Emerson FBxEdge™ User Guide
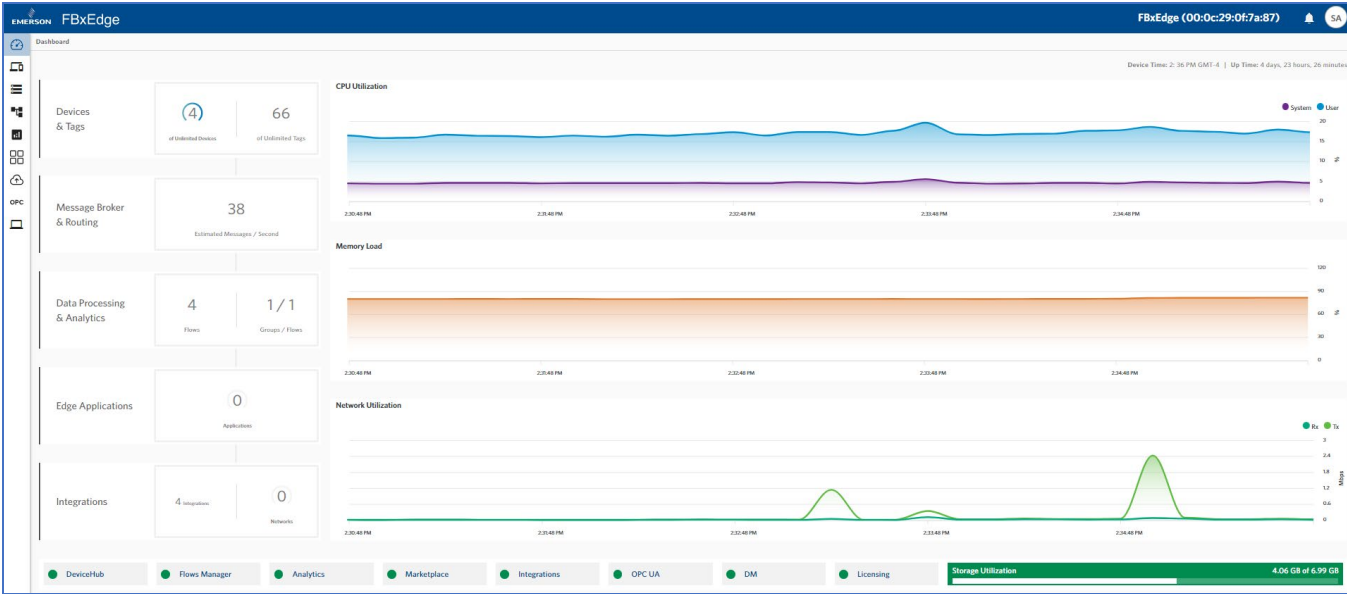

Energy and Transportation Solutions

EMERSON™

Application & Device Safety Considerations

- **Reading these Instructions**

  Before operating a device or application, read these instructions carefully and understand their safety implications. In some situations, improper use may result in damage or injury. Keep this manual in a convenient location for future reference. Note that these instructions may not cover all details or variations in equipment or cover every possible situation regarding installation, operation, or maintenance. Should problems arise that are not covered sufficiently in the text, immediately contact Customer Support for further information.

- **Protecting Operating Processes**

  The failure of a device or application – for whatever reason – may leave an operating process without appropriate protection and could result in possible damage to property or injury to persons. To protect against this, review the need for additional backup equipment or provide alternate means of protection (such as alarm devices, output limiting, fail-safe valves, relief valves, emergency shutoffs, emergency switches, etc.). Contact Energy and Transportation Automation Solutions for additional information.

- **Using Qualified Personnel**

  Installation, configuration, and any subsequent modifications to a device or application should only be performed by qualified, suitably trained personnel information.

- **System Training**

  A well-trained workforce is critical to the success of your operation. Knowing how to correctly install, configure, program, calibrate, and trouble-shoot your Emerson equipment provides your engineers and technicians with the skills and confidence to optimize your investment. Energy and Transportation Solutions offers a variety of ways for your personnel to acquire essential system expertise. Our full-time professional instructors can conduct classroom training at several of our corporate offices, at your site, or even at your regional Emerson office. You can also receive the same quality training via our live, interactive Emerson Virtual Classroom and save on travel costs. For our complete schedule and further information, contact the Energy and Transportation Solutions Training Department at 800-338-8158 or email us at *education@emerson.com*.

- **Grounding Equipment**

  Refer to Emerson Machine Automation Solutions product documentation for further information.

- **Protecting from Electrostatic Discharge (ESD)**

  Refer to Emerson Machine Automation Solutions product documentation for further information.

- **Ethernet Connectivity**

  This automation device is intended to be used in an Ethernet network which **does not** have public access. The inclusion of this device in a publicly accessible Ethernet-based network is **not recommended**.

- **Returning Equipment**

  If you need to return any equipment to Energy and Transportation Solutions (ETS), it is your responsibility to ensure that the equipment has been cleaned to safe levels, as defined and/or determined by applicable federal, state and/or local law regulations or codes. You also agree to indemnify ETS and hold ETS harmless from any liability or damage which ETS may incur or suffer due to your failure to ensure device cleanliness.

Contents

Chapter 1. Introduction

This guide provides a quick introduction to the Emerson FBxEdge™ solution, which consists of an edge device (either the Emerson RXi2 – LP Industrial PC or the Emerson RXi2 – BP Industrial PC) connecting to one or more Emerson FB3000 RTUs, Emerson FB1000 or FB2000 series flow computers, or Emerson ROC800 RTUs. This guide covers the installation of the physical edge device and details the process you use to link field devices to that FBxEdge device.

Note

Using FBxEdge, you can create a network of field devices linked into a single edge device. You can then use the FBxEdge Manager™ web-based software to connect multiple FBxEdge devices into larger network. For more information on FBxEdge Manager, refer to the *Emerson FBxEdge Manager User Guide* (part D301916X012).

Figure 1-1. The FBxEdge Environment
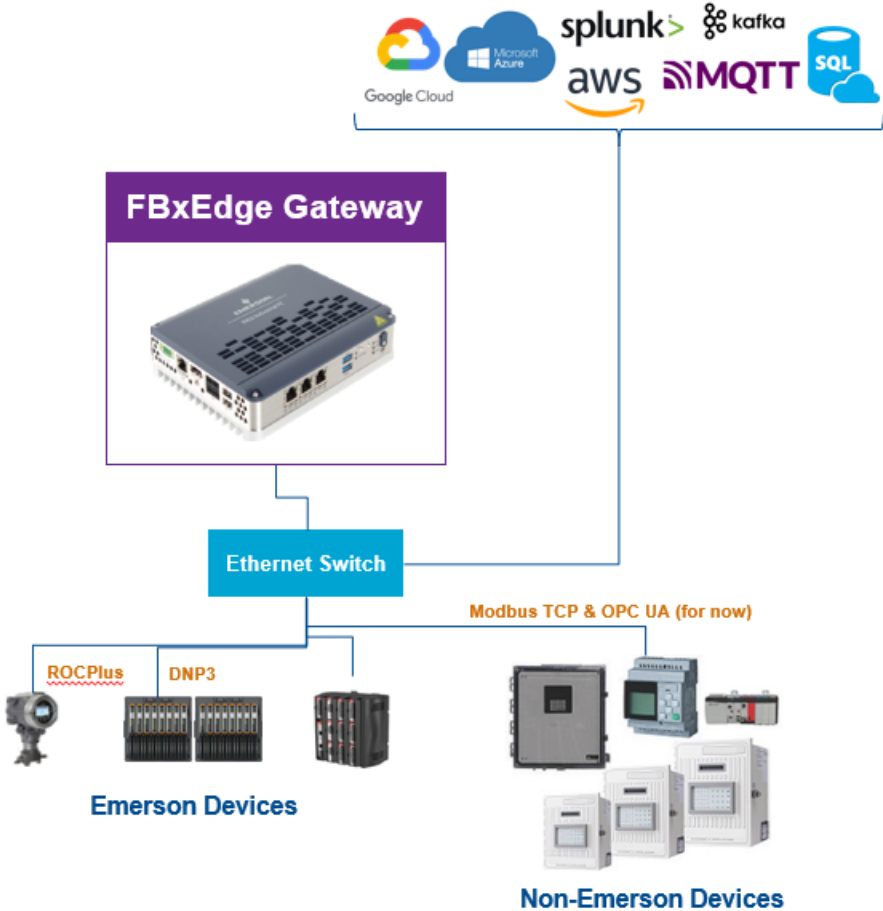
FBxEdge is a keystone component in an integrated combination of controllers, software, and IIoT solutions.

You can connect an unlimited number of devices and map an unlimited number of tags to an individual FBxEdge device. The edge device provides drivers for a multitude of devices and protocols, including DNP3 and ROC Plus.

1.1 Security Recommendations

Emerson recommends using encrypted protocols for communication with field devices. When this is not practical, consider the following:

- Use converters to encrypt/decrypt the communication path. As an example, use terminal servers with advanced security functions.

Alternately:

- Use a direct connection between the FBxEdge gateway and the field devices without connections to other networks.

Notes
- The current version of FBxEdge does not support FloBoss 107 flow computers or ROC800/ROC800L RTUs with Enhanced Security enabled.
- To use Tunneling protocol, disable the **Require Login** option.

1.2 LP and BP Device Ethernet Port Identification

Important
Note the following anomalies in the Ethernet port labels on both the LP and BP edge devices.

The **RXi2-LP** edge device provides four Ethernet ports: two to the left of the serial connections and two to the right of the pair of USB 2x ports. All ports support 10/100/1000 Base-T. For a proper 100/1000 Mbit connection, Emerson recommends using a CAT5 cable.

Figure 1-2. LP Ethernet Port Labeling

The **RXi2-BP** provides four Ethernet ports: three on the front panel (labeled ETH 1, ETH 2, and ETH 3) and one on its left side (labeled ETH 0). All ports support 10/100/1000 Base-T. For a proper 100/1000 Mbit connection, Emerson recommends using a CAT5 cable.

Figure 1-3. BP Ethernet Port Labeling
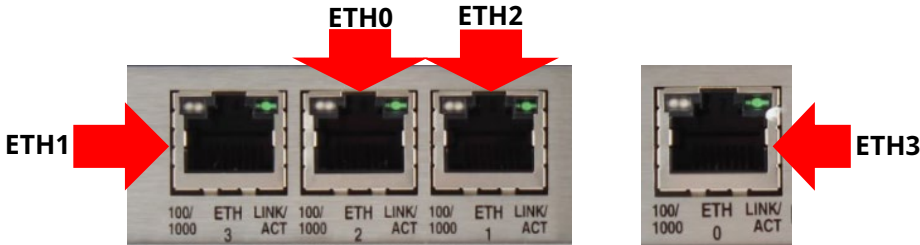
Chapter 2. Installing the FBxEdge Device

⚠️ **Important**

Emerson offers two edge devices as part of the FBxEdge solution: the default RXi2-LP and the optional RXi2-BP. Consult with your Emerson Impact Partner to determine which edge device best meets your organization's needs. This section discusses the installation of the **RXi2-LP** edge device. Refer to *Appendix A* for installation processes for the RXi2-BP edge device.

The RXi2-LP uses an AMD® G-Series Quad Core 1.2GHz processor, with 4Gb of RAM and 65Gb of storage. For further specifications, refer to the *FBxEdge Platform* product data sheet (D301940X012). When delivered from the factory, the FBxEdge software is pre-installed on the RXi2-LP edge device. You are responsible for installing the edge device in a suitable location.

Figure 2-1. RXi2-LP Industrial PC (Rear View)

2.1   Unpacking and Inspecting

🔶 **⚠ WARNING**

If the RXi2-LP edge device operates in an area of high ambient temperature up to 65 °C (149 F°), the surface of the enclosure, especially the heat sink, can reach a temperature of 80 °C (176 °F) and above. Be careful and do not touch the RXi2-LP with bare fingers.

2.1.1   Package Contents

Verify that the delivered package contains the following contents:

Item	Quantity	Description
RXi2-LP IPC	1	RXi2-LP Industrial PC
Serial Connector Plug	2	Serial Connector Plug
24V Power-in Connector Plug	1	Power Connector Ring
Emerson FBxEdge User Guide	1	User manual for device (part D301913X012)

2.2 Power Requirements

The RXi2-LP requires a DC power supply with 24V (± 20%) that delivers at least 1.8A. The corresponding plug is a Phoenix Contact 1748367. Use the same connector type or its equivalent.

Note

Once you have connected power, use the power button (on the left side of the device) to power up the edge device. The LED status indicator is solid amber as the unit starts up and switches to solid green during normal operation.

Figure 2-2. Power Connector

Signal Name	Pin (left to right)
FGND	2
Power – (24V DC)	2
Power + (24V DC)	1

2.3 Ports

The RXi2-LP provides several ports you can use to connect devices.

Figure 2-3. Connection Ports on RXi2 LP

2.3.1 DP Display Port

The RXi2-LP provides one digital display interface (located between the power connector and two USB ports). It transmits audio and video simultaneously. Use the port to directly connect a monitor with a DP input or use standard off-the-shelf adapters to convert the DP signals to HDMI or VGA.

Figure 2-4. DP Display Port

2.3.2   USB3.2 Gen1 and USB2 Ports

The RXi2-LP provides four USB ports, all using Type A connectors. Two (which support USB 3.2 Gen1) are located between the DP port and a pair of Ethernet ports. Two additional USB ports (which support USB2) are located to the left of a second pair of Ethernet ports. Each USB port is protected with an electrical fuse rated up to 1A. For normal operation, do not exceed 900mA for USB 3.2 Gen1 or 500mA for USB2. Limit cable length to no more than 3m.

Figure 2-5. USB Ports (3.2 and 2)
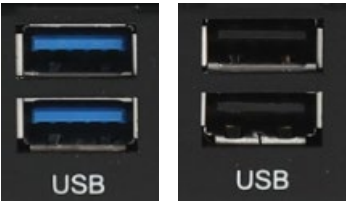
2.3.3   Ethernet Ports

The RXi2-LP provides four Ethernet ports: two to the left of the serial connections and two to the right of the pair of USB 2x ports. All ports support 10/100/1000 Base-T. For a proper 100/1000 Mbit connection, Emerson recommends using a CAT5 cable.

⚠️ **Important**
See *Figure 2-6* for the assignment of Ethernet ports on the LP:

Figure 2-6. Ethernet Ports
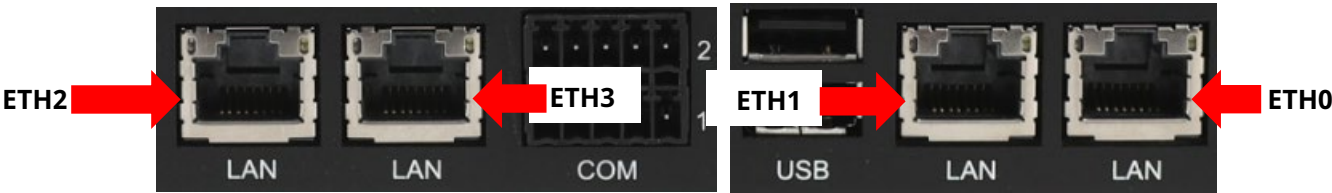
2.3.3.1   Ethernet Port LEDs

All Ethernet ports use the same LED configuration.

Figure 2-7. Ethernet LEDs
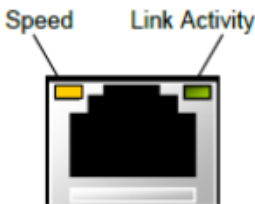
Pin	LED Color	LED Status Indicator
13/14	**Green** **Yellow** Off	LINK1000 (steady on) LINK100 (steady on) LINK19
12	**Green**	ACT/LINK Blink with activity Steady on with no activity at 10/100/100

2.3.4   Serial Ports

Note

The FBxEdge software does not currently support serial-based communications.

The RXi2-LP provides two serial interfaces, one (1) configured to RS-232 and one (2) configurable to RS-422 or RS-485 (2W/4W). The connector is a Phoenix Contact 1953745 or equivalent and mates with a Phoenix Contact 1952296. Two mating plugs are shipped with the unit. The RS-232 cable can be no longer than 15m. The RX-4xx cable can be more than 30m, depending on capacitive cable load.

Figure 2-8. Serial Ports

Signal Name RS-232	Pin
TXD	1
RXD	2
RTS	3
CTS	4
GND	5
Signal Name RS-485	**Pin**
TX+	6
TX−	7
RX+	8
RX−	9
GND	10

For RS–422 and RS–485-4-wire modes, connect the corresponding RX+/− signals with the TX+/− signals and vice versa on the remote device. For RS–485 2-wire mode, connect RX+

and TX+ with the + line of the cable and the RX– and the TX– together with the – line of the cable.

The TX/RX signal control is difference between the various RS–4xx modes. In the RS–422 mode, TX and RX are always active. In RS–485 **4-wire** mode, TX is active only when there is something to transmit, while RX is always active. In RS–485 **2-wire** mode, TX and RX are active when transmitting and inactive when not transmitting.

Note

The RXi2-LP system does not provide any termination resistors. If required, attach the termination resistor directly to the plug.

2.3.5   Audio Jacks

The RXi2-LP provides two audio jacks (Line-Out and MIC). Connect external speakers or a headphone to the lime-colored Line-Out jack. Connect an external microphone to the pink-colored MIC jack.

Figure 2-9. Audio Jacks
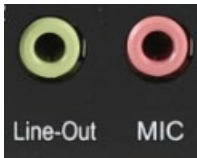
2.4   Coin Cell Battery

A CR2032 lithium-ion coin cell battery powers the real-time clock and CMOS memory. The battery provides an auxiliary source of power when the main power is shut off or disconnected.

Figure 2-10. Location of Coin Cell Battery
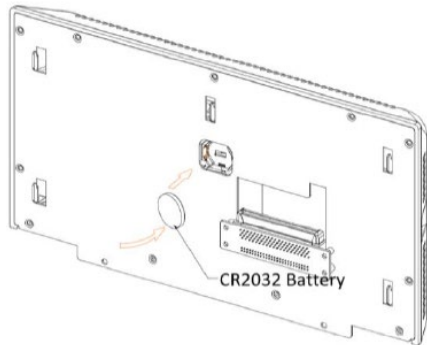
2.5   Mounting the RXi2 LP Edge Device

> ### ⚠ CAUTION
>
> Install the RXi2-LP edge device **only** in restricted access locations.

⚠ **Important**

The RXi2-LP edge device is designed **only** to be mounted **horizontally**. Mounting it vertically prevents the housing's heatsink fins from appropriately cooling the device.

All units ship with a wall mount bracket attached to the base of the CPU. The figure below shows the attachment specifications for the wall mount bracket.

Figure 2-11. Minimum Clearances for RXi2 LP

Chapter 3. Configuring the Edge Device

Each FBxEdge device requires an IP address for communications and configuration.

3.1   Acquiring an IP Address

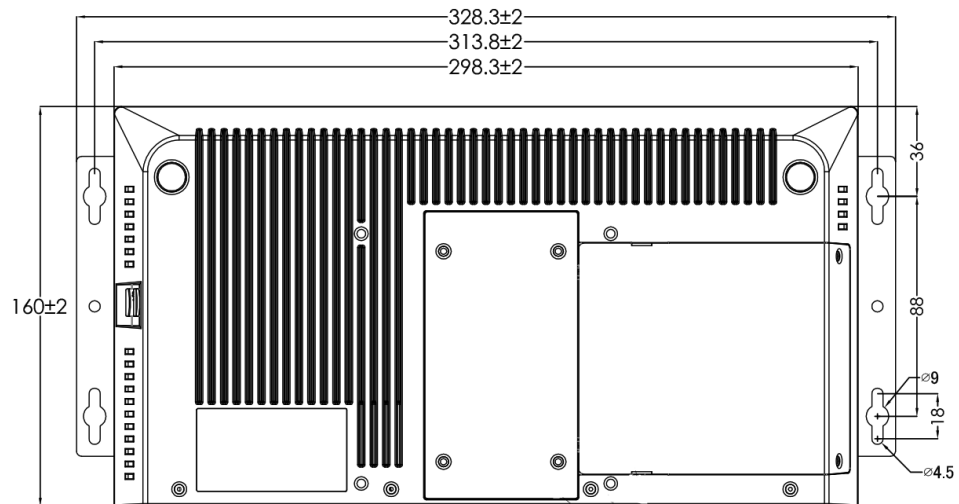By default configuration, an FBxEdge device acquires an IP address dynamically from its DHCP server. However, if the device is connected to a network which does not have a DHCP server, you must manually assign a static IP address to the device.

3.1.1   IP Address Assigned by DHCP Server

Before configuring an FBxEdge device, you first need the IP address the DHCP server dynamically assigns to that device:

1. Attach a keyboard (using the USB port) and a monitor (using the DP port) to the edge device.
2. Connect the edge device to your network with an Ethernet cable.
3. Connect the edge device to power.
4. Press the power button (located at the left rear of the RXi2 LP) and wait for the edge device to boot.

Figure 3-1. Edge Device Welcome Screen
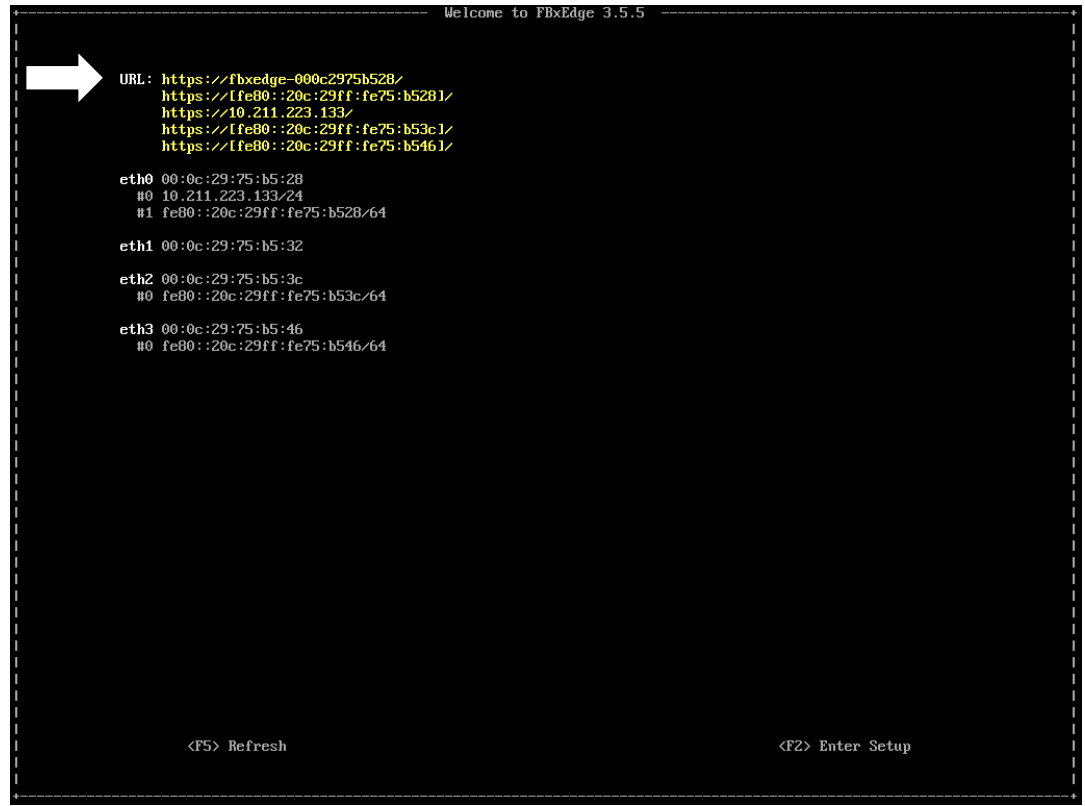
5. Review the screen and record the server-assigned IP value (here, **https://10.211.223.133**).

Once you have the IP address for the edge device, proceed to *Section 3.2, Accessing FBxEdge*.

3.1.2   IP Address Assigned Manually

To assign a static IP address to an FBxEdge device:

1. Attach a keyboard (using the USB port) and a monitor (using the DP port) to the edge device.

    Note
    The device's user interface **does not** support a mouse. You must use the keyboard to navigate. Use the **Tab** key to move from one field to the next. Use the arrow keys (⌃⌄) to select list items, and use the **Enter** key to select an option or move to the next display in the workflow.

    The user interface logs you out if no activity occurs within a few minutes. You must then press **F2** to log back in.

2. Connect the edge device to your network with an Ethernet cable.

3. Connect the edge device to power.

4. Press the power button (located at the left rear of the RXi2 LP) to boot the edge device. When the system startup is complete, the device's welcome screen displays.

5. Press **F2** to enter the setup.

6. For the initial login, you must select a keyboard layout. Use the up and down arrows (▲▼) on your keyboard to select a keyboard layout. The **us** keyboard is sufficient for most English keyboards.

Figure 3-2. Edge Device Keyboard Layout Screen
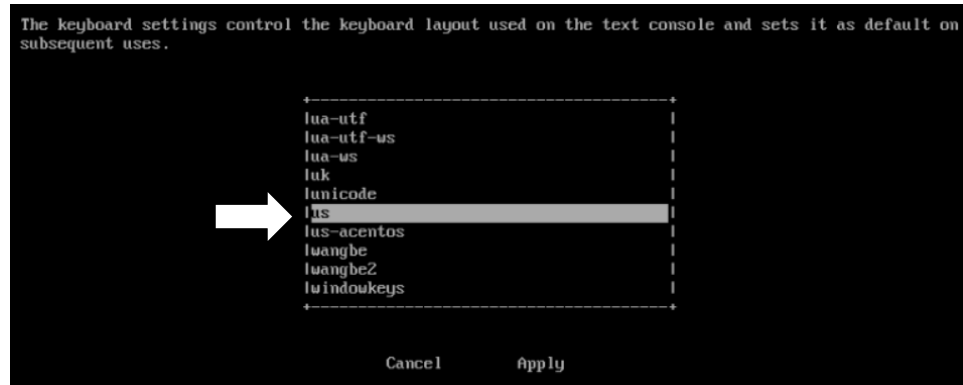
7. Press **Enter** to select that layout. The login screen displays:

Figure 3-3. Edge Device Login Screen
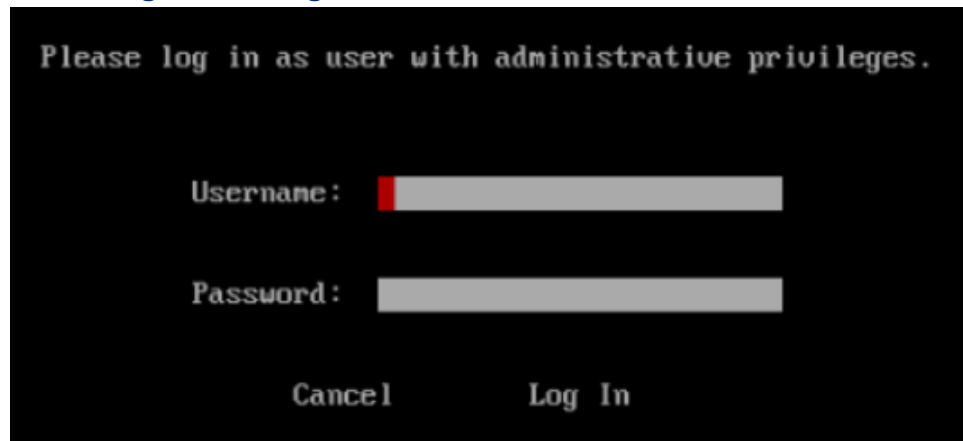
For the initial login, the credentials are **admin** and **edge**.

8. Enter the initial credentials (use the Tab key to move from one field to the next).

9. Tab to **Log In** and press **Enter**.

For the initial login when using a static IP address, the License Agreement screen displays:

Figure 3-4. License Agreement Screen
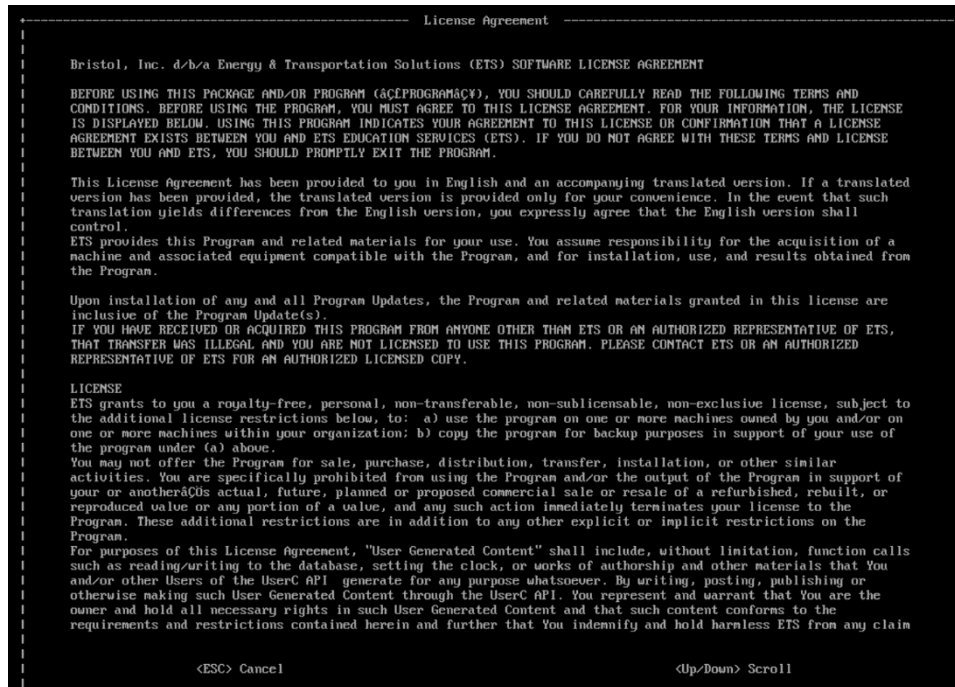
10. Use the down arrow key to scroll through the license agreement.

11.   Press **Enter** to accept the license. The Change Password screen displays:

Figure 3-5. Change Password Screen
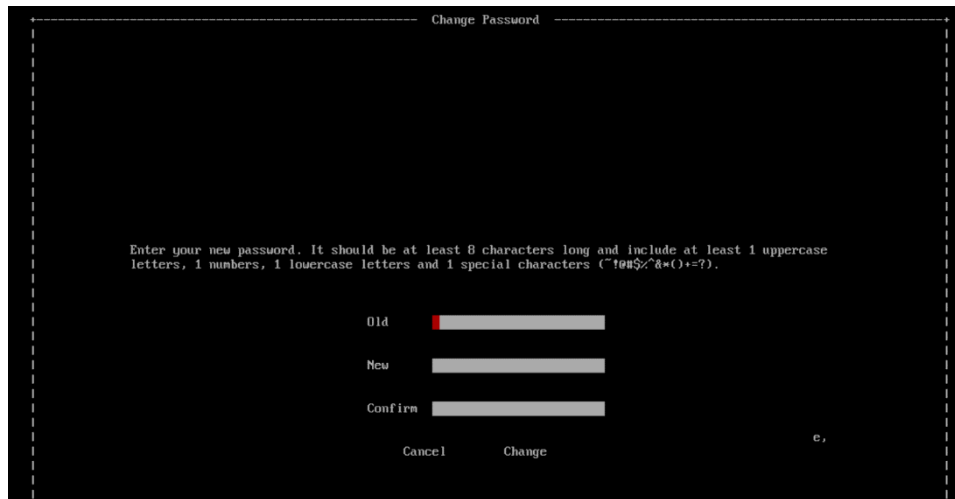
12. Press **Enter** to accept the license. The Change Password screen displays:

13. Enter the old password (**edge**). Tab to the New field and enter a new password (based on the password recommendations).

14. Tab to the Confirm field and re-enter the new password.

15. Tab to select **Change** and press **Enter**. The System Settings screen (*Figure 3-6*) displays.

3.1.2.1 Setting the Static IP Address

The user interface for the FBxEdge device duplicates many of the configuration options available through the web interface. To set a static IP address, select the **Configure Interfaces** option.

Figure 3-6. System Settings Screen
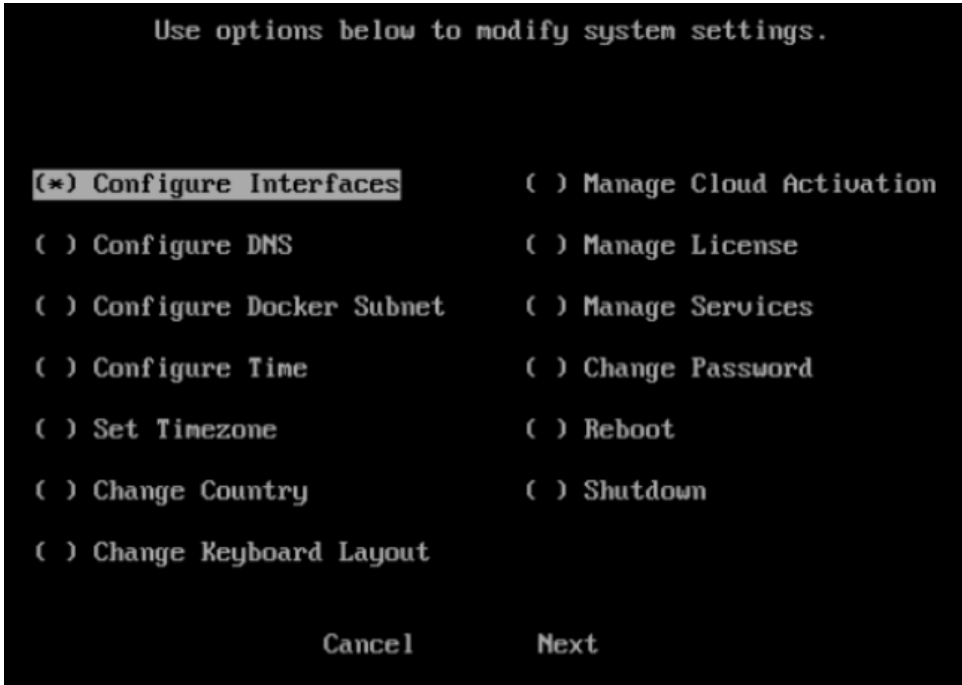
1. Tab to the **Configure Interfaces** option and press **Enter**. The Select interface screen displays.

Figure 3-7. Interface Configuration Screen
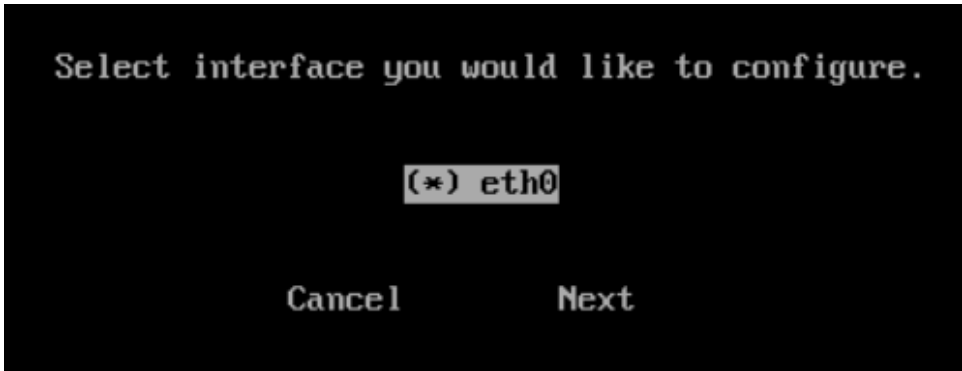
2. Enter the name of an interface (here, **eth0**), tab to **Next**, and press **Enter.** The Interface screen displays for the selected interface:

Figure 3-8. Interface Screen
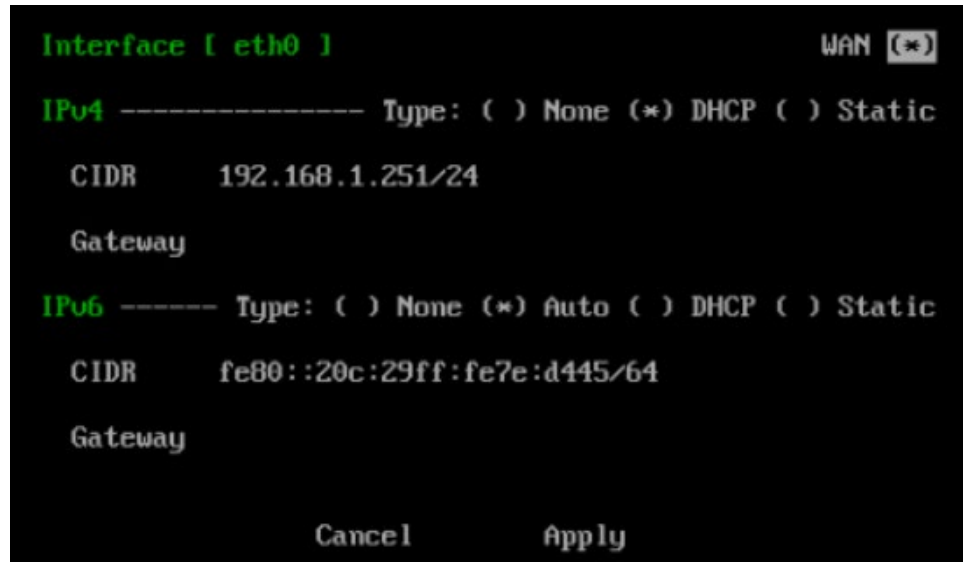
3. Use the Tab key to select the desired option (here, **IPv4** or **IPv6**) and then tab over the fields (Type, None, Auto, etc.) to select **Static**. Tab down to **Apply** and press **Enter**. The screen adds CIDR and Gateway fields:

Figure 3-9. Interface Screen

4. Complete the fields as necessary:

- **CIDR**: Classless Inter-Domain Routing notation defines a block of IP addresses (similar to network subnetting). This example notation (**192.168.0.251/24**) means that the first 24 bits of the IP address are used for network routing.

- **Gateway**: Defines the default gateway address on a network, which can be locating using the *ipconfig* command.

5. Tab to **Apply** and press **Enter**. The System Settings screen displays.

Figure 3-10. System Setting Screen

6. Tab to **Reboot** and press **Enter**. The Reboot screen displays.

Figure 3-11. Reboot Screen

7. Press **Enter** to confirm the reboot. Once the reboot completes, the Welcome to FBxEdge screen displays, showing the static IP address (here, **192.168.1.251**).

Figure 3-12. Welcome to FBxEdge Screen

8. At this point you can either press F2 to log into the console or use the IP address to log into the Web user interface.

> ⚠ **CAUTION**
>
> Make sure your TCP/IP settings reflect the port the Ethernet cable is using. Refer to *Figure 3-1* to identify the connected port. If you mistakenly save TCP/IP settings to an unconnected port, the edge device **does not** save those settings.

FBxEdge uses a self-signed certificate. Follow the browser guidelines for how to bypass a self-signed security error message.

The initial username and password (**admin** and **edge**) are provided so that the administrator can define a local username and password. Change them on the first use.

3.2 Accessing FBxEdge

The FBxEdge software requires a license to function. When first installed, FBxEdge uses a 15-day trial license. After 15 days, the system will not function unless you apply an actual (non-trial) license.

⚠️ **Important**

To access the web-based UI, use the Google™ Chrome™ browser and ensure it can establish a network connection to the edge device. The browser **must be able** to establish a network connection to the edge device.

To access FBxEdge:

1. Enter the IP address (such as **https://12.345.678.910**) for the edge device into the browser's address/URL bar and press **Enter**. The FBxEdge Login screen displays:

   Figure 3-13. FBxEdge Login Screen

2. Enter the default credentials (Username=**admin**; Password=**edge**).

3. Click **Login**.

⚠️ **Important**

So that an administrator can define a local user name and password, these default login credentials function **only** for the **first** login. You **must** change your password for any subsequent logins.

4. FBxEdge opens in your browser, displaying the Dashboard by default.

Figure 3-14. FBxEdge Dashboard
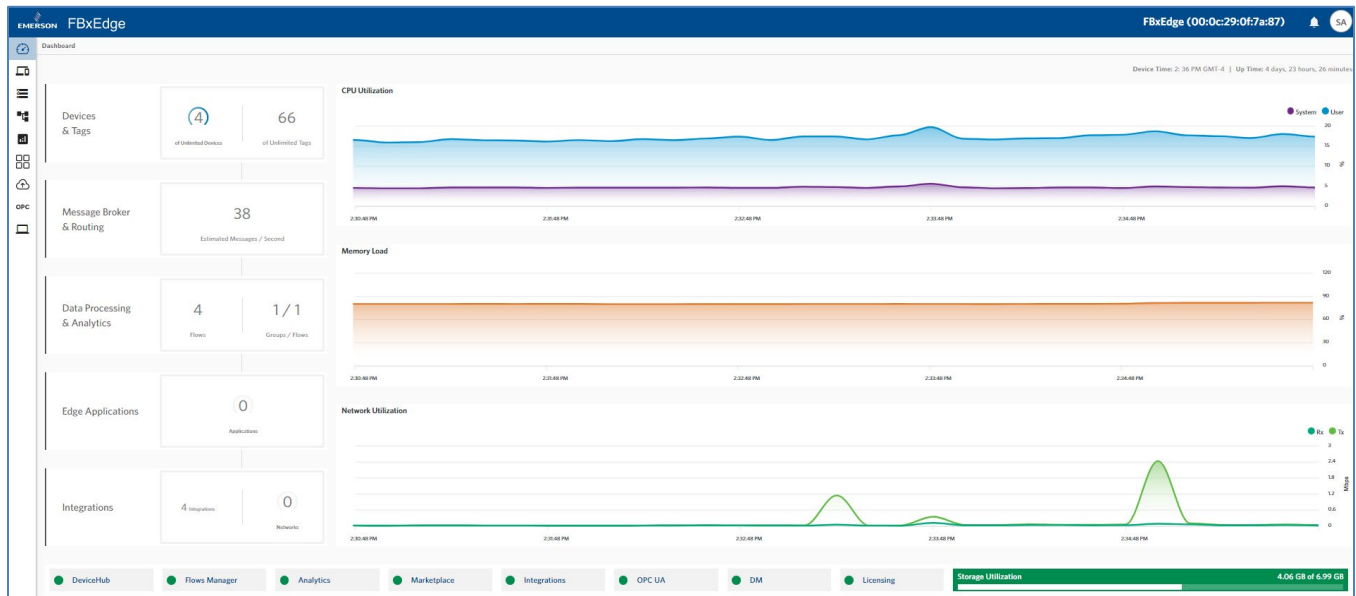
Notes

- **Do not** forget your password. For security reasons, there is **no** password recovery. If you lose the administrator password, you must reinstall the software.

- You can reset your password at any time.

- When logging in, you can use an internal username and password or (if the network is connected to LDAP or Active Directory) you can use this password as well. The software displays an additional Provider ID field after LDAP configuration. LDAP configurations allow you to use existing company credentials for authentication. See *Section 4.7, LDAP/AD Authorization* for more information about LDAP configuration settings.

- You can always access the software so long as your browser is on the same network as the software and device, even if you do not have an Internet connection.

3.2.1   Useful Links

A navigation panel at the left side of the Dashboard contains several icons arranged vertically. Click the icons to access FBxEdge modules:

Figure 3-15. FBxEdge Module Icons
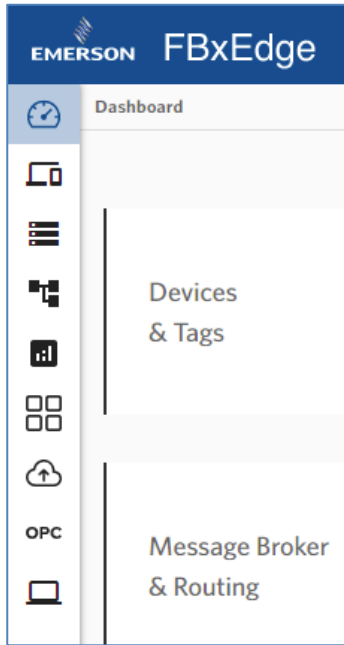
Icon	Description
	Click to access the **Dashboard** module, which displays a summary overview of the FBxEdge system **Note**: The Dashboard displays by default when you access FBxEdge.
	Click to access the **DeviceHub** module and its component options (Devices, Tags, Device Discovery, and Utilities)
	Click to access **Database Management** module and its component options (DB Management and DB Users)
	Click to access the **Flows Manager** module
	Click to access the **Analytics** module's workspace and its component options (Instances, Instances Table, and Models)
	Click to access the **Applications** module and its component options (Dashboard, Catalog Apps, Configure, Marketplace, Containers, Networks, Images, Registry, Volumes, System Info, and Disk Usages)
	Click to access the **Integration** module
	Click to access the **OPC UA** module and its component options (Hierarchy, Management, and Connections)
	Click to access the **System** module and its component options (Info, Certificates, Network, Remote Access, Device Management, LDAP/AD Authorization, Users, Tokens, Services, External Storage, Policy Management, License, Events, Support, and Backup/Restore)

At the extreme right end of the FBxEdge toolbar is the circular UserName icon (here, **SA** for System Administrator). Click it to display a menu with support and information options:

Figure 3-16. Support/Information Menu
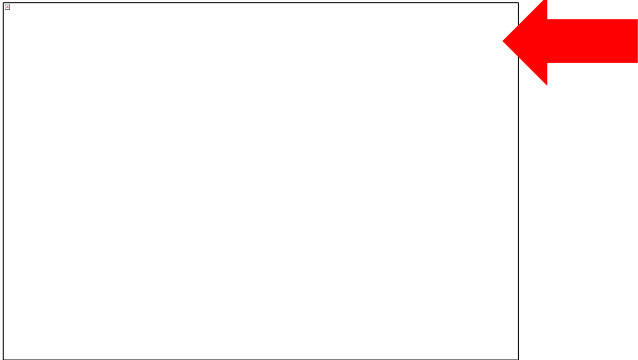
3.2.2 Setting the Timezone

One of the first configurations you need is to reset the default timezone to your organization's location. (The default setting is Universal Time Coordinated or UTC.) Setting the timezone ensures that the system performs backups and produces reports according to your organization's requirements.

1. Select the **System** icon, the **Network** option, and the **Configure** tab. The Configure page displays:

Figure 3-17. Configure Options
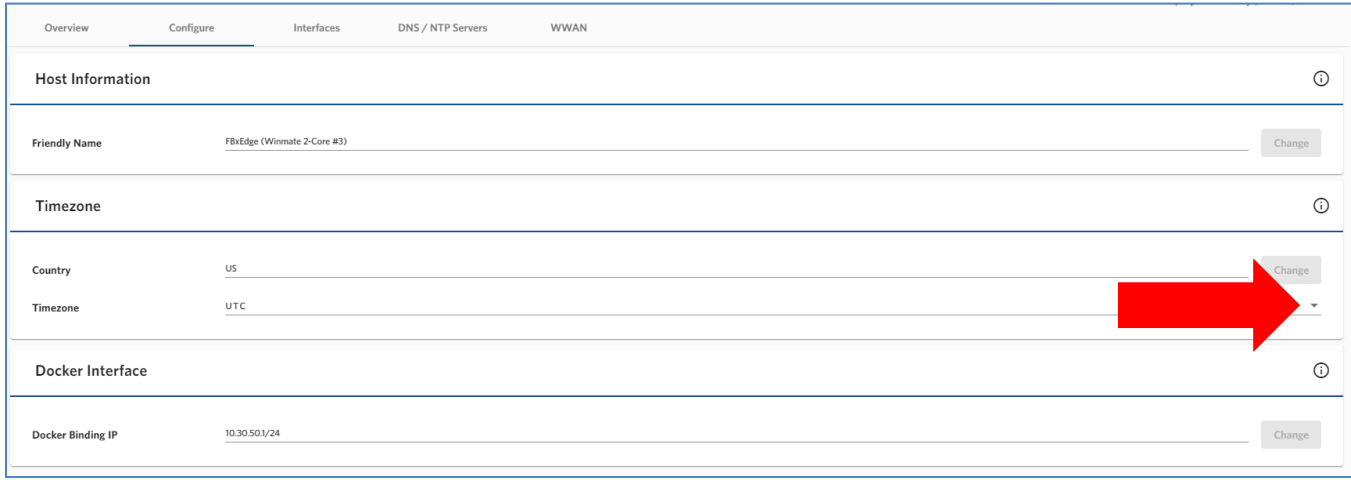
2. Select the ▼ at the extreme right of the Timezone field on the page. The system displays an alphabetic listing of defined timezones.

3. Select a timezone for your organization. The system displays a warning message:

Figure 3-18. Timezone Warning

You must reboot the device for timezone change to take effect. Are you sure you want to change the timezone?

No   Yes
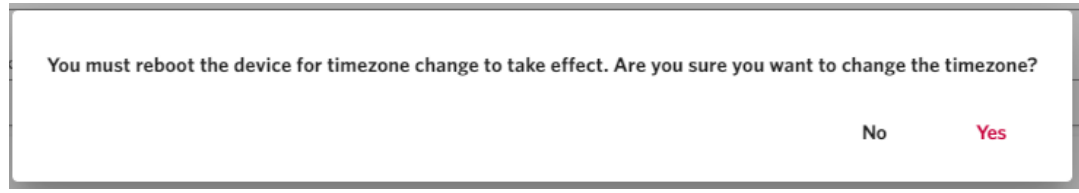
Changing the timezone requires a system reboot.

4. Click **Yes** to implement your change (or **No** to exit). The system reboots.

When the system reboots, repeat step 1 to verify that the timezone is now changed.

Important

For **DNP3 devices**, the timezone you configure in FBxEdge is the timezone the system applies to a DNP3 device when you enable the option to synchronize time. Although the DNP3 standard dictates the use of UTC at all times, customers may prefer to set the timezone of their DNP3 devices to the timezone in which that device is located. To prevent FBxEdge from resetting the timezone for DNP3 devices to UTC, follow the procedure in steps 1 through 4.

3.3   Adding a ROC Device

Once you have logged into FBxEdge, select the **DeviceHub** icon.

Figure 3-19. DeviceHub Icon
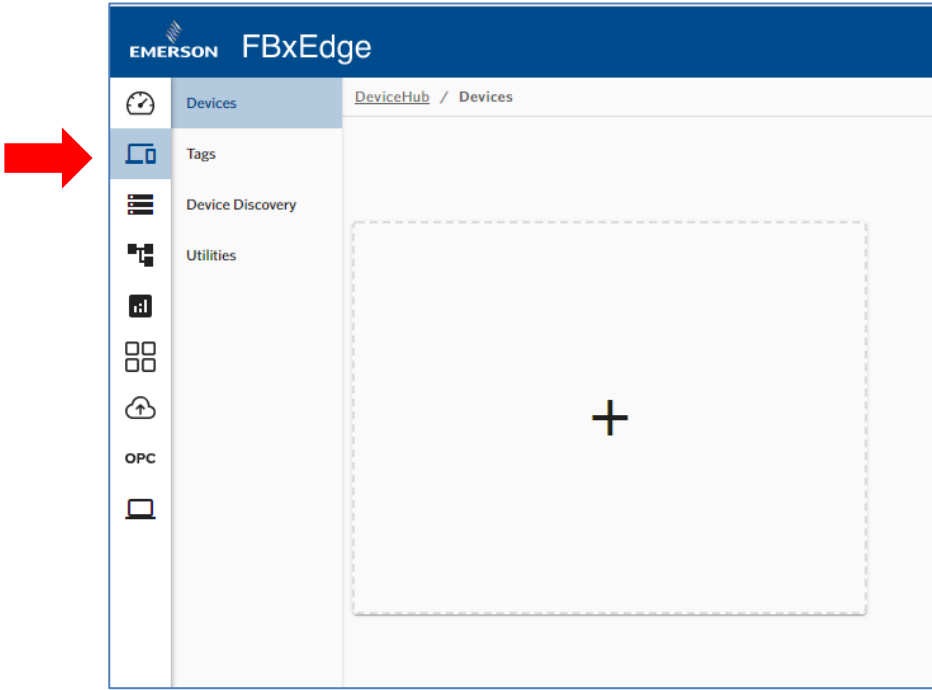
The DeviceHub module allows you to connect **devices** (PLCs, controllers, sensors, etc.) to FBxEdge, as well as add register values as **tags** for data polling. DeviceHub currently supports only Emerson devices although drivers from all major manufacturers (ABB, Siemens, Allen Bradley, Hitachi, etc.) are available for testing.

Once you have added a tag to a connected device, FBxEdge polls that tag for data according on the frequency you define. The system normalizes the polled data and posts it to the internal Message Broker. You can then subscribe to the data available from the Message Broker for processing, visualization, and analysis.

The DeviceHub module's UI has four components:

Component	Description
Devices	Adds or connects devices to FBxEdge. You can then manage (modify, refresh, stop/start, etc.) the connected devices, and optionally add custom metadata to devices in the form of key/value pairs.
Tags	Adds tags individually, in bulk, or by browsing a connected device and manages (modify, view, add an OMA binding, copy, etc.) tags.
Device Discovery	Enables/disables the discovery mode. When discovery mode is enabled, FBxEdge allows you to view devices on the connected network.

Component	Description
Utilities	Tests the connectivity of IP addresses and the accessibility of specific ports.

When you connect to a device, the tiles on the pane show how many devices are currently connected or disconnected. A green CONNECTED indicator means that a connection to the device has been established. You **must** stop a device to delete or disconnect it.

To add a device from the DeviceHub tab:

1. Select the **Devices** tab and select the + sign (the **Add** option):

Figure 3-20. Devices Tab
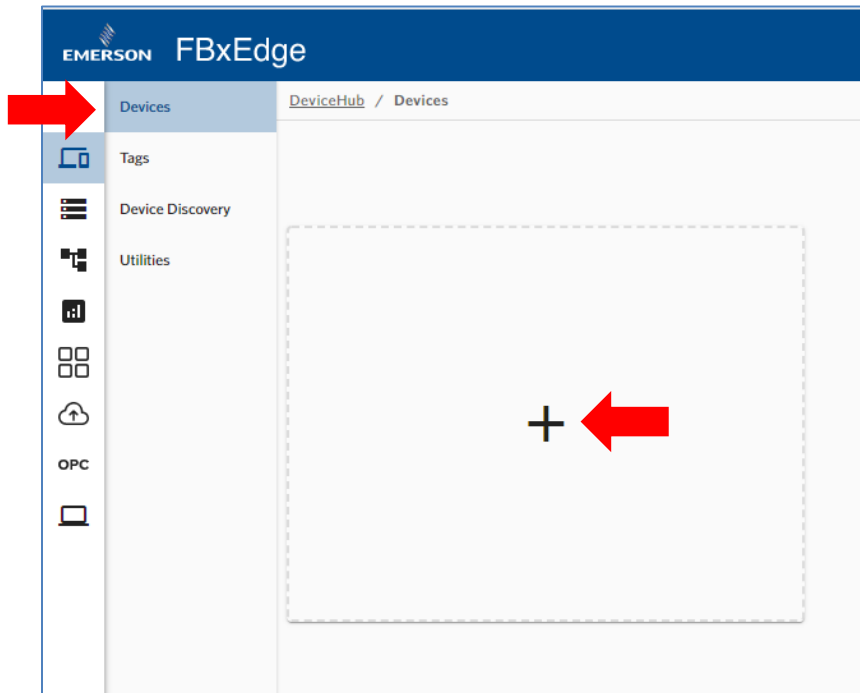
The **Connect Device** prompt displays:

Figure 3-21. Device Type Prompt
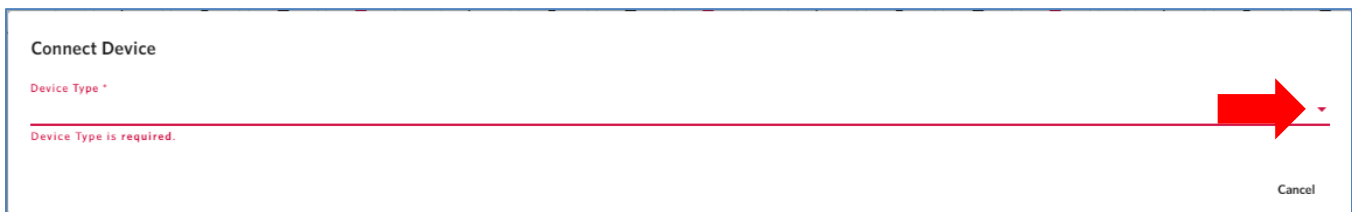
2. Click ▼ at the right end of the Device Type field to display a drop-down list of device vendors. Select a vendor (here, **Emerson**). The system then adds a Driver Name field:

Figure 3-22. Device Driver Prompt

3. Click ▼ at the right end of the Driver Name field to display a drop-down list of device drivers. Select a device vendor (here, **ROC800 Ethernet**). The system then displays a Connect Device screen with your chosen device type and driver name:

Figure 3-23. Connect Device Screen

Based on the information stored in the system for the selected device type and driver, the system pre-populated some fields on the screen.

4. Review and modify these fields, if appropriate.

Note
An asterisk (*) to the right of the field name on the page indicates a mandatory field.

| Field	Description
Name	Provides the system-assigned driver name. You can modify this name if appropriate.
Description	Provides a description of the device.
Network Address	Indicate the system-provided Ethernet address for this device (here, **192.168.0.1**).
Network Port	Indicates the network port for this Ethernet address (here, **4000**).
Operator ID	Indicates the operator ID for this device (here, **LOI**).
Password	Indicates the password for the operator ID, masked for security purposes.
Device Group	Indicates the group to which this device belongs (here, **240**).
Device Address	Indicates the address for this device (here, **240**).
Host Group	Indicates the host group for this device (here, 1).
Host Address	Indicates the address of the host group for this device (here, **239**).
Next Request Delay	Defines, in milliseconds, how long the system waits before submitting the next polling request.
Optimizations	Enables or disables how FBxEdge gathers tag values. Click ▼ at the end of the field to display and select the appropriate state.
	Select **Enable** to allow FBxEdge to collect as many values as quickly as possible during a polling request. Select **Disable** (the default) to restrict retrieval to only one value at a time.
	Note: We recommend that you enable optimizations and then specify a small value (such as 20 milliseconds) for the Next Request Delay field.
Meta Tags	Select to add meta tags to the device. See *Section 3.5, Adding Tags*.
Status Register	Select to define an optional register for keeping track of the device's status. See *Section 3.4, Defining the Status Register*.
Enable Alias Topics	Select to allow use of a "friendly" name when referencing the tag in other areas of FBxEdge. If you do not enable alias topics, FBxEdge automatically uses GUID (such as *devicehub.raw.5D7D4E72-DB16-41E5-9E5D-A0AFAE801A04.43B10C12-3A14-4B76-8973-52D5A9694DC6*) to ensure unique tag names.
	Note: This option is enabled by default.

Field	Description
Enable logging	Select to enable system logging.
Enable Data Store	Select to indicate how many hours the system should retain locally stored data. If you select this option, use the Retention Hours field to define the number of hours. **Caution**: Enable this feature **only** if you have additional applications or algorithms that **require** access to previously stored FBxEdge data. Carefully consider the number of hours specified to prevent FBxEdge from using all available storage to keep hours. **Note**: This is an **optional** field.
Buttons	
Cancel	Click to cancel all changes and return to the DeviceHub screen.
Add Device	Click to add the device.

5. Click **Add Device**.

Once the device has been successfully created, the system adds a new device tile to the DeviceHub page:

Figure 3-24. New Device on DeviceHub Page
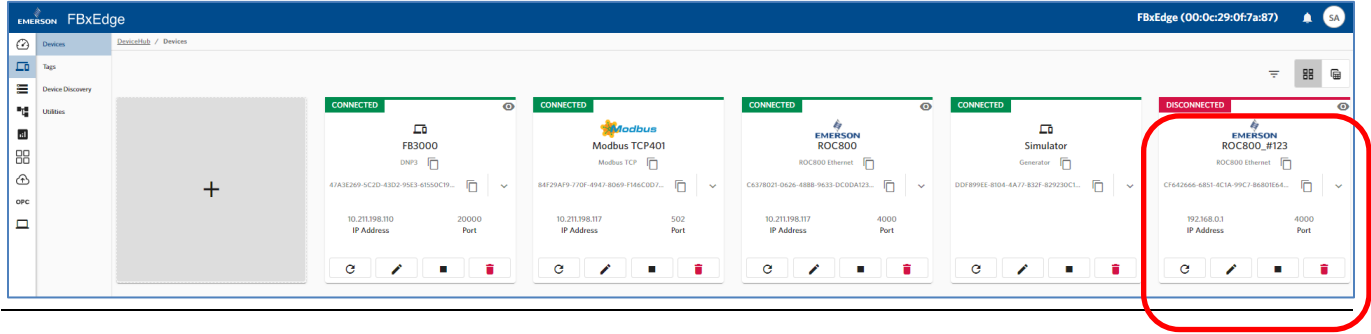
Notes

▪ If you have selected **Enable Data Store** to use local storage, a data store icon ( ) appears in the top right corner of the device tile.

▪ If your device can browse tags, a browse icon ( ) appears in the top right corner of the device tile (see above).

3.4   Adding Tags

Once you connect a device to FBxEdge, you can add tags to that device. Every device has memory registers that store sensor and system values. These registers can be analog or

digital, input or output, and each register is dedicated to a specific data topic. Tags identify a device's particular memory registers from which DeviceHub can collect data. You can add tags individually or as a group.

A tag generates a raw topic, which is the topic for publishing and subscribing through the local message broker. The raw topic consists of normalized data, which can be sent to multiple data destinations and data consumers. Use the Integration section of FBxEdge to specify those destinations.

Note

When a tag generates a raw topic, the topic name appears in the Raw Topic column of the Tags list in a system-generated format (such as *devicehub.raw.5D7D4E72-DB16-41E5-9E5D-A0AFAE801A04.43B10C12-3A14-4B76-8973-52D5A9694DC6*). The Message Broker can copy and use this system-generated label. However, if you select the **Enable alias topics** option when adding or modifying a device, the system replaces the topic ID with a more readable name (such as *devicehub.alias.ROC2.SoftPoint*) that you define.

3.4.1   Adding a Tag

To add a single tag to a device:

1.   Select the **Tags** option; the system displays a list of all defined tags.

Figure 3-25. Tags Listing
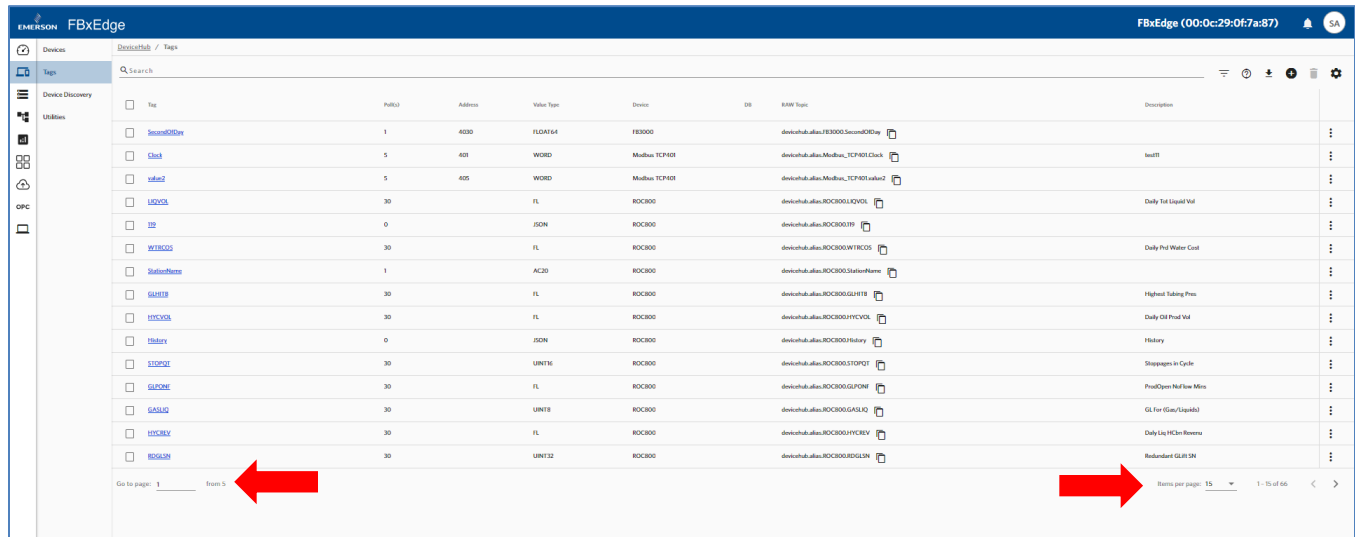
Note

By default, this page shows only the first 15 items. Use the **Items per page** selector (in the bottom right of the page) to expand that display to 20, 50, or 100 tags. Use the **Go to page** select (in the bottom left of the page) to move quickly from one display page to another.

2. Review the available tags and select one by clicking the checkbox to the extreme left of the tag listing:

Figure 3-26. Tag Selection

☐	SecondOfDay	1	4030	FLOAT64	FB3000	devicehub.alias.FB3000.SecondOfDay	⧉
☑	Clock	5	401	WORD	Modbus TCP401	devicehub.alias.Modbus_TCP401.Clock	⧉

3. From the toolbar at the right top of the screen, click the **Add Tag** icon and select the **Add a Tag** option:

Figure 3-27. Add Tag Icon
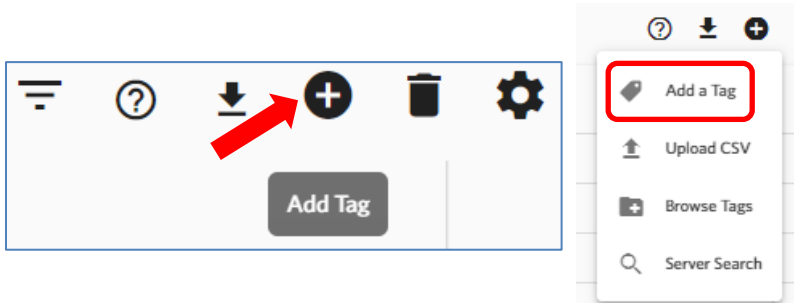
4. Select a device for that tag (click ▼ at the end of the field to display all defined devices):

⚠️ **Important**
The system displays the Add Tag screen if you currently have no devices defined. If you have added at least one device and click **Add** a **Tag**, the system populates the Add Tag screen with the first device on your device list. You can select a different device.

Figure 3-28. Add Tag Screen
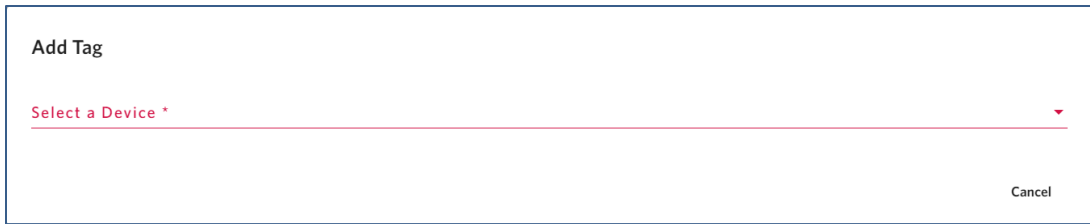
FBxEdge displays the Add Tag page:

Figure 3-29. Add Tag Page

> **Note**
>
> For a ROC device you could select between setting up the tag to read a specific opcode (**OP**), a specific point type (**PT**), or Alarms, Events, or History. The example uses a **OP**.

5. Complete at very least the mandatory fields (noted with an asterisk, *). This activates the **Add Tag** button at the bottom of the page:

Figure 3-30. Add Tag Page (2)

> **Note**
>
> For most devices, polling intervals are expressed in seconds. FBxEdge allows you to enter a fraction of a second (such as **0.5** to represent a half-second), provided the RTU can accommodate that interval. Additionally, you can enter **0** as a polling interval, in which case FBxEdge never **routinely** polls that tag, although FBxEdge does enable you to manually trigger a poll and even write a value back to the tag (provided the tag is writeable).

6. Click **Add Tag**; FBxEdge adds your tag to the tag listing, showing its association with the selected device:

Figure 3-31. Tag Listing
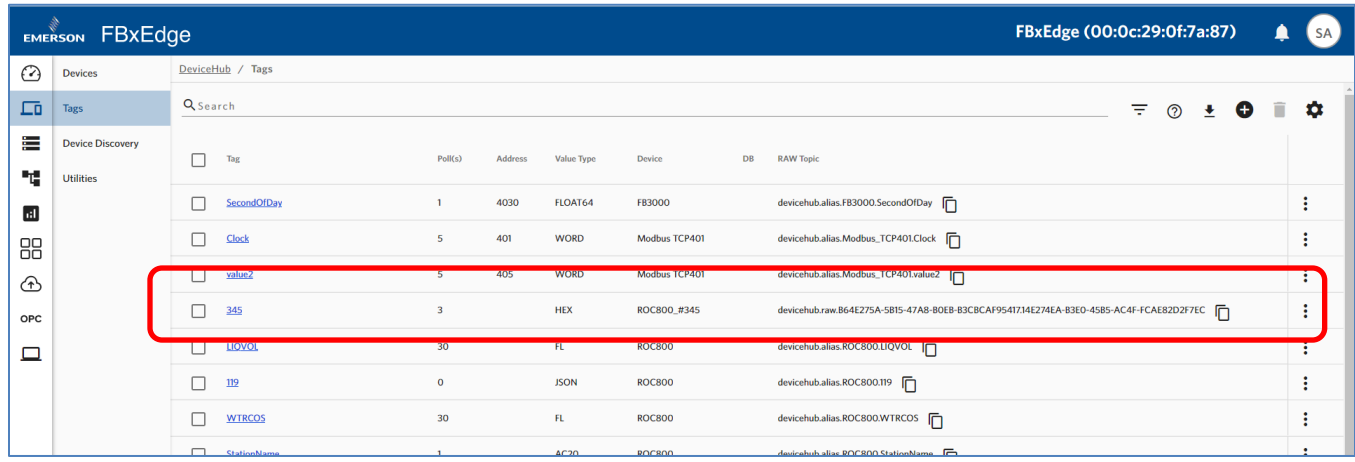
3.4.2 Adding a Group of Tags

Adding individual tags to a device is useful when you have a small number of tags. However, you may have a set of multiple tags you would like to apply to a group of devices. FBxEdge enables you to package that set of tags into a *comma-separated variable* (.CSV) file, which it outputs as a Microsoft® Excel® worksheet. You can then upload this file to any defined device.

3.4.2.1 Creating the CSV File

To create the .CSV file:

1. From the **Tags** page, select the appropriate tags.

2. Click the **Download** icon from the tool bar located in the upper right of the Tags page. A drop-down menu displays, enabling you to either download all tags for all devices or download the selected tags for the selected device.

3. When you select an option, FBxEdge creates the download file using the current year-month-day (such as *tag-2023-06-08.csv*) as a filename, places the file in your PC's Downloads folder, and displays a notification pop-up.

3.4.2.2 Uploading the CSV File

To upload the .CSV file:

1. From the **Tags** page, click the **Add Tag** icon from the tool bar and select the **Upload CSV** menu option.

Figure 3-32. Upload CSV Option
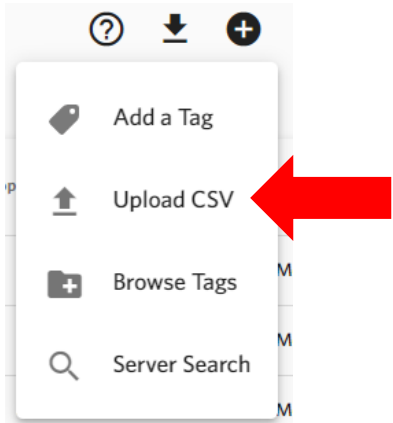
The Upload Tag screen displays:

Figure 3-33. Upload Tags Screen
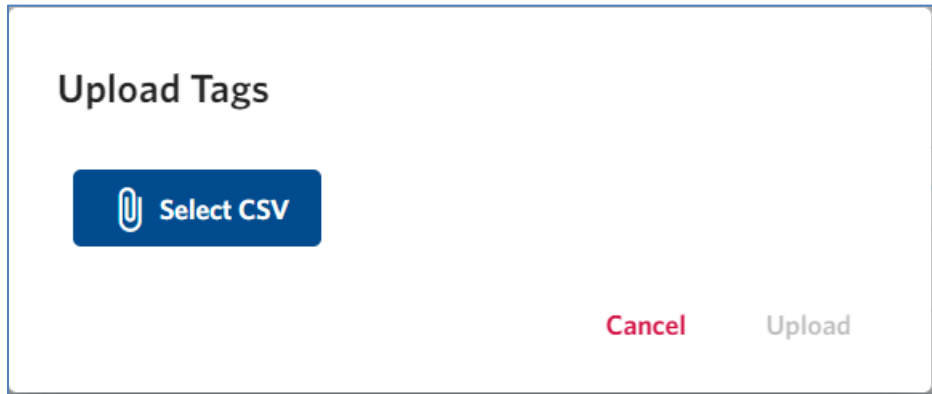
2. Click **Select CSV**. A file explorer window opens, showing the folders on your PC.

3. Navigate to the Downloads folder and select a .CSV file. The Upload Tag screen changes to include your chosen file and an activated **Upload** button:

Figure 3-34. Upload Tags Screen
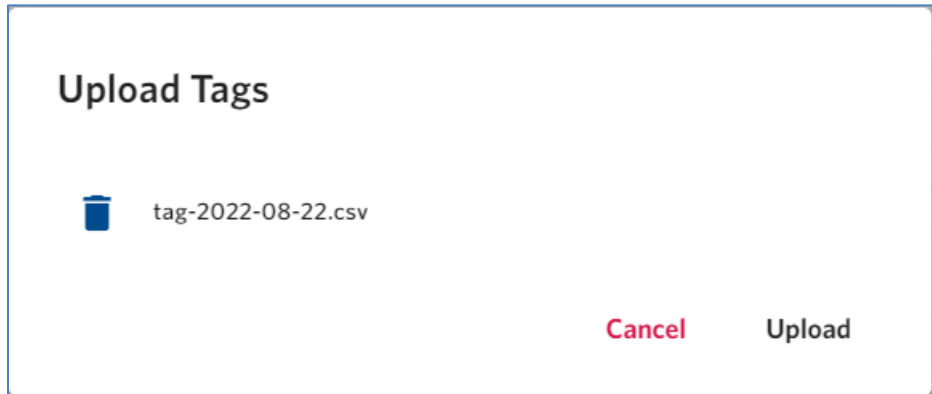
4. Click **Upload.** The system generates an error message (*Could not find Device XXX*) if the tag **does not** upload to the device. If no error message appears, you can browse the tag list to verify that the file uploaded.

3.4.2.3   Browse the Available Tags

FBxEdge provides an alternate way to select the tags for the CSV.

1. From the menu that displays when you select the **Add Tag** icon, select **Browse Tags**.

Figure 3-35. Browse Tags Selection
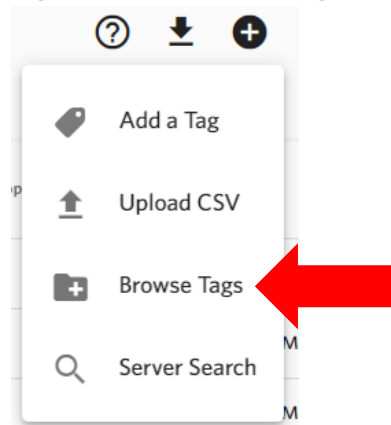
2. FBxEdge displays a device selection screen.

Figure 3-36. Device Selection
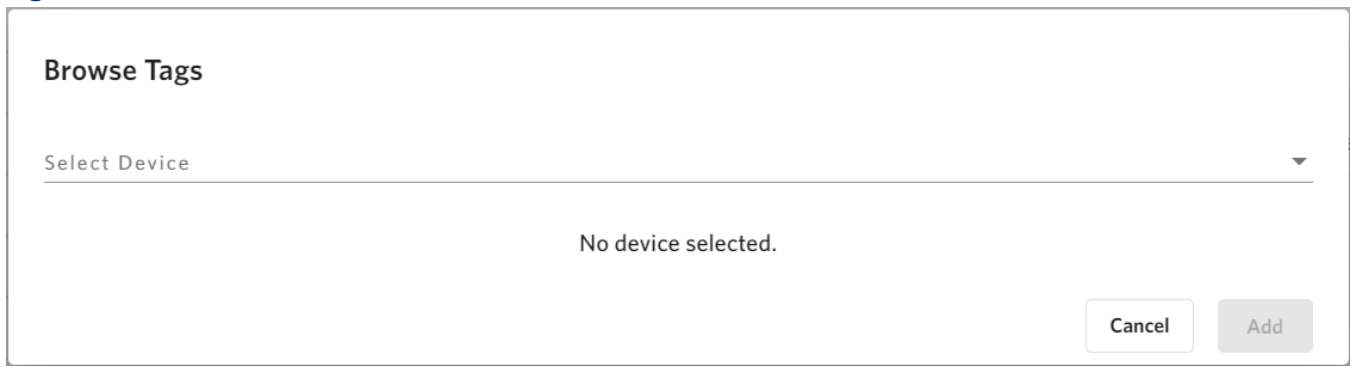
3. Click ▼ to display a list of all defined devices. When you select a device, FBxEdge displays a screen showing the tags (opcodes and point types) associated with that device:

Figure 3-37. Selected Device
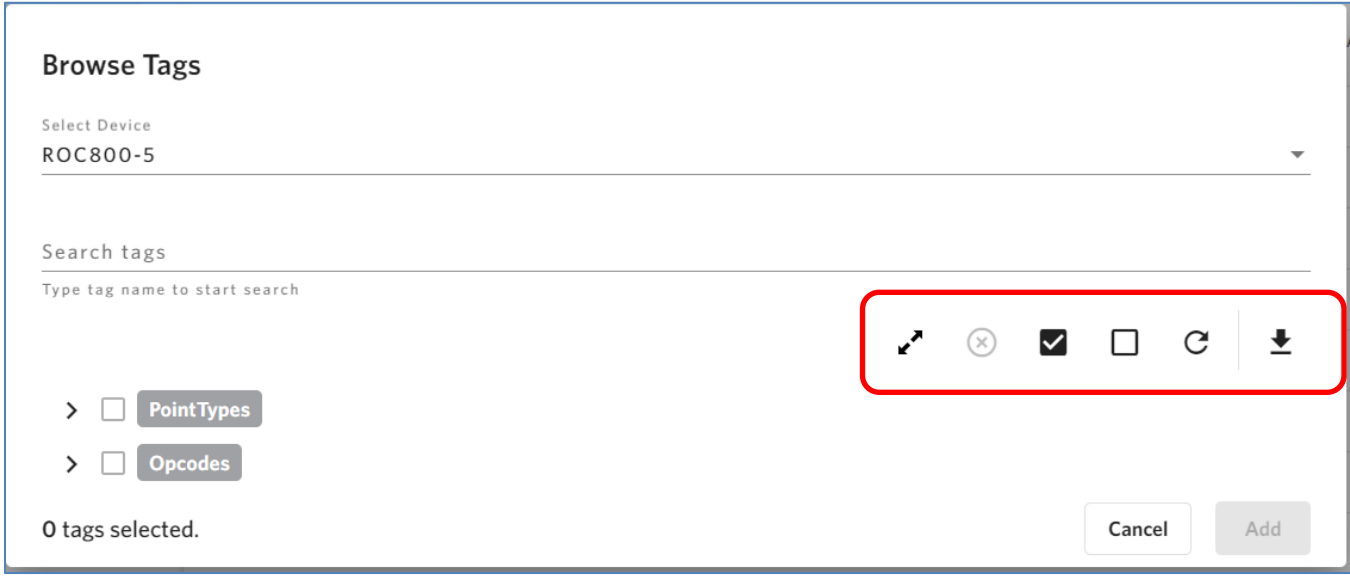
You can use the screen's search field or click > to the left of the PointTypes and Opcodes labels to expand those tag listings. The tool bar on the right side of the screen enables you to expand the display to show all tag, select all tags, clear any selections, or refresh the screen, or download tags as a .CSV file. Once you have selected tags, you can download the selection to a .CSV file.

3.5 Defining the Status Register

To define an optional register for keeping track of the device's status (connected or disconnected):

1. Select the **Status Register** option; the system expands the Status Register section of the screen:

Figure 3-38. Status Register

2. Complete the following fields:

Field	Description
Name	Indicates the name of the register. Click ▼ to display all defined names (PT, OP, History, Events, Alarms) and select a name from that list.
ValueType	Indicates the register's data type. Click ▼ to display all defined data types (**HEX** or **JSON**) and select a data type from that list.
Polling Interval	Indicates how often the system polls the driver; enter **0** to disable auto-polling.
Description	Provides a description of the status register.
Opcode	Identifies the opcode associated with this status register. . Click ▼ to display all defined opcodes.

3. Click **Add**.

Note

ROC Plus and DNP3 protocols do not require you to define a status register to determine a device's status: FBxEdge reports that automatically. A status register is more suited to devices using the Modbus protocol. However, FBxEdge does allow you to configure a specific tag as a status register if the need exists.

3.6   Setting Up Flows Manager

The Flows Manager module allows you to connect to your devices and configure the output so you can better visualize how the device is operating. Additionally, flows enable you to visually develop custom data processing algorithms, to prototype applications, and to generate calculated values that can be converted to setpoints for the RTUs or sent to the SCADA or the cloud.

The connection to your device can be both incoming and outgoing, allowing you to affect the device. For example, you can start and stop a device from a flow write to a topic, or trigger events.

Note

The Flows Manager option is based on Node-RED, a visual programming tool (*https://nodered.org*) that visually presents relations and functions and enables you to program and create JavaScript functions without having to write code. FBxEdge enables you to run up to four independent instances of Node-RED to maximize resource utilization on the edge device when relying on algorithms built with flows.

With FBxEdge Manager, you can deploy Node-RED flows in bulk to multiple edge devices, synchronizing data processing logic and customer applications. (For further information, see the *Emerson FBxEdge Manager User Guide*, D301916X012.)

Flows and subflows consist of separate canvases located in tabs of the Flow view, which you use to perform operations that are useful when processing collected data.

Flows allow you to:

1. Collect data from devices in DeviceHub, databases, enterprises systems, and files of various types
2. Process, filter, and analyze data while implementing JavaScript logic, adding functions, and including rules and alerts for event processing
3. Create flow templates and deploy them to multiple edge devices.
4. Start, stop, and delete up to four flows
5. Update the memory limit, upload custom node modules, download a *flow.json* file, and download the logs for a flow
6. Add new flows up to the maximum allowed memory
7. Include flows in backup/restore and template
8. Set up a dashboard to organize and better visualize your flows

3.6.1   Subscribing to the Datahub

Select the **Flows Manager** icon from the FBxEdge toolbar on the left side of the screen.

1. Select the **Go to Flows Definition** icon (immediately to the right of the green **Running** notification at the right-hand side of the page):

Figure 3-39. Flow icon
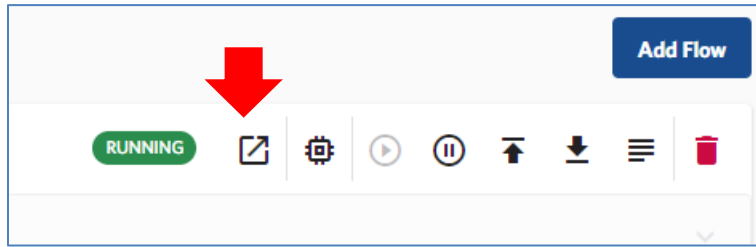
The system opens a new Flow workspace.

Note

Selecting the Flow module **adds** a topic tab for that flow at the top of the screen (here, labeled **Flows : 10.211.198.25**):
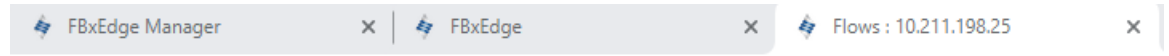
2. Select the dark green **Datahub Subscribe** icon on the left side of the screen and drag it onto the workspace:

Figure 3-40. Datahub Subscribe option
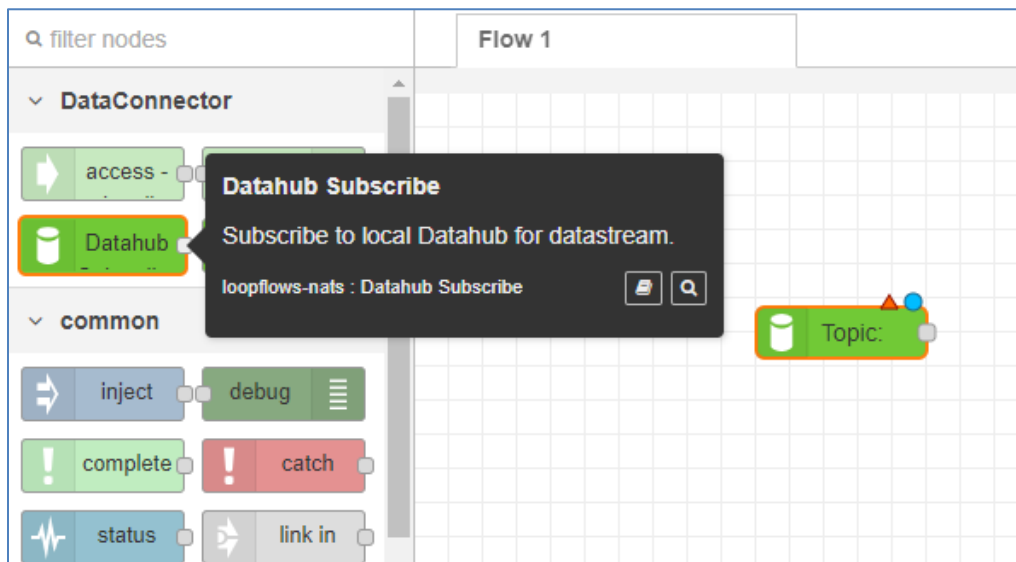
3. Double-click the **Datahub Subscribe** node; the Edit Datahub Subscribe node dialog displays at the right side of the screen. Complete the **Topic** field on the Edit Datahub Subscribe node dialog:

Figure 3-41. Datahub Subscribe node dialog
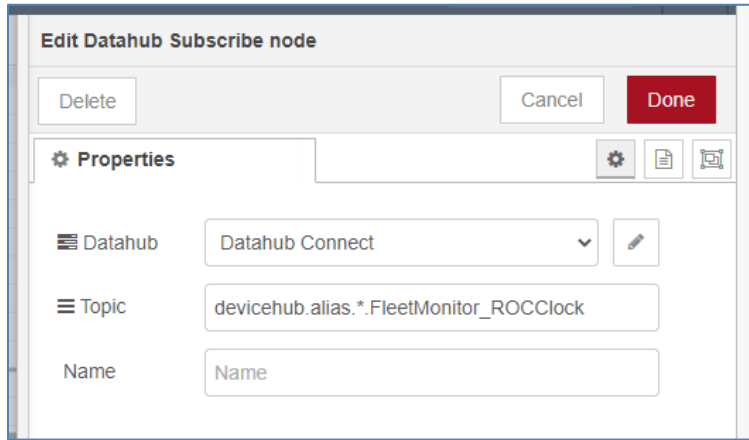
This subscribes the node to a topic. Usually, this topic corresponds to a tag you have already configured. To select a pre-configured topic:

1. Click the **FBxEdge** tab at the top of the screen and select the **DeviceHub** icon (which displays all devices).

2. Select a device and then select **Tags**.

Figure 3-42. Selecting a Topic
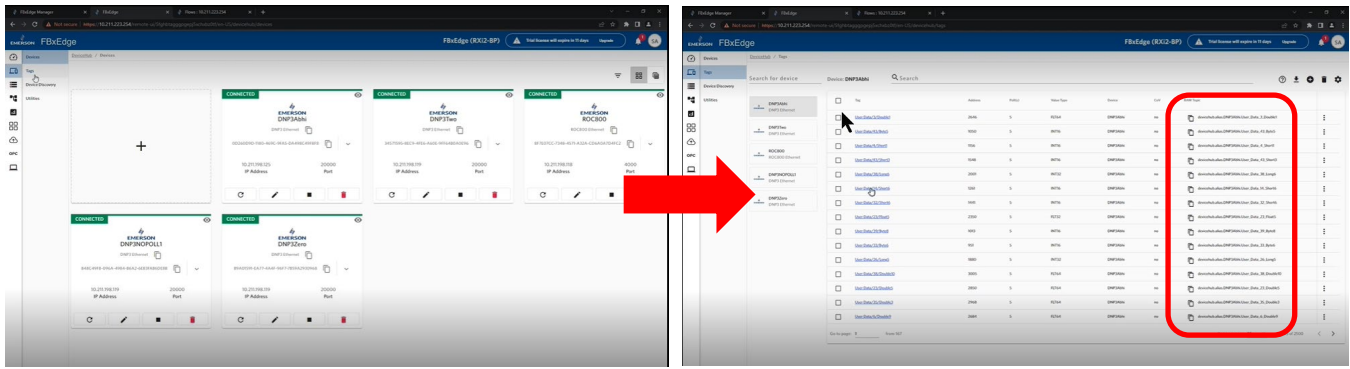
3. When the Tags screen displays, click on the copy icon (to the left of the tag lists) to copy a specific tag to the clipboard. (The system displays a *Copied to clipboard successfully* message at the bottom of the screen.)

4. Select the flow-specific tab (at the top of the screen) and complete the Topic field on the Edit Datahub Subscribe node dialog by pasting in (**CTRL+V**) the tag.

Figure 3-43. Datahub Subscribe node dialog
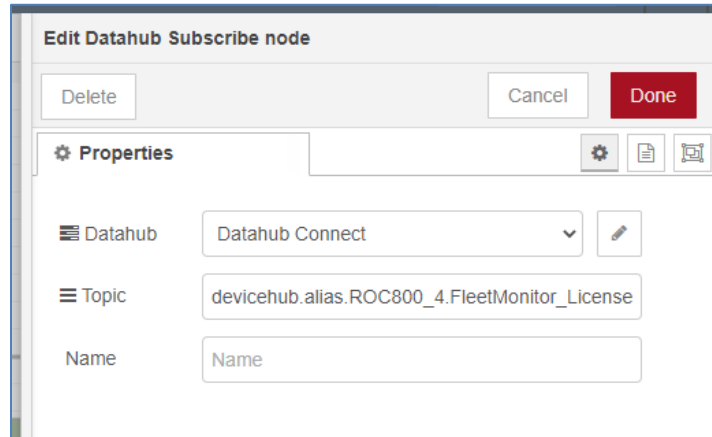
5. Click **Done**; the dialog closes and the system displays the flow with the label for the selected topic (note the *connected* label under the topic):

Figure 3-44. Datahub Subscribe node dialog
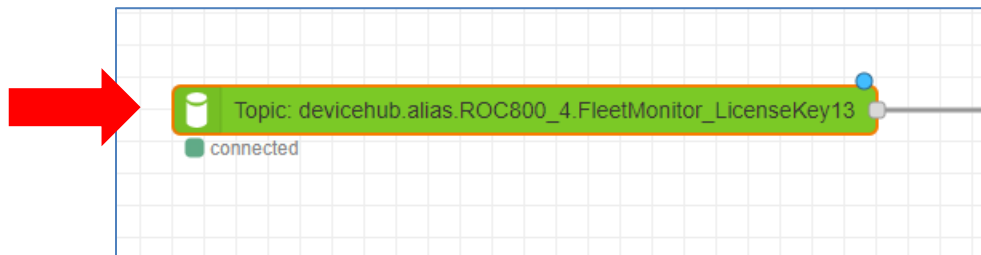
3.6.2 Configuring a Flow

Once you have successfully subscribed to the Datahub, you can configure a flow:

1. From the Nodes menu on the left-hand side of the screen, select and drag a **debug** node (in the common group) and a **json** conversion node (from the parser group) onto the Flow 1 workspace:

Figure 3-45. Flows Workspace (2)
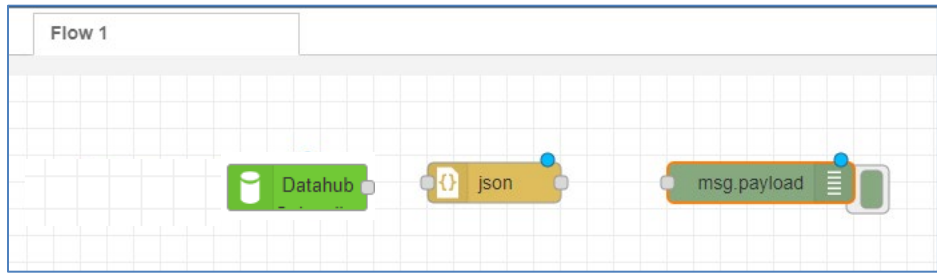
2. Wire the nodes together, enable the debug console, and click **Deploy** (at the top right of the workspace) to engage the flow.

The system retrieves data based on the polling interval set for the tag and you can see the data retrieval in the Debug console.

Note

After **any** edit process, you **must** click **Deploy** so the system can apply any changes.

Figure 3-46. Flows Workspace
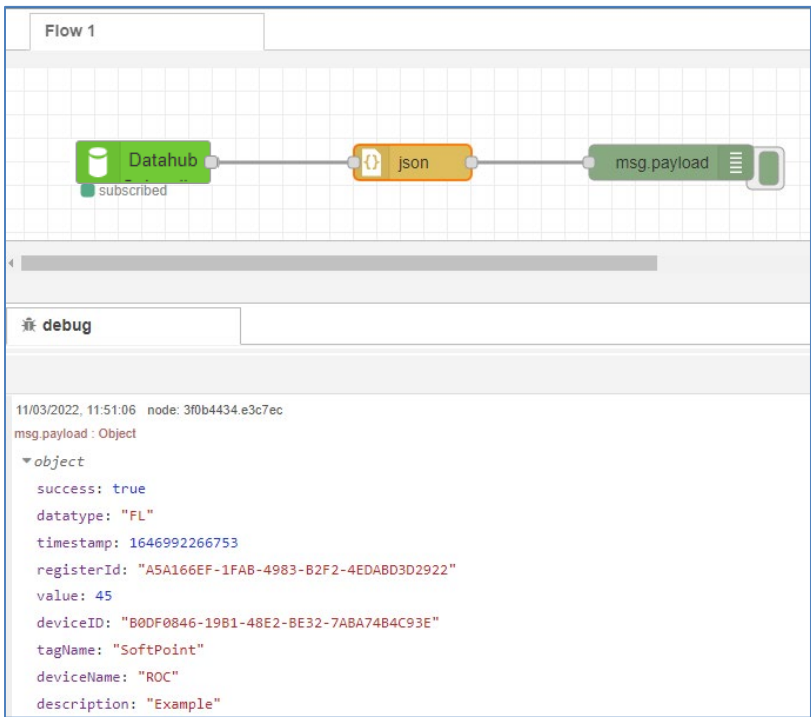
3.7 Adding an MQTT Connector

MQTT connectors enable you to export data that FBxEdge extracts. You can define individual exports or group exports.

3.7.1 Adding an MQTT Connector

To add an MQTT connector:

1. Select the **Integration** icon from the FBxEdge toolbar and click the **+** to display the Add a connector dialog.

Figure 3-47. Add a connector dialog

2. Click ▼ in the Provider field and select one of the options in the drop-down menu. For this explanation, we chose **MQTT – Generic**:

Figure 3-48. Selecting a Connector

The Add a connector page displays.

Figure 3-49. Add a Connector Page

3. Scroll down and complete all the fields on this screen:

Field	Description
Name	Indicates the name for this connector
Hostname	Indicates the DNS name for the MQTT host
Port	Indicates the port of the MQTT host. **Note**: This is an **optional** field.
Client ID	Indicates the unique ID for a client (required by the MQTT protocol) connecting to an MQTT broker. **Note**: The client ID **must** be unique to each edge device; no two edge devices can use the same client ID.
Username	Indicates the username for this connector
Password	Indicates the password for this connector
QoS	Indicates the QoS attribute **Note**: This is an **optional** field.

Field	Description
Parallel Publish Count	Indicates the number of messages that can be published simultaneously
Integration Topic	Indicates the integration topic for this connector.
LWT Topic	Indicates this connector's LWT (Last Will and Testament) topic **Note**: This is an optional field.
LWT payload	Indicates this connector's LWT payload
LWT payload type	Indicates this connector's LWT payload type
LWT QoS	Indicates this connector's LWT QoS
LWT retained	Select to flag the LWT message to be retained.
Throttling limit	Indicates this connector's throttling limit
Persistent Storage	Select to indicate this connector has persistent storage. By default, this option is selected.
Queue Mode	Indicates the storage mode, Last In First Out (**lifo)** or First In First Out (**fifo**).
Buttons	
Cancel	Click to cancel the connector definition.
Add	Click to add the defined connector.

4. Click **Add** to create the connector. By default, the new connector is disabled:

Figure 3-50. Connector Added
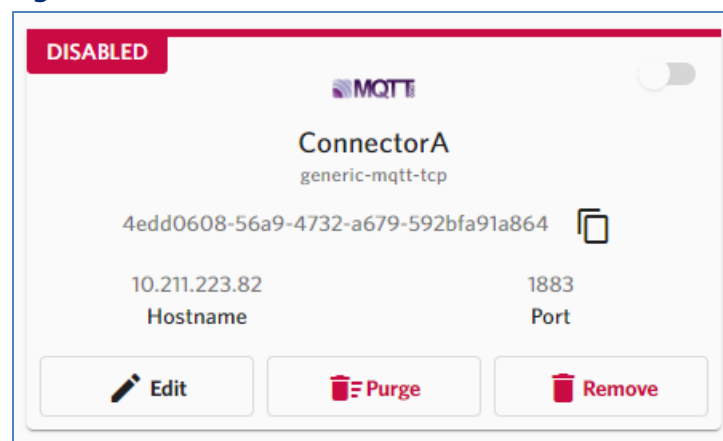
5. Click the new connector tile to display the connector's Dashboard page:

Figure 3-51. Connector Dashboard Page
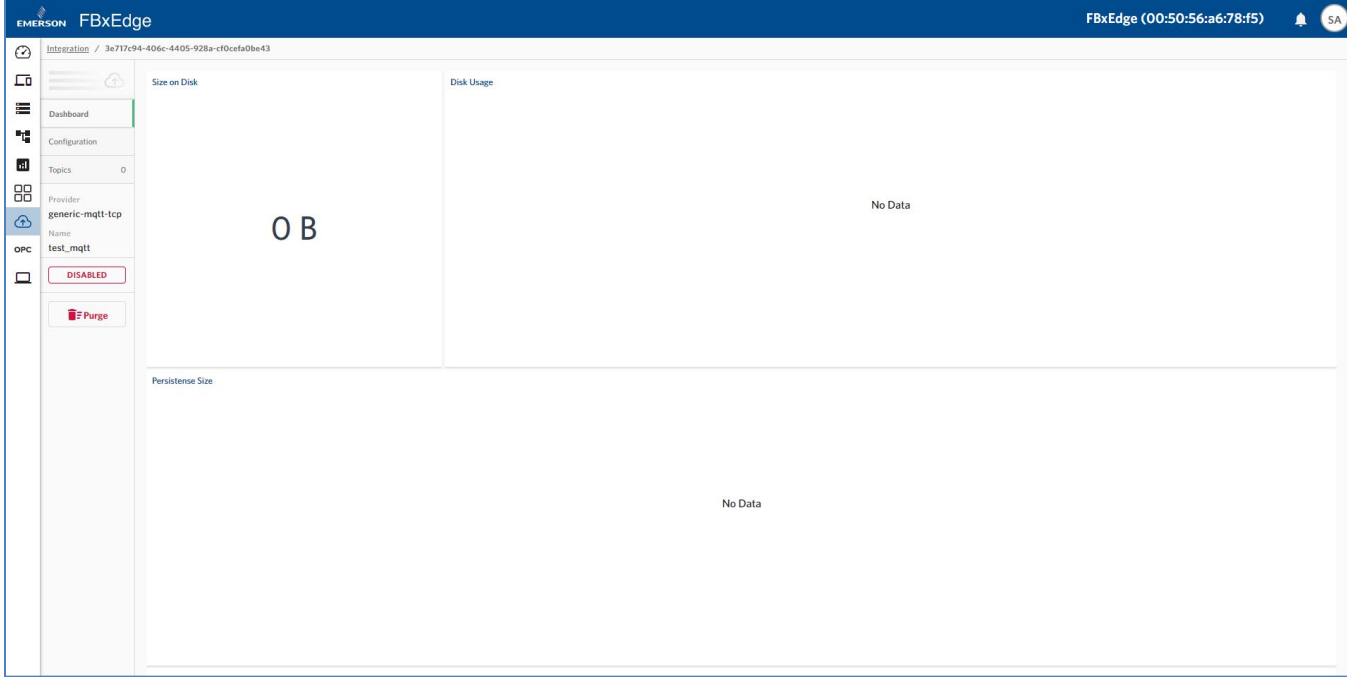
> **Note**
>
> By default, a newly created and disabled connector has **no** default topics.

6.   Click the **Topics** option on the Dashboard menu.

Figure 3-52. Topic Icon on Dashboard
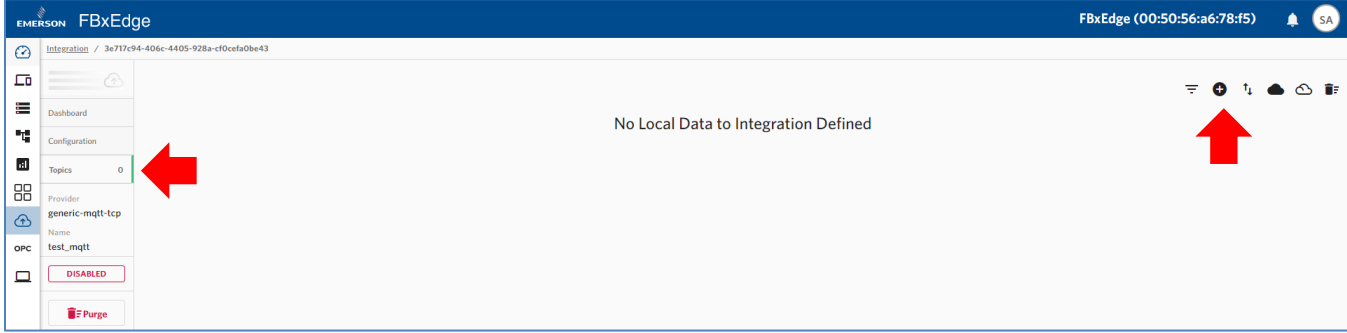
7.   Click the Add Topic button ⊕. The Data Integration screen displays:

Figure 3-53. Data Integration Page

8. Complete the following fields:

Field	Description
Data Direction	Indicates the data direction, either **Local to Remote – Outbound** or **Remote to Local - Inbound**.
Local Data Topic	Indicates a raw topic tag.
Remote Data Topic	Indicates the destination's MQTT address. **Note**: This is an **optional** field. If you choose not a specify a remote data topic, the system uses the connector's Integration Topic address.
Description	Describes the connection. **Note**: This is an **optional** field.
Qos	Indicates the quality of service value.
Buttons	
Enable	Select to enable or disable the topic.
Cancel	Click to cancel the integration definition.
Add	Click to add the integration definition.

9. Enable the topic and click **OK**. The system displays the Dashboard, which now includes the newly defined topic.

Figure 3-54. Modified Dashboard

☐	Local Topic	Remote Topic	Description	Data Direction	Status	Actions
☐	devicehub.raw.B0DF0846-19B1-48E2-BE32-7ABA74B4C93E.A5A166EF-1FAB-4983-B2F2-4EDA...	scada\raw		Outbound	Enabled	⋮

> **Note**
>
> To configure an **inbound** topic, select **Remote to Local – Inbound** as the Data Direction on the Data Integration page and complete all other fields as necessary.

3.7.2 Adding an MQTT Connector (for SparkplugB Messages)

⚠️ **Important**

The MQTT connector used here is *MQTT Standard over SSL*, **not** *MQTT-Generic*.

To add an MQTT connector to handle SparkplugB messages, define a connector with the following:

1. Select the Integration icon from the FBxEdge toolbar and click **+**. The **Add a connector** dialog displays:

Figure 3-55. Add a connector dialog

Add a connector

Provider *

Provider is required

Cancel   **Add**

2. Click ▼ at the extreme right of the Provider field and select one of the options in the drop-down menu that displays (here, **MQTT Standard over SSL**):

Figure 3-56. Provider drop-down menu

Add a connector

Standard   ✕

⬛MQTT   MQTT Standard

⬛MQTT   MQTT Standard over SSL

3. The Add a connector screen displays:

Figure 3-57. Add a connector screen

4.   Complete the fields on this screen (asterisks indicate mandatory fields)

Field	Description
Name	Indicates the name for this connector.
Group ID	Represents a logical grouping of edge nods. This can be a region, a facility name, or any meaningful grouping of edge nodes within your application.
Node ID	Indicates the ID of the logical edge node.
Application ID	Specifies the ID of the main application to receive the MQTT data, ensuring that data doesn't get lost and is delivered to the desired application.
Hostname	Indicates the DNS name for the MQTT host.
Port	Indicates the port of the MQTT host. The default value is **8883**.
CA Certificate	Indicates where to add the contents from the certificate file. **Note**: This field is mandatory.
Certificate	Indicates the certificate.

Field	Description
Client ID	Indicates the unique ID for a client (required by the MQTT protocol) connecting to an MQTT broker. **Note**: The client ID must be unique to each edge device; no two edge devices can use the same client ID.
Username	Indicates the username for this connector on SSL.
Password	Indicates the password for this connector on SSL.
Buttons	
Cancel	Click to cancel the connector definition.
Add	Click to add the defined definition.

5. Click **Add** to create the connector. The Dashboard displays, showing the new connector (which is disabled by default). ==THIS SEEMS TO BE A GENERIC MQTT==

Figure 3-58. Added MQTT Connector
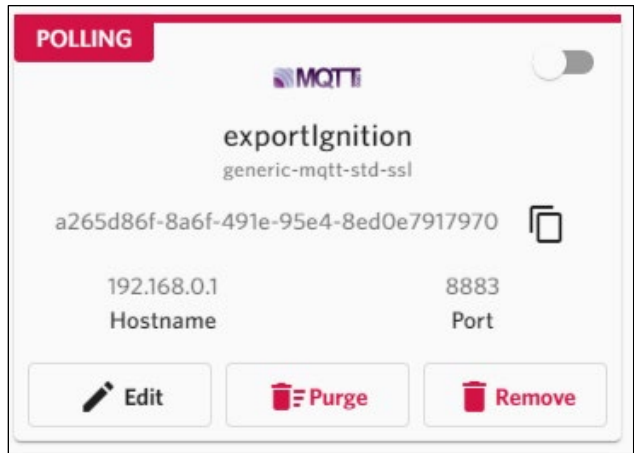
The SparkplugB application then handles the newly added connector.

3.8 Mapping Tags to an MQTT Connector

FBxEdge enables you to map tags associated with one or more edge devices. This option **does not** define the Remote topic for these tags, so you need to use the MQTT Connector's **Integration** topic for each export. Similarly, you can update remote topics for these tags, but you must perform that action for **each** tag.

↑↓   1. Select the **Topics** menu item and click the **Import from DeviceHub tags** option (in the upper right of the page). The DeviceHub Import page displays:

Figure 3-59. DeviceHub Import Page

2. In the **Raw/Alias** column, select the device(s) to provide tags to import (here, **ROC800**).

3. Click **Yes** to proceed with the import.

3.8.1   Using Wildcards

Another option for exporting topics in bulk to MQTT is to use wildcards in the local topic. NATS topics accept two types of wildcards:

- ***** (asterisk)

  Matches a **single** topic (token) in the topic format. For example, if an application wanted to listen for eastern time zones, it could subscribe to *time.*.east*, which would match *time.us.east* and *time.eu.east* (*us* and *eu* replacing the asterisk)

- **>** (greater than)

  Matches **one or more** tokens and can occur only at the **end** of the subject. In this case, *time.us.>* matches *time.us.east* and *time.us.east.atlanta*.

In this example, *time.us.** could match only *time.us.east*, since it is limited to matching a single token. .

Note

For an **outbound** topic, the remote topic **cannot** have wildcards but the local topic **can** have wildcards. Conversely, for an **inbound** topic, the local topic **cannot** have wildcards but the **remote** topic **can** have wildcards.

Once you are done setting up the topics, make sure the topic you would like to use are enabled, and enable the MQTT connector. Its new connected state is CONNECTED and green:

Figure 3-60. Connected Connection
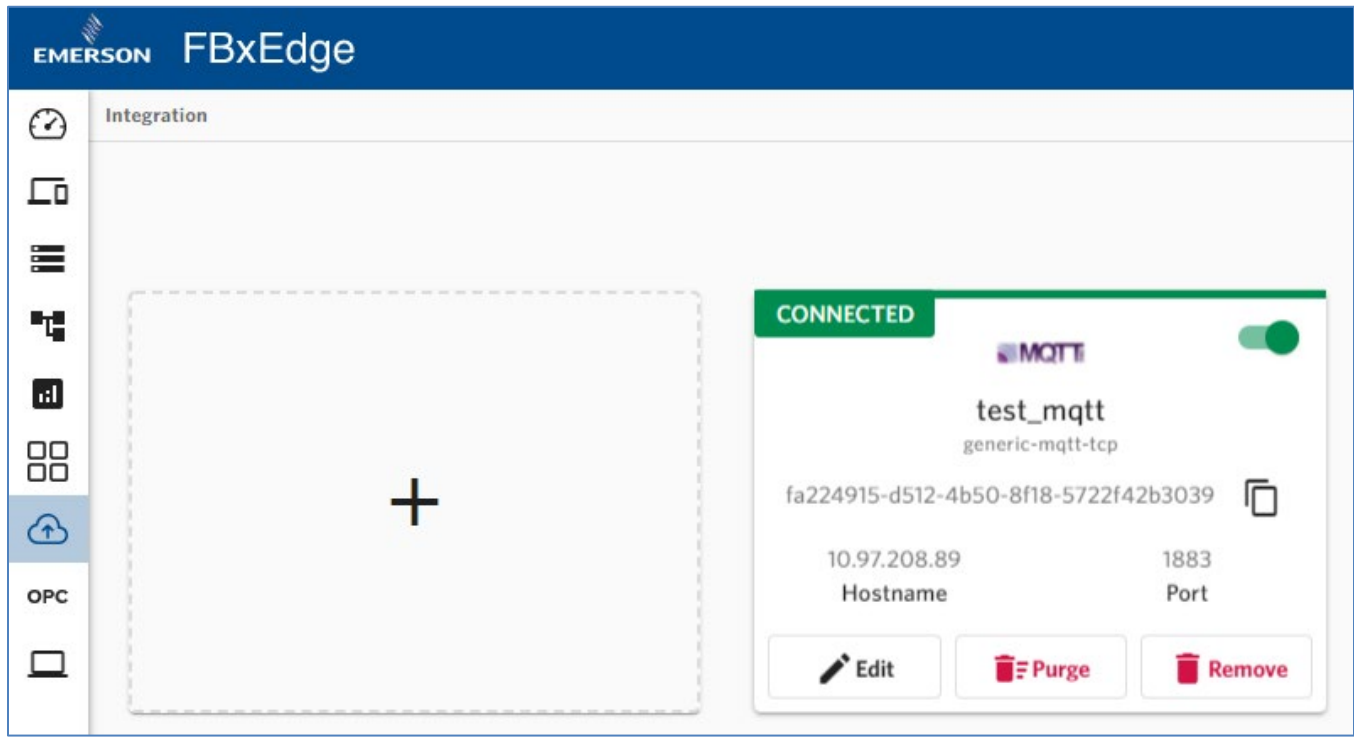
To apply further edits to a topic, you do not need to disable the MQTT connection before editing. There may be circumstances when the connector automatically disconnects (as when you change the LWT), but the system immediately reconnects.

Chapter 4. System Reference

 Click the **System** icon to display the System Module and its component functions:

Figure 4-1. System Module Components
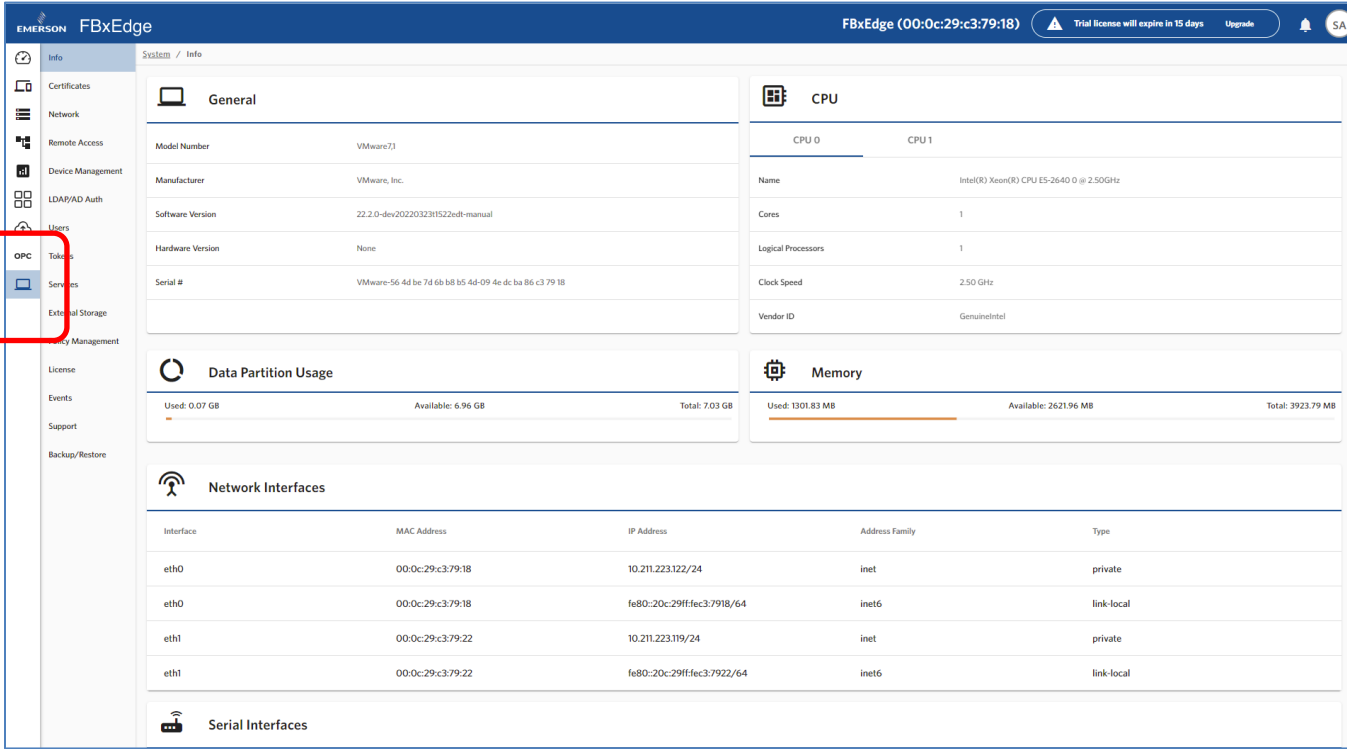
Use the System module to view and modify configurations throughout FBxEdge. From the Navigation panel, click **System** to access the list of system features:

Table 4-1. System Features

Feature	Capabilities
Info *(see Section 4.1)*	▪ General ▪ CPU ▪ Data Partition Usage ▪ Memory ▪ Network Interfaces ▪ Modem Interfaces (if present) ▪ Serial Interfaces (if present) ▪ CAN Interfaces (if present)
Certificates *(see Section 4.2)*	▪ Add a device certificate ▪ Add a custom certificate ▪ Copy device public key

Feature	Capabilities
Network *(see Section 4.3)*	- Modify Host information - View/modify edge device (for static Ethernet settings) - Modify DNS/NTP - Configure Ethernet settings
Wi-Fi *(Section 4.4)*	Not supported in the initial product release.
Remote Access *(see Section 4.5)*	Add more remote access
Device Management *(see Section 4.6)*	- Add/modify activation for cloud - View management status - Manage FBxEdge device - View object instances
LDAP/AD Authentication *(see Section 4.7)*	Add authentication provider
Users *(see Section 4.8)*	Manage users
Tokens *(see Section 4.9)*	- Create/edit/remove/validate REST API keys - Manage access account
Services *(see Section 4.10)*	- Start/stop/disable/enable FTP services - Add/remove FTP users - Enable/disable a user - Reset FTP user password - Start/stop Remote Access and SSH services
External Storage *(see Section 4.11)*	Add external storage
Policy Management *(see Section 4.12)*	- Modify password policy - Modify disk space policy
License *(see Section 4.13)*	- Add/upgrade a license - View current version - Disable/enable modules - View number of devices and tags allowed in a plan
Events *(see Section 4.14)*	View log of live and historical events that have occurred for specified components
Support *(see Section 4.15)*	- View component status - Generate/download a support bundle - Download a file and view file information
Backup/Restore *(see Section 4.16)*	- Backup/restore Edge device configuration - Save current backup and restore configuration for cloud - Upload/download backup templates

4.1   Info

The **Info** pane allows you to view information about your system. It appears by default when you select the **System** icon from the **Navigation** pane.

Select **General** to view:

Label	Information
Model Number	The FBxEdge model number
Manufacturer	The FBxEdge manufacturer
Software Version	The current firmware version for FBxEdge
Hardware Version	The hardware version for FBxEdge
Serial Number	The FBxEdge serial number

Select **CPU** to view:

Label	Information
Name	The name of the installed CPU
Cores	The number of cores in the installed CPU
Logical Processor	The number of logical processors in the installed CPU
Clock Speed	The maximum clock speed for the installed CPU
Vendor ID	The manufacturer of the installed CPU

Select **Data Partition Usage** to view:

Label	Information
Used	The amount of space (in GB) used on the hard drive partition
Available	The amount of space (in GB) available on the hard drive partition
Total	The total amount of space (in GB) available on the hard drive partition

Select **Memory** to view:

Label	Information
Used	The amount of memory (in GB) used for the device
Available	The amount of memory (in GB) available for the device
Total	The total amount of memory (in GB) available for the device

Select **Network Interfaces** to view:

Label	Information
Interface	The type of network interface: • Ethernet (eth0 or eth1) • Wi-Fi (wlan0) • LTE (wwan0)
MAC Address	The physical address of the network interface
IP Address	The logical address the software assigns to the network interface
Address Family	The type of traffic running through the interface, either **inet** (IPv4) or **inet6** (IPv6)
Type	The type of address space for the network: • Private; the network interface can interact with any other network because the IP has global scope • Link-local; the IP address is valid only on local network segments **Note**: IPv6 requires a link-local address on every network interface.

Select **Modem Interfaces** to view:

Label	Information
Status	The network area of the LTE modem. Home, for example, indicates that all devices are in close proximity to the modem
Bars	The signal strength of the LTE modem, ranging from 0 (no signal) to 5 (a very strong signal)
Network	The mobile network from which the modem communicates
IPv4	The modem's IPv4 address
IPv6	The modem's IPv6 address
IMEI	International Mobile Equipment Identity: a unique number that identifies mobile network devices
ICCID	Integrated Circuit Card Identifier: the SIM card's serial number
APN	Access Point Name: serves as a gateway for mobile network to connect to another network or the public Internet

Note

Direct modem connectivity is **not** supported in the initial release of the product.

Select **Serial Interfaces** to view:

Label	Information
Name	The device's name
Alias	The name defined as an alias for the device
Model	The device's model
Path	The path used to connect to the device

Select **CAN Interfaces** to view:

Label	Information
Interface	The device name
Set "open"	An option that configures the selected device
Set "closed"	An option that configures the selected device
Set "status reset"	An option that configures the selected device
CAN Speed, Kbit/s	The high-speed baud rates from 40 Kbit/s to 1 Mbit/s, depending on cable length
UART Speed, baud	The maximum rate at which information is transferred

4.2 Certificates

The **Certificates** pane stores certificates locally in FBxEdge: .

- The **Device Certificate** tab allows you to add and refresh SSL certificates.

- The **Custom CA Certificates** tab allows you to add a default self-signed certificate, making all communications secure by default. A certificate is required only if you want to give the device a DNS name and remove the browser's security warning.

- The **Identity** tab allows you to view and copy the Device Public Key and install, download or copy the Certificate Signing Request.

- The public key is used to authenticate data coming from FBxEdge. This requires a private key for the device and a server with all the device's public keys.

- The **Identity Certificates s**ection in the Identity tab allows you to Install an identity certificate locally, and view, copy, and download a certificate signing request.

The Certificate Signing Request is a block of encoded text that you can give to a Certificate Authority when applying for an SSL certificate. It also contains the public key that is included in the certificate. A private key is usually created while you create the Certificate Signing Request, making a key pair.

4.3　　　Network

Use the Network pane to view and configure network settings:

- **Overview**: Includes the Host Information, Edge Devices, Interfaces List, Modem Interfaces, and Docker Interface sections where you can view information.

- **Configure**: Includes the Host Information, Timezone, and Docker Interface sections where you can perform changes to the Friendly Name, Country ,and Docker Binding IP address.

> ⚠️ **Important**
> You **must** select the **WAN** option on the top left of the Network's Configure screen to provide remote access to FBxEdge and allow FBxEdge to access resources (like SCADA systems) located outside of the local network. FBxEdge automatically activates the WAN feature **only** if you intentionally connect to the **eth0** interface.

- **Interfaces**: Includes the Interfaces section where you can update the eth0 network and eth1 private network interfaces.

- **DNS/NTP Servers**: Includes the Fallback DNS Resolvers, NTP Servers, and Host file sections where you can add, modify, or delete DNS Resolvers, NTP Servers, and Host File.

- **WWAN**: Includes the Modem Configuration section where you can modify the modem configuration. This functionality is reserved for a future release.

FBxEdge includes two Ethernet interfaces:

- **eth0** is always connected to the Internet. It is located in the DMZ (demilitarized zone), a separate network that has restricted access to a company's internal network.

- **eth1** is connected to a private network with a DHCP server.

FBxEdge has two optional Wireless Network interfaces:

- **wlan0** represents a Wi-Fi network connection.
  Note: If your device supports Wi-Fi, the interface appears on the Wi-Fi pane in the System module where you can establish a connection.

- **wwan0** represents a connection to an LTE mobile network. You must set up an LTE modem for this type of connection.
  Note: If your device supports LTE, after you configure the associated APN, you can view its information in the Info pane in the System module in the Modem Interfaces section.

You can view information about networks with which you currently connect.

⚠️ **Important for Cloud Deployment**
The license Host ID depends on the Media Access Control (MAC) address for the device. The manufacturer-supplied MAC address uniquely identifies each Ethernet port on the device.

4.4 Wi-Fi

⚠️ **Important**
The **Wi-Fi** option in the Navigation panel appears **only** if your edge device supports Wi-Fi. This functionality – as well as serial communications – is **not** supported in the initial product release. The initial product release supports **only** wired Ethernet.

4.5 Remote Access

When using a software-defined private network, the **Remote Access** pane allows you to:

- Access FBxEdge software, no matter where in the world it resides.

- Diagnose FBxEdge issues without requiring on-premise intervention.

Using the network's unique Node ID as a secure token, an end-to-end handshake between devices ensures a direct, secure connection.

You can access a Zero Tier network, a private network, or directly access a device

4.6 Device Management

The **Device Management** pane includes the following sections:

- Cloud Activation: Allows you to connect (activate) or disconnect (deactivate) your edge device using an endpoint IP address. You can view the company name, project name, device ID and status of the device. Set or modify the endpoint with this option.

   Note
   "Cloud activation" is an onboarding activity to the FBxEdge Manager. It can be cloud-hosted, but initially is hosted by customers on their own on-premise servers.

- Manage: Allows you to reboot and factory-reset your edge device, as well as upload the edge device software.

Cloud activation configures an FBxEdge device so that users can have remote access from anywhere in the world.

4.7   LDAP/AD Authorization

Use the **LDAP/AD Auth** pane to enable FBxEdge to leverage a local Active Directory domain for user authentication and authorization. This enables you to manage account credentials centrally through Active Directory without having to create local user accounts on each edge device.

4.8   Users

Use the **Users** pane to add and manage your edge device users. You can define custom roles, custom permissions, and custom user groups and then assign those users to the groups, permission sets, and roles.

4.9   Tokens

⚠️ **Important**
Tokens are required **only** when configuring one edge device to communicate *directly* with another edge device **or** when building a docker container that needs to access the FBxEdge's local API.

Use the **Tokens** pane to create and REST API keys and API access accounts.

An API token is a unique identifier of an application requesting access to a service. It is used when FBxEdge uses REST API endpoints for sending requests and retrieving data from the cloud.

The REST API Keys section allows you to add, modify, validate, and remove a key. You can copy the API token from the Value column for a key.

4.10   Services

Use the **Services** pane to start and stop the File Transfer Protocol (FTP) Server, the Secure Socket Shell (SSH), and Remote Access services.

4.10.1   FTP

⚠️ **Important**
FTP is a non-encrypted and insecure protocol. We highly recommend that you routinely disable it, enabling it **only** when the rapid transfer of files is required.

FTP is a standard network protocol used to transfer files between a client and server on a computer network.

- FBxEdge supports FTP, which allows devices to securely exchange files with the edge devices. FBxEdge is the server in this exchange and the client is running on the device that is on the same network as FBxEdge.

- FTP can be used to transfer data into a CSV file or similar formats. It also can be used to read a file from the drive and send data to the cloud.

- SFTP is the secure version of FTP.

The FTP client must be running on a device that is on the same network as FBxEdge.

Use the following details to configure the FTP client and establish a connection to the FBxEdge server.

> **Important**
>
> When you create a user for FTP access the system presents the password for that user **only once**. Additionally, the system displays a dialog indicating that you must copy the password at that time. If you do not, the system invalidates that password and you must then create a new FTP user.

- Host: The IP address of the FBxEdge device

- Username: The FBxEdge FTP username

- Password: The password

- Port: The default FTP port is 21. The default SSH port is 22. SFTP uses port 22.

Filezilla® works well as the FTP client communicating with FBxEdge. To establish a connection with FBxEdge (the FTP server) from Filezilla, enter the Host, Username, and Password values (as described above), then click **Quickconnect**. Once connected, drag files from their source location to the default FTP directory in FBxEdge. This directory is */ftp-data.*

Figure 4-2. DeviceHub Import Page
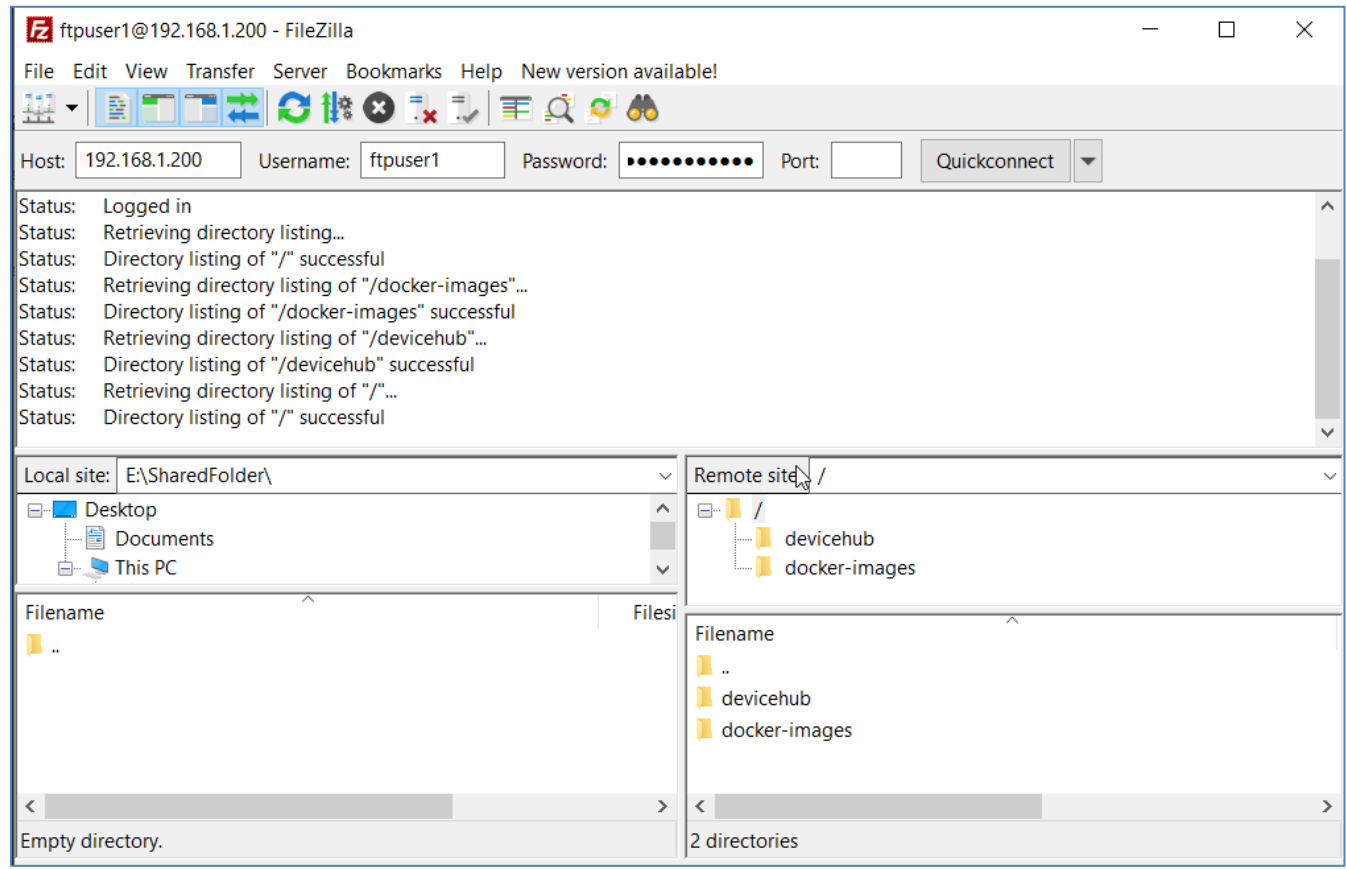
> **Note**
>
> If you are using FBxEdge as a client of FTP, there is no need to configure an FTP server.

4.10.2   Secure Socket Shell (SSH)

> **Note**
>
> SSH access is provided **only** for technical support usage; customers have no SSH access.

SSH is typically used to log into a remote machine and execute commands, but it also supports tunneling, forwarding TCP ports, and X11 connections. It can also transfer files using the associated SSH file transfer (SFTP) or secure copy (SCP) protocols. SSH uses the client-server model. In most cases, FBxEdge-maintained servers **require** SSH-based connections.

4.10.3   Remote Access

Remote Access allows you to access FBxEdge software from another network location.

4.11   External Storage

Select the **External Storage** option on the Navigation panel to open the Mount Points pane. Use the **Mount Points** pane to mount and manage network storage. This enables you to share the same storage location with all marketplace applications. Network storage expands the storage pool and facilitates enterprise backup/restore processes.

You can use either CIFS or FTP to mount external storage. **Before** you can add a CIFS mount point in FBxEdge, you must make a shared folder for Windows 10 or Linux.

4.12   Policy Management

> **Note**
> You must be an administrator to view the Policy Management pane.

Use the Policy Management pane to modify current policies. Default policies are part of the System module and are added during installation or upgrade.

- **Password Policy**
  You can modify a password policy from the **Password Policy** section. Password requirements are applied when you reset your password or create user accounts in FBxEdge.

  > **Notes**
  > - Some passwords (such as FTP and OPC UA) are system-generated and are part of the password policy.
  >
  > - Saving or resetting a password policy saves it to the system configuration file.

- **Disk Space Policy**
  You can add or modify a disk space policy from the User Limit panel in the Disk Space Policy section. Before saving the policy, you **must** also select a Warning or Stop Data Collection action.

  The System Limit (the amount of disk space reserved for the system) cannot be modified. You *can* add a policy for additional disk space for user data from the User Limit. You **cannot** assign less disk space than what is reserved for the System Limit.

  This means that if you have added a policy for additional disk space, the system either warns you about the disk space limit or stops the data collection (depending on your settings) when the disk space you have designated has been reached. You can view any warnings from **System** > **Events**.

If the System Limit is exceeded, an immediate stop data collection action occurs. If the User Limit is low, a 10-minute delay occurs before a Warning or Stop Data Collection action occurs. Service is restored once disk space becomes available.

When you view the Data Partition Usage section in **System** > **Info**, you can view the used, available, and total disk space. This helps you determine how much disk space you should add to the User Limit policy.

4.13   License

Important

License keys are perpetual, although each license is linked to a specific *version* of FBxEdge. As subsequent versions of FBxEdge occur, customers who are current with the yearly subscription/contract receive the corresponding revised license. Customers who are not current cannot upgrade to the most-current version unless they re-subscribe, at which point the license for the new version of software is provided.

FBxEdge supports two types of licenses:

- **Node-locked**
  Each license is locked to an edge device

- **Site**
  Activated with a license server embedded in FBxEdge Manager. During the activation of an edge device activation, this server can provide a site-license, which offers an unlimited usage of devices (except for configurable tag limits and reservations). You can define the limit (upper limit) and reservation (lower limit) of assets such as tags for each site license.

The License pane includes the following sections:

- **Installed Features**: Allows you to view the currently installed modules, as well as view and configure the number of devices and tags allowed under your license

- **License**: Allows you to add a standard license to replace the trail license, upgrade a license, add additional licenses to increase the number of devices and tags, or add new modules, as well as to remove licenses

- **Version**: Allows you to view the currently installed FBxEdge version

Trial Licenses

A trial license is valid for 15 days. During the trial period, notifications indicate the remaining number of days that the trial license is valid. Once a purchasing decision is made, a permanent license is issued. A trial license includes the following:

- **Modules**: Dashboard, DeviceHub, DataHub, Flows, Applications, Integration, OPC UA, and System

Contact your FBxEdge representative to request a license key.

Standard (Core) License

A standard core license is valid for 1 year. The license type, license key, and expiration date are visible from **System** > **License**. The license key contains 16-digits (such as 2411-3629-5461-7935) and *includes* all dashes. A standard core license includes the following:

- **Modules**: Dashboard, DeviceHub, DataHub, Flows, Applications, Integration, OPC UA, System

You can purchase, add, and activate multiple licenses to increase the number of device and tags or for products in addition to the standard core license.

When a standard core license expires, you cannot access any modules except the license section in System. A banner appears in **System** > **License** informing you which license has expired. You must contact your admin to add a new license and restore system functionality. Expiration dates apply to core and additional licenses.

You can upgrade an existing core license to replace it.

Notes

- You can active a standard core license without being connected to the internet.

- You cannot deactivate a license.

- A license can be used on the same edge device (same Host ID) any number of times as long as the use occurs **before** the license's date of expiration.

4.14   Events

Use the **Events** pane to display a list of events that have occurred in FBxEdge. "Events" are the actions an edge device performs, identifies, and then logs during its operation.

You can view information for each of the listed events: the edge device component where the event had occurred, the event severity, and so on.

The system tracks events for the following components:

- Integration (cc)

- DeviceHub (dh)

- System (dm)

- Authentication (auth)

- Marketplace (mp)

- Licensing (lic)

The Events pane has two tabs:

- **Live Events**

  Shows events as they occur, in inverse chronological order.

- **Events History**

  Filters and sorts events using a number of criteria (date and time range, component name, etc.)

4.15 Support

Use the **Support** pane to review the status of the edge device's components, download any support bundles, and identify any available file downloads.

4.16 Backup/Restore

Use the **Backup/Restore** pane to configure and initiate system backups and restore operations. Because an FBxEdge device can have hardware failures, a disaster recovery plan needs to be in place to support device replacement. You can create detailed, granular backup templates and exchange these templates between edge devices as JavaScript Object Notation (*.JSON*) files.

4.16.1 Backup/Restore Tab

The backup/restore feature supports the following use cases:

- Restoring the last know good configuration following an accidental deletion/overwrite of a portion of a configuration.

- Device hardware fails and the device must be replaced with another one

- Device hardware is upgraded

Note

Backup and restore operations are **not** intended to replicate configurations.

4.16.1.1 What Is Backed Up

The feature saves configurations, including OPC UA configurations, in a DAT file, which is downloadable from the Backup/Restore Configuration section in the **Backup/Restore** tab. Currently, databases and container volumes/images are **not** part of backup.

Included in a backup are:

- Device IP

- DNS

- NTP

- Device Configuration

- Tags

- Flows

- OPC UA

- Integration Connectors and Configurations

- Users

- Timezone

The lightweight backup file efficiently uses storage resources and employs encryption to secure credentials.

4.16.1.2   Before Beginning

- The FBxEdge license key provides a backup/restore functionality.

- Once you receive the license key, go to **System** > **License** to enter the license key and activate the license

- Make sure you have activated the device with FBxEdge Manager.

4.16.1.3   Best Practices

Note
Refer to your organization's standards and requirement to determine the frequency for performing device backups.

The following recommendations help to ensure seamless recovery:

- As a default, the system names the backup file using the format *backup_1624983948318.dat*, where "*1624983948318*" is a system-assigned identification. Rename the file using a naming convention that enables you to quickly identify the date the backup occurred (such as *2022-09-18-18:12:51-backup.dat*).

- Move the backup file from the default *Downloads* directory to an operational directory on a server that can be accessed by the operations team.

4.16.1.4   Successful Backup

Extract and open the backup DAT file using Notepad.

- The backup DAT file contains the FBxEdge configurations, OPC UA configurations, and Flows configurations.

- Use this file to restore your edge device.

> ### ⚠ CAUTION
>
> Modifying the contents of the backup DAT file may render it unusable for restoring an edge device.

4.16.2 Template Tab

The **Template** tab allows you to select configurations available for the edge device and download them to a JavaScript Object Notation (*.JSON*) file, which creates an edge device configuration template. Flows are included as part of the backup restore template.

You can create multiple versions of edge device configuration files. You can then upload the template file to another edge device. A successful upload applies the configuration to that device.

Using FBxEdge Manager, you can also apply templates to one or more edge devices at one time, considerably reducing the effort involved in configuring edge devices. Refer to the *FBxEdge Manager User Guide* (D301916X012) for further information.

Appendix A. Installing the RXi2-BP Gateway

⚠️ **Important**

Emerson offers two gateway devices as part of the FBxEdge solution: the default RXi2-LP and the optional RXi2-BP. Consult with your Emerson Impact Partner to determine which gateway device meets your organization's needs. **This appendix discusses the installation of the RXi2-BP gateway**.

When delivered from the factory, the FBxEdge software is pre-installed on the RXi2-BP gateway. You must still find a suitable location for the gateway.

Figure A-1.   RXi2-BP Industrial PC

A.1   Unpacking and Inspecting

⚠️ **WARNING**

If the RXi2-BP IPC operates in an area of high ambient temperature up to 70 °C (149 F°), the surface of the enclosure, especially the heat sink, can reach a temperature of 80 °C (185 °F) and above. Be careful and do not touch the RXi2-BP IPC with bare fingers.

A.1.1   Package Contents

Verify that the delivered package contains the following contents:

Item	Quantity	Description
RXi2-BP IPC	1	RXi2-BP Industrial PC

Item	Quantity	Description
Serial Connector Plug	2	Serial Connector Plug
24V Power-in Connector Plug	1	Power Connector Ring
Emerson FBxEdge User Guide (part D301913X012)	1	User guide for gateway

A.2 Power Requirements

The RXi2-BP requires a DC power supply with 24V (± 25%) that delivers at least 1.8A. The corresponding plug is a Phoenix Contact 1748367. Use the same connector type or its equivalent.

Note

Unlike the RXi2-LP, the RXi2-BP **does not** have a dedicated power button; it powers up when you apply power to the gateway.
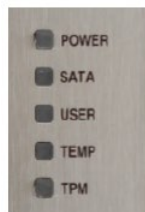
Figure A-2. Power Connector

Signal Name	Pin (left to right)
Power + (24V DC)	1
Power − (24V DC)	2
FGND	2

A.3 LEDs

The RXi2-BP provides color-coded status LEDs on the front panel to indicate various functions.

Figure A-3. LEDs

LED Name	Color	LED Status Indicator
	Green	All power rails available and valid (S0)

LED Name	Color	LED Status Indicator
POWER (also a button)	Yellow	Standby power valid (S3/S4/S5)
	Red	Error condition; contact Emerson support for help
STA	Green	SATA access in progress (M.2)
USER	Green	Reserved for future use
TEMP	Green	Temperatures are below T_{hot} and T_{crit}
	Yellow	Temperatures are above T_{hot} and below T_{crit} If supported by the OS, a graceful shutdown is initiated
	Red	Temperatures are above T_{hot} and T_{crit} An immediate shutdown has occurred to protect the system
TPM (also a button)	Yellow	If physical presence is activated, this LED shows the current status of the physician presence

A.4 Ports

The RXi2-BP provides several ports you can use to connect devices.

A.4.1 Ethernet Ports

The RXi2-BP provides four Ethernet ports: three on the front panel (labeled ETH 1, ETH 2, and ETH 3) and one on its left side (labeled ETH 0). All ports support 10/100/1000 Base-T. For a proper 100/1000 Mbit connection, Emerson recommends using a CAT5 cable.

⚠️ **Important**
As *Figure A-4* shows, the port addresses on the BP gateway do not correspond to how the FBxEdge OS recognizes those ports.
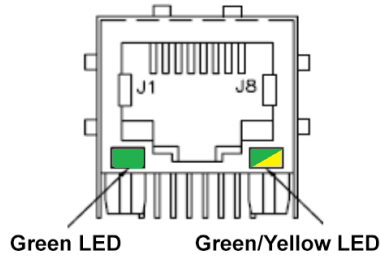
Figure A-4. Ethernet Ports

10/100 BaseT Name	1000 BaseT Name	Pin
TxD+	LP_DA+	1
TxD−	LP_DA−	2

10/100 BaseT Name	1000 BaseT Name	Pin
RxD+	LP_DB+	3
NC	LP_DC+	4
NC	LP_DC–	5
RxD–	LP_DB–	6
NC	LP_DD+	7
NC	LP_DD–	8

A.4.1.1   Ethernet Port LEDs

All Ethernet ports use the same LED configuration.

Figure A-5. Ethernet LEDs

Pin	LED Color	LED Status Indicator
12	**Green**	ACT/LINK Blink with activity Steady on with no activity at 10/100/100
13/14	**Green** **Yellow** Off	LINK1000 (steady on) LINK100 (steady on) LINK19

A.4.2   Display Port

The RXi2-BP provides one display port (located on the left side of the gateway next to the ETH 0 port). Use it to directly connect a monitor with a DP input or use standard off-the-shelf adapters to convert the DP signals to HDMI or VGA.

Figure A-6. Display Port

Signal Name	Pin
TxD0+/–	1/3

Signal Name	Pin
TxD1+/−	4/6
TxD2+/−	7/9
TxD3+/−	10/12
AUXSEL	13
NC	14
CLK/AUX+	15
DAT/AUX−	17
HTPLG	18
DP_VCC	20
GND	2, 5, 8, 11, 26, 19

A.4.3   USB3.2 Gen1 and USB2 Ports

The RXi2-BP provides four USB ports, all using Type A connectors. Two (USB 1 and USB 2, which support USB 3.2 Gen1) are located on the front of the gateway to the right of the bank of three Ethernet ports. Two additional ports (USB 3 and USB 4, which support USB2) are located on the left side of the gateway. Each USB port is protected with an electrical fuse rated up to 1A. For normal operation, do not exceed 900mA for USB 3.2 Gen1 or 500mA for USB2. Limit the cable length to no more than 3m.

Figure A-7. USB Ports (3.2 and 2)
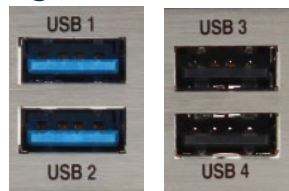
USB3.2 Signal Name	Pin
VCC (5V_SBY)	1
USB−	2
USB+	3
GND	4
SSRX−	5
SSRX+	6
GNC	7
SSTX−	8
SSTX+	9

USB3.2 Signal Name	Pin
USB2 Signal Name	**Pin**
VCC (5V_SBY)	1
USB−	2
USB+	3
GND	4

A.4.4 Serial Ports

The RXi2-BP provides two serial interfaces, one (P0) configured to RS-232 and one (P1) configurable to RS-422 or RS-485 (2W/4W). The connector is a Phoenix Contact 1953745 or equivalent and mates with a Phoenix Contact 1952296. Two mating plugs are shipped with the unit. The RS-232 cable can be no longer than 15m. The RX-4xx cable can be more than 30m, depending on capacitive cable load.

Figure A-8. Serial Ports

Signal Name Pin RS-232	Pin
TX	1
RTS	2
GND	3
CTS	4
RX	5
Signal Name Pin RS-4xx	**Pin**
RX+	6
RX−	7
GND	8
TX−	9
TX+	10

For RS−422 and RS−485-4-wire modes, connect the corresponding RX+/− signals with the TX+/− signals and vice versa on the remote device. For RS−485 2-wire mode, connect RX+

and TX+ with the + line of the cable and the RX– and the TX– together with the – line of the cable.

The TX/RX signal control is difference between the various RS–4xx modes. In the RS–422 mode, TX and RX are always active. In RS–485 **4-wire** mode, TX is active only when there is something to transmit, while RX is always active. In RS–485 **2-wire** mode, TX and RX are active when transmitting and inactive when not transmitting. Use the Operating System device driver to select various modes.

Note

The RXi2-BP gateway does not provide any termination resistors. If required, attach the termination directly to the plug text here.

A.4.5 microSD Slot

The RXi2-BP provides a slot that accommodates a microSD (μSD) card, protected with a mechanical lock. Loosen the mechanical lock to insert the microSD card and tighten to re-secure.

Figure A-9. microSD Slot

Signal Name	Pin
DATA2	1
DATA3	2
CMD	3
VDD	4
CLK	5
VSS	6
DATA0	7
DATA1	8
CD	9

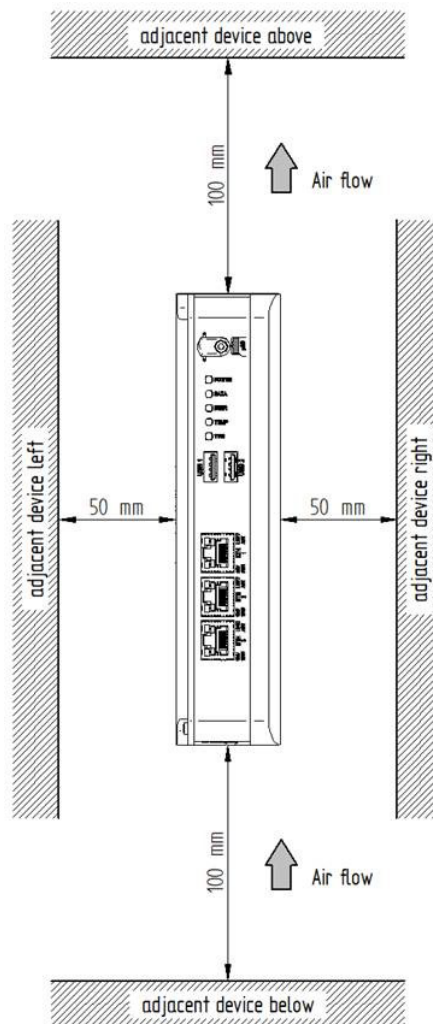# A.5 Mounting the Gateway

> ⚠ **CAUTION**
>
> Install the RXi1-BP IPC **only** in locations with restricted access.

The gateway is designed to be mounted vertically, whether attached directly to a panel or to a DIN rail.

A.5.1 Required Clearances

As shown in *Figure A-10*, whether you panel-mount the gateway or connect it to a DIN rail, you must provide sufficient clearances around the gateway to ensure optimal thermal performance.

Figure A-10. Minimum Clearances for Gateway

A.5.2 DIN Rail Mounting

Depending on the size of the DIN rail connector, use either of the two DIN rail mounting options:

- If the DIN connector is **7.5 mm** in height, use a **single** DIN rail support to offset the bottom of the gateway
- If the DIN connector is **15 mm** in height, use **two** DIN rail supports in a stack to increase the height to offset the bottom of the gateway.

To connect the gateway to a DIN rail, first connect the DIN Rail Clamp #R2B00ACCRM01 to the rear of the gateway:

1. Place the DIN rail on the rear face of the gateway.

2. Use a T9 Torx® driver to secure the DIN rail with the provided M3x5-A2 screws, tightening to 0.6 Nm (do not overtighten). In rugged applications, use a thread-locking compound to prevent the screws from loosening.

Figure A-11. Attaching a DIN Rail to the Gateway
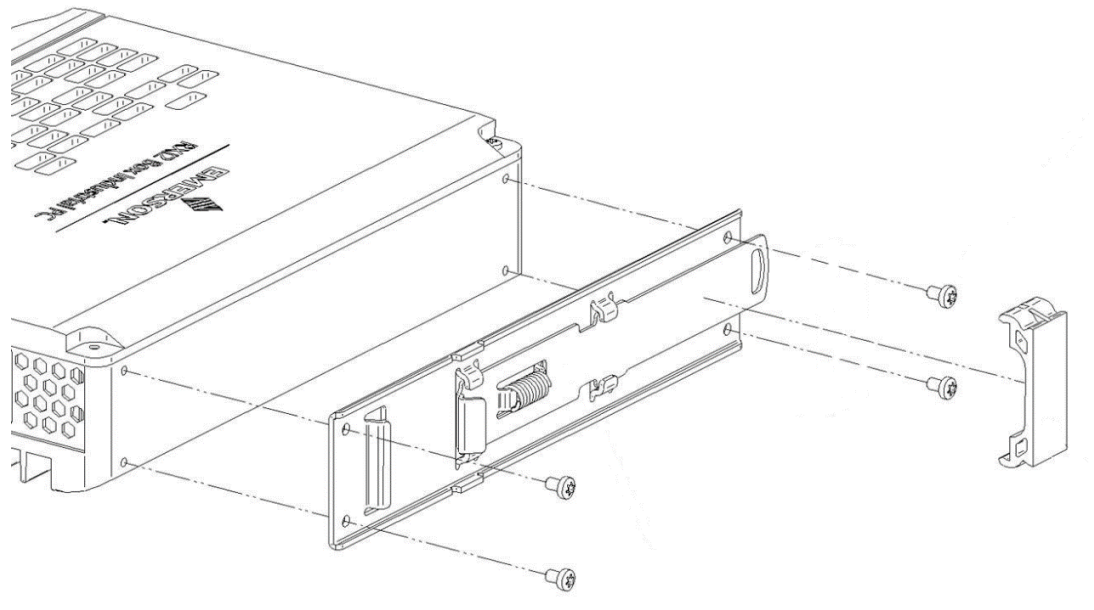
Figure A-12. DIN Rail Mounting Options
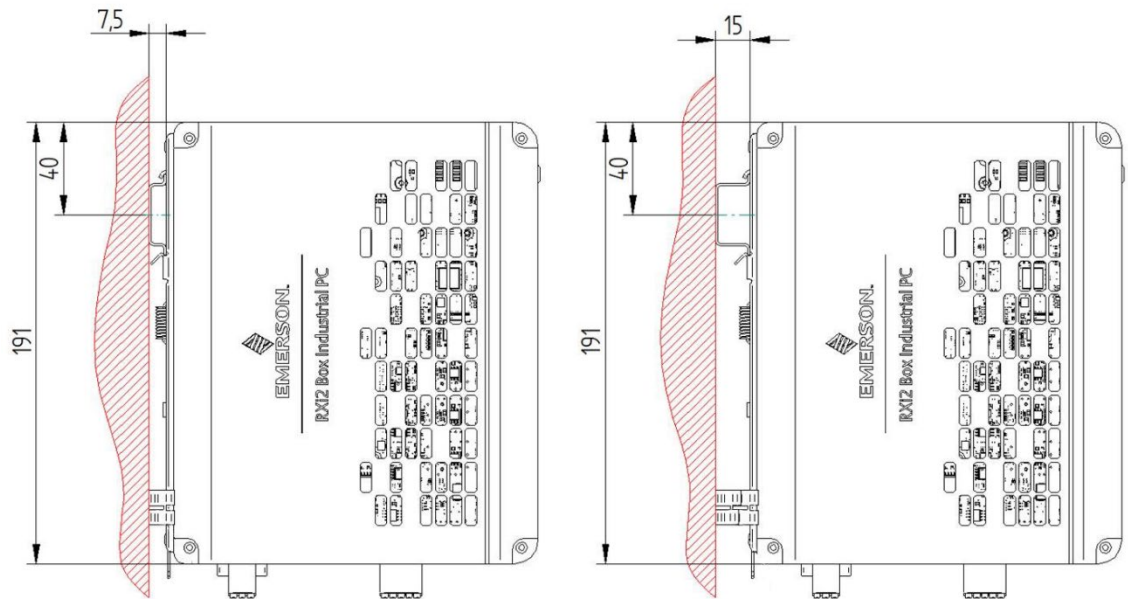
A.5.3 Panel Mounting

To mount the gateway to a panel, connect the Mounting Plate #R2B00ACCMP01 to the rear of the gateway:

1. Place the mounting plate on the rear of the gateway.

2. Use a T9 Torx driver to secure the mounting plate with the two provided M3x6 screws, tightening to 0.6 Nm (do not overtighten).

3. For regular mounting, secure the mounting plate and gateway through the top and center holes. For more rugged applications, secure the mounting plate with the four provided M3x6 screws in all four corners of the mounting plate.

Figure A-13. Attaching the Mounting Plate
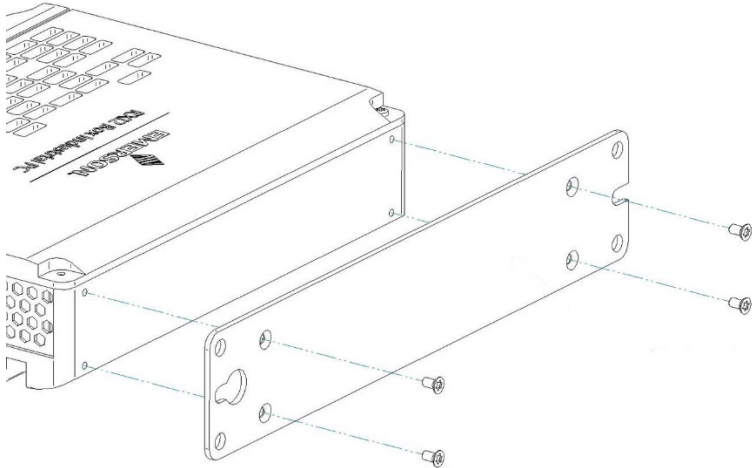
Figure A-14. Panel-mounting the Gateway
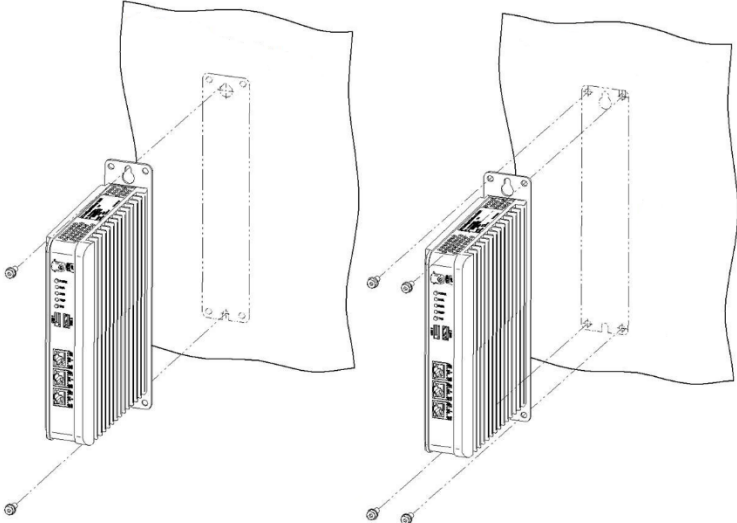
Emerson FBxEdge User Guide

D301913X012

April 2024

For customer service and technical support, visit *Emerson.com/Guardian*.

North America and Latin America:
Emerson Automation Solutions
Energy and Transportation Solutions
6005 Rogerdale Road
Houston, TX 77072 U.S.A.
T +1 281 879 2699 | F +1 281 988 4445
Emerson.com/SCADAforEnergy

United Kingdom:
Emerson Process Management Limited
Fosse House, 6 Smith Way
Grover Park, Enderby
Leicester LE19 1SX UK
T +44 0 870 240 1987

Europe:
Emerson S.R.L
Regulatory Compliance Shared Services
Department
Company No. J12/88/2006
Emerson 4 Street
Parcul Industrial Tetarom 11
Romania
T +40 374 132 000

Middle East/Africa:
Emerson Automation Solutions
Energy and Transportation Solutions
Emerson FZE
P.O. Box 17033
Jebel Ali Free Zone – South 2
Dubai U.A.E.
T +971 4 8118100 | F +971 4 8865465

Asia-Pacific:
Emerson Automation Solutions
Energy and Transportation Solutions
1 Pandan Crescent
Singapore 128461
T +65 6777 8211| F +65 6777 0947

Energy and Transportation Solutions

EMERSON™