PACEdge™

USER MANUAL

CONTENTS

Warnings and Caution Notes as Used in this Publication

⚠ WARNING

Warning notices are used in this publication to emphasize that hazardous voltages, currents, temperatures, or other conditions that could cause personal injury exist in this equipment or may be associated with its use.

In situations where inattention could cause either personal injury or damage to equipment, a Warning notice is used.

⚠ CAUTION

Caution notices are used where equipment might be damaged if care is not taken.

Note: Notes merely call attention to information that is especially significant to understanding and operating the equipment.

These instructions do not purport to cover all details or variations in equipment nor to provide for every possible contingency to be met during installation, operation, and maintenance. The information is supplied for informational purposes only, and Emerson makes no warranty on the accuracy of the information included herein. Changes, modifications, and/or improvements to equipment and specifications are made periodically, and these changes may or may not be reflected herein. It is understood that Emerson may make changes, modifications, or improvements to the equipment referenced herein or to the document itself at any time. This document is intended for trained personnel familiar with the Emerson products referenced herein.

Emerson may have patents or pending patent applications covering the subject matter in this document. The furnishing of this document does not provide any license whatsoever to any of these patents.

Emerson provides the following document and the information included therein as-is and without warranty of any kind, expressed or implied, including but not limited to any implied, statutory warranty of merchantability or fitness for a particular purpose.

Section 1: Introduction

PACEdge processing unlocks the full potential of your operational data by enhancing reliability, strengthening safety, and reducing energy consumption across your industrial systems. As a comprehensive edge computing platform, PACEdge streamlines the development, deployment, and management of your IIoT applications.

By integrating every essential component of the IIoT application lifecycle into a single, cohesive package, PACEdge provides a unified environment for engineers and developers. This reduces complexity, shortens development cycles, and accelerates time-to-deployment. The result is a scalable, efficient solution that expands your deployable footprint while maintaining consistency from prototype to production—empowering you to build robust, future-ready industrial applications with confidence.

1.1 Revision History

Rev	Date	Description
N	Mar 2026	Adds support for PACEdge v3.0.0 release
M	Jul 2025	Adds support for PACEdge v2.9 release
L	Apr 2025	Adds support for PACEdge v2.8 release
K	Dec 2024	Adds support for PACEdge v2.7 release
J	Jun 2024	Adds support for PACEdge v2.5 release
H	Mar 2024	Adds support for PACEdge v2.4 release
G	Oct 2023	Updates related to the PACEdge v2.3 release
F	Mar 2023	Added cautions warning against the use of dollar signs ($) in passwords
E	Nov 2022	Updates related to the PACEdge v2.2 release
D	Dec 2021	Added details on Accessing the Connext OPC UA Server
C	Sep 2021	PACEdge 2.1 Initial release
B	Nov 2020	Added Section 7.2 Node-RED Dashboard Performance Indication
A	Sep 2020	PACEdge 2.0 Initial release

1.2 New Features in the PACEdge 3.0.x

1.2.1 New Graphical Front End

PACEdge v3.0.0 introduces a redesigned Graphical User Interface (GUI) with an updated look and feel. The new interface provides two distinct views tailored to different user roles:

Administrator and Developer View – This view features a left-hand navigation menu that provides quick access to all key PACEdge tools and system functions. It is designed to support system configuration, development, and maintenance activities.

Operator View – Intended for end users interacting with the finished solution, this view can be deployed in kiosk mode. It presents a simplified, customized interface with shortcuts to WebHMIs, dashboards, and other operational user interfaces.

This dual-view design ensures that each user role has an environment optimized for their responsibilities and workflow.

1.2.2 Enhanced Modularity of the PACEdge Platform

With PACEdge v3.0, platform modularity has been significantly improved, allowing users to tailor the set of tools required for their specific applications. Some components—such as **Node-RED**, **Grafana**, and the **reverse proxy**—are considered essential and remain permanently enabled.

A second group of tools, including **Movicon**, **Chronograf**, **pgAdmin**, **mqttExplorer**, and **Jupyter/Python**, can be easily enabled or disabled through the GUI. This flexibility helps streamline the environment, ensuring that only the necessary tools are active for a given solution.

1.2.3 Enhanced Group Management Tool

As of PACEdge v3.0.0, a **Group Management (GM)** tool is now available through the GUI. The GM tool retrieves both **Linux operating system updates** and **container-based application updates** from the online software repository and applies them to the devices it manages. This feature is designed to simplify deployment, maintenance, and updates across fleets of PACEdge devices—scaling efficiently to hundreds of units.

In this release, the Group Management tool supports updates for:

- **Host Linux OS updates**
- **PACEdge Application updates**
- **Node-RED flow deployments**
- **Grafana dashboard deployments**

Users can create groups of PACEdge devices and execute updates across all devices within a selected group, enabling consistent and centralized management.

For more information on Group Management, refer to **Section 4.6, Group Manager**.

1.2.4 Online Marketplace

PACEdge v3.0.0 now includes an online app marketplace, which will feature additional value-added applications available for the users.

PACEdge integrates the **Marketplace** as a standardized software distribution mechanism that enables the installation, update, and management of industrial automation applications packaged for containerized execution on Linux-based edge devices. The Marketplace provides a structured catalogue of automation-focused applications delivered through a secure, browser-based interface designed for consistent and automated deployment flows. As of PACEdge v3.0.0 release Marketplace only has PACEdge standard applications, but as new applications get qualified or developed, they will show up in the Marketplace for users to take advantage of.

1.2.5 Operators Dashboard

PACEdge v3.0.0 is prepared to be used by the operators and has a simplified and clean view using kiosk mode, which contains only the required shortcuts to the Node-RED or Grafana dashboards, as well as to WebHMI. Tools within PACEdge allow users to configure operators' views by enabling/disabling standard shortcuts as well as by adding custom shortcuts.

1.2.6 New Licensing Tool

PACEdge v3.0.0 is using a new and improved licensing tool, which will enable finer granularity of features being licensed.

1.2.7 Jupyter and Python Container and Example (optional)

PACEdge v3.0.0 includes an optional Jupyter/Python container and Python-Node-RED application example. When enabled, users can access the Jupyter web interface by using the tab on the left side menu. Refer to Section 3.1.5 Jupyter-Python, for instructions on enabling the container and using the example.

Jupyter and Python container, providing an isolated, containerized environment for interactive Python development, data analysis, and rapid prototyping directly on the edge device. The container is based on standard Jupyter Docker Stack images, which bundle Jupyter Lab/Notebook together with common scientific Python libraries in a ready-to-run Docker image, ensuring consistent environments and avoiding dependency conflicts between applications running on PACEdge. These images support full Jupyter Server

functionality—including token-based authentication, notebook execution, and port-mapped browser access—and follow established container lifecycle practices such as persistent volume mounting and controlled updates.

1.2.8 MQTT Explorer

A new tool, MQTT Explorer, has been included in the PACEdge v3.0.0. **MQTT Explorer** is a containerized diagnostic and monitoring tool for MQTT-based systems. MQTT Explorer is a comprehensive MQTT client that provides a structured, hierarchical view of MQTT topics, enabling users to visualize topic activity, browse retained messages, filter or search topic trees, and inspect or publish MQTT payloads in real time. Its interface supports detailed topic inspection, payload formatting (including JSON pretty-printing), and real-time message monitoring, making it suitable for verifying MQTT traffic and troubleshooting device interactions on PACEdge. Containerized versions of MQTT Explorer run as lightweight services accessible through a web browser, aligning with PACEdge's modular, container-managed environment.

1.2.9 Applications Updated to a Newer Version

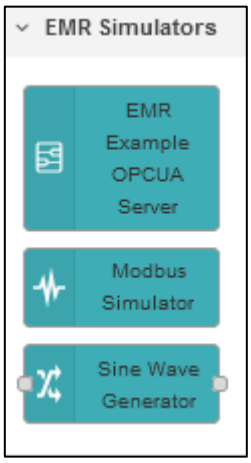
In PACEdge v3.0.0, all applications have been updated to a newer version. GFK-3198, PACEdge IPI lists the exact versions of each application, but the most important updates are as follows:

- Updated Movicon Connext © and WebHMI to Movicon.NExT™ v4.4.0
- Updated Node-Red to version 4.1.5. This includes functional updates, new nodes, improved editor, and look and feel improvements.
- Updated Grafana® to version 12.3.1.

1.2.10 Functional Improvements in Node-RED

New examples are now available in the **Import->Examples->node-red-contrib-emerson** section, which now includes an OPC-UA Server Simulator, an example Modbus TCP Simulator, an example Sine Wave generator, and examples to store data in Timescale database. Upon installation, PACEdge-customized nodes will be added to the palette EMR Simulators category, which can be utilized to simulate external devices that generate data.

Figure 1: Data Source Simulators in Node-RED



Section 2: PACEdge Getting Started

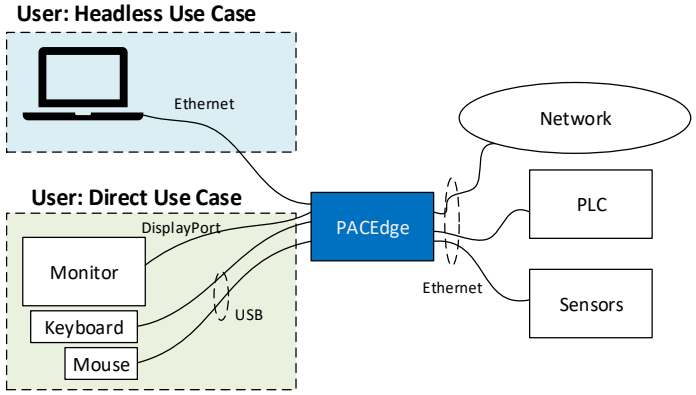
Note: PACEdge software comes pre-installed on Emerson Industrial PCs and Controllers, and depending on the ordered configuration, might include WebHMI and Connext or Group Manager.

2.1 PACEdge Usage Models

PACEdge software has 3 usage models:

1. **Direct Use Model**: Running on the Industrial PC., which has a directly attached Monitor, keyboard, and mouse.
   Note: this mode is not supported on CPL410 and CPE400 Controllers, as well as on 2-core and 2GB RAM IPC2010 models
2. **Headless Use Model**: Running on the Industrial PC, which operates in headless mode, the user accesses it remotely via Ethernet using a web interface.
3. **Virtual Machine (Remote Desktop)**: Running on a VMware or Hyper-V virtual machine (should only be used for group management).

Figure 2: Use Case Models



Note: for configuration, administrative tasks, or file transfer, the user can also use an SSH Client to access PACEdge. The same Linux (Cockpit) login credentials apply.

2.2 PACEdge in a Direct-Use Configuration

2.2.1 Getting Started

1. Connect the monitor to the device using a DisplayPort cable (Check the hardware, Manual).

   Note: If the monitor of choice has an HDMI or VGA input, use a standard off-the-shelf DP-HDMI or DP-VGA adapter.
   In case of 4-core and 4GB RAM IPC 2010 model, use a special USB-C to DisplayPort cable (can be ordered as an accessory from Emerson)

2. Connect a keyboard and mouse to any of the USB ports.
3. Power up the PACEdge device and wait until it boots.
4. The boot process will pause and ask for login details. Log in as **admin** with the password **edgestack**.
   Note: The user will be asked to change the default password to a unique password at the first login.
5. Most interactions with PACEdge are done via a browser-based interface. Click on Activities->Show Applications and start the Firefox browser to get started.

   Within the Firefox browser, go to **https://localhost** or, to use the pre-installed PACEdge CA and certificate, go to: **https://hostname.local.**
   Hostname is: pacedge-xxx, where xxx is a serial number that can be found on the device label.
6. Proceed to the section entitled *Section 2.4 Device Initialization.*

2.3 PACEdge in Headless Configuration

In a Remote Headless configuration, the user interfaces with PACEdge via Ethernet using a remote device's (Panel PC, laptop) web browser.

2.3.1 Getting Started

1. Connect the Ethernet cable to the Ethernet port, depending on the hardware, labeled as follows:
    a. IPC6010/7010/8010: ETH2
    b. RXi2-BP: ETH0
    c. IPC 2010: Port 2
    d. CPL410/CPE400: ETH
2. Set up the User PC Ethernet port IP address to be statically assigned as follows:
    a. **IPv4 Static IP: 192.168.3.10**
    (or similar in the same subnet)
    b. Netmask: 255.255.255.0
3. Power up the PACEdge unit and wait until it boots.
Note: on CPL410/CPE400, wait until the GPOK LED is lit.
4. Open the browser of your choice and type in **192.168.3.100** or, if known, ***hostname*.local,** in the address bar. Hostname is: pacedge-xxx, where xxx is a serial number that can be found on the device label.
5. Proceed to *Section 2.4 Device Initialization.*
6. **Note**: Access via web browser uses pre-installed certificates and provides extra insurance that you are indeed connecting with the expected PACEdge device. The hostname is **pacedge-xxx**, where xxx is the serial number of the HW. If not known, log in for the first time using the static IP address, and take note of what the hostname is.

Note: All Ethernet ports are configured to get IP addresses assigned by the DHCP server. This dynamically assigned IP address can also be used to access PACEdge. On CPL410 and CPE400, the first two IP addresses can be read from a built-in display by going into **Edge Settings->Network Config**.

2.4 Device Initialization

2.4.1 First-Time Login and Certificate Provisioning

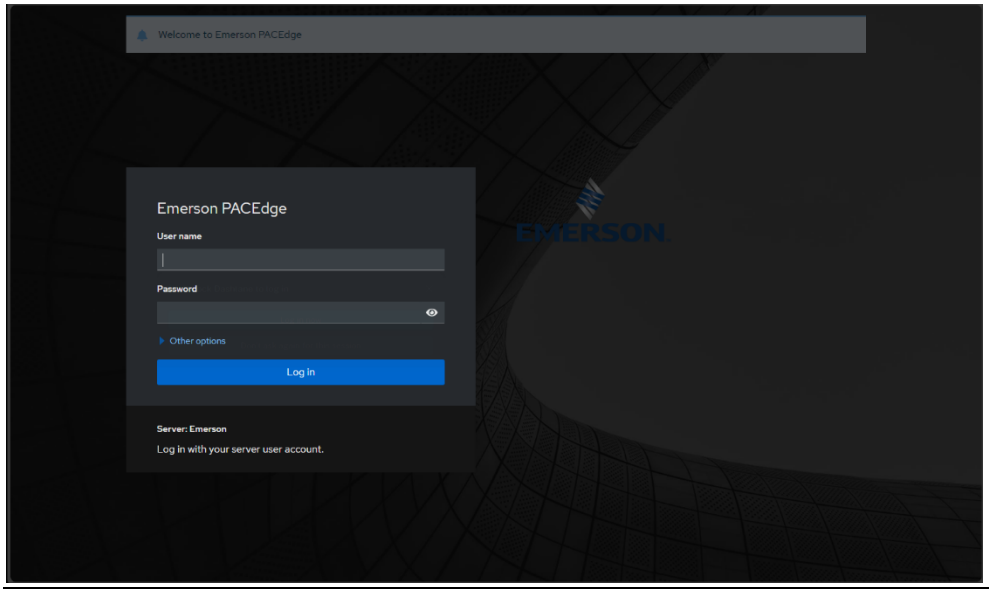
When accessing the device for the first time using its **IP address**, the browser may display a security warning. This occurs because the PACEdge certificate is issued for the device's **hostname**, not its IP address, and the browser may report that the device's identity cannot be verified. To proceed, select **Advanced** and then **Accept**.

As an alternative to using the IP address, you can access the device via its hostname: **pacedge-xxx.local**, where **xxx** is the device's serial number. For further details on certificate infrastructure, refer to Section: *3.11 PKI and its use in PACEdge.*

To ensure the device certificate is trusted, download the **PACEdge Certificate Authority (CA) certificate**—available from the Emerson Customer Center or from the PACEdge Cockpit utility—and install it in your browser's trusted certificate store.

After connecting, you will be automatically redirected to the Cockpit. Here, the default user login entry will be displayed.

Figure 3: Login Screen



Use the username: **admin** and password: **edgestack** to sign in to the Cockpit dashboard. The system will prompt the user to change the password at the first login. The password is the same as the Linux/Cockpit password. In the next step, the system will prompt the user to set services/applications passwords for each user role.

Next, the End User License Agreement (EULA) will be shown. Please read it carefully and accept the terms to proceed.

2.4.2 Device Configuration

Device Configuration will require the setup of both **Services** and **Passwords;** these settings will be used to provision the device for use and are a requirement before anything else can be done on the device.

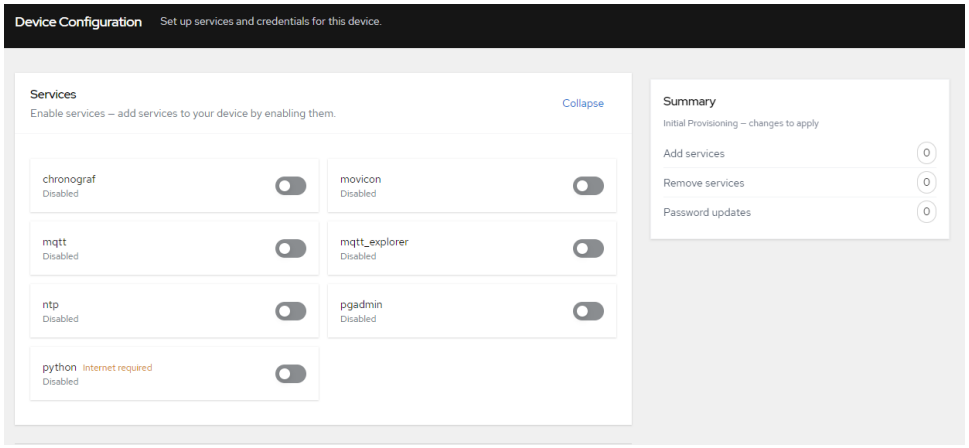
The Device Configuration screen is divided into 3 cards.

- Service – What service will be deployed and enabled in the device
- Password – The default list of user and a means to set their passwords
- Summary – Which will display a summary of the item to be deployed.

2.4.3 Setting Services

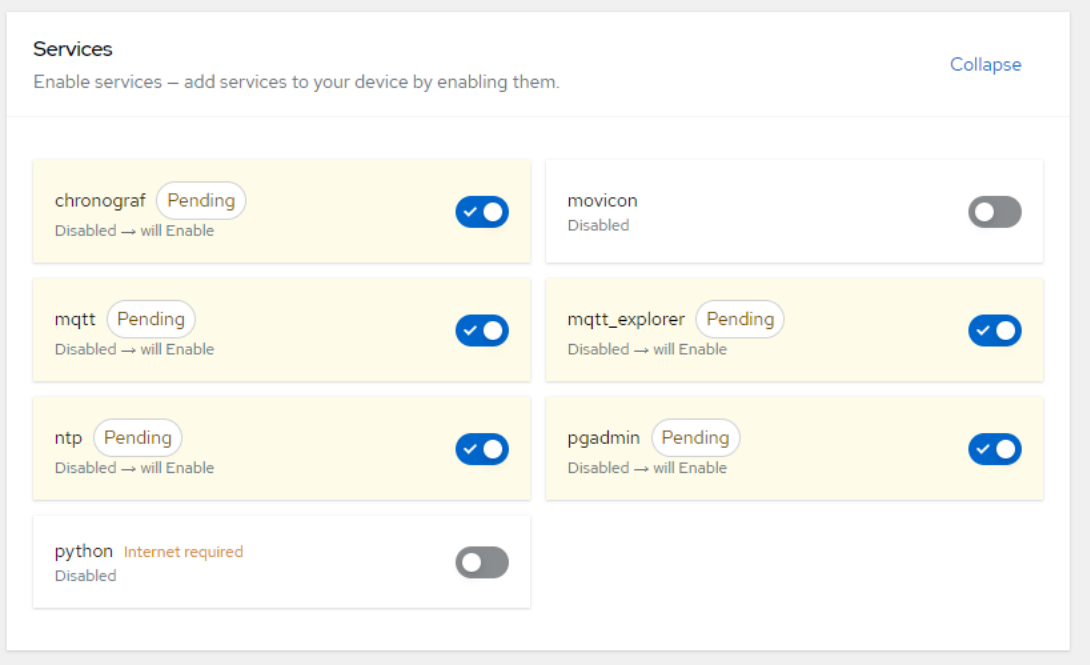
In the PACEdge, services are split into a mandatory set and an optional set. Mandatory services will always be enabled, but users can choose what optional services should be activated as required by the device's purpose and requirements.

Figure 4: Device Configuration - Services Card



Once selected, the Services section will indicate which services are pending deployment. Some services, such as Movicon, require a valid license to operate. Others, for example, Python, require an internet connection for deployment. These requirements will be clearly indicated where applicable.

Figure 5: Services Section



2.4.4 Setting Initial Password

PACEdge includes multiple applications and tools, each with its own user authentication requirements. To simplify account handling, PACEdge provides four predefined user accounts:

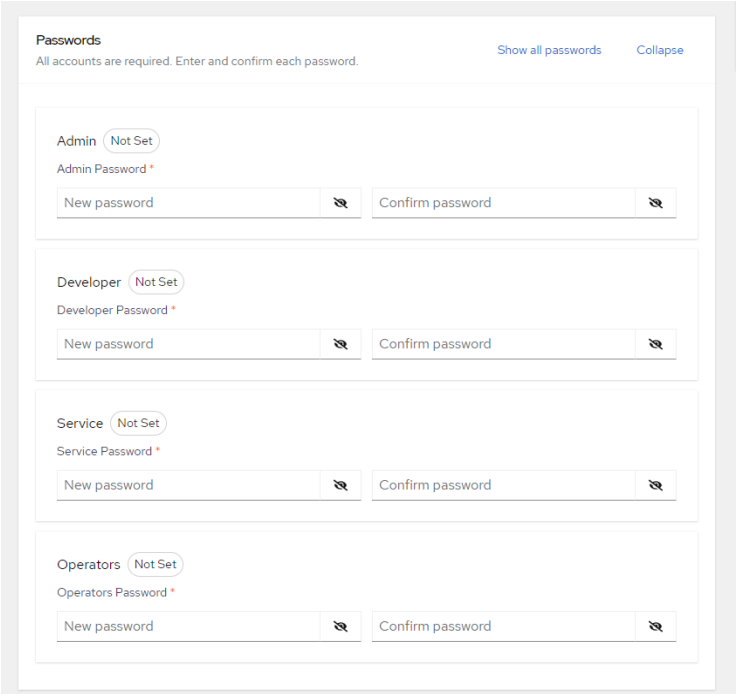
- admin
- developer
- service
- operators

Important Note: PACEdge uses two separate password domains: one for the host Linux operating system and one for PACEdge services and applications.
The **admin** user exists in both domains; however, these accounts are independent and are not linked. Each must be configured with its own password. For more information, see *Section 3.4 PACEdge Users, Rights, and Passwords*.

Important Note: For cybersecurity compliance, all default passwords must be changed at first login.

During the initial password setup, the user **MUST** set passwords for each user role, as this process also initializes roles in databases and supporting utilities.

Figure 6: Initial Password Setup



During the provisioning process, user accounts and passwords are deployed to all PACEdge applications. After the initial deployment, returning to this page allows users to update passwords as needed.

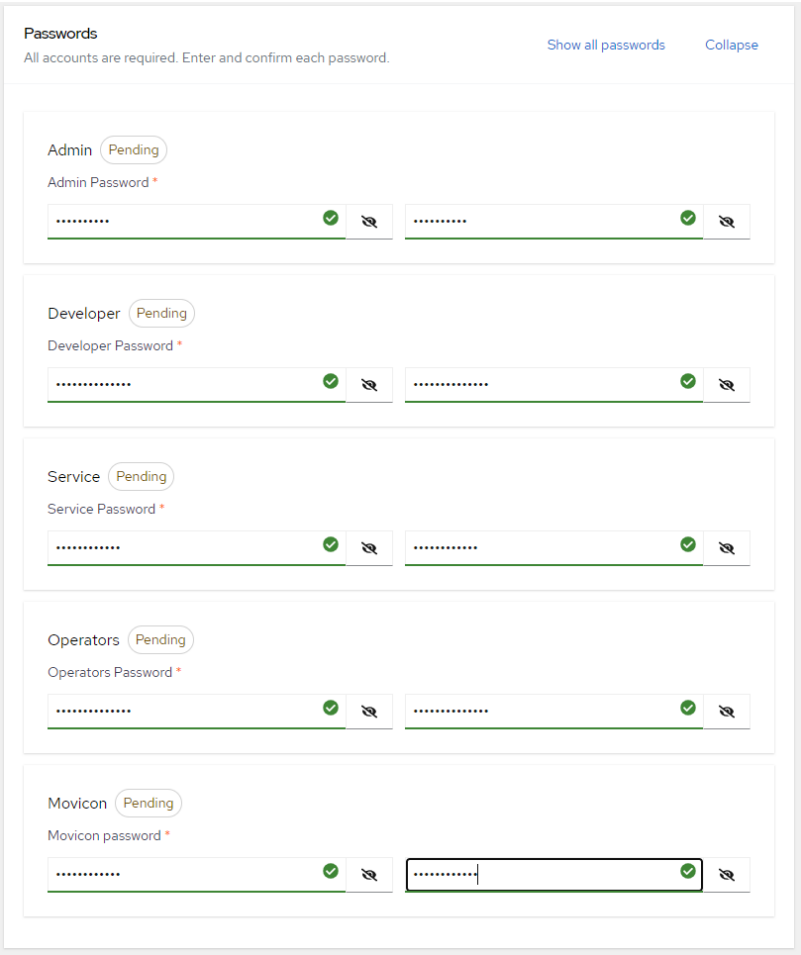
Account Practices

In Cockpit/Linux, non-admin accounts are disabled by default. Enable accounts and assign passwords only when required. Do **not** set a password for the **root** user. This account is intentionally disabled for security reasons, and setting a password would enable it.

Important

Please consult the PACEdge Secure Deployment Guide (GFK-3197) for recommended password changes and other cybersecurity-relevant settings. Detailed password change procedures can be found in 3.5, *PACEdge Users, Rights, and Passwords.*

Figure 7: Updated Passwords



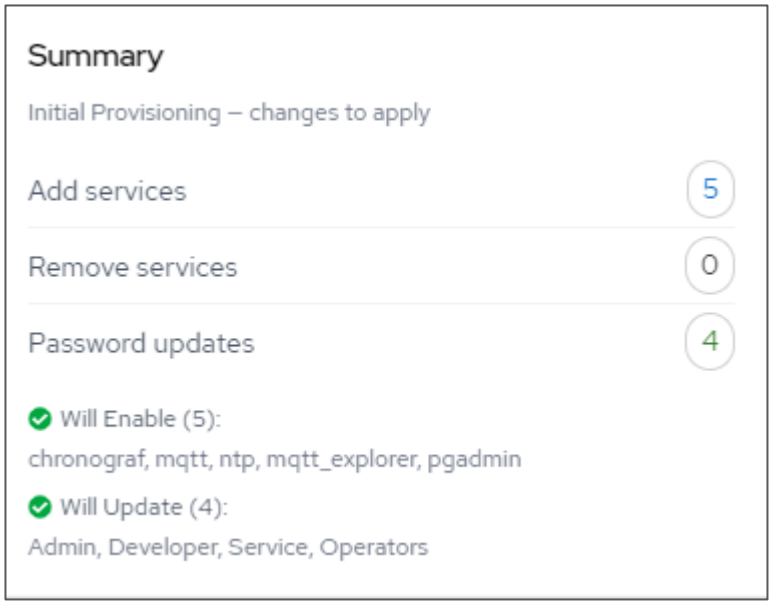
When all passwords have been entered successfully and meet the minimum criteria, the initial configuration will be ready for deployment.

Note: Passwords must be at least 8 characters long, include one uppercase letter, one lowercase letter, one number, and one special character (! or -), and cannot start with a special character.

2.4.5 Device Deployment

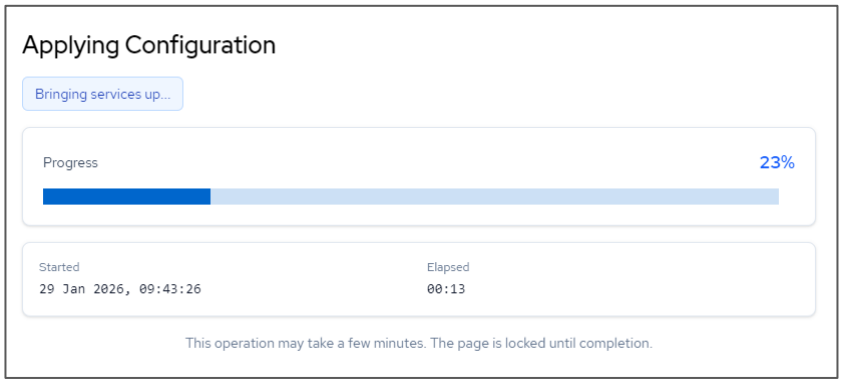
Once the **Services** and **Password** have been successfully entered, the **Configure Device** button will be enabled in the bottom-right corner of the page. The summary card will then display an overview of the configuration that will be deployed to the device.

Figure 8: Device Deployment



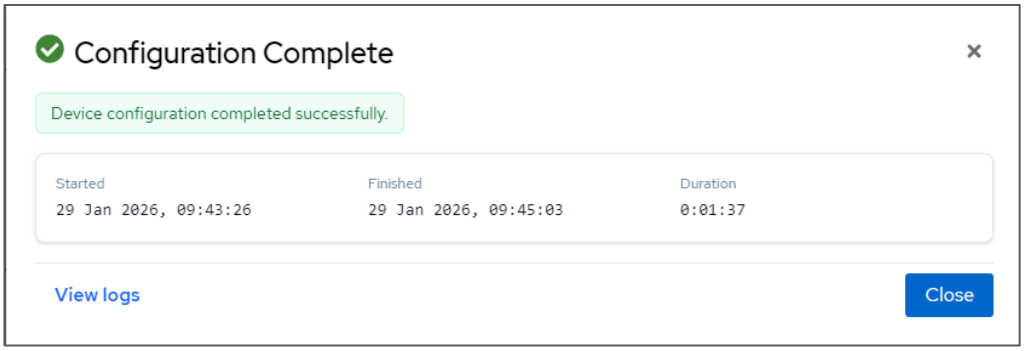
When deployment begins, a pop-up window will inform the user of its progress.

Figure 9: Apply Configuration



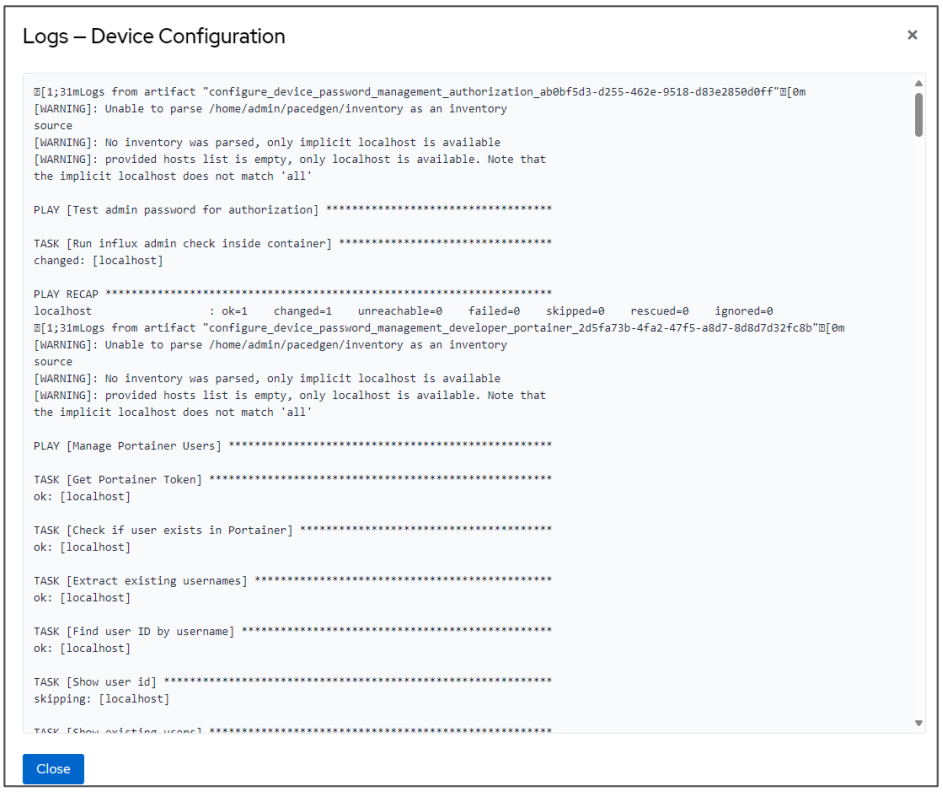
When the process has completed, the pop-up window will change to green.

Figure 10: Configuration Complete



For more details on the deployment process, at the bottom left of the pop-up is a View logs button, which will display more information around the deployment process and may be useful information for diagnostic purposes.

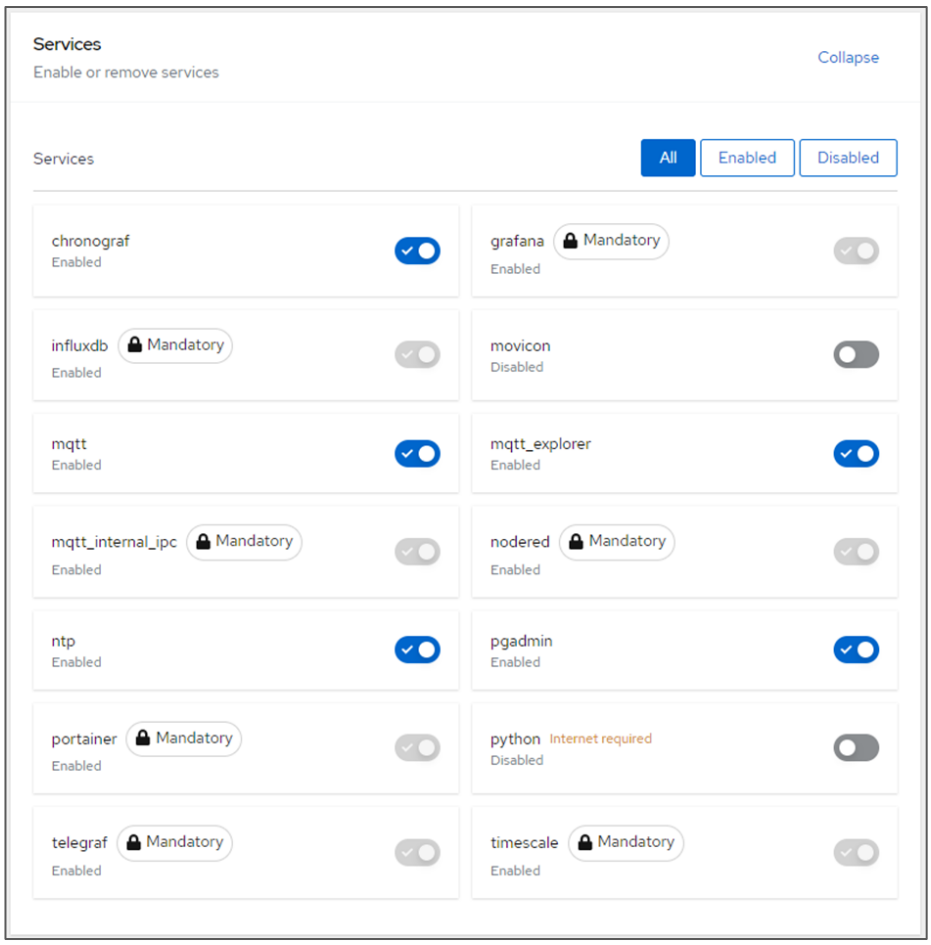
Figure 11: Logs



Deployment Completion

Once the deployment is complete and the deployment pop-up is closed, the user will be returned to the device configuration page. This will now be updated to show additional services that can be deployed or disabled.

Figure 12: Deployment Completion



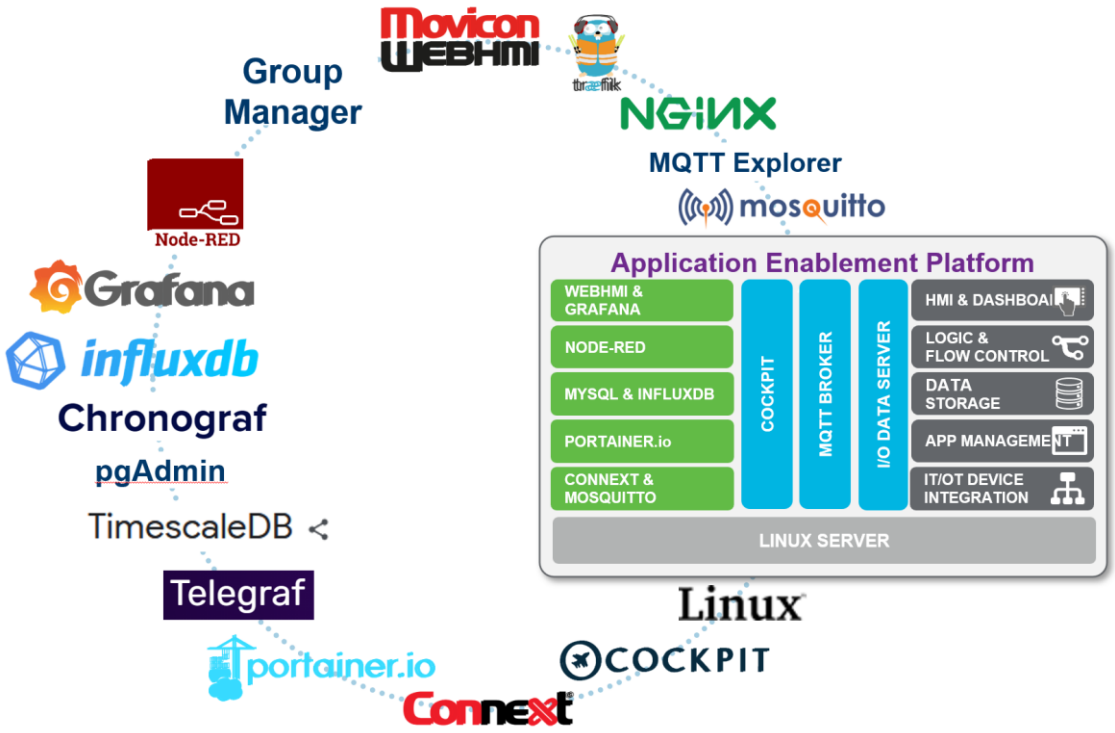
At this point, PACEdge is ready for use. Refer to the available how-to examples for developing applications with Node-RED, Grafana, or Movicon WebHMI/Connext.

Section 3: PACEdge Architecture Details

3.1 PACEdge Services/Applications

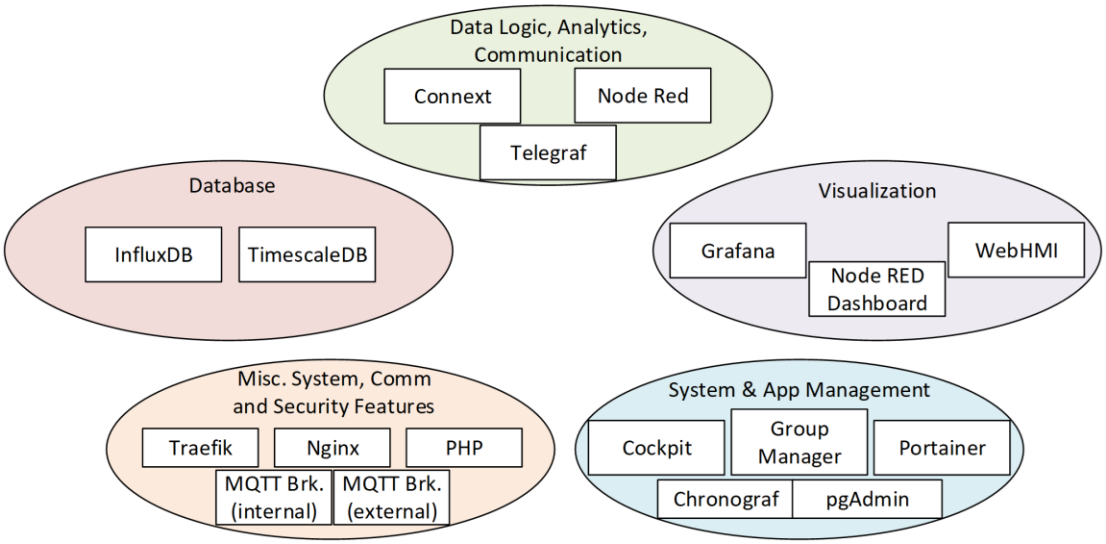
PACEdge entails several communications, data processing, data storage, and visualization applications that run on the Linux operating system. The following diagram gives an overview of the components that make up PACEdge:

Figure 13: Software Overview



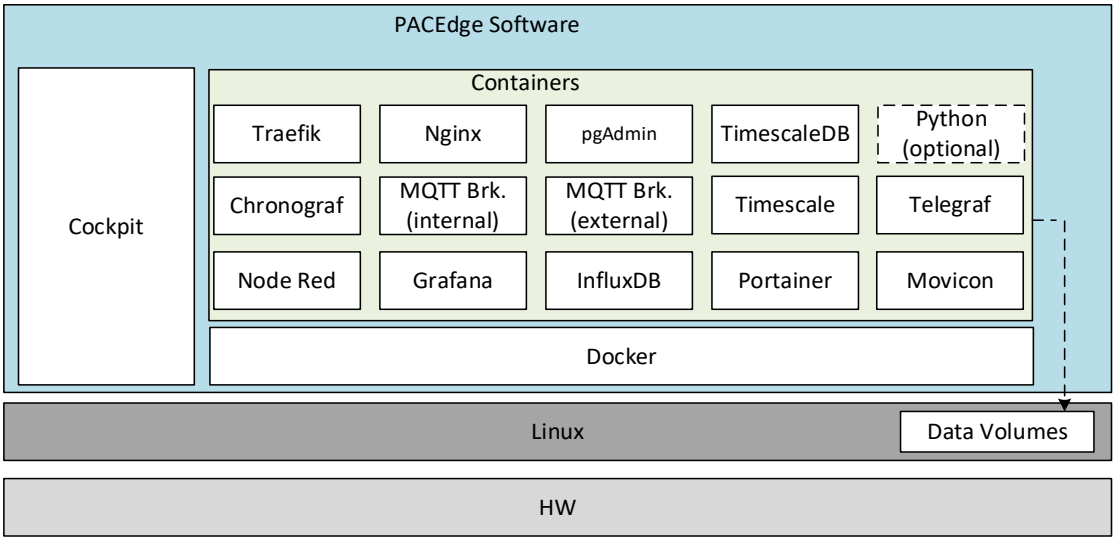
PACEdge tools and applications, based on the function that they perform, can be grouped into functional categories as follows:

Figure 14: PACEdge Application Categories



PACEdge was designed using Docker architecture, in which each application runs in its own Docker container (Figure 15). Since containers are designed to be easily replaceable, they do not retain an internal state between reboots unless specifically designed. With PACEdge, selected containers will map some of their data to data volumes on the host Linux system so that Node-RED, Grafana, and database changes can be saved between Container restarts and updates.

Figure 15: Containerized PACEdge Implementation



3.1.1 Node-RED

Node-RED is the logic engine of the PACEdge. It provides a graphical way to wire together different APIs and services, enabling event-driven logic implementations. Node-RED is well known for its broad adoption in the software community and has many freely available nodes that can be easily installed. PACEdge comes with a large selection of pre-installed nodes, allowing users to easily send and receive data via MQTT, OPC-UA, ModbusTCP, and ModbusRTU interfaces. It also allows users to process and visualize data via the dashboard, store data in InfluxDB and TimescaleDB databases, and send email alerts. Node-Red also has nodes for cloud connectivity.

For more details about Node-RED, please refer to examples later in this document, as well as to *www.nodered.org*

3.1.2 Movicon Components and Tools

Connext and WebHMI

Connext is a data gateway, supporting a large number of field buses and proprietary communication protocols, allowing the reception of data, internally sharing data with other applications, historizing data, and making it available to other software services via an OPC UA Server

To access the Connext OPC UA server from outside the PACEdge device, specify either the hostname. local or the IP address of the PACEdge device, and append the following port number **62841**. The example should look like this:

opc.tcp://pacedge-e3c228.local:**62841** or opc.tcp://192.168.3.100:**62841**

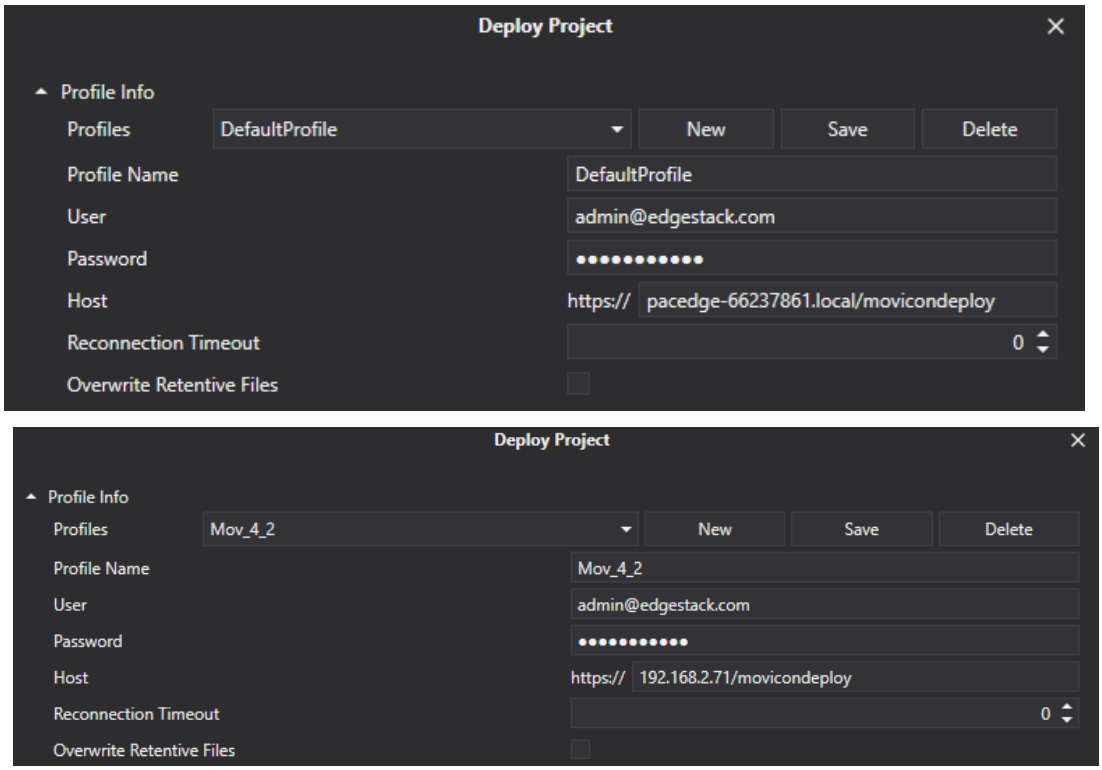
WebHMI, in addition to data gateway functionality, adds HMI visualization capability.

Movicon.NExT Editor

Movicon.NExT software, running typically on Windows computers, is used to develop Connext and WebHMI applications. Once development is done, these applications must be uploaded to an industrial PC running PACEdge. To establish this upload, the following credentials need to be specified in Movicon.NExT:

- User: admin@edgestack.com
- Password: as set by the user
- Host: xx.xx.xx.xx/movicondeploy
  (where xx.xx.xx.xx is either the *hostname*. local or an IP address of the remote industrial PC, such as 192.168.3.100)

Figure 16: List of credentials to deploy the Movicon project



Note: User password is set by using the PACEdge Password Management Utility accessible via Cockpit->Configure Device page.

Accessing Connext OPC UA Server

Connext has an integrated OPC UA Server, which can be used by internal PACEdge applications, such as Node-RED, but also accessed externally by using OPC UA Clients and Browsers.

To access the Connext OPC UA server from outside the PACEdge device, specify either the hostname.local or the IP address of the PACEdge device and append the following port number: **62841**. The example should look like this:

opc.tcp://pacedge-e3c228.local:**62841** or opc.tcp://192.168.3.100:**62841**

Accessing Connext OPC UA Server from Movicon.NExT Browser

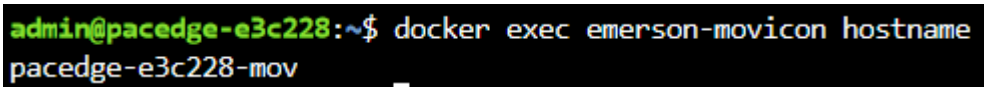
When accessing the Connext OPC UA server on the PACEdge device from Movicon.NExT browser note that Movicon.NExT browser uses the Hostname instead of an IP address. The Movicon.NExT browser will check for a cybersecurity certificate on the target device, which is issued using the Hostname. Therefore, to pass the security check, the Hostname

of the Connext container (not the hostname of the Linux OS), not the IP address, has to be used.

To find out the hostname of the Connext Docker container, please follow the steps below:

1. Open Cockpit, go to the Terminal tab
2. Type command: **docker exec emerson-movicon hostname** and hit enter
3. Copy the hostname shown:

Figure 17: Finding the Hostname with Terminal



Note: Starting with PACEdge v2.2.0, the main Linux and Movicon container hostnames have been changed to be unique**.** As a result, the Movicon hostname is no longer derived from the container ID and cannot be read using the Cockpit Docker tab.

4. If Movicon.NExT Editor runs on a Windows computer; the Hostname must be associated with the PACEdge device IP address. This association is established in the host's file:
   C:\Windows\System32\drivers\etc\hosts
   This file is protected and cannot be edited directly. Use the following procedure:
   a. Copy the host file to the Desktop folder.
   b. Open the host file with Notepad or another editor.
   c. Add a line with the PACEdge IP address, space, and Hostname of the container, such as:

      ```
      192.168.3.100 130d8143d8bd
      ```

   d. Save the file and copy it back to the original location, overwriting the original file.
   e. Restart Windows.

Accessing OPC UA Server via Port Forwarding

Starting with version v2.2, PACEdge implements the OPC UA Port Forwarding feature. The OPC UA Port Forwarding feature enables temporary forwarding of OPC UA traffic from one Ethernet port to another on the PACEdge device. This feature is very handy when using Movicon.NExT editor to browse OPC UA variables on the PLC, which is connected to

PACEdge, but is not directly accessible from the user PC where Movicon is.NExT editor is running. This is the case on CPL410/CPE400 device, where the PLC's OPC UA server is accessible via an internal virtual Ethernet port (VNIC) or in RXi2-BP/IPC6010/7010/8010 systems, where one Ethernet port is used to connect to a PLC and another Ethernet port is used to connect to an engineering PC where Movicon.NExT is running.

The OPC UA Port Forwarding tab has a detailed description of how to initialize and to use this feature.

3.1.3 Grafana

Grafana is a visualization tool that lets users view and analyze data and create alerts. Even though the Node-RED Dashboard already has its own data visualization, Grafana brings extra features and ways to scroll and zoom into specific portions of the graph. Grafana works with several databases, but in PACEdge, it is suggested to use TimescaleDB and InfluxDB.

Within the PACEdge Grafana comes pre-configured to access the following databases:

1. InfluxDB (database: data):
    a. URL: http://emerson-influxdb:8086
    b. HTTP Method: GET
2. InfluxDB (database: telegraf_metrics):
    a. URL: http://emerson-influxdb:8086
    b. HTTP Method: GET
3. TimescaleDB (database: data):
    a. URL: emerson-timescale:5432
    b. TLS/SSL Mode: disabled

For more details about Grafana, please refer to examples later on in this document, as well as to *www.grafana.com*

3.1.4 MQTT

PACEdge implements two MQTT brokers: one is meant to be used for PACEdge internal communication between Docker containers, and the second one for external communication. Node-RED does have MQTT nodes pre-installed. MQTT brokers are implemented using Mosquitto open-source software.

MQTT brokers can be accessed as follows:

1. Internal broker:
    a. Server: emerson-mqtt-internal-ipc
    b. Port: 1883

2. External broker:
    a. Server: emerson-mqtt
    b. Port: 1883
    c. Secured by: username/password

For more details about MQTT, please refer to www.mqtt.org

3.1.5 Jupyter-Python

Jupyter is an open-source interactive computing environment that allows users to create and share documents containing live code, equations, visualizations, and narrative text. When used with Python, it provides a powerful platform for data analysis, machine learning, and scientific computing. Users can run Python scripts interactively, visualize data in real time, and document their workflow in a single environment, making it ideal for experimentation and analysis on PACEdge devices.

Note that since Jupyter/Python is an optional service, its credentials are not being managed by PACEdge Password Management Utility and should be properly set by the user. Default Jupyter password is: edgestack

For more details about Jupyter, please refer to: https://jupyter.org/

3.1.6 Traefik

In PACEdge, Traefik acts as a reverse proxy, allowing access to applications through the path extension and closing most of the ports. This greatly increases the security of the PACEdge.

For more details about Traefik, please refer to docs.traefik.io/

3.1.7 Nginx

NGNIX is being used as the front-end router directing access to Cockpit and to other PACEdge applications.

3.1.8 Telegraf

PACEdge implements Telegraf agent, which is plugin-based and can pull data, statistics, and logs from a variety of databases, underlying system resources (CPU, memory, disc, kernel, software logs, docker containers, etc.), and external devices, heavily focusing on IoT protocols, such as MQTT, AMQP, Cloud resources, etc. For the complete list of available plug-ins, please refer to: https://www.influxdata.com/products/integrations/?_integrations_dropdown=telegraf-plugins

By default, Telegraf is configured to gather system health statistics, listen to a specific MQTT topic on the internal MQTT Broker, and store resulting data in the InfluxDB database.

3.1.9 InfluxDB

InfluxDB is a time-series database. Node-RED has nodes that enable the user to store and query data to and from InfluxDB, and Grafana connects to InfluxDB and retrieves data for visualization. Telegraf uses InfluxDB to historize data it receives via input connectors.

InfluxDB is implemented in a Docker Container and is expected to be managed by either Node-RED or Chronograf applications. Note that InfluxDB direct access from the outside of the PACEdge system is blocked.

Parameters to access InfluxDB:

- Host: emerson-influxdb
- Port: 8086 (internal access only)

For more details about InfluxDB, please refer to *www.influxdata.com*

3.1.10 TimescaleDB

TimescaleDB is a type of PostgreSQL database that is specifically designed for managing time series data and has a user-friendly SQL interface.

TimescaleDB is implemented in a Docker Container and is expected to be managed by either Node-RED or pgAdmin applications

Parameters to access TimescaleDB:

- Host: emerson-timescale
- Port: 5432 (internal access only)

For more information about TimescaleDB, please refer to *https://www.timescale.com/*

3.1.11 Cockpit Description

PACEdge is designed to offer the user a GUI experience. Even though it is based on a Linux operating system, all main system management tasks can be done via GUI, and Cockpit is a tool that makes it happen. Cockpit provides system status and health information, resource (CPU, memory, storage, network) usage, network (IP address) management options, user management options, and different logs for troubleshooting.

Since Cockpit is meant to manage Linux operating system tasks, it runs on Linux as a native application and not in a Docker Container.

For more details about Cockpit, please refer to *www.cockpit-project.org*

3.1.12 Portainer

PACEdge is heavily utilizing Docker's container-based implementation, allowing users to add their own containers. Even though Cockpit already has Docker Container

management features, a dedicated Docker management tool, Portainer, adds additional functions and visualization options. Portainer allows users to monitor, start, and stop containers, check the container log file, configure restart policies, open ports, etc.

For more details about Portainer, please refer to www.portainer.io/

3.1.13 InfluxDB Manager (Chronograf)

Chronograf is a management interface for InfluxDB. With Chronograf, users can search and query data that is stored in InfluxDB, as well as perform database management tasks. Chronograf also offers data visualization capabilities, similar to Grafana.

For more details about Chronograf, please refer to *www.influxdata.com/time-series-platform/chronograf/*

3.1.14 TimescaleDB Manager (pgAdmin)

pgAdmin is a web-based administration and management tool for PostgreSQL databases. It provides a graphical interface that allows users to create, configure, and manage databases, tables, users, and permissions. With pgAdmin, users can execute SQL queries, monitor database activity, and perform backup and restore operations through an intuitive interface.

Note that to log into pgAdmin with admin credentials, a user name: admin@edgestack.com needs to be used

For more details about pgAdmin, please refer to:

https://www.pgadmin.org/

3.1.15 MQTT Explorer

MQTT Explorer is a comprehensive MQTT client designed for visualizing and managing MQTT topics and messages. It allows users to connect to an MQTT broker, subscribe to topics, and monitor message flows in real time. MQTT Explorer provides an intuitive hierarchical view of topics, supports message publishing and editing, and is useful for debugging and testing MQTT-based IoT and industrial applications.

For more details about MQTT Explorer, please refer to:

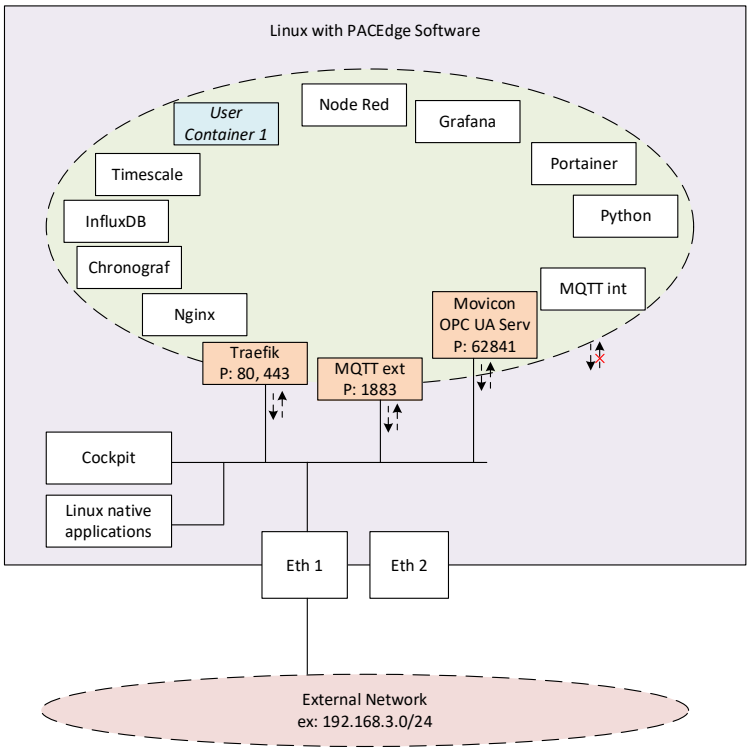
https://mqtt-explorer.com/

3.2 PACEdge Data Communications and Security

Considering that most of the applications in PACEdge are implemented using Docker Containers, the main communication between them is implemented using network interfaces. For security and traffic segregation reasons, PACEdge uses two internal user-defined bridge networks, named CoreNet and GatewayNet. CoreNet is being used for internal container communication without access outside of the system. GatewayNet, on the other hand, also connects Traefik, which allows containers to be accessed from outside of the system. Some services, such as Traefik, an external MQTT broker, and an OPC UA server, have open ports (80, 443, 1883, 62841), enabling these services to be reached from the outside.

External Ethernet ports and IP addresses can be easily managed via Cockpit or other standard Linux tools.

Figure 18: PACEdge Network Communication Paths



3.3 PACEdge System Level Settings

PACEdge is Linux-based software but designed to be user-friendly with a graphical user interface (Cockpit) for all basic configuration tasks. To access Cockpit, open the browser and type in the IP address of PACEdge. This will bring you directly to the Cockpit.

3.3.1 System Configuration Changes via Cockpit

Cockpit supports most system configuration tasks, such as:

- Changing Cockpit/Linux User Password
- Adding /Removing user accounts
- Changing Hostname
- Modifying IP addresses, VLANs, and enabling the firewall
- Managing Storage
- Browsing and moving files between PACEdge and a remote computer
- Monitoring CPU, Memory, Network, Storage usage, and performance
- Analyzing system logs
- Monitoring system services
- Setting up the OPC UA Port Forwarding feature
- Shortcuts to other PACEdge applications
- Linux Terminal (for users who desire further customization)

Changing Host Name

PACEdge supports mDNS/DNS-SD protocols, allowing devices to be discovered on the network using Hostname. By default, PACEdge systems are delivered with Hostname set to **pacedge-xxxxxxxx,** where xxxxxxxx is either an 8-digit serial number of the hardware device or the last 6-digit MAC address.

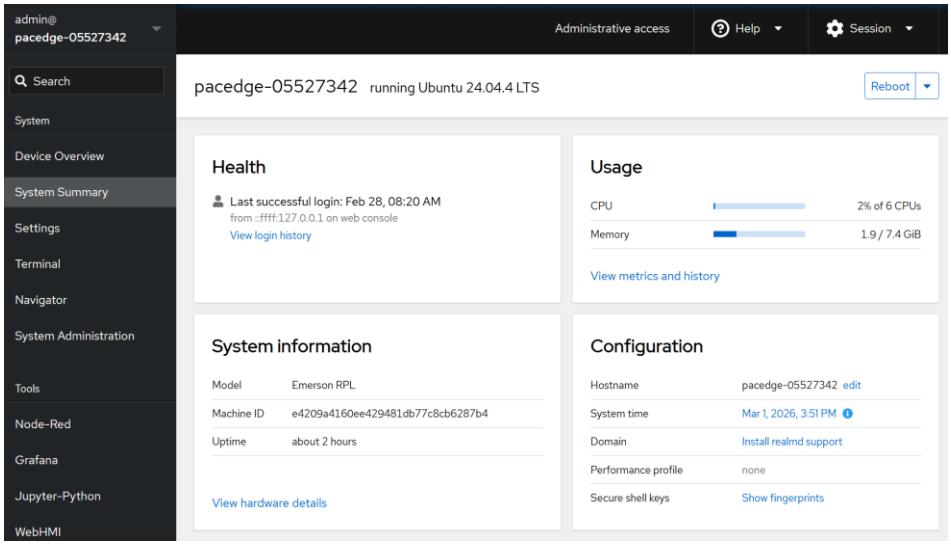
Note: Devices are delivered with a cybersecurity certificate issued using the device's hostname; changing the hostname to some other value will invalidate this certificate. Please refer to the 3.11 PKI and its use in PACEdge for details.

Gracefully Restarting, Shutting Down the System

To gracefully shut down the system, log in to Cockpit and select the desired action in the System Summary tab in the upper-right corner. User needs to have **Administrative**

access when performing a reboot. Note that when selecting an action, there is also an option to select a time delay.

Figure 19: Cockpit Screen



For further Cockpit details and documentation, please consult online resources.

3.3.2 Physical – Logical Ethernet Port Mapping

The Linux Operating system enumerates Ethernet ports in a way that is not obvious, which physical port corresponds to which logic port, as seen in Cockpit. The tables below will provide physical to logical Ethernet port mapping for different HW devices.

Table 1 IPC6010/7010/8010 Physical to Logical Ethernet Port Mapping

Physical Ethernet port (Label on device)	Logical Ethernet Port (seen in Cockpit)
Port 1	enp98s0
Port 2	enp89s0
Port 3	enp90s0
Port 4	enp91s0
Port 5	enp92s0

Table 2 RXi2-BP Physical to Logical Ethernet Port Mapping

Physical Ethernet port (Label on device)	Logical Ethernet Port (seen in Cockpit)
ETH 0	enp1s0f0
ETH 1	enp10s0
ETH 2	enp2s0
ETH 3	enp7s0

Table 3 IPC 2010 Physical to Logical Ethernet Port Mapping

Physical Ethernet port (Label on device)	Logical Ethernet Port (seen in Cockpit)
Port 1	eth1
Port 2	eth0

Table 4 CPL410/CPE400 Physical to Logical Ethernet Port Mapping

Physical Ethernet port (Label on device)	Logical Ethernet Port (seen in Cockpit)
ETH	enp1s0

3.4 PACEdge Users, Rights, and Passwords

In PACEdge, user roles and their associated passwords fall into two distinct groups:

- Linux/Cockpit users and passwords
- PACEdge Application users and passwords (Password Management Utility, Node-RED, Grafana, Portainer, InfluxDB, Timescale, Chronograf, pgAdmin, MQTT Explorer)

These two groups are separate. Passwords must be managed independently for each group.

It is strongly recommended that different passwords be used for Linux/Cockpit accounts and PACEdge application accounts—particularly for the admin role. Although an admin account exists in both groups, the accounts serve different purposes and do not share credentials. One admin account manages the host Linux operating system, while the other manages PACEdge system functions.

Each PACEdge application is initially configured with default credentials and includes its own user and credential management interface.

During initial device configuration, the Password Management Utility changes all default passwords. This centralized process eliminates the need for users to log in to each application and manually update credentials through separate interfaces. Password updates are handled in one place, ensuring consistent and secure configuration across the entire PACEdge system.

All default passwords must be changed at first login. Emerson strongly recommends using long (10 characters or more), complex passwords for all accounts requiring authentication. The PACEdge password management system enforces strong password requirements as part of its security design.

Guidance on password complexity and password management best practices is available in NIST Special Publication 800-63-3: Digital Identity Guidelines:

https://pages.nist.gov/800-63-3/sp800-63b.html

Table 5: Default Passwords

Functionality	Authenticated Subjects (user)	Default Passwords
SSH remote login	admin	Default password: “edgestack”
Cockpit/Linux	admin	Default password: “edgestack”
Chronograf	admin	Default password: “edgestack”
Grafana	admin	Default password: “edgestack”
Node-RED	admin	Default password: “edgestack”
Portainer	admin	Default password: “edgestack”
InfluxDB	admin	Default password: “edgestack”
TimescaleDB	admin	Default password: “edgestack”
pgAdmin	admin@edgestack.com	Default password: “edgestack”
MQTT Explorer	admin	Default password: “edgestack”
Connext/WebHMI	admin@edgestack.com	Default password: "Edgestack123!"
Jupyter		Default password: “edgestack” **

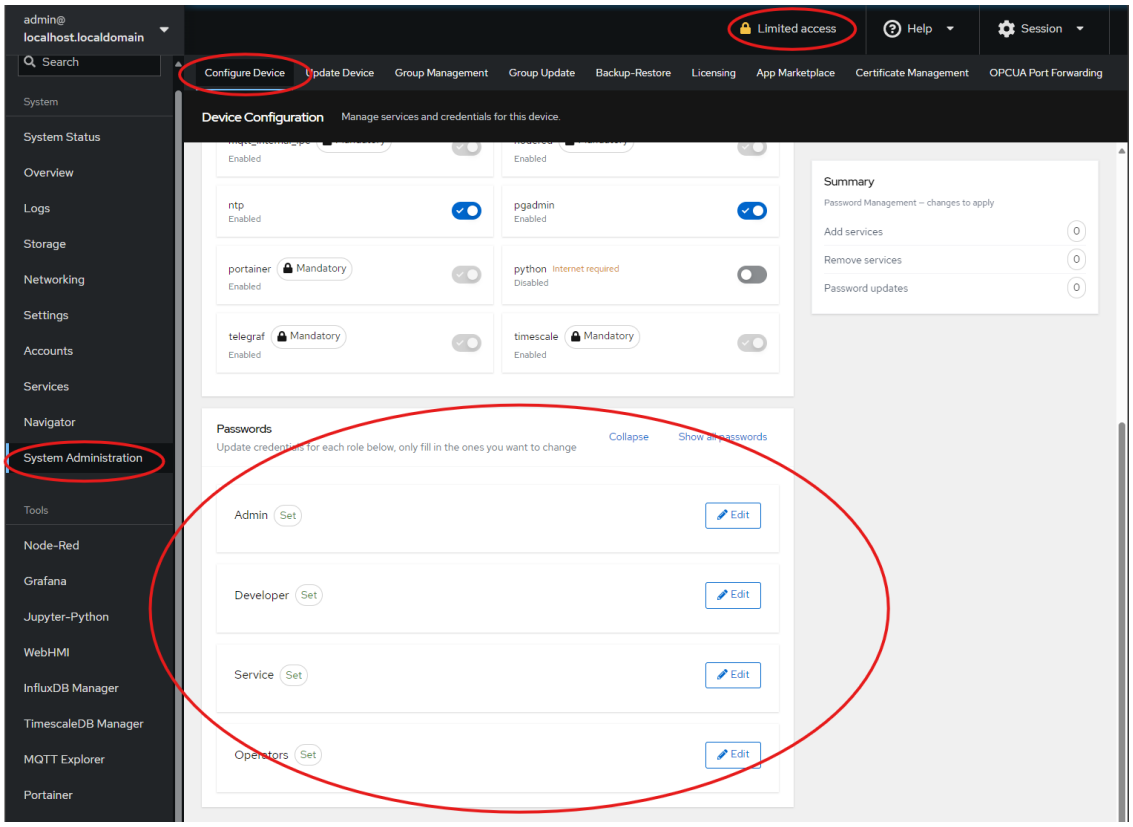
** Note: Since Jupyter/Python is an optional service, its password is not being controlled by the PACEdge Password Management Utility. If the user chooses to enable Jupyter, its password needs to be changed manually in the Docker Compose file. For details, please contact Emerson tech support.

3.4.1 Password Management System

To enhance PACEdge security, a centralized Password Management System is provided. It includes pre-configured user roles with defined access rights and associated passwords. The Password Management Utility enables administrators to manage user role passwords across all PACEdge applications from a single interface.

This utility is accessible via **Cockpit → System Administration → Configure Devices**. Only users with the admin role are permitted to update passwords for other user roles.

Figure 20: Password Management



Important

It is highly recommended to change passwords by using the provided automated utility instead of manually going into a specific application (such as Node-Red) and changing the password there. If passwords between different applications get out of sync, the password management utility will fail.

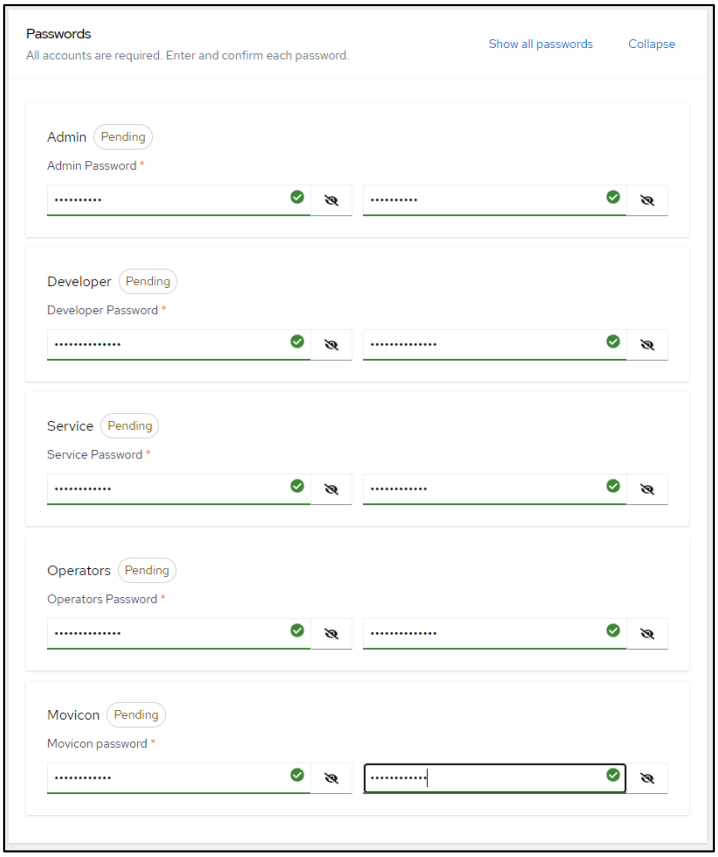
3.4.2 Changing Passwords via Automated Password Management Utility

The Password Management utility will automatically set passwords for all PACEdge applications and each user role.

Note: When logging into the TimescaleDB Manager service (pgAdmin), the user name needs to be entered as **admin@edgestack.com**.

To change PACEdge Application passwords, please click on each field and enter the new password meeting the minimum criteria, and then click on the **Submit** button at the bottom of this table. Notice that the **Submit** button will be greyed out and inactive if some of the passwords are incorrect.
Conditions are not met.

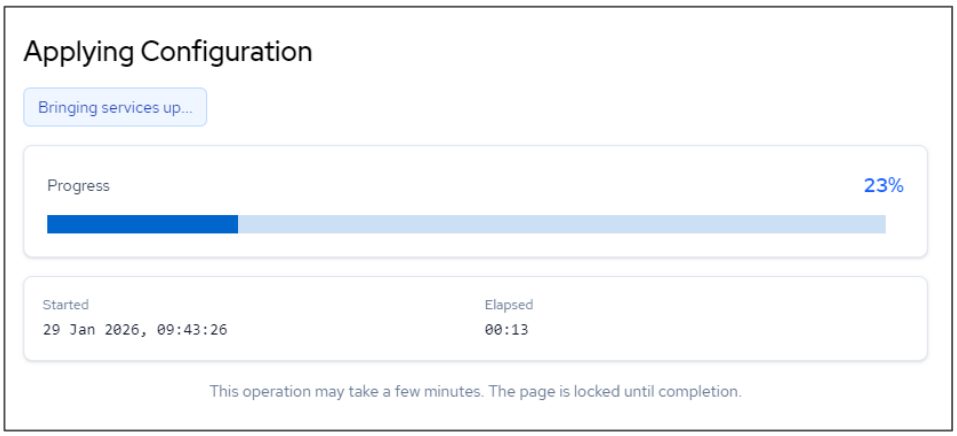
Figure 21: PACEdge Application Password

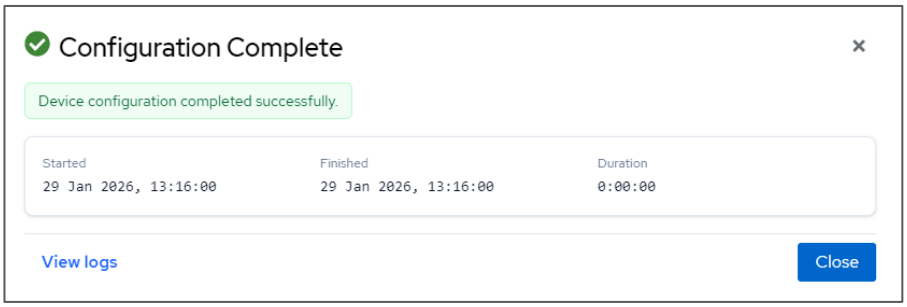


Note: The user may choose to change only a subset of passwords in the future; however, during the initial setup, **all passwords must be set.** This step also initializes roles in databases and supporting utilities.

Once the **Submit** button is clicked, the progress pop-up appears. When the process finishes, the pop-up updates to **Configuration Complete**.

Figure 22: Applying Configuration





If an error occurs while changing passwords, check the following:

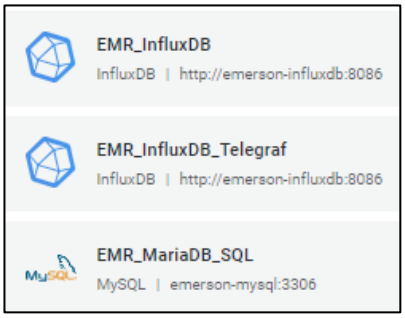
- **Incorrect admin password:** The current admin password may have been entered incorrectly. Password Management Utility requires **PACEdge Applications admin password**, not the Linux/Cockpit admin password.
- **Mismatched application passwords:** The admin password in one PACEdge application (for example, Grafana, Portainer, InfluxDB, or TimescaleDB) may differ from the others. This can occur if the password was changed directly within an application instead of using the PACEdge Password Management Utility. In this case, manually reset the password in the affected application so that it matches the others, then use the PACEdge Password Management Utility to apply the new password consistently across all applications.

Note: The Password Management Utility updates passwords for each user role across all PACEdge applications. However:

- In Node-RED, any flow that connects to InfluxDB or TimescaleDB requires manual password updates within the corresponding nodes.

- In Grafana, the utility automatically updates credentials for the three default PACEdge databases (see Figure 12). Any additional user-configured databases must be updated manually.

Figure 23: PACEdge default databases pre-configured in Grafana



3.4.3 Changing Cockpit/Linux User Passwords

When accessing PACEdge for the first time, the system prompts the user to change the default admin user password for the Linux/Cockpit environment.

Note: The automated Password Management utility described in the previous chapter does **not** change Cockpit/Linux user passwords.

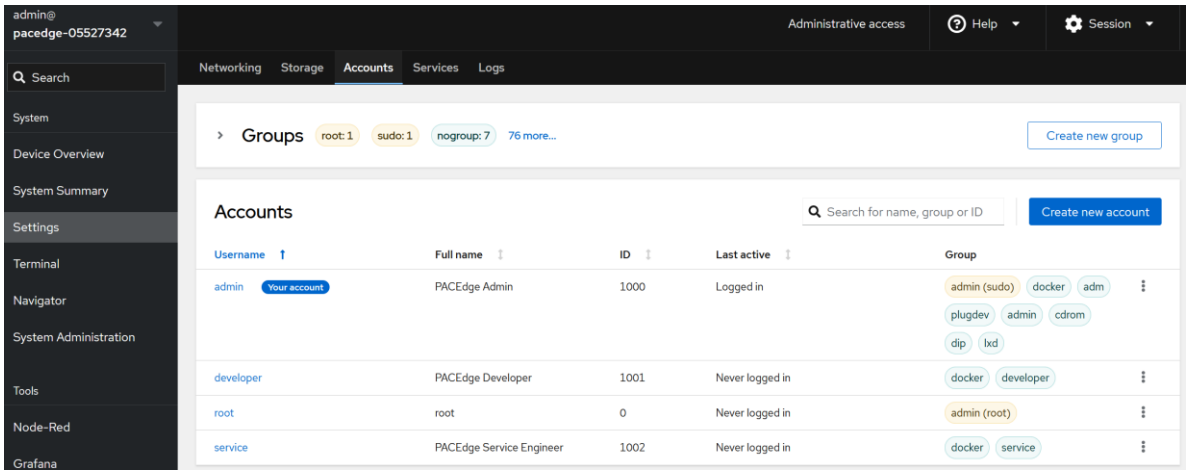
After changing the **admin** password, log out and log in to Cockpit again so that changes can take effect and the admin privileges are granted. The user can do this by accessing a drop-down menu in the screen's upper-right corner.

Once logged in as admin, the user may set passwords for the **developer**, **service**, and **operators** roles. By default, user roles other than **admin** are disabled and will remain disabled until the password is set. Therefore, if additional user roles in Linux/Cockpit are not required, it is more secure to keep them disabled and not assign any password.

The easiest way to manage the Cockpit/Linux user passwords is to click on **Settings** and select the **Accounts** tab in Cockpit.

Note: Administrative access rights (displayed in the upper-right corner) are required to set or modify user passwords.

Figure 24: Accounts Tab



⚠ CAUTION

Do not set any password for the **root** user, as this would enable the **root** account and create a cybersecurity vulnerability.

3.5 PACEdge License File

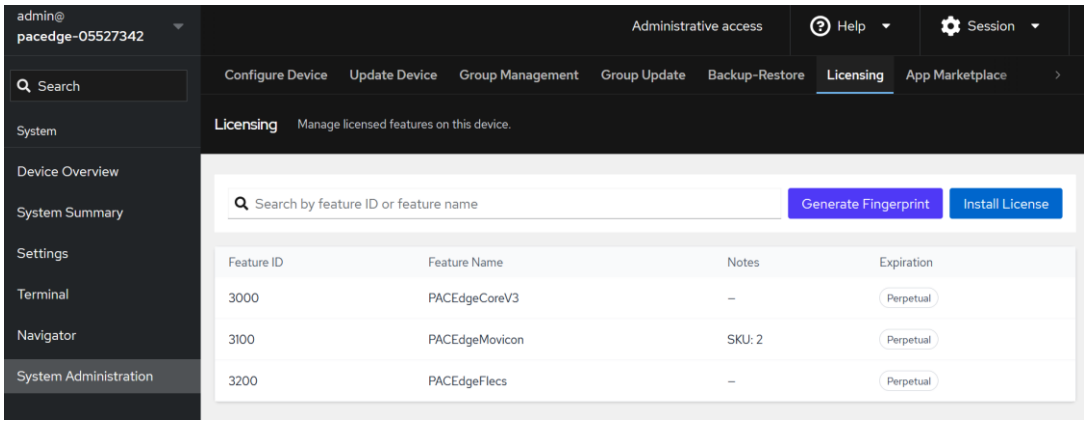
PACEdge is protected by the license file, which is locked to the physical device that PACEdge is running on. With PACEdge v3.0.0, the licensing mechanism has changed, and new licenses will have to be issued to each device when upgrading from older PACEdge versions. PACEdge license controls both what software package is enabled (PACEdge only, with Connext, with WebHMI) and also if the Group Manager feature for a certain number of managed devices is enabled. PACEdge devices will come with software and a valid license pre-installed from the factory. However, if performing a backup restore or restore to the factory default, as described in **Section 5:PACEdge Software Backup/Restore/Recovery** A license will have to be manually installed.

Note: after the backup restore, an extra step is required prior to generating a hardware fingerprint. Otherwise, an error will be returned when trying to install a newly generated license file. Follow the backup restore procedure for your hardware as documented in the: Section 5: PACEdge Software Backup/Restore/Recovery

To provision the new license, follow the steps below:

1. Generate a hardware fingerprint file by going to: Cockpit->System Administration-> Licensing. Click on **Generate Fingerprint** and save the fingerprint file locally on your computer.

Figure 25: Generate Fingerprint



2. Send the hardware the fingerprint file (file with extension .c2v) and the device's serial number to Emerson's technical support team. In return, you will receive a license file (file with extension .v2cp).
3. Click on **Install License** and, via file browser dialog, point to the license file you received.
4. If the license activation is successful, you will see a list of features.

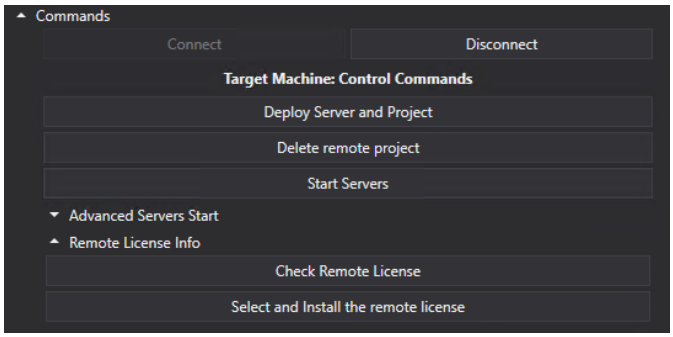
3.5.1 Licensed Connext and WebHMI Features

PACEdge license file enables certain Movicon features, such as Connext or WebHMI. To verify what Movicon features are enabled, please connect to the unit running PACEdge from your workstation where Movicon is installed. NExT software is installed and does the following:

1. Follow the steps described in *Section 3.1.2, Movicon Components and Tools* to establish a connection to PACEdge using the Deploy Project window

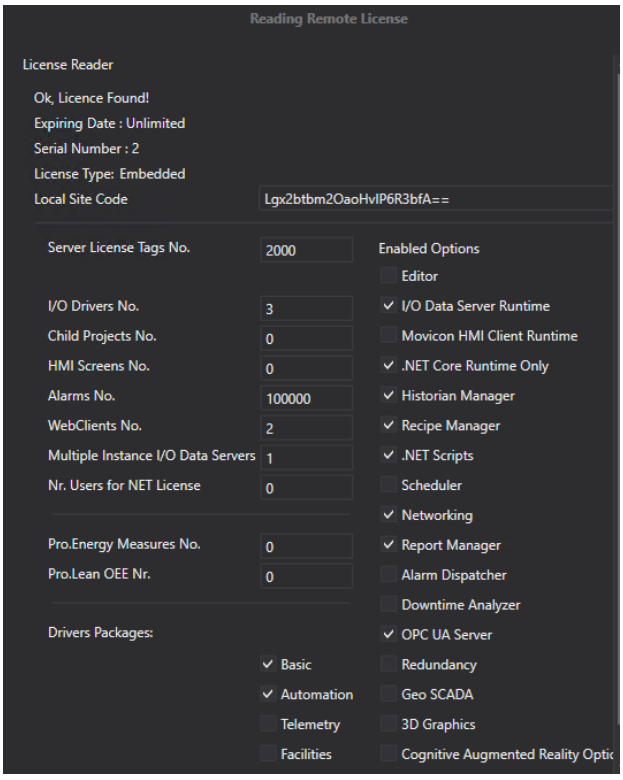
Go to the Remote License Info section and click on Check Remote License:

Figure 26: Connext and WebHMI License Check Dialog



2. The picture below shows the enabled features for the Connext SKU:

Figure 27: License Enabled Features in Connext SKU



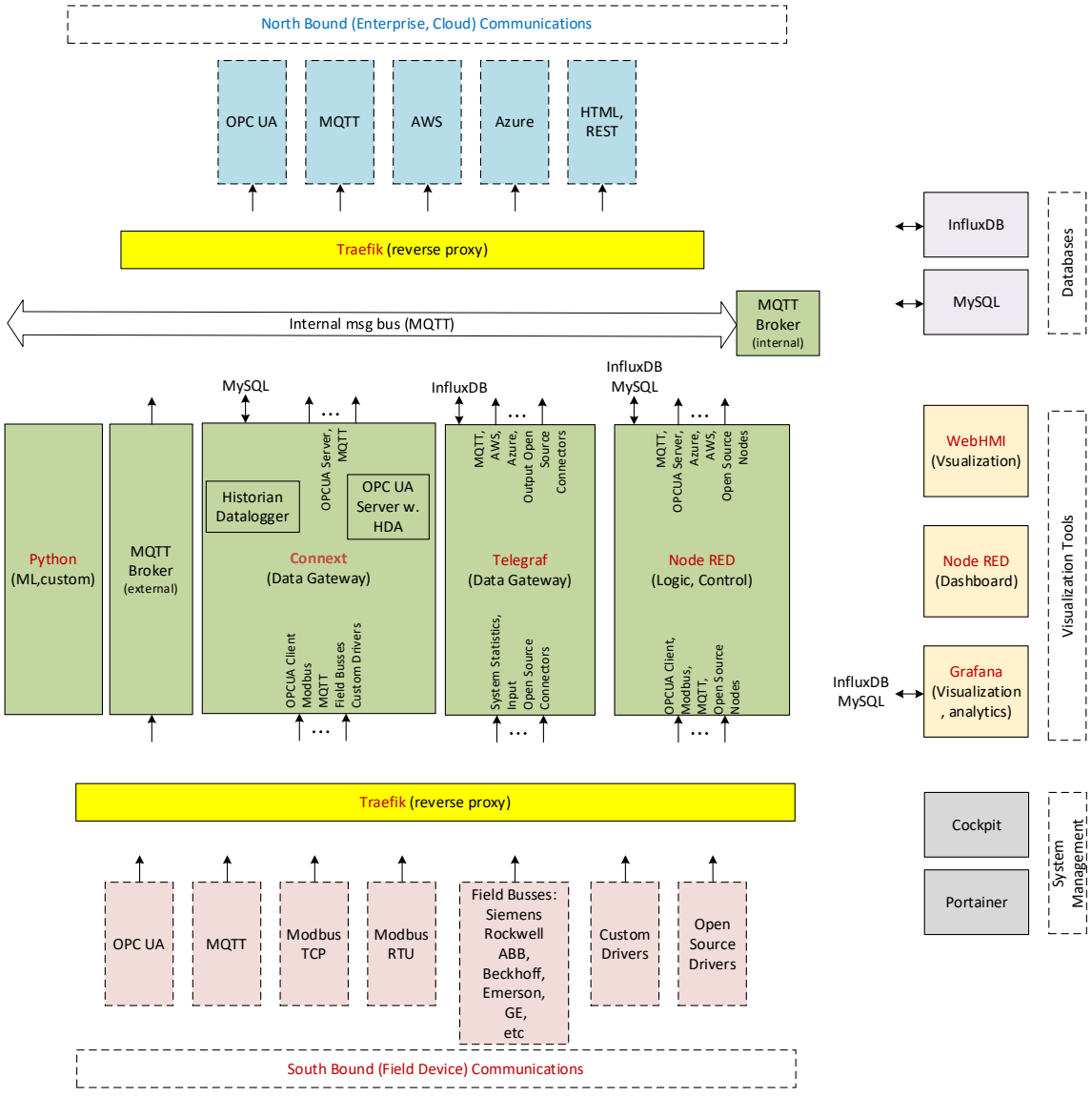
3.5.2 Licensed Group Manager Features

The Group Manager feature can be licensed for a specific number of PACEdge devices that can be managed. How many devices can be managed is indicated in the Licensing tab. For more information, please refer to *Section 3.9, Software Updates.*

3.6 PACEdge Data Communication Recommendations

In Edge applications, it is common to define data flow as “Southbound” (from field devices, sensors, and PLCs to the gateway) and “Northbound” (from the gateway to SCADA, Enterprise applications, and cloud applications). PACEdge implementation is ideally suited for such data flow scenarios. The following diagram shows different components and their communication capabilities:

Figure 28: PACEdge Communication Capabilities



3.6.1 Southbound Communication Capabilities

To communicate with different field devices, aka Southbound communication, PACEdge has the following capabilities:

Connext I/O Drivers

Connext data gateway component implements the so-called I/O Driver infrastructure, which is designed to communicate with many different field devices, supporting open as well as proprietary communication protocols, such as MQTT, OPC UA Client, Modbus, IEC 60870-5-104, IEC 61850 MMS, Siemens, Beckhoff, GE, Hilscher, Mitsubishi, Omron, Phoenix, and many more. For the complete list, please refer to: https://www.progea.com/i-o-driver-list-movicon-next/?lang=en. Furthermore, the I/O Driver infrastructure was designed to add new and custom drivers supporting efficient customization. Data that the driver is receiving is internally stored in the form of a data tag, which can be historized in MySQL, sent out via another driver (such as MQTT), or made available via the OPC UA Server.

Node-RED Nodes

Node-RED has a large open-source community developing and constantly adding new communication nodes. Node-RED supports OPC UA clients and servers, MQTT, Modbus TCP, Modbus RTU, as well as a large number of proprietary protocols from Siemens, Rockwell, Beckhoff, and others. Once data is received by Node-RED, it can easily be processed, stored in MySQL or InfluxDB databases, and sent out via another interface.

Telegraf

PACEdge implements Telegraf agent, which is a plugin-based utility and can pull data, statistics, and logs from a variety of databases, underlying system resources (CPU, memory, disc, kernel, software logs, docker containers, etc.), and external devices, heavily focusing on IoT protocols, such as MQTT, AMQP, Cloud resources, etc. For the complete list of available plug-ins, please refer to: https://www.influxdata.com/products/integrations/?_integrations_dropdown=telegraf-plugins

Custom Driver

Given the open nature of PACEdge, users can also add their existing communication drivers, for example, written in Python, that run in a separate customer-specific Python Docker container.

3.6.2 North Bound Communication Capabilities

To communicate with upper software layers, such as SCADA, enterprise systems, and Cloud, aka Northbound communication, PACEdge has the following capabilities:

OPC UA Server

PACEdge has different options to set up an OPC UA Server and make data available to other applications and systems.

Connext comes with an integrated high-performance OPC UA Server and is a recommended option. All data tags within the Connext environment are automatically published via the OPC UA Server, which can be accessed at the address: opc.tcp://xx.xx.xx.xx:62841, where xx.xx.xx.xx is the IP address of the IPC.

Alternatively, Node-RED comes with pre-installed OPC UA Nodes, which include OPC UA servers.

MQTT

PACEdge comes with an MQTT Broker, which can be accessed outside the host IPC. The MQTT Broker used is based on the Mosquitto open-source implementation and supports Sparkplug B specification and security and encryption features. For access details, please refer to Section **3.1.4 MQTT**

Cloud Connectivity

Cloud connectivity can be established using Node-RED nodes, which readily support AWS, Azure, and other Cloud providers.

Another option is to use Telegraf plug-ins.

Yet another option is to use a custom Docker container and install cloud agents or Python libraries.

3.6.3 PACEdge Internal Communications and Data Flow

PACEdge can be seen as a Swiss army knife when solving a particular problem. Typically, there is more than one solution and implementation option. It is recommended that the user first understand what tools and options are available and then select the most appropriate implementation to solve a particular problem.

MQTT – Internal Communication Bus

PACEdge has two MQTT Brokers, one of which is dedicated to internal communication only and not accessible from outside. MQTT protocol using an Internal MQTT Broker is a recommended internal data bus within the PACEdge. MQTT is fast, simple to set up, and has low overhead, saving CPU resources. Most agents and applications within PACEdge,

such as Connext, Node-RED, Telegraf, and Python, readily support MQTT communication. For example, data received by one of the Connext drivers can be automatically published via MQTT, and Node-RED can subscribe to it. Alternatively, Node-RED can publish MQTT data, and Connext can receive it via the MQTT driver. Telegraf can also publish received data via MQTT, such as CPU utilization statistics. Starting with PACEdge v2.2.0, Telegraf is configured by default to subscribe to the Internal MQTT broker, topics starting with emr_v1/..., parse received data, and store it in InfluxDB. This setup can store Connext data in InfluxDB by publishing it to the MQTT internal broker with the appropriate topic.

OPC UA – Alternative for Internal Communication

OPC UA can also be used for internal data communication as an alternative to MQTT. For instance, Connext has an OPC UA server, and all data variables that Connext receives are published via the OPC UA Server. Consequently, Node-RED can use the OPC UA Client and get data from Connext. Compared with MQTT, note that the OPC UA protocol is significantly heavier on CPU resources and more complicated to set up.

Sharing data via Databases

For not-so-real-time-critical data sharing, an excellent way to consider is storing data in the database and letting other applications extract data directly from it. For example, Connext has a Historian and a datalogger functionality, which can keep the data in a Timescale database. Consequently, Node-RED or Grafana can directly access the data in Timescale and perform further processing or offer visualization.

3.7 PACEdge Remote Access

PACEdge is designed to operate within the internal networks, protected by firewalls and other cybersecurity devices, the so-called on-premise use model. Nevertheless, there are use cases where remote access to the PACEdge system is required.

The following subjects are a few remote access options that have been tested to work well with PACEdge.

3.7.1 Remote Access using ZeroTier

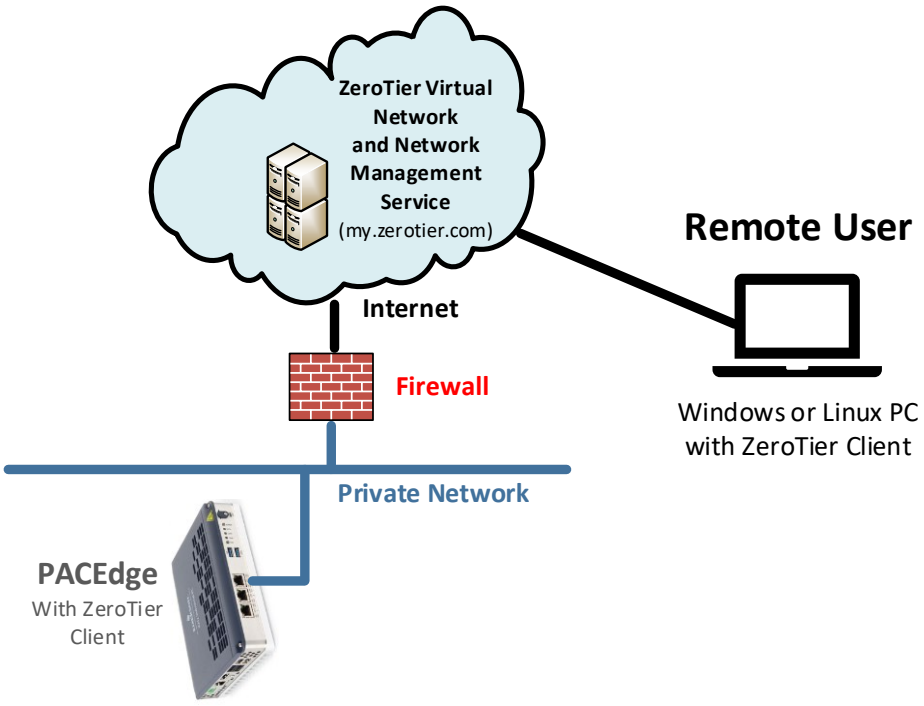
ZeroTier is a commercial service offering allowing the user to create a virtual network that spans different physical sites and devices behind NAT and firewalls. This can connect a user's PC to one or more remote PACEdge devices as if plugged into the same local physical network.

Although ZeroTier is a commercial offering, the Basic version, limited to 25 nodes, is free of charge and is well-suited for testing.

To set up ZeroTier, the following steps need to be executed:

1. Create a ZeroTier account.
2. Download and install ZeroTier onto your PC.
3. ZeroTier is already pre-installed on PACEdge version 2.2 or later devices, but deactivated by default.
4. Configure devices to join the same virtual network.

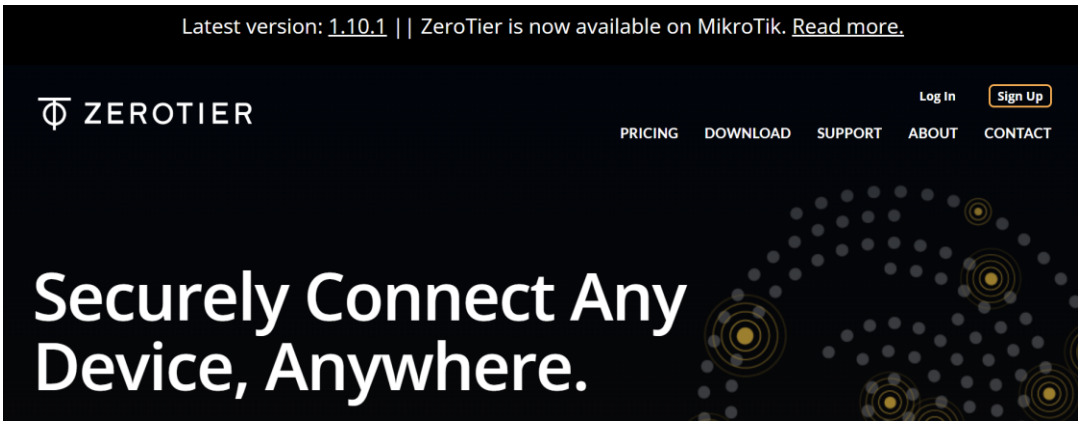
Figure 29 Remote Access using ZeroTier Software



3.7.2 Create ZeroTier account

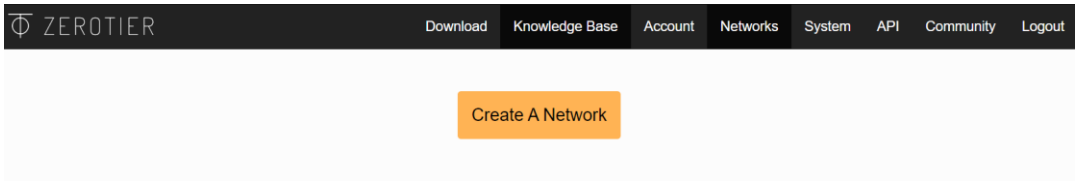
1. Using a browser on your PC, go to www.zerotier.com and click on **Sign Up.**

Figure 30: ZeroTier Account



2. Once signed up, go to my.zerotier.com and log in.
3. Click on the **Create a Network** button.

Figure 31: Create a Network



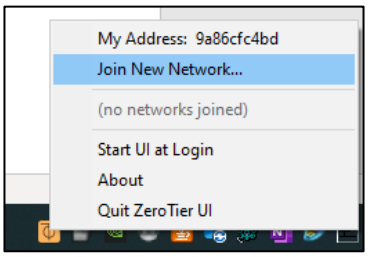
4. If you want to edit the network name or other properties, click on the newly created network.
5. Copy the **Network ID** and keep it handy for the next steps.

Figure 32: Network ID

Install ZeroTier on PC

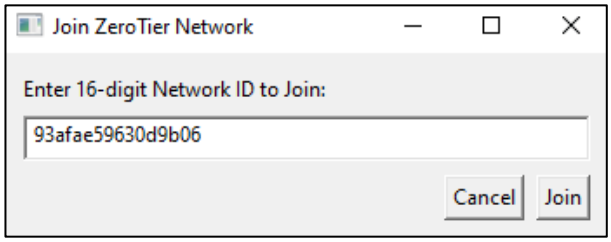
1. Go to www.zerotier.com/download/, select your operating system, download, and install ZeroTier.
2. Launch ZeroTier on your PC.
   Note: The ZeroTier service might appear as one of the icons in the lower-right corner of Windows. In such a case, right-click on the ZeroTier icon and select **Join New Network**.

Figure 33: Join New Network



3. Enter the **Network ID** that was copied in the previous steps and click on **Join.**

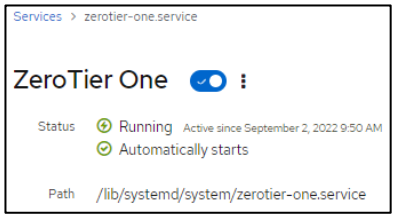
Figure 34: Enter Network ID



Configure PACEdge Device to Join ZeroTier Network

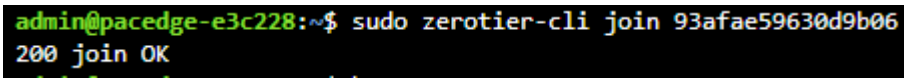
1. By default, the ZeroTier service is installed in PACEdge but is disabled. To enable it, go to Cockpit, Services tab, scroll down to the zerotier-one service, and click on it.
2. Click on the button to **Start and Enable**. The controller will turn blue, and the status will show Running.

Figure 35: ZeroTier Enabled Toggle



3. Copy **Network ID**, steps above, go to Cockpit, Terminal, and type the following:
   sudo zerotier-CLI join ***Network_ID***
   Where **Network_ID** is a 16-digit number from the steps above, enter the password if requested. The result will be: **join OK.**

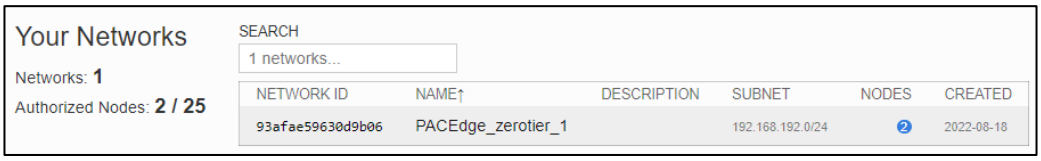
Figure 36: Join OK



Configure and Start Virtual Network

1. Log in to your account on the my.zerotier.com site.
2. Click on the network.

Figure 37: Click on Network



3. Scroll down to where both devices (your PC and PACEdge) are listed with the option to authenticate access to the network.

Figure 38: Locate Devices

4. Check **Auth?** Box for each device or optionally assign a specific IP address for each device. **Last Seen** status will be showing: **ONLINE**

Accessing PACEdge Remotely

1. From your PC, open a browser and type in the IP address assigned in the step above. In this particular example, it would be: **192.168.192.10**
2. The PACEdge landing page will open with access to all PACEdge applications and Cockpit.

3.7.3 Remote Access using OpenVPN

Starting with version 2.2.0, PACEdge comes with pre-installed OpenVPN software. OpenVPN software can be used to create secure point-to-point connections. PACEdge can be configured to act as both an OpenVPN Server and a Client. If desired, the user can use the OpenVPN service, but it must be properly configured and started.
Note: if configured as Server, a network port in the router/firewall will need to be opened so that the external Client can reach PACEdge and establish a secure tunnel.

For OpenVPN configuration and use details, please consult the following:

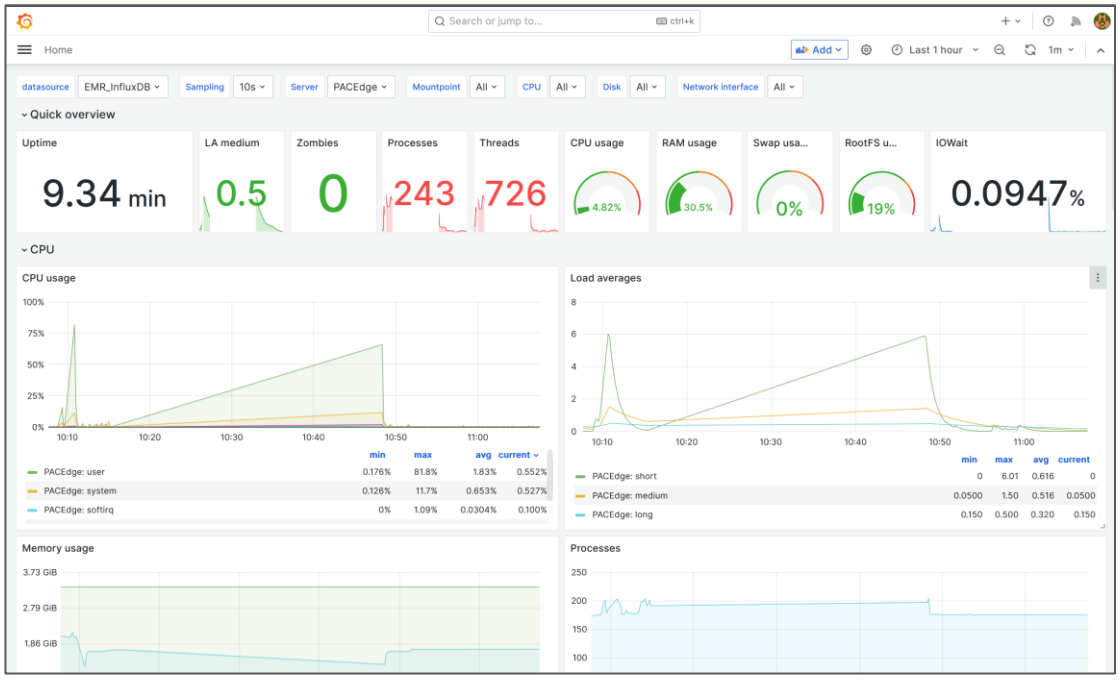
- github.com/OpenVPN/openvpn
- openvpn.net (commercial offering based on OpenVPN)

3.8 PACEdge Hardware and Software Utilization and Statistics

PACEdge is configured by default to collect system statistics, such as CPU utilization, memory usage, storage, network, and kernel activities. This data is stored in the InfluxDB

database. Grafana has a pre-configured dashboard that allows users to view and analyze these statistics. By default, InfluxDB is configured to have a 7-day data retention period.

Figure 39: HW and SW Utilization and Statistics



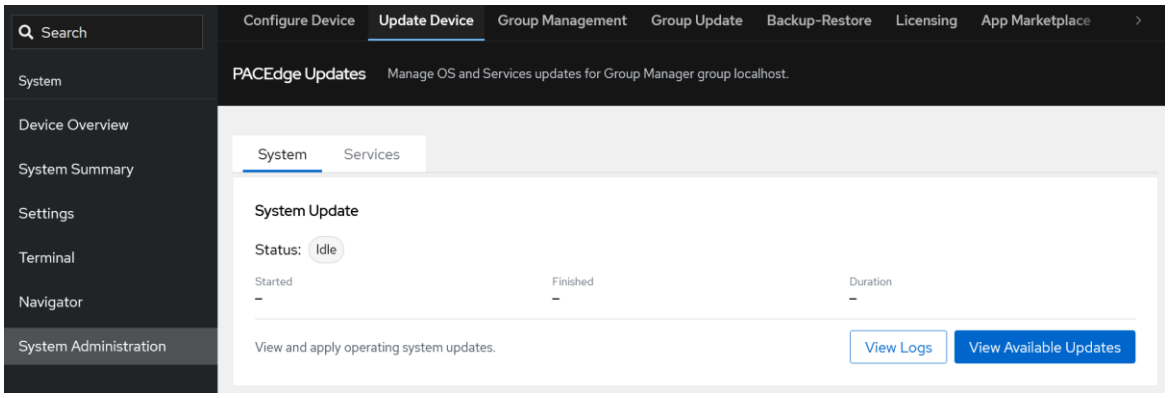
3.9 Software Updates

PACEdge software updates are split into two groups: **PACEdge system updates**, which include host Linux OS updates, and **service updates**, which apply to containerized services. Software updates can be performed in a few different ways:

- **Internet-connected systems**: Updates can be downloaded automatically from the Emerson Marketplace.
- **Air-gapped systems**: Updates can be installed via Navigator or a USB drive.
- **Group-managed devices**: Updates can be performed via Group Manager. In this case, target devices do not have to have Internet connectivity, but they must be connected to the Group Manager. For the instructions and details, consult: *Section 3.10 Group Manager*

To perform software updates, navigate to *Cockpit-> System Administration-> Update Device page:*

Figure 40: Device Software Update Page



3.9.1 Performing System Software Updates

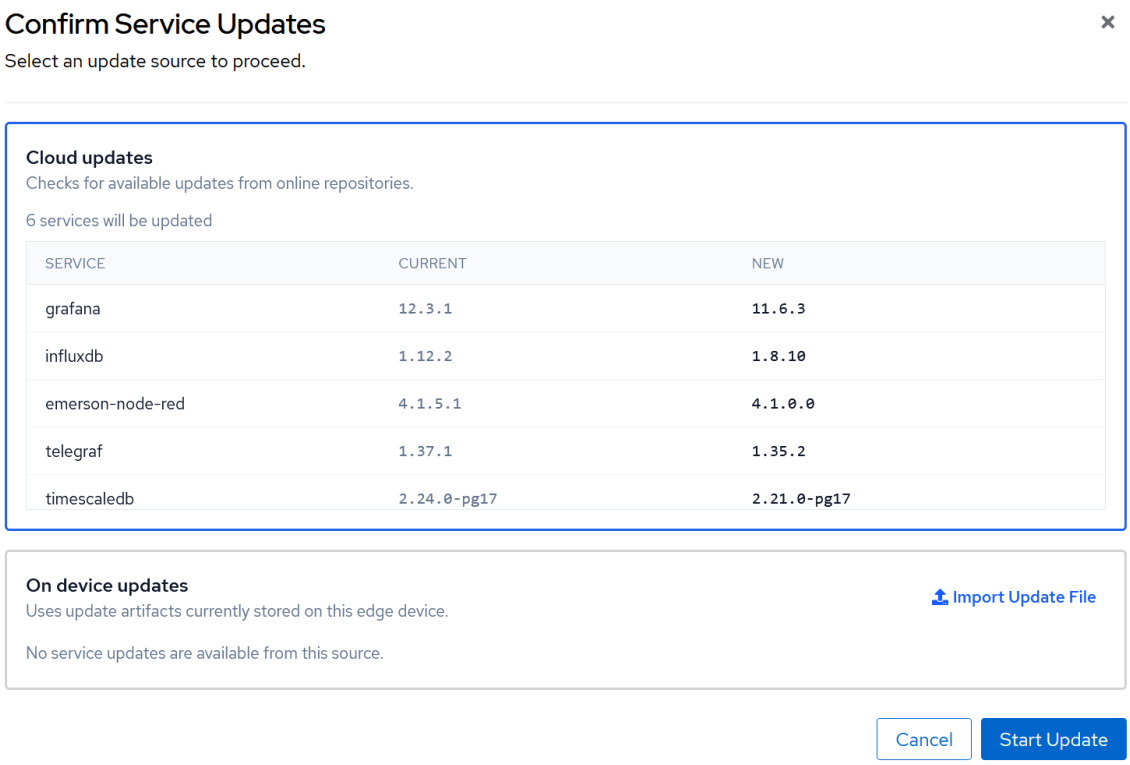
To perform a system update (PACEdge and host Linux OS), click on the **System** tab and then on the **View Available Updates** button. The system will check the online Marketplace for the latest software versions and will display both the current and new versions. Click on the **Start Update** button to proceed to the new version.

Figure 41: Dialog Showing System Software Upgrade Option

3.9.2 Performing Services Software Updates

To perform a service (containers) update, click on the **Services** tab and then on the **View Available Updates** button. The system will check the online Marketplace for the latest software versions and will display both the current and new versions. Click on the **Start Update** button to proceed to the new version.

Figure 42: Dialog showing the services software upgrade option



3.10 Group Manager

PACEdge Group Manager is a feature that allows users to manage and update multiple PACEdge devices at once, as a group. As of PACEdge version 3.0.0, the Group Manager supports the following features:

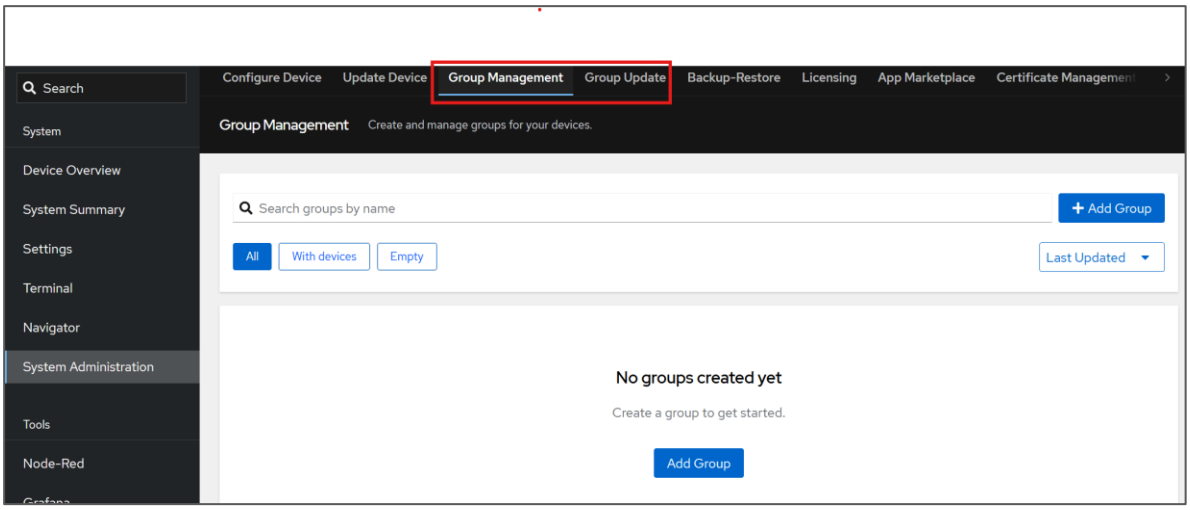
- Configuring and managing services and user credentials
- Host Linux operating system update
- PACEdge Application (container) image updates
- Node-RED flow updates
- Grafana dashboard updates

To use the Group Manager feature, a PACEdge Group Manager device needs to be connected to the internet so that up-to-date software packages can be downloaded from the PACEdge Marketplace.

3.10.1 Group Manager Initialization

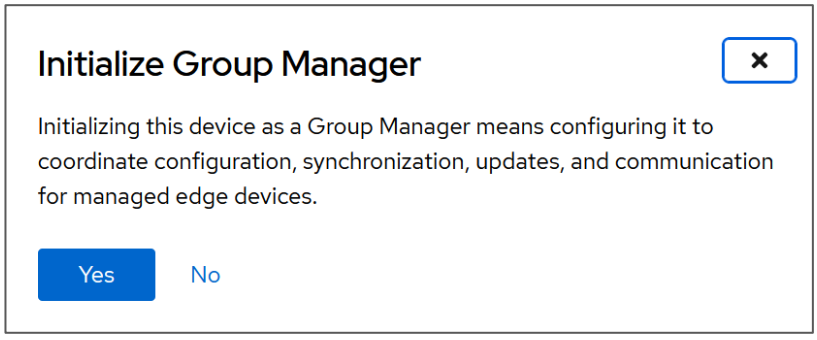
When the device has a Group Manager license, on the Cockpit->System Administration page, two additional tabs will be shown:

Figure 43: Group Manager configuration tabs



When the **Group Manager** tab is accessed for the first time, the user will be asked if the Group Manager should be initialized. This step will set up a number of container images. Depending on the hardware speed, this step will take a few minutes.

Figure 44: Notice that the Group Manager is to be initialized



Once initialization is complete, a page allowing users to create new groups will be shown.

3.10.2 Configuring Device Groups

Before the Group Manager can be used, PACEdge devices need to be added to the Groups.

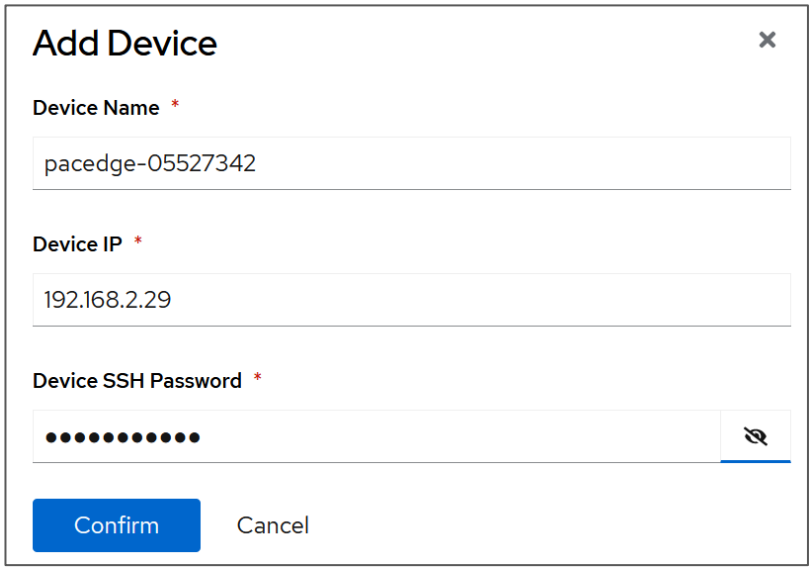
Note: When adding new devices with only factory default configuration to the group, first log directly into the device, follow prompts to change the Linux password, and accept the EULA. It is expected that the device already has a valid PACEdge license on it. If performing a Factory Default Restore operation, make sure the PACEdge license is manually installed.

Creating a New Group and Adding the 1st Device

To create a new group, click on the Add Group button and enter the group name. Next, click on the More Actions symbol and select **Add device.** Fill in the required information. Notice that for the Device Name, it is recommended to use the device's hostname, and the Device SSH Password is the admin password on the target device.

Note: It takes a few seconds to show activity after clicking the Confirm button. Please be patient

Figure 45: Dialog to define the device being added to the group



Note: Group Manager depends on IP and SSH connectivity between the GM and devices. In case of connectivity errors, please consult the debugging steps in the *Section 7.1.3 Group Manager - Device Connectivity Diagnostics.*

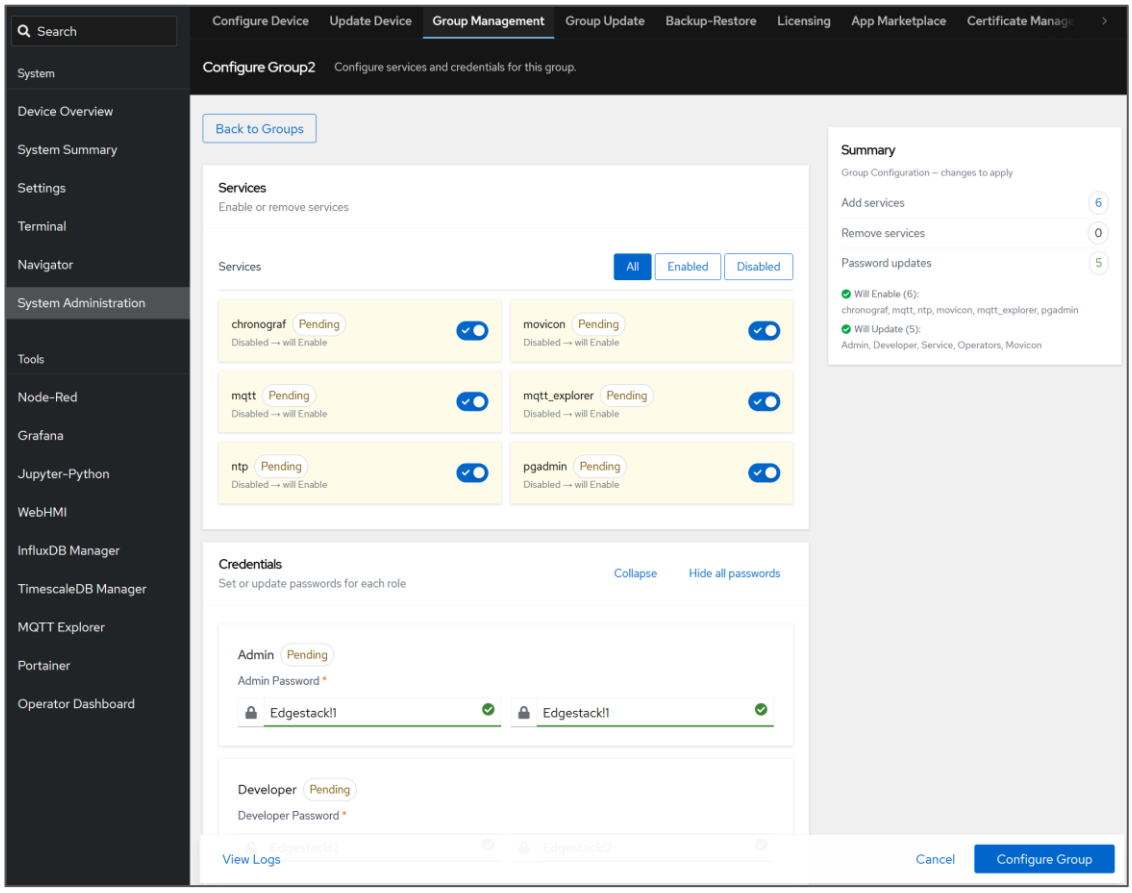
Part of the Group Manager functionality is to control what services should be enabled across the whole group of devices and to set/change credentials for the services. When creating a new group and adding the first device, a distinction is made if the device has already been configured with services and credentials or if the device is at the factory default state. If the device has already been configured, then Group Manager queries the

device and adds all running services to the group configuration. If the device is not configured, then first a Group Services dialog is displayed, allowing users to choose what services are to be configured in this new group. Select the required services and set the passwords for each user role, then click the Configure Group button.

Note: Depending on the hardware configuration, services will take a while (up to 20 minutes on the CPL410).

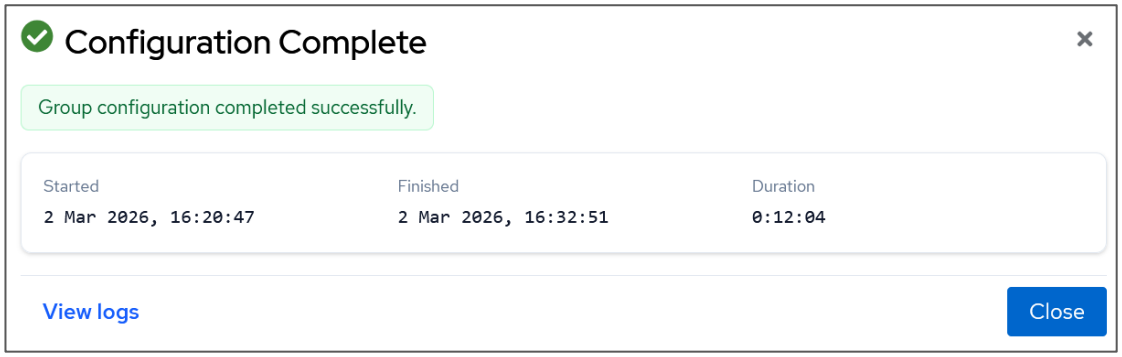
Note: Jupyter/Python is an optional service at this time, and is not part of the group-managed functionality.

Figure 46: Page asking user to set the default configuration for the whole group (1st device is unconfigured)



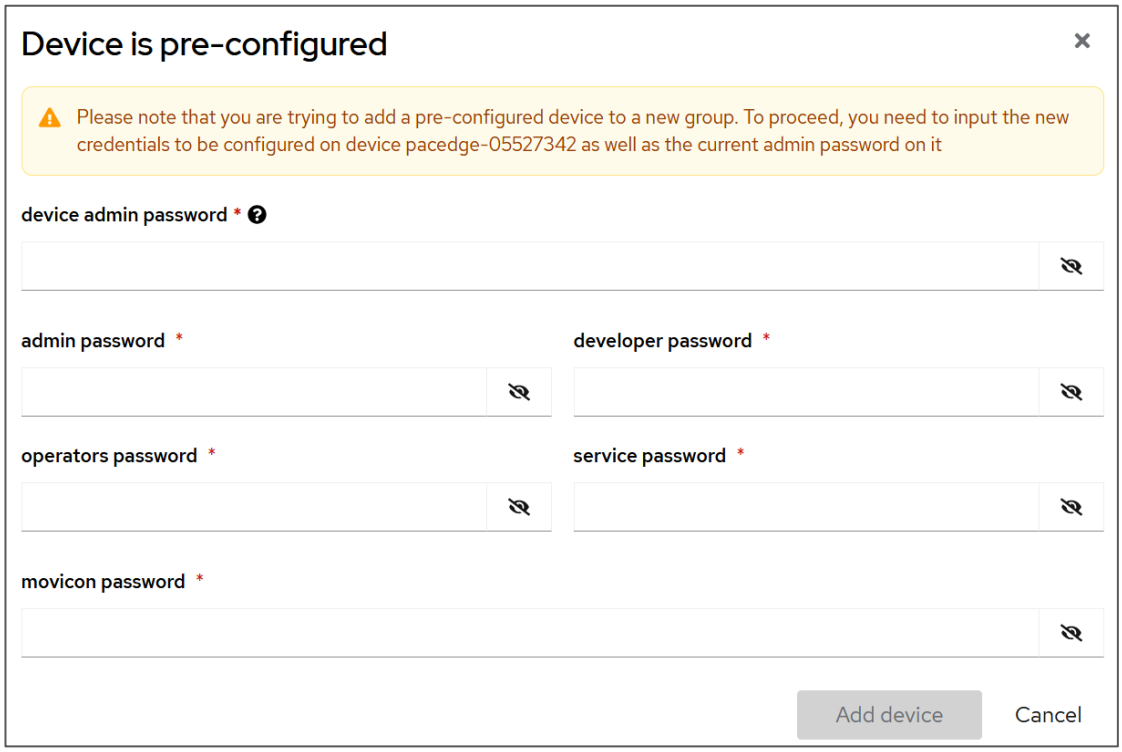
At the end of configuration, the following message will be shown:

Figure 47: Notice that the unconfigured device has been configured and added to the group



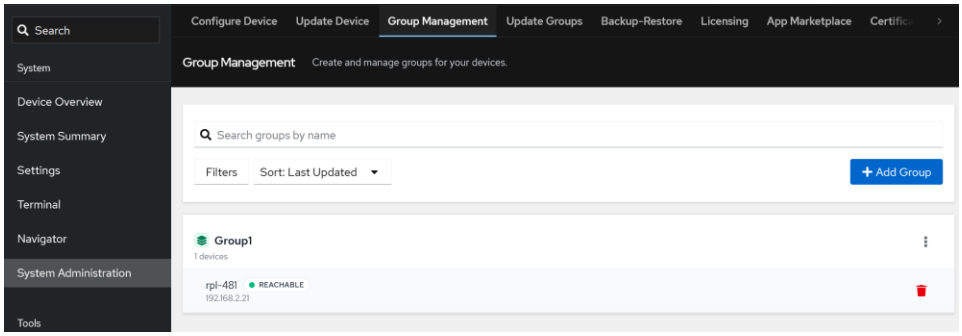
If the first device has already been configured, then Group Manager will ask the user to provide the Linux admin password and allow the user to set new Services passwords. It is allowed to re-enter existing passwords.

Figure 48: Dialog informing that the group's configuration will be set based on this device's configuration, asking to confirm passwords



After the device has been added to the group, its name and IP address will be listed as shown below:

Figure 49: Group with One Device



Adding More Devices to the Group

When adding 2nd and following devices to the group, Group Manager assumes that the same services and credentials already configured for the group will be replicated across all the other devices within the same group. For each additional device, the following message will be displayed. Click on the **Confirm** button and wait a few minutes until services and credentials on the new device are set based on the group's configuration.

Figure 50: Notice that the new device will be configured based on the group's settings

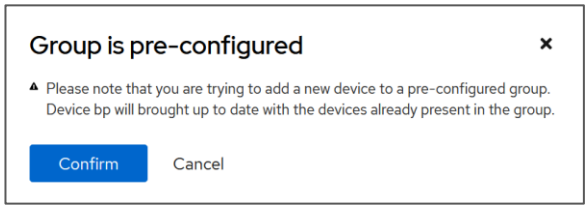
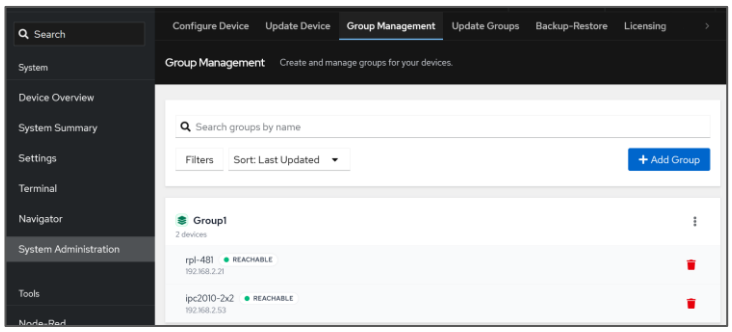


Figure 51: Group with two devices



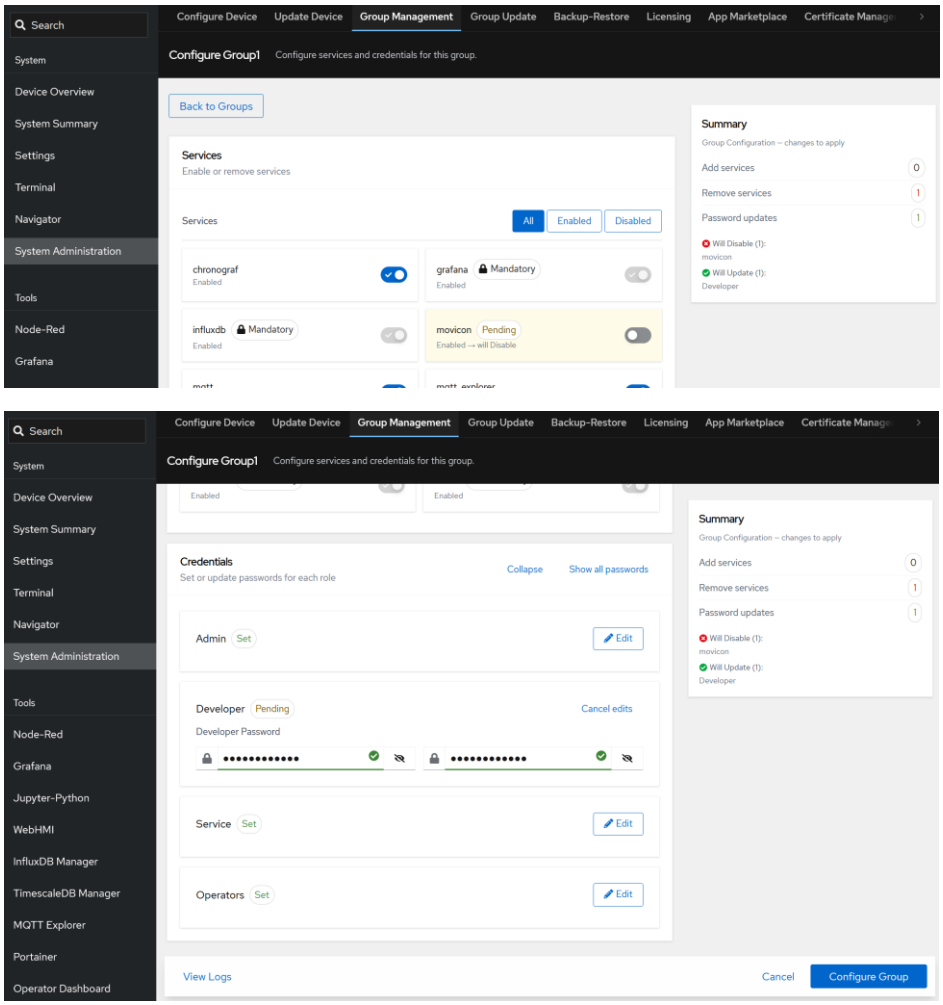
3.10.3 Changing the Group's Configuration

User has full flexibility from the Group Manager to delete devices from the given group and add them to another group.

The device can only be part of one group. Conflicting configurations may lead to unexpected failures.

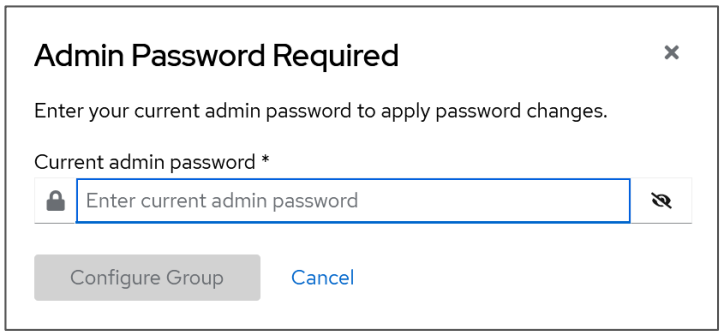
The user can also modify which services are running and update user passwords. To do so, click the **More Actions** icon for the desired group and select **Configure**. In the example below, the **Movicon** service is disabled, and the **developer password** is being changed.

Figure 52: Changing the Group's Configuration by Disabling the Movicon Service and Changing the Developer's Password



Once the user clicks on the **Configure Group** button, a dialog to provide the Linux admin password will be shown. Please enter your password and click on the **Configure Group** button.

Figure 53: Dialog asking for the Linux admin password so that group configuration changes can be applied



3.10.4 Performing Software Updates

Pulling Latest OS and Service Updates

Before performing an update, the latest host Linux OS and service containers software versions need to be retrieved from the Emerson Marketplace. To do this, open the **Group Update** page and click **Pull Latest Updates**.

Figure 54: Page to perform software updates at the group level

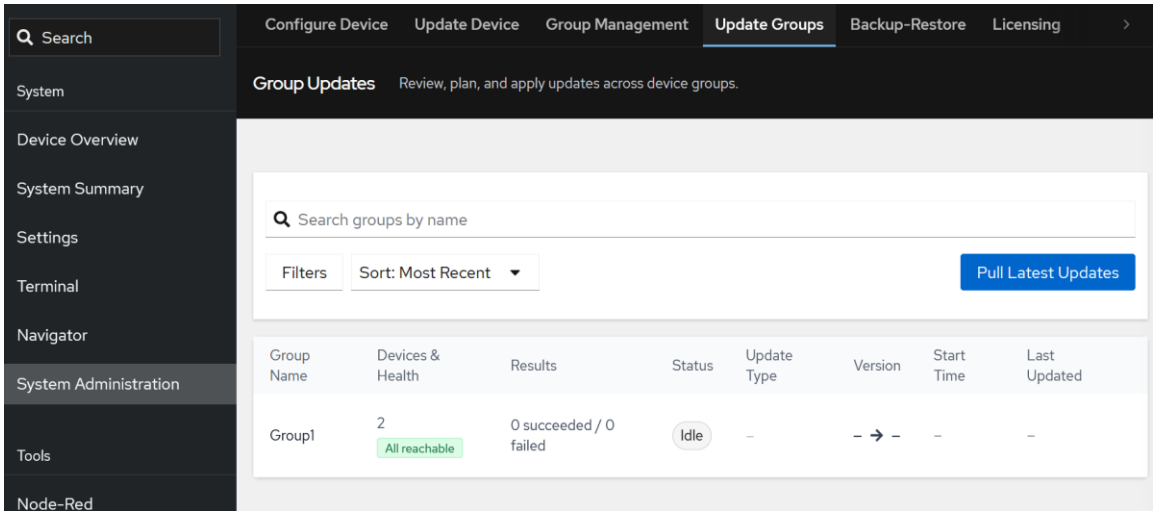
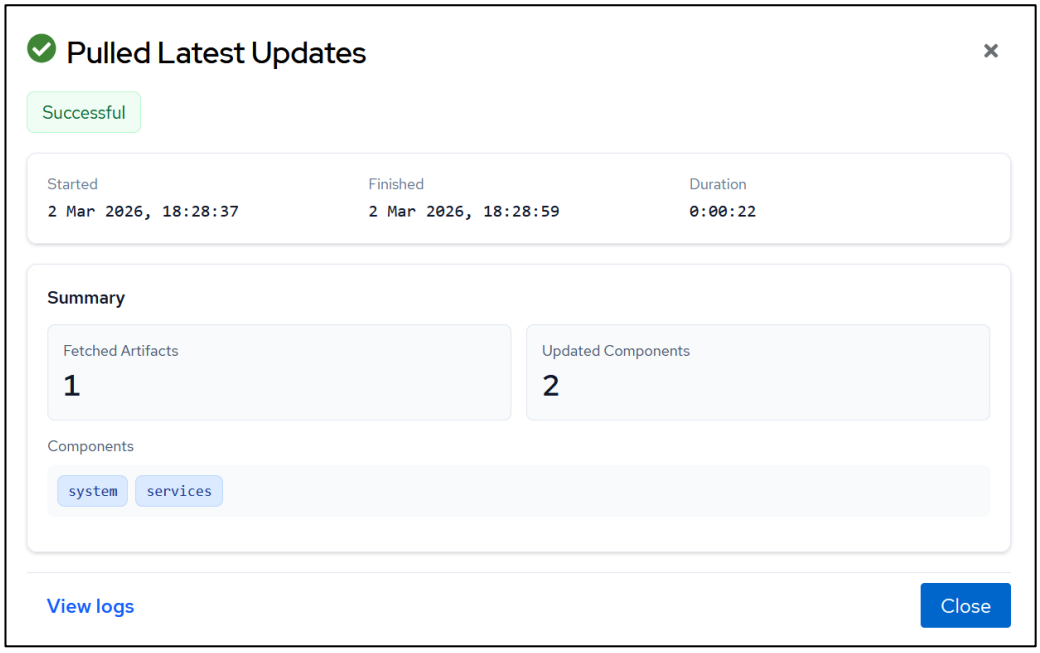


Figure 55: Notice showing how many updates have been pulled from the Marketplace



Note: Group Manager depends on the Internet connectivity and the ability to connect to the online Marketplace.

Preparing Node-RED Flows and Grafana Dashboards

Group Manager also allows users to upload Node-RED flows and Grafana dashboards to all devices within a group. Before doing so, the flows and dashboards must first be copied to the appropriate folders on the group manager:

- Using Navigator, copy Node-RED flows to the folder:
  `/home/admin/pacedge_assets/nodered/deploy`
- Using Navigator, copy Grafana dashboards to the folder:
  `/home/admin/pacedge_assets/grafana/dashboards/deploy`

Performing PACEdge System (Host Linux OS) Updates at the Group Level

To update the PACEdge system, including the host Linux OS, on all devices within a specific group, navigate to the Group Update page, locate the desired group, and click **Update**. This will open a dialog that allows the user to select the update to perform. Select **System Update.** At the bottom of the dialog, the current system version and the next available system version will be displayed. To proceed, click **Deploy Update**.

Figure 56: PACEdge System Update from v3.0.0 to v3.0.1

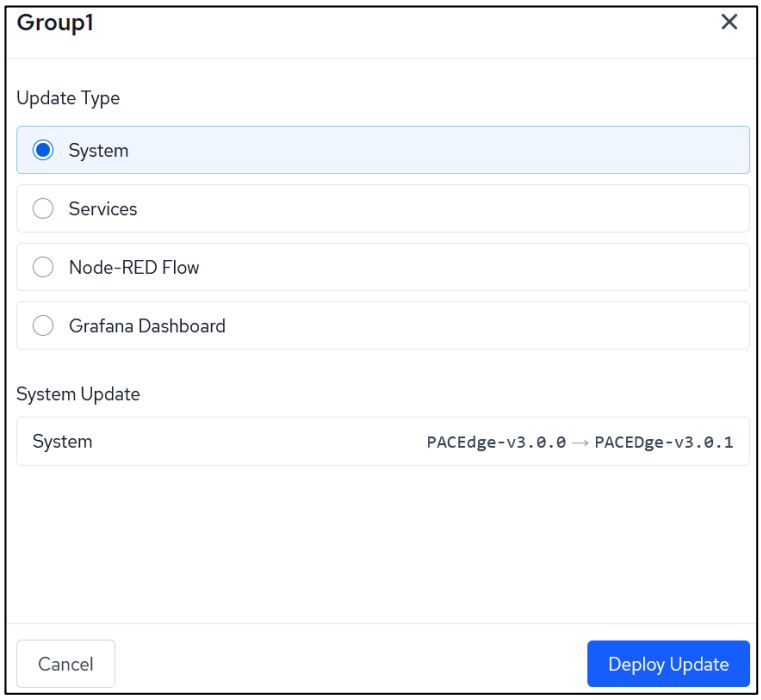


Figure 57: Dialog Showing System Update in Progress

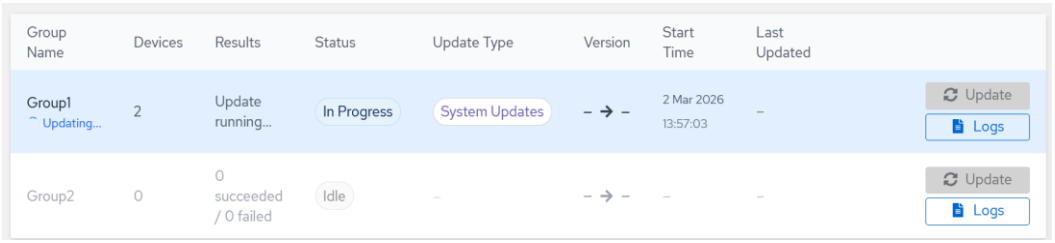
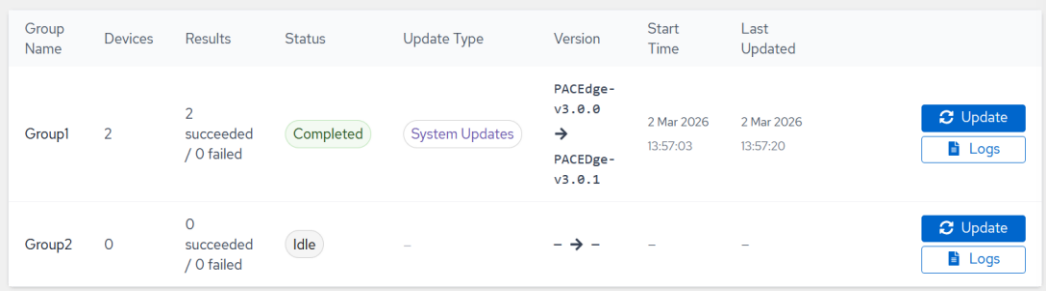


Figure 58:: Dialog Showing System Update Completed



Performing Services Update at the Group Level

When **Services** is selected, a list of currently running service versions and the available new versions will be displayed. Services shown in grey indicate that the new version is the same as the currently running version. To proceed, click **Deploy Update**.

Figure 59: PACEdge Services Update (note, in the image below, it is actually showing a downgrade, which is used only for testing purposes)

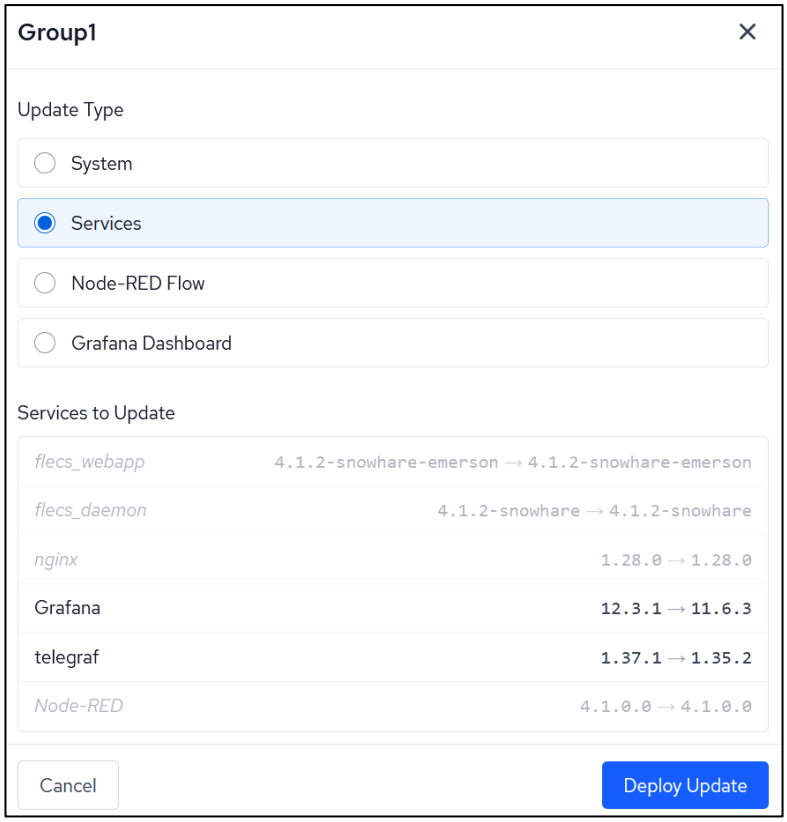
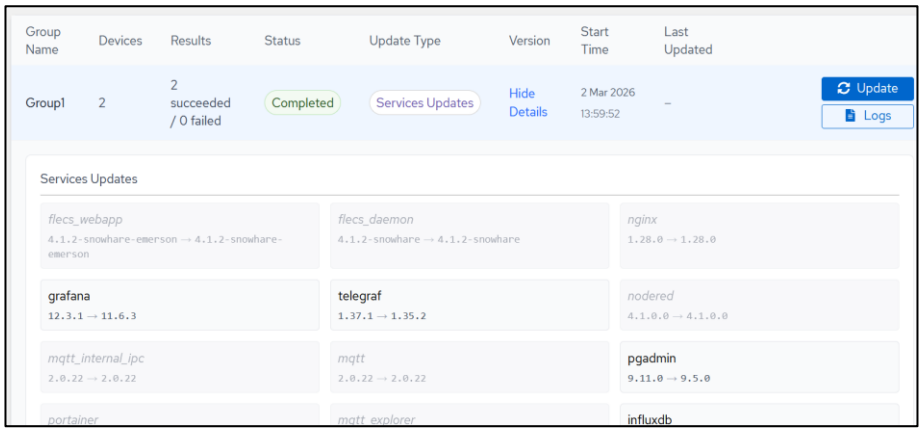


Figure 60: Dialog showing Services Update completed



Uploading Node-RED Flow at the Group Level

When selecting a Node-RED Flow option, a dialog will appear to prompt the user to choose a flow file. The file must be placed in the required folder on the device, as described above, before performing this step. Select the desired flow file and click **OK**.

Note: If the Node-RED flows have nodes that will require credentials (such as database access or MQTT nodes), these credentials will need to be set manually on each device. The credentials are automatically removed when exporting Node-RED flow for security purposes.

Figure 61: Dialog to select Node-RED flow file

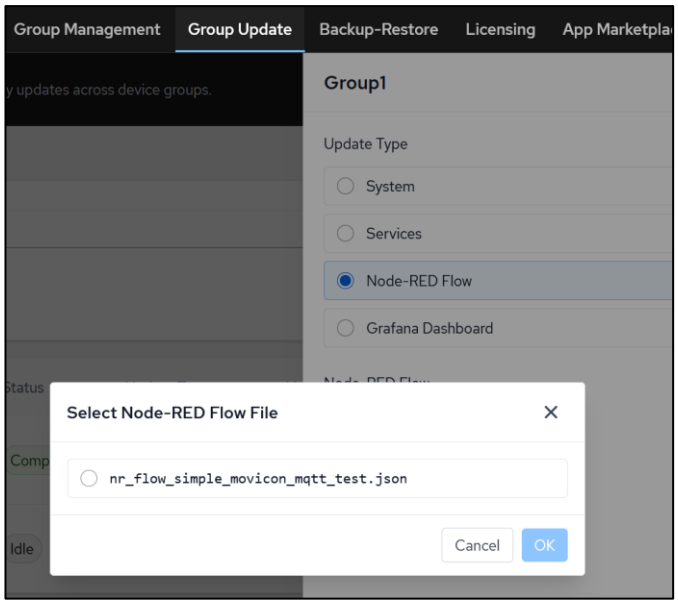
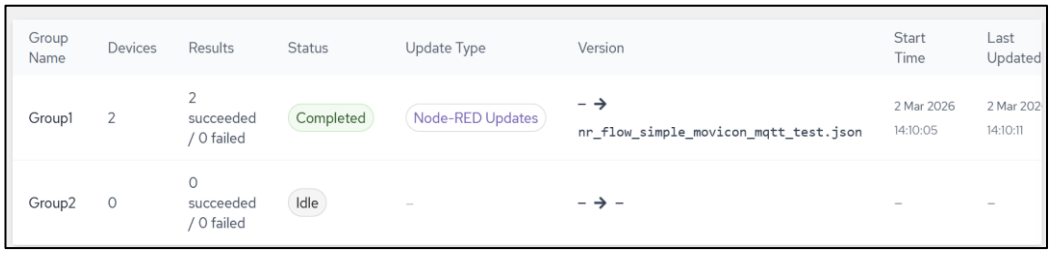


Figure 62: Dialog showing Node-RED flow upload completed



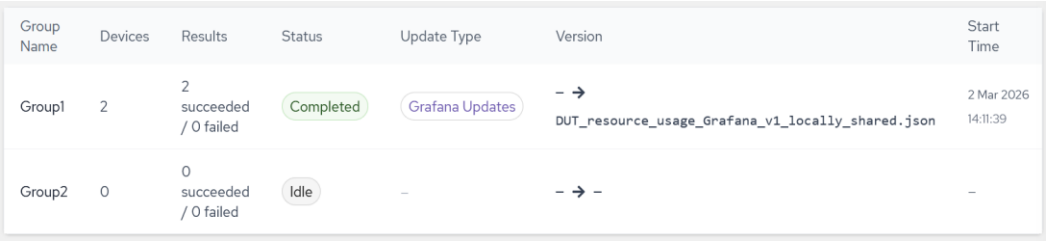
Group Name	Devices	Results	Status	Update Type	Version	Start Time	Last Updated
Group1	2	2 succeeded / 0 failed	Completed	Node-RED Updates	– → nr_flow_simple_movicon_mqtt_test.json	2 Mar 2026 14:10:05	2 Mar 202 14:10:11
Group2	0	0 succeeded / 0 failed	Idle	–	– → –	–	–

Uploading Grafana Dashboard at the Group Level

When selecting a Grafana Dashboard option, a dialog to choose a dashboard file will be displayed. Note that the file needs to be placed in the required folder on the device, as instructed above, before this step. Select the desired dashboard file and click the **OK** button.

Note: When exporting a Grafana dashboard to be uploaded by the Group Manager, make sure that the **Export for sharing externally** button is disabled.

Figure 63: Dialog showing Grafana dashboard upload completed

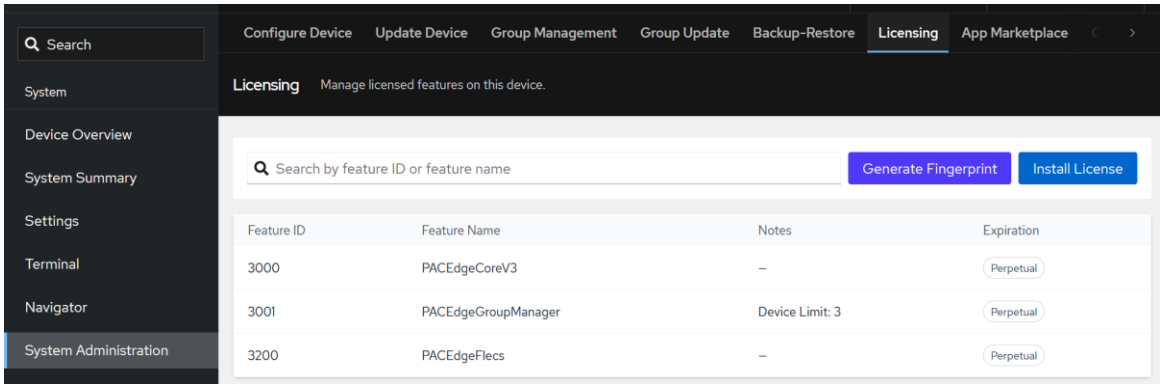


3.10.5 Group Manager Licensing

The Group Manager feature requires a license, which limits how many target PACEdge devices can be updated. The license can be viewed by navigating to the *Cockpit->System Administration->Licensing* tab, where a line item with **PACEdgeGroupManager** and **Device Limit** is shown.

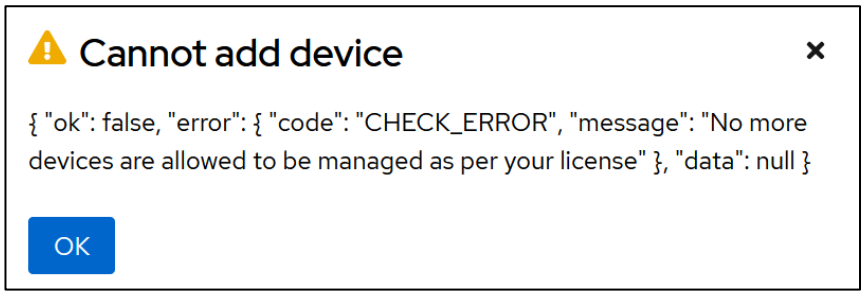
Note: If this line is missing, then the device does not have a valid Group Manager license.
Note: The Group Manager license is only required for the Group Manager device. Devices being managed do not require any additional license.

Figure 64: Group Manager license information



If you reach the license limit of devices to be managed, the following error will be shown:

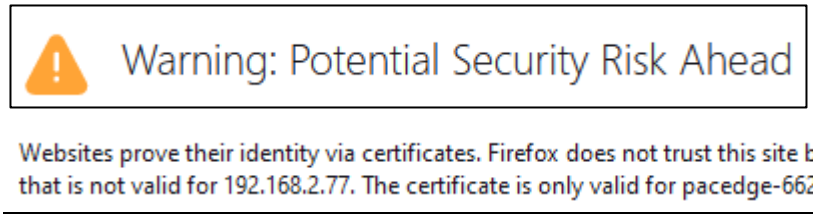
Figure 65: Cannot Add Device



3.11 PKI and its use in PACEdge

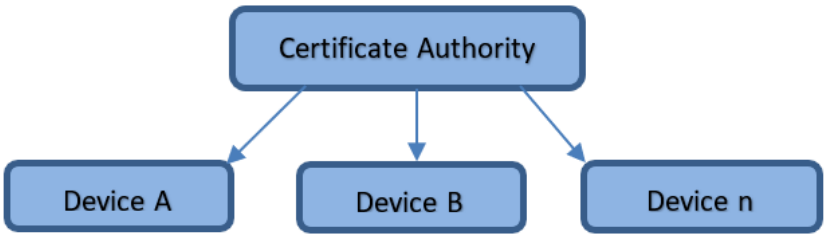
PACEdge includes a Certificate Management Utility, which helps users create and manage certificates. The purpose of these certificates is not only to encrypt communication and prevent Man-In-The-Middle attacks, but also to ensure that your internet browser is indeed connecting to a PACEdge device and not to an attacker's device. When configured improperly, a security warning message will display.

Figure 66 Browser Security warning message example



Public Key Infrastructure (PKI) works along with a **Certificate Authority (CA),** which signs certificates specific to devices. When the CA certificate is added to the trusted CA list in the browser, all devices with certificates signed by that CA are deemed trusted. This is useful because each device has a unique certificate, which will change if the device's hostname changes.

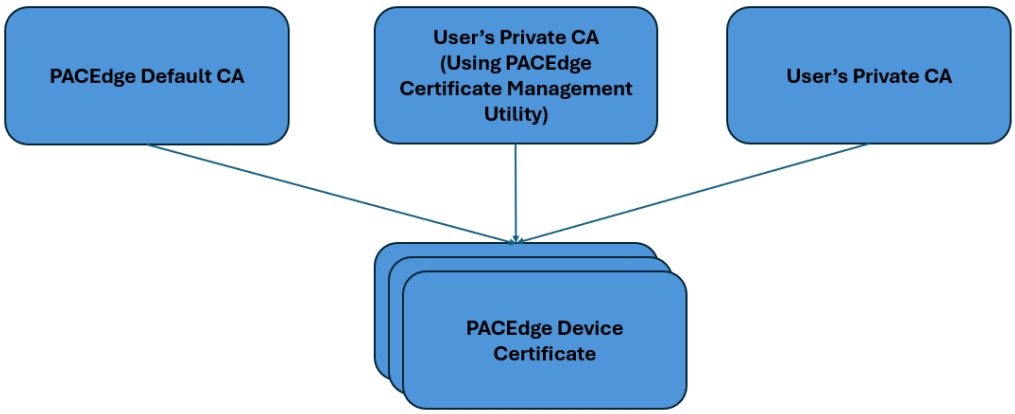
Figure 67: Figure 71 Certificate Authority trust chain



Note: To take advantage of the certificate when using a browser, instead of using the IP address, use the host name of the device, with **.local** appended. For example, `https://<hostname>.local`

There are multiple usage models of how the certificates can be used with the PACEdge devices:

Figure 68: Certificate Usage Options



3.11.1 Default PACEdge CA

All PACEdge devices are shipped from the factory with a device certificate that is signed by the PACEdge CA. Furthermore, the PACEdge CA Certificate will be available for download via the PACEdge certificate management utility or from the Emerson Customer Center website. Once this CA is added to the browser's trusted CA list, all PACEdge devices can be accessed using the device's hostname, ensuring device identity.

Note: If a pre-installed certificate on the device is lost, or a factory default recovery is exercised, this certificate will be lost. Emerson's second-level technical support can re-issue certificates; however, users are recommended to issue and manage their own CA certificates.

3.11.2 User's Private CA

User's Private CA (Using Certificate Management Utility)

With the PACEdge Certificate Management utility, users can create their own CA and issue certificates for other PACEdge devices. By creating a private CA, users can ensure that only their own PACEdge devices are trusted, providing greater security than relying on the default PACEdge CA. Instructions on how to set up your own CA and issue your own certificates are documented below.

User's Private CA (Using Existing Infrastructure)

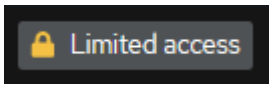
Some users will already have an existing PKI and will be able to issue certificates. In such cases, the PACEdge certificate management utility will allow users to upload those certificates onto a PACEdge device.

3.11.3 Services Provided by Certificate Management

To perform certificate management functions, the

user needs to have administrative access rights. Administrative access can be requested by pressing the **Limited Access** button at the top of the Cockpit screen.

Figure 69: Limited Access button

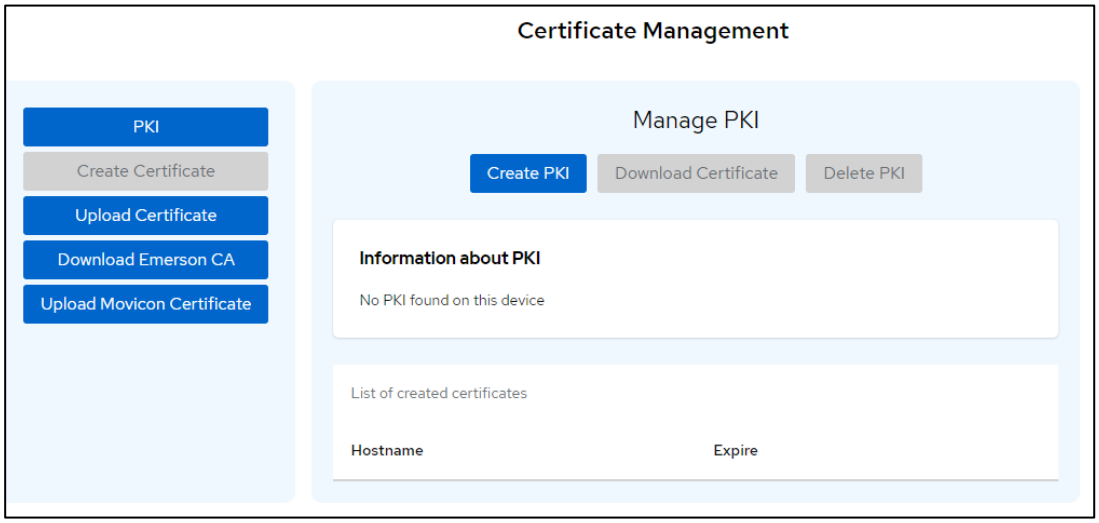


The following services are provided by certificate management:

- Enable users to create their own PKI (CA).
- Enable users to use the existing CA to issue certificates for this and other devices and download a CA certificate (which should be installed in the browser).

- Upload previously created certificates (either by PACEdge certificate management or by other services) to this PACEdge device.
- Download PACEdge's CA certificate (used to sign PACEdge device certificates during production), which should be installed in the browser.
- Upload Movicon certificates, such as OPCUA certificates that come with OPCUA Servers.

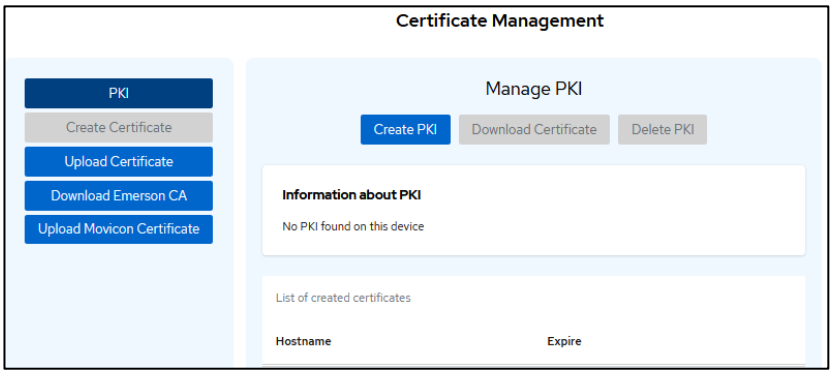
Figure 70 Certificate Management Utility View



PKI tab

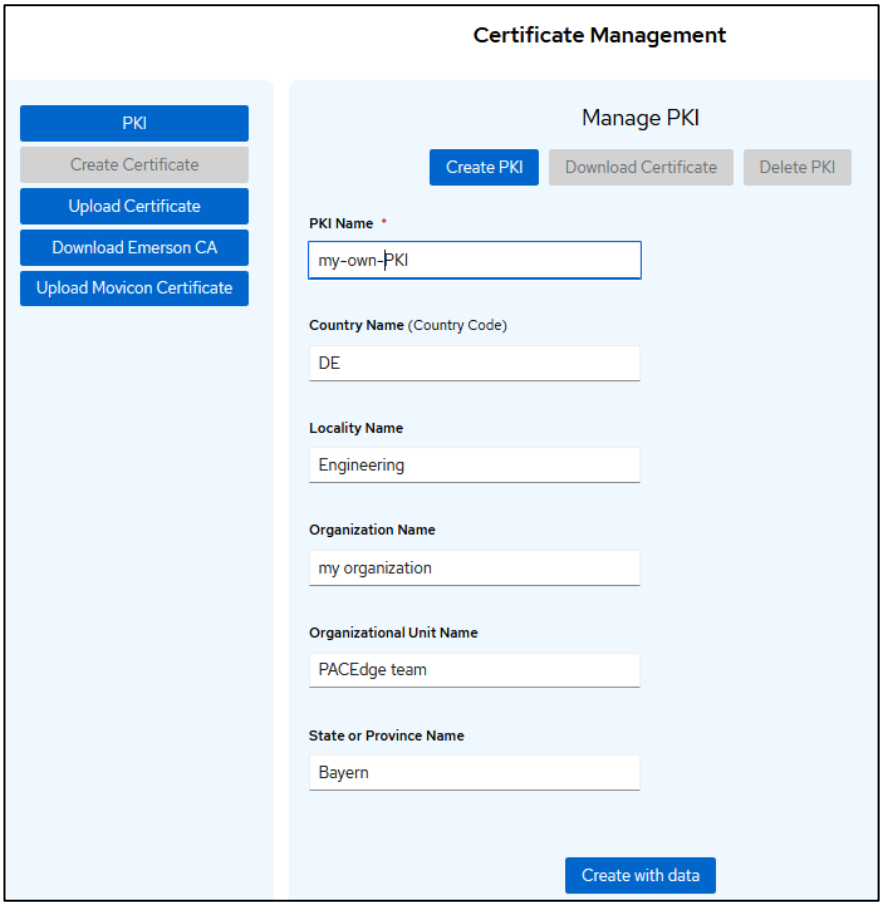
When accessing the **PKI** tab, the system searches for an existing PKI configuration and, if found, displays its details. By default, PACEdge units do not have a PKI configured, which results in the screen below:

Figure 71 PKI Tab View with No Existing PKI



In this tab, the user has the option to click on the **Create PKI** button, then fill in required information, such as:

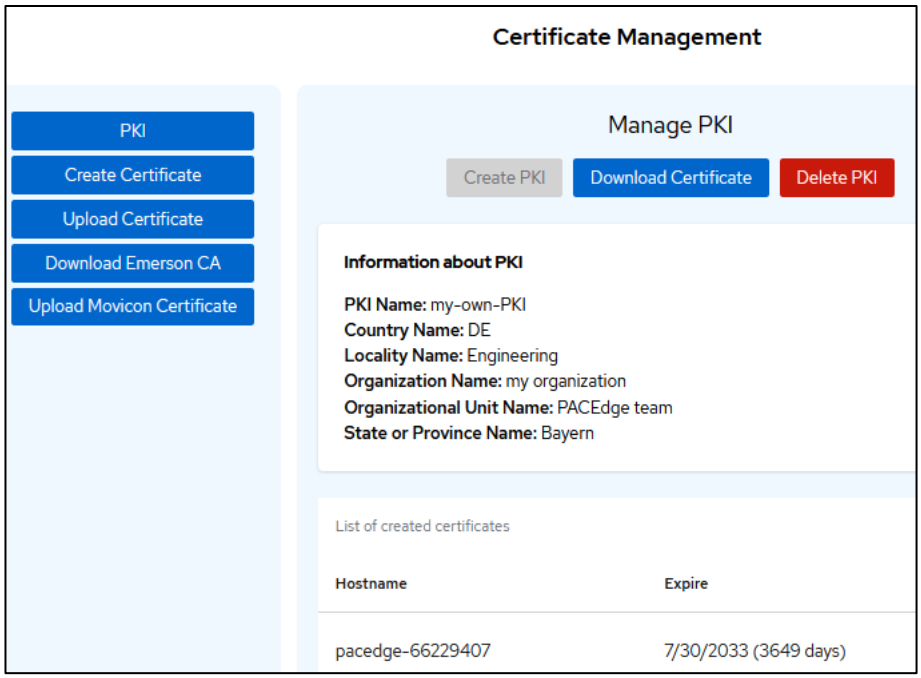
Figure 72 Fill in the Information to Create Your own PKI



Once the **Create with data** button has been clicked, the required PKI will be created, along with the CA certificate and device certificate. Since the device's certificate is being replaced, the PKI creation process will result in connection loss to the PACEdge device, which requires a restart to refresh the browser.

Now that your own PKI has been established, you will see the following screen:

Figure 73: Enabled View Once its PKI has Been Created



The user can now use the **Download Certificate** button, which enables the user to download and then add the certificate to the browser. Going forward, all device certificates will be trusted automatically.

The user can also **delete PKI** along with the CA certificates.

Once completed, the user can go to the **Create Certificate** tab and create certificates for other PACEdge devices as needed.

Create Certificate tab

In this tab, the user has the option to create one or more device certificates. For successful certificate creation, it is critical to provide an accurate device hostname. The PACEdge device hostname can be found by using *Cockpit->Overview* in the Configuration tab. **Note**: At this point, the user can also change the hostname. If changing the hostname, please make sure that it is a unique name. It should also be noted that the

associated certificate that was issued using the old hostname will no longer be valid. Additionally, the user will need administrative access rights to change the hostname.

Figure 74 PACEdge Hostname in Cockpit

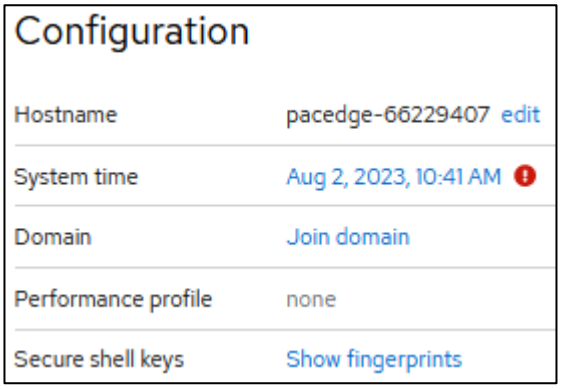
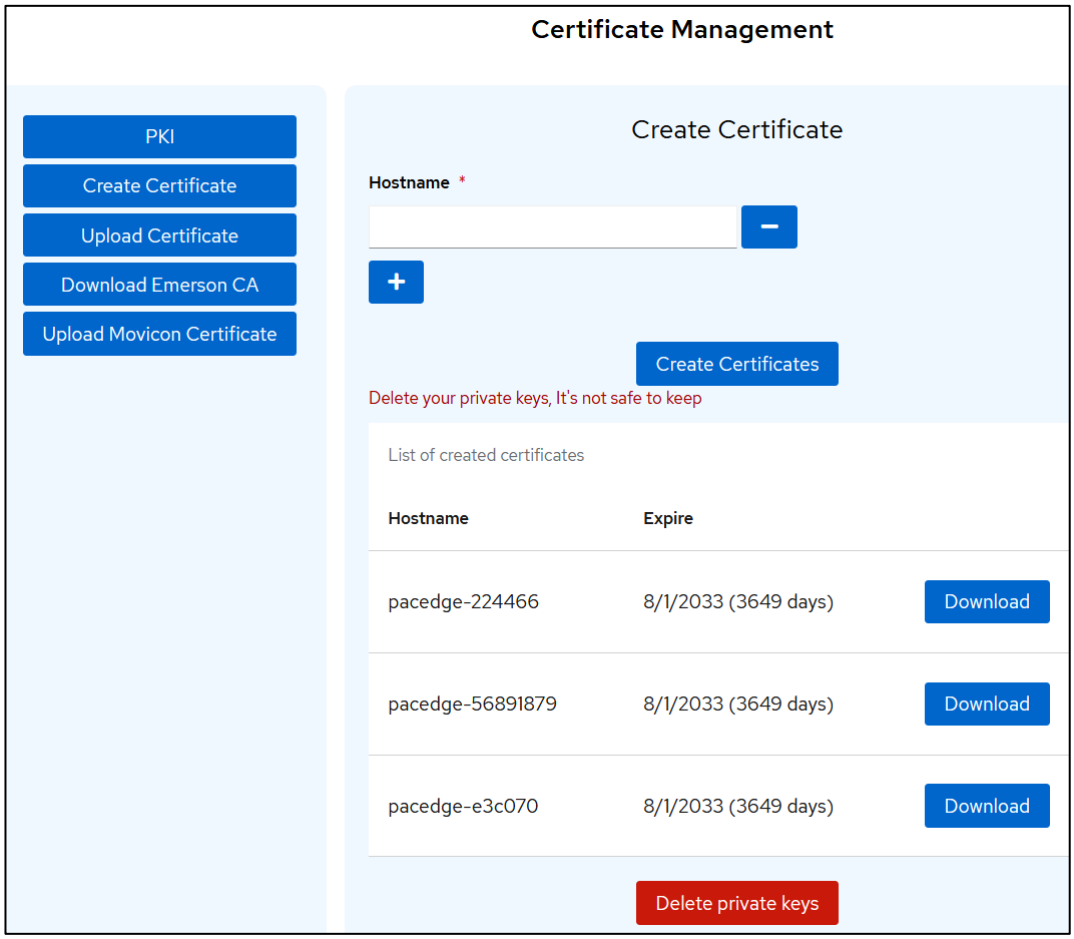


Figure 75 View when creating device certificates.



Once the required certificates and associated keys have been created, they can be downloaded by pressing the **Download** button. Next, these certificate/key files can be uploaded to the required PACEdge device using the **Upload Certificate** tab.

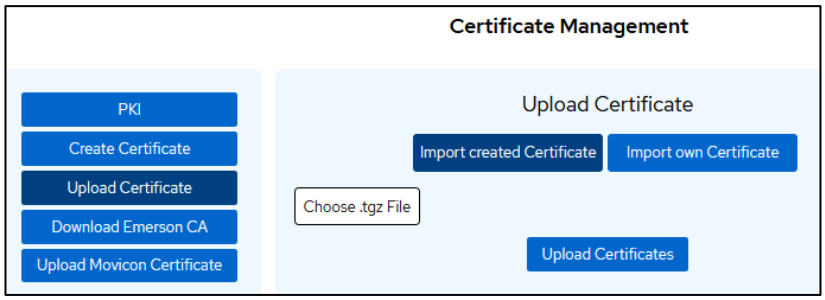
Note: Creating a certificate for the device will also create a key for it. Once the certificate and the key have been transferred to the intended device, storing their keys is not required and not desired (for security purposes). Therefore, it is recommended to delete the key by pressing the **Delete private keys** button.

Upload Certificate tab

Using the Upload Certificate tab, the user can upload certificate and private key files onto a PACEdge device. The following two main use cases are supported:

1. The User has created his own PKI using the Certificate Management utility on another PACEdge device and generated a certificate and private key for this particular PACEdge device, which now needs to be uploaded. In this case, the certificate and private key are packaged into a .tgz archive. When clicking on the **Choose .tgz File** button, the user is given the opportunity to select the required archive file on their computer. Clicking on **Upload Certificates** completes this operation.
2. The user has his own PKI and can generate certificates and private keys. Clicking on the **Import own Certificate** button and then on the **Choose .key File** and **Choose .crt File** buttons will allow the user to select the required files on their computer. Clicking on **Upload Certificates** completes this operation.

Figure 76 Upload Certificate Tab View



Note: The user needs to have administrative access privileges to use these functions.

Note: Uploading the certificate will result in a connection loss to the PACEdge device, requiring the user to refresh the browser.

Download Emerson CA Tab

This tab provides detailed information about the PACEdge Root CA, which signs the CAs used to sign certificates for the units. These certificates are pre-installed. By clicking the **download** button, the user can download the CA certificate onto their computer and then install it in their browser.

Upload Movicon Certificate Tab

On this tab, users can upload the certificates necessary for certain field bus communications to function properly. One common example is the OPC-UA interface, which may require that the OPC-UA Client have an OPC-UA Server certificate to work. If using Movicon Connext, the server certificate can be uploaded to Connext by using this tab. To upload, click on the **Choose the File** button, select the required file on your computer, and then click on **the Upload Certificate** button.

3.11.4 Adding CA Certificates to Browsers

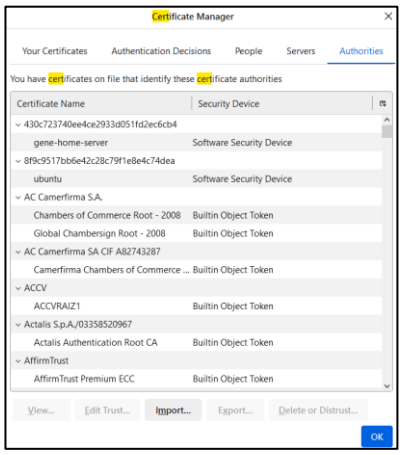
To be able to access PACEdge devices without a security warning, a new trusted authority must be added to the browser

Firefox

To add a CA certificate to the Firefox browser:

1. Click on the menu icon button in the top- right corner and then click **Settings**.
2. Search for **cert**.
3. Click on **View Certificates** and go to the **Authorities** tab, and click **Import**.
4. Choose the required certificate file on your computer.
5. Select **Trust for Websites** and click **OK**.

Figure 77 Firefox Certificate Manager View

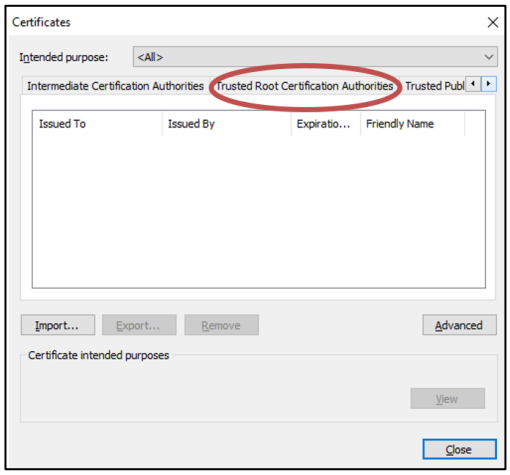


Chrome

To add a CA certificate to the Chrome browser:

1. In the top-right corner, click on the three vertical dots button and select **Settings.**
2. Click on **Privacy and Security**, then **Security**, **Manage device certificates Trusted Root Certification Authorities**, and finally **Import**.
3. In the wizard that opens, click **Next** and choose the Root Certificate file on your computer. Click **Next, Next**, and finally **Finish**.

Figure 78: Trusted Root Certification Authorities



3.12 Operator's View

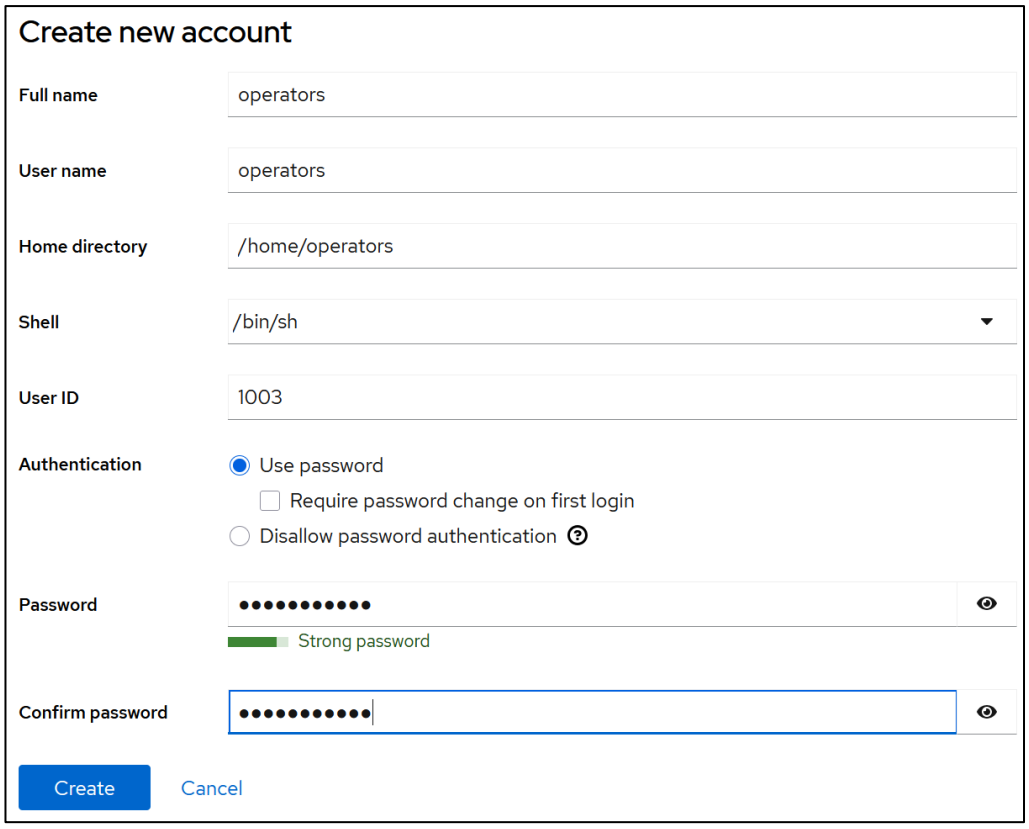
PACEdge has different user roles, one of which is **operators**. The **operator's** role is meant for the personnel that are operating equipment and have access to dashboards and HMI screens with minimal privileges.

Note: please pay attention that the role name operators have an "s" at the end and are written all lowercase.

3.12.1 Creating Operator's Account

To log in as operators, first, an account has to be created in Linux via Cockpit. To do so, log in as an administrator, switch to Administrative access in the Cockpit upper right corner, then navigate to Cockpit->Settings->Accounts page. Click on the **Create** button and enter the following information:

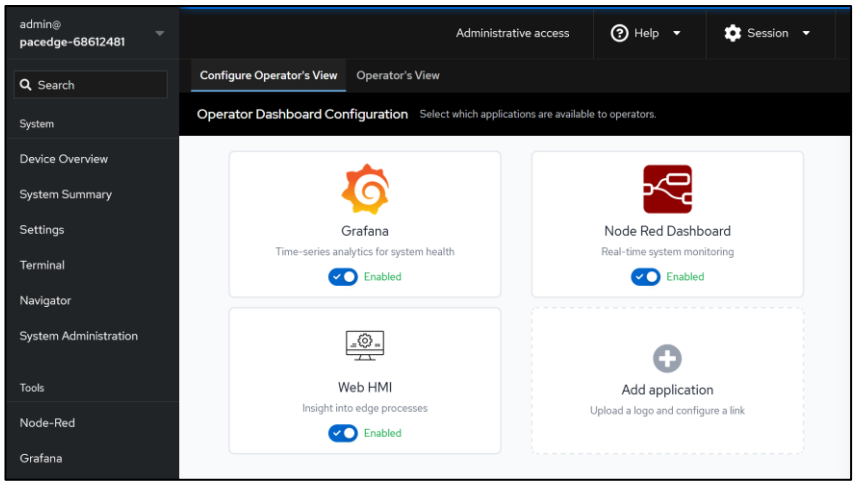
Figure 79: Creating Operators Account



3.12.2 Configure Operator's Views

As an admin or developer, the user can configure the **Operator's View**. To do so, navigate to *Cockpit->Operator Dashboard Configuration*. From here, the user can enable/disable Grafana, Node-RED, or WebHMI shortcuts, as well as add their own personalized shortcuts:

Figure 80: Configuring operators View



To test what the view would look like, select the **Operator's View** tab at the top.

3.12.3 Login as Operator Role

Once configured, the user can log out of the Cockpit and log in again as a user **operator**. Cockpit will automatically redirect to the Operators' **View displayed** in the kiosk mode:

Figure 81: Logging in as operators

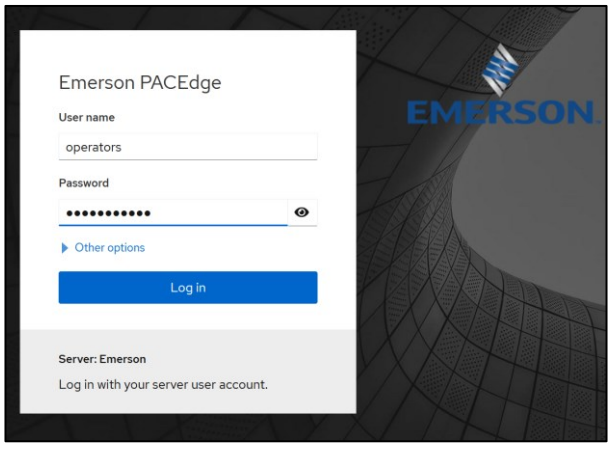
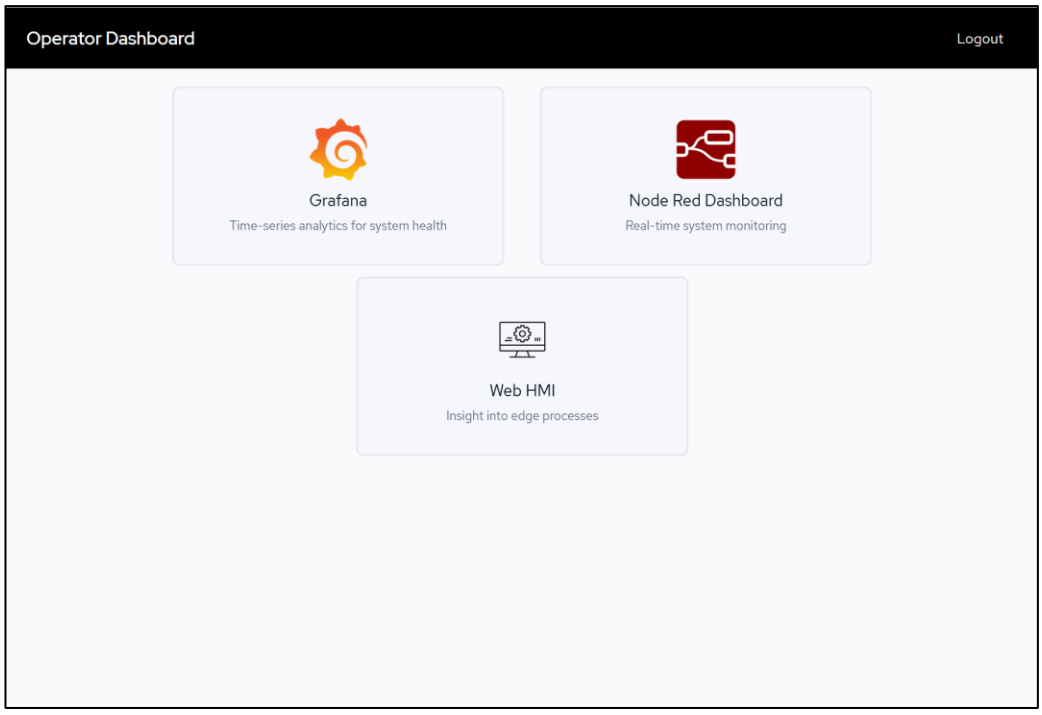


Figure 82: Operators Dashboard in the Kiosk Mode



Section 4: Saving and Restoring User Data

PACEdge software includes several applications, such as Node-RED, Grafana, InfluxDB, TimescaleDB, Connext, and WebHMI. When users create application flows and store data in the databases, this user-specific configuration and data are stored within the Linux file system. For backup purposes, this data can be periodically copied and stored in an external location, such as a USB storage device or a user's computer.

PACEdge provides multiple methods for backing up and restoring user data. Beginning with this version, a centralized Backup/Restore Utility is included. The following sections describe how to back up and restore data using:

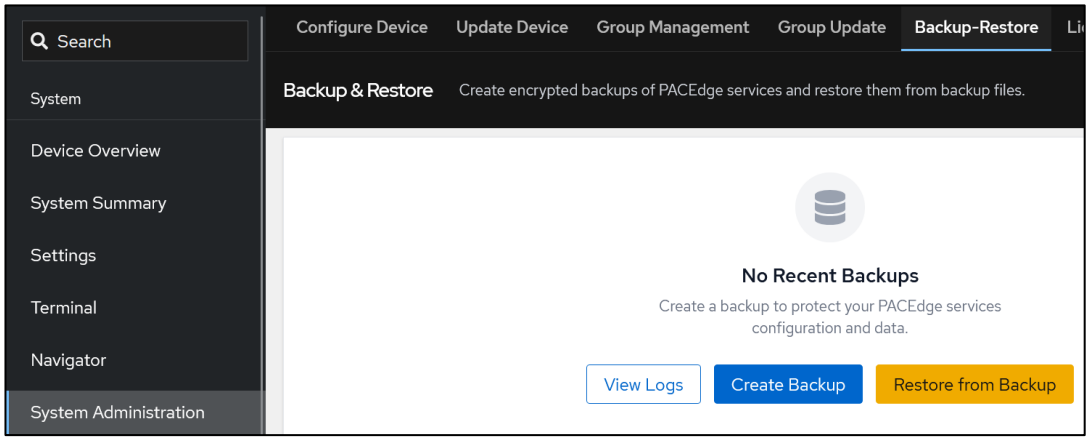
- PACEdge Backup/Restore utility
- Using native Node-RED and Grafana utilities
- Using Movicon.NExT Editor for WebHMI and Connext projects

4.1 Using PACEdge Backup/Restore Utility

The Backup/Restore Utility is available in:

Cockpit → System Administration → Backup-Restore

Figure 83: PACEdge Backup/Restore Utility



4.1.1 Important Considerations

Use this tool carefully to avoid password-related issues.

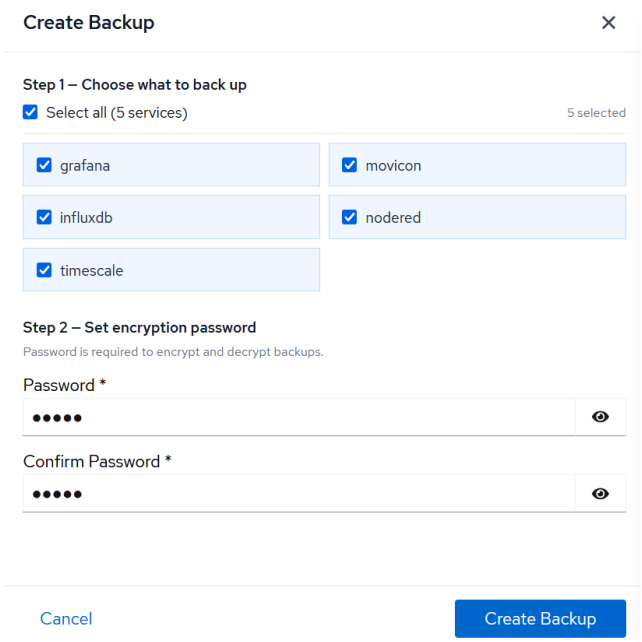
A PACEdge backup file includes service passwords. If a backup is restored on a system where the admin passwords differ from those stored in the backup file, authentication problems may occur.

Before restoring a backup, ensure that the admin passwords for the services match the passwords used when the backup was created.

4.1.2 Creating a Backup

- Click **Create Backup.**
- Select the services to include in the backup.
- Enter an encryption password to secure the backup file.

Figure 84: Creating a Backup



The backup process encrypts the file for security purposes. During this process, selected services are temporarily stopped and then restarted. This may take several minutes.

Once completed, a dialog will open prompting the user to specify a location to store the encrypted backup file on the user's computer.

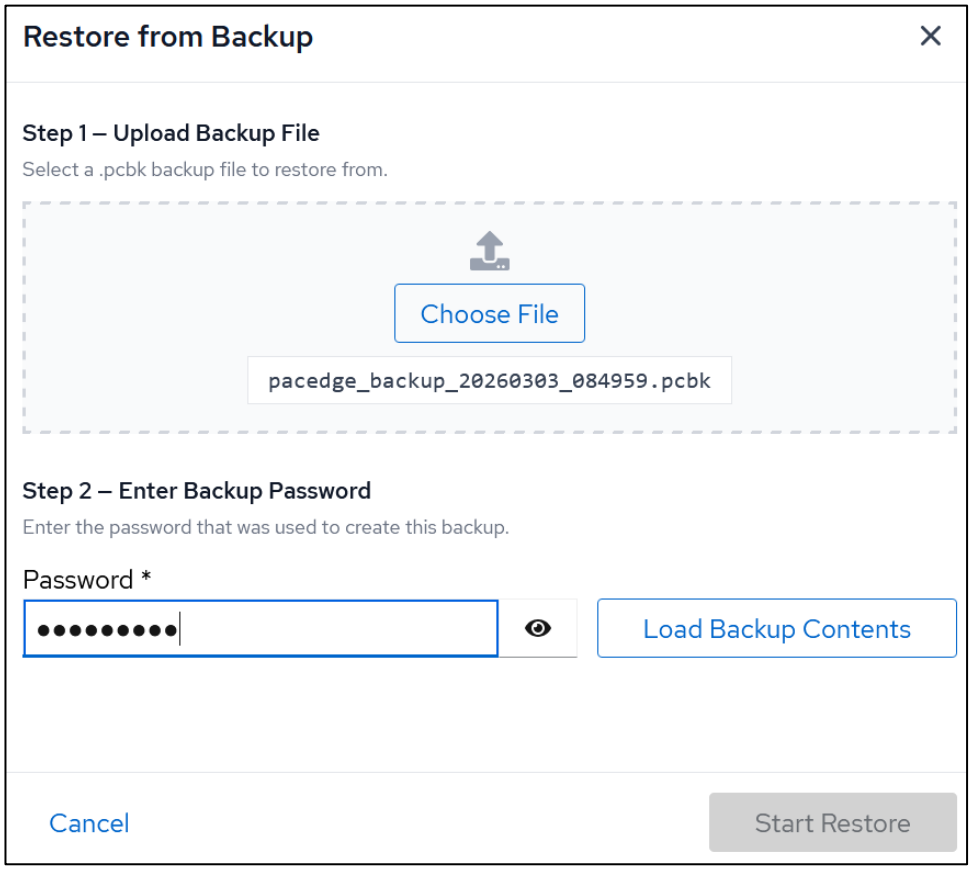
4.1.3 Restoring a Backup

CAUTION

When restoring from the backup file, all current data will be overwritten with data in the backup file. This means that if some measurements were stored in the databases after the backup was created, this data will be lost.

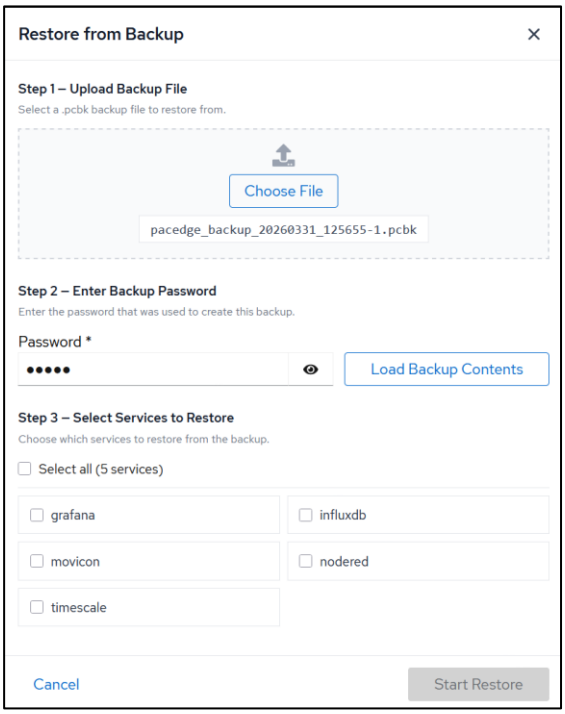
1. Click on **Restore from Backup.**
2. Consider the potential data loss warning and accept to proceed.
3. Click on **Choose File** and point to the backup file you wish to restore from.
4. Enter the encryption password used during backup creation to decrypt the file.

Figure 85: Starting Restore operation



5. Click **Load Backup Contents**. All backup contents will be displayed. Services that are available on the current system can be selected for restoration. Services not currently installed or running will be listed, but cannot be selected.

Figure 86: Selecting data to be restored



6. Select the desired services and click **Restore**. The restore process may take several minutes, as affected services will be restarted during the operation.

4.2 Exporting and Importing Flows in Node-RED

4.2.1 Export Flow

While in the Node-RED application:

1. Click on the menu icon on the right side of the screen  .
2. Select either the **current flow** or the **all flows** option.
3. Click on the **Download** button.
4. Select the location (on your client system, not PACEdge) where to store the **flow.json** file.

4.2.2 Import Flow

While in the Node-RED application:

1. Click on the menu icon on the right side of the screen  .
2. Click on " Select a file to import.
3. Navigate to your client system's desired flow xxx.json file (not PACEdge).
4. Click on **Open**.
5. Click on **Import**.

4.3 Exporting and Importing Dashboards in Grafana

4.3.1 Export Dashboard

While in the Grafana application:

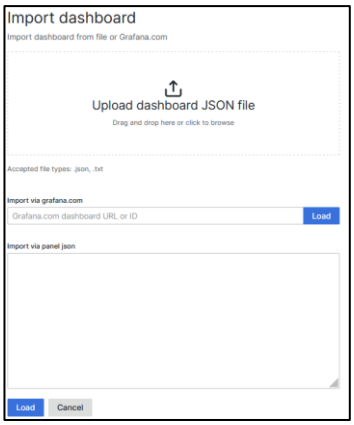
1. Navigate to your desired Dashboard.
2. Click on the **Share Dashboard** icon  .
3. Click on **Export.**
4. Click on **Save to file** and select the location to store it on your client system (not PACEdge).

4.3.2 Import Dashboard

While in the Grafana application:

1. Click on the hamburger icon in the upper-left corner and then click on **Dashboards**
2. Click to open a drop-down list under **New** (right side of the screen) and select **Import**

Figure 87: Import Dashboard Menu



3. Click on Upload dashboard JSON File.
4. Select your desired Grafana view file xxx.json and click on **Load**.
5. If asked, select the required database from the drop-down menu
   Note: If there is no valid InfluxDB database there, then most likely Grafana was not configured yet to connect with the database. Please follow the steps in configuring Grafana in this manual first to configure the required database.
6. Click on the **Import** button.

4.4 Importing Projects in Connext/WebHMI

Connext and WebHMI projects are first created on engineering workstations using Movicon.NExT software and then loaded into the PACEdge device. Therefore, there is no need to export projects from PACEdge. Projects can be loaded from the engineering workstation onto the PACEdge device when recovery is needed.

4.5 Backing Up and Restoring InfluxDB and MySQL Databases

InfluxDB and MySQL databases are stored in the main Linux file system at the following path:

- /home/admin/docker/volumes/emersonedgestack_influxdb/_data/
- /home/admin/docker/volumes/emersonedgestack_mysql/_data/

As an example, see the figure below:

Figure 88: Example paths

```
admin@pacedge:~$ sudo ls -l docker/volumes/emersonedgestack_influxdb/_data/data
total 12
drwx------ 4 root root 4096 Aug 12 11:48 _internal
drwx------ 4 root root 4096 Aug 12 11:48 telegraf_metrics
drwx------ 4 root root 4096 Aug 23 18:03 test_1_db
```

```
admin@pacedge:~$ sudo ls -l docker/volumes/emersonedgestack_mysql/_data/data
total 104
-rw-rw---- 1 systemd-coredump systemd-coredump    67 Aug 12 11:48 db.opt
-rw-rw---- 1 systemd-coredump systemd-coredump  1556 Aug 23 18:03 gj_test_data.frm
-rw-rw---- 1 systemd-coredump systemd-coredump 98304 Aug 23 18:40 gj_test_data.ibd
```

When a backup is desired, the user can copy all folders from **..../_data/** folder and restore them to the same location later. Cockpit Navigator can be conveniently used for the copy operations.

Note: Access to these folders requires admin privileges.

4.6 Saving License Files

PACEdge devices come with pre-installed software and valid factory license files. Under normal circumstances, the user does not have to worry about keeping a copy of the valid license file. Still, if restoring to PACEdge Factory Default needs to be done on RXi2-BP, IPC6010/7010/8010, and IPC 2010 Industrial PCs, then a valid license file will be required afterward to fully activate the PACEdge software. In such a situation, the user can always request a new license file from the Customer Care representative, as described in Section. *3.5, PACEdge License File.* An alternative would be to make a copy of the license file before performing a restore operation. The easiest way to copy files is using the Navigator application in Cockpit. To do so:

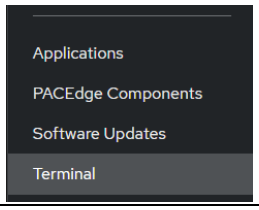
1. Open Navigator
2. Navigate to: `/home/admin/pacedge/emerson-software/license/ folder`
3. Right-click on the **license.json** file and choose the Download option, specify the location to store the file on your local PC

NOTE: If the download fails with the error: **Failed – Network error**, log out from Cockpit and log in again as the admin user.

4. Repeat the steps for the **license.sig** file in the same folder.
5. Alternatively, one can store license files on a USB storage device directly attached to the PACEdge device by following the steps below:

6. Mount the USB storage device by following the procedure in *Section 7.1, PACEdge Health Diagnostics*.
7. Within the Cockpit, go to the Terminal screen and enter the following commands:

Figure 89: Open Cockpit's Terminal



   a. **sudo cp pacedge/emerson-software/license/license.json /mnt/usb**
   b. Enter the admin password (if requested).
   c. **sudo cp pacedge/emerson-software/license/license.sig /mnt/usb**
8. Next, unmount the USB storage device by following: *7.3 Unmounting .*
9. You may remove the USB storage device and save the files: 1) license.json and 2) license.sig on your Windows workstation.

Section 5: PACEdge Software Backup/Restore/Recovery

With PACEdge software, users have the ability to install additional software packages and customized configurations to their liking. During the development and validation phases, it's common for users to want to either back up their current setup or revert to the original PACEdge state.

The backup procedure allows the user to create a copy of the PACEdge software with their own customizations, flows, views, databases, Connext, and WebHMI projects, including the Linux operating system. This step might be useful for creating an operational backup or duplicating the existing setup onto several additional systems.

Users can use the restore procedure to restore PACEdge either to its Factory Default state or to a previously saved backup. Restoring to the Factory Default state can also be used to upgrade PACEdge to the latest version, where it is acceptable to overwrite any user-specific data on the old unit. Additionally, the backup/restore procedure can also be used to create a golden setup image, which can then be restored to multiple other PACEdge devices. This process even allows for migration between IPC models, for example, from an RXi2-BP to an IPC6010 or vice versa.

Note: Restoring the device will result in the erasure of all current data, including databases and license files. To avoid losing important information, please ensure the backup of critical data using the procedures documented in *the section. 4.1.3, Restoring a Backup.*

Note: This procedure shows how to recover the PACEdge software installation back to Factory Default; however, if the user has entered UEFI setting menus and modified UEFI settings, these will remain as is (applicable to RXi2-BP and IPC6010/7010/8010 hardware). To restore UEFI settings to Factory Defaults, enter the UEFI Settings menu and choose the recovery option on the Save & Exit page.

Based on the hardware type, please refer to the applicable sections below.

5.1 PACEdge Software Backup on RXi2-BP, IPC6010/7010/8010 IPCs

From the Emerson Software Downloads site, download **PACEdge v3.0.0 Backup Restore Install RXi2-BP IPC6010/7010/8010** (file name: **PEv300BRIUtilBP.zip**). Then follow the steps below to perform a backup:

1. Obtain an empty USB storage device with a minimum capacity of 32 GB. Ensure the device is empty, as existing files may cause conflicts.

   Note: If using old USB storage devices, one might experience a problem in which a device may not boot from the USB storage device. This is typically due to the file system incompatibility and boot record configuration on the USB storage device. If this occurs, try one of the following workarounds:

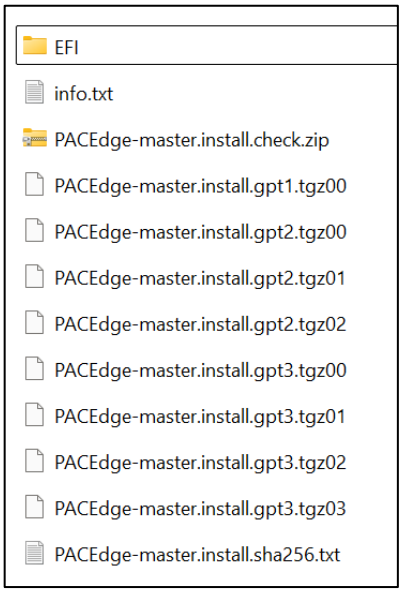
   a. Use a new USB storage device

   b. Reformat the device using the FAT32 file system

   c. Download a Linux installation ISO image and use a Windows utility such as **Rufus** to create a bootable USB storage device. After the process completes, delete all files from the USB storage device and proceed with the next steps.

2. Copy all extracted files to the **root directory** of the USB storage device. The directory structure should appear as follows:

Figure 90: Files at the Root Directory of the USB storage device



Note: Double-check if the automatic PACEdge Factory Image install is disabled; otherwise, it will automatically overwrite all your data and install a Factory Default PACEdge image. To check:

a. In Notepad or a similar editor, open file: `EFI\BOOT\unattendedinstall`

b. Look at the top of the file for a line **action=" install"** or **action=" backup."** Make sure this line is commented out with **#** in front of it. This way, the utility will stop and ask you what operation should be executed.

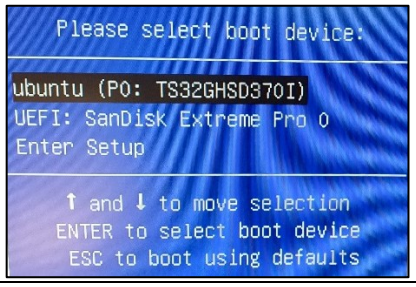
Figure 91: Line=" backup"

```
# action: action to perform
# if set no user input is required
# valid values: "backup", "restore", "install"
# default: not set (== user needs to select action in gui)
# action="backup"
```

c. Make any necessary changes and save the modified file.

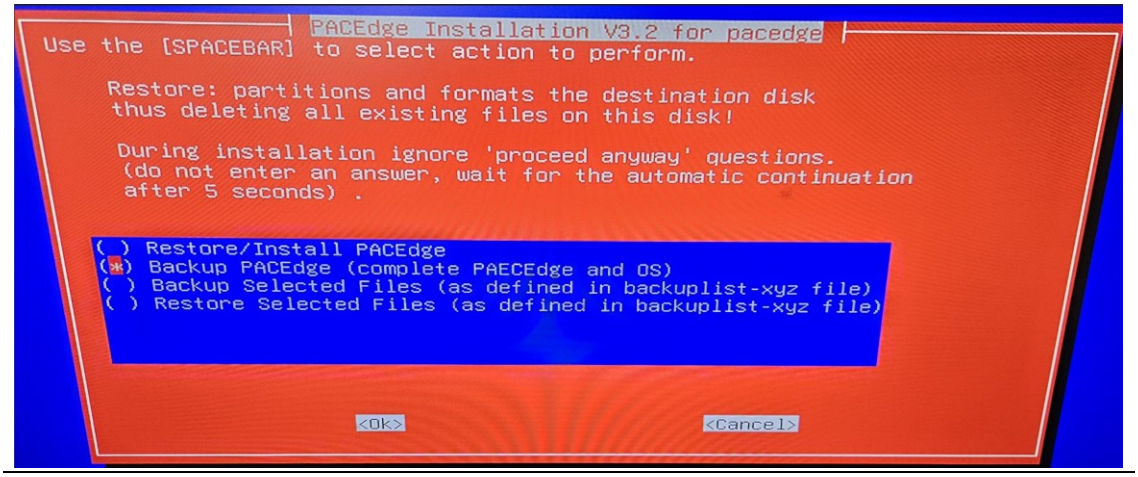
2. Plug the USB storage device into any of the USB ports, power up the IPC, and keep pressing the F7 button to get into the boot selection menu; select the USB storage device to boot from (in the figure below, this would be the second line item: **UEFI: SanDisk Extreme Pro 0**)

Figure 92: Select the Boot Device



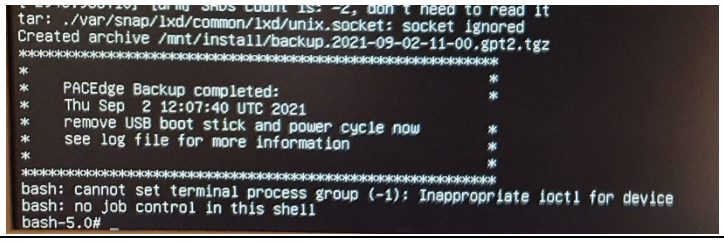
3. Wait until the following dialog appears. Use the arrow keys to move the cursor and the space key to select the **Backup** option. Then use the Tab key to move the cursor to the **OK** button and hit Enter.

Figure 93: Select the Backup Option



4. Wait for the completion message as shown below. Depending on the hardware type, creating a backup might take 10 to 90 minutes.

Figure 94: Backup Completed Screen



Note: After the backup, on the USB storage device, you will see the second set of installation files with the word **backup** in them.

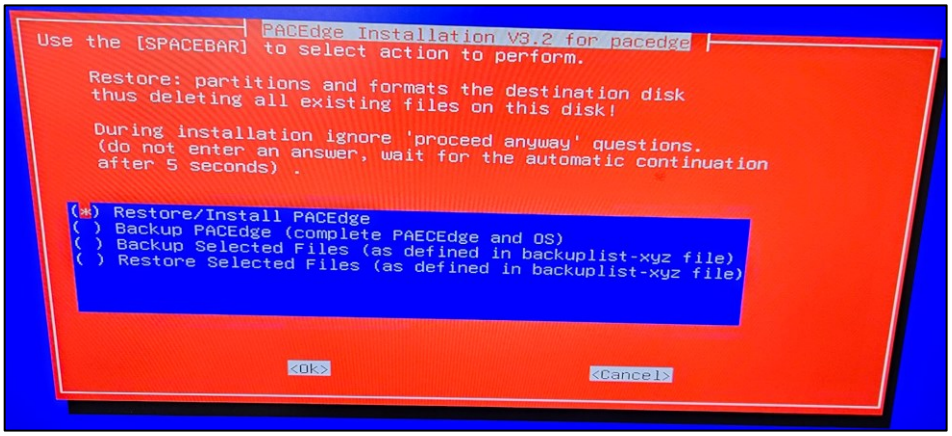
5.2 PACEdge Software Restore/Recovery on RXi2-BP, IPC6010/7010/8010 IPCs

To restore PACEdge software, either to your previously made backup or to the Factory Default (Recovery), please perform the following steps:

1. Perform steps 1-5 in *Section 5.1 PACEdge Software Backup on RXi2-BP, IPC6010/7010/8010 IPCs.*

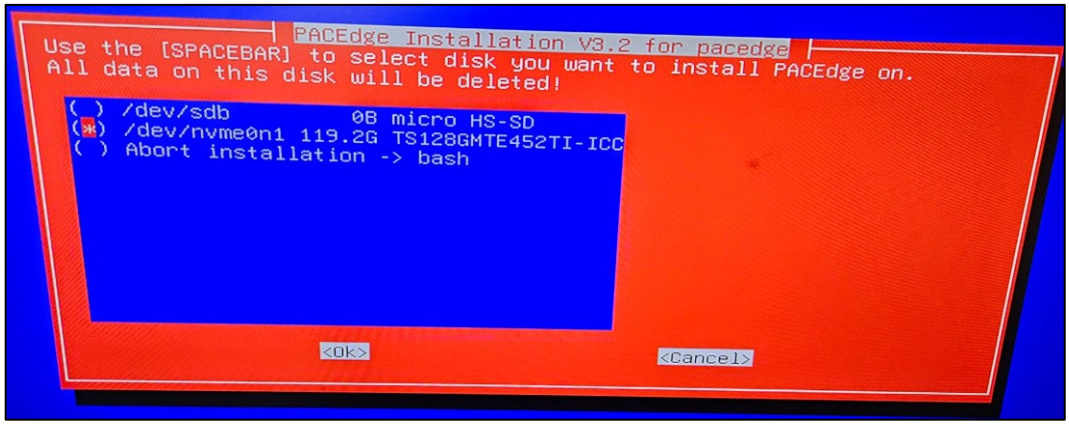
2. Wait until the following dialog appears, and then use the arrow keys to move the cursor and the space key to select the applicable option:
   Choose the **Restor/Install PACEdge** option when restoring a previously backed-up version on the same hardware unit.
   Then use the Tab key to move the cursor to the **OK** button and hit Enter.

Figure 95: Select the Restore/Install option



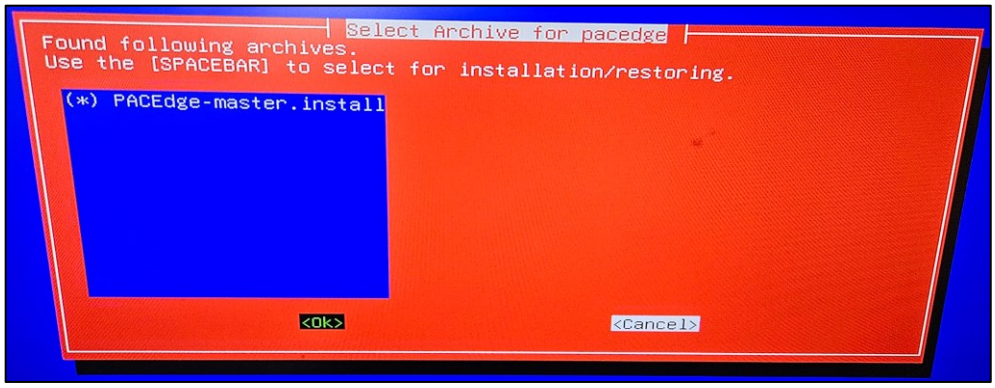
3. If asked for a disk partition, use the arrows, space, and Tab keys to select the main (largest) partition listed and click **OK** to proceed.

Figure 96: Select the Disk Partition (If Applicable)



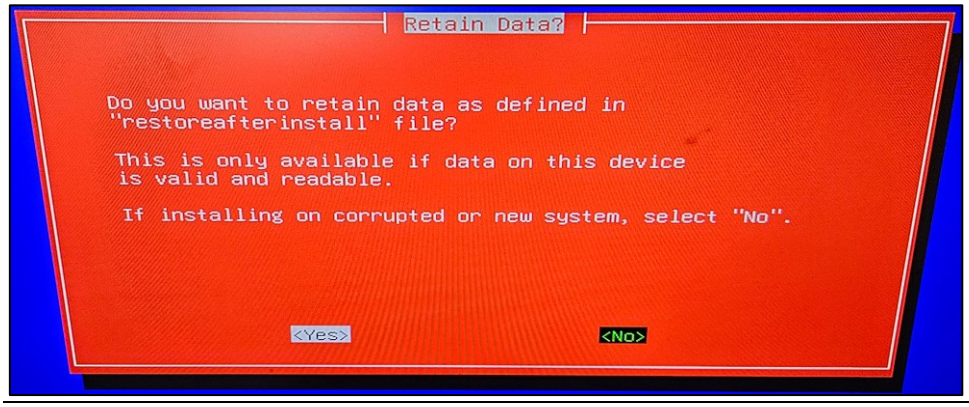
5. If you have previously created a device backup, it will show up here. Use arrows, Space, and Tab keys to select either a factory default image (**PACEdge-master.install**) or one of your backups, then choose **OK** and hit enter.

Figure 97: Select the Backup (if created) or Factory Default Image



6. The last step is an option to back up and then restore certain user files (such as Node-RED flows, etc). To take advantage of this option, first, a **restoreafterinstall** file needs to be created and placed on the USB stick in the root directory. This is a text file that simply lists file paths that the system would first back up onto the USB stick, then install the specified image, deleting all previous data, and then restore specified files from the USB stick to the system. This is helpful if you want to perform a Factory Default Restore, but do not want to lose your Node-RED flows, as an example.
   Note: this option only works if the file system is still readable.

Figure 98: Option to Backup and Restore user files



Example content of a **restoreafterinstall** file:

Figure 99: Example of the Restoreafterinstall File Content

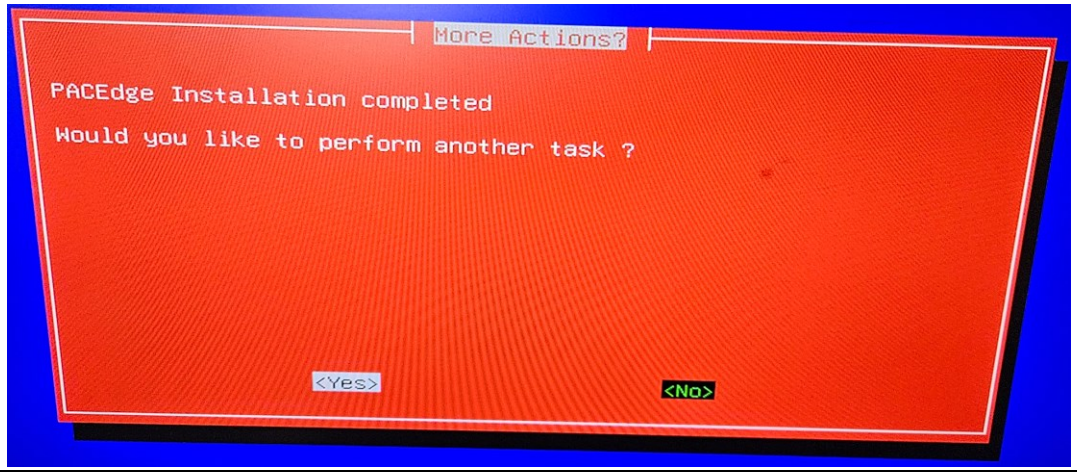
```
# This file contains a list of files or directories which are to be backed up before PACEdge is installed.
# After the PACEdge installation theses files are automatically restored in the new installation.
# This can be useful in the case of a reinstallation of PACEdge, if files from the old installation are to
# continue to be used in the new installation (e.g. Node-RED flows).
# If a listed file does not exist, PACEdge installaton is aborted unless strictbackup="no" is defined
# in the unattendedinstall file.
# Comment lines start with a #
# Absolut path must be defined for files and directories
# e.g.

/home/admin/docker/volumes/pacedge_nodered/_data/flows.json
```

7. Wait until the restore procedure completes, as indicated by a message. When asked if you want to perform another task, respond as No and then reboot the system.
   Note: during the installation process, please ignore any questions that might come up on the screen, letting them time out and continue. No user intervention is required.

Note: Depending on the HW type, this step may take anywhere from a couple of minutes to 10-20 minutes.

Figure 100: PACEdge Restore Completed



8. When restoring from the backup image or performing a recovery to the factory default image, a new license will be required. Perform the following steps:
   a. First, go to the Cockpit-> Navigator and navigate to the /home/admin/ folder.
   b. Switch on the **show hidden** files option in the bottom right corner of the screen.
   c. Delete file folder: **.hasplm**. Confirm recursive delete operation.

d. Generate hardware fingerprint and install new license, as described in 3.5 PACEdge License File

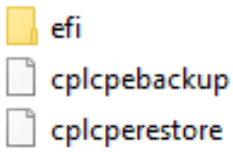
NOTE: After PACEdge restore, you might have to upload the Movicon project (if used) by using Movicon.NExT Editor.

5.3 PACEdge Software Backup on CPL410, CPE400 Controllers

To perform a PACEdge software backup, from the Emerson Software Downloads site, download **PACEdge 3.0.0 Backup Restore CPL410 CPE400** (file name: **PEv300BRUtilCPL.zip**).
Please use the following procedure to perform a backup:

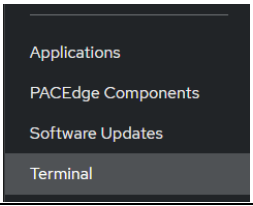
1. Copy the files to an empty USB storage device. Make sure the USB stick is formatted as FAT32. The following are the required files:

Figure 101: Copy Files to USB storage device



2. Insert USB-Stick into CPL/CPE, USB1 port.
3. Mount the USB storage device in Linux OS as described in **7.2 Mounting a USB Storage** Device
4. Now, within the Cockpit, go to the Terminal screen and enter the following commands:

Figure 102: Cockpit's Terminal

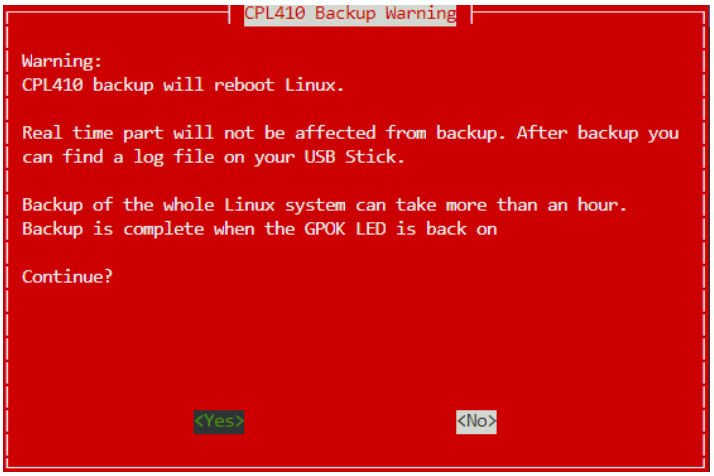


a. **cd /mnt/usb/**
b. **sudo ./cplcpebackup**

c. Enter the admin password if asked for.

5. Using the arrow keys, select **Yes** and press **Enter**.

Figure 103: Select the Backup



6. When the backup starts, the GPOK LED will turn off. It will remain off until the backup is complete, the PACEdge side of the controller is rebooted, and the GPOK LED is ON. It might take close to 2h to perform a backup. You can observe the SSD LED, and as long as it periodically flashes backup process is in progress.

Before removing the USB storage device, please properly un-mount it by the following procedure in ***7.3* Unmounting USB Storage Device**

7. At this point, you can remove the USB storage device and inspect the content on Windows PC. It will have several large archives with names starting with backup.

5.4 PACEdge Software Restore/Recovery on CPL410, CPE400 Controllers

5.4.1 CPL410, CPE400 PACEdge Recovery to Factory Default

CPL410 and CPE400 have a pre-installed Factory Default image. If Factory Default recovery is needed, please follow the steps below. Switching to the Factory Default image will delete all existing data, including Node-Red flows, Grafana views, and database content, including the license.

1. Using CPL410/CPE400 built-in display trigger Reset to Factory Default process:

   a. Press the DISP button until the arrow points at the menu entry: **Edge Settings**, then press SEL.

b. Press the DISP button until the **Commands** option is selected, then press SEL.

c. Press the DISP button until the **Factory Reset** option is selected, then press SEL.

d. Press the DISP button until the **OK** option is selected, then press SEL.

2. At this point, the GPOK LED will go OFF, and you need to reboot the complete unit by removing and applying power again. After the unit is up again, check the update status via the display:

    a. Press the DISP button until the **Edge Settings** option is selected, then press SEL.

    b. Check that the message **Resetting GP** is shown. Also, a blinking SSD LED will indicate that the recovery is in progress.

3. Wait until the GPOK LED turns ON. This can take up to 20 minutes.

4. Next, a new hardware fingerprint will have to be generated and a license file installed. Perform the following steps:

    a. First, go to the Cockpit-> Navigator and navigate to the /home/admin/ folder.

    b. Switch on the **show hidden** files option in the bottom right corner of the screen.

    c. Delete file folder: **.hasplm**. Confirm recursive delete operation.

    d. Generate hardware fingerprint and install new license, as described in 3.5 PACEdge License File

5. At this point, Factory Default restore is done.

5.4.2 CPL410, CPE400 Restore of PACEdge Backup Image

If a PACEdge backup image was created, it could be later restored on the same HW family unit (meaning CPL410 to CPL410 or CPE400 to CPE400). If restoring to a physically different unit, new valid licenses will be required afterward to activate the PACEdge.

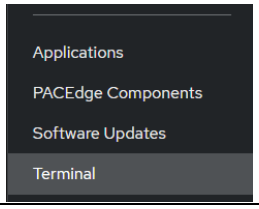
Note that the backup restore operation will overwrite all existing data, including Node-Red flows, Grafana views, and database content.

To perform a PACEdge software restore from the backup, use the same USB storage device that was used to create a backup. Please use the following procedure to perform a restore

1. Insert USB-Stick into CPL410/CPE400, USB1 port.

2. Mount the USB storage device in the Linux OS as described in **7.2 Mounting a USB Storage** Device
3. Now, within the Cockpit, go to the Terminal screen and enter the following commands:

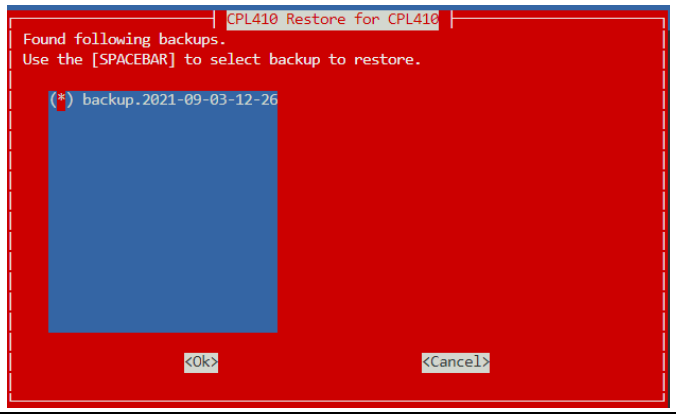
Figure 104: Cockpit's Terminal



   a. **cd /mnt/usb/**
   b. **sudo ./cplcperestore**
   c. Enter the admin password (if applicable).

4. Using the arrow keys, select **Yes** and press **Enter.**
5. Using arrow keys and space keys, mark the backup image you would like to restore, then with the Tab key, select OK and **enter**.

Figure 105: Select the Backup File



6. When restore starts, the GPOK LED will turn off. It will remain off until the backup is complete, the PACEdge side of the controller is rebooted, and the GPOK LED is ON. Restore can take up to 1h to complete. Observe the SSD LED on the front panel; if it periodically flashes, the Restore operation is in progress.
7. Before removing the USB storage device, please properly unmount it by following the procedure in Section *7.3 Unmounting USB Storage Device.*
8. Remove the USB storage device.

9. Next, a new hardware fingerprint will have to be generated and a license file installed. Perform the following steps:
    a. First, go to the Cockpit-> Navigator and navigate to the /home/admin/ folder.
    b. Switch on the **show hidden** files option in the bottom right corner of the screen.
    c. Delete file folder: **.hasplm**. Confirm recursive delete operation.
10. Generate a hardware fingerprint and install a new license, as described in 3.5 PACEdge License File

NOTE: After PACEdge restore, you might have to upload the Movicon project (if used) by using Movicon.NExT Editor.

5.5 PACEdge 3.0.0 Software Backup on IPC 2010

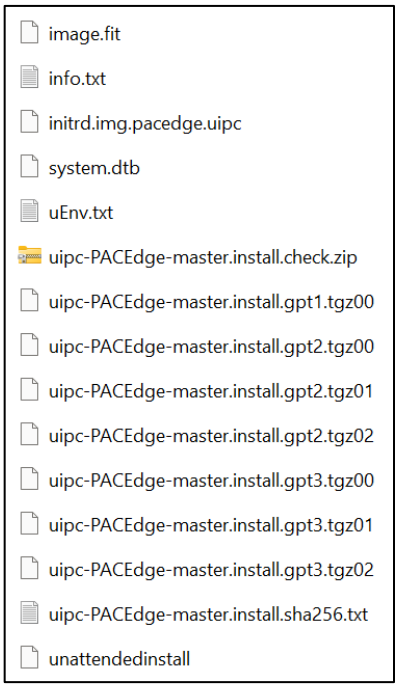
To perform Backup/Restore operations on the IPC 2010, an off-the-shelf serial cable will be required. Cable pinout is defined in 7.4, Serial RS232 Cable for IPC 2010.

Download file PACEdge 3.0.0 Backup Restore Install IPC2010 (**PEv230BRIUtilIPC2010.zip**) from the Emerson Customer Support Center site, then follow the steps below to perform a backup:

1. Insert a USB storage device with a minimum of 32 GB of storage into the USB port. Ensure the storage device is empty, as otherwise, conflicts may arise.

    Note: If using an old USB storage device, one might experience a problem in which the device may not boot from the USB storage device. This is typically due to the file system changes and boot record configuration on the USB storage device. The workaround, in this case, is either: 1) use a brand new USB storage device, 2) format USB stick using FAT32 file system, 3) download from the Internet one of Linux installation ISO images, use a Windows utility such as Rufus, to make a bootable USB storage device, then delete all the files from the USB storage device and proceed with next steps.
2. Copy all files to the root directory of the USB storage device. The directory structure should look like this:

Figure 106: Files at the Root Directory of the USB storage device



Note: Double-check if the automatic PACEdge Factory Image install is disabled; otherwise, it will automatically overwrite all your data and install a Factory Default PACEdge image. To check:

a. In Notepad or a similar editor, open file: **unattendedinstall**

b. Look at the top of the file for a line **action=" install"** or **action=" backup."** Make sure this line is commented out with **#** in front of it. This way, the utility will stop and ask you what operation should be executed.

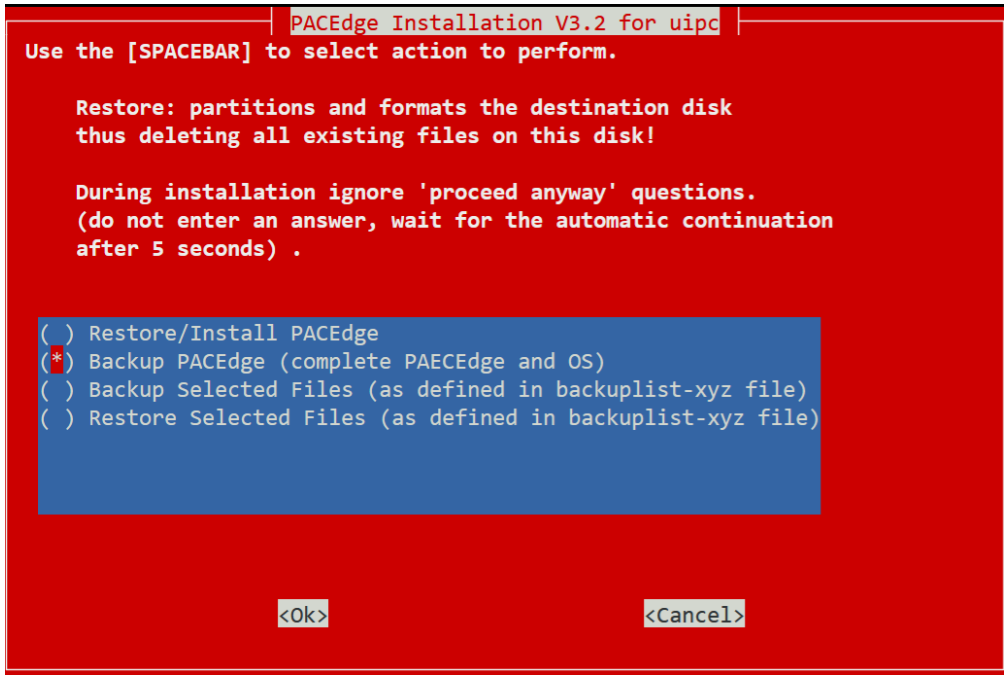
```
# action: action to perform
# if set no user input is required
# valid values: "backup", "restore", "install"
# default: not set (== user needs to select action in gui)
# action="backup"
```

c. Make changes as necessary and save the modified file.

3. Connect the serial cable between the IPC 2010 RS232 connector and your PC's serial port. For cable details, refer to: 7.4 Serial RS232 Cable for IPC 2010.

4. Plug the USB storage device into any of the USB ports, power up the IPC, and wait until the following screen appears:

Figure 107: IPC 2010 Backup Operation Selection



5. Using the space bar, mark the entry: Backup PACEdge, then using the Tab key, highlight (turns black) the OK button and hit the Enter key.

6. Wait until backup is complete (can take 2-3 hours)
7. Remove power and USB storage device. Now, the USB storage device contains a backup image of your IPC 2010.

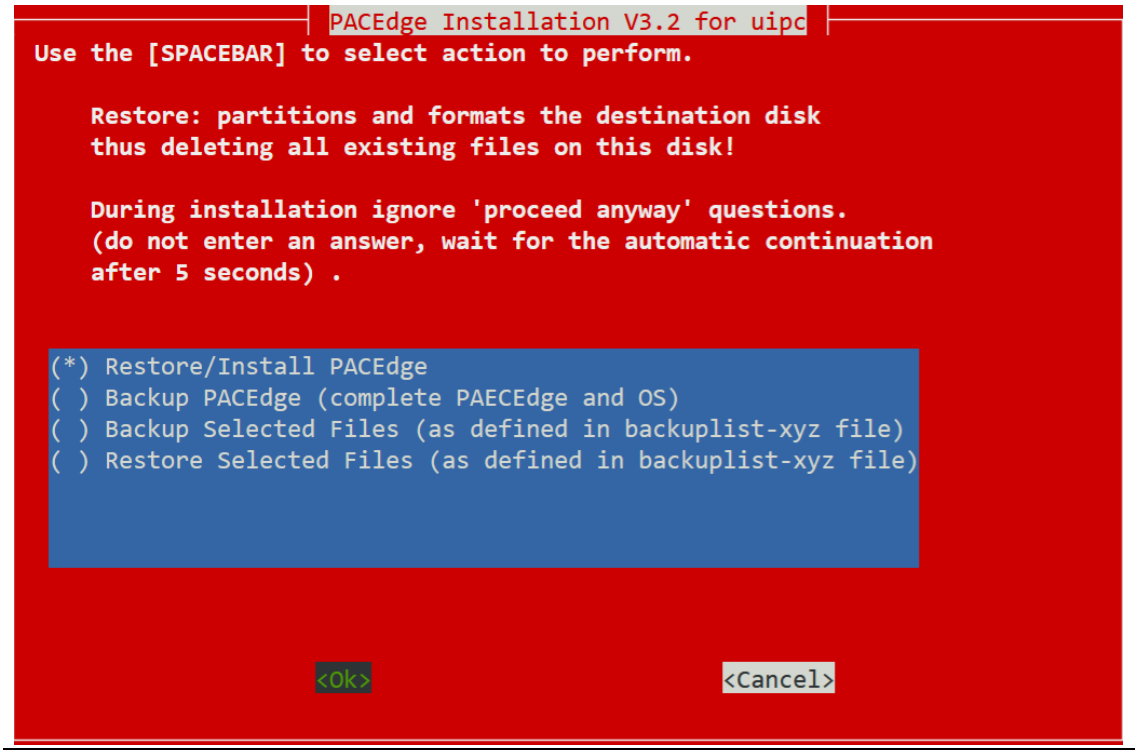
5.6 PACEdge Software Restore/Recovery on IPC 2010

To restore a previously backed-up image of IPC 2010 or to recover to Factory Default installation, you will need a serial cable and a USB storage device with software. Prepare a USB stick as described in the 5.5 PACEdge 3.0.0 Software Backup on IPC 2010. If you are performing a backup restore, then use the same USB storage device you used for the backup.

Then, perform the following steps:

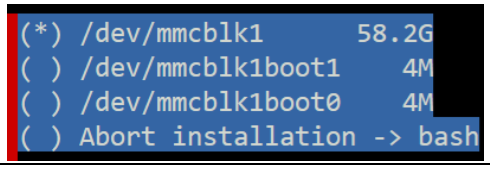
1. In the first screen, using arrow keys and the space bar, mark the first entry that says: Restore/Install PACEdge, then highlight OK and hit Enter. Note: Please use this entry for both Restore and Recovery operations

Figure 108: IPC 2010 Selecting Restore/Install Option



2. Next, in the screen that appears, using the arrow keys and the space bar, mark the entry that corresponds to the internal disc (typically the third entry that is close to 60GB in size). Highlight OK and hit the Enter key

Figure 109: IPC 2010 Disc Partition Selection Screen 4

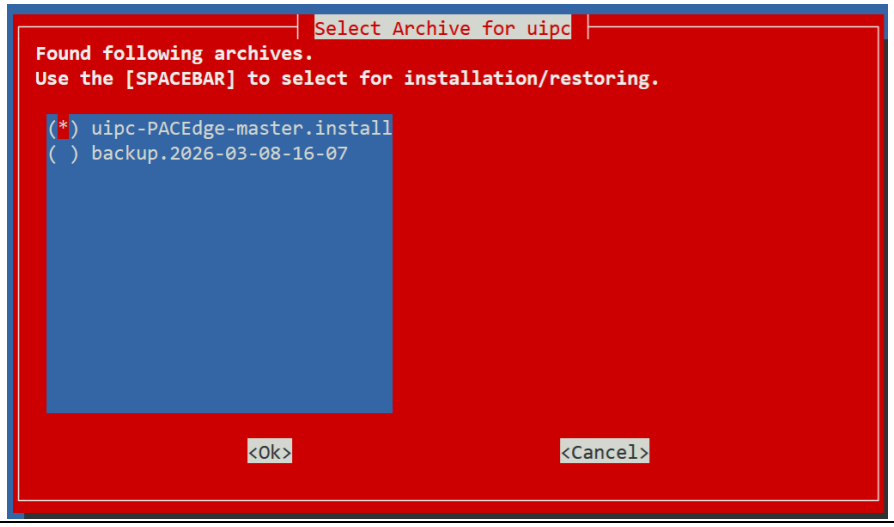


3. In the screen that appears, mark the image that you want to restore.

    a. In case you want to perform Factory Default recovery, please select uIPC-PACEdge-master.install. Note: All your existing data on the IPC 2010, including license file, will be overwritten, and the unit will be reset to factory defaults. You will have to request and install a new license file.

    b. In case you want to perform a restore from a backup operation, please select one of the images that you have previously backed up. Backup images have the word “backup” and the time of the backup in the file name.

Figure 110: Select Archive



c. Highlight the OK option and hit the enter key to proceed. Next, the screen asking if you want to back up and restore specific files appears. To take advantage of this option, first, a **restoreafterinstall** file needs to be created and placed on the USB stick in the root directory. This is a text file that simply lists file paths that the system would first back up onto the USB stick, then install the specified image, deleting all previous data, and then restore specified files from the USB stick to the system. This is helpful if you want to perform a Factory Default Restore, but do not want to lose your Node-RED flows.
Note: this option only works if the file system is still readable

Figure 111: Screen Asking if Specific Files Should be Backed up and Restored

Figure 112: Example of the restoreafterinstall file content

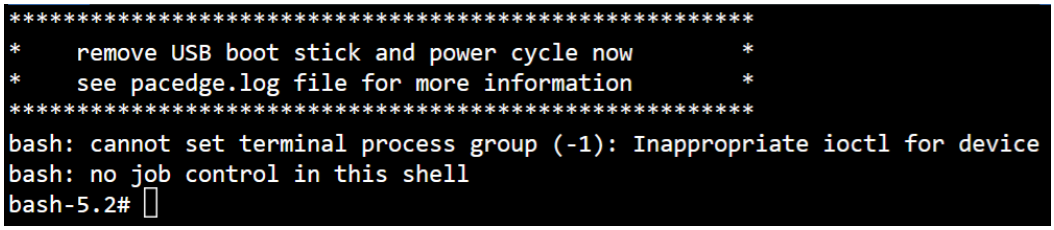
```
# This file contains a list of files or directories which are to be backed up before PACEdge is installed.
# After the PACEdge installation theses files are automatically restored in the new installation.
# This can be useful in the case of a reinstallation of PACEdge, if files from the old installation are to
# continue to be used in the new installation (e.g. license files).
# If a listed file does not exist, PACEdge installaton is aborted unless strictbackup="no" is defined
# in the unattendedinstall file.
# Comment lines start with a #
# Absolut path must be defined for files and directories
# e.g.

/home/admin/pacedge/emerson-software/license
```

Once installation is finished, the following screen will be shown. Please select option No and hit enter. Once the command line prompt shows up, remove the power and the USB storage device, then reapply power to boot the new image.

Figure 113: IPC 2010 Restore/Recovery Finished Screen

Figure 114: Installation Complete Screen



d. Next, a new hardware fingerprint will have to be generated and a license file installed. Perform the following steps:

   i. First, go to the Cockpit-> Navigator and navigate to the /home/admin/ folder.

   ii. Switch on the **show hidden** files option in the bottom right corner of the screen.

   iii. Delete file folder: **.hasplm**. Confirm recursive delete operation.

   iv. Generate hardware fingerprint and install new license, as described in 3.5 PACEdge License File

Section 6: PACEdge Version Update

6.1 Upgrading to PACEdge v3.0.0

PACEdge v3.0.0 is a new major PACEdge software release. It includes newly redesigned PACEdge services infrastructure, a new GUI, and is based on the newer Linux 24.04 operating system. Therefore, an upgrade to v3.0.0 from an older PACEdge will require installing a new software image, overwriting the old image.

NOTE: Data loss. Since the installation of v3.0.0 will overwrite everything on the system, user data loss might occur. Make sure to first back up all user data (Node-RED flows, Grafana dashboards, databases). You will have to manually restore this data after installing PACEdge v3.0.0

NOTE: PACEdge v3.0.0 is using a new licensing mechanism, which will require a new license to be created and installed on each device. License generation is a two-step process: 1) Generate a hardware fingerprint file and send it to Emerson tech support, 2) Install a license file onto the device. For detailed instructions, please refer to: 3.5 PACEdge License File

The installation process will require creating a USB stick with the provided software, then booting from this stick and executing installation steps. For most of the hardware options (excluding CPL410/CPE400), installation of PACEdge v3.0.0 is identical to the Factory Default Recovery procedure. Follow the links below for the instructions:

6.1.1 Upgrading IPC6010/7010/8010 or RXi2-BP to v3.0.0

Follow the procedure in *Section 5.2 PACEdge Software Restore/Recovery on RXi2-BP, IPC6010/7010/8010 IPCs.*

6.1.2 Upgrading IPC2010 to v3.0.0

Follow the procedure in *Section 5.6 PACEdge Software Restore/Recovery on IPC 2010.*

6.1.3 Upgrading CPE400 or CPL410

When upgrading CPE400 or CPL410, download software from the Emerson Customer Software Center called: PACEdge 3.0.0. Install CPL410 CPE400 (**PEv300InstUtilCPL.zip**)

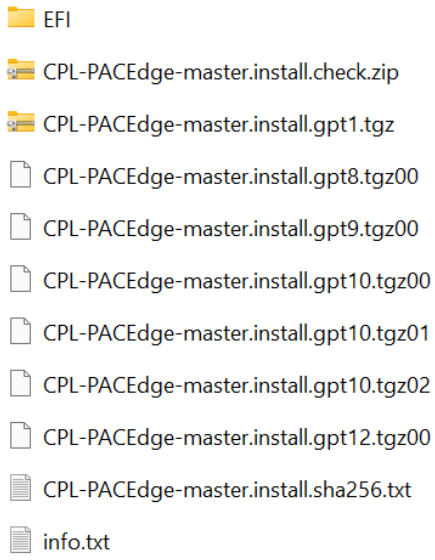
Get an empty, min 32 GB USB storage device. Make sure it is empty, as conflicts might arise.

Note: if using old USB storage devices, one might experience a problem in which a device may not boot from the USB storage device. This is typically due to the file system

incompatibility and boot record configuration on the USB storage device. The workaround, in this case, is either: 1) use a brand new USB storage device, 2) change format to FAT32, 3) download from the Internet one of Linux installation ISO images, use a Windows utility such as Rufus, to make a bootable USB storage device, then delete all the files from the USB storage device and proceed with next steps.

Copy all files to the root directory of the USB storage device. The directory structure should look like this:

Figure 115: Files at the Root Directory of the USB storage device



Insert the USB stick into one of the USB ports on the device and apply power. The device will automatically boot from the stick and perform installation. The end of the installation process will be indicated by LEDs on the device running from the edges into the middle.

Remove the USB stick and cycle the power.

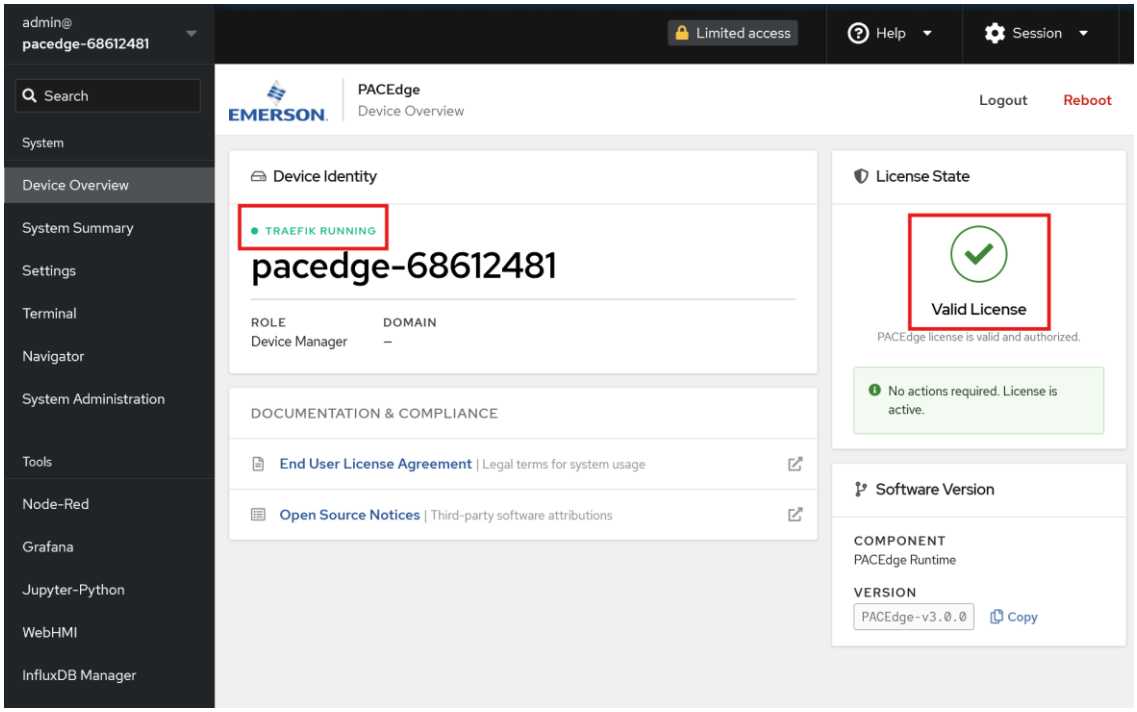
Section 7: Utilities and Troubleshooting

7.1 PACEdge Health Diagnostics

7.1.1 Checking if Services are Running

In case of difficulties reaching some of the PACEdge services, such as Node-RED, verify that the reverse proxy service Traefik is running. To do so, go to Cockpit->Device Overview and check if the " Traefik Running message is shown and if the license is valid:

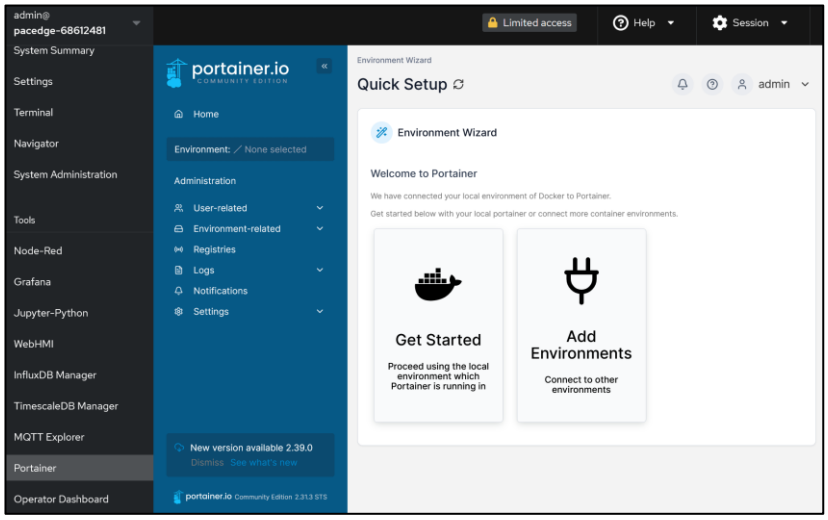
Figure 116: PACEdge Device Overview Page



7.1.2 Checking Individual Services

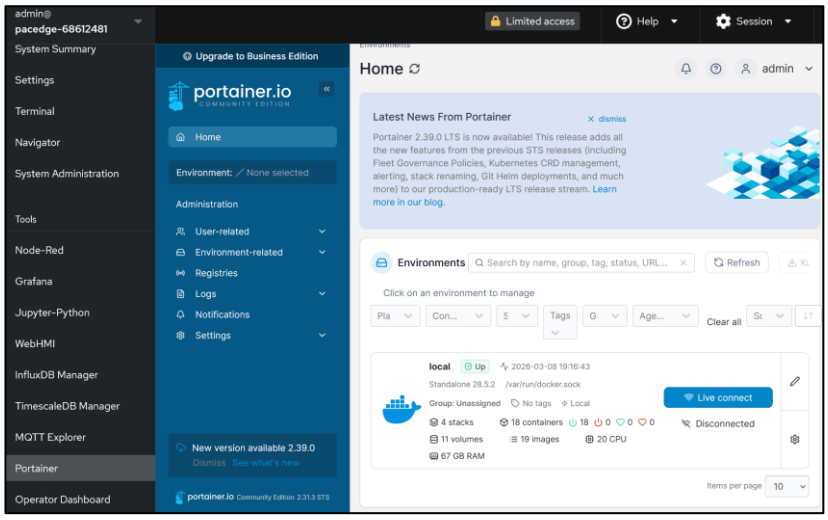
If some of the PACEdge services are malfunctioning, more information can be obtained by using Portainer. To do so, navigate to *Cockpit->Portainer* and log in with admin credentials.

Figure 117: Portainer Starting Page



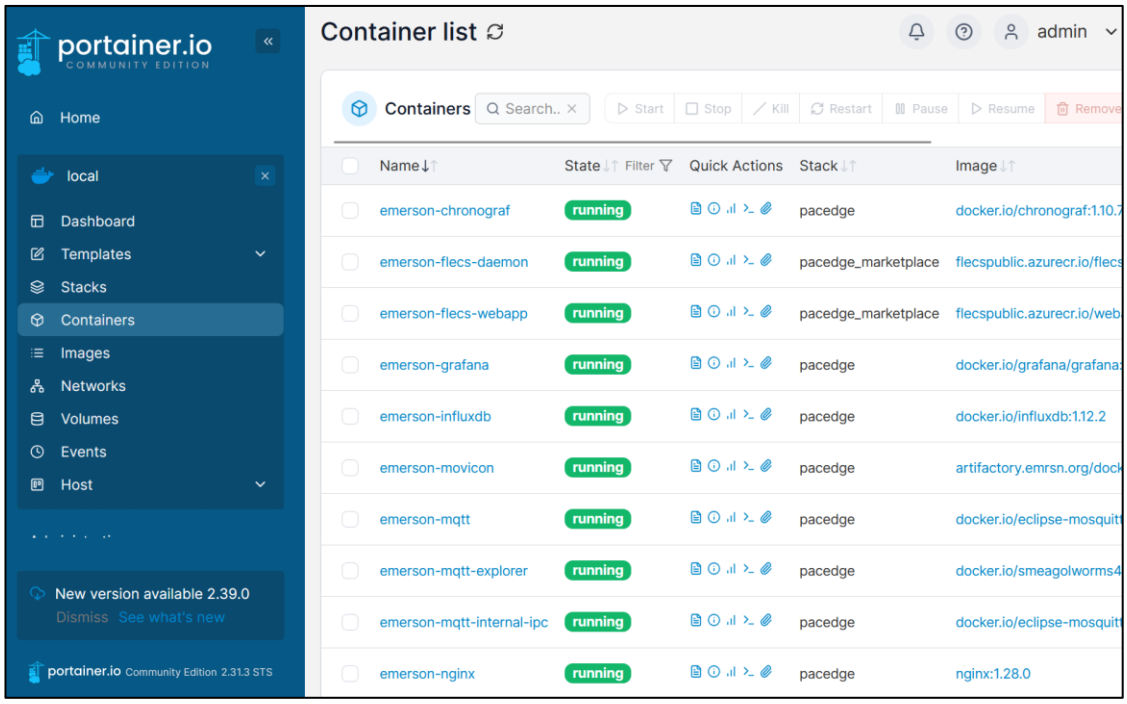
1. Click on Get Started and then click on the **Live Connect** button:

Figure 118: Portainer Connecting to Local Services



2. Click on the **Containers** button to see the list of all services and their statuses. The user can review the details by going into a specific service, such as Node-RED.

Figure 119: Portainer List of Services



7.1.3 Group Manager - Device Connectivity Diagnostics

Group Manager controls multiple devices and requires that the devices are reachable via IP and SSH protocols. At the same time, devices shall be able to reach the Group Manager. To test this connectivity, consider the following steps:

From Group Manager Ping Each Device

Open *Cockpit->Terminal* on the Group Manager and issue: **ping xxx.xxx.xxx.xxx**, where x is the IP address of the device.

From each device, ping the Group Manager.

Open Cockpit->Terminal on each device and issue: **ping xxx.xxx.xxx.xxx**, where x is an IP address of the GM.

Test SSH into the Device

Open Cockpit->Terminal on GM and issue: ssh admin@xxx.xxx.xxx.xxx, where x is the IP address of the Device. Use the Linux admin password to log in.

7.1.4 Group Manager – Marketplace Connectivity Diagnostics

Group Manager pulls software updates from the online marketplace and therefore requires internet connectivity. Internet connection might have configuration issues, especially when Group Manager is running as a virtual machine on the server. In case *Group Manager-> Update Groups-> Pull Latest Updates* fails, check that the online Marketplace is reachable from the Group Manager. Only the Group Manager requires internet connectivity. The devices connected do not. To test, perform the following steps:

Open *Cockpit->Terminal* on the Group Manager and enter the command:

Figure 120: Testing Marketplace Name Resolution

```
admin@localhost:~$ getent hosts flecs.blob.core.windows.net
20.60.23.161    blob.fra23prdstr03a.store.core.windows.net flecs.blob.core.windows.net
```

Make sure it returns an IP address. If not, then check the routing table by issuing the command**: ip route.**

Figure 121: Checking Routing Table

```
admin@localhost:~$ ip route
default via 192.168.2.1 dev ens32 proto dhcp src 192.168.2.20 metric 100
default via 192.168.88.2 dev ens33 proto dhcp src 192.168.88.149 metric 101
172.17.0.0/16 dev docker0 proto kernel scope link src 172.17.0.1 linkdown
172.18.0.0/16 dev br-95181de6955d proto kernel scope link src 172.18.0.1
172.19.0.0/16 dev br-baa835c96014 proto kernel scope link src 172.19.0.1
```

If you see multiple default gateways, like in the example above, try deleting one by keeping the primary gateway.

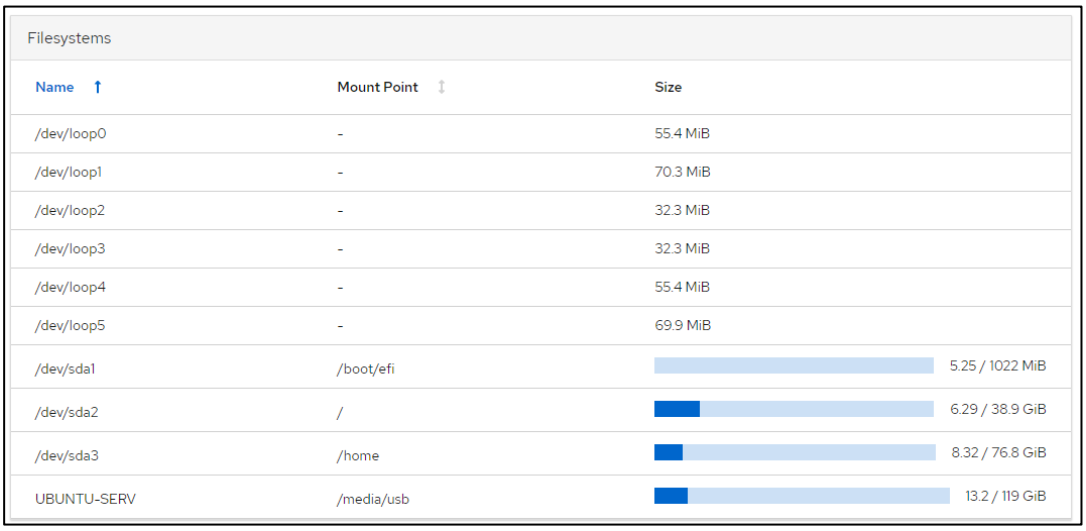
7.2 Mounting a USB Storage Device

PACEdge can read and write data from/to a USB storage device. However, the USB storage device must first be properly mounted in the Linux OS. The procedure to mount a USB storage device is the same for RXi2-BP, IPC6010/7010/8010, IPC2010, CPL410, and CPE400; the only difference between devices will be the disk partitioning scheme that you see in Navigator. Ignore inconsistencies with the images shown below.
To mount the USB storage device, please follow the steps below:

1. Insert the USB storage device into any USB port.
2. Log in to Cockpit as **admin**.
3. Go to the **Storage** tab on the left side of the screen, look for the USB storage device in the list of Filesystems (typically at the very bottom of the list, UBUNTU-

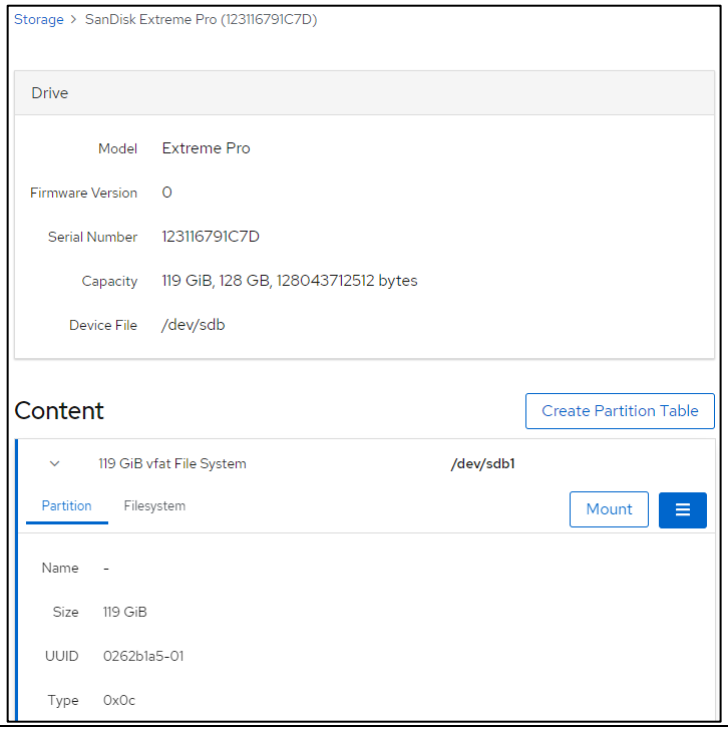
SERV in the example below), and click on it.

Figure 122: List of Filesystems (CPL410, CPE400)



4. On the next page, click to expand the view of the Content and then click on the **Mount** button on the right side of the screen.

Figure 123: Mount the Device



5. In the open dialog, enter Mounting Point**: /media/usb** or **/mnt/usb** and click on the **Mount** button.
   NOTE: By default, the owner of the USB storage device will be **root**. If a specific procedure asks to mount a USB storage device with owner **admin**, please check the **Custom mount options** box and enter **uid=admin** as shown below.

Figure 124: Mount the USB storage device with the owner root

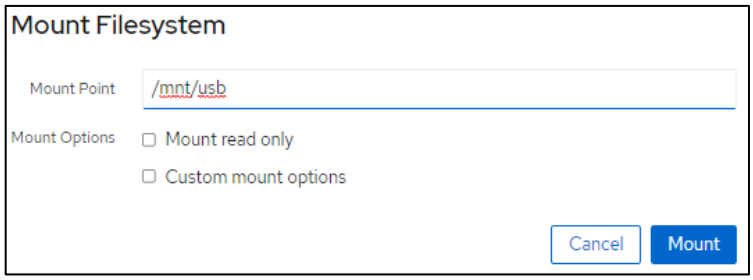
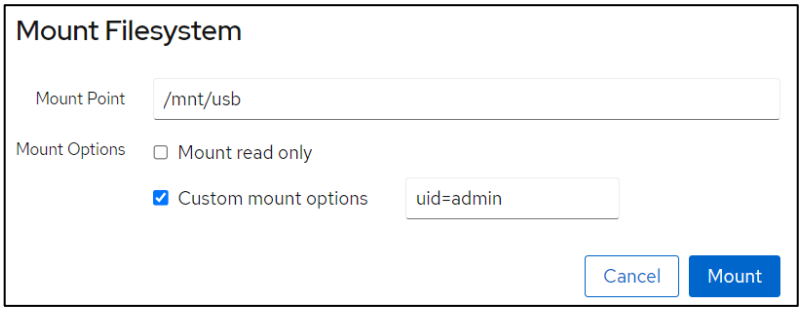
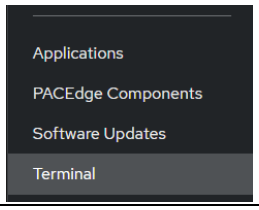


Figure 125: Mount the USB storage device with the owner admin



6. At this point, the USB storage device is mounted and accessible. To see the files, you can use Navigator or go to the Cockpit->Terminal screen and enter the following commands:

Figure 126: Cockpit's Terminal

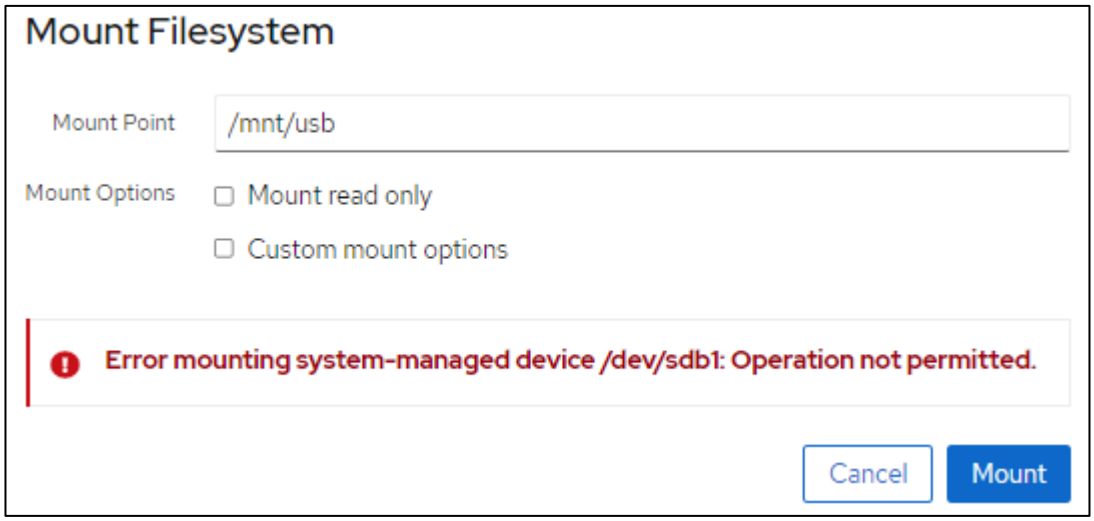


a. **cd /mnt/usb/**

b. **ll**

Note: If the USB storage device has not been properly unmounted in the past, it might lead to an error

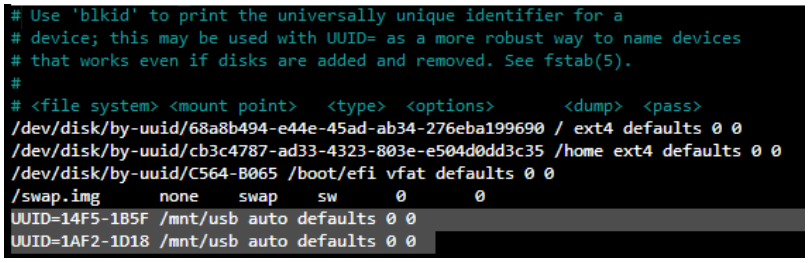
Figure 127: Mount File System



In such a case, entries in the `/etc/fstab` file need to be cleaned up as follows:

a. Log in as **admin** into Cockpit
b. Go to Terminal
c. Type: **sudo nano /etc/fstab**
d. Using arrow keys, move your cursor behind the last character and delete all lines that start with UUID at the end of the file (last two lines in the given example):

Figure 128: Example



e. Press **CTRL+X** key combination, then the **y** key to confirm changes
f. Try to mount the USB storage device again.

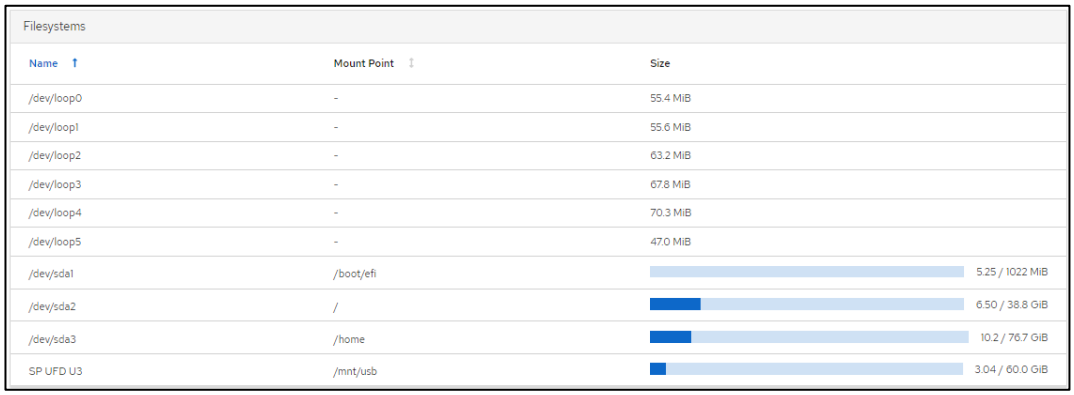
7.3 Unmounting USB Storage Device

In the Linux operating system, it is important to properly unmount the USB storage device before its removal.

To unmount the USB storage device:

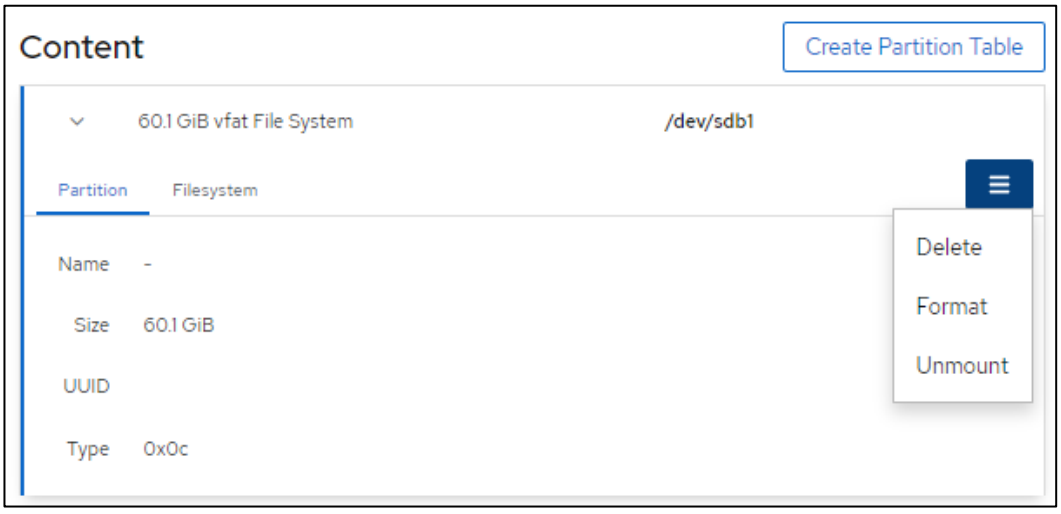
1. In Cockpit, go to the Storage tab.
2. Click on the line that represents the USB storage device. One way to identify it is by Mount Point being `/mnt/usb` or `/media/usb`.

Figure 129: Select Storage to Unmount



3. Next, click on the disc within the Content window to open more details Then, click on the three lines to open options, and then click on **Unmount.**

Figure 130: Unmount Storage



7.4 Serial RS232 Cable for IPC 2010

On IPC 2010, to gain access to the system, utilize the serial console port by connecting it to the host PC's RS232 interface using a null modem cable. Once connected, the host can establish a connection by running a terminal emulator such as HyperTerminal or minicom. The default serial port parameters are **115200, 8N1.**

The connector is RJ-45 style with pinout as defined in EIA/TIA-561, so that off-the-shelf adapters to DB9 or USB can be used.

The pinout for the RJ-45 (8P8C) connector is defined as follows:

Table 6 IPC 2010 Serial Cable Pinout

Signal	RJ-45 Pin
GND	4
RxD	5
TxD	6

7.5 Difficulties Accessing PACEdge Components, Erratic Behavior

- It is always a good first step to reboot the hardware.
- If you can log in, go to Cockpit and analyze the Logs. Logs contain several warnings and notices about different services as part of normal operation, so search for the messages related to the specific problem.
- If you have a problem accessing a specific PACEdge application, say Node-RED, Grafana, or InfluxDB, either log in to Cockpit, go to Docker Containers, or log into Portainer and check the status of the container that hosts the specific application. Clues to look for:
    - Check if the container is not continuously restarting. You can see the last start time in the statement, such as: “Up since Today xxx.”
    - In Portainer, look into the log file specific to each container for further clues.

For technical support, it is helpful to provide an exported Syslog file. To do that, please log in via a terminal window and execute **journalctl > log**.

7.6 PACEdge Files

On Emerson IPCs with preinstalled PACEdge, you will find the PACEdge-Files in the Admin's home directory (*/home/admin/pacedge* and */home/admin/pacedgen*). Expert users can use these files to adapt and modify the PACEdge Docker environment to their needs and stop and start the PACEdge system via the docker-compose command (see below). Normally, there is no need to use these files.

7.7 Docker Commands

PACEdge is heavily based on Docker and Docker application images. Docker is a kind of lightweight virtualization allowing applications to be grouped together in a protected, self-contained environment within the Linux operating system. Setting up and configuring such a set of applications is a complex task whose description is beyond the scope of this document. Fortunately, this arrangement is already mastered by PACEdge, and you only need some commands to manage PACEdge.
PACEdge uses a command-line-based utility to perform different tasks on the PACEdge system. Although most of the tasks are too complex to describe here, two tasks could be helpful when debugging the system

7.7.1 Bringing all PACEdge Services Down

To bring all the PACEdge Services down, so that they can be restarted, use the Terminal and issue the following command: **pacedgectl stack down**

7.7.2 Bringing all PACEdge Services Up

To bring all the PACEdge Services up, so that they can be restarted, use the Terminal issue following command: **pacedgectl stack up**.

Contact Information and Support Guide

Questions? We are here to help.

Before starting a case or making a call, try searching our Knowledge Base on the Customer Center website—it might have the answer you need right away.

If you have a question, try the following steps:

Search our Knowledge Base	Open a Support Ticket	Register for a Customer Account
pacsystems.co/knowledge	pacsystems.co/support	pacsystems.co/signup

Other Helpful Links

Customer Center Home Page	Commercial Website	Contact Information
pacsystems.co/customercenter	pacsystems.co/commercial	pacsystems.co/contactus

Emerson reserves the right to modify or improve the designs or specifications of the products mentioned in this manual at any time without notice. Emerson does not assume responsibility for the selection, use, or maintenance of any product. Responsibility for proper selection, use, and maintenance of any Emerson product remains solely with the purchaser.