

# PDU Network Module

## Gigabit Network Module (GNM) User's Guide

English



11/13/2023



Eaton is a registered trademark of Eaton Corporation or its subsidiaries and affiliates.

Phillips and Pozidriv are a registered trademarks of Phillips Screw Company.

National Electrical Code and NEC are registered trademarks of National Fire Protection Association, Inc.

Microsoft®, Windows®, and Windows Server® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

UNIX® is a registered trademark of The Open Group.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions.

Google™ is a trademark of Google Inc.

All other trademarks are properties of their respective companies.

©Copyright 2023 Eaton Corporation. All rights reserved.

No part of this document may be reproduced in any way without the express written approval of Eaton Corporation.

# 1 Table of Contents

<b>1</b>	<b>TABLE OF CONTENTS .....</b>	<b>4</b>
<b>2</b>	<b>INSTALLING THE NETWORK MANAGEMENT MODULE .....</b>	<b>10</b>
2.1	Wiring the power redundancy (PDU+1) .....	10
2.1.1	Power redundancy principle .....	10
2.1.2	Examples .....	11
2.2	Connecting PDUs in cascade .....	14
2.3	Accessing the Network Module .....	15
2.3.1	Accessing the web interface through Network.....	15
2.3.2	Finding and setting the IP address .....	16
2.3.3	Accessing the web interface through RNDIS.....	16
2.3.4	Accessing the card through serial terminal emulation.....	19
2.3.5	Modifying the Proxy exception list .....	21
<b>3</b>	<b>LCD INTERFACE OPERATION .....</b>	<b>24</b>
3.1	Display and control buttons .....	24
3.1.1	Presentation .....	24
3.1.2	How to use the control buttons.....	24
3.2	Operation mode.....	24
3.2.1	Startup screen .....	24
3.2.2	Main menu selections .....	25
3.2.3	Password protection menus.....	26
3.2.4	Screensaver .....	27
3.2.5	Backlight.....	27
3.3	Alarms .....	28
3.3.1	Active alarms.....	29
3.3.2	Alarms history.....	29
3.4	PDU info .....	30
3.5	Meter.....	30
3.5.1	Input .....	31
3.5.2	Branch .....	32
3.5.3	Outlet.....	32
3.5.4	Environment .....	33
3.6	Admin .....	34
3.6.1	Network.....	34
3.6.2	Settings .....	36
3.6.3	Control.....	38
<b>4</b>	<b>CONTEXTUAL HELP OF THE WEB INTERFACE .....</b>	<b>40</b>
4.1	Login page.....	40
4.1.1	Logging in for the first time .....	40
4.1.2	Troubleshooting.....	41
4.2	Home.....	42
4.2.1	Header structure.....	42
4.2.2	Menu structure.....	43
4.2.3	PDU input .....	44
4.2.4	Environment .....	44
4.2.5	Alarms .....	44
4.2.6	Branches, outlet status and details .....	45



4.2.7	Access rights per profiles .....	46
4.3	Meters .....	46
4.3.1	Input .....	46
4.3.2	Group .....	48
4.4	Controls .....	49
4.4.1	Outlets .....	49
4.4.2	Group .....	51
4.5	Environment .....	53
4.5.1	Commissioning/Status .....	53
4.5.2	Alarm configuration .....	58
4.5.3	Information .....	61
4.6	Settings .....	63
4.6.1	General .....	63
4.6.2	Local users .....	76
4.6.3	Remote users .....	81
4.6.4	Ports .....	96
4.6.5	TCP/IP .....	100
4.6.6	Firewall .....	109
4.6.7	Protocols .....	114
4.6.8	SNMP .....	118
4.6.9	Certificate .....	126
4.7	PDU settings .....	134
4.7.1	General .....	134
4.7.2	Input thresholds .....	135
4.7.3	Branch thresholds .....	136
4.7.4	Outlet thresholds .....	138
4.7.5	Outlet switching .....	140
4.7.6	Group definition .....	142
4.8	Maintenance .....	142
4.8.1	Firmware .....	143
4.8.2	Sessions .....	147
4.8.3	Services .....	148
4.8.4	Resources .....	154
4.8.5	System logs .....	156
4.8.6	System information .....	157
4.9	Alarms .....	158
4.9.1	Alarm sorting .....	158
4.9.2	Active alarm counter .....	158
4.9.3	Alarm details .....	158
4.9.4	Alarm paging .....	158
4.9.5	Export .....	158
4.9.6	Clear .....	159
4.9.7	Alarms list with codes .....	159
4.9.8	Access rights per profiles .....	159
4.10	User profile .....	160
4.10.1	Access to the user profile .....	160
4.10.2	User profile .....	160
4.10.3	Legal information .....	163
4.10.4	Component .....	163
4.10.5	Availability of source code .....	163
4.10.6	Notice for proprietary elements .....	163
4.10.7	Default settings and possible parameters - User profile .....	164
4.10.8	Access rights per profiles .....	164
4.10.9	CLI commands .....	165

4.10.10	Troubleshooting.....	165
4.10.11	Save and Restore .....	166
4.11	Documentation .....	167
4.11.1	Access to the embedded documentation .....	167
4.11.2	Access rights per profiles.....	168
<b>5</b>	<b>SERVICING THE NETWORK MANAGEMENT MODULE .....</b>	<b>169</b>
5.1	Configuring/Commissioning/Testing LDAP .....	169
5.1.1	Commissioning.....	169
5.1.2	Testing LDAP connection.....	170
5.1.3	Limitations .....	170
5.2	Checking the current firmware version of the Network Module.....	170
5.3	Accessing to the latest Network Module firmware/driver/script.....	170
5.4	Upgrading the card firmware (Web interface / shell script).....	170
5.4.1	Web interface .....	170
5.4.2	Shell script.....	170
5.4.3	Example:.....	171
5.5	Updating the time of the Network Module precisely and permanently (ntp server) .....	172
5.6	Changing the language of the web pages .....	172
5.7	Resetting username and password.....	172
5.7.1	As an admin for other users .....	172
5.7.2	Resetting its own password.....	172
5.8	Recovering main administrator password .....	172
5.9	Switching to static IP (Manual) / Changing IP address of the Network Module.....	175
5.10	Subscribing to a set of alarms for email notification.....	176
5.10.1	Example #1: subscribing only to one alarm (load unprotected).....	176
5.10.2	Example #2: subscribing to all Critical alarms and some specific Warnings .....	177
5.11	Saving/Restoring/Duplicating Network module configuration settings .....	178
5.11.1	Modifying the JSON configuration settings file.....	178
5.11.2	Saving/Restoring/Duplicating settings through the CLI.....	182
5.11.3	Saving/Restoring/Duplicating settings through the Web interface.....	182
5.12	Replacing the PDU Gigabit Network Module .....	182
5.12.1	To replace the GNM .....	183
5.13	Restarting the PDU Gigabit Network Module and Resetting the PDU.....	187
<b>6</b>	<b>SECURING THE NETWORK MANAGEMENT MODULE.....</b>	<b>188</b>
6.1	Cybersecurity considerations for electrical distribution systems .....	188
6.1.1	Purpose .....	188
6.1.2	Introduction .....	188
6.1.3	Connectivity—why do we need to address cybersecurity for industrial control systems (ICS)? .....	188
6.1.4	Cybersecurity threat vectors .....	188
6.1.5	Defense in depth .....	189
6.1.6	Designing for the threat vectors.....	190
6.1.7	Policies, procedures, standards, and guidelines.....	192
6.1.8	Conclusion .....	194
6.1.9	Terms and definitions .....	194
6.1.10	Acronyms .....	194
6.1.11	References .....	195
6.2	Cybersecurity recommended secure hardening guidelines .....	196
6.2.1	Introduction .....	196
6.2.2	Secure configuration guidelines .....	196
6.2.3	References .....	202
6.3	Configuring user permissions through profiles.....	203
6.4	Decommissioning the Network Management module .....	203

<b>7</b>	<b>SERVICING THE EMP .....</b>	<b>205</b>
7.1	Description and features .....	205
7.2	Unpacking the EMP .....	205
7.3	Installing the EMP .....	205
7.3.1	Defining EMPs address and termination .....	205
7.3.2	Mounting the EMP .....	206
7.3.3	Cabling the first EMP to the device .....	209
7.3.4	Daisy chaining EMPs .....	210
7.3.5	Connecting an external contact device .....	211
7.4	Commissioning the EMP .....	211
7.4.1	On the Network Module device .....	211
<b>8</b>	<b>INFORMATION.....</b>	<b>212</b>
8.1	Front panel connectors and LED indicators .....	212
8.2	Specifications/Technical characteristics .....	214
8.3	Default settings and possible parameters .....	214
8.3.1	Meters .....	214
8.3.2	Settings .....	215
8.3.3	Sensors alarm configuration .....	221
8.3.4	User profile .....	221
8.4	Access rights per profiles .....	223
8.4.1	Home .....	223
8.4.2	Meters .....	223
8.4.3	Controls .....	223
8.4.4	Environment .....	223
8.4.5	Settings .....	224
8.4.6	Maintenance .....	226
8.4.7	Alarms .....	226
8.4.8	User profile .....	226
8.4.9	Contextual help .....	227
8.4.10	CLI commands .....	227
8.5	List of event codes .....	229
8.5.1	System log codes .....	229
8.5.2	PDU alarm log codes .....	234
8.5.3	EMP alarm log codes .....	238
8.5.4	Network module alarm log codes .....	239
8.6	SNMP traps .....	239
8.6.1	Sensor Mib .....	239
8.6.2	PDU Mib .....	240
8.7	CLI .....	241
8.7.1	Commands available .....	241
8.7.2	Contextual help .....	242
8.7.3	get release info .....	242
8.7.4	history .....	243
8.7.5	logout .....	243
8.7.6	maintenance .....	244
8.7.7	netconf .....	245
8.7.8	ping and ping6 .....	247
8.7.9	reboot .....	247
8.7.10	rest list .....	248
8.7.11	rest get .....	248
8.7.12	rest set .....	249
8.7.13	rest exec .....	249

8.7.14	save_configuration   restore_configuration.....	249
8.7.15	sanitize.....	250
8.7.16	ssh-keygen .....	251
8.7.17	time .....	251
8.7.18	traceroute and traceroute6.....	252
8.7.19	whoami.....	253
8.7.20	email-test.....	253
8.7.21	systeminfo_statistics.....	254
8.7.22	certificates.....	255
8.8	Legal information.....	256
8.8.1	Availability of Source Code.....	256
8.8.2	Notice for Open Source Elements.....	256
8.8.3	Notice for our proprietary (i.e. non-Open source) elements.....	257
8.9	Acronyms and abbreviations .....	258
<b>9</b>	<b>TROUBLESHOOTING.....</b>	<b>261</b>
9.1	EMP communication status shows "Lost".....	261
9.1.1	Symptom #1 .....	261
9.2	EMP detection fails at discovery stage .....	261
9.2.1	Symptom #1 .....	261
9.2.2	Symptom #2.....	262
9.3	How do I log in if I forgot my password? .....	262
9.3.1	Action .....	262
9.4	LDAP configuration/commissioning is not working.....	262
9.5	Password change in My profile is not working.....	263
9.5.1	Symptoms .....	263
9.5.2	Possible cause.....	263
9.5.3	Action .....	263
9.6	The alarm list has been cleared after an upgrade.....	263
9.6.1	Symptom.....	263
9.6.2	Action .....	263
9.7	The Network Module fails to boot after upgrading the firmware .....	263
9.7.1	Possible Cause .....	263
9.7.2	Action .....	264
9.8	Web user interface is not up to date after a FW upgrade .....	264
9.8.1	Symptom.....	264



## 2 Installing the Network Management Module

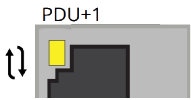

### 2.1 Wiring the power redundancy (PDU+1)

#### 2.1.1 Power redundancy principle

Interconnect 2 Network Modules using the power redundancy port (PDU+1) with a standard Ethernet cable (not supplied).

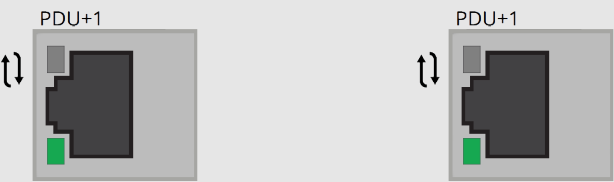
Power the 2 Network Modules with 2 different feeds so that if one feed is down, the Network Module will still be powered ON and alive, providing useful information on the power outage situation.

##### 2.1.1.1 LEDs

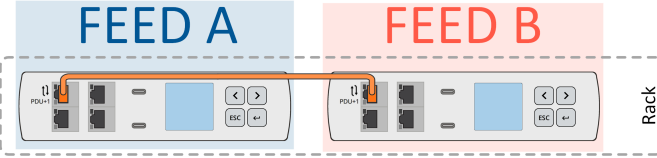
	<ul style="list-style-type: none"><li>Off — no active redundancy</li><li>Solid yellow — the PDU Network Module is powered by another PDU Network Module through the redundancy port.</li></ul>
	<ul style="list-style-type: none"><li>Off — PDU Network Module is not connected to another PDU.</li><li>Solid green — The PDU Network Module is connected to another PDU Network Module power redundancy port.</li></ul>

##### 2.1.1.2 Power redundancy connection with 2 modules

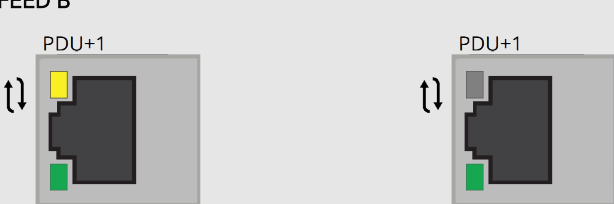
2 modules:



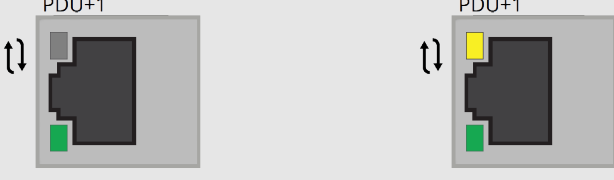
- Interconnected with the PDU+1 port ✓
- Powered with 2 different feeds ✓

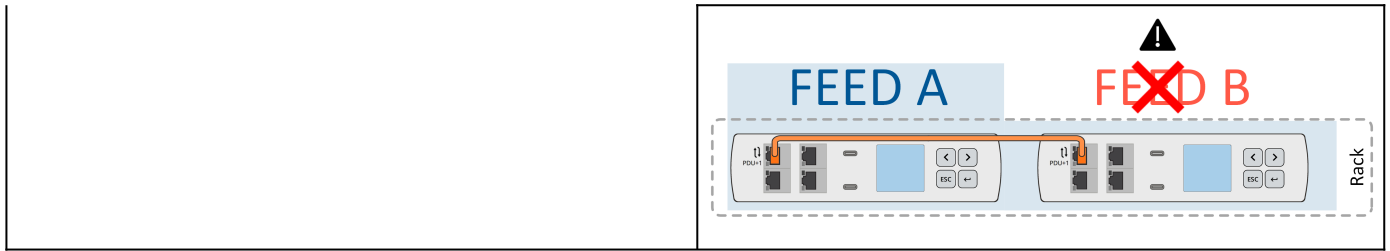


Result with a power cut on FEED A = all the modules are powered by FEED B



Result with a power cut on FEED B = all the modules are powered by FEED A

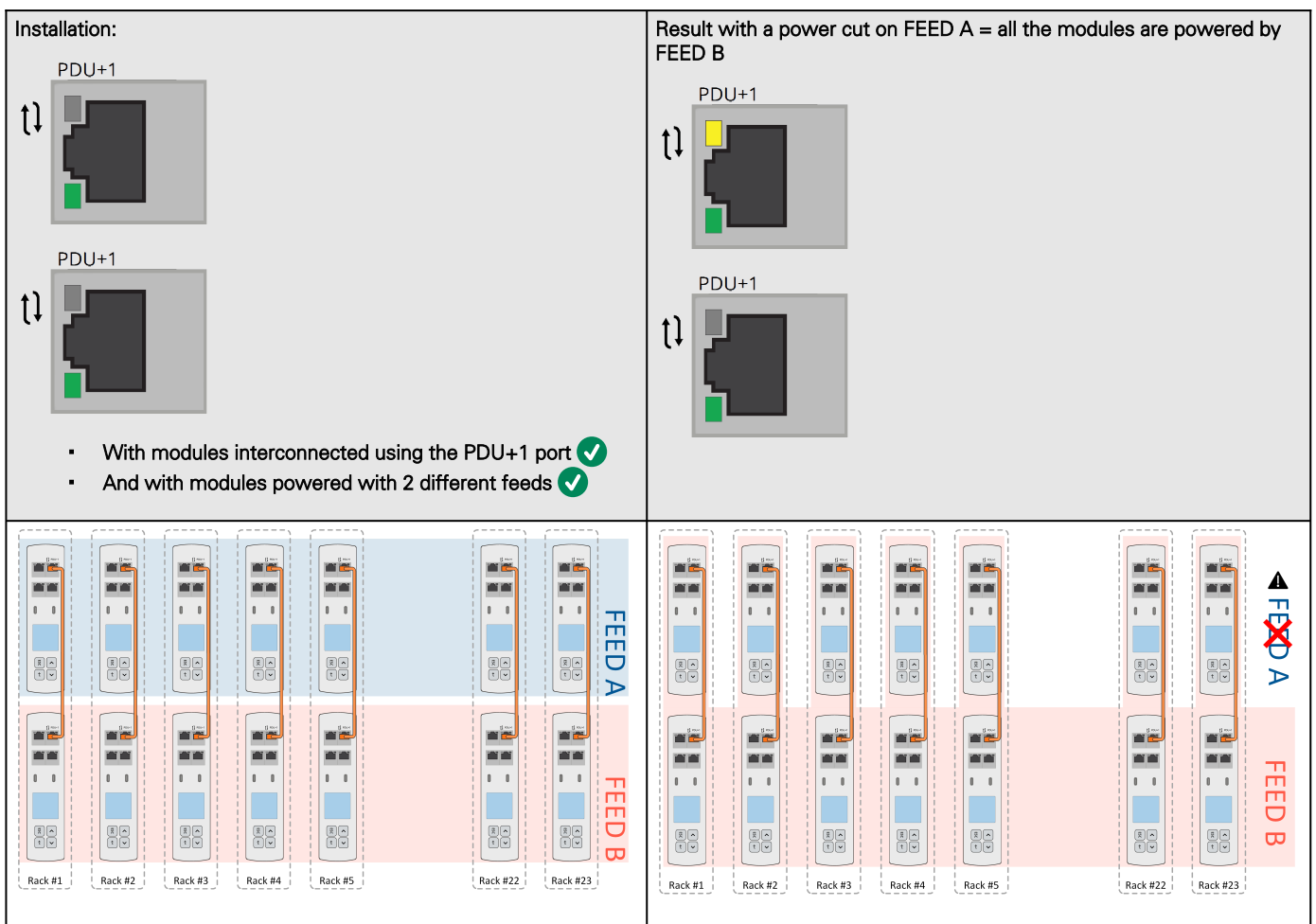


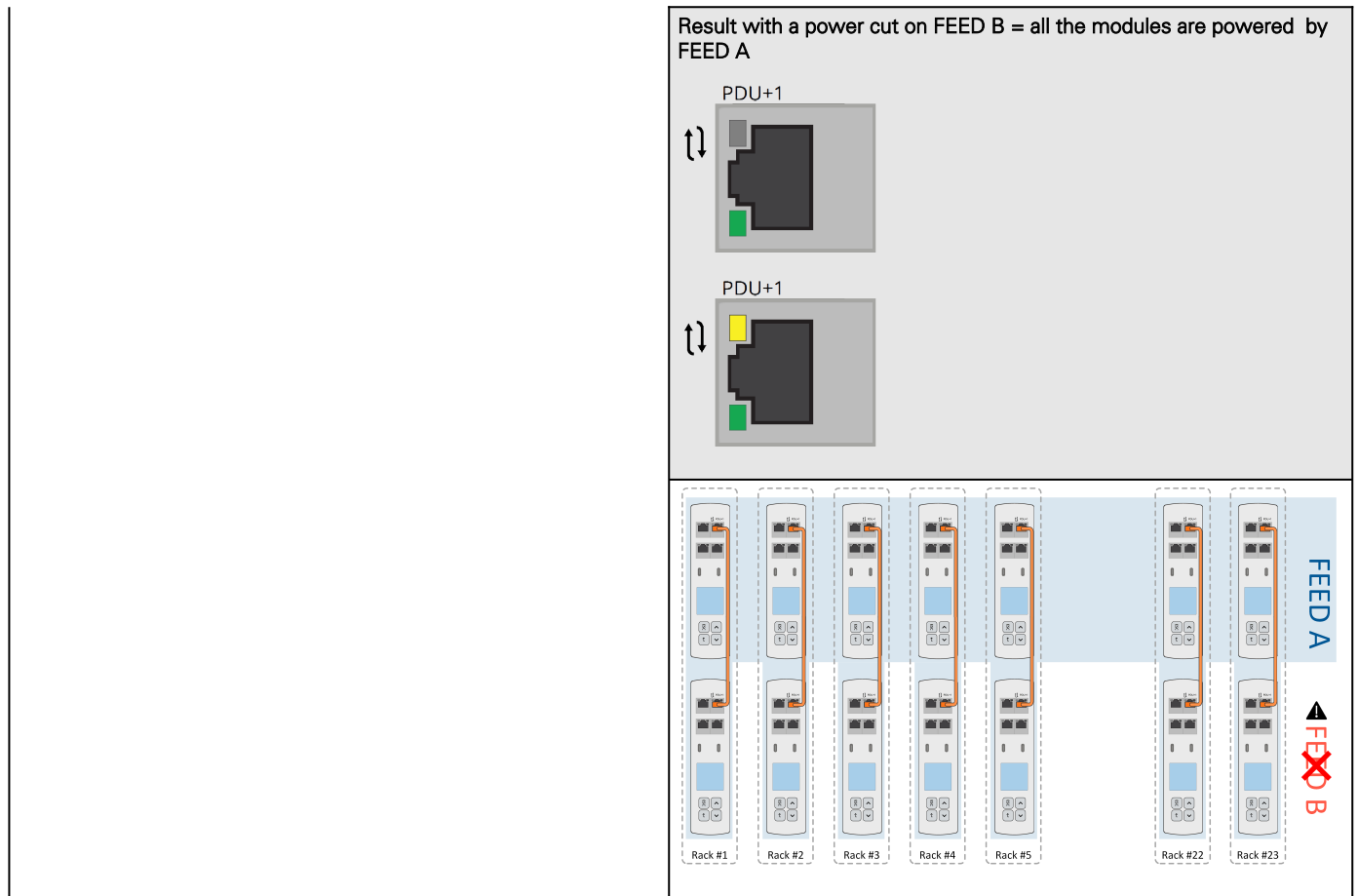

**Warning:**

In case of a power cut on FEED A, if the module of the FEED B is rebooted, the module on FEED A will reboot as well

## 2.1.2 Examples

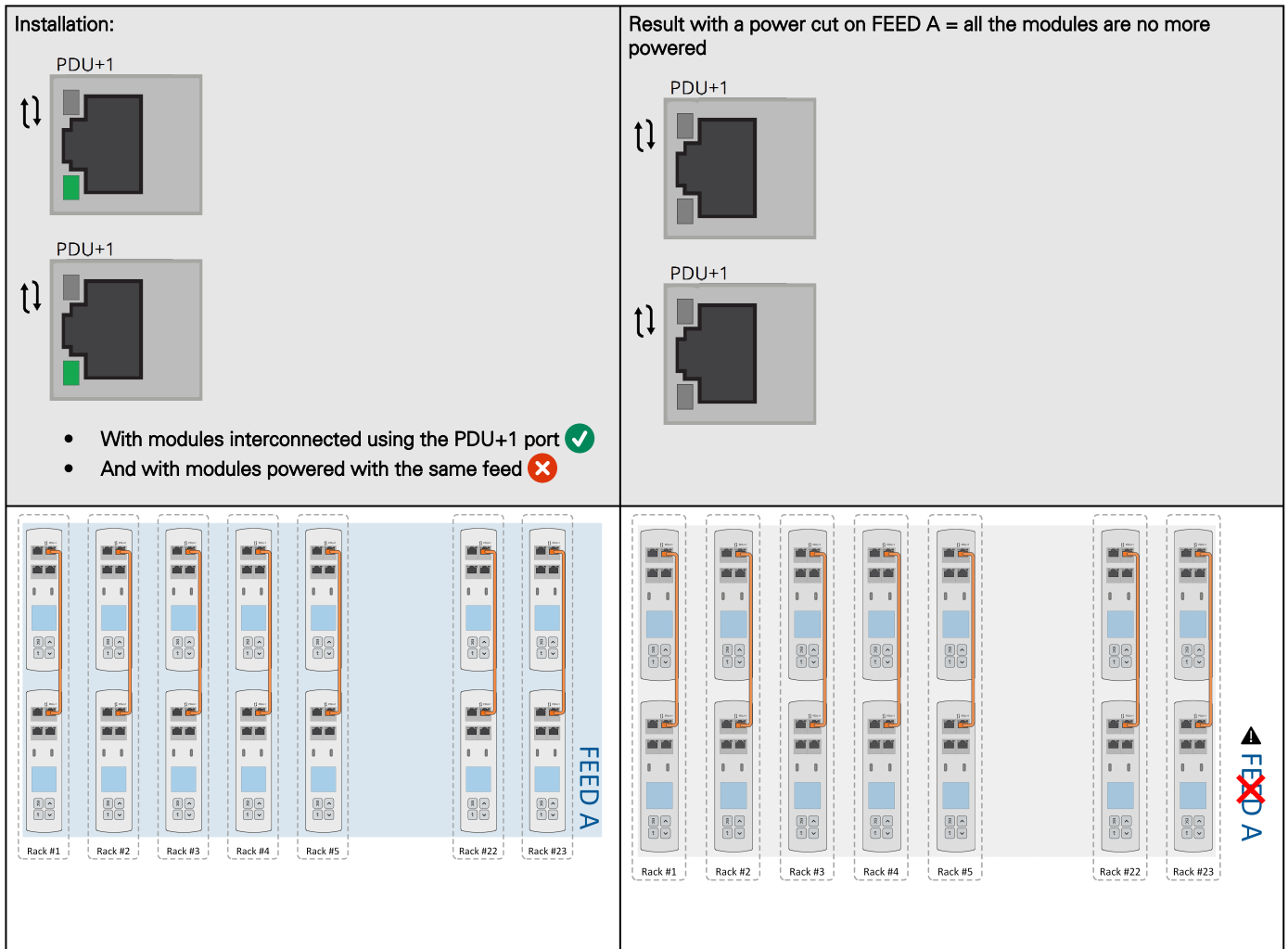
### 2.1.2.1 Power redundancy connection with 2 feeds = OK



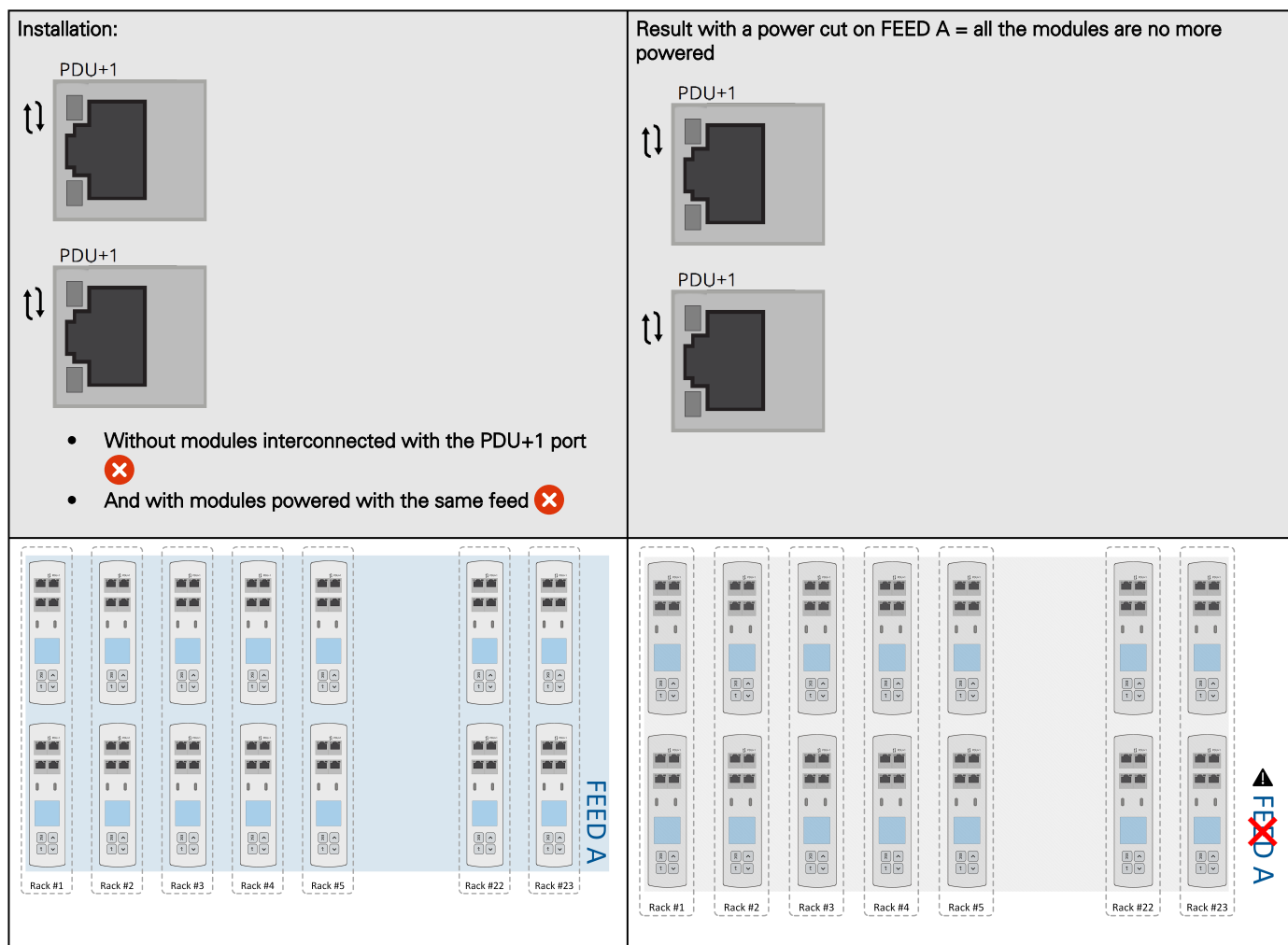




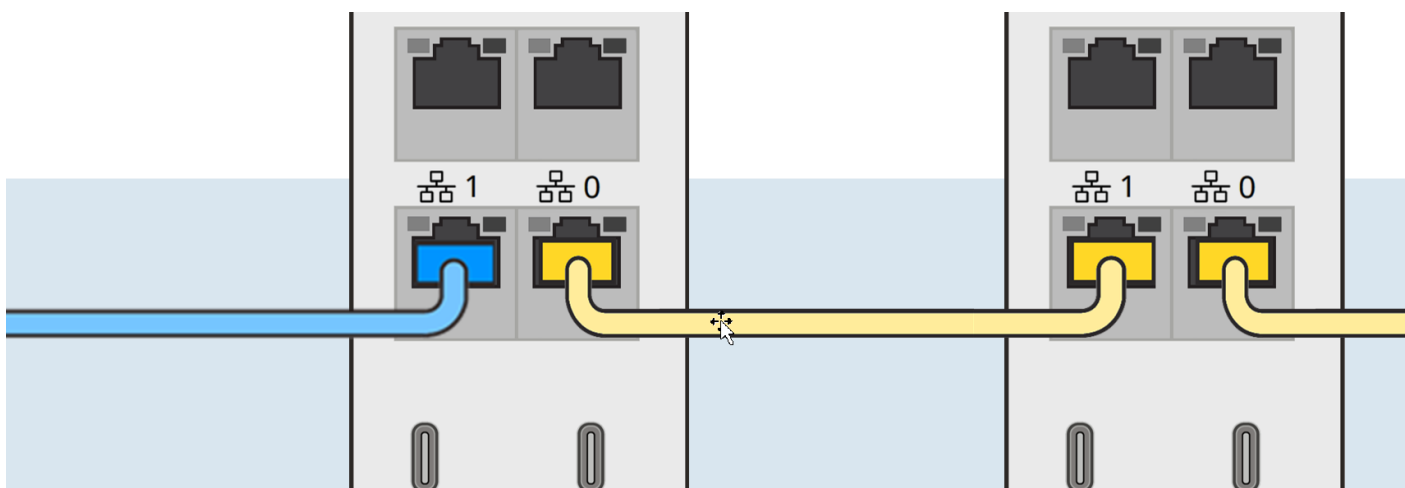
## 2.1.2.2 Power redundancy connection but with only one feed = Not OK

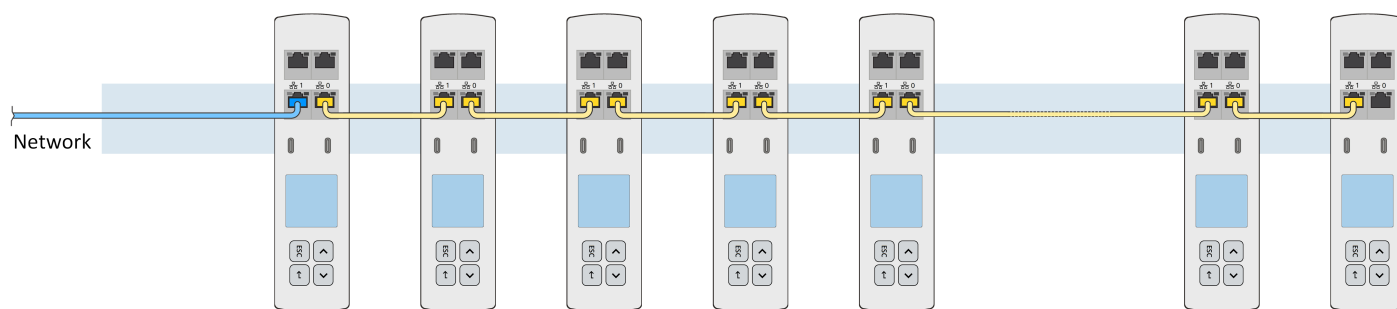


### 2.1.2.3 No power redundancy connection = Not OK



## 2.2 Connecting PDUs in cascade





## 2.3 Accessing the Network Module

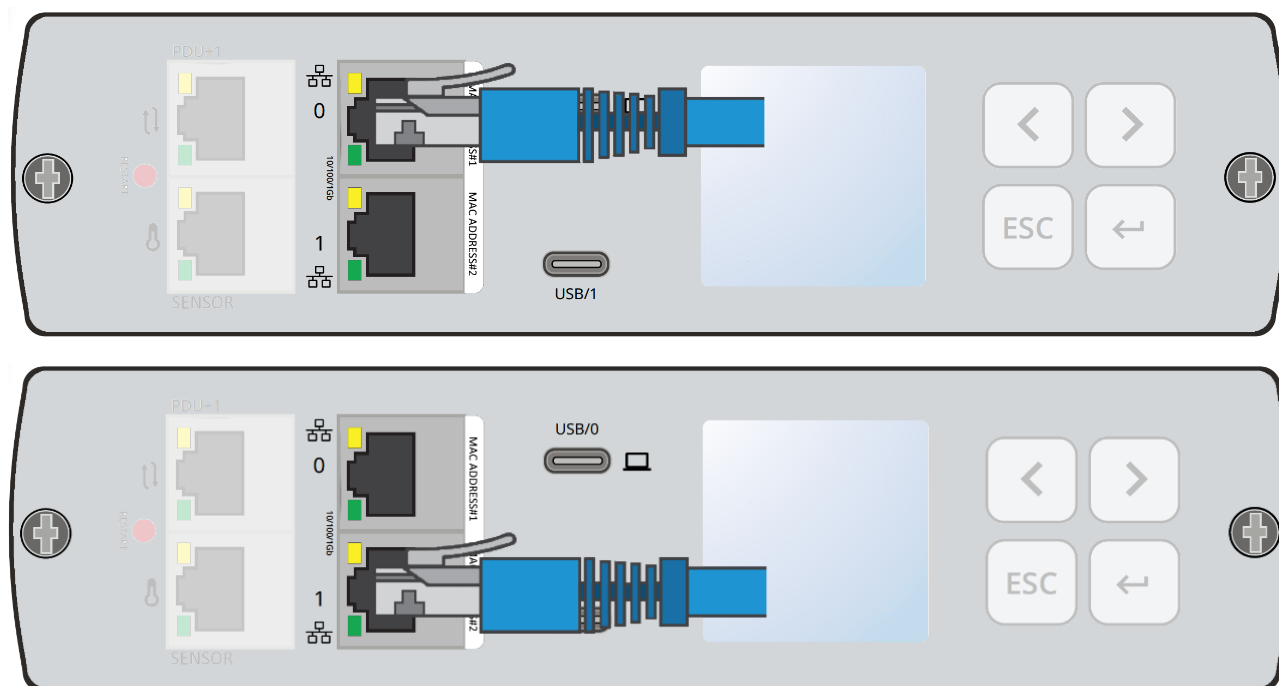
### 2.3.1 Accessing the web interface through Network

#### 2.3.1.1 Connecting the network cable



Security settings in the Network Module may be in their default states.  
For maximum security, configure through a USB connection before connecting the network cable.

Connect a standard *gigabit compatible shielded ethernet cable (F/UTP or F/FTP)* between the network connector on the Network Module and a network jack.



#### 2.3.1.2 Accessing the web interface



It is highly recommended that browser access to the Network Module is isolated from outside access using a firewall or isolated network.

**STEP 1** – On a network computer, launch a supported web browser. The browser window appears.

**STEP 2** – In the Address/Location field, enter `https://[IP address]` with the static IP address of the Network Module.

**STEP 3** – The login screen appears.

**STEP 4** – Enter the user name in the User Name field. The default user name is **admin**.

**STEP 5** – Enter the password in the Password field. The default password is **admin**.

**STEP 6** – The password must be changed at first login.

**STEP 7** – Click **Login**. The Network Module web interface appears.

At first login:

**STEP 8** - Accept License Agreement. The Network Module web interface appears.

**STEP 9** - Set the LCD PIN code (Can be disabled).



## 2.3.2 Finding and setting the IP address

### 2.3.2.1 Your network is equipped with a BOOTP/DHCP server (default)

#### 2.3.2.1.1 Read from the device LCD

If your device has an LCD, from the LCD's menu, navigate to Identification>>>"COM card IPv4".

- Note the IP address of the card.
- Go to the section: Accessing the web interface through Network.

#### 2.3.2.1.2 With web browser through the configuration port

For example, if your device does not have an LCD, the IP address can be discovered by accessing the web interface through RNDIS and browsing to Settings>Network.

To access the web interface through RNDIS, see the [Accessing the web interface through RNDIS](#) section.

- Navigate to Contextual help>>>Settings>>>Network & Protocol>>>IPv4.
- Read the IPv4 settings.

### 2.3.2.2 Your network is not equipped with a BOOTP/DHCP server

#### 2.3.2.2.1 Define from the configuration port

The IP address can be defined by accessing the web interface through RNDIS.

To access web interface through RNDIS, see the [Accessing the web interface through RNDIS](#) section.

Define the IP settings:

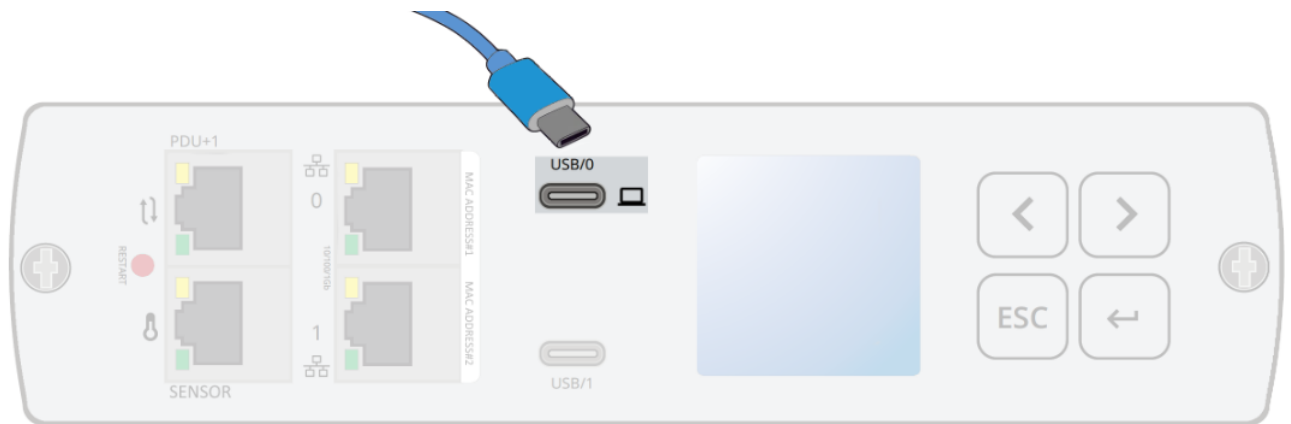
- Navigate to Contextual help>>>Settings>>>Network & Protocol>>>IPv4.
- Select Manual (Static IP).
- Input the following information: Address, Subnet Mask, Default Gateway
- Save the changes.

## 2.3.3 Accessing the web interface through RNDIS

This connection is used to access and configure the Network Module network settings locally through a RNDIS (Ethernet over USB interface).

### 2.3.3.1 Connecting the configuration cable

1. Connect a USB-C cable to the USB-C connector on the host computer.
2. Connect the cable to the Settings connector on the Network Module.



### 2.3.3.2 Web interface access through RNDIS

#### 2.3.3.2.1 Configuring the RNDIS

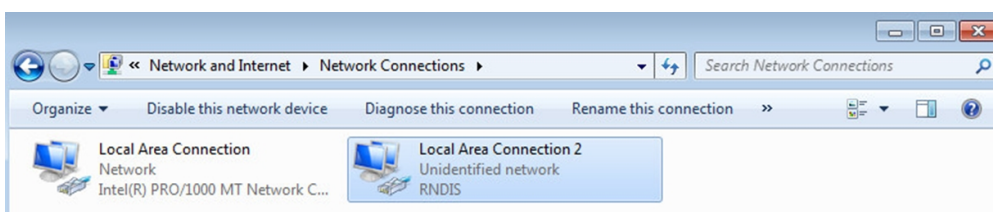
##### a Automatic configuration



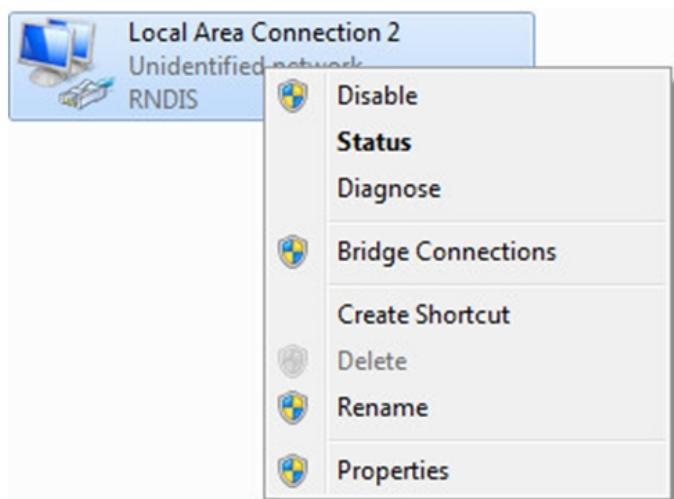
RNDIS driver is used to emulate a network connection from USB. After the card is connected to the PC, **Windows®** OS will automatically search for the RNDIS driver. On some computers, the OS can find the RNDIS driver then configuration is completed, and you can go to Accessing the web interface. On some others it may fail then proceed to manual configuration.

##### b Manual configuration

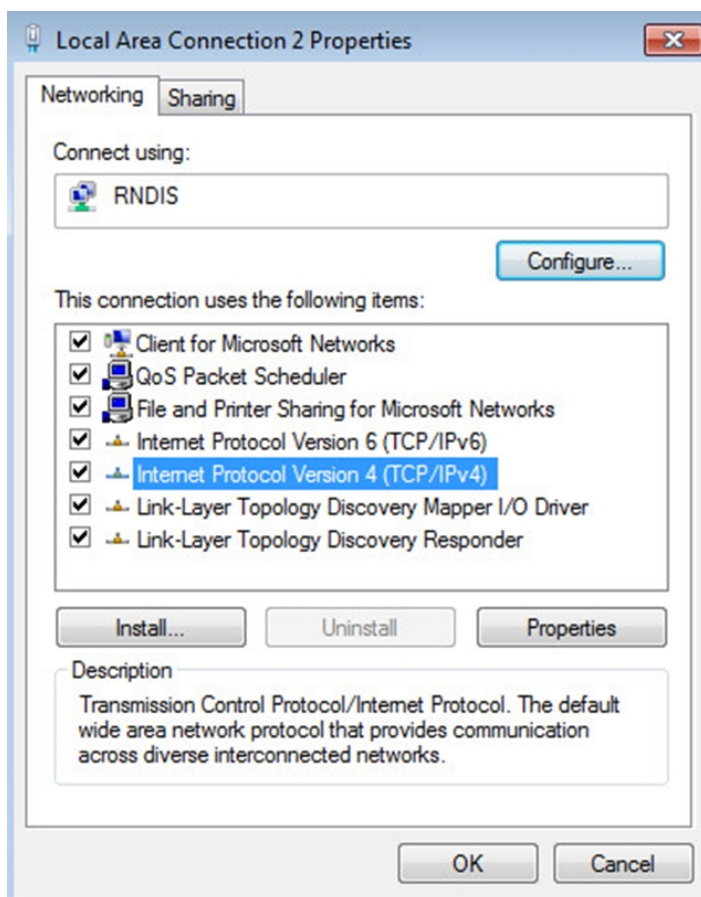
**STEP 1** – In case **Windows®** OS fails to find driver automatically, go to the Windows control panel>Network and sharing center>Local area connection



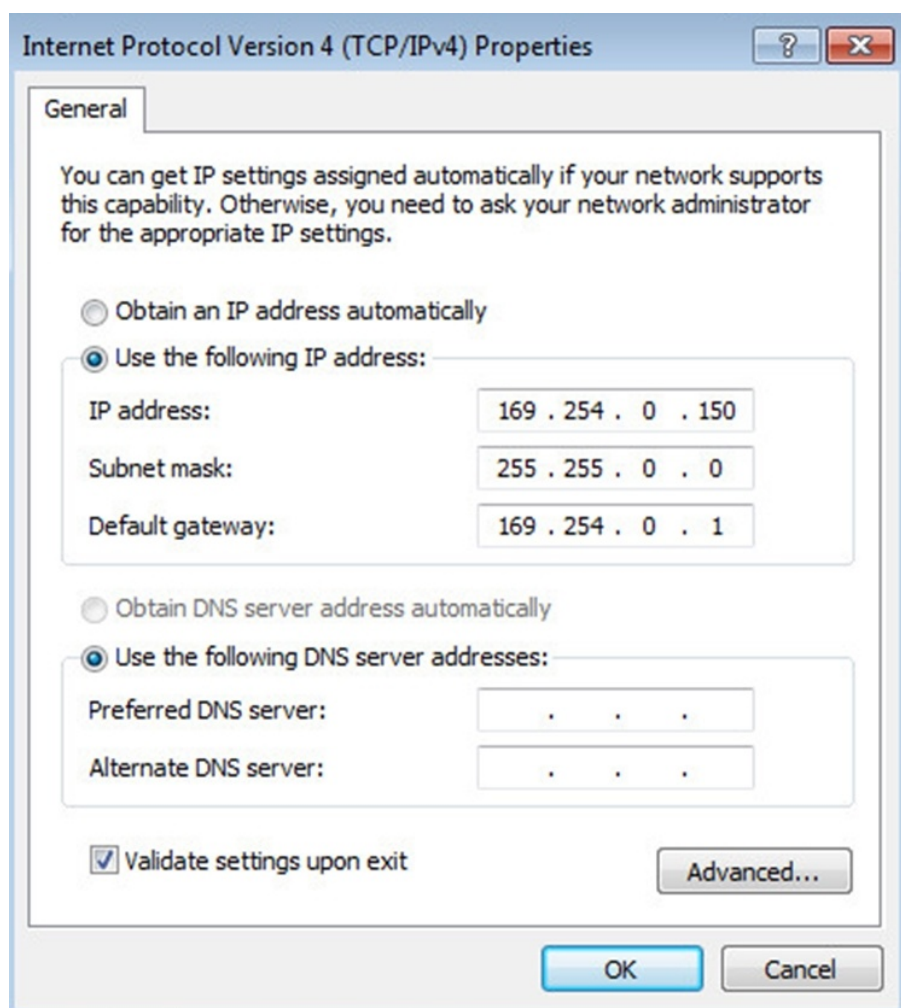
**STEP 2** – Right click on the RNDIS local area connection and select Properties.



**STEP 3** – Select Internet Protocol Version 4 (TCP/IPv4) and press the Properties button



**STEP 4** – Then enter the configuration as below and validate (IP = 169.254.0.150 and mask = 255.255.0.0), click OK, then click on Close.



### 2.3.3.2.2 Accessing the web interface

**STEP 1** – Be sure that the Device is powered on.

**STEP 2** – On the host computer, download the rndis.7z file from the website [www.eaton.com/downloads](http://www.eaton.com/downloads) and extract it. For more information, navigate to [Servicing the Network Management Module>>>Accessing to the latest Network Module firmware/driver](#) section.

**STEP 3** – Launch setProxy.bat to add 169.254.\* in proxy's exceptions list, if needed. For manual configuration, navigate to [Installing the Network Management Module>>>Accessing the Network Module>>>Modifying the Proxy exception list](#) section in the full documentation.

**STEP 4** – Launch a supported browser, the browser window appears.

**STEP 5** – In the Address/Location field, enter: **https://169.254.0.1**, the static IP address of the Network Module for RNDIS. The log in screen appears.

**STEP 6** – Enter the user name in the User Name field. The default user name is **admin**.

**STEP 7** – Enter the password in the Password field. The default password is **admin**.

**STEP 8** – Click **Login**. The Network Module local web interface appears.

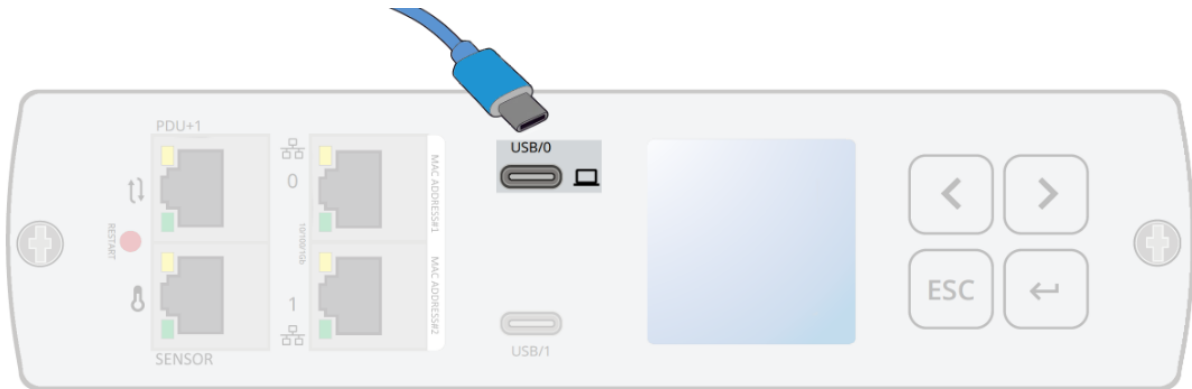
## 2.3.4 Accessing the card through serial terminal emulation

This connection is used to access and configure the Network Module network settings locally through Serial (Serial over USB interface).

### 2.3.4.1 Connecting the configuration cable

**STEP 1** – Connect the USB-C cable to a USB connector on the host computer (RS232 to RS232 cable).

**STEP 2** – Connect the cable to the USB/0 connector on the Network Module.



### 2.3.4.2 Manual configuration of the serial connection

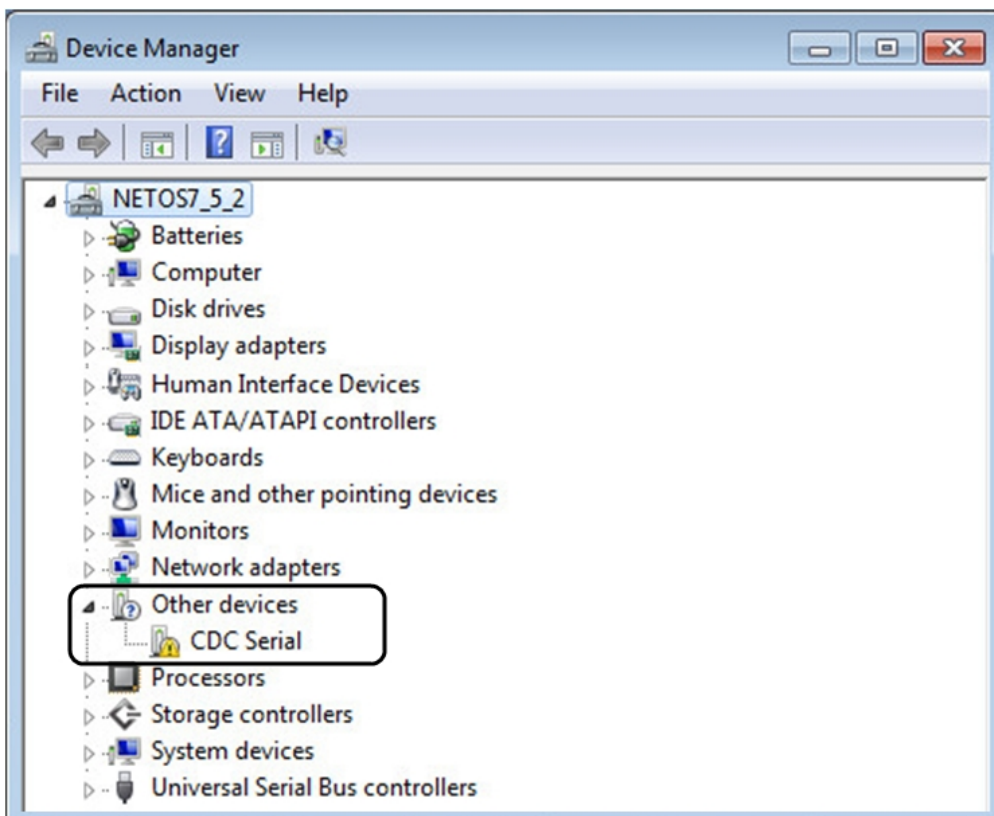


Serial driver is used to emulate a serial connection from USB.  
After the card is connected to the PC, manual configuration of the driver is needed for **Windows®** OS to discover the serial connection.

**STEP 1** – On the host computer, download the rndis.7z file from the website [www.eaton.com/downloads](http://www.eaton.com/downloads) and extract it.

**STEP 2** – Plug the USB cable and go to **Windows®** Device Manager.

**STEP 3** – Check the CDC Serial in the list, if it is with a yellow exclamation mark implying that driver has not been installed follow the steps 4-5-6-7 otherwise configuration is OK.



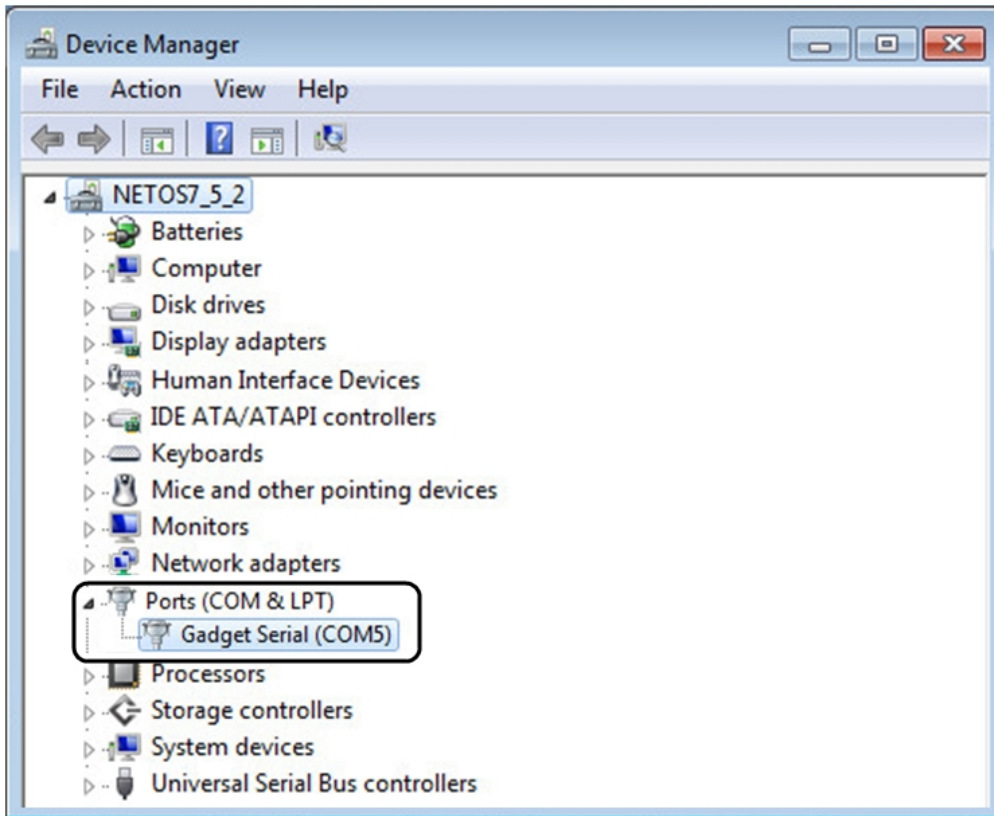


**STEP 4** – Right click on it and select Update Driver Software. When prompted to choose how to search for device driver software, choose Browse my computer for driver software. Select Let me pick from a list of device drivers on my computer.

**STEP 5** – Select the folder where you have previously downloaded the driver file Click on Next.

**STEP 6** – A warning window will come up because the driver is not signed. Select Install this driver software anyway

**STEP 7** – The installation is successful when the COM port number is displayed for the Gadget Serial device in the **Windows®** Device Manager.



### 2.3.4.3 Accessing the card through Serial

It is intended mainly for automated configuration of the network and time settings of the network card. It can also be used for troubleshooting and remote reboot/reset of the network interface in case the web user interface is not accessible.

CLI can be accessed through:

- SSH
- Serial terminal emulation.



Changing network parameters may cause the card to become unavailable remotely. If this happens it can only be reconfigured locally through USB.



You can see this list of available commands by typing in the CLI: **?**  
You can see the help by typing in the CLI: **help**

For more details, refer to [Information>>>CLI](#) section

### 2.3.5 Modifying the Proxy exception list

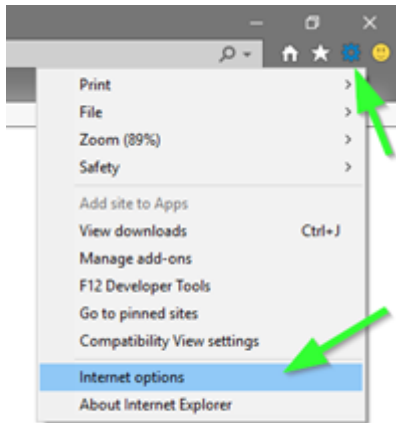
To connect to the Network Module via a USB cable and your system uses a Proxy server to connect to the internet, the proxy settings can reject the IP address 169.254.0.1.

The 169.254. \* Sequence is used to set up communication with devices via a physical connection.

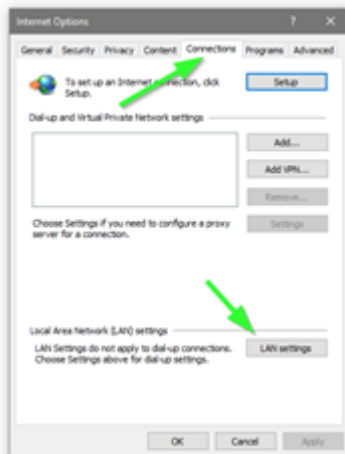
To activate this connection, exceptions will have to be made in the proxy settings.

## Accessing the Network Module

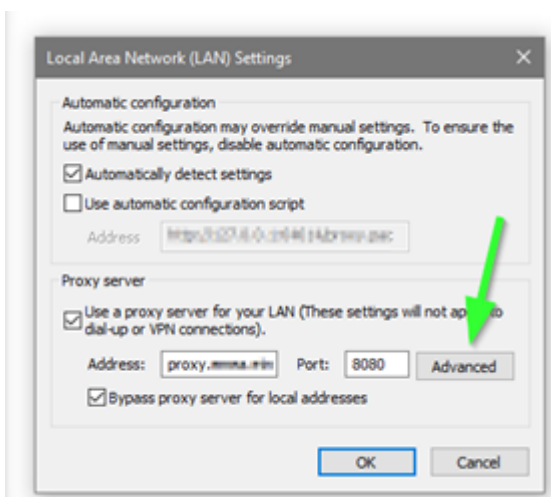
- Open Internet Explorer
- Navigate to settings, Internet options;



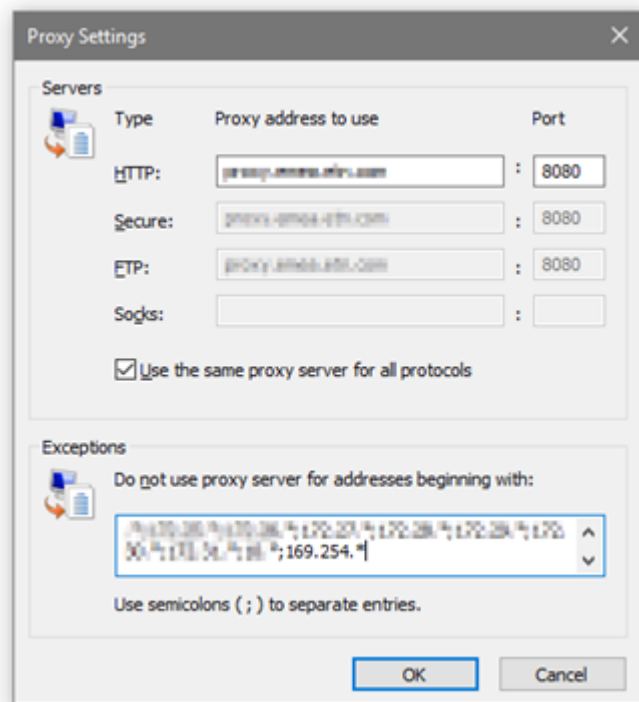
- Select the Connections tab
- Press LAN Settings



- Press ADVANCED



- Add the address 169.254. \*



- Press OK.
- Close Internet Explorer and re-open it.
- Now you can access the address 169.254.0.1 with Internet Explorer and any other browser.

## 3 LCD interface operation

### 3.1 Display and control buttons

#### 3.1.1 Presentation

The PDU has a four-button, graphical LCD display. Use the control buttons to change the screen display, retrieve specific performance data, or change configuration values.




The display view can also change automatically.

For example, the display changes to show active alarms as they occur, or particular displays update due to a change in operating state.

A backlight is used to light up the display with white and blue:

- The backlight turns off automatically when no button has been pressed for 15 minutes and there is no active alarm.
- Any active alarm will cause the backlight to turn on automatically.

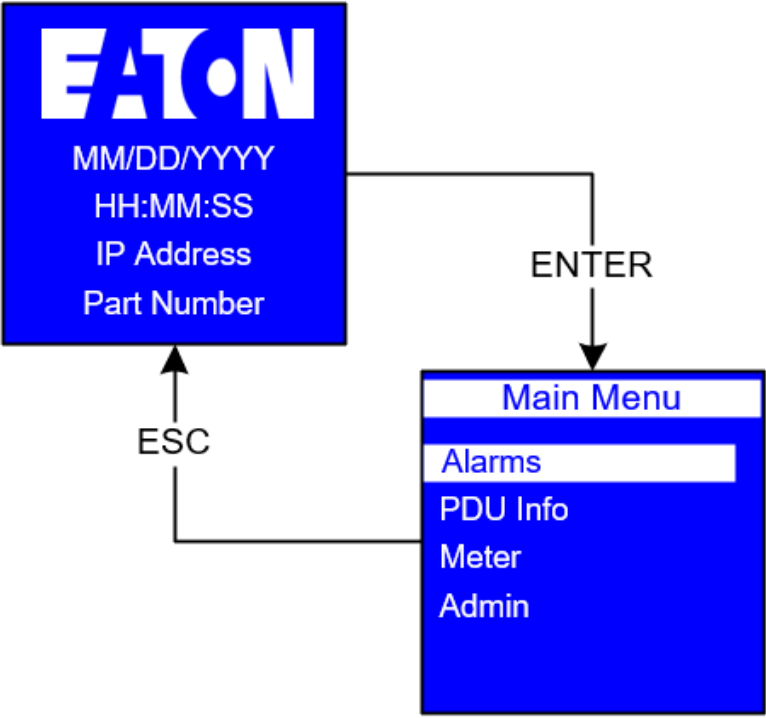
#### 3.1.2 How to use the control buttons

Button	When on the Main menu	When in Screensaver mode	When in Menu mode
	Returns to the Start-up screen.	Returns to the previous display screen before entering the screensaver mode.	Returns to the previous display screen.
	Opens the selected menu. <b>NOTE:</b> When menu items are highlighted, they are selected.	Returns to the previous display screen before entering the screensaver mode.	Signals that you want to set the values as displayed on the screen. <b>NOTE:</b> On information screens, this button has no action.
	Scrolls up or down through the list of menu items.	Returns to the previous display screen before entering the screensaver mode.	Scrolls up or down to the next screen or value.

### 3.2 Operation mode

#### 3.2.1 Startup screen

When the PDU powers up, the Startup screen displays. Press **ENTER** to go to the Main Menu.

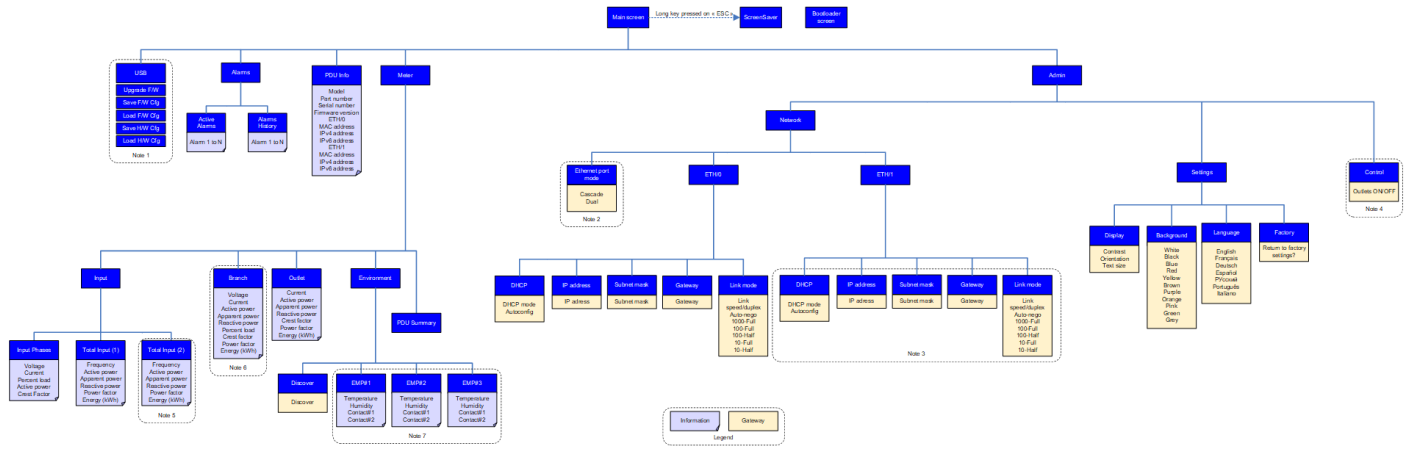


### 3.2.2 Main menu selections

The PDU menu provides useful performance information, alarms, PDU identification, and configuration settings.

- Use the scroll buttons to select a menu item from the Main Menu.
- Selected menu items are highlighted and display as blue text on a white bar.
- Press **ENTER** to go the selected menu item.
- Press **ESC** from the Main Menu to return to the Startup Screen.

#### 3.2.2.1 Menu structure



- Note 1 :** This menu and submenus are only available if USB ports are enabled through the web page and if an USB device is plugged.
- Note 2 :** This menu is only available is single ETH mode is not selected.
- Note 3 :** These submenus are only available if dual network is selected.
- Note 4 :** This menu is not available for Metered Input (MI) and Metered Outlet (MO).

**Note 5** : This menu is only available for dual inputs PDU.  
**Note 6** : This menu is only for sections with current measurement.  
**Note 7** : These menus are only available if Environmental Monitoring Probes (EMP) are plugged.

3.2.2.2 Available menu by topologies

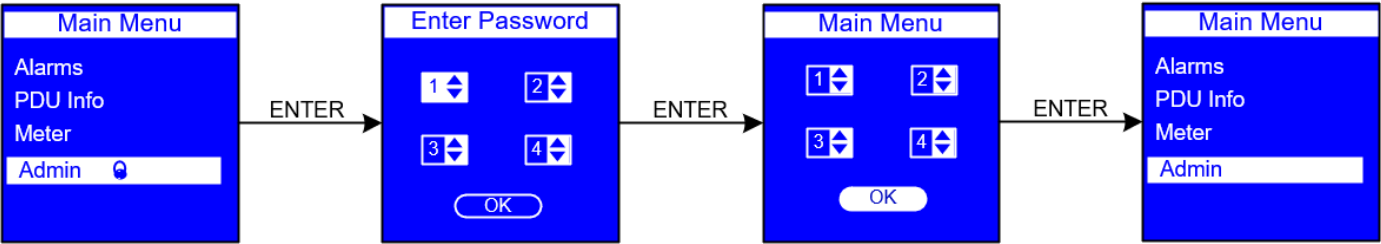
Topologies			MI	AM	SW	MA	DI PDU	3PI DI PDU	3PI PDU	PDU + EMP
Alarms	Active Alarms		✓	✓	✓	✓	✓	✓	✓	✓
	Alarm History		✓	✓	✓	✓	✓	✓	✓	✓
PDU Info			✓	✓	✓	✓	✓	✓	✓	✓
Meter	Input	Input Phase						✓	✓	
		Total Input [1]	✓	✓	✓	✓	✓	✓	✓	✓
		Total Input [2]					✓	✓		
	Branch		✓	✓	✓	✓	✓	✓	✓	✓
	Outlet			✓		✓				
	Environment									✓
	PDU Summary		✓	✓	✓	✓	✓	✓	✓	✓
Network			✓	✓	✓	✓	✓	✓	✓	✓
Settings			✓	✓	✓	✓	✓	✓	✓	✓
Control					✓	✓				

3.2.3 Password protection menus

Network, Control and the Settings menus can be password-protected.

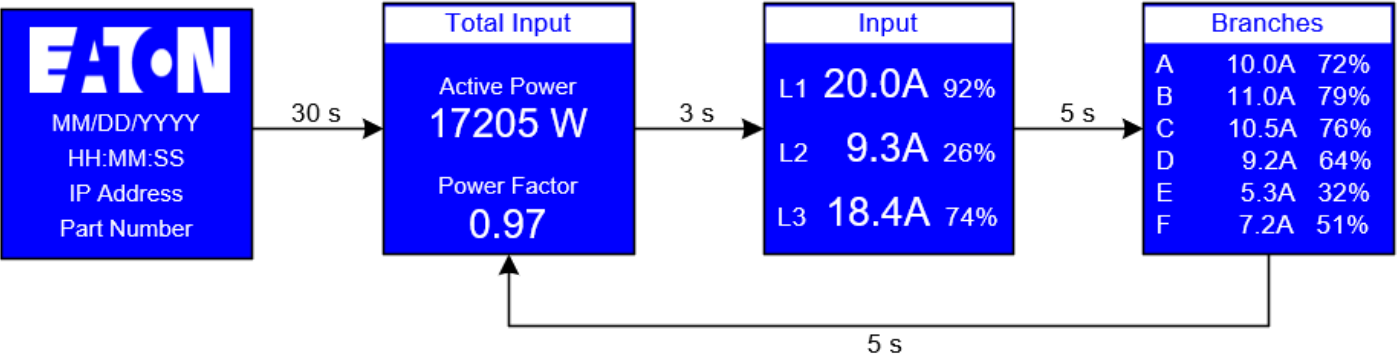
This locks out the menus to any user who does not know the password. Password configuration can only be done through the [Web interface](#).

3.2.3.1 Sequence to enter a password for a locked menu

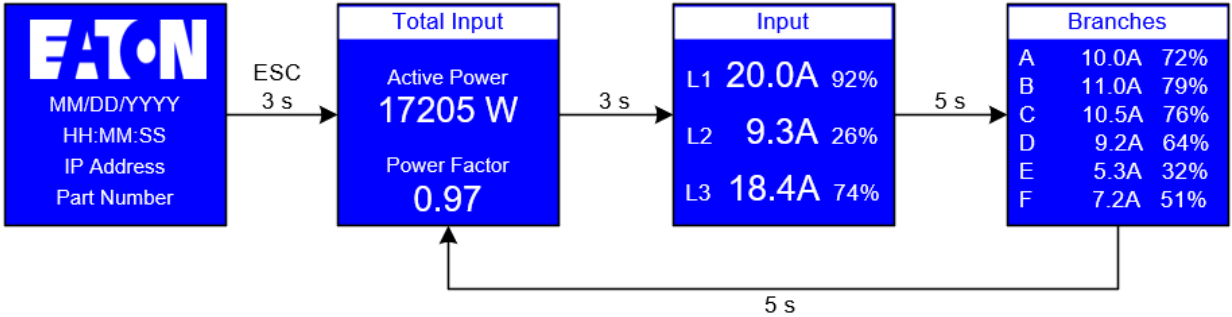


### 3.2.4 Screensaver

The screensaver displays automatically after 30 seconds of inactivity from the start-up screen, a menu, or a submenu. Values are reset every five seconds. These cycles are not user-configurable.

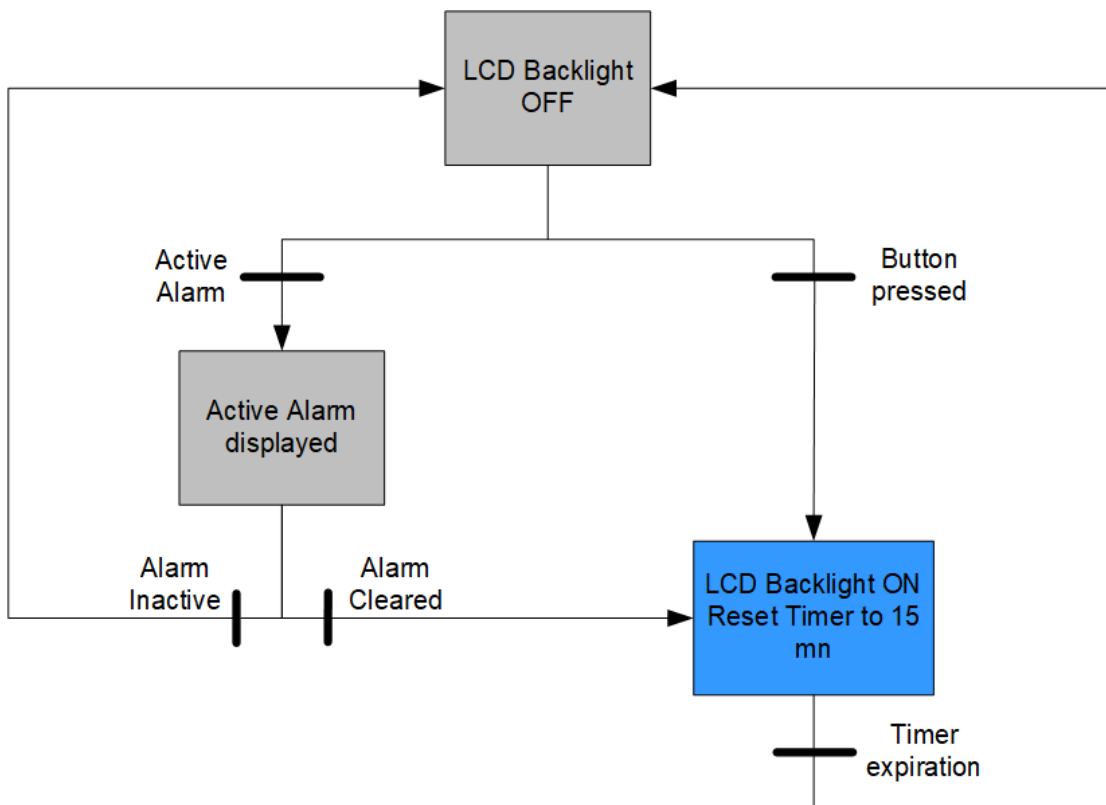


Access to the screensaver information from the startup screen is enabled with a long key press on **ESC**, it can also be used as a screensaver deactivation.



### 3.2.5 Backlight

LCD backlight remains OFF until a button is pressed or if an alarm occurs.

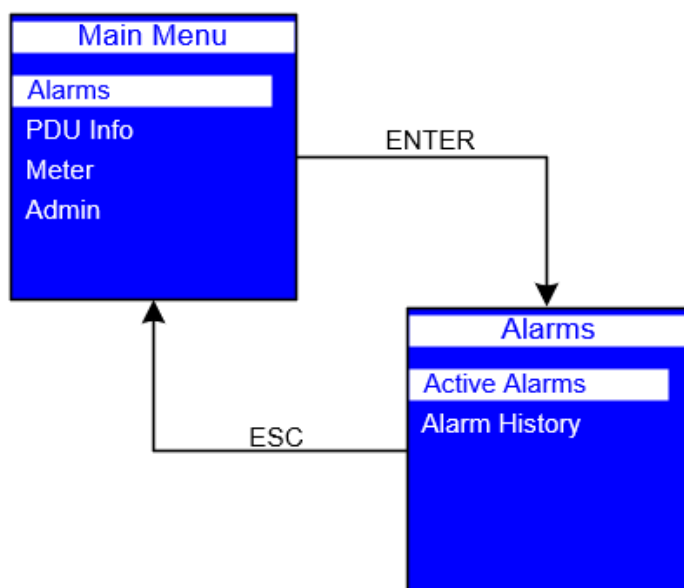


When backlight is OFF:

- The text is extremely hard to see
- Pressing any button does not act as a validation or selection but only to turn the backlight ON

### 3.3 Alarms

The Alarms menu gathers all the alarms in two submenus:

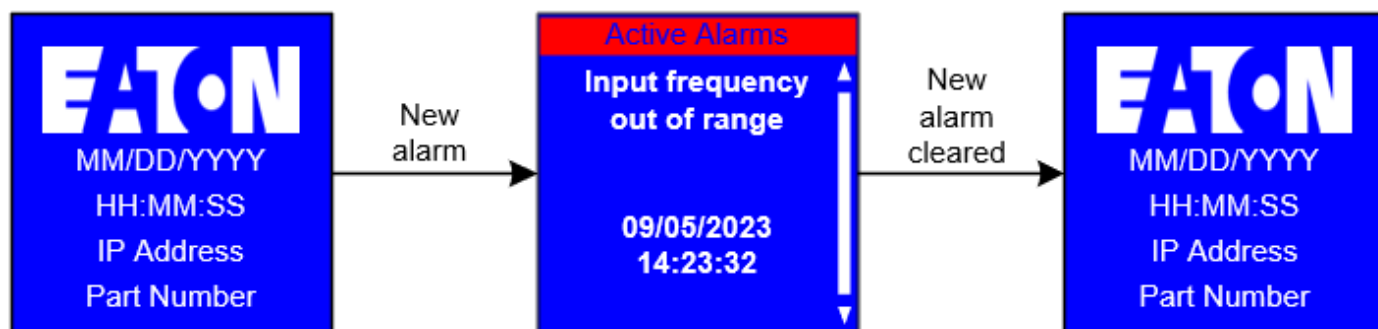




### 3.3.1 Active alarms

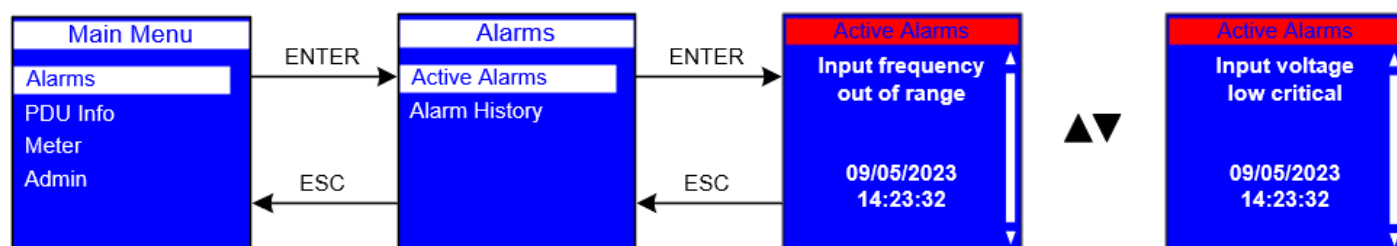
#### 3.3.1.1 Display when an alarm occurs

The Active Alarms menu filters and displays only active alarms for the PDU. Active alarm screens have priority over other screens. When an alarm occurs, the Active Alarms screen replaces the current screen and the border becomes red. Up to 100 active alarms can be displayed.



#### 3.3.1.2 Access from the main menu

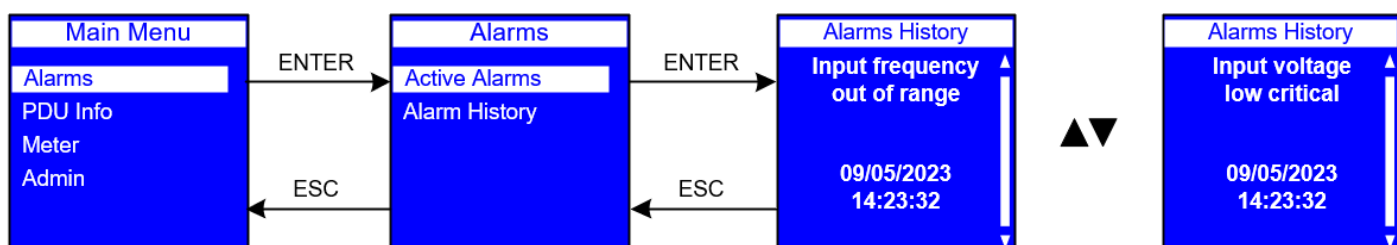
On the Main Menu, scroll up or down to highlight Active Alarms. Press ENTER to display the first active alarm screen. Scroll up or down if needed to view active alarm data. When you finish your review, press ESC to return to the previous menu. If the backlight was blinking red to indicate an active alarm, the backlight returns to normal.



### 3.3.2 Alarms history

The Alarms History menu allows you to scroll through the last 50 logged alarms, beginning with the most recent alarm. The Alarms History screens contain the type of alarm, the date (MM/DD/YYYY), and time (hh:mm:ss) when the alarm occurred.

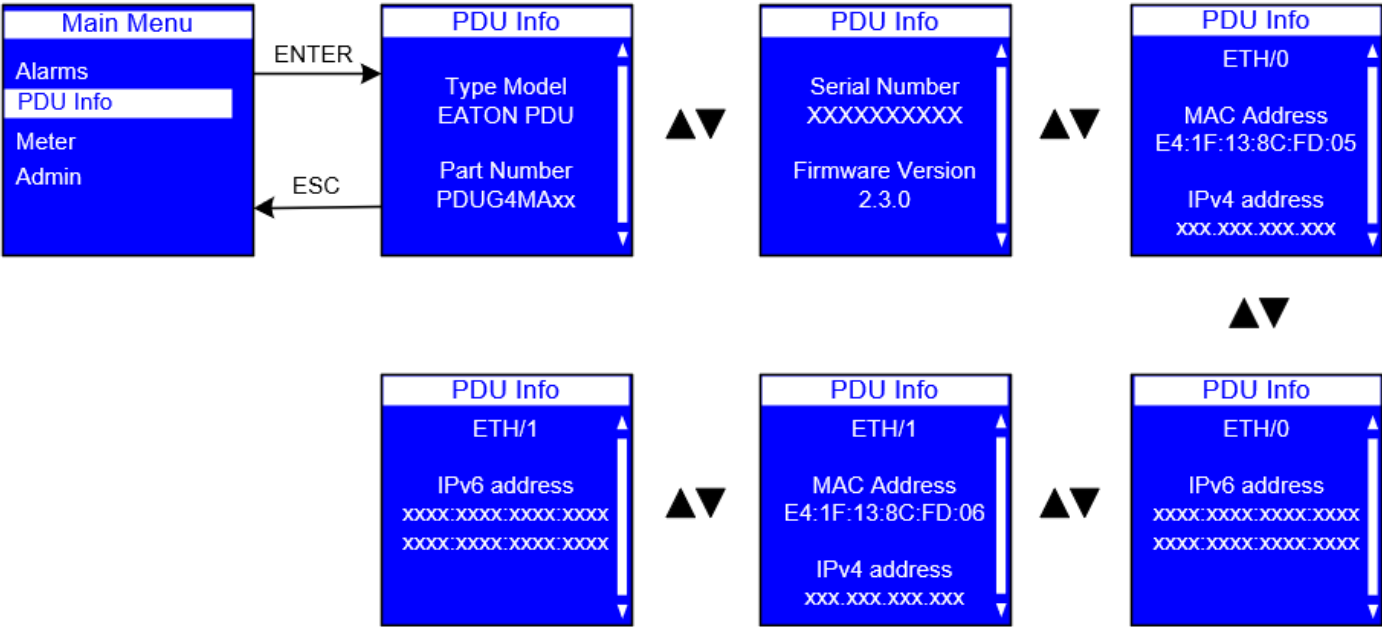
On the Alarm menu, scroll up or down to highlight Alarms History. Press ENTER to display the most recent alarm in the history log. Scroll up or down to view the alarms. When you finish your review, press ESC to return



### 3.4 PDU info

The PDU Info menu provides identification information for this PDU. The identification information includes the PDU model type and part number, serial number, PDU Gigabit Network Module (GNM) firmware version number, IP address, and PDU Gigabit Network Module (GNM) MAC (Media Access Control) address. These are information-only screens.

On the Main Menu, scroll up or down to highlight PDU Info. Press ENTER to navigate to each screen. Scroll up or down on the screen if needed to view the PDU information displays. Press ESC to return to the previous menu.




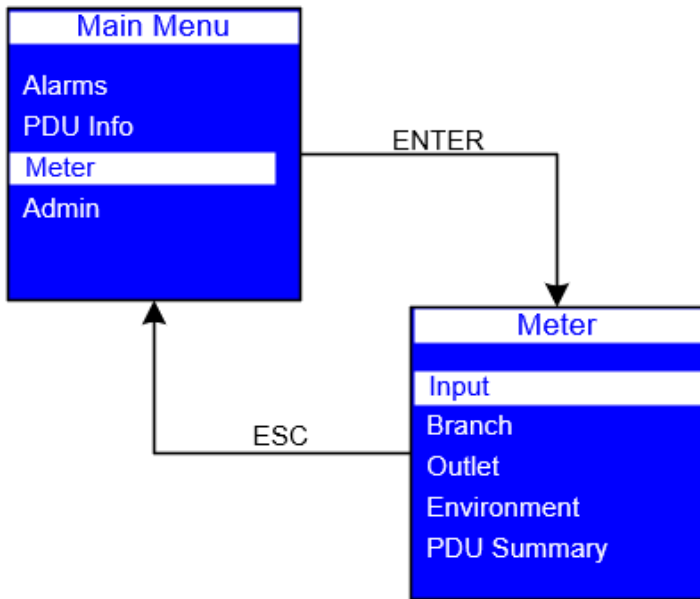
### 3.5 Meter

The Meter menu provides measurement data for the following submenus:

- Input
- Branch
- Outlet
- Enviroment
- PDU Summary

On the Main Menu, scroll up or down to highlight Meter. Press ENTER. Scroll up or down to select a submenu and press ENTER to display the submenu options. Press ESC to return to the previous menu.

**NOTE :** The measurement data for each screen is refreshed every two seconds.



### 3.5.1 Input

These screens display Total Input data measurements for PDUs. In addition to Total Input measurements, you can view Phase Input data measurements for 3Ph, split-phase, and dual input PDUs. Depending on the PDU electrical topology, different PDU measures will display in the Total Input and the Input Phase meter screens.

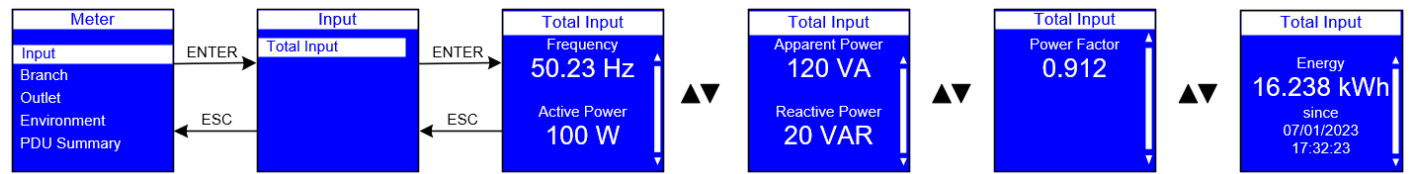
The table below shows which measures will be present.

Measure	Total Input	Wye-Wired Input Phase	Delta-Wired Input Phase
Frequency	✓	✗	✗
Voltage	✗	✓	✓
Current	✗	✓	✓
Percent Load	✗	✓	✓
Active Power	✓	✓	✗
Crest Factor	✗	✓	✓
Apparent Power	✓	✗	✗
Reactive Power	✓	✗	✗
Power Factor	✓	✗	✗
Energy	✓	✗	✗
Peak Power	✓	✗	✗

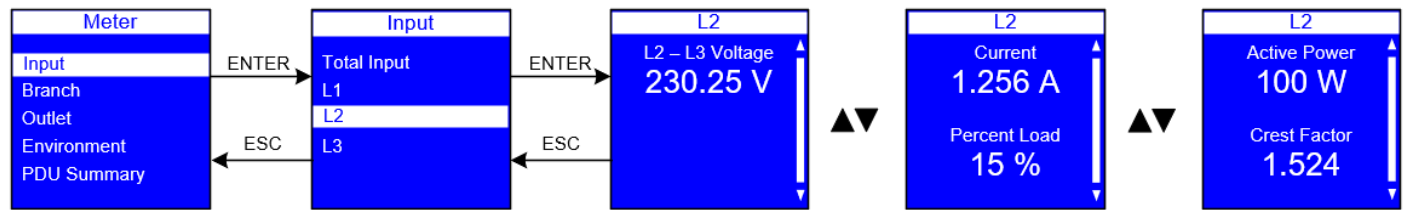
### 3.5.1.1 Total Input Meter Data

On the Meter menu, scroll up or down to highlight Input . Press ENTER to display the Total Input submenu for your 1Ph, 3Ph, split-phase, or dual input PDU. Press ENTER again to see Total Input meter data measurements. Scroll up or down to review other Total Input meter data measurements. After you review the data, you can press ESC to return to the Input Meter menu and select L1, L2, or L3 to see Phase Input measurements. Press ESC to return to the previous menu.

Example for 1Ph total display:



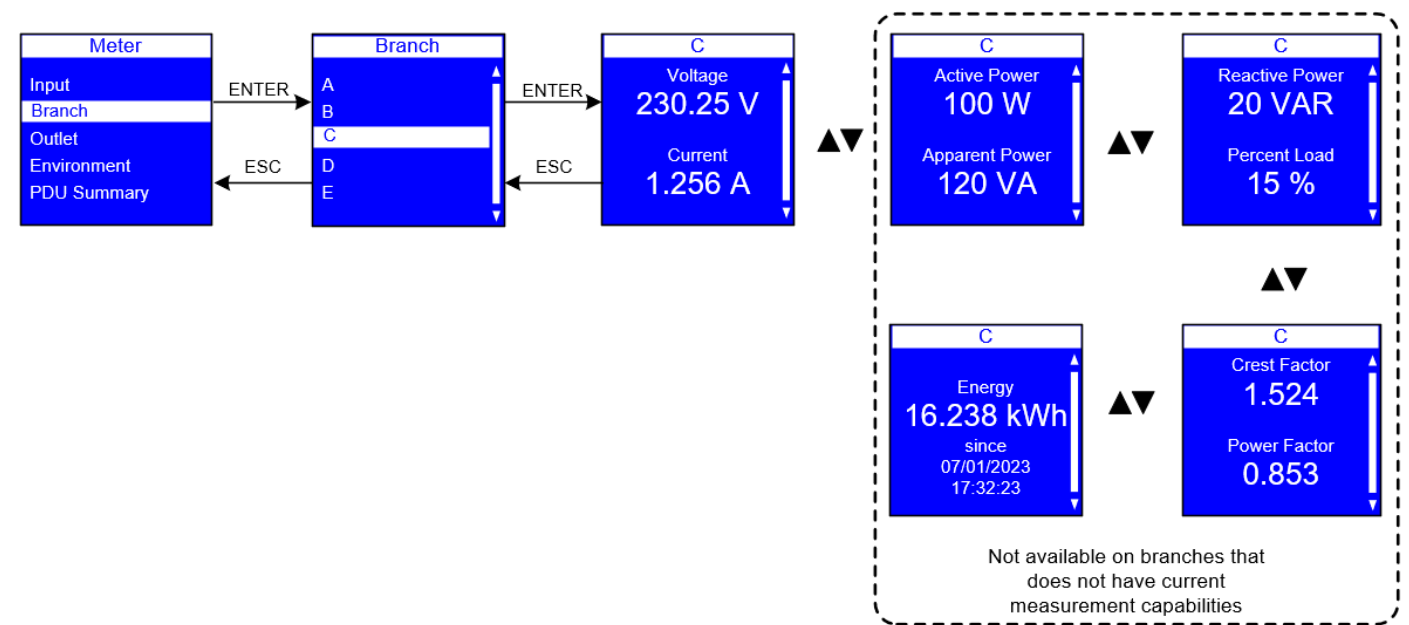
Example for 3Ph second phase display :



### 3.5.2 Branch

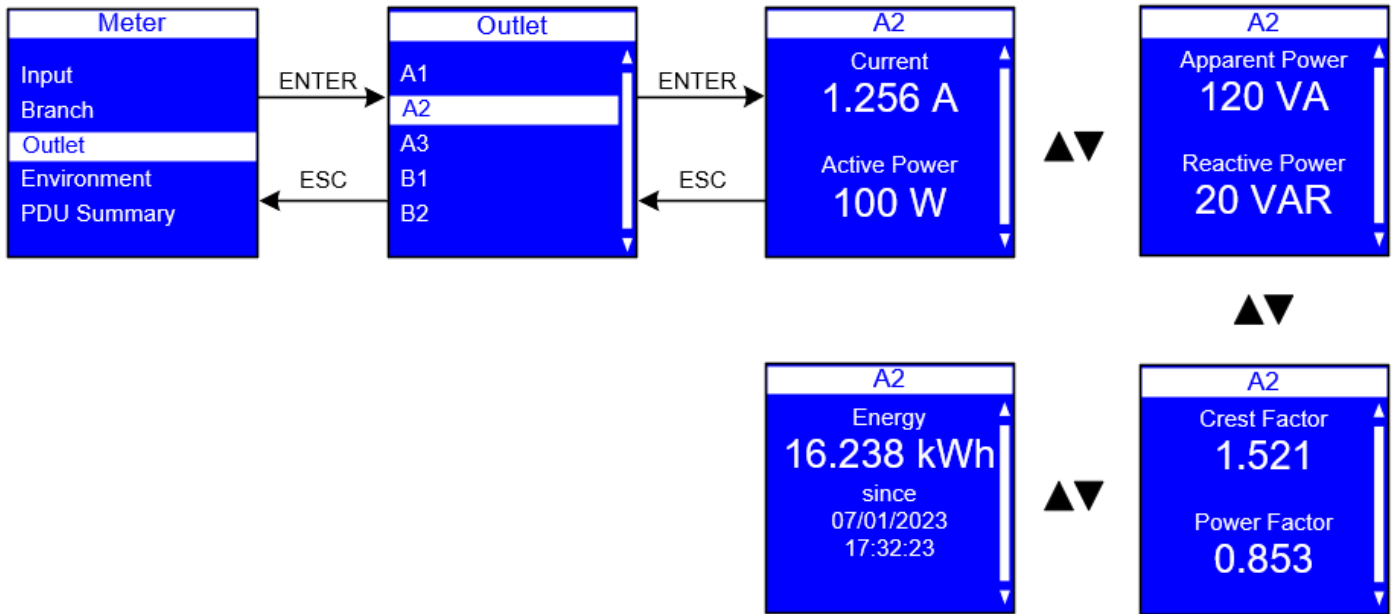
Branch measurements include voltage data for all PDU branches. Other branch measurements are only available on PDUs that have current measurement capabilities.

On the Meter menu, scroll up or down to highlight Branch. Press ENTER to display the Branch submenu. Scroll up or down to review the data for your selection. After you review the data, press ESC twice to return to the previous menu



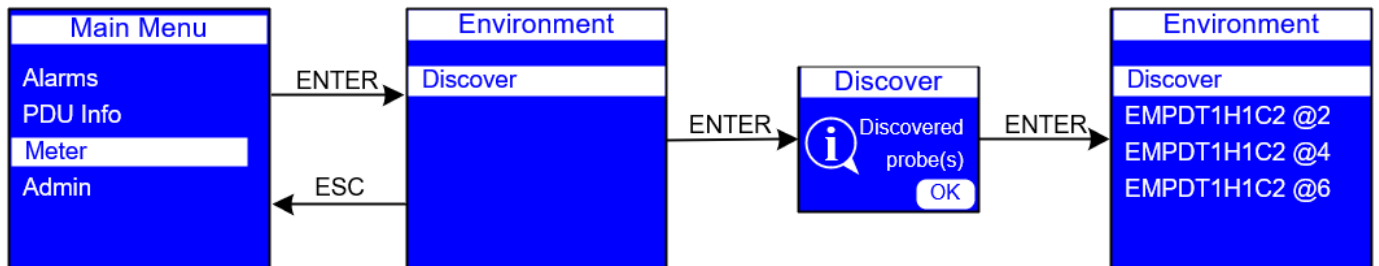
### 3.5.3 Outlet

On the Meter menu, scroll up or down to highlight Outlet. Press ENTER to display the Outlet submenu. Scroll up or down to review the data for your selection. After you review the data, press ESC twice to return to the previous menu .



### 3.5.4 Environment

The Environment submenu provides temperature and humidity data for the EMP. This menu allows to discover the plugged EMP's. On the Meter menu, scroll up or down to highlight Environment. Press ENTER to display the Environment submenu. Press ENTER to discover new EMP.



Scroll up or down and press ENTER to review the data for your selection. After you review the data, press ESC to return to the previous menu. (Contact closures are not displayed on the LCD.)

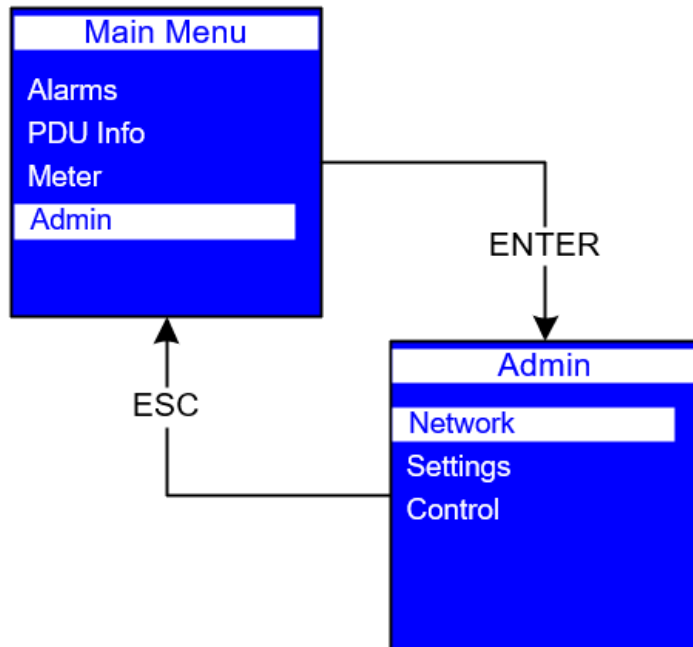


## 3.6 Admin

The Admin menu provides access to:



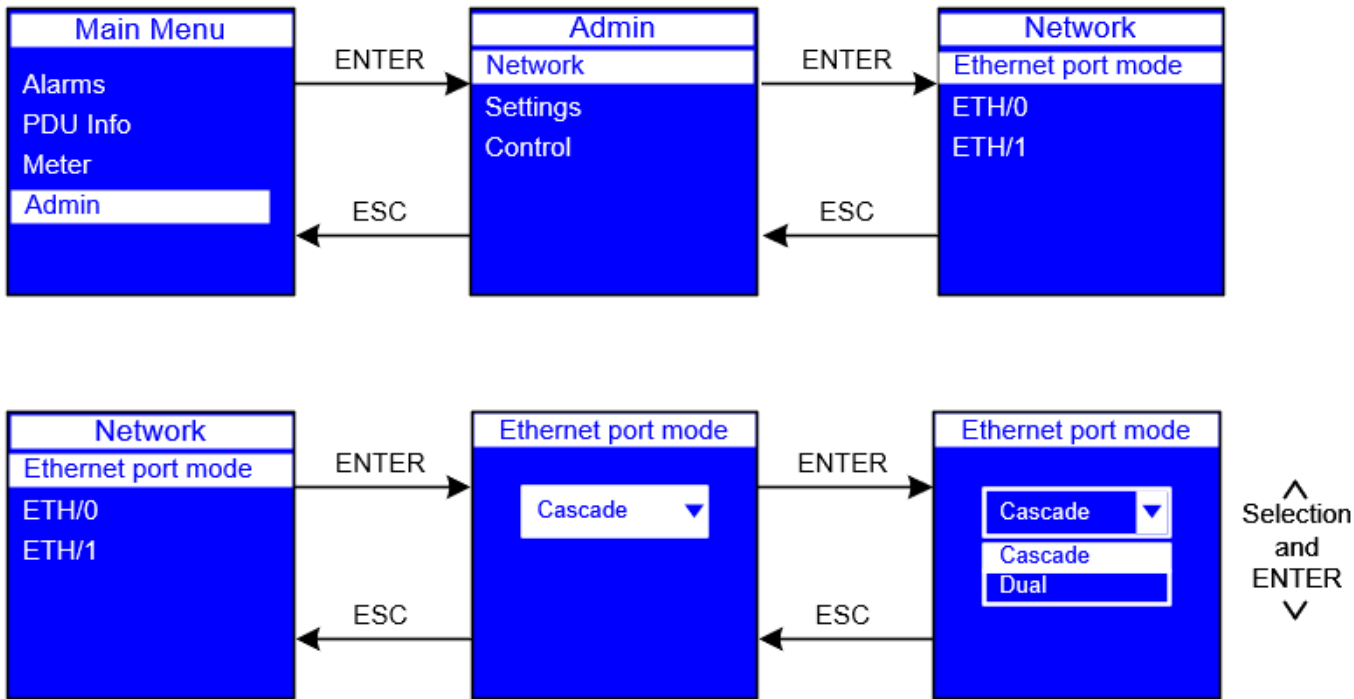
Network, Control and the Settings menus can be password-protected (refer to [Password protected menu](#)).



### 3.6.1 Network

#### 3.6.1.1 Ethernet mode

On the Network menu, scroll up or down to highlight Ethernet port mode. Press ENTER. Press ENTER to display the options in the drop list. Scroll up or down to highlight the desired option from the menu. Press ENTER validate the choice. Press ESC to return to the previous menu.



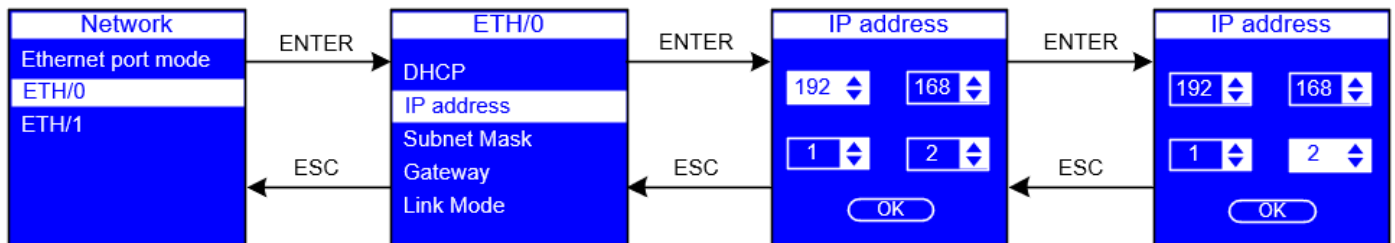
WARNING 1 Moving from Dual to Cascade will bridge the two networks into one network and reboot the card.  
WARNING 2 Moving from Cascade to Dual will separate the ports into two networks and reboot the card.

### 3.6.1.2 ETH/X

The ETH0 or ETH1 submenus allows you to set options for:

- DHCP
- IP address
- Subnet Mask
- Gateway
- Link Mode

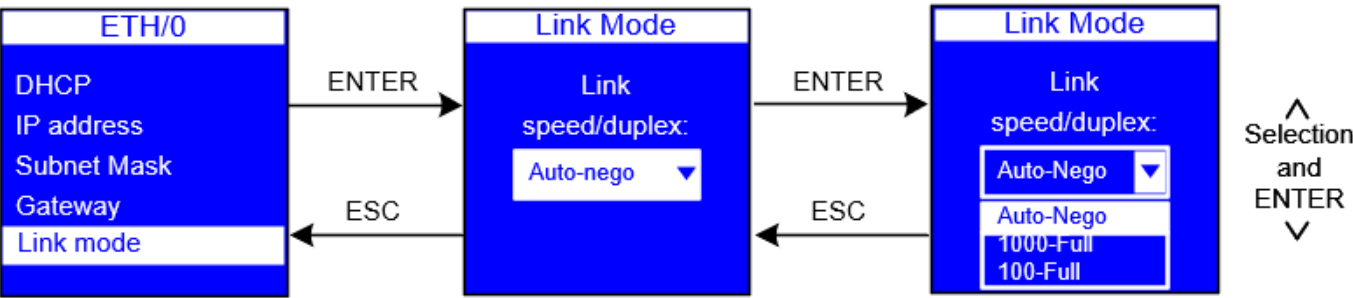
On the Network menu, scroll up or down to highlight ETH/X. Press ENTER to display the options screen. Scroll up or down to highlight the selected option from the menu. Press ENTER to display the screens to set the values for the selected option. After you select the values, press ENTER to set the values as displayed on the screen. Press ESC to return to the previous menu.



On the ETH/X menu, scroll down to highlight Link Mode. Press ENTER. Press ENTER to display the options in the drop list. Scroll up or down to highlight the desired option from the menu. Press ENTER validate the choice. Press ESC to return to the previous menu.

There are 5 choices available:

- Auto-Nego
- 1000-Full
- 100-Full
- 100-Half
- 10-Full
- 10-Half



### 3.6.2 Settings

The Settings menu provides user configuration options. Only the available options display, depending on the assigned user privileges.

There are four standard Settings submenus and one optional submenu:

- Display
- Background
- Language
- Reset to default

On the Main Menu, scroll up or down to highlight Settings. Press ENTER. Scroll up or down to select a submenu and press ENTER to display the submenu options. Press ESC to return to the previous menu.



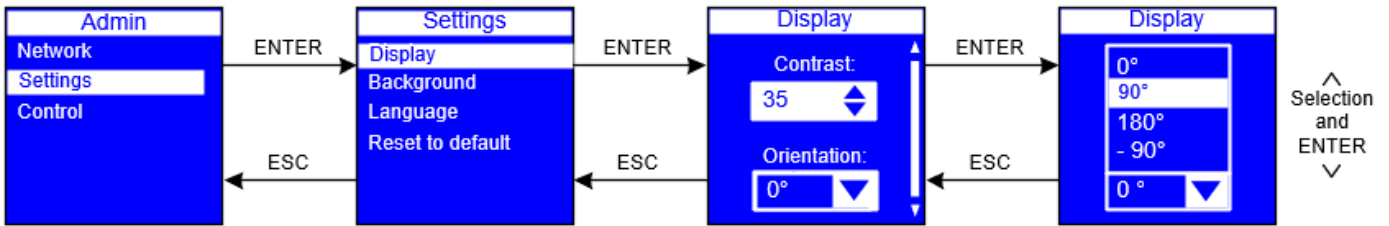
#### 3.6.2.1 Display

The Display submenu allows you to customize settings for LCD contrast and orientation.

On the Settings menu, scroll up or down to highlight Display. Press ENTER to display the screens to set the values for the submenu. After you select the values, press ENTER

to set the values as displayed on the screen. Press ESC to return to the previous menu.

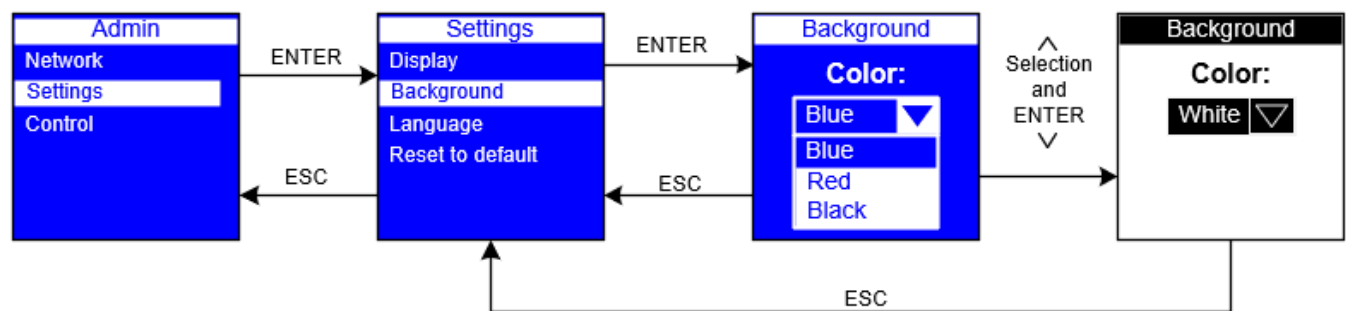




### 3.6.2.2 Background

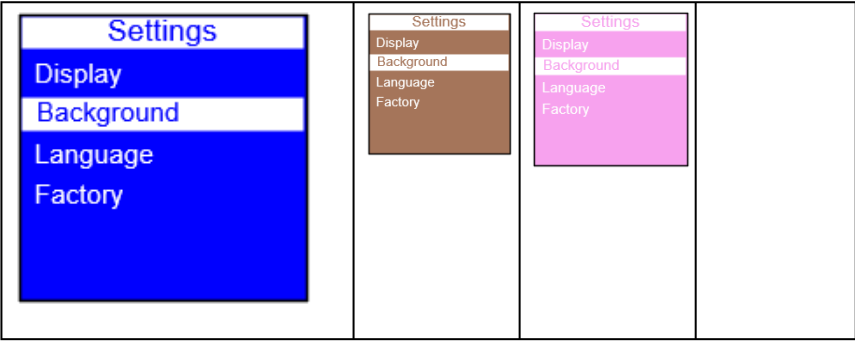
The Background submenu allows you to set the background color of PDU LCD screen.

On the Settings menu, scroll up or down to highlight Background. Press ENTER. Scroll up or down to highlight the selected background option from the menu. Press ENTER to set the selected background color. Press ESC to return to the previous menu.



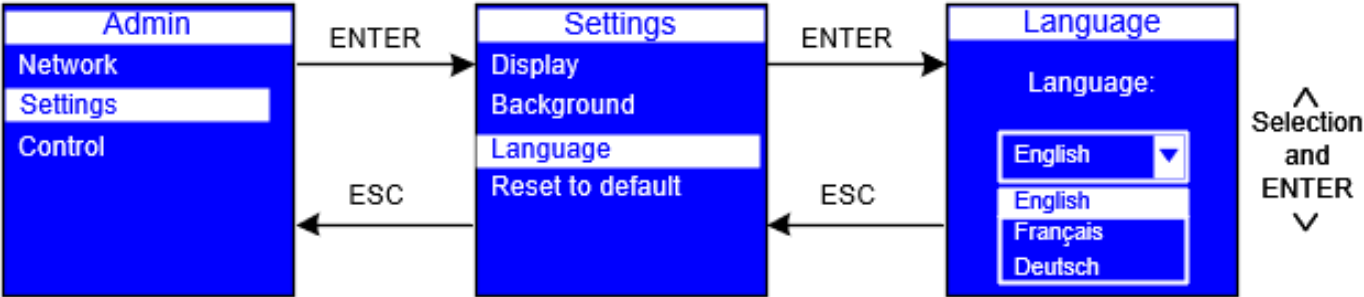
There are 11 background colors.

White	Red	Purple	Green
<div>Settings</div> <div>Display</div> <div>Background</div> <div>Language</div> <div>Factory</div>	<div>Settings</div> <div>Display</div> <div>Background</div> <div>Language</div> <div>Factory</div>	<div>Settings</div> <div>Display</div> <div>Background</div> <div>Language</div> <div>Factory</div>	<div>Settings</div> <div>Display</div> <div>Background</div> <div>Language</div> <div>Factory</div>
Black	Yellow	Orange	Gray
<div>Settings</div> <div>Display</div> <div>Background</div> <div>Language</div> <div>Factory</div>	<div>Settings</div> <div>Display</div> <div>Background</div> <div>Language</div> <div>Factory</div>	<div>Settings</div> <div>Display</div> <div>Background</div> <div>Language</div> <div>Factory</div>	<div>Settings</div> <div>Display</div> <div>Background</div> <div>Language</div> <div>Factory</div>
Blue	Brown	Pink	



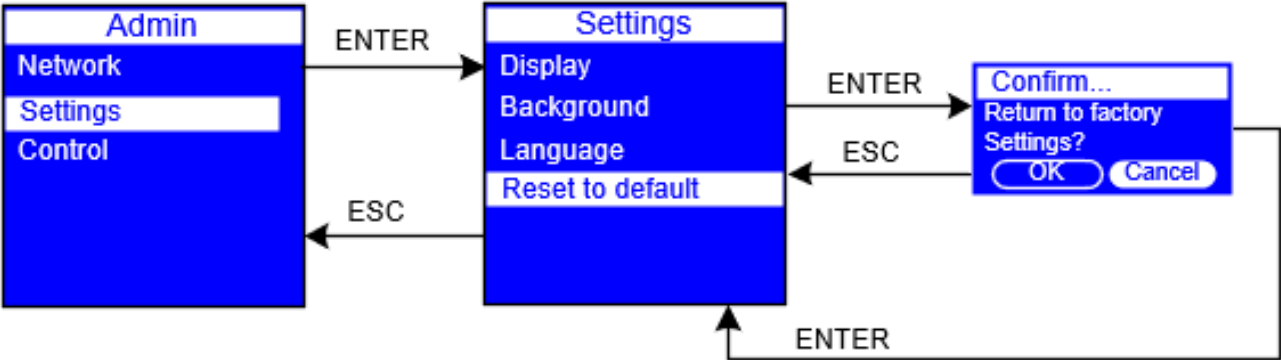
### 3.6.2.3 Language

On the Settings menu, scroll up or down to highlight Language. Press ENTER. Scroll up or down to highlight the selected language option from the menu. Press ENTER to set the selected language. Press ESC to return to the previous menu.



### 3.6.2.4 Reset to default

The Reset to default submenu allows you to reset the PDU to the factory settings. On the Settings menu, scroll down to highlight Reset to default. Press ENTER to display the screens to set and confirm the return to factory settings. After you make the selections, press ENTER to set the values as displayed on the screen. Press ESC to return to the previous menu.



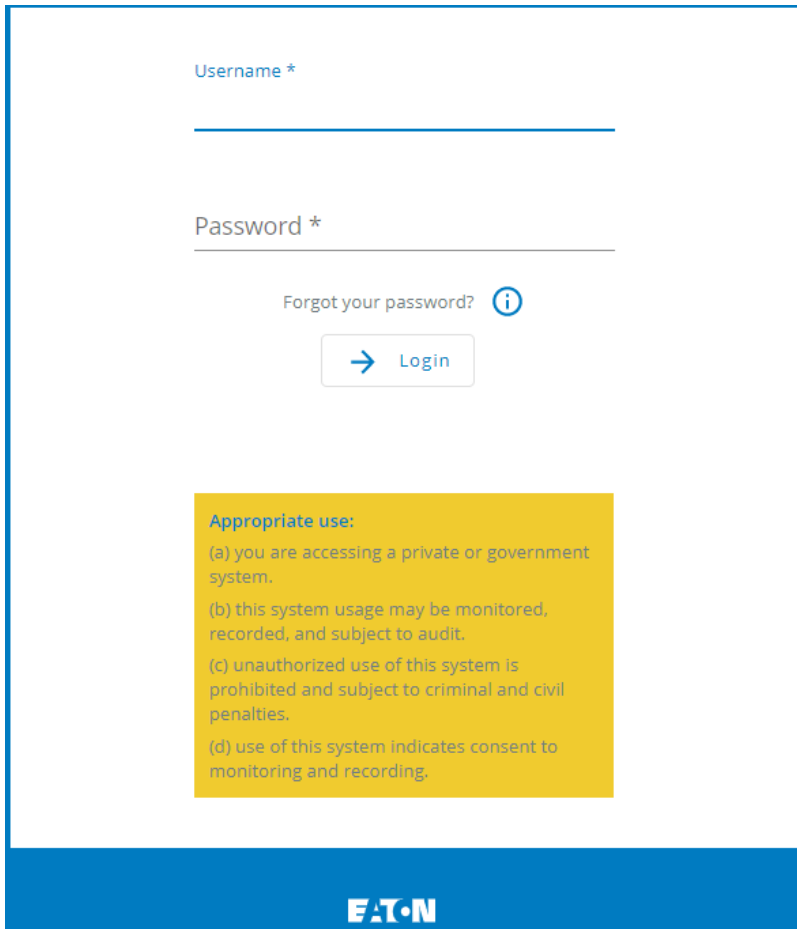
### 3.6.3 Control

For Switched (SW) and Managed (MA) PDUs only. On the Main Menu, scroll up or down to highlight Control. Press ENTER. Scroll up or down to see a list of outlet group IDs. Select an outlet group. The On/Off drop down list displays. Select On or Off. The selected state of the outlet displays. Scroll up or down to see other lists of outlet group IDs (if available). Press ESC to return to the previous menu.



## 4 Contextual help of the web interface

### 4.1 Login page



The screenshot shows a login page with a white background and a blue border. At the top, there is a label "Username \*" followed by a text input field. Below it is a label "Password \*" followed by a password input field. Under the password field, there is a link "Forgot your password?" with an information icon (i) to its right. Below the link is a button with a right arrow and the text "Login". At the bottom of the form area, there is a yellow box with the heading "Appropriate use:" and four bullet points: (a) you are accessing a private or government system, (b) this system usage may be monitored, recorded, and subject to audit, (c) unauthorized use of this system is prohibited and subject to criminal and civil penalties, and (d) use of this system indicates consent to monitoring and recording. At the very bottom of the page, there is a blue footer bar with the "E.T.N" logo in white.

The page language is set to English by default but can be switched to browser language when it is managed.

After navigating to the assigned IP address, accept the untrusted certificate on the browser.

#### 4.1.1 Logging in for the first time

##### 4.1.1.1 1. Enter default password

As you are logging into the Network Module for the first time you must enter the factory set default username and password.

- Username = admin
- Password = admin

##### 4.1.1.2 2. Change default password

Changing the default password is mandatory and requested in a dedicated window.

Enter your current password first, and then enter the new password twice.

Follow the password format recommendations on the tooltip in order to define a secure password.

### 4.1.1.3 3. Accept license agreement

On the next step, License Agreement is displayed.

Read and accept the agreement to continue.



#### Accounts with identical names

When an user attempt to log with a user name that exist both locally & remotely, then only the local account can successfully be logged in by default.

Two options for the remote user to successfully log in

1. You can use a prefix to access the remote account. For example ldap\johndoe or radius\johndoe depending on the remote configuration you set in the card.
2. Change the user name of the local account

### 4.1.1.4 4. Set LCD pin code

Once the license agreement has been accepted, you'll be asked to define a 4 digit pin code to lock the admin menu on LCD screen.

It's recommended to activate this security but it remains optional.

← LCD PIN

#### LCD Pin

☐ Inactive

☒ Activate LCD PIN to improve security

PIN



0/4

Confirm PIN



0/4

Save

## 4.1.2 Troubleshooting

### How do I log in if I forgot my password?

#### Action

- Ask your administrator for password initialization.
- If you are the main administrator, your password can be reset manually by following steps described in the [Servicing the Network Management Module>>>Recovering main administrator password](#) .

### Web user interface is not up to date after a FW upgrade

#### Symptom

After an upgrade:

- The Web interface is not up to date
- New features of the new FW are not displayed
- An infinite spinner is displayed on a tile

#### Possible causes

The browser is displaying the Web interface through the cache that contains previous FW data.

#### Action

Empty the cache of your browser using F5 or CTRL+F5.

### 4.1.2.1 For other issues









For details on other issues, see the [Troubleshooting](#) section.

## 4.2 Home









The Home screen provides status information for the device including key measures and active alarms.

### 4.2.1 Header structure

<b>Name</b>	Displays the Network module name.
<b>Device name</b>	Displays by default the Device model or the system name if filled in the section <a href="#">Contextual help&gt;&gt;&gt;Maintenance&gt;&gt;&gt;System information</a> .
	Shortcut to the Device details: <ul style="list-style-type: none"> <li>• Name</li> <li>• Location</li> <li>• Model</li> <li>• P/N</li> <li>• S/N</li> <li>• FW version</li> </ul>
<b>Part No</b>	Displays the Device Part Number.
<b>Serial No</b>	Displays the Device Serial Number.

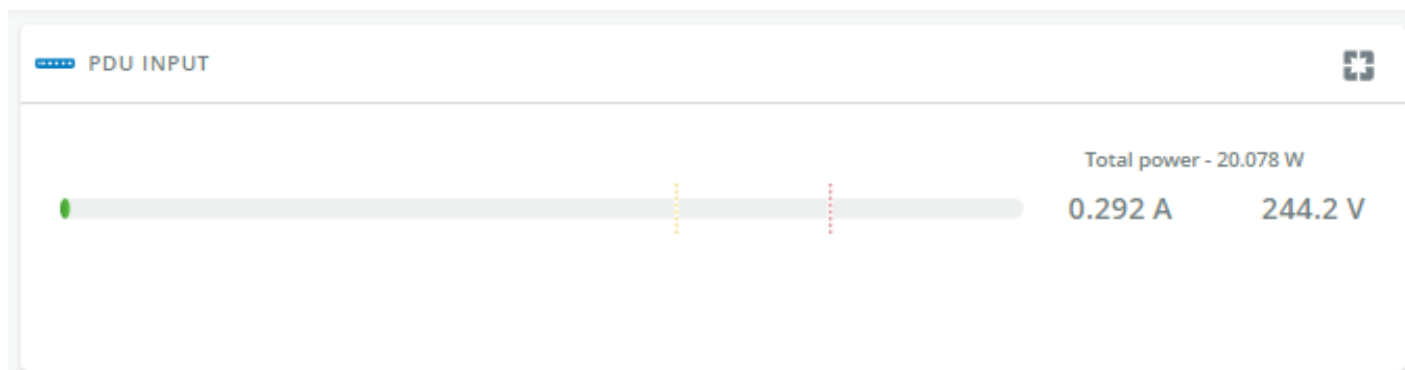
	Output load level
	<b>Help:</b> Opens full documentation in a separate browser page.
	<b>Profile:</b> Displays user profile, password change, account information, logout and legal information.
 	<b>Alarms:</b> Open alarm page and displays the number of active alarms.

## 4.2.2 Menu structure

	Extend menu display.
	<b>Home:</b> Overview and status of the Device (Active alarms, Outlet status, ...).
	<b>Meters:</b> Power quality meters and logs.
	<b>Controls:</b> Device and outlets control.
	<b>Environment:</b> Commissioning/Status, Alarm configuration, Information.
	<b>Settings:</b> Network Module settings.
	<b>PDU settings:</b> General settings, thresholds, group definition.
	<b>Maintenance:</b> Firmware, Services, Resources, System logs.

## 4.2.3 PDU input

Provides input measures (Current, Voltage, Total power).



Note: To access the Meters menu, press the icon:



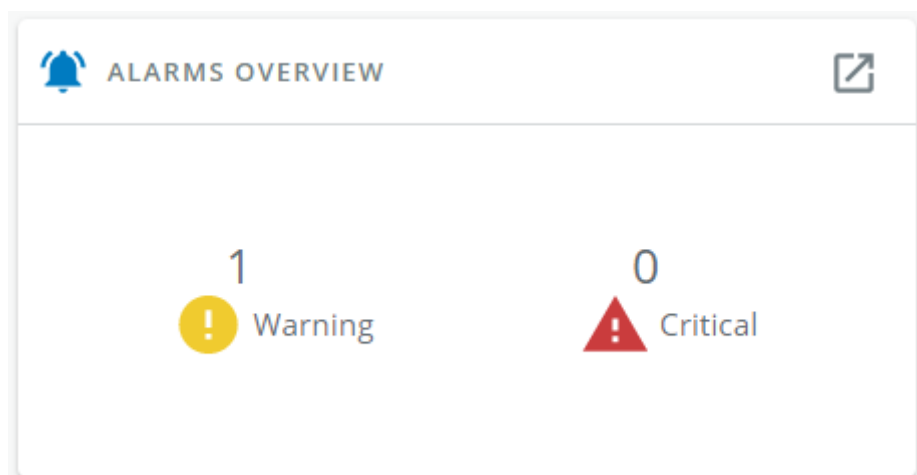
## 4.2.4 Environment

Sensor status and data are displayed if available, MIN-MAX shows the minimal and maximal temperature or humidity measured by the sensor.

**Note:** To see detailed sensor data, press the icon:



## 4.2.5 Alarms



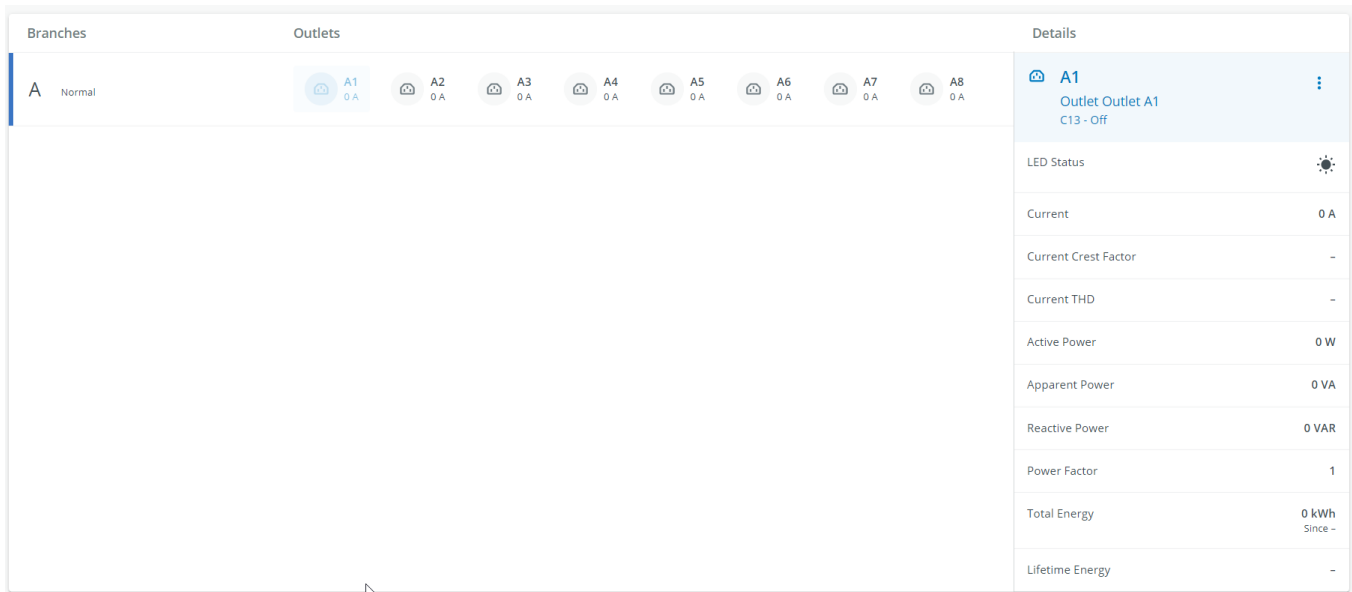
Display of the number of active Critical and Warning alarms.

Note: To see the alarm history, press the icon:





## 4.2.6 Branches, outlet status and details



### 4.2.6.1 Branches

Provides the name, color and status of the branch.

When selected, it provides the detailed status of the selected PDU branch:

- Identification
- Type
- Current
- Current crest factor
- Current THD
- Voltage
- Voltage THD
- Active power
- Apparent power
- Reactive power
- Power factor
- Total energy (since)
- Lifetime energy



**Note:** To access branch Settings menu, press the icon:

### 4.2.6.2 Outlets

Provides the name, type, color and status of the outlets.

Provides the detailed status of the selected PDU outlet:

- Identification and status
- LED status
- Current
- Current crest factor
- Current THD
- Voltage
- Voltage THD
- Active power
- Apparent power
- Reactive power
- Power factor

Meters

- Total energy (since)
- Lifetime energy



**Note:** To access outlet Settings/Control/Identify menu, press the icon:

4.2.7 Access rights per profiles

	Administrator	Operator	Viewer
Home			

4.2.7.1 For other access rights

For other access rights, see the [Information>>>Access rights per profiles](#) section.

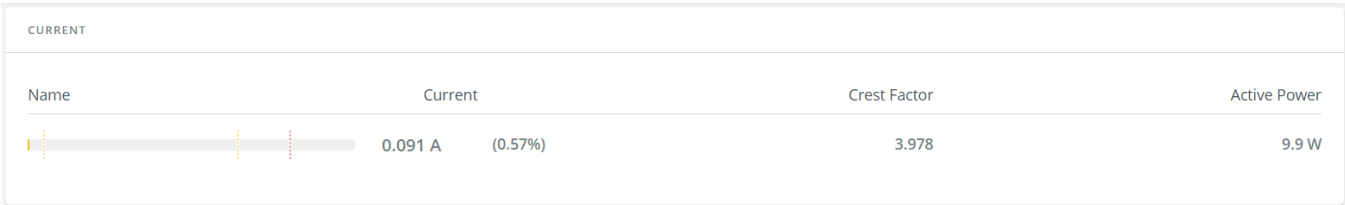
4.3 Meters

4.3.1 Input

Gauge color code:

- Green: Value inside thresholds.
- Orange/Red: Value outside thresholds.
- Blue: No thresholds provided by the device.

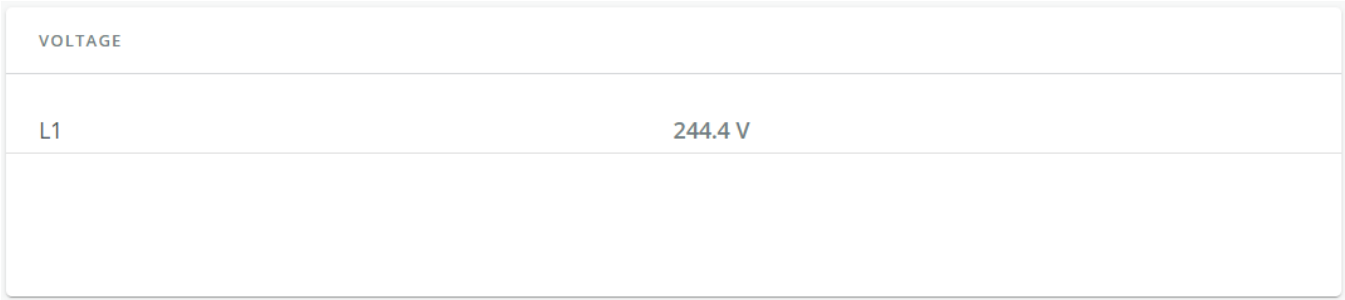
4.3.1.1 Current



Displays the product input current measures.

- Current (A) and (%)
- Crest factor
- THD

4.3.1.2 Voltage



Displays the product input voltage measures per phases.

- L1 voltage (V) and (THD)
- L2 voltage (V) and (THD)
- L3 voltage (V) and (THD)

### 4.3.1.3 Total input

TOTAL INPUT	
Frequency	50 Hz
Active Power	9.7 W
Apparent Power	23.5 VA
Reactive Power	-21.3 VAR
Power Factor	0.41167
Total Energy	-
Since	-
Leakage Current	-

Displays the product total input measures.

- Frequency (Hz)
- Active power (W)
- Apparent power (VA)
- Reactive power (VAR)
- Power factor
- Total energy (W/h)
- Since

### 4.3.1.4 Access rights per profiles

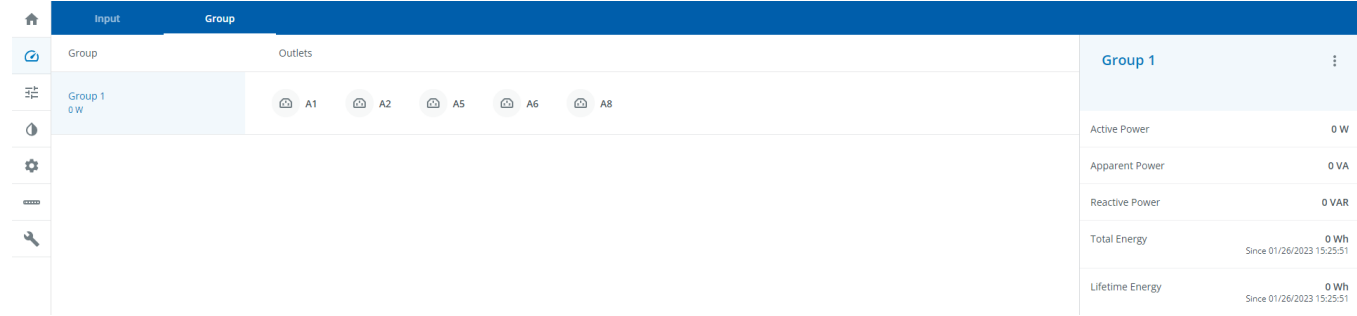
	Administrator	Operator	Viewer
Meters input	✓	✓	✓

#### 4.3.1.4.1 For other access rights



For other access rights, see the [Information>>>Access rights per profiles](#) section.

# 4.3.2 Group



Displays measures for the created groups.

- Current (A)
- Active power (W)
- Apparent power (VA)
- Reactive power (VAR)
- Total energy (W/h)
- Lifetime energy (W/h)

## 4.3.2.1 Access rights per profiles

	Administrator	Operator	Viewer
Meters group	✓	✓	✓

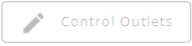
### 4.3.2.1.1 For other access rights









 For other access rights, see the [Information>>>Access rights per profiles](#) section.

## 4.4 Controls

### 4.4.1 Outlets

#### 4.4.1.1 Outlets status table

Control Outlets

<input type="checkbox"/>	ID	Name	Current (A)	State
A <input type="checkbox"/>	 A1	Outlet A1	0	Off
A <input type="checkbox"/>	 A2	Outlet A2	0	On
A <input type="checkbox"/>	 A3	Outlet A3	0	On
A <input type="checkbox"/>	 A4	Outlet A4	0	On
A <input type="checkbox"/>	 A5	Outlet A5	0	On
A <input type="checkbox"/>	 A6	Outlet A6	0	On
A <input type="checkbox"/>	 A7	Outlet A7	0	On
A <input type="checkbox"/>	 A8	Outlet A8	0	On

The table displays the outlets information and includes the following details.

- **Outlet icon**
- **ID** – Outlet identification number
- **Name**
- **Current (A)**
- **State** – On or Off

#### 4.4.1.2 Control outlets

Select outlets and press the **Control outlets** button to display the control panel.

Control Outlets



Command Type

- ☐ Turn On
- ☐ Turn Off
- ☐ Reboot

Delay Before Command

Seconds \*

Selected Outlets

3

A1 - Outlet A1



A2 - Outlet A2



A3 - Outlet A3



EXIT

EXECUTE

#### 4.4.1.2.1 Commands

A set of commands are available and activated when the **Execute** button is pressed.

The outlet selection is listed with the capability to remove outlets from the selection if needed.

- **Turn On**

This will switch ON the outlet selection.

- **Turn Off**

This will switch OFF the outlet selection.

- **Reboot**

This will shut off and then switch ON the outlet selection.

- **Delay before command**

This will add a delay set in seconds before the execution of the command.

#### 4.4.1.3 Access rights per profiles

	Administrator	Operator	Viewer
Controls - Outlets	✓	✓	✗

##### 4.4.1.3.1 For other access rights



For other access rights, see the [Information>>>Access rights per profiles](#) section.

#### 4.4.2 Group

Control	
Group	Outlets
<input type="checkbox"/> Group 1	<div>A1 0 mA</div> <div>A2 0 mA</div> <div>A3 0 mA</div> <div>A7 0 mA</div> <div>A8 0 mA</div>
<input type="checkbox"/> Group 2	<div>A4 0 mA</div> <div>A5 0 mA</div> <div>A6 0 mA</div>
<input type="checkbox"/> Group 3	<div>A1 0 mA</div> <div>A3 0 mA</div> <div>A5 0 mA</div> <div>A7 0 mA</div>

The table displays the outlets information and includes the following details.

- **Group name**
- **Outlets** - Outlets included in the group and the current for each outlet

##### 4.4.2.1 Control groups

Select groups and the **Control** button to display the control panel.

# Control Groups



Command Type

- ☐ Turn On
- ☐ Turn Off
- ☐ Reboot

Delay Before Command

Seconds \*

0

## Selected Groups

1

Group 1





#### 4.4.2.1.1 Commands

A set of commands are available and activated when the **Execute** button is pressed.

The group selection is listed with the capability to remove groups from the selection if needed.

- **Turn On**

This will switch ON the outlets included in the group selection.

- **Turn Off**

This will switch OFF the outlets included in the group selection.

- **Reboot**

This will shut off and then switch ON the outlets included in the group selection.

- **Delay before command**

This will add a delay set in seconds before the execution of the command.

#### 4.4.2.2 Access rights per profiles

	Administrator	Operator	Viewer
Controls - Group	✓	✓	✗

##### 4.4.2.2.1 For other access rights



For other access rights, see the [Information>>>Access rights per profiles](#) section.

## 4.5 Environment

### 4.5.1 Commissioning/Status

#### 4.5.1.1 Sensors commissioning/Status table

The table displays the sensors commissioning information and includes the following details.

- **Name**
- **Location** – location-position-elevation
- **Temperature**
- **Humidity**
- **Dry contact #1** – Status and name
- **Dry contact #2** – Status and name
- **Communication** – Connected/Lost with dates

#### 4.5.1.2 Actions

##### 4.5.1.2.1 Download sensors measures

Press the **Download sensors measures** button to download the sensors log file: 

If available, possible measures are listed below:

- Temperature of <sensor\_1> (in K, 1 decimal digit)
- Humidity of <sensor\_1> (in %, 1 decimal digit)
- Temperature of <sensor\_2>> (in K, 1 decimal digit)

- Humidity of <sensor\_2> (in %, 1 decimal digit)
- Temperature of <sensor\_3> (in K, 1 decimal digit)
- Humidity of <sensor\_3> (in %RH, 1 decimal digit)



°C = K - 273.15  
°F = K x 9/5 -459.67

4.5.1.2.2 Discover

At first the table is empty, press the **Discover** button to launch the sensor discovery process.  
If sensors are discovered, the table is populated accordingly

4.5.1.2.3 Delete

Select a sensor and press the **Delete** button to delete the sensor.



When a sensor is deleted, all the commissioning information are deleted.

4.5.1.2.4 Define offsets

Define offsets

Temperature

EMPDT1H1C2 @1 \*

0

28.9°C → 28.9°C

Humidity

EMPDT1H1C2 @1 \*

0

20.8% → 20.8 %

Save

1. Select the sensors.
2. Press the **Define offset** button to adjust the temperature and humidity offsets of the selected sensors.
3. Extend the temperature or humidity section.
4. Set the offsets in the cell, temperatures and humidity will be updated accordingly.
5. Press the **Save** button when done.



Deactivated humidity or temperatures are not displayed and replaced by this icon:



4.5.1.2.5 Edit

Sensor commissioning

Product

Eaton EMPDT1H1C2

Part number

EMPDT1H1C2

Serial number

GB13J28239

Name \*

EMPDT1H1C2 @1

Location

Rack#1 Server room #2

Temperature

Name \*

EMPDT1H1C2 @1-T1

Humidity

Name \*

EMPDT1H1C2 @1-H1

Dry contact #1

Name \*

EMPDT1H1C2 @1-C1

Polarity \*

Normally open

Dry contact #2


Name \*

EMPDT1H1C2 @1-C2

Polarity \*





Normally open

Save

Press the pen logo to edit sensor communication information: 

You will get access to the following information and settings:

- Product reference
- Part number
- Serial number
- Name
- Location
- Temperature and humidity – Active (Yes, No)
- Dry contacts – Active (Yes, No)/Name/Polarity (Normally open, Normally closed)

	The dry contact is close and this is normal because it is configured as normally close.
	The dry contact is open and this is normal because it is configured as normally open.
	The dry contact is open and this is not normal because it is configured as normally close.
	The dry contact is close and this is not normal because it is configured as normally open.

Contextual help of the web interface – 55

Press **Save** after modifications.



Deactivated dry contacts are not displayed and replaced by this icon:



### 4.5.1.3 Access rights per profiles

	Administrator	Operator	Viewer
Environment/Commissioning	✓	✓	✗
Environment/Status	✓	✓	✓

#### 4.5.1.3.1 For other access rights



For other access rights, see the [Information>>>Access rights per profiles](#) section.

### 4.5.1.4 Troubleshooting

#### EMP communication status shows "Lost"

In the Network Module, in [Contextual help>>>Environment>>>Commissioning/Status](#) , EMPs are missing in the Sensor commissioning table.

##### Symptom #1

The connection status of the sensor is "Lost"

##### Possible causes

The EMPs are not powered by the Network module.

##### Action #1-1

Launch again the discovery, if it is still not ok, go to Action #1-2.

##### Action #1-2

1- Check the EMPs connection and cables.

Refer to the sections [Servicing the EMP>>>Installing the EMP>>>Cabling the first EMP to the device](#) and [Servicing the EMP>>>Installing the EMP>>>Daisy chaining 3 EMPs](#) .

2- Disconnect and reconnect the USB to RS485 cable.

3- Launch the discovery, if it is still not ok, go to Action #1-3.

##### Action #1-3

1- Reboot the Network module.

2- Launch the discovery.

## EMP detection fails at discovery stage

In the Network Module, in [Contextual help>>>Environment>>>Commissioning/Status](#) , EMPs are missing in the Sensor commissioning table.

### Symptom #1

The EMPs green RJ45 LED (FROM DEVICE) is not ON.

### Possible causes

The EMPs are not powered by the Network module.

### Action #1-1

Launch again the discovery, if it is still not ok, go to Action #1-2.

### Action #1-2

1- Check the EMPs connection and cables.

Refer to the sections [Servicing the EMP>>>Installing the EMP>>>Cabling the first EMP to the device](#) and [Servicing the EMP>>>Installing the EMP>>>Daisy chaining 3 EMPs](#) .

2- Disconnect and reconnect the USB to RS485 cable.

3- Launch the discovery, if it is still not ok, go to Action #1-3.

### Action #1-3

1- Reboot the Network module.

2- Launch the discovery.

### Symptom #2

The EMPs orange RJ45 LEDs are not blinking.

### Possible causes

C#1: the EMP address switches are all set to 0.

C#2: the EMPs are daisy chained, the Modbus address is the same on the missing EMPs.

### Action #2-1

1- Change the address of the EMPs to have different address and avoid all switches to 0.

Refer to the section [Servicing the EMP>>>Defining EMPs address and termination>>>Manual addressing](#) .

2- Disconnect and reconnect the USB to RS485 cable. The address change is only taken into account after an EMP power-up.

3- Launch the discovery, if it is still not ok, go to Action #2-2.


### Action #2-2

1- Reboot the Network module.

Refer to the section [Contextual help>>>Maintenance>>>Services>>>Reboot](#) .


2- Launch the discovery.

4.5.1.4.1 For other issues



For details on other issues, see the [Troubleshooting](#) section.

4.5.2 Alarm configuration



Humidity, temperatures or dry contacts deactivated during commissioning are not displayed.

Gauge color code:

- Green: Value inside thresholds.
- Orange/Red: Value outside thresholds.
- Grey: No thresholds provided by the device.

4.5.2.1 Temperature

TEMPERATURE

Name	Location	Enabled	Low critical	Low warning	High warning	High critical	Hysteresis	Visual update	Live reading
EMPD1H1C2 @1-T1	Rack#1 Server room #2	<input type="checkbox"/>	0	10	70	80	1	<div><div></div></div>	28.9°C

Save

The table shows the following information and settings for each sensor:

- Name
- Location
- Enabled – yes/no
- Low critical threshold – xx°C or xx°F
- Low warning threshold – xx°C or xx°F
- High warning threshold – xx°C or xx°F
- High critical threshold – xx°C or xx°F
- Hysteresis – x°C or x°F
- Visual update
- Live reading (MIN-MAX shows the minimal and maximal temperature measured by the sensor)

4.5.2.1.1 Actions

a Set Enabled

Select and directly change the setting in the table and then **Save**.

When disabled, no alarm will be sent.

b Set alarm threshold

Enable the alarm first and then change the setting in the table and then **Save**.

When a warning threshold is reached, an alarm will be sent with a warning level.

When a critical threshold is reached, an alarm will be sent with a critical level.

c Set Hysteresis

Enable the alarm first and change the setting in the table and then **Save**.

The hysteresis is the difference between the value where the alarm turns ON from turning OFF and the value where it turns OFF from turning ON.

## 4.5.2.2 Humidity

Name	Location	Enabled	Low critical	Low warning	High warning	High critical	Hysteresis	Visual update	Live reading
EM PDT1H1C2 @1-H1	Rack#1 Server room #2	<input type="checkbox"/>	10	20	80	90	1		20.8%

Save

The table shows the following information and settings for each sensor:

- Name
- Location
- Enabled – yes/no
- Low critical threshold – xx%
- Low warning threshold – xx%
- High warning threshold – xx%
- High critical threshold – xx%
- Hysteresis – x%
- Visual update
- Live reading (MIN-MAX shows the minimal and maximal humidity measured by the sensor)

### 4.5.2.2.1 Actions

#### a Set Enabled

Select and directly change the setting in the table and then **Save**.

When disabled, no alarm will be sent.

#### b Set alarm threshold

Enable the alarm first and then change the setting in the table and then **Save**.

When a warning threshold is reached, an alarm will be sent with a warning level.


When a critical threshold is reached, an alarm will be sent with a critical level.

#### c Set Hysteresis

Enable the alarm first and then change the setting in the table and then **Save**.

The hysteresis is the difference between the value where the alarm turns ON from turning OFF and the value where it turns OFF from turning ON.

4.5.2.3 Dry contacts

 DRY CONTACTS

Name	Location	Enabled	Alarm severity
EMPDT1H1C2 @1-C1	Rack#1 Server room #2	<input type="checkbox"/>	<div><div>Info</div><div>Warning</div><div>Critical</div></div>
EMPDT1H1C2 @1-C2	Rack#1 Server room #2	<input type="checkbox"/>	<div><div>Info</div><div>Warning</div><div>Critical</div></div>

Save

The table shows the following settings for each dry contact:

- Name
- Location
- Enabled – yes/no
- Alarm severity – Info/Warning/Critical

4.5.2.3.1 Actions

a Set Enabled



Enable the alarm first and then change the setting in the table and then **Save**.

When disabled, no alarm will be sent.

b Set alarm severity

Enable the alarm first and then change the setting in the table and then **Save**.

When the dry contacts is not in a normal position, an alarm will be sent at the selected level.

	The dry contact is open and this is not normal because it is configured as normally close.
	The dry contact is close and this is not normal because it is configured as normally open.

4.5.2.4 Default settings and possible parameters - Environment Alarm configuration

	Default setting	Possible parameters
Temperature	Enabled — No Low critical – 0°C/32°F Low warning – 10°C/50°F High warning – 70°C/158°F High critical – 80°C/176°F	Enabled — No/Yes low critical<low warning<high warning<high critical



<b>Humidity</b>	Enabled — No Low critical – 10% Low warning – 20% High warning – 80% High critical – 90%	Enabled — No/Yes 0%<low critical<low warning<high warning<high critical<100%
<b>Dry contacts</b>	Enabled — No Alarm severity – Warning	Enabled — No/Yes Alarm severity – Info/Warning/Critical

#### 4.5.2.4.1 For other settings



For other settings, see the [Information>>>Default settings parameters](#) section.

#### 4.5.2.5 Access rights per profiles

	Administrator	Operator	Viewer
Environment/Alarm configuration	✓	✓	✗

#### 4.5.2.5.1 For other access rights



For other access rights, see the [Information>>>Access rights per profiles](#) section.

### 4.5.3 Information

Sensor information is an overview of all the sensors information connected to the Network Module.

EMPDT1H1C2 @1	
<b>Name</b>	Eaton EMPDT1H1C2
<b>Vendor</b>	Eaton
<b>UUID</b>	5c93d236-088d-5d77-bcd4-1afbd03af181
<b>Part number</b>	EMPDT1H1C2
<b>Serial number</b>	GB13J28239
<b>Version</b>	01.02.0009
<b>Location</b>	Rack#1 Server room #2

- Physical name
- Vendor
- Part number
- Firmware version
- UUID
- Serial number
- Location

#### 4.5.3.1 Access rights per profiles

	Administrator	Operator	Viewer
Environment/Information	✓	✓	✓

##### 4.5.3.1.1 For other access rights




For other access rights, see the [Information>>>Access rights per profiles](#) section.

## 4.6 Settings

### 4.6.1 General

#### 4.6.1.1 System details

 **SYSTEM DETAILS**

Location

myLocation

Contact

myName@myComany.com

System name

mySystemName

Save

##### 4.6.1.1.1 Location

Text field that is used to provide the card location information.

Card system information is updated to show the defined location.

##### 4.6.1.1.2 Contact

Text field that is used to provide the contact name information.


Card system information is updated to show the contact name.



##### 4.6.1.1.3 System name

Text field that is used to provide the system name information.

Card system information is updated to show the system name.

## 4.6.1.2 Date & Time

 DATE & TIME


Current date & time	12/07/2021 09:43:15
Time zone	Europe/Paris
Mode	Dynamic (NTP)
Status	 In service
NTP server 1	121.110.120.12  InUse



Edit

The current date and time appears at the top of the screen.

You can set the time either manually or automatically.

### 4.6.1.2.1 Manual mode: Manually entering the date and time

Date and time settings 

Time zone	Europe/Paris
Mode	Manual
Current date & time *	12/07/2021 09:43:15  

Save

1. Select the time zone for your geographic area.
2. Select the date and time.
3. Save the changes.

#### 4.6.1.2.2 Dynamic (NTP): Synchronizing the date and time with an NTP server

Date and time settings

Time zone

Europe/Paris

Mode

Dynamic (NTP)

☐

Get NTP server from DHCP

NTP Serveur 1

NTP Serveur 2

Save

1. Select the time zone for your geographic area.
2. Enter the IP address or host name of the NTP servers in the NTP server fields (up to 5 servers).
3. Save the changes.

#### 4.6.1.2.3 Dynamic (NTP): Synchronizing the date and time from the DHCP server

Date and time settings

Time zone

Europe/Paris

Mode

Dynamic (NTP)

☒

Get NTP server from DHCP

Save

1. Select the time zone for your geographic area.
2. Select Get NTP server from DHCP
3. Save the changes.



DST is managed based on the time zone.

### 4.6.1.3 LCD Pin

Allows to activate/disactivate the LCD pin code and edit the code.

#### LCD Pin

☒ Active

Password

\*\*\*\*

Only numbers allowed

4/4

Confirm Password

Passwords must match





0/4

SAVE

### 4.6.1.4 Email notification settings



For examples on email sending configuration see the [Servicing the Network Management Module>>>Subscribing to a set of alarms for email notification](#) section.

EMAIL NOTIFICATION SETTINGS				
<div> <div>New</div> <div>Delete</div> </div>				
	Custom name ↑	Email	Notification updates	Status
<input type="checkbox"/>	 Configuration #1	myName@myCompany.com	<div> <div>Scheduled</div> <div>Alarms</div> </div>	 Active
<input type="checkbox"/>	 Configuration#2	myName@myCompany.com	<div> <div>Alarms</div> </div>	 Active

#### 4.6.1.4.1 Email sending configuration table

The table shows all the email sending configuration and includes the following details:

- **Configuration name**
- **Email address**
- **Notification updates** – Displays Events notification/Periodic report icons when active.
- **Status** – Active/Inactive/In delegation

#### 4.6.1.4.2 Actions

##### a Add

Press the **New** button to create a new email sending configuration.

##### b Remove

Select an email sending configuration and press the **Delete** button to remove it.

c Edit

Custom name \*

Configuration #1

Email address \*

myName@myCompany.com

Status

Active

☒ Hide the IP address from the email body

Schedule report

☐

Recurrence \*

Every day

Starting date \*

07/15/2020 13:53:00

Subscribe	Attach measures	Attach logs	
<input type="checkbox"/>		<input type="checkbox"/>	Card events
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Device events

Alarm notifications

☒

All card events

All device events

[List of event codes](#)

Always notify events with code

Separate each code with a comma

Never notify events with code

Separate each code with a comma

Test

Save

Press the pen icon to edit email sending configuration: 

You will get access to the following settings:

- Custom name
- Email address
- Status – Active/Inactive
- Hide the IP address from the email body – Disabled/Enabled  
This setting will be forced to Enabled if Enabled in the SMTP settings.
- Schedule report – Active/Recurrence/Starting/Topic selection – Card/Devices




Attachment will contains only logs that have occurred during the recurrence.

- **Alarm notifications** – Severity level/Attach logs/Exceptions on events notification



#### 4.6.1.5 SMTP settings

 SMTP SETTINGS

Server IP / Hostname \*

Port \*

25

Default sender address \*

☒ Hide the IP address from the email body

Security ▼

☐ Verify certificate authority

☐ SMTP server authentication

Username \*

Password

Test server

Save

SMTP is an internet standard for electronic email transmission.

The following SMTP settings are configurable:

- **Server IP/Hostname** – Enter the host name or IP address of the SMTP server used to transfer email messages in the SMTP Server field.
- **Port**
- **Default sender address**
- **Hide the IP address from the email body** – Disabled/Enabled  
If Enabled, it will force this setting to Enabled in the Email notification settings.
- **Secure SMTP connection** – Verify certificate authority
- **SMTP server authentication** – Username/Password ( Read below note for Gmail Configuration regarding the password )

Select the SMTP server authentication checkbox to require a user name and a password for SMTP authentication, enter the Username and the Password.



#### Gmail Users

Google no more allow the card to send email using your Gmail account password, but requires you to use a dedicated "App passwords" instead.

To proceed, you need first to enable a [2-Step Verification](#) on your Google account.

Then you need to follow these steps to generate an "App password" that you'll be required to configure SMTP server authentication in the card (instead of your google account usual password):

1. Go to <https://security.google.com/settings/security/apppasswords> and sign in to your account.
2. Choose **Mail** from the list of available apps.
3. Choose **Other** from the device list.
4. Enter your **Custom Name**. You can put any name such as "my-card" in it.
5. Click the **Generate** button.
6. Copy the password and put in the password field. ( The same password can be reused across multiple cards)  
Be careful, this password cannot be recovered after clicking the "Done" button. If lost, you'll have to regenerate a new password & reapply it in the settings.
7. Click the **Done** button, and that's it.

- Save and test server configuration

### 4.6.1.6 Default settings and possible parameters - General

	Default setting	Possible parameters
<b>System details</b>	Location — empty Contact — empty System name — empty Time & date settings — Manual (Time zone: Europe/Paris)	Location — 31 characters maximum Contact — 255 characters maximum System name — 255 characters maximum Time & date settings — Manual (Time zone: selection on map/Date) / Dynamic (NTP)

Email notification settings	No email	<p>5 configurations maximum</p> <p>Custom name — 128 characters maximum</p> <p>Email address — 128 characters maximum</p> <p>Hide IP address from the email body — enable/disabled</p> <p>Status — Active/Inactive</p> <ul style="list-style-type: none"> <li>Alarm notifications           <ul style="list-style-type: none"> <li>Active — No/Yes</li> <li>All card events – Subscribe/Attach logs</li> <li>Critical alarm – Subscribe/Attach logs</li> <li>Warning alarm – Subscribe/Attach logs</li> <li>Info alarm – Subscribe/Attach logs</li> </ul> </li> <li>All device events – Subscribe/Attach measures/Attach logs</li> <li>Critical alarm – Subscribe/Attach measures/Attach logs</li> <li>Warning alarm – Subscribe/Attach measures/Attach logs</li> <li>Info alarm – Subscribe/Attach measures/Attach logs</li> <li>Always notify events with code</li> <li>Never notify events with code</li> <li>Schedule report           <ul style="list-style-type: none"> <li>Active — No/Yes</li> <li>Recurrence – Every day/Every week/Every month</li> <li>Starting – Date and time</li> <li>Card events – Subscribe/Attach logs</li> <li>Device events – Subscribe/Attach measures/Attach logs</li> </ul> </li> </ul>
SMTP settings	<p>Server IP/Hostname — blank</p> <p>SMTP server authentication — disabled</p> <p>Port — 25</p> <p>Default sender address — <a href="#">device@networkcard.com</a></p> <p>Hide IP address from the email body — disabled</p> <p>Security — enabled</p> <p>Verify certificate authority — disabled</p> <p>SMTP server authentication — disabled</p>	<p>Server IP/Hostname — 128 characters maximum</p> <p>SMTP server authentication — disable/enable (Username/Password — 128 characters maximum)</p> <p>Port — x-xxx</p> <p>Sender address — 128 characters maximum</p> <p>Hide IP address from the email body — enable/disabled</p> <p>Secure SMTP connection — enable/disable</p> <p>Verify certificate authority — disable/enable</p>

#### 4.6.1.6.1 For other settings



For other settings, see the [Information>>>Default settings parameters](#) section.

#### 4.6.1.7 Access rights per profiles

	Administrator	Operator	Viewer
General	✓	✗	✗

#### 4.6.1.7.1 For other access rights



For other access rights, see the [Information>>>Access rights per profiles](#) section.

#### 4.6.1.8 CLI commands

##### email-test

###### Description

mail-test sends test email to troubleshoot SMTP issues.

###### Help

```
Usage: email-test <command> ...
Test SMTP configuration.

Commands:
email-test -h, --help, Display help page

email-test -r, --recipient <recipient_address>
Send test email to the
    <recipient_address>      Email address of the recipient
```

##### time

###### Description

Command used to display or change time and date.

###### Help

For Viewer and Operator profiles:

```
time -h
Usage: time [OPTION]...
Display time and date.

-h, --help      display help page
-p, --print     display date and time in YYYYMMDDhhmmss format
```

For Administrator profile:

```
time -h
Usage: time [OPTION]...
Display time and date, change time and date.
-h, --help          display help page
-p, --print          display date and time in YYYYMMDDhhmmss format
-s, --set <mode>
    Mode values:
    - set date and time (format YYYYMMDDhhmmss)
      manual <date and time>
    - set preferred and alternate NTP servers
      ntpmanual <preferred server> <alternate server>
    - automatically set date and time
      ntpauto
Examples of usage:
-> Set date 2017-11-08 and time 22:00
    time --set manual 201711082200
-> Set preferred and alternate NTP servers
    time --set ntpmanual fr.pool.ntp.org de.pool.ntp.org
```

#### Examples of usage

```
-> Set date 2017-11-08 and time 22:00
    time --set manual 201711082200
-> Set preferred and alternate NTP servers
    time --set ntpmanual fr.pool.ntp.org de.pool.ntp.org
```

#### 4.6.1.8.1 For other CLI commands



See the CLI commands in the [Information>>>CLI](#) section.

#### 4.6.1.9 Save and Restore

	SRR section	SRR sub section	Settings	Sub Settings	Possible values
System details	card	identification	name		String: refer to default settings and possible parameters for constraints.
			contact		String: refer to default settings and possible parameters for constraints.
			location		String: refer to default settings and possible parameters for constraints.
Time and Date settings	date	ntp	enabled		true/false
			getServersFromDhcp		true/false
			servers	preferredServer	*

				alternateServer	*
			timeZone		Examples: Europe/Paris Africa/Johannesburg America/New_York Asia/Shanghai
Email	email	notifyOnEvents	enabled		true/false
			cardEvents	<b>critical</b> subscribe attachEventsLog	true/false true/false
				<b>warning</b> subscribe attachEventsLog	true/false true/false
				<b>info</b> subscribe attachEventsLog	true/false true/false
			devicesEvents	<b>critical</b> subscribe attachEventsLog attachMeasuresLog	true/false true/false true/false
				<b>warning</b> subscribe attachEventsLog attachMeasuresLog	true/false true/false true/false
				<b>info</b> subscribe attachEventsLog attachMeasuresLog	true/false true/false true/false
		periodicReport	exceptions	notifiedEvents	evenst codes separated by coma
				noneNotifiedEvents	evenst codes separated by coma
			enabled periodicity startTime		true/false Every day/week/month Unix timestamp
			card	subscribe attachEventsLog	true/false true/false
			devices	subscribe attachEventsLog attachMeasuresLog	true/false true/false true/false

SMTP	smtp	<b>message</b>	sender		String: refer to default settings and possible parameters for constraints.
			subject		String: refer to default settings and possible parameters for constraints.
			hidelpAddress		true/false
		<b>certificateData</b>	ca		Certificate Authority of SMTP server
			port		Number: refer to default settings and possible parameters for constraints.
			enabled		true/false
			server		IP address or hostname of SMTP server
			requireAuth		true/false
			user		Username for server authentication
			<b>password</b>	plaintext cyphered	String: refer to default settings and possible parameters for constraints. -
			fromAddress		email address format
			ssl		1: None 2: STARTTLS 3: SSL
			verifyTlsCert		true/false


#### 4.6.1.9.1 Additional information



For details on Save and Restore, see the [Save and Restore](#) section.

## 4.6.2 Local users

### 4.6.2.1 Local users table

LOCAL USERS					
<div> <a href="#">Global Settings</a> <a href="#">+ New</a> <a href="#">Delete</a> </div>					
		Username ↑	Email	Profile	Status
<input type="checkbox"/>		admin	myemail@mycompany.com	Administrator	Active

The table shows all the supported local user accounts and includes the following details:

- **Username**
- **Email**
- **Profile**
- **Status** – Status could take following values – Inactive/Locked/Password expired/Active



For the list of access rights per profile refer to the section [Full documentation>>>Information>>>Access rights per profiles](#).

#### 4.6.2.1.1 Actions

##### a Add

Press the **New** button to add new local users.



You can add up to 20 local users. Kindly note that above 10 users connected simultaneously, it is likely to consume a lot of CPU resources resulting in slower card performance.

##### b Remove

Select a user and press the **Delete** button to remove it.

##### c Edit

Press the pen logo to edit user information: 

You will get access to the following settings:

- Active
- Profile
- Username
- Full name
- Email
- Phone
- Organization – Notify by email about account modification/Password
- Reset password
- Generate randomly
- Enter manually
- Force password to be changed on next login



## d Global settings

## Global user settings

## Password settings

Minimum length	8
<input checked="" type="checkbox"/> Minimum upper case	1
<input checked="" type="checkbox"/> Minimum lower case	1
<input checked="" type="checkbox"/> Minimum digit	1
<input checked="" type="checkbox"/> Special character	1

## Password expiration

- ☐ Number of days until password expires 90
- ☒ Main administrator password never expires

## Lock account

- ☐ Lock account after 4 invalid tries
- ☒ Main administrator account never blocks

## Account timeout

- No activity timeout 15 minutes
- Session lease time 120 minutes

[Save](#)

Press **Save** after modifications.

## Password settings

To set the password strength rules, apply the following restrictions:

- Minimum length
- Minimum upper case
- Minimum lower case
- Minimum digit
- Special character

## Password expiration

To set the password expiration rules, apply the following restrictions:

- Number of days until password expires
- Main administrator password never expire



#### Main administrator password never expires

1. If this feature is disabled, the administrator account can be locked after the password expiration.
2. If Enabled, the administrator password never expires, make sure it is changed regularly.

#### Lock account

- Lock account after a number of invalid tries
- Main administrator account will never block



#### Main administrator account will never block

1. If this feature is disabled, the administrator account can be locked after the number of failed connections defined.
2. If Enabled, the security level of the administrator account is reduced because unlimited password entry attempts are allowed.

#### Account timeout

To set the session expiration rules, apply the following restrictions:

- No activity timeout (in minutes).  
If there is no activity, session expires after the specified amount of time.
- Session lease time (in minutes).  
If there is activity, session still expires after the specified amount of time.



#### Main administrator password never expires

When new settings are set, parameters will be taken into account on their next connection to the card.

### 4.6.2.2 Default settings and possible parameters - Global user settings and Local users

	Default setting	Possible parameters
<b>Password settings</b>	Minimum length — enabled (8) Minimum upper case — enabled (1) Minimum lower case — enabled (1) Minimum digit — enabled (1) Special character — enabled (1)	Minimum length — enable (6-32)/disable Minimum upper case — enable (0-32)/disable Minimum lower case — enable (0-32)/disable Minimum digit — enable (0-32)/disable Special character — enable (0-32)/disable
<b>Password expiration</b>	Number of days until password expires — disabled Main administrator password never expires — disabled	Number of days until password expires — disable/enable (1-99999) Main administrator password never expires — disable/enable
<b>Lock account</b>	Lock account after xx invalid tries — disabled Main administrator account never blocks — disabled	Lock account after xx invalid tries — disable/enable (1-99) Main administrator account never blocks — disable/enable
<b>Account timeout</b>	No activity timeout — 60 minutes Session lease time — 120 minutes	No activity timeout — 1-60 minutes Session lease time — 60-720 minutes

<b>Local users</b>	1 user only: <ul style="list-style-type: none"> <li>• Active — Yes</li> <li>• Profile — Administrator</li> <li>• Username — admin</li> <li>• Full Name — blank</li> <li>• Email — blank</li> <li>• Phone — blank</li> <li>• Organization — blank</li> </ul>	20 users maximum: <ul style="list-style-type: none"> <li>• Active — Yes/No</li> <li>• Profile — Administrator/Operator/Viewer</li> <li>• Username — 255 characters maximum</li> <li>• Full Name — 128 characters maximum</li> <li>• Email — 128 characters maximum</li> <li>• Phone — 64 characters maximum</li> <li>• Organization — 128 characters maximum</li> </ul>
--------------------	---	---

#### 4.6.2.2.1 For other settings



For other settings, see the [Information>>>Default settings parameters](#) section.

#### 4.6.2.3 Access rights per profiles

	Administrator	Operator	Viewer
Local users			

#### 4.6.2.3.1 For other access rights



For other access rights, see the [Information>>>Access rights per profiles](#) section.

#### 4.6.2.4 CLI commands

##### whoami

###### Description

whoami displays current user information:

- Username
- Profile
- Realm

##### logout

###### Description

Logout the current user.

Help

```
logout
<cr> logout the user
```

4.6.2.4.1 For other CLI commands



See the CLI commands in the [Information>>>CLI](#) section.


4.6.2.5 Troubleshooting

**How do I log in if I forgot my password?**

Action

- Ask your administrator for password initialization.
- If you are the main administrator, your password can be reset manually by following steps described in the [Servicing the Network Management Module>>>Recovering main administrator password](#) .

4.6.2.5.1 For other issues



For details on other issues, see the [Troubleshooting](#) section.

4.6.2.6 Save and Restore

	SRR section	SRR sub section	Settings	Possible values
Password settings	accountService	passwordRules	<b>strength</b> minLengthminUpperCase minLowerCase minDigit minSpecialCharacter	Numbers: refer to default settings an possible parameters for constraints.
Password expiration			<b>expiration</b> expiration enabled afterDays defaultAccountNeverExpires	true/false Number: refer to default settings an possible parameters for constraints. true/false

Lock account	lockoutRules	<b>lockoutRules</b> enabled threshold defaultAccountNeverBlocks	true/false Number: refer to default settings an possible parameters for constraints. true
Account timeout	sessionsService	sessionTimeout sessionLeaseTime	Numbers: refer to default settings an possible parameters for constraints.
Local users	PredefinedAccounts	<b>credentials</b> enabled username passwordExpired locked profile <b>password</b> plaintext cyphered	true/false String: refer to default settings an possible parameters for constraints. true/false true/false administrators/operators/viewers  String: refer to default settings an possible parameters for constraints. -

#### 4.6.2.6.1 Additional information



For details on Save and Restore, see the [Save and Restore](#) section.

### 4.6.3 Remote users

#### 4.6.3.1 LDAP

LDAP						
Activate Ldap <input checked="" type="checkbox"/>		<a href="#">Configure</a> <a href="#">Profile mapping</a> <a href="#">User preferences</a>				
Name	Address	Port	security	Certificate	Status	
OpenLDAP	genepi-rum-openldap.mbt.lab.etn.com	389	None	Not verified	Ok	
Secondary	test.mbt.lab.etn.com	389	None	Not verified	No contact	

The table shows all the supported severs and includes the following details:

- Name
- Address
- Port
- Security

- Certificate
- Status – Status could take following values – Unreachable/Active

### 4.6.3.1.1 Actions

#### a Configure

LDAP configuration

Primary server

Name \*

mbt

Hostname \*

192.168.1.101

Port

389

Request parameters

User base DN \*

uid

User name attribute \*

ou=Users,dc=mbt,dc=lab,dc=etn,dc=com

Group base DN \*

cn

Group name attribute \*

ou=Groups,dc=mbt,dc=lab,dc=etn,dc=com

Security

SSL

☐ Verify server certificate

Secondary server

Name

Secondary

Hostname

Port

389

Credentials

☐ Anonymous search bind

Search user DN \*

cn=Manager,dc=mbt,dc=lab,dc=etn,dc=com

Password

Save

1.Enable LDAP to be able to configure settings

2. Press **Configure** to access the following LDAP settings:

- Connectivity
  - Security
    - SSL – None/Start TLS/SSL
    - Verify server certificate
  - Primary server – Name/Hostname/Port
  - Secondary server – Name/Hostname/Port
  - Credentials – Anonymous search bind/Search user DN/Password
  - User base DN
  - User name attribute
  - Group base DN
  - Group name attribute

2. Click **Save**.

## b Profile mapping

Profile mapping

Remote group

Local profile

Save



For the list of access rights per profile refer to the section [Full documentation>>>Information>>>Access rights per profiles](#).

1. Press **Profile mapping** to map remote groups to local profiles.
2. Click **Save**.

c Users preferences



All users preferences will apply to all remote users (LDAP, RADIUS).

Remote Users preferences ✕

Global Settings

Language

English

Temperature

°C

Date format

m/d/Y

Time format

24h

Save

1. Press **Users preferences** to define preferences that will apply to all newly logged in LDAP users
  - Language
  - Temperature
  - Date format
  - Time format
2. Click **Save**.



## d LDAP Test

**Ldap test** [X]

Username \*  
lionel

Password

- ✓ Primary
- ✓ Bind
- ✓ User domain dn
- ✓ User name attribute
- ✓ Group domain dn
- ✓ Group name attribute
- ✓ Mapped profile      Administrators
- ✗ Credentials

**Test**


1. At the end of each LDAP primary or secondary configuration row you'll be able to launch a LDAP test by clicking on the button.
2. The LDAP test will give you a status ( ok / ko ) on below parameters to make it easier to troubleshoot
  - Primary
  - Bind
  - User domain dn
  - User name attribute
  - Group domain dn
  - Group name attribute
  - Mapped profile
  - Credentials
3. Click **Test** to check your configuration.


## 4.6.3.2 RADIUS




Radius is not a secured protocol, for a maximum security, it is recommended to use LDAP over TLS.

RADIUS

 Configure

 Profile mapping

 Delete

Name	Address	Status
Please note that there is no configured server.		

The table shows all the supported servers and includes the following details:

- Name - descriptive name for the RADIUS server
- Address - hostname or IP address for the RADIUS server
- Port - connection port of the RADIUS Server

### 4.6.3.2.1 Actions

#### a Configure

RADIUS configuration

×

**Activity**

Active
No

**Authentication**

Authentication protocol
PAP

Retry number
0

**Primary server**

Name

Secret

Address \*

UDP port
1812

Time out (sec)
3

**Secondary server**

Name

Secret

Address \*

UDP port
1812

Time out (sec)
3

Save

1. Enable Radius to be able to configure settings
2. Press **Configure** to access the following RADIUS settings:
  - Primary server
    - Name - descriptive name for the RADIUS server
    - Secret - a shared secret between the client and the RADIUS server

- Address - hostname or IP address for the RADIUS server
- UDP port - the UDP port for the RADIUS server (1812 by default)
- Time out (s) - length of time the client waits for a response from the RADIUS server
- Retry count - the number of time a connection is retried
- Secondary server
  - Name - descriptive name for the RADIUS server
  - Secret - a shared secret between the client and the RADIUS server
  - Address - hostname or IP address for the RADIUS server
  - UDP port - the UDP port for the RADIUS server (1812 by default)
  - Time out (s) - length of time the client waits for a response from the RADIUS server
  - Retry count - the number of time a connection is retried
- NAS
  - Identifier - descriptive identifier for the radius server to identify the device
  - IP - IP address of the card or a domain name ( FQDN )



Note: The radius protocol supported by the card is PAP

2. Click **Save**.

## b Profile mapping

Profile mapping test

Default Profile

☐ Grant access to all radius users as

Specific Rules

attribute	vendor	value	profile	
28	534	1	Administrator	×
0	0	0		×
0	0	0		×
0	0	0		×

Save



For the list of access rights per profile refer to the section [Full documentation>>>Information>>>Access rights per profiles](#).

1. Press **Profile mapping** to map RADIUS profile to local profiles.

### Default Profile

You can enable & define a default profile for all Radius that are not subject to any specific rules (see below).

### Specific Rules

Fill the usual triplet of information as per your radius configuration:

- Attribute - The attribute value - Mandatory
- Vendor - The vendor value associated to the attribute - Mandatory ( 0 as default value )
- Value - The value of the attribute needed for this mapping - Mandatory

Fill the profile you want your specific radius configuration to be mapped with

- Profile - the local profile you want users to be mapped

Note: The default mapping is used for eaton-specific value : Attribute 28, Vendor 534, Value 1 and Profile administrator. **Please refer to your RADIUS protocol provider documentation for further information.**

2. Click **Save**.

### c Users preferences

Remote Users preferences ✕

Global Settings

Language

English

Temperature

°C

Date format

m/d/Y

Time format

24h

Save

1. Press **Users preferences** to define preferences that will apply to all RADIUS users

- Language
- Temperature
- Date format
- Time format

2. Click **Save**.

### 4.6.3.3 Default settings and possible parameters - Remote users

	Default setting	Possible parameters
LDAP	<p>Configure</p> <ul style="list-style-type: none"> <li>• Active – No</li> <li>• Security SSL – SSL Verify server certificate – enabled</li> <li>• Primary server Name – Primary Hostname – blank Port – 636</li> <li>• Secondary server Name – blank Hostname – blank Port – blank</li> <li>• Credentials Anonymous search bind – disabled Search user DN – blank Password – blank</li> <li>• Search base Search base DN – dc=example,dc=com</li> <li>• Request parameters User base DN – ou=people,dc=example,dc=com User name attribute – uid UID attribute – uidNumber Group base DN – ou=group,dc=example,dc=com Group name attribute – gid GID attribute – gidNumber</li> </ul> <p>Profile mapping – no mapping</p> <p>Users preferences</p> <ul style="list-style-type: none"> <li>• Language – English</li> <li>• Temperature unit – °C (Celsius)</li> <li>• Date format – m/d/Y</li> <li>• Time format – hh:mm:ss (24h)</li> </ul>	<p>Configure</p> <ul style="list-style-type: none"> <li>• Active – No/yes</li> <li>• Security SSL – None/Start TLS/SSL Verify server certificate – disabled/enabled</li> <li>• Primary server Name – 128 characters maximum Hostname – 128 characters maximum Port – x-xxx</li> <li>• Secondary server Name – 128 characters maximum Hostname – 128 characters maximum Port – x-xxx</li> <li>• Credentials Anonymous search bind – disabled/enabled Search user DN – 1024 characters maximum Password – 128 characters maximum</li> <li>• Search base Search base DN – 1024 characters maximum</li> <li>• Request parameters User base DN – 1024 characters maximum  User name attribute – 1024 characters maximum UID attribute – 1024 characters maximum Group base DN – 1024 characters maximum  Group name attribute – 1024 characters maximum GID attribute – 1024 characters maximum</li> </ul> <p>Profile mapping – up to 5 remote groups mapped to local profiles</p> <p>Users preferences</p> <ul style="list-style-type: none"> <li>• Language – English, French, German, Italian, Japanese, Russian, Simplified Chinese, Spanish, Traditional Chinese</li> <li>• Temperature unit – °C (Celsius)/°F (Fahrenheit)</li> <li>• Date format – MM-DD-YYYY / YYYY-MM-DD / DD-MM-YYY / DD.MM.YYY / DD/MM/YYY / DD MM YYYY</li> <li>• Time format – hh:mm:ss (24h) / hh:mm:ss (12h)</li> </ul>

RADIUS	<p>Configure</p> <ul style="list-style-type: none"> <li>• Active – No</li> <li>• Retry number – 0</li> <li>• Primary server <ul style="list-style-type: none"> <li>Name – blank</li> <li>Secret – blank</li> <li>Address – blank</li> <li>UDP port – 1812</li> <li>Time out – 3</li> </ul> </li> <li>• Secondary server <ul style="list-style-type: none"> <li>Name – blank</li> <li>Secret – blank</li> <li>Address – blank</li> <li>UDP port – 1812</li> <li>Time out – 3</li> </ul> </li> </ul> <p>Users preferences</p> <ul style="list-style-type: none"> <li>• Language – English</li> <li>• Temperature unit – °C (Celsius)</li> <li>• Date format – m/d/Y</li> <li>• Time format – hh:mm:ss (24h)</li> </ul>	<p>Configure</p> <ul style="list-style-type: none"> <li>• Active – Yes/No</li> <li>• Retry number – 0 to 128</li> <li>• Primary server <ul style="list-style-type: none"> <li>Name – 128 characters maximum</li> <li>Address – 128 characters maximum</li> <li>Secret – 128 characters maximum</li> <li>UDP port – 1 to 65535</li> <li>Time out – 3 to 60</li> </ul> </li> <li>• Secondary server <ul style="list-style-type: none"> <li>Name – 128 characters maximum</li> <li>Address – 128 characters maximum</li> <li>Secret – 128 characters maximum</li> <li>UDP port – 1 to 65535</li> <li>Time out – 3 to 60</li> </ul> </li> </ul> <p>Users preferences</p> <ul style="list-style-type: none"> <li>• Language – English, French, German, Italian, Japanese, Russian, Simplified Chinese, Spanish, Traditional Chinese</li> <li>• Temperature unit – °C (Celsius)</li> <li>• Date format – MM-DD-YYYY</li> <li>• Time format – hh:mm:ss (24h)</li> </ul>
--------	--	--

#### 4.6.3.3.1 For other settings



For other settings, see the [Information>>>Default settings parameters](#) section.

#### 4.6.3.4 Access rights per profiles

	Administrator	Operator	Viewer
Remote users	✓	✗	✗

#### 4.6.3.4.1 For other access rights



For other access rights, see the [Information>>>Access rights per profiles](#) section.

#### 4.6.3.5 CLI commands

##### ldap-test

##### Description

Ldap-test help to troubleshoot LDAP configuration issues or working issues.

## Help

Usage: ldap-test <command> [OPTION]...  
Test LDAP configuration.

## Commands:

ldap-test -h, --help, Display help page

ldap-test --checkusername <username> [--primary|--secondary] [-v]

Check if the user can be retrieve from the LDAP server

<username> Remote username to test  
 --primary Force the test to use primary server (optional)  
 --secondary Force the test to use secondary server (optional)  
 -v, --verbose Print the exchanges with LDAP server (optional)

ldap-test --checkauth <username> [--primary|--secondary] [-v]

Check if remote user can login to the card

<username> Remote username to test  
 -p, --primary Force the test to use primary server (optional)  
 -s, --secondary Force the test to use secondary server (optional)  
 -v, --verbose Print the exchanges with LDAP server (optional)

ldap-test --checkmappedgroups [--primary|--secondary] [-v]

Check LDAP mapping

-p, --primary Force the test to use primary server (optional)  
 -s, --secondary Force the test to use secondary server (optional)  
 -v, --verbose Print the exchanges with LDAP server (optional)

## Quick guide for testing:

In case of issue with LDAP configuration, we recommend to verify the configuration using the commands in the following order:

1. Check user can be retrieve on the LDAP server  
 ldap-test --checkusername <username>
2. Check that your remote group are mapped to the good profile  
 ldap-test --checkmappedgroups
3. Check that the user can connect to the card  
 ldap-test --checkauth <username>

**logout**

## Description

Logout the current user.

## Help

```
logout
<cr> logout the user
```

**whoami**

## Description

whoami displays current user information:

- Username
- Profile
- Realm

## 4.6.3.5.1 For other CLI commands



See the CLI commands in the [Information>>>CLI](#) section.

## 4.6.3.6 Troubleshooting

**How do I log in if I forgot my password?**

## Action

- Ask your administrator for password initialization.
- If you are the main administrator, your password can be reset manually by following steps described in the [Servicing the Network Management Module>>>Recovering main administrator password](#) .

**LDAP configuration/commissioning is not working**

Refer to the section [Servicing the Network Management Module>>>Commissioning/Testing LDAP](#) .

## 4.6.3.6.1 For other issues



For details on other issues, see the [Troubleshooting](#) section.



### 4.6.3.7 Save and Restore

	SRR section	Sub section	Sub section	Sub section	Sub section	Settings	Sub settings	Possible values
LDAP	ldap	1.0	settings	enabled				true/false
				connectivity	primaryServer	name		String: refer to default settings an possible parameters for constraints.
						uri		String: refer to default settings an possible parameters for constraints.
						port		Unsigned number
				secondaryServer		name		String: refer to default settings an possible parameters for constraints.
						uri		String: refer to default settings an possible parameters for constraints.
						port		Unsigned number
				userDomain		nameAttribute		String: refer to default settings an possible parameters for constraints.
						dn		String: refer to default settings an possible parameters for constraints.
				groupDomain		nameAttribute		String: refer to default settings an possible parameters for constraints.
						dn		String: refer to default settings an possible parameters for constraints.
				bind		dn		String: refer to default settings an possible parameters for constraints.
						password	plaintext	String: refer to default settings an possible parameters for constraints.
							ciphared	String: refer to default settings an possible parameters for constraints.


					<b>security</b>	type	1: ssl 2: starttls 3: none
						verifyCertificate	true/false
				<b>mappings</b>		remoteGroup	String: refer to default settings an possible parameters for constraints.
						profileName	<ul style="list-style-type: none"> <li>administrators</li> <li>viewers</li> <li>operators</li> </ul>
				<b>preferences</b>		language	String: refer to default settings an possible parameters for constraints.
						dateFormat	String: refer to default settings an possible parameters for constraints.
						timeFormat	String: refer to default settings an possible parameters for constraints.
						temperatureUnit	String: refer to default settings an possible parameters for constraints.
						licenceAgreement	String: refer to default settings an possible parameters for constraints.

	SRR section	Sub section	Sub section	Sub section	Sub section	Settings	Sub settings	Possible values
RADIUS	radius	1.0	settings	enabled				true/false
				connectivity		protocol		<ul style="list-style-type: none"> <li>pap</li> <li>chap</li> </ul>
					primaryServer	name		String: refer to default settings an possible parameters for constraints.
						secret		String: refer to default settings an possible parameters for constraints.
						uri		String: refer to default settings an possible parameters for constraints.
						port		Unsigned number

		timeout	Unsigned number
		retryCount	Unsigned number
	<b>secondaryServer</b>	name	String: refer to default settings an possible parameters for constraints.
		secret	String: refer to default settings an possible parameters for constraints.
		uri	String: refer to default settings an possible parameters for constraints.
		port	Unsigned number
		timeout	Unsigned number
		retryCount	Unsigned number
	<b>nas</b>	identifier	String: refer to default settings an possible parameters for constraints.
		ip	String: refer to default settings an possible parameters for constraints.
	<b>mappings</b>	profile	String: refer to default settings an possible parameters for constraints.
		attribute	Number
		value	Number
		vendor	Number
	<b>preferences</b>	language	String: refer to default settings an possible parameters for constraints.
		dateFormat	String: refer to default settings an possible parameters for constraints.
		timeFormat	String: refer to default settings an possible parameters for constraints.
		temperatureUnit	String: refer to default settings an possible parameters for constraints.

					licenceAgreement	String: refer to default settings an possible parameters for constraints.
--	--	--	--	--	------------------	---

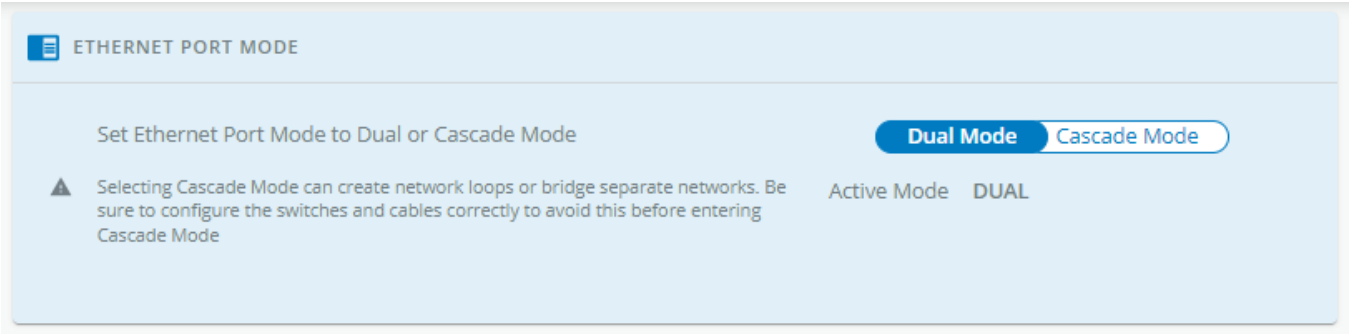
4.6.3.7.1 Additional information

 For details on Save and Restore, see the [Save and Restore](#) section.

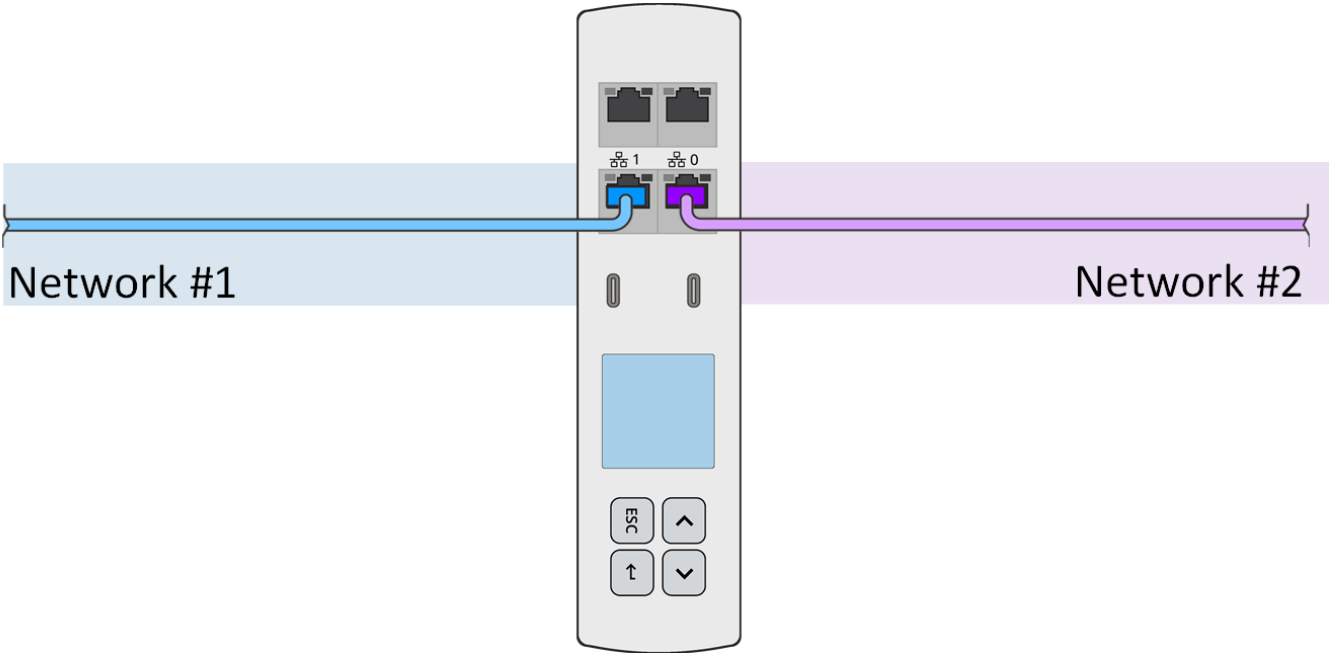
4.6.4 Ports

4.6.4.1 Ethernet port mode

4.6.4.1.1 Dual mode



When **Dual mode** is selected, the 2 Ethernet ports are activated and connected to different networks.



#### 4.6.4.1.2 Cascade mode



Selecting **Cascade mode** can create network loops or bridge separate networks. Be sure to configure switches and cables correctly to avoid this before entering Cascade mode.



##### ETHERNET PORT MODE

Set Ethernet Port Mode to Dual or Cascade Mode

Dual Mode

**Cascade Mode**

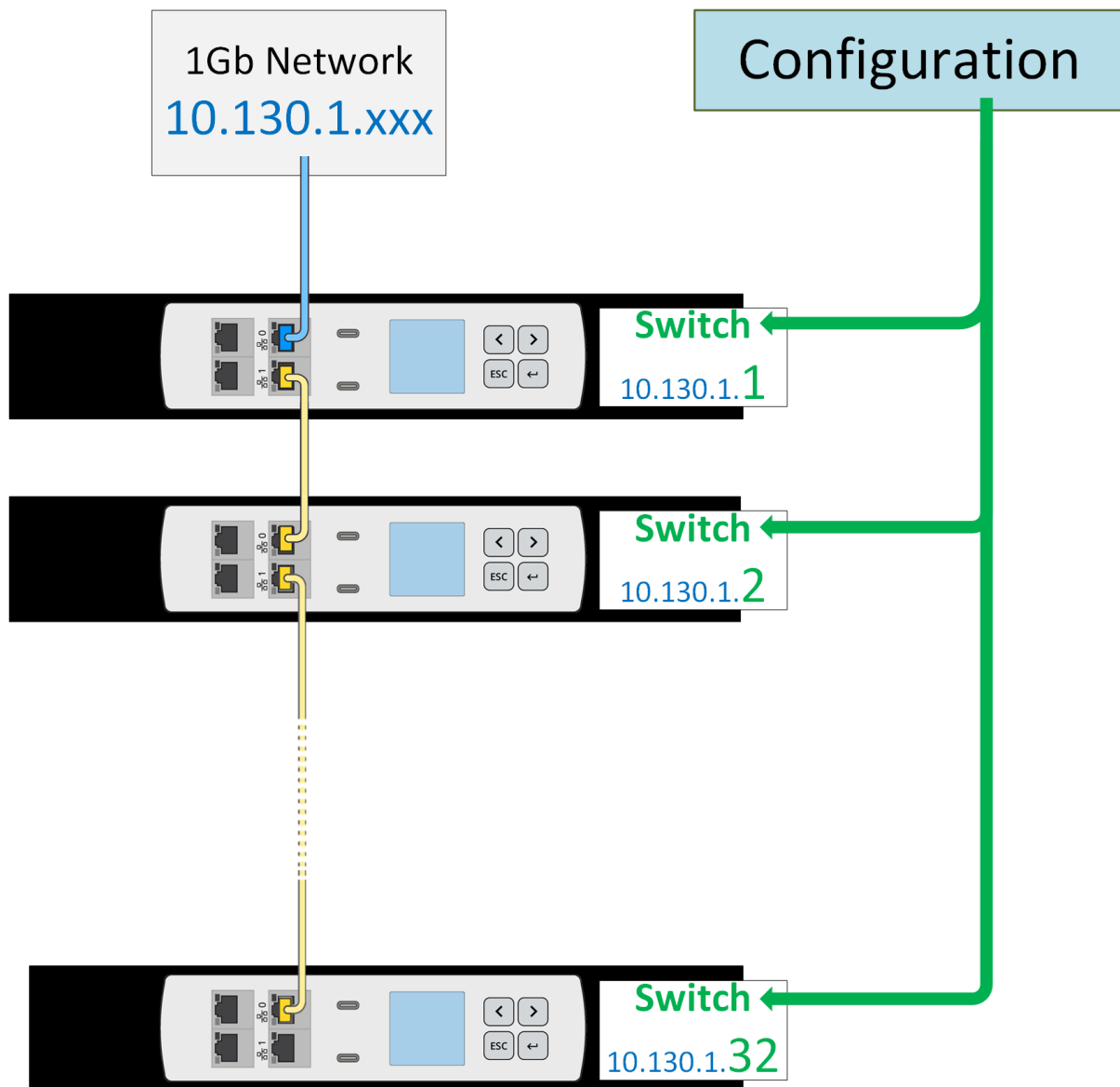


Selecting Cascade Mode can create network loops or bridge separate networks. Be sure to configure the switches and cables correctly to avoid this before entering Cascade Mode

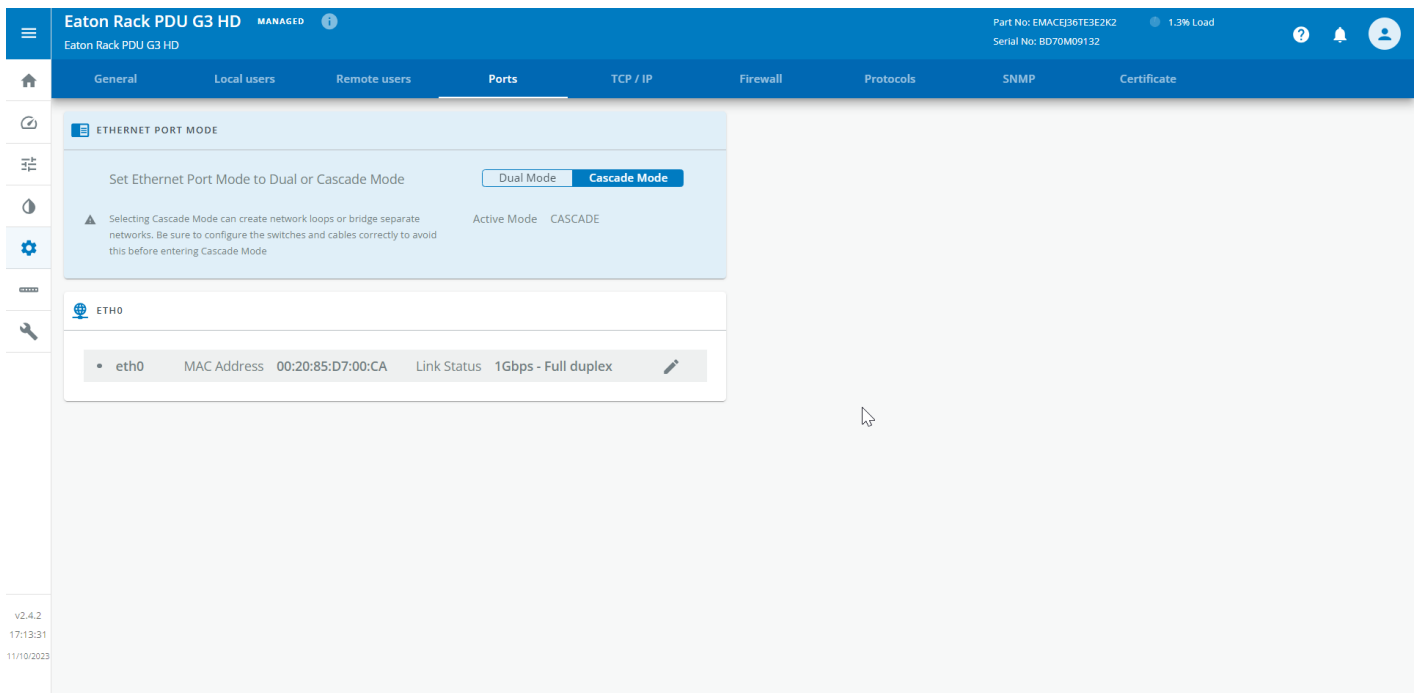
Active Mode **CASCADE**

#### 4.6.4.1.3 Port forwarding mode

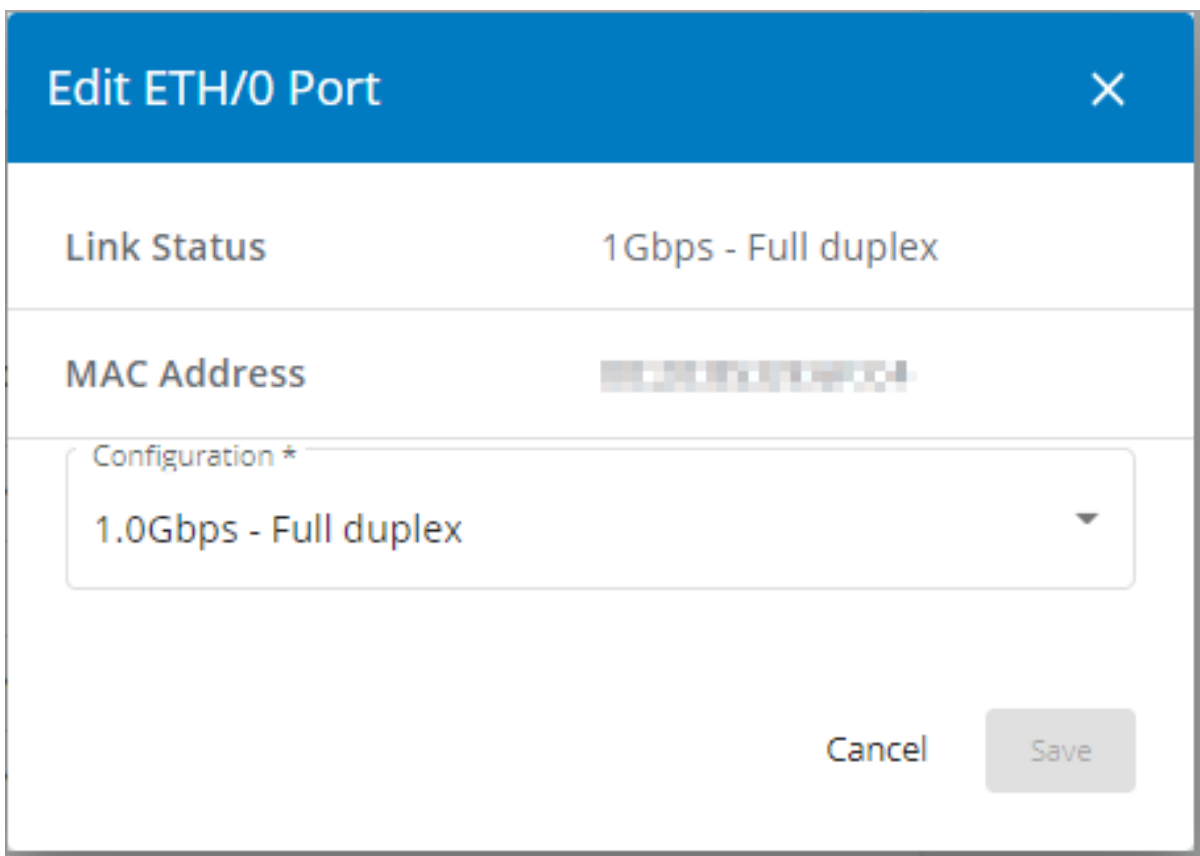
One IP address per PDU.



## 4.6.4.2 Ethernet port and interface settings



### 4.6.4.2.1 Edit port



Allows to edit the link configuration of the selected port through The different options are listed below.

- Auto negotiation
- 10 Mbps - Half duplex
- 10 Mbps - Full duplex

- 100Mbps - Half duplex
- 100Mbps - Full duplex
- 1.0Gbps - Full duplex

#### 4.6.4.3 Default settings and possible parameters - Ports

	Default setting	Possible parameters
Ports- Ethernet port mode	Cascade Mode	Cascade Mode / Dual Mode
Ports- Ethernet port	Auto negotiation	Auto negotiation / 10Mbps - Half duplex / 10Mbps - Full duplex / 100Mbps - Half duplex / 100Mbps - Full duplex / 1.0Gps - Full duplex
Ports- Serial console	Enabled	Enabled / Disabled

##### 4.6.4.3.1 For other settings



For other settings, see the [Information>>>Default settings parameters](#) section.

#### 4.6.4.4 Access rights per profiles

	Administrator	Operator	Viewer
Ports	✓	✗	✗

##### 4.6.4.4.1 For other access rights



For other access rights, see the [Information>>>Access rights per profiles](#) section.

#### 4.6.4.5 Save and Restore

	SRR section	SRR sub section	Settings	Possible values
Ethernet port	peripherals	ethernet	mode	cascade/dual
USB port		usb	enabled	true/false

##### 4.6.4.5.1 Additional information



For details on Save and Restore, see the [Save and Restore](#) section.



### 4.6.5 TCP/IP

#### 4.6.5.1 Hostname

Text field to Enter the Network Module **Hostname**.



## 4.6.5.2 IPV4

IPV4					
Interface Name	Status	Mode	Address	Netmask	Gateway
Eth0	In service 	Manual	-	-	-
Eth1	In service 	Manual	-	-	-




Any modifications are applied after the Network Module reboots.

The table shows includes the following details:


- Interface name
- Status
- Mode
- Address
- Netmask
- Gateway

### 4.6.5.2.1 IPV4 configuration

After a mouse over on the table, click the edit icon  to access settings and configure the network settings for a dedicated interface.

### IPv4 configuration

Mode \*

Manual 

Address \*

169.254.0.1

Netmask \*

255.255.0.0

Gateway

169.254.254.254

Save

Select either the Manual or DHCP settings option.

## a Manual

Select Manual, and then enter the network settings if the network is not configured with a BootP or DHCP server.



- Enter the IP Address.  
The Network Module must have a unique IP address for use on a TCP/IP network.
- Enter the netmask.  
The netmask identifies the class of the sub-network the Network Module is connected to.
- Enter the gateway address.  
The gateway address allows connections to devices or hosts attached to different network segments.

## b DHCP

Select dynamic DHCP to configure network parameters by a BootP or DHCP server.

If a response is not received from the server, the Network Module boots with the last saved parameters from the most recent power up. After each power up, the Network Module makes five attempts to recover the network parameters.


### 4.6.5.3 IPV6

IPV6						
Interface Name	Status	State	Mode	Addresses	Prefix	Gateway
Eth0	In service 	Inactive	Manual		0	-
Eth1	In service 	Inactive	Manual		0	-

The table shows includes the following details:

- **Interface name**
- **Status**
- **Mode**
- **Addresses**
- **Prefix**
- **Gateway**

#### 4.6.5.3.1 IPV6 configuration

After a mouse over on the table, click the edit icon  to access settings and configure the network settings for a dedicated interface.

IPv6 configuration ✕

Enabled

Inactive

Mode \*

Manual

Address \*

FD00::2

Prefix \*

0

Gateway \*

FD00::1

Save

Select either the Manual or Router settings option.

#### a Manual

Select Manual and enter below settings:

- Address
- Prefix
- Gateway

**Enable** the configuration and **Save** it.

#### b Router


Select Router, **Enable** the configuration and **Save** it.

## 4.6.5.4 DNS

DNS				
Interface Name	Mode	FQDN	Primary DNS	Secondary DNS
Eth0	In service	adobe.com	1.1.1.1	1.2.3.4.5
Eth1	In service	adobe.com	1.1.1.1	1.2.3.4.5

The table shows includes the following details:

- Interface name
- Mode
- FQDN
- Primary DNS
- Secondary DNS

After a mouse over on the table, click the edit icon  to access settings and configure the DNS settings for a dedicated interface.

DNS configuration

Hostname \*

Mode \*

Manual

Domain name \*

Primary DNS \*

Secondary DNS \*

Save

Select either the Manual or DHCP settings option.

4.6.5.4.1 Manual

Select Manual and enter below settings:

- Domain name
- Primary DNS
- Secondary DNS

**Save** the configuration.

4.6.5.4.2 DHCP

Select DHCP and **Save** the configuration.

4.6.5.5 Default settings and possible parameters - TCP/IP

	Default setting	Possible parameters
Protocol - Hostname	device-[MAC address]	Hostname — 128 characters maximum
Protocol - IPV4	Enable — checked Mode — DHCP	Enabled — Active/Inactive Mode — DHCP/Manual (Address/Prefix/Gateway)
Protocol - IPV6	Enable — checked Mode — DHCP	Enabled — Active/Inactive Mode — DHCP/Manual (Address/Prefix/Gateway)

Protocol - DNS	Mode — DHCP	Mode :DHCP/Manual (Domain name/Primary DNS/Secondary DNS)
----------------	-------------	---

#### 4.6.5.5.1 For other settings



For other settings, see the [Information>>>Default settings parameters](#) section.

#### 4.6.5.6 Access rights per profiles

	Administrator	Operator	Viewer
TCP/IP	✓	✗	✗

#### 4.6.5.6.1 For other access rights



For other access rights, see the [Information>>>Access rights per profiles](#) section.

#### 4.6.5.7 CLI commands

##### netconf

##### Description

Tools to display or change the network configuration of the card.

##### Help

For Viewer and Operator profiles:

```
netconf -h
Usage: netconf [OPTION]...
Display network information and change configuration.

-h, --help      display help page
-l, --lan       display Link status and MAC address
-4, --ipv4      display IPv4 Mode, Address, Netmask and Gateway
-6, --ipv6      display IPv6 Mode, Addresses and Gateway
-d, --domain    display Domain mode, FQDN, Primary and Secondary DNS
```

For Administrator profile:

```
netconf -h
Usage: netconf [OPTION]...
Display network information and change configuration.
-h, --help      display help page
-l, --lan       display Link status and MAC address
-d, --domain    display Domain mode, FQDN, Primary and Secondary DNS
```

```

-4, --ipv4      display IPv4 Mode, Address, Netmask and Gateway
-6, --ipv6      display IPv6 Mode, Addresses and Gateway
Set commands are used to modify the settings.
-s, --set-lan <link speed>
Link speed values:
auto           Auto negotiation
10hf           10 Mbps - Half duplex
10ff           10 Mbps - Full duplex
100hf          100 Mbps - Half duplex
100ff          100 Mbps - Full duplex
1000ff         1.0 Gbps - Full duplex
-f, --set-domain hostname <hostname>    set custom hostname
-f, --set-domain <mode>
Mode values:
- set custom Network address, Netmask and Gateway:
  manual <domain name> <primary DNS> <secondary DNS>
- automatically set Domain name, Primary and Secondary DNS
  dhcp
-i, --set-ipv4 <mode>
Mode values:
- set custom Network address, Netmask and Gateway
  manual <network> <mask> <gateway>
- automatically set Network address, Netmask and Gateway
  dhcp
-x, --set-ipv6 <status>
Status values:
- enable IPv6
  enable
- disable IPv6
  disable
-x, --set-ipv6 <mode>
Mode values:
- set custom Network address, Prefix and Gateway
  manual <network> <prefix> <gateway>
- automatically set Network address, Prefix and Gateway
  router

```

#### Examples of usage:

```

-> Display Link status and MAC address
netconf -l
-> Set Auto negotiation to Link
netconf --set-lan auto
-> Set custom hostname
netconf --set-domain hostname ups-00-00-00-00-00-00
-> Set Address, Netmask and Gateway
netconf --set-ipv4 manual 192.168.0.1 255.255.255.0 192.168.0.2
-> Disable IPv6

```

#### Examples of usage

```

-> Display Link status and MAC address
netconf -l
-> Set Auto negotiation to Link
netconf -s auto
-> Set custom hostname
netconf -f hostname ups-00-00-00-00-00-00
-> Set Address, Netmask and Gateway
netconf -i manual 192.168.0.1 255.255.255.0 192.168.0.2

```

```
-> Disable IPv6
    netconf -6 disable
```

## ping and ping6

### Description

Ping and ping6 utilities are used to test network connection.

### Help

#### ping

The ping utility uses the ICMP protocol's mandatory ECHO\_REQUEST datagram to elicit an ICMP ECHO\_RESPONSE from a host or gateway. ECHO\_REQUEST datagrams ('`pings'') have an IP and ICMP header, followed by a ``struct timeval'' and then an arbitrary number of ``pad'' bytes used to fill out the packet.

```
-c          Specify the number of echo requests to be sent
-h          Specify maximum number of hops
<Hostname or IP> Host name or IP address
```

#### ping6

The ping6 utility uses the ICMP protocol's mandatory ECHO\_REQUEST datagram to elicit an ICMP ECHO\_RESPONSE from a host or gateway. ECHO\_REQUEST datagrams ('`pings'') have an IP and ICMP header, followed by a ``struct timeval'' and then an arbitrary number of ``pad'' bytes used to fill out the packet.

```
-c          Specify the number of echo requests to be sent
<IPv6 address> IPv6 address
```

## traceroute and traceroute6

### Description

Traceroute and traceroute6 utilities are for checking the configuration of the network.

## Help

```

traceroute
  -h          Specify maximum number of hops
  <Hostname or IP> Remote system to trace

```

```

traceroute6
  -h          Specify maximum number of hops
  <IPv6 address> IPv6 address

```

## 4.6.5.7.1 For other CLI commands



See the CLI commands in the [Information>>>CLI](#) section.

## 4.6.5.8 Save and Restore

	SRR section	SRR sub section	Setting s	Sub settings	Possible values
Ethernet	network Interfaces	link	config		0
DNS/ DHCP		domain	mode		1
			manual	domain Name	String: refer to default settings an possible parameters for constraints.
			dns	preferredServer alternateServer	xx.xxx.xx.xx xx.xxx.xx.xx
IPv4		ipv4	enabled dhcpEnabled		true/false true/false
			manual	address	xx.xxx.xx.xx
				subnet Mask	xxx.xxx.xxx.x
gateway		xx.xxx.xx.x			
IPv6		ipv6	enabled		true/false
			addressing		*
			mode		*
	manual		address	*	



			prefixLength	*
			gateway	*
Hostname		Hostname		String: refer to default settings an possible parameters for constraints.

#### 4.6.5.8.1 Additional information



For details on Save and Restore, see the [Save and Restore](#) section.

## 4.6.6 Firewall

This page allows to set the firewall settings to filter incoming network packets by defining a set of rules based on network, IP addresses and ports combinations.

Below settings can be done for each protocols:

- Communication through ETH0, ETH1 can be activated or not.
- Port can be set for ETH0 and ETH1.
- An IP whitelists can be defined for ETH0 and ETH1.



By default the firewall comes with a **predefined set of network services**

- Web UI (service always enabled at first boot, otherwise no configuration of the firewall is possible by the user)
- SSH
- SNMP
- MQTT
- Ping capabilities

All other network services are disabled by default for remote access and can be configured afterwards.

### 4.6.6.1 HTTP redirect to HTTPS



HTTP REDIRECT TO HTTPS

Name	State	Port	Address Filter
ETH0	<input checked="" type="checkbox"/> Active	80	

Save

4.6.6.2 Secure web (HTTPS)




SECURE WEB (HTTPS)

Name	State	Port	Address Filter 
ETH0	 Active	443	

Save

4.6.6.3 SSH




SSH

Name	State	Port	Address Filter 
ETH0	 Active	22	
ETH1	 Active	22	

Save

4.6.6.4 SNMP

SNMP

Name	State	Port	Address Filter 
ETH0	 Active	161	192.168.1.1-192.168.255.255
ETH1	 Active	161	192.168.1.1-192.168.255.255

Save

### 4.6.6.5 MQTT

MQTT

Name	State	Port	Address Filter ⓘ
ETH0	<input checked="" type="checkbox"/> Active	8833	192.168.0.1-192.168.255.255
ETH1	<input checked="" type="checkbox"/> Active	8833	192.168.0.1-192.168.255.255

Save

### 4.6.6.6 ICMP V4

ICMP V4

Name	State	Address Filter ⓘ
ETH0	<input checked="" type="checkbox"/> Active	
ETH1	<input checked="" type="checkbox"/> Active	

Save

### 4.6.6.7 ICMP V6

ICMP V6

Name	State	Address Filter ⓘ
ETH0	<input checked="" type="checkbox"/> Active	
ETH1	<input checked="" type="checkbox"/> Active	

Save

### 4.6.6.8 Default settings and possible parameters - Firewall

	Default setting	Possible parameters
Firewall - WEB	State : Active Port : 80 Address Filter : Empty	Active / Inactive Integer IP address

Firewall - Secure WEB	State : Active Port : 443 Address Filter : Empty	Active / Inactive Integer IP address
Firewall - SSH	State : Active Port : 22 Address Filter : Empty	Active / Inactive Integer IP address
Firewall - SNMP	State : Active Port : 161 Address Filter : Empty	Active / Inactive Integer IP address
Firewall - MQTT	State : Active Port : 8883 Address Filter : Empty	Active / Inactive Integer IP address
Firewall - ICMP V4	State : Active Address Filter : Empty	Active / Inactive IP address
Firewall - ICMP V6	State : Active Address Filter : Empty	Active / Inactive IP address

#### 4.6.6.8.1 For other settings



For other settings, see the [Information>>>Default settings parameters](#) section.

#### 4.6.6.9 Access rights per profiles

	Administrator	Operator	Viewer
Firewall	✓	✗	✗

#### 4.6.6.9.1 For other access rights



For other access rights, see the [Information>>>Access rights per profiles](#) section.

#### 4.6.6.10 Save and Restore

	SRR section	Interface	SRR sub section	Settings	Sub settings	Possible values
ICMP	Firewall	ETHx	ICMP	V4	Enabled	true/false
				V6	Enabled	true/false
HTTP_REDIRECT			HTTP_REDIRECT	Enabled		true/false
				port		Number : refer to default settings an possible parameters for constraints.

				address (White list)	xx.xxx.xx.xx
SECURE_WEB			SECURE_WEB	Enabled	true/false
				port	Number : refer to default settings an possible parameters for constraints.
				address (White list)	xx.xxx.xx.xx
SSH			SSH	Enabled	true/false
				port	Number : refer to default settings an possible parameters for constraints.
				address (White list)	xx.xxx.xx.xx
SNMP			SNMP	Enabled	true/false
				port	Number : refer to default settings an possible parameters for constraints.
				address (White list)	xx.xxx.xx.xx
MQTT			MQTT	Enabled	true/false
				port	Number : refer to default settings an possible parameters for constraints.
				address (White list)	xx.xxx.xx.xx

#### 4.6.6.10.1 Additional information



For details on Save and Restore, see the [Save and Restore](#) section.

## 4.6.7 Protocols

### 4.6.7.1 Syslog

SYSLOG

Inactive

Active

	Name	Address	Security	Port	Protocol	Status
<div></div>	Primary		TLS - Syslog Certificate	6514	TCP	<div></div> Inactive
<div></div>			TLS - Syslog Certificate	6514	TCP	<div></div> Inactive

Save

#### 4.6.7.1.1 Settings

This screen allows an administrator to configure up to two syslog servers.

To configure the syslog server settings:

1- **Enable** syslog.

Press **Save** after modifications.

2- **Configure** the syslog server:

Edit syslog server configuration

Name \*

Primary

Port \*

6514

Status

Disabled

Protocol

TCP

Hostname \*

Message transfer method


SSL

TLS

Using unicode byte order mask (BOM)

Verify server certificate

Save

- Click the edit icon  to access settings.
- Enter or change the server name.
- Select **Yes** in the Active drop-down list to activate the server.

- Enter the Hostname and Port.
- Select the Protocol – UDP/TCP.
- In TCP, select the message transfer method – Octet counting/Non-transparent framing.
- Select the option Using Unicode BOM if needed.
- Press **Save** after modifications.

#### 4.6.7.2 Default settings parameters and limitations

	Default setting	Possible parameters
HTTPS	Port — 443	Port — x-xxx
Syslog	Enable — disabled <ul style="list-style-type: none"> <li>• Server#1               <ul style="list-style-type: none"> <li>Name – Primary</li> <li>Active – No</li> <li>Hostname – empty</li> <li>Port – 514</li> <li>Protocol – UDP</li> <li>Message transfer method – Non transparent framing</li> <li>Using unicode byte order mask (BOM) – disabled</li> </ul> </li> <li>• Server#2               <ul style="list-style-type: none"> <li>Name – empty</li> <li>Active – No</li> <li>Hostname – empty</li> <li>Port – 514</li> <li>Protocol – UDP</li> <li>Message transfer method – Disabled in UDP</li> <li>Using unicode byte order mask (BOM) – disabled</li> </ul> </li> </ul>	Enable — disable/enable <ul style="list-style-type: none"> <li>• Server#1               <ul style="list-style-type: none"> <li>Name – 128 characters maximum</li> <li>Active – No/Yes</li> <li>Hostname – 128 characters maximum</li> <li>Port – x-xxx</li> <li>Protocol – UDP/TCP</li> <li>Message transfer method – Non transparent framing</li> <li>Using unicode byte order mask (BOM) – disable/enable</li> </ul> </li> <li>• Server#2               <ul style="list-style-type: none"> <li>Name – 128 characters maximum</li> <li>Active – No/Yes</li> <li>Hostname – 128 characters maximum</li> <li>Port – x-xxx</li> <li>Protocol – UDP/TCP</li> <li>Message transfer method (in TCP) – Octet counting/Non transparent framing</li> <li>Using unicode byte order mask (BOM) – disable/enable</li> </ul> </li> </ul>

#### 4.6.7.3 Default settings and possible parameters - Protocols

	Default setting	Possible parameters
--	-----------------	---------------------

Syslog	Inactive	Inactive/Active
	<ul style="list-style-type: none"> <li>Server#1               <ul style="list-style-type: none"> <li>Name – Primary</li> <li>Status – Disabled</li> <li>Hostname – empty</li> <li>Port – 514</li> <li>Protocol – UDP</li> <li>Message transfer method – Non transparent framing</li> <li>Using unicode byte order mask (BOM) – disabled</li> </ul> </li> <li>Server#2               <ul style="list-style-type: none"> <li>Name – empty</li> <li>Status – Disabled</li> <li>Hostname – empty</li> <li>Port – 514</li> <li>Protocol – UDP</li> <li>Message transfer method – Disabled in UDP</li> <li>Using unicode byte order mask (BOM) – disabled</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Server#1               <ul style="list-style-type: none"> <li>Name – 128 characters maximum</li> <li>Status – Disabled/Enabled</li> <li>Hostname – 128 characters maximum</li> <li>Port – x-xxx</li> <li>Protocol – UDP/TCP</li> <li>Message transfer method – Non transparent framing</li> <li>Using unicode byte order mask (BOM) – disable/enable</li> </ul> </li> <li>Server#2               <ul style="list-style-type: none"> <li>Name – 128 characters maximum</li> <li>Status – Disabled/Enabled</li> <li>Hostname – 128 characters maximum</li> <li>Port – x-xxx</li> <li>Protocol – UDP/TCP</li> <li>Message transfer method (in TCP) – Octet counting/Non transparent framing</li> <li>Using unicode byte order mask (BOM) – disable/enable</li> </ul> </li> </ul>

#### 4.6.7.3.1 For other settings



For other settings, see the [Information>>>Default settings parameters](#) section.

#### 4.6.7.4 Access rights per profiles

	Administrator	Operator	Viewer
Protocols	✓	✗	✗

#### 4.6.7.4.1 For other access rights



For other access rights, see the [Information>>>Access rights per profiles](#) section.

#### 4.6.7.5 Save and Restore

	SRR section	SRR sub section	Settings	Sub settings	Possible values
Syslog	rsyslog	certificates	ca trustedClient		*
		Settings	enabled		true/false



		<b>servers</b>	name		String: refer to default settings an possible parameters for constraints.
			enabled		true/false
			hostname		String: refer to default settings an possible parameters for constraints.
			protocol		1: UDP 2: TCP
			port		Number: refer to default settings an possible parameters for constraints.
			tcpFraming		1: TRADITIONAL 2: OCTET_COUNTING
			usingByteOrderMask		true/false
			<b>security</b>	ssl	*
				verifyTlsCert	true/false
			name		String: refer to default settings an possible parameters for constraints.
			enabled		true/false
			hostname		String: refer to default settings an possible parameters for constraints.
			protocol		1: UDP 2: TCP
			port		Number: refer to default settings an possible parameters for constraints.
			tcpFraming		1: TRADITIONAL 2: OCTET_COUNTING
			usingByteOrderMask		true/false
			<b>security</b>	ssl	*
				verifyTlsCert	true/false


#### 4.6.7.5.1 Additional information



For details on Save and Restore, see the [Save and Restore](#) section.


# 4.6.8 SNMP

This tab contains settings for SNMP protocols used for network management systems.




Changes to authentication settings need to be confirmed by entering a valid password for the active user account.


## 4.6.8.1 SNMP tables



The default port for SNMP is 161 and normally this should not be changed. Some organizations prefer to use non-standard ports due to cybersecurity, and this field allows that.





SNMP

Supported MIBs 





 **Reminder**

SNMP Protocol will not be functional unless you enable the corresponding port in the [Firewall page](#)

SNMP V1 / V2C ☐

Community	Access	Status	
public	Read only	Inactive 	
private	Read/Write	Inactive 	

SNMP V3 ☒

Users	Access	Security level	Status	
readonly	Read only	Auth (SHA_256) , Priv (AES)	Inactive 	
readwrite	Read/Write	Auth (SHA_256) , Priv (AES)	Inactive 	

Save

SNMP monitoring Battery status, power status, events, and traps are monitored using third-party SNMP managers.

To query SNMP data, you do not need to add SNMP Managers to the Notified Application page.

To set-up SNMP managers:

- Configure the IP address.
- Select SNMP v1/v2 or v3.
- Compile the MIB you selected to be monitored by the SNMP manager.

List of supported MIBs: *PDU MIB / Sensor MIB*

Press the **Supported MIBs** button to download the MIBs.

### 4.6.8.1.1 Settings

This screen allows an administrator to configure SNMP settings for computers that use the MIB to request information from the Network Module.

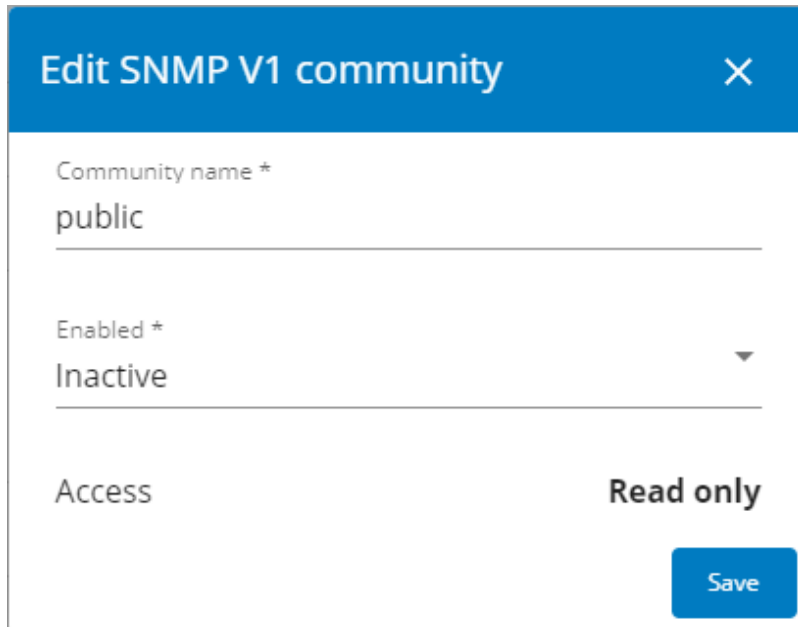
Default ports for SNMP are 161 (SNMP v1 and v3, set/get) and 162 (traps). These ports can be changed on the settings screen for additional security.

To configure the SNMP settings:

**a Enable the SNMP agent**

In addition to this, v1/V2C and/or v3 must be enabled, along with appropriate communities and activated user accounts to allow SNMP communication.

Press **Save** after modifications.

**b Configure the SNMP V1/V2C settings:**


**Edit SNMP V1 community** X

Community name \*  
public

Enabled \*  
Inactive

Access  
Read only

Save

1. Click the edit icon on either Read Only or Read/Write account to access settings: 
2. Enter the SNMP Community Read-Only string. The Network Module and the clients must share the same community name to communicate.
3. Select **Active** in the Enabled drop-down list to activate the account.
4. Access level is set to display information only.

## c Configure the SNMP V3 settings:

Edit SNMP V3 user

×

User name \*

readonly

Enabled \*

Inactive

▼

Access \*

Read only

▼

Security \*

Auth, Priv

▼

Authentication algorithm \*

SHA 256

▼

Password

Confirm Password

Privacy algorithm \*

AES

▼


Key

Confirm key

Please enter your own password to confirm

Confirm Password \*

Save

1. Click the edit icon on either Read Only or Read/Write account to access settings: 
2. Edit the user name.
3. Select **Active** in the Enabled drop-down list to activate the account.
4. Select access level.
  - **Read only**—The user does not use authentication and privacy to access SNMP variables.
  - **Read/Write**—The user must use authentication, but not privacy, to access SNMP variables.
5. Select the communication security mechanism.
  - **Auth, Priv**—Communication with authentication and privacy.
  - **Auth, No Priv**—Communication with authentication and without privacy.
  - **No Auth, No Priv**—Communication without authentication and privacy.

6. If Auth is selected on the communication security mechanism, select the Authentication algorithms.



It is recommended to set SHA256/SHA384/SHA512 with the AES192/AES256 Privacy algorithms.

- **SHA**—SHA1 is not recommended as it is not secured.
- **SHA256**—fill in password and privacy keys. The password can be between 8 and 24 characters and use a combination of alphanumeric and the following special characters <>&@#%\_=:;,./?|\$\*.
- **SHA384**—fill in password and privacy keys. The password can be between 8 and 24 characters and use a combination of alphanumeric and the following special characters <>&@#%\_=:;,./?|\$\*.
- **SHA512**—fill in password and privacy keys. The password can be between 8 and 24 characters and use a combination of alphanumeric and the following special characters <>&@#%\_=:;,./?|\$\*.
- **AES / AES192 / AES256**

7. If Priv is selected on the communication security mechanism, select the Privacy algorithms.



It is recommended to set AES192/AES256 with the SHA256/SHA384/SHA512 Authentication algorithms.

- **AES**—fill in password and privacy keys. The password can be between 8 and 24 characters and use a combination of alphanumeric and the following special characters <>&@#%\_=:;,./?|\$\*.
- **AES192**—fill in password and privacy keys. The password can be between 8 and 24 characters and use a combination of alphanumeric and the following special characters <>&@#%\_=:;,./?|\$\*.
- **AES256**—fill in password and privacy keys. The password can be between 8 and 24 characters and use a combination of alphanumeric and the following special characters <>&@#%\_=:;,./?|\$\*.

8. Enter your own login password and click **Save**.

## 4.6.8.2 Trap receivers

TRAP RECEIVERS

+ New

🗑 Delete

🔄 Test trap

Application name	Host	Protocol	Port	Status

The table shows all the trap receivers and includes the following details:

- **Application name**
- **Host**
- **Protocol**
- **Port**
- **Status:** Active/Inactive/Error(configuration error)

### 4.6.8.2.1 Actions

#### a Add

## New trap receiver ×

Enabled  
Inactive ▼

Protocol  
V1 ▼

Application name \*

User ▼

Hostname or IP address \*

Trap community \*

Port \*  
162

Cancel

Save

1. Press the **New** button to create new trap receivers.

2. Set following settings:


- Enabled – Yes/No
- Application name
- Hostname or IP address
- Port
- Protocol – V1/V2C/V3
- Trap community (V1/V2C) / User (V3)

3. Press the **SAVE** button.

#### b Remove

Select a trap receiver and press the **Delete** button to remove it.

#### c Edit

Press the pen icon to edit trap receiver information and access to its settings: 

#### d Test trap

Press the **Test trap** button to send the trap test to all trap receivers.

Separate window provides the test status with following values:

- In progress
- Request successfully sent
- invalid type



For details on SNMP trap codes, see the [Information>>>SNMP traps](#) section.

#### 4.6.8.3 Link to SNMP traps

- [Sensor Mib](#)
- [PDU Mib](#)

#### 4.6.8.4 Default settings and possible parameters - SNMP

	Default setting	Possible parameters
SNMP	Activate SNMP — disabled Port — 161 SNMP V1 — disabled <ul style="list-style-type: none"> <li>• Community #1 — public Enabled — Inactive Access — Read only</li> <li>• Community #2 — private Enabled — Inactive Access — Read/Write</li> </ul> SNMP V3 — enabled <ul style="list-style-type: none"> <li>• User #1 — readonly Enabled — Inactive Access — Read only Authentication — Auth (SHA-1) Password — empty Confirm password — empty Privacy — Secured - AES Key — empty Confirm key — empty</li> <li>• User#2 — readwrite Enabled — Inactive Access — Read/Write Authentication — Auth (SHA-1) Password — empty Confirm password — empty Privacy — Secured - AES Key — empty Confirm key — empty</li> </ul>	Activate SNMP — disable/enable Port — x-xxx SNMP V1 — disable/enable <ul style="list-style-type: none"> <li>• Community #1 — 128 characters maximum Enabled — Inactive/Active Access — Read only</li> <li>• Community #2 — 128 characters maximum Enabled — Inactive/Active Access — Read/Write</li> </ul> SNMP V3 — disable/enable <ul style="list-style-type: none"> <li>• User #1 — 32 characters maximum Enabled — Inactive/Active Access — Read only/Read-Write Authentication — Auth (SHA-1)/None Password — 128 characters maximum Confirm password — 128 characters maximum Privacy — Secured - AES/None Key — 128 characters maximum Confirm key — 128 characters maximum</li> <li>• User#2 — 32 characters maximum Enabled — Inactive/Active Access — Read only/Read-Write Authentication — Auth (SHA-1)/None Password — 128 characters maximum Confirm password — 128 characters maximum Privacy — Secured - AES/None Key — 128 characters maximum Confirm key — 128 characters maximum</li> </ul>

Trap receivers	No trap	Enabled — No/Yes Application name — 128 characters maximum Hostname or IP address — 128 characters maximum Port — x-xxx Protocol — V1/V2C/V3 Trap community — 128 characters maximum
----------------	---------	---

#### 4.6.8.4.1 For other settings



For other settings, see the [Information>>>Default settings parameters](#) section.

#### 4.6.8.5 Access rights per profiles

	Administrator	Operator	Viewer
SNMP	✓	✗	✗

#### 4.6.8.5.1 For other access rights



For other access rights, see the [Information>>>Access rights per profiles](#) section.

#### 4.6.8.6 Troubleshooting

##### 4.6.8.6.1 For other issues



For details on other issues, see the [Troubleshooting](#) section.

#### 4.6.8.7 Save and Restore

	SRR section	SRR sub section	Settings	Sub settings	Example
SNMP	snmp		enabled		true
			port		Number: refer to default settings an possible parameters for constraints.
	v1		enabled		true
			communities	readOnly	
				Name	String: refer to default settings an possible parameters for constraints.
				Enabled	
				readWrite	



		Name	String: refer to default settings an possible parameters for constraints.
		Enabled	true/false
v3	enabled		true
	users	name	String: refer to default settings an possible parameters for constraints.
		allowWrite	true/false
		enabled	true/false
		<b>auth</b>	
		enabled	true/false
		algorithm	*
		<b>password</b>	
		plaintext	String: refer to default settings an possible parameters for constraints.
		cyphered	-
		<b>priv</b>	
		enabled	true/false
		algorithm	*
		<b>password</b>	
		plaintext	String: refer to default settings an possible parameters for constraints.
		cyphered	-
		name	String: refer to default settings an possible parameters for constraints.
		allowWrite	true/false
		enabled	true/false
		<b>auth</b>	
		enabled	true/false
		algorithm	*
		<b>password</b>	
		plaintext	String: refer to default settings an possible parameters for constraints.

				cyphered	-
				<b>priv</b>	
				enabled	true/false
				algorithm	*
				<b>password</b>	
				plaintext	String: refer to default settings an possible parameters for constraints.
				cyphered	-
		<b>traps</b>	receivers	name	String: refer to default settings an possible parameters for constraints.
				host	*
				port	Number: refer to default settings an possible parameters for constraints.
				community	*
				protocol	1 : V1 2 : V2C 3 : V3
				user	*
				enabled	true/false

#### 4.6.8.7.1 Additional information



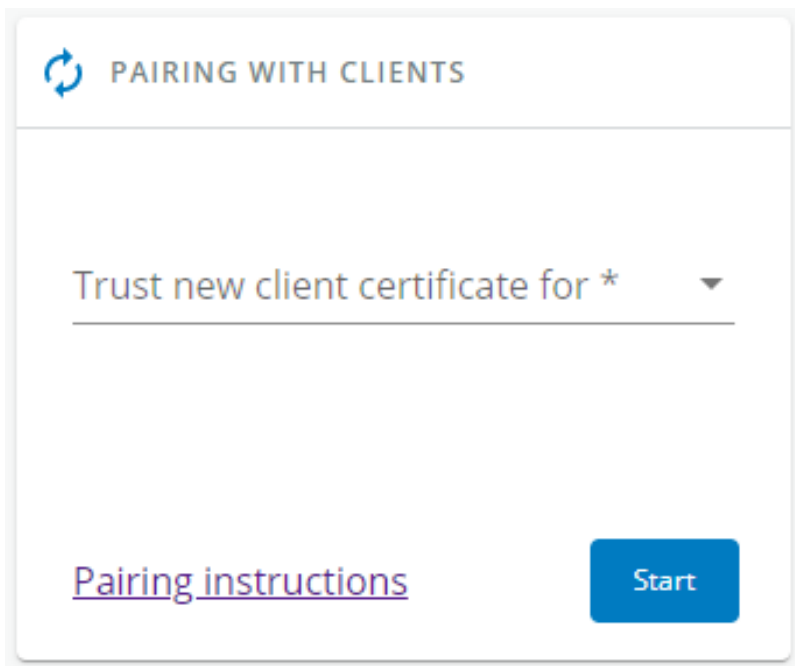
For details on Save and Restore, see the [Save and Restore](#) section.

## 4.6.9 Certificate

### 4.6.9.1 Pairing with clients



For details on pairing instructions, follow the link [pairing instructions](#) in the tile or see the Servicing the Network Management Module>>>*Pairing agent to the Network Module* section.



**PAIRING WITH CLIENTS**

Trust new client certificate for \*

[Pairing instructions](#) **Start**

During the selected timeframe, new connections to the Network Module are automatically trusted and accepted.

After automatic acceptance, make sure that all listed clients belong to your infrastructure. If not, access may be revoked using the Delete button.

The use of this automatic acceptance should be restricted to a secured and trusted network.

For maximum security, we recommend following one of the two methods on the certificate settings page:

- Import agent's certificates manually.
- Generate trusted certificate for both agents and Network Module using your own PKI.

#### 4.6.9.1.1 Actions

##### a Start

Starts the pairing window during the selected timeframe or until it is stopped.

Time countdown is displayed.

##### b Stop

Stops the pairing window.

#### 4.6.9.2 Local certificates

Manage local certificates by :

- Generating CSR and import certificates signed by the CA.
- Generating new self-signed certificates.

4.6.9.2.1 Local certificates table

LOCAL CERTIFICATES

Revoke

Export

Configure issuer

	Used for	Issued by	Valid from	Expiration	Status
<input type="checkbox"/>	Web Server	1920.1000.0000-0000-0000-0000-000000000000 selfsigned	2020-01-01 00:00:00	2024-01-01 00:00:00	Valid
<input type="checkbox"/>	Syslog	1920.1000.0000-0000-0000-0000-000000000000 selfsigned	2020-01-01 00:00:00	2024-01-01 00:00:00	Valid
<input type="checkbox"/>	Protected applications (MQTT)	1920.1000.0000-0000-0000-0000-000000000000 selfsigned	2020-01-01 00:00:00	2024-01-01 00:00:00	Valid

The table shows the following information for each local certificate.

- Used for
- Issued by
- Valid from
- Expiration
- Status — valid, expires soon, or expired

4.6.9.2.2 Actions

a Revoke

This action will take the selected certificate out of use.

Select the certificate to revoke, and then press the **Revoke** button.

A confirmation window appears, press **Continue** to proceed, this operation cannot be recovered.

Revoke will replace current certificate by a new self-signed certificate.  
This may disconnect connected applications:

- Web browsers
- Shutdown application
- Monitoring application

The certificate that is taken out of use with the revoke action cannot be recovered.

b Export

Exports the selected certificate on your OS browser window.

c Configure issuer

Press the **Configure issuer** button.

A configuration window appears to edit issuer data.

## Issuer configuration



Country \*

FR - France

State or province \*

38

City or locality \*

Grenoble

Organization name \*

Eaton

Organization unit

Power Quality

Contact email address

Modification will take effect at next certificate generation

Cancel

Save

- Common name (CN)
- Country (C)
- State or Province (ST)
- City or Locality (L)
- Organization name (O)
- Organization unit (OU)
- Contact email address

Press **Save** button.



Issuer configuration will be applied only after the revoke of the certificate.

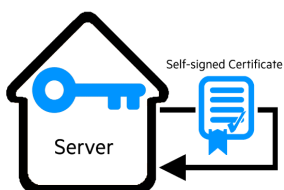
#### d Edit

Press the pen logo: 

You will get access to the following:

- Certificate summary
- Actions
  - Generate a new self-signed certificate
  - Generate a certificate signing request ( CSR )
  - Generate a certificate signing request excluding IP addresses ( CA / CB compliance )
  - Import certificate (only available when CSR is generated).
- Details

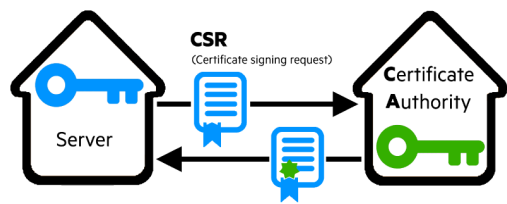
#### e Generate a new self-signed certificate



To replace a selected certificate with a new self-signed certificate.

This may disconnect applications such as a Web browser, shutdown application, or monitoring application.  
This operation cannot be recovered.

f Create new certificates:



g CSR

Press **Generate Signing Request** button in the in the certificate edition.  
The CSR is automatically downloaded.  
CSR must be signed with the CA, which is managed outside the card.

h Import certificate

When the CSR is signed by the CA, it can be imported into the Network Module.  
When the import is complete, the new local certificate information is displayed in the table.

4.6.9.3 Certificate authorities (CA)

Manages CAs.

4.6.9.3.1 CA table

CERTIFICATE AUTHORITIES (CA)					
<div><div><div><div></div><div>Import</div></div><div><div></div><div>Revoke</div></div></div></div>					
Used for	Issued by	Issued To	Valid from	Expiration	Status
No certificate authorities.					

The table displays certificate authorities with the following details:

- Used for
- Issued by
- Issued to
- Valid from
- Expiration
- Status — valid, expires soon, or expired

4.6.9.3.2 Actions

a Import

When importing the CA, you must select the associated service, and then upload process can begin through the OS browser window.

### b Revoke


Select the certificate to revoke, and then press the **Revoke** button.

A confirmation window appears, press **Continue** to proceed, this operation cannot be recovered.

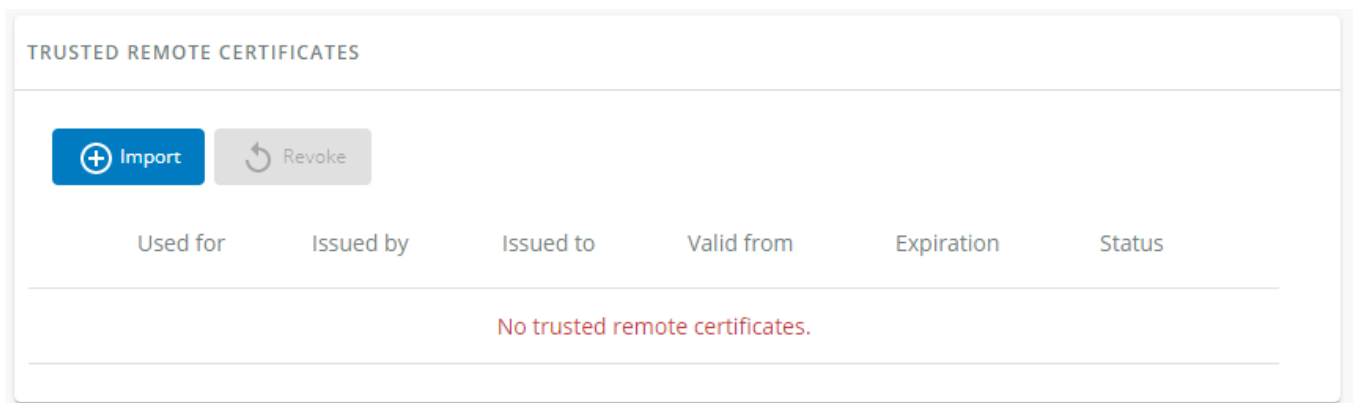
## Export

Exports the selected certificate on your OS browser window.

### c Edit

Press the pen logo to access to the certificate summary: 

## 4.6.9.4 Trusted remote certificates



The table shows the following information for each trusted remote certificate.

- Used for
  - Issued by
  - Issued to
  - Valid from
  - Expiration
  - Status — valid, expires soon, or expired
- In case a certificate expires, the connection with the client will be lost. If this happens, the user will have to recreate the connection and associated certificates.

### 4.6.9.4.1 Actions

#### a Import


When importing the client certificate, you must select the associated service, and then upload process can begin through the OS browser window.

#### b Revoke

Select the certificate to revoke, and then press the **Revoke** button.

A confirmation window appears, press **Continue** to proceed, this operation cannot be recovered.

#### c Edit

Press the pen logo to the certificate summary: 

### 4.6.9.5 Default settings and possible parameters - Certificate

	Default setting	Possible parameters
<b>Local certificates</b>	Common name — Service + Hostname + selfsigned Country — FR State or Province — 38 City or Locality — Grenoble Organization name — Eaton Organization unit — Power quality Contact email address — blank	Common name — 64 characters maximum Country — Country code State or Province — 64 characters maximum City or Locality — 64 characters maximum Organization name — 64 characters maximum Organization unit — 64 characters maximum Contact email address — 64 characters maximum

#### 4.6.9.5.1 For other settings



For other settings, see the [Information>>>Default settings parameters](#) section.

### 4.6.9.6 Access rights per profiles

	Administrator	Operator	Viewer
Certificate	✓	✗	✗

#### 4.6.9.6.1 For other access rights



For other access rights, see the [Information>>>Access rights per profiles](#) section.

### 4.6.9.7 CLI commands

#### certificates

##### Description

Allows to manage certificates through the CLI.

##### Help

```
certificates <target> <action> <service_name>
<target> :
- local
<action> :
- print: provides a given certificate detailed information.
- revoke: revokes a given certificate.
- export: returns a given certificate contents.
- import: upload a given certificate for the server CSR. This will replace the
CSR with the certificate given.
- csr: get the server CSR contents. This will create the CSR if not already
```



```
existing.
<service_name>: mqtt/syslog/webserver
```

### Examples of usage

From a linux host:

```
print over SSH: sshpass -p $PASSWORD ssh $USER@$CARD_ADDRESS certificates local print $SERVICE_NAME
revoke over SSH: sshpass -p $PASSWORD ssh $USER@$CARD_ADDRESS certificates local revoke $SERVICE_NAME
export over SSH: sshpass -p $PASSWORD ssh $USER@$CARD_ADDRESS certificates local export $SERVICE_NAME
import over SSH: cat $FILE | sshpass -p $PASSWORD ssh $USER@$CARD_ADDRESS certificates local import $SERVICE_NAME
csr over SSH: sshpass -p $PASSWORD ssh $USER@$CARD_ADDRESS certificates local csr mqtt
```

From a Windows host: (plink tools from putty is required)

```
print over SSH: plink $USER@$CARD_ADDRESS -pw $PASSWORD -batch certificates local print $SERVICE_NAME
revoke over SSH: plink $USER@$CARD_ADDRESS -pw $PASSWORD -batch certificates local revoke $SERVICE_NAME
export over SSH: plink $USER@$CARD_ADDRESS -pw $PASSWORD -batch certificates local export $SERVICE_NAME
import over SSH: type $FILE | plink $USER@$CARD_ADDRESS -pw $PASSWORD -batch certificates local import $SERVICE_NAME
csr over SSH: plink $USER@$CARD_ADDRESS -pw $PASSWORD -batch certificates local csr mqtt
```

Where:

- \$USER is user name (the user shall have administrator profile)
- \$PASSWORD is the user password
- \$PASSPHRASE is any passphrase to encrypt/decrypt sensible data.
- \$CARD\_ADDRESS is IP or hostname of the card
- \$FILE is a certificate file
- \$SERVICE\_NAME is the name one of the following services : mqtt / syslog / webserver.

#### 4.6.9.7.1 For other CLI commands



See the CLI commands in the [Information>>>CLI](#) section.

### 4.6.9.8 Troubleshooting

#### 4.6.9.8.1 For other issues




For details on other issues, see the [Troubleshooting](#) section.

### 4.6.9.9 Save and Restore

	SRR section	Settings	Example
Certificate issuer configuration	certificateSettings	country	String: refer to default settings an possible parameters for constraints.

		state	String: refer to default settings an possible parameters for constraints.
		location	String: refer to default settings an possible parameters for constraints.
		organizationName	String: refer to default settings an possible parameters for constraints.
		organizationUnit	String: refer to default settings an possible parameters for constraints.
		contact	String: refer to default settings an possible parameters for constraints.
Local certificate (mqtt)	mqtt	certificateData	
		ca	*
		trustedClient	*

4.6.9.9.1 Additional information

 For details on Save and Restore, see the [Save and Restore](#) section.

4.7 PDU settings

4.7.1 General

4.7.1.1 PDU general

4.7.1.1.1 PDU Name

Text field that is used to provide the PDU name information.

4.7.1.1.2 Input Measurement Mode

Allows to configure the input measurement mode with these four options.

- Auto-detect
- Single phase
- 3-Phase Delta 208V
- 3 Phases Wye 230/440V

4.7.1.2 Access rights per profiles

	Administrator	Operator	Viewer
PDU settings - General	✓	✓	✗

#### 4.7.1.2.1 For other access rights



For other access rights, see the [Information>>>Access rights per profiles](#) section.

## 4.7.2 Input thresholds

### 4.7.2.1 Current thresholds

CURRENT THRESHOLDS					
Name	Low warning (A)	Current (A)	High warning (A)	High critical (A)	Energy (kWh)
L1	1	0.092	12.8	16	-

The table shows the following Input current information for each phases and allow alarm thresholds settings:

- Name
- Low warning (A)
- Current (A)
- High warning (A)
- High critical (A)
- Energy (kWh)

#### 4.7.2.1.1 Set alarm threshold

Change the setting in the table and then **Save**.

When a warning threshold is reached, an alarm will be sent with a warning level.

When a critical threshold is reached, an alarm will be sent with a critical level.

### 4.7.2.2 Voltage thresholds

VOLTAGE THRESHOLDS					
Name	Low critical (V)	Low warning (V)	Voltage (V)	High warning (V)	High critical (V)
L1	180	190	243.85	255	265

The table shows the following Input voltage information for each phases and allow alarm thresholds settings:

- Name
- Low critical (V)
- Low warning (V)
- Voltage (V)
- High warning (V)
- High critical (V)

4.7.2.2.1 Set alarm threshold

Change the setting in the table and then **Save**.  
When a warning threshold is reached, an alarm will be sent with a warning level.  
When a critical threshold is reached, an alarm will be sent with a critical level.

4.7.2.3 Access rights per profiles

	Administrator	Operator	Viewer
PDU settings - Input thresholds	✓	✓	✗

4.7.2.3.1 For other access rights

 For other access rights, see the [Information>>>Access rights per profiles](#) section.

4.7.3 Branch thresholds

Eaton Rack PDU G3 HD

MANAGED

Part No: EMACEJ36TE3E2K2

Serial No: BD70M09132

1.3% Load

?

General

Input Thresholds

Branch Thresholds

Outlet Thresholds

Outlet Switching

Group Definition

Current

Voltage

Edit settings

Branch

Low warning (A)

Current (A)

High warning (A)

High critical (A)

A

0

0

16

20

B

0

0

16

20

C

0

0.362

16

20

Save

v2.4.2

17:26:35

11/10/2023

Eaton Rack PDU G3 HD MANAGED

Part No: EMACEJ36TE3E2K2  
Serial No: BD70M09132

1.3% Load

General Input Thresholds **Branch Thresholds** Outlet Thresholds Outlet Switching Group Definition

Current Voltage

Edit settings

Branch	Low critical (V)	Low warning (V)	Voltage (V)	High warning (V)	High critical (V)
A	180	190	244	255	265
B	180	190	244	255	265
C	180	190	243.8	255	265

Save

v2.4.2  
17:27:21  
11/10/2023

The tables shows the following information for each branch and allow current and voltage alarm thresholds settings:

For Current	For Voltage
<ul style="list-style-type: none"> <li>Branch</li> <li>Low warning (A)</li> <li>Current (A)</li> <li>High warning (A)</li> <li>High critical (A)</li> </ul>	<ul style="list-style-type: none"> <li>Branch</li> <li>Low critical (V)</li> <li>Low warning (V)</li> <li>Voltage (V)</li> <li>High warning (V)</li> <li>High critical (V)</li> </ul>

### 4.7.3.1 Set alarm threshold for individual branch

Change the setting in the table and then **Save**.

When a warning threshold is reached, an alarm will be sent with a warning level.

When a critical threshold is reached, an alarm will be sent with a critical level.

### 4.7.3.2 Set identical alarm threshold for a group of branches

Select the branches.

Press the **Edit settings** button.

Select the thresholds to be modified.

Set the thresholds values and then **Save**.

### 4.7.3.3 Access rights per profiles

	Administrator	Operator	Viewer
PDU settings - Branch thresholds	✓	✓	✗

4.7.3.3.1 For other access rights











For other access rights, see the [Information>>>Access rights per profiles](#) section.

4.7.4 Outlet thresholds

4.7.4.1 Title

Edit settings

<input type="checkbox"/>	Name	Low warning (A)	Current (A)	High warning (A)	High critical (A)	Energy (kWh)	Outlet state
<input checked="" type="checkbox"/>	 A1 - Outlet A1	0	0	1	2	-	Off
<input checked="" type="checkbox"/>	 A2 - Outlet A2	0	0	1	2	-	On
<input checked="" type="checkbox"/>	 A3 - Outlet A3	0	0	1	2	-	On
<input checked="" type="checkbox"/>	 A4 - Outlet A4	0	0	1	2	-	On
<input checked="" type="checkbox"/>	 A5 - Outlet A5	0	0	1	2	-	On
<input checked="" type="checkbox"/>	 A6 - Outlet A6	0	0	1	2	-	On
<input checked="" type="checkbox"/>	 A7 - Outlet A7	0	0	1	2	-	On
<input checked="" type="checkbox"/>	 A8 - Outlet A8	0	0	1	2	-	On

Save

The table shows the following information for each outlets and allow current alarm thresholds settings:

- Name
- Low warning (A)
- Current (A)
- High warning (A)
- High critical (A)
- Energy (kWh)
- Outlet state

4.7.4.1.1 Set alarm threshold for individual outlets

Change the setting in the table and then **Save**.

When a warning threshold is reached, an alarm will be sent with a warning level.

When a critical threshold is reached, an alarm will be sent with a critical level.

4.7.4.1.2 Set identical alarm threshold for a group of outlets

Select the outlets.

Press the **Edit settings** button.

## Measurement Settings



☐ Low warning

Amps

0

☐ High warning

Amps

0

☐ High critical

Amps

0

☐ Reset energy

kWh

0

EXIT

APPLY (8)

Select the thresholds to be modified.  
Set the thresholds values and then **Save**.

### 4.7.4.2 Access rights per profiles

	Administrator	Operator	Viewer
PDU settings - Outlet thresholds	✓	✓	✗









4.7.4.2.1 For other access rights



For other access rights, see the [Information>>>Access rights per profiles](#) section.

4.7.5 Outlet switching

Edit settings

<input type="checkbox"/>	ID	Name	State of startup	Startup delay	Reboot period	Control lock
<input checked="" type="checkbox"/>	A1	 Outlet A1	Last known state	1	5	Disable
<input checked="" type="checkbox"/>	A2	 Outlet A2	Last known state	1	10	Disable
<input checked="" type="checkbox"/>	A3	 Outlet A3	Last known state	1	10	Disable
<input checked="" type="checkbox"/>	A4	 Outlet A4	Last known state	1	10	Disable
<input checked="" type="checkbox"/>	A5	 Outlet A5	Last known state	1	10	Disable
<input checked="" type="checkbox"/>	A6	 Outlet A6	Last known state	1	10	Disable
<input checked="" type="checkbox"/>	A7	 Outlet A7	Last known state	1	10	Disable
<input checked="" type="checkbox"/>	A8	 Outlet A8	Last known state	1	10	Disable

The table shows the following information for each outlets and allow switching settings:

- ID
- Name
- State of startup
- Startup delay
- Reboot period
- Control lock

4.7.5.1 Set switching settings for individual outlets

Change the setting in the table and then **Save**.

4.7.5.2 Set identical switching settings for a group of outlets

Select the outlets.

Press the **Edit settings** button.



Switching Settings



☐ State on startup

State \*

☐ Startup delay

Seconds \*

☐ Reboot period

Seconds \*

☐ Lock outlet control

State \*

EXIT

APPLY (8)

Select the settings to be modified.  
Set the settings values and then **Save**.

4.7.5.3 Access rights per profiles

	Administrator	Operator	Viewer
PDU settings - Outlet switching	✓	✓	✗

4.7.5.3.1 For other access rights



For other access rights, see the [Information>>>Access rights per profiles](#) section.

# 4.7.6 Group definition

Delete

Create group

<input type="checkbox"/>	Group		Outlets				
<input type="checkbox"/>	Group 1		A1 0 mA	A2 0 mA	A3 0 mA	A7 0 mA	A8 0 mA
<input type="checkbox"/>	Group 2		A4 0 mA	A5 0 mA	A6 0 mA		
<input type="checkbox"/>	Group 3		A1 0 mA	A3 0 mA	A5 0 mA	A7 0 mA	

This page allows to create, edit and delete groups of outlets.

The table shows the list of the existing groups, with an overview on the outlets included in each group.

## 4.7.6.1 Create a group

After clicking on *Create* button, select the outlets you want to add, set a group name and click on *Create* in the bottom right hand corner.

## 4.7.6.2 Edit a group

Click on the pencil in the line of the group you want to edit.

## 4.7.6.3 Delete one or several groups

Select the groups using the checkboxes and click on *Delete*

## 4.7.6.4 Access rights per profiles

	Administrator	Operator	Viewer
PDU settings - Group definition			



### 4.7.6.4.1 For other access rights

For other access rights, see the [Information>>>Access rights per profiles](#) section.

# 4.8 Maintenance

## 4.8.1 Firmware

### 4.8.1.1 Update Network Card Firmware

Update Firmware						
 Upload						
Status	Version	Sha	Generated On	Installed On	Activated on	
Invalid	1.7.7	aa12be2	03/17/2020	03/17/2020	03/17/2020	
 Active	2.0.0	f8d1f71	03/18/2020	03/19/2020	03/19/2020	

- Monitors the information for the two-embedded firmware.
- Upgrade the Network Module firmware.

#### 4.8.1.1.1 Card Firmware information

##### a Status

- Uploading
- Invalid
- Valid
- Pending reboot
- Active

##### b Version/Sha

Displays the associated firmware version and associated Sha.

##### c Generated on

Displays the release date of the firmware.

For better performance, security, and optimized features, Eaton recommends to upgrade the Network Module regularly.

##### d Installation on

Displays when the firmware was installed in the Network Module.

##### e Activated on

Displays when the firmware was activated in the Network Module.

#### 4.8.1.1.2 Upgrade the Network Module firmware

During the upgrade process, the Network Module does not monitor the Device status.

To upgrade the firmware:

1. Download the latest firmware version from the website. For more information, see the [Servicing the Network Management Module>>>Accessing to the latest Network Module firmware/driver](#) section.
2. Click **+Upload**.
3. Click **Choose file** and select the firmware package by navigating to the folder where you saved the downloaded firmware.
4. Click **Upload**. The upload can take up to 5 minutes.

The firmware that was inactive will be erased by this operation.

When an upgrade is in progress, the upload button is disabled, and the progress elements appear below the table with the following steps:


Transferring > Verifying package > Flashing > Configuring system > Rebooting

A confirmation message displays when the firmware upload is successful, and the Network Module automatically restarts.

Network module is not reachable


X

Typical reasons: reboot, shutdown, IP address change, port change, certificate regeneration and network disconnect. Please wait for a while and refresh the browser. If problem persists, please contact your system administrator.



Do not close the web browser or interrupt the operation.  
Depending on your network configuration, the Network Module may restart with a different IP address.  
Refresh the browser after the Network module reboot time to get access to the login page.  
Press F5 or CTRL+F5 to empty the browser to get all the new features displayed on the Web user interface.  
Communication Lost and Communication recovered may appear in the [Contextual help>>>Alarms](#) section.

4.8.1.2 Update Device Firmware

UPDATE DEVICE FIRMWARE		
<div>Upload &amp; Activate</div>		
	Status	Version
	Active	01.13.8377
Eaton 95X 700i	Programming in progress	

- Upgrade Device Firmware linked to the card.

4.8.1.2.1 Device Firmware information

a Status

- Uploading
- Invalid
- Valid
- Pending reboot
- Active

b Version/Sha

Displays the associated firmware version and associated Sha.

4.8.1.2.2 Upgrade the Device firmware

During the upgrade process, loads are not protected. Any interruption to input power will result in an interruption of power to protected loads

To upgrade the device firmware:

1. Download the latest firmware version from the website. For more information, see the [Servicing the Network Management Module>>>Accessing to the latest Network Module firmware/driver](#) section.
2. Click on **Upload & Activate** button.
3. **Select a file** and pick the firmware package by navigating to the folder where you saved the downloaded firmware.

4. Click **Upload**. The upload can take up to 5 minutes.

The firmware that was inactive will be erased by this operation.

When an upgrade is in progress, the upload button is disabled, and the progress elements appear below the table with the following steps:

Entering bootloader > Erasing Memory > Programming in progress > Restarting to application mode

A confirmation message displays when the firmware upload is successful.

### 4.8.1.3 Access rights per profiles

	Administrator	Operator	Viewer
Firmware	✓	✗	✗

#### 4.8.1.3.1 For other access rights



For other access rights, see the [Information>>>Access rights per profiles](#) section.

### 4.8.1.4 CLI commands

#### get release info

##### Description

Displays certain basic information related to the firmware release.

##### Help

```
get_release_info
-d Get current release date
-s Get current release sha1
-t Get current release time
-v Get current release version number
```

#### 4.8.1.4.1 For other CLI commands



See the CLI commands in the [Information>>>CLI](#) section.

### 4.8.1.5 Troubleshooting

#### The Network Module fails to boot after upgrading the firmware

#### Possible Cause

- 1- The IP address has changed.
- 2- The Network module LED shows solid red after the upgrade.
- 3- The first boot after the upgrade takes a longer time.

**Note:** If the application is corrupt, due to an interruption while flashing the firmware for example, the boot will be done on previous firmware.

#### Action

- 1- Recover the IP address and connect to the card.
- 2- Reset the Network module by using the Restart button on the front panel.
- 3- Wait until the Network module LED shows flashing green.

Refer to [Installing the Network Management Module>>>Accessing the Network Module>>>Finding and setting the IP address](#) section.

### Web user interface is not up to date after a FW upgrade

#### Symptom

After an upgrade:

- The Web interface is not up to date
- New features of the new FW are not displayed
- An infinite spinner is displayed on a tile

#### Possible causes

The browser is displaying the Web interface through the cache that contains previous FW data.

#### Action

Empty the cache of your browser using F5 or CTRL+F5.

### 4.8.1.5.1 For other issues



For details on other issues, see the [Troubleshooting](#) section.

## 4.8.2 Sessions

### 4.8.2.1 Sessions

Username	Profile	Service	IP address	Interface	Connected since
admin ( Local )	Administrator	WEB	192.168.1.10	LAN	01/20/2023 10:10:51
Administrator ( Local )	Administrator	WEB	192.168.1.10	LAN	01/20/2023 10:11:09

- Monitors the information for the connected sessions
- End any session as an admin with a re-authentication

#### 4.8.2.1.1 Session information

##### a Username

This can be either a default profile name or a custom name

##### b Profile

Displays if the session belongs to an administrator, operator or viewer profile

##### c Service

Displays on which service the session is going on (Web, SSH, Serial , etc...)

##### d IP Address

Displays the IP address of the active session.

##### e Interface

Displays the type of connection (Web, LAN, etc...)

##### f Connected since

Displays the last opened session time

### 4.8.2.2 Access rights per profiles

	Administrator	Operator	Viewer
Firmware	✓	✗	✗

#### 4.8.2.2.1 For other access rights



For other access rights, see the [Information>>>Access rights per profiles](#) section.

## 4.8.3 Services

### 4.8.3.1 Service options

#### 4.8.3.1.1 Sanitization

Sanitization removes all the data; the Network Module will come back to factory default settings.

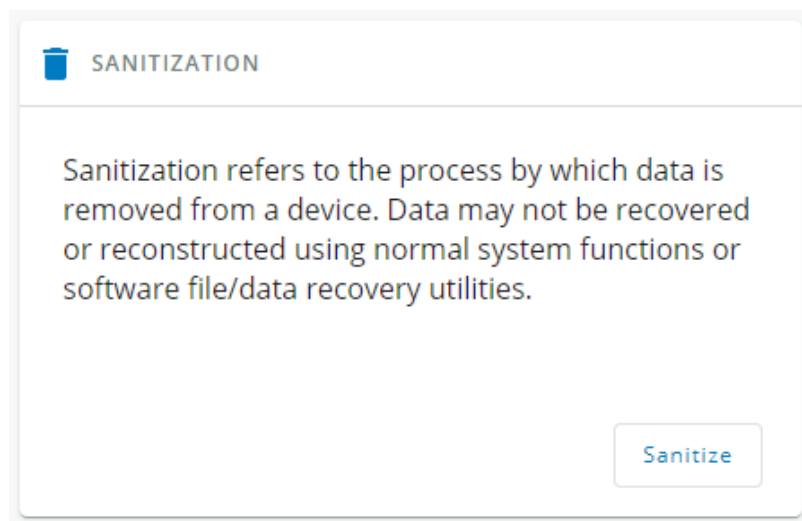


For details on default settings, see the [Information>>>Default settings parameters](#) section.

To sanitize the Network Module:

1. Click **Sanitize**.

A confirmation message displays, click **Sanitize** to confirm.



Depending on your network configuration, the Network Module may restart with a different IP address. Only main administrator user will remain with default login and password. Refresh the browser after the Network module reboot time to get access to the login page.

#### 4.8.3.1.2 Reboot

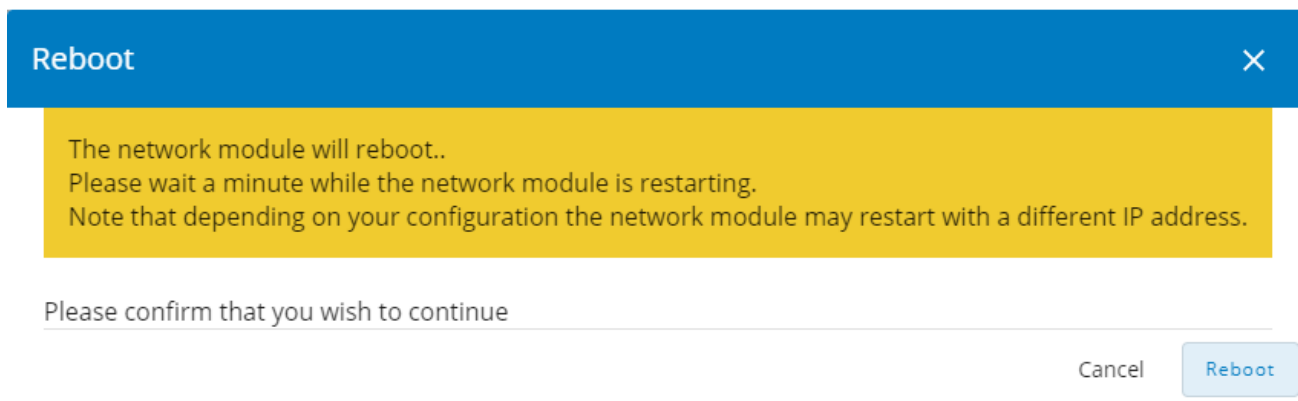
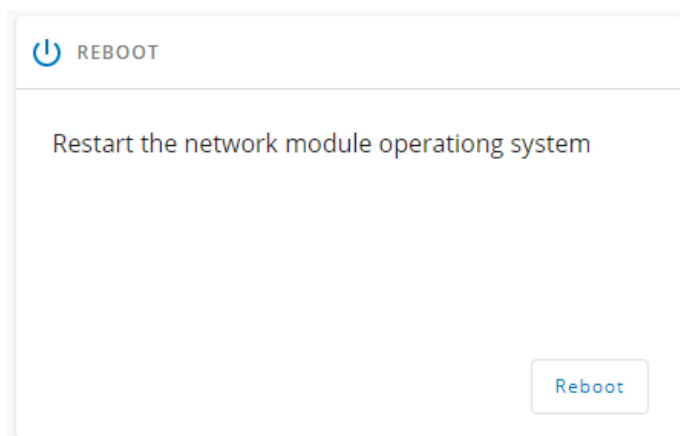
Reboot means restarting the network module operating system.

To reboot the Network Module:

- Click **Reboot**.

A confirmation message displays, click **Reboot** to confirm, the reboot time will take approximately less than 2min.





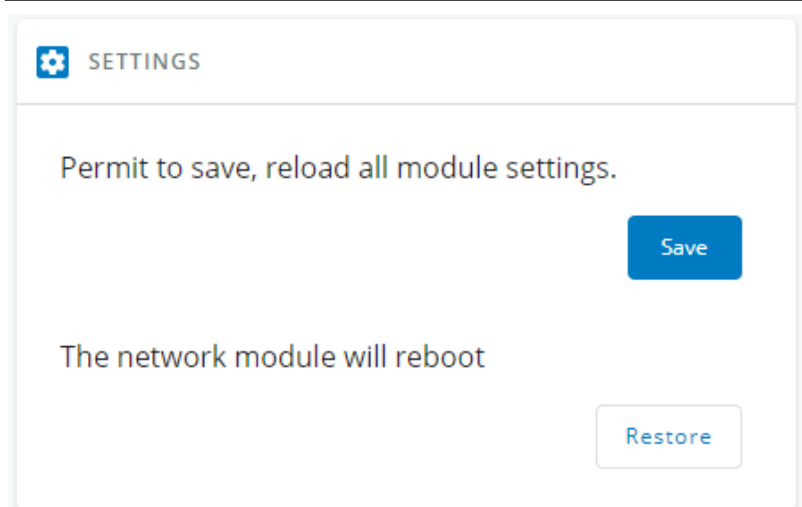
Depending on your network configuration, the Network Module may restart with a different IP address. Refresh the browser after the Network module reboot time to get access to the login page. Communication Lost and Communication recovered may appear in the Alarm section.

### 4.8.3.1.3 Settings

Allow to save and restore the Network module settings.



For more details, navigate to [Servicing the Network Management Module>>>Saving/Restoring/Duplicating](#) section.



#### 4.8.3.1.4 Save



Below settings are not saved:  
Local users other than the main administrator  
Sensor settings (commissioning, alarm configuration)

##### Save Settings



☐ Include Network

Passphrase is required to cipher the sensitive data \*

Confirm Passphrase \*

Cancel

Save

To save the Network module settings:

1. Click on **Save**
  2. Select to include the Network settings if needed.
- A passphrase need to be entered twice to cypher the sensitive data.
3. Click on **Save**

#### 4.8.3.1.5 Restore



Restoring settings may result in the Network module reboot.

##### Restore Settings



This action is not recoverable. The network module will reboot

☐ Include Network

Passphrase \*

No file chosen

Cancel

Restore

To restore the Network module settings:

1. Click on **Restore**
2. Select to include the Network settings if needed.
3. Enter the passphrase used when the file was saved.
4. Click on **Choose file** and select the JSON file

- 5. Click on **Restore** to confirm
- 6. For safety reason, **re-enter your own password** to confirm your identity

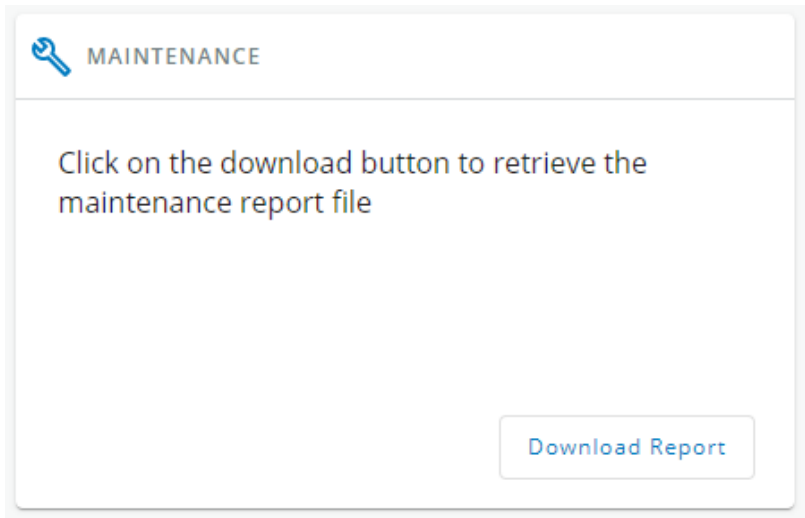
4.8.3.1.6 Maintenance

The maintenance report is for the service representative use to diagnose problems with the network module. It is not intended for the user, which is why the file is protected by a password.

To download the maintenance report file:

Click **Download report**.

A confirmation message displays, Maintenance report file successfully downloaded.



4.8.3.2 Access rights per profiles

	Administrator	Operator	Viewer
Services	✓	✗	✗

4.8.3.2.1 For other access rights

 For other access rights, see the [Information>>>Access rights per profiles](#) section.

4.8.3.3 CLI commands

maintenance
<div>Description</div> <div>Creates a maintenance report file which may be handed to the technical support.</div>

## Help

```

maintenance
  <cr> Create maintenance report file.
  -h, --help Display help page

```

## Examples of usage

Generate the maintenance report by running the "maintenance" command.

Then retrieve the report from the card using SCP

From a linux host:

```
sshpass -p $PASSWORD scp $USER@$CARD_ADDRESS:report.zip .
```

From a Windows host:

```
pscp -scp -pw $PASSWORD $USER@$CARD_ADDRESS:report.zip report.zip
```

(Require pscp tools from putty)

Where:

- \$USER is user name (the user shall have administrator profile)
- \$PASSWORD is the user password
- \$CARD\_ADDRESS is IP or hostname of the card

**reboot**

## Description

Tool to Reboot the card.

## Help

```

Usage: reboot [OPTION]
  <cr>                Reboot the card
  --help              Display help
  --withoutconfirmation Reboot the card without confirmation

```

**save\_configuration | restore\_configuration**

## Description

Save\_configuration and restore\_configuration are using JSON format to save and restore certain part of the configuration of the card.

## Help

```
save_configuration -h
save_configuration: print the card configuration in JSON format to standard output.
```

```
restore_configuration -h
restore_configuration: restore the card configuration from a JSON-formatted standard
input.
```

## Examples of usage

From a linux host:

**Save over SSH:** `sshpass -p $PASSWORD ssh $USER@$CARD_ADDRESS save_configuration -p $PASSPHRASE > $FILE`

**Restore over SSH:** `cat $FILE | sshpass -p $PASSWORD ssh $USER@$CARD_ADDRESS restore_configuration -p $PASSPHRASE`

From a Windows host:

**Save over SSH:** `plink $USER@$CARD_ADDRESS -pw $PASSWORD -batch save_configuration -p $PASSPHRASE > $FILE`

**Restore over SSH:** `type $FILE | plink $USER@$CARD_ADDRESS -pw $PASSWORD -batch restore_configuration -p $PASSPHRASE`

(Require plink tools from putty)

Where:

- \$USER is user name (the user shall have administrator profile)
- \$PASSWORD is the user password
- \$PASSPHRASE is any passphrase to encrypt/decrypt sensible data.
- \$CARD\_ADDRESS is IP or hostname of the card
- \$FILE is a path to the JSON file (on your host computer) where the configuration is saved or restored.

**sanitize**

## Description

Sanitize command to return card to factory reset configuration.

## Access

- Administrator

## Help

```
sanitize
-h, --help          Display help page
--withoutconfirmation Do factory reset of the card without confirmation
<cr>               Do factory reset of the card
```

### 4.8.3.3.1 For other CLI commands



See the CLI commands in the [Information>>>CLI](#) section.

## 4.8.4 Resources

Card resources is an overview of the Network Module processor, memory and storage information.

The **COPY TO CLIPBOARD** button will copy the information to your clipboard so that it can be past.

For example, you can copy and paste information into an email.

### 4.8.4.1 Processor

PROCESSOR	
Used	7.1 %
Up since	03/24/2020 15:32:38

- Used in %
- Up since date

### 4.8.4.2 Memory

MEMORY	
Total	245 MB
Available	155 MB
Application	90 MB
Temporary files	816 kB

- Total size in MB
- Available size in MB
- Application size in MB

- Temporary files size in MB

4.8.4.3 Storage

STORAGE	
Total	32 MB
Available	28 MB
Used	5 MB

- Total size in MB
- Available size in MB
- Used size in MB

4.8.4.4 Access rights per profiles

	Administrator	Operator	Viewer
Resources	✓	✓	✓

4.8.4.4.1 For other access rights

 For other access rights, see the [Information>>>Access rights per profiles](#) section.

4.8.4.5 CLI commands

systeminfo\_statistics

Description

Displays the following system information usage:

1. CPU

a. usage : %

b. upSince : date since the system started

2. Ram

a. total: MB

b. free: MB

c. used: MB

d. tmpfs: temporary files usage (MB)

3. Flash


- a. user data
  - i. total: MB
  - ii. free: MB
  - iii. used: MB

Help

`systeminfo_statistics`  
Display systeminfo statistics

`-h, --help` Display the help page.

4.8.4.5.1 For other CLI commands


 See the CLI commands in the [Information>>>CLI](#) section.

4.8.5 System logs





4.8.5.1 System logs


There are 4 types of logs available:

- Update
- Account
- Session
- System

Select the log files to download and press the download icon: 




SYSTEM LOGS

Log File name	
system-logs-update.csv	
system-logs-account.csv	
system-logs-session.csv	
system-logs-system.csv	

 For the list of system logs, see the [Information>>>System Logs codes](#) section.



## 4.8.5.2 Access rights per profiles

	Administrator	Operator	Viewer
System logs			

### 4.8.5.2.1 For other access rights



For other access rights, see the [Information>>>Access rights per profiles](#) section.

## 4.8.6 System information

System information is an overview of the main Network Module information.

The **COPY TO CLIPBOARD** button will copy the information to the clipboard.




### 4.8.6.1 Identification

- System name – if filled, it replaces the Device model name in the top bar
- Product
- Physical name
- Vendor
- UUID
- Part number
- Serial number
- Hardware version
- Location
- Contact
- MAC address

### 4.8.6.2 Firmware information

- Version
- SHA
- Build date
- Installation date
- Activation date
- Bootloader version

### 4.8.6.3 Access rights per profiles

	Administrator	Operator	Viewer
System information			

#### 4.8.6.3.1 For other access rights



For other access rights, see the [Information>>>Access rights per profiles](#) section.

## 4.9 Alarms

### 4.9.1 Alarm sorting

Alarms can be sorted by selecting:

- All
- Active only

### 4.9.2 Active alarm counter



Alarms with a severity set as Good are not taken into account into the counter of active alarms.

### 4.9.3 Alarm details

All alarms are displayed and sorted by date, with alert level, time, description, and status.

	Info/Warning/Critical logo	Alarm description text
Active	In color	In bold with "Active" label
Opened	In color	
Closed	Greyed	

### 4.9.4 Alarm paging

The number of alarms per page can be changed (10-15-25-50-100).

When the number of alarms is above the number of alarms per page, the buttons **First**, **Previous** and **Next** appears to allow navigation in the Alarm list.

### 4.9.5 Export

Press the **Export** button to download the file.

## 4.9.6 Clear

Clear alarms

×

Older than \*

03/22/2021 10:28:11

🕒 📅

Up to severity \*

Critical

▼

Cancel

Clear

Press the **Clear** button to clear alarms that are older than a specified date and up to a defined severity.

## 4.9.7 Alarms list with codes

To get access to the Alarm log codes or the System log codes for email subscription, see sections below:

- [System log codes](#)
- [PDU alarm log codes](#)
- [EMP alarm log codes](#)
- [Network module alarm log codes](#)

## 4.9.8 Access rights per profiles

	Administrator	Operator	Viewer
Alarm list	✓	✓	✓
Export	✓	✓	✓
Clear	✓	✓	✗

### 4.9.8.1 For other access rights



For other access rights, see the [Information>>>Access rights per profiles](#) section.

## 4.10 User profile

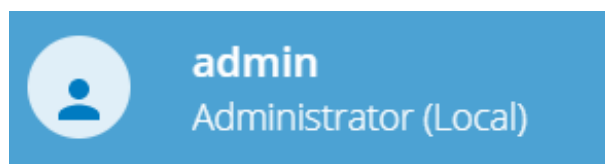
### 4.10.1 Access to the user profile

Press the icon on the top right side of the page to access the user profile window:



This page is in read-only mode when connected through LDAP and it displays the preferences applied to all LDAP users as configured in the [Contextual help>>>Settings>>>Remote users>>>LDAP](#) section.

### 4.10.2 User profile



Account settings



Change password



Log out



Legal information


This page displays the current username with its realm (local, remote) and allows to Change passwords, Edit account and Log out.

### 4.10.2.1 Account settings


Account Settings

Account Details


Full Name

 My name


Email

 myName@myCompany.com

Phone

 00 1 256 35 205

Organization

 My company

Preferences

Language

English

Date Format

d/m/Y

Time Format

24h

Temperature

Celsius

Save

If you have the administrator's rights, you can click on **Edit account** to edit user profile and update the following information:

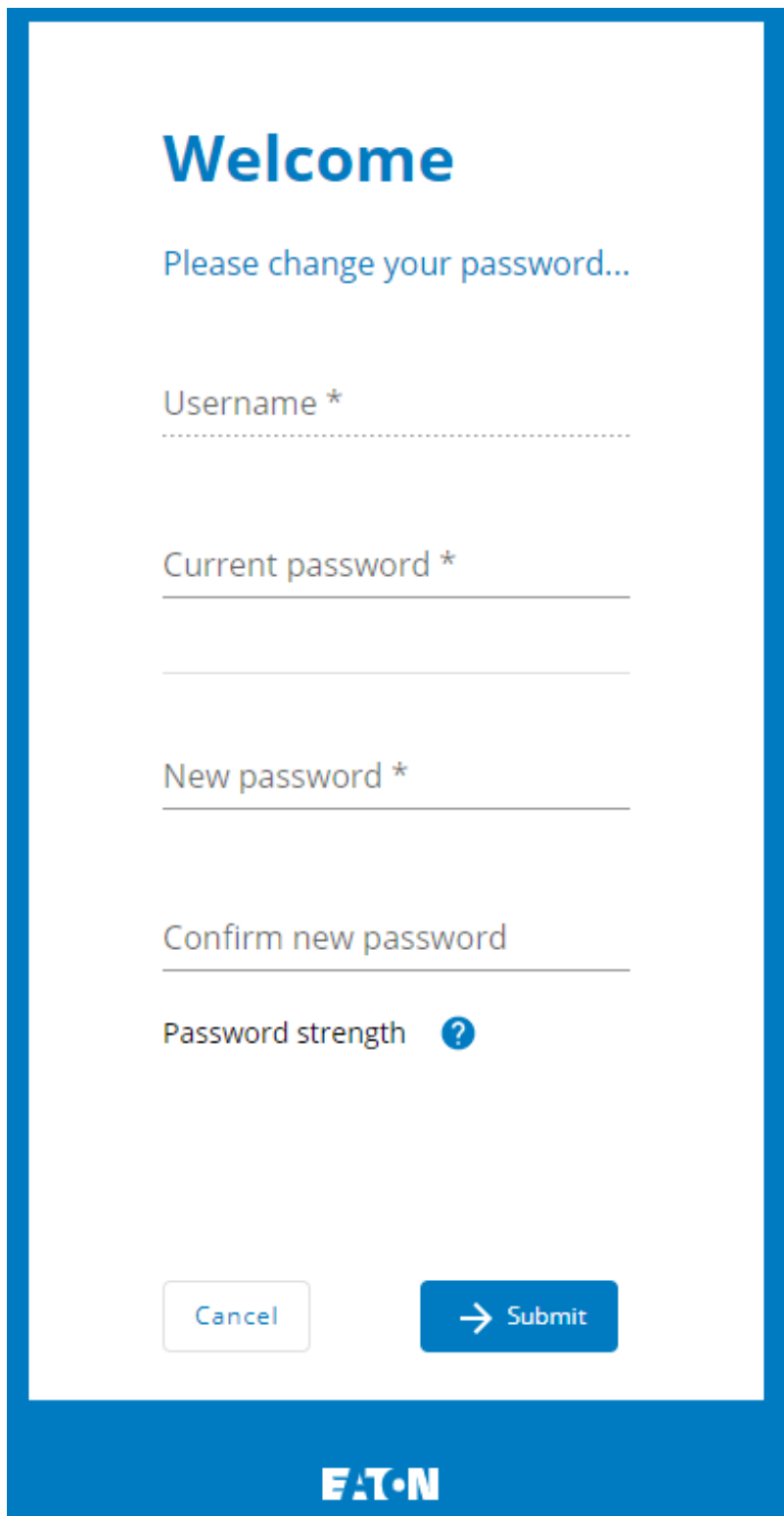
#### Account details

- Full name
- Email
- Phone
- Organization

#### Preferences

- Language
- Date format
- Time format
- Temperature

#### 4.10.2.2 Change password



The screenshot shows a web interface for changing a password. It features a blue header with the 'Welcome' text. Below the header, there is a prompt to change the password. The form includes four input fields: 'Username \*', 'Current password \*', 'New password \*', and 'Confirm new password'. A 'Password strength' indicator with a question mark icon is located below the input fields. At the bottom of the form, there are two buttons: 'Cancel' and 'Submit'. The Eaton logo is visible in the bottom right corner of the form area.

**Welcome**

Please change your password...

Username \*

Current password \*

New password \*

Confirm new password

Password strength ?

Cancel Submit

**EAT•N**

Click on **Change password** to change the password.



In some cases, it is not possible to change the password if it has already been changed within a day period. Refer to the troubleshooting section.

### 4.10.2.3 Log out

Click **Log out** to close the session.

## 4.10.3 Legal information

This Eaton network module includes software components, which are licensed under various open source licenses, or under a proprietary license.

Availability of source code

Notice for proprietary elements

Component	
...	...
...	...

This Network Module includes software components that are either licensed under various open source license, or under a proprietary license.

### 4.10.4 Component

All the open source components included in the Network Module are listed with their licenses.

### 4.10.5 Availability of source code

Provides the way to obtain the source code of open source components that are made available by their licensors.

Availability of source code

The source code of open source components which are made available by their licensors (including Eaton where applicable) may be obtained upon written express request by contacting: [network-m2-opensource@Eaton.com](mailto:network-m2-opensource@Eaton.com)

Eaton reserves the right to charge minimal administrative costs, in compliance with the terms of the underlying open source licenses, when necessary.

### 4.10.6 Notice for proprietary elements

Provides notice for our proprietary (i.e. non-Open source) elements.

## Notice for proprietary elements



Copyright © 2019 Eaton. This software is confidential and licensed under Eaton Proprietary License or End User License Agreement (EPL or EULA).  
 This software is not authorized to be used, duplicated or disclosed to anyone without the prior written permission of Eaton.  
 Limitations, restrictions and exclusions of the Eaton applicable standard terms and conditions, such as its EPL and EULA, apply.  
 The full text of the Eaton EULA is included hereafter:

Legal Information

The Eaton 93PM100 Network Card and Eaton Industrial Gateway Card include software components, which are licensed under various open source licenses, or under a proprietary license.

For more detailed information, please refer to the Legal Information link from the main user interface.

## 4.10.7 Default settings and possible parameters - User profile

	Default setting	Possible parameters
Profile	<p>Account details:</p> <ul style="list-style-type: none"> <li>Full name — Administrator</li> <li>Email — blank</li> <li>Phone — blank</li> <li>Organization — blank</li> </ul> <p>Preferences:</p> <ul style="list-style-type: none"> <li>Language — English</li> <li>Date format — MM-DD-YYYY</li> <li>Time format — hh:mm:ss (24h)</li> <li>Temperature — °C (Celsius)</li> </ul>	<p>Account details:</p> <ul style="list-style-type: none"> <li>Full name — 128 characters maximum</li> <li>Email — 128 characters maximum</li> <li>Phone — 64 characters maximum</li> <li>Organization — 128 characters maximum</li> </ul> <p>Preferences:</p> <ul style="list-style-type: none"> <li>Language — English, French, German, Italian, Japanese, Russian, Simplified Chinese, Spanish, Traditional Chinese</li> <li>Date format — MM-DD-YYYY / YYYY-MM-DD / DD-MM-YYY / DD.MM.YYY / DD/MM/YYY / DD MM YYYY</li> <li>Time format — hh:mm:ss (24h) / hh:mm:ss (12h)</li> <li>Temperature — °C (Celsius)/°F (Fahrenheit)</li> </ul>

### 4.10.7.1 For other settings



For other settings, see the [Information>>>Default settings parameters](#) section.

## 4.10.8 Access rights per profiles

	Administrator	Operator	Viewer
User profile	✓	✓	✓
Legal information	✓	✓	✓



### 4.10.8.1 For other access rights



For other access rights, see the [Information>>>Access rights per profiles](#) section.

## 4.10.9 CLI commands

### logout

#### Description

Logout the current user.

#### Help

```
logout  
<cr> logout the user
```

### whoami

#### Description

whoami displays current user information:

- Username
- Profile
- Realm

### 4.10.9.1 For other CLI commands



See the CLI commands in the [Information>>>CLI](#) section.

## 4.10.10 Troubleshooting

### Password change in My profile is not working

#### Symptoms

The password change shows "*Invalid credentials*" when I try to change my password in My profile menu:



### Possible cause

The password has already been changed once within a day period.

### Action

Let one day between your last password change and retry.

## 4.10.10.1 For other issues



For details on other issues, see the [Troubleshooting](#) section.

## 4.10.11 Save and Restore

	SRR section	Settings	Possible values
Account details	vCard	fullName	String: refer to default settings an possible parameters for constraints.
		email	String: refer to default settings an possible parameters for constraints.
		phone	String: refer to default settings an possible parameters for constraints.
		organization	String: refer to default settings an possible parameters for constraints.
Preferences	preferences	notifyByMail	true/false
		licenseAgreed	true/false
		language	de: Deutsch en: English es: Español fr: Français it: Italiano ja: 日本語 ru: русский zh_Hans: 简体中文 zh_Hant: 繁體中文

	dateFormat	Y-m-d: YYYY-MM-DD d-m-Y: DD-MM-YYYY d.m.Y: DD.MM.YYYY d/m/Y: DD/MM/YYYY m/d/Y: MM/DD/YYYY d m Y: DD MM YYYY
	timeFormat	1: 24h 0: 12h
	temperatureUnit	1: °C 2: °F

#### 4.10.11.1 Additional information



For details on Save and Restore, see the [Save and Restore](#) section.

## 4.11 Documentation

### 4.11.1 Access to the embedded documentation



Press the ? icon on the top right side of the page to access the documentation in a new window:

The focus will be made on the contextual page.

You can then navigate into below sections:







<b>Installing the Network Management Module</b>	How to install and access the Network module.
<b>LCD interface operation</b>	Information on the LCD interface and how to use it.
<b>Contextual help of the web interface</b>	Help for each webpage. Extracts from the sections below when they are related to the web page.
<b>Servicing the Network Management Module</b>	How to install and use the Network module.
<b>Securing the Network Management Module</b>	How to secure the Network module.
<b>Servicing the EMP</b>	Information on the EMP, how to install and use it.
<b>Information</b>	General information of the Network Module and Devices.
<b>Troubleshooting</b>	How to troubleshoot the Network Module.





Search feature is indexed.

4.11.2 Access rights per profiles

	Administrator	Operator	Viewer
Contextual help			
Full documentation			

4.11.2.1 For other access rights



For other access rights, see the [Information>>>Access rights per profiles](#) section.

## 5 Servicing the Network Management Module

### 5.1 Configuring/Commissioning/Testing LDAP

#### 5.1.1 Commissioning

Refer to the section [Contextual help>>>Settings>>>Remote users>>>LDAP](#) to get help on the configuration.

##### 5.1.1.1 Configuring connection to LDAP database

This step configures the LDAP client of the network module to request data from an LDAP base.

1. Activate LDAP.
2. Define security parameters according to LDAP servers' requirements.
3. Configure primary server (and optionally a secondary one).
4. If security configuration needs server certificate verification, import your LDAP server certificate.  
Refer to the section [Importing certificates](#) to get help on certificate import.
  - a. In case LDAP server certificate is self-signed, import the self-signed certificate in the *Trusted remote certificate* list **for LDAP service**.
  - b. in case LDAP server certificate has been signed by a CA, import the corresponding CA in the *Certificate authorities (CA)* list **for LDAP service**.
5. Configure credentials to bind with the LDAP server or select *anonymous* if no credentials are required.
6. Configure the *Search base DN*.
7. Configure the request parameters (see examples below).

##### 5.1.1.1.1 Typical request parameters

Parameter	OpenLDAP	Active Directory™ with POSIX account activated	Active Directory™
User base DN	ou=users, dc=example, dc=com	ou=users, dc=example, dc=com	ou=users, dc=example, dc=com
User name attribute	uid	uid	sAMAccountName
Group base DN	ou=groups, dc=example, dc=com	ou=groups, dc=example, dc=com	ou=groups, dc=example, dc=com
Group name attribute	gid	gid	sAMAccountName

##### 5.1.1.2 Map remote users to profile



This step is mandatory and configures the Network module to give permissions to the LDAP users. Users not belonging to a group mapped on a profile will be rejected.

Configure the rules to mapped LDAP users to profile:

1. Enter LDAP group name.
2. Select the profile to assigned.

You can define up to 20 mapping rules.

All LDAP users belonging to the configured LDAP group will have permissions granted by the associated profile.



If a user belongs to multiple LDAP groups mapped to different profiles, the behavior is undefined.

### 5.1.1.3 Define LDAP user's preferences

This step configures the user's preferences to apply to **all** LDAP users.

## 5.1.2 Testing LDAP connection

1. Click on Test icon right to Status column
2. Enter the User credentials then click on Test.
3. This test will verify all the parameters from the connection to the Database to the user credentials.
4. In case of error, the test displays where the issue is located.

## 5.1.3 Limitations

- If the same username exists in both local and LDAP databases, the behavior is undefined.
- If a user belongs to multiple LDAP groups mapped to different profiles, the behavior is undefined.
- No client certificate provided. It is not possible for the server to verify the client authenticity.
- It is not possible to configure LDAP to work with 2 different search bases.
- LDAP user's preferences are common to all LDAP users.
- LDAP users cannot change their password through the Network Module.
- The remote groupname entered in profile mapping settings must be composed only of alphanumeric, underscore and hyphen characters (but this last one can't be at the beginning).

## 5.2 Checking the current firmware version of the Network Module

Current firmware of the Network Module can be accessed in :

- The Top bar: Firmware version: x.xx.x
- The Card menu : [Contextual help>>>Maintenance>>>System information>>>Firmware information](#): Version x.xx.x
- The Card menu : [Contextual help>>>Maintenance>>>Firmware](#): Active FW version x.xx.x

## 5.3 Accessing to the latest Network Module firmware/driver/script

Download the latest Network Module firmware, driver or script from the Eaton website [www.eaton.com/downloads](http://www.eaton.com/downloads)

## 5.4 Upgrading the card firmware (Web interface / shell script)



For instructions on accessing to the latest firmware and script, refer to: [Accessing to the latest firmware and script](#)

### 5.4.1 Web interface

To upgrade the Network module through the Web interface, refer to the section: [Firmware upgrade through the Web interface](#).

### 5.4.2 Shell script

#### 5.4.2.1 Prerequisite

Shell script uses the following tools: sshpass, scp.

To get it installed on your Linux host, use the following commands.

**Debian/Ubuntu**

```
$ sudo apt-get install sshpass scp
```

**RedHat/Fedora/CentOS**

```
$ sudo dnf install sshpass scp
```

Make shell script executable:

```
$ chmod 700 install_updatePackage.sh
```

### 5.4.2.2 Procedure

To upgrade the Network module using:

1. Open a shell terminal on your computer (Linux or cygwin; meaning real or emulated Linux operating system).
2. Use the shell script *install\_updatePackage.sh*

```
Usage: 'install_updatePackage.sh' [options]
Upgrade tool
Mandatory arguments are -f, -i, -u and -p
-h : show help
-f <path> : path of the upgrade file
-u <username> : username of a card user allowed to start upgrade
-p <password> : user password
-i <ipaddress> : ip address of the card to upgrade
-r : reboot the card after upgrade
```

### 5.4.3 Example:

```
$ ./install_updatePackage.sh -u admin -p <mypassword> -f FW_Update.tar -i <cardIpAddress> -r
```

```
STARTING UPDATE FROM: [FW_Update.tar] to [X.X.X.X]
```

```
Transfer by scp (FW_Update.tar) to [X.X.X.X]
```

```
Warning: Permanently added 'X.X.X.X' (ECDSA) to the list of known hosts.
```

```
Transfer done.
```

```
Check running upgrade status ...
```

```
Check firmware binary signature
```

```
Uncompress and flash upgrade - inProgress():11
```

```
Uncompress and flash upgrade - inProgress():28
```

```
Uncompress and flash upgrade - inProgress():44
```

```
Uncompress and flash upgrade - inProgress():61
```

```
Uncompress and flash upgrade - inProgress():78
```

```
Uncompress and flash upgrade - inProgress():92
```

```
Uncompress and flash upgrade - inProgress():100
```

```
Uncompress and flash upgrade - inProgress():100
```

```
Uncompress and flash upgrade
```

```
Executing post_post_upgrade.sh script upgrade
```

```
Upgrade done
```

```
Warning: Permanently added 'X.X.X.X' (ECDSA) to the list of known hosts.
```

```
Rebooting...
res: Y
Update: OK
```

## 5.5 Updating the time of the Network Module precisely and permanently (ntp server)

For an accurate and quick update of the RTC for the Network Module, we recommend implementing a NTP server as time source for the Network Module.

LANs have an internal NTP server (Domain Controller, mail servers, Outlook servers are generally time servers too) but you can use a public ntp server like pool.ntp.org (after addition of the related rules to your firewall system).

For more information, see the [Contextual help>>>Settings>>>General>>>System details>>>Time & date settings](#) section.

## 5.6 Changing the language of the web pages

Update the language of the web page in the Settings menu.


1. Navigate to [Contextual help>>>User profile>>>Edit account](#).
2. Select the language, and then press the **Save** button.



The language of the login page is English by default or browser language when it is supported.

## 5.7 Resetting username and password

### 5.7.1 As an admin for other users

1. Navigate to [Contextual help>>>Settings>>>Local users](#).
2. Press the pen icon to edit user information: 
3. Change username and **save** the changes.
4. Select **Reset password** and choose from the following options :
  - Generate randomly
  - Enter manually
  - Force password to be changed on next login
5. Enter your own password to confirm the changes.
6. **Save** the changes.

### 5.7.2 Resetting its own password

1. Navigate to [Contextual help>>>User profile](#).
2. Press [Change password](#)
3. Enter your current password, the new password twice.
4. Press **Submit** to save the changes.

## 5.8 Recovering main administrator password

To recover the main administrator password, ask another administrator to initialize the password.



If it is not possible, proceed to the card sanitization:



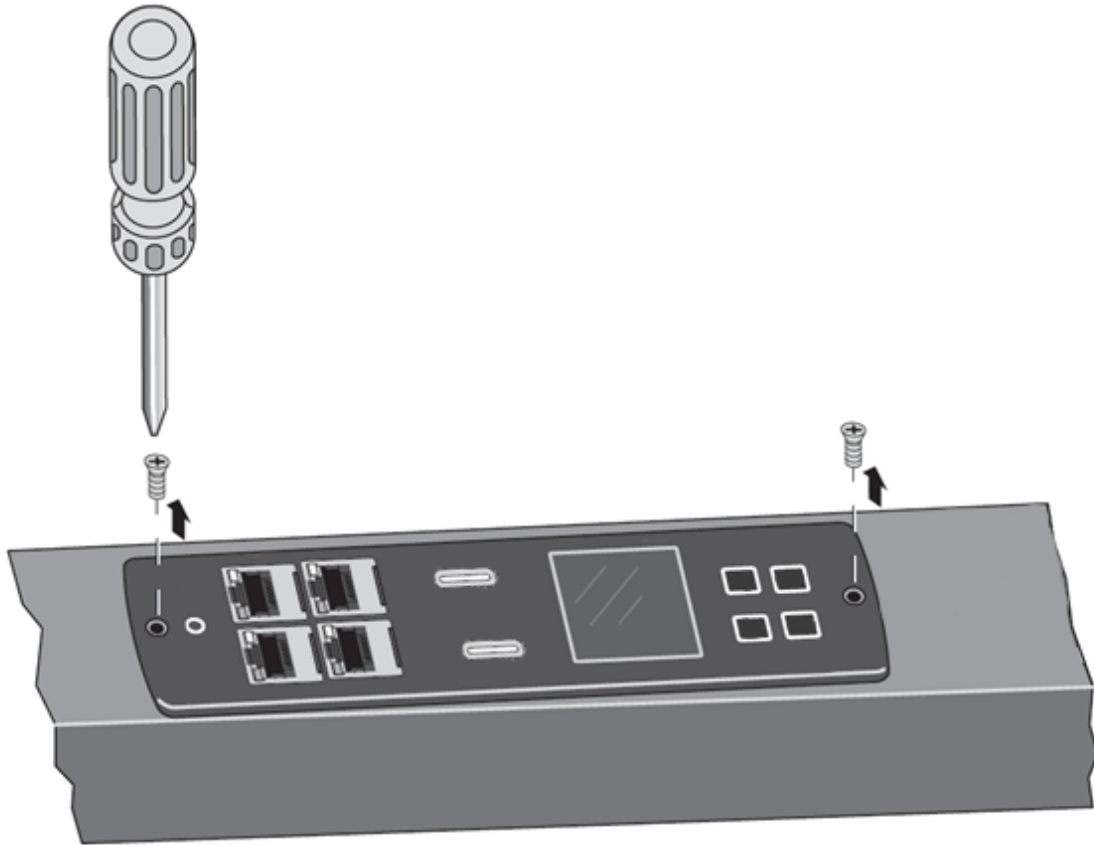
**Below instruction will sanitize the card and blank all the data.**

Depending on your network configuration, the Network Module may restart with a different IP address.

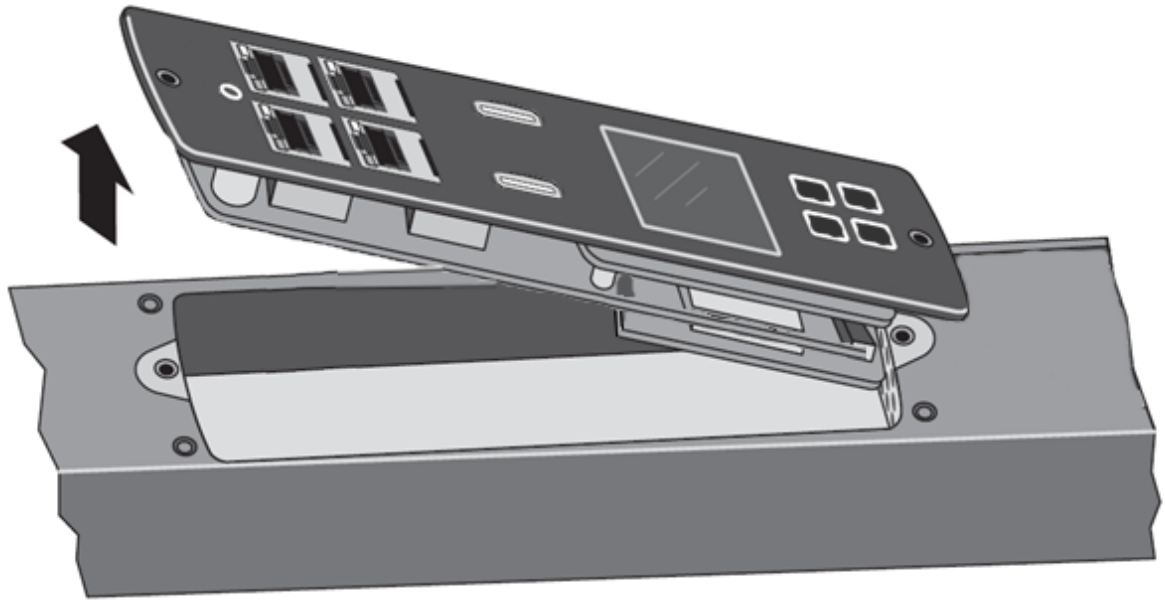
Only main administrator user will remain with default login and password.

Refresh the browser after the Network module reboot time to get access to the login page.

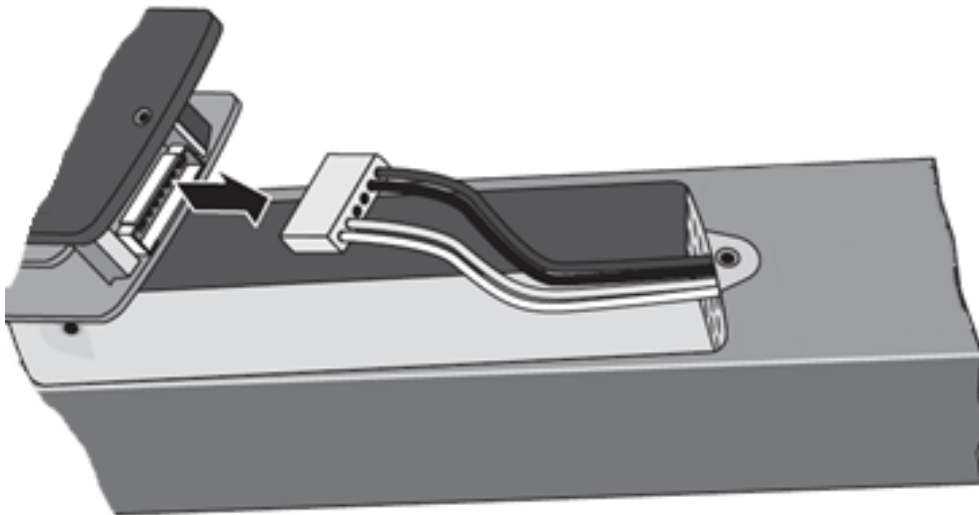
1. Access the Network Module, disconnect the Network cable, if needed.
2. Remove the two GNM mounting screws.



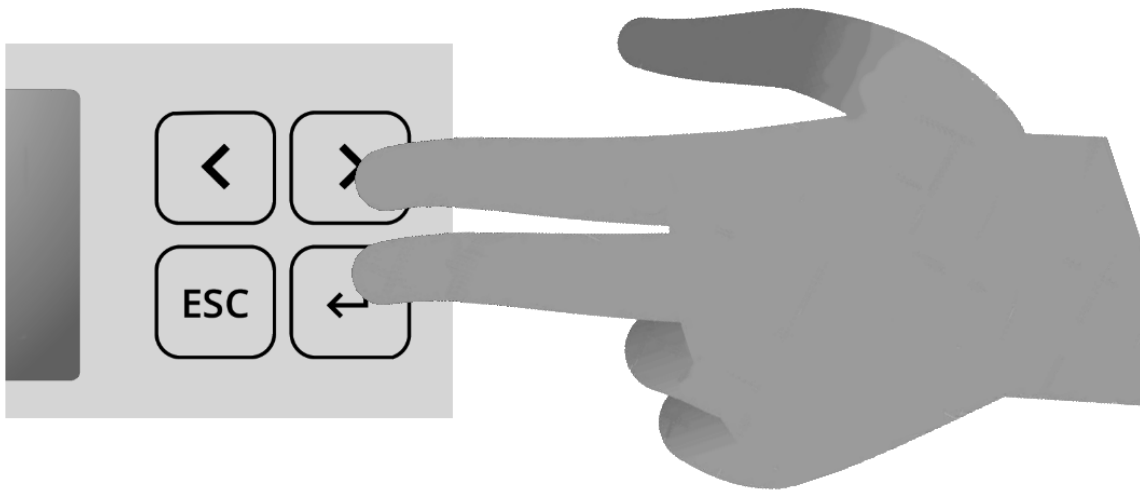
3. Tilt up one side of the GNM and locate the attached cable harness.



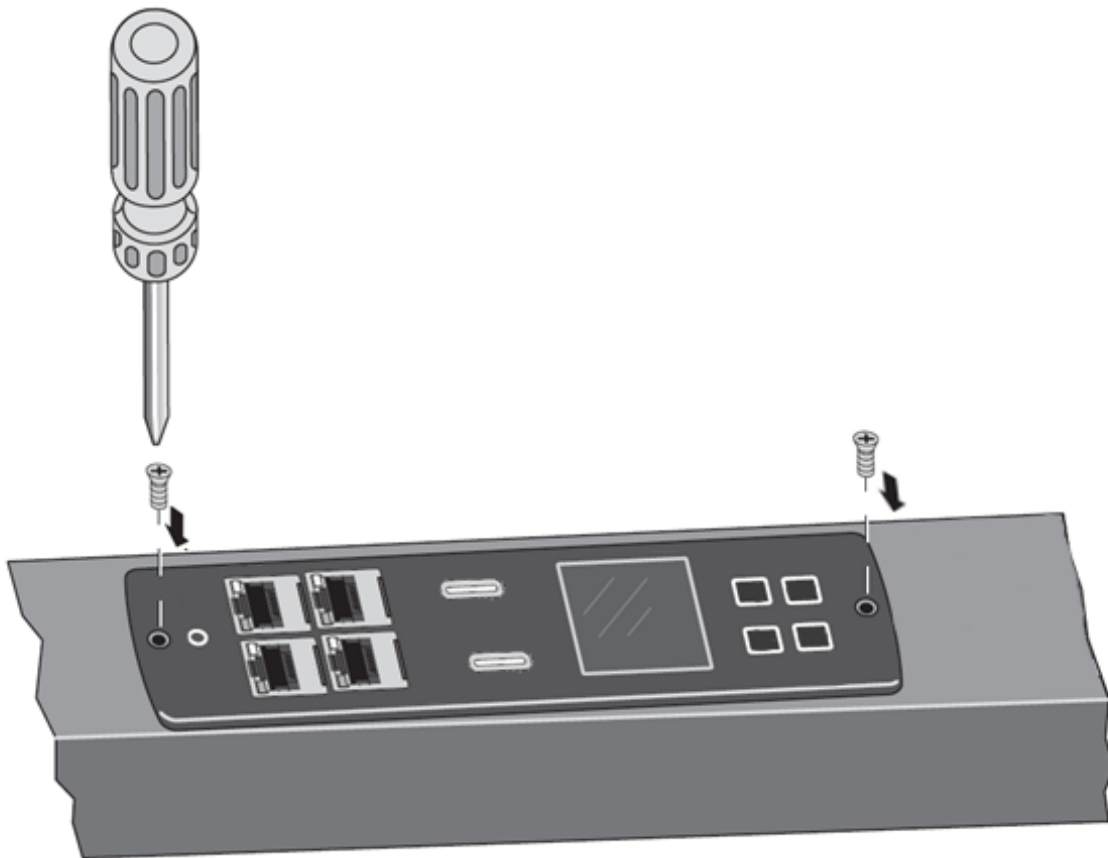
4. Disconnect the cable harness and remove the GNM.



5. Plug the cable back and hold Enter + Right Arrow buttons until seeing "System is booting" screen.



6. Put back the two GNM mounting screws.



7. Connect the Network Module by using the default credentials of the main administrator : admin/admin.
8. You will be forced to change the password accordingly to the current password strength rules.

## 5.9 Switching to static IP (Manual) / Changing IP address of the Network Module

Administrators can switch to static IP in the Settings menu and change the IP address of the Network Module.

1. Navigate to Contextual help>>>Settings>>>Network & Protocol>>>IPv4.
2. Select Manual (Static IP).

3. Input the following information:
  - IPv4 Address
  - Subnet Mask
  - Default Gateway
4. Save the changes.

## 5.10 Subscribing to a set of alarms for email notification

### 5.10.1 Example #1: subscribing only to one alarm (load unprotected)

Follow the steps below:

1. Navigate to [Contextual help>>>Settings>>>General>>>Email notification settings](#).
2. Press the button **New** to create a new configuration.
3. Select:
  - Active: Yes
  - Configuration name: Load unprotected notification
  - Email address: myaddress@mycompany.com
  - Notify on events: Active
  - Always notify events with code: 81E (Load unprotected)

### Edit email notification settings

Custom name \*

Load unprotected notification

Email address \*

myaddress@mycompany.com

Status

Active

Schedule report

Recurrence \*

Every day

Starting date

09/21/2019 16:56:00

Subscribe

Attach measures

Attach logs

☒

☒

Card Events

☒

☐

☒

Device events

Alarm notifications

Subscribe

Attach measures

Attach logs

☐

☐

All card Events

☐

☐

☐

All device events

List of event codes

Always notify events with code

81E

Separate each code with a comma

Never notify events with code

Separate each code with a comma

Test

Save



Logs will be attached by default in that example even if there is no subscription on card or device events.

4. Press **Save**, the table will show the new configuration.

EMAIL NOTIFICATION SETTINGS			
<div> <div>New</div> <div>Delete</div> </div>			
Custom name ↑	Email	Notification updates	Status
<div> <div></div> <div>Load unprotected notification</div> </div>	myaddress@mycompany.com	<div> <div>Alarms</div> </div>	<div> <div>Active</div> </div>

## 5.10.2 Example #2: subscribing to all Critical alarms and some specific Warnings

Follow the steps below:

1. Navigate to [Contextual help>>>Settings>>>General>>>Email notification settings](#).
2. Press the button **New** to create a new configuration.
3. Select:
  - Active: Yes
  - Configuration name: ALL Critical and User account Warning notification
  - Email address: myaddress@mycompany.com
  - Notify on events: Active
  - Subscribe to Critical card events and Critical device events
  - Always notify events with code: 0800700, 0800900 (User account - password expired, User account- locked)

Edit email notification settings

×

Custom name \*

All critical and User account Warning notification

Email address \*

myaddress@mycompany.com

Status

Active

Schedule report

Recurrence \*

Every day

Starting date

09/21/2019 16:56:00

Subscribe

Attach measures

Attach logs

Card Events

Device events

Alarm notifications

Subscribe

Attach measures

Attach logs

All card Events

Critical alarm

Warning alarm

Info alarm

All device events

Critical alarm

Warning alarm

Info alarm

Always notify events with code

0800700,0800900

Never notify events with code

Test

Save

4. Press **Save**, the table will show the new configuration.

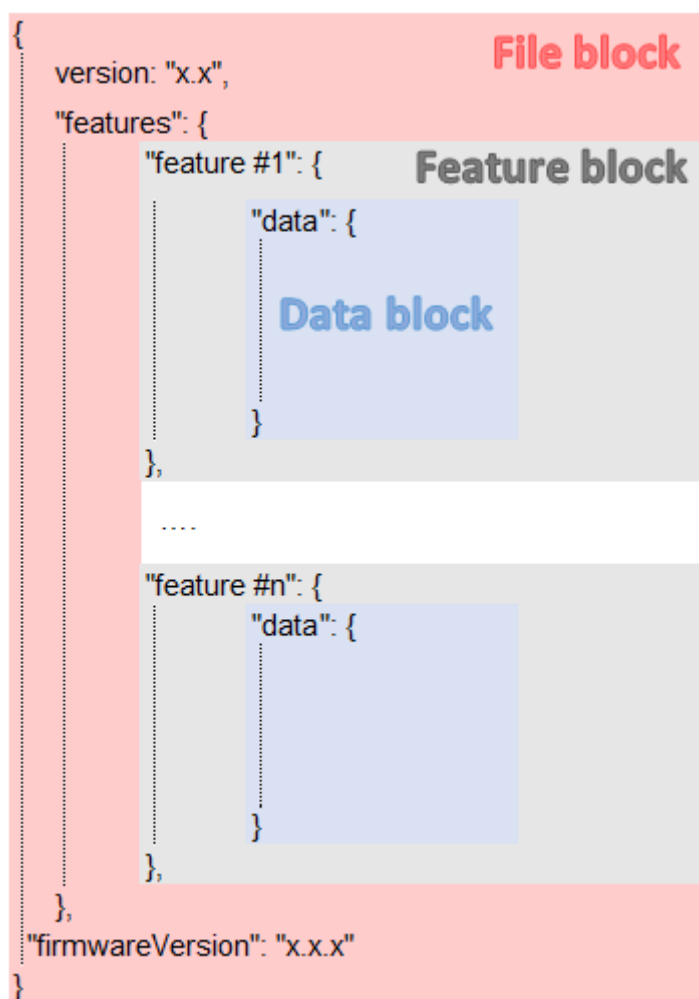
EMAIL NOTIFICATION SETTINGS				
<div> <div>+ New</div> <div>Delete</div> </div>				
Custom name ↑	Email	Notification updates	Status	
<input type="checkbox"/> All critical and User account Warning notification	myaddress@mycompany.com	Alarms	Active	

## 5.11 Saving/Restoring/Duplicating Network module configuration settings

### 5.11.1 Modifying the JSON configuration settings file

#### 5.11.1.1 JSON file structure

The JSON file is structured into 3 blocks:



### 5.11.1.1.1 File block

File block cannot be modified, this is the mandatory structure of the JSON file.

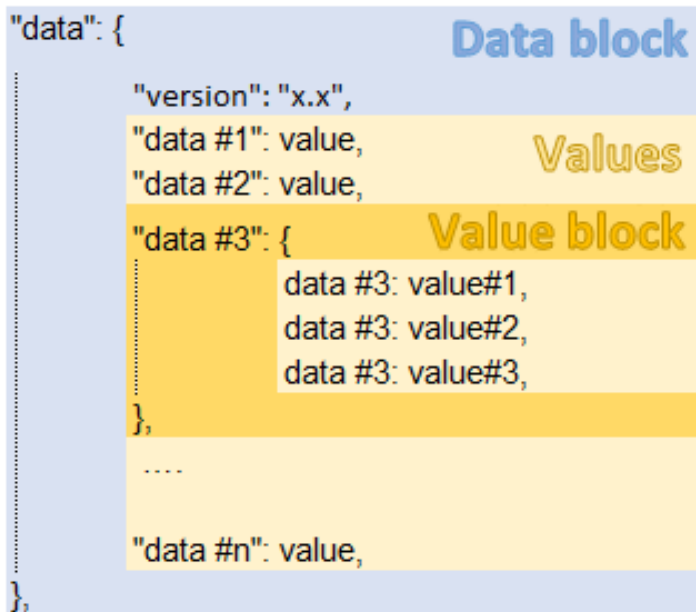
### 5.11.1.1.2 Feature block

Feature block contains the full definition of a feature.

If it is removed from the JSON file, this feature settings will not be updated/restored in the card.

### 5.11.1.1.3 Data block

Data block contains all the feature settings values.



#### a Data block

Data block cannot be modified, this is the mandatory structure of the JSON file.

#### b Value block

If some values inside the Value block need to be kept, Value block structure cannot be modified, this is the mandatory structure of the JSON file.

If it is removed from the JSON file, these values will not be updated/restored.

#### c Values

Values can be kept as is, modified or removed.

Removed values will not be updated/restored.

## 5.11.1.2 Sensitive data (like passwords)

JSON file structure will slightly varies if sensitive data are exported with passphrase or not.

### 5.11.1.2.1 The JSON file is saved using passphrase (preferred)

All sensitive data will have below structure:

```
"password": {
  plaintext: "null",
  cyphered: "p-twlcjoV-a8FjMjkagL6w"
},
```



When restoring the file, the corresponding setting will be updated based on the cyphered value.

5.11.1.2.2 The JSON file is saved without passphrase

All sensitive data will have below structure:

```
"password": {
  plaintext: "null",
},
```



When restoring the file, the corresponding setting will not be set.  
This may lead to restoration failure if corresponding setting was not previously set with a valid value.

5.11.1.3 Modifying JSON file examples

5.11.1.3.1 Modifying sensitive data

To change sensitive data, plain text must be filled with the new value and the Cyphered entry (if existing) must be removed:

```
"password": {
  plaintext: "New password",
},
```

5.11.1.3.2 Adding local users

Adding or modifying local users is not yet available, only the predefined account (main administrator) can be modified.

5.11.1.3.3 Modifying SNMP settings

Original file:	Modified file:
SNMP disabled	SNMP enabled on port 161 SNMPv1 disabled SNMPv3 enabled 2 x accounts 1 x read only user (enabled) with Auth-Priv security level and passwords 1x read write user (enabled) with Auth-Priv security level and passwords 1 x active trap



Original file:	Modified file:
<pre>snmp: {   data: {     version: "x.x",     dmeData: {       enabled: false,       port: xxxx,       v1: {         enabled: false,         communities: {           .....         }       },       v3: {         enabled: false,         users: [           .....         ]       },       traps: {         receivers: [         ]       }     }   } },</pre>	<pre>snmp: {   data: {     version: "x.x",     dmeData: {       enabled: true,       port: 161,       v1: {         enabled: false,         communities: {           .....         }       },       v3: {         enabled: true,         users: [           {             name: "readonly",             allowWrite: false,             enabled: true,             auth: {               enabled: true,               password: {                 plaintext: xxxxxxxxxxxxxx               }             },             priv: {               enabled: true,               password: {                 plaintext: yyyyyyyyyyyyyyy               }             }           },           {             name: "readwrite",             allowWrite: true,             enabled: true,             auth: {               enabled: true,               password: {                 plaintext: zzzzzzzzzzzzzzzzzz               }             },             priv: {               enabled: true,               password: {                 plaintext: wwwwwwwwww               }             }           }         ]       },       traps: {         receivers: [           {             name: "xxxxxxx",             host: "xxx.xx.xxx.xx",             port: xxx,             community: "xxxxx",             protocol: x,             user: "",             enabled: xxxx           }         ]       }     }   } },</pre>

5.11.1.3.4 Making a partial update/restoration

a Example: Updating/Restoring only LDAP settings

If you restore below JSON content, only LDAP settings will be updated/restored, everything else will remain unchanged.

```
{
  "version": "x.x",
  "features": {
```

```

    "ldap": {
      "data": {
        "version": "x.x",
        "certificateData": [],
        "dmeData": {
          "enabled": true,
          "baseAccess": {
            "security": {"ssl": 1, "verifyTlsCert": false},
            "primary": {"name": "Primary", "hostname": "xxxxxxxx", "port": xxxx},
            "secondary": {"name": "xxxxxx", "hostname": "xxxxxx", "port": xxxx},
            "credentials": {
              "anonymousSearchBind": false,
              "searchUserDN":
                "CN=xxxx,OU=xxxx,OU=xxxx,OU=xxxx,DC=xxxx,DC=xxxx",
              "password": {"plaintext": null}},
            "searchBase": {"searchBaseDN": "DC=xxx,DC=xxx,DC=xxx"}
          },
          "requestParameters": {
            "userBaseDN": "OU=xxxx,DC=xxxx",
            "userNameAttribute": "xxxx",
            "uidAttribute": "objectSid:x-x-x-xx-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx",
            "groupBaseDN": "OU=xxxx,DC=xxxx",
            "groupNameAttribute": "xx",
            "gidAttribute": "objectSid:x-x-x-xx-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx"
          },
          "profileMapping": [
            { "remoteGroup": "xxxxxxxxxxxxxxxx", "profile": 1},
            { "remoteGroup": "xxxxxxxxxxxxxxxx", "profile": 2},
            { "remoteGroup": "", "profile": 0},
            { "remoteGroup": "", "profile": 0},
            { "remoteGroup": "", "profile": 0}
          ]
        }
      },
    },
    "firmwareVersion": "x.x.x"
  }
}

```

### 5.11.2 Saving/Restoring/Duplicating settings through the CLI

Navigate to [Information>>>CLI>>>save\\_configuration | restore\\_configuration](#) section to get example on how to save and restore settings through the CLI.

### 5.11.3 Saving/Restoring/Duplicating settings through the Web interface

Navigate to [Contextual help>>>Maintenance>>>Services](#) section to get information on how to save and restore settings through the Web interface.

## 5.12 Replacing the PDU Gigabit Network Module



Handle the GNM with care. Be aware that there is a risk of electrostatic discharge (ESD). As a preventive measure, wear ESD protection, such as an ESD shoe strap, while replacing the GNM. Do not put stress on the connection cable during installation.

A hardware configuration file specific to the PDU model needs to be uploaded to the new GNM so that the GNM knows the characteristics of the PDU model in which it resides (such as what type of input, how many circuit breakers, how many outlets, and how measurements should be displayed).

Typically, the GNM in your PDU is being replaced because it is not working. In this case, you need to get a copy of the PDU model's hardware configuration file from the Product Model Web site or from another working PDU of the same model type and configuration. Then, you need to upload the PDU model-specific hardware description file to the new GNM after it is installed.

However, if you are replacing a working GNM, the resident PDU model's hardware description file can be downloaded before you remove the GNM to a USB drive or your computer using FTP.

Then, you can restore this file to the new GNM after you install it.

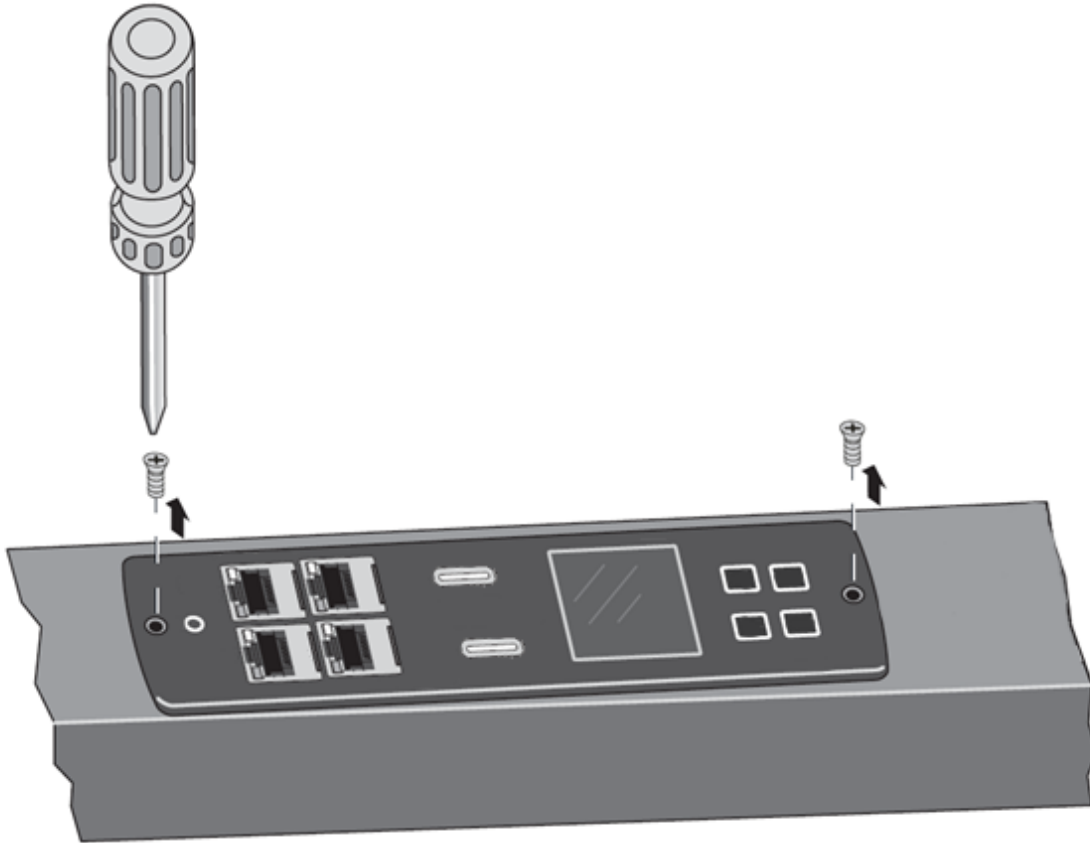


**NOTE 1** The GNM is hot-swappable. This means outlets will not be affected or change on/off state during the replacement process.

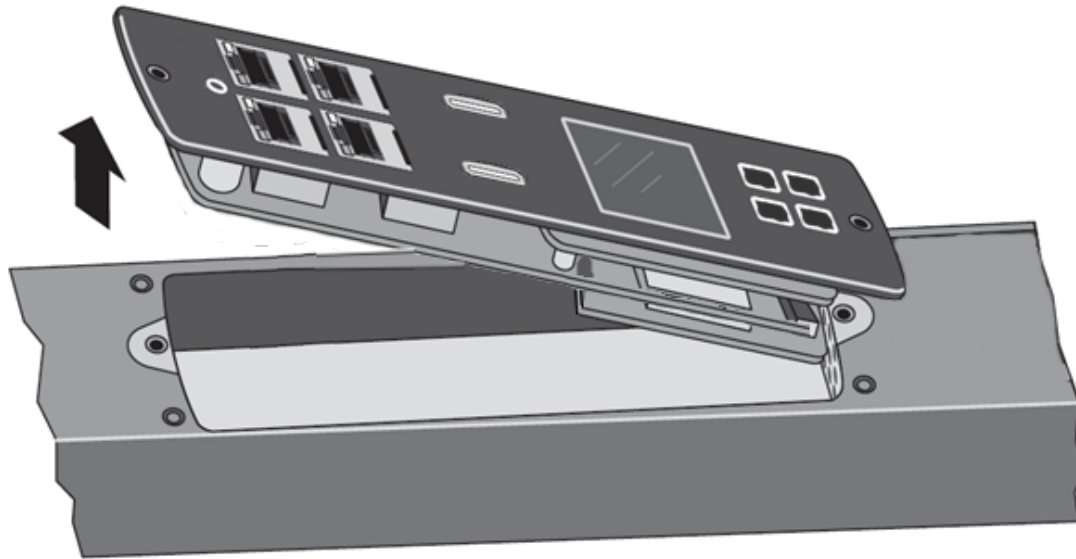
**NOTE 2** See "USB Flash Mode Submenu" on page 71 for more information about saving and uploading the user configuration files that store the settings customized by the user, such as the network parameters, outlet names, and threshold values.

## 5.12.1 To replace the GNM

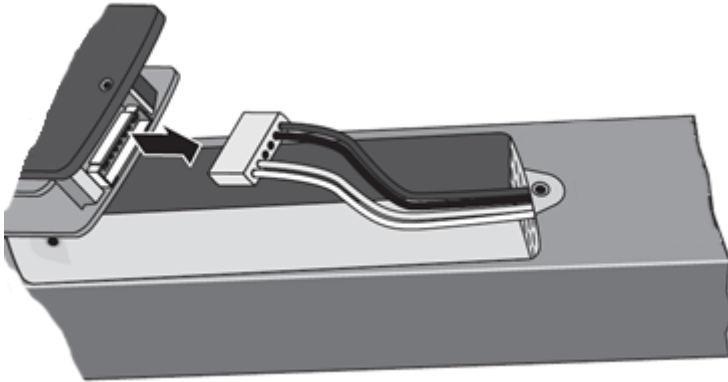
1- Remove the two GNM mounting screws.



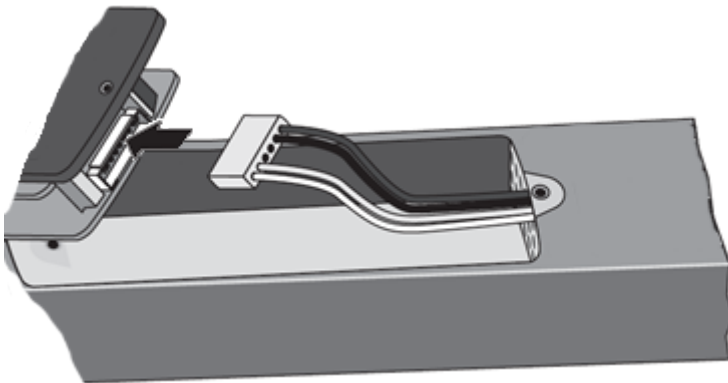
2- Tilt up one side of the GNM and locate the attached cable harness.



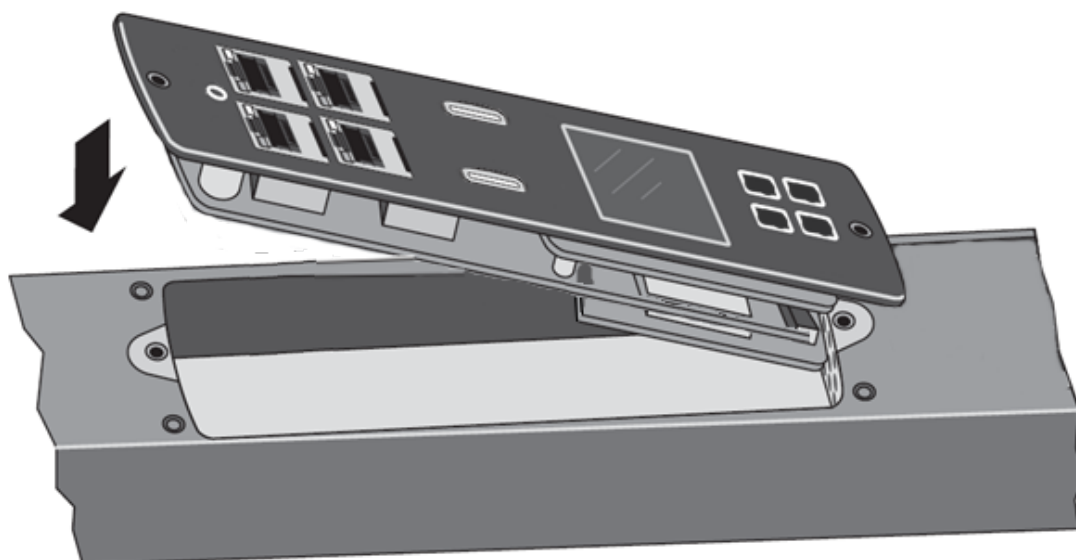
3- Disconnect the cable harness and remove the GNM.



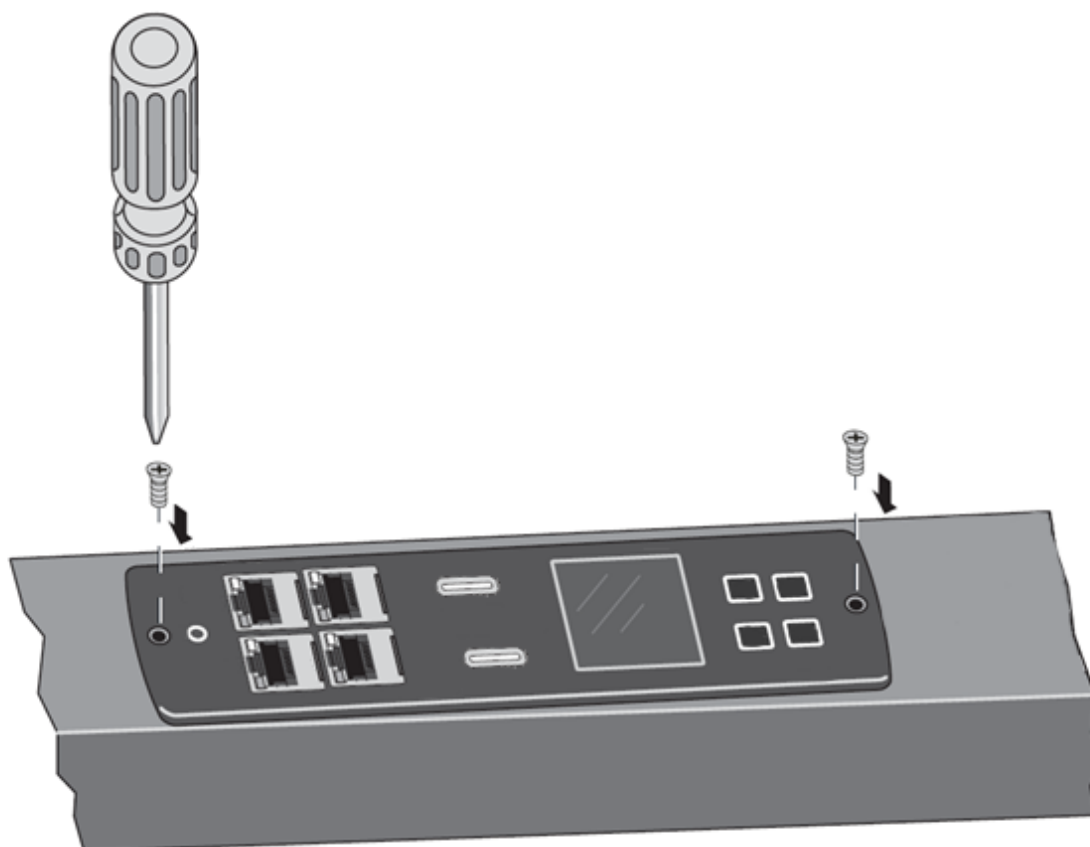
4- Locate and unwrap the new GNM. Connect the cable harness to the new GNM.



5- Reinsert the new GNM.



6- Install the two GNM mounting screws.



After the new GNM is connected, the “internal communication error” message displays until the configuration file is uploaded to the GNM.

7- The new GNM will not have the same MAC address as the one you are replacing. Ensure the old MAC address label is discarded, and that new MAC address label is firmly adhered to the product.

8- Download the PDU model’s hardware configuration file using one of the following processes:

- From the Web (go to Step 9)
- To the USB with an PDU with the same configuration (go to Step 15)

9- Go to [www.eaton.com/PDU](http://www.eaton.com/PDU).

10- If available, click the Sign In button in the upper left corner of the page to sign in. Return to the PDU home page. (The Sign In button will not be available if you are already logged in. The button selection will be "Sign Out" instead of "Sign In.")

11- Enter the part number of your PDU in the Eaton Product Wizards "PDU Part Number Search" field. Click **Search**. The Search Results page displays.

12- On the Search Results page, click the linked part number under the part number column. The Product page for the specified PDU opens.

13- Copy and save the PDU model-specific hardware configuration file to your computer using the link near the bottom of the page.



The link to the configuration file only displays if you are signed in.



Be sure that the Configuration number on the unit rating label also appears in the file name of the model specific PDU hardware configuration file.

14- Go to Step 21.

15- Make sure the GNM is powered ON. Connect a USB flash drive to a working PDU.



This PDU must be of the same model type and configuration as the PDU that houses the GNM you will replace.

16- When the LCD interface pop-up confirms that the USB flash drive is detected, click OK, and press Enter to return to the Main Menu. (If not confirmed within 10 seconds, the pop-up goes away by itself.)

17- From the Settings menu, select USB Flash Mode. Press Enter, select yes to confirm, and then press Enter again. The module restarts. (If there is no action within one minute, the GNM exits USB Flash Mode. Remove and reinsert the flash drive to access this menu again.)

18- Select Save GNM file to save the PDU hardware configuration file to the USB drive. The file will save to the eNMC2/config/hw path at the USB drive root directory.

19- When the file is saved, click OK to confirm.

20- Disconnect the USB drive from the working PDU.

21- Upload the PDU hardware configuration file using one of the following processes:

- FTP (Step 22)
- USB (Step 32)



**NOTE 1** To perform the GNM configuration upload with USB, only one hardware configuration file must be stored in the USB key.

**NOTE 2** For FTP operation, FTP must be enabled (default setting) in the Web pages (**Network > Security > Global > FTP enable**).

22- Open a DOS command window on a computer that is also connected to network.

23- Change directory (CD) to the location of the XML file.

24- Open an FTP session using the following command:

```
>ftp <IPAddress>
```

*Where <IPAddress>* = the IP address displayed on LCD

25- Type the default login and password ("admin" and "admin").

26- At the command prompt, type the following command:

```
>cd config/hw
```

```
>dir
```

27- If an PDU hardware configuration file (XML) file already exists, type the following command to delete the file:

```
>delete <config file>
```

28- To upload the PDU hardware configuration file to the GNM, type the following command:

```
>put <config file>
```

*Where <config file> = the file name to be downloaded to the GNM*



Keep the <config file> name exactly as it is downloaded from the website. It must begin with the prefix "PDU\_cfg\_" or the GNM will not recognize it.

29- Type the following command to verify the file has been uploaded:

```
>dir
```

30- Type the following command to quit the FTP session:

```
>quit
```

31- Go to the "Restarting the GNM and Resetting the PDU" procedure that follows.

32- Make sure the GNM is powered ON. Connect the USB flash drive to the PDU with the new GNM.

33- When the LCD interface pop-up confirms that the USB flash drive is detected, click OK, then press Enter to return to the Main Menu. (If not confirmed within 10 seconds, the pop-up goes away by itself.)

34- From the LCD Settings menu, select USB Flash Mode. Press Enter, select yes to confirm, and then press Enter again. The module restarts. (If there is no action within one minute, the GNM exits USB Flash Mode. Remove and reinsert the USB flash drive to access this menu again.)

35- Select Load GNM file, then click OK to upload the PDU hardware configuration file to the GNM.

36- When the file is successfully loaded, click OK to confirm.

37- Remove the USB flash drive and select Exit.

## 5.13 Restarting the PDU Gigabit Network Module and Resetting the PDU

1- Restart the GNM using either the reset button on the LCD front panel, or using a serial or network connection to a terminal emulator or Web interface.

2- Reset the PDU to factory default settings using one of the following:

- Web interface: Maintenance>Services>Sanitization
- LCD menu "Factory Submenu": Settings > Factory > Return to Factory Settings > Yes > OK



Step 1 and Step 2 must be performed, or the new configuration will not be properly accepted by the GNM. If something doesn't look right afterward, perform Step 2 (reset to defaults) a second time. After the PDU hardware configuration file is uploaded and GNM is rebooted and reset to factory defaults, the PDU settings return to default settings and the energy counter restarts from 0. Only the serial number is recovered.

## 6 Securing the Network Management Module

### 6.1 Cybersecurity considerations for electrical distribution systems

#### 6.1.1 Purpose

The purpose of this section is to provide high-level guidance to help customers across industries and applications apply Eaton solutions for power management of electrical systems in accordance with current cybersecurity standards.

This document is intended to provide an overview of key security features and practices to consider in order to meet industry recommended standards and best practices.

#### 6.1.2 Introduction

Every day, cyber-attacks against government and commercial computer networks number in the millions. According to U.S. Cyber Command, Pentagon systems are probed 250,000 times per hour. Similar attacks are becoming more prevalent on other kinds of information-based smart networks as well, such as those that operate buildings and utility systems. Whether the objective is to steal intellectual property or halt operations, the tools and the techniques used for unauthorized network access are increasingly sophisticated.

#### 6.1.3 Connectivity—why do we need to address cybersecurity for industrial control systems (ICS)?

There is increasing concern regarding cybersecurity across industries where companies are steadily integrating field devices into enterprise-wide information systems. This occurs in discrete manufacturing and process industrial environments, a wide range of general and specific purpose commercial buildings, and even utility networks. Traditionally, electrical systems were controlled through serial devices connected to computers via dedicated transceivers with proprietary protocols. In contrast, today's control systems are increasingly connected to larger enterprise networks, which can expose these systems to similar vulnerabilities that are typically found in computer systems. The differences between information technology (IT) and ICS networks can be summarized as follows:

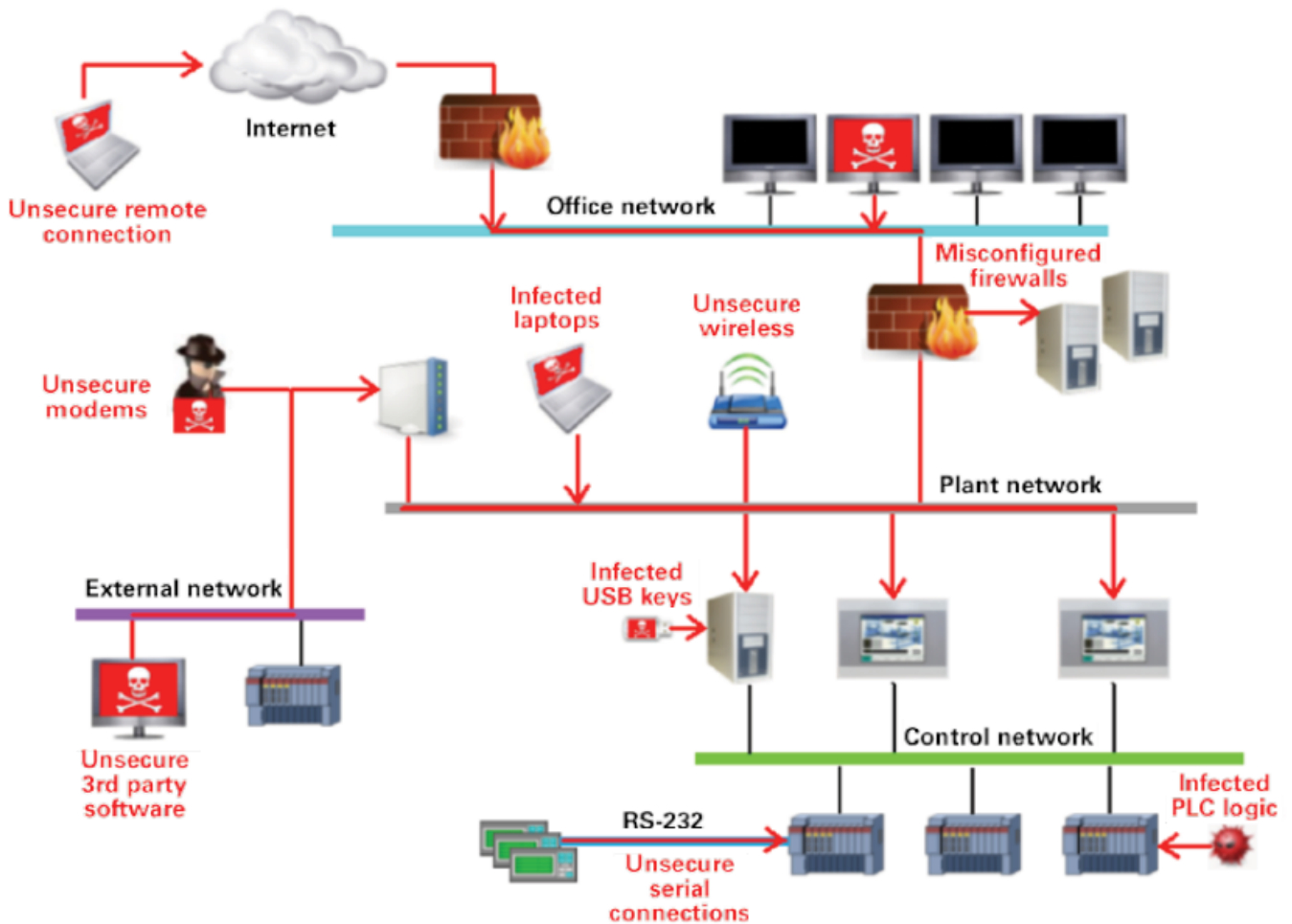
- The main focus of the IT network is to ensure the **confidentiality** and the **integrity** of the data using rigorous access control and data encryption
- The main focus of the ICS network is **safety, availability, and integrity** of data
- Enterprise security protects the servers' data from attack
- Control system security protects the facility's ability to safely and securely operate, regardless of what may befall the rest of the network

#### 6.1.4 Cybersecurity threat vectors

Cybersecurity threat vectors are paths or tools that an entity can use to gain access to a device or a control network in order to deliver a malicious attack. Figure below shows examples of attack vectors on a network that might otherwise seem secure.



### 6.1.4.1 Paths to the control network



The paths in above figure include:

- External users accessing the network through the Internet
- Misconfigured firewalls
- Unsecure wireless routers and wired modems
- Infected laptops located elsewhere that can access the network behind the firewall
- Infected USB keys and PLC logic programs
- Unsecure RS-232 serial links

The most common malicious attacks come in the following forms:

- Virus—a software program that spreads from one device to another, affecting operation
- Trojan horse—a malicious device program that hides inside other programs and provides access to that device
- Worm—a device program that spreads without user interaction and affects the stability and performance of the ICS network
- Spyware—a device program that changes the configuration of a device

### 6.1.5 Defense in depth

While there are differences between traditional IT systems and ICS, the fundamental concept of “defense in depth” is applicable to both. Defense in depth is a strategy of integrating technology, people, and operations capabilities to establish variable barriers across multiple layers of an organization. These barriers include electronic countermeasures such as firewalls, intrusion detection software/components, and antivirus software, coupled with physical protection policies and training. Fundamentally, the barriers are intended to reduce the probability of attacks on the network and provide mechanisms to detect “intruders.”

## 6.1.6 Designing for the threat vectors

### 6.1.6.1 Firewalls

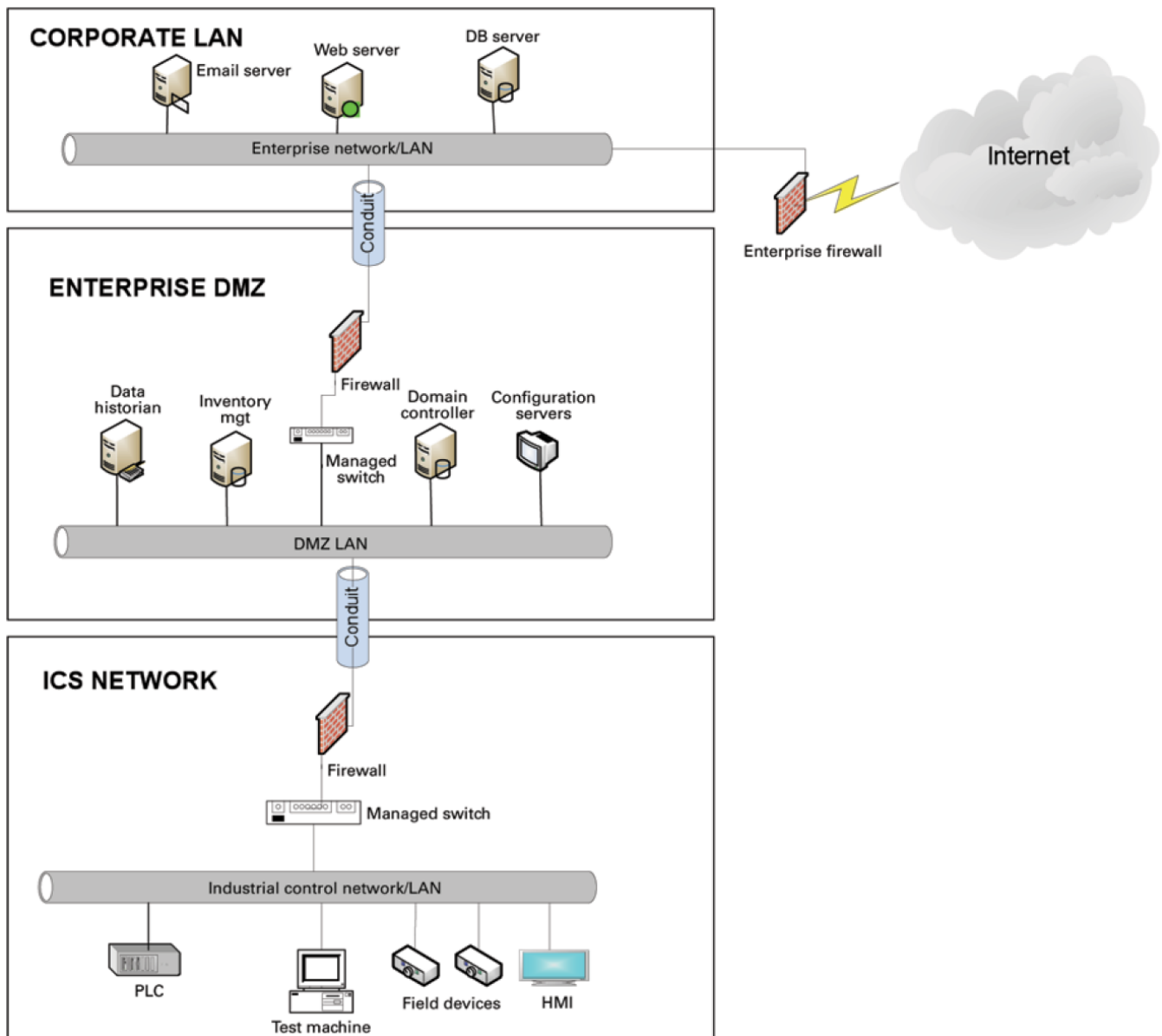
Firewalls provide the capability to add stringent and multifaceted rules for communication between various network segments and zones in an ICS network. They can be configured to block data from certain segments, while allowing the relevant and necessary data through. A thorough understanding of the devices, applications, and services that are in a network will guide the appropriate deployment and configuration of firewalls in a network. Typical types of firewalls that can be deployed in a network include:

- **Packet filter or boundary firewalls that work on the network layer**  
These firewalls mainly operate at the network layer, using pre-established rules based on port numbers and protocols to analyze the packets going into or out of a separated network.  
These firewalls either permit or deny passage based on these rules.
- **Host firewalls**  
These firewalls are software firewall solutions that protect ports and services on devices. Host firewalls can apply rules that track, allow, or deny incoming and outgoing traffic on the device and are mainly found on mobile devices, laptops, and desktops that can be easily connected to an ICS.
- **Application-level proxy firewalls**  
These firewalls are highly secure firewall protection methods that hide and protect individual devices and computers in a control network. These firewalls communicate at the application layer and can provide better inspection capabilities. Because they collect extensive log data, application-level proxy firewalls can negatively impact the performance of an ICS network.
- **Stateful inspection firewalls**  
These firewalls work at the network, session, and application layers of the open system interconnection (OSI). Stateful inspection firewalls are more secure than packet filter firewalls because they only allow packets belonging to allowed sessions.  
These firewalls can authenticate users when a session is established and analyze a packet to determine whether they contain the expected payload type or enforce constraints at the application layer.
- **SCADA hardware firewalls**  
These are hardware-based firewalls that provide defense for an ICS based on observing abnormal behavior on a device within the control network. For example, if an operator station computer suddenly attempts to program a PLC, this activity could be blocked and an alarm could be raised to prevent serious risk to the system.

### 6.1.6.2 Demilitarized zones (DMZ)

Network segmentation is a key consideration in establishing secure control networks. Firewalls should be used to create DMZ by grouping critical components and isolating them from the traditional business IT network. A three-tier architecture should be employed at a minimum, with a DMZ between the organization's core network and an isolated control system's network as shown in below figure.

### 6.1.6.2.1 Three-tier architecture for a secure control network



Above figure shows that the control networks are divided into layers or zones based on control functions, which are then connected by conduits (connections between the zones) that provide security controls to:

- Control access to zones
- Resist denial of services (DOS) attacks or the transfer of malware
- Shield other network systems
- Protect the integrity and the confidentiality of network traffic

Beyond network segmentation, access control (both physical and logical) should be defined and implemented.

The key consideration when designing access control is defining the **required** interactions both within a given zone and between zones. These interactions should be mapped out clearly and prioritized based on need. It is important to realize that every hole poked in a firewall and each non-essential functionality that provides access or creates additional connectivity increases potential exposure to attacks. A system then becomes only as secure as the devices connecting to it.

If mapped correctly, the potential adverse impact to control system reliability and functionality should be negligible. However, this element introduces additional costs (in terms of firewall and other network infrastructure) and complexity to the environment.

### 6.1.6.3 Intrusion detection and prevention systems (IDPS)

These are systems that are primarily focused on identifying possible incidents in an ICS network, logging the information about them, attempting to stop them, and reporting them to ICS security administrators.

Because these systems are critical in an ICS network, they are regular targets for attacks and securing them is extremely important. The type of IDPS technology deployed will vary with the type of events that need to be monitored.

There are four classes of IDPS technology:

- Network-based IDPS monitors network traffic for particular ICS network segments or devices and analyzes the network and application protocol activity to identify suspicious activity
- Wireless IDPS monitors and analyzes wireless network traffic to identify suspicious activity involving the ICS wireless network protocol
- Network behavior analysis IDPS examines ICS network traffic to identify threats that generate unusual traffic flows such as DOS attacks
- Host-based IDPS monitors the characteristics and the events occurring within a single ICS network host for suspicious activity

### 6.1.7 Policies, procedures, standards, and guidelines

For the defense in depth strategy to succeed, there must be well-documented and continuously reviewed policies, procedures, standards, and guidelines.

- **Policies** provide procedures or actions that must be carried out to meet objectives and to address the who, what, and why
- **Procedures** provide detailed steps to follow for operations and to address the how, where, and when
- **Standards** typically refer to specific hardware and software, and specify uniform use and implementation of specific technologies or parameters
- **Guidelines** provide recommendations on a method to implement the policies, procedures, and standards

#### 6.1.7.1 Understanding an ICS network

Creating an inventory of all the devices, applications, and services that are hosted in a network can establish an initial baseline for what to monitor. Once those components are identified and understood, control, ownership, and operational consideration can be developed.

#### 6.1.7.2 Log and event management

It is important to understand what is happening within the network from both a performance and security perspective. This is especially true in a control systems environment.

Log and event management entails monitoring infrastructure components such as routers, firewalls, and IDS/IPS, as well as host assets. Security Information and Event Management (SIEM) systems can collect events from various sources and provide correlation and alerts.

Generating and collecting events, or even implementing a SIEM is not sufficient by itself. Many organizations have SIEM solutions, but alerts go unwatched or unnoticed.

Monitoring includes both the capability to monitor environments and the capacity to perform the monitoring. Capability relates to the design and the architecture of the environment. Has it been built in a manner that takes into consideration the ability to monitor? Capacity speaks to the resources (personnel, tools, expertise) needed to perform meaningful interpretation of the information and initiate timely and appropriate action.

Through monitoring, the organization can identify issues such as suspicious or malicious activities. Awareness can be raised when new (potentially unauthorized) devices appear in the environment. Careful consideration should be taken into account to ensure that log and event management does not adversely impact the functionality or the reliability of the control system devices.

#### 6.1.7.3 Security policy and procedures

It is important to identify “asset owners,” and to develop policies and procedures for a cybersecurity program. These policies need to be practical and enforceable in order to be effective. Policies should also address access related issues, such as physical access, contractors, and vendors.

Existing (traditional) IT standards and policies may not apply (or have not been considered) for control systems. A gap analysis should be performed to determine which components are not covered (or not adequately covered) by existing policies. Relationships with existing policies and standards should be explicitly identified and new or supporting policies should be developed. It is important that industrial control system administrators have proper authorizations and full support of their management to implement policies that will help secure the ICS network.

#### 6.1.7.4 ICS hardening

The goal for system hardening is to reduce as many security risks as possible by securely configuring ICS networks. The idea is to establish configurations based on what is required and eliminate unnecessary services and applications that could potentially provide another possible entry point to an intruder.

Minimum security baselines should be established for the various platforms and products deployed (operating system, application, and infrastructure elements such as drives, meters, HMI devices). The following actions should be implemented where applicable:

- Disable unnecessary services
- Disable anonymous FTP
- Do not use clear text protocols (e.g., use SSH v2 instead of Telnet)
- Install only required packages/applications/features
- Deploy antivirus solutions (where possible)
- Disable or otherwise control use of USB devices
- Establish a warning banner
- Change default passwords (e.g., SNMP)

It may be easier to implement these actions on devices for which you control the base operating system platform. However, several

of the items listed above can be configured from the product specific configuration options.

Changes such as these could potentially impact the functionality of a control system device. Extensive testing needs to be conducted before deployment to minimize this impact.

#### 6.1.7.5 Continuous assessment and security training

It is critical that ICS network administrators and regular users be properly trained to ensure the security of the ICS and the safety of the people who operate and depend on it.

Ongoing vulnerability assessments are critical to identify issues and understand the effectiveness of other defensible network elements.

Assessments should include testing and validating the following:

- Monitoring capabilities and alerts are triggered and responded to as expected
- Device configuration of services and applications
- Expected connectivity within and between zones
- Existence of previously unknown vulnerabilities in the environment
- Effectiveness of patching

A program should be established for performing assessments.

The actual assessment should be performed by a qualified resource, which can be an in-house or third-party organization. Regardless of who performs the assessments, in-house resources need to be involved in the planning, scoping, and supporting of assessment activities and must be appropriately trained to do so.

Assessments should be conducted according to a methodology that is clearly defined to address:

- Physical security
- People and processes
- Network security
- Host security
- Applications security (both internally developed and commercially off-the-shelf (COTS))

#### 6.1.7.6 Patch management planning and procedures

A patching and vulnerability management process should be established based on the timely awareness of issues and appropriate action. This process should take all of the elements that make up the control system environment into consideration.

Information resources should be identified for vulnerability and advisory information for the various components in the environment. These should include vendor-specific sources as well as other public or commercial services that provide vulnerability advisory information. For example, the National Vulnerability Database (NVD) provides information related to vulnerabilities identified in

general IT components, while the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) publishes advisories specific to control systems.

A regular patch deployment schedule should be established for each component in the environment. Depending on the component, this could range from a monthly schedule to an as-needed deployment, depending on the historical frequency of patch or vulnerability related issues for the component or the vendor. Additionally, out-of-band or emergency patch management needs to be considered and qualifications need to be defined.

Vulnerability information and advisories should be reviewed regularly and assessments should be performed to determine the relative severity and urgency of issues.

Elements of the process should also include the preparation, scheduling, and change controls; testing and rollback procedures; and pre-deployment notification to stakeholders that includes scope, expectations, and reporting. Testing is a significant element, as the effect of the patch application needs to be clearly understood; unintended or unexpected impacts to a control system component influence the decision to deploy a patch. In the event that it is determined that a patch cannot be safely deployed but the severity of the issue represents a significant concern, compensating controls should be investigated.

## 6.1.8 Conclusion

To protect important assets, all organizations must take cybersecurity threats seriously and meet them proactively with a system-wide defensive approach specific to organizational needs.

There is no protection method that is completely secure. A defense mechanism that is effective today may not be effective tomorrow– the ways and means of cyber-attacks constantly change. It is critical ICS administrators remain aware of changes in cybersecurity and continue to work to prevent any potential vulnerabilities in the systems they manage.

## 6.1.9 Terms and definitions

<b>DMZ</b>	A demilitarized zone is a logical or physical sub network that interfaces an organization's external services to a larger, untrusted network and providing an additional layer of security.
<b>Encryption</b>	The process of transforming plain or clear text using an algorithm to make it unreadable to anyone except those possessing special knowledge.
<b>ICS</b>	A device or set of device that manage, command, direct, or regulate the behavior of other devices or systems.
<b>Protocol</b>	A set of standard rules for data representation, signaling, authentication, and error detection required to send information over a communications channel

## 6.1.10 Acronyms

<b>COTS</b>	Commercially Off-the-Shelf
<b>DMZ</b>	Demilitarized Zone
<b>DOS</b>	Denial of Service
<b>FTP</b>	File Transfer Protocol
<b>HMI</b>	Human Machine Interface
<b>ICS</b>	Industrial Control Systems
<b>ICS-CERT</b>	Industrial Control Systems - Cyber Emergency Response Team
<b>IDPS</b>	Intrusion Detection and Prevention Systems
<b>IDS</b>	Intrusion Detection Systems

IPS	Intrusion Prevention Systems
IT	Information Technology
NVD	National Vulnerability Database
OSI	Open System Interconnection
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SIEM	Security Information and Event Management
USB	Universal Serial Bus

## 6.1.11 References

- [1] Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies, October 2009  
[https://ics-cert.us-cert.gov/sites/default/files/FactSheets/NCCIC%20ICS\\_FactSheet\\_Defense\\_in\\_Depth\\_Strategies\\_S508C.pdf](https://ics-cert.us-cert.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_Defense_in_Depth_Strategies_S508C.pdf)
- [2] NIST.SP.800-82 Guide to Industrial Control Systems (ICS) Security, June 2011  
<http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf>
- [3] NIST.SP.800-94 Guide to Intrusion Detection and Prevention Systems (IDPS), Feb 2007  
<http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf>
- [4] Common Cybersecurity Vulnerabilities in Industrial Control Systems, May 2011  
[http://ics-cert.uscert.gov/sites/default/files/recommended\\_practices/DHS\\_Common\\_Cybersecurity\\_Vulnerabilities\\_ICS\\_2010.pdf](http://ics-cert.uscert.gov/sites/default/files/recommended_practices/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf)
- [5] The Tao of Network Security Monitoring, 2005 Richard Bejtlich

## 6.2 Cybersecurity recommended secure hardening guidelines

- [Introduction](#)
- [Secure configuration guidelines](#)
  - [Asset Management](#)
  - [Defense in Depth](#)
  - [Risk Assessment](#)
  - [Physical Security](#)
  - [Account management](#)
  - [Time Synchronization](#)
  - [Deactivate unused features](#)
  - [Network Security](#)
  - [Remote access](#)
  - [Logging and Event Management](#)
  - [Malware defenses](#)
  - [Secure Maintenance](#)
  - [Business Continuity / Cybersecurity Disaster Recovery](#)
  - [Sensitive Information Disclosure](#)
  - [Decommissioning or Zeroization](#)
- [References](#)

### 6.2.1 Introduction

This Network module has been designed with cybersecurity as an important consideration. Number of features are offered in the product to address cybersecurity risks. These Cybersecurity Recommendations provide information to help users to deploy and maintain the product in a manner that minimizes the cybersecurity risks. These Cybersecurity Recommendations are not intended to provide a comprehensive guide to cybersecurity, but rather to complement customers' existing cybersecurity programs.

Eaton is committed to minimizing the cybersecurity risk in its products and deploying cybersecurity best practices in its products and solutions, making them more secure, reliable and competitive for customers.

The following whitepapers are available for more information on general cybersecurity best practices and guidelines:

**Cybersecurity Considerations for Electrical Distribution Systems (WP152002EN):** [http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct\\_1603172.pdf](http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf)

**Cybersecurity Best Practices Checklist Reminder (WP910003EN):** [http://www.cooperindustries.com/content/dam/public/powersystems/resources/library/1100\\_EAS/WP910003EN.pdf](http://www.cooperindustries.com/content/dam/public/powersystems/resources/library/1100_EAS/WP910003EN.pdf)

**Cybersecurity Best Practices for Modern Vehicles - NHTSA:** [https://www.nhtsa.gov/staticfiles/nvs/pdf/812333\\_CybersecurityForModernVehicles.pdf](https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf)

### 6.2.2 Secure configuration guidelines

#### 6.2.2.1 Asset Management

Keeping track of software and hardware assets in your environment is a pre-requisite for effectively managing cybersecurity. Eaton recommends that you maintain an asset inventory that uniquely identifies each important component.

To facilitate this, Network module supports the following identifying information:

##### 6.2.2.1.1 Network Module identification and its firmware information

It can be retrieved by navigating to *Card>>>System information or Maintenance>>>System information*.

###### Identification

- System name
- Product
- Physical name
- Vendor
- UUID
- Part number



- Serial number
- Hardware version
- Location
- Contact

#### Firmware information

- Firmware version
- Firmware SHA
- Firmware date
- Firmware installation date
- Firmware activation date
- Bootloader version

### 6.2.2.1.2 Communication settings

It can be retrieved by navigating to *Settings>>>Network* or *Settings>>>Network & Protocol*

#### LAN

- Link status
- MAC address
- Configuration

#### IPV4

- Status
- Mode
- Address
- Netmask
- Gateway


#### Domain

- Mode
- FQDN
- Primary DNS
- Secondary DNS

#### IPV6

- Status
- Mode
- Addresses

### 6.2.2.1.3 UPS details

It can be retrieved by navigating to *Home>>>Details* or *Home>>>Energy flow* .

#### Details

- Name
- Model
- P/N
- S/N
- Location
- FW version



Most of above information are discoverable using SNMP, refer to *Settings>>>SNMP*.

### 6.2.2.2 Defense in Depth

Defense in Depth basically means applying multiple counter-measures for mitigating risks, in a layered or step wise manner. A layered approach to security as shown in the below diagram is what is recommended. Defense in Depth is the responsibility of both the manufacturer and the customer.



### 6.2.2.3 Risk Assessment

Eaton recommends conducting a risk assessment to identify and assess reasonably foreseeable internal and external risks to the confidentiality, availability and integrity of the system | device and its environment. This exercise should be conducted in accordance with applicable technical and regulatory frameworks such as IEC 62443 and NERC-CIP. The risk assessment should be repeated periodically.

### 6.2.2.4 Physical Security

An attacker with unauthorized physical access can cause serious disruption to system/device functionality. Additionally, Industrial Control Protocols don't offer cryptographic protections, making ICS and SCADA communications especially vulnerable to threats to their confidentiality. Physical security is an important layer of defense in such cases. The Network module is designed to be deployed and operated in a physically secure location. Following are some best practices that Eaton recommends to physically secure your system/device:

- Secure the facility and equipment rooms or closets with access control mechanisms such as locks, entry card readers, guards, man traps, CCTV, etc. as appropriate.
- Restrict physical access to cabinets and/or enclosures containing the Network module and the associated system. Monitor and log the access at all times.
- Physical access to the telecommunication lines and network cabling should be restricted to protect against attempts to intercept or sabotage communications. It's a best practice to use metal conduits for the network cabling running between equipment cabinets.
- The Network module supports the following physical access ports: RJ45, USB A, USB Micro-B. Access to these ports should be restricted.
- Do not connect removable media (e.g., USB devices, SD cards, etc.) for any operation (e.g., firmware upgrade, configuration change, or boot application change) unless the origin of the media is known and trusted.
- Before connecting any portable device through a USB port or SD card slot, scan the device for malware and viruses.

### 6.2.2.5 Account management

Logical access to the system | device should be restricted to legitimate users, who should be assigned only the privileges necessary to complete their job roles/functions. Some of the following best practices may need to be implemented by incorporating them into the organization's written policies:

- Ensure default credentials are changed upon first login Network module should not be deployed in production environments with default credentials, as default credentials are publicly known.
- No account sharing – Each user should be provisioned a unique account instead of sharing accounts and passwords. Security monitoring/logging features in the product are designed based on each user having a unique account. Allowing users to share credentials weakens security.
- Restrict administrative privileges - Attackers seek to gain control of legitimate credentials, especially those for highly privileged accounts. Administrative privileges should be assigned only to accounts specifically designated for administrative duties and not for regular use.
- Leverage the roles / access privileges *admin*, *operator*, *viewer* to provide tiered access to the users as per the business / operational need. Follow the principle of least privilege (allocate the minimum authority level and access to system resources required for the role).

- Perform periodic account maintenance (remove unused accounts).
- Ensure password length, complexity and expiration requirements are appropriately set, particularly for all administrative accounts (e.g., minimum 10 characters, mix of upper- and lower-case and special characters, and expire every 90 days, or otherwise in accordance with your organization's policies).
- Enforce session time-out after a period of inactivity.

#### 6.2.2.5.1 Description of the User management in the Network Module:

- User and profiles management: (Navigate to Settings>>>Users)
  - Add users (admin, operator, viewer)
  - Remove users
  - Edit users
- Password/Account/Session management: (Navigate to Settings>>>Users)
  - Password strength rules – Minimum length/Minimum upper case/Minimum lower case/Minimum digit/Special character
  - Account expiration – Number of days before the account expiration/Number of tries before blocking the account
  - Session expiration – No activity timeout/Session lease time
  - See "Default settings parameters" in the embedded help for (recommended) default values.
  - Additionally, it is possible to enable account expiration to force users renew their password periodically.
- Default credentials: admin/admin
  - The change of the default "admin" password is enforced at first connection.
  - It is also recommended to change the default "admin" user name through the *Settings>>>Users or Settings>>>Local users* page.
  - Follow embedded help for instructions on how to edit a user account.
- Local and Trusted remote certificate configuration: (Navigate to Settings>>>Certificate)
  - Follow embedded help for instructions on how to configure it.
- Supported authentication: LDAP and Radius, follow embedded help for instructions on how to configure it.

#### 6.2.2.6 Time Synchronization

Many operations in power grids and IT networks heavily depend on precise timing information.

Ensure the system clock is synchronized with an authoritative time source (using manual configuration, NTP). (Navigate to Settings>>>General>>>Time&date settings)

Follow embedded help for instructions on how to configure it.

#### 6.2.2.7 Deactivate unused features

Network module provides multiple options to upgrade firmware, change configurations, set power schedules, etc. The device also provide multiple options to connect with the device i.e. SSH, SNMP,SMTP,HTTPS etc. Services like SNMPv1 are considered insecure and Eaton recommends disabling all such insecure services.

- It is recommended to disable unused physical ports like USB and SD card.
- Disable insecure services like SNMP v1

#### 6.2.2.8 Network Security

Network module supports network communication with other devices in the environment. This capability can present risks if it's not configured securely. Following are Eaton recommended best practices to help secure the network. Additional information about various network protection strategies is available in *Eaton Cybersecurity Considerations for Electrical Distribution Systems [R1]*.

Eaton recommends segmentation of networks into logical enclaves, denying traffic between segments except that which is specifically allowed, and restricting communication to host-to-host paths (for example, using router ACLs and firewall rules). This helps to protect sensitive information and critical services and creates additional barriers in the event of a network perimeter breach. At a minimum, a utility Industrial Control Systems network should be segmented into a three-tiered architecture (as recommended by NIST SP 800-82[R3]) for better security control.

Communication Protection: Network module provides the option to encrypt its network communications. Please ensure that encryption options are enabled. You can secure the product's communication capabilities by taking the following steps:

- Local and Trusted remote certificate configuration: (Navigate to Settings>>>Certificate)  
Follow embedded help for instructions on how to configure it.

Eaton recommends opening only those ports that are **required** for operations and protect the network communication using network protection systems like firewalls and intrusion detection systems / intrusion prevention systems. Use the information below to configure your firewall rules to allow access needed for Network module to operate smoothly

- Navigate to *Information>>>Specifications/Technical characteristics>>>Port* to get the list of all ports and services running on the device.
- SNMP V1/SNMP V3 can be disabled or configured by navigating to *Settings>>>SNMP*.  
Follow embedded help for instructions on how to configure it.
- If available, Modbus and Bacnet can be configured by navigating to Settings>>>Protocols or Settings>>>Industrial protocols.  
Follow embedded help for instructions on how to configure it.

### 6.2.2.9 Remote access

Remote access to devices/systems creates another entry point into the network. Strict management and validation of termination of such access is vital for maintaining control over overall ICS security.

Remote access capabilities and permissions can be configured in Settings>>>Remote users for LDAP and Radius.

Follow embedded help for instructions on how to configure it.

### 6.2.2.10 Logging and Event Management

Navigate to Information>>>List of events codes to get log information and how to export it.

#### Good Practices

- Eaton recommends logging all relevant system and application events, including all administrative and maintenance activities.
- Logs should be protected from tampering and other risks to their integrity (for example, by restricting permissions to access and modify logs, transmitting logs to a security information and event management system, etc.).
- Ensure that logs are retained for a reasonable and appropriate length of time.
- Review the logs regularly. The frequency of review should be reasonable, taking into account the sensitivity and criticality of the system | device and any data it processes.

### 6.2.2.11 Malware defenses

Eaton recommends deploying adequate malware defenses to protect the product or the platforms used to run the Eaton product.

### 6.2.2.12 Secure Maintenance

Troubleshooting information are available in the embedded help for diagnostic purposes.

The Network module includes also Servicing, Securing sections to allow a service engineer with help from site administrator to trouble shoot the device functionality.

- Configuring/Commissioning/Testing LDAP
- Pairing agent to the Network Module
- Powering down/up applications (examples)
- Checking the current firmware version of the Network Module
- Accessing to the latest Network Module firmware/driver/script
- Upgrading the card firmware (Web interface / shell script)
- Changing the RTC battery cell
- Updating the time of the Network Module precisely and permanently (ntp server)
- Synchronizing the time of the Network Module and the UPS
- Changing the language of the web pages
- Resetting username and password
- Recovering main administrator password
- Switching to static IP (Manual) / Changing IP address of the Network Module
- Reading device information in a simple way
- Subscribing to a set of alarms for email notification
- Saving/Restoring/Duplicating Network module configuration settings
- Configuring user permissions through profiles
- Decommissioning the Network Management module

Eaton publishes patches and updates for its products to protect them against vulnerabilities that are discovered. Eaton encourages customers to maintain a consistent process to promptly monitor for and install new firmware updates.

#### Good Practices

- Update device firmware prior to putting the device into production.
- Thereafter, apply firmware updates and software patches regularly.

Please check Eaton's cybersecurity website for information bulletins about available firmware and software updates.

- Navigate in the help to *Contextual help>>>Card>>>Administration* to get information on how to upgrade the Network Module.
- Eaton also has a robust vulnerability response process. In the event of any security vulnerability getting discovered in its products, Eaton patches the vulnerability and releases information bulletin through its cybersecurity web site - <https://eaton.com/cybersecurity> and patch through [www.eaton.com/downloads](http://www.eaton.com/downloads).

## 6.2.2.13 Business Continuity / Cybersecurity Disaster Recovery

### 6.2.2.13.1 Plan for Business Continuity / Cybersecurity Disaster Recovery

Eaton recommends incorporating the Network module into the organization's business continuity and disaster recovery plans. Organizations should establish a Business Continuity Plan and a Disaster Recovery Plan and should periodically review and, where possible, exercise these plans. As part of the plan, important system | device data should be backed up and securely stored, including:

- Updated firmware for the Network module. Make it a part of standard operating procedure to update the backup copy as soon as the latest firmware is updated.
- The current configuration.
- Documentation of the current permissions / access controls, if not backed up as part of the configuration.

The following section describes the details of failures states and backup functions:

- Communication and power status indicators: Navigate in the help to *Information>>>Front panel connectors and LED indicators*.
- Configuration of backup and recovery: Navigate in the help to *Servicing the Network Management Module>>>Saving/Restoring/Duplicating Network module configuration settings*.

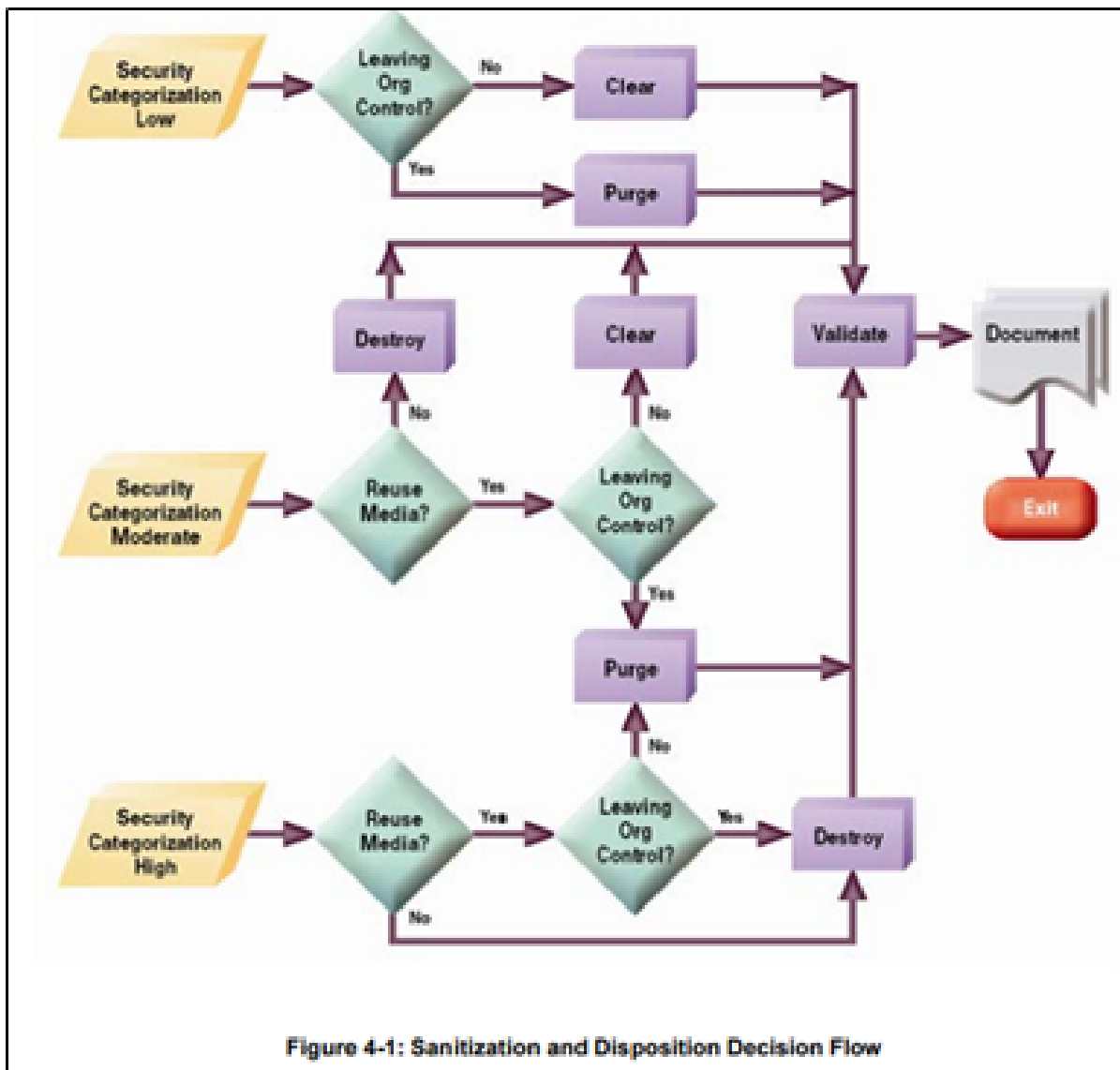
## 6.2.2.14 Sensitive Information Disclosure

Eaton recommends that sensitive information (i.e. connectivity, log data, personal information) that may be stored by Network module be adequately protected through the deployment of organizational security practices.

- Full name
- Email
- Phone
- Organization
- The mail credentials in the CDS storage
- PKI signed server's (HTTP + MQTT) certificate and associated private key
- Server's (HTTP + MQTT) self-signed private keys (they are self-generated by the device upon user request, so unique per device)
- Username's (in clear) and their "vCard" (Full name, Organization, Phone, Email, ...)
- Hashed passwords
- IP addresses, hostnames (DNS, Gateway, mail servers, ...) of customer network devices (in database or logs)
- Maintenance report AES key/password

## 6.2.2.15 Decommissioning or Zeroization

It is a best practice to purge data before disposing of any device containing data. Guidelines for decommissioning are provided in NIST SP 800-88. Eaton recommends that products containing embedded flash memory be securely destroyed to ensure data is unrecoverable.



\*Figure and data from NIST SP800-88

- **Embedded Flash Memory on Boards and Devices**
- Eaton recommends the following methods for disposing of motherboards, peripheral cards such as network adapters, or any other adapter containing non-volatile flash memory.
- **Clear:** If supported by the device, reset the state to original factory settings.  
Navigate to Securing the Network Management Module>>>Decommissioning the Network Management module.
- **Purge:** If the flash memory can be easily identified and removed from the board, the flash memory may be destroyed independently of the board that contained the flash memory. Otherwise, the whole board should be destroyed. For the Network module the whole board should be destroyed.
- **Destroy:** Shred, disintegrate, pulverize, or Incinerate by burning the device in a licensed incinerator.

## 6.2.3 References

- [R1] Cybersecurity Considerations for Electrical Distribution Systems (WP152002EN): [http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct\\_1603172.pdf](http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf)
- [R2] Cybersecurity Best Practices Checklist Reminder (WP910003EN): [http://www.cooperindustries.com/content/dam/public/powersystems/resources/library/1100\\_EAS/WP910003EN.pdf](http://www.cooperindustries.com/content/dam/public/powersystems/resources/library/1100_EAS/WP910003EN.pdf)
- [R3] NIST SP 800-82 Rev 2, Guide to Industrial Control Systems (ICS) Security, May 2015: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf>
- [R4] National Institute of Technology (NIST) Interagency "Guidelines on Firewalls and Firewall Policy, NIST Special Publication 800-41", October 2009: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf>

[R5] NIST SP 800-88, Guidelines for Media Sanitization, September 2006: [http://ws680.nist.gov/publication/get\\_pdf.cfm?pub\\_id=50819](http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=50819)

[R6] Cybersecurity Best Practices for Modern Vehicles - NHTSA: [https://www.nhtsa.gov/staticfiles/nvs/pdf/812333\\_CybersecurityForModernVehicles.pdf](https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf)

[R7] A Summary of Cybersecurity Best Practices - Homeland Security: <https://www.hsdl.org/?view&did=806518>

[R8] Characterization of Potential Security Threats in Modern Automobiles - NHTSA: [https://www.nhtsa.gov/DOT/NHTSA/NVS/Crash%20Avoidance/Technical%20Publications/2014/812074\\_Characterization\\_PotentialThreatsAutos\(1\).pdf](https://www.nhtsa.gov/DOT/NHTSA/NVS/Crash%20Avoidance/Technical%20Publications/2014/812074_Characterization_PotentialThreatsAutos(1).pdf)

[R9] Threat Modeling for Automotive Security Analysis: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf>

## 6.3 Configuring user permissions through profiles

The user profile can be defined when creating a new users or changed when modifying an existing one.

Refer to the section [Contextual help>>>Settings>>>Local users](#) in the settings.

## 6.4 Decommissioning the Network Management module

With the increased frequency of reported data breaches, it's becoming more and more necessary for companies to implement effective and reliable decommissioning policies and procedures.

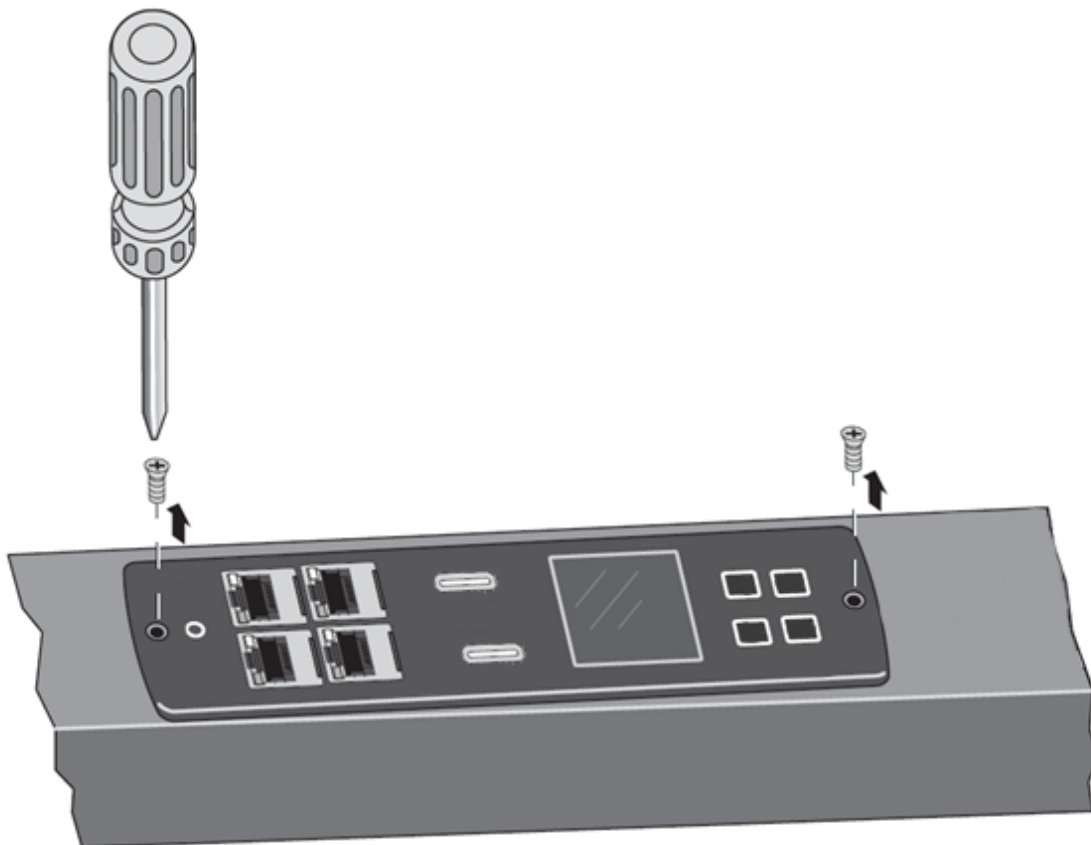
In order to protect the data stored on retired IT equipment from falling into the wrong hands, or a data breach, we recommend to follow below decommissioning steps:

### 1- Sanitize the Network Module

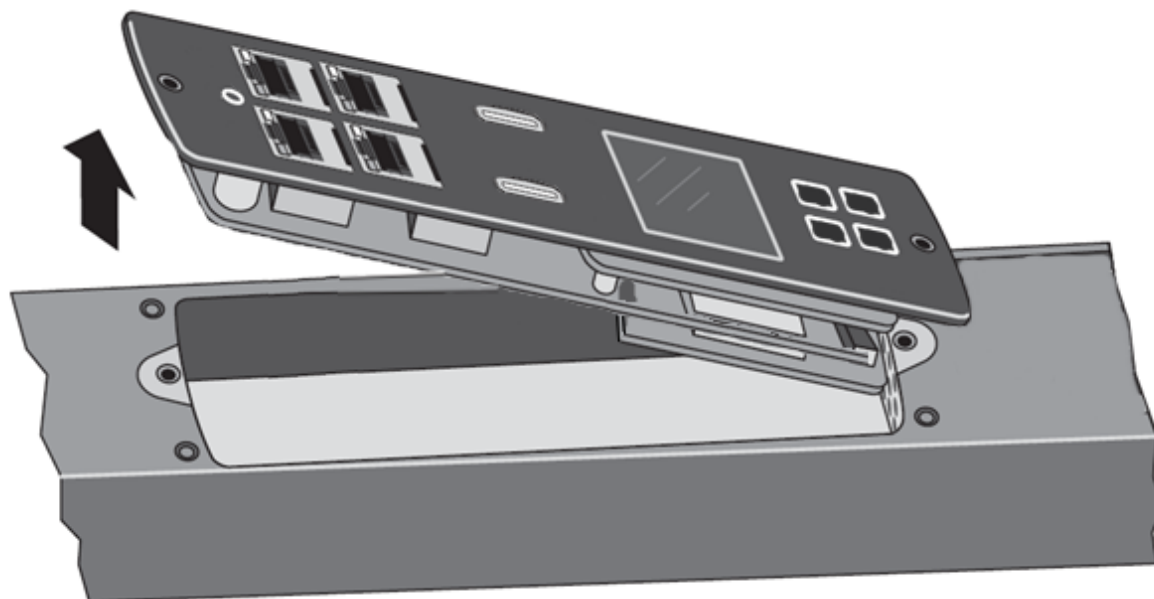
Sanitization erases all the data (user name and password, certificates, keys, settings, logs...).

To sanitize the Network Module refer to the [Contextual help>>>Maintenance>>>Services>>>Sanitization](#) section.

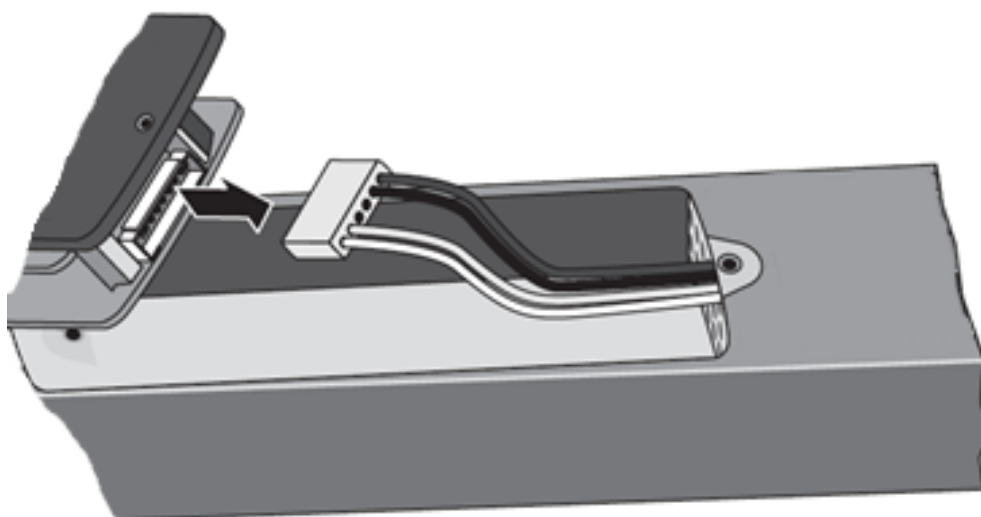
### 2- Remove the two GNM mounting screws.



3- Tilt up one side of the GNM and locate the attached cable harness.



4- Disconnect the cable harness and remove the GNM.





## 7 Servicing the EMP

### 7.1 Description and features

The optional Environmental Monitoring Probe EMPDT1H1C2 enables you to collect temperature and humidity readings and monitor the environmental data remotely.

You can also collect and retrieve the status of one or two dry contact devices (not included).

Up to 3 Environmental Monitoring Probe can be daisy chained on one device.

You can monitor readings remotely using SNMP or a standard Web browser through the Network module.

This provides greater power management control and flexible monitoring options.

The EMP device is delivered with a screw and screw anchor, nylon fasteners, tie wraps, and magnets. You can install the device anywhere on the rack or on the wall near the rack.



For more information, refer to the device manual.

The EMP has the following features:

- The hot-swap feature simplifies installation by enabling you to install the probe safely without turning off power to the device or to the loads that are connected to it.
- The EMP monitors temperature and humidity information to help you protect critical equipment.
- The EMP measures temperatures from 0°C to 70°C with an accuracy of  $\pm 2^\circ\text{C}$ .
- The EMP measures relative humidity from 10% to 90% with an accuracy of  $\pm 5\%$ .
- The EMP can be located some distance away from the device with a CAT5 network cable up to 50m (165 ft) long.
- The EMP monitors the status of the two user-provided contact devices.
- Temperature, humidity, and contact closure status can be displayed through a Web browser through the Network module or LCD interface (if available)
- A Temperature and Humidity Offset can be set.

### 7.2 Unpacking the EMP

The EMPDT1H1C2 sensor will include the following:

- Dry contact terminal block
- Installation instructions
- Wall mounting screw and anchor
- Rack mounting screw nut and washer
- Tie wraps (x2)
- Nylon fastener



Packing materials must be disposed of in compliance with all local regulations concerning waste. Recycling symbols are printed on the packing materials to facilitate sorting.

### 7.3 Installing the EMP

#### 7.3.1 Defining EMPs address and termination

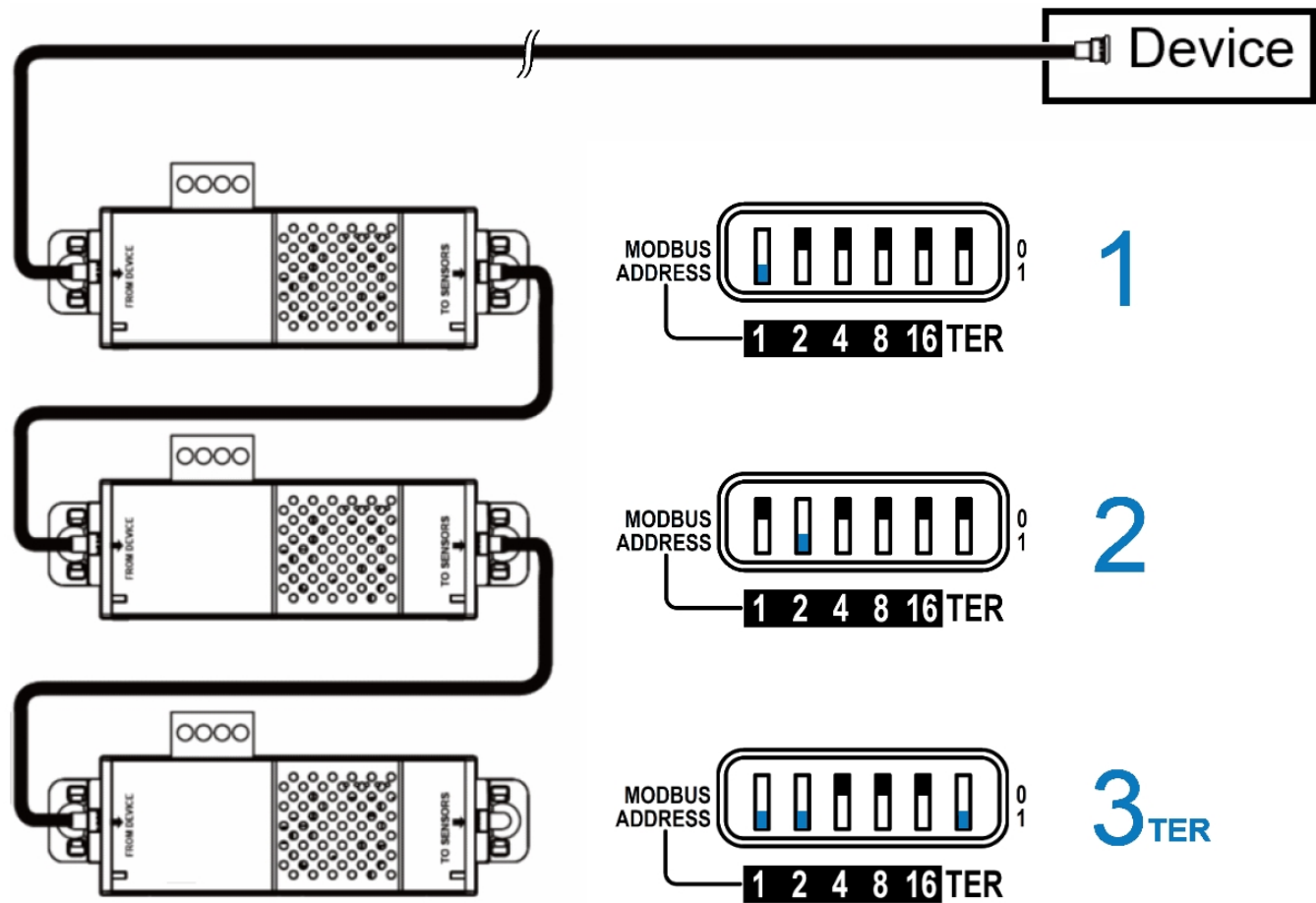
##### 7.3.1.1 Manual addressing



Address must be defined before the EMP power-up otherwise the changes won't be taken into account. Do not set Modbus address to 0, otherwise the EMP will not be detected.

Define **different address** for all the EMPs in the daisy-chain.  
Set the RS485 termination (TER) to 1 on the last EMP of the daisy chain, set it to 0 on all the other EMPs.

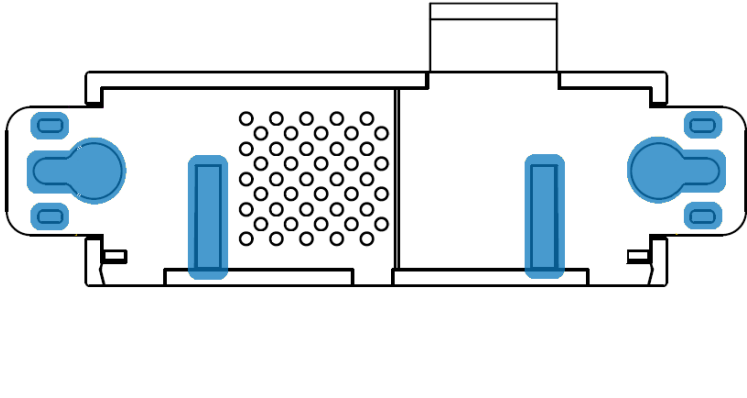
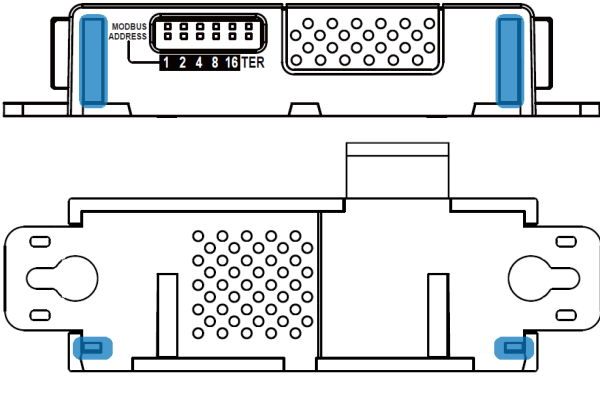
7.3.1.1.1 Example: manual addressing of 3 EMPs connected to the Device



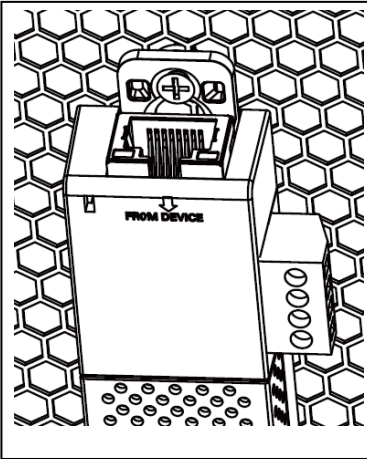
Green LED of the TO DEVICE RJ45 connector shows if the EMP is powered by the Network module.

7.3.2 Mounting the EMP

The EMP includes magnets, cable ties slots and keyholes to enable multiple ways of mounting it on your installation.

<p>Bottom mounting capabilities:</p> <ul style="list-style-type: none"><li>• magnets</li><li>• keyholes</li><li>• tie wraps</li><li>• nylon fastener</li></ul>	<p>Side mounting:</p> <ul style="list-style-type: none"><li>• magnets</li><li>• tie wraps</li></ul>
 <p>A top-down diagram of the EMP device showing various mounting points. On the left and right sides, there are blue circular magnets. In the center, there are two vertical blue rectangular keyholes. The bottom edge features a series of small circles representing tie wrap slots. A central rectangular cutout is also visible.</p>	 <p>A side-view diagram of the EMP device. The top section shows a 'MODBUS ADDRESS' switch with positions 1, 2, 4, 8, 16, and TER. Below this, there are blue rectangular magnets on the left and right sides. The bottom section shows the device's profile with blue circular magnets at the base corners. The central cutout and tie wrap slots are also visible from this perspective.</p>

7.3.2.1 Rack mounting with keyhole example

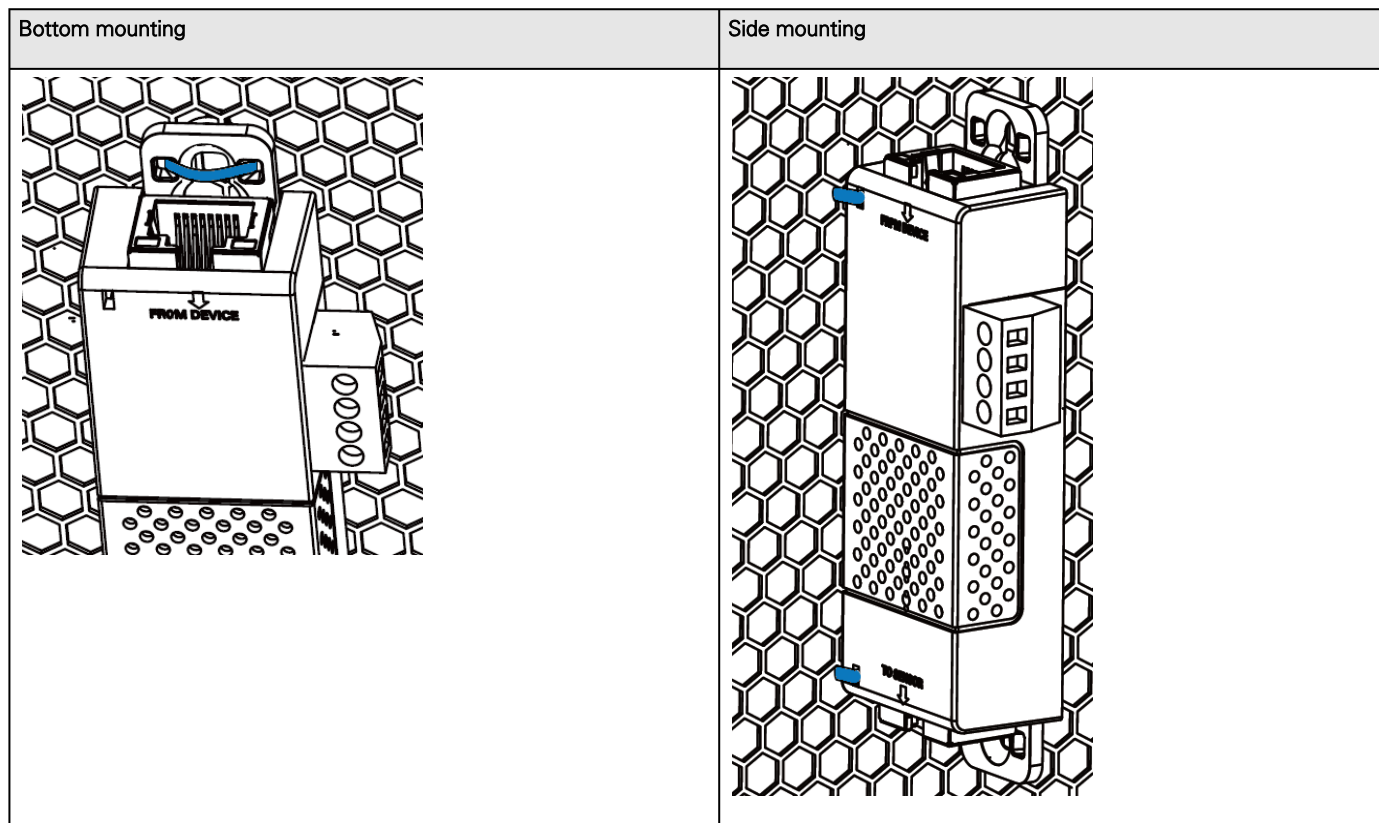


A diagram showing the EMP device being mounted into a rack. The device is positioned within a rack slot, and a screw is being used to secure it. The rack has a honeycomb pattern. A label 'FROM DEVICE' with an arrow points to the top of the EMP unit.

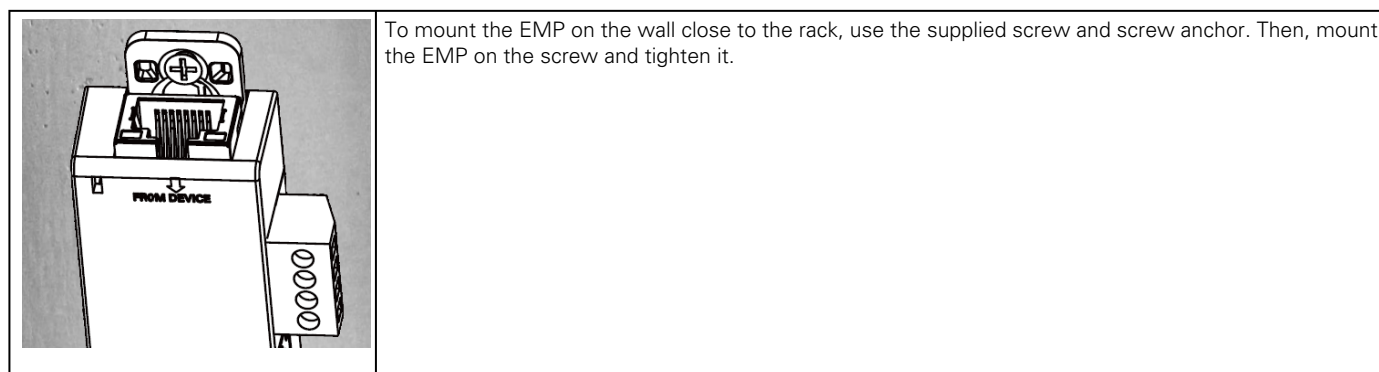
To mount the EMP on the rack, use the supplied screw, washer and nut. Then, mount the EMP on the screw and tighten it.

7.3.2.2 Rack mounting with tie wraps example

To mount the EMP on the door of the rack, use the supplied cable ties.



### 7.3.2.3 Wall mounting with screws example

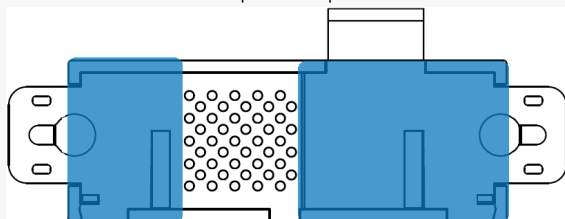


### 7.3.2.4 Wall mounting with nylon fastener example

To mount the EMP within the enclosure environment, attach one nylon fastener to the EMP and the other nylon fastener to an enclosure rail post. Then, press the two nylon strips together to secure the EMP to the rail post.



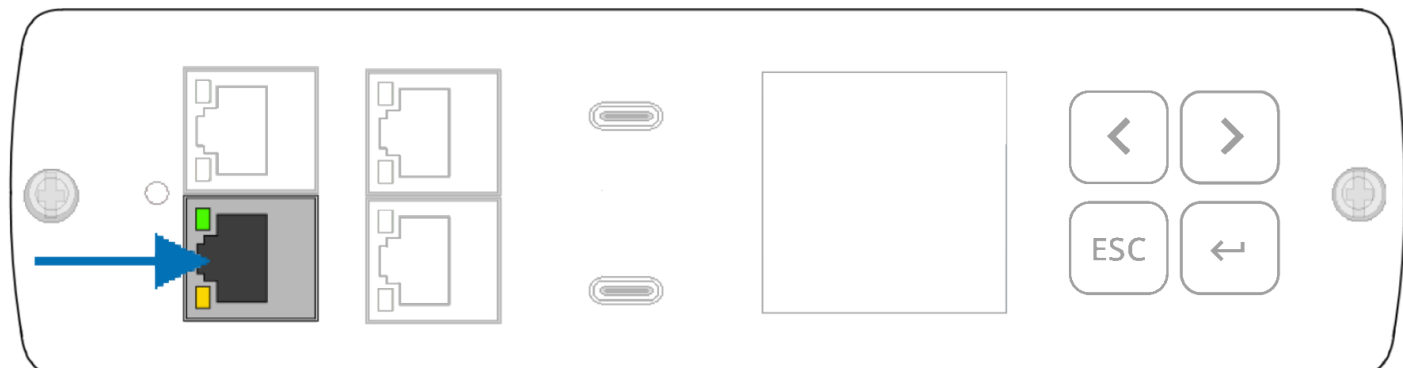
Cut nylon fastener and stick it on the EMP bottom on the location highlighted below; this will prevent it from interfering with the EMP data acquisition parts.



## 7.3.3 Cabling the first EMP to the device

### 7.3.3.1 Available Devices

#### 7.3.3.1.1 GNM PDU control module



### 7.3.3.2 Connecting the EMP to the device

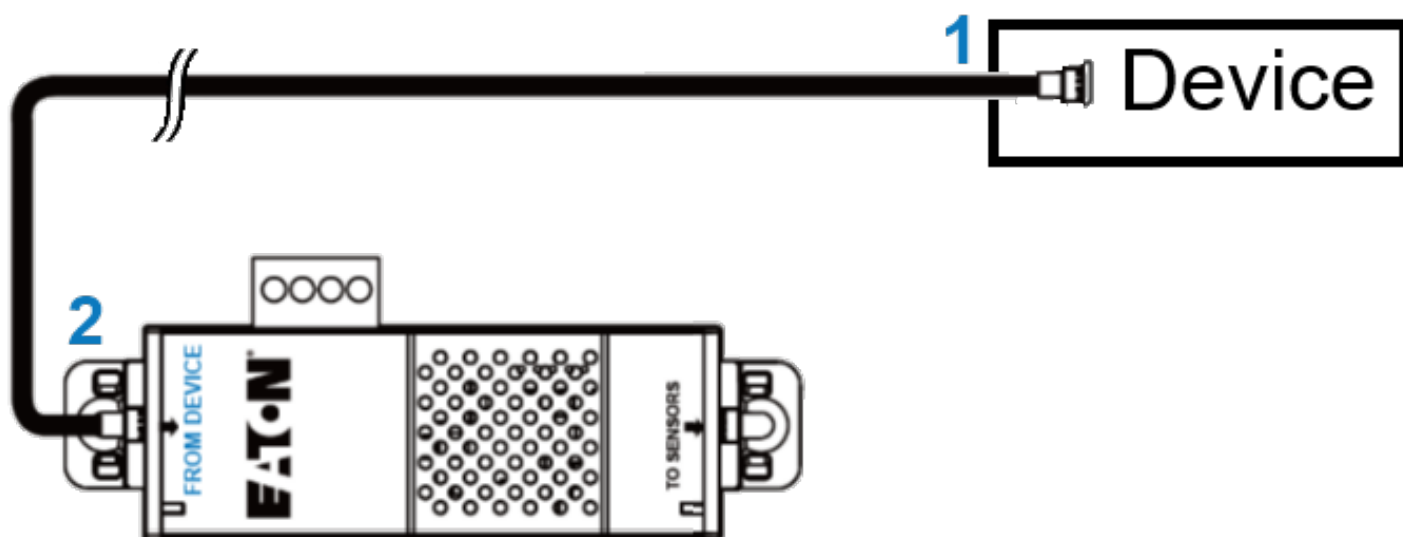


Address must be defined before the EMP power-up otherwise the changes won't be taken into account.  
Do not set Modbus address to 0, otherwise the EMP will not be detected.

#### 7.3.3.2.1 Material needed:

- EMP
- RJ45 female/female connector (supplied in EMP accessories)
- USB to RS485 converter cable (supplied in EMP accessories)
- Ethernet cable (**not supplied**).
- Device

#### 7.3.3.2.2 Connection steps



**STEP 1** – Connect the Ethernet cable to the RJ45 port of the Device.

**STEP 2** – Connect the other end of the Ethernet cable to the RJ-45 port on the EMP (FROM DEVICE).

## 7.3.4 Daisy chaining EMPs

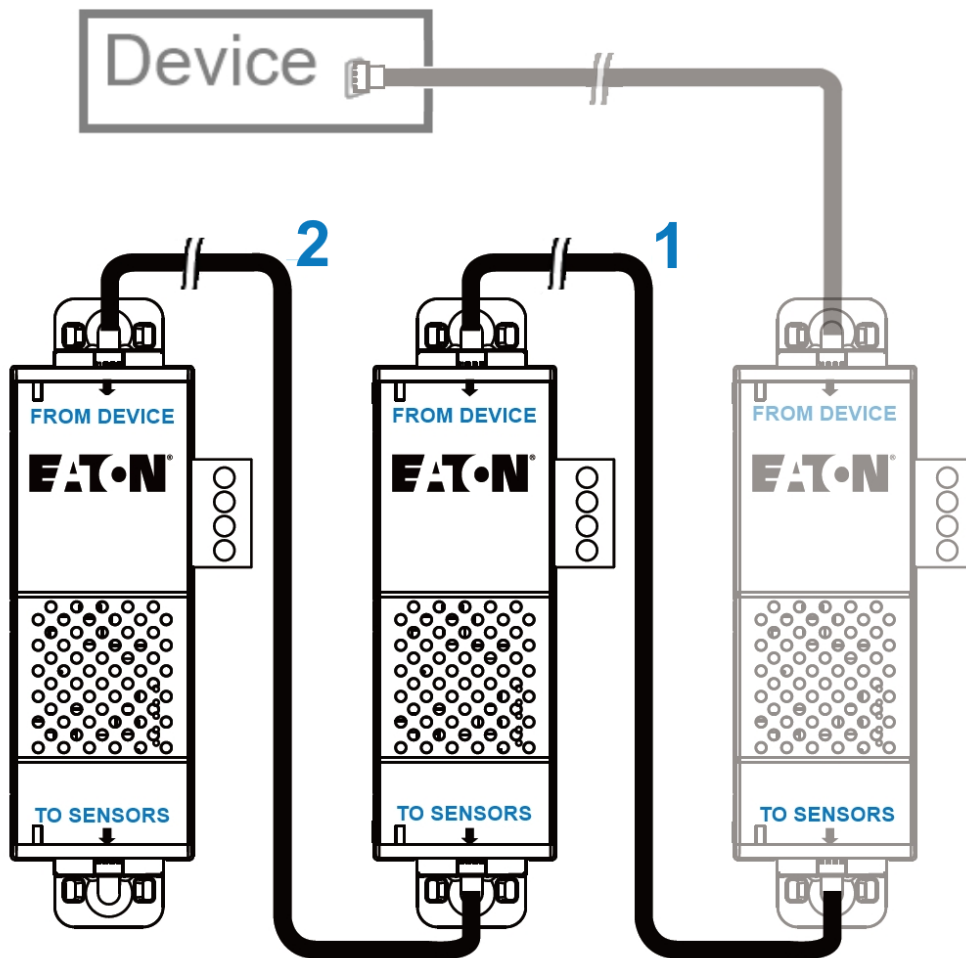


Address must be defined before EMP power-up; otherwise, the changes will not be applied.  
Do not set Modbus address to 0; otherwise, the EMP will not be detected.

### 7.3.4.1 Material needed:

- First EMP connected to the device (refer to previous section)
- Additional EMPs
- 2 x Ethernet cable (**not supplied**).
- Device

### 7.3.4.2 Connection steps



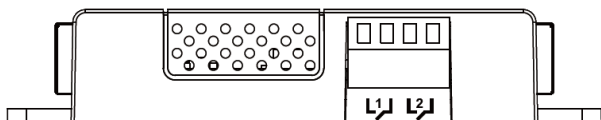
**STEP 1** – Connect the Ethernet cable to the "TO SENSORS" port of the first EMP, and to the "FROM DEVICE" port of the second EMP.

**STEP 2** – Connect the Ethernet cable to the "TO SENSORS" port of the second EMP, and to the "FROM DEVICE" port of the third EMP.



Up to 3 EMP can be daisy chained on one device.

## 7.3.5 Connecting an external contact device



To connect an external device to the EMP:

**STEP 1** – Connect the external contact closure inputs to the terminal block on the EMP (see the table and the figure below):

- External contact device 1. Connect the return and signal input wires from device 1 to screw terminals 1.
- External contact device 2. Connect the return and signal input wires from device 2 to screw terminals 2.

**STEP 2** – Tighten the corresponding tightening screws on top of the EMP to secure the wires.

## 7.4 Commissioning the EMP

### 7.4.1 On the Network Module device

**STEP 1** – Connect to the Network Module

- On a network computer, launch a supported web browser. The browser window appears.
- In the Address/Location field, enter: <https://xxx.xxx.xxx.xxx/> where xxx.xxx.xxx.xxx is the IP address of the Network Module.
- The log in screen appears.
- Enter the user name in the User Name field.
- Enter the password in the Password field.
- Click **Login**. The Network Module web interface appears.

**STEP 2** – Navigate to Environment menu:



**STEP 3** – Proceed to the commissioning, refer to the contextual help for details.

- Click **Discover**. The EMP connected to the Network module appears in the table.



When discovered, the orange LEDs of the EMP RJ45 connectors shows the data traffic.  
If the discovery process fails refer to the troubleshooting section.

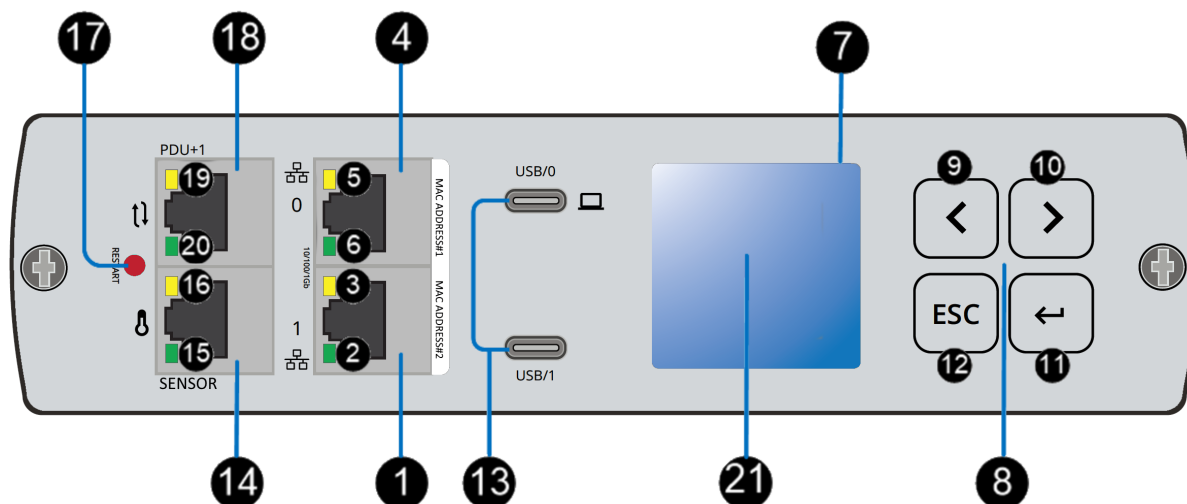
- Press the pen logo to edit EMP information and access its settings.
- Click **Define offsets** to define temperature or humidity offsets if needed.

**STEP 4** – Define alarm configuration, refer to the contextual help for details.

- Select the **Alarm configuration** page.
- Enable or disable alarms.
- Define thresholds, hysteresis and severity of temperature, humidity and dry contacts alarms.




## 8 Information

### 8.1 Front panel connectors and LED indicators



Nbr	Name	Description
1	Network connector	Ethernet port 1
2	Network speed LED	Flashing green sequences: <ul style="list-style-type: none"> <li>1 flash — Port operating at 10Mbps</li> <li>2 flashes — Port operating at 100Mbps</li> <li>3 flashes — Port operating at 1Gbps</li> </ul>
3	Network link/activity LED	<ul style="list-style-type: none"> <li>Off — PDU Network Module is not connected to the network.</li> <li>Solid yellow — PDU Network Module is connected to the network, but no activity detected.</li> <li>Flashing yellow — PDU Network Module is connected to the network and sending or receiving data.</li> </ul>
4	Network connector	Ethernet port 0
5	Network speed LED	Flashing green sequences: <ul style="list-style-type: none"> <li>1 flash — Port operating at 10Mbps</li> <li>2 flashes — Port operating at 100Mbps</li> <li>3 flashes — Port operating at 1Gbps</li> </ul>
6	Network link/activity LED	<ul style="list-style-type: none"> <li>Off — PDU Network Module is not connected to the network.</li> <li>Solid yellow — PDU Network Module is connected to the network, but no activity detected.</li> <li>Flashing yellow — PDU Network Module is connected to the network and sending or receiving data.</li> </ul>



<b>7</b>	LCD display	The LCD display provides information about load status, events, measurements, identification, and settings. The LCD interface also provides some basic configuration.
<b>8</b>	Navigation buttons	Navigate through the display with buttons.
<b>9</b>	Down	Press to scroll down on screen or menu.
<b>10</b>	Up	Press to scroll up on screen or menu.
<b>11</b>	Enter	Press it to select settings, enter a menu, or leave screen saver mode.
<b>12</b>	Escape	Press it to escape selection, leave a menu, or return to start-up screen.
<b>13</b>	USB-C connectors	<p>USB/0  : Configuration port.</p> <p>Access to Network Module's web interface through RNDIS (Emulated Network port).</p> <p>Access to the Network Module console through Serial (Emulated Serial port).</p> <p>USB/0 and USB/1 : Network Module accessories ports.</p> <hr/> <p> <b>Do not use for general power supply or USB charger.</b></p> <hr/>
<b>14</b>	EMP port	To connect EMP sensor to the PDU Network module.
<b>15</b>	Power LED	<ul style="list-style-type: none"> <li>Off — PDU Network Module is not powering the EMP.</li> <li>Solid green — PDU Network Module is powering the EMP.</li> </ul>
<b>16</b>	Activity LED	<ul style="list-style-type: none"> <li>Off — PDU Network Module is not connected to the EMP.</li> <li>Flashing yellow — PDU Network Module is connected to the EMP receiving data.</li> </ul>
<b>17</b>	Restart button	<p>Ball point pen or equivalent will be needed to restart:</p> <ul style="list-style-type: none"> <li>Short press (&lt;6s) — Safe software restart (firmware safely shutdown before restart).</li> <li>Long press (&gt;9s) — Forced hardware restart.</li> </ul> <hr/> <p> Restarting the Network module does not affect the power to the PDU outlets.</p> <hr/>
<b>18</b>	Power redundancy (PDU +1)	
<b>19</b>	Power redundancy status	<ul style="list-style-type: none"> <li>Off — no active redundancy</li> <li>Solid yellow — the PDU Network Module is powered by another PDU Network Module through the redundancy port.</li> </ul>

20	Power redundancy readiness	<ul style="list-style-type: none"> <li>Off — PDU Network Module is not connected to another PDU.</li> <li>Solid green — The PDU Network Module is connected to another PDU Network Module power redundancy port.</li> </ul>
----	----------------------------	---

## 8.2 Specifications/Technical characteristics

Module performance	
Date/Time backup	The RTC (CR1220 battery) is able to keep the date and the time when Network Module is OFF.
Functions	
Languages	English, French, German, Italian, Japanese, Russian, Simplified Chinese, Spanish, Traditional Chinese
Alarms/Log	Email, SNMP trap, web interface / Log on events
Network	Gigabit ETHERNET, 10/100/1000Mb/s, auto neg., HTTP 1.1, SNMP V1, SNMP V3, NTP, SMTP, DHCP
Security	Restricted to TLS 1.2
Supported MIBs	<i>PDU MIB / Sensor MIB</i>
Browsers	Google Chrome, Firefox, Safari
Settings (default values)	
IP network	DHCP enabled   NTP server: <a href="http://pool.ntp.org">pool.ntp.org</a>
Port	443 (https), 22 (ssh), 161 (snmp), 162 (snmp trap), 25 (smtp), 8883 (mqtt), 123 (ntp), 5353 (mdns-sd), 80 (http), 514 (syslog), 636 (LDAP), 1812 (RADIUS)
Web interface access control	User name: admin   Password: admin
Settings/Device data connector	USB RNDIS Apipa compatible   IP address: 169.254.0.1   Subnet mask: 255.255.0.0

## 8.3 Default settings and possible parameters

### 8.3.1 Meters

Default settings and possible parameters - Meters		
	Default setting	Possible parameters
Meters/Logs	Log measures every — 60s	Log measures every — 3600s maximum

## 8.3.2 Settings

### Default settings and possible parameters - General

	Default setting	Possible parameters
<b>System details</b>	Location — empty Contact — empty System name — empty Time & date settings — Manual (Time zone: Europe/Paris)	Location — 31 characters maximum Contact — 255 characters maximum System name — 255 characters maximum Time & date settings — Manual (Time zone: selection on map/Date) / Dynamic (NTP)
<b>Email notification settings</b>	No email	5 configurations maximum Custom name — 128 characters maximum Email address — 128 characters maximum Hide IP address from the email body — enable/disabled Status — Active/Inactive <ul style="list-style-type: none"> <li>Alarm notifications               <ul style="list-style-type: none"> <li>Active — No/Yes</li> <li>All card events – Subscribe/Attach logs</li> <li>Critical alarm – Subscribe/Attach logs</li> <li>Warning alarm – Subscribe/Attach logs</li> <li>Info alarm – Subscribe/Attach logs</li> </ul> </li> <li>All device events – Subscribe/Attach measures/Attach logs</li> <li>Critical alarm – Subscribe/Attach measures/Attach logs</li> <li>Warning alarm – Subscribe/Attach measures/Attach logs</li> <li>Info alarm – Subscribe/Attach measures/Attach logs</li> <li>Always notify events with code</li> <li>Never notify events with code</li> <li>Schedule report               <ul style="list-style-type: none"> <li>Active — No/Yes</li> <li>Recurrence – Every day/Every week/Every month</li> <li>Starting – Date and time</li> <li>Card events – Subscribe/Attach logs</li> <li>Device events – Subscribe/Attach measures/Attach logs</li> </ul> </li> </ul>

<b>SMTP settings</b>	Server IP/Hostname — blank SMTP server authentication — disabled Port — 25 Default sender address — <a href="mailto:device@networkcard.com">device@networkcard.com</a> Hide IP address from the email body — disabled Security — enabled Verify certificate authority — disabled SMTP server authentication — disabled	Server IP/Hostname — 128 characters maximum SMTP server authentication — disable/enable (Username/Password — 128 characters maximum) Port — x-xxx Sender address — 128 characters maximum Hide IP address from the email body — enable/disabled Secure SMTP connection — enable/disable Verify certificate authority — disable/enable
----------------------	---	---

### Default settings and possible parameters - Global user settings and Local users

	Default setting	Possible parameters
<b>Password settings</b>	Minimum length — enabled (8) Minimum upper case — enabled (1) Minimum lower case — enabled (1) Minimum digit — enabled (1) Special character — enabled (1)	Minimum length — enable (6-32)/disable Minimum upper case — enable (0-32)/disable Minimum lower case — enable (0-32)/disable Minimum digit — enable (0-32)/disable Special character — enable (0-32)/disable
<b>Password expiration</b>	Number of days until password expires — disabled Main administrator password never expires — disabled	Number of days until password expires — disable/enable (1-99999) Main administrator password never expires — disable/enable
<b>Lock account</b>	Lock account after xx invalid tries — disabled Main administrator account never blocks — disabled	Lock account after xx invalid tries — disable/enable (1-99) Main administrator account never blocks — disable/enable
<b>Account timeout</b>	No activity timeout — 60 minutes Session lease time — 120 minutes	No activity timeout — 1-60 minutes Session lease time — 60-720 minutes
<b>Local users</b>	1 user only: <ul style="list-style-type: none"> <li>Active — Yes</li> <li>Profile — Administrator</li> <li>Username — admin</li> <li>Full Name — blank</li> <li>Email — blank</li> <li>Phone — blank</li> <li>Organization — blank</li> </ul>	20 users maximum: <ul style="list-style-type: none"> <li>Active — Yes/No</li> <li>Profile — Administrator/Operator/Viewer</li> <li>Username — 255 characters maximum</li> <li>Full Name — 128 characters maximum</li> <li>Email — 128 characters maximum</li> <li>Phone — 64 characters maximum</li> <li>Organization — 128 characters maximum</li> </ul>

### Default settings and possible parameters - Remote users

	Default setting	Possible parameters
--	-----------------	---------------------

LDAP	<p>Configure</p> <ul style="list-style-type: none"> <li>• Active – No</li> <li>• Security           <ul style="list-style-type: none"> <li>SSL – SSL</li> <li>Verify server certificate – enabled</li> </ul> </li> <li>• Primary server           <ul style="list-style-type: none"> <li>Name – Primary</li> <li>Hostname – blank</li> <li>Port – 636</li> </ul> </li> <li>• Secondary server           <ul style="list-style-type: none"> <li>Name – blank</li> <li>Hostname – blank</li> <li>Port – blank</li> </ul> </li> <li>• Credentials           <ul style="list-style-type: none"> <li>Anonymous search bind – disabled</li> <li>Search user DN – blank</li> <li>Password – blank</li> </ul> </li> <li>• Search base           <ul style="list-style-type: none"> <li>Search base DN – dc=example,dc=com</li> </ul> </li> <li>• Request parameters           <ul style="list-style-type: none"> <li>User base DN – ou=people,dc=example,dc=com</li> <li>User name attribute – uid</li> <li>UID attribute – uidNumber</li> <li>Group base DN – ou=group,dc=example,dc=com</li> <li>Group name attribute – gid</li> <li>GID attribute – gidNumber</li> </ul> </li> </ul> <p>Profile mapping – no mapping</p> <p>Users preferences</p> <ul style="list-style-type: none"> <li>• Language – English</li> <li>• Temperature unit – °C (Celsius)</li> <li>• Date format – m/d/Y</li> <li>• Time format – hh:mm:ss (24h)</li> </ul>	<p>Configure</p> <ul style="list-style-type: none"> <li>• Active – No/yes</li> <li>• Security           <ul style="list-style-type: none"> <li>SSL – None/Start TLS/SSL</li> <li>Verify server certificate – disabled/enabled</li> </ul> </li> <li>• Primary server           <ul style="list-style-type: none"> <li>Name – 128 characters maximum</li> <li>Hostname – 128 characters maximum</li> <li>Port – x-xxx</li> </ul> </li> <li>• Secondary server           <ul style="list-style-type: none"> <li>Name – 128 characters maximum</li> <li>Hostname – 128 characters maximum</li> <li>Port – x-xxx</li> </ul> </li> <li>• Credentials           <ul style="list-style-type: none"> <li>Anonymous search bind – disabled/enabled</li> <li>Search user DN – 1024 characters maximum</li> <li>Password – 128 characters maximum</li> </ul> </li> <li>• Search base           <ul style="list-style-type: none"> <li>Search base DN – 1024 characters maximum</li> </ul> </li> <li>• Request parameters           <ul style="list-style-type: none"> <li>User base DN – 1024 characters maximum</li> <li>User name attribute – 1024 characters maximum</li> <li>UID attribute – 1024 characters maximum</li> <li>Group base DN – 1024 characters maximum</li> <li>Group name attribute – 1024 characters maximum</li> <li>GID attribute – 1024 characters maximum</li> </ul> </li> </ul> <p>Profile mapping – up to 5 remote groups mapped to local profiles</p> <p>Users preferences</p> <ul style="list-style-type: none"> <li>• Language – English, French, German, Italian, Japanese, Russian, Simplified Chinese, Spanish, Traditional Chinese</li> <li>• Temperature unit – °C (Celsius)/°F (Fahrenheit)</li> <li>• Date format – MM-DD-YYYY / YYYY-MM-DD / DD-MM-YYY / DD.MM.YYY / DD/MM/YYYY / DD MM YYYY</li> <li>• Time format – hh:mm:ss (24h) / hh:mm:ss (12h)</li> </ul>
------	---	--

RADIUS	Configure	Configure
	<ul style="list-style-type: none"> <li>Active – No</li> <li>Retry number – 0</li> <li>Primary server               <ul style="list-style-type: none"> <li>Name – blank</li> <li>Secret – blank</li> <li>Address – blank</li> <li>UDP port – 1812</li> <li>Time out – 3</li> </ul> </li> <li>Secondary server               <ul style="list-style-type: none"> <li>Name – blank</li> <li>Secret – blank</li> <li>Address – blank</li> <li>UDP port – 1812</li> <li>Time out – 3</li> </ul> </li> </ul> <p>Users preferences</p> <ul style="list-style-type: none"> <li>Language – English</li> <li>Temperature unit – °C (Celsius)</li> <li>Date format – m/d/Y</li> <li>Time format – hh:mm:ss (24h)</li> </ul>	<ul style="list-style-type: none"> <li>Active – Yes/No</li> <li>Retry number – 0 to 128</li> <li>Primary server               <ul style="list-style-type: none"> <li>Name – 128 characters maximum</li> <li>Address – 128 characters maximum</li> <li>Secret – 128 characters maximum</li> <li>UDP port – 1 to 65535</li> <li>Time out – 3 to 60</li> </ul> </li> <li>Secondary server               <ul style="list-style-type: none"> <li>Name – 128 characters maximum</li> <li>Address – 128 characters maximum</li> <li>Secret – 128 characters maximum</li> <li>UDP port – 1 to 65535</li> <li>Time out – 3 to 60</li> </ul> </li> </ul> <p>Users preferences</p> <ul style="list-style-type: none"> <li>Language – English, French, German, Italian, Japanese, Russian, Simplified Chinese, Spanish, Traditional Chinese</li> <li>Temperature unit – °C (Celsius)</li> <li>Date format – MM-DD-YYYY</li> <li>Time format – hh:mm:ss (24h)</li> </ul>

### Default settings and possible parameters - Ports

	Default setting	Possible parameters
Ports- Ethernet port mode	Cascade Mode	Cascade Mode / Dual Mode
Ports- Ethernet port	Auto negotiation	Auto negotiation / 10Mbps - Half duplex / 10Mbps - Full duplex / 100Mbps - Half duplex / 100Mbps - Full duplex / 1.0Gbps - Full duplex
Ports- Serial console	Enabled	Enabled / Disabled

### Default settings and possible parameters - Firewall

	Default setting	Possible parameters
Firewall - WEB	State : Active Port : 80 Address Filter : Empty	Active / Inactive Integer IP address
Firewall - Secure WEB	State : Active Port : 443 Address Filter : Empty	Active / Inactive Integer IP address

<b>Firewall - SSH</b>	State : Active Port : 22 Address Filter : Empty	Active / Inactive Integer IP address
<b>Firewall - SNMP</b>	State : Active Port : 161 Address Filter : Empty	Active / Inactive Integer IP address
<b>Firewall - MQTT</b>	State : Active Port : 8883 Address Filter : Empty	Active / Inactive Integer IP address
<b>Firewall - ICMP V4</b>	State : Active Address Filter : Empty	Active / Inactive IP address
<b>Firewall - ICMP V6</b>	State : Active Address Filter : Empty	Active / Inactive IP address

### Default settings and possible parameters - Firewall

	Default setting	Possible parameters
<b>Firewall - WEB</b>	State : Active Port : 80 Address Filter : Empty	Active / Inactive Integer IP address
<b>Firewall - Secure WEB</b>	State : Active Port : 443 Address Filter : Empty	Active / Inactive Integer IP address
<b>Firewall - SSH</b>	State : Active Port : 22 Address Filter : Empty	Active / Inactive Integer IP address
<b>Firewall - SNMP</b>	State : Active Port : 161 Address Filter : Empty	Active / Inactive Integer IP address
<b>Firewall - MQTT</b>	State : Active Port : 8883 Address Filter : Empty	Active / Inactive Integer IP address
<b>Firewall - ICMP V4</b>	State : Active Address Filter : Empty	Active / Inactive IP address
<b>Firewall - ICMP V6</b>	State : Active Address Filter : Empty	Active / Inactive IP address

**Default settings and possible parameters - SNMP**

	Default setting	Possible parameters
<b>SNMP</b>	Activate SNMP — disabled Port — 161 SNMP V1 — disabled <ul style="list-style-type: none"> <li>Community #1 — public Enabled — Inactive Access — Read only</li> <li>Community #2 — private Enabled — Inactive Access — Read/Write</li> </ul> SNMP V3 — enabled <ul style="list-style-type: none"> <li>User #1 — readonly Enabled — Inactive Access — Read only Authentication — Auth (SHA-1) Password — empty Confirm password — empty Privacy — Secured - AES Key — empty Confirm key — empty</li> <li>User#2 — readwrite Enabled — Inactive Access — Read/Write Authentication — Auth (SHA-1) Password — empty Confirm password — empty Privacy — Secured - AES Key — empty Confirm key — empty</li> </ul>	Activate SNMP — disable/enable Port — x-xxx SNMP V1 — disable/enable <ul style="list-style-type: none"> <li>Community #1 — 128 characters maximum Enabled — Inactive/Active Access — Read only</li> <li>Community #2 — 128 characters maximum Enabled — Inactive/Active Access — Read/Write</li> </ul> SNMP V3 — disable/enable <ul style="list-style-type: none"> <li>User #1 — 32 characters maximum Enabled — Inactive/Active Access — Read only/Read-Write Authentication — Auth (SHA-1)/None Password — 128 characters maximum Confirm password — 128 characters maximum Privacy — Secured - AES/None Key — 128 characters maximum Confirm key — 128 characters maximum</li> <li>User#2 — 32 characters maximum Enabled — Inactive/Active Access — Read only/Read-Write Authentication — Auth (SHA-1)/None Password — 128 characters maximum Confirm password — 128 characters maximum Privacy — Secured - AES/None Key — 128 characters maximum Confirm key — 128 characters maximum</li> </ul>
<b>Trap receivers</b>	No trap	Enabled — No/Yes Application name — 128 characters maximum Hostname or IP address — 128 characters maximum Port — x-xxx Protocol — V1/V2C/V3 Trap community — 128 characters maximum

**Default settings and possible parameters - Certificate**

	Default setting	Possible parameters
--	-----------------	---------------------



Local certificates	Common name — Service + Hostname + selfsigned	Common name — 64 characters maximum
	Country — FR	Country — Country code
	State or Province — 38	State or Province — 64 characters maximum
	City or Locality — Grenoble	City or Locality — 64 characters maximum
	Organization name — Eaton	Organization name — 64 characters maximum
	Organization unit — Power quality	Organization unit — 64 characters maximum
	Contact email address — blank	Contact email address — 64 characters maximum

### 8.3.3 Sensors alarm configuration

#### Default settings and possible parameters - Environment Alarm configuration

	Default setting	Possible parameters
Temperature	Enabled — No Low critical – 0°C/32°F Low warning – 10°C/50°F High warning – 70°C/158°F High critical – 80°C/176°F	Enabled — No/Yes low critical<low warning<high warning<high critical
Humidity	Enabled — No Low critical – 10% Low warning – 20% High warning – 80% High critical – 90%	Enabled — No/Yes 0%<low critical<low warning<high warning<high critical<100%
Dry contacts	Enabled — No Alarm severity – Warning	Enabled — No/Yes Alarm severity – Info/Warning/Critical

### 8.3.4 User profile

#### Default settings and possible parameters - User profile

	Default setting	Possible parameters
--	-----------------	---------------------

Profile	<div>Account details:</div> <ul style="list-style-type: none"><li>Full name — Administrator</li><li>Email — blank</li><li>Phone — blank</li><li>Organization — blank</li></ul> <div>Preferences:</div> <ul style="list-style-type: none"><li>Language — English</li><li>Date format — MM-DD-YYYY</li><li>Time format — hh:mm:ss (24h)</li><li>Temperature — °C (Celsius)</li></ul>	<div>Account details:</div> <ul style="list-style-type: none"><li>Full name — 128 characters maximum</li><li>Email — 128 characters maximum</li><li>Phone — 64 characters maximum</li><li>Organization — 128 characters maximum</li></ul> <div>Preferences:</div> <ul style="list-style-type: none"><li>Language — English, French, German, Italian, Japanese, Russian, Simplified Chinese, Spanish, Traditional Chinese</li><li>Date format — MM-DD-YYYY / YYYY-MM-DD / DD-MM-YYY / DD.MM.YYY / DD/MM/YYY / DD MM YYYY</li><li>Time format — hh:mm:ss (24h) / hh:mm:ss (12h)</li><li>Temperature — °C (Celsius)/°F (Fahrenheit)</li></ul>
---------	--	--

## 8.4 Access rights per profiles

### 8.4.1 Home

	Administrator	Operator	Viewer
Home	✓	✓	✓

### 8.4.2 Meters

	Administrator	Operator	Viewer
Logs configuration	✓	✓	✗

### 8.4.3 Controls

	Administrator	Operator	Viewer
Controls - Outlets	✓	✓	✗

	Administrator	Operator	Viewer
Controls - Group	✓	✓	✗

	Administrator	Operator	Viewer
Controls - Identify	✓	✓	✗

	Administrator	Operator	Viewer
Control - Schedule	✓	✓	✗

	Administrator	Operator	Viewer
Switching settings	✓	✓	✗

### 8.4.4 Environment

	Administrator	Operator	Viewer
Environment/Commissioning	✓	✓	✗
Environment/Status	✓	✓	✓

	Administrator	Operator	Viewer
Environment/Alarm configuration	✓	✓	✗

	Administrator	Operator	Viewer
Environment/Information	✓	✓	✓

## 8.4.5 Settings

	Administrator	Operator	Viewer
General	✓	✗	✗

	Administrator	Operator	Viewer
Local users	✓	✗	✗

	Administrator	Operator	Viewer
Remote users	✓	✗	✗

	Administrator	Operator	Viewer
Ports	✓	✗	✗

	Administrator	Operator	Viewer
Firewall	✓	✗	✗

	Administrator	Operator	Viewer
Protocols	✓	✗	✗

	Administrator	Operator	Viewer
--	---------------	----------	--------

TCP/IP	✓	✗	✗
--------	---	---	---

	Administrator	Operator	Viewer
SNMP	✓	✗	✗

	Administrator	Operator	Viewer
Certificate	✓	✗	✗

	Administrator	Operator	Viewer
PDU settings - General	✓	✓	✗

	Administrator	Operator	Viewer
PDU settings - Input thresholds	✓	✓	✗

	Administrator	Operator	Viewer
PDU settings - Branch thresholds	✓	✓	✗

	Administrator	Operator	Viewer
PDU settings - Outlet thresholds	✓	✓	✗

	Administrator	Operator	Viewer
PDU settings - Outlet switching	✓	✓	✗

	Administrator	Operator	Viewer
PDU settings - Group definition	✓	✓	✗

	Administrator	Operator	Viewer
--	---------------	----------	--------

PDU settings - Group thresholds	✓	✓	✗
---------------------------------	---	---	---

## 8.4.6 Maintenance

	Administrator	Operator	Viewer
System information	✓	✓	✓

	Administrator	Operator	Viewer
Firmware	✓	✗	✗

	Administrator	Operator	Viewer
Services	✓	✗	✗

	Administrator	Operator	Viewer
Resources	✓	✓	✓

	Administrator	Operator	Viewer
System logs	✓	✗	✗

## 8.4.7 Alarms

	Administrator	Operator	Viewer
Alarm list	✓	✓	✓
Export	✓	✓	✓
Clear	✓	✓	✗

## 8.4.8 User profile

	Administrator	Operator	Viewer
--	---------------	----------	--------

User profile	✓	✓	✓
	Administrator	Operator	Viewer
Legal information	✓	✓	✓

## 8.4.9 Contextual help

	Administrator	Operator	Viewer
Contextual help	✓	✓	✓
Full documentation	✓	✓	✓

## 8.4.10 CLI commands

	Administrator	Operator	Viewer
get release info	✓	✓	✓

	Administrator	Operator	Viewer
history	✓	✓	✓

	Administrator	Operator	Viewer
ldap-test	✓	✗	✗

	Administrator	Operator	Viewer
logout	✓	✓	✓

	Administrator	Operator	Viewer
maintenance	✓	✗	✗

	Administrator	Operator	Viewer
netconf	✓	✓ (read-only)	✓ (read-only)

	Administrator	Operator	Viewer
--	---------------	----------	--------

ping	✓	✗	✗
ping6	✓	✗	✗

	Administrator	Operator	Viewer
reboot	✓	✗	✗

	Administrator	Operator	Viewer
save_configuration	✓	✗	✗
restore_configuration	✓	✗	✗

	Administrator	Operator	Viewer
sanitize	✓	✗	✗

	Administrator	Operator	Viewer
ssh-keygen	✓	✗	✗

	Administrator	Operator	Viewer
time	✓	✓ (read-only)	✓ (read-only)

	Administrator	Operator	Viewer
traceroute	✓	✗	✗
traceroute6	✓	✗	✗

	Administrator	Operator	Viewer
whoami	✓	✓	✓

	Administrator	Operator	Viewer
email-test	✓	✗	✗

	Administrator	Operator	Viewer
--	---------------	----------	--------



systeminfo_statistics	✓	✓	✓
-----------------------	---	---	---

	Administrator	Operator	Viewer
certificates	✓	✗	✗

## 8.5 List of event codes

To get access to the Alarm log codes or the System log codes for email subscription, see sections below:

### 8.5.1 System log codes



To retrieve System logs, navigate to [Contextual help>>>Maintenance>>>System logs](#) section and press the **Download System logs** button.



Below codes are the one to be used to add "Exceptions on events notification" on email sending configurations. Some zeros maybe added in front of the code when displayed in emails or logs.

#### 8.5.1.1 Critical

Code	Severity	Log message	File
0801000	Alert	User account - admin password reset to default	logAccount.csv
0E00400	Critical	The [selfsign/PKI] signed certificate of the <service> server is not valid	logSystem.csv
0A00700	Error	Network module file system integrity corrupted <f/w: xx.yy.zzzz>	logUpdate.csv
0000D00	Error	Card reboot due to database error	logSystem.csv
0700200	Error	Failed to start execution of script "<script description>". Client not registered. (<script uuid>)	logSystem.csv
0700400	Error	Execution of script "<script description>" failed with return code: <script return code>. (<script uuid>)	logSystem.csv
0700500	Error	Execution of script "<script description>" timeout! (<script uuid>)	logSystem.csv
0700700	Alert	Failed to prepare isolated environment for script execution. Protection service startup is aborted.	logSystem.csv

#### 8.5.1.2 Warning

Code	Severity	Log message	File
0A00200	Warning	Network module upgrade failed <f/w: xx.yy.zzzz>	logUpdate.csv
0A00A00	Warning	Network module bootloader upgrade failed <f/w: xx.yy.zzzz>	logUpdate.csv

0B00500	Warning	RTC battery cell low	logSystem.csv
0E00200	Warning	New [self/PKI] signed certificate [generated/imported] for <service> server	logSystem.csv
0E00300	Warning	The [self/PKI] signed certificate of the <service> server will expires in <X> days	logSystem.csv
0800700	Warning	User account - password expired	logAccount.csv
0800900	Warning	User account- locked	logAccount.csv
0C00100	Warning	Unable to send email: Smtplib server is unknown	logSystem.csv
0C00200	Warning	Unable to send email: Authentication method is not supported	logSystem.csv
0C00300	Warning	Unable to send email: Authentication error	logSystem.csv
0C00500	Warning	Unable to send email: Certificate Authority not recognized	logSystem.csv
0C00600	Warning	Unable to send email: Secure connection required	logSystem.csv
0C00800	Warning	Unable to send email: Unknown error	logSystem.csv
0C00B00	Warning	Unable to send email: Recipient not specified	logSystem.csv
0F01300	Warning	Card reboot due to Device FW upgrade	logSystem.csv
1000F00	Warning	<feature> settings partial restoration	logSystem.csv
1001000	Warning	<feature> settings restoration error	logSystem.csv
1000C00	Warning	Settings partial restoration	logSystem.csv
1000D00	Warning	Settings restoration error	logSystem.csv
1200100	Warning	Authentication to remote server failed	logSystem.csv
1200200	Warning	Fetching configuration file failed with HTTP response: <http_code>	logSystem.csv
1200300	Warning	Fetching configuration file failed with cURL code: <curl_code>	logSystem.csv
1200400	Warning	<protocol_type> protocol is disabled	logSystem.csv
1200500	Warning	Config file is empty	logSystem.csv
1200600	Warning	Config file size <real_file_size> exceeds maximum of bytes <max_size>	logSystem.csv
1200800	Warning	Invalid url	logSystem.csv
1200900	Warning	Internal error	logSystem.csv
1200A00	Warning	Wrong config file format	logSystem.csv
1200B00	Warning	Config file has been applied partially	logSystem.csv
1200C00	Warning	Config file restore failed with SRR code: <code>	logSystem.csv

### 8.5.1.3 Info

Code	Severity	Log message	File
0300D00	Notice	User action - sanitization launched	logSystem.csv
0A00500	Notice	Network module sanitized	logUpdate.csv
0A00900	Notice	Network module bootloader upgrade success <f/w: xx.yy.zzzz>	logUpdate.csv
0A00B00	Notice	Network module bootloader upgrade started <f/w: xx.yy.zzzz>	logUpdate.csv
0A00C00	Notice	Periodic system integrity check started	logUpdate.csv
0B00100	Notice	Time manually changed	logSystem.csv
0B00700	Notice	NTP sever not available <NTP server address>	logSystem.csv
0900100	Notice	Session - opened	logSession.csv
0900200	Notice	Session - closed	logSession.csv
0900300	Notice	Session - invalid token	logSession.csv
0900400	Notice	Session - authentication failed	logSession.csv
0300F00	Notice	User action - network module admin password reset switch activated	logSystem.csv
0E00500	Notice	[Certificate authority/ Client certificate] <id> is added for <service>	logSystem.csv
0E00600	Notice	[Certificate authority/ Client certificate] <id> is revoked for <service>	logSystem.csv
0700100	Info	Start execution of script "<script description>". (<script uuid>)	logSystem.csv
0700300	Info	Execution of script "<script description>" succeeded. (<script uuid>)	logSystem.csv
0700600	Info/Notice/ Error/Debug	<Script execution log message>	logSystem.csv
0800100	Notice	User account - created <user account id>	logAccount.csv
0800200	Notice	User account - deleted <user account id>	logAccount.csv
0800400	Notice	User account - name changed <user account id>	logAccount.csv
0800600	Notice	User account - password changed	logAccount.csv
0800800	Notice	User account- password reset <user account id>	logAccount.csv
0800A00	Notice	User account- unlocked	logAccount.csv
0800B00	Notice	User account - activated <user account id>	logAccount.csv
0800C00	Notice	User account - deactivated <user account id>	logAccount.csv
0801401	Info	User account - Invalid credentials reserved username	logAccount.csv
0900D00	Notice	<user> connected into interactive CLI with session id XXXXXX	logSession.csv

0900E00	Notice	<user> disconnected from interactive CLI with session id XXXXXX	logSession.csv
0900F00	Notice	<user> doesn't have access to CLI - CLI session id XXXXXX	logSession.csv
0901000	Notice	<user> connected and executes remote command <command> into the CLI - CLI session id XXXXXX	logSession.csv
0901100	Notice	<user> finished executing remote command <command> into the CLI - CLI session id XXXXXX	logSession.csv
0901200	Notice	<user> connection rejected - CLI session id XXXXXX	logSession.csv
0901300	Notice	<user> disconnected from interactive CLI with session id XXXXXX due to session timeout	logSession.csv
0901400	Notice	<user> disconnected from interactive CLI with session id XXXXXX due to concurrent connection with session id XXXXXX	logSession.csv
0100C00	Notice	Syslog is started	logSystem.csv
0100B00	Notice	Syslog is stopping	logSystem.csv
0100D00	Notice	Network module is booting	logSystem.csv
0100E00	Notice	Network module is operating	logSystem.csv
0100F00	Notice	Network module is starting shutdown sequence	logSystem.csv
0101000	Notice	Network module is ending shutdown sequence	logSystem.csv
0101400	Notice	Network module shutdown requested	logSystem.csv
0101500	Notice	Network module reboot requested	logSystem.csv
0101600	Notice	Network module reboot rejected	logSystem.csv
0100200	Notice	<nb alarms> alarms exported and flushed	logSystem.csv
0A00100	Info	Network module upgrade success <f/w: xx.yy.zzzz>	logUpdate.csv
0A00300	Info	Network module upgrade started	logUpdate.csv
0A00600	Info	Network module file system integrity OK <f/w: xx.yy.zzzz>	logUpdate.csv
0B00300	Info	Time with NTP synchronized	logSystem.csv
0B00600	Info	Time settings changed	logSystem.csv
0B01100	Info	Time reset to last known date: "date"	logSystem.csv
0C00F00	Info	Test email	
1000100	Info	Settings saving requested	logSystem.csv
1000200	Info	<feature> settings saved	logSystem.csv
1000A00	Info	Settings restoration requested	logSystem.csv
1000E00	Info	<feature> settings restoration success	logSystem.csv
1000B00	Info	Settings restoration success	logSystem.csv

0301500	Notice	Sanitization switch changed	logSystem.csv
0A01600	Notice	Major version downgrade	logUpdate.csv
0D00800	Notice	DHCP client script called with <script parameters>	logSystem.csv
0D00900	Notice	IPv4 configuration changed to <ipsv4_address>	logSystem.csv
0D01000	Notice	IPv6 configuration changed to <ipsv6_address>	logSystem.csv
0E00100	Notice	Outlet State change	logSystem.csv
1200700	Notice	Config file has been applied	logSystem.csv



Event with code 0700600 is used within shutdown script. The severity may vary according to the event context.

## 8.5.2 PDU alarm log codes



To retrieve Alarm logs, navigate to [Contextual help>>>Alarms](#) section and press the **Download alarms** button.



Below codes are the one to be used to add "Exceptions on events notification" on email sending configurations. Some zeros maybe added in front of the code when displayed in emails or logs. The below reported codes match as much as possible to the G3 PDU firmware code.

Code	Severity	Active message	Non-active message	Advice
211101 ... 211103	Warning	Input1 phase1 Current measure out of range (lower warning) ... Input1 phase3 Current measure out of range (lower warning)		
211301 ... 211303	Warning	Input1 phase1 Current measure out of range (upper warning) ... Input1 phase3 Current measure out of range (upper warning)		
211401 ... 211403	Critical	Input1 phase1 Current measure out of range (upper Critical) ... Input1 phase3 Current measure out of range (upper Critical)		
211601 ... 211603	Warning	Input2 phase1 Current measure out of range (lower warning) ... Input2 phase3 Current measure out of range (lower warning)		
211801 ... 211803	Warning	Input2 phase1 Current measure out of range (upper warning) ... Input2 phase3 Current measure out of range (upper warning)		
211901 ... 211903	Critical	Input2 phase 1 Current measure out of range (upper Critical) ... Input2 phase 3 Current measure out of range (upper Critical)		
212101 ... 212103	Warning	Input1 phase1 voltage measure out of range (lower warning) ... Input1 phase3 voltage measure out of range (lower warning)		

212201 ... 212203	Critical	Input1 phase1 voltage measure out of range (lower Critical) ... Input1 phase3 voltage measure out of range (lower Critical)		
212301 ... 212303	Warning	Input1 phase1 voltage measure out of range (upper warning) ... Input1 phase3 voltage measure out of range (upper warning)		
212401 ... 212403	Critical	Input1 phase1 voltage measure out of range (upper Critical) ... Input1 phase3 voltage measure out of range (upper Critical)		
212601 ... 212603	Warning	Input2 phase1 voltage measure out of range (lower warning) ... Input2 phase3 voltage measure out of range (lower warning)		
212701 ... 212703	Critical	Input2 phase1 voltage measure out of range (lower Critical) ... Input2 phase3 voltage measure out of range (lower Critical)		
212801 ... 212803	Warning	Input2 phase1 voltage measure out of range (upper warning) ... Input2 phase3 voltage measure out of range (upper warning)		
212901 ... 212903	Critical	Input2 phase1 voltage measure out of range (upper Critical) ... Input2 phase3 voltage measure out of range (upper Critical)		
213200	Critical	Input1 frequency measure out of range (lower Critical)		
213300	Critical	Input1 frequency measure out of range (upper Critical)		
213700	Critical	Input2 frequency measure out of range (lower Critical)		
213800	Critical	Input2 frequency measure out of range (upper Critical)		

221101 ... 221112	Warning	Branch1 Current measure out of range (lower warning) ... Branch12 Current measure out of range (lower warning)		
221301 ... 221312	Warning	Branch1 Current measure out of range (upper warning) ... Branch12 Current measure out of range (upper warning)		
221401 ... 221412	Critical	Branch1 Current measure out of range (upper Critical) ... Branch12 Current measure out of range (upper Critical)		
222101 ... 222112	Warning	Branch1 voltage measure out of range (lower warning) ... Branch12 voltage measure out of range (lower warning)		
222201 ... 222212	Critical	Branch1 voltage measure out of range (lower Critical) ... Branch12 voltage measure out of range (lower Critical)		
222301 ... 222312	Warning	Branch1 voltage measure out of range (upper warning) ... Branch12 voltage measure out of range (upper warning)		
222401 ... 222412	Critical	Branch1 voltage measure out of range (upper Critical) ... Branch12 voltage measure out of range (upper Critical)		
223101 ... 223112	Critical	Branch1 breaker tripped ... Branch12 breaker tripped	Branch1 breaker closed ... Branch12 breaker closed	
231101 ... 231164	Warning	Outlet1 Current measure out of range (lower warning) ... Outlet64 Current measure out of range (lower warning)		



231301 ... 231364	Warning	Outlet1 Current measure out of range (upper warning) ... Outlet64 Current measure out of range (upper warning)		
231401 ... 231464	Critical	Outlet1 Current measure out of range (upper Critical) ... Outlet64 Current measure out of range (upper Critical)		
243100	Info	Communication lost		
[Not yet implemented]	Critical	Daisy Chain communication failure		
[Not yet implemented]	Critical	IT equipment communication failure		

### 8.5.2.1 Info

Code	Severity	Active message	Non-active message	Advice
xxx				

### 8.5.2.2 Good



Alarms with a severity set as Good are not taken into account into the counter of active alarms.

Code	Severity	Active message
xxx		

## 8.5.3 EMP alarm log codes



To retrieve Alarm logs, navigate to [Contextual help>>>Alarms](#) section and press the **Download alarms** button.



Below codes are the one to be used to add "Exceptions on events notification" on email sending configurations. Some zeros maybe added in front of the code when displayed in emails or logs.

### 8.5.3.1 Critical

Code	Severity	Active message	Non-active message	Advice
1201	Critical	Temperature is critically low	Temperature is back to low	-
1204	Critical	Temperature is critically high	Temperature is back to high	-
1211	Critical	Humidity is critically low	Humidity is back to low	-
1214	Critical	Humidity is critically high	Humidity is back to high	-

### 8.5.3.2 Warning

Code	Severity	Active message	Non-active message	Advice
1200	Warning	Communication lost	Communication recovered	-
1202	Warning	Temperature is low	Temperature is back to normal	-
1203	Warning	Temperature is high	Temperature is back to normal	-
1212	Warning	Humidity is low	Humidity is back to normal	-
1213	Warning	Humidity is high	Humidity is back to normal	-

### 8.5.3.3 With settable severity

Code	Severity	Active message	Non-active message	Advice
1221	Settable	Contact is active	Contact is back to normal	-

## 8.5.4 Network module alarm log codes



To retrieve Alarm logs, navigate to [Contextual help>>>Alarms](#) section and press the **Download alarms** button.



Below codes are the one to be used to add "Exceptions on events notification" on email sending configurations. Some zeros maybe added in front of the code when displayed in emails or logs.

### 8.5.4.1 Warning

#### 8.5.4.1.1 Alarms

Code	Severity	Active message	Non-active message	Advice
1303	Warning	Alarms: the number of alarms is too high and above 6 000	Alarms: the number of alarms is back to normal	2 000 alarms have been erased and saved in a backup file.

### 8.5.4.2 Info

#### 8.5.4.2.1 Communication

Code	Severity	Active message	Non-active message	Advice
1300	Info	Communication: No device connected	Communication: Communication with the device is back	-
1301	Info	Communication: Device not supported	Communication: Communication with the device is back	-

#### 8.5.4.2.2 Alarms

Code	Severity	Active message	Non-active message	Advice
1302	Info	Alarms: the number of alarms is high and above 5 000	Alarms: the number of alarms is back to normal	It is recommended to Export and Clear the alarm log.

## 8.6 SNMP traps

### 8.6.1 Sensor Mib

#### 8.6.1.1 Sensor Mib traps

This information is for reference only.

Trap oid : .1.3.6.1.4.1.534.6.8.1.x.x.x	Trap description
.1.3.6.1.4.1.534.6.8.1.1.0.1	Sent whenever the sensor count changes after a discovery or removing from the UI.
.1.3.6.1.4.1.534.6.8.1.1.0.2	Sent whenever one status of each sensor connected changes.
.1.3.6.1.4.1.534.6.8.1.2.0.1	Sent whenever one status of each temperature changes.
.1.3.6.1.4.1.534.6.8.1.3.0.1	Sent whenever one status of each humidity changes.
.1.3.6.1.4.1.534.6.8.1.4.0.1	Sent whenever one status of each digital input alarm changes.

## 8.6.2 PDU Mib

### 8.6.2.1 EATON PDU traps

This information is for reference only.

PDU Traps OID base : 1.3.6.1.4.1.534.6.6.7.0  eatonEpdu { iso(1) org(3) dod(6) internet(1) private(4) enterprises(1) eaton(534) products(6) pduAgent(6) (7) }	Description :	OID Data sent with the Trap
notifyUserLogin .1	Sent whenever a user logs in.	username, commInterface
notifyUserLogout .2	Sent whenever a user logs out.	username, commInterface
notifyFailedLogin .3	Sent when someone attempts to log in and fails. On some models, may be sent after three failed login attempts.	username, commInterface
notifyBootUp .4	Sent whenever an PDU finishes booting up (hard or soft reboot).	strappingIndex
	<b>Input Traps (11-19)</b>	
notifyInputVoltageThStatus .11	Sent whenever an input voltage threshold status changes.	strappingIndex, inputIndex, inputVoltageIndex, inputVoltage, inputVoltageThStatus
notifyInputCurrentThStatus .12	Sent whenever an input current threshold status changes.	strappingIndex, inputIndex, inputCurrentIndex, inputCurrent, inputCurrentThStatus
notifyInputFrequencyStatus .13	Sent whenever the input frequency status changes.	strappingIndex, inputIndex, inputFrequency, inputFrequencyStatus
	<b>Group Traps (21 -29)</b>	

notifyGroupVoltageThStatus .21	Sent whenever a group voltage threshold status changes.	strappingIndex, groupIndex, groupVoltage, groupVoltageThStatus
notifyGroupCurrentThStatus .22	Sent whenever a group current threshold status changes.	strappingIndex, groupIndex, groupCurrent, groupCurrentThStatus
notifyGroupBreakerStatus .23	Sent whenever a group status changes to indicate whether the circuit breaker is on or off.	strappingIndex, groupIndex, groupBreakerStatus
<b>Outlet Traps (31-39)</b>		
notifyOutletVoltageThStatus .31	Sent whenever an outlet voltage threshold status changes.	strappingIndex, outletIndex, outletVoltage, outletVoltageThStatus
notifyOutletCurrentThStatus .32	Sent whenever an outlet current threshold status changes.	strappingIndex, outletIndex, outletCurrent, outletCurrentThStatus
notifyOutletControlStatus .33	Sent whenever an outlet state On / Off changes.	strappingIndex, outletIndex, outletControlStatus
<b>Environment / Sensors Traps (41-49)</b>		
DEPRECATED => please use the Eaton Sensor MIB instead		
<b>System Traps (51-59)</b>		
notifyCommunicationStatus .51	Sent whenever the PDU communication status changes.	strappingIndex, communicationStatus
notifyInternalStatus .52	Sent whenever the PDU internal status changes.	strappingIndex, internalStatus
notifyTest .53	Sent whenever the trap test feature is used by the communication card.	
notifyStrappingStatus .54	Sent whenever the strapping communication status changes.	strappingIndex, strappingStatus

## 8.7 CLI

CLI can be accessed through:

- SSH
- Serial terminal emulation (refer to section [Servicing the Network Management Module>>>Installing the Network Module>>>Accessing the card through serial terminal emulation](#)).

It is intended mainly for automated configuration of the network and time settings of the network card. It can also be used for troubleshooting and remote reboot/reset of the network interface in case the web user interface is not accessible.

**Warning:** Changing network parameters may cause the card to become unavailable remotely. If this happens it can only be reconfigured locally through USB.

### 8.7.1 Commands available

You can see this list anytime by typing in the CLI:

?

## 8.7.2 Contextual help

You can see this help anytime by typing in the CLI:

```
help
```

### CONTEXT SENSITIVE HELP

[?] - Display context sensitive help. This is either a list of possible command completions with summaries, or the full syntax of the current command. A subsequent repeat of **this** key, when a command has been resolved, will display a detailed reference.

### AUTO-COMPLETION

The following keys both perform auto-completion **for** the current command line. If the command prefix is not unique then the bell will ring and a subsequent repeat of the key will display possible completions.

[enter] - Auto-completes, syntax-checks then executes a command. If there is a syntax error then offending part of the command line will be highlighted and explained.

[space] - Auto-completes, or **if** the command is already resolved inserts a space.

### MOVEMENT KEYS

[CTRL-A] - Move to the start of the line  
 [CTRL-E] - Move to the end of the line.  
 [up] - Move to the previous command line held in history.  
 [down] - Move to the next command line held in history.  
 [left] - Move the insertion point left one character.  
 [right] - Move the insertion point right one character.

### DELETION KEYS

[CTRL-C] - Delete and abort the current line  
 [CTRL-D] - Delete the character to the right on the insertion point.  
 [CTRL-K] - Delete all the characters to the right of the insertion point.  
 [CTRL-U] - Delete the whole line.  
 [backspace] - Delete the character to the left of the insertion point.

### ESCAPE SEQUENCES

!! - Substitute the last command line.  
 !N - Substitute the Nth command line (absolute as per 'history' command)  
 !-N - Substitute the command line entered N lines before (relative)

## 8.7.3 get release info

### 8.7.3.1 Description




Displays certain basic information related to the firmware release.

8.7.3.2 Help

```
get_release_info
-d Get current release date
-s Get current release sha1
-t Get current release time
-v Get current release version number
```

8.7.3.3 Specifics

8.7.3.4 Access rights per profiles

	Administrator	Operator	Viewer
get release info			

8.7.4 history

8.7.4.1 Description




Displays recent commands executed on the card.

8.7.4.2 Help

```
history
<cr>          Display the current session's command line history(by default display
last 10 commands)
<Unsigned integer> Set the size of history list (zero means unbounded). Example 'history
6' display the 6 last command
```

8.7.4.3 Specifics

8.7.4.4 Access rights per profiles

	Administrator	Operator	Viewer
history			

8.7.5 logout

8.7.5.1 Description




Logout the current user.

### 8.7.5.2 Help

```
logout
  <cr> logout the user
```

### 8.7.5.3 Specifics

### 8.7.5.4 Access rights per profiles

	Administrator	Operator	Viewer
logout			

## 8.7.6 maintenance

### 8.7.6.1 Description

Creates a maintenance report file which may be handed to the technical support.

### 8.7.6.2 Help

```
maintenance
  <cr> Create maintenance report file.
  -h, --help Display help page
```

### 8.7.6.3 Examples of usage

Generate the maintenance report by running the "maintenance" command.  
Then retrieve the report from the card using SCP

#### 8.7.6.3.1 From a linux host:

```
sshpass -p $PASSWORD scp $USER@$CARD_ADDRESS:report.zip .
```

#### 8.7.6.3.2 From a Windows host:

```
pscp -scp -pw $PASSWORD $USER@$CARD_ADDRESS:report.zip report.zip
```

(Require pscp tools from putty)

Where:

- \$USER is user name (the user shall have administrator profile)
- \$PASSWORD is the user password
- \$CARD\_ADDRESS is IP or hostname of the card



### 8.7.6.4 Specifics

### 8.7.6.5 Access rights per profiles

	Administrator	Operator	Viewer
maintenance	✓	✗	✗

## 8.7.7 netconf

### 8.7.7.1 Description

Tools to display or change the network configuration of the card.

### 8.7.7.2 Help

For Viewer and Operator profiles:

```
netconf -h
Usage: netconf [OPTION]...
Display network information and change configuration.

-h, --help      display help page
-l, --lan       display Link status and MAC address
-4, --ipv4      display IPv4 Mode, Address, Netmask and Gateway
-6, --ipv6      display IPv6 Mode, Addresses and Gateway
-d, --domain    display Domain mode, FQDN, Primary and Secondary DNS
```

For Administrator profile:

```
netconf -h
Usage: netconf [OPTION]...
Display network information and change configuration.
-h, --help      display help page
-l, --lan       display Link status and MAC address
-d, --domain    display Domain mode, FQDN, Primary and Secondary DNS
-4, --ipv4      display IPv4 Mode, Address, Netmask and Gateway
-6, --ipv6      display IPv6 Mode, Addresses and Gateway
Set commands are used to modify the settings.
-s, --set-lan <link speed>
Link speed values:
auto           Auto negotiation
10hf           10 Mbps - Half duplex
10ff           10 Mbps - Full duplex
100hf          100 Mbps - Half duplex
100ff          100 Mbps - Full duplex
1000ff         1.0 Gbps - Full duplex
-f, --set-domain hostname <hostname>  set custom hostname
-f, --set-domain <mode>
Mode values:
```

```

- set custom Network address, Netmask and Gateway:
  manual <domain name> <primary DNS> <secondary DNS>
- automatically set Domain name, Primary and Secondary DNS
  dhcp
-i, --set-ipv4 <mode>
  Mode values:
- set custom Network address, Netmask and Gateway
  manual <network> <mask> <gateway>
- automatically set Network address, Netmask and Gateway
  dhcp
-x, --set-ipv6 <status>
  Status values:
- enable IPv6
  enable
- disable IPv6
  disable
-x, --set-ipv6 <mode>
  Mode values:
- set custom Network address, Prefix and Gateway
  manual <network> <prefix> <gateway>
- automatically set Network address, Prefix and Gateway
  router
Examples of usage:
-> Display Link status and MAC address
  netconf -l
-> Set Auto negotiation to Link
  netconf --set-lan auto
-> Set custom hostname
  netconf --set-domain hostname ups-00-00-00-00-00-00
-> Set Address, Netmask and Gateway
  netconf --set-ipv4 manual 192.168.0.1 255.255.255.0 192.168.0.2
-> Disable IPv6

```

### 8.7.7.3 Examples of usage

```

-> Display Link status and MAC address
  netconf -l
-> Set Auto negotiation to Link
  netconf -s auto
-> Set custom hostname
  netconf -f hostname ups-00-00-00-00-00-00
-> Set Address, Netmask and Gateway
  netconf -i manual 192.168.0.1 255.255.255.0 192.168.0.2
-> Disable IPv6
  netconf -6 disable

```

### 8.7.7.4 Specifics

### 8.7.7.5 Access rights per profiles

	Administrator	Operator	Viewer
netconf	✓	✓ (read-only)	✓ (read-only)

## 8.7.8 ping and ping6

### 8.7.8.1 Description

Ping and ping6 utilities are used to test network connection.

### 8.7.8.2 Help

```
ping
The ping utility uses the ICMP protocol's mandatory ECHO_REQUEST datagram
to elicit an ICMP ECHO_RESPONSE from a host or gateway. ECHO_REQUEST
datagrams ('`pings`') have an IP and ICMP header, followed by a ``struct
timeval`` and then an arbitrary number of ``pad`` bytes used to fill out
the packet.

-c          Specify the number of echo requests to be sent
-h          Specify maximum number of hops
<Hostname or IP> Host name or IP address


ping6
The ping6 utility uses the ICMP protocol's mandatory ECHO_REQUEST datagram
to elicit an ICMP ECHO_RESPONSE from a host or gateway. ECHO_REQUEST
datagrams ('`pings`') have an IP and ICMP header, followed by a ``struct
timeval`` and then an arbitrary number of ``pad`` bytes used to fill out
the packet.

-c          Specify the number of echo requests to be sent
<IPv6 address> IPv6 address
```

### 8.7.8.3 Specifics

### 8.7.8.4 Access rights per profiles

	Administrator	Operator	Viewer
ping	✓	✗	✗
ping6	✓	✗	✗

## 8.7.9 reboot

### 8.7.9.1 Description

Tool to Reboot the card.




### 8.7.9.2 Help

```
Usage: reboot [OPTION]
```

```
<cr>          Reboot the card
--help        Display help
--withoutconfirmation  Reboot the card without confirmation
```

8.7.9.3 Specifics

8.7.9.4 Access rights per profiles

	Administrator	Operator	Viewer
reboot			

8.7.10 rest list

8.7.10.1 Usage

**rest list <path>**  
This command shall list the endpoints starting from <path>  
If no path provided, the command shall list all resources starting from "/"

**rest list ?**  
This command print the help for the command.

8.7.10.2 Options

-d <number> : number of levels to show in the response  
if no number provided, the default value is 1

8.7.10.3 Example

Command :  
rest list /managers/1/networkService/networkInterfaces/eth0/ipv4  
Result :  
/managers/1/networkService/networkInterfaces/eth0/ipv4/status  
/managers/1/networkService/networkInterfaces/eth0/ipv4/address  
/managers/1/networkService/networkInterfaces/eth0/ipv4/subnetMask  
/managers/1/networkService/networkInterfaces/eth0/ipv4/gateway  
/managers/1/networkService/networkInterfaces/eth0/ipv4/settings

8.7.11 rest get

8.7.11.1 Usage

**rest get <option> <path>**  
This command returns the payload starting from <path>  
If no path provided, the command returns the payload starting from "/" with a depth of 1

**rest get ?**  
This command print the help for the command.

## 8.7.11.2 Options

-d <number> : number of levels to show in the response  
if no number provided, the default value is 1

## 8.7.11.3 Example

```
rest get /managers/1/networkService/networkInterfaces/eth1/ipv4/address
=>
10.130.33.195
```

## 8.7.12 rest set

### 8.7.12.1 Usage

**rest set <path> <payload>**

This command sets the resource identified by <path> with the given <payload>

**rest set ?**

This command print the help for the command.

### 8.7.12.2 Example

Set IPv4 address :

```
rest set /managers/1/networkService/networkInterfaces/eth1/ipv4/settings/manual/address 192.168.47.136
```

Set a field to an empty value or reset a field :

```
rest set /managers/1/identification/location ""
```

## 8.7.13 rest exec

### 8.7.13.1 Usage

**rest exec <path> [payload]**

This command runs the action at the resource identified by <path>. <payload> is an optional argument and is action dependent.

**rest exec ?**

This command will print the help for the command.

### 8.7.13.2 Example

Switch On immediately:

```
rest exec /powerDistributions/1/outlets/1/actions/switchOn
```

Switch On After 5 second delay:

```
rest exec /powerDistributions/1/outlets/1/actions/switchOn 5
```

## 8.7.14 save\_configuration | restore\_configuration

### 8.7.14.1 Description

Save\_configuration and restore\_configuration are using JSON format to save and restore certain part of the configuration of the card.

### 8.7.14.2 Help

```
save_configuration -h
save_configuration: print the card configuration in JSON format to standard output.

restore_configuration -h
restore_configuration: restore the card configuration from a JSON-formatted standard input.
```

### 8.7.14.3 Examples of usage

#### 8.7.14.3.1 From a linux host:

**Save over SSH:** sshpass -p \$PASSWORD ssh \$USER@\$CARD\_ADDRESS save\_configuration -p \$PASSPHRASE> \$FILE  
**Restore over SSH:** cat \$FILE | sshpass -p \$PASSWORD ssh \$USER@\$CARD\_ADDRESS restore\_configuration -p \$PASSPHRASE

#### 8.7.14.3.2 From a Windows host:

**Save over SSH:** plink \$USER@\$CARD\_ADDRESS -pw \$PASSWORD -batch save\_configuration -p \$PASSPHRASE > \$FILE  
**Restore over SSH:** type \$FILE | plink \$USER@\$CARD\_ADDRESS -pw \$PASSWORD -batch restore\_configuration -p \$PASSPHRASE  
(Require plink tools from putty)

Where:

- \$USER is user name (the user shall have administrator profile)
- \$PASSWORD is the user password
- \$PASSPHRASE is any passphrase to encrypt/decrypt sensible data.
- \$CARD\_ADDRESS is IP or hostname of the card
- \$FILE is a path to the JSON file (on your host computer) where the configuration is saved or restored.

### 8.7.14.4 Specifics

### 8.7.14.5 Access rights per profiles

	Administrator	Operator	Viewer
save_configuration	✓	✗	✗
restore_configuration	✓	✗	✗

## 8.7.15 sanitize

### 8.7.15.1 Description

Sanitize command to return card to factory reset configuration.

### 8.7.15.2 Access

- Administrator

### 8.7.15.3 Help

```
sanitize
-h, --help           Display help page
--withoutconfirmation Do factory reset of the card without confirmation
<cr>                Do factory reset of the card
```

### 8.7.15.4 Access rights per profiles

	Administrator	Operator	Viewer
sanitize	✓	✗	✗

## 8.7.16 ssh-keygen

### 8.7.16.1 Description

Command used for generating the ssh keys.

### 8.7.16.2 Help

```
ssh-keygen
-h, --help  Display help
<cr>       Renew SSH keys
```

### 8.7.16.3 Specifics

### 8.7.16.4 Access rights per profiles

	Administrator	Operator	Viewer
ssh-keygen	✓	✗	✗

## 8.7.17 time

### 8.7.17.1 Description

Command used to display or change time and date.

### 8.7.17.2 Help

For Viewer and Operator profiles:

```
time -h
Usage: time [OPTION]...
Display time and date.
```

```
-h, --help      display help page
-p, --print     display date and time in YYYYMMDDhhmmss format
```

For Administrator profile:

```
time -h
Usage: time [OPTION]...
Display time and date, change time and date.
-h, --help      display help page
-p, --print     display date and time in YYYYMMDDhhmmss format
-s, --set <mode>
Mode values:
- set date and time (format YYYYMMDDhhmmss)
  manual <date and time>
- set preferred and alternate NTP servers
  ntpmanual <preferred server> <alternate server>
- automatically set date and time
  ntpauto
Examples of usage:
-> Set date 2017-11-08 and time 22:00
   time --set manual 201711082200
-> Set preferred and alternate NTP servers
   time --set ntpmanual fr.pool.ntp.org de.pool.ntp.org
```

8.7.17.3 Examples of usage

```
-> Set date 2017-11-08 and time 22:00
   time --set manual 201711082200
-> Set preferred and alternate NTP servers
   time --set ntpmanual fr.pool.ntp.org de.pool.ntp.org
```

8.7.17.4 Specifics

8.7.17.5 Access rights per profiles

	Administrator	Operator	Viewer
time	✓	✓ (read-only)	✓ (read-only)

8.7.18 traceroute and traceroute6

8.7.18.1 Description

Traceroute and traceroute6 utilities are for checking the configuration of the network.

8.7.18.2 Help

```
traceroute
```



```
-h          Specify maximum number of hops
<Hostname or IP> Remote system to trace
```

```
traceroute6
-h          Specify maximum number of hops
<IPv6 address> IPv6 address
```

### 8.7.18.3 Specifics

### 8.7.18.4 Access rights per profiles

	Administrator	Operator	Viewer
traceroute	✓	✗	✗
traceroute6	✓	✗	✗

## 8.7.19 whoami

### 8.7.19.1 Description

whoami displays current user information:

- Username
- Profile
- Realm

### 8.7.19.2 Specifics

### 8.7.19.3 Access rights per profiles

	Administrator	Operator	Viewer
whoami	✓	✓	✓

## 8.7.20 email-test

### 8.7.20.1 Description

mail-test sends test email to troubleshoot SMTP issues.

### 8.7.20.2 Help

```
Usage: email-test <command> ...
Test SMTP configuration.

Commands:
```

```
email-test -h, --help, Display help page

email-test -r, --recipient <recipient_address>
Send test email to the
    <recipient_address>      Email address of the recipient
```

8.7.20.3 Specifics

8.7.20.4 Access rights per profiles

	Administrator	Operator	Viewer
email-test	✔	✘	✘

8.7.21 systeminfo\_statistics

8.7.21.1 Description

Displays the following system information usage:

- 1. CPU
  - a. usage : %
  - b. upSince : date since the system started
- 2. Ram
  - a. total: MB
  - b. free: MB
  - c. used: MB
  - d. tmpfs: temporary files usage (MB)
- 3. Flash
  - a. user data
    - i. total: MB
    - ii. free: MB
    - iii. used: MB

8.7.21.2 Help

```
systeminfo_statistics
    Display systeminfo statistics

    -h, --help    Display the help page.
```

8.7.21.3 Specifics

8.7.21.4 Access rights per profiles

	Administrator	Operator	Viewer
systeminfo_statistics	✔	✔	✔

## 8.7.22 certificates

### 8.7.22.1 Description

Allows to manage certificates through the CLI.

### 8.7.22.2 Help

```
certificates <target> <action> <service_name>
<target> :
- local
<action> :
- print: provides a given certificate detailed information.
- revoke: revokes a given certificate.
- export: returns a given certificate contents.
- import: upload a given certificate for the server CSR. This will replace the CSR
with the certificate given.
- csr: get the server CSR contents. This will create the CSR if not already existing.
<service_name>: mqtt/syslog/webserver
```

### 8.7.22.3 Examples of usage

#### 8.7.22.3.1 From a linux host:

**print over SSH:** `sshpass -p $PASSWORD ssh $USER@$CARD_ADDRESS certificates local print $SERVICE_NAME`

**revoke over SSH:** `sshpass -p $PASSWORD ssh $USER@$CARD_ADDRESS certificates local revoke $SERVICE_NAME`

**export over SSH:** `sshpass -p $PASSWORD ssh $USER@$CARD_ADDRESS certificates local export $SERVICE_NAME`

**import over SSH:** `cat $FILE | sshpass -p $PASSWORD ssh $USER@$CARD_ADDRESS certificates local import $SERVICE_NAME`

**csr over SSH:** `sshpass -p $PASSWORD ssh $USER@$CARD_ADDRESS certificates local csr mqtt`

#### 8.7.22.3.2 From a Windows host: (plink tools from putty is required)

**print over SSH:** `plink $USER@$CARD_ADDRESS -pw $PASSWORD -batch certificates local print $SERVICE_NAME`

**revoke over SSH:** `plink $USER@$CARD_ADDRESS -pw $PASSWORD -batch certificates local revoke $SERVICE_NAME`

**export over SSH:** `plink $USER@$CARD_ADDRESS -pw $PASSWORD -batch certificates local export $SERVICE_NAME`

**import over SSH:** `type $FILE | plink $USER@$CARD_ADDRESS -pw $PASSWORD -batch certificates local import $SERVICE_NAME`

**csr over SSH:** `plink $USER@$CARD_ADDRESS -pw $PASSWORD -batch certificates local csr mqtt`

#### 8.7.22.3.3 Where:

- \$USER is user name (the user shall have administrator profile)
- \$PASSWORD is the user password
- \$PASSPHRASE is any passphrase to encrypt/decrypt sensible data.
- \$CARD\_ADDRESS is IP or hostname of the card
- \$FILE is a certificate file
- \$SERVICE\_NAME is the name one of the following services : mqtt / syslog / webserver.

## 8.7.22.4 Specifics

### 8.7.22.5 Access rights per profiles

	Administrator	Operator	Viewer
certificates	✓	✗	✗

## 8.8 Legal information

This Network Module includes software components that are either licensed under various open source license, or under a proprietary license.

For more information, see to the legal Information link from the main user interface in the footer.

### 8.8.1 Availability of Source Code

The source code of open source components that are made available by their licensors may be obtained upon written express request by contacting [network-m2-opensource@Eaton.com](mailto:network-m2-opensource@Eaton.com). Eaton reserves the right to charge minimal administrative costs, in compliance with the terms of the underlying open source licenses, when the situation requires.

### 8.8.2 Notice for Open Source Elements

This product includes software released under BSD or Apache v2 licenses, and developed by various projects, peoples and entities, such as, but not limited to:

- \* the Regents of the University of California, Berkeley and its contributors,
- \* the OpenEvidence Project,
- \* Oracle and/or its affiliates,
- \* Mike Bostock,
- \* JS Foundation and other contributors,
- \* 2011-2014 Novus Partners, Inc.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. ([www.openssl.org/](http://www.openssl.org/)).

This product includes cryptographic software written by Eric Young ([eay@cryptsoft.com](mailto:eay@cryptsoft.com)).

This product includes software released under MIT license, and developed by various projects, peoples and entities, such as, but not limited to:

- \* Google, Inc.,
- \* the AngularUI Team
- \* Lucas Galfasó
- \* nerv
- \* Angular
- \* Konstantin Skipor
- \* Filippo Oretti, Dario Andrei
- \* The angular-translate team and Pascal Precht,
- \* Twitter, Inc.
- \* Zeno Rocha
- \* Kristopher Michael Kowal and contributors
- \* JS Foundation and other contributors
- \* Jonathan Hieb
- \* Mike Grabski
- \* Sachin N.

This product includes contents released under Creative Commons Attribution 4.0, Creative Commons Attribution-ShareAlike 3.0 Unported and SIL Open Font License licenses, and created by:

- \* IcoMoon
- \* Dave Gandy
- \* Stephen Hutchings and the Typicons team.

In order to access the complete and up to date copyright information, licenses, and legal disclaimers, see the Legal Information pages, available from the HTML user interface of the present product.

### **8.8.3 Notice for our proprietary (i.e. non-Open source) elements**

Copyright © 2020 Eaton. This firmware is confidential and licensed under Eaton Proprietary License (EPL or EULA).

This firmware is not authorized to be used, duplicated, or disclosed to anyone without the prior written permission of Eaton.

Limitations, restrictions and exclusions of the Eaton applicable standard terms and conditions, such as its EPL and EULA, apply.

## 8.9 Acronyms and abbreviations

**AC:** Alternating current.

**bps:** bit per second

**BOM:** In Syslog, placing an encoded Byte Order Mark at the start of a text stream can indicate that the text is Unicode and identify the encoding scheme used.

**CA:** Certificate Authority

**CLI:** Command Line Interface.

Aim is to interact with the Network Module by using commands in the form of successive lines of text (command lines).

**CSR:** Certificate Signing Request

**DC:** Direct current.**DN:** Distinguished Name (LDAP).

**DHCPv6:** The Dynamic Host Configuration Protocol version 6 is a network protocol for configuring Internet Protocol version 6 (IPv6) hosts with IP addresses, IP prefixes and other configuration data required to operate in an IPv6 network. It is the IPv6 equivalent of the Dynamic Host Configuration Protocol for IPv4.

**DNS:** The Domain Name System is a hierarchical decentralized naming system for computers, services, or other resources connected to the Internet or a private network.

**DST:** The daylight saving time.

**EMP:** Environmental monitoring probe

**GD:** Group Identifier is a numeric value used to represent a specific group (LDAP).

**GNM:** Gigabit Network Module of the PDU.

**HTTPS:** HTTPS consists of communication over Hypertext Transfer Protocol (HTTP) within a connection encrypted by Transport Layer Security (TLS).

**IPP:** Intelligent Power Protector is a web-based application that enables administrators to manage an Devices from a browser-based management console. Administrators can monitor, manage, and control a single Device (UPS, ATS, PDU) locally and remotely. A familiar browser interface provides secure access to the Device Administrator Software and Device Client Software from anywhere on the network. Administrators may configure power failure settings and define UPS load segments for maximum uptime of critical servers. The UPS can also be configured to extend runtimes for critical devices during utility power failures. For most UPSs, the receptacles on the rear panel are divided into one or more groups, called load segments, which can be controlled independently. By shutting down a load segment that is connected to less critical equipment, the runtime for more critical equipment is extended, providing additional protection.

**IPv4:** Internet Protocol version 4 is the fourth version of the Internet Protocol (IP).

**IPv6:** Internet Protocol version 6 is the most recent version of the Internet Protocol (IP).

**JSON:** JavaScript Object Notation is an open-standard file format that uses human-readable text to transmit data objects consisting of attribute–value pairs and array data types.**LAN:** A LAN is a local area network, a computer network covering a small local area, such as a home or office.

**LDAP:** The Lightweight Directory Access Protocol is an industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol.

**MAC:** A media access control address of a computer is a unique identifier assigned to network interfaces for communications at the data link layer of a network segment.

**MIB:** A management information base is a database used for managing the entities in a communication network. Most often associated with the Simple Network Management Protocol (SNMP).

**NTP:** Network Time Protocol is a networking protocol for clock synchronization between computer systems.

**PDU:** A power distribution unit (PDU) is a device fitted with multiple outputs designed to distribute electric power, especially to racks of computers and networking equipment located within a data center.

**P/N:** Part number.

**RTC:** Real time clock.**S/N:** Serial number.

**SMTP:** Simple Mail Transfer Protocol is an Internet standard for electronic mail (email) transmission.

**SNMP:** Simple Network Management Protocol is an Internet-standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior.

**SSH:** Secure Shell is a cryptographic network protocol for operating network services securely over an unsecured network.

**SSL:** Secure Sockets Layer, is a cryptographic protocol used for network traffic. **TLS:** Transport Layer Security is cryptographic protocol that provide communications security over a computer network.

**TFTP:** Trivial File Transfer Protocol is a simple lockstep File Transfer Protocol which allows a client to get a file from or put a file onto a remote host.

**UID:** User identifier (LDAP).

**UTC:** Coordinated Universal Time is the primary time standard by which the world regulates clocks and time.





## 9 Troubleshooting

### 9.1 EMP communication status shows "Lost"

In the Network Module, in [Contextual help>>>Environment>>>Commissioning/Status](#), EMPs are missing in the Sensor commissioning table.

#### 9.1.1 Symptom #1

The connection status of the sensor is "Lost"

##### 9.1.1.1 Possible causes

The EMPs are not powered by the Network module.

##### 9.1.1.2 Action #1-1

Launch again the discovery, if it is still not ok, go to Action #1-2.

##### 9.1.1.3 Action #1-2

1- Check the EMPs connection and cables.

Refer to the sections [Servicing the EMP>>>Installing the EMP>>>Cabling the first EMP to the device](#) and [Servicing the EMP>>>Installing the EMP>>>Daisy chaining 3 EMPs](#).

2- Disconnect and reconnect the USB to RS485 cable.

3- Launch the discovery, if it is still not ok, go to Action #1-3.

##### 9.1.1.4 Action #1-3

1- Reboot the Network module.

2- Launch the discovery.

### 9.2 EMP detection fails at discovery stage

In the Network Module, in [Contextual help>>>Environment>>>Commissioning/Status](#), EMPs are missing in the Sensor commissioning table.

#### 9.2.1 Symptom #1

The EMPs green RJ45 LED (FROM DEVICE) is not ON.

##### 9.2.1.1 Possible causes

The EMPs are not powered by the Network module.

##### 9.2.1.2 Action #1-1

Launch again the discovery, if it is still not ok, go to Action #1-2.

### 9.2.1.3 Action #1-2

1- Check the EMPs connection and cables.

Refer to the sections [Servicing the EMP>>>Installing the EMP>>>Cabling the first EMP to the device](#) and [Servicing the EMP>>>Installing the EMP>>>Daisy chaining 3 EMPs](#).

2- Disconnect and reconnect the USB to RS485 cable.

3- Launch the discovery, if it is still not ok, go to Action #1-3.

### 9.2.1.4 Action #1-3

1- Reboot the Network module.

2- Launch the discovery.

## 9.2.2 Symptom #2

The EMPs orange RJ45 LEDs are not blinking.

### 9.2.2.1 Possible causes

C#1: the EMP address switches are all set to 0.

C#2: the EMPs are daisy chained, the Modbus address is the same on the missing EMPs.

### 9.2.2.2 Action #2-1

1- Change the address of the EMPs to have different address and avoid all switches to 0.

Refer to the section [Servicing the EMP>>>Defining EMPs address and termination>>>Manual addressing](#).

2- Disconnect and reconnect the USB to RS485 cable. The address change is only taken into account after an EMP power-up.

3- Launch the discovery, if it is still not ok, go to Action #2-2.

### 9.2.2.3 Action #2-2

1- Reboot the Network module.

Refer to the section [Contextual help>>>Maintenance>>>Services>>>Reboot](#).

2- Launch the discovery.

## 9.3 How do I log in if I forgot my password?

### 9.3.1 Action

- Ask your administrator for password initialization.
- If you are the main administrator, your password can be reset manually by following steps described in the [Servicing the Network Management Module>>>Recovering main administrator password](#).

## 9.4 LDAP configuration/commissioning is not working

Refer to the section [Servicing the Network Management Module>>>Commissioning/Testing LDAP](#).

## 9.5 Password change in My profile is not working

### 9.5.1 Symptoms

The password change shows "*Invalid credentials*" when I try to change my password in My profile menu:



### 9.5.2 Possible cause

The password has already been changed once within a day period.

### 9.5.3 Action

Let one day between your last password change and retry.

## 9.6 The alarm list has been cleared after an upgrade

### 9.6.1 Symptom

After a FW upgrade, the alarm list has been cleared and is now empty.

### 9.6.2 Action

The alarm list has been saved on a csv file and can be retrieved using Rest API calls.

#### 9.6.2.1 Authenticate:

```
curl --location --request POST 'https://{{domain}}/rest/mbdetnrs/1.0/oauth2/token' \
--header 'Content-Type: application/json' \
--data-raw '{ "username":"admin", "password":"supersecretpassword", "grant_type":"password",
"scope":"GUIAccess" }'
```

#### 9.6.2.2 Get Alarm Log Backup:

```
curl --location --request GET 'https://{{domain}}/rest/mbdetnrs/1.0/alarmService/actions/
downloadBackup' \
--header 'Authorization: Bearer {{access_token}}'
```

## 9.7 The Network Module fails to boot after upgrading the firmware

### 9.7.1 Possible Cause

- 1- The IP address has changed.
- 2- The Network module LED shows solid red after the upgrade.
- 3- The first boot after the upgrade takes a longer time.

Web user interface is not up to date after a FW upgrade

**Note:** If the application is corrupt, due to an interruption while flashing the firmware for example, the boot will be done on previous firmware.

## 9.7.2 Action

- 1- Recover the IP address and connect to the card.
- 2- Reset the Network module by using the Restart button on the front panel.
- 3- Wait until the Network module LED shows flashing green.

Refer to [Installing the Network Management Module>>>Accessing the Network Module>>>Finding and setting the IP address](#) section.

# 9.8 Web user interface is not up to date after a FW upgrade

## 9.8.1 Symptom

After an upgrade:

- The Web interface is not up to date
- New features of the new FW are not displayed
- An infinite spinner is displayed on a tile

### 9.8.1.1 Possible causes

The browser is displaying the Web interface through the cache that contains previous FW data.

### 9.8.1.2 Action

Empty the cache of your browser using F5 or CTRL+F5.

