LiveAction®

# LiveNX Operations Dashboard

# Admin Guide

LiveAction, Inc. 901 Campisi Way, Ste. 222 Campbell, CA 95008, USA +1 (888) 881-1116 https://www.liveaction.com

Copyright © 2023 LiveAction, Inc. All rights reserved

20230504-LNXAG\_232a

# Contents

Chapter 1	Introduction	1
	About this Admin Guide	
	Configuration & Setting Menus	
		5
Chapter 2	Configuration	4
	Alert Management	
	Maintenance Mode	
	Application Management	
	Custom Applications	
	Application Groups	
	OID Polling	
	Pre-Configured	
	Custom	
	Device Management	
	SNMP Monitored Devices	
	Non-SNMP Monitored Devices	
	Filter Management	
	Site Management	
	Site Details	3
	Site Address	4
	Site Business Hours	5
Chapter 3	Settings	B
•	Settings	
	Data Source Management	
	Data Store Management	
	Disk Overview	
	Nodes Data Store	
	Web UI Data Store	
	Device Entity Page Reports	
	Email Configuration	
	Integrations	
	Cisco APIC-EM/DNA-C	
	ServiceNow	
	LiveNCA	
	Cisco ISE	_
	Cisco SD-WAN	
	Licensing	
	LiveNA Configuration	
	Mounted Data	
	Nodes	
	Properties	2
	Proxy	4
	Reports	4
	Security	7
	Single Sign On	8
	SNMP Trap	
	Syslog	9
	Troubleshooting	
	System Diagnostics	
	, ,	

	Flow Data Status	
	User Management	
	Adding a New Group	
	Sessions	
	LDAP Management	
	WMIC Management	
	TACACS+ Authentication	
	LiveNX Server	123
Chapter 4	LiveNX Appliance	
-	About LiveNX Appliance	
	What's Included	
	Front / Rear Panels	127
	LiveNX Appliance Front Panel	
	LiveNX Appliance Rear Panel	
	Inside LiveNX Appliance	
	LiveNX Appliance Internal Components	
	Installing LiveNX Appliance	
	Connecting Network Cables	
	System Fans	
	Connecting Extended Storage to LiveNX Appliance	
	Starting / Shutting Down LiveNX Appliance.	
	Attaching the Front Bezel	
	Contacting LiveAction Support	
	S 11	

# CHAPTER 1

# Introduction

# In this chapter:

About this Admin Guide	2
Configuration & Setting Menus	3

### **About this Admin Guide**

This LiveNX Operations Dashboard Admin Guide is provided to help a Network Administrator configure and set up LiveNX on your network. It is organized into the following three chapters:

- Chapter 1, Introduction: Provides an introduction to the Admin Guide.
  - About this Admin Guide on page 2
  - Configuration & Setting Menus on page 3
- Chapter 2, *Configuration*: Defines the devices LiveNX will monitor, their sites and semantics, and how LiveNX will monitor the network.
  - Alert Management on page 5
  - Application Management on page 21
  - OID Polling on page 29
  - Device Management on page 33
  - Filter Management on page 50
  - Site Management on page 52
- Chapter 3, Settings: Provides the details for customizing system configuration and user management.
  - Settings on page 59
  - System Diagnostics on page 102
  - Flow Data Status on page 104
  - User Management on page 104
  - LiveNX Server on page 123

# **Configuration & Setting Menus**

The *Configure* settings are available from the Navigation Bar, while the *Settings* are available from the gear menu on the Status Bar:



# CHAPTER 2

# Configuration

# In this chapter:

Alert Management	5
Application Management	21
OID Polling	29
Device Management	33
Filter Management	50
Site Management	52

# **Alert Management**

*Alert Management* is where LiveNX's Alerts can be enabled, thresholds configured, and sharing options defined. LiveNX's alerting engine can track multiple KPIs, notify when thresholds have been crossed, and provide both in-app and external notification.

۶	Configure	
	Alert Management	
	Application Management	
	OID Polling	
	Device Management	
	Filter Management	
	Site Management	

The *Alerts Management* page lists all available alerts and a summary of their configuration.

•									<b>a</b> 104	<b>6</b> 2 •	3 🐥 439	{-}	0-	¢-	<b>å</b>
lert N	lanagement												Maintenanc	ce Mode	View Alert
					LiveNX Ale	erts									
Ena	ble Disable										Q Search				
	ALERT TYPE	CATEGORY	¢	SEVERITY	0	ENABLED	0 1	THRESHOLDS		SHARING					0
		All	~	All	~	All	-								
	Application Performance - App Delay	Application		Multiple		~	,	Multiple		Web UI					
	Application Performance - Network Delay	Application		Multiple		~	1	Multiple		ServiceN	w, Web UI				
	BGP Peer Connection Change	Network		A Critical		~	1	for at least > 0 minutes		Email, We	b UI				
	Cisco IWAN Path Change	Network		A Critical		~	1	for at least > 0 minutes		ServiceN	w, Web UI				
	Cisco IWAN Threshold Crossing	Network		A Critical		~	1	for at least > 0 minutes		ServiceN	w, Web UI				
	Cisco SD-WAN SLA Class Path Change	Network		A Critical		~	1	for at least > 0 minutes		ServiceN	w, Web UI				
	Critical Traffic Response Time	Application		A Critical		~	1	Response Time >= 1 ms for at least > 0 minutes		ServiceN	w, Web UI				
	Custom OID - birmingham	Device, Interface		<ul> <li>Info</li> </ul>		~	1	Value ≻= 100 percent for at least > 0 minutes		Web UI					
	Device CPU Utilization 0	Device, Interface		Multiple		~		Multiple		Web UI					
	Device Flow Stop	Device, Interface		Critical		~	1	for at least > 0 minutes		ServiceN	w, Web UI				
	Device Memory Utilization 0	Device, Interface		Multiple		~	1	Multiple		ServiceN	w, Web UI				
	Device Reachability 0	Device, Interface		Multiple		~	1	Multiple		ServiceN	w, Web UI				
	Interface Errors (CRC, Frame, Overruns, Ignore, Abort)	Device, Interface		Critical		~	1	Number of Errors >= 40 Errors for at least > 0 minutes		ServiceN	w, Web UI				
	Interface Reachability	Device, Interface		Multiple		~	1	Multiple		ServiceN	w, Web UI				
	IPSLA Test	Network		Critical		~	1	Total Test Errors > 3 Errors for at least > 0 minutes		ServiceN	w, Web UI				
	IPSLA Voice/Jitter Test	Network		Critical		~	1	Total Test Errors > 3 Errors for at least > 0 minutes		Web UI					
	LiveNX CPU Utilization	System		Critical		~	1	Local/Server >= 40 % for at least > 0 minutes		ServiceN	w, Web UI				
	LiveNX Disk Utilization	System		Critical		~	l	Local/Server >= 60 % for at least > 0 minutes		ServiceN	w, Web UI				
	LiveNX Memory Utilization	System		Critical		~	I	Local/Server >= 40 % for at least > 0 minutes		ServiceN	w, Web UI				
	LiveNX Node Connectivity	System		Critical		~	1	for at least > 0 minutes		ServiceN	w, Web UI				
	Media Jitter Max	Application		Critical		~	,	Jitter Max >= 10 ms for at least > 0 minutes		ServiceN	w, Web UI				
	Media Jitter Min	Application		Critical		~		Jitter Min ≻= 10 ms for at least > 0 minutes		ServiceN	w, Web UI				
	Media Packet Loss	Application		Critical		~	1	Packet Loss >= 1 % for at least > 0 minutes		ServiceN	w, Web UI				

Single threshold Alerts can be enabled/disabled by selecting the alert and clicking **Enable** or **Disable**.

ert M	anagement									Maintenance Mode	View Aler
					Liv	eNX Al	erts				
Enal	Disable								Q Search		
	ALERT TYPE	0	CATEGORY	0	SEVERITY	0	ENABLED	THRESHOLDS	SHARING		0
	Alert Type		All	~	All	~	All ~				
	Application Performance - App Delay	0	Application		Multiple		~	Multiple	ServiceNow, Web UI		
	Application Performance - Network Delay	0	Application		Multiple		~	Multiple	ServiceNow, Web UI		
-	BGP Peer Connection Change		Network		Critical			for at least > 0 minutes	Web UI		
4	Cisco IWAN Path Change		Network		Critical		~	for at least > 0 minutes	ServiceNow, Web UI		
	-Ciece IWAN-Thresheld Grossing:		Network		Critical		~	for at least > 0 minutes	ServiceNow, Web UI		
	Cisco SD-WAN SLA Class Path Change		Network		Critical		~	for at least > 0 minutes	ServiceNow, Web UI		
	Critical Traffic Response Time		Application		Critical		~	Response Time >= 1 ms for at least > 0 minutes	ServiceNow, Web UI		
	Custom OID - BHM bps		Device, Interface		<ul> <li>Info</li> </ul>			Value >= 100 bps for at least > 0 minutes	Web UI		
	Custom OID - MyOID		Device, Interface		<ul> <li>Info</li> </ul>			Value >= 100 bps for at least > 0 minutes	Web UI		
	Device CPU Utilization	0	Device, Interface		Multiple		~	Multiple	Web UI		
	Device Flow Stop		Device, Interface		Critical		~	for at least > 0 minutes	ServiceNow, Web UI		
	Device Memory Utilization	0	Device, Interface		Multiple		~	Multiple	Web UI		
	Device Reachability	0	Device, Interface		Multiple		~	Multiple	ServiceNow, Web UI		
	High WAN Interface Utilization	0	Device, Interface		Multiple		~	Multiple	Web UI		
	Interface Errors (CRC, Frame, Overruns, Ignore, Abo	rt)	Device, Interface		Critical		~	Number of Errors >= 40 Errors for at least > 0 minutes	ServiceNow, Web UI		
	Interface Reachability	0	Device, Interface		Multiple		~	Multiple	ServiceNow, Web UI		
	IPSLA Test		Network		Critical		~	Total Test Errors > 3 Errors for at least > 0 minutes	ServiceNow, Web UI		
	IPSLA Voice/Jitter Test		Network		Critical		~	Total Test Errors > 3 Errors for at least > 0 minutes	Web UI		

#### Clicking on an alert will show its configuration detail settings.

	-							BGP Peer Connection Change	
				LiveNX A	Verts				
Enat	le Disable							Enabled	
	ALERT TYPE	CATEGORY	SEVERITY	0	ENABL	ED O	THRESHOLDS	Severity	
		All	All		All	~		Critical	
		All			-			Thresholds	
	Application Performance - App Delay	Application	Multip	le		~	Multiple		
e b	Application Performance - Network Delay	Application	Multip	le		~	Multiple	For at Least	
Ŷ.	BGP Peer Connection Change	Network	Critica	4		~	for at least > 0 minutes	> 0 min	
5	Cisco IWAN Path Change	Network	Critica	4		~	for at least > 0 minutes		
	Cisco IWAN Threshold Crossing	Network	Critica	4		~	for at least > 0 minutes	Sharing	
	Cisco SD-WAN SLA Class Path Change	Network	A Critica	4		~	for at least > 0 minutes	Email	
	Critical Traffic Response Time	Application	A Critica	4		~	Response Time >= 1 ms for at least > 0 minutes	Type email	
	Custom OID - birmingham	Device, Interface	<ul> <li>Info</li> </ul>			~	Value >= 100 percent for at least > 0 minutes	Type email	
	Device CPU Utilization 0	Device, Interface	Multip	le		~	Multiple	ServiceNow	
	Device Flow Stop	Device, Interface	A Critica	4		~	for at least > 0 minutes	Servicenow	
	Device Memory Utilization	Device, Interface	Multip	le		~	Multiple	SNMP trap 💥	
	Device Reachability 0	Device, Interface	Multip	le		~	Multiple		
	Interface Errors (CRC, Frame, Overruns, Ignore, Abort)	Device, Interface	A Critica	4		~	Number of Errors >= 40 Errors for at least > 0 minutes	Veb UI	
	Interface Reachability	Device, Interface	Multip	le		~	Multiple		
	IPSLA Test	Network	A Critica	4		~	Total Test Errors > 3 Errors for at least > 0 minutes	Syslog X	
	IPSLA Voice/Jitter Test	Network	A Critica	4		~	Total Test Errors > 3 Errors for at least > 0 minutes		
	LiveNX CPU Utilization	System	A Critica	1		~	Local/Server >= 40 % for at least > 0 minutes		
	LiveNX Disk Utilization	System	A Critica	4		~	Local/Server >= 60 % for at least > 0 minutes		
	LiveNX Memory Utilization	System	A Critica	4		~	Local/Server >= 40 % for at least > 0 minutes		
	LiveNX Node Connectivity	System	A Critica	4		~	for at least > 0 minutes		
	Media Jitter Max	Application	A Critica	4		~	Jitter Max >= 10 ms for at least > 0 minutes		
	Media Jitter Min	Application	A Critica	1		~	Jitter Min >= 10 ms for at least > 0 minutes		
	Media Packet Loss	Application	A Critica			~	Packet Loss >= 1 % for at least > 0 minutes	Cancel	

Each Alert's details will have similar, yet distinct capabilities based on their respective use cases. For example, all alerts will provide the following general configuration settings:

- Enable switch
- Severity
- Threshold
- Sharing

But the level of complexity of the options presented are driven by the use case's needs.

Example of a simple, single threshold Alert:

BGP Peer Connection Change	×
Enabled On	
Severity	
▲ Critical	$\sim$
Thresholds	
For at Least > 0 min	
Sharing	
C Email	
test@test.com × X Type email	
ServiceNow	~
SNMP trap	
Veb UI	
Syslog	
Cancel	Save

Example of a complex, multi threshold/ multi-Instance Alert:

ligh WAN Interface Utilization						
IST OF INSTANCES 🚯	ADD NEW INSTANCE	INSTANCE DETAILS				
1. LiveWire Interface eth1	Enabled 📄 💼 📋	General Settings				
2. Birmingham router1	Enabled 📄 💼 🗃					
3. Austin site	Enabled 📄 💼	Instance Name		Time Wir All Hou		
Default threshold	Disabled	LiveWire Interface eth1	irs			
		Alert Source				
		Device: SE-LiveWire	-NY	Interface:	SE-LiveWire-N	$N \rightarrow eth1$
		Business Hours Setting: this setting will be ignore	For sites v d.	without busir	ness hours cor	figuration
		Business Hours Setting: this setting will be ignore Thresholds	For sites v d.			
		Business Hours Setting: this setting will be ignore	For sites v d. min		ness hours cor	
		Thresholds	d.	Automati	ic Resolution 1	ime
		Business Hours Setting: this setting will be ignore Thresholds Time to Trigger	d.	Automati 5	ic Resolution 1	ime
		Thresholds	d.	Automati 5 Utilization	ic Resolution 1	ime min
		Thresholds	d.	Automati 5 Utilization >= 60	ic Resolution 1	ime min

#### **Enable Switch**

All alerts will have at least one enable switch:



#### Severity

LiveNX provides the following severity levels for all Alerts:

- Critical
- Warning
- Info

Simple Alerts have just one severity level for the Alert's one threshold:

Severity			
▲ Critical			$\sim$
Thresholds			
Total Test Errors		For at Least	
> 3	Errors	> 0	min

While other, more complex Alerts may provide unique severities per threshold level, as well as *Time to Trigger* and *Automatic Resolution Time* settings.

Thresholds	
Time to Trigger	Automatic Resolution Time
> 15 mi	n 5 min
	Average Application Delay
CRITICAL 🔺	>= 500 ms
WARNING	Average Application Delay
WARNING	>= <b>400</b> ms
	Average Application Delay
INFO 💿	>= 100 ms
	>- 100

#### Thresholds

There are threshold options that could be present for any given type of Alert.

The following are commonly seen across many Alert types:

Average Application Delay		Packet Loss	
>= 400	ms	>= 1	%
Utilization		Drop Rate	
>= 60	%	> 20 kbps	

The Alert's threshold must be crossed for at least this time period for the Alert to trigger. A Value of 0 will immediately trigger the Alert as soon as the threshold is crossed.

For at Least	
> 0	min

#### **Time to Trigger**

The time to wait before clearing an Alert after the threshold is no longer being crossed. This will help ensure an Alert is not "noisy" when the threshold is frequently being crossed and resolved. A value of 0 will immediately trigger the Alert as soon as its threshold is crossed.

Time to Trigger	
> 0	min

#### **Automatic Resolution Time**

This value controls the duration of time that a threshold must have returned to its normal state before an Alert is cleared. This will help ensure an Alert is not "noisy" when the threshold is frequently being crossed and resolved. A value of 0 will immediately clear the alert when the threshold is resolved.

Automatic Resolu	ition Time
5	min

#### Example:

Threshold settings will work in conjunction with one another to determine when a specific alert should trigger or be cleared. The following provides a practical example of how a complex, multi-threshold alert will operate in LiveNX. The following is the configuration for a High WAN Utilization alert:

#### Thresholds

Time to Trigger		Automatic Resolution	on Time
> 1	min	4	min
		Utilization	
CRITICAL 🔺		>= 80	%
		Utilization	
VARNING		>= 60	%
		Utilization	
INFO •		>= 40	%

Time to Trigger >= 1 min

Automatic Resolution Time = 4 min Critical >= 80% Warning >= 60%

Info >= 40% (Disabled)

Next, consider the following time series graph representing a WAN interfaces utilization over time.



- 10:00am Utilization elevated over critical threshold
- 10:01am Time to Trigger exceeded, critical alert is opened
- 10:05am Utilization falls below all configured thresholds
- 10:09am Automatic Resolution Time exceeded, alert is resolved
- 10:10am Utilization elevated over critical threshold
- 10:11am Time to Trigger exceeded, critical alert is opened
- 10:15am Utilization falls below critical threshold, but above warning thresholds
- 10:19am Automatic Resolution Time exceeded, and critical alert is resolved. But Time to Trigger is exceeded and new Warning alert is opened
- 10:25am Utilization falls below all configured thresholds
- 10:29am Automatic Resolution Time exceeded, and warning alert is resolved

#### Sharing

Alerts can be shared when triggered via the following methods:

Email – Alerts can be forwarded to one or more email destinations.

ServiceNow – via API integration, LiveNX can forward its Alerts as either Events or Incidents.

- **SNMP Trap** Alert can be forwarded to an external SNMP server configured to receive traps
- WebUI Alerts will be included in the LiveNX Operations Dashboard Notification Sidebar

Syslog - Alert can be forwarded to an external Syslog server

haring	
Email	
test@test.com ×	×
ServiceNow	^
Default ServiceNow settings set on Global settings page. You ca override individual settings below.	in
Category	
Database ~	
Subcategory	Ê
DB2 v	
Add value to override	
Select override value from the list	~
SNMP trap 🔆	
🖌 Web UI	
Syslog	

Please see the Integration section of this document for configuration prerequisite for Email, ServiceNow, SNMP Traps, and Syslog sharing.

Example of the LiveNX Operations Dashboard Notification Sidebar showing Alert notifications.

LiveAction <sup>®</sup> •••				▲ 83 <b>■</b> 2 ● 0 🐥 5	ssi {−} • Ø • ¢ •	<b>å</b> **•
Enter Filter Request Here						<b>O</b> ff
s, Devices, Interfaces by Statuses				Active Alerts		=
TES: 22	DEVICES: 52	INTERFACES: 184	_	ALERTS C <sup>2</sup> KITR-DC-CORE had 236.00 ms network delay for the application traceroute KITR-DC-CORE had 236.00 ms network delay for the application invegrafile 1 RTR-SetHID GoS Class VOIC DOR Patte was GS SIX DDS	CRITICAL TRAFFIC RESPONSE TIME     RTR-DC-CORE running application Suzett      CRITICAL TRAFFIC RESPONSE TIME	2h ago  2h ago
SITES 🗗 🛛 🚯	DEVICES 2	INTERFACES	0	cEdgeART-IPFix running application rtp-audio had voice/video traffic with 200.00 ms may	RTR-DC-CORE running application Suzett	
DC-New_York Unspecified	RTR-DC-CORE     cEdgeART-IPFix	GigabitEthernet2 RTR_Birmingham     GigabitEthernet2 RTR_Seattle	n	RTR_Louisville IP SLA total test errors is greater than threshold value: 3     RTR_LosAngeles.liveaction.com IP SLA Voice/Jitter total errors is greater than threshold     RTR_Louisville IP SLA Voice/Jitter total errors is greater than threshold value: 3	() QOS CLASS DROP RTR_Seattle QoS Class VOICE Drop Rate	2h ego -
Los_Angeles Indianapolis Birmingham	RTR_LosAngeles     RTR_Indianapolis     SE-LiveWire-LA	O(Gigamon-AMI9400MTU     O(TEST-LubrizoL_Velo     I(TEST-LubrizoL_Velo		CEdgoART-IPFix running application rtp-audio had 200.00 ms of jitter for traffic with 4 DSi RTR_LosAngeles.liveaction.com running application rtp-video had 35.40 % of packet loss	QOS CLASS DROP RTR_Seattle QoS Class VOICE Drop Rate	2h ago -
Austin Seattle Tokyo	RTR_Birmingham1     SE-LiveWire-Aus     RTR_Seattle	eth0jAppleFastLane-3560     eth0jAppleFastLane-4331     eth0jFortiGate Firewall		RTR_Indianapolis running application rtp-video had 35.40 % of packet loss for traffic with     SE-LiveWire-LA running application rtp-audio had 84.23 % of packet loss for traffic with a     RTR_Birmingham1.liveaction.com running application VoIP had 8.27 % of packet loss for	VOICE, VIDEO APPLICATIONS PERFORMANCE SE-LiveWire-Aus running application Vol	2h ago -
Internet AWS_Oregon	RTR-DC-MPLS     SE-LiveWire-NY	etholick usate mewaii     etholic gamon-GTPEncryptIPFix     EtholicMonIPFixJul20		RTR_Birmingham1.liveaction.com running application VoIP had voice/video traffic with 2     SE-LiveWire-LA running application rtp-audio had 57.71 ms of jitter for traffic with a DSCR	CRITICAL TRAFFIC RESPONSE TIME RTR_Seattle running application Suzette	2h ego 
Impairment London Louisville	<ul> <li>f5-sedemo</li> <li>IWAN-BR_MPLS</li> <li>SE-F5-VE-LTM</li> </ul>	eth0jiPv6FlowDevice     Eth0jLiveWireAWS     eth0jPaloAltoNetwork Firewall		RTR_Birmingham1.liveaction.com QoS Class VOICE Drop Rate was 71.46 Kbps     RTR_Birmingham1.liveaction.com running application VoIP had 200.00 ms of jitter for tra     SE-LiveWre-Aus running application VoIP had 200.00 ms of jitter for traffic with a DSCP v	<ul> <li>APPLICATION PERFORMANCE - NETWORK DELAY</li> <li>Network delay for application avt-profile</li> </ul>	
Madison San Jose	<ul> <li>RTR_PaloAlto-Wan</li> <li>PA-MX64-B16</li> <li>CS-2960-23-22</li> </ul>	Eth0jSilverpeakMSN     eth0jVeloNetflowMar20     Eth0jVersalPFixDevice		RTR_LosAngeles.liveaction.com running application VoIP had 10.87 % of packet loss for     Local/Server memory utilization is above threshold     OSPF polling error encountered for CS-C3650-23-36.Liveaction: Request timed out t8 10.	APPLICATION PERFORMANCE - NETWORK DELAY Network delay for application traceroute	
Sydney Walnut Creek 1234567891234567891234567788	AppleFastLane-3560     AppleFastLane-4331	Eth0[VersaNetFlowDevice     eth0[VxLanRackSW		EIGRP polling error encountered for CS-C3650-23-36.Liveaction: Request timed out to 10     ISIS polling error encountered for CS-C3650-23-36.Liveaction: Request timed out to 0.10     RTR_Seattle had 208.00 ms network delay for the application secure-pop3	<ul> <li>APPLICATION PERFORMANCE - NETWORK DELAY</li> <li>Network delay for application avt-profile</li></ul>	
[TEST] é à ë î ç è ô ö Florida	ASA Firewall     AwsCM-Oregon	eth0[WLC-BasicFlowReplay     eth0[WLC-NetflowReplay		In regearder and zob.co insinermonic delay for the application secure pops     SE-LiveWire-NY had 331.33 ms network delay for the application DemoServer		

There are two types of Alerts in LiveNX:

- Single Instance Alert
- Multi-Instance Alert

#### **Single Instance Alerts**

Single Instance Alerts are global in scope. All Sites/ Devices/ Interface will share the same threshold and sharing configuration.

Below is an example of a Single Threshold Alert:

BGP Peer Connection Change	×
Enabled on	
Severity	
Critical	
Thresholds	
For at Least	
> 0 min	
Sharing	
Email	
test@test.com ×	×
ServiceNow	~
SNMP trap	
🗹 Web UI	
Syslog	
Cancel	Save

One Single Instance Alert worth noting is the QoS Class Drop Alert. This alert is global in scope and applies to all devices, but unique thresholds can be configured for each class (queue) name.

QoS (	Class Drop					>
	Severity for this ale When the severity					
Automa	atic Resolution Tir	ne				
5						min
Ignore alert.	alert fluctuations a	and wait 5	minute	s before aut	omatically re	esolving an
Thres	holds					
	Qos Class					
	VOICE					
						Ê
	Drop Rate		_	t Least		
	20	kbps	> 0	)	min	
	Oos Class					
	VIDEO					
	Drop Rate		For a	t Least		Î
	50	kbps	> 1		min	
	Catch All Thresh	old				
	Drop Rate			For at Leas	t	
	0	k	bps	> 0		min
Add	Specific QoS Clas	s Alert				

#### **Multi-Instance Alerts**

Multi-Instance Alerts help solve the following types of use cases:

- Alert when Chicago's WAN circuit is > 85% for the last 15 minutes and send a notification to just the Chicago admin.
- Alert when New York's WAN circuit is >75% utilized for the last 10 minutes and send a notification email both to the New York and Chicago admins.
- Alert when all other WAN circuits are >95% utilized for the last 15 minutes and send a notification email to an all admins.

Multi-Instance Alerts could be conceptualized like an access list found in a router or firewall. They are an ordered list of thresholds that are matched in a top-down manner. Each Instance has an Alert Source Filter that defines the Sites/Devices/Interfaces/etc. that are matched by the Instance. Once a match is found, the associated Instance's threshold will be considered for the KPI being measured and no additional Instances will be considered. If no specific Instance is matched, the KPI being measured will use the default instance, if it is enabled. If an Instance is not enabled, it will be ignored.

Below is an example of a Multi-threshold Alert:

ADD NEW INSTANCE	INSTANCE DETAILS		
Enabled 📄 🛅	General Settings		
Enabled 📄 🛅	General Settings		
Enabled 💿 🔟	Instance Name	Time Window	
Disabled	LiveWire Interface eth1	All Hours	
	Alert Source		
	Device: SE-LiveWire-NY		
	•	111	- F
	this setting will be ignored.	sites without business hours	configuration
	Thresholds Time to Trigger	Automatic Resolutio	n Time
	>1	min 5	min
		Utilization	
		>= 60	5
		Utilization	
	WARNING =	>= <b>50</b>	5
		Utilization	
	INFO •	>= <b>4</b> 0	8
	Sharings O Defa	ult Configuration O Custo	m Configuration
	Cmail		
	Email test@test.com ×		×
	Cmail		×
	Email test@test.com ×		×
	Email test@test.com X Type email		×
	Email     Itest@test.com Xi     Type email     ServiceNow		×
	Enabled D C T	Created       Image: Created Settings         Created       Image: Created Settings         Created       Image: Created Settings         Disabled       Image: Created Settings <td>General Settings General Settings General Settings General Settings General Settings Time Window University of the set of</td>	General Settings General Settings General Settings General Settings General Settings Time Window University of the set of

In this example of the High WAN Interface Utilization Alert, there are three instances enabled and the Default threshold (Instance) is disabled. This configuration ensures only interfaces matching the Alert Source Filter of these three instances can generate an alert.

The top Instance named *LiveWire interface eth1* provides the following configuration:

- The Alert Source filter that is matching Device: SE-LiveWire-NY AND Interface SE-LiveWire-NY -> ethl. This means that this instance will only apply to the utilization of this specific interface.
- The Threshold will monitor the utilization of this interface and can generate a Critical, Warning, and Info alert for it.
- The Sharing settings will send an Email notification to <u>test@test.com</u> and also populate the LiveNX Notification sidebar.

By Default, Multi-Instance Alerts only have their Default threshold configured. If enabled, all applicable Sites/Devices/Interfaces/Applications will match this instance.

IST OF INSTANCES 🚯	ADD NEW INSTANCE	INSTANCE DETAILS			
Default threshold	Enabled	General Settings			
		Instance Name	1	ime Window	
		Default Threshold		All Hours	
		Severity			
		<ul> <li>Critical</li> </ul>			
		Note: Severity for this aler the status. When the sever	t will be refle	cted as the same s	everity used in
		Alert Source			
		Alert Source			
		Alert Source			
		Alert Source Enter Filter Request Here Thresholds Time to Trigger		Automatic Resolutio	
		Alert Source Enter Filter Request Here Thresholds			
		Alert Source Enter Filter Request Here Thresholds Time to Trigger > 0		Automatic Resolutio	on Time
		Alert Source Enter Filter Request Here Thresholds Time to Trigger		Automatic Resolutio	on Time
		Alert Source Enter Filter Request Here Thresholds Time to Trigger 0 Utilization	min	Automatic Resolutio	on Time
		Alert Source Enter Filter Request Here Thresholds Time to Trigger 0 Utilization	min	Automatic Resolutio	on Time
		Alert Source Enter Filter Request Here Thresholds > 0 Utilization = 1	min	Automatic Resolutio	on Time

When a new Instance is configured, the Alert Source filter must be configured. This will define which Sites/Devices/Interfaces/Applications will match this instance.

T OF INSTANCES 🚯	ADD NEW INSTANCE	INSTANCE DETAILS		
1. New Alert	Enabled 📄 🛅 🗃	General Settings		
Default threshold	Enabled	Instance Name	Time Window	
		New Alert	All Hours	
		Severity		
		▲ Critical		
		the status. When the sev	ert will be reflected as the same verity is info, it does not contribu	ite to the status.
		the status. When the sev Alert Source Enter Filter Request He	rerity is info, it does not contribu	ite to the status.
		the status. When the sev Alert Source Enter Filter Request He Business Hours Setting this setting will be ignore	rerity is info, it does not contribu	Filter is Required ris configuration
		the status. When the sev Alert Source Enter Fitter Request He Business Hours Setting: this setting will be ignore Thresholds	refty is info, it does not contribu re . För sites without business hou ed.	Ite to the status.
		the status. When the sev Alert Source Enter Friter Request He Business Hours Setting: this setting will be ignore Thresholds Time to Trigger	Por šites without business hou d. Automatic Resolu	Ite to the status.
		the status. When the sev Alert Source Enter Fitter Request He Business Hours Setting this setting will be ignore Thresholds Time to Trigger > 0	Por šites without business hou d. Automatic Resolu	Ite to the status.

In this example, the new Instance's name is "Austin Router" and the Alert Source has been configured to only match "Device: RTR\_Austin.liveaction.com". Since Instances are matched in a top-down order, the Austin router will be measured against this specific Instance's Threshold settings and all other devices will use the Default threshold Instance.

Default threshold       Exadded         General Settings         General Settings         Instance Name       Time Window         Austin Router       All Hours         Severity       Critical         Critical       Critical         Instance Name the severity is info, it does not contribute to the status. When the severity is info, it does not contribute to the status.         Alert Source       Device:         Rest Setting: For sites without business hours configuration this setting will be ignored.         Thresholds         Time to Trigger       Automatic Resolution Time	IST OF INSTANCES ()	ADD NEW INSTANCE	INSTANCE DETAILS			
Instance Name       Time Window         Austin Router       All Hours         Severity       Critical         Critical       Critical         Note: Severity for this alert will be reflected as the same severity used it the status. When the severity is info, it does not contribute to the status.         Alert Source       Device:         Restland       Enter Filter Request Here         Busineses Hours Setting: For sites without business hours configuration this setting will be ignored.         Thresholds         Utilization         Image: Im	1. Austin Router	Enabled 📄 🛱 🗃	General Settings			
Severity  Critical  Note: Severity for this alert will be reflected as the same severity used in the status. When the severity is info, it does not contribute to the status  Alert Source  Device: RTR_Austin.liveaction.com Enter Filter Request Here  Business Hours Setting: For sites without business hours configuration this setting will be ignored.  Thresholds  Time to Trigger Automatic Resolution Time 0 min 5 min  Utilization  Utilization  I I I I I I	Default threshold	Enabled	Instance Name	Tin	ne Window	
Critical Note: Severity for this alert will be reflected as the same severity used in the status. When the severity is info, it does not contribute to the status. Alert Source Device: RTR_Austin.liveaction.com Enter Filter Request Here Business Hours Setting: For sites without business hours configuration this setting will be ignored. Thresholds Time to Trigger Automatic Resolution Time 0 min 5 min Utilization 1 1 1			Austin Router	A	All Hours	
Note: Severity for this alert will be reflected as the same severity used in the status. When the severity is info, it does not contribute to the status.         Alert Source         Device:       RTR_Austin.liveaction.com         Enter Filter Request Here         Business Hours Setting: For sites without business hours configuration this setting will be ignored.         Thresholds         Utilization         > 0       min         5       min			Severity			
the status. When the severity is info, it does not contribute to the status Alert Source Device: RTR_Austin_liveaction.com Enter Filter Request Here Business Hours Setting: For sites without business hours configuration this setting will be ignored. Thresholds Time to Trigger Automatic Resolution Time 0 min 5 min Utilization 1 1			Critical			
Device:       RTR_Austin.liveaction.com       Enter Filter Request Here         Business Hours Setting:       For sites without business hours configuration         this setting will be ignored.       Timesholds         Time to Trigger       Automatic Resolution Time         0       min         5       min         Utilization       5			the status. When the sev			
Business Hours Setting: For sites without business hours configuration this setting will be ignored.         Thresholds         Time to Trigger       Automatic Resolution Time         0       min         5       min         Utilization         1       1			Alort Courso			
Time to Trigger     Automatic Resolution Time       > 0     min       5     min       Utilization       >= 1     %				n.liveaction.com		quest Here
> 0 min 5 min Utilization > 1 %			Device: RTR_Austin Business Hours Setting:	: For sites withou		
Utilization			Device: RTR_Austin Business Hours Setting: this setting will be ignore	: For sites withou		
>= <b>1</b> %			Device: RTR_Austii Business Hours Setting this setting will be ignore Thresholds	: For sites withou ed.	nt business hours c	onfiguration
>= <b>1</b> %			Device: RTR_Austii Business Hours Setting: this setting will be ignore Thresholds Time to Trigger	: For sites withou ed. Au	t business hours of	onfiguration
			Device: RTR_Austii Business Hours Setting: this setting will be ignore Thresholds Time to Trigger > 0	: For sites withou ed. Au	t business hours of	onfiguration
Sharing O Default Configuration O Custom Configura			Device: RTR_Austii Business Hours Setting: this setting will be ignore Thresholds Time to Trigger > 0 Utilization	For sites withou ed.	t business hours of	onfiguration
			Device: RTR_Austii Business Hours Setting: this setting will be ignore Thresholds Time to Trigger > 0 Utilization	For sites withou ed.	t business hours of	onfiguration

#### **Alert Status**

Some Alerts will drive Site, Device, and Interface status on other pages in LiveNX. LiveNX status is the real-time performance state of a monitored object. The available status severities are:

- Green/ Good
- Yellow/ Warning
- Red/ Critical
- Grey/Unknown

Below are example page views that use status driven from Alerts:



, Devices, Interfaces by Statuses				Active Alerts		
				ALERTS 🗹		TIME OPENED
TES: 22	DEVICES: 52		INTERFACES: 184	RTR_Seattle QoS Class VOICE Drop F	tate was 68.48 Kbps	09 Mar 2021, 0
				<ul> <li>SE-LiveWire-Aus running application</li> </ul>	VoIP had voice/video traffic with 31.23 ms max jitter	09 Mar 2021, 0
				<ul> <li>cEdgeART-IPFix running application</li> </ul>	tp-audio had voice/video traffic with 200.00 ms max jitter	09 Mar 2021, 0
ittes 🗹 🛛 🔘	DEVICES C	0	INTERFACES	RTR_Louisville IP SLA total test error	s is greater than threshold value: 3	09 Mar 2021, 0
DC-New_York	RTR-DC-MPLS		<ul> <li>GigabitEthernet2 RTR_Birmingham1</li> </ul>	RTR-DC-MPLS running application Vi	oIP had 59.48 % of packet loss for traffic with a DSCP value of 46 (EF)	09 Mar 2021, I
Birmingham	RTR_Birmingham1		<ul> <li>GigabitEthernet2 RTR_Seattle</li> </ul>	<ul> <li>RTR_Birmingham1.liveaction.com ru</li> </ul>	nning application VoIP had 33.49 % of packet loss for traffic with a DSCP value of	09 Mar 2021, I
Indianapolis	RTR_Indianapolis		<ul> <li>GigabitEthernet2 RTR_SanJose</li> </ul>	<ul> <li>Local/Server memory utilization is al</li> </ul>	sove threshold	09 Mar 2021, I
Los_Angeles	SE-LiveWire-LA		<ul> <li>GigabitEthernet2;RTR_Louisville</li> </ul>	RTR_LosAngeles.liveaction.com IP S	LA Voice/Jitter total errors is greater than threshold value: 3	09 Mar 2021, I
Austin	RTR_LosAngeles		OlGigamon-AMI9400MTU	<ul> <li>RTR_Indianapolis running application</li> </ul>	rtp-video had 35.40 % of packet loss for traffic with a DSCP value of 0 (BE)	09 Mar 2021, I
Unspecified	SE-LiveWire-Aus		OITEST-Lubrizol_Velo	<ul> <li>SE-LiveWire-LA running application r</li> </ul>	tp-audio had 84.59 % of packet loss for traffic with a DSCP value of 46 (EF)	09 Mar 2021, I
Seattle	cEdgeART-IPFix		1/TEST-Lubrizol_Velo	RTR_LosAngeles.liveaction.com run	ing application rtp-video had 32.65 % of packet loss for traffic with a DSCP value	09 Mar 2021, I
Internet	RTR-DC-CORE		eth0(AppleFastLane-3560	RTR_LosAngeles.liveaction.com run	ing application VoIP had 10.69 % of packet loss for traffic with a DSCP value of 4	09 Mar 2021, 1
Tokyo	SE-LiveWire-NY		eth0(AppleFastLane-4331	<ul> <li>SE-LiveWire-Aus running application</li> </ul>	VoIP had 200.00 ms of jitter for traffic with a DSCP value of 46 (EF)	09 Mar 2021, 1
San Jose	RTR_Seattle		eth0[FortiGate Firewall	<ul> <li>cEdgeART-IPFix running application r</li> </ul>	tp-audio had 200.00 ms of jitter for traffic with a DSCP value of 0 (BE)	09 Mar 2021, 1
Louisville	RTR_PaloAlto-Wan		eth0(Gigamon-GTPEncryptIPFix	RTR-DC-MPLS running application Vi	IP had 200.00 ms of jitter for traffic with a DSCP value of 0 (BE)	09 Mar 2021, 1
AWS_Oregon	SEF5-VE-LTM		Eth0jGMonIPFixJul20	<ul> <li>RTR_Birmingham1.liveaction.com ru</li> </ul>	nning application VoIP had 133.59 ms of jitter for traffic with a DSCP value of 0 (BE)	09 Mar 2021, 1
Impairment	IWAN-BR_INET		eth0(IPv6FlowDevice	RTR_Birmingham1.liveaction.com Qr	S Class VOICE Drop Rate was 39.79 Kbps	09 Mar 2021, 1
London	IWAN-BR_MPLS		Eth0jLiveWireAWS	SE-LiveWire-LA running application r	tp-audio had 200.00 ms of jitter for traffic with a DSCP value of 46 (EF)	08 Mar 2021, 1
Madison	PA-MX64-B16		eth0(PaloAltoNetwork Firewall	<ul> <li>SE-LiveWire-LA running application V</li> </ul>	IoIP had voice/video traffic with 12.17 ms max jitter	08 Mar 2021, I
Sydney	CS-2960-23-22		Eth0jSillverpeakMSN	<ul> <li>LiveNX has not received flows from</li> </ul>	MPLS-CORE.liveaction.com for 1120 minutes	08 Mar 2021, I
Walnut Creek	<ul> <li>f5-sedemo</li> </ul>		eth0(VeloNetflowtMar20		tal errors is greater than threshold value: 3	08 Mar 2021, (
1234567891234567891234567788.	<ul> <li>SilverpeakAUS</li> </ul>		Eth0/VersalPFixDevice	<ul> <li>RTR-DC-MPLS running application Vi</li> </ul>	IP had 200.00 ms of jitter for traffic with a DSCP value of 46 (EF)	08 Mar 2021, (
[TEST] éà ë î ç è ô ō	RTR SanJose		EthOlVersaNetFlowDevice	RTR-DC-MPLS running application Research in the second	n'sApp had 51.78 % of packet loss for traffic with a DSCP value of 0 (BE)	08 Mar 2021, 0

Enter Filter Request He									Apply filter Mar 09, 2021 13:20:	00 → Mar 09, 2021 13:35:0	U TS Min	Configu	e su
										Q Search			
SITE NAME	SITE STATUS	0	DEVICE REACHABILITY	٥	DEVICE CPU/MEMORY	0	PEAK UTILIZATION IN	0	PEAK UTILIZATION OUT	CONGESTION DROPS	٥	INTERFACE ERRORS	
	All	~	All	~	All	~				All	~		
Austin	•		•		•			0%	0%	•			
Birmingham	•		•		•		80.4	18%	150.22%	•			
DC-New_York	•		•		•		2.3	18%	1.26%	•			
indianapoliis	•		•		•			0%	0%	•			
nternet	•		•		•			0%	0%	•			
Los_Angeles	•		•		•		0.0	18%	0.3%	•			
Seattle	•		•		•		77.4	1%	150.18%	•			
Tokyo	•		•		•		0.5	1%	0.66%	•			
Unspecified	•		•		•			0%	0%	•			
San Jose	•		•		•		53.7	'3%	100.01%	•			
AWS_Oregon	•		•		•			0%	0%	•			
Impairment	•		•		•			•		•			
London	•		•		•			16%	14.7%	•			
Louisville	•		•		•			12%	0.03%	•			
Madison	•		•		•			12%	0.03%	•			
Sydney	•		•		•			15%	0.56%	•			
Walnut Creek	•		•		•			0%	0%	•			
12345678912345678912345677	•		•		•					•			

Alerts that drive status will be designated with a badge as shown below:

ALERT TYPE	\$
Alert Type	
Application Performance - Network Delay	
BGP Peer Connection Change	
Cisco IWAN Path Change	
Cisco IWAN Threshold Crossing	
Cisco SD-WAN SLA Class Path Change	
Critical Traffic Response Time	
Custom OID - birmingham	
Device CPU Utilization	0
Device Flow Stop	
Device Memory Utilization	0
Device Reachability	0
Interface Errors (CRC, Frame, Overruns, Ignore, Abort)	·i
Interface Reachability	
IPSLA Test	
IPSLA Voice/Jitter Test	
LiveNX CPU Utilization	
LiveNX Disk Utilization	

### **Maintenance Mode**

LiveNX provides an Alert maintenance mode for temporarily suppressing Alerts from triggering from either devices or interfaces. Its configuration is accessed via the **Maintenance Mode** button at the top right of the Alert Management page.

									104	62 •	3 🐥 439		
ert M	Aanagement											intenance Mod	View Alert
				Live	NX Ale	rts						 	
Ena	able Disable										Q Search		
	ALERT TYPE	CATEGORY	0 8	IEVERITY	0	ENABLED	0	THRESHOLDS		SHARING			0
		All	×	All	~	All	~						
	Application Performance - App Delay	Application		Multiple		~		Multiple		Web UI			
	Application Performance - Network Delay	Application		Multiple		~		Multiple		Service	Now, Web UI		
	BGP Peer Connection Change	Network		Critical		~		for at least > 0 minutes		Email, V	Veb UI		
	Cisco IWAN Path Change	Network		Critical		~		for at least > 0 minutes		Service	Now, Web UI		
	Cisco IWAN Threshold Crossing	Network		Critical		~		for at least > 0 minutes		Service	Now, Web UI		
	Cisco SD-WAN SLA Class Path Change	Network		Critical		~		for at least > 0 minutes		Service	Now, Web UI		
	Critical Traffic Response Time	Application		Critical		~		Response Time >= 1 ms for at least > 0 minutes		Service	Now, Web UI		

By default, no devices or interfaces are in maintenance mode. Click **Add**, to enable maintenance mode.

Maintenance Mode	×
Devices and Interfaces under Maintenance	ADD

A list of devices appears.

Maintenance Mode	×
Add Devices and Interfaces under Maintenance	SAVE
Enter Filter Request Here	Apply filter
Sort by: Name ~	
« < Page 1 / 3 > »	
✓ ♦ AppleFastLane-3560	
✓ ♦ AppleFastLane-4331	
✓ ♦ ASA Firewall	
AwsCM-Oregon	
✓ ♦ AzureCM-USWest	
✓ ♦ cEdgeART-IPFix	
S-2960-23-22	
✓ ♦ CS-C3650-23-36	
✓ S CS-C3850-23-31	

The filter at the top of the device list makes it simple to find devices of interest.

Maintenance Mode	×
Add Devices and Interfaces under Maintenance	SAVE
Enter Filter Request Here	Apply filter
Site	
Device	
Тад	
✓	<sup>i</sup>
✓ ♦ ASA Firewall	
V 😔 AwsCM-Oregon	
V 😵 AzureCM-USWest	
✓ S cEdgeART-IPFix	
S CS-2960-23-22	
✓ S CS-C3650-23-36	
✓ S CS-C3850-23-31	
V 😵 f5-sedemo	
✓ SortiGate Firewall	

Maintenance Mode		×
Add Devices and Interfaces under Mainte	enance	SAVE
Device: RTR_Austin.liveaction.com	Enter Filter Request Her App	ly filter
Sort by: Name ~		
<pre>《 Page 1 / 1 &gt; 》</pre>		

Select the checkbox corresponding to a device to put the device and all of its interfaces into maintenance mode. When finished click **Save**.

Maintenance Mode	×	
Add Devices and Interfaces under Maintenance	SAVE	
Device: RTR_Austin.liveaction.com Enter Filter Requestion	y filter	
Sort by: Name ∽	_	
≪ < Page 1 / 1 > ≫	<b></b>	_
∧ 😵 RTR_Austin		ļ
Gi5		
GigabitEthernet2	<b>~</b>	
GigabitEthernet3		
GigabitEthernet4	<b>~</b>	

Or only select the checkbox corresponding to just an interface(s) to put it in maintenance mode. When finished click **Save**.

Maintenance Mode		×
Add Devices and Interfaces under Mainte	enance	SAVE
Device: RTR_Austin.liveaction.com	Enter Filter Request He	Apply filter
Sort by: Name 🗸		
<pre>《 &lt; Page 1 / 1 &gt; 》</pre>		<b>~</b>
∧ 😵 RTR_Austin		1/4 -
Gi5		
GigabitEthernet2		
GigabitEthernet3		
GigabitEthernet4		

The selected devices and interfaces will be listed in Maintenance Mode.

evices and Interfaces under Maintenance	EDIT
Enter Filter Request Here	Apply filter
<pre>% &lt; Page 1 / 1 &gt; &gt;&gt;</pre>	
∧ ⊗ RTR_Austin	
Gi5	
GigabitEthernet2	
GigabitEthernet3	
GigabitEthernet4	

To remove a device/interface from maintenance mode, click Edit.

Maintenance Mode	×
Devices and Interfaces under Maintenance	EDIT
Enter Filter Request Here	Apply filter
≪ < Page 1 () / 1 > ≫	

Deselect the selected devices and interfaces of interest and click Save.

Maintenance Mode		×
Add Devices and Interfaces under Maintenance		SAVE
Device: RTR_Austin.liveaction.com	Enter Filter R	Apply filter
Sort by: Name ~		
≪ < Page 1 € /1 > ≫		
∧ ⊗ RTR_Austin		
Gi5		
GigabitEthernet2		
GigabitEthernet3		
GigabitEthernet4		

### **Application Management**

Application Management provides the ability to define Custom Applications for Flow data in LiveNX and assign Applications Groups for simplified application management.

۶	Configure
	Alert Management
	Application Management
	OID Polling
	Device Management
	Filter Management
	Site Management

#### **Custom Applications**

LiveNX will represent Flow data by application name for various reports, dashboards, topologies, and alerts. By default, LiveNX will try to learn the application identity of Flow, but when this is not possible or an alternate definition is desired, custom names can be used for identifying traffic as desired. Custom names will override any other auto learned application identification method.

LiveNX can use a combination of the following delimiters for defining custom applications:

- IP Addresses
- Ports
- Protocols
- DSCPs
- Application Names
- URLs

To add the first custom application, from the Custom Applications tab, click Add Custom Application.

Application Management	View WAN Applications
Custom Applications	Application Groups
You have not added any	custom applications yet
Add Custor	n Application

The Add Custom Application modal appears.

The custom application can be based on either Network Attributes or HTTP Host or SSL Common Name.

Name *	Description
Enter Custom Application Name	Enter Custom Application Description
Network attributes	
IP Ranges	Include Application
Specify IPs or IP ranges (ex: 192.168.1.1-192.168.1.200)	Start typing for more results
Layer 4 Protocol	Port Ranges
Specify protocols. Matches any protocol by default	
DSCP	
Specify DSCP classes	
URLs	
HTTP host or SSL common name	URI
You can use wildcards in host names	You can use wildcards in UR

When Network Attributes are selected, any combination of IP range, application, layer 4 protocol, port range, or DSCP can be used. Like kind options use OR logic and different kind options use AND logic.

In the following example, the layer 4 protocol must be UDP and port must fall into the range of 19400-19440 for a Flow to be classified as VoIP:

Name *		Description		
VoIP		My VoIP Traffic		
O Network attributes				
IP Ranges		Include Application		
Specify IPs or IP ranges (ex: 192.168.1.1-192.168.1.200)		Start typing for more results		
Layer 4 Protocol Add	ded: 1	Port Ranges		
UDP ×	×	19400-19440		
Select protocol				
DSCP				
Specify DSCP classes				
URLs				
HTTP host or SSL common name		URI		
You can use wildcards in host	names		You can use w	vildcards in UR
			Cancel	Save

In this example, the IP address 172.16.200.10 or 172.16.200.11 would be classified as Citrix:

Name *		Description
Citrix		Enter Custom Application Description
O Network attributes		
IP Ranges	Added: 2	Include Application
172.16.200.10 × 172.16.200.11 ×	×	Start typing for more results
Specify IPs or IP ranges (ex: 192.168.1.1-192.168.1.2		
Layer 4 Protocol		Port Ranges
Specify protocols. Matches any protocol by default		Specify ports or port ranges (ex: 2427-2430), one per line
DSCP		
Specify DSCP classes		
URLs		
HTTP host or SSL common name		URI
You can use wildcards in	host names	You can use wildcards in UF

After defining the Custom Application, click **Save**. The list of applications appears on the *Custom Applications* tab.

olicati	ion Manag	gement								View WAN Application
			Custom Application	ns				Application Group	s	
Add	Edit	Delete Move Up	Move Down						Q Search	
F	RANK	APPLICATION NAME	IP RANGES	PORT RANGES	LAYER 4 PROTOCOL	DSCP	NBAR APPLICATIONS	HTTP HOST	URI	DESCRIPTION
	Rank	Application Name								
	1	VolP		19400-19440	UDP					My VoIP traffic
	2	Citrix	172.16.200.10, 172.16.20							

To edit a custom application, select the desired application and click Edit.

catio	on Manag	ement									View WAN App	plication
			Custom Application	ns				Application Grou	ips			
dd	Edit	Delete Move Up	Move Down						Q Search			
RJ	ANK	APPLICATION NAME	IP RANGES	PORT RANGES	LAYER 4 PROTOCOL	DSCP	NBAR APPLICATIONS	HTTP HOST	URI	D	ESCRIPTION	
	Rank											
	1	VolP		19400-19440	UDP						My VoIP traffic	
	2	Citrix	172.16.200.10, 172.16.20									

The Edit Custom Application modal appears. Make any desired changes and click Save.

≡	Live∧c				<b>▲</b> 280	= 11	• 18	146588	{−} ₹	0 - ¢	•
Applica	tion Manag	jement								View W	VAN Applications
			Custom Applica				slication Grou	ups			
				EDIT CUSTOM APPLICATION		×					
Add	Edit	Delete Move Up	Move Down	Name *	Description			Q Search			
	RANK	APPLICATION NAME	IP RANGES	Citrix	My Citrix Traffic			URI		DESCRIPTION	
			IP Ranges	<ul> <li>Network attributes</li> </ul>							
	1	VoIP		IP Ranges Added: 2	Include Application					My VoIP tra	ffic
	2	Citrix	172.16.200.10, 172.16.20.	172.16.200.10 × 172.16.200.11 × × Specify IPs or IP ranges (ex: 192.168.1.1-192.168.1.200)							
				Layer 4 Protocol	Port Ranges						
				Specify protocols. Matches any protocol by default							
				DSCP							
				OURLS							
				HTTP host or SSL common name	URI						
				You can use wildcards in host names	You can use wildcards in	URI					
					Cancel Save						
Rows	2/2 Se	lected: 1									

**Note** It is possible to have multiple Custom Application definitions with the same name, this ensures the most flexibility in naming applications as desired.

cau	ion Manag	ement								View WAN Applicatio
			Custom Application	ns				Application Grou	ps	
dd	Edit	Delete Move Up	Move Down						Q Search	
R	lank	APPLICATION NAME	IP RANGES	PORT RANGES	LAYER 4 PROTOCOL	DSCP	NBAR APPLICATIONS	HTTP HOST	URI	DESCRIPTION
	Rank	Application Name								
	1	VolP		19400-19440	UDP					My VoIP traffic
	2	Citrix	172.16.200.10, 172.16.20							
			172.10.200.10, 172.10.20							My Citrix Traffic
	3	VoiP	172.10.200.10, 172.10.20	19500	UDP	EF				My Citrix Traffic My VoIP Traffic 2
			17210.200.10, 17210.20-	19500	UDP	EF				
			17210.200.10, 17210.20-	19500	UDP	EF				
			17210200.10,1721020-	19500	UDP	ĒF				
			17210200.10,1721020-	19500	UDP	6F				
			1721020010 1721020-	19500	UDP	EF				
			1721020010 1721020-	19500	UDP	ĘF				

In this example there are two custom applications with the name "VoIP".

Custom Applications are a prioritized list of definitions. Traffic is matched in a top-down order. In large configurations, it is often best to ensure the most frequently used applications are placed higher in the list to ensure optimum performance.

To change the priority order of a custom application, select the application and click either **Move Up** or **Move Down**.

			Custom Application	ns				Application Groups		
dd	Edit	Delete Move Up	Move Down						Q Search	
RJ	ANK	APPLICATION NAME	IP RANGES	PORT RANGES	LAYER 4 PROTOCOL	DSCP	NBAR APPLICATIONS	HTTP HOST	URI	DESCRIPTION
		Application Name								
	1	VolP		19400-19440	UDP					My VoIP traffic
	2	Citrix	172.16.200.10, 172.16.20							My Citrix Traffic
	3	VoIP		19500	UDP	EF				My VoIP Traffic 2
	3	VolP		19500	UDP	EF				
	3	VelP		19500	UDP	EF				
	3	VolP		19500	UDP	EF				
	3	VolP		19900	UOP	6F				
	3	VolP		19500	UCP	6F				
	3	VolP		19900	UCP	61				

In this example, Citrix has been moved down to lower its match priority.

sati	on Manag	ement								View WAN Applicat
			Custom Application	ns				Application Groups	s	
dd	Edit	Delete Move Up	Move Down						Q Search	
	Edit	indre op							C. OCOTOLL	
F	ANK	APPLICATION NAME	IP RANGES	PORT RANGES	LAYER 4 PROTOCOL	DSCP	NBAR APPLICATIONS	HTTP HOST	URI	DESCRIPTION
		Application Name								
	1	VolP		19400-19440	UDP					My VoIP traffic
	2	VolP		19500	UDP	EF				My VoIP Traffic 2
	3	Citrix	172.16.200.10, 172.16.20							My Citrix Traffic

Custom applications can also be defined using HTTP Host or SSL Common Name. Optionally, UIR can also be included.

When defining custom applications in this manner, it is possible to use "\*" for wildcard matching of sub-domains.

Name *	Description
MyWebsite	My WebSite Traffic
Network attributes	
IP Ranges	Include Application
Layer 4 Protocol	Port Ranges
DSCP	
O URLS	
HTTP host or SSL common name	Added: 2 URI
mywebsite.com ×         *.mywebsite.com ×           Enter HTTP host or SSL common name. Ex.: *.web	
	in host names You can use wildcards in

### **Application Groups**

Applications Groups can be used for simplified application management. For example, an application can be identified by different names by various manufactures, hardware models, and even different version of OS from the same device type. To help simplify inconsistent names Application Groups can be used.

LiveAction LiveNA will also use these Application Groups to identify which applications need residual monitoring for baselining and anomaly detection.

 Application Management
 Custom Applications

 Custom Applications
 Application Groups

 Vou Have not added any application groups yet
 Add Application Croup

To add the first application group, from the Application Group tab, click Add Application Group.

The Add Application Group modal appears.

Group Name nclude Application * Start typing for more results	Group Name *	
	Group Name	
Start typing for more results	nclude Application *	
	Start typing for more results	

Provide a name and add the desired applications to the group. When finished, click Save.

AllVoIP					
nclude Applicat	ion *			A	dded: 7
cisco-collab-a	udio ×	cisco-phone-	audio ×	cisco-jabber-audio	××
codima-rtp ×	rtp ×	rtp-audio ×	VoIP ×		
Start typing for	r more r	esults			

To edit the Application Group, select the group and click Edit.

Letter       Applications         And       Edit       Central         And a	Applic	ation Management			View WAN Applications
Add       Edd       Q. clauch.         APPLICATION CROOP       0       APPLICATIONS         Participation Group       Replications       Image: Clauch C	Applica	ation Management			view walk Applications
APPLICATION IS GROUP               APPLICATION IS GROUP               Application Group              Applications                ANVOP              cisco-collab-audio, cisco-phone-audio, codima-rtp, rtp, rtp-audio			Custom Applications	Application Groups	
Application Chaup       Applications         IMARP       cisco collab audio, cisco jabber-audio, codimart(p, t(p, t(p-audio)))	Add	Edit Delete			Q Search
ANVOIP       cisco-collab-audio, cisco-jabber-audio, cisco-jabber-		APPLICATION GROUP	APPLICATIONS		
		AllVoIP	cisco-collab-audio, cisco-phone-audio, cisco-jabber-audio, codima-rtp, rtp, rtp-audio		
KOWS: 1/1 SELECTED: 1	Row	s: 1 / 1 Selected: 1			

Update the group and when finished, click Save.

			View WAN Applications
Custom Applications		Application Groups	
		Q Search	
APPLICATIONS			
Applications			
cisco-collab-audio, cisco-phone-audio, cisco-jabber-audio, codin	EDIT APPLICATIONS GROUP		
	Group Mane * _AllvolP Include Application * Added. 7 		
			View WAN Applications
Custom Applications		Application Groups	View WAN Applications
Custom Applications		Application Groups	View WAN Applications
Custom Applications			View WAN Applications
			View WAN Applications
APPLICATIONS	-rtp, rtp, tp-audio, VoP		View WAN Applications
	APPLICATIONS	APPLCATIONS  Cisco collab-audio, cisco jabber-audio, codi  EDIT APPLICATIONS GROUP  Group Name *  AVer  Include Application *  Added 7  Cisco-collab-audio ×  Cisco-phone-audio ×	APPLICATIONS  Applications  Cisco collab-audio, cisco jabber-audio, cod  EDIT APPLICATIONS GROUP  Group Name *  AlvelP  Include Application *  Added: 7  Cisco-collab-audio × (cisco phone-audio × x (codmartp × rtp-audio × VoP ×  Bart typing for more results

# **OID Polling**

OID Polling allows you to monitor and alert on SNMP KPIs that are not monitored by default.



OID Polling provides two tabs:

- Pre-Configured
- Custom

### **Pre-Configured**

This tab provides built-in use cases.

OID Polling					Configure OID Alerts
	Pre-Configured		Cu	stom	
				Q Search	
TECHNOLOGY 🗘	orbs	¢	DEVICES		0
CEQFP	ceqfpThroughputLevel				
HSRP	cHsrpGrpVirtuallpAddr, cHsrpGrpActiveRouter, cHsrpGrpStandbyRouter, cHsrpGrpStandbyState				
VRRP	vrrpOperVrld, vrrpOperVirtualMacAddr, vrrpOperState, vrrpOperMasterIpAddr, vrrpOperPrimaryIpAddr				
Rows: 3 / 3					

Clicking a pre-configured use case opens the *Edit Technology* modal.

		Pre-Configured
TECHNOLOGY	0	oros
Technology		
CEQFP		ceqfpThroughputLevel
HSRP		cHsrpGrpVirtualIpAddr, cHsrpGrpActiveRouter, cHsrpGrpStandbyRouter, cHsrpGrpStandbyState
VRRP		vrrpOperVrld, vrrpOperVirtualMacAddr, vrrpOperState, vrrpOperMasterlpAddr, vrrpOperPrimarylpAddr

#### Select the device(s) of interest and click Save.

<u>(</u> )	This use case will poll the	e fol	lowing OID: ceqfpThrou	ghput	Level					
Al	devices will be polled for	this	OID 🚯							
								Q Search		
	DEVICE	\$	SITE	\$	IP ADDRESS	\$ VENDOR	\$ MODEL	\$ TAGS	\$ DESCRIPTION	0
	Device						Model			
	NewYorkEdge		NewYorkEdge		10.1.2.211	Viptela	vedge-cloud	one	Viptela SNMP agent	
	IWAN-BR_INET		Site 5		10.100.51.32	Cisco	ciscoCSR1000v		Cisco IOS Software, CS	
	RTR_SanJose		PaloAlto-VE-01		10.100.51.12	Cisco	ciscoCSR1000v		Cisco IOS Software [De	
Row	s: 32 / 32									

### Custom

This tab allows for user defined OIDs

From the *Custom* tab, click **Add Custom OID**.

OID Polling	Configure OID Alerts
Pre-Configured	Custom
You have not create	d any OIDs yet
Add Guston	n 010

The Add OID modal appears.

From the General tab, enter the Name, OID Index, and Units.

	General	Devices (0)	
Name *		OID Index * 📵	
MyCustomOID		.1.3.6.1.4.1.9.9.48.1.1.1.6.1	
rocessing Type 🚯		Units *	
None	~	Mb	
onversion Type 🚯		Conversion Factor * 🚯	
		Conversion Factor	
Multiply	~	1	
	v		
	v		
	v		
	v		
	v		

From the *Devices* tab, select the device(s) that should be polled with this OID.

#### When finished click **Save**.

		General							Devices (1)		
AI	I devices will be polled for thi	s OID 📵									
lote:	At least one device is require	d. Make sure that the curre	ent O	ID is configured for all s	selecte	ed devices.			Q Search		
	DEVICE $\Diamond$	SITE	¢	IP ADDRESS	¢	VENDOR 0	MODEL	¢	TAGS	0	DESCRIPTION
	Device										
	vSmart			10.4.201.216		Viptela	vsmart				
<b>×</b>	RTR_Louisville	Louisville		10.100.51.10		Cisco	ciscoCSR1000v				Cisco IOS Software [De
	HE-CSR-207	PaloAlto-VE-01		10.4.201.207		Cisco	ciscoCSR1000v				Cisco IOS Software, CS
	PaloAltoEdge-TLOC-Ext	PALOALTO		10.4.201.214		Viptela	vedge-cloud				
	CS-2960-23-22	Site 5		10.100.51.22		Cisco	catalyst29608TCS				Cisco IOS Software, C2
	RTR-DC-CORE	New York - DC		10.100.51.3		Cisco	ciscoCSR1000v				Cisco IOS Software, CS
	RTR_Madison	Madison		10.100.51.11		Cisco	ciscoCSR1000v				Cisco IOS Software [De
	RTR_PaloAlto-Wan	Site 5		10.100.51.14		Cisco	ciscoCSR1000v				Cisco IOS Software, CS
Row	rs: 32 / 32 Selected: 1			40 400 24 0		A1					ai iana ti fa

The Custom OID will be added to the Custom tab.

D Polling						Configure OID Alerts
Pre-Configure	Custom					
Add Edit Delete					Q Search	
NAME	OID INDEX 🗘	UNITS \$	PROCESSING TYPE \$	DEVICES		0
			All ~			
MyCustom0ID	.1.3.6.1.4.1.9.9.48.1.1.1.6.1	Mb	None	RTR_Louisville		
Rows: 1 / 1						

To edit the custom OID, select th OID and click **Edit**.

Polling	g									Configure OID Aler
Pre-Configured			Custom							
Add	Edit Delete							Q Search		
NJ	ame 🗘	OID INDEX	0	UNITS 🗘	F	PROCESSING TYPE 🗘	DEVICES			
1						All ~				
M	lyCustomOID	.1.3.6.1.4.1.9.9.48.1.1.1.6.1		Mb	١	None	RTR_Louisville			
	/1 Selected: 1									

After a custom OID rule is created, a corresponding Alert will automatically be created.

	LiveN	IX Alerts					
		LIST OF INSTANCES	ADD NEW INSTANCE	INSTANCE DETAILS			
Enable Disable			Default threshold				Disabled
	ALERT TYPE 0	CATEGORY					
		All			Instance Name	Time Window	
	Cisco SD-WAN Performance - Network Delay	Network			Default Instance	All Hours 🗸	
	Cisco SD-WAN Performance - Packet Loss	Network			Alert Source		
	Cisco SD-WAN SLA Class Path Change	Network					
	Critical Traffic Response Time	Application					
Ť	Custom OID - MyCustomOID Device, Interface				Thresholds		
j.	Device CPU Utilization 8	Device, Interface			Time to Trigger	Automatic Resolution Time	
	Device Flow Stop	Device, Interface			> 0 min	5 min	
	Device Memory Utilization (3)	Device, Interface					
	Device Reachability (3	Device, Interface				Value	
	Fan Tray Operational State	Device, Interface			CRITICAL A	>= 30 Mb	
	High WAN Interface Utilization	Device, Interface					
	HSRP Standby State	Network				Value	
	Interface Errors (CRC, Frame, Overruns, Ignore, Abo	Device, Interface			WARNING	>= 20 Mb	
	Interface Reachability	Device, Interface					
	IPSLA Test	Network					
	IDCL & Vision/ littler Test	Maturali					

Additionally, a Custom OID report will be automatically created too.
CREATE REPORT							×
GENERAL SETTINGS		REPORT LIST	F	REPORT DETAILS			
Name	Â	Please choose report type		Q Search			Â
		Add New Report +					
Presentation Mode				Top Reports			
Standard ~				🕀 Test			
				LiveNA			=
Footnote	=			Flow			
			L	SNMP			
Sharing Settings				Availability		~	
Email				Custom OID		^	
Enter an email address or AD entity			i.	Custom OID			
File Format			1.	IPSLA			
Send PDF Send CSV						~	
PDF Row Limits				Interface		~	-
	Ŧ			ΙΔN		~	Ŧ
					Cancel	Save As Template	Execute

# **Device Management**

Device Management provides the ability to add devices into LiveNX's inventory and configure their monitoring settings.

۶	Configure	
	Alert Management	
	Application Management	
	OID Polling	
	Device Management	
	Filter Management	
	Site Management	

There are two types of monitored devices in LiveNX:

- SNMP Monitored Devices
- Non-SNMP Monitored Devices

### **SNMP Monitored Devices**

LiveNX will collect SNMP and Flow from these devices.

To add an SNMP Monitored device into LiveNX, select the **Discover Devices** button.

Note that appendent         Output         Output         Output         Output         Add Non SAMP Output           Monopolity         Output         Monopolity         Output         Monopolity         Output         Monopolity         Output         Monopolity         Output         Monopolity         Output         Monopolity         Output         Monopolity         Output         Ou	reAction 🛚 🛤 💷			▲ 100 = 55 • 2 ▲ 318 {-} · ② · ③ · ▲ ·
Edit         Refresh.List         Configure         Delefe         Rediscover Interfaces           Edit         Refresh.List         Configure         Delefe         Rediscover Interfaces         V	igement 🔍		CSV Import/Export ~ Cre	
	My Devices (0)	My Interfaces (0)	Discovered Devices (0)	③ Autodiscovery (13)
	Refresh List Configure Delete Rediscover Interfaces			Q. Search
Image: Second	VICE 0 DEVICE STATE 0 IP ADDRESS 0 VENDOR 0 MODE	a. O Node O Site O Interfaces	0 POLL 0 005 0 FLOW 0 IP-SLA	O ROUTING O LAN O TAGS O INTERVAL
	Device All v IP Address All v Mo		Al v Al v Al	▼ AI ▼ AI ▼ Tops AI ▼
	Device Alt V PAddress Alt V Mo		II v IA v Al	V     All     V     Taps     All
No Data		No	Data	

The Discover Devices workflow appears, highlighting the What to Scan tab.

-		
O SPECIFY IP RANGES		
IP Range (ex. 192.168.1.1 - 200) or CIDR Notation, or one per line Choos	se a site 🗸 🗸	
IP address	Hops	
	Save & I	Next

One or more devices can be added into LiveNX's inventory by either:

- 1. Specifying an IP address or a range of addresses.
- 2. Discovery by specifying a Seed device IP and the number hops away.

In this example, a single IP address is specified.

Click Save & Next to choose the SNMP configuration for monitoring these devices.

1. What to scan	2. SNMP Settings	3. No	ie
O SPECIFY IP RANGES			
10.100.51.10		e a site 🛛 🗸	
Add More			
SPECIFY SEED DEVICE TO SCAN			
IP address		Hops	
			Save & Next
			Save a NEXT

SNMP Settings can be selected using either:

1. Using the Default SNMP Connection Settings.

1. What to s	can	2. SNMP Settings	3. Nod	е
	NECTION SETTINGS age Configuration Page CTION SETTINGS FOR TI	HIS DEVICE		
Back				Save & Nex

Tip If desired, the default SNMP credentials can be managed by selecting the SNMP Credential Store Configuration Page button.

2. Entering the specific SNMP Connection Settings for this Device(s).

1. What to scan	2. SNMP Settings	3. Node
DEFAULT SNMP CONNECTION SETTIN	GS	
ENTER SNMP CONNECTION SETTING	S FOR THIS DEVICE	
SNMP Version *	Target Port *	
Version 2c	~ 161	
Community String *		
Enter Community String		
Back		Save & Ne

Click Save & Next to choose the LiveNX Node that monitors the device(s).

1. What to scan	2. SNMP Settings	3. Node	
Specify Node			
Local/Server			$\sim$
Back			

When ready, click *Discover*.

The *Discover Devices* modal closes, and a discovery progress bar is displayed.

		<u>a</u> 100	■ 55 • 2 🌲 318 {-}	<b>⇔</b> - <b>≛</b> /2/.•
Device Management		CSV Import/Export ~ Credential Store	View Devices Add Non SNMP Device	Discover Devices
My Devices (0)	My Interfaces (0)	Discovered Devices (1)	② Autodiscovery (0)	
DISCOVERY LOGS: 1/1				
_				
Stop				

Once discovery is complete, any found devices will be added to the *Discovered Devices* tab. These devices can be added into the inventory by clicking **Add All Devices**. The device(s) is added with the default discovered interfaces and settings. These settings can be changed later.

	agement 60						CSV Import/Export ~	Credential	Store View Devices	Add Non SNMP Device	Discover Devi
	My Devices (0)			My Interfaces (0)		Disco	overed Devices (1)		0	Autodiscovery (13)	
					i						
SELE	CT DEVICES										
	Edit								Q Search		
	DEVICE	÷	SERIAL	\$ IP ADDRESS	VENDOR	MODEL	÷	NODE	\$	INTERFACES	0
	RTR_Louisville		9E3XJK8MTIX	10.100.51.10	Cisco	ciscoCS	SR1000v	Local/Ser	ver	5	
	/ 1										

Or the devices' settings can be updated by selecting the device(s) of interest and clicking Edit.

							▲ 100 <b>■</b>	55 • 2 🌲 318	{-} • • •	•• <b>*</b> •••
Device Management					CSV Import	Export ~	Credential Store	View Devices	Add Non SNMP Device	Discover Devices
My Devices (0)		My Interfaces (0)			Discovered Devices (1)			C	Autodiscovery (13)	
1/2 SELECT DEVICES Devices: 1 Interfaces: 5 Add All Devices Edit			Select					Q Search		
DEVICE 🗘 SERIAL	0	IP ADDRESS	VENDOR	¢	MODEL	¢	NODE	0	INTERFACES	\$
Device Serial										
RTR_Louisville 9E3XJK8N	TIX	10.100.51.10	Cisco		ciscoCSR1000v		Local/Server		5	
All rows / 1										
										Select Interfaces

Site	Group		Interval	
(no site selected)	✓ No Group Selecte	d ~	1 Minute	~
P Address*				
10.100.51.2				
POLL IP SLA	QOS	ROUTING	FLOW	LAN
Associate Probe at IP Address	Hardcode Sample F	tatio		
Type IP Address	1/			
Tags				

Or the monitored interfaces can be updated by selecting the device(s) of interest and clicking **Select Interfaces**.

Management <sup>©</sup>								CSV Import/Export ~	Credential Store	View Devices	Add Non SNMP De	evice Discover Devi
My	levices (0)			My Interfaces (0)			Discovered De	vices (1)			<ol> <li>Autodiscovery (13)</li> </ol>	3)
SELECT DEVICES Dev	ices: 1 Interfaces: 5											
					Se	lected: 1				Q Search		
Add All Devices Edit										~		
Add All Devices Edit	¢	SERIAL	0	IP ADDRESS	C VENDOR		MODEL	¢	NODE		INTERFACES	
	٥	SERIAL Serial	٥	IP ADDRESS			MODEL	٥	Node			4

Monitored Interfaces can be chosen by ensuring their corresponding check box is selected.

	My Devic	es (34)		My Inte	rfaces (123)		_	Disc	overed Devices (1)			<li>② Autodiscovery (</li>	))
SELE	CT INTERFACES Dev	ices: 1 Interfaces: 5											
Edit						Selec	cted: 4				Q Sear		
	NAME ¢	INTERFACE STATE	DEVICE \$	LINE RATE (Kbps)	IP ADDRESS \$	LABEL	0	INPUT CAPACITY (K 🗘	OUTPUT CAPACITY (_ 🗘	WAN/XCON ¢	SERVICE PROVIDER	TAGS O	DESCRIPTION
		All ~	All ~							All 🗸	All ~		
	GigabitEthernet2	Up	RTR_Louisville	1000000	199.199.1.5	Conn-MPLS-Pro	ovider			WAN	Conn-MPLS-Provider		Conn-MPLS-Provid
	GigabitEthernet1	Up	RTR_Louisville	1000000	10.100.51.10								Connected to Mgn
	GigabitEthernet3	Up	RTR_Louisville	1000000	192.168.101.254								Conn-AdminSE-PC
	NullO	Up	RTR_Louisville	10000000									
	VolP-Null0	Up	RTR_Louisville	10000000									

Selected monitored interface settings can also be updated by clicking Edit.

	anagement	(and 10.0)					-4 (400)				and Devices (A)					
	My Dev	ices (34)				My Int	erfaces (123)			Disc	overed Devices (1)				② Autodiscovery (	
SELE	ECT INTERFACES De	wices: 1 Interfaces	5													
Edit									Selected: 2					Q Search		
	NAME C	INTERFACE STATE	0	DEVICE	0	LINE RATE (Kbps)	IP ADDRESS	0	LABEL 🗘	INPUT CAPACITY (K_	OUTPUT CAPACITY ( 🗘	WAN/XCON 🗘	SERVIC	E PROVIDER 🗘	TAGS Ô	DESCRIPTION
		All	~	All	~							All V	All	~		
<b>~</b>	GigabitEthernet2	Up		RTR_Louisville		1000000	199.199.1.5		Conn-MPLS-Provider			WAN	Conn-P	MPLS-Provider		Conn-MPLS-Provider
	GigabitEthernet1	Up		RTR_Louisville		1000000	10.100.51.10									Connected to Mgmt.
~	GigabitEthernet3	Up		RTR_Louisville		1000000	192.168.101.254									Conn-AdminSE-PC
	NullO	Up		RTR_Louisville		10000000										
	VoIP-Null0	Up		RTR_Louisville		10000000										
I rows Back	, s															+ Add Selecter
															-	+ Add Selected
															]	+ Add Selected

Service Provider
Conn-MPLS-Provider
Cancel Apply

Once Finished, click **+Add Selected**.

	My Devi	ces (34)		My Inte	erfaces (123)	_	Disc	overed Devices (1)			⑦ Autodiscovery (	
SELI	ECT INTERFACES De	vices: 1 Interfaces: 5										
Edit						Selecte	ed: 2			Q Searc		
	NAME O	INTERFACE STATE	DEVICE 0	LINE RATE (Kbps)	IP ADDRESS	LABEL	○ INPUT CAPACITY (K_ ○	OUTPUT CAPACITY ( 🗘	WAN/XCON 0	SERVICE PROVIDER	TAGS O	DESCRIPTION
		All 🗸	All ~						All ~	All ~		
<b>~</b>	GigabitEthernet2	Up	RTR_Louisville	1000000	199.199.1.5	Conn-MPLS-Prov	ider		WAN	Conn-MPLS-Provider		Conn-MPLS-Provider
	GigabitEthernet1	Up	RTR_Louisville	1000000	10.100.51.10							Connected to Mgmt.
<b>~</b>	GigabitEthernet3	Up	RTR_Louisville	1000000	192.168.101.254							Conn-AdminSE-PC
	NullO	Up	RTR_Louisville	10000000								
	VoIP-Null0	Up	RTR_Louisville	10000000								

The Device will now be listed on the My Devices tab with a summary of their configuration.

	gement 🙆																		CSV Impor	t/Export		Credentia	Store	View D	miner	Add	ion Shill	IP Device		Discover D	Davied
	gement -										442										×	Credentia	Store	view D	revices					Discover D	Devk
		_	Devices (1)			_			My Interfa	aces (	(3)							liscovered D	evices (0)							(?) Autor	discovery	y (13)			
sit	Refresh Lis		Configure	Delete	Redisco	er Inter	faces																	Q							
DE	EVICE	C DEVI	ICE STATE 🗘	IP ADORESS	C VEN	OR	٥	MODEL	\$ NODE	0	SITE	٥	INTERFACES	\$	POLL	0	QOS	\$	FLOW	0	IP SL/		ROUTING	٥	LAN	0	TAGS	5	0	INTERVAL	
		AI	l v		A		~								All	~	All	~	All	~	All	~	All	~	All	~				All	
R	TR_Louisvi	X Up		10.100.51.10	Cisc	~		ciscoCSR100	Local/Server					3																1.	

The Device will now be listed on the *My Devices* tab with a summary of their configuration.

	0																												0 -	_		_
e Mana	agement <sup>©</sup>																			CSV Impor	t/Export	×	Credential	Store	View D	evices	Add N	on SNM	IP Device		Discover De	evici
			My Devices (1)						M	y Interface	is (3)							Disc	overed De	rvices (0)							<ol> <li>Autod</li> </ol>	iscovery	7 (13)			
		1-		i -																												
lit	Refresh Li	st	Configure	Delete	Rediscov	er Interfa	ices																		Q							
D	EVICE	¢	DEVICE STATE	IP ADDRESS	C VEND	OR	٥	MODEL	NODE		¢ sit	me 0	; INTE	RFACES (		POLL	٥	qos	0	FLOW	\$	IP SLA	0	ROUTING	٥	LAN	0	TAGS			ITERVAL	
			Al v		All		~									All	~	All	~	All	~	All	~	All	~	All	~				All	
) R	TR_Louisvi	16	110	10.100.51.10	Cisc			ciscoCSR1000v	Local						3						/										1 m	

To edit the configuration of a device(s) in LiveNX's inventory, select the device and click Edit.

≡ Liv	/eAction <sup>~</sup>	NX	ux ux										
evice Mana	agement 😨												
		My Dev	vices (1)							My Interfa	aces	(3)	
Edit	Refresh List	Со	nfigure	Delete	Re	discover Int	erfaces						
DE	EVICE 🗘	DEVICE	STATE 🗘	IP ADDRESS	÷	VENDOR	\$	MODEL	\$	NODE	\$	SITE	\$
	Device	All	~	IP Address		All	~	Model		Node			
RI RI	TR_Louisvi 🔀	Up		10.100.51.10		Cisco		ciscoCSR	1000v	Local/Server			
EDIT RTR Site	LOUISVILLE		Group			Interv	al		2	x			
Louisville			No Group				inute		~				
IP Address*													
10.100.51.1	10												
POLL	🔽 IP SI				ROUTII	10							
		LA	<b>Q</b> 05		RUUTII	IG	FL0	w					
Associate Pro	obe at IP Address		Hardcode S	ample Ratio									
Tags													
								Cancel	Apply				

Note the check boxes associated with the SNMP monitored devices.

Site	Group		Interval	
Louisville	No Group Selected	~	1 Minute	$\sim$
P Address*				
10.100.51.10				
POLL IP SLA	🗹 QOS	ROUTING	Z FLOW	LAN
Associate Probe at IP Address	Hardcode Sample Ratio			
	1/			
Tags				

These define the technology LiveNX will use to monitor the device.

- Poll This is the master on/off switch for polling SNMP on a device. LiveNX will poll basic device and interface statistics.
- IP SLA LiveNX will poll IP SLA related SNMP MIBs
- QoS LiveNX will poll QoS related SNMP MIBs
- Routing LiveNX will poll routing protocol related MIBs
- Flow LiveNX will accept and store Flow from the device. LiveNX does not poll any SNMP MIBs related to Flow.
- LAN LiveNX will poll LAN related MIBs

To ensure minimal SNMP overhead to both the device and network, it is often best to limit these options to the minimal requirements of a specific device. For example, it is not necessary to poll routing on a Layer 2 only switch or poll LAN on a WAN router.

The **Refresh List** button ensures the selected devices' details in LiveNX are up to date with the current state of the device itself.

DEVICE	
Device All · IP Address All · Model Node Site	0
RTR_Louisvi 🔆 Up 10.100.51.10 Cisco ciscoCSR1000v Local/Server	
RTR_Louisvi X Up 10.100.51.10 Cisco ciscoCSR1000v Local/Server	

To edit the SNMP credentials for a device in the inventory, select the device(s) and click Configure.

The **Delete** button will remove a selected device(s) from the LiveNX inventory.

lit	Refresh List	Configure	Delete Re	ediscover Interfaces	3		
DEV	VICE 🗘	DEVICE STATE	IP ADDRESS	VENDOR	MODEL 🗘	NODE	SITE
	Device	All ~		All ~	Model	Node	Site
RT	R_Louisvi 🔀	Up	10.100.51.10	Cisco	ciscoCSR1000v	Local/Server	

Clicking **Rediscover Interfaces** causes LiveNX to rescan all available Interfaces for the selected device(s). This is like the process that was done on initial device discovery and will allow for the selection or removal of monitored Interfaces.

DEVICE   DEVICE STATE  IP ADDRESS  VENDOR  MODEL  NODE		
	SITE	ł
Device     All     IP Address     All     Model     Node	Site	
2 RTR_Louisvi 🔆 Up 10.100.51.10 Cisco ciscoCSR1000v Local/Ser	erver	

After the *Rediscover Interfaces* process is run, the view changes to the *Discovered Interfaces* tab and shows all applicable Interfaces available. Select/deselect the interfaces for monitoring and click **Apply**.

e Mana	igement						CSV II	mport/Export ~	Credential Store	View Devices	Add Non SNMP Device	Discover Device:
	My Devic	es (35)		My Inte	erfaces (125)		Disc	overed Devices (1)		_	② Autodiscovery (0)	)
ELECT INT	TERFACES Devi	ices: 1 Interfaces: 5				Selecte	ed: 2			Q Search		
1	NAME 🗘	INTERFACE STATE	DEVICE 🗘	LINE RATE (Kbps)	IP ADDRESS	LABEL	○ INPUT CAPACITY (K ◇	OUTPUT CAPACITY ( 🗘	WAN/XCON 🗘	SERVICE PROVIDER 🗘	TAGS 🗘	DESCRIPTION
		All v	All 🗸						All v	All v		
	GigabitEthernet2	Up	RTR_Louisville	1000000	199.199.1.5	Conn-MPLS-Prov	rider		WAN	Conn-MPLS-Provider		Conn-MPLS-Provider
	GigabitEthernet1	Up	RTR_Louisville	1000000	10.100.51.10						hellokitty1	Connected to Mgmt
	GigabitEthernet3	Up	RTR_Louisville	1000000	192.168.101.254							Conn-AdminSE-PC
	Null0	Up	RTR_Louisville	10000000								
	VoIP-Null0	Up	RTR_Louisville	1000000								

Selecting the *My Interfaces* tab lists the interfaces being monitored by LiveNX.

	м	ly Devices (2)		1.1		My	Interfaces (1)			Discove	ered Devices (0)				Autodi	iscovery (0)		
				1					÷									
Sit								:	Selected: 1				a	Search				
	NAME 0	INTERFACE ST 🗘	DEVICE 0	DEVICE STATE	\$ SITE	0	SERVICE PROV_ 🗘	IP ADDRESS	SUBNET MASK 🗘	LABEL \$	BANDWIDTH ( 🗘	INPUT CAPACI 🗘	OUTPUT CAPA 🗘	WAN/XCON	\$	TAGS	٥	DESCRIPTION
		All v		All			All v							All	~			
	GigabitEthernet2	Up	RTR_Louisville	Up	Louisvi	le	MPLS	199.199.1.5	255.255.255.2	MPLS	1000000			WAN				Conn-MPLS
	GigabitEthernet3	Un	RTR_Louisville	Up	Louisvi	lle		192.168.101.2	255.255.255.0		1000000							Conn-Admi

Select an interface(s) and click **Edit** to modify its settings.

Devic	Management 💿											CSV Imp	ort/Export ~	Credential Store	View Devices	Add No	on SNI	MP Device	Discover Devices
		My Devices (2)					vly In	iterfaces (1)				Discove	ered Devices (0)			(?) A	utodi	iscovery (0)	
Edit	1									Selected: 1					a	Search			
	NAME 🗘	INTERFACE ST_ 🗘	DEVICE \$	DEVICE STA	TE Q	SITE	٥	SERVICE PROV 🗘	IP ADDRESS	SUBNET MASK 🗘	LABEL	٥	BANDWIDTH ( 🗘	INPUT CAPACI 🗘	OUTPUT CAPA 🗘	WAN/XCON	0	tags 🗘	DESCRIPTION \$
		All ~		All	~			All v								All 🗠	-		
	GigabitEthernet2	Up	RTR_Louisville	Up		Louisville		MPLS	199.199.1.5	255.255.255.2	MPLS		1000000			WAN			Conn-MPLS-Pr
	GigabitEthernet3	Up	RTR_Louisville	Up		Louisville			192.168.101.2	255.255.255.0			1000000						Conn-AdminS
All roy	s / 2																	« <	1 /1 > >

IP Address	Subnet Mask		Service Provi	ider	
199.199.1.5	255.255.255.252		MPLS		$\sim$
Input Capacity	Output Capacity		Label		
1000000 Kbps		Kbps	MPLS		
Value is inherited by bandwidth until set	Value is inherited by	bandwidth until set			
Tags	WAN/XCon				
	WAN	~			

LiveNX can provide easy onboarding of devices based on the reception of Flow. If Flow is received by LiveNX, but the device is not already in the inventory, LiveNX will attempt to query it with the default SNMP credentials stored in the Credential store. If a match is found the device will be listed in the *Autodiscover* tab.

	My Devices (1)						CSV Import/Export ~				
				My Interfaces (3)			Discovered Devices (1)			Autodiscovery (13)	
									٤.		
al / Deer	ver (13 devices)										
av ser	ver (15 devides)										
SELI	ECT DEVICES										
Add #	All Devices Edit								Q Search		
	DEVICE	SERIAL	0	IP ADDRESS	VENDOR	¢	MODEL	NODE	0	INTERFACES	4
	IWAN-BR_INET	9CTAOXXFZRV		10.100.51.32	Cisco		ciscoCSR1000v	Local/Server		9	
	IWAN-BR_MPLS	9WECNLKQF8E		10.100.51.31	Cisco		ciscoCSR1000v	Local/Server		9	
	IWAN-Br1_Sydney	97VTDJN7Q3X		10.100.51.35	Cisco		ciscoCSR1000v	Local/Server		10	
	IWAN-DC-MC	9AS8ZP25WQM		10.100.51.30	Cisco		ciscoCSR1000v	Local/Server		5	
	RTR_Austin	9BHNVDKXGHF		10.100.51.6	Cisco		ciscoCSR1000v	Local/Server		6	
	RTR_Birmingham1	941TA4ZK29S		10.100.51.7	Cisco		ciscoCSR1000v	Local/Server		5	
	RTR_London	90P9G9WXH52		10.100.51.8	Cisco		ciscoCSR1000v	Local/Server		6	
	RTR_LosAngeles	9AKRDFDZ0LR		10.100.51.9	Cisco		ciscoCSR1000v	Local/Server		5	
	RTR_Madison	908ZP9I1WAT		10.100.51.11	Cisco		ciscoCSR1000v	Local/Server		5	
	RTR_SanJose	94B8BTT129G		10.100.51.12	Cisco		ciscoCSR1000v	Local/Server		5	
	RTR_Seattle	93MW11NY55L		10.100.51.2	Cisco		ciscoCSR1000v	Local/Server		5	
	RTR-DC-CORE	9MFVEP11UMZ		10.100.51.3	Cisco		ciscoCSR1000v	Local/Server		5	
	RTR-DC-MPLS	9NGODVXRC6R		10.100.51.4	Cisco		ciscoCSR100Dv	Local/Server		5	

The process to add these auto-discovered devices is like that of manual device discovery as described above. Do note to use the Node Selection picker to ensure these auto-discovered devices are monitored by the desired LiveNX Node Collector.

	My Devices (1)			My Interfaces (3)			Discover	ed Devices (1)			<ol> <li>Autodiscovery (13)</li> </ol>	
	ver (13 devices)	~										
	ECT DEVICES											
SEL	ECT DEVICES											
Add #	All Devices Edit									Q Search.		
			~		~							
	DEVICE	SERIAL	ç	IP ADDRESS	÷	VENDOR \$	MODEL	0	NODE	Ç	INTERFACES	4
		Serial							Node			
	IWAN-BR_INET	9CTAOXXFZRV		10.100.51.32		Cisco	ciscoCSR10	100v	Local/Serv	er	9	
	IWAN-BR_MPLS	9WECNLKQF8E		10.100.51.31		Cisco	ciscoCSR10	00v	Local/Serv	er	9	
	IWAN-Br1_Sydney	97VTDJN7Q3X		10.100.51.35		Cisco	ciscoCSR10	100v	Local/Serv	er	10	
	IWAN-DC-MC	9AS8ZP25WQM		10.100.51.30		Cisco	ciscoCSR10	100v	Local/Serv	er	5	
	RTR_Austin	9BHNVDKXGHF		10.100.51.6		Cisco	ciscoCSR10	100v	Local/Serv	er	6	
	RTR_Birmingham1	941TA4ZK29S		10.100.51.7		Cisco	ciscoCSR10	00v	Local/Serv	er	5	
	RTR_London	90P9G9WXH52		10.100.51.8		Cisco	ciscoCSR10	00v	Local/Serv	er	6	
	RTR_LosAngeles	9AKRDFDZ0LR		10.100.51.9		Cisco	ciscoCSR10	100v	Local/Serv	er	5	
	RTR_Madison	908ZP9I1WAT		10.100.51.11		Cisco	ciscoCSR10	100v	Local/Serv	er	5	
	RTR_SanJose	94B8BTT129G		10.100.51.12		Cisco	ciscoCSR10	100v	Local/Serv	er	5	
	RTR_Seattle	93MW11NY55L		10.100.51.2		Cisco	ciscoCSR10	100v	Local/Serv	er	5	
	RTR-DC-CORE	9MFVEP11UMZ		10.100.51.3		Cisco	ciscoCSR10	100v	Local/Serv	er	5	
	RTR-DC-MPLS	9NGODVXRC6R		10.100.51.4		Cisco	ciscoCSR10	100v	Local/Serv	er	5	

CSV Import/ Export provides another method to bulk add and edit the device and interface inventory via CSV.

	CSV Impo	rt/Export ~	Credential S	tore View	w Devices	Add Non S	NMP Device	Discover D	Devices
vere	ed Devices (1)	Export CSV			?	Autodisco	very (13)		
		Import CSV							
	L				Q Search.				
	А	В	С	D	E	F	G	Н	
1	ADD/UPDATE	NAME	TYPE	DEVICE SERIAL	IP ADDRESS	VENDOR	MODEL	IOS VERSION	DESCRIPTION
2	TRUE	RTR_Louisville	Router	9E3XJK8MTIX	10.100.51.10	Cisco	ciscoCSR1000v	16.3.7	Cisco IOS Software [Denali], CSR1000
3	TRUE	GigabitEthernet1	Interface		10.100.51.10				Connected to MgmtNtw
4	TRUE	GigabitEthernet2	Interface		199.199.1.5				Conn-MPLS-Provider
5	TRUE	GigabitEthernet3	Interface		192.168.101.254				Conn-AdminSE-PC
6	FALSE	Null0	Interface						
7	FALSE	VoIP-Null0	Interface						
8									
0									

Import CSV will add new devices/interfaces and overwrite any exiting configuration with the data of the CSV.

CSV Import/Export ~	Credential Store	View Devices	Add Non SNMP Device	Discover Devices
overed Devices (1) Export CSV Import CSV			? Autodiscovery (13)	
		Q Sear		

📦 File Upload			×
O D D Downloads		<b>- 4</b> ∳ S	earch Downloads
Organize   New folder			ii • 🗍 📀
★ Favorites	Name	Date modified	Type Size
E Desktop	2021-03-08_105842_devices.csv	3/8/2021 12:01 PM	Microsoft Excel Co
Downloads			
Desktop Libraries Documents Music Pictures Libraries Li			
Computer T			4
	-08_105842_devices.csv	*.csv	en V Cancel

LiveNX is ready to import your CSV file. 27 Devices, (85 Interfaces) will be checked and added. Abort Proceed	27 Devices, (85 Interfaces) will be checked and added.	CSV IMPORT	
	CSV IMPORT		Abort Proceed
CSV IMPORT		CSV IMPORT	

The SNMP Credential Store and format is provided to assist networks that may have multiple SNMP credentials in use within the infrastructure. When discovering new devices using the *Credential Store*, the discovery engine will use the credentials from the store in the order they are listed.

Close

CSV Impo	rt/Export 🗸	Credential Store	View Devices	Add Non SNMP Device	Discover Devices
overed Devices (1)	Export CSV			? Autodiscovery (13)	
	Import CSV				
			Q Se		

NJ	AME	VERSION	TARGET PORT	COMMUNITY STRING	USER NAME
	Name	Version	Target Port	Community Str	User Name
R	0 v2c*	v2c	161	liveaction	
R	0 v3	v3	161		admin
All rows	/ 2				

Once a match is made via the discovery process, the specific SNMP credential will be associated with the respective device(s) until SNMP is reconfigured.

The store will hold up to a maximum of 50 SNMP v2c or v3 credentials. When discovering devices by manually entering SNMP credentials as shown below, if at least one device is discovered using the credential, the credential will automatically be added to the SNMP credential store. If the store is full, the credential will not be added.

SNN	MP Credentials				
	Choose profile from store				
0	Enter SNMP connection settings for this device				
	SNMP Version *		Target Port *		
	Version 2c	~	161		
	Community String *				
	liveaction				

### **Non-SNMP Monitored Devices**

LiveNX can monitor the Flow of Non-SNMP devices. They can be added to LiveNX by clicking **Add Non SNMP Device**.

			,	
CSV Import/Export ~	Credential Store	View Devices	Add Non SNMP Device	Discover Devices
			L	
Discovered Devices (0)			② Autodiscovery (0)	

1 General Settings					2 Add Interface
evice Name*	IP Address*	Site Name	Group	Node*	
Type Device Name				<ul> <li>Local/Server</li> </ul>	
ags		D	escription		

The *Add Non SNMP Device* dialog appears. A Device Name and IP Address must be defined to proceed.

Once a Device Name and IP Address has been entered and any desired additional data, click **Next Step**.

1 General Settings —					Add Interface
evice Name*	IP Address*	Site Name	Group	Node*	
MyRouter	10.100.51.11			<ul> <li>Local/Server</li> </ul>	
ags		D	escription		

The Add Interface view appears. Click Add.

ADD NON SNMP DEVICE		×
General Settings		Add Interface
Device Name: MyRouter Device IP Address: 10.100.51.11	No Interfaces defined Please add an Interface	
Back		Add To My Devices

A pop-out appears to enter Interface details. The *IfIndex* and *Interface Name* fields are mandatory.

lfindex*		Interface Name*		IP Address	Subnet Mask	Label
Type Ifindex		Type Interface Name			Type Subnet Mask	Type Label
Input Capacity		Output Capacity		Service Provider	Tags	WAN/XCon
	kbps		kbps			None

Once the IfIndex and Interface Name fields are entered as well as any desired optional fields, click **Add Interface**.

	IP Address	Subnet Mask	Label
MyInt[1		Type Subnet Mask	
Output Capacity	Service Provider	Tags	WAN/XCon
Type output capacity kbps			None 🗸
	Output Capacity	Output Capacity Service Provider	Output Capacity Service Provider Tags

The Add Non SNMP Device dialog appears. Click Add to My Devices.

OUTPUT CAPACL	Tags

The Non-SNMP device appears under *My Devices*.

		3												CSV In	nport/E	xport ~	C	redential St	ore	View D	Devices	Add	Non SI	NMP Devic	e	Discover De	evices
		My Devices (2)						My Interf	faces	s (3)				Disco	wered (	Devices (0	)						) Auto	discovery	(0)		
Edit	Refresh Li	st Configure	Delete	Redisc	over Inf	erfaces														Q							
	DEVICE 0	DEVICE STATE 🗘	IP ADDRESS	VENDOR	٥	MODEL	0	NODE	0	SITE	0	INTERFACES 🗘	HARDCODED 🗘	POLL	0	QOS	0	FLOW	0	IP SLA	0	ROUTING	0	LAN	0	TAGS	0
		All ~		All	~									All	~	All	~	All	~	All	~	All	~	All	~		
	MyRouter 🔆	Up	10.100.51.11	Non-SNM	Р	Non-SNMP		Local/Serve	er			1		~				~									
	RTR_Loui 🔀	11n	10.100.51.10	Cisco		ciscoCSR10		Local/Serve		Louisville				~													

To Edit a Non-SNMP device, select the device and click Edit.

My Devices (2)         My Interfaces (3)           Edit         Refresh List         Configure         Delete         Rediscover Interfaces           pervice         pervice state         in Address 0         velacion         0         more         more	Selected: 1	Discovered Devices (0)			② Auto	discovery (0)		
	Selected: 1							
	Selected: 1							
				Q Search				
	INTERFACES O HARDCODED_O	D_⊖ POLL ○ QOS	O FLOW O	IP SLA 🗘	ROUTING \$	LAN	C TAGS	<
Device All V IP Address All V Model Node Site		Al v Al v	All ~	All ~	All ~	All ~		
2 MyRouter 🔆 Up 10.100.51.11 Non-SNMP Non-SNMP Local/Server	1	~	~					
RTR_Loui_ X Up 10.100.51.10 Cisco ciscoCSR100_ Local/Server Louisville	2	~ ~	~	~				

The *Edit Device* modal appears. Since this is a Non-SNMP device, note the *Interfaces* tab.

	Devices			Interfaces		
evice Name*	IP Address*	Site Name	Group	,	Node*	
MyRouter	10.100.51.11				Local/Server	
ags		Desc	cription			

On the Interfaces tab, select an interface and click Edit.

			Devices								Interfaces			
Add	Edit	emove												
	IFINDEX \$	NAME	IP ADDRESS	0	SUBNET MASK	LABEL	0	WAN/XCON	0	INPUT CAPACIT 0	OUTPUT CAPACL_ 🗘	SERVICE PROVIL	TAGS	0
		Name						All	~					
	1	MyInt1												
JI rows	14													

After making any desired changes, click Update Interface.

Ifindex*		Interface Name*		IP Address	Subnet Mask	Label
1		MyInt1		1.1.1.1	255.255.255.0	
Input Capacity		Output Capacity		Service Provider	Tags	WAN/XCon
	kbps	Type output capacity	kbps	(No service provider selected) $\sim$		None
	корз		KDps	(No service provider selected)		None
						Cancel Update Interface

The *Edit Device* modal appears again, click **Apply** to save any changes.

Devices								Interfaces							
Add	Edit	Remove													
	IFINDEX	© NAME	0	IP ADDRESS	¢ s	SUBNET MASK 0	LABEL	0 WA	N/XCON	0		OUTPUT CAPACI 🗘	SERVICE PROVI 🗘	TAGS	
								A	ui -	~					
	1	MyInt1													
All rows	/1														
All rows	_/1														

# **Filter Management**

Custom Filters can be created and saved to ease the administrative burden of often used filters. These filters can be shared for usage by other users.



To add the first Custom Filter, click Add Filter.

Filter Management
You have not created any filters yet.
Add Filter

The *Add Filter* modal appears. Add the Custom Filter's configuration as desired and click **Save** when finished.

Name				
MyFilter				
Description				
This is MyFilter				
Details				
Application: V	OIP DSCP:	EF	nter Filter Request Here	
Sharing				
Off				

The custom filter appears on the *Filter Management* page.

Filter Ma	nagement 🥯				
Add	Edit Copy Delete				Q Search
	FILTER NAME	PUBLIC	CREATED BY	DESCRIPT	ion O
		All	All V		
	MyFilter		10100	This is M	tyFilter
All rows	/ 1				

To edit a custom filter, select the desired filter and click Edit.

Filter M	anagement <sup>®</sup>				
Add	Edit Copy Delete	Selected:	1		Q Search
	FILTER NAME	PUBLIC	CREATED BY	DESCRIP	rion C
		All ~	All V		
	MyFilter		ditte	This is I	ЛуFilter
All rows	/1				

Update the filter as desired and click **Save** when finished.

Name MyFilter			
Description			
This is MyFilter			
Details			
Application: VoIP	DSCP: EF	Enter Filter Request Here	
Sharing Off			

Currently, saved custom filters can be used by LiveNX's Logical Topology (Preview).

≡ LiveAction <sup>-</sup> N×	UX			<b>▲</b> 104	61	• 2	28679	{-} -	0- ¢	• 🔒 arab 🗸		
Logical Topology PREVIEW					Nov 1	2, 2020 0	09:15:00 → No	v 12, 2020 09:20	00 5 Mins	✓ 😄 Refresh		
	New Tab					+ Add ta	b					
Selected sites and devices shown on topology	EDIT	uest Here							Φ	Apply filter		
topology	Application											
	DSCP									+		
	Site											
Sort by: Name ~	Service Provid	ler								8		
V O AWS_Oregon	let Custom											
V O DC-New_York	DC									-		
V O Florida												
V O Hurricane Electric												
V O Impairment												
V O Indianapolis												
San Jose	Site Status	^										
✓ ○ Seattle	<ul> <li>Normal</li> <li>Critical</li> </ul>	<ul> <li>Warning</li> <li>Polling Disabled</li> </ul>										
	N/A											
	Legend	^										
	Display By											
	WAN Application											
Show other sites On	<ul> <li>Video</li> <li>citrix-static</li> <li>ka0wuc</li> <li>rtp-video</li> <li>unknown</li> <li>Other 2</li> </ul>	<ul> <li>VoIP</li> <li>iop</li> <li>rtp-audio</li> <li>ssl</li> <li>youtube</li> </ul>										

## **Site Management**

Sites provides a logical grouping of devices in LiveNX. This fundamental concept is used throughout the solution by Dashboards, Reports, Stories, and Filtering and should be considered a mandatory configuration task. Site Management is where Sites can be defined and managed for the system.



When configuring LiveNX for the first time, no sites are configured. To add a Site, either:

- 1. Click Import Sites to import from a CSV.
- 2. Click Add Sites.



Importing Sites will be discussed later in this section. To add an individual Site, click Add Site.



The *Add Site* modal appears and has three tabs: *Details, Address,* and *Business hours*. A *Site Name* is mandatory, once assigned the Site definition can be saved.

	Site IP Range (CIDR	Notation IP's)	Site name	e is require
0/1000				
0/1000	Tags			
	0/1000	0/1000		CIDR Notation IPs

#### Site Details

- Site Description a courtesy free-text field.
- Site IP Rage Used for defining the IP space used by the site. This is used by various workflows and Flow Filters. Based on other page's reliance on this data, it could be considered a mandatory field.
- *Devices* List of devices that are members of the Site. Click on this field to add devices to the Site or assign Site to devices via Device Management.
- Tags An administratively assigned delimiter that can be used for Filtering.
- Number of Employees A courtesy field for helping to provide context to LiveNX users.
- Data Center A delimiter that can be used for Filtering.

Details	Add	ress	Bu	isiness hours	
Site Name					
Site name					
Site Description		Site IP Range (CIDR	Notation IP's)	Site name is requi	red
Devices	0/1000	Tags			
Number of Employees					
Number of Employees					
Data Center					

### **Site Address**

The primary purpose of the Site Address is for assigning Geo coordinates for the Geo Topology and in turn, deriving the Region.

Details	Address Business hours
Address	Latitude & Longitude
Address Line 1	Latitude
Address Line 2	Longitude
City	Phone Number
	Phone Number
State/Province/Region	Email
Zip Code	Region
Zip Code	Input valid address and press "Geo Coordinate Lookup" to populate region
Country	
Country	
Geo Coordinate Lookup     Remove Regi	ND
♦ Geo Coordinate Lookup Remove Regis	

Once any portion of the Site's Address, City, State/Provence/Region, or Zip Code is entered, the **Geo Coordinate Lookup** button can be used to auto-assign the Latitude & Longitude. Latitude & Longitude can also be added manually.

The Region will be assigned based on the *Latitude & Longitude*. Region includes: *Continent, Country, State, City*. Region is a hierarchical filter of sites that can be used on various pages of the solutions such as Topologies, Dashboard, Reports, Alerts, etc.

Once a Region has been assigned, it can be removed by using the **Remove Region** button.

Details	Address	Business hours
Address	Latitude & Long	gitude
Address Line 1	38.25489	
Address Line 2	-85.76666	
City	Phone Number	
Louisville	Phone Numb	
State/Province/Region	Email	
KY		
Zip Code	Region	
Zip Code	Continent: Nor State: Kentucky	th America → Country: United States → / → City: Louisville
Country		
Geo Coordinate Lookup     Remove Region		
	-	

## **Site Business Hours**

Business Hours can be assigned per site. These can used by Reports and Alerts for Filtering.

	Details			Ado	iress		В	usiness hours	
Days of Week					Time Zone				🔽 DST
Su 🚺	τυ	We 🕩	Fr Sa		(GMT-05:0	0) Ameri	ca/Louisville		
Start time					End time				
^	^				^	^			
08 :	00	AM			05	: 00	РМ		
~	~				~	~			

Sites can also be managed in bulk by the menu icon at the top right or the *Site Management* page.

Add	Edit Delete													Q Search			
	SITE O	DATA CENTER	O DEVIC	ces O	CONTAINS	DEVICES O	NO. OF EMPLOYEES 🗘	BUSINESS HOURS	IP RANGES	0	GEO LOC	0	ADDRESS C	REGION O	DESCRIPTION C	TAGS	
		Al	De		All	~					All	~					
	()/,[]Test							Mo - Fr   8:00 am							a test site		
	<test\$site></test\$site>							Mo - Fr   8:00 am									
	Apple							Mo - Fr   8:00 am			1				New description		
	AT&T							Mo - Fr   8:00 am			1				New description		
	Austin							Mo - Fr   8:00 am			1		Austin, Texas	Austin, Texas, Uni	New description		
	Austria							Mo - Fr   8:00 am	192.168.65.2   1	9	1		Austria	Austria, Europe		Europe	
	Beljing							Mo   8:00 am - 5:	172.50.50.0/24		1		beijing	Beijing, Beijing, C		tag1, tag2	
	Birmingham		RTR.	_Birmingham		~		Mo - Fr   8:00 am			1		Birmingham, AL	Birmingham, Ala		stuff	
	Black Hole							Mo - Fr   8:00 am	81.1.1   10.1.1	5	1						
	Branch1							Mo   8:00 am - 5:			1					tag1, tag2	
	Branch2							Mo - Fr   8:00 am			1					tag1	
	Brazil						1000	We - Fr   10:00 a			1		Rio, Rio	San Antonio, Tex	tada		
	Brown							Mo - Fr   8:00 am	10.175.20.154	1							
	BuggySite							Mo - Fr   8:00 am								tag1, tag2	, tag
	BugSite							Mo - Fr   8:00 am								tag1, tag3	
	Chicago							Mo - Fr   8:00 am	10.177.1.116   2	1	1		chicago	Chicago, Illinois,			
	china							Mo - Fr   8:00 am			1		China	China, Asia	tada		



Selecting *Import/Export Sites* provides bulk management of Sites via CSV.

		•••
SCRIPTION	Import/Export Sites	B
	Geocode Sites	
	Reverse Geocode R	egions
IMPOR	T/EXPORT SITES	×
Imp	ort Sites:	Export:
<b>~</b>	Geocode sites	<ul> <li>Current sites (.csv)</li> </ul>
Sele	ect CSV file for import	<ul> <li>Example sites (.csv)</li> </ul>
		<ul> <li>Valid time zones (.csv)</li> </ul>
		Close

#### Import

- The *Geocode Sites* check box allows you to perform a Geocode lookup of all Sites as they are imported via the CSV. This can take time and deselecting this box will skip this step
- Select CSV file for Import will begin the import process

#### Export

- Current Sites exports a list of the exiting Site configuration for editing via a spreadsheet.
- Selecting *Example Sites* provides an example CSV that can be used to flesh out the Site configuration in a spreadsheet.
- Valid Time Zones provides a CSV that list the valid syntax for time zones in the Site CSV.

Below is a view of the Example CSV File:

 A
 B
 C
 D
 E
 F
 G
 H
 I
 J
 K
 L
 M
 N
 O
 P
 Q
 R
 S
 T
 U
 V
 W

 1
 Site Name Number olitoata:
 Site Nam

# CHAPTER 3

# Settings

# In this chapter:

Settings	
System Diagnostics	
Flow Data Status	
User Management	
LiveNX Server	

# Settings

Settings

The *Server* menu is where system specific configuration parameters are set. These include items such as licensing configuration, reporting options, and data retention policies.



### **Data Source Management**

Data Source defines which traffic is pre-aggregated into the Long Term Flow Store.

Settings	
Q Search	DATA SOURCE MANAGEMENT
Configuration	The data source is a flex search which determines what flow data will be pre-aggregated. Modifying this setting may
Data Source Management	affect report performance for queries of large time ranges. This setting should be modified with caution as it may introduce performance issues.
Data Store Management	
Device Entity Page Reports	Flex String: wan I xcon
Email Configuration	Reset to Default Apply
Integrations ~	
Lionaina	

### **Data Store Management**

*Data Store Management* allows for the review and configuration LiveNX's database retention polices.

### **Disk Overview**

Disk Overview provides a summary of disk consumption by each data store.

ings			
Search		DISK OVERVIEW	
onfiguration	^		
ata Source Management		LOCAL/SERVER	
ata Store Management		Available Free Space: 167.38 GB	Total Disk Space: 249.88 GB
Disk Overview			
lodes Data Store		Nodes Data Store     Web Alerts Store     Reports Store	re 🔍 Web UI Data Store 🔍 Other Data Store
eb UI Data Store		PA-NODE	① Disconnected
vice Entity Page Reports			
il Configuration		Available Free Space: 0 Bytes	Total Disk Space: 0 Bytes
grations ~		Nodes Data Store      Web Alerts Store      Other Data	Store
ensing ~			

#### **Nodes Data Store**

*Nodes Data Store* provides management for the data stores used by LiveNX. From this page, retention periods, size warnings, and archive destinations can be defined. Data retention policies can be set up for all Nodes (using default settings) or configured uniquely for each Node.

Settings							
Q Search		I	DEFAULT SETTINGS		DEFAULT SETTINGS		
Configuration		^	Are applied for all nodes that do not use custom settings				
Data Source Management					SNMP		^
Data Store Management	^	10			Display a warning when any database exceeds:		
Disk Overview			LOCAL Default settings applied		O MB		
Nodes Data Store			Available Free Space: 167.38 GB	Total Disk Space: 249.88 GB	Automatically purge data older than:	Reset now	
Web UI Data Store					10 Days	Purge now	
Device Entity Page Reports			Other Store Size: 63.69 GB      SNMP Store Size: 1.03 GB     Flow Store Size: 14.56 G     Engineering Console Alert Store Size: 28.31 MB     Long-Term Store Size: 3.19 GB	38	Before purging, archive to:		
Email Configuration							
Integrations	~						
Licensing	~		PA-NODE Default settings applied	Disconnected	Flow		
LiveNA Configuration			Available Free Space: 0 Bytes	Total Disk Space: 0 Bytes	Display a warning when any database exceeds:		
Mounted Data					V MO		
Nodes			Other Store Size: 0 Bytes SNMP Store Size: 0 Bytes Flow Store Size: 0 Bytes     Engineering Console Alert Store Size: 0 Bytes Long-Term Store Size: 0 Bytes		Automatically purge data older than:	Reset now	
Properties	~				10 🗘 Days	Purge now	
Proxy					Before purging, archive to:		
Reports	~						
Security	~				Enaineerina Console Alert		$\sim$
Single Sign On						t ale and a sector	
SNMP Trap					Reve	t changes Apply	
		~					

#### Web UI Data Store

LiveNX will cache some data to ensure accelerated performance for Dashboards, Notifications and Entity pages. These data stores can be configured to cache data for 1 day, 7 days, or 1 month (default).

Settings									
Q Search			VEB UI DATA STORE						
Configuration		^	VED OF DATA STORE						
Data Source Management			Retention Policy Clear Data						
Data Store Management Disk Overview	^		COLLECTION NAME		SIZE	COUNT	LAST PURGE	RETENTION PERIOD	
Nodes Data Store								All	~
Web UI Data Store			Dashboard Widgets	0	0.00 bytes	0	Mon Jun 03, 2019 19:57:48 (GMT -04:00)	1 month	
Device Entity Page Reports			Notifications	0	0.00 bytes	0	Mon Jun 03, 2019 19:57:48 (GMT -04:00)	1 month	
Email Configuration			Entity Pages	0	96.10 KB	1	Mon Jun 03, 2019 19:57:48 (GMT -04:00)	1 month	
ntegrations	~								
icensing	~								
iveNA Configuration									
founted Data									
Nodes									
Properties	~		Rows: 3 / 3						
roxy									

### **Device Entity Page Reports**

Device Entity Page Reports allows customization of the reports shown on the Device Page.

js	
n	
rce Management	
e Management	~
y Page Reports	
ation	
	~
	~
	~
	~
	~
	~

TRL.colisville   Brade code   State: Code   State: Code   State: Code   Code Cetadis     Code CetAddis     Code CetAddis <th>es &gt; Louisville &gt; Device: RTR_Louisvi</th> <th>lle</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th>Apr 06, 2021 09:35:00 Apr 06, 2021 09:50:00 15 Min</th>	es > Louisville > Device: RTR_Louisvi	lle						Apr 06, 2021 09:35:00 Apr 06, 2021 09:50:00 15 Min
Device CPU/Memory Usage	Status: Good		Current Flows				0	=
Image: Control of the control of t	evice Details						~	Î
Image: spin and spin a	levice CPU/Memory Usage						^	
10     0 </td <td>20</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>=</td> <td></td>	20						=	
035     036     038     040     044     044     044     044       Q touch     Q touch     Q touch     Q touch     Q touch     Q touch       CPU Usage     7%     Peak C     Peak C     Peak C       Memory Usage     16%     16%     16%	/ 10				~			
Legend O Name O Peak O		09:40			46	09:48 0		
CPU Usage 7% 8% Memory Usage 16% 16% Top Applications (inbound) ^ 75	Levend Q Name Q			Q Search	Dark A		1 L	
Memory Usage 16% 16%			Avg 🗸				8%	RTR_Louisville
Top Applications (Inbound)								
								Louisville
	50						-	Critical D Warring D Good D Pol

Below is an example Device page that could be modified by these settings:

Updates allow you to manage system updates.

Settings			
Q Search			
Integrations	~	^	UPDATES
Licensing	~		Information
LiveNA Configuration			Latest Version: No data 🖸 Current Version: - View All Versions
Mounted Data			Online Update Office Update
Nodes			
Properties	~		Note: Enter server upgrade package URL from: https://cbudkeys.liveaction.com/downloads
Proxy			Upgrade Package URL *
Reports	~		https://download.liveaction.com/LiveACV/restion/jfsoftware_package.liveas.earver.versionj.enc Start Update
Security	~		
Single Sign On			
SNMP Trap			
Syslog			
Troubleshooting	~		
CPU Profiling			
Heap Dump			
Logs			
Packet Capture			
Upload History			
User Activity Tracking			
Updates		~	

From the Online Update tab, enter the full URL of the update package and click Start Update.

LiveNX will download the upgrade package from the *liveaction.com* website, install it, and reboot the system.

Information	ø		Current Version	21.2.0		View All Versions
		Online Update			Offline Update	
③ Note: Enter server	upgrade packa	ge URL from: http://www.liveaction.com/	go/software-download			
grade Package URL						
Start Update						
Start Update						
Start Update						

If required, the *Offline Update* tab allows for manual upload of the upgrade packet to the LiveNX server.

PDATES								
Information								
Latest Version	ø		Cu	rrent Version	21.2.0			View All Vers
		Online Update					Offline Update	
Note: Download u	pdate file from: h	ttp://www.liveaction.com/go,	software-download					
lect update file								
No file chosen (enc,	asc, zip)			🕞 Ch	oose File			
Start Update								

# **Email Configuration**

*Email Configuration* provides SMTP configuration parameters for LiveNX to integrate with an external email server.

	~
	~
	~
~	
~	

### Integrations

LiveNX can optionally interact with external solutions to enrich its data and provide Alert messaging to external systems. Configuring the connections to these external systems is done via *Integrations*.

Settings
Q Search
Configuration
Data Source Management
Data Store
Device Entity Page Reports
Email Configuration
Integrations ~
Licensing ~
LiveNA Configuration
Mounted Data
Nodes
Properties ~
Proxy
Reports ~
Security ~
Single Sign On
SNMP Trap
Syslog
Troubleshooting ~
Updates

### Cisco APIC-EM/DNA-C

LiveNX can connect to an external Cisco APIC-EM or DNA-C environment to:

- Discover Inventory
- Cross-launch to Client 360
- Cross-launch to Device 360
- Health Score and Issues List

From the Cisco APIC-EM/ DNA-C tab, enter the *Hostname*, *Username* and *Password* and click **Sub**mit.

Jetunya	
Q Search	
	^
Configuration	
Data Source Management	
Data Store	
Device Entity Page Reports	
Email Configuration	
Integrations	~
Cisco APIC-EM / DNA-C	
Cisco ISE	
Cisco SD-WAN	
LiveNCA	
ServiceNow	
Licensing	~

Once connected to APIC-EM/ DNA-C, the integration status will show as *Connected*.

	CO APIC-EM / DNA-C SURATION
Hostname	100.119.104.241
Username	admin
Status	<ul> <li>Connected</li> </ul>
Edit 🌶	Delete 🛚
Discover	Recheck Status

If desired, use the **Discover** button for LiveNX to import APIC-EM/ DNA-C's inventory for device discovery.



	My Devices (9)		My interfaces (i					odiscovery (0)
2 SELE	CT DEVICES							
8-64 A	I Devices Edit						Q. Search	
AGG A	EDIC CON						st startn	
	DEVICE NAME	SITE	O SERIAL O	IP ADDRESS 0	VENDOR 0	MODEL 0	NODE 0	INTERFACES 0
	A1-3650b		FD02035Q1X2, FD02035E35	10.4.207.4	Cisco	Cisco Catalyst 3650 Series S	Local/Server	0
	A1-3850a		FOC1652V1LW, FOC1705V04	10.4.207.3	Cisco	Cisco Catalyst 3850 Series Et	Local/Server	0
	A1-3850mc		FCW2016D07K	10.4.207.5	Cisco	Cisco Catalyst 3850 Series Et	Local/Server	0
	A2-3850md		FCW1949C1TX	10.4.200.58	Cisco	Cisco Catalyst 3850 Series Et	Local/Server	52
	A2-9300a		FCW2125L0UK, FCW2125L10	10.4.200.55	Cisco	Cisco Catalyst 9300 Series S	Local/Server	206
	A2-9407c		FXS2131Q3YF	10.4.200.57	Cisco	Cisco Catalyst 9400 Series S	Local/Server	0
	A3-3650c		FDO1747Q005, FDO2040E0N	10.4.200.67	Cisco	Cisco Catalyst 3650 Series S	Local/Server	0
	AIR-CT5520-WLC1		FCH2024V2HN	10.4.202.66	Cisco	Cisco 5500 Series Wireless L	Local/Server	0
	AP0042		FJC2025F1US	10.4.231.13	Cisco	Cisco 3800E Series Unified A	Local/Server	0
	AP00D7		FDW2044D0FY	10.4.211.10	Cisco	Cisco 2800I Series Unified Ac	Local/Server	0

Once DNA-C is integrated with LiveNX, from the *SD Access Traffic Assessment Story*, click on a *Client IP/ Username* to cross-launch to DNA-C's *Client 360* view.

≡ LiveAction <sup>™</sup> ™			New Featurest	• 0 🔺 0 🕞 📮 - (	0 * O * 🍐 admin *
SD Access Traffic Assessment				< Jun 08, 2018 08:40:00 → Jun 08, 2018 09	Hour Y C Auto
Flow Details		SD Access Campus			
VIRTUAL NETWORK	SCALABLE GROUP	CLIENT IP / USER	APPLICATION	DSCP	SERVER IP
AI -	All U	AI V	All 🗸	- IA	AI ~
		Tracy (10.4.235.5)	unknown	# 48 (CS6)	224.0.0.13
4099		- System1 (10.4.250.104) = System2 (10.4.235.7)	= otp		jon (10.4.234.11)
	Unknown (0)	Tim (10.4.250.115)		24 (CS3)	Contractor-Tom (10.4.233.12)
		Server1 (10.4.250.102)	NO NO		emp2123 (10.4.233.11) 13.68.93.109
	Contractors (5)	Contractor-Tom (10.4.233.12)		0 (198)	64.4.54.254 = Server1 (10.4.250.102)
VN.Campus	Employees (4)	john (10.4.232.14)	domain	46 (05)	Tim (10.4.250.112)
		emp2123 (10.4.233.11)	https	16(052)	21.72.186.90
		Bob (10.4.232.11)	II netbios-dgm	10((52)	13.78.130.220 = 40.69.153.67
			= pesync-https		64.4.54.253 -
		Jon (10.4.234.11)			40.79.85.125
		Stacy (10.4.234.12)			
					13,66.56,243
					\$2.183.114.179 = 65.53.252.190
					13.76.168.230
					10.4.250.116 =
https://100.119.104.239					

cisco	<b>DNA</b> CENTER	DESIGN	POLICY	PROVISION	ASSURANC	E	
Health 🗸	Dashb	oards 🗸	Issues	Manage 🗸			
Clie	nt 36	60					
<b>1</b> /10 <b>0</b>	emp2	123					
•	·						
10 HEALTH							
0	11:00a 12	:00p 1:00p	2:00p 3:	00p 4:00p	5:00p 6:00p	7:00p 8:00p	9:00p
			Issues and	Trends	Onboarding	Path Trace	Ap

Once DNA-C is integrated with LiveNX, the Site view will include % healthy devices and issue count.



LiveAction 🕺 Sites > Site: SJC Campus Jun 06, 2018 09:05:00 -- Jun 06, 2018 10:05:00 Hour --O Last 15 minutes SJC\_Campus 9 67 54 100% Δ 0 Status: Good Importance: Unspecified R Col Inte ۲ -۲ ×  $^{+}$ ( 0 DEVICE 0 ô CPU AVERAGE 🗘 MEMORY A ... All A2-9300a 2% 38% 0 errors Cisco IOS So. A2-9300b 2% 36 % 0 errors Cisco IOS So. AIR-CT8540 0 errors C-N7706-1 11 % 18% 0 errors Cisco NK-OS C-N7706-2 11 % 18% 0 errors Cisco NX-OS. D2-9500-1 1% 34% 0 errors 02-9500-2 1.96 34% 0 errors IE-ASR1001. 1% 7% 0 errors IE-ASR1001. 1 % 7% 0 errors Cisco IOS So-10 a. < < 1/1 > > 100 rows / 9  $\odot$ 😑 Critical 🥚 Warning 🕒 Good ble 😑 Polling Disabled 🌒 N/A Unr

Additionally, the device summary view will include device health score and issue count.

Finally, the *Device* view includes the device health score and issue count. Click link to cross-launch to *Device 360* view.



CISCO DESIGN POLICY PROVISION ASSURANCE	Q		0	
Health V Dashboards V Issues Manage V				
Device 360	hours 🗸		Domain	•~
-/10 Router IE-ASR1001HX-2.sda-lab.com Gener/Genon,Descense/150-23			View D	etalls
Device Model ADR1001+HK IP Address: 10.4.200.2 Software Version: 56.6.3 Role: BORDER RDV/TBR HA Status: Non-redundance: Uptime: 3 days 1450.54				
1 KARN 2				
0 12000 1000 2000 3000 4000 5000 6000 7000 8000 9000 11000 4/6 1008 2008 5008 6008 5008 8008 8008	9:00a	10:00a	11:00a	
Issues Physical Neighbor Topology Path Tacca Device Connectivity				
<ul> <li>Issues (5) Jun 6, 2018 1152 am</li> </ul>				edback
Connected Fallin Bould 10.4 2002 Ltdl Connectivity to the CHCP Server 10.4 250 152 In the Physical Network Net Kolumeness 113		Jun 6, 2	018 11:3	
Connected				

#### ServiceNow

Cottingo

LiveNX can integrate with ServiceNow for forwarding its Alerts as either Incidents or Events.

From the ServiceNow tab, enter the Hostname, Username, Password, and choose the Integration type.

ango			
tion	^		CREATE SERVICENOW CONFIGURATION
irce Management			
			Hostname *
intity Page Reports			
iguration			Username *
ons	~		
1 / DNA-C			Password *
N			Integration type
			Incident
Now			Event Management Plugin - Get started with Event Management
	~		Save
A Configuration			

Once connected, the *Status* will show as *Connected*.

CONFIGURED SERVICENOW		
Hostname	service-now.com	
Username	admi	
Integration type	Incide	
Status	Connecte	
E	DIT DELETE	
Recheck St	tatus General Settings	

Each ServiceNow implementation can be highly customized. To ensure LiveNX can deliver its alerts in the best possible format, many settings can be defined on either a global or per alert basis. Global ServiceNow settings will be applied to all alerts that are forwarded by LiveNX to ServiceNow. Per-alert settings only apply to the unique alert and will override any global settings. To customize the global implementation, click **General Settings**.

CONFIGURED SERVICENOW		
Hostname	service-now.com	
Username	admin	
Integration type	Incident	
Status	Connected	
1	EDIT DELETE	
Recheck S	General Settings	

The LiveNX alert description can be forwarded to any free text field available in the ServiceNow implementation.

LiveNX will poll ServiceNow, learn the potential options, and provide a picker to choose the field that bests serves the implementation.

Integrations > ServiceNow global settings					
SERVICENOW GLOBAL SETTINGS ServiceNow general settings will affect all alert types. You can override input fields per o proje. LiveNx alert description This field will display LiveNX alert description instead of custom value. Send LiveNX and description to Send LiveNX alert description to	t on Alert management				
Default ServiceNow values					
Approval	Cr	ontact type			
Select LiveNX value	1	Select LiveNX value 🗸			
Category	Ur.	pon approval			
Database ~		Select LiveNX value			
Subcategory	υγ	pon reject			
D82 ~		Select LiveNX value 🗸			
				Revert changes Save	

The Default ServiceNow values will provide a list of the available parameters that were discovered by LiveNX.

These selected value(s) will be applied to all LiveNX alerts, unless they are overridden by per-alert settings.

The screenshot below provides an example of the Default ServeNow values. These could be different in each network, so more or fewer options may be presented.

Integrations > ServiceNow global settings					
SERVICENOW GLOBAL SETTINGS ServiceNow general settings will affect all allert types. You can override input fields per allert on Allert management page.					
LiveNx alert description					
This field will display LiveNX alert description instead of custom value.					
Send LiveKX ident description to					
Select ServiceNow field V					
Default Scrifection values					
Approval	Contact type				
Select LiveNX value	Select LiveNX value 🗸				
Category	Upon approval				
Database	Select LiveNX value				
Subcategory DB2	Upon reject Select LiveNX value				
Low .	Server Schertz Hans				
	!				
		Revert changes Save			

ServiceNow Per-alert settings can be adjusted withing each alert's Sharing configuration.
Email		
test@test.com ×		×
Type email		
ServiceNow		^
Default ServiceNow settings set on Global s override individual settings below.	settings page. You	u can
Category		
Database	$\sim$	
Subcategory		Î
DB2	~	
DB2 Add value to override	~	

#### LiveNCA

LiveNX can provide cross-launch capabilities to LiveNCA. LiveNCA is a partner product that provides comprehensive network configuration and change management (NCCM), configuration backup, restore, and audit capability.

Settings	
Q Search	
Configuration	^
Data Source Management	
Data Store Device Entity Page Reports	
Email Configuration	
Integrations	^
Cisco APIC-EM / DNA-C	
Cisco ISE	
Cisco SD-WAN	
LiveNCA ServiceNow	
	~
Licensing	~

From the LiveNCA tab, provide the full URL to the LiveNCA server and click Connect.

Conne

After a browser refresh, the **LiveNCA** button appears in the top left of the window.



Click LiveNCA to open the LiveNCA login page in a new browser tab.



#### Cisco ISE

The Cisco ISE tab can be used to integrate LiveNX with Cisco ISE and PXGRID. This allows for identifying users in Flow reports based on IP address to username mapping.

Settings	
Q Search	
Configuration	^
Data Source Management	
Data Store	
Device Entity Page Reports	
Email Configuration	
Integrations	~
Cisco APIC-EM / DNA-C	
Cisco ISE	
Cisco SD-WAN	
LiveNCA	
ServiceNow	
Licensing	~

Cisco ISE and PXGRID must be configured to support this integration.

From Cisco Identity Service Engine Go to Administration > pxGrid Services > Settings and select Allow password based account creation, and then click Save.



From the *Cisco ISE* tab, configure the ISE IP address or hostname and enter a pxGrid username. When finished, click **Create** (LiveNX will utilize pxGrid northbound API's to create the new user account).

CONFIGURE CISCO ISE	CREATE NEW PXGRID USER
Hostname *	Hostname *
	Hostname
	PXGrid Username *
PXGrid Username *	PXGrid Username
PXGrid Username Password *	Cre
	l
Connect	

Once the ISE user is created successfully, the auto generated password is displayed.

- Required: Copy the password and save it for future use.
- Required: **Do Not Click Connect**
- The user must first be approved from the Cisco ISE admin portal.

HOSTNAMES *	Hostname	10.4.250
	PXGrid Username	liveac
PXGRID USERNAME *	Password	Ltx6Uu2t8RWXUtCs
PXGrid Username		
PASSWORD *		Create New User Connec
Password		
Conne		
Conne		

From Cisco ISE admin portal, navigate to *Administration* > *pxGrid Services* and select the newly created pxGrid user.

• Click **Approve** to approve the user.

Identity Services Engine System Identity Managem		Operations     Policy     Policy     Policy     Policy     Policy	Administration Work Cent	ers at Centric NAC	1 License Warning	
-, <b>,,,</b>		I			Click here to do wireles	s setup Do not show this agai
I Clients Web Clients	Capabilities Live Log Settings	Certificates				
inable 🧭 Disable 📿 Approve	🕘 Group 📫 Decline 🔞 Delete 👻	Refresh Total Pending Approval(1) +		1 se	lected item 1 - 12 of 12 Show 25	▼ perpage Page 1
Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method	Log
ise-mnt-ise222		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Administrator	Certificate	View
ise-fanout-ise222		Capabilities(0 Pub, 0 Sub)	Online (XMPP)		Certificate	View
ise-admin-ise222		Capabilities(3 Pub, 1 Sub)	Online (XMPP)	Administrator	Certificate	View
ise-bridge-ise221		Capabilities(0 Pub, 5 Sub)	Online (XMPP)	Administrator	Certificate	View
ise-mnt-ise221		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Administrator	Certificate	View
ise-admin-ise221		Capabilities(5 Pub, 2 Sub)	Online (XMPP)	Administrator	Certificate	View
ise-fanout-ise221		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Administrator	Certificate	View
ise-pubsub-ise221		Capabilities(0 Pub, 0 Sub)	Online (XMPP)		Certificate	View
ise-pubsub-ise222		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)		Certificate	View
Iveaction		Capabilities(0 Pub, 0 Sub)	Pending	Basic	UserName/Password	View
ise221-dnac-intg		Capabilities(0 Pub, 2 Sub)	Online (XMPP)	Session	Certificate	View
▶ ise221		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)	Session	Certificate	View

Validate the new user is Online.

Identity Services Engine     System Identity Management		Operations         Policy         Ac           tal Management         pxGrid Service	Imministration         Work Center           s         • Feed Service         • Thread	at Centric NAC	Click here to do wireles	ss setup Do not show this again
All Clients Web Clients Cap PEnable ØDisable ØApprove @		ertificates			1 - 12 of 12 Show 25	5 ▼ per page Page 1
Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method	Log
] ▶ ise-mnt-ise222		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Administrator	Certificate	View
▶ ise-fanout-ise222		Capabilities(0 Pub, 0 Sub)	Online (XMPP)		Certificate	View
〕 ▶ ise-admin-ise222		Capabilities(3 Pub, 1 Sub)	Online (XMPP)	Administrator	Certificate	View
▶ ise-bridge-ise221		Capabilities(0 Pub, 5 Sub)	Online (XMPP)	Administrator	Certificate	View
〕 ▶ ise-mnt-ise221		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Administrator	Certificate	View
▶ ise-admin-ise221		Capabilities(5 Pub, 2 Sub)	Online (XMPP)	Administrator	Certificate	View
▶ ise-fanout-ise221		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Administrator	Certificate	View
▶ ise-pubsub-ise221		Capabilities(0 Pub, 0 Sub)	Online (XMPP)		Certificate	View
▶ ise-pubsub-ise222		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)		Certificate	View
Iveaction		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Basic	UserName/Password	View
▶ ise221-dnac-intg		Capabilities(0 Pub, 2 Sub)	Online (XMPP)	Session	Certificate	View
▶ ise221		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Session	Certificate	View

From the LiveNX Cisco ISE Integration page, click **Connect** to connect the newly created user to the Cisco ISE host.

me	10.4.25
Username	livea
rd L	.tx6Uu2t8RWXUtCs
C	Create New User Conn

The Cisco ISE status displays as *Connected*.

		Cisco ISE configuration has saved × successfully.
CONFIGURED CISCO I	SE	CREATE NEW CISCO ISE USER
Hostname	10.4.250.221	HOSTNAME *
PXGrid Username	liveaction	Hostname
Status	<ul> <li>Connected</li> </ul>	PXGRID USERNAME *
Edit 🖉	Delete 🗃	PXGrid Username
Lon g		Create

Usernames learned from ISE will now appear in LiveNX reports.



#### Cisco SD-WAN

The Cisco SD-WAN tab provides integration to Cisco vManage. In Cisco SDWAN environments, LiveNX will poll vManage for SDWAN alerts, configuration and tunnel statistics.

		^		ADD CISCO SD	-WAN
nt			Occurrentian October		
			Connection Settings		
			Hostname *	Username *	Password *
			Hostname	Username	
	^		Bypass Proxy		
			Additional HTTP Header		
			Add HTTP Header		
					Submit
	~				

To integrate LiveNX to vManage enter the vManage hostname or IP address, set the username and password, and click **Save**.

If required, and a proxy is required to connect to vManage, click **Add HTTP Header** and enter the *Key* and *Value*. When finished, click **Submit**.

Connection Settings			
Hostname *	Username *	Password *	
Hostname	Username		
	Value *	🔘 Plain Text 🔵 Base64	
Key * Header	Value		Ē

Once LiveNX has established a connection with vManage, the *Status* shows as *Connected*. LiveNX can import cEdge and vEdge router inventory from vManage.

Usetnesse			100 10 1 10
Hostname:			198.18.1.10
Username:			admin
Status:			Connected
	EDIT	DELETE	
	Recheck Status	Discover	(!)

To begin this process, click **Discover**.

CONFIGURED CISCO SD-WAN		
Hostname Username Status	198.18.1.10 admin Connected	
EDIT	DELETE	
Recheck Status	Discover ①	

Enter the IP address(es) of interest in the *Specify IP Ranges* field to define the IP range of SD-WAN devices LiveNX will discover from vManage. These device's management IPs must have connectivity to LiveNX.

1. What to scan	2.	SNMP Settings	3. Nod	9
SPECIFY IP RANGES		CISCO SD-WAN TO L	IVENX SITE MAPPING	
198.18.134.100-106		Map the site IDs for S Sites Mapped: 0	D-WAN devices to LiveN	X sites
Add More		Set Mapping		
				Save & Next

LiveNX Sites and vManage Sites are defined differently. To ensure vManage sites are accurately mapped to LiveNX sites, click **Set Mapping**.

1. What to scan	2. SNMP Settings	3. Node
SPECIFY IP RANGES	CISCO SD-WAN TO	LIVENX SITE MAPPING
198.18.134.100-106	Map the site IDs for Sites Mapped: 0	SD-WAN devices to LiveNX sites
Add More	Set Mapping	
		Save & Next

The Cisco SD-WAN Site Mapping modal appears.

SCO SD-WAN SITE MAPPING view the site IDs for SD-WAN devices, go to vManage > Configuration > Devices s marked as "New" will be created only if a device(s) with the matching site ID is found.				
	to download an example	, ,, ,	2.	
Add	Import CSV File	Edit Delete		
	SD-WAN SITE ID	LIVENX SITE NAME	NEW LIVENX SITE	
	SD-WAN Site ID	LiveNX Site Name	All ~	
		No Data		

To add an individual site, click Add.

CISCO	SD-WAN SITE MAPPIN	IG	×		
	To view the site IDs for SD-WAN devices, go to vManage > Configuration > Devices Sites marked as "New" will be created only if a device(s) with the matching site ID is found.				
Click here	Click here to download an example CSV file				
Add	Import CSV File	Edit Delete			
	SD-WAN SITE ID	LIVENX SITE NAME	NEW LIVENX SITE		
	SD-WAN Site ID	LiveNX Site Name	All ~		
		No Data			
		c	Cancel Apply		

Enter the SD-WAN Site ID and LiveNX Site Name and click Add.

EDIT SITE MAPPING	×
SD-WAN SITE ID	LIVENX SITE NAME
100	DC1-San-Jose
	Cancel Add

Repeat for all *SD-WAN Site ID's* and *LiveNX Site Names* to be added into the system. When done, the site mapping is listed.

CISCO	CISCO SD-WAN SITE MAPPING X						
		es, go to vManage > Configuration > Devices only if a device(s) with the matching site ID is found.					
Click her	e to download an example C	SV file					
Add	Add Import CSV File Edit Delete						
	SD-WAN SITE ID	LIVENX SITE NAME	NEW LIVENX SITE				
	SD-WAN Site ID	LiveNX Site Name	All ~				
	100	DC1-San-Jose					
	200	DC2-RTP	✓				
	300	Branch1-Miami	~				
	400	Branch2-Chicago 🗸					
All rows	/ 4						

If desired, sites can also be added via CSV file. Click Import CSV File to import a CSV.

Cancel

Apply

dd	Import CSV File	Edit Delete	NEW LIVENX SITE
	SD-WAN Site ID	LiveNX Site Name	All
	100	DC1-San-Jose	All
	200	DC2-RTP	~
	300	Branch1-Miami	~
	400	Branch2-Chicago	~

Below is an example CSV.

	A	В
1	vManage Side ID	LiveNX Site Name
2	[You can use Configurations > Devices at Cisco vManage console to get Side ID's]	[required]
3	100	DC1-San-Jose
4	200	DC2-RTP
5	300	Branch1-Miami
6	400	Branch2-Chicago

**Note** The example file also includes the existing LiveNX site(s) already defined in LiveNX. These sites can be associated with Cisco SD-WAN (Viptela) site ID's.

If there are any invalid entries in the .csv file, the rows will be ignored.

When ready, click Save & Next.

DISCOVER DEVICES		×
1. What to scan	2. SNMP Settings	3. Node
SPECIFY IP RANGES	CISCO SD-WAN TO	LIVENX SITE MAPPING
198.18.134.100-106	Map the site IDs for Sites Mapped: 0	r SD-WAN devices to LiveNX sites
Add More	Set Mapping	
		Save & Next
		Cancel Discover

The *SNMP Settings* tab appears. Select the desired SNMP credentials for LiveNX to monitor these SDWAN devices.

Note: Easy onboarding via API integration to vManage and the SNMP polling of the devices are separate processes. If the SNMP settings are incorrect or if LiveNX does not have connectivity to the devices via SNMP – the devices will show up as gray or unreachable.

When ready, click Save & Next.

DISCOVER DEVICES		×
1. What to scan	2. SNMP Settings	3. Node
DEFAULT SNMP CONNECTION SETTINGS SNMP Credential Storage Configuration Page     ENTER SNMP CONNECTION SETTINGS FOR		
Back		Save & Next
		Cancel Discover

The *Node* tab appears. From the *Specify Node* picker, select the LiveNX Node that will monitor these SDWAN devices. When ready, click **Discover**.

DISCOVER DEVICES		×
1. What to scan	2. SNMP Settings	3. Node
SPECIFY NODE		
Local/Server		
Back		
		Cancel Discover

The Device Management page appears and displays the discovery progress log.

≡	LiveAction	NX	
Device	e Management 📀		
	My I	Devices (1)	My Interfaces (5)
DI	SCOVERY LOGS:	1/9	•
•	Stop		

The devices discovered from vManage appears on the LiveNX *Discovered Devices* tab.

	14- P (0)						P Device Discover Device
	My Devices (0)		My Interfaces (0)		Discovered Devices (7)	0	Autodiscovery (0)
1/2 SELECT DE	EVICES Devices: 7	Interfaces: 39					
Add All Devi	ices Edit			Selected: 7		Q Search	
DEV	/ICE 🗘	SERIAL \$	IP ADDRESS	VENDOR 🗘	MODEL \$	NODE \$	INTERFACES \$
	Device	Serial	IP Address	Vendor	Model	Node	Interfaces
BR1	1-VEDGE1	1B86EC86	198.18.134.104	Viptela	vedge-cloud	Local/Server	8
BR1	1-VEDGE2	A8709F71	198.18.134.105	Viptela	vedge-cloud	Local/Server	6
BR2	2-VEDGE1	9E8556D6	198.18.134.106	Viptela	vedge-cloud	Local/Server	5
DC1	1-VEDGE1	EE08F743	198.18.134.100	Viptela	vedge-cloud	Local/Server	5
DC1	1-VEDGE2	B02445F6	198.18.134.101	Viptela	vedge-cloud	Local/Server	5
DC2	2-VEDGE1	4222EF5F	198.18.134.102	Viptela	vedge-cloud	Local/Server	5
DC2	2-VEDGE2	1CA57AE3	198.18.134.103	Viptela	vedge-cloud	Local/Server	5
All rows / 7							

Adding these discovered devices to the LiveNX inventory is now identical to device discovery of any other SNMP monitored device.

If desired, select the devices and click **Edit** to set or override the device site name, group and polling settings.

If desired, click **Select Interfaces** to define which interfaces LiveNX should monitor on these SDWAN devices. Or, to use the default learned settings, click **Add All Devices**.

# Licensing

*License Configuration* is used for managing the system's license. This can be done using the LiveAction's cloud licensing portal or via a traditional license file supply by LiveNX Support.

Settings			
Q Search			
		LICENSE CONFIGURATION	
Configuration			
Data Source Management		Description	LiveNX License type
Data Store Management	~	Internet access is not a must	Cloud Tradition
Davies Fatily Dava Davasta		Licenses can also be managed with the Management Console	
Device Entity Page Reports		CONSOL	Actions
Email Configuration		LiveNX	
Integrations	~		Change License
Cisco APIC-EM / DNA-C		Compatible version: 21.1, 21.2, 21.3, 21.4, 21.5 License expires: Jul 07, 2025 02:59:59 EDT (GMT-04:00)	Described a Manager
		License expires: Jul 07, 2023 02:39:39 EDT (GMT-04:00) License issue date: Jul 07, 2015 20:00:00 EDT (GMT-04:00)	Deactivate License
Cisco ISE		License number: LiveAction-Web-Clark	
Cisco SD-WAN		License type: Permanent	
LiveNCA		Maintenance expiration date: No maintenance	
ServiceNow		Maximum number of devices: Unlimited	
Licensing	~	Maximum historical data: No limit	
Licensing	^	Status: License OK	
License Configuration		Technology modules: LiveNX QoS, LiveNX Flow, LiveNX	
License Expiration Notification		Routing, LiveNX IP SLA, LiveNX LAN	
LiveNA Configuration			
	-	Cloud Monitor	
Mounted Data		Maximum number of Cloud Entity Count (CEC): N/A	
Nodes			
Properties	~	LiveUX	
Proxy		Maximum number of agents supported: N/A	
Reports	~		

When using LiveNX for the first time, a license must be applied. It is recommended to use the cloud license portal.

To apply a cloud license, from the *Cloud* section of the Licensing page, click **Add License**.

Settings		
Q Search	LICENSING	
Licensing ^		
License Configuration	RECOMMENDED	
Proxy	Cloud Requires internet access Online license management	Traditional Internet access is not a must Licenses can also be managed with the Management Console
	I already have a license key and secret Add License Register for a cloud license account and obtain a 14 day trial license. Use Trial License	Laiready have a license file Add License Use the 14 day trial license bundled with the installation. Use Trial License

Supply the license Key and Secret and click Next.

**Note** The key and Secret can be found from the LiveAction Licensing Portal.

Settings		
Q Search		
Licensing ^	LICENSIN	
License Configuration	ADDING CLOUD LICENSE	×
Proxy	Log into your LiveAction Licensing Portal account to obtain the key and secret for your license.	Traditional
	Кеу	Internet access is not a must
	Key	Licenses can also be managed with the Management Console
	Secret	
	Secret	I already have a license file
	Cancel Next	Add License
		Use the 14 day trial license bundled with the installation.
	Use Trial License	Use Trial License

Review the license's details and click Yes.

re you sure you want to activate this	license?
Compatible version :	9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 21.1, 21.2
License number :	a0f2G0000015tTT
License type :	Permanent
Maximum number of devices :	100
Maximum number of agents supported :	2
Maximum number of Cloud Entity Count (CEC) :	10
Maximum historical data :	No limit
Technology modules :	LiveNX QoS, LiveNX Flow, LiveNX Routing, LiveNX IP SLA, LiveNX LAN
License issue date :	Oct 21, 2020 00:42:00 PDT (GMT-07:00)
License expires :	No expiration
Maintenance expiration date :	Oct 21, 2025 00:42:00 PDT (GMT-07:00)
Status :	License OK

The license will be applied and LiveNX will be ready to use.

LICENSING	
Description	LiveNX License type
Requires internet access	Cloud Traditional
Online license management	
Requires WebUI available via All-in-One OVA to manage licenses	Actions
LiveNX	Change License
Compatible version : 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 21.1, 21.2	Refresh License
License number : a0f2G00000I5tTT	
License type : Permanent	Deactivate License
Maximum number of devices : 100 devices	
Maximum historical data : No limit	
Technology modules : LiveNX QoS, LiveNX Flow, LiveNX	
Routing, LiveNX IP SLA, LiveNX LAN	
License issue date : Oct 21, 2020 00:42:00 PDT (GMT-07:00)	
License expires : No expiration	
Maintenance expiration date : Oct 21, 2025 00:42:00 PDT	
(GMT-07:00)	
Status : License OK	

If necessary, a Traditional license file can also be used. This can be supplied by LiveAction Support. To add a Traditional license, from the *Traditional* section of the *Licensing* page, click **Add License**.

Settings		
Q Search	LICENSING	
Licensing ^		
License Configuration	RECOMMENDED	
Proxy	Cloud	Traditional
	Requires internet access Online license management	Internet access is not a must Licenses can also be managed with the Management Console
	I already have a license key and secret Add License Register for a cloud license account and obtain a 14 day trial license. Use Trial License	Laiready have a license file Add License Use the 14 day trial license bundled with the installation. Use Trial License

The *Adding Traditional License* modal appears. Browse to find the ".key" license file supplied by LiveAction Support and click **Next**.

Settings		
Q Search	LICENSING	
Licensing		
License Configuration		
Proxy	ADDING TRADITIONAL LICENSE × Traditional Upload Your License File LiveAction-9.0-EXT-D100-210904.key ■ Browse Cancel Next I already have a license file Add License	
	Register for a cloud license account and obtain a 14 day trial license. Use the 14 day trial license bundled with the installation. Use Trial License Use Trial License	

The license will be applied and LiveNX will be ready to use.

LICENSING	
Description	LiveNX License type
Internet access is not a must	Cloud Traditional
Licenses can also be managed with the Management Console	
	Actions
LiveNX	Change License
Compatible version : 21.1, 21.2, 21.3	
License number : LiveAction-Web-Clark	Deactivate License
License type : Permanent	
Maximum number of devices : Unlimited	
Maximum historical data : No limit	
Technology modules : LiveNX QoS, LiveNX Flow, LiveNX	
Routing, LiveNX IP SLA, LiveNX LAN	
License issue date : Jul 07, 2015 20:00:00 EDT (GMT-04:00)	
License expires : Jul 07, 2025 02:59:59 EDT (GMT-04:00)	
Maintenance expiration date : No maintenance Status : License OK	
Status : License OK	
Cloud Monitor	
Maximum number of Cloud Entity Count (CEC) : N/A	
LiveUX	
Maximum number of agents supported : N/A	

*License Expiration Notification* can be used to send an email for notification of impending license expiration.

Settings	
Q Search	
Configuration	
Data Source Management	
Data Store Management	~
Device Entity Page Reports	
Email Configuration	
Integrations	~
Cisco APIC-EM / DNA-C	
Cisco ISE	
Cisco SD-WAN	
LiveNCA	
ServiceNow	
Licensing	^
License Configuration	
License Expiration Notification	
LiveNA Configuration	

## **LiveNA Configuration**

LiveNA is a big data AIOps platform that applies machine learning and heuristics to LiveNX datasets for advanced anomaly detection, predictive analytics for deeper network understanding.

Its role in the LiveAction portfolio is to provide "expert in the box" insights. It accomplished this by baselining and trending what is normal in a network, detecting anomalies, and correlating events for deeper network and application performance insights.

Settings		
Q Search		
Configuration	^	LIVENA CONFIGURATION
Data Source Management		
Data Store		
Device Entity Page Reports		
Email Configuration		
Integrations	~	
Licensing	^	There is no connected LiveNA system.
License Configuration		Connect LiveNA
License Expiration Notification		CORECT DIRAK
LiveNA Configuration Mounted Data		
Nodes		
Properties	~	
Proxy		
Reports	~	
Security	~	
Single Sign On		
SNMP Trap		
Syslog		
Troublashaating	U V	

To Integrate LiveNX to a LiveNA, click **Connect LiveNA**.

LiveNA
©
There is no connected LiveNA system.
Connect LiveNA

Add the LiveNA Hostname, Port, and API key and click Submit.

Hostname *		
Port *		
		-
API Key *		
API Key		
	Cancel	Submit

After the LiveNA connection has been established, LiveNA will need to be configured with which devices in LiveNX's inventory it needs to monitor. To add devices for LiveNA to monitor, from the *Monitored Devices* tab click **Add**.

NA Information			
	1.0-20210205-3253651 Status: • Connected		
Monitored D	wices	Monitored &	optications 🕤
dd Delete			Q Search
DEVICE NAME		REGION	TAGS O

The Add Devices modal appears, select the devices of interest and click Add.

			Q Search			
	DEVICE NAME	SITE	0	REGION	\$ TAGS	
1						
1	IWAN-BR_INET.liveaction.cisco	Tokyo		Tokyo	iwan, IPSLA	
	IWAN-BR_MPLS.liveaction.com	Tokyo		Tokyo		
	IWAN-Br1_Sydney.liveaction.com	Sydney		Sydney		
	IWAN-DC-MC.liveaction.com					
	IWAN-DC-MC.IIVeaction.com	Tokyo		Tokyo		
2	s: 4/4 Selected: 4	Tokyo		Tokyo		

The selected devices appears on the *Monitor Devices* tab.

	Monitored Devices			Monitored Ap	pplications	
Delete	port SNMP Data			Q		
DEVICE NAME	≎ sn	те	REGION	\$	TAGS	
IWAN-BR_INET.liveaction	.cisco.com To	iokyo	Tokyo		IPSLA, Cisco RTRs, Cisco, iwan	
IWAN-BR_MPLS.liveactio	n.com Tc	okyo	Tokyo		mpls, Cisco RTRs, Cisco	
IWAN-Br1_Sydney.liveact	ion.com Sy	ydney	Sydney		Cisco RTRs, Cisco	
IWAN-DC-MC.liveaction.c	om To	okyo	Tokyo		Cisco RTRs, Cisco	

The **Import SNMP Data** button can be used for LiveNA to query and import any relevant historic device data that is available from LiveNX. This will allow LiveNA to immediately provide value for SNMP use cases as it can learn and trend the patterns of this historic data.

LiveNA	Status				
Hostna	me: 172.22.0.110 Port: 34524	v	/ersion: 21.2.1-2021042		
	Monitored De	vices			
Add	Delete Import SNMP Data				
	DEVICE NAME	\$ SITE			
	IWAN-BR_INET.liveaction.cisco.com	Tokyo			
	IWAN-BR_MPLS.liveaction.com	Tokyo			
	IWAN-Br1_Sydney.liveaction.com	Sydney	IMPOR	SNMP DATA	×
	IWAN-DC-MC liveaction.com	Trikun	will be ove Are you su	out to import SNMP data from LiveN? rwritten. re you want to proceed? <b>a for selected time range:</b>	X. All previous LiveNA data
			90 days		$\sim$
					Cancel Proceed

By default, LiveNA will learn and monitor the top 100 application on the devices it is monitoring. This is based on network utilization. These top 100 could change over time. To ensure LiveNA residually monitors key applications of interest, Application Groups can be added to the *Monitored Applications* tab. These will be monitored in addition to the auto-learned top 100 applications. To add an Application Group, from the *Monitored Applications* tab, click **Add**.

LiveNA Information				
Hostname: 172.22.0.110	Port: 34524	Version: 21.1.0-20210205-3253651	Status:  Connected	
		Monitored Devices		Monitored Applications ()
Add Delete				Q Search
APPLICATION GROUP	APPLICATIONS			٥

The *Add Applications* modal appears and lists the Application Groups defined in LiveNX. Select an Application Group and click **Add**.

		Q Search	
	APPLICATION GROUP	APPLICATIONS	
		Applications	
	pop3-group	pop3, secure-pop3	
	instant-messaging	aol-protocol, gtalk-chat, irc, ntalk, kakao-talk, secure-irc, cuseeme, msnp, fring, w	1
	prm-group	prm-nm, prm-sm	
4	ipsec-group	ipsec, isakmp	
	terminal	uucp-rlogin, secure-telnet, ssh, nextstep, login, 914c/g, supdup, nest-protocol, ha	
	vnc-group	vnc, vnc-http	
	peer-to-peer	waste, filetopia, soulseek, tomatopang, goboogy, manolito, perfect-dark, pando,	
	oracle-group	oracle, oracle-bi, oracle-ebsuite-unsecured, oraclenames, oraclenet8cman, oracl	
	kerberos-group	kerberos, kpasswd	
	amazon-group	amazon, amazon-s3, amazon-cloudfront, amazon-ec2, amazon-instant-video, a	

The selected Application Groups will be listed on the *Monitored Applications* tab.

Delete		Version: 21.1.0-20210265-3253651 Monitored Devices	Status:   Connected	Monitored Applications (1)	Q Seath.
Delete	h APPLICATIONS		Status:    Connected	Monitored Applications (1)	O Cauch
ATTON GROUP   Cation Group	APPLICATIONS	Monitored Devices		Monitored Applications (*)	O Sauch
ATTON GROUP   Cation Group	APPLICATIONS	Monitored Devices		Monitored Applications 🕥	C Sauch
ATTON GROUP   Cation Group					Q Search
Ication Group					G central.
					0
messenger-group	yahoo-messenger, yahoo-mess	senger-video, yahoo-voip-messenger, yahoo-voip-over	sip		
k-service	texar, hmp, hamachi, icmp, egp	, vid, tacnews, creativepartnr, mobilip-mn, rap, surf, xf	ler, amanda, kryptolan, profile, any-host-inter	mal, apo-powerchute, an, openport, genrad-mux, dgp, worldfusion, cddbp-alt, compaq-peer, uis, set, scps, statistic	cal-p2p, dcn-meas, idpr, tnETOS, ieee-mms, utmpsd, bdp, cisco
rideo	rdt, facetime, dmp, rsvp_tunnel,	l, shockwave, ppstream, tpip, adobe-connect, rtcp, airg	play, rpc2portmap, sflow, dnp, rtsp, web-rtc-	video, cisco-tv, web-rtc, mgcp, audio-over-http, napster, ups, itunes-media, zattoo, h225, netshow, rtsps, netvmg-t	raceroute, mpeg2-ts, netflix, viber, cisco-ip-camera, sip-tis, date
ew-Custom	tr-rsrb-p3, codima-rtp				
roup	gtaik, gtaik-chat, gtaik-ft, gtaik-	video, gtalk-voip			
	brighttalk, hotmail, ms-dynamic	cs-crm-online, quic, instagram, tianya, tus-files, twitch	-tv, nate-com, wikia, ted, retailmenot, mail g	mx-mail, priceline-com, goodreads, california-gov, livedoor, windows-azure, jimdo, bbc, mailchimp, gilthub, indiego	ogo, dangdang, nbc-news, ameba, http-local-net, hostgator, letv
ver	activesync, sift-uft, pftp, td-repi	lica, cvsup, afpovertcp, sst, backup-service, softros-m	essenger-ft, cifs, rcp, uucp-path, connected	Hackup, prospero, mftp, saft, smartpackets, xact-backup, zannet, novastorbakcup, binary-over-http, rsync, crash	plan, fatserv, tapeware, nfs, lockd, remotefs, adobe-services, net
roup	fring, fring-video, fring-voip				
video ew-C roup ver	ustom	rdt, facetime, dmp, rsvp, tunne ustom tr-rsrb-p3, codima-rtp gtalk, gtalk-chat, gtalk-ft, gtalk brighttalk, hotmail, ms-dynami	ndt, fauelime, dmp, nvp_tunnel, shockwave, posteaum, tpip, adobe-connect, stop, alig ustom tr-sas-bit_codima-tp gfatak, datak-chat, gfatak-rtig gfatak-vision, gfatak-vojp brightatak, hotmak, ord-paramics.cmm-ortion, quici, instagram, tianya, tus-files, hetich activesync, sitt-utt, pfatp, to-replica, crisap, afpowritop, sit, backup-service, softworm	ret, facefime, drng, rsyng, turnei, sknockware, pastream, tpip, adobe-connect, rtop, airpiazy, rpc2portmap, alfow, drp, rtop, web-rto- ter seb-p3, codima-rtp graak, graak-chat, graak-rt, graak-viop bigtratak, homain, en opknames-erm-oninie, gaie, instagraam, tianya, tue-fiee, twitch-ty, nate-com, wikia, ted, retainmend, mair activesync, sint-st, pfip, tor-replica, croup, alpovertop, sst, backup-service, softwor-messenger R, clifs, rop, suc-path, connected	rd, facetime, dmg, roys, Junnel, shockwave, postewam, tpig, adobe-connect, rictp, anjszer, pc2portmap, aflow, drg, ritap, web-ric-videro, cisco-tv, web-ric, mgcp, audio-ver-http, naptizer, ups, fitunes-media, zatiloo, h225, netshow, ritaps, netming- terseb-p2, coloma-rb grafast, batal-main, equipartias-to-monitor, equip. Intragram, tiamy, tau-fite, het/c-br, nate-com, wikis, ted, retailment, mail gms-mail, proceine-com, goodreads, california-gor, livedoc, window-azure, jimdo, bbc, mailchamp, githua, indeg activesync, sift-ut, fptis-frequence-com, equip. Intragram, tiamy, tau-fites, het/c-br, nate-com, wikis, ted, retailment, mail gms-mail, proceine-com, goodreads, california-gor, livedoc, window-azure, jimdo, bbc, mailchamp, githua, indeg activesync, sift-ut, fptis-frequence-com, equip. stat. backup-service, softwos-mesenger-R, cifs, rup, sucp-path, connected-backup, prospen, mttp, saft, smartpacets, xachackup, zanned, novastoralacup, binary-over-http, rync, crash

The **Edit Data Source** button allows customization of which interfaces LiveNA will monitor for its baselining and predictive use cases.

View Device Management	Edit Data Source Delete Configuration	Recheck Status	Edit Connectio
	EDIT DATA SOURCE	×	
	WAN interfaces provide data by default. Also, you o service provider tags to provide data to LiveNA.	can select interface and	
	• WAN WAN and XCon		
	Select interface tag		
	Service provider tags		
	Select service provider tag		
		Cancel Save	

The **Recheck Status** button ensures LiveNX is in sync the latest health of LiveNA.

					1	
	View Device Manage	ement Edit Da	ta Source	Delete Configuration	Recheck S	Status
					i	;
A Information			,			
name: 172.22.0.110	Port: 34524 Vers	sion: 21.1.0-20210205-3253651	Status: • Error			
			'			
reNA Information			1			
ostname: 172.22.0.110	Port: 34524 Version	x 21.1.0-20210205-3253651	Status: Connected			

## **Mounted Data**

*Mounted Data* allows archived LiveNX data stores to be re-mounted for historic investigation.

Settings					
Q Search	м	DUNTED DATA			
Configuration	∧ Yo	can mount a data directory that contains flow, alert, or QoS data by clicking on th			
Data Source Management	m	ant directory button. All directories in the list below are grouped together by type.			
Data Store Management	~	Nount Unmount Increase Priority Decrease Priority			Q Search
Device Entity Page Reports		PRIORITY TYPE DATA DIRECTORY	STATUS	D	
Email Configuration		PRIORITY TYPE DATA DIRECTORY	STATUS	ID	
Integrations	v (				
Cisco APIC-EM / DNA-C					
Cisco ISE					
Cisco SD-WAN					
LiveNCA					
ServiceNow					
Licensing	~		No Data		
License Configuration			NO Data		
License Expiration Notification					
LiveNA Configuration					
Mounted Data					
Nodes					
Properties	~				
Proxy		ows: -			

#### Nodes

*Nodes* is where additional LiveNX Node collectors are integrated to the LiveNX Server.

The LiveNX Server has a built in Node. When additional Nodes are used, a configuration file must be created on the LiveNX server for each Node. This file must be copied to the respective Node to complete the integration.

Settings							
Q Search							
		NODES					
Updates	<u>^</u>						
Reports ~		Add	Remove			Edit Node Configuration	Node Config Export
Email Configuration			NODE NAME	STATUS	NODE ID	LOCATION	0
Single Sign On							
Mounted Data			Local/Server	Connected	269889f7-3887-45e8-87e0-5ebfadabfd31	Local	
Properties ~		All rows	14				
Data Store							
Web UI Data Store							
SNMP Trap							
Syslog							
Nodes							
Configuration	=						
Troubleshooting ^							
Heap Dump							
CPU Profiling							
Logs							
User Activity Tracking							
Packet Capture							
Upload History							

To add a new Node, click Add.

Settings									
Q Search		NODES							
Configuration	^	NUDE	5						
Data Source Management		Add	Remove					Edit Node Configuration	Node Config Export
Data Store Management	~	h	NODE NAME	0	STATUS	\$ NODE ID	0	LOCATION	0
Device Entity Page Reports									
Email Configuration			Local/Server		Connected	269889f7-3887-45e8-87e0-5ebfadabfd31		Local	
Integrations	~		Local/Server		Connected	20988917-3887-4568-6760-5601adabid31		Local	
Cisco APIC-EM / DNA-C									
Cisco ISE									
Cisco SD-WAN									
LiveNCA									
ServiceNow									
Licensing	~								
License Configuration									
License Expiration Notification									
LiveNA Configuration									
Mounted Data									
Nodes									
Properties	~								
Proxy		Rows:	1/1						

The Add Node modal appears. Define the Node's name and IP address and click Save.

NODES						
Add						
	NODE NAME	C STATUS		•	LOCATION	0
		ADD NODE	×			
	Local/Server			387-45e8-87e0-5ebfadabfd31	Local	
All rows	/ 1	PA-Node				
		IP Address				
		10.1.40.21				
			Cancel Save			

The Node appears but displays a status of *Disconnected*.

ODES							
Add	Remove					Edit Node Configuration	Node Config Export
	NODE NAME	\$	STATUS	٥	NODE ID	LOCATION	:
	Node Name						
	Local/Server		Connected		269889f7-3887-45e8-87e0-5ebfadabfd31	Local	
	PA-Node	Node Disconnected 109b75c1-bcae-4d78-bf1c-5d56e46f8a81		10.1.40.21			

To copy the Node's configuration, click Node Config Export.

Add	Remove				Edit Node Configuration	Node Config Export
	NODE NAME	\$ STATUS	¢	NODE ID	LOCATION	
	Local/Server	Connected		269889f7-3887-45e8-87e0-5ebfadabfd31	Local	
	PA-Node	Disconnected		109b75c1-bcae-4d78-bf1c-5d56e46f8a81	10.1.40.21	

The Export Node Configuration File appears. An optional password may be entered. Click Export.

NODES							
Add	Remove					Edit Node Configuration	Node Config Export
	NODE NAME	EXPORT NODE CONNECTION FILE	×		^	LOCATION	0
	NODE NAME	Node Name			ř	LOCATION	×
		PA-Node					
	Local/Server	IP Address		387-45e8-87e0-5ebfadabfd31		Local	
	PA-Node	10.1.40.21		04-4a52-80d4-b0ebbfbc16b3		10.1.40.21	
All rows	/ 2	Encrypt					
		Password					
		Add password	۲				
		Repeat Password					
		Confirm password	۲				
		Cancel Export					

Save the Node's config file for import into the Node.

Opening PA-Node.nodeconn	X
You have chosen to open:	
PA-Node.nodeconn	
which is: nodeconn File (3.3 KB)	
from: blob:	
What should Firefox do with this file?	
Open with Browse	
Save File	
	OK Cancel

Once the Node has been installed and its configuration file imported into it, the Node appears as connected.

Settings												
Q Search												
Reports Access Management	^	NODES										
Email Configuration		Add	Remove						Ed	it Node Configuration	Node Config Export	
Single Sign On		0	NODE NAME	0	STATUS	0	NC	IODE ID	0	LOCATION	0	
Mounted Data												
Properties	^		Node Name		Status			Node ID				
Server Name			PA-Node Local/Server		Connected Connected			ib4ebbb8-8828-4f1a-852d-ce7ca3fbecd7 269889f7-3887-45e8-87e0-5ebfadabfd31		10.1.40.21 Local		
LiveNX Properties Device Auto-refresh		All rows			oonnected		20	0700717-0007-4060-0760-060100001001		Loour		
Web Properties	- n .											
Data Store												
Web UI Data Store												
SNMP Trap												
Syslog	=											
Nodes												
Configuration												
Troubleshooting	~											
Security	~											

*Configuration* provides the ability to backup or restore the LiveNX configuration, restart the server, or reset the configuration to default.

ettings	
Q Search	
onfiguration	
ata Source Management	
ta Store Management	~
rice Entity Page Reports	
onfiguration	
ations	~
ng	~
se Configuration	
e Expiration Notification	
nfiguration	
Data	
S	~

# **Properties**

*Server Name* defines the LiveNX server's name. If the name is modified, the LiveNX service needs to be restarted.

Settings	
Q Search	
Licensing	~
License Configuration	
License Expiration Notification	
LiveNA Configuration	
Mounted Data	
Nodes	
Properties	~
Device Auto-refresh	
LiveNX Properties	
Server Name	
Third-party Services	
Web Properties	
Proxy	
Reports	$\sim$

*LiveNX Properties* are a list of system settings that could need to be adjusted in some circumstances.

Care should be taken when changing these parameters and it is suggested to work with the LiveNX support team.

sing	~ ^	LIVENX PROPERTIES If any of the settings below are modified, the set	ervice needs to be restarted in order for the changes to take effect.	
ense Configuration				
ense Expiration Notification		NAME	VALUE	-
IA Configuration		app.datadir	/data/livenx-server/data	
ed Data		cache.application.enabled	True	~
rties	~	clientgateway.ssl.port	7000	0
es Auto-refresh		collectormode.enabled	False	~
Properties		dnac.enabled	False	~
Name				
party Services		flow.collector.netflow.port	2055	٥
operties		flow.collector.sflow.port	6343	0
		hide.historical.devices	False	~
	~	httpserver.api.enabled	True	~
gn On	~	httpserver.api.port	8093	٥
Trap		httpserver.host	216.218.254.20	
ih.				``````````````````````````````````````

*Device Auto-Refresh* can be enabled to ensure LiveNX does a full SNMP refresh of the devices in its inventory at a residual interval.

Settings	
Q Search	
Licensing	~ ^
License Configuration	
License Expiration Notification	
LiveNA Configuration	
Mounted Data	
Nodes	
Properties	^
Device Auto-refresh	
LiveNX Properties	
Server Name	
Third-party Services	
Web Properties	
Proxy	

*Third Party Services* determines if LiveNX will reach out to external APIs for enhancing the user experience. These features may be disabled by deselecting the respective service.

Settings			
Q Search			
Uata source Management			THIRD PARTY SERVICES
Data Store Management	~		
	Ť		Select All Unselect All
Device Entity Page Reports	_		☑ WalkMe
Email Configuration			Used to present users with release notes as well as provide walk-throughs for specific features. When disabled release notes and walk-throughs will not be shown.
Integrations	~		Google Maps API
Licensing	Ň		Used for geo lookup initiated from Site Edit dialog in Site Management. Maybe used as the fallback for bulk lookup if HERE service fails. When disabled, geo lookup will not be available.
License Configuration			
License Expiration Notification			HERE Maps API Used for geo lookup and reverse geo lookup when bulk importing sites. When disabled, geo lookup will not be
LiveNA Configuration			available
Mounted Data			Leaflet Maps Used to display map underlay using cartodb tiles on GeoTopology. When disabled, simplified map will be
Nodes			displayed instead.
Properties	^		Apply
Device Auto-refresh			
LiveNX Properties			
Server Name			
Third-party Services			
Web Properties			
Proxy			
Reports	~		
Flow Reports Results Limit			

*Web Properties* defined the default *Auto Refresh Time* of Dashboards, Site, Devices, Interfaces, WAN Applications, Network Users, Site to Site Analysis, and Geo Topology.

Settings	
Q Search	
Licensing	~
License Configuration	
License Expiration Notification	
LiveNA Configuration	
Mounted Data	
Nodes	
Properties	^
Device Auto-refresh	
LiveNX Properties	
Server Name	
Third-party Services Web Properties	
Proxy	
Reports	~
Reports	Ý

## Proxy

*Proxy* configuration settings can be used if LiveNX needs to communicate through a proxy server.

C Search  Licensing License Configuration License Expiration Notification LiveNA Configuration	~ ^
License Configuration	~ ^
License Configuration	~ ~
License Expiration Notification	
Mounted Data	
Nodes	
Properties	~
Device Auto-refresh	
LiveNX Properties	
Server Name	
Third-party Services	
Web Properties	
Proxy	
Reports	~
Security	~

## Reports

*Time Range Restrictions* allows for the limiting of the duration of Analysis Reports. This can be used to ensure processor intensive reports do not hold up the report queue.

The Analysis reports are currently:

- All Unique Flows
- IPs and Ports
- Security Analysis
- Top Analysis

Settings	
Q Search	
License Configuration	1
License Expiration Notification	
LiveNA Configuration	
Mounted Data	
Nodes	
Properties	~
Proxy	
Reports Flow Reports Results Limit	^
Logo	
Long Term Processing Reports	
Report History	
Reports Management	
Time Range Restrictions	
Security	~
Single Sign On	

*Flow Report Results Limit* allow for adjustment of the returned results of Flow reports. By default, most Flow reports limit the returned results to 1000 rows, but this setting allows for more returned results. Caution should be used when adjusting this setting to not impact the overall system performance.

Settings	
Q Search	
License Configuration	^
License Expiration Notification	
LiveNA Configuration	
Mounted Data	
Nodes	
Properties	~
Proxy	
Reports	^
Flow Reports Results Limit	
Logo	
Long Term Processing Reports	
Report History	
Reports Management	
Time Range Restrictions	
Security	~

*Logo* allows you give a custom logo to shared and PDF reports. The logo page allows for the uploading and management of logos.

Settings	
Q Search	
License Configuration License Expiration Notification	^
Mounted Data	
Nodes	
Properties	~
Proxy	
Reports	^
Flow Reports Results Limit	
Long Term Processing Reports	
Report History	
Reports Management	
Time Range Restrictions	
Security	~
Single Sign On	

*Report History* provides management to each users personalized report history.

		REPORT HISTORY
	^	
		Available Free Space: 167.37 GB Total Disk Space: 249.88 GB
		Other Store Size:     Peport Store Size:     Max Report Store Size:     0.74 GB     1.77 GB     200     C GB
		00.74 GD 1.77 GD 200 🗸 GD
	~	You can set how long different report type results are stored on LiveNX server.
Ť		
		AD HOC Reports
	^	1 Oays
		Scheduled Reports
		365 Oays
		Shared Reports
		7 Days
		Reset to Default Revert Changes Submit
~		

*Long Term Processing Reports* allows for selection of which reports will have their data sent to the Long Term Flow store.

ttings						
icense Configuration	^	<b>`</b>	Note: Enablin	RM PROCESSING REPORTS glong term processing can significantly impact LiveNX memor	y and CPU usa	ge
eNA Configuration			Reports			
Data			Disabled	AS Pair	Disabled	Application Performance By Device
			Disabled	Application Performance By Interface	Disabled	Application Performance By Service Provi
	~		Disabled	Application Performance By Site	Disabled	Bidirectional AS Pair
5	*		Disabled	Bidirectional Network Pair	Disabled	Bidirectional Source/Destination Pair
			Disabled	Business Relevance	Disabled	Destination AS
	^		Disabled	Destination Network	Disabled	Destination Site Traffic
orts Results Limit			Disabled	Jitter/Loss	Disabled	Network Pair
			Disabled	Out of Policy Events	Disabled	Protocol
rm Processing Reports			Disabled	Protocol Port	Disabled	Site Traffic
rt History			Disabled	Source AS	Disabled	Source Network
rts Management			Disabled	Source Site Traffic	Disabled	Source or Destination AS
ange Restrictions			Disabled	Source or Destination Address	Disabled	Source or Destination Network
	~		Disabled	Top Applications Performance	Disabled	Top Voice/Video Performance Summary
ign On			Enabled	Top Voice/Video Performance by SSRC	Disabled	Traffic Class
ар			Enabled	Voice/Video Performance By Device	Disabled	Voice/Video Performance By Interface
			Disabled	Voice/Video Performance By Service Provider	Enabled	Voice/Video Performance By Site
hooting	~		Dynamic re			

*Reports Management* allows deletion and ownership re-assignment to report templates of both active and deleted users.

Q Search			DED	ORTS MANAGEMENT					
icense Configuration		^	KEF	JATS MANAGEMENT					
icense Expiration Notification			Re-	assign Ownership Delete				Q Search	
eNA Configuration				REPORT TEMPLATE NAME	0	SCHEDULED REPORT	OWNER	OWNER STATUS	0
punted Data									
odes				Report Template Name		All		All	×
roperties	~			21 reports-test2			amyadmin	Active	
oxy				Application			amyadmin	Active	
				BKP app all		~	kparsons	Active	
ports	^			IWAN-I			rlonie	Active	
low Reports Results Limit				chadss voice template			chadadmin	Active	
ogo				dscp			jloo	Active	
ong Term Processing Reports				Slow report			amyadmin	Active	
Report History				FlexSearchTesting			amyadmin	Active	
Reports Management				21 reports			amyadmin	Active	
ime Range Restrictions				Top SNMP			gaurav	Active	
				Report Group Parameter Test - Hari			hari	Active	
curity	~			Interface Availability, Last Fifteen Minutes			amyadmin	Active	
gle Sign On				Top Interface Bandwidths			amyadmin	Active	
MP Trap				Weekly avail			chadadmin	Active	
log				SNMP Flex Search			amyadmin	Active	
publeshooting	~		Row	s: 55 / 55					

*Reports Access Management* defines which reports non-Admin users can run. Do note that some reports which drive workflows cannot be disabled.

Settings		
Q Search	REPORTS ACCESS MANAGEMENT	
Licensing ^		
License Configuration	Q Search	
License Expiration Notification	✓ Test	
Proxy	☑ LiveNA	
Device Entity Page Reports	Flow	
Updates	SNMP V	
Reports ^	Cisco SD-WAN V	
Time Range Restrictions	Z Alert 🗸	
Flow Reports Results Limit		
Logo		
Report History		
Long Term Processing Report		
Reports Management		
Reports Access Management		
Email Configuration		
Single Sign On		
Mounted Data	Select All Unselect All Apply	
Properties ~		

## Security

*Login* provides session timeout and failed login attempt parameters of users.

Settings			
Q Search			
License Configuration	^	LOGIN	
License Expiration Notification		Default session timeout *	
NA Configuration		15	$\bigcirc$
unted Data		Number of failed consecutive login attempts *	
les		100	
operties	~	Lock user if number of failed attempts occur in	1
			ho
ts	~		
eports Results Limit			Ap
Term Processing Reports			
ort History			
rts Management			
e Range Restrictions			
ity	^		
n			
word			
Single Sign On			

Password defines the password policy for users.

guration	^
on Notification	
	~
	~
^	

# Single Sign On

*Single Sign On* provides SAML integration via either Okta or ADFS IDPs.

Settings	
Q Search License Configuration License Expiration Notification	^
LiveNA Configuration	
Mounted Data	
Nodes	
Properties	~
Proxy	
Reports	~
Flow Reports Results Limit	
Logo	
Long Term Processing Reports	
Report History	
Reports Management	
Time Range Restrictions	
Security	× I
Login Password	
Single Sign On	
SNMP Trap	

# **SNMP** Trap

*SNMP Traps* allows for configuration of a SNMP server. Any LiveNX alert configured for sharing with SNMP Traps, will be forward to this destination.

Settings	
Q Search	
LiveNA Configuration	1
Mounted Data	
Nodes	
Properties	~
Proxy	
Reports	~
Flow Reports Results Limit	
Logo	
Long Term Processing Reports Report History	- 1
Reports Management	
Time Range Restrictions	
Security	~
Login	
Password	
Single Sign On	
SNMP Trap	
Syslog	
Troubleshooting	~

# Syslog

*Syslog* allows for configuration of a Syslog server. Any LiveNX alert configured for sharing with Syslog, will be forward to this destination.

Settings	
Q Search	
	^
LiveNA Configuration Mounted Data	
Nodes	
Properties	~
Proxy	-
Reports	~
Flow Reports Results Limit	
Logo	
Long Term Processing Reports	
Report History	
Reports Management	
Time Range Restrictions	
Security	~
Login	
Password Single Sign On	
SNMP Trap	
Syslog	
Troubleshooting	~

# Troubleshooting

Heap Dump generates a snapshot of memory for troubleshooting by LiveAction Support.

ettings								
Q Search								
eports ~	^	HEAP DUMP						
Flow Reports Results Limit		Generate Sanitize Existi	Delete				Q Search	
Logo								
Long Term Processing Reports		NODE NAME	NODE PATH	♦ COLL	LECTION START TIME	STATE	♦ SIZE	ODWNLOAD
Report History		Node Name			ollection Start Time	All	<ul> <li>Size</li> </ul>	
Reports Management								
Time Range Restrictions								
curity ~								
.ogin								
Password								
ngle Sign On								
MP Trap					No Data			
yslog					No Data			
roubleshooting ^								
CPU Profiling								
Heap Dump								
Logs								
Packet Capture								
Upload History								
User Activity Tracking		Rows: -						

CPU Profiling generates a snapshot of CPU usage for troubleshooting by LiveAction Support.

Settings															
Q Search															
leports	× ^	CPU PROP	FILING												
Flow Reports Results Limit		Start CPU	Profiling Delete	2						Q					
Long Term Processing Reports		NODE	NAME	0	FILE NAME	0	COLLECTION START TIME	0	DURATION	0	STATE	0	SIZE	0 DO	WNLOAD
Report History Reports Management											All	~			
Time Range Restrictions															
ecurity Login Password	ř														
ngle Sign On															
NMP Trap tyslog			No Data												
roubleshooting CPU Profiling	^														
Heap Dump															
Logs															
Packet Capture Upload History															

Logs generates system log files for troubleshooting by LiveAction Support.

Settings						
Q Search		LOGS				
Reports	× ^	1003				
Flow Reports Results Limit		LiveNX Log Level				
Logo		INFO		✓ Set		
Long Term Processing Reports						
Report History		Manage Logs				
Reports Management						[ <b>-</b>
Time Range Restrictions		Get LiveNX Logs Delete				Q Search
Security	~	NODE NAME	SOURCE	FILE PATH	COLLECTION START TIME	♦ STATE ♦ SIZE ♦ DOWNLOAD
Login						All ~ Size
Password						
Single Sign On						
SNMP Trap						
Syslog						
Troubleshooting	^					
CPU Profiling				No Data		
Heap Dump						
Logs						
Packet Capture						
Upload History						
User Activity Tracking		Rows: -				

*User Activity Tracking* generates system log files of which users have logged into the system and what actions they have taken.

Settings					
Q Search			USER	R ACTIVITY TRACKING	
Integrations	~	^	UULI		
Licensing	~		Activit		
LiveNA Configuration			All	~	
Mounted Data			Do	winload last 6 month logs	
Nodes			Time R	λange	
Properties	~		Last	Fifteen Minutes	
Proxy				USER NAME	0
Reports	~			Vala Mak	× 1
Security	~			User name	
Single Sign On				full-config	^
SNMP Trap				charles	
Syslog				mhampson-clerk tma	
Troubleshooting	~				
CPU Profiling				davat	
Heap Dump				ssidheeq	
Logs				inna_demo1	
Packet Capture				100/103 100/103	~
Upload History					
User Activity Tracking			Dow	vnload All	

Packet Capture generates a TCP	Dump of the LiveNX :	Server's network card.
0		

Cottingo

settings					
Q Search					
Reports	× ^	PACKET CAPTURE			
Flow Reports Results Limit		Capture Packets Delete			Q Search
Logo					
Long Term Processing Reports		NODE NAME	FILE NAME	COLLECTION START TIME	♦ STATE ♦ SIZE ♦ DOWNL
Report History		Node Name		Collection Start Time	All ~ Size
Reports Management					
Time Range Restrictions					
curity	~				
Login					
Password					
ngle Sign On					
IMP Trap				No Data	
rslog				No Data	
oubleshooting	^				
CPU Profiling					
Heap Dump					
Logs					
Packet Capture					
Upload History					
User Activity Tracking		Rows: -			

*Upload History* provides a list of files uploaded to LiveAction support. Copy Link provides a URL to access these files.

Settings										
Q Search		UPLOAD HISTORY								
License Configuration	^									
License Expiration Notification		LICENSE KEY	0	FILE NAME	SIZE	0	UPLOAD DATE	0	UPLOAD LINK	(
iveNA Configuration										
lounted Data										
odes		IskaAw43WfKAmYpXWUSpoP		2021-09-10_2218_logs.zip	67.46 MB		10 Sep 2021, 06:21PM		Copy Link	
		IskaAw43WfKAmYpXWUSpoP		2021-06-25_0810_logs.zip	36.69 MB		25 Jun 2021, 05:20AM		Copy Link	
roperties	~	IskaAw43WfKAmYpXWUSpoP		2021-05-05_2126_logs.zip	56.62 MB		08 Jun 2021, 01:00PM		Copy Link	
roxy		lskaAw43WfKAmYpXWUSpoP		2021-04-29_1522_logs.zip	48.55 MB		29 Apr 2021, 11:23AM		Copy Link	
eports	~	lskaAw43WfKAmYpXWUSpoP		2021-02-11_0913_logs.zip	59.32 MB		11 Feb 2021, 04:14AM		Copy Link	
ecurity	~	lskaAw43WfKAmYpXWUSpoP		2021-01-22_0113_logs.zip	50.24 MB		21 Jan 2021, 08:15PM		Copy Link	
ingle Sign On		lskaAw43WfKAmYpXWUSpoP		2020-12-08_1637_logs.zip	51.96 MB		08 Dec 2020, 11:38AM		Copy Link	
		lskaAw43WfKAmYpXWUSpoP		1602179643230_10.100.51.8_2055_eth0_60	202.00 B		08 Oct 2020, 01:55PM		Copy Link	
NMP Trap		All rows / 8								
yslog										
roubleshooting	^									
CPU Profiling										
Heap Dump										
Logs										
Packet Capture										
Upload History										
User Activity Tracking										

# **System Diagnostics**

*System Diagnostics* will present the LiveNX Server's and any associated Node collector's health. It also provides visibility into System, Node, and device Flow rates.



System	Diagnostics

Nodes									Flow Data Status									
	LOCAL/SERVER     Status: Ok Conformance: Ok Current Deployment: Small IP: Local									Last Update Time: 10/28/2021 7:31:00								
CPU Model	Intel(R) Xeon(R) CPU E5-2660 v4 @ 2.00GHz	OS Util.	2.1 %	OS RAM	31.40 GB	JVM RAM	16.00 GB	DISK Total	249.88 GB	RTT Server to Node	N/A	DEVICES Total	35	Configurable	0	Loading	0	
Cores	32	JVM Util.	0.2 %	Used	17.01 GB	Used	3.23 GB	Free	167.23 GB	Node to Server	N/A	Active	19	Down	16	Last Days Flow Rate	610.16 fps	

From the Nodes tab, by clicking on the summary bar, you can drill-down to more details.

System Dia	gnostics																
			Nodes									Flow Data S	tatus				
E LOCA	L/SERVER	st	atus: Ok Cor	formance: Ok	Current	Deployment: Small	IP: Local								Last Upda	ate Time: 10/28/	'2021 7:31:00 AM
CPU				OS RAM		JVM RAM		DISK		RTT		DEVICES					
Model	Intel(R) Xeon(R) CPU E5-2660 v4 @ 2.00GHz	OS Util.	2.1 %	Amount	31.40 GB	Committed	16.00 GB	Total	249.88 GB	Server to Node	N/A	Total	35	Configurable	0	Loading	0
Cores	32	JVM Util.	0.2 %	Used	17.01 GB	Used	3.23 GB	Free	167.23 GB	Node to Server	N/A	Active	19	Down	16	Last Days Flow Rate	610.16 fps

When drilling-down into a specific Server/Node appliance, more details are available on three tabs:

- System
- Data Store

#### • Report Queue

The System tab provides the recent history of the appliance's performance statistics.



The Data Store tabs breaks down the last 30 day's utilization of appliance's the disk usage.



The Report Queue will list any reports that are being processed or a waiting in queue for processing.

LOCA	AL/SERVER	51	nus: Ok Conform	ance: Ok	Current Deployment:	Small IP: Local											Last Update Tim	ie: 3/12/2021 7:51:
PU				OS RAM		JVM RAM		DISK			RTT		DEVICES					
odel	Intel(R) Xeon(R) CPU E5-2550 v4 @ 2.000Hz	OS Util.	1.3 %	Amount	31.40 GB	Committed	16.00 GB	Total	249.88 08		Server to Node	N/A	Total	27	Configurable	0	Loading	0
ores	32	JVM U6I.	0.6 %	Used	17.56 08	Used	5.87 08	Free	106.76 GB		Node to Server	N/A	Active	19	Down	8	Last Days Flow Rate	564.17 fps
	Svi	stem					De	ta Store							Report Qu			
port Q	Queues 😋																	
Cancel																		
Cancel																		
Cancel	Cancel All																	
Cancel	Cancel All	REPORT ID		¢	REPORT STATE		0 USER NAME		٥	QUEUE TYPE		0	QUEUED TIME			© RUNNING	3 TIME	
	Cancel All REPORT NAME O			0					0				QUEUED TIME			C RUNNING	) TIME	
	Cancel All	REPORT ID		0	REPORT STATE		0 USER NAME		¢	QUEUE TYPE		•	QUEUED TIME			C RUNNING	D TIME	
	Cancel All REPORT NAME O Report name				Al		• User name			All		×						
	6 Cancel AB REPORT NAME O Report name Voice Analysis	Report id 9c0c4e2a-ad85	41bc-9c12-cd6#8b	3d8960	All Running		Veername			All Priority 4		¥ ]	1 second			1 minut	e 3 seconds	
	Cancel All REPORT NAME O Report name	Report id 9c0c4e2a-ad85	41bc-9c12-cd6a8b 64e4f-950f-b85bf4	3d8960	Al		• User name			All		¥ ]					e 3 seconds	
	6 Cancel AB REPORT NAME O Report name Voice Analysis	Report Id 9c0c4e2a-ad85 19d66931-13co		3d89b0 7e65c8	All Running		Veername			All Priority 4		× .	1 second			1 minut	e 3 seconds indis	
	Cancel AB REFORT NAME O Fagor Frame Vice Ankylos MANA Fersite Applications	Report id 9c0c4e2a-ad85 19d66931-13cc aa646d47-ed36	i-4e4f-950f-b86bf4 i-4bc7-9dae-ee8c5f	3d8960 7e65c8 Y8c86e	All Running Running Running		<ul> <li>Username</li> <li>dødi</li> <li>dødi</li> <li>ggslå</li> </ul>			All Priority 4 Priority 4 Priority 4		· · · · · · · · · · · · · · · · · · ·	1 second 1 second 1 second			1 minut 44 seco	e 3 seconds indis	
	Cancel All     REPORT NAME     O     Report name      Vide Analysis     MAN	Report id 9c0c4e2a-ad85 19d66931-13cc aa646447-ed36 ba272813-da95	i-4e4f-950f-b86bf4	3d89b0 7e65c8 Y8c86e I418ec7	All Running Running		V Username SSQ2- 4545			All Priority 4 Priority 4		×	1 second			1 minut 44 seco 33 seco	e 3 seconds indis	

To cancel a report from running, select the report and click Cancel.

#### To cancel all reports, click **Cancel All**.

D LOCA	L/SERVER	Statu	a: Ok Conform	ance: Ok	Current Deployment: Sm	all IP: Local											Last Update Time:	3/12/2021 7:51:00 AM
PU				OS RAM		JVM RAM		DISK			RTT		DEVICES					
todel	Intel(R) Xeon(R) CPU E5-2660 v4 @ 2.000Hz	os u <sub>til.</sub>	1.3 %	Amount	31.40 08	Committed	16.00 08	Total	249.88 08		Server to Node	N/A	Total	27	Configurable	0	Loading	0
lores	32	JVM Usl.	0.6%	Used	17.56 GB	Used	5.87 08	Free	106.76 08		Node to Server	N/A	Active	19	Down		Last Days Flow Rate	564.17 fps
	Sys	em.						Data Store							Report Queu			
leport (	lueues 😋																	
Cance	Cancel All							Selected: 1										
	REPORT NAME	REPORT ID		0	REPORT STATE		USER NAME		0	QUEUE TYPE		۰	QUEUED TIME			RUNNING	TIME	0
					All	v				All		v						
	Voice Analysis	9c0c4e2a-ad8f-41	1bc-9c12-cd6a8b	049960	Running		dim			Priority 4			<1 second			1 minute	3 seconds	
	IWAN	19d66931-13cd-4	e4f-950f-6866f47	le65c8	Running		0440			Priority 4			<1 second			44 secon	da	
	Favorite Applications	aa646d47-ed36-4	bc7-9dae-ee8c5f	f8c86e	Running		6470			Priority 4			<1 second			33 secon	də	
	WAN Capacity Planning	ba272813-da95-4	8b1-b13d-0f9683	418ac7	Queued		9500			Priority 4			20 seconds					
	Voice/Video Performance Vs. Network Performan	06307c33-b5bc-4	cc7-a4e7-120447	1600acf	Queued		49985			Priority 4			7 seconds					

## **Flow Data Status**

The *Flow Data Status* tab provides viability into system wide, per Node, and per device Flow rates. It also shows any Flow drops that may be occurring.

	Nodes						Flow Data			
VERFLOW STATUS			FLOW COUNTS							
Refresh Data			Refresh Data				Data for	last 5 minutes V	Perform a full query	for the count
rrent Overflow:		false	Totals							
is Ever Overflowed:		false	Overall: 0 flows 0 flows	ner eccend						
rrent Packet Rate:		246.2 pps	overall: 0 nows 0 nows	s per second						
tal Drop:		0%	NODE	0	DEVICE COUNT	0 F	LOW COUNT	0 FL	OW RATE (FPS)	c
irrent Drop:		0%								
			All	~						
ODE	TOTAL DROPS	۰	Local			35		0		(
Local/Server		0								
			Flow Count by Device							
									FLOW RATE (FPS)	
			DEVICE	NODE	0	IP ADDRESS	FLOW COUNT		FLOW RATE (FPS)	4
			DEVICE	♦ NODE	0	IP ADDRESS	FLOW COUNT		FLOW RATE (FPS)	

# **User Management**

*User Management* is where users are added to the system, authorization groups are managed, user sessions can be reviewed, and external authentication integration can be configured.


User accounts can be authenticated locally or LiveNX can integrate with external user repositories for user authentication. Today, LiveNX supports the following external authentication methods:

- LDAP
- RADIUS
- TACACS+
- SSO

Please review this chapter for configuring LiveNX to these external repositories.

All user account authorization is done in LiveNX via Groups.

The User Management tab is where users are added to the system and managed.

0							
User Management							
User Management	Add	Edit Delete				Q Search	
Group Management							
Sessions		USER NAME	DISPLAY NAME	DIRECTORY	GROUP	STATUS 🗘	SESSION TIMEOUT
LDAP Management							
WMIC Management		admin	admin	Local	Admin	Enabled	1 Day
TACACS+ Authentication							
RADIUS Authentication							
	All rows	/ 103					

### To add a new user, click Add.

User Management	Add	Edit Delete					Q Search		
Group Management	1								
Sessions		USER NAME	DISPLAY NAME	DIRECTORY	GROUP	STATUS	0	SESSION TIMEOUT	0
DAP Management									
WMIC Management		admin	admin	Local	Admin	Enabled		1 Day	
FACACS+ Authentication									
ADIUS Authentication									

The Add New User modal appears.

1	Authentication Type	2 Settings
	Authentication Type	
	Select Authentication Type	

Select the Authentication Type and click Next Step.

- 1		
	Authentication Type	2 Settings
	Authentication Type	
	Select Authentication Type	
	LOCAL	
	LDAP	
	RADIUS	Cancel Next Step
	TACACS+	
	SSO	
ADD NEW US	Authentication Type	2 Settings
ADD NEW US		2 Settings

Define the user:

- Username
- Display Name
- Group
- Session Timeout
- Choose a password
- Repeat Password

Authentication Type			Settings
Addientication type		4	Settings
Username *		Display Name *	
Add username		Display Name	
Group *		Session Timeout *	
View		15 Minutes	
Choose Password *		Repeat Password *	
Add password	۲		۲

When finished, click **Add User**.

Authentication Type		2 Se	tings
Username *		Display Name *	
Alex		Alex2	
Group *		Session Timeout *	
View		15 Minutes	
Choose Password *		Repeat Password *	
	۲	••••••	۲

The new user will now be listed on the User Management tab.

User Management									
User Management	Add	Edit Delete					Q Search		
Group Management									
Sessions		USER NAME	DISPLAY NAME	DIRECTORY	GROUP	🗘 STATUS	0	SESSION TIMEOUT	0
LDAP Management									
WMIC Management		admin	admin	Local	Admin	Enabled		1 Day	
TACACS+ Authentication		alex	alex2	Local	View	Enabled		15 Minutes	
RADIUS Authentication									

To edit the user, select the user and click Edit.

User Management							
User Management	Add	Edit Delete		Selected:	1	Q Search	
Group Management							
Sessions			DISPLAY NAME 0	DIRECTORY	GROUP 0	STATUS O	SESSION TIMEOUT 0
LDAP Management							
WMIC Management		admin	admin	Local	Admin	Enabled	1 Day
TACACS+ Authentication		alex	alex2	Local	View	Enabled	Never
RADIUS Authentication							

Username		Display Name	
		alex2	
Group		Status	
View	~	Enabled	
Directory		Session timeout	
Local		Never	~
Choose Password *		Repeat Password *	
Add password	۲	Confirm password	۲

All user account authorization is done in LiveNX via Groups. The *Group Management* tab is where Groups are added and managed.

User Management						
User_Management	GR	UP MANAGEMENT				
Sessions	A	1 Delete			Q Search	
WMIC Management		NAME	٥	ROLE		0
TACACS+ Authentication				All		~
RADIUS Authentication		Admin	0	Admin		-
				Config		
		View	0	View		_

Authentication Groups have four components:

- **Role** Defines the authorized capabilities of the group members, i.e., monitor only vs. config changes
- **Device Authorization** defines which devices are visible for monitoring by group members
- **Page Access** defines which pages are available in the Operations Dashboard (WebUI) for group members
- **Users** which LiveNX users are a member of the group

#### Role

The group's Role defines the authorized capabilities for the members of the group.

There are three Roles available: *Admin, Config*, and *View*. There capabilities will be summarized in the table below:

New Role	Description	Device Access	Capabilities
Admin	Can perform any action for all resources. Is capable of making changes to the system that impact other users	All devices	All capabilities
Config	Can perform any action for its selected resources. Is capable of making changes to the system that impact other users but at more lim- ited level than admin. An example is that a "con- fig" user will not be able to access "Settings"	Only devices for which a user has been given permission to access (All Devices by Default)	<ul> <li>In the Operations Dashboard: Config can optionally manage Devices, Custom Applications, Fil- ters, Site</li> <li>In the Engineering Console: Con- fig can optionally control CLI GUIs (ie. Manage QoS, IP SLA, ACLs, PBR, etc.)</li> </ul>
View	Can primarily only monitor data for its selected resources. Is unable to make changes that impact other users.	Only devices for which a user has been given permission to access (All Devices by Default)	Monitor Only

#### **Device Authorization**

Device Authorization defines which device's SNMP and NetFlow metrics are visible by group members.

By default, all devices are available for all roles. Restricting visibility to selected devices can be accomplished by filtering devices, sites, or regions.

#### Page Access

- Operations Dashboard (WebUI) page access can be limited per role
- Most pages are accessible by all Roles.
- Some pages are accessible to only Admins.
- Some pages are accessible to Admins and Config.

The table below shows the pages only available to Admin and Config roles:

Section	Page	Required Page Access	Required Role
Configure	Alert Managment	-	config/admin
Configure	Application Management	Application Management	config/admin
Configure	OID Polling	OID Polling	config/admin
Configure	Device Management	Device Management	config/admin
Configure	Filter Management	Filter Management	config/admin
Configure	Site Management	Site Management	config/admin
Gear Icon	Settings	-	admin
Gear Icon	User Management	-	admin
Gear Icon	LiveNX Server	-	admin

### Users

Defines which LiveNX users are a member of the group.

## Adding a New Group

By default, there are three Groups: *Admin, Config,* and *View*. Each is assigned the role that corresponds to the Group's name. These default roles have no device or page restrictions and cannot deleted. Additional roles can be added and customized to meet a specific Group's needs.

GI	ROL	OUP MANAGEMENT								
	Add	Delete			Q Search					
		NAME	0	ROLE		0				
				All		~				
		Admin	0	Admin						
		View	0	View						
		Add	Internet     Atria     Confg	Ad Deste	Add         Destr           NAME         0         NO.E           International Adminition         0         Adminition           Config         0         Config         0	Add         Denter         Qfareth           NAME         0         mit.           Information         Admin         0           Admin         0         Admin           Cordg         0         Cordg				

### 1. To add a new Group, click Add.

User Management						
User Management						
Group Management	GROU	JP MANAGEMENT				
Sessions	1					
LDAP Management	Add				Q Search	
WMIC Management		NAME	0	ROLE		0
TACACS+ Authentication				All		~
RADIUS Authentication		Admin	0	Admin		
		Config		Config		
		View	0	View		

### 2. Provide a Name and Role.

User Management User Management Group Management ADD GROUP	
User Management ADD GROUP	
Sessions Applications  O General Settings  Device Authorization  Page Access  O Report Access  O	Users
Lurr malageneta	
WM/CManagement TACACS+ Authentication Role * Role *	
PADII/S Authentication Mem	^
Admin	
Comp View View	
	-
Cancel Next S	tep

**3.** Assign device authorization.

A group may:

- View and configure all devices (Config role only)
- View with CLI access all devices (View role only)
- Only view all devices

• Use a specific filter

By default, a *Config* role group is authorized to view and configure all devices and a View role group is authorized to view with CLI access all devices.

*Config* and *View* role groups can further restrict authorized devices by applying a Filter(s). To restrict authorization to a specific device(s), tick Use specific filers, click **Add**.

≡ LiveAction <sup>~</sup>	X LivenCA New Featurest ▲ 280 ■ 11 • 25 ▲ 145402 {-} * ③ *	<b>a</b>
User Management		
User Management		
Group Management	ADD GROUP	
Sessions	General Settings 2 Device Authorization 3 Page Access 2 Report Access 3	Users
LDAP Management		03013
WMIC Management	Group is authorized to: 🕐 View with CLI access all devices 🕜 Only view all devices 🔹 Use specific filters	
TACACS+ Authentication	Add Edit Delete	
RADIUS Authentication	Autor Can Deeve	
	ENTRY TYPE VALUES CLI ACCESS	
	Citity Type Control Co	~
	Specific Filter Options Table No Filters: All devices are hidden	
	Rows: -	
	Cancel Previous Step Next	Step

Filters can be applied by Device, Site, or Region.

Config roles can optionally have CLI access for managing QOS, IPSLA, etc. in the Engineering Console.

ADD DEVICE AUTHORIZA	ATION	×
Site: Austin		
CLI Access for managing QO	DS, IPSLA, etc in the Engineering Console.	Cancel Add

In the following example, the devices matching the filters would be authorized for monitoring by this Group:

- Site=Austin
- Device=LondonEdge
- Region=Florida

≡ LiveAction <sup>-</sup>	NX LiveNCA New Featurest A 285	5 📕 11 🔹 20 🜲 145667 🛛 {} 👻 🔞 👻	<b>♦</b> - <b>≛</b> : : :
User Management 🙆			
User Management			
Group Management	ADD GROUP		
Sessions	General Settings     2 Device Authorization     3 Page Access	Report Access	5 Users
LDAP Management	General Settings Using Levice Authonization	Report Access	Users
WMIC Management	Annu hashadada 🔿 Manadadada a 🖉 Abada 🖉 dalar 🖉 Abada da dalar		
TACACS+ Authentication	Group is authorized to: View and configure all devices Only view all devices O Use specific filters		
RADIUS Authentication	Add Edit Delete	Q Search	
	ENTITY TYPE VALUES		CLI ACCESS
			All v
	Site Austin		~
	Device LondonEdge		~
	Region Florida, United States, North America		~
	Rows: 3 / 3		
	Canoel	Previous Step	Next Step

**4.** Assign Operations Dashboard (WebUI) page access.

≡ LiveAction <sup>-</sup>	NX LiveNCA							New Features!	<b>A</b> 285	<mark>=</mark> 11	• 20	45667	{-} -	0 -	۰.	. <b>≜</b> o ⊲.≁
User Management																
User Management																
Group Management	AD	DD GROUP														
Sessions																
LDAP Management	<b>~</b>	General Settin	-gs		ev Dev	vice Authorization		3 Page Access			- 0	Report Access				5 Users
WMIC Management																
TACACS+ Authentication	S	Select All	Unselect All						Q Sear							
RADIUS Authentication		Dashboard														^
		Entity Pages (Si	tes/Devices/Interf	faces/Application	ons)											
		Network Users														
		Topology														
		Report Manager	nent													
		Alert View														
		Device Inventor	/ Story													
		Flow Path Analy	sis Story													
		Sd Access Story	1													
		IPSLA Story														
		Security Flow A	alysis Story													
		Site To Site Ana	lysis Story													
		Calls By Numbe	r Story													$\checkmark$
	•	Cancel												Previous Step	Ne	ext Step

In this example, only Dashboards and Entity Pages (*Sites/Devices/Interfaces/WAN Applications*) will be available for this Group.

≡	LiveAction	NX LivenCA New Features: * 285 = 11 • 20 🗍 145731 (-) - 6	0 <b>· ↓ </b> ≛ •
User I	Management 🙆		
User M	fanagement		
Group	Management	ADD GROUP	
Sessio	กร	Centeral Settings Device Authorization 😑 Live Archiom Page Access	5 Users
LDAP	Management		Users
WMIC	Management	eff Main	
TACAG	S+ Authentication	Select All Unselect All Overlear Q, Search	
RADIU	S Authentication	☑ Dashboard Som	^
		Entity Pages (Sites/Devices/Interfaces/Applications)     Sources	
		Network Uses      Watches      Watches	
		Depology WAA Applications	
		Report Management	
		Alert View	
		Device Inventory Story	
		Flow Path Analysis Story	
		Sd Access Story	
		□ IPSLA Story	
		Security Flow Analysis Story	
		Site To Site Analysis Story	
		Calls By Number Story	$\sim$
		Cancel	ious Step Next Step

Do note that even though the Navbar may be restricted, some drill-down workflows will still allow limited functionality to pages not directly available from the Navbar. Using the previous example, where Dashboards were one of the limited options made available, these pages allow drill-down to reports, but the reports are limited to just the results.

i≡	LiveAction
î	Main
	Overview

5. Select which reports are available to the group. By default, all reports are available.

≡	LiveAction <sup>-</sup>	NX Live	ICA			🔺 280 💻 11 🔹 24 🌲 146437	{-}▼ @▼ ≗▼
User N	fanagement						
User M	anagement						
Group I	Management		EDIT GROUP MYGROUP				
Session	15		General Settings	Device Authorization	Page Access	Report Access	5 Users
LDAP N	fanagement		General Setungs	Device Authorization	Page Access	Report Access	o Users
	Management						
	S+ Authentication		Select All Unselect All			Q Search	
RADIUS	Authentication		Test				×
			LiveNA				× _
			Flow				~
			SNMP				~
			Cisco SD-WAN				×
			Alert				Ť
			Cancel				Previous Step Next Step

Optionally, deselect any report that should not be available to the group.



EDIT GROUP MYGROUP				
General Settings	Device Authorization	Page Access	Report Access	5 Users
Select All Unselect All		Q Search		
				^
V IPSLA				~
Z LAN				~
QoS				~
NBAR and Post-Policy				
Post-Policy Drops				
Pre-Policy and Post-Policy				
Pre-Policy and Post-Policy Drops				
Top Class Bandwidths				
Top Class Drops				
Top Layer 2 QoS Queue Drops				
Status				~
System				×
				~
Cancel			Prev	vious Step Next Step

### 6. Add user(s) to group by clicking Add.

$\equiv$ LiveAction <sup>-</sup>	NX LiveN	CA				<b>▲</b> 285 <b>■</b> 11	1 • 20	145789	Ø - •	•• ≜
User Management										
User Management										
Group Management		ADD GROUP								
Sessions		General Settings	Device Authorizat	100	Page Access			Report Access		5 Users
LDAP Management		General Settings	Device Authorizat	ion	Page Access		Ľ	Report Access		o Users
WMIC Management		(								
TACACS+ Authentication		Add						Q Search		
RADIUS Authentication		USER NAME	٥	DISPLAY NAME		© DI	RECTORY			0
		User Name								
		Rows – Cancel			No Data				Previous Ste	p Save

#### Select the users of interest and click Add.

Jser Management											
Broup Management	ADD GROUP	ADD	USER TO GROUP				×				
Sessions	ADD GROUP										
	General Settings	Select	ed users will be assigned to t	he new group	Q Search				Report Access		👩 User
DAP Management	Contra contra se										•
WMIC Management			USER NAME	DISPLAY NAME	DIRECTORY	GROUP					
ACACS+ Authentication	Add			Display Name					Q Search		
ADIUS Authentication	USER NAME		full-config	full-config	Local	full-config	^	TORY			
			tma	tma	Local	Admin					
	User Name		mhampson-clerk	mhampson-clerk	Local	Admin		rectory			
			charles	Charles	Local	MyGroup					
			acameron	acameron	Local	Admin					
			dhaivat	dhaivat	Local	Admin					
			ssidheeq	ssidheeq	Local	Admin					
			inna_demo1	inna demo 1	Local	Admin					
			gbsfo	gbsfo	Local	Admin					
			inna_demo2	inna demo 2	Local	Admin					
			dkimura	dkimura	Local	Admin	$\sim$				
		Row	s: 102 / 102								
						Cancel	Add				
	Rows: -										

In this example, users *Charles* and *Bill* will be a member of this group.

≡ LiveAction <sup>-</sup>	NX LiveNCA				New Features! 4 286	s =	11 •	21	145861	{} -	<b>8</b> -	۰.	<b>.</b> -	
User Management														
User Management														
Group Management		ADD GROUP												
Sessions			•											
LDAP Management		General Settings	Device Authoriza	ation	Page Access			- <b>(</b>	Report Access			-	5 Use	75
WMIC Management														
TACACS+ Authentication		Add							Q Search					
RADIUS Authentication		USER NAME	\$	DISPLAY NAME		0	DIRECTOR	Y					0	
		charles		Charles			Local							
		bill		bill			Local							
		Rows: 2 / 2												
		Cancel									Previou	s Step	Save	

The new Group is now listed on the *Group Management* page.

GRO	UP MANAGEMENT				
Add	1 Delete			Q Search	
	NAME	¢	ROLE		0
	Name		All		~
			Admin		
			Config		
	View C Start		View View		
	in yoroop		¥ 1514		

### Sessions

The *Sessions* tab lists users that are currently and historically logged into LiveNX. Active users can be logged out by selecting the user and clicking **Logout Users**.

Biological Constraints         Logist Uters         Constraints         Constraint												
	er Management											
PAdaganet Adden and Adden and Adden	oup Management	Logout	t Users							Q S		
// Management       Chasagement       Chasagement       Chasagement       Chasagement       Corport for the form       Corport form       Corport for the form       Corport for th	ssions											
Adds Authentication       Is 192173       adm       Athe       We       Adm       4 is       Thu Jul 08 2021 09.45.       •         NSS Autoentication       Is 192173       adm       Athe       We       Adm       4 is       Image: State of the state of th	AP Management		CONNECTION ID	USER NAME	STATUS O	TYPE O	ROLE	LODGED-ON DURATION 0	IDLE DURATION (MINS)	LAST MASTER TOPOLO O	LAST LOGIN TIME	CLIENT TO SERVER RTT
WS Authentication	IIC Management											
	CACS+ Authentication		10.4.192.175	admin	Active	Web	Admin	45	4		Thu Jul 08 2021 06:45	
	NUS Authentication											
2000 1												
Mana 1												
Anna 1												
Now 1												
20mm ] 1												
Read 1												
20mm ] 1												
Read 1												
Mana 1												
Arman 1												
Mone 1												
Arman 1												
Arman 1												
Arma 1												
Alone 1												
Afree 1												
Afrees 1												
Altern 1												
Amm 1												
All rows 1												

### LDAP Management

The *LDAP Management* tab allows for the configuration of one or more LDAP server(s) with which LiveNX can use for authentication users. To add an LDAP server, click **Add**.



The Add LDAP Server Modal appears. From the Main Settings tab, configure the following:

- Name
- LDAP Server Address/Hostname
- LDAP Server Port
- Identity
- Password
- Search Base
- Auto Add/Update Users
- Groupz

Main Settings	Advanced Setting	
Name *	Search Base *	
LiveAction	DC=liveaction, DC=com	
LDAP Server Address/Hostname *	Auto Add/Update Users Group	
10.0.0.10	View	~
LDAP Server Port SSL/TLS 636	+ Add Additional Search Base	
Identity *		
CN=users,DC=liveaction,DC=cpm		
Password *		
•••••		
•••••		

If necessary, click + Add Additional Search Base.

Main Settings	Advanced Setting
Name *	Search Base *
LiveAction	DC=liveaction, DC=com
LDAP Server Address/Hostname *	Auto Add/Update Users Group
10.0.0.10	View
LDAP Server Port SSL/TLS	Search Base *
636	DC=admin,DC=liveaction,DC=com
Identity *	Auto Add/Update Users Group
CN=users,DC=liveaction,DC=cpm	Admin ~
Password *	+ Add Additional Search Base
****	

From the *Advanced Settings* tab, if necessary, additional parameters can be modified:

- Username
- Display Name
- User Search String
- Group Search String

When finished, click **Update**.

Main Settings	Advanced Setting
Username *	User Search String *
sAMAccountName	(&(objectCategory=Person)(objectClass=User))
Display name *	Group Search String *
displayName	(&(objectCategory=Group)(objectClass=Group))

The LDAP Server will be listed.

r Management		
Management		
p Management	LDAP GENERAL SETTINGS	
ions	LDAP GENERAL SETTINGS	
P Management	LDAP Poller: Enabled Poll Interval (Days): 1 Poll Time: 12:00 AM Time Zone: (GI	MT) Europe/Isle of Man DST: Enabled
C Management	Configure Polling	
ACS+ Authentication		
IUS Authentication	LDAP SERVER	
	Add Edit Delate Retrest O Addee	
	UveAction Idap:	//10.0.0.10

To edit an LDAP server's settings, select the server and click **Edit**.

User Management	
User Management	
Group Management	LDAP GENERAL SETTINGS
Sessions	LDAP GENERAL SETTINGS
LDAP Management	LDAP Poller: Enabled Poll Interval (Days): 1 Poll Time: 12:00 AM Time Zone: (GMT) Europe/Isle of Man DST: Enabled
WMIC Management	Configure Polling
TACACS+ Authentication	
RADIUS Authentication	LDAP SERVER
	Add Edit Delete Refresh Selected 1 Q Search
	Manifer - Manifer Andrey, Die dans Mitte (Mercente - Mercente

To manage LDAP polling auto-updates, click **Configure Polling**.

0		
User Management		
User Management		
Group Management	LDAP GENERAL SETTINGS	
Sessions		
LDAP Management	LDAP Poller: Enabled Poll Interval (Days): 1 Poll Time: 12:00 AM Time Zone: (GMT) Europe/Isle of Man DST: Enabled	
WMIC Management	Configure Polling	
TACACS+ Authentication	·	
RADIUS Authentication	LDAP SERVER	
	Add Edit Dehe Refresh Select LDAP SETTINGS  NAME  NAME  LDAP SetTINGS  LDAP poller  Disable  Poll Interval (Days)  1  Poll Time  2 00 AM  2 0	×
	Time Zone (GMT-08:00) US/Pacific	DST
	Cancel Save	

## **WMIC Management**

*WMIC Management* allows LiveNX to integrate with AD servers for parsing user login/logout events which contain the source IP information. This provides LiveNX the ability to populate username in NetFlow reports.

lanagement 🤷		
anagement		
Aanagement	WMIC SERVER	
IS		
nagement	WMIC Poller: Enabled Poll Interval (Minutes): 1	
nagement	Configure Polling	
Authentication		
umentication	WMIC SERVER	
	Add Edit Delete	Q Search
	NAME O DOMAIN	ADMIN USER     O     HOST     O

To enable the WMIC poller and set the polling interval, click **Configure Polling**.

Jser Management 💿					
Jser Management					
Sroup Management	WMI	C SERVER			
Sessions		OULIVER			
DAP Management	WMIC	Poller: Enabled Poll Interval (Min	tes): 1		
WMIC Management	Con	nfigure Polling			
FACACS+ Authentication	L				
RADIUS Authentication	WMI	C SERVER			
	Add	f Edit Delete		Q Search	
		NAME	DOMAIN Ô	ADMIN USER	0 HOST
		Name			

After making changes, click Save.

WMIC Polle	er	
Enable	Disable	
Nell Indemin		
Poll Interva	ii (Minutes)	

To add an WMIC server, click Add.

Jser Management 💿
er Management
roup Management
Sessions
AP Management
MIC Management
ACACS+ Authentication
RADIUS Authentication

Enter the configuration details and when finished, click Save.

Name			
My Domain Cont	roller		
Domain			
LiveAction			
Admin User			
WMIC User			
Password			
Host			
172.1.1.1			

The server appears on the WMIC General Settings page.

WMIC	SERVER			
Add	Edit Delete		Q Search	
	NAME	DOMAIN C	ADMIN USER	HOST
	Name			Host
	SEDemo-LDAP	demo.com	administrator	192.168.100.201

To Edit the server's settings, select the server and click **Edit**.

	ure Polling	al (Minut	es): 1						
WMIC	SERVER								
Add	Edit Delete			Selected: 1		Q Search			
	NAME	0	DOMAIN	0	ADMIN	N USER	0	HOST	0
	Name							Host	
	SEDemo-LDAP		EDIT Name SEDerno-LDAP Domain demo.com Admin User administrator				×	2.168.100.201	
			Password Host 192.168.100.201	Cancel	Sar	we			

## **TACACS+** Authentication

The *TACACS*+ *Authentication* tab allows for the configuration of a Primary and Secondary TACACS+ server with which LiveNX can use for authentication users.

ient				
ment	GENERAL SETTINGS			
	Server Timeout Re 5 sec 3	try Count		
tion				
!	SERVERS CONFIGURATI	ION		
	Primary Server IP/Hostname	Server Port	Shared Secret	
	172.16.21.1	49	••••	Clear
	Secondary Server IP/Hostname	Server Port	Shared Secret	
		49		Clear

Click **Test Connection** to validate the Servers' IP connectivity and Shared Secret.

Jsername *	Password *	
Type Username	Type Password	۲
	Cancel	

The *RADIUS Authentication* tab allows for the configuration of a Primary and Secondary RADIUS server with which LiveNX can use for authentication users.

er Management	GENERAL SETTINGS				
sions AP Management	Server Timeout Retry	Count			
Management CS+ Authentication JS Authentication	SERVERS CONFIGURATION	4			
	Primary Server IP/Hostname	Server Port	Shared Secret		
		1812		۲	Clear
	Secondary Server IP/Hostname	Server Port	Shared Secret		
		1812		۲	Clear
			Test Connection Revert	Changes	Apply

Click **Test Connection** to validate the Servers' IP connectivity and Shared Secret.

Type Username Type Password	۲

# **LiveNX Server**

The *LiveNX Server* setting defines the IP address that LiveNX expects to utilize for running the Operations Dashboard (WebUI). If the WebUI needs to run from an alternate IP address, click **Log Out And Change**.



LIVENX SERVER	RSETTINGS	×
Your current LiveN		
Before changing the to be logged out.	he LiveNX Server configuration you will need	

Update the *IP Address* and *Port* and click **Save**.

Liv	/e <mark>NX</mark>
LiveN3	Server Settings
IP Address or Hostname	
Port	
8093	
Cancel	Save

# CHAPTER 4

# **LiveNX Appliance**

# In this chapter:

About LiveNX Appliance	126
What's Included	126
Front / Rear Panels	127
Inside LiveNX Appliance	128
Installing LiveNX Appliance	129
Connecting Extended Storage to LiveNX Appliance	130
Starting / Shutting Down LiveNX Appliance	131
Contacting LiveAction Support	131

# **About LiveNX Appliance**

If you purchased LiveAction LiveNX appliance, this chapter describes the LiveNX appliance in further details. LiveNX appliance and LiveNX is a network and application performance monitoring platform with patented end-to-end visualization for a global view of the network and the ability to drill-down to individual devices. Using LiveNX, enterprises gain real- time and historic insight into network traffic based on application and user level activity. LiveNX offers the ability to gather and analyze volumes of network data at scale from network device, applications, and user to reduce mean time to repair, and it performs exploratory and explanatory analysis of network performance.

LiveNX appliance is available in the following configuration:

	LiveNX appliance
Chassis	10
Processor	2 x Intel <sup>®</sup> Xeon <sup>®</sup> Gold 5218
Base Frequency Max Turbo Frequency Cores Thread	2.30 GHz 16 32
Memory	768 GB
Expansion Slots	2 x 16 LP PCIe 3.0 slots
Integrated Network Interfaces	2 x 10GBASE-T 2 x 1GBASE-T iDRAC
Storage-OS	Included as part of Storage-Data
Storage-Data	4 x 8 TB NLSAS (32 TB, RAID 10)

# What's Included

Your standard LiveNX appliance package includes:

- LiveNX appliance
- LiveNX software pre-installed in LiveNX appliance
- Two power cords
- Rack-mount rails
- Chassis bezel

# Front / Rear Panels

See the illustrations and descriptions of the front and back panel of LiveNX appliance in the sections below.

## LiveNX Appliance Front Panel



ltem	Indicator, Button, or Connector	Description
1	Left control panel	Contains system health and system ID, status LED, and optional iDRAC Quick Sync 2 (wireless) LED.
2	Drive slots (4)	Contains 3.5 inch hot-swappable hard drives/SSDs.
3	Optical drive	One optional slim SATA DVD-ROM drive or DVD+/-RW drive.
4	VGA port	Enables you to connect a display device to the system.
5	Right control panel	Contains the power button, USB port (USB 3.0 compliant), iDRAC Direct micro USB port, and the iDRAC Direct status LED.
6	Information tag	The Information Tag is a slide-out label panel that contains system information such as service tag, NIC, MAC address, and so on.

**Note** To access the front panel, the front bezel must be removed.

# LiveNX Appliance Rear Panel



ltem	Indicator, Button, or Connector	Description
1	Full height riser slot	Use the card slots to connect full-height PCIe expansion cards on full height riser.
2	Power supply unit (2)	AC 550 W. Both power supplies should be plugged in to power to provide redundancy.
3	Ethernet ports (4) (The port labeled 'Gb 1' is the eth0 management port)	Use the Ethernet ports to connect Local Area Networks (LANs) to the system.
4	USB 3.0 port (2)	Use the USB 3.0 port to connect USB devices to the system. These ports are 9-pin, USB 3.0-compliant.

Item	Indicator, Button, or Connector	Description
5	VGA port	Use the VGA port to connect a display to the system.
6	Serial port	Allows you to connect a serial device to the system.
8	CMA power port	The Cable Management Arm (CMA) power port enables you to connect to the CMA.
9	System identification button	The System Identification (ID) button is available on the front and back of the systems. Press the button to iden- tify a system in a rack by turning on the system ID button. You can also use the system ID button to reset iDRAC and to access BIOS using the step through mode.

# **Inside LiveNX Appliance**

**CAUTION!** Many repairs may only be done by a certified service technician. You should only perform troubleshooting and simple repairs as directed by the LiveAction support team. Damage due to servicing that is not authorized by LiveAction is not covered by your warranty. Read and follow the safety instructions that are shipped with your product.

### LiveNX Appliance Internal Components



**Note** The graphic above shows a configuration of ten internal drives installed in the front drive cage of the appliance; however, only a four drive configuration installed in the front drive cage is available with LiveNX appliance.

ltem	Description
1	Left control panel cable cover
2	Hard drive backplane
3	Backplane expander board
4	Cabling latch
5	Air shroud
6	Intrusion switch
7	Power interposer board
8	Internal expansion riser
9	Low profile expansion riser 1
10	Low profile expansion riser 2
11	Processor blank
12	Heat sink
13	Air shroud
14	Cooling fan blank
15	Left control panel cable cover
16	Information tag

**Note** A defective drive should have a consistent RED blinking LED which should make it easier to detect.

# Installing LiveNX Appliance



LiveNX Appliance

### To install LiveNX appliance:

- 1. Place LiveNX appliance on a flat surface, or mount it in a standard 19-inch equipment rack.
- 2. Connect a power cable to each of the two power outlets at back of the unit.

**Note** LiveNX appliance has two redundant high-efficiency "hot-swappable" power supplies. If a power module fails, it should be replaced immediately. If your LiveNX appliance is under warranty, please contact Technical Support to arrange for a replacement power supply.

3. Plug the other end of the power cables to an AC outlet.

**Important!** WARNING: This device has more than one power cord. Disconnect **ALL** power supply cords before servicing.

AVERTISSEMENT: Cet appareil a plus d'une cordon d'alimentation. Débranchez TOUTES les cordons d'alimentation avant l'entretien.

### **Connecting Network Cables**

LiveNX appliance includes Gigabit Ethernet ports and Integrated Remote Access Controller (iDRAC) ports used for remotely accessing and troubleshooting LiveNX appliance. See *Front / Rear Panels* on page 127 for the location of these ports.

### To connect network cables:

- Use a standard Ethernet cable to connect these ports to your network.
  - **Tip** To reach LiveNX appliance through an SSH connection, you can use an Ethernet cable connected directly between the Gigabit Ethernet port on LiveNX appliance and your PC or laptop. LiveNX appliance eth0 port is configured at the factory with a default static IP address of 10.10.10.21. The PC or laptop must be configured to be on the same IP subnet.

### **System Fans**

LiveNX appliance has multiple cooling fans that are used to the cool the system chassis. If any one of the fans fail, it should be replaced immediately. If your LiveNX appliance is under warranty, please contact Live-Action Technical Support to arrange for a replacement fan.

Important!	The chassis top cover must be properly installed in order for the cooling air to circulate correctly through the chassis and cool the components.
important!	WARNING: Slide/rail mounted equipment is not to be used as a shelf or a work space.
	AVERTISSEMENT: Le matériel monté sur rails/coulisseaux ne doit pas être utilisé comme étagère ou espace de travail.

# **Connecting Extended Storage to LiveNX Appliance**

The storage capacity of LiveNX appliance can be increased through the addition of Extended Storage for LiveNX appliance. Extended Storage is available in a configuration of 96 TB. Up to four Extended Storage units can be added for a total of 208 TB (RAID10). If you purchased Extended Storage with LiveNX appliance, the instructions to connect it to LiveNX appliance are provided below.

### To connect Extended Storage to LiveNX appliance:

- 1. Make sure both Extended Storage and LiveNX appliance are powered OFF.
- 2. Select a suitable location for both Extended Storage and LiveNX appliance. Both units can be installed on a flat surface, or mounted in a standard 19-inch equipment rack.
- 3. Run the SAS external cascading cable between the units so that the cable is not kinked, bent, or twisted. The SAS external cascading cable is included with Extended Storage.
  - **Note** If you have multiple Extended Storage boxes, and the system is disconnected for any reason, the cabling of the boxes needs to be exactly as it was before, otherwise the RAID won't be seen correctly. To assist you with the cabling, every Extended Storage box is labeled with a number, and every Extended Storage cable is labeled to the exact port it needs to get plugged into.

- 4. Facing the rear of LiveNX appliance, insert one connector of the SAS external cascading cable into the left RAID port (RAID 1) of the RAID controller on LiveNX appliance so that the release handle is on the top. The connector is keyed and only fits in one way.
  - **Note** It may be necessary to remove the handle on the rear of the appliance in order to connect the SAS external cascading cable into the left RAID port of the RAID controller.
- 5. Facing the rear of Extended Storage, insert the other end of the SAS external cascading cable into the RAID 1 port of the RAID controller on Extended Storage so that the release handle is on the top. The connector is keyed and only fits in one way.



Extended

- **Note** Be certain the connectors are installed completely as it can look and feel as if the cable is secured without actually making a connection. Give the connector body a tug, then push it in again to be sure.
- 6. Turn on power to Extended Storage by pressing the power button on the front of the chassis. You may see brief bursts of LED activity as the expander in Extended Storage scans the drives.
- 7. Turn on the power to LiveNX appliance. The system is ready for use as soon as the LiveNX appliance boot sequence completes.

# Starting / Shutting Down LiveNX Appliance

### To start LiveNX appliance:

• Press the power button in the upper right corner on the front of the chassis.

### To shutdown LiveNX appliance:

• SSH, or use a console connection to LiveNX appliance and use the 'shutdown' command from the command prompt (*admin@livenx*):

shutdown -h now

# **Attaching the Front Bezel**

### To attach the front bezel:

• Attach the front bezel by inserting the locking hooks into the front chassis of LiveNX appliance. The bezel should be centered between the two black tabs on the left and right of the LiveNX appliance chassis.

# **Contacting LiveAction Support**

Please contact LiveAction support at *https://www.liveaction.com/contact-us* if you have any questions about the installation and use of LiveNX appliance.

An RMA (Return Material Authorization) number must be obtained from LiveAction before returning hardware. Please contact LiveAction technical support at <u>https://www.liveaction.com/support/technical-support/</u> for instructions.