

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	2
	Configuration & Setting Menus	3
Chapter 2	Configuration	4
	Alert Management	5
	Maintenance Mode	17
	Application Management	21
	Custom Applications	21
	Application Groups	26
	OID Polling	29
	Pre-Configured	29
	Custom	30
	Device Management	33
	SNMP Monitored Devices	33
	Non-SNMP Monitored Devices	46
	Filter Management	50
	Site Management	52
	Site Details	53
	Site Address	54
	Site Business Hours	55
Chapter 3	Settings	58
	Settings	59
	Data Source Management	59
	Data Store Management	59
	Disk Overview	59
	Nodes Data Store	59
	Web UI Data Store	60
	Device Entity Page Reports	60
	Email Configuration	62
	Integrations	63
	Cisco APIC-EM/DNA-C	63
	ServiceNow	67
	LiveNCA	69
	Cisco ISE	70
	Cisco SD-WAN	73
	Licensing	80
	LiveNA Configuration	83
	Mounted Data	89
	Nodes	89
	Properties	92
	Proxy	94
	Reports	94
	Security	97
	Single Sign On	98
	SNMP Trap	99
	Syslog	99
	Troubleshooting	100
	System Diagnostics	102

Flow Data Status	104
User Management.....	104
Adding a New Group	110
Sessions	115
LDAP Management.....	116
WMIC Management.....	119
TACACS+ Authentication	122
LiveNX Server.....	123
Chapter 4 LiveNX Appliance	125
About LiveNX Appliance.....	126
What's Included	126
Front / Rear Panels.....	127
LiveNX Appliance Front Panel.....	127
LiveNX Appliance Rear Panel.....	127
Inside LiveNX Appliance.....	128
LiveNX Appliance Internal Components	128
Installing LiveNX Appliance	129
Connecting Network Cables.....	130
System Fans.....	130
Connecting Extended Storage to LiveNX Appliance	130
Starting / Shutting Down LiveNX Appliance.....	131
Attaching the Front Bezel.....	131
Contacting LiveAction Support	131

Introduction

In this chapter:

<i>About this Admin Guide</i>	2
<i>Configuration & Setting Menus</i>	3

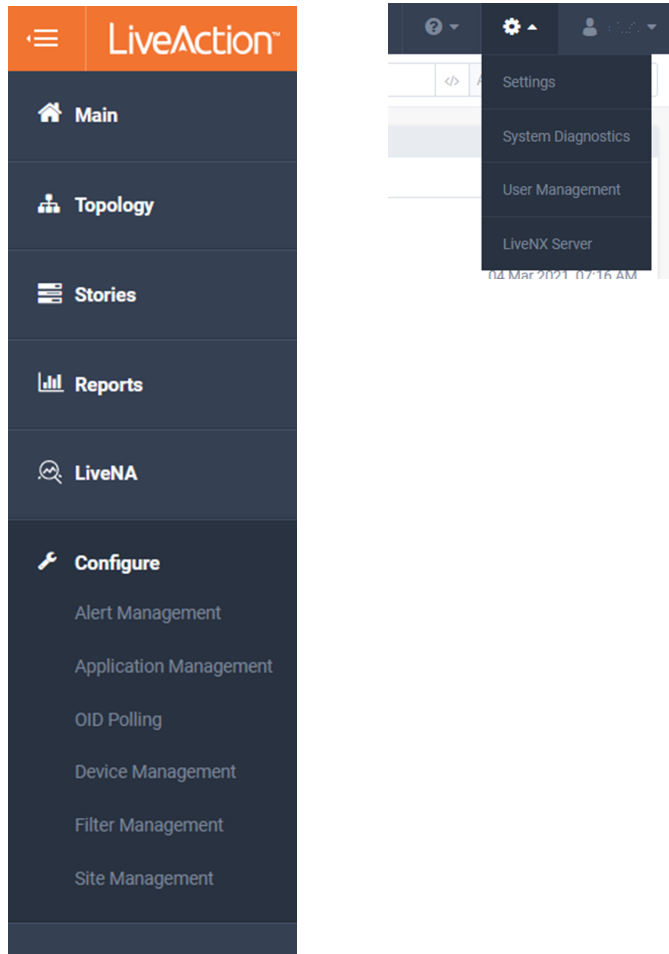
About this Admin Guide

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:



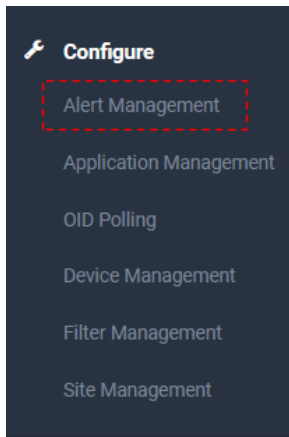
Configuration

In this chapter:

<i>Alert Management</i>	5
<i>Application Management</i>	21
<i>OID Polling</i>	29
<i>Device Management</i>	33
<i>Filter Management</i>	50
<i>Site Management</i>	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.



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

ALERT TYPE	CATEGORY	SEVERITY	ENABLED	THRESHOLDS	SHARING
Application Performance - App Delay	Application	Multiple	✓	Multiple	Web UI
Application Performance - Network Delay	Application	Multiple	✓	Multiple	ServiceNow, Web UI
BGP Peer Connection Change	Network	▲ Critical	✓	for at least = 0 minutes	Email, Web UI
Cisco IWAN Path Change	Network	▲ Critical	✓	for at least = 0 minutes	ServiceNow, Web UI
Cisco IWAN Threshold Crossing	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 - birmingham	Device, Interface	● Info	✓	Value >= 100 percent for at least = 0 minutes	Web UI
Device CPU Utilization	Device, Interface	Multiple	✓	Multiple	Web UI
Device Flow Stop	Device, Interface	▲ Critical	✓	for at least = 0 minutes	ServiceNow, Web UI
Device Memory Utilization	Device, Interface	Multiple	✓	Multiple	ServiceNow, Web UI
Device Reachability	Device, Interface	Multiple	✓	Multiple	ServiceNow, Web UI
Interface Errors (CRC, Frame, Overruns, Ignore, Abort)	Device, Interface	▲ Critical	✓	Number of Errors >= 40 Errors for at least > 0 minutes	ServiceNow, Web UI
Interface Reachability	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
LiveNX CPU Utilization	System	▲ Critical	✓	Local/Server >= 40 % for at least = 0 minutes	ServiceNow, Web UI
LiveNX Disk Utilization	System	▲ Critical	✓	Local/Server >= 60 % for at least = 0 minutes	ServiceNow, Web UI
LiveNX Memory Utilization	System	▲ Critical	✓	Local/Server >= 40 % for at least = 0 minutes	ServiceNow, Web UI
LiveNX Node Connectivity	System	▲ Critical	✓	for at least = 0 minutes	ServiceNow, Web UI
Media Jitter Max	Application	▲ Critical	✓	Jitter Max >= 10 ms for at least > 0 minutes	ServiceNow, Web UI
Media Jitter Min	Application	▲ Critical	✓	Jitter Min >= 10 ms for at least > 0 minutes	ServiceNow, Web UI
Media Packet Loss	Application	▲ Critical	✓	Packet Loss >= 1 % for at least > 0 minutes	ServiceNow, Web UI

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

Alert Management Maintenance Mode View Alerts

LiveNX Alerts

Enable Disable
Q Search...

ALERT TYPE	CATEGORY	SEVERITY	ENABLED	THRESHOLDS	SHARING
<input type="checkbox"/> Alert Type	All	All	All	Thresholds	Sharing
<input type="checkbox"/> Application Performance - App Delay	Application	Multiple	✓	Multiple	ServiceNow, Web UI
<input type="checkbox"/> Application Performance - Network Delay	Application	Multiple	✓	Multiple	ServiceNow, Web UI
<input checked="" type="checkbox"/> BGP Peer Connection Change	Network	▲ Critical	✓	for at least > 0 minutes	Web UI
<input checked="" type="checkbox"/> Cisco IWAN Path Change	Network	▲ Critical	✓	for at least > 0 minutes	ServiceNow, Web UI
<input type="checkbox"/> Cisco IWAN Threshold Crossing	Network	▲ Critical	✓	for at least > 0 minutes	ServiceNow, Web UI
<input type="checkbox"/> Cisco SD-WAN SLA Class Path Change	Network	▲ Critical	✓	for at least > 0 minutes	ServiceNow, Web UI
<input type="checkbox"/> Critical Traffic Response Time	Application	▲ Critical	✓	Response Time >= 1 ms for at least > 0 minutes	ServiceNow, Web UI
<input type="checkbox"/> Custom OID - BHM bps	Device, Interface	● Info	✓	Value >= 100 bps for at least > 0 minutes	Web UI
<input type="checkbox"/> Custom OID - MyOID	Device, Interface	● Info	✓	Value >= 100 bps for at least > 0 minutes	Web UI
<input type="checkbox"/> Device CPU Utilization	Device, Interface	Multiple	✓	Multiple	Web UI
<input type="checkbox"/> Device Flow Stop	Device, Interface	▲ Critical	✓	for at least > 0 minutes	ServiceNow, Web UI
<input type="checkbox"/> Device Memory Utilization	Device, Interface	Multiple	✓	Multiple	Web UI
<input type="checkbox"/> Device Reachability	Device, Interface	Multiple	✓	Multiple	ServiceNow, Web UI
<input type="checkbox"/> High WAN Interface Utilization	Device, Interface	Multiple	✓	Multiple	Web UI
<input type="checkbox"/> Interface Errors (CRC, Frame, Overruns, Ignore, Abort)	Device, Interface	▲ Critical	✓	Number of Errors >= 40 Errors for at least > 0 minutes	ServiceNow, Web UI
<input type="checkbox"/> Interface Reachability	Device, Interface	Multiple	✓	Multiple	ServiceNow, Web UI
<input type="checkbox"/> IPSLA Test	Network	▲ Critical	✓	Total Test Errors > 3 Errors for at least > 0 minutes	ServiceNow, Web UI
<input type="checkbox"/> IPSLA Voice/Jitter Test	Network	▲ Critical	✓	Total Test Errors > 3 Errors for at least > 0 minutes	Web UI

Rows: 35 / 35 Selected: 2

Clicking on an alert will show its configuration detail settings.

Alert Management LiveNX Alerts

Enable Disable
Q Search...

ALERT TYPE	CATEGORY	SEVERITY	ENABLED	THRESHOLDS	SHARING
<input type="checkbox"/> Alert Type	All	All	All	Thresholds	Sharing
<input type="checkbox"/> Application Performance - App Delay	Application	Multiple	✓	Multiple	ServiceNow, Web UI
<input type="checkbox"/> Application Performance - Network Delay	Application	Multiple	✓	Multiple	ServiceNow, Web UI
<input checked="" type="checkbox"/> BGP Peer Connection Change	Network	▲ Critical	✓	for at least > 0 minutes	Web UI
<input checked="" type="checkbox"/> Cisco IWAN Path Change	Network	▲ Critical	✓	for at least > 0 minutes	ServiceNow, Web UI
<input type="checkbox"/> Cisco IWAN Threshold Crossing	Network	▲ Critical	✓	for at least > 0 minutes	ServiceNow, Web UI
<input type="checkbox"/> Cisco SD-WAN SLA Class Path Change	Network	▲ Critical	✓	for at least > 0 minutes	ServiceNow, Web UI
<input type="checkbox"/> Critical Traffic Response Time	Application	▲ Critical	✓	Response Time >= 1 ms for at least > 0 minutes	ServiceNow, Web UI
<input type="checkbox"/> Custom OID - Birmingham	Device, Interface	● Info	✓	Value >= 100 percent for at least > 0 minutes	Web UI
<input type="checkbox"/> Device CPU Utilization	Device, Interface	Multiple	✓	Multiple	Web UI
<input type="checkbox"/> Device Flow Stop	Device, Interface	▲ Critical	✓	for at least > 0 minutes	ServiceNow, Web UI
<input type="checkbox"/> Device Memory Utilization	Device, Interface	Multiple	✓	Multiple	Web UI
<input type="checkbox"/> Device Reachability	Device, Interface	Multiple	✓	Multiple	ServiceNow, Web UI
<input type="checkbox"/> Interface Errors (CRC, Frame, Overruns, Ignore, Abort)	Device, Interface	▲ Critical	✓	Number of Errors >= 40 Errors for at least > 0 minutes	ServiceNow, Web UI
<input type="checkbox"/> Interface Reachability	Device, Interface	Multiple	✓	Multiple	Web UI
<input type="checkbox"/> IPSLA Test	Network	▲ Critical	✓	Total Test Errors > 3 Errors for at least > 0 minutes	ServiceNow, Web UI
<input type="checkbox"/> IPSLA Voice/Jitter Test	Network	▲ Critical	✓	Total Test Errors > 3 Errors for at least > 0 minutes	ServiceNow, Web UI
<input type="checkbox"/> LiveNX CPU Utilization	System	▲ Critical	✓	Local/Server >= 40 % for at least > 0 minutes	Web UI
<input type="checkbox"/> LiveNX Disk Utilization	System	▲ Critical	✓	Local/Server >= 60 % for at least > 0 minutes	Web UI
<input type="checkbox"/> LiveNX Memory Utilization	System	▲ Critical	✓	Local/Server >= 40 % for at least > 0 minutes	Web UI
<input type="checkbox"/> LiveNX Node Connectivity	System	▲ Critical	✓	for at least > 0 minutes	Web UI
<input type="checkbox"/> Media Jitter Max	Application	▲ Critical	✓	Jitter Max >= 10 ms for at least > 0 minutes	Web UI
<input type="checkbox"/> Media Jitter Min	Application	▲ Critical	✓	Jitter Min >= 10 ms for at least > 0 minutes	Web UI
<input type="checkbox"/> Media Packet Loss	Application	▲ Critical	✓	Packet Loss >= 1 % for at least > 0 minutes	Web UI

BGP Peer Connection Change

Enabled

Severity ▲ Critical

Thresholds

For at Least

0 min

Sharing

Email

Type email

ServiceNow

SNMP trap ?

Web UI

Syslog ?

Cancel Save

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

Thresholds
 For at Least
 min

Sharing

Email
 ✕
Type email

ServiceNow

SNMP trap

Web UI

Syslog

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

High WAN Interface Utilization ✕

LIST OF INSTANCES

- 1. LiveWire Interface eth1 Enabled
- 2. Birmingham router1 Enabled
- 3. Austin site Enabled
- Default threshold Disabled

INSTANCE DETAILS

General Settings

Instance Name: LiveWire Interface eth1 | Time Window: All Hours

Alert Source: Device: SE-LiveWire-NY | Interface: SE-LiveWire-NY -> eth1

Business Hours Setting: For sites without business hours configuration this setting will be ignored.

Thresholds

Time to Trigger: > 1 min | Automatic Resolution Time: 5 min

CRITICAL ▲ | Utilization: >= 60 %

WARNING ■ | Utilization: >= 50 %

Enable Switch

All alerts will have at least one enable switch:

Enabled
 On

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 ▼

Thresholds

Total Test Errors > 3 Errors

For at Least > 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 > 15 min

Automatic Resolution Time 5 min

CRITICAL ▲

Average Application Delay >= 500 ms

WARNING ■

Average Application Delay >= 400 ms

INFO ●

Average Application Delay >= 100 ms

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 >= 400 ms

Packet Loss >= 1 %

Utilization >= 60 %

Drop Rate > 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 Resolution 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

<p>Time to Trigger</p> <div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;"> > 1 min </div>	<p>Automatic Resolution Time</p> <div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;"> 4 min </div>
<p><input checked="" type="checkbox"/> CRITICAL ▲</p>	<p>Utilization</p> <div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;"> >= 80 % </div>
<p><input checked="" type="checkbox"/> WARNING ■</p>	<p>Utilization</p> <div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;"> >= 60 % </div>
<p><input type="checkbox"/> INFO ●</p>	<p>Utilization</p> <div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;"> >= 40 % </div>

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

Sharing

Email

Type email

ServiceNow ^

Default ServiceNow settings set on [Global settings](#) page. You can override individual settings below.

Category

Subcategory

Add value to override

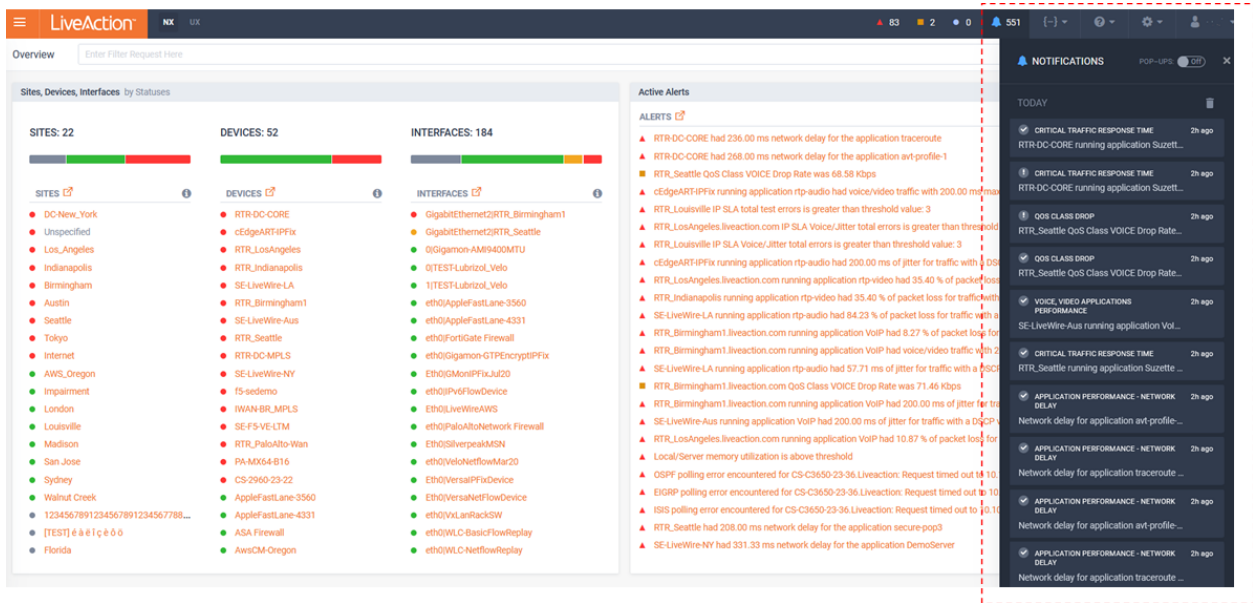
SNMP trap ⌵

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.



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
 min

Sharing

Email
 ✕
Type email

ServiceNow

SNMP trap

Web UI

Syslog

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 ✕

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.

Automatic Resolution Time

5 min

Ignore alert fluctuations and wait 5 minutes before automatically resolving an alert.

Thresholds

QoS Class

VOICE

Drop Rate **For at Least**

20 kbps

> 0 min

QoS Class

VIDEO

Drop Rate **For at Least**

50 kbps

> 1 min

Catch All Threshold

All non-specified QoS Classes

Drop Rate **For at Least**

0 kbps

> 0 min

Add Specific QoS Class 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:

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 -> eth1. 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 test@test.com 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.

The screenshot shows the 'Device CPU Utilization' configuration window. On the left, the 'LIST OF INSTANCES' panel contains one entry: 'Default threshold' with an 'Enabled' toggle. The 'INSTANCE DETAILS' panel on the right is for the 'Default Threshold' instance. It includes the following settings:

- Instance Name:** Default Threshold
- Time Window:** All Hours
- Severity:** Critical
- Alert Source:** Enter Filter Request Here
- Thresholds:**
 - Time to Trigger:** > 0 min
 - Automatic Resolution Time:** 5 min
 - Utilization:** >= 1 %
- Sharing:**
 - Email
 - Type email

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.

The screenshot shows the 'Device CPU Utilization' configuration window with a new instance. The 'LIST OF INSTANCES' panel now shows two entries: '1. New Alert' (selected) and 'Default threshold'. The 'INSTANCE DETAILS' panel is for the 'New Alert' instance. The 'Alert Source' field is highlighted with a red dashed box and contains the text 'Enter Filter Request Here'. A red error message 'Filter is Required' is visible next to the field. The 'Business Hours Setting' is also visible below the Alert Source field.

General Settings:

- Instance Name:** New Alert
- Time Window:** All Hours
- 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:** Enter Filter Request Here (Filter is Required)
- Business Hours Setting:** For sites without business hours configuration this setting will be ignored.

Thresholds:

- Time to Trigger:** > 0 min
- Automatic Resolution Time:** 5 min
- Utilization:** >= 1 %

Sharing:

- Default Configuration
- Custom Configuration

Sharing configuration for all alert instances can be changed in the **Default Threshold** instance.

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.

Device CPU Utilization ✕

LIST OF INSTANCES ⓘ

1. Austin Router	Enabled <input type="checkbox"/>	
Default threshold	Enabled <input type="checkbox"/>	

ADD NEW INSTANCE

INSTANCE DETAILS

General Settings

Instance Name

Time Window

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

> 0

min

Automatic Resolution Time

5

min

Utilization

>= 1

%

Sharing

Default Configuration
 Custom Configuration

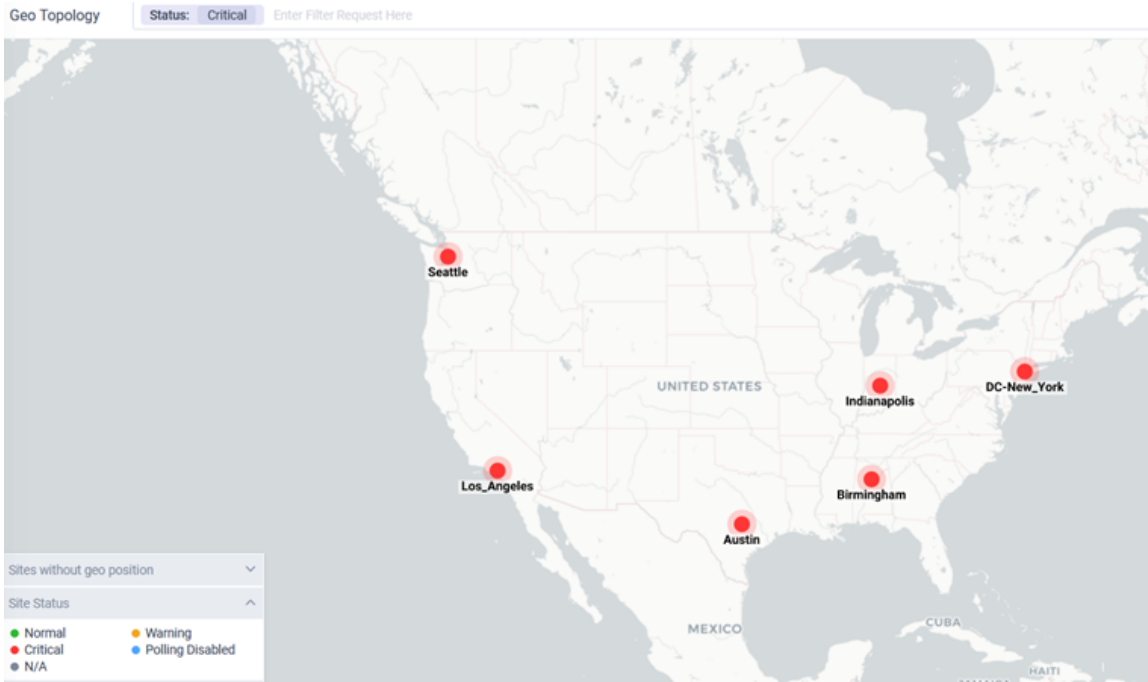
Sharing configuration for all alert instances can be changed in the **Default Threshold** instance.

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:



Overview | Enter Filter Request Here | Apply filter | Auto

Sites, Devices, Interfaces by Statuses

SITES: 22 | **DEVICES: 52** | **INTERFACES: 184**

- SITES:** DC-New_York, Birmingham, Indianapolis, Los_Angeles, Austin, Unspecified, Seattle, Internet, Tokyo, San_Jose, Louisville, AWS_Oregon, Impairment, London, Madison, Sydney, Walnut_Creek, [TEST] 6 8 1 c 6 0 0, Florida
- DEVICES:** RTR-DC-MPLS, RTR_Birmingham1, RTR_Indianapolis, SE-LiveWire-LA, RTR_LosAngeles, SE-LiveWire-Aus, cEdgeART-IPFix, RTR-DC-CORE, SE-LiveWire-NY, RTR_Seattle, RTR_PaloAlto-Wan, SE-F5-VE-LTM, IWAN-SR-LINET, IWAN-SR-MPLS, PAX-MX4-016, CS-2060-23-22, IS-sedemo, Silverpeak-AUS, RTR_SanJose, CS-C850-23-31
- INTERFACES:** GigabitEthernet2/RTR_Birmingham1, GigabitEthernet2/RTR_Seattle, GigabitEthernet2/RTR_SanJose, GigabitEthernet2/RTR_Louisville, 0/Gigamon-AM9400MTU, 0/TEST-LuBrizol_Velo, eth0/AppleFastLane-3560, eth0/FortGate_Firewall, eth0/Gigamon-GTP-EncryptIPFix, eth0/IPv6FlowDevice, ETH0/MonIPFixJud0, eth0/NetFlowMar20, ETH0/NetFlowMar20, ETH0/VersaIPFlowDevice, eth0/WLamRack3W

Active Alerts

ALERTS | TIME OPENED

- RTR_Seattle QoS Class VOICE Drop Rate was 66.48 Kbps (09 Mar 2021, 01:39 PM)
- SE-LiveWire-Aus running application VoIP had voice/video traffic with 31.23 ms max jitter (09 Mar 2021, 01:38 PM)
- cEdgeART-IPFix running application rtp-audio had voice/video traffic with 200.00 ms max jitter (09 Mar 2021, 01:35 PM)
- RTR_Louisville IP SLA total test errors is greater than threshold value: 3 (09 Mar 2021, 01:22 PM)
- RTR-DC-MPLS running application VoIP had 59.48 % of packet loss for traffic with a DSCP value of 46 (EF) (09 Mar 2021, 01:17 PM)
- RTR_Birmingham1.Iveaction.com running application VoIP had 33.49 % of packet loss for traffic with a DSCP value of ... (09 Mar 2021, 01:17 PM)
- Local/Server memory utilization is above threshold (09 Mar 2021, 01:16 PM)
- RTR_LosAngeles.Iveaction.com IP SLA Voice/Jitter total errors is greater than threshold value: 3 (09 Mar 2021, 01:16 PM)
- RTR_Indianapolis running application rtp-video had 35.40 % of packet loss for traffic with a DSCP value of 0 (BE) (09 Mar 2021, 01:13 PM)
- SE-LiveWire-LA running application rtp-audio had 84.59 % of packet loss for traffic with a DSCP value of 46 (EF) (09 Mar 2021, 01:12 PM)
- RTR_LosAngeles.Iveaction.com running application rtp-video had 32.65 % of packet loss for traffic with a DSCP value ... (09 Mar 2021, 01:04 PM)
- RTR_LosAngeles.Iveaction.com running application VoIP had 10.69 % of packet loss for traffic with a DSCP value of 4... (09 Mar 2021, 12:51 PM)
- SE-LiveWire-Aus running application VoIP had 200.00 ms of jitter for traffic with a DSCP value of 46 (EF) (09 Mar 2021, 12:32 PM)
- cEdgeART-IPFix running application rtp-audio had 200.00 ms of jitter for traffic with a DSCP value of 0 (BE) (09 Mar 2021, 12:25 PM)
- RTR-DC-MPLS running application VoIP had 200.00 ms of jitter for traffic with a DSCP value of 0 (BE) (09 Mar 2021, 11:43 AM)
- RTR_Birmingham1.Iveaction.com running application VoIP had 133.59 ms of jitter for traffic with a DSCP value of 0 (BE) (09 Mar 2021, 11:41 AM)
- RTR_Birmingham1.Iveaction.com QoS Class VOICE Drop Rate was 39.79 Kbps (09 Mar 2021, 11:02 AM)
- SE-LiveWire-LA running application rtp-audio had 200.00 ms of jitter for traffic with a DSCP value of 46 (EF) (08 Mar 2021, 11:29 PM)
- SE-LiveWire-LA running application VoIP had voice/video traffic with 12.17 ms max jitter (08 Mar 2021, 07:49 PM)
- LiveNX has not received flows from MPLS-CORE.Iveaction.com for 1120 minutes (08 Mar 2021, 07:08 PM)
- RTR_Louisville IP SLA Voice/Jitter total errors is greater than threshold value: 3 (08 Mar 2021, 09:23 AM)
- RTR-DC-MPLS running application VoIP had 200.00 ms of jitter for traffic with a DSCP value of 46 (EF) (08 Mar 2021, 08:31 AM)
- RTR-DC-MPLS running application NetApp had 51.78 % of packet loss for traffic with a DSCP value of 0 (BE) (08 Mar 2021, 08:17 AM)
- GigabitEthernet2 on RTR_Birmingham1.Iveaction.com was over utilized at 31.45% in the inbound direction. (07 Mar 2021, 02:15 AM)

Sites | Enter Filter Request Here | Apply filter | Mar 09, 2021 13:20:00 – Mar 09, 2021 13:35:00 | 15 Min | Auto | Configure Sites

SITE NAME	SITE STATUS	DEVICE REACHABILITY	DEVICE CPU/MEMORY	PEAK UTILIZATION IN	PEAK UTILIZATION OUT	CONGESTION DROPS	INTERFACE ERRORS
Austin	●	●	●	0%	0%	●	0
Birmingham	●	●	●	80.48%	150.22%	●	0
DC-New_York	●	●	●	2.38%	1.26%	●	0
Indianapolis	●	●	●	0%	0%	●	0
Internet	●	●	●	0%	0%	●	0
Los_Angeles	●	●	●	0.08%	0.3%	●	0
Seattle	●	●	●	77.41%	150.18%	●	0
Tokyo	●	●	●	0.51%	0.66%	●	0
Unspecified	●	●	●	0%	0%	●	0
San_Jose	●	●	●	53.73%	100.01%	●	0
AWS_Oregon	●	●	●	0%	0%	●	0
Impairment	●	●	●	-	-	●	0
London	●	●	●	8.06%	14.7%	●	0
Louisville	●	●	●	0.02%	0.03%	●	0
Madison	●	●	●	0.02%	0.03%	●	0
Sydney	●	●	●	0.45%	0.56%	●	0
Walnut_Creek	●	●	●	0%	0%	●	0
12345678912345678912345677...	●	●	●	-	-	●	0

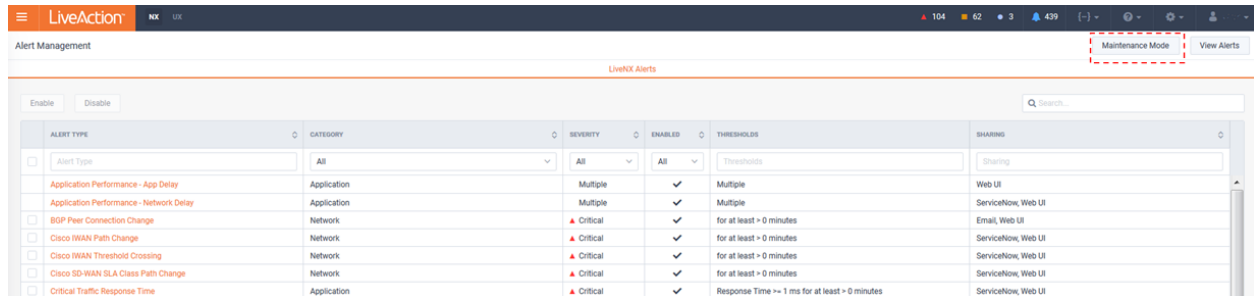
All rows 22

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

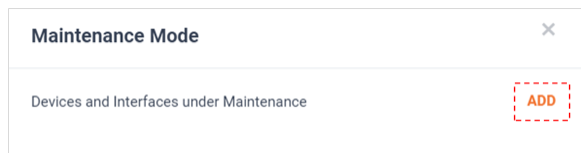
ALERT TYPE	
<input type="checkbox"/>	Alert Type
	Application Performance - Network Delay
<input type="checkbox"/>	BGP Peer Connection Change
<input type="checkbox"/>	Cisco IWAN Path Change
<input type="checkbox"/>	Cisco IWAN Threshold Crossing
<input type="checkbox"/>	Cisco SD-WAN SLA Class Path Change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



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



A list of devices appears.

Maintenance Mode

Add Devices and Interfaces under Maintenance **SAVE**

Enter Filter Request Here

Sort by: Name ▾

Page 1 / 3

AppleFastLane-3560	<input type="checkbox"/>
AppleFastLane-4331	<input type="checkbox"/>
ASA Firewall	<input type="checkbox"/>
AwsCM-Oregon	<input type="checkbox"/>
AzureCM-USWest	<input type="checkbox"/>
cEdgeART-IPFix	<input type="checkbox"/>
CS-2960-23-22	<input type="checkbox"/>
CS-C3650-23-36	<input type="checkbox"/>
CS-C3850-23-31	<input type="checkbox"/>

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**

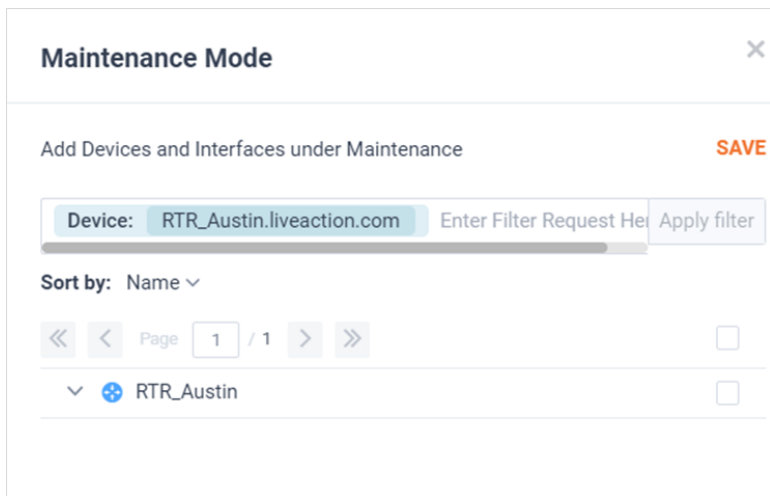
Enter Filter Request Here

Site

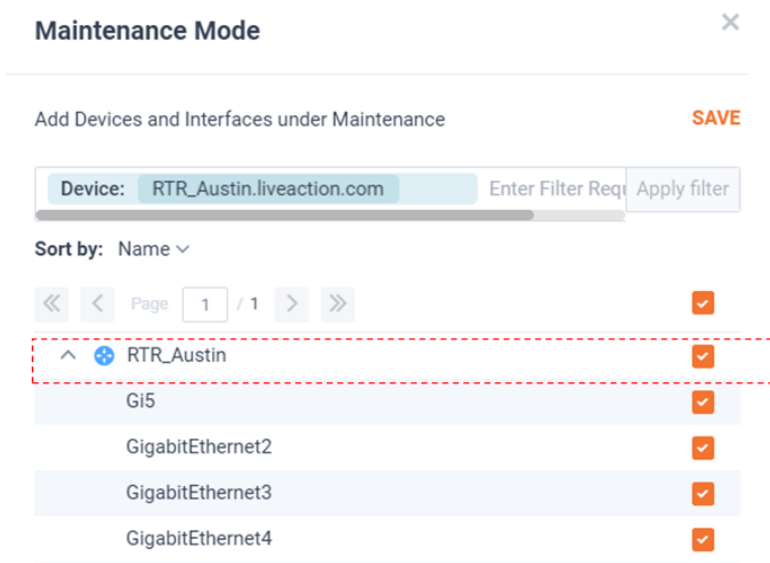
Device

Tag

AppleFastLane-4331	<input type="checkbox"/>
ASA Firewall	<input type="checkbox"/>
AwsCM-Oregon	<input type="checkbox"/>
AzureCM-USWest	<input type="checkbox"/>
cEdgeART-IPFix	<input type="checkbox"/>
CS-2960-23-22	<input type="checkbox"/>
CS-C3650-23-36	<input type="checkbox"/>
CS-C3850-23-31	<input type="checkbox"/>
f5-sedemo	<input type="checkbox"/>
FortiGate Firewall	<input type="checkbox"/>



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



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 Maintenance SAVE

Device: RTR_Austin.liveaction.com Enter Filter Request Here Apply filter

Sort by: Name ▾

Page 1 / 1 ✓

Device	Count	Selected
^ + RTR_Austin	1/4	-
Gi5		<input type="checkbox"/>
GigabitEthernet2		<input checked="" type="checkbox"/>
GigabitEthernet3		<input type="checkbox"/>
GigabitEthernet4		<input type="checkbox"/>

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

Maintenance Mode ✕

Devices and Interfaces under Maintenance EDIT

Enter Filter Request Here Apply filter

Page 1 / 1

^ + RTR_Austin

- Gi5
- GigabitEthernet2
- GigabitEthernet3
- GigabitEthernet4

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

Maintenance Mode ✕

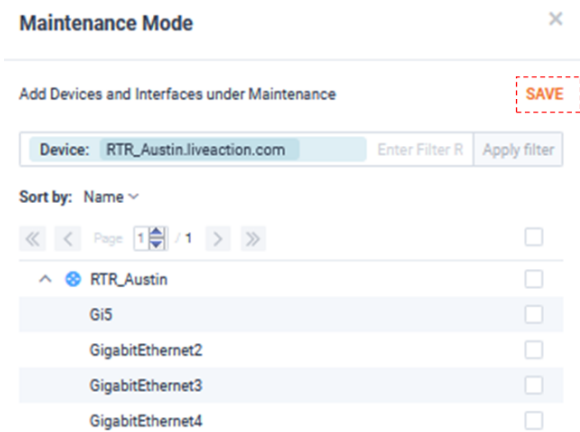
Devices and Interfaces under Maintenance EDIT

Enter Filter Request Here Apply filter

Page 1 / 1

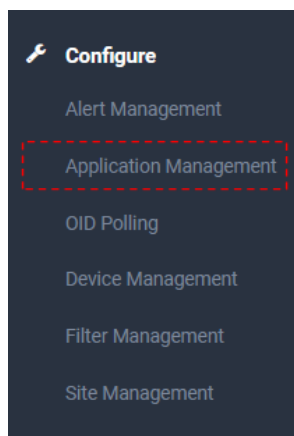
^ + RTR_Austin

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



Application Management

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



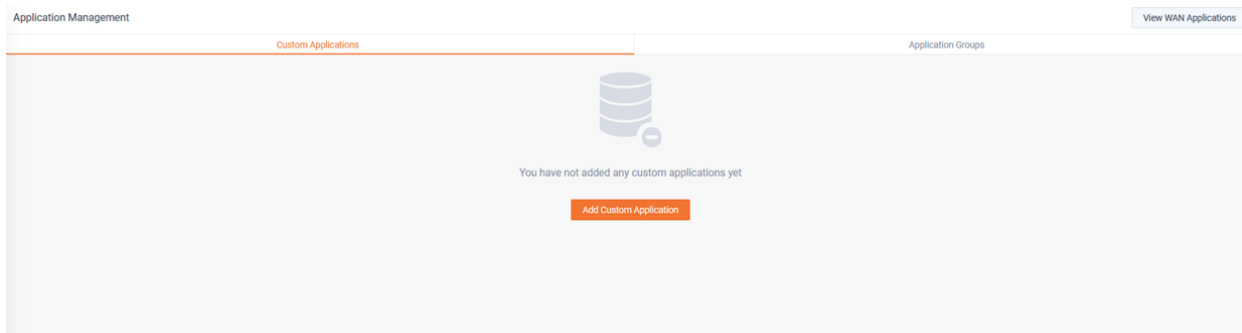
Custom Applications

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**.



The *Add Custom Application* modal appears.

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

ADD CUSTOM APPLICATION ✕

<p>Name *</p> <input style="width: 90%;" type="text" value="Enter Custom Application Name"/>	<p>Description</p> <input style="width: 90%;" type="text" value="Enter Custom Application Description"/>
<p><input checked="" type="radio"/> Network attributes</p>	
<p>IP Ranges</p> <input style="width: 90%;" type="text" value="Specify IPs or IP ranges (ex: 192.168.1.1-192.168.1.200)"/>	<p>Include Application</p> <input style="width: 90%;" type="text" value="Start typing for more results"/>
<p>Layer 4 Protocol</p> <input style="width: 90%;" type="text" value="Specify protocols. Matches any protocol by default"/>	<p>Port Ranges</p> <input style="width: 90%;" type="text" value="Specify ports or port ranges (ex: 2427-2430), one per line"/>
<p>DSCP</p> <input style="width: 90%;" type="text" value="Specify DSCP classes"/>	
<p><input type="radio"/> URLs</p>	
<p>HTTP host or SSL common name</p> <input style="width: 90%;" type="text" value="Enter HTTP host or SSL common name. Ex: *.webex.com"/> <p style="font-size: small; text-align: center;">You can use wildcards in host names</p>	<p>URI</p> <input style="width: 90%;" type="text" value="Enter URI"/> <p style="font-size: small; text-align: center;">You can use wildcards in URI</p>
<p><input type="button" value="Cancel"/> <input style="background-color: #f4a460;" type="button" value="Save"/></p>	

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:

ADD CUSTOM APPLICATION ✕

Name *

Description

Network attributes

IP Ranges

Include Application

Layer 4 Protocol Added: 1

UDP ✕
✕

Select protocol

Port Ranges

DSCP

URLs

HTTP host or SSL common name

You can use wildcards in host names

URI

You can use wildcards in URI

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

ADD CUSTOM APPLICATION ✕

Name *

Description

Network attributes

IP Ranges Added: 2

172.16.200.10 ✕
172.16.200.11 ✕
✕

Specify IPs or IP ranges (ex: 192.168.1.1-192.168.1.200)

Include Application

Layer 4 Protocol

Port Ranges

DSCP

URLs

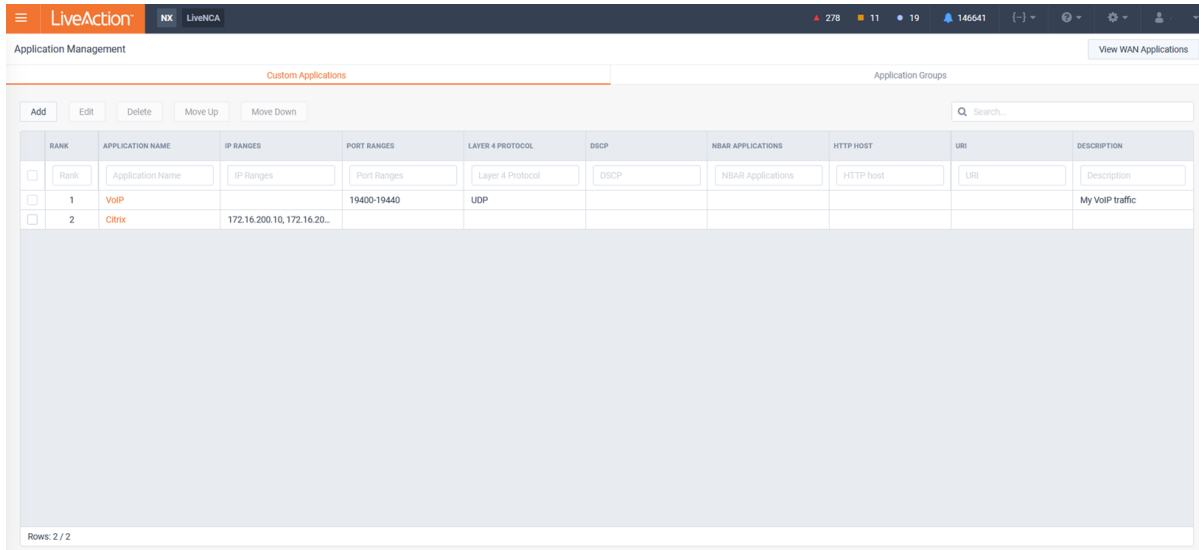
HTTP host or SSL common name

You can use wildcards in host names

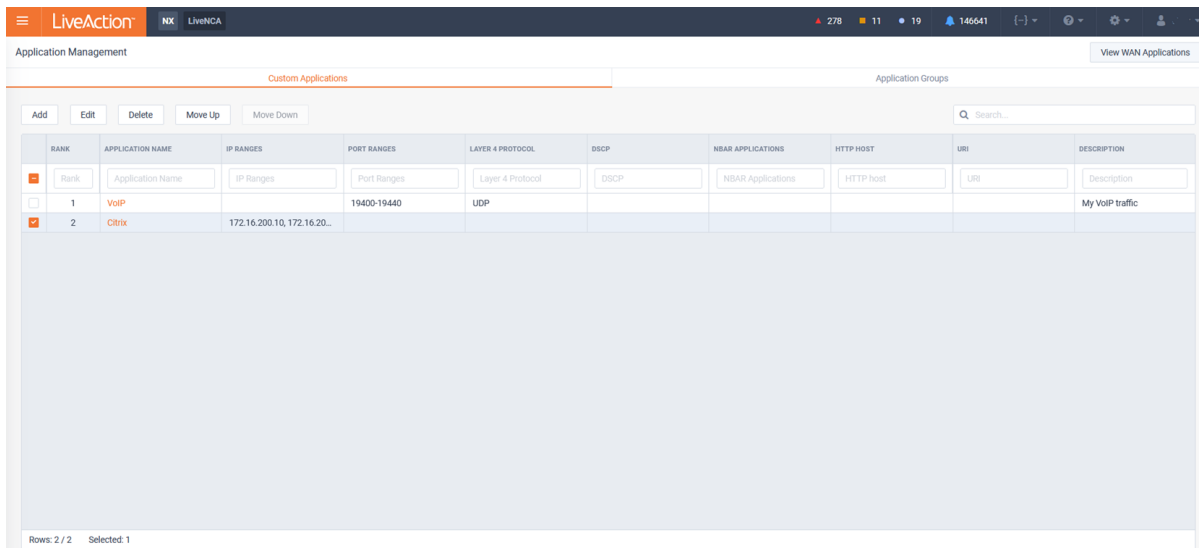
URI

You can use wildcards in URI

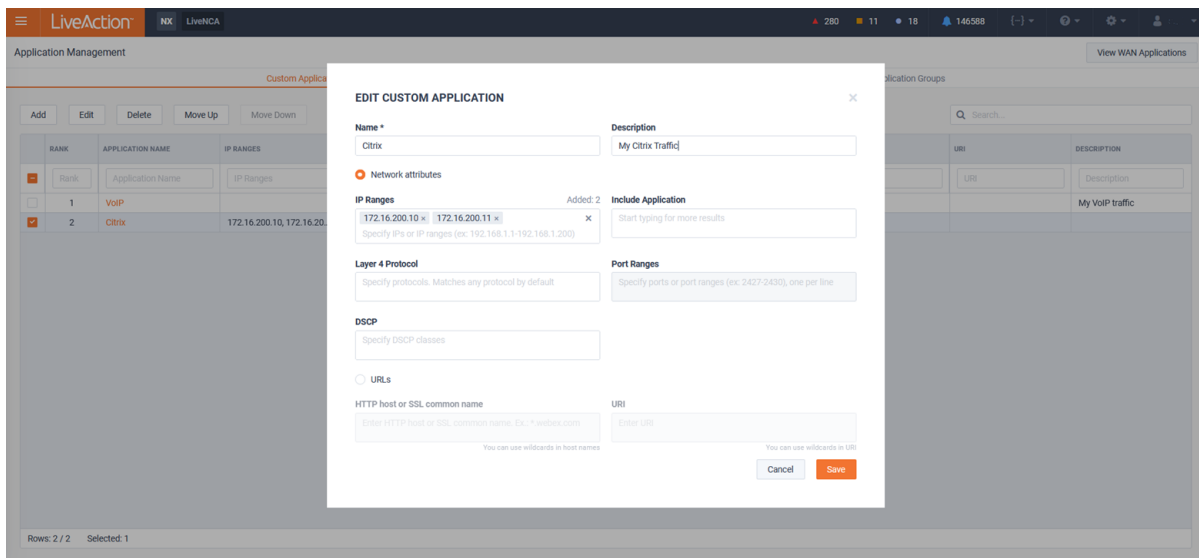
After defining the Custom Application, click **Save**. The list of applications appears on the *Custom Applications* tab.



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

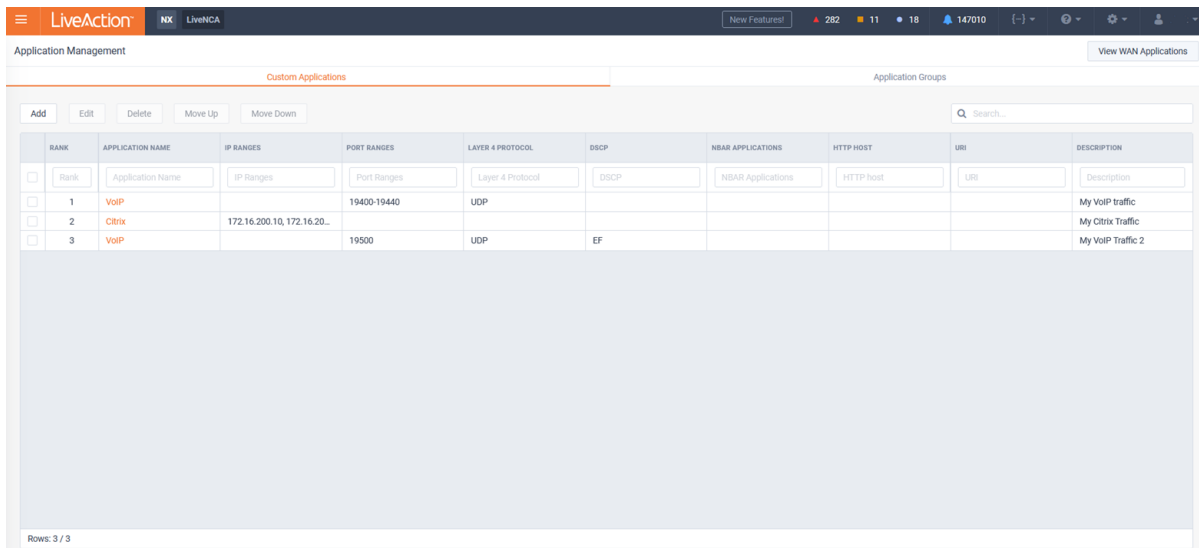


The *Edit Custom Application* modal appears. Make any desired changes and click **Save**.



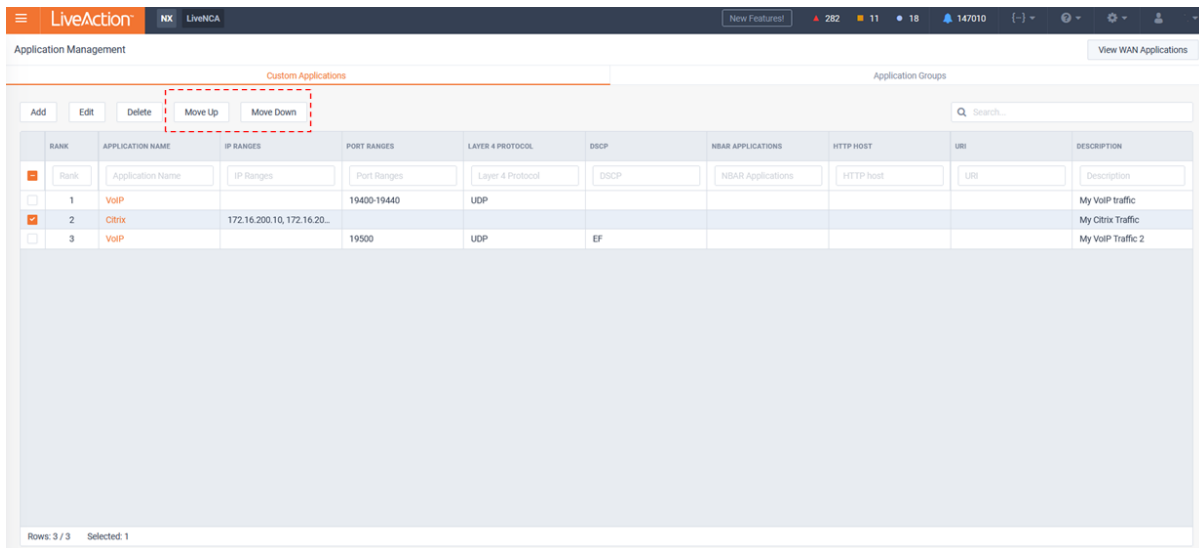
Note It is possible to have multiple Custom Application definitions with the same name, this ensures the most flexibility in naming applications as desired.

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**.



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

RANK	APPLICATION NAME	IP RANGES	PORT RANGES	LAYER 4 PROTOCOL	DSCP	NSAR APPLICATIONS	HTTP HOST	URI	DESCRIPTION
1	VoIP		19400-19440	UDP					My VoIP traffic
2	VoIP		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, URI can also be included.

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

ADD CUSTOM APPLICATION ✕

Name *

Network attributes

IP Ranges

Layer 4 Protocol

DSCP

URLs

HTTP host or SSL common name Added: 2
 ✕
Enter HTTP host or SSL common name. Ex.: *.webex.com
You can use wildcards in host names

Description

Include Application

Port Ranges

URI

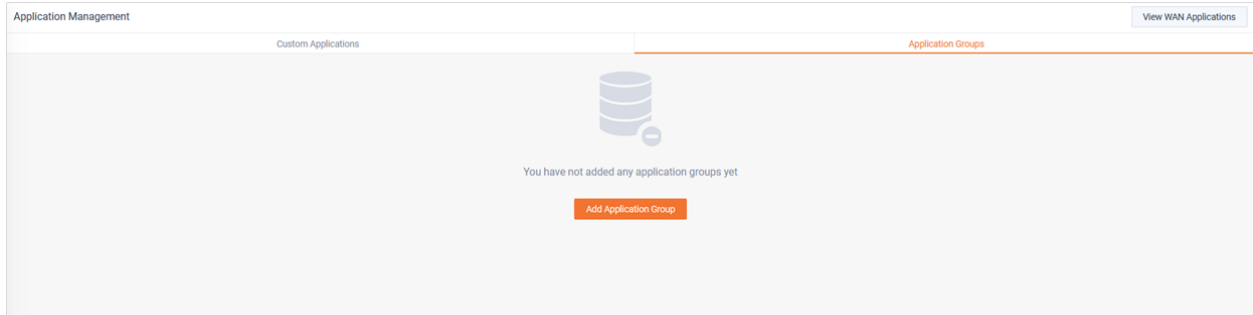
You can use wildcards in URI

Application Groups

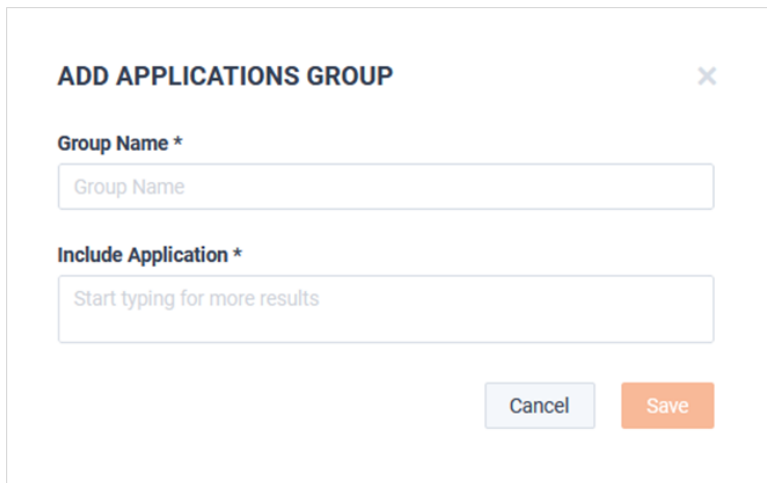
Applications Groups can be used for simplified application management. For example, an application can be identified by different names by various manufactures, hardware models, and even different version of OS from the same device type. To help simplify inconsistent names Application Groups can be used.

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

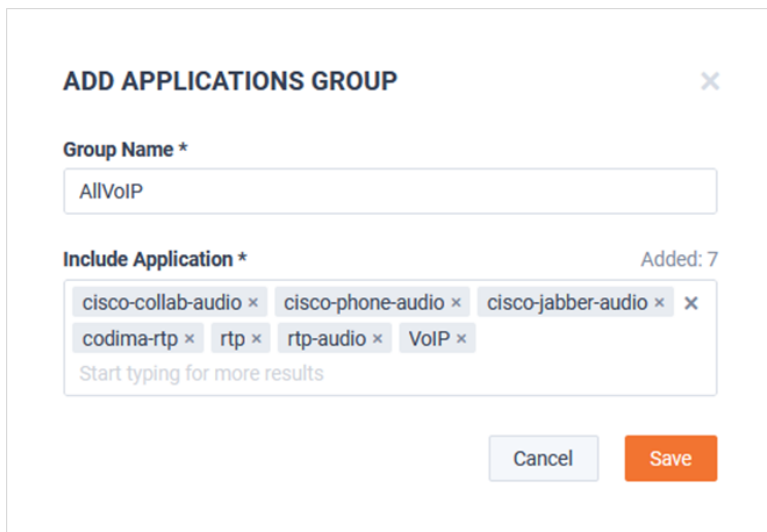
To add the first application group, from the *Application Group* tab, click **Add Application Group**.



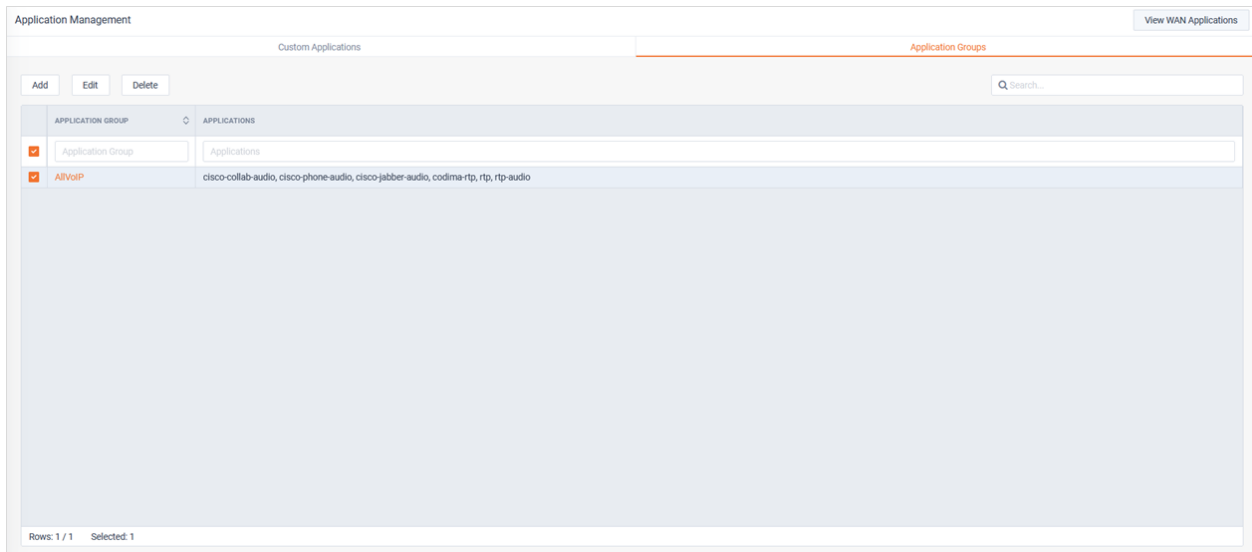
The *Add Application Group* modal appears.



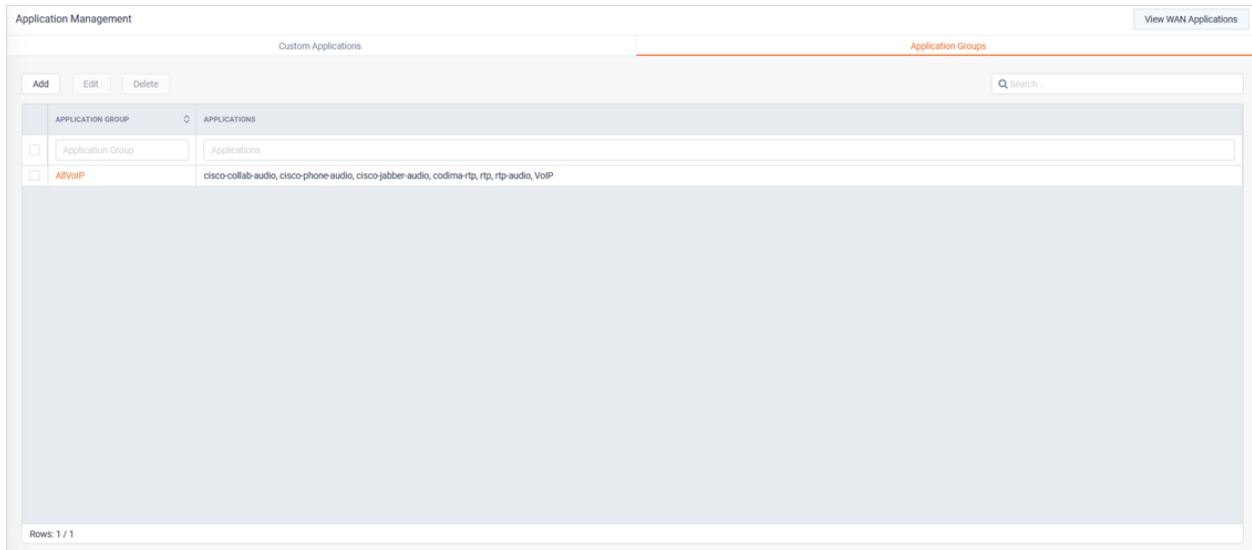
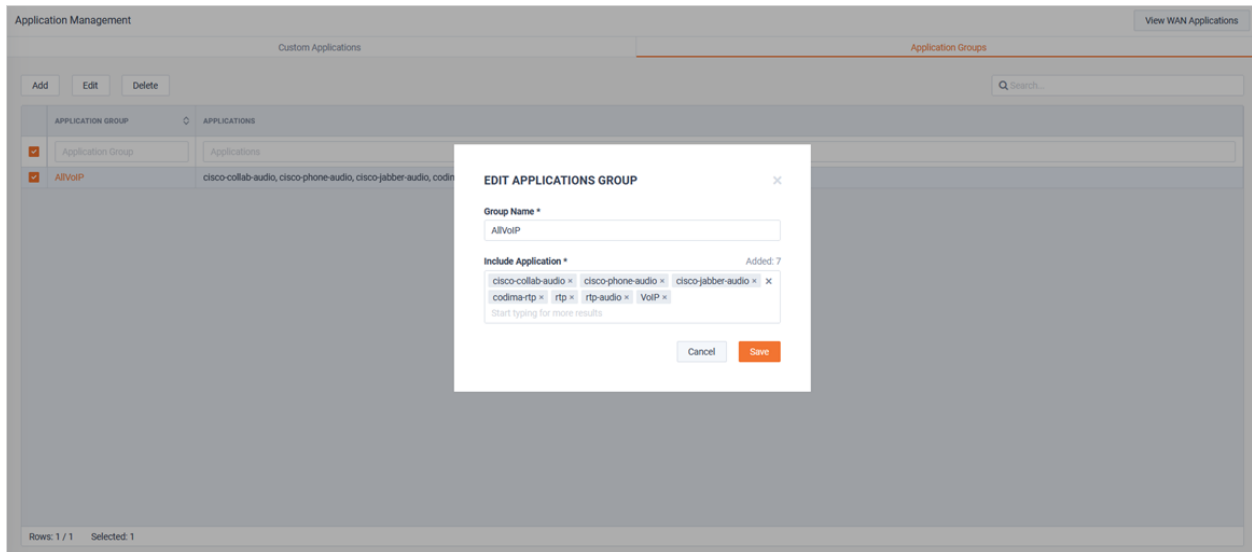
Provide a name and add the desired applications to the group. When finished, click **Save**.



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

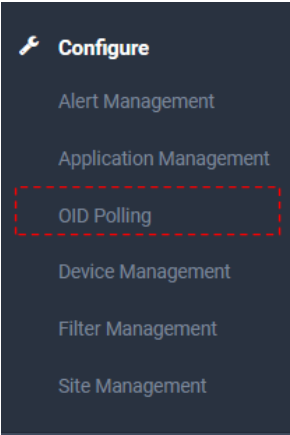


Update the group and when finished, click **Save**.



OID Polling

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

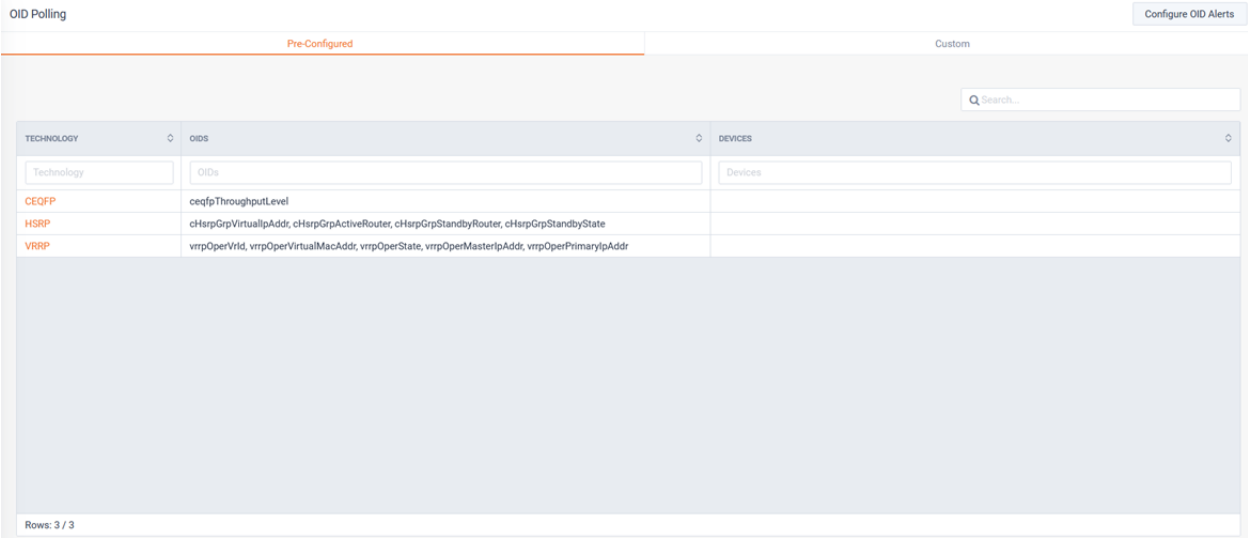


OID Polling provides two tabs:

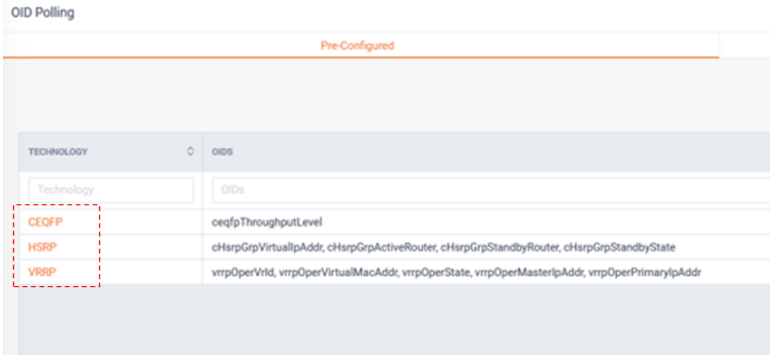
- *Pre-Configured*
- *Custom*

Pre-Configured

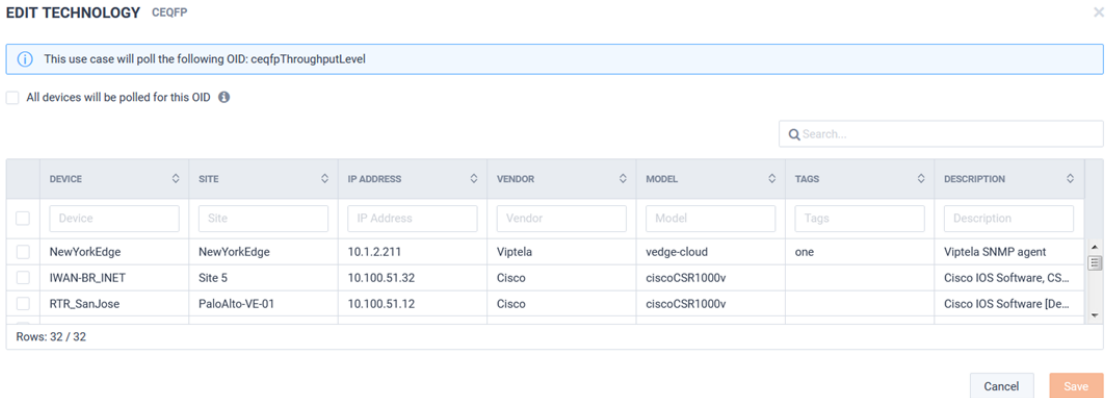
This tab provides built-in use cases.



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



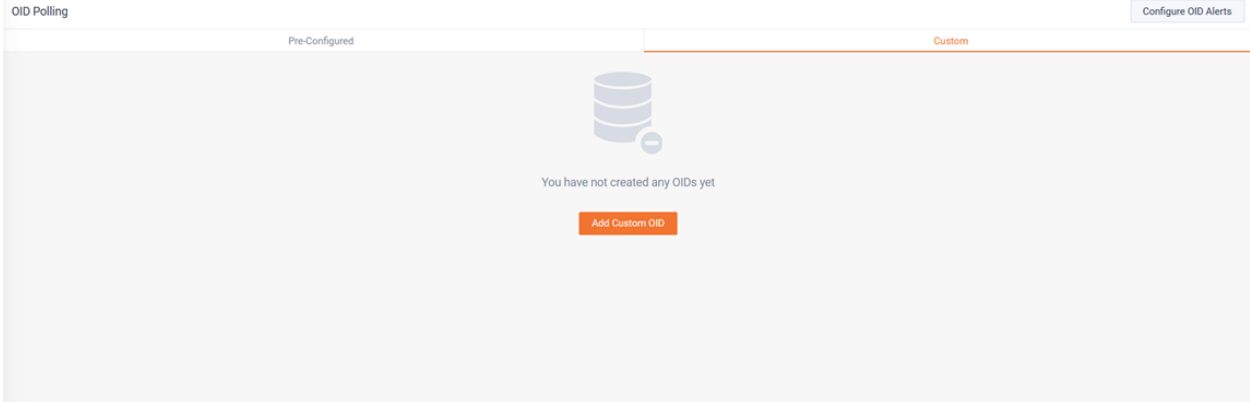
Select the device(s) of interest and click **Save**.



Custom

This tab allows for user defined OIDs

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



The *Add OID* modal appears.

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

ADD OID
✕

General
Devices (0)

Name *

OID Index * ⓘ

Processing Type ⓘ

Units *

Conversion Type ⓘ

Conversion Factor * ⓘ

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

ADD OID
✕

General
Devices (1)

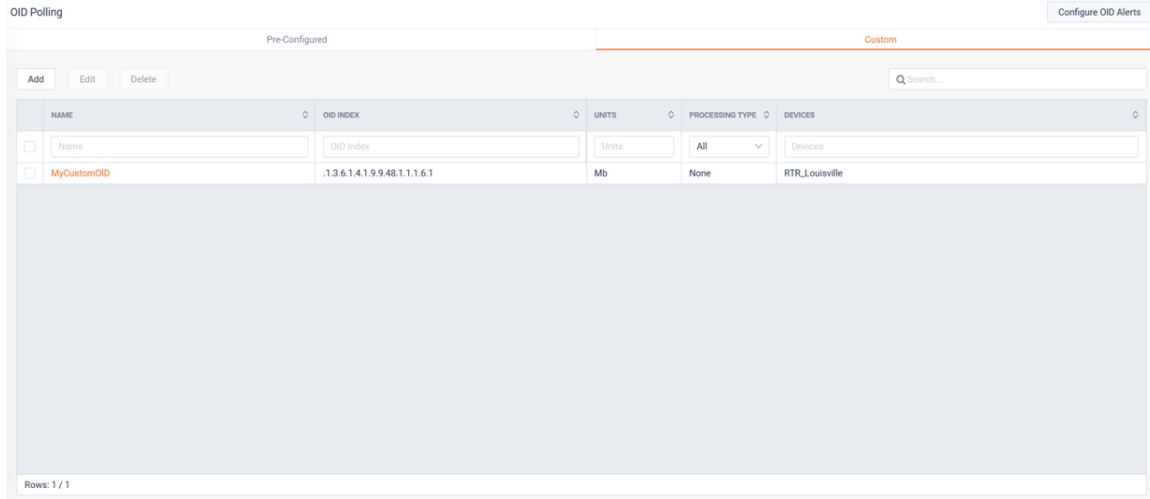
All devices will be polled for this OID ⓘ

Note: At least one device is required. Make sure that the current OID is configured for all selected devices.

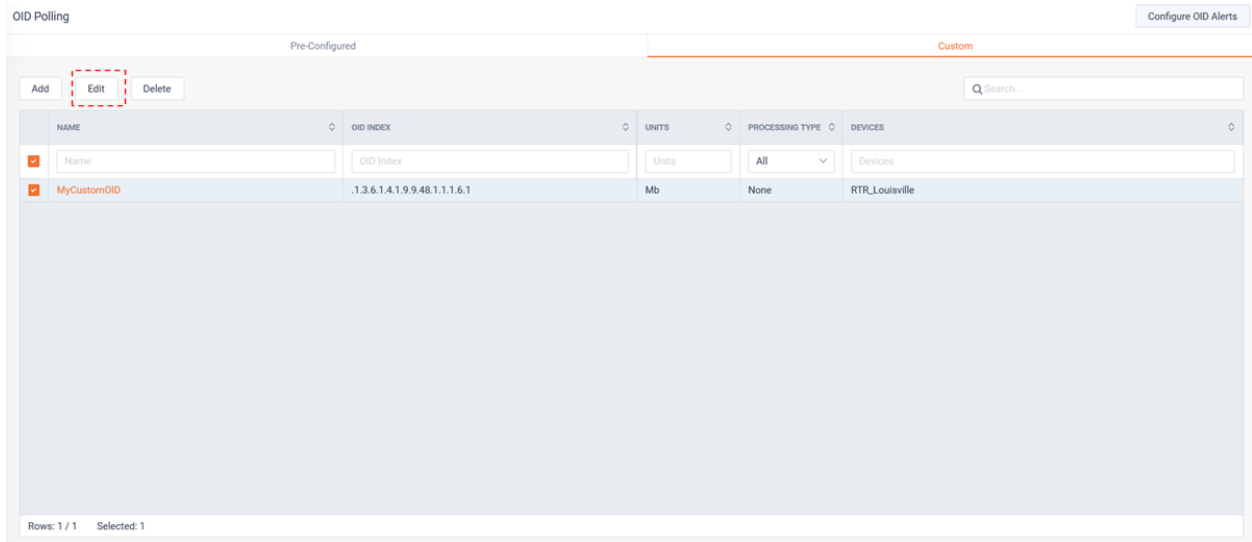
DEVICE	SITE	IP ADDRESS	VENDOR	MODEL	TAGS	DESCRIPTION
<input type="checkbox"/> Device	<input type="text" value="Site"/>	<input type="text" value="IP Address"/>	<input type="text" value="Vendor"/>	<input type="text" value="Model"/>	<input type="text" value="Tags"/>	<input type="text" value="Description"/>
<input type="checkbox"/> vSmart		10.4.201.216	Viptela	vsmart		
<input checked="" type="checkbox"/> RTR_Louisville	Louisville	10.100.51.10	Cisco	ciscoCSR1000v		Cisco IOS Software [De...
<input type="checkbox"/> HE-CSR-207	PaloAlto-VE-01	10.4.201.207	Cisco	ciscoCSR1000v		Cisco IOS Software, CS...
<input type="checkbox"/> PaloAltoEdge-TLOC-Ext...	PALOALTO	10.4.201.214	Viptela	vedge-cloud		
<input type="checkbox"/> CS-2960-23-22	Site 5	10.100.51.22	Cisco	catalyst29608TCS		Cisco IOS Software, C2...
<input type="checkbox"/> RTR-DC-CORE	New York - DC	10.100.51.3	Cisco	ciscoCSR1000v		Cisco IOS Software, CS...
<input type="checkbox"/> RTR_Madison	Madison	10.100.51.11	Cisco	ciscoCSR1000v		Cisco IOS Software [De...
<input type="checkbox"/> RTR_PaloAlto-Wan	Site 5	10.100.51.14	Cisco	ciscoCSR1000v		Cisco IOS Software, CS...

Rows: 32 / 32 Selected: 1

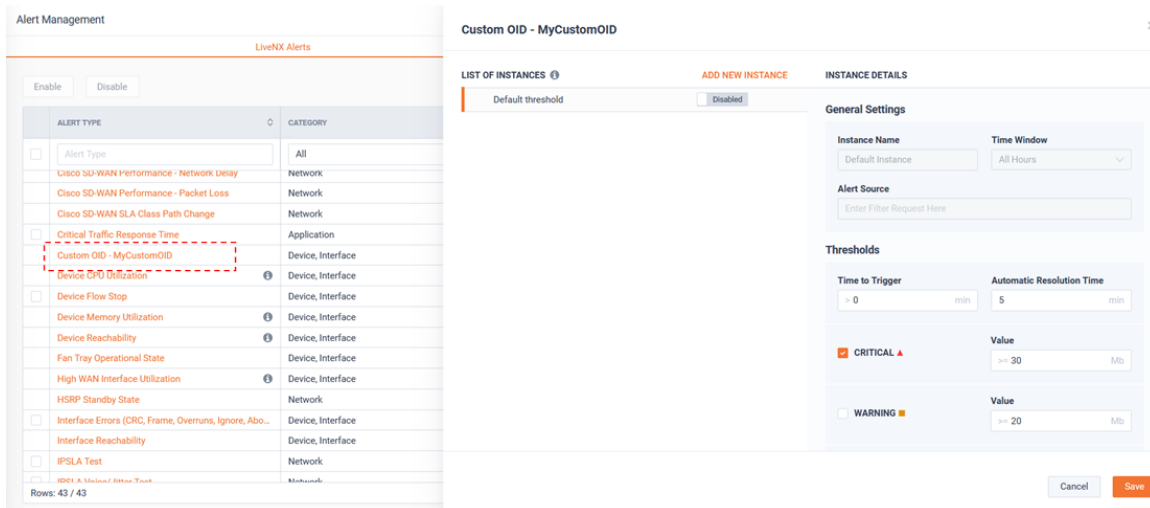
The Custom OID will be added to the Custom tab.



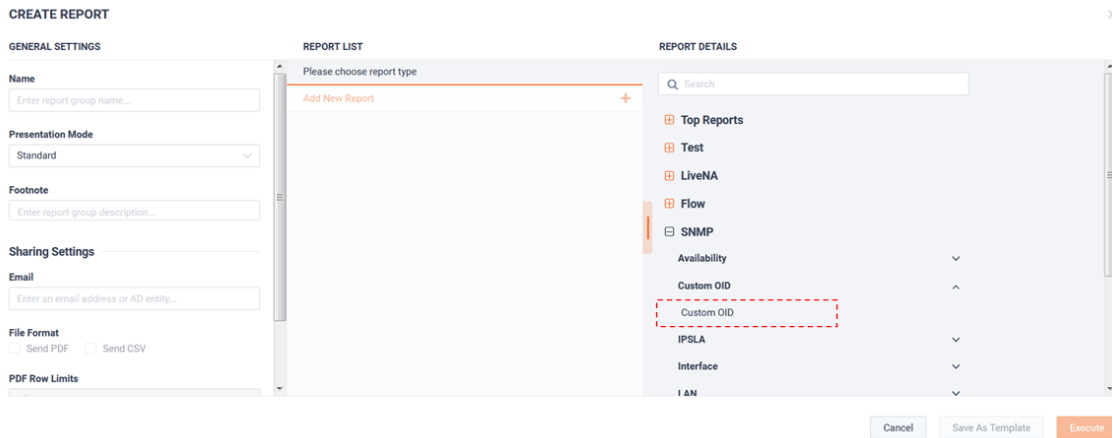
To edit the custom OID, select the OID and click **Edit**.



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

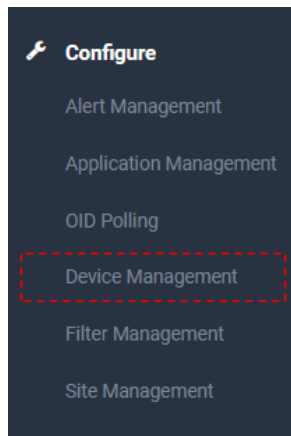


Additionally, a Custom OID report will be automatically created too.



Device Management

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



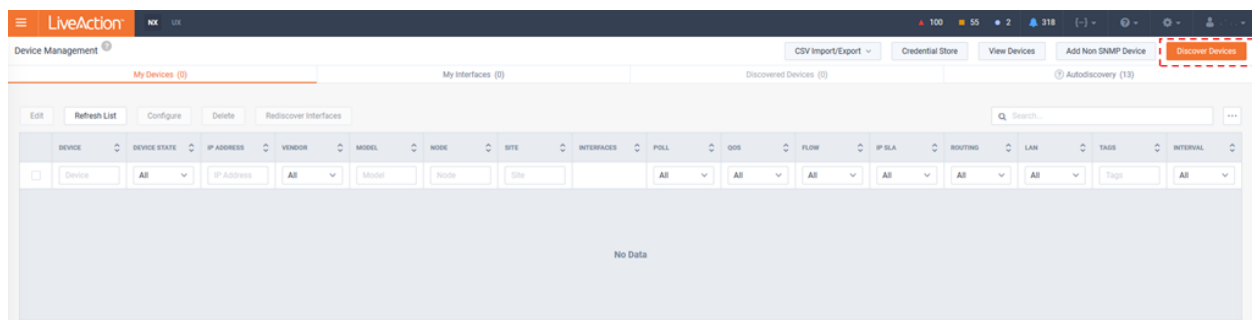
There are two types of monitored devices in LiveNX:

- *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.



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

DISCOVER DEVICES [X]

1. What to scan | 2. SNMP Settings | 3. Node

SPECIFY IP RANGES

IP Range (ex. 192.168.1.1 - 200) or CIDR Notation, or one per line Choose a site

SPECIFY SEED DEVICE TO SCAN

IP address Hops

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.

DISCOVER DEVICES [X]

1. What to scan | 2. SNMP Settings | 3. Node

SPECIFY IP RANGES

10.100.51.10 Choose a site

SPECIFY SEED DEVICE TO SCAN

IP address Hops

SNMP Settings can be selected using either:

1. Using the Default SNMP Connection Settings.

DISCOVER DEVICES [Close]

1. What to scan | **2. SNMP Settings** | 3. Node

DEFAULT SNMP CONNECTION SETTINGS
SNMP Credential Store Configuration Page

ENTER SNMP CONNECTION SETTINGS FOR THIS DEVICE

Back Save & Next Cancel Discover

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).

DISCOVER DEVICES [Close]

1. What to scan | **2. SNMP Settings** | 3. Node

DEFAULT SNMP CONNECTION SETTINGS

ENTER SNMP CONNECTION SETTINGS FOR THIS DEVICE

SNMP Version * Target Port *

Version 2c 161

Community String *

Enter Community String

Back Save & Next Cancel Discover

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

DISCOVER DEVICES [Close]

1. What to scan | 2. SNMP Settings | **3. Node**

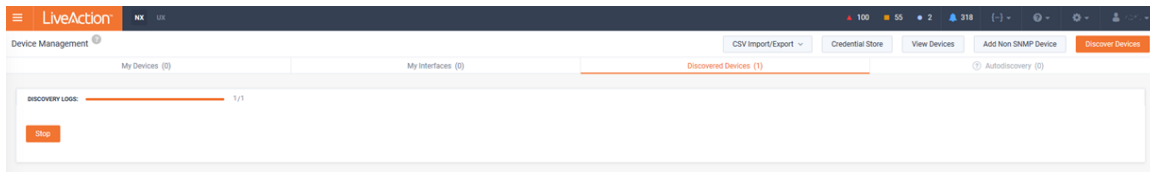
Specify Node

Local/Server

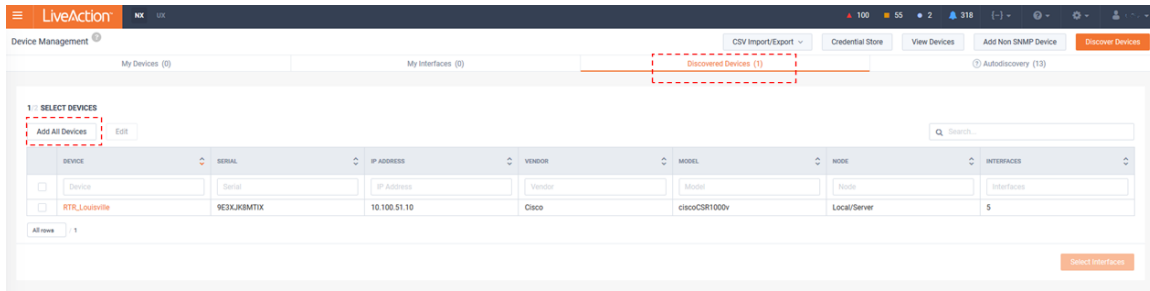
Back Cancel Discover

When ready, click *Discover*.

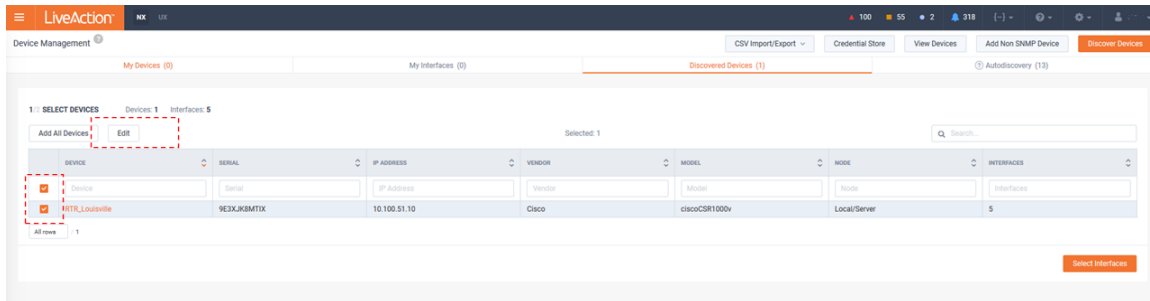
The *Discover Devices* modal closes, and a discovery progress bar is displayed.



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.



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



EDIT RTR_SEATTLE ✕

Site (no site selected) **Group** (No Group Selected) **Interval** (1 Minute)

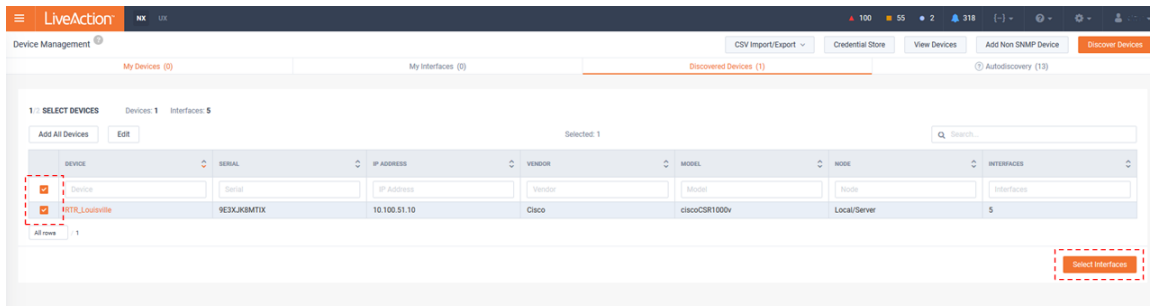
IP Address*
 10.100.51.2

POLL
 IP SLA
 QOS
 ROUTING
 FLOW
 LAN

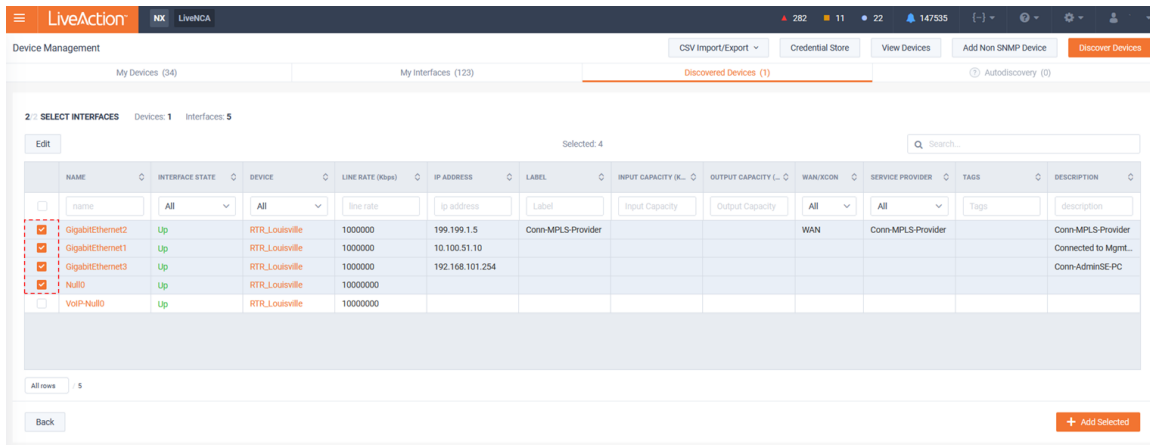
Associate Probe at IP Address (Type IP Address)
 Hardcode Sample Ratio (1/)

Tags

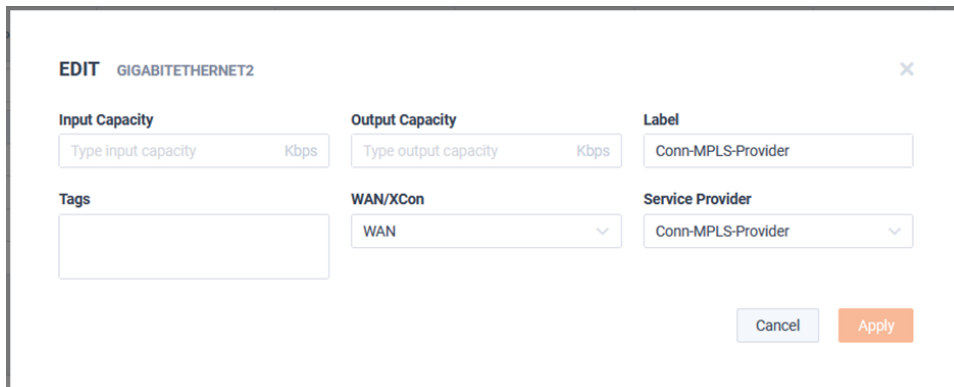
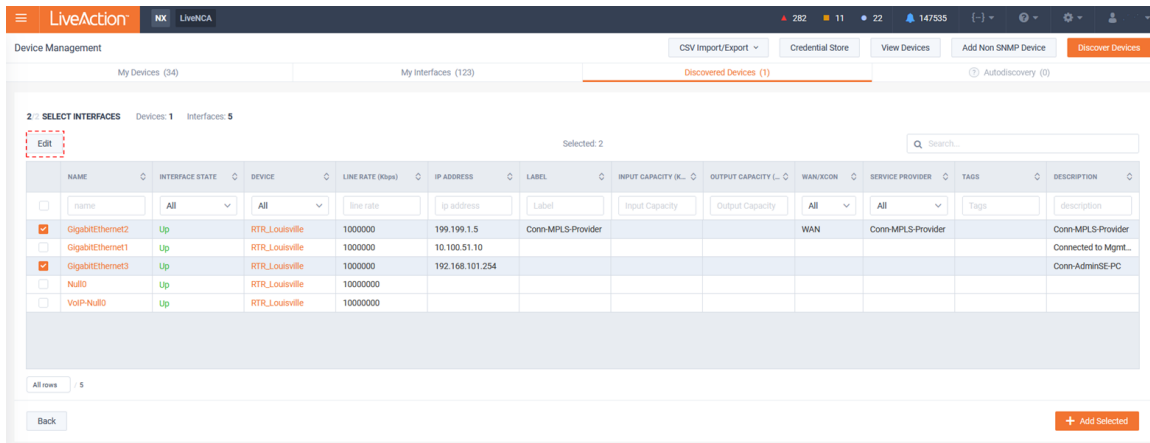
Or the monitored interfaces can be updated by selecting the device(s) of interest and clicking **Select Interfaces**.



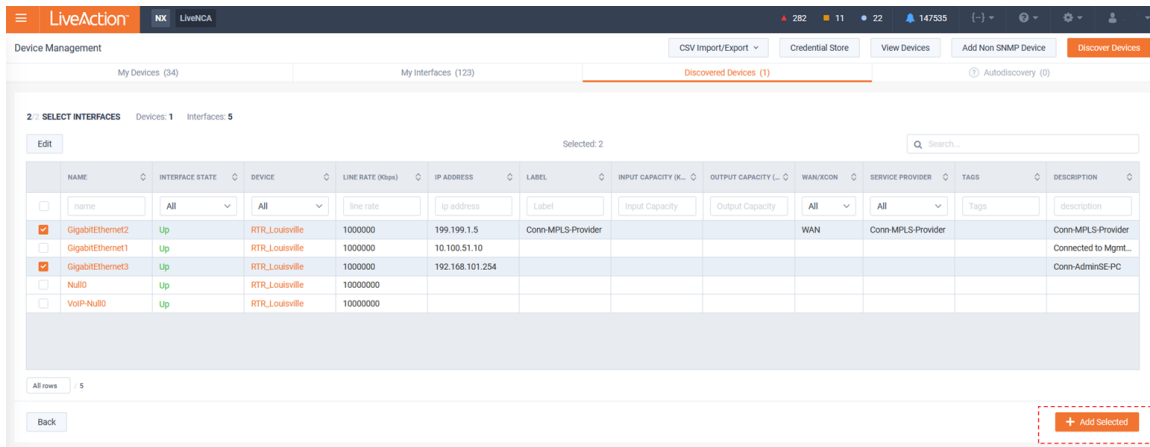
Monitored Interfaces can be chosen by ensuring their corresponding check box is selected.



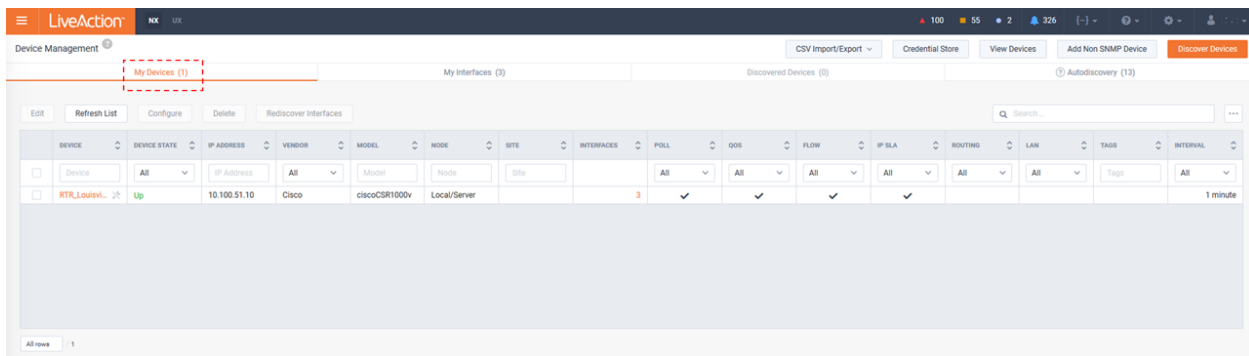
Selected monitored interface settings can also be updated by clicking **Edit**.



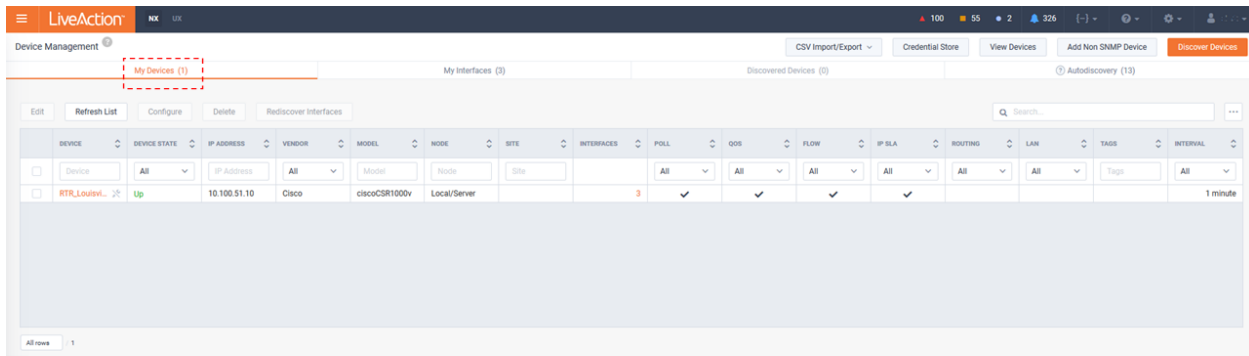
Once Finished, click **+Add Selected**.



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



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



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

The screenshot shows the 'Device Management' section of the LiveAction dashboard. At the top, there are two tabs: 'My Devices (1)' and 'My Interfaces (3)'. Below the tabs is a toolbar with buttons for 'Edit', 'Refresh List', 'Configure', 'Delete', and 'Rediscover Interfaces'. The 'Edit' button is highlighted with a red dashed box. Below the toolbar is a table with columns: DEVICE, DEVICE STATE, IP ADDRESS, VENDOR, MODEL, NODE, and SITE. The first row of data shows a device named 'RTR_Louisvi...' with a state of 'Up', IP address '10.100.51.10', vendor 'Cisco', model 'ciscoCSR1000v', and node 'Local/Server'. At the bottom left, there is a pagination control showing 'All rows / 1'.

This is the configuration form for editing the device 'RTR_LOUISVILLE'. It includes the following fields and options:

- Site:** Louisville
- Group:** No Group Selected
- Interval:** 1 Minute
- IP Address*:** 10.100.51.10
- Checkboxes:** POLL (checked), IP SLA (checked), QOS (checked), ROUTING (unchecked), FLOW (checked), LAN (unchecked)
- Associate Probe at IP Address:** Type IP Address
- Hardcode Sample Ratio:** 1/
- Tags:** (empty text area)
- Buttons:** Cancel, Apply

Note the check boxes associated with the SNMP monitored devices.

This is the same configuration form as above, but with a red dashed box highlighting the row of checkboxes: POLL, IP SLA, QOS, ROUTING, FLOW, and LAN. All checkboxes in this row are checked.

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.

The screenshot shows the LiveAction NX UX interface for Device Management. At the top, there are tabs for 'My Devices (1)' and 'My Interfaces (3)'. Below the tabs, there are several action buttons: 'Edit', 'Refresh List' (highlighted with a red dashed box), 'Configure', 'Delete', and 'Rediscover Interfaces'. Below the buttons is a table with the following columns: DEVICE, DEVICE STATE, IP ADDRESS, VENDOR, MODEL, NODE, and SITE. The table contains one row of data:

DEVICE	DEVICE STATE	IP ADDRESS	VENDOR	MODEL	NODE	SITE
<input checked="" type="checkbox"/> RTR_Louisvi...	Up	10.100.51.10	Cisco	ciscoCSR1000v	Local/Server	

At the bottom left of the table, there is a pagination control showing 'All rows / 1'.

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

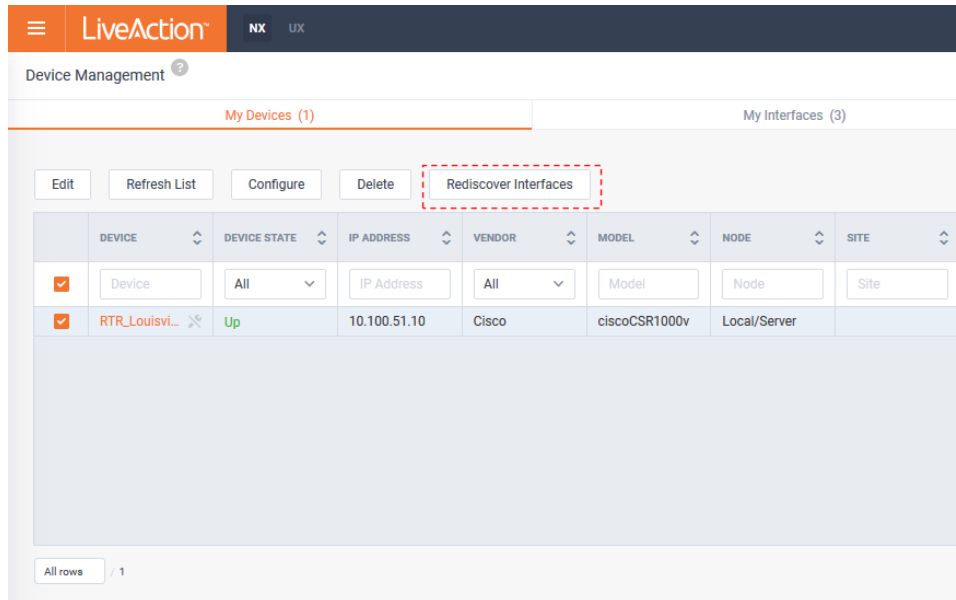
The screenshot shows the LiveAction Device Management interface. At the top, there is a navigation bar with the LiveAction logo and 'NX UX' tabs. Below this, the 'Device Management' section is active, showing 'My Devices (1)' and 'My Interfaces (3)'. A toolbar contains buttons for 'Edit', 'Refresh List', 'Configure', 'Delete', and 'Rediscover Interfaces'. The 'Configure' button is highlighted with a red dashed box. Below the toolbar is a table with columns: DEVICE, DEVICE STATE, IP ADDRESS, VENDOR, MODEL, NODE, and SITE. The table contains one row for a device named 'RTR_Louisvi...' with IP address '10.100.51.10', Vendor 'Cisco', Model 'ciscoCSR1000v', and Node 'Local/Server'. The device state is 'Up'. At the bottom left, there is a pagination control showing 'All rows / 1'.

The screenshot shows a 'CONFIGURE RTR_LOUISVILLE' dialog box. It has a close button (X) in the top right corner. Under the heading 'SNMP Credentials', there are two radio buttons: 'Choose profile from store' (unselected) and 'Enter SNMP connection settings for this device' (selected). Below the selected option, there are three input fields: 'SNMP Version *' (set to 'Version 2c'), 'Target Port *' (set to '161'), and 'Community String *' (set to 'liveaction'). At the bottom right, there are 'Cancel' and 'Save' buttons.

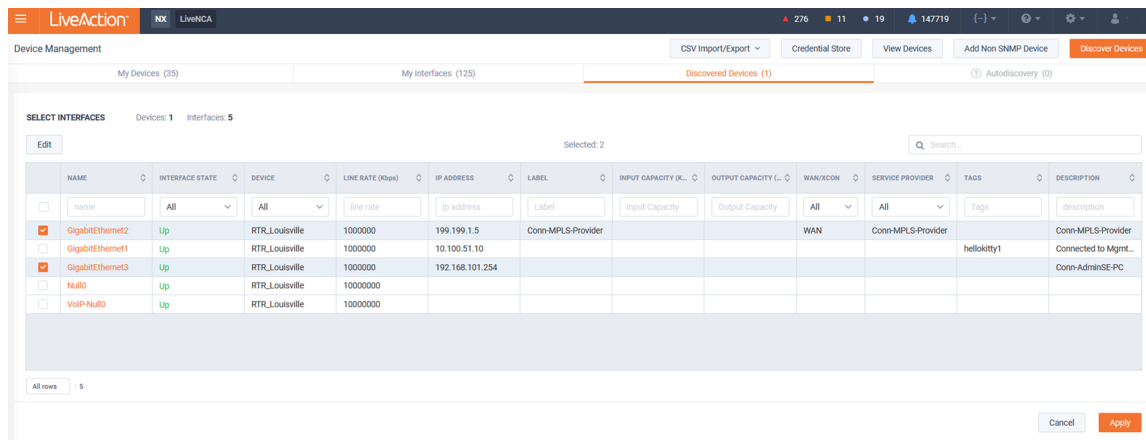
The **Delete** button will remove a selected device(s) from the LiveNX inventory.

This screenshot is identical to the first one, showing the LiveAction Device Management interface. However, in this view, the 'Delete' button in the toolbar is highlighted with a red dashed box, indicating the action to be performed on the selected device.

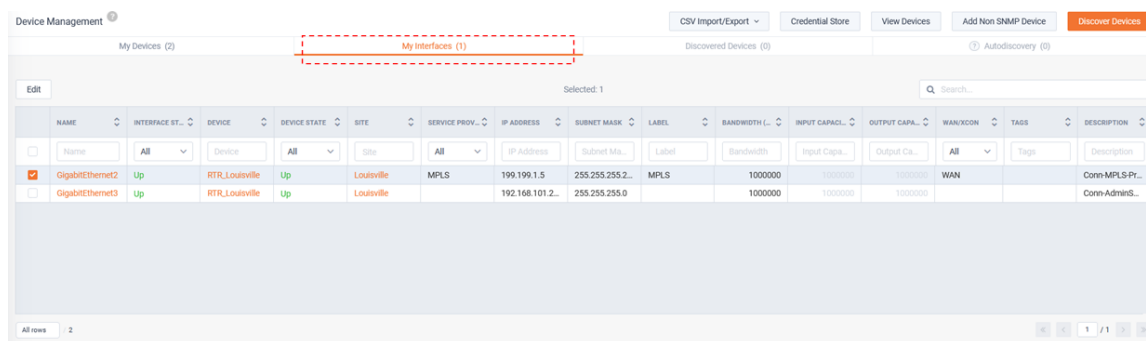
Clicking **Rediscover Interfaces** causes LiveNX to rescan all available Interfaces for the selected device(s). This is like the process that was done on initial device discovery and will allow for the selection or removal of monitored Interfaces.



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**.



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



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

Device Management

My Devices (2) | My Interfaces (1) | Discovered Devices (0) | Autodiscovery (0)

Selected: 1

NAME	INTERFACE ST...	DEVICE	DEVICE STATE	SITE	SERVICE PROV...	IP ADDRESS	SUBNET MASK	LABEL	BANDWIDTH (...)	INPUT CAPAC...	OUTPUT CAPA...	WAN/XCON	TAGS	DESCRIPTION
GigabitEthernet2	Up	RTR_Louisville	Up	Louisville	MPLS	199.199.1.5	255.255.255.2...	MPLS	1000000	1000000	1000000	WAN		Conn-MPLS-Pr...
GigabitEthernet3	Up	RTR_Louisville	Up	Louisville		192.168.101.2...	255.255.255.0		1000000	1000000	1000000			Conn-AdminS...

All rows 2

EDIT GIGABITETHERNET2

IP Address: 199.199.1.5

Subnet Mask: 255.255.255.252

Service Provider: MPLS

Input Capacity: 1000000 Kbps
Value is inherited by bandwidth until set

Output Capacity: 1000000 Kbps
Value is inherited by bandwidth until set

Label: MPLS

Tags: [Empty]

WAN/XCon: WAN

Buttons: Cancel, Apply

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.

LiveAction

Device Management

My Devices (1) | My Interfaces (3) | Discovered Devices (1) | Autodiscovery (13)

Node: Local/Server (13 devices)

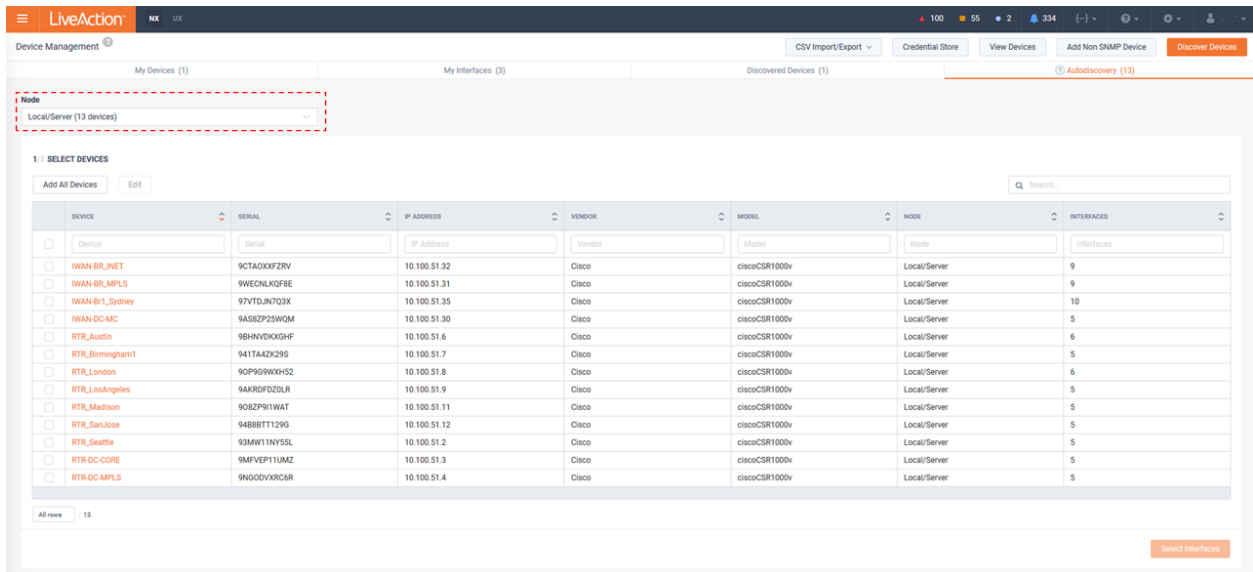
1: SELECT DEVICES

DEVICE	SERIAL	IP ADDRESS	VENDOR	MODEL	NODE	INTERFACES
IWAN_BR_INET	9CTA0XKFZRV	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	9ASZP25WQM	10.100.51.30	Cisco	ciscoCSR1000v	Local/Server	5
RTR_Austin	9BHNVDKXGHF	10.100.51.6	Cisco	ciscoCSR1000v	Local/Server	6
RTR_Birmingham1	941TA4ZK9S	10.100.51.7	Cisco	ciscoCSR1000v	Local/Server	5
RTR_London	90P96W9W52	10.100.51.8	Cisco	ciscoCSR1000v	Local/Server	6
RTR_LosAngeles	9AKRGFDZLR	10.100.51.9	Cisco	ciscoCSR1000v	Local/Server	5
RTR_Madison	90BZP9I1WAT	10.100.51.11	Cisco	ciscoCSR1000v	Local/Server	5
RTR_SanJose	948B8TT129G	10.100.51.12	Cisco	ciscoCSR1000v	Local/Server	5
RTR_Seattle	93MW11NY5SL	10.100.51.2	Cisco	ciscoCSR1000v	Local/Server	5
RTR-DC-CORE	9MFPVP11UMZ	10.100.51.3	Cisco	ciscoCSR1000v	Local/Server	5
RTR-DC-MPLS	9NGODVXRC6R	10.100.51.4	Cisco	ciscoCSR1000v	Local/Server	5

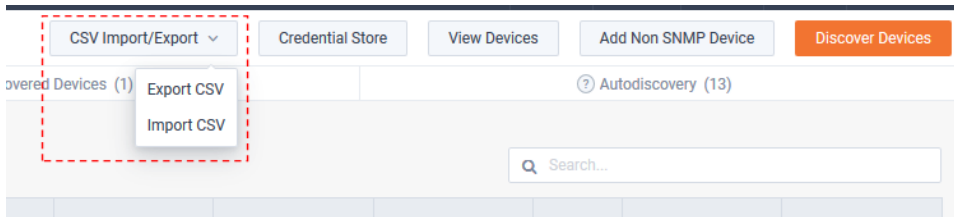
All rows 13

Select Interfaces

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.

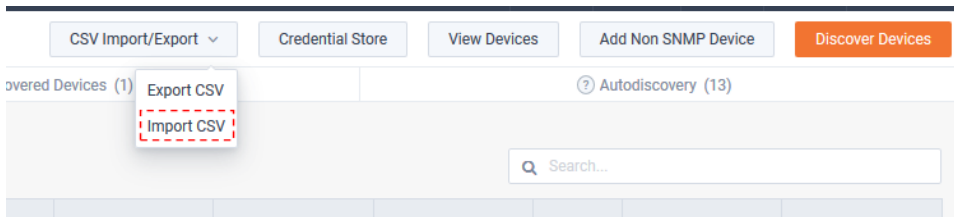


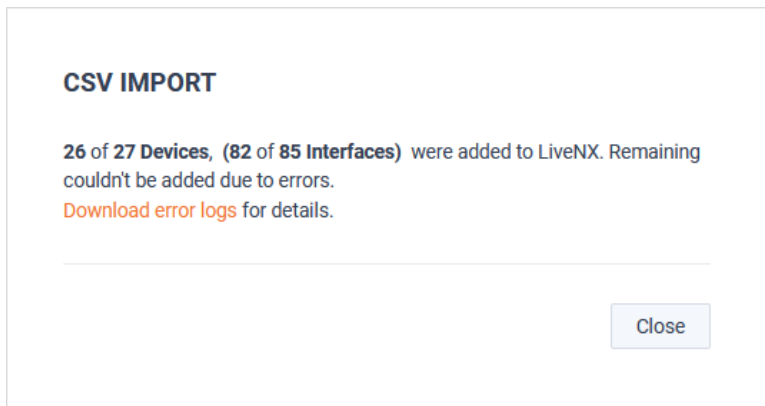
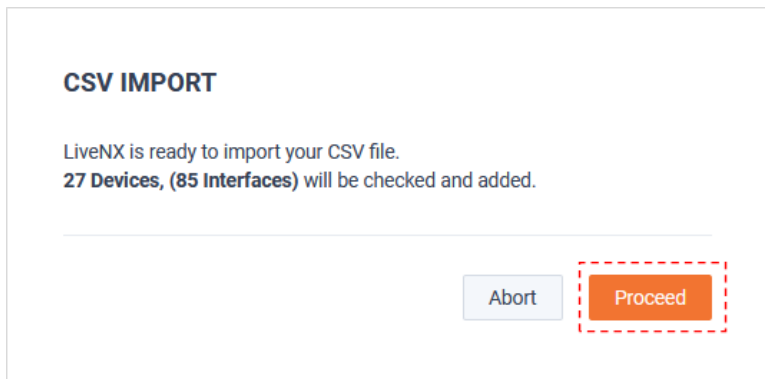
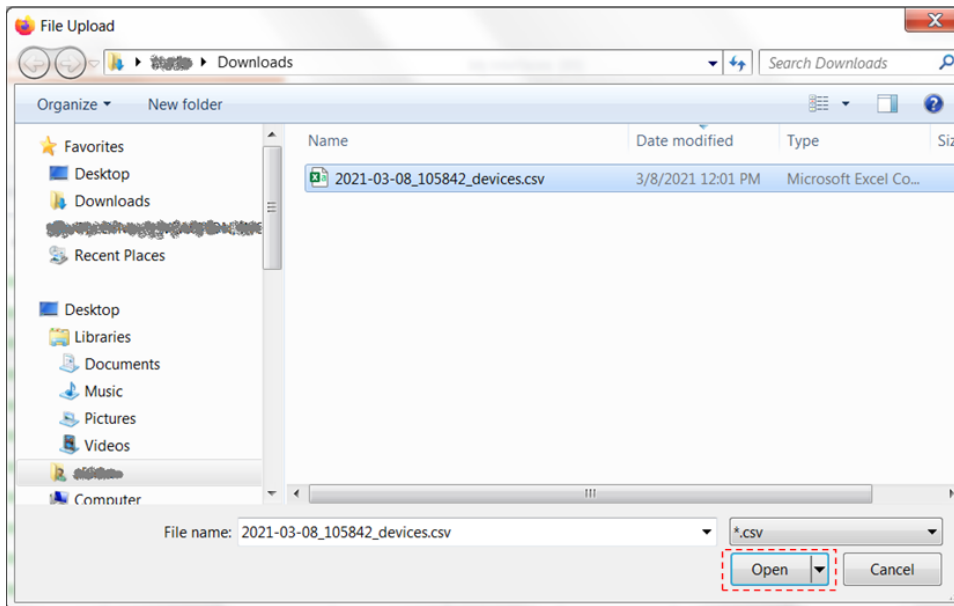
CSV Import/ Export provides another method to bulk add and edit the device and interface inventory via CSV.



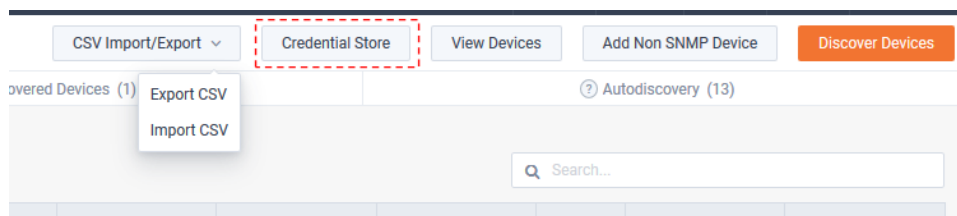
	A	B	C	D	E	F	G	H	
1	ADD/UPDATE	NAME	TYPE	DEVICE SERIAL	IP ADDRESS	VENDOR	MODEL	IOS VERSION	DESCRIPTION
2	TRUE	RTR_Louisville	Router	9E3XJK8MTIX	10.100.51.10	Cisco	ciscoCSR1000v	16.3.7	Cisco IOS Software [Denali], CSR1000v
3	TRUE	GigabitEthernet1	Interface		10.100.51.10				Connected to MgmtNtw
4	TRUE	GigabitEthernet2	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									

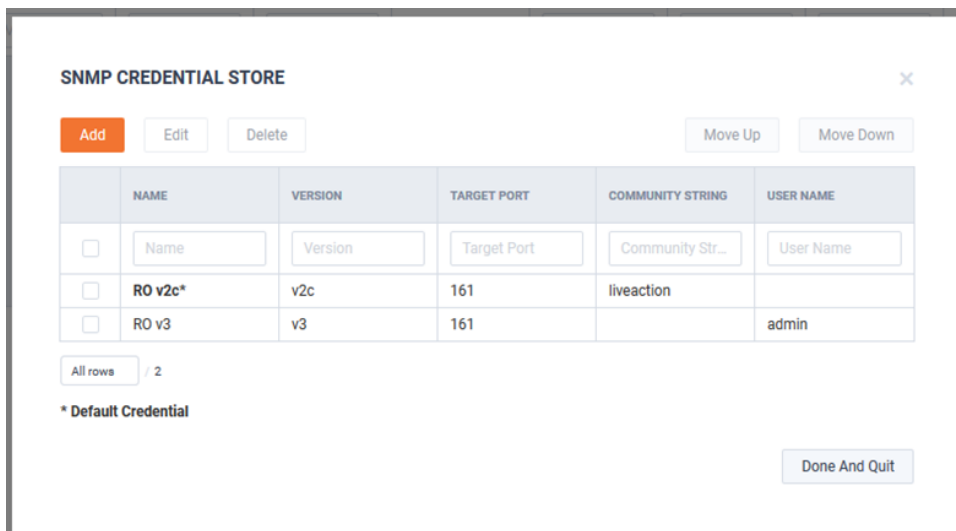
Import CSV will add new devices/interfaces and overwrite any exiting configuration with the data of the CSV.





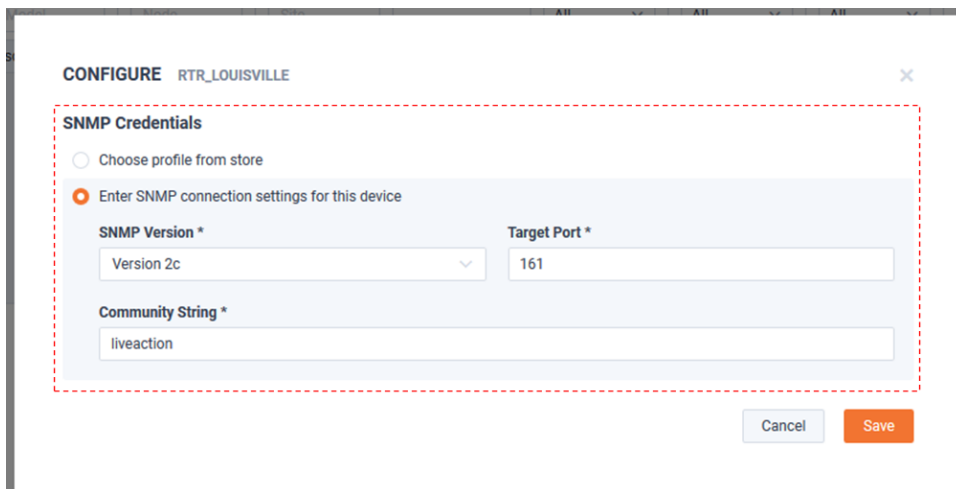
The SNMP Credential Store and format is provided to assist networks that may have multiple SNMP credentials in use within the infrastructure. When discovering new devices using the *Credential Store*, the discovery engine will use the credentials from the store in the order they are listed.





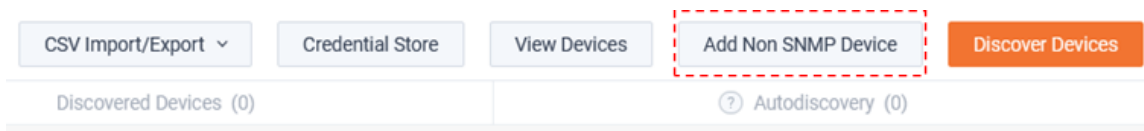
Once a match is made via the discovery process, the specific SNMP credential will be associated with the respective device(s) until SNMP is reconfigured.

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.



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**.



ADD NON SNMP DEVICE

1 General Settings 2 Add Interface

Device Name* IP Address* Site Name Group Node*

Tags Description

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**.

ADD NON SNMP DEVICE

1 General Settings 2 Add Interface

Device Name* IP Address* Site Name Group Node*


Tags Description

The *Add Interface* view appears. Click **Add**.

ADD NON SNMP DEVICE

General Settings 2 Add Interface

Device Name: MyRouter Device IP Address: 10.100.51.11


 No Interfaces defined
 Please add an interface

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

Ifindex* Interface Name* IP Address Subnet Mask Label

Input Capacity kbps Output Capacity kbps Service Provider Tags WAN/XCon

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

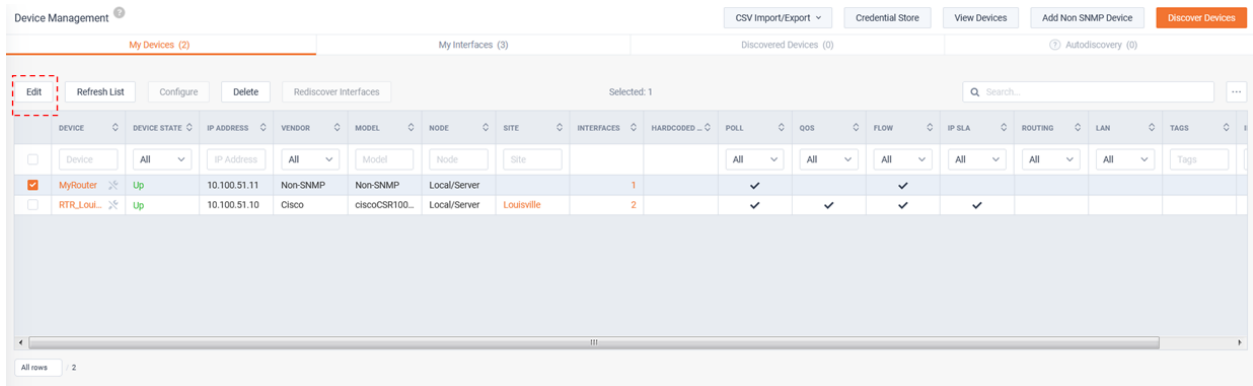
The *Add Non SNMP Device* dialog appears. Click **Add to My Devices**.

IFINDEX	NAME	IP ADDRESS	SUBNET MASK	LABEL	WAN/XCON	INPUT CAPAC...	OUTPUT CAPAC...	SERVICE PROVL...	TAGS
1	MyInt1				All	Input Capac...	Output Cap...	Service Prov...	Tags

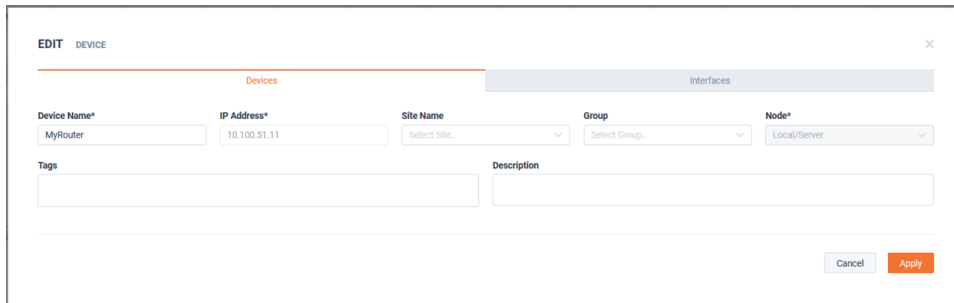
The Non-SNMP device appears under *My Devices*.

DEVICE	DEVICE STATE	IP ADDRESS	VENDOR	MODEL	NODE	SITE	INTERFACES	HARDCODED...	POLL	QOS	FLOW	IP SLA	ROUTING	LAN	TAGS
MyRouter	Up	10.100.51.11	Non-SNMP	Non-SNMP	Local/Server		1		✓	✓	✓	✓			
RTR_Lou...	Up	10.100.51.10	Cisco	ciscoCSR100...	Local/Server	Louisville	2		✓	✓	✓	✓			

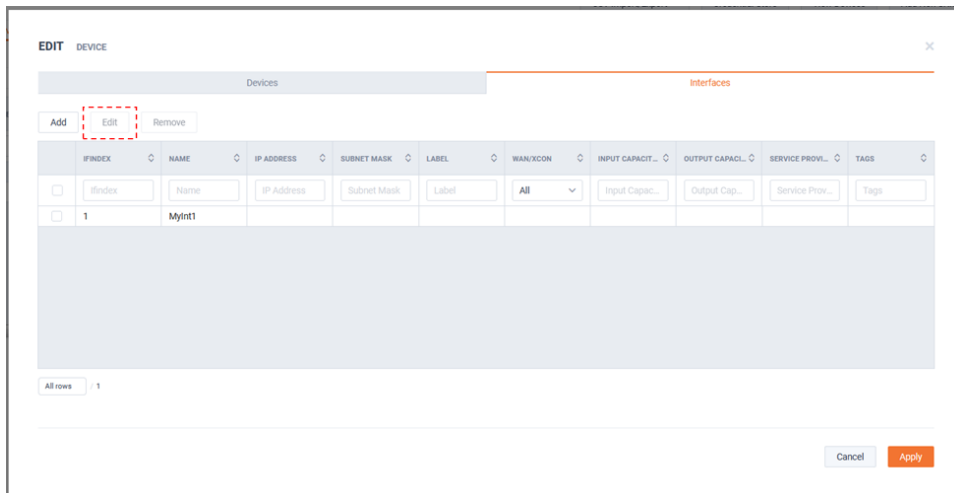
To Edit a Non-SNMP device, select the device and click **Edit**.



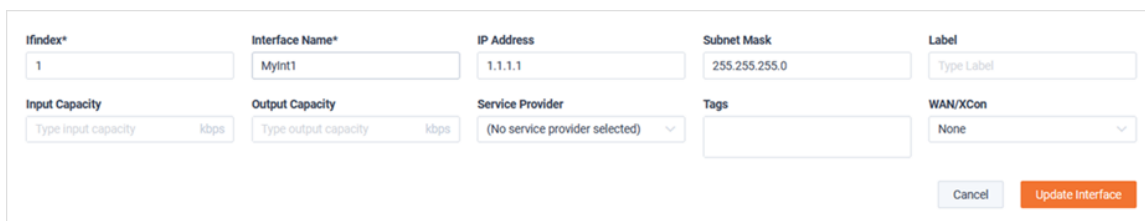
The *Edit Device* modal appears. Since this is a Non-SNMP device, note the *Interfaces* tab.



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



After making any desired changes, click **Update Interface**.



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

EDIT DEVICE

Devices | Interfaces

Add Edit Remove

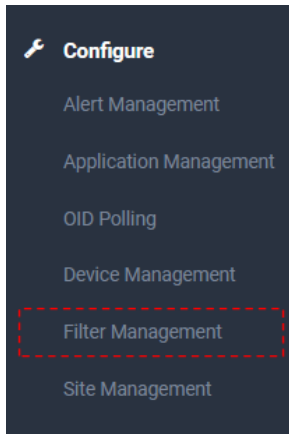
INDEX	NAME	IP ADDRESS	SUBNET MASK	LABEL	WAN/CON	INPUT CAPACIT...	OUTPUT CAPACL...	SERVICE PROVL...	TAGS
1	MyInt1				All	Input Capac...	Output Cap...	Service Prov...	Tags

All rows 1

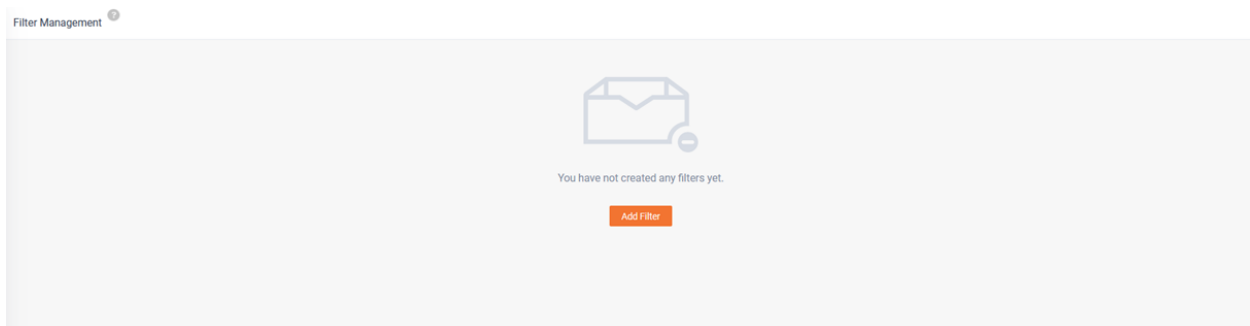
Cancel Apply

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**.



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

ADD FILTER ✕

Name
MyFilter

Description
This is MyFilter

Details
Application: VoIP DSCP: EF Enter Filter Request Here

Sharing
 Off

Cancel Save

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

Filter Management ¹

Add Edit Copy Delete Search...

FILTER NAME	PUBLIC	CREATED BY	DESCRIPTION
<input type="checkbox"/> Filter Name	All	All	Description
<input checked="" type="checkbox"/> MyFilter			This is MyFilter

All rows 1

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

Filter Management ¹

Add Edit Copy Delete Search...

Selected: 1

FILTER NAME	PUBLIC	CREATED BY	DESCRIPTION
<input checked="" type="checkbox"/> Filter Name	All	All	Description
<input checked="" type="checkbox"/> MyFilter			This is MyFilter

All rows 1

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

EDIT FILTER ✕

Name
MyFilter

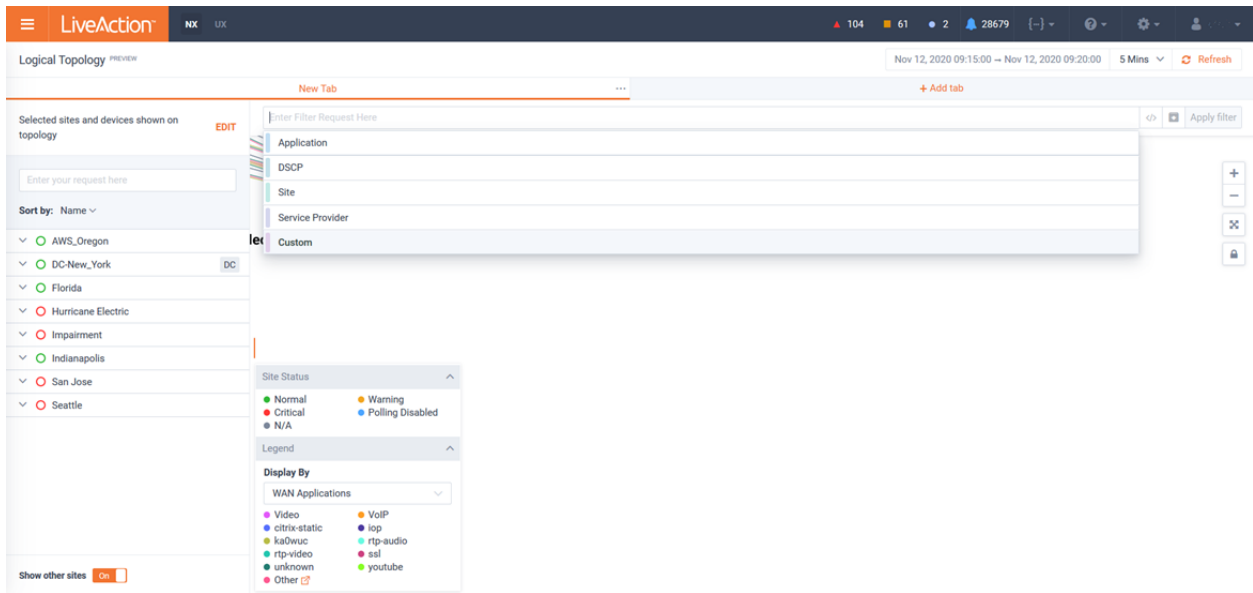
Description
This is MyFilter

Details
Application: VoIP DSCP: EF Enter Filter Request Here

Sharing
 Off

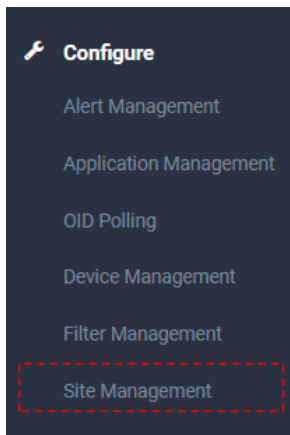
Cancel Save

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



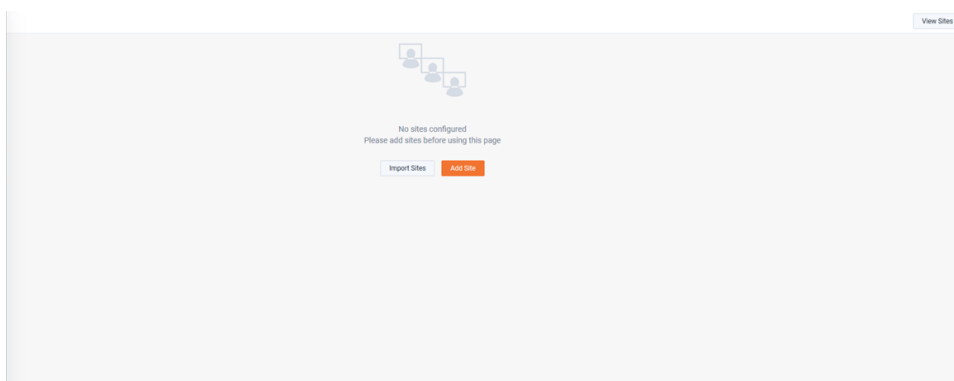
Site Management

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.

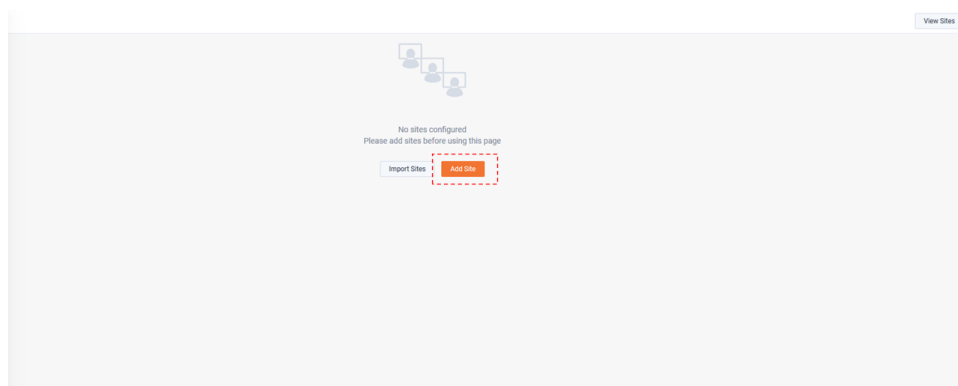


When configuring LiveNX for the first time, no sites are configured. To add a Site, either:

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.

 A screenshot of the 'ADD SITE' modal form. The modal has a title bar with 'ADD SITE' and a close button. Below the title bar are three tabs: 'Details' (selected), 'Address', and 'Business hours'. The form contains the following fields:

- Site Name:** A text input field with the placeholder 'Site name'. A red error message 'Site name is required' is displayed below it.
- Site Description:** A text area with the placeholder 'Enter site description' and a character count '0/1000'.
- Site IP Range (CIDR Notation IP's):** A text input field with the placeholder 'CIDR Notation IP's'.
- Devices:** A text input field.
- Tags:** A text input field.
- Number of Employees:** A text input field with the placeholder 'Number of Employees'.
- Data Center:** A checkbox labeled 'Data Center'.

 At the bottom right of the modal are 'Cancel' and 'Save' buttons.

Site Details

- *Site Description* – a courtesy free-text field.
- *Site IP Range* – 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.

Site Address

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

Once any portion of the Site’s Address, City, State/Province/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.

EDIT 1 SITE < LOUISVILLE >

Details | **Address** | Business hours

Address

Address Line 1: 38.25489

Address Line 2: -85.76666

City: Louisville

State/Province/Region: KY

Zip Code: Zip Code

Country: Country

Latitude & Longitude

38.25489

-85.76666

Phone Number: Phone Number

Email: Email

Region
Continent: North America -> Country: United States -> State: Kentucky -> City: Louisville

Site Business Hours

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

EDIT 1 SITE < LOUISVILLE >

Details | Address | **Business hours**

Days of Week

Su **Mo** **Tu** **We** **Th** **Fr** Sa

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

Start time

08 : 00 AM

End time

05 : 00 PM

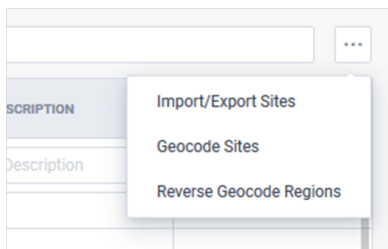
Sites can also be managed in bulk by the menu icon at the top right or the *Site Management* page.

Site Management View Sites

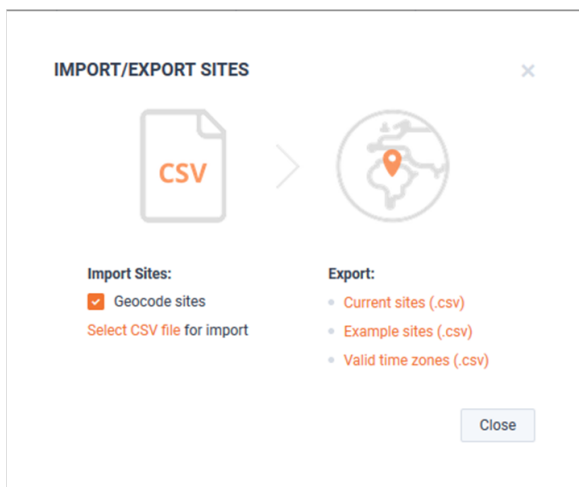
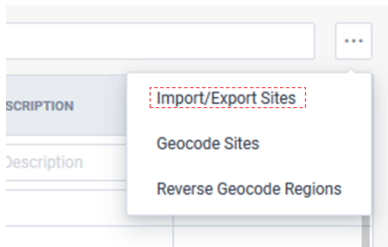
Add Edit Delete Q Search...

SITE	DATA CENTER	DEVICES	CONTAINS DEVICES	NO. OF EMPLOYEES	BUSINESS HOURS	IP RANGES	GEO LOC	ADDRESS	REGION	DESCRIPTION	TAGS
(X)Test	All	Devices	All	No. of Emplo...	Business Hou...	IP Ranges	All	Address	Region	Description	Tags
<TestSite>					Mo - Fr 8:00 am ...					a test site	
Apple					Mo - Fr 8:00 am ...					New description	
AT&T					Mo - Fr 8:00 am ...					New description	
Austin					Mo - Fr 8:00 am ...			Austin, Texas	Austin, Texas, Uni...	New description	
Austria					Mo - Fr 8:00 am ...	192.168.65.2 19...		Austria	Austria, Europe		Europe
Beijing					Mo 8:00 am - 5...	172.50.50.0/24		beijing	Beijing, Beijing, C...		tag1, tag2
Birmingham		RTR_Birmingham...	✓		Mo - Fr 8:00 am ...			Birmingham, AL	Birmingham, Ala...		stuff
Black Hole					Mo - Fr 8:00 am ...	81.1.1.1 10.1.15...					
Branch1					Mo 8:00 am - 5...						tag1, tag2
Branch2					Mo - Fr 8:00 am ...						tag1
Brazil				1000	We - Fr 10:00 a...			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, tag3
BugSite					Mo - Fr 8:00 am ...						tag1, tag3
Chicago					Mo - Fr 8:00 am ...	10.177.1.116 21...		chicago	Chicago, Illinois, ...		
china					Mo - Fr 8:00 am ...			China	China, Asia	tada	

All rows 102



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



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 existing 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 of isDataCen	Site IP Ran	Description	Address 1	Address 2	City	State	Country	Zip Code	Latitude	Longitude	Phone Nur	Email	Days	Time Zone	Start Time	End Time	DST	Tags	City Short	City Long	St	
2	[required]	[numerical]	[true or fa	[comma se	[up to 1000 characters]									[automatic	[automatically generated if left t	[comma se	[see list of	[based off	[based off	[true/false	[comma se	[automatic	[do not in	[a
3	Site 1	25	FALSE	192.168.11.0/24	3500 W Bayshore Rd	Palo Alto	California	United Sta		94303	37.43411	-122.118	+1(888)88	user@live	monday,tu	US/Mount	8:00	17:00	TRUE	siteTag1,	siteTag2,	siteTag3		

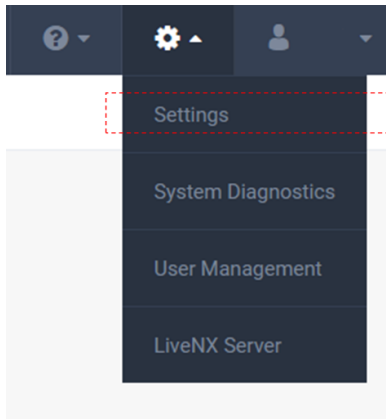
Settings

In this chapter:

<i>Settings</i>	59
<i>System Diagnostics</i>	102
<i>Flow Data Status</i>	104
<i>User Management</i>	104
<i>LiveNX Server</i>	123

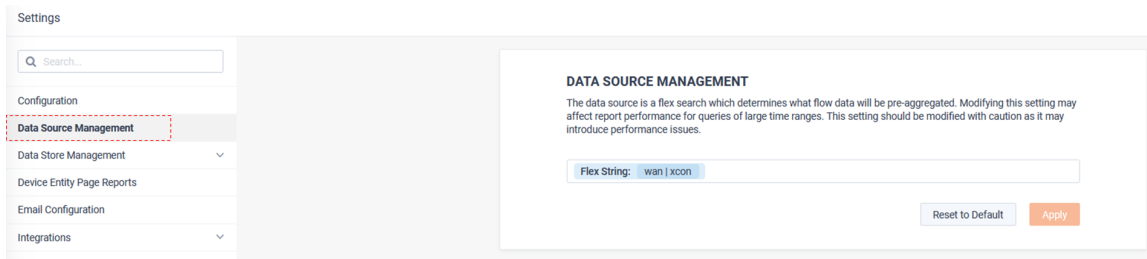
Settings

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.

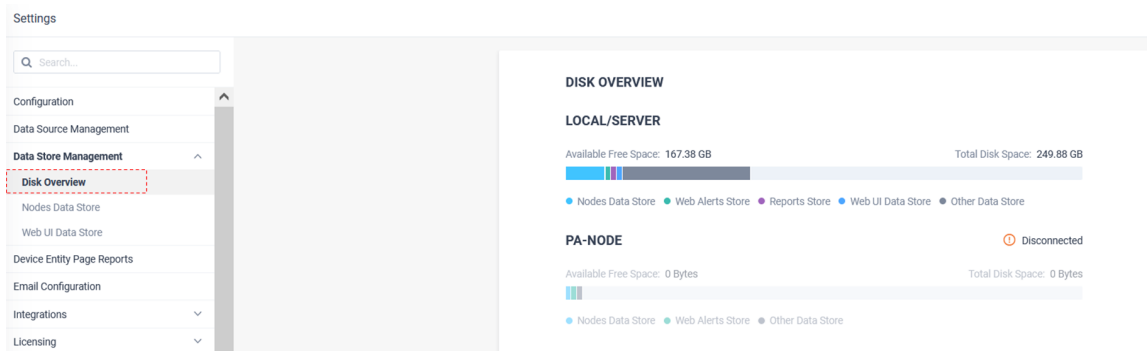


Data Store Management

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

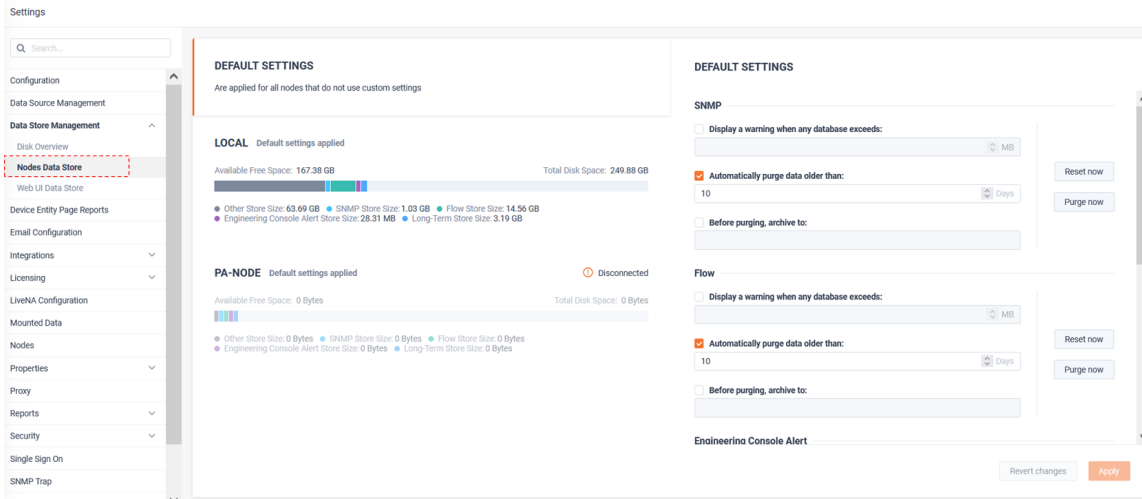
Disk Overview

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



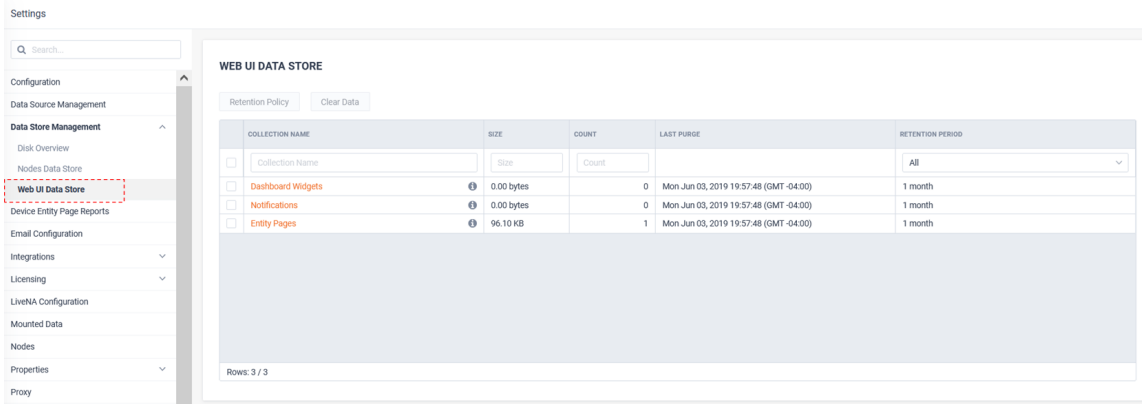
Nodes Data Store

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.



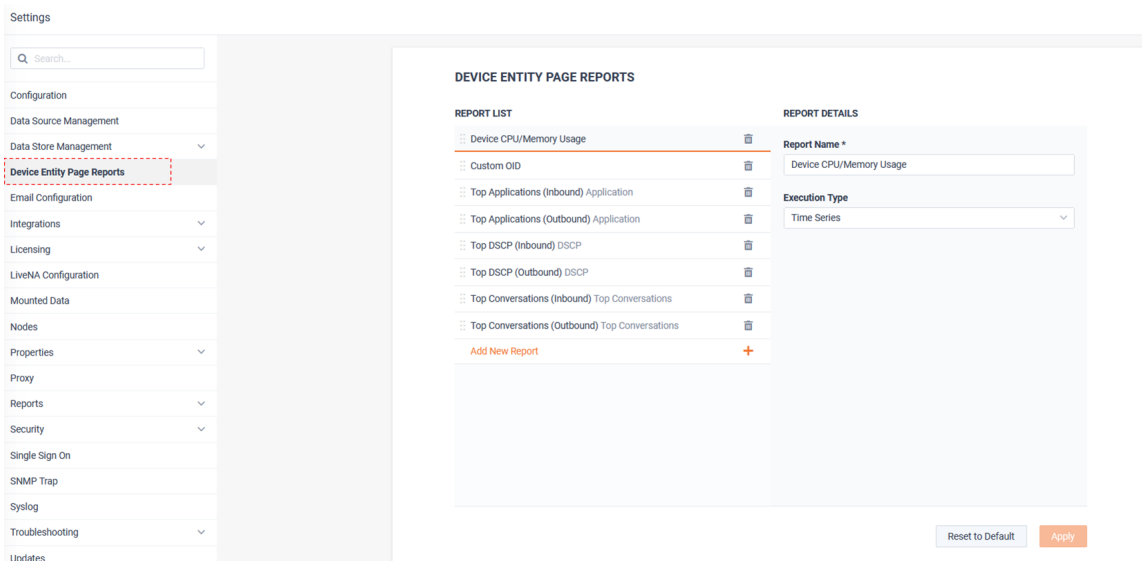
Web UI Data Store

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).



Device Entity Page Reports

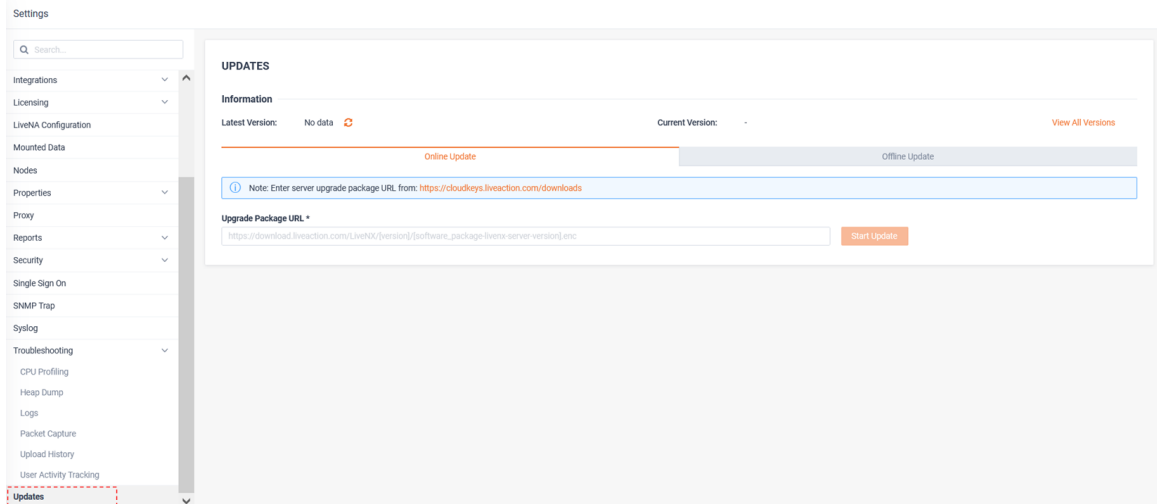
Device Entity Page Reports allows customization of the reports shown on the Device Page.



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

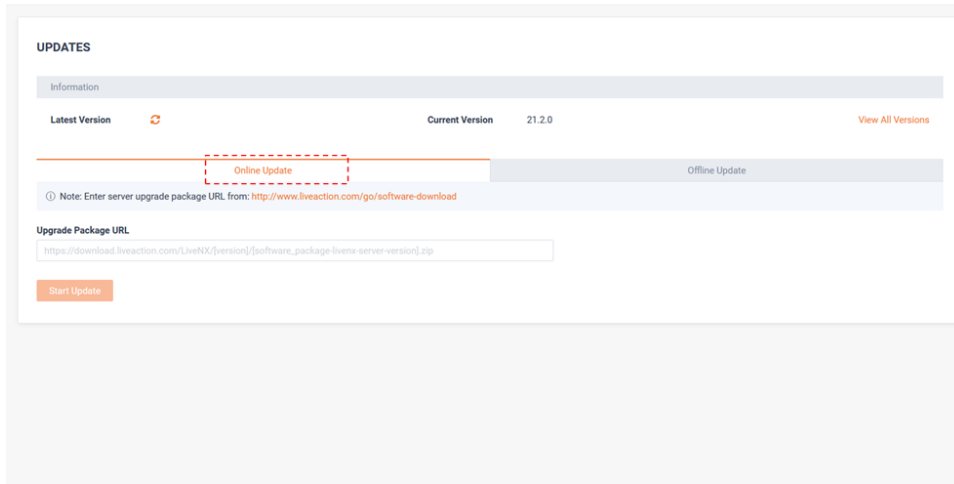


Updates allow you to manage system updates.

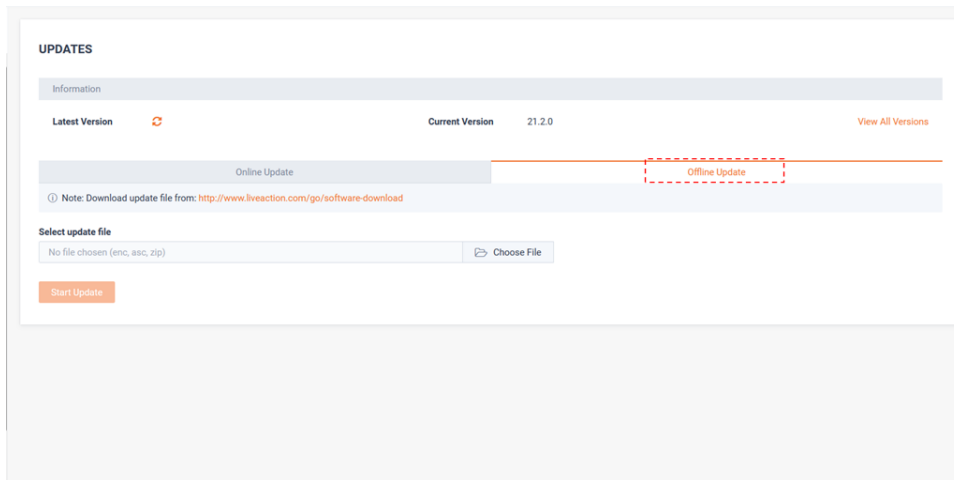


From the *Online Update* tab, enter the full URL of the update package and click **Start Update**.

LiveNX will download the upgrade package from the [liveaction.com](https://cloudkeys.liveaction.com/downloads) website, install it, and reboot the system.

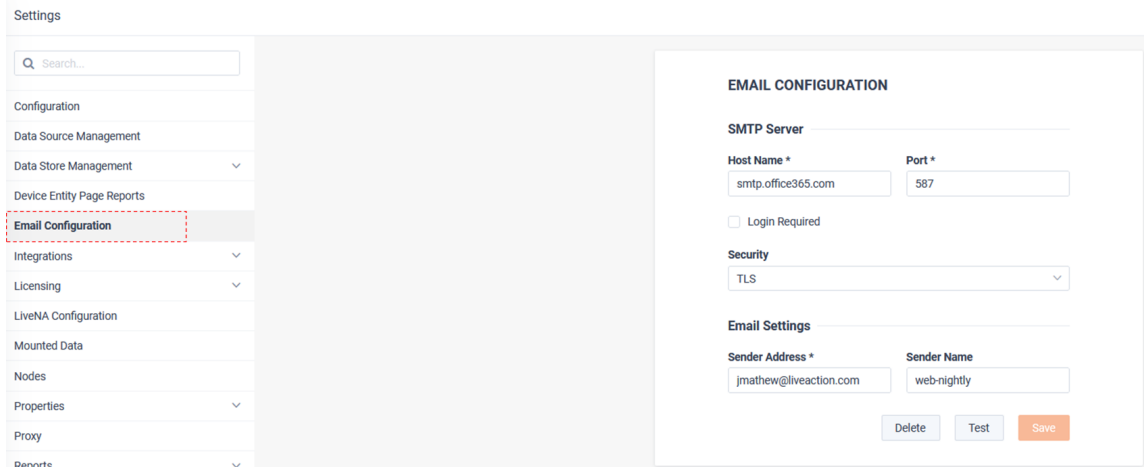


If required, the *Offline Update* tab allows for manual upload of the upgrade packet to the LiveNX server.



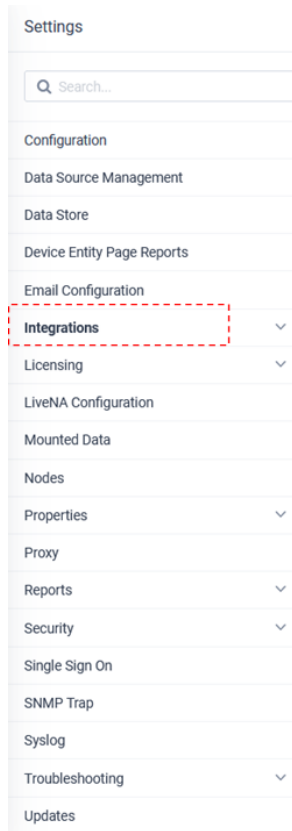
Email Configuration

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*.

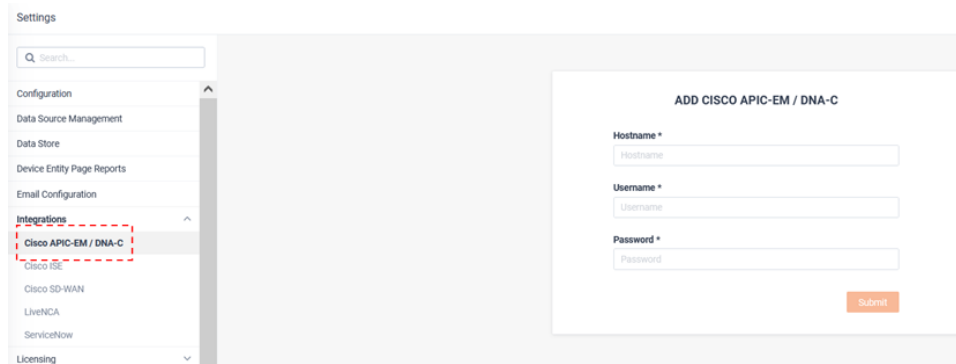


Cisco APIC-EM/DNA-C

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

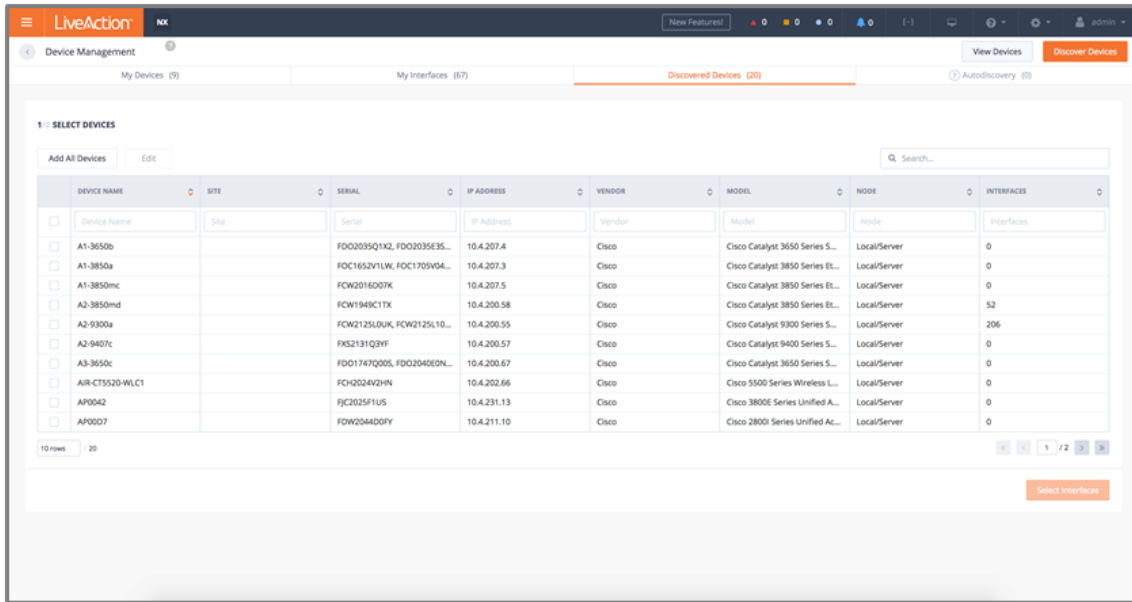
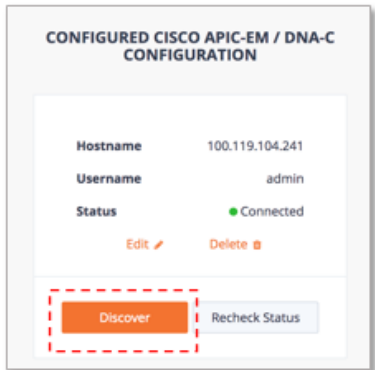
From the Cisco APIC-EM/ DNA-C tab, enter the *Hostname*, *Username* and *Password* and click **Submit**.



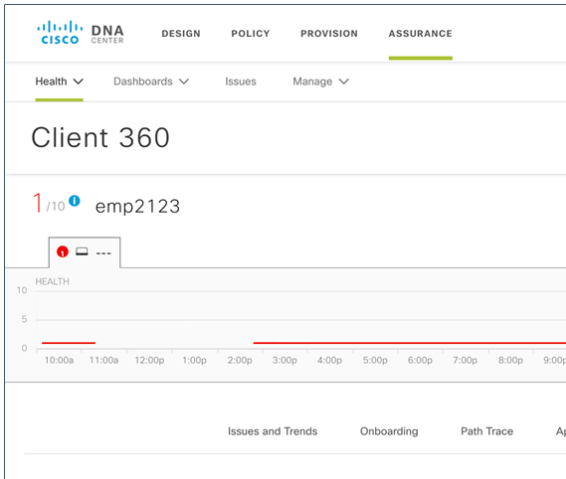
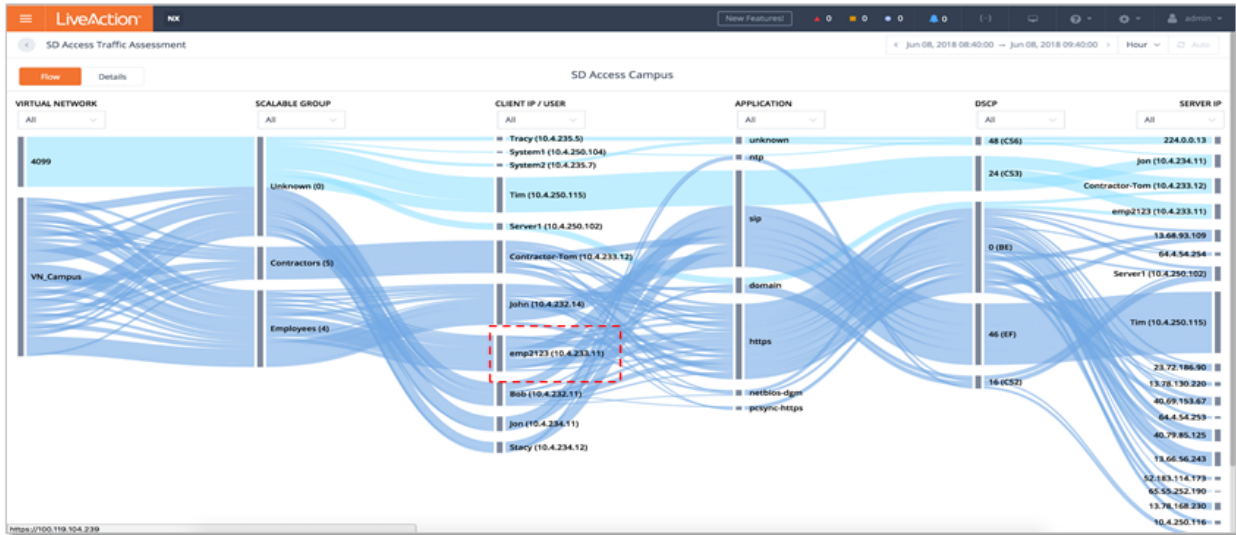
Once connected to APIC-EM/ DNA-C, the integration status will show as *Connected*.



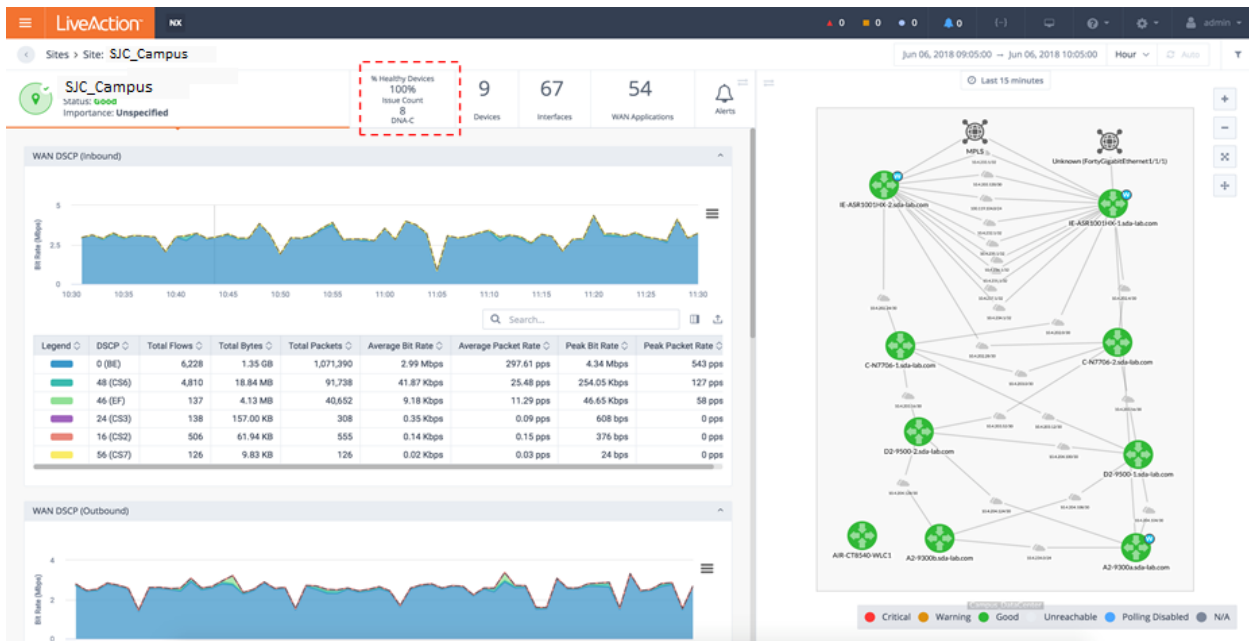
If desired, use the **Discover** button for LiveNX to import APIC-EM/ DNA-C's inventory for device discovery.



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.



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



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

SJC_Campus
 Status: Good
 Importance: Unspecified

% Healthy Devices: 100%
 Issue Count: 8
 DNA-C

9 Devices | 67 Interfaces | 54 WAN Applications

DEVICE	GROUP	DEVICE STA...	CPU AVERAGE	MEMORY A...	INTERFACE ...	CONGESTIO...	DESCRIPTION	HEALTH SCORE	ISSUE
A2-9300a	-	All	2%	38%	0 errors	●	Cisco IOS So...	-	-
A2-9300b	-	All	2%	36%	0 errors	●	Cisco IOS So...	-	0
AIR-CT8540...	-	All	-	-	0 errors	●	-	10	0
C-N7706-1	-	All	11%	18%	0 errors	●	Cisco NX-OS...	-	-
C-N7706-2	-	All	11%	18%	0 errors	●	Cisco NX-OS...	-	-
D2-9500-1	-	All	1%	34%	0 errors	●	-	-	0
D2-9500-2	-	All	1%	34%	0 errors	●	-	-	0
IE-ASR1001...	-	All	1%	7%	0 errors	●	-	-	4
IE-ASR1001...	-	All	1%	7%	0 errors	●	Cisco IOS So...	10	4

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

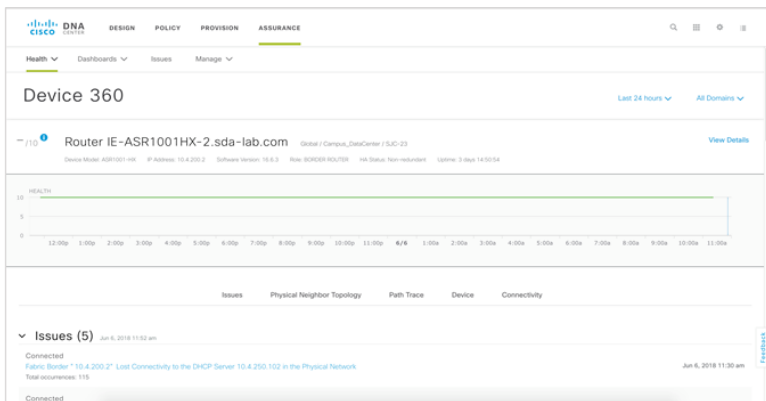
IE-ASR1001HX-1
 Status: Good
 IP Address: 10.4.200.1

100% Availability | 5 Interfaces | 21 WAN Application | 0 Active Alerts

DNA-C Health Score: 3 Issue Count: 0

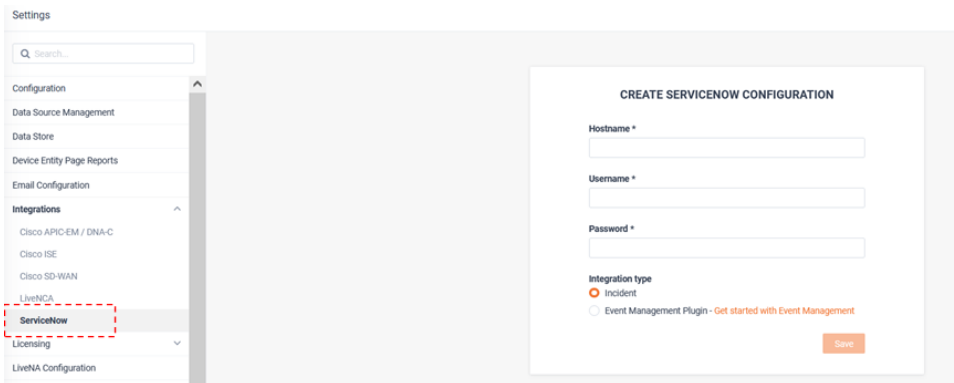
Device CPU/Memory Usage

Legend	Name	Avg	Peak
CPU Usage	C	1%	2%
Memory Usage	M	6%	6%

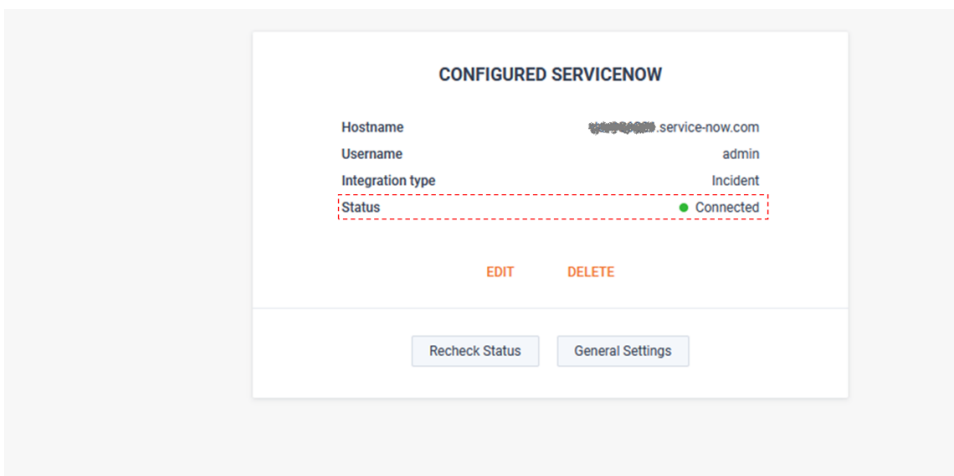


ServiceNow

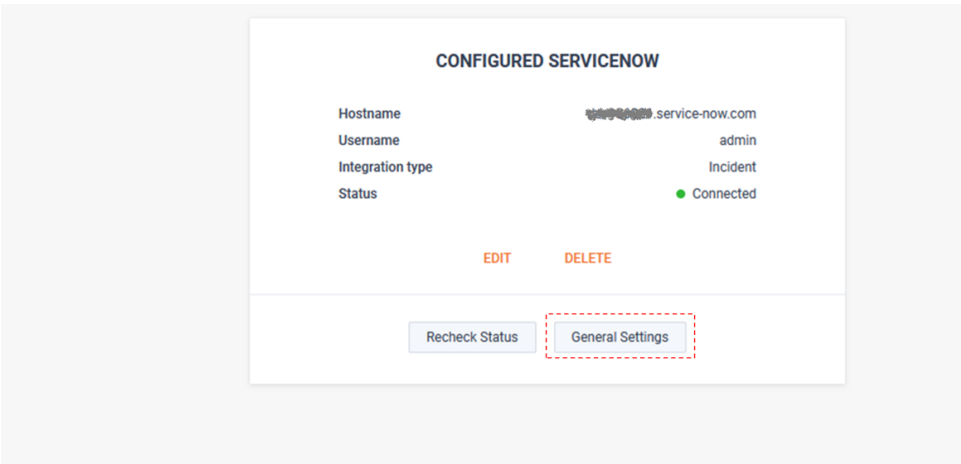
LiveNX can integrate with ServiceNow for forwarding its Alerts as either Incidents or Events. From the ServiceNow tab, enter the Hostname, Username, Password, and choose the Integration type.



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

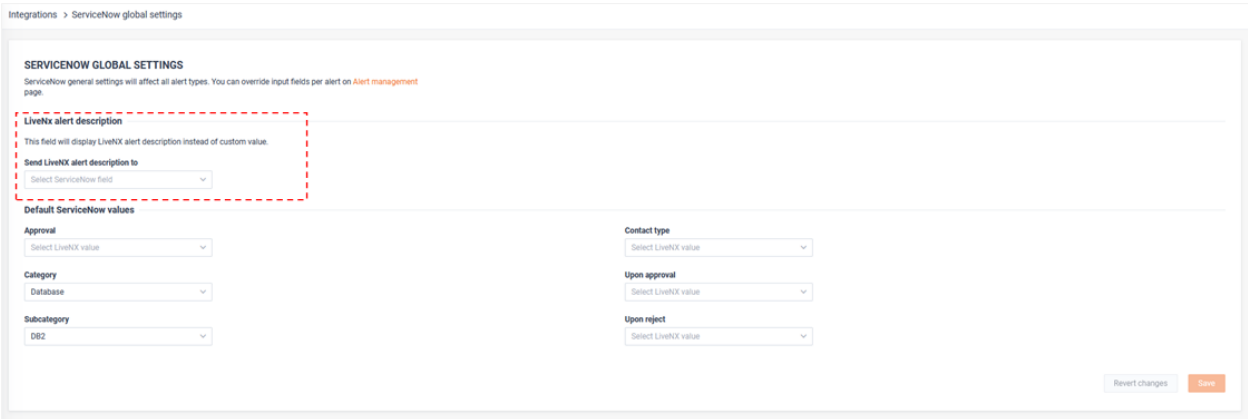


Each ServiceNow implementation can be highly customized. To ensure LiveNX can deliver its alerts in the best possible format, many settings can be defined on either a global or per alert basis. Global ServiceNow settings will be applied to all alerts that are forwarded by LiveNX to ServiceNow. Per-alert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



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

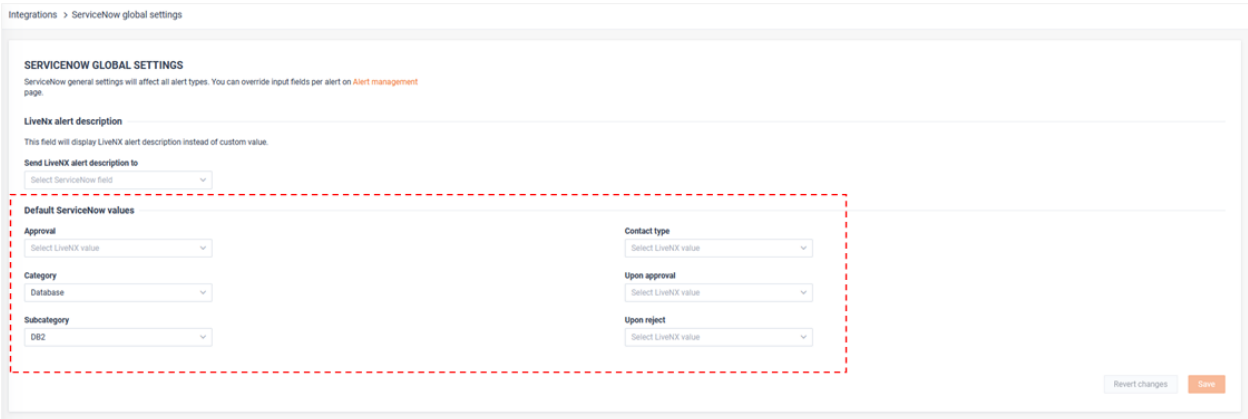
LiveNX will poll ServiceNow, learn the potential options, and provide a picker to choose the field that best serves the implementation.



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 ServiceNow values. These could be different in each network, so more or fewer options may be presented.



ServiceNow Per-alert settings can be adjusted with each alert's Sharing configuration.

Sharing

Email

test@test.com x
Type email

ServiceNow ^

Default ServiceNow settings set on [Global settings](#) page. You can override individual settings below.

Category
Database

Subcategory
DB2

Add value to override
Select override value from the list

SNMP trap

Web UI

Syslog

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

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

ADD LIVENCA

Hostname *

Connect

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

EDIT LIVENCA

Hostname *

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

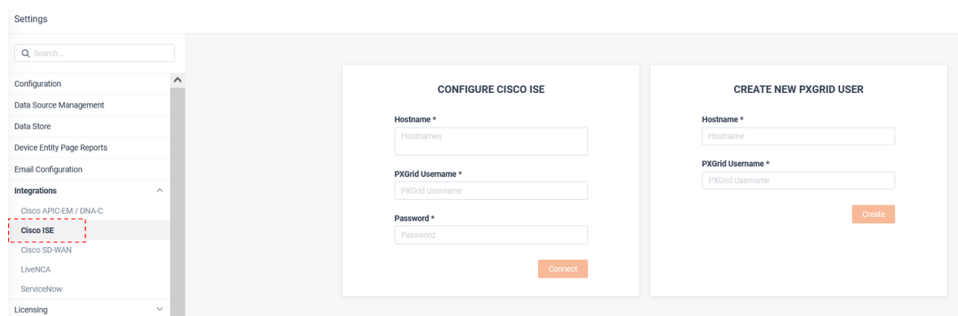


Click **LiveNCA** to open the LiveNCA login page in a new browser tab.



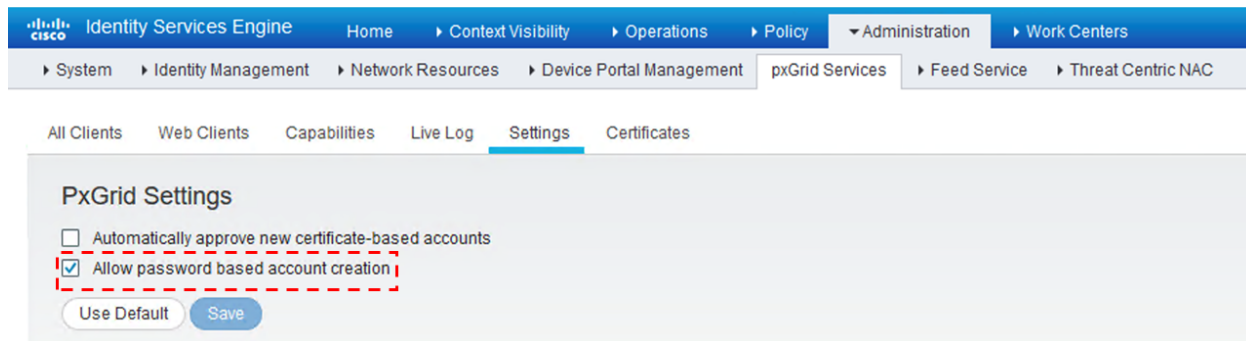
Cisco ISE

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.

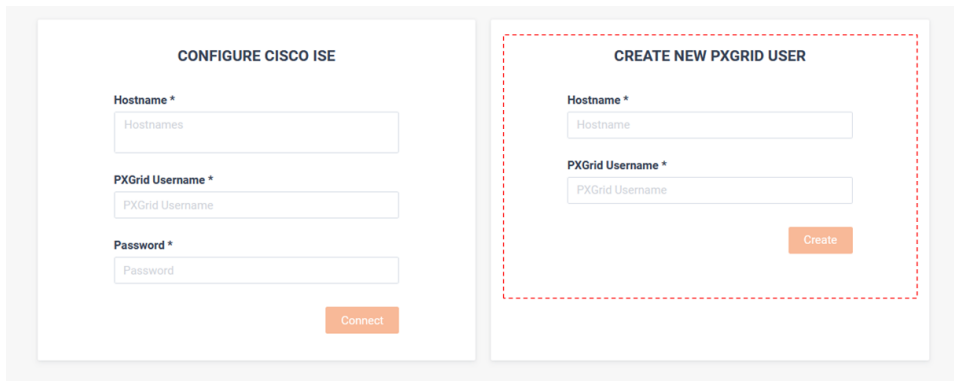


Cisco ISE and PXGRID must be configured to support this integration.

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

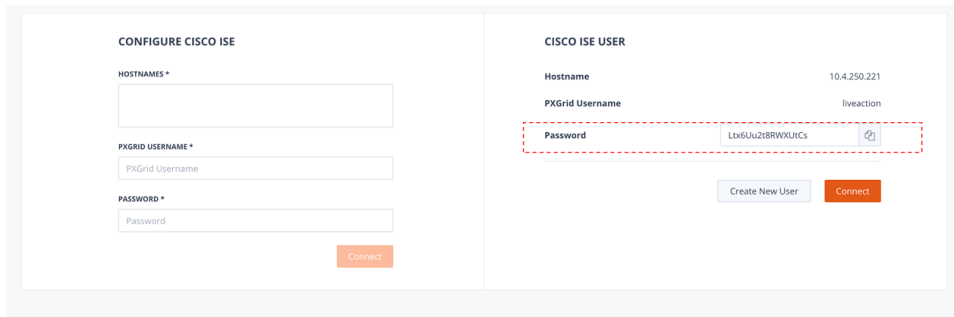


From the *Cisco ISE* tab, configure the ISE IP address or hostname and enter a pxGrid username. When finished, click **Create** (LiveNX will utilize pxGrid northbound API's to create the new user account).



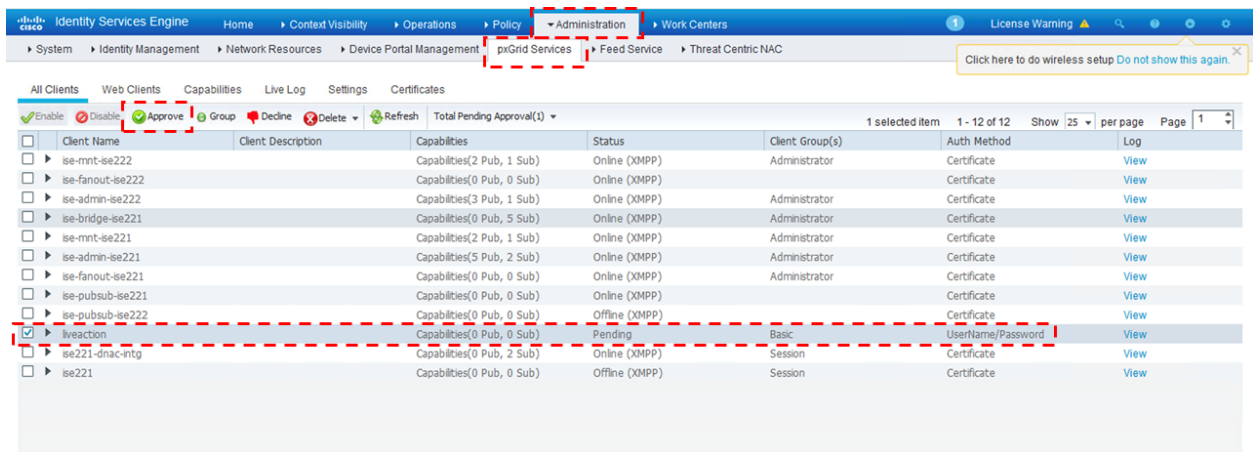
Once the ISE user is created successfully, the auto generated password is displayed.

- 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.



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

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



Validate the new user is *Online*.

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
liveaction		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.

CONFIGURE CISCO ISE

HOSTNAMES *

PXGRID USERNAME *

PASSWORD *

Connect

CISCO ISE USER

Hostname: 10.4.250.221

PXGrid Username: liveaction

Password: Ltx6UuZt8RWXUICs

The Cisco ISE status displays as *Connected*.

CONFIGURED CISCO ISE

Hostname: 10.4.250.221

PXGrid Username: liveaction

Status: ● Connected

[Edit](#) [Delete](#)

CREATE NEW CISCO ISE USER

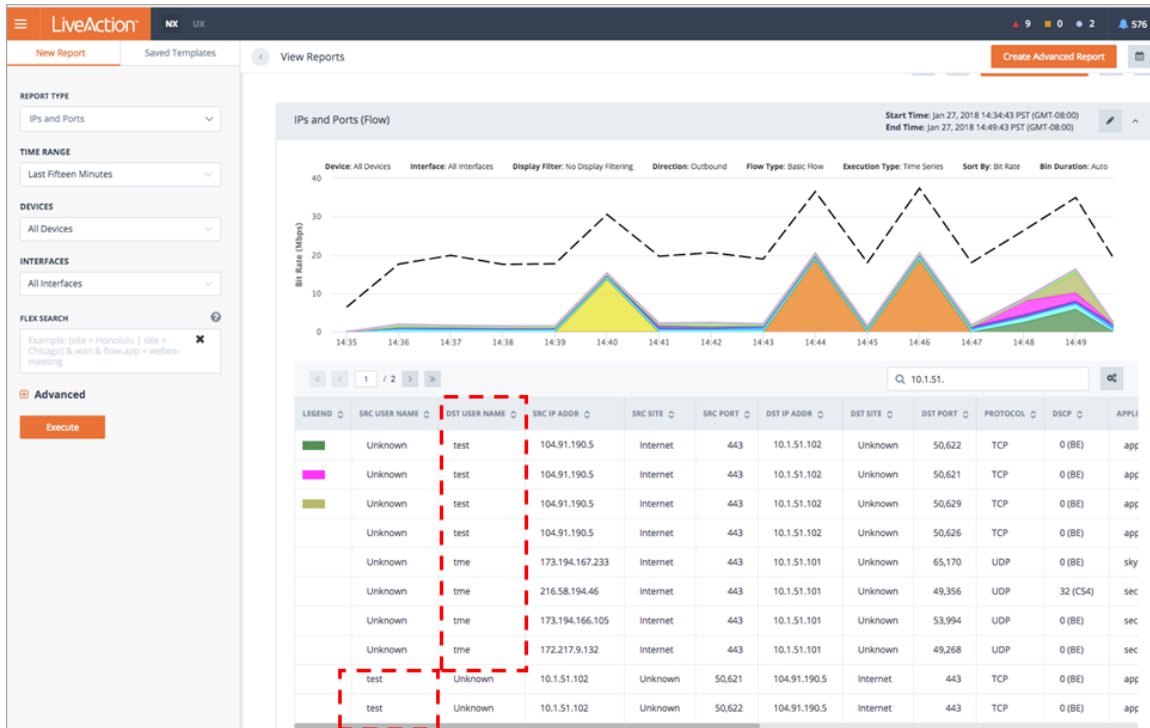
HOSTNAME *

PXGRID USERNAME *

Create

✔ Cisco ISE configuration has saved successfully.

Username 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.

The screenshot shows the LiveNX Settings page with the "ADD CISCO SD-WAN" configuration form. The form includes fields for Hostname, Username, and Password. There is a checkbox for "Bypass Proxy" and an "Add HTTP Header" button. A "Submit" button is located at the bottom right of the form.

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**.

ADD CISCO SD-WAN

Connection Settings

Hostname *
 Username *
 Password *

Additional HTTP Header

Key *
 Value *
 Plain Text
 Base64

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

CONFIGURED CISCO SD-WAN

Hostname: 198.18.1.10
 Username: admin
 Status: ● Connected

 ⓘ

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

CONFIGURED CISCO SD-WAN

Hostname 198.18.1.10
 Username admin
 Status ● Connected

 ⓘ

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.

DISCOVER DEVICES ✕

1. What to scan | 2. SNMP Settings | 3. Node

SPECIFY IP RANGES

198.18.134.100-106

Add More

CISCO SD-WAN TO LIVENX SITE MAPPING

Map the site IDs for SD-WAN devices to LiveNX sites

Sites Mapped: 0

Set Mapping

Save & Next

Cancel Discover

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

DISCOVER DEVICES ✕

1. What to scan | 2. SNMP Settings | 3. Node

SPECIFY IP RANGES

198.18.134.100-106

Add More

CISCO SD-WAN TO LIVENX SITE MAPPING

Map the site IDs for SD-WAN devices to LiveNX sites

Sites Mapped: 0

Set Mapping

Save & Next

Cancel Discover

The *Cisco SD-WAN Site Mapping* modal appears.

CISCO SD-WAN SITE MAPPING ✕

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](#) to download an example CSV file

Add Import CSV File Edit Delete

	SD-WAN SITE ID	LIVENX SITE NAME	NEW LIVENX SITE
<input type="checkbox"/>	SD-WAN Site ID	LiveNX Site Name	All
No Data			

Cancel Apply

To add an individual site, click **Add**.

CISCO SD-WAN SITE MAPPING



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](#) to download an example CSV file

	SD-WAN SITE ID	LIVENX SITE NAME	NEW LIVENX SITE
<input type="checkbox"/>	<input type="text" value="SD-WAN Site ID"/>	<input type="text" value="LiveNX Site Name"/>	All <input type="button" value="v"/>
No Data			

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

EDIT SITE MAPPING X

SD-WAN SITE ID:

LIVENX SITE NAME:

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 SD-WAN SITE MAPPING



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](#) to download an example CSV file

	SD-WAN SITE ID	LIVENX SITE NAME	NEW LIVENX SITE
<input type="checkbox"/>	<input type="text" value="SD-WAN Site ID"/>	<input type="text" value="LiveNX Site Name"/>	All <input type="button" value="v"/>
<input type="checkbox"/>	100	DC1-San-Jose	
<input type="checkbox"/>	200	DC2-RTP	✓
<input type="checkbox"/>	300	Branch1-Miami	✓
<input type="checkbox"/>	400	Branch2-Chicago	✓

All rows / 4

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

CISCO SD-WAN SITE MAPPING



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](#) to download an example CSV file

	SD-WAN SITE ID	LIVENX SITE NAME	NEW LIVENX SITE
<input type="checkbox"/>	<input type="text" value="SD-WAN Site ID"/>	<input type="text" value="LiveNX Site Name"/>	All <input type="button" value="v"/>
<input type="checkbox"/>	100	DC1-San-Jose	
<input type="checkbox"/>	200	DC2-RTP	✓
<input type="checkbox"/>	300	Branch1-Miami	✓
<input type="checkbox"/>	400	Branch2-Chicago	✓

All rows / 4

Below is an example CSV.

	A	B
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.

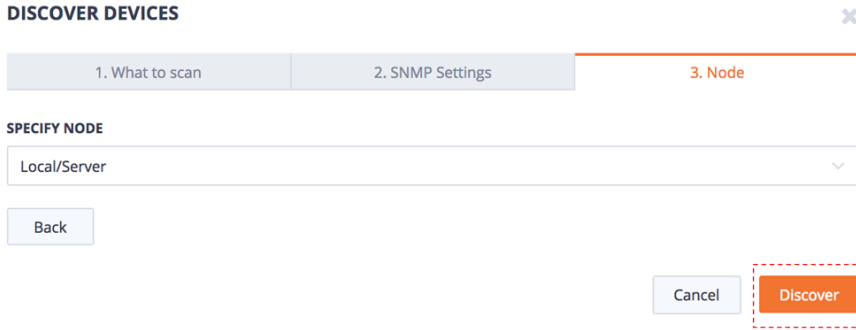
When ready, click **Save & Next**.

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

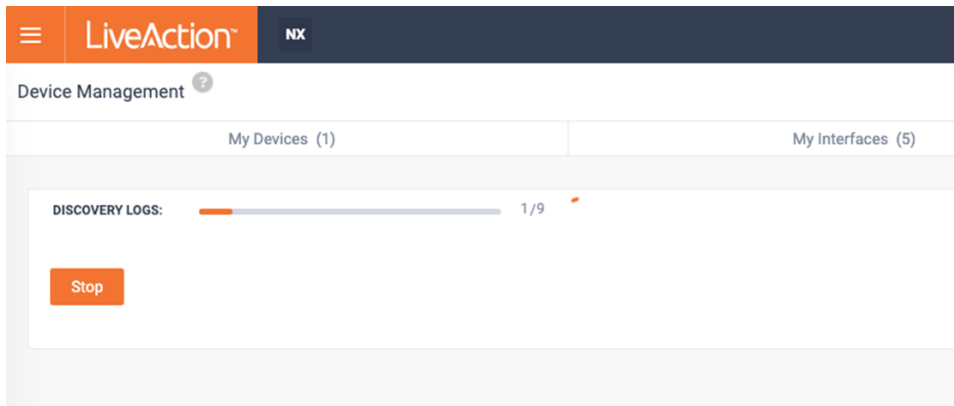
Note: Easy onboarding via API integration to vManage and the SNMP polling of the devices are separate processes. If the SNMP settings are incorrect or if LiveNX does not have connectivity to the devices via SNMP – the devices will show up as gray or unreachable.

When ready, click **Save & Next**.

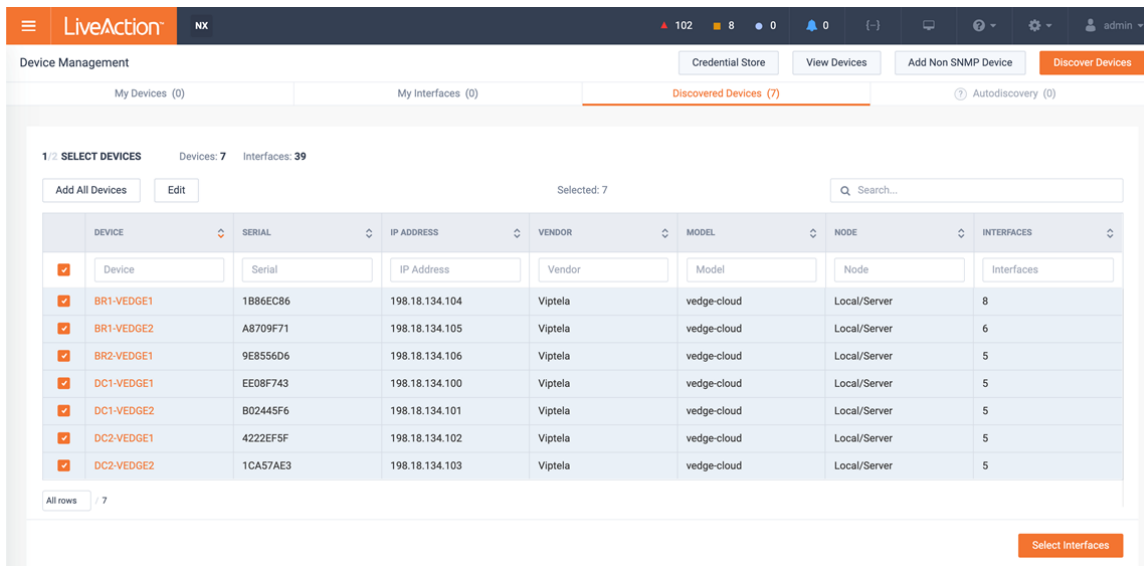
The *Node* tab appears. From the *Specify Node* picker, select the LiveNX Node that will monitor these SDWAN devices. When ready, click **Discover**.



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



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



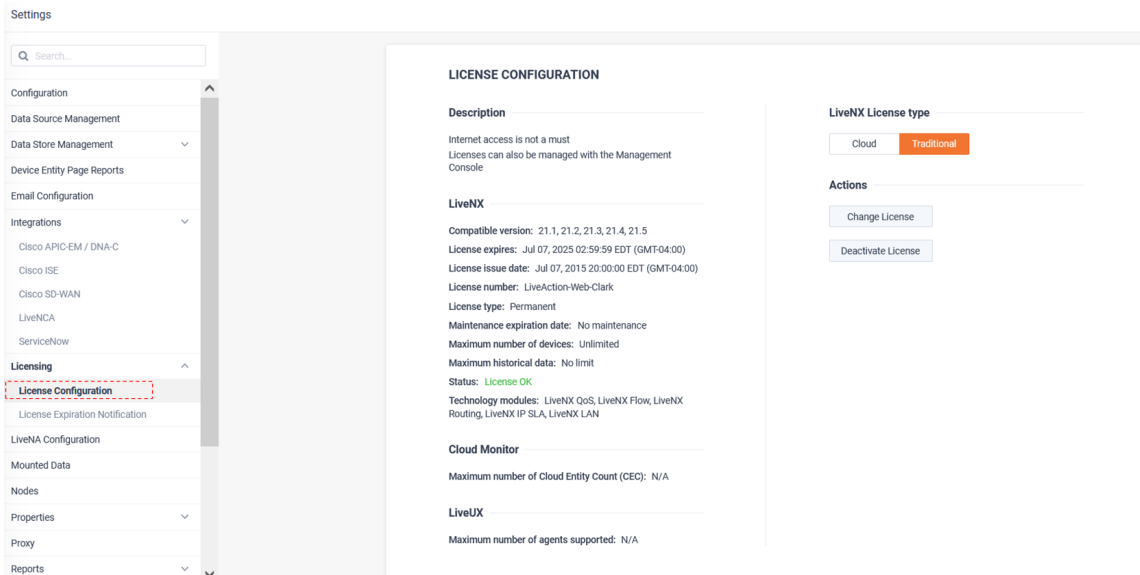
Adding these discovered devices to the LiveNX inventory is now identical to device discovery of any other SNMP monitored device.

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**.

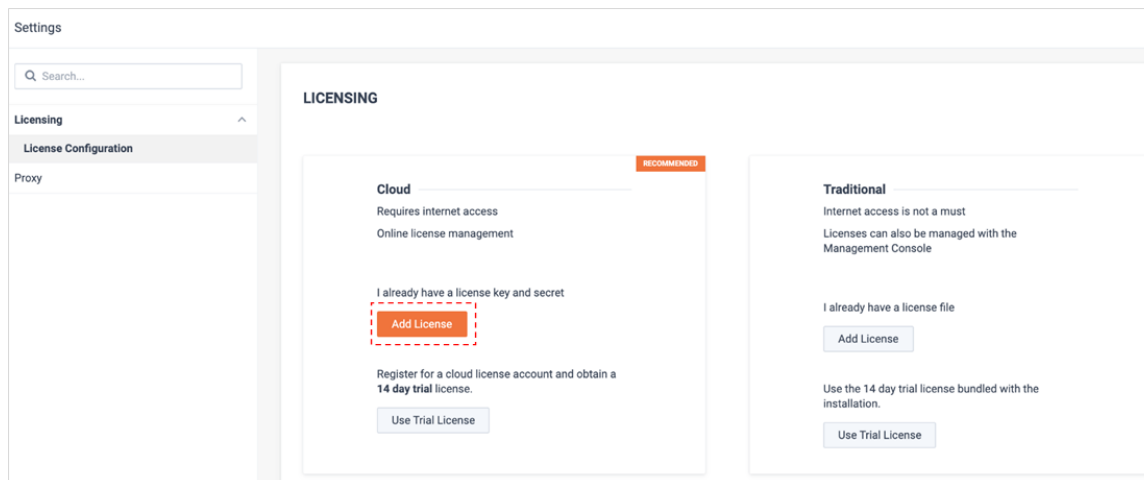
Licensing

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.



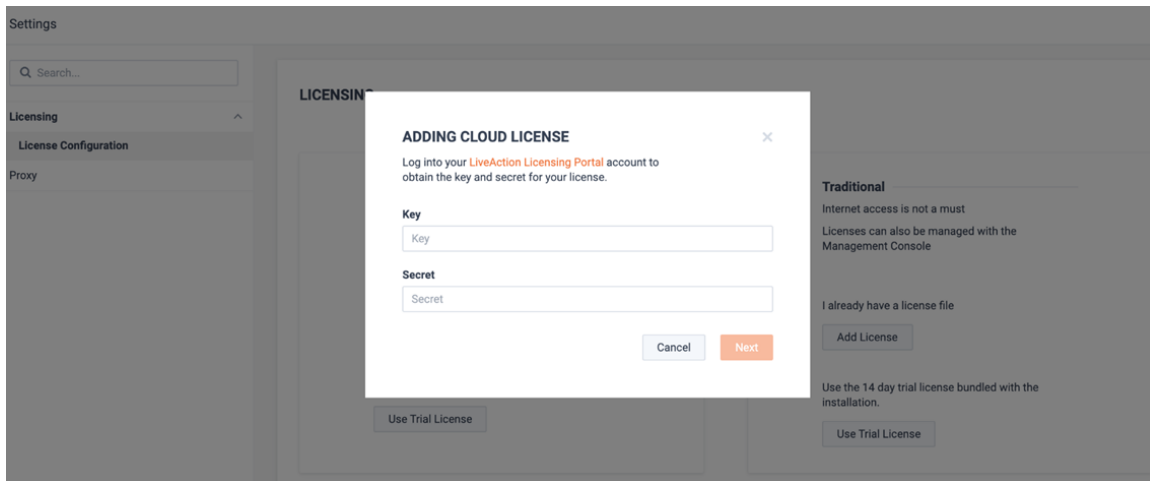
When using LiveNX for the first time, a license must be applied. It is recommended to use the cloud license portal.

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

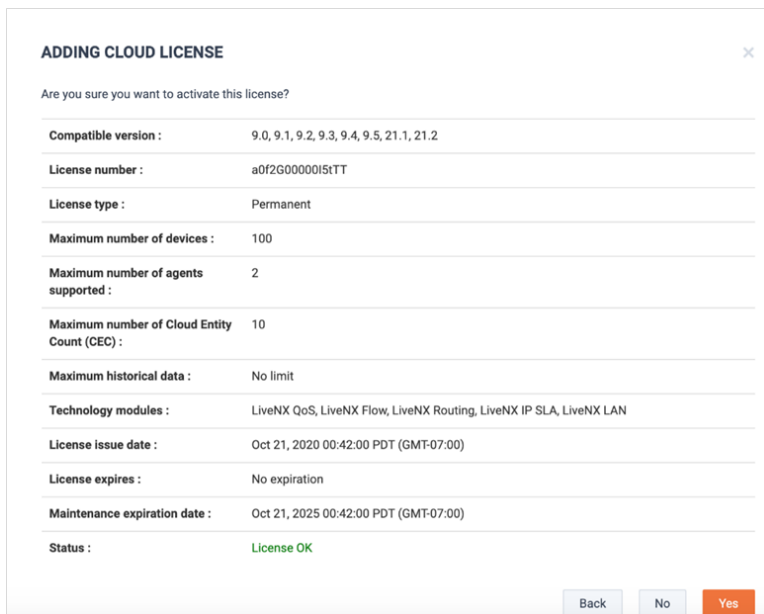


Supply the license *Key* and *Secret* and click **Next**.

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



Review the license’s details and click **Yes**.



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

LICENSING

Description
 Requires internet access
 Online license management
 Requires WebUI available via All-in-One OVA to manage licenses

LiveNX

Compatible version : 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 21.1, 21.2
License number : a0f2G00000IS1TT
License type : Permanent
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

LiveNX License type
 Cloud Traditional

Actions
 Change License
 Refresh License
 Deactivate License

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**.

LICENSING

Cloud RECOMMENDED
 Requires internet access
 Online license management
 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

Traditional
 Internet access is not a must
 Licenses can also be managed with the Management Console
 I already 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**.

ADDING TRADITIONAL LICENSE

Upload Your License File
 LiveAction-9.0-EXT-D100-210904.key Browse
 Cancel Next

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

LICENSING

Description

Internet access is not a must
Licenses can also be managed with the Management Console

LiveNX

Compatible version : 21.1, 21.2, 21.3
License number : LiveAction-Web-Clark
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

Cloud Monitor

Maximum number of Cloud Entity Count (CEC) : N/A

LiveUX

Maximum number of agents supported : N/A

LiveNX License type

Cloud Traditional

Actions

Change License

Deactivate License

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
- License Configuration
- License Expiration Notification**
- LiveNA Configuration

LICENSE EXPIRATION NOTIFICATION

Enter email(s) to get notifications. You will be getting daily notifications starting 10 days before license expiration.

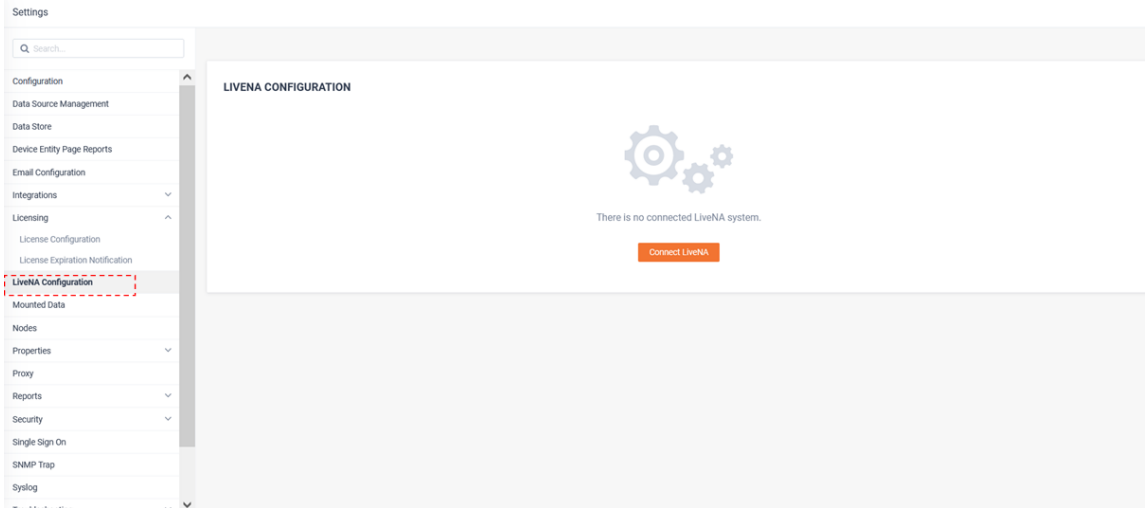
Email

Save

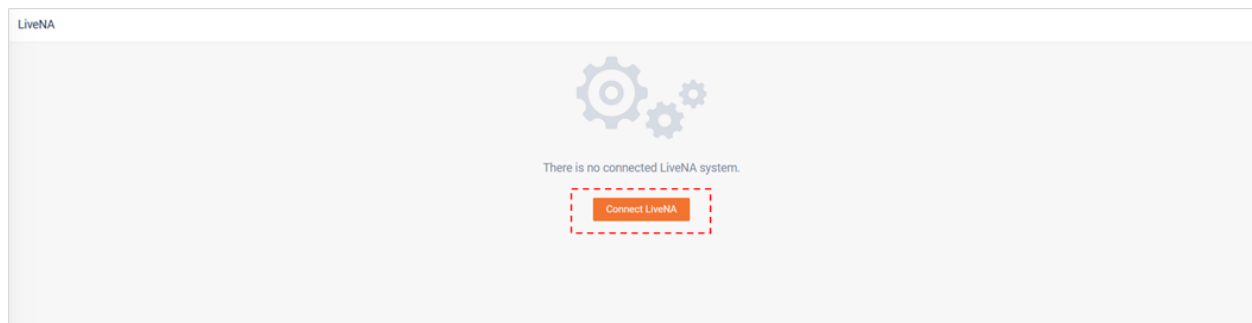
LiveNA Configuration

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.



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

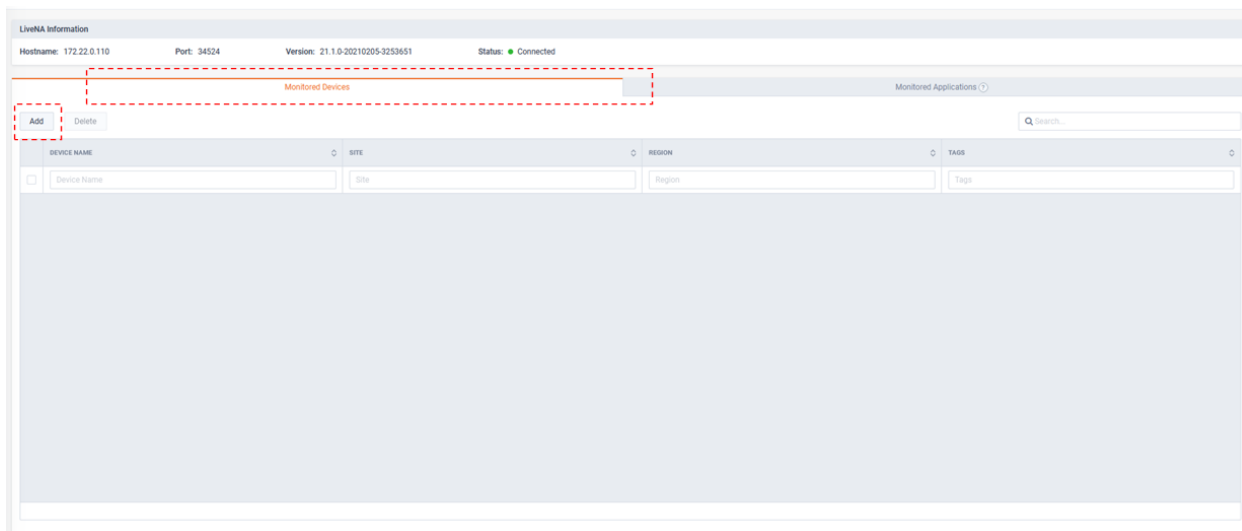


Add the LiveNA *Hostname*, *Port*, and *API key* and click **Submit**.

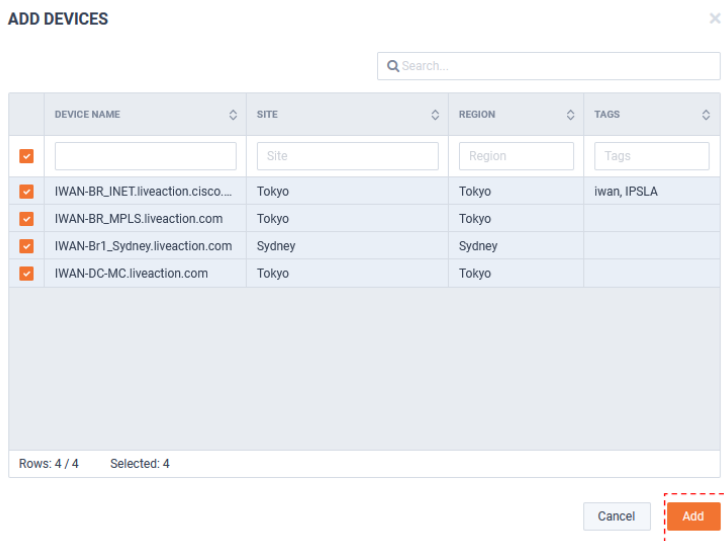
The 'CONNECT LIVENA' dialog box contains the following fields and buttons:

- Hostname ***: A text input field.
- Port ***: A dropdown menu with a small icon on the right.
- API Key ***: A text input field with a placeholder 'API Key'.
- Cancel**: A light blue button.
- Submit**: An orange button.

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**.



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



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

LiveNA Status
 Hostname: 172.22.0.110 Port: 34524 Version: 21.2.1-20210429-30a5f10 Status: ● Connected

Monitored Devices Monitored Applications

Add Delete **Import SNMP Data**

	DEVICE NAME	SITE	REGION	TAGS
<input type="checkbox"/>	<input type="text"/>	<input type="text" value="Site"/>	<input type="text" value="Region"/>	<input type="text" value="Tags"/>
<input type="checkbox"/>	IWAN-BR_INET.liveaction.cisco.com	Tokyo	Tokyo	IPSLA, Cisco RTRs, Cisco, Iwan
<input type="checkbox"/>	IWAN-BR_MPLS.liveaction.com	Tokyo	Tokyo	mpls, Cisco RTRs, Cisco
<input type="checkbox"/>	IWAN-Br1_Sydney.liveaction.com	Sydney	Sydney	Cisco RTRs, Cisco
<input type="checkbox"/>	IWAN-DC-MC.liveaction.com	Tokyo	Tokyo	Cisco RTRs, Cisco

Rows: 4 / 16

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
 Hostname: 172.22.0.110 Port: 34524 Version: 21.2.1-2021042

Monitored Devices

Add Delete **Import SNMP Data**

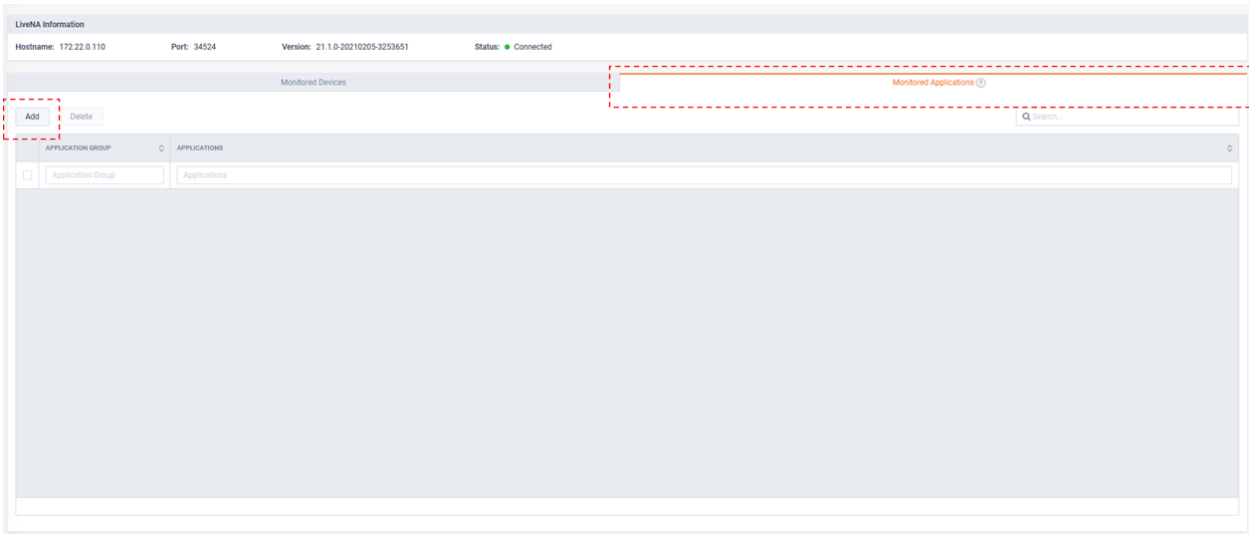
	DEVICE NAME	SITE
<input type="checkbox"/>	<input type="text"/>	<input type="text" value="Site"/>
<input type="checkbox"/>	IWAN-BR_INET.liveaction.cisco.com	Tokyo
<input type="checkbox"/>	IWAN-BR_MPLS.liveaction.com	Tokyo
<input type="checkbox"/>	IWAN-Br1_Sydney.liveaction.com	Sydney
<input type="checkbox"/>	IWAN-DC-MC.liveaction.com	Tokyo

IMPORT SNMP DATA ✕

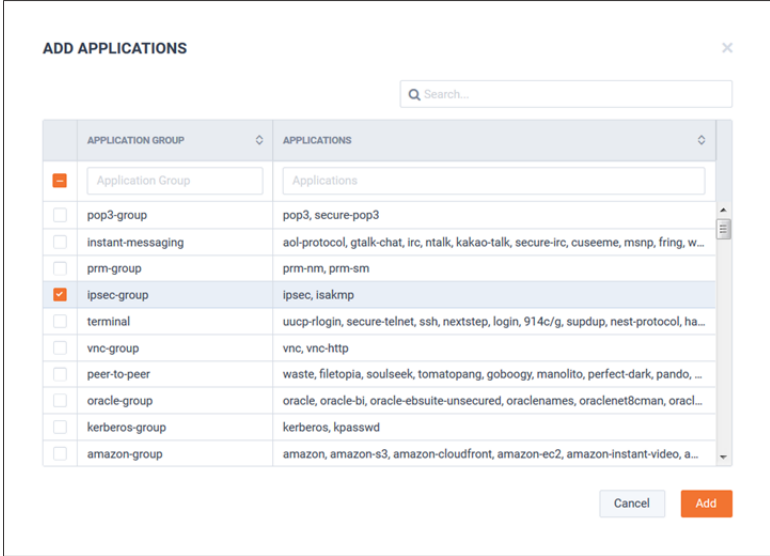
You are about to import SNMP data from LiveNX. All previous LiveNA data will be overwritten.
 Are you sure you want to proceed?

Import data for selected time range:

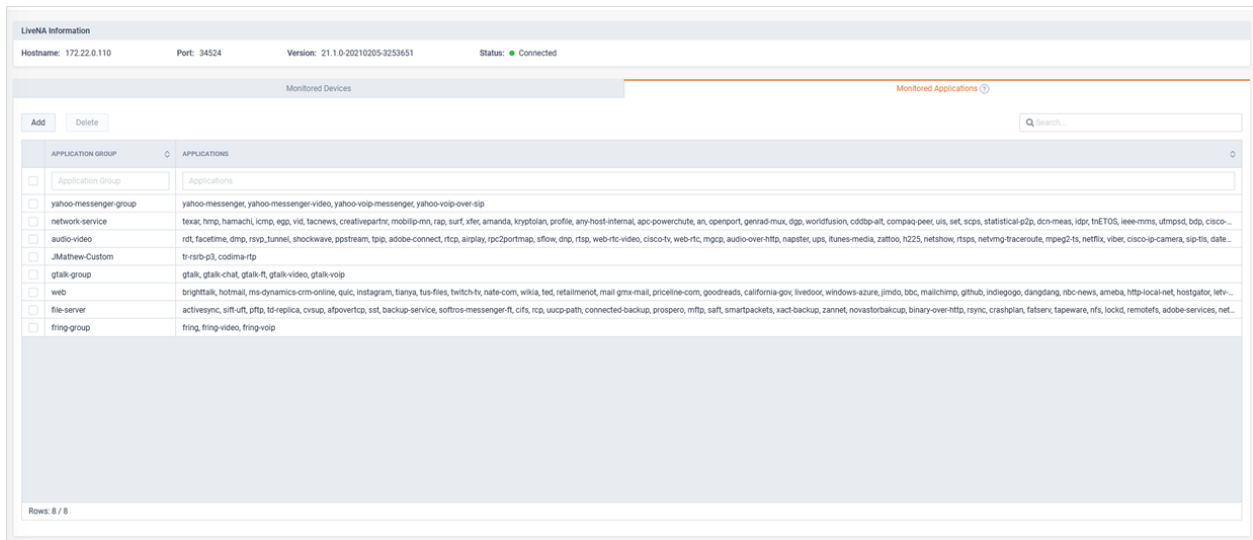
By default, LiveNA will learn and monitor the top 100 application on the devices it is monitoring. This is based on network utilization. These top 100 could change over time. To ensure LiveNA residually monitors key applications of interest, Application Groups can be added to the *Monitored Applications* 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**.



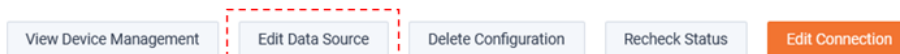
The *Add Applications* modal appears and lists the Application Groups defined in LiveNX. Select an Application Group and click **Add**.



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



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



EDIT DATA SOURCE ✕

WAN interfaces provide data by default. Also, you can select interface and service provider tags to provide data to LiveNA.

WAN
 WAN and XCon

Interface tags

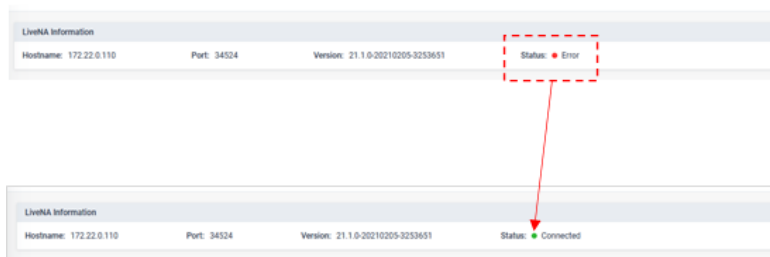
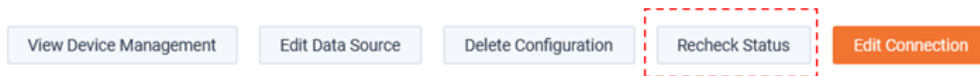
Select interface tag

Service provider tags

Select service provider tag

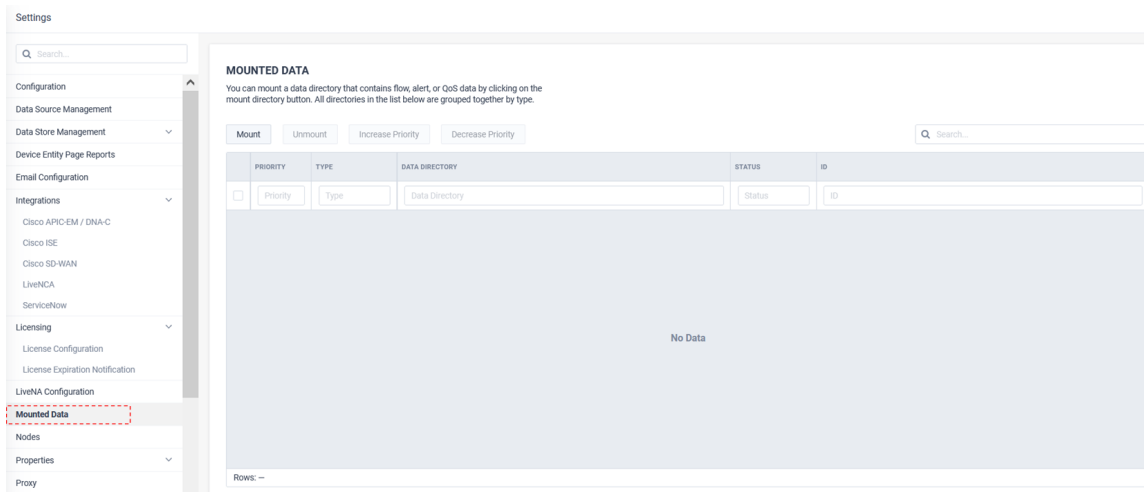
Cancel
Save

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



Mounted Data

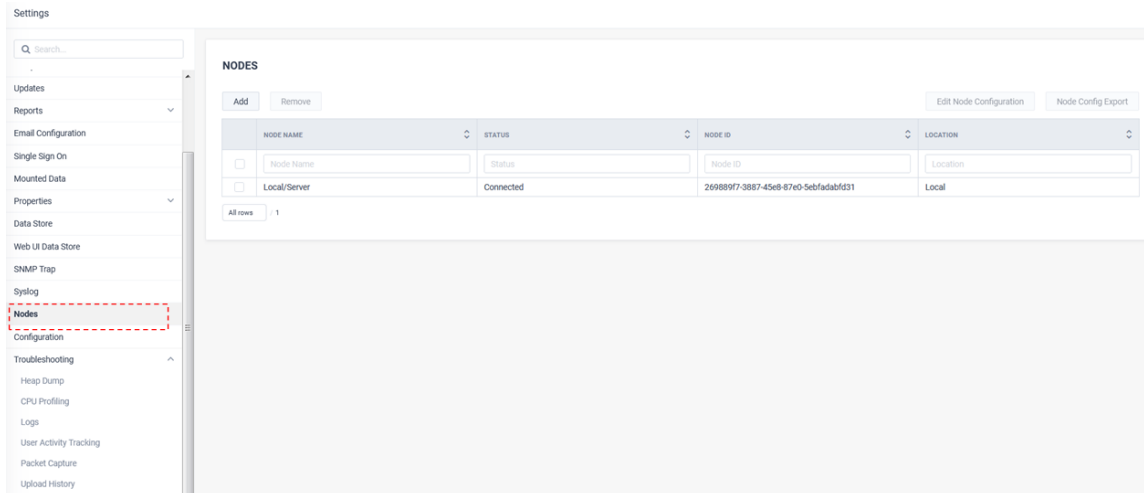
Mounted Data allows archived LiveNX data stores to be re-mounted for historic investigation.



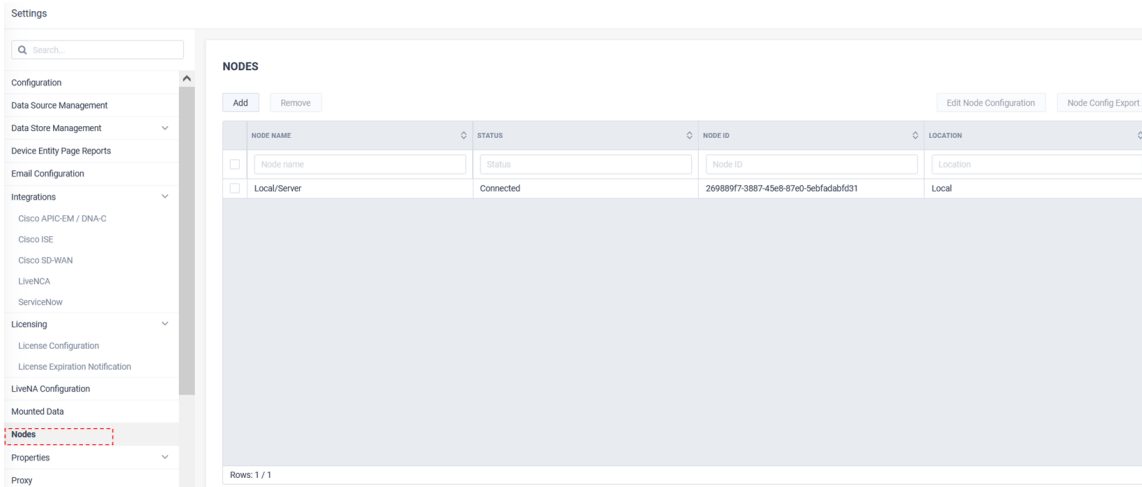
Nodes

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

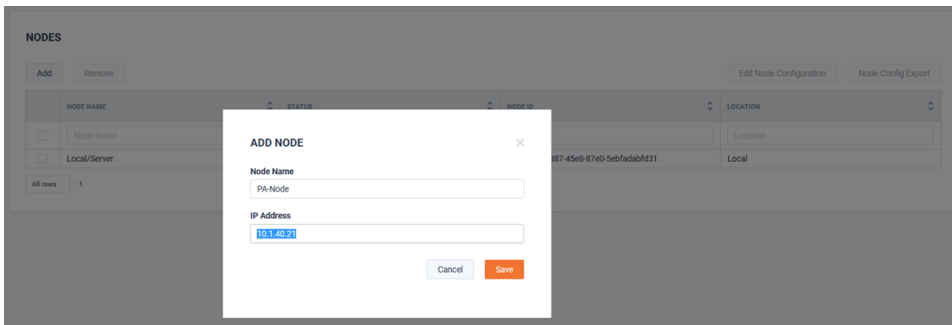
The LiveNX Server has a built in Node. When additional Nodes are used, a configuration file must be created on the LiveNX server for each Node. This file must be copied to the respective Node to complete the integration.



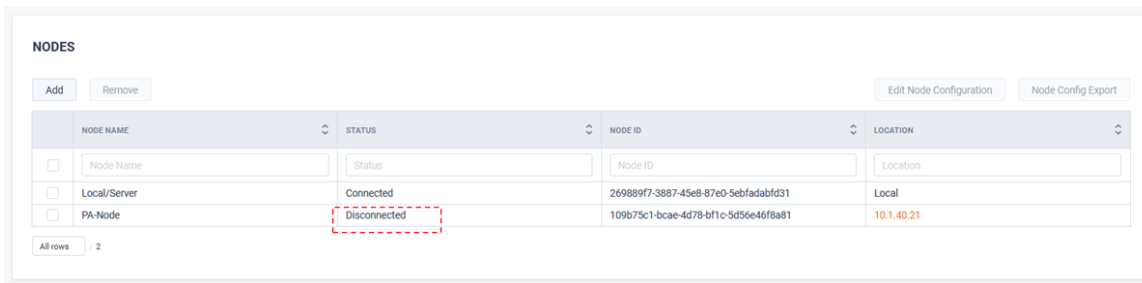
To add a new Node, click **Add**.



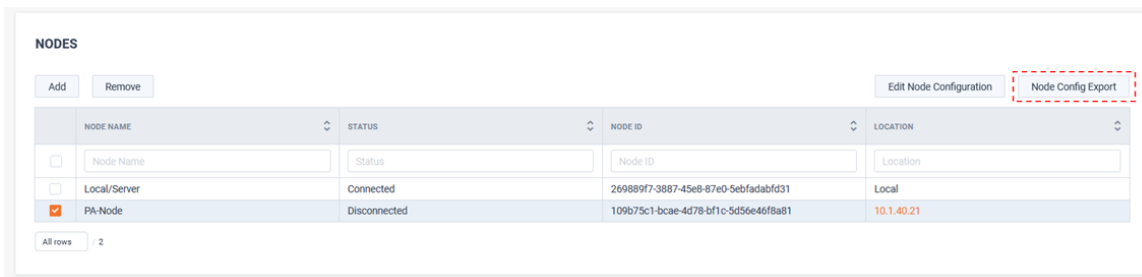
The *Add Node* modal appears. Define the Node's name and IP address and click **Save**.



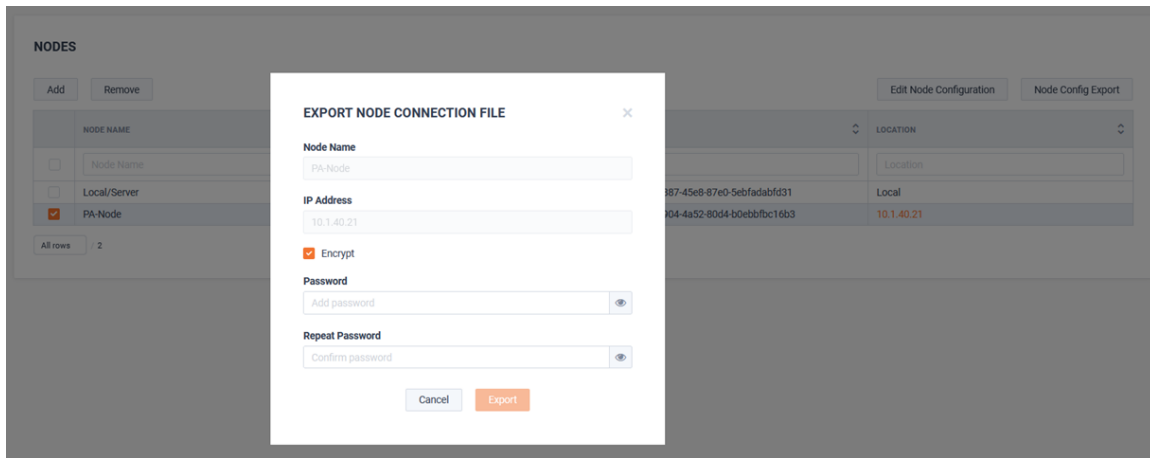
The Node appears but displays a status of *Disconnected*.



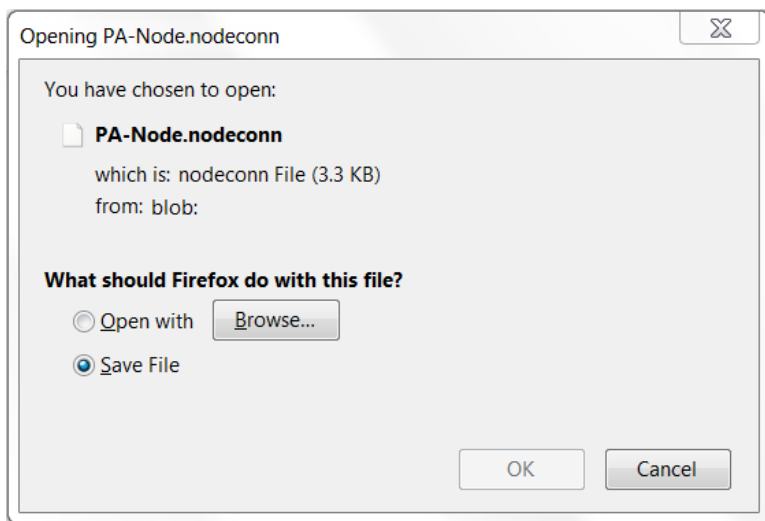
To copy the Node's configuration, click **Node Config Export**.



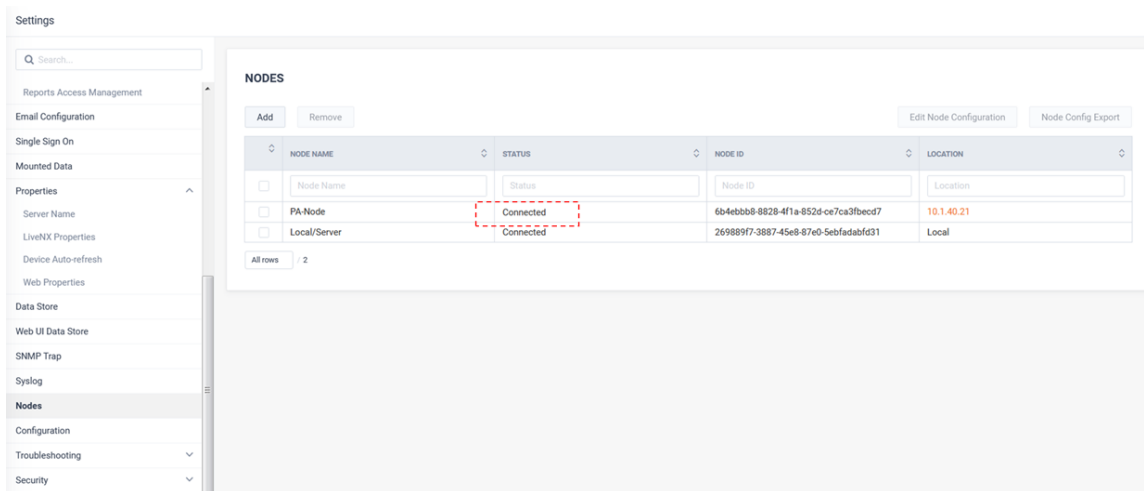
The *Export Node Configuration File* appears. An optional password may be entered. Click **Export**.



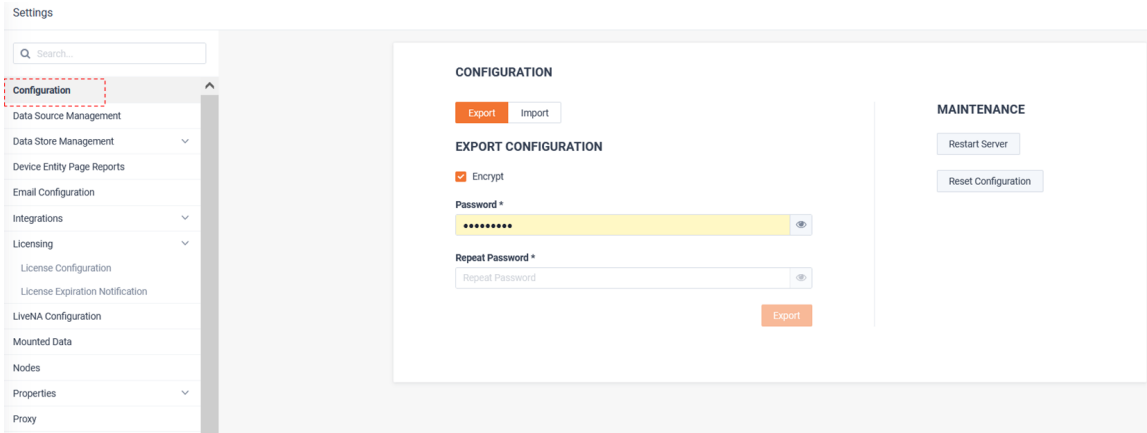
Save the Node's config file for import into the Node.



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

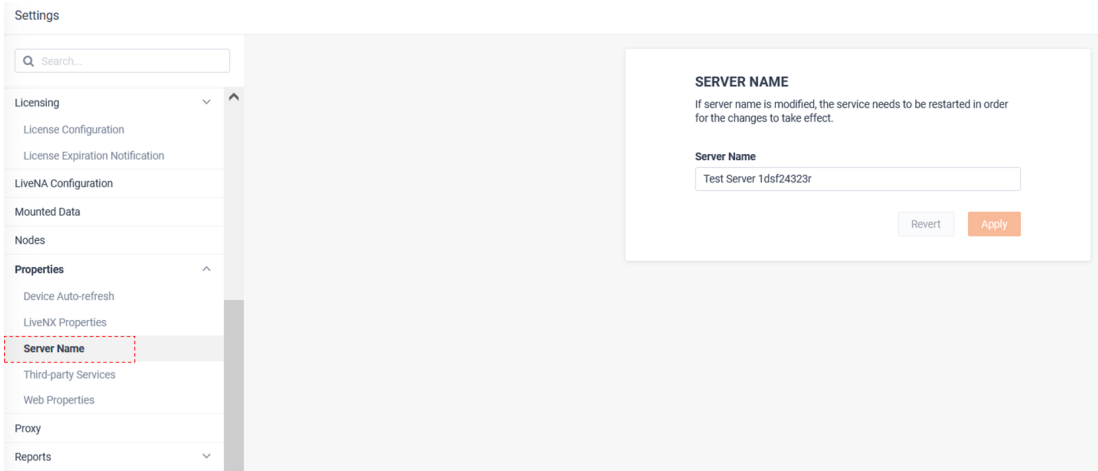


Configuration provides the ability to backup or restore the LiveNX configuration, restart the server, or reset the configuration to default.



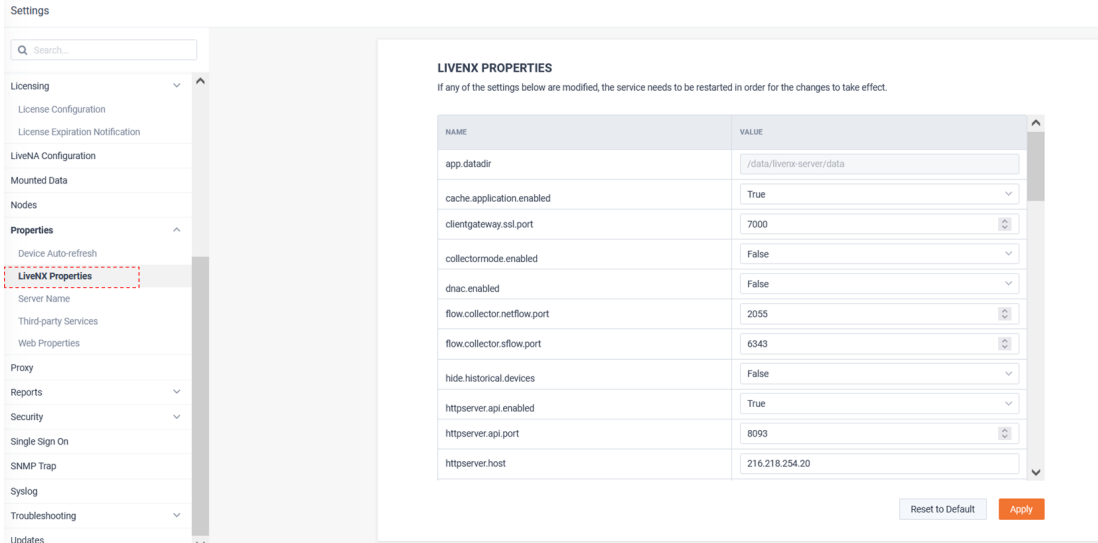
Properties

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

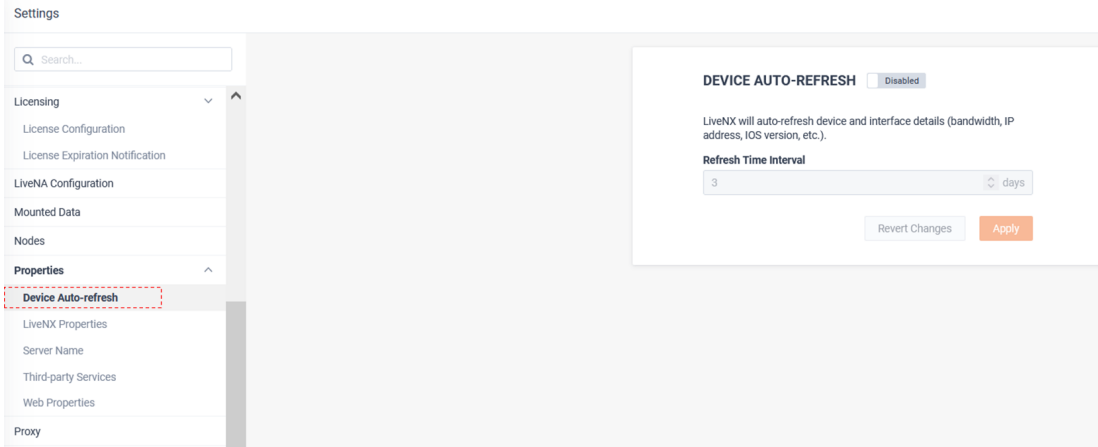


LiveNX Properties are a list of system settings that could need to be adjusted in some circumstances.

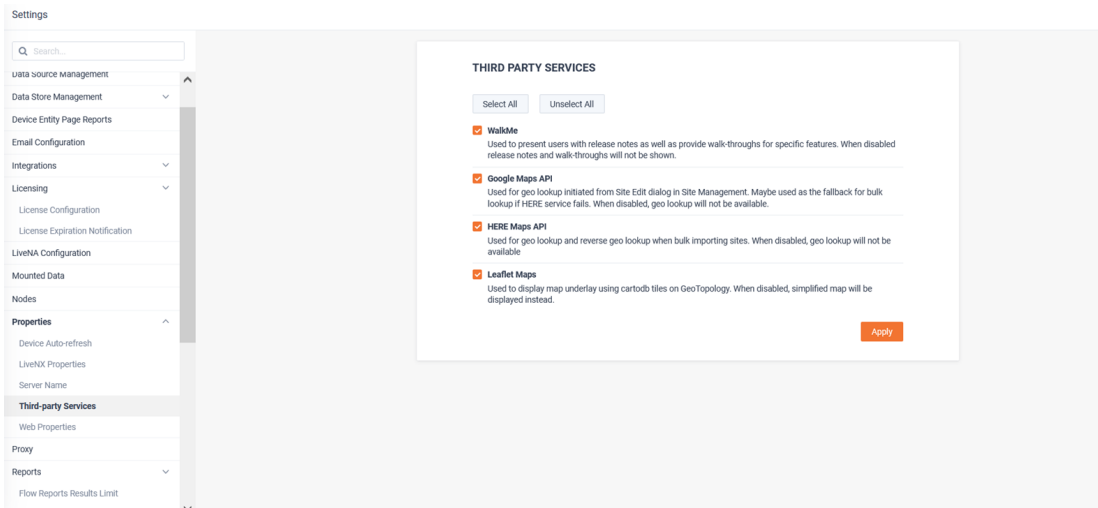
Care should be taken when changing these parameters and it is suggested to work with the LiveNX support team.



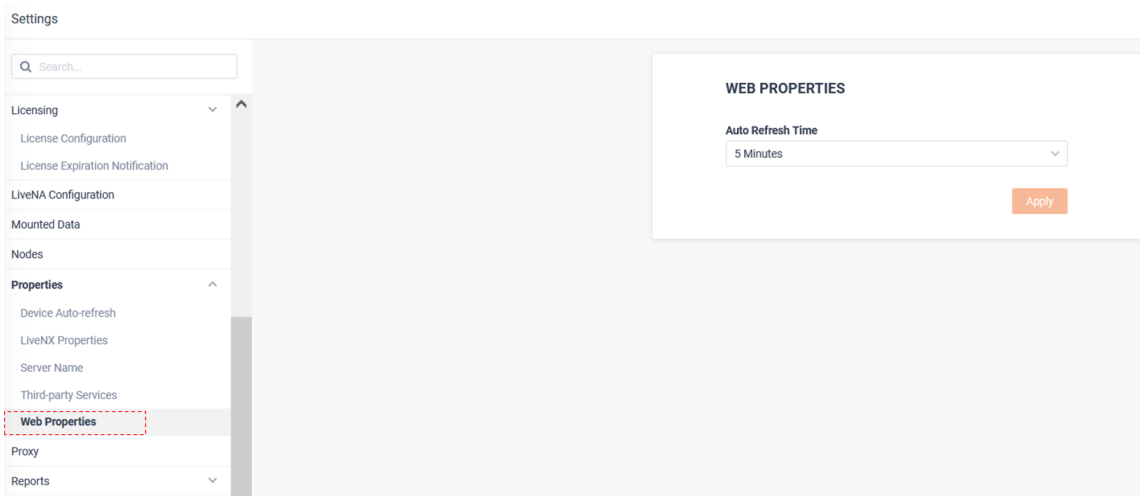
Device Auto-Refresh can be enabled to ensure LiveNX does a full SNMP refresh of the devices in its inventory at a residual interval.



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.

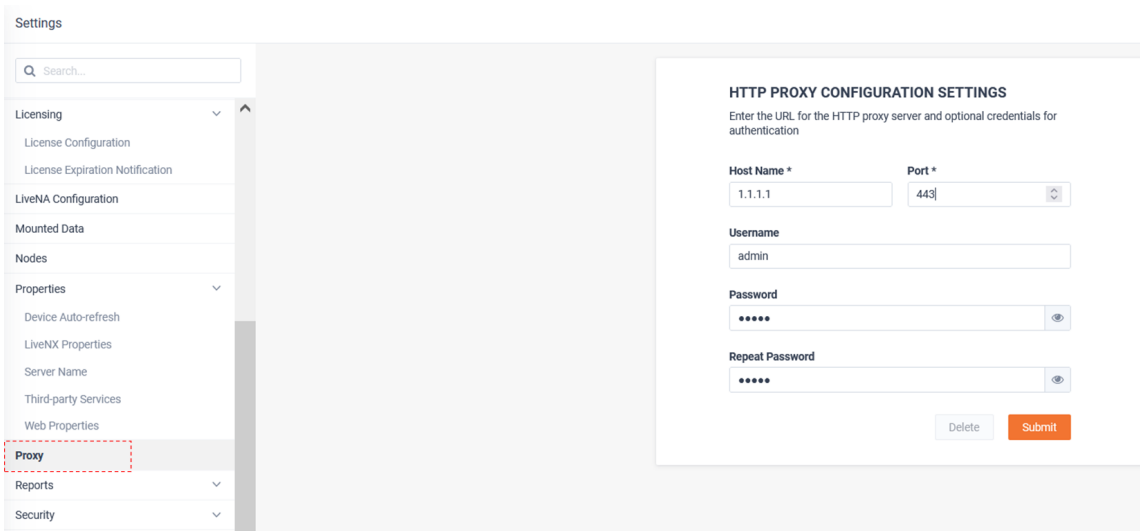


Web Properties defined the default *Auto Refresh Time* of Dashboards, Site, Devices, Interfaces, WAN Applications, Network Users, Site to Site Analysis, and Geo Topology.



Proxy

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

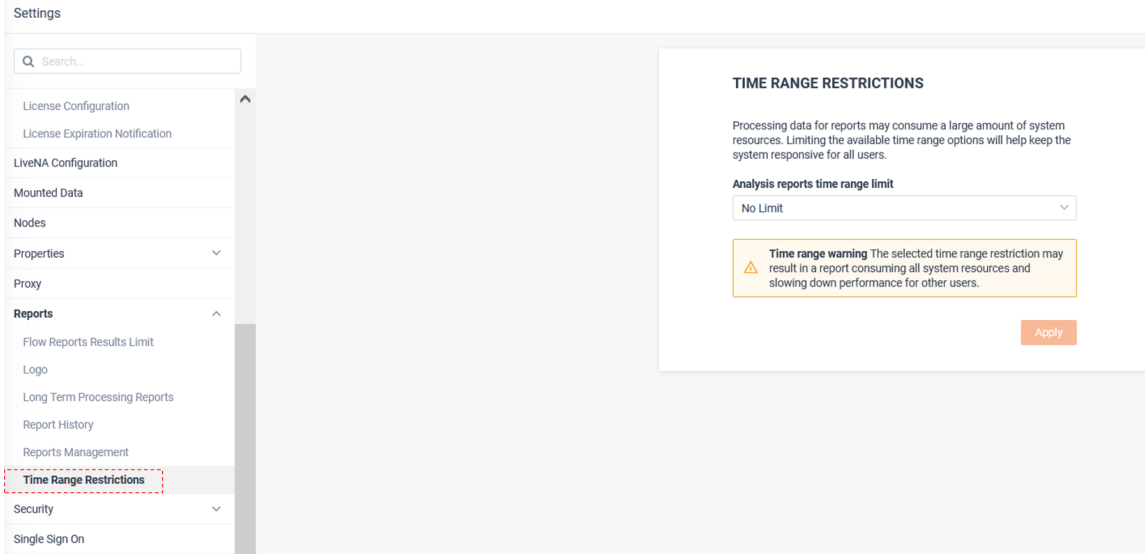


Reports

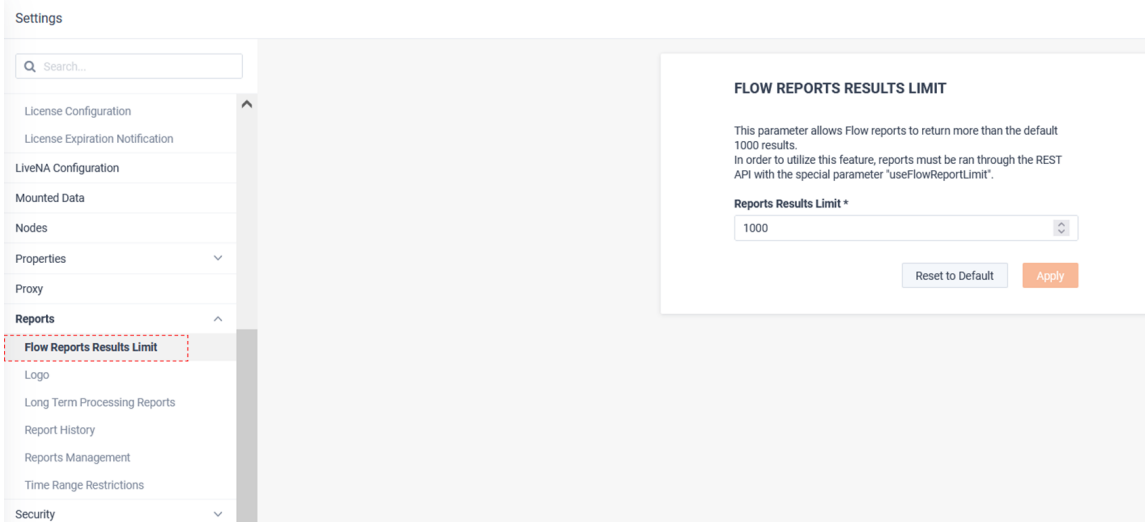
Time Range Restrictions allows for the limiting of the duration of Analysis Reports. This can be used to ensure processor intensive reports do not hold up the report queue.

The Analysis reports are currently:

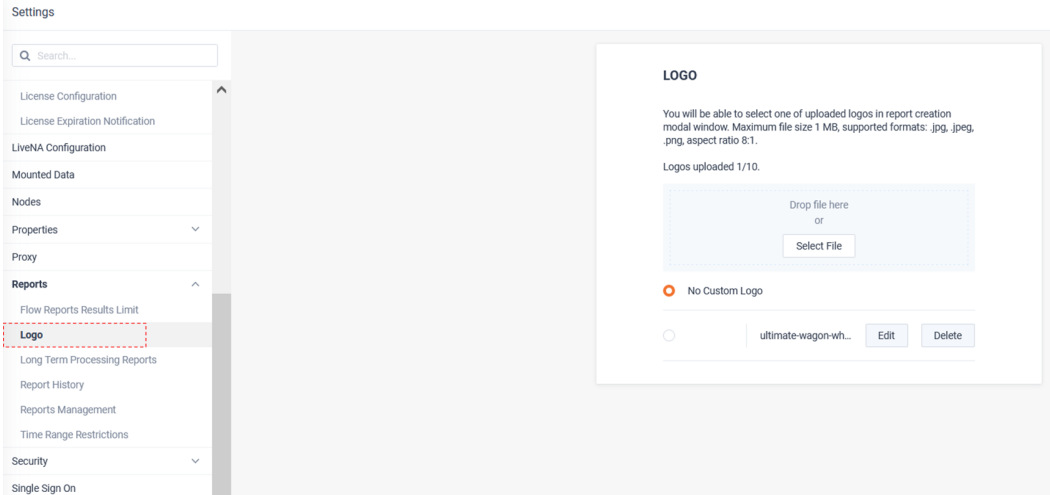
- All Unique Flows
- IPs and Ports
- Security Analysis
- Top Analysis



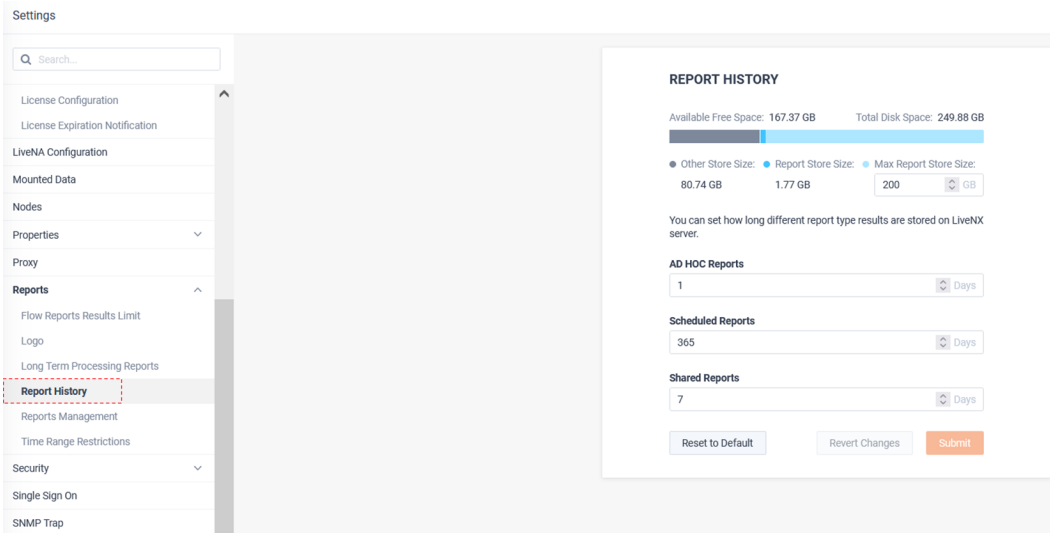
Flow Report Results Limit allow for adjustment of the returned results of Flow reports. By default, most Flow reports limit the returned results to 1000 rows, but this setting allows for more returned results. Caution should be used when adjusting this setting to not impact the overall system performance.



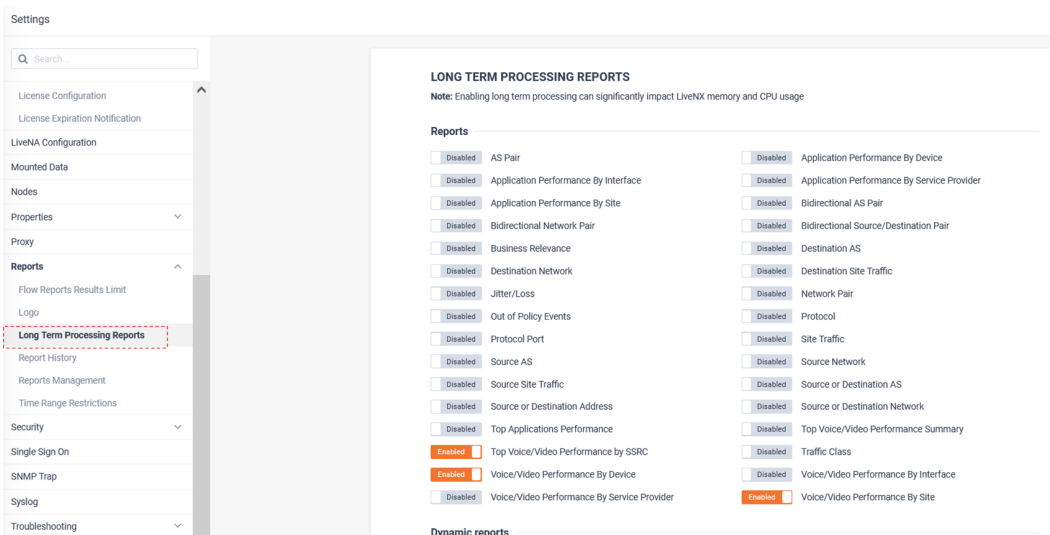
Logo allows you give a custom logo to shared and PDF reports. The logo page allows for the uploading and management of logos.



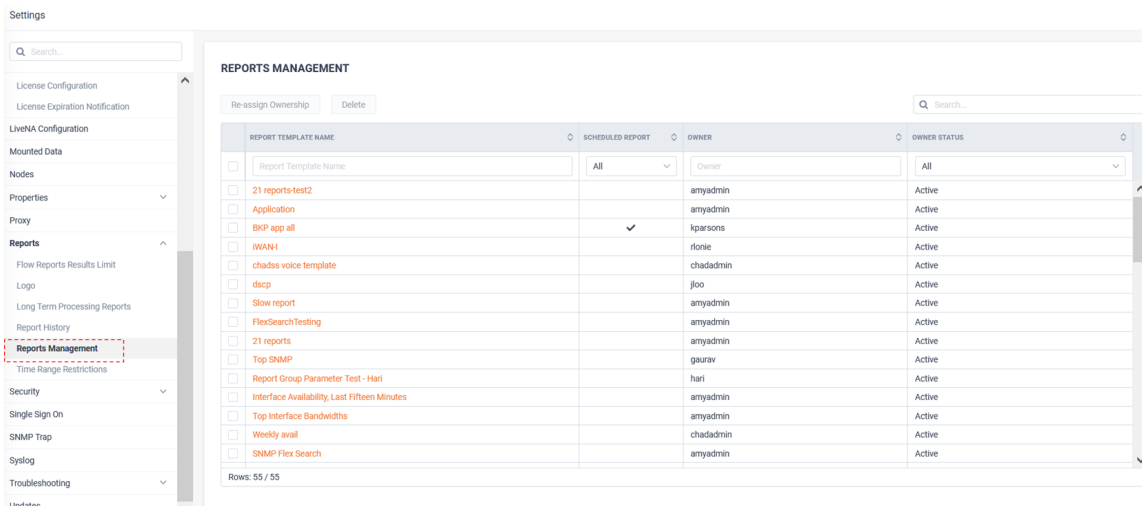
Report History provides management to each users personalized report history.



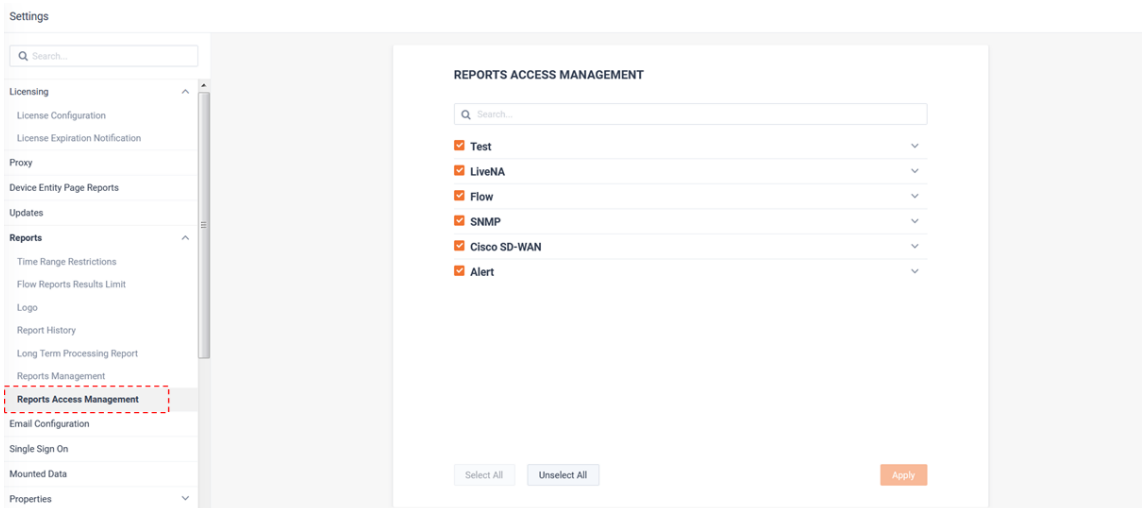
Long Term Processing Reports allows for selection of which reports will have their data sent to the Long Term Flow store.



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

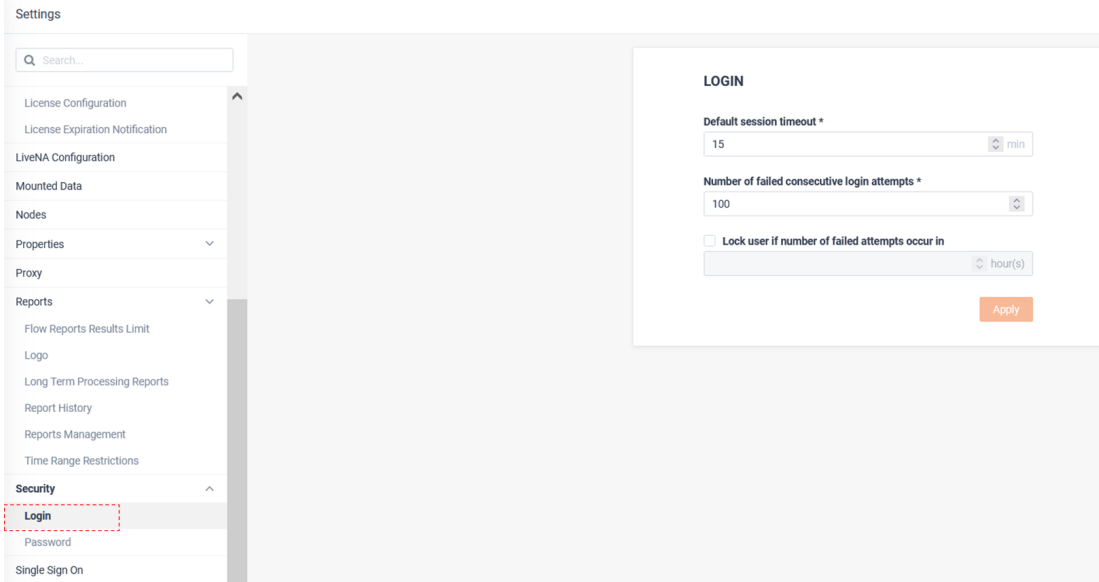


Reports Access Management defines which reports non-Admin users can run. Do note that some reports which drive workflows cannot be disabled.

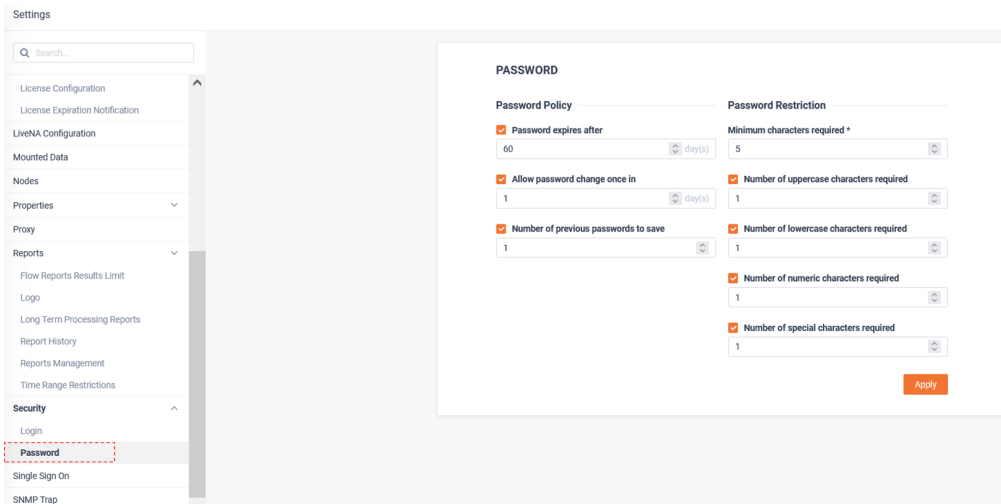


Security

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

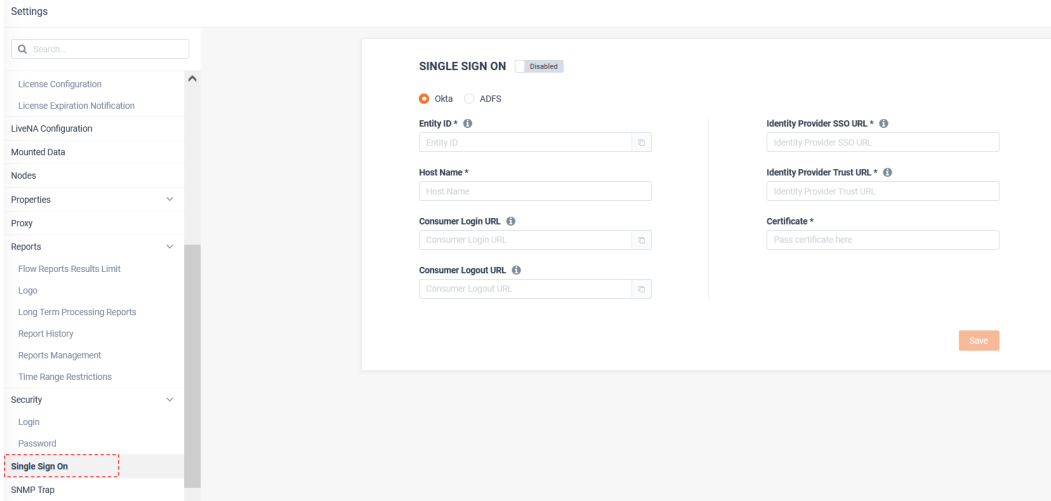


Password defines the password policy for users.



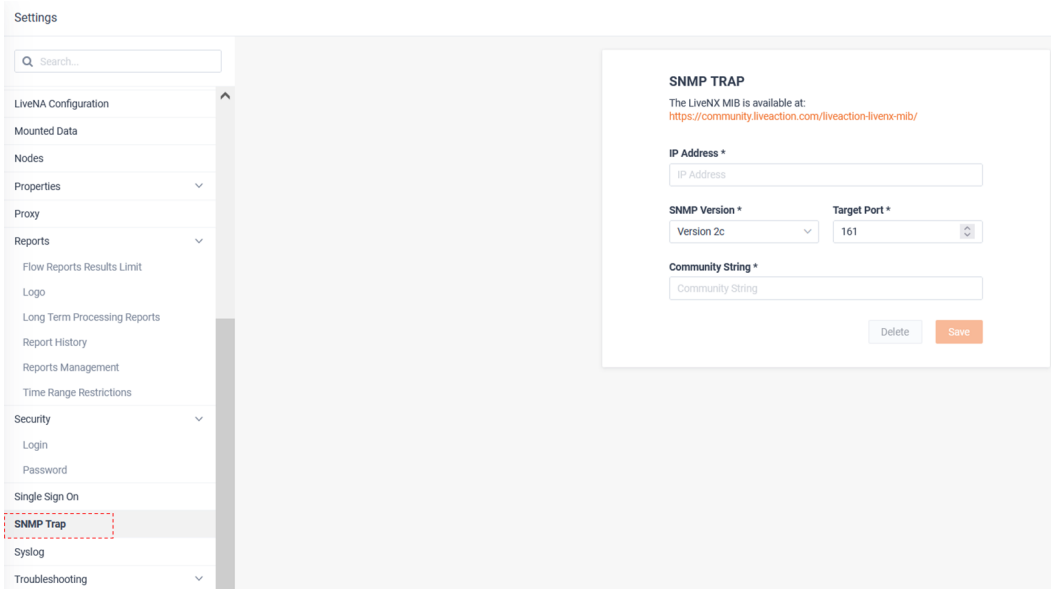
Single Sign On

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



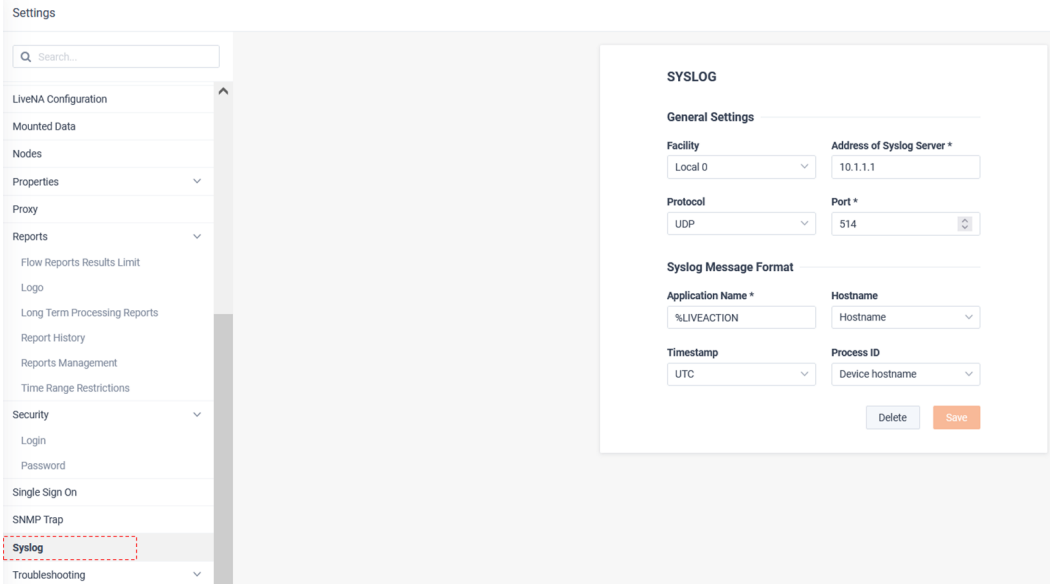
SNMP Trap

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



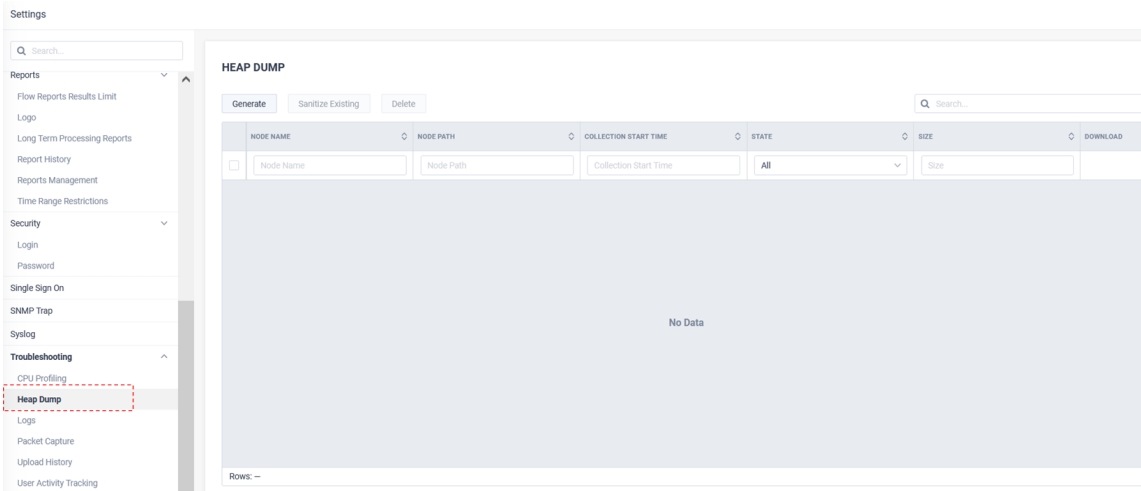
Syslog

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

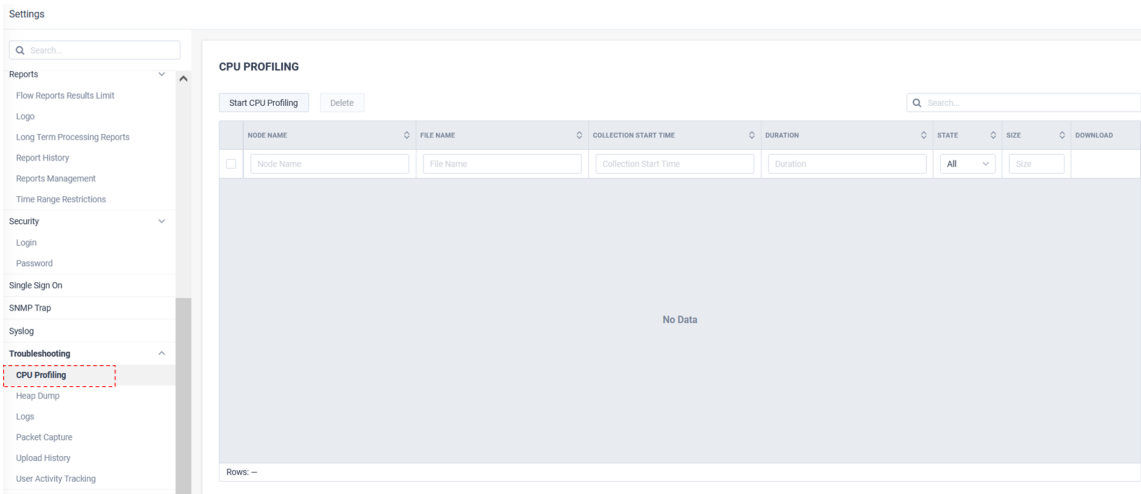


Troubleshooting

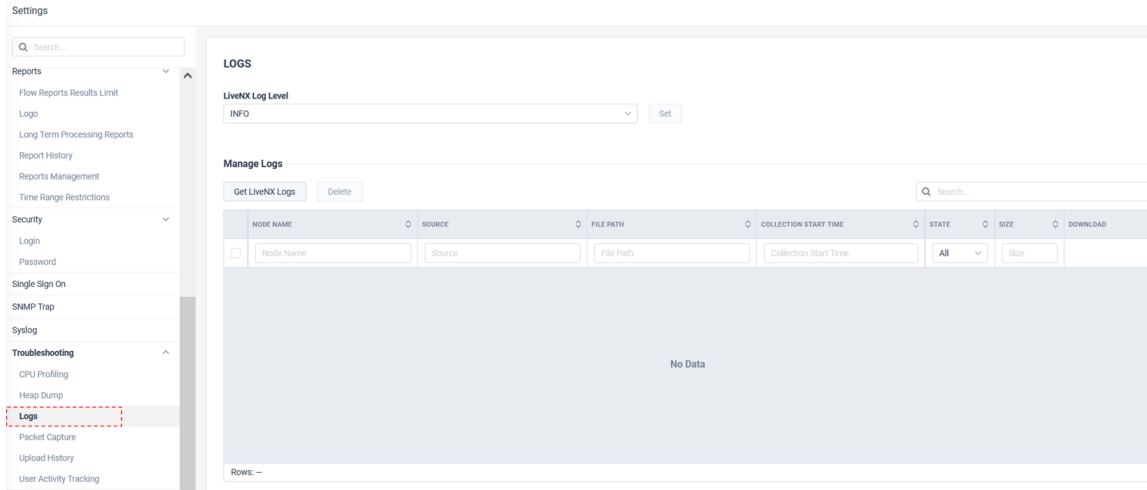
Heap Dump generates a snapshot of memory for troubleshooting by LiveAction Support.



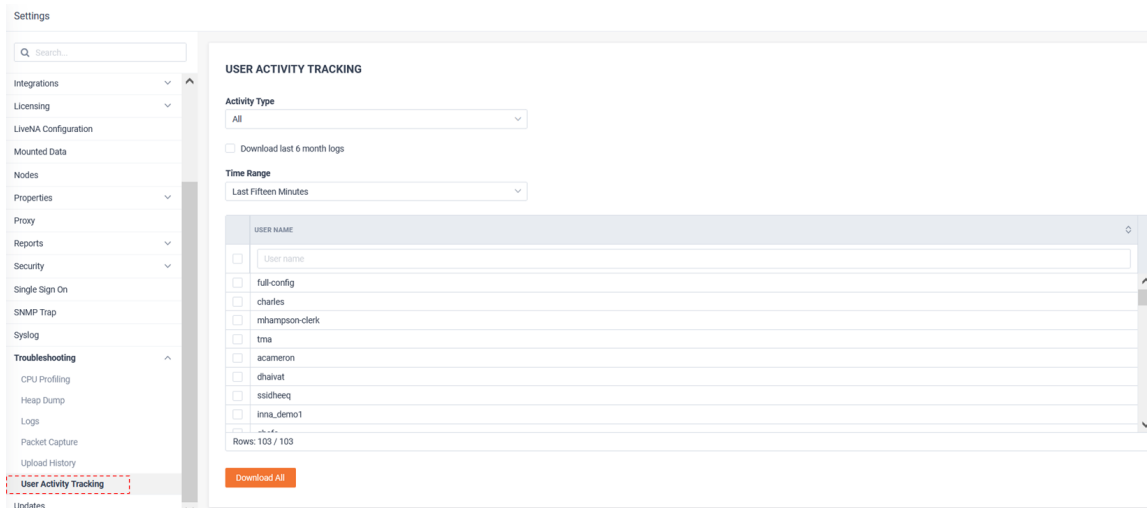
CPU Profiling generates a snapshot of CPU usage for troubleshooting by LiveAction Support.



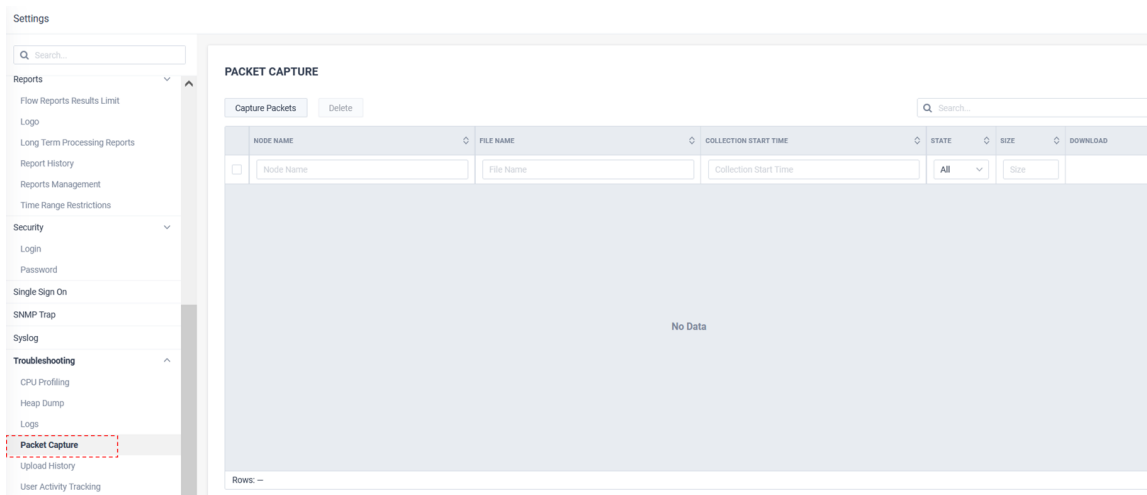
Logs generates system log files for troubleshooting by LiveAction Support.



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



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



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

The screenshot shows the 'Upload History' section of the LiveNX dashboard. On the left is a navigation menu with 'Upload History' highlighted. The main area contains a table with the following columns: License Key, File Name, Size, Upload Date, and Upload Link. The table lists several log files with their respective sizes and upload dates, each with a 'Copy Link' button.

LICENSE KEY	FILE NAME	SIZE	UPLOAD DATE	UPLOAD LINK
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
IskaAw43WfKAmYpXWUSpoP	2021-05-05_2126_logs.zip	56.62 MB	08 Jun 2021, 01:00PM	Copy Link
IskaAw43WfKAmYpXWUSpoP	2021-04-29_1522_logs.zip	48.55 MB	29 Apr 2021, 11:23AM	Copy Link
IskaAw43WfKAmYpXWUSpoP	2021-02-11_0913_logs.zip	99.32 MB	11 Feb 2021, 04:14AM	Copy Link
IskaAw43WfKAmYpXWUSpoP	2021-01-22_0113_logs.zip	50.24 MB	21 Jan 2021, 08:15PM	Copy Link
IskaAw43WfKAmYpXWUSpoP	2020-12-08_1637_logs.zip	51.96 MB	08 Dec 2020, 11:38AM	Copy Link
IskaAw43WfKAmYpXWUSpoP	1602179643230_10.100.51.8_2055_eth0_60...	202.00 B	08 Oct 2020, 01:55PM	Copy Link

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.

The screenshot shows the navigation menu of the LiveNX dashboard. The menu items are Settings, System Diagnostics, User Management, and LiveNX Server. 'System Diagnostics' is highlighted with a red dashed box.

The screenshot shows the 'Nodes' tab in the System Diagnostics section. It displays a summary bar for a 'LOCAL/SERVER' node. The summary bar includes status (Ok), conformance (Ok), current deployment (Small), and IP (Local). Below the summary bar is a table with various system metrics.

LOCAL/SERVER				Status: Ok	Conformance: Ok	Current Deployment: Small	IP: Local	Flow Data Status																	
CPU	Model	Intel(R) Xeon(R) CPU E5-2660 v4 @ 2.00GHz	Cores	32	OS UTIL.	2.1 %	OS RAM	Amount	31.40 GB	JVM RAM	Committed	16.00 GB	DISK	Total	249.88 GB	RTT	Server to Node	N/A	DEVICES	Total	35	Configurable	0	Loading	0
					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.

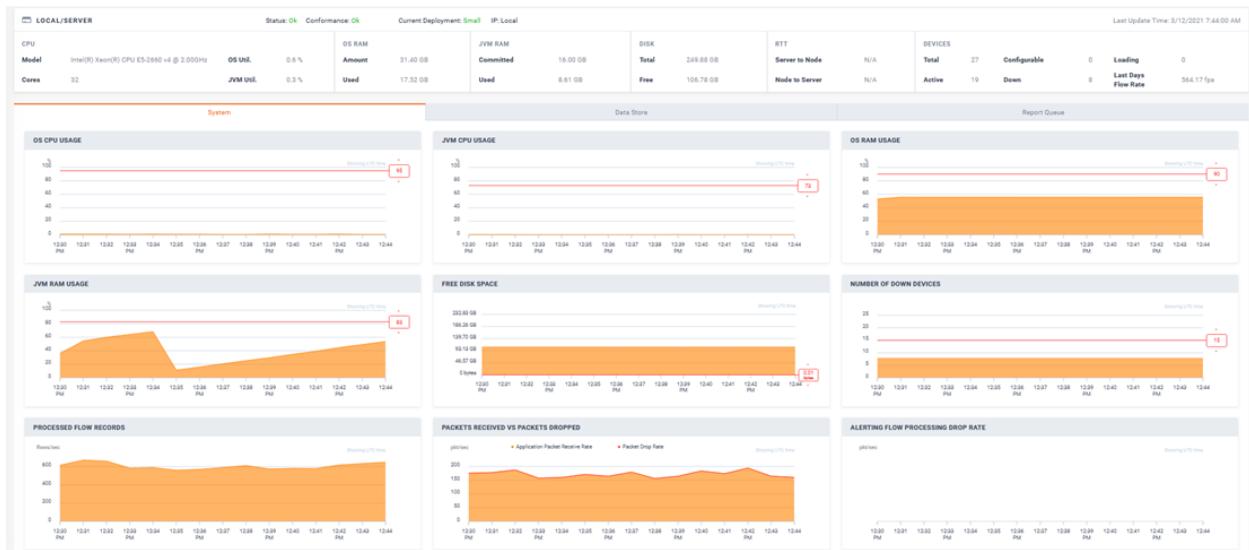
The screenshot shows the 'Nodes' tab with the summary bar expanded. The expanded view shows more details for the 'LOCAL/SERVER' node, including CPU model, cores, OS utilization, OS RAM, JVM RAM, disk usage, and RTT.

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

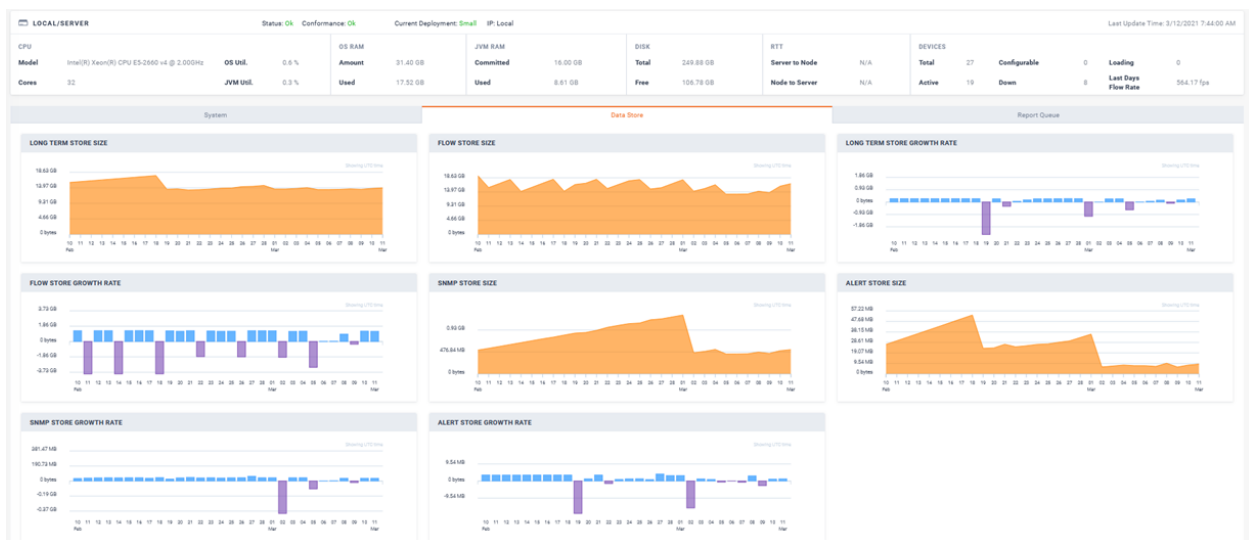
- System
- Data Store

- 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.

The screenshot shows the 'Report Queue' tab with a table of report details. The table has columns for Report Name, Report ID, Report State, User Name, Queue Type, Queued Time, and Running Time. There are also 'Cancel' and 'Cancel All' buttons at the top left of the table area.

Report Name	Report ID	Report State	User Name	Queue Type	Queued Time	Running Time
<input type="checkbox"/> Voice Analysis	9d0c42e-ad8f413c-9c12-c08a83d819d0	Running	[User Icon]	Priority 4	<1 second	1 minute 3 seconds
<input type="checkbox"/> IRAN	19666931-13d-dae1f3c-93f0-b88547e65d8	Running	[User Icon]	Priority 4	<1 second	44 seconds
<input type="checkbox"/> Favorite Applications	aa645d47-ed95-4bc7-0d9a-ee8c3f9c08de	Running	[User Icon]	Priority 4	<1 second	33 seconds
<input type="checkbox"/> WAN Capacity Planning	ba272813-d695-4851-b13d-09683418ac7	Queued	[User Icon]	Priority 4	20 seconds	-
<input type="checkbox"/> Voice/Video Performance Vs. Network Perform...	06907d933b5c-4cc7-4da7-120447900de7	Queued	[User Icon]	Priority 4	7 seconds	-

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

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

REPORT NAME	REPORT ID	REPORT STATE	USER NAME	QUEUE TYPE	QUEUED TIME	RUNNING TIME
Voice Analysis	9c0c42a-e8f4130-6c12-e8a8b388980	Running	admin	Priority 4	<1 second	1 minute 3 seconds
WAN	19-d66931-13dc-4a4f-932f-68b664c7e75c8	Running	admin	Priority 4	<1 second	14 seconds
Favorite Applications	aa4464d7-e83c-4b47-8bae-ea8b5f9f80e	Running	admin	Priority 4	<1 second	33 seconds
WAN Capacity Planning	ba272813-d495-4851-8136-0f9882418ac7	Queued	admin	Priority 4	20 seconds	-
Voice/Video Performance Vs. Network Perform...	06307c33-85b0-4cc7-a4e7-120447600ecf	Queued	admin	Priority 4	7 seconds	-

Flow Data Status

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

NODE	DEVICE COUNT	FLOW COUNT	FLOW RATE (FPS)
All	Device Count	Flow Count	Flow Rate (fps)
Local		35	0

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.

- Settings
- System Diagnostics
- User Management
- LiveNX Server

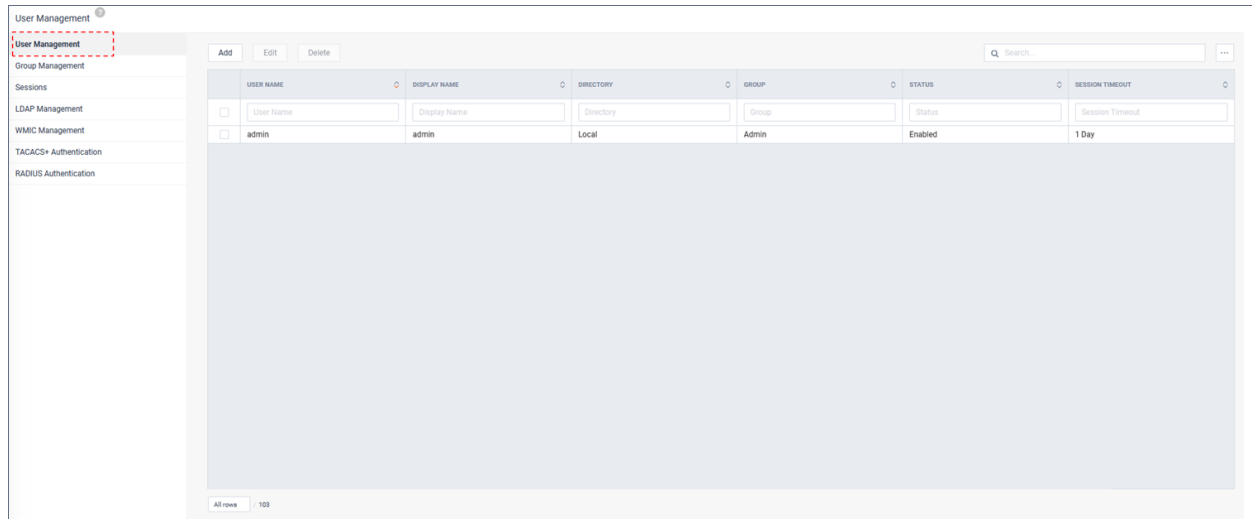
User accounts can be authenticated locally or LiveNX can integrate with external user repositories for user authentication. Today, LiveNX supports the following external authentication methods:

- LDAP
- RADIUS
- TACACS+
- SSO

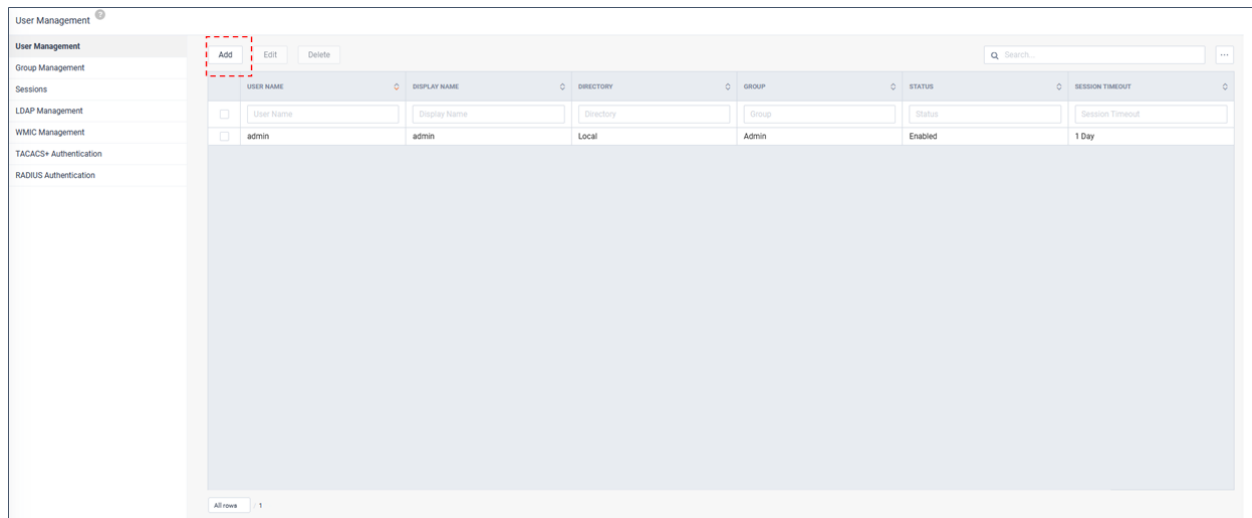
Please review this chapter for configuring LiveNX to these external repositories.

All user account authorization is done in LiveNX via Groups.

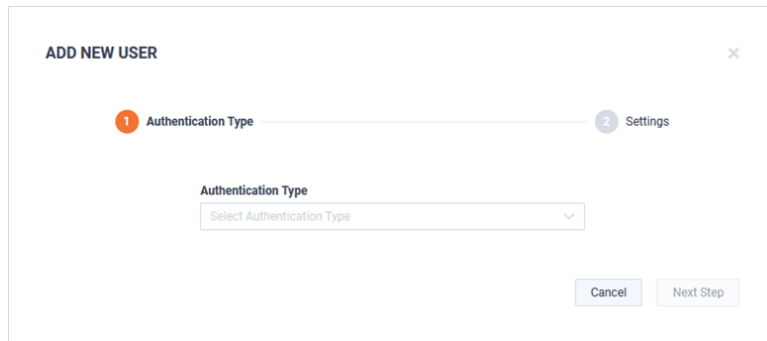
The *User Management* tab is where users are added to the system and managed.



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

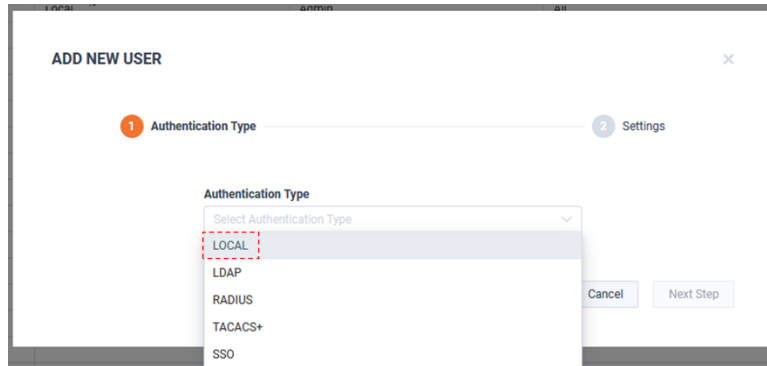


The *Add New User* modal appears.

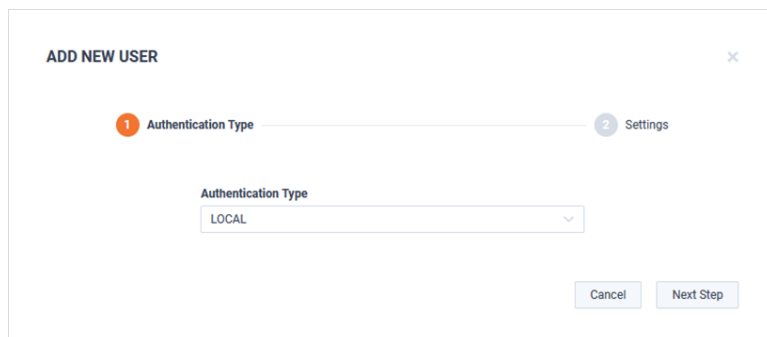


The screenshot shows the 'ADD NEW USER' form with a progress indicator showing '1 Authentication Type' and '2 Settings'. The 'Authentication Type' dropdown menu is open, displaying the text 'Select Authentication Type' and a downward arrow.

Select the *Authentication Type* and click **Next Step**.



The screenshot shows the 'ADD NEW USER' form with the 'Authentication Type' dropdown menu open. The 'LOCAL' option is highlighted with a red dashed box. The other options listed are LDAP, RADIUS, TACACS+, and SSO.



The screenshot shows the 'ADD NEW USER' form with the 'Authentication Type' dropdown menu closed and 'LOCAL' selected. The progress indicator shows '1 Authentication Type' and '2 Settings'.

Define the user:

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

ADD NEW USER
✕

✔ Authentication Type
 2 Settings

Username *

Display Name *

Group *

Session Timeout *

Choose Password *

Repeat Password *

Back
Add User

When finished, click **Add User**.

ADD NEW USER
✕

✔ Authentication Type
 2 Settings

Username *

Display Name *

Group *

Session Timeout *

Choose Password *

Repeat Password *

Back
Add User

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

User Management
⊕

- User Management
- Group Management
- Sessions
- LDAP Management
- WMIC Management
- TACACS+ Authentication
- RADIUS Authentication

Add Edit Delete
Search

USER NAME	DISPLAY NAME	DIRECTORY	GROUP	STATUS	SESSION TIMEOUT
<input type="checkbox"/> User Name	<input type="text" value="Display Name"/>	<input type="text" value="Directory"/>	<input type="text" value="Group"/>	<input type="text" value="Status"/>	<input type="text" value="Session Timeout"/>
<input type="checkbox"/> admin	admin	Local	Admin	Enabled	1 Day
<input type="checkbox"/> alex	alex2	Local	View	Enabled	15 Minutes

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

User Management
⊕

- User Management
- Group Management
- Sessions
- LDAP Management
- WMIC Management
- TACACS+ Authentication
- RADIUS Authentication

Add Edit Delete
Selected: 1
Search

USER NAME	DISPLAY NAME	DIRECTORY	GROUP	STATUS	SESSION TIMEOUT
<input type="checkbox"/> User Name	<input type="text" value="Display Name"/>	<input type="text" value="Directory"/>	<input type="text" value="Group"/>	<input type="text" value="Status"/>	<input type="text" value="Session Timeout"/>
<input type="checkbox"/> admin	admin	Local	Admin	Enabled	1 Day
<input checked="" type="checkbox"/> alex	alex2	Local	View	Enabled	Never

EDIT USER

Username: alex

Display Name: alex2

Group: View

Status: Enabled

Directory: Local

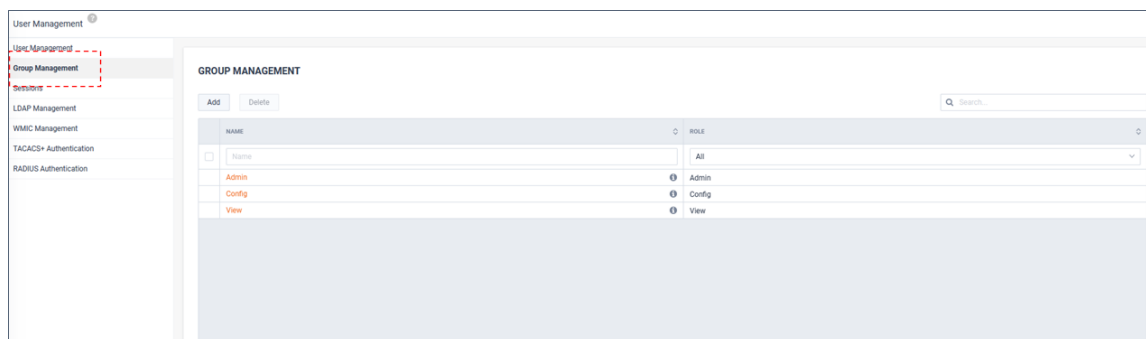
Session timeout: Never

Choose Password *: Add password

Repeat Password *: Confirm password

Buttons: Cancel, Save Changes

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



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*. Their 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 limited level than admin. An example is that a “config” 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 style="list-style-type: none"> In the Operations Dashboard: Config can optionally manage Devices, Custom Applications, Filters, Site In the Engineering Console: Config can optionally control CLI GUIs (ie. Manage QoS, IP SLA, ACLs, PBR, etc.)
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:

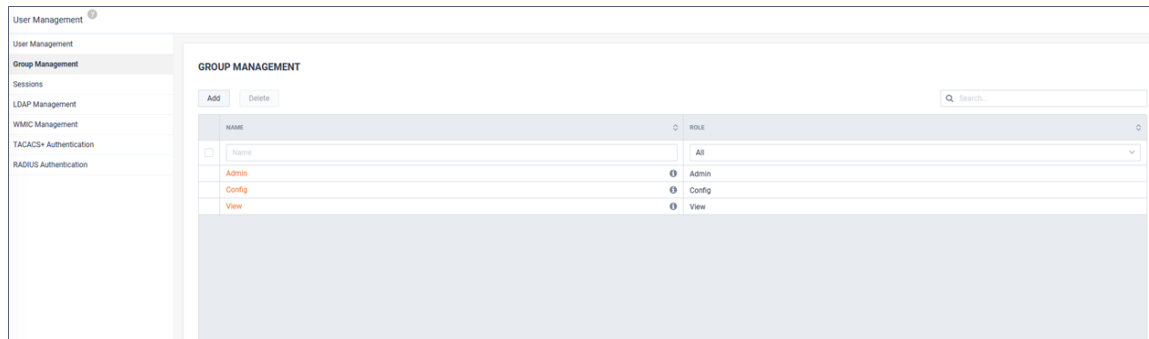
Section	Page	Required Page Access	Required Role
Configure	Alert Management	–	config/admin
Configure	Application Management	Application Management	config/admin
Configure	OID Polling	OID Polling	config/admin
Configure	Device Management	Device Management	config/admin
Configure	Filter Management	Filter Management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

Users

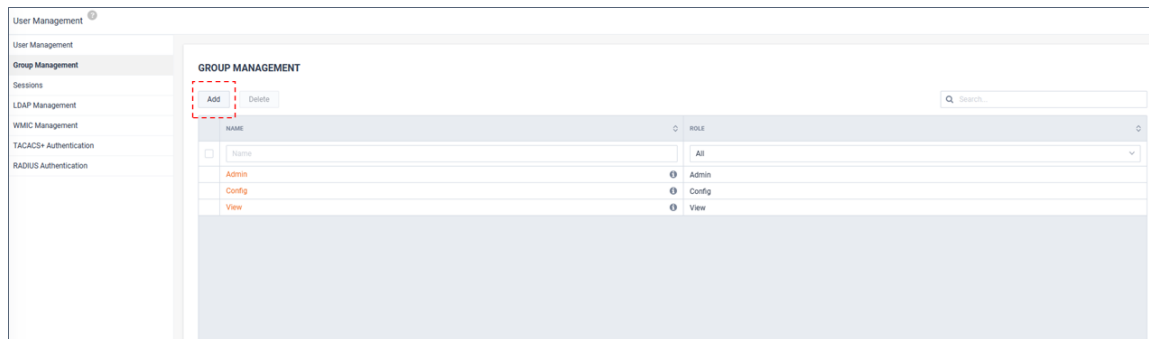
Defines which LiveNX users are a member of the group.

Adding a New Group

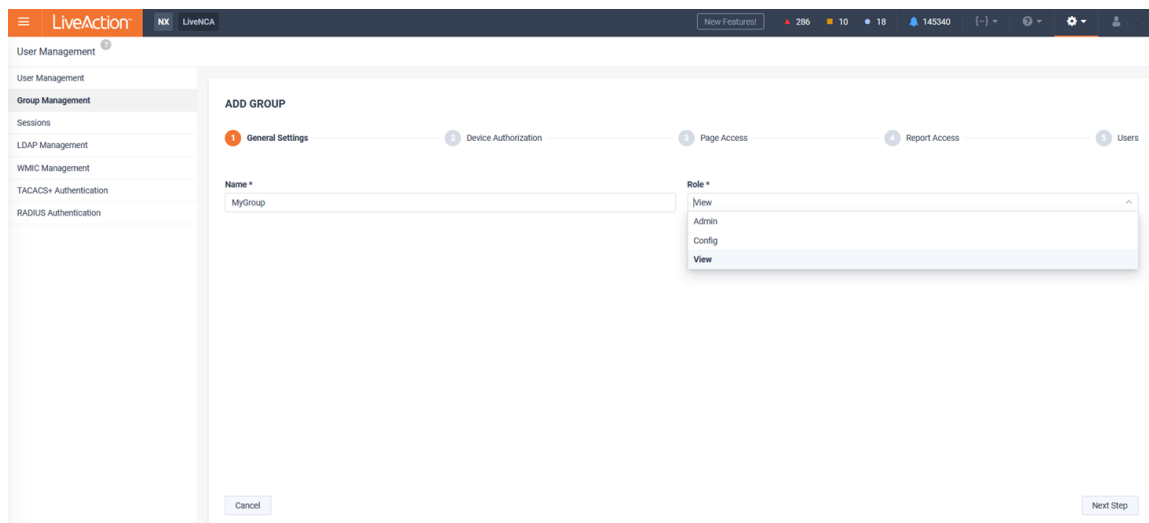
By default, there are three Groups: *Admin*, *Config*, and *View*. Each is assigned the role that corresponds to the Group's name. These default roles have no device or page restrictions and cannot be deleted. Additional roles can be added and customized to meet a specific Group's needs.



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



2. Provide a Name and Role.



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 filters, click **Add**.

The screenshot shows the 'ADD GROUP' configuration page in the LiveAction dashboard. The 'Device Authorization' step is selected. The 'Group is authorized to:' section has three radio buttons: 'View with CLI access all devices', 'Only view all devices', and 'Use specific filters' (which is selected). Below this are 'Add', 'Edit', and 'Delete' buttons and a search box. A table with columns 'ENTITY TYPE', 'VALUES', and 'CLI ACCESS' is present. The table contains one row with 'Entity Type' and 'Values' in the first two columns, and 'All' in the third. Below the table, a message reads 'Specific Filter Options Table No Filters: All devices are hidden'. At the bottom, there are 'Cancel', 'Previous Step', and 'Next Step' buttons.

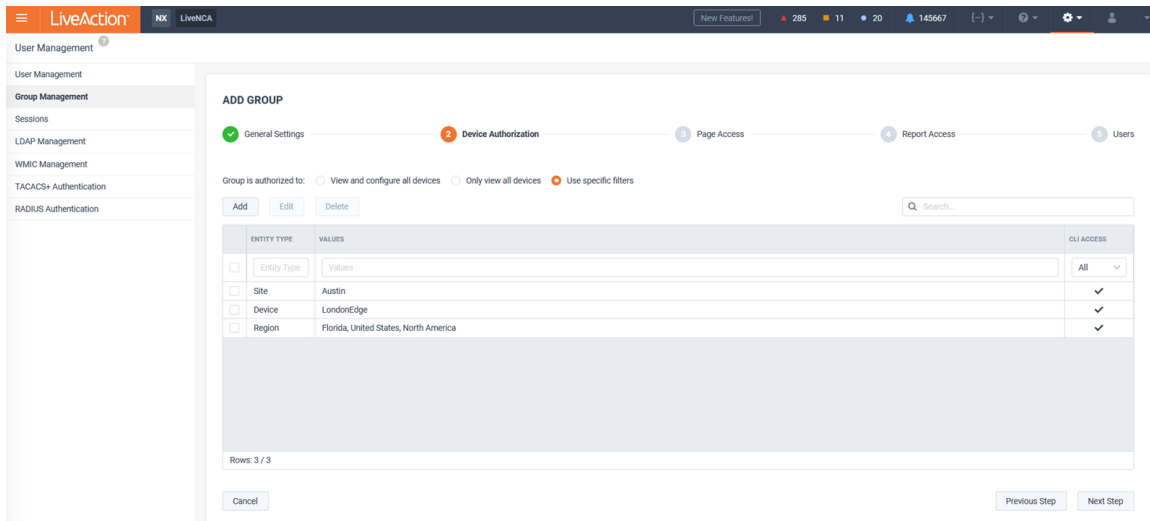
Filters can be applied by *Device*, *Site*, or *Region*.

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

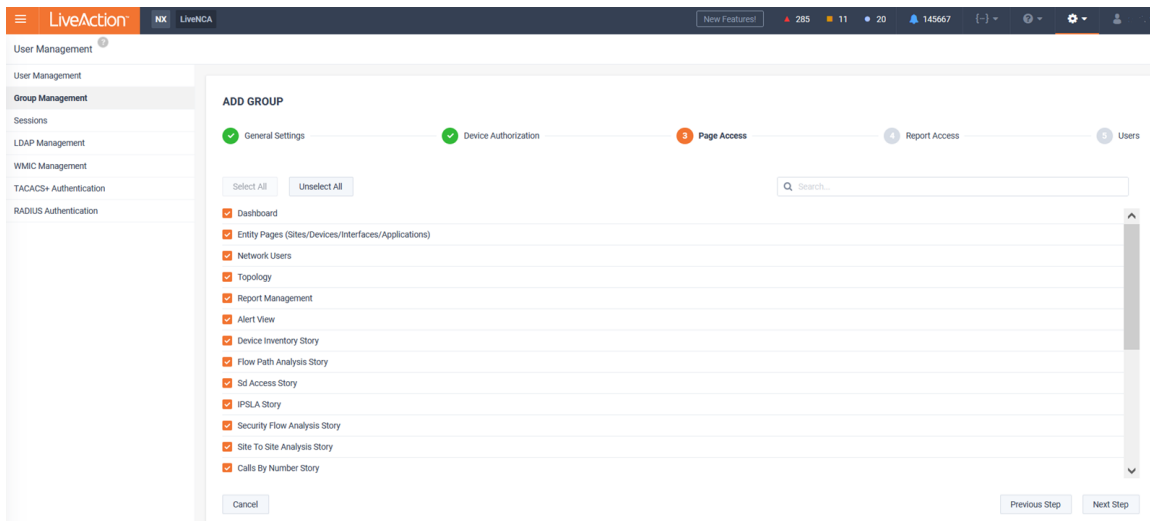
The screenshot shows the 'ADD DEVICE AUTHORIZATION' dialog box. The 'Site' field is set to 'Austin'. There is a checkbox for 'CLI Access for managing QOS, IPSLA, etc. in the Engineering Console.' which is unchecked. 'Cancel' and 'Add' buttons are at the bottom.

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

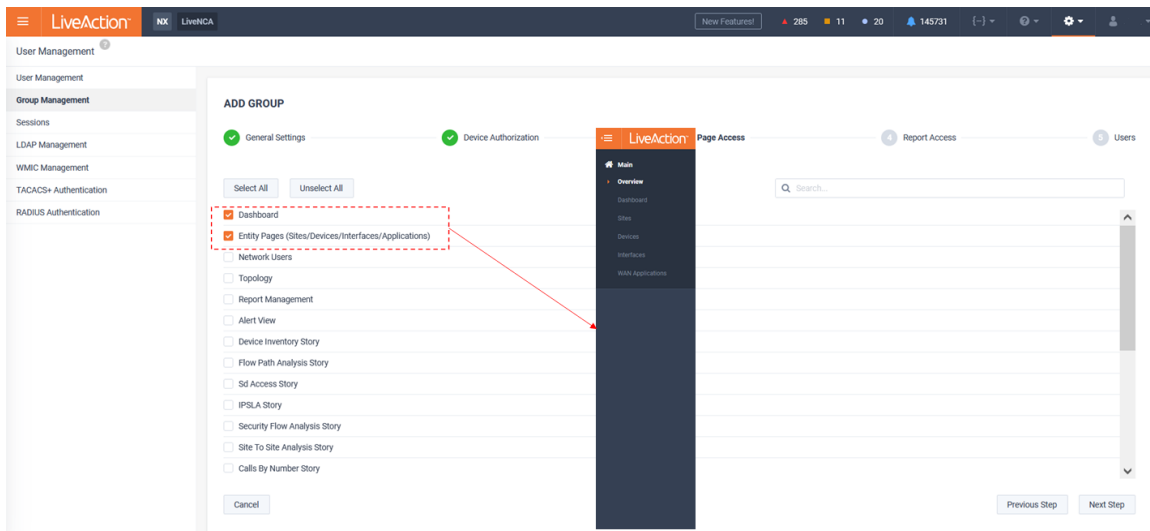
- Site=Austin
- Device=LondonEdge
- Region=Florida



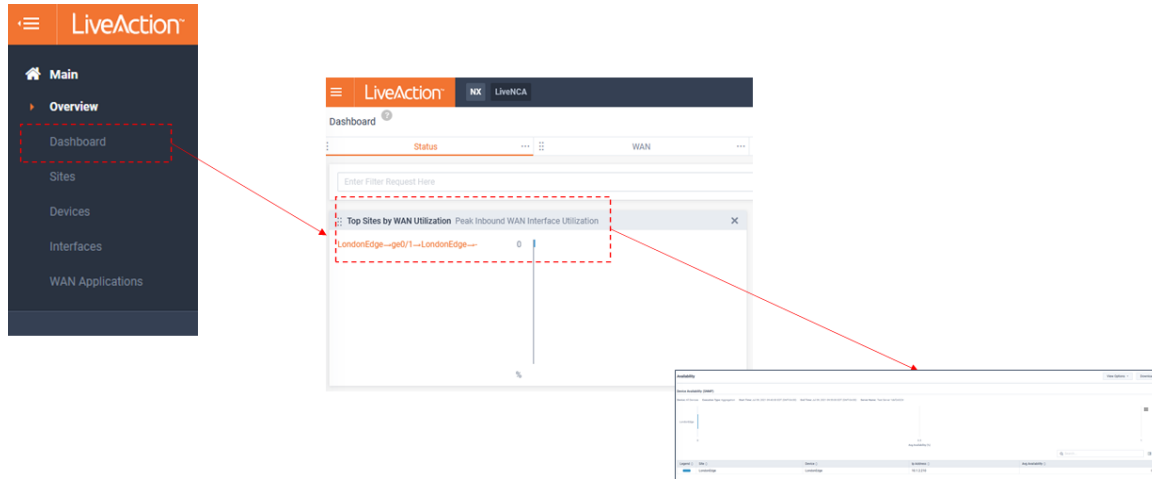
4. Assign Operations Dashboard (WebUI) page access.



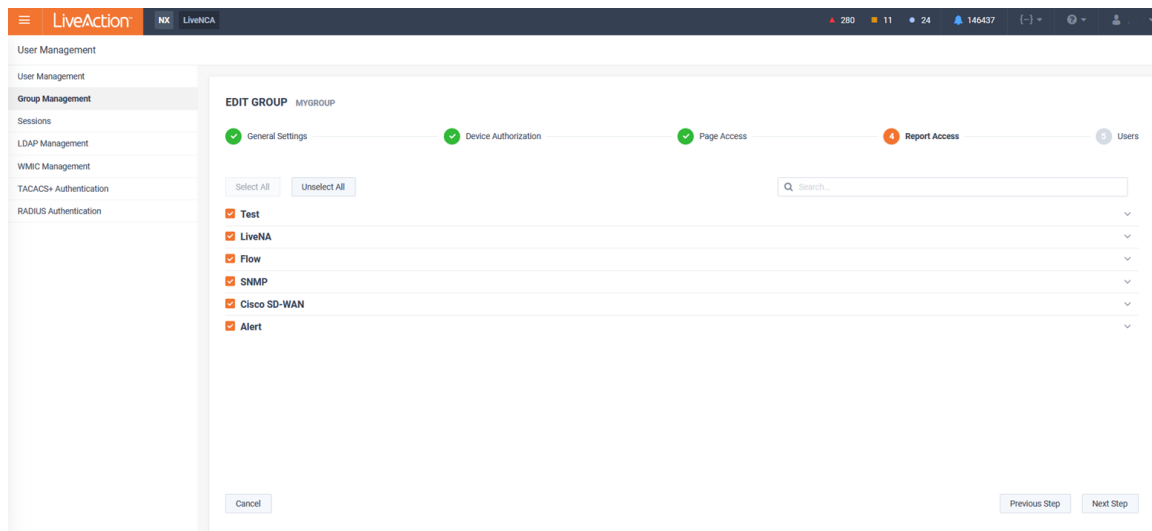
In this example, only Dashboards and Entity Pages (*Sites/Devices/Interfaces/WAN Applications*) will be available for this Group.



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.

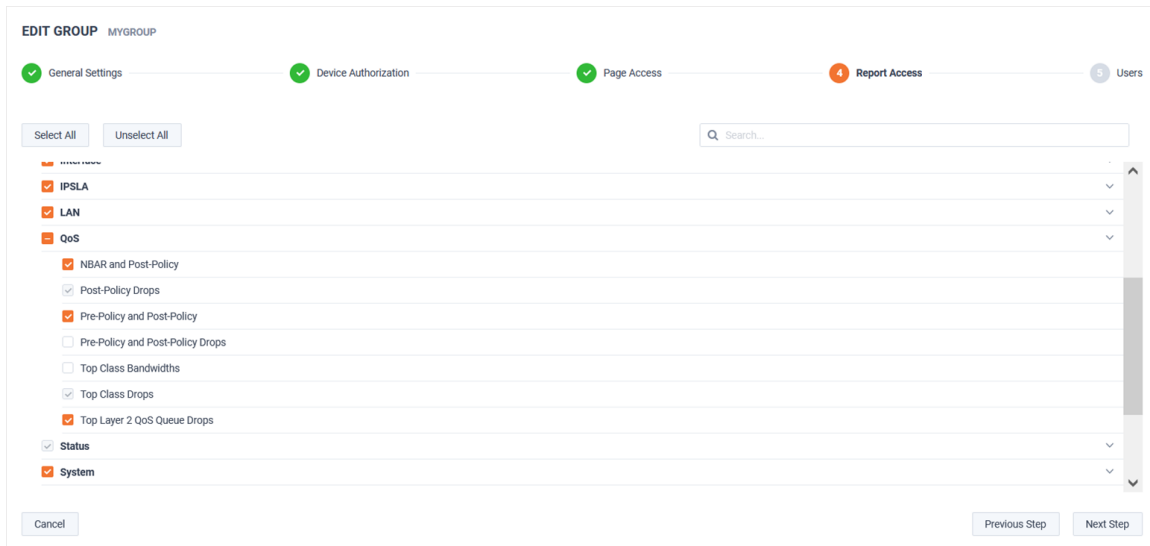


5. Select which reports are available to the group. By default, all reports are available.

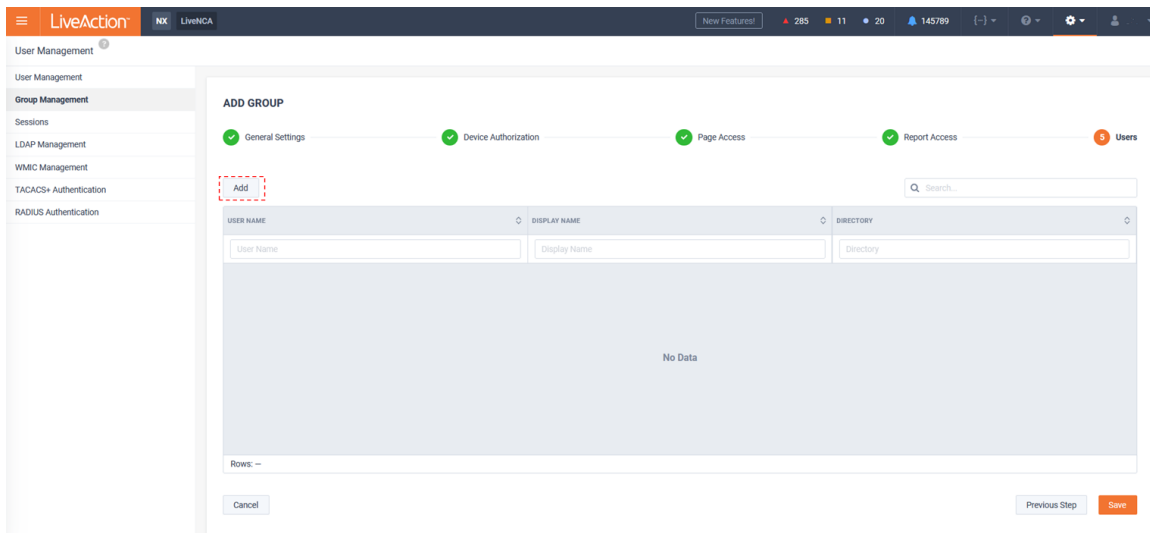


Optionally, deselect any report that should not be available to the group.

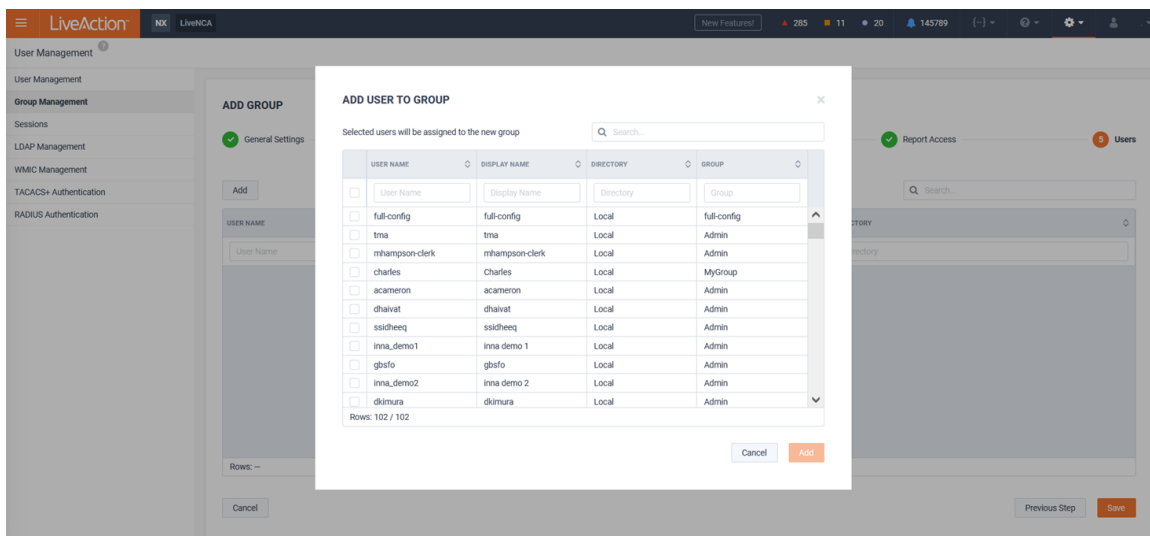
Note Some reports that drive fundamental workflows cannot be deselected.



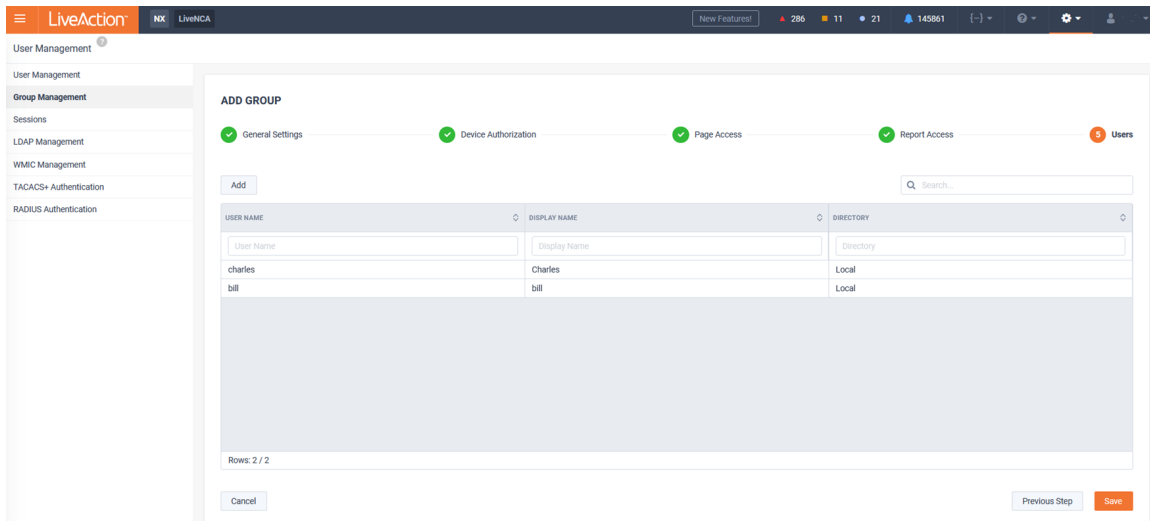
6. Add user(s) to group by clicking **Add**.



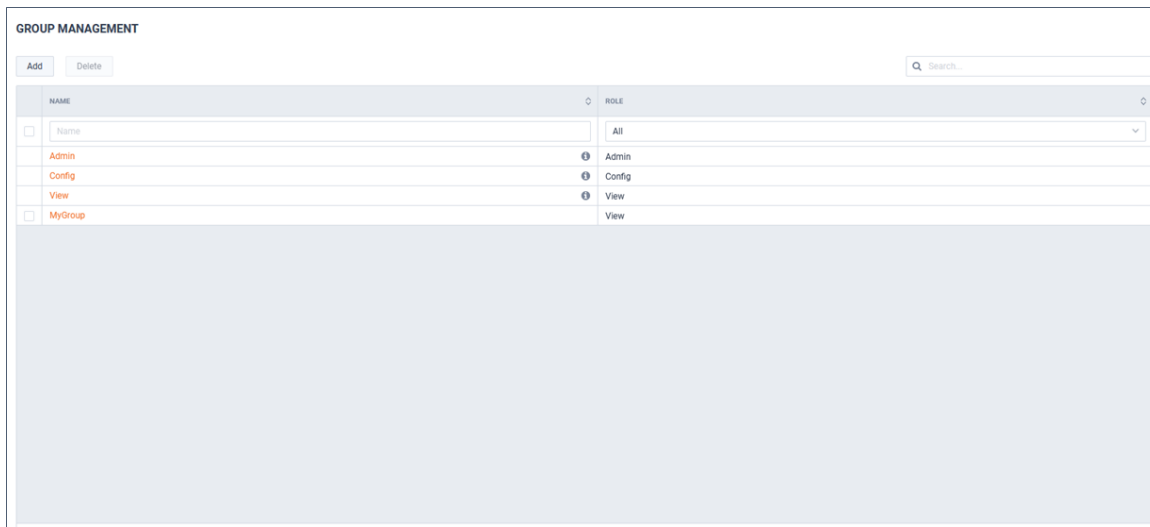
Select the users of interest and click **Add**.



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

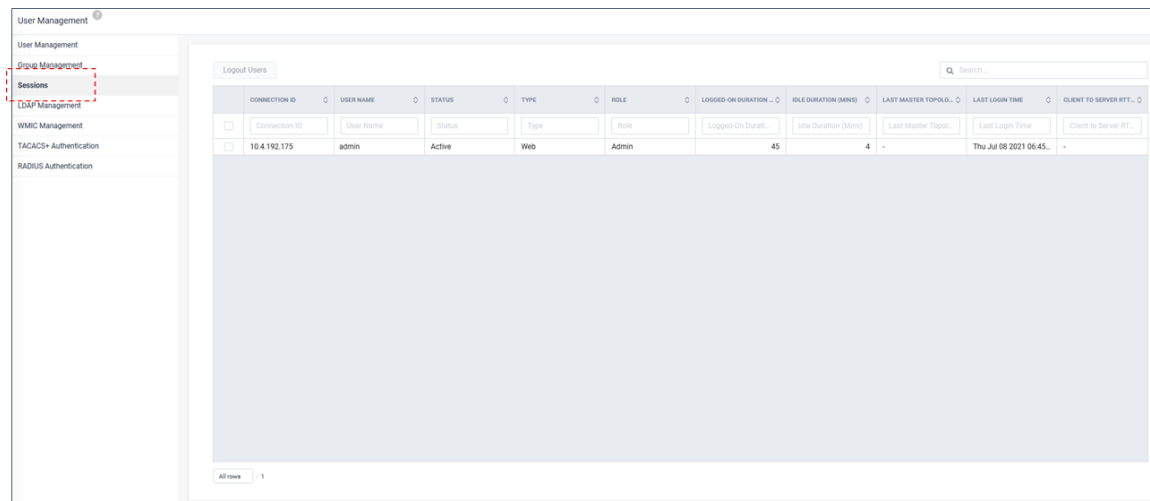


The new Group is now listed on the *Group Management* page.



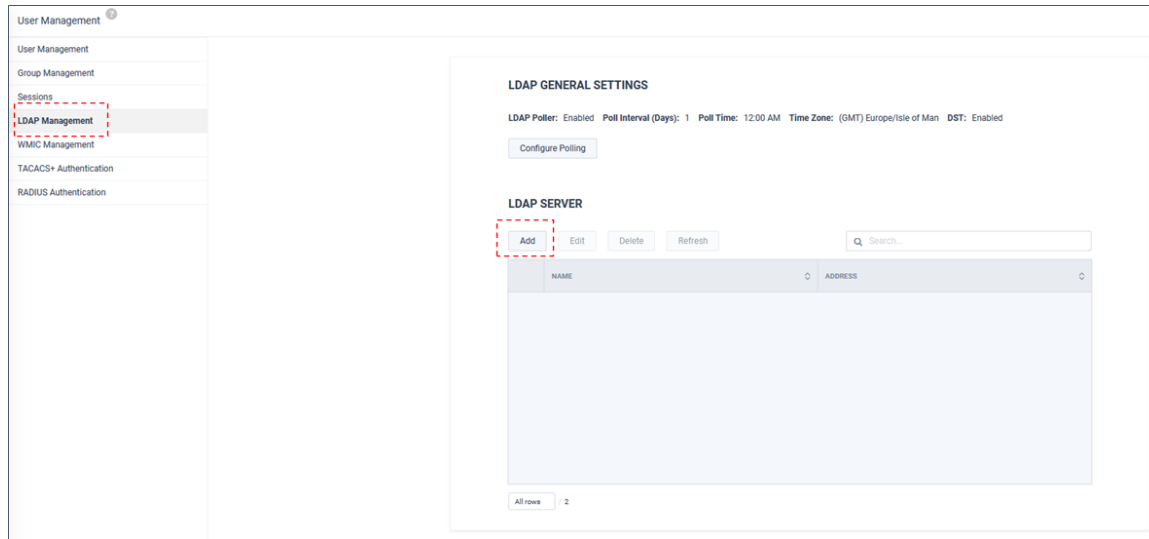
Sessions

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**.



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

ADD LDAP SERVER
✕

Main Settings
Advanced Setting

Name *

Search Base *

LDAP Server Address/Hostname *

Auto Add/Update Users

LDAP Server Port

SSL/TLS

Group

Identity *

+ Add Additional Search Base

Password *

Cancel
Save

If necessary, click **+ Add Additional Search Base**.

ADD LDAP SERVER
✕

Main Settings
Advanced Setting

Name *

Search Base *

LDAP Server Address/Hostname *

Auto Add/Update Users

LDAP Server Port

SSL/TLS

Group

Identity *

Search Base *

Auto Add/Update Users

Group

Password *

+ Add Additional Search Base

Cancel
Save

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**.

EDIT
✕

Main Settings

Advanced Setting

Username *

User Search String *

Display name *

Group Search String *

Cancel
Update

The LDAP Server will be listed.

- User Management
- User Management
- Group Management
- Sessions
- LDAP Management
- WMIC Management
- TACACS+ Authentication
- RADIUS Authentication

LDAP GENERAL SETTINGS

LDAP Poller: Enabled Poll Interval (Days): 1 Poll Time: 12:00 AM Time Zone: (GMT) Europe/Isle of Man DST: Enabled

Configure Polling

LDAP SERVER

Add
Edit
Delete
Refresh
Q Search...

	NAME	ADDRESS
<input type="checkbox"/>	Name	Address
<input type="checkbox"/>	LiveAction	ldap://10.0.0.10

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

- User Management
- User Management
- Group Management
- Sessions
- LDAP Management
- WMIC Management
- TACACS+ Authentication
- RADIUS Authentication

LDAP GENERAL SETTINGS

LDAP Poller: Enabled Poll Interval (Days): 1 Poll Time: 12:00 AM Time Zone: (GMT) Europe/Isle of Man DST: Enabled

Configure Polling

LDAP SERVER

Add
Edit
Delete
Refresh
Selected: 1 Q Search...

	NAME	ADDRESS
<input type="checkbox"/>	Name	Address
<input checked="" type="checkbox"/>	LiveAction	ldap://10.0.0.10

EDIT
✕

Main Settings

Advanced Setting

Name *

Search Base *

LDAP Server Address/hostname *

Base

+ Add Advanced search base

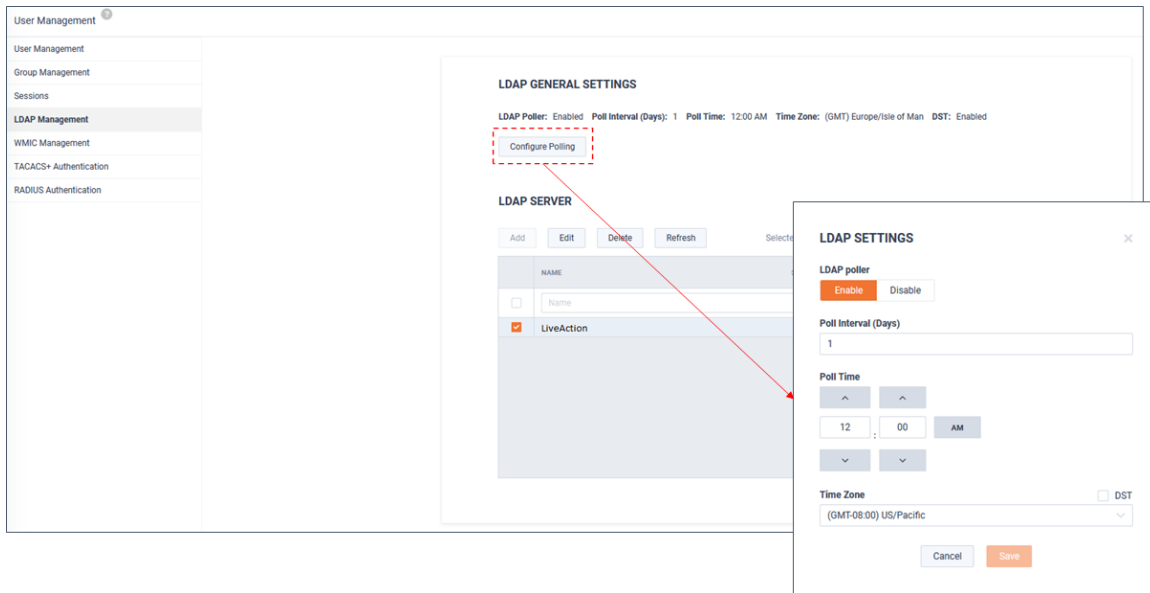
LDAP Server Port

Identity *

Password *

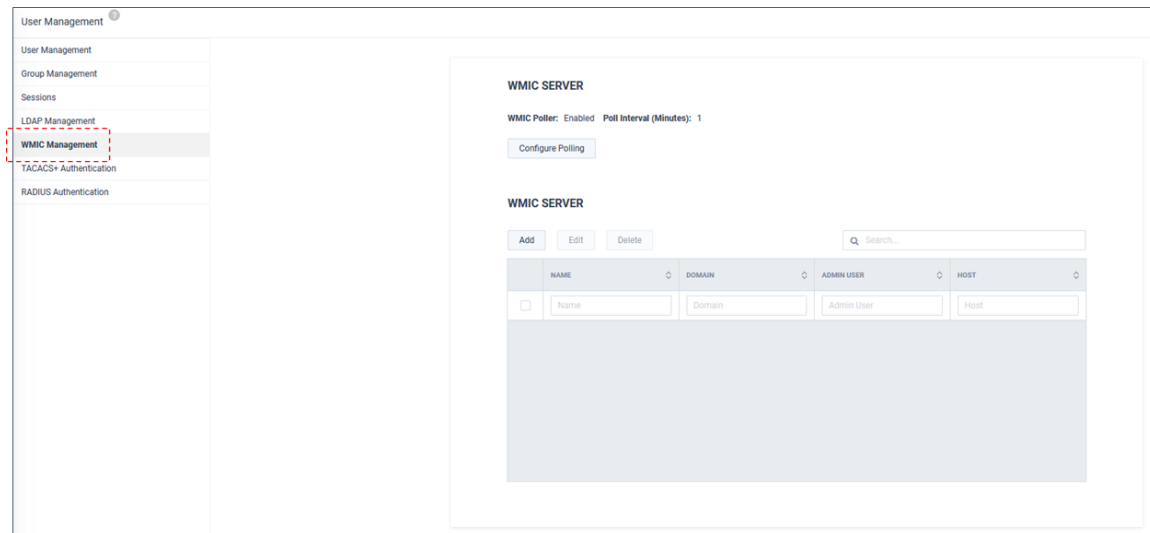
Cancel
Update

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

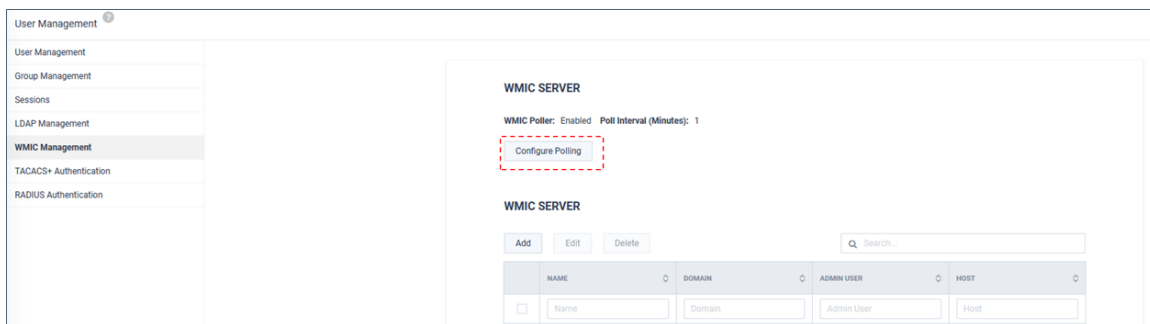


WMIC Management

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.



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



After making changes, click **Save**.

WMIC SETTINGS

WMIC Poller

Poll Interval (Minutes)

To add an WMIC server, click **Add**.

User Management

- User Management
- Group Management
- Sessions
- LDAP Management
- WMIC Management**
- TACACS+ Authentication
- RADIUS Authentication

WMIC SERVER

WMIC Poller: Enabled Poll Interval (Minutes): 1

WMIC SERVER

	NAME	DOMAIN	ADMIN USER	HOST
<input type="checkbox"/>	<input type="text" value="Name"/>	<input type="text" value="Domain"/>	<input type="text" value="Admin User"/>	<input type="text" value="Host"/>

Enter the configuration details and when finished, click **Save**.

ADD WMIC SERVER ✕

Name

Domain

Admin User

Password

Host

The server appears on the *WMIC General Settings* page.

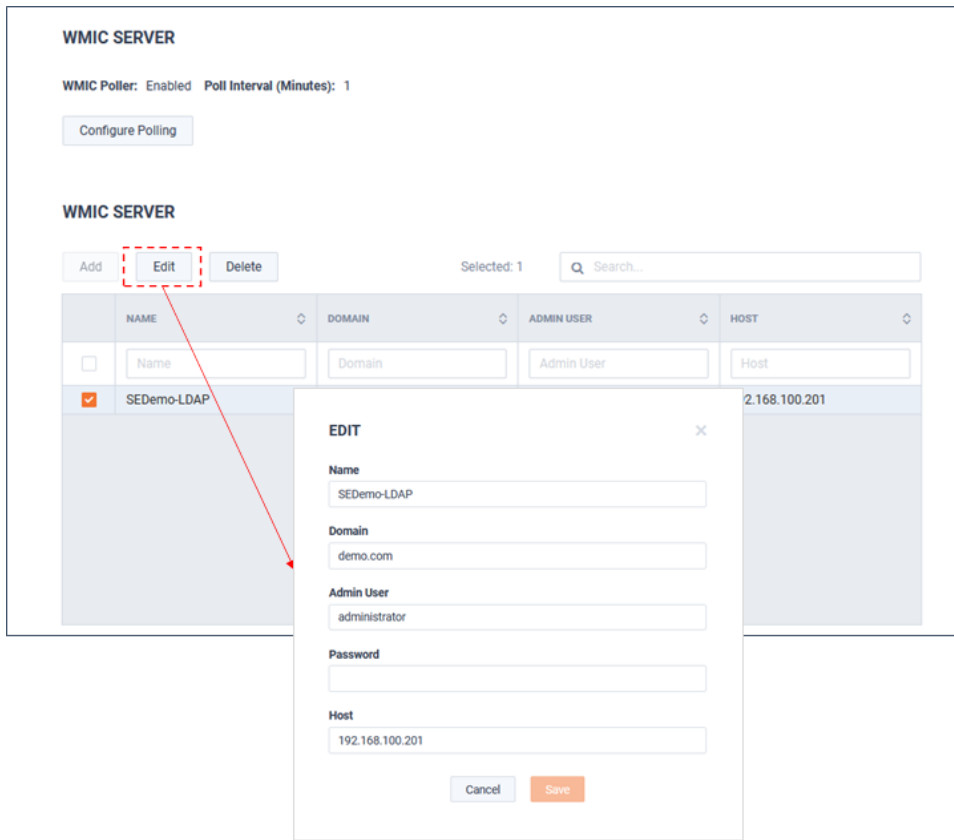
WMIC SERVER

WMIC Poller: Enabled Poll Interval (Minutes): 1

WMIC SERVER

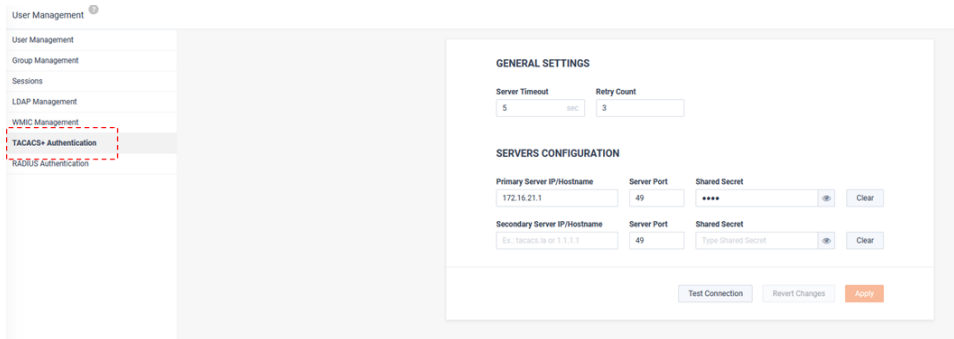
	NAME	DOMAIN	ADMIN USER	HOST
<input type="checkbox"/>	<input type="text" value="Name"/>	<input type="text" value="Domain"/>	<input type="text" value="Admin User"/>	<input type="text" value="Host"/>
<input type="checkbox"/>	SEDemo-LDAP	demo.com	administrator	192.168.100.201

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

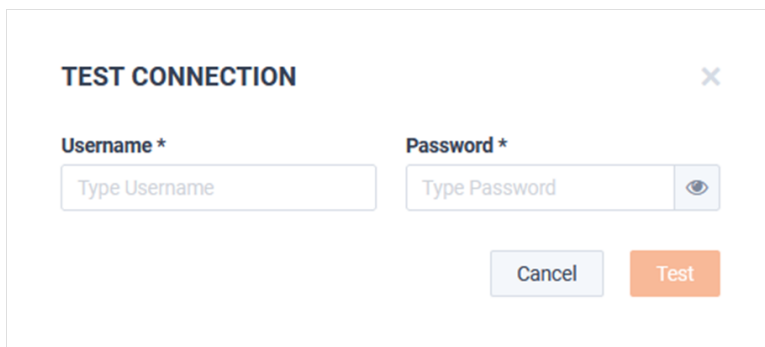


TACACS+ Authentication

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



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

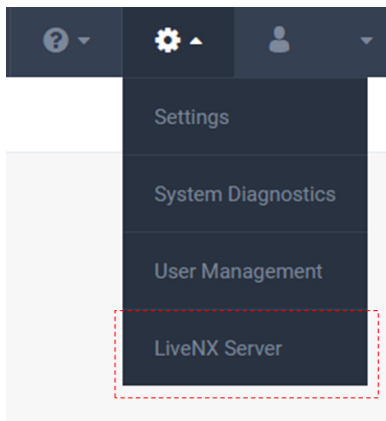


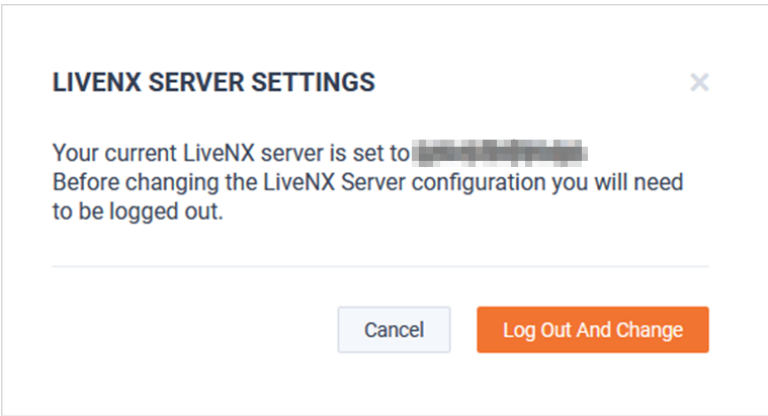
The *RADIUS Authentication* tab allows for the configuration of a Primary and Secondary RADIUS server with which LiveNX can use for authentication users.

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

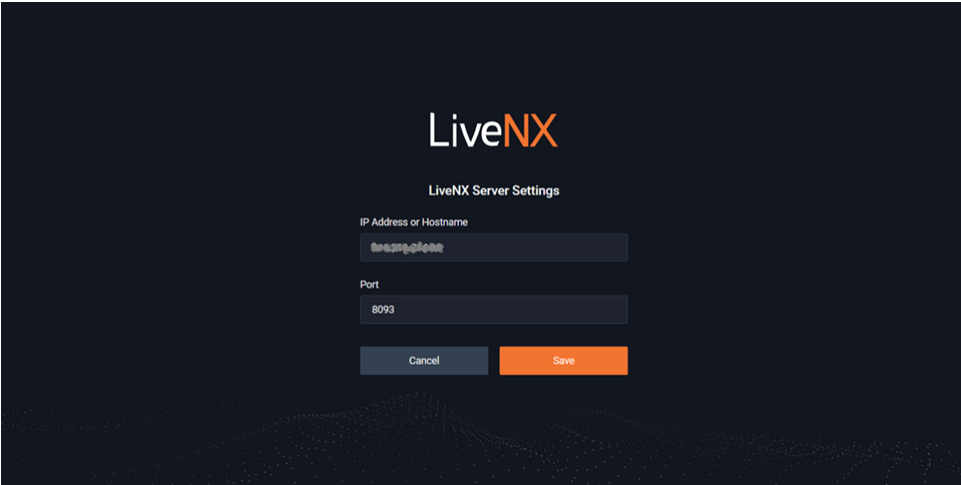
LiveNX Server

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**.





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



LiveNX Appliance

In this chapter:

<i>About LiveNX Appliance</i>	126
<i>What's Included</i>	126
<i>Front / Rear Panels</i>	127
<i>Inside LiveNX Appliance</i>	128
<i>Installing LiveNX Appliance</i>	129
<i>Connecting Extended Storage to LiveNX Appliance</i>	130
<i>Starting / Shutting Down LiveNX Appliance</i>	131
<i>Contacting LiveAction Support</i>	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	1U
Processor	2 x Intel® Xeon® Gold 5218
Base Frequency	2.30 GHz
Max Turbo Frequency	
Cores	16
Thread	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.

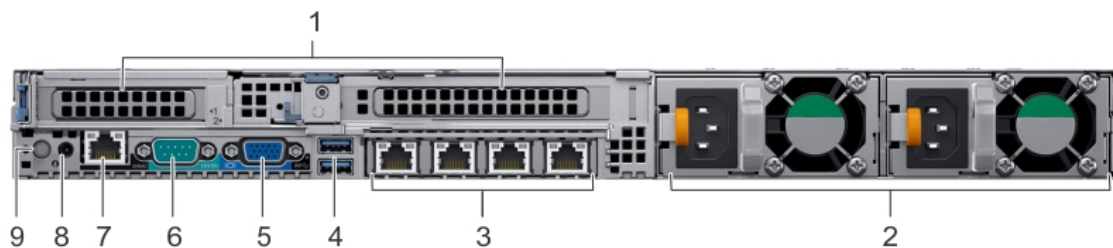
LiveNX Appliance Front Panel



Item	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



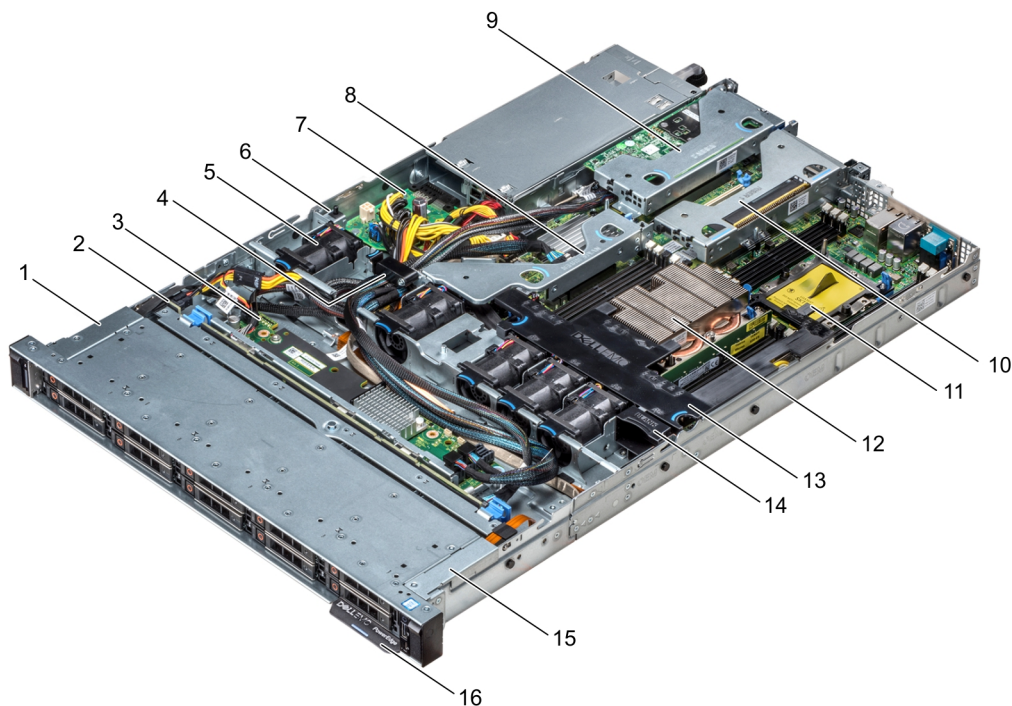
Item	Indicator, Button, or Connector	Description
1	Full height riser slot	Use the card slots to connect full-height PCIe expansion cards on full height riser.
2	Power supply unit (2)	AC 550 W. Both power supplies should be plugged in to power to provide redundancy.
3	Ethernet ports (4) (The port labeled '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 identify 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.

Item	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 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:

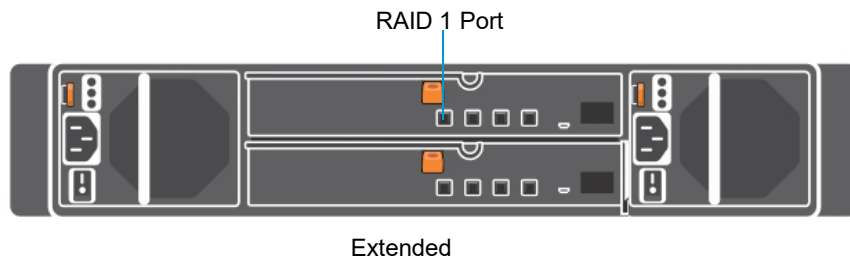
1. Make sure both Extended Storage and LiveNX appliance are powered OFF.
2. Select a suitable location for both Extended Storage and LiveNX appliance. Both units can be installed on a flat surface, or mounted in a standard 19-inch equipment rack.
3. Run the SAS external cascading cable between the units 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.



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 <https://www.liveaction.com/support/technical-support/> for instructions.