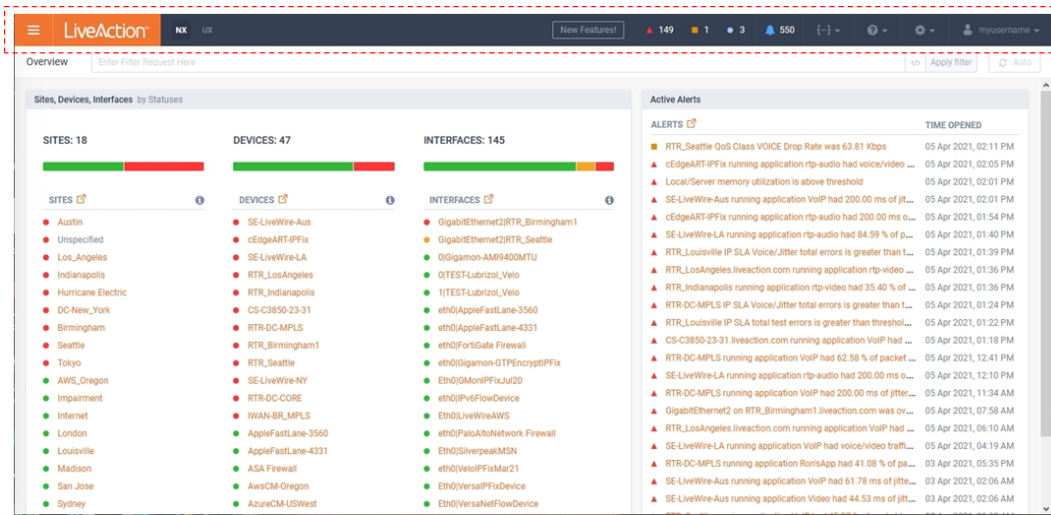
- SITES: 103** (Total: 103, Green: 103, Red: 0)
- DEVICES: 26** (Total: 26, Green: 26, Red: 0)
- INTERFACES: 79** (Total: 79, Green: 79, Red: 0)

**Active Alerts:**

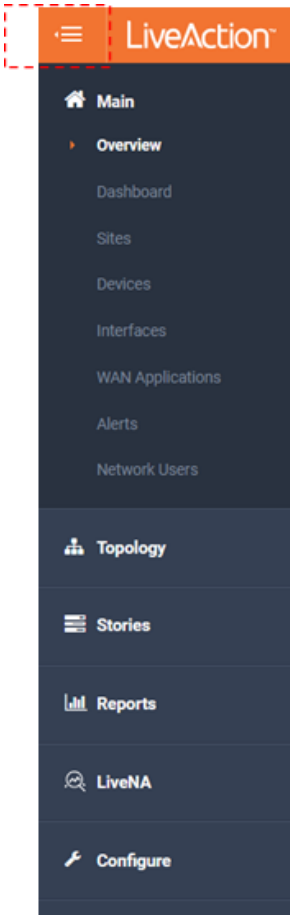
Alert Description	Time Opened
LiveWire running application rtp had 49.18 % of packet loss for traffic with a DSCP value of 0 (BE)	08 Feb 2021, 08:15 AM
RTR_Seattle QoS Class VIDEO Drop Rate was 34.30 Kbps	08 Feb 2021, 08:15 AM
RTR_Seattle running application VoIP had 200.00 ms of jitter for traffic with a DSCP value of 46 (EF)	08 Feb 2021, 08:15 AM
RTR_SanJose QoS Class SET_DSCP_VOICE Drop Rate was 82.53 Kbps	08 Feb 2021, 08:15 AM
RTR_Austin liveaction.com QoS Class VOICE Drop Rate was 2.51 Kbps	08 Feb 2021, 08:15 AM
LiveWire running application QoS Class VoIP had 44.27 % of packet loss for traffic with a DSCP value of 46 (EF)	08 Feb 2021, 08:14 AM
RTR_Austin liveaction.com had 55.00 ms network delay for the application mongo	08 Feb 2021, 08:12 AM
RTR_LosAngeles.liveaction.com running application rtp-video had 18.31 % of packet loss for traffic with a DSCP value ...	08 Feb 2021, 08:11 AM
RTR_Madison IP SLA Voice/After total errors is greater than threshold value: 3	08 Feb 2021, 08:09 AM
LiveWire running application VoIP had 200.00 ms of jitter for traffic with a DSCP value of 46 (EF)	08 Feb 2021, 08:07 AM
RTR_Seattle running application VoIP had 29.73 % of packet loss for traffic with a DSCP value of 46 (EF)	08 Feb 2021, 08:03 AM
RTR_SanJose QoS Class Default Drop Rate was 3.99 Kbps	08 Feb 2021, 07:57 AM
RTR_LosAngeles.liveaction.com QoS Class VoIP 19427 Drop Rate was 0.09 Kbps	08 Feb 2021, 07:56 AM
Local Server memory utilization is above threshold!	08 Feb 2021, 05:29 AM
ITR-DC-MPLS running application rtp had 34.24 % of packet loss for traffic with a DSCP value of 46 (EF)	08 Feb 2021, 05:22 AM
GigabitEthernet2 on RTR_Madison was over utilized at 54.69% in the Inbound direction.	08 Feb 2021, 04:04 AM
GigabitEthernet2 on RTR_Birmingham1 liveaction.com was over utilized at 54.71% in the Inbound direction.	08 Feb 2021, 01:10 AM
GigabitEthernet2 on RTR_Seattle was over utilized at 51.97% in the Inbound direction.	08 Feb 2021, 01:09 AM
GigabitEthernet2 on RTR_SanJose was over utilized at 49.87% in the Inbound direction.	08 Feb 2021, 01:09 AM
GigabitEthernet2 on RTR_London was over utilized at 46.35% in the Inbound direction.	08 Feb 2021, 01:09 AM
GigabitEthernet2 on RTR_Austin liveaction.com was over utilized at 44.12% in the Inbound direction.	08 Feb 2021, 01:09 AM
RTR_LosAngeles.liveaction.com running application VoIP had 4.07 % of packet loss for traffic with a DSCP value of 46 ...	08 Feb 2021, 01:08 AM
RTR_Seattle running application VoIP had 2.63 % of packet loss for traffic with a DSCP value of 0 (BE)	08 Feb 2021, 01:08 AM
RTR-DC-MPLS running application rtp had 35.22 % of packet loss for traffic with a DSCP value of 0 (BE)	07 Feb 2021, 01:58 PM

## Status Bar

The Status Bar at the top of the *Overview* page provides status and access to the main Navigation Bar, and to a variety of LiveNX functions.

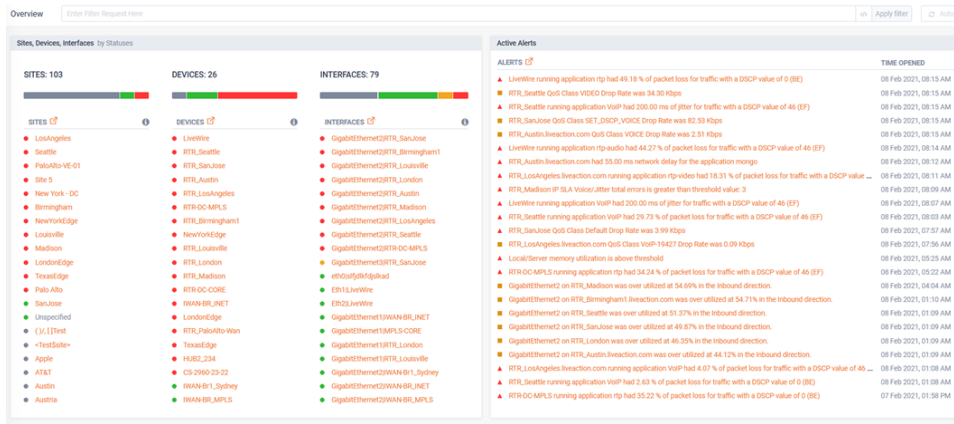


The status bar's menu icon at the top left of the page expands the Navigation Bar. The majority of LiveNX daily usage tasks are found from this menu. See [Navigation Bar](#) on page 10.

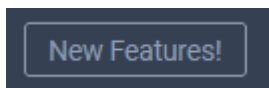


The status bar's LiveAction icon provides quick access back to the Overview page.

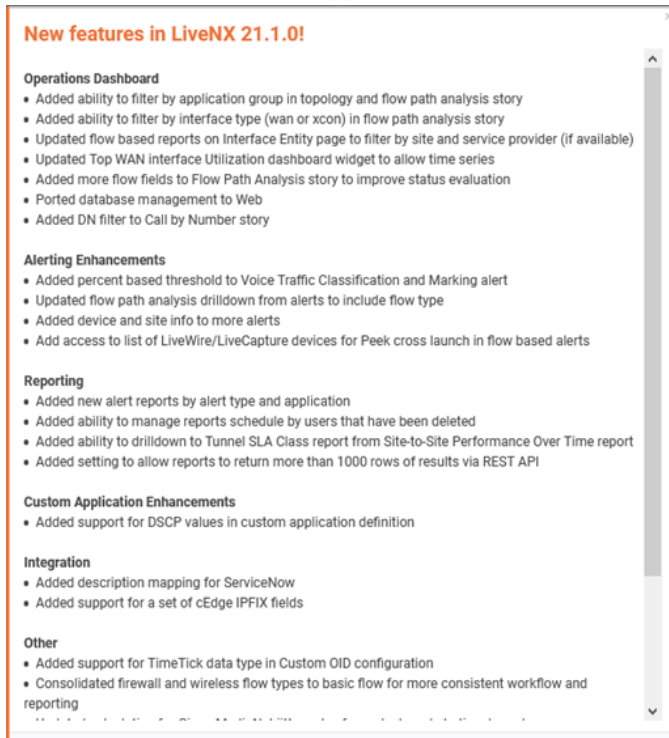




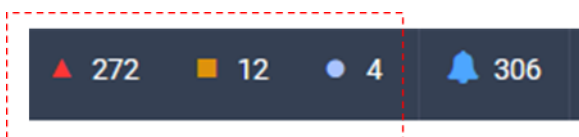
The **New Features!** button appears on the status bar after upgrading LiveNX to a new major or minor version.



Clicking the **New Features** button will present a list of the new features.



The status bar shows the number of active Alerts organized by severity.



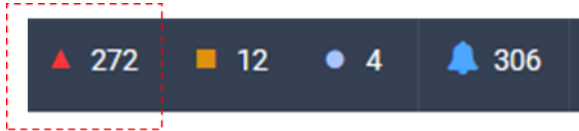
The LiveNX Alert severities are:

● Info

■ Warning

▲ Critical

Clicking on a severity will open the *Alert* page, pre-filtered by the selected severity.



Alerts  Apply Filter Configure Alerts

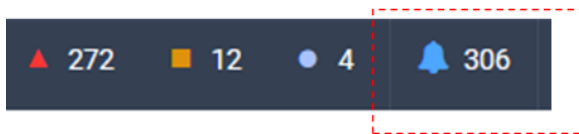
Active History

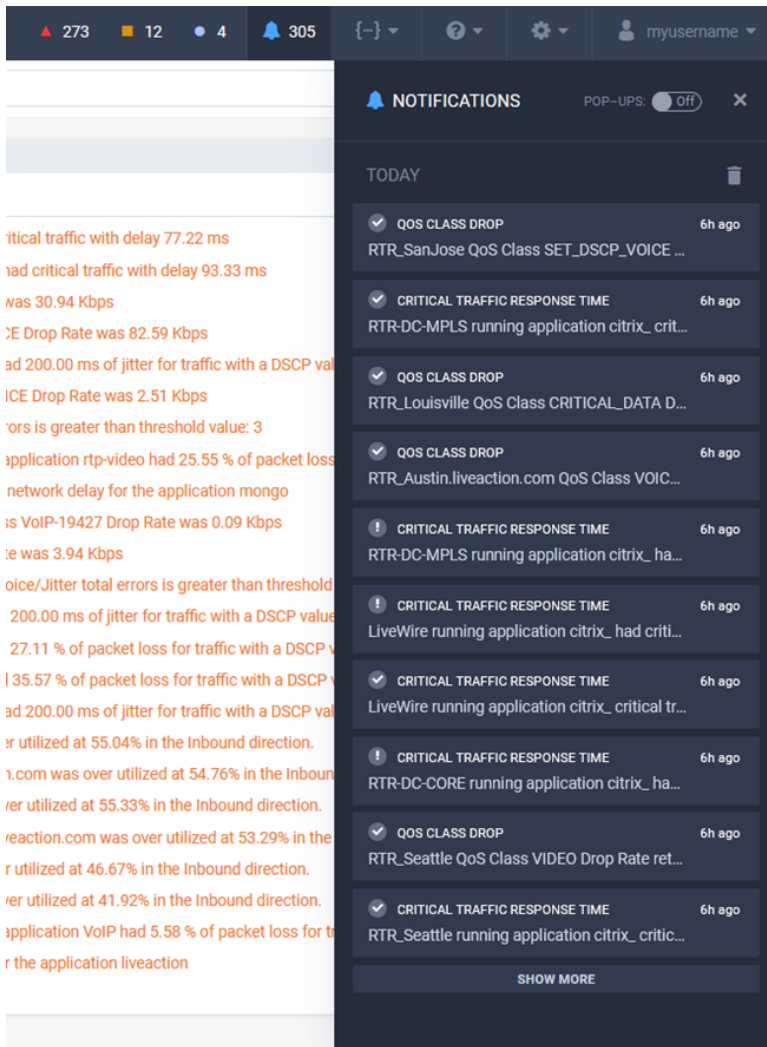
Resolve Ignore Acknowledge Refresh Alerts

SEVERITY	DESCRIPTION	TIME OPENED	ACTIVE FOR	CATEGORY	TYPE	THIRD PARTY INTEGRATIONS
▲ Critical	RTR_SanJose QoS Class Default Drop Rate was 78.46 Kbps	09 Feb 2021, 01:58PM	a few seconds	Device, Interface	QoS Class Default Drop	Third Party Integrations
▲ Critical	SE-LiveWire-NY had 68.00 ms network delay for the application youtube	09 Feb 2021, 01:58PM	a few seconds	Application	Network Delay Per Connection	
▲ Critical	SE-LiveWire-NY had 80.00 ms network delay for the application ms-office-web-apps	09 Feb 2021, 01:58PM	a few seconds	Application	Network Delay Per Connection	
▲ Critical	SE-LiveWire-NY had 104.00 ms network delay for the application outlook-web-service	09 Feb 2021, 01:58PM	a few seconds	Application	Network Delay Per Connection	
▲ Critical	RTR-DC-CORE had 80.00 ms network delay for the application ms-office-web-apps	09 Feb 2021, 01:58PM	a few seconds	Application	Network Delay Per Connection	
▲ Critical	RTR-DC-CORE had 68.00 ms network delay for the application youtube	09 Feb 2021, 01:58PM	a few seconds	Application	Network Delay Per Connection	
▲ Critical	RTR-DC-MPLS running application VoIP had 4695.83 ms of jitter for traffic with a DSCP value of 0 ...	09 Feb 2021, 01:57PM	a minute	Application	Media Jitter Max	
▲ Critical	AppleFastLane-4331 running application kaseya had critical traffic with delay 77.83 ms	09 Feb 2021, 01:57PM	a minute	Application	Critical Traffic Response Time	
▲ Critical	RTR_Birmingham1.liveaction.com QoS Class Default Drop Rate was 60.31 Kbps	09 Feb 2021, 01:57PM	a minute	Device, Interface	QoS Class Default Drop	
▲ Critical	SE-LiveWire-NY had 62.00 ms network delay for the application http	09 Feb 2021, 01:57PM	a minute	Application	Network Delay Per Connection	
▲ Critical	SE-LiveWire-NY had 64.00 ms network delay for the application skype	09 Feb 2021, 01:57PM	a minute	Application	Network Delay Per Connection	

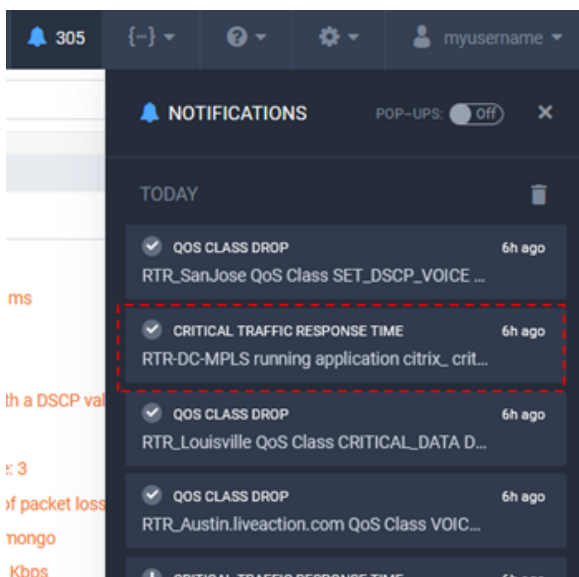
All rows 999

Clicking on the status bar's **Notification** button will open the *Notifications* sidebar.





Alerts that have been configured for Web UI sharing (a form of notification setting) will appear in this list. Clicking a specific event will pivot to its Alert details.



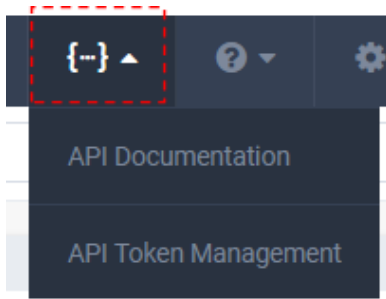
The screenshot shows the LiveAction Alerts interface. At the top, there's a bar chart labeled 'Active' with a red-to-yellow gradient. Below it is a table of alerts. The table has columns for severity (Critical, Warning), site (e.g., Seattle, New York - DC), service (e.g., RTR, RTR-DC-CORE), description (e.g., 'citrix\_ had critical traffic with delay 281.33 ms'), and status (Active, Resolved). A right-hand panel shows details for a selected alert, including 'Status & Time', 'Source Info', and 'Description'.

The Notifications *Pop-Ups* switch will ensure new notification events are visible as they are triggered.

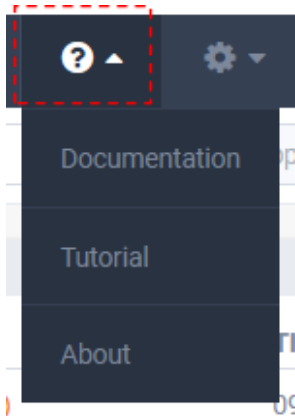
This block illustrates the notification workflow. It starts with a 'NOTIFICATIONS' bar containing a bell icon and a 'POP-UPS: Off' toggle switch. Below this is the main status bar showing a notification count of 302. A 'HIDE ALL POP-UPS' button is shown, which triggers a detailed notification pop-up. The pop-up displays a critical alert: 'RTR-DC-MPLS running application citrix\_ had critical traffic with delay 149.06 ms'. Below the pop-up is a table of notification events with columns for the message and 'TIME OPENED'.

Notification Message	TIME OPENED
with a DSCP value of 0 (BE)	09 Feb 2021, 08:21 AM
	09 Feb 2021, 08:20 AM
	09 Feb 2021, 08:20 AM
s of packet loss for traffic with a DSCP value ...	09 Feb 2021, 08:20 AM
	09 Feb 2021, 08:20 AM
.33 ms	09 Feb 2021. 08:20 AM

The Status bar's API menu icon provides navigation to API documentation and API Token Management. This topic is out of scope of this document. For more information, please go to <https://docs.liveaction.com>.



The Status bar's help icon provides access to *Documentation*, *Tutorial*, and *About* page.



The *About* page shows LiveNX version, license, and server time information. It also provides access to configure http proxy settings.

About

**INFORMATION**

APPLICATION VERSION

Server Version :	21.1.0-20210127-73f540b
Web Version :	21.1.0-20210127-0d0696e6d3+b121

SERVER

Server Time :	Feb 09, 2021 13:29:03 UTC (GMT+00:00)
---------------	---------------------------------------

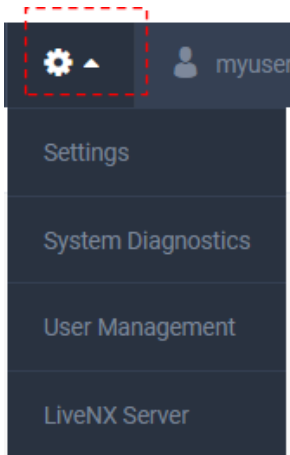
HTTP PROXY

Configure Proxy

LIVENX LICENSE

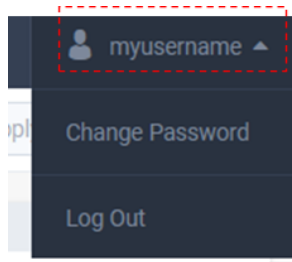
License number :	LiveAction-Web-Clark
License issue date :	Jul 07, 2015 20:00:00 EDT (GMT-04:00)
License expires :	Jul 07, 2025 02:59:59 EDT (GMT-04:00)
Maintenance expiration date :	No maintenance
Compatible version :	21.1
License type :	Permanent
License mode :	Legacy

Selecting the Settings icon from the status bar provides access to *Settings*, *System Diagnostics*, *User Management*, and *LiveNX Server* pages. These are outside the scope of this document. Please see the LiveNX Admin Guide for more information, <https://docs.liveaction.com>.



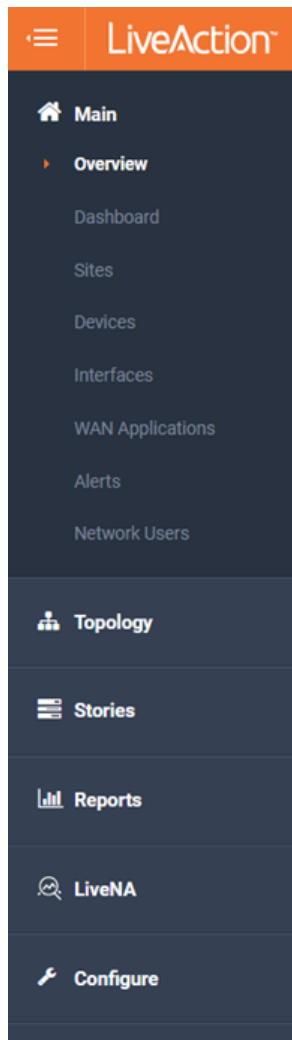
Selecting the username from the status bar will allow the current user to change their password (if using a local account) or log out of LiveNX.





## Navigation Bar

Most of the tasks that you will perform in LiveNX are accessible from the Navigation Bar. The Navigation Bar is available by clicking the menu icon at the top left of the Status Bar. The remaining chapters of this *User Guide* provide details on how to perform the tasks available from the Navigation Bar.



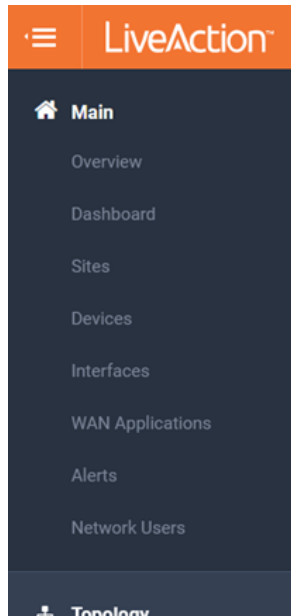
## Main

### In this chapter:

<i>Main</i> .....	12
<i>Overview</i> .....	12
<i>Dashboard</i> .....	14
<i>Sites</i> .....	25
<i>Devices</i> .....	33
<i>Interfaces</i> .....	42
<i>WAN Applications</i> .....	47
<i>Alerts</i> .....	49
<i>Network Users</i> .....	56

## Main

The LiveNX *Main* menu option provides quick navigation and exploration of the health and performance of the network. It also includes access to the LiveNX *Dashboard* and *Alerts*.

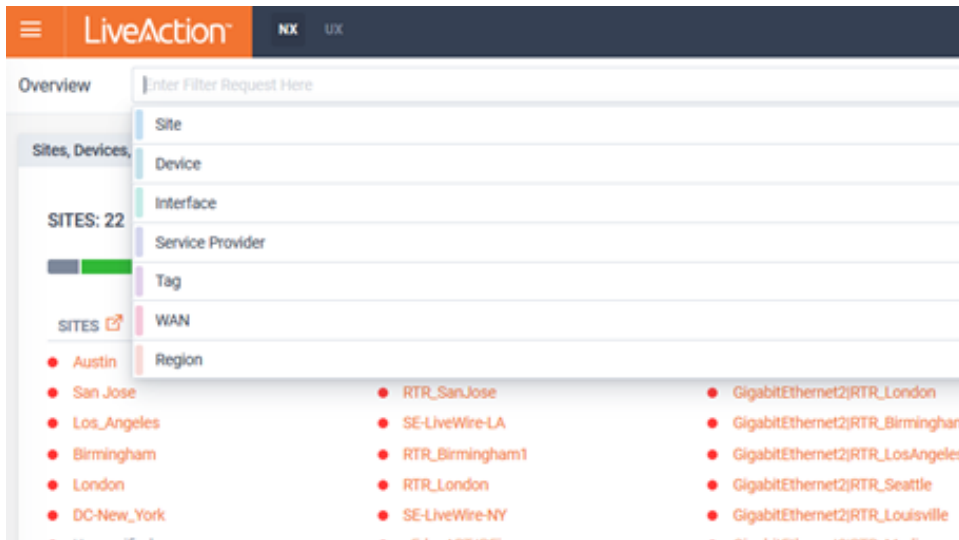


## Overview

The LiveNX *Overview* page provides a situational overview of the health of the network. It includes a breakdown of *Sites*, *Devices*, and *Interfaces*. These are ordered based on worst status severity. It also includes a list of the latest *Alerts*.

SITES: 22	DEVICES: 56	INTERFACES: 185	Active Alerts
<ul style="list-style-type: none"> <li>Austin</li> <li>San Jose</li> <li>Los Angeles</li> <li>Birmingham</li> <li>London</li> <li>DC New York</li> <li>Unspecified</li> <li>Hurricane Electric</li> <li>Indianapolis</li> <li>Seattle</li> <li>Louisville</li> <li>Sydney</li> <li>Tokyo</li> <li>Internet</li> <li>Madison</li> <li>Impairment</li> <li>AWS_Oregon</li> <li>AzureWest</li> <li>Florida</li> <li>Sunnyvale</li> </ul>	<ul style="list-style-type: none"> <li>SE-LiveWire-Aus</li> <li>RTR_SanJose</li> <li>SE-LiveWire-LA</li> <li>RTR_Birmingham1</li> <li>RTR_London</li> <li>SE-LiveWire-NY</li> <li>eEdgeARTIPFix</li> <li>CS-C3650-23-36</li> <li>RTR_LosAngeles</li> <li>RTR_Indianapolis</li> <li>RTR-DC-MPLS</li> <li>RTR_Seattle</li> <li>RTR_Louisville</li> <li>CS-C3650-23-31</li> <li>IWAN-B1_Sydney</li> <li>IWAN-B1_NET</li> <li>SE-F5-VE-LTM</li> <li>RTR_Madison</li> <li>RTR-DC-CORE</li> <li>CS-2960-23-22</li> </ul>	<ul style="list-style-type: none"> <li>GigabitEthernet2/RTR_SanJose</li> <li>GigabitEthernet2/RTR_London</li> <li>GigabitEthernet2/RTR_Birmingham1</li> <li>GigabitEthernet2/RTR_LosAngeles</li> <li>GigabitEthernet2/RTR_Seattle</li> <li>GigabitEthernet2/RTR_Louisville</li> <li>Gigamon-AM6940MTU</li> <li>01TEST_Lubrizol_Velo</li> <li>11TEST_Lubrizol_Velo</li> <li>11TEST_Niagara_Netflow</li> <li>default/AzureCMUSWest</li> <li>eth0/AppleasLine-3560</li> <li>eth0/AppleasLine-4331</li> <li>eth0/fortGate-Firewall</li> <li>eth0/Gigamon-GT7EncrystIPFix</li> <li>ETH0/MonIPFix_s20</li> <li>eth0/IPv6FlowDevice</li> <li>eth0/LiveAgent360Concentrator</li> <li>eth0/LiveAgentConcentrator</li> </ul>	<ul style="list-style-type: none"> <li>Voice traffic for RTR-DC-MPLS running application sip is not marked as DSCP EF.</li> <li>Voice traffic for RTR_LosAngeles.liveaction.com running application sip is not marked as DSCP EF.</li> <li>Voice traffic for RTR_Seattle running application unclassified is not marked as DSCP EF.</li> <li>Voice traffic for SE-LiveWire-Aus running application VoIP is not marked as DSCP EF.</li> <li>RTR_LosAngeles.liveaction.com IP SLA Voice/rtter total errors is greater than threshold value: 3</li> <li>GigabitEthernet2 on RTR_Seattle had a drop rate of 15.48 pps in the Output direction.</li> <li>RTR_SanJose QoS Class Default Drop Rate was 44.12 kbps</li> <li>RTR_Madison IP SLA Voice/rtter total errors is greater than threshold value: 3</li> <li>Voice traffic for RTR_Birmingham1.liveaction.com running application VoIP is not marked as DSCP EF.</li> <li>RTR_Seattle running application Citrix had critical traffic with delay 450.06 ms</li> <li>SE-LiveWire-LA running application rtp-audio had 84.51 % of packet loss for traffic with a DSCP value of 46 (EF)</li> <li>Voice traffic for RTR_Madison running application VoIP is not marked as DSCP EF.</li> <li>RTR_Birmingham1.liveaction.com running application VoIP had 55.77 % of packet loss for traffic with a DSCP value of ...</li> <li>SE-LiveWire-Aus CPU utilization is above threshold</li> <li>Interface GigabitEthernet1/0/18 on CS-C3650-23-36.Liveaction could not be reached.</li> <li>Interface Vlan114 on CS-C3650-23-36.Liveaction could not be reached.</li> <li>Interface GigabitEthernet1/0/13 on CS-C3650-23-36.Liveaction could not be reached.</li> <li>Interface GigabitEthernet1/0/21 on CS-C3650-23-36.Liveaction could not be reached.</li> <li>Interface GigabitEthernet1/0/21 on CS-C3650-23-36.Liveaction could not be reached.</li> <li>Interface GigabitEthernet1/0/4 on CS-C3650-23-36.Liveaction could not be reached.</li> <li>Interface GigabitEthernet1/0/4 on CS-C3650-23-36.Liveaction could not be reached.</li> <li>Interface Vlan1 on CS-C3650-23-36.Liveaction could not be reached.</li> <li>Interface GigabitEthernet1/0/7 on CS-C3650-23-36.Liveaction could not be reached.</li> <li>Interface GigabitEthernet1/0/10 on CS-C3650-23-36.Liveaction could not be reached.</li> </ul>

Filters can be applied to focus on the specific entities of interest:

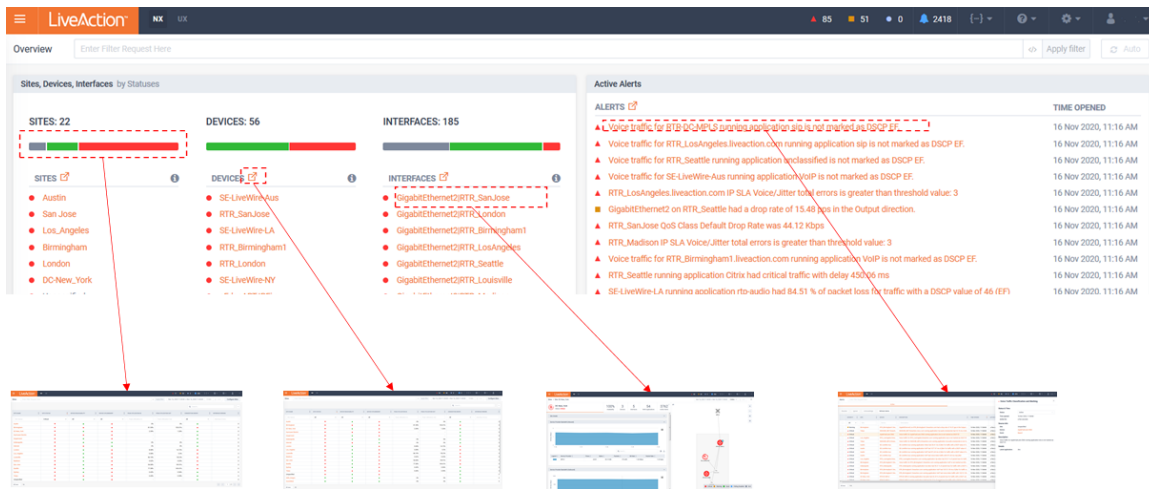


The page can optionally be auto-refreshed by toggling the **Auto** button in the top right of the page.

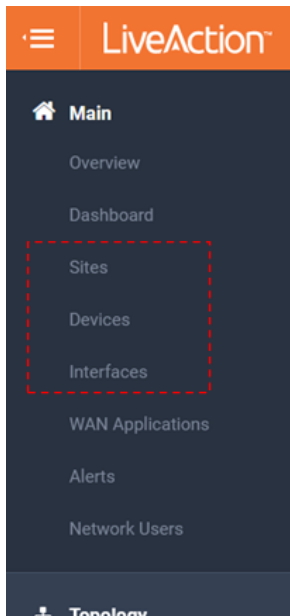


The *Overview* page allows for quick access to more data about the link selected. By selecting different areas of the *Sites*, *Devices*, *Interfaces* widget, drill-down to a corresponding page will provide context aware data.

Clicking on an alert will drill-down to the alert's details.

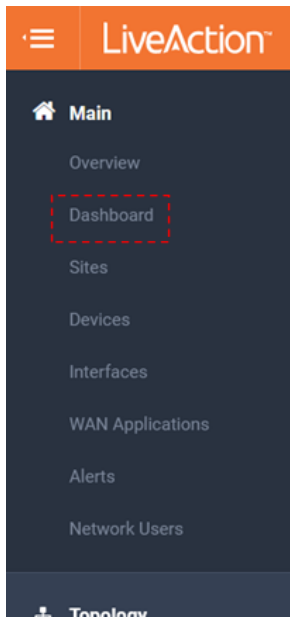


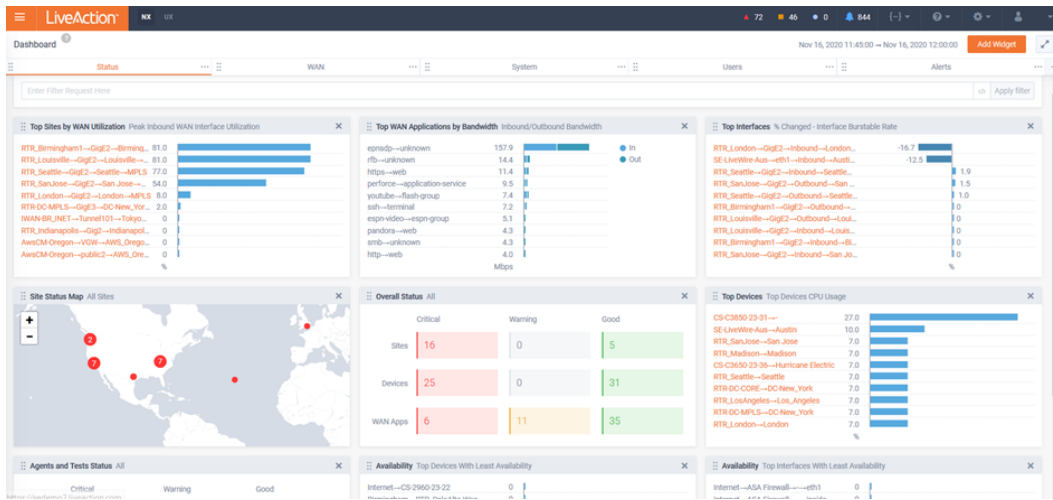
Manual exploration of *Sites*, *Devices*, and *Interfaces* can be done from the *Main* menu navigation bar.



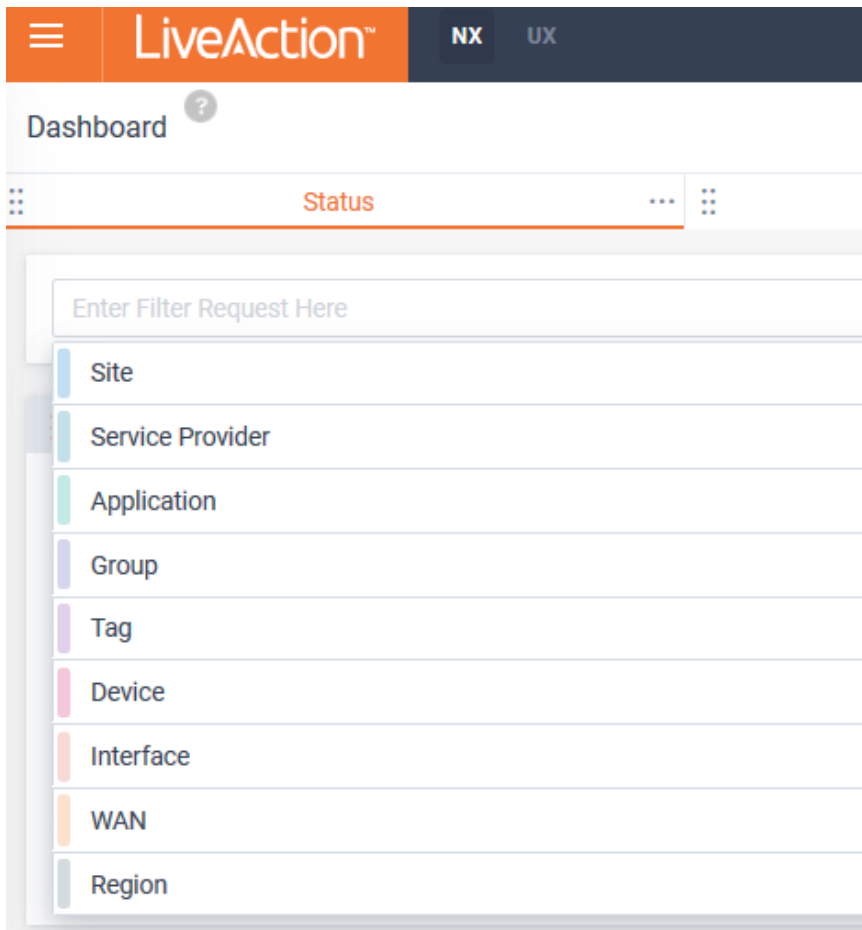
## Dashboard

The LiveNX *Dashboard* provides quick navigation and exploration of the health and performance of the network and application running on it. Dashboards are a collection of widgets that are can be customized and organized as desired. Each user can have up to 12 tabs of dashboards.

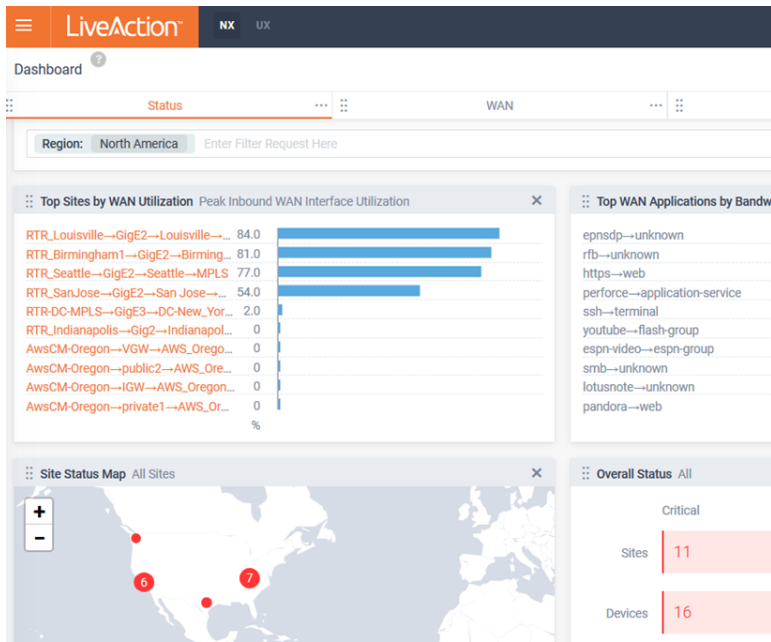




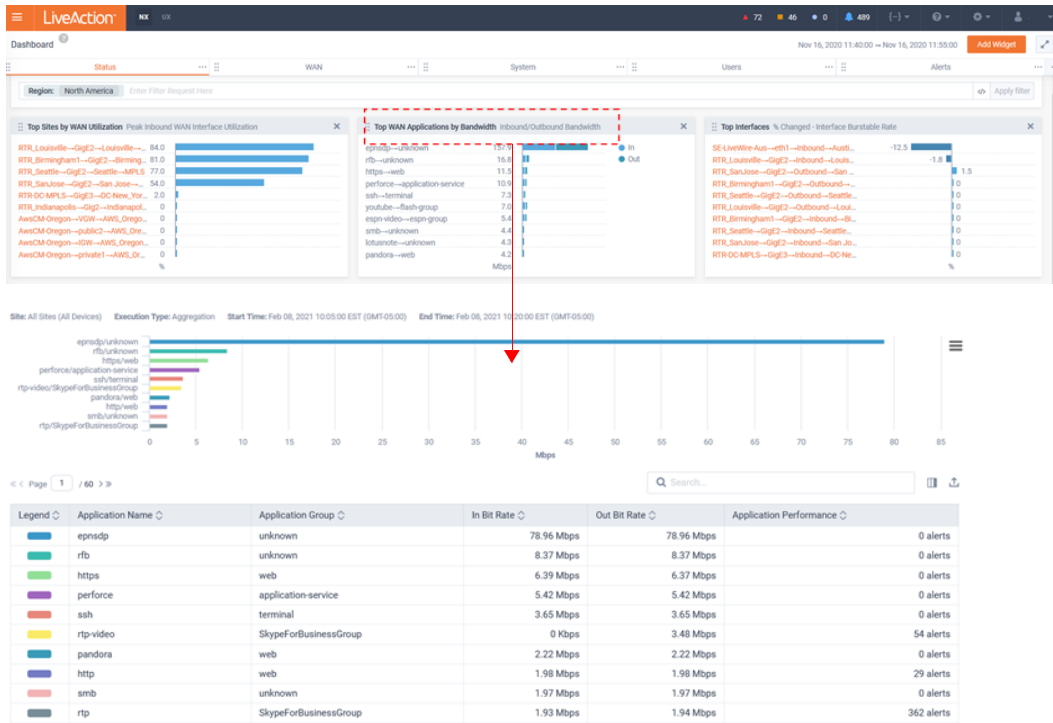
Filters can be applied to focus on the specific data set of interest:

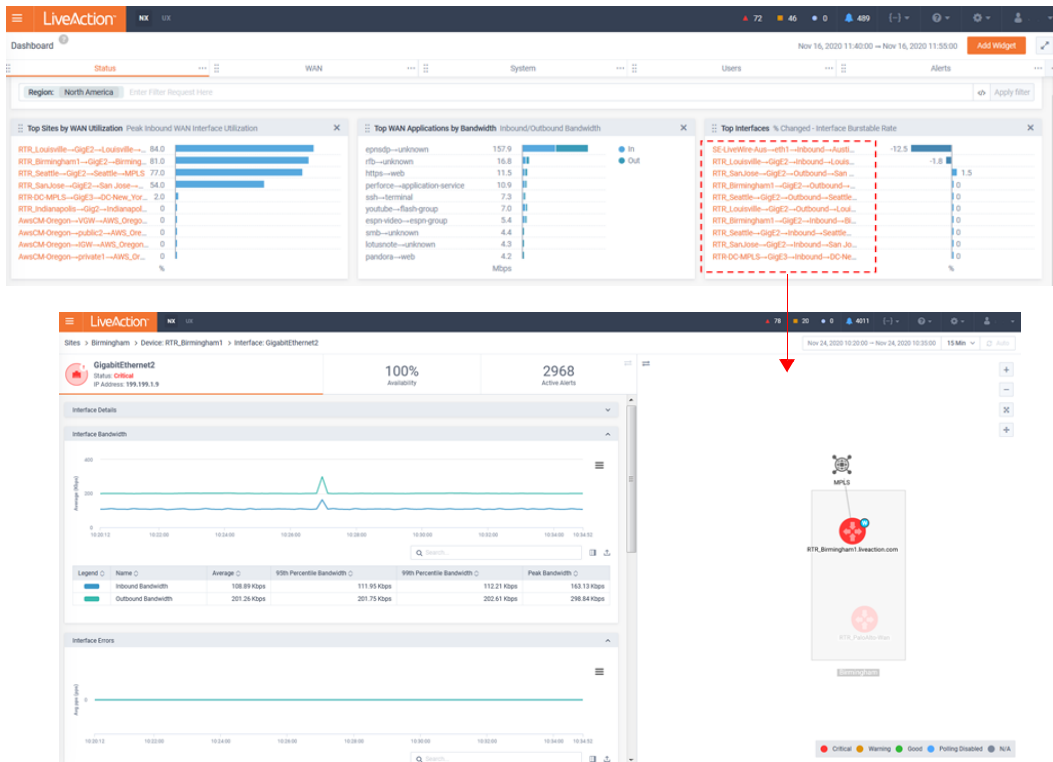


In this example, a filter of *Region: North America* has been applied. All widgets on this *Dashboard* tab will only present data relevant to the devices in this region.

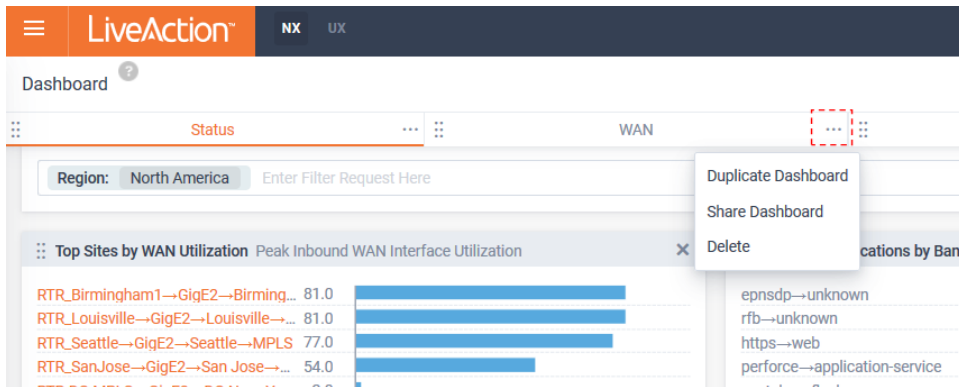


Many widgets are interactive. By clicking on a widget's header or data, many will drill-down to a corresponding historical report or *Entity* page for data:

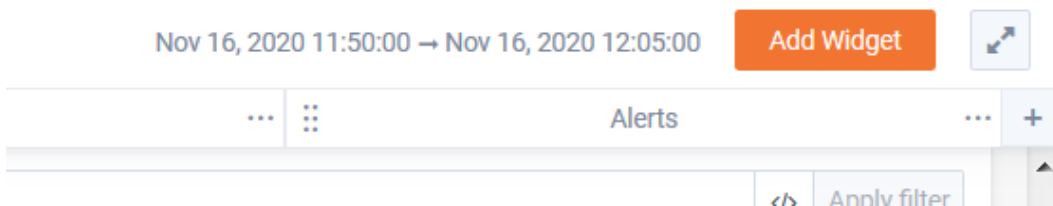




By Selecting the *Dashboard* tab's menu, the tab can be duplicated, shared or deleted.



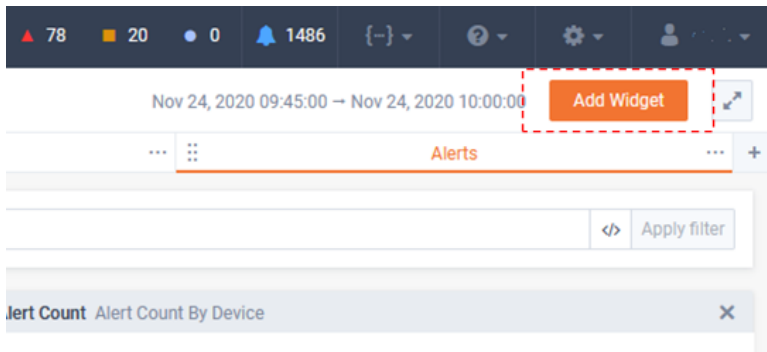
New widgets can be added to a *Dashboard* tab by clicking the **Add Widget** button at the top right of the page.



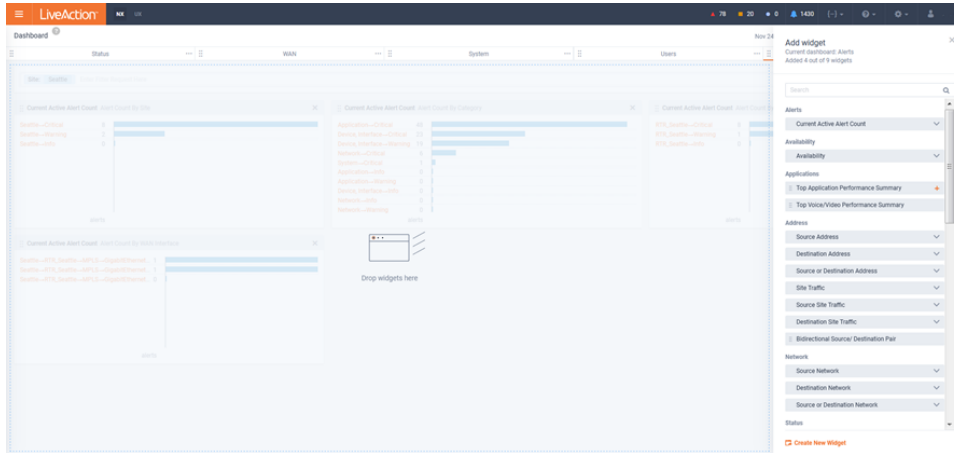
In the following example a default widget will be added to the *Dashboard* tab:

1. Click the **Add Widget** button.

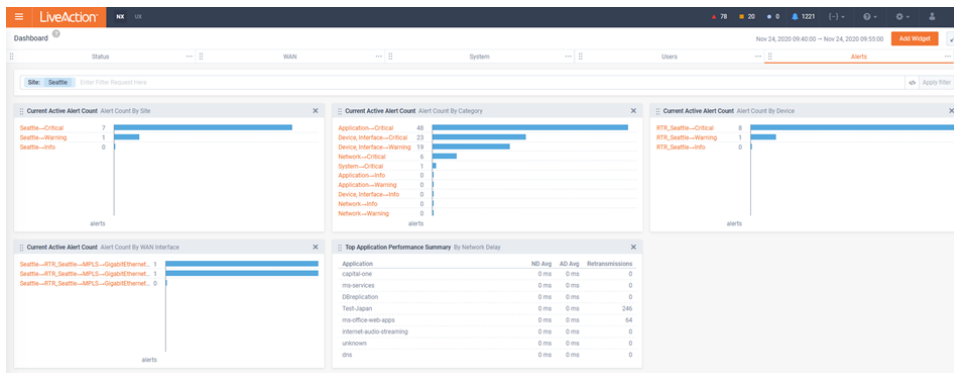




2. Click the *Add* icon next to the widget of interest.

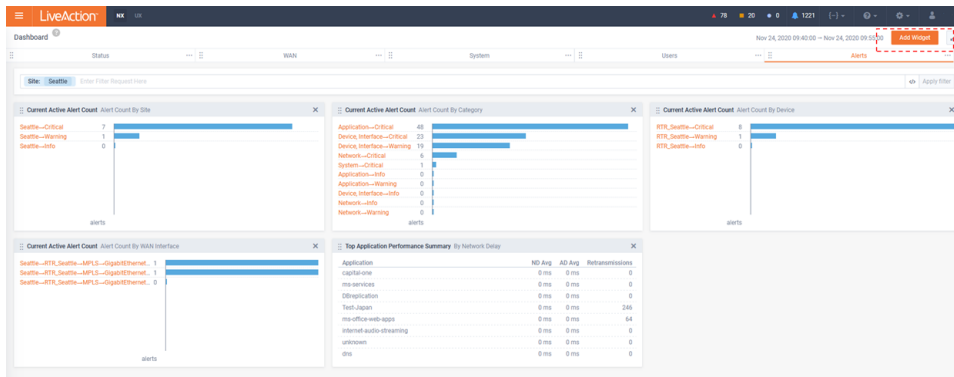


3. The new widget will appear on the *Dashboard* tab.

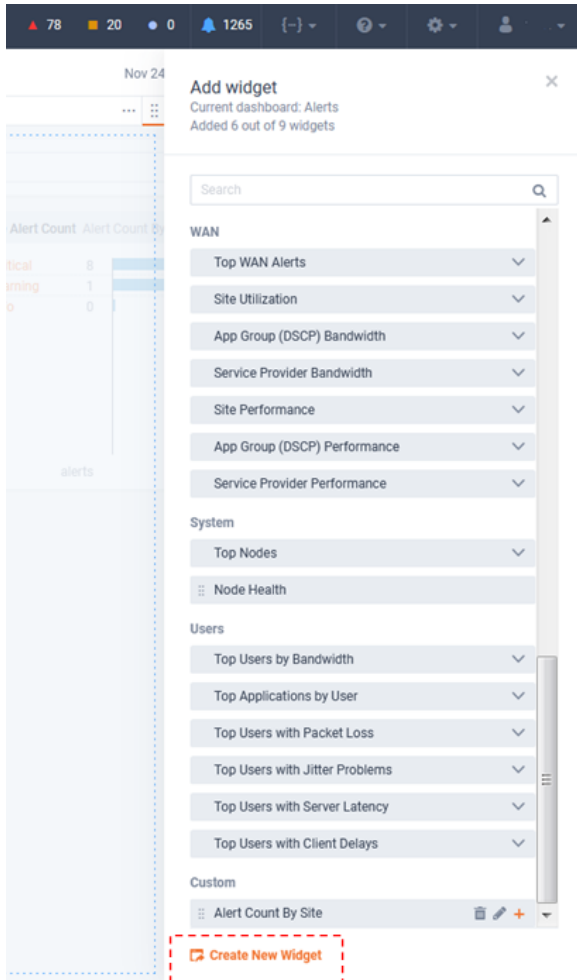


In the following example a new custom widget will be created and added to the *Dashboard* tab.

1. Click the **Add Widget** button.



2. Click *Create New Widget* link at that bottom of the *Add Widget* list.



3. Follow the steps to select the underlying report that will be the basis of the widget, its parameters, and create widget.

### CREATE CUSTOM WIDGET

1 Report parameters
2 Widget parameters

**Report Type**  
Application (Flow)

**Time Zone**  
(GMT-05:00) America/New York  DST

**Devices**  
All WAN Devices

**Interfaces**  
All WAN Interfaces

**Flex Search**  
Ex: site=Honolulu & wan & flow.app=http

**Direction**  
Outbound

**Flow Type**  
Basic Flow

**Sort By**  
Bit Rate

**Business Hours**  
All Hours

**Bin Duration**  
Auto

**Raw Flow Data**  
Due to the options selected, this report will utilize the Raw Flow datastore (slower).

Cancel
Next Step

### CREATE CUSTOM WIDGET

1 Report parameters
2 Widget parameters

**Report summary:**

**Device Serial:** All WAN Devices  
**Direction:** Outbound  
**Sort By:** Bit Rate  
**Bin Duration:** Auto  
**Enable DST:** true

**Interface:** All WAN Interfaces  
**Flow Type:** Basic Flow  
**Business Hours:** All Hours  
**Time Zone:** (GMT-05:00) America/New York

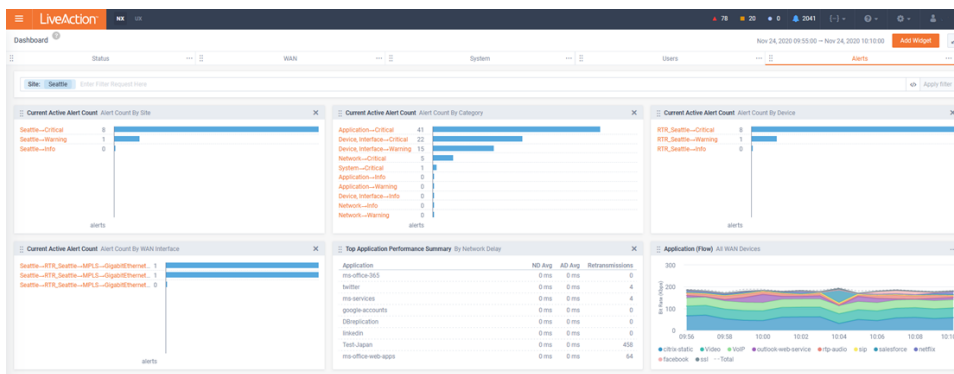
**Widget title**  
Application (Flow)

**Widget subtitle**  
All WAN Devices

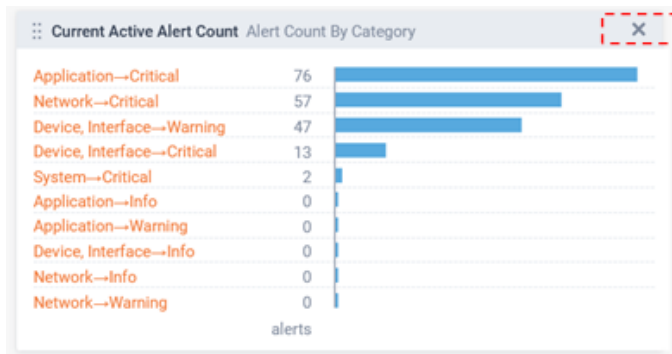
**Save to a Dashboard**  
Alerts

**View as**  
Aggregation

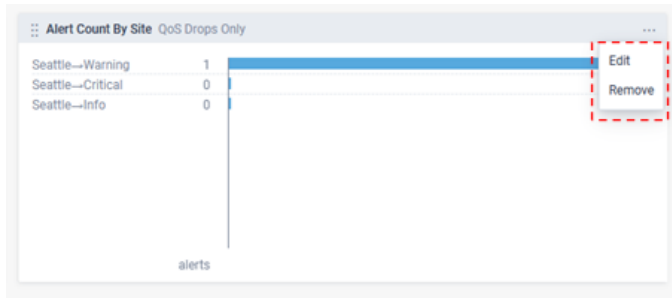
Cancel
Previous Step
Create Widget



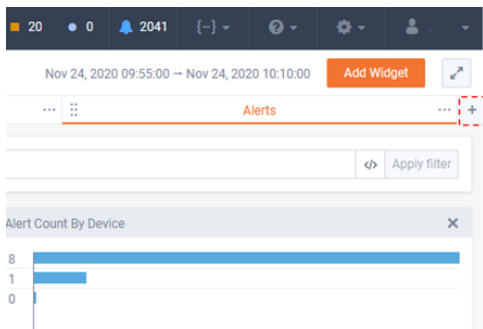
Default widgets can be deleted by clicking the close icon at the top-right of the widget.



Custom widgets can be edited or removed clicking the menu icon at the top-right of the widget.

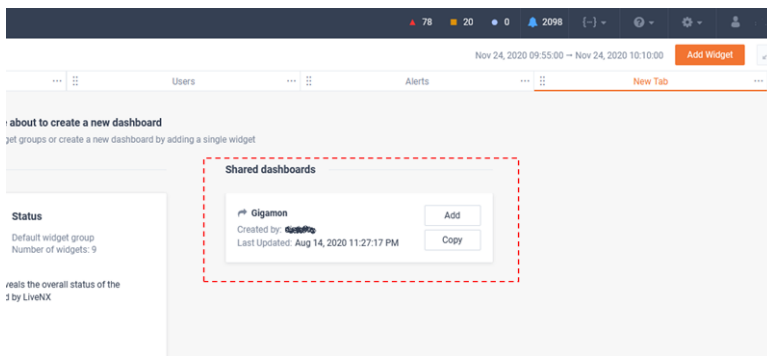


To add a new *Dashboard* tab, click the add icon at the top right of the page.

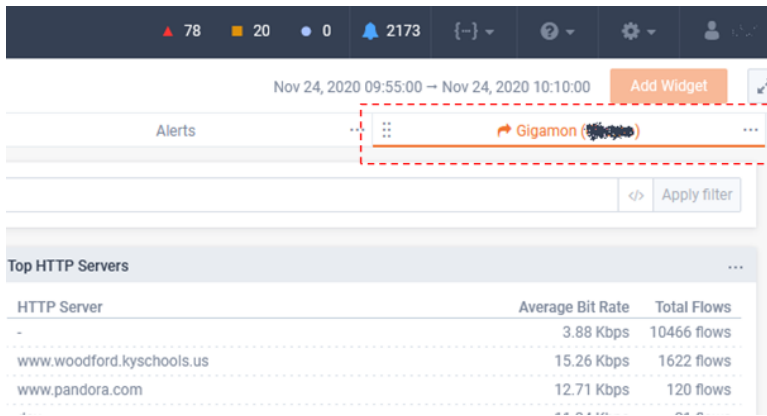


A new tab will appear. Select either a *Default* template or a *Shared Dashboard*. If *Shared Dashboard* is selected, it can either be added or copied.

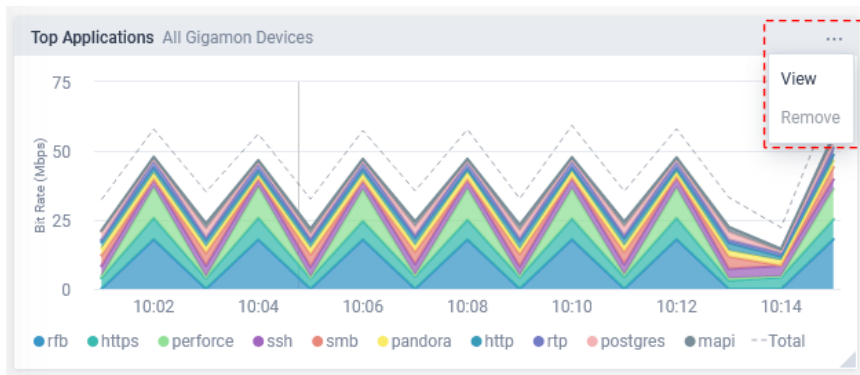
- Added - the original owner will retain ownership. They will continue to be able to modify the dashboard and its widgets. The current user cannot modify the shared dashboard.
- Copied - A copy of the shared dashboard will be used as a starting template and the current user will have full ownership of the dashboard and its widgets.



Below is an example of a shared dashboard.



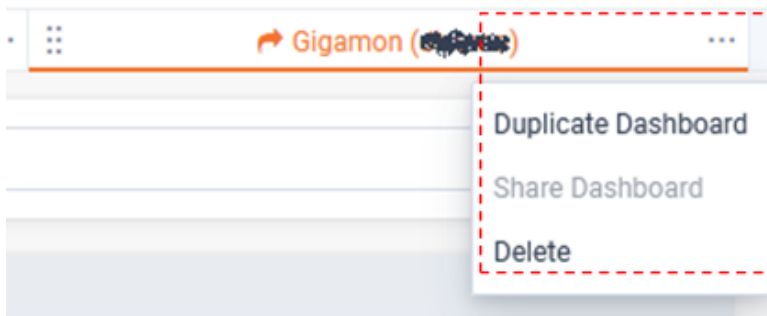
The widget options are limited to just *View*.



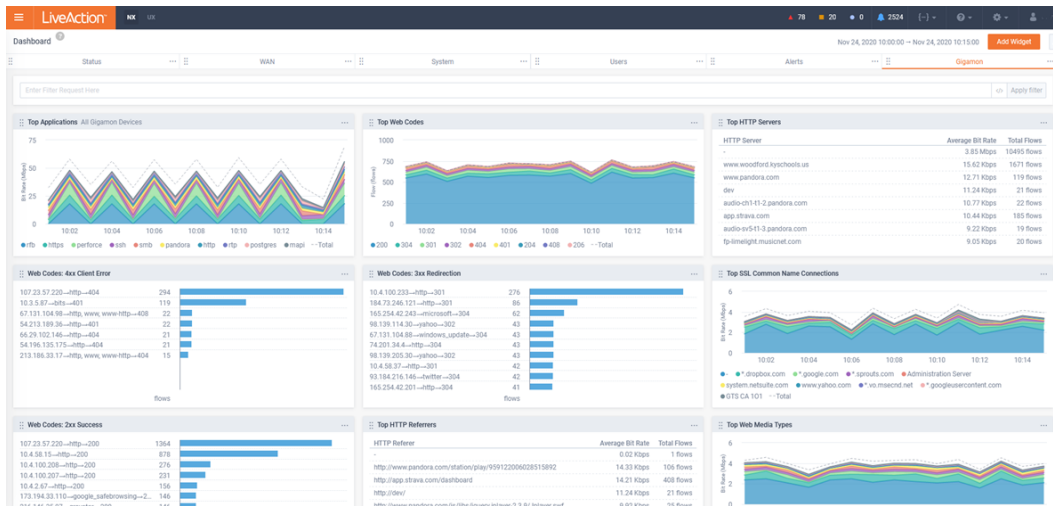
**WIDGET PARAMETERS** ✕

<b>Device:</b> All WAN Devices	<b>Interface:</b> All WAN Interfaces
<b>Direction:</b> Outbound	<b>Flow Type:</b> Basic Flow
<b>Execution Type:</b> Time Series	<b>Sort By:</b> Bit Rate
<b>Flex Search:</b> tag = Gigamon	<b>Business Hours:</b> All Hours
<b>Bin Duration:</b> Auto	<b>Time zone:</b> (GMT-05:00) America/New York
<b>DST:</b> Enabled	

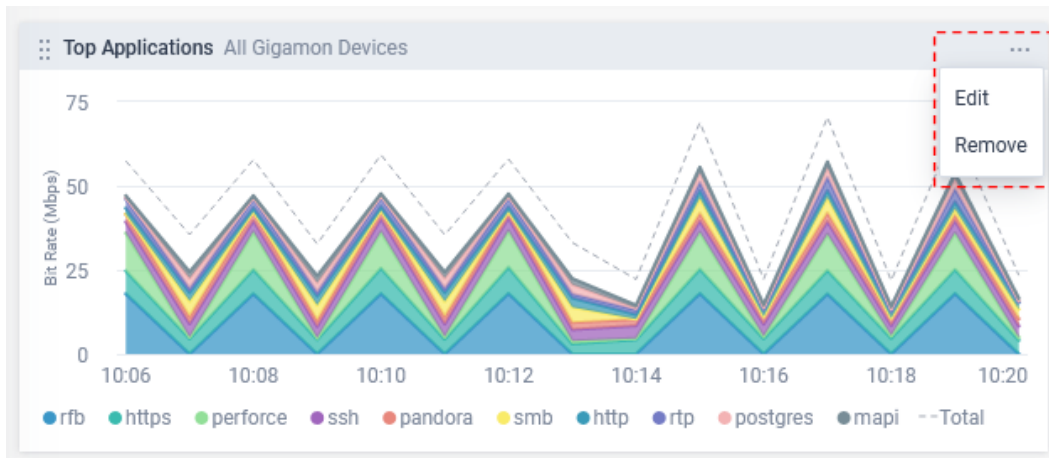
The shared dashboard can only be duplicated (copied) or deleted.



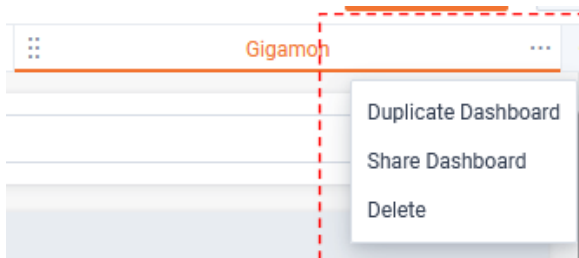
Below is the same dashboard, but in this example, it has been copied. The current user has full control over this *Dashboard* tab. Any changes have no effect on the original shard dashboard from the other user.



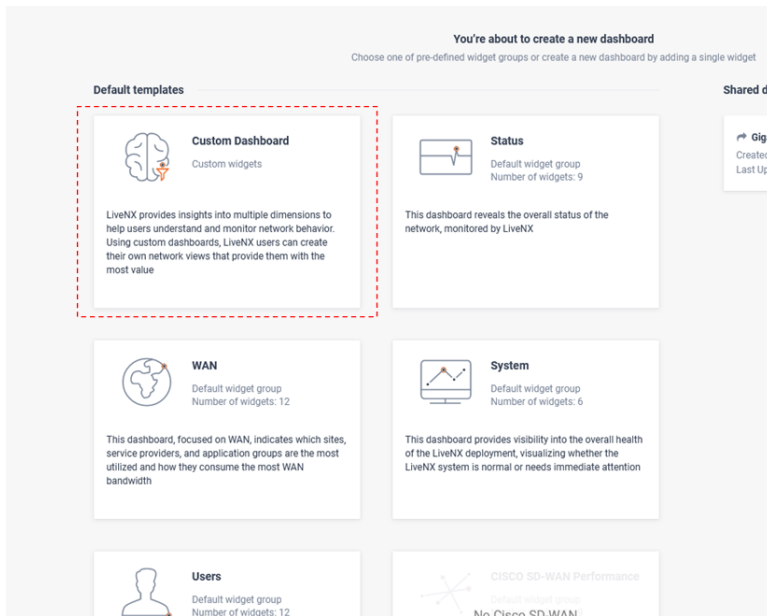
The widgets can be edited by the current user.



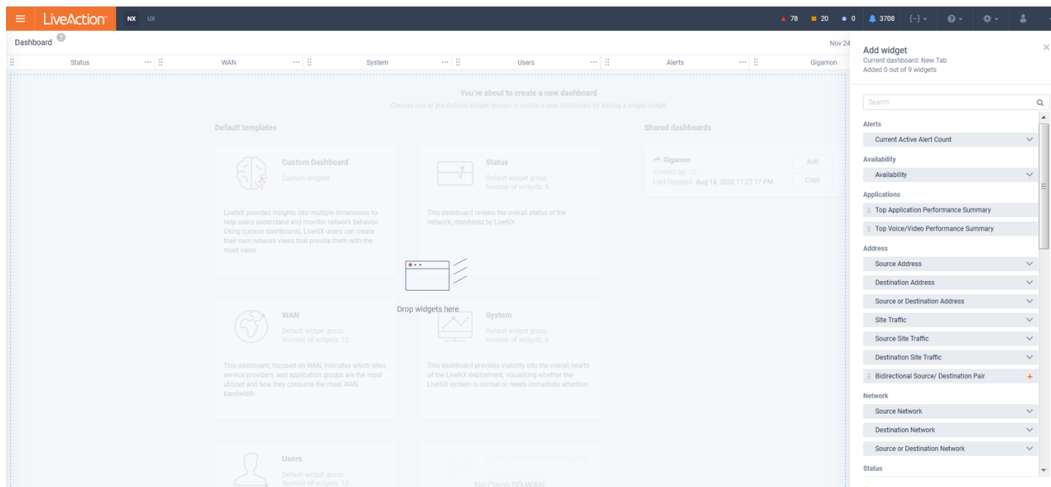
The dashboard can be duplicated, shared, or deleted.



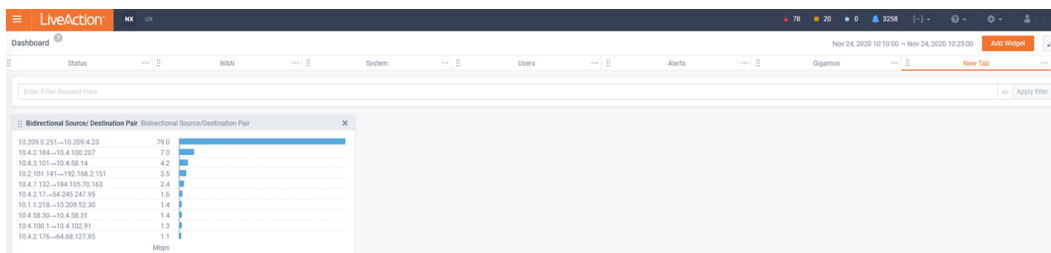
To create a new *Dashboard* tab from scratch, select *Custom Dashboard* when adding a new dashboard tab.



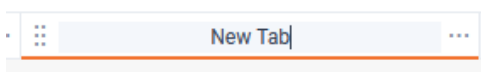
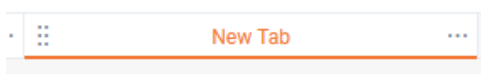
Select a default or custom widget.

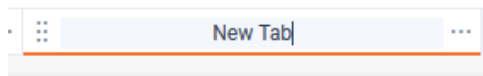


The new dashboard will appear with the new widget.

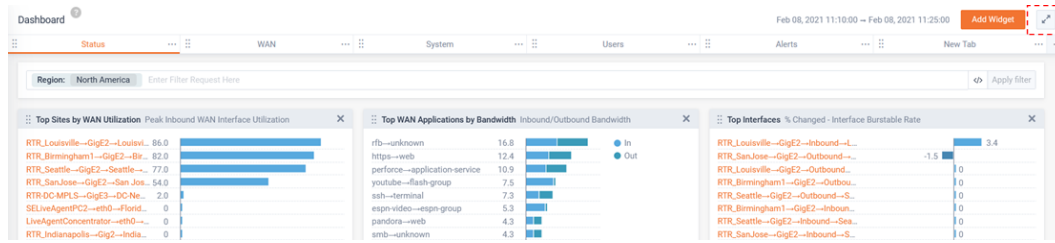


The name of the new dashboard will be *New Tab*. To rename the tab, click the tab's name and edit.





Dashboards can be presented in a dark background format for presenting on a wallboard.



## Sites

The *Sites* navigation page presents a list of all sites in LiveNX and highlights a summary of their performance statuses.

Clicking on a site will drill-down to the site's detail page.

SITE NAME	SITE STATUS	DEVICE REACHABILITY	DEVICE CPU/MEMORY	PEAK UTILIZATION IN	PEAK UTILIZATION OUT	CONGESTION DROPS	INTERFACE ERRORS
Austin	●	●	●	0%	0%	0%	0
Birmingham	●	●	●	82.15%	150.73%	1.27%	0
DC-New_York	●	●	●	2.4%	-	-	0
Hurricane Electric	●	●	●	-	-	-	0
Equipment	●	●	●	0%	0%	-	0
Indianapolis	●	●	●	0%	0%	-	0
Internet	●	●	●	0%	0%	-	0
London	●	●	●	8.01%	14.73%	-	0
Los_Angeles	●	●	●	0.08%	0.3%	-	0
Louisville	●	●	●	85.17%	151.3%	-	0
Madison	●	●	●	0.02%	0.03%	-	0
San_Jose	●	●	●	54.61%	100.71%	-	0
Seattle	●	●	●	76.89%	148.73%	-	0
Sydney	●	●	●	0.43%	0.56%	-	0
Tokyo	●	●	●	0.45%	0.59%	-	0
Unspecified	●	●	●	-	-	-	0
AWS_Oregon	●	●	●	-	-	-	0
AzureWest	●	●	●	-	-	-	0
Florida	●	●	●	0%	0%	-	0
Summit	●	●	●	0%	0%	-	0
Walnut_Creek	●	●	●	0%	0%	-	0
Oregon	●	●	●	0%	0%	-	0

Clicking on a status bubble will provide more details and optional drill-down for further exploration.



SITE NAME	SITE STATUS	DEVICE REACHABILITY	DEVICE CPU/MEMORY	PEAK UTILIZATION IN
<input type="text" value="Site Name"/>	<input type="button" value="All"/>	<input type="button" value="All"/>	<input type="button" value="All"/>	<input type="text" value="Peak Utilization In"/>
Austin				0%
Birmingham				81.33%
DC-New_York				2.39%
Indianapolis				0%
Internet				0%
Los_Angeles				0.08%
Louisville				90.78%
Seattle	●	●	●	76.86%
Unspecified	●	●	●	0%
San Jose	●	●	●	53.55%
AWS_Oregon	●	●	●	

Site: Austin

Active Alerts Impacting Status: 3

▲ Critical:

- SE-LiveWire-Aus running application Video had 32.36 ms of jitter for traffic with a DSCP value of 34 (AF41)
- SE-LiveWire-Aus running application VoIP had 2843.99 ms of jitter for traffic with a DSCP value of 0 (BE)
- SE-LiveWire-Aus running application VoIP had 10167.90 ms of jitter for traffic with a DSCP value of 46 (EF)

Active Alerts

Alert History

Filters can be applied to focus on the specific entities of interest:

The page can optionally be auto-refreshed by toggling the **Auto** button in the top right of the page.



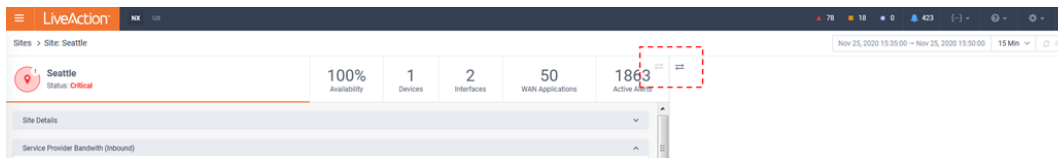
The Site detail page has multiple tabs to quickly understand different dimensions of the entity. There is also a simple topology map to provide context of the entity.

Historic data can be explored on the entity's tabs.

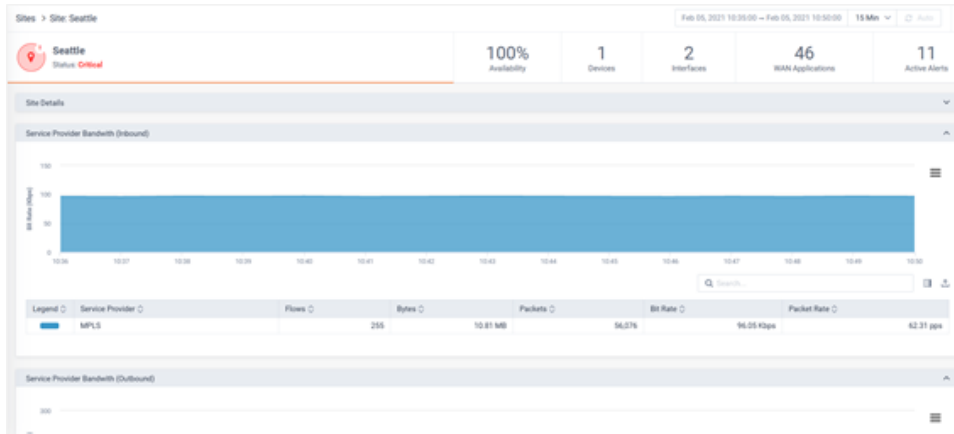
The page can optionally be auto-refreshed by toggling the **Auto** button in the top right of the page.



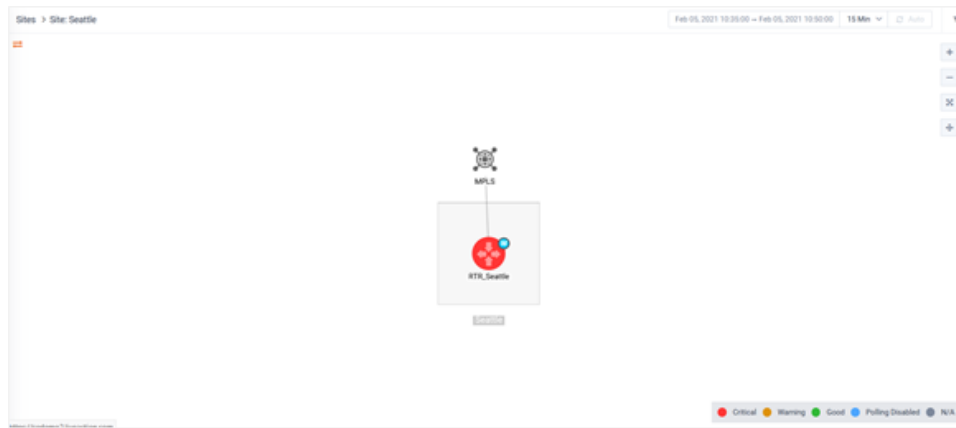
The page view can be modified to allow the tabs or topology to be full page.



Full page *Tab* view:



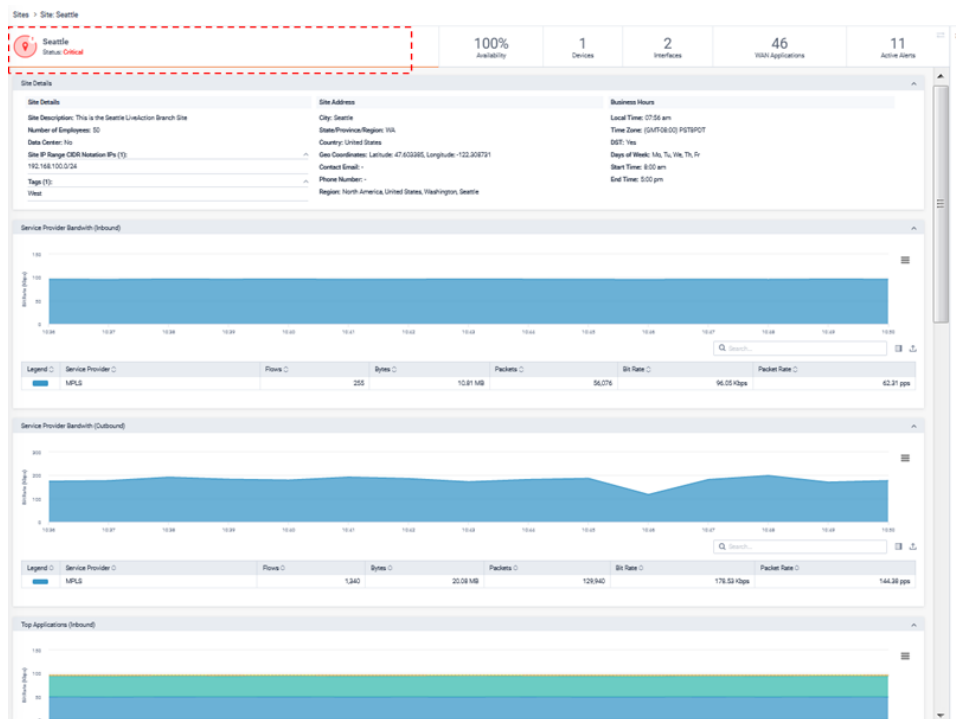
Full page *Topology* view:



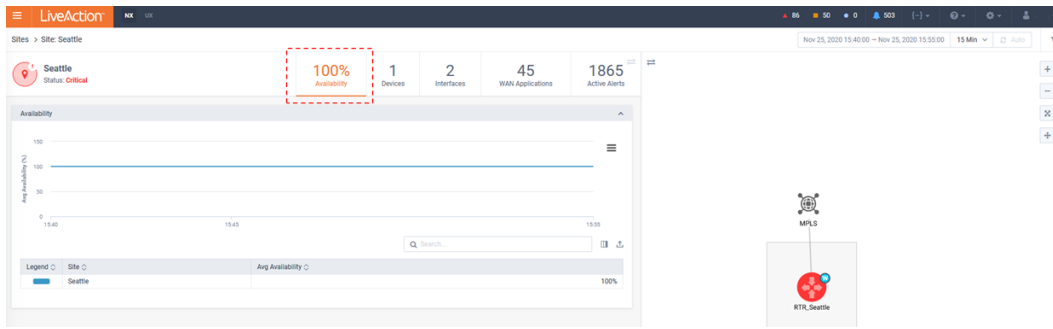
The status tab of the Site page provides a curated list of reports for quick understanding of the Sites' status.

These reports include:

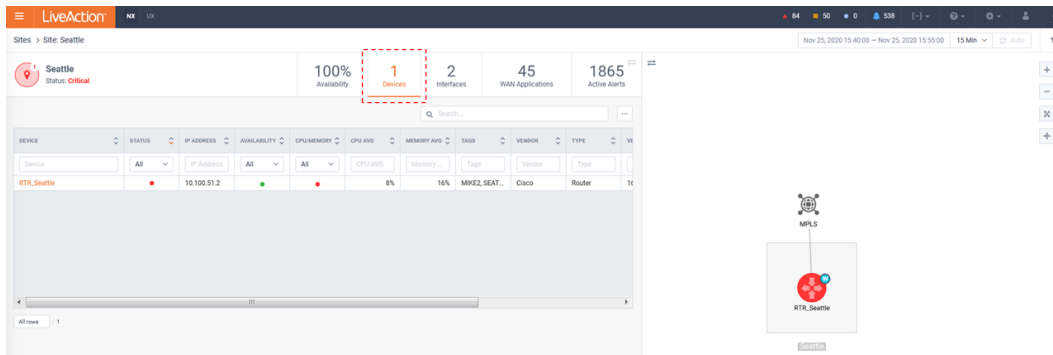
- Site Details
- Service Provide Bandwidth (Inbound)
- Service Provide Bandwidth (Outbound)
- Top Application(Inbound)
- Top Application(Outbound)
- Top DSCP(Inbound)
- Top DSCP(Outbound)
- Top Conversation(Inbound)
- Top Conversation(Outbound):



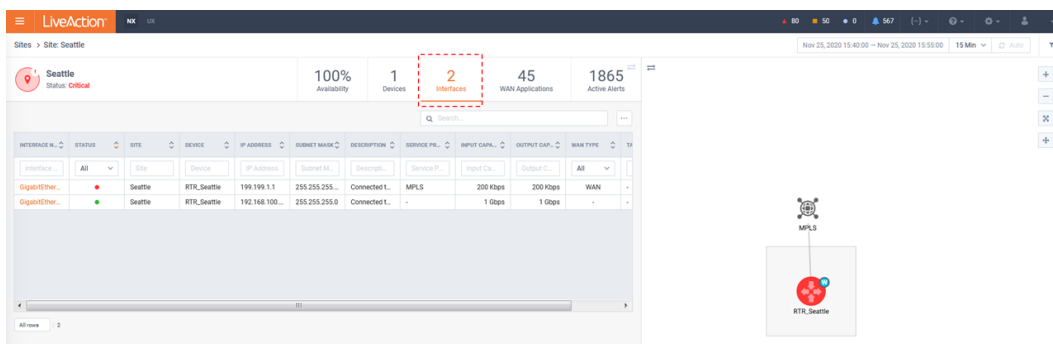
The *Availability* tab of the Site page provides the Sites *Availability* report.



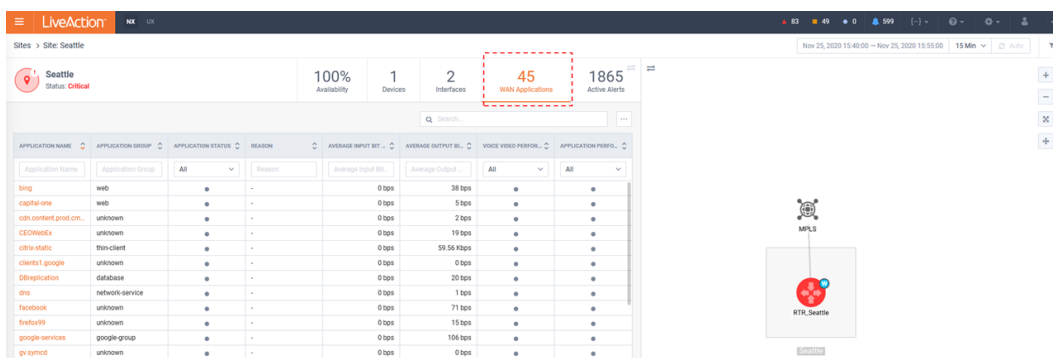
The *Devices* tab of the Site page provides a list of all member devices in the Site. Clicking on a device's link will drill-down into its details.



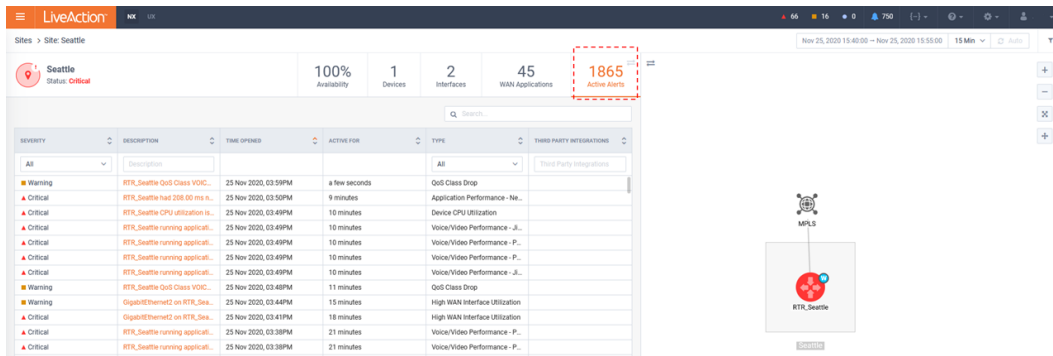
The *Interfaces* tab of the Site page provides a list of all monitored interfaces of the member devices in the Site. Clicking on an interface's link will drill-down into its details.



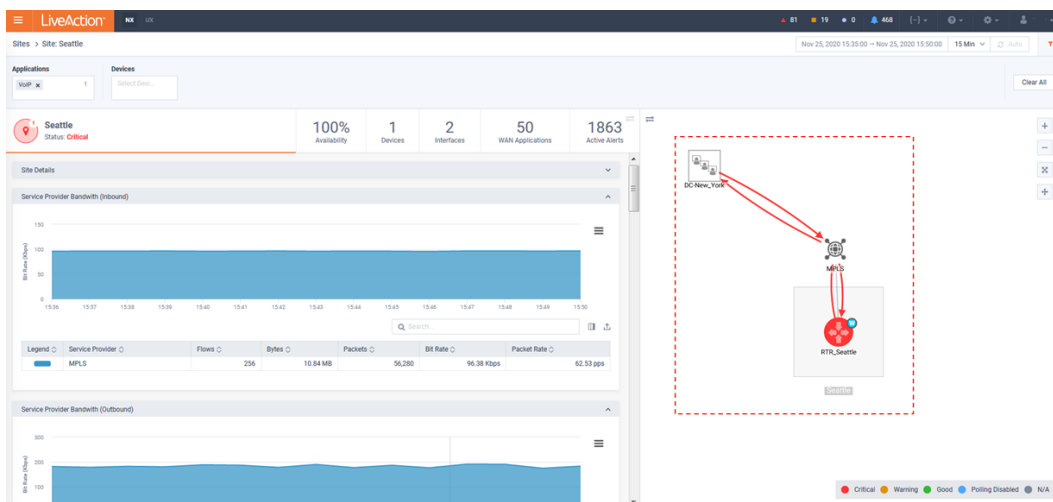
The *WAN Applications* tab of the Site page provides a list of all WAN applications in the Site. Clicking on an application will drill-down into its details.



The *Active Alerts* tab of the Site page provides a list of all active Alerts at the Site. Clicking on an Alert will drill-down into its details.



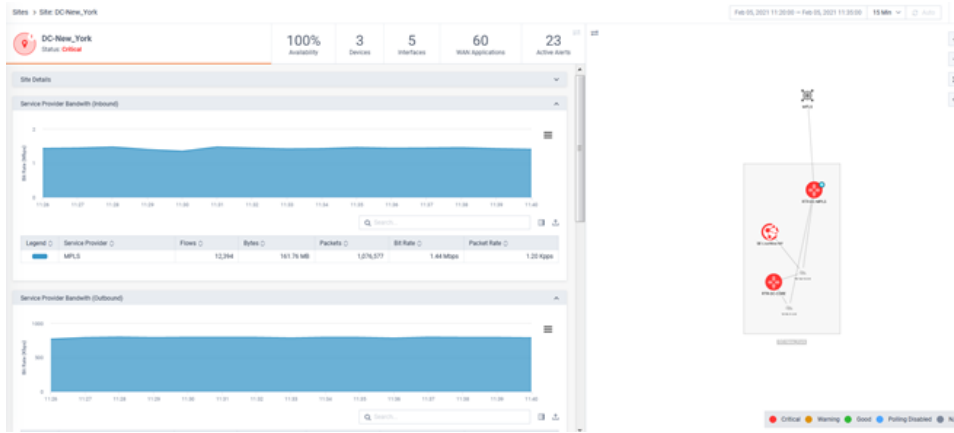
Select the *Filter* Icon at the top right of the page to see an *Application* and *Devices* filter. These only control the topology map. By entering an application(s), flow will be projected on the topology map. Relevant external sites that are part of the communication with the select application(s) are also shown. Entering a device(s) will highlight those entities.



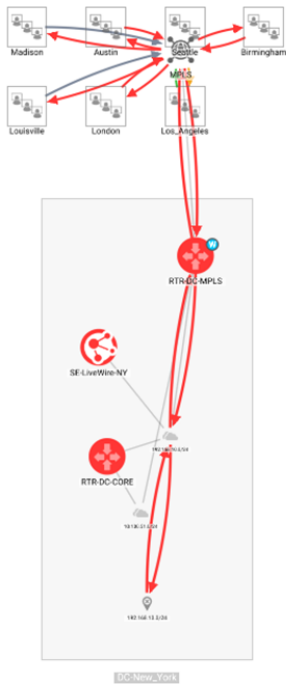
Click on an external site to be provided an option for **Site Details**.



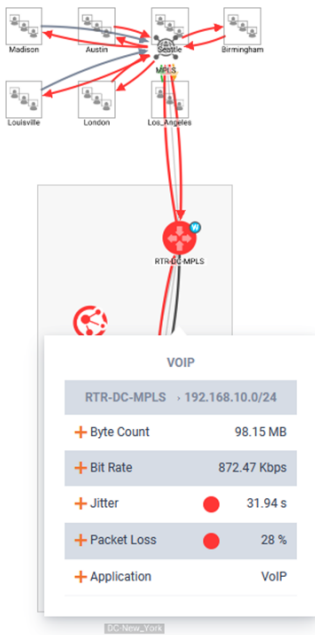
Click the **Site Details** button to drill-down to the details of the other Site.



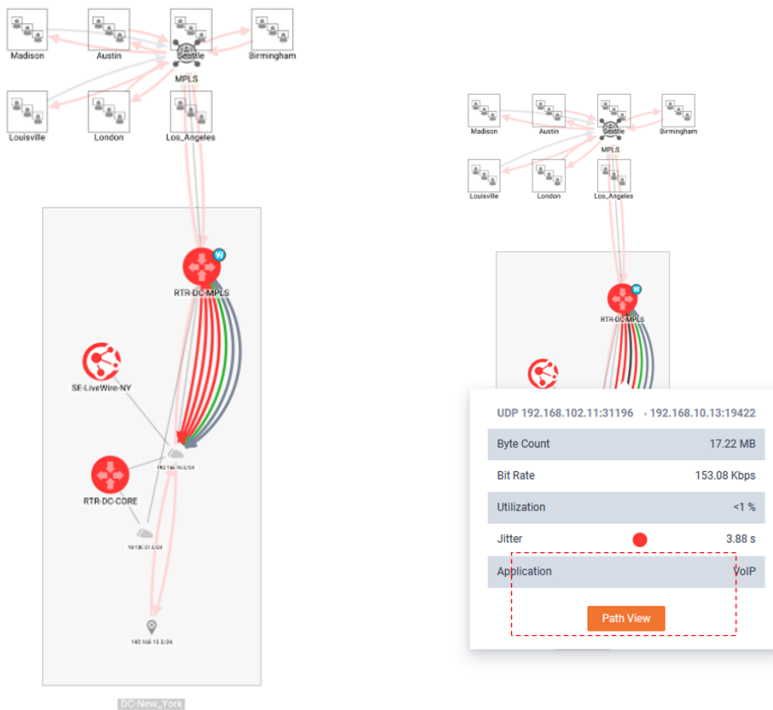
Clicking on a flow arrow will pop-up details about the application.



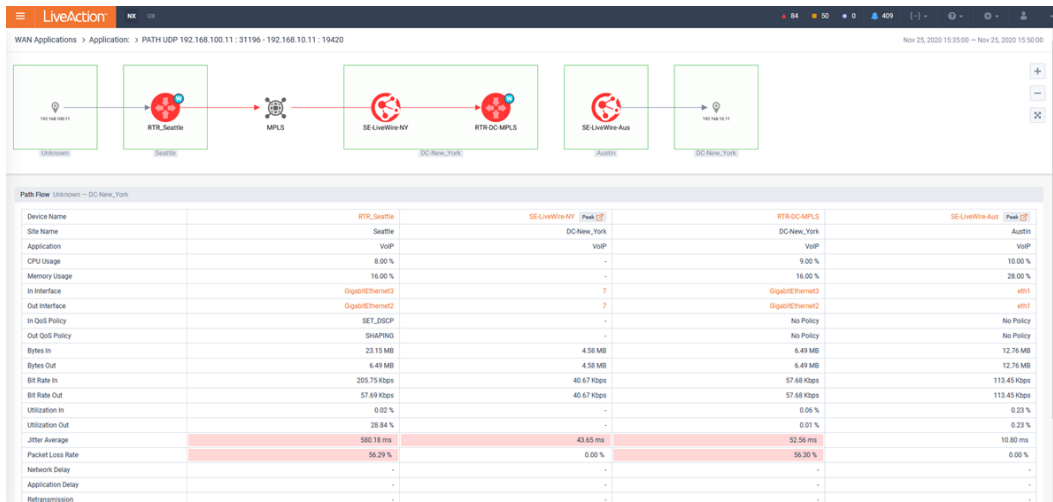
Expand the details to see all flows for the selected segment.



Click on an expanded flow to see its details.



Click **Path View** for drill-down to Flow Path Analysis.



## Devices

The Devices navigation page presents a list of all devices in LiveNX and highlights a summary of their performance statuses.

Clicking on a Device will drill-down to the Device's detail page. Clicking on a Site will drill-down to the Site's detail page.

Device	Site	Status	IP Address	Availability	CPU Memory	CPU Avg	Memory Avg	Tags	Vendor	Type	Version	Description
CS-2900-23-22	Internet	●	10.100.51.22	●	●	-	-	test2jett, TEST_IPSLA...	Cisco	Router	12.2(50)SE5	Cisco IOS Software...
PA-MX4-816	Internet	●	10.1.10.71	●	●	-	-	-	Meraki	Router	Unknown OS	Meraki MX44 Cloud...
RTR-DC-CORE	DC-New_York	●	10.100.51.3	●	●	7%	15%	CORE_IPSLA, custb...	Cisco	Router	15.5(3)S4	Cisco IOS Software...
RTR-DC-MPLS	DC-New_York	●	10.100.51.4	●	●	11%	16%	CORE_IPSLA, custb...	Cisco	Router	16.3.7	Cisco IOS Software...
RTR-Birmingham1	Birmingham	●	10.100.51.7	●	●	6%	16%	Birmingham_IPSLA...	Cisco	Router	16.3.7	Cisco IOS Software...
RTR-Indianapolis	Indianapolis	●	10.100.51.40	●	●	-	-	INDY_USA, INDIANA...	Non-SNMP	Non-SNMP	-	Advanced TCP Neff...
RTR-LosAngeles	LosAngeles	●	10.100.51.9	●	●	6%	16%	IPSLA_LOS_ANGELE...	Cisco	Router	16.3.7	Cisco IOS Software...
RTR-Louisville	Louisville	●	10.100.51.10	●	●	9%	16%	LOUISVILLE_IPSLA...	Cisco	Router	16.3.7	Cisco IOS Software...
RTR-PaloAlto-Wan	-	●	10.100.51.14	●	●	-	-	OSH	Cisco	Router	15.5(3)S4	Cisco IOS Software...
RTR-Seattle	Seattle	●	10.100.51.2	●	●	9%	16%	IPSLA_CSR_USA, RO...	Cisco	Router	16.3.7	Cisco IOS Software...
SE-FS-VE-ITM	Internet	●	10.100.51.39	●	●	-	-	test2jett, test2jett, FS	FS	Router	Unknown OS	Big-IP Virtual Edito...
SE-LiveWire-Aus	Austin	●	10.100.51.81	●	●	9%	41%	LiveWire_Inverine	LiveAction	Router	Unknown OS	LivePCA 20.2.0.7-v1
SE-LiveWire-LA	LosAngeles	●	10.100.51.38	●	●	1%	48%	LiveWire	LiveAction	Router	Unknown OS	LivePCA 20.2.1-v1
SE-LiveWire-NY	DC-New_York	●	10.100.50.80	●	●	-	-	LiveWire_ontsprianc...	Non-SNMP	Non-SNMP	-	LiveWire Virtual 12.3...
ShirepasAUS	-	●	10.100.51.41	●	●	-	-	-	Non-SNMP	Non-SNMP	-	ShirepasAUS
eEdgeART-IPFfx	-	●	10.100.51.102	●	●	-	-	-	Non-SNMP	Non-SNMP	-	eEdgeART-IPFfx
ES-sedemo	-	●	10.1.2.202	●	●	-	-	-	Non-SNMP	Non-SNMP	-	ES-IP Virtual Edito...
CS-C3850-23-36	-	●	10.100.155.1	●	●	7%	36%	test2jett, IPSLA, test...	Cisco	Router	03.06.03E	Cisco IOS Software...
CS-C3850-23-31	-	●	10.100.51.1	●	●	21%	38%	test2jett, LiveAgent...	Cisco	Router	03.06.08E	Cisco IOS Software...
RTR-SanJose	San_Jose	●	10.100.51.12	●	●	7%	16%	RouterTest	Cisco	Router	16.3.7	Cisco IOS Software...
ASA-Firewall	Internet	●	10.100.51.19	●	●	-	-	test2jett, test2jett	Non-SNMP	Non-SNMP	-	ASA Firewall
AppFastLane-3560	-	●	10.100.51.20	●	●	-	-	-	Non-SNMP	Non-SNMP	-	AppFastLane-3560

Clicking on a status bubble will provide more details and optional drill-down for further exploration.

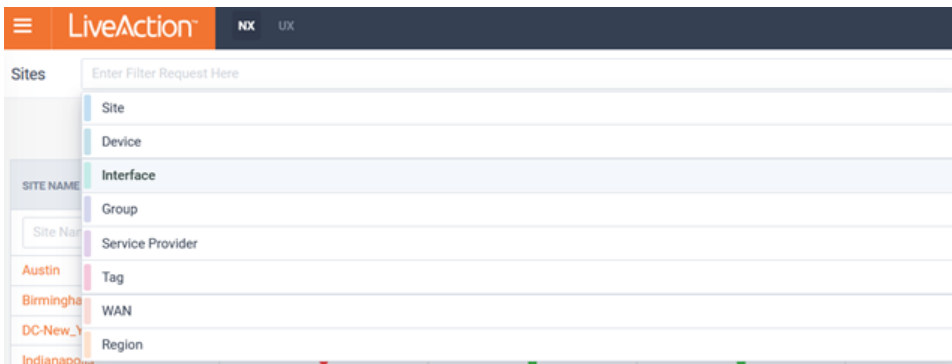
Device	Site	Status	IP Address	Availability	CPU Memory	CPU Avg	Memory Avg	Tags	Vendor	Type	Version	Description
RTR-Louisville	Louisville	●	10.100.51.10	●	●	9%	16%	LOUISVILLE_IPSLA...	Cisco	Router	16.3.7	Cisco IOS Software...



LiveAction LiveWire and LiveCapture appliance devices will have an icon to allow cross-launch to Peek (Omnipeek).

Device	Site	Status	IP Address	Availability	CPU/MEMORY	CPU AVG	MEMORY AVG	TAGS	VENDOR	TYPE	VERSION	DESCRIPTION
CS-2960-23-22	Internet	●	10.100.51.22	●	●	-	-	test2jett, TEST_IPSLA...	Cisco	Router	12.2(20)5E5	Cisco IOS Software...
PA-M54-816	Internet	●	10.1.10.71	●	●	-	-	-	Meraki	Router	Unknown OS	Meraki M54 Cloud...
RTR-DC-CORE	DC-New_York	●	10.100.51.3	●	●	7%	15%	CORE_IPSLA, custb...	Cisco	Router	15.5(3)54	Cisco IOS Software L...
RTR-DC-MPLS	DC-New_York	●	10.100.51.4	●	●	11%	16%	CORE_IPSLA, custb...	Cisco	Router	16.3.7	Cisco IOS Software L...
RTR_Birmingham1	Birmingham	●	10.100.51.7	●	●	6%	16%	Birmingham_IPSLA...	Cisco	Router	16.3.7	Cisco IOS Software L...
RTR_Indianapolis	Indianapolis	●	10.100.51.40	●	●	-	-	INDY_USA, INDIANA...	Non-SNMP	Non-SNMP	-	Advanced TCP NeffL...
RTR_LosAngeles	Los_Angeles	●	10.100.51.9	●	●	6%	16%	IPSLA_LOS_ANGELE...	Cisco	Router	16.3.7	Cisco IOS Software L...
RTR_Louisville	Louisville	●	10.100.51.10	●	●	9%	16%	LOUISVILLE_IPSLA...	Cisco	Router	16.3.7	Cisco IOS Software L...
RTR_PaloAlto-Wan	-	●	10.100.51.14	●	●	-	-	OSH	Cisco	Router	15.5(3)54	Cisco IOS Software L...
RTR_Seattle	Seattle	●	10.100.51.2	●	●	9%	16%	IPSLA_CSR_USA, RO...	Cisco	Router	16.3.7	Cisco IOS Software L...
SE-FS-VE-LTM	Internet	●	10.100.51.39	●	●	-	-	test2jett, test2jett, FS	FS	Router	Unknown OS	BIG-IP Virtual Editio...
SE-LiveWire-Aus	Austin	●	10.100.51.81	●	●	9%	41%	LiveWire, livewire	LiveAction	Router	Unknown OS	LivePCA 20.2.0.7-v1
SE-LiveWire-LA	Los_Angeles	●	10.100.51.38	●	●	1%	48%	LiveWire	LiveAction	Router	Unknown OS	LivePCA 20.2.1.1-v1
SE-LiveWire-NY	DC-New_York	●	10.100.50.80	●	●	-	-	LiveWire_omnipri...	Non-SNMP	Non-SNMP	-	LiveWire Virtual 12.3...
Shimpeak-AUS	-	●	10.100.51.41	●	●	-	-	-	Non-SNMP	Non-SNMP	-	ShimpeakAUS
cEdgeART-PTX	-	●	10.100.51.102	●	●	-	-	-	Non-SNMP	Non-SNMP	-	cEdgeART-PTX
ES-socoma	-	●	10.1.2.202	●	●	-	-	-	FS	Router	Unknown OS	85-IP Virtual Editio...
CS-C3850-23-36	-	●	10.100.155.1	●	●	7%	36%	test2jett, IPSLA, test...	Cisco	Router	03.06.03.E	Cisco IOS Software L...
CS-C3850-23-31	-	●	10.100.51.1	●	●	21%	38%	test2jett, LiveAgent...	Cisco	Router	03.06.08E	Cisco IOS Software L...
RTR_SanJose	San_Jose	●	10.100.51.12	●	●	7%	16%	RouterTest	Cisco	Router	16.3.7	Cisco IOS Software L...
ASA-Firewall	Internet	●	10.100.51.19	●	●	-	-	test2jett, test2jett	Non-SNMP	Non-SNMP	-	ASA Firewall
ApprFastLane-3560	-	●	10.100.51.20	●	●	-	-	-	Non-SNMP	Non-SNMP	-	ApprFastLane-3560

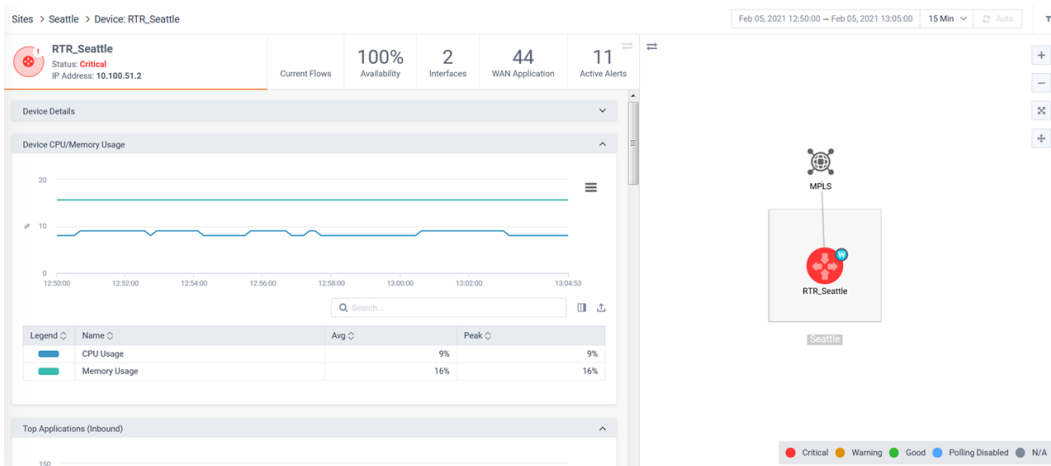
Filters can be applied to focus on the specific entities of interest:



The page can optionally be auto-refreshed by toggling the **Auto** button in the top right of the page.



The Device's detail page has multiple tabs to quickly understand different dimensions of the entity. There is also a simple topology map to provide context of the entity.



Historic data can be explored on the entity's tabs.

Feb 05, 2021 10:35:00 → Feb 05, 2021 10:50:00
15 Min ▾

### SET THE END DATE & TIME

< Feb 2021 >
Today

S	M	T	W	T	F	S
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	1	2	3	4	5	6
7	8	9	10	11	12	13

↑

10

↓

:

↑

50

↓

AM

Reset to Now
Apply

### INTERVAL

5 Mins

15 Min

Hour

Day

Week

30 Days

The page can optionally be auto-refreshed by toggling the **Auto** button in the top right of the page.



The page view can be modified to allow the tabs or topology to be full page.

Sites > Seattle > Device: RTR\_Seattle
Feb 05, 2021 12:50:00 – Feb 05, 2021 13:05:00 15 Min ▾  Auto ▾

**RTR\_Seattle**  
Status: Critical  
IP Address: 10.100.51.2

Current Flows

100%

Interfaces

2

WAN Application

44

Active Alerts

11

+  
-  
⊗

Device Details ▾

Full page tab view:

Sites > Seattle > Device: RTR\_Seattle
Feb 05, 2021 12:50:00 – Feb 05, 2021 13:05:00 15 Min ▾  Auto ▾

**RTR\_Seattle**  
Status: Critical  
IP Address: 10.100.51.2

Current Flows

100%

Interfaces

2

WAN Application

44

Active Alerts

11

+  
-  
⊗

Device Details ▾

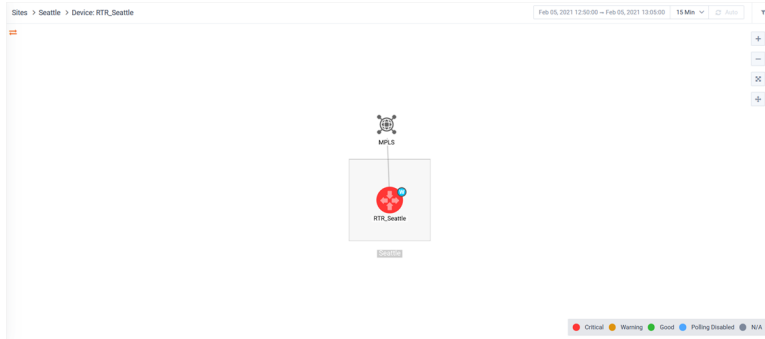
Device CPU/Memory Usage

Legend	Name	Avg	Peak
CPU Usage	CPU Usage	9%	9%
Memory Usage	Memory Usage	16%	16%

Top Applications (Inbound)

100
-----

Full page Topology view:



The status tab of the Device page provides a curated list of reports for quick understanding of the Devices' Status.

These reports include:

- Device Details
- Device CPU/ Memory Usage
- Top Application(Inbound)
- Top Application(Outbound)
- Top DSCP(Inbound)
- Top DSCP(Outbound)
- Top Conversation(Inbound)
- Top Conversation(Outbound)

**Current Flows Summary:**

- Current Flows: 4
- Availability: 100%
- Interfaces: 2
- WAN Application: 44
- Active Alerts: 11

**Device Details:**

- Serial: 92M011N155L
- Version: 16.3.7
- Pulling interval: 10 seconds
- Model: ciscoCSR1000v
- Node: Local/Server
- Vendor: Cisco
- Description: Cisco IOS Software [Denali], CSR1000V Software (936\_94\_LINUX\_IOSD-UNIVERSALK9-M, Version 16.3.7, RELEASE SOFTWARE (std) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1999-2018 by Cisco Systems, Inc. Compiled Sat 04-Aug-18 00:09 by
- Tag: IPSLA, CSR, USA, ROUTER, SEATTLE, MNQ2, OSH, RTR

**Device CPU/Memory Usage:**

Name	Avg	Peak
CPU Usage	9%	9%
Memory Usage	16%	16%

**Top Applications (Inbound):**

Application	Total Flows	Total Bytes	Total Packets	Average Bit Rate	Average Packet Rate	Peak Bit Rate	Peak Packet Rate
Video	15	5.57 MB	27,855	49.52 Kbps	20.95 pps	50.24 Kbps	21 pps
VoIP	15	5.05 MB	25,271	44.90 Kbps	28.08 pps	45.12 Kbps	28 pps
ooh-YouTube-Sample	212	174.42 KB	2,907	1.55 Kbps	3.23 pps	1.68 Kbps	3 pps
netbios-dgm	6	5.39 KB	29	0.05 Kbps	0.03 pps	0.06 Kbps	0 pps
netbios-ns	2	780 bytes	10	0.01 Kbps	0.01 pps	0.01 Kbps	0 pps
icmp	3	280 bytes	5	0.00 Kbps	0.01 pps	0.01 Kbps	0 pps

**Top Applications (Outbound):**

The *Current Flows* tab will show the raw flows being received by the device.

Sites > Seattle > Device: RTR\_Seattle

RTR\_Seattle  
Status: Critical  
IP Address: 10.100.51.2

Current Flows

100% Availability   2 Interfaces   43 WAN Application   1878 Active Alerts

Basic Flow   Refresh table   Enter Filter Request Here   Apply filter

TIME	FLOW R...	SRC IP...	DST IP...	IN IP	SRC PO...	DST PO...	SWICT...	SRC DE...	PROTO...	SRC PR...	DST PR...	TCP FL...	DSCP
Time	Flow Bk	Src IP A	Dst IP A	In IP	Src Pnr	Dst Pnr	Directo	Src DSt	Protoc	Src Pnr	Dst Pnr	TCP Fls	DSCP
Wed, 25 ...	1	72.234.3...	12.33.22...	VoIP-NuID	0	0	Ingress	0 (BE)	ESP	28	0		0 (BE)
Wed, 25 ...	1	72.234.3...	12.33.22...	VoIP-NuID	0	0	Egress	0 (BE)	ESP	28	0		0 (BE)
Wed, 25 ...	1	72.234.3...	184.72.6...	VoIP-NuID	59701	443	Egress	0 (BE)	TCP	28	0	ACK PSH	0 (BE)
Wed, 25 ...	1	72.234.3...	12.33.22...	VoIP-NuID	59701	443	Ingress	0 (BE)	TCP	28	0	ACK PSH	0 (BE)
Wed, 25 ...	1	72.234.3...	12.33.22...	VoIP-NuID	7000	43561	Ingress	0 (BE)	TCP	28	0	ACK PSH	0 (BE)
Wed, 25 ...	1	72.234.3...	12.33.22...	VoIP-NuID	7000	43561	Egress	0 (BE)	TCP	28	0	ACK PSH	0 (BE)
Wed, 25 ...	1	72.234.3...	70.197.1...	VoIP-NuID	7000	8246	Ingress	0 (BE)	TCP	28	0	ACK PSH	0 (BE)
Wed, 25 ...	1	72.234.3...	70.197.1...	VoIP-NuID	7000	8246	Egress	0 (BE)	TCP	28	0	ACK PSH	0 (BE)
Wed, 25 ...	1	12.33.22...	72.234.3...	8	0	0	Ingress	18 (AF21)	ESP	0	28		18 (AF21)
Wed, 25 ...	1	12.33.22...	72.234.3...	8	0	0	Egress	18 (AF21)	ESP	0	28		18 (AF21)
Wed, 25 ...	1	192.168...	192.168...	GigabitEL	1604	1604	Ingress	0 (BE)	UDP	24	24		0 (BE)
Wed, 25 ...	1	192.168...	192.168...	GigabitEL	31196	19420	Ingress	46 (EF)	UDP	24	24		46 (EF)
Wed, 25 ...	1	72.234.3...	66.128.1...	VoIP-NuID	0	0	Egress	0 (BE)	ESP	28	0		0 (BE)
Wed, 25 ...	1	72.234.3...	66.128.1...	VoIP-NuID	0	0	Ingress	0 (BE)	ESP	28	0		0 (BE)
Wed, 25 ...	1	192.168...	192.168...	GigabitEL	31196	19500	Ingress	0 (BE)	UDP	24	24		0 (BE)
Wed, 25 ...	1	72.234.3...	12.33.22...	VoIP-NuID	7000	6207	Egress	0 (BE)	TCP	28	0	ACK PSH	0 (BE)
Wed, 25 ...	1	72.234.3...	12.33.22...	VoIP-NuID	7000	6207	Ingress	0 (BE)	TCP	28	0	ACK PSH	0 (BE)
Wed, 25 ...	1	192.168...	192.168...	GigabitEL	1604	1604	Egress	0 (BE)	UDP	24	24		0 (BE)
Wed, 25 ...	1	192.168...	192.168...	GigabitEL	19500	31196	Ingress	34 (AF41)	UDP	24	24		34 (AF41)
Wed, 25 ...	1	192.168...	192.168...	GigabitEL	19500	31196	Egress	34 (AF41)	UDP	24	24		34 (AF41)

● Critical ● Warning ● Good ● Polling Disabled ● N/A

The Flow Type picker will one to focus on the Flow of interest.

Sites > Seattle > Device: RTR\_Seattle

RTR\_Seattle  
Status: Critical  
IP Address: 10.100.51.2

Current Flows

100% Availability   2 Interfaces   43 WAN Application   1878 Active Alerts

Basic Flow   Refresh table   Enter Filter Request Here   Apply filter

The **Refresh Table** button forces the screen to refresh.

Sites > Seattle > Device: RTR\_Seattle

RTR\_Seattle  
Status: Critical  
IP Address: 10.100.51.2

Current Flows

100% Availability   2 Interfaces   43 WAN Application   1878 Active Alerts

Basic Flow   Refresh table   Enter Filter Request Here   Apply filter

Flex search Filters can be used to focus on the Flow type of interest.

Sites > Seattle > Device: RTR\_Seattle

RTR\_Seattle  
Status: Critical  
IP Address: 10.100.51.2

Current Flows

100% Availability   2 Interfaces   43 WAN Application   1878 Active Alerts

Basic Flow   Refresh table   Enter Filter Request Here   Apply filter

If Auto is selected, flows will automatically be refreshed.

Sites > Seattle > Device: RTR\_Seattle

RTR\_Seattle  
Status: Critical  
IP Address: 10.100.51.2

Current Flows

100% Availability   2 Interfaces   43 WAN Application   1878 Active Alerts

Basic Flow   Refresh table   Enter Filter Request Here   Apply filter

The *Availability* tab of the Device page provides the *Device Availability* report.

LiveAction

Sites > Seattle > Device: RTR\_Seattle

RTR\_Seattle  
Status: Critical  
IP Address: 10.100.51.2

Current Flows

100% Availability   2 Interfaces   43 WAN Application   1878 Active Alerts

Availability

Any availability (%)

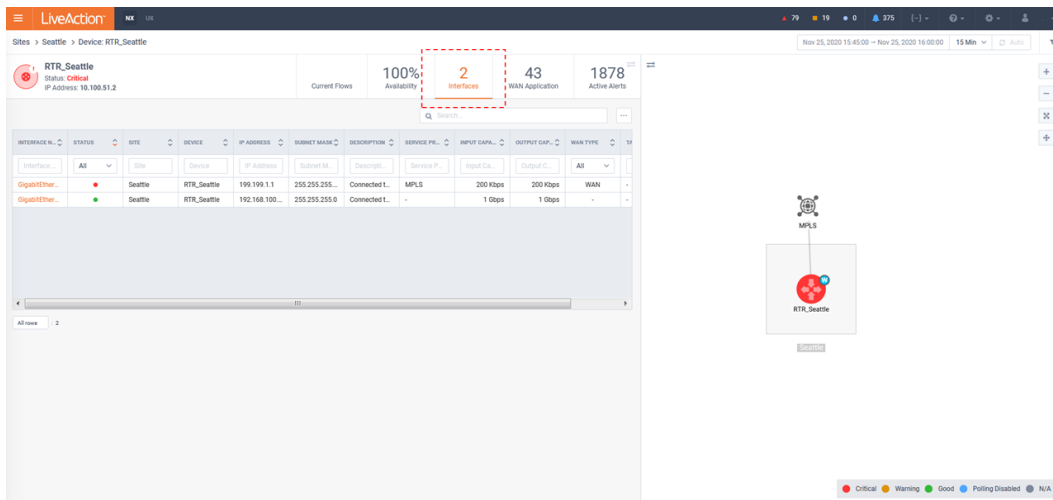
15:30:00   15:32:00   15:34:00   15:36:00   15:38:00   16:00:00   16:02:00   16:04:00   16:06:00

Legend

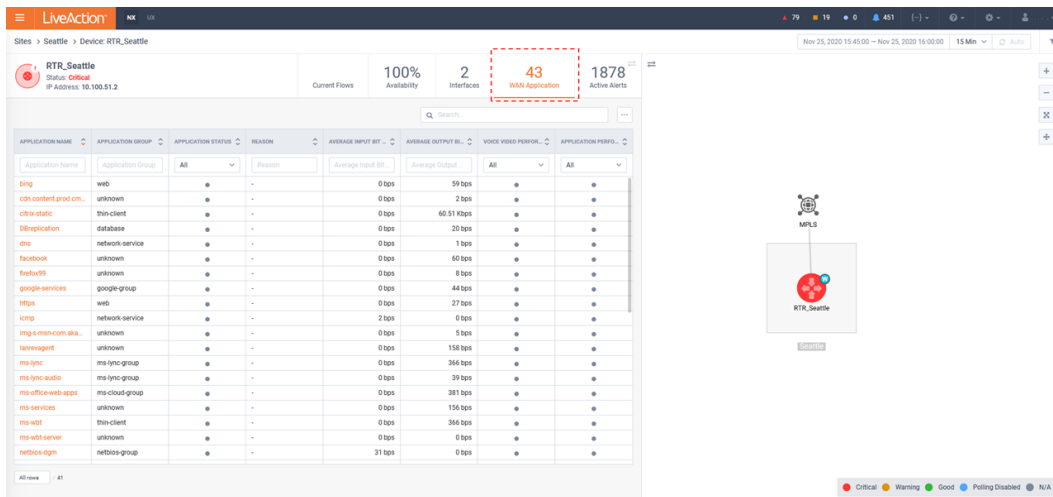
Site	Device	IP Address	Any Availability
Seattle	RTR_Seattle	10.100.51.2	100%

● Critical ● Warning ● Good ● Polling Disabled ● N/A

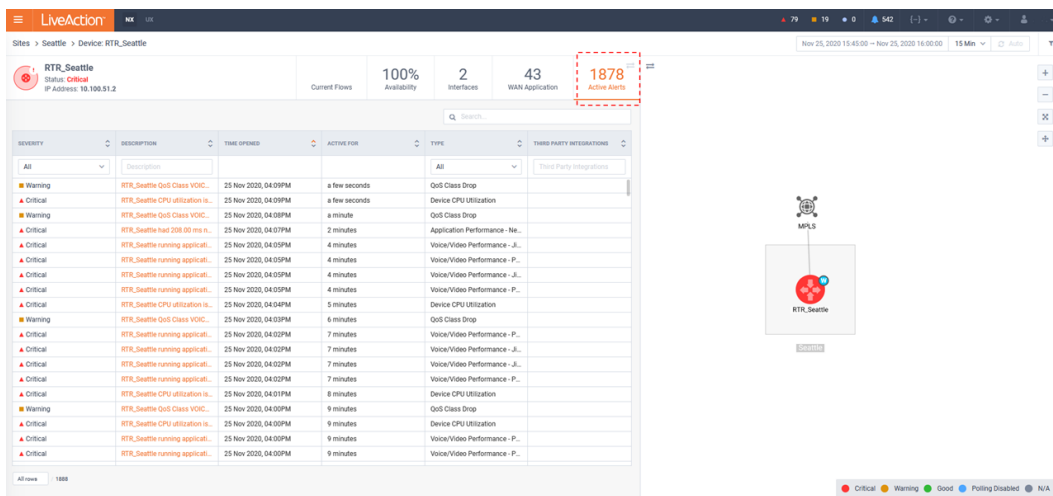
The *Interfaces* tab of the Devices page provides a list of all monitored interfaces of the devices. Clicking on an interface's link will drill-down into its details.



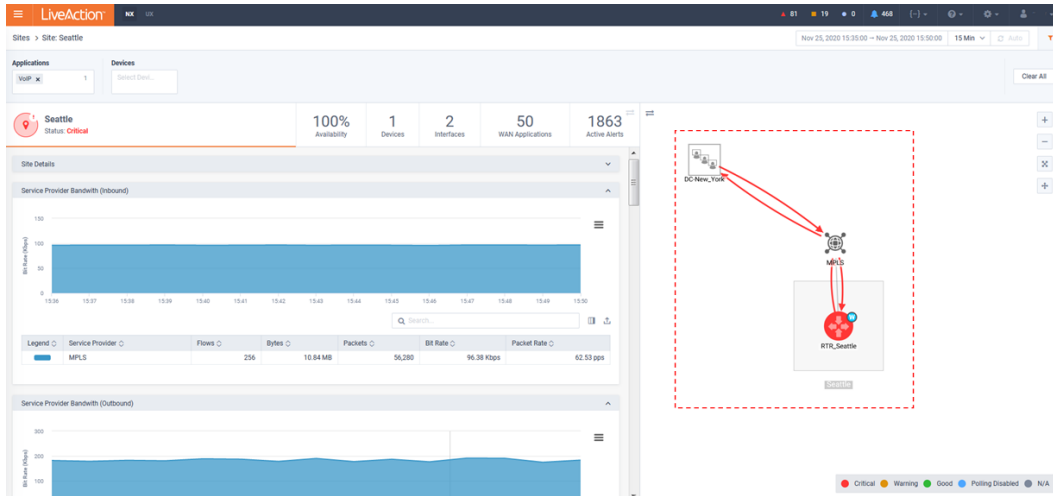
The *WAN Application* tab of the Device page provides a list of all WAN applications traversing the Device. Clicking on an application will drill-down into its details.



The *Active Alerts* tab of the Device page provides a list of all active Alerts on the Device. Clicking on an Alert will drill-down into its details.



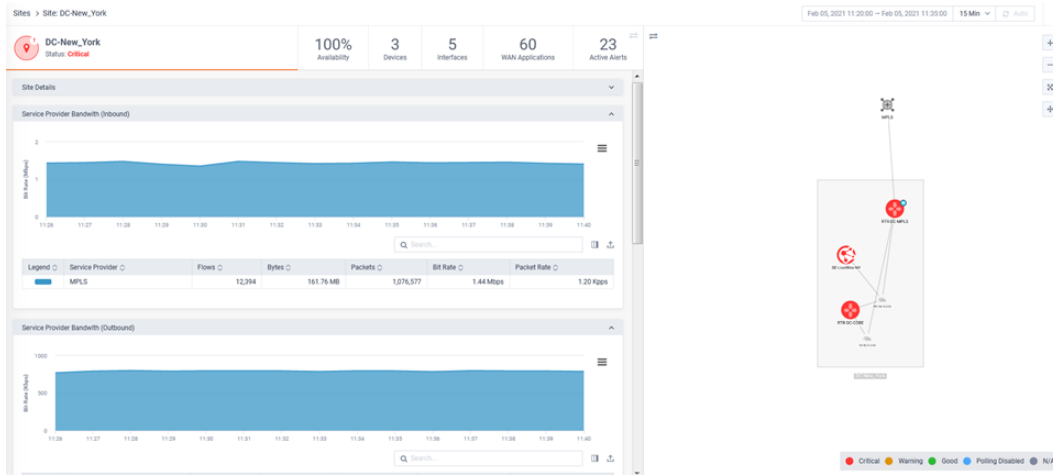
Select the Filter Icon at the top right of the page to see an *Application* and *Devices* filter. These only control the topology map. By entering an application(s), Flow will be projected on the topology map. Relevant external sites that are part of the communication with the select application(s) are also shown. Entering a device(s) will highlight those entities.



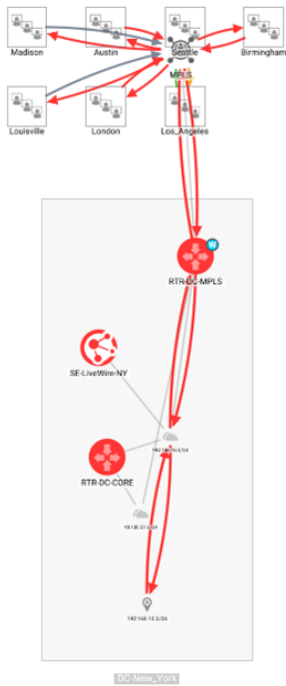
Click on an external site to be provided an option for **Site Details**.



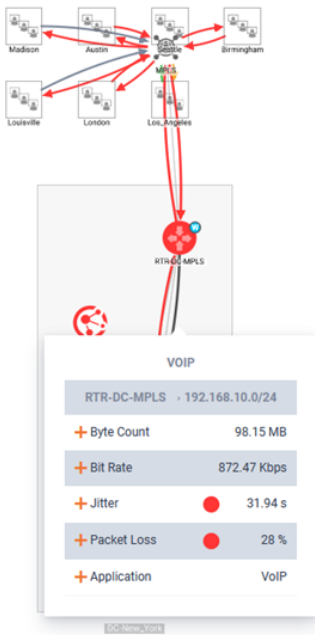
Click the **Site Details** button to drill-down to the details of the other Site.



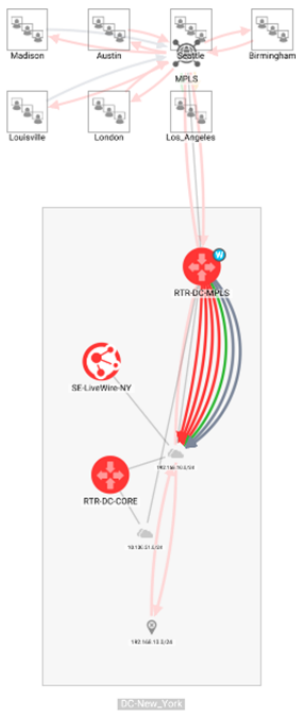
Clicking on a Flow arrow will pop-up details about the application.



Expand the details to see all flows for the selected segment.

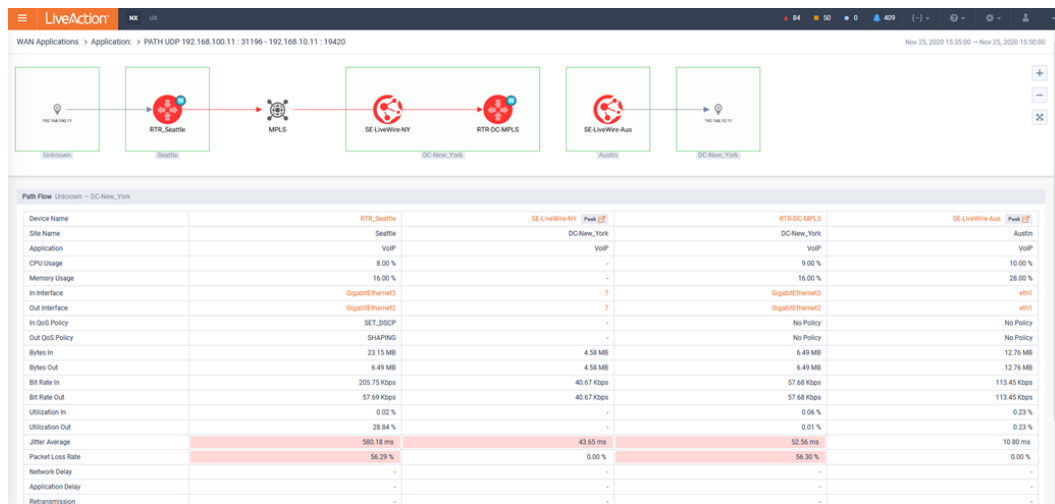
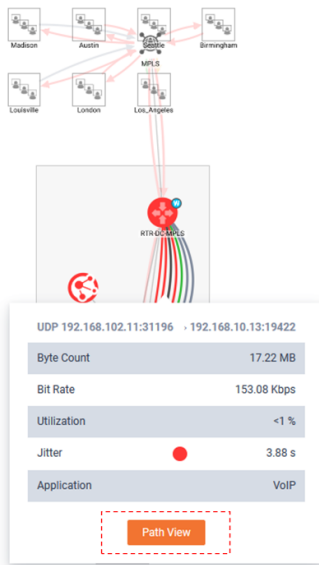


Click on an expanded Flow to see its details.



Click **Path View** for drill-down to Flow Path Analysis.





## Interfaces

The Interface navigation page presents a list of all interfaces in LiveNX and highlights a summary of their performance statuses.

Clicking on an Interface will drill-down to the Interface's detail page. Clicking on a Device will drill-down to the Devices' detail page. Clicking on a Site will drill-down to the Site's detail Page.

INTERFACE NAME	STATUS	SITE	DEVICE	IP ADDRESS	SUBNET MASK	DESCRIPTION	SERVICE PROVIDER	INPUT CAPACITY	OUTPUT CAPACITY	WAN TYPE	TAGS
GigabitEthernet2	●	Seattle	RTR_Seattle	199.199.1.1	255.255.255.252	Connected to MPLS Co.	MPLS	200 Kbps	200 Kbps	WAN	-
GigabitEthernet2	●	Birmingham	RTR_Birmingham1	199.199.1.9	255.255.255.252	Connected to MPLS Co.	MPLS	200 Kbps	200 Kbps	WAN	-
GigabitEthernet2	●	San Jose	RTR_SanJose	199.199.1.13	255.255.255.252	Conn-MPLS-Provider	MPLS	301 Kbps	301 Kbps	WAN	userbacking_test_wan
GigabitEthernet2	●	Louisville	RTR_Louisville	199.199.1.5	255.255.255.252	Conn-MPLS-Provider	MPLS	200 Kbps	200 Kbps	WAN	-
lan1	●	Internet	FA-MASA-B16	-	-	-	-	1 Gbps	1 Gbps	-	-
wan1	●	Internet	FA-MASA-B16	-	-	-	-	1 Gbps	1 Gbps	WAN	-
eth1	●	DC-New_York	SE-LiveWire-NY	192.168.10.101	255.255.255.0	-	-	0 Kbps	0 Kbps	-	-
eth5	●	Los_Angeles	SE-LiveWire-LA	192.168.107.200	255.255.255.0	-	-	0 Kbps	0 Kbps	-	-
eth1	●	Austin	SE-LiveWire-Aus	192.168.106.253	255.255.255.0	-	-	50 Mbps	50 Mbps	-	-
GigabitEthernet3	●	Seattle	RTR_Seattle	192.168.100.254	255.255.255.0	Connected to AdminSE	-	1 Gbps	1 Gbps	-	-
GigabitEthernet3	●	Birmingham	RTR_Birmingham1	192.168.102.254	255.255.255.0	Connected to SE@Birm...	-	1 Gbps	1 Gbps	-	-
GigabitEthernet3	●	San Jose	RTR_SanJose	192.168.103.254	255.255.255.0	Conn-AdminSE-PC	-	1 Gbps	1 Gbps	-	-
GigabitEthernet4	●	Sydney	IWAN-Br1_Sydney	22.1.1.254	255.255.255.0	-	-	1 Gbps	1 Gbps	-	-
Loopback0	●	Sydney	IWAN-Br1_Sydney	10.0.0.104	255.255.255.255	-	-	8 Gbps	8 Gbps	-	-
Tunnel100	●	Sydney	IWAN-Br1_Sydney	172.16.1.1	255.255.255.0	DMVPN over MPLS	MPLS	5 Mbps	5 Mbps	WAN	MPLS
Tunnel101	●	Sydney	IWAN-Br1_Sydney	172.16.2.1	255.255.255.0	DMVPN over Internet	INET	10 Mbps	10 Mbps	WAN	-
GigabitEthernet2	●	Los_Angeles	RTR_LosAngeles	199.199.1.29	255.255.255.252	Conn-MPLS-Provider	MPLS	100 Mbps	100 Mbps	WAN	-
GigabitEthernet3	●	Los_Angeles	RTR_LosAngeles	192.168.107.254	255.255.255.0	Conn-AdminSE-PC	-	1 Gbps	1 Gbps	-	-
GigabitEthernet2	●	Tokyo	IWAN-OC-MC	11.111.11.1	255.255.255.0	-	-	1 Gbps	1 Gbps	-	-
Loopback0	●	Tokyo	IWAN-OC-MC	10.0.0.103	255.255.255.255	-	-	8 Gbps	8 Gbps	-	-
GIS	●	Austin	RTR_Austin	10.100.60.253	255.255.255.0	AustinAgentNtw	-	0 Kbps	0 Kbps	-	-
GigabitEthernet2	●	Austin	RTR_Austin	199.199.1.25	255.255.255.252	Conn-MPLS-Provider	MPLS	200 Kbps	200 Kbps	WAN	-

Clicking on a status bubble will provide more details and optional drill-down for further exploration.

Alerts for GigabitEthernet2 on RTR\_Louisville:

- Critical:** GigabitEthernet2 on RTR\_Louisville was over utilized at 97.92% in the Outbound direction.
- Info:** GigabitEthernet2 on RTR\_Louisville was over utilized at 41.58% in the Inbound direction.

Filters can be applied to focus on the specific entities of interest:

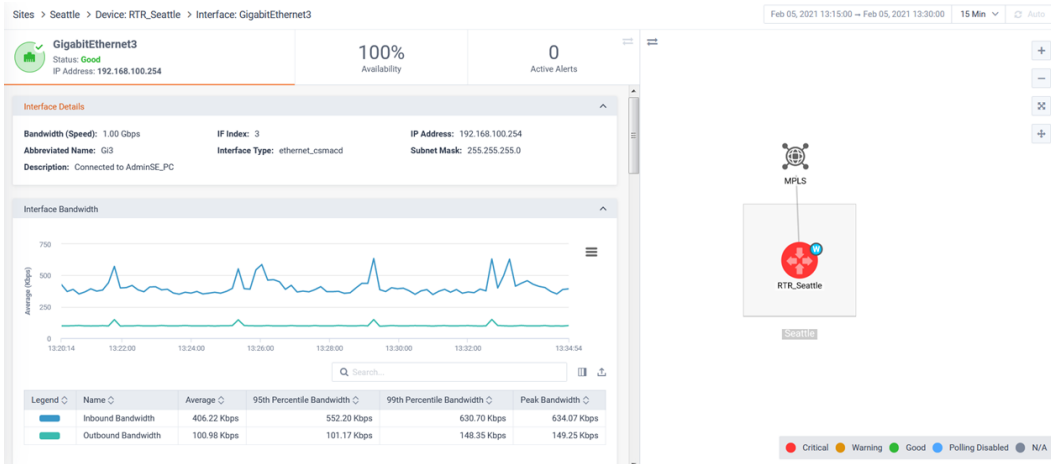
Filterable categories in the LiveAction NX UX interface:

- Site
- Device
- Interface
- Group
- Service Provider
- Tag
- WAN
- Region

The page can optionally be auto-refreshed by toggling the **Auto** button in the top right of the page.



The Interface detail page has multiple tabs to quickly understand different dimensions of the entity. There is also a simple topology map to provide context of the entity.

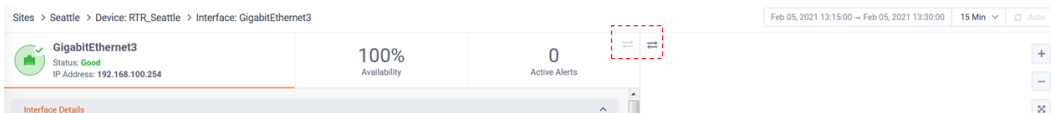


Historic data can be explored on the entity's tabs.

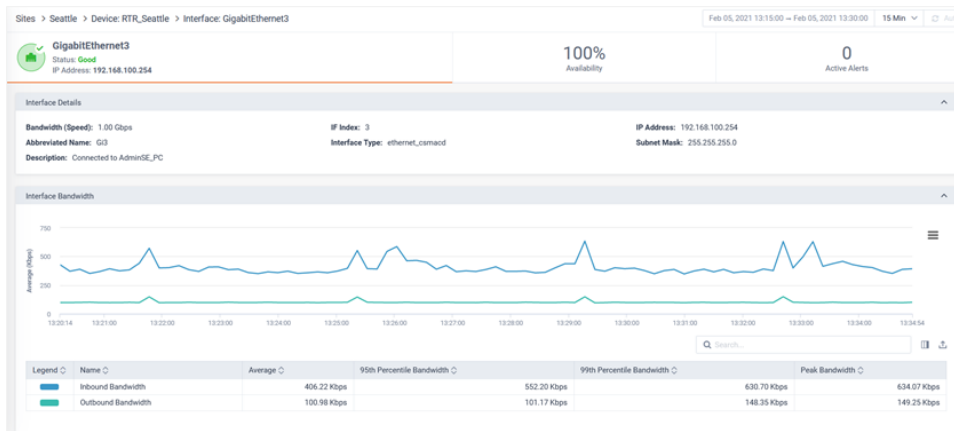
The page can optionally be auto-refreshed by toggling the **Auto** button in the top right of the page.



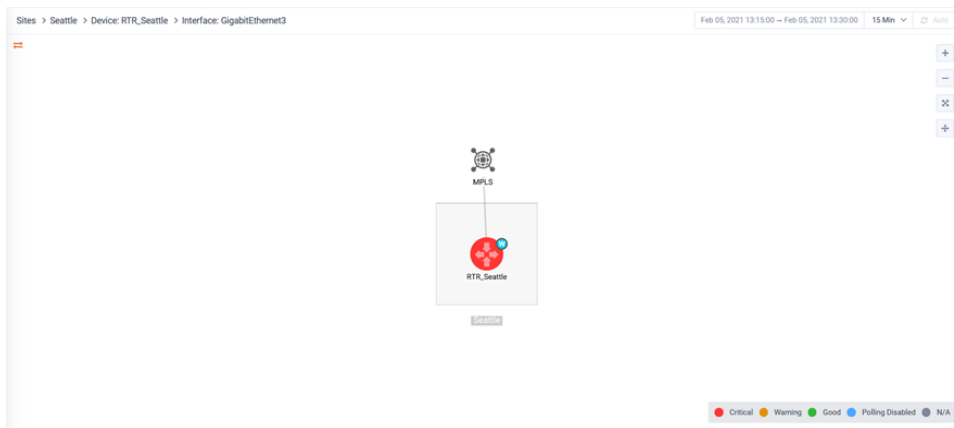
The page view can be modified to allow the tabs or topology to be full page.



Full page tab view:



Full page Topology view:



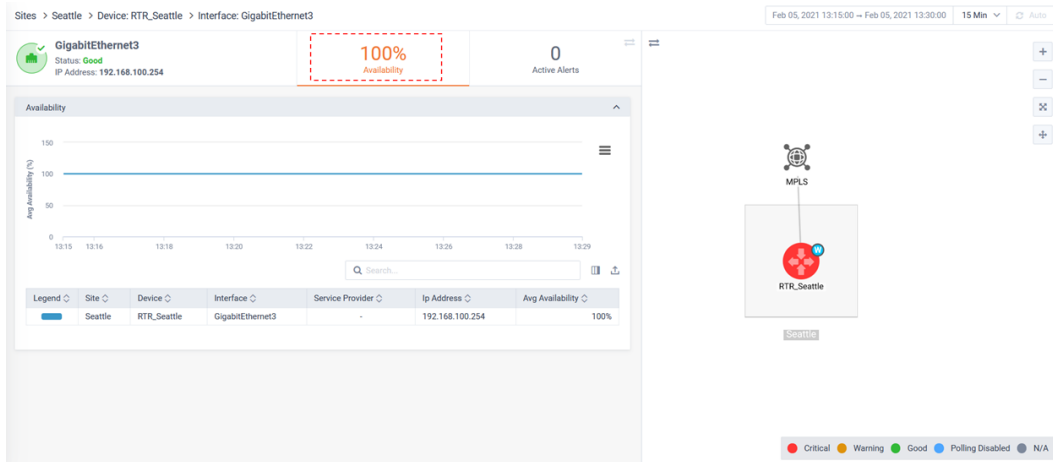
The status tab of the Interface page provides a curated list of reports for quick understanding of the Interfaces' Status.

These reports include:

- Site Details
- Interface Bandwidth
- Interface Errors
- Interface Utilization
- Top Class Drops (Outbound)
- Top Application (Inbound)
- Top Application (Outbound)
- Top DSCP (Inbound)
- Top DSCP (Outbound)
- Top Conversation (Inbound)
- Top Conversation (Outbound)



The *Availability* tab of the Site page provides the Sites *Availability* report.



The *Active Alerts* tab of the Interface page provides a list of all active Alerts on the Interface. Clicking on an Alert will drill-down into its details.

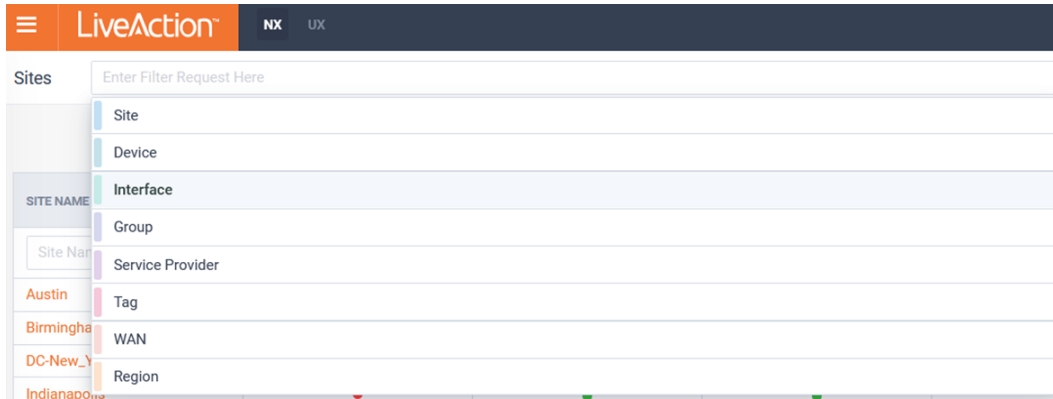
## WAN Applications

Manual exploration of WAN Applications can be done via the *Main* menu navigation bar.

The *WAN Applications* summary page provides a list of all WAN applications and a summary of their status. Clicking on an application will drill-down to its details page.

APPLICATION NAME	APPLICATION GROUP	APPLICATION STATUS	AVERAGE INPUT BIT RATE	AVERAGE OUTPUT BIT RATE	NETWORK PERFORMANCE	APPLICATION PERFORMANCE
Application Name	Application Group	All	Average Input Bit Rate	Average Output Bit Rate	All	All
30104	unknown	●	140.53 Kbps	140.53 Kbps	●	●
2048	unknown	●	851.82 Kbps	851.82 Kbps	●	●
30-nfs	unknown	●	1 bps	1 bps	●	●
644	unknown	●	6.05 Kbps	6.05 Kbps	●	●
914c, 914c/g	unknown	●	0 bps	0 bps	●	●
99fs	network-service	●	0 bps	0 bps	●	●
a248-a-amal	unknown	●	68 bps	26 bps	●	●
accoconnect	unknown	●	0 bps	0 bps	●	●
actor	unknown	●	0 bps	0 bps	●	●
actiforepic	unknown	●	0 bps	0 bps	●	●
adcp	unknown	●	0 bps	0 bps	●	●
addtlis	web	●	3.79 Kbps	3.79 Kbps	●	●
admin	unknown	●	0 bps	0 bps	●	●
adms	unknown	●	1.11 Kbps	2.12 Kbps	●	●
adobe	unknown	●	5.08 Kbps	5.08 Kbps	●	●
adobeconnect-5	unknown	●	0 bps	0 bps	●	●
adobeconnect	unknown	●	3.18 Kbps	2.59 Kbps	●	●
adps	unknown	●	80 bps	33 bps	●	●
adps	unknown	●	0 bps	0 bps	●	●
afc3-mtaps	unknown	●	0 bps	0 bps	●	●
afc3-tserver	unknown	●	0 bps	0 bps	●	●
agins	unknown	●	324 tps	140 tps	●	●

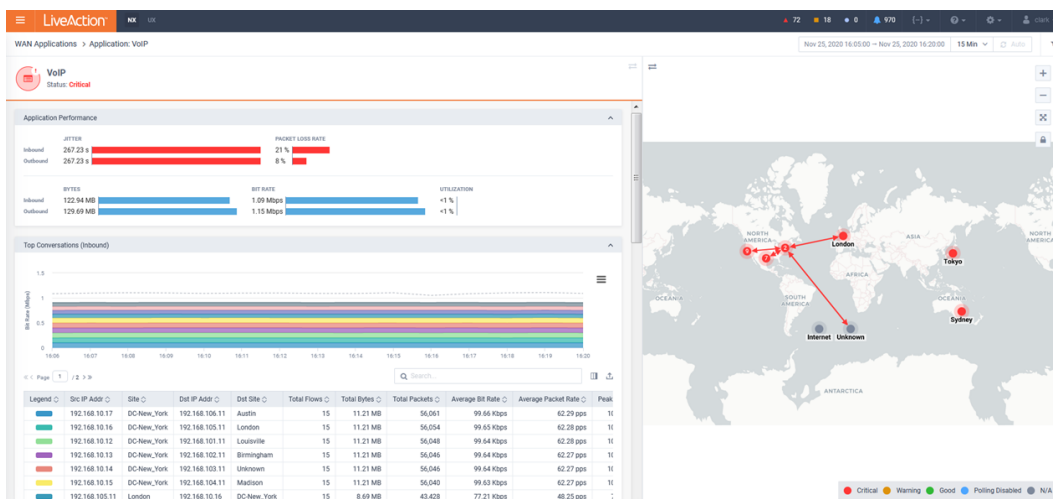
Filters can be applied to focus on the specific entities of interest:



The page can optionally be auto-refreshed by toggling the **Auto** button in the top right of the page.



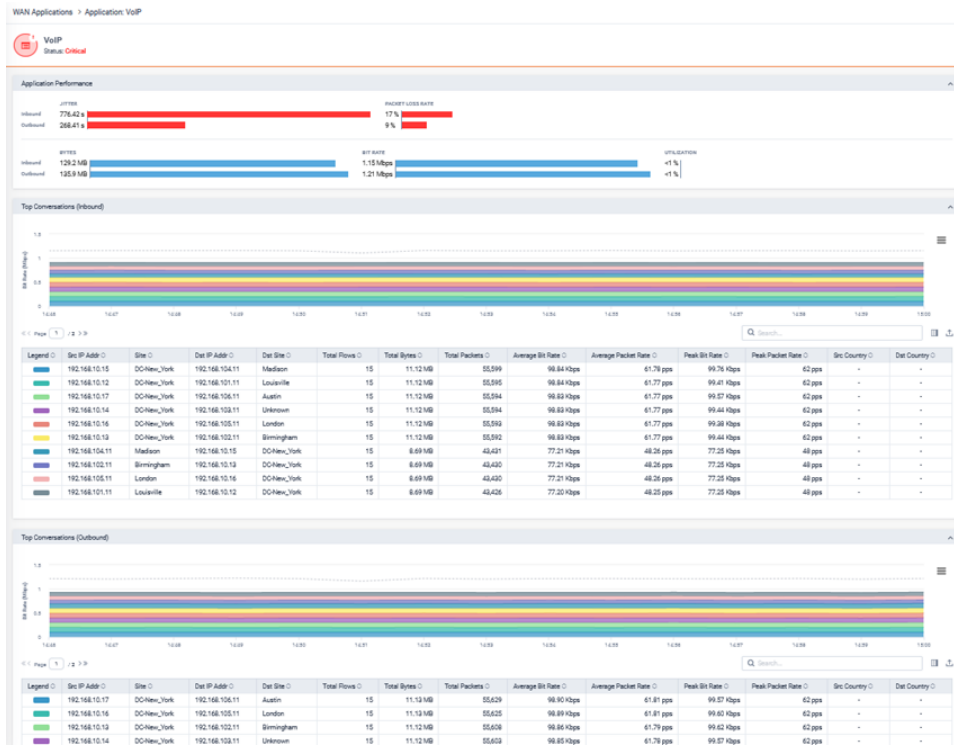
The WAN Applications' detail page provides a summary of the selected applications utilization and, if applicable, its performance metrics. There is also a simple topology map to provide context of the application.



The status tab of the WAN Applications page provides a curated list of reports for quick understanding of the Interfaces' Status.

These reports include:

- Application Summary
- Top Conversation (Inbound)
- Top Conversation (Outbound)
- Top DSCP (Inbound)
- Top DSCP (Outbound)
- Jitter/ Loss
- Application Performance by Interface



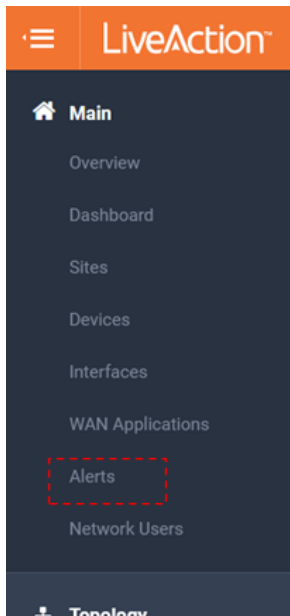
## Alerts

The LiveNX Alerts page provide active and historic events detected by the solution.

LiveNX Alerts have the following states:

- **Active** – An Alert has been triggered due to underlying event(s) and is currently unresolved.
- **Ignored** – An Alert is Active, but the User has put the alert in Ignore state. Do not trigger any notification. Do not count these Alerts towards dashboard/current summary. A user can change state back to Active to start receiving alerts again.
- **Acknowledged** – An Alert is Active but the User has acknowledged its existence. So do not trigger any notification. However, count these Alerts towards dashboard/current summary. A user can change state back to Active to start receiving alerts again.
- **Resolved** – An Active alert has been resolved either due to the underlying events being resolved (Cleared) or via User action. Resolved should be the final state of an alert.





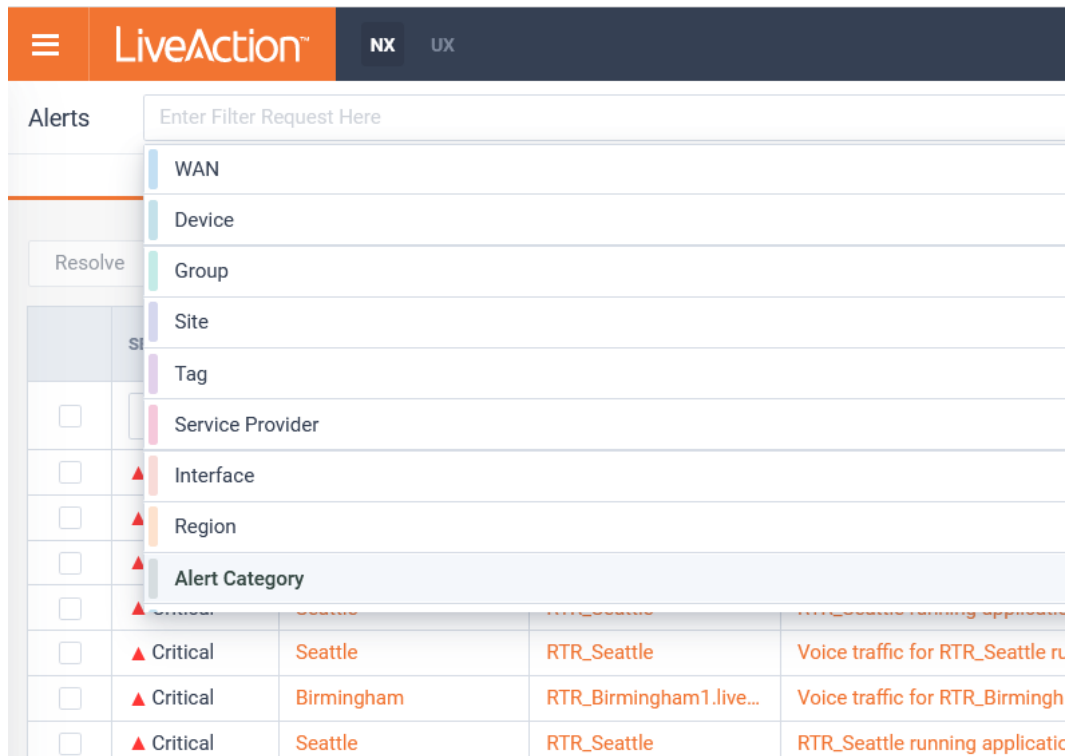
LiveNX provides three (3) Alert severity levels. These are:

- Info
- Warning
- ▲ Critical

The Alerts Active tab will present any active Alerts known to the system.

SEVERITY	SITE	DEVICE	DESCRIPTION	TIME OPENED	ACTIVE FOR	CATEGORY	TYPE
▲ Critical	Seattle	RTR_Seattle	RTR_Seattle running application VoIP had 38.49 % of packet loss for traffic with a DSCP value of 0...	30 Nov 2020, 01:50PM	a few seconds	Application	Voice/Video Perf...
▲ Critical	Seattle	RTR_Seattle	RTR_Seattle running application VoIP had voice/video traffic with 32.16 ms max jitter 38.49% pack...	30 Nov 2020, 01:50PM	a few seconds	Application	Voice/Video appl...
▲ Critical	Seattle	RTR_Seattle	RTR_Seattle running application VoIP had 56.86 % of packet loss for traffic with a DSCP value of 4...	30 Nov 2020, 01:50PM	a few seconds	Application	Voice/Video Perf...
▲ Critical	Seattle	RTR_Seattle	RTR_Seattle running application VoIP had 32.16 ms of jitter for traffic with a DSCP value of 0 (BE)	30 Nov 2020, 01:50PM	a few seconds	Application	Voice/Video Perf...
▲ Critical	Seattle	RTR_Seattle	Voice traffic for RTR_Seattle running application Video is not marked as DSCP EF.	30 Nov 2020, 01:50PM	a few seconds	Application	Voice Traffic Clas...
▲ Critical	Birmingham	RTR_Birmingham1.live...	Voice traffic for RTR_Birmingham1.liveaction.com running application VoIP is not marked as DSC...	30 Nov 2020, 01:50PM	a few seconds	Application	Voice Traffic Clas...
▲ Critical	Seattle	RTR_Seattle	RTR_Seattle running application VoIP had 33.76 ms of jitter for traffic with a DSCP value of 46 (EF)	30 Nov 2020, 01:50PM	a few seconds	Application	Voice/Video Perf...
▲ Critical	Los_Angeles	RTR_LosAngeles.livea...	RTR_LosAngeles.liveaction.com IP SLA Voice/Jitter total errors is greater than threshold value: 3	30 Nov 2020, 01:50PM	a few seconds	Network	IP SLA Voice/Jitte...
▲ Critical	Los_Angeles	RTR_LosAngeles.livea...	RTR_LosAngeles.liveaction.com IP SLA Voice/Jitter total errors is greater than threshold value: 3	30 Nov 2020, 01:50PM	a few seconds	Network	IP SLA Voice/Jitte...
▲ Critical	Los_Angeles	RTR_LosAngeles.livea...	RTR_LosAngeles.liveaction.com CPU utilization is above threshold	30 Nov 2020, 01:50PM	a few seconds	Device, Interface	Device CPU Utiliz...
▲ Critical	Los_Angeles	RTR_LosAngeles.livea...	RTR_LosAngeles.liveaction.com running application VoIP had 10.96 % of packet loss for traffic wt...	30 Nov 2020, 01:50PM	a few seconds	Application	Voice/Video Perf...
▲ Critical	Los_Angeles	RTR_LosAngeles.livea...	RTR_LosAngeles.liveaction.com running application VoIP had 28.33 ms of jitter for traffic with a D...	30 Nov 2020, 01:50PM	a few seconds	Application	Voice/Video Perf...
▲ Critical	Los_Angeles	WLC-NetflowReplay	Voice traffic for WLC-NetflowReplay running application dns is not marked as DSCP EF.	30 Nov 2020, 01:50PM	a few seconds	Application	Voice Traffic Clas...

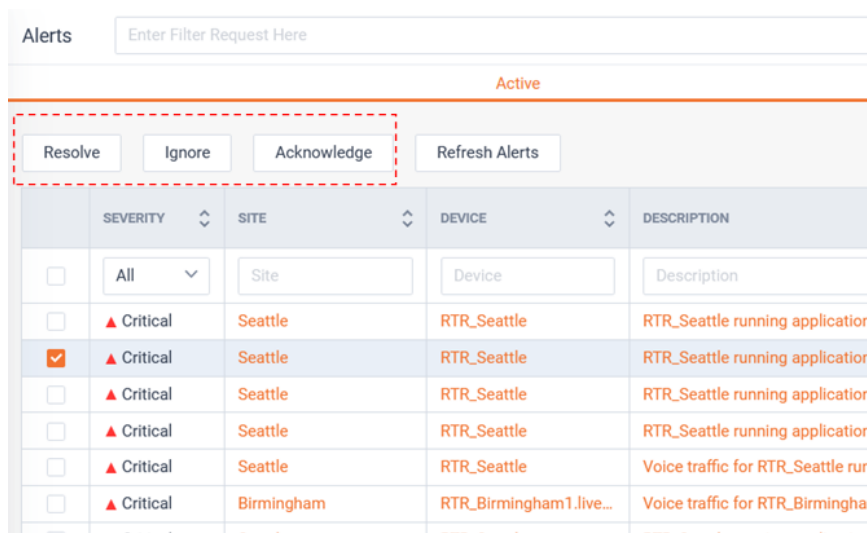
Filters can be applied to focus on alerts of interest.



By selecting an Alert(s), the state can be modified:

- Resolve - Manually mark this alert as resolved.
- Ignored - The Alert is Active, but the User has put the alert in Ignore state. Do not trigger any notification. Do not count these Alerts towards dashboard/current summary. A user can change state back to Active to start receiving alerts again.
- Acknowledged - An Alert is Active, but the User has acknowledged its existence. So do not trigger any notification. However, count these Alerts towards dashboard/current summary. A user can change state back to Active to start receiving alerts again.

Refresh Alerts will update the page with any changes.



Clicking on a Site or Device will drill-down to its respective entity detail's page.

Alerts  Apply Filter Configure Alerts

Active History

Resolve Ignore Acknowledge Refresh Alerts View Options

SEVERITY	SITE	DEVICE	DESCRIPTION	TIME OPENED	ACTIVE FOR	CATEGORY	TYPE
Critical	New York - DC	RTR_DC-MPLS	RTR_DC-MPLS running application citrix, had critical traffic with delay 74.44 ms	08 Feb 2021, 07:29AM	a few seconds	Application	Critical Traffic Res
Critical	LosAngeles	LiveWire	LiveWire running application citrix, had critical traffic with delay 74.44 ms	08 Feb 2021, 07:29AM	a few seconds	Application	Critical Traffic Res
Critical	New York - DC	RTR_DC-CORE	RTR_DC-CORE running application citrix, had critical traffic with delay 74.44 ms	08 Feb 2021, 07:29AM	a few seconds	Application	Critical Traffic Res
Critical	LosAngeles	LiveWire	LiveWire running application rtp had 47.05 % of packet loss for traffic with a DSCP value of 0 (BE)	08 Feb 2021, 07:29AM	a few seconds	Application	Voice/Video Perf
Warning	Seattle	RTR_Seattle	RTR_Seattle QoS Class VIDEO Drop Rate was 34.38 Kbps	08 Feb 2021, 07:28AM	a few seconds	Device, Interface	QoS Class Drop
Warning	PaloAlto-VE-01	RTR_SanJose	RTR_SanJose QoS Class SET_DSCP_VOICE Drop Rate was 82.52 Kbps	08 Feb 2021, 07:28AM	a few seconds	Device, Interface	QoS Class Drop
Warning	Site 5	RTR_Austin.liveaction.com	RTR_Austin.liveaction.com QoS Class VOICE Drop Rate was 2.54 Kbps	08 Feb 2021, 07:28AM	a few seconds	Device, Interface	QoS Class Drop
Critical	LosAngeles	RTR_LosAngeles.liveaction.com	RTR_LosAngeles.liveaction.com had 161.65 ms network delay for the application pespn.chartbeat	08 Feb 2021, 07:28AM	a minute	Application	Application Perfo
Critical	LosAngeles	LiveWire	LiveWire running application rtp-audio had 50.94 % of packet loss for traffic with a DSCP value of 0 (L)	08 Feb 2021, 07:27AM	a minute	Application	Voice/Video Perf
Critical	New York - DC	RTR_DC-MPLS	RTR_DC-MPLS running application VoIP had 200.00 ms of jitter for traffic with a DSCP value of 0 (L)	08 Feb 2021, 07:27AM	a minute	Application	Voice/Video Perf
Critical	Seattle	RTR_Seattle	RTR_Seattle running application VoIP had 62.65 ms of jitter for traffic with a DSCP value of 46 (EF)	08 Feb 2021, 07:22AM	6 minutes	Application	Voice/Video Perf
Critical	LosAngeles	RTR_LosAngeles.liveaction.com	RTR_LosAngeles.liveaction.com IP SLA Voice/Jitter total errors is greater than threshold value: 3	08 Feb 2021, 07:18AM	10 minutes	Network	IP SLA Voice/Jitte

LiveAction Nov 30, 2020 13:50:00 - Nov 30, 2020 14:05:00 15 Min

Sites > Site: Birmingham

**Birmingham** Status: Critical

100% Availability 2 Devices 4 Interfaces 54 WAN Applications 8222 Active Alerts

Site Details

Service Provider Bandwidth (Inbound)

Legend: Service Provider, Flows, Bytes, Packets, Bit Rate, Packet Rate

Service Provider Bandwidth (Outbound)

https://selemo2.liveaction.com

Map showing RTR\_Birmingham1.liveaction.com and RTR\_PaloAlto-Wan.

Alerts  Apply Filter Configure Alerts

Active History

Resolve Ignore Acknowledge Refresh Alerts View Options

SEVERITY	SITE	DEVICE	DESCRIPTION	TIME OPENED	ACTIVE FOR	CATEGORY	TYPE
Critical	New York - DC	RTR_DC-MPLS	RTR_DC-MPLS running application citrix, had critical traffic with delay 74.44 ms	08 Feb 2021, 07:29AM	a few seconds	Application	Critical Traffic Res
Critical	LosAngeles	LiveWire	LiveWire running application citrix, had critical traffic with delay 74.44 ms	08 Feb 2021, 07:29AM	a few seconds	Application	Critical Traffic Res
Critical	New York - DC	RTR_DC-CORE	RTR_DC-CORE running application citrix, had critical traffic with delay 74.44 ms	08 Feb 2021, 07:29AM	a few seconds	Application	Critical Traffic Res
Critical	LosAngeles	LiveWire	LiveWire running application rtp had 47.05 % of packet loss for traffic with a DSCP value of 0 (BE)	08 Feb 2021, 07:29AM	a few seconds	Application	Voice/Video Perf
Warning	Seattle	RTR_Seattle	RTR_Seattle QoS Class VIDEO Drop Rate was 34.38 Kbps	08 Feb 2021, 07:28AM	a few seconds	Device, Interface	QoS Class Drop
Warning	PaloAlto-VE-01	RTR_SanJose	RTR_SanJose QoS Class SET_DSCP_VOICE Drop Rate was 82.52 Kbps	08 Feb 2021, 07:28AM	a few seconds	Device, Interface	QoS Class Drop
Warning	Site 5	RTR_Austin.liveaction.com	RTR_Austin.liveaction.com QoS Class VOICE Drop Rate was 2.54 Kbps	08 Feb 2021, 07:28AM	a few seconds	Device, Interface	QoS Class Drop
Critical	LosAngeles	RTR_LosAngeles.liveaction.com	RTR_LosAngeles.liveaction.com had 161.65 ms network delay for the application pespn.chartbeat	08 Feb 2021, 07:28AM	a minute	Application	Application Perfo
Critical	LosAngeles	LiveWire	LiveWire running application rtp-audio had 50.94 % of packet loss for traffic with a DSCP value of 0 (L)	08 Feb 2021, 07:27AM	a minute	Application	Voice/Video Perf
Critical	New York - DC	RTR_DC-MPLS	RTR_DC-MPLS running application VoIP had 200.00 ms of jitter for traffic with a DSCP value of 0 (L)	08 Feb 2021, 07:27AM	a minute	Application	Voice/Video Perf
Critical	Seattle	RTR_Seattle	RTR_Seattle running application VoIP had 62.65 ms of jitter for traffic with a DSCP value of 46 (EF)	08 Feb 2021, 07:22AM	6 minutes	Application	Voice/Video Perf
Critical	LosAngeles	RTR_LosAngeles.liveaction.com	RTR_LosAngeles.liveaction.com IP SLA Voice/Jitter total errors is greater than threshold value: 3	08 Feb 2021, 07:18AM	10 minutes	Network	IP SLA Voice/Jitte

LiveAction Nov 30, 2020 13:50:00 - Nov 30, 2020 14:05:00 15 Min

Sites > Birmingham > Device: RTR\_Birmingham1

**RTR\_Birmingham1** Status: Critical IP Address: 19.199.81.7

Current Flows 100% Availability 2 Interfaces 54 WAN Application 6821 Active Alerts

Device Details

Device CPU/Memory Usage

Legend: Name, Avg, Peak

CPU Usage	5%	6%
Memory Usage	10%	15%

Top Applications (Inbound)

Top Applications (Outbound)

Map showing RTR\_Birmingham1.liveaction.com and RTR\_PaloAlto-Wan.

Clicking on the Alert description will provide more information about the Alert's details.

The Alerts dashboard shows a list of active alerts. A detailed view for a 'Voice/Video Performance - Packet Loss' alert is shown on the right. The alert details include:

- Status & Time:** Status: Active, Time opened: 30 Nov 2020, 01:50PM, Active for: 6 minutes.
- Source Info:** Region: Birmingham, Alabama, United States, North America; Site: Birmingham; Device: RTR\_Birmingham1.liveaction.com; Conversation: UDP 192.168.102.113:1196 to 192.168.10.13:19422; Source Site: Birmingham; Destination Site: DC-New\_York; Event: Report.
- Description:** RTR\_Birmingham1.liveaction.com running application VoIP had 8.15 % of packet loss for traffic with a DSCP value of 0 (BE).
- Details:** Latest dscp: 0 (BE), Latest configured threshold: 1 %, Latest packet loss: 0.44 %, Latest application: VoIP.

Most alerts provide drill-downs to insight. These include:

- Site Details

The LiveAction dashboard shows Site Details for Birmingham. The site status is Critical. Key metrics include:

- Availability: 100%
- Devices: 2
- Interfaces: 4
- WAN Applications: 54
- Active Alerts: 8222

The Site Details section includes a Service Provider Bandwidth (Inbound) chart and a Service Provider Bandwidth (Outbound) chart. The legend for the charts includes:

- Service Provider
- Flows
- Bytes
- Packets
- Bit Rate
- Packet Rate

- Interface Details

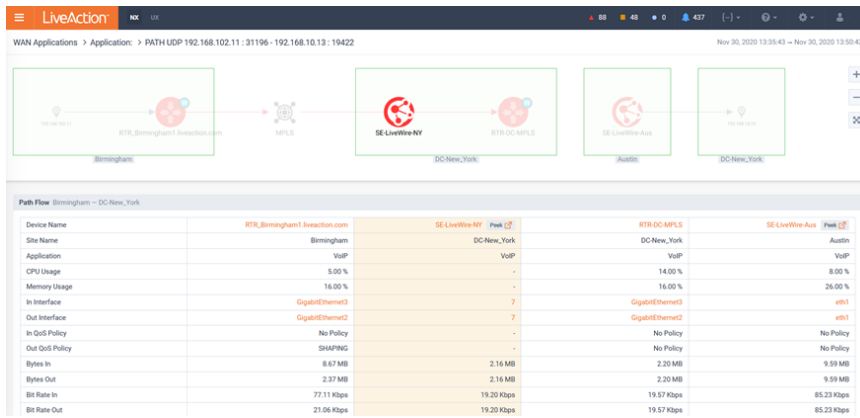
The LiveAction dashboard shows Interface Details for RTR\_Birmingham1. The device status is Critical. Key metrics include:

- Current Flows: 100%
- Interfaces: 2
- WAN Application: 54
- Active Alerts: 6821

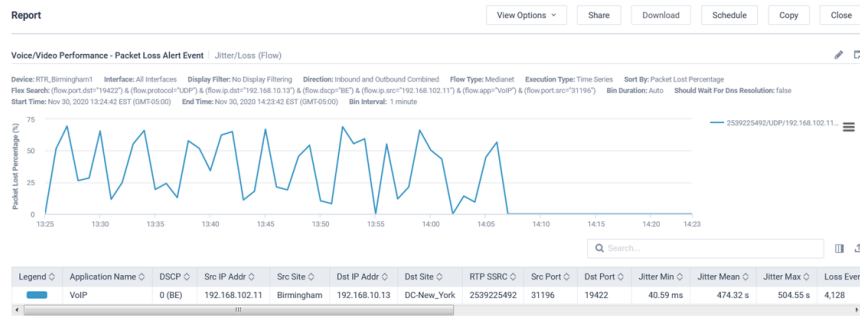
The Interface Details section includes a Device CPU/Memory Usage chart and a Top Applications (Inbound) chart. The legend for the charts includes:

- CPU Usage
- Memory Usage
- Name
- Avg
- Peak

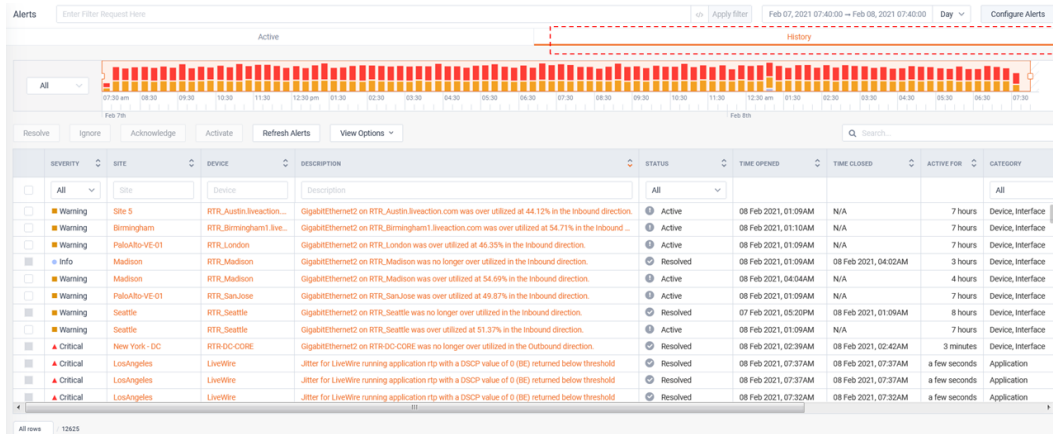
- Flow Path Analysis



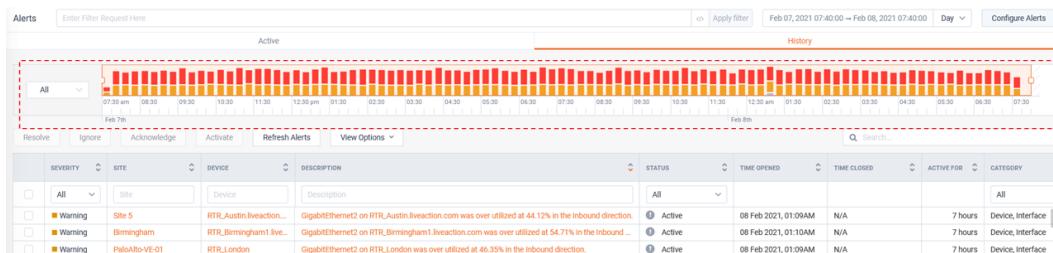
• Historic Report(s)



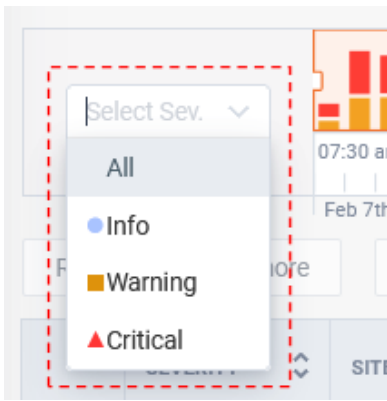
The Alerts *History* tab will present any resolved Alerts known to the system.



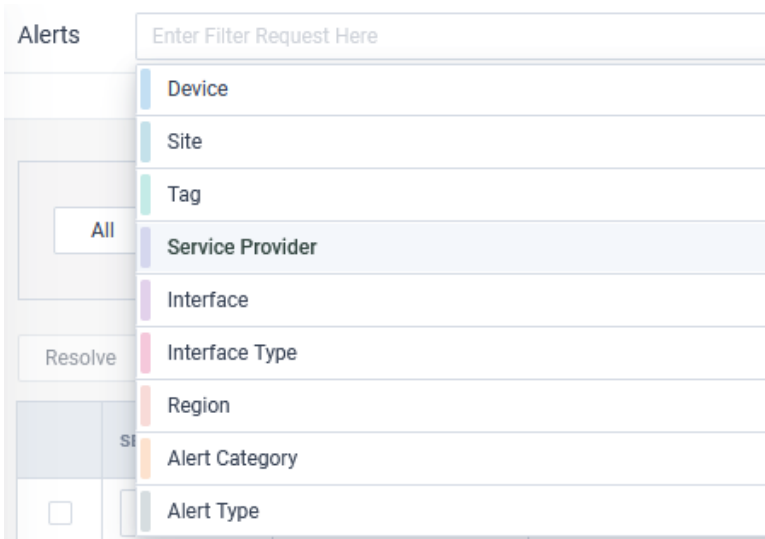
A timeline is available to understand the Alerts over time.



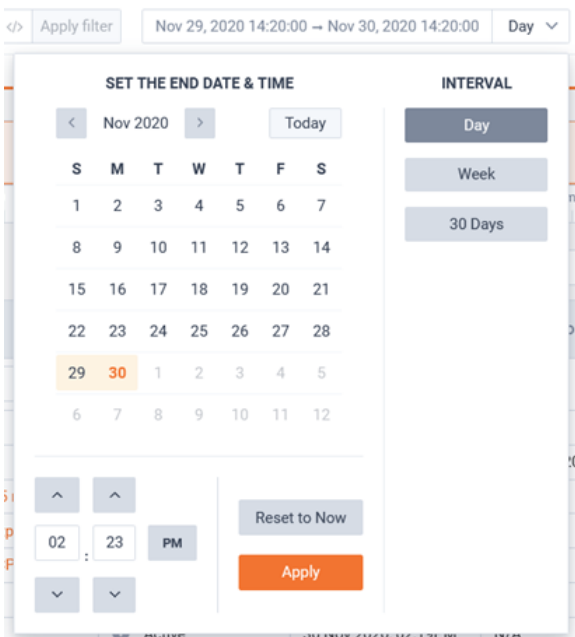
The timeline can be filtered by Alert severity.



Filters can be applied to focus on alerts of interest.



Historic data can be explored on the Alerts *History* tab.

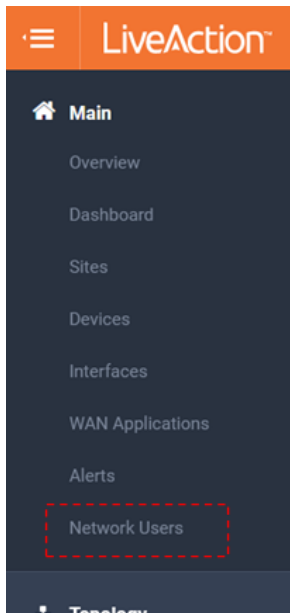


If authorized, the **Configure Alerts** button will be available for managing the configuration of Alerts. Please see *LiveNX Admin Guide* for further information regarding the configuration of Alerts.

SEVERITY	SITE	DEVICE	DESCRIPTION	TIME OPENED	ACTIVE FOR	CATEGORY	TYPE
Critical	Seattle	RTR_Seattle	RTR_Seattle running application VoIP had 38.49 % of packet loss for traffic with a DSCP value of 0...	30 Nov 2020, 01:50PM	a few seconds	Application	Voice/Video Perf...
Critical	Seattle	RTR_Seattle	RTR_Seattle running application VoIP had voice/video traffic with 32.16 ms max jitter 38.49% pack...	30 Nov 2020, 01:50PM	a few seconds	Application	Voice/Video app...
Critical	Seattle	RTR_Seattle	RTR_Seattle running application VoIP had 56.86 % of packet loss for traffic with a DSCP value of 4...	30 Nov 2020, 01:50PM	a few seconds	Application	Voice/Video Perf...
Critical	Seattle	RTR_Seattle	RTR_Seattle running application VoIP had 32.16 ms of jitter for traffic with a DSCP value of 0 (BE)	30 Nov 2020, 01:50PM	a few seconds	Application	Voice/Video Perf...
Critical	Seattle	RTR_Seattle	Voice traffic for RTR_Seattle running application Video is not marked as DSCP EF	30 Nov 2020, 01:50PM	a few seconds	Application	Voice Traffic Clas...
Critical	Birmingham	RTR_Birmingham1.live...	Voice traffic for RTR_Birmingham1.liveaction.com running application VoIP is not marked as DSC...	30 Nov 2020, 01:50PM	a few seconds	Application	Voice Traffic Clas...
Critical	Seattle	RTR_Seattle	RTR_Seattle running application VoIP had 33.76 ms of jitter for traffic with a DSCP value of 46 (EF)	30 Nov 2020, 01:50PM	a few seconds	Application	Voice/Video Perf...
Critical	Los_Angeles	RTR_LosAngeles.livea...	RTR_LosAngeles.liveaction.com IP SLA Voice/Jitter total errors is greater than threshold value: 3	30 Nov 2020, 01:50PM	a few seconds	Network	IP SLA Voice/Jitt...
Critical	Los_Angeles	RTR_LosAngeles.livea...	RTR_LosAngeles.liveaction.com IP SLA Voice/Jitter total errors is greater than threshold value: 3	30 Nov 2020, 01:50PM	a few seconds	Network	IP SLA Voice/Jitt...
Critical	Los_Angeles	RTR_LosAngeles.livea...	RTR_LosAngeles.liveaction.com CPU utilization is above threshold	30 Nov 2020, 01:50PM	a few seconds	Device, Interface	Device CPU Utiliz...
Critical	Los_Angeles	RTR_LosAngeles.livea...	RTR_LosAngeles.liveaction.com running application VoIP had 10.96 % of packet loss for traffic wit...	30 Nov 2020, 01:50PM	a few seconds	Application	Voice/Video Perf...
Critical	Los_Angeles	RTR_LosAngeles.livea...	RTR_LosAngeles.liveaction.com running application VoIP had 28.33 ms of jitter for traffic with a D...	30 Nov 2020, 01:50PM	a few seconds	Application	Voice/Video Perf...
Critical	Los_Angeles	WLC.NetflowReplay	Voice traffic for WLC.NetflowReplay running application dns is not marked as DSCP EF	30 Nov 2020, 01:50PM	a few seconds	Application	Voice Traffic Clas...

## Network Users

Manual exploration of Network Users can be done via the Main menu navigation bar.



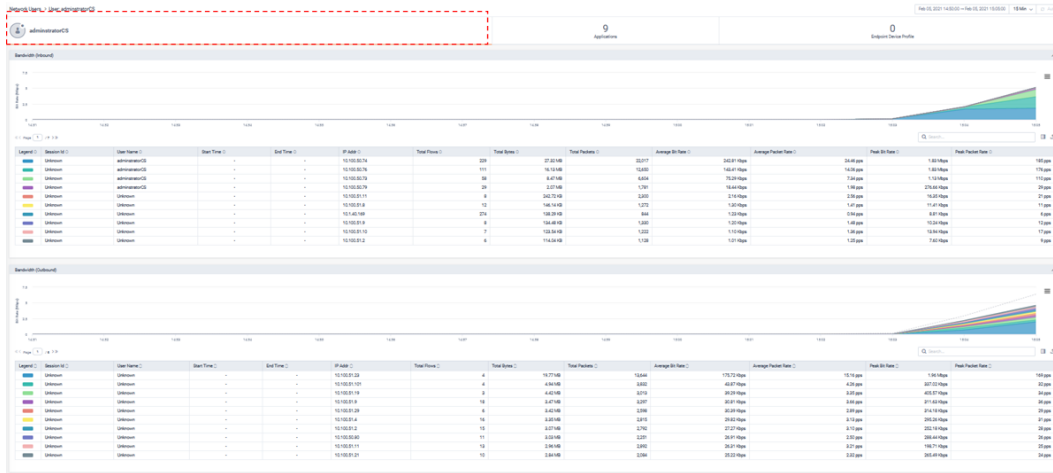
The Network Users summary page provides a list of all detected networks users and stats of their network activity. Clicking on a specific user will drill-down to its details page.

USER NAME	DEVICE COUNT	APPLICATION COUNT	SESSION COUNT	TOTAL FLOWS	TOTAL BYTES	TOTAL PACKETS	AVERAGE BIT RATE	AVERAGE PACKET RATE
Unknown	0	8	0	422	41.63 MB	34,204	370.04 Kbps	38.00 pps
administratorCS	0	7	0	358	17.09 MB	17,165	151.95 Kbps	19.07 pps
AnyConnect AnyConnect	0	1	0	15	8.58 MB	5,916	76.28 Kbps	6.57 pps

The status tab of the Device page provides a curated list of reports for quick understanding of the Devices' Status.

These reports include:

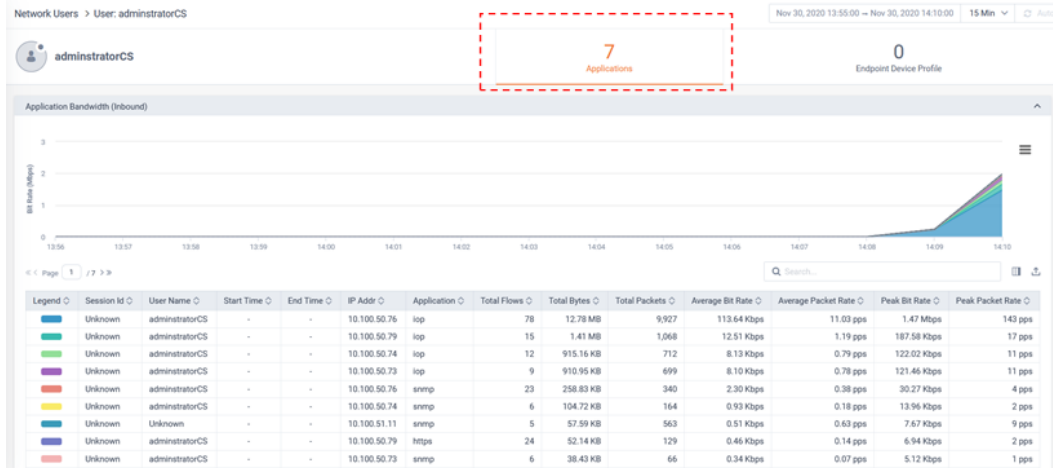
- Bandwidth (Inbound)
- Bandwidth (Outbound)



The *Applications* tab shows a curated list of reports for quick understanding of the Network Users application performance.

These reports include:

- Application Bandwidth (Inbound)
- Application Bandwidth (Outbound)
- Application Audio/Video Issues Summary (Inbound)
- Application Audio/Video Issues Summary (Outbound)
- Application Audio/Video Issues Detail (Inbound)
- Application Audio/Video Issues Detail (Outbound)
- Application HTTP/TCP Issues Summary (Inbound)
- Application HTTP/TCP Issues Summary (Outbound)
- Application HTTP/TCP Issues Detail (Inbound)
- Application HTTP/TCP Issues Detail (Outbound)



The *Endpoint Device Profile* tab shows a curated list of the devices utilizing the network by user.



Network Users > User: dhaivat Jul 03, 2018 16:40:00 – Jul 03, 2018 16:55:00 15 Min Auto

**dhaivat** 17 Applications 2 Endpoint Device Profile

ENDPOINT PROFILE	IP ADDRESS	SESSION ID	MAC ADDRESSES	STATE	LAST UPDATE TIME
All	IP Address	Session ID	All	All	
Unknown	10.1.51.110	0233010a0000018f58a1fd5a	7C:67:A2:ED:BC:6E	STARTED	May 17, 2018 21:06:03 (GMT+05:30)
Apple-Device	10.1.51.102	0233010a000003519c7a3a5b	24:A0:74:09:6C:12	STARTED	Jul 03, 2018 00:48:52 (GMT+05:30)

10 rows / 2 1 / 1

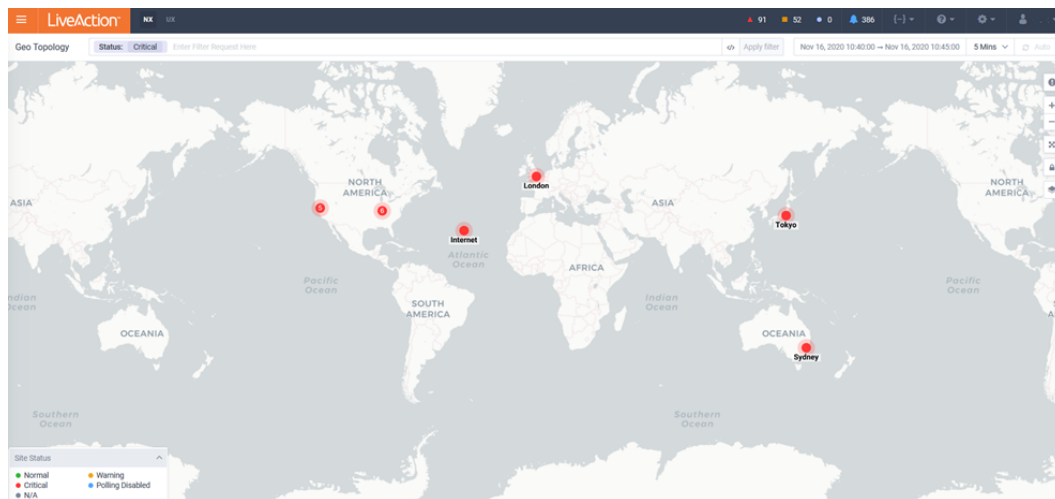
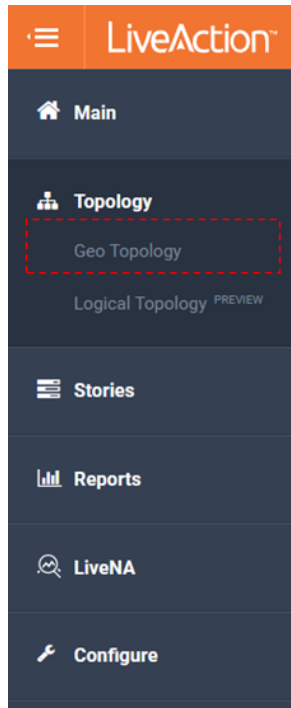
## Topology

### In this chapter:

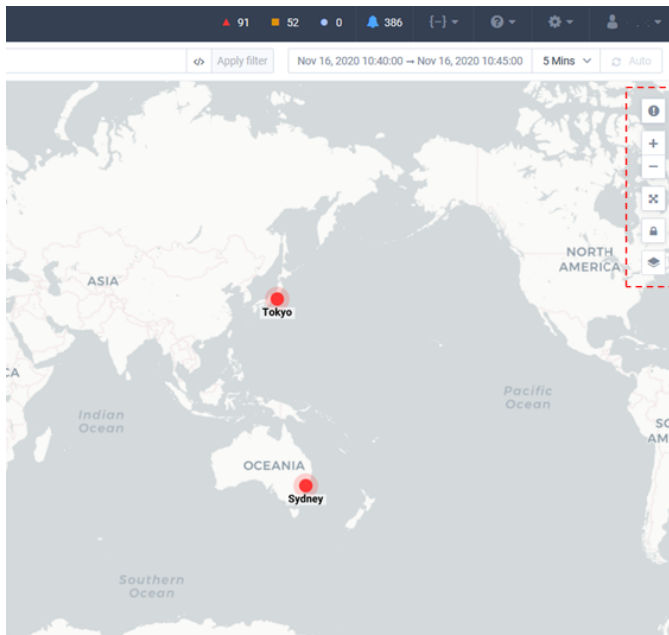
<i>Geo Topology</i> .....	60
<i>Logical Topology</i> .....	72

## Geo Topology

The *Geo Topology* provides an overview of the sites monitored by LiveNX. It can be used for understanding site status, projecting application traffic between sites and monitoring SDWAN.



The icons to the upper right of the map provide context to what is shown on the topology.



The *Current Alerts* icon will provide a list of the most recent active Alerts. Clicking on an alert will provide more details and drill-down to additional data.

Feb 03, 2021 12:35:00 → Feb 03, 2021 12:40:00 5 Mins Auto

Location	Alert Type	Time
Seattle	QoS Class Drop	12:53 PM
Los_Angeles	Voice/Video Performance - Jitter Max	12:53 PM
DC-New_York	Application Performance - Network Delay	12:40 PM
DC-New_York	Application Performance - Network Delay	12:40 PM
Austin	Voice/Video Performance - Jitter Max	12:39 PM
DC-New_York	Voice/Video Performance - Packet Loss	12:30 PM

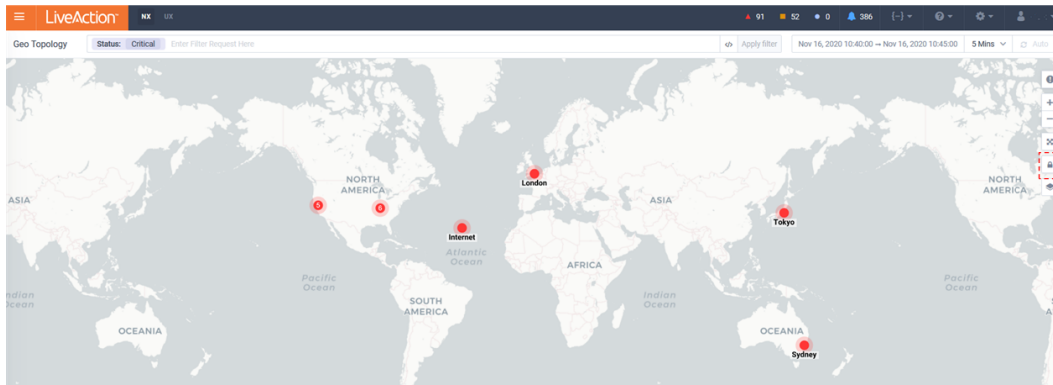
The screenshot displays the LiveNX Operations Dashboard interface. At the top, there is a navigation bar with a filter icon, the text 'Apply filter', a time range 'Feb 03, 2021 12:35:00 → Feb 03, 2021 12:40:00', a duration of '5 Mins', and an 'Auto' refresh button. Below this, the main content area is split into two panels. The left panel shows a map of North America with a red dot labeled 'Internet' and a red circle with a white 'P' and a red arrow pointing to it. The right panel is titled 'DC-New\_York' and 'Application Performance - Network Delay'. It contains several sections: 'Status & Time' with fields for State (Active), Time Opened (03 Feb 2021, 12:40PM), and Active for (20 minutes); 'Source Info' with fields for Region (New York, New York, United States, North America), Site (DC-New\_York), Device (RTR-DC-CORE), Conversation (TCP 72.234.37.49 to 23.203.227.121:443), Source Site (Internet), Destination Site (Internet), and Event (Report); 'Description' with the text 'RTR-DC-CORE had 434.86 ms network delay for the application ms-office-365'; and 'Details'.

The below icons allow you to focus on the desired area of the map.

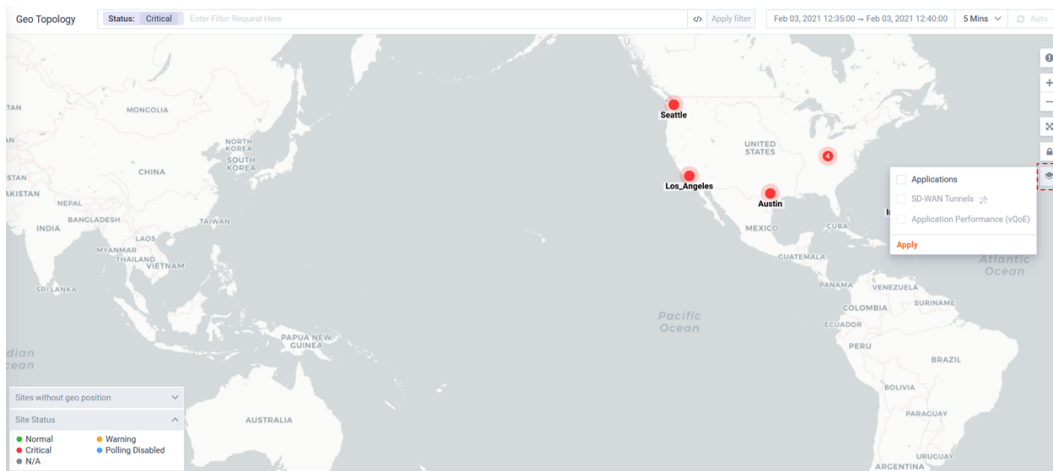
- Zoom In
- Zoom Out
- Zoom Fit

This screenshot shows the LiveNX Operations Dashboard interface with a different time range: 'Nov 16, 2020 10:40:00 → Nov 16, 2020 10:45:00'. The map on the left shows a red dot labeled 'Tokyo' in East Asia. On the right side of the map, a vertical toolbar contains several icons. A red dashed box highlights the 'Zoom In' (+), 'Zoom Out' (-), and 'Zoom Fit' (⊞) icons. The rest of the dashboard interface, including the top navigation bar, is consistent with the previous screenshot.

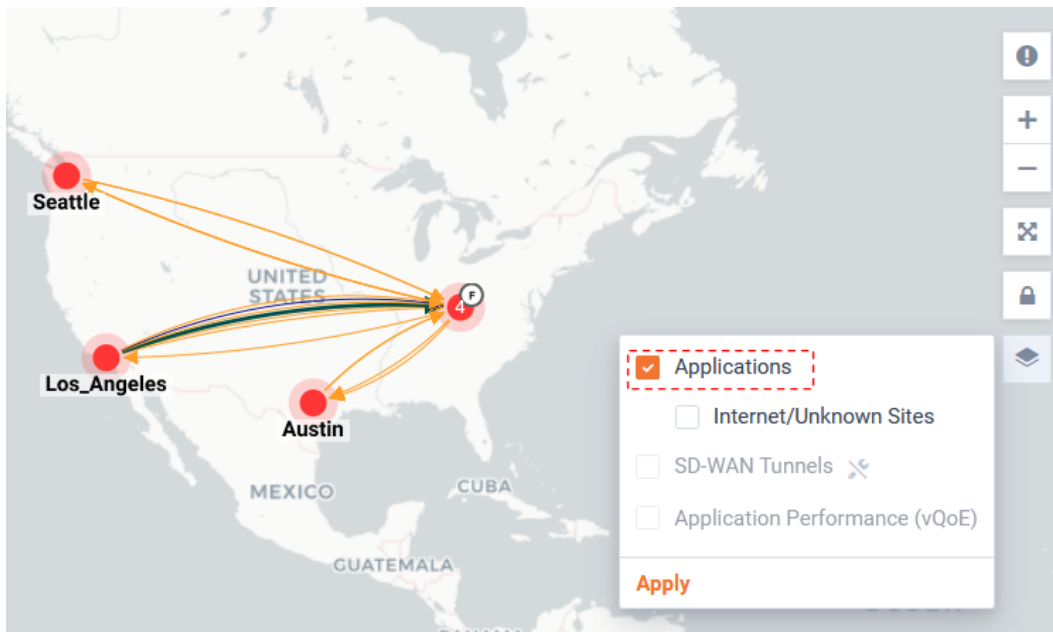
When the Toggle Layout Lock is unlocked, it allows you to click-and-drag a Site icon to the position desired. If geo location has been configured for a Site, the Site will default to the Site's geo-coordinates.



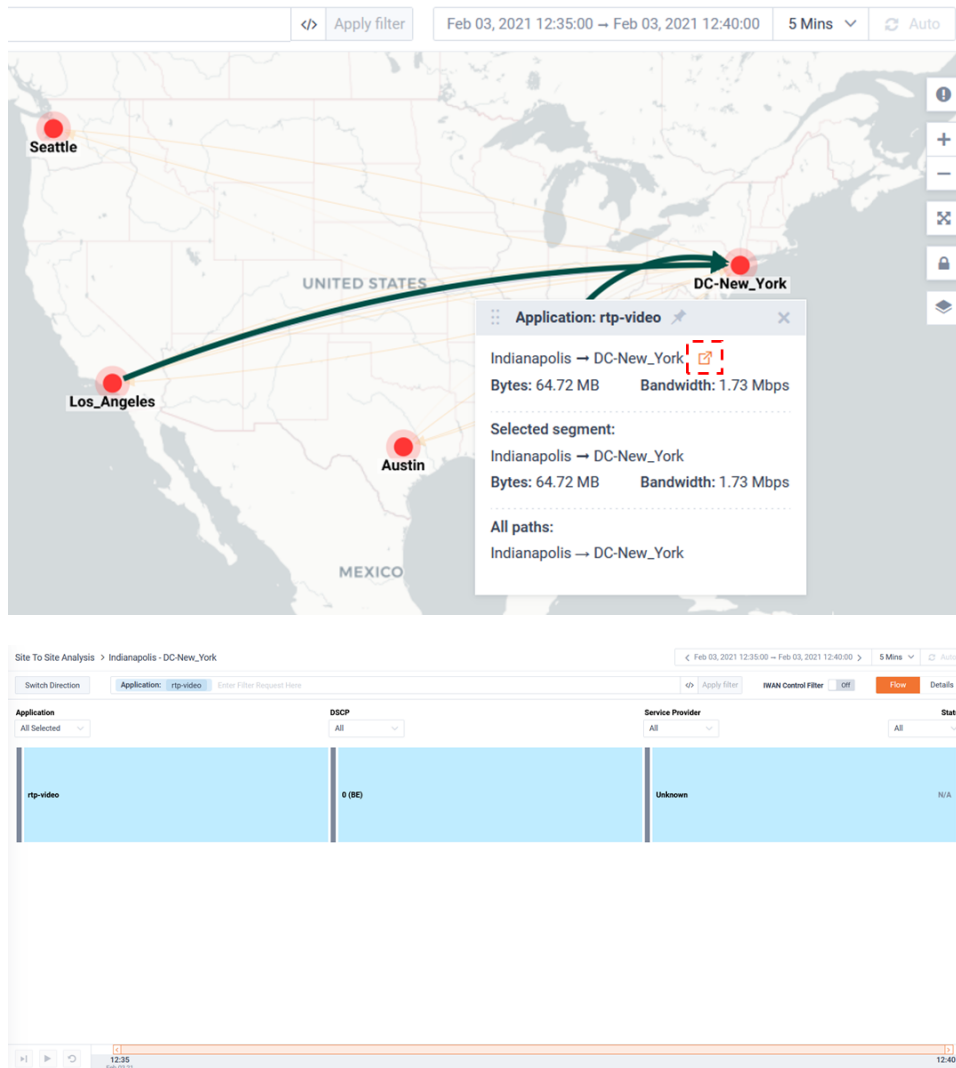
The *Toggle Display Mode* icon controls what technologies area overlaid on the Geo Map.



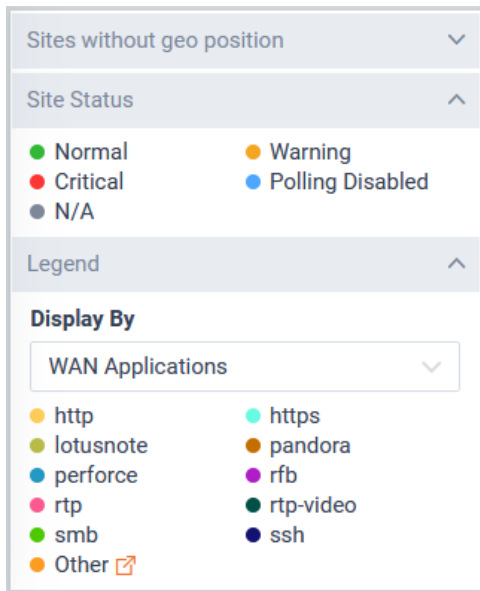
*Applications* will overlay application traffic on the Geo Map.



By clicking on the Application traffic of interest, a pop-up will show details of the Flow. Click on the cross-launch icon will open a curated Sankey diagram on a new browser tab.



The Legend can be updated to select the context to show the application data.



Sites without geo position

Site Status

- Normal
- Critical
- N/A
- Warning
- Polling Disabled

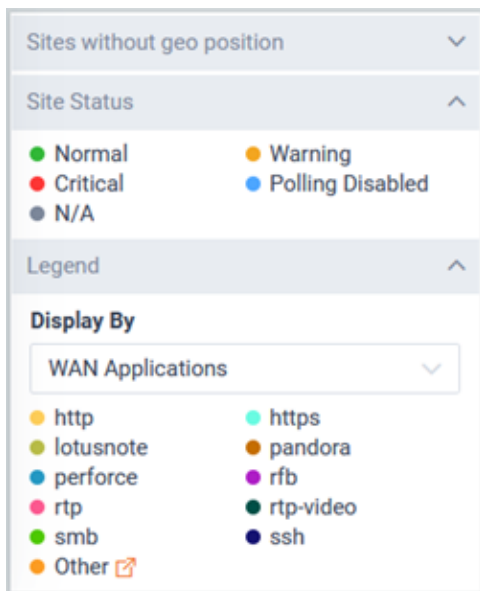
Legend

Display By

WAN Applications

- http
- lotusnote
- perforce
- rtp
- smb
- Other
- https
- pandora
- rfb
- rtp-video
- ssh

The Legend can be updated to select the context to show the Application traffic. In this example the *Display By* is set to *WAN Applications*.



Sites without geo position

Site Status

- Normal
- Critical
- N/A
- Warning
- Polling Disabled

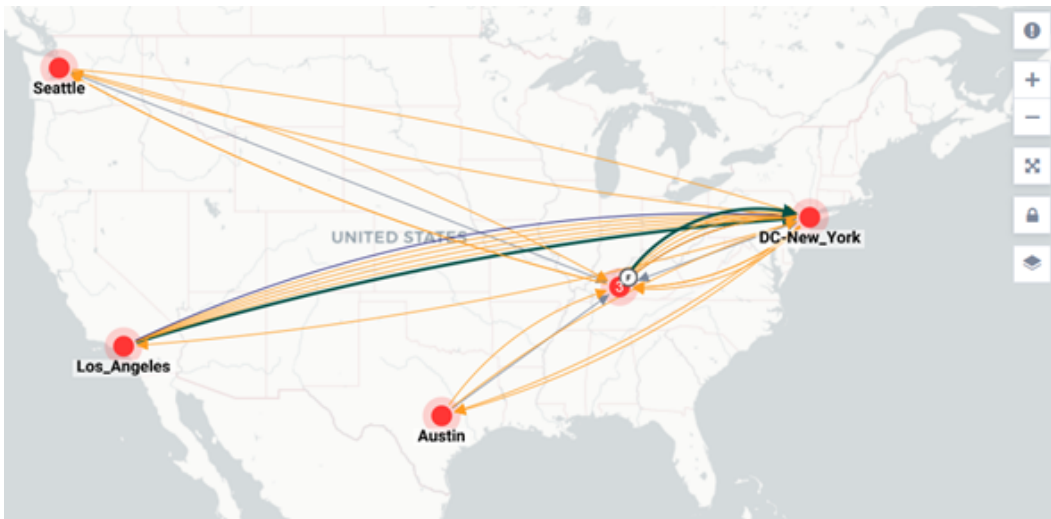
Legend

Display By

WAN Applications

- http
- lotusnote
- perforce
- rtp
- smb
- Other
- https
- pandora
- rfb
- rtp-video
- ssh





In this example the *Display By* is set to *Service Provider*.

Sites without geo position v

---

Site Status ^

- Normal
- Critical
- N/A
- Warning
- Polling Disabled

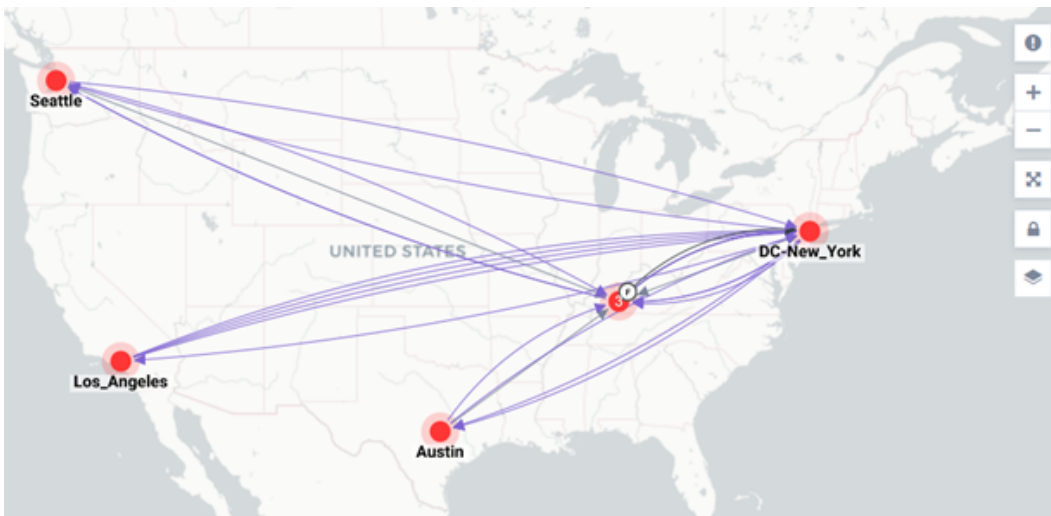
---

Legend ^

**Display By**

Service Provider v

- INET
- MPLS
- Unknown



In this example the *Display By* is set to *DSCP*.

Sites without geo position ▼

Site Status ▲

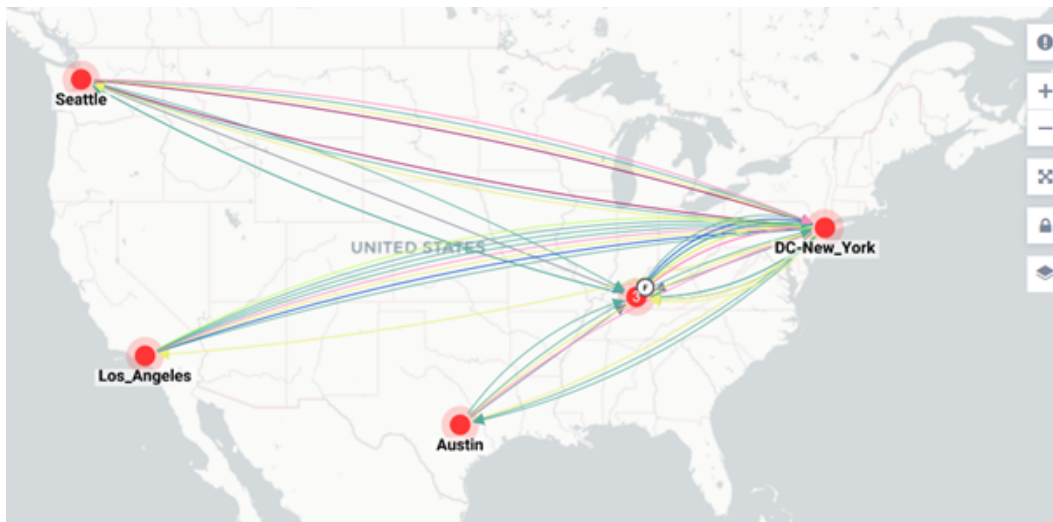
- Normal
- Critical
- N/A
- Warning
- Polling Disabled

Legend ▲

Display By

DSCP ▼

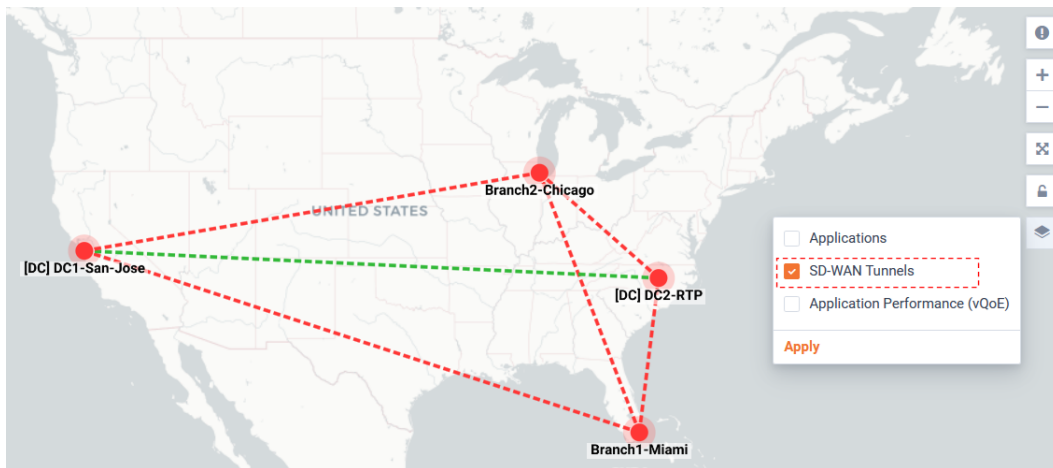
- 0 (BE)
- 18 (AF21)
- 26 (AF31)
- 46 (EF)
- 63
- Other
- 16 (CS2)
- 24 (CS3)
- 34 (AF41)
- 48 (CS6)
- 8 (CS1)



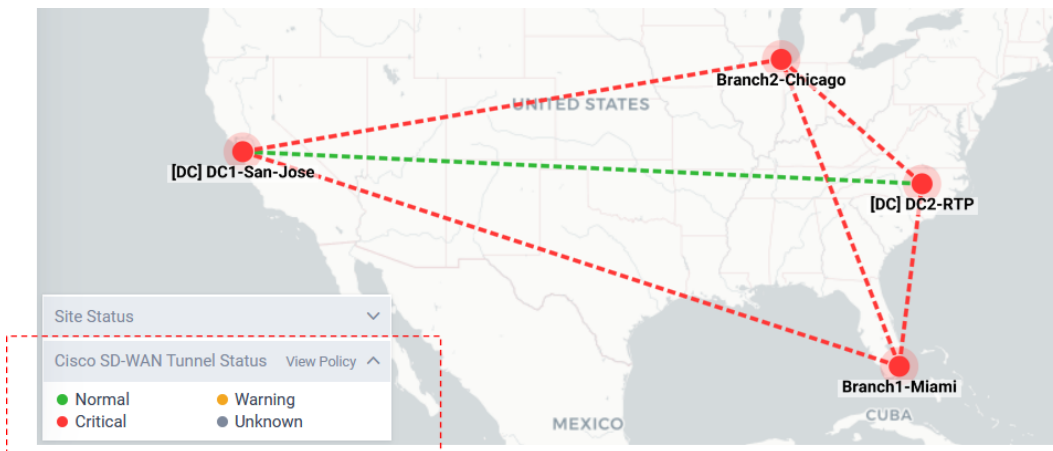
Internet/Unknown will toggle showing applicable icons for each site sending Flow to either Internet or Unknown sites.



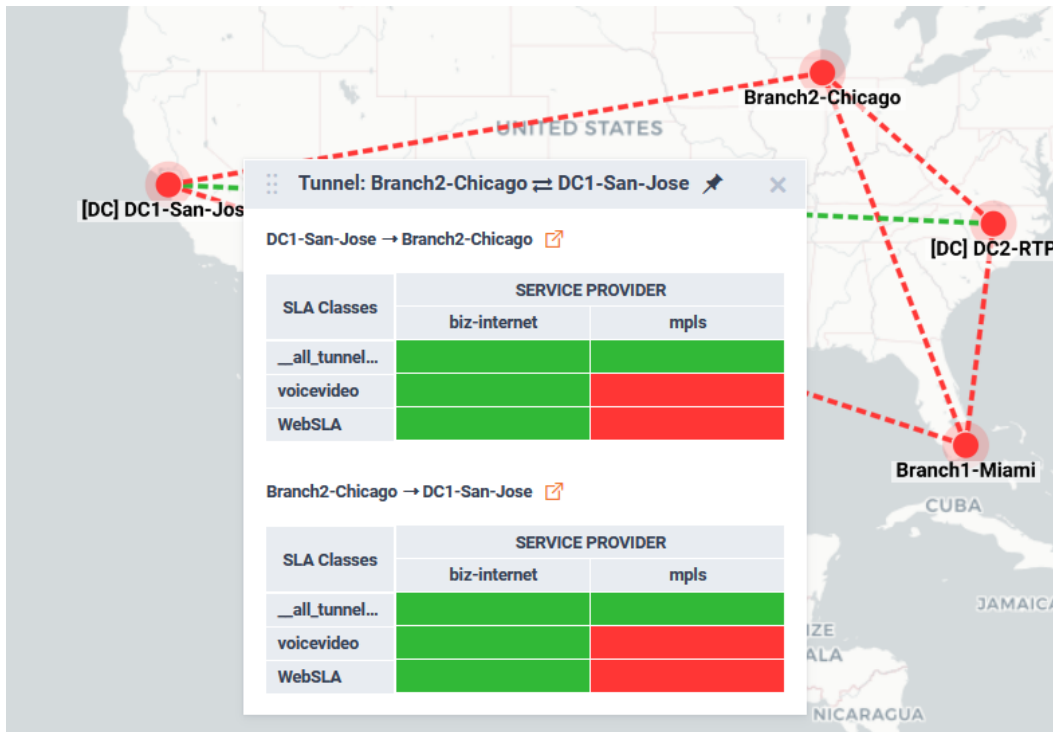
SD-WAN will toggle showing SDWAN tunnels between sites.



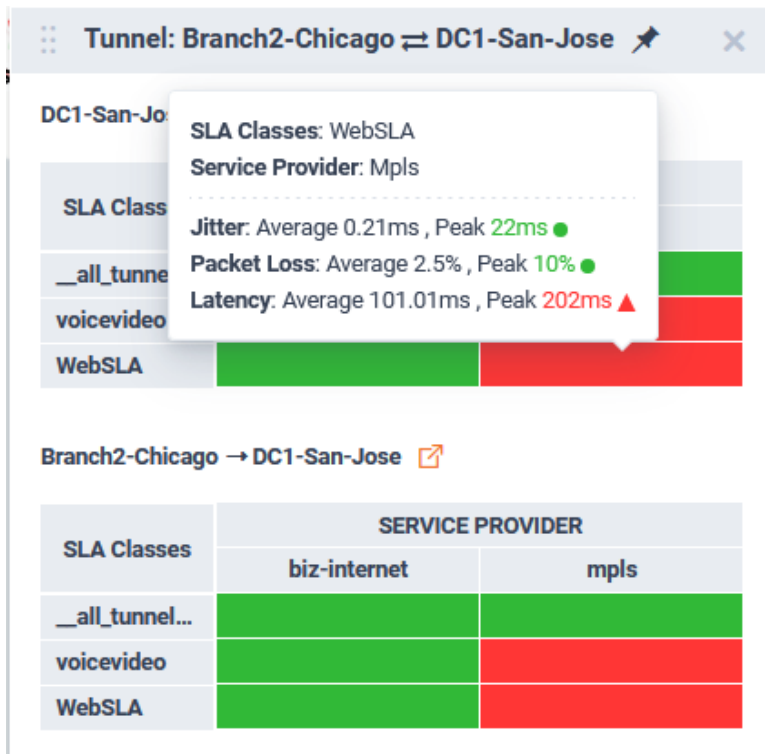
Tunnels are color coded by status.

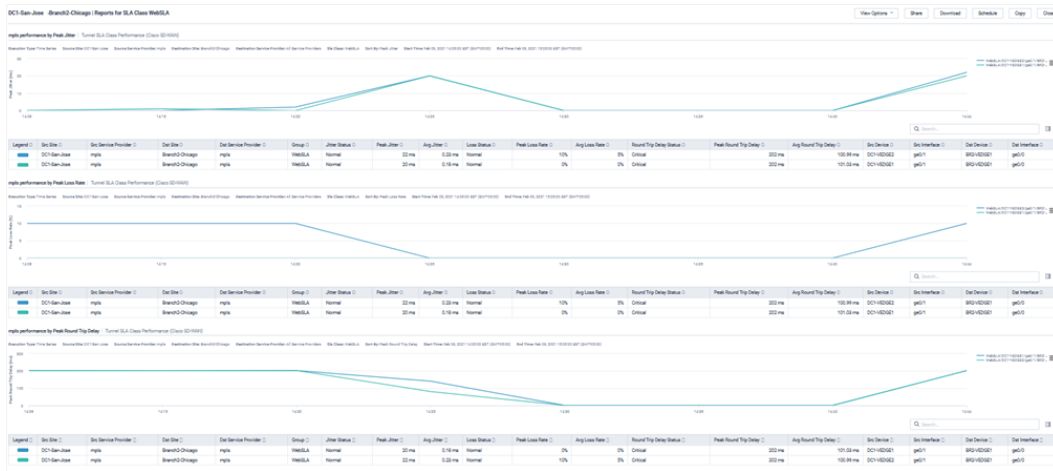


Clicking on a tunnel, will pop-up summary details about the tunnel status.



Hovering over a *SLA Class/ Service Provider* status block will provide more details. Clicking on the status block will open a curated SDWAN report highlight Jitter, loss, and delay metrics for the tunnel.





Clicking on a tunnels pop-up icon will open a Sankey diagram for the tunnel.

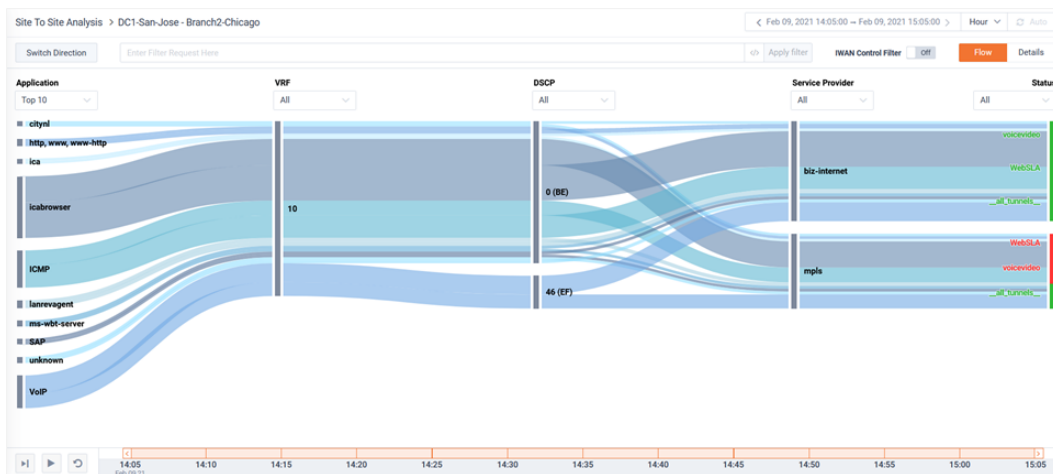
Tunnel: Branch2-Chicago ⇌ DC1-San-Jose

DC1-San-Jose → Branch2-Chicago

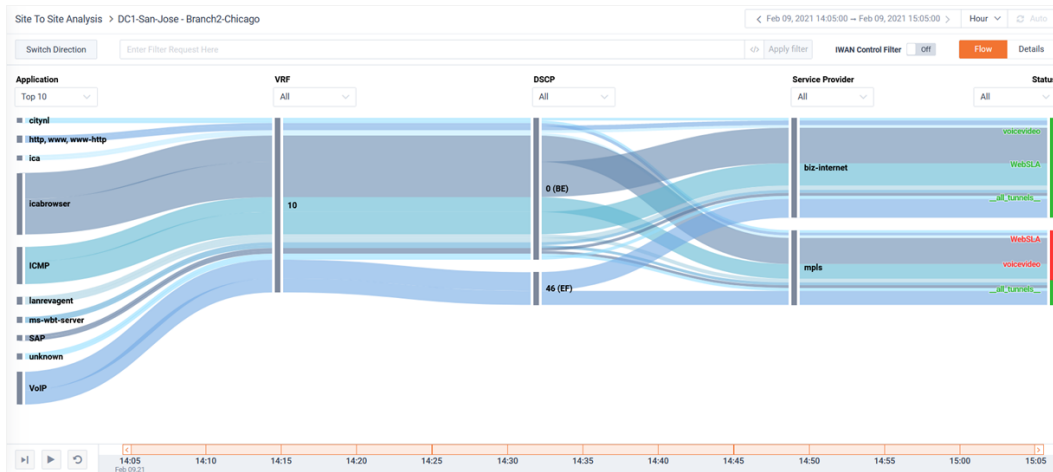
SLA Classes	SERVICE PROVIDER	
	biz-internet	mpls
__all_tunnel...	Green	Green
voicevideo	Green	Red
WebSLA	Green	Red

Branch2-Chicago → DC1-San-Jose

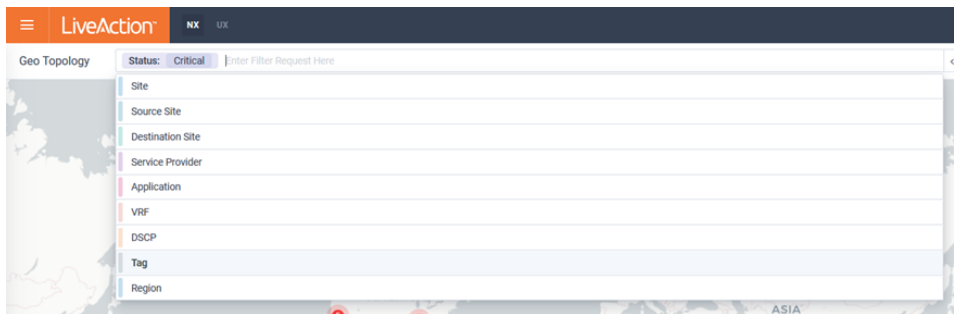
SLA Classes	SERVICE PROVIDER	
	biz-internet	mpls
__all_tunnel...	Green	Green
voicevideo	Green	Red
WebSLA	Green	Red



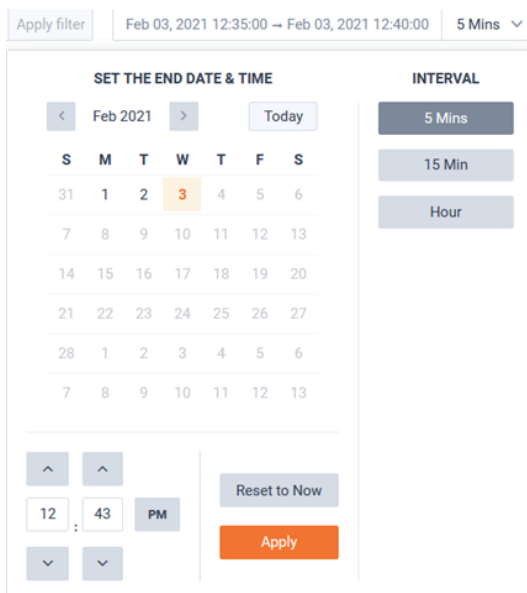
This Sankey is curated to focus on SDWAN performance. The Sankey diagram highlights the applications, the VRF, their DSCP, the service provider path the application took, and its status. For more details for the options of the Sankey page please refer to the Site To Site Analysis Story.



Filtering can be applied to find the specific Flows, Tunnels, and/or sites with specific status of interests.



Historic time ranges can be selected for finding the Flows of interests.



The page can optionally be auto-refreshed by toggling the Auto button in the top right of the page.

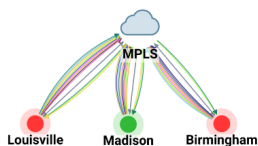


## Logical Topology

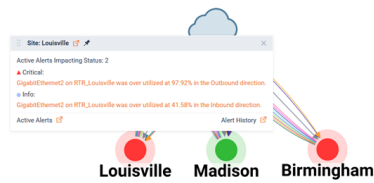
LiveNX *Logical Topology* is a virtual interactive network diagram that provides enhanced situational awareness. It represents selected devices and sites of interest and their LAN and WAN networks connecting them. The topology projects Application traffic to visualize the path traffic traverses the network. Multiple tabs can be created and shared to build manageable, personalized use cases of interest.

The screenshot displays the LiveAction dashboard's Logical Topology interface. The sidebar on the left contains navigation links for Main, Topology (with sub-links for Geo Topology and Logical Topology PREVIEW), Stories, Reports, LiveNA, and Configure. The main content area features a 'Logical Topology' view with a search bar, a filter for 'Selected sites and devices shown on topology', and a list of sites: Birmingham, Louisville, and Madison. A legend for 'Site Status' and 'WAN Applications' is visible. The central diagram shows three sites (Louisville, Madison, Birmingham) connected to a central cloud labeled 'MPLS'.

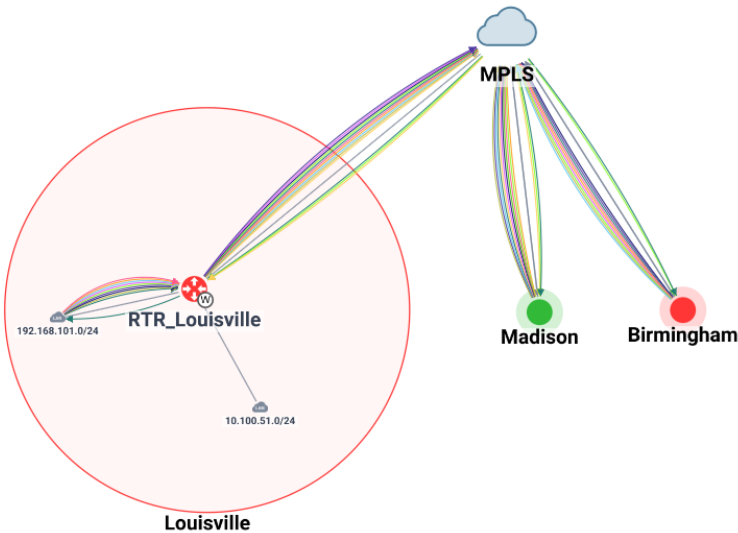
The example below shows three sites: *Louisville*, *Madison*, and *Birmingham*. They are interconnected via a WAN cloud called *MPLS*.



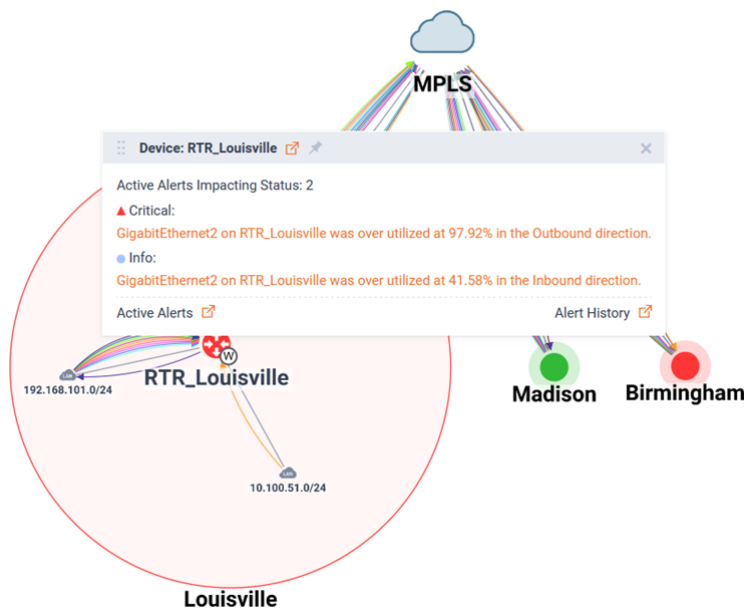
By single-clicking on the site *Louisville*, a pop-up will show the status of the object and provide links for more information.



By double-clicking on the site icon of *Louisville*, the icon will expand to show the site's selected devices. Application traffic will also be projected within the LAN.

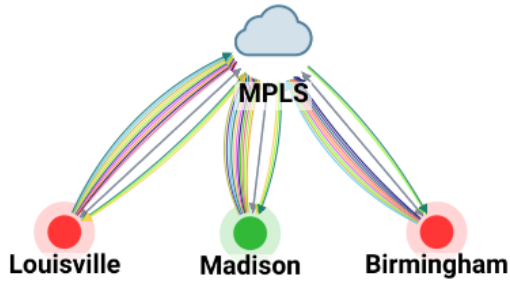


By single-clicking on the device *RTR\_Louisville*, a pop-up will show the status of the object and provide links for more information.



Double-clicking on the *Louisville* site will return it back to a collapsed state.





A legend is available at the bottom left of the Topology.

Site Status ^

- Normal
- Critical
- N/A
- Warning
- Polling Disabled

Legend ^

Display By

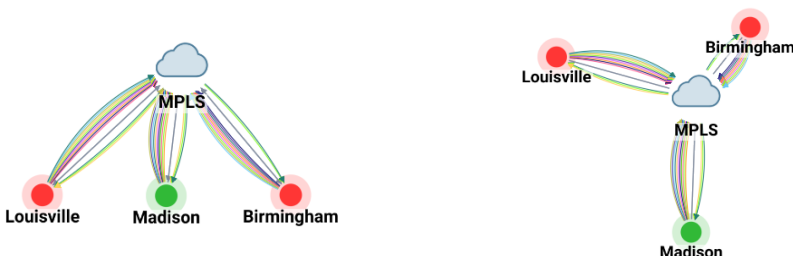
WAN Applications v

- MS-SQL
- citrix-static
- https
- outlook-web-servi...
- sip
- Other [↗](#)
- VoIP
- complex-main
- netflix
- rtp
- youtube

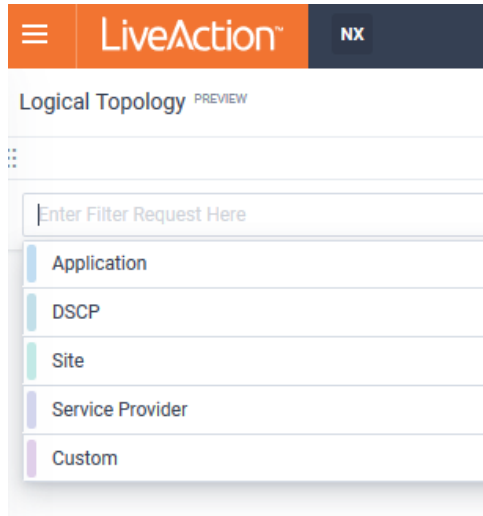
The Topology's view can be re-organized by using the control icons to the upper right. These icons represent: Zoom In, Zoom Out, Zoom Fit, and Toggle Layout Lock.



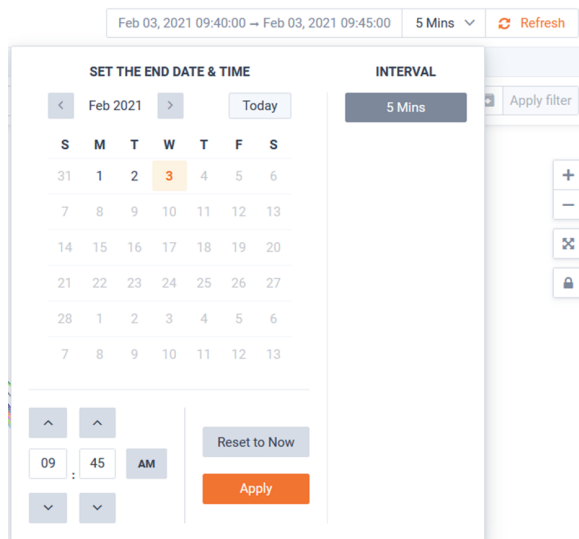
By clicking the Toggle Layout Lock, the icon will update to the unlocked position. In this state the diagram can be re-organized.



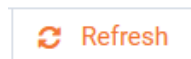
Filtering can be applied to find the specific Flows of interests.



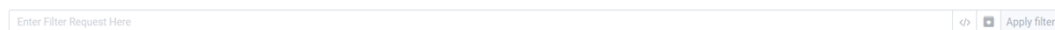
Historic time ranges can be selected for finding the Applications of interests.



The page can be refreshed by toggling the Refresh button in the top right of the page.



In the following example, note there is no Filter applied and the Legend's set to Display By WAN Application.



The display's legend will show the Top 10 Applications plus other.

Site Status ∨

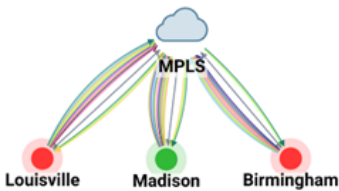
Legend ∧

**Display By**

WAN Applications ∨

- MS-SQL
- citrix-static
- https
- outlook-web-servi...
- sip
- Other
- VoIP
- complex-main
- netflix
- rtp
- youtube

The Application traffic data projected on the Topology will represent these applications.



In the following example, a Filter of Application: VoIP has been applied and the Legend's set to Display By WAN Application.

Application:  Enter Filter Request Here ↩️

The display's legend has updated to just so VoIP plus other.

Site Status ∧

- Normal
- Critical
- N/A
- Warning
- Polling Disabled

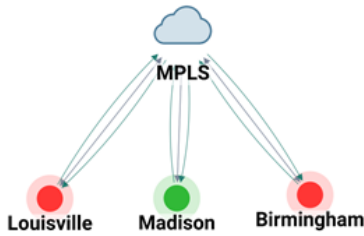
Legend ∧

**Display By**

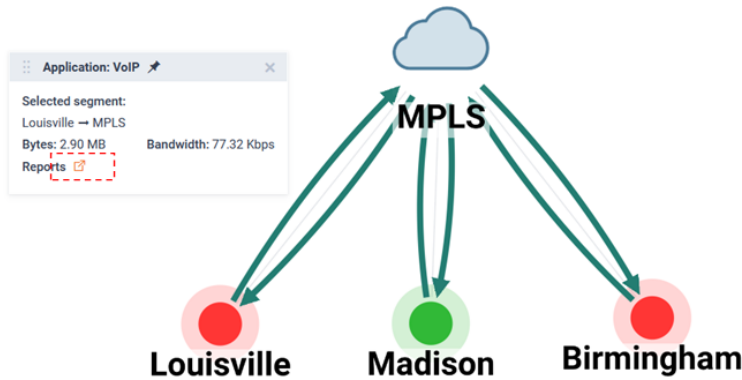
WAN Applications ∨

- VoIP
- Other

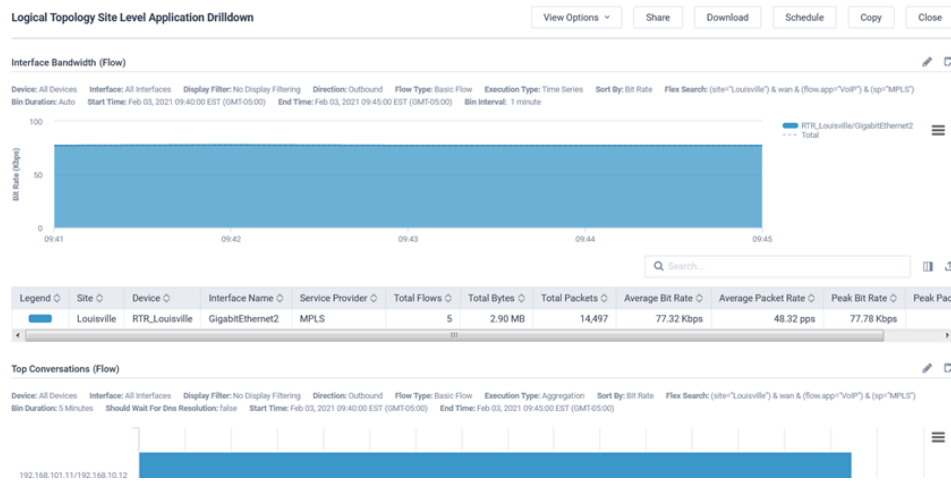
The Flow data projected on the Topology will represent just VoIP.



Clicking on the Flow arrows representing VoIP, will highlight them and cause a pop-up with more detail.



Clicking the Reports Icon will open a curated historic Report in a new tab.



In the following example, a Filter of *Application: VoIP* has been applied but the Legend's set to Display By WAN DSCP.

Application: VoIP Enter Filter Request Here

The display's legend has updated to show the DSCP value of 0 (BE), 46(EF), and other.

Site Status

- Normal
- Critical
- N/A
- Warning
- Polling Disabled

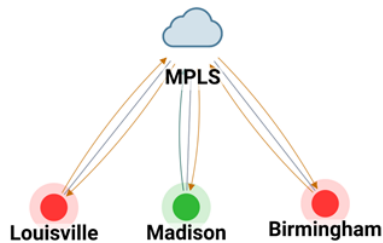
Legend

Display By

WAN DSCP

- 0 (BE)
- Other
- 46 (EF)

The Flow data projected on the Topology will represent these DSCP.



The Devices and Sites shown on the topology can be updated by using the control bar to the left.

Select the **Edit** button.

Logical Topology PREVIEW

---

Selected sites and devices shown on topology EDIT

Sort by: Name ▾

- ▾  Birmingham
- ▾  Louisville
- ▾  Madison

Select the desired options and **Save** button.

Logical Topology PREVIEW

---

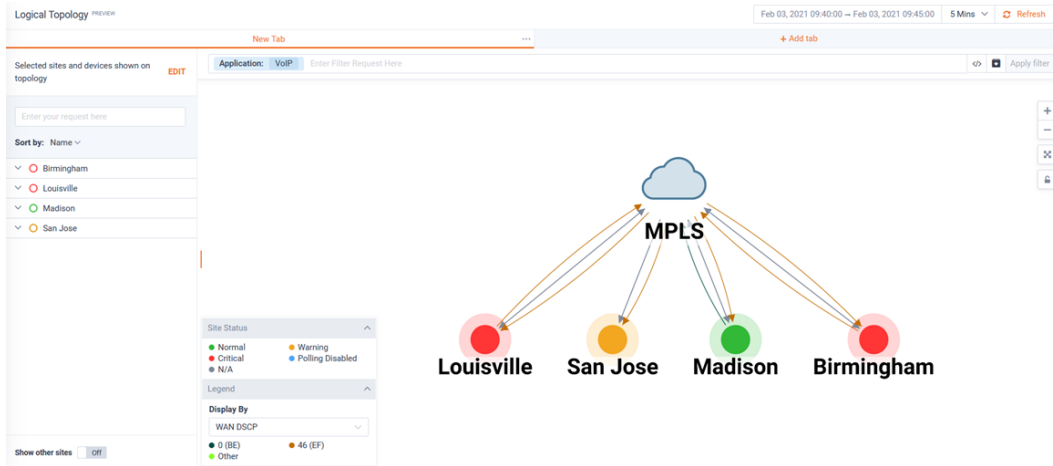
Select sites and devices which need to be displayed SAVE

Sites selected: 4 / 25

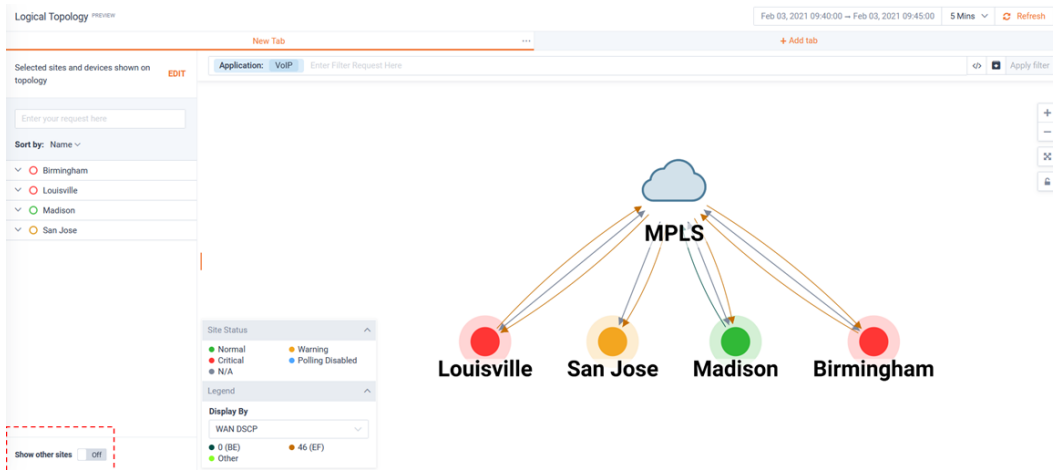
Sort by: Name ▾

▾ <input type="radio"/> Birmingham	<input checked="" type="checkbox"/>
▾ <input type="radio"/> LondonEdge	<input type="checkbox"/>
▾ <input type="radio"/> LosAngeles	<input type="checkbox"/>
▾ <input type="radio"/> Louisville	<input checked="" type="checkbox"/>
▾ <input type="radio"/> Madison	<input checked="" type="checkbox"/>
▾ <input type="radio"/> New York - DC	<input type="checkbox"/>
▾ <input type="radio"/> NewYorkEdge	<input type="checkbox"/>
▾ <input type="radio"/> Palo Alto	<input type="checkbox"/>
▾ <input type="radio"/> PaloAlto-VE-01	<input type="checkbox"/>
▾ <input type="radio"/> SanJose	<input checked="" type="checkbox"/>
▾ <input type="radio"/> Seattle	<input type="checkbox"/>

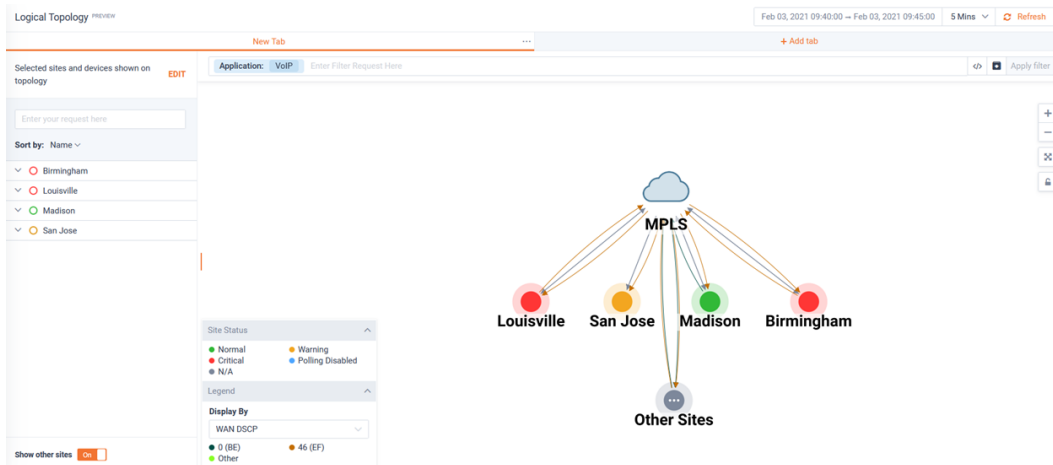
The Topology will be updated with the selected changes.



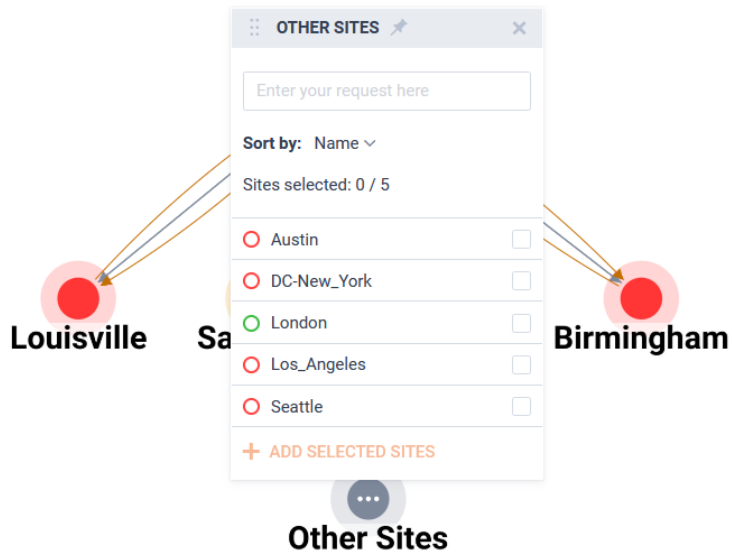
Note the Show Other Sites switch at the bottom of the site/device control bar.



By enabling this switch, a new site named Other Sites appears. This will represent any Application traffic relevant to the applied Filter that is being sent/received both sites not added to the Topology.



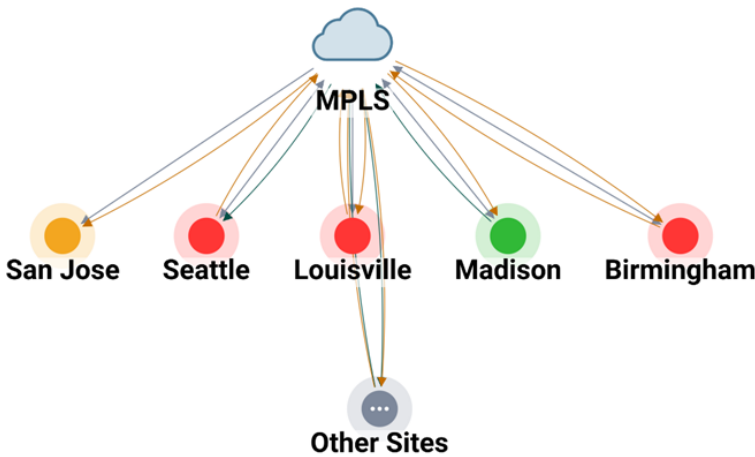
By clicking on the *Other Sites* icon, a list of the other sites sending/receiving the applicable Application will be listed.



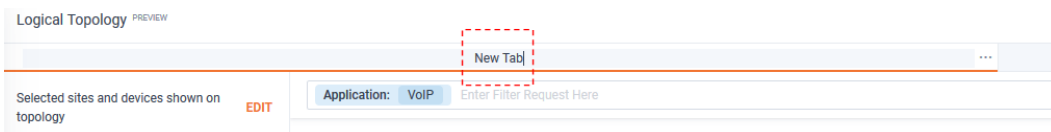
These sites can then be added to the Topology.



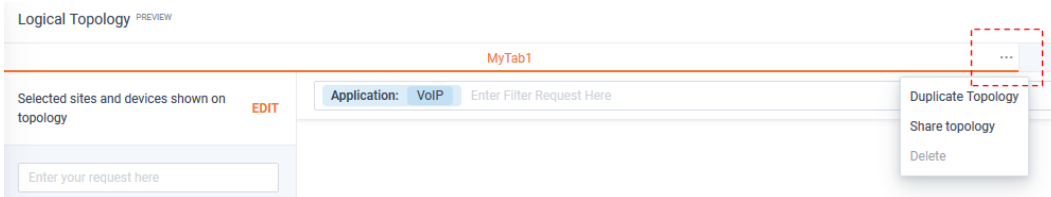




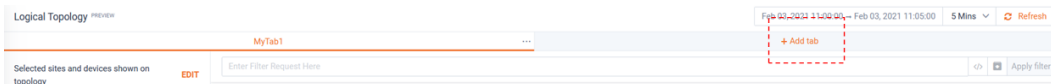
By clicking on a tab name at the top of the Topology, a tab can be renamed.



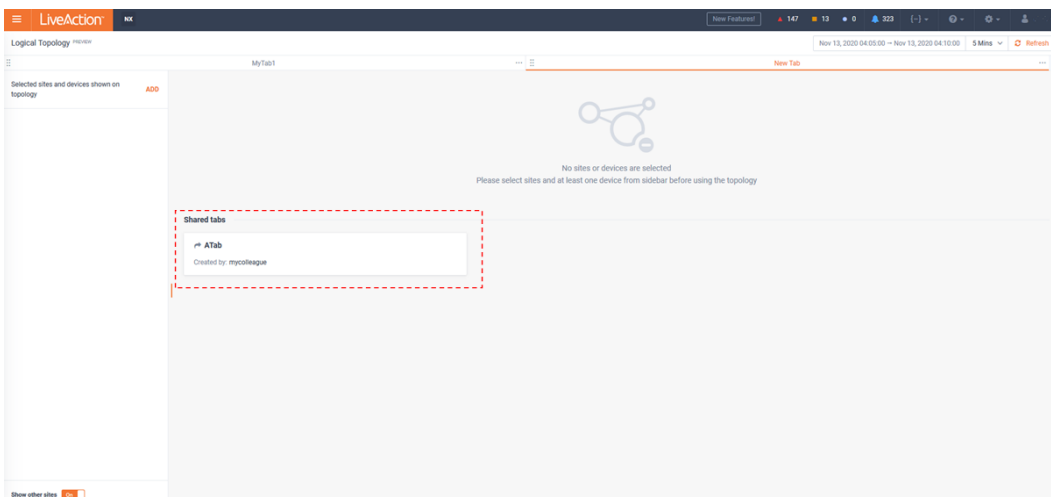
By clicking on a tab's menu icon, a tab can be duplicated, shared, or deleted.



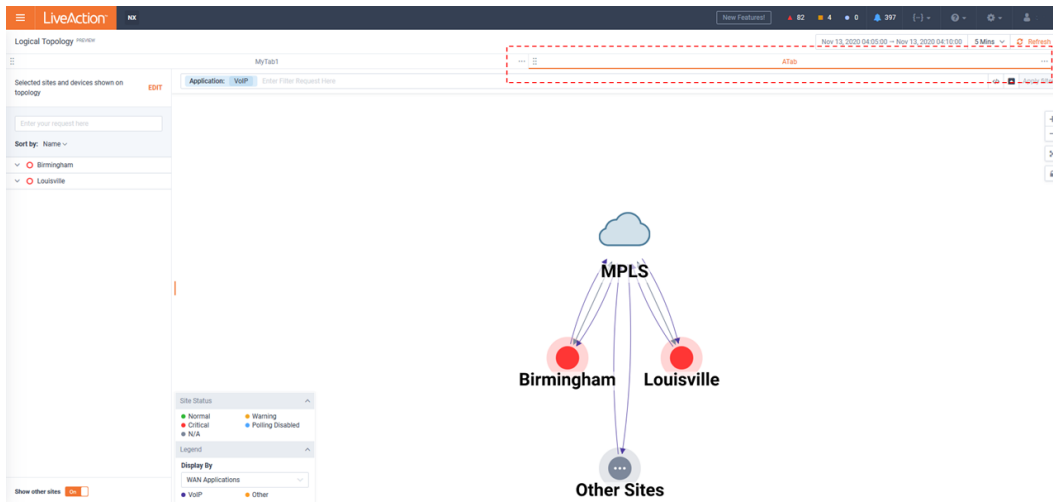
To create a new tab, select the + Add Tab icon.



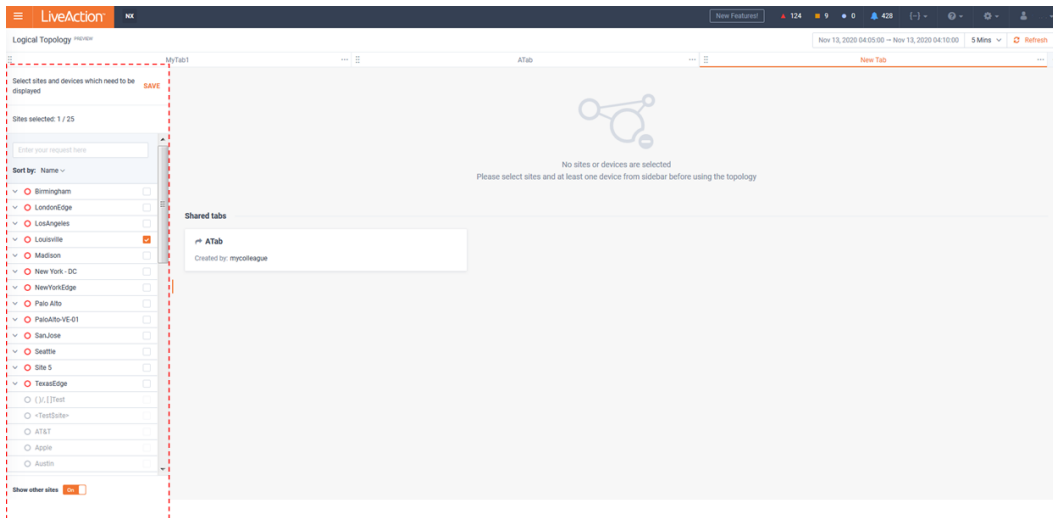
To add a shared a tab, click on the desired icon in the shard tabs list.



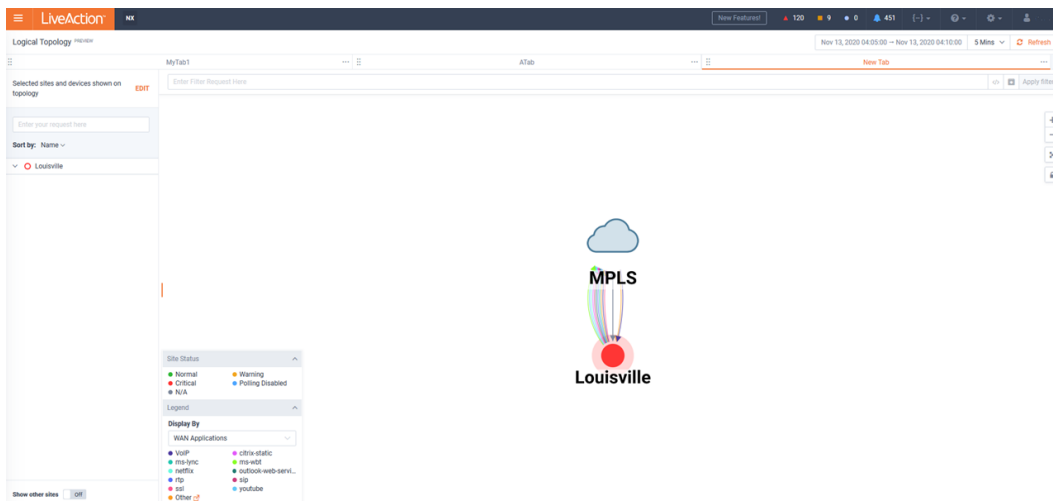
A new tab will be created with the topology of the shared tab.



To create a new tab from scratch, select the desired sites/devices from the control bar to the left of the window and select save.



A new tab will appear with the select sites, devices and any relevant WAN clouds shown.



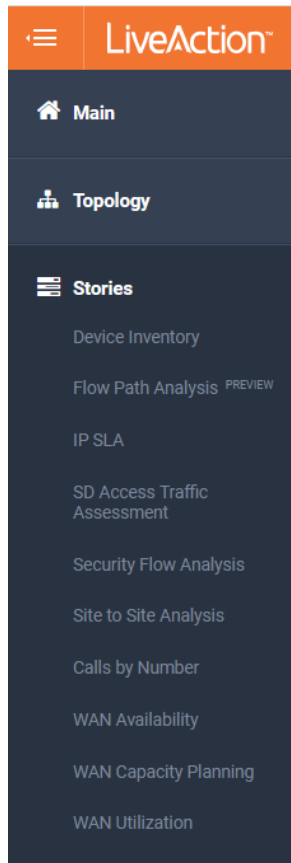
## Stories

### In this chapter:

<i>Stories</i> .....	85
<i>Device Inventory</i> .....	85
<i>Flow Path Analysis</i> .....	86
<i>IP SLA</i> .....	89
<i>SD Access Traffic Assessment</i> .....	91
<i>Security Flow Analysis</i> .....	93
<i>Site to Site Analysis</i> .....	94
<i>Calls by Number</i> .....	99
<i>WAN Availability</i> .....	102
<i>WAN Capacity Planning</i> .....	103
<i>WAN Utilization</i> .....	106

## Stories

LiveNX stories provide reports and workflows to assist network operators with advanced datasets. These are available via the *Operations Dashboard's* menu.



## Device Inventory

The *Device Inventory* story provides a list of all devices and interfaces being monitored by LiveNX. By clicking on the individual entry in the table, the selected device/interface performance can be further explored.

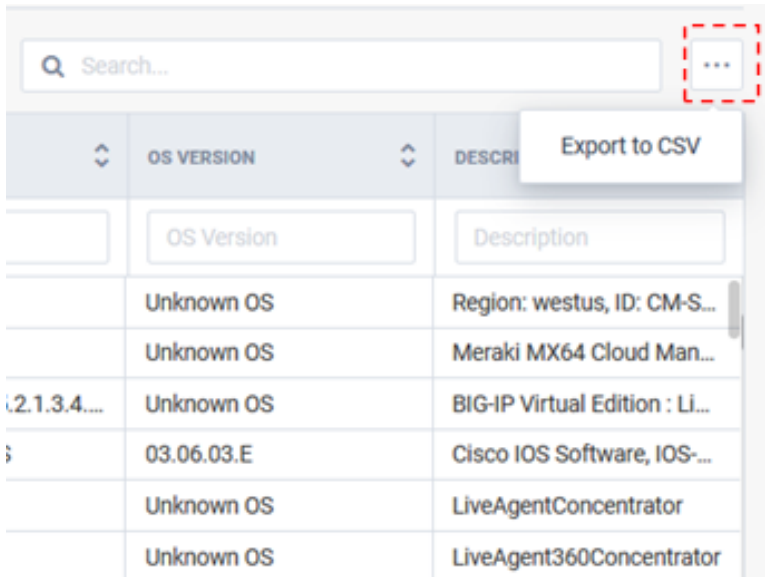
The screenshot shows the LiveAction dashboard with the 'Devices' story selected. The table displays a list of devices with columns for Device, Device Serial, IP Address, Site, Node, Tags, Group, Model, OS Version, and Description. Below the table, there is a section for 'Interfaces' with a similar table structure.

DEVICE	DEVICE SERIAL	IP ADDRESS	SITE	NODE	TAGS	GROUP	MODEL	OS VERSION	DESCRIPTION
AzureCM45West	CM-SEDemo-vnet	10.0.5.0	AzureWest	Local	CM-SEDemo-vnet, we...	Azure West US	Non-SNMP	Unknown OS	Region: westus, ID: C...
PA-MX64-816	10.1.10.71:16010567...	10.1.10.71	Internet	Local	Meraki	Internet	mx60	Unknown OS	Meraki MX64 Cloud M...
f5-sedemo	10.1.2.202:15998698...	10.1.2.202	Hurricane Electric	Local	-	Hurricane Electric	enterprises.3375.2.1...	Unknown OS	BIG-IP Virtual Edition ...
CS-C3650-23-36	FD01926E3H6	10.100.155.1	Hurricane Electric	Local	IPSLA, test2(jeff, test1)...	Hurricane Electric	ciscoC365024PS	03.06.03.E	Cisco IOS Software, L...
LiveAgentConcentrator	LiveAgentConcentrat...	10.100.50.77	Florida	Local	liveagent	Florida	Non-SNMP	Unknown OS	LiveAgentConcentrator
LiveAgent360Concent...	LiveAgent360Concent...	10.100.50.78	Florida	Local	liveagent_liveagent360	Florida	Non-SNMP	Unknown OS	LiveAgent360Concent...
SE-LiveWire-NY	10.100.50.80:154161...	10.100.50.80	DC-New_York	Local	livewire_LiveWire, cus...	DC-New York	Non-SNMP	Unknown OS	LiveWire Virtual 12.3...
CS-C3850-23-31	FOC1911X0U5	10.100.51.1	-	Local	test2(jeff, LiveAgent, L...	Hurricane Electric	cat3850stack	03.06.08E	Cisco IOS Software, L...

INTERFACE N...	IP ADDRESS	SUBNET MASK	DEVICE	SITE	WAN	SERVICE PR...	INPUT CAP...	OUTPUT CAP...	ABBREVIATE...	IF INDEX	DESCRIPTION	SPEED	TYPE	LABEL
GigabitEther...	199.199.1.13	255.255.255...	RTR_SanJose	San Jose	WAN	MPLS	301 Kbps	301 Kbps	G2	2	Conn-MPLS...	1 Gbps	ethernet_cs...	MPLS
GigabitEther...	192.168.103...	255.255.255.0	RTR_SanJose	San Jose	-	-	1 Gbps	1 Gbps	G3	3	Conn-Admin...	1 Gbps	ethernet_cs...	-

By selecting the table menu icon at the top right of the device/ inventory table, the table data can be exported to CSV.



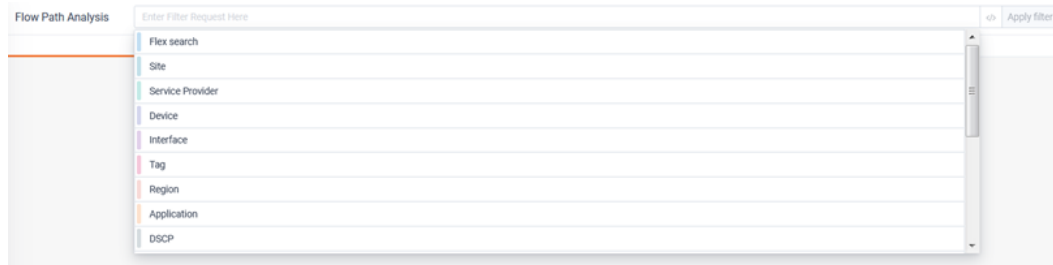
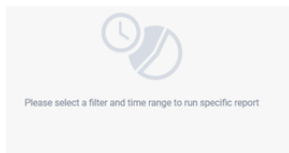
## Flow Path Analysis

The *Flow Path Analysis* story provides a workflow for exploring traffic of interest for a specific time range. This story allows:

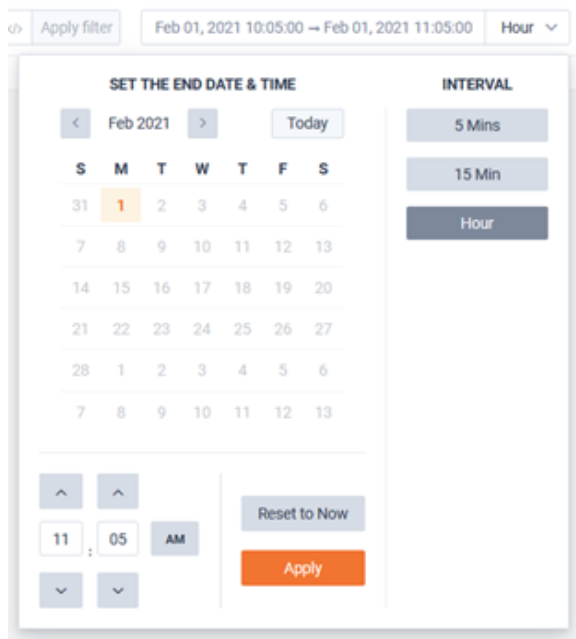
1. Cross-launch to LiveNX Peek for packet analysis.
2. Drill-down to a hop-by-hop visualization of a conversation of interest.

The image shows a screenshot of the LiveAction interface. At the top, there is a "LiveAction" header and a "Flow Path Analysis" sub-header. Below this is a table with columns for "PEEK", "FLOW ID", "TIME", "PROTOCOL", "SRC IP ADDR", "SRC SITE", "SRC PORT", "DST IP ADDR", "DST SITE", "DST PORT", "DSCP", "APPLICATION", "TOTAL FLOWS", "TOTAL BYTES", "TOTAL PACKETS", "AVERAGE BIT R...", and "AVERAGE PKET...". The table contains multiple rows of data, each representing a flow path analysis entry. The "TIME" column shows timestamps from 12 Nov 2020, 03:40AM to 12 Nov 2020, 03:55AM. The "PROTOCOL" column is consistently "UDP". The "SRC IP ADDR" and "SRC SITE" columns vary, while "DST IP ADDR", "DST SITE", and "DST PORT" are consistent across many rows. The "APPLICATION" column is consistently "VoIP".

To use this story, a Filter must first be applied.



Historic Flow data can be explored.



The *Flow Path Analysis* story has three tabs for monitoring statistics from the specific Flow type of interest and will present details specific to their respective use case. These tabs are:

- Basic
- Voice/Video Performance
- Application Performance

PREK	FLOW P.	TIME	PROTOCOL	SRC IP ADDR	SRC SITE	SRC PORT	DST IP ADDR	DST SITE	DST PORT	ESCP	APPLICATION	TOTAL FLOWS	TOTAL BYTES	TOTAL PACKETS	AVERAGE BIT	AVERAGE PKT.
		12 Nov 2020, 03:40AM	UDP	192.168.10.15	Site 5	19424	192.168.104.11	Site 5	31196	46 (EF)	VoIP	28	4.18 MB	19,193	9.30 Kbps	5.33 pps
		12 Nov 2020, 03:30AM	UDP	192.168.10.13	Site 5	19422	192.168.102.11	Site 5	31196	46 (EF)	VoIP	28	4.18 MB	19,179	9.29 Kbps	5.33 pps
		12 Nov 2020, 04:10AM	UDP	192.168.10.15	Site 5	19424	192.168.104.11	Site 5	31196	46 (EF)	VoIP	28	4.18 MB	19,167	9.29 Kbps	5.32 pps
		12 Nov 2020, 04:10AM	UDP	192.168.10.11	Site 5	19420	192.168.100.11	Seattle	31196	46 (EF)	VoIP	28	4.16 MB	19,089	9.25 Kbps	5.30 pps
		12 Nov 2020, 04:10AM	UDP	192.168.10.14	Site 5	19423	192.168.103.11	PaltoAtto-VE01	31196	46 (EF)	VoIP	28	4.16 MB	19,087	9.25 Kbps	5.30 pps
		12 Nov 2020, 04:15AM	UDP	192.168.10.13	Site 5	19422	192.168.102.11	Site 5	31196	46 (EF)	VoIP	28	4.16 MB	19,069	9.24 Kbps	5.30 pps
		12 Nov 2020, 03:20AM	UDP	192.168.10.11	Site 5	19420	192.168.100.11	Seattle	31196	46 (EF)	VoIP	28	4.15 MB	19,024	9.22 Kbps	5.28 pps
		12 Nov 2020, 03:40AM	UDP	192.168.10.13	Site 5	19422	192.168.102.11	Site 5	31196	46 (EF)	VoIP	28	4.15 MB	19,022	9.22 Kbps	5.28 pps
		12 Nov 2020, 03:20AM	UDP	192.168.10.14	Site 5	19423	192.168.103.11	PaltoAtto-VE01	31196	46 (EF)	VoIP	28	4.15 MB	19,020	9.21 Kbps	5.28 pps
		12 Nov 2020, 03:40AM	UDP	192.168.10.12	Site 5	19421	192.168.101.11	Site 5	31196	46 (EF)	VoIP	28	4.15 MB	19,018	9.21 Kbps	5.28 pps
		12 Nov 2020, 04:05AM	UDP	192.168.10.13	Site 5	19422	192.168.103.11	Site 5	31196	46 (EF)	VoIP	28	4.14 MB	18,995	9.20 Kbps	5.28 pps
		12 Nov 2020, 04:05AM	UDP	192.168.10.14	Site 5	19423	192.168.103.11	PaltoAtto-VE01	31196	46 (EF)	VoIP	28	4.14 MB	18,995	9.20 Kbps	5.28 pps
		12 Nov 2020, 04:05AM	UDP	192.168.10.11	Site 5	19420	192.168.100.11	Seattle	31196	46 (EF)	VoIP	28	4.14 MB	18,991	9.20 Kbps	5.28 pps
		12 Nov 2020, 04:05AM	UDP	192.168.10.15	Site 5	19424	192.168.104.11	Site 5	31196	46 (EF)	VoIP	28	4.14 MB	18,987	9.20 Kbps	5.27 pps
		12 Nov 2020, 03:45AM	UDP	192.168.10.14	Site 5	19423	192.168.103.11	PaltoAtto-VE01	31196	46 (EF)	VoIP	28	4.13 MB	18,940	9.19 Kbps	5.26 pps
		12 Nov 2020, 03:45AM	UDP	192.168.10.16	Site 5	19425	192.168.105.11	PaltoAtto-VE01	31196	46 (EF)	VoIP	28	4.13 MB	18,939	9.17 Kbps	5.26 pps
		12 Nov 2020, 03:45AM	UDP	192.168.10.17	Site 5	19426	192.168.106.11	Site 5	31196	46 (EF)	VoIP	28	4.13 MB	18,935	9.17 Kbps	5.26 pps
		12 Nov 2020, 03:45AM	UDP	192.168.10.11	Site 5	19420	192.168.100.11	Seattle	31196	46 (EF)	VoIP	28	4.13 MB	18,926	9.17 Kbps	5.26 pps
		12 Nov 2020, 04:05AM	UDP	192.168.10.16	Site 5	19425	192.168.105.11	PaltoAtto-VE01	31196	46 (EF)	VoIP	28	4.12 MB	18,919	9.17 Kbps	5.26 pps
		12 Nov 2020, 04:05AM	UDP	192.168.10.12	Site 5	19421	192.168.101.11	Site 5	31196	46 (EF)	VoIP	28	4.12 MB	18,913	9.16 Kbps	5.25 pps
		12 Nov 2020, 03:35AM	UDP	192.168.10.14	Site 5	19423	192.168.103.11	PaltoAtto-VE01	31196	46 (EF)	VoIP	28	4.12 MB	18,912	9.16 Kbps	5.25 pps

The *Voice/Video Performance* tab will include Jitter and Packet Loss metrics included in Performance Monitor Flow data.

STATUS	PREK	FLOW P.	TIME	SRC IP	SRC PORT	SRC SITE	DST IP	DST PORT	DST SITE	APPLICATION	RTP SRC	ESCP	PACKET LOSS	JITTER AVG	JITTER MAX	AVG MOS
			01 Feb 2021, 11:15AM	192.168.102...	31196	Birmingham	192.168.10.13	19422	DC-New_York	VoIP	2539225492	0 (BE)	70.88%	803.53 ms	267.28 s	NaN
			01 Feb 2021, 11:35AM	192.168.102...	31196	Birmingham	192.168.10.13	19422	DC-New_York	VoIP	2539225492	0 (BE)	70.85%	267.83 s	488.67 s	NaN
			01 Feb 2021, 11:25AM	192.168.102...	31196	Birmingham	192.168.10.13	19422	DC-New_York	VoIP	2539225492	0 (BE)	70.83%	251.87 s	267.28 s	NaN
			01 Feb 2021, 12:10PM	192.168.102...	31196	Birmingham	192.168.10.13	19422	DC-New_York	VoIP	2539225492	0 (BE)	70.81%	275.51 s	511.79 s	NaN
			01 Feb 2021, 11:50AM	192.168.102...	31196	Birmingham	192.168.10.13	19422	DC-New_York	VoIP	2539225492	0 (BE)	70.58%	267.28 s	267.28 s	NaN
			01 Feb 2021, 11:15AM	192.168.102...	31196	Birmingham	192.168.10.13	19422	DC-New_York	VoIP	2539225492	0 (BE)	69.50%	9.42 s	267.28 s	NaN
			01 Feb 2021, 11:55AM	192.168.102...	31196	Birmingham	192.168.10.13	19422	DC-New_York	VoIP	2539225492	0 (BE)	69.16%	267.28 s	267.28 s	NaN
			01 Feb 2021, 12:10PM	192.168.102...	31196	Birmingham	192.168.10.13	19422	DC-New_York	VoIP	2539225492	0 (BE)	68.51%	481.10 s	511.79 s	NaN
			01 Feb 2021, 11:50AM	192.168.102...	31196	Birmingham	192.168.10.13	19422	DC-New_York	VoIP	2539225492	0 (BE)	68.05%	2.31 s	267.28 s	NaN
			01 Feb 2021, 11:30AM	192.168.102...	31196	Birmingham	192.168.10.13	19422	DC-New_York	VoIP	2539225492	0 (BE)	68.05%	458.32 ms	268.48 s	NaN
			01 Feb 2021, 11:45AM	192.168.102...	31196	Birmingham	192.168.10.13	19422	DC-New_York	VoIP	2539225492	0 (BE)	67.84%	267.23 s	504.52 s	NaN
			01 Feb 2021, 12:00PM	192.168.102...	31196	Birmingham	192.168.10.13	19422	DC-New_York	VoIP	2539225492	0 (BE)	67.18%	1.42 s	268.50 s	NaN
			01 Feb 2021, 11:40AM	192.168.102...	31196	Birmingham	192.168.10.13	19422	DC-New_York	VoIP	2539225492	0 (BE)	66.81%	292.39 s	488.67 s	NaN
			01 Feb 2021, 12:09PM	192.168.102...	31196	Birmingham	192.168.10.13	19422	DC-New_York	VoIP	2539225492	0 (BE)	65.62%	818.82 ms	268.50 s	NaN
			01 Feb 2021, 11:55AM	192.168.102...	31196	Birmingham	192.168.10.13	19422	DC-New_York	VoIP	2539225492	0 (BE)	65%	19.06 s	267.28 s	NaN
			01 Feb 2021, 11:35AM	192.168.100...	31196	Seattle	192.168.10.11	19420	DC-New_York	VoIP	2539225492	46 (EF)	63.72%	16.76 s	268.34 s	NaN

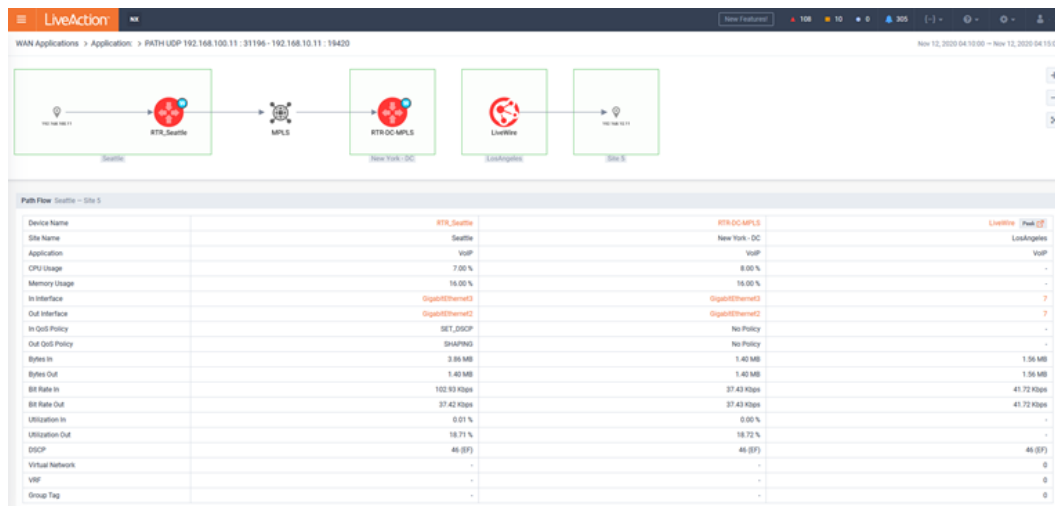
The *Application Performance* tab will include Application Delay (AD), Network Delay (ND), and additional metrics included in Performance Monitor Flow data.

STATUS	PREK	FLOW PATH	TIME	CLIENT IP	SRC SITE	SERVER IP	DST SITE	PORT	APPLICATION	AD AVG	AD MAX	CND AVG	CND MAX	END AVG	END MAX	ND AVG
			01 Feb 2021, 11:20AM	192.168.2.151	Indianapolis	104.244.36.20	Internet	80	ted	1 ms	1 ms	54 ms	65 ms	200 ms	201 ms	231 ms
			01 Feb 2021, 11:20AM	192.168.2.151	Indianapolis	104.244.36.20	Internet	80	ted	1 ms	1 ms	54 ms	65 ms	200 ms	201 ms	231 ms
			01 Feb 2021, 11:40AM	192.168.2.151	Indianapolis	104.244.36.20	Internet	80	ted	1 ms	1 ms	54 ms	65 ms	200 ms	201 ms	231 ms
			01 Feb 2021, 11:40AM	192.168.2.151	Indianapolis	104.244.36.20	Internet	80	ted	1 ms	1 ms	54 ms	65 ms	200 ms	201 ms	231 ms
			01 Feb 2021, 11:55AM	192.168.2.151	Indianapolis	104.244.36.20	Internet	80	ted	1 ms	1 ms	54 ms	65 ms	200 ms	201 ms	231 ms
			01 Feb 2021, 11:55AM	192.168.2.151	Indianapolis	104.244.36.20	Internet	80	ted	1 ms	1 ms	54 ms	65 ms	200 ms	201 ms	231 ms
			01 Feb 2021, 12:10PM	192.168.2.151	Indianapolis	104.244.36.20	Internet	80	ted	1 ms	1 ms	54 ms	65 ms	200 ms	201 ms	231 ms
			01 Feb 2021, 12:10PM	192.168.2.151	Indianapolis	104.244.36.20	Internet	80	ted	1 ms	1 ms	54 ms	65 ms	200 ms	201 ms	231 ms
			01 Feb 2021, 11:25AM	192.168.2.151	Indianapolis	104.244.36.20	Internet	80	ted	5 ms	5 ms	50 ms	146 ms	129 ms	144 ms	165 ms
			01 Feb 2021, 11:25AM	192.168.2.151	Indianapolis	104.244.36.20	Internet	80	ted	5 ms	5 ms	50 ms	146 ms	129 ms	144 ms	165 ms
			01 Feb 2021, 12:15PM	192.168.2.151	Indianapolis	104.244.36.20	Internet	80	ted	5 ms	5 ms	50 ms	146 ms	129 ms	144 ms	165 ms
			01 Feb 2021, 12:15PM	192.168.2.151	Indianapolis	104.244.36.20	Internet	80	ted	5 ms	5 ms	50 ms	146 ms	129 ms	144 ms	165 ms
			01 Feb 2021, 11:55AM	192.168.2.151	Indianapolis	104.244.36.20	Internet	80	ted	1 ms	2 ms	61 ms	89 ms	129 ms	153 ms	163 ms
			01 Feb 2021, 11:55AM	192.168.2.151	Indianapolis	104.244.36.20	Internet	80	ted	1 ms	2 ms	61 ms	89 ms	129 ms	153 ms	163 ms
			01 Feb 2021, 12:10PM	192.168.2.151	Indianapolis	104.244.36.20	Internet	80	ted	1 ms	2 ms	61 ms	89 ms	129 ms	153 ms	163 ms
			01 Feb 2021, 12:10PM	192.168.2.151	Indianapolis	104.244.36.20	Internet	80	ted	1 ms	2 ms	61 ms	89 ms	129 ms	153 ms	163 ms
			01 Feb 2021, 11:35AM	192.168.2.151	Indianapolis	104.244.36.20	Internet	80	ted	5 ms	5 ms	57 ms	89 ms	128 ms	153 ms	161 ms

Selecting the *Flow Path* icon will drill-down to a hop-by-hop analysis of the conversation of interest.

Flow Path Analysis Applicati

PEEK	FLOW PATH	TIME
		Time
☰	↗	01 Fe
☰	↗	01 Fe
☰	↗	01 Fe
☰	↗	01 Fe
☰	↗	01 Fe



## IP SLA

The IP SLA story will list any IP SLA tests being monitored via SNMP by LiveNX and report on their status.



TEST STATUS	REPORTS	ID	GROUP ID	TYPE	TAG	PROPERTIES	ATTEMPTS	ERROR
●	📄	2		ICMP Echo		RTR_Madison 199.199.1.29	33,107	Timeout
●	📄	1		Jitter	TestSLA	RTR_Madison 199.199.1.29	75,552	Not connected
●	📄	2		Jitter		RTR_LosAngeles 10.100.51.4	17,817	Not connected
●	📄	1		Jitter		RTR_LosAngeles 199.199.1.5	17,817	Success
●	📄	1		ICMP Echo	Branch Latency	IWAN_ER_MPLS 10.100.51.33	0	
●	📄	2		ICMP Echo	Branch Latency	IWAN_ER_MPLS 10.100.51.33	0	
●	📄	3		ICMP Echo	Branch Latency	IWAN_ER_MPLS 10.100.51.33	0	
●	📄	4		Jitter	Branch Latency	IWAN_ER_MPLS 10.100.51.33	0	
●	📄	5		Jitter	Branch Latency	IWAN_ER_MPLS 10.100.51.33	0	
●	📄	6		Jitter	Branch Latency	RTR_Seattle 10.100.51.33	0	
●	📄	2		ICMP Echo	Branch Latency	RTR_Seattle 10.100.51.33	0	
●	📄	3		ICMP Echo	Branch Latency	RTR_Seattle 10.100.51.33	0	
●	📄	4		Jitter	Branch Latency	RTR_Seattle 10.100.51.33	0	
●	📄	5		Jitter	Branch Latency	RTR_Seattle 10.100.51.33	0	
●	📄	6		Jitter	Branch Latency	RTR_Seattle 10.100.51.33	0	
●	📄	13		ICMP Echo	Branch Latency	MPLS-CORE 10.100.51.31	0	
●	📄	14		ICMP Echo	Branch Latency	MPLS-CORE 10.100.51.31	0	
●	📄	15		ICMP Echo	Branch Latency	MPLS-CORE 10.100.51.31	0	
●	📄	19		ICMP Echo	Branch Latency	MPLS-CORE 10.100.51.2	0	
●	📄	1		ICMP Echo	Branch Latency	MPLS-CORE 10.100.4.1	0	
●	📄	2		ICMP Echo	Branch Latency	MPLS-CORE 10.100.4.1	0	
●	📄	3		ICMP Echo	Branch Latency	MPLS-CORE 10.100.4.1	0	

The statistics shown in the table can be presented as either the latest or an average by using the switch at the top right of the page.



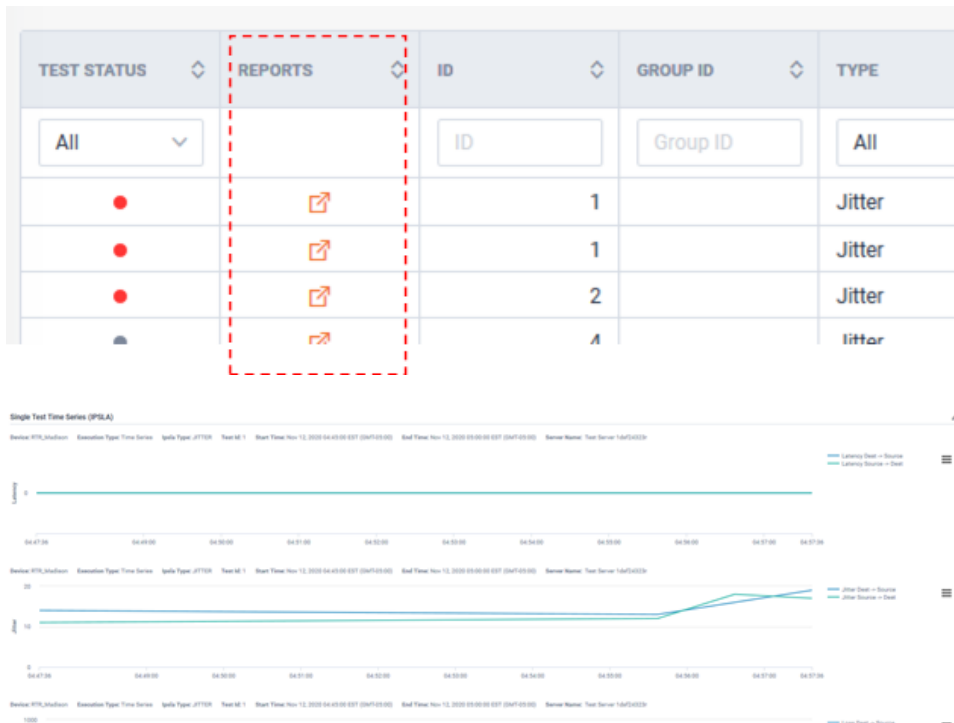
The All Test tab will show a summary of all tests being monitored.

The Errors shown on this story are learned via SNMP from the IP SLA status from device itself.

Each IP SLA test type also has its own tab that will show the details of each respective test.

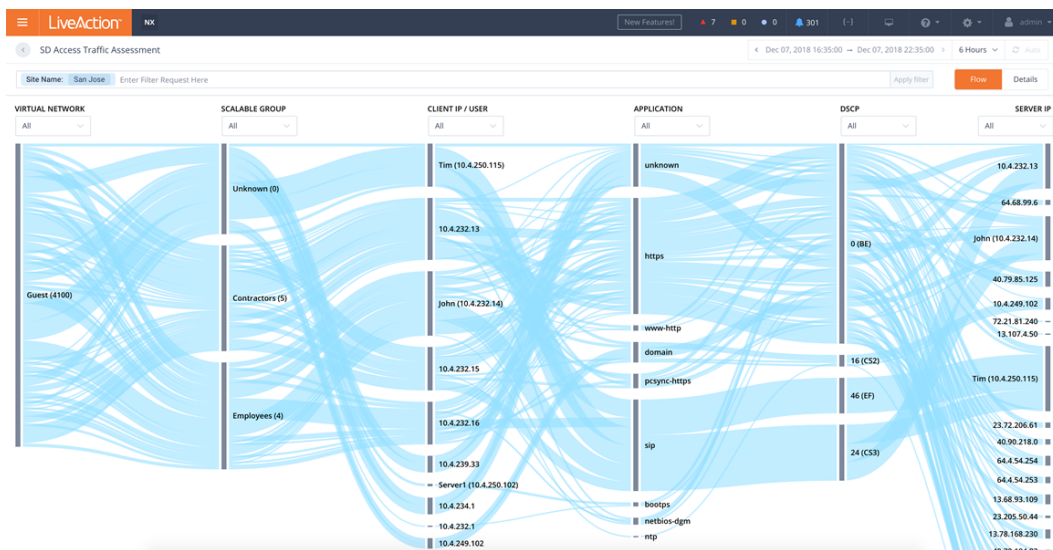
TEST STATUS	REPORTS	ID	GROUP ID	TYPE	TAG	PROPERTIES	LATENCY (MS)	JITTER (MS)	LOSS (PACKETS)	MOD	ERROR	
●	📄	1		Jitter	TestSLA	RTR_Madison 199.199.1.29	0 ms	0 ms	0 ms	0 ms	0	Not connected
●	📄	1		Jitter		RTR_LosAngeles 199.199.1.5	0 ms	0 ms	0 ms	0 ms	0	Not connected
●	📄	2		Jitter		RTR_LosAngeles 10.100.51.4	0 ms	0 ms	0 ms	0 ms	0	Not connected

Clicking a report icon will show the historic report of the specific IP SLA test selected.



## SD Access Traffic Assessment

The *SD Access Traffic Assessment* story provides a Sankey diagram for visibility into both macro and micro level segmentation of traffic controlled by a SD-Access fabric.



Filters can be applied to focus on the specific conversations of interest.

SD Access Traffic Assessment

Enter Filter Request Here

- Site
- Device
- Group
- DSCP

Historic time ranges can be selected for finding the Flows of interests.

< Feb 12, 2021 12:20:00 → Feb 12, 2021 12:25:00 > | 5 Mins ▾

**SET THE END DATE & TIME**

< Feb 2021 > Today

S	M	T	W	T	F	S
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	1	2	3	4	5	6
7	8	9	10	11	12	13

Time: 12 : 25 PM

Reset to Now

Apply

**INTERVAL**

5 Mins

15 Min

Hour

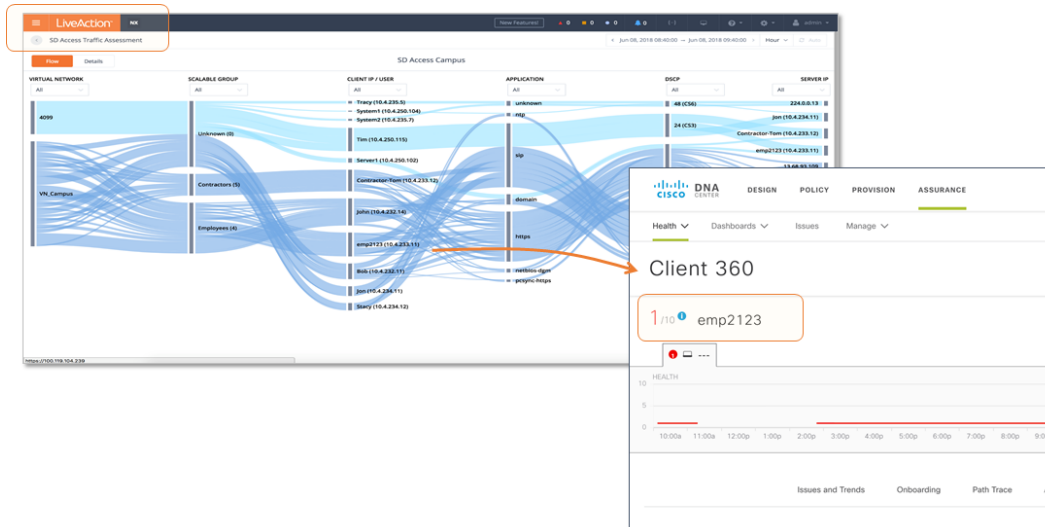
6 Hours

Day

Week

The page can optionally be auto-refreshed by toggling the **Auto** button in the top right of the page.

 Auto



## Security Flow Analysis

The *Security Flow Analysis* story provides a list of all devices that “see” a specific Flow during a selected time period. The utilization of each Flow in this story is de-duplicated.

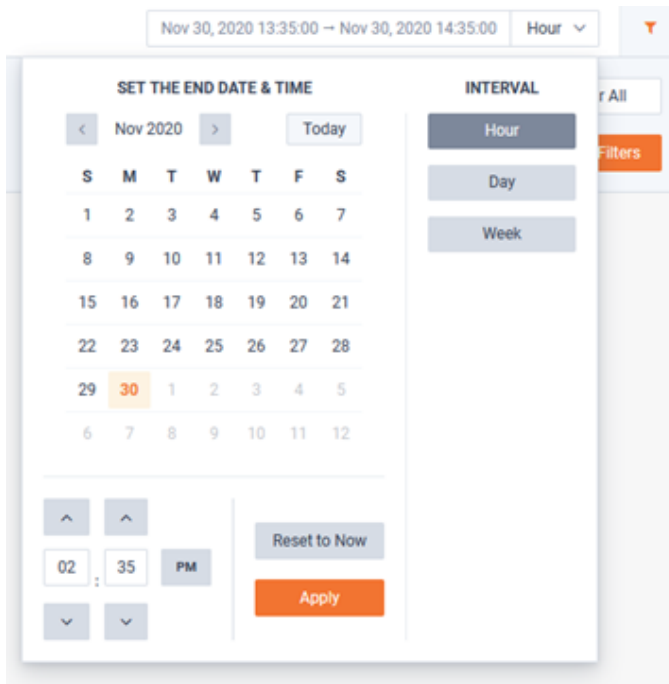
The screenshot shows the 'Security Flow Analysis' dashboard. At the top, there are filter sections for 'IP Addresses (Source / Destination)', 'Ports (Source / Destination)', 'Applications', and 'Protocols'. Below these filters is a large table with columns for 'TIME', 'DEVICES', 'FIRST SWITCH', 'LAST SWITCH', 'SRC IP ADDR', 'DST IP ADDR', 'SRC PORT', 'DST PORT', 'PROTOCOL', 'APPLICATION', 'BYTES', 'SRC COUNTRY', 'SRC SITE', and 'DST COUNTRY'. The table contains multiple rows of data representing network flows.

TIME	DEVICES	FIRST SWITCH	LAST SWITCH	SRC IP ADDR	DST IP ADDR	SRC PORT	DST PORT	PROTOCOL	APPLICATION	BYTES	SRC COUNTRY	SRC SITE	DST COUNTRY	DST SITE
Thu, 12 Nov 2020 09:05:00 GMT	RTR_SanJose	Thu, 12 Nov 2020 15:07:11 GMT	Thu, 12 Nov 2020 15:07:19 GMT	192.168.103...	40.97.169.10	59191	443	TCP	outlook-web...	6.06 KB	N/A	PaoloAlto-VE-01	US/United States	Intern
Thu, 12 Nov 2020 09:05:00 GMT	RTR_SanJose	Thu, 12 Nov 2020 15:07:15 GMT	Thu, 12 Nov 2020 15:07:19 GMT	192.168.103...	40.97.134.232	59195	443	TCP	http*	152 B	N/A	PaoloAlto-VE-01	US/United States	Intern
Thu, 12 Nov 2020 09:05:00 GMT	RTR_SanJose	Thu, 12 Nov 2020 15:07:19 GMT	Thu, 12 Nov 2020 15:07:19 GMT	192.168.103...	40.97.155.210	59546	443	TCP	outlook-web...	40 B	N/A	PaoloAlto-VE-01	US/United States	Intern
Thu, 12 Nov 2020 09:05:00 GMT	FWAN_BR_NET	Thu, 12 Nov 2020 15:06:37 GMT	Thu, 12 Nov 2020 15:06:37 GMT	22.1.1.20	192.36.148.17	17360	53	UDP	dns	56 B	US/United St.	Internet	SE/Sweden	Intern
Thu, 12 Nov 2020 09:05:00 GMT	FWAN_BR_NET	Thu, 12 Nov 2020 15:06:37 GMT	Thu, 12 Nov 2020 15:06:37 GMT	22.1.1.20	192.36.148.17	16131	53	UDP	dns	71 B	US/United St.	Internet	SE/Sweden	Intern
Thu, 12 Nov 2020 09:05:00 GMT	FWAN_BR_NET	Thu, 12 Nov 2020 15:06:37 GMT	Thu, 12 Nov 2020 15:06:37 GMT	22.1.1.20	192.36.148.17	55002	53	UDP	dns	71 B	US/United St.	Internet	SE/Sweden	Intern
Thu, 12 Nov 2020 09:05:01 GMT	FWAN_BR_NET	Thu, 12 Nov 2020 15:06:38 GMT	Thu, 12 Nov 2020 15:06:38 GMT	172.16.2.254	224.0.0.13	0	0	IPM	pin	58 B	N/A	Unknown	N/A	Intern
Thu, 12 Nov 2020 09:05:02 GMT	FWAN_BR_NET	Thu, 12 Nov 2020 15:06:39 GMT	Thu, 12 Nov 2020 15:06:39 GMT	172.16.2.254	224.0.0.140	0	22	IGMP	unknown	32 B	N/A	Unknown	N/A	Intern
Thu, 12 Nov 2020 09:05:02 GMT	RTR_SanJose	Thu, 12 Nov 2020 15:06:21 GMT	Thu, 12 Nov 2020 15:07:21 GMT	199.199.1.26	224.0.0.10	0	0	EGRP	igmp	840 B	US/United St.	Internet	N/A	Intern
Thu, 12 Nov 2020 09:05:02 GMT	RTR_SanJose	Thu, 12 Nov 2020 15:07:21 GMT	Thu, 12 Nov 2020 15:07:21 GMT	192.168.103...	40.97.30.130	59194	443	TCP	outlook-web...	12.38 KB	N/A	PaoloAlto-VE-01	US/United States	Intern
Thu, 12 Nov 2020 09:05:02 GMT	RTR_SanJose	Thu, 12 Nov 2020 15:07:13 GMT	Thu, 12 Nov 2020 15:07:21 GMT	192.168.103...	209.197.193...	59189	443	TCP	webex-meet...	5.83 KB	N/A	PaoloAlto-VE-01	US/United States	Intern
Thu, 12 Nov 2020 09:05:02 GMT	RTR_SanJose	Thu, 12 Nov 2020 15:07:19 GMT	Thu, 12 Nov 2020 15:07:21 GMT	192.168.103...	40.97.169.168	59199	443	TCP	http*	104 B	N/A	PaoloAlto-VE-01	US/United States	Intern
Thu, 12 Nov 2020 09:05:02 GMT	RTR_SanJose	Thu, 12 Nov 2020 15:07:20 GMT	Thu, 12 Nov 2020 15:07:21 GMT	192.168.103...	204.79.197.2...	59200	443	TCP	bing	1.19 KB	N/A	PaoloAlto-VE-01	US/United States	Intern
Thu, 12 Nov 2020 09:05:02 GMT	RTR_SanJose	Thu, 12 Nov 2020 15:07:20 GMT	Thu, 12 Nov 2020 15:07:21 GMT	192.168.103...	74.125.196.1...	59964	443	TCP	youtube	166 B	N/A	PaoloAlto-VE-01	US/United States	Intern
Thu, 12 Nov 2020 09:05:03 GMT	FWAN_BR_NET	Thu, 12 Nov 2020 15:06:40 GMT	Thu, 12 Nov 2020 15:06:40 GMT	22.1.1.20	202.12.27.33	55513	53	UDP	dns	56 B	US/United St.	Internet	JP/Japan	Intern
Thu, 12 Nov 2020 09:05:03 GMT	FWAN_BR_NET	Thu, 12 Nov 2020 15:06:40 GMT	Thu, 12 Nov 2020 15:06:40 GMT	22.1.1.20	202.12.27.33	53479	53	UDP	dns	71 B	US/United St.	Internet	JP/Japan	Intern
Thu, 12 Nov 2020 09:05:03 GMT	FWAN_BR_NET	Thu, 12 Nov 2020 15:06:40 GMT	Thu, 12 Nov 2020 15:06:40 GMT	22.1.1.20	202.12.27.33	51420	53	UDP	dns	71 B	US/United St.	Internet	JP/Japan	Intern
Thu, 12 Nov 2020 09:05:03 GMT	RTR_SanJose	Thu, 12 Nov 2020 15:06:22 GMT	Thu, 12 Nov 2020 15:07:22 GMT	199.199.1.2	224.0.0.10	0	0	EGRP	igmp	840 B	US/United St.	Internet	N/A	Intern
Thu, 12 Nov 2020 09:05:03 GMT	RTR_SanJose	Thu, 12 Nov 2020 15:07:18 GMT	Thu, 12 Nov 2020 15:07:22 GMT	192.168.103...	13.76.718.117	59187	443	TCP	ms.office-w...	1.47 KB	N/A	PaoloAlto-VE-01	US/United States	Intern

Filters can be applied to focus on the specific conversations of interest.

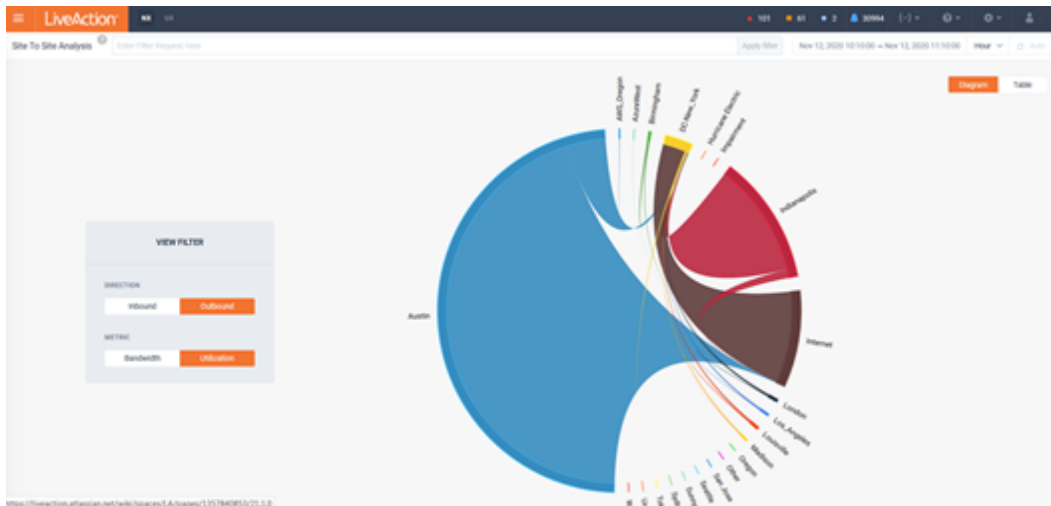
This screenshot shows the filter section of the Security Flow Analysis dashboard. It includes four filter groups: 'IP Addresses (Source / Destination)', 'Ports (Source / Destination)', 'Applications', and 'Protocols'. Each group has a text input field with an example value: 'ex: 192.168.1.1-200' for IP addresses, 'ex: 2416' for ports, 'ex: http' for applications, and 'ex: TCP' for protocols.

Historic time ranges can be selected for finding the Flows of interest.

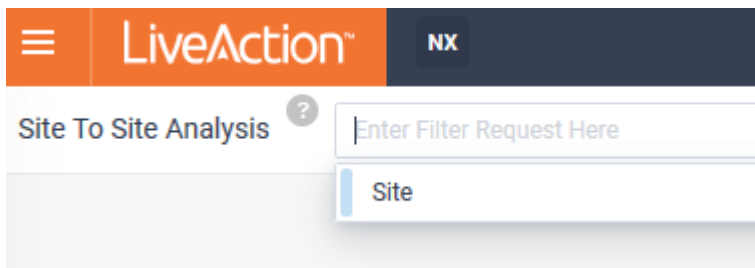


## Site to Site Analysis

The *Site to Site Analysis* story provides a chord diagram for understanding the bandwidth/ utilization between sites.



Filters can be applied to focus on the specific conversations of interest:



Historic time ranges can be selected for finding the Flows of interests.

Apply filter Feb 02, 2021 09:50:00 – Feb 02, 2021 10:05:00 15 Min ▾

**SET THE END DATE & TIME**

< Feb 2021 > Today

S	M	T	W	T	F	S
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	1	2	3	4	5	6
7	8	9	10	11	12	13

10 09 AM

Reset to Now

Apply

**INTERVAL**

5 Mins

15 Min

Hour

6 Hours

Day

Week

The page can optionally be auto-refreshed by toggling the **Auto** button in the top right of the page.



A *View Filter* is available for controlling the Flow's direction and metric in the diagram.

**VIEW FILTER**

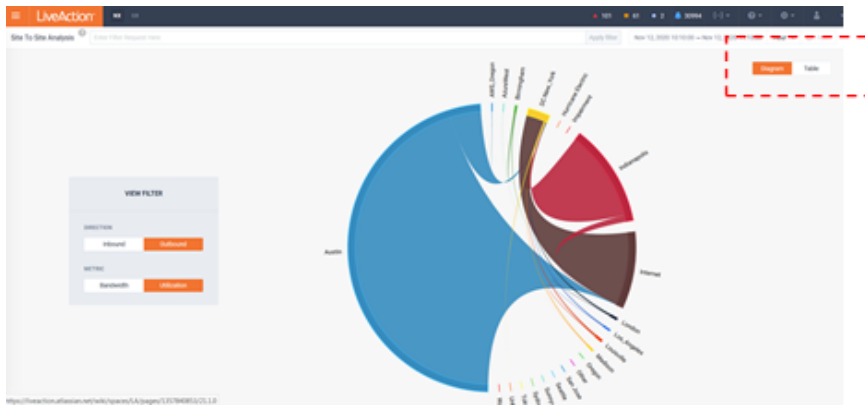
**DIRECTION**

Inbound Outbound

**METRIC**

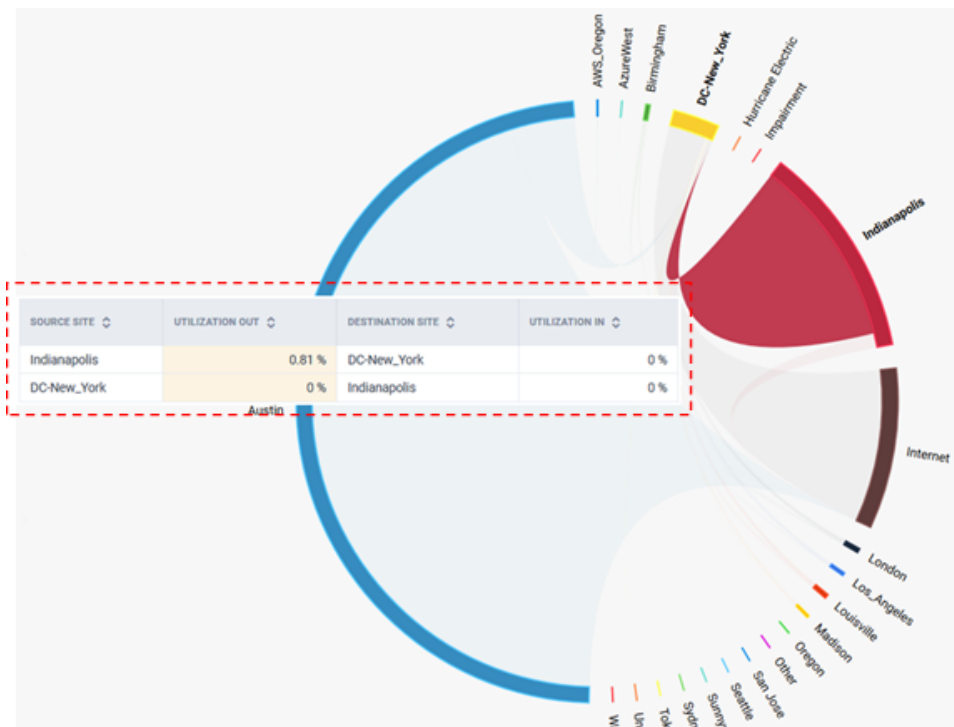
Bandwidth Utilization

The story can be displayed as either a *Chord Diagram* or *Table*.

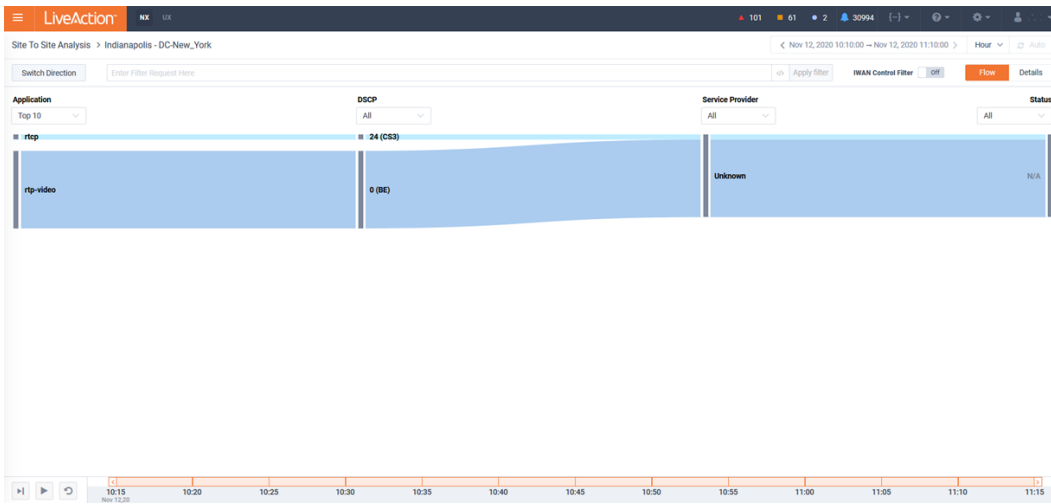


SOURCE SITE	UTILIZATION OUT	DESTINATION SITE	UTILIZATION IN
Austin	0.07%	Internet	0.08%
Indianapolis	0.01%	DC-New_York	0%
Internet	0.03%	DC-New_York	0.01%
Austin	0.07%	DC-New_York	0.01%
DC-New_York	0.16%	Internet	0.05%
Indianapolis	0.01%	Internet	0%
London	0.01%	DC-New_York	0.01%
DC-New_York	0.01%	Internet	0%
Louisville	0.01%	DC-New_York	0.01%
Birmingham	0.01%	DC-New_York	0.01%

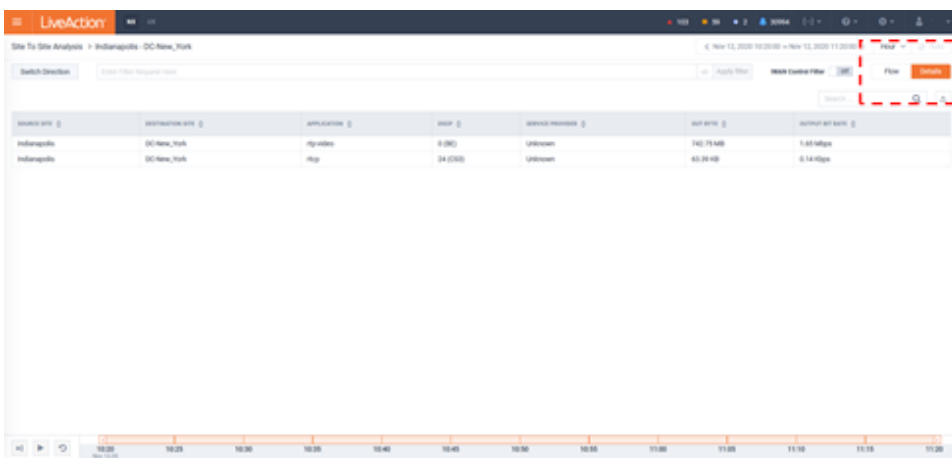
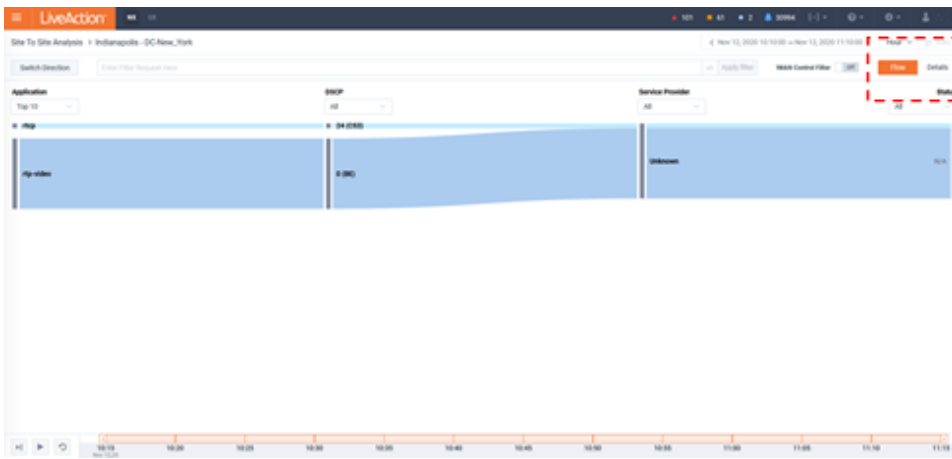
Highlighting a chord will show the details of the bandwidth/ utilization between the sites highlighted. Clicking on a chord will launch a Sankey diagram.



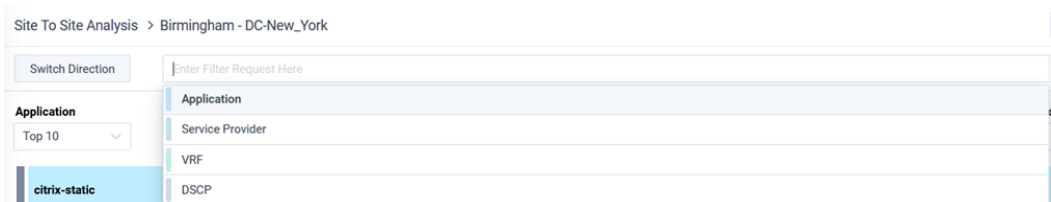
The *Site To Site* story Sankey diagram provides further details on the bandwidth/utilization between the sites selected.



The Sankey diagram can be viewed in either a *Flow* or *Details* view.



Filters can be applied to focus on the specific conversations of interest:



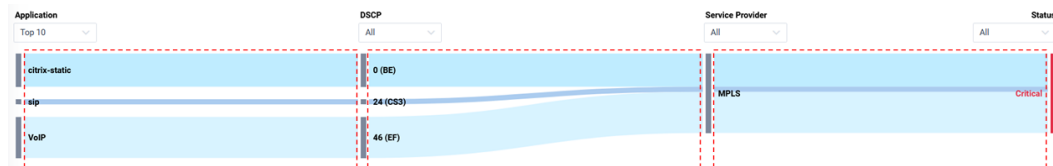


Historic time ranges can be selected for finding the Flows of interests.

The page can optionally be auto-refreshed by toggling the **Auto** button in the top right of the page.



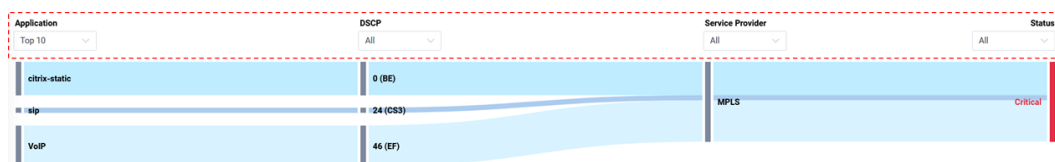
The Sankey diagram highlights the applications, their DSCP, the service provider path the application took, and its status. Clicking on the chords in the Sankey diagram will pivot to a curated historic report template.



This template includes the following reports:

- Application
- DSCP
- App Group (DSCP) by Service Provider
- Jitter/ Loss
- Application Performance (AVC)
- Service Provider Performance (PFR)

Filters located at the top of the Sankey diagram can be used to further refine the data shown.



The *IWAN Control Filter* can be used to hide IWAN Smartprobe traffic on the Sankey diagram.

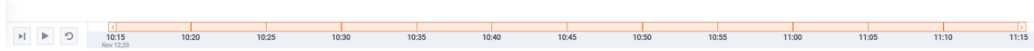
**IWAN Control Filter**  Off

The **Switch Direction** button can be used to reverse the source/destination site visualized in the Sankey diagram.

Site To Site Analysis > Birmingham - DC-New\_York

Switch Direction

A timeline slider is available at the bottom of the Sankey diagram to understand the context over time.



Advanced to next bin window:



“Play” the Sankey Diagram bin by bin:



“Pause” the Sankey Diagram on the current bin:



Reset view to complete time window:



## Calls by Number

LiveAction LiveWire devices can send a unique type of Flow called LiveAction LiveFlow that includes the IP address of VoIP endpoints and their associated SIP Directory Numbers (DN). This allows operators the ability to find specific conversations of interest based on phone number.

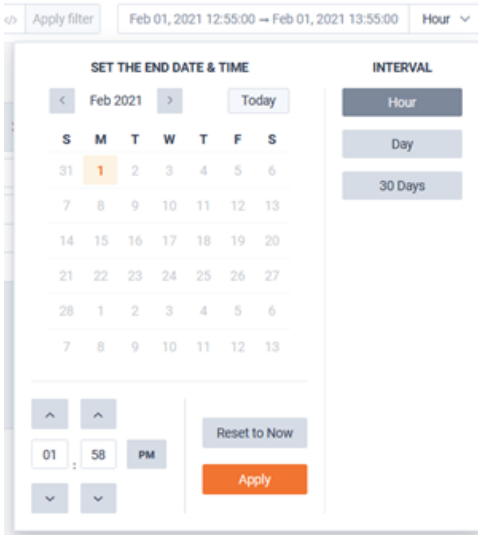
The screenshot shows a web interface titled 'Search Calls By Number'. It includes a search bar, a filter dropdown set to 'All', and a table of call records. The table has columns for TIME, PROTOCOL, DN1, MEDIA ENDPOINT IP, MEDIA ENDPOINT PORT, PEEK, JITTER/LOSS REPORT, and FLOW PATH ANALYSIS. Three call records are visible, each with a 'Peek' button and a red error icon.

TIME	PROTOCOL	DN1	MEDIA ENDPOINT IP	MEDIA ENDPOINT PORT	PEEK	JITTER/LOSS REPORT	FLOW PATH ANALYSIS
15 Nov 2020, 12:36PM	SIP	1009	0.0.0.0	5012	Peek		
15 Nov 2020, 12:35PM	SIP	1007	208.73.56.155	12000	Peek		
15 Nov 2020, 12:35PM	SIP	1009	192.168.10.202	5012	Peek		

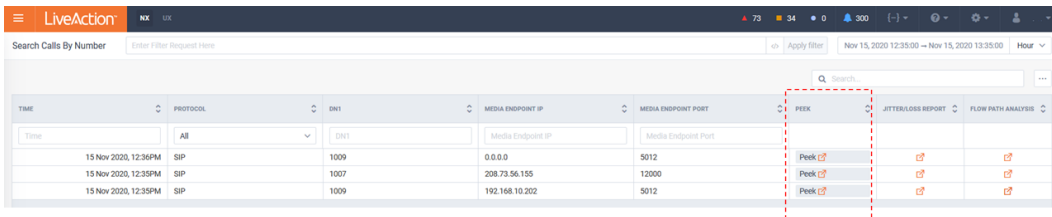
Filtering can be applied to find the specific calls of interests.



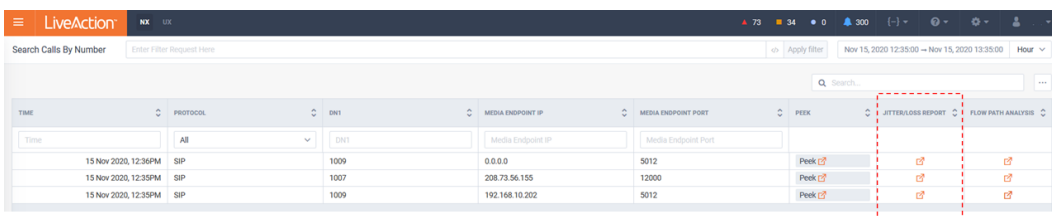
Historic time ranges can be selected for finding the conversations of interests.

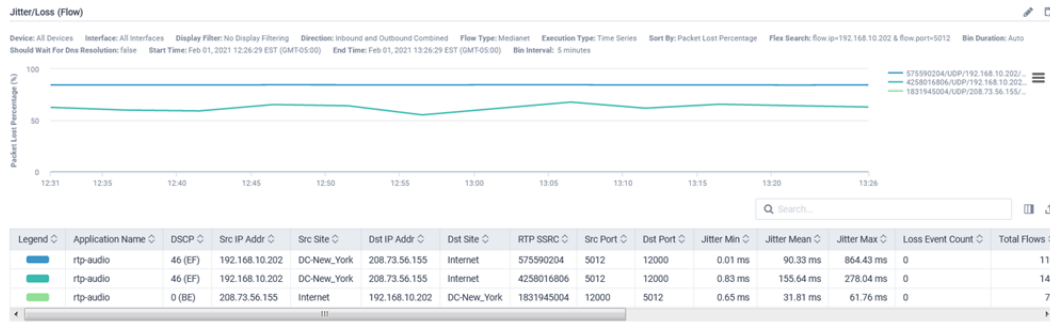


Selecting **Peek** will cross-launch to LiveNX Peek (Packets) with a filter of IP Address and Port of the selected Flow.



Selecting *Jitter/Loss Report* will drill-down to the applicable historic report.





Selecting *Flow Path Analysis* will drill-down to the Flow Path Analysis Story with the Filter pre-assigned for the selected conversation. Operators can perform a hop-by-hop analysis on a selected Flows.

TIME	PROTOCOL	DN1	MEDIA ENDPOINT IP	MEDIA ENDPOINT PORT	PEEK	JITTER/LOSS REPORT	FLOW PATH ANALYSIS
15 Nov 2020, 12:36PM	SIP	1009	0.0.0.0	5012	Peek		
15 Nov 2020, 12:35PM	SIP	1007	208.73.56.155	12000	Peek		
15 Nov 2020, 12:35PM	SIP	1009	192.168.10.202	5012	Peek		

STATUS	PEEK	FLOW P.	TIME	SRC IP	SRC PORT	SRC SITE	DST IP	DST PORT	DST SITE	APPLICATION	RTP SSRC	DSCP	PACKET LOSS	JITTER AVG	JITTER MAX	AVG MOS
●	≡	🔍	01 Feb 2021, 12:00PM	192.168.10.202	5012	DC-New_York	208.73.56.155	12000	Internet	rtp-audio	575590204	46 (EF)	84.64%	67.98 ms	863.45 ms	4.3
●	≡	🔍	01 Feb 2021, 12:40PM	192.168.10.202	5012	DC-New_York	208.73.56.155	12000	Internet	rtp-audio	575590204	46 (EF)	84.64%	67.98 ms	863.46 ms	4.3
●	≡	🔍	01 Feb 2021, 12:50PM	192.168.10.202	5012	DC-New_York	208.73.56.155	12000	Internet	rtp-audio	575590204	46 (EF)	84.61%	67.95 ms	863.49 ms	4.3
●	≡	🔍	01 Feb 2021, 12:05PM	192.168.10.202	5012	DC-New_York	208.73.56.155	12000	Internet	rtp-audio	575590204	46 (EF)	84.61%	67.95 ms	863.45 ms	4.3
●	≡	🔍	01 Feb 2021, 12:13PM	192.168.10.202	5012	DC-New_York	208.73.56.155	12000	Internet	rtp-audio	575590204	46 (EF)	84.61%	67.95 ms	863.48 ms	4.3
●	≡	🔍	01 Feb 2021, 12:30PM	192.168.10.202	5012	DC-New_York	208.73.56.155	12000	Internet	rtp-audio	575590204	46 (EF)	84.61%	67.95 ms	863.46 ms	4.3
●	≡	🔍	01 Feb 2021, 12:23PM	192.168.10.202	5012	DC-New_York	208.73.56.155	12000	Internet	rtp-audio	575590204	46 (EF)	84.59%	67.92 ms	863.45 ms	4.3
●	≡	🔍	01 Feb 2021, 12:45PM	192.168.10.202	5012	DC-New_York	208.73.56.155	12000	Internet	rtp-audio	575590204	46 (EF)	84.56%	67.90 ms	863.49 ms	4.3
●	≡	🔍	01 Feb 2021, 12:55PM	192.168.10.202	5012	DC-New_York	208.73.56.155	12000	Internet	rtp-audio	575590204	46 (EF)	84.54%	67.90 ms	864.43 ms	NAN
●	≡	🔍	01 Feb 2021, 12:35PM	192.168.10.202	5012	DC-New_York	208.73.56.155	12000	Internet	rtp-audio	575590204	46 (EF)	84.48%	67.82 ms	863.45 ms	4.3
●	≡	🔍	01 Feb 2021, 12:20PM	192.168.10.202	5012	DC-New_York	208.73.56.155	12000	Internet	rtp-audio	575590204	46 (EF)	84.46%	67.79 ms	863.47 ms	4.3
●	≡	🔍	01 Feb 2021, 12:10PM	192.168.10.202	5012	DC-New_York	208.73.56.155	12000	Internet	rtp-audio	575590204	46 (EF)	84.46%	67.79 ms	863.48 ms	4.3
●	≡	🔍	01 Feb 2021, 11:55AM	192.168.10.202	5012	DC-New_York	208.73.56.155	12000	Internet	rtp-audio	575590204	46 (EF)	84.38%	67.71 ms	863.47 ms	4.3
●	≡	🔍	01 Feb 2021, 11:55AM	192.168.10.202	5012	DC-New_York	208.73.56.155	12000	Internet	rtp-audio	4258016806	46 (EF)	67.10%	134.39 ms	252.21 ms	NAN
●	≡	🔍	01 Feb 2021, 12:40PM	192.168.10.202	5012	DC-New_York	208.73.56.155	12000	Internet	rtp-audio	4258016806	46 (EF)	65.46%	130.21 ms	229.84 ms	NAN
●	≡	🔍	01 Feb 2021, 12:00PM	192.168.10.202	5012	DC-New_York	208.73.56.155	12000	Internet	rtp-audio	4258016806	46 (EF)	64.84%	140.47 ms	260.48 ms	NAN
●	≡	🔍	01 Feb 2021, 12:45PM	192.168.10.202	5012	DC-New_York	208.73.56.155	12000	Internet	rtp-audio	4258016806	46 (EF)	64.28%	124.98 ms	213.54 ms	NAN

WAN Applications > Application: > PATH UDP 192.168.10.202 : 5012 - 208.73.56.155 : 12000



Device Name	SE-LiveWire-NY	SE-LiveWire-LA
Site Name	DC-New_York	Los_Angeles
Application	rtp-audio	rtp-audio
CPU Usage	-	2.00 %
Memory Usage	-	49.00 %
In Interface	7	eth1
Out Interface	7	eth1
In QoS Policy	-	No Policy
Out QoS Policy	-	No Policy
Bytes In	0.00 bytes	0.00 bytes
Bytes Out	0.00 bytes	0.00 bytes
Jitter Average	140.47 ms	67.98 ms
Packet Loss Rate	53.63 %	77.88 %

# WAN Availability

The *WAN Availability* story will highlight the available statistics of the WAN interfaces monitored by LiveNX.

Site	Device	Interface	Service Provider	IP Address	Avg Availability	Avg Daily Downtime
Palo Alto	HNL-CSR1K1	GigabitEthernet2	MPLS	-	0%	1,640 minutes
LondonEdge	LondonEdge	ge0/1	mpls	-	0%	1,640 minutes
TexasEdge	TexasEdge	ge0/0	isp-internet	-	0%	1,640 minutes
TexasEdge	TexasEdge	ge0/5	public-internet	-	0%	1,640 minutes
NewYorkEdge	NewYorkEdge	ge0/0	isp-internet	172.16.11.4	98.51%	21.44 minutes
NewYorkEdge	NewYorkEdge	ge0/1	mpls	52.0.11.1	98.51%	21.44 minutes
NewYorkEdge	NewYorkEdge	ge0/5	public-internet	115.192.195.30	98.51%	21.44 minutes
Site 5	IWAN-BR_INET	Tunnel101	DMVPN over Internet	172.16.2.254	99.68%	4.63 minutes
Site 5	IWAN-BR_INET	GigabitEthernet2	Default Service Provider	11.11.11.3	99.68%	4.63 minutes
Site 5	IWAN-BR_INET	GigabitEthernet4	Default Service Provider	21.11.254	99.68%	4.63 minutes
Site 5	IWAN-BR_MPLS	Tunnel100	DMVPN over MPLS	172.16.1.254	99.71%	4.14 minutes
Site 5	IWAN-BR_MPLS	GigabitEthernet2	Default Service Provider	11.11.11.2	99.71%	4.14 minutes
Site 5	IWAN-BR_MPLS	GigabitEthernet4	Default Service Provider	20.11.254	99.71%	4.14 minutes
PaloAlto-VE-01	RTL_SanJose	GigabitEthernet2	Conn-MPLS-Provider	199.199.1.13	99.97%	0.44 minutes
SanJose	MPLS-CORE	GigabitEthernet2	MPLS	10.255.0.253	99.98%	0.29 minutes
Seattle	RTL_Seattle	GigabitEthernet2	MPLS	199.199.1.1	99.98%	0.24 minutes
New York - DC	RTL-DC-CORE	GigabitEthernet2	MPLS	199.199.1.13	100%	0.05 minutes
Site 5	IWAN-BR_Sydney	GigabitEthernet2	Default Service Provider	199.199.1.13	100%	0 minutes
Site 5	IWAN-BR_Sydney	GigabitEthernet4	Default Service Provider	21.11.254	100%	0 minutes
Site 5	IWAN-BR_Sydney	Tunnel100	DMVPN over MPLS	172.16.1.1	100%	0 minutes
Site 5	IWAN-BR_Sydney	Tunnel101	DMVPN over Internet	172.16.2.1	100%	0 minutes

A Filter can be used to narrow the scope of the story.

LiveAction NX

WAN Availability

Enter Filter Request Here

- Site
- Service Provider
- Device
- Interface
- Tag
- Group
- Region

Historic Time intervals can be used.

ter Jan 02, 2021 14:40:00 -> Feb 01, 2021 14:40:00 30 Days

Search...

AVAILABILITY

AVG DAILY D

g Availability

Avg Daily

0%

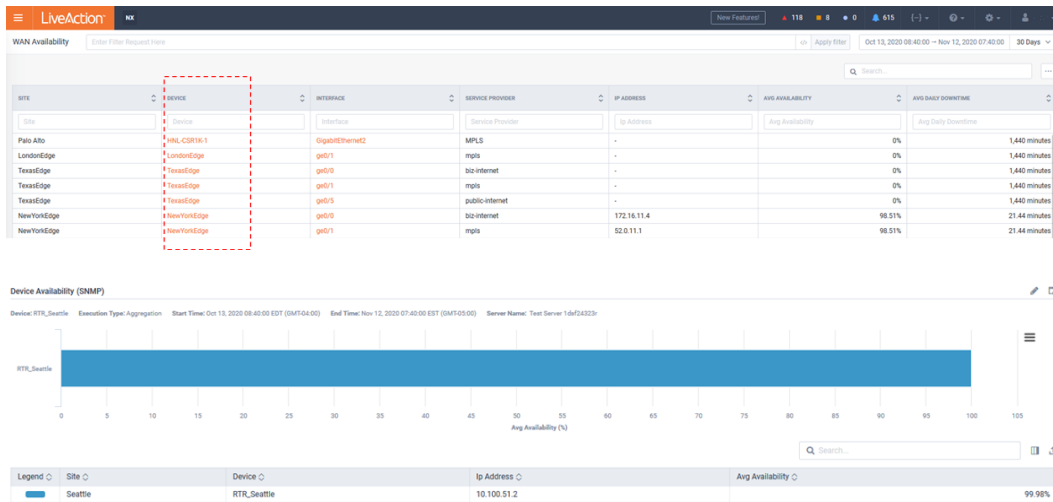
0%

1,640 minutes

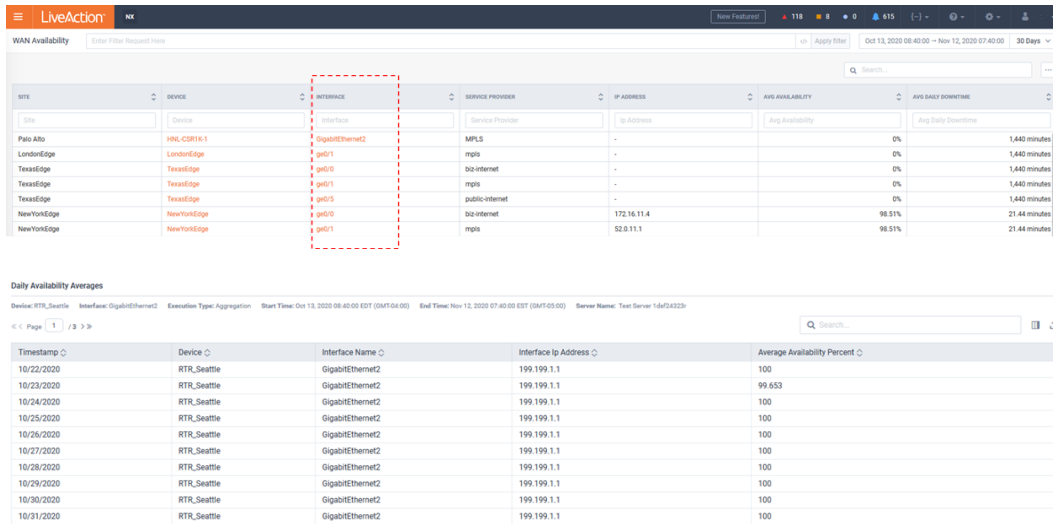
INTERVAL

- 30 Days
- 3 Months
- 6 Months
- Year

Selecting a device will drill-down to a *Device Availability* report.

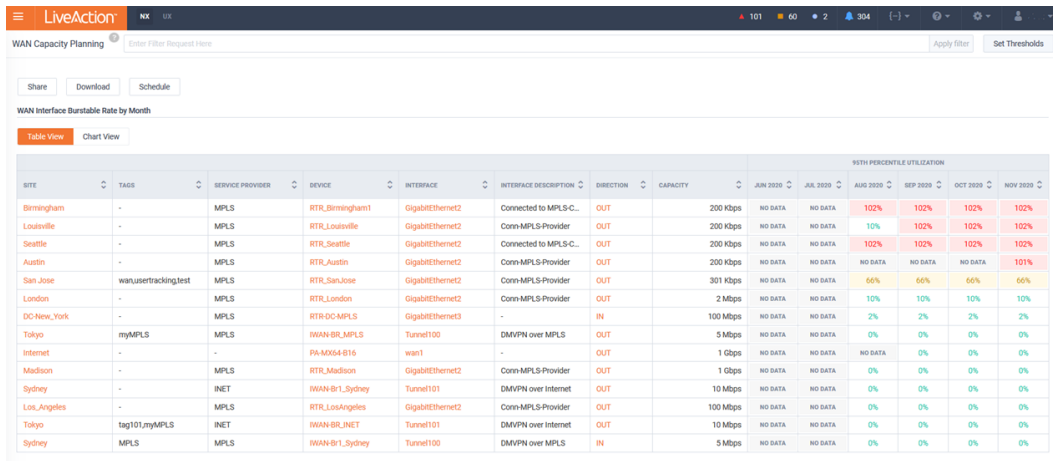


Selecting an interface will drill-down to a *Daily Availability Average* report.

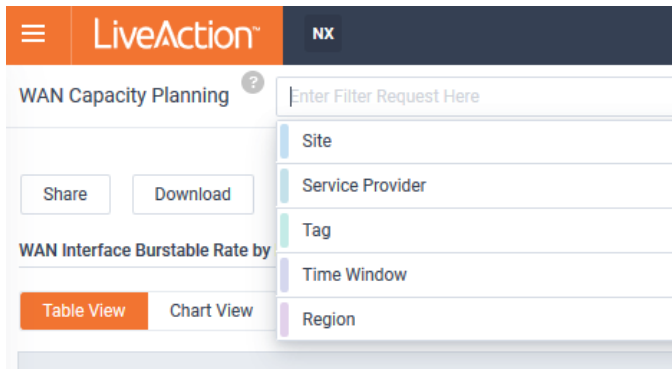


## WAN Capacity Planning

The *WAN Capacity Planning* story will monitor each WAN interface's monthly utilization for the previous six months. This data is based on SNMP utilization.



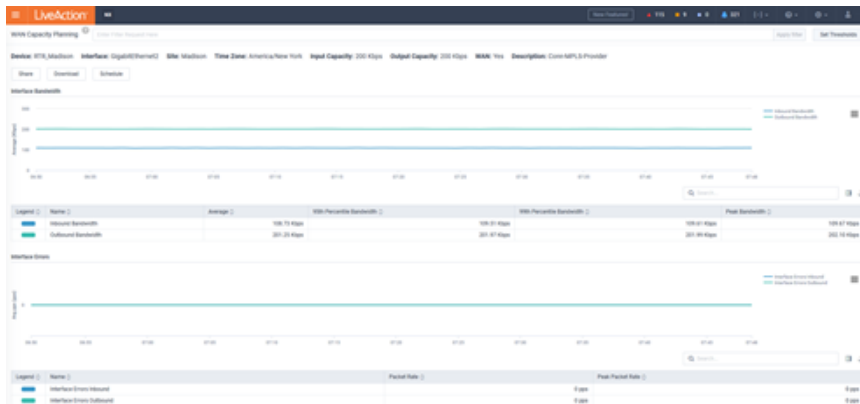
The reported interfaces can be Filtered to focus the scope of the Story.



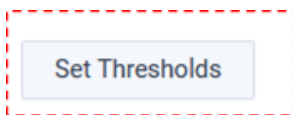
Clicking the details of the story will pivot to a curated historic report template for the WAN interface during the month selected.

The screenshot displays a table view of WAN Capacity Planning data. The table has columns for Site, Provider, Service, Reference, Reference Description, Direction, Capacity, and a 'WAN Performance Metrics' section with sub-columns for Avg 2020, Jul 2020, Aug 2020, Sep 2020, Oct 2020, and Nov 2020. A red dashed box highlights the right side of the table, including the performance metrics columns.

Site	Provider	Service	Reference	Reference Description	Direction	Capacity	WAN Performance Metrics					
							Avg 2020	Jul 2020	Aug 2020	Sep 2020	Oct 2020	Nov 2020
Birmingham	MPLS	BTB_Birmingham	SignalTherm02	Connected to MPLS-C	OUT	200 Kbps	NO DATA	NO DATA	100%	100%	100%	100%
LosAngeles	MPLS	BTB_LosAngeles	SignalTherm02	Conn-MPLS-Provider	OUT	200 Kbps	NO DATA	NO DATA	100%	100%	100%	100%
Seattle	MPLS	BTB_Seattle	SignalTherm02	Connected to MPLS-C	OUT	200 Kbps	NO DATA	NO DATA	100%	100%	100%	100%
Austin	MPLS	BTB_Austin	SignalTherm02	Conn-MPLS-Provider	OUT	200 Kbps	NO DATA	NO DATA	NO DATA	NO DATA	NO DATA	100%
San Jose	www.lackofsignal.com	BTB_SanJose	SignalTherm02	Conn-MPLS-Provider	OUT	300 Kbps	NO DATA	NO DATA	90%	90%	90%	90%
London	MPLS	BTB_London	SignalTherm02	Conn-MPLS-Provider	OUT	2 Mbps	NO DATA	NO DATA	10%	10%	10%	10%
DCNew_York	MPLS	BTB_DC_MPLS	SignalTherm02	-	IN	100 Mbps	NO DATA	NO DATA	2%	2%	2%	2%
Tokyo	Hybrid MPLS	WAN01_MPLS	Tun01100	DMVPN over MPLS	OUT	5 Mbps	NO DATA	NO DATA	0%	0%	0%	0%
Internet	-	WAN0004-010	wan1	-	OUT	1 Gbps	NO DATA	NO DATA	0%	0%	0%	0%
Madison	MPLS	BTB_Madison	SignalTherm02	Conn-MPLS-Provider	OUT	1 Gbps	NO DATA	NO DATA	0%	0%	0%	0%
Sydney	NET	WAN01_Sydney	Tun01101	DMVPN over Internet	OUT	10 Mbps	NO DATA	NO DATA	0%	0%	0%	0%
Los_Angeles	MPLS	BTB_LosAngeles	SignalTherm02	Conn-MPLS-Provider	OUT	100 Mbps	NO DATA	NO DATA	0%	0%	0%	0%
Tokyo	Hybrid MPLS	WAN01_MPLS	Tun01101	DMVPN over Internet	OUT	10 Mbps	NO DATA	NO DATA	0%	0%	0%	0%
Sydney	MPLS	WAN01_Sydney	Tun01100	DMVPN over MPLS	IN	5 Mbps	NO DATA	NO DATA	0%	0%	0%	0%



To manage the color coding of the table in the story, select *Set Thresholds*.



95TH PERCENTILE UTILIZATION			
AUG 2020	SEP 2020	OCT 2020	NOV 2020
102%	102%	102%	102%
10%	102%	102%	102%
102%	102%	102%	102%
NO DATA	NO DATA	NO DATA	101%
66%	66%	66%	66%
10%	10%	10%	10%
2%	2%	2%	2%
0%	0%	0%	0%
NO DATA	0%	0%	0%
0%	0%	0%	0%
0%	0%	0%	0%
0%	0%	0%	0%
0%	0%	0%	0%
0%	0%	0%	0%

Multi-instance Filters can be used to set the thresholds colors used by the story.

**WAN Interface Capacity Thresholds** ×

---

LIST OF INSTANCES ③
ADD NEW INSTANCE
INSTANCE DETAILS

Default threshold

**General Settings**

Instance Name

Time Window

Threshold Source

**Thresholds**

▲ CRITICAL

Utilization > 80 %

■ WARNING

Utilization > 50 %

● INFO

Utilization More than 20 %

Filters and Time Window can be used for instance to further refine these thresholds.



WAN Interface Capacity Thresholds

## WAN Utilization

The *WAN Utilization* story provides a utilization summary of each WAN interface. This includes Average, Peak, and 95<sup>th</sup> Percentile statistics for the selected time period. This data is based on SNMP utilization.

Site	Device	Service Provider	Interface Name	Direction	Capacity	Average Utilization	Peak Utilization	95th Percentile Utilization	Status
New York-DC	RTR-DC-MPLS	MPLS	GigabitEthernet2	Outbound	200 Kbps	51%	53%	53%	Good
New York-DC	RTR-DC-MPLS	MPLS	GigabitEthernet2	Inbound	200 Kbps	42%	42%	42%	Good
Louisville	RTR-Louisville	Conn-MPLS-Provider	GigabitEthernet2	Outbound	200 Kbps	102%	102%	102%	Critical
Birmingham	RTR-Birmingham1	MPLS	GigabitEthernet2	Outbound	200 Kbps	102%	102%	102%	Critical
PaloAlto-VE-G1	RTR-London	Conn-MPLS-Provider	GigabitEthernet2	Outbound	200 Kbps	101%	101%	101%	Good
Site 5	RTR-Austin	MPLS	GigabitEthernet2	Outbound	200 Kbps	101%	101%	101%	Good
Seattle	RTR-Seattle	MPLS	GigabitEthernet2	Outbound	200 Kbps	101%	101%	101%	Critical
Madison	RTR-Madison	MPLS	GigabitEthernet2	Outbound	200 Kbps	101%	101%	101%	Good
PaloAlto-VE-G1	RTR-SanJose	Conn-MPLS-Provider	GigabitEthernet2	Outbound	200 Kbps	96%	99%	99%	Good
New York-DC	RTR-DC-CORE	MPLS	GigabitEthernet2	Outbound	500 Kbps	88%	96%	96%	Critical
Louisville	RTR-Louisville	Conn-MPLS-Provider	GigabitEthernet2	Inbound	200 Kbps	56%	56%	56%	Critical
PaloAlto-VE-G1	RTR-London	Conn-MPLS-Provider	GigabitEthernet2	Inbound	200 Kbps	54%	54%	54%	Good
Site 5	RTR-Austin	MPLS	GigabitEthernet2	Inbound	200 Kbps	54%	54%	54%	Good
Birmingham	RTR-Birmingham1	MPLS	GigabitEthernet2	Inbound	200 Kbps	54%	54%	54%	Critical
PaloAlto-VE-G1	RTR-SanJose	Conn-MPLS-Provider	GigabitEthernet2	Inbound	200 Kbps	54%	54%	54%	Good
Madison	RTR-Madison	MPLS	GigabitEthernet2	Inbound	200 Kbps	54%	54%	54%	Good
Seattle	RTR-Seattle	MPLS	GigabitEthernet2	Inbound	200 Kbps	54%	54%	54%	Good
Site 5	RTR-Seattle	MPLS	GigabitEthernet2	Inbound	200 Kbps	52%	52%	52%	Critical
Site 5	WAN-Bri_Sydney	Default Service Provider	GigabitEthernet2	Inbound	1 Mbps	2%	2%	2%	Good
Site 5	WAN-Bri_Sydney	Default Service Provider	GigabitEthernet2	Outbound	1 Mbps	2%	2%	2%	Good
New York-DC	RTR-DC-MPLS	MPLS	GigabitEthernet3	Inbound	1 Gbps	0%	0%	0%	Good
New York-DC	RTR-DC-MPLS	MPLS	GigabitEthernet3	Outbound	1 Gbps	0%	0%	0%	Good
NewYorkEdge	NewYorkEdge	bz-internet	ge0/0	Outbound	1 Gbps	0%	0%	0%	Good

A Filter can be used to narrow the scope of the story.

Historic Time intervals can be used.

Apply filter Feb 02, 2021 10:25:00 → Feb 02, 2021 11:25:00 Hour

**SET THE END DATE & TIME**

< Feb 2021 > Today

S	M	T	W	T	F	S
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	1	2	3	4	5	6
7	8	9	10	11	12	13

11 : 28 AM

Reset to Now

Apply

**INTERVAL**

Hour

Day

Week

30 Days

3 Months

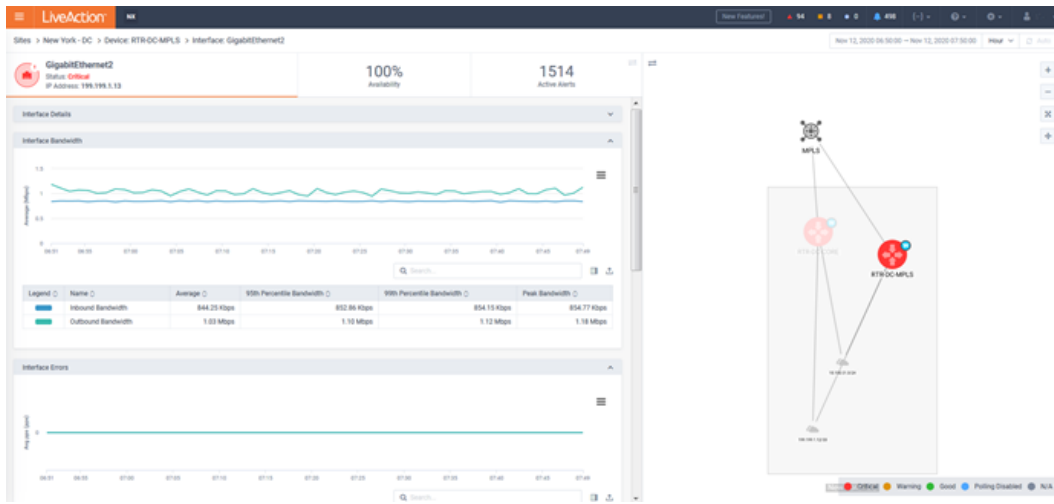
6 Months

Year

Clicking on an interface will pivot to the Interface Entity page for further investigation.

LiveAction WAN Utilization

Site	Service	Service Provider	Interface Name	Direction	Capacity	Average Utilization	Peak Utilization	95th Percentile Utilization	Status
New York - DC	RTS-DC-MPLS	MPLS	igmp01@net02	Outbound	200 Kbps	516%	516%	516%	Good
New York - DC	RTS-DC-MPLS	MPLS	igmp01@net02	Inbound	200 Kbps	422%	424%	424%	Good
Louisville	RTS-Louisville	Com-MPLS-Provider	igmp01@net02	Outbound	200 Kbps	102%	102%	102%	Critical
Birmingham	RTS-Birmingham1	MPLS	igmp01@net02	Outbound	200 Kbps	102%	102%	102%	Critical
PaloAlto-VE-01	RTS-London	Com-MPLS-Provider	igmp01@net02	Outbound	200 Kbps	101%	101%	101%	Good
Site 5	RTS-Austin	MPLS	igmp01@net02	Outbound	200 Kbps	101%	101%	101%	Good
Seattle	RTS-Seattle	MPLS	igmp01@net02	Outbound	200 Kbps	101%	101%	101%	Critical
Madison	RTS-Madison	MPLS	igmp01@net02	Outbound	200 Kbps	101%	101%	101%	Good
PaloAlto-VE-01	RTS-SanJose	Com-MPLS-Provider	igmp01@net02	Outbound	200 Kbps	96%	96%	96%	Good
New York - DC	RTS-DC-CORE	MPLS	igmp01@net02	Outbound	200 Kbps	96%	96%	96%	Critical
Louisville	RTS-Louisville	Com-MPLS-Provider	igmp01@net02	Inbound	200 Kbps	54%	54%	54%	Critical
PaloAlto-VE-01	RTS-London	Com-MPLS-Provider	igmp01@net02	Inbound	200 Kbps	54%	54%	54%	Good
Site 5	RTS-Austin	MPLS	igmp01@net02	Inbound	200 Kbps	54%	54%	54%	Good
Birmingham	RTS-Birmingham1	MPLS	igmp01@net02	Inbound	200 Kbps	54%	54%	54%	Critical
PaloAlto-VE-01	RTS-SanJose	Com-MPLS-Provider	igmp01@net02	Inbound	200 Kbps	54%	54%	54%	Good
Madison	RTS-Madison	MPLS	igmp01@net02	Inbound	200 Kbps	54%	54%	54%	Good
Seattle	RTS-Seattle	MPLS	igmp01@net02	Inbound	200 Kbps	52%	52%	52%	Critical
Site 5	ISAAA@1_Sydney	Default Service Provider	igmp01@net02	Inbound	1 Mbps	2%	2%	2%	Good
Site 5	ISAAA@1_Sydney	Default Service Provider	igmp01@net02	Outbound	1 Mbps	2%	2%	2%	Good
New York - DC	RTS-DC-MPLS	MPLS	igmp01@net03	Inbound	1 Gbps	0%	0%	0%	Good
New York - DC	RTS-DC-MPLS	MPLS	igmp01@net03	Outbound	1 Gbps	0%	0%	0%	Good
NewYorkEdge	NewYorkEdge	IS-internet	g010	Outbound	1 Gbps	0%	0%	0%	Good



## Reports

### In this chapter:

<i>Reports</i> .....	110
<i>View Reports</i> .....	117
<i>Custom Reports</i> .....	135
<i>View Schedule</i> .....	140

## Reports

### List of Reports

The following table lists the reports available in LiveNX:

Report
Alert Count By Category (alert)
Alert Count By Device (alert)
Alert Count By Region (alert)
Alert Count By Severity (alert)
Alert Count By Site (alert)
Alert Count By Type (alert)
Alert Count By Wan Interface (alert)
Alerts (qos)
Alerts All (flow)
Alerts by App Group (DSCP) (flow)
Alerts by App Group (DSCP) and Service Provider (flow)
Alerts by Device (qos)
Alerts by Interface (qos)
Alerts by Service Provider (flow)
Alerts by Site (flow)
Alerts by Site and App Group (DSCP) (flow)
Alerts by Site and Service Provider (flow)
Alerts by Site Pair (flow)
Alerts by Site Pair and App Group (DSCP) (flow)
Alerts by Site Pair and Service Provider (flow)
Alerts/Utilization by Site (qos)
All Unique Flows (flow)
AnyConnect Application Versions (flow)
AnyConnect Applications (flow)
AnyConnect User Devices (flow)
AnyConnect User Summary (flow)
AnyConnect Users (flow)
App Group (DSCP) Bandwidth (flow)
App Group (DSCP) Bandwidth by Service Provider (flow)
App Group (DSCP) Bandwidth by Site (flow)
Application (Analytics) (test)
Application by Device (alert)
Application by Region (alert)
Application by Site (alert)
Application DSCP Audit (flow)
Application Performance Audit (flow)
Application Performance By Device (flow)
Application Performance By Interface (flow)
Application Performance By Service Provider (flow)

**Report**

Application Performance By Site (flow)

Application Performance By User (flow)

Application Performance Over Time (flow)

Application Site to Site (alert)

Application Thresholding (Analytics) (test)

Application Troubleshooting Over Time (flow)

Availability Totals (qos)

AVC Test (flow)

Bandwidth Summary (flow)

Business Relevance (flow)

Corrected vs. Uncorrected (flow)

Destination Country (flow)

Destination Site Traffic (flow)

Device and Interface Top 10 Applications and Other (flow)

Device and Interface Top 10 DSCPs and Other (flow)

Device Flow Count (flow)

Dynamic 2 (flow)

Dynamic1 (flow)

Exporter Site Bandwidth (flow)

Flow Path Analysis (AVC) (flow)

Flow Path Analysis (Basic) (flow)

Flow Path Analysis (Medianet) (flow)

Interface Bandwidth (flow)

Interface Bandwidth Summary (flow)

IPs and Ports (flow)

Jitter/Loss (flow)

LiveAgent Hostname (flow)

LiveAgent OS Platform (flow)

LiveAgent Process Command (flow)

LiveAgent User Account ID (flow)

Multicast Audit (flow)

Network Users Applications Audio/Video Issues Detail (flow)

Network Users Applications Audio/Video Issues Summary (flow)

Network Users Applications Detail (flow)

Network Users Applications HTTP/TCP Issues Detail (flow)

Network Users Applications HTTP/TCP Issues Summary (flow)

Network Users Applications Summary (flow)

Network Users Bandwidth Detail (flow)

Network Users Bandwidth Summary (flow)

Network Users Endpoint Profile Detail (flow)

Network Users Endpoint Profile Summary (flow)

Network Users Summary (flow)

Outbound Bandwidth Utilization (flow)

Performance by App Group (DSCP) (flow)

**Report**

Performance by Service Provider (flow)
Performance by Site (flow)
Performance by Site and App Group (DSCP) (flow)
Performance by Site and Service Provider (flow)
Performance by Site Pair (flow)
Performance by Site Pair and App Group (DSCP) (flow)
Performance by Site Pair and Service Provider (flow)
Search Calls By Number (flow)
Service Provider Bandwidth (flow)
Service Provider Bandwidth by App Group (DSCP) (flow)
Service Provider Bandwidth by Site (flow)
Site and Service Provider Top 10 WAN Applications and Other (flow)
Site and Service Provider Top 10 WAN DSCPs and Other (flow)
Site Capacity Utilization (flow)
Site Capacity Utilization by App Group (DSCP) (flow)
Site Capacity Utilization by Service Provider (flow)
Site to Site Application Performance (flow)
Site to Site Application Response Time (flow)
Site to Site Jitter/Loss by Service Provider (flow)
Site to Site Outbound Service Provider (flow)
Site to Site Outbound Top 10 Applications and Other (flow)
Site to Site Outbound Top 10 DSCPs and Other (flow)
Site to Site Outbound VRF (flow)
Site Traffic (flow)
Site Traffic App (flow)
Site Traffic WAN (flow)
Source Country (flow)
Source Site Traffic (flow)
Test AVC (flow)
test basic (flow)
Top Applications By LiveAgent User (flow)
Top Conversations By LiveAgent User (flow)
Top DSCP By LiveAgent User (flow)
Top Voice/Video Performance by SSRC (flow)
Top Voice/Video Performance Summary (flow)
Traffic Class (flow)
Type by Device (alert)
Type by Interface (alert)
Type by Region (alert)
Type by Site (alert)
User Filter (flow)
User Filter DSCP Audit (flow)
Voice/Video Performance Audit (flow)
Voice/Video Performance By Device (flow)

**Report**

Voice/Video Performance By Interface (flow)

Voice/Video Performance By Service Provider (flow)

Voice/Video Performance By Site (flow)

Voice/Video Performance By User (flow)

VPN (flow)

VRF (flow)

Wireless Access Point (flow)

Wireless Access Point Application (flow)

Wireless Access Point Unique Clients (flow)

Wireless Client (flow)

Wireless SSID (flow)

Wireless SSID Application (flow)

Wireless SSID DSCP (flow)

Wireless SSID Unique Clients (flow)

ACL Pair (flow)

Application (flow)

Application Group (flow)

AS Pair (flow)

Bidirectional AS Pair (flow)

Bidirectional Network Pair (flow)

Bidirectional Source/Destination Pair (flow)

Destination Address (flow)

Destination Address Popularity (flow)

Destination AS (flow)

Destination Network (flow)

DSCP (flow)

DSCP vs Application (flow)

HTTP Host (flow)

Network Pair (flow)

Network Security Denied Events (flow)

Out of Policy Events (flow)

Protocol (flow)

Protocol Port (flow)

Security Analysis (flow)

Source Address (flow)

Source Address Popularity (flow)

Source AS (flow)

Source Network (flow)

Source or Destination Address (flow)

Source or Destination AS (flow)

Source or Destination Network (flow)

Top Analysis (flow)

Top Applications Performance (flow)

Top Conversations (flow)



**Report**

Top WAN Applications (flow)
Traffic Volume Pair (flow)
Custom OID (qos)
Daily Interface Bandwidth Summary (qos)
Device Availability (qos)
Device Count by Alert Type (qos)
Device CPU/Memory Usage (qos)
Device Status (qos)
Devices (qos)
Fan Tray Operational Status (qos)
Interface Availability (qos)
Interface Bandwidth (qos)
Interface Bandwidth Summary (qos)
Interface Burstable Rate (qos)
Interface Errors (qos)
Interface Status (qos)
Interface Utilization (qos)
Interface Utilization Above Threshold Over Time (qos)
Interface Utilization Summary (qos)
Interface Utilization Under Threshold Over Time (qos)
Interface/Interface Drops (qos)
Interfaces (qos)
NBAR and Post-Policy (qos)
Port Bandwidth (qos)
Port Drops (qos)
Post-Policy Drops (qos)
Power Supply Operational Status (qos)
Pre-Policy and Post-Policy (qos)
Pre-Policy and Post-Policy Drops (qos)
Service Provider Availability (qos)
Site Alert (qos)
Site Alert Detail (qos)
Site Availability (qos)
Site Bandwidth (qos)
Site Count by Alert Type (qos)
Site WAN Interface Bandwidth by Application (qos)
Site WAN Interface Utilization (qos)
Spanning Tree State Report (qos)
Top Application Bandwidth (qos)
Top Changed - CPU Usage (qos)
Top Changed - Interface Burstable Rate (qos)
Top Changed - Memory Usage (qos)
Top Changed Comparison - CPU Usage (qos)
Top Changed Comparison - Interface Burstable Rate (qos)

**Report**

Top Changed Comparison - Memory Usage (qos)

Top Class Bandwidths (qos)

Top Class Drops (qos)

Top CPU Usage (qos)

Top Interface Bandwidths (qos)

Top Interface Drops (qos)

Top Interface Errors (qos)

Top Interface Utilization (qos)

Top Layer 2 QoS Queue Drops (qos)

Top Memory Usage (qos)

WAN Alerts/Bandwidth by Application (qos)

WAN Interface Burstable Rate by Month (qos)

Cloud onRamp for SaaS Performance by Site (viptela)

Cloud onRamp for SaaS Performance Details by Site (viptela)

Cloud onRamp for SaaS Performance Time Series (viptela)

Insights by Application (Analytics) (test)

Insights by Device (Analytics) (test)

Insights by Site (Analytics) (test)

Enumeration Time Series Test Report (test)

Latest Insights (Analytics) (test)

Network Delay Anomalies (Analytics) (test)

Overall Health (IPSLA)

Overall System Health (IPSLA)

Scaling Test Report (test)

Service Provider Performance (viptela)

Single Test Time Series (IPSLA)

Single Type Health (IPSLA)

Site Pair Status (viptela)

Site to Site Performance (viptela)

Site to Site Performance Details (viptela)

Site to Site Performance Over Time (viptela)

SLA Class Performance (viptela)

SNMP Bandwidth Anomalies (Analytics) (test)

Test Status (IPSLA)

Threshold Test Report (test)

Top Analysis - AVC (analytics)

Top Analysis - AVC (Analytics) (test)

Top Analysis - Basic (analytics)

Top Analysis - Basic (Analytics) (test)

Top Analysis - Medianet (analytics)

Top Analysis - Medianet (Analytics) (test)

Top Conversations (Analytics) (test)

Tunnel SLA Class Performance (viptela)

Anomalies by Application (analytics)

Report
Anomalies by Device (analytics)
Anomalies by Site (analytics)
Application (analytics)
Application Bandwidth Anomalies (analytics)
DSCP (analytics)
Latest Insights (analytics)
Network Delay Anomalies (analytics)
SNMP Bandwidth Anomalies (analytics)
SNMP Bandwidth Prediction (analytics)

## List of Report Parameters

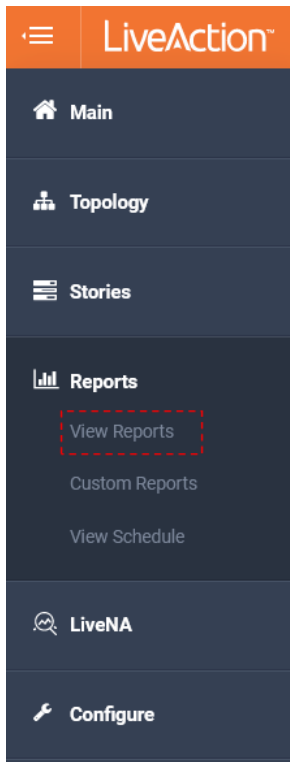
The following table lists the report parameters in LiveNX:

Report Parameter
Duration
businessHours
cancellationDelaySeconds
comparisonMonth
customOidConfig
delayThreshold
destinationServiceProvider
destinationSite
deviceSerial
direction
displayFilter
endTime
excludeClassDefaults
executionDelaySeconds
executionType
flexSearch
flowType
interface
interfaceUtilizationThreshold
ipslaStatAggregationType
ipslaSystemTest
ipslaType
jitterThreshold
layer2QosStatsParameter
otherAggregation
packetLossRateThreshold
qosClass
regionType
relativeTime
rowCount

Report Parameter
serviceProvider
shouldWaitForDnsResolution
site
site1
site2
slaClass
sortBy
sourceServiceProvider
sourceSite
startTime
testId
unit
utilizationAboveThresholdDurationInHours
utilizationUnderThresholdDurationInHours
violationDurationThreshold
vlanIndex
wan
timeZone
topAnalysisDisplayType
topAnalysisLimit

## View Reports

LiveNX provides very flexible Reporting for monitoring multiple dimensions of network and application performance. One report can be run individually, or multiple reports can be bundled together into a Template. These reports can run ad-hoc or saved and scheduled on a residual basis. Reports can be shared with colleagues via a shared URL or via email. Reports can also be run programmatically via REST API.



By default, the View Reports page is laid out to provide quick access to:

- Favorite Reports
- Top Reports
- Default Templates

View Reports View Schedule Create Report

Table Tile

**Favorite Reports** +

Add Report

**Top Reports** + -

NAME	DESCRIPTION
Application	This Flow-based report will highlight the Top 10 applications' bandwidth, based on the selected filter criteria. It will also list up to 1000 applications.
Top Conversations	This Flow-based report will highlight the Top 10 conversions, based on the selected filter criteria. It will also list up to 1000 conversations.
Interface Bandwidth	This Flow-based report will highlight the Top 10 interfaces' bandwidth, based on the selected filter criteria. It will list up to 1000 interfaces.
DSCP	This Flow-based report will highlight the Top 10 DSCP markings' bandwidth, based on the selected filter criteria. It will list up to 64 DSCP values.
Top Interface Bandwidths	This SNMP-based report shows a table of all the interfaces' bandwidth utilization per the specified filter.
Top Interface Errors	This SNMP-based report shows a table of all interface errors (CRC/Runt/ Overruns, etc.) per the specified filter.
Top Class Bandwidths	This SNMP-based report shows a table of all QoS class bandwidths for all interfaces per the specified filter.
Top Class Drops	This SNMP-based report shows a table of all QoS class drops on all interfaces per the specified filter.
Interface Bandwidth	This SNMP-based report graphs bandwidth utilization of a specific interface.
Interface Utilization	This SNMP-based report graphs the interface bandwidth utilization (by percentage) of a specific interface.
Interface Errors	This SNMP-based report graphs the number of interface errors (CRC/ Runt/ Overruns/ etc.) of a specific interface.
Post-Policy Drops	This SNMP-based report graphs the QoS drops of all classes on a specific interface.
Application DSCP Audit	This Flow-based report will show the DSCP markings of applications organized by site, based on the selected filter criteria.
Interface Bandwidth Summary	This Flow-based report will highlight the ingress and egress interface bandwidth, based on the selected filter criteria. It will list up to 50 interfaces.

Default Templates

NAME	DESCRIPTION
Voice Analysis	This group of reports is useful for understanding enterprise-wide QoS performance for VoIP. It includes DSCP marking validation per site, QoS performance information, and Voice/Video performance data (jitter and packet loss), based on the selected filter criteria.
IWAN	This group of reports provides rapid understanding of Cisco IWAN performance and utilization. It includes an understanding of which service provider a specific class of traffic is utilizing, delay/loss/jitter measurements by traffic class, and business relevance.
Favorite Applications	This group of reports provides an understanding of the applications seen at a specific site, their performance (based on the Cisco Performance Monitor), traffic class, and business relevance.
Apple Fastlane Applications	This group of reports provides an understanding of the Apple Fastlane applications seen at a specific site, their performance (based on the Cisco Performance Monitor), traffic class, and business relevance.
Apple Fastlane Voice Analysis	This group of reports is useful for understanding enterprise-wide Apple Fastlane QoS performance for VoIP. It includes DSCP marking validation per site, QoS performance information, and Voice/Video performance data (jitter and packet loss), based on the selected filter criteria.
WAN Capacity Planning	This group of reports provides visibility into the performance of a WAN interface. It includes interface bandwidth, interface utilization, interface errors, QoS performance, top applications, top talkers, and top DSCP reports.
Site Network Performance Audit	This group of reports provides application performance and network performance statistics for defined applications at a site.
Voice/Video Performance Vs. Network Performance	This group of reports provides Voice/Video and network performance statistics for defined applications at a site.
Site-to-Site Traffic Utilization Audit	This group of reports provides utilization statistics of traffic leaving "Site A" and being received by "Site B".
Service Provider DSCP Audit	This group of reports validates the DSCP value of traffic leaving "Site A" and being received by "Site B".
Track Single Site WAN Path Changes	This group of reports highlights when traffic changes WAN path at a specific site.
Application Vs. Network Performance	This group of reports provides application and network performance statistics for defined applications at a site.
Voice/Video Service Provider Performance Audit	This group of reports validates that DSCP values are being both transmitted and received successfully across a WAN for Voice/Video. It also provides application performance visibility across a WAN.
Application Service Provider Performance Audit	This group of reports validates that DSCP values are being both transmitted and received successfully across a WAN. It also provides application performance visibility across a WAN.
SDWAN Application Service Provider Performance Audit	This group of reports validates that DSCP values are being both transmitted and received successfully across a SDWAN network. It also provides application performance visibility across a WAN.
SDWAN Application Vs. Network Performance	This group of reports provides application and SDWAN network performance statistics for defined applications at a site.
SDWAN Voice/Video Performance Vs. Network Performance	This group of reports provides Voice/Video and SDWAN network performance statistics for defined applications at a site.
SDWAN Voice/Video Service Provider Performance Audit	This group of reports validates that DSCP values are being both transmitted and received successfully across a SDWAN network. It also provides application performance visibility across a WAN.
IWAN Application Vs. Network Performance	This group of reports provides application and IWAN network performance statistics for defined applications at a site.
IWAN Application Service Provider Performance Audit	This group of reports validates that DSCP values are being both transmitted and received successfully across a IWAN network. It also provides application performance visibility across a WAN.
IWAN Voice/Video Performance Vs. Network Performance	This group of reports provides Voice/Video and IWAN network performance statistics for defined applications at a site.
IWAN Voice/Video Service Provider Performance Audit	This group of reports validates that DSCP values are being both transmitted and received successfully across a IWAN network for Voice/Video. It also provides application performance visibility across a WAN.

The presentation style for the page can be either a Table (default) or Tile view. This can be selected by using the switch at the top right of the page.



### Table View:

View Reports View Schedule Create Report

**Favorite Reports** +

**Top Reports** + -

NAME	DESCRIPTION
Application	This Flow-based report will highlight the Top 10 applications' bandwidth, based on the selected filter criteria. It will also list up to 1000 applications.
Top Conversations	This Flow-based report will highlight the Top 10 conversations, based on the selected filter criteria. It will also list up to 1000 conversations.
Interface Bandwidth	This Flow-based report will highlight the Top 10 interfaces' bandwidth, based on the selected filter criteria. It will list up to 1000 interfaces.
DSCP	This Flow-based report will highlight the Top 10 DSCP markings' bandwidth, based on the selected filter criteria. It will list up to 64 DSCP values.
Top Interface Bandwidths	This SNMP-based report shows a table of all the interfaces' bandwidth utilization per the specified filter.
Top Interface Errors	This SNMP-based report shows a table of all interface errors (CRC/Runt/Overruns, etc.) per the specified filter.
Top Class Bandwidths	This SNMP-based report shows a table of all QoS class bandwidths for all interfaces per the specified filter.
Top Class Drops	This SNMP-based report shows a table of all QoS class drops on all interfaces per the specified filter.
Interface Bandwidth	This SNMP-based report graphs bandwidth utilization of a specific interface.
Interface Utilization	This SNMP-based report graphs the interface bandwidth utilization (by percentage) of a specific interface.
Interface Errors	This SNMP-based report graphs the number of interface errors (CRC/ Runt/ Overruns/ etc.) of a specific interface.
Post-Policy Drops	This SNMP-based report graphs the QoS drops of all classes on a specific interface.
Application DSCP Audit	This Flow-based report will show the DSCP markings of applications organized by site, based on the selected filter criteria.
Interface Bandwidth Summary	This Flow-based report will highlight the ingress and egress interface bandwidth, based on the selected filter criteria. It will list up to 50 interfaces.

### Tile View:

Table Tile

**Favorite Reports** +

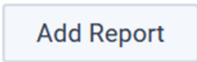
**Top Reports** + -

<p><b>Application</b></p> <p>This Flow-based report will highlight the Top 10 applications' bandwidth, based on the selected filter criteria. It will also list up to 1000 applications.</p>	<p><b>Top Conversations</b></p> <p>This Flow-based report will highlight the Top 10 conversations, based on the selected filter criteria. It will also list up to 1000 conversations.</p>	<p><b>Interface Bandwidth</b></p> <p>This Flow-based report will highlight the Top 10 interfaces' bandwidth, based on the selected filter criteria. It will list up to 1000 interfaces.</p>
<p><b>DSCP</b></p> <p>This Flow-based report will highlight the Top 10 DSCP markings' bandwidth, based on the selected filter criteria. It will list up to 64 DSCP values.</p>	<p><b>Top Interface Bandwidths</b></p> <p>This SNMP-based report shows a table of all the interfaces' bandwidth utilization per the specified filter.</p>	<p><b>Top Interface Errors</b></p> <p>This SNMP-based report shows a table of all interface errors (CRC/Runt/Overruns, etc.) per the specified filter.</p>
<p><b>Top Class Bandwidths</b></p> <p>This SNMP-based report shows a table of all QoS class bandwidths for all interfaces per the specified filter.</p>	<p><b>Top Class Drops</b></p> <p>This SNMP-based report shows a table of all QoS class drops on all interfaces per the specified filter.</p>	<p><b>Interface Bandwidth</b></p> <p>This SNMP-based report graphs bandwidth utilization of a specific interface.</p>
<p><b>Interface Utilization</b></p> <p>This SNMP-based report graphs the interface bandwidth utilization (by percentage) of a specific interface.</p>	<p><b>Interface Errors</b></p> <p>This SNMP-based report graphs the number of interface errors (CRC/ Runt/ Overruns/ etc.) of a specific interface.</p>	<p><b>Post-Policy Drops</b></p> <p>This SNMP-based report graphs the QoS drops of all classes on a specific interface.</p>
<p><b>Application DSCP Audit</b></p> <p>This Flow-based report will show the DSCP markings of applications organized by site, based on the selected filter criteria.</p>	<p><b>Interface Bandwidth Summary</b></p> <p>This Flow-based report will highlight the ingress and egress interface bandwidth, based on the selected filter criteria. It will list up to 50 interfaces.</p>	

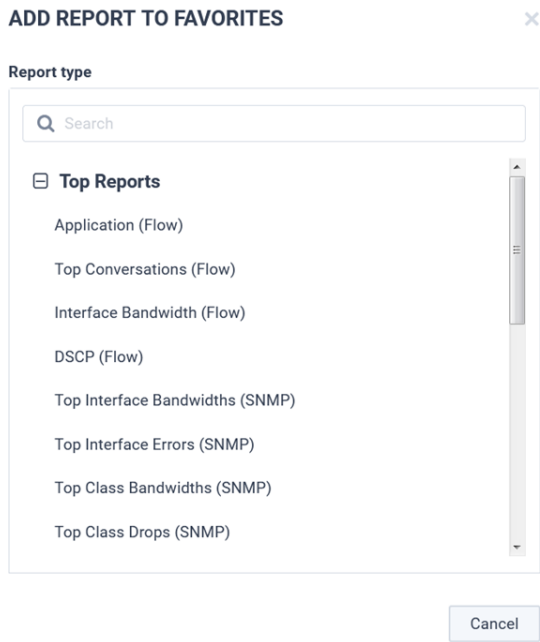
Default Templates

To Add a Favorite Report, click the Add Report button.

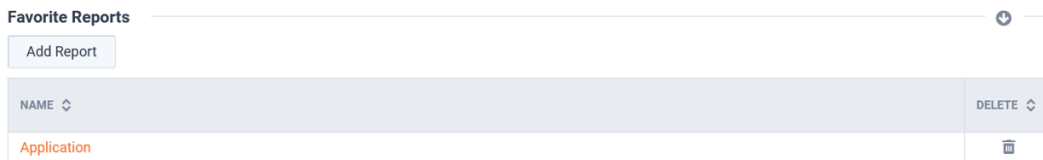
### Favorite Reports



From the pop-up, select a report.



The Report will show up under *Favorite Reports*.



If collapsed, the sidebar tab can be expanded to expose a quick-access Report sidebar.

View Reports

**Favorite Reports**

Add Report

**Top Reports**

NAME	DESCRIPTION
Application	This Flow-ba:
Top Conversations	This Flow-ba:
Interface Bandwidth	This Flow-ba:
DSCP	This Flow-ba:
Top Interface Bandwidths	This SNMP-b
Top Interface Errors	This SNMP-b
Top Class Bandwidths	This SNMP-b
Top Class Drops	This SNMP-b
Interface Bandwidth	This SNMP-b
Interface Utilization	This SNMP-b
Interface Errors	This SNMP-b
Post-Policy Drops	This SNMP-b
Application DSCP Audit	This Flow-ba:
Interface Bandwidth Summary	This Flow-ba:

View Reports

View Schedule Create Report

Templates Reports History

By Template Name

**Default Templates**

- Voice Analysis
- WAN
- Favorite Applications
- Apple Fastlane Applications
- Apple Fastlane Voice Analysis
- WAN Capacity Planning
- Site Network Performance Audit
- Voice/Video Performance Vs. Netwo...
- Site-to-Site Traffic Utilization Audit
- Service Provider DSCP Audit
- Track Single Site WAN Path Changes
- Application Vs. Network Performance
- Voice/Video Service Provider Perform...
- Application Service Provider Perform...
- SDWAN Application Service Provider ...
- SDWAN Application Vs. Network Perf...
- SDWAN Voice/Video Performance V...
- SDWAN Voice/Video Service Provide...

**Favorite Reports**

Add Report

**Top Reports**

NAME	DESCRIPTION
Application	This Flow-based report will highlight the Top 10 applications' bandwidth, based on the selected filter criteria. It will also list up to 1000 applications.
Top Conversations	This Flow-based report will highlight the Top 10 conversations, based on the selected filter criteria. It will also list up to 1000 conversations.
Interface Bandwidth	This Flow-based report will highlight the Top 10 interfaces' bandwidth, based on the selected filter criteria. It will list up to 1000 interfaces.
DSCP	This Flow-based report will highlight the Top 10 DSCP markings' bandwidth, based on the selected filter criteria. It will list up to 64 DSCP values.
Top Interface Bandwidths	This SNMP-based report shows a table of all the interfaces' bandwidth utilization per the specified filter.
Top Interface Errors	This SNMP-based report shows a table of all interface errors (CRC/Runts/Overruns, etc.) per the specified filter.
Top Class Bandwidths	This SNMP-based report shows a table of all QoS class bandwidths for all interfaces per the specified filter.
Top Class Drops	This SNMP-based report shows a table of all QoS class drops on all interfaces per the specified filter.
Interface Bandwidth	This SNMP-based report graphs bandwidth utilization of a specific interface.
Interface Utilization	This SNMP-based report graphs the interface bandwidth utilization (by percentage) of a specific interface.
Interface Errors	This SNMP-based report graphs the number of interface errors (CRC/ Runts/ Overruns/ etc.) of a specific interface.
Post-Policy Drops	This SNMP-based report graphs the QoS drops of all classes on a specific interface.
Application DSCP Audit	This Flow-based report will show the DSCP markings of applications organized by site, based on the selected filter criteria.
Interface Bandwidth Summary	This Flow-based report will highlight the ingress and egress interface bandwidth, based on the selected filter criteria. It will list up to 50 interfaces.

The quick-access Report sidebar contains two tabs: Templates and Reports History.

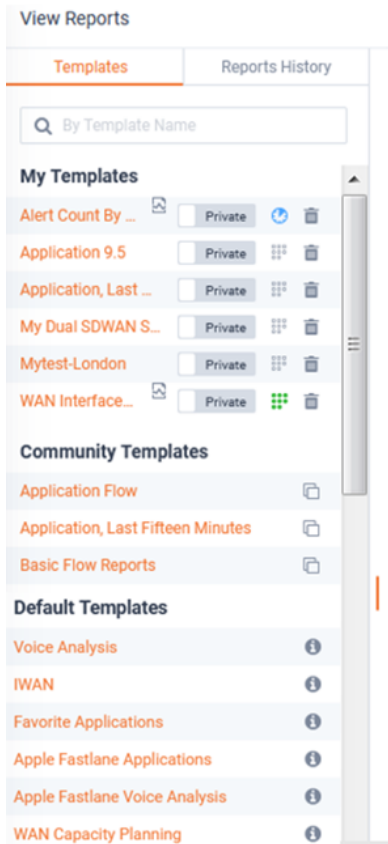
The Template tab provides:

- My Templates - Templates saved by the current user
- Community Templates – Templates saved and shared by other users
- Default Templates – curated Templates that ship with LiveNX

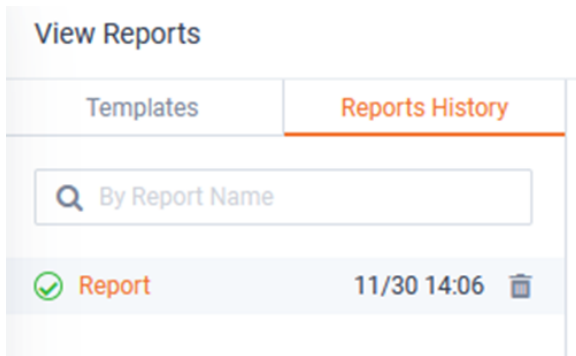
The Reports History tab provides a list of reports recently run by the current user.

Template Tab:



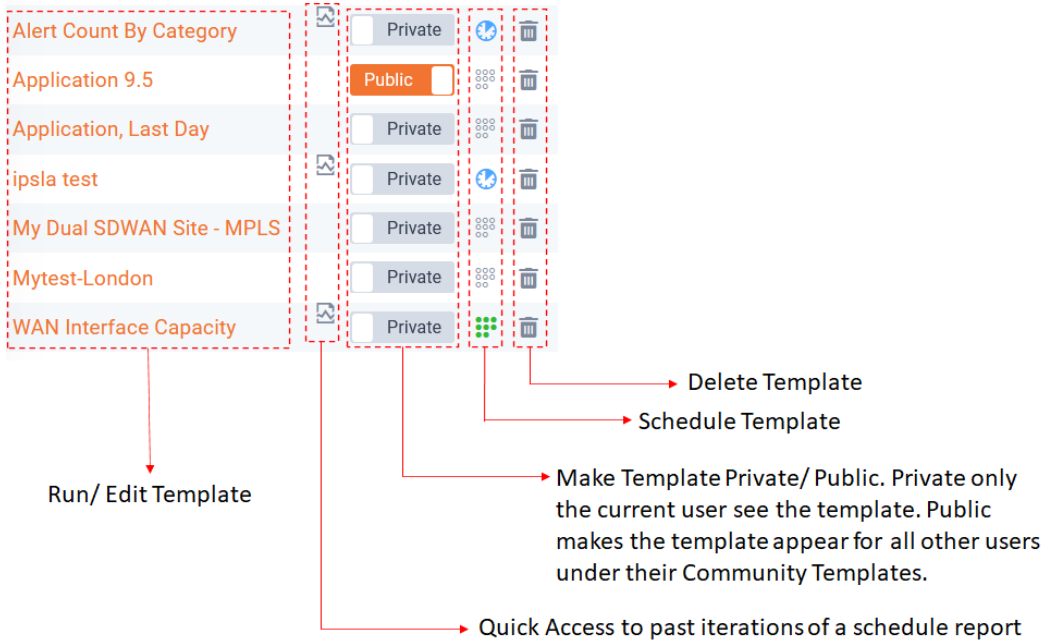


Reports History Tab:



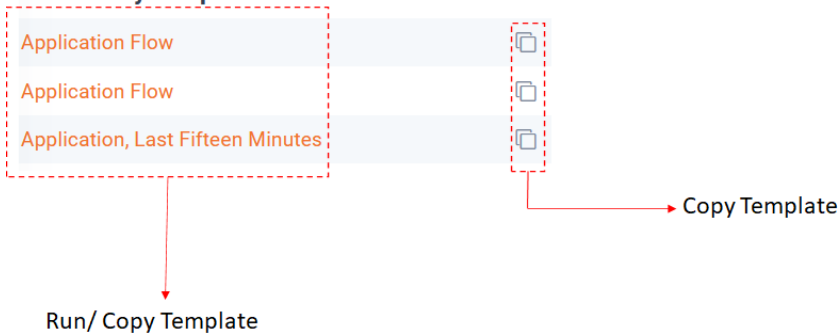
Report Templates listed under *My Templates* provides the following options:

### My Templates

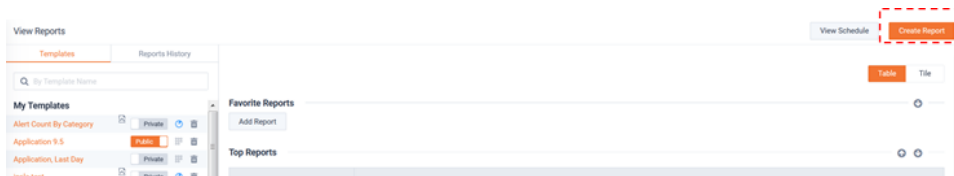


Community Templates provides the following options:

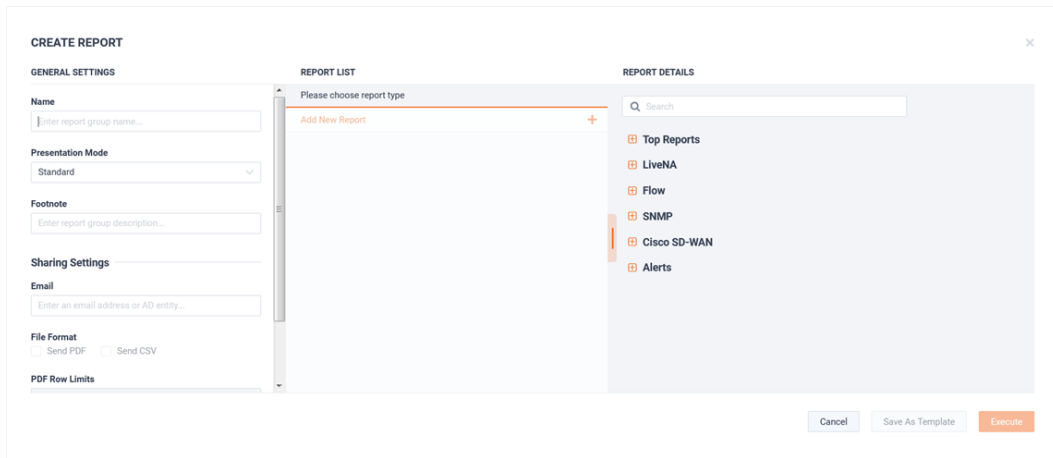
### Community Templates



To Run a report from scratch, click the **Create Report** button.



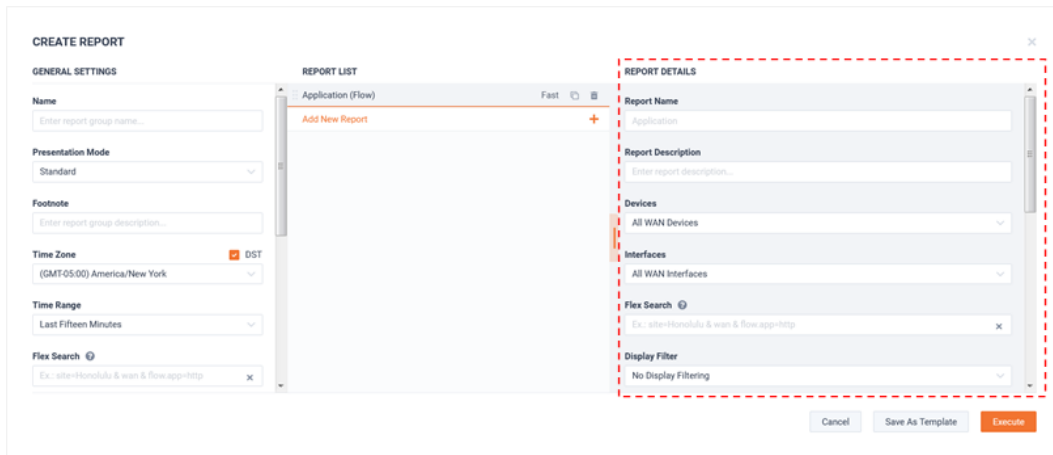
The *Create Report* modal will appear. This modal has three sections, *General Settings*, *Report List*, and *Report Details*.



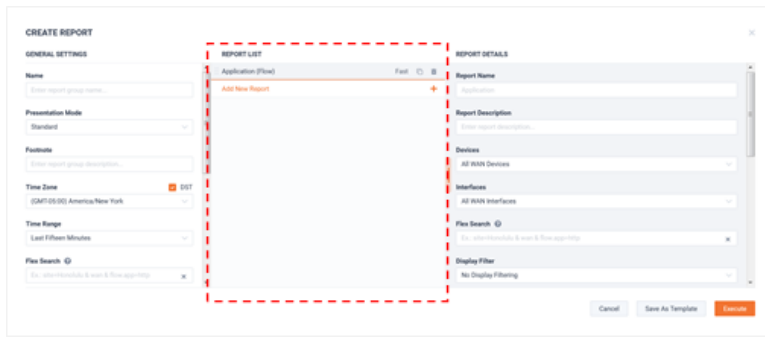
By default, the *Report Details* section will list all available reports until a report is selected. Select a report from the list.



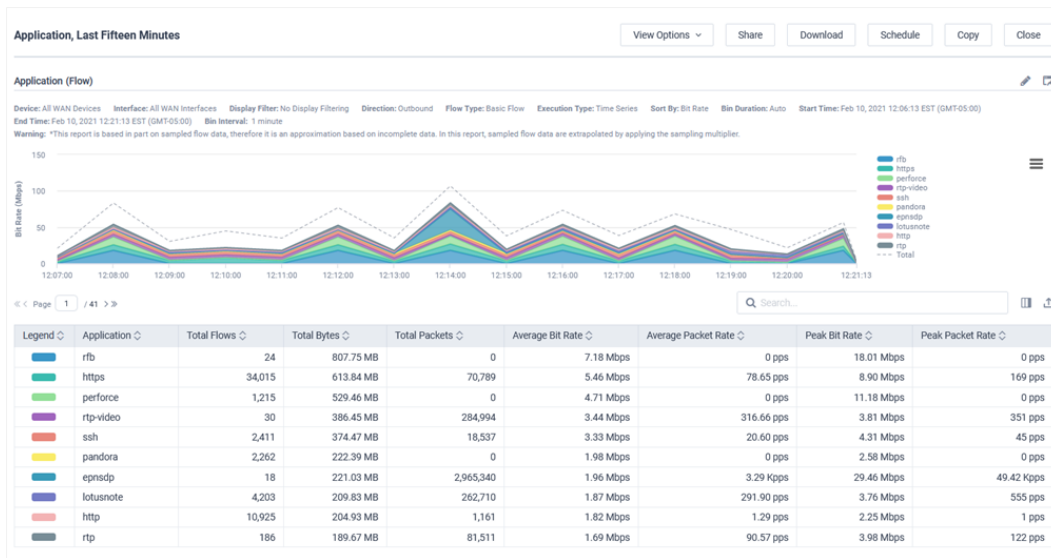
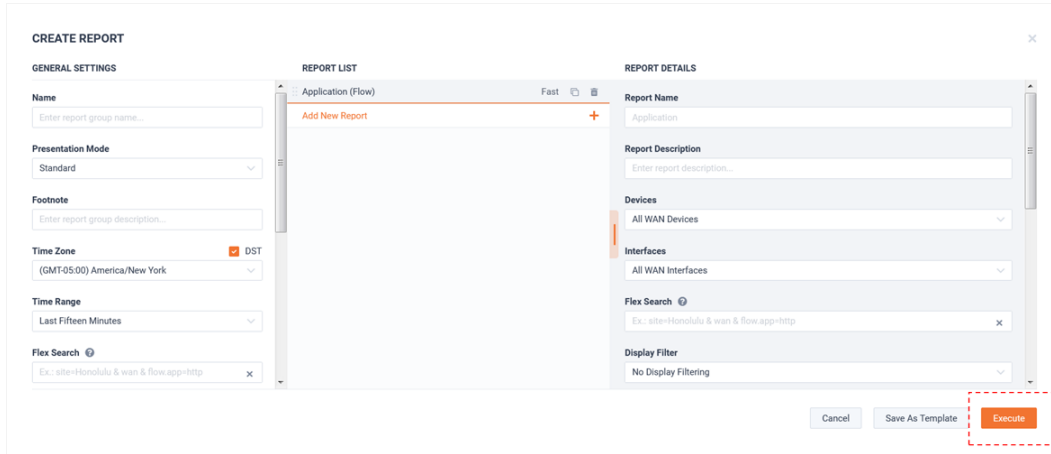
Once a report has been selected, the *Report Details* section will show the customization options available for the report.



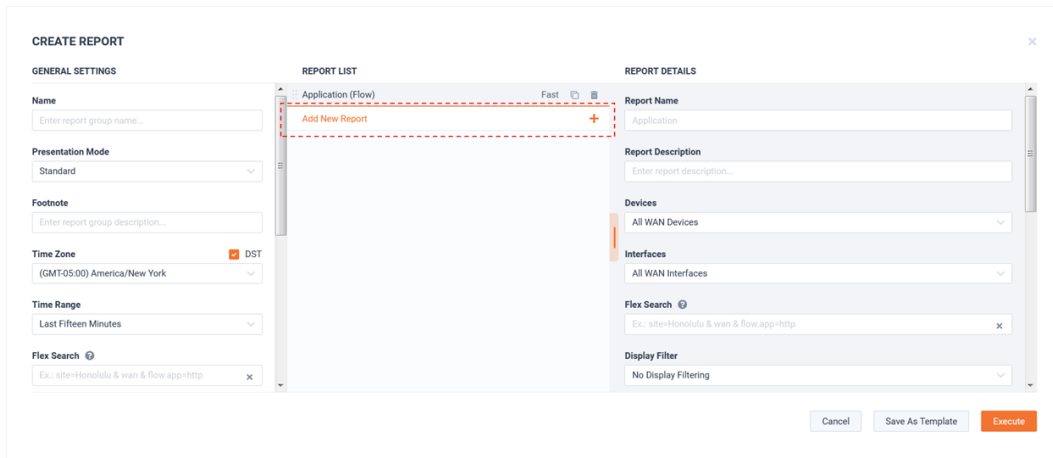
The report will also show up in the *Report List*.



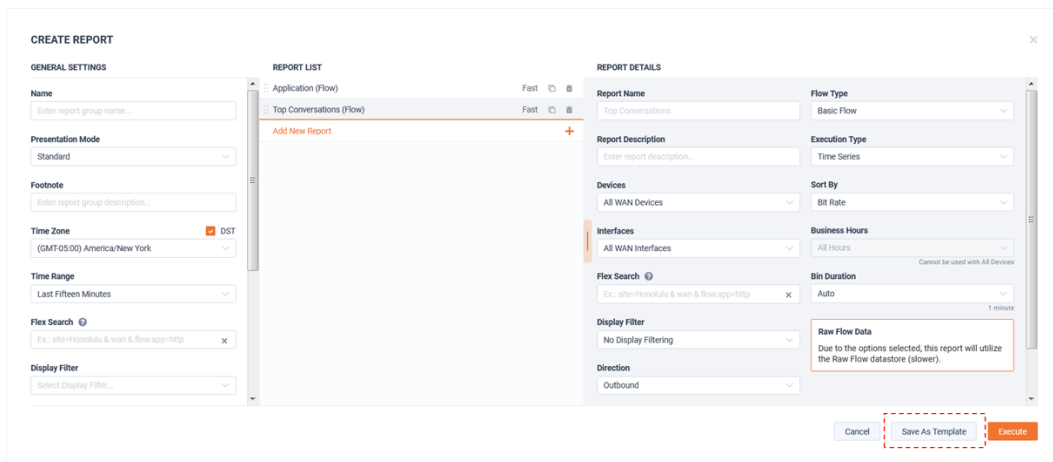
To run the report with its default parameters, click **Execute**.



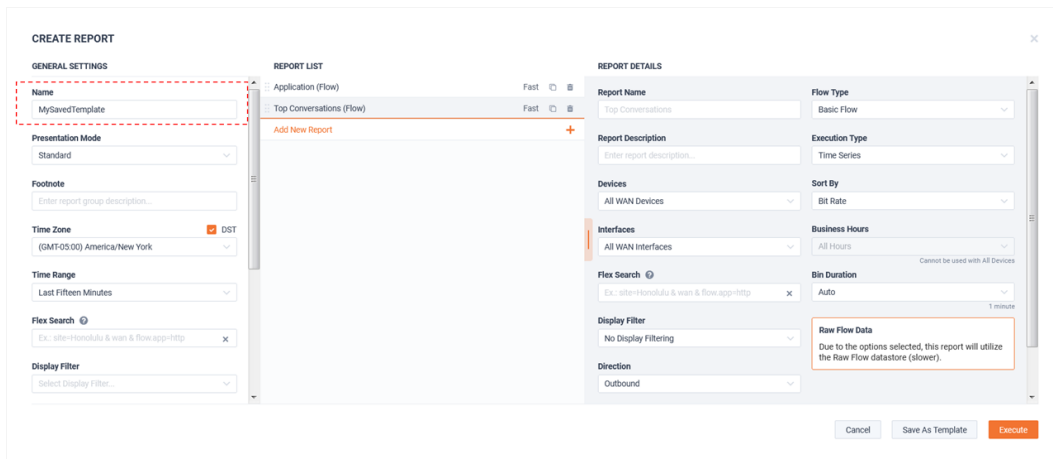
Additional reports can be added to the *Report List*.



To save, click **Save Template**.



By default, LiveNX will name the template. If desired, the template name can be customized from the *Name* field.



Once saved, the template will appear under *My Templates*.

### My Templates

Alert Count By Category	<input type="checkbox"/> Private		
Application 9.5	<input checked="" type="checkbox"/> Public		
Application, Last Day	<input type="checkbox"/> Private		
ipsla test	<input type="checkbox"/> Private		
My Dual SDWAN Site - MPLS	<input type="checkbox"/> Private		
MySavedTemplate	<input type="checkbox"/> Private		
Mytest-London	<input type="checkbox"/> Private		
WAN Interface Capacity	<input type="checkbox"/> Private		

To edit the template, click its name under *My Templates*.

### My Templates

Alert Count By Category	<input type="checkbox"/> Private		
Application 9.5	<input checked="" type="checkbox"/> Public		
Application, Last Day	<input type="checkbox"/> Private		
ipsla test	<input type="checkbox"/> Private		
My Dual SDWAN Site - MPLS	<input type="checkbox"/> Private		
MySavedTemplate	<input type="checkbox"/> Private		
Mytest-London	<input type="checkbox"/> Private		
WAN Interface Capacity	<input type="checkbox"/> Private		

The *RUN* or *Edit Report(s)* modal will appear.

#### RUN OR EDIT REPORT(S)

##### GENERAL SETTINGS

Name: MySavedTemplate

Presentation Mode: Standard

Footnote: Enter report group description...

Time Zone:  DST (GMT-05:00) America/New York

Time Range: Last Fifteen Minutes

Flex Search: Ex: site=Honolulu & wan & flow.app=http

Display Filter: Select Display Filter...

##### REPORT LIST

Application (Flow) Fast

- Top Conversations (Flow)

Add New Report

##### REPORT DETAILS

Report Name: Application

Flow Type: Basic Flow

Report Description: Enter report description...

Execution Type: Time Series

Devices: All WAN Devices

Sort By: Bit Rate

Interfaces: All WAN Interfaces

Business Hours: All Hours

Flex Search: Ex: site=Honolulu & wan & flow.app=http

Bin Duration: Auto

Display Filter: No Display Filtering

Direction: Outbound

**Raw Flow Data**  
Due to the options selected, this report will utilize the Raw Flow datastore (slower).

Cancel Update Save As Template **Execute**

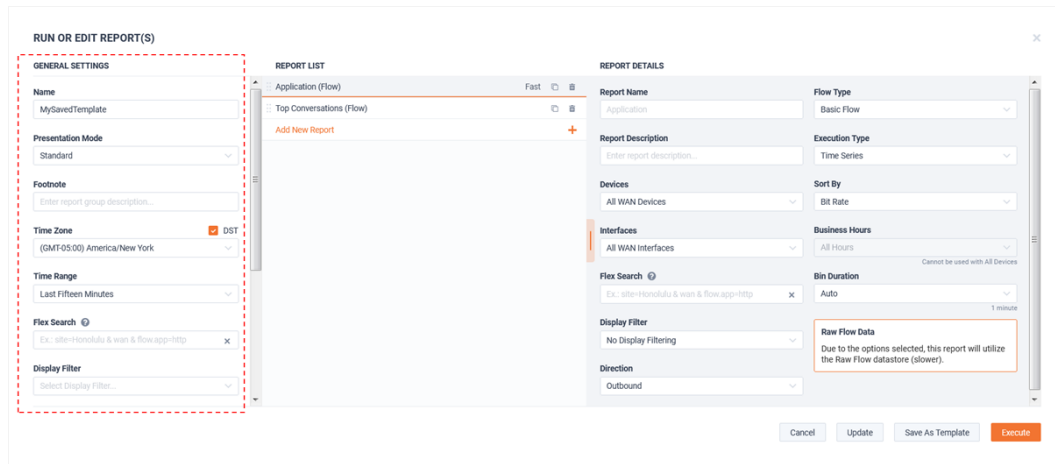
To save any changes to this template, click **Update**.

Update

To save any changes as a new template, click **Save As Template**.

Save As Template

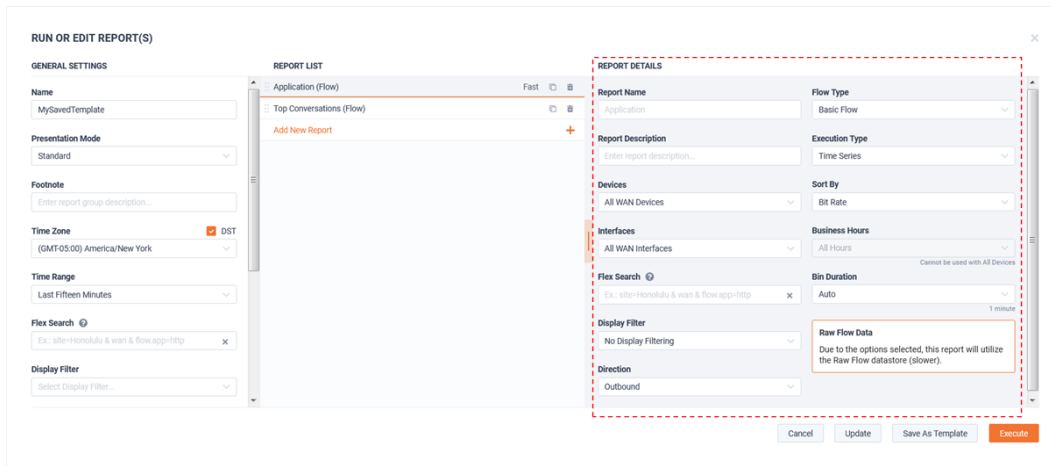
LiveNX reports are highly customizable. The section will review the available options. *General Settings* apply to all reports in the template.



General Settings	Description
Name	Report Template's Name
Presentation Mode	Normal – Report will fill complete page width Executive – Report will be presented like a dashboard widget
Footnote	Free text field presented at the bottom of the page
Time Zone	Designates the time zone used by all member reports
DST	uses Daylight Savings time offset
Time Range	Selects the time window used by all member reports
Flex Search	Advanced filtering capability for selecting the data of interest to be presented by the member reports. This Flex search will be “ANDed” with any report specific Flex Search.
Display Filter	The legacy Flow filtering capability. This is configured in the Engineering Console.

Shared Settings	Description
Email	Specify one or more email destinations that will receive a notification when the report is finished rendering and a link to access the report.
File Format	Option for deliver of PDF or CSV report results with the email.
PDF Row Limits	Selects the number of rows to be show in the PDF results.
Custom Log	Select picture that can accompany PDF and shared report results.

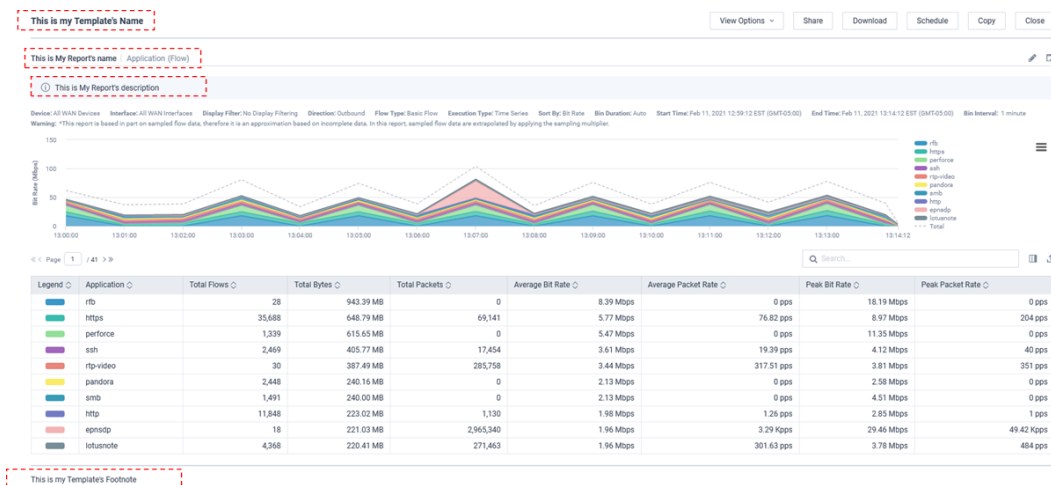
Report details only apply to the specific highlighted report in the template.



Below is a list of the most common *Report Detail* options for Flow based reports. Not all options are available for all reports.

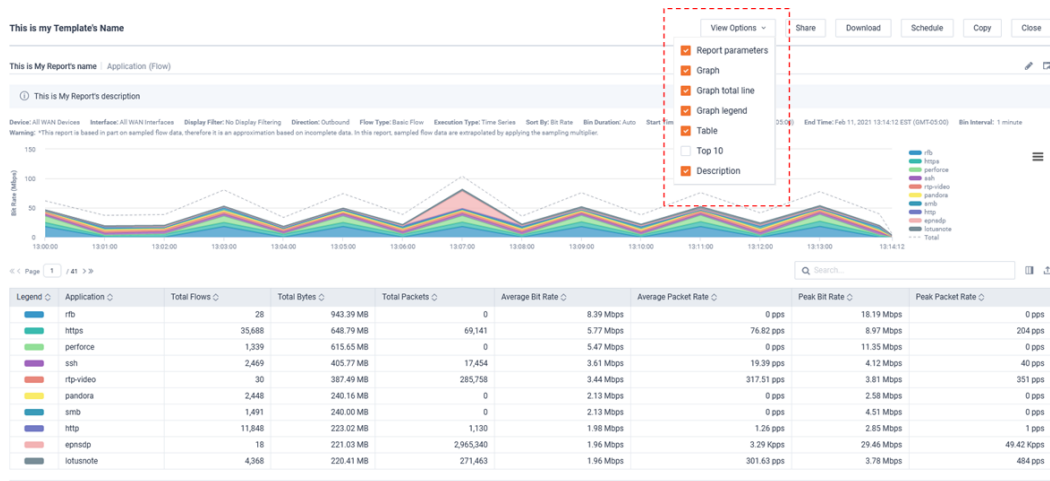
Report Details	Description
• Report Name	Name of the report
• Report Description	Description of the report.
• Devices	Which device's data are in scope for the report results.
• Interfaces	Which device's interfaces data will be in scope for the report results.
• Flex Search	Advanced filtering capability for selecting the data of interest to be presented by the member reports.
• Display Filter	The legacy Flow filtering capability. This is configured in the Engineering Console.
• Direction	Which Flow direction will be in scope for the report results.
• Flow Type	Which Flow type will be used for the report
• Execution Type	Report will be graphed as either an aggregation or times series view.
• Sort By	Select the sorting method for the report.
• Business Hours	If the report is focused on one interface, this option will be available for using the corresponding Site's business hours for calculating the report's results.
• Bin Duration	The Bin duration determines the granularity of the report results.
• Should Wait For Dns Resolution	When this option is selected, the report will wait for dns resolution to complete before returning results.

This is an example of a report with customized names, description, and footnote.



*View Options* are available to customize a report. These can persist when saved in a template.





This is the same report with *View Options* customized.

This is my Template's Name

This is My Report's name | Application (Flow)

Legend

Application	Total Flows	Total Bytes	Total Packets	Average Bit Rate	Average Packet Rate	Peak Bit Rate	Peak Packet Rate
rtb	28	943.39 MB	0	8.39 Mbps	0 pps	18.19 Mbps	0 pps
https	35,688	648.79 MB	69,141	5.77 Mbps	76.82 pps	8.97 Mbps	204 pps
perforce	1,339	615.65 MB	0	5.47 Mbps	0 pps	11.35 Mbps	0 pps
ssh	2,469	405.77 MB	17,454	3.61 Mbps	19.39 pps	4.12 Mbps	40 pps
rtp-video	30	387.49 MB	285,758	3.44 Mbps	317.51 pps	3.81 Mbps	351 pps
pandora	2,448	240.16 MB	0	2.13 Mbps	0 pps	2.58 Mbps	0 pps
smb	1,491	240.00 MB	0	2.13 Mbps	0 pps	4.51 Mbps	0 pps
http	11,848	223.02 MB	1,130	1.98 Mbps	1.26 pps	2.85 Mbps	1 pps
epnsdp	18	221.03 MB	2,965,340	1.96 Mbps	3.29 Kpps	29.46 Mbps	49.42 Kpps
lotusnote	4,368	220.41 MB	271,463	1.96 Mbps	301.63 pps	3.78 Mbps	484 pps

This is my Template's Footnote

Report table columns can be customized. These can persist when saved in a template.

This is my Template's Name

This is My Report's name | Application (Flow)

Legend

Application	Average Bit Rate	Peak Bit Rate
rtb	8.39 Mbps	18.19 Mbps
https	5.77 Mbps	8.97 Mbps
perforce	5.47 Mbps	11.35 Mbps
ssh	3.61 Mbps	4.12 Mbps
rtp-video	3.44 Mbps	3.81 Mbps
pandora	2.13 Mbps	2.58 Mbps
smb	2.13 Mbps	4.51 Mbps
http	1.98 Mbps	2.85 Mbps
epnsdp	1.96 Mbps	29.46 Mbps
lotusnote	1.96 Mbps	3.78 Mbps

This is my Template's Footnote

This is the same report with its columns customized.

This is my Template's Name

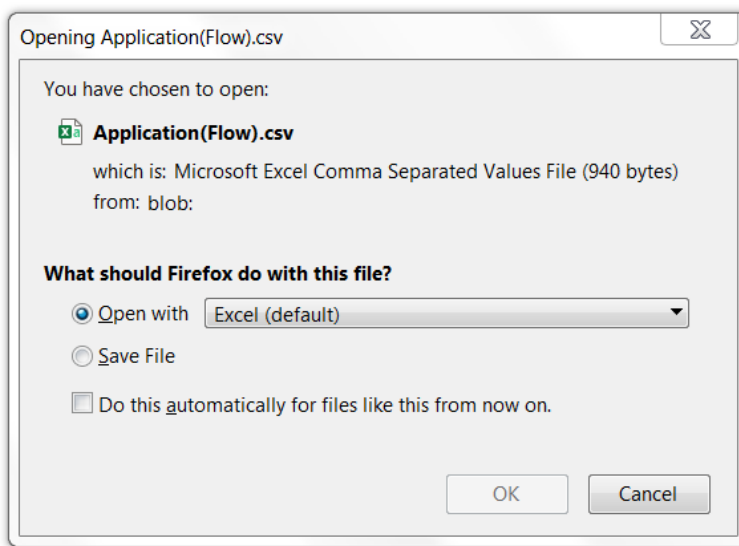
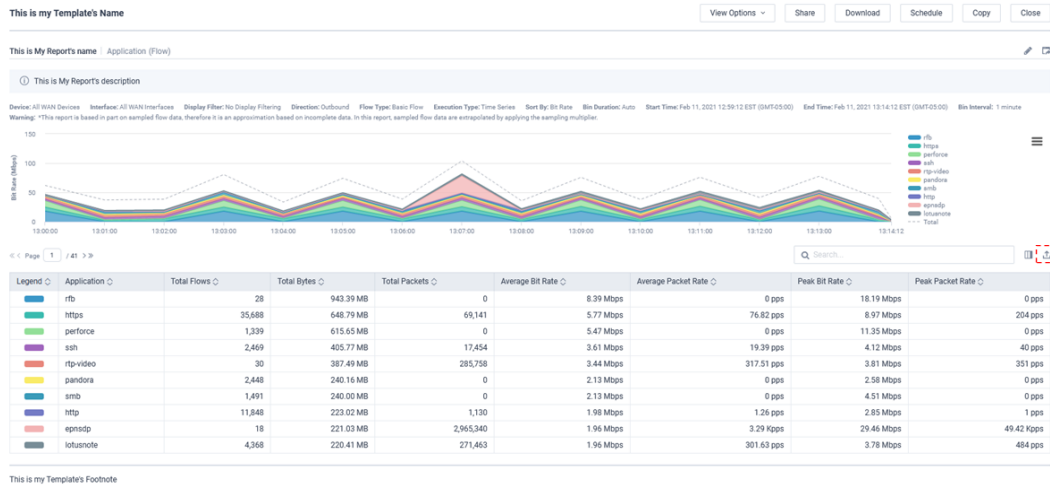
This is My Report's name | Application (Flow)

Legend

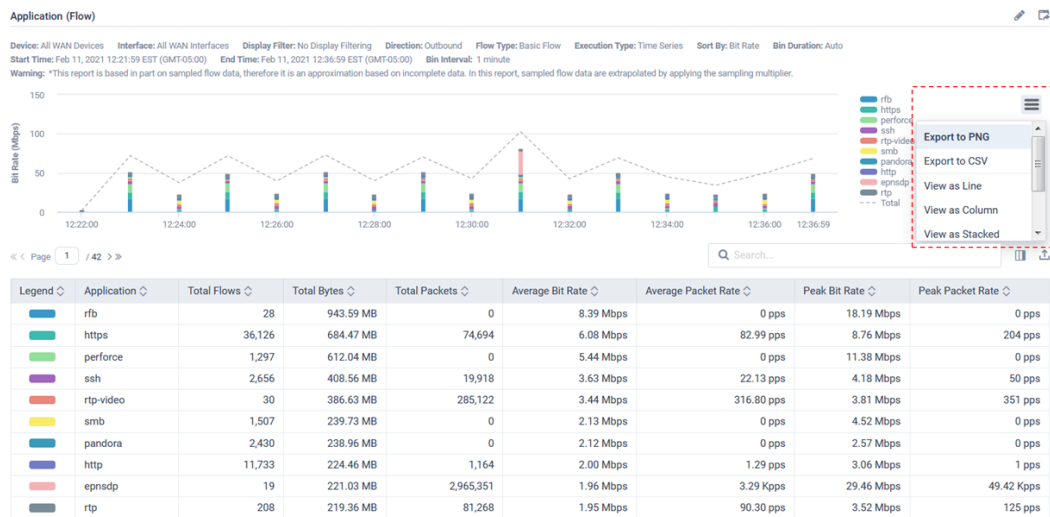
Application	Average Bit Rate	Peak Bit Rate
rtb	8.39 Mbps	18.19 Mbps
https	5.77 Mbps	8.97 Mbps
perforce	5.47 Mbps	11.35 Mbps
ssh	3.61 Mbps	4.12 Mbps
rtp-video	3.44 Mbps	3.81 Mbps
pandora	2.13 Mbps	2.58 Mbps
smb	2.13 Mbps	4.51 Mbps
http	1.98 Mbps	2.85 Mbps
epnsdp	1.96 Mbps	29.46 Mbps
lotusnote	1.96 Mbps	3.78 Mbps

This is my Template's Footnote

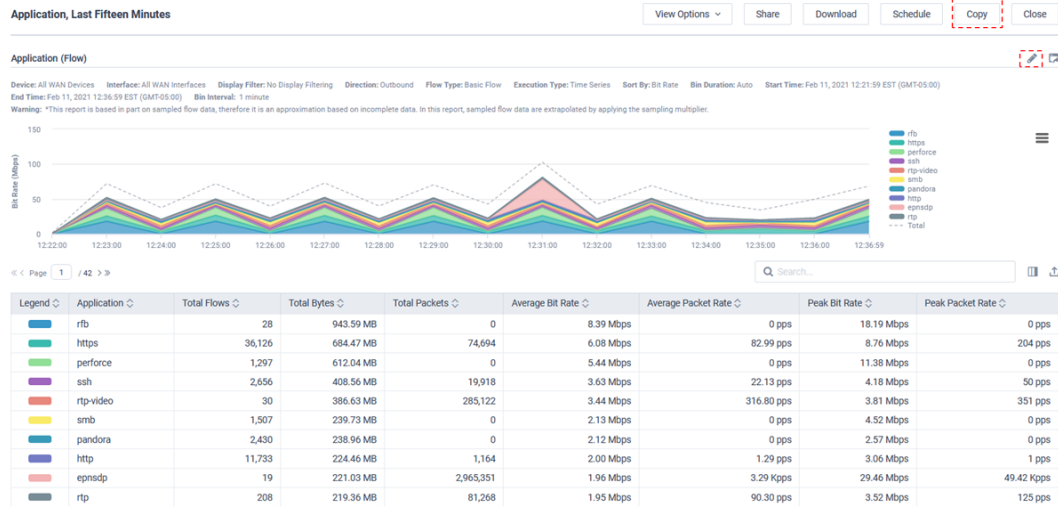
The table can be exported as a CSV.



The Report's graph view can be customized and exported as either PNG or CSV.



To edit a report, use either the **Copy** and **Load Parameters** buttons.



RUN OR EDIT REPORT(S)

GENERAL SETTINGS

Footnote:

Time Zone: DST (GMT-05:00) America/New York

Time Range: Custom

Start Date: 02/11/2021 | Start Time: 12:21 | End Date: 02/11/2021 | End Time: 12:36

Flex Search:

Display Filter:

REPORT LIST

Application (Flow) | Fast |  |

+ Add New Report

REPORT DETAILS

Report Name:

Report Description:

Devices: All WAN Devices

Interfaces: All WAN Interfaces

Flex Search:

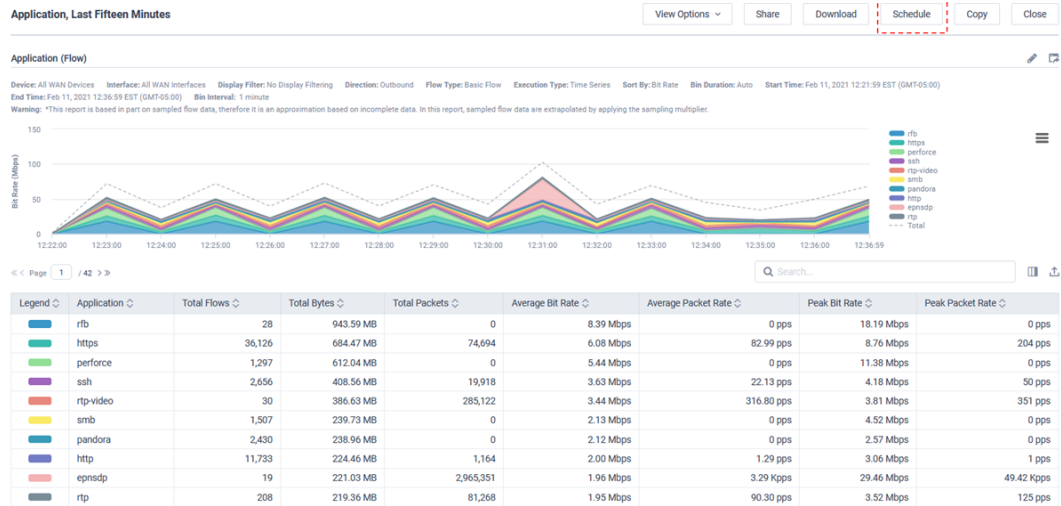
Display Filter: No Display Filtering

Buttons: Cancel | Save As Template | Execute

Both buttons provide similar capabilities, with subtle key differences.

Button	Description
	Copy will keep the Time Range picker the same as the original report Time Range: Last Fifteen Minutes
	The Load Parameters icon will use the absolute time of the original report. Time Range: Custom Start Date: 02/11/2021   Start Time: 12:21   End Date: 02/11/2021   End Time: 12:36

The **Schedule** button opens the *Schedule Report* modal.



### SCHEDULE REPORT

Name

Run Report

*Reports will be created on the hour for the previous hour.*

Schedule Ends

Time Zone  DST

The **Schedule** button opens the *Schedule Report* modal.

### SCHEDULE REPORT ✕

**Name**

**Run Report**

**Start Day**  **End Date**

**Schedule Ends**  **End date**  **End time**

**Time Zone**  DST

The Schedule button opens the Schedule Report Modal.

Schedule Ends	Description
Never	
Run Report	Description
Hourly	Reports will be created on the hour for the previous hour.
Daily	Reports will be run at midnight using the Start Time / End Time
Weekly	Reports will be run at midnight on Sunday for previous week with the Start Day/ End Day
Monthly	Reports will be created on the 1 <sup>st</sup> for the previous month.
Schedule Ends	Description
Never	
After	
By	Provide a specific date
General Settings	Description
Time Range	Selects the time window used by all member reports
Flex Search	Advanced filtering capability for selecting the data of interest to be presented by the member reports. This Flex search will be "ANDed" with any report specific Flex Search.

The **Download** button will provide a PDF copy of the report.

Application, Last Fifteen Minutes View Options ▾ Share **Download** Schedule Copy Close

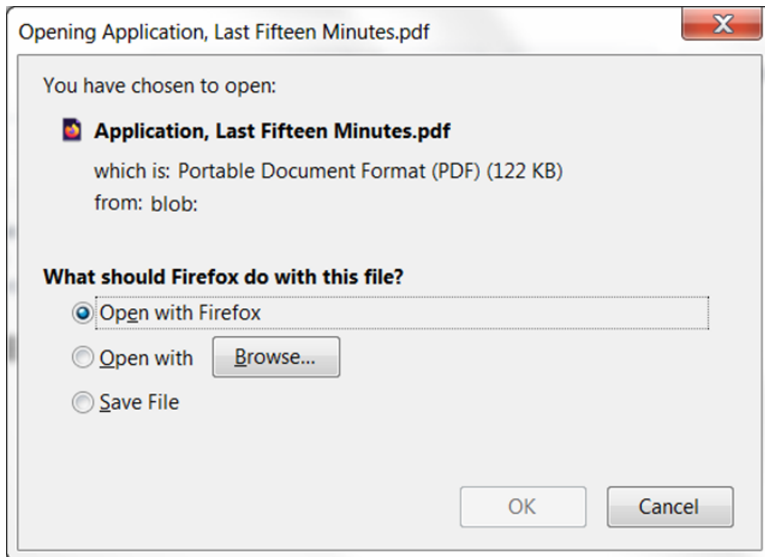
---

Application (Flow) 📄

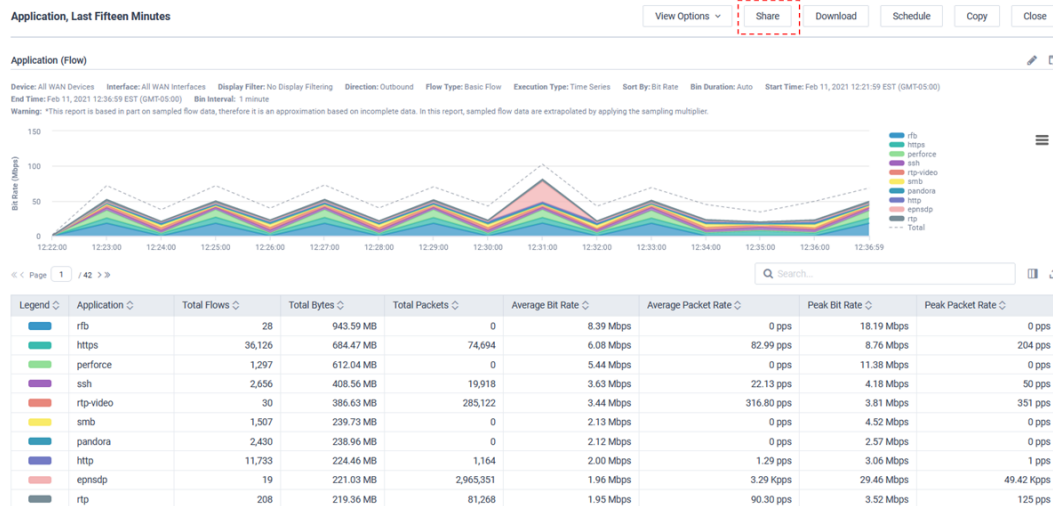
Device: All WAN Devices Interface: All WAN Interfaces Display Filter: No Display Filtering Direction: Outbound Flow Type: Basic Flow Execution Type: Time Series Sort By: Bit Rate Bin Duration: Auto Start Time: Feb 11, 2021 12:21:59 EST (GMT-05:00) End Time: Feb 11, 2021 12:36:59 EST (GMT-05:00) Bin Interval: 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 1 / 42 >> 🔍 Search... 📄

Legend	Application	Total Flows	Total Bytes	Total Packets	Average Bit Rate	Average Packet Rate	Peak Bit Rate	Peak Packet Rate
<span style="color: blue;">■</span>	rtb	28	943.59 MB	0	8.39 Mbps	0 pps	18.19 Mbps	0 pps
<span style="color: green;">■</span>	https	36,126	684.47 MB	74,694	6.08 Mbps	82.99 pps	8.76 Mbps	204 pps
<span style="color: lightgreen;">■</span>	perforce	1,297	612.04 MB	0	5.44 Mbps	0 pps	11.38 Mbps	0 pps
<span style="color: purple;">■</span>	ssh	2,656	408.56 MB	19,918	3.63 Mbps	22.13 pps	4.18 Mbps	50 pps
<span style="color: orange;">■</span>	rtp-video	30	386.63 MB	285,122	3.44 Mbps	316.80 pps	3.81 Mbps	351 pps
<span style="color: yellow;">■</span>	smb	1,507	239.73 MB	0	2.13 Mbps	0 pps	4.52 Mbps	0 pps
<span style="color: teal;">■</span>	pandora	2,430	238.96 MB	0	2.12 Mbps	0 pps	2.57 Mbps	0 pps
<span style="color: blue;">■</span>	http	11,733	224.46 MB	1,164	2.00 Mbps	1.29 pps	3.06 Mbps	1 pps
<span style="color: red;">■</span>	epsndp	19	221.03 MB	2,965,351	1.96 Mbps	3.29 Kpps	29.46 Mbps	49.42 Kpps
<span style="color: grey;">■</span>	rtp	208	219.36 MB	81,268	1.95 Mbps	90.30 pps	3.52 Mbps	125 pps



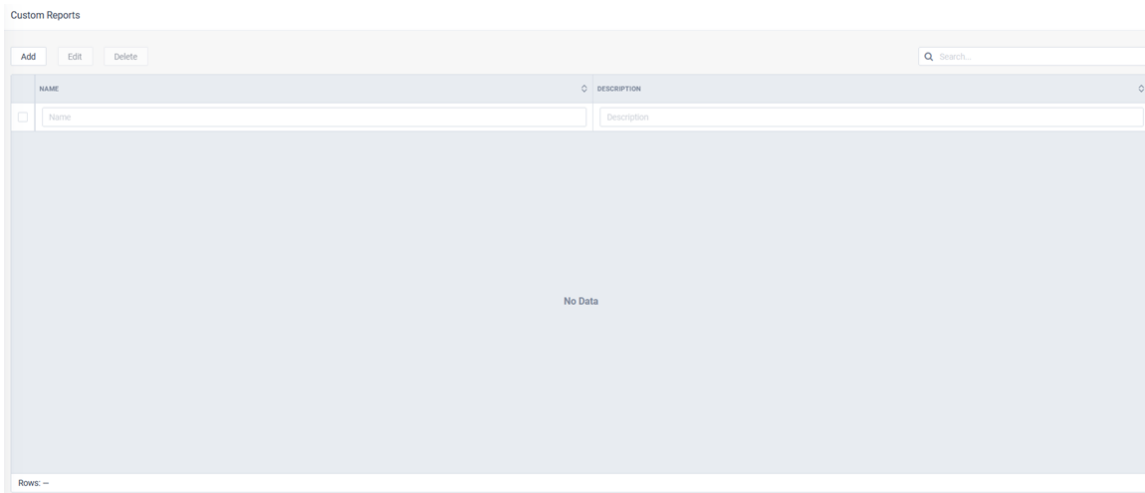
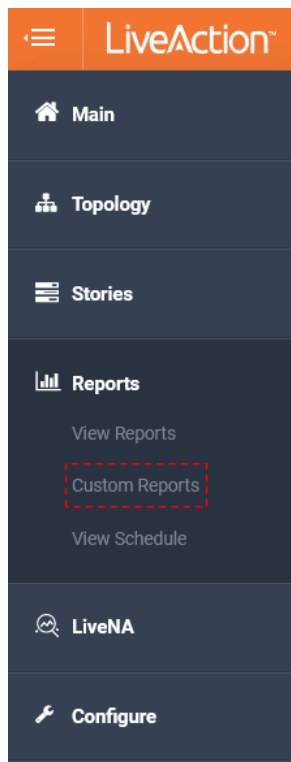
The **Share** button will copy a URL to the clipboard. When this URL is used, sign-in is not required to see the report.



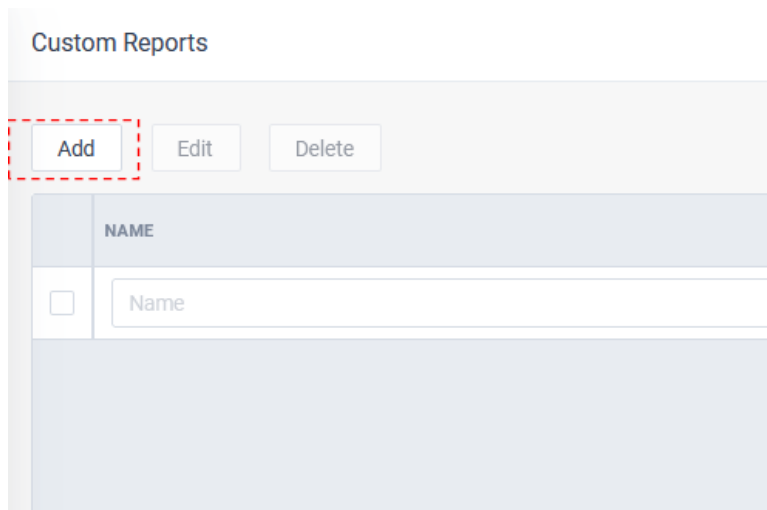
✓ Sharable URL Copied to Clipboard ✕

## Custom Reports

Custom reports allow you to design your own Flow report(s) based on most any Flow key and metric field.



To create a new *Custom Report*, click **Add**.



The *Create Custom Report* modal appears. Enter a *Name*, *Type*, *Direction*, and optionally provide a *Report Description*. When finished, click **Next Step**.

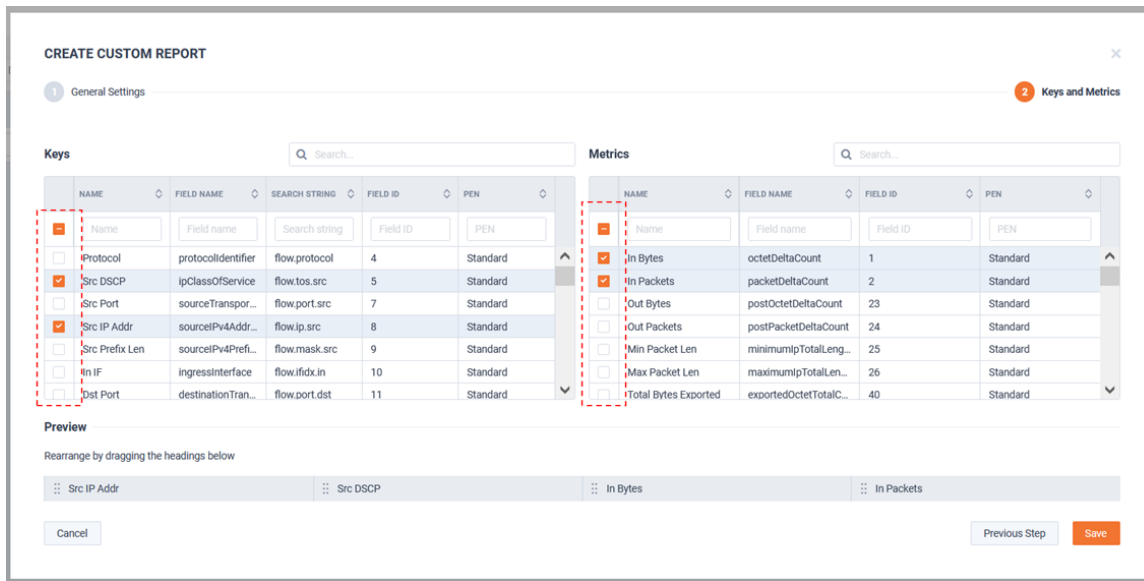
The screenshot shows the 'CREATE CUSTOM REPORT' modal. It has a title bar with a close button (X) and two tabs: 'General Settings' (active) and 'Keys and Metrics'. The form contains the following fields:

- Name \***: A text input field containing 'MyCustomReport'.
- Type**: A dropdown menu with 'Basic Flow' selected.
- Direction**: A dropdown menu with 'Inbound' selected.
- Report Description**: A text area containing 'This is my custom report'.

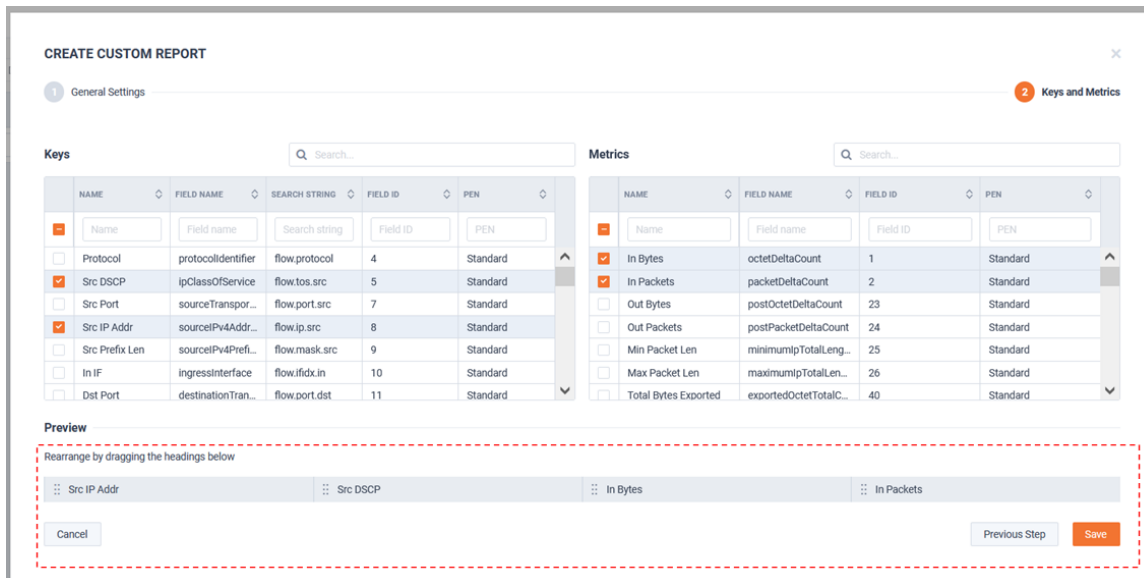
At the bottom left is a 'Cancel' button, and at the bottom right is a 'Next Step' button highlighted with a red dashed border.

Select the desired *Keys* and *Metrics* flow fields.

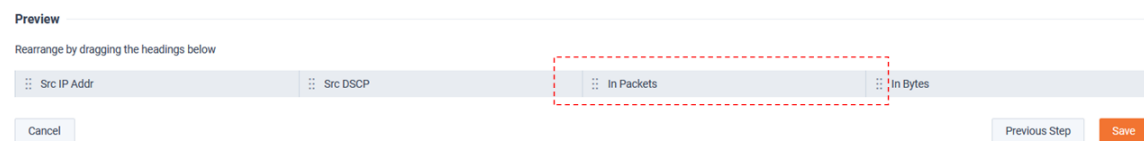




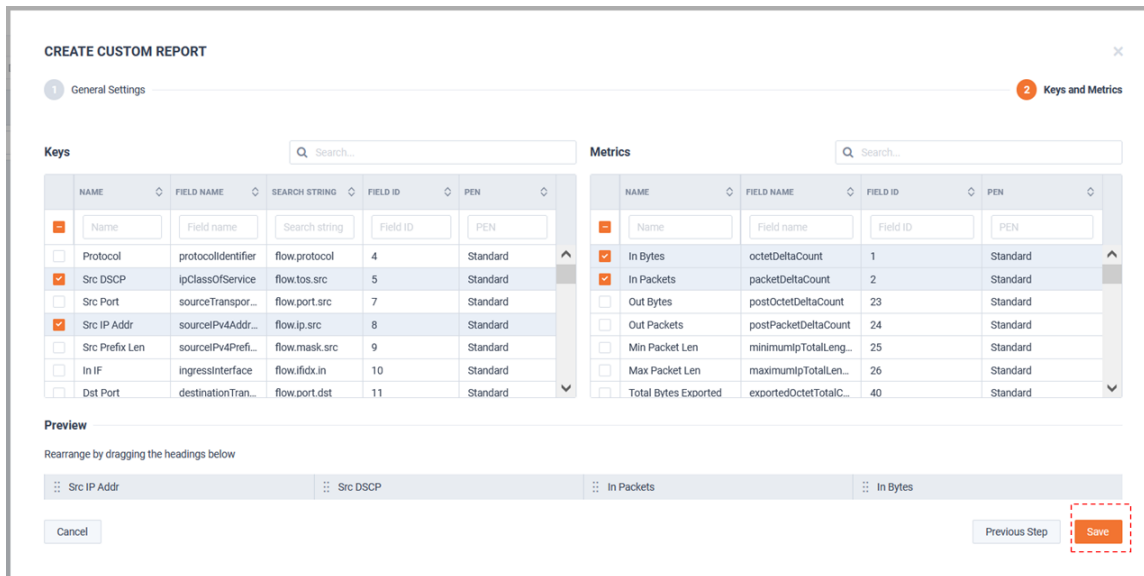
Under the *Preview* section, you can drag the headings to reorder them.



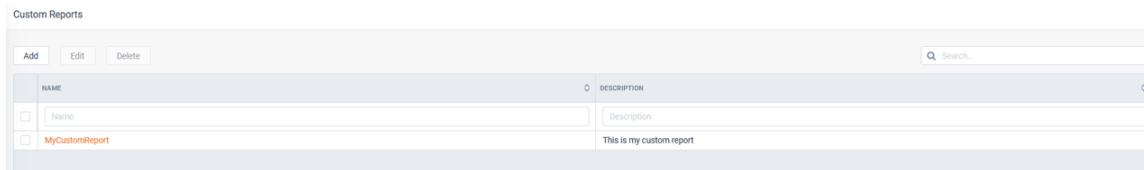
In this example, the *In Packets* field has been moved.



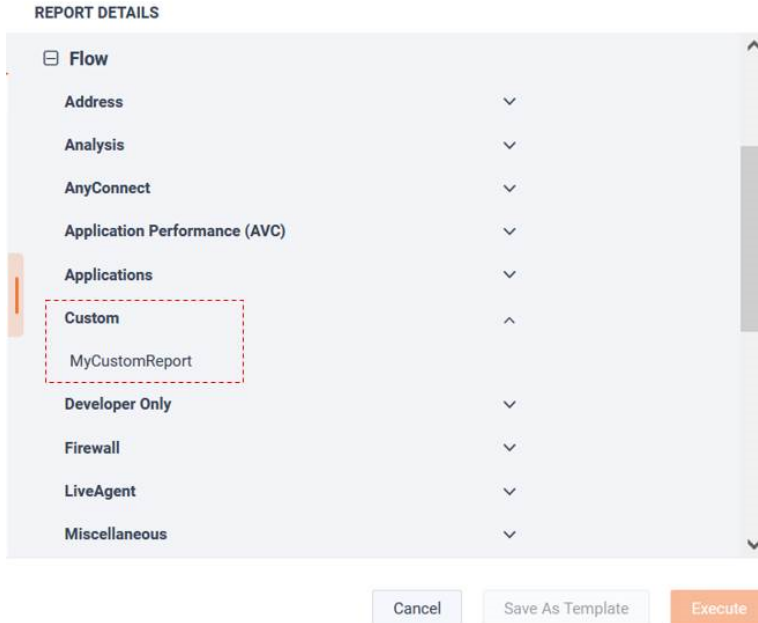
When finished, click **Save**.



The report will be listed under *Custom Reports*.



To run the custom report, go to *Flow > Custom*.



It will have the same familiar parameters as any other built-in Flow report.

**CREATE REPORT**

**GENERAL SETTINGS**

Name:

Presentation Mode:

Footnote:

Time Zone:  DST

Time Range:

Flex Search:

Display Filter:

**REPORT LIST**

MyCustomReport (Flow)

+ Add New Report

**REPORT DETAILS**

Report Description:

Sort By:

Devices:

Interfaces:

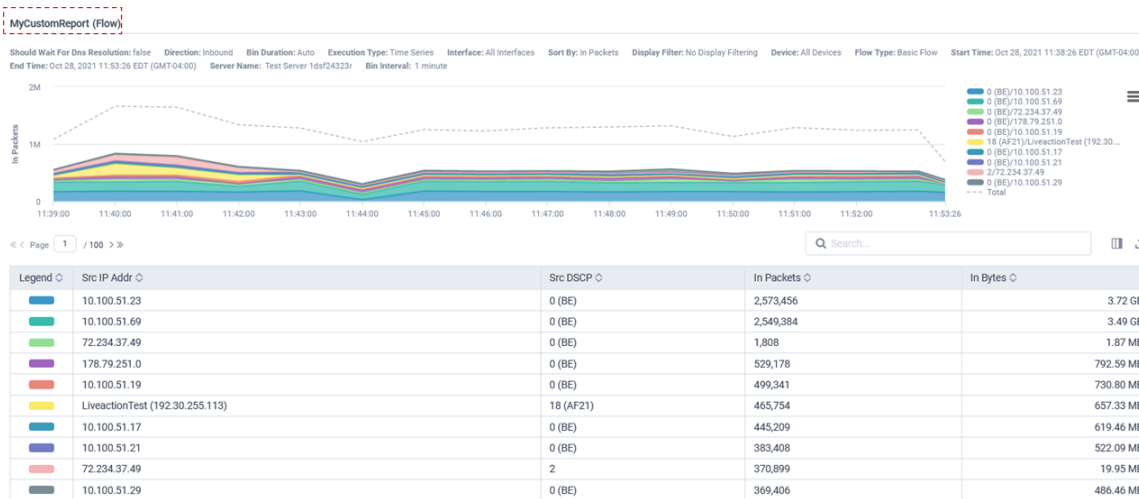
Flex Search:

Should Wait For DNS Resolution:

Direction:

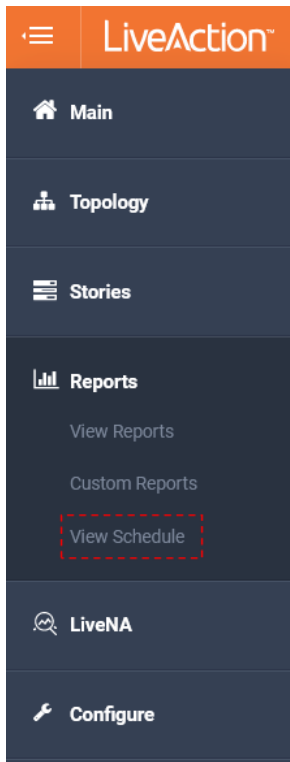
Display Filter:

Below are the results of this example custom report.

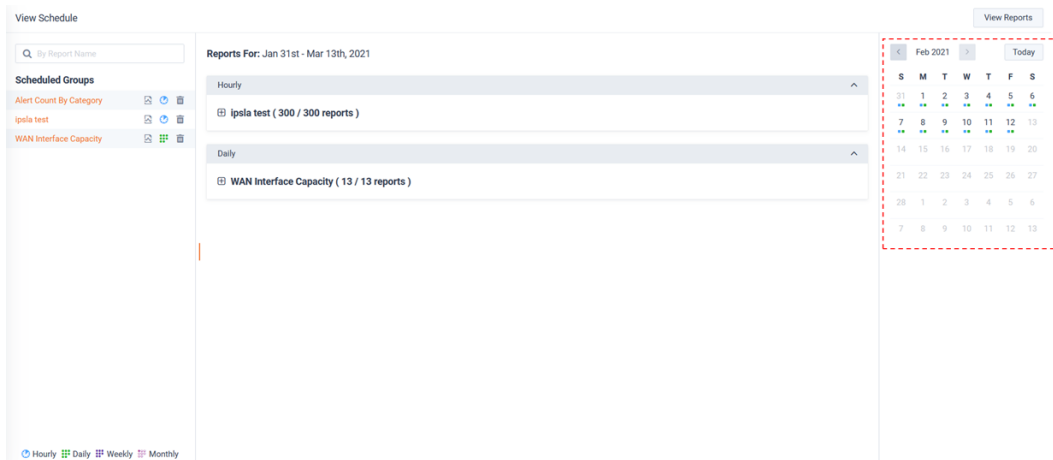


## View Schedule

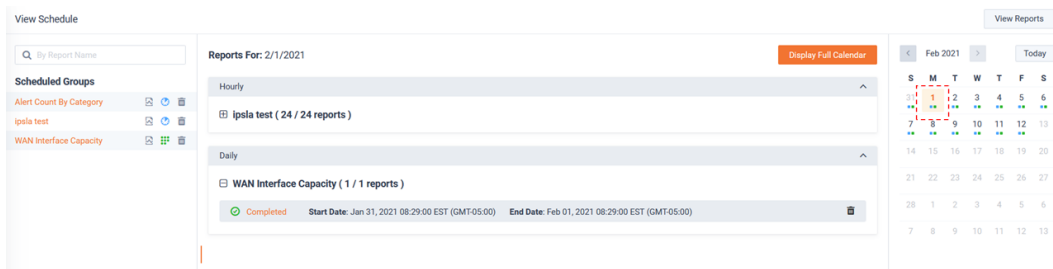
LiveNX allows one to schedule reports hourly, daily, weekly, and monthly. These can be accessed from *View Schedule* for easy access to past iterations of a report of interest.



The calendar at the far right of the page provides quick access to focus the view to a specific day's schedule reports. By default it will list all possible results.



In this example the, one day has been selected and just that day's reports are shown.



Use the **Display Full Calendar** button to see all results.

Display Full Calendar

Click on the *Completed* link to see the report scheduled report results of interest.

The screenshot shows the 'View Schedule' interface. On the left, there's a search bar and a 'Scheduled Groups' list containing 'Alert Count By Category', 'Ipsla test', and 'WAN Interface Capacity'. The main area shows reports for '2/1/2021'. Under the 'Hourly' group, there's 'Ipsla test ( 24 / 24 reports )'. Under the 'Daily' group, there's 'WAN Interface Capacity ( 1 / 1 reports )' with a 'Completed' status highlighted by a red dashed box. Below it, the start and end dates are shown: 'Start Date: Jan 31, 2021 08:29:00 EST (GMT-05:00)' and 'End Date: Feb 01, 2021 08:29:00 EST (GMT-05:00)'. On the right, there's a calendar view for February 2021.

The screenshot shows the 'View Reports > Schedule History: WAN Interface Capacity' page. It displays a report for 'Feb 01, 2021' at '08:29'. The report title is 'WAN Interface Capacity' with a 'Daily' frequency. The 'Executed at' time is 'Feb 01, 2021 08:29:05 EST (GMT-05:00)'. Below the title, there's a section for 'Interface Bandwidth (SNMP)' with a line graph showing 'Average Kbps' over time. The graph shows two lines: 'Inbound Bandwidth' (blue) and 'Outbound Bandwidth' (green). Below the graph is a table with the following data:

Legend	Name	Average	95th Percentile Bandwidth	99th Percentile Bandwidth	Peak Bandwidth
Inbound Bandwidth		103.91 Kbps	105.43 Kbps	105.56 Kbps	156.31 Kbps
Outbound Bandwidth		202.09 Kbps	205.04 Kbps	205.18 Kbps	301.43 Kbps

Below the table is a section for 'Interface Errors (SNMP)' with a line graph showing 'Errors (per)' over time. The graph shows two lines: 'Interface Errors Inbound' (blue) and 'Interface Errors Outbound' (green).

*Scheduled Groups* provides management for the scheduled reports.










The screenshot shows the 'View Schedule' interface. On the left, there's a search bar and a 'Scheduled Groups' list containing 'Alert Count By Category', 'Ipsla test', and 'WAN Interface Capacity'. The main area shows reports for 'Jan 31st - Mar 13th, 2021'. Under the 'Hourly' group, there's 'Ipsla test ( 300 / 300 reports )'. Under the 'Daily' group, there's 'WAN Interface Capacity ( 13 / 13 reports )'. On the right, there's a calendar view for February 2021. At the bottom left, there are radio buttons for 'Hourly', 'Daily', 'Weekly', and 'Monthly'.

Clicking on the template name allows editing of the template's configuration.

### View Schedule

By Report Name

#### Scheduled Groups

Alert Count By Category	  
ipsla test	  
WAN Interface Capacity	  

### RUN OR EDIT REPORT(S)

#### GENERAL SETTINGS

Name: WAN Interface Capacity

Presentation Mode: Standard

Footnote: Enter report group description...

Time Zone: (GMT-05:00) America/New York  DST

Time Range: Last Fifteen Minutes

Flex Search: Enter search criteria & report & flow settings

#### REPORT LIST

- Interface Bandwidth (SNMP)
- Interface Errors (SNMP)
- Interface Utilization (SNMP)
- Post-Policy Drops (SNMP)
- Application (Flow)
- Application (Flow)
- DSCP (Flow)
- DSCP (Flow)
- Source Address (Flow)
- Destination Address (Flow)
- Add New Report

#### REPORT DETAILS

Report Name: Interface Bandwidth

Report Description: Enter report description...

Devices: Select Device...

Interfaces: GigabitEthernet2

Bin Duration: Auto Bin

Execution Type: Time Series










Cancel Update Save As Template Execute

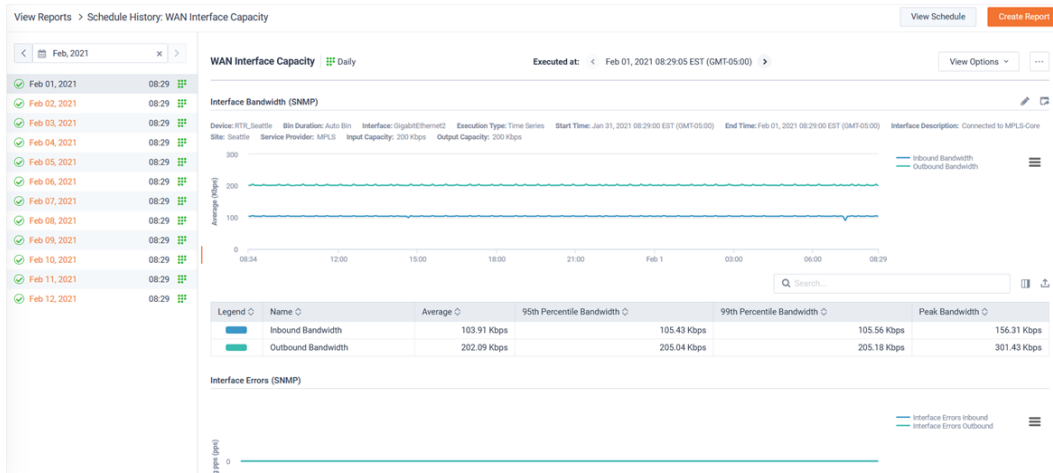
The **Show Recent Results** button provides quick access to the *Scheduled Report* data.

### View Schedule

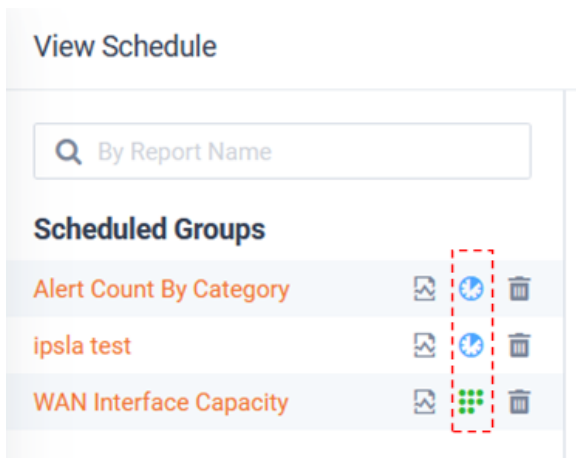
By Report Name

#### Scheduled Groups

Alert Count By Category	  
ipsla test	  
WAN Interface Capacity	  



The **Schedule** button provides access to modify the template’s schedule.



**SCHEDULE REPORT** [X]

**Name**  
WAN Interface Capacity

**Run Report**  
Daily

**Start Time**  
08:29

**End Time**  
08:29

**Schedule Ends**  
Never

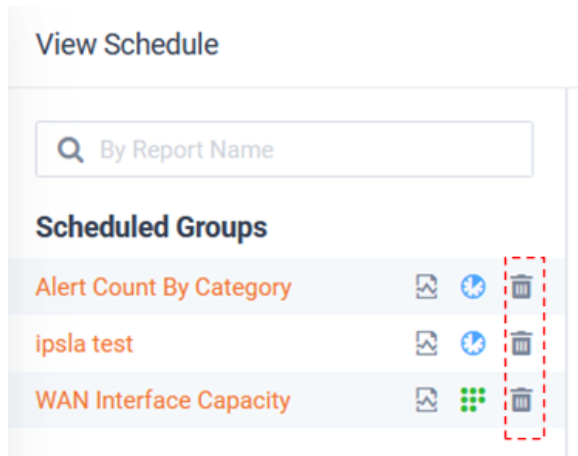
**Time Zone**  DST  
(GMT-05:00) America/New York

Cancel Update

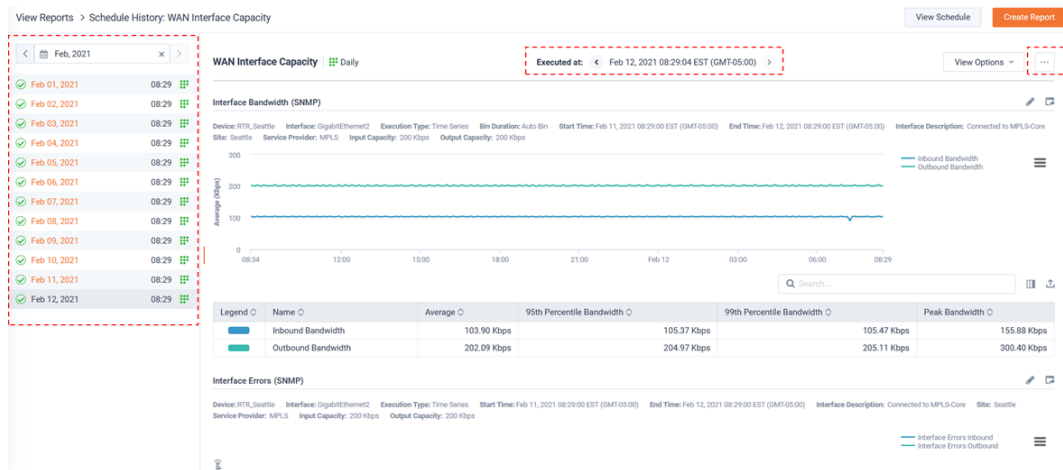
The icons indicate the type of schedule enabled for the template.

Hourly Daily Weekly Monthly

The **Delete** button disables the template's schedule. It does not delete the template.



The scheduled *View Reports* page is very similar to a standard *Report* view, but for the following exceptions:



The calendar can be used for quick navigation to specific past iterations of a report.



View Reports > Schedule History: WAN Int

< 📅 Feb, 2021 × >

✓	Feb 01, 2021	08:29	🟢
✓	Feb 02, 2021	08:29	🟢
✓	Feb 03, 2021	08:29	🟢
✓	Feb 04, 2021	08:29	🟢
✓	Feb 05, 2021	08:29	🟢
✓	Feb 06, 2021	08:29	🟢
✓	Feb 07, 2021	08:29	🟢
✓	Feb 08, 2021	08:29	🟢
✓	Feb 09, 2021	08:29	🟢
✓	Feb 10, 2021	08:29	🟢
✓	Feb 11, 2021	08:29	🟢
✓	Feb 12, 2021	08:29	🟢

< 📅 Feb, 2021
×
>

Feb 2021 Today

S	M	T	W	T	F	S
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	1	2	3	4	5	6
7	8	9	10	11	12	13

WAN Interface Capacity 🟢 Dai

< 2021 >

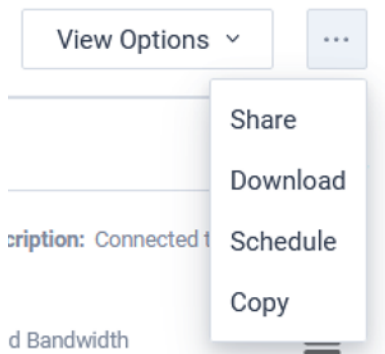
Jan	Jul
Feb	Aug
Mar	Sep
Apr	Oct
May	Nov
Jun	Dec

Cancel
Apply

Past and future iterations of a template can be controlled via the paddles at the top of the report.

**Executed at:** < Feb 12, 2021 08:29:04 EST (GMT-05:00) >

The familiar options are rolled up under a menu button.



## LiveNA

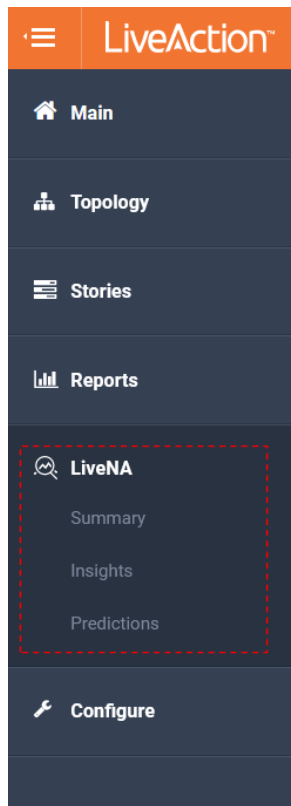
### In this chapter:

<i>LiveNA</i> .....	149
<i>Predictions</i> .....	153

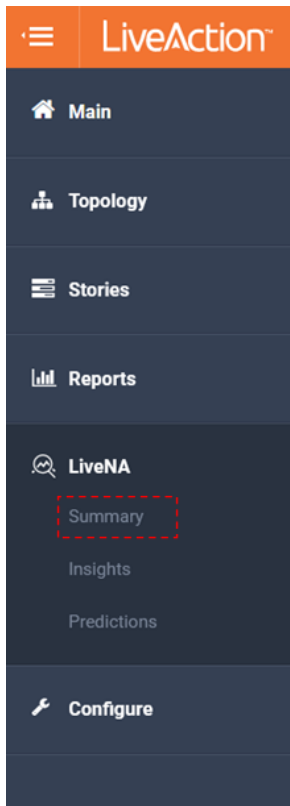
## LiveNA

LiveAction LiveNA is an optional AIOps platform that integrates with LiveNX.

It is accessed via LiveNX's Operation Dashboard. LiveNA applies ML/AI for learning the network's normal and detecting anomalies and making predictions of performance changes.



The LiveNA *Summary* page provides an overview of the Insights and Anomalies detected.



**LiveNA Summary**  Apply Filter

Insights by Recent Detection	Last Detection (EST)	Anomaly Count
Application maffio (saas/vendor) showing anomalies at Seattle	23-Jan-2021 02:00PM	128
Application cbr-elastic (db/vendor) showing anomalies at DC-New_York	23-Jan-2021 02:00PM	8
Application cbr-elasticsearch (db/vendor) showing anomalies at Madison	23-Jan-2021 02:00PM	8
Application esp-jira (saas/vendor) showing anomalies at San Jose	23-Jan-2021 02:00PM	3
Application maffio (saas/vendor) showing anomalies at Los_Angeles	23-Jan-2021 01:00PM	3
Application m-affice-365 (mca/cloud/group) showing anomalies at San Jose	23-Jan-2021 01:00PM	3
Application maffio-meeting (saas/vendor) showing anomalies at DC-New_York	23-Jan-2021 01:00PM	2
Application hmcagroup showing anomalies at London	23-Jan-2021 01:00PM	2
Application m-affice-vaas-eps (mca/cloud/group) showing anomalies at San Jose	23-Jan-2021 01:00PM	1
Application http (web) showing anomalies at Unspecified	23-Jan-2021 12:00PM	45
Application m-graphql showing anomalies at Unspecified	23-Jan-2021 12:00PM	19
Application m-graphql (mca/cloud/group) showing anomalies at DC-New_York	23-Jan-2021 12:00PM	4
Application ad (encrypted) showing anomalies at Los_Angeles	23-Jan-2021 12:00PM	1
Application https (web) showing anomalies at DC-New_York	23-Jan-2021 11:00AM	28
Application smtp (smtp/group) showing anomalies at Austin	23-Jan-2021 11:00AM	1
Application sfsaads (saas/vendor) showing anomalies at Louisville	23-Jan-2021 11:00AM	1
Application conferencing showing anomalies at DC-New_York	23-Jan-2021 10:00AM	1
Application http (web) showing anomalies at Madison	23-Jan-2021 09:00AM	19
Application facebook showing anomalies at Seattle	23-Jan-2021 09:00AM	3
Application facebook showing anomalies at DC-New_York	23-Jan-2021 09:00AM	2
Application facebook showing anomalies at Louisville	23-Jan-2021 08:00AM	2
Application m- (mca/cloud/group) showing anomalies at San Jose	23-Jan-2021 08:00AM	1
Application m-jira (saas/vendor) showing anomalies at Madison	23-Jan-2021 07:00AM	20
Application esp (saas/vendor) showing anomalies at Los_Angeles	23-Jan-2021 07:00AM	19
Application https (web) showing anomalies at Louisville	23-Jan-2021 07:00AM	16
Application esp (network/service) showing anomalies at Unspecified	23-Jan-2021 07:00AM	16
Application com-jira-email showing anomalies at Los_Angeles	23-Jan-2021 07:00AM	14
Application com-jira-email showing anomalies at Madison	23-Jan-2021 07:00AM	14
Application com-jira-email showing anomalies at Louisville	23-Jan-2021 07:00AM	4
Application m-affice (saas/vendor) showing anomalies at DC-New_York	23-Jan-2021 07:00AM	4
Application m-affice showing anomalies at Seattle	23-Jan-2021 07:00AM	3
Application maffio (saas/vendor) showing anomalies at Austin	23-Jan-2021 07:00AM	2

Applications by Anomalies	Last 30 days	Site	Last 30 days
Application maffio (saas/vendor)	128	DC-New_York	459
https (web)	141	San Jose	223
esp (saas/vendor)	122	Madison	209
esp (saas/vendor)	129	Seattle	144
http (web)	123	Unspecified	98
facebook (web)	42	Austin	96
http (web)	80	Los_Angeles	94
smtp (network/service)	60	Louisville	92
m- (network/service)	58	London	47
Other	492	Indianapolis	8

Devices by Anomalies	Last 30 days
Device	361
RTN_02040103	223
RTN_SanJose	209
RTN_Madison	144
CG-02050-23-21	98
RTN_Austin	96
RTN_LosAngeles	94
RTN_Louisville	92
RTN_London	47
Other	53

Sites by Anomalies	Last 30 days
Site	459
DC-New_York	223
San Jose	209
Seattle	144
Unspecified	98
Austin	96
Los_Angeles	94
Louisville	92
London	47
Indianapolis	8

Sites by Recent Detection	Last 30 days
Site	459
DC-New_York	223
San Jose	209
Seattle	144
Unspecified	98
Austin	96
Los_Angeles	94
Louisville	92
London	47
Indianapolis	8

**Total Sites Anomalies Over Time** Last 30 days

Filters can be applied to focus on the specific entities of interest:

### LiveNA Summary

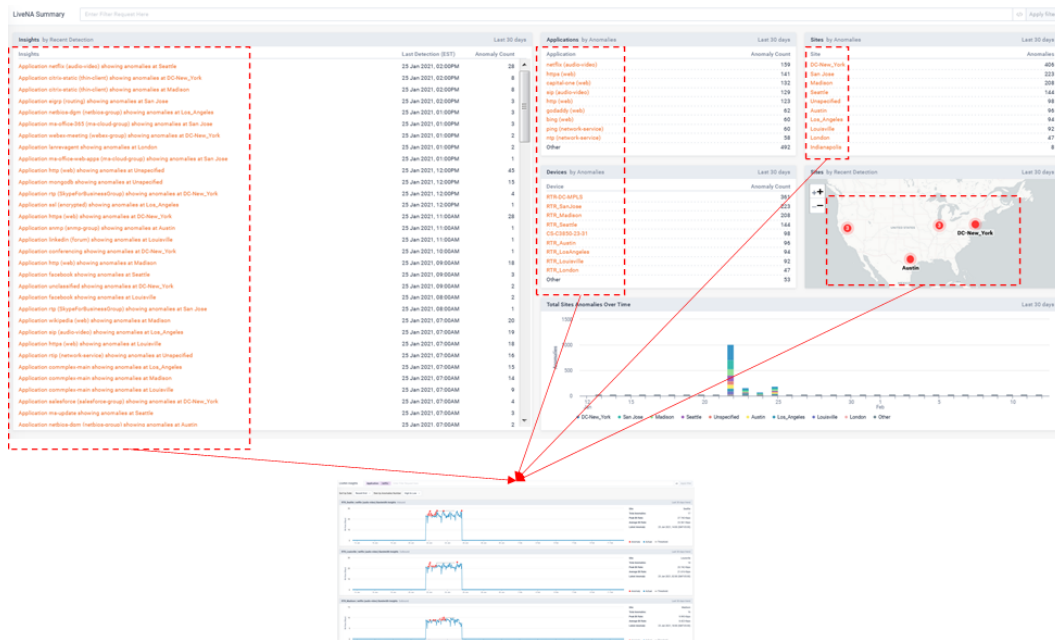
Enter Filter Request Here

- Site
- Device
- Tag
- Region
- Application
- Interface
- Service Provider

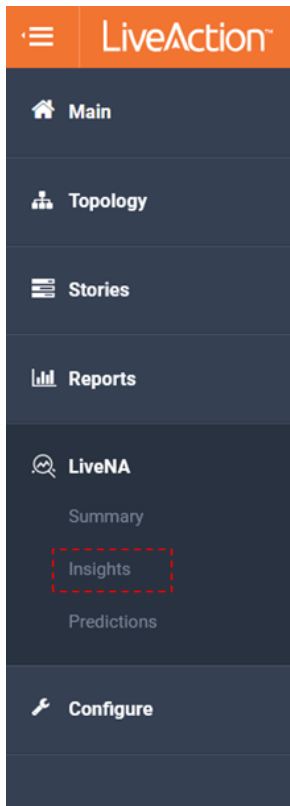
#### Insights by Recent Detection

Insights	Last 30 days
Application netfli...	25
Application citrix...	25
Application citrix...	25
Application eigrp...	25
Application netbi...	25
Application ms-o...	25
Application web...	25 Jan 2021, 01:00PM
Application lanre...	25 Jan 2021, 01:00PM

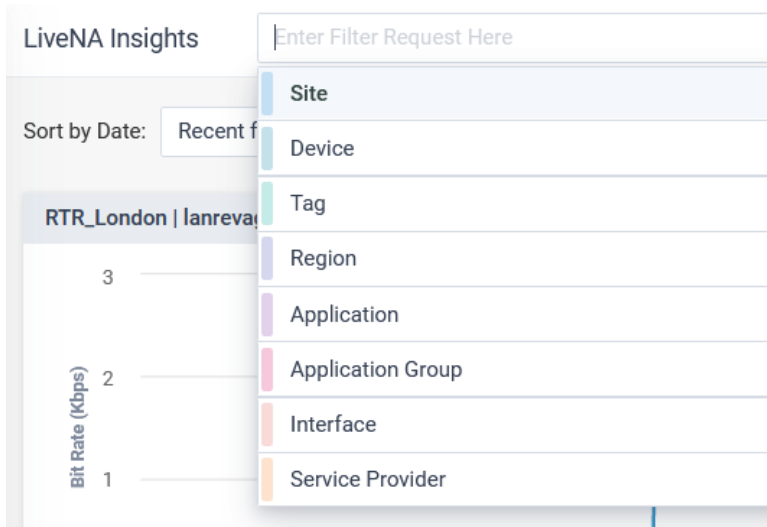
Widgets provide links to a curated list of Insight.



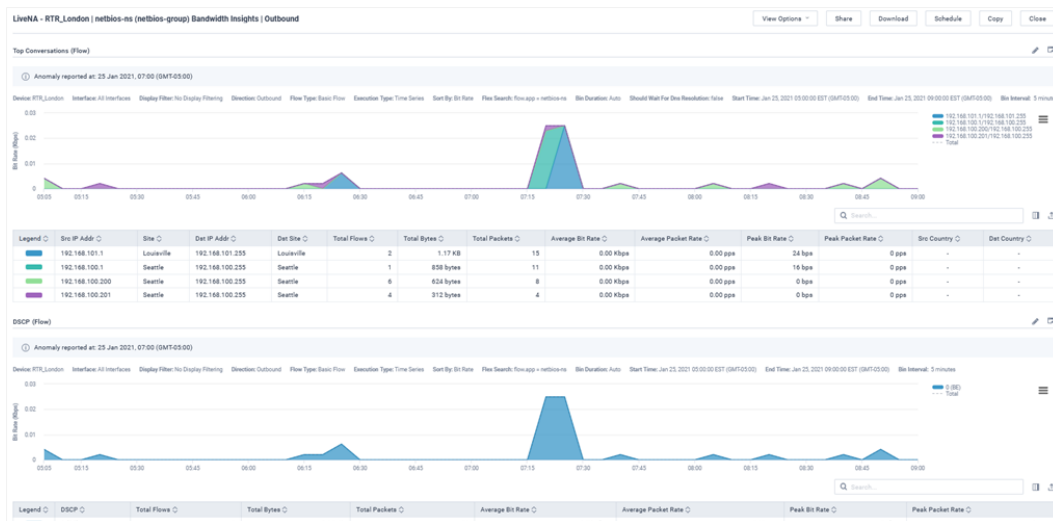
LiveNA will baseline tracked metrics and learn its normal threshold. The threshold will evolve with the underlying network usage and performance. Detected anomalies will be highlighted on the graph.



Filters can be applied to focus on the specific entities of interest:



Clicking an anomaly will bring up more detail and an option to cross-launch into a curated LiveNX report template for more details.



## Predictions

LiveNA predictions will collect the previous 13 months of historic data and trend its usage. It will highlight any past threshold crossing events and predict up to 4 months of future events.



