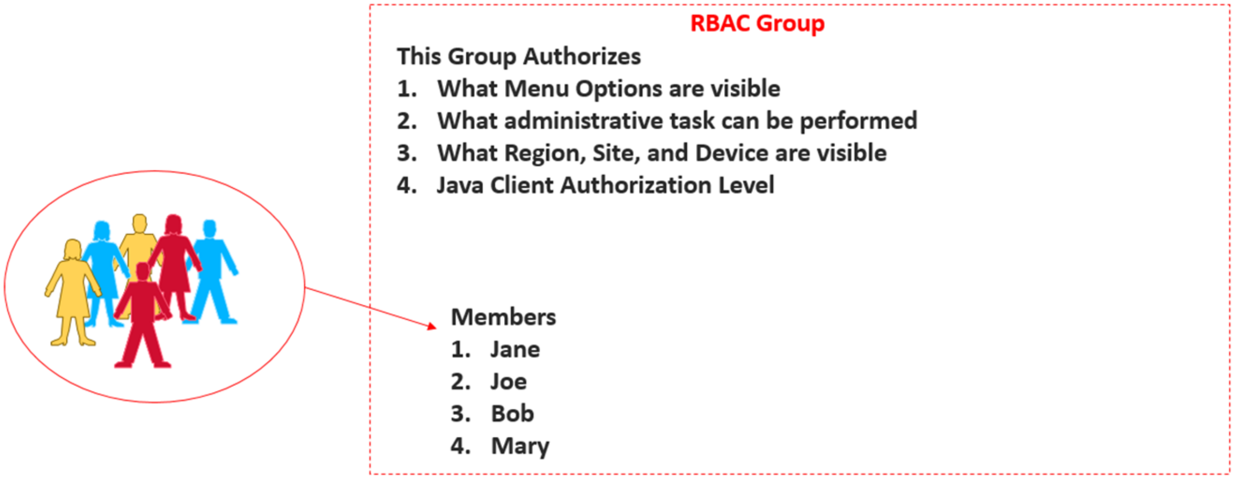
LiveAction

RBAC Updates in LiveNX 21.3.0

The Role Based Access Control (RBAC) framework has been updated in LiveNX 21.3.0 to be based on groups. This document will act as a supplemental addendum to the *LiveNX Operations Dashboard Admin Guide*.

Groups

The following diagram depicts the updated design:



RBAC Group

This Group Authorizes

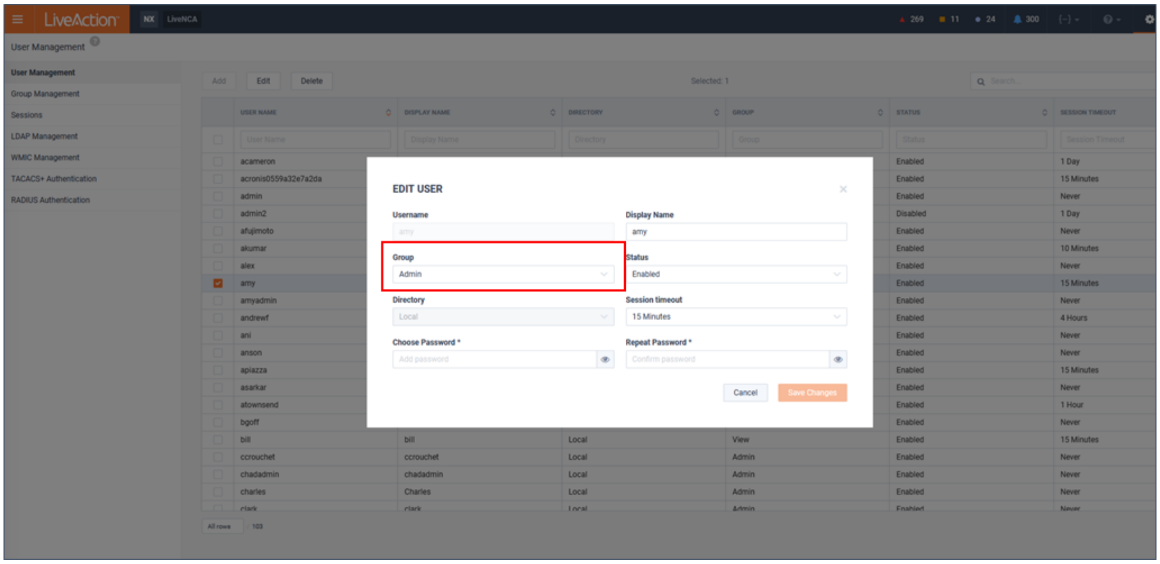
1. **What Menu Options are visible**
2. **What administrative task can be performed**
3. **What Region, Site, and Device are visible**
4. **Java Client Authorization Level**

Members

1. **Jane**
2. **Joe**
3. **Bob**
4. **Mary**

Groups are given authorization to access specific LiveNX capabilities, perform specific tasks, and access specific devices' data for monitoring and reporting. Users are added as members to a Group. Roles that were formally assigned directly to Users are now assigned to Groups.

After upgrading to 21.3, LiveNX Users will be assigned to a Group. The Group given to a User during the update process will be based on the User's Role in the previous version of LiveNX.



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
□	acameron				Enabled	1 Day
□	acronis0559a32e7a2da				Enabled	15 Minutes
□	admin				Enabled	Never
□	admin2				Disabled	1 Day
□	afujimoto				Enabled	Never
□	akumar				Enabled	10 Minutes
□	alex				Enabled	Never
☑	amy				Enabled	15 Minutes
□	amyadmin				Enabled	Never
□	andrewf				Enabled	4 Hours
□	ani				Enabled	Never
□	anson				Enabled	Never
□	apiazza				Enabled	15 Minutes
□	asarkar				Enabled	Never
□	atownsend				Enabled	1 Hour
□	bgoff				Enabled	Never
□	bill	bill	Local	View	Enabled	15 Minutes
□	ccrouchet	ccrouchet	Local	Admin	Enabled	Never
□	chadadmin	chadadmin	Local	Admin	Enabled	Never
□	charles	Charles	Local	Admin	Enabled	Never
□	clark	clark	Local	Admin	Enabled	Never

All rows 103

EDIT USER

Username: amy

Display Name: amy

Group: Admin

Status: Enabled

Directory: Local

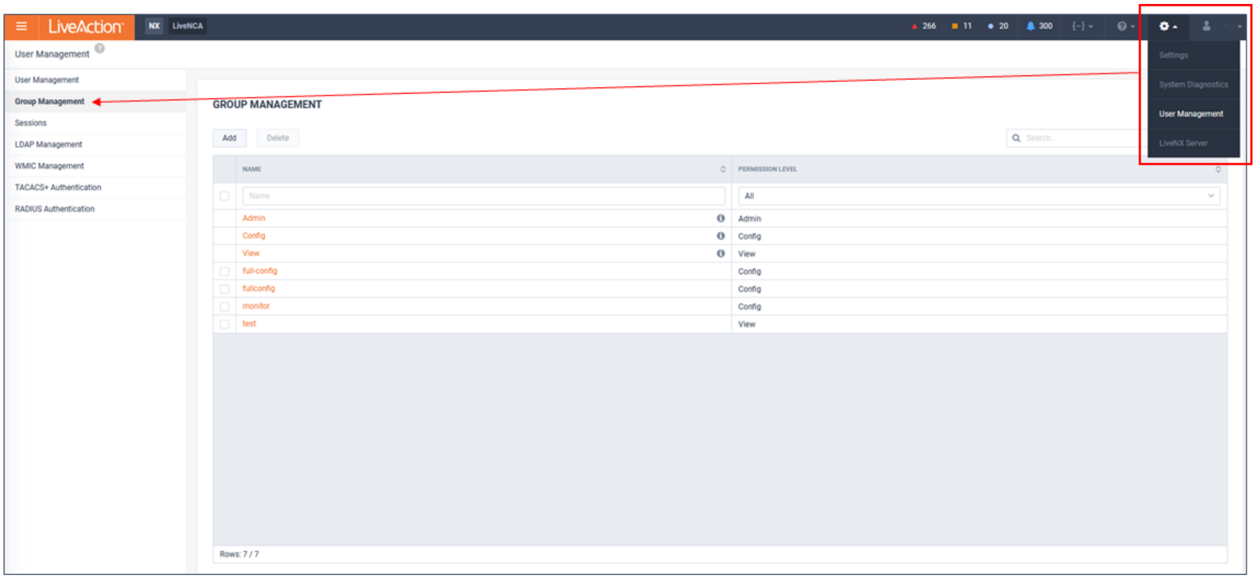
Session timeout: 15 Minutes

Choose Password *: Add password

Repeat Password *: Confirm password

Cancel Save Changes

Groups are managed from *Settings* > *User Management* > *Group Management*:

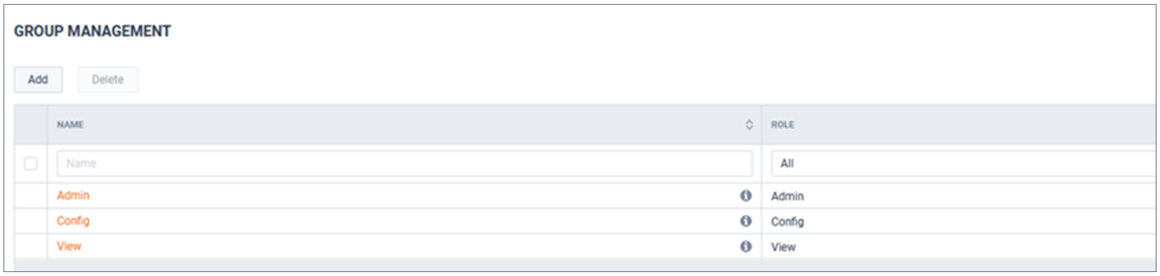


GROUP MANAGEMENT

	NAME	PERMISSION LEVEL
□	Name	All
	Admin	Admin
	Config	Config
	View	View
□	full-config	Config
□	fullconfig	Config
□	monitor	Config
□	test	View

Rows: 7 / 7

By default, there are three Groups in LiveNX: *Admin*, *Config*, and *View*. These three default groups cannot be deleted, and their role cannot be modified. Additional Groups can be added and fully modified. When upgrading from past versions of LiveNX, more groups may be automatically created to support any custom RBAC configuration that may have been implemented previously.



GROUP MANAGEMENT

	NAME	ROLE
□	Name	All
	Admin	Admin
	Config	Config
	View	View

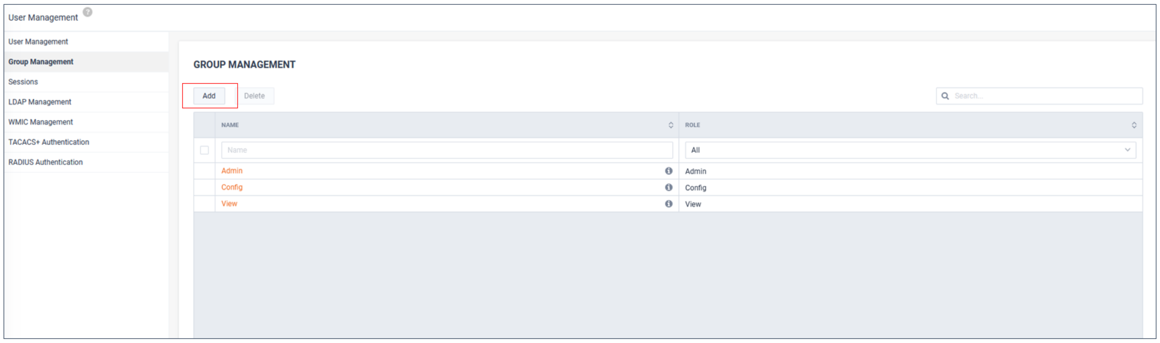
Role

As mentioned previously, LiveNX Roles are assigned to Groups. These Roles have been consolidated in 21.3.0 from six to three. The Group's Role defines the authorized capabilities for the members of the Group. There are three Roles available: *Admin*, *Config*, and *View*. There capabilities will be summarized in the table below:

New Role	Description	Device Access	Capabilities
Admin	Can perform any action for all resources. Is capable of making changes to the system that impact other users.	All devices	All capabilities
Config	Can perform any action for its selected resources. Is capable of making changes to the system that impact other users but at more 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)	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

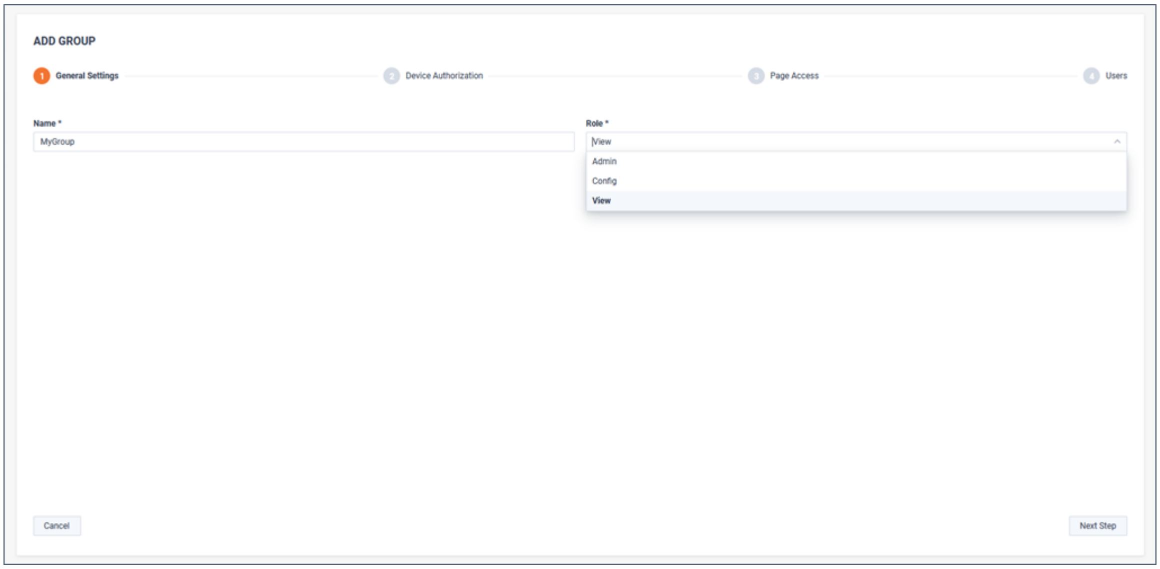
Adding a New Group

1. To begin Group management, click **Add**.



NAME	ROLE
Admin	Admin
Config	Config
View	View

2. Provide a *Name* and *Role*.

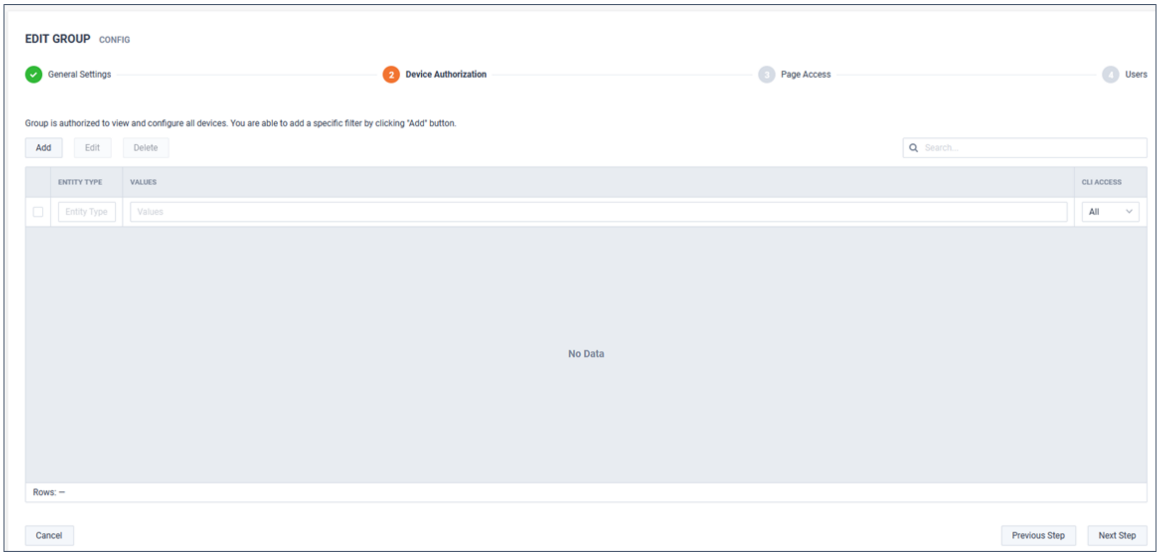


Name * MyGroup

Role * View

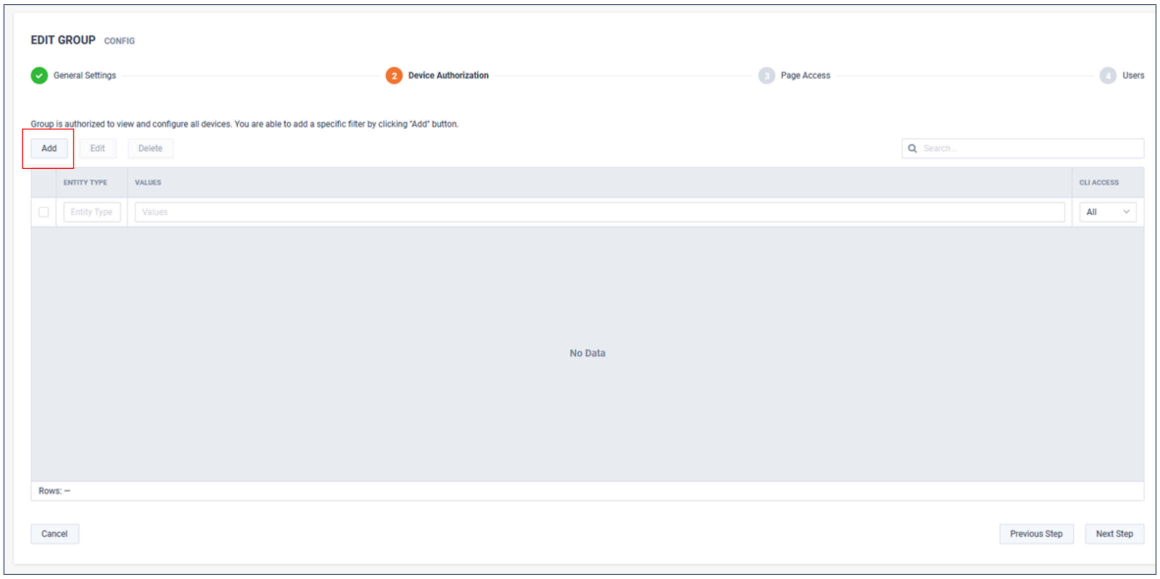
3. Assign device authorization.

   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.



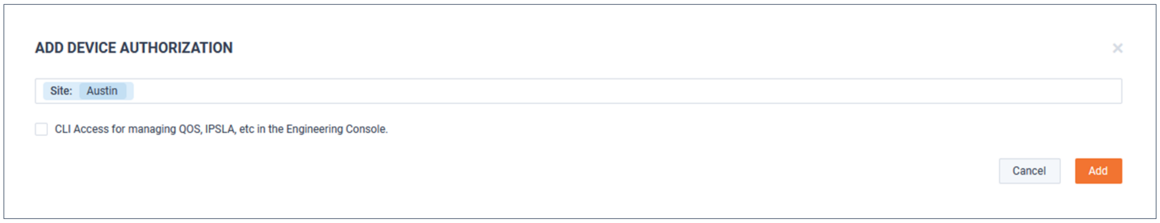
Group is authorized to view and configure all devices. You are able to add a specific filter by clicking "Add" button.

To restrict authorization to a specific device(s), click **Add**.



Group is authorized to view and configure all devices. You are able to add a specific filter by clicking "Add" button.

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



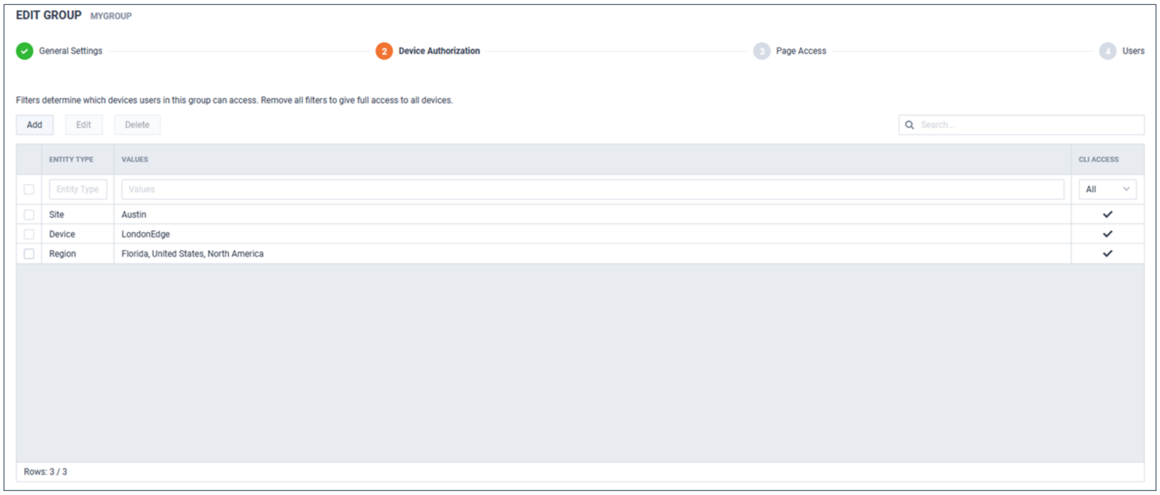
Site: Austin

□ CLI Access for managing QOS, IPSLA, etc in the Engineering Console.

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

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

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



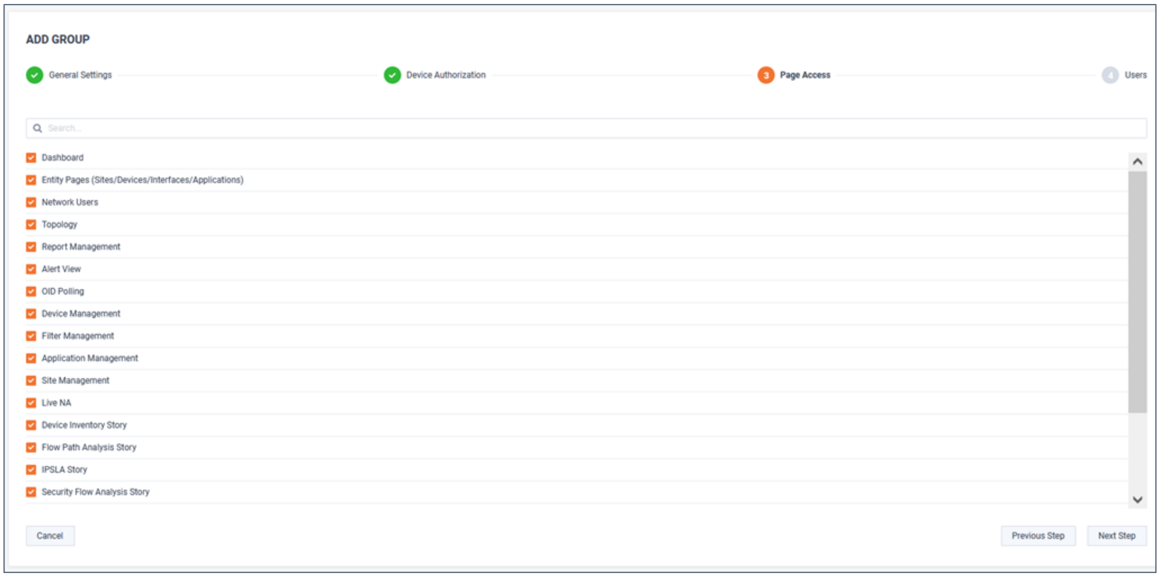
EDIT GROUP MYGROUP

Filters determine which devices users in this group can access. Remove all filters to give full access to all devices.

	ENTITY TYPE	VALUES	CLI ACCESS
□	Entity Type	Values	All
□	Site	Austin	✓
□	Device	LondonEdge	✓
□	Region	Florida, United States, North America	✓

Rows: 3 / 3

4. Assign Operations Dashboard (WebUI) page access.



ADD GROUP

- ☑ Dashboard
- ☑ Entity Pages (Sites/Devices/Interfaces/Applications)
- ☑ Network Users
- ☑ Topology
- ☑ Report Management
- ☑ Alert View
- ☑ OID Polling
- ☑ Device Management
- ☑ Filter Management
- ☑ Application Management
- ☑ Site Management
- ☑ Live NA
- ☑ Device Inventory Story
- ☑ Flow Path Analysis Story
- ☑ IPSLA Story
- ☑ Security Flow Analysis Story

Operations Dashboard (WebUI) page access can be limited per role:

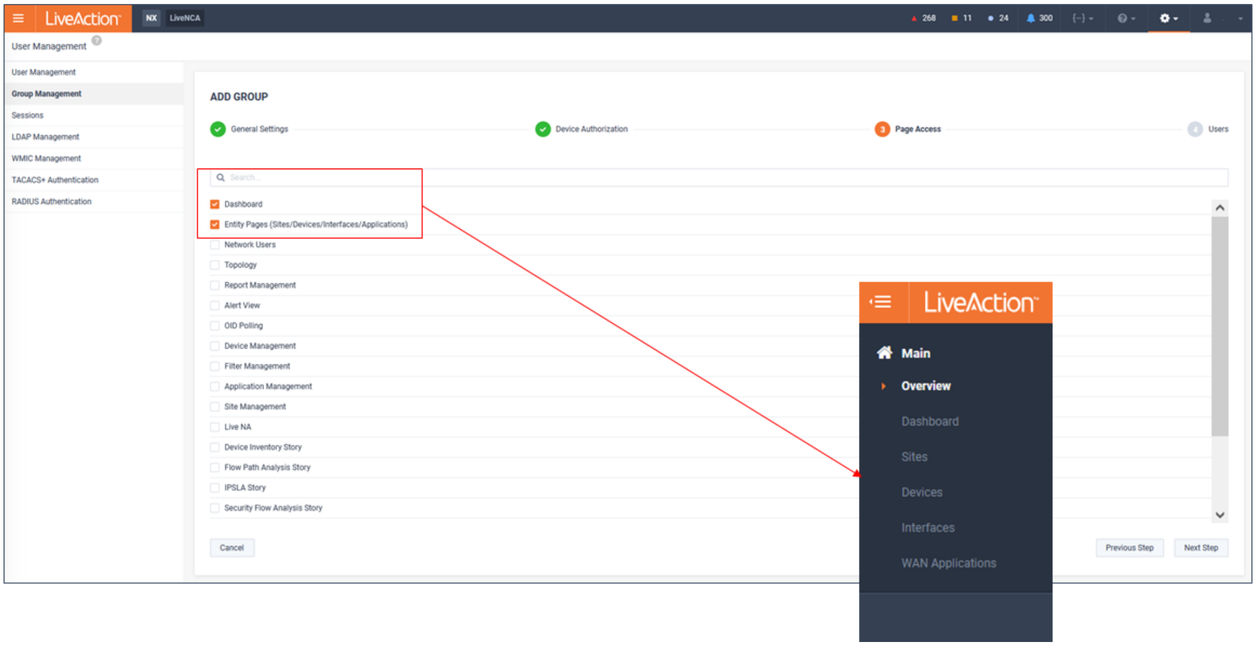
- Most pages are accessible by all Roles.
- Some pages are accessible to only Admins.
- Some pages are accessible to Admins and Config.

Below is a table showing the pages only available to Admin and Config Roles:

Section	Page	Required Page Access	Required Role
Configure	Alert Management	–	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

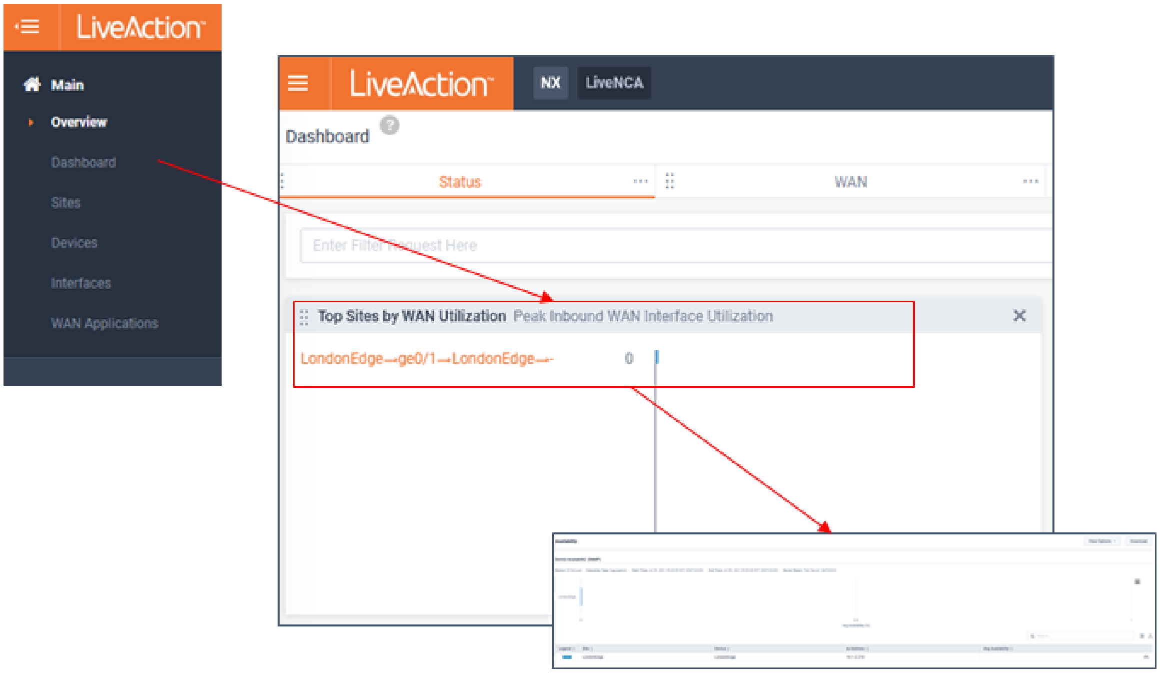
Section	Page	Required Page Access	Required Role
Configure	Site Management	Site Management	config/admin
Gear Icon	Settings	–	admin
Gear Icon	User Management	–	admin
Gear Icon	LiveNX Server	–	admin

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

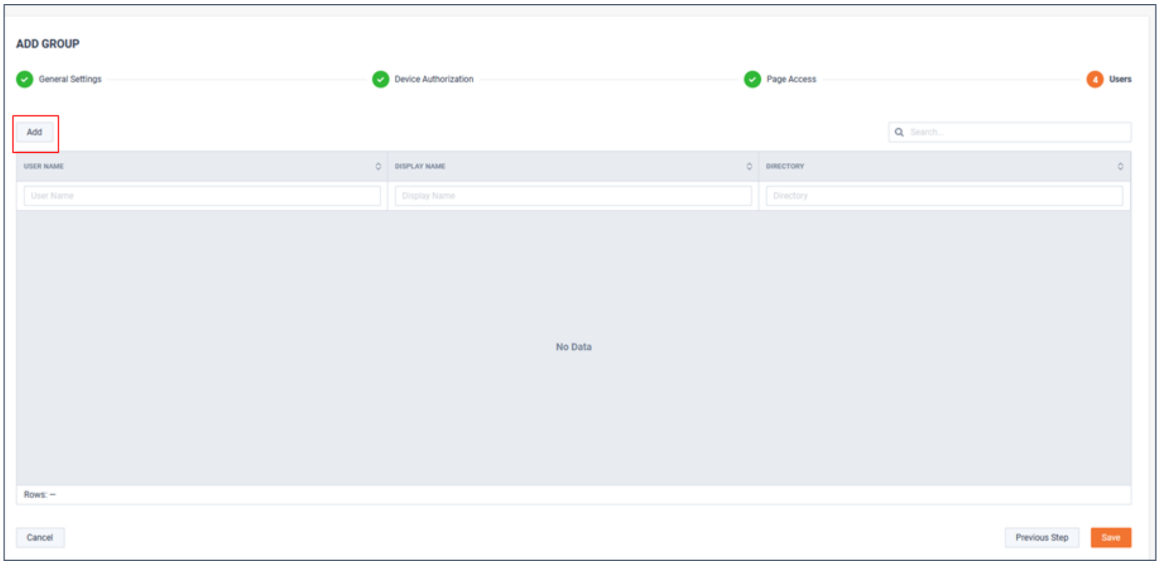


☑ Dashboard
☑ Entity Pages (Sites/Devices/Interfaces/Applications)
☐ Network Users
☐ Topology
☐ Report Management
☐ Alert View
☐ OID Polling
☐ Device Management
☐ Filter Management
☐ Application Management
☐ Site Management
☐ Live NA
☐ Device Inventory Story
☐ Flow Path Analysis Story
☐ IPSLA Story
☐ Security Flow Analysis Story

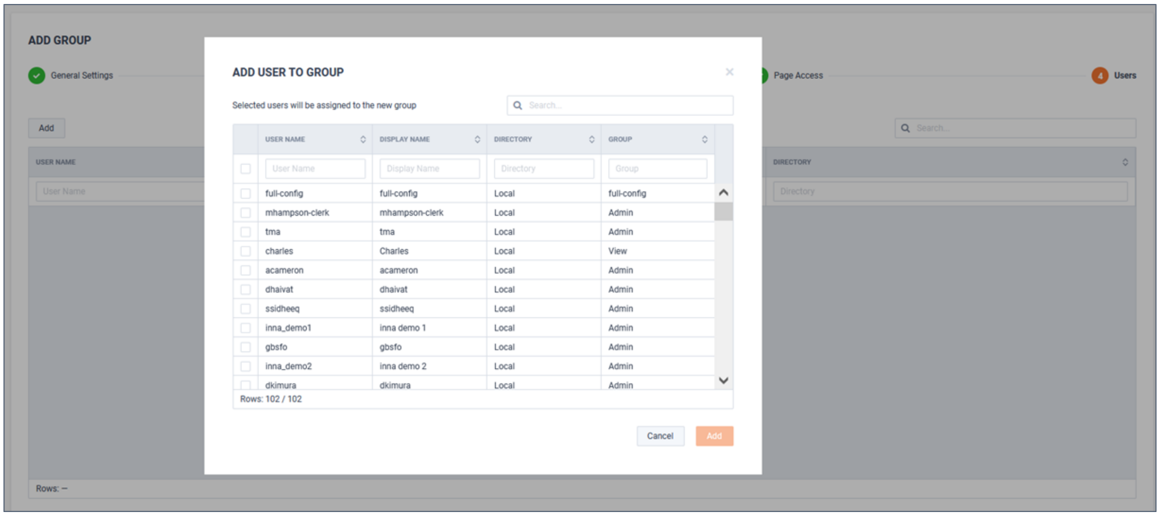
Do note that even though the Navbar may be restricted, some drill-down workflows will still allow limited functionality to pages not directly available from the Navbar. Using the previous example, where Dashboards were one of the limited options made available, these pages allow drill-down to reports,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


LiveAction
Main
Overview
Dashboard
Sites
Devices
Interfaces
WAN Applications
LiveAction
NX
LiveNCA
Dashboard
Status
WAN
Enter Filter Request Here
Top Sites by WAN Utilization Peak Inbound WAN Interface Utilization
LondonEdge→ge0/1→LondonEdge→-
0

5. Add a user(s) to group by clicking **Add**.



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

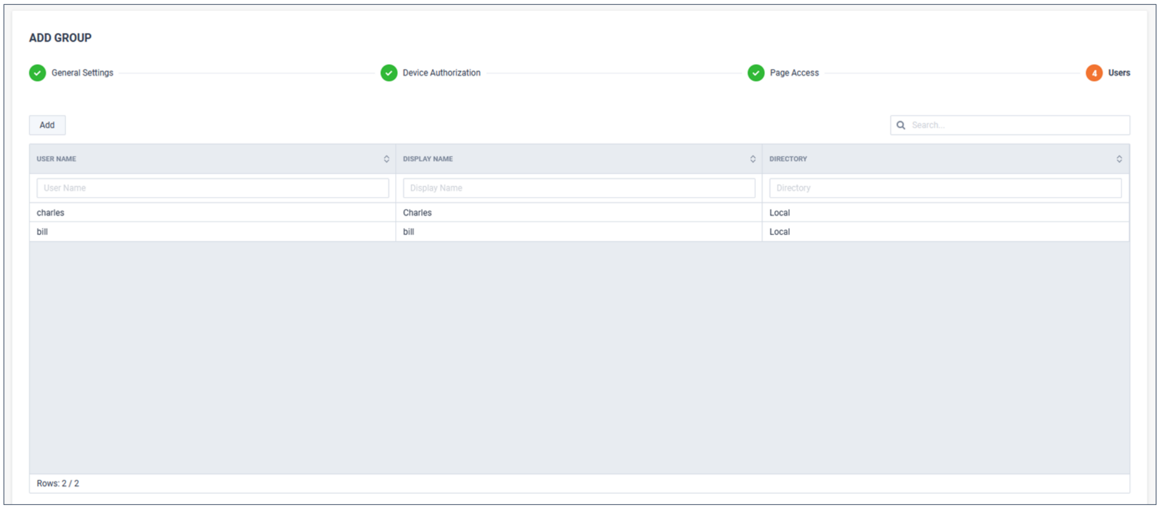


Selected users will be assigned to the new group

□	USER NAME	DISPLAY NAME	DIRECTORY	GROUP
□	User Name	Display Name	Directory	Group
□	full-config	full-config	Local	full-config
□	mhampson-clerk	mhampson-clerk	Local	Admin
□	tma	tma	Local	Admin
□	charles	Charles	Local	View
□	acameron	acameron	Local	Admin
□	dhaivat	dhaivat	Local	Admin
□	ssidheeq	ssidheeq	Local	Admin
□	inna_demo1	inna demo 1	Local	Admin
□	gbsfo	gbsfo	Local	Admin
□	inna_demo2	inna demo 2	Local	Admin
□	dkimura	dkimura	Local	Admin

Rows: 102 / 102

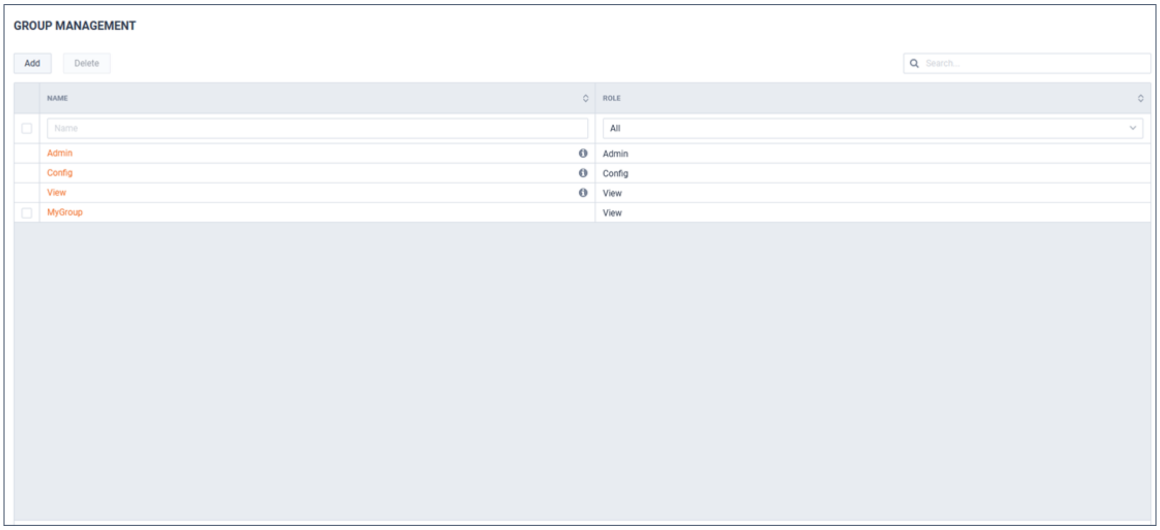
In this example, users *Charles* and *Bill* will be a member of this group.



USER NAME	DISPLAY NAME	DIRECTORY
User Name	Display Name	Directory
charles	Charles	Local
bill	bill	Local

Rows: 2 / 2

The new Group will now be listed on the *Group Management* page.



□	NAME	ROLE
□	Name	All
	Admin	Admin
	Config	Config
	View	View
□	MyGroup	View