ProSoft TECHNOLOGY

Where Automation Connects.

ELX3

Industrial Edge Gateway

December 19, 2025

USER MANUAL

Your Feedback Please

We always want you to feel that you made the right decision to use our products. If you have suggestions, comments, compliments or complaints about our products, documentation, or support, please write or call us.

ProSoft Technology, Inc.
+1 (661) 716-5100
+1 (661) 716-5101 (Fax)
www.prosoft-technology.com
ps.support@belden.com

ELX3 User Manual
For Public Use.

December 19, 2025

Content Disclaimer

This documentation is not intended as a substitute for and is not to be used for determining suitability or reliability of these products for specific user applications. It is the duty of any such user or integrator to perform the appropriate and complete risk analysis, evaluation and testing of the products with respect to the relevant specific application or use thereof. Neither ProSoft Technology nor any of its affiliates or subsidiaries shall be responsible or liable for misuse of the information contained herein. Information in this document including illustrations, specifications and dimensions may contain technical inaccuracies or typographical errors. ProSoft Technology makes no warranty or representation as to its accuracy and assumes no liability for and reserves the right to correct such inaccuracies or errors at any time without notice. If you have any suggestions for improvements or amendments or have found errors in this publication, please notify us.

No part of this document may be reproduced in any form or by any means, electronic or mechanical, including photocopying, without express written permission of ProSoft Technology. All pertinent state, regional, and local safety regulations must be observed when installing and using this product. For reasons of safety and to help ensure compliance with documented system data, only the manufacturer should perform repairs to components. When devices are used for applications with technical safety requirements, the relevant instructions must be followed. Failure to use ProSoft Technology software or approved software with our hardware products may result in injury, harm, or improper operating results. Failure to observe this information can result in injury or equipment damage.

For professional users in the European Union
If you wish to discard electrical and electronic equipment (EEE), please contact your dealer or supplier for further information.

Prop 65 Warning – Cancer and Reproductive Harm – www.P65Warnings.ca.gov

Agency Approvals and Certifications

Please visit our website: www.prosoft-technology.com

Open-Source Information

Open-Source Software used in the product

The product contains, among other things, Open-Source Software files, as defined below, developed by third parties and licensed under an Open-Source Software license. These Open-Source Software files are protected by copyright. Your right to use the Open-Source Software is governed by the relevant applicable Open-Source Software license conditions. Your compliance with those license conditions will entitle you to use the Open-Source Software as foreseen in the relevant license. In the event of conflicts between other ProSoft Technology, Inc. license conditions applicable to the product and the Open-Source Software license conditions, the Open-Source Software conditions shall prevail. The Open-Source Software is provided royalty-free (i.e. no fees are charged for exercising the licensed rights). Open-Source Software contained in this product and the respective Open-Source Software licenses are stated in the module webpage, in the link Open-Source.
If Open-Source Software contained in this product is licensed under GNU General Public License (GPL), GNU Lesser General Public License (LGPL), Mozilla Public License (MPL) or any other Open-Source Software license, which requires that source code is to be made available and such source code is not already delivered together with the product, you can order the corresponding source code of the Open-Source Software from ProSoft Technology, Inc. - against payment of the shipping and handling charges - for a period of at least 3 years since purchase of the product. Please send your specific request, within 3 years of the purchase date of this product, together with the name and serial number of the product found on the product label to:

ProSoft Technology, Inc.
Director of Engineering
9201 Camino Media, Suite 200
Bakersfield, CA 93311
USA

Warranty regarding further use of the Open-Source Software

ProSoft Technology, Inc. provides no warranty for the Open-Source Software contained in this product, if such Open-Source Software is used in any manner other than intended by ProSoft Technology, Inc. The licenses listed define the warranty, if any, from the authors or licensors of the Open-Source Software. ProSoft Technology, Inc. specifically disclaims any warranty for defects caused by altering any Open-Source Software or the product's configuration. Any warranty claims against ProSoft Technology, Inc. if the Open-Source Software contained in this product infringes the intellectual property rights of a third party are excluded. The following disclaimer applies to the GPL and LGPL components in relation to the rights holders:
"This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License and the GNU Lesser General Public License for more details."
For the remaining Open-Source components, the liability exclusions of the rights holders in the respective license texts apply. Technical support, if any, will only be provided for unmodified software.

Table of Contents

1 Start Here

1.1 About ELX3

The ELX3 Industrial Edge Gateway is designed to bring edge computing capabilities to your local automation infrastructure while providing secure remote connectivity through the Belden Horizon Console to meet your most demanding Industrial Internet of Things (IIoT) applications. The ELX3 enables highly secure and reliable device-to-device and device-to-cloud communications. The gateway includes multiple Ethernet ports, allowing for local connectivity to devices like PAC/PLCs, RTUs, DCS systems, smart instruments, electronic billboards, and communication towers.
The ELX3 can be configured and managed through the webpage or via the Belden Horizon Console. The Belden Horizon Console is a secure and intuitive cloud native platform that supports multiple applications like on-demand (secure remote access) or always-on (persistent data network) connectivity, data monitoring and alert notification.

The ELX3 supports deployment of edge applications via Docker containers, which can be installed either locally through the device interface or remotely through the Belden Horizon Console.

ProSoft Industrial Protocol containers (such as the ELX-EIP-MBTCP Container) are first installed via Belden Horizon only (i.e. Belden Featured Applications). Once the container image is deployed to the ELX3 then the user can create more containers via Belden Horizon or Local UI. Other third-party containers can be installed via Belden Horizon or Local UI.

1.2 Information sheet

The ELX3 Quick Start Guide is provides basic installation and configuration information. It is included in the ELX3 packaging.

1.3 Installation Guide

The ELX3 Installation Guide provides detailed power, wiring, cables, and diagnostics information. It can be downloaded from www.prosoft-technology.com.

2 Initial Configuration

This chapter covers the initial configuration of the ELX3 via the webpage. The initial configuration includes setting up the LAN port. These steps are required, even if the ELX3 is going to be registered via Belden Horizon Console for cloud connectivity.

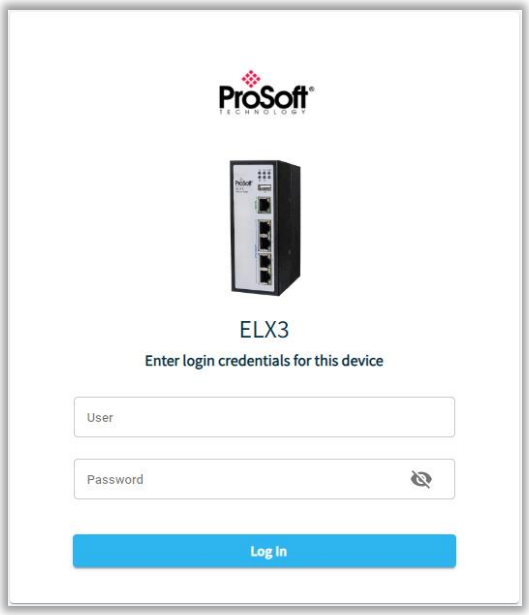
Once the ELX3 is registered on Belden Horizon Console, the ELX3 can be maintained via Belden Horizon Console (See *Chapter 3 Registration in Belden Horizon Console* for more details).

2.1 Connecting to the ELX3 Webpage

Perform the following steps to connect to the ELX3 webpage:

1. Ensure the ELX3 is connected to the network using Ethernet port 1, then apply power to the ELX3.
2. Open a web browser and log in to the ELX3 configuration webpage using the default IP address: **https://192.168.0.250**. If the PC is on a different subnet, temporarily set the IP address of the PC to **192.168.0.xxx** with a subnet of **255.255.255.0**.

   The login page is displayed.

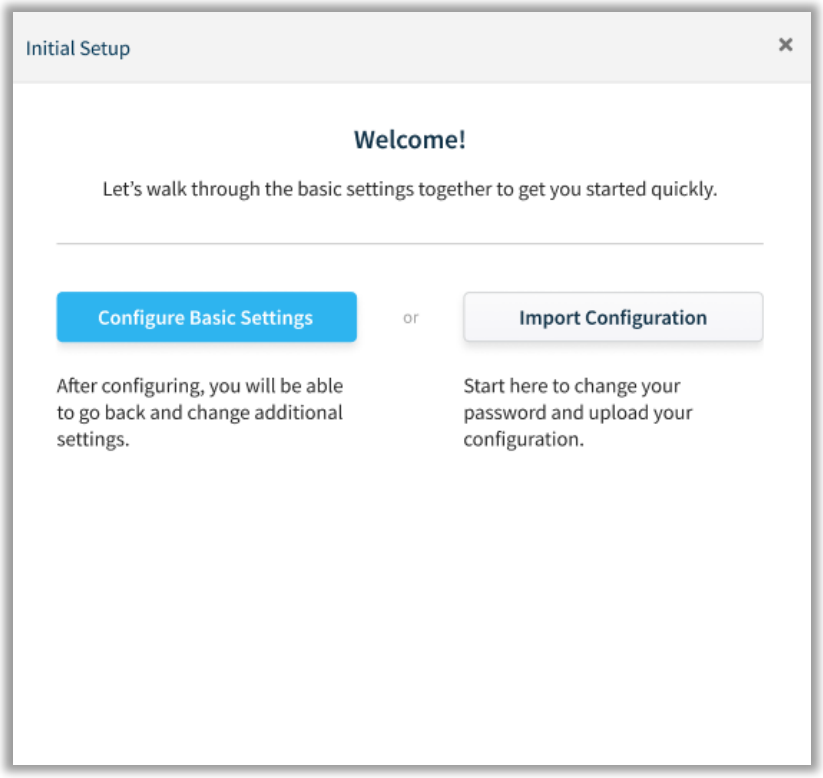


3. Enter the login credentials. The default *username* and *password* are **admin** and **password**.

Note: The user will be prompted to change the password after the first login. Provide a new password and apply the changes. After successful login with the new password, future password changes are made in the *System* tab of the webpage.

4 The *Initial Setup* dialog allows the following operations:

- Configure Basic Settings (assigning module name and LAN IP address) or Import Configuration
- Change Default Login Credentials



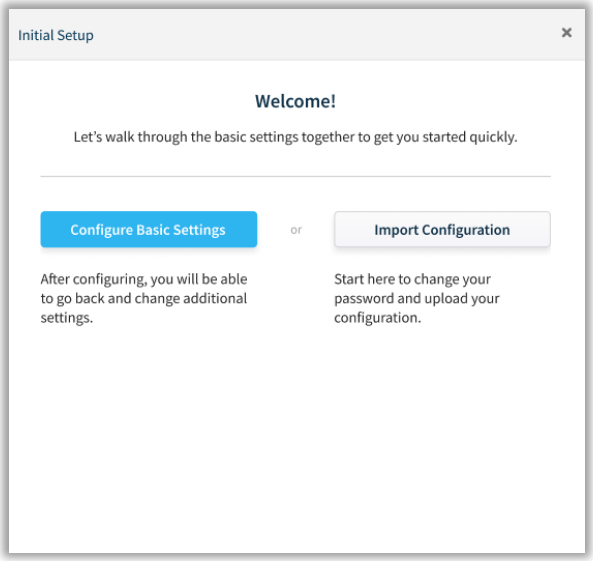
2.1.1 Configuration

Perform a basic configuration or upload an existing configuration.

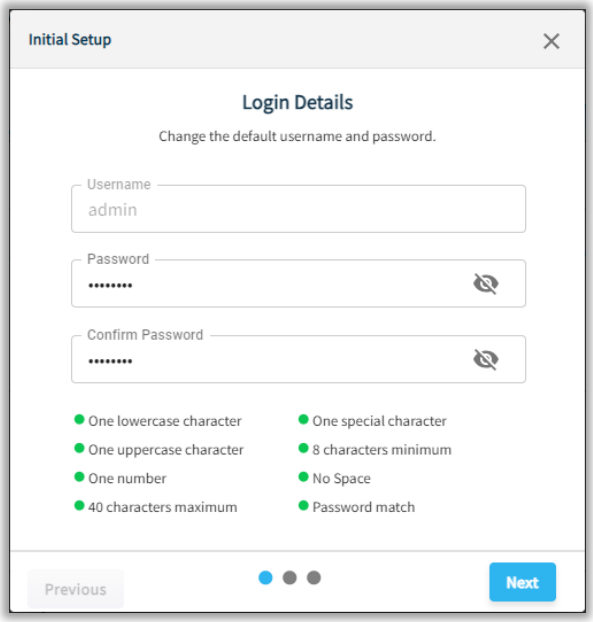
2.1.1.1 Configure Basic Settings

To perform basic configuration settings:

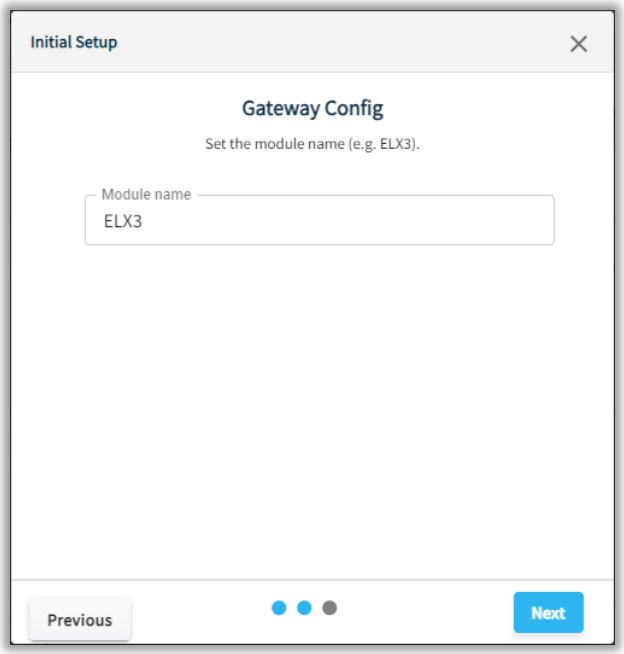
1 In the *Initial Setup* dialog, click **CONFIGURE BASIC SETTINGS**.



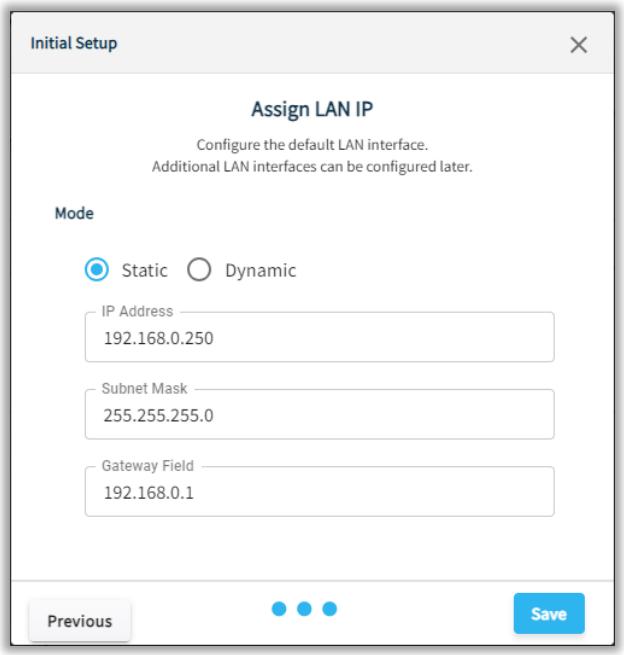
2 In the *Login Details* dialog, change the default login credentials and click **NEXT.**



3 In the *Gateway Config* dialog, the *Module Name* can be edited. Click **NEXT.**



4 In the *Assign LAN IP* dialog, select a mode (*Static* or *Dynamic*). Enter the ELX3's *IP Address, Subnet Mask* and *Gateway*.



5 Click **SAVE** to save the configuration changes.

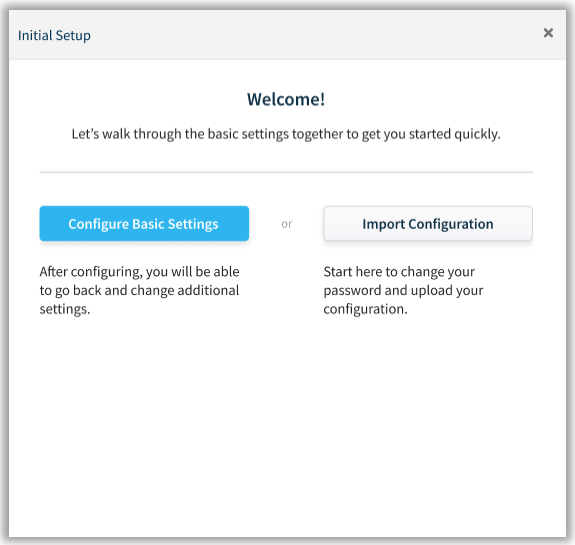
2.1.1.2 Import Configuration

Note: For information on exporting the configuration, please see section *4.1.2 […] Button*.

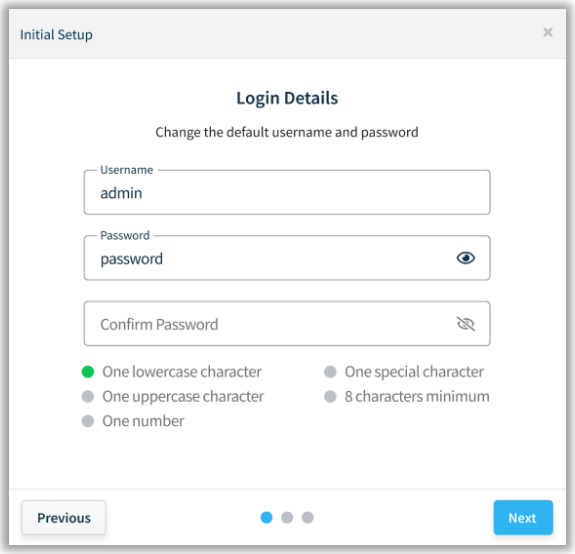
Note: During the initial ELX3 configuration, the default Username and Password must be changed.

To import a configuration file:

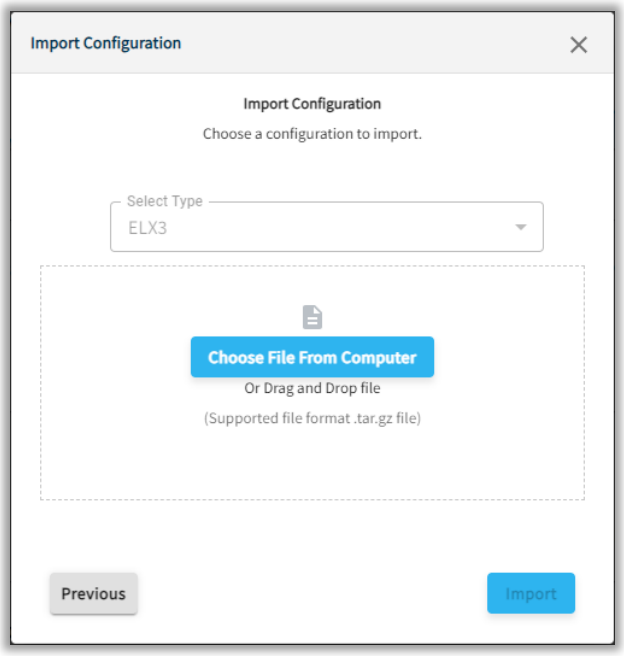
1 In the *Initial Setup* dialog, click **IMPORT CONFIGURATION**.



2 In the *Login Details* dialog, change the default login credentials and click **NEXT**.



3 In the *Import Configuration* dialog, drag and drop a *.tar.gz* configuration file in the dialog or click **CHOOSE FILE FROM COMPUTER** to browse and upload a file.

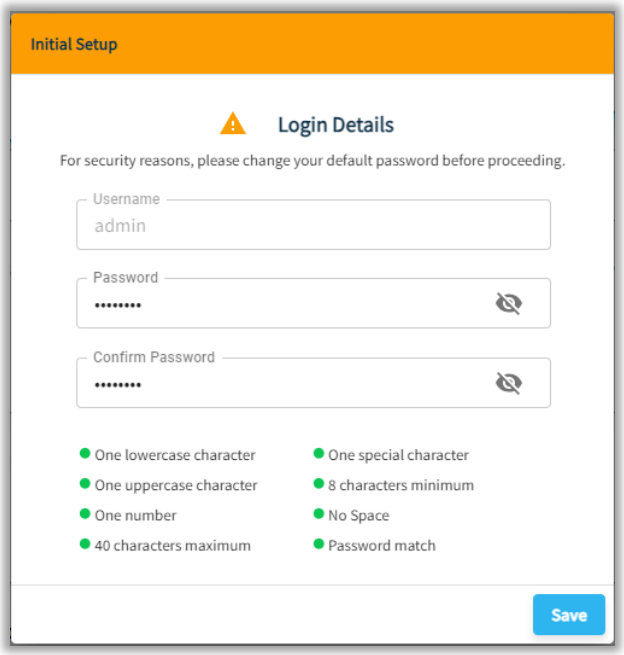


4 Click **IMPORT** to import the selected configuration file.

2.1.2 Change Default Login Credentials

To change the default login credentials for the ELX3 webpage:

1 Close the *Initial Setup* dialog to display the *Login Details* dialog as shown below:



2 Enter the new login credentials.

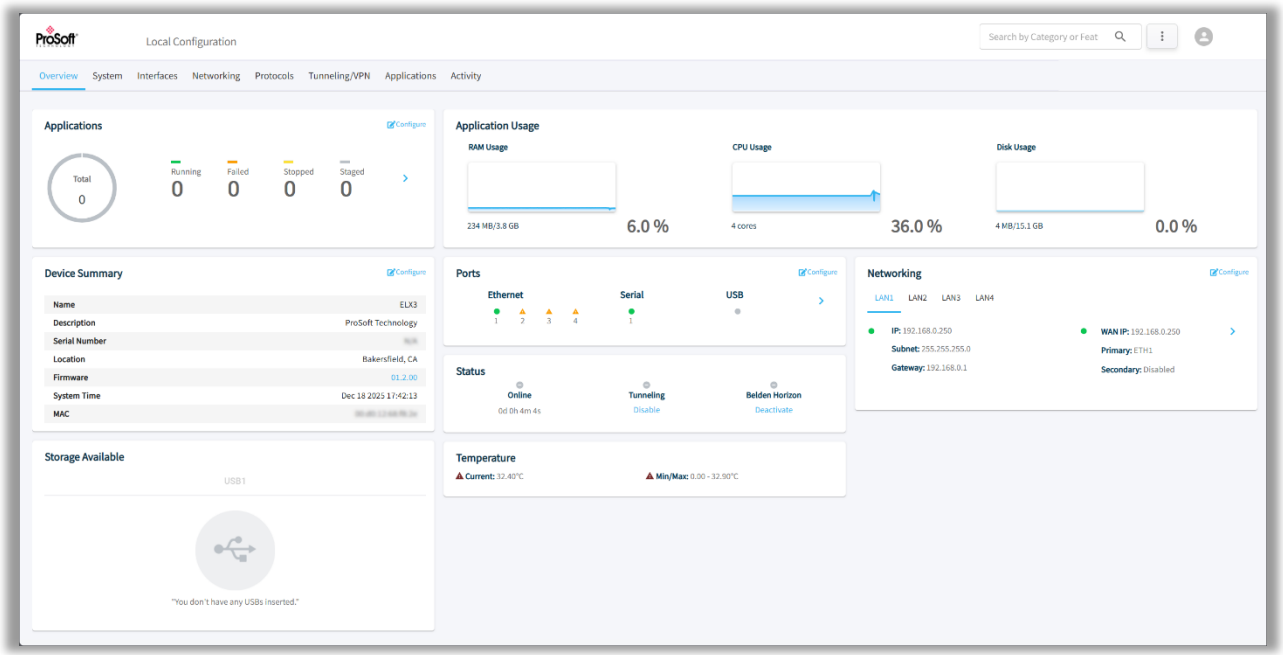
> **Note:** The password must be a minimum of 8 characters, including at least one lowercase character, one uppercase character, one special character, and one number.

3 Click **SAVE** to save the changes.

2.1.4 Successful Login

After a successful login, the *Overview* tab is displayed and contains the following information:

- Status (such as *Online*, *Tunneling*, or *Belden Horizon Console*)
- Device Summary (such as *Gateway Name, Description, Serial Number, Location, Firmware, System Time and MAC*)
- Ports (4 Ethernet ports)
- Networking (such as *Status* for LAN and WAN)
- Device temperature
- Available storage
- Other features



Note: The stats of each parameter will vary.

Note: The user is automatically logged out after 15 minutes of inactivity.

3 Registration in Belden Horizon Console

Belden Horizon Console is a secure and intuitive cloud-native platform. The ELX3 can be managed in Belden Horizon Console once registered. Before using the ELX3 it must be registered in Belden Horizon Console by entering an Activation Key.

3.1 Registration Using Activation Key

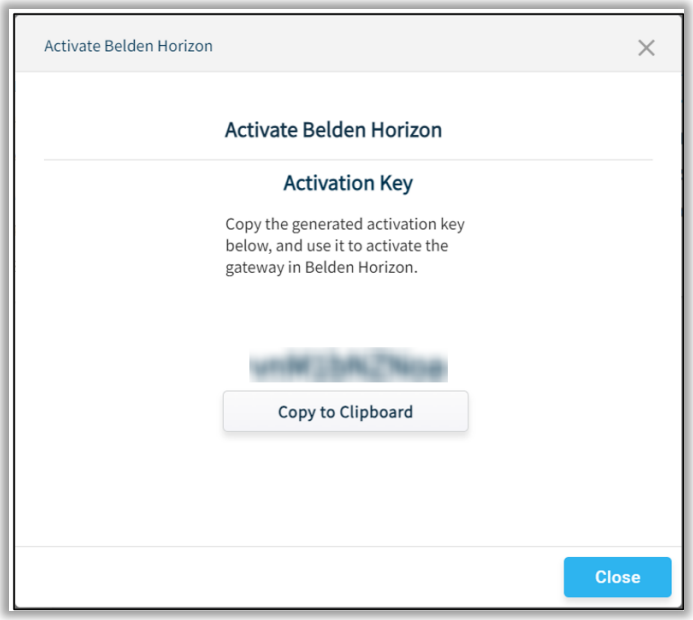
Use the following procedure to obtain the activation key from the ELX3, and to register the ELX3 with Belden Horizon Console:

Note: The ELX3 must be connected to the Internet through the WAN port. See section *4.5.1 WAN* for more details.

1. Access the local user interface of the ELX3.
2. In the *Overview* tab > *Status* tile, click the **ACTIVATE** link under the *Belden Horizon Console* label.

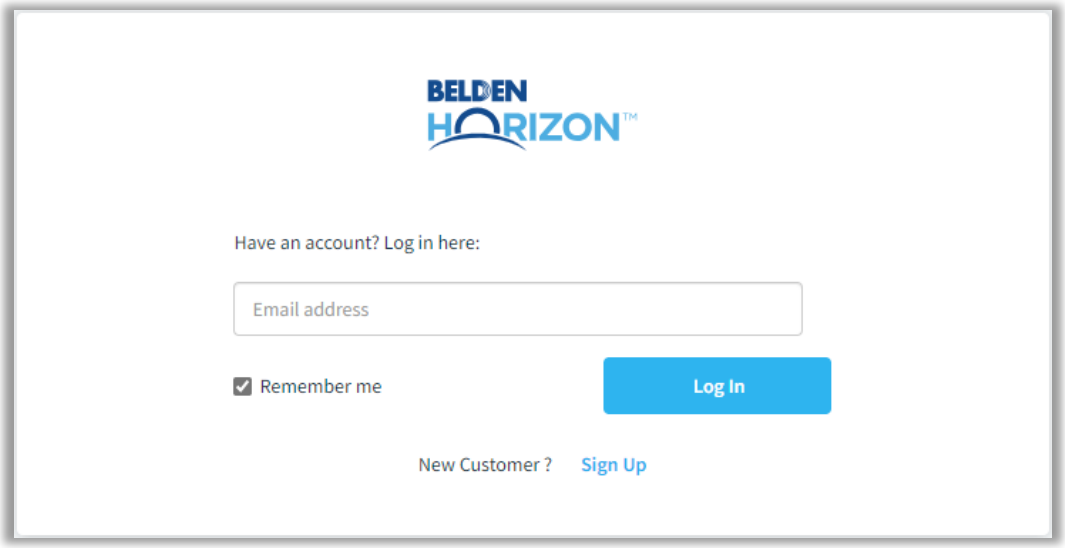
Note: If the ELX3 is already connected to a Belden Horizon Console account, the link states "**Deactivate**".

3 The ELX3 securely retrieves an alphanumeric activation key from Belden Horizon Console that is valid for three hours. Record this activation key.



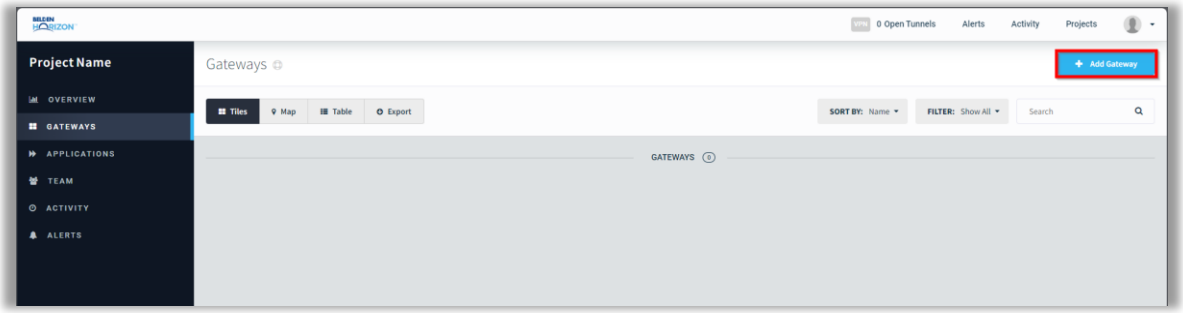
4 Open a new tab in a web browser, enter **www.belden.io** in the address bar, and then press **ENTER**.

5 On the *Belden Horizon Console Login* screen, enter the Belden Horizon Console login email and click **LOG IN**, or click **SIGN UP** to create a new account. Login credentials are not interchangeable between Belden Horizon Console and the webpage.

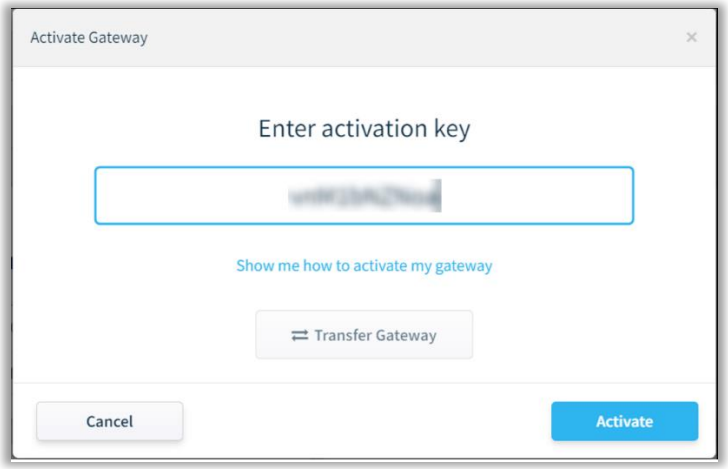


6 Once logged in, follow the prompts to create a project.

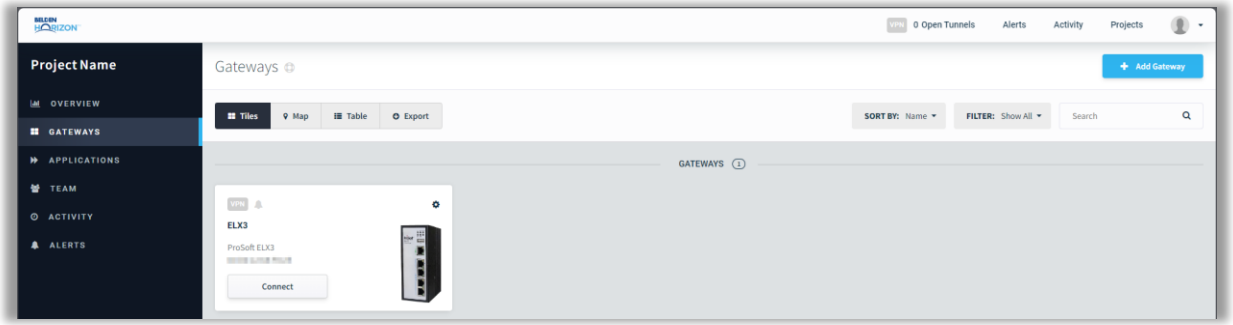
7 Click the *Gateways* tab, and then click **ADD GATEWAY**.



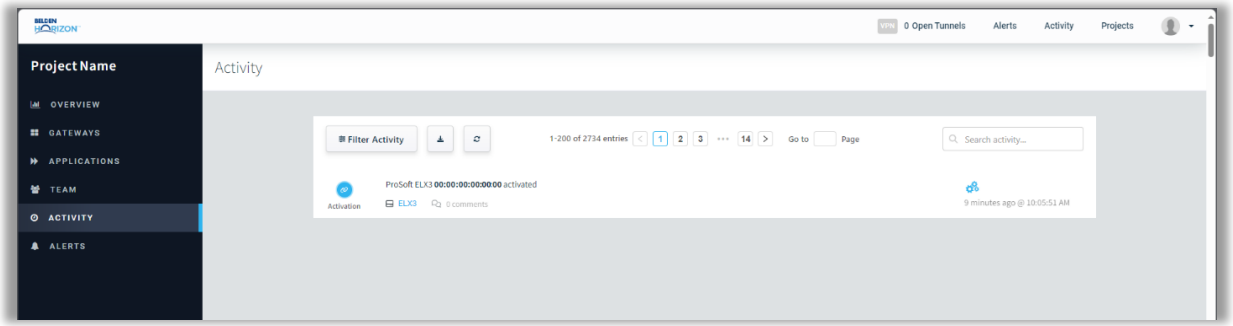
8 In the *Activate Gateway* dialog, enter the activation key that was recorded earlier. Click **ACTIVATE**.



9 Upon successful activation, the ELX3 appears on the *Gateways* tab.



The ELX3 will also be updated in the *Activity* logs. Click the **ACTIVITY** option at the top of the Belden Horizon Console window.



3.2 Activation Errors

The following error messages correspond to failed registration issues:

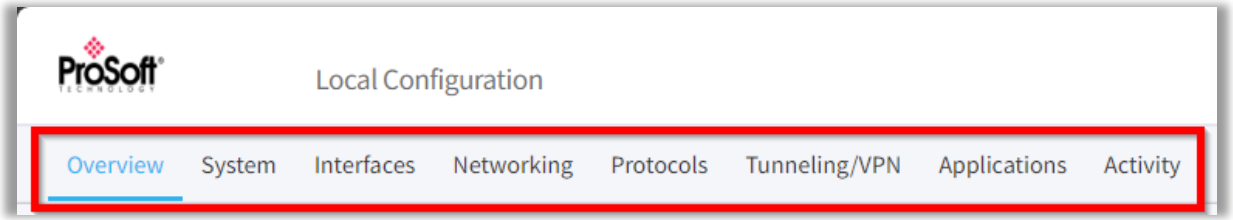
Error	Description	Solution
Key is corrupted.	The key is invalid.	Please make sure this is the correct key.
Device Activation record was found for activation key.	Failed to find an activation record in the Belden Horizon Console database.	Please try another activation key.
Found a Device Activation record in ACTIVATED state for device.	The device is already activated.	Please try another activation key.
Activation key has expired.	This activation key has expired, and a new one has been generated.	Please check device for the latest activation key.

4 ELX3 Local User Interface

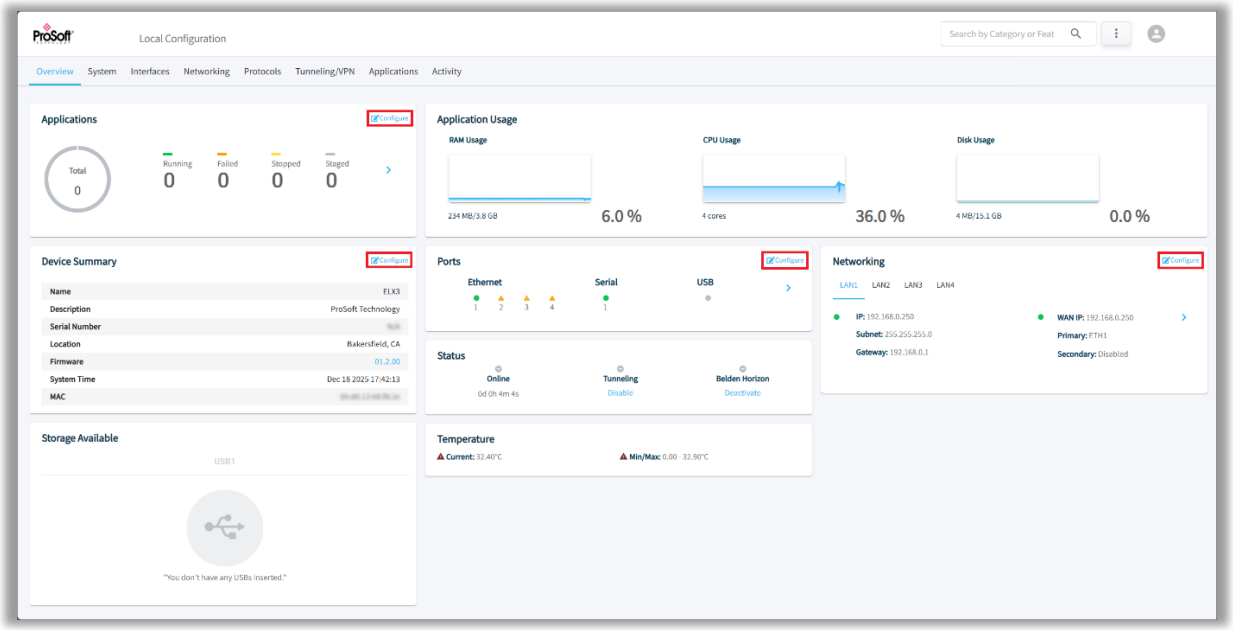
4.1 ELX3 Webpage Navigation

The ELX3 webpage is used for configuration and diagnostics. There are different ways to access the configuration parameters of the ELX3 webpage:

- From the tabs on the *Local Configuration* webpage.

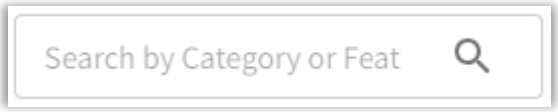


- From the **CONFIGURE** link in each tile of the *Overview* tab.



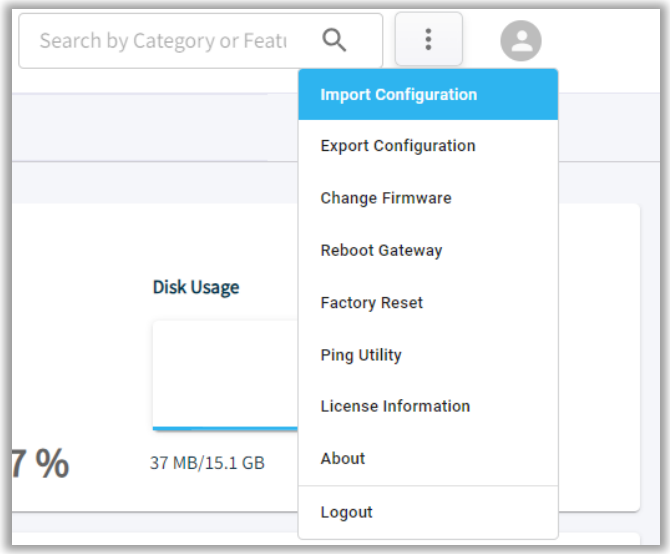
4.1.1 Search Bar

The search bar is used to navigate to a specific configuration by entering a keyword in the search box.



4.1.2 […] Button

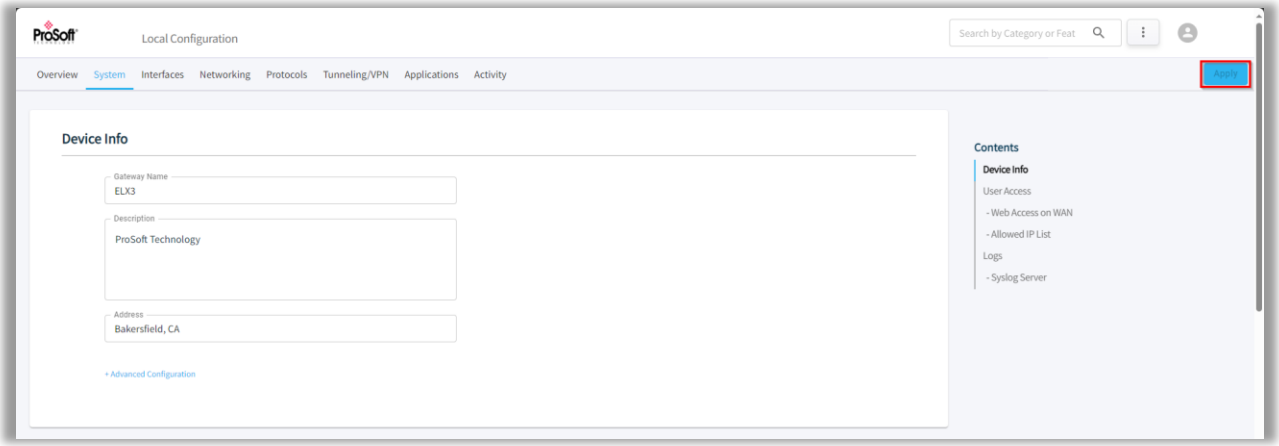
The ⋮ button contains additional options for the ELX3.



Parameter	Description
Import Configuration	Imports the gateway configuration.
Export Configuration	Exports the gateway configuration.
Change Firmware	Updates the gateway firmware.
Reboot Gateway	Reboots the gateway.
Factory Reset	Resets the ELX3 settings to default configuration.
Ping Utility	Tests for internet and general network connectivity between the ELX3 and external, local devices.
License Information	Information about the present licenses.
About	Information about device and firmware.
Logout	Logs out the current user.

4.1.3 Apply Button

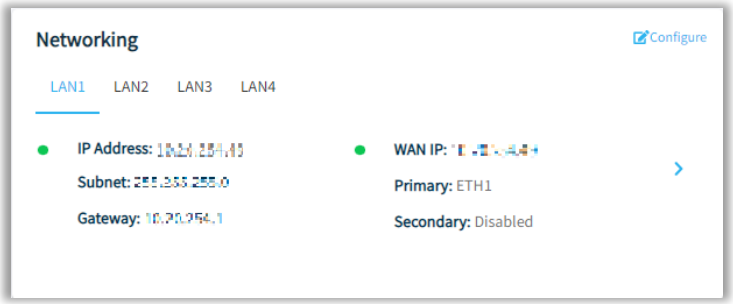
The **APPLY** button is used to send the current configuration to the ELX3. When configuration edits are made on the webpage, this button becomes active.

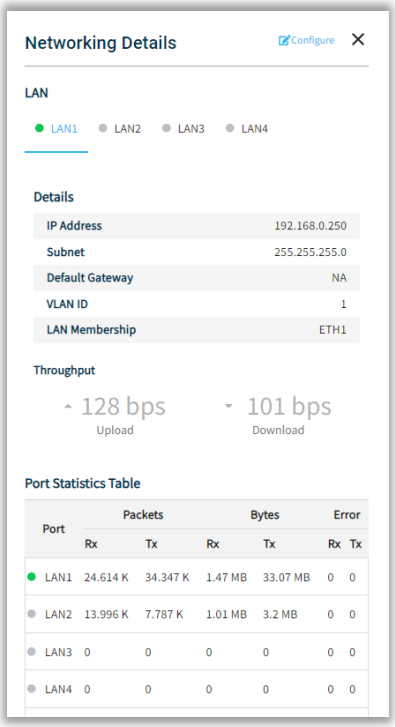


4.1.4 Side sheet Launcher

Within the configuration tiles in the *Overview* tab, the › icon expands the menu to display additional details.

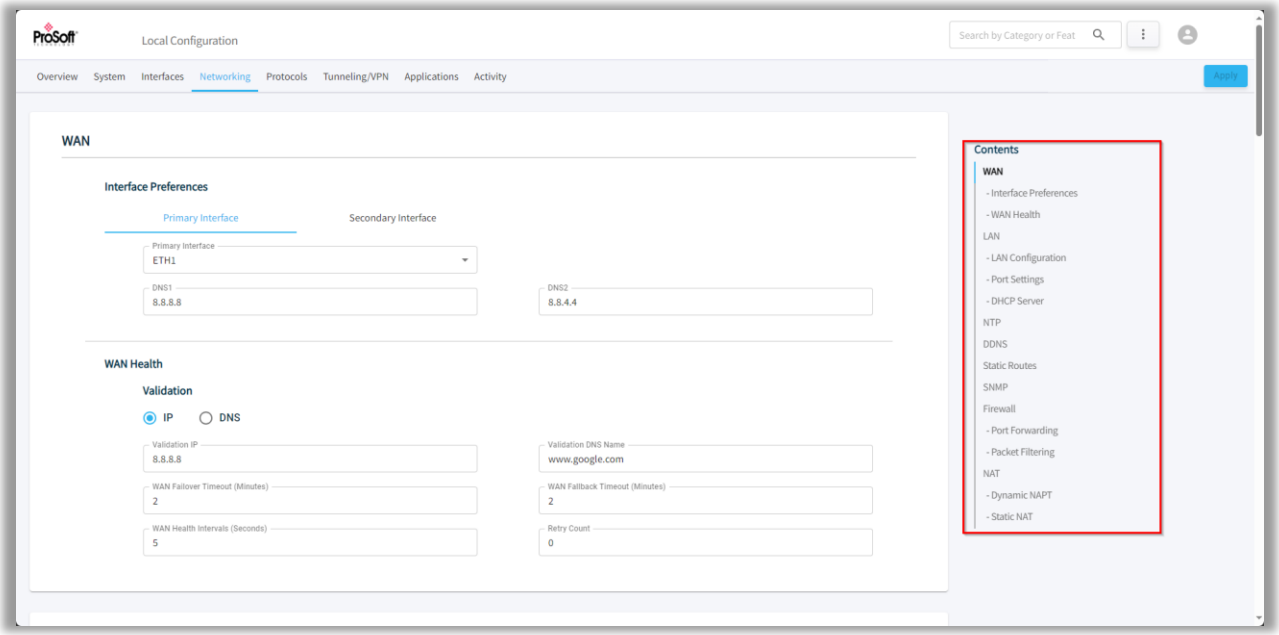
Example:





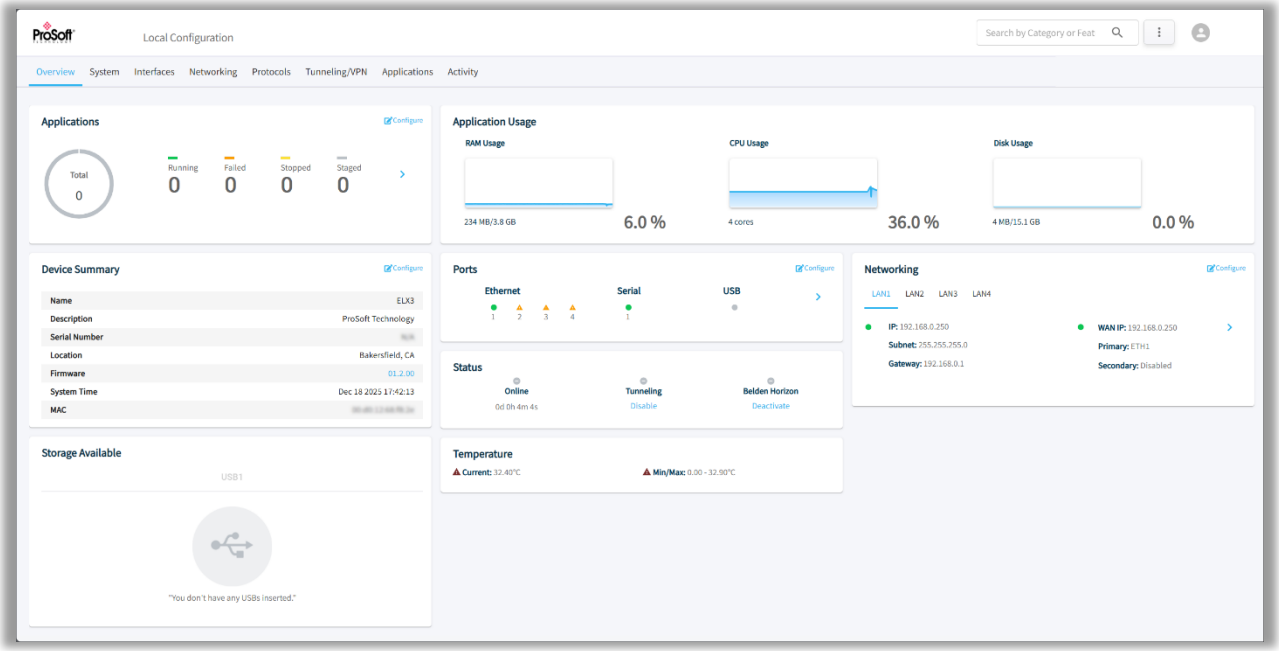
4.1.5 Side Menu Scrolling

The scrolling menu on the side of the page can be used to quickly jump to each parameter.



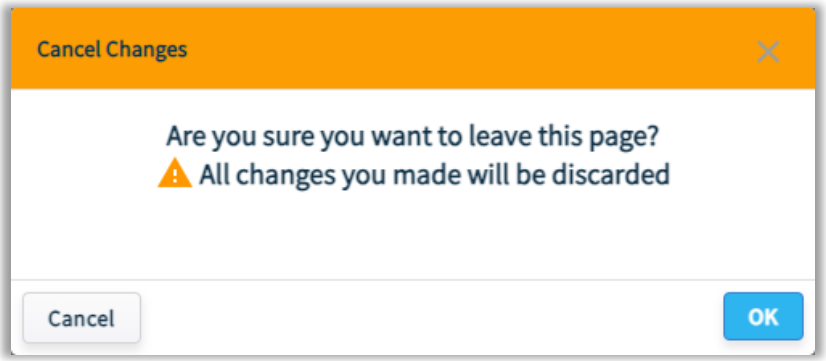
4.2 Overview Tab

The *Overview* tab contains details of the device status, storage, networking interface, and ports.



Additionally, click **CONFIGURE** on a specific tile to open its configuration option.

Note: Click **APPLY** on each configuration page to apply the changes. Otherwise, the system will display a pop-up message. Click **OK** to discard the changes or **CANCEL** to close the pop-up message.



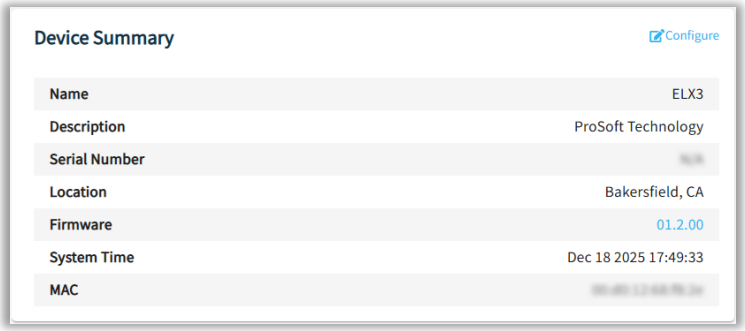
4.2.1 Status

The *Status* tile displays the following device status parameters:

Parameter	Description
Online	The status of the ELX3: **Online** (Green) **Offline** (Grey) **Note:** The status will be Online only if WAN is connected and communicating with the internet.
Tunneling	The icon displays the current Belden Horizon Console tunneling status of the ELX3. Grey: Tunneling is not in operation Green: Tunneling is in operation Click **ENABLE** to enable tunneling, or **DISABLE** to disable tunneling
Belden Horizon	The current ELX3 status in Belden Horizon Console. **Activate** (Grey), **View activation key/Deactivate** (Green), or **Deactivate** (Green) **Note:** View activation key status is displayed only if the activation key is generated but not activated in Belden Horizon Console.

4.2.2 Device Summary

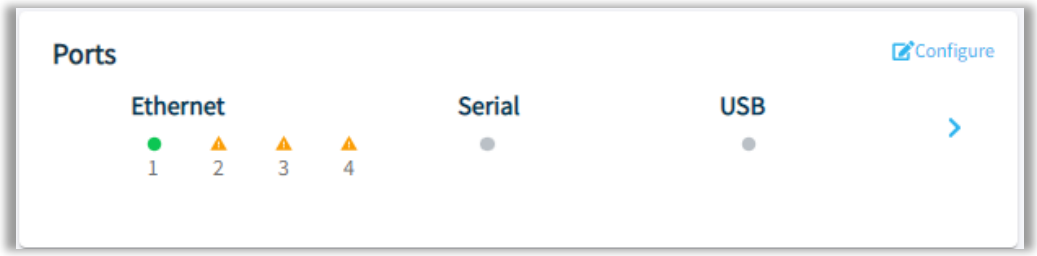
The *Device Summary* tile displays the following device information:



Parameter	Description
Name	Gateway name configured by user.
Description	Gateway description configured by user.
Serial Number	Serial number of the ELX3.
Location	Location of gateway configured by user.
Firmware	Current firmware version that is loaded on the ELX3.
System Time	Date and time in UTC format.
MAC	ELX3 MAC Address.

4.2.3 Ports

The *Ports* tile displays the indicators of the ELX3 Ethernet ports.

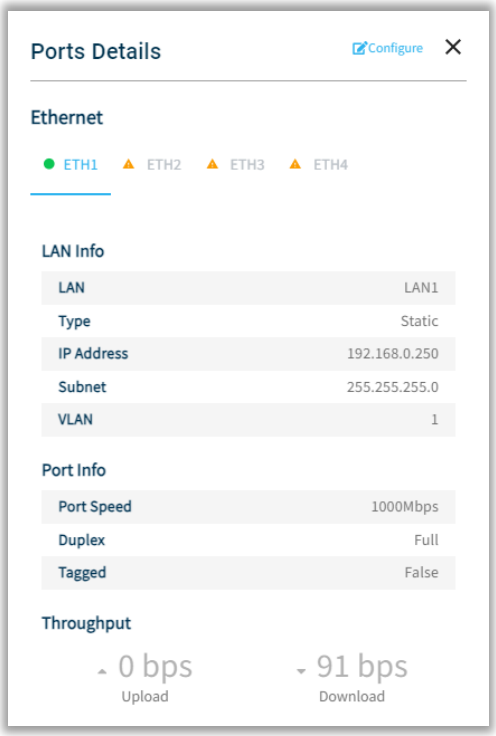


Note: The **USB** port is reserved for future use.

Port Indicator	Description
Green	The port is configured and communicating.
Grey	The port is not configured, and no cable detected.
Yellow	The port is configured but not communicating, or no cable has been detected.

Click the › icon to display the *Ports Details* dialog.

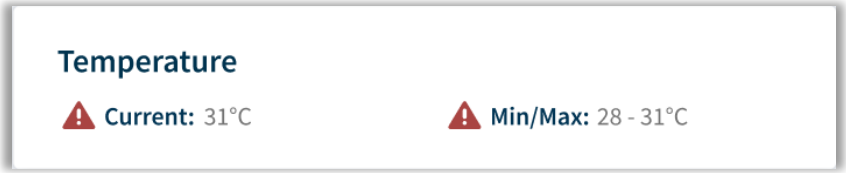
4.2.3.1 Ports Details



Parameter		Description
Ethernet	ETH1 ETH2 ETH3 ETH4	Green: Port is configured and communicating. Grey: Port is not configured. Yellow Triangle: Port is configured but no communications, or no cable detected.
LAN Info	LAN	LAN configuration assigned to the port.
	Type	Type of mode, dynamic or static.
	IP Address	IP address assigned to the port.
	Subnet	Subnet mask of the IP address.
	VLAN	VLAN ID.
Port Info	Port Speed	Data transfer speed for the port.
	Duplex	Transmission mode for the port, such as half duplex or full duplex.
	Tagged	VLAN tagging.
Throughput	Upload	Upload speed (Mbps) of data on the Ethernet port.
	Download	Download speed (Mbps) of data on the Ethernet port.

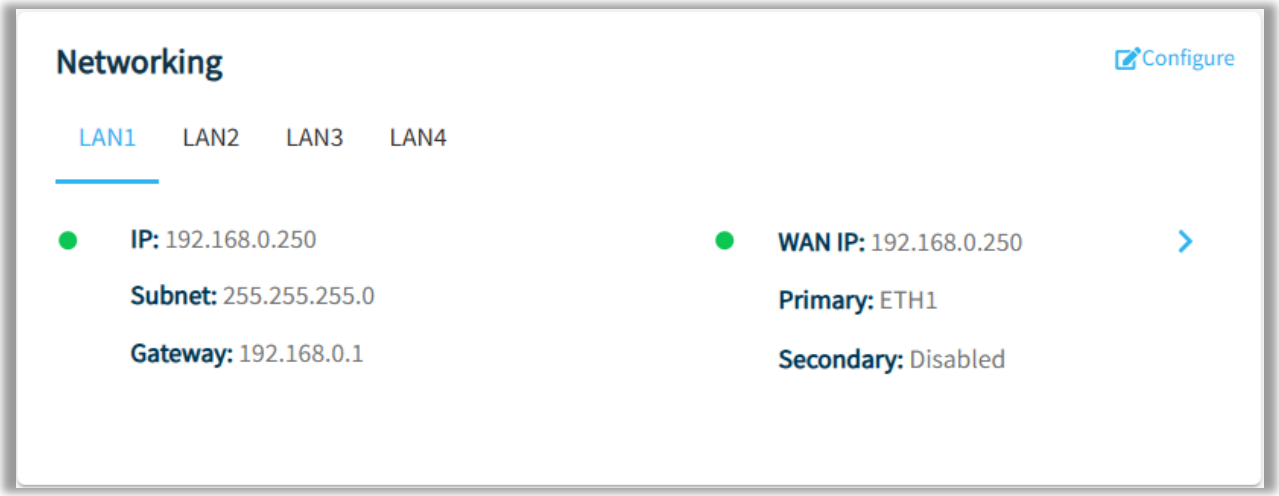
4.2.4 Temperature

The *Temperature* tile displays the current and minimum/maximum operating temperatures of the ELX3.



4.2.5 Networking

The *Networking* tile displays the LAN and WAN configurations of the ELX3.

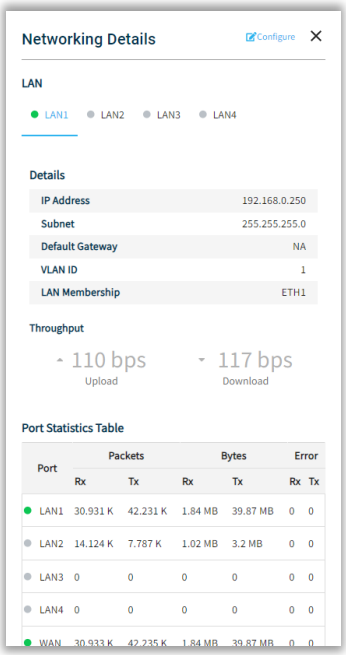


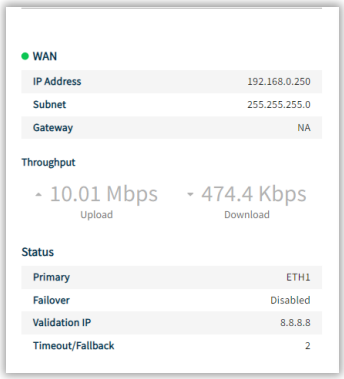
Parameter	Description
IP	IP address provided by the operator.
Subnet	Subnet mask of the IP address.
Gateway	Default IP address of the gateway.
WAN IP	IP address assigned to the WAN.
Primary/Secondary	Primary and Secondary WAN interface.

Click the › icon to display the *Networking Details* dialog.

4.2.5.1 Network Details

The *Networking Details* dialog provides the following additional information:





Click the **LAN1** to **LAN4** tabs to view the details for each LAN.

Parameter		Description
LAN	**Details**	View the following details for LAN configuration.
	IP Address	IP address assigned to the LAN.
	Subnet	Subnet mask of the IP address.
	Default Gateway	Default IP address of the gateway.
	VLAN ID	Displays the VLAN ID assigned to the port.
	LAN Membership	Defines LAN membership of Ethernet ports.
	Throughput	
	Upload	Upload speed (Mbps) of data on the LAN network.
	Download	Download speed (Mbps) of data on the LAN network.

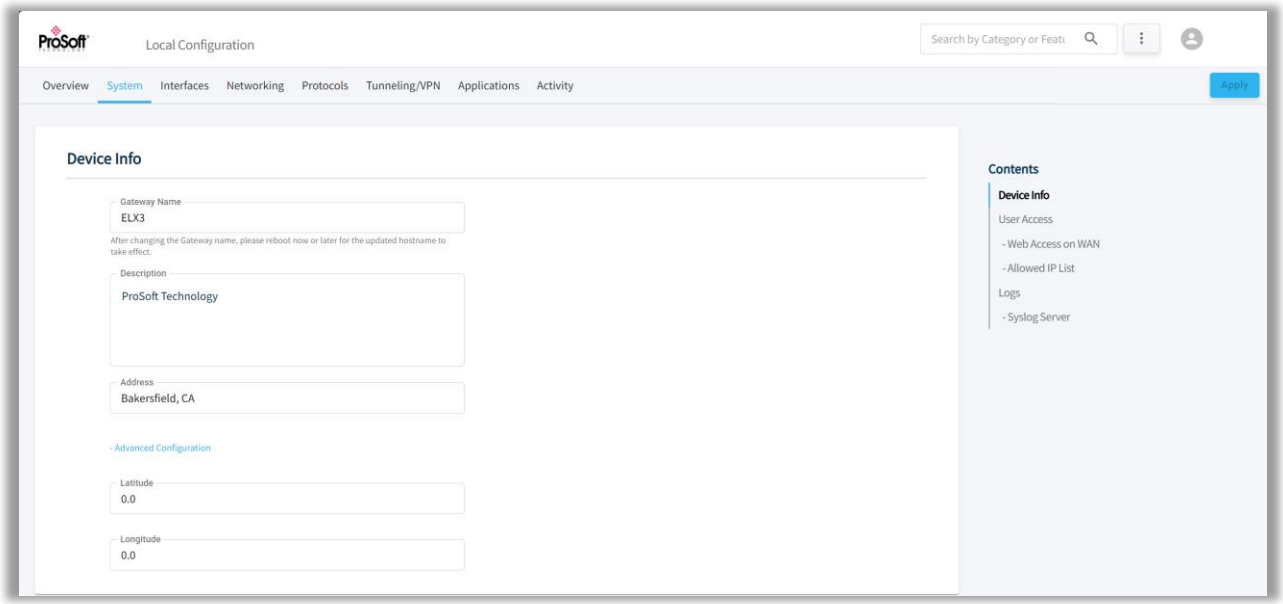
Parameter		Description
WAN	IP Address	IP address assigned to the WAN.
	Subnet	Subnet mask of the IP address.
	Gateway	IP address of the gateway.
	Throughput	
	Upload	Upload speed (Mbps) of data on the WAN network.
	Download	Download speed (Mbps) of data on the WAN network.
	Status	
	Primary	Primary WAN Interface.
	Failover	The failed timeout, in minutes, after which primary network will be switched to secondary, or vice versa.
	Validation IP	The system will ping the IP and confirm if the WAN network is operational.
	Timeout/Failback	WAN failback time in minutes.

4.3 System Tab

The *System* tab contains the *Device Info*, *User Access*, and *Logs* parameters.

4.3.1 Device Info

Device Info allows the user to define the gateway name, description, address, and latitude/longitude coordinates of the ELX3.



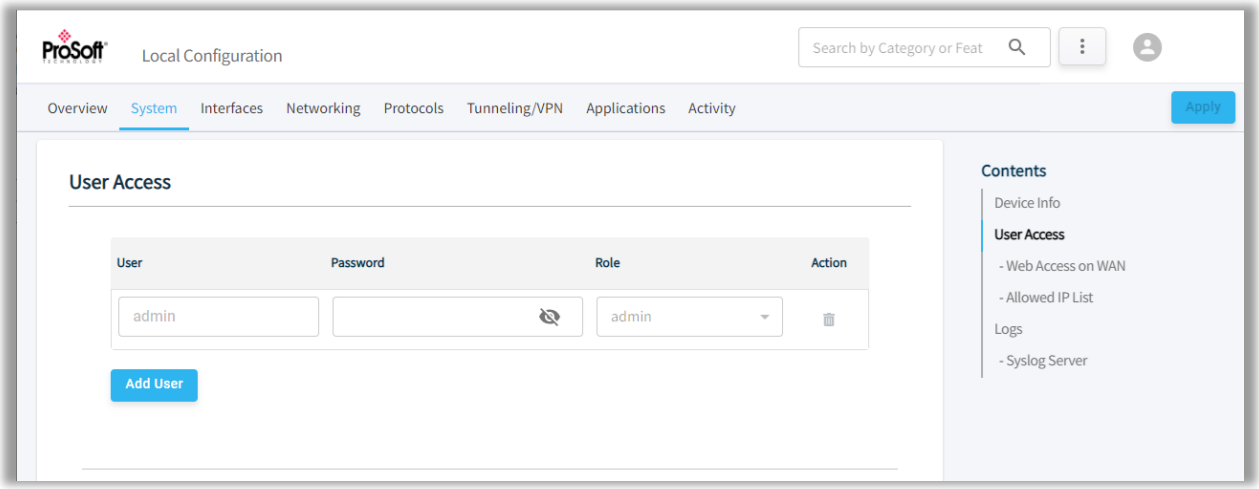
Parameter	Description
Gateway Name	Name of the gateway. **Note:** The ELX3 must be rebooted for this parameter to take effect.
Description	Brief description of the gateway.
Address	Address of the gateway.
Latitude	Latitude coordinates the gateway.
Longitude	Longitude coordinates of the gateway.

4.3.2 User Access

The ELX3 allows the management of user access to the device WAN. Up to 8 users can be created and assigned different roles to limit their access.

The following types of roles can be assigned to a user:

- **Admin**: Includes complete user privileges. An *Admin* can do any desired change. Maximum two admins are allowed. For security reasons, only the **Admin** can edit the configuration. Refer to section *7.2 Defense in Depth* for more information about privileges.
- **Viewer**: Includes permissions to view the configurations and to monitor the gateway and activity feed. A *Viewer* cannot make configuration changes.



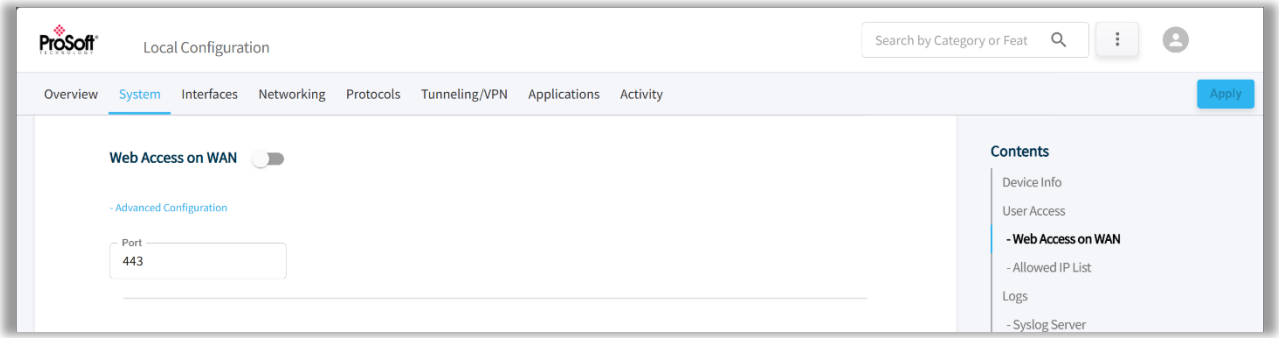
To add a new user:

1. Open the ELX3 configuration webpage and click the *System* tab.
2. Under *User Access*, enter the following parameters:

Parameter	Description
User	Username to be defined. Minimum 5 characters, maximum 30 characters.
Password	Default password for the user account. **Note:** The username and password are used for the first time login by the new user. After the first login, the new user is prompted to change the default password.
Role	Role to be assigned to the new user. **Admin** or **Viewer**

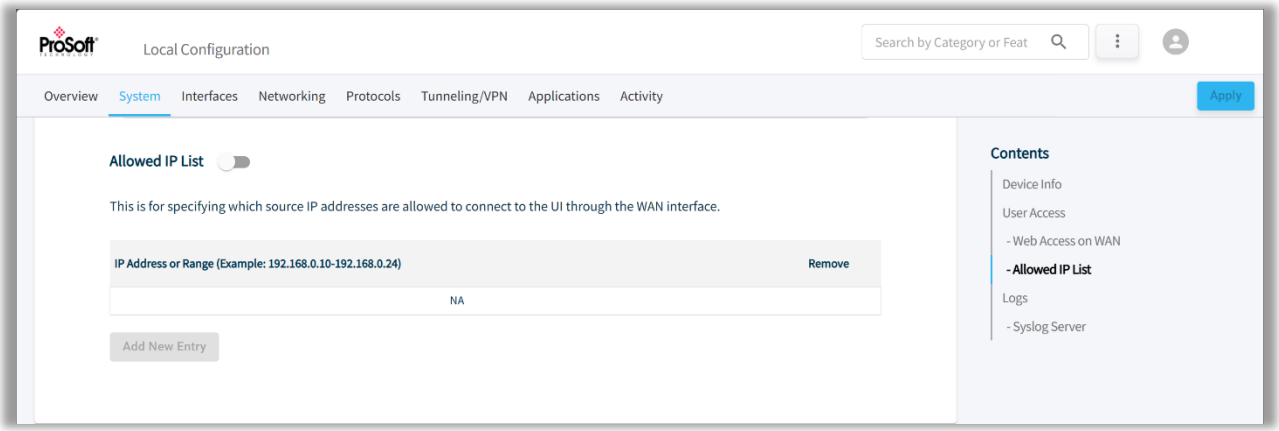
4.3.2.1 Web Access on WAN

This feature allows or blocks webpage access on the WAN.



4.3.2.2 Allowed IP List

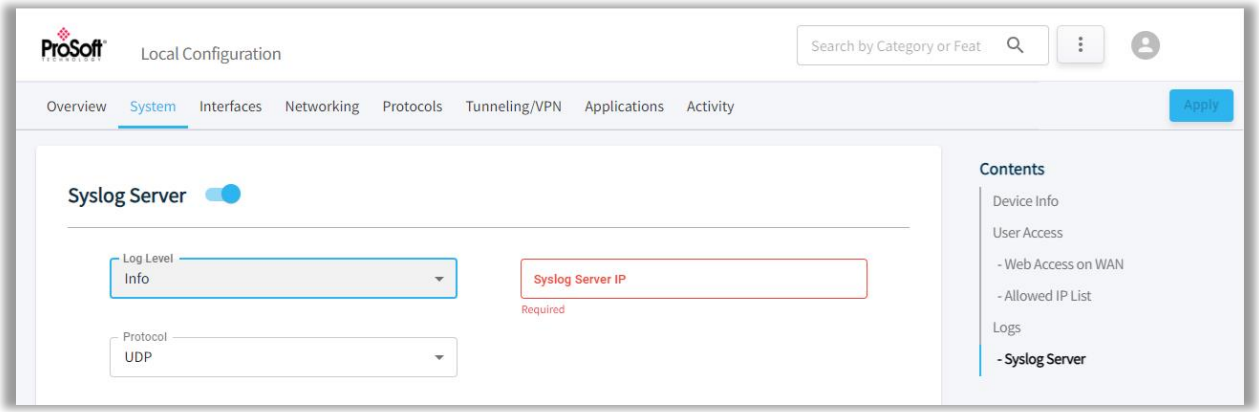
To specify the source IP addresses that are allowed to connect to the webpage through the WAN interface, toggle the **ALLOWED IP LIST** button. Then enter the source IP addresses.



4.3.3 Logs

4.3.3.1 Syslog Server

The Syslog Server allows the user to send all network device log information to one centralized place.



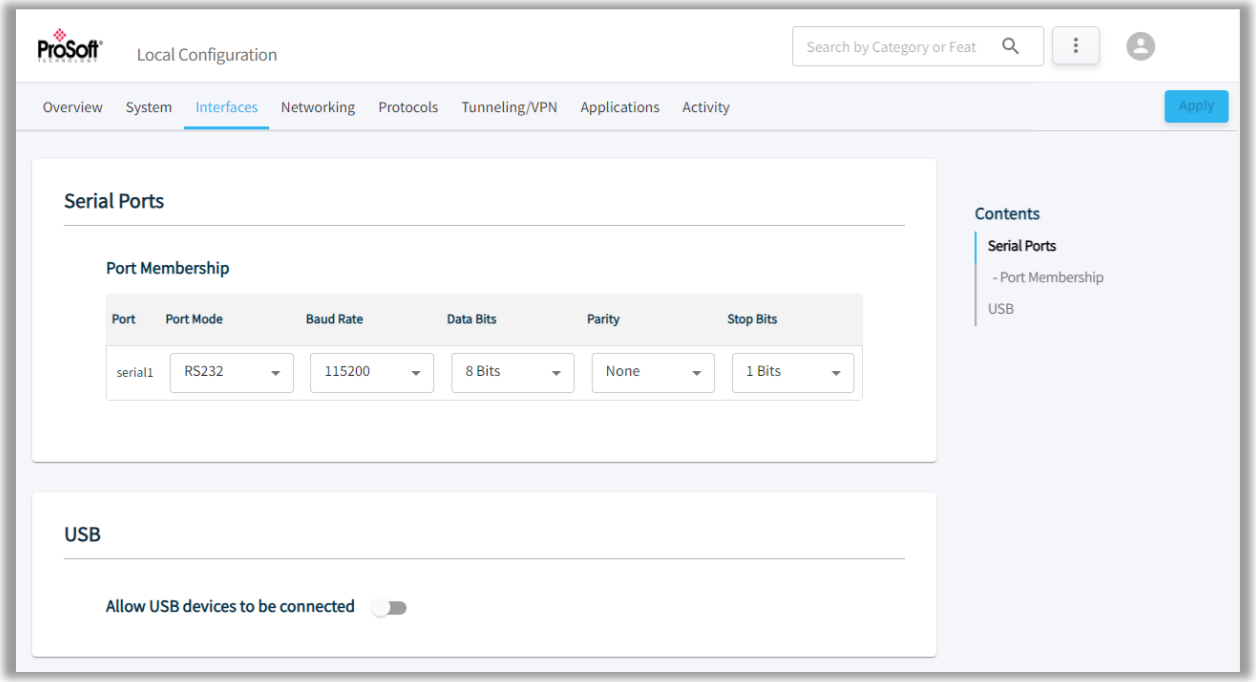
The Syslog Server can be configured by providing the following details:

Parameter	Description
Log Level	Select the log level from the drop-down depending on the severity of the logs.
Protocol	The Protocol to use to send information to the server.
Server IP	The IP address of the server to store the system logs.

4.4 Interfaces Tab

The *Interfaces* tab is used to configure the *Serial* port of the gateway.

Note: The **USB** port is reserved for future use.

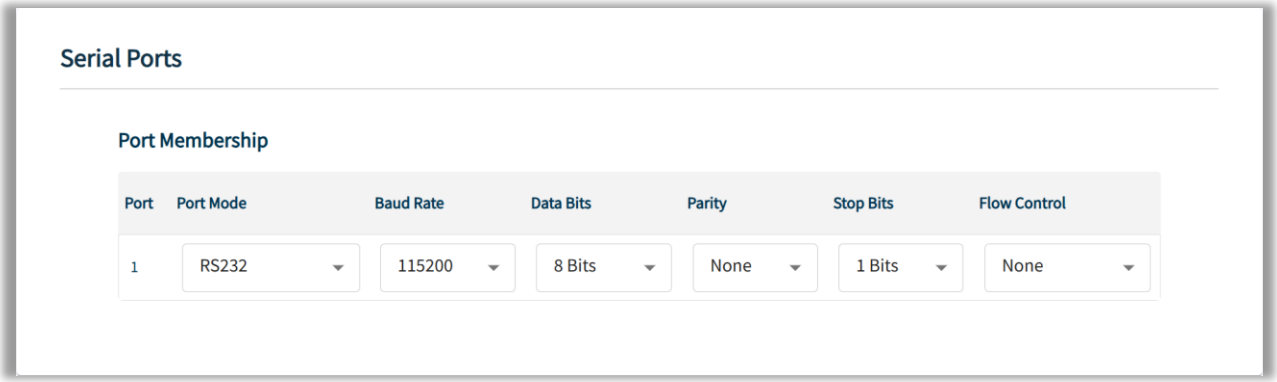


4.4.1 Serial Ports

The ELX3 has one serial port with parameters that include port mode, baud rate, data bits, parity and stop bits.

To configure a serial port:

1. Click on the *Interfaces* tab.
2. Under *Serial Ports* > *Port Membership*, provide the following details:

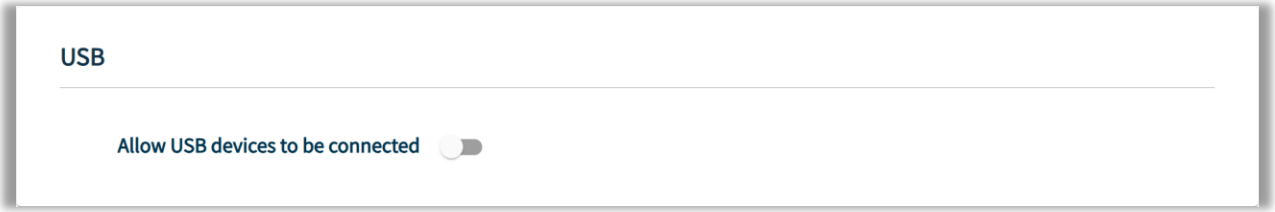


Parameter	Description
Port Mode	ELX3 provides one mode i.e. RS232
Baud Rate	Selects the speed at which data is transmitted between devices or over a communication channel. Measured in bits per second (bps).
Data Bits	Selects the size of the information chunk being sent or received.
Parity	Selects the error checking mechanism in serial data transmission.
Stop Bits	Selects the specific bit that is added to end of each transmitted data.

3. Click **APPLY** to save the changes.

4.4.2 USB

Note: The **USB** port is reserved for future use.

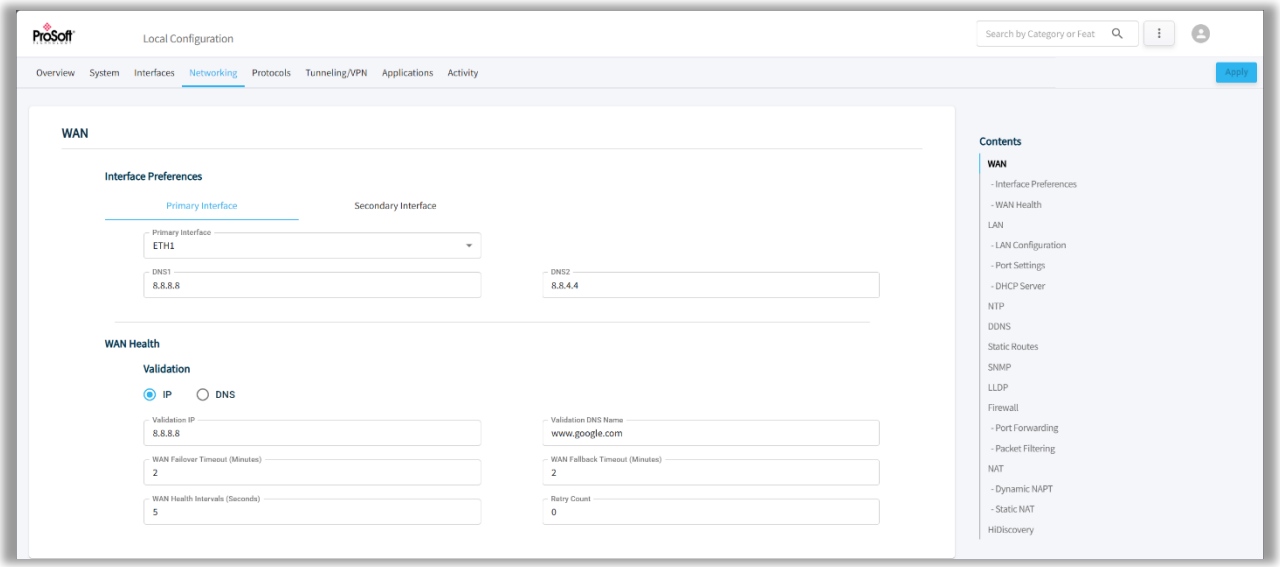


4.5 Networking Tab

The *Networking* tab contains details on the WAN, LAN, NTP, Static Routes, SNMP, Firewall, and NAT features.

4.5.1 WAN

The WAN configuration is used to set up interfaces used for WAN, backup WAN, and conditions to switch WANs.



Note: Internet access is possible via one of the four LAN ports.

4.5.1.1 WAN Interface Preferences

Parameter	Description
Primary or Secondary Interface	ETH1 to ETH4 **Note:** The ETH**x** port must be assigned to a specific LAN configuration. More information is detailed in section *4.5.2 LAN*.
DNS1 and DNS2	DNS IP addresses assigned by the user.

4.5.1.2 WAN Health

Parameter	Description
Validation IP	The system will ping the IP and confirm if the WAN network is operational.
Validation DNS Name	The system will ping the DNS and confirm if the WAN network is operational.
WAN Failover Timeout	The failed timeout, in minutes, after which primary network will be switched to secondary, or vice versa.
WAN Fallback Timeout	If the primary network fails after timeout period, in minutes, the system will re-check the network. If successful, it will switch back.
WAN Health Intervals	The time, in seconds, for which the system will test the WAN network.
Retry Count	The retry count to confirm that the network is operational.

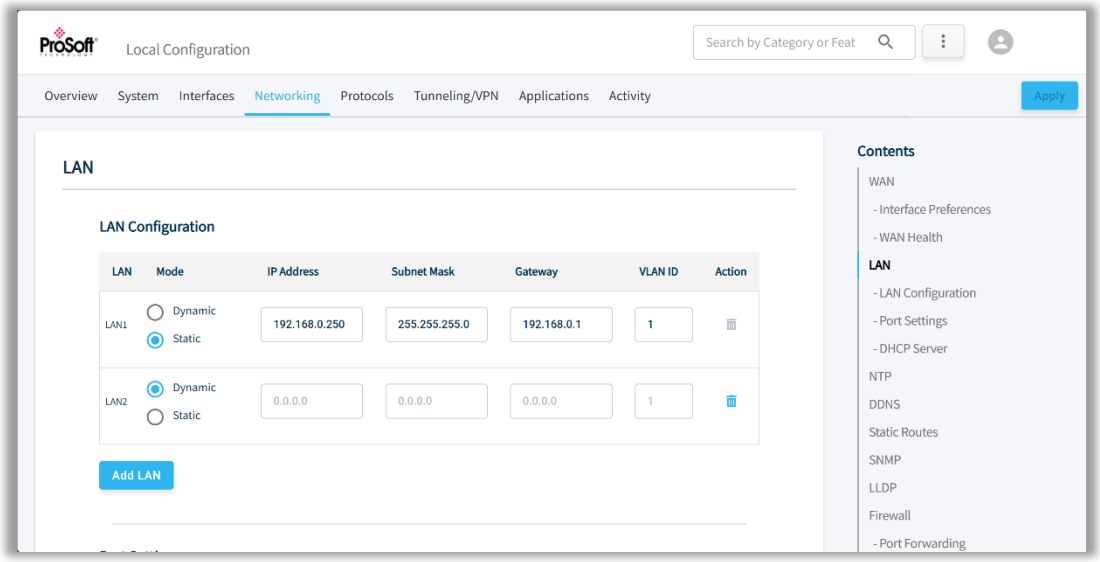
4.5.2 LAN

The *LAN Configuration* defines the type of Ethernet connection for a port, i.e., Static or Dynamic.

4.5.2.1 LAN Configuration

To create a LAN configuration:

1. Click on the *Networking* tab.
2. Under **LAN Configuration**, click the **ADD LAN** button. A maximum of four LAN ports can be added.



3. Select the *Mode*: **DYNAMIC** or **STATIC**.

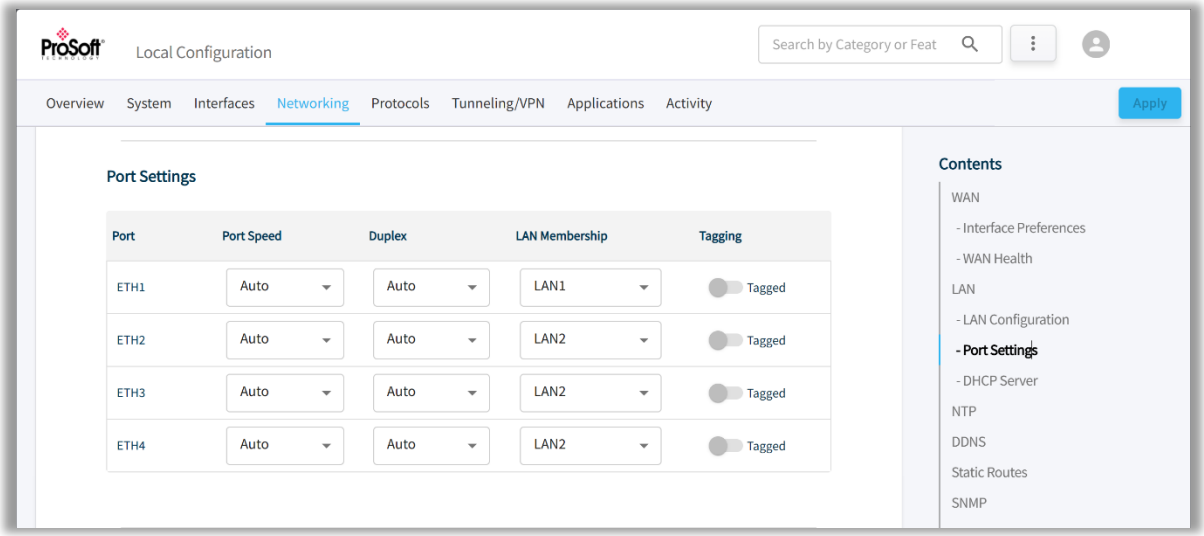
   For **STATIC** configuration, enter the following parameters:

Parameter	Description
IP Address	Static IP Address for the port.
Subnet Mask	Subnet mask of the IP Address.
Gateway	Default IP Address of the ELX3.
VLAN ID	VLAN identification number.

4. Click **APPLY** to save the changes.

4.5.2.2 Port Settings

To assign a LAN Configuration to a specific ELX3 Ethernet port:



1 Enter the following values:

Parameter	Description
Port Speed	Data transfer speed for the port. • Auto • 10Mbps • 100Mbps • 1Gbps
Duplex	Transmission mode for the port. • Auto • Half-Duplex • Full-Duplex
LAN Membership	Assign an existing LAN Membership (**LANx**) to the corresponding **ETHx** Port.
Tagging	VLAN tagging. **Note:** This parameter is currently not available.

Note: By default, the LAN2 DHCP IP address is set to **Dynamic** and configured to physical ports **ETH2**, **ETH3**, and **ETH4**.

2 Click **APPLY** to save the changes.

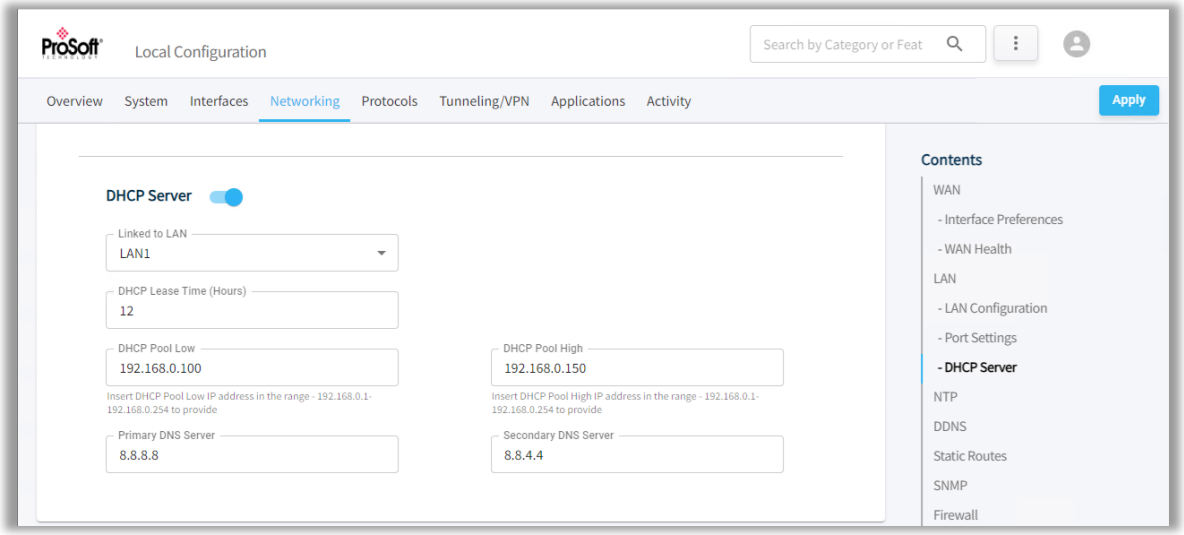
4.5.2.3 DHCP Server

The ELX3 can operate as a DHCP server that assigns IP address, DNS server, and default gateway address configurations to all devices connected via LAN. By default, this feature is disabled.

Dynamic allocation allows automatic reuse of addresses by granting temporary address leases to hosts as they are requested. When a lease expires, the host must renew the lease with the server. If the lease is not renewed, that address may be allocated to a new host. For dynamic allocation, a set of address pools (or "ranges") are configured on the server and new addresses are selected from these pools.

To configure the DHCP server on ELX3:

1. Click on the *Networking* tab.
2. Click the **DHCP SERVER** toggle button to enable the *DHCP Server* configuration.



3. Enter the following values:

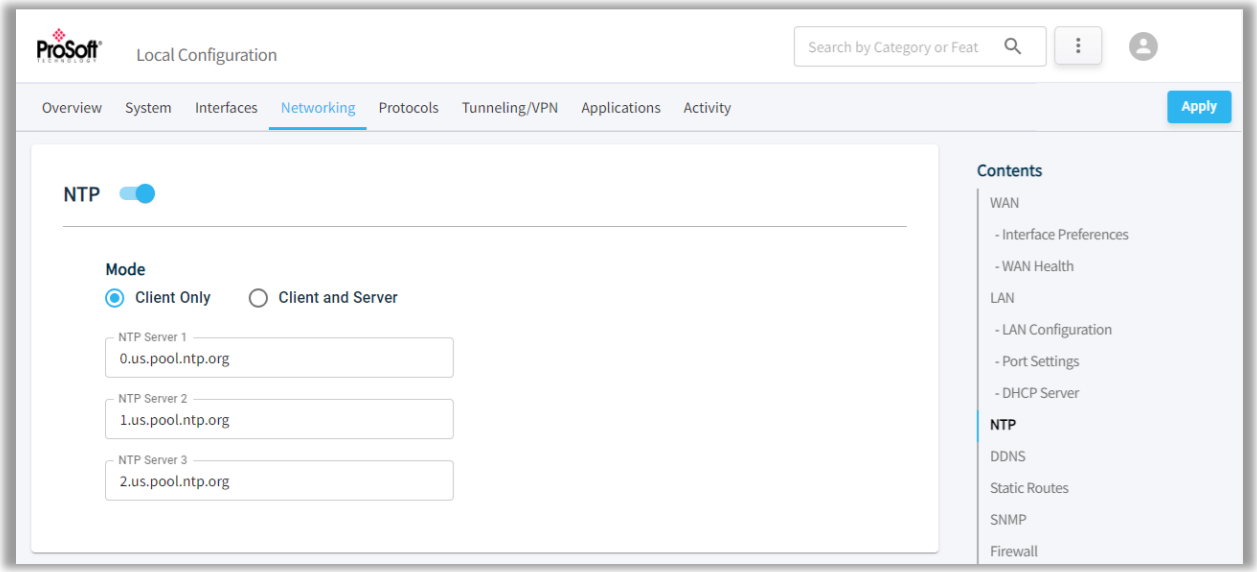
Parameter	Description
Linked to LAN	LAN port to be used to connect the end device to the network.
DHCP Lease Time	Lease period in hours (Range: 0 to 23)
DHCP Pool Low	Start of the range for the pool of IP addresses in the same subnet as the device.
DHCP Pool High	End of the range for the pool of IP addresses in the same subnet as the device.
Primary DNS Server	Primary DNS server IP address.
Secondary DNS Server	Secondary DNS server IP address.

4. Click **APPLY** to save the changes.

4.5.3 NTP

This feature enables the Network Time Protocol (NTP) to synchronize the clocks of data networks and the ELX3.

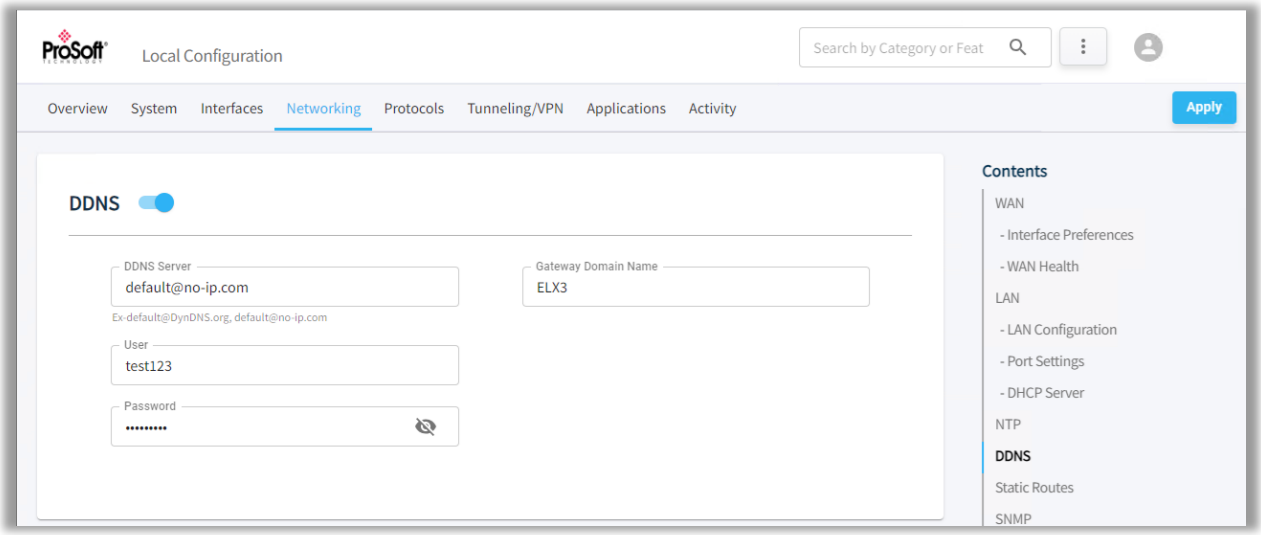
Click the **NTP** toggle button to enable the *NTP* configuration.



Parameter	Description
Mode	**Client Only**: NTP process will query NTP server and update ELX3 system time. **Client and Server**: NTP process will query NTP server and update ELX3 system time and resolve NTP requests from the LAN clients.
NTP Server 1, 2, 3	Server time updates for the ELX3. Default: **x.us.pool.ntp.org**

4.5.4 DDNS

The DDNS (Dynamic Domain Name System) feature is a method of mapping the configured WAN IP address to a domain name.

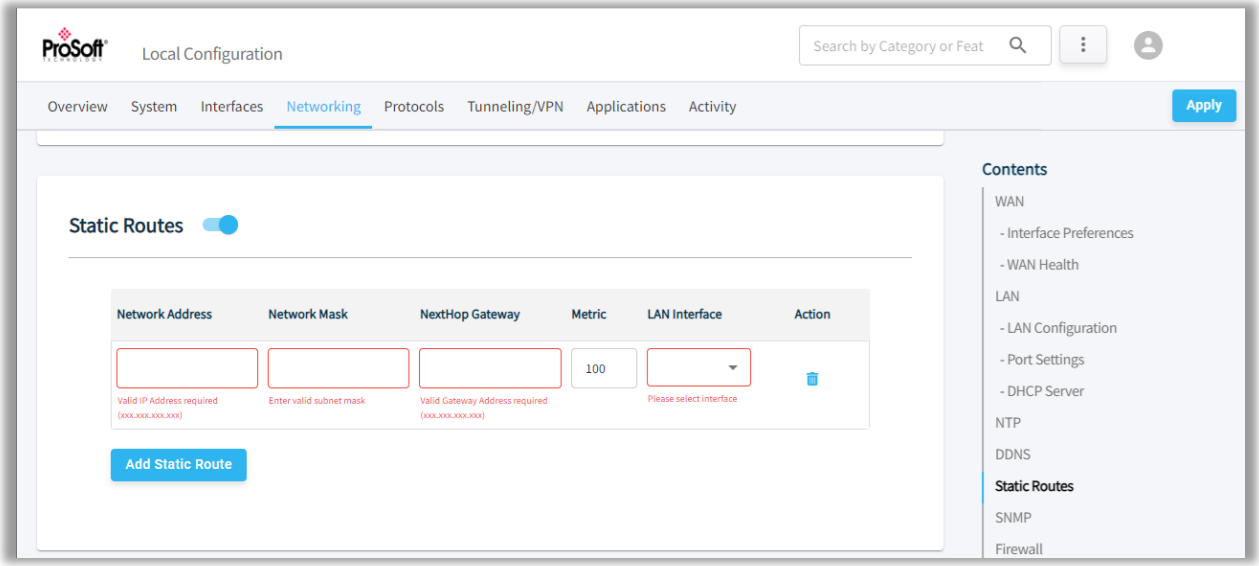


Parameter	Description
DDNS Server	DDNS Server Name. Default is set to default@no-ip.com. Max characters: 255
Gateway Domain Name	Gateway Domain Name. Max characters: 255
User	Username for DDNS Server. Default is set to **test123**. Length: 5 to 40 characters.
Password	Password for DDNS Server. Default is set to **Test@1234**. Length: 8 to 40 characters.

4.5.5 Static Routes

Static routing occurs when a router uses a manually configured routing entry, rather than information from dynamic routing traffic.

1. Click the **STATIC ROUTES** toggle button to enable the *Static Routes* configuration.
2. Click the **ADD STATIC ROUTE** button.



3. Enter the following values:

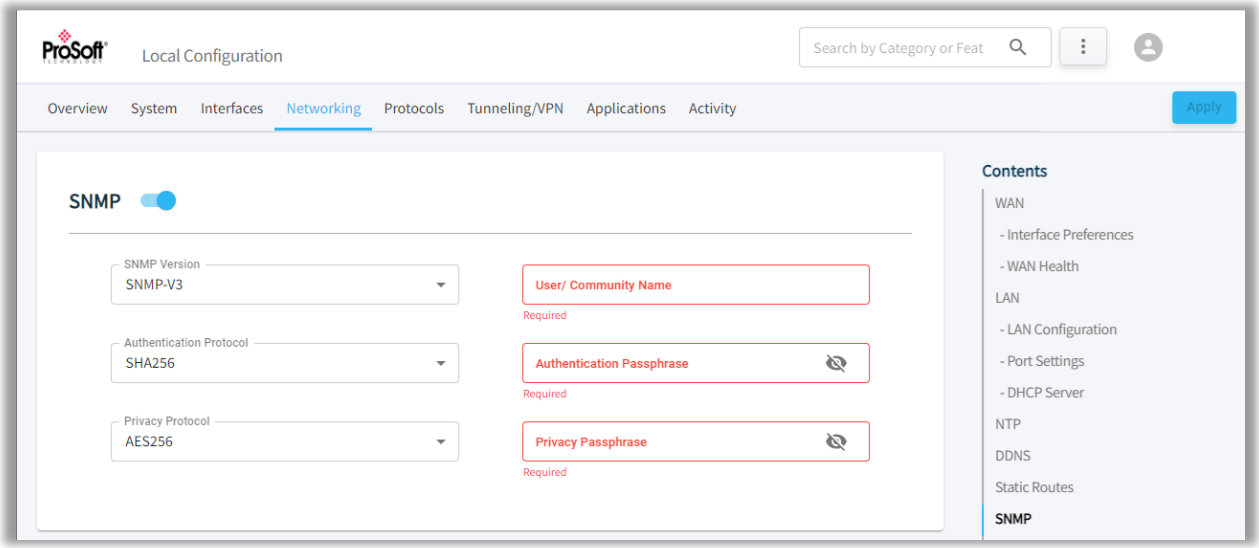
Parameter	Description
Network Address	IP Address of the network.
Network Mask	Subnet mask of the network.
NextHop Gateway	Next hop gateway address.
Metric	Metric can be any positive 32-bit number. Default is **100**.
LAN Interface	Select from the available LAN interfaces where static route needs to be added.
Action	Action button provides the option to delete the static route.

4.5.6 SNMP

Simple Network Management Protocol (SNMP) is an application-layer protocol for monitoring and managing network devices on a local area network (LAN) or wide area network (WAN).

The purpose of SNMP is to provide network devices, such as routers, servers, and printers, with a common language for sharing information with a network management system.

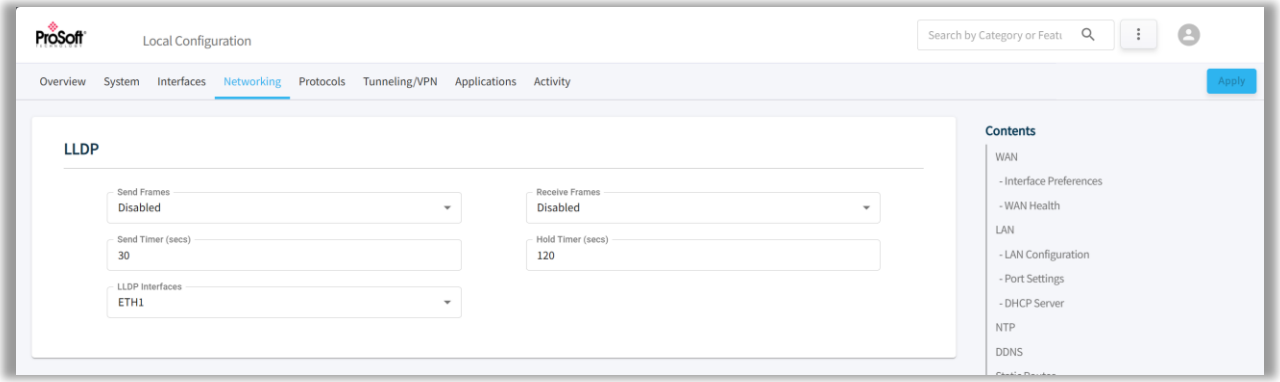
Click the **SNMP** toggle button to enable the SNMP configuration.



Parameter	Description
SNMP Version	Version of SNMP. Currently, only SNMP version 3 is supported.
Authentication Protocol	Protocol used for authentication which is preset to SHA256.
Privacy Protocol	Privacy protocol. Default: AES256.
User/Community Name	Username to be provided by user. It must be 5-20 characters alphanumeric.
Authentication Passphrase	A password is required for authentication to be added by the user. It must be 8 to 20 characters alphanumeric.
Privacy Passphrase	This is the password for privacy which needs to be provided by the user. It must be 8 to 20 characters alphanumeric.

4.5.7 LLDP

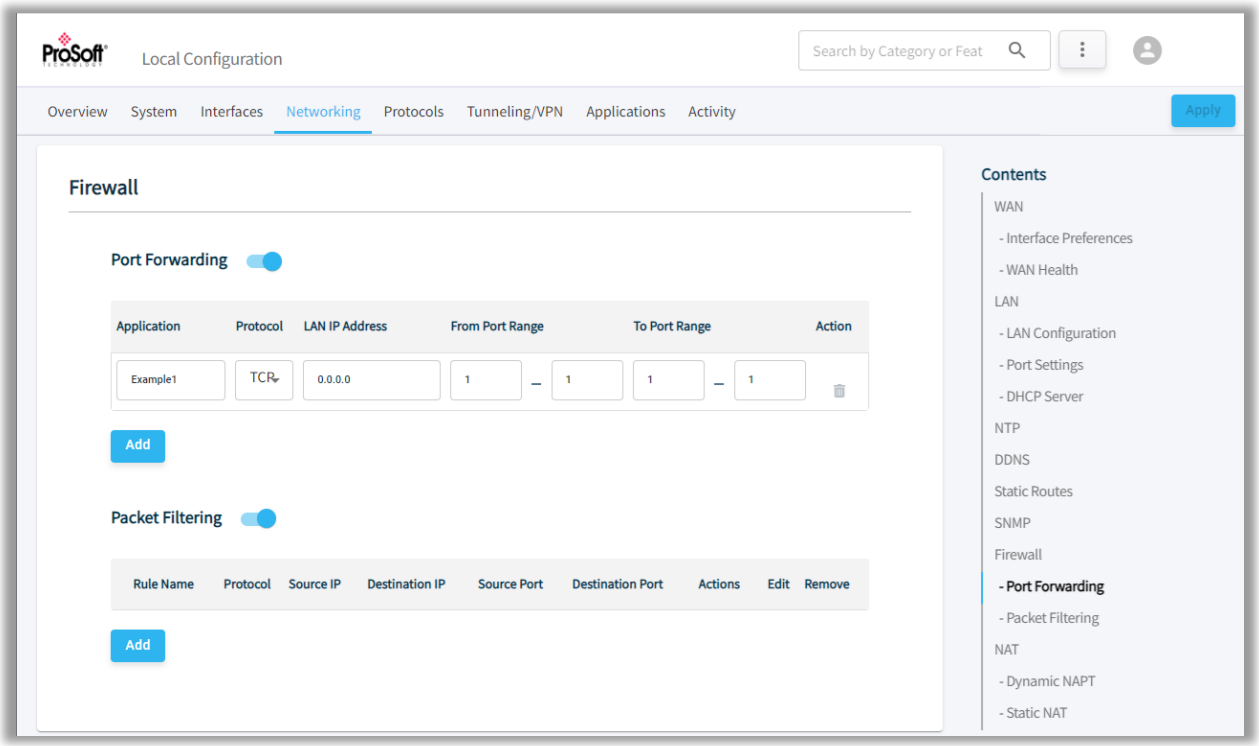
LLDP (Link Layer Discovery Protocol) is a vendor-neutral, layer 2 protocol used to discover and advertise information about neighboring network devices on a local area network (ETH). It allows network administrators to obtain a better understanding of the devices connected to the network, facilitating network management tasks such as device tracking, inventory management, and troubleshooting.



Parameter	Description
Send Frames	Allows the gateway to generate LLDP frames and transmit them to neighboring devices.
Receive Frames	Allows the gateway to accept LLDP frames transmitted by neighboring devices.
Send Timer	Configures the LLDP transmit timer in seconds (Range: 5 to 65534 seconds)
Hold Timer	The multiplier of *Send Timer* to determine the value of the TTL TLV sent to neighboring devices. (Range: 10 to 255 seconds)
LLDP Interfaces	Selects which physical Ethernet ports the LLDP packets should be transmitted and/or process received LLDP frames.

4.5.8 Firewall

The ELX3 implements the firewall feature to control the traffic flow between a trusted network (such as corporate LAN) and an untrusted or public network (such as Internet). It supports Port Forwarding and Packet Filtering.



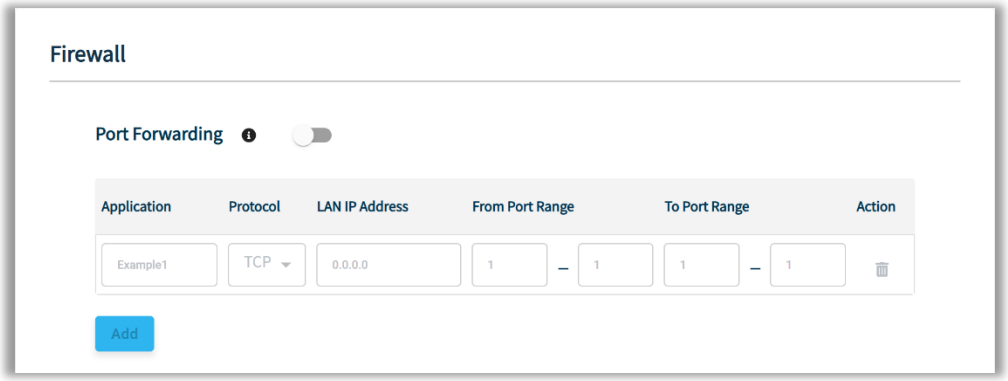
4.5.8.1 Port Forwarding

This feature allows a remote client device to access the multiple server devices connected to the ELX3 LAN by associating each one of these devices to an ELX3 port number. Up to 10 mappings can be created.

To configure Port Forwarding:

1 In the ELX3 configuration webpage, click on the *Networking* tab and toggle the **PORT FORWARDING** button.

> **Note:** The following TCP/UDP ports should not be configured with Port Forwarding:
> 21, 22, 67, 123, 161, 502, 2222, 4433, 5355, 44818, 50000.



2 Enter the following parameters:

Parameter	Description
Application	Name of the mapping.
Protocol	Select the protocol for packet delivery: *TCP*, *UDP* or *Both*
LAN IP Address	IP address of the destination LAN device. **Note:** When configuring the end device, make sure: The IP Address of the end device must match the value entered in the *End Device Address* field in the ELX3. The Gateway address on the end device must point to the ELX3 IP Address and Subnet Mask addresses.
From Port Range	The WAN port range through which data must be forwarded to each device.
To Port Range	The LAN device port range listening to the forwarded traffic.
Action	Deletes the mapping.

3 Click **ADD PORT** to add additional ports.

4 Click **APPLY** to save the changes.

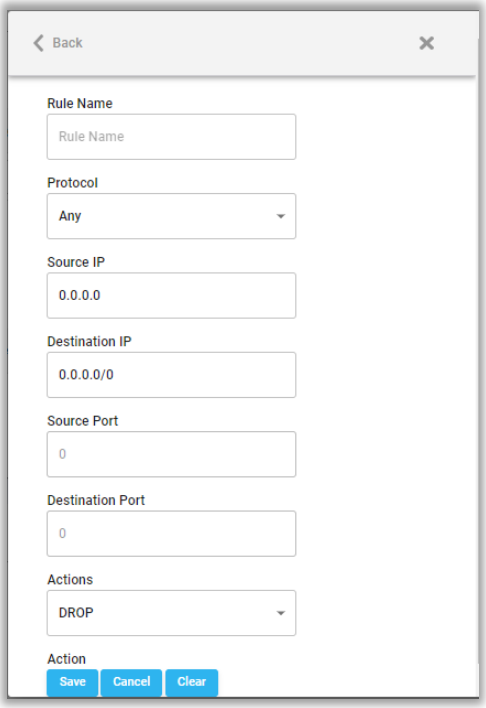
5.3.6.2 Packet Filtering

Packet Filtering specifies values in the Transport/Network layer header of TCP/IP protocol suite. The user can choose to accept the packet for forwarding OR drop the packet silently.

The *Packet Filtering* feature, also called 5T firewall, applies to routed (forwarded) traffic only. It controls the packets that are allowed to pass from **WAN-to-LAN** or **LAN-to-WAN** or **LAN-to-LAN** interface.

1 In the ELX3 configuration webpage, click on the *Networking* tab and toggle the **PACKET FILTERING** button to enable the *Packet Filtering* configuration

2 Click on the **ADD** button to configure a packet filtering rule.



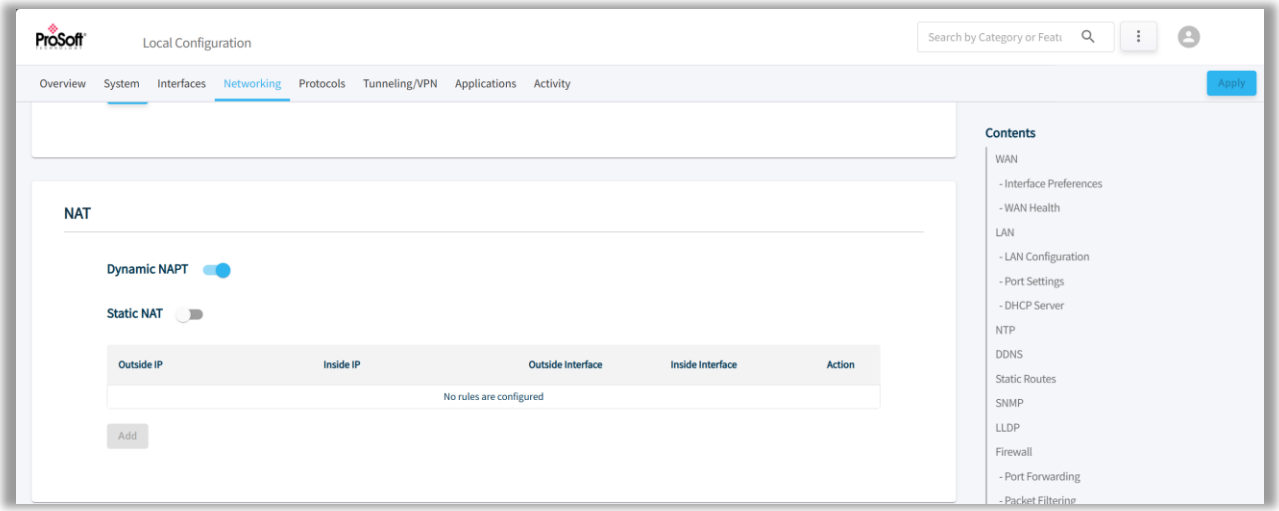
3 Enter the values for the following parameters:

Parameter	Description
Rule Name	Name of rule. Allows up to 40 alphanumeric and special characters “_”, “-”
Protocol	Protocol used for packet filtering.
Source IP	IP of the source device.
Destination IP	IP address of destination device.
Source Port	Port used for source device.
Destination Port	Port used for destination device.
Actions	The action to **Accept** the packet for forwarding or **Drop** the packet.

4 Click on the **SAVE** button.

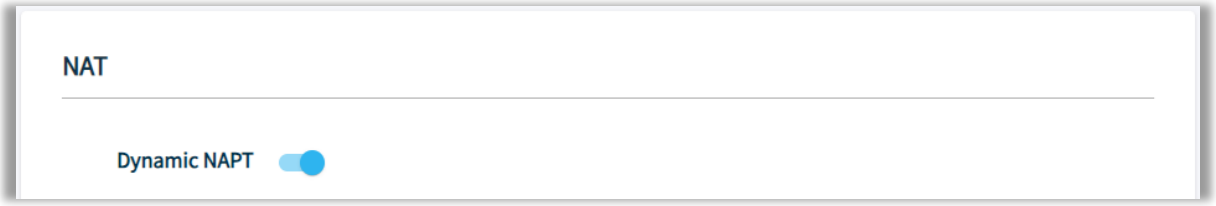
4.5.9 NAT

The ELX3 supports Dynamic NAPT and Static NAT. It allows the port and the IP address to connect to the internet or outside world.



4.5.9.1 Dynamic NAPT

The ELX3 supports dynamic network address and port translation (DNAPT). This allows the port and IP address to dynamically change while accessing the WAN from the LAN. Multiple devices can then connect to the outside.

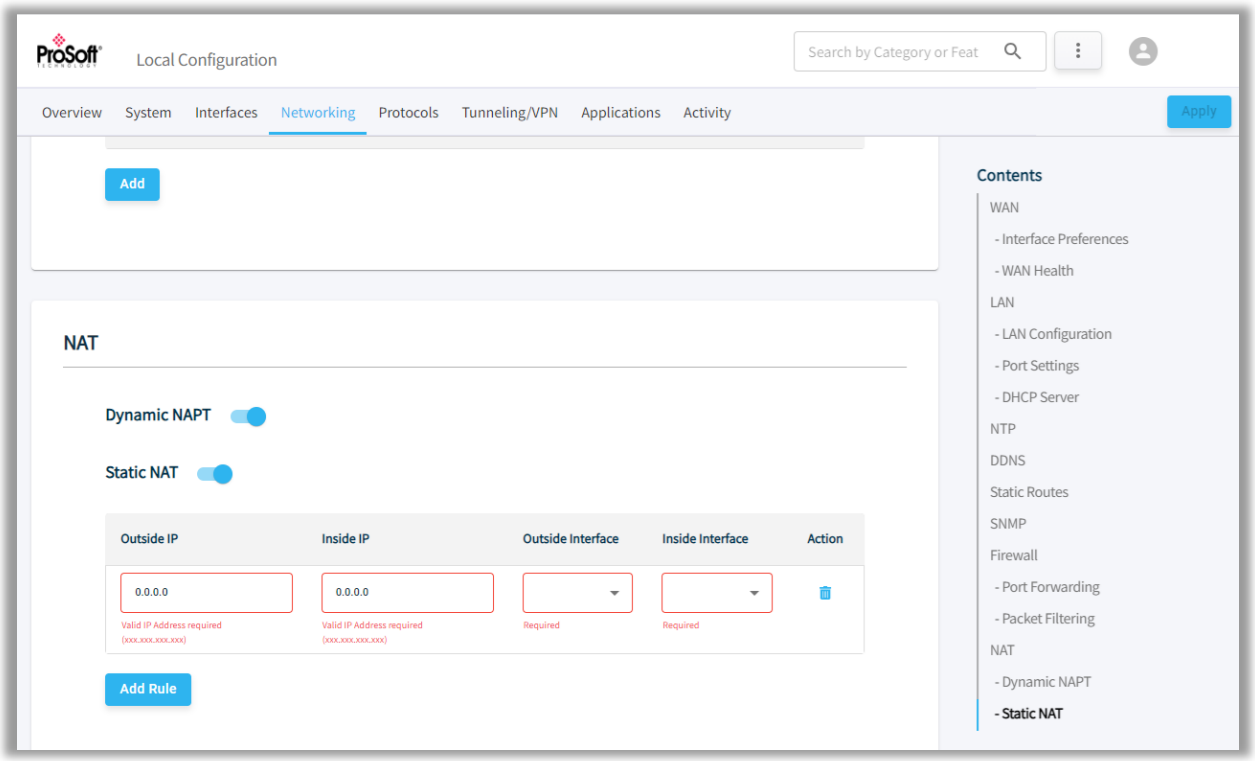


4.5.9.2 Static NAT

Static Network Address Translation (NAT) is a one-to-one mapping of a private IP address to a public IP address. *Static NAT* is useful when a network device inside a private network needs to be accessible from the internet.

To configure *Static NAT*, the Packet Filter rules must be pre-configured. Refer to section *5.3.6.2 Packet Filtering* to configure the Packet Filtering rules.

1 Click the **STATIC NAT** toggle button to enable its configuration and then click on **ADD RULE** to add an entry.



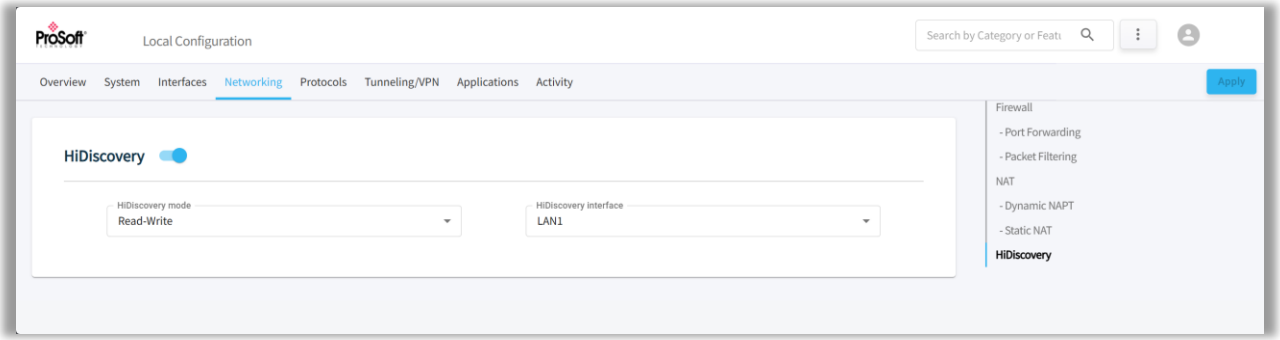
2 Enter the values for the following parameters:

Parameter	Description
Outside IP	The public IP address on which the user will access the end device.
Inside IP	The private IP address on which the end device is connected to the ELX3.
Outside Interface	WAN/Internet interface
Inside Interface	LAN/End-device interface.
Action	Delete icon removes the rule.

3 Click on the **APPLY** button.

4.5.10 HiDiscovery

HiDiscovery is a discovery protocol that has 2 ends i.e. PC side application and device side application. It follows a client/server architecture. The PC side application acts as a client and device side application acts as a server.

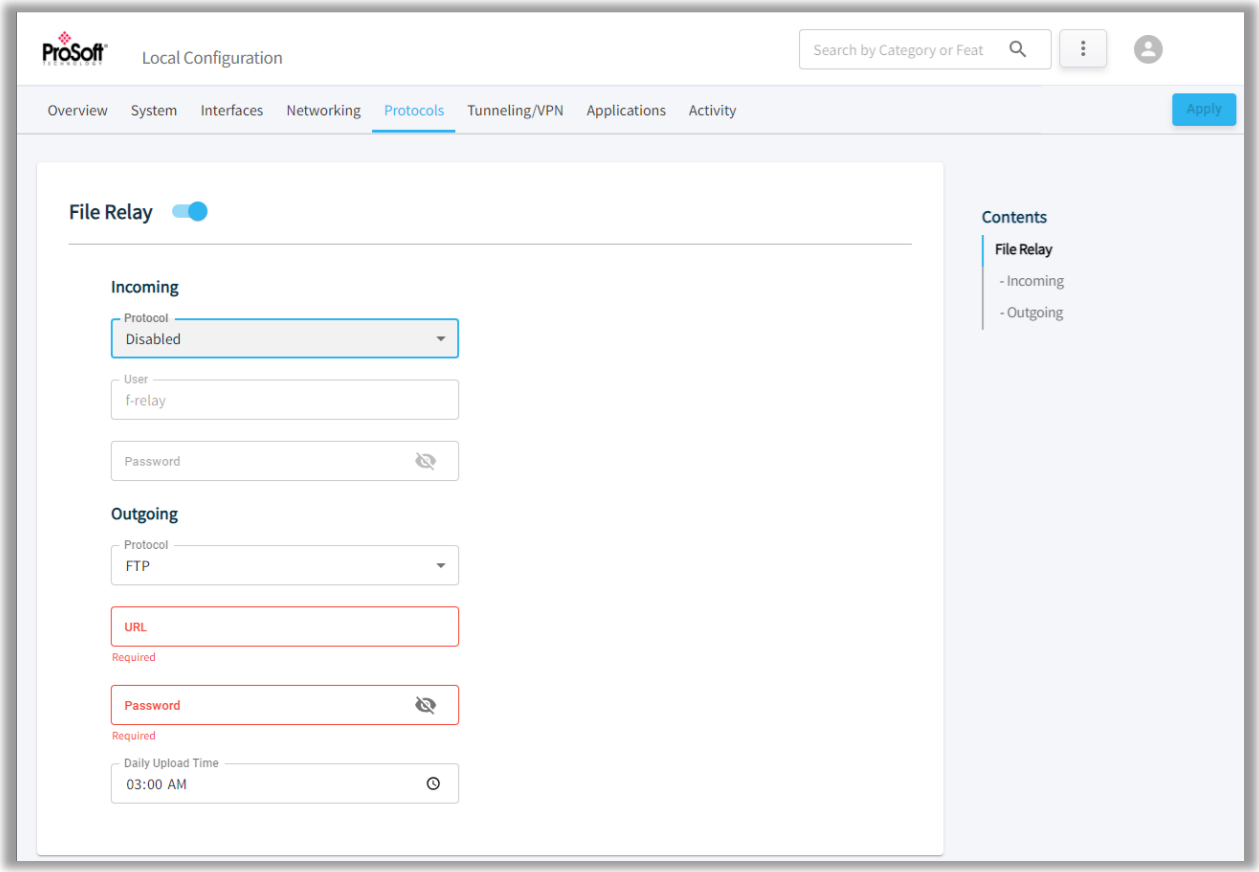


Parameter	Description
HiDiscovery Mode	**Read-Only** or **Read-Write**
HiDiscovery Interface	LAN interface used for HiDiscovery

4.6 Protocols Tab

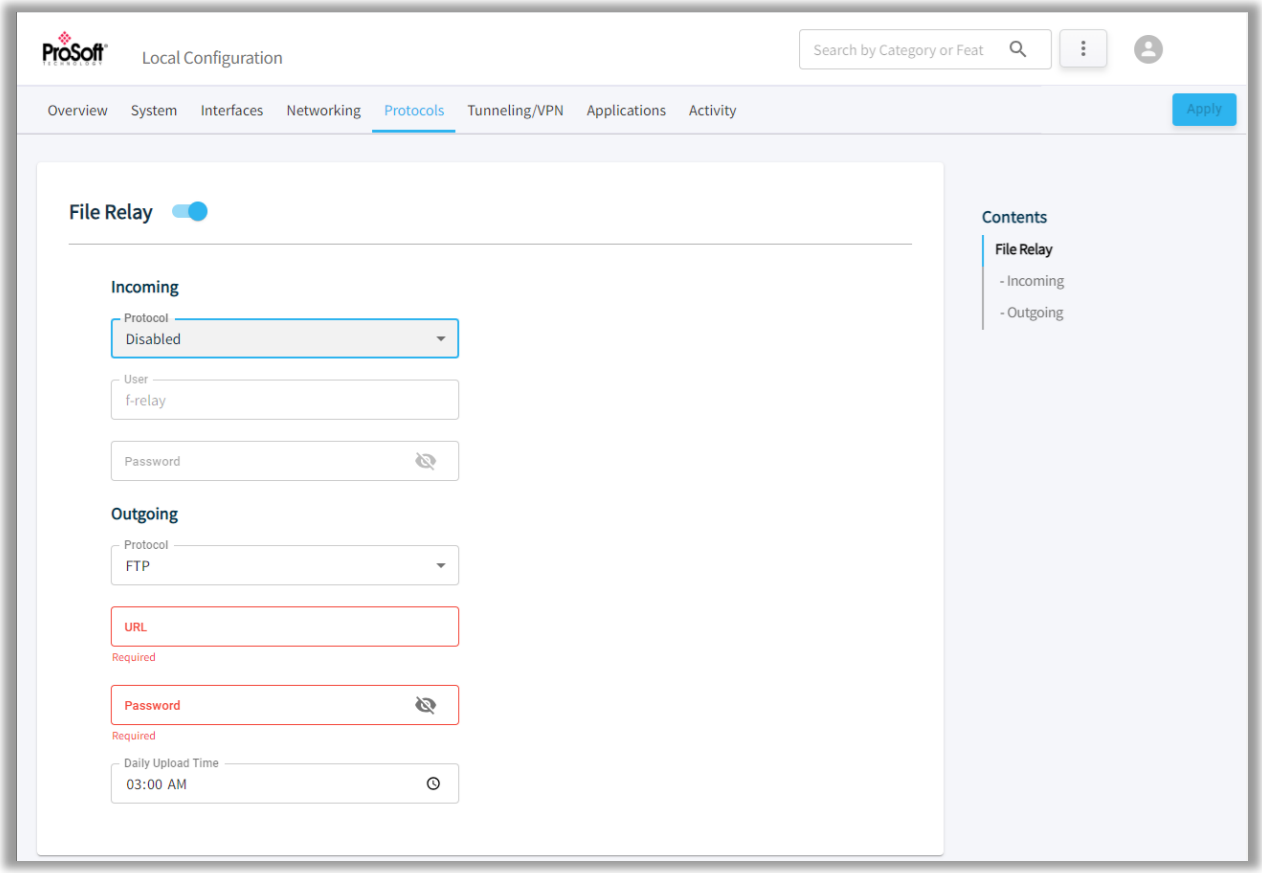
The *Protocols* tab contains the *File Relay* feature. This feature allows the user to use the ELX3 Internal Storage (/user folder) as a temporary storage medium for large files that can be automatically transferred to a remote location.

Files can be copied to the ELX3 Internal Storage from an FTP/SFTP Client. The files can then be transferred to a remote FTP/SFTP Server, or via Belden Horizon Console.



4.6.1 File Relay

The *File Relay* functionality enables simple and secure transfer of files across segmented networks. For example, if the user would like to back up their OT equipment configuration files on the server without wanting to create a link between the IT and OT network, the ELX3 can be used to segment between the two networks.



1 In the *Incoming* section of the *File Relay* tab, select the **FTP** or **SFTP** protocol to enable FTP or SFTP Incoming file transfer.

2 Use the following table to enter the appropriate parameters:

Parameter	Description
Incoming	
Protocol	Disabled FTP (File Transfer Protocol) SFTP (Secure File Transfer Protocol)
User	The username is for uploading files through FTP to the Internal storage. The default value is **f-relay**.
Password	Password for FTP access. The password must have at least 8 characters, contain at least one uppercase letter, one lowercase letter, and one special character.
Outgoing	
Protocol	The protocol of the server used as the destination for the File Relay. Supported protocols for upload are: • FTP • SFTP • Belden Horizon
URL	URL of the server used as the destination for the File Relay. Supported protocols for upload are FTP/SFTP/Belden Horizon Console. • FTP: ftp://user@host/ • SFTP: sftp://user@host:port/ • Belden Horizon Console cloud.
Password	(FTP only) Password used to upload to the remote server. The configured value can be viewed by pressing the "eye" button.
Host Key	(SFTP only) Public Key that authenticates SFTP Server and proves its identity to the ELX3 client. This should be copied from the SFTP Server and pasted here. The Public Key from the SFTP Server should be exported as **OpenSSH** format.
Generate SSH-Key	(SFTP only) Public key that authenticates the SFTP Server user for file transfer. Once generated, it should be copied to the SFTP Server as a **.pub** file and associated with the designated user. The SSH-Key pair generation takes place the first time it is requested. Subsequent requests return the same public key. SSH keys will be removed upon gateway factory reset.
Daily Upload Time	The upload time, shown in the Local UI is **UTC** – similar with the time on the *Overview* page. Default time is 03:00.

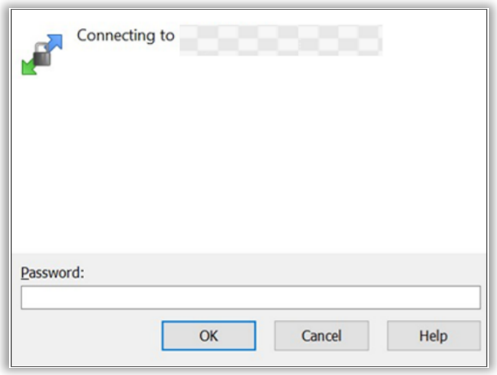
3 Click **APPLY** when complete.

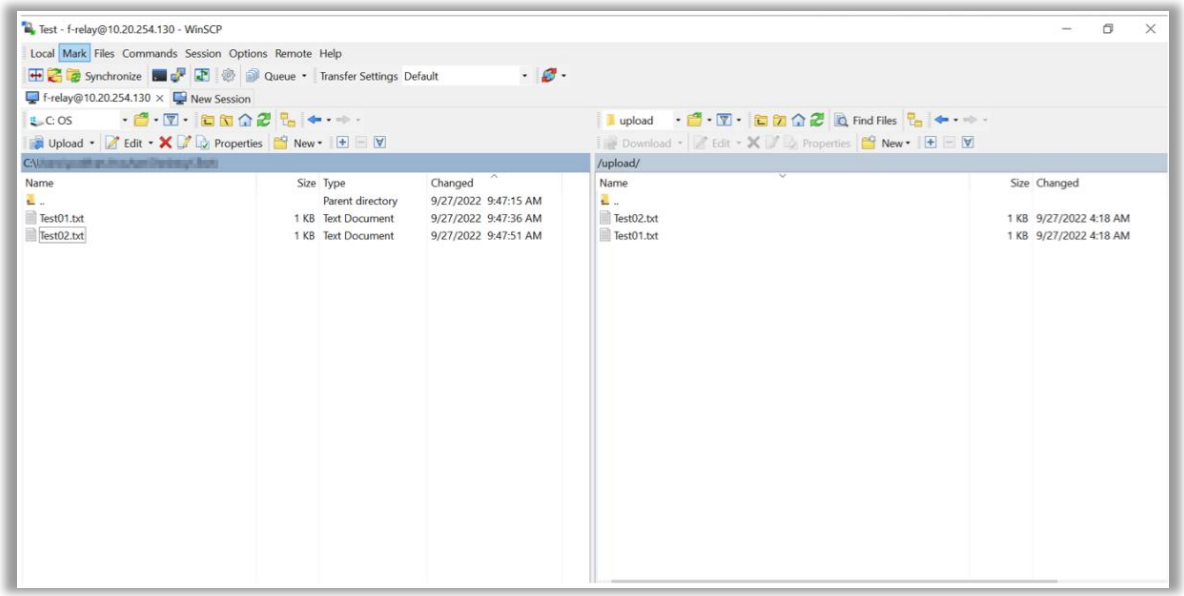
4.6.2 File Transfer to Belden Horizon Console

Users can transfer files from ELX3 to Belden Horizon Console.

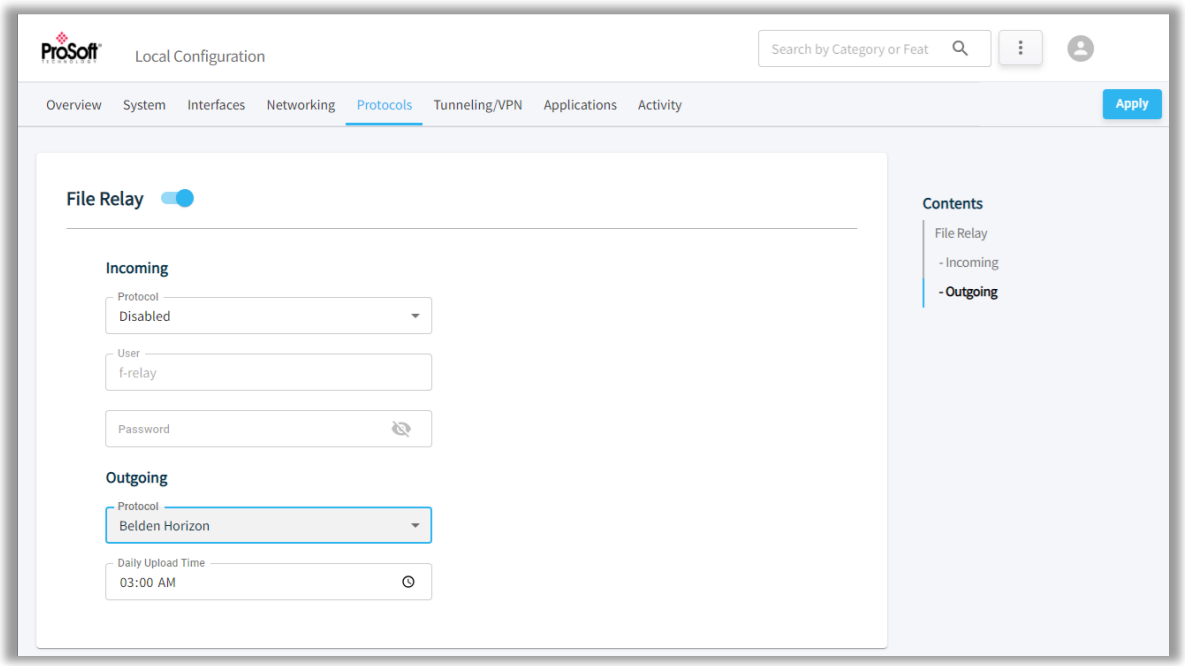
1. Generate the Activation key from the *Overview* tab and add the gateway on Belden Horizon Console. See section *3.1 Registration Using Activation Key* for more information.
2. Open the WinSCP application.
3. From the WinSCP Client, open a SFTP/FTP session to ELX3. Transfer the files to the *Upload* folder in ELX3 Internal Storage. Use the same username and password for the SFTP/FTP session as given on the ELX3 Incoming file relay. For more information, see section *0*

4 *File* Relay.


Connecting to
Password:
OK
Cancel
Help

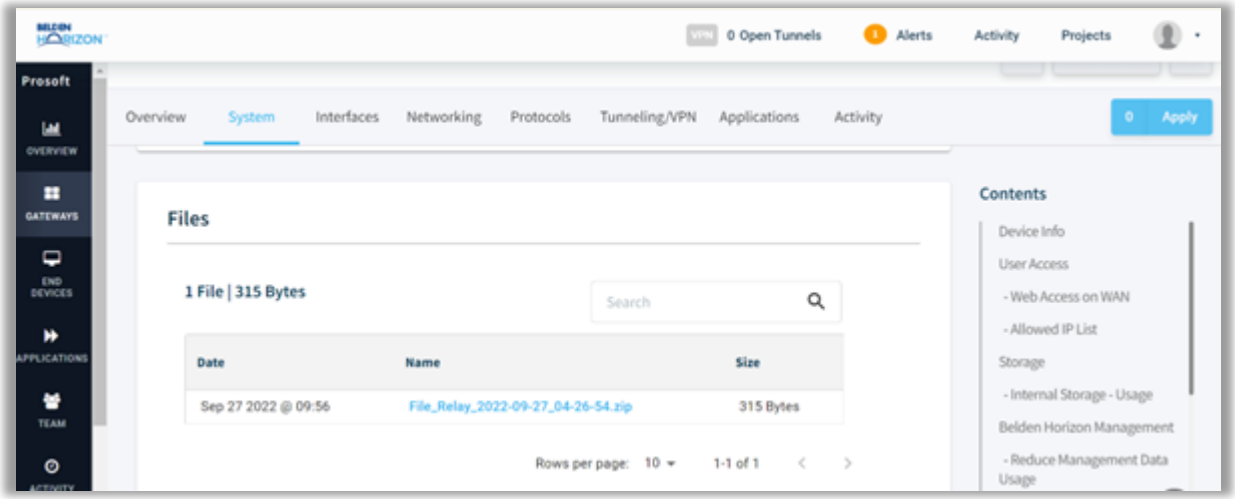

Test - f-relay@10.20.254.130 - WinSCP
Local Mark Files Commands Session Options Remote Help
Synchronize Queue Transfer Settings Default
f-relay@10.20.254.130 New Session
C: OS
Upload Edit Properties New
upload
Download Edit Properties New
Find Files
/upload/
Name Size Type Changed
Parent directory 9/27/2022 9:47:15 AM
Test01.txt 1 KB Text Document 9/27/2022 9:47:36 AM
Test02.txt 1 KB Text Document 9/27/2022 9:47:51 AM
Name Size Changed
Test02.txt 1 KB 9/27/2022 4:18 AM
Test01.txt 1 KB 9/27/2022 4:18 AM

5 From the Local User Interface *Protocols* tab, set the *Outgoing* > *Protocol* parameter to *Belden Horizon Console*. Also, set an appropriate time for file transfer in the *Daily Upload Time* parameter.



6 After uploading the files to the */upload* folder, the user can find the transferred file on Belden Horizon Console. It may take up to 10 minutes for file transfer as the file transfer cycle is triggered once in 10 minutes.

The files can be found in the Belden Horizon Console at *Gateway* > *System* tab > *Files*.

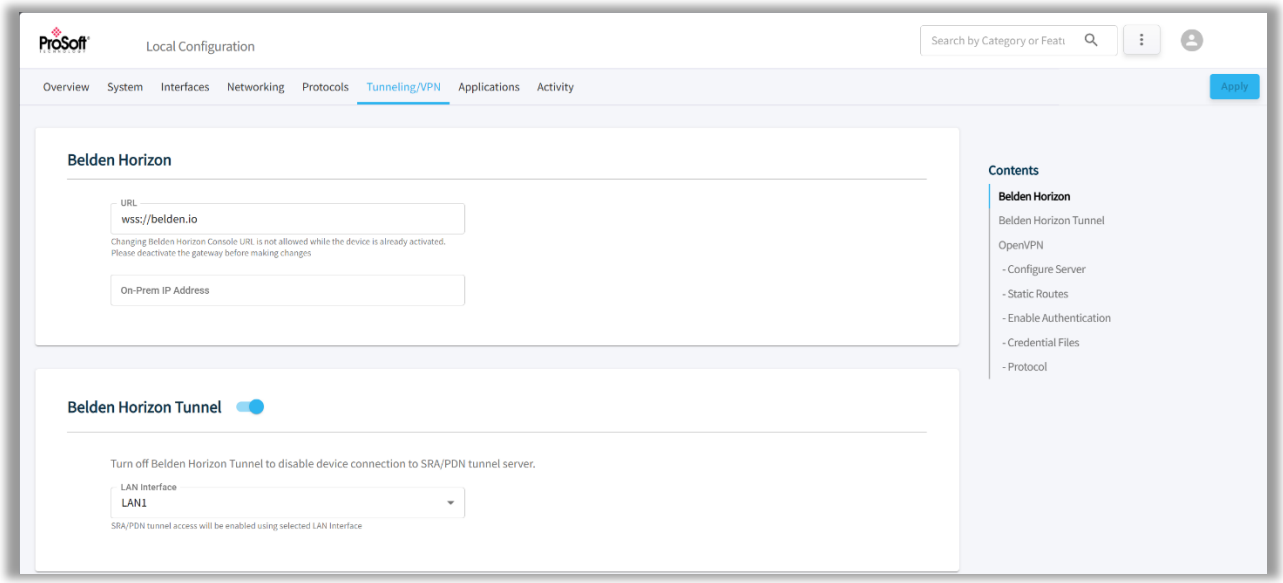


The user can download the .zip file and extract the transferred files from it.

Note: Belden Horizon Console files can be transferred only once in 24 hours.

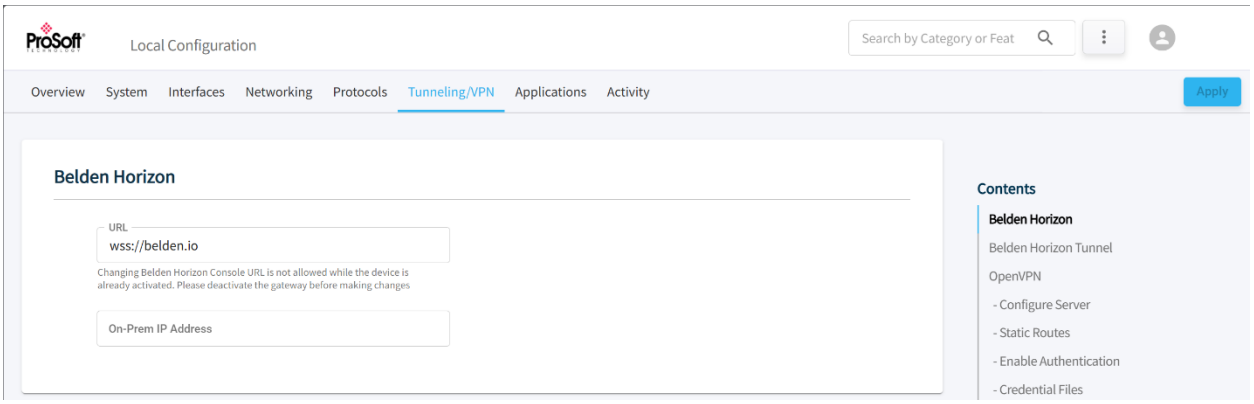
4.7 Tunneling / VPN Tab

The *Tunneling/VPN* tab allows the configuration of a Virtual Private Network (VPN) tunnel using Belden Horizon Console, SRA & PDN Tunnel, and Open VPN.



4.7.1 Belden Horizon

The Belden Horizon configuration defines the Belden Horizon Console instance used to activate the ELX3.

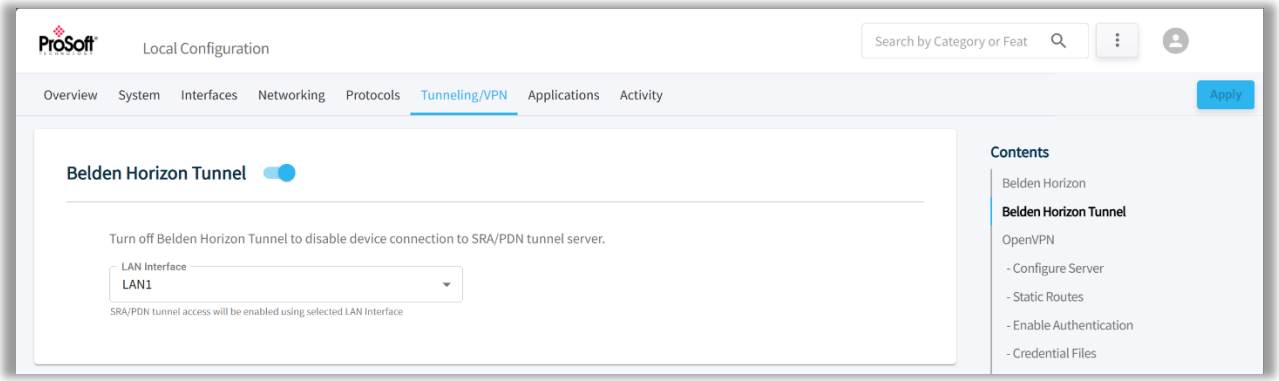


Parameter	Description
URL (Default)	wss://belden.io **or** wss://onprem.belden.io **Note:** The Belden Horizon Console URL cannot be changed if the device is already activated. The gateway must be deactivated to edit.
On-Prem IP Address	https://onprem.belden.io/ The On-Prem IP Address when using the wss://onprem.belden.io in the above parameter.

4.7.2 Belden Horizon Tunnel

This section controls the enable/disable of the Belden Horizon Console SRA/PDN tunnel configuration feature. Select the LAN interface (Default **LAN1**) to be used.

Select the **LAN INTERFACE** of the local network that the ELX3 will provide access to when establishing a VPN tunnel through Belden Horizon Console.

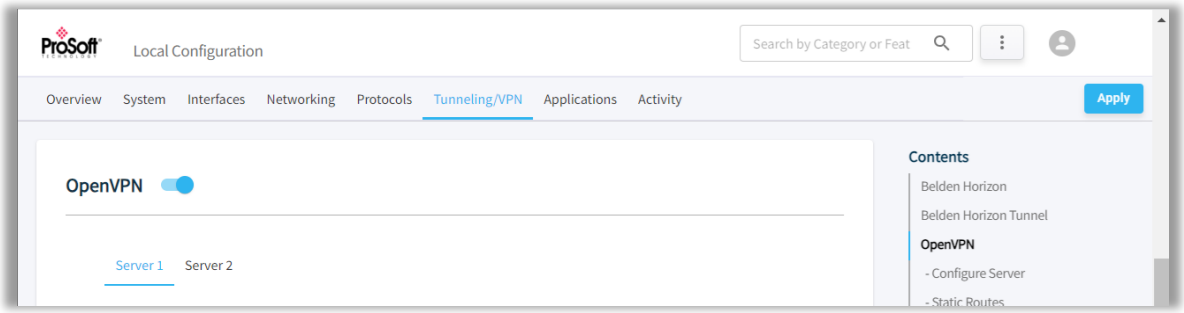


Note: The SRA/PDN tunnel is enabled by using the selected LAN Interface.

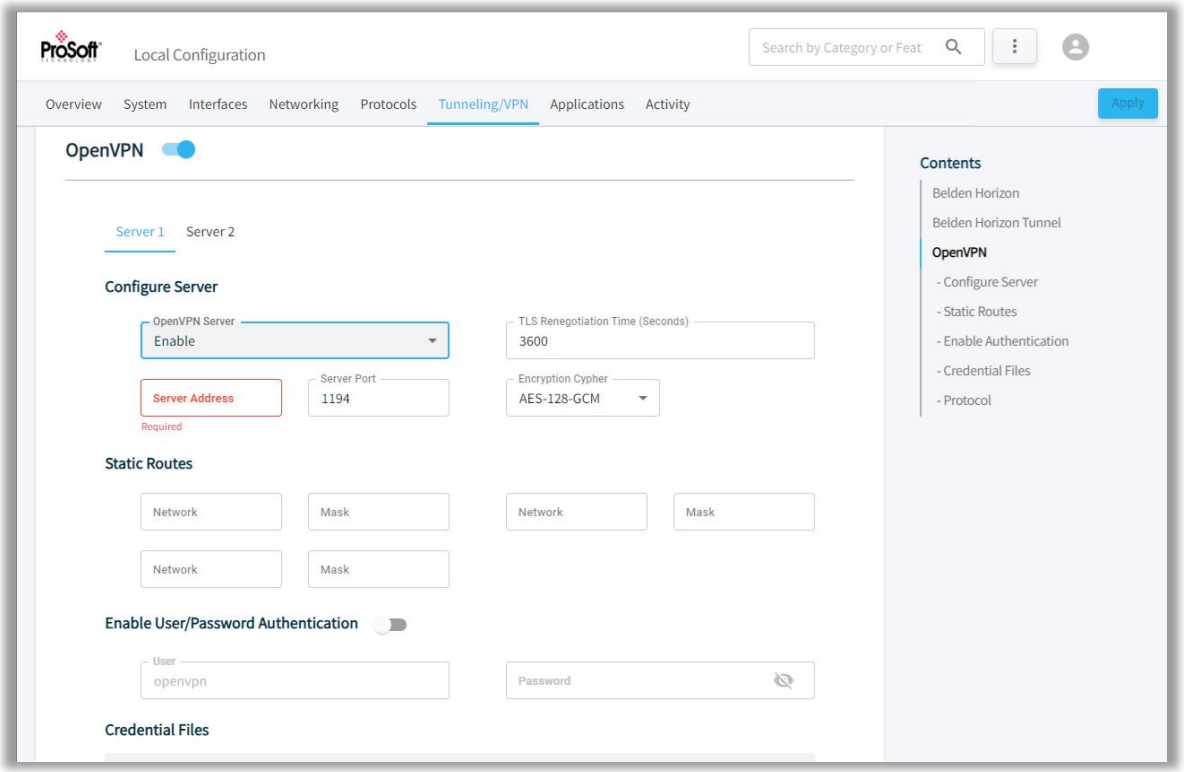
4.7.3 OpenVPN

The Virtual Private Network (VPN) Tunnel allows access to a private local network. OpenVPN is an open-source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange.

1 The **OPENVPN** toggle button allows user to turn on/off the feature after clicking on the **APPLY** button.



2 To configure OpenVPN, the following parameters are required:



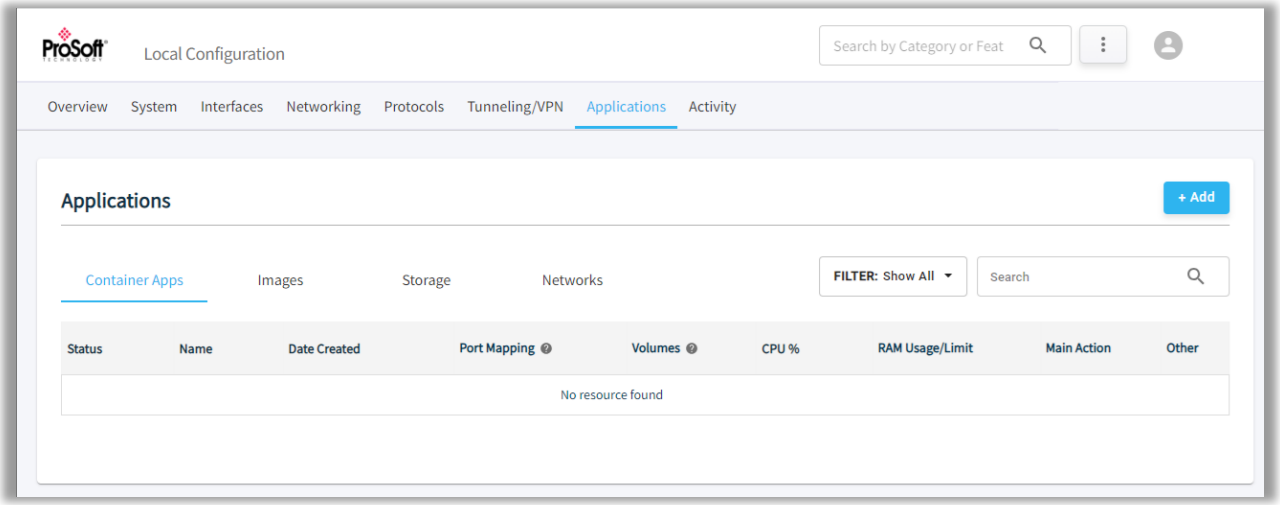
Parameter	Description
Configure Server	
OpenVPN server	A dropdown to enable or disable the server.
TLS Renegotiation Time	Transport layer Security renegotiation time in seconds. This controls how often the underlying SSL/TLS session renegotiates. This provides additional security by frequently rekeying the session keys. Default value: 3600.
Server Address	IP address or hostname of the VPN server. This is the target IP Address to tunnel to. Default value: 3.216.155.83
Server Port	Server port number for the OpenVPN. Default value: 1194
Encryption Cypher	Cypher used to encrypt data channel packets. Some of the cyphers that are supported by OpenVPN are not available in this list because they are considered insecure. However, these can still be used by using a custom configuration file.
Static Routes	Static routes to remote networks to be specifically accessed through the configured OpenVPN connection. A maximum of 3 static routes are supported per tunnel.
Enable User / Password Authentication	Alternative authentication method based on username and password. Enter a Username and Password.
Credential Files	Click the **BROWSE FILE** button to locate the corresponding files. **Note**: These Credential files are mandatory to enable OpenVPN. They can either be uploaded individually or have their content added inline, within the custom configuration file. If the credential files are inline in the configuration file, the individually uploaded files will take precedence.
Certificate Authority	VPN authentication that issues certificates for VPN, Secure Internal Communication (SIC), and users.
Client Certificate	Issued by a certificate authority as proof of identity
Client Key	Password to the corresponding client certificate.
Custom Configuration File	Click the **CHOOSE FILE** button to locate and upload a custom OpenVPN configuration file. If the user has not previously uploaded any credential files, the *Custom Configuration File* should include them.
Protocol	The protocol to use when connecting with the remote: **TCP** or **UDP**

3 Click on the **APPLY** button when complete.

4.8 Applications Tab

The *Applications* tab allows the user to perform actions on containers.

For more information about the *Applications* tab and its features, please see section *5.2 Local User Interface*.



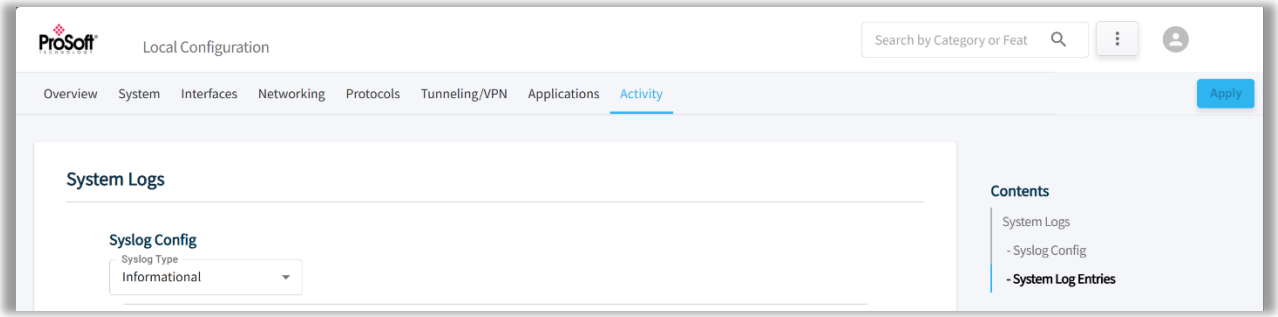
4.9 Activity Tab

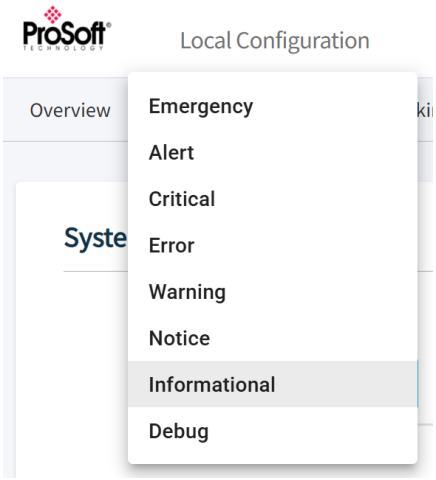
The *Activity* tab displays ELX3 diagnostics information including System Logs.

4.9.1 System Logs

The ELX3 can record various system log and event messages and store them in a local log file.

4.9.1.1 Syslog Config

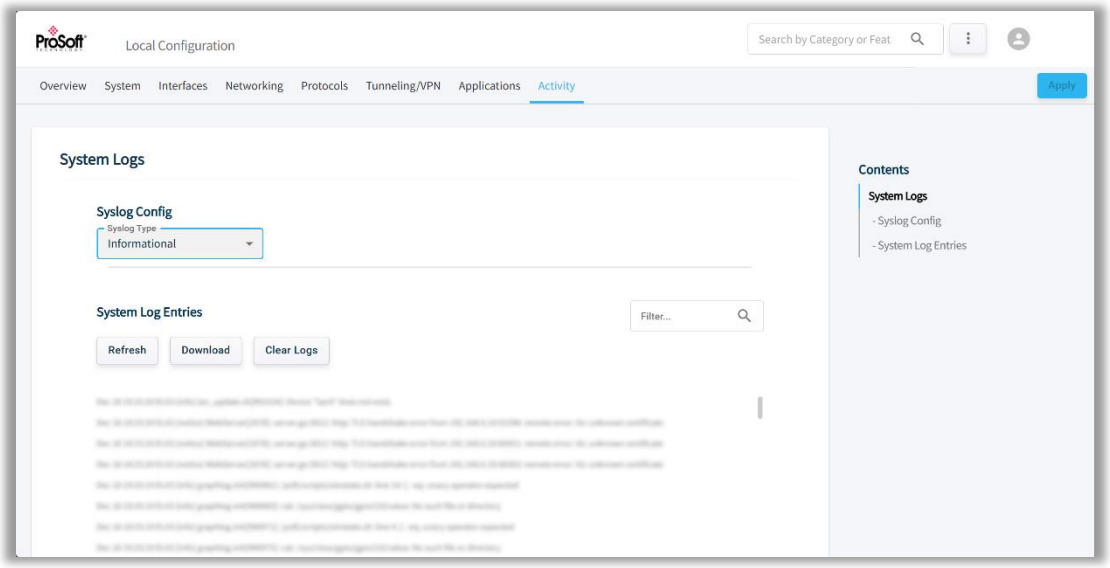




Parameter		Description
Syslog Config	Syslog Type	**EMERGENCY**: System unusable. **ALERT**: Immediate action required. **CRITICAL**: Critical conditions detected. **ERROR**: Error conditions detected. **WARNING**: Displays system messages and failures only. **NOTICE**: Normal but significant conditions detected. **INFORMATIONAL**: Displays all Warning messages, plus additional messages. **DEBUG**: Logs all messages; used for resolving issues.

5.7.1.2 System Log Entries

The *System Log Entries* displays the details of the following parameters:



Parameter	Description
Refresh	Refreshes the log results.
Download	Transfers the log file from the ELX3 to PC.
Clear Logs	Clears the recorded logs.
Search/Filter bar	Search/filter for a specific log entry.

5 Container Deployment

This chapter covers a typical deployment of containerized applications on the ELX3 Gateway via the Local User Interface and Belden Horizon Console.

A container is a light-weight, self-contained environment that holds everything an app needs to run. All containers on the host machine run in isolation of each other and share the host's resources but keeps the containers isolated making it easy to run consistently across different environments without the need of a full operating system.

Once the Belden/ProSoft Application (Example: ProSoft Technology's *ELX-EIP-MBTCP Container*) is initially deployed from the Belden Horizon Console, the Application can be managed in the Belden Horizon Console or Local User Interface. The user can monitor the following information for a particular container:

- Processor use, in percentage
- Memory use, in MB

5.1 Belden Horizon

5.1.1 Container Network Configuration

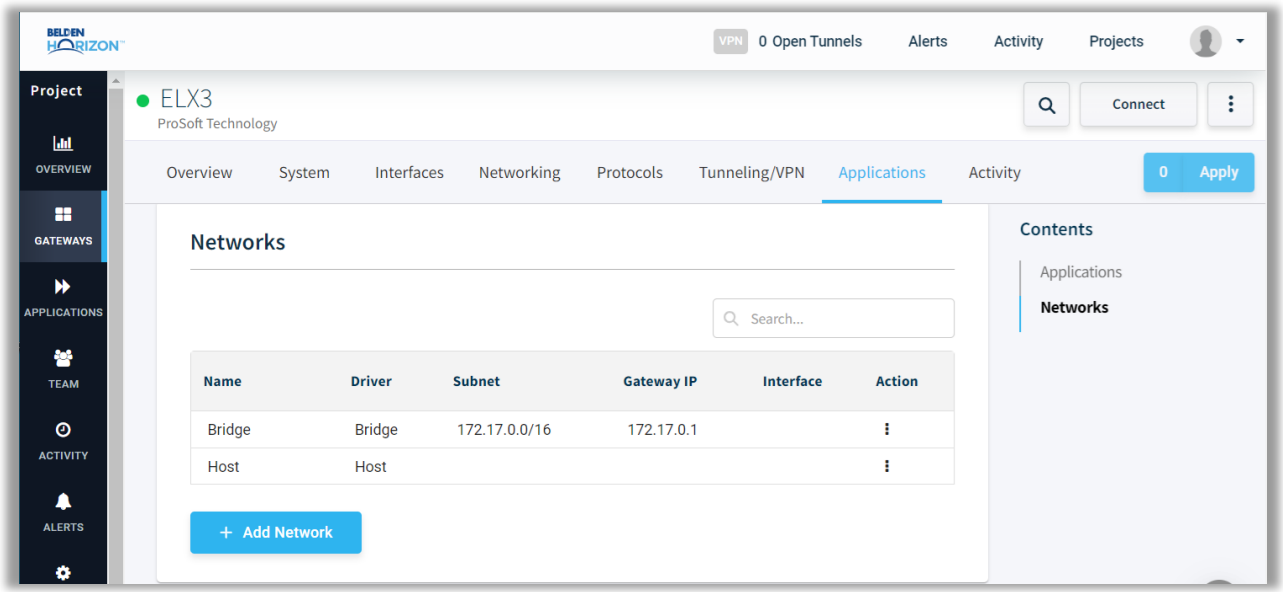
An ELX3 gateway container network must be configured before deploying the container.

A network is the functionality that allows a container to communicate to external devices by using the host's configured LANs. This section concentrates specifically on the virtual network between containers also known as Docker networks.

A Docker network is a powerful feature that enables containers to communicate with each other and the outside world. It provides isolated and secure networking environments, allowing seamless connectivity and easy management of containerized applications.

The ELX3 provides the ability to run Docker containers providing the flexibility to run custom code for advanced applications such as machine learning, predictive maintenance, or custom protocol drivers.

5.1.1.1 Adding a Network to Gateway

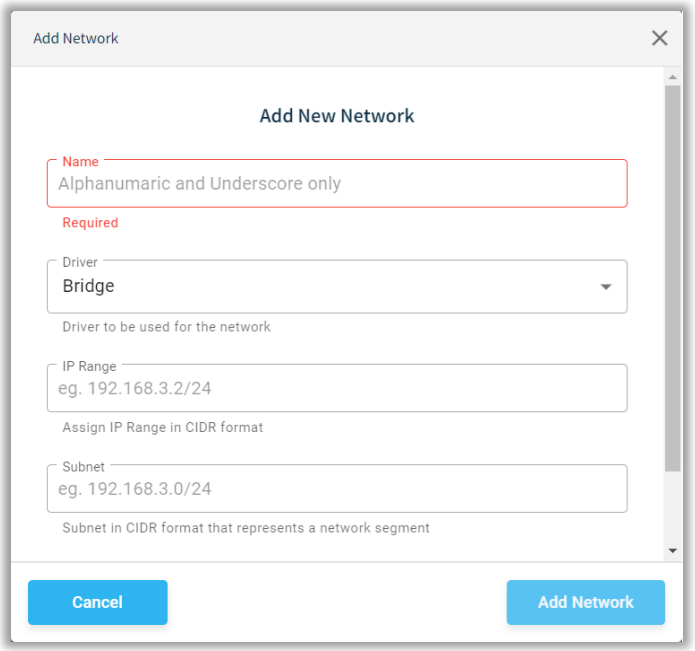


Note: The *Network* tab has two default networks - *Bridge* and *Host*. These two networks cannot be deleted.

To create a network:

1. In the Belden Horizon Console, navigate to the *Gateway* > *Applications* > *Networks* section.
2. Click **ADD NETWORK** to open the *Add Network* wizard.

3 Enter the name of the network to be created.

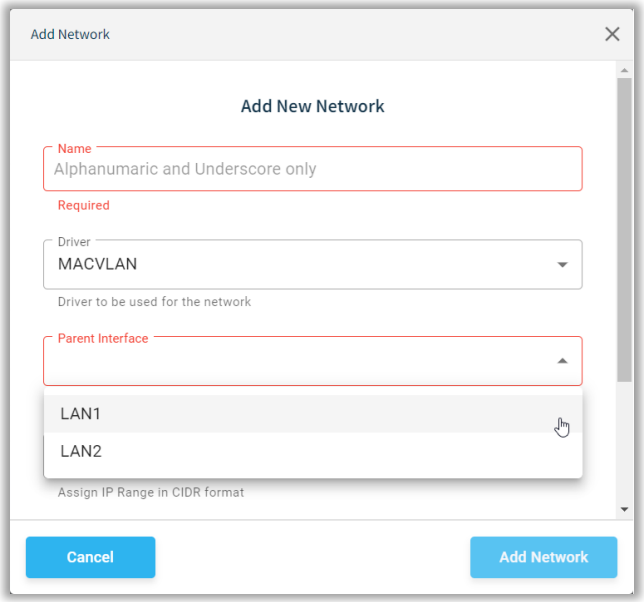


Note: The user can create a network name with an alphanumeric character with a minimum length of 2 and maximum length of 49.

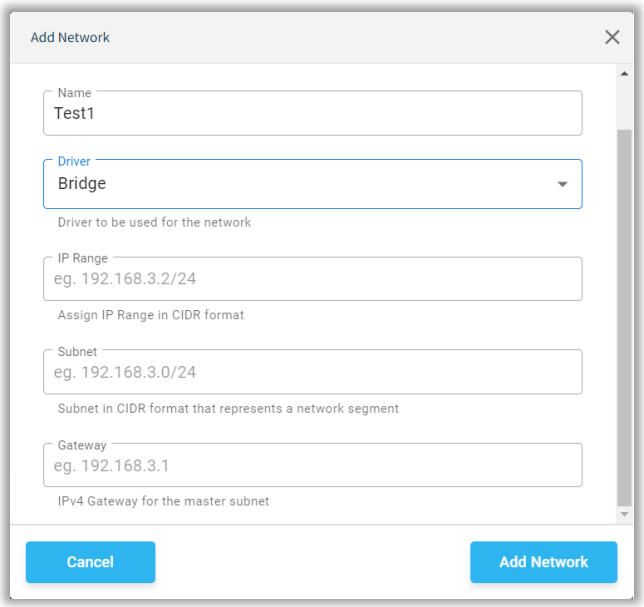
The following characters are allowed:
a to z
A to Z
0 to 9
Only Special character "_" is allowed in network name creation.

4 Select a *Driver* from the dropdown menu. **Bridge** or **MACVLAN**

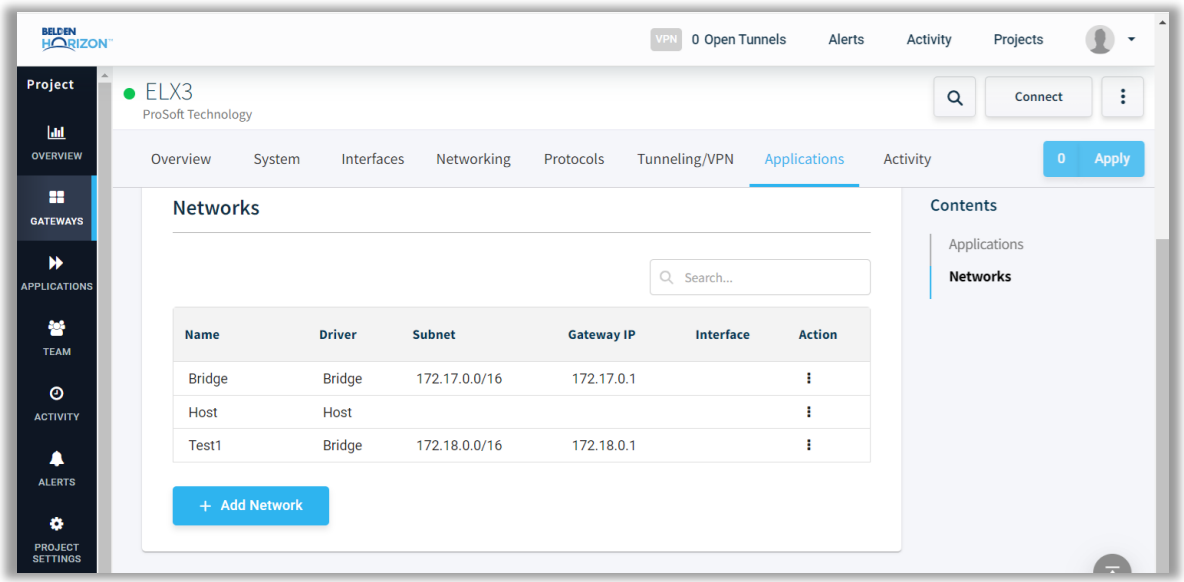
If **MACVLAN** is selected, the *Parent Interface* field is required. Select the **LANx** interface from the dropdown.



5 Assign the *IP Range* to the network in CIDR (Classless Inter Domain Routing) format.
6 Assign the IP range to the *Subnet* in CIDR format.
7 Assign the IP address for the *Gateway* to master subnet in IPv4 format.
8 Click the **ADD NETWORK** button.



9 Upon successful network creation, the network will display in the *Gateway* > *Applications* > *Networks* section.



Parameter	Description
Name	Name of the network.
Driver	The Driver selected from MACVLAN and bridge during network creation.
Subnet	IP range for the master subnet.
Gateway IP	IP address of the gateway associated with master subnet.
Interface	Interface (on host) to be used for MACVLAN network.
Action	Delete the network using this parameter.

5.1.2 Importing an Image

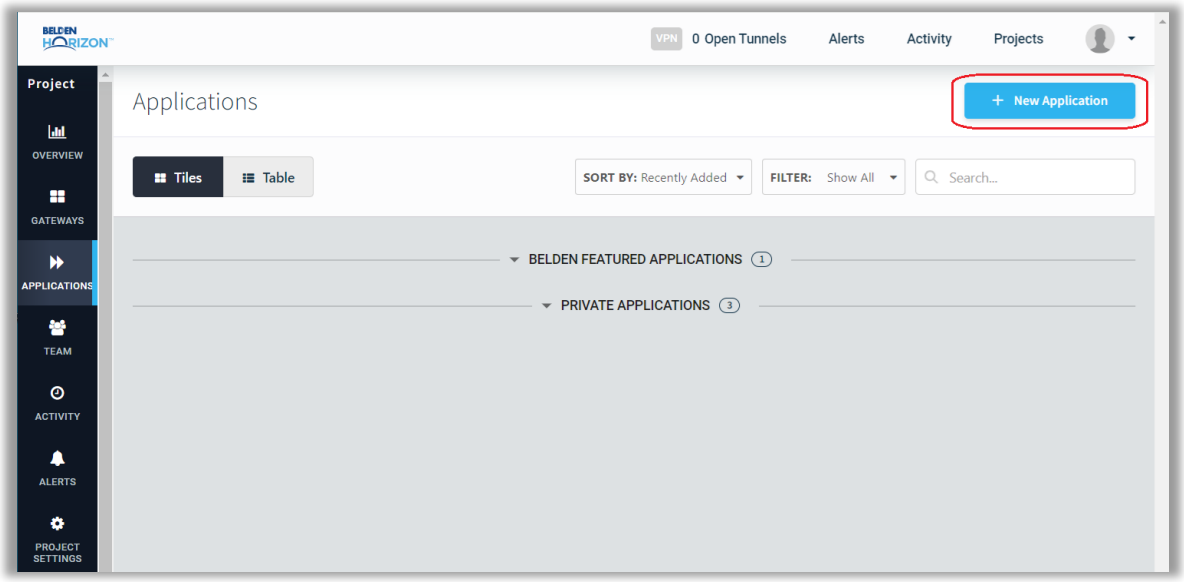
There are two ways to import a container image:

- URL
- Local File

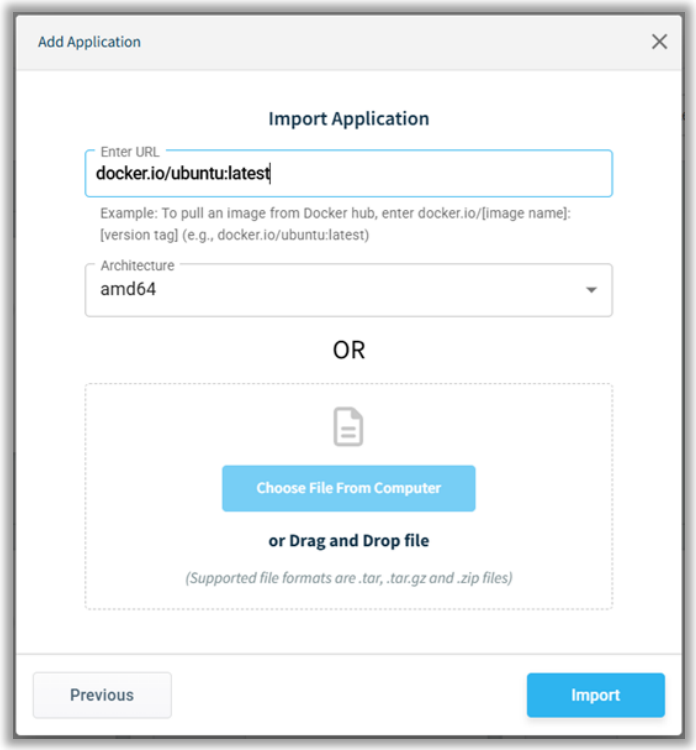
5.1.2.1 URL

Perform the following steps to import the image from a URL Source:

1. In the Belden Horizon Console, navigate to the *Applications* tab.
2. Click on the **NEW APPLICATION** button to open the *Import Application* wizard.



3 In the *Add Application* window, add the image from the docker hub by entering the URL and tag value in the *Enter URL* field: **docker.io/<image_name>:<tag >**

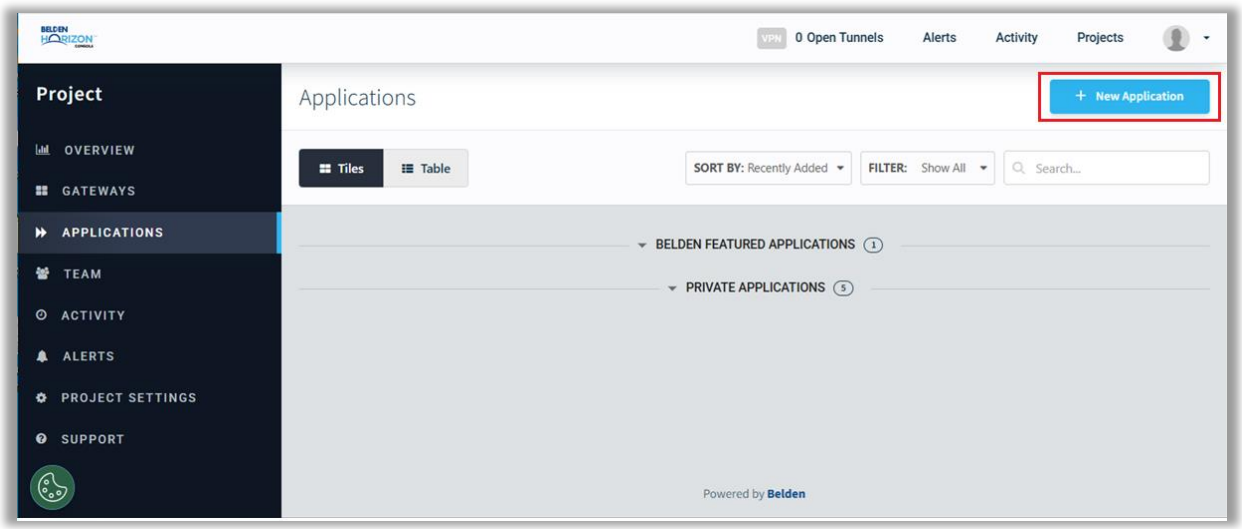


4 Click **IMPORT** to add image.

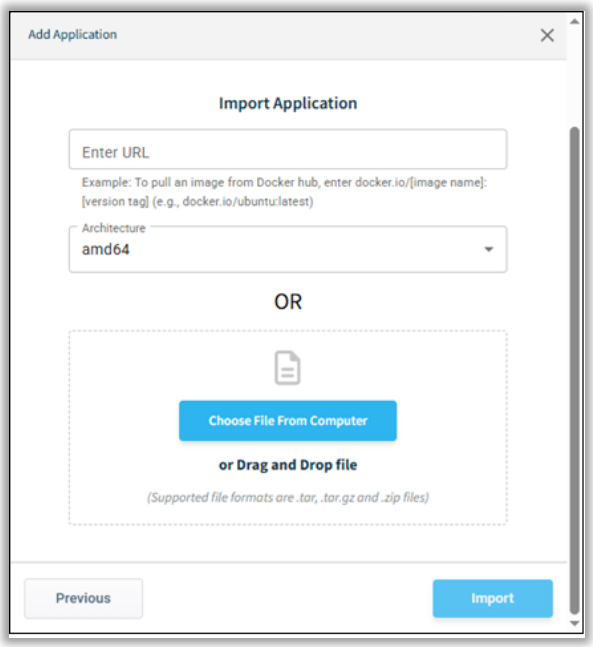
5.1.2.2 Local File

Perform the following steps to import the image from a local file:

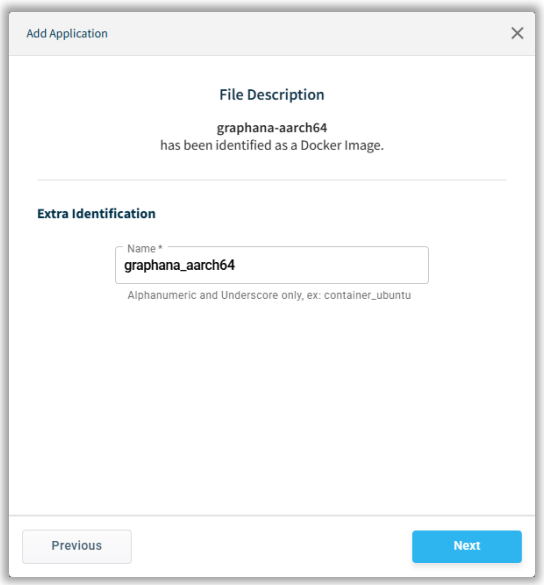
1. In the Belden Horizon Console, navigate to the *Applications* tab.
2. Click on the **NEW APPLICATION** button to open the *Import Application* wizard.



3. In the *Add Application* window, *Choose* or *Drag and Drop* the (**.tar** or **.tar.gz**) file. Click **IMPORT** to add image.



4 After the image file has been imported, enter the name of the container in the *Name* field. Click **NEXT**.



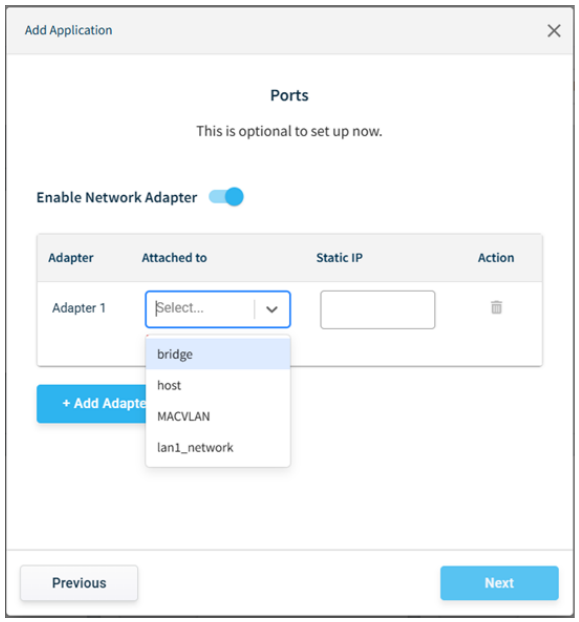
Note: The user can create a container name with an alphanumeric character with a minimum length of 1 and a maximum length of 49.

The following characters are allowed:
a to z
A to Z
0 to 9
Only Special character "_" is allowed for container name creation.

5 The **Ports** wizard contains the network configuration. Select an option for attaching the network adapter to the container in the *Attached to* parameter:

- Bridge
- Host
- User-created custom network (MACVLAN/Bridge)

The user can also enter the (optional) Static IP corresponding to the selected network in the *Static IP* field.



Note: The user must first create the custom network to be able to create a container using that network. Detailed information regarding the creation of a custom network can be found in section *5.1.1.1 Adding a Network to Gateway*.

Note: A maximum of four network adapters can be added.

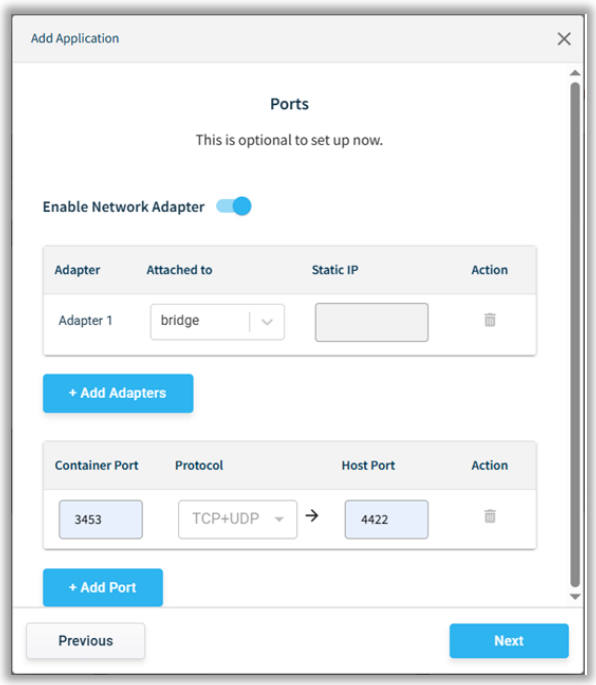
a) For *Bridge* networks, the container and host ports must be configured.

i. In the *Container Port* field, enter the container port number.

ii. In the *Host Port* field, enter the host port number.

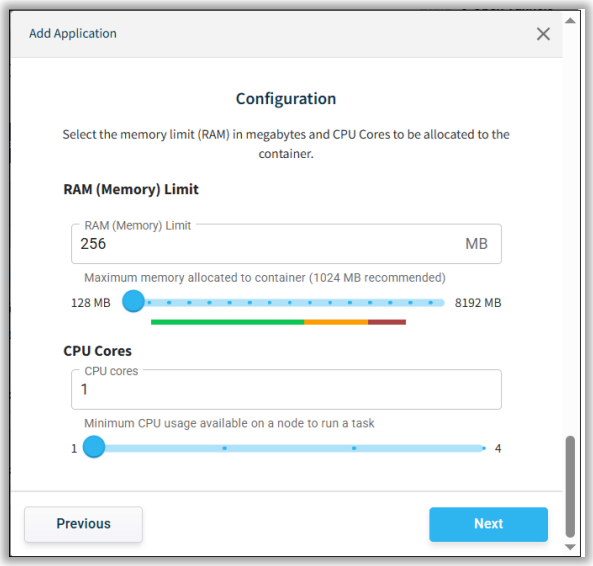
Note: A maximum of four Container and Host ports can be added.

The user is not allowed to create a container without a Container port and Host port in **Bridge** mode. A minimum of one Docker and Host port is required to create a container with a Bridge network.



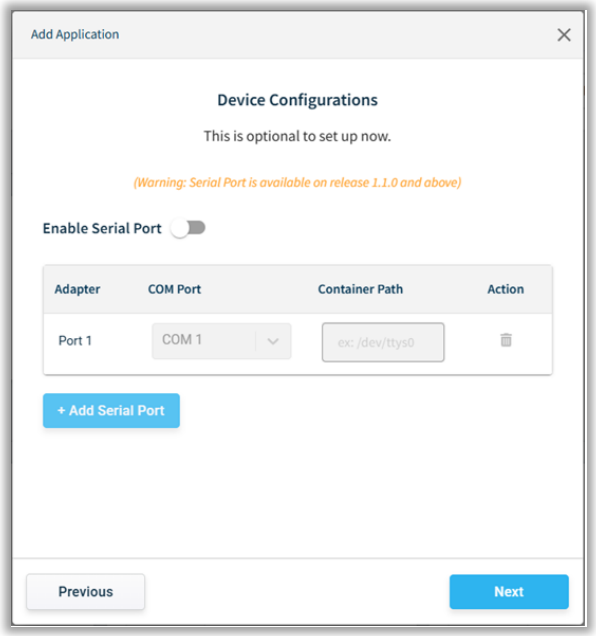
Click **NEXT**.

6 The **Memory & CPU** configuration defines the memory and CPU. Click **NEXT**.



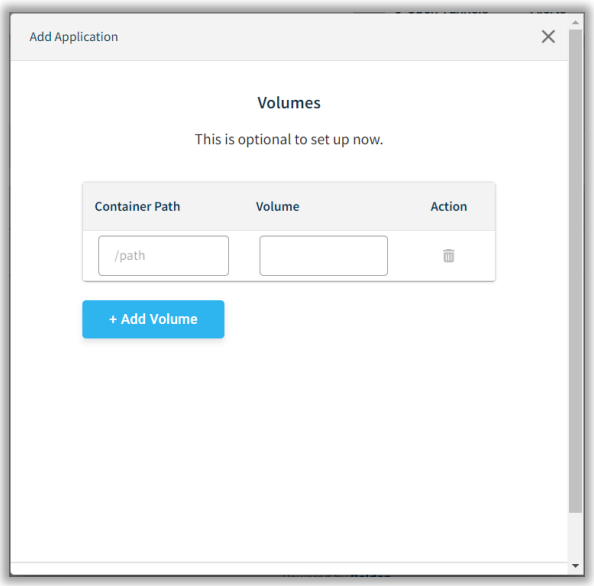
- In the *RAM (Memory) Limit* field, enter the size of memory (MB) for the container. The minimum memory value for creating containers is 4MB.
- In the *CPU Cores* field, enter the number of CPU cores to be used by the container. The number of processors is expressed in number of physical CPU cores.

7 The **Device Configurations** configuration defines the COM1 serial port for access to the ELX3 Command Line Interface (CLI) to check the assigned IP addresses of the ELX3 LAN Interfaces, set an IP address, reboot, and factory reset. Click **NEXT**.

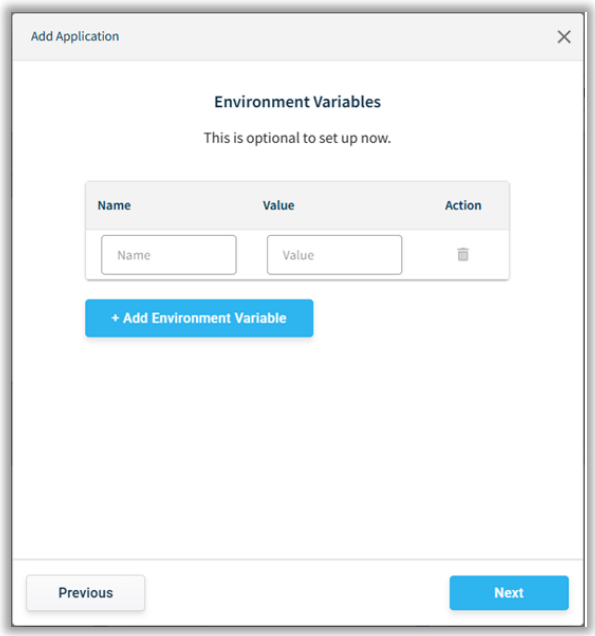


8 (Optional) In the **Volumes** configuration, enter the *Container Path* and select the *Volume* from an existing list to attach to the container. Click **NEXT**.

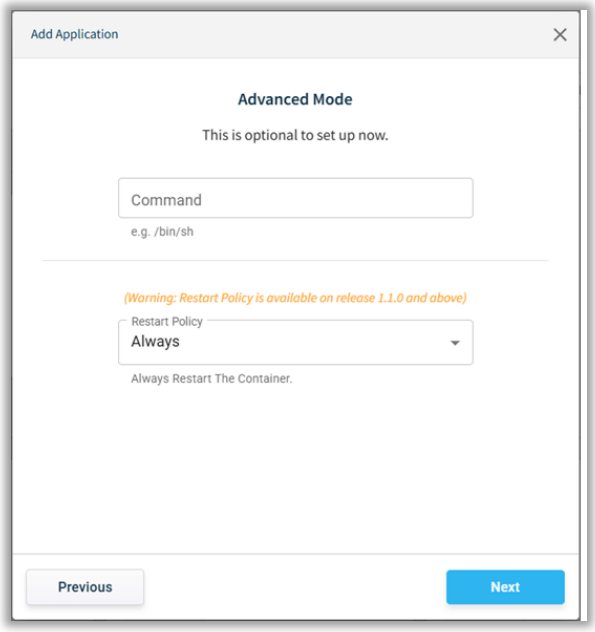
Note: Refer to section *5.2.2.1 Adding a Storage Volume (optional)* to add a new volume when there is no volume available to attach to the container.



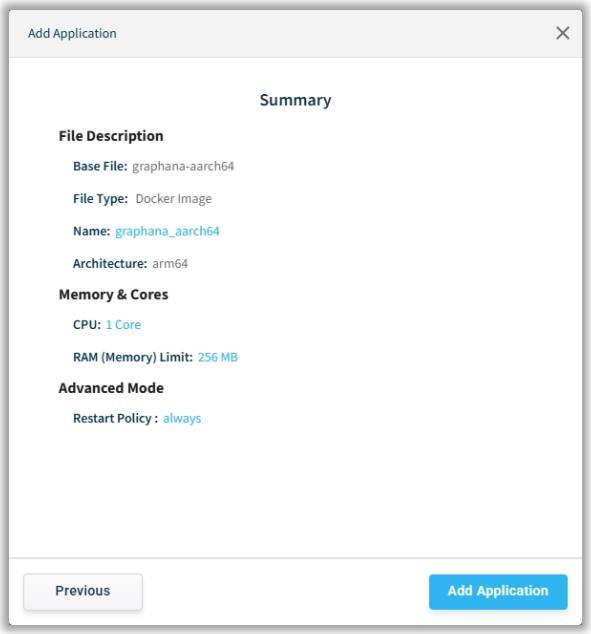
9 (Optional) In the **Environment Variables** configuration, enter the *Name* and *Value* of the environment variable. Click **NEXT**.



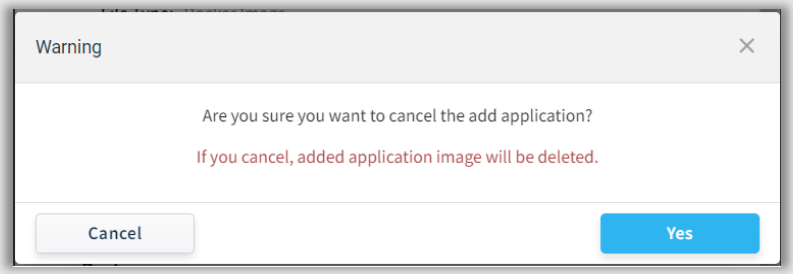
10 (Optional) In the **Advanced Mode** configuration, enter the advanced Docker commands that are supported by the specific Docker image. Click **NEXT**.



11 In the **Summary** dialog, check all details and click **ADD APPLICATION** to create the container. If edits are needed before creating the container, click the **PREVIOUS** button.



Note: Clicking the "X" button on the top-right corner of the dialog at any step during container configuration will display the following:



When clicking the **CANCEL UPLOAD** button, the container creation will be stopped and the image will be stored under the *Images* tab. It must be manually deleted.

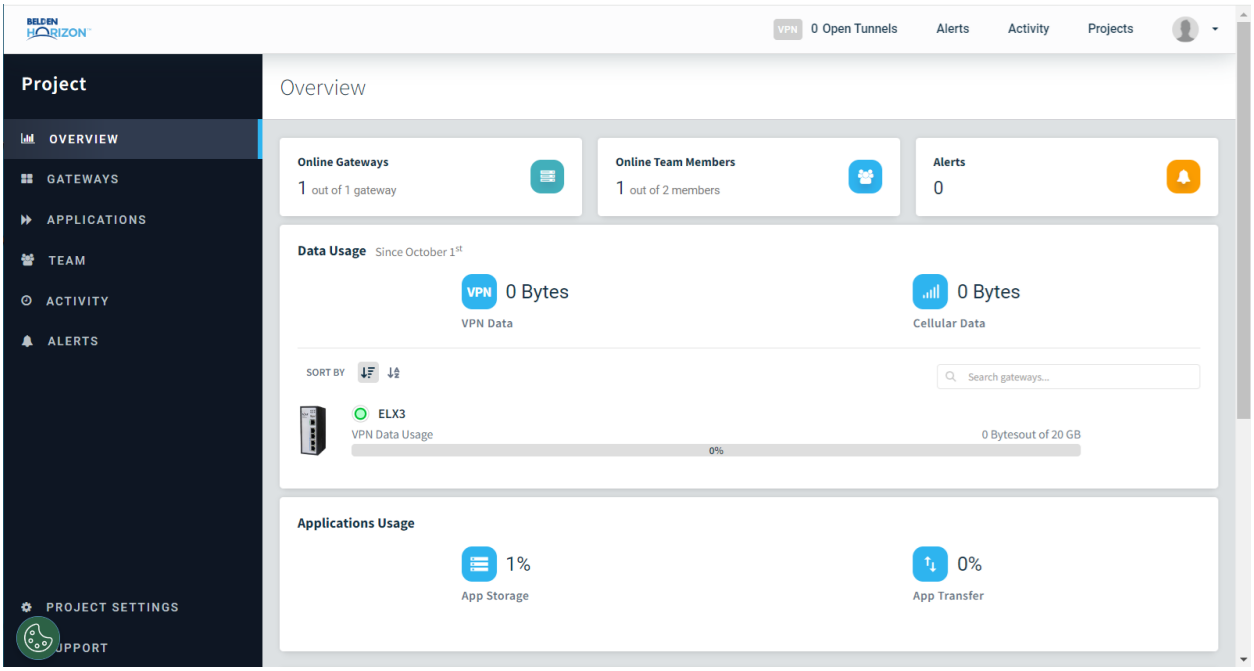
5.1.3 Deploying Container

5.1.3.1 Deploy to Gateway

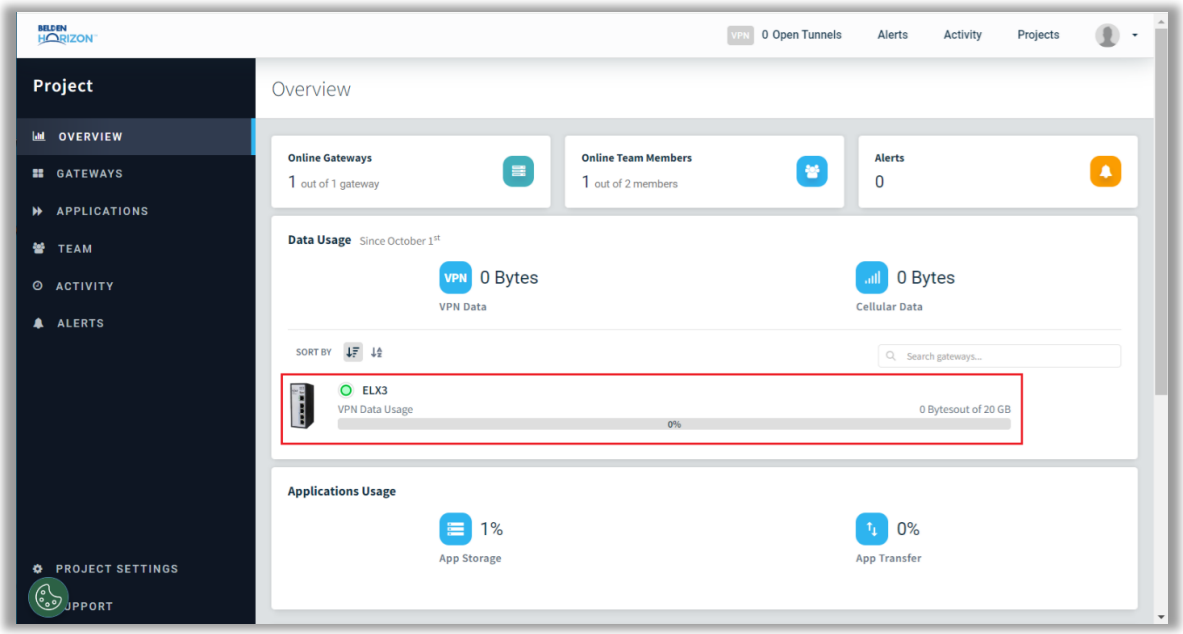
This section covers the deployment of the Container from Belden Horizon Console.

Note: Belden Featured Applications are Belden approved containers. Private Applications are containers manually uploaded by user.

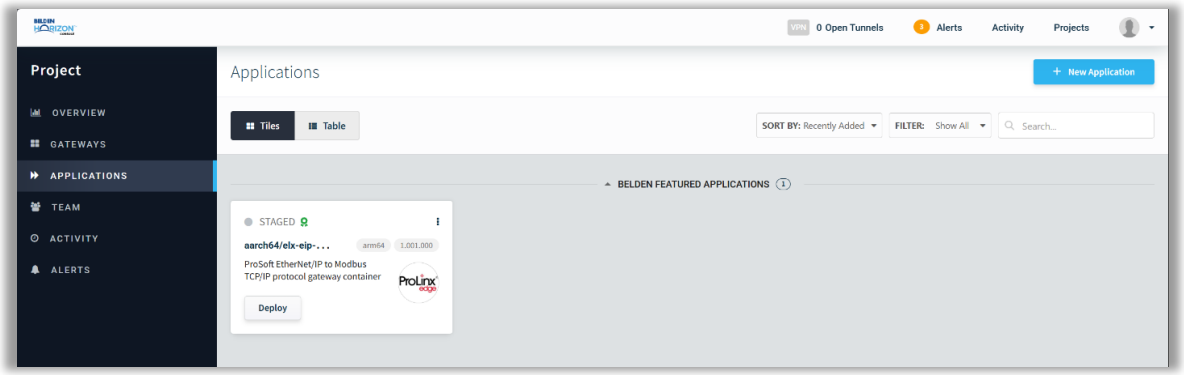
The ELX3 gateway must be activated within its Belden Horizon Console project. An activated device is indicated by a green dot next to the device graphic, as shown below.



1 Click on the device to open the device *Overview*.

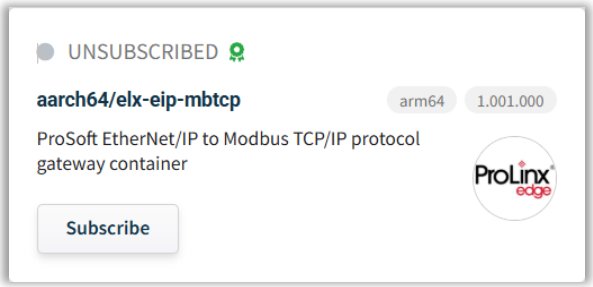


2 Click on the *Applications* tab, then navigate to the Container Application.

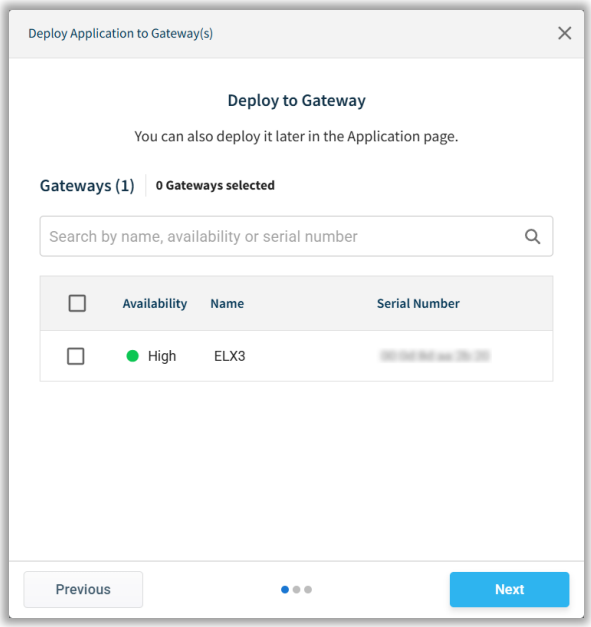


3 In the Container Application tile, click **DEPLOY**.

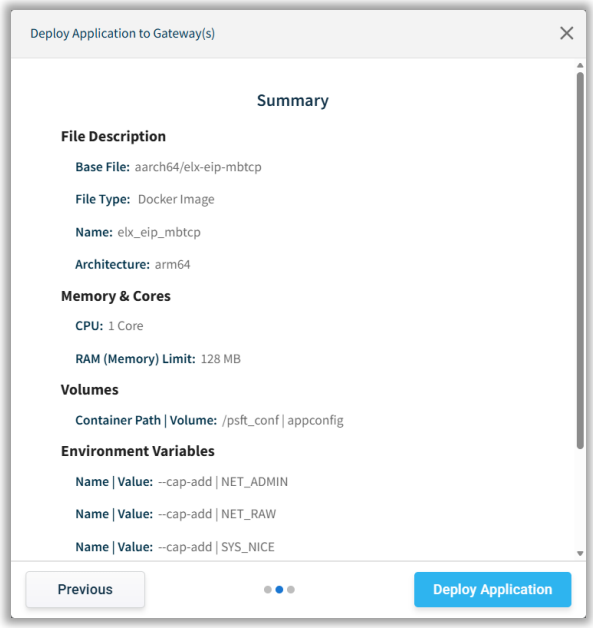
For Belden Featured applications, click the **SUBSCRIBE** button and accept the *End User License Agreement*. Then click **DEPLOY**.



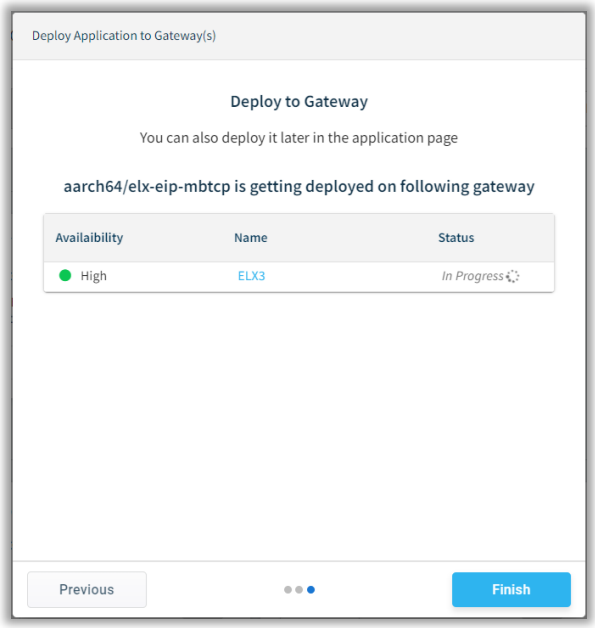
4 In the *Deploy Application to Gateway(s)* dialog, select the ELX3 gateway and click **NEXT**.



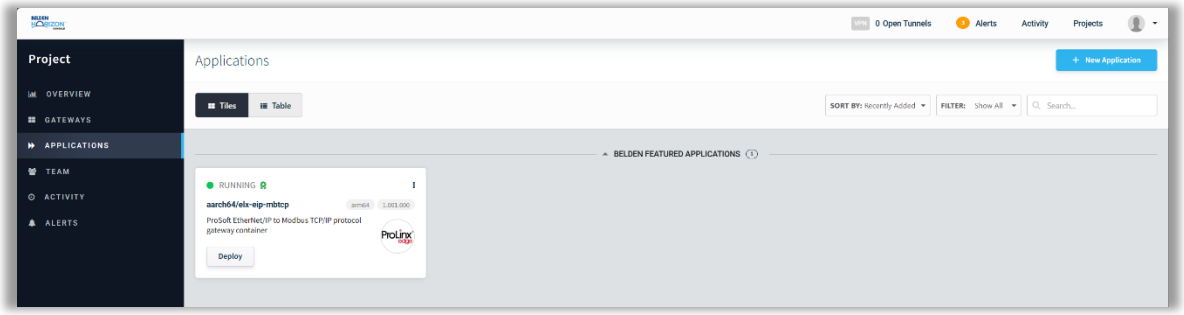
5 Review the configuration information as needed in the **Summary** dialog. Click **DEPLOY APPLICATION**.



6 The *In Progress* status is displayed and completes the deployment process. Click **FINISH**.

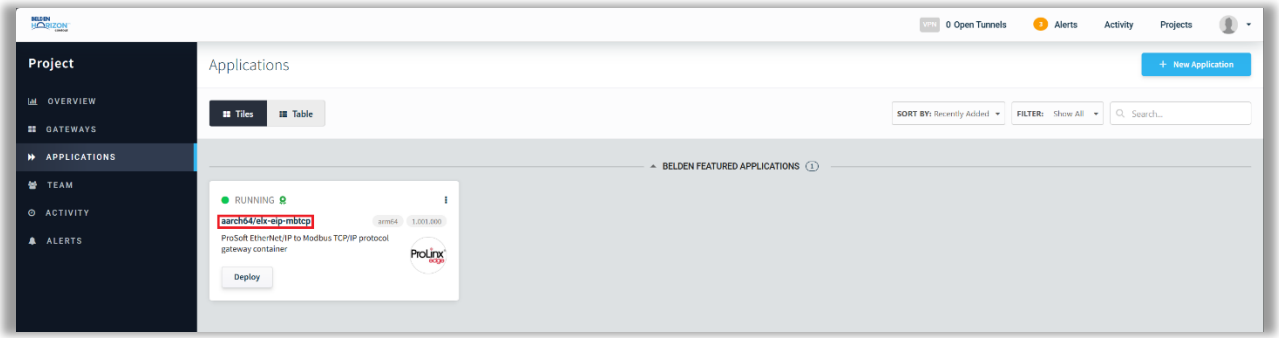


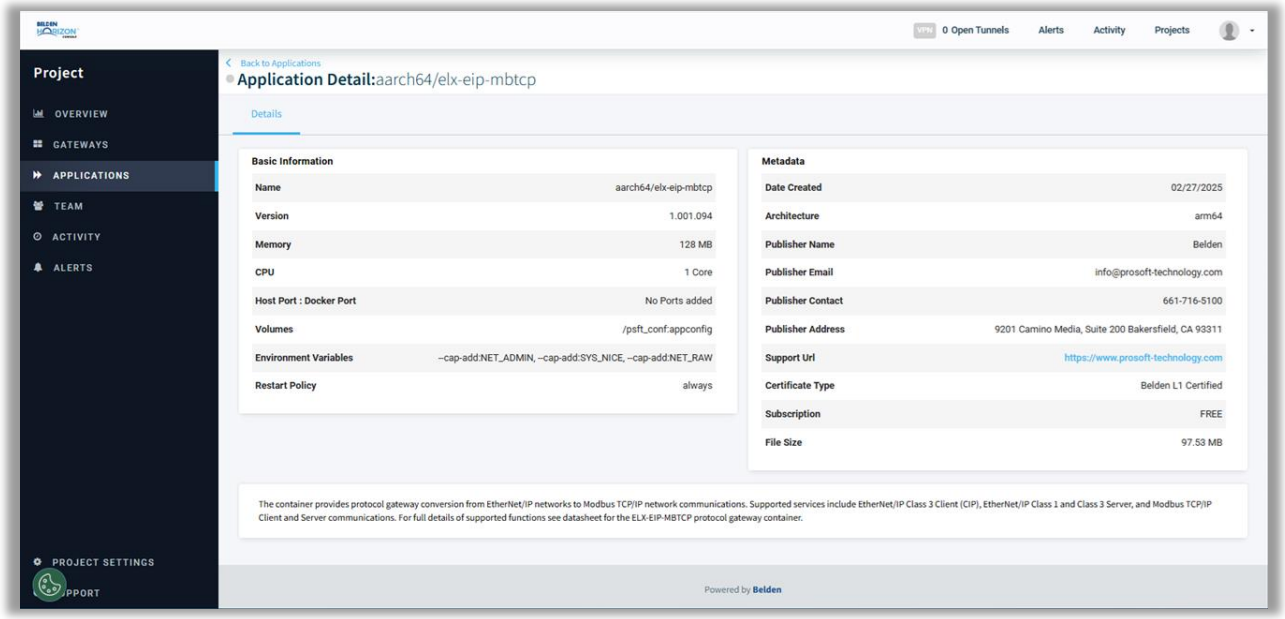
7 In the *Applications* tab, the application will indicate it is running.



5.1.4 Accessing Application Details

The configuration of an application can be edited by clicking on the Application name in the tile.





5.2 Local User Interface

5.2.1 Container Network Configuration

An ELX3 gateway container network must be configured before deploying the container.

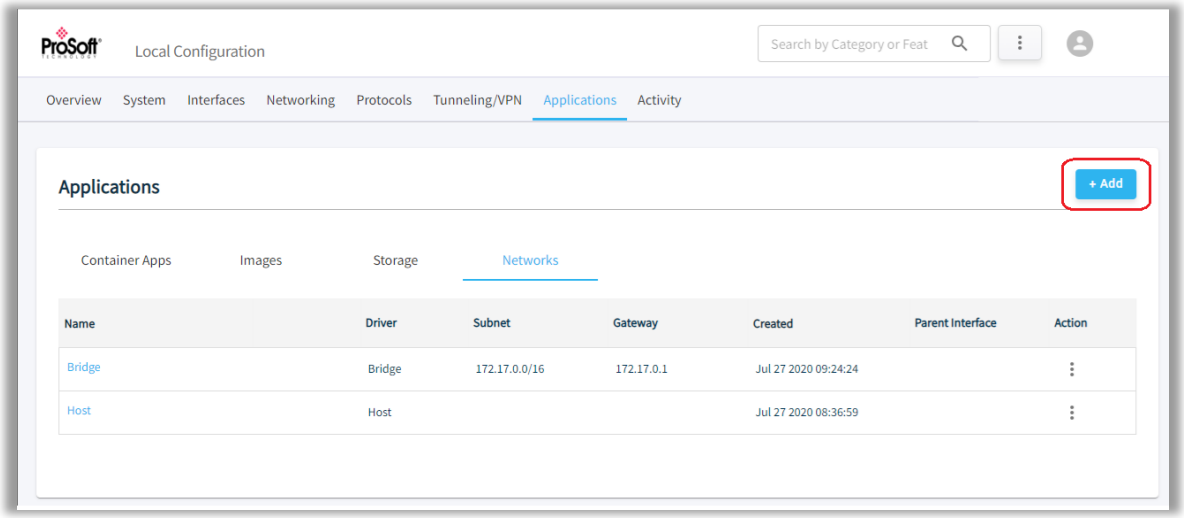
A network is the functionality that allows a container to communicate to external devices by using the host's configured LANs. This section concentrates specifically on the virtual network between containers also known as Docker networks.

A Docker network is a powerful feature that enables containers to communicate with each other and the outside world. It provides isolated and secure networking environments, allowing seamless connectivity and easy management of containerized applications.

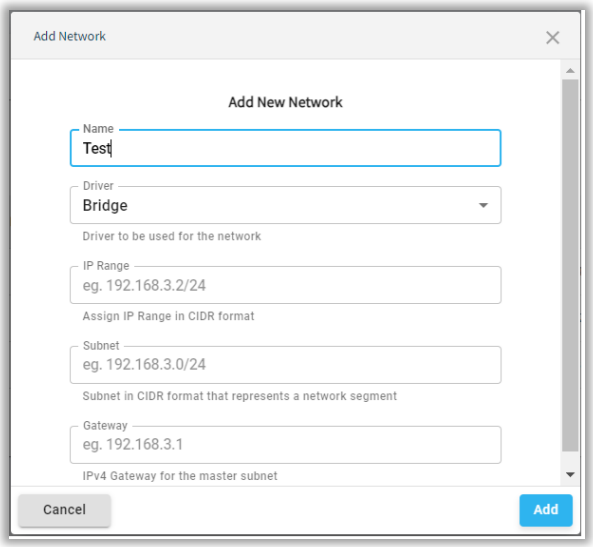
5.2.1.1 Adding a Network

Note: If the desired network subnets differ from the gateway's default network configuration, ensure the gateway's LAN interfaces are configured before continuing. For more information, please refer to section *4.5 Networking Tab*.

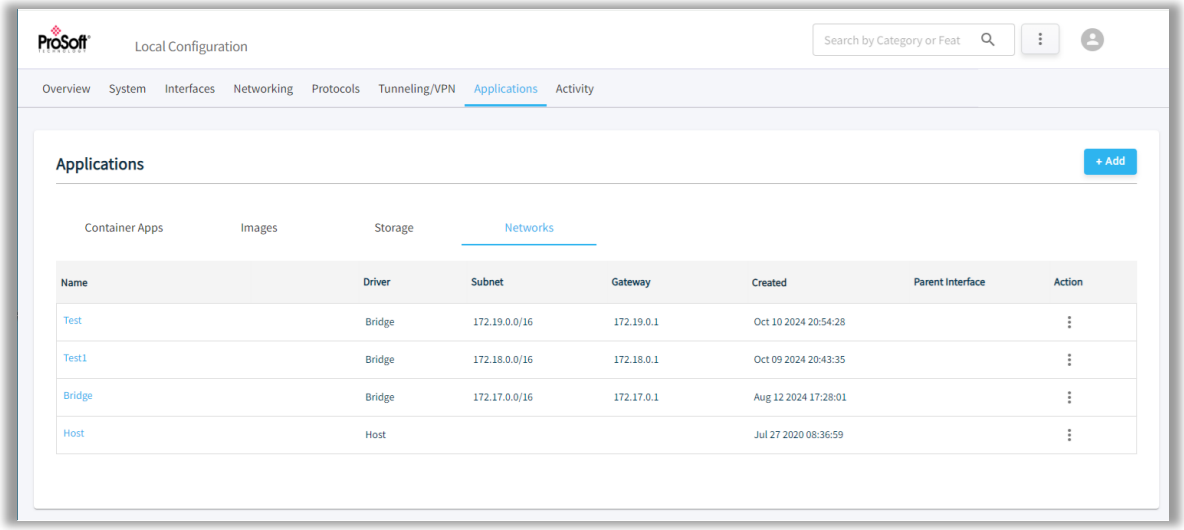
1 Go to the *Applications* tab > *Networks* tab and click the **ADD** button.



2 In the *Add Network* dialog, enter the network information then click the **ADD** button.



3 The new network will display in the refreshed *Networks* tab.

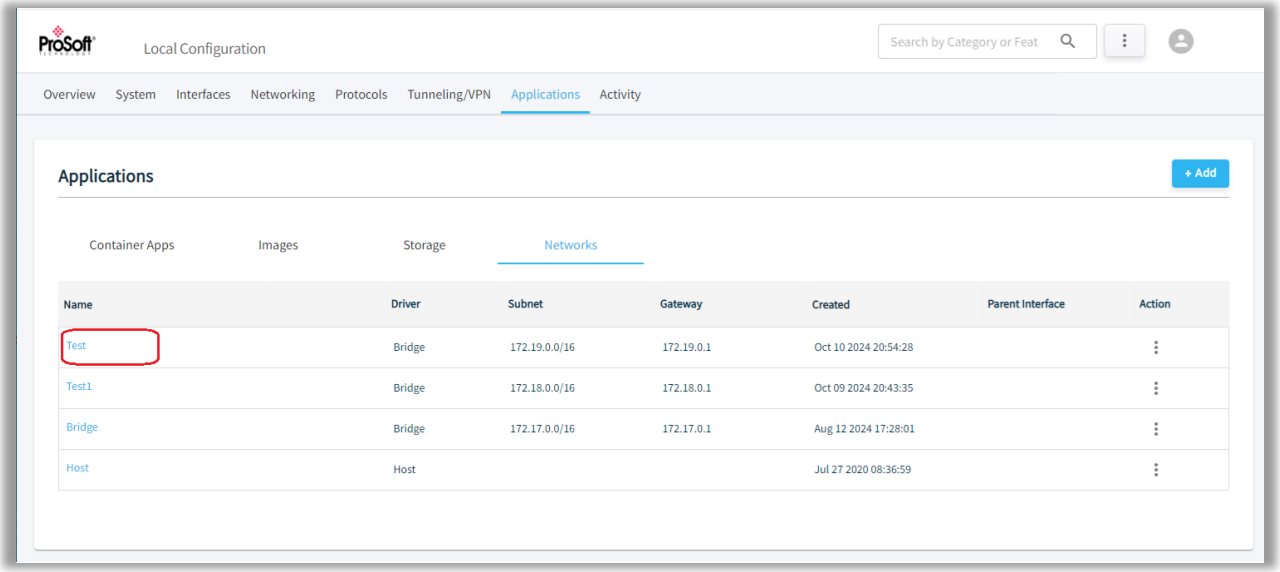


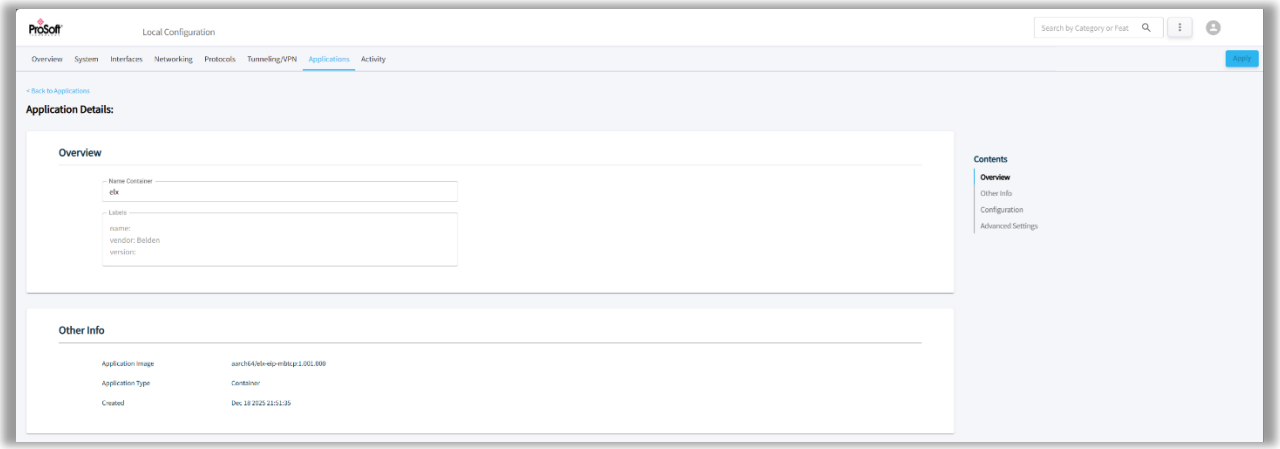
Note: The *Network* tab has two default networks - *Bridge* and *Host*. These two networks cannot be deleted.

Parameter	Description
Name	Name of the network. **Note:** Create a network name with an alphanumeric character with a minimum length of 2 and maximum length of 49. The following characters are allowed: a to z A to Z 0 to 9 Only Special character "_" is allowed in network name creation.
Driver	The Driver used for the network. Select **MACVLAN** or **Bridge**
Parent Interface	LAN port to be used for MACVLAN network. **Note:** MACVLAN network only
IP Range	IP address range for the master IP address in CIDR (Classless Inter Domain Routing) format.
Subnet	Subnet range for the master subnet in CIDR (Classless Inter Domain Routing) format.
Gateway	IP address of the gateway associated with master subnet in IPv4 format.
Created	Time stamp of network creation.
Action	Delete the network using this parameter.

5.2.1.2 Network Details

In the local UI, clicking on the network name opens the *Application Details* page.





Parameter		Description
Overview		
	Name Container	Name of the container application
	Labels	Assign a label to a container for organizing – Name, Vendor, Version
Other Info		
	Application Image	The file name of the application image.
	Application Type	Type of application - Container
	Created	Date of container creation.
Configuration		
	Memory & CPU Cores	
	RAM Allocation	The size of memory (MB) for the container.
	CPU Cores	The number of CPU cores to be used by the container. The number of processors is expressed in number of physical CPU cores.
Advanced Settings		
	Volume Mapping	
	Container	Path of directory to mount to a persistent data volume.
	Volume	Host storage volume created to provide persistent data storage to a container.
	Network	
	Network Name	Name of the virtual network created to provide the container with access to the host's local network.
	Driver	Network driver type used of the configured network.
	IP Address	IP Address assigned to the container.
	MAC Address	MAC address assigned to the container.
	Environment Variables	
	Name	Name of the environment variable.
	Value	Value of the environment variable.
	Advanced Mode	
	Advanced Mode	
	Restart Policy	
	Restart Policy	Behavior of restarting the container. **Always:** Always restarts the container. **No:** Do not restart the container. **Unless-Stopped:** Always restarts unless the container is stopped. **On-Failure:** Restart if the container exits due to an error.

5.2.2 Container Storage Configuration

A container volume allows data to persist, even when a container is deleted. Volumes are also a convenient way to share data between two or more containers.

Note: Volume size is dynamic and subject to host storage.

From the container, the volume acts like a folder to store and retrieve data. The volume can be mounted on the container directory.

Advantages of volume containers:

- A docker volume resides outside the container. Since the container resides on the host machine, the size remains the same after volume creation.
- The user can manage volumes using the ELX3 UI.
- Volumes work on Linux containers.
- Storing data within volumes allows different internal operations (e.g. redeploying a container with another tag version) to be performed without affecting or losing data.

Common uses cases for docker volumes:

- Providing persistent data volumes for use with containers.
- Sharing a defined data volume at different locations on different containers on the same container instance.

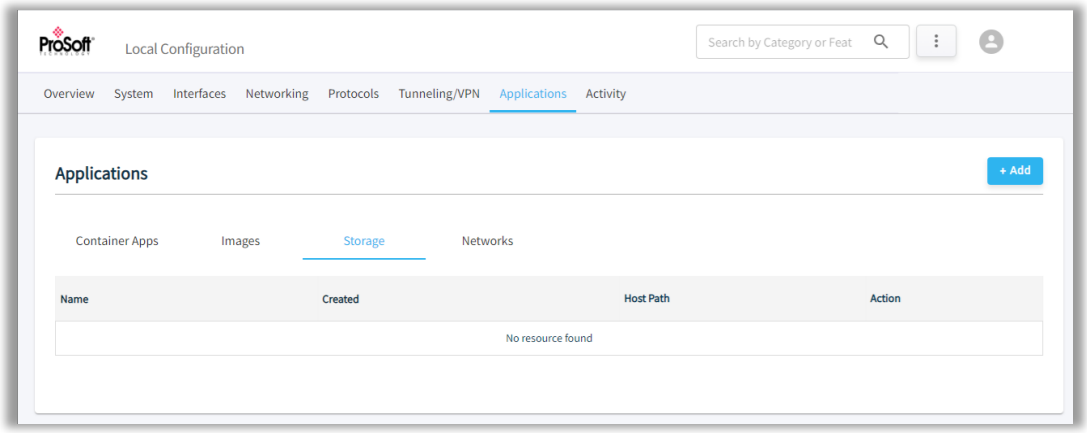
If a container is recreated due to a failure, a reboot, a new release, or any other reason, the volume data will not be lost.

For volume deletion, a scheduler will run every 5 minutes to check the consumed volume space when it exceeds 90% of the reserved space.

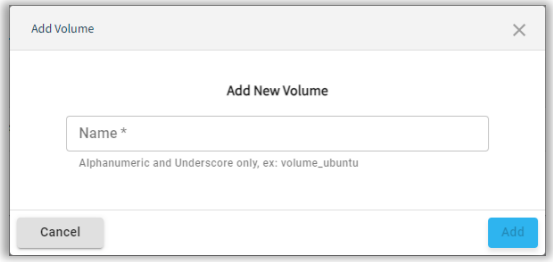
5.2.2.1 Adding a Storage Volume (optional)

The storage volume acts as persistent storage for a container and may not be required. If more storage volumes are required, create additional volumes here.

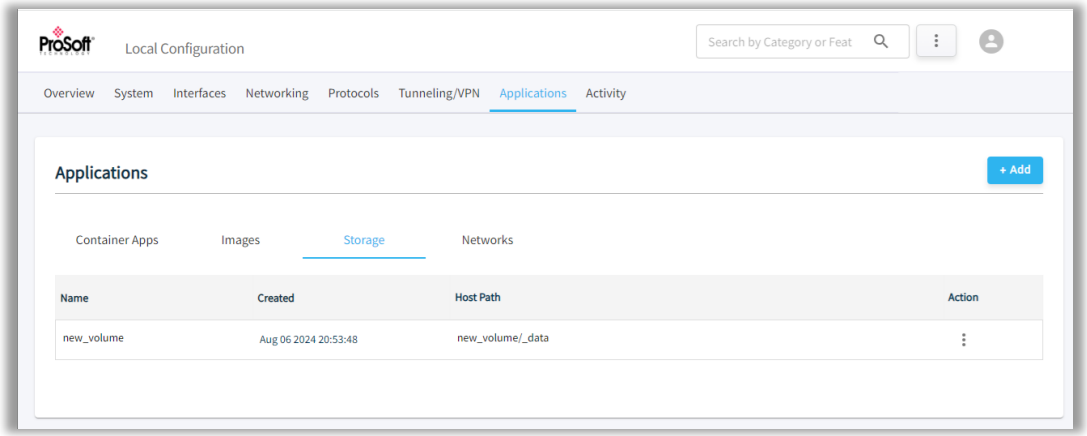
1 Navigate to the *Applications* tab > *Storage* tab and click on the **ADD** button.



2 Enter name of the volume in the *Name* field, then click **ADD**.



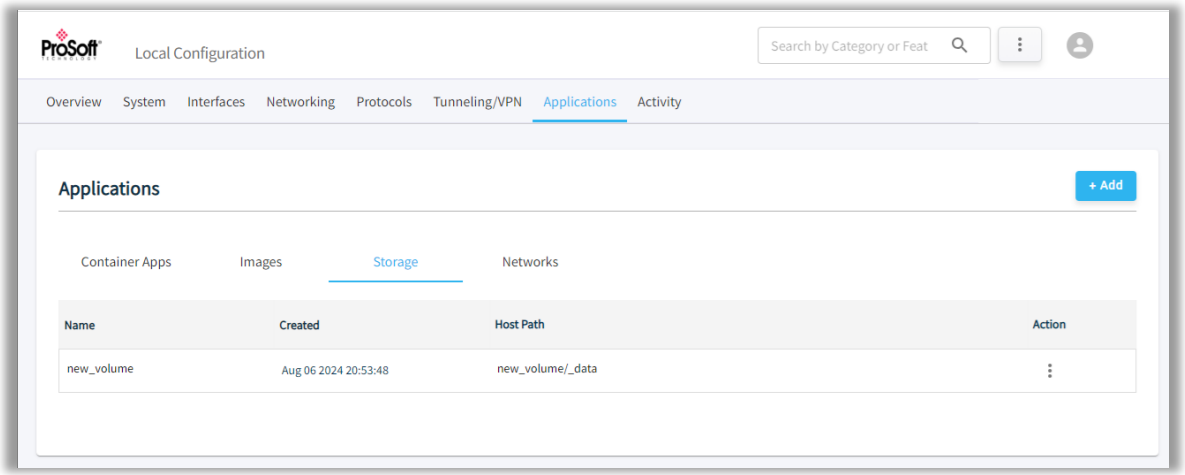
3 The list of *Volumes* is updated.



5.2.2.2 Deleting a Volume

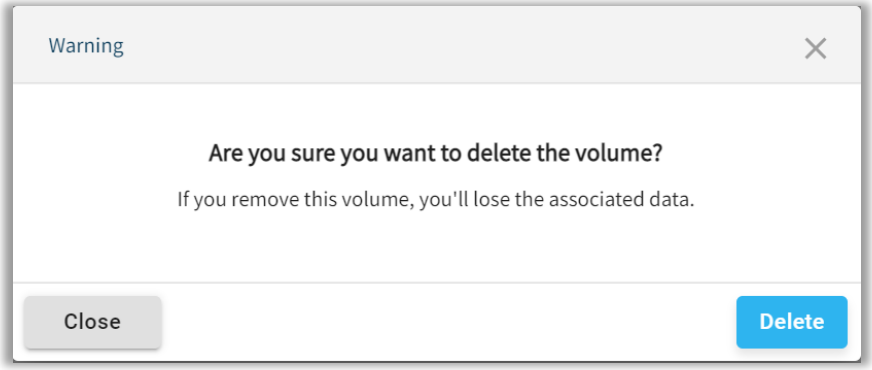
To delete a volume:

1 Click on the *Action* button  .



2 Click the **DELETE** option.

3 The user will be asked for confirmation.



4 Click **DELETE** to confirm.

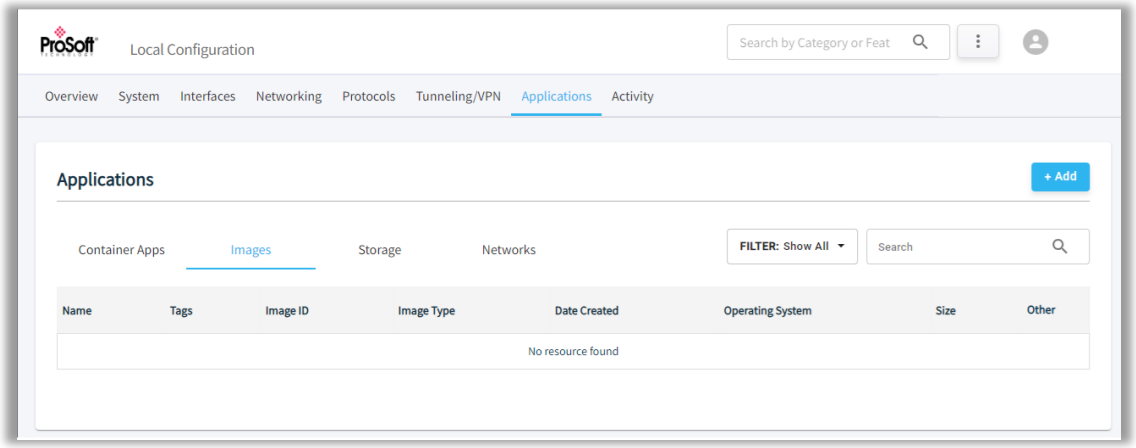
5.2.3 Deploying a Container

This section covers the deployment of the Container.

5.2.3.1 Loading the Image Only

Perform the following steps to import the docker image (.tar or .tar.gz) to the ELX3 environment.

1 Navigate to the *Applications* tab > *Images* tab.



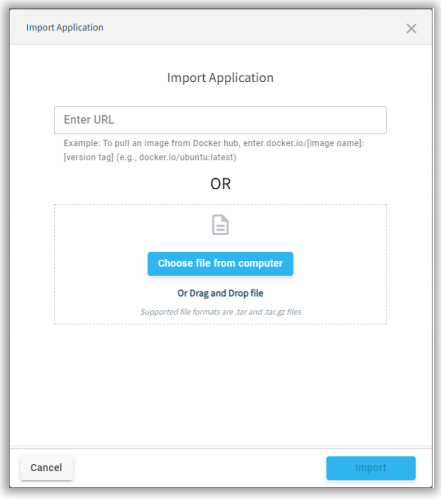
2 Click the **+ ADD** button to open the *Import Application* wizard.

3 There are two options to upload the image: By **URL** or **File**

a) **URL**

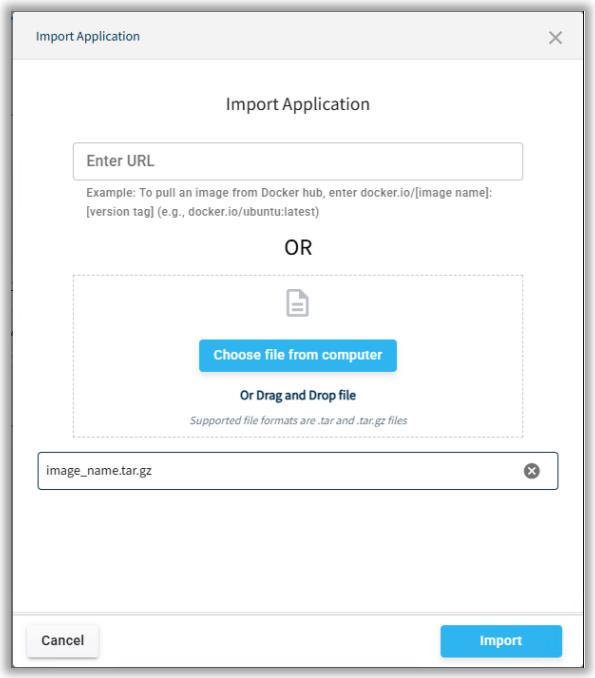
> **Note:** The ELX3 must have internet access to be able to request a docker.io application image.

In the *Import Application* window, enter the URL in the *Enter URL* field to add the image from the docker hub: **docker.io/<image_name>:<tag>**



b) **File**

In the *Import Application* window, click on **CHOOSE FILE FROM COMPUTER** and select the docker image from the local PC.

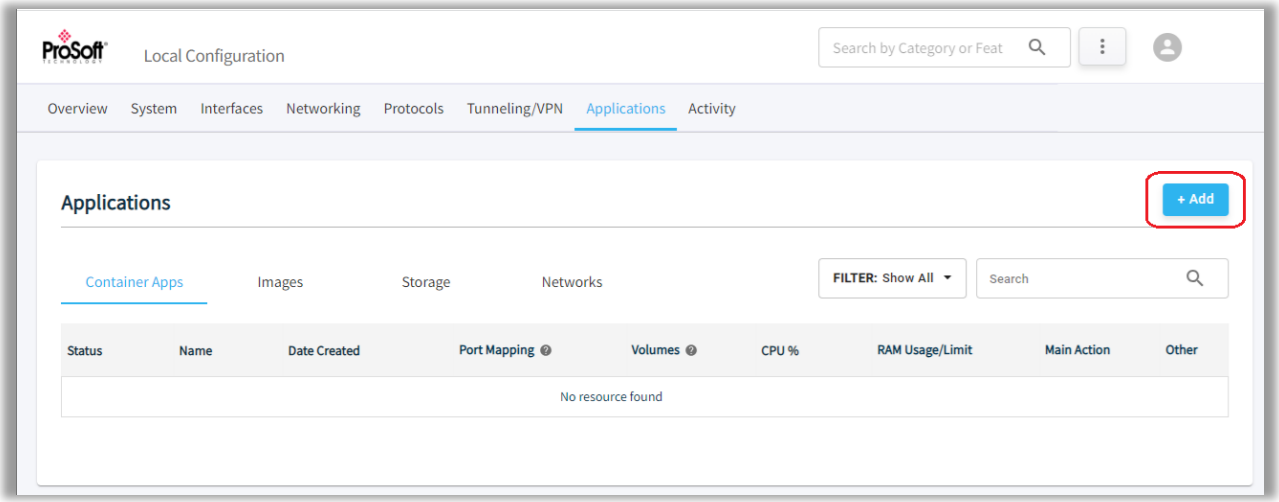


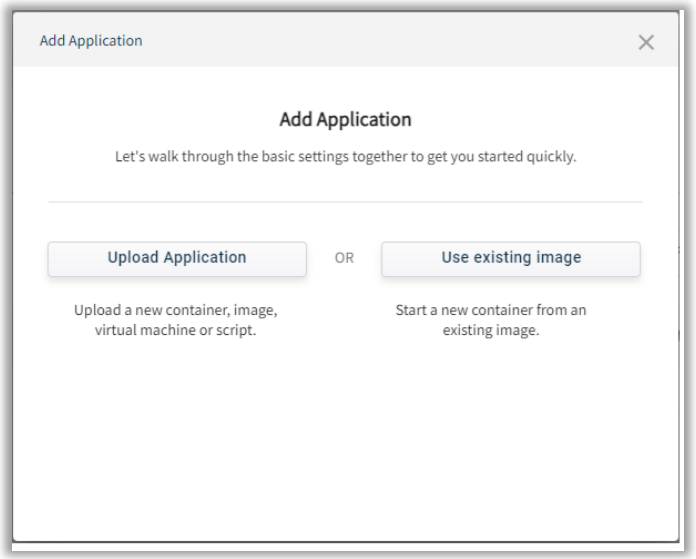
4 Click **IMPORT** to add image.

5.2.3.2 Deploying Container

There are two ways to deploy the Application to a target device. The Application can be uploaded or an existing container can be selected.

Navigate to the *Applications* tab > *Container Apps* tab and click the **ADD** button to open the *Add Application* wizard.

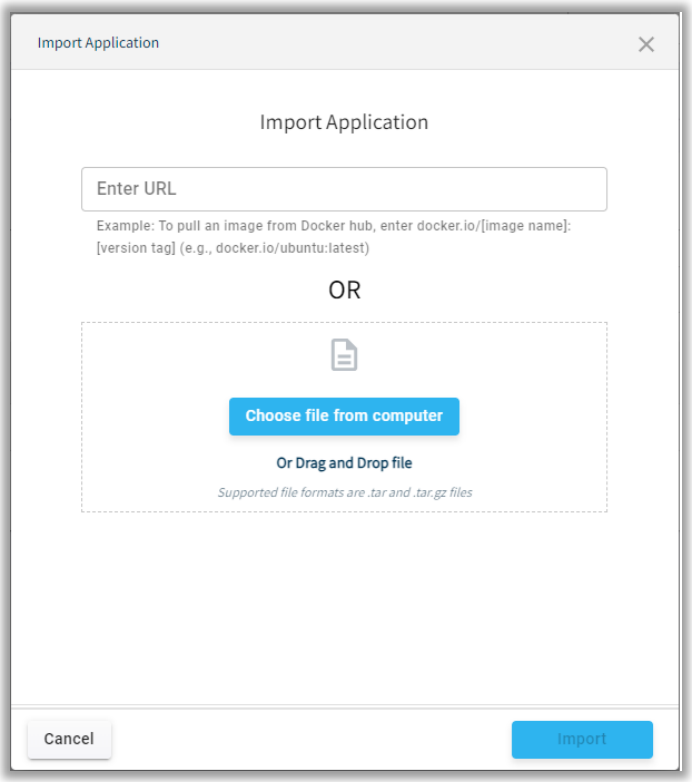




5.2.3.2.1 Upload Application

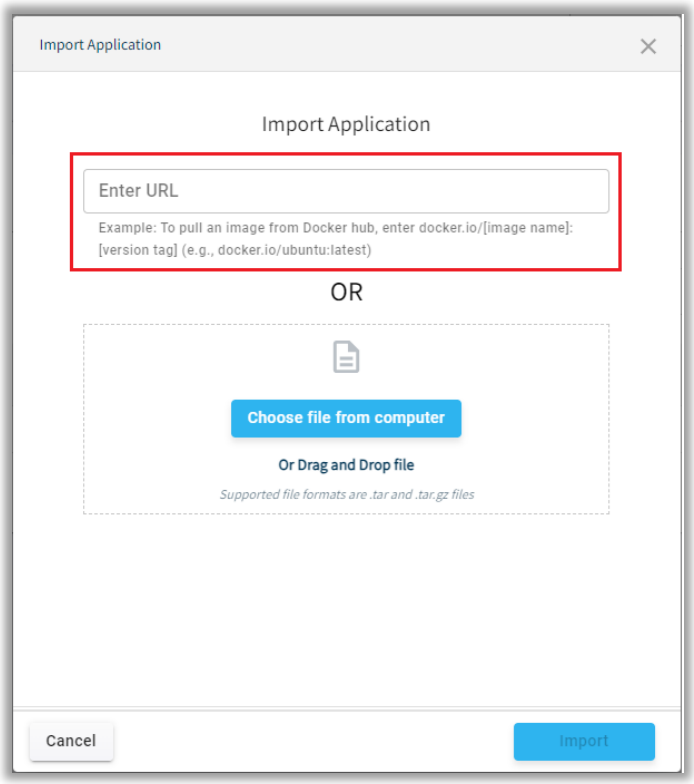
Click on the **UPLOAD APPLICATION** button to open the *Import Application* wizard.

The application can be imported by either entering a URL or selecting an existing file.



5.2.3.2.1.1 URL

1 Enter the URL in the *Enter URL* field to add the image from the docker hub.

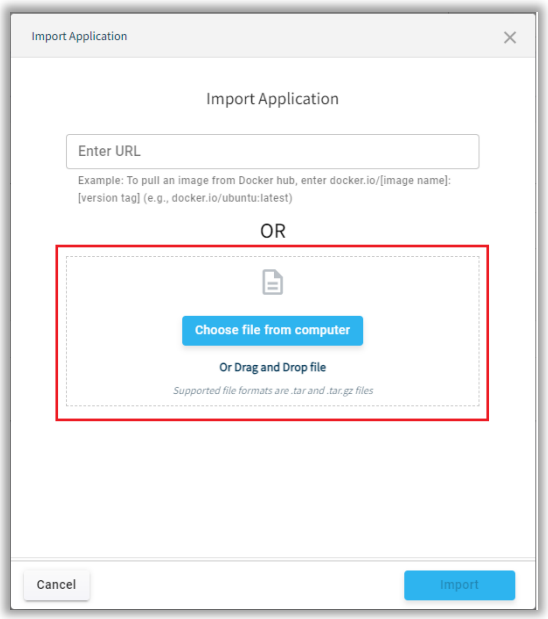


2 Enter the tag value along with the image name as: **docker.io/<image_name>:<tag>**

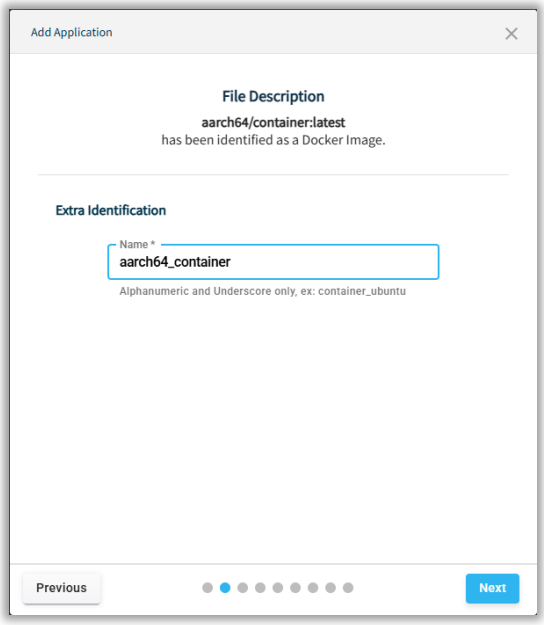
3 Click on the **IMPORT** button.

5.2.3.2.1.2 File

1 Select the **.tar** or **.tar.gz** file and click **IMPORT**.



2 After the image file has been successfully imported, enter a name of the container in the *Name* field. Click **NEXT**.



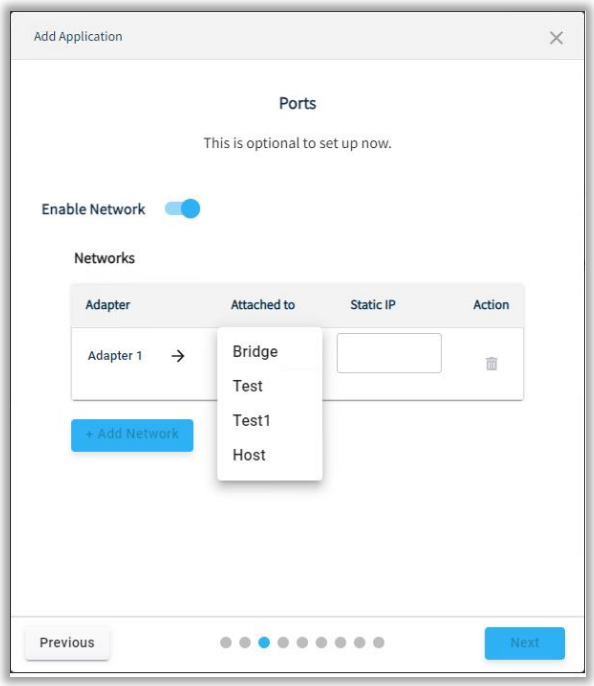
Note: The user can create a container name with an alphanumeric character with a minimum length of 1 and a maximum length of 49.

The following characters are allowed:
a to z
A to Z
0 to 9
Only Special character "_" is allowed for container name creation.

3 The **Ports** configuration defines the network configuration. Select an option for attaching the network adapter to the container in the *Attached to* parameter and click **NEXT**.

- Bridge
- Host
- User-created custom network (MACVLAN/Bridge)

The user can also enter the (optional) Static IP corresponding to the selected network in the *Static IP* field.



Note: The user must first create the custom network to be able to create a container using that network. Detailed information regarding the creation of a custom network can be found in section *5.1.1.1 Adding a Network to Gateway*.

Note: A maximum of four network adapters can be added.

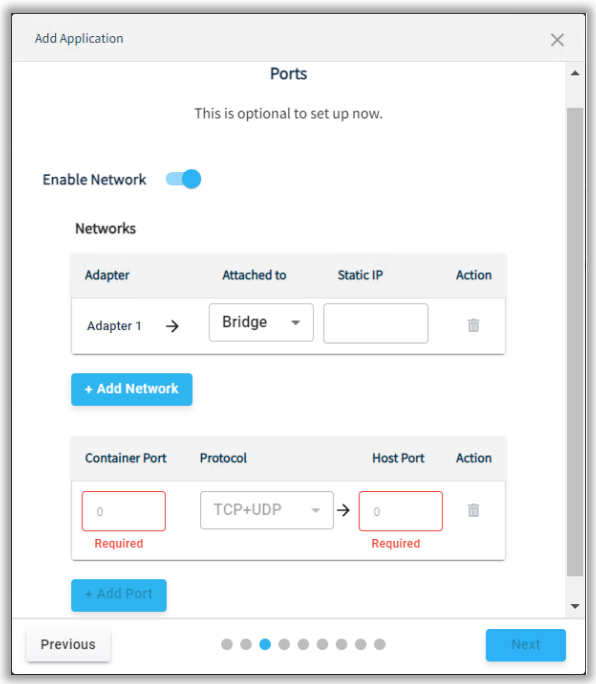
a) For *Bridge* networks, the container and host ports must be configured.

i. In the *Container Port* field, enter the container port number.

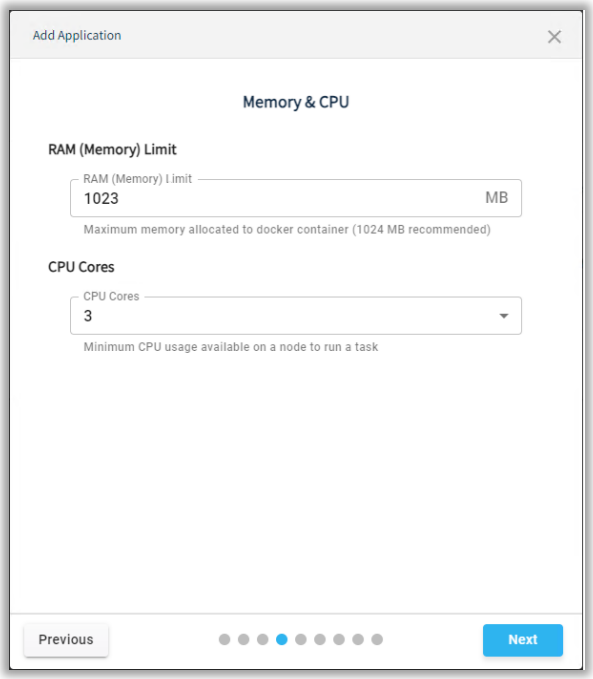
ii. In the *Host Port* field, enter the host port number.

Note: A maximum of four Container and Host ports can be added.

The user is not allowed to create a container without a Container port and Host port in **Bridge** mode. A minimum of one Docker and Host port is required to create a container with a Bridge network.



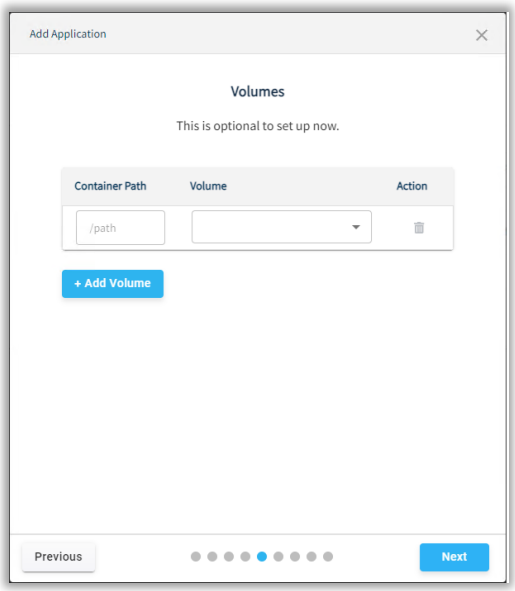
4 The **Memory & CPU** configuration defines the memory and CPU. Click **NEXT**.



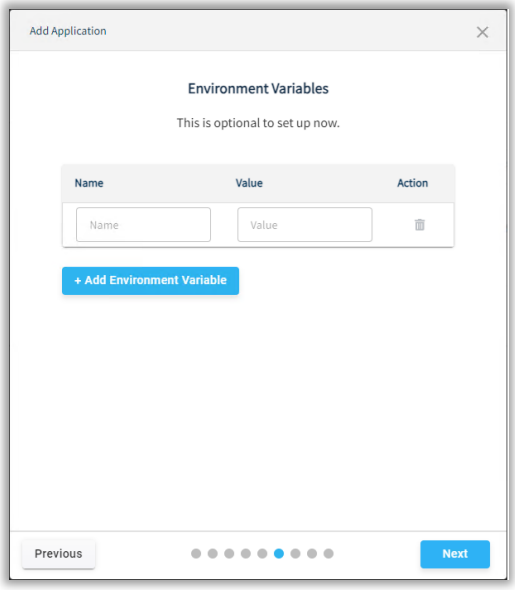
- In the *RAM (Memory) Limit* field, enter the size of memory (MB) for the container. The minimum memory value for creating containers is 4MB.
- In the *CPU Cores* field, enter the number of CPU cores to be used by the container. The number of processors is expressed in number of physical CPU cores.

5 (Optional) In the **Volumes** configuration, enter the *Container Path* and select the *Volume* from an existing list to attach to the container. Click **NEXT**.

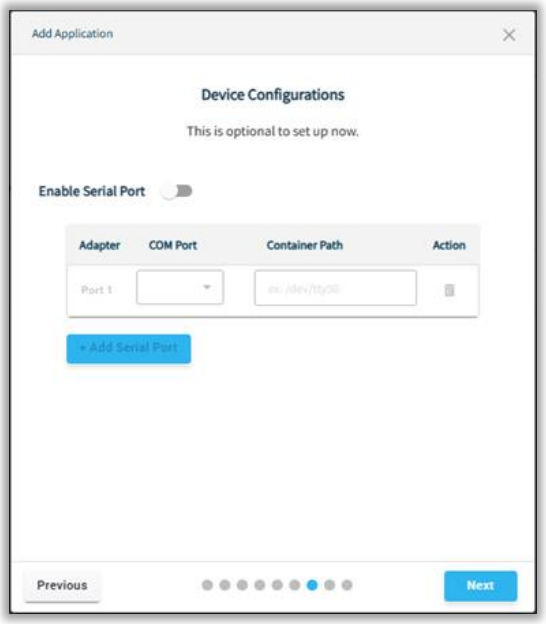
Note: Refer to section *5.2.2.1 Adding a Storage Volume (optional)* to add a new volume when there is no volume available to attach to the container.



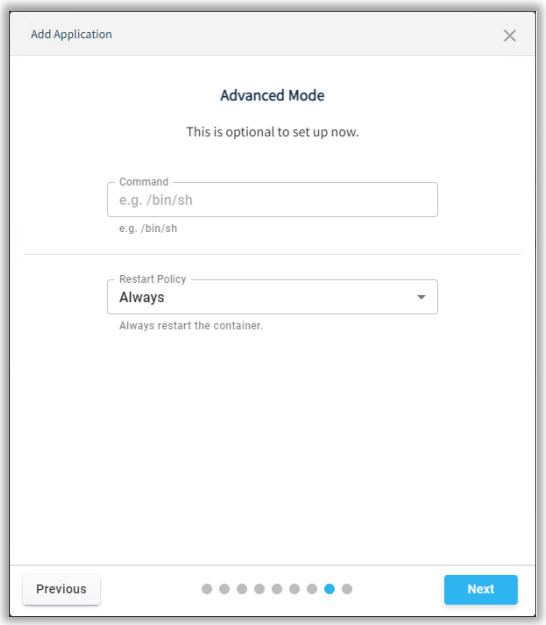
6 (Optional) In the **Environment Variables** configuration, enter the *Name* and *Value* of the environment variable. Click **NEXT**.



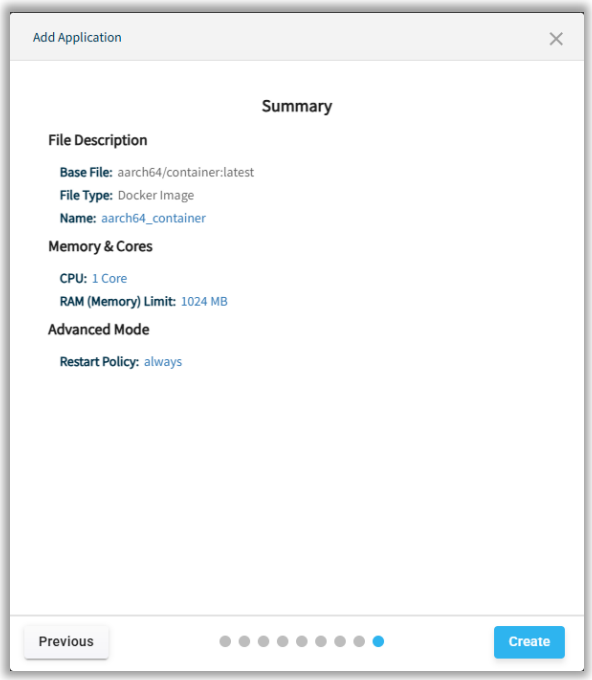
7 (Optional) In the **Device Configurations** configuration, enter the serial port settings. Click **NEXT**.



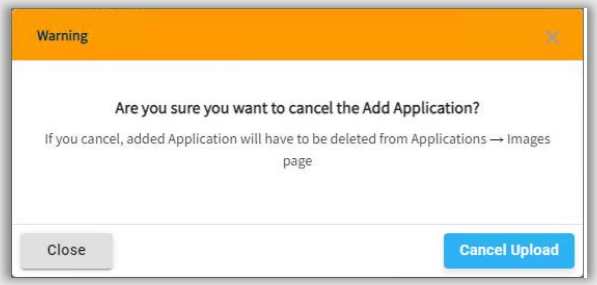
8 (Optional) In the **Advanced Mode** configuration, enter the advanced container *Command* and *Restart Policy*. Click **NEXT**.



9 In the **Summary** dialog, check all details and click **ADD APPLICATION** to create the container. If edits are needed before creating the container, click the **PREVIOUS** button.



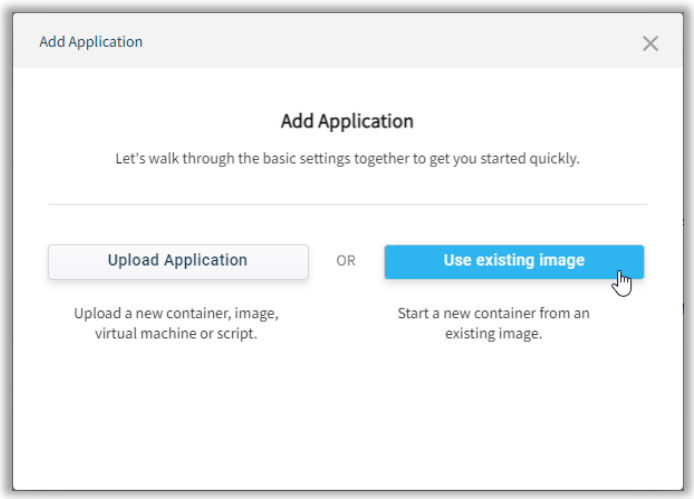
Note: Clicking the "X" button on the top-right corner of the dialog at any step during container configuration will display the following:



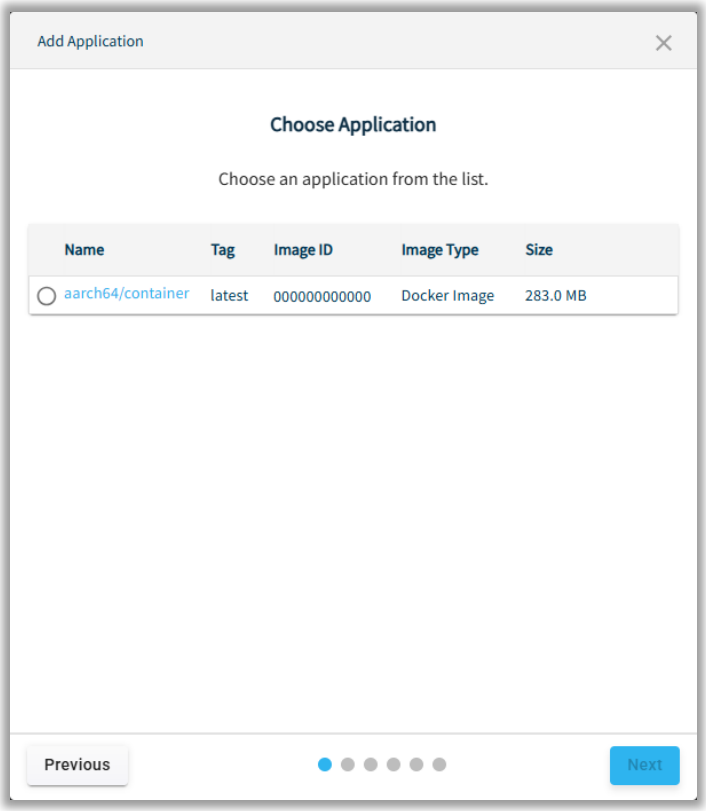
When clicking the **CANCEL UPLOAD** button, the container creation will be stopped and the image will be stored under the *Images* tab. It must be manually deleted.

5.2.3.2.2 Use Existing Image

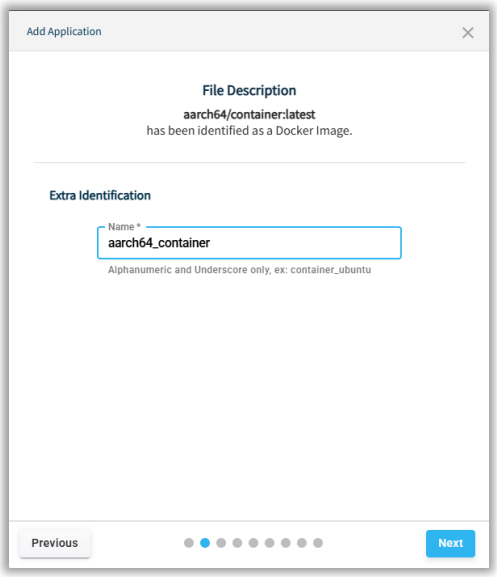
Use this option if the image file has been previously imported.



1 In the *Choose Application* configuration, select the application. Click **NEXT**.



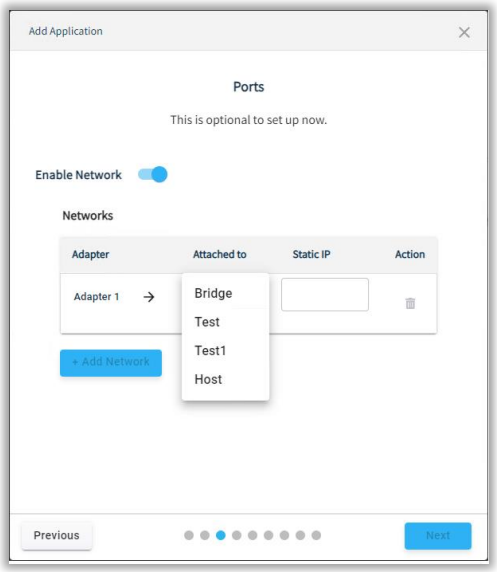
2 In the *File Description* configuration, enter a *Name* and *Labels*. Click **NEXT**.



3 The **Ports** configuration defines the network configuration. Select an option for attaching the network adapter to the container in the *Attached to* parameter and click **NEXT**.

- Bridge
- Host
- User-created custom network (MACVLAN/Bridge)

The user can also enter the (optional) Static IP corresponding to the selected network in the *Static IP* field.



Note: The user must first create the custom network to be able to create a container using that network. Detailed information regarding the creation of a custom network can be found in section *5.1.1.1 Adding a Network to Gateway*.

Note: A maximum of four network adapters can be added.

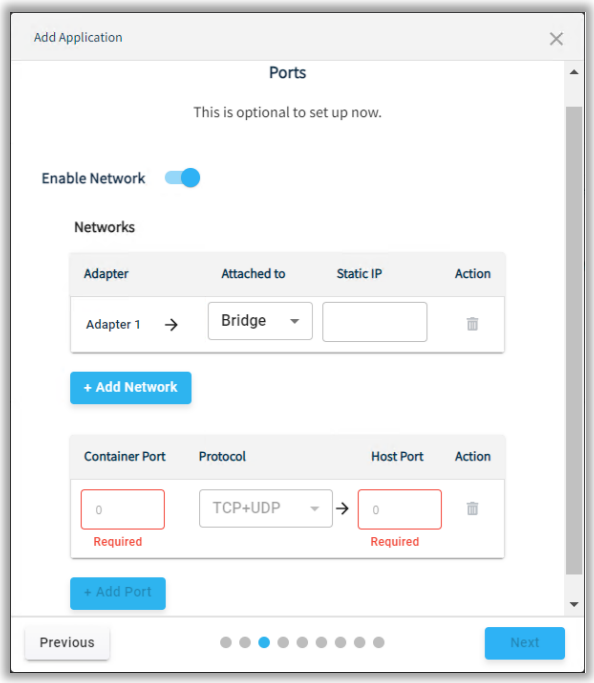
a) For *Bridge* networks, the container and host ports must be configured.

i. In the *Container Port* field, enter the container port number.

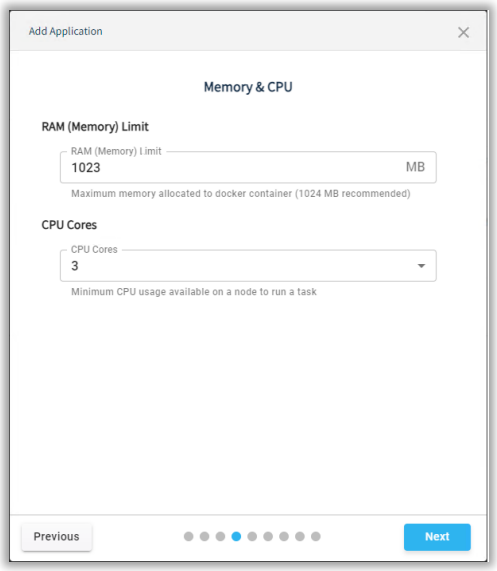
ii. In the *Host Port* field, enter the host port number.

Note: A maximum of four Container and Host ports can be added.

The user is not allowed to create a container without a Container port and Host port in **Bridge** mode. A minimum of one Docker and Host port is required to create a container with a Bridge network.

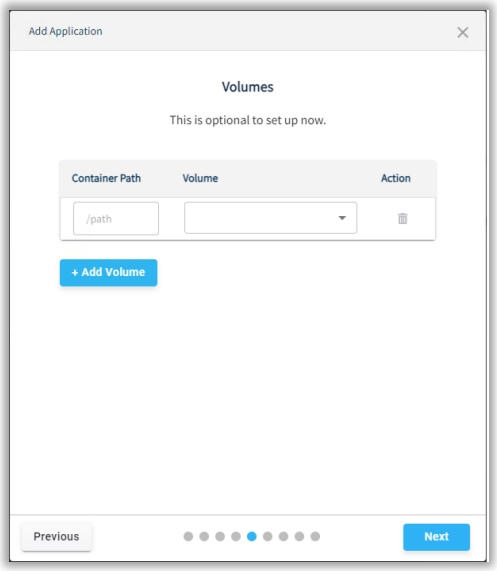


4 The **Memory & CPU** configuration defines the memory and CPU. Click **NEXT**.

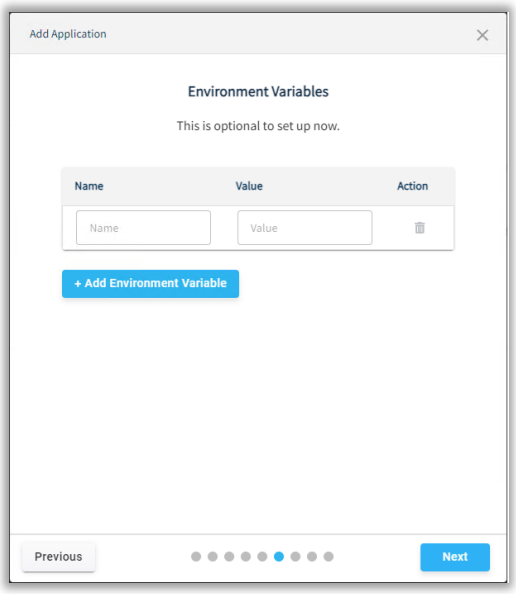


- In the *RAM (Memory) Limit* field, enter the size of memory (MB) for the container. The minimum memory value for creating containers is 4MB.
- In the *CPU Cores* field, enter the number of CPU cores to be used by the container. The number of processors is expressed in number of physical CPU cores.

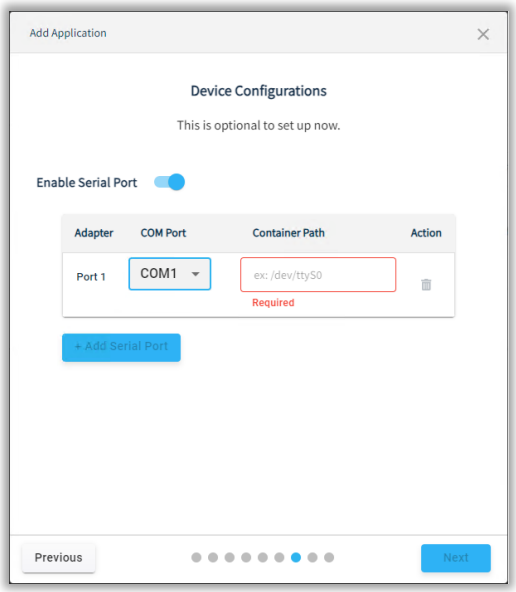
5 (Optional) In the **Volumes** configuration, enter the *Container Path* and select the *Volume* from an existing list to attach to the container. Click **NEXT**.



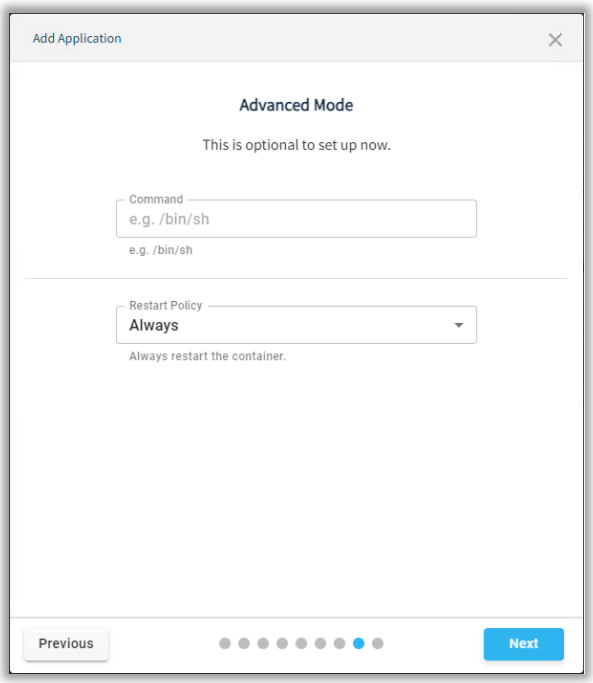
6 (Optional) In the **Environment Variables** configuration, enter the *Name* and *Value* of the environment variable. Click **NEXT**.



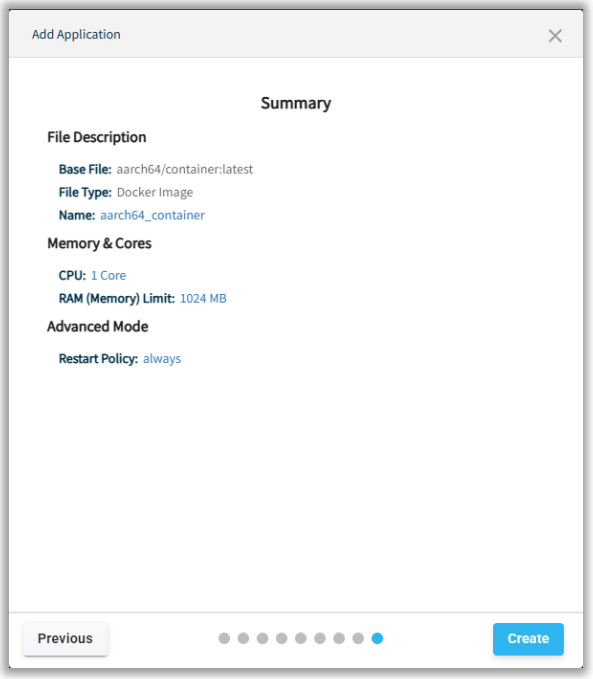
7 (Optional) In the **Device Configurations** configuration, enter the serial port settings. Click **NEXT**.



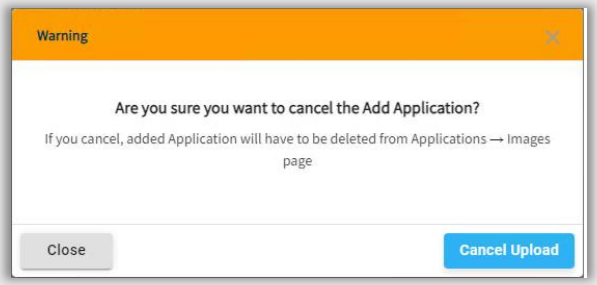
8 (Optional) In the **Advanced Mode** configuration, enter the advanced container *Command* and *Restart Policy*. Click **NEXT**.



9 In the **Summary** dialog, check all details and click **ADD APPLICATION** to create the container. If edits are needed before creating the container, click the **PREVIOUS** button.



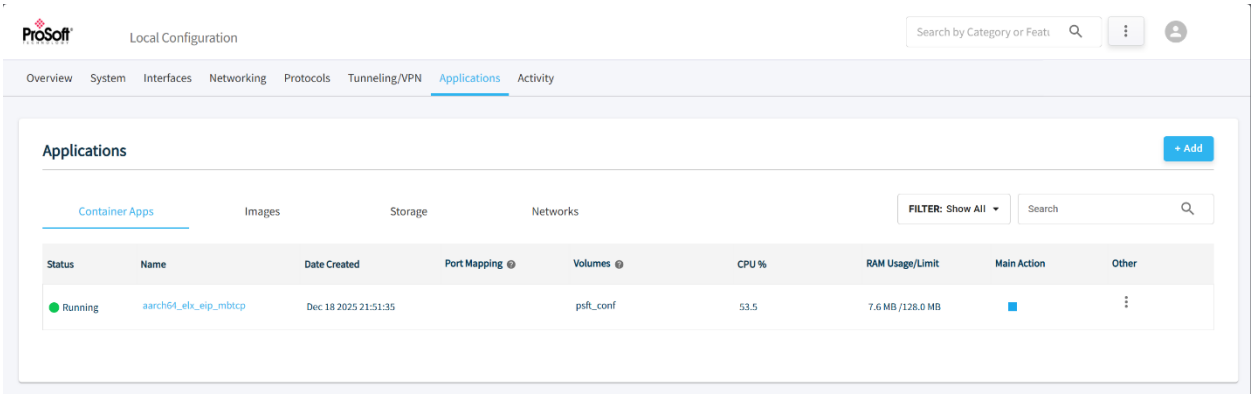
Note: Clicking the "**X**" button on the top-right corner of the dialog at any step during container configuration will display the following:



When clicking the **CANCEL UPLOAD** button, the container creation will be stopped and the image will be stored under the *Images* tab. It must be manually deleted.

5.2.4 Container Status

Upon successful creation of a container, the status information is displayed as follows:



Parameter	Description
Status	The current operating status of a container: • Running • Stopped • Paused
Name	Name of the container.
Date Created	Date of container creation.
Port Mapping	This field describes the following ports: • Container Port: The Container port number. • Host Port: The Host port number.
Volumes	The container volumes that are attached to a particular container.
CPU %	The sum of work handled by a processor on the container. It is also used to estimate system performance.
RAM Usage/Limit	The memory utilization of a container and total allocated memory to a container.
Main Action	Quick action available according to the state of container.
Other	Click on the *Other* button ⋮ on a container to reveal the following:

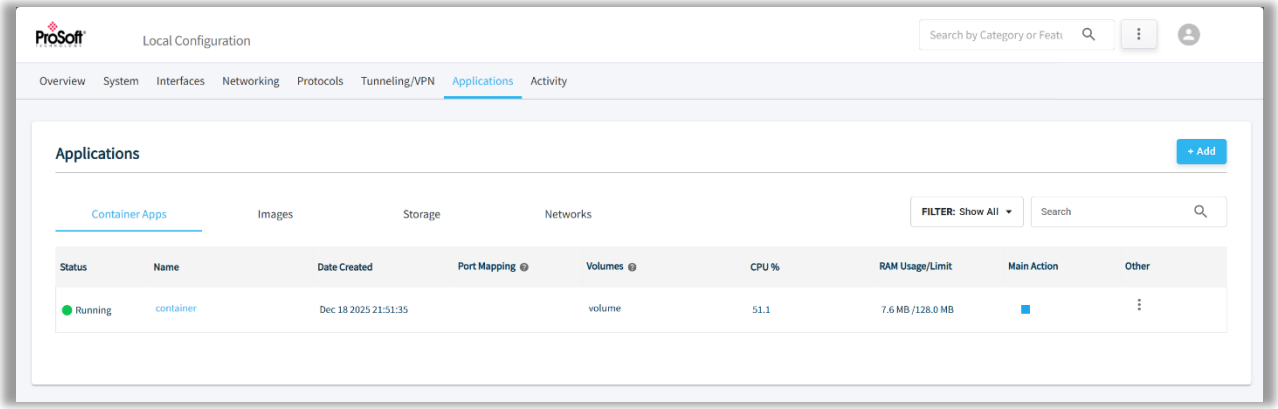
Action Button	Description
Start	Power On the Stopped container.
Stop	Stop the container.
Pause	Pause the container.
Restart	Restart the container.
Shell	User can log into a Docker container from GUI with the help of Docker exec shell functionality.
Save	Save the container as an image. For more information, see section *5.2.5 Saving a Container as an Image*.
Edit Container Details	Edit the *Name* of a container.
Delete	Delete the container.
Resume	Resume a Paused container.

Note: The *Restart*, *Pause* and *Shell* buttons are disabled when a container is in the **Stopped** or **Paused** state.

5.2.5 Saving a Container as an Image

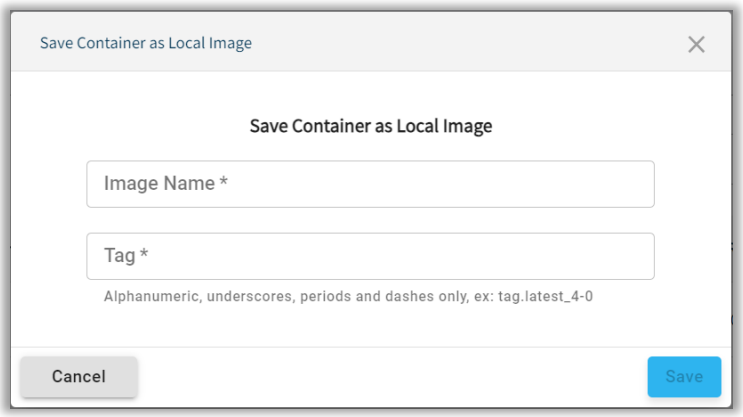
In the *Applications* > *Container Apps* tab, the user can save a particular container as a container image.

Note: The Container state will become Paused for few seconds while the image is being saved.



To save a container as an image:

1. In the *Containers* tab, click the Actions button  .
2. Click the **SAVE** button.



3. Enter the *Image Name* and *Tag* number.

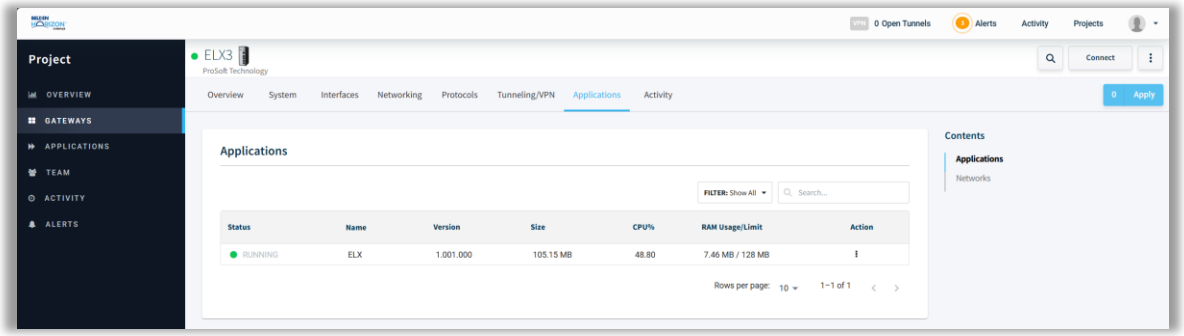
Note: The user is allowed to use "/" in the *Name* field. These images will not be downloaded directly to the local machine. To download to the local machine, browse to the *Images* tab and select *Download*.

4. Click **SAVE**.

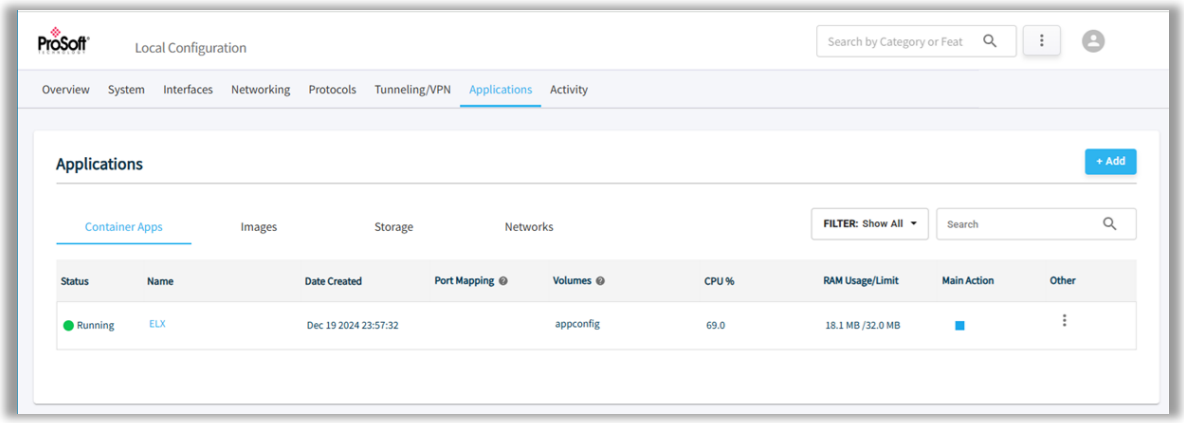
5.3 Verifying Successful Container Deployment

There are two ways to verify successful Container deployment. The *Status* will display as **RUNNING**.

- **Belden Horizon Console**
  Go to *Gateways* > *ELX3* > *Applications* tab



- **ELX3 Local UI**
  Go to *Applications* tab > *Container Apps* tab



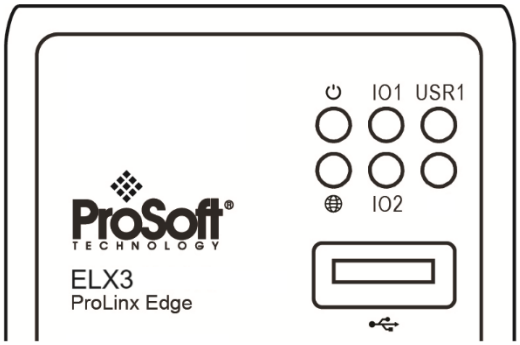
6 Diagnostics

6.1 LEDs

The LEDs express the existence and possible cause of a problem. The LEDs provide valuable diagnostic information such as:

- The state of each port
- System configuration errors
- Application errors
- Fault indications

6.1.1 Main LEDs



The following table describes the main ELX3 LEDs:

LED	Function	State	Description
⏻	System Status	Off	The ELX3 is not powered up.
		Solid Green	The ELX3 is operational.
		Flashing Green	Indicates an unconfigured state of the ELX3.
		Solid Red	An unrecoverable error has occurred. A reset or power cycle may clear the error. Call tech support if the problem persists.
		Flashing Red	Indicates a major recoverable fault such as a power input error.
		Alternating Red & Green	Firmware update is underway. It will remain in this state until update is complete.
🌐	Internet Status	Off	Belden Horizon Console is disabled **and** OpenVPN is not configured.
		Solid Green	The gateway is managed by a Belden Horizon Console account.
		Flashing Green	Belden Horizon Console tunnel is connected.
		Solid Yellow	OpenVPN is configured but Belden Horizon Console is not.
		Flashing Red	Belden Horizon Console is disconnected but DNS and Internet is working. **Or** OpenVPN is not able to discover the other side/OpenVPN server.
		Solid Red	Belden Horizon Console is enabled but internet has failed. **Or** Belden Horizon Console is disabled and OpenVPN is in a failed state.
IO1	Digital I/O 1	-	Not implemented.
IO2	Digital I/O 2	-	Not implemented.
USR1	N/A	N/A	Reserved for future use.

6.1.2 Serial Port LEDs

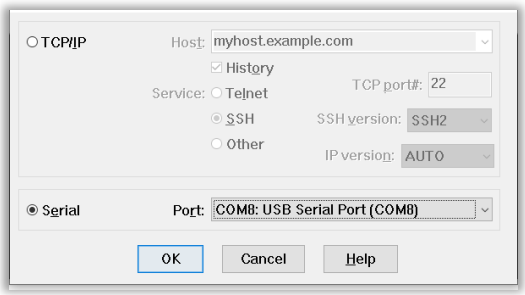
This table describes the serial port LEDs.

LED	State	Description
RX	Off	No activity on the port.
	Flashing Green	The port is actively receiving data.
TX	Off	No activity on the port.
	Flashing Yellow	The port is actively transmitting data.

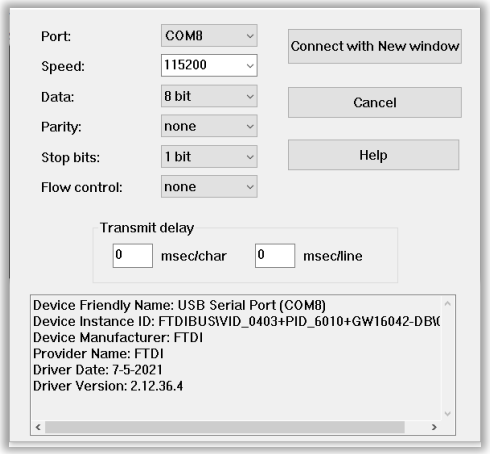
6.1.3 Command Line Interface

To factory reset the ELX3 using the Command Line Interface, perform the following steps:

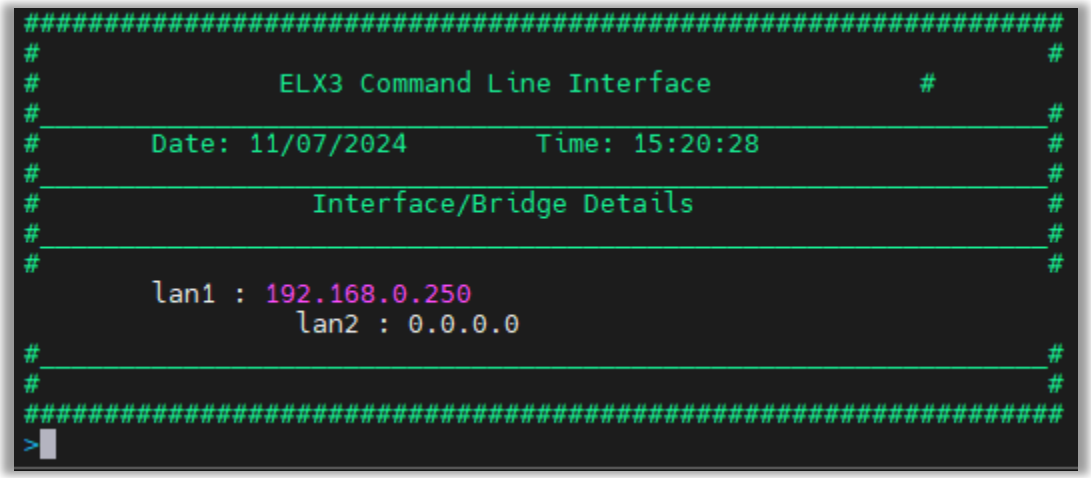
1. Connect to the serial port of the ELX3 using a Terminal Emulator.
2. Select the COM Port on which the console shall be connected.



3. Set the following serial port parameters:
   - Baud Rate/ Speed: **115200**
   - Data: **8 bit**
   - Parity: **None**
   - Stop Bits: **1 bit**
   - Flow Control: **None**

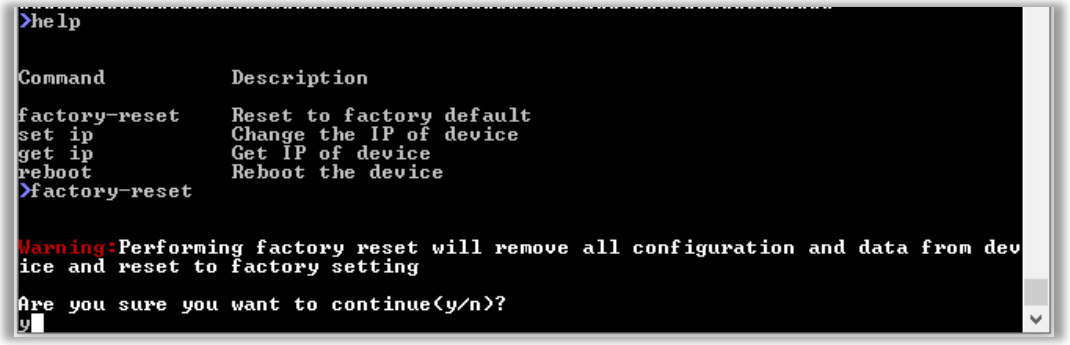


4 Upon successful console connection to the ELX3, the command line interface will be available.

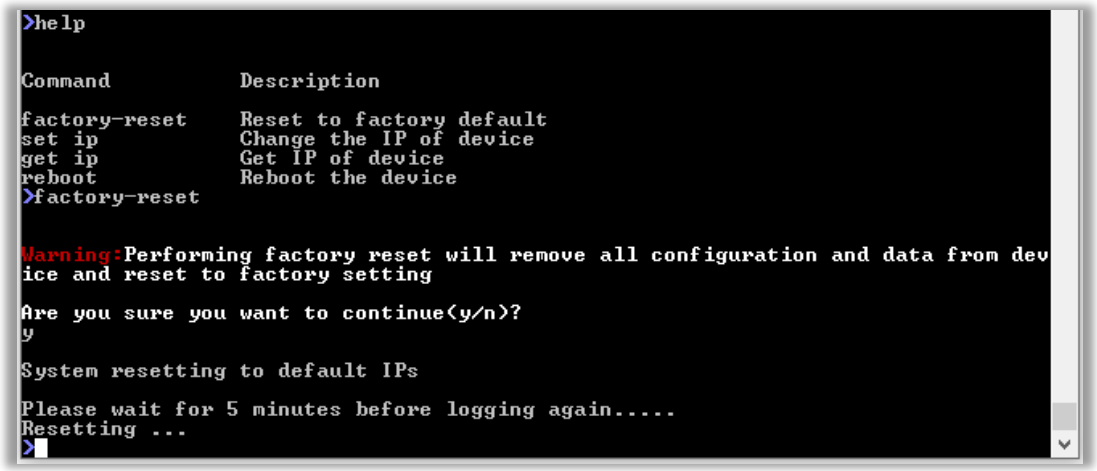


5 The `help` command will display all the supported commands.

6 Execute the `factory-reset` command to reset the ELX3 to factory settings. Confirm with a ***y*** (for yes).



7 After the factory reset is complete, the ELX3 will be available to connect to using its default IP of **192.168.0.250** on the LAN1 port.



6.1.4 Ethernet Port LEDs

This table describes the Ethernet port LEDs.

LED	State	Description
Green	Solid	100mbps link with no activity.
	Flashing	100mbps link with activity.
Yellow	Solid	GbE link with no activity.
	Flashing	GbE link with activity.
Green and Yellow	Both off	10mbps link/activity.

6.2 Factory Reset

A factory reset will reset the ELX3 to factory defaults, requiring re-activation and re-configuration. There are three ways to perform a factory reset:

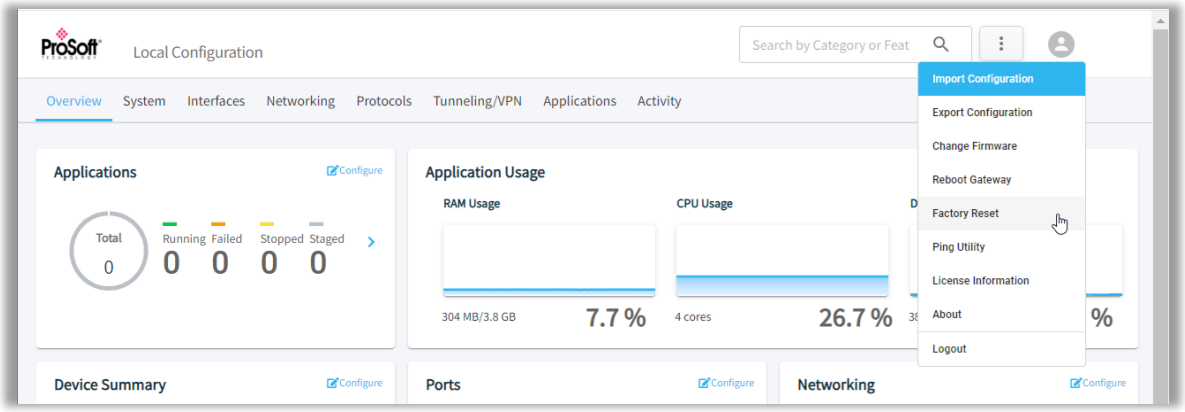
- Configuration Webpage
- Command Line Interface
- Reset button

6.2.1 Configuration Webpage

To factory reset the ELX3 from the configuration webpage, perform the following steps:

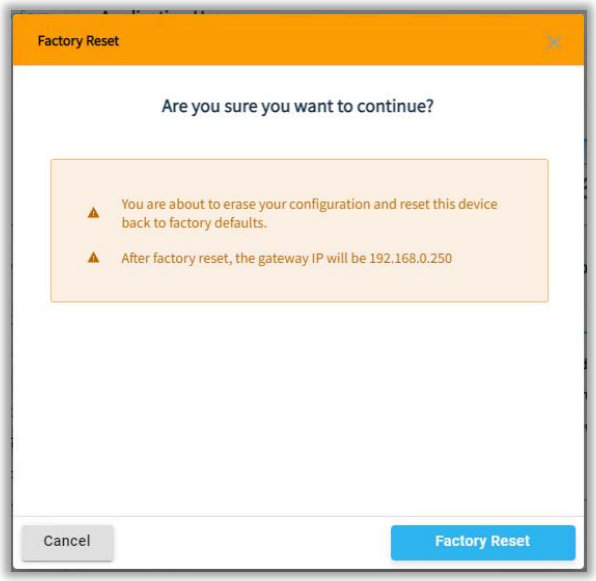
1. Establish a default connection to the ELX3 and perform the initial setup as described in *Chapter 2 Initial Configuration*.

2. On the ELX3 webpage, click the **SETTINGS** icon  in the top right corner of the page.

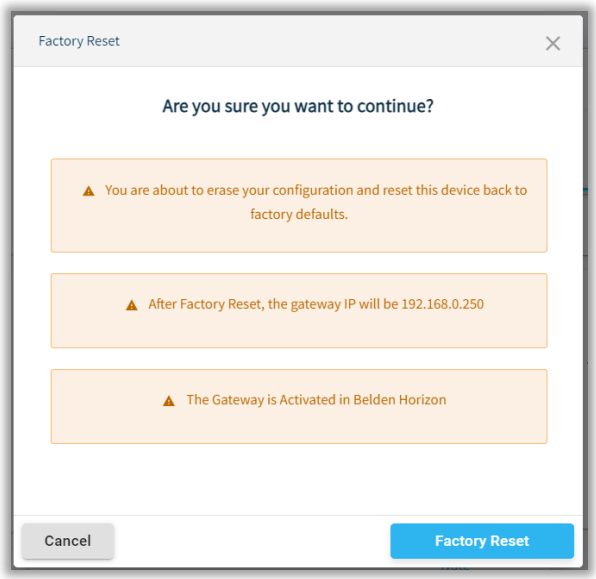


3. From the drop-down list, select **FACTORY RESET**.

4 The *Factory Reset* dialog is displayed.



If the ELX3 device is connected via Belden Horizon Console, the following pop-up is displayed:

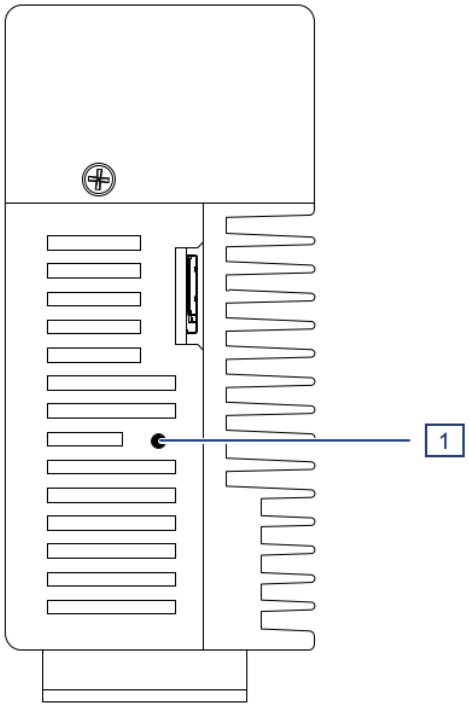


5 Click **FACTORY RESET** to initiate the factory reset procedure.

Once the factory reset procedure is completed, log in to the gateway using the default credentials (admin/password). After the initial login, the user is prompted to change the default password.

6.2.2 Reset Button

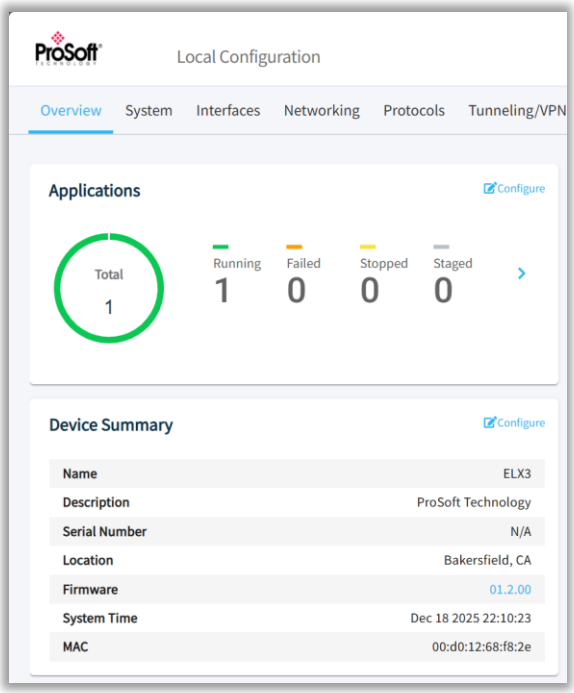
To factory reset the ELX3, hold the **Reset** button on the bottom of the gateway for about 10 seconds.



Label	Description
1	Reset button

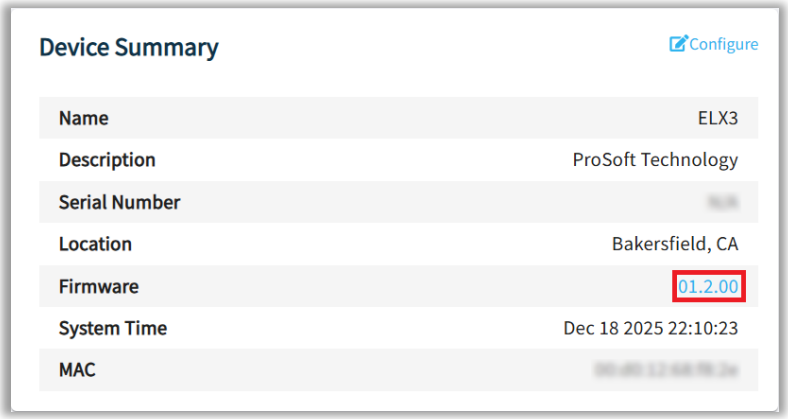
6.3 Updating Firmware

The current firmware versions can be found in the *Overview* tab > *Device Summary* tile.

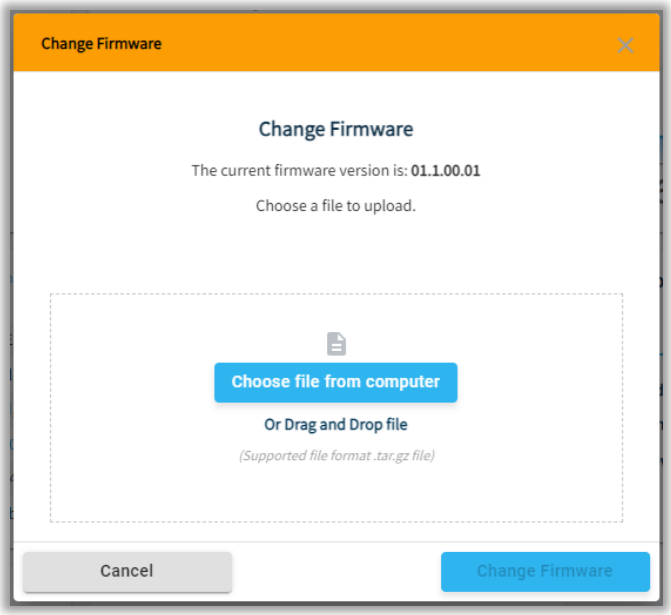


To upgrade the ELX3 firmware, perform the following steps:

1. Open the ELX3 configuration webpage.
2. In the *Overview* tab > *Device Summary* tile, click on the firmware version number.



3 The *Change Firmware* dialog will open.



4 Drop the **.tar.gz** file into the *Change Firmware* dialog box or click the **CHOOSE FILE FROM COMPUTER,** then click **OK**.

5 Click **SUBMIT** to upgrade the ELX3 firmware. The installation process takes approximately 5 minutes and automatically reboots the gateway.

6 Verify the Firmware version in the *Overview* tab > *Device Summary* tile.

7 Security

This chapter contains security recommendations for the ELX3. It covers the following lifecycle phases:

- Secure installation
- Secure commissioning
- Secure administration and operation
- Secure maintenance
- Secure decommissioning

A secure device can help maintain the security and availability of the network.

7.1 Scope

This chapter covers the recommended device security measures throughout the lifecycle of the device. These recommendations include:

- How to achieve defense in depth for the device
- How to harden the device
- How a specifically configured device can help achieve defense in depth for the system
- How a specifically configured device can help harden the system

A network device is part of a superordinate system. Therefore, the device and the system are interdependent. The system lifecycle and the requirements of the system for defense in depth are outside the scope of this document. References to the system lifecycle are made only if necessary, and only for informational purposes.

For the network, additional planning and implementation steps may be necessary. For example, an L3 network plan may be needed in addition to the VLAN plan mentioned in this document. The L3 network plan and the VLAN plan are both outside the scope of this document.

7.2 Defense in Depth

Defense in depth is a strategy that employs various independent security measures to guard an asset under consideration against specific attacks.

A system that employs defense in depth first confronts an attacker with a particular barrier. If an attacker overcomes this barrier, the system presents another barrier of a different type. A minimum of 2 barriers of different types shall guard any system asset under consideration. This layered security approach is considered best practice. It potentially demoralizes an attacker while taking the imperfection of real-world security barriers into account.

7.2.1 Defense in Depth vs. Hardening

In comparison to hardening, defense in depth is a more selective and structured approach. Defense in depth employs a specific subset of all conceivable security measures.

Hardening can be characterized as defense in broad. It aims at closing as many weaknesses in any barriers as reasonably possible. A strategy for hardening may include the concepts "least necessary functions" for the device and "least necessary privileges" for user accounts.

Develop a strategy for defense in depth first, then complement it by hardening.

For more information about secure installation recommendations, see section *7.4.1 Secure Installation Location*.

7.2.2 Responsibilities

Defense in depth as well as hardening need planning, implementation and maintenance. It is the responsibility of the system operator to perform these steps.

It is recommended to consider all security measures given in this document, and to select those that are most relevant for the actual situation.

7.2.3 Example

ID	Barrier	Description
	System Level	
1	Internet Firewall	An attacker must overcome the internet firewall to gain access to the company Intranet.
2	Industrial Firewall	An attacker must overcome the industrial firewall to gain access to the industrial network. The industrial firewall separates the industrial network from the company Intranet.
3	Dedicated device management VLAN	An attacker must overcome VLAN restrictions to snoop packets like unknown unicast frames of device management traffic.
	Device Level	
4	Secure management protocols	An attacker must overcome encryption to snoop packet contents.
5	Non-default user account names[1]	An attacker must guess or discover the actual user account names.
6	Non-default passwords[2]	An attacker must guess or discover the actual passwords.
7	Specific, restricted account privileges	An attacker must guess or discover the administrator account credentials to read privileged data or manipulate device settings.

[1] Dedicated user account names can be device-specific and can be deliberately chosen to be non-descriptive.

[2] Passwords can be specific to a certain access protocol (for example HTTPS or SNMPv3) and can be device specific.

7.3 Impact of the System Lifecycle to the Device Lifecycle

A network device is a component in a superordinate system. The system lifecycle determines parts of the device lifecycle. A system lifecycle involves a planning phase. The decisions taken in the planning phase affect the device lifecycle directly or indirectly.

Typical decisions during system planning include:

- The physical position of the device, for example, its installation location and environment
- The logical position of the device, for example, the security zone
- The requirements of the system for defense in depth

7.3.1 VLAN Plan

VLANs are a software-configurable concept to segregate a LAN (layer 1) into separate Virtual LANs (VLANs) on layer 2. Advantages include the separation of data packets belonging to different VLANs. The separation also applies to flooded multicast, broadcast, and unknown unicast frames. This helps confidentiality besides helping reduce the network load on layer 1.

A VLAN plan is a prerequisite for a secure configuration of the device and in turn for the security and availability of the system. Create a VLAN plan that segregates the network on layer 2. A dedicated management VLAN can be a barrier component in the defense in depth strategy.

For simple networks, a VLAN plan and the configuration of VLANs may be considered unnecessary from a functional perspective. However, VLANs are recommended from a security perspective.

Note: For the network, additional planning and implementation steps may be necessary. For example, an L3 network plan (outside the scope of this document) may be needed in addition to the VLAN plan.

7.4 Impact of Device Requirements on System Planning

Some requirements of the device have an impact on the system lifecycle phases and system planning.

Topics of this interdependence include:

- A secure installation location, including the following aspects:
  - Device availability: Power supply, power budget, and data link redundancy
  - Properties of the USB port
  - Device and port LEDs
- The detailed physical device security requirements
- The user account policy parameters the device offers:
  - For the login policy
  - For the password policy
  - For the user name and access role policy
  - For the SNMPv3 authentication and encryption type, and password policy
- VLAN ID restrictions arising from certain redundancy protocols: VLAN IDs ≥2 for payload traffic and device management.

7.4.1 Secure Installation Location

Refer to the *ELX3 Installation Guide* (www.prosoft-technology.com) for a suitable physical installation location.

Select a location that offers appropriate device security by restricting physical access:

- Install the device in a room that can be locked and where only authorized personnel have access.
- Install the device in a cabinet to which only authorized personnel have access.
- Install the device in a cabinet with an opaque door.

7.4.1.1 Device Availability

Device availability can be an important base for the security of the superordinate system. Check that the following device availability requirements are met as needed:

- Provide redundant power supply
- Provide an adequate power budget
- Provide data link redundancy

7.4.1.2 Device and Port LEDs

The device and port LEDs show important information about the device state and the port states.

To prevent information leakage, consider the following security aspects as needed in addition to the secure installation location:

- Install the device in a cabinet with an opaque door.
- Cover or obstruct the LEDs with a removable cover.

7.4.2 Dedicated User Account Login Policy

The device allows for the configuration of a login policy for the user accounts. The login policy applies to all user accounts.

Configure the following requirements for the user login:

- User
- Password
- Role

Note: It is recommended to plan an overarching user account login policy and apply it to each device.

7.4.3 Dedicated User Account Password Policy

The device allows for the configuration of a password policy for the user accounts. Configure the following requirements for the password:

- Minimum password length
- Minimum number of uppercase characters
- Minimum number of lowercase characters
- Minimum number of digits
- Minimum number of special characters

Note: The default password must be changed on the first login. It is recommended to plan an overarching user account password policy and apply it to each device. To deter attackers, consider planning different passwords on different devices.

7.4.4 Dedicated User Account Name and Access Role Policy for Device Management

Configure dedicated user accounts as needed:

- Assign the login and password policies.
- Create user accounts with:
  - Dedicated names
  - Chosen access roles that offer only the least necessary privileges
- Assign user accounts strong, individual passwords and apply the password policy check.
  - Plan strong SNMPv3 authentication and encryption types and strong related passwords for the new user accounts.
- Remove user accounts with standard names.

Note: It is recommended to plan an overarching user account and access role policy and apply it to each device. To deter attackers, consider planning different user account names and different passwords on different devices.
It is also recommended to plan an overarching policy for SNMPv3 authentication and encryption types, and the related passwords. To deter attackers, consider planning different SNMPv3 passwords on different devices.

7.4.5 Dedicated Logging Policy

Configure device logging settings:

- Assign the required logging destinations.
- Assign the required syslog types.

Note: It is recommended to plan an overarching device logging policy and apply it to each device.

User account can also be chosen to be non-descriptive.

8 Device Security

This chapter covers the device security throughout the lifecycle phases of the ELX3.

8.1 Prerequisites

It is assumed that the following system planning steps have been addressed, including:

- Suitable physical location for the devices
- Creating a dedicated user account login policy
- Creating a dedicated user account password policy
- Creating a dedicated user account and access role policy for device management

8.2 Recommended Installation Sequence

The device security lifecycle phases in a practical order are:

- Choice of a secure installation location
- Initial software update
- Initial security configuration
- Possible hardware modification for security
- Initial device installation
- Operation
- Maintenance
- Decommissioning

Note: Depending on needs of the system, the work steps can be performed in a different sequence.

8.2.1 Reasons for the Recommended Installation Sequence

Performing the initial configuration and the initial software update before the initial device installation can have the following benefits:

- The required resources, for example, prepared configuration files and device labels, may be more conveniently available in an office location.
- Time-consuming steps like software updates can be performed in parallel.
- Associated devices, for example, devices participating in a ring redundancy, can be configured contiguously.
- For certain hardware measures like physically securing a USB port, the USB port may be needed for the initial configuration and software update before the USB port is locked.
- The remaining work steps in the field require less time.

8.2.2 Recommended Preparation for Installation

The following recommendations can help reduce the initial effort and save time:

- Decide which device software release run on the devices.
- Download the selected software files.
- Prepare device configuration files based on the network plan.
- Prepare device labels.

Note: It is recommended to use the latest available release of the device software.

8.3 Choice of a Secure Installation Location

Refer to the *ELX3 Installation Guide* (www.prosoft-technology.com) for a suitable physical installation location. Select an installation location that in addition offers appropriate device security by restricting physical access.

Check that the following device security requirements are fulfilled if needed:

- Install the device in a room that can be locked and where only authorized personnel have access.
- Install the device in a cabinet to which only authorized personnel have access.
- Install the device in a cabinet with an opaque door.

8.3.1 Device Availability Requirements

Device availability can be an important base for the security of the superordinate system. Also consider implementing measures that increase device availability.

Check that the following device availability requirements are fulfilled if needed:

- Provide redundant power supply.
- Provide an adequate power budget.

8.3.1.1 Power Supply Redundancy Requirements

Check that the power supply redundancy requirements are fulfilled if needed:

- The device is powered by 2 redundant power sources.
- The power supply cables to the device run along different paths as far as possible.
- The power supplies are powered in a redundant way, for example, by 2 separate mains cables.
- The mains cables to the redundant power supplies run along different paths.

8.3.1.2 Power Supply Power Budget Requirements

Refer to the *ELX3 Installation Guide* (www.prosoft-technology.com) for the power requirements of the device. Check that the power requirements are fulfilled if needed:

- One single power supply can deliver power for all the connected devices.

8.4 Software Update

The following description applies to:

- The initial software update for a device out-of-the-box.
- A software update as part of operation or maintenance.

Check if an updated release of the device software is available at www.belden.com/security.

Note: To check the running software release on a device that does not yet have an IP configuration, it is recommended to use the Belden Horizon Console. For more information, please see: www.prosoft-technology.com/Products/Remote-Access/Belden-Horizon

To update the software on the device, management access to the device is needed. It requires at least a preliminary IP configuration. It is recommended to use the Belden Horizon Console to assign an IP configuration to the device. Belden Horizon then offers to open the device management.

At the first login with the default password, the device requires the password to be changed. Use a dedicated password according to the password policy.

If the device software is to be updated:

1. Back up the device configuration.
2. Update the device software.
3. Reboot the device for the new software to take effect.

Note: It is recommended to regularly check for device software updates and use the latest available release. A new release of the device software can provide security improvements or benefits like new security-related device functions.

8.5 Security Configuration

The following description applies to:

- The initial security configuration for a device out-of-the-box.
- Changes in the security configuration as part of operation or maintenance.

To save time and effort, perform the following security configuration steps by loading a prepared configuration profile into the device.

At the first login with the default password, the device requires the password to be changed. Use a dedicated password according to the password policy.

Perform the following steps as needed:

- Assign a static IP address for the device management.
- Configure a VLAN dedicated to management access.
- Disable insecure management protocols.
- Enable IP access restrictions.
- Configure a dedicated HTTPS certificate.
- Configure a dedicated user account login policy.
- Configure a dedicated user account password policy.
- Configure dedicated user accounts.
- Configure logging.

When the device configuration is complete:

- Create a backup copy of the configuration.
- Include other device-related data like private keys.

8.5.1 Assign a Static IP Address for the Device Management

Note: At the first login with the default password, the device requires the password to be changed. Use a dedicated password according to the password policy.

The device offers the following options of assigning a management IP address: **Local**, **DHCP** (default), and **BOOTP**. Selecting **Local** (that is: static) helps make the device more immune to potential attacks via the DHCP protocol.

8.5.2 Disable Insecure Management Protocols

Disable insecure management protocols:

- Disable SNMPv1 (delivery state: disabled)
- Disable SNMPv2 (delivery state: disabled)

8.5.3 Configure Management IP Access Restrictions

The device allows restricting the management access to the device to a source IP address range. Specify the address range by providing an IP address and a netmask.

Configure the management access IP restrictions individually for each protocol or for a group of protocols.

Protocol	Recommendation for production	Delivery state
HTTPS	Enabled	Enabled
SNMPv1	Disabled	Disabled
SNMPv2	Disabled	Disabled
SNMPv3	Enabled	Disabled

8.5.4 Configure Dedicated User Account Names and Access Roles for Device Management

Note: It is assumed that a dedicated user account name and access role policy has been created.

It is assumed that a dedicated policy has been created for SNMPv3 authentication and encryption types, and for the related passwords.

Configure dedicated user accounts as needed:

- Assign the device login policy.
- Assign the device password policy.
- Create user accounts. For each new user account, perform the following steps:
  1. Create a user account with a dedicated name.
     - Assign the new user account to an access role that offers only the least necessary privileges.
     - Assign the new user account a strong, individual password.
     - Apply the password policy check to the new user account.
- Remove user accounts with standard names.

Note: To deter attackers, consider using different user account names and different passwords on different devices. Also consider using different SNMPv3 passwords on different devices.

8.5.5 Create a Backup of Device-specific Data

When the device configuration is complete:

- Consider creating a backup copy of the configuration. For example, place the backup file in a device-specific folder.
- Include other device-specific data. For example, copy device-specific private keys or certificates to the same device-specific folder.
- Keep the backup files separate from the device in a secure location.

This minimizes effort to replace a device should the hardware become inoperable.

8.6 Possible Hardware Modifications for Security

The following descriptions apply to:

- The possible hardware modifications for a device out-of-the-box.
- Possible hardware modifications as part of operation or maintenance.

Perform the following hardware modification steps, like covering or obstructing a slot or a port, as needed:

- Restrict physical access to the USB port.
- Restrict physical (visual) access to the device and port LEDs.

8.6.1 Restrict Physical Access to the USB Port

If there are high security requirements and the USB port is not needed after commissioning, consider covering or obstructing the USB port.

8.6.2 Restrict Physical Access to Network Ports

If there are high security requirements and certain network ports are not needed, consider covering or obstructing these network ports.

8.6.3 Restrict Physical (Visual) Access to the Device and Port LEDs

For high security requirements, perform the following steps as needed:

- Install the device in a cabinet with an opaque door.
- Cover or obstruct the LEDs with a removable cover.

8.7 Device Installation

The following description applies to:

- The installation of a device in a new system.
- Changes to the device as part of operation or maintenance.

Perform the device installation according to the *ELX3 Installation Guide*. For more information, please see: www.prosoft-technology.com

8.7.1 Data Connections

Perform the data connections according to the *ELX3 Installation Guide*. For more information, please see: www.prosoft-technology.com. If high device availability is required, use redundant data uplinks.

8.8 Operation

In the operation phase of the device, it is assumed the appropriate physical and logical steps to set up the device and operate properly regarding the functional and security aspects of the device are observed. This reduces the required security steps during the operation phase to the considerations already described in this document.

8.8.1 Environmental Conditions

Obey the environmental conditions given in the *ELX3 Installation Guide*. For more information, please see: www.prosoft-technology.com. Do not open the device.

8.8.2 Connectivity

Obey instructions for connecting the Ethernet ports.

8.9 Maintenance

8.9.1 Software Update

If necessary, perform a software update:

- For the security aspects.
- For the detailed steps, see the *ELX3 User Manual* (www.prosoft-technology.com)

8.9.2 Hardware Enhancement

Typical application cases include:

- Connecting a new end device to an existing Ethernet port.
- Using redundant power supplies.
- Planning the power supply for worst case device power budget, in case one of the redundant power supplies fails.
- Providing redundant data uplinks.

8.9.3 Hardware Replacement

Note: Do not open the device.

Perform the following steps:

- Perform an initial software update.
- Perform the software configuration, for example, by transferring the existing configuration of the old device to the new device.

8.9.4 Hardware Repair

Should the device need repair, consider the following recommendations:

- Do not open the device.
- Send the device to the manufacturer for repair.
- Keep a backup copy of the device configuration.

If necessary and possible, delete the configuration and other confidential data.

8.10 Decommissioning

For high security requirements, consider physical destruction. Secure physical destruction addresses the possible reading-out of memory blocks from the flash memory and makes deletion and wiping redundant.

Note: If the device is to be used in the future, consider leaving the device and its software intact and deleting or wiping only the data on the device and on the external memory.

8.10.1 Destruction of Confidential Data

Note: Resetting the device to the default state performs normal file deletion operations on the device and the external memory which may leave some of the file contents or blocks in the flash memory intact. Also, the audit trail persists after a reset to the default state.

If there are high security requirements, consider the physical destruction of the device and the external memory.

8.10.1.1 Reset to the Delivery State

- For the deletion of data, perform the following steps as needed:
- Reset the device to the default state. This performs the following operations:
  - Deletes the current HTTPS certificate in the device and creates a new, self-signed HTTPS certificate.
  - Deletes the current SSH host key pair in the device and creates a new, self-signed SSH host key pair.
  - Deletes the configuration profiles and configuration scripts in the device.
  - Resets the boot parameters.
  - If the external memory is plugged in, the device deletes configuration profiles on the external memory.
- If necessary, manually delete the configuration profiles on the external memory and/or any other files on it.

Note: The audit trail persists after a reset to the delivery state.

8.10.2 Secure Physical Destruction of Device and Components

For the secure physical destruction of physical components, perform the following steps as needed:

- Physically destroy the external memory. This addresses:
  - The configuration profiles on the external memory.
  - The software files on the external memory.
  - Any other files on the external memory.
- Physically destroy the device, including the flash memory chips. This addresses:
  - The HTTPS certificate in the device.
  - The SSH host key pair in the device.
  - The configuration profiles in the device.
  - Any other files in the device.

9 Glossary

Abbreviation	Description
ASCII	American Standard Code for Information Interchange.
CIDR	Classless Inter-Domain Routing. A CIDR address is written with a forward slash preceding a suffix indicating the number of bits in the prefix length, such as 192.168.0.0/16.
DHCP	Dynamic Host Configuration Protocol.
HTTP	Hyper Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IIoT	Industrial Internet of Things
IP	Internet Protocol
LAN	A computer network covering a small geographic area, like a home, office, or group of buildings. Compare to WAN.
MAC	Media Access Control. A MAC address is a unique identifier attached to most forms of networking equipment.
MIB	Management Information Base. A database used by SNMP to manage devices such as switches and routers in a network.
PC	Personal Computer
QR	Quick Response
RTU	Remote Terminal Unit. A device that collects data from data acquisition equipment and sends it to the main system over a network.
SSH	Secure Shell. A network protocol using public key cryptography to provide secure remote login.
SSL	Secure Socket Layer. A cryptographic protocol that creates a secure data transfer session over a standard TCP connection.
Syslog	A protocol for sending event messages over an IP network to remote servers called “event message collectors.”
TCP	Transmission Control Protocol
TLS	Transport Layer Security.
UDP	User Datagram Protocol. One of the communications protocols of the Internet Protocol Suite. Replaces TCP when a reliable delivery is not required.
URL	Uniform Resource Locator
VID	VLAN Identifier
VLAN	Virtual Local Area Network. A logical subgroup within a local area network that is created with software rather than by physically manipulating cables.
WAN	Wide Area Network. A computer network that crosses metropolitan, regional, or national boundaries. Compare to LAN.

10 Appendix

10.1 Syslog Description

The ELX3 supports a System Logging Protocol used to send system log or event messages to a specific server, called a Syslog server. It is primarily used to collect various device logs from multiple machines/applications to monitor and examine the device.

The ELX3 supports the System Logs feature which allows capturing various system log or event messages in a local ELX3 log file.

The Syslog protocol supports the following severity levels:

Code	Severity	Description
0	Emergency	System unusable.
1	Alert	Immediate action required.
2	Critical	Critical conditions detected.
3	Error	Error conditions detected.
4	Warning	Displays system messages and failures only.
5	Notice	Normal but significant conditions detected.
6	Informational	Displays all Warning messages, plus additional messages.
7	Debug	Logs all messages; used for resolving issues.

Example of Syslog messages:

<165> 2017-05-11T21:14:15.003Z mymachine.example.com appname[su] – ID47 [exampleSDID@32473 iut=”3” eventSource=” eventID=”1011”] BOMAn application log entry…

Part of Syslog message:

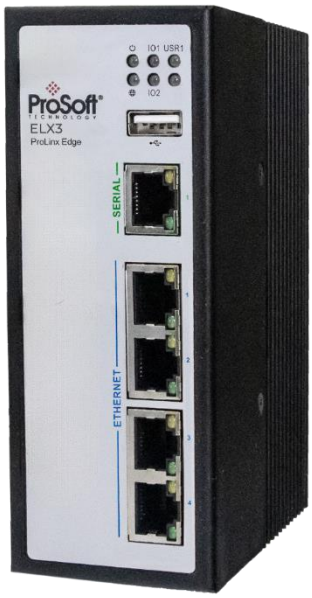
Part	Value	Information
PRI	165	Facility = 20, Severity = 5
VERSION	1	Version 1
TIMESTAMP	2017-05-11T21:14:15.003Z	Message created on 11 May 2017 at 09:14:15 pm, 3 milliseconds into the next second
HOSTNAME	mymachine.example.com appname	Message originated from host “mymachine.example.com”
APP-NAME	su	App-Name: “su”
PROCID	-	PROCID unknown
MSGID	ID47	Message ID: 47
STRUCTURED-DATA	[exampleSDID@32473 iut=”3” eventSource=” eventID=”1011”]	Structure data element with a non-IANA controlled SD-ID of type "exampleSDID@32473”, which has three parameters
MSG	BOMAn application log entry…	BOM indicates UTF-8 encoding, the message itself is “An Application log entry…”

10.2 Serial Port

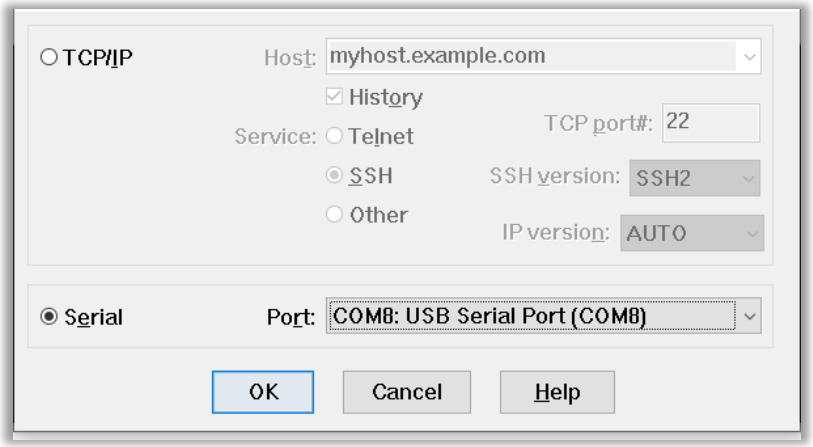
Using the RJ45 serial port provides a serial interface to the user's container application. A Minimal CLI can be used to check the assigned IP addresses of the ELX3 LAN Interfaces, reboot, and factory reset.

Note: If a container has control of the serial port, it will prevent access from all other input options. Likewise, if the CLI has control of the serial port the container would not be able to control it. First come, first serve has the priority.

1 Connect to the ELX3's RJ45 serial port using a serial interface.

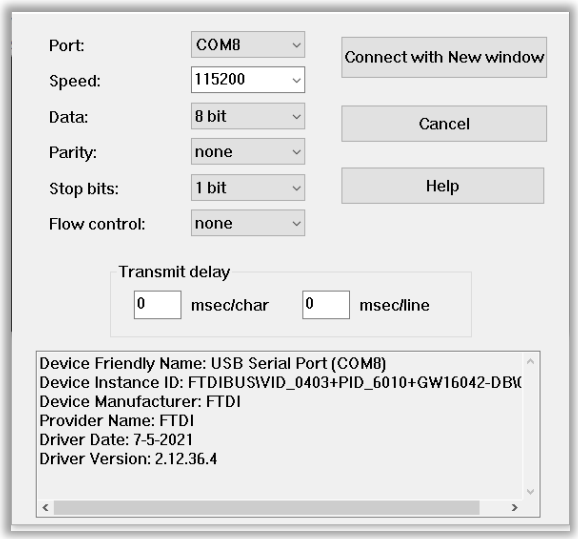


2 Select the COM Port on which the console shall be connected.

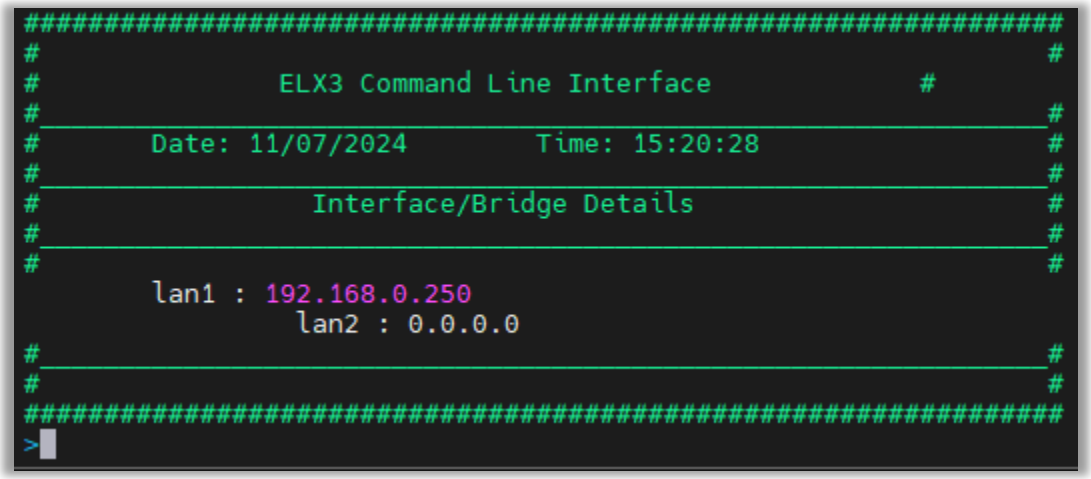


3 Set the following serial port parameters:

- Baud Rate/ Speed: **115200**
- Data: **8 bit**
- Parity: **None**
- Stop Bits: **1 bit**
- Flow Control: **None**



4 Upon successful console connection to the ELX3, the command line interface will be available.



5 Enter `help` and press **ENTER**.

```
>help


Command          Description

factory-reset    Reset to factory default
set ip           Change the IP of device
get ip           Get IP of device
reboot           Reboot the device
>
```

6 Enter `get ip` and press **ENTER** to check the assigned IP address of the LAN Interfaces for the ELX3.

```
>get ip
#_____________________________________________________________________#
#                                                                     #
        lan1 : 192.168.0.250
               lan2 : 0.0.0.0
#_____________________________________________________________________#
#                                                                     #
>
```

7 To configure the IP address of the ELX3.

a. Enter the following:

`set ip <`**`IP Address`**`> gw <`**`Gateway`**`> dev <`**`Name of the LAN to set IP`**`>`

b. Press **ENTER**.

c. Enter username: `admin`

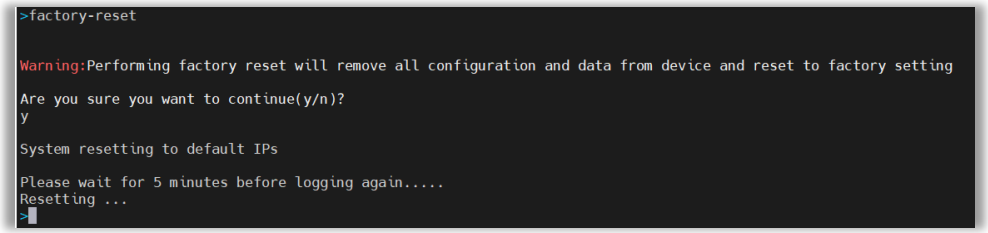
d. The default password is **PASSWORD**. If the UI password has already been changed, use the updated password.

e. Press **ENTER**.

```
>set ip 192.168.0.250/24 gw 192.168.0.1 dev lan1
Please input Login credentials
Login: admin
Password:
Login Successfull !!!
Please wait  ...
IP updated successfully!!!
>
```

8 To perform the factory reset operation, enter `factory-reset` and press **ENTER**. Press **y** to confirm the factory reset, or **n** to cancel. Press **ENTER**.

Note: The user must be logged in to perform a factory reset.



9 To restart the gateway, enter `reboot` and press **ENTER.**

Note: The user must be logged in to perform a reboot.

11 Frequently Asked Questions

1. **How do I configure one of the Ethernet ports on the ELX3 as a WAN port?**
   There are four Ethernet ports on the ELX3. Any port can be configured as a WAN or LAN port. There can only be a maximum of one WAN port. The WAN and LAN ports can have different subnets. The ports can be configured using the local webpage or via Belden Horizon Console.

2. **What is an Allowed IP List?**
   The terms *Allowed IP List* and *IP Whitelist* have the same meaning. It is a list of specific IP addresses or a range of IP addresses that will be allowed to connect to the ELX3's webpage through the WAN interface. To configure the ELX3's *Allowed IP List*, go to the *System* tab.

   Note: The ELX3's *Allowed IP List* is different to the *Allowed IP Connections* setting in Belden Horizon Console. *Allowed IP Connections* can only be configured in Belden Horizon Console. This is a list of specific end device IP addresses that a user can access when they tunnel (remotely connect via Belden Horizon Console) into the ELX3. To configure the *Allowed IP Connections* setting, make sure the ELX3 is activated in Belden Horizon Console and then go to the *Tunneling/VPN* tab.

3. **Can more than one of the on-board Ethernet ports be configured as a WAN port?**
   Yes, there can only be one active WAN port but the user can configure a Secondary WAN port on another interface if the Primary WAN port loses internet connectivity and there is a switch over.

4. **Can the Ethernet ports be on different subnets?**
   Yes, the LAN and WAN ports can be on different subnets. The LAN interfaces will only support a single subnet.

5. **How do I activate the ELX3 in Belden Horizon Console? Do I need to do this?**
   It is highly recommended that the ELX3 be activated in Belden Horizon Console. Please refer to *Chapter 3 Registration in Belden Horizon Console* or the *ELX3 Quick Start Guide* for more details.

6. **Can I access the internet through the ELX3?**
   Yes, the internet can be accessed through the ELX3. Internet access is disabled by default. It is not recommended to 'always' enable the internet access.

7. **Does the ELX3 include a firewall?**
   Yes, it includes integrated firewall capabilities.

8. **Does the ELX3 support port forwarding?**
   Yes, it supports port forwarding.

12 Support, Service, and Warranty

12.1 Contacting Technical Support

ProSoft Technology, Inc. is committed to providing the most efficient and effective support possible. Before calling, please gather the following information to assist in expediting this process:

1. Product Version Number
2. System architecture
3. Network details

If the issue is hardware related, we will also need information regarding:

1. Module configuration and associated ladder files, if any
2. Module operation and any unusual behavior
3. Configuration/Debug status information
4. LED patterns
5. Details about the interfaced serial, Ethernet or Fieldbus devices

North America (Corporate Location)	Europe / Middle East / Africa Regional Office
Phone: +1 661-716-5100 ps.prosofttechnology@belden.com Languages spoken: English, Spanish REGIONAL TECH SUPPORT ps.support@belden.com	Phone: +33.(0)5.34.36.87.20 ps.europe@belden.com Languages spoken: English, French, Hindi, Italian REGIONAL TECH SUPPORT ps.support.emea@belden.com
Latin America Regional Office	**Asia Pacific Regional Office**
Phone: +52.222.264.1814 ps.latinam@belden.com Languages spoken: English, Spanish, Portuguese REGIONAL TECH SUPPORT ps.support.la@belden.com	Phone: +60.3.2247.1898 ps.asiapc@belden.com Languages spoken: Bahasa, Chinese, English, Hindi, Japanese, Korean, Malay REGIONAL TECH SUPPORT ps.support.ap@belden.com

For additional ProSoft Technology contacts in your area, please see:
www.prosoft-technology.com/About-Us/Contact-Us

12.2 Warranty Information

For details regarding ProSoft Technology's legal terms and conditions, please see:
www.prosoft-technology.com/ProSoft-Technology-Legal-Terms-and-Conditions

For Return Material Authorization information, please see:
www.prosoft-technology.com/Services-Support/Return-Material-Instructions