LiveNX 25.1.0 New Features

QUICK GUIDE



Making Bulk Changes in Custom Application and Application Group

In LiveNX 25.1.0 user would be able to make bulk changes in Custom Application and Application Group of LiveNX using the ability of importing and exporting Custom Applications and application Groups in CSV format.

How to Import / Export CSV to Make Changes

- Login to LiveNX Web
- Navigate to Configure and Application Management.



 On Application Management Page, select CSV Import / Export Button. It will give an option to select option between Custom Application and Application Group of LiveNX. Select any one which you want to edit / modify in bulk.



• After importing make the desired changes in csv file and import back using same workflow.



Application Report Percent Bandwidth

Overview

In LiveNX 25.1.0, user can get bandwidth percentage usage by an Application.

Report Execution

This capability is available in Application (Flow) report with FlowStore V1 only. User who wants to check the Application Bandwidth percentage they need to select the FlowStore V1 from Report Data Source.

Name			Applic	ation (Flow)	Fa	st 🗈 🔳	Interfaces			
Enter repo	rt group name		Add N	ew Report		+	All WAN INC	enaces		
							Flex Search	0		
Standard	n Mode		~				Ex.: site=Ho	nolulu & wan & flow.app	>=http	
Standard							Report Data	Source		
ootnote							Auto	_		^
Enter repo	rt group description						Flow Store	1		lba
Time Zone		D	ST 🔁				Flow Store	12		Flow Stor
(GMT+05:3	30) Asia/Calcutta		~				Auto			
							Direction			
									View Schedule	Create Repor
									View Schedule	Create Repor
plication	n, Last Fifteen M	nutes			View	Options ~	Share	Print \$	View Schedule Schedule Copy	Create Repor
plication	n, Last Fifteen M	nutes			View	Options ~	Share	Print S	View Schedule Schedule Copy	Create Repor
plication	n, Last Fifteen M	nutes			View	Options ~	Share	Print \$	View Schedule Schedule Copy	Create Repor
plication plication (n, Last Fifteen M Flow) I Devices Interface:	nutes All WAN Interfacea	Display Filter: No D	isplay Filtering Direction	View	Options v	Share ution Type: times	Print S eries Sort By: BIT_RAT	View Schedule Schedule Copy TE Bin Duration: auto	Create Repor
plication blication (ice: All WAN	n, Last Fifteen M Flow) I Devices Interface: urce: flowstore Star	nutes All WAN Interfaces Time: Mar 09, 2025	Display Filter: No D 20:55:00 IST (GMT+6	isplay Filtering Direction 5530) End Time: Mar OS	View n: outbound Flow Type , 2025 21:10:00 IST (GM	Dptions V E basic Exect F+05:30) Bus	Share ation Type: times iness Hours: nor	Print \$ eries Sort By: BIT_RAT e Execution Data Sou	View Schedule Schedule Copy TE Bin Duration: auto rce: flowstore Bin Inter	Create Repor
plication (vlication (ce: All WAN wrt Data Sou 20	n, Last Fifteen M Flow) I Devices Interface: urce: flowstore Star	nutes All WAN Interfaces Time: Mar 09, 2025	Display Filter: No D 20:55:00 IST (GMT+1	lisplay Filtering Direction 55:30) End Time: Mar 09	n: outbound Flow Type 0, 2025 21:10:00 IST (GM	Dptions ~ Ebasic Exect F+05:30) Bus	Share ution Type: times iness Hours: nor	Print S eries Sort By: BIT_RA e Execution Data Sou	View Schedule Schedule Copy FE Bin Duration: auto rece: flowstore Bin Inter unknown e al	Create Repor
plication lication (ce: All WAN rt Data Sou 20	n, Last Fifteen M Flow) I Devices Interface: urce: flowstore Start	nutes All WAN Interfaces Time: Mar 09, 2025	Display Filter: No D 20-55:00 IST (GMT+4	iisplay Filtering Direction 55:30) End Time: Mar 05	View n: outbound Flow Type 0, 2025 21:10:00 IST (GM	Cptions V 2: basic Exects F+05:30) Bus	Share ation Type: times iness Hours: nor	Print S eries Sort By: BIT_RA e Execution Data Sou	View Schedule Schedule Copy FE Bin Duration: auto ree: flowstore Bin Inter unknown sal Total	Create Repor
dication (dication (ce: All WAN ort Data Sou 20	n, Last Fifteen M Flow) i Devices Interface: urce: flowstore Start	NUTES	Display Filter: No D 20-55-00 IST (GMT+1	iisplay Filtering Direction 35:30) End Time: Mar 09	N: outbound Flow Type 9, 2025 21:10:00 IST (GM	Dptions ~ :: basic Exect +05:30) Bue	Share ation Type: times Hours: nor	Print S eries Sort By: BIT_RA e Execution Data Sou	View Schedule Schedule Copy TE Bin Duration: auto ree: flowstore Bin Inter unknown e sal - Total	Create Repor
lication (lication (ce: All WAN ort Data Sou 20	n, Last Fifteen M Flow) I Devices Interface: urce: flowstore Star	All WAN Interfaces Time: Mar 09, 2025	Display Filter: No D 20:55:00 IST (GMT+4	iisplay Filtering Direction 25:30) End Time: Mar OS	View n: outbound Flow Type 9, 2025 21:10:00 IST (GM	Dptions ~ :: basic Exect +05:30) Bus	Share ation Type: times Hours: nor	Print S eries Sort By: BIT_RA e Execution Data Sou	View Schedule Schedule Copy TE Bin Duration: auto rree: flowstore Bin Inter auknown al al	Create Repor
lication (ce: All WAN ort Data Soc 20	n, Last Fifteen M Flow) I Devices Interface: urce: flowstore Star	NUTES	Display Filter: No D 20:55:00 IST (GMT+I	ilsplay Filtering Direction D5:30) End Time: Mar 05	View n: outbound Flow Type 2, 2025 21:10:00 IST (GM	Dptions ~ :: basic Exec :+05:30) Bus	Share ation Type: times Hours: nor	Print S eries Sort By: BIT_RAI e Execution Data Sou	View Schedule Schedule Copy TE Bin Duration: auto rce: flowstore Bin Inter unknown e sal - Total	Create Repor
lication (ce: All WAN ort Data Sou 20 10 20:56	n, Last Fifteen M Flow) I Devices Interface: urce: flowstore Star	nutes All WAN Interfacea Time: Mar 09, 2025	Display Filter: No D 20:55:00 IST (GMT+4	iisplay Filtering Direction 5530) End Time: Mar 05 21:02 2	View n: outbound Flow Type 9, 2025 21:10:00 IST (GM 21:04 2	Dptions v s basic Exect +0530) Bus 1:06	Share ation Type: times iness Hours: nor 21:08	eries Sort By: BIT_RAT e Execution Data Sou	View Schedule Schedule Copy TE Bin Duration: auto area: flowstore Bin Inter and antown a sel Total	Create Repor
lication (ice: All WAN rt Data Soi 20 10 0 20:56	h, Last Fifteen M Flow) I Devices Interface: urce: flowstore Start 20:58	All WAN Interfaces Time: Mar 09, 2025	Display Filter: No D 20-55-00 IST (GMT+4	isplay Filtering Direction 55:30) End Time: Mar 05 21:02 2	View n: outbound Flow Type 0, 2025 21:10:00 IST (GM 21:04 2	Dptions V to basic Exect t+05:30) Bus 1:06	Share ation Type: times Hours: hor 21:08 Search	Print S eries Sort By: BIT_RA e Execution Data Sou	View Schedule Schedule Copy TE Bin Duration: auto ree: flowstore Bin Inter unknown al - Total	Create Repor
lication (ce: All WAN ort Data Soc 20 10 20:56	n, Last Fifteen M Flow) I Devices Interface: urce: flowstore Start 20:58 Application ≎	nutes All WAN Interfaces Time: Mar 09, 2025 21 Total Flows 🗘	Display Filter: No D 20:55:00 IST (GMT+4 00 Total Bytes 🗘	tisplay Filtering Direction 5530) End Time: Mar 05 21:02 2 % of Total Bytes ≎	View a: outbound Flow Type a, 2025 21:10:00 IST (GM 21:04 2 Total Packets ≎	Dptions ~ c basic Exect F+05:30) Bus 1:06 Q Average Bit	Share ation Type: times iness Hours: nor 21:08 & Search Rate \diamondsuit Ay	Print S eries Sort By: BIT_RA e Execution Data Sou 21:10 erage Packet Rate 🛇	View Schedule Schedule Copy FE Bin Duration: auto ree: flowstore Bin Inter aal Total : Peak Bit Rate \bigcirc	Create Repor
plication dication (ce: All WAN ort Data Sec 20 10 20:56 egend \diamondsuit	n, Last Fifteen M Flow) I Devices Interface: urce: flowstore Start 20:58 Application ≎ unknown	nutes All WAN Interfaces Time: Mar 00, 2025 21 Total Flows \$ 130	Display Filter: No D 20.55:00 IST (GMT+1 20.55:00 IST (GMT+1 20.00 Total Bytes \$ 164.24 KB	Naplay Filtering Direction 25:30) End Time: Mar 09 21:02 2 % of Total Bytes 99.86%	View n: outbound Flow Type p, 2025 21:10:00 IST (GM 21:04 2 Total Packets \$ 1,951	Dptions ~ 2: basic Exect F+05:30) Bus 1:06 C Average Bit 1.4	Share ation Type: times iness Hours: nor 21:08 & Search Rate \diamondsuit Av 46 Kbps	Print S eries Sort By: BIT_RA e Execution Data Sou 21:10 erage Packet Rate 2.17 pps	View Schedule Copy TE Bin Duration: auto rece: flowstore Bin Inter unknown eal Total CPeak Bit Rate \$ 5 15.09 Kbps	Create Repor

Calculations

The "% of total bytes" is the percentage of bandwidth that the application is using relative to the other applications returned in the report result.

Caveat

- If there are applications not included in the table, they are not included in the percentage calculation (e.g., if the report limit is 1000, the percentage is only relative to the 1000 apps returned).
- As of 25.1.0, this column is not available for flowstore v2.

Updating Docker IP Ranges

Overview

By default LiveNX uses 172.17.x.x or 172.18.x.x IPs for docker. If customer uses these IPs in their network it will create a conflict. In LiveNX 25.1.0 user will get ability to change the Docker IP ranges via the LiveAdmin utility.

Configuration

- Login to LiveAdmin utility (livenx ip:8443)
- Navigate to LiveNX and then select *Configure Docker*.

Li	veAdmin			🐣 Administrator 👻
*	DASHBOARD	LiveNX		
\$	AUTHENTICATION			
8	LIVENX	Change Admin Password	Change LiveNX admin Password	
*	MONITOR	Migrate InfluxDB	New Password*	
"	NETWORK	Configure Docker	Password	
٥	SUPPORT		Repeat password*	
	REMOTE SYSLOG		Repeat password	
	TIME	*0	Update	
•	TLS			
6	UPDATE			

• On the configuration page, Enter Bridge IP in CIDR fomat. This should be an IP address and netmask, not a subnet address. For example, do not use a .0 IP in a /24 subnet.

Li	veAdmin				🔒 Administrator 🕶
A	DASHBOARD	LiveNX			
4	AUTHENTICATION	Change Admin	Conference De altra ID anna an		
00	LIVENX	Password	Configure Docker IP ranges		
÷	MONITOR	Migrate InfluxDB	Data Root		
#	NETWORK	Configure Docker	/data/docker		
Ф	SUPPORT		Bridge IP 172.17.0.0/16		
	REMOTE SYSLOG		Address Pools		
	TIME		Base	Size	
a	TLS		Base (e.g., 172.17.0.0/16)	Size	Remove
æ	UPDATE		Add Pool		
			Additional config		
			Key value pairs e.g., "storage-driver": "overlay2", "dns-search": "example.com"		<i>i</i> e

- Click on Add Pool button to enter one or more Address Pools. For 25.1.0, a single subnet will be chosen from the pool for the livenx bridge network.
 - Base is the CIDR of the address pool
 - Size is the network prefix used for creating subnets from the pool.
 - Example: Base=10.1.0.0/16, Size=24 would create 256 / 24 subnets with 256 addresses each.
- Click Save. This will update the docker config and restart docker and all containers.

How To Setup DDI Dashboard

Overview

These instructions guide you to set up DDI dashboard in LiveNX. Once LiveNX and LiveWire have been configured properly for DDI integration, data related to DDI health will be populated in the DDI Dashboard of LiveNX. There are two dashboard options, one in native LiveNX and one in Grafana.

Prerequsite

Before starting DDI dashboard setup user should download the DDI dashboard plugin.

LiveNX Native DDI Dashboard

Importing the DDI dashboard Plugin

- Download the *ddi-dashboard-plugin.nxp* from the LiveNX Integrations public repo.
- Log in to LiveNX web and click on the gear icon available on the Navigation bar and select Settings option.

≡	Live∧ction	NX LiveAss	urance				▲ 0 ■ 0 • 0	🜲 14		🔅 🔺 💄 admin 👻
Overvie	Enter Filter Reque	est Here							<>> 1	Settings
Sites,	Devices, Interfaces by Stat	tuses					Active Alerts			System Diagnostics
SIT	ES: 8		DEVICES: 22		INTERFACES: 178		ALERTS			User Management
										LiveNX Server
SI	TES 🗗	0		0	INTERFACES 🗹	0				
•	Barcelona		Barcelona		docker0 livewire					

• On the Settings page, navigate to Mounted Data and select Plugins.

	ssurance	New Features! 🔺 0 💻 0	0 • 0 🔺 1		۰.	
Settings						
Q Search	PLUGINS					
Entity Page Reports 🗸 🗸						
External Authentication 🗸	Add Enable Disable Delete Import	Export	Q Sea	arch		
Integrations ~	NAME 🗘 TYPE	O IMPORTED O EI	NABLED 🗘 DASI	HBOARDS 🗘 REPORTS	O DESCRIPT	
Licensing ^						
License Configuration	Name Type		All V D	ashboards	Descri	ption
License Expiration Notification						
Mounted Data ^						
Flow, Alerts and QoS Data						
Plugins		No Data				
Network Intelligence Conliguration						
Properties						
Prov						
Paparta V	Rows: -					

• On the *Plugins* page click on *Import* button, and import the plugin which we downloaded in the first step.

\equiv LiveAction	NX LiveAs	ssurance		New Features!		0 0	🌲 14			0 -	
Settings											
Q Search		PLUGINS									
Entity Page Reports	~										
External Authentication	~	Add Enable Disable Delete	Import	Export			Q Search.				
Integrations	~	NAME	¢ TYPE	\$ IM	IPORTED 🗘	ENABLED	DASHBOA	RDS 🗘 R	EPORTS	DESCRII	PTION 🗘
Licensing	^										
License Configuration	- 1	Name	Туре		All ~	All	Dashb	oards	Reports	Des	cription
License Expiration Notification	- 1										
Mounted Data	^										
Flow, Alerts and QoS Data	_										
Plugins				No Rows	To Show						
Network Intelligence Configuration	~										
Nodes											
Properties	~										
Proxy		Rows: -									

• After importing the plugin file, a DDI dashboard will be listed on the *Plugins* page. Select the plugin and click *Enable*.

≡ Live∧ction	NX LiveAss	surance	New Featur		0 0	🌲 14 🛛 {}		🤨 🚽 💄 admin 🚽
Settings								
Q Search		DUTCING						
Entity Page Reports	~	FLUGINS						
External Authentication	~	Add Enable Disable Delete	Import Export			Q Search		
Integrations	~	NAME	O TYPE O	IMPORTED Ô	ENABLED	C DASHBOARDS C	REPORTS	
Licensing	^							
License Configuration		Name	Туре	All ~	All ~	Dashboards	Reports	Description
License Expiration Notification		DDI	Dashboards	~		DDI		DDI Health Da
Mounted Data	^							
Flow, Alerts and QoS Data								
Plugins								
Network Intelligence Configuration	~							
Nodes								
Properties	~	l₃						
Proxy		Rows: 1 / 1 Selected: 1						
Reports	~							

• Now to add the dashboard, navigate to Dashboard page of LiveNX web

• On LiveNX Dashboard page click on + icon to add a new dashboard.

	New Features! 🔺 0	■ 0 • 0 🜲 14 {-} - 🛛 😧 - 🏶 - 🌲 admin -
Dashboard	Mar 09, 2025 18:45	5:00 → Mar 09, 2025 19:00:00 Dashboards List Add Widget
II Status ···· II WAN	··· III System ··· III Cisco S	D-WAN Performance ···· 🗄 Alerts ···· +
Enter Filter Request Here		
Top Sites by WAN Utilization Peak Inbound WAN Interface Utilization Unspecified—TechSupport10 Unspecified—CSR-Toul-Red00 Unspecified—CSR-Toul-Red00 Unspecified—CSR-Toul-Red00 Unspecified—Honolulu—ge00 Unspecified—Honolulu—ge00 Unspecified—Honolulu—ge00 Unspecified=Honolulu—ge00 Unspecified=Honolulu—ge00 Unspecified=Honolulu—ge00 Unspecified=Honolulu—ge00 Unspecified=Honolulu—ge00 Unspecified=Honolulu—ge00 Unspecified=Honolulu—ge00 Unspecified=Barcelona=g00 Unspecified=B	Image: Top WAN Applications by Bandwidth Inbound/Outbound Bandwidth X unknownnetwork-service 2.9 Image: Im	** Top Interfaces % Changed - Interface Burstable Rate X CEDGE-Greenwich—CEDG17.8
%	Kbps	" Ten Devices Ten Devices ODUIteres
t dire datas may an alca A	Critical Warning Good	UnspecifiedHonolulu 40.0 UnspecifiedBarcelona 40.0

• On *Dashboard* configuration page you will get a DDI dashboard option under imported Dashboards menu. Click on *Copy* button to add the dashboard.



• After clicking on the Copy button, a new DDI dashboard will be added to LiveNX dashboard tab.

=	Live/Action	NX	LiveAssurance				New Features!		0	0 🌲 14				
Dash	nboard						Mar	09, 2025 18:	50:00 → Ma	ar 09, 2025 19:05:00	Dashb	oards List	Add Wi	dget 🖉
8	Status	::	WAN	:	System	::	Cisco SD-WAN Perfor	mance …		Alerts			DDI	·· +
	DHCP Alerts by Type				DNS and DHCP Traffic									
		No dat	a		0.6 (edg) 0.4 0.2 0 18:52 0 dos es total	1	3:54 18:	56	18:58	19:00		19:02	19	04
	Alerts by Destination				: Alerts by Source									

LiveNX Grafana DDI Dashboard

- To launch the Grafana dashboard browse to LiveNX server IP:3000 in browser.
- Log in to Grafana with credentials (default credentials are admin / livenx-changeme).

	Welcome to Graf	ana
	Email or username	Unlock 1Password
	email or username	60
	Password	
	password	۲
	Log in	
	Forgot yo	our password?
Documentation ③ Supp	port Community Open Source Grafana v	/11.1.4 (13173c9874)

• Navigate to Home > Dashboard and select DDI Health Dashboard.

Ø	Q Search or jump to	⊞ ctrl+k				4
⊟ Home → Dashboards						
				_		
Dashboards				Ne	w ~	
Create and manage dashboards to visualize your data						
Q Search for dashboards and folders						
Second Starred			t≣ Sort			
Name		Tags				
> 🗅 Analytics					Í	ì
> C Monitoring						
器 Application (Basic Flow)		npm				
器 Application Dscp Audit (Basic Flow)		npm				
器 Bandwidth Summary (Basic Flow)		npm				
器 DDI Heath Dashboard						
B Device Flow Audit (Basic/AVC/MediaNet Flow)		npm				-

• After clicking on DDI Health Dashboard, it will open the DDI Health Dashboard.



Note Grafana Dashboard requires the use of FlowStore v2 data. LiveNX needs to be configured to "opt-in" to FlowStore v2 for these panels to be populated with data.

How To Setup DDI / OTel in LiveNX

Overview

LiveNX is now able to ingest LiveWire and LiveAssurance alerts. This is accomplished via OTEL. This document will cover the configuration of communication. This setup is classified in two parts; one is configuration at the LiveNX end; and second is configuration at LiveAssurance / LiveWire side.

Configuration at LiveNX side

For DDI / OTEL setup, configuration at livenx end is explained below.

Configuring LiveNX for DDI / OTEL setup via Operation Dashboard (LIveNX Web GUI)

• Log in to LiveNX web and select the gear icon available on the navigation bar, and then select Settings.



• Under Network Intelligence Configuration, select Network Configuration.

Cisco SD-WAN		
LiveNCA		
ServiceNow		
Licensing	~	
Mounted Data	~	
Network Intelligence Configuration	^	
LiveAssist PREVIEW		
Network Configuration PREVIEW		
Nodes		
Properties	~	
Properties Proxy	~	
Properties Proxy Reports	~ ~	

• On Network Configuration page, configure LiveNX REST API Token. (You can get the LiveNX REST API Token from LiveNX Swagger page).

LiveNX REST API Token *	
6ilvhECDZt56HV	
LiveAction Otel Configuration 🚯	
Send Findings Send Tags Send U	ser Activity Send Alerts Send Root Cause An
Send Findings Send Tags Send U	ser Activity Send Alerts Send Root Cause Ana
Send Findings Send Tags Send U Disabled Platform Otel Configuration	ser Activity Send Alerts Send Root Cause Ana
Send Findings Send Tags Send U Disabled Platform Otel Configuration Token	ser Activity Send Alerts Send Root Cause And
Send Findings Send Tags Send U	ser Activity Send Alerts Send Root Cause An
Send Findings Send Tags Send U: Disabled Platform Otel Configuration Token Token Platform Bearer Token Endpoint Endpoint	ser Activity Send Alerts Send Root Cause An

• Scroll to the bottom of page and enable the *LiveAction Receiver Configuration* option.

Token		
Token		
Endpoint	Splunk Index	
Endpoint	Splunk Index	
Enabled LiveAction Rec	eiver Configuration	
Token *		
a387c80e-c9ee-4e93-8da7-8c	956afa5819	

- Create a token for the LiveAction Receiver Configuration (if none is present). Note: green field deployments will always be pre-populated with a UUID.
 - The user can manually enter any value.
 - The user can automatically generate a UUID value by re-saving the configuration. A trick for this is temporarily modify a field and press "save".

Configuration at LiveAssurance to Ingest LiveAssurance Alerts in LiveNX

LiveAssurance can be configured by two methods which are described below.

Configuring LiveAssurance to ingest liveAssurance Alerts via LiveAssurance Web.

- Login to liveAssurance (open LiveNX IP:5443 in a browser).
- From sidebar menu select Settings and then select Integrations.

🖯 Infras	structure	e Assu	irance								C	Critical 0	Error
	Adı	min	About	Security	Integrations	Users	Groups	Roles	Application	Audit			
Dashboard													
Հ ٩		Sec	curity			Cor	nfiguration						
Issues		Sec	urity			Арр	lication						
2		Use	rs			Prox	ky Settings						
Reports		Gro	ups			Add	litional						
000		Aud	es lit log			Abo	ut						
Devices													
]¢]		Inte	egrations			ß							
Settings		Inte	grations										
Code													

• From the Add New Integration drop-down list, select LiveNX.

Admin	About	Security	Integrations	Users	Groups	Roles	Application	Audit					
Q Se	arch Integr	ations									Add New	Integrat	ion 👻
Integrat	ion Name						=	Туре				≡	≡
							No Ro	ws To Show					

- Configure the following parameters:
 - Integration Name: Enter a name for the LiveNX integration.
 - URL: Enter http://localhost as the URL.
 - **Token**: Enter the LiveAction Receiver token that grants authorized access tosend alerts to LiveNX. This is the same token which we generated above in first part.
 - Click Save.
 - For the integration to start, you must restart the authserver by using the following command.

cd /data/bcia && docker compose restart authserver

$\leftarrow \rightarrow$	C	O 🗛 http	os://10.244.29.1	17 :5443/s	ettings/inte	grations				☆		6 e	0	e 🥯	6 🛛	٩	🌸 🌠	ా ≕
🗑 Infras														E Error 15	(W) W		2	0
6	Admin About	Security	Integrations	Users	Groups	Roles	Application	Audit										
Dashboard	Q Search Inte	grations														Add	New Integr	ation 🔻
چ. Issues	Integration Name							≡	Туре								≡	=
la º	New LiveNX Int								LIVENX									:
Reports											-							
Dovisoo						Live	NX Intear	ation										
Devices						For s	toring BCIA ale	erts in LiveNX										
Settings						Integra	ation Name*											
						My	LiveNX Integr	ation										
Code						URL*	://localhost											
						Token	*											
						eNA	AqDWBmYiqhj6	8hGj1BELCtq	JweFKPt89qk7	EKCRwjw=	1							
						Can	cel			Save								

Configuring LiveAssurance to Ingest LiveAssurance Alerts via LiveNX CLI

- SSH into LiveNX
- o sudo data/bcia/authserver/otel/la-otelcol.yaml

• Configure this YAML file and add the Token which we generated in LiveNX under bearertokenauth/ withscheme.

exporters:
otlphttp/liveaction:
auth:
authenticator: bearertokenauth/withscheme
endpoint: http://lnx-local:4318/
headers:
x-customer-id: liveaction_dev
tls:
insecure: false
insecure_skip_verify: true
extensions:
bearertokenauth/withscheme:
scheme: Bearer
token: 8a25f6ef-4099-1b37-522e-6cee61eb5c95 #Must match TOKEN from livenx
processors:
batch:
timeout: Os
batch/logs:
send batch max size: 100
Hit Ctrl+O and then Hit "Enter".

• Hit Ctrl+X to save and exit.

Configuration at LiveWire to Ingest LiveAssurance Alerts in LiveNX

Capture Engine Configuration

- Login to LiveWire / Omnipeek Web
- On the Home Page Click on Configure Engine button.

≡ 🦙 LiveWire Omnipeek					\$ -	💄 admin ᠇
Engines / Capture Engine / Home						
Home Captures Forensics Files Forensic Searches Events	Adapters Settings Admin					
NAME Capture En HOST NAME TechSupp ADDRESS 10.8.10.43 USER admin ENGINE TYPE LiveWre VERSION 24.3 (build ENNIE CALTIME 09/3/2025 TIME ZONE GMT-27/00 UPTIME 2916.56: OPERATING SYSTEM Ubuntu 22. IPM ADDRESS 10.8.10.53 MEMORY 19.20.29 M CPU TYPE Inte(R) Xe CPU TYPE Inte(R) Xe CPU COURT 48 DATA FOLDER /var/Ib/on CAPTURE STORAGE	line 1-3100-288T 24.3.0.19) 04:22:04 4 14.5 LTS i Total Phys; 128,626 MB Avail Phys n(R) Gold 6126 CPU @ 2.60GHz ni/data/ 222,508 GB Total; 100,539 GB Avail		L.	Configure Engine Configure System Update License		
1		01	100	110		

• On Configure Engine page, scroll down to OpenTelemetry section.

• Click Enable Open Telemetry.

≡ 🨪 LiveWire Omnipeek			🏟 👻 💄 admin 👻
Engines / Capture Engine / Configure Engine			
Home Captures Forensics Files Forensic Searches Even	ts Adapters Settings Admin		
Access Control		~	^
	Enable access control		
	_		
OpenTelemetry		~	
	Disable OpenTelemetry		
	C Enable Open Lelemetry		
CUSTOMER ID	0		
ENDPOINT	0		
TOKEN	0		
SEND	LiveFlow Expert Events		
	At least 1 option must be enabled		
	Use TLS		ý.

- Under Open Telemetry configure items below:
 - **Customer ID**: This value is not used by LiveNX but it must be populated, and it must be a string (not an integer).
 - Endpoint: This value should point to the LiveNX server/port.
 - Token: This value should match the token generated in LiveNX.
 - **Send**: This section of the configuration details what the OTel collector will be sending in OTel format to the specified endpoint. At the moment, the user may only choose to either send or not send LiveFlow Alerts The user must select at least one option to send otherwise a message will be displayed and the user will be unable to apply the engine settings. If the user has an existing LiveFlow capture that is configured to generate OpenTelemetry records, the user will not be allowed to turn off sending LiveFlow Alerts. The "LiveFlow Alerts" switch will be disabled and a message is displayed indicating why.

LiveFlow Capture Configuration

- From LiveWire Omnipeek, click Captures.
- Create a new LiveFlow Capture or edit existing LiveFlow capture.

• Home Captures (1)	Engines / Capture Engine / Captures	k								0 -	å a	idmin -
LiveFlow Capture STATUS Capturing ADAPTER 100-0P (High Performance) Adapter - 2 DIATA SIZE RESERVED 51,273 GB MERIA Element CAPTURE TO DISK Yes INTELLIGENT CTO NO NUMERIA BOTHED NUMCING VES PACKETS INCEPTED 28 PACKETS INCEPTED 0 FLOWS BIOOPED 0 COMPRESSION 0 COMP	Home <u>Captures</u> Forensics Files Forensic Captures (1)	Searches Events Adapters Settings Admin		Search	×	+ New Capture *	► Start All	Stop All		=		Ø
		LiveFlow Capture STATUS Capturing ADAPTER 10G-4P (High Performance) Adapter - 2 Link SPEED 10,000 Mbtb/s MBDA Ethernet CAPTURE TO INSK Yes INTELLIGENT TOT NO NIDEXINA Yes PACKTTS RECEIVED 28 PACKTTS FILTERED 28 PACKTTS FILTERED 28 PACKTS BROPPED 0 FLOWS DROPPED 0	START TIME 05 STOP TIME 05 DURATION 0. DATA SIZE RESERVED 51 FILTERS HARDWARE PROFILE OWNER ac MODIFIED BY ac ACTION Se	y/3/2025 17:38:22 y/3/2025 17:45:05 06:43 _278 GB Imin Imin ItCaptureOptions			E Stop (Capture Delete	apture Options Capture	G			
UNIA REDUCTION RETENTION TACTOR RETENTION TIME		COMPRESSION - 36.1% TOTAL - 36.1% DATA REDUCTION	1.6× RETENTION FACTOR	2	0:0	06:32						

• In LiveFlow Capture configuration, find and configure *LiveFlow Alerts*.

INTERVAL (SECONDS)	Must be between 10 and 1,800 (inclusive)
FLOW REFRESH	60
INTERVAL (SECONDS)	Must be between 1 and 1,800 (inclusive)
GENERAL ANALYSIS	Enforce 3-Way Handshake
	ULAN/VXLAN/MPLS
RECORD SPECIFIC	Application Performance
OPTIONS	Application Delay (AD), Client Network Delay (CND), Network Delay (ND), and Server Network Delay (SND)
	Include Direction Field
	TCP LiveFlow Alerts - Connection Lost, Connection Refused, Low Window, and Zero Window
	Configure
	TCP Retransmissions
	4 Configure
	Web Analytics
	Basic Flow
	Include Direction Field
	Cisco SNA
	Byte Distribution and Entropy Analysis
	Include First Packet Data
_	Sequence of Packet Lengths and Times
	LiveFlow Alerts
	& Configure
	Platform
	Include Direction Field
	Voice/Video Performance
	Include Direction Field
	& Configure
OUTDUT	

LIVEFLOW ALERTS CONFIGURATION				>
LIVEFLOW ALERT	THRESHOLD		MINIMUM S	AMPLES
DHCP Frequent Retransmissions	3	retransmissions	10	seconds
DHCP Low Lease Time	1	minutes		
 DHCP Request Rejected 				
DHCP Request Storm	500	requests	10	seconds
DHCP Slow Response Time	2000	milliseconds		
DNS Error				
 DNS Frequent Retransmissions 	3	retransmissions	10	seconds
ONS Idle Too Long	10	seconds		
 DNS Query Format Error 				
Enable All Disable All Detailed INFORMATION DHCP Frequent Retransmissions Description				
Repeated DHCPDISCOVER or DHCPREQUEST messages observed from a given c	ient within a short time p	eriod.		
Cause Retransmission occurs when the DHCP client isn't receiving a response from a see the server isn't configured to provide leases for the client subnet, or because the receiving a DHCPOFFER for a lease it can't accept: for example, the offer may be 43) or options specifying where the device can load a boot image and/or configu	rver in a timely fashion. Tl subnet has been exhaust missing DHCP options cri ration file.	nis may be because the client's ed of free leases. Retransmissi tical to the device's operation,	s message ons can al such as v	isn't reaching the server, because so occur when the DHCP client is endor-specific information (option
				Cancel OK

• Under *Output* section, Click on *+Add Options* button to add one new LiveNX Telemetry for LiveFlow Alerts.

💳 🦙 LiveWire Omnipeek				🛟 - 🛛 🛔 admin -
Engines / Capture Engine / Captures / LiveFlow Capture / Capture Options				
Home Captures Forensics Files Forensic Searches Events Adapters Settings Admin				
OUTPUT			+ Add Output -	•
	LiveNX Teleme	try	8	
	SERVER ADDRESS	10.8.104.16 Must he an IDuá or IDuá address		
	SERVER PORT	2055		
	IPELY RECORDS	Default is 2055		
	I TA REGINDO	Basic Flow Cisco SNA		
		Platform		
		Voice/Video Performance II		
	LiveNX Teleme	etry 2	1 8	1
	SERVER ADDRESS	10.8.014.16 Must be an IDuf or IDuf address		1
	SERVER PORT	2055		
		Default is 2055		
	IPFIX RECORDS	Application Performance Application Performance Basic Flow Cisco SNA		1
	·			Cancel OK

• Click *OK* to save and exit.

LiveAssurance - Network Security

Overview

LiveAssurance - Network Security, proactively identifies firewall issues and provides remediation steps to prevent disruptions. It detects hidden configuration drifts, run-time anomalies, maintenance gaps, and adherence to best practices.

Powered by AI and machine learning, LiveAssurance auto-triages issues, reducing Mean Time to Resolution (MTTR) by investigating problems, performing root cause analysis, and executing troubleshooting tasks autonomously.

Freemium Licensing

- BlueCat is providing LiveAssurance Network Security with five device licenses at no cost for 12 months.
- This freemium offer is available to customers with an active LiveNX subscription (no initial license fee).
- Customers can access LiveAssurance after upgrading to LiveNX 25.1.0 or later.
- The freemium offer does not include any warranties or support. If full technical support is needed, BlueCat recommends purchasing a regular license that includes support.
- Customers who wish to continue using LiveAssurance after 12 months must purchase a license.
- BlueCat reserves the right to modify or discontinue this freemium offer at any time on prior notice.

Features and Benefits

- **Proactive Issue Detection**: Identifies potential security and performance issues before they escalate.
- Automated Troubleshooting: Reduces manual intervention with auto-triage capabilities.
- **Continuous Monitoring**: Ensures 24/7 network security and compliance adherence.
- Freemium Licensing: Includes licenses for up to five devices, valid for 12 months with LiveNX 25.1.0 or later.

Prerequisites

To use LiveAssurance, ensure:

- LiveNX is upgraded to version 25.1.0 or later.
- LiveAssurance Freemium requires a working Internet connection to download the BCIA Freemium containers from our privately-maintained docker registry. If necessary, please add indeni-docker.jfrog.io to your firewall whitelist.
- Devices have SSH enabled on port 22.
- Device credentials (username and password) are available.
- TCP Port 5443 is open.
- SMTP server details are available if email notifications are required.

Installation and Setup

Enabling LiveAssurance (BCIA)

- SSH into the LiveNX server CLI.
- Enter root mode: sudo su.

• Navigate to the LiveAssurance working directory: cd /data/bcia.



• Verify the LiveAssurance files: 1s -1a.

[page] bappy								
root@livenx-	vap251:/	/home/ad	lmin#	cd /	/dat	a/bcia	a	Т
root@livenx-	vap251:/	/data/bo	ia#]	ls -1	L			Т
total 44								
drwxrwxr 5	livenx	livenx	62	Feb	10	19:57		
drwxrwxr 4	livenx	livenx	47	Feb	10	19:57		
-rwxrwxr 1	livenx	livenx	311	Nov	14	16:56	bcia-config.json	
-rwxrwxr 1	livenx	livenx	515	Feb	10	20:16	bcia-docker.service	
drwxrwxr 2	livenx	livenx	75	Feb	10	19:57	build	
drwxrwxr 3	livenx	livenx	18	Feb	10	19:57	collector	
-rwxrwxr 1	livenx	livenx	437	Feb		14:59	docker-compose.dev.yml	
-rwxrwxr 1	livenx	livenx	644	Feb	10	19:58	docker-compose.lnx.yml	
-rwxrwxr 1	livenx	livenx	6815	Feb	10	19:57	docker-compose.yml	
-rwxrwxr 1	livenx	livenx	732	Feb	10	21:34	docker-run-pre.sh	
-rwxrwxr 1	livenx	livenx	2398	Feb	10	19:57	docker-run.sh	
drwxrwxr 3	livenx	livenx	21	Nov	14	16:56	manifest	
drwxrwxr 2	livenx	livenx	26	Nov	14	16:56	parser	
-rwxrwxr 1	livenx	livenx	834	Feb	10	19:57	README.md	
drwxrwxr 4	livenx	livenx	45	Feb	10	19:57	server	
-rwxrwxr 1	livenx	livenx	1035	Jan	2	14:52	services.json	
-rwxrwxr 1	livenx	livenx	337	Feb	10	19:57	start-bcia.sh	
drwxrwxr 5	livenx	livenx	116	Feb	10	19:57	traefik	
root@livenx-	vap251:/	/data/bo	ia#					

- Initiate Docker: sudo ./docker-run-pre.sh (run once).
- Start LiveAssurance: ./start-bcia.sh <bcia-version> (Please reach out to Bluecat support to get version details). It may take 1 minute to start all the LiveAssurance services. After completing you will get completion message as below.



• Access LiveAssurance via a browser at <LiveNX-URL>:5443.

Accessing the LiveAssurance Web Interface

• Open <LiveNX-URL>:5443 in a browser.

• Log in using default credentials (*admin/admin123!*).

ØBLUECAT					
Login to Infrastructure Assurance					
Enter your username and password to log into the BlueCat Infrastructure Assurance				•	
Username*					
admin					
Password*					
Login 🄊					
© 2024 BlueCat Networks. All rights reserved.					

• Acknowledge the LiveAssurance Insight Confirmation.

Changing Default Credentials

• Navigate to Settings > Users.

🖰 Infra	structure	Assurance								Critical 0	🖲 Error 0	🥨 Warning 0	æ	٩
Dasbboard	Adm	in About	Security	Integrations	Users	Groups	Roles	Application	Audit					
		Security			Cor	nfiguration								
Issues		Security			Арр	lication								
Reports		Groups			Pro	ky Settings								
00		Roles			Ado	ut								
Devices														
↓ Settings		Integrations												
>														
Code														

• Click on the admin user and select Edit.

₿ Infrast	ructure Assurance								Critical 0	🕒 Error 0		W Warning 0	₽	٢
	Admin About	Security	Integrations	Users	Groups	Roles	Application	Audit						
Dashboard	Q Search User	5											New U	ser +
لچ Issues	User Name		=	Na	me / Email			≡	Groups / Roles		≡	Created	≡	≡
	admin			- N	one -				Admin			N/A		:
Reports														_
Devices														
↓ Settings														
>Code														

• Provide First Name, Last Name, and enable "Ask for password change at next login". It will ask to change the password on next login.

🔂 Edit User	User will not receive any emails as SMTP is not configured. Add SMTP Configuration
1 User details and Email notifications	2 Groups and Roles
User Name*	Email*
admin	vpandey@xyz.com
First Name	
Vaibhav	Email Notifications
Last Name	Select severities to receive email notifications
Pandey	All Critical Error Warning Info
Generate password automatically	
Ask for a password change at the next log-in	
Cancel	Next

• Click Next and then Save.

• Log out and log back in to change the password.

ØBLUECAT					
	Change password to login				
Password					
 Ø Min password lengt 	h is 1 [AaZz1]]				
Confirm Password					
	Change Password				
© 20	124 BlueCat Networks. All rights reserved.				

Device Onboarding and Credential Management

Creating Credential Sets

The first step to inspecting your devices is to create the credential set - the login credentials that will be used to query the devices.

• Navigate to Devices > Credential Sets.

€ Infra	structure Assurance						Critical 0	😑 Error 0	😗 Warning 0	₽	8
5	Devices Credential Sets	Scheduled Tasks Label M	anagement								
Dashboard	Back to Devices Credential Sets										
Issues	Credential Sets List	New +	Credentials							New	+
Reports	New test Credential set	/ 1	Туре	Username	Description						
Devices						No credentials were defined					
Code			Subnets to use	Credentials on						New	+
			Subnet	Mask							
						No subnets were defined					

• Click New to create a credential set.

Back to Devices Credential Sets	
Credential Sets List	New +
New Credential Set	/ 1

- To Create Credentials, click on *New* to create New Credential Define a custom name and select a credential method:
 - Username + Password
 - SH Private Key
 - SNMPv2
 - SNMPv3
- Configure the username, password, and description.

I	New Credentials Add new credentials			
tials	Username + Password	¥		
5	vpandey			
	Password			ials were de
	Privileged Password			
s to u				
net	Credential to connect with device			
	Cancel	Save	1	ts were 🔀

Configuring Subnets for Credentials

The credentials also include the subnet which will use those credentials. If all of your devices are using the same credentials, you can simply set this to 0.0.0/0 to have it apply to all devices. Otherwise, if your devices use different credentials, you can create multiple credential sets, and then specify the network and mask for each (which can be an exact IP address such as 94.94.94.17/32 or a subnet such as 94.94.0.0/16).

If there are overlapping Subnets (such as 94.94.94.17/32 and 94.94.0.0/16), the LiveAssurance server will try to connect using the most specific subnet. If those credentials fail, it will then try the next most specific subnet. In our example, the /32 subnet would be tried first and then the /16 subnet.

• To add the Subnets, click on the New button to add the subnets.

Cancel Save	ash basic	New Subnet Add new network subnet		Description			
	Subnets to u		Ş	Cancel	Save		Ne

- Assign credentials to specific subnets.
- Use 0.0.0/0 for all devices.
- Configure multiple credential sets for different subnet ranges.
- If overlapping subnets exist, LiveAssurance prioritizes the most specific subnet.

Adding Devices for Inspection

- Navigate to Devices > Device Inventory.
- Click New Device +.

🖯 Infras	structure Assurance						Critical	0 🕒 Error	0	Warning 0	#° ©
8	Devices Credential Sets Scheduled Tasks	Label Management									
Dashboard	Q Search Devices									8	New Device +
ے۔ Issues	\Box = = = Device Name \uparrow	IP Address	Device Vendor	\equiv Labels	≡	Software Version	≡	Software Model	≡	© Iss ≡	(E) Issues
les?											
Reporta											
Devices											
191											
Settings				No Rows To Show							
>Code											
						2					

• Enter the device name and IP address.

Jeme	Add D)evice	New + Import ① Add Known Devices +	
3	⊗	Device Name Enter a unique name	Device IP	sion
l	8	Device Name Enter a unique name	Device IP	
l				
l				
l	Labels (0))		
L			Cancel 7 Interrogate	

• Click Interrogate.

LiveAssurance will interrogate the device (using the credential sets you have created) to determine the device vendor, OS, etc. If the LiveAssurance server is unable to communicate with the device, it will return an error. The most common reasons for a communication issue are:

- An issue with the credentials either
 - You have mis-typed the username/password in the Credential Set.
 - The device's IP Address is not in the subnet(s) assigned to the Credential Set.
 - Those credentials don't exist on that device or don't have the correct permissions.
- Connectivity issues between the device and the LiveAssurance server. This could be,
 - Basic connectivity between LiveAssurance server and device. The easiest way to test this is to logon directly to the LiveAssurance server's Linux interface and ping the device.
 - SSH connectivity between the LiveAssurance server and the device. Validate that SSH is enabled on the device using port 22

LiveAssurance queries the firewalls on a scheduled basis, varying from every minute to every day depending on the data being retrieved. You should therefore begin to see Alerts within a few minutes.

Sending LiveAssurance Alerts to LiveNX

You can send the LiveAssurance Alerts to Livenx by integrating LiveAssurance with LivenX. Follow the steps below to integrate the LiveAssurance with LiveNX.

Collecting LiveAction Receiver Configuration Token From LiveNX

To integrate LiveAssurance with LiveNX user need to generate and collect a Token from LiveNX. Follow the Steps below.

• Login to LiveNX web and select the gear icon available on the navigation bar.



• Under Network Intelligence Configuration, select *Network Configuration*.

Cisco SD-WAN		
LiveNCA		
ServiceNow		
Licensing	~	
Mounted Data	~	
Network Intelligence Configuration	^	
LiveAssist PREVIEW		ß
Network Configuration PREVIEW		6
Nodes		2
Nodes Properties		<i>₽</i>
Network Configuration PREVIEW Nodes Properties Proxy	Ý	
Network Configuration PREVIEW Nodes Properties Proxy Reports	~	

• On the Network Configuration page, configure LiveNX REST API Token. (You can get LiveNX REST API Token from LiveNX Swagger page).

LiveNX REST API Token *	
6ilvhECDZt56HV	
LiveAction Otel Configuration ()	
Send Findings Send Tags Send	User Activity Send Alerts Send Root Cause An:
	User Activity Send Alerts Send Noot Gause An
Disabled Platform Otel Configuration	
Disabled Platform Otel Configuration	
Disabled Platform Otel Configuration Token Platform Bearer Token	
Disabled Platform Otel Configuration Token Platform Bearer Token Endpoint	

• Scroll to the bottom of page and enable the *LiveAction Receiver Configuration* option.

Token		
Token		
Endpoint	Splunk Index	
Endpoint	Splunk Index	
Enabled LiveAction Rec	eiver Configuration	
Token *		
a387c80e-c9ee-4e93-8da7-8c	956afa5819	
<u></u>		

• Create a token for the LiveAction Receiver Configuration (if none is present).

Note Green field deployments will always be pre-populated with a UUID.

- The user can manually enter any value.
- The user can automatically generate a UUID value by re-saving the configuration. A trick for this is temporarily modify a field and press "save".

Configuring LiveAssurance For LiveNX integration.

This is the second part of the LiveAssurance and LiveNX integration.

- Login to LiveAssurance (open LiveNX IP:5443 in a browser).
- From the sidebar menu select *Settings* and then select *Integrations*.

₿ Infrastru	icture Assi	Jrance									C	Critical	0	E Error
	Admin	About	Security	Integrations	Users	Groups	Roles	Application	Audit					
Dashboard														
<u>ل</u>	See	curity			Con	figuration								
Issues	Sec	urity			Appl	ication								
8	Use	ers			Prox	y Settings								
Reports	Gro	ups			Add	Additional								
00	Rol	es			Abo	ıt								
Devices	AUC	unting												
افا	Int	egrations			ß									
Settings	Inte	grations												
Code														

• From the Add New Integration drop-down list, select LiveNX.

Admin	About	Security	Integrations	Users	Groups	Roles	Application	Audit						
Q S	earch Integr	ations										Add Ne	w Integra	tion 👻
Integra	tion Name						≡	Туре					≡	≡
							No Ro	ws To Show						

- Configure the following parameters:
 - Integration Name: Enter a name for the LiveNX integration.
 - URL: Enter http://localhost as the URL.
 - **Token**: Enter the LiveAction Receiver token that grants authorized access tosend alerts to LiveNX. This is the same token which we generated above in first part.
- Click Save.
- For the integration to start, user must restart the authserver by using the following command.

cd /data/bcia && docker compose restart authserver

After successful integration, the LiveAssurance alerts are displayed in your *LiveAssuranceEvents* dashboard within LiveNX. Clicking an alert will take you to the *Issues* tab in the LiveAssurance UI, which displays a detailed view of the alert.

In addition to storing alert data in the LiveNX database, the data is also preserved in the file */usr/share/indeni-services/config/livenx.env*. When the LiveNX integration is deleted, this file will also be deleted.

Operations and Monitoring

Reviewing Alerts

As the LiveAssurance system identifies configuration drift, security or performance issues or other potential problems, it will generate an Alert

- Navigate to Issues from the left-hand menu.
- On the Alerts screen, LiveAssurance displays a short headline of the issue, the name of the device and other information. Selecting the Alert will then show the full description of the Alert and the suggested remediation steps.

Policy Tuning

- Out of the box, LiveAssurance's Policies are based upon industry best practices.
- However, each organization's environment is unique. Therefore, you may need to tune the policies, and their thresholds based upon your own standards.

Generating Reports

You may want to configure reports which can be automatically emailed on a scheduled basis.

LiveAssurance (BCIA) Dashboard

- User can see all LiveAssurance alerts and issue details on LiveAssurance Dashboard.
- Browse to <LiveNX-URL>:3000 to access the LiveAssurance Dashboard.

Troubleshooting

Common Errors and Resolutions

lssue	Possible Cause	Resolution
Unable to Access LiveAssurance Web UI	LiveAssurance Services Not Started	Restart LiveAssurance using ./start-bcia.sh
SSH Authentication Fails	Incorrect Credentials	Verify Username Password in credentialsets
Device Not Detected	IP Missconfiguration	Ensure device is within the subnet range

Connectivity Issues

- Verify connectivity using ping.
- Check SSH access: telnet <device-IP> 22.
- Ensure firewall rules allow TCP 5443.

Conclusion

LiveAssurance provides proactive network security, reducing troubleshooting time and enhancing system efficiency. Organizations should regularly review alerts, fine-tune policies, and leverage reporting to maximize LiveAssurance's effectiveness.

Maintenance Mode Schedule

Overview

Maintenance mode is used to disable alerting for selected devices for a period of time. This ensures no false positive alerts are created while network maintenance is being done. In LiveNX 25.1.0 user would have ability to schedule the maintenance mode so that they do not need to manually enable or disable the maintenance mode.

Maintenance Mode Configuration

Maintenance mode can be configured and schedule via Alert Management page. Please see the steps below.

- Login to LiveNX Web.
- Navigate to Configure and the Alert Management page.

١	Live/Action	NX	LiveAssurance	2			New Features!	
^	Main	iest Here						
		ituses						
<u>.</u>	Topology		DE	/ICES: 22		INTERFACES: 178		
1	Stories							
	Reports		() DE		0		0)
			•	Barcelona		docker0 livewire		
1	Configure		•	CEDGENEW		docker0 TechSupport	-3100-288T	
<u> </u>	conngare		•	CEDGENEW		eth0 livewire		
	Alert Management		•	CS-ISR4461-105		eth0 MoscowVedge2		
	Application		•	CSR-Toul-Red		eth0 TechSupport-310	00-288T	
	Management		•	HE-CSR-207		eth0 Toulouse		
	OID Polling		•	HE-CSR-208		ge0/0 Barcelona		
			•	Honolulu		ge0/0 Honolulu		
	Device Management		•	ivewire		ge0/0 MoscowVedge	2	
	Filter Management		•	VoscowVedge2		ge0/0 PaloAlto		
			•	PaloAlto		ge0/0 Toulouse		
	Site Management		•	TechSupport-3100-288T		ge0/0.20 PaloAlto		
	Semantic Management		•	Toulouse		ge0/0.21 PaloAlto		
			-	Dorlin		 do0/11Parcolona 		

• On the Alert Management page click on the Maintenance Mode button.

Eive∧ction NX LiveAssurance			New Features! ▲ 0 ■ 0 ▲ 158 {-} → ② ※ ▲ admin ▼						
Alert Management 📀			Maintenance Mode View Alerts						
LiveNX Alerts			Cisco SD-WAN Integrations						
Enable Disable		Enabled All	✓ Affect Status All ✓ Category All ✓ Q. Search						
ALERT TYPE	ENABLED	AFFECT STATUS	CATEGORY						
> Application Bandwidth		~	Application						
> Application Performance - App Delay		~	Application						
> Application Performance - Network Delay		~	Application						
> BGP Peer Connection Change		~	Network						
Cisco IWAN Path Change		~	Network						
Cisco IWAN Threshold Crossing		~	Network						
> Cisco SD-WAN Performance - Jitter		~	Network						
> Cisco SD-WAN Performance - Network Delay		~	Network						
> Cisco SD-WAN Performance - Packet Loss		~	Network						

- On Maintenance Mode configuration page click on the Add button.
- On the configuration page, configure options below.
 - **Start Time** Optional: Indicates when maintenance mode will start. If not configured, maintenance mode will begin immediately.
 - **End Time** Optional: Indicates when maintenance mode should end. If not configured will last until manually disabled.
 - **Time Zone** Sets the time zone to use for the start and end time configurations.
 - Devices and Interfaces Choose which devices and interfaces should go into maintenance mode.

• Once configured, you will notice that the details around maintenance mode will be displayed as well as a **status** indicator on whether maintenance mode is currently active.

▲ 0 ■	0 • 0 🌲 158	{} ▼	€.	۰.	💄 admin 🔻
	Maintenance Mode				×
Category A	Status: En Start Date and Time: Ma End Date and Time: Ma	abled ar 10, 2025 11 ar 10, 2025 23	:24:00 UTC (:24:00 UTC (GMT+00:00) GMT+00:00)	
	Enter Filter Request Her	e		A	pply filter
			« <	1 / 1	> >>
	Barcelona		վե)	~
	CEDGE-Greenwich		0		~
	CEDGENEW				
	CEDGENEW				~
	😚 CS-ISR4461-105				~
					Edit