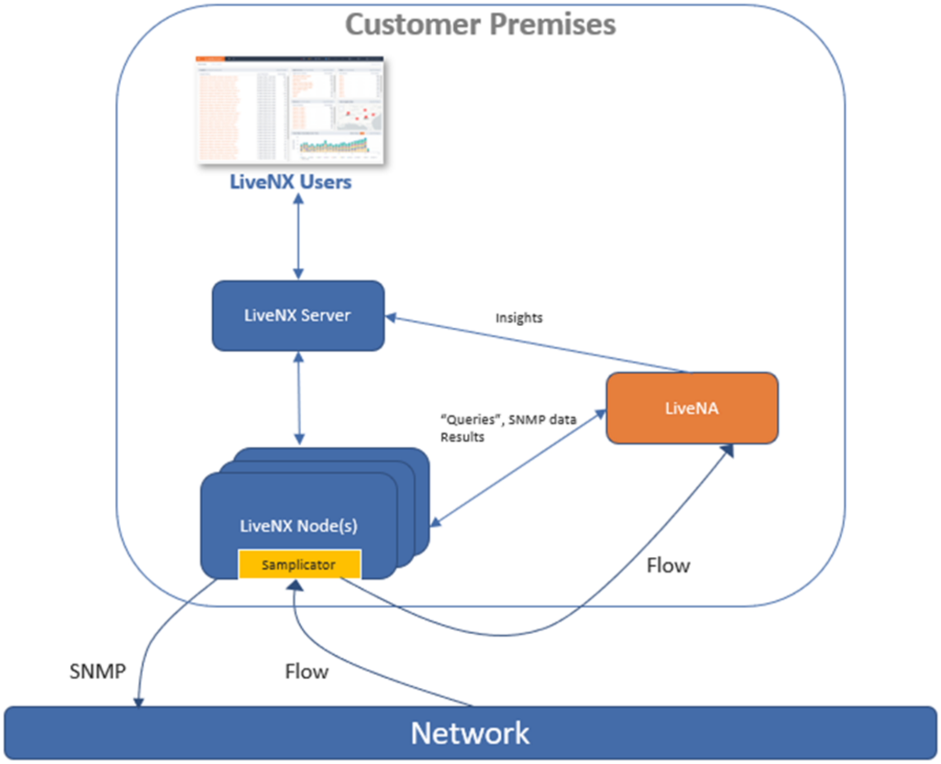
LiveNA Quick Start Guide

Introduction

This LiveNA Quick Start Guide will provide you with the necessary steps to set up the LiveNA software, as well as the network configuration needed to ensure LiveNA can integrate with LiveNX, collect relevant data from the network, and deliver enhanced Insights.

Integration and Component Architecture



LiveNA provides Insights for devices that are already monitored via LiveNX. It is a physical appliance that sits in parallel to LiveNX Node collectors. It usually resides in the same data center as LiveNX Node(s). It is accessed and configured via the LiveNX Operations Dashboard (WebUI). All management communication is accomplished via REST API. Any SNMP, Alert, or other data is used by LiveNA is accessed from LiveNX's datastores via REST API.

LiveNA also acts as a Flow collector. It does not request Flow data from LiveNX, but instead receives Flow directly from the monitored devices. It is recommended to use a UDP repeater such as the Samplicator that is included in LiveNX Nodes to efficiently and transparently deliver Flow the LiveNA Appliance.

Configuration

This following section details the steps necessary to integrate LiveNX and LiveNA together. At a high level, these steps are:

- Validate LiveNX Environment
- Install and Stage LiveNA Appliance
- Open Required Ports
- Configure NetFlow/ Samplicator
- Setup SSL certificate
- Create API Key
- Configure LiveNX to connect with LiveNA
- Add Devices to LiveNA
- Define Custom Application Groups (Optional)

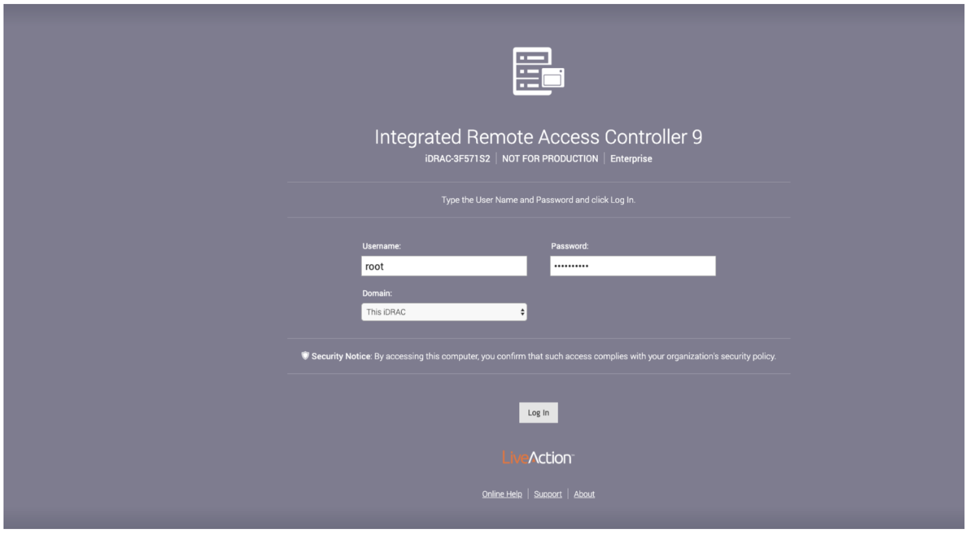
Validate LiveNX Environment

LiveNA is a system that provides further insights into the data available to LiveNX. It is assumed that LiveNX is already in place and successfully monitoring the network infrastructure via SNMP and NetFlow. For further information please visit: *https://community.liveaction.com/*

Install and Stage LiveNA Appliance

After installing the LiveNA physical appliance, the LiveNA console must be accessed to define the IP configuration for network connectivity. The LiveNA console is accessed via the Integrated Remote Access Controller (iDRAC) built into LiveNA appliance. iDRAC lets you remotely access the device as if you were in the same room as the platform. Using an Internet browser, you can easily perform tasks such as accessing a remote console, reimaging the platform, rebooting, shutting down, and powering up the device. By default, the IDRAC IP address is 10.10.10.22.

1. Log into iDRAC WebUI, the default credentials are: root/liveaction.



Integrated Remote Access Controller 9

iDRAC-3F571S2 | NOT FOR PRODUCTION | Enterprise

Type the User Name and Password and click Log In.

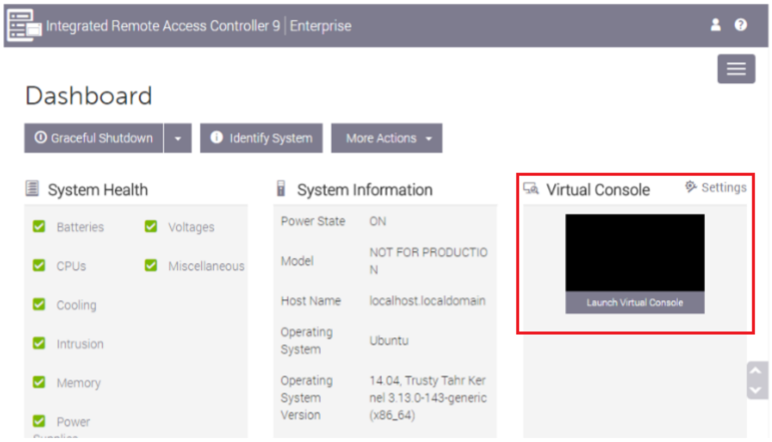
Username: root

Password: ••••••••••

Domain: This iDRAC

Security Notice: By accessing this computer, you confirm that such access complies with your organization's security policy.

2. Click on “Launch Virtual Console” (*Enable pop-up's if your browser blocks).



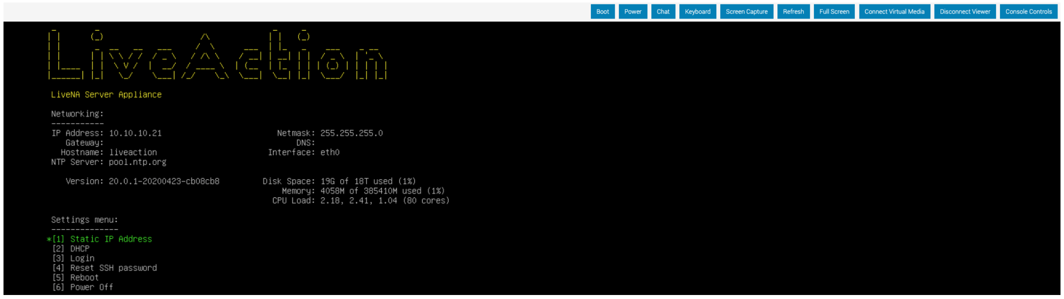
System Health

☑ Batteries ☑ Voltages
☑ CPUs ☑ Miscellaneous
☑ Cooling
☑ Intrusion
☑ Memory
☑ Power

System Information

Power State	ON
Model	NOT FOR PRODUCTION
Host Name	localhost.localdomain
Operating System	Ubuntu
Operating System Version	14.04, Trusty Tahr Kernel 3.13.0-143-generic (x86_64)

3. Select **[1] Static IP Address** to configure LiveNA's IP address, Netmask, Hostname, Gateway, DNS server(s), Interface, and NTP Server.



```
LiveNA Server Appliance

Networking:
-----------
IP Address: 10.10.10.21                    Netmask: 255.255.255.0
   Gateway:                                    DNS:
  Hostname: liveaction               Interface: eth0
NTP Server: pool.ntp.org

   Version: 20.0.1-20200423-cb08cb8       Disk Space: 19G of 18T used (1%)
                                              Memory: 4058M of 385410M used (1%)
                                            CPU Load: 2.18, 2.41, 1.04 (80 cores)

Settings menu:
--------------
*[1] Static IP Address
 [2] DHCP
 [3] Login
 [4] Reset SSH password
 [5] Reboot
 [6] Power Off
```

4. It is recommended to change the LiveNA shell access credentials by selecting "**[4] Reset SSH password**."

Open Required Ports

LiveNA utilizes a gRPC connection to the LiveNX server for all communication, but Flow. Flow is delivered directly via the infrastructure devices or via a UDP replicator. If a firewall(s) is in the connectivity path, it will require the following ports to be open to allow connectivity:

- UDP 123 – NTP
- UDP 161 – SNMP (optional)
- TCP 22 - SSH for cli
- TCP 8443 – Live admin
- TCP 34524 – gRPC API
- UDP 2055 – NetFlow/ IPFIX
- UDP 6343 – sFlow

Configure NetFlow / Samplicator

LiveNA acts as a NetFlow collector. Flow can either be sent directly to LiveNA by configuring additional Flow destination on the infrastructure devices or by a UDP repeater (preferred) such as Samplicator, which is included in the LiveNX Node Collectors. For further information please visit: *https://community.liveaction.com/*

Setup SSL Certificate

LiveNA and LiveNX communicate over a secure gRPC channel. This is secured using SSL. Out-of-the-box LiveNA generates a self-signed certificate, but a CA signed certificate can also be used and is recommended. This following section outlines how to install a CA Signed Certificate.

A. LiveNA SSL Certification Setup

1. Certificate verification – To ensure that the import of CA-signed certificate works as expected, the CN specified in the certificate should match with the host name of the LiveNA server. LiveNX should be able to reach LiveNA using that host name as well.
2. Access the LiveNA shell – Use ssh to access LiveNA's shell.
3. Copy CA-signed certificate to LiveNA – To copy the certificate and key files to LiveNA, it is recommended to use the tool such as scp to perform a secured network copy.

   To copy the certificate and its key, perform the following:

   ```
   $ scp [certificate] admin@[LiveNA IP]:/home/admin
   $ scp [key] admin@[LiveNA IP]:/home/admin
   ```

   where `[certificate]` is the path of the certificate file on the local machine, `[key]` is the path of the key file on the local machine, and `[LiveNA IP]` is the IP of the LiveNA Machine.
4. Convert the certificate into a java keystore format – LiveNA supports the certificates only in keystore format. Therefore, the first step is to convert the user's certificate file and key file into a keystore file:

   - On the LiveNA shell perform the following:

     ```
     $ openssl pkcs12 -export -in [certificate] -inkey [key] -name server -
     out livena-PKCS-12.p12
     ```

     where `[certificate]` is the file name of the certificate file, and `[key]` is the file name of the key file.
   - When prompted with the export password, use:

     ```
     3i3FGY7c1WMWqTz2RSKg
     ```

   This command will generate a file called `livena-PKCS-12.p12`. With `livena-PKCS-12.p12`, we import it into a keystore format file:

   - On the LiveNA perform the following:

     ```
     $ keytool -importkeystore -deststorepass 3i3FGY7c1WMWqTz2RSKg -
     destkeystore public-grpc-server-ca-signed.keystore -srckeystore
     livena-PKCS-12.p12 -srcstoretype PKCS12
     ```
   - When prompted with the source keystore password, use:

     ```
     3i3FGY7c1WMWqTz2RSKg
     ```

   This command will generate a file called `public-grpc-server-ca-signed.keystore.` This is the keystore file that LiveNA reads in for SSL connection.
5. Replace the self-signed certificate with the CA-signed certificate – With the new file `public-grpc-server-ca-signed.keystore`, we can replace the self-signed keystore file with the CA-signed keystore file.

   - First make a backup of the self-signed keystore file, if it exists:

     ```
     $ mv /data/livena/data/public-grpc-server.keystore ~/public-grpc-
     server-self-signed.keystore
     ```

- Next, move the new CA-signed keystore into the the data directory of LiveNA:
  ```
  $ cp public-grpc-server-ca-signed.keystore /data/livena/data/public-grpc-server.keystore
  ```

6. Restart LiveNA Server - Restart LiveNA server to load in the new keystore:

   ```
   $ sudo service livena restart
   ```

B. LiveNX SSL Certification Setup

1. Remove the self-signed truststore file – With LiveNA now using a CA-signed truststore file, LiveNX will need to drop the old self-signed truststore file if it exists. From the LiveNX shell, do the following:
   ```
   $ mv /data/livenx-server/data/live-insight-edge.truststore ~/live-insight-edge-self-signed.truststore
   ```

   This command moves the `live-insight-edge.truststore truststore` file to the home directory as a backup.

2. Restart LiveNX Server – Restart the LiveNX server to load in the new truststore configuration:
   ```
   $ sudo service livenx-server restart
   ```

Self-Signed Certificate

A self-signed certificate is already generated out-of-the-box based on a default network setup. This generated self-signed certificate assumes that the network interface that will be used to connect with LiveNX is eth0.

A. LiveNA SSL Certification Setup

1. Access the LiveNA shell – Use ssh to access LiveNA's shell.

2. Locate the self-signed certificate - The self-signed certificate, named public-grpc-client.cert, is in: */data/livena/data/public-grpc-client.cert*

   This certificate contains the identification of the LiveNA machine using the IP provided in the network interface.

3. Transferring the self-signed certificate to LiveNX - With the certificate, it needs to be transferred over to LiveNX so LiveNX can properly identify LiveNA through scp. In the example command below, we assume that the IP of LiveNX appliance is 10.0.0.1:

   ```
   $ scp /data/livena/data/public-grpc-client.cert admin@10.0.0.1:/data/livenx-server/data
   ```

   This command copies the certificate over the LiveNX machine into the directory:

   /data/livenx-server/data

4. Creating a truststore in LiveNX - Now that we have prepared the certificate for LiveNA, and copied it over the LiveNX, we need to set up a truststore in LiveNX to tell LiveNX to trust that certificate:

   ```
   $ cd /data/livenx-server/data
   $ keytool -import -trustcacerts -file public-grpc-client.cert -alias liveNxClient -keystore live-insight-edge.truststore -storepass 2pLTYHWlqlbZrLDFuBSi
   ```

   This command should generate live-insight-edge.truststore file under */data/livenx-server/data/ directory*

5. Create API Key - LiveNA comes with an executable called `auth-management`. This executable serves as the internal tool to create, list, and delete API keys within LiveNA. This key will be needed for by LiveNX during LiveNA configuration.

To create a key from the LiveNA shell, do the following:

```
$ auth-management -create LiveNX
Created client token for "LiveNX"
Client ID            Access Token
--------------------------------------------
LiveNX               AnnxerPFL8PLjewvJhV9PQSaDn1RmOThlY+njWzB+HU=
```

As the example shown above, a Client ID "LiveNX," with the API key `AnnxerPFL8PLjewvJhV9PQSaDn1RmOThlY+njWzB+HU=` was created.

For LiveNA to recognize the change, LiveNA will need to be restarted:

```
$ sudo service livena restart
```

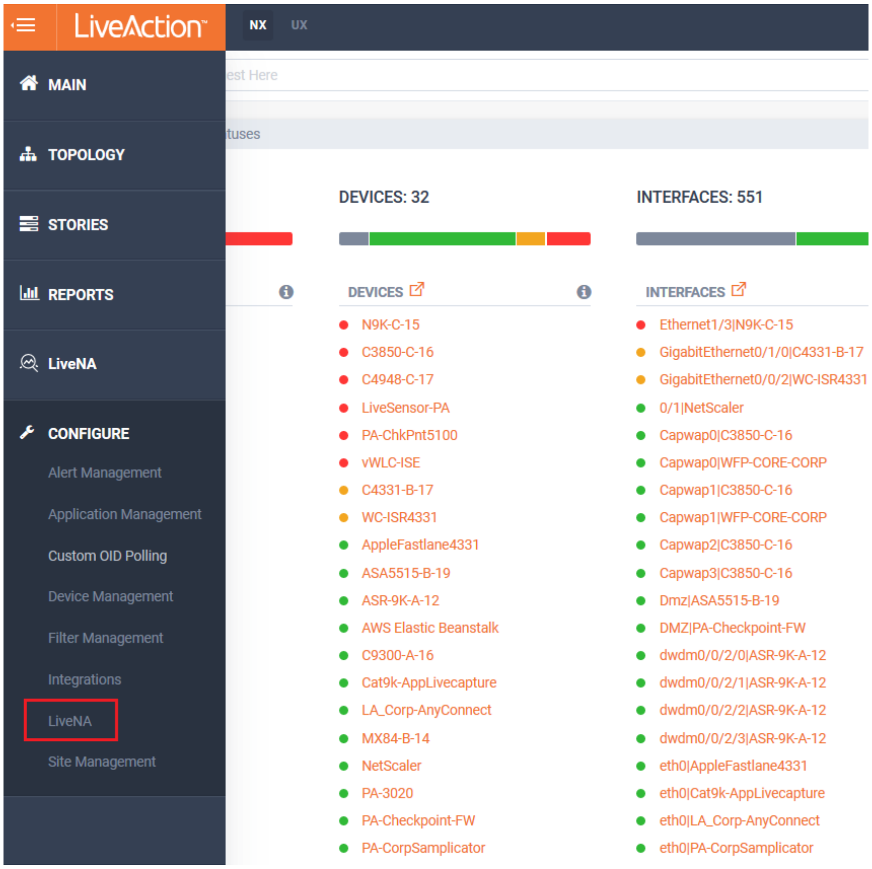
If a key has already been created, it can be viewed via:

```
$ auth-management -list
Client ID            Access Token
--------------------------------------------
LiveNX               AnnxerPFL8PLjewvJhV9PQSaDn1RmOThlY+njWzB+HU=
```

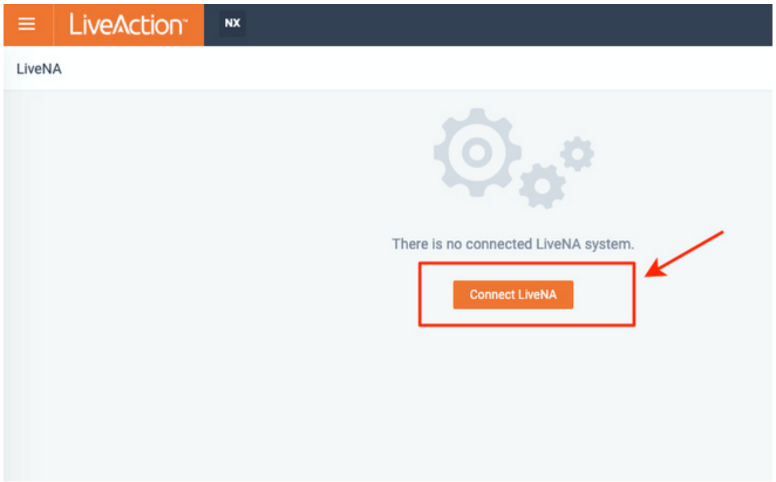
Configure LiveNX to connect with LiveNA

LiveNA is configured via the LiveNX Operations Dashboard (WebUI). To establish the connection:

1. Open LiveNX Operations Dashboard (WebUI).
2. Select **Configure > LiveNA**.



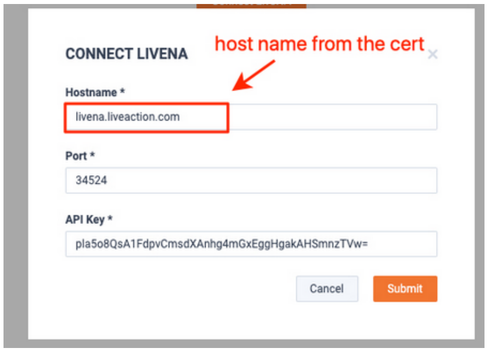
3. Click **Connect LiveNA**



There is no connected LiveNA system.

4. Enter the host name, port number, and API key of LiveNA.

Note The API key was created from LiveNA’s shell in the previous step.



CONNECT LIVENA

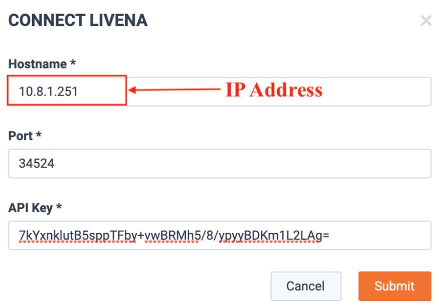
host name from the cert

Hostname *
livena.liveaction.com

Port *
34524

API Key *
pla5o8QsA1FdpvCmsdXAnhg4mGxEggHgakAHSmnzTVw=

Note For Self-Signed Certificate, use IP address instead of DNS name.



CONNECT LIVENA

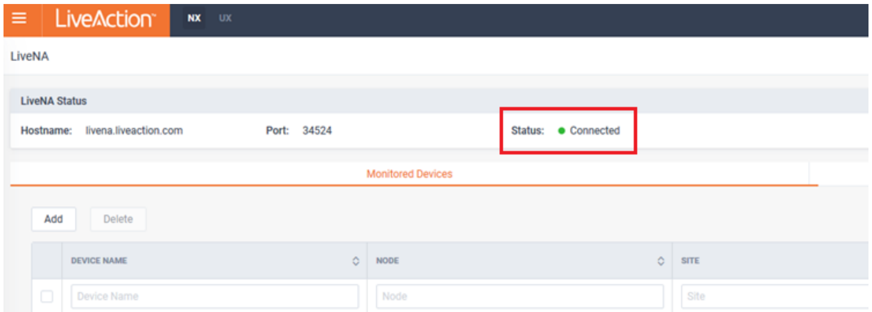
Hostname *
10.8.1.251

IP Address

Port *
34524

API Key *
7kYxnklutB5sppTFby+vwBRMh5/8/ypyyBDKm1L2LAg=

5. Verify the status is **Connected**



LiveNA Status

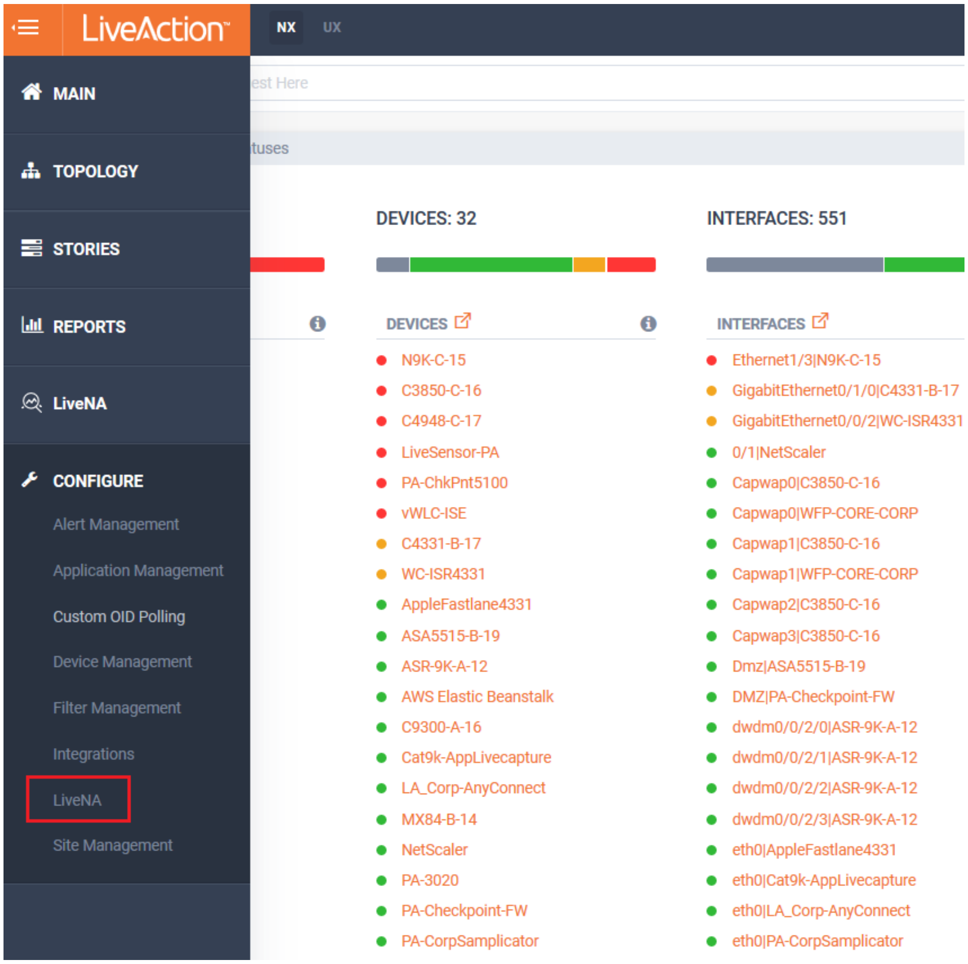
Hostname: livena.liveaction.com Port: 34524 Status: ● Connected

	DEVICE NAME	NODE	SITE
□	Device Name	Node	Site

Add Devices to LiveNA

LiveNA must be configured to monitor devices that are already in LiveNX's inventory. To enable LiveNA to monitor devices, follow these steps:

1. Open LiveNX Operations Dashboard (WebUI).
2. Select **Configure > LiveNA**.



DEVICES: 32

INTERFACES: 551

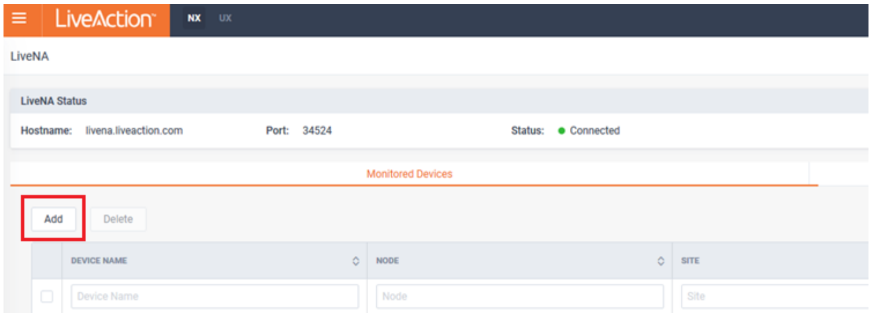
DEVICES

- ● N9K-C-15
- ● C3850-C-16
- ● C4948-C-17
- ● LiveSensor-PA
- ● PA-ChkPnt5100
- ● vWLC-ISE
- ● C4331-B-17
- ● WC-ISR4331
- ● AppleFastlane4331
- ● ASA5515-B-19
- ● ASR-9K-A-12
- ● AWS Elastic Beanstalk
- ● C9300-A-16
- ● Cat9k-AppLivecapture
- ● LA_Corp-AnyConnect
- ● MX84-B-14
- ● NetScaler
- ● PA-3020
- ● PA-Checkpoint-FW
- ● PA-CorpSamplicator

INTERFACES

- ● Ethernet1/3|N9K-C-15
- ● GigabitEthernet0/1/0|C4331-B-17
- ● GigabitEthernet0/0/2|WC-ISR4331
- ● 0/1|NetScaler
- ● Capwap0|C3850-C-16
- ● Capwap0|WFP-CORE-CORP
- ● Capwap1|C3850-C-16
- ● Capwap1|WFP-CORE-CORP
- ● Capwap2|C3850-C-16
- ● Capwap3|C3850-C-16
- ● Dmz|ASA5515-B-19
- ● DMZ|PA-Checkpoint-FW
- ● dwdm0/0/2/0|ASR-9K-A-12
- ● dwdm0/0/2/1|ASR-9K-A-12
- ● dwdm0/0/2/2|ASR-9K-A-12
- ● dwdm0/0/2/3|ASR-9K-A-12
- ● eth0|AppleFastlane4331
- ● eth0|Cat9k-AppLivecapture
- ● eth0|LA_Corp-AnyConnect
- ● eth0|PA-CorpSamplicator

3. From the Monitored Devices tab, select Add.



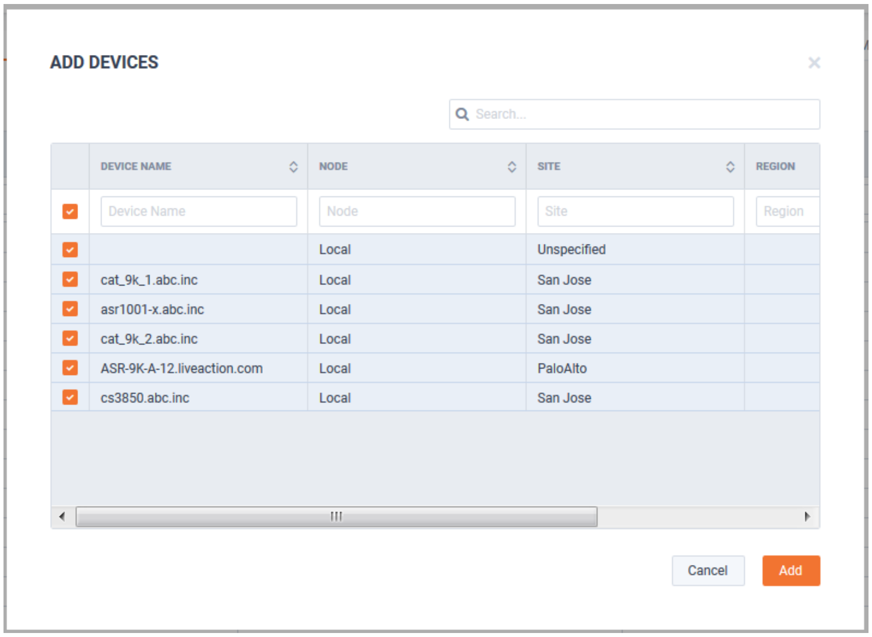
LiveNA Status

Hostname: livena.liveaction.com Port: 34524 Status: ● Connected

Monitored Devices

	DEVICE NAME	NODE	SITE
□	Device Name	Node	Site

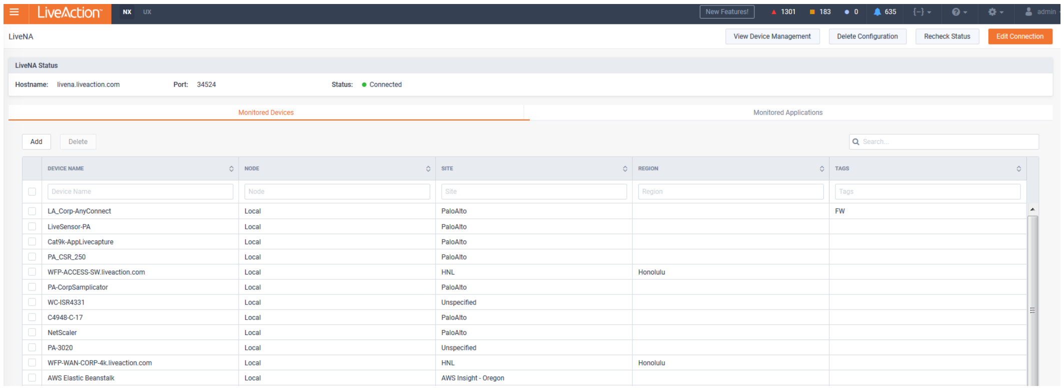
4. Select the device(es) LiveNA should monitor



ADD DEVICES

	DEVICE NAME	NODE	SITE	REGION
☑	Device Name	Node	Site	Region
☑		Local	Unspecified	
☑	cat_9k_1.abc.inc	Local	San Jose	
☑	asr1001-x.abc.inc	Local	San Jose	
☑	cat_9k_2.abc.inc	Local	San Jose	
☑	ASR-9K-A-12.liveaction.com	Local	PaloAlto	
☑	cs3850.abc.inc	Local	San Jose	

5. Once devices are added, the Monitored Device tab will look similar to this:



LiveNA Status

Hostname: livena.liveaction.com Port: 34524 Status: ● Connected

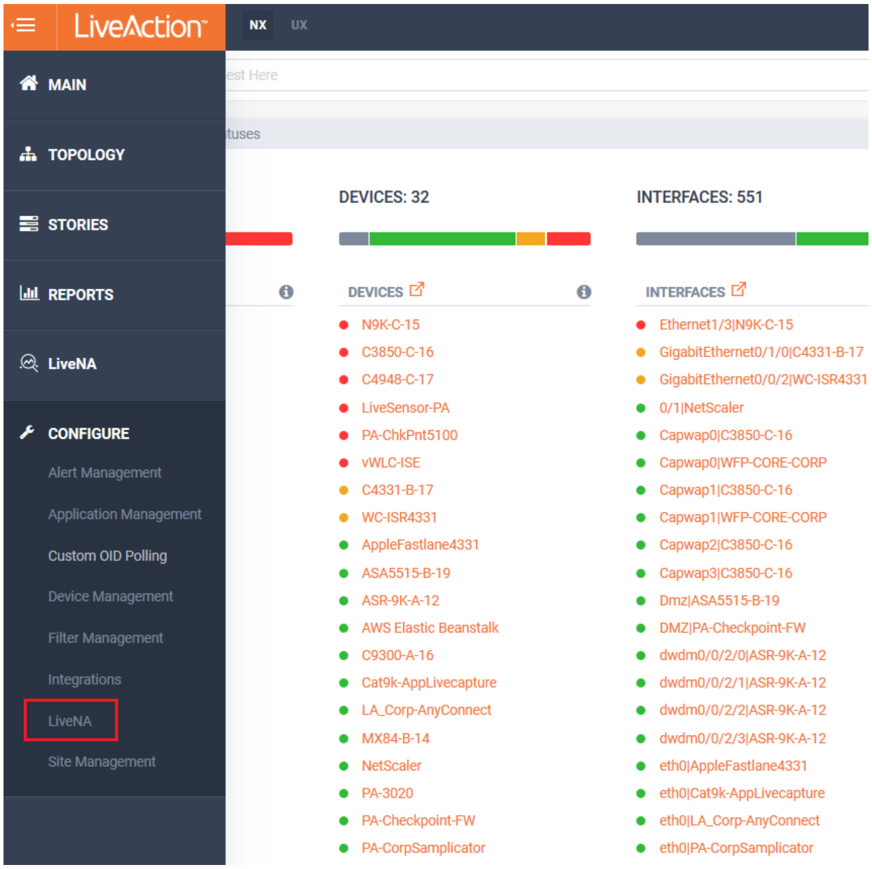
Monitored Devices | Monitored Applications

	DEVICE NAME	NODE	SITE	REGION	TAGS
□	Device Name	Node	Site	Region	Tags
□	LA_Corp-AnyConnect	Local	PaloAlto		FW
□	LiveSensor-PA	Local	PaloAlto		
□	Cat9k-AppLivecapture	Local	PaloAlto		
□	PA_CSR_250	Local	PaloAlto		
□	WFP-ACCESS-SW.liveaction.com	Local	HNL	Honolulu	
□	PA-CorpSamplicator	Local	PaloAlto		
□	WC-ISR4331	Local	Unspecified		
□	C4948-C-17	Local	PaloAlto		
□	NetScaler	Local	PaloAlto		
□	PA-3020	Local	Unspecified		
□	WFP-WAN-CORP-4k.liveaction.com	Local	HNL	Honolulu	
□	AWS Elastic Beanstalk	Local	AWS Insight - Oregon		

Define Custom Application Groups (Optional)

LiveNA will automatically discovery the top 100 applications (by volume) on the network. This list is dynamic and will change over time with the conditions of the network. In addition to the top 100, specific applications by can continuously be monitored by LiveNA via Application Groups defined LiveNX. To reference these application groups, follow these steps:

1. Open LiveNX Operations Dashboard (WebUI).
2. Select Configure > LiveNA.

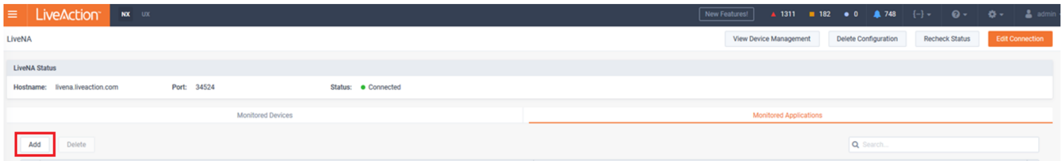


DEVICES: 32

INTERFACES: 551

DEVICES	INTERFACES
● N9K-C-15	● Ethernet1/3|N9K-C-15
● C3850-C-16	● GigabitEthernet0/1/0|C4331-B-17
● C4948-C-17	● GigabitEthernet0/0/2|WC-ISR4331
● LiveSensor-PA	● 0/1|NetScaler
● PA-ChkPnt5100	● Capwap0|C3850-C-16
● vWLC-ISE	● Capwap0|WFP-CORE-CORP
● C4331-B-17	● Capwap1|C3850-C-16
● WC-ISR4331	● Capwap1|WFP-CORE-CORP
● AppleFastlane4331	● Capwap2|C3850-C-16
● ASA5515-B-19	● Capwap3|C3850-C-16
● ASR-9K-A-12	● Dmz|ASA5515-B-19
● AWS Elastic Beanstalk	● DMZ|PA-Checkpoint-FW
● C9300-A-16	● dwdm0/0/2/0|ASR-9K-A-12
● Cat9k-AppLivecapture	● dwdm0/0/2/1|ASR-9K-A-12
● LA_Corp-AnyConnect	● dwdm0/0/2/2|ASR-9K-A-12
● MX84-B-14	● dwdm0/0/2/3|ASR-9K-A-12
● NetScaler	● eth0|AppleFastlane4331
● PA-3020	● eth0|Cat9k-AppLivecapture
● PA-Checkpoint-FW	● eth0|LA_Corp-AnyConnect
● PA-CorpSamplicator	● eth0|PA-CorpSamplicator

3. From the **Monitored Applications** tab, select **Add.**

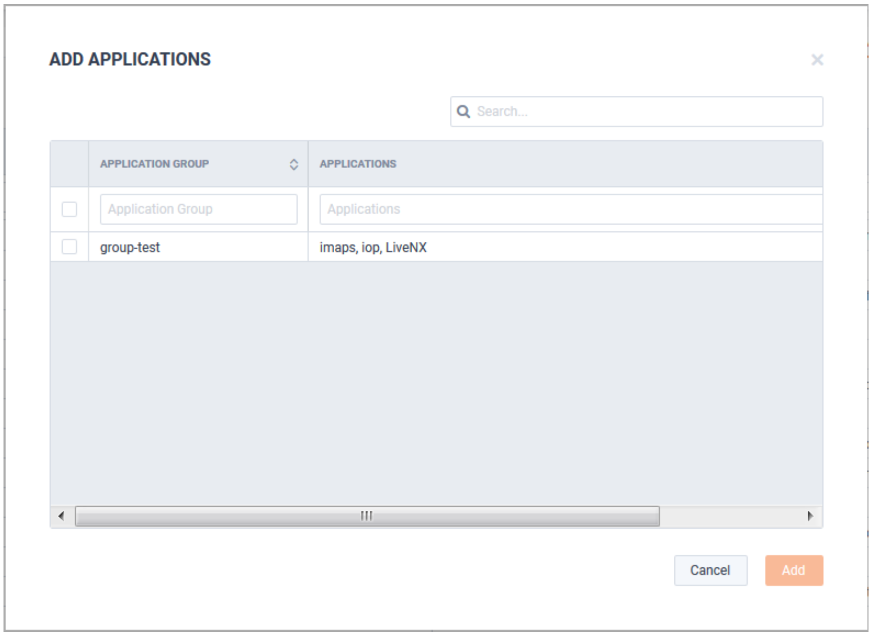


LiveNA

LiveNA Status

Hostname: livena.liveaction.com Port: 34524 Status: ● Connected

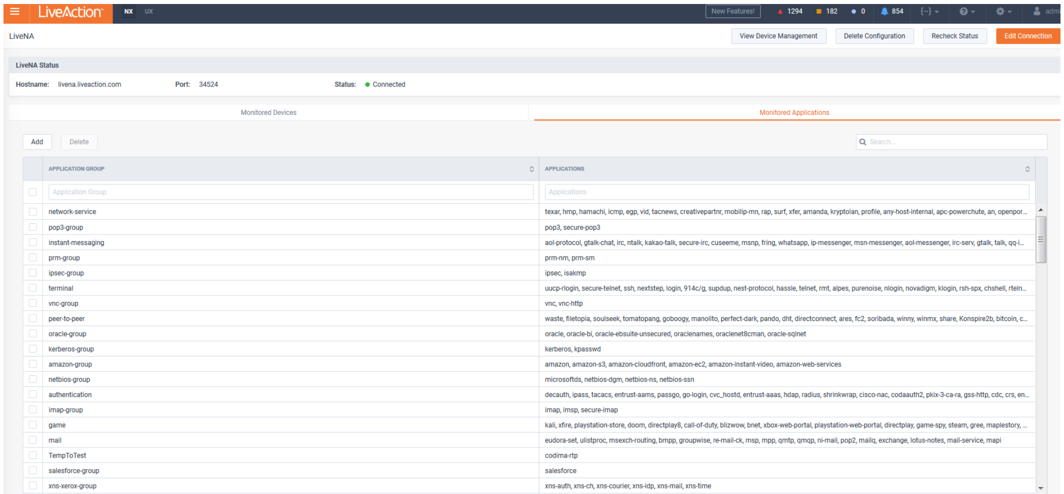
4. Select the application group(s) LiveNA should continuously monitor.



ADD APPLICATIONS

	APPLICATION GROUP	APPLICATIONS
□	Application Group	Applications
□	group-test	imaps, iop, LiveNX

5. Once application(s) are added, the Monitored Applications tab will look similar to this:



LiveNA Status

Hostname: livena.liveaction.com Port: 34524 Status: ● Connected

APPLICATION GROUP	APPLICATIONS
network-service	texar, hmp, hamachi, icmp, egp, vid, tacnews, creativepartnr, mobilip-mn, rap, surf, xfer, amanda, kryptolan, profile, any-host-internal, apc-powerchute, an, openpor...
pop3-group	pop3, secure-pop3
instant-messaging	aol-protocol, gtalk-chat, irc, ntalk, kakao-talk, secure-irc, cuseeme, msnp, fring, whatsapp, ip-messenger, msn-messenger, aol-messenger, irc-serv, gtalk, talk, qq-i...
prm-group	prm-nm, prm-sm
ipsec-group	ipsec, isakmp
terminal	uucp-rlogin, secure-telnet, ssh, nextstep, login, 914c/g, supdup, nest-protocol, hassle, telnet, rmt, alpes, purenoise, nlogin, novadigm, klogin, rsh-spx, chshell, rteln...
vnc-group	vnc, vnc-http
peer-to-peer	waste, filetopia, soulseek, tomatopang, goboogy, manolito, perfect-dark, pando, dht, directconnect, ares, fc2, soribada, winny, winmx, share, Konspire2b, bitcoin, c...
oracle-group	oracle, oracle-bi, oracle-ebsuite-unsecured, oraclenames, oraclenet8cman, oracle-sqlnet
kerberos-group	kerberos, kpasswd
amazon-group	amazon, amazon-s3, amazon-cloudfront, amazon-ec2, amazon-instant-video, amazon-web-services
netbios-group	microsoftds, netbios-dgm, netbios-ns, netbios-ssn
authentication	decauth, ipass, tacacs, entrust-aams, passgo, go-login, cvc_hostd, entrust-aaas, hdap, radius, shrinkwrap, cisco-nac, codaauth2, pkix-3-ca-ra, gss-http, cdc, crs, en...
imap-group	imap, imsp, secure-imap
game	kali, xfire, playstation-store, doom, directplay8, call-of-duty, blizwow, bnet, xbox-web-portal, playstation-web-portal, directplay, game-spy, steam, gree, maplestory, ...
mail	eudora-set, ulistproc, msexch-routing, bmpp, groupwise, re-mail-ck, msp, mpp, qmtp, qmqp, ni-mail, pop2, mailq, exchange, lotus-notes, mail-service, mapi
TempToTest	codima-rtp
salesforce-group	salesforce
xns-xerox-group	xns-auth, xns-ch, xns-courier, xns-idp, xns-mail, xns-time

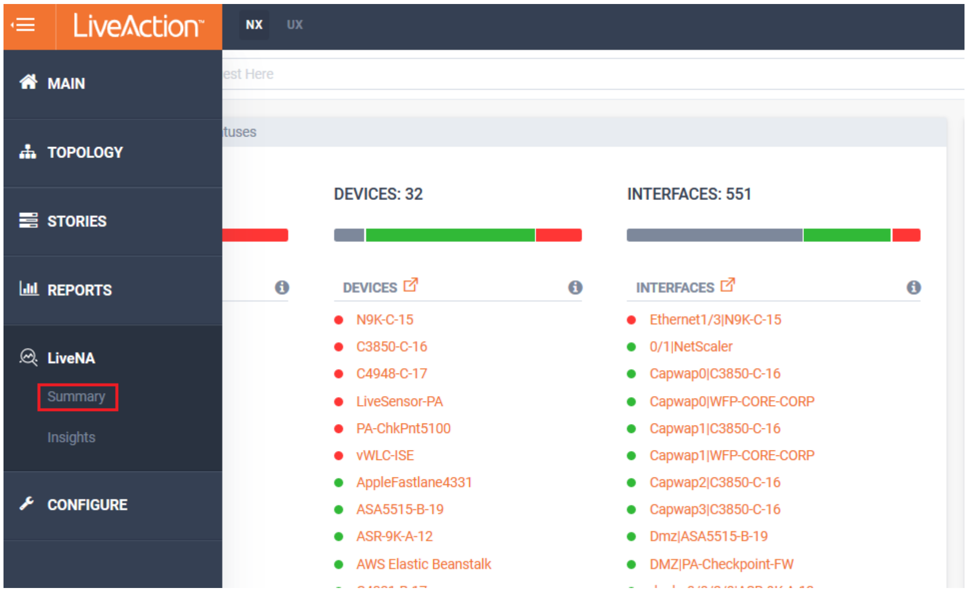
Using LiveNA

LiveNA is access via the LiveNX Operations Dashboard (WebUI). Once LiveNA is configured, it will learn the behavior of network and provide insights of anomalies. It takes **4-5 days of learning** before LiveNA provides any insights. After the initial learning phase LiveNA will continue to update its baselines and understanding of the network over time. There are two pages that provide visibility of the insights; Summary and Network Analytics. These are outlined below.

Summary

To access the LiveNA Summary page:

1. Open LiveNX Operations Dashboard (WebUI).
2. Select **Analytics** > **Summary**.



DEVICES: 32

INTERFACES: 551

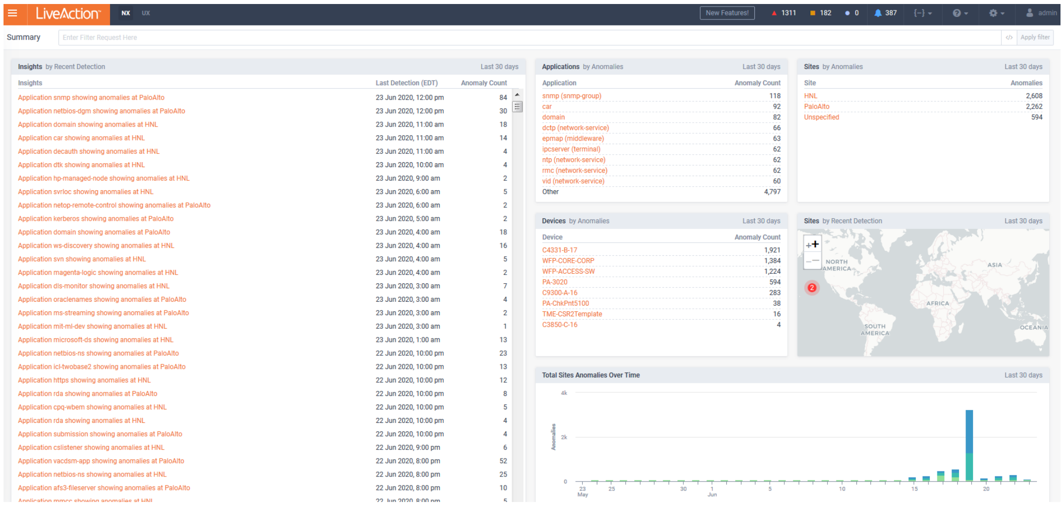
DEVICES

- N9K-C-15
- C3850-C-16
- C4948-C-17
- LiveSensor-PA
- PA-ChkPnt5100
- vWLC-ISE
- AppleFastlane4331
- ASA5515-B-19
- ASR-9K-A-12
- AWS Elastic Beanstalk

INTERFACES

- Ethernet1/3|N9K-C-15
- 0/1|NetScaler
- Capwap0|C3850-C-16
- Capwap0|WFP-CORE-CORP
- Capwap1|C3850-C-16
- Capwap1|WFP-CORE-CORP
- Capwap2|C3850-C-16
- Capwap3|C3850-C-16
- Dmz|ASA5515-B-19
- DMZ|PA-Checkpoint-FW

3. The Summary page provides an overview of the Insights and anomalies detected by LiveNA. Filters can be used to focus the view to specific devices/application/etc. Clicking on the Widget details will pivot to the Network Analytics page with appropriate filters applied.



Insights by Recent Detection — Last 30 days

Insights	Last Detection (EDT)	Anomaly Count
Application snmp showing anomalies at PaloAlto	23 Jun 2020, 12:00 pm	84
Application netbios-dgm showing anomalies at PaloAlto	23 Jun 2020, 12:00 pm	30
Application domain showing anomalies at HNL	23 Jun 2020, 11:00 am	18
Application car showing anomalies at HNL	23 Jun 2020, 11:00 am	14
Application decauth showing anomalies at HNL	23 Jun 2020, 11:00 am	4
Application dtk showing anomalies at HNL	23 Jun 2020, 10:00 am	4
Application hp-managed-node showing anomalies at HNL	23 Jun 2020, 9:00 am	2
Application svrloc showing anomalies at HNL	23 Jun 2020, 6:00 am	5
Application netop-remote-control showing anomalies at PaloAlto	23 Jun 2020, 6:00 am	2
Application kerberos showing anomalies at PaloAlto	23 Jun 2020, 5:00 am	2
Application domain showing anomalies at PaloAlto	23 Jun 2020, 4:00 am	18
Application ws-discovery showing anomalies at HNL	23 Jun 2020, 4:00 am	16
Application svn showing anomalies at HNL	23 Jun 2020, 4:00 am	5
Application magenta-logic showing anomalies at HNL	23 Jun 2020, 4:00 am	2
Application dls-monitor showing anomalies at HNL	23 Jun 2020, 3:00 am	7
Application oraclenames showing anomalies at PaloAlto	23 Jun 2020, 3:00 am	4
Application ms-streaming showing anomalies at PaloAlto	23 Jun 2020, 3:00 am	2
Application mit-ml-dev showing anomalies at HNL	23 Jun 2020, 3:00 am	1
Application microsoft-ds showing anomalies at HNL	23 Jun 2020, 1:00 am	13
Application netbios-ns showing anomalies at PaloAlto	22 Jun 2020, 10:00 pm	23
Application icl-twobase2 showing anomalies at PaloAlto	22 Jun 2020, 10:00 pm	13
Application https showing anomalies at HNL	22 Jun 2020, 10:00 pm	12
Application rda showing anomalies at PaloAlto	22 Jun 2020, 10:00 pm	8
Application cpq-wbem showing anomalies at HNL	22 Jun 2020, 10:00 pm	5
Application rda showing anomalies at HNL	22 Jun 2020, 10:00 pm	4
Application submission showing anomalies at PaloAlto	22 Jun 2020, 10:00 pm	4
Application cslistener showing anomalies at HNL	22 Jun 2020, 9:00 pm	6
Application vacdsm-app showing anomalies at PaloAlto	22 Jun 2020, 8:00 pm	52
Application netbios-ns showing anomalies at HNL	22 Jun 2020, 8:00 pm	25
Application afs3-fileserver showing anomalies at PaloAlto	22 Jun 2020, 8:00 pm	10
Application mmcc showing anomalies at HNL	22 Jun 2020, 8:00 pm	5

Applications by Anomalies — Last 30 days

Application	Anomaly Count
snmp (snmp-group)	118
car	92
domain	82
dctp (network-service)	66
epmap (middleware)	63
ipcserver (terminal)	62
ntp (network-service)	62
rmc (network-service)	62
vid (network-service)	60
Other	4,797

Sites by Anomalies — Last 30 days

Site	Anomalies
HNL	2,608
PaloAlto	2,262
Unspecified	594

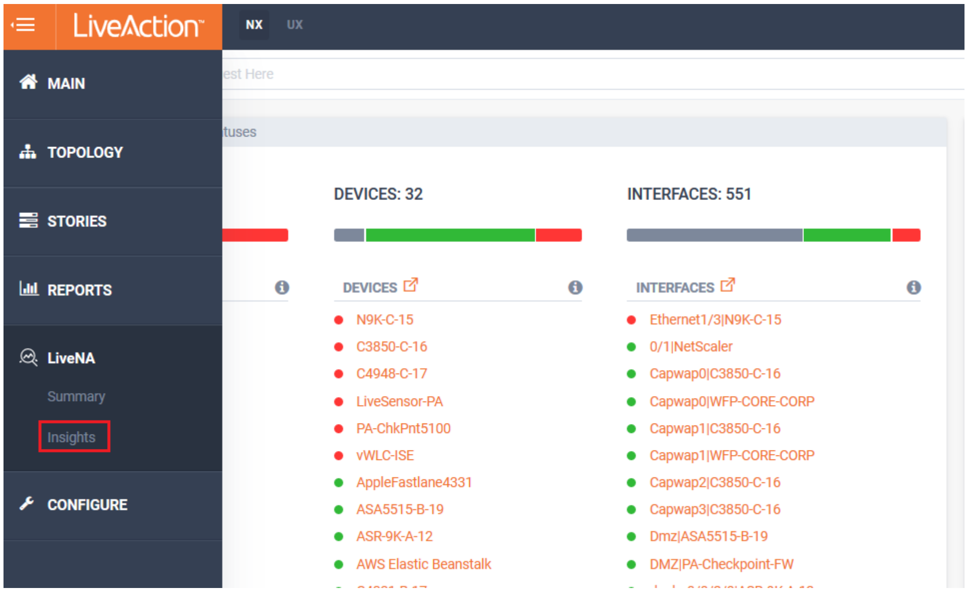
Devices by Anomalies — Last 30 days

Device	Anomaly Count
C4331-B-17	1,921
WFP-CORE-CORP	1,384
WFP-ACCESS-SW	1,224
PA-3020	594
C9300-A-16	283
PA-ChkPnt5100	38
TME-CSR2Template	16
C3850-C-16	4

Network Analytics

To access the LiveNA Summary page:

1. Open LiveNX Operations Dashboard (WebUI).
2. Select **Analytics** > **Insights**.



DEVICES: 32

INTERFACES: 551

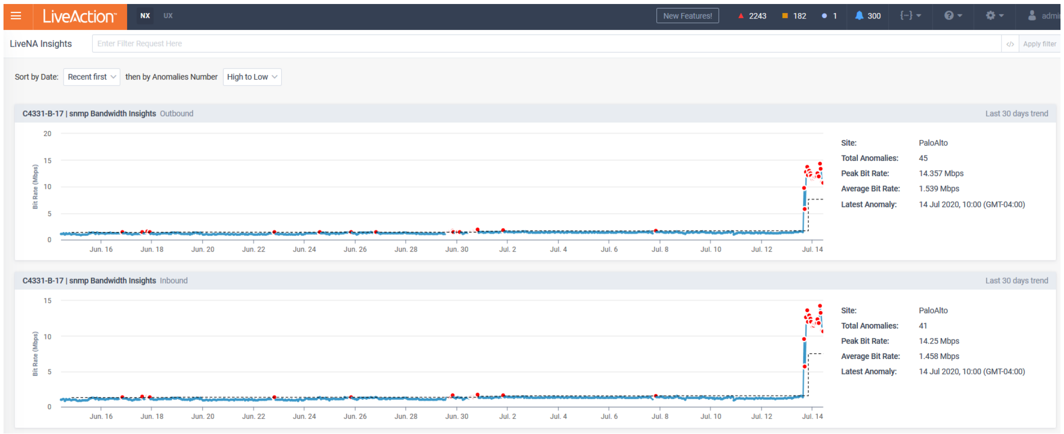
DEVICES

- N9K-C-15
- C3850-C-16
- C4948-C-17
- LiveSensor-PA
- PA-ChkPnt5100
- vWLC-ISE
- AppleFastlane4331
- ASA5515-B-19
- ASR-9K-A-12
- AWS Elastic Beanstalk

INTERFACES

- Ethernet1/3|N9K-C-15
- 0/1|NetScaler
- Capwap0|C3850-C-16
- Capwap0|WFP-CORE-CORP
- Capwap1|C3850-C-16
- Capwap1|WFP-CORE-CORP
- Capwap2|C3850-C-16
- Capwap3|C3850-C-16
- Dmz|ASA5515-B-19
- DMZ|PA-Checkpoint-FW

3. The Network Analytics page the details of the anomalies detected by LiveNA. Filters can be used to focus the view to specific devices/application/etc.



Sort by Date: Recent first then by Anomalies Number High to Low

C4331-B-17 | snmp Bandwidth Insights Outbound

Last 30 days trend

Site: PaloAlto
Total Anomalies: 45
Peak Bit Rate: 14.357 Mbps
Average Bit Rate: 1.539 Mbps
Latest Anomaly: 14 Jul 2020, 10:00 (GMT-04:00)

C4331-B-17 | snmp Bandwidth Insights Inbound

Last 30 days trend

Site: PaloAlto
Total Anomalies: 41
Peak Bit Rate: 14.25 Mbps
Average Bit Rate: 1.458 Mbps
Latest Anomaly: 14 Jul 2020, 10:00 (GMT-04:00)