LiveNX 24.3.0 New Features

QUICK GUIDE



LiveNX TCP Flags Flow Flex Filter

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

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

Display Filter

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

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

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

▲ Flow Display Filters Setup	×
🌾 Create Filter 🛛 🤯 Copy 🏹 Delete 🚮 Rename	Filter Entry Details
Filter: TCP ACK Flood Attack	Filter Entry Action: Show or Hide the following
Filter Entries	IP Type: IPv4 Only IPv6 Only Both IPv4 & IPv6
🕒 Add Entry 🛛 🕞 Add Other Filter 🕞 Delete Entry 🌇 🌇	Color Mapping Label & Color:
TCP ACK Flood Attack	Basic Advanced
I] Show IPv4 Only (TCP Flags [AND]=A)	Match Flow Size
	Rate V 0 - 4294967 Kbps Max
	Match TCP Flags
	CWR ECE URG ACK PSH RST SYN FIN AND OR
	Match Autonomous System Number
	Match ASN Regardless of Source or Destination $\qquad \lor$
	Source:
	Destination: Enter individual autonomous system numbers or ranges separated by spaces
	(e.g., 125 256-300 5000)
	Match Next Hop IP, Range, Subnet
	Enter IP addresses, ranges, and/or subnets separated by spaces (e.g., 172, 120.0.1 192, 168.0.0/24 10.0.0.1-10.100.0.1)
	Match IPv6 Flow Label
	Enter IPv6 flow label values or ranges separated by spaces (e.g., 10 20-30)
	Match MAC Address
Note: Other filters added as entries are not editable here, but can be edited by selecting them in the Filter	Match Mac Addresses Regardless of Source or Destination
drop-down box.	Source.
Help	OK Cancel Apply

Improvements in 24.3.0

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

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

Flow Display Filters Setup	
🕻 Create Filter 😽 Copy 🏹 Delete 😿 Rename	Filter Entry Details
ter: TCP ACK Flood Attack 🗸	Filter Entry Action: O Show or Hide the following
ter Entries	IP Type: O IPv4 Only O IPv6 Only O Both IPv4 & IPv6
👌 Add Entry 🛛 📴 Add Other Filter 🕞 Delete Entry 🌇 🐘	Color Mapping Label & Color: 1
TCP ACK Flood Attack	Basic Advanced
[1] Show IPv4 Only (TCP Flags [Exact Match] =A)	□ □ Match Flow Size
	Rate V 0 - 4294967 Kbps Max
	Match TCP Flags
	CWR ECE URG ACK PSH RST SYN FIN Contains Any
	Contains All Contains All Exact Match Exact Match
	Match ASN Regardless of Source or Destination
	Source:
	Enter individual autonomous system numbers or ranges separated by spaces (e.g.,
	125 256-300 5000)
	☐ Match Next Hop IP, Range, Subnet
	Enter IP addresses, ranges, and/or subnets separated by spaces (e.g., 172.120.0.1 192.168.0.0/24 10.0.0.1-10.100.0.1)
	Match IPv6 Flow Label
	Enter IPv6 flow label values or ranges separated by spaces (e.g., 10 20-30)
	Match MAC Address
te: Other filters added as entries are not editable here, but can be edited by selecting them in	Match Mac Addresses Regardless of Source or Destination $\qquad \lor$
Filter drop-down box.	Causase

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

Implementation

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

Туре	Syntax	Description
Exact Match	 flow.tcpFlags=ACK,FIN flow.tcpFlags.cwr=false & flow.tcpFlags.ece=false & flow.tcpFlags.urg=false & flow.tcpFlags.ack=true & flow.tcpFlags.psh=false & flow.tcpFlags.rst=false & flow.tcpFlags.syn=false & flow.tcpFlags.syn=false & flow.tcpFlags.fin=true 	 The TCP flags field must only contain the ACK and FIN flags. With the second form of the filter string all of the TCP flags must be specified. Drill downs on the TCP flags field will us
Exact Match	flow.tcpFlags=""	The TCP flags field must contain no TCP flags.
Contains Any	flow.tcpFlags.ack=true flow.tcpFlags.fin=true	 The TCP flags field must contain the ACK or FIN flag. Note that flags set to false will be ignored when OR'ed together. Equivalent to the "contains any" display filter
Contains All	flow.tcpFlags.ack=true & flow.tcpFlags.fin=true	 The TCP flags field must contain both the ACK or FIN flags, but could contain other flags. Equivalent to the "contains all" display filter
Mixed	flow.tcpFlags.urg=false & flow.tcpFlags.ack=true & flow.tcpFlags.fin=true	 The TCP flags field must contain both the ACK or FIN flags, but could contain other flags except for the URG flag. The display filter does not support this type of matching
Mixed	flow.tcpFlags.ack= true flow.tcpFlags.syn=true & flow.tcpFlags.fin=true	This is equivalent to flow.tcpFlags.ack= true (flow.tcpFlags.syn=true & flow.tcpFlags.fin=true). The TCP flags field must contain either the ACK flag or both SYN and FIN flags.

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

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

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

• Note that almost all TCP flags filtering will be using the raw flow store vI because it is not a key in any longterm aggregated standard report. Currently, the only case where the long-term store might be used is with a custom report where the TCP flags field is the only key and the custom report is enabled for long-term aggregation. • Support for this filter has not been added to the ClickHouse report filtering and there are no currently plans to do this.

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

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

Related Updates

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

9	eneral Settings											2 Keys and Me
ys				Q	Search			Metri	ics		Q Search	
	NAME \$	FIELD NAME	SEARCH STRING	0	FIELD ID	PEN	0		NAME 🗘	FIELD NAME	FIELD ID	PEN \$
	Name	Field name	Search string		Field ID	PEN			Name	Field name	Field ID	PEN
~	Protocol	protocolldentifier	flow.protocol		4	Standard			In Bytes	octetDeltaCount	1	Standard
	Src DSCP	ipClassOfService	flow.tos.src		5	Standard			In Packets	packetDeltaCount	2	Standard
-	TCP Flags	tcpControlBits	flow.tcpFlags		6	Standard			Total Bytes	postOctetDeltaCount	23	Standard
~	Src Port	sourceTransportPort	flow.port.src		7	Standard			Total Packets	postPacketDeltaCount	24	Standard
~	Src IP Addr	sourcelPv4Address	flow.ip.src		8	Standard			Min Packet Len	minimumIpTotalLength	25	Standard
	Src Prefix Len	sourcelPv4PrefixLength	flow.mask.src		9	Standard			Max Packet Len	maximumIpTotalLength	26	Standard
	In IF	ingressInterface	flow.ifidx.in		10	Standard			Total Bytes Exported	exportedOctetTotalCount	40	Standard
~	Dst Port	destinationTransportP	flow.port.dst		11	Standard			Total Packets Exported	exportedMessageTotalCount	41	Standard
~	Dst IP Addr	destinationIPv4Address	flow.ip.dst		12	Standard			Total Flows	exportedFlowRecordTotalCo	42	Standard
	Dst Prefix Len	destinationIPv4Prefix	flow.mask.dst		13	Standard			Initiator Octets	initiatorOctets	231	Standard
	Out IF	egressInterface	flow.ifidx.out		14	Standard			Responder Octets	responderOctets	232	Standard
	Next Hop IP Addr	ipNextHopIPv4Address	flow.ip.nextHop		15	Standard			L2 Frame Delta Count	layer2FrameDeltaCount	430	Standard
	Src AS	bgpSourceAsNumber	flow.as.src		16	Standard			L2 Frame Total Count	layer2FrameTotalCount	431	Standard
	Dst AS	bgpDestinationAsNu	flow.as.dst		17	Standard			Ignored L2 Frame Total Count	ignoredLayer2FrameTotalCo	433	Standard
evie	W											
arra	nge by dragging the heading	gs below										
: p	rotocol	. Src IP Addr			. Src Port				: TCP Flags		Average Bit Rate	Average Packet Rate

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

	08, 2024 22:54:00 H	n Type: timeseries Sort B ST (GMT-10:00) End Time rt on sampled flow data, the	e: Aug 08, 2024 23:09:00 HS	ST (GMT-10:00) Busin	ess Hours: none Bi	n Interval: 1 m	ninute			Duration: auto	
600k	22:56	22-58	23.00	23:02		3:04	23:06			ICMP/192.168.0.100/19; UDP/192.168.1.252/255 PIM/192.168.1.52/255 PIM/192.168.1.172/224 PIM/192.168.1.173/224 PIM/192.168.1.173/224 PIM/192.168.1.173/224 PIM/192.168.0.173/224 UDP/192.1.23/10.1.211 ICMP/192.1.1/10.1.1.1 ICMP/192.1.1.1/10.1.1.1 Total	.255.255 0.0.13/-/ 168.1.17 0.0.13/-/ 0.0.13/-/ 0.0.13/-/ 15/13958 /-/2048/
Page 182	/200 >≫							Q Search			
egend 🗘	Protocol 🗘	Src IP Addr 🗘	Dst IP Addr 🛇	Src Port 🗘	Dst Port 🗘	TCP Flags	c Total	Flows 🗘	Average Bit Rate 🗘	Average Packet	Rate 🗘
	UDP	10.2.101.146	10.131.1.24	30001	161	-		15	2.53 Kb	ps	1.51 p
	TCP	10.122.71.140	10.131.101.2	2156	80	ACK FIN		15	0.15 Kb	ns	0.48 p
	ICMP	172.31.43.2	172.49.50.60	-	-			I to Search Filt			0.02 p
	ICMP	172.26.43.26	172.49.50.227	-	-			Flow to Searc			0.02
	ICMP	172.31.43.2	172.49.50.63	-	-			ACK FIN as Ap			0.02
	ICMP	172.31.43.2	172.49.50.108	-	-				Conversations		0.02
	UDP	10.4.201.207	10.4.203.156	161	42945			ACK FIN as Inte ACK FIN as DS	erface Bandwidth		0.93
	ICMP	172.31.43.2	172.49.50.143	-	-		Drill down on				0.02
	TCP	192.168.2.207	188.65.124.59	47476	443	ACK PSH			n Flow Path Analysis Stor	TV III	0.24
		192,168,2,211	10.2.101.141	54437	5004		2			·	

Auto Rotating Dashboards

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

Configuration

There are two aspects of configuration.

Global auto cycle configuration interval -

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

To configure the Global Auto cycle Configuration Interval:

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

■ LiveAction	NX			New F	eatures!	3 🗖	2 • 0	🌲 26384	{} • • • •	adm
Enter Filter Reque						Activ	ve Alerts			A Settings Settings System Diagnostics
SITES: 7		DEVICES: 16		INTERFACES: 145		1	Drop Rate was	s 187660.58 Kbp	06 had a drop rate of s for HE-CSR-206 on i	User Management LiveNX Server
	0	DEVICES 🗗	0	INTERFACES 🗗	0		CEDGE-Green	wich could not b	e reached.	06 Nov 2024, 10:20 PM
CEDGE-Greenwich		CEDGE-Greenwich		 GigabitEthernet0 CEDGE-G 	eenwich					
 Unspecified 		HE-CSR-206		 GigabitEthernet0/0/0 CED0 	E-Greenwich					
Barcelona		Barcelona		 GigabitEthernet0/0/1 CED0 	E-Greenwich					
Honolulu		CEDGENEW		GigabitEthernet0/0/1.1 CE)GE-Green					

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

≡ LiveAction	NX	New Features! 2 2 0	6 {)	}- 0-	0 -	💄 admi
Settings						
Q Search		AUTO CYCLE CONFIGURATION				
Configuration	×					
Dashboards	^	Note: Auto-cycle is for the full screen dashboard view only. Cycle-rate *				
Auto Cycle Configuration		1 min				
Widgets Management		Apply				
Data Source Management						
Data Store Management	× .					

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

Note: Auto-cycle is for the full screen Cycle-rate *	dashboard view offly.
1	Π
	Арр

Full Screen Dashboard

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

				New Features!	▲ 4 ■ 2	• 0 🐥 2	6390 {]	- 8-	Q -	.
Main				No	v 20, 2024 17:00:0	0 → Nov 20, 2024	17:15:00	Dashboards List	Add Wid	lget
Overview	··· :: WAN		System	:	Cisco SD	WAN Performance	::	,	Alerts	
Dashboard									<> F	Apply f
Sites										
Devices Peak Ir	bound WAN Interface Utilization 🗙	: Top WAN Applicat	tions by Bandwidth Inb	oound/Outbound Ban	dwidth 🗙	: Top Interfaces	% Changed - Ir	nterface Burstable	Rate	
		ssl→encrypted	10.7	in 💿		Toulouse→Toulo	use	-100.0	_	
Interfaces 0		ms-office-web-apps-		Out		CEDGE-Greenwic		-50.0		
WAN Applications 0		unknown→network-		0.00		PaloAlto→PaloAl			25.0	
n Art Applications		webex-meeting→we				Unspecified→CS		-25		
Alerts 0		ftp-data→ftp-group	1.6			CEDGE-Greenwic			2.3	
		rtp→audio-video	0.7			Unspecified→HE		-12	9.2	
Network Users 0		ndmp→network-serv				CEDGE-Greenwic			-3.1	
		lv-auth→unknown	<0.1			Unspecified→HE			0.0	
ve/Action Status		5:21:20 pm	November	r 20, 2024			Das Das	hboards List 🗸	2	
op Sites by WAN Utilization Peak Inbour		fop WAN Applications by Ba	Indwidth Inbound/Outbo			ces % Changed - Inte	un auto cycle rface Burstable F			
op Sites by WAN Utilization Peak Inbour nspecified→HE-CSR-20 514.0	nd WAN Interface Utilization	Top WAN Applications by Ba ssl→encrypted	Indwidth Inbound/Outbo	und Bandwidth	Toulouse→	ces % Changed - Inte	un auto cycle rface Burstable F -100.0	tate		
pp Sites by WAN Utilization Peak Inbour nspecified→HE-CSR-20 514.0 nspecified→HE-CSR-20 14.0	nd WAN Interface Utilization	fop WAN Applications by Ba sl→encrypted ns-office-web-apps→ms	indwidth Inbound/Outbo		Toulouse→ CEDGE-Gre	ces % Changed - Inte Toulouse→ge0/1.1_ enwich→CEDGENE	un auto cycle rface Burstable F		<i>•</i>	
op Sites by WAN Utilization Peak Inbour nspecified → HE CSR-20 514.0 Inspecified → HE CSR-20 14.0 I onolutu → Honolutu → ge 6.0	Nd WAN Interface Utilization	fop WAN Applications by Ba ssl—encrypted ns-office-web-apps—rns inknown—network-service	andwidth Inbound/Outboo 10.7	und Bandwidth	Toulouse→ CEDGE-Gre PaloAlto→I	ces % Changed - Inte Toulousege0/1.1 enwich>CEDGENE PaloAlto>ge0/0.20	rface Burstable F -100.0 -50.0	late		
op Sites by WAN Utilization Peak Inbour nspecifiedHE-CSR-20514.0 mspecifiedHE-CSR-2014.0 incolubuHonolubu -ge6.0 oulouseToulouseg1.0	nd WAN Interface Utilization	Top WAN Applications by Ba ssl→encrypted ns-office-web-apps→ms- inknownnetwork-service vebex-meetingwebex-g.	andwidth Inbound/Outboo 10.7	und Bandwidth	Toulouse→ CEDGE-Gre PaloAlto→I Unspecified	R ces % Changed - Inte Toulouse→ge0/1.1 enwich→CEDGENE PaloAlto→ge0/0.20 I→CS-ISR4461-105	rface Burstable R -100.0 -50.0 -25.	tate		
op Sites by WAN Utilization Peak Inbour nspecified→HE-CSR-20514.0 inspecified→HE-CSR-2014.0 ionolulu-ge	nd WAN Interface Utilization	fop WAN Applications by Ba ssl⊸encrypted ns-office-web-apps→ms inknownnetwork-service vebex-meeting-webex-g_ tp-data→ftp-group	10.7	und Bandwidth	Toulouse→ CEDGE-Gre PaloAlto→I Unspecified CEDGE-Gre	R ces % Changed - Inte Toulouse→ge0/1.1 enwich→CEDGENE PaloAlto→pe0/0.20 →CS-ISR4461-105 enwich→CEDGENE	rface Burstable F -100.0 -50.0	tate 25.0 0 3		
sp Sites by WAN Utilization Peak Inbour nspecified—HE-CSR-20514.0 mspecified—HE-CSR-2014.0 poulouse—Toulouse—g10 pulouse—Toulouse—g10 nspecified—HE-CSR-2000)	id WAN Interface Utilization	Fop WAN Applications by Ba ssl→encrypted ns-office-web-apps→ms inknownnetwork-service vebex-meetingwebex-g_ tp-datatfp-group tp-audio-video	Indwidth Inbound/Outboo 6.4 4.0 2.9 1.6 1.6 1.0 0.7	und Bandwidth	Toulouse→ CEDGE-Gre PaloAlto→I Unspecified CEDGE-Gre Unspecified	R ces % Changed - Inte Toulouse	rface Burstable R -100.0 -50.0 -25/ -12	tate 25.0 0 3 9.2	2	
op Sites by WAN Utilization Feak Inbour nspecifiedHE-CSR-201140 InnoluluHonoluluge00 nspecifiedHE-CSR-2000 nspecifiedHE-CSR-2000 nspecifiedHE-CSR-2000	nd WAN Interface Utilization	For WAN Applications by Ba soffice-web-apps-ims- inknown-inetwork-service vebex-meeting-webex-g. tp-data-fitp-group tp-audio-video dimp-network-service	10.7	und Bandwidth	Toulouse→ CEDGE-Gre PaloAlto→I Unspecified CEDGE-Gre Unspecified CEDGE-Gre	R Toulouse	rface Burstable R -100.0 -50.0 -25/ -12	tate 25.0 0 3		
pp Sites by WAN Utilization Peak Inbourn nspecified—HE-CSR-20 514.0 molulu—ge	nd WAN Interface Utilization	Fop WAN Applications by Ba sist-encrypted ns:office web apps-ms- mknown-network-service webex-meeting-webex-g- ty-data-ft-p-orup tp-audit-video dmpnetwork-service audit-unknown	Indwidth Inbound/Outboo 10.7	und Bandwidth	Toulouse CEDGE-Gre PaloAltoI Unspecified CEDGE-Gre Unspecified CEDGE-Gre Unspecified	R ces % Changed - Inte Toulouse	rface Burstable R -100.0 -50.0 -25/ -12	tate 25.0 0 3 9.2 3.1		
op Sites by WAN Utilization Peak Inbour InspecifiedHE-CSR-20. 514.0 InspecifiedHE-CSR-20. 14.0 InspecifiedHE-CSR-20. 0.0 InspecifiedHE-CSR-20. 0.0 InspecifiedHE-CSR-2	Id WAN Interface Utilization	Top WAN Applications by Ba sist-encrypted ns:sifte-web apps-ms- inknown - network-service websc-meeting-websc-gu tp-data-ftp-group tp-aat/de-video dmpnetwork-service v-authunknown bynamic3dunknown locentunknown	Indwidth Inbound/Outboo	und Bandwidth	Toulouse – CEDGE-Gre PaloAlto – J Unspecified CEDGE-Gre Unspecified Unspecified Unspecified	R Toulouse	rface Burstable R -100.0 -50.0 -25/ -12	Late 25.0 3.1 9.2 3.1 9.2 3.1		
op Sites by WAN Utilization Peak Inbour InspecifiedHE-CSR-20. 514.0 InspecifiedHE-CSR-20. 14.0 InspecifiedHE-CSR-20. 0.0 InspecifiedHE-CSR-20. 0.0 InspecifiedHE-CSR-2	Id WAN Interface Utilization	Top WAN Applications by Ba sist-encrypted ns:sifte-web apps-ms- inknown - network-service websc-meeting-websc-gu tp-data-ftp-group tp-aat/de-video dmpnetwork-service v-authunknown bynamic3dunknown locentunknown	Inbound/Outbook 10.7	und Bandwidth	Toulouse – CEDGE-Gre PaloAlto – J Unspecified CEDGE-Gre Unspecified Unspecified Unspecified	R toulouse	rface Burstable R -100.0 -50.0 -25/ -12	tate 25.0 25.0 0 9.2 3.1 0.0 0.0		
op Sites by WAN Utilization Peak Inbour nspecifiedHE-CSR-20514.0 InspecifiedHE-CSR-20514.0 oulouseToulouseg10 InspecifiedHE-CSR-2000 InspecifiedHE-CSR-2000 InspecifiedHE-CSR-2000 oulouseToulouselo00 InducesToulouselo00	id WAN Interface Utilization	Top WAN Applications by Ba sist-encrypted ns:sifte-web apps-ms- inknown - network-service websc-meeting-websc-gu- tp-data-ftp-group tp-data-ftp-group tp-data-ftp-group tp-auto-wide dmpnetwork-service watthunknown locentunknown	Indwidth Inbound/Outboo	und Bandwidth	Toulouse CEDGE-Gre PaloAlto Unspecifier CEDGE-Gre Unspecifier CEDGE-Gre Unspecifier Honolulu	R toulouse	rface Burstable R -100.0 -50.0 -250 -12 -12	tate 25.0 25.0 0 9.2 3.1 0.0 0.0		
op Sites by WAN Utilization Peak Inbour nspecified -HE-CSR-20514.0 isopecified -HE-CSR-20514.0 Inspecified -HE-CSR-200.0 Inspecified -HE-CSR-20	id WAN Interface Utilization	Top WAN Applications by Ba sslencrypted ms-office-web-appsms inshownnetwork-service vebex-meetingwebex-g- tp-datathp-group tp-audio-vide-service dmpnetwork-service	Indwidth Inbound/Outboo	und Bandwidth	Toulouse CEDGE-Gre PaloAltoI Unspecified CEDGE-Gre Unspecified Unspecified Unspecified Honolulu	Sees % Changed - Intel Toulcusege0/1.1. mwichCE06FNE_ rabatio_pe0/0.20. CS:ISR4461-105. mwichCE06FNE_ HE CSR 206-00. HE CSR 208-00. CS:ISR4461-105. Hen CSR 208-00. CS:ISR4461-105. Honolulu_ge0/0	In auto cycle	tate 25.0 25.0 0 9.2 3.1 0.0 0.0		
op Sites by WAN Utilization Peak Inbour Inspecified -HE-CSR-20514.0 Inspecified -HE-CSR-20514.0 Inspecified -HE-CSR-200.0 Inspecified -HE-CSR	id WAN Interface Utilization	Top WAN Applications by Ba sisl→encrypted ns:sli→encrypted ns:sli→encrypted particle apps=ims_ inknown - network-service vacht→unknown dipm=network-service vacht→unknown locent→unknown M Dverall Status All	Indwidth Inbound/Outboo	und Bandwidth ● In ● Out	Toulouse CEDGE-Gre PaloAlto1 Unspecified CEDGE-Gre Unspecified Unspecified Unspecified Honolulu	See % Changed - Inte Toulicusege0/1.1. enwichCEOGENE. alaAitoge0/20.2. CSI:SR4461-105. HECSR:208-06I. CSI:SR4461-105. HECSR:208-06I. CSI:SR4461-105. Monoluluge0/0 a Top Devices CPU U	un auto cycle -100.0 -50.0 -25. -12 -25 -25 -25 -25 -25 -25 -25 -25 -22 -25 -22 -25 -22 -25 -22 -22	tate 25.0 25.0 0 9.2 3.1 0.0 0.0		
op Sites by WAN Utilization Peak Inbour InspecifiedHE-CSR-205140 InspecifiedHE-CSR-205140 Inspecified-HE-CSR-2000 Inspecifi	Id WAN Interface Utilization	Top WAN Applications by Ba sisl→encrypted ns:sli→encrypted ns:sli→encrypted particle apps=ims_ inknown - network-service vacht→unknown dipm=network-service vacht→unknown locent→unknown M Dverall Status All	Indwidth Inbound/Outboo	und Bandwidth ● In ● Out	Toulouse CEDGE-Gre PaloAlto1 Unspecified CEDGE-Gre Unspecified Unspecified Unspecified Honolulu	Compared and a set of the se	un suto cycle face Burstable R -100.0 -500 -25. -12 -3 -3 -3 -3 -3 -3 -3 -3 -3 -3	tate 25.0 25.0 0 9.2 3.1 0.0 0.0		
oulouseToulouseg10 1 InspecifiedHE_CSR-2000 0 InspecifiedHE_CSR-2000 1 Stestatus Map_All Sites 1	Id WAN Interface Utilization	fop WAN Applications by Ba sisi-encrypted ns office web apps -ms - mknown -network-service ty-data - ftp-proup tp-audio-video dimpnetwork-service wauthunknown isocentunknown isocentunknown isocentunknown isocentunknown isocentunknown isocentunknown isocentunknown	individth Inbound/Outboo 0.7	und Bandwidth ● In ● Out	Toulouse CEDGE-Gre PaloAlto1 Unspecified CEDGE-Gre Unspecified CEDGE-Gre Unspecified Honolulu	Compared and a set of the se	un auto cycle -100.0 -25. -12 -25. -12 -25. -12 -25. -12 -25. -12 -25. -12 -25. -12 -25. -12 -25. -12 -25. -10.0 -25. -25. -10.0 -25. -2	tate 25.0 25.0 0 9.2 3.1 0.0 0.0		
Sites by WAN Utilization Peak Inbour Inspecified →HE-CSR-205140 Inspecified →E-CSR-205140 Outouse →Toutouse →0100 Inspecified →HE-CSR-2000 Inspecified →	Id WAN Interface Utilization	top WAN Applications by Ba sslencrypted ns office web appsms inhnownnetwork-service webscmeeting-websc-0 top-datafb-group tp-addio-video dmpnetwork-service webscunknown locentunknown locentunknown Moreall Status All Critical Sites 3	individth Inbound/Outboo 0.7	ocod	Toulouse CEDGE-Gre PaioAlto Unspecified CEDGE-Gre Unspecified Unspecified Honolulu Top Device Barcelona- CEDGE-Gre Honolulu Moscowite Toulouse	Bit Construction Bit Construction Dess % Changed - Intermediation Bit Construction Pailoditio - ge0/0 20. Construction Construction CEOGENE. Intermediation Marcelon. Intermediation Marcelon.<	an outo cycle rface Burstable Fi -1000 -500 -25 -12 -3 -3 -3 -3 -3 -3 -3 -3 -3 -3	tate 25.0 25.0 0 9.2 3.1 0.0 0.0		
Sites by WAN Utilization Peak Inbour InspecifiedHE-CSR-2014.0 InspecifiedHE-CSR-2014.0 InspecifiedHE-CSR-2001 InspecifiedHE-CSR-2000	nd WAN Interface Utilization	fop WAN Applications by Ba sisi-encrypted ns office web apps -ms - mknown -network-service ty-data - ftp-proup tp-audio-video dimpnetwork-service wauthunknown isocentunknown isocentunknown isocentunknown isocentunknown isocentunknown isocentunknown isocentunknown	andwidth Inbound/Outboo 10.7 6.4 4.0 11.7 2.9 1.6 1.0 0.7 0.7 0.7 0.7 0.7 0.7 0.7 0	und Bandwidth ● In ● Out	Toulouse CEDGE-Gre PaloAlto Junspecified CEDGE-Gre Unspecified CEDGE-Gre Unspecified Honolulu Top Device Barcelona CEDGE-Gre Honolulu MoscowVe Toulouse PaloAlto PaloAlto	Bit Control Bit Control Sees % Changed - Inte Environ environ - CEDGENE FaloAto - Jog0/2020. raioAto - Jog0/2020. Environ L-INE CSR 206 - 01. Environ environ - CEDGENE - INE CSR 206 - 01. environ - CEDGENE - INE CSR 206 - 01. - INE CSR 206 - 01. - INE CSR 206 - 01. environ - CEDGENE - INE CSR 206 - 01. - INE CSR 206 - 01. - INE CSR 206 - 01. - INE CSR 206 - 01. - INE CSR 206 - 01. - INE CSR 206 - 01. - INE CSR 206 - 01. - INE CSR 206 - 01. - INE CSR 206 - 01. - INE CSR 206 - 01. - INE CSR 206 - 01. - INE CSR 206 - 01. - INE CSR 206 - 01. - INE CSR 206 - 01. - INE CSR 206 - 01. - CEDGENEW 60. - Monobilu - 40. - Manobilu - 40.	an suto cycle rface Burstable R -1000 -500 -255 -12 -25 -12 -25 -12 -25 -12 -25 -12 -25 -12 -25 -10 -25 -10 -25 -10 -25 -10 -25 -10 -25 -10 -25 -10 -25 -25 -25 -25 -25 -25 -25 -25	tate 25.0 25.0 0 9.2 3.1 0.0 0.0		
op Sites by WAN Utilization Peak Inbour Inspecified -HE-CSR-2014.0 Inspecified -HE-CSR-2014.0 Inspecified H-ECSR-2010.0 Inspecified H-ECSR-2000.1 Inspecified -HE-CSR-2000.0 Inspecified -HE-CSR-20_	Id WAN Interface Utilization	top WAN Applications by Ba sslencrypted ms-office-web-appa-ms innonwn-melwork-service vebex-meetingwebex-g tp-datathp-group tp-audio-video dmpnetwork-service of main-service dmpnetwork-service of main-service dmpnetwork-service of main-service dmpnetwork-service main-service dmpnetwork-service main-service dmpnetwork-s	andwidth Inbound/Outboo 10.7 6.4 4.0 11.7 2.9 1.6 1.0 0.7 0.7 0.7 0.7 0.7 0.7 0.7 0	e in Cood Good 4 8	Toulouse CEDGE-Gre PaloAlto1 Unspecifiet CEDGE-Gre Unspecifiet CEDGE-Gre Unspecifiet Honolulu Top Device Barcelona- CEDGE-Gre Honolulu MoscowVe Toulouse PaloAlto-1 MoscowVe	Bit Control Bit Control Toulousege0/11 envichCEOGENE.	un suto cycle -100.0 - -500 -25. -12. - - - - - - - - - - - - -	tate		
op Sites by WAN Utilization Peak Inbour nspecified_HE-CSR-20_5140 Inspecified_HE-CSR-20_5140 Inspecified_HE-CSR-20_01 Inspecified_HE-CSR-20_00	nd WAN Interface Utilization	top WAN Applications by Ba sslencrypted ns office web appsms inhnownnetwork-service webscmeeting-websc-0 top-datafb-group tp-addio-video dmpnetwork-service webscunknown locentunknown locentunknown Moreall Status All Critical Sites 3	andwidth Inbound/Outboo 10.7 6.4 4.0 11.7 2.9 1.6 1.0 0.7 0.7 0.7 0.7 0.7 0.7 0.7 0	ocod	Toulouse CEDGE-Gre PaloAlto1 Unspecified CEDGE-Gre Unspecified Unspecified Honolulu Top Device Barcelona- CEDGE-Gre Honolulu Moscowite Toulouse PaloAlto1 Moscowite Unspecified	Bit Control Bit Control Sees % Changed - Intel Toulouse - ge0/12.0. amwich - CEDGENE raioAto - ge0/12.0. - Intel CSR 206 - 01. Environ - CEDGENE - IntE CSR 206 - 01. Environ - CEDGENE - IntE CSR 206 - 01. Environ - CEDGENE - IntE CSR 206 - 01. Environ - CEDGENE - IntE CSR 206 - 01. Environ - CEDGENE - IntE CSR 206 - 01. Environ - CEDGENE - IntE CSR 206 - 01. Environ - CEDGENE - IntE CSR 206 - 01. Environ - CES ISR 404-105. Honolului - ge0/0	an suto cycle frace Burstable R -100.0 -50.0 -25. -12 -25 -12 -25 -25 -12 -25 -12 -25 -12 -25 -12 -25 -12 -25 -10 -25 -12 -12 -25 -25 -12 -25 -25 -25 -25 -25 -25 -25 -2	tate		

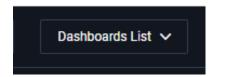
Enabling Auto Rotation of Dashboard

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

LiveAction Status	5:24:55 pm November 20, 2024	Dashboards List 🗸
Top Sites by WAN Utilization Peak Inbound WAN Interface Utilization	Top WAN Applications by Bandwidth Inbound/Outbound Bandwidth	Top Interfaces % Changed - Interface Burstable Rate
Unspecified→HE-CSR-20 514.0	ssi→encrypted 9.0 In	Unspecified—CS-ISR44 -105 60.0
Unspecified—HE-CSR-20 15.0	ms-office-web-apps→ms 4.9 Out	Unspecified—CS-ISR4461-105 60.0
Honolulu-Honolulu-ge 10.0	unknown	CEDGE-Greenwich→CEDGENE50.0
	webey-meeting_webey-g 3.0	PaloAtto-PaloAtto-ge0/0.20 -40.0

Configuration Options Available on Full Screen Dashboard

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



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



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



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

M

Individual dashboard options

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

Improved Third Party Auth Login UX

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

Logging In

The login experience has changed in the following ways:

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

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

Configuration

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

Please find the steps below to configure the "Default Login Method"

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

■ LiveAction	NX			New Features		3	2 • () 🙏 26445			۰.	
verview Enter Filter Reque	est Here										Settings	
Sites, Devices, Interfaces by Stat	tuses					Ac	tive Alerts				System E	
SITES: 7		DEVICES: 16		INTERFACES: 145				7.testexample.com	could not be re	ached	User Mar	
		~			- 1			6 could not be read		acheu.	LiveNX S	
						1.5	GigabitEth	ernet3 on HE-CSR-2	06 had a drop r	ate of	20 Nov 2024	4, 06:34 PM
SITES 🛃	0	DEVICES 🗗	0	INTERFACES 🗹	0	1.5	Drop Rate	was 181930.66 Kbp	os for HE-CSR-2	:06 on i	20 Nov 2024	4, 06:32 PM
 Unspecified 		HE-CSR-207		GigabitEthernet1 HE-CSR-207			CEDGE-Gre	enwich could not b	e reached.		06 Nov 2024	4, 10:20 PM
CEDGE-Greenwich		HE-CSR-206		GigabitEthernet2 HE-CSR-207								
 Barcelona 		CEDGE-Greenwich		GigabitEthernet3 HE-CSR-207								

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

≡ LiveAction	NX	
Settings		
Q Search		ß
Configuration	~	
Dashboards	~	
Data Source Management		
Data Store Management	~	
Default Login Method		
Email Configuration		
Entity Page Reports	~	
External Authentication	~	
Integrations	~	
Licensing	^	

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

Notable functionality

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

Unlimited Dashboards

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

Use Case

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

Functionality and Limitations

Functionality

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

Limitations

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

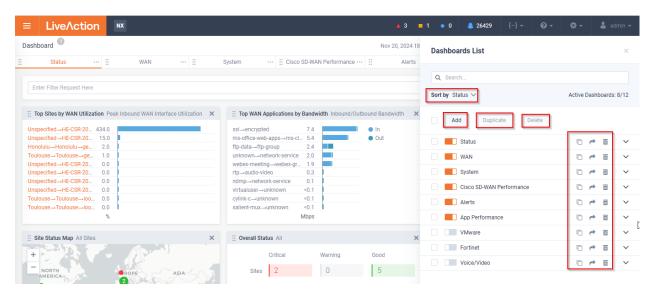
Accessing Dashboards List

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

	Live/Action	NX								1	• 0	26429				
Dashb	oard							Nov 20	, 2024 1	8:00:00	→ Nov	20, 2024 18:15:00	Dasht	oards List	Add Wi	lget 🖉
	Status	8	WAN ···	8	System	E Cisco SD-W	AN Performance ···	8	Alerts			: App Perfo	mance	··· 8	Web	
Ent	ter Filter Request Here															Apply filter
·		m. Deale taken	and MIAN Interface Litilia	ation M	11 The Middle Area I	ontione by Dand										
:: 10	op Sites by WAN Utilizatio	n Peak Indou	and wain interface offic	auon 🔨	:: TOP WAN APPI	Cations by band	width Inbound/Out	ound Bandwic	dth 🗙		Тор	nterfaces % Chan	ged - Interfa	ce Burstable F	Rate	×

Dashboard List Functionality

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



Caveat

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

SSO Static Group Assignment

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

Static SAML Group Assignment

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

		New Features! 🔺 287 🔳 23 🔹 177 🌲 14595 🧮
Settings		
Q, single		
External Authentication	SINGLE SIGN ON Enabled	
Single Sign On	SAML ADFS	
	Entity ID *)	Identity Provider SSO URL *
	LIVE_NX 🖸	
	Host Name *	Identity Provider Entity ID / Issuer * 🚯
	10.2.101.169	
	Consumer Login URL 🚯	Certificate *
	https://10.2.101.169/auth/saml/login	
	Consumer Logout URL 🚯	
	https://10.2.101.169/auth/saml/logout	
	Group Assignment	
	Dynamic O Static	
	LiveNX Group * 📵	
	ßelect LiveNX group	
	Admin	
	Config View	Save
	adfa	
	news	
	nothing somepower	
	test	

Edge Case

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

😳 LiveNX	
User group is not defined. A group must be set by an admin.	
Single Sign On	
OR	
Login and Password Authentication 🗸 🗸	
Username	
Password	
Login	
By clicking "Login", I agree to the terms of LiveAction's EULA	
First time user information	

Alert Root Cause Analysis

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

Supported Alerts for Root Cause Analysis

In LiveNX 24.3.0, we are targeting application performance alerts.

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

Configuration

Steps to enable and setup Alert Root Cause Analysis.

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

Eive∧ction	x
Settings	
Q Search	
figuration	×
ards	×
Management	~
fanagement n Method	Ť
on	
s	~
ion	~
	~
	^
n	
tification	
	~
Configuration	^
ADM	_
Configuration PREMEW	
	_
erties	~
rts	_
	×

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

LIST OF INSTANCES 🚯	ADD NEW INSTANCE	INSTANCE DETAILS		
1. New Alert		> 15	min Manual	Time U
Default Instance		- 15	Manua	
		O Static 🔵 Dynar	nic 🕜 Static and Dynamic 🔷 Static or	Dynamic
		CRITICAL A	Average Application Delay *	
			>= 500	ms
			Average Application Delay *	
		VARNING	>= 400	ms
			Average Application Delay *	
		INFO •	>= 100	ms
		AI Diagnostics		
			stic useful for correlating various alerts toget ms on the network. Information can be queried	
		potential remediat	is tion will be gathered to provide guidance on th on. A synopsis will be added to alerts when av pact system performance and should be enat	ailable. This level of
		Sharing		
		Email		
		Type Email		

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

Workflow

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

	LiveNX Ali	erts							
				LIST OF INSTANCES ()	ADD NEW INSTANCE	INSTANCE DETAILS			
Enable Disable				1. New Alert	• •••	> 0	min Manual	· · · · · · · · · · · · · · · · · · ·	
ALERT TYPE	ENABLED	AFFECT STATUS	CATEGORY	Default Instance					
> Application Bandwidth	~	~	Application						
> Application Performance - App Delay	~	~	Application			CRITICAL 🔺	Delay Time *		
> Application Performance - Network Delay	~	~	Application				>= 4		
> BGP Peer Connection Change	~	~	Network				Delay Time *		
Cisco IWAN Path Change	~	~	Network			WARNING =	>= 2	ms	
Cisco IWAN Threshold Crossing	~	~	Network						
> Cisco SD-WAN Performance - Jitter	~	~	Network				Delay Time *		
> Cisco SD-WAN Performance - Network Delay	~	~	Network			INFO 🔹	>= 0	ms	
> Cisco SD-WAN Performance - Packet Loss	~	~	Network						
> Cisco SD-WAN SLA Class Path Change	~	~	Network			AI Diagnostics			
Cisco SD-WAN VManage Connectivity	~		System			Al Diagnostics			
Critical Traffic Response Time	~	~	Application			Basic Analysis A high level diagon	ostic useful for correlating various alerts togeth	er to better	
> Device CPU Utilization	~	~	Device, Interface				ms on the network. Information can be queried		
> Device Flow Stop	~	~	Device, Interface						
> Device Memory Utilization	~	~	Device, Interface			Root Cause Analysis Additional information will be gathered to provide guidance on the root cause and			
> Device Reachability	~	~	Device, Interface				potential remediation. A synopsis will be added to alerts when available. This level of diagnostics can impact system performance and should be enabled sparingly.		
EIGRP Neighbor Count Decrease	~	~	Network						
> EIGRP Neighbor Count Increase	~	~	Network			Sharing			
> Fan Tray Operational State	~	~	Device, Interface			Email			
> Fortinet Performance SLA - Jitter	~	~	Network			Type Email			
> Fortinet Performance SLA - Network Delay	~	~	Network						
> Fortinet Performance SLA - Packet Loss	~	~	Network						
> High WAN Interface Utilization	~	~	Device. Interface					Cancel	

Notable details about alert configuration

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

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

Viewing Root Cause Analysis

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

Root Cause Analysis Pending

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

 Application Performance 	rmance - App Delay ×
Status & Time	
Status:	Active ~
Time opened:	09 Nov 2024, 04:15 PM
Active for:	2 minutes
Source Info	
Site:	CSR
Device:	HE-CSR-208
Conversation:	TCP 48.10.0.11:443 to 66.1.0.11
Server Site:	Internet
Client Site:	Internet
Event:	Report
Description	
HE-CSR-208 had 0.00 ms	s application delay for the application youtube
Details	
Application Name:	youtube
Initial Average Application Flow Delay:	0.00 ms
Latest Average Application Flow Delay:	0.00 ms
Configured Threshold:	0.00 ms
Al Analysis Levels:	Basic Analysis, Root Cause Analysis
AI Diagnostics	
Summary:	Root cause analysis in progress Please check back later for the results.
Notes	
Notes	
	Save

Root Cause Analysis Complete

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

Status & Time Status: Active Time opened: 12 Nov 2024, 07:11 PM Active for: 1 day Source Info Source Info Site: San Jose Device: Media Conversation: UDP 192.168.2.202:49991 to 10.2.101.141:5004 Source Site: Unspecified Destination Site: Unspecified Destination Site: Unspecified Description Media running application rtp-video had voice/video traffic with 15.17 ms max jitter Details 0.00 % Latest Packet Loss: 0.00 % Application: rtp-video Packet Loss Threshold: 1.00 ms Initial Jitter Max: 15.17 ms Latest Jitter Max: 15.62 ms Al Analysis Levels: Basic Analysis, Root Cause Analysis Summary: Analysis of the network path reveals significant packet loss and potential quality issues for media traffic. Issues: S issues detected Notes Notes	Voice, Video appli	cations performance ×
Time opened: 12 Nov 2024, 07:11 PM Active for: 1 day Source Info Site: Site: San Jose Device: Media Conversation: UDP 192.168.2.202:49991 to 10.2.101.141:5004 Source Site: Unspecified Description Media running application rtp-video had voice/video traffic with 15.17 ms max jitter Details Initial Packet Loss: 0.00 % Latest Packet Loss: 0.00 % Latest Packet Loss: 0.00 % Application: rtp-video Packet Loss Threshold: 1.00 % Jitter Max Threshold: 1.00 % Initial Jitter Max: 15.17 ms Latest Jitter Max: 15.62 ms Al Analysis Levels: Basic Analysis, Root Cause Analysis Al Diagnostics Analysis of the network path reveals significant packet loss and potential quality issues for media traffic. Issues: 5 issues detected Notes 5	Status & Time	
Active for:1 daySource InfoSite:San JoseDevice:MediaConversation:UDP 192.168.2.202:49991 to 10.2.101.141:5004Source Site:UnspecifiedDestination Site:UnspecifiedDescriptionMedia running application rtp-video had voice/video traffic with 15.17 ms max jitterDetailsInitial Packet Loss:0.00 %Initial Packet Loss:0.00 %Application:rtp-videoPacket Loss Threshold:1.00 %Jitter Max:15.17 msLatest Jitter Max:15.62 msAl Analysis Levels:Basic Analysis, Root Cause AnalysisAl DiagnosticsAnalysis of the network path reveals significant packet loss and potential quality issues for media traffic.Issues:S issues detectedNotesIssues:	Status:	Active \checkmark
Source Info Site: San Jose Device: Media Conversation: UDP 192.168.2.202:49991 to 10.2.101.141:5004 Source Site: Unspecified Destination Site: Unspecified Description Media running application rtp-video had voice/video traffic with 15.17 ms max jitter Details Initial Packet Loss: 0.00 % Latest Packet Loss: 0.00 % Application: rtp-video Packet Loss Threshold: 1.00 % Jitter Max Threshold: 1.00 ms Initial Jitter Max: 15.17 ms Latest Jitter Max: 15.62 ms Al Analysis Levels: Basic Analysis, Root Cause Analysis AI Analysis Levels: Basic Analysis of the network path reveals significant packet loss and potential quality issues for media traffic. Issues: 5 issues detected Notes Summary:	Time opened:	12 Nov 2024, 07:11 PM
Site: San Jose Device: Media Conversation: UDP 192.168.2.202:49991 to 10.2.101.141:5004 Source Site: Unspecified Description Media running application rtp-video had voice/video traffic with 15.17 ms max jitter Details Initial Packet Loss: 0.00 % Initial Packet Loss: 0.00 % Application: rtp-video Packet Loss Threshold: 1.00 % Jitter Max Threshold: 1.00 ms Initial Jitter Max: 15.17 ms Latest Jitter Max: 15.62 ms Al Analysis Levels: Basic Analysis, Root Cause Analysis Al Diagnostics Analysis of the network path reveals significant packet loss and potential quality issues for media traffic. Issues: 5 issues detected Notes Summary:	Active for:	1 day
Device: Media Conversation: UDP 192.168.2.202:49991 to 10.2.101.141:5004 Source Site: Unspecified Destination Site: Unspecified Description Media running application rtp-video had voice/video traffic with 15.17 ms max jitter Details Initial Packet Loss: 0.00 % Initial Packet Loss: 0.00 % Application: rtp-video Packet Loss Threshold: 1.00 % Jitter Max Threshold: 1.00 ms Initial Jitter Max: 15.17 ms Latest Jitter Max: 15.62 ms Al Analysis Levels: Basic Analysis, Root Cause Analysis Al Diagnostics Analysis of the network path reveals significant packet loss and potential quality issues for media traffic. Issues: 5 issues detected Notes Summary:	Source Info	
Conversation:UDP 192.168.2.202:49991 to 10.2.101.141:5004Source Site:UnspecifiedDestination Site:UnspecifiedDescriptionMedia running application rtp-video had voice/video traffic with 15.17 ms max jitterDetailsInitial Packet Loss:0.00 %Initial Packet Loss:0.00 %Latest Packet Loss:0.00 %Application:rtp-videoPacket Loss Threshold:1.00 %Jitter Max Threshold:1.00 msInitial Jitter Max:15.17 msLatest Jitter Max:15.62 msAl Analysis Levels:Basic Analysis, Root Cause AnalysisAl DiagnosticsAnalysis of the network path reveals significant packet loss and potential quality issues for media traffic.Issues:5 issues detectedNotesIssues:	Site:	San Jose
Source Site:UnspecifiedDestination Site:UnspecifiedDescriptionMedia running application rtp-video had voice/video traffic with 15.17 ms max jitterDetailsInitial Packet Loss:0.00 %Initial Packet Loss:0.00 %Application:rtp-videoPacket Loss Threshold:1.00 %Jitter Max Threshold:1.00 msInitial Jitter Max:15.17 msLatest Jitter Max:15.62 msAI Analysis Levels:Basic Analysis, Root Cause AnalysisAI DiagnosticsAnalysis of the network path reveals significant packet loss and potential quality issues for media traffic.Issues:5 issues detected	Device:	Media
Destination Site: Unspecified Description Media running application rtp-video had voice/video traffic with 15.17 ms max jitter Details Initial Packet Loss: 0.00 % Latest Packet Loss: 0.00 % Application: rtp-video Packet Loss Threshold: 1.00 % Jitter Max Threshold: 1.00 ms Initial Jitter Max: 15.17 ms Latest Jitter Max: 15.62 ms Al Analysis Levels: Basic Analysis, Root Cause Analysis Al Diagnostics Analysis of the network path reveals significant packet loss and potential quality issues for media traffic. Issues: 5 issues detected Notes Summary: 5 issues detected	Conversation:	UDP 192.168.2.202:49991 to 10.2.101.141:5004
Description Media running application rtp-video had voice/video traffic with 15.17 ms max jitter Details Initial Packet Loss: 0.00 % Latest Packet Loss: 0.00 % Application: rtp-video Packet Loss Threshold: 1.00 % Jitter Max Threshold: 1.00 ms Initial Jitter Max: 15.17 ms Latest Jitter Max: 15.62 ms Al Analysis Levels: Basic Analysis, Root Cause Analysis Al Diagnostics Analysis of the network path reveals significant packet loss and potential quality issues for media traffic. Issues: 5 issues detected Notes Summary:	Source Site:	Unspecified
Media running application rtp-video had voice/video traffic with 15.17 ms max jitter Details Initial Packet Loss: 0.00 % Latest Packet Loss: 0.00 % Application: rtp-video Packet Loss Threshold: 1.00 % Jitter Max Threshold: 1.00 ms Initial Jitter Max: 15.17 ms Latest Jitter Max: 15.62 ms Al Analysis Levels: Basic Analysis, Root Cause Analysis Al Diagnostics Analysis of the network path reveals significant packet loss and potential quality issues for media traffic. Issues: 5 issues detected Notes Summary:	Destination Site:	Unspecified
Media running application rtp-video had voice/video traffic with 15.17 ms max jitter Details Initial Packet Loss: 0.00 % Latest Packet Loss: 0.00 % Application: rtp-video Packet Loss Threshold: 1.00 % Jitter Max Threshold: 1.00 ms Initial Jitter Max: 15.17 ms Latest Jitter Max: 15.62 ms Al Analysis Levels: Basic Analysis, Root Cause Analysis Al Diagnostics Analysis of the network path reveals significant packet loss and potential quality issues for media traffic. Issues: 5 issues detected Notes Summary:	Description	
Initial Packet Loss: 0.00 % Latest Packet Loss: 0.00 % Application: rtp-video Packet Loss Threshold: 1.00 % Jitter Max Threshold: 1.00 ms Initial Jitter Max: 15.17 ms Latest Jitter Max: 15.62 ms Al Analysis Levels: Basic Analysis, Root Cause Analysis Al Diagnostics Analysis of the network path reveals significant packet loss and potential quality issues for media traffic. Issues: 5 issues detected Notes Initial Statest	Media running applicatio	n rtp-video had voice/video traffic with 15.17 ms max
Latest Packet Loss:0.00 %Application:rtp-videoPacket Loss Threshold:1.00 %Jitter Max Threshold:1.00 msInitial Jitter Max:15.17 msLatest Jitter Max:15.62 msAl Analysis Levels:Basic Analysis, Root Cause AnalysisAl DiagnosticsAnalysis of the network path reveals significant packet loss and potential quality issues for media traffic.Summary:5 issues detectedNotes	Details	
Application:rtp-videoPacket Loss Threshold:1.00 %Jitter Max Threshold:1.00 msInitial Jitter Max:15.17 msLatest Jitter Max:15.62 msAl Analysis Levels:Basic Analysis, Root Cause AnalysisAl DiagnosticsAnalysis of the network path reveals significant packet loss and potential quality issues for media traffic.Summary:5 issues detectedNotes	Initial Packet Loss:	0.00 %
Packet Loss Threshold: 1.00 % Jitter Max Threshold: 1.00 ms Initial Jitter Max: 15.17 ms Latest Jitter Max: 15.62 ms AI Analysis Levels: Basic Analysis, Root Cause Analysis AI Diagnostics Analysis of the network path reveals significant packet loss and potential quality issues for media traffic. Issues: 5 issues detected	Latest Packet Loss:	0.00 %
Jitter Max Threshold: 1.00 ms Initial Jitter Max: 15.17 ms Latest Jitter Max: 15.62 ms Al Analysis Levels: Basic Analysis, Root Cause Analysis Al Diagnostics Analysis of the network path reveals significant packet loss and potential quality issues for media traffic. Issues: 5 issues detected	Application:	rtp-video
Initial Jitter Max: 15.17 ms Latest Jitter Max: 15.62 ms AI Analysis Levels: Basic Analysis, Root Cause Analysis AI Diagnostics Analysis of the network path reveals significant packet loss and potential quality issues for media traffic. Issues: 5 issues detected Notes	Packet Loss Threshold:	1.00 %
Latest Jitter Max: 15.62 ms AI Analysis Levels: Basic Analysis, Root Cause Analysis AI Diagnostics Analysis of the network path reveals significant packet loss and potential quality issues for media traffic. Issues: 5 issues detected Notes	Jitter Max Threshold:	1.00 ms
AI Analysis Levels: Basic Analysis, Root Cause Analysis AI Diagnostics Analysis of the network path reveals significant packet loss and potential quality issues for media traffic. Issues: 5 issues detected Notes	Initial Jitter Max:	15.17 ms
AI Diagnostics Analysis of the network path reveals significant packet loss and potential quality issues for media traffic. Issues: 5 issues detected Notes	Latest Jitter Max:	15.62 ms
Analysis of the network path reveals significant Summary: packet loss and potential quality issues for media traffic. Issues: 5 issues detected Notes	Al Analysis Levels:	Basic Analysis, Root Cause Analysis
Summary: packet loss and potential quality issues for media traffic. Issues: 5 issues detected Notes	AI Diagnostics	
Notes	Summary:	packet loss and potential quality issues for media
	Issues:	5 issues detected
Notes	Notes	
	Notes	

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

Recommendation: Enable collection of these metrics to get a more comprehensive view of media quality and end-to-end performance.

Additional Column Filter

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

=	Live/\ct		V			New Features!	▲ 282 ■ 25 •	• 181 🌲 14612 🖷	{-} -	0- ¢	8- 8	admin ·
Alerts	Enter Filter	Request Here								Apply filter	Configur	re Alerts
				Active				History				
Res	olve Ignore	Acknowledge	Refresh Alerts Vi	ew Options 🕤				Q Search				
	SEVERITY 0	SITE O	DEVICE 0	DESCRIPTION	TIME OPENED	ACTIVE FOR	CATEGORY	TYPE	0	THIRD PARTY 🗘	AI DIAGNO	с _па
	All ~	Site	Device	Description		All 🗸	All ~	All	~	Third Party I	μı	~
	A Critical	LiveAction	MICRO-CSR-15.sd.live	MICRO-CSR-15.sd.liveaction.com. had 511.22 ms application delay for the application cdn.vimeo.tv	12 Nov 2024, 11:37 PM	less than a mi	Application	Application Performance - App Dela	y .			
	Info	LiveAction	MICRO-CSR-15.sd.live	MICR0-CSR-15.sd.liveaction.com. had 124.00 ms application delay for the application ts01-b.clou	12 Nov 2024, 11:33 PM	3 minutes	Application	Application Performance - App Dela	W.			
	Info	LiveAction	MICRO-CSR-15.sd.live	MICR0-CSR-15.sd.liveaction.com. had 113.38 ms network delay for the application tidalty	12 Nov 2024, 10:27 PM	about 1 hour	Application	Application Performance - Network	Delay		~	,
	Info	Heaven	ASR1001.liveaction.co	Tunnel1 on ASR1001.liveaction.com was over utilized at 109.22% in the Outbound direction.	12 Nov 2024, 08:17 PM	about 3 hours	Device, Interface	High WAN Interface Utilization				
	Critical	PaloAlto	PaloAlto	PaloAlto to MoscowVedge1 on mpls: 0 % of packet loss (1.1.9.4 to 1.1.2.4)	12 Nov 2024, 06:16 PM	about 5 hours	Network	Cisco SD-WAN Performance - Packe	et Loss			
	Info	LiveAction	MICRO-CSR-15.sd.live	MICRO-CSR-15.sd.liveaction.com. had 150.33 ms application delay for the application cdn3.wowza	12 Nov 2024, 05:41 PM	about 6 hours	Application	Application Performance - App Dela	y .			
	Critical	PaloAlto	PaloAlto	PaloAlto to MoscowVedge1 on mpls: 0 % of packet loss (1.1.9.4 to 111.111.111.6)	12 Nov 2024, 05:23 PM	about 6 hours	Network	Cisco SD-WAN Performance - Packe	et Loss			
	Info	Toulouse	Toulouse	Toulouse to Barcelona on mpls: 0 ms of jitter (1.1.20.4 to 1.1.4.4)	12 Nov 2024, 03:04 PM	about 9 hours	Network	Cisco SD-WAN Performance - Jitter				
	Critical	LiveAction	MICRO-CSR-15.sd.live	MICRO-CSR-15.sd.liveaction.com. had 109.57 ms network delay for the application us tvsquared	12 Nov 2024, 02:23 PM	about 9 hours	Application	Application Performance - Network	Delay		~	,
	Info	PaloAlto	PaloAlto	PaloAlto to Toulouse on mpls: 0 ms of jitter (1.1.9.4 to 2.2.20.4)	12 Nov 2024, 01:40 PM	about 10 hours	Network	Cisco SD-WAN Performance - Jitter				
	Critical	LiveAction	MICRO-CSR-15.sd.live	MICR0-CSR-15.sd.liveaction.com. had 112.63 ms network delay for the application granicus	12 Nov 2024, 01:21 PM	about 10 hours	Application	Application Performance - Network	Delay		~	1
	Critical	PaloAlto	PaloAlto	PaloAlto to MoscowVedge1 on private1: 0 % of packet loss (1.1.10.4 to 111.111.111.10)	12 Nov 2024, 01:10 PM	about 10 hours	Network	Cisco SD-WAN Performance - Packe	et Loss			
	Critical	LiveAction	MICRO-CSR-15.sd.live	MICR0-CSR-15.sd.liveaction.com. had 121.57 ms network delay for the application a47b	12 Nov 2024, 11:26 AM	about 12 hours	Application	Application Performance - Network	Delay		~	1
	Info	LiveAction	MICRO-CSR-15.sd.live	MICRO-CSR-15.sd.liveaction.com. had 67.77 ms network delay for the application event.prod.bidr.io	12 Nov 2024, 11:18 AM	about 12 hours	Application	Application Performance - Network	Delay		~	1
	Critical	LiveAction	MICRO-CSR-15.sd.live	MICR0-CSR-15.sd.liveaction.com. had 67.33 ms network delay for the application segment.prod.b	12 Nov 2024, 11:18 AM	about 12 hours	Application	Application Performance - Network	Delay		~	·
	 Info 	LiveAction	MICRO-CSR-15.sd.live	MICRO-CSR-15.sd.liveaction.com. had 117.60 ms network delay for the application nbcuas	12 Nov 2024, 11:17 AM	about 12 hours	Application	Application Performance - Network	Delay		~	1
	 Info 	LiveAction	MICRO-CSR-15.sd.live	MICR0-CSR-15.sd.liveaction.com. had 337.00 ms application delay for the application buffer-com	12 Nov 2024, 11:13 AM	about 12 hours	Application	Application Performance - App Delay	a de la companya de l			
	Critical	LiveAction	MICRO-CSR-15.sd.live	MICRO-CSR-15.sd.liveaction.com. had 194.60 ms network delay for the application adx.opera	12 Nov 2024, 11:12 AM	about 12 hours	Application	Application Performance - Network	Delay		~	·
	Critical	LiveAction	MICRO-CSR-15.sd.live	MICRO-CSR-15.sd.liveaction.com. had 73.00 ms network delay for the application pulseinsights	12 Nov 2024, 11:10 AM	about 12 hours	Application	Application Performance - Network	Delay		~	·
	Critical	LiveAction	MICRO-CSR-15.sd.live	MICRO-CSR-15.sd.liveaction.com. had 119.25 ms network delay for the application events.launch	12 Nov 2024, 11:10 AM	about 12 hours	Application	Application Performance - Network	Delay		~	·
	Critical	LiveAction	MICRO-CSR-15.sd.live	MICRO-CSR-15.sd.liveaction.com. had 104.86 ms network delay for the application bs.serving-sys	12 Nov 2024, 11:10 AM	about 12 hours	Application	Application Performance - Network	Delay		~	·
	Info	LiveAction	MICRO-CSR-15.sd.live	MICRO-CSR-15.sd.liveaction.com. had 12.96 ms network delay for the application map.mp.nbc	12 Nov 2024, 11:10 AM	about 12 hours	Application	Application Performance - Network	Delay		~	·
	 Info 	LiveAction	MICRO-CSR-15.sd.live	MICRO-CSR-15.sd.liveaction.com. had 6.71 ms network delay for the application identity.mparticle	12 Nov 2024, 11:10 AM	about 12 hours	Application	Application Performance - Network	Delay		, v	,

Technical details

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

Advanced Configuration

This section is for fine tuning systems experiencing problems.

Connection Timeouts

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

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

Polling Interval

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

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

LiveNX Security Dashboard

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

Prerequisites

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

Steps To Configure Security Dashboard

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

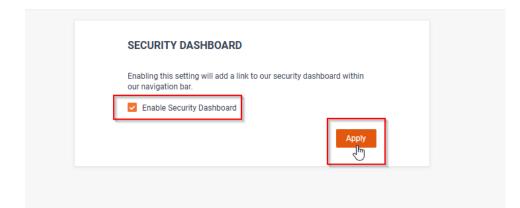
1. From LiveNX Web, select gear icon available on navigation bar and then select settings menu.

	Live/Action	NX				New Features!	•	2 • 0	26725 🌲			۰	
Overv	iew Enter Filter Reque	est Here										Settings	Settings
Site	s, Devices, Interfaces by Stat	uses					Active	Alerts				System D	Diagnostics
s	TES: 7		DEVICES: 16		INTERFACES: 145		ALER	-	et3 on HE-CSR-20	06 had a drop	rate of	User Man	nagement
							■ D	rop Rate wa	s 193976.00 Kbp	s for HE-CSR-		LiveNX S	
	RITES 🗗	0		0	INTERFACES 🗹	0	▲ C	EDGE-Green	wich could not be	e reached.		06 Nov 2024	4, 10:20 PM
	CEDGE-Greenwich		CEDGE-Greenwich		 GirabitEthernet0ICI 	EDGE-Greenwich							

2. On the Settings page, find and select "Security Dashboard" option.

Settings		
Q Search		
License Expiration Notification		
Mounted Data	~	
Network Intelligence Configuration	~	
Nodes		
Properties	~	
Ргоху		
Reports	~	
Security	~	
Security Dashboard		
SNMP Trap		
Syslog		
Troubleshooting	~	
Updates		

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



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

≡ Liv	eAction	NX Security Dashboard		New Features!	▲ 13 ■ 1	• 0	29620 🌲			💄 admin 🗸
Overview	Enter Filter Request H	Here	G-						Apply filter	

5. Click the **Security Dashboard** button to access the Security Dashboard.

<u> </u>															
Home > Dashboards > A	Analytics > Security Find														
Top Security Findings by Type					Top Security Finding	s by Indicator					Top Security Find	lings by Rule ID			
			Hissing 3N Hosscurk/wak cipher Hosscure/Wak cipher Hossai certificate Self Styred Cert Accrosola Prips Valar BOP Connection After Bin New Encorpoints Sincle Unsepacial Encorpoint Chrosystein Cert Valares ISK baser ann How Encorpoint Walan Valares ISK baser ann How Encorpoint Walan Valares IS 25% baser ann New Encorpoint Walan Valares IS 25% baser ann New Text Sin Valares	te Force Attempt signed Port nal					9.0 209 4130 09 2.76 06 1 4 4 4 4 4 4 6dge,jivewire-10.4 6dge,jivewire-10.4					e dal tis.9 - tis.9 - valu - valu - otal - ot	900 901 90 200 200 300 600 500 500 100 101 700 100
Security Findings (# findings) 45 40 35 30 25															
20	00:00 09/12 08:00 09/12	12.00 09/12 18:00 09	13 00.00 09/13 06:00 09/13 12:0	0 09/13 18:00 09/1	4 00:00 09/14 06:00 09/14	12:00 09/14 18:00 0	a/15 00:00 09/15 0	e.00 09/15 12:00 0	ia/15 18:00 09/16	00.00 09/16 06:00	09/16 12:00 09/16 18:0	00 09/17 00:00 08/17 06	600 09/17 12:00 09/17 18:		/18 06:00
Top 1000 Security Findings															
time	event_type	source	flowid		daddr	sport	dport pro			type		core indicator	description	category	
2024-09-18 02:59:35	finding	livewire	360287970190684300		239.255.255.250	63782	1900 ud		-18 02:46:12	policy		8 10.1.6.206	Anomalous IP hop		н
2024-09-18 02:46:25	finding	livewire	360287970190684300		239.255.255.250	63782	1900 ud		-18 02:46:06	policy		8 10.1.6.206	Anomalous IP hop		н
2024-09-17 15:41:35	finding	livewire	432345564228611000		192.168.54.130	49159	3389 tcp		-17 15:39:48	policy		8 192.168.54.129	Anomalous IP hop		
2024-09-17 23:48:55	finding	livewire	360287970190683900		239.255.255.250	63782	1900 ud		-17 23:35:30	policy		8 10.1.6.206	Anomalous IP hop		н
2024-09-17 23:35:45	finding	livewire	360287970190683900	10.1.6.206	239.255.255.250	63782	1900 ud	p 2024-09	-17 23:35:24	policy		8 10.1.6.206	Anomalous IP hop	anomalous_ttl	н
2024-09-17 20:38:15	finding	livewire	360287970190683460		239.255.255.250	63782	1900 ud		-17 20:24:49	policy		8 10.1.6.206	Anomalous IP hop		

Grafana Dashboards

Overview

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

Dashboard

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

Security

Firewall Changes

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

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

Encryption and Authorization

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

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

Simplified Interface Deletion

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

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

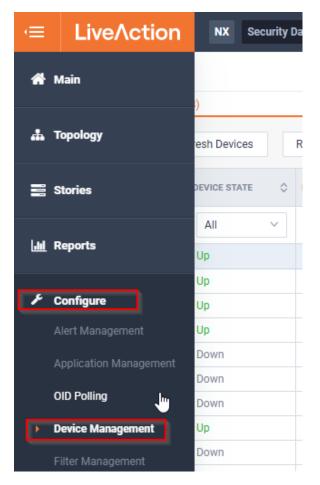
Removing Interfaces

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

From My Devices Page

To Remove the Interfaces please follow the steps below.

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



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

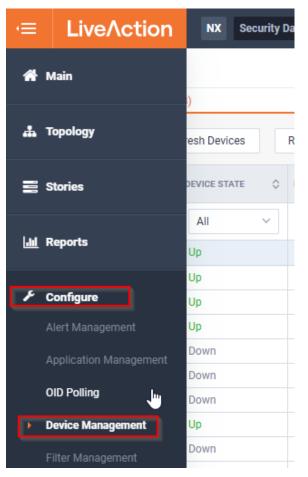
≡	LiveAction	NX Security Da
Devic	e Management	
	My Devices	(18)
Edit	Delete	Refresh Devices R
	DEVICE	DEVICE STATE
	Device	All ~
	CSR-Toul-Red 🕺	Up
	CEDGENEW 🔀	Up
	TechSupport-310 🔀	Up
	Toulouse 🔀	Up
	HE-CSR-207	Down
	vbond 🔀	Down
	CEDGE-Greenwich 🔀	Down
	CEDGENEW 🕺	Up
	vmanage 🔀	Down

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

		General Se	ttings					Inte	rfaces			
ld	Edit Dele	te				Q Search						
	NAME 🗘	SNMP INTE 🗘	IFINDEX 🗘	IP ADDR 🗘	SUBNET 🗘	INPUT C 🗘	OUTPUT 💲	SERVICE 🗘	WAN/XC 💲	LABEL 🗘	TAGS	٥
	Name	All V	Ifindex	IP Addre	Subnet	Input Ca	Output (Service	A ~	Label	Tags	
	GigabitEthernet1	~	1]						
	GigabitEthernet2	~	2					Default S	WAN			
	GigabitEthernet3	~	3									
	GigabitEthernet3.10	~	6					Default S	WAN			
	GigabitEthernet3.20	~	7					Default S	WAN			
	NullO	~	5									
	VoIP-Null0	~	4									
	5											

From My Interfaces Page

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



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

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

evic	e Management					CSV Import/Expo
	My Devices (18)		My Interfaces (155)		
Edit	Delete					
	NAME \$	INTERFACE STATE	DEVICE \$	DEVICE STATE	SITE 🗘	SERVICE PR 🗘
-	Name	All ~	Device	All ~	Site	Service Pro
~	GigabitEthernet1	qL	CSR-Toul-Red	Up	MoscowVed	
	GigabitEthernet2	Up	CSR-Toul-Red	Up	MoscowVed	Default Servi
	GigabitEthernet3	Up	CSR-Toul-Red	Up	MoscowVed	
	GigabitEthernet3.10	Up	CSR-Toul-Red	Up	MoscowVed	Default Servi
	GigabitEthernet3.20	Up	CSR-Toul-Red	Up	MoscowVed	Default Servi
	NullO	Up	CSR-Toul-Red	Up	MoscowVed	
	VoIP-Null0	Up	CSR-Toul-Red	Up	MoscowVed	
	eth0	Un	TechSunnort-31	Un		

Dynamic Alert Thresholds

Overview

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

Alerts Supported as of 24.3.0

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

Configuration

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

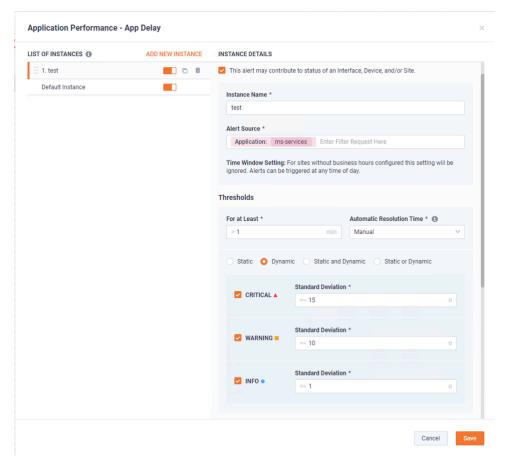
Static

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

ST OF INSTANCES	ADD NEW INSTANCE	INSTANCE DETAILS		
1. test		This alert may contrib	oute to status of an Interface, Device, an	d/or Site.
Default Instance		Instance Name *		
		test		
		Alert Source *		
		Application: ms-s	services Enter Filter Request Here	
			For sites without business hours config triggered at any time of day.	jured this setting will be
		Thresholds		
		For at Least *	Automatic Res	olution Time * 📵
		> 1	min Manual	~
		 Static Dynar CRITICAL A 	mic Static and Dynamic St Average Application Delay * >= 500	atic or Dynamic
			Average Application Delay *	
		VARNING =	>= 400	ms
			Average Application Delay *	
		V INFO •	>= 0	ms

Dynamic

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



Static and Dynamic

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

ST OF INSTANCES ()	ADD NEW INSTANCE	INSTANCE DETAILS			
1. test		This alert may contrib	ute to status of an Inter	face, Device, and,	/or Site.
Default Instance		Instance Name *			
		test			
		Alert Source *			
		Application: ms-s	services Enter Filter	Request Here	
			For sites without busine triggered at any time of		red this setting will be
		Thresholds			
		For at Least *		Automatic Resolu	ution Time * 🚯
		> 1	min	Manual	~
		🔿 Static 🔷 Dynar	nic 🔘 Static and Dy	namic 🔵 Stat	ic or Dynamic
		CRITICAL 🔺	Average Application	AND	Standard Deviation *
			>= 500	ms	>= 15 0
			Average Application		Standard Deviation *
		VARNING =	>= 400	ms	>= 10 0
		INFO •	Average Application		Standard Deviation *
			>= 0	ms	>= 1 σ

Static or Dynamic

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

ST OF INSTANCES	ADD NEW INSTANCE	INSTANCE DETAILS					
1. test		This alert may contrib	oute to status of an Interface, De	vice, and	d/or Site.		
Default Instance		Instance Name *					
		test					
		Alert Source *					
		Application: ms-services Enter Filter Request Here					
			For sites without business hour triggered at any time of day.	s config	ured this setting will be		
		Thresholds					
		For at Least *	Automa	tic Reso	lution Time * 🚯		
		> 1	min Manu:	al	~		
		Static Dynar	mic Static and Dynamic Average Application Delay * >= 500 ms	-	standard Deviation * >= 15 σ		
		Varning =			Standard Deviation *		
		WARNING -	>= 400 ms	OR	>= 10 0		
		V INFO •	Average Application Delay * >= 0 ms	OR	Standard Deviation *		

Implementation Details

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

Caveats

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

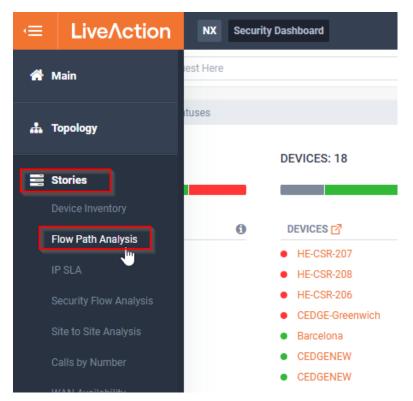
Device Model on Flow Path Analysis

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

Step To Get Flow Path Analysis

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

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



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

low Path A	nalysis	Site: = V 6 values	Enter Fil	ter Request He	re					∢> A ^Q _{PP} ly fil	ter Nov 2	5, 2024 17:10:0	00 → Nov 25, 2	024 17:15:00	5 Mins V
		Basic				Voice/Video	Performance					Applicatio	n Performance		
											Q Search	.			
LIVEWI 🗘	FLOW P 🗘	TIME 🗘	PROTOC 🗘	SRC IP	SRC SITE	SRC PORT 🗘	DST IP	DST SITE 🗘	DST PORT 🗘	DSCP 🗘	APPLIC 🗘	DIRECTI 🗘	TOTAL F 🗘	TOTAL B 🗘	TOTAL P
		Time	Protocc	Src IP	Src Site	Src Por	Dst IP	Dst Site	Dst Por	DSCP	Applica	Directio	Total FI	Total B ₁	Total F
=	ď	25 Nov 2024, 05:15 PM	TCP	172.26.4	Unknown	13797	172.27.4	Unknown	54605	46 (EF)	ftp-data	Unknown	1	45.2 MB	32,0
=	ď	25 Nov 2024, 05:15 PM	TCP	172.26.4	Unknown	42864	172.27.4	Unknown	47039	46 (EF)	ftp-data	Unknown	1	45.19 MB	32,0
-	-7		700	470.04.4		00070	470.07.4		04070	10 (PP)				15 10 100	

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

LIVEWI 🗘	FLOW P 🗘	TIME \$	PROTOC 🗘	SRC IP	SRC SITE 🗘	SRC PORT 🗘	DST IP
		Time	Protocc	Src IP	Src Site	Src Por	Dst IP
=	ď	25 Nov 2024, 05:15 PM	TCP	172.26.4	Unknown	13797	172.27.4
=	ď	25 Nov 2024, 05:15 PM	TCP	172.26.4	Unknown	42864	172.27.4
		05.11 000.1 05.45 D14	700	470.04.4		00070	470.07.4

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

			Nov 25, 2024 17:15:00 - Nov 25, 2024 17:
PaloAlto	Honolulu	PaloAlto	
th Flow PaloAlto - PaloAlto			
Device Name		Langlulu	DeleAlte
		Honolulu vedaeCloud	PaloAlto
Device Model		Honolulu vedgeCloud Honolulu	PaloAlto vedgeCloud PaloAlto
Device Model Site Name		vedgeCloud	vedgeCloud
Device Model Site Name Application		vedgeCloud Honolulu	vedgeCloud PaloAlto
Device Name Device Model Site Name Application CPU Usage Memory Usage		vedgeCloud Honolulu unknown	vedgeCloud PaloAito unknown

Application Bandwidth Alert

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

Alert

Functionality

This alert supports our standard set of functionality, including:

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

Evaluation

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

Alert Keys

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

- Device
- Interface
- Direction
- Application

Example Alert

 Application Bar 	ndwidth	×
Status & Time		
Status:	Active	~
Time opened:	13 Nov 2024, 09:53 PM	
Active for:	less than a minute	
Source Info		
Site:	LiveAction	
Device:	MICRO-CSR-15.sd.liveaction.com.	
Interface:	GigabitEthernet3	
Application:	imrworldwide	
Event:	Report	

Description

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

Details

Application Name:	imrworldwide
Direction:	Outbound
Initial Application Bandwidth:	33.86 Kbps
Latest Application Bandwidth:	33.86 Kbps
Configured Threshold:	1.00 Kbps
AI Analysis Levels:	Basic Analysis

Notes

Notes		

Example Report Drill Down

port						View Options	Share	Print	Schedule	Сору
plication Ba	ndwidth Alert Event Application (Flow)								
	SR-15 Interface: GigabitEthernet3 Dis 2024 22:22:02 HST (GMT-10:00) Busin				by: BIT_RATE Flex Search: flow.app="imrwor	dwide" Bin Duration: auto Report Data	Source: auto Start T	'ime: Nov 13, 2024 21:	:23:02 HST (GMT-10:00	1)
20									imrworldwide 🛑	
21:25	21:30	21:35 21:40	21:45	21:50 21:55	22:00 22:05	22:10 22	Q Search	22:20 22:23		
gend 🗘	Application \diamondsuit	Total Flows 🗘	Total Bytes	≎ Tota	I Packets ⇔	Average Bit Rate 🛇		Average Packet R	ate 🗘	
	imrworldwide		131	293.76 KB	1,241		0.66 Kbps			0.

Caveats

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