HIRSCHMANN
A BELDEN BRAND

User Manual

Configuration
Industrial Edge Gateway
OpEdge

The naming of copyrighted trademarks in this manual, even when not specially indicated, should not be taken to mean that these names may be considered as free in the sense of the trademark and tradename protection law and hence that they may be freely used by anyone.

The performance features described here are binding only if they have been expressly agreed when the contract was made. This document was produced by Hirschmann Automation and Control GmbH according to the best of the company's knowledge. Hirschmann reserves the right to change the contents of this document without prior notice. Hirschmann can give no guarantee in respect of the correctness or accuracy of the information in this document.

Hirschmann can accept no responsibility for damages, resulting from the use of the network components or the associated operating software. In addition, we refer to the conditions of use specified in the license contract.

You can get the latest version of this manual on the Internet at:
https://www.doc.hirschmann.com

Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Germany

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

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 Hirschmann Automation and Control GmbH 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). Information about used Open Source Software is available in the graphical user interface under Help (3 ellipses on top right) > License Information. You can find the Open Source Software and their respective licenses on the DVD shipped with the product. For products shipped without DVD use the written offer (located in the graphical user interface under Help > License Information) to request the DVD. The DVD contains the necessary elements and instructions to rebuild your own version of the Open Source Software.
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 Hirschmann Automation and Control GmbH - 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:

Hirschmann Automation and Control GmbH
Head of R&D
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Germany

Warranty regarding further use of the Open Source Software

Hirschmann Automation and Control GmbH 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 Hirschmann Automation and Control GmbH. The licenses listed below define the warranty, if any, from the authors or licensors of the Open Source Software. Hirschmann Automation and Control GmbH specifically disclaims any warranty for defects caused by altering any Open Source Software or the product’s configuration. Any warranty claims against Hirschmann Automation and Control GmbH in the event that 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.

Contents

1 Start Here

1.1 About OpEdge

OpEdge is an industrial gateway designed for secure remote connectivity and Industrial Internet of Things (IIoT) applications.

OpEdge enables highly secure and reliable device-to-device and device-to-cloud communications. The gateway includes a serial (RS-232) port and multiple Ethernet ports, allowing for local connectivity to devices like PAC/PLCs, RTUs, DCS systems, smart instruments, electronic billboards, and communication towers.

OpEdge can be configured and managed through the webpage or via the Belden Horizon platform. Belden Horizon is a secure and intuitive cloud native platform that supports multiple applications like on-demand (secure machine access) or always-on (persistent data network) connectivity, data monitoring and alert notification.

OpEdge provides cloud connectivity to Belden Horizon via the Ethernet port.

1.2 Information sheet

The Hirschmann Safety and general information sheet and the OpEdge information sheet are provided in the OpEdge packaging. They provide basic installation and configuration information.

1.3 Installation Guide

The OpEdge Installation Guide provides detailed power, wiring, cables, and diagnostics information. It can be downloaded from www.doc.hirschmann.com.

2 Initial Configuration

This chapter covers the initial configuration of the OpEdge via the webpage. Once the OpEdge is registered on Belden Horizon, the OpEdge can be maintained via Belden Horizon (See Chapter 3 for more details).

The initial configuration includes setting up the LAN port. These steps must be followed, even if the OpEdge is going to be registered via Belden Horizon for cloud connectivity.

2.1 Connecting to the OpEdge Webpage

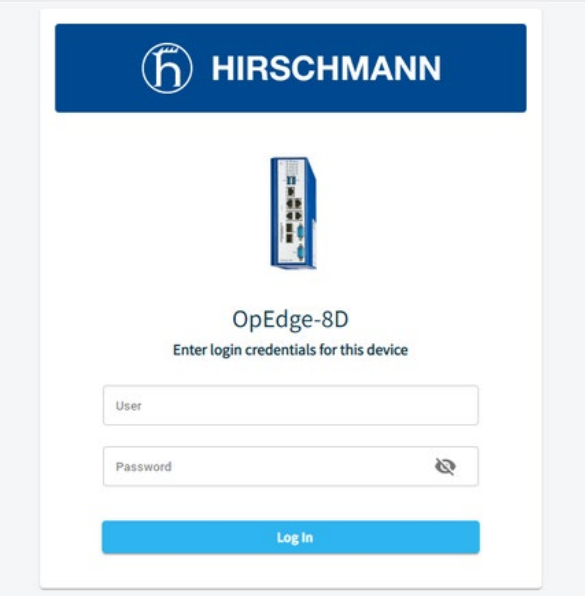
Perform the following steps to connect to the OpEdge webpage:

1 Ensure that the module is connected to the network to Ethernet port 1, and apply power to the module.

> **NOTE:** The PC must be on the same subnet as the OpEdge's default IP address settings.

2 Open a web browser and log in to the OpEdge configuration webpage. The default IP address is: **https://192.168.0.250:8080**. 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.

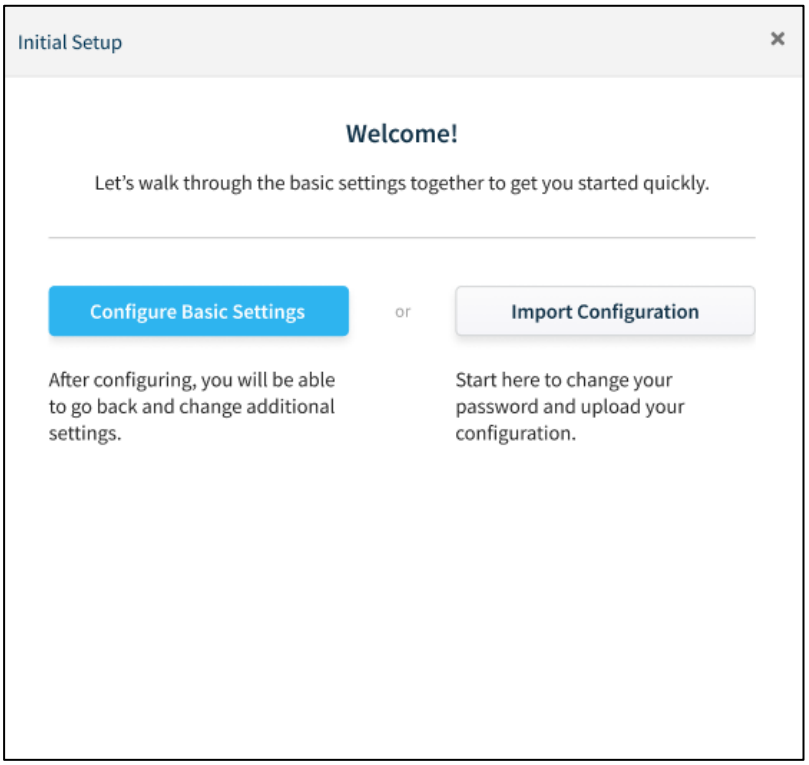


3 Enter the login credentials. The default *username* and *password* are **admin** and **password**.

> **NOTE:** The user is prompted to change the password after the first login. Provide a new password and apply the changes. After successful login with the new password, further password changes are done from the *System* tab on the webpage.

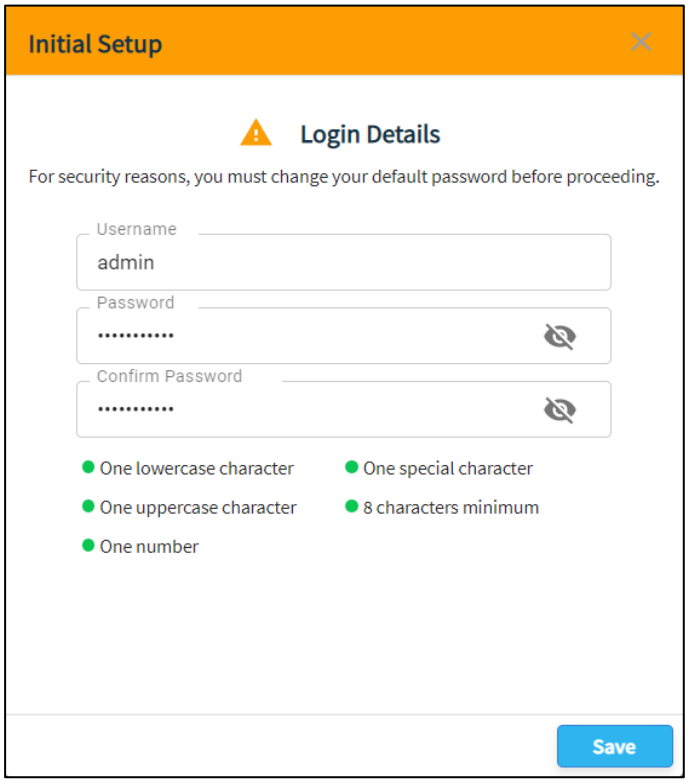
4 The *Initial Setup* dialog allows the following operations:

- Change Default Login Credentials
- Configure Basic Settings
- Import Configuration
- Manual Configuration



A. **Change Default Login Credentials**: To change the default login credentials for the OpEdge webpage:

i. Close the *Initial Setup* dialog to display another dialog as shown below:



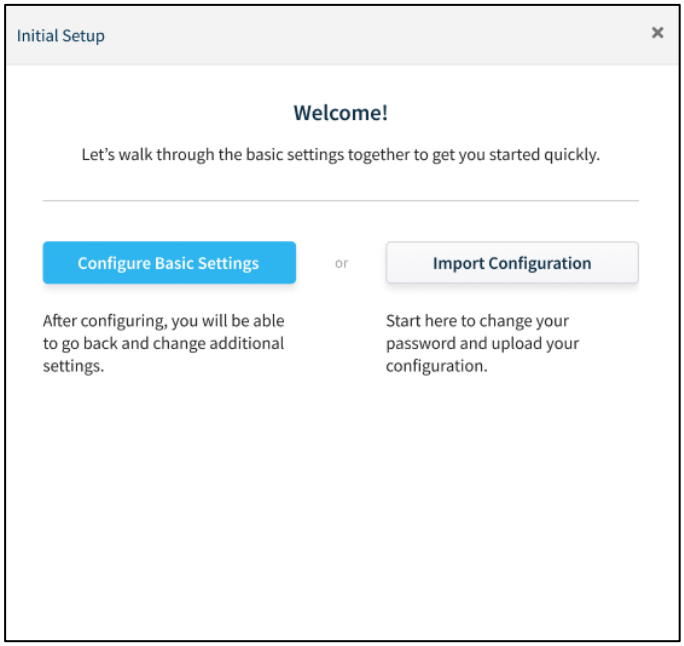
ii. Enter the new login credentials.

> **NOTE:** The password must be minimum 8 characters, including one lowercase character, one uppercase character, one special character, and one number.

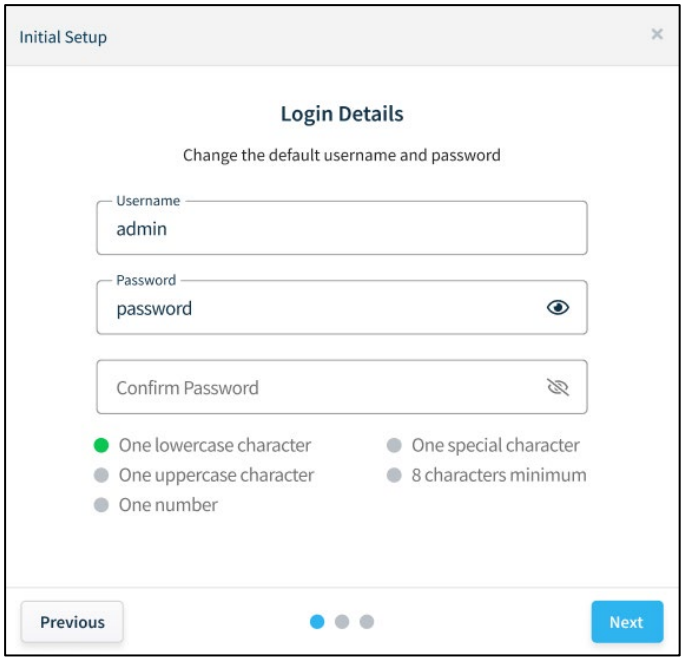
iii. Click **SAVE** to save the changes.

B. **Configure Basic Settings**: To perform basic configuration settings:

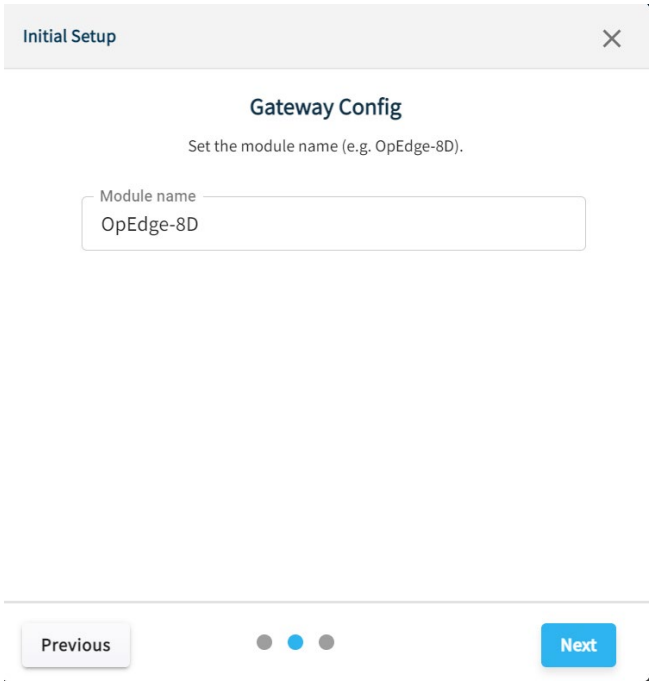
i. In the *Initial Setup* dialog, click **CONFIGURE BASIC SETTINGS**.



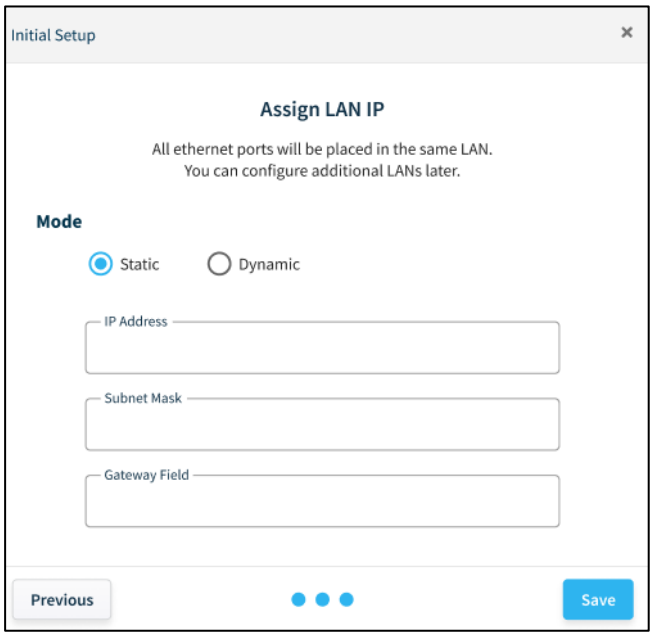
ii. In the *Login Details* dialog, change the default login credentials and click **NEXT.**



iii. In the *Gateway Config* dialog, provide the module name. Click **NEXT.**



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



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

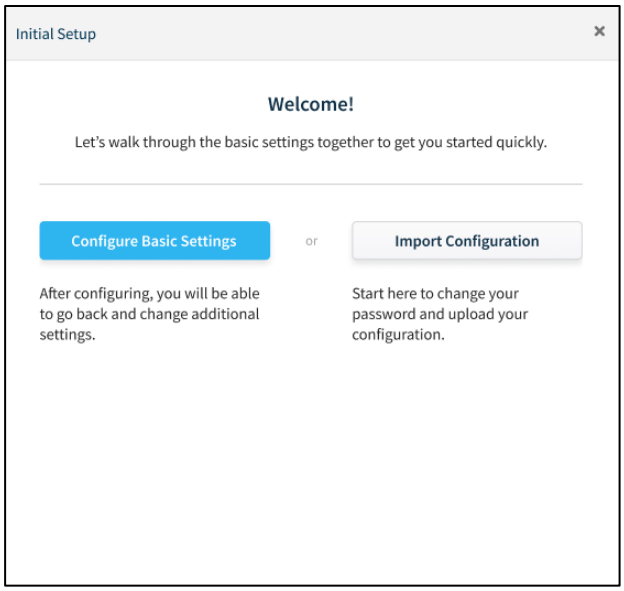
C. **Import Configuration**:

NOTE: For information on exporting the configuration to a *.tar.gz* file, please see page 22.

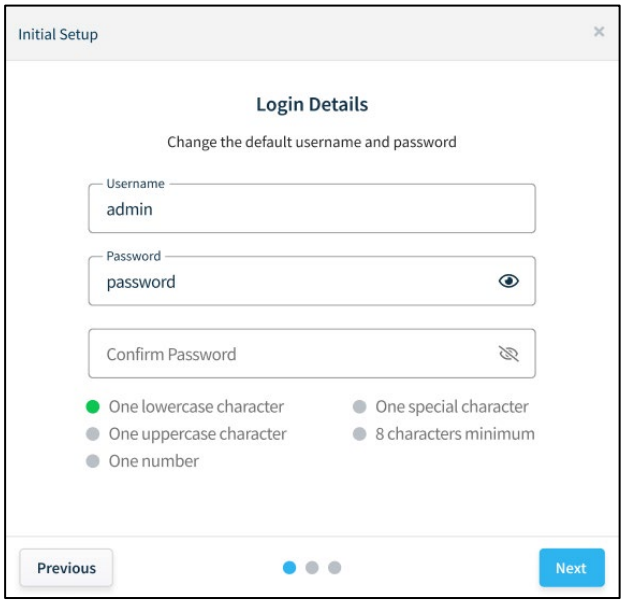
NOTE: During the initial module configuration, the default Username and Password must be changed.

To import a configuration file:

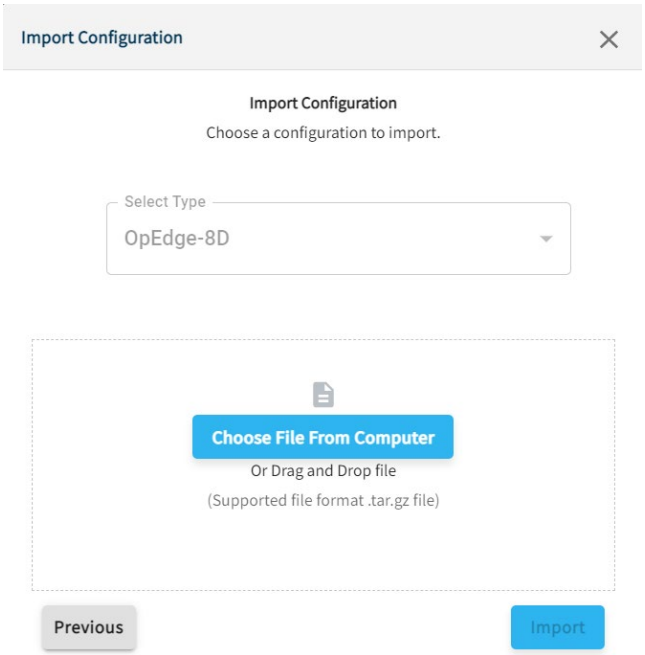
i. In the *Initial Setup* dialog, click **IMPORT CONFIGURATION**.



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



iii. 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.

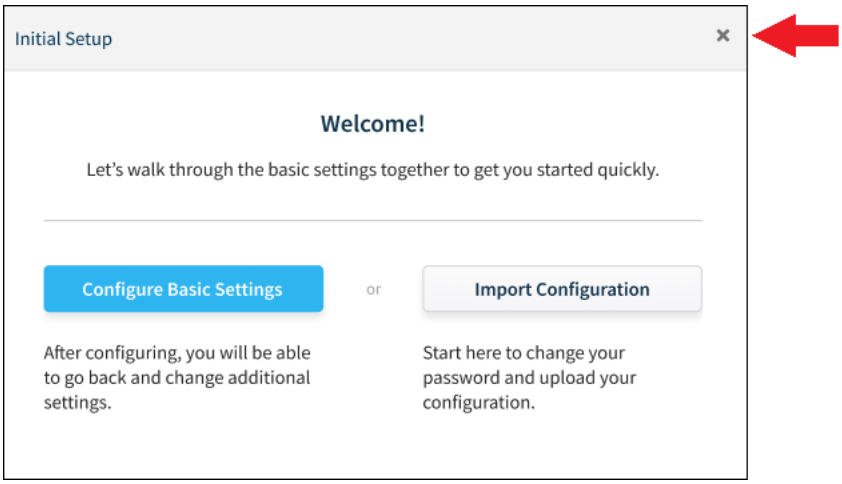


iv. Click **IMPORT** to import the selected configuration file.

D. **Exit from Initial Setup Dialog to Manually Configure**:

NOTE: During the initial module configuration, the default Username and Password must be changed.

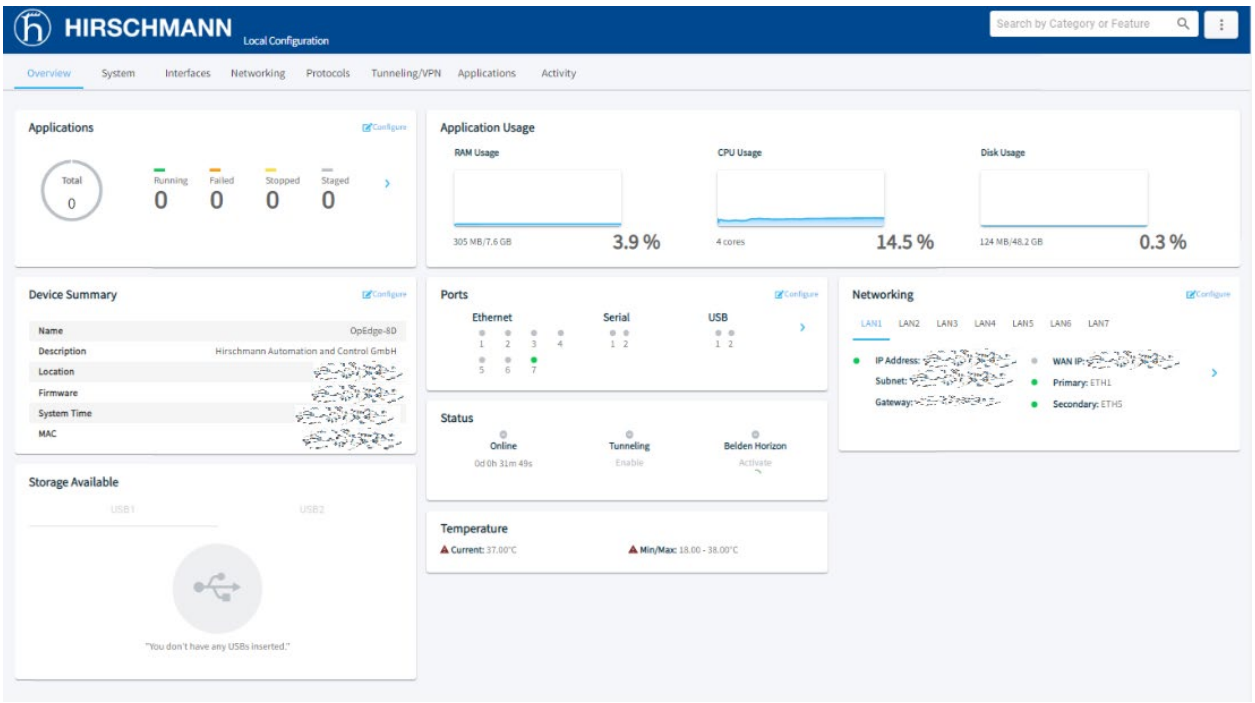
i. Click '**X**' to bypass the initial setup process.



ii. Log in to the OpEdge.

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

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



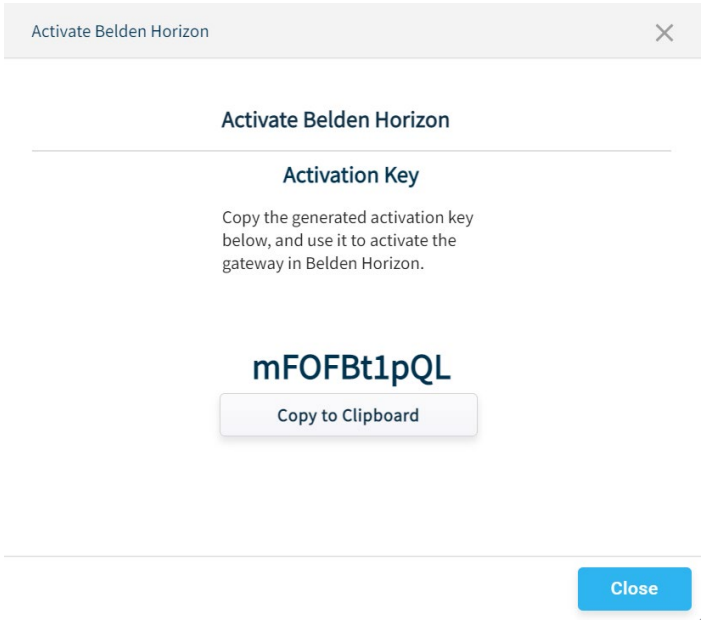
NOTE: The status of each parameter will vary.

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

3 Registration in Belden Horizon

Belden Horizon is a secure and intuitive cloud-native platform. It supports multiple applications like on-demand (secure machine access) or always-on (persistent data network) connectivity, data monitoring, and alert notification. The OpEdge can be managed in Belden Horizon once registered. This includes making configuration changes and scheduling firmware changes.

Before using the OpEdge, it must be registered in Belden Horizon by entering an Activation Key.



3.1 Registration Using Activation Key

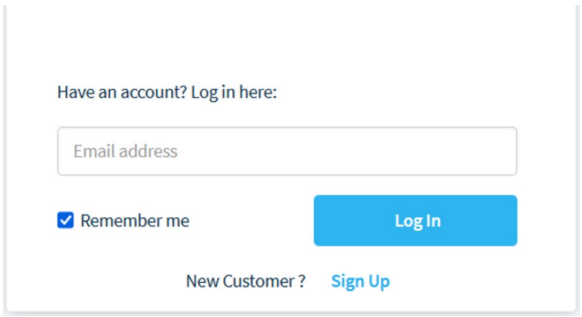
Use the following procedure to obtain the activation key from the OpEdge, and to register the OpEdge with Belden Horizon:

NOTE: The OpEdge must be connected to the Internet through the WAN port. See *WAN Configuration* on page 39 for more details.

1. Establish a default connection to the OpEdge and perform the initial setup as described in the *Initial Configuration* section on page 8.
2. In the *Overview* tab > *Status* tile, click the **ACTIVATE** link under the *Belden Horizon* label.

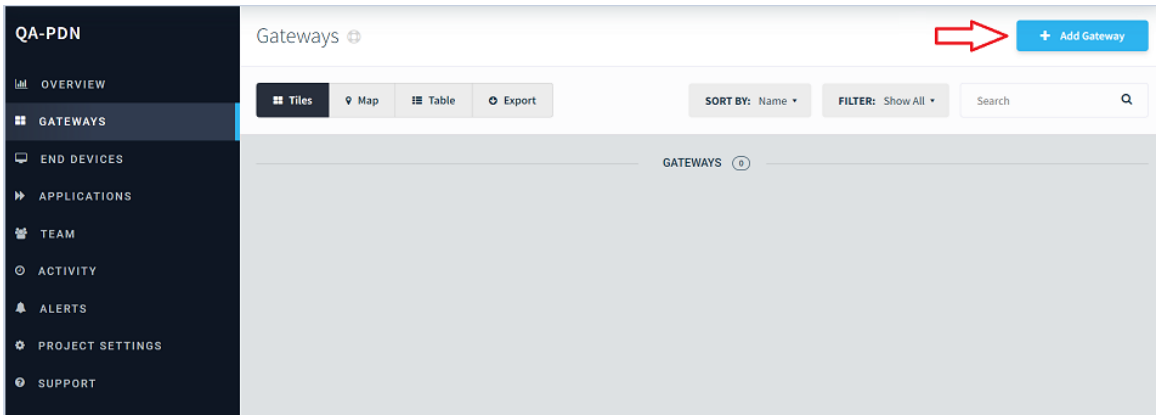
NOTE: If the OpEdge is already connected to a Belden Horizon account, the link reads “Deactivate”.

3. The OpEdge securely retrieves an alphanumeric activation key from Belden Horizon that is only 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 press **ENTER**.
5. On the *Belden Horizon Login* screen, enter the Belden Horizon login email and click **LOG IN**, or click **SIGN UP** to create a new account. Login credentials are not interchangeable between Belden Horizon and the webpage.

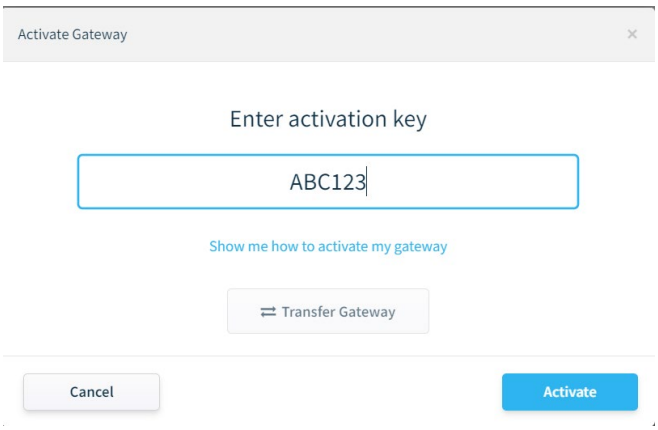


6. Once logged in, follow the prompts to create a project.

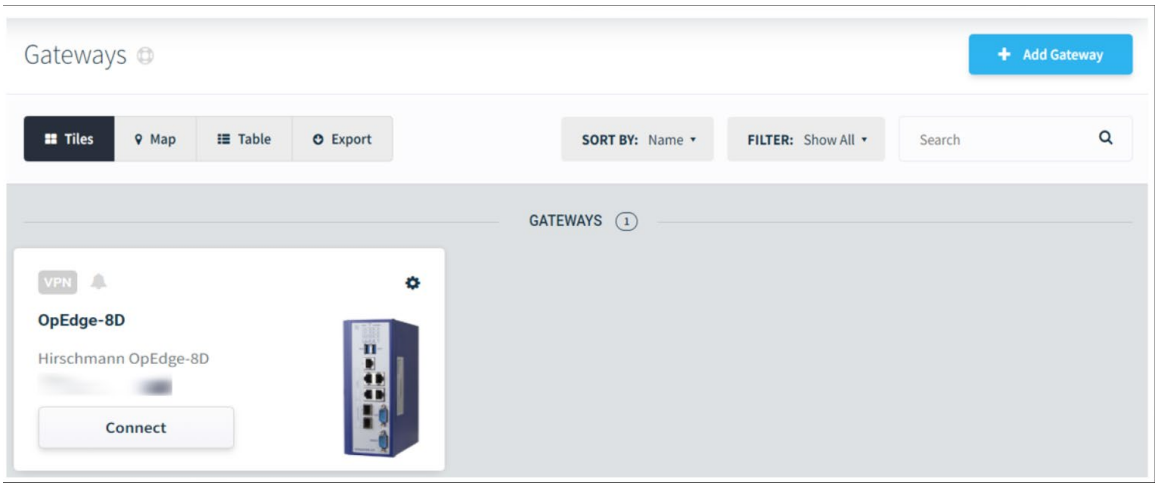
7 Click the *Gateways* tab, and then click **ADD GATEWAY**.



8 The user will be prompted for the activation key recorded earlier. Click **ACTIVATE**.



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



3.2 Activation Errors

The following error messages correspond to failed registration issues:

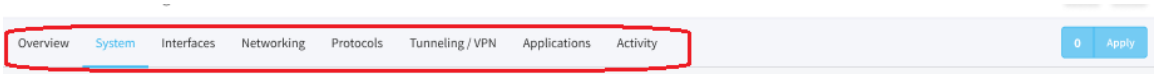
Error	Description	Solution
Key is corrupted.	The key is invalid.	Please make sure this is the correct key.
Device Activation record was found for activation key.	Failed to find an activation record in the Belden Horizon database.	Please try another activation key.
Found a Device Activation record in 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 Overview

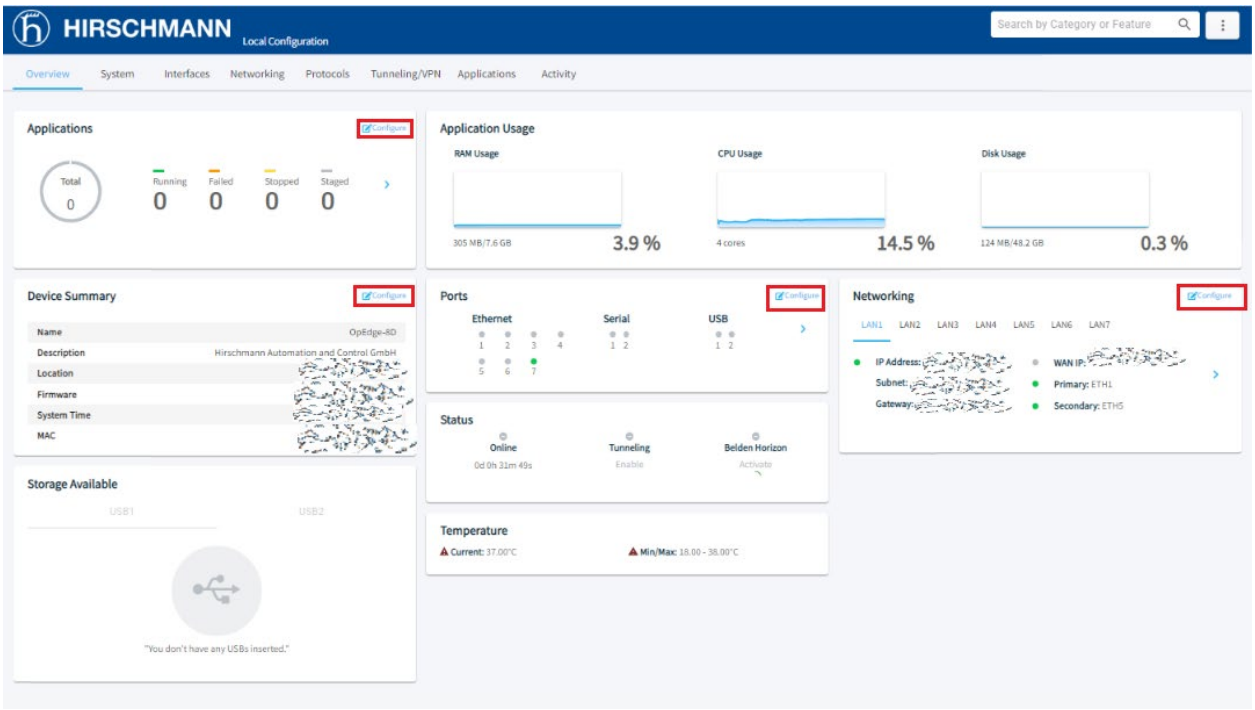
4.1 OpEdge Webpage Navigation

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

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

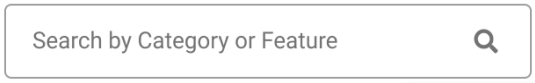


- From the **CONFIGURE** link in each tile of the *Overview* tab.



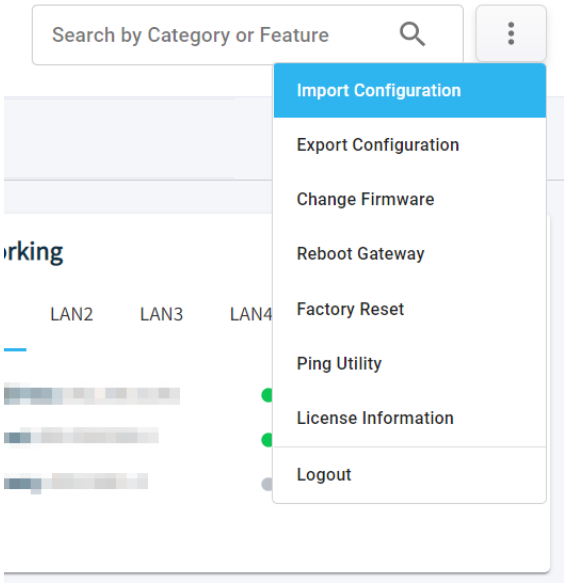
4.1.1 Search Bar

The search bar allows user to navigate to a specific configuration by searching a keyword in the search box.



4.1.2 […] Button

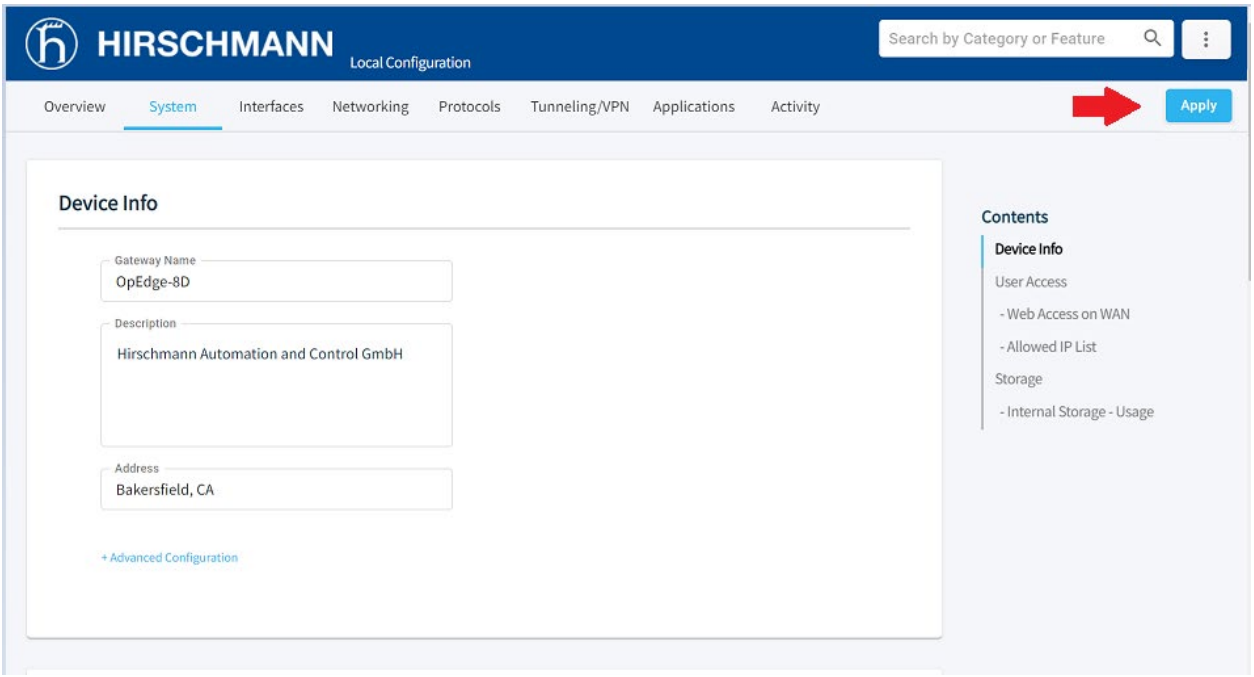
The ⋮ button includes additional options for the OpEdge.



Parameter	Description
Import Configuration	Imports an OpEdge configuration.
Export Configuration	Exports an OpEdge configuration.
Change Firmware	Updates the OpEdge firmware.
Reboot Gateway	Reboots the OpEdge.
Factory Reset	Resets the OpEdge settings to default configuration.
Ping Utility	Tests internet connection.
License Information	Information about the present licenses.
Logout	Logs out the current user.

4.1.3 Apply Button

The *Apply* button is used to send the current configuration to the OpEdge.



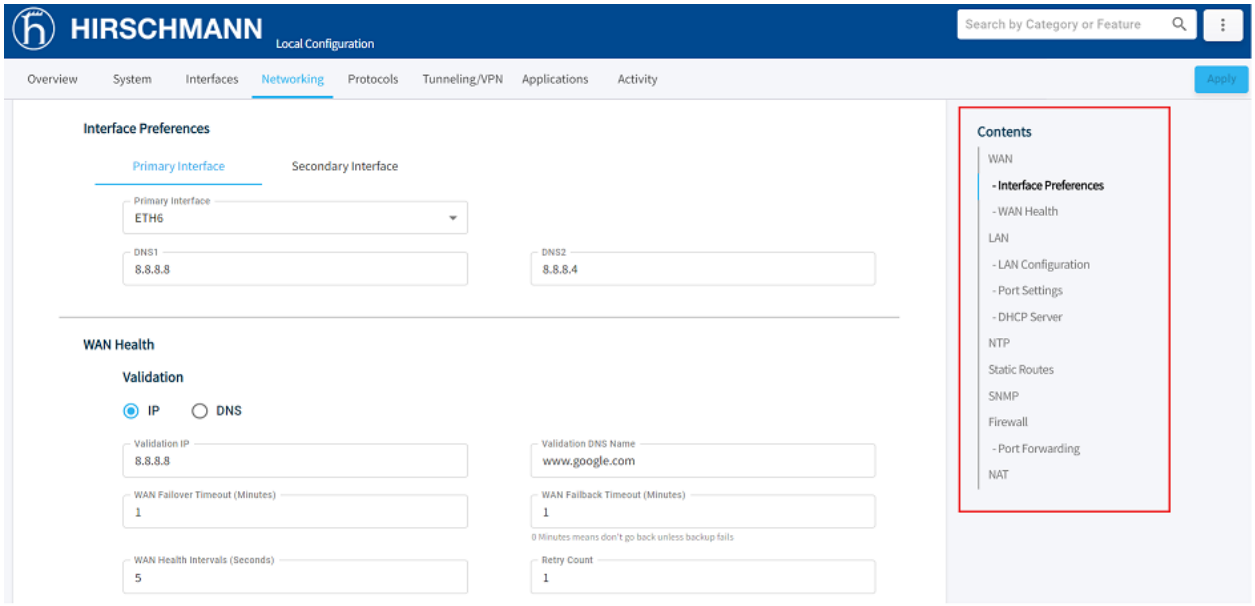
4.1.4 Sidesheet Launcher

Within the configuration tiles, the › icon expands the menu to display additional details.

Example:

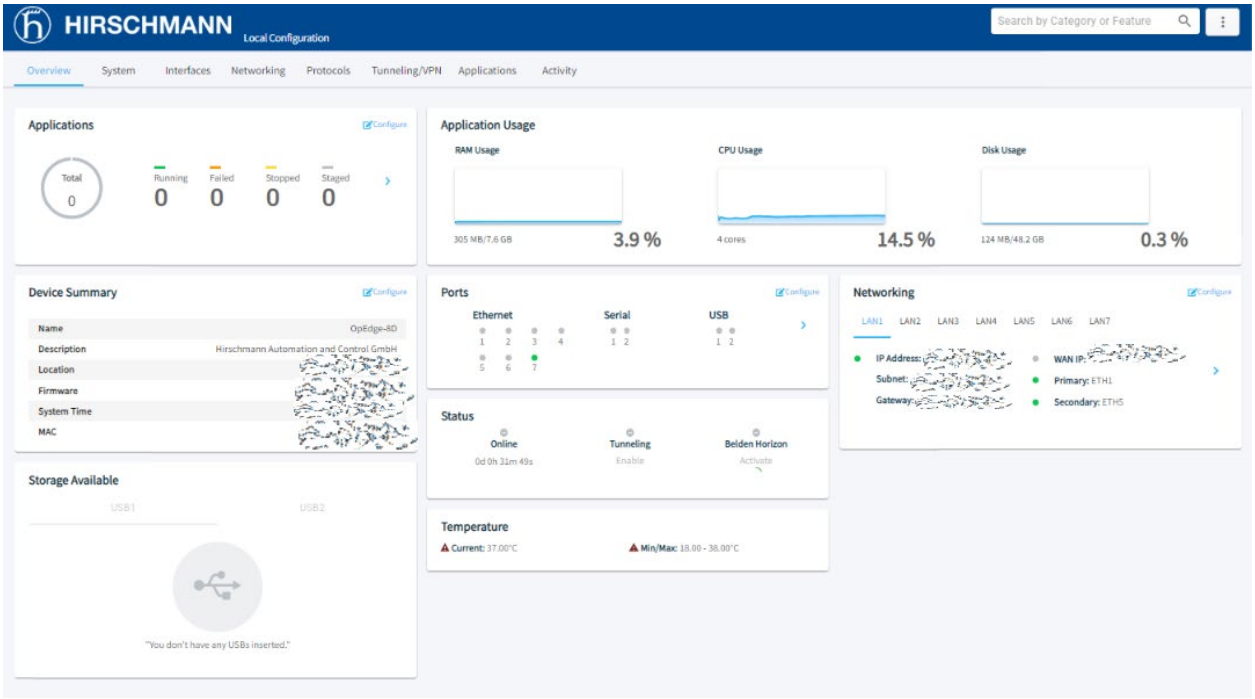
4.1.5 Side Menu Scrolling

The scrolling menu within each tab can be used to quickly jump to each parameter.



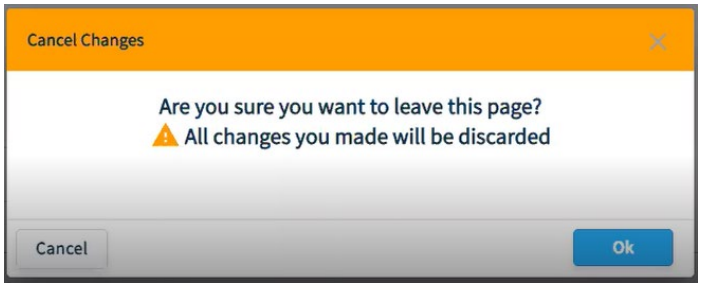
4.2 Overview Tab

Use the *Overview* tab to view details of the device status, storage, networking interface, and ports.



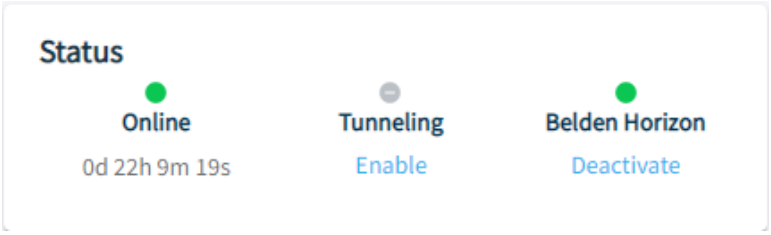
Additionally, click **CONFIGURE** to open the configuration option for a specific tile.

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

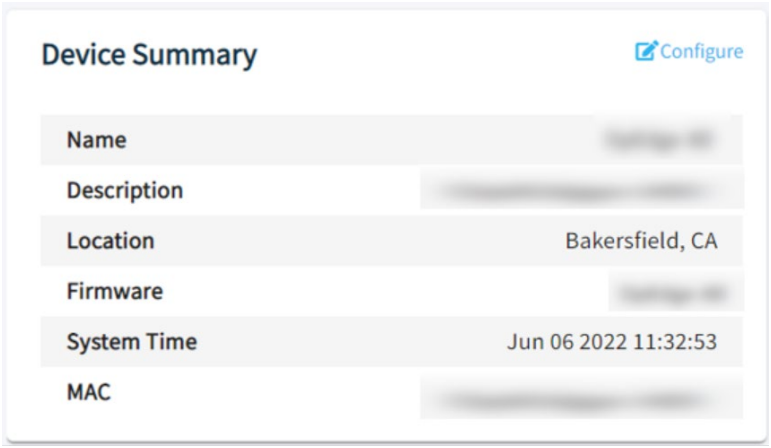
The *Status* tile displays the following device status parameters:



Parameter	Description
Online	The current status of the OpEdge: **Online** (Green) **Offline** (Grey) **Note:** The status will be Online only if WAN is connected.
Tunneling	The icon displays the current Belden Horizon tunneling status of the OpEdge. 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 OpEdge status in Belden Horizon. **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.

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.
Location	Location of gateway configured by user.
Firmware	Current firmware version loaded on the OpEdge.
System Time	Date and time in UTC format.
MAC	OpEdge MAC Address.

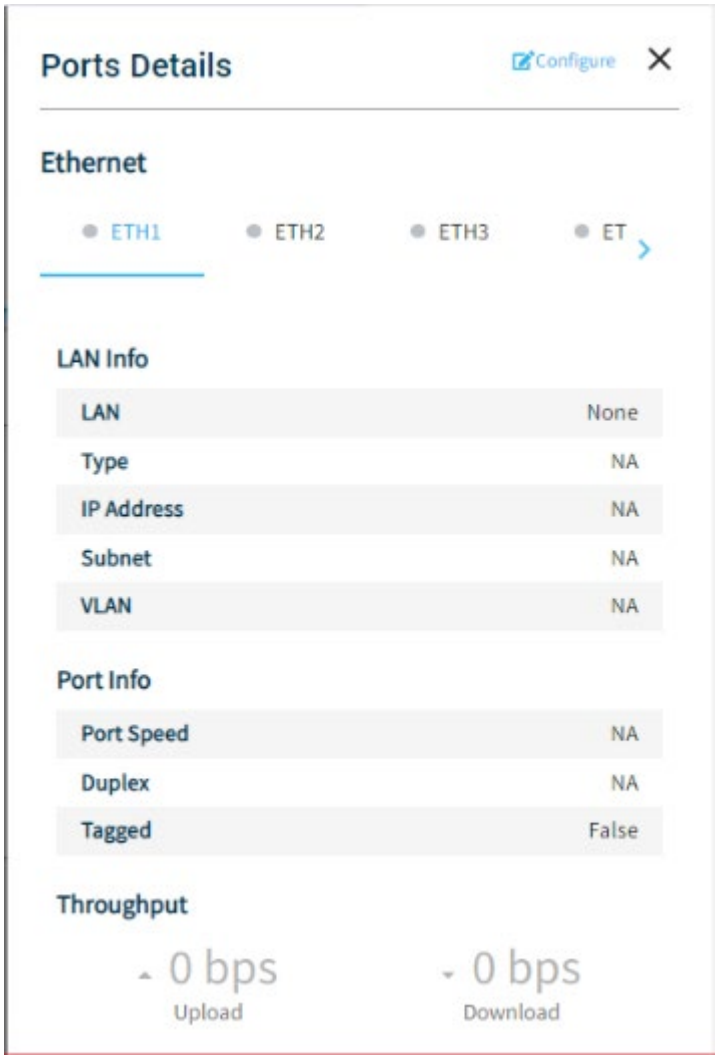
4.2.3 Ports

The *Ports* tile displays indicators for the Ethernet ports on the OpEdge.

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



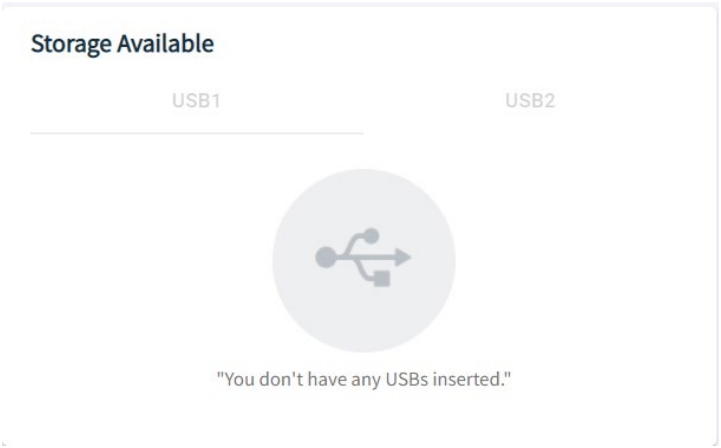
Parameter		Description
Ethernet	ETH1 ETH2 … ETH7	Green = Port is configured and communicating. Grey = Port is not configured. Yellow Triangle = Port is configured but no communications, or no cable detected.
LAN Info	LAN	LAN configuration assigned to the port.
	Type	Type of mode, dynamic or static.
	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

View the current, minimum and maximum operating temperature of the OpEdge.

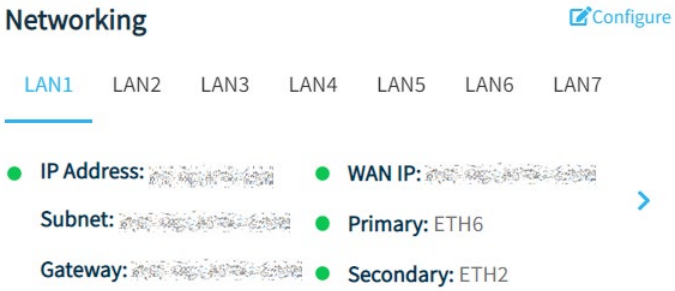
4.2.5 Storage Available

View the amount of free storage space on the external USB device.



4.2.6 Networking

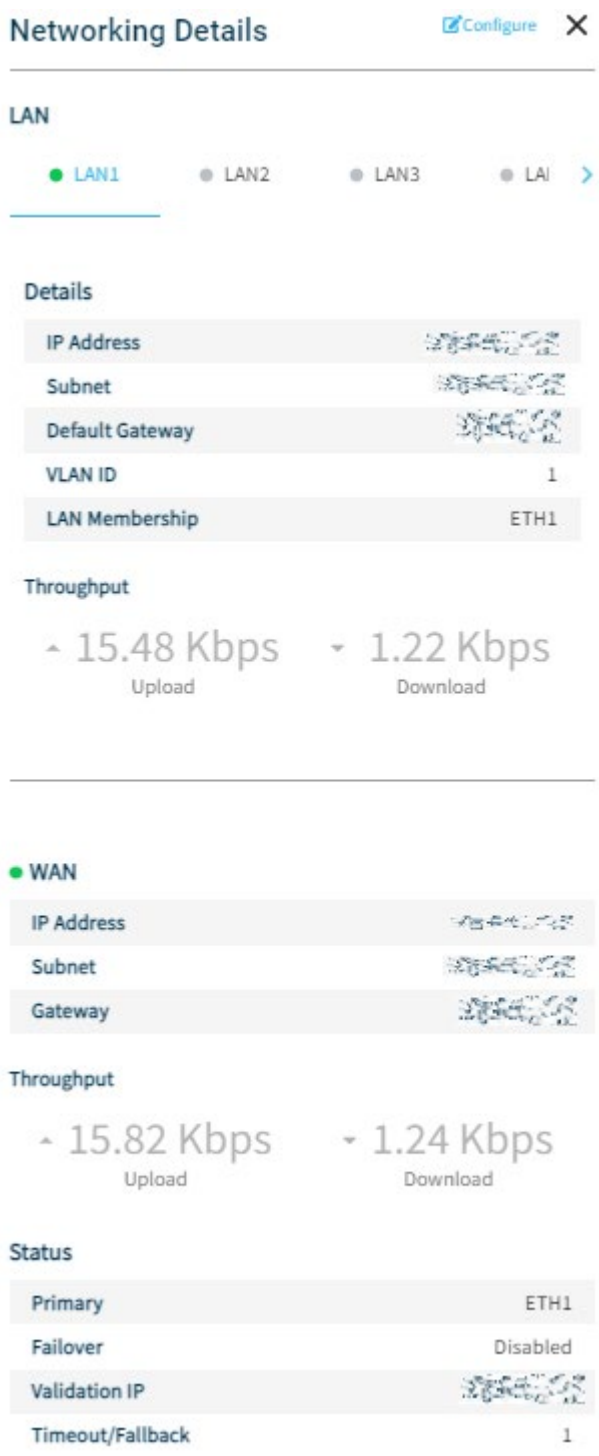
The *Networking* tile displays the LAN and WAN configurations for OpEdge.



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.

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



Click the **LAN1** to **LAN7** 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.

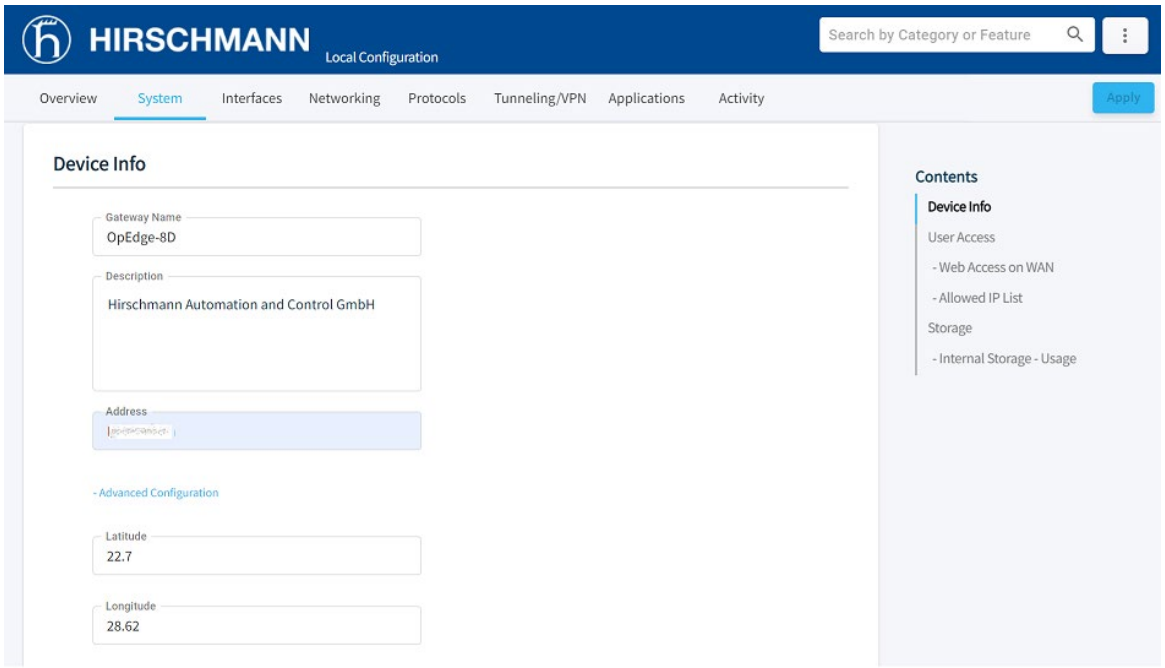
5 Configuring the OpEdge

5.1 System Tab

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

5.1.1 Device Info

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



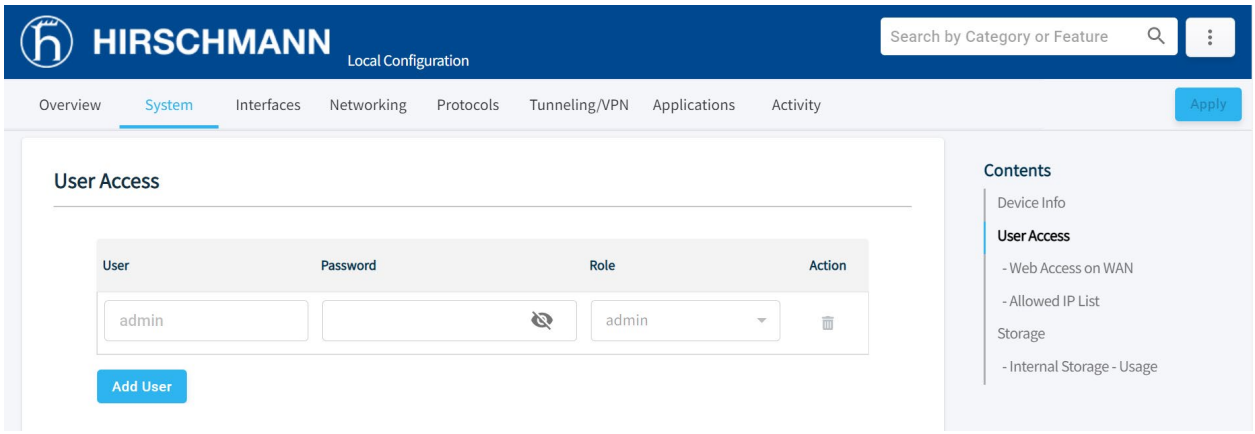
Parameter	Description
Gateway Name	Name of the device.
Description	Brief description of the device.
Address	Address of the device.
Latitude	Latitude coordinate.
Longitude	Longitude coordinate.

5.1.2 User Access

The OpEdge allows managing user access to the device WAN. The OpEdge configuration webpage allows adding users (up to 8) and assigning different roles to these users for limiting their access.

The following types of roles are assigned to a user:

- **Admin**: Includes complete user privileges. An admin can do any desired change. Maximum two admins are allowed.
- **Viewer**: Includes permissions to view the configurations and to monitor the gateway and activity feed. A viewer cannot change any configuration.



Use the following steps to add a new user:

1 Open the OpEdge configuration webpage and click the *System* tab.

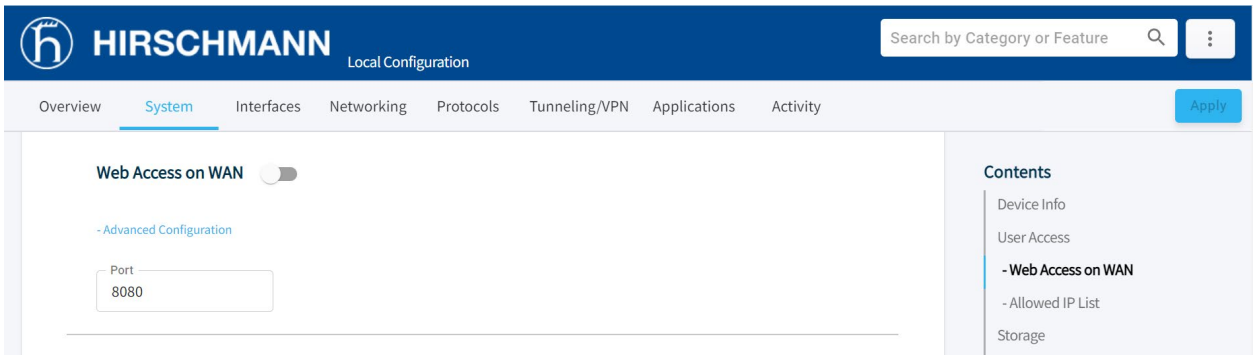
2 Under *User Access*, enter the following parameters:

Parameter	Description
User	User name to be defined.
Password	Default password for the user account. **Note:** The user name 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* (read only)

5.1.2.1 Web Access on WAN

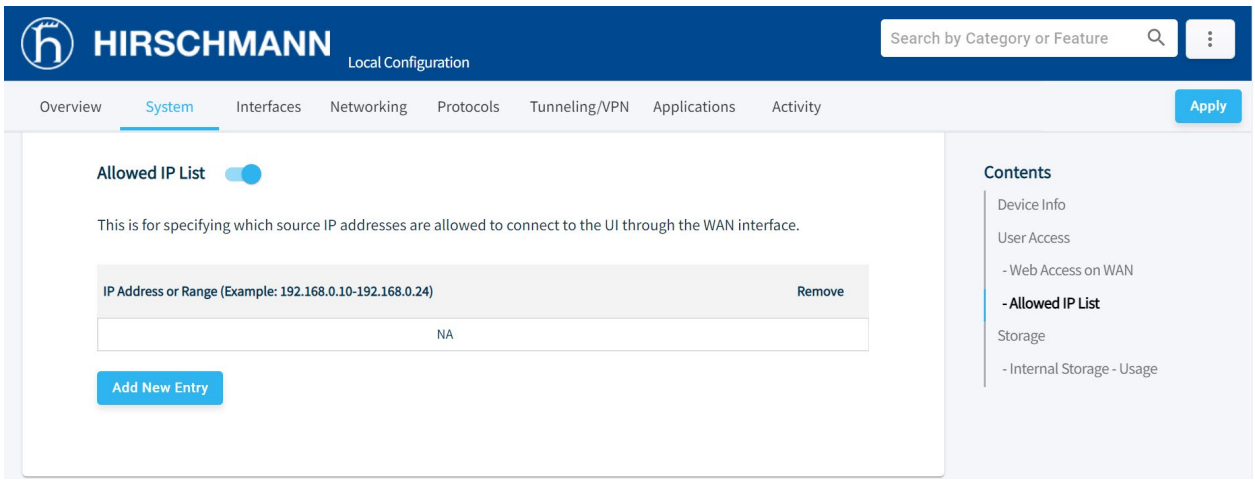
This feature allows or blocks webpage access on the WAN.

Warning: Belden Horizon currently uses port 443 to tunnel. Selecting port 443 will prevent Belden Horizon from functioning properly. HTTPS can function properly using port 8080 or other ports.



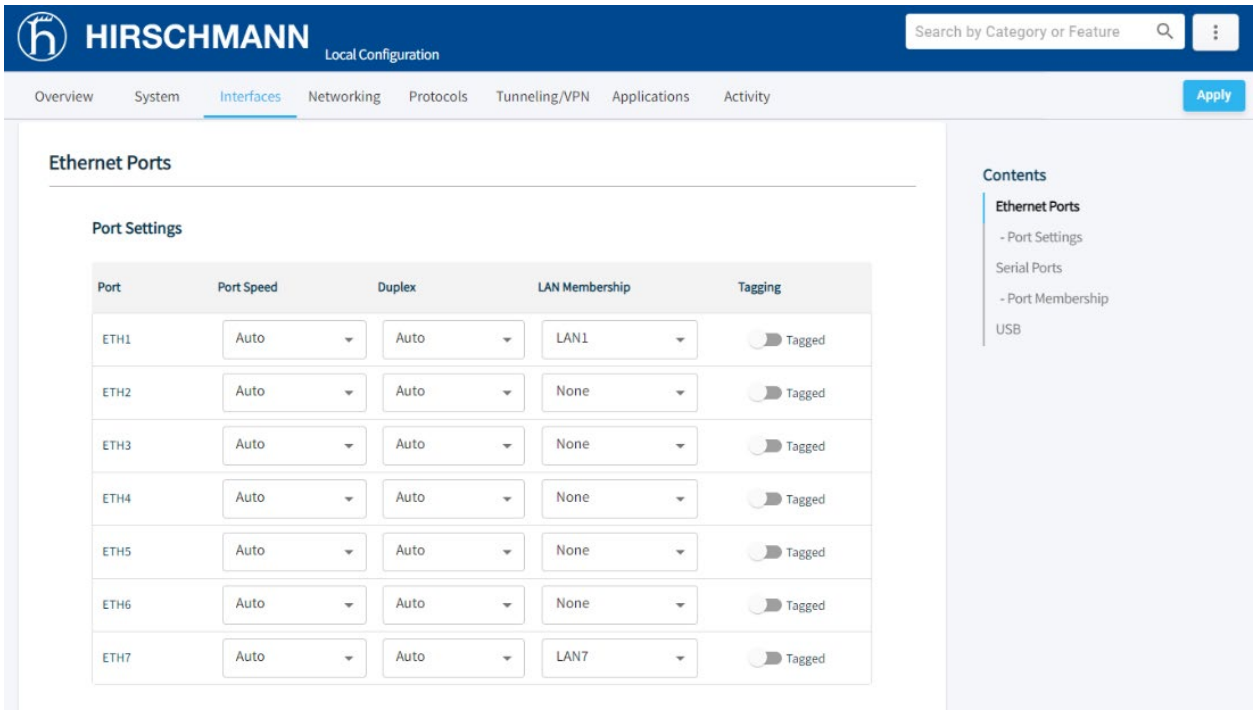
5.1.2.2 Allowed IP List

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



5.2 Interfaces Tab

The *Interfaces* tab is used to configure the Ethernet ports on the OpEdge.



5.2.1 Ethernet Ports

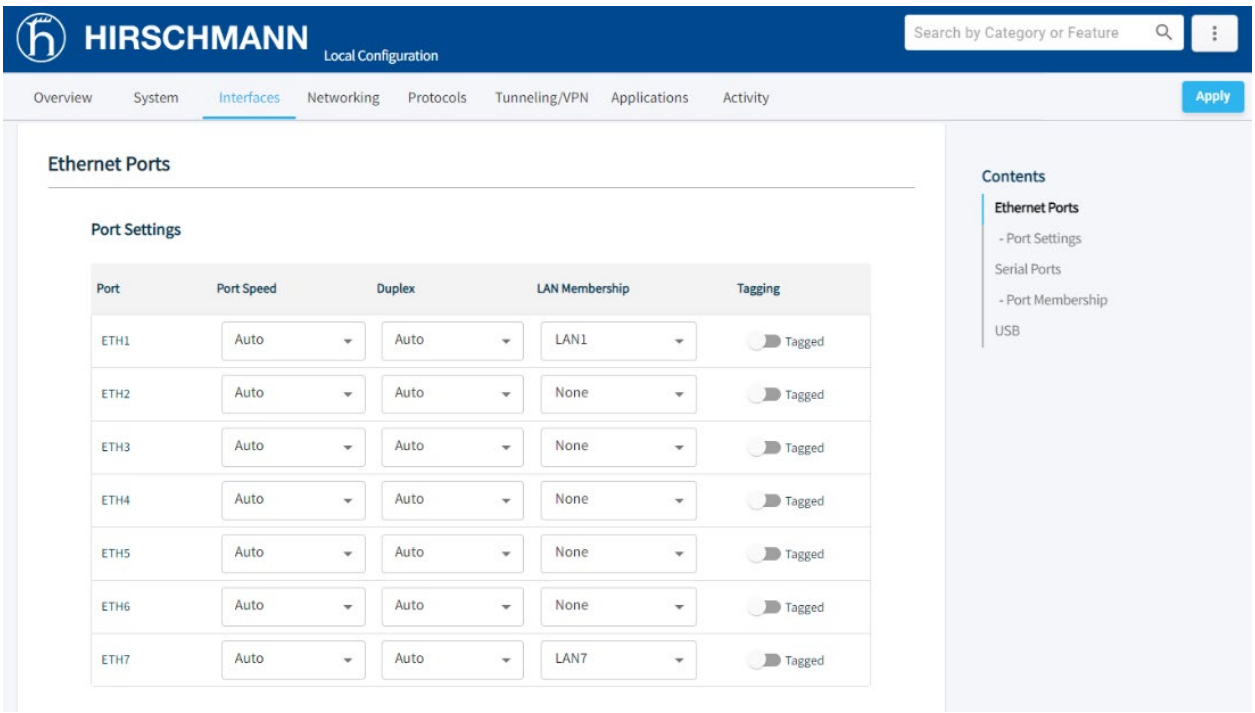
The OpEdge configuration webpage allows configuring seven Ethernet ports on the module and assigning specific LAN configurations. Additionally, the OpEdge can be configured as a DHCP server for end devices.

The configuration options for OpEdge Ethernet ports include speed, duplex mode, LAN membership, and tagging.

To configure an Ethernet port on OpEdge:

1 Click the *Interfaces* tab on the OpEdge configuration webpage.

2 Under *Port Settings*, provide the following details:

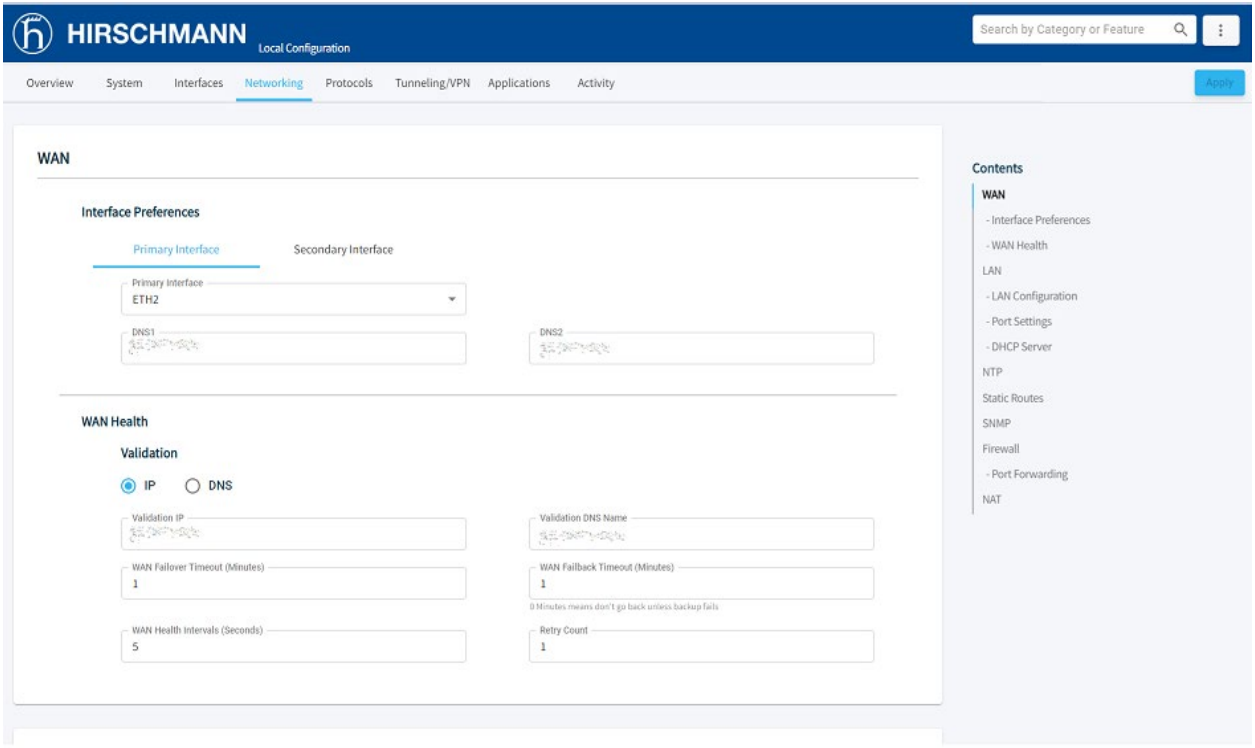


Parameter	Description
Port	OpEdge Ethernet port number: **ETH1** to **ETH7**
LAN Membership	LAN configuration to be assigned to the port. More information is detailed in the *LAN Configuration* in section 5.3.2.

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

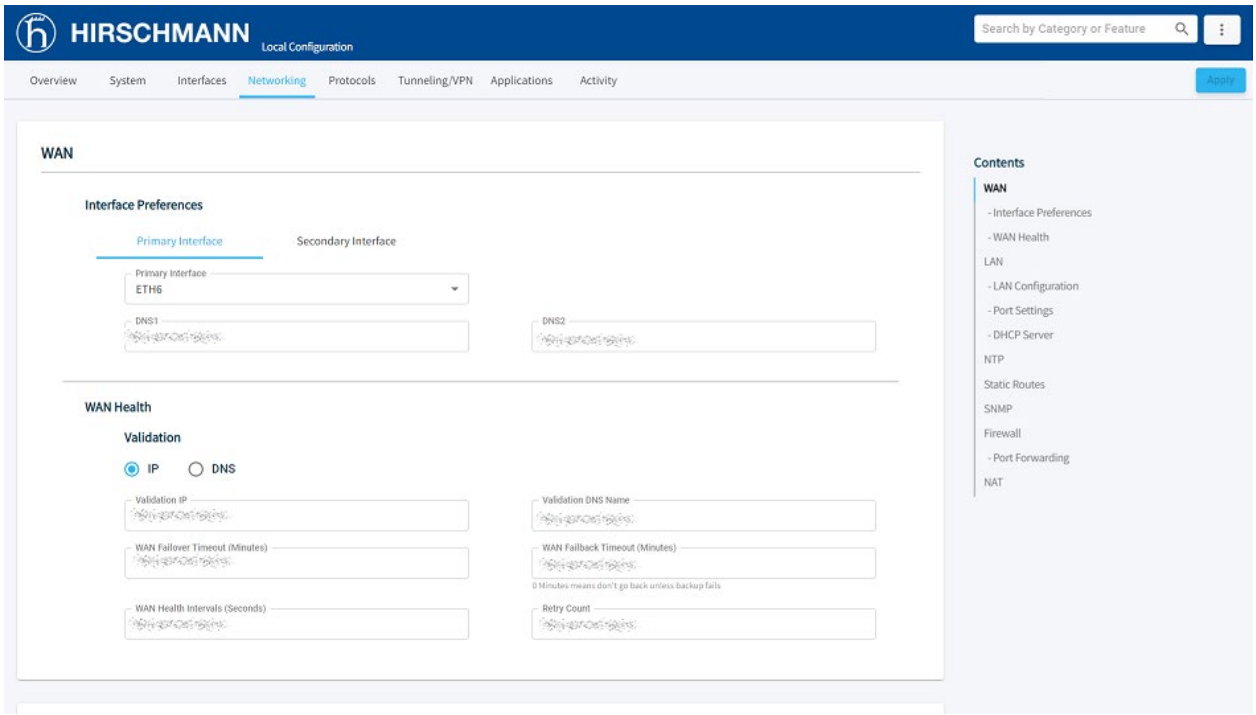
5.3 Networking Tab

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



5.3.1 WAN Configuration

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 seven LAN ports. WAN interface is disabled when LAN is enabled.

5.3.1.1 WAN Interface Preferences

Parameter	Description
Primary or Secondary Interface	ETH1 to ETH7 **Note:** The ETH**x** port must be assigned to a specific LAN configuration. More information is detailed in the *LAN Configuration* section 5.3.2.
DNS1 and DNS2	DNS IP's assigned by the user.

5.3.1.2 WAN Health

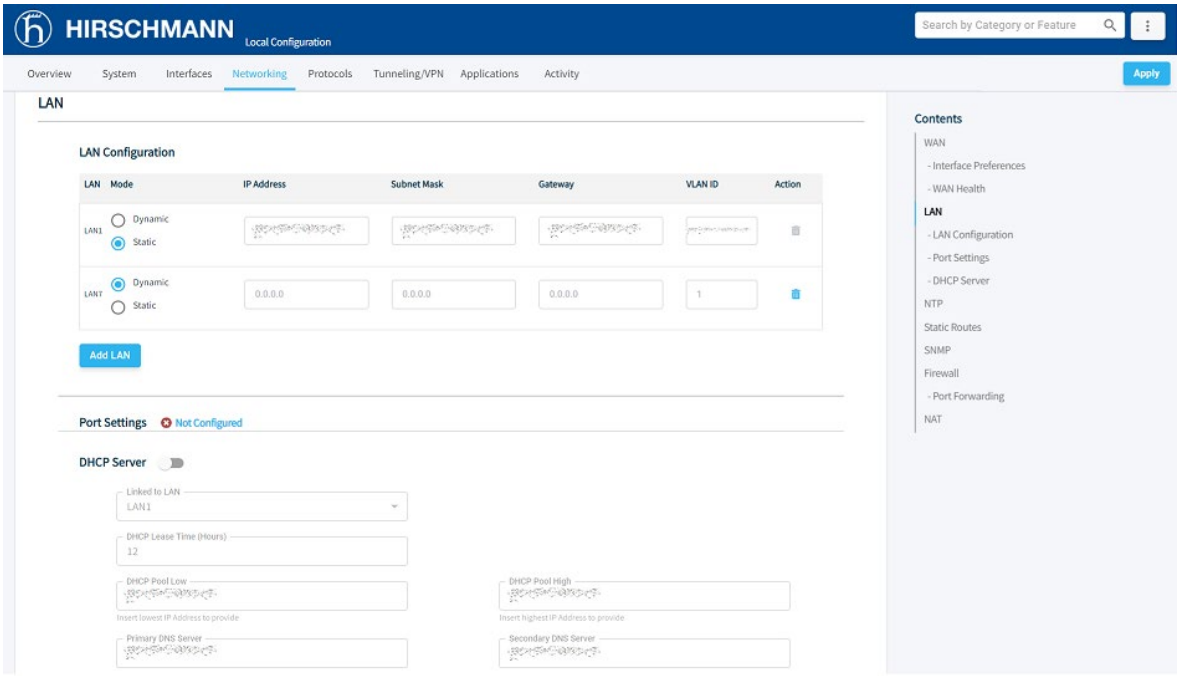
Parameter	Description
Validation IP	The system will ping the IP and confirm if the WAN network is operational.
Validation DNS Name	The system will ping the DNS and confirm if the WAN network is operational.
WAN Failover Timeout	The failed timeout, in minutes, after which primary network will be switched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

5.3.2 LAN Configuration

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

To create a LAN configuration:

1 Click the *Networking* tab on the OpEdge configuration webpage.



2 Under **LAN Configuration**, click the **ADD LAN** button.

> **Note:** The user can add a maximum of seven LAN ports.

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

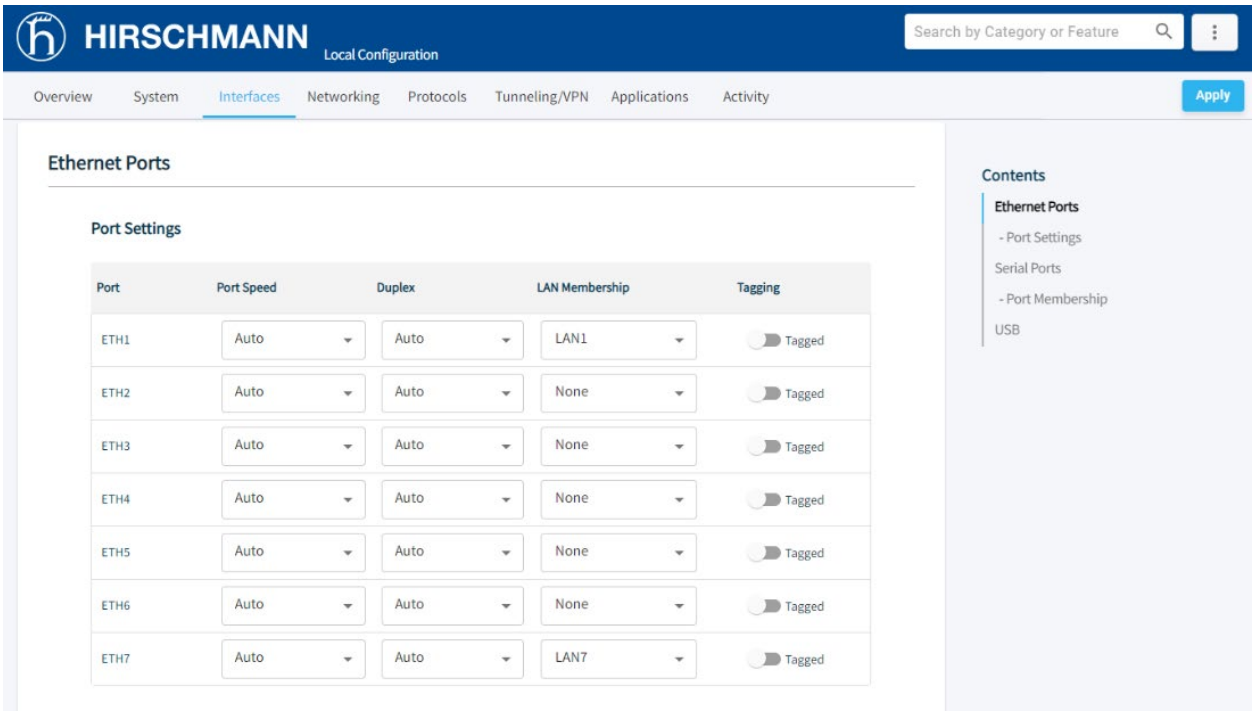
For **STATIC** configuration, enter the following parameters:

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

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

5 To assign a LAN Configuration to a specific OpEdge Ethernet port, click the *Interfaces* tab.

6 Under *Ethernet Ports* > *Port Settings*, assign the *LAN Membership* to the LANx configuration made in the previous section (*LAN Configuration* in section 5.3.2).



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

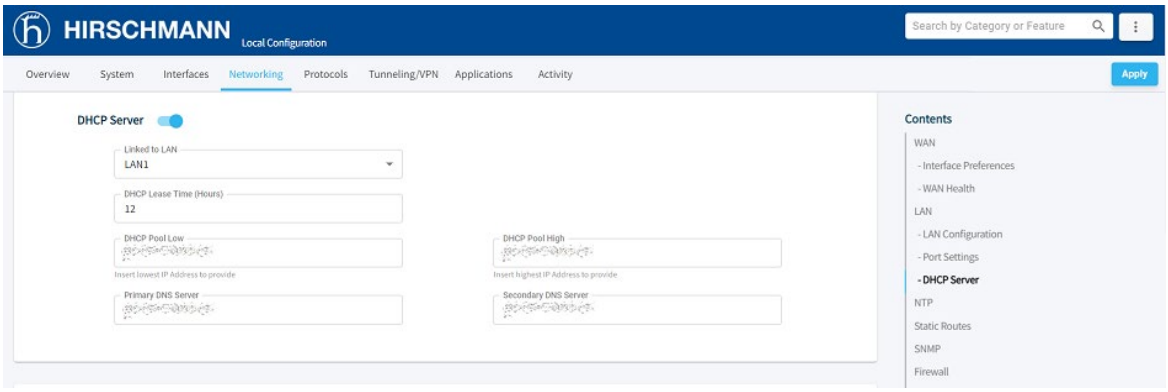
5.3.2.1 DHCP Server

The OpEdge 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 a 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 OpEdge:

1 Click the *Networking* tab on the OpEdge configuration webpage.



2 Click the **DHCP SERVER** toggle button to enable the *DHCP Server* configuration.

3 Enter the following values:

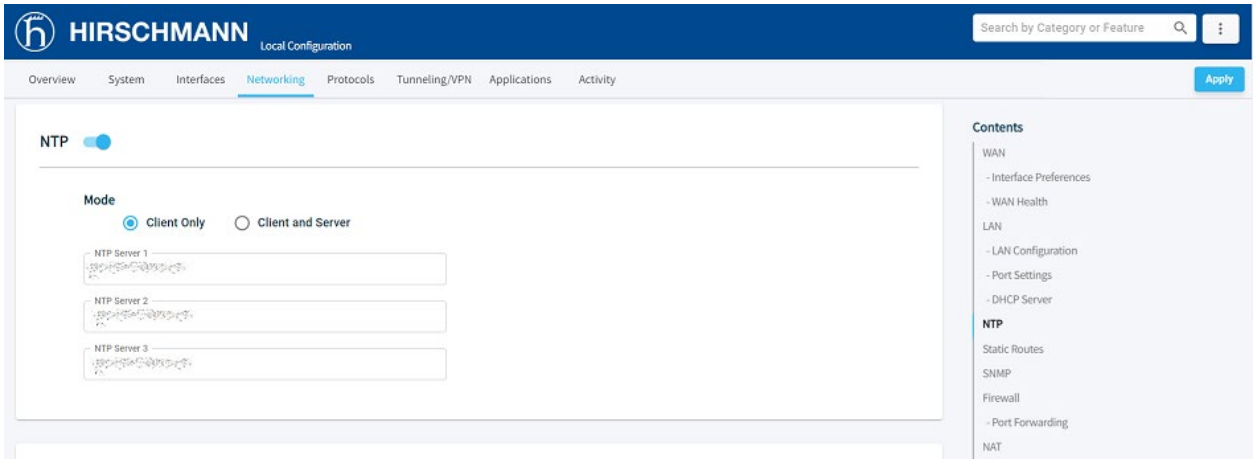
Parameter	Description
Linked to LAN	LAN port to be used to connect the end device to the network.
DHCP Lease Time	Lease period in hours (Range: 0 to 23)
DHCP Pool Low	Start of the range for the pool of IP addresses in the same subnet as the device.
DHCP Pool High	End of the range for the pool of IP addresses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

5.3.3 NTP

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

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

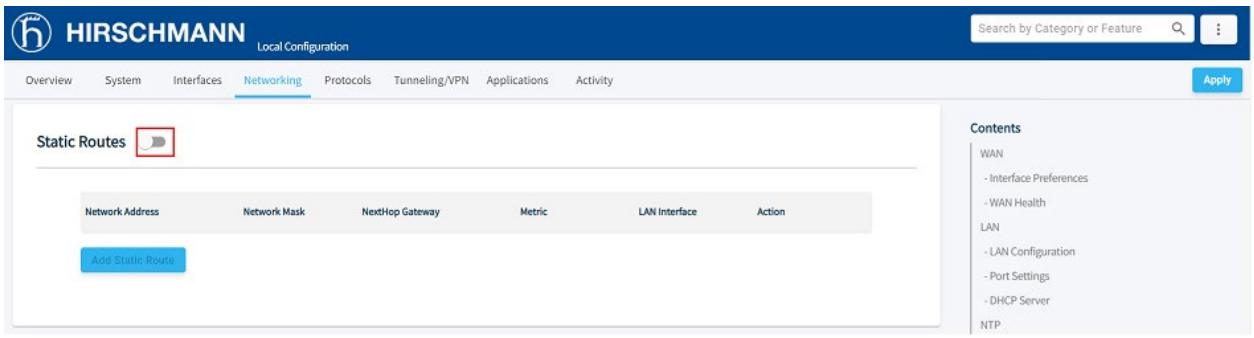


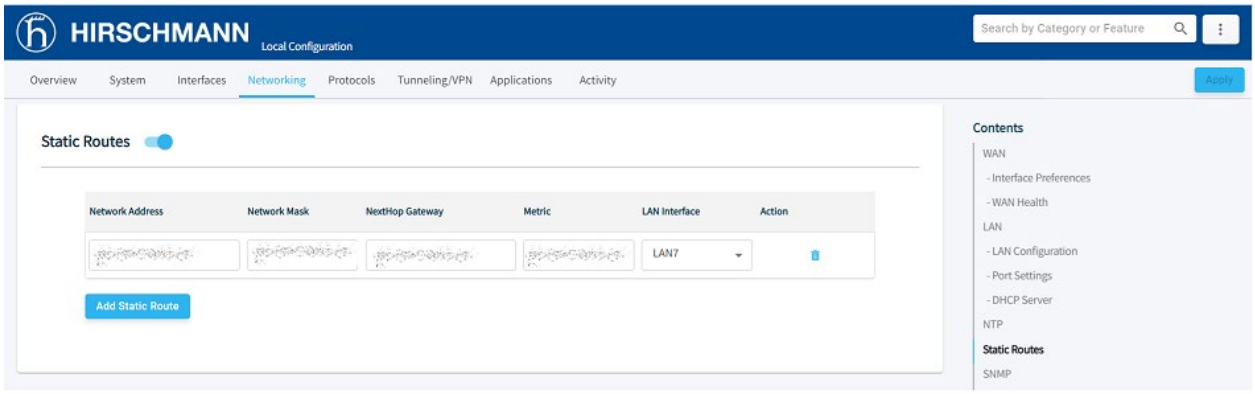
Parameter	Description
Mode	**Client Only** - NTP process will query NTP server and update OpEdge system time. **Client/Server** - NTP process will query NTP server and update OpEdge system time and resolve NTP requests from the LAN clients.
NTP Server 1, 2, 3	Server time updates for the OpEdge. Example: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

5.3.4 Static Routes

Static routing is a form of routing that occurs when a router uses a manually-configured routing entry, rather than information from dynamic routing traffic.

Click the **STATIC ROUTES** toggle button to enable the *Static Routes* configuration.





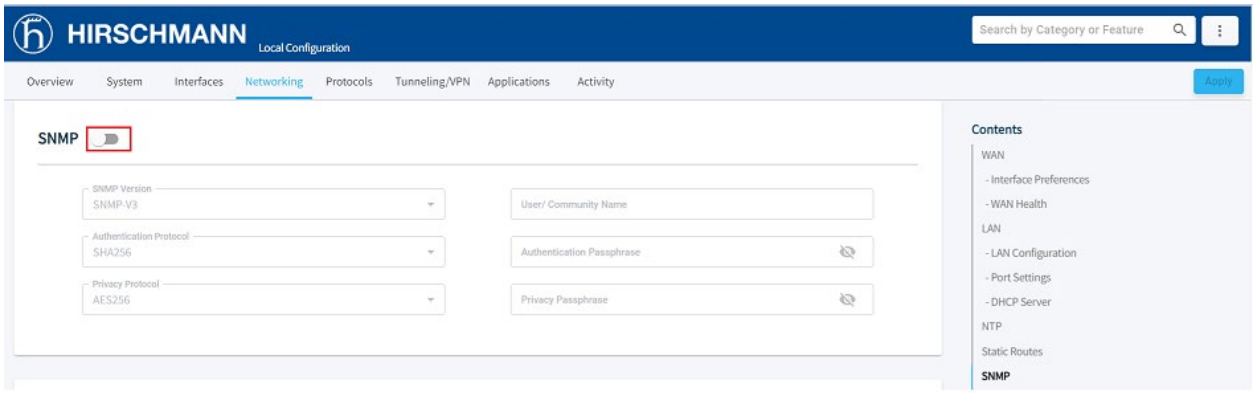
Parameter	Description
Network Address	IP Address of the network.
Network Mask	Subnet mask of the network.
NextHop Gateway	Nexthop gateway address.
Metric	Metric can be any positive 32 bit number. Default is **100**.
LAN Interface	Select from the available LAN interfaces where static route need to be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

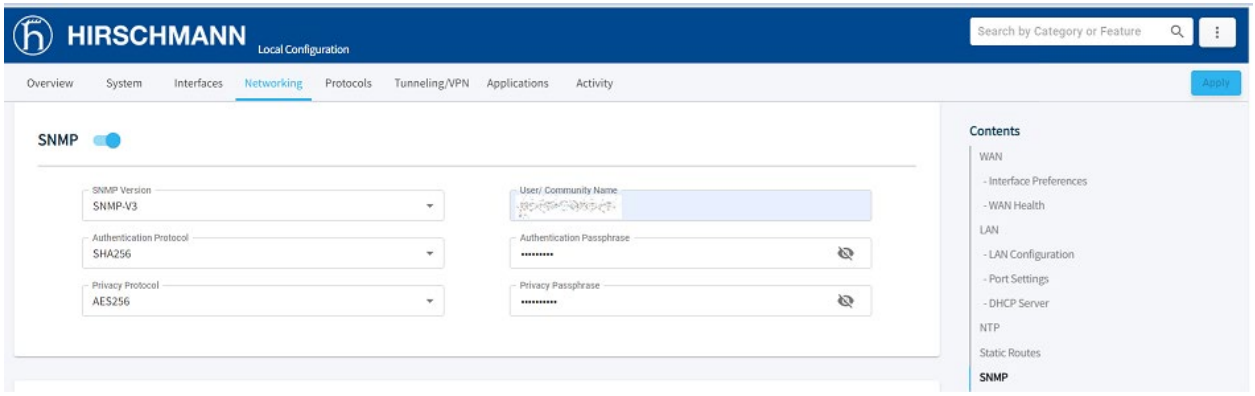
5.3.5 SNMP

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.



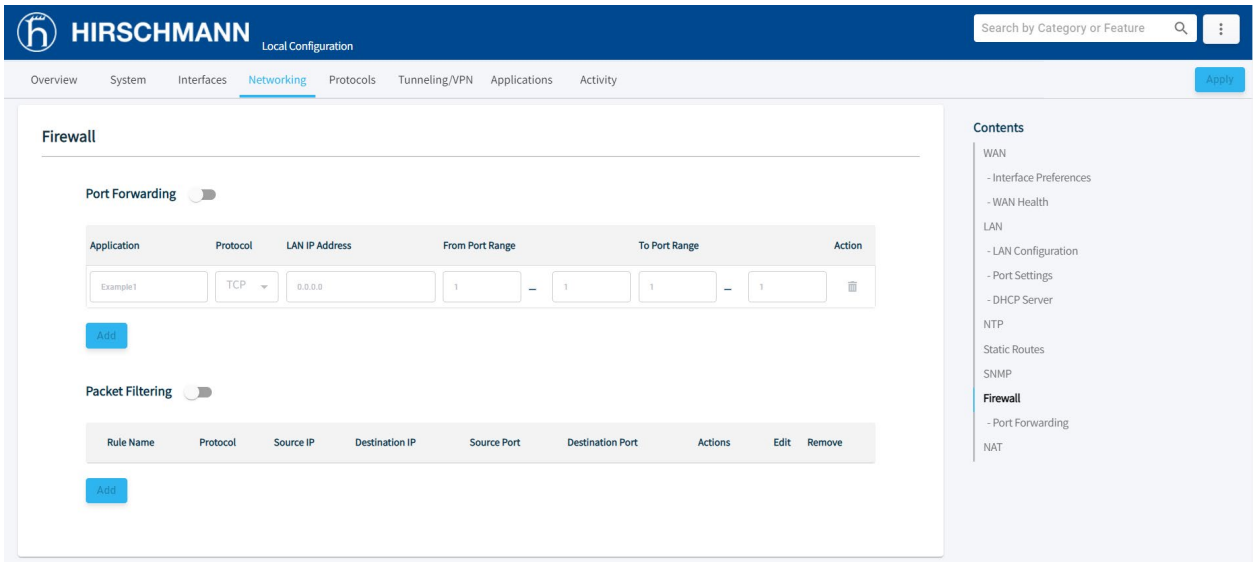


Note: The *User/Community Name* must be 5-20 characters alphanumeric. The *Authentication Passphrase* and *Privacy Passphrase* must be 8-20 characters alphanumeric.

Parameter	Description
SNMP Version	Version of SNMP which is preset to SNMP-V3.
Authentication Protocol	Protocol used for authentication which is preset to SHA256.
Privacy Protocol	Privacy protocol – Default: AES256.
User/ Community Name	User name to be provided by user.
Authentication Passphrase	Password required for authentication to be added by the user.
Privacy Passphrase	This is the password for privacy which needs to be provided by the user

5.3.6 Firewall

The OpEdge 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.

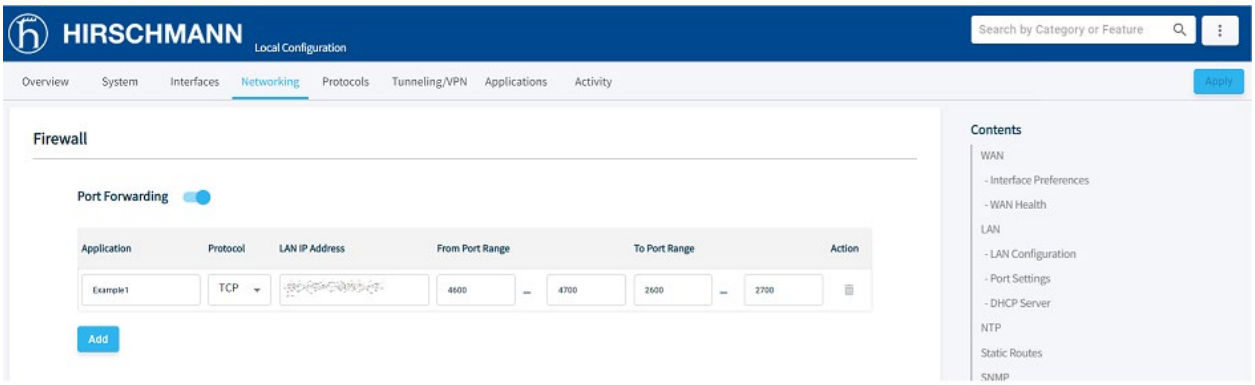


5.3.6.1 Port Forwarding

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

To configure Port Forwarding:

1. Open the OpEdge configuration webpage.
2. Click the *Networking* tab and toggle the **PORT FORWARDING** button.



3 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 OpEdge. The Gateway address on the end device must point to the OpEdge 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.

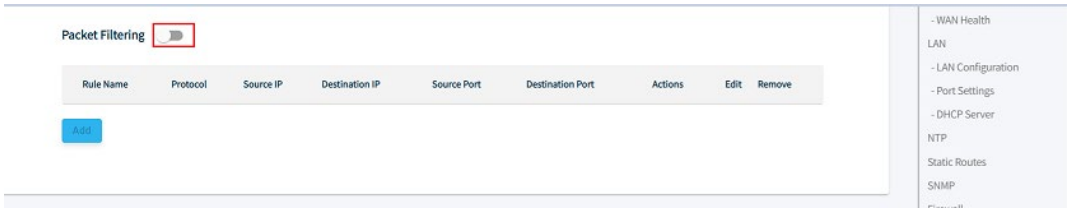
4 Click **ADD PORT** to add ports.

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

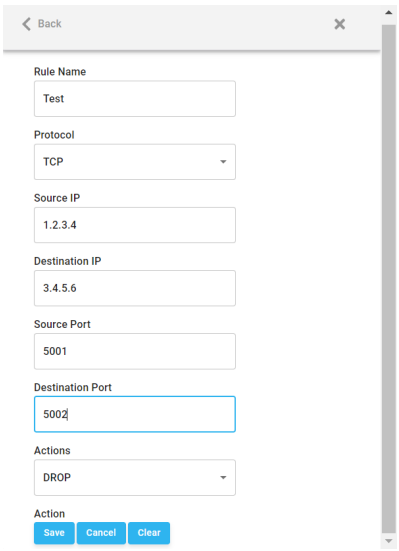
5.3.6.2 Packet Filtering

Packet Filtering provides the user to specify values for 5 fields 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 filter feature, called as 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**.

Click the **PACKET FILTERING** toggle button to enable the *Packet Filtering* configuration.



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



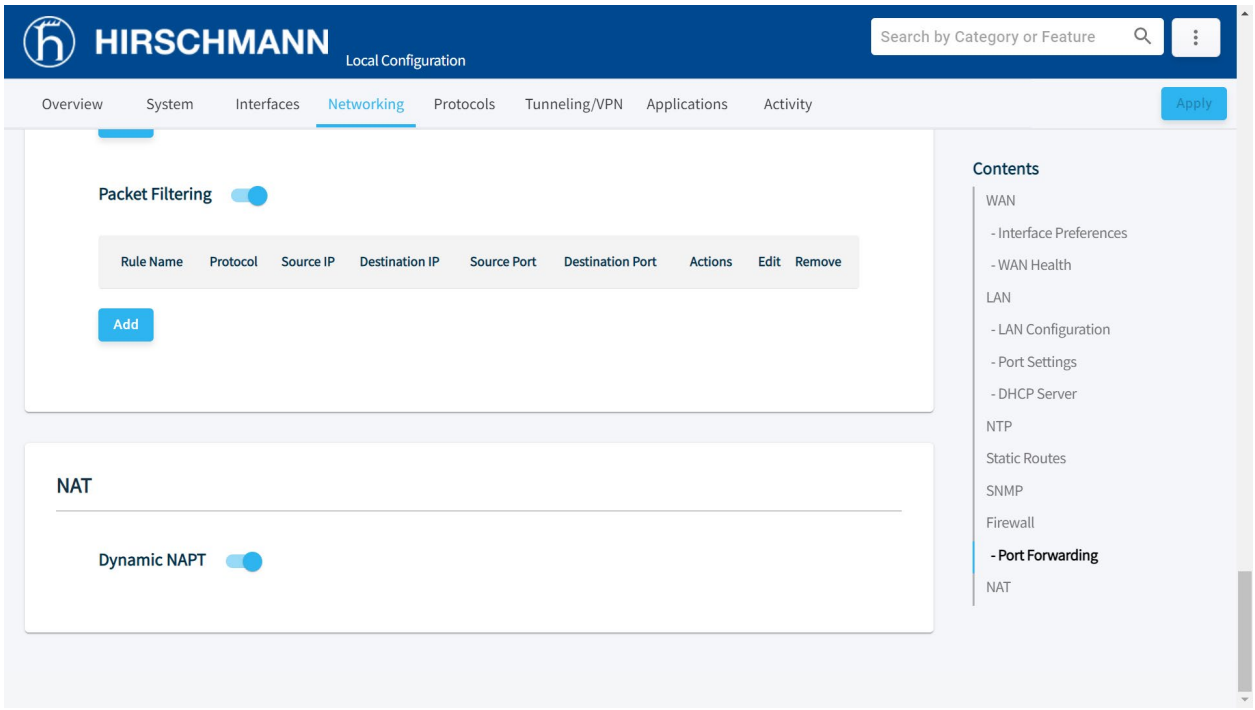
2 Provide values for the following parameters:

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.
Edit	The rule can be edited by using this option.
Remove	Removes the rule from the list.

3 Click on the **SAVE** button.

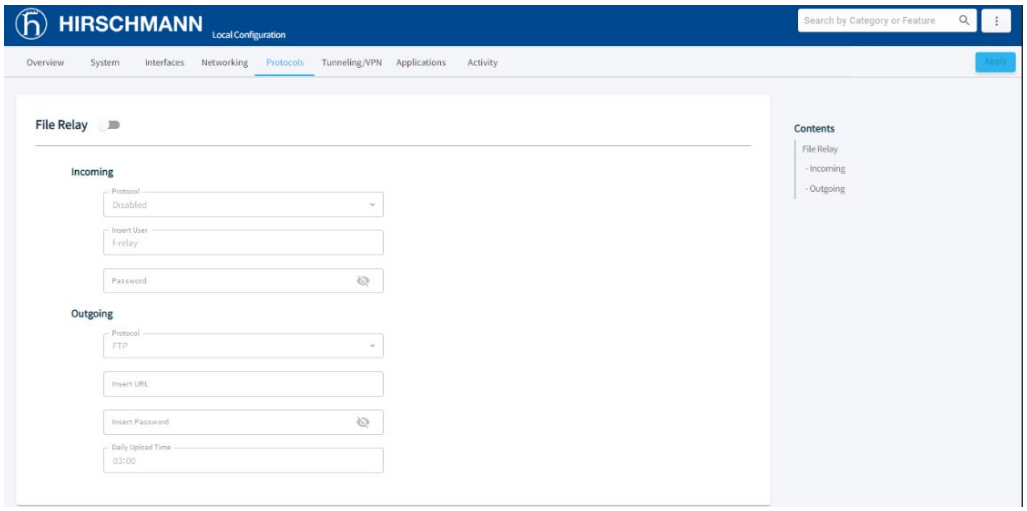
5.3.7 NAT

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



5.4 Protocols Tab

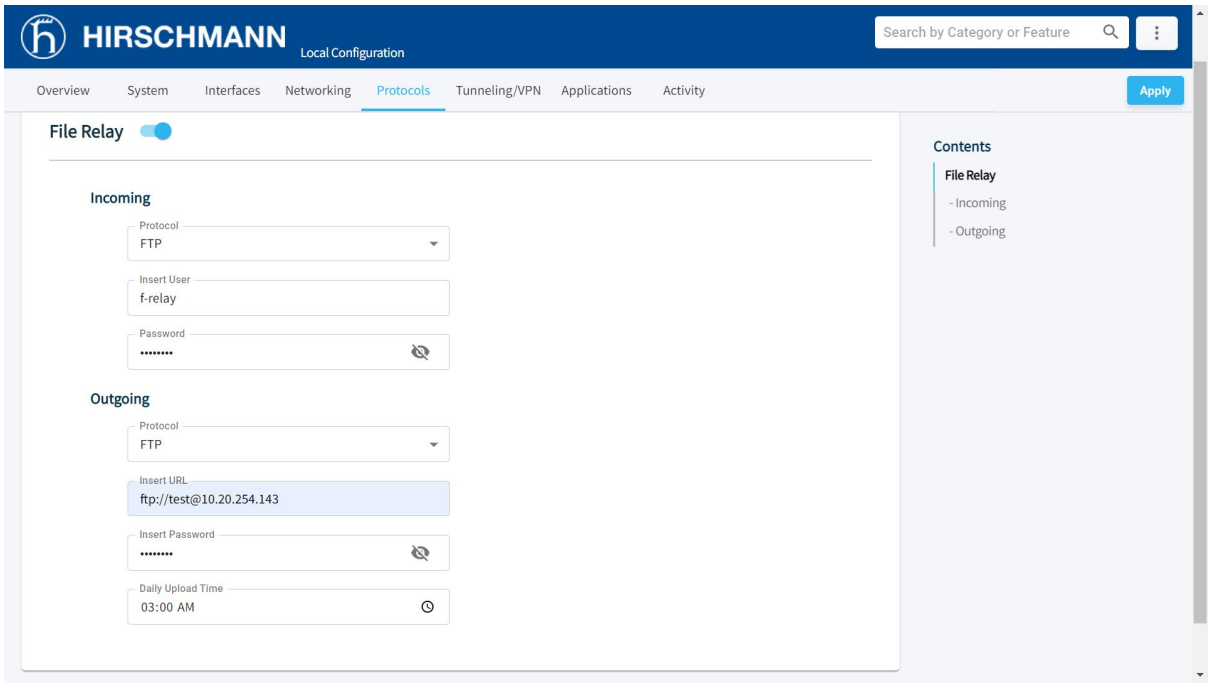
The *Protocols* tab is used to transfer files from the device to Belden Horizon.



5.4.1 File Relay

The LAN and WAN ports on the OpEdge are physically isolated. The File Relay functionality enables simple and secure transfer of files across segmented networks. For example, if the customer would like to back up all of their OT equipment configuration files on the server without wanting to create a link between the IT and OT network, the OpEdge can be used to segment between the two networks.

The *File Relay* tab allows you to use the Internal Storage (/user folder) on the device as a temporary storage medium for large files that can be automatically transferred to a remote location. Files can be copied to the OpEdge Internal Storage from a FTP/SFTP Client. The files can then be transferred to a remote FTP/SFTP Server, or via Belden Horizon.



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	FTP (File Transfer Protocol) SFTP (Secure File Transfer Protocol)
User	The user name 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	Protocol of the server used as final destination for the File Relay. □ Supported protocols for upload are FTP/SFTP/Belden Horizon
URL	URL of the server used as final destination for the File Relay. • Supported protocols for upload are FTP/SFTP/Belden Horizon • For FTP the format is specified in the field: ftp://user@host/ • For SFTP the format is: sftp://user@host:port/
Password	Password used to upload to the remote server. You can view the configured value by pressing the "eye" button. • Password is used only for FTP
Host Key	Public Key that authenticates SFTP Server and proves its identity to OpEdge client. This should be copied from SFTP Server and pasted here. Public Key from SFTP Server should be exported as **OpenSSH** format.
SSH-Key	SSH-Key is the 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. • Used only for SFTP
Daily Upload Time	The upload time, shown in the Local UI is UTC – similar with the time on the *Overview* page. Default time value is 03:00.

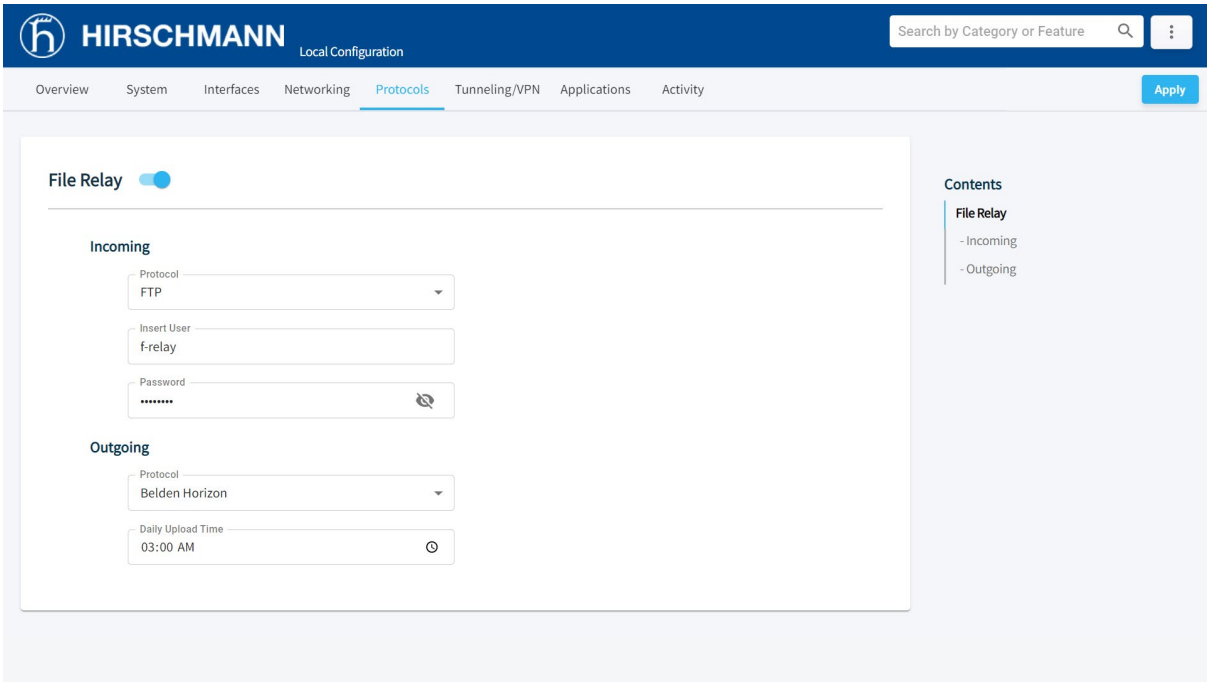
3 Click **APPLY** when complete.

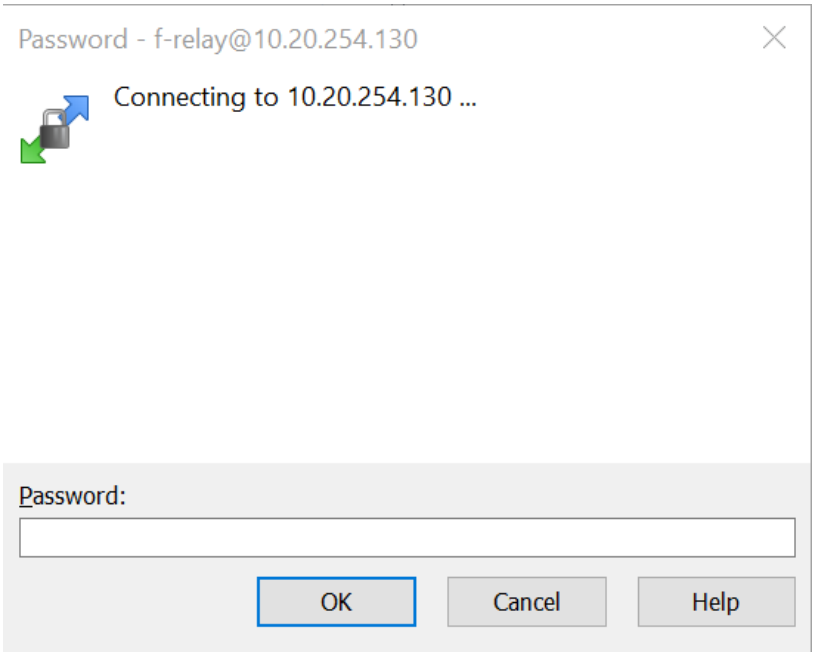
5.4.2 File Transfer to Belden Horizon

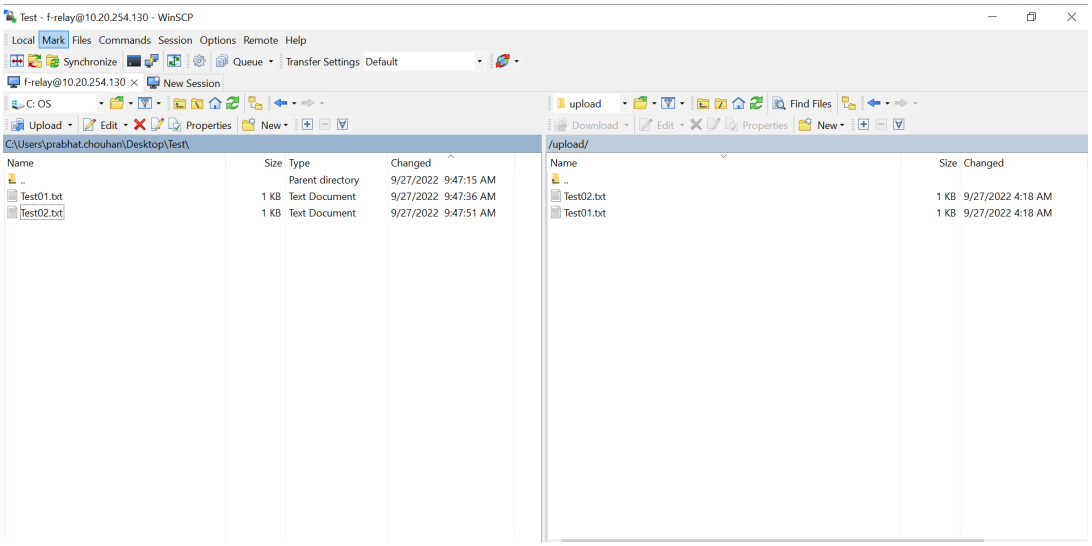
Users can transfer files from OpEdge to Belden Horizon. Below is the example for Belden Horizon file transfer.

1. Generate the Activation key from the overview page and add gateway on Belden Horizon. Detailed steps are given in section 3.1 for activating gateway on Belden Horizon.
2. From the WinSCP Client, open a SFTP/FTP session to OpEdge and transfer few files to the Upload folder on OpEdge Internal Storage. Select *Belden Horizon* for *Outgoing* and also set a time for the file transfer.

   Use the same username and password for the SFTP/FTP session as given on the OpEdge Incoming file relay section.

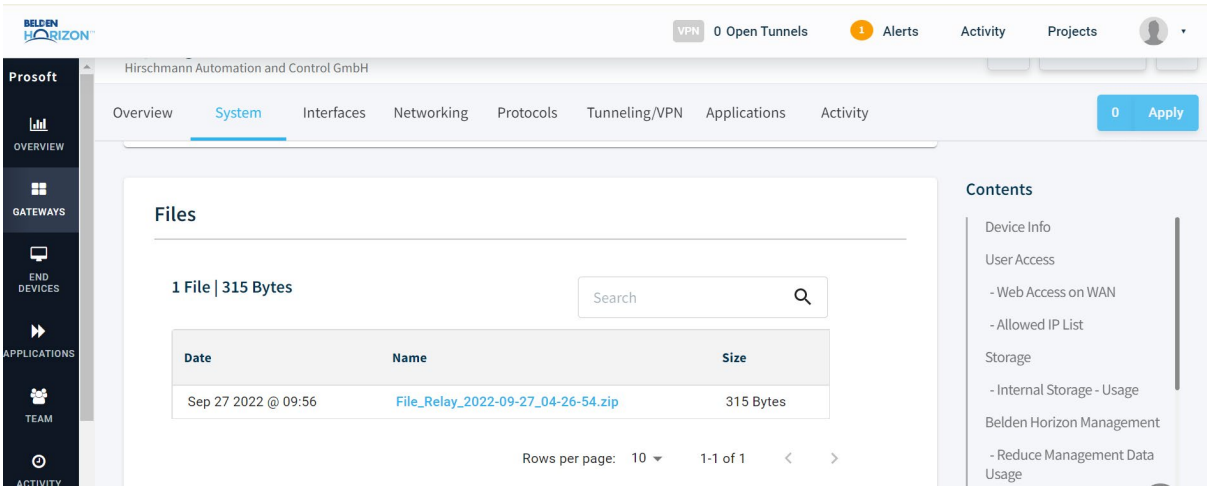


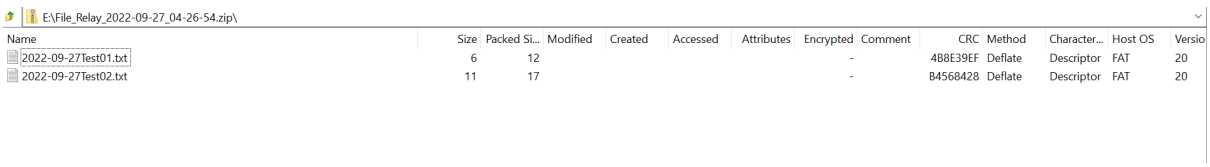




3 After uploading the files to /upload folder, the user can find the transferred file on Belden Horizon. It may take up to 10 minutes from the time given for the file transfer as the file transfer cycle is triggered once in 10 minutes.

The files can be found on Gateway > *System* tab > Files of Belden Horizon. The user can download the zip file and extract the transferred files from it.

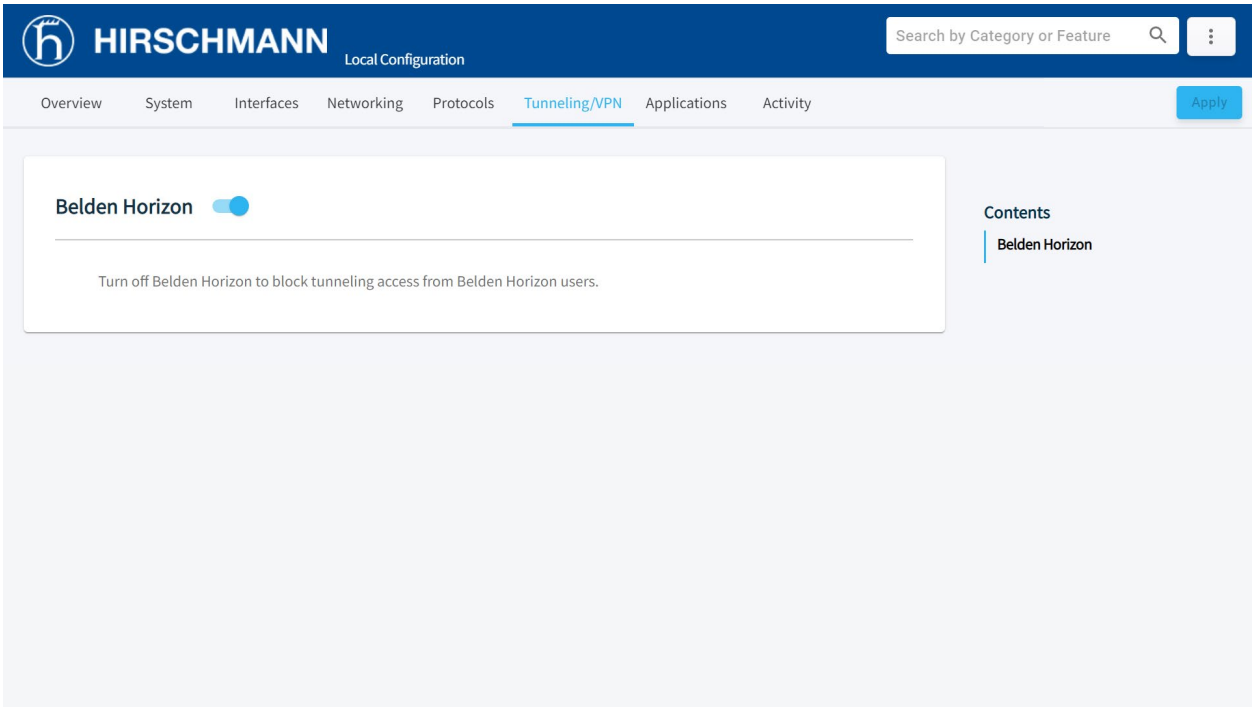




Note: Belden Horizon files can be transferred only once in 24 hours.

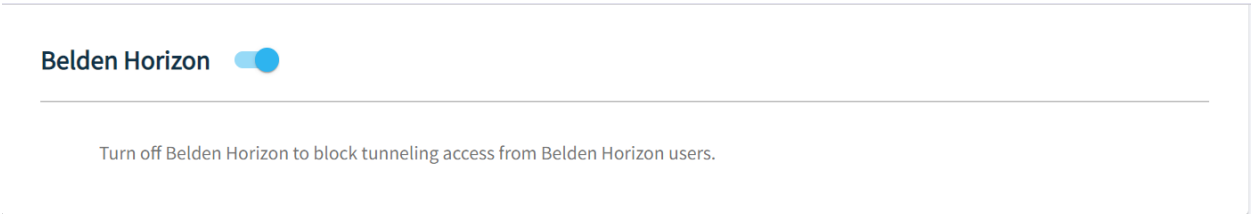
5.5 Tunneling / VPN Tab

The *Tunneling/VPN* tab allows the configuration of a Virtual Private Network (VPN) tunnel using Belden Horizon.



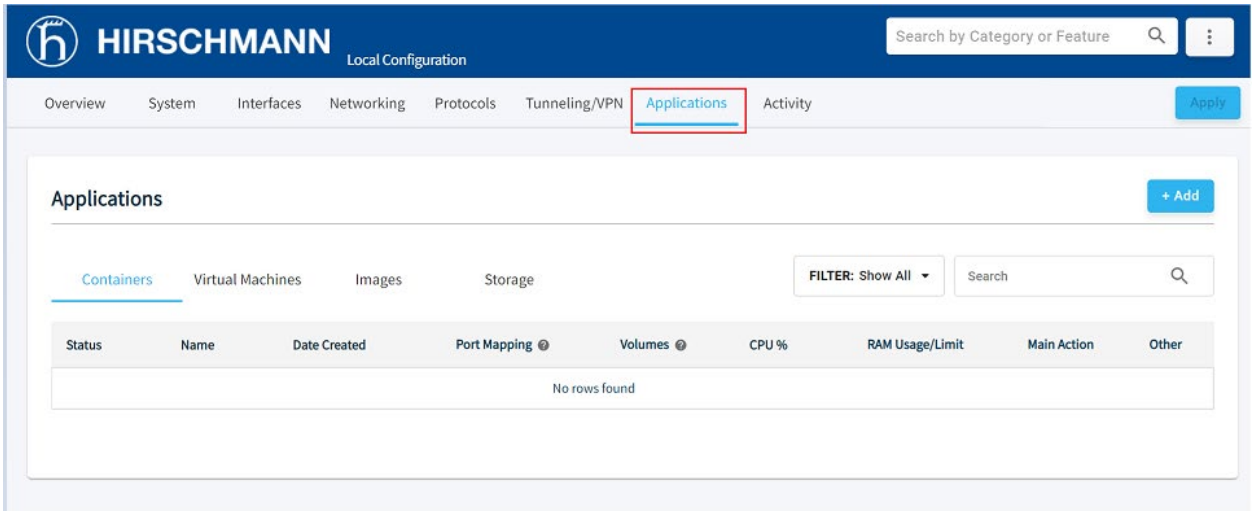
5.5.1 Belden Horizon

The **BELDEN HORIZON** toggle button allows user to turn off Belden Horizon to block tunneling access from Belden Horizon users.



5.6 Applications Tab

The *Applications* tab allows the user to perform actions on containers and virtual machines. For more information about the *Applications* tab and its features, please see the *Applications* chapter in section 6.



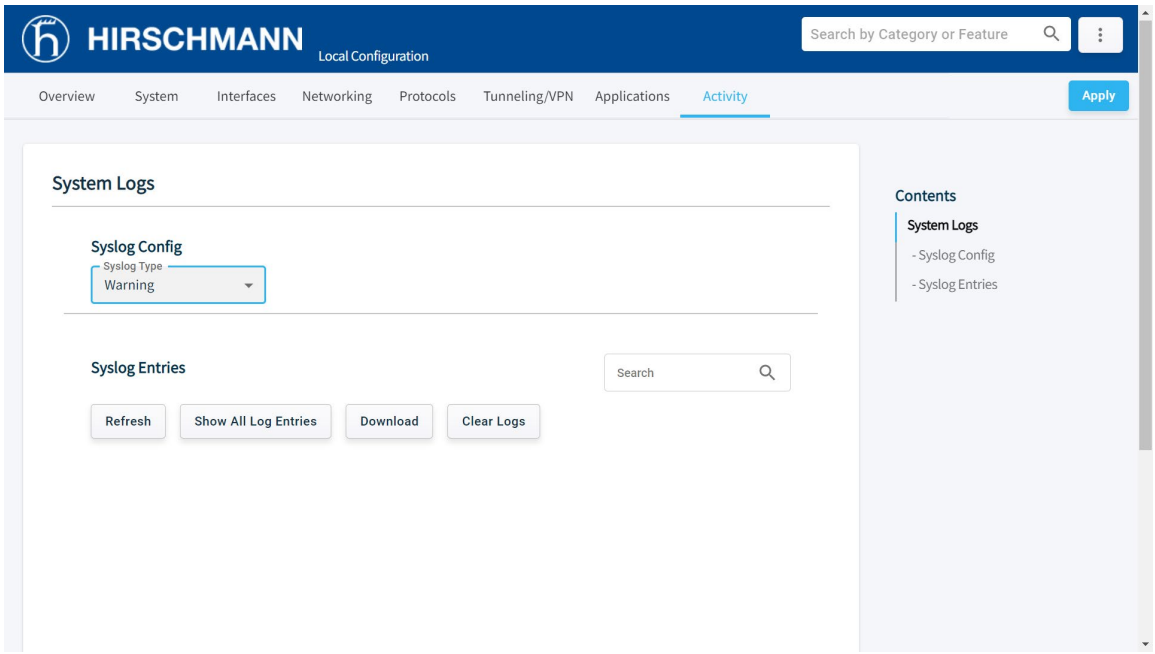
5.7 Activity Tab

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

5.7.1 System Logs

The OpEdge supports **System Logs** which captures various system log or event messages in a local log file.

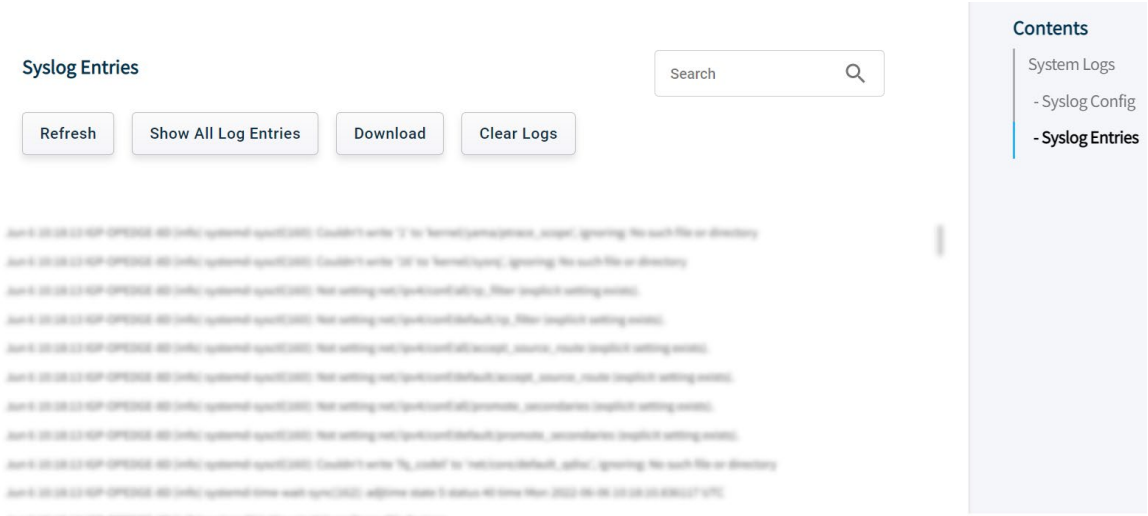
5.7.1.1 System Log Configuration



Parameter		Description
Syslog Config	Syslog Type	**WARNING** - Displays system messages and failures only. **INFO** - 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.
Show All Log Entries	Refreshes and displays all log entries.
Download	Transfers the log file from the OpEdge to PC.
Clear Logs	Clears the recorded logs.
Search/Filter bar	Search/filter for a specific log.

6 Applications

The OpEdge allows users to run Edge applications as containers or virtual machines. The OpEdge supports Docker containers technology to allow user applications to run independently of the OpEdge software.

6.1 Containers

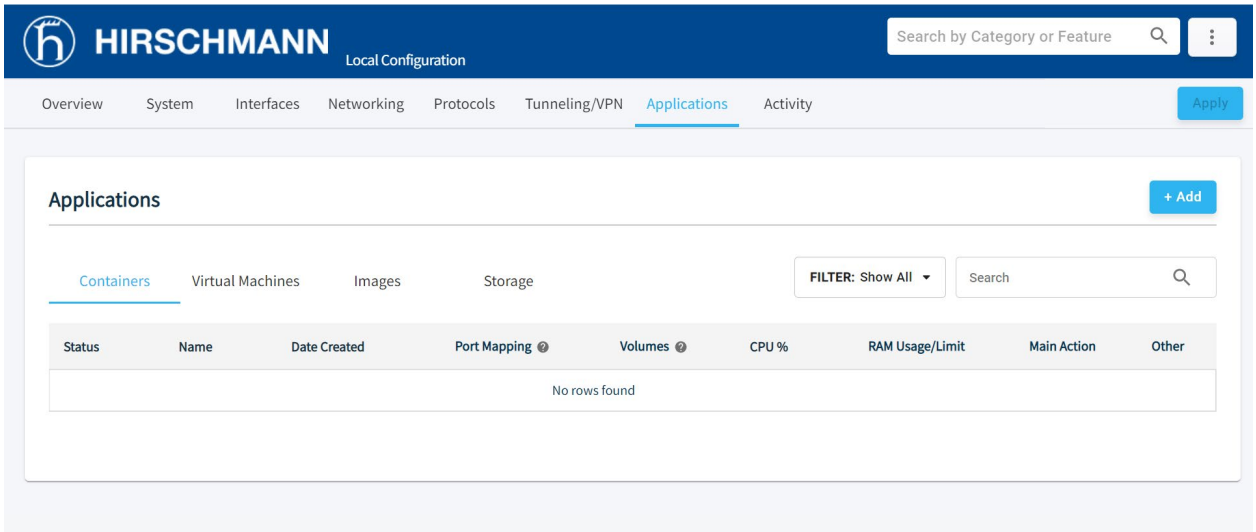
A container is a lightweight virtual computer system with its own CPU, memory, network interface, and storage, created on a physical hardware system (located off- or on-premises).

This feature allows the user to create multiple containers and run them on the same host operating system.

The user can monitor the following information for a particular container:

- Processor used in percentage
- Memory used in MB

All containers on the host machine run in isolation from one another and share the same physical hardware resources. The user can manage container operations such as start, stop, pause, etc.

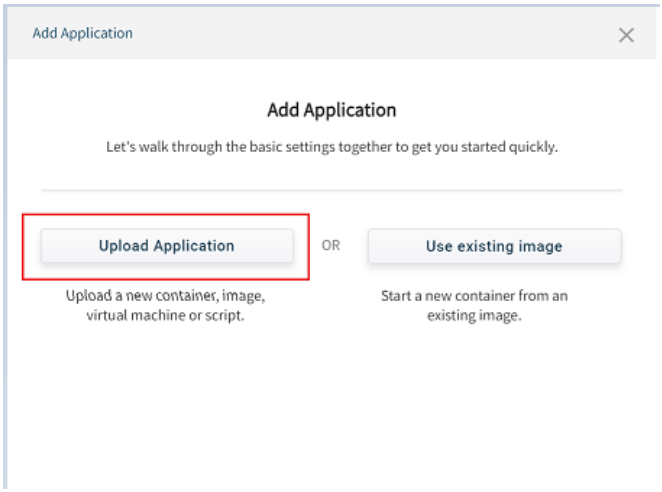


6.1.1 Creating a Container

Perform the following steps to create a container:

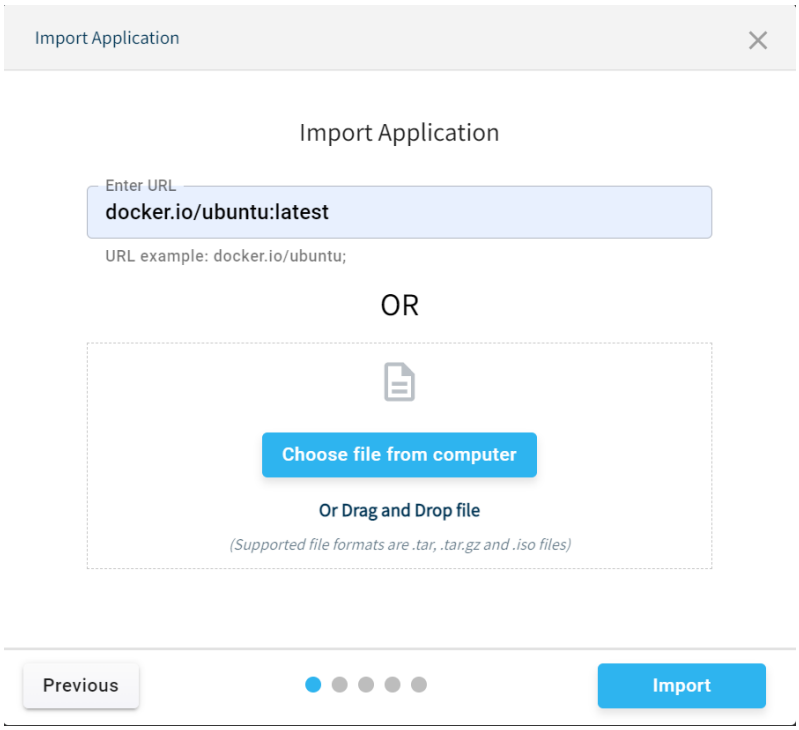
1. Navigate to the *Containers* tab.
2. Click the + Add button to open the *Add Application* wizard.
3. There are two options in the *Add Application* wizard:
   - **Upload Application**: Uploads a new docker image for container creation.
   - **Use existing image**: Creates a container with the existing docker image on the device.

   a) Upload Application option.

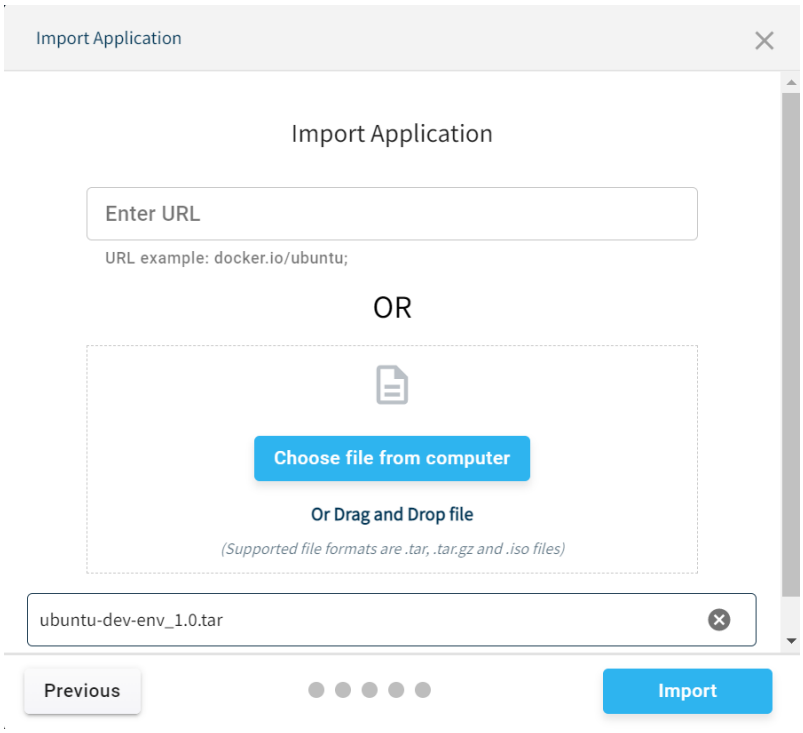


i. There are two ways to upload the image:

- 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>**

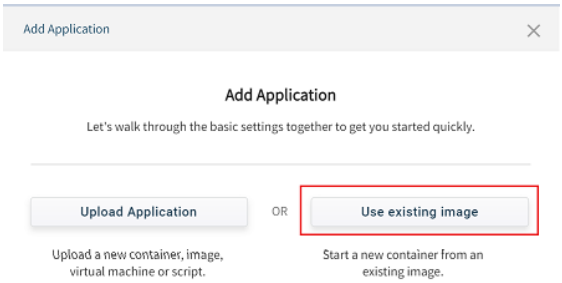


- In the *Import Application* window, click on **CHOOSE FILE FROM COMPUTER** and select the docker image from the local PC.

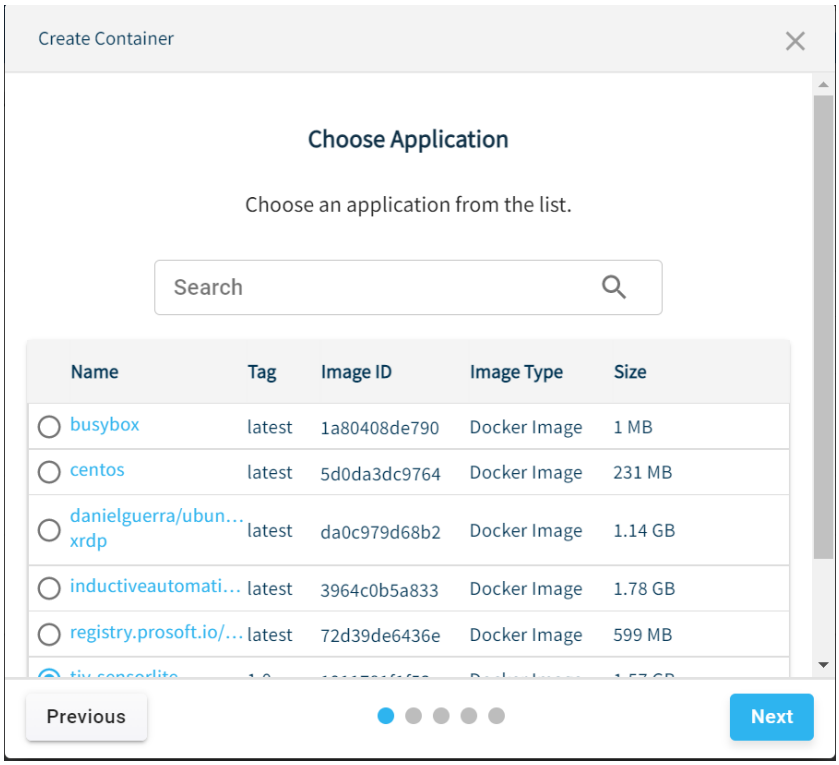


ii. Click **IMPORT** to add image.

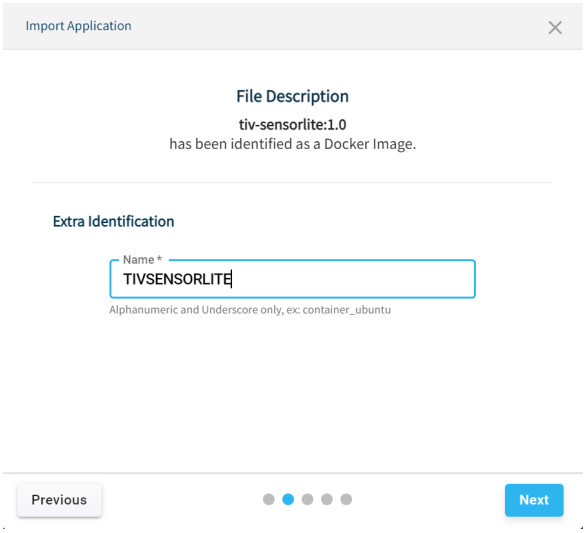
b) **Use existing image** option.



i. Select an image from the list of existing images and click **NEXT**.



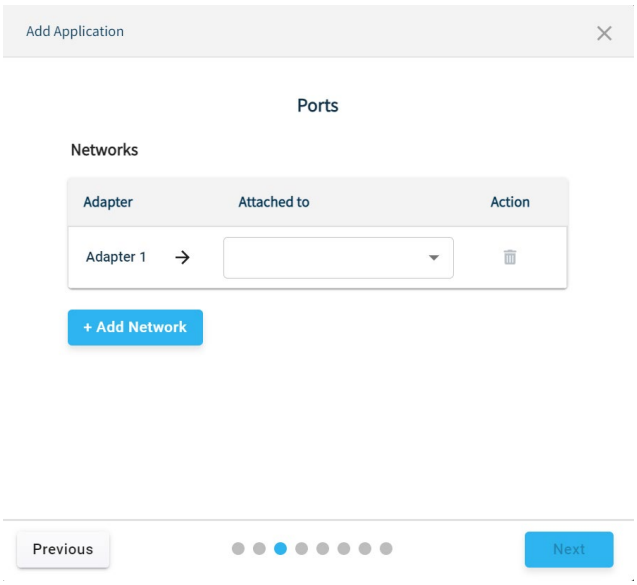
4 In the *Name* field, enter the name of the container.



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.

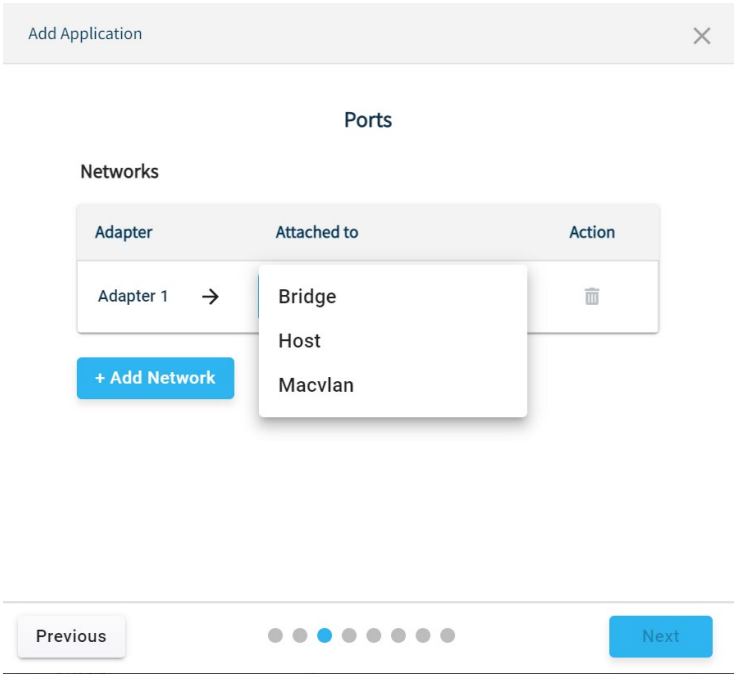
5 Click **NEXT** for **Ports** wizard to choose the network type **.**



Note: The user can add a maximum of three network adapters.

6 The *Ports* tab contains the *Networks* configuration. Select an option for attaching the network adapter to the container:

- Bridge
- Host
- Macvlan



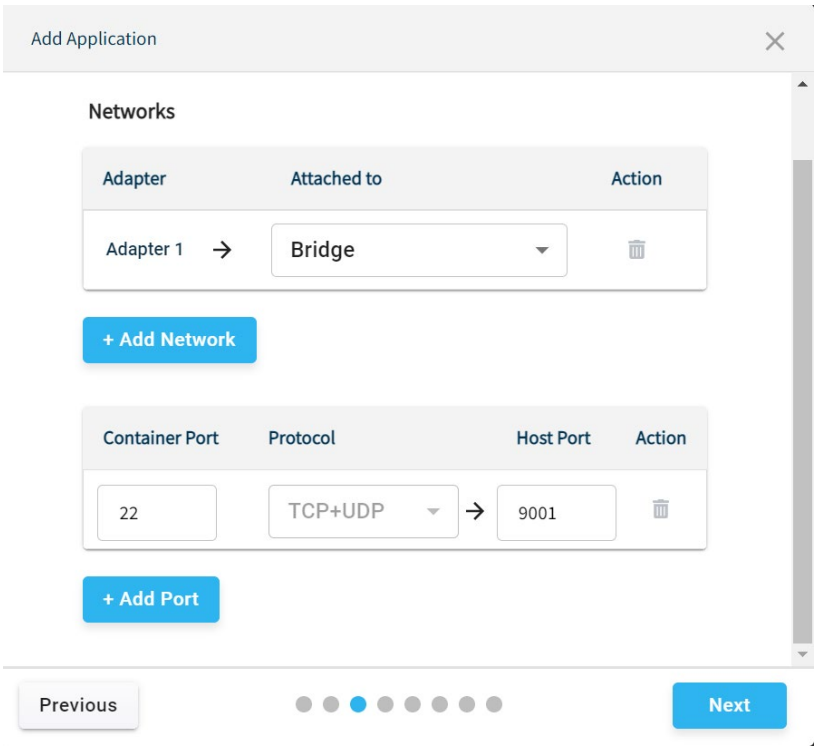
a) For Bridge network, user need to configure the container and host ports.

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

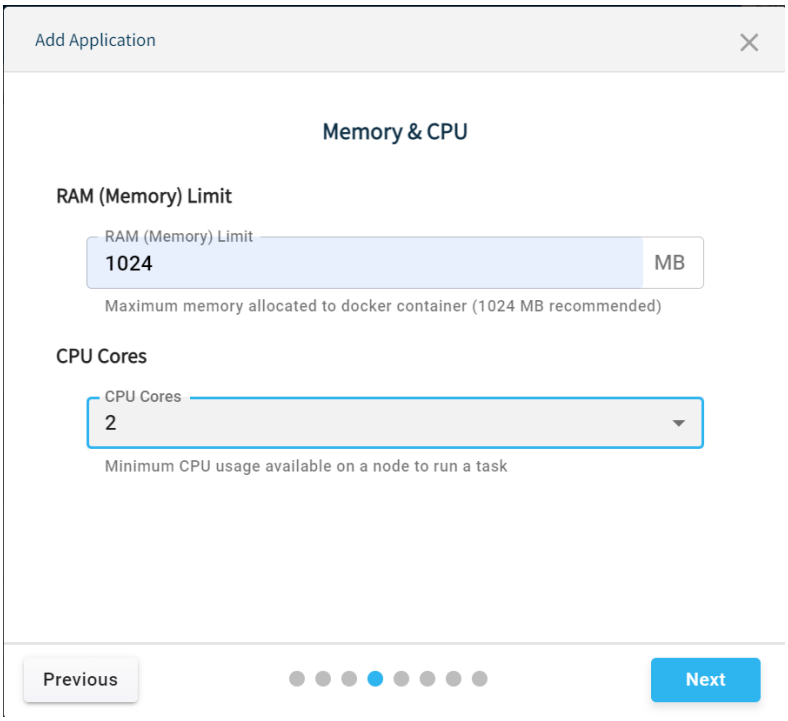
ii. In the *Host Port* box, enter the host port number.

Note: The user can add a maximum of four Container and Host ports.

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



7 Click **NEXT** for *Memory & CPU* wizard to configure Memory and CPU.



- In the *Memory* field, enter the size of memory (MB) for the container.

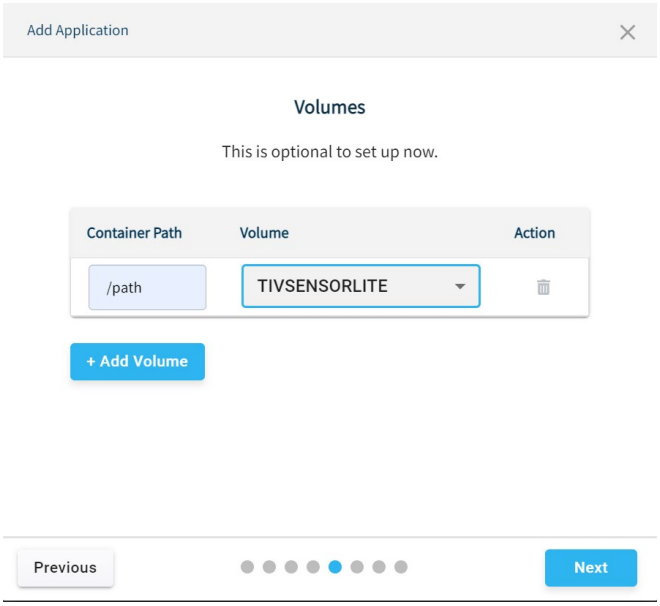
> **Note:** The minimum allowed memory value for creating containers is 4MB.

- In the *CPU* field, enter the number of the CPU cores to be used by the container. The number of processors is expressed in number of physical CPU cores.

8 Click **NEXT** for **Volumes** wizard.

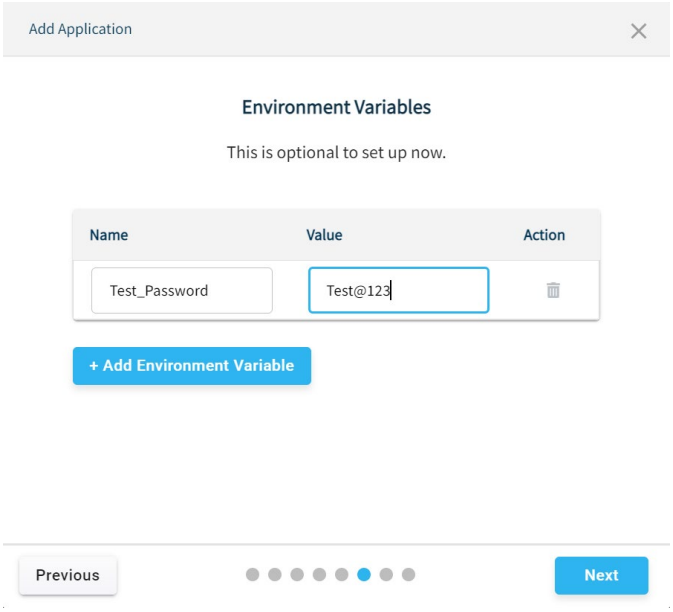
9 (Optional) In **Volumes** wizard, enter *Container Path* and select the *Volume* from an existing list to attach to the container.

> **Note:** Refer to section 6.2.1 to add a new volume when there is no volume available to attach to the container.



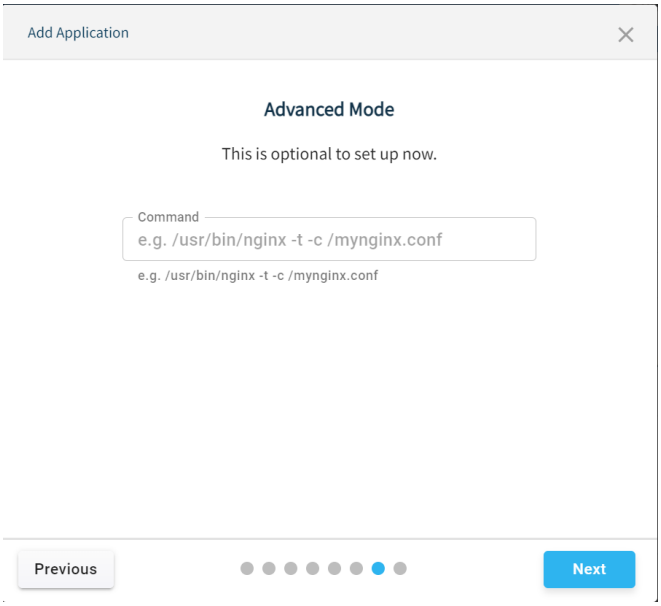
10 Click **NEXT** for **Environment Variables** wizard.

11 (Optional) In **Environment Variables** wizard, enter the Name and Value of the environment variable.

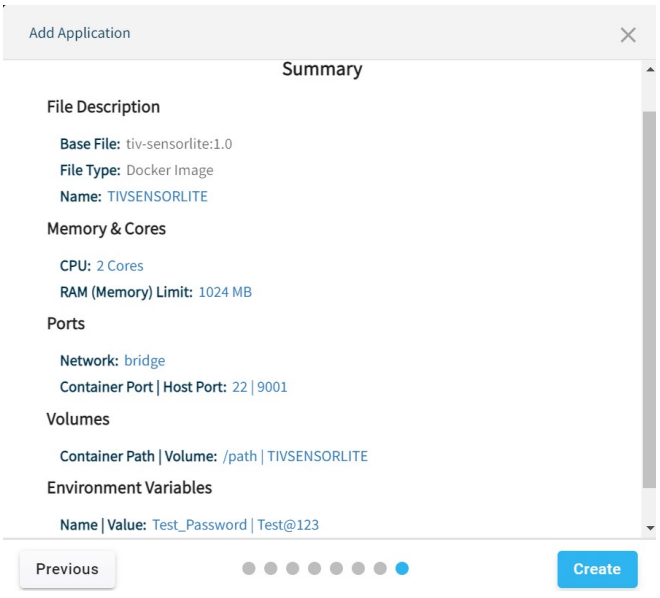


12 Click **NEXT** for **Advanced Mode** wizard.

13 (Optional) In Advanced Mode, the user can enter advanced docker commands which are supported by the specific docker image.



14 Click **NEXT** for **Summary** page.

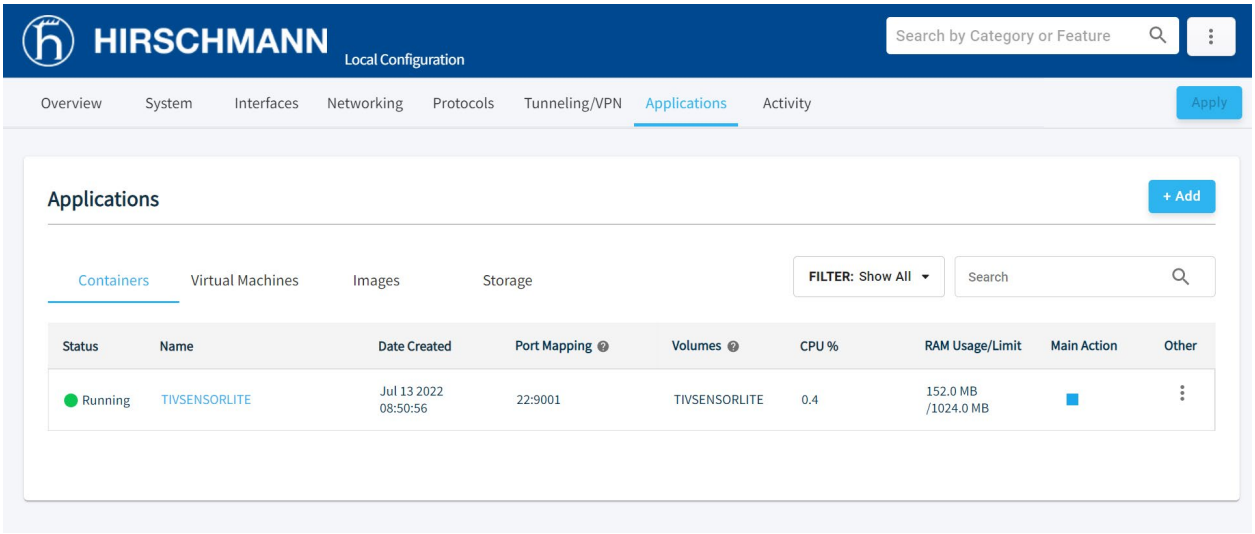


15 Check all details entered in the Summary wizard and click **CREATE** to create the container.

Note: If edits are needed before creating the container, click the **PREVIOUS** button in the wizard.

6.1.2 Container Status

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



Parameter	Description
Status	The current operating status of a container: • Running • Stopped • Paused
Name	Name of a container.
Date Created	Date of container creation
Port Mapping	This field describes the detail of the following ports: • *Container Port*: The Container port number. • *Host Port*: The Host port number.
Volumes	The container volumes attached with 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	Main Action is quick action available according to the state of container.
Action buttons	Click on the Actions button ⋮ on a container:

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 in a docker container from GUI with the help of docker exec shell functionality.
Save	Save the container as an image. See *Saving a Container as an Image* section 6.1.2.1 for more details.
Edit container details	Edit the container. **Note:** User is allowed to 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 state.

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

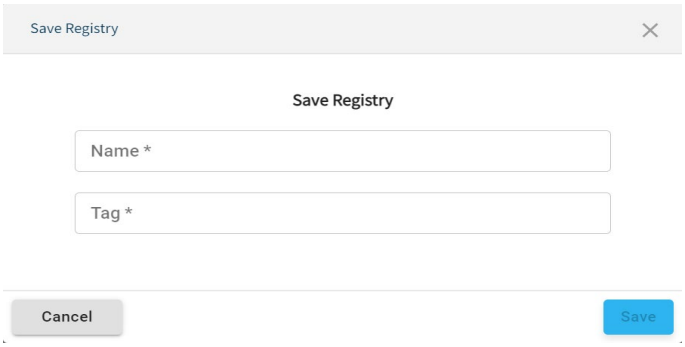
6.1.2.1 Saving a Container as an Image

The user can save a particular container as a container image that is visible under the *Images* tab under *Applications*.

To save a container as an image:

1 In the *Containers* tab, click the Actions button  .

2 Click the  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*.

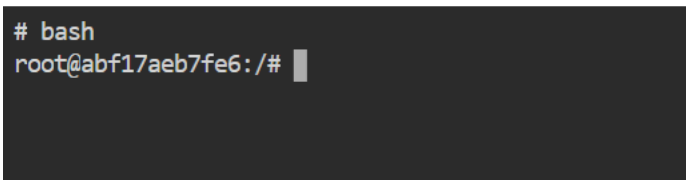
4 Click **SAVE**.

6.1.3 SSH Connectivity to Containers

The user can access the shell of a container and run different commands on it.
To access the shell of a container:

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

button to open a prompt to run commands.



6.2 Container Volumes

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 (**/opt/apps/**).

When the user creates a container, two default volumes are created (one default private and one default public). If a docker image has any volumes included, then the same will be created and mapped with the container.

By default, the volume location on the host device is: **/var/lib/docker/volumes**.

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

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.
- User can manage volumes using OpEdge UI.
- Volumes work on both Linux and Windows 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.

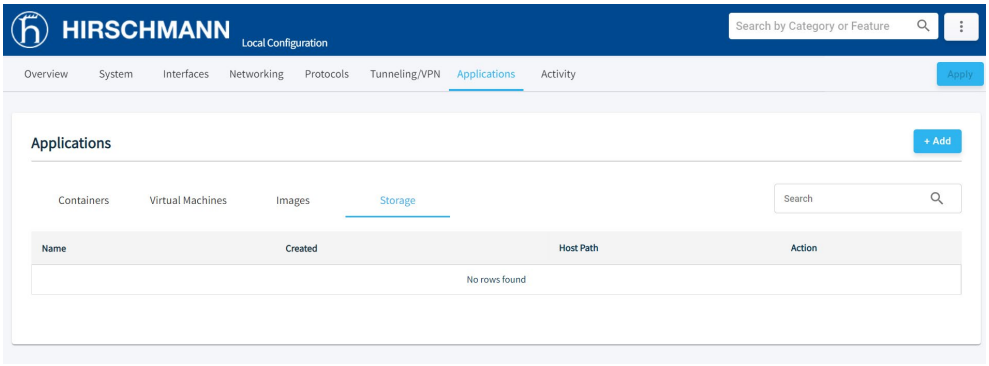
Common use cases for docker volumes:

- 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.

6.2.1 Adding a Volume

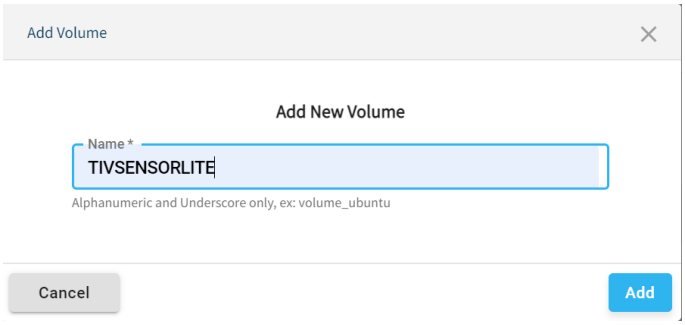
To add a volume:

1 Navigate to the *Storage* tab.

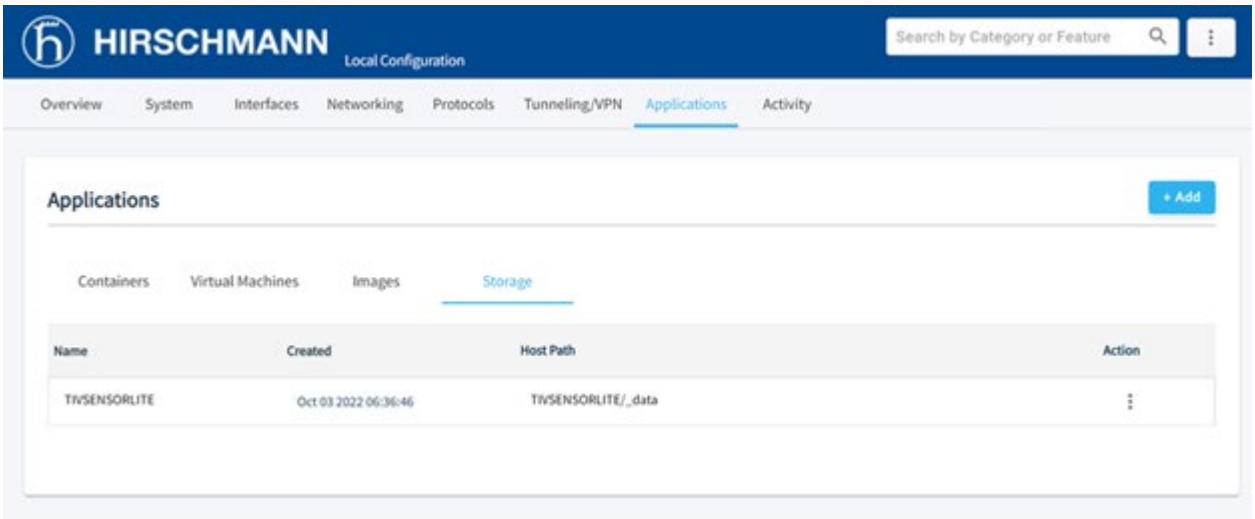


2 Click on + Add button.

3 Enter name of the volume in the *Name* field and click **ADD**.



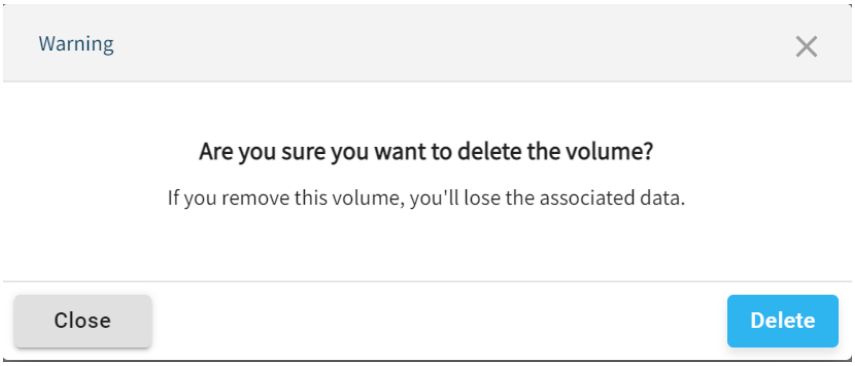
4 The list of *Volumes* is updated.



6.2.2 Deleting a Volume

To delete a volume:

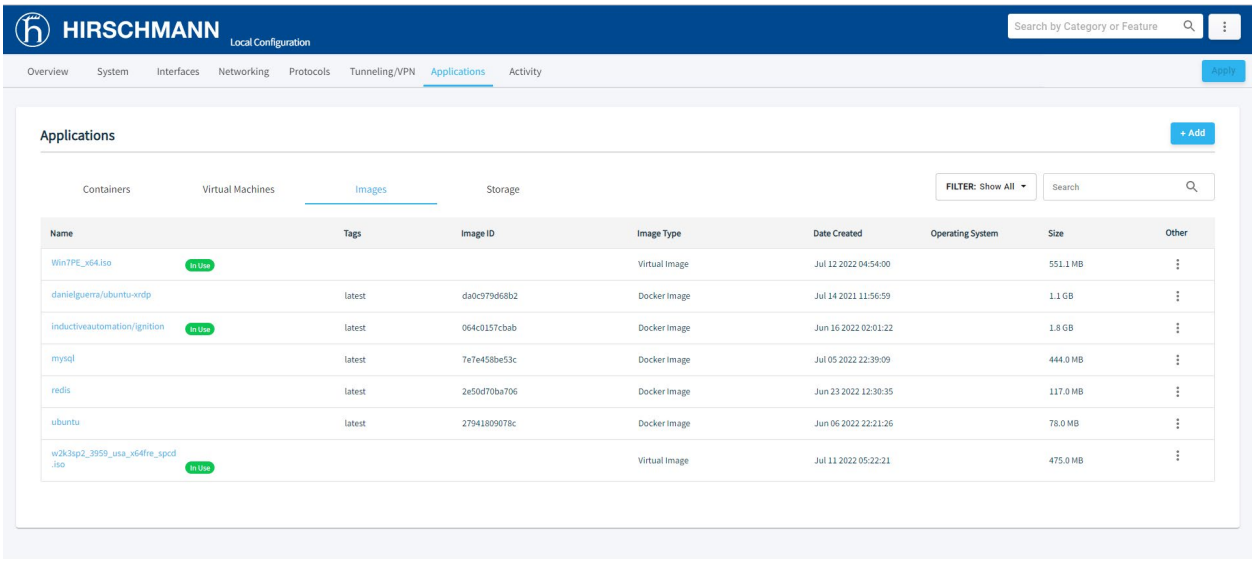
1. For the volume to be deleted, click on Actions button  .
2. Click on  button.
3. The user will be asked for the confirmation to delete.



4. Click **DELETE** to confirm.

6.3 Images

This page lists all Docker and Virtual Machine Images present on device.



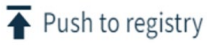
Parameter	Description
Name	The name of the Image.
Tags	The version/tag of the Image.
Image ID	The unique ID of each Image
Image Type	Image type: Docker **or** Virtual Machine.
Date Created	The date of Image upload on device.
Operating System	Operating system of the Image.
Size	The disk size in MB/GB of the virtual disk.
Other	**Action Button** / **Description** Push to registry — Push Image to registry. Enter the *URL*, *Username*, and *Password*. Download — Download Base Image. **Note:** The user can check the default download folder selected in the browser for the Base Image file downloaded. Delete — Deletes Base Image.

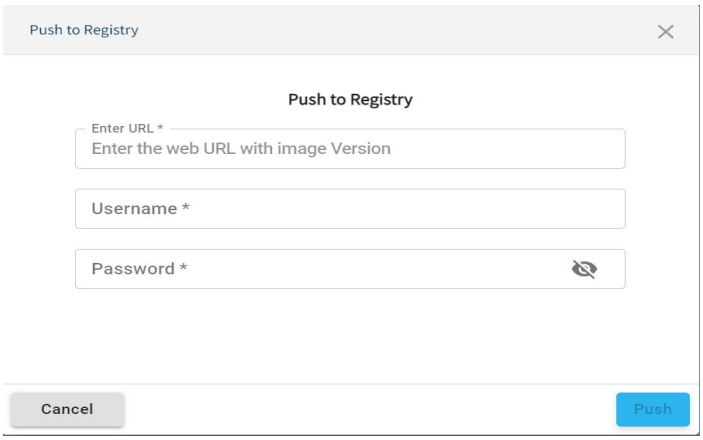
Note: Images being used for Container/Virtual Machine will show **In Use**.

Note: The *Push to registry* and *Download* actions are supported for docker image only. The *Delete* action is supported for both docker and iso images.

6.3.1 Push Docker Image to Registry

The user can push a docker image from the OpEdge to the docker registry.
To push an image to the registry:

1. Locate the docker image and click on Actions button  .
2. Click the  button.
3. Enter the *URL*, *Username*, and *Password* for the registry.



4. Click the  button to push the image.

6.4 Virtual Machines

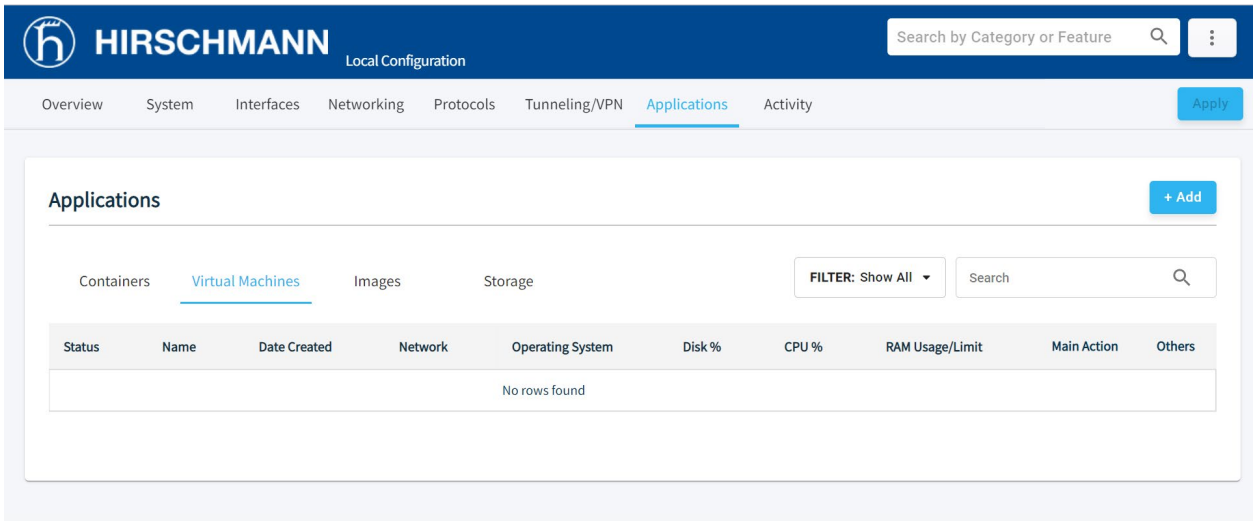
A virtual machine functions as a virtual computer system with its own CPU, memory, network interface, and storage, created on a physical hardware system (located off- or on-premises).

This feature allows the user to create multiple virtual machines and run them on the same physical server.

The user can monitor the following information for a virtual machine:

- Processor used in percentage
- Memory used in percentage
- Disk used in percentage

All virtual machines on the host machine run in isolation from one another and share the same physical hardware resources. The user can manage operations such as start, stop, pause, and delete.

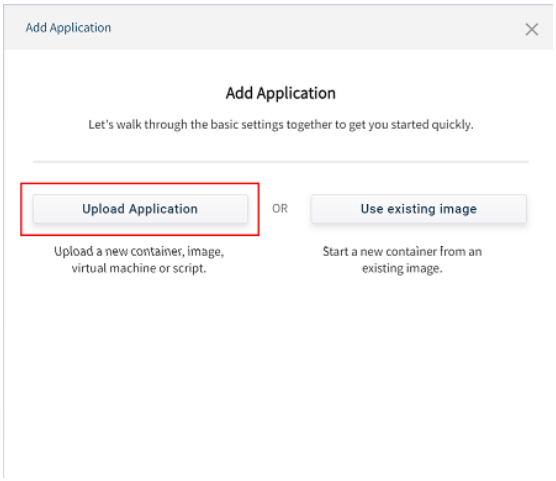


6.4.1 Creating a Virtual Machine

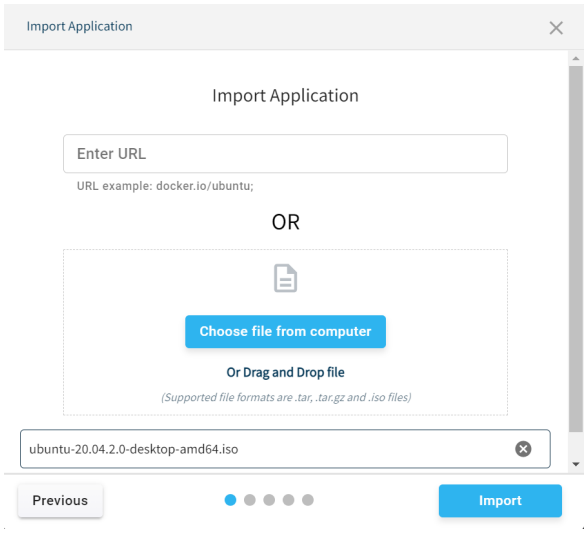
To create a guest virtual machine:

1. Go to the *Virtual Machines* tab.
2. Click + Add to open the *Add Application* wizard.
3. Click **NEXT** to navigate through the wizard.
4. There are two options for adding a .iso image for virtual machine creation:
   - **Upload Application:** Uploads a new .iso Image for virtual machine creation.
   - **Use existing image:** Creates a virtual machine with an existing .iso image on the device.

a) Upload Application option**.**

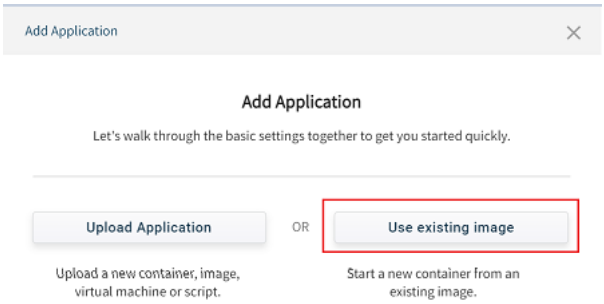


i. Upload the virtual machine image by selecting a virtual machine image from local PC by clicking **CHOOSE FILE FROM COMPUTER.**

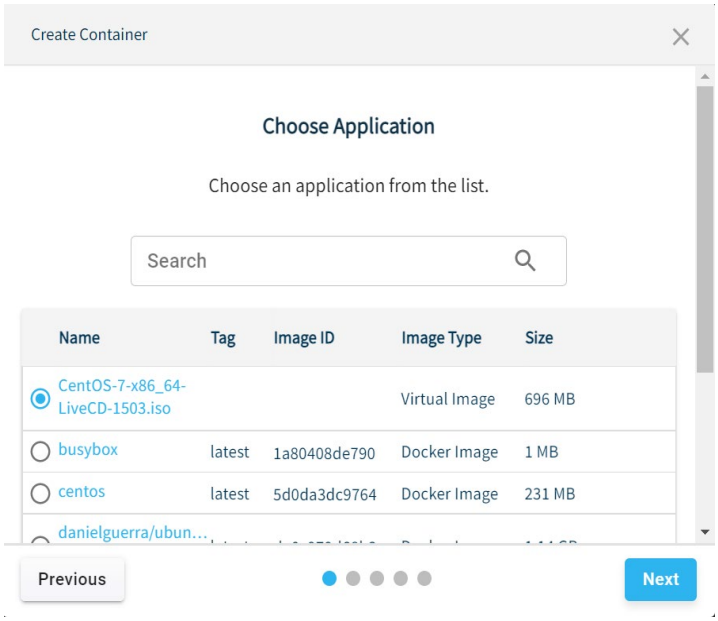


ii. Click **IMPORT** to add the image.

b) Use Existing Image option.

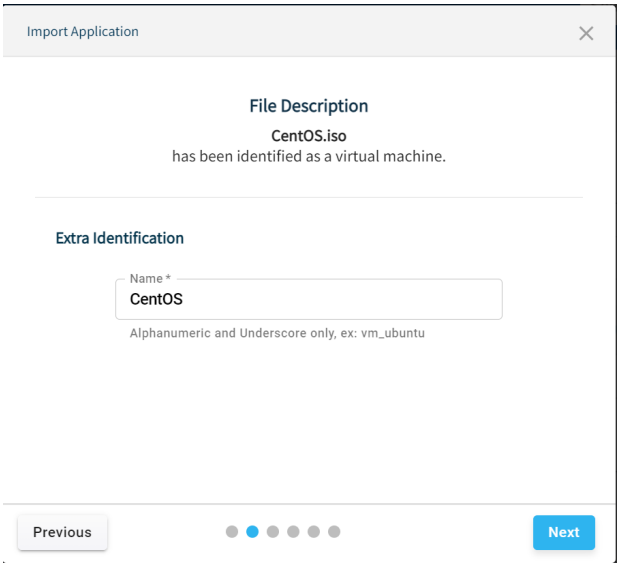


i. Select an .iso image from a list.



ii. Click **NEXT**.

5 Enter a name for the virtual machine.

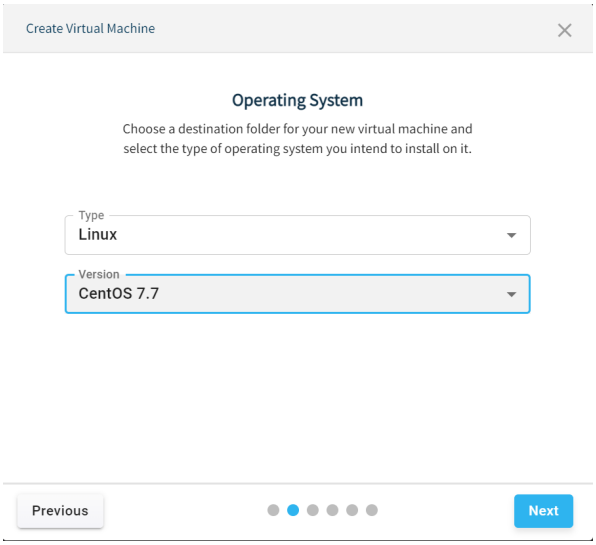


Note: The user can create a virtual machine name with an alphanumeric character with a minimum length of 1 and a maximum length of 30.

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

6 Click **NEXT**.

7 In the *Operating System* wizard, enter the *Type* and *Version* of the Operating System.



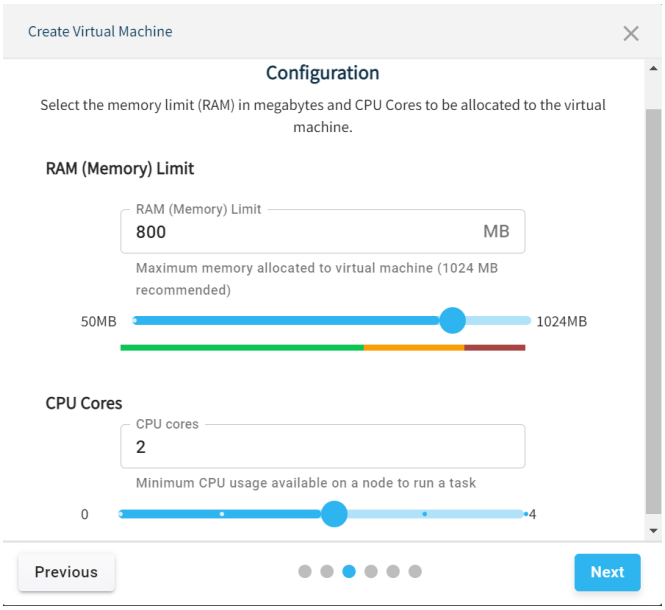
Parameter	Description
Type	The operating system of a virtual machine. User can select the respective operating system: Linux and Windows.
Version	Type or select the respective OS family. For example, Linux OS type user can select OS family as Ubuntu.

The current supported OS Types and Operating Systems:

Parameter	Description
Linux	CentOS 7.6 CentOS 7.7 CentOS 7.8 Ubuntu 16.04 Ubuntu 18.04
Windows	Microsoft Windows Server 2008 Microsoft Windows Server 2012

8 Click **NEXT**.

9 In the *Configuration* wizard, select the *RAM (Memory) Limit* and *CPU Cores* for the virtual machine.

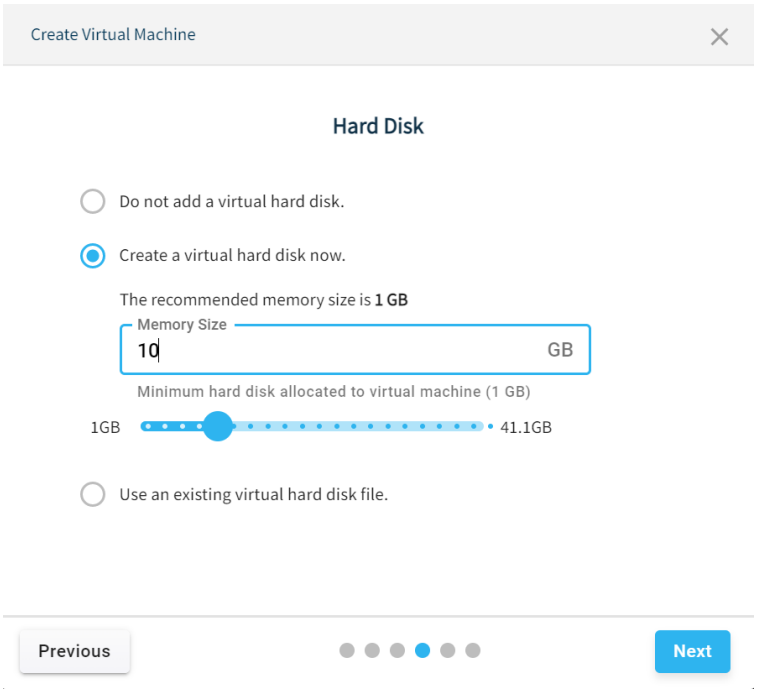


Parameter	Description
RAM (Memory) Limit	Select or provide memory for virtual machine.
CPU Cores	Select number of CPU Cores for the virtual machine.

10 Click **NEXT**.

11 In the *Hard Disk* wizard, select a hard disk option:

- Do not add a virtual hard disk.
- Create a virtual hard disk now.
- Use an existing virtual hard disk file.

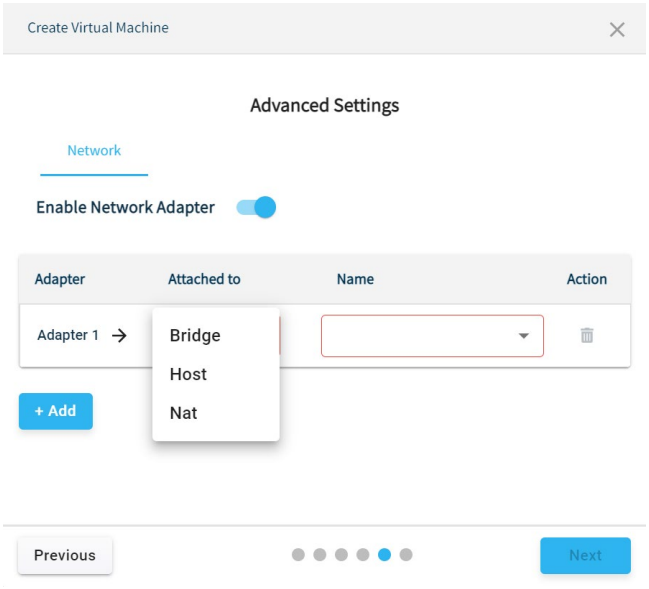


Note: The **CREATE A VIRTUAL HARD DISK NOW** option is the only available option in the current implementation.

12 Click **NEXT**.

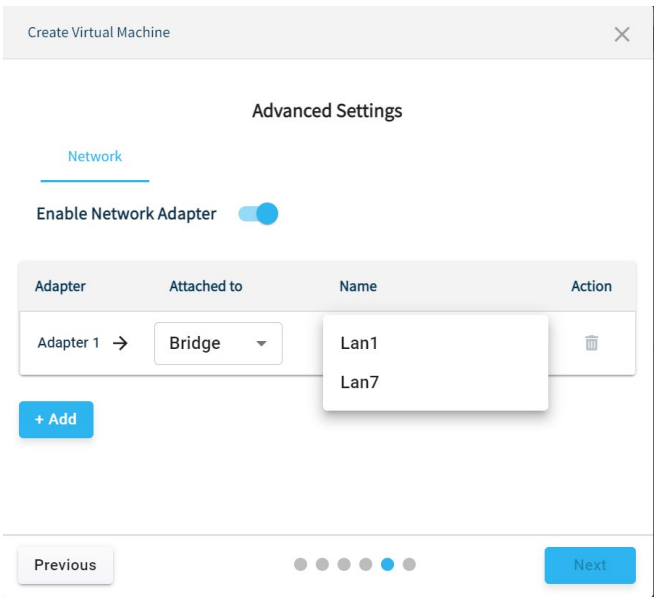
13 In the *Advanced Settings* wizard, toggle the **ENABLE NETWORK ADAPTOR** button and select a *Network Adapter* to attach with the virtual machine:

- **Bridge**
- **Host**
- **NAT**



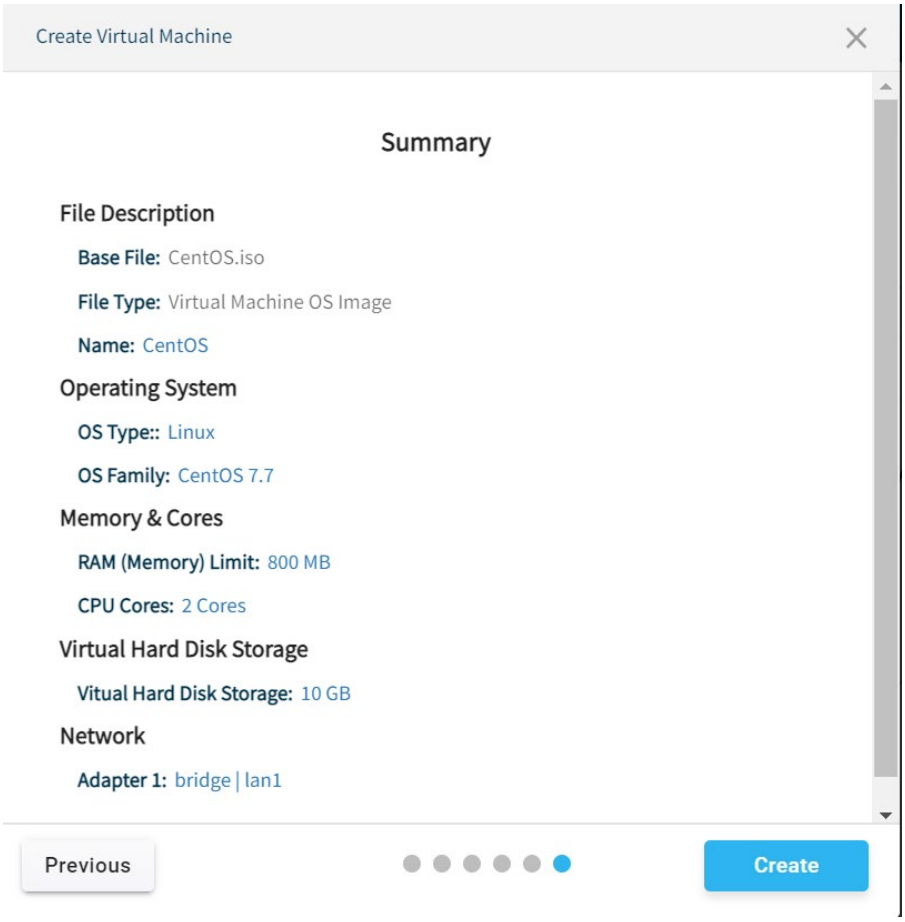
14 Select the **NAME** associated with the selected *Network Adapter*:

- **Bridge**: Select a virtual LAN port. (Example: **LAN1**)
- **Host**: Select a physical Ethernet port. (Example: **ETH1**).
- **NAT**: Select **DEFAULT**.

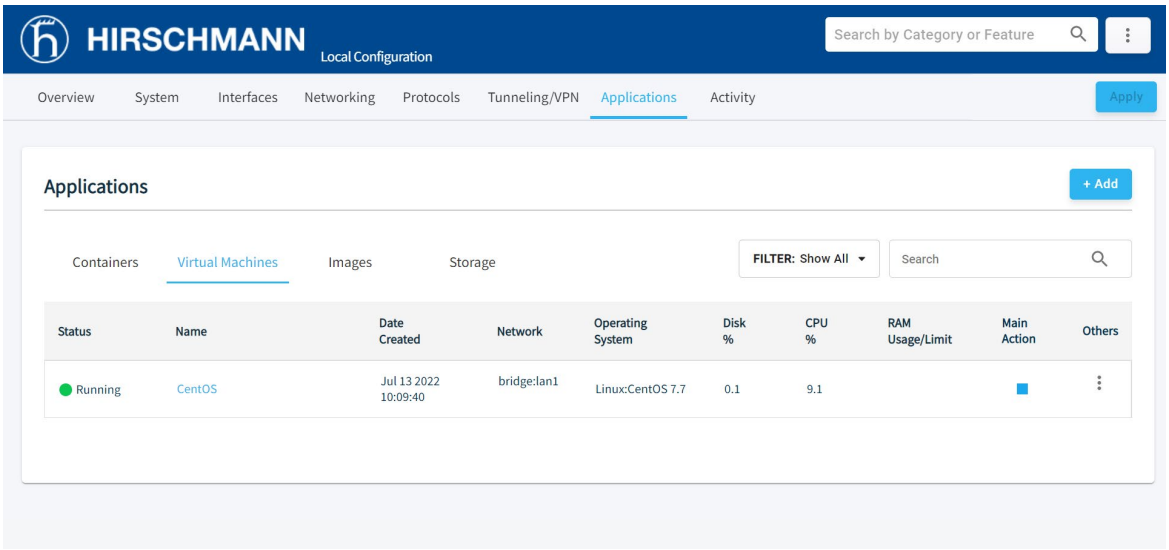


15 Click **NEXT**.

16 In the *Summary* wizard, verify all details and click Create to create the virtual machine.



17 Example of a successfully created virtual machine:



Parameter	Description	
Status	**Status**	**Description**
	Running	Virtual machine is in Running state.
	Paused	Virtual machine is in Paused state.
	Stopped	Virtual machine is Powered Off state.
Name	Lists the name of all virtual machines.	
Date Created	It shows the date of virtual machine creation.	
Network	It shows the type of network given at time of virtual machine creation.	
Operating System	The operating system of a particular virtual machine.	
Disk%	The amount of storage space used in a percentage of total storage allocated at a certain point of time.	
CPU%	The sum of work handled by a processor on the virtual machine. It also used to estimate system performance.	
RAM Usage/Limit	The amount of RAM used by a particular virtual machine at a certain point of time/ The total RAM allocated to the virtual machine.	
Main Action	This option enables user to perform quick action on the virtual machine. For example, When a virtual machine is stopped, the Start button is displayed.	
Others	**Action Button**	**Description**
	Start	Power On or resumes the virtual machine. **Note:** When resuming a suspended machine, the operating system and applications start from the point the user suspended the virtual machine.
	Stop	Power Off the virtual machine. The virtual machine is stopped. The state of the virtual machine is Powered-off after the shutdown is complete.
	Suspend	Suspend the virtual machine. When suspended, the current state of the operating system and applications is saved. When the user resumes the virtual machine, the operating system and applications continue from the same point the user suspended the virtual machine.
	Restart	Restart the virtual machine.

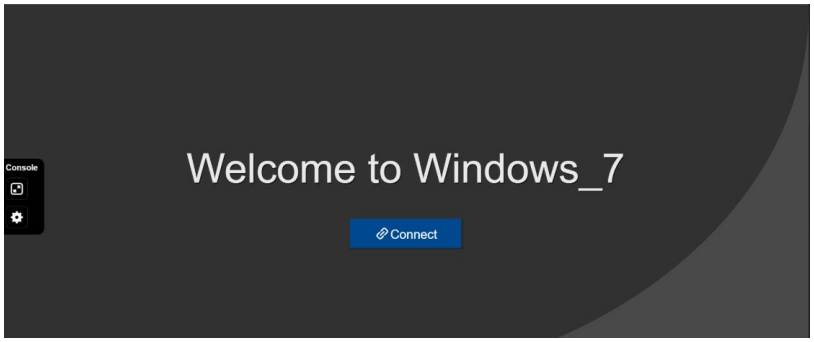
	Console	Console for virtual machine. The console is the remote control system of virtual machine, and enables the user to work and interact with the created virtual machines. Please see *Connecting to a Virtual Machine* in section 6.4.1.1 for more information.
	Edit	Edit the virtual machine.
	Delete	Delete the virtual machine.

6.4.1.1 Connecting to a Virtual Machine

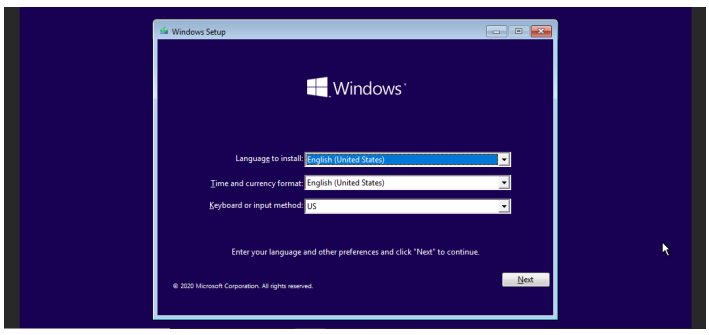
The user can connect to a virtual machine by using its console. The console is the remote control system of a virtual machine.

Note: For first time login to the virtual machine, the user must to install the operating system selected for the virtual machine.

1. In the *Virtual Machines* tab, place the cursor on a particular virtual machine to display the Action buttons.
2. Click the button to open a new tab in the browser.

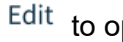


3. Click on **Connect** to proceed with the installation of VM.



6.4.1.2 Editing a Virtual Machine

1 In the *Virtual Machines* tab, click on a container's Action button  .

2 Click  to open the *Edit Virtual Machine* wizard.

3 Follow the steps in the wizard to edit the virtual machine.

Note:
The user is allowed to edit *Name, CPU Cores* and *RAM* when the virtual machine is in Powered Off state.
The user is allowed to edit *Network Adapters* and *Storage* when the virtual machine is in Power On state.
The user is allowed to edit *RAM* and *Storage* when the virtual machine is in Paused state.

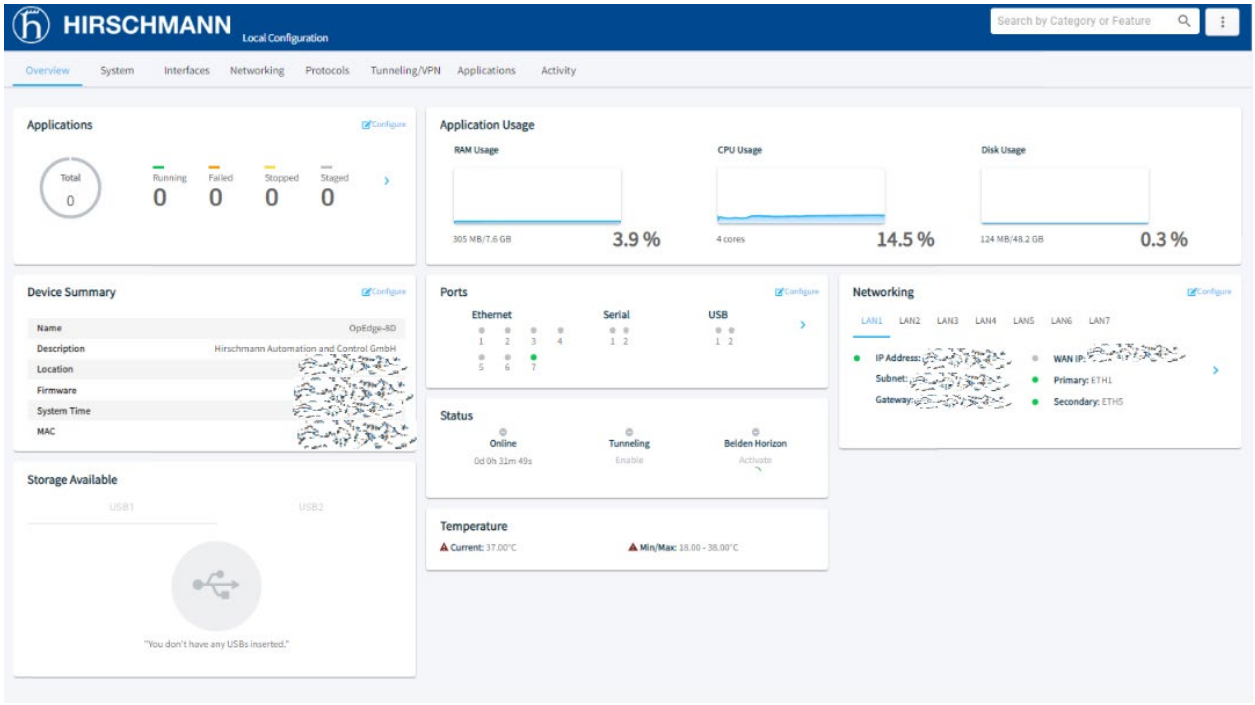
7 Diagnostics

7.1 Factory Reset – Configuration Webpage

To reset the OpEdge to factory default, perform the following steps:

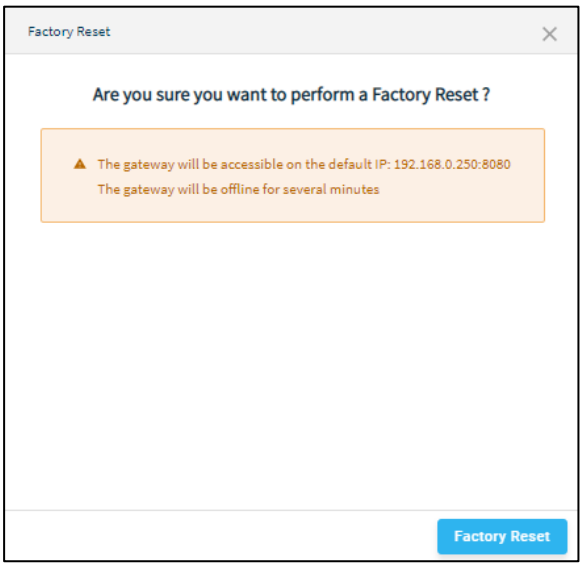
1. Establish a default connection to the OpEdge and perform the initial setup as described in the *Initial Configuration in* section 2.

2. On the OpEdge webpage, click the **SETTINGS** button  in the top right corner of the page.



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

   The *Factory Reset* pop-up is displayed.



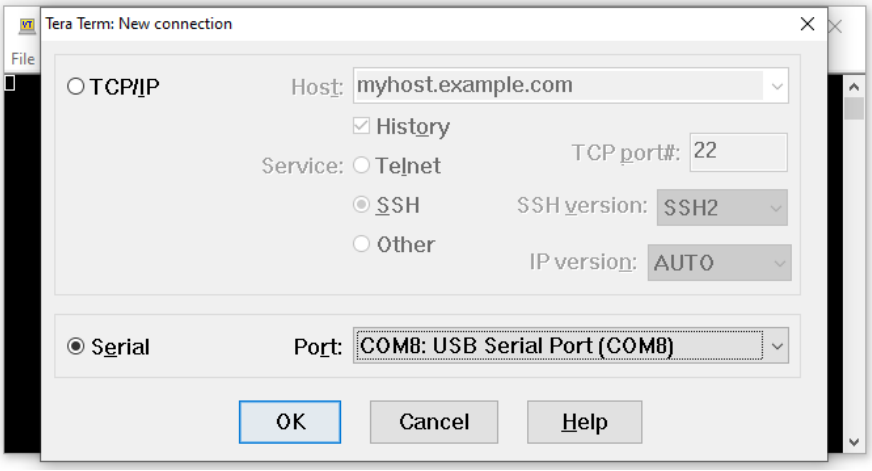
4 Click **FACTORY RESET** to initiate the factory reset procedure.

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.

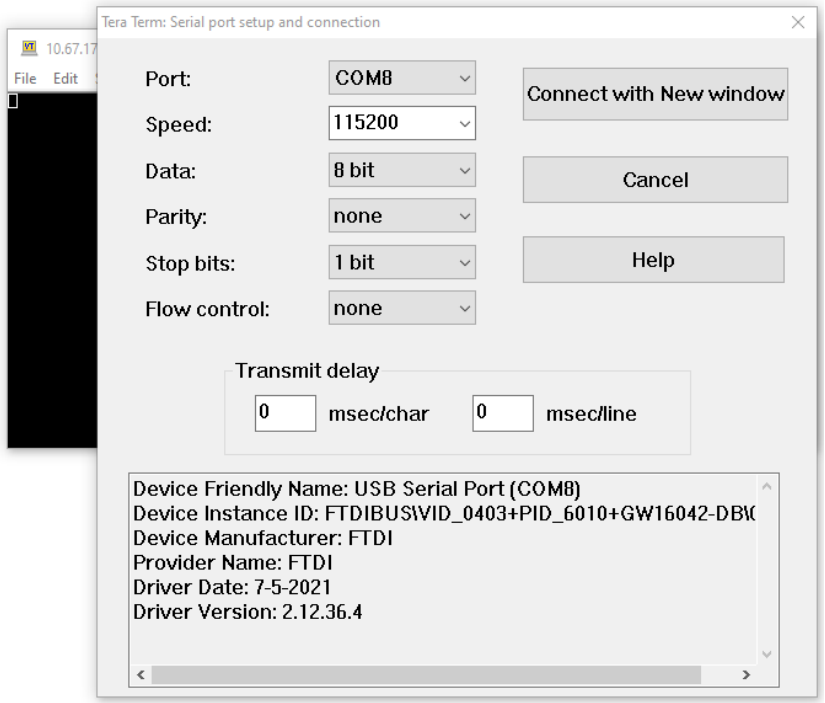
7.2 Factory Reset – Command Line Interface

To reset the OpEdge to factory default using the CLI, perform the following steps:

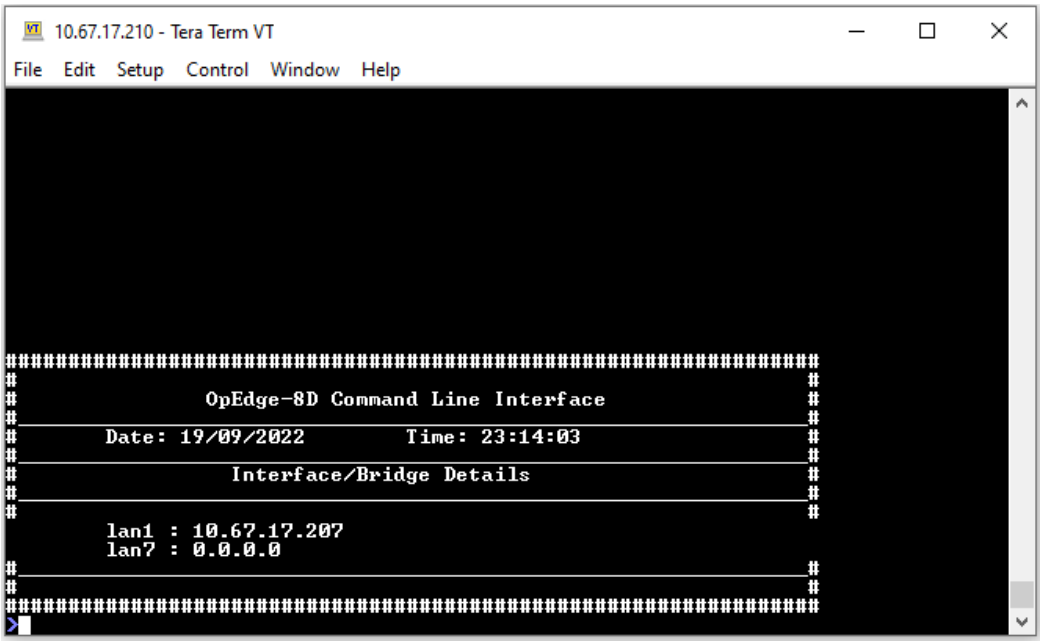
1. Connect to the console port of the OpEdge-8D using a Terminal Emulator like Tera Term or Putty.
2. Select the COM Port on which the console shall be connected.



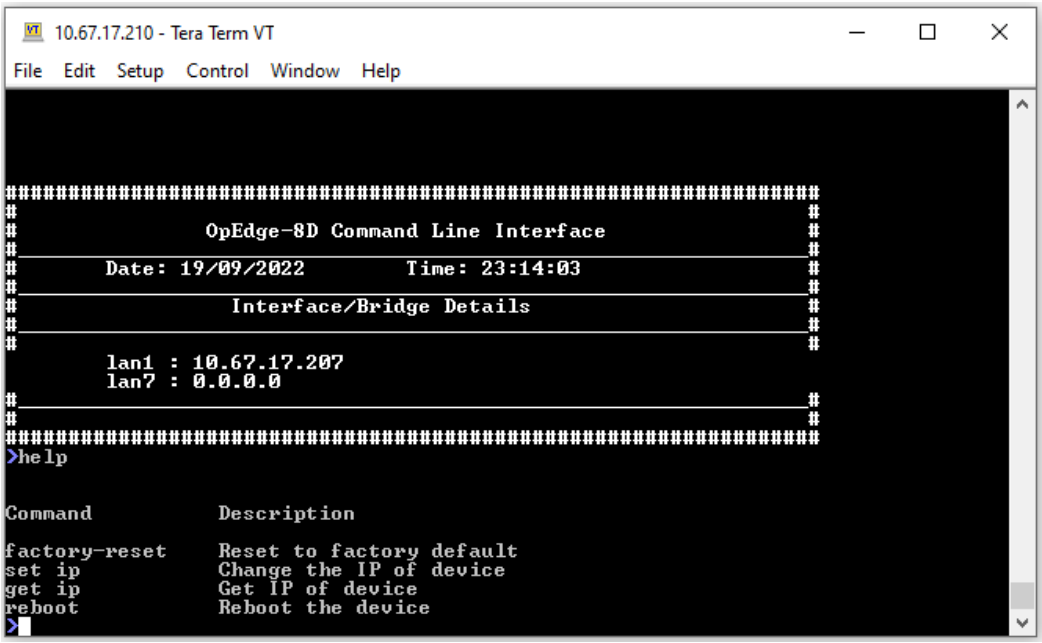
3. Set the below mentioned parameters for the Serial Ports:
   - **a)** Baud Rate/ Speed: 115200
   - **b)** Data: 8 bit
   - **c)** Parity: None
   - **d)** Stop Bits: 1 bit
   - **e)** Flow Control: None



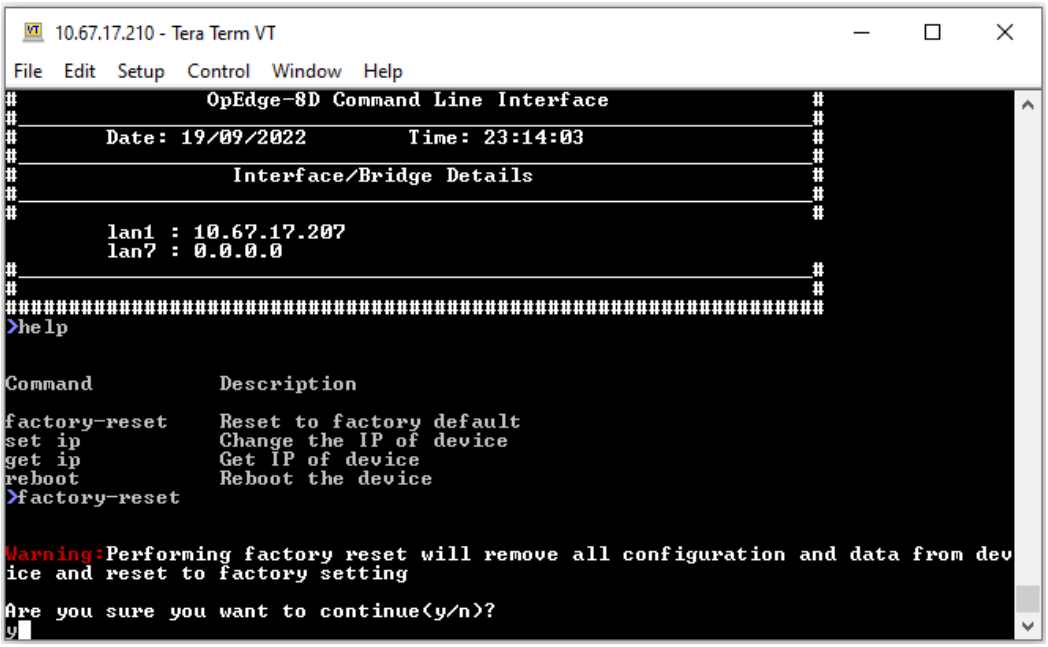
4 The command line interface will be available, on successful console connection to the OpEdge-8D.



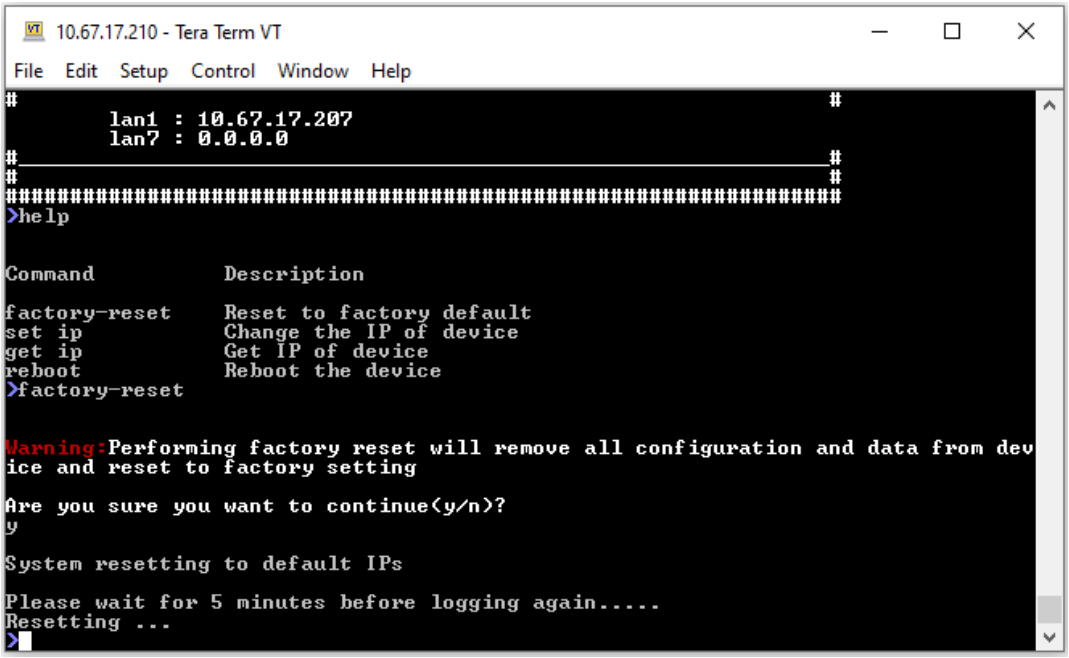
5 The help command on the CLI will display all the supported commands.



6 Execute the *factory-reset* command to reset the OpEdge-8D to factory settings. Confirm with a *y* (for yes) to do the factory-reset.

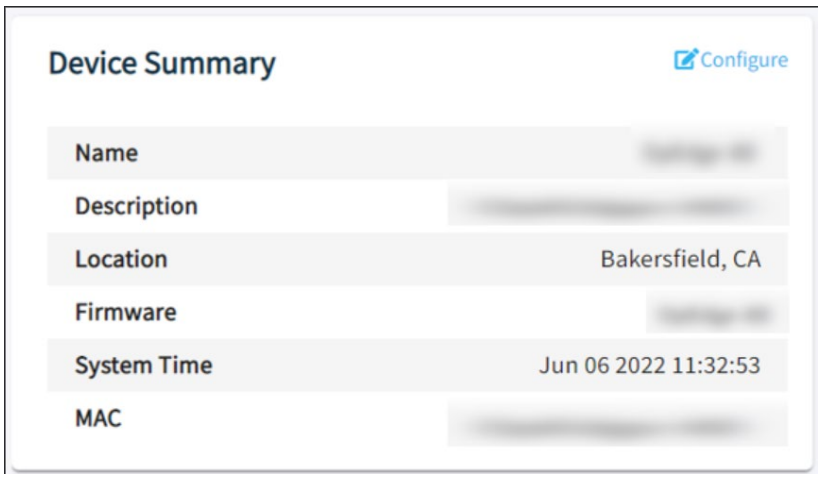


7 The OpEdge-8D will go into the factory-reset state and will be available to be connected on the default IP of 192.168.0.250 on LAN1 port after the process completes.



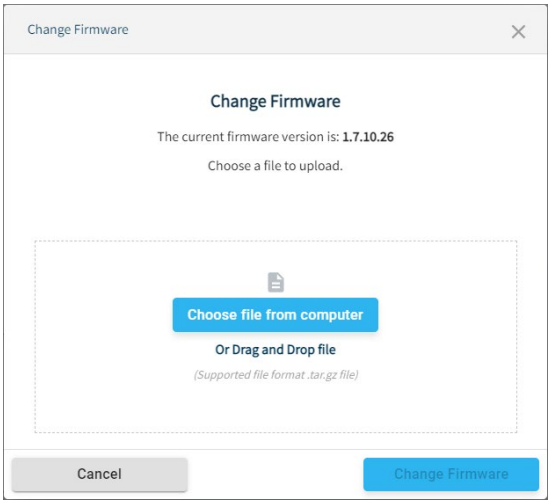
7.3 Updating Firmware

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



To upgrade the gateway firmware on the device, perform the following steps:

1. Open the OpEdge configuration webpage.
2. In the *Overview* tab > *Device Summary* tile, click **FIRMWARE** to open the *Change Firmware* dialog box.



3. Drop the **.tar.gz** file into the *Change Firmware* dialog box or click the **CHOOSE FILE FROM COMPUTER,** then click **OK**.
4. Click **SUBMIT** to upgrade the OpEdge firmware. The installation process takes approximately 5 minutes, and automatically reboots the OpEdge.
5. Verify the Firmware version in the *Overview* tab > *Device Summary* tile.

A. Abbreviations

Abbreviation	Description
ASCII	American Standard Code for Information Interchange.
CHAP	Challenge-Handshake Authentication Protocol. A method of authentication of remote clients used by Point to Point Protocol (PPP) servers and based on a shared secret.
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.
CRC	Cyclic Redundancy Check. A method of detecting errors in transmitted data.
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.
PAP	Password Authentication Protocol. An authentication protocol using unencrypted ASCII passwords over a network.
PC	Personal Computer
PPP	Point-to-Point Protocol. A data link protocol to establish a direct connection between two networking nodes.
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.
SCADA	Supervisory Control And Data Acquisition. A process control application that collects data from networked devices.
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.

B. Appendix

B.1 Syslog Description

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

The Syslog protocol supports the following severity levels:

Code	Severity	Description
0	Emergency	System is unusable
1	Alert	Action must be taken immediately
2	Critical	Critical conditions
3	Error	Error conditions
4	Warning	Warning conditions
5	Notice	Normal but significant condition
6	Information	Informational messages
7	Debug	Debug-level messages

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 "examp“eSDID@3243”, which has three parameters
MSG	BOMAn application log entry…	BOM indicates UTF-8 encoding, the message itself is “An Application log entry…”

B.2 Maintenance

Hirschmann is continually working on improving and developing their software. Check regularly whether there is an updated version of the software that provides you with additional benefits. You find information and software downloads on the Hirschmann product pages on the Internet at: http://www.hirschmann.com

C. Troubleshooting the OpEdge

1. **How do I configure one of the Ethernet ports on the OpEdge as a WAN port?**

   There are seven GB Ethernet ports on the OpEdge. 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 webserver or via Belden Horizon.

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 OpEdge's webpage through the WAN interface. To configure the OpEdge's *Allowed IP List*, go to the *System* tab.

   NOTE: The OpEdge's *Allowed IP List* is different to the *Allowed IP Connections* setting in Belden Horizon. *Allowed IP Connections* can only be configured in Belden Horizon. This is a list of specific end device IP addresses that a user can access when they tunnel (remotely connect via Belden Horizon) into the OpEdge. To configure the *Allowed IP Connections* setting, make sure the OpEdge is activated in Belden Horizon 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?**

   No, only one of the Ethernet ports can be configured as a WAN interface.

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 OpEdge in Belden Horizon? Do I need to do this?**

   It is highly recommended that the OpEdge be activated in Belden Horizon. Please refer to the User Manual or the Quick Start Guide for more details.

6. **I am unable to remotely access the OpEdge webpage. Why?**

   By default, the webpage is disabled when connecting remotely. The OpEdge can be managed via Belden Horizon when connecting remotely.

7. **Can I access the internet through the OpEdge?**

   Yes, the internet can be accessed through the OpEdge. Internet access is disabled by default. It is not recommended to 'always' enable the internet access.

8. **Does the OpEdge include a firewall?**

   Yes, it includes integrated firewall capabilities.

9. **Does the OpEdge support port forwarding?**

   Yes, it supports port forwarding.

D. Further support

Technical Questions

For technical questions, please contact any Hirschmann dealer in your area or Hirschmann directly.

You will find the addresses of our partners on the Internet at http://www.hirschmann.com

A list of local telephone numbers and email addresses for technical support directly from Hirschmann is available at

https://hirschmann-support.belden.com

This site also includes a free of charge knowledge base and a software download section.

Customer Innovation Center

The Customer Innovation Center is ahead of its competitors on three counts with its complete range of innovative services:

- Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planning.
- Training offers you an introduction to the basics, product briefing and user training with certification.

You find the training courses on technology and products currently available at
https://www.belden.com/solutions/customer-innovation-center

- Support ranges from the first installation through the standby service to maintenance concepts.

With the Customer Innovation Center, you decide against making any compromises in any case. Our client-customized package leaves you free to choose the service components you want to use.

Internet:
https://www.belden.com/solutions/customer-innovation-center