Monitoring Port for Vertiv™ Liebert® iCOM™3

Configuration and Usage Reference Manual

The information contained in this document is subject to change without notice and may not be suitable for all applications. While every precaution has been taken to ensure the accuracy and completeness of this document, Vertiv assumes no responsibility and disclaims all liability for damages resulting from the use of this information or for any errors or omissions.

Refer to local regulations and building codes relating to the application, installation, and operation of this product. The consulting engineer, installer, and/or end user is responsible for compliance with all applicable laws and regulations in relation to the application, installation, and operation of this product.

The products covered by this instruction manual are manufactured and/or sold by Vertiv. This document is the property of Vertiv and contains confidential and proprietary information owned by Vertiv. Any copying, use, or disclosure of it without the written permission of Vertiv is strictly prohibited.

Names of companies and products are trademarks or registered trademarks of the respective companies. Any questions regarding usage of trademark names should be directed to the original manufacturer.

Technical Support Site

If you encounter any installation or operational issues with your product, check the pertinent section of this manual to see if the issue can be resolved by following outlined procedures.

Visit https://www.vertiv.com/en-us/support/ for additional assistance.

TABLE OF CONTENTS

This page intentionally left blank

1 Scope

This document describes how to upload and activate a usable monitoring model into the monitoring port of an Vertiv™ Liebert® iCOM™3 controller.

This page intentionally left blank

2 Terms and Abbreviations

Term/Condition	Description
Monitoring port	The Ethernet Gateway card pluggable into the Vertiv™ Liebert® iCOM™3 controller

This page intentionally left blank

3 Hardware Connections

Figure 3.1 Ethernet Connection on Vertiv™ Liebert® iCOM™3 Medium/Large

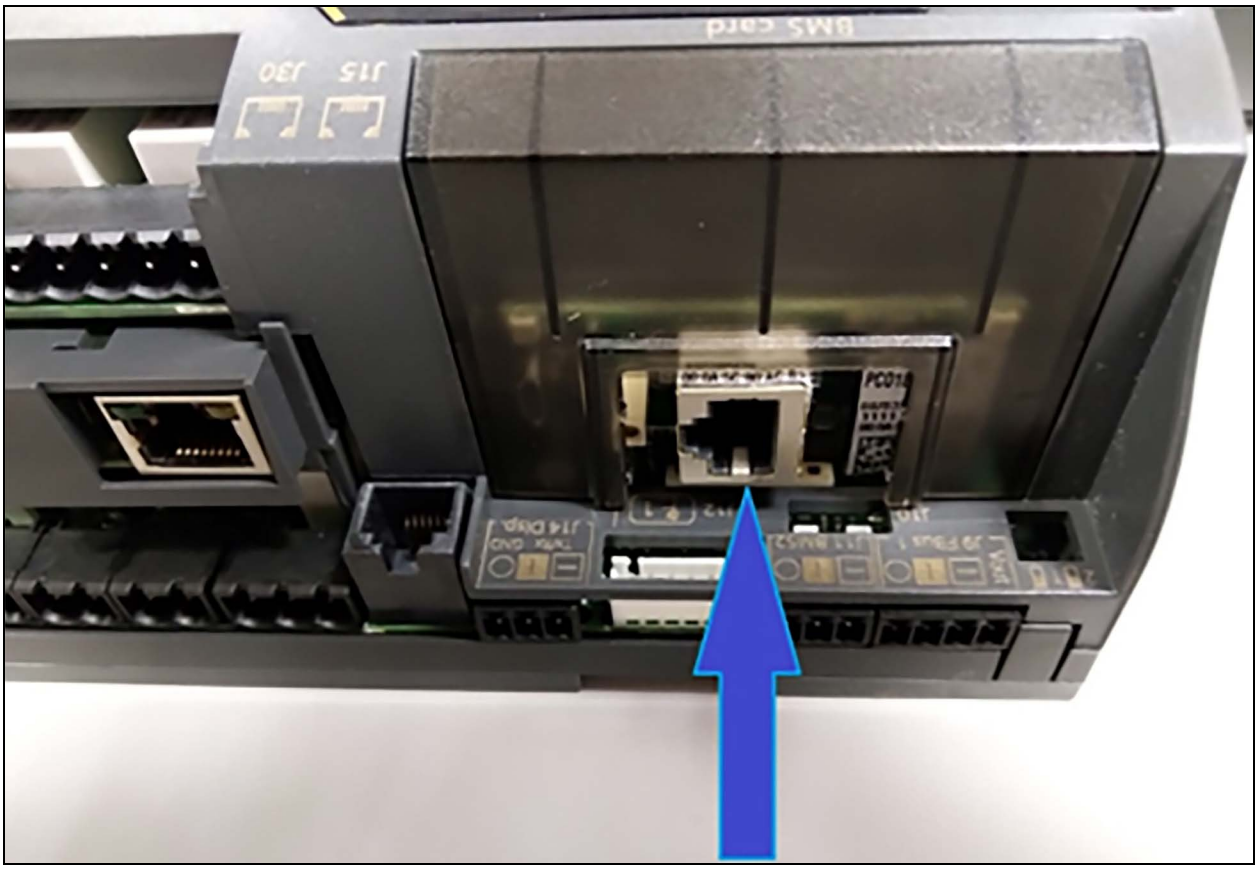
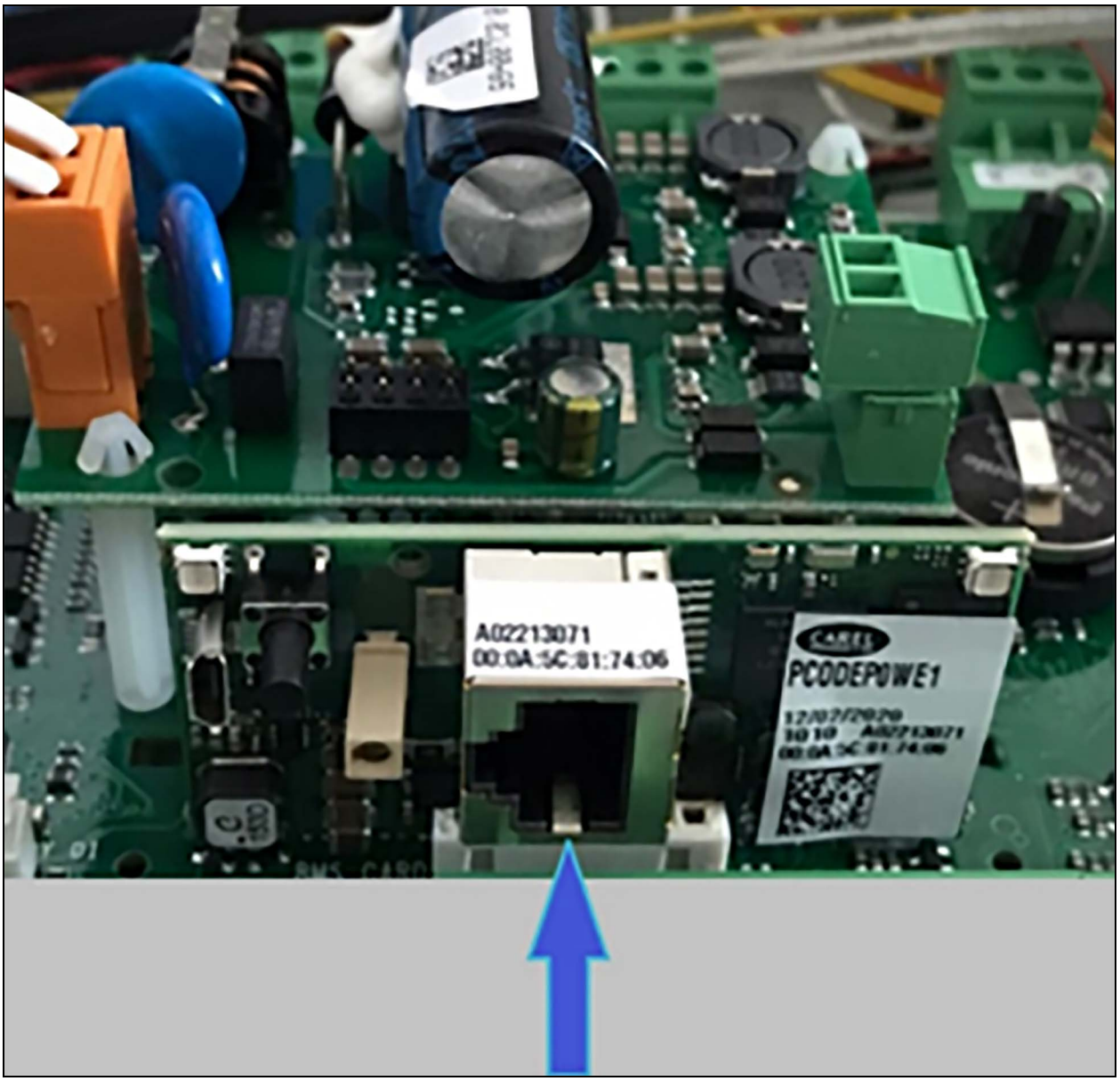


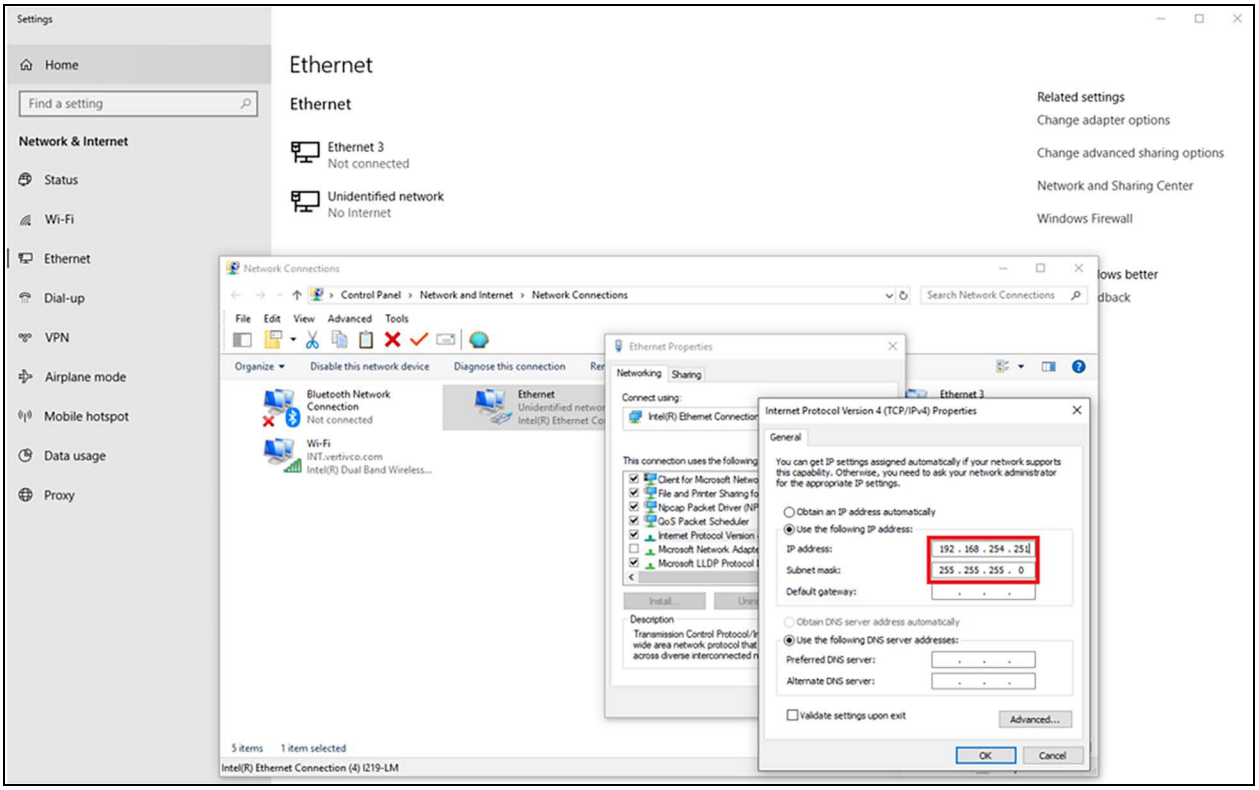
Figure 3.2 Ethernet Connection on Vertiv™ Liebert® iCOM™3 Small



4 Monitoring Port Configuration and Usage

1. Set up an Ethernet port for the PC in order to make a point-to-point connection with the monitoring port Ethernet port (whether it's cross or patch cable) See **Figure 4.1** below .
   - Set IP Address: 192.168.254.251
   - Subnet Mask: 255.255.255.0

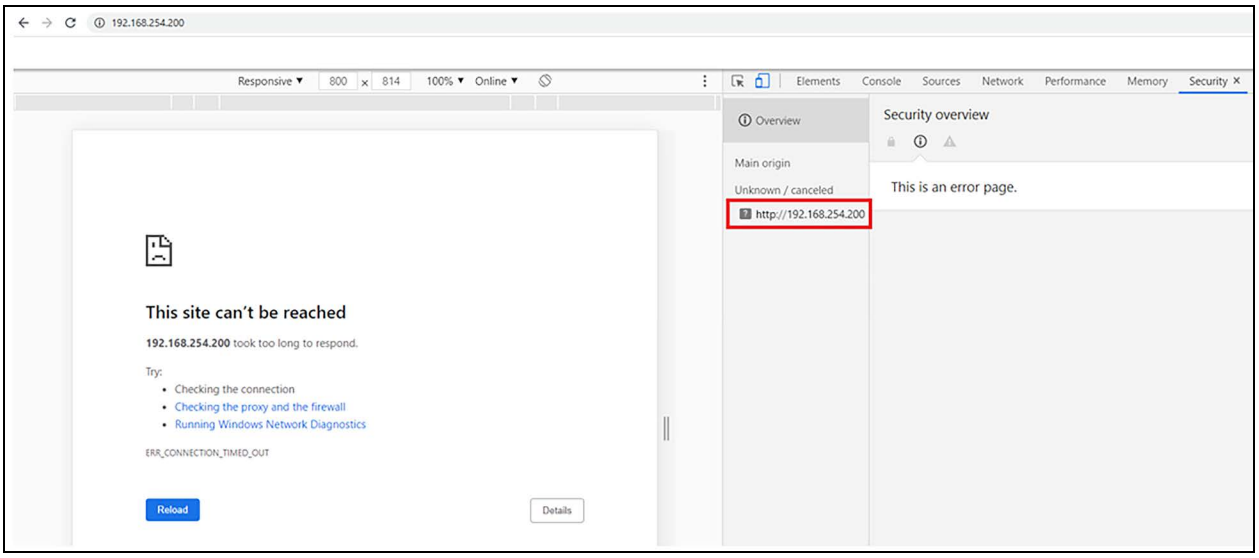
Figure 4.1 Ethernet Port Setup



2. Point to https://192.168.254.200 with the Chrome browser.

NOTE: Pay attention to the https prefix on the address bar, it is necessary to invoke the HTTPS protocol. By default, the browser will activate HTTP and if the IP address is typed without the https prefix, this will result in a refused connection error. See Figure 4.2 on the next page .

Figure 4.2 Connection Error



NOTE: Before the browser can reach the monitoring port web server, it must be up and running. This status is operative five minutes after powering On the board.

3. If the monitoring port is in an unknown state with the Status LED OFF, please power it OFF and ON again (also disconnecting the ultracapacitor if present).

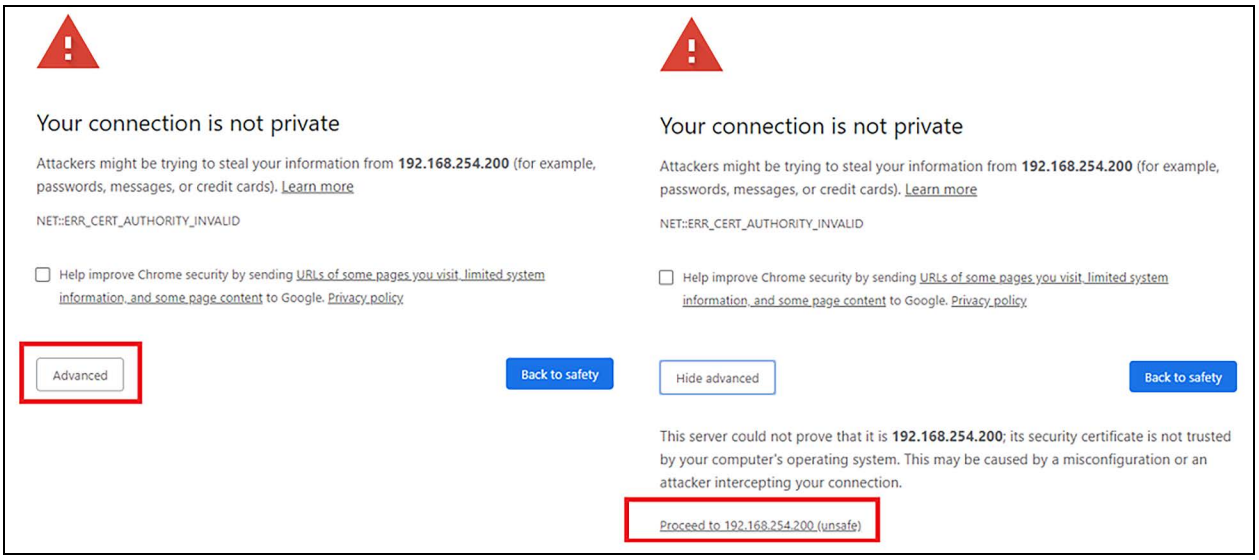
   During the booting process, the LED status changes behavior as shown in Table 4.1 below before the connection is available (timing is approximated).

Table 4.1 LED Status

LED Status	Duration (s)
OFF	5
ON (Light GREEN)	3
Flashing Fast (RED)	3
Fixed ON (GREEN)	12
FLASHING Slow (GREEN)	35
OFF	1:25
FIXED ON	1:30

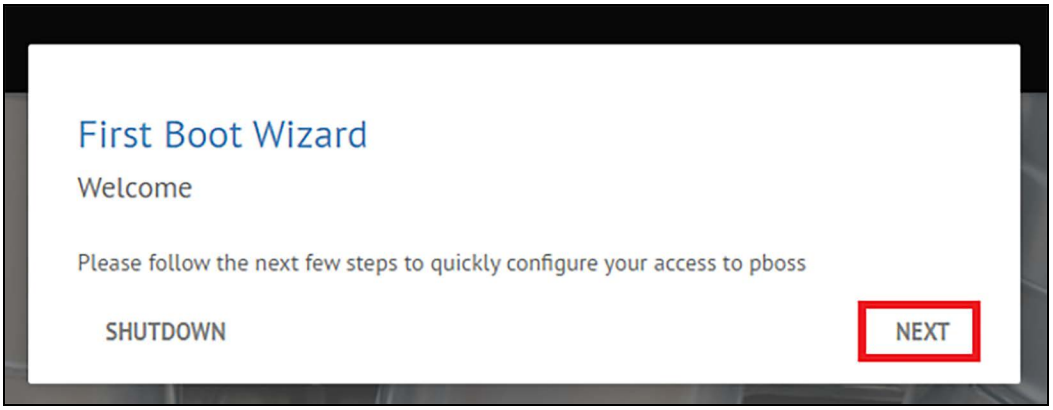
4. Wait for the security protocol handshake, then agree to proceed to potentially unsafe location. See Figure 4.3 on the facing page .

Figure 4.3 Connection not Private



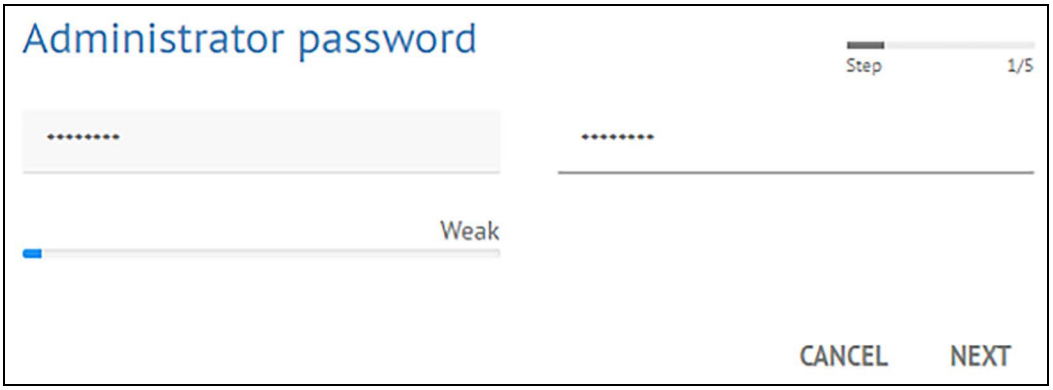
5. Start the First Boot Wizard by clicking Next on the popup window. See Figure 4.4 below .

Figure 4.4 First Boot Wizard Screen



6. Define the Administrator password. See Figure 4.5 below .

Figure 4.5 Administrator Password Setup



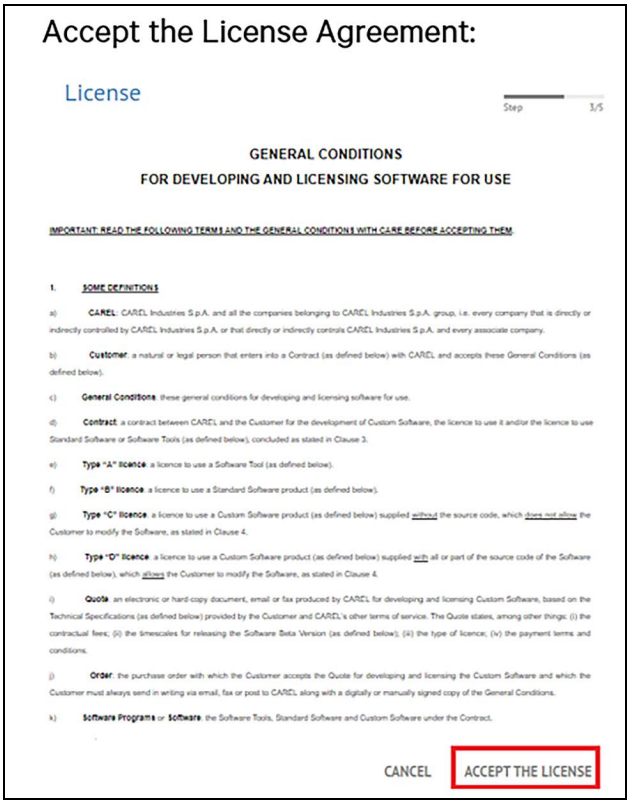
NOTE: Write down the administrator password, considering uppercase letters and special characters. In case of forgotten password, it will be necessary to recover the factory settings. See Restoring Factory Settings on page 30 .

7. Select the Application Language: English. See Figure 4.6 below .

Figure 4.6 Language Setup

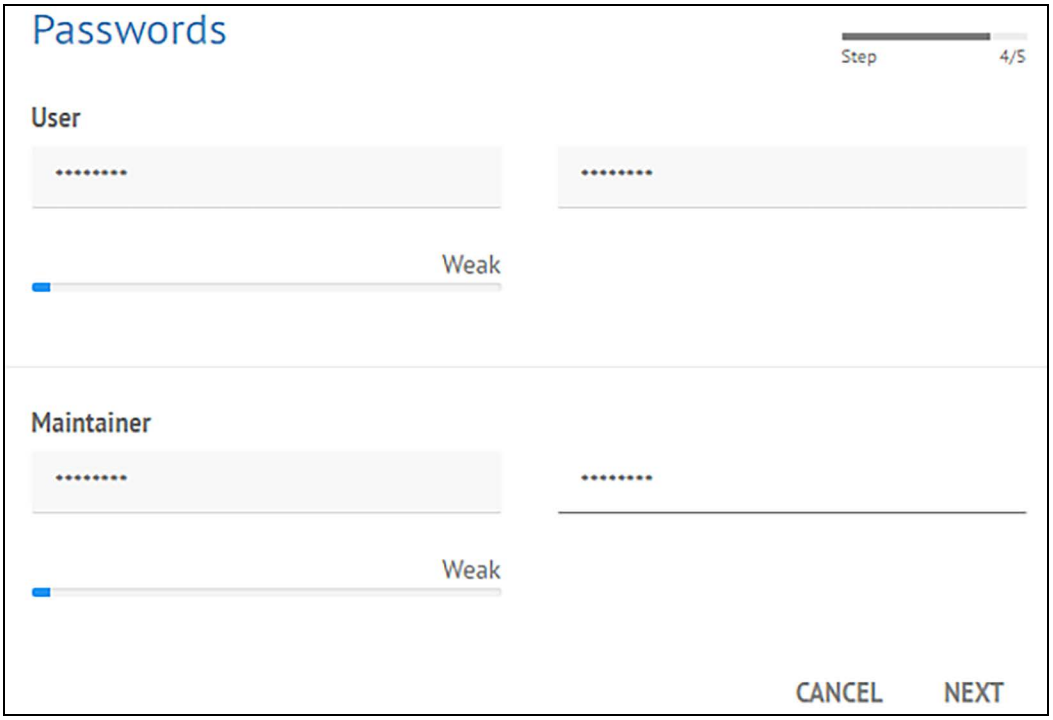
8. Accept the License Agreement. See Figure 4.7 below .

Figure 4.7 License Agreement



9. Set up User and Maintainer passwords. See Figure 4.8 below .

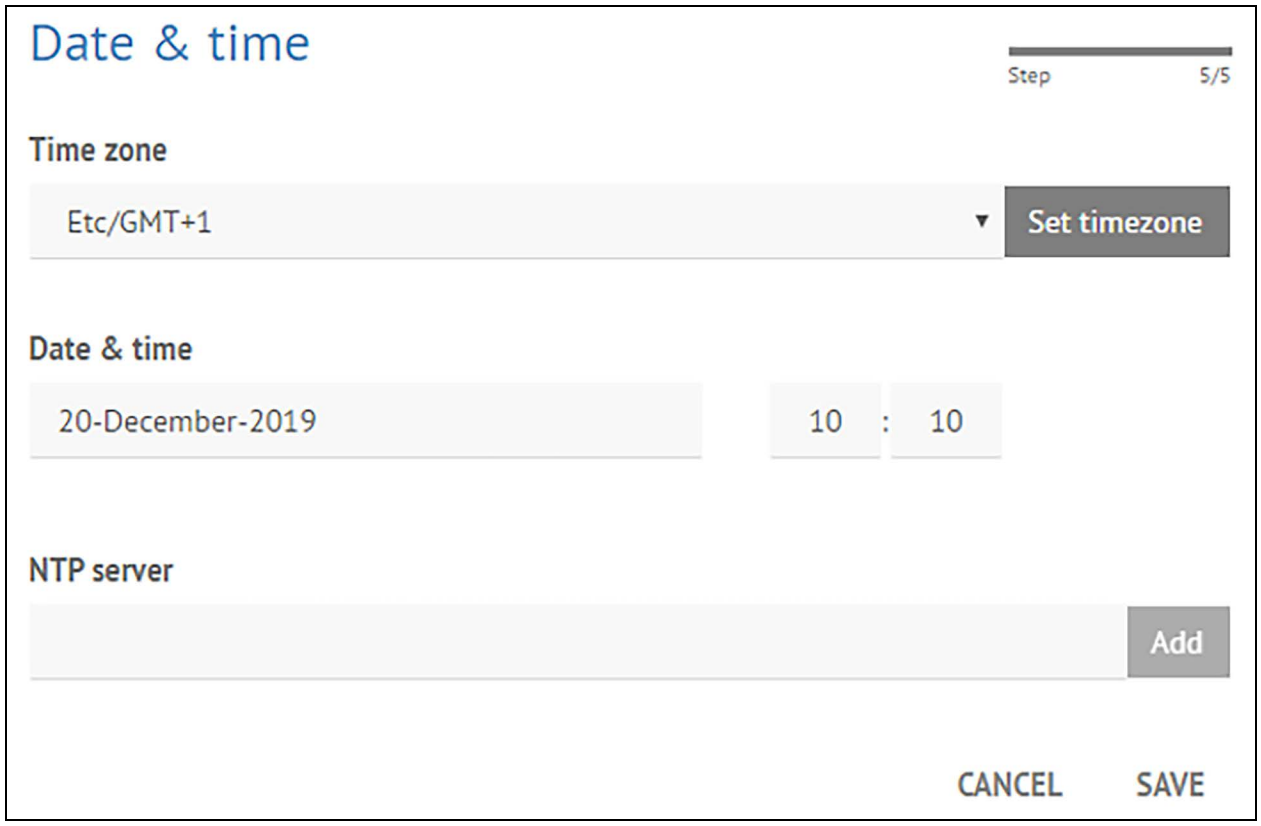
Figure 4.8 Password Setup



NOTE: Do not lose the passwords. There is no way to reset them because there are no default values.

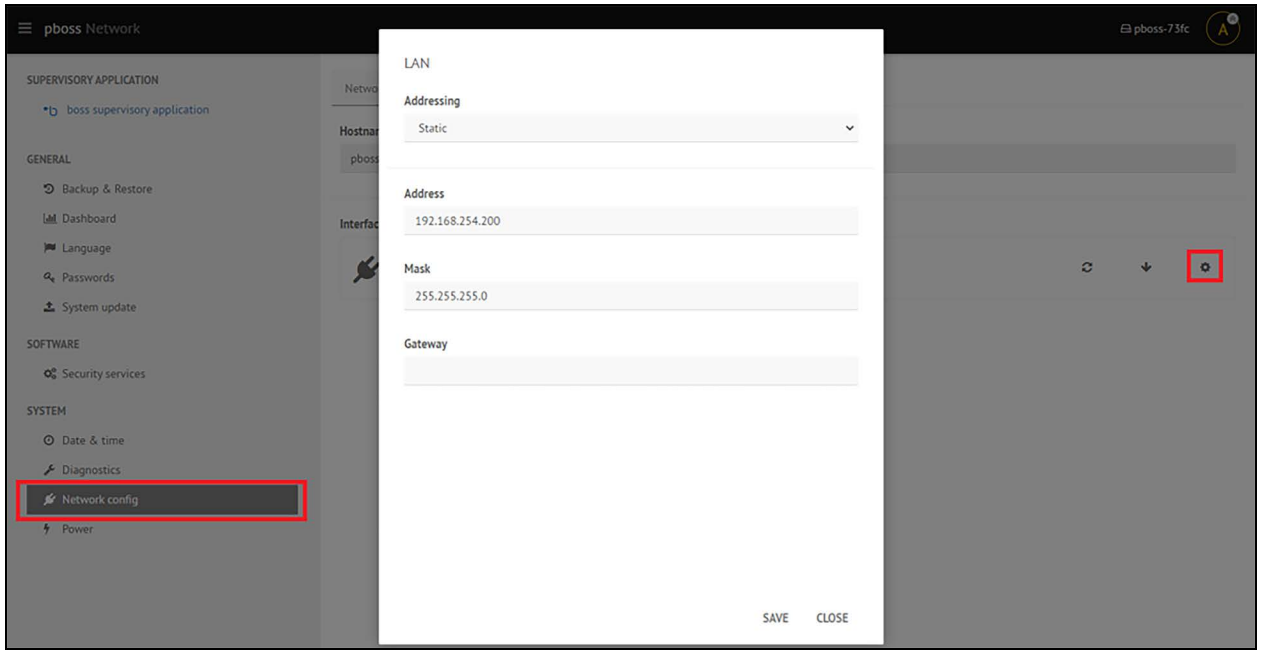
10. Set the Time zone and press Set timezone, then adjust the Date and Time and click SAVE. See Figure 4.9 on the facing page .

Figure 4.9 Set Time Zone, Date, and Time



11. Once re-directed to the Administrator Home page it is possible to change the default IP Address/Netmask/Gateway by clicking on Network config. See Figure 4.10 below .

Figure 4.10 Network Configuration



12. Click on RESTART and then reboot the card to apply the new IP address. See **Figure 4.11** below and **Figure 4.12** below .

Figure 4.11 Network Interface Restart Warning

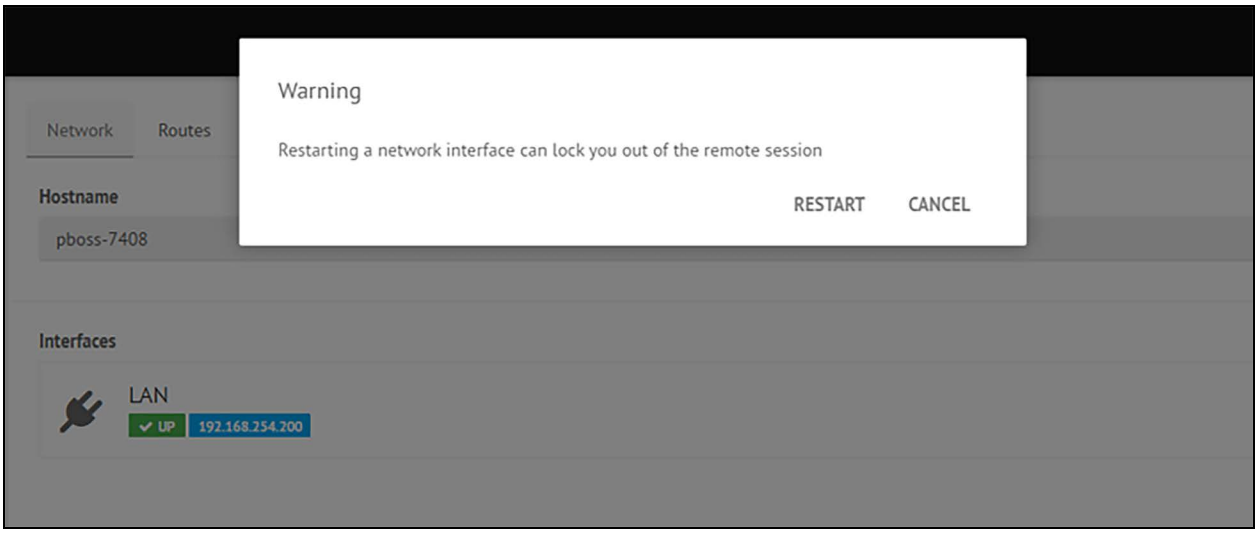
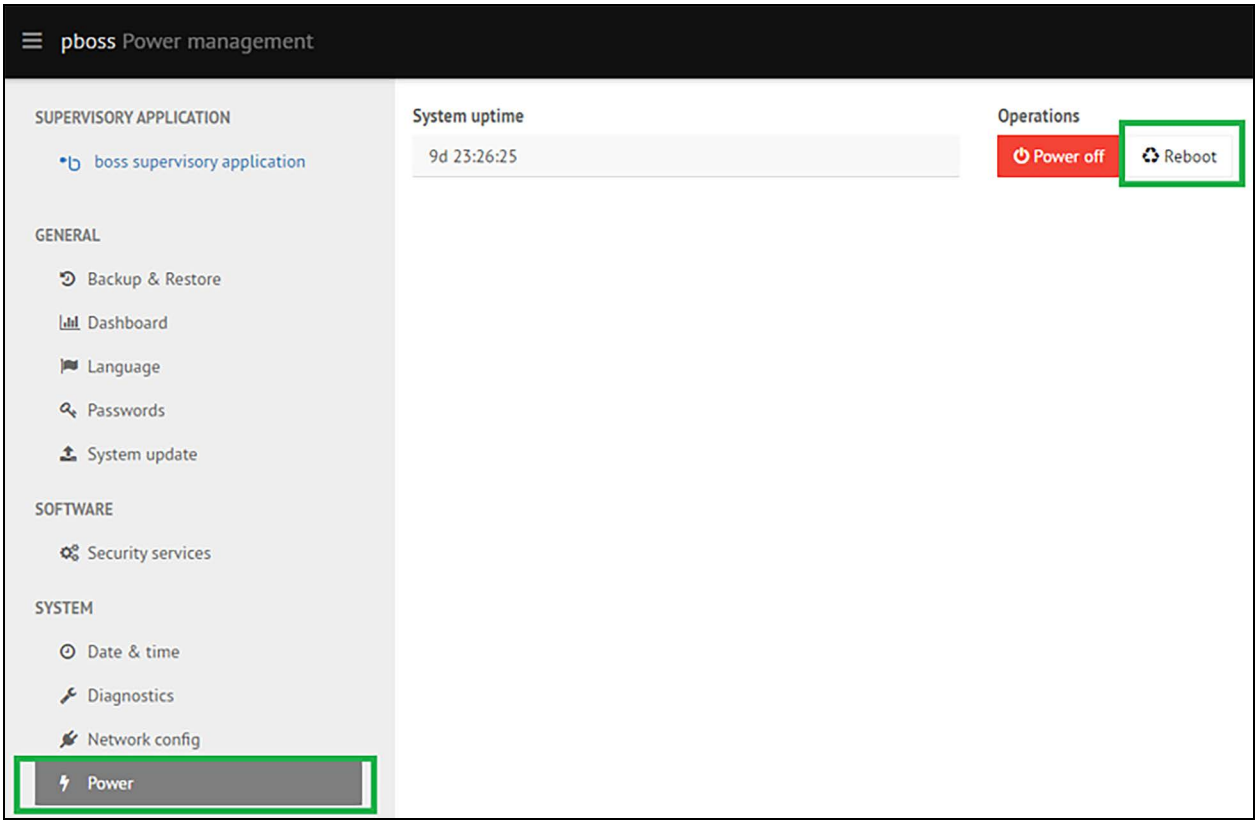
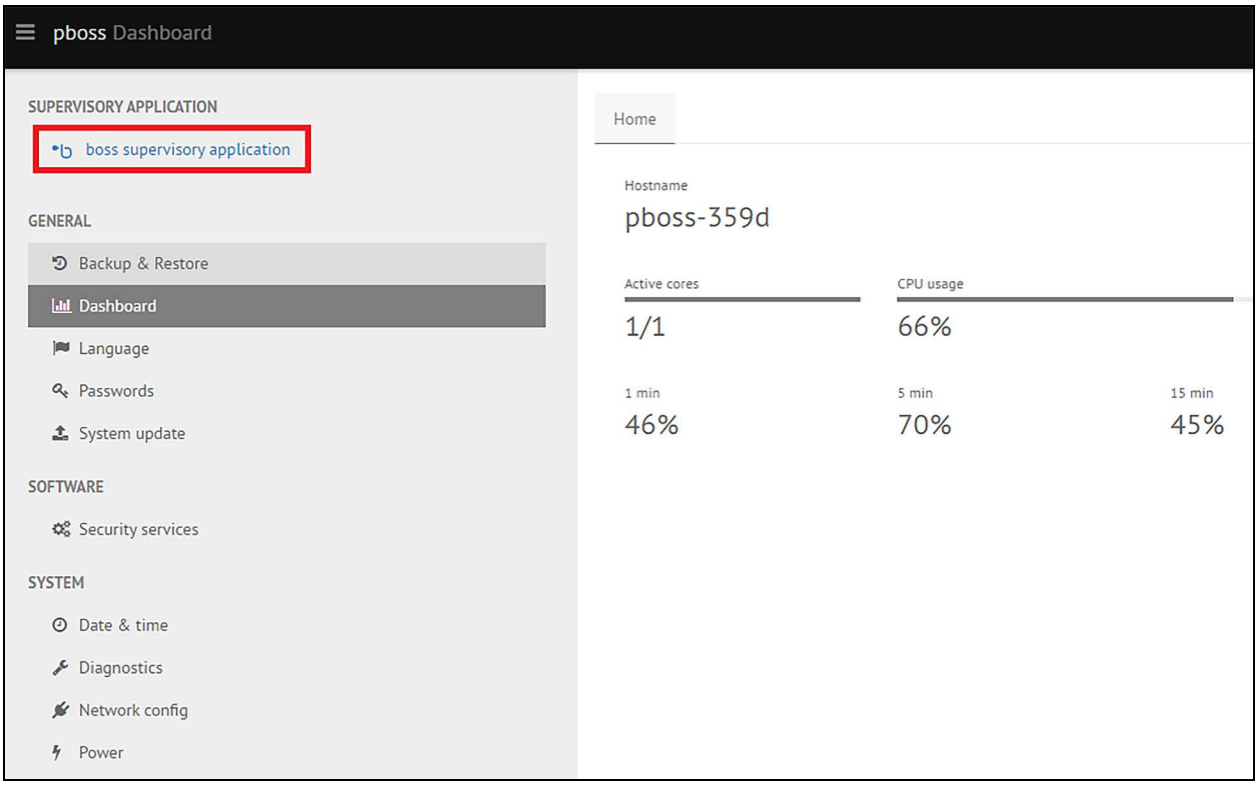


Figure 4.12 Rebooting the Card



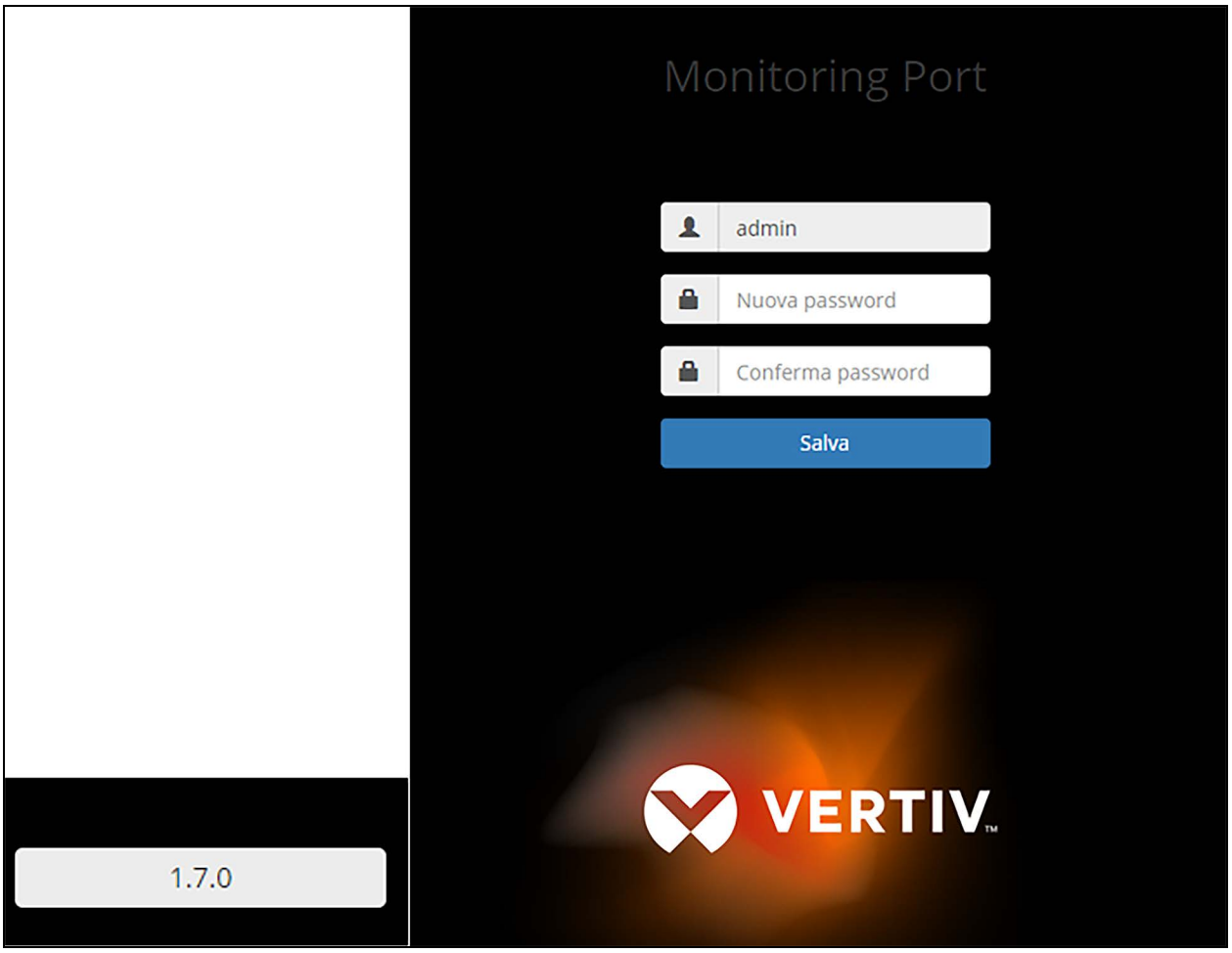
13. The reboot will require four to five minutes. Set your PC network settings accordingly to the Static IP address and subnet mask. At this point the minimum settings are done so it is time to go to the User web site. See **Figure 4.13** on the facing page .

Figure 4.13 Boss Supervisory Application



14. Once re-directed, setup the Admin password respecting the minimum complexity requirements (at least one number and one special character). See **Figure 4.14** on the next page .

Figure 4.14 Password Setup



The current software version is indicated in the bottom left corner of **Figure 4.14** above .

The admin is a fixed user and must be setup. Later on, it is possible to define other users from within the web site.

NOTE: Do not lose the passwords. There is no way to reset them because there are no default values.

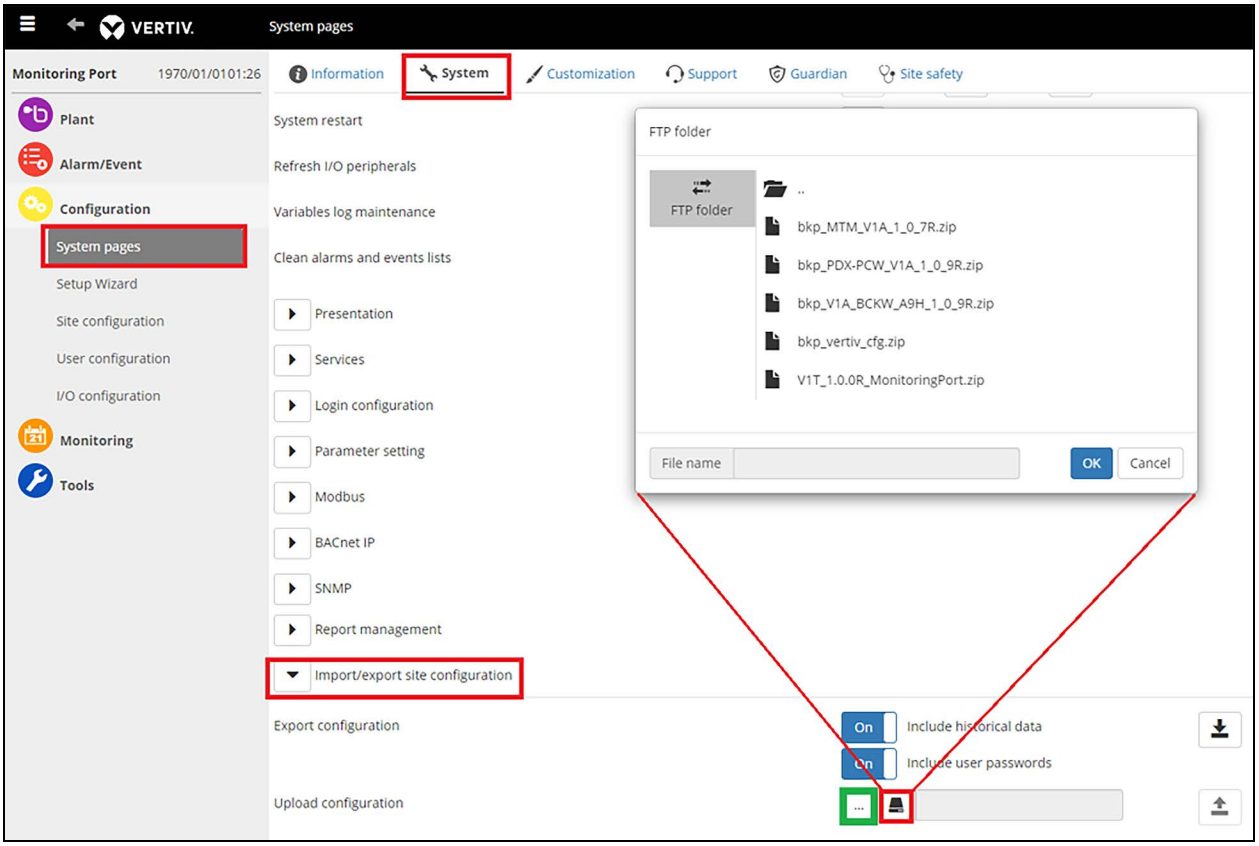
Once inside the user web site activate the right configuration based on the actual unit type. See Import of Full Configuration on the facing page .

4.1 Import of Full Configuration

The monitoring port device is already pre-programmed and contains all of the released configurations for different types of units.

1. During the first commissioning activate the backup.zip package for the relevant type of unit. The packages are resident in the internal memory of the device. To activate the backup.zip package, go to Configuration > System pages > System, and open the bottom section called Import/Export site configuration. See **Figure 4.15** below .

Figure 4.15 System Pages, System



2. Click on the browsing icons and search for the backup image files (.zip).

   The files can be located either in the PC file system or in the repository embedded into the monitoring port card at: /mnt/data/customer/. The selection is based on the unit type:

   a. PDX/PCW V1A Software

   b. Mobile V1A Software

   c. AFC V1C Software

   d. T-Wall V1T Software

3. The upload of the SW package can take several minutes, depending on the size. Once the upload is complete you will be requested to log-off and log-in again.

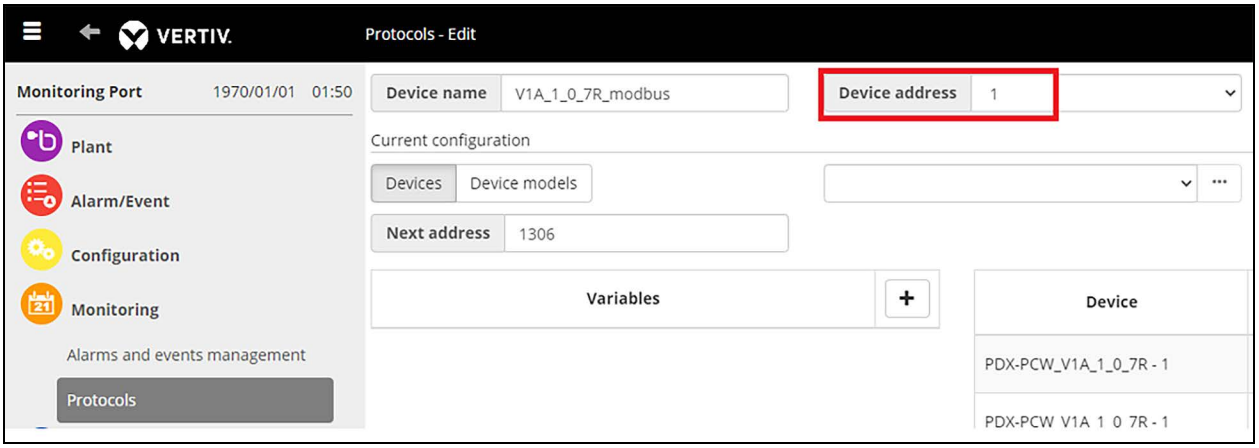
4.2 Changing Monitoring Protocol Parameters

1. To change the Modbus IP node address go to Monitoring > Protocols > Modbus. Select the device row, and click on Modify in the top bar. See Figure 4.16 below .

Figure 4.16 Protocols Screen

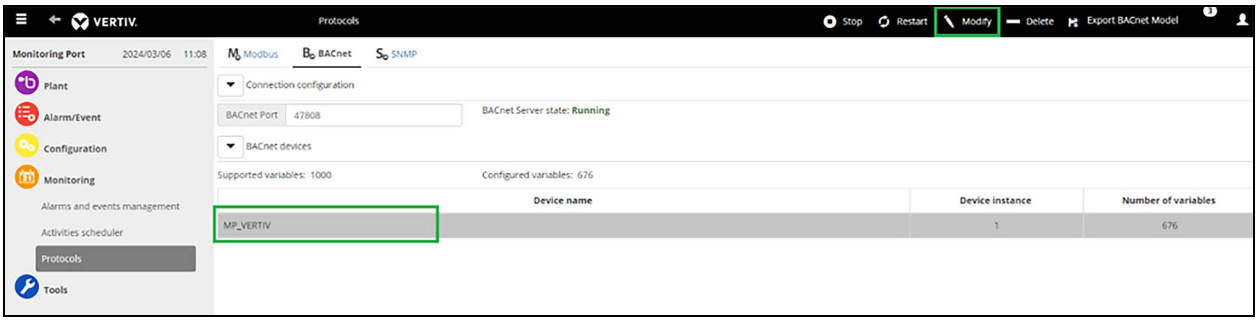
2. Change the device address. See Figure 4.17 below .

Figure 4.17 Changing Device Address



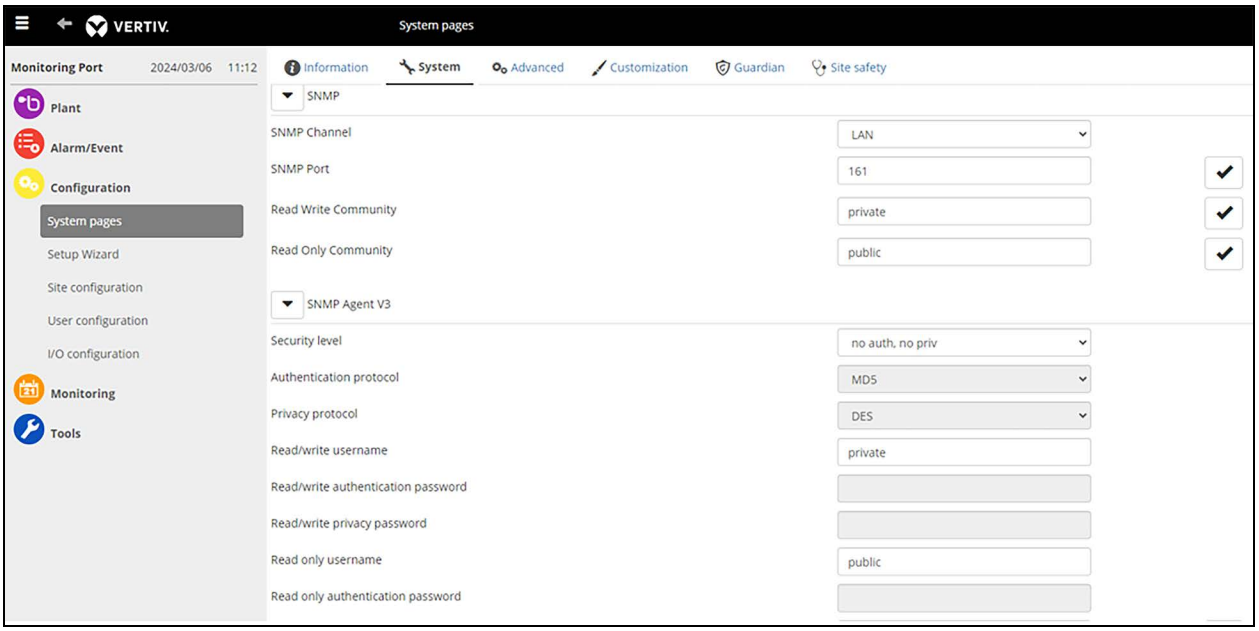
3. To change the configuration parameter related to BACnet go to Monitoring > Protocols > BACnet. Click on the device line and then on Modify on the top bar. See Figure 4.18 below .

Figure 4.18 Changing the BACnet Configuration Parameter



4. To change the configuration parameter related to SNMP and SNMP v3 communication go to System Pages > System. See **Figure 4.19** below .

Figure 4.19 Changing SNMP and SNMP Communication Configuration Parameters



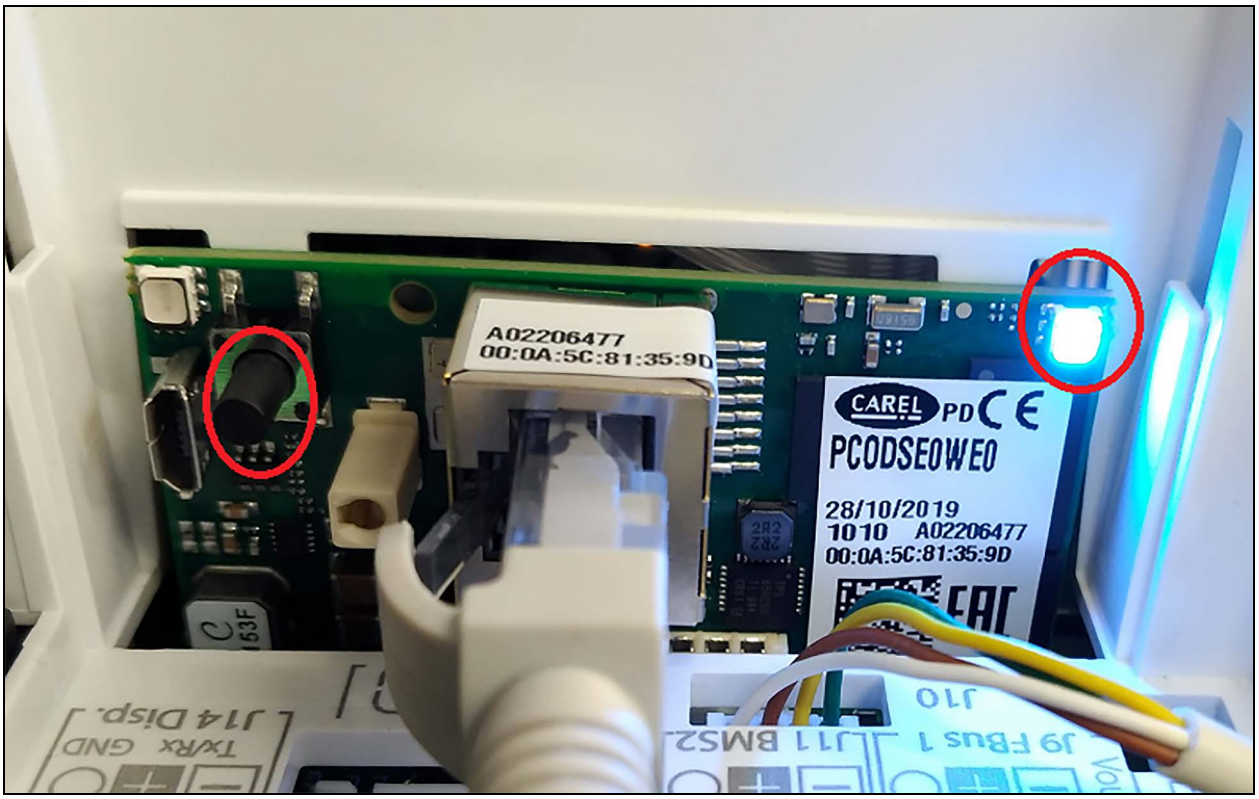
4.3 IP Address Recovery

The IP recovery procedure does not work while the monitoring port is booting (wait three minutes after reboot).

In the case of a forgotten IP address it is possible to enable a temporary IP address.

1. To enable a temporary IP address press the black button on the gateway for five seconds. The status LED will become light blue after releasing the button (after pressing for five seconds a short flashing indicates the status change). See Figure 4.20 below .

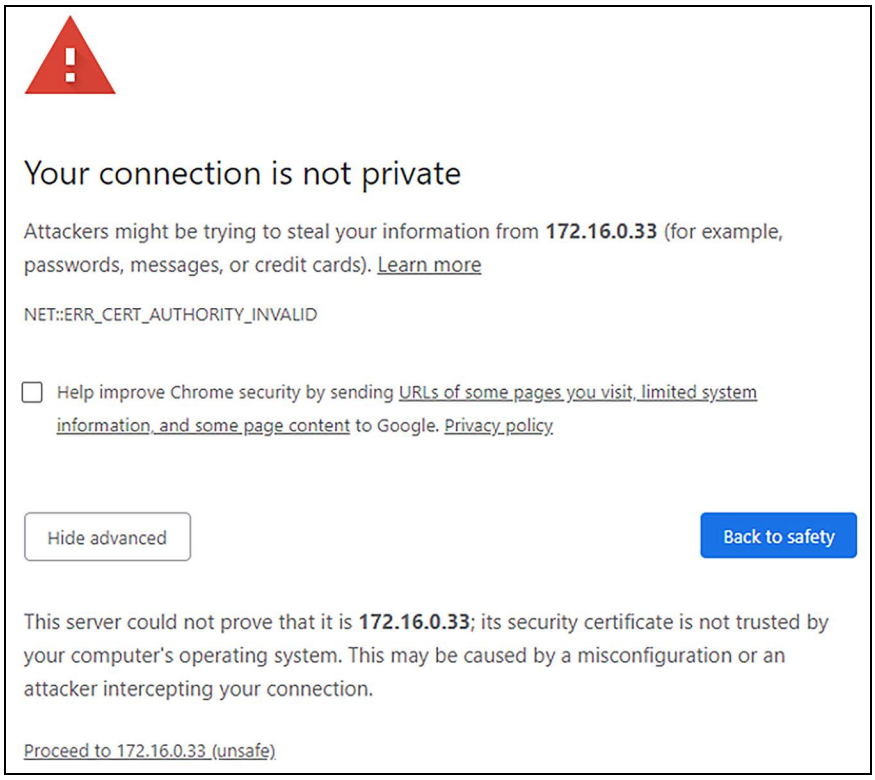
Figure 4.20 Black Button and LED Light



For one hour (or until the next power cycle), it is possible to use the secondary IP address: https://172.16.0.33 and connect via a browser. The address is available in parallel to the set IP.

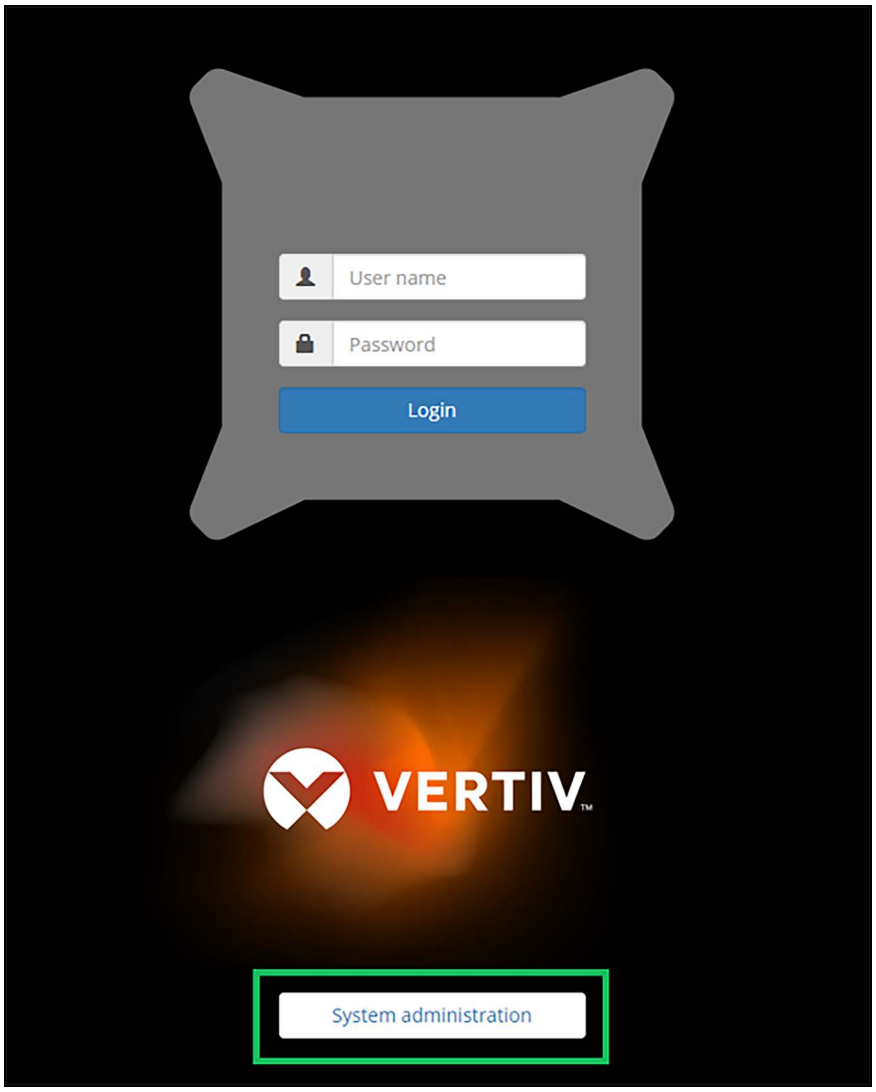
2. Activate the HTTPS protocol by typing https://172.16.0.33
3. After changing the IP address on the ETH port of the PC, see Figure 4.21 on the facing page .

Figure 4.21 Connection not Private



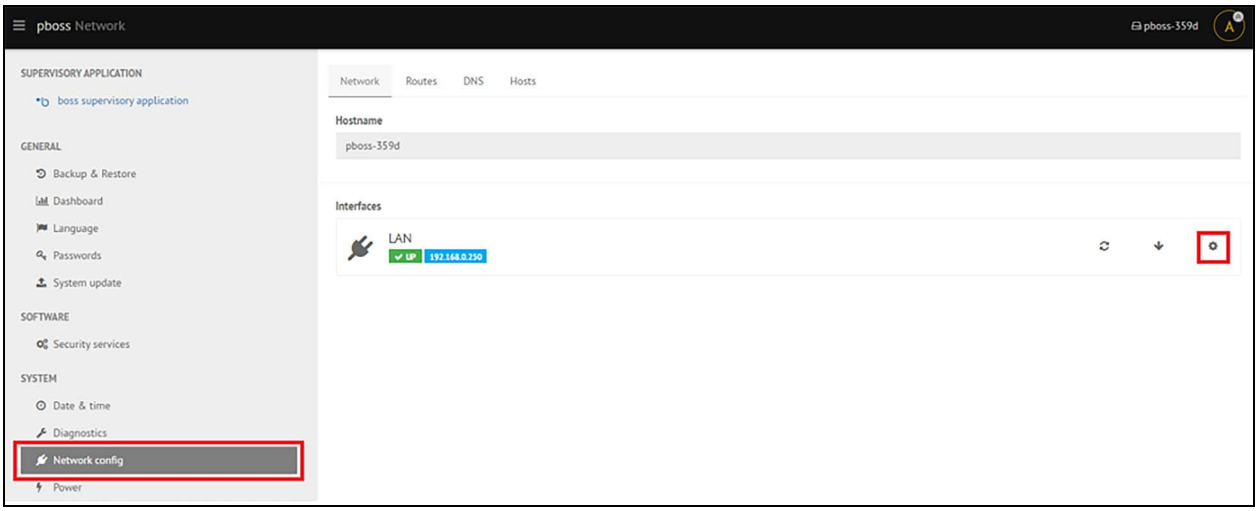
4. Log into the System Administration site. See Figure 4.22 on the next page .

Figure 4.22 System Administration



5. Check/modify the network settings. See Figure 4.23 on the facing page .

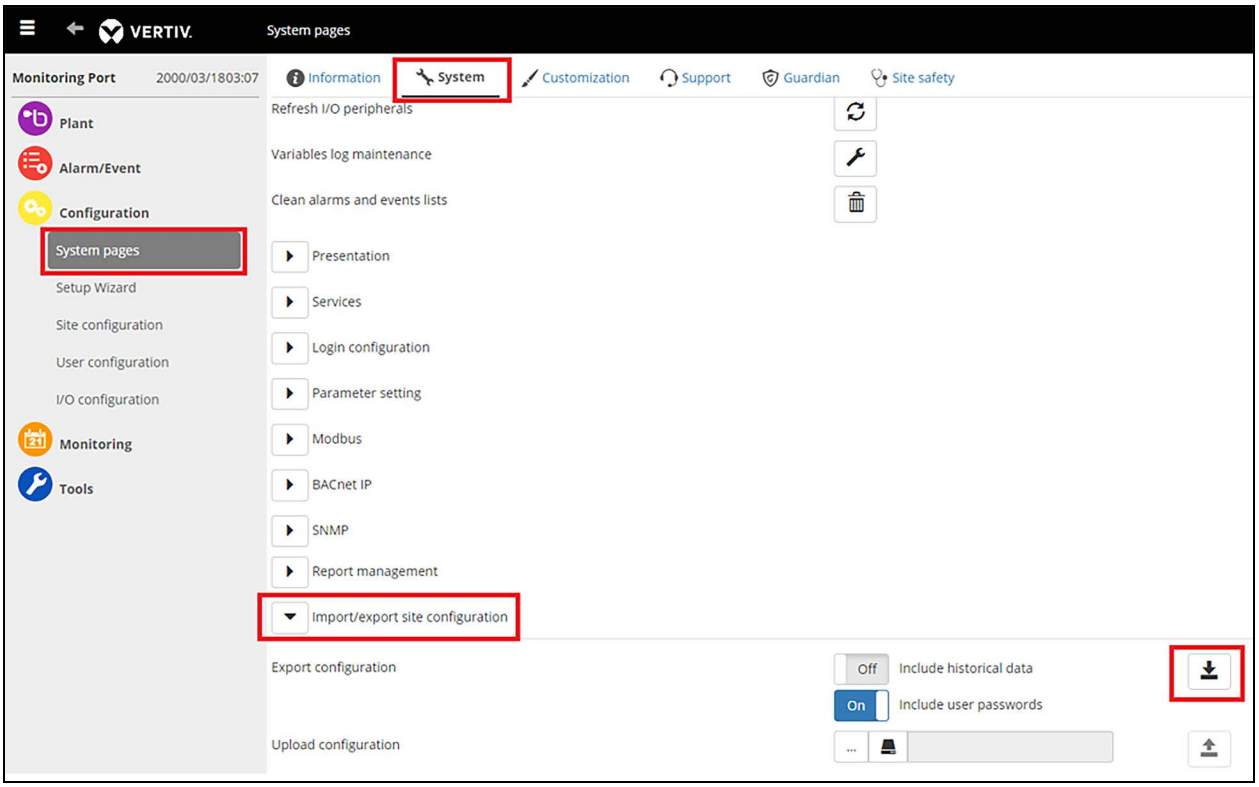
Figure 4.23 Network Configuration



4.4 Exporting a Full Configuration

1. The monitoring port permits exporting a full configuration as a backup.zip file. This is useful when there is a specific customization to BMS files that you want to replicate on the other units in the field. To export a full configuration, go in Configuration > System pages > System. See Figure 4.24 below .

Figure 4.24 System Pages, System



2. Click on Import/Export site configuration and set the following:
   - Set include historized data to Off (backup will be applied to a different unit).
   - Set include user passwords to On if you want to apply the same credentials to the next units.
   - Click the download icon.

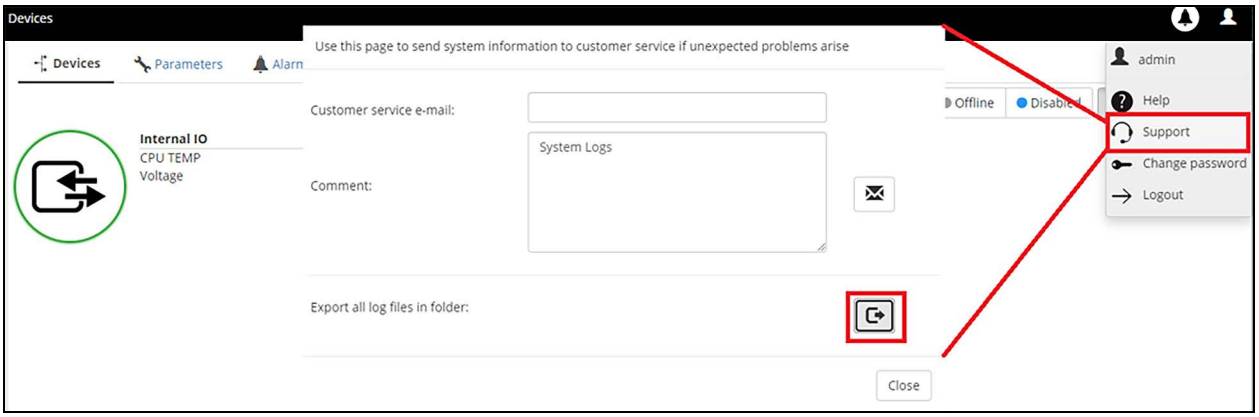
   The download takes several minutes and the .zip package file is saved in the default Downloads folder of the PC.

   The file is ready to be used as is, and uploaded into another unit.

4.5 Exporting Log Files

The user can export monitoring port log files when they are requested for engineering investigation. See **Figure 4.25** below .

Figure 4.25 Exporting Log Files

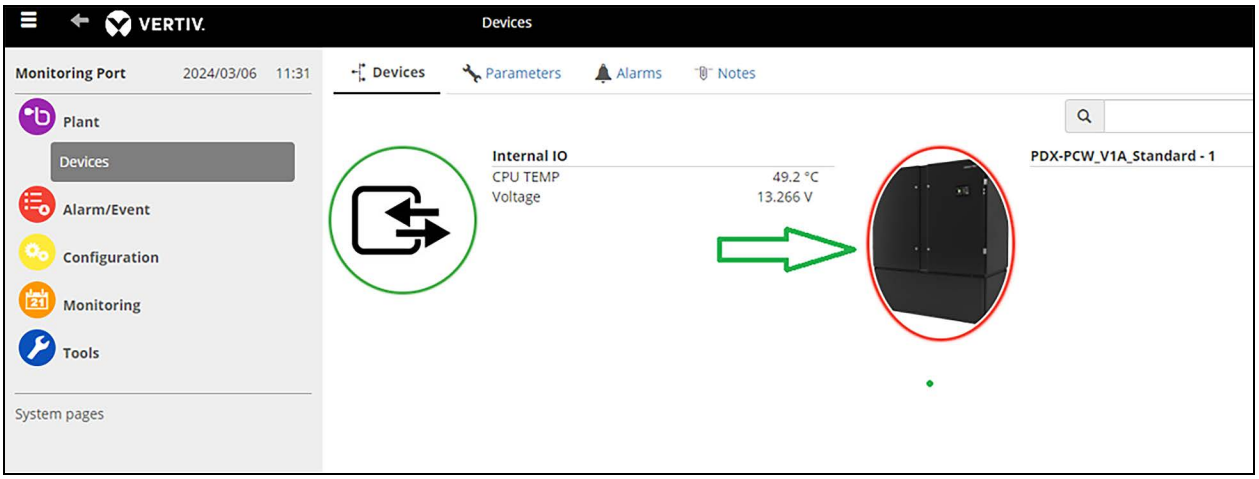


The log will be saved as a single file in the Downloads folder with a name similar to: diagnose_YYYYMMDDhhmmss.tar.gz.

4.6 Search of Parameters

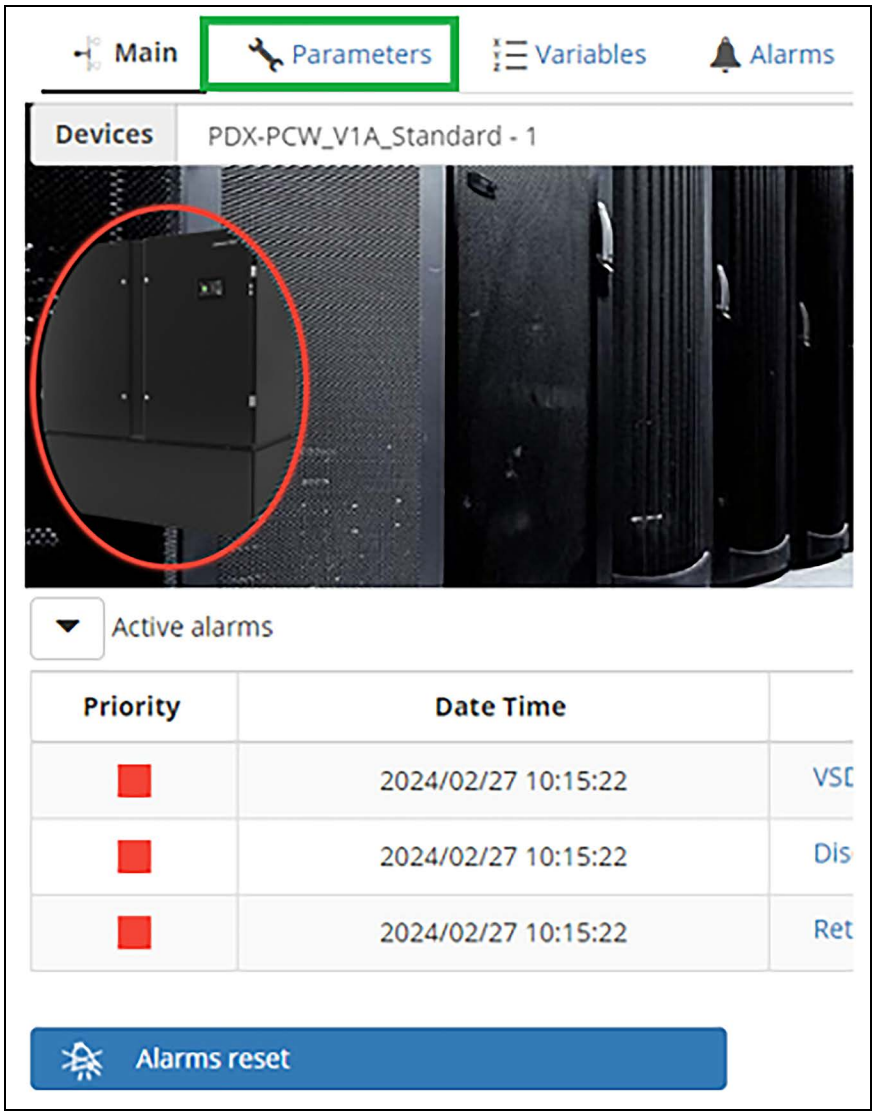
1. Unit parameters and alarms can be searched for reading or writing. Click on the device image. See Figure 4.26 below .

Figure 4.26 Devices



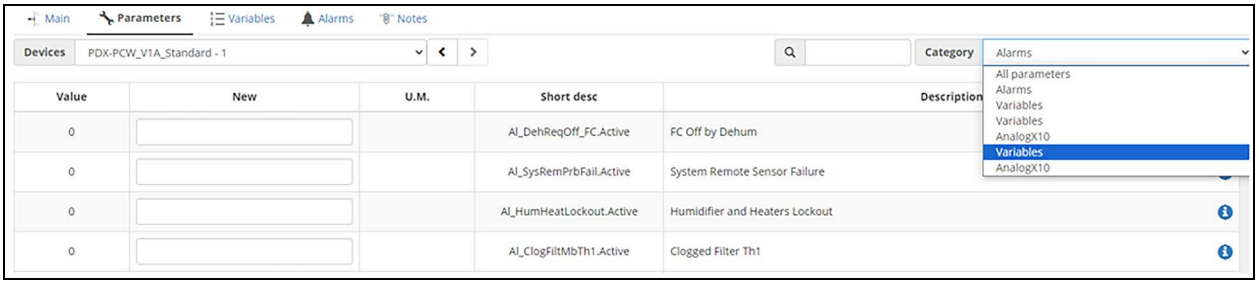
2. Click Parameters. See Figure 4.27 on the next page .

Figure 4.27 Parameters



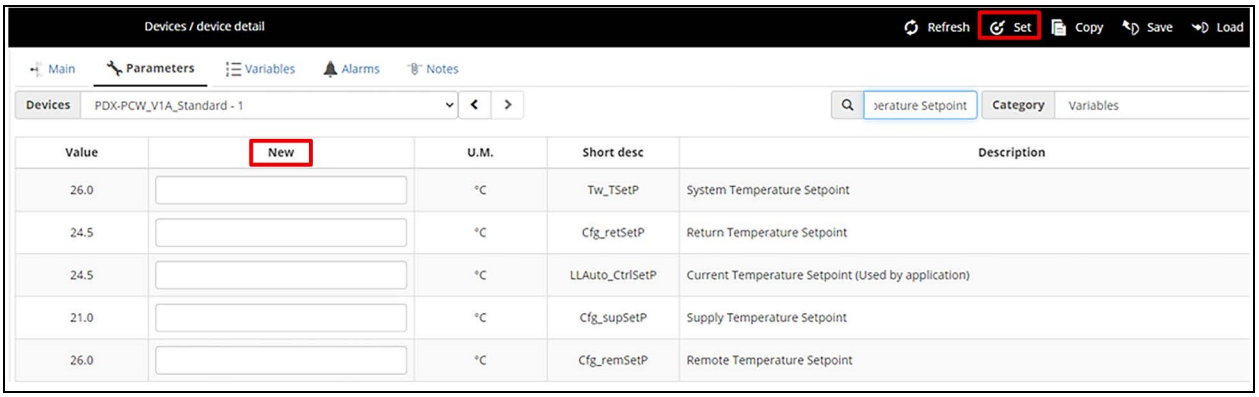
3. Change Category to the last Variables Selection See **Figure 4.28** below .

Figure 4.28 Changing Variable



4. Type the parameter description into the Search field, e.g., Temperature Setpoint. See **Figure 4.29** on the facing page .

Figure 4.29 Searching for Parameters



5. Set the new value using the New field and the Set button on top bar. See Figure 4.29 above .

NOTE: This functionality is fully working only from FW version 1.11.

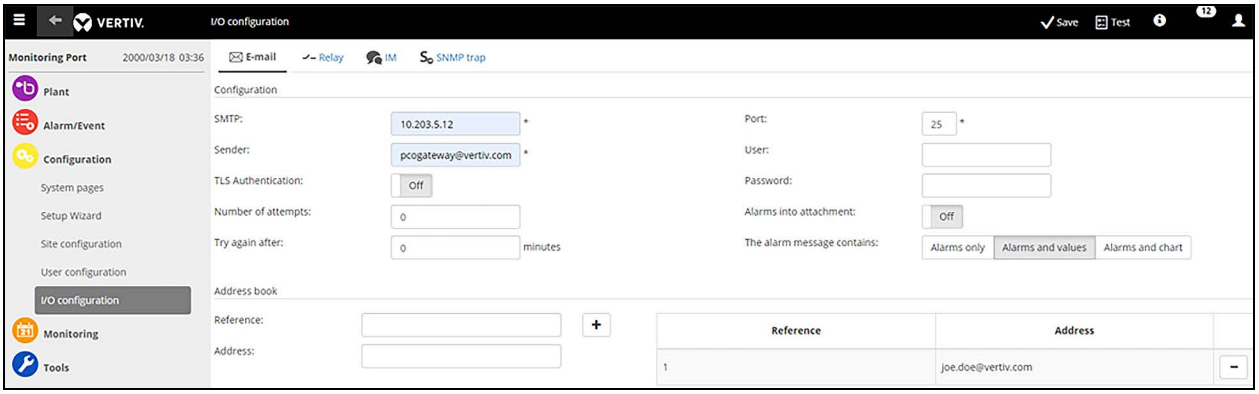
4.7 E-mail and Trap Settings

4.7.1 E-mail Configuration

1. Alarms can be associated to outgoing emails by setting the requested parameters in Configuration > I/O Configuration > E-mail. See Figure 4.30 below .

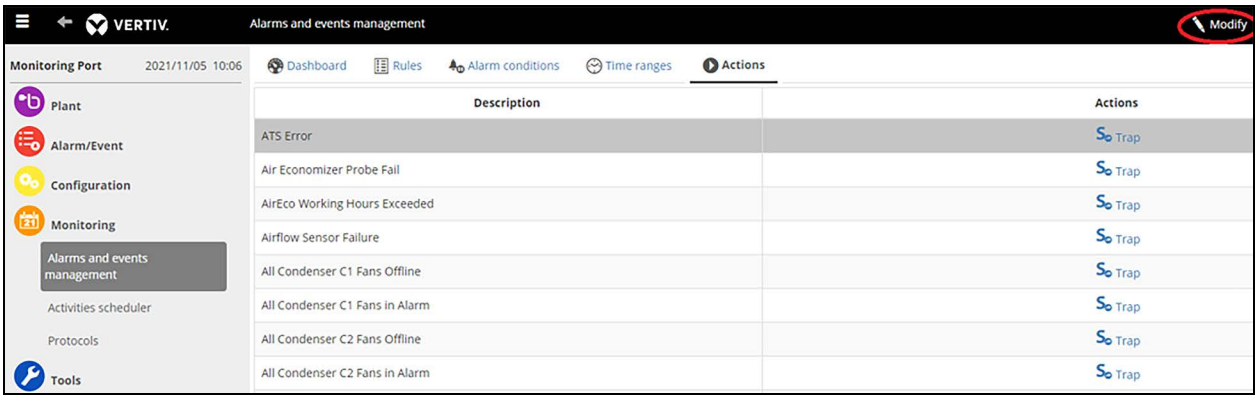
   In the Address Book at least one destination e-mail address must be set up.

Figure 4.30 I/O Configuration, Email



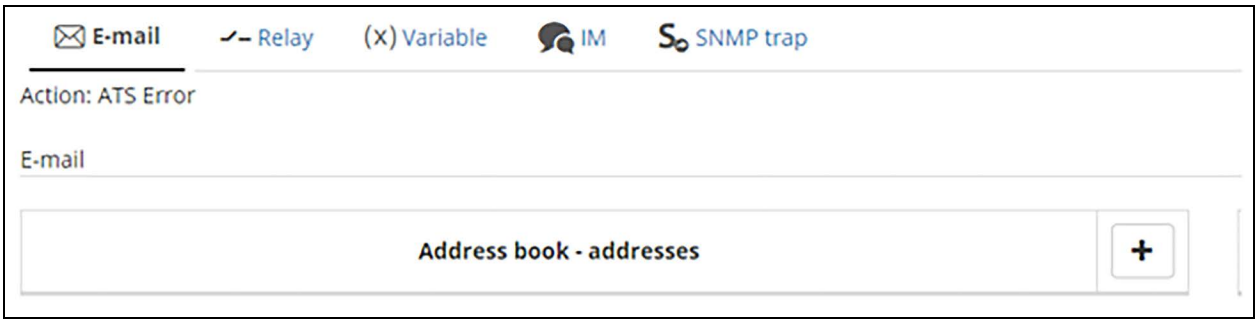
2. In Monitoring > Alarms and events management > Actions select the alarm that will trigger the e-mail and modify it. See Figure 4.31 on the next page .

Figure 4.31 Alarms and Events Management



3. Associate the alarm to the Address book e-mail. See Figure 4.32 below .

Figure 4.32 Address Book

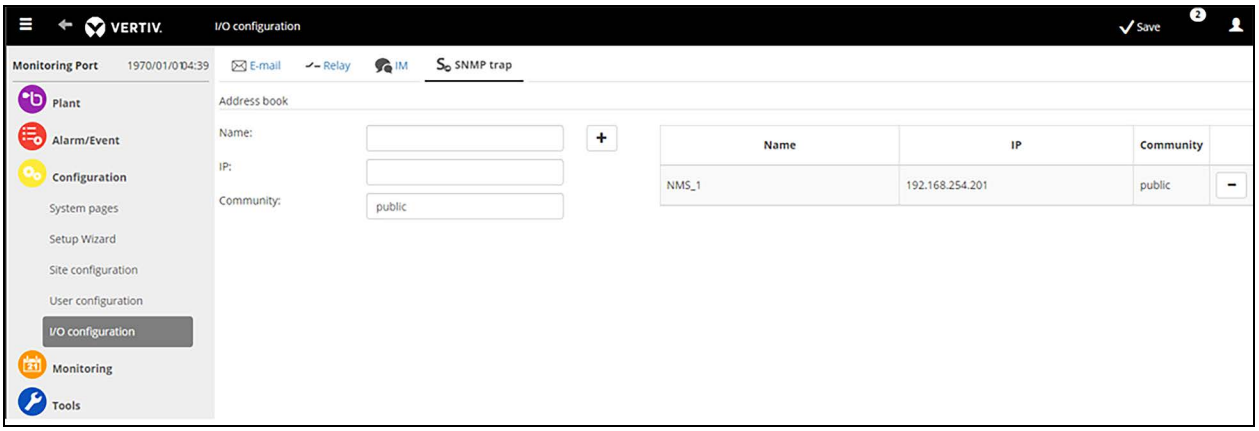


4. Save the new settings.

4.7.2 SNMP Trap Configuration

SNMP traps must be configured first in Configuration > I/O Configuration > SNMP Trap by defining at least one item in the destination address book. See Figure 4.33 below .

Figure 4.33 I/O Configuration, SNMP Trap

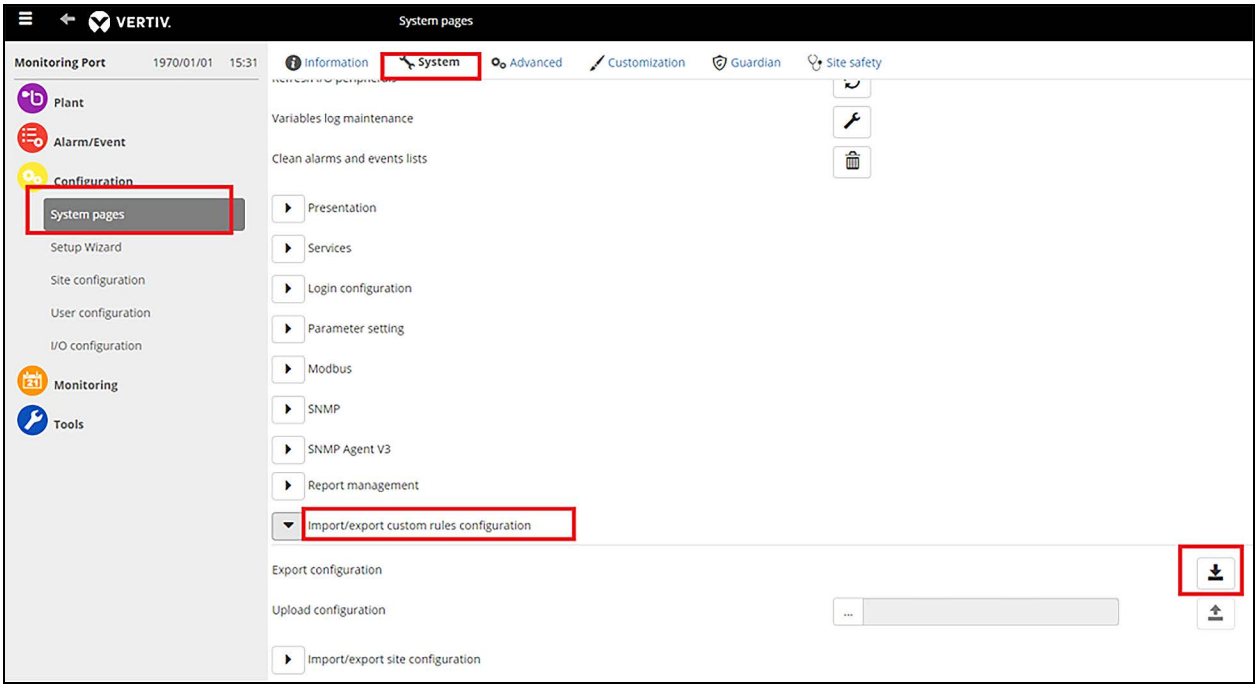


The default 192.168.254.201 should be changed by the Customer Engineer of field with the actual NMS IP address. The change will be applied to all of the pre-defined traps.

4.7.3 Export SNMP Configuration

From OS version 1.11 it is possible to export the full SNMP Trap configuration in XML file. See Figure 4.34 below .

Figure 4.34 System Pages, System



Exporting the full SNMP trap configuration creates an XML file in the Downloads folder that can be re-imported into another card.

4.8 Restoring Factory Settings

If the board configuration is compromised, restore the factory settings as follows:

1. Power Off the monitoring card.
2. Power On by pressing and holding the button.

   After a few seconds, the Status LED will turn red and flash slowly.
3. When the LED starts flashing quickly, release the button.

   The Status LED flashes slowly again.
4. When the LED starts flashing quickly, press and hold the button again.

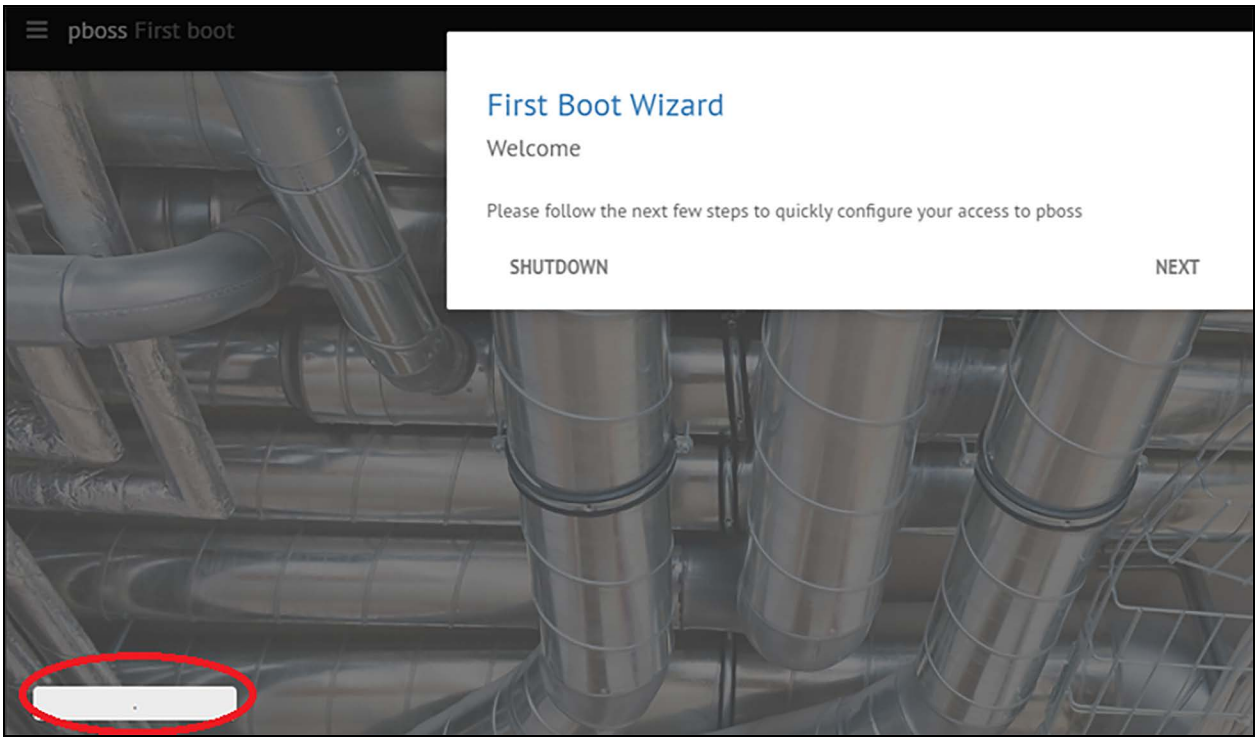
   The Status LED then flashes slowly for the third time.
5. When it starts to flash quickly, release the button.
6. The factory reset procedure is now in progress. Wait for the monitoring card to restart, then repeat the first boot procedure.

NOTE: Consider that the reset procedure returns the monitoring port to factory status. So, if for example you had previously upgraded it from v1.5.0 to v1.6.0, it will be reverted to v1.5.0, and a new manual upgrade would be necessary.

NOTE: DHCP is set because of the factory reset. If it is necessary to connect to a known IP, the default IP procedure is always available, so just press the Service button for five seconds until the Communication LED turns blue and connects to https://172.16.0.33.

7. If at first boot on field the First Reboot Wizard screen appears at https://192.168.254.200 with a "." in place of the FW version (e.g., 1.11.0), then the reset procedure explained above must be performed. See Figure 4.35 on the facing page .

Figure 4.35 First Boot Wizard



8. As a second step the standard network settings shall be restored by connecting to the temporary https://172.16.0.33 URL and following the instructions in IP Address Recovery on page 20 .

This page intentionally left blank

Appendices

Appendix A: Technical Support and Contacts

A.1 Technical Support/Service in the United States

Vertiv Group Corporation

24x7 dispatch of technicians for all products.

1-800-543-2378

Liebert® Thermal Management Products

1-800-543-2778

Liebert® Channel Products

1-800-222-5877

Liebert® AC and DC Power Products

1-800-543-2378

A.2 Locations

United States

Vertiv Headquarters

505 N Cleveland Ave

Westerville, OH, 43082, USA

Europe

Via Leonardo Da Vinci 8 Zona Industriale Tognana

35028 Piove Di Sacco (PD) Italy

Asia

7/F, Dah Sing Financial Centre

3108 Gloucester Road, Wanchai

Hong Kong

This page intentionally left blank

Connect with Vertiv on Social Media

 https://www.facebook.com/vertiv/

 https://www.instagram.com/vertiv/

 https://www.linkedin.com/company/vertiv/

 https://www.x.com/Vertiv/

Vertiv.com | Vertiv Headquarters, 505 N Cleveland Ave, Westerville, OH 43082 USA

SL-80349_REVA_11-25