LiveAction

LiveNX 25.1.0 New Features

QUICK GUIDE

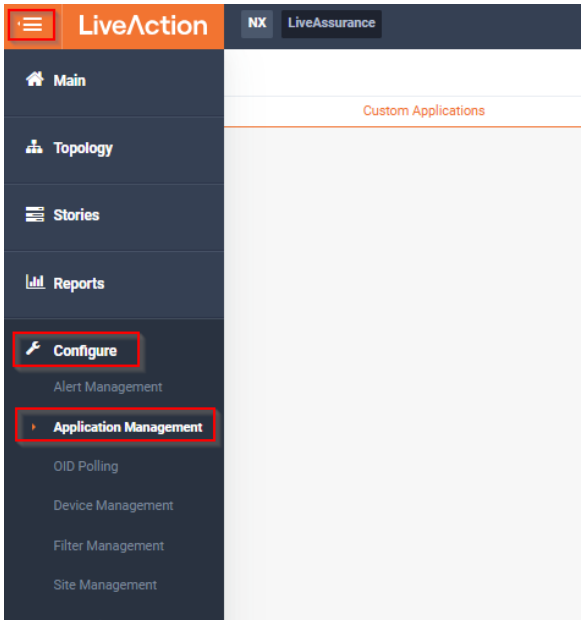
ver. 25.1.0b

Making Bulk Changes in Custom Application and Application Group

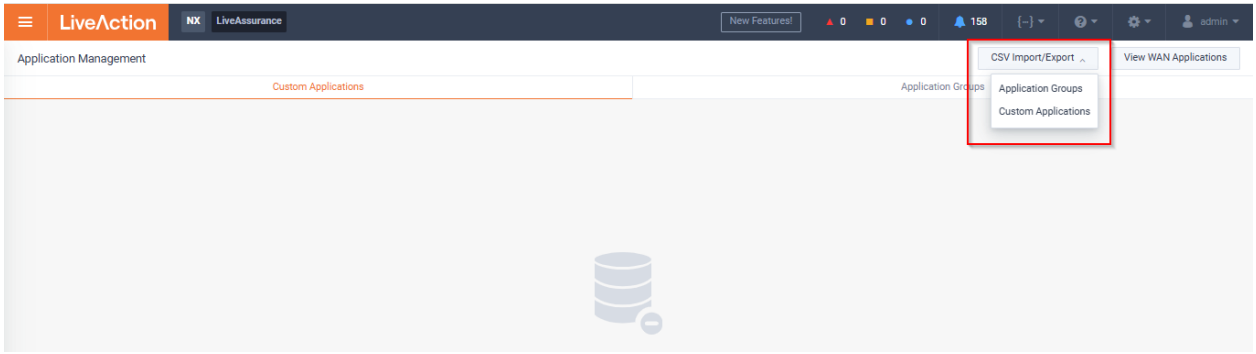
In LiveNX 25.1.0 user would be able to make bulk changes in Custom Application and Application Group of LiveNX using the ability of importing and exporting Custom Applications and application Groups in CSV format.

How to Import / Export CSV to Make Changes

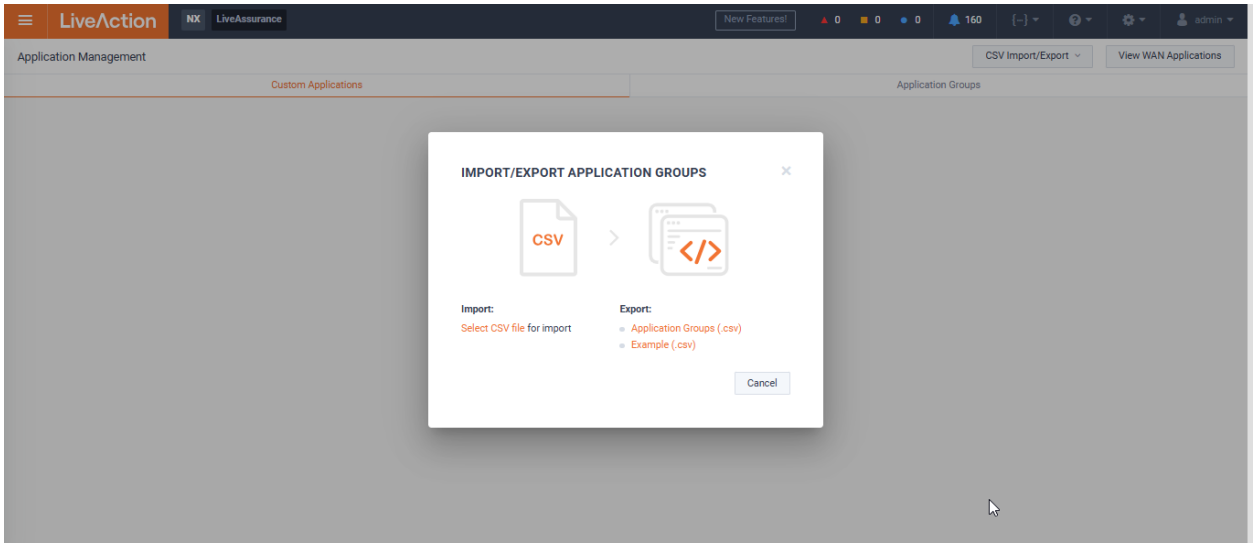
- Login to LiveNX Web
- Navigate to *Configure* and *Application Management*.



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



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



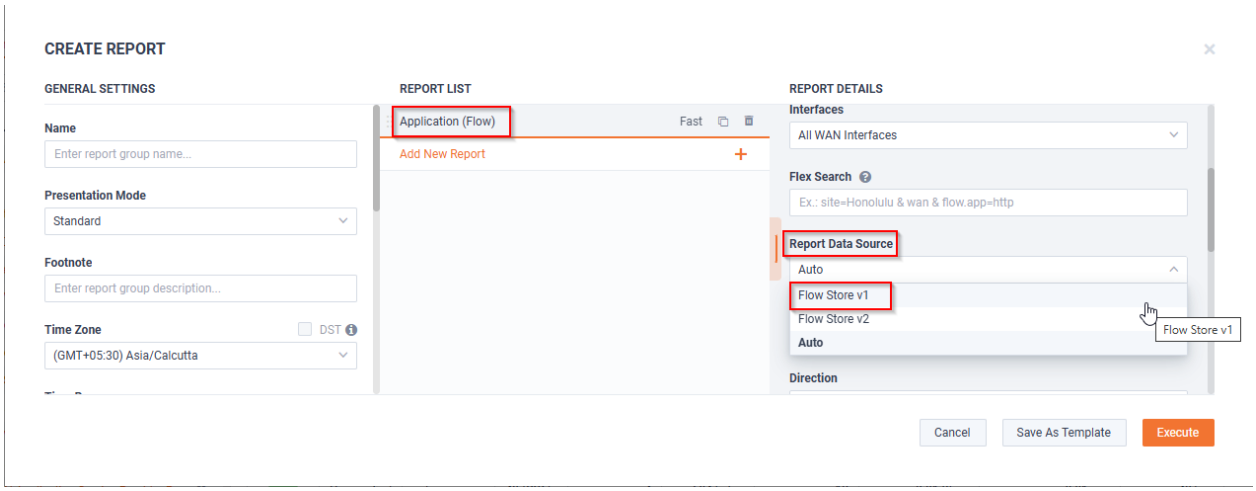
Application Report Percent Bandwidth

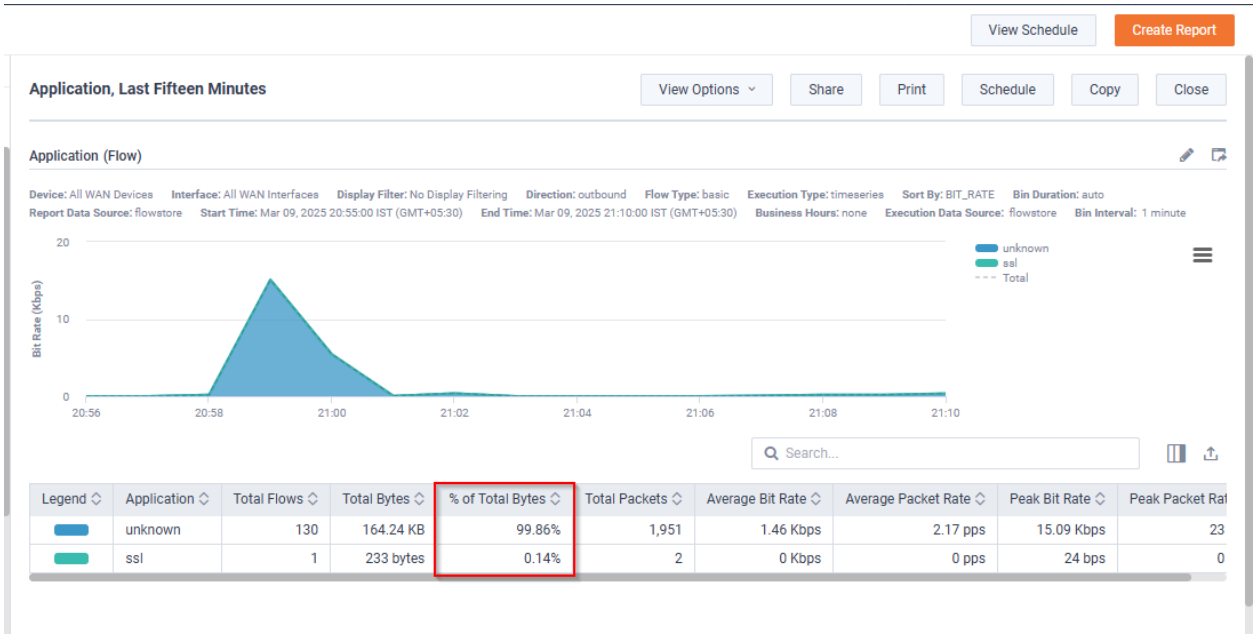
Overview

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

Report Execution

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





Calculations

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

Caveat

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

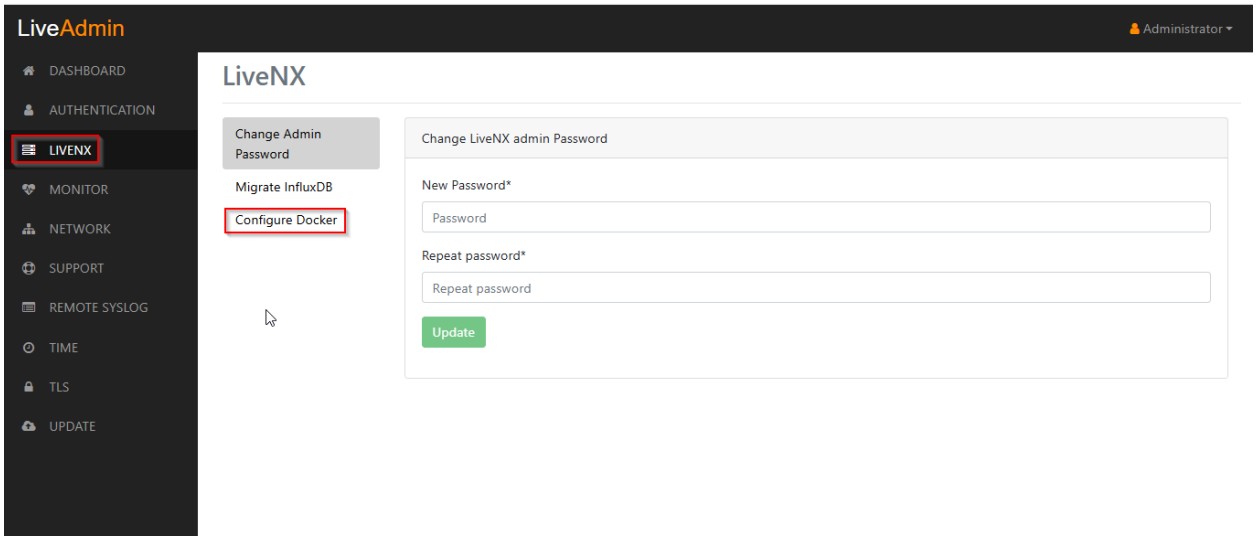
Updating Docker IP Ranges

Overview

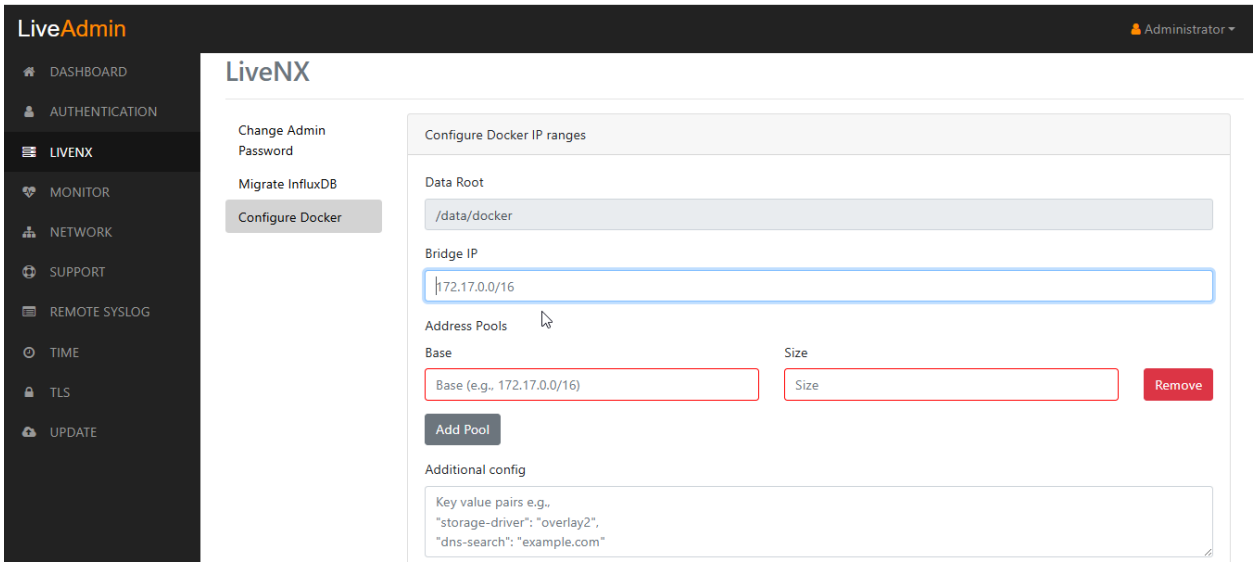
By default LiveNX uses 172.17.x.x or 172.18.x.x IPs for docker. If customer uses these IPs in their network it will create a conflict. In LiveNX 25.1.0 user will get ability to change the Docker IP ranges via the LiveAdmin utility.

Configuration

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



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



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

How To Setup DDI Dashboard

Overview

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

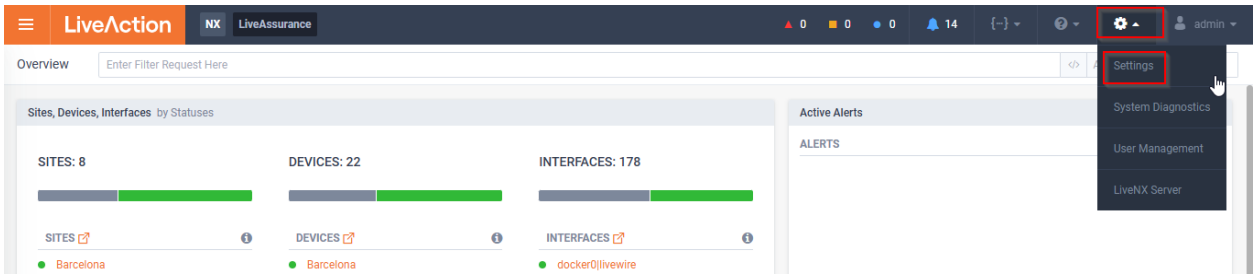
Prerequsite

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

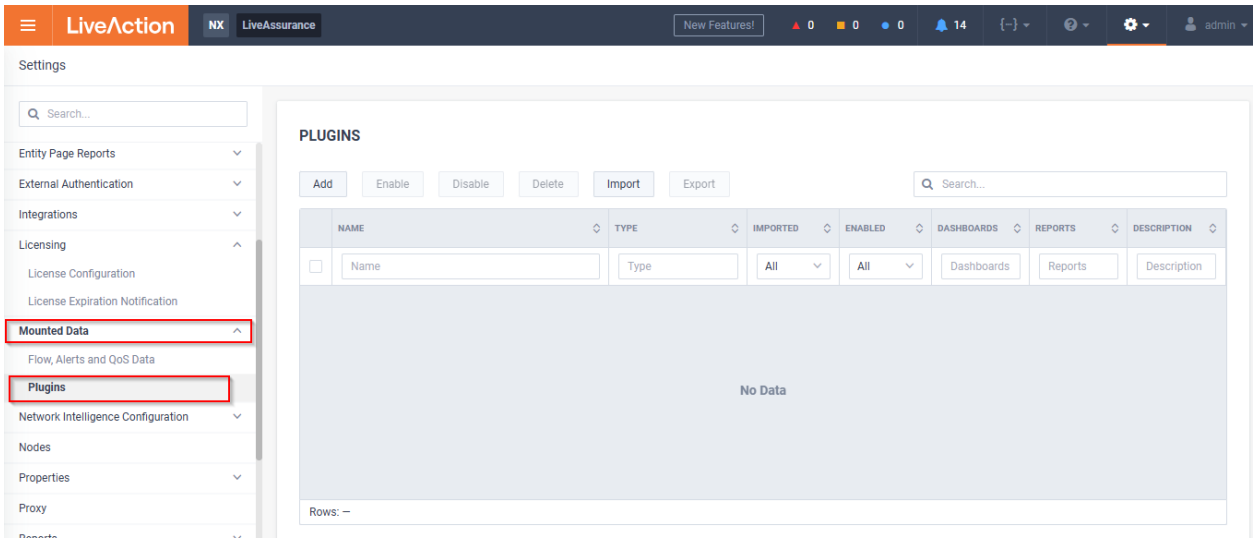
LiveNX Native DDI Dashboard

Importing the DDI dashboard Plugin

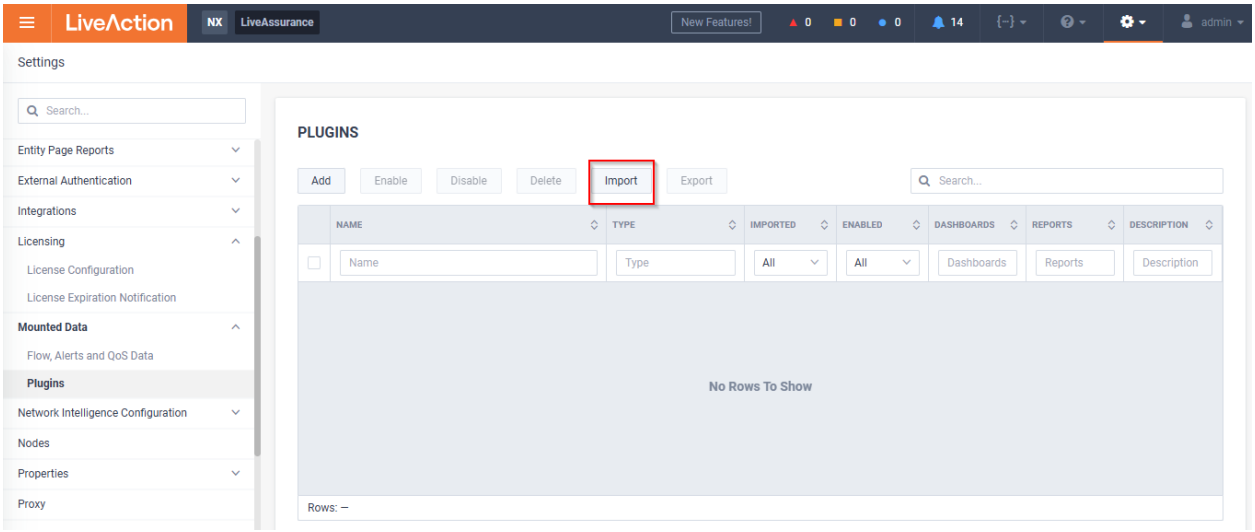
- Download the *`ddi-dashboard-plugin.nxp`* from the LiveNX Integrations public repo.
- Log in to LiveNX web and click on the gear icon available on the *Navigation* bar and select *Settings* option.



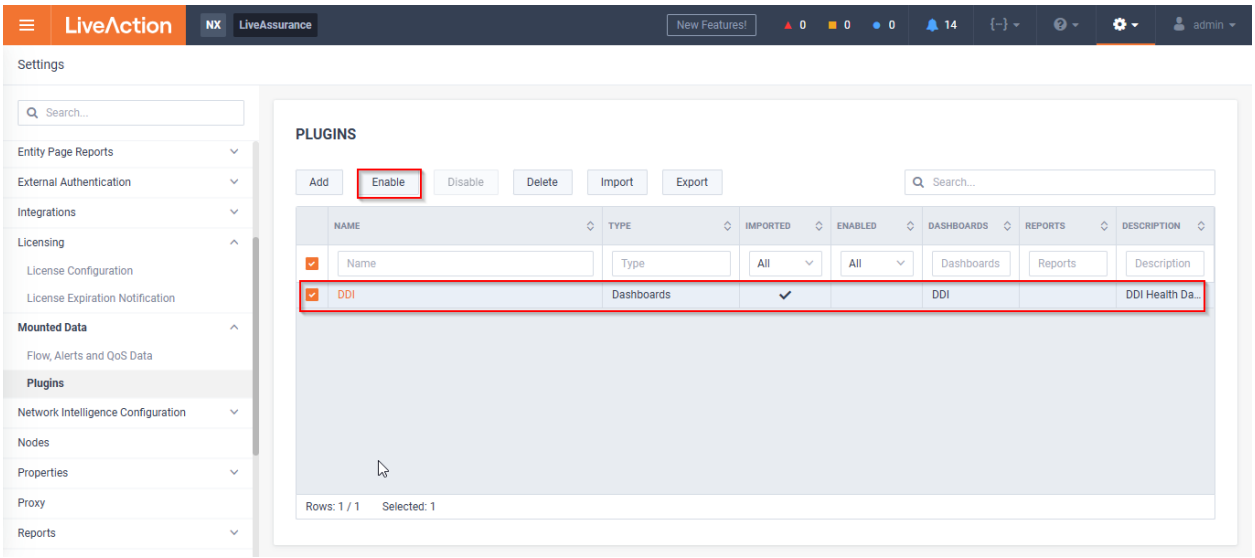
- On the *Settings* page, navigate to *Mounted Data* and select *Plugins*.



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

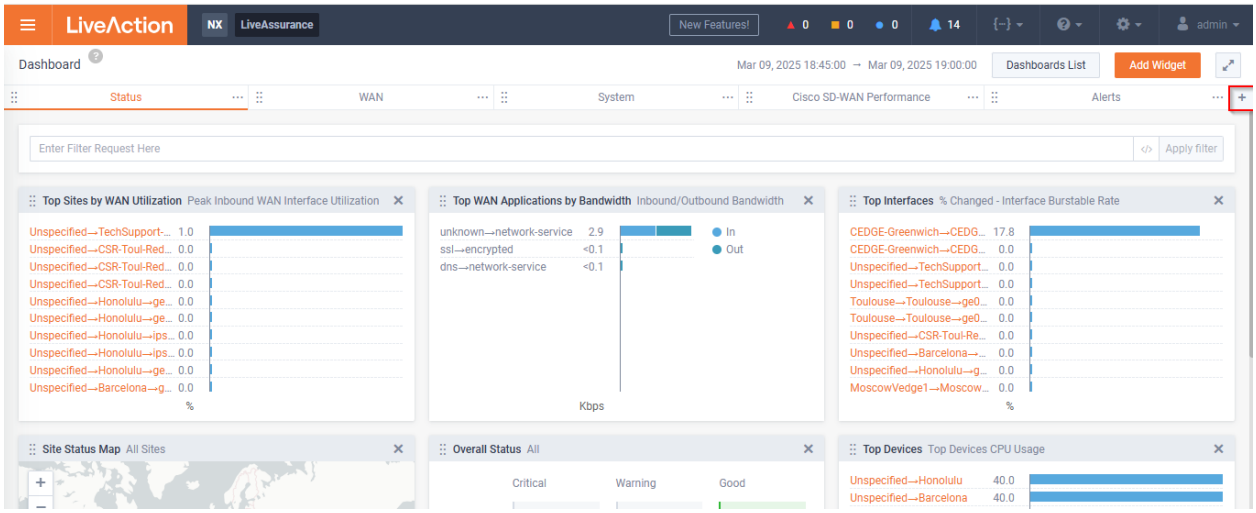


◦ After importing the plugin file, a DDI dashboard will be listed on the *Plugins* page. Select the plugin and click *Enable*.

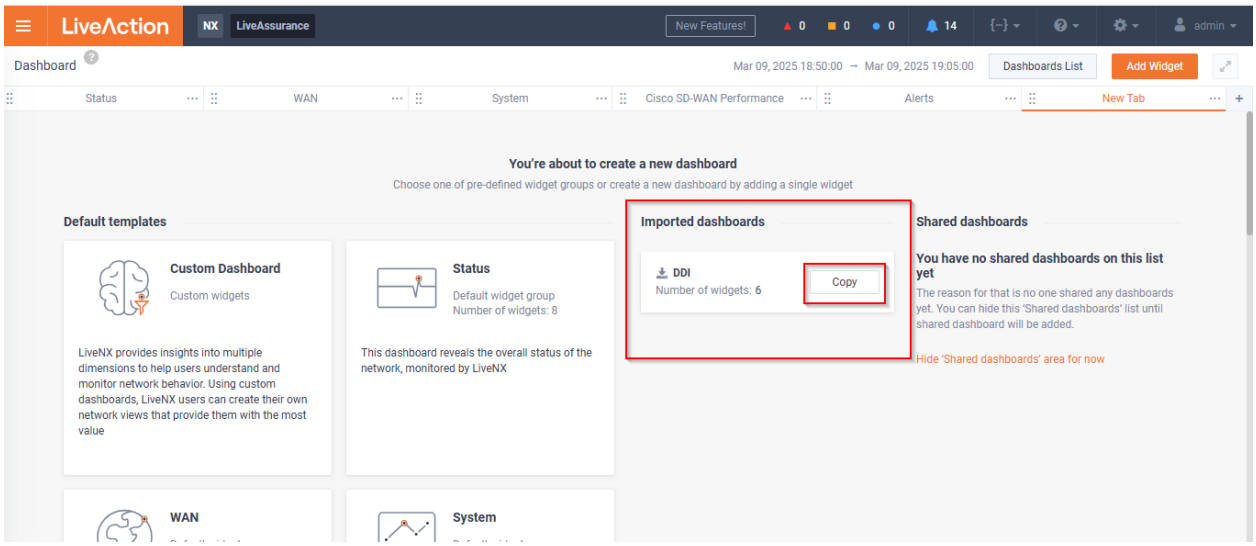


◦ Now to add the dashboard, navigate to *Dashboard* page of LiveNX web

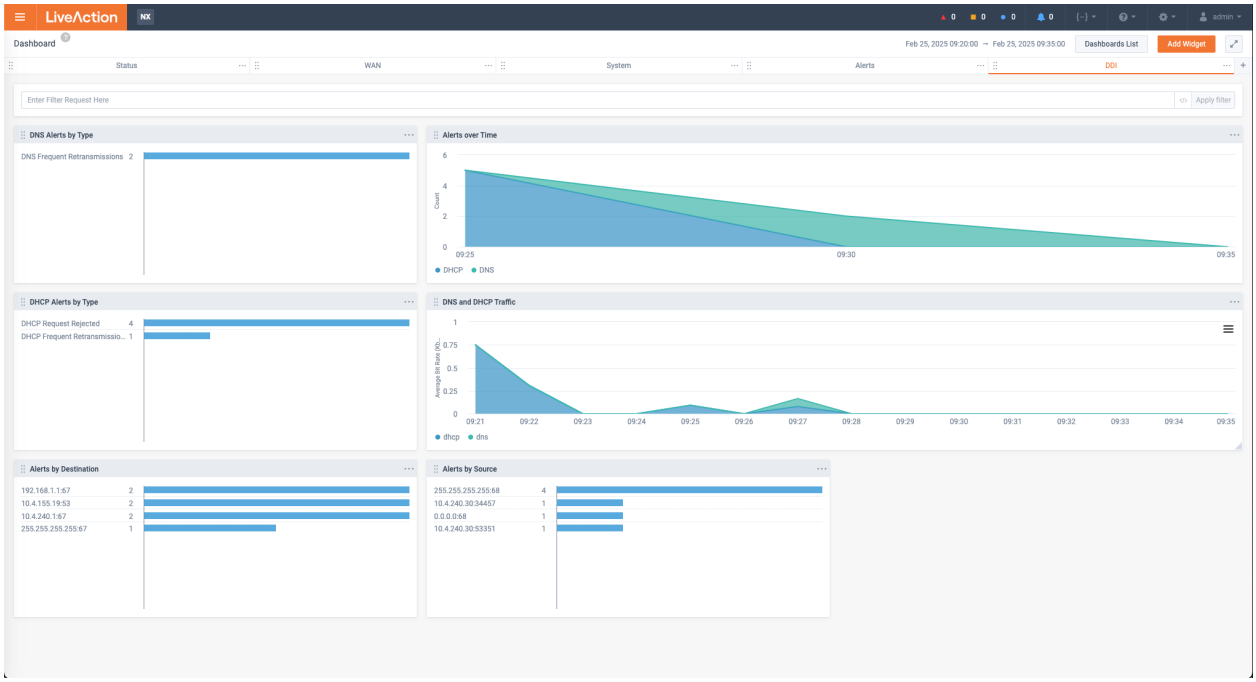
- On *LiveNX Dashboard* page click on + icon to add a new dashboard.



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

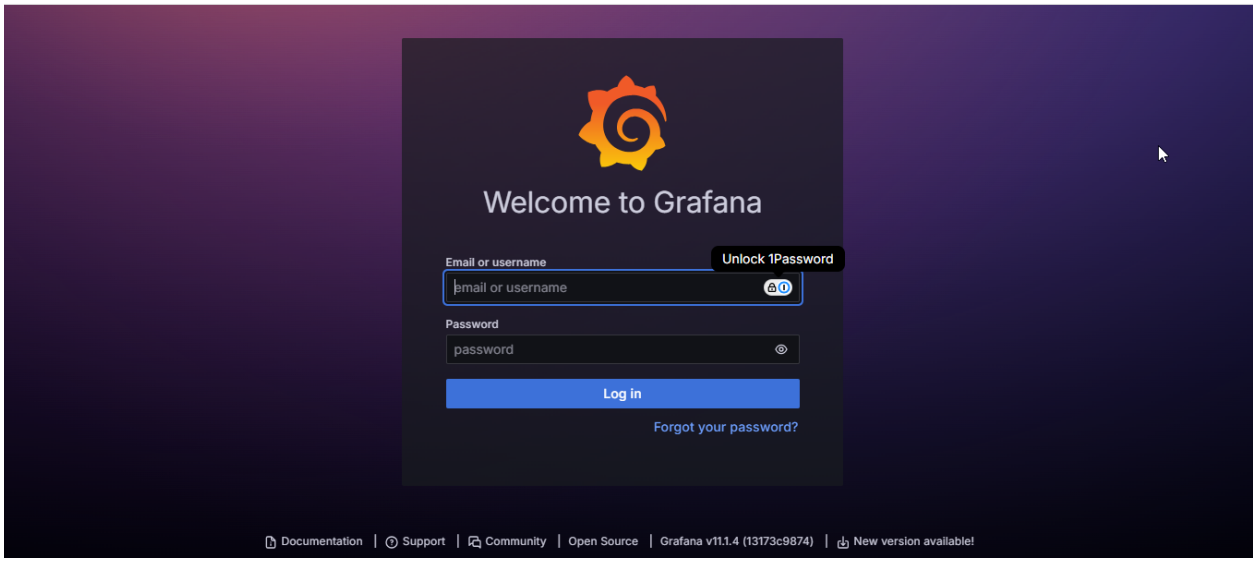


- After clicking on the *Copy* button, a new DDI dashboard will be added to LiveNX dashboard tab.

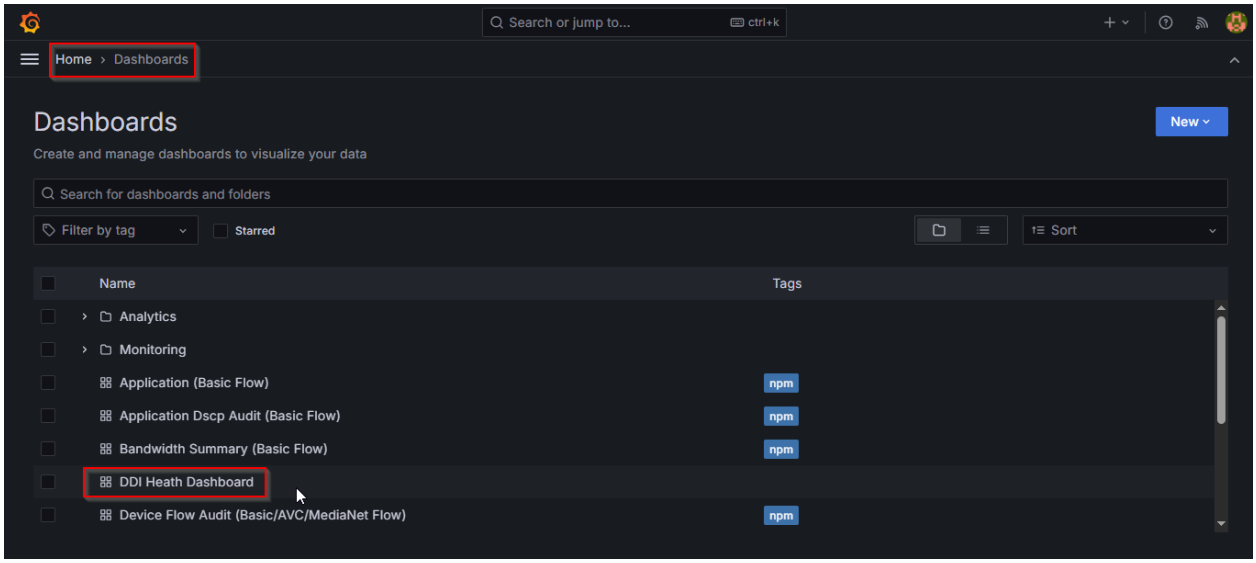


LiveNX Grafana DDI Dashboard

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



◦ Navigate to *Home* > *Dashboard* and select *DDI Health Dashboard*.



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

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

How To Setup DDI / OTel in LiveNX

Overview

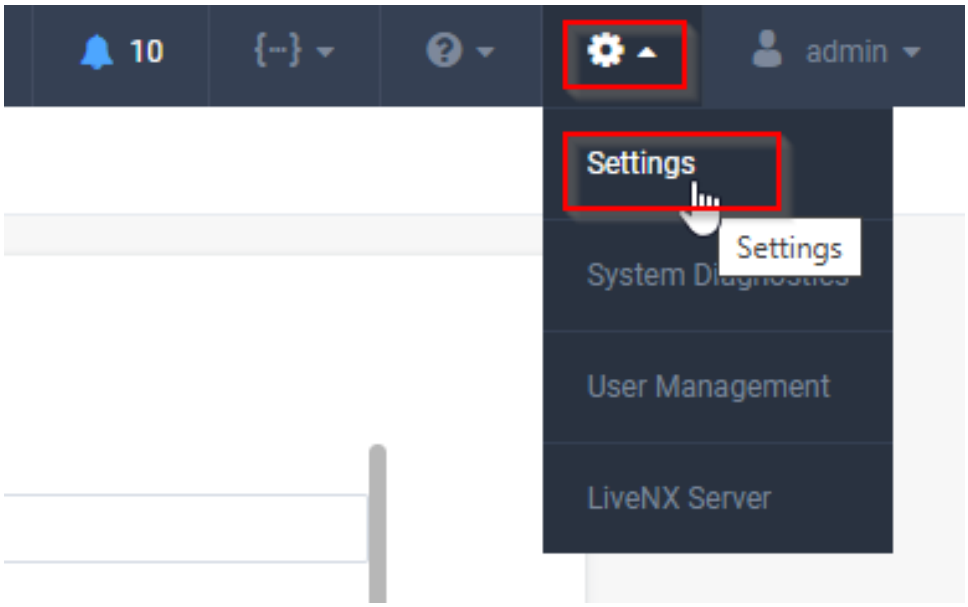
LiveNX is now able to ingest LiveWire and LiveAssurance alerts. This is accomplished via OTEL. This document will cover the configuration of communication. This setup is classified in two parts; one is configuration at the LiveNX end; and second is configuration at LiveAssurance / LiveWire side.

Configuration at LiveNX side

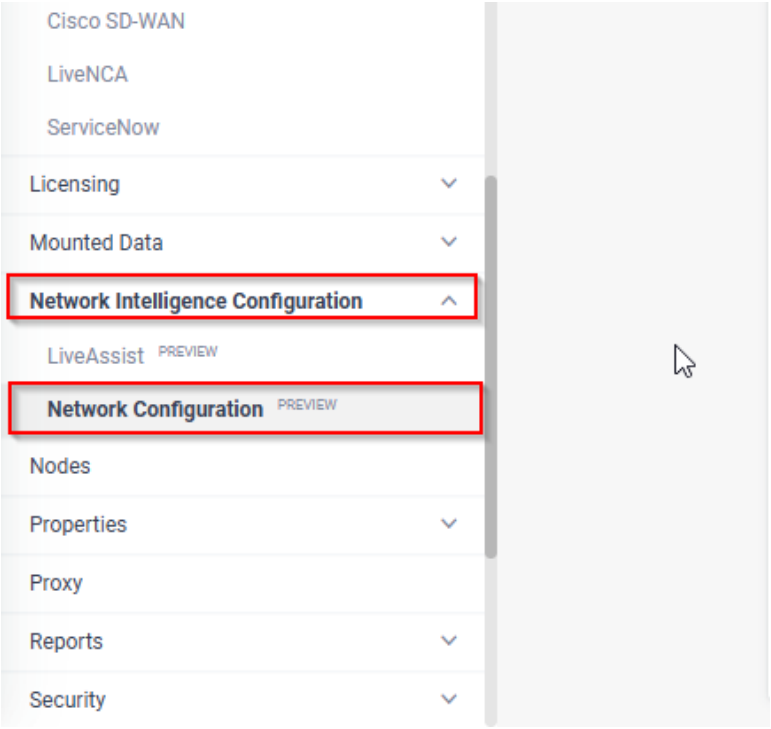
For DDI / OTEL setup, configuration at livenx end is explained below.

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

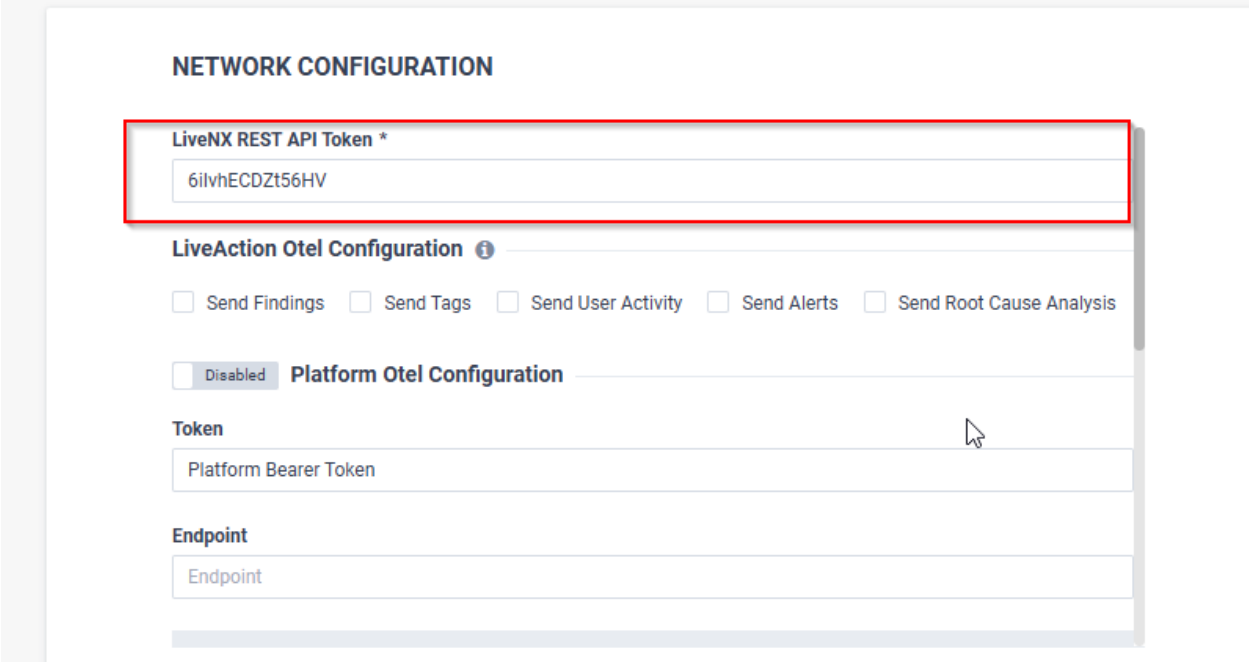
- Log in to LiveNX web and select the gear icon available on the navigation bar, and then select *Settings*.



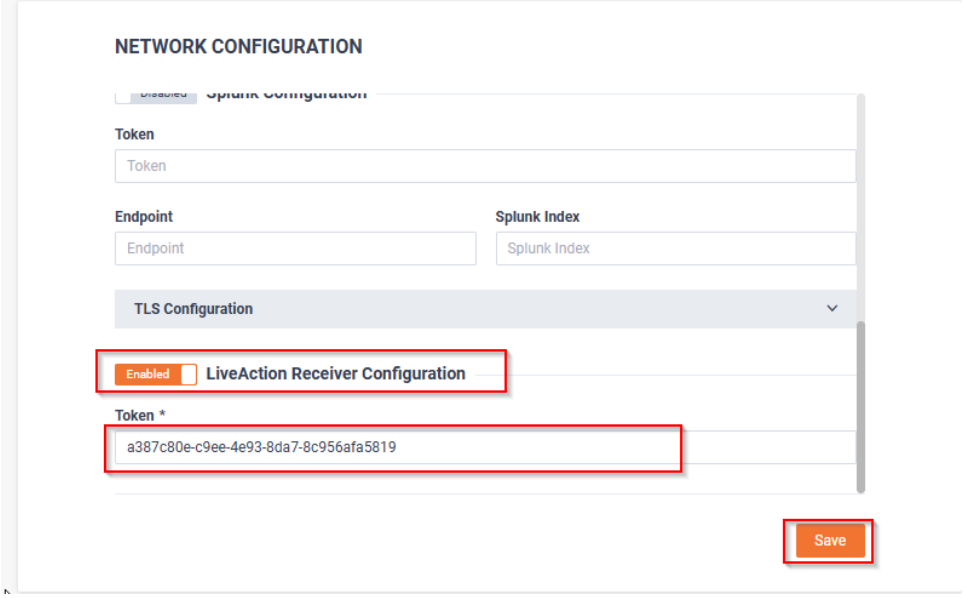
- Under *Network Intelligence Configuration*, select *Network Configuration*.



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



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



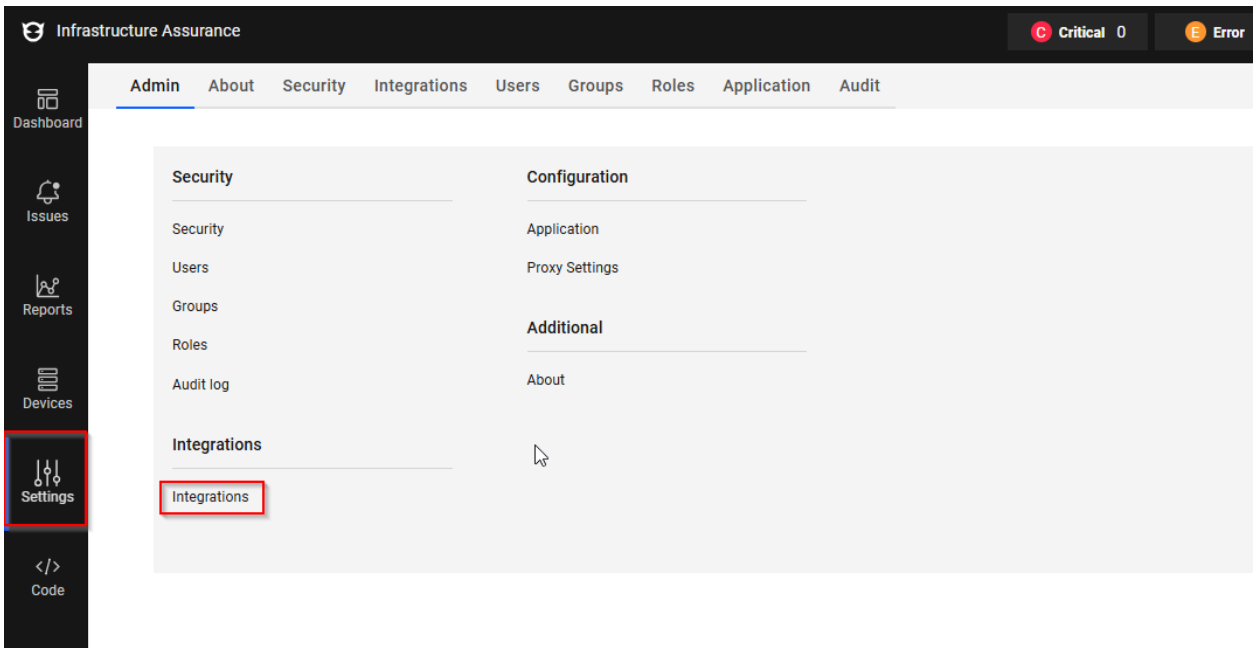
- Create a token for the *LiveAction Receiver Configuration* (if none is present). *Note: green field deployments will always be pre-populated with a UUID.*
  - The user can manually enter any value.
  - The user can automatically generate a UUID value by re-saving the configuration. A trick for this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

Configuration at LiveAssurance to Ingest LiveAssurance Alerts in LiveNX

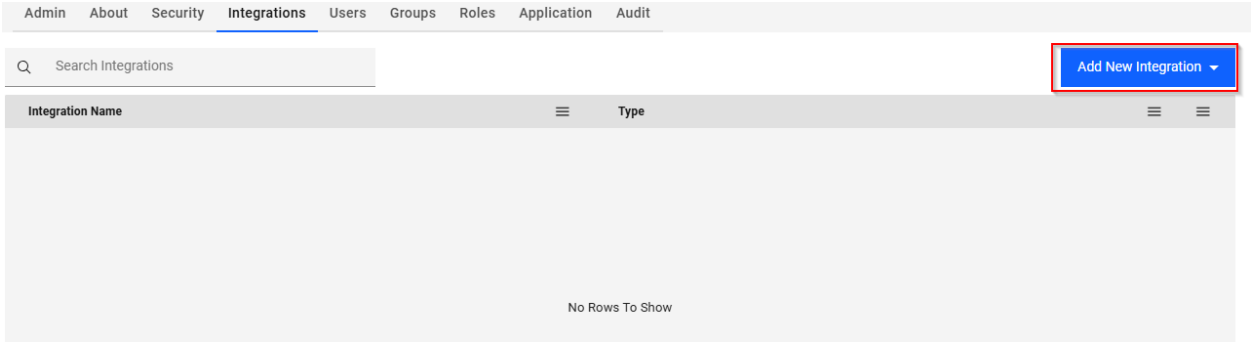
LiveAssurance can be configured by two methods which are described below.

Configuring LiveAssurance to ingest liveAssurance Alerts via LiveAssurance Web.

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

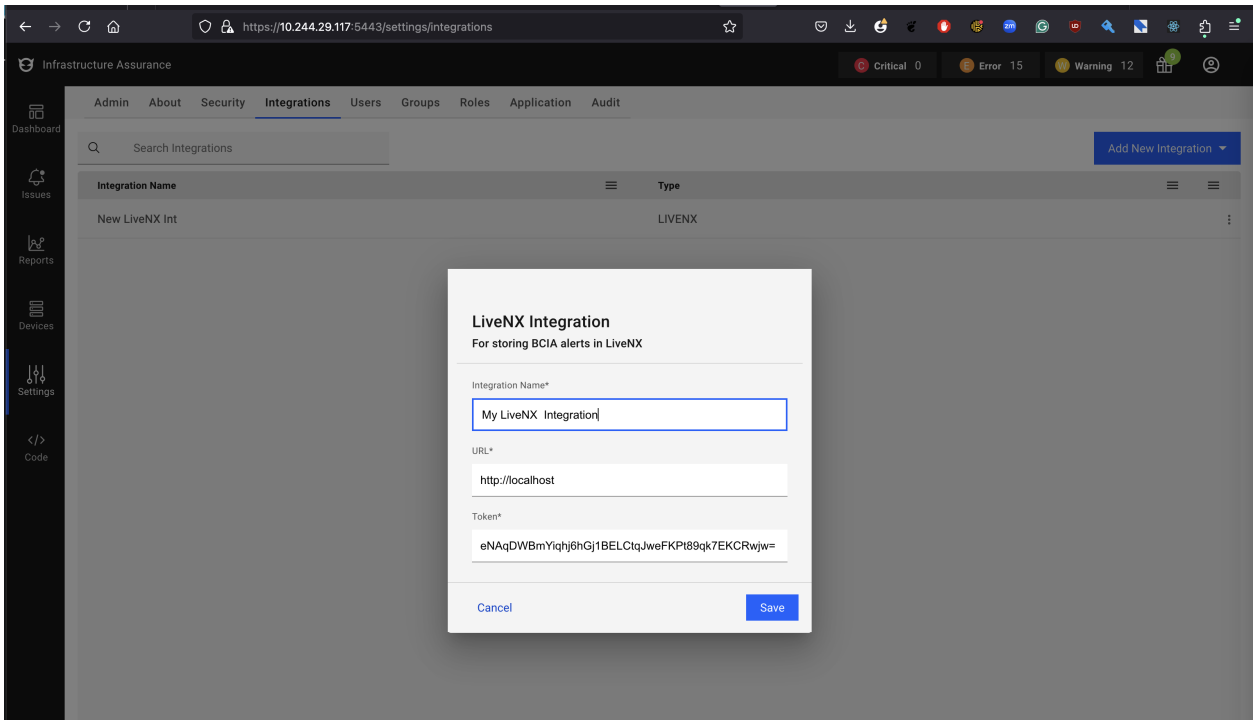


- From the *Add New Integration* drop-down list, select *LiveNX*.



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

    ```
    cd /data/bcia && docker compose restart authserver
    ```



Configuring LiveAssurance to Ingest LiveAssurance Alerts via LiveNX CLI

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

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

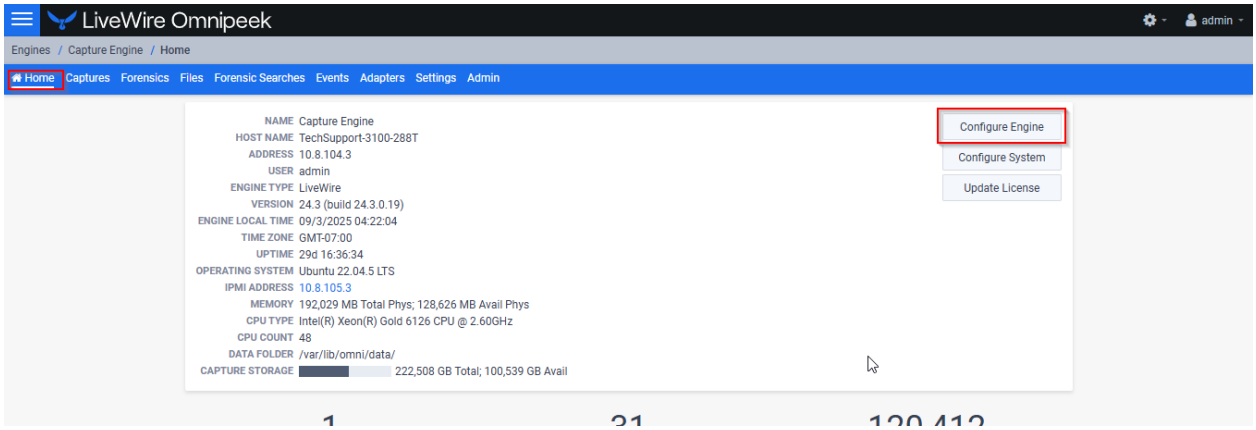
```
exporters:
  otlphttp/liveaction:
    auth:
      authenticator: bearertokenauth/withscheme
    endpoint: http://lnx-local:4318/
    headers:
      x-customer-id: liveaction_dev
    tls:
      insecure: false
      insecure_skip_verify: true
extensions:
  bearertokenauth/withscheme:
    scheme: Bearer
    token: 8a25f6ef-4099-1b37-522e-6cee61eb5c95 #Must match TOKEN from livenx
processors:
  batch:
    timeout: 0s
  batch/logs:
    send batch max size: 100
```

- Hit Ctrl+O and then Hit "Enter".
- Hit Ctrl+X to save and exit.

Configuration at LiveWire to Ingest LiveAssurance Alerts in LiveNX

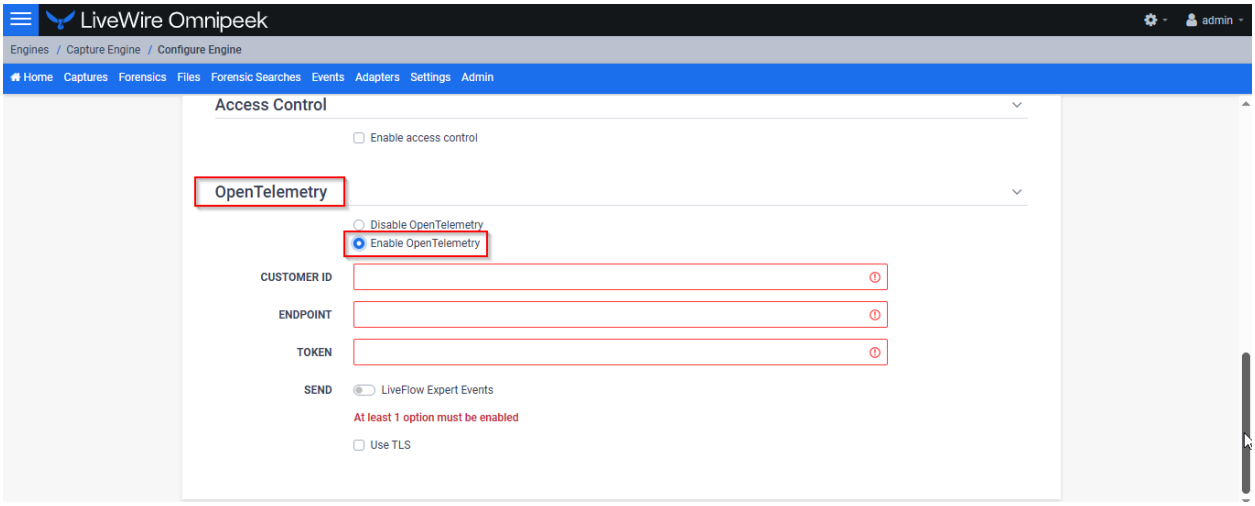
Capture Engine Configuration

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



- On *Configure Engine* page, scroll down to *OpenTelemetry* section.

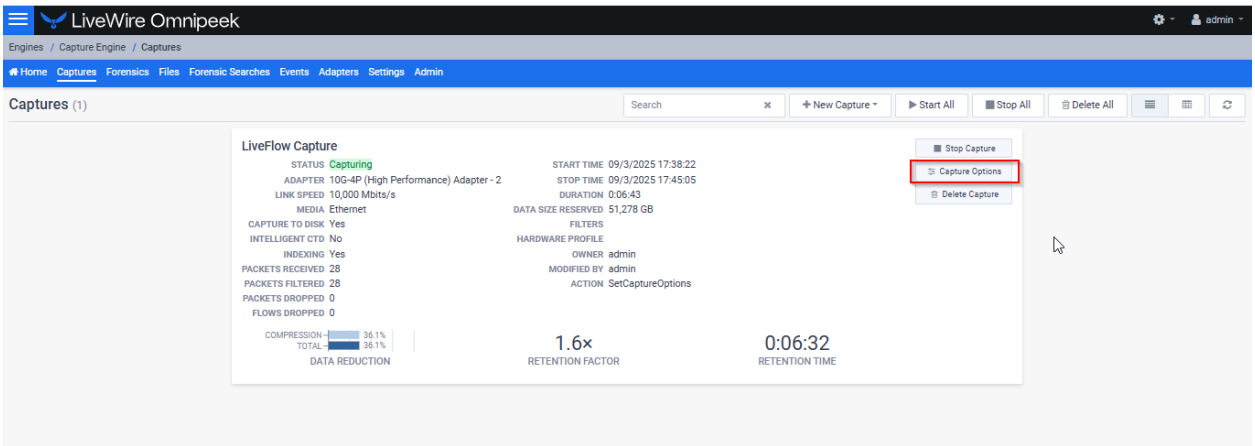
- Click *Enable Open Telemetry*.



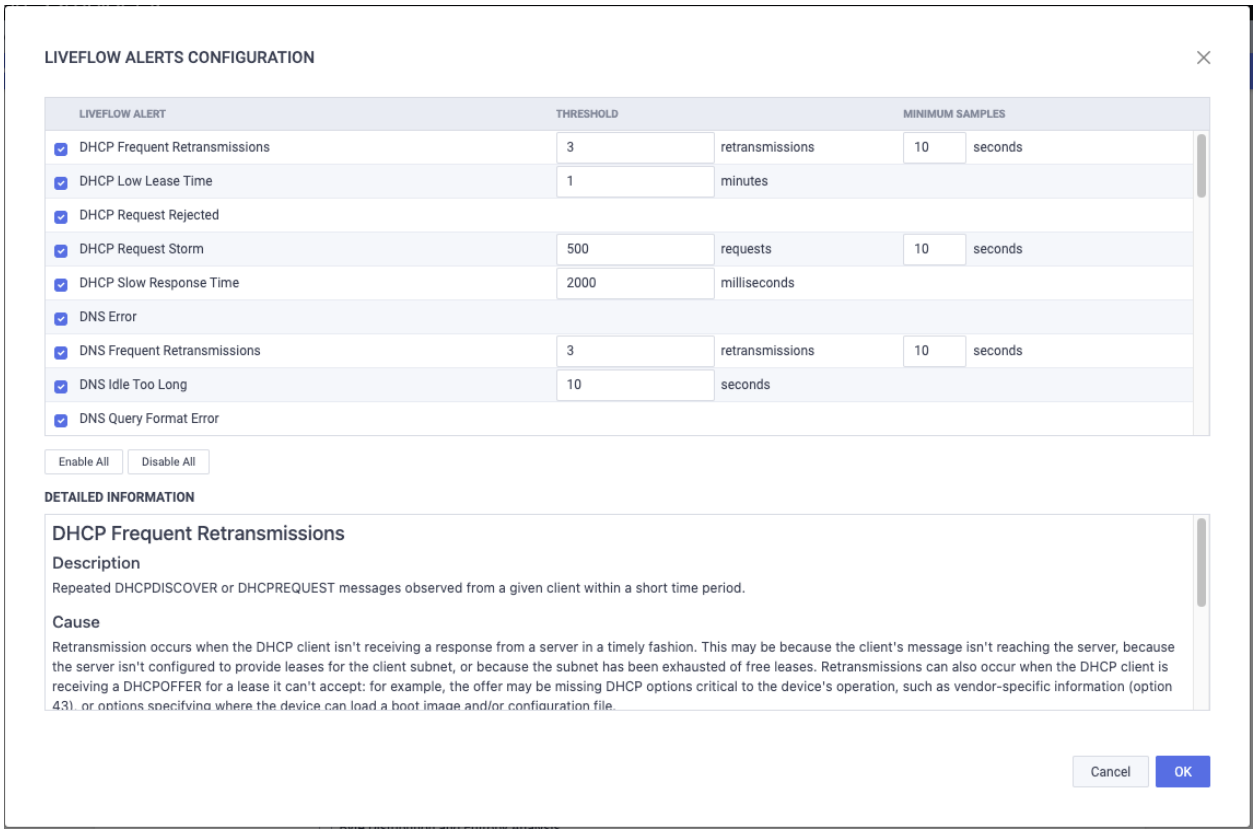
- Under *Open Telemetry* configure items below:
  - **Customer ID**: - This value is not used by LiveNX but it must be populated, and it must be a string (not an integer).
  - **Endpoint**: - This value should point to the LiveNX server/port.
  - **Token**: - This value should match the token generated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

LiveFlow Capture Configuration

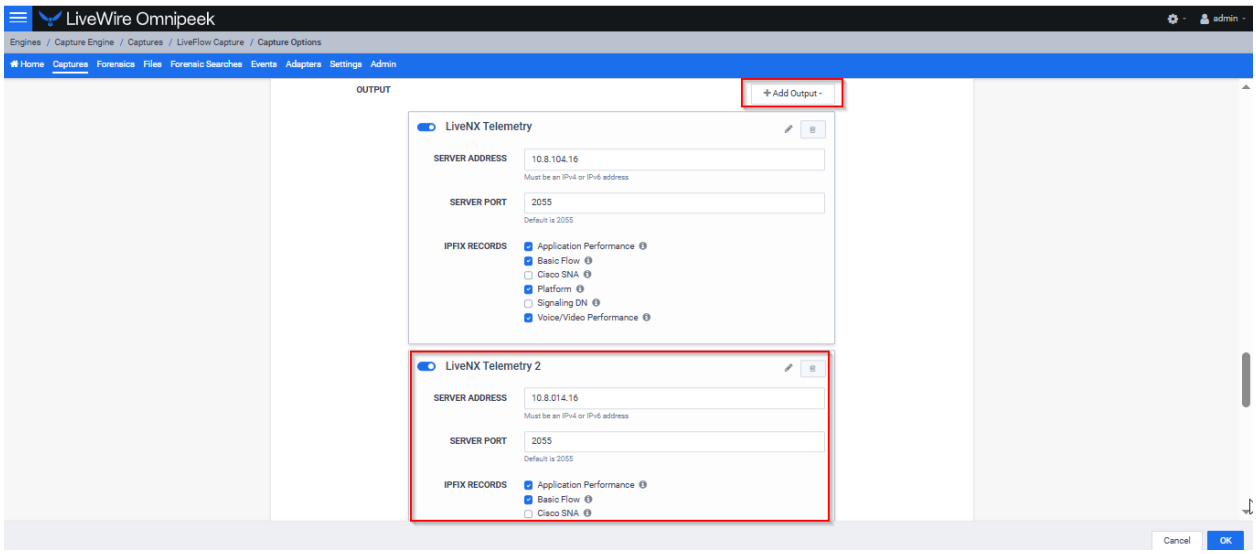
- From LiveWire Omnipeek, click *Captures*.
- Create a new LiveFlow Capture or edit existing LiveFlow capture.



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



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



◦ Click *OK* to save and exit.

LiveAssurance – Network Security

Overview

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

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

Freemium Licensing

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

Features and Benefits

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

Prerequisites

To use LiveAssurance, ensure:

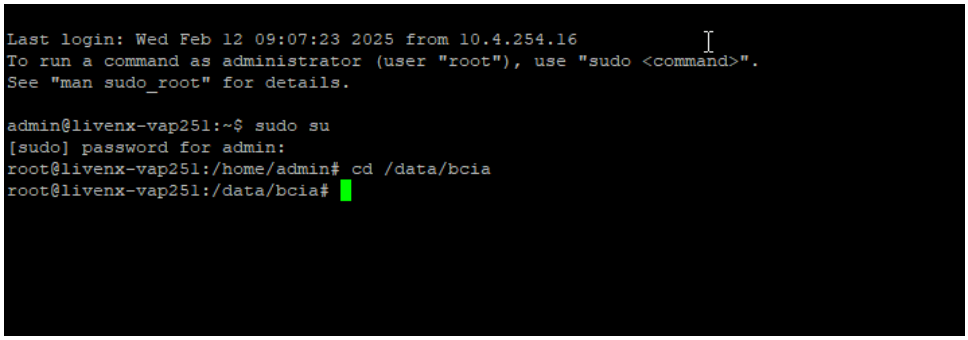
- LiveNX is upgraded to version 25.1.0 or later.
- LiveAssurance Freemium requires a working Internet connection to download the BCIA Freemium containers from our privately-maintained docker registry. If necessary, please add `indeni-docker.jfrog.io` to your firewall whitelist.
- Devices have SSH enabled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

Installation and Setup

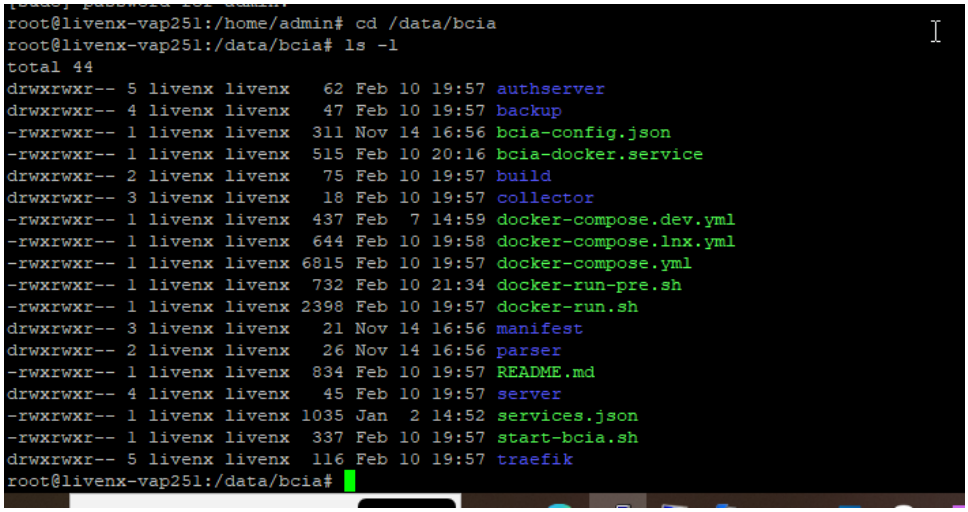
Enabling LiveAssurance (BCIA)

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

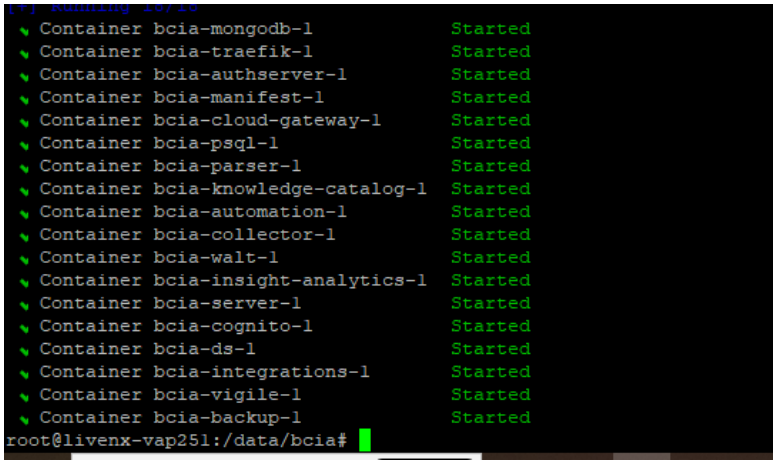
- Navigate to the LiveAssurance working directory: *cd /data/bcia*.



- Verify the LiveAssurance files: `ls -la`.



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

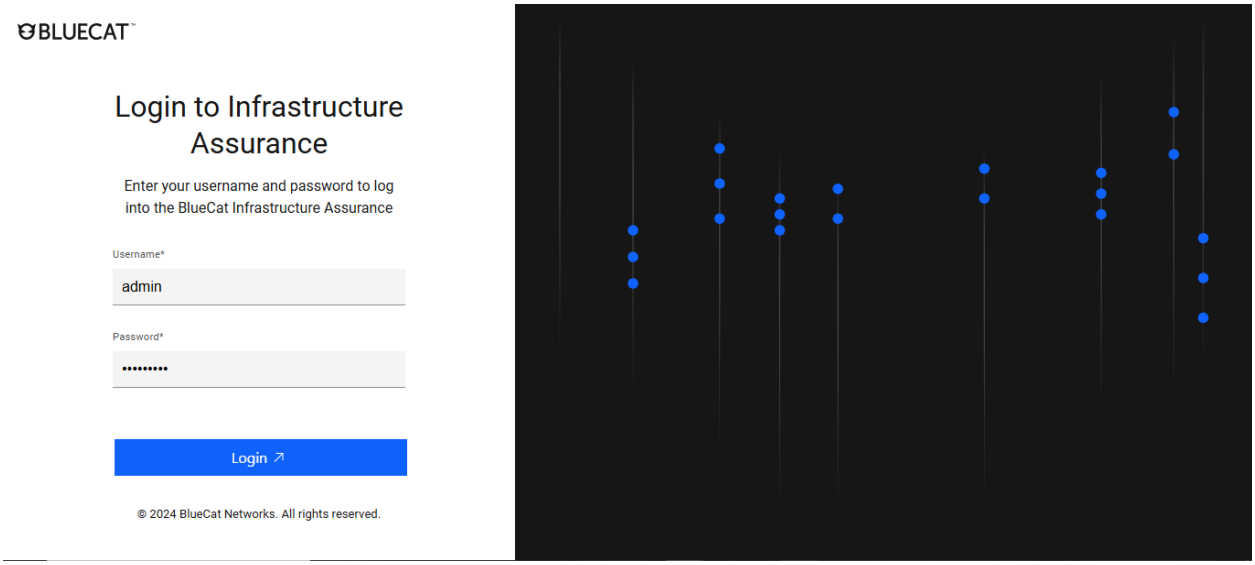


- Access LiveAssurance via a browser at *<LiveNX-URL>:5443*.

Accessing the LiveAssurance Web Interface

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

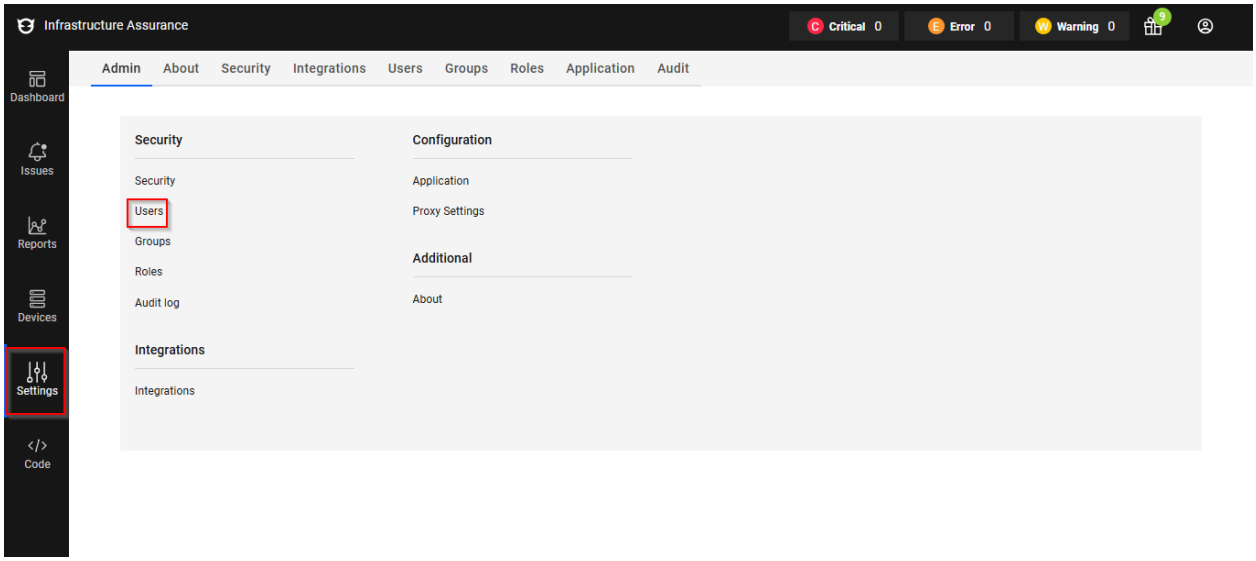
- Log in using default credentials (*admin/admin123!*).



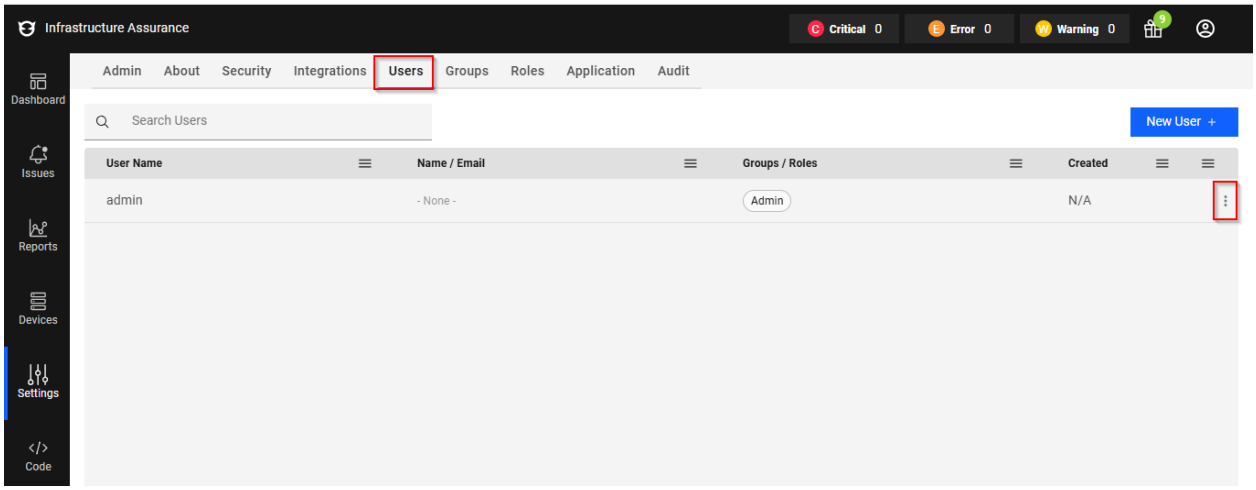
- Acknowledge the LiveAssurance Insight Confirmation.

Changing Default Credentials

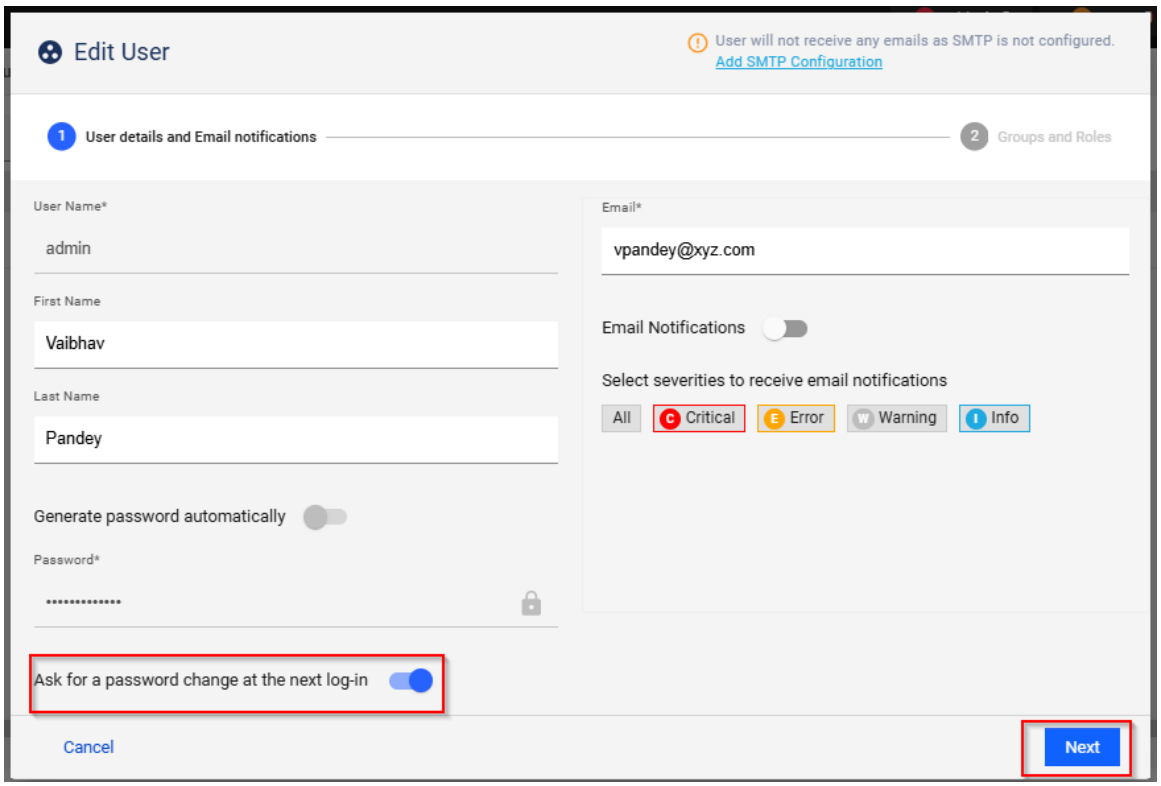
- Navigate to *Settings > Users*.



- Click on the admin user and select *Edit*.



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



- Click *Next* and then *Save*.

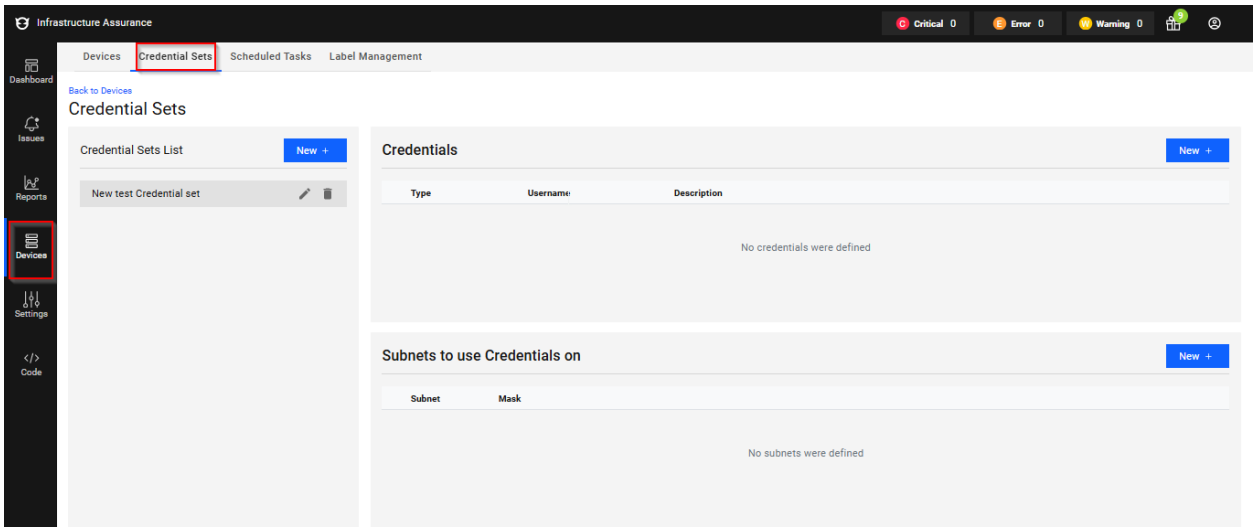
- Log out and log back in to change the password.

Device Onboarding and Credential Management

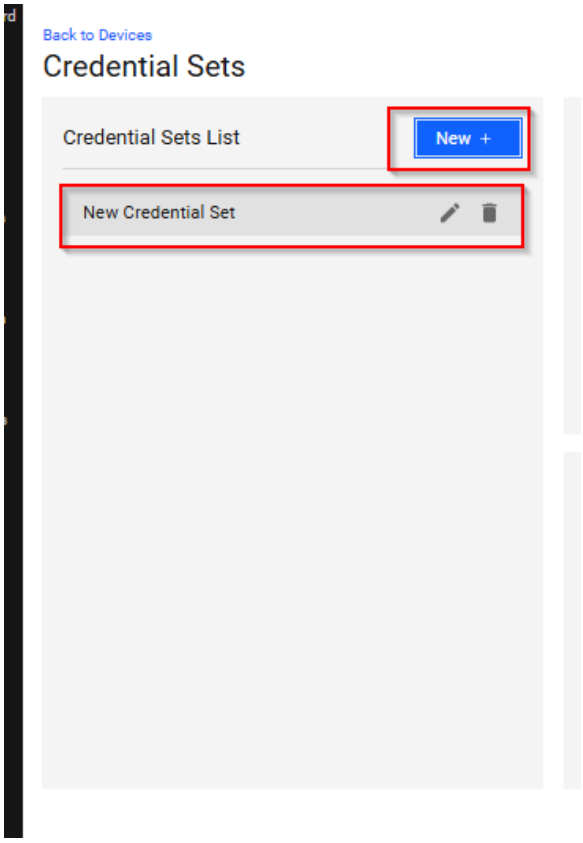
Creating Credential Sets

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

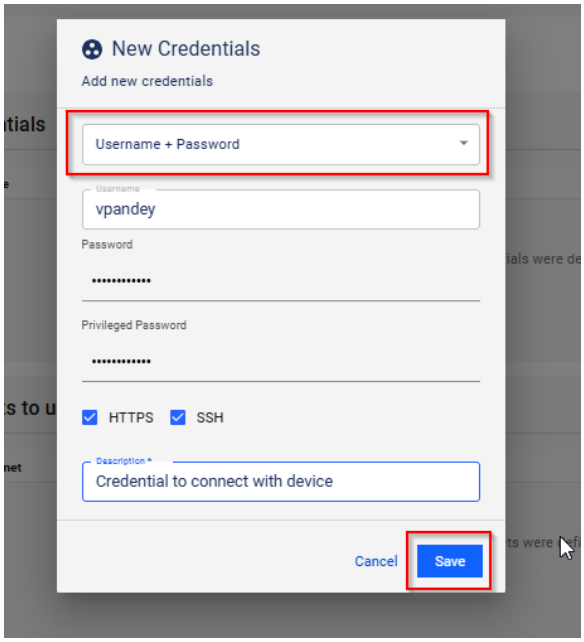
- Navigate to *Devices* > *Credential Sets*.



- Click *New* to create a credential set.



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

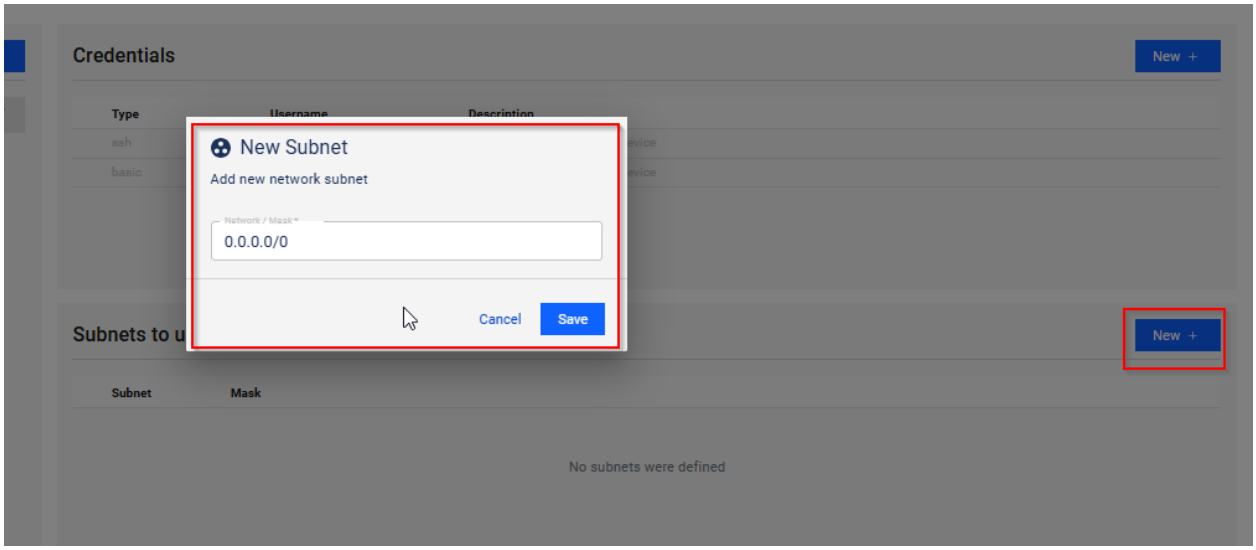


Configuring Subnets for Credentials

The credentials also include the subnet which will use those credentials. If all of your devices are using the same credentials, you can simply set this to 0.0.0.0/0 to have it apply to all devices. Otherwise, if your devices use different credentials, you can create multiple credential sets, and then specify the network and mask for each (which can be an exact IP address such as 94.94.94.17/32 or a subnet such as 94.94.0.0/16).

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

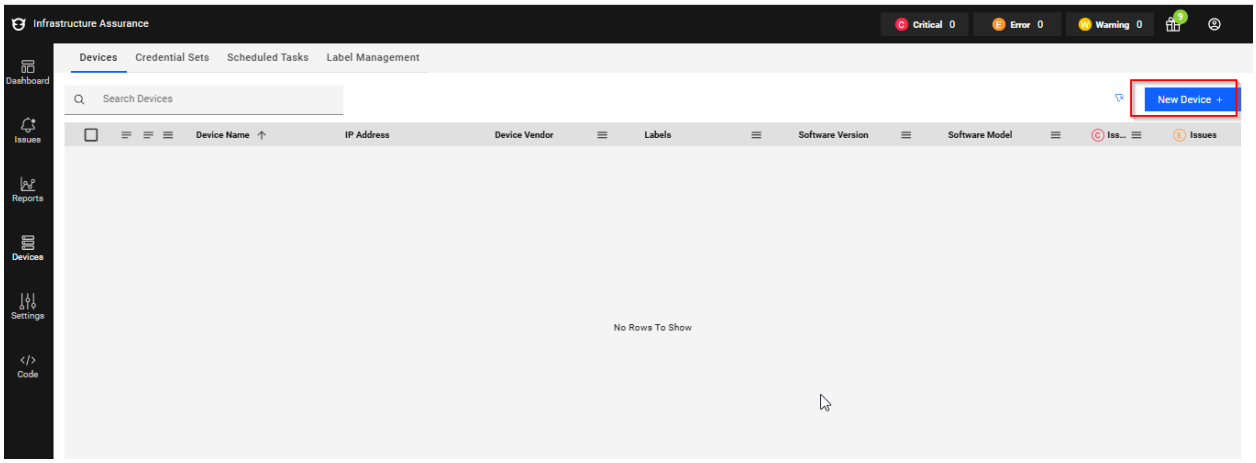
- To add the Subnets, click on the *New* button to add the subnets.



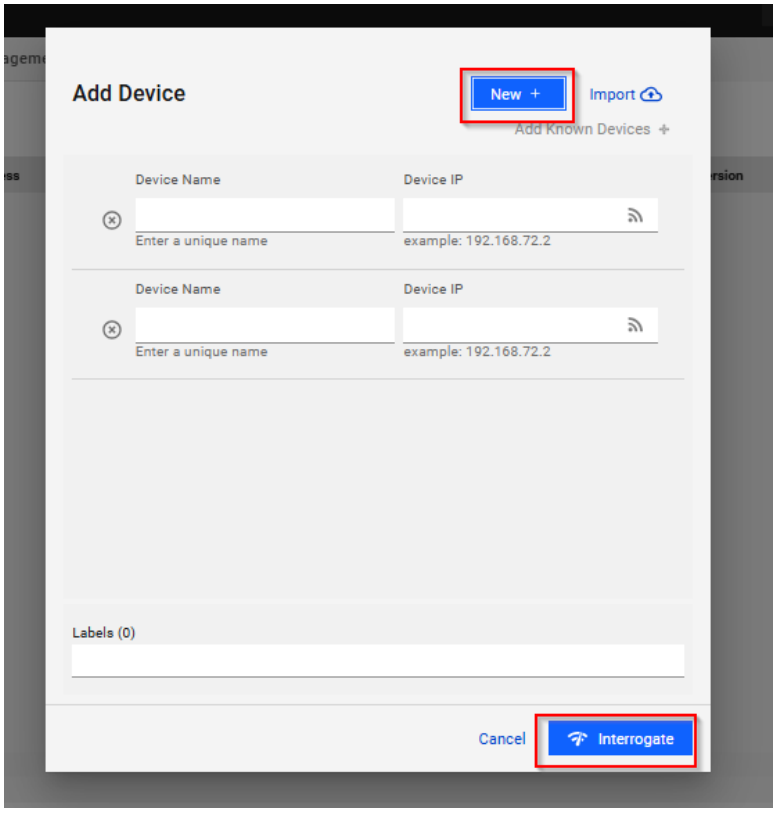
- Assign credentials to specific subnets.
- Use `0.0.0.0/0` for all devices.
- Configure multiple credential sets for different subnet ranges.
- If overlapping subnets exist, LiveAssurance prioritizes the most specific subnet.

Adding Devices for Inspection

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



- Enter the device name and IP address.



- Click *Interrogate*.

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

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

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

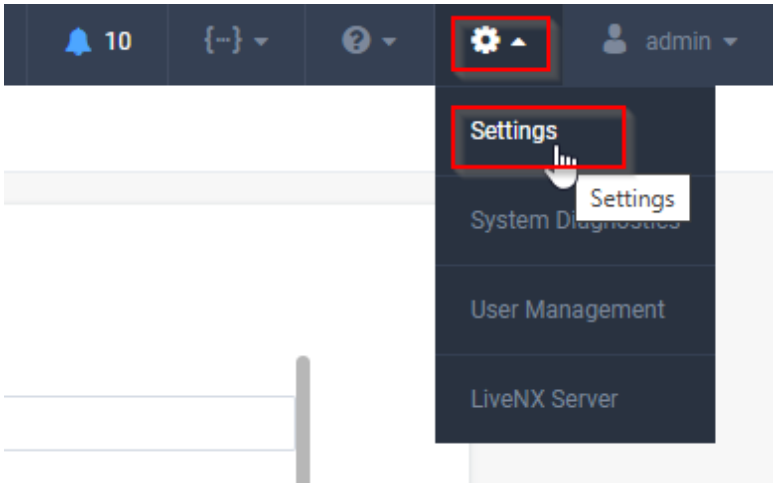
Sending LiveAssurance Alerts to LiveNX

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

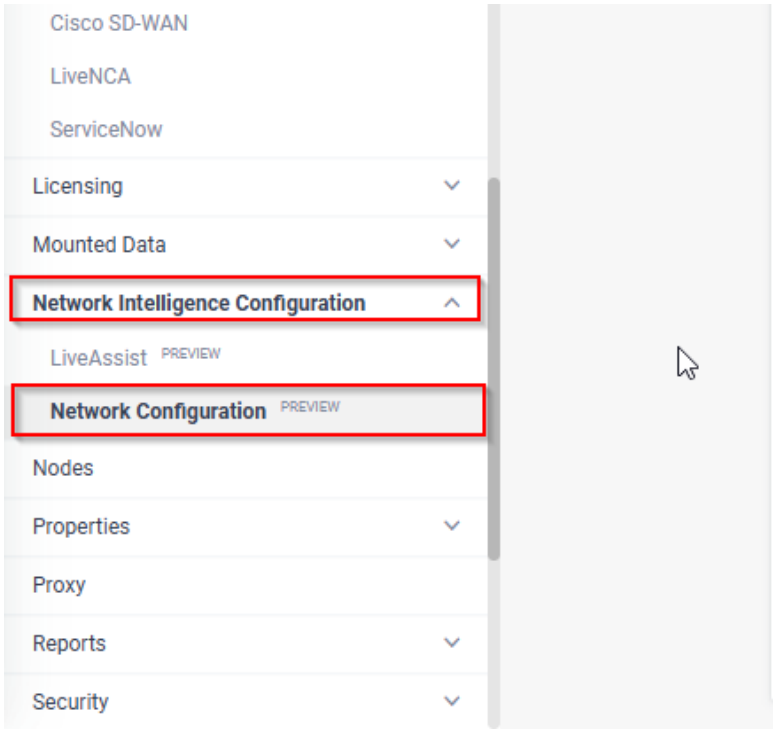
Collecting LiveAction Receiver Configuration Token From LiveNX

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

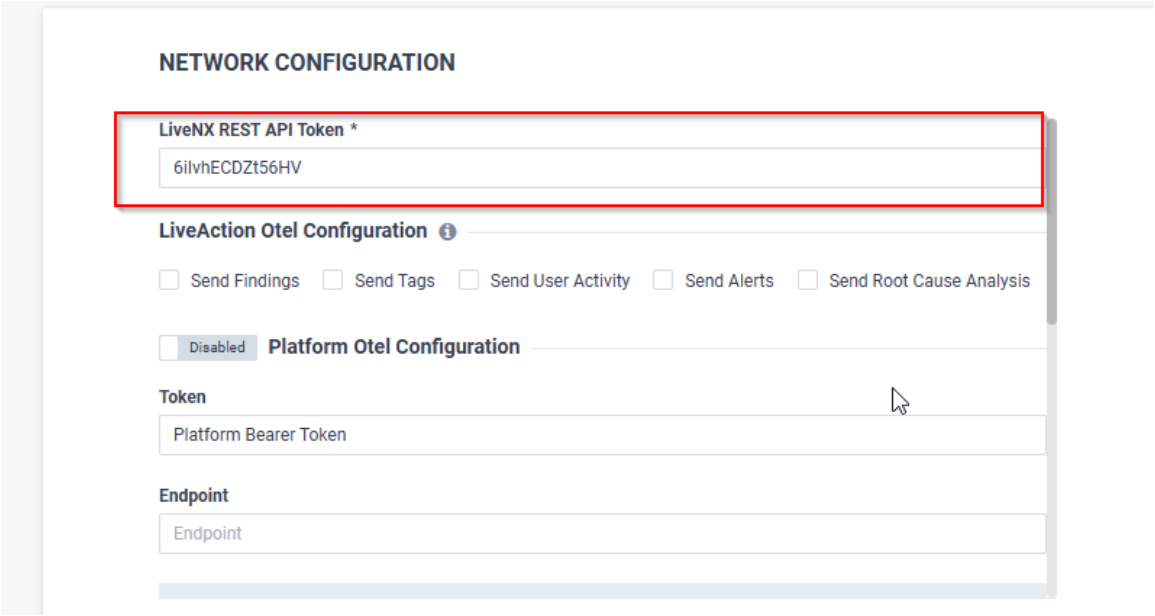
- Login to LiveNX web and select the gear icon available on the navigation bar.



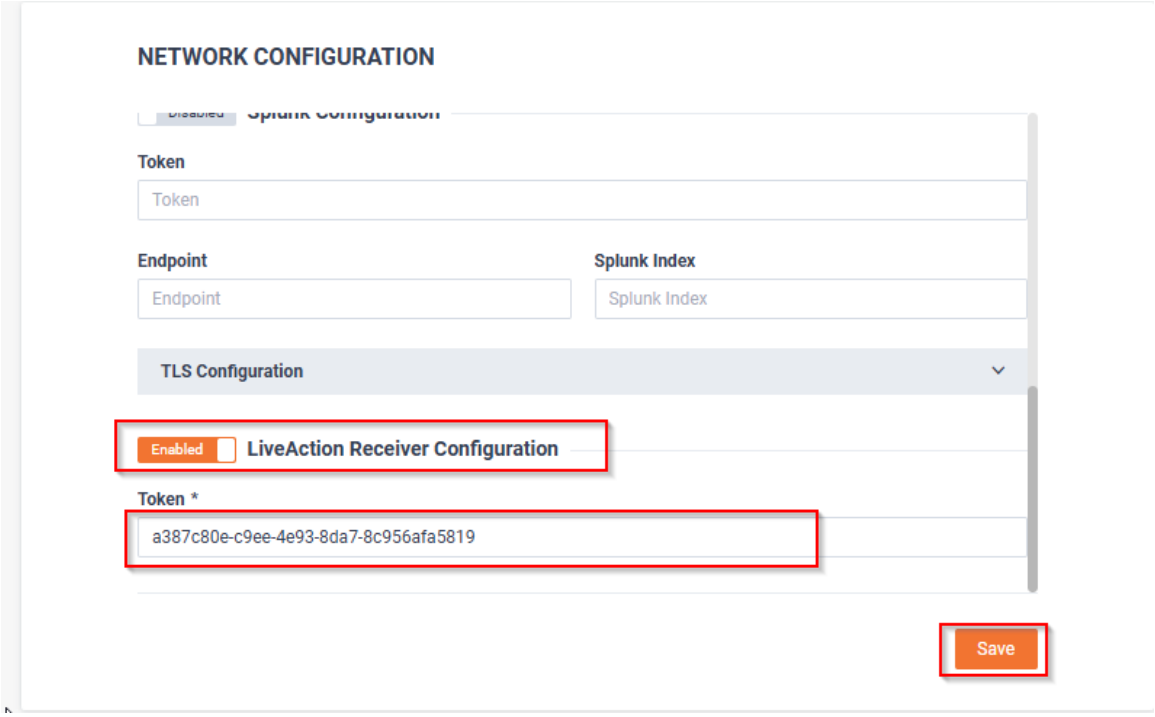
- Under Network Intelligence Configuration, select *Network Configuration*.



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



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



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

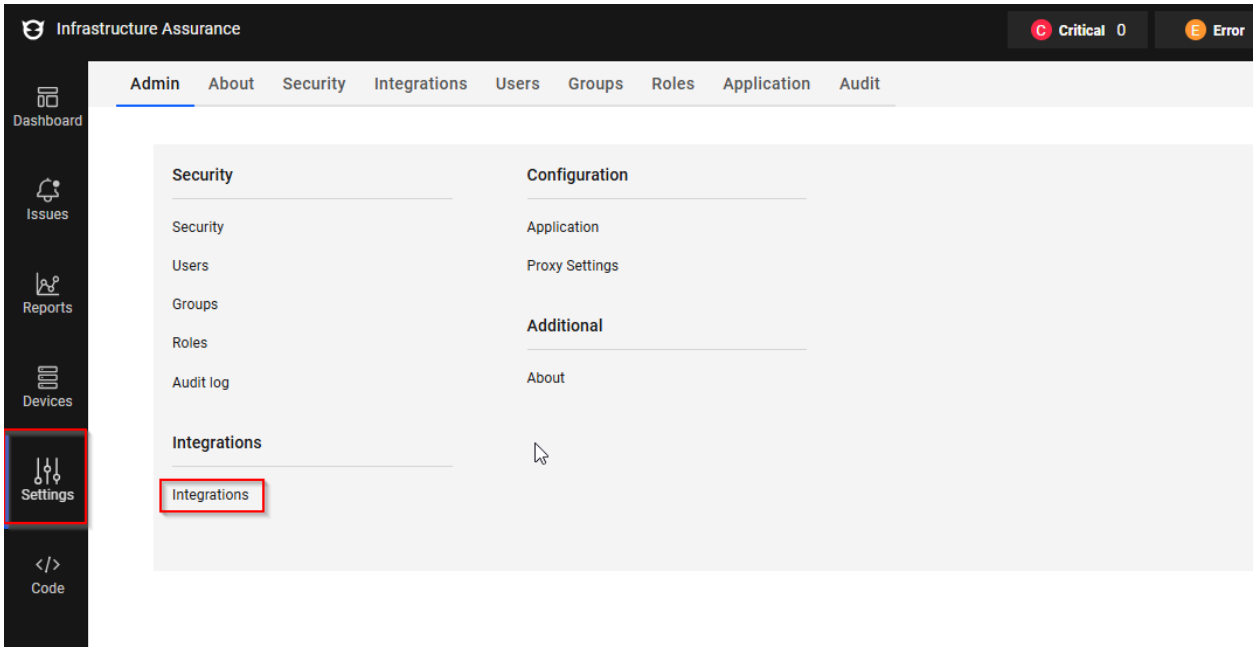
Note Green field deployments will always be pre-populated with a UUID.

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

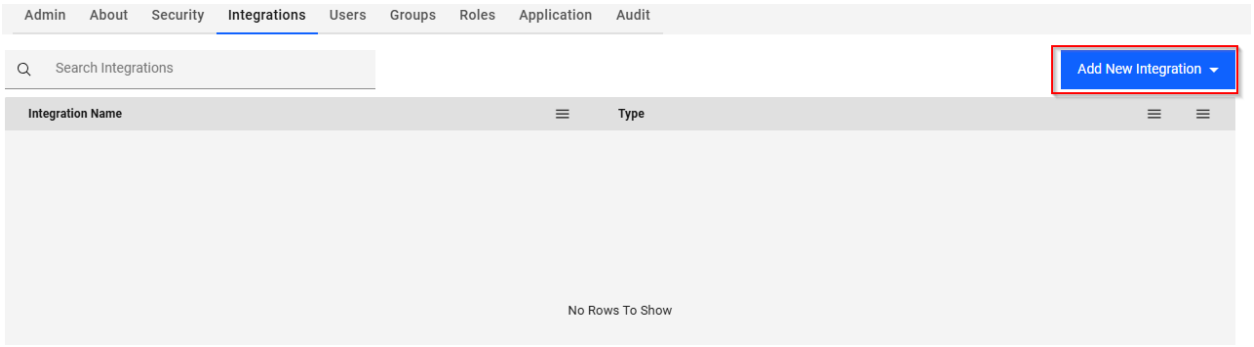
Configuring LiveAssurance For LiveNX integration.

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

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



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



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

```
cd /data/bcia && docker compose restart authserver
```

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

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

Operations and Monitoring

Reviewing Alerts

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

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

Policy Tuning

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

Generating Reports

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

LiveAssurance (BCIA) Dashboard

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

Troubleshooting

Common Errors and Resolutions

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

Connectivity Issues

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

Conclusion

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

Maintenance Mode Schedule

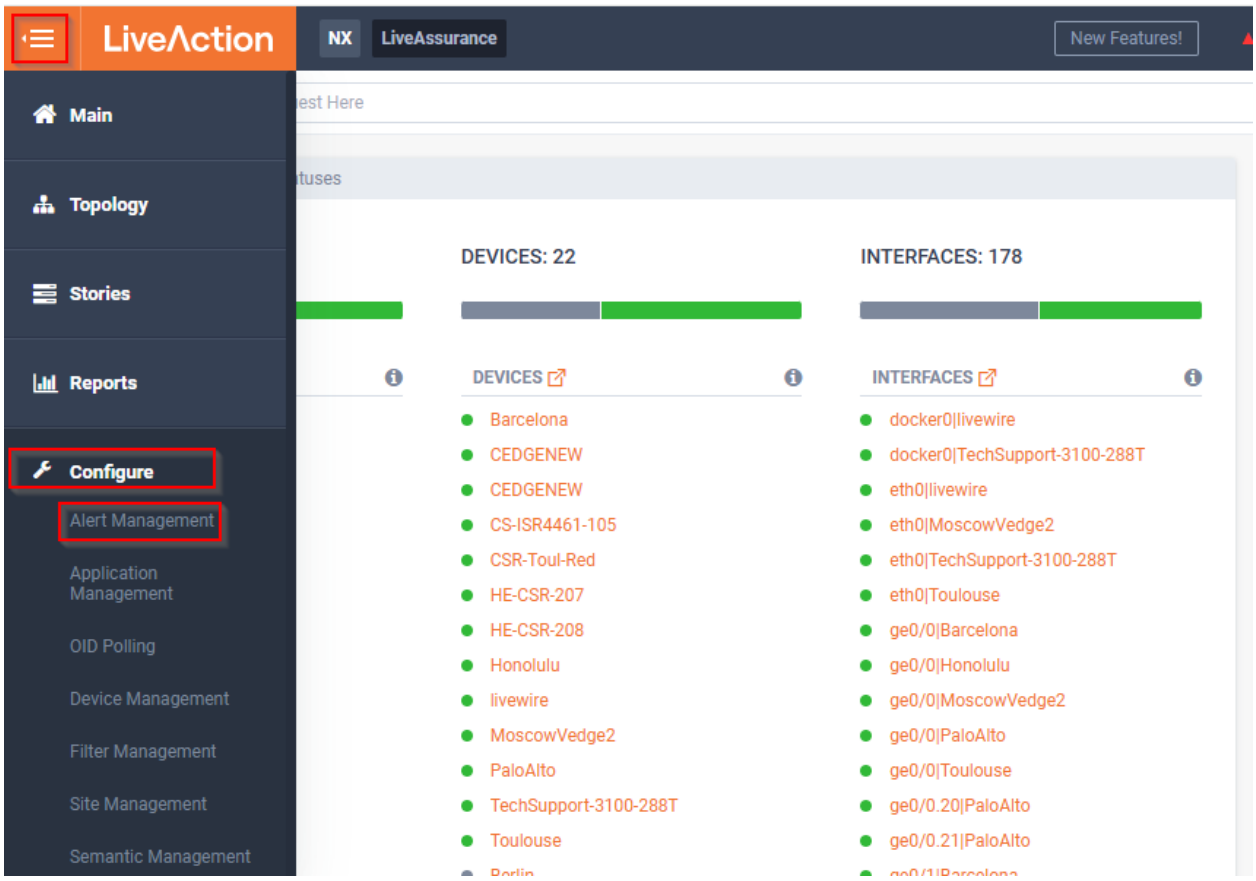
Overview

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

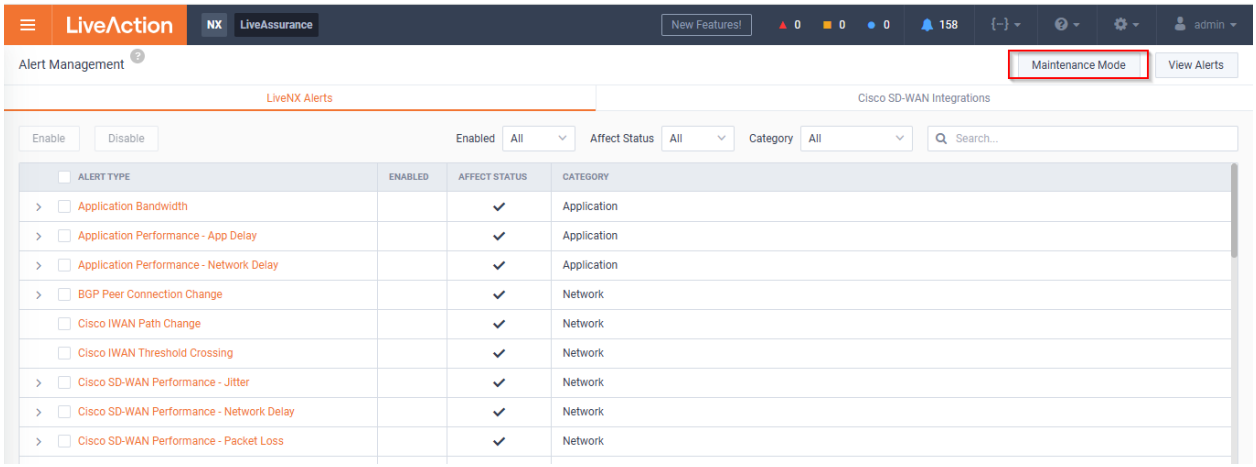
Maintenance Mode Configuration

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

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



- On the *Alert Management* page click on the *Maintenance Mode* button.



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

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