# 1 Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table of Contents</td>
<td>4</td>
</tr>
<tr>
<td>2 Contextual Help</td>
<td>11</td>
</tr>
<tr>
<td>2.1 Login page</td>
<td>11</td>
</tr>
<tr>
<td>2.1.1 Logging in for the first time</td>
<td>11</td>
</tr>
<tr>
<td>2.1.1.1 Enter default password</td>
<td>11</td>
</tr>
<tr>
<td>2.1.1.2 Change default password</td>
<td>11</td>
</tr>
<tr>
<td>2.1.1.3 Accept license agreement</td>
<td>11</td>
</tr>
<tr>
<td>2.1.2 Troubleshooting login issues</td>
<td>11</td>
</tr>
<tr>
<td>2.2 Home</td>
<td>12</td>
</tr>
<tr>
<td>2.2.1 Menu structure</td>
<td>12</td>
</tr>
<tr>
<td>2.2.2 Energy flow diagram</td>
<td>13</td>
</tr>
<tr>
<td>Line interactive</td>
<td>13</td>
</tr>
<tr>
<td>Online</td>
<td>16</td>
</tr>
<tr>
<td>2.2.3 Top bar</td>
<td>18</td>
</tr>
<tr>
<td>2.2.4 Details</td>
<td>18</td>
</tr>
<tr>
<td>2.2.5 Show measures</td>
<td>18</td>
</tr>
<tr>
<td>Example #1:</td>
<td>18</td>
</tr>
<tr>
<td>Example #2:</td>
<td>19</td>
</tr>
<tr>
<td>2.2.6 Outlet status</td>
<td>19</td>
</tr>
<tr>
<td>2.2.7 Active Alarms</td>
<td>19</td>
</tr>
<tr>
<td>2.3 Alarms</td>
<td>20</td>
</tr>
<tr>
<td>2.3.1 Alarm sorting</td>
<td>20</td>
</tr>
<tr>
<td>2.3.2 Alarm details</td>
<td>20</td>
</tr>
<tr>
<td>2.3.3 Alarm paging</td>
<td>20</td>
</tr>
<tr>
<td>2.3.4 Alarm export</td>
<td>20</td>
</tr>
<tr>
<td>2.3.5 Clear alarm logs</td>
<td>21</td>
</tr>
<tr>
<td>2.3.6 Alarm list with codes</td>
<td>21</td>
</tr>
<tr>
<td>2.4 Settings</td>
<td>21</td>
</tr>
<tr>
<td>2.4.1 General</td>
<td>21</td>
</tr>
<tr>
<td>Location</td>
<td>21</td>
</tr>
<tr>
<td>Contact</td>
<td>21</td>
</tr>
<tr>
<td>System name</td>
<td>22</td>
</tr>
<tr>
<td>Default settings parameters and limitations</td>
<td>22</td>
</tr>
<tr>
<td>2.4.2 Date &amp; Time</td>
<td>22</td>
</tr>
<tr>
<td>Manual: Manually entering the date and time</td>
<td>22</td>
</tr>
<tr>
<td>Dynamic (NTP): Synchronizing the date and time with an NTP server</td>
<td>22</td>
</tr>
<tr>
<td>Default settings parameters and limitations</td>
<td>22</td>
</tr>
<tr>
<td>2.4.3 Users</td>
<td>23</td>
</tr>
<tr>
<td>Password strength rules</td>
<td>23</td>
</tr>
<tr>
<td>Account expiration</td>
<td>23</td>
</tr>
<tr>
<td>Session expiration</td>
<td>24</td>
</tr>
<tr>
<td>Local users table</td>
<td>24</td>
</tr>
<tr>
<td>LDAP</td>
<td>26</td>
</tr>
<tr>
<td>Default settings parameters and limitations</td>
<td>30</td>
</tr>
<tr>
<td>2.4.4 Network</td>
<td>31</td>
</tr>
<tr>
<td>LAN</td>
<td>31</td>
</tr>
<tr>
<td>IPv4</td>
<td>31</td>
</tr>
<tr>
<td>Domain</td>
<td>32</td>
</tr>
<tr>
<td>IPv6</td>
<td>33</td>
</tr>
<tr>
<td>Default settings parameters and limitations</td>
<td>35</td>
</tr>
<tr>
<td>2.4.5 Protocols</td>
<td>35</td>
</tr>
<tr>
<td>HTTPS</td>
<td>35</td>
</tr>
<tr>
<td>Default settings parameters and limitations</td>
<td>35</td>
</tr>
<tr>
<td>2.4.6 SNMP</td>
<td>35</td>
</tr>
<tr>
<td>SNMP tables</td>
<td>36</td>
</tr>
</tbody>
</table>
Actions

Note:

2.9 Sensors
2.9.1 Status (sensors)
  Temperature table
  Humidity table
  Dry contacts table
2.9.2 Alarm configuration (sensors)
  Temperature
  Humidity
  Dry contacts
  Default settings parameters and limitations
2.9.3 Information (sensors)

2.10 Legal information (footer)
2.10.1 Component list
2.10.2 Notice for our proprietary (i.e. non-Open source) elements
2.10.3 Availability of source code

2.11 Contextual help and full documentation
2.11.1 Access to contextual help
2.11.2 Access to full documentation

3 Servicing the Network Management Module

3.1 Unpacking the Network module
3.2 Installing the Network Module
  3.2.1 Mounting the Network Module
  3.2.2 Accessing the web interface through Network
    Connecting the network cable
    Accessing the web interface
  3.2.3 Finding and setting the IP address
    Your network is equipped with a BOOBP/DHCP server (default)
    Your network is not equipped with a BOOOP/DHCP server
  3.2.4 Accessing the web interface through RNDIS
    Connecting the configuration cable
    Web interface access through RNDIS
  3.2.5 Accessing the card through serial terminal emulation
    Connecting the configuration cable
    Manual configuration of the serial connection
    Accessing the card through Serial
  3.2.6 Configuring the UPS Network Module settings
3.3 Configuring/Commissioning/Testing LDAP
  3.3.1 Commissioning
    Configuring connection to LDAP database
    Testing connection to LDAP database
    Map remote users to profile
    Testing profile mapping
    Define LDAP users preferences
  3.3.2 Testing LDAP authentication
  3.3.3 Limitations

3.4 Pairing agent to the Network Module
  3.4.1 Pairing with automatic acceptance (recommended if done in a secure and trusted network)
  3.4.2 Pairing with manual acceptance (maximum security)

3.5 Powering down/up applications (examples)
  3.5.1 Powering down IT system in a specific order
    Target
    Step 1: Installation setup
    Step 2: Agent settings
    Step 3: Power outage policy settings
  3.5.2 Powering down non-priority equipment first
    Target
    Step 1: Installation setup
3.6 Checking the current firmware version of the Network Module

3.7 Accessing to the latest Network Module firmware/driver/script

3.8 Upgrading the card firmware (Web interface / shell script)

3.8.1 Web interface

3.8.2 Shell script

Prerequisite

Procedure

3.8.3 Example:

3.9 Changing the RTC battery cell

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

3.11 Synchronizing the time of the Network Module and the UPS

3.11.1 Automatic time synchronization

Everyday at 5 a.m

If the Network Module time is lost

3.11.2 Manual time synchronization

From the Network Module

From the UPS

3.12 Changing the language of the web pages

3.13 Resetting username and password

3.14 Recovering main administrator password

3.15 Switching to static IP (Manual) / Changing IP address of the Network Module

3.16 Reading product (UPS) information in a simple way

3.16.1 Web page

3.17 Subscribing to a set of alarms for email notification

3.17.1 Example #1: subscribing only to one alarm (load unprotected)

3.17.2 Example #2: subscribing to all Critical alarms and some specific Warnings

4 Securing the Network Management Module

4.1 Cybersecurity considerations for electrical distribution systems

4.1.1 Purpose

4.1.2 Introduction

4.1.3 Connectivity—why do we need to address cybersecurity for industrial control systems (ICS)?

4.1.4 Cybersecurity threat vectors

Paths to the control network

4.1.5 Defense in depth

Firewalls

Demilitarized zones (DMZ)

Intrusion detection and prevention systems (IDPS)

4.1.6 Designing for the threat vectors

Demilitarized zones (DMZ)

Intrusion detection and prevention systems (IDPS)

4.1.7 Policies, procedures, standards, and guidelines

Understanding an ICS network

Log and event management

Security policy and procedures

ICS hardening

Continuous assessment and security training

Patch management planning and procedures

4.1.8 Conclusion

4.1.9 Terms and definitions

4.1.10 Acronyms

4.1.11 References

4.2 Cybersecurity recommended secure hardening guidelines

4.2.1 Introduction
7 Troubleshooting

7.1 Action not allowed in Control/Schedule/Power outage policy

7.1.1 Symptom

7.1.2 Possible Cause

7.1.3 Action

7.2 Client server is not restarting

7.2.1 Symptom

7.2.2 Possible Cause

7.2.3 Action

7.3 EMP detection fails at discovery stage

7.3.1 Symptom #1

Possible causes

Action #1-1

Action #1-2

Action #1-3

7.3.2 Symptom #2

Possible causes

Action #2-1

Action #2-2
7.4 How do I log in if I forgot my password?
7.4.1 Action
7.5 IPP is not able to communicate with the Network module
7.5.1 Symptoms
7.5.2 Possible cause
7.5.3 Setup
7.5.4 Action #1
7.5.5 Action #2
7.6 LDAP configuration/commissioning is not working
7.7 Password change in My preferences is not working
7.7.1 Symptoms
7.7.2 Possible cause
7.7.3 Action
7.8 UPS Network Module fails to boot after upgrading the firmware
7.8.1 Possible Cause
7.8.2 Action
7.9 Web user interface is not up to date after a FW upgrade
7.9.1 Symptom
    Possible causes
    Action
2 Contextual Help

2.1 Login page

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.

2.1.1 Logging in for the first time

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

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.

3. Accept license agreement
   On the next step, License Agreement is displayed.
   Read and accept the agreement in order to continue.

2.1.2 Troubleshooting login issues

ℹ️ For details on troubleshooting, see the Troubleshooting section.
2.2 Home

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

![Home Screen Diagram]

2.2.1 Menu structure

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Home** | *Overview and status of UPS Module:*  
  - Synoptic  
  - Active alarms  
  - Outlet status |
| **Settings** | *Module settings:*  
  - General  
  - Date & Time  
  - Users  
  - Network  
  - Protocols  
  - SNMP  
  - Certificates  
  - Email  
  - My Preferences |
| **Alarms** | *List of alarms with date and time:*  
  - Details  
  - Clear  
  - Export |
### Meters

**Power:**
- Frequency
- Voltage
- Current
- Power

**Measure logs:**
- Configuration
- Measure logs

### Controls

**Control of:**
- Entire UPS
- Battery Test
- Outlets

### Protection

- Scheduled shutdown
- Agent list
- Agent settings
- Power outage policy

### Sensors*

- Status
- Alarm configuration
- Information

### Card

- System information
- System logs
- Administration
- Commissioning (Sensors)

* Displayed when sensors are commissioned in Card menu.

### 2.2.2 Energy flow diagram

**Line interactive**

```
Main utility  |  Inverter  |  Output
            |   AVR     |   
            |  Battery  |   
```

--

**Diagram:**

- Main utility
- Inverter
- AVR
- Battery
- Charger
- Output
## Diagram elements description

<table>
<thead>
<tr>
<th>Symbols</th>
<th>Description</th>
<th>Possible states</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Main utility]</td>
<td><strong>Main utility</strong>&lt;br&gt;Possible states: Powered, Out of nominal range, Not present, Unknown</td>
<td><strong>Green</strong>&lt;br&gt;<strong>Yellow</strong>&lt;br&gt;<strong>Red</strong>&lt;br&gt;<strong>Black / White / Greyed</strong></td>
</tr>
<tr>
<td>![AVR]</td>
<td>The equipment is protected and powered through an <strong>AVR</strong> device.&lt;br&gt;Possible states: Normal mode, Buck mode, Boost mode, In overload, Not powered, Unknown</td>
<td><strong>Green</strong>&lt;br&gt;<strong>Yellow</strong>&lt;br&gt;<strong>Red</strong>&lt;br&gt;<strong>Black / White / Greyed</strong></td>
</tr>
<tr>
<td>![Output]</td>
<td>Output of the UPS.&lt;br&gt;Possible states: Protected, In overload, Not protected, In short circuit, Not powered, Unknown</td>
<td><strong>Green</strong>&lt;br&gt;<strong>Yellow</strong>&lt;br&gt;<strong>Red</strong>&lt;br&gt;<strong>Black / White / Greyed</strong></td>
</tr>
<tr>
<td>![Internal battery charger]</td>
<td>Internal battery charger.&lt;br&gt;Possible states: Charging, Floating, In fault, Resting, Not powered, Unknown</td>
<td><strong>Green</strong>&lt;br&gt;<strong>Yellow</strong>&lt;br&gt;<strong>Red</strong>&lt;br&gt;<strong>Black / White / Greyed</strong></td>
</tr>
<tr>
<td>![Battery]</td>
<td>Battery for the backup power.&lt;br&gt;Possible states: Powering the load, End of life, Not present, Not used to power the load, Unknown</td>
<td><strong>Green</strong>&lt;br&gt;<strong>Yellow</strong>&lt;br&gt;<strong>Red</strong>&lt;br&gt;<strong>Black / White / Greyed</strong></td>
</tr>
<tr>
<td>![Battery level]</td>
<td>Battery level&lt;br&gt;Possible states: &gt; 50% and &gt; low battery threshold (Settable on the UPS), &lt; 50% and &gt; low battery threshold (Settable on the UPS), &lt; Below low battery threshold (Settable on the UPS)</td>
<td><strong>Green</strong>&lt;br&gt;<strong>Yellow</strong>&lt;br&gt;<strong>Red</strong>&lt;br&gt;<strong>Black / White / Greyed</strong></td>
</tr>
<tr>
<td>![Inverter]</td>
<td>Inverter: convert DC power to AC power.&lt;br&gt;Possible states: Powered, In overload, In short circuit, In fault, Not powered, Unknown</td>
<td><strong>Green</strong>&lt;br&gt;<strong>Yellow</strong>&lt;br&gt;<strong>Red</strong>&lt;br&gt;<strong>Black / White / Greyed</strong></td>
</tr>
<tr>
<td>![Wiring]</td>
<td>Wiring&lt;br&gt;Possible states: Energy flow, In overload, Out of nominal range, No energy, Unknown</td>
<td><strong>Green</strong>&lt;br&gt;<strong>Yellow</strong>&lt;br&gt;<strong>Red</strong>&lt;br&gt;<strong>Black / White / Greyed</strong></td>
</tr>
</tbody>
</table>
Line interactive diagram examples

**Normal mode**

**Buck/Boost mode**

**Battery mode**
## Diagram elements description

<table>
<thead>
<tr>
<th>Symbols</th>
<th>Description</th>
<th>Possible states</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Symbol" /></td>
<td><strong>Main utility or second utility</strong>&lt;br&gt;Powered&lt;br&gt;Out of nominal range</td>
<td>Green</td>
</tr>
<tr>
<td><img src="image2.png" alt="Symbol" /></td>
<td><strong>Rectifier</strong>: convert AC power to DC power.&lt;br&gt;Powered&lt;br&gt;HE mode (ready)&lt;br&gt;In overload&lt;br&gt;In short circuit&lt;br&gt;In fault&lt;br&gt;Not powered&lt;br&gt;Unknown</td>
<td>Green</td>
</tr>
<tr>
<td><img src="image3.png" alt="Symbol" /></td>
<td><strong>Inverter</strong>: convert DC power to AC power.&lt;br&gt;Powered&lt;br&gt;HE mode (ready)&lt;br&gt;In overload&lt;br&gt;In short circuit&lt;br&gt;In fault&lt;br&gt;Not powered&lt;br&gt;Unknown</td>
<td>Green</td>
</tr>
<tr>
<td><img src="image4.png" alt="Symbol" /></td>
<td><strong>Output of the UPS.</strong>&lt;br&gt;Protected&lt;br&gt;In overload&lt;br&gt;Not protected&lt;br&gt;In short circuit&lt;br&gt;Not powered&lt;br&gt;Unknown</td>
<td>Green</td>
</tr>
<tr>
<td><img src="image5.png" alt="Symbol" /></td>
<td><strong>Internal battery charger.</strong>&lt;br&gt;Charging&lt;br&gt;Floating&lt;br&gt;In fault&lt;br&gt;Resting&lt;br&gt;Not powered&lt;br&gt;Unknown</td>
<td>Green</td>
</tr>
<tr>
<td><img src="image6.png" alt="Symbol" /></td>
<td><strong>Battery for the backup power.</strong>&lt;br&gt;Powering the load&lt;br&gt;End of life&lt;br&gt;In fault&lt;br&gt;Not present&lt;br&gt;Not used to power the load&lt;br&gt;Unknown</td>
<td>Green</td>
</tr>
<tr>
<td><img src="image7.png" alt="Symbol" /></td>
<td><strong>Battery level</strong>&lt;br&gt;(&gt; 50%) and (&lt; \text{low battery threshold (Settable on the UPS)})&lt;br&gt;(&lt; 50%) and (&gt; \text{low battery threshold (Settable on the UPS)})&lt;br&gt;(&lt; \text{below low battery threshold (Settable on the UPS)})</td>
<td>Green</td>
</tr>
<tr>
<td><img src="image8.png" alt="Symbol" /></td>
<td><strong>Automatic bypass</strong>&lt;br&gt;Powered (standby, auto bypass, forced bypass, high efficiency mode)&lt;br&gt;In overload&lt;br&gt;In fault&lt;br&gt;Not powered&lt;br&gt;Unknown</td>
<td>Green</td>
</tr>
</tbody>
</table>
### Maintenance bypass (optional)
- Powered (maintenance bypass)
- Not powered
- Unknown

### Wiring
- Energy flow
- In overload
- Out of nominal range
- No energy
- Unknown

### Online diagram examples

<table>
<thead>
<tr>
<th>Online mode</th>
<th>Single input source</th>
<th>Dual input sources</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Diagram" /></td>
<td><img src="image2" alt="Diagram" /></td>
<td><img src="image3" alt="Diagram" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bypass mode</th>
<th>Single input source</th>
<th>Dual input sources</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image4" alt="Diagram" /></td>
<td><img src="image5" alt="Diagram" /></td>
<td><img src="image6" alt="Diagram" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Battery mode</th>
<th>Single input source</th>
<th>Dual input sources</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image7" alt="Diagram" /></td>
<td><img src="image8" alt="Diagram" /></td>
<td><img src="image9" alt="Diagram" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>HE mode</th>
<th>Single input source</th>
<th>Dual input sources</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image10" alt="Diagram" /></td>
<td><img src="image11" alt="Diagram" /></td>
<td><img src="image12" alt="Diagram" /></td>
</tr>
</tbody>
</table>
2.2.3 Top bar

Current user – Display current user name
Logout – Logs the current user out by destroying the current user session
Status – Provides device (example UPS) status information
Output power – Provides output power status information
Battery status – Provides battery status information
Alarms button – Open alarm page
Settings button – Open settings page

2.2.4 Details

This view provides a summary of device identification information and nominal values:

- Name
- Model
- P/N
- S/N
- Location
- Firmware version
- Input Voltage
- Input Frequency
- Output Voltage
- Output Frequency

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.

2.2.5 Show measures

Provides input and output measures on the synoptic.

Example #1:

- Single input source
- 1 phase in
- 1 phase out
<table>
<thead>
<tr>
<th>Input measures</th>
<th>Output measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voltage (V)</td>
<td>Voltage (V)</td>
</tr>
<tr>
<td>Current (A)</td>
<td>Current (A)</td>
</tr>
<tr>
<td>Frequency (Hz)</td>
<td>Frequency (Hz)</td>
</tr>
</tbody>
</table>

Example #2:

Dual input sources

- 3 phases in
- 3 phases out

<table>
<thead>
<tr>
<th>Input measures (main and secondary)</th>
<th>Output measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase #1 Voltage (V)</td>
<td>Phase #1 Voltage (V)</td>
</tr>
<tr>
<td>Phase #1 Current (A)</td>
<td>Phase #1 Current (A)</td>
</tr>
<tr>
<td>Phase #2 Voltage (V)</td>
<td>Phase #2 Voltage (V)</td>
</tr>
<tr>
<td>Phase #2 Current (A)</td>
<td>Phase #2 Current (A)</td>
</tr>
<tr>
<td>Phase #3 Voltage (V)</td>
<td>Phase #3 Voltage (V)</td>
</tr>
<tr>
<td>Phase #3 Current (A)</td>
<td>Phase #3 Current (A)</td>
</tr>
<tr>
<td>Frequency (Hz)</td>
<td>Frequency (Hz)</td>
</tr>
</tbody>
</table>

2.2.6 Outlet status

Provides the status of the UPS outlets (ON/OFF) by load segmentation:

- Status (ON/OFF—Protected/Not protected/Not powered)
- Load level (W) – availability depending on the UPS model
- Shutdown countdown
- Startup countdown

Note: Load segmentations allow non-priority equipment to automatically power down during an extended power outage in order to keep battery runtime on essential equipment.

This feature is also used to remote reboot and sequential start servers in order to restrict inrush currents.

2.2.7 Active Alarms

Only active alarms are displayed, the Alarms icon will also display the number of active alarms.

Alarms are sorted by date, alert level, time, and description.

Note: To see the alarm history, press the Alarms button.
2.3 Alarms

2.3.1 Alarm sorting
Alarms can be sorted by selecting:

- All
- Active only

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

Example:

<table>
<thead>
<tr>
<th>Active</th>
<th>Opened</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Info</td>
<td><img src="image1" alt="Image" /> 10:35:52</td>
<td><img src="image2" alt="Image" /> 10:35:52 Group 1 - Group is OFF</td>
</tr>
<tr>
<td>Warning</td>
<td><img src="image3" alt="Image" /> 10:35:52</td>
<td><img src="image4" alt="Image" /> 10:35:52 Eaton 5P 850 - Load not powered</td>
</tr>
<tr>
<td>Critical</td>
<td><img src="image5" alt="Image" /> 11:11:13</td>
<td><img src="image6" alt="Image" /> 11:11:13 Eaton 5P 850 - No battery</td>
</tr>
</tbody>
</table>

2.3.3 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.

2.3.4 Alarm export
Press the Export button to download the file.
2.3.5 Clear alarm logs

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

2.3.6 Alarm list with codes

For details on alarm codes, see the *Information>>>Alarm log codes* section.

2.4 Settings

2.4.1 General

**Location**

Text field that is used to provide the card location information.
Card system information is updated to show the defined location.

**Contact**

Text field that is used to provide the contact name information.
Card system information is updated to show the contact name.
System name
Text field that is used to provide the system name information.
Card system information is updated to show the system name.

Default settings parameters and limitations

For details on default parameters and limitations, see the Information>>>Default settings parameters section.

2.4.2 Date & Time

The current date and time appears in the footer at the bottom of the screen.
You can set the time either manually or automatically.

Manual: Manually entering the date and time
1. Select the time zone for your geographic area from the time zone pull-down menu or with the map.
2. Select the date and time.
3. Save the changes.

Dynamic (NTP) : Synchronizing the date and time with an NTP server
1. Enter the IP address or host name of the NTP server in the NTP server field.
2. Select the time zone for your geographic area from the time zone pull-down menu or with the map.
3. Save the changes.

Note:
DST is managed based on the time zone.

Default settings parameters and limitations

For details on default parameters and limitations, see the Information>>>Default settings parameters section.
2.4.3 Users

Password strength rules

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

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

Press **Save** after modifications.

Account expiration

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

- Password expires after (in days).
- The 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.
• Block account when invalid password is entered after (in number of attempts).

The 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.

Press **Save** after modifications.

### Session expiration

<table>
<thead>
<tr>
<th>No activity timeout</th>
<th>15 minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session lease time</td>
<td>120 minutes</td>
</tr>
</tbody>
</table>

Modification on the session lease time will take effect at next session

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.

Press **Save** after modifications.

### Local users table

<table>
<thead>
<tr>
<th>New</th>
<th>Delete</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Username</th>
<th>Email</th>
<th>Profile</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td></td>
<td>Administrator</td>
<td>Active</td>
</tr>
<tr>
<td>user1</td>
<td></td>
<td>Viewer</td>
<td>Active</td>
</tr>
</tbody>
</table>

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

• **Username**
### Email

- Profile

<table>
<thead>
<tr>
<th></th>
<th>Viewer</th>
<th>Administrator</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Home</strong></td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>Alarms</strong></td>
<td>✔️ Alarm list</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>✔️ Export</td>
<td></td>
</tr>
<tr>
<td></td>
<td>✗ Clear</td>
<td></td>
</tr>
<tr>
<td><strong>Settings</strong></td>
<td>✗ General Date &amp; Time</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>✗ Users</td>
<td></td>
</tr>
<tr>
<td></td>
<td>✗ Network</td>
<td></td>
</tr>
<tr>
<td></td>
<td>✗ Protocols</td>
<td></td>
</tr>
<tr>
<td></td>
<td>✗ SNMP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>✗ Certificates</td>
<td></td>
</tr>
<tr>
<td></td>
<td>✔️ Email</td>
<td></td>
</tr>
<tr>
<td></td>
<td>✔️ My preferences</td>
<td></td>
</tr>
<tr>
<td><strong>Meters</strong></td>
<td>✔️ Power</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>✔️ Measure logs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>✗ Configuration</td>
<td></td>
</tr>
<tr>
<td><strong>Controls</strong></td>
<td>✗</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>Protection</strong></td>
<td>✗</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>Sensors</strong></td>
<td>✔️ Status</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>✗ Alarm configuration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>✔️ Information</td>
<td></td>
</tr>
<tr>
<td><strong>Card</strong></td>
<td>✔️ System information</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>✗ System logs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>✗ Administration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>✗ Commissioning (Sensors)</td>
<td></td>
</tr>
<tr>
<td><strong>Legal information (footer)</strong></td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>Contextual and Full documentation</strong></td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>Command Line Interface</strong></td>
<td>✗</td>
<td>✔️</td>
</tr>
</tbody>
</table>

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

### Actions

**Add**

Press the **New** button to create up to ten new users.

**Remove**

Select a user and press the **Delete** button to remove it.
Edit
Press the pen logo to edit user information and 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

LDAP

<table>
<thead>
<tr>
<th>Name</th>
<th>Address</th>
<th>Port</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site1</td>
<td>Site1</td>
<td>636</td>
<td>SSL + Server verified LDAP certificate</td>
</tr>
<tr>
<td>Site2</td>
<td>Site2</td>
<td></td>
<td>SSL + Server verified LDAP certificate</td>
</tr>
</tbody>
</table>

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

- Name
- Address
- Port
- Security
- Status – Status could take following values – Unreachable/Active
Actions
Configure
1. Press **Configure** to access the following LDAP settings:
• Active
• Base access
  • 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
  • Search base – Search base DN

• Request parameters
  • User base DN
  • User name attribute
  • UID attribute
  • Group base DN
  • Group name attribute
  • GID attribute

2. Click Save.

Profile mapping

1. Press Profile mapping to map remote groups to local profiles.
2. Click Save.
## LDAP users preferences

This settings will apply to all LDAP users

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Language</td>
<td>English</td>
</tr>
<tr>
<td>Temperature</td>
<td>°C</td>
</tr>
<tr>
<td>Date format</td>
<td>MM/DD/YYYY</td>
</tr>
<tr>
<td>Time format</td>
<td>24h</td>
</tr>
</tbody>
</table>

1. Press **Users preferences** to define preferences that will apply to all LDAP users
   - Language
   - Temperature
   - Date format
   - Time format

2. Click **Save**.

### Default settings parameters and limitations

For details on default parameters and limitations, see the Information>>>Default settings parameters section.
2.4.4 Network

LAN

A LAN is a computer network that interconnects computers within a limited area.

The available values for LAN configuration are listed below:

• Auto negotiation
• 10Mbps - Half duplex
• 10Mbps - Full duplex
• 100Mbps - Half duplex
• 100Mbps - Full duplex
• 1.0 Gbps - Full duplex

Any modifications are applied after the next Network Module reboot.

IPv4

Press the More button to configure the network settings, select either the Manual or Dynamic settings option:

Any modifications are applied after the Network Module reboots.
• **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.

• **Dynamic (DHCP)**
  Select dynamic DHCP to configure network parameters by a BootP or DHCP server.
  If a response is not received from the server, the UPS Network Module boots with the last saved parameters from the most recent power up. After each power up, the UPS Network Module makes five attempts to recover the network parameters.

**Domain**

The DNS is a hierarchical decentralized naming system for computers, services, or other resources connected to the Internet or a private network.

Press the **More** button to configure the network settings, select either the Static or Dynamic settings.
**Domain configuration**

- **Hostname**: `genap-0021`
- **Mode**: `Manual`
- **Domain name**: `mblab.em.com`
- **Primary DNS**: `10.198.32.2`
- **Secondary DNS**: `100.198.32.6`

**Static**
- Enter the Network Module Hostname.
- Enter the Network Module Domain name.
- Primary DNS server.
  - Enter the IP address of the DNS server that provides the translation of the domain name to the IP address.
- Secondary DNS server.
  - Enter the IP address of the secondary DNS server that provides the translation of the domain name to the IP address when the primary DNS server is not available.

**Dynamic**
- Enter the Network Module Hostname.

**IPv6**

- **Enable**: `✓`
- **Status**: `In service`
- **Mode**: `Router`
- **Address**: `2 Address`

IPv6 status and the first three addresses are displayed.

Press the **More** button to configure the network settings and get more information, press the **More** button for access to the following IPv6 details.
Current configuration
• Address
• Gateway

Address settings
• Mode
  • Manual
• Address
• Prefix
• Gateway
• Gateway
• Router
• DNS settings
  • Get automatically (will hide the following settings)
  • Primary DNS
  • Secondary DNS

Default settings parameters and limitations

For details on default parameters and limitations, see the Information>>>Default settings parameters section.

2.4.5 Protocols
This tab contains settings for communication protocols used to get information from the device through the network, such as https for web browser.

HTTPS

**HTTPS**

<table>
<thead>
<tr>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
</tr>
</tbody>
</table>

Only https is available.
The default network port for https is 443. For additional security, the ports can be changed on this page. Press **Save** after modifications.

Since only https is available, port 80 is not supported.

Default settings parameters and limitations

For details on default parameters and limitations, see the Information>>>Default settings parameters section.

2.4.6 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.
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:
1. Configure the IP address.
2. Select SNMP V1 or V1 and V3.
3. Compile the MIB you selected to be monitored by the SNMP manager.

For a list of supported MIBs, see the Information>>>Specifications/Technical characteristics section.

Press the Supported MIBs button to download the MIBs.

Settings
This screen allows an administrator to configure SNMP settings for computers that use the MIB to request information from the UPS 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:

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

Press Save after modifications.
2- Configure the SNMP V1 settings:

![Edit SNMP V1 community](image)

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

3- Configure the SNMP V3 settings:

![Edit SNMP V3 user](image)

1. Click the edit icon on either Read Only or Read/Write account to access settings.
2. Edit the user name.

3. Select Yes in the Active 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 Authentication level.
   - **None**—no further information is needed.
   - **SHA-1**—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 <&@#%_=:;,./?|$*

6. Click **Save**.

**Trap receivers**

<table>
<thead>
<tr>
<th>Application name</th>
<th>Host</th>
<th>Protocol</th>
<th>Port</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trap V1 1</td>
<td>000.000.0.0</td>
<td>V1</td>
<td>162</td>
<td>Active</td>
</tr>
<tr>
<td>Trap V1 2</td>
<td>000.000.0.0</td>
<td>V1</td>
<td>162</td>
<td>Active</td>
</tr>
<tr>
<td>Trap V3 1</td>
<td>000.000.0.0</td>
<td>V3</td>
<td>162</td>
<td>Active</td>
</tr>
</tbody>
</table>

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

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

Add

### New trap receiver

<table>
<thead>
<tr>
<th>Active</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application name</td>
<td></td>
</tr>
<tr>
<td>Hostname or IP address</td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td></td>
</tr>
<tr>
<td>Protocol</td>
<td></td>
</tr>
</tbody>
</table>

1. Press the **New** button to create new trap receivers.
2. Set following settings:
   - **Active** – Yes/No
   - **Application name**
   - **Hostname or IP address**
   - **Port**
   - **Protocol** – V1/V3
   - **Trap community (V1) / User (V3)**
3. Press the **SAVE** button.

Remove

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

Edit

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

Test all traps

Press the **Test all traps** 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 oid, see the **Information>>>SNMP trap oid** section.
Default settings parameters and limitations

For details on default parameters and limitations, see the Information>>>Default settings parameters section.

2.4.7 Certificates

Local certificates
Manage local certificates by:
- Generating CSR and import certificates signed by the CA.
- Generating new self-signed certificates.

Local certificates table

<table>
<thead>
<tr>
<th>Used for</th>
<th>Issued by</th>
<th>Valid from</th>
<th>Expiration</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protected applications (MQTT)</td>
<td>MQTT-prep-demos2 certified</td>
<td>01/11/2018</td>
<td>01/11/2020</td>
<td>Valid</td>
</tr>
<tr>
<td>Web Server</td>
<td>Web server-</td>
<td>01/06/2018</td>
<td>01/06/2019</td>
<td>Valid</td>
</tr>
</tbody>
</table>

The table shows the following information for each local certificates.
- Used for
- Issued by
- Valid from
- Expiration
- Status — valid, expires soon, or expired

Actions

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 appear, 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.

Export
Exports the selected certificate on your OS browser window.

Edit
Allows access to the following:
- Certificate summary
• Actions
  Generate a new self-signed certificate.
  Generate CSR.
  Import certificate (only available when CSR is generated).
• Details

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.

Create new certificates:

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.

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.

Certificate authorities (CA)
Manages CAs.

CA table

The table displays certificate authorities with the following details:
• Used for
• Issued by
• Issued to
• Valid from
• Expiration
• Status — valid, expires soon, or expired
Actions

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

**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.

**Edit**
Gives access to a summary of the certificate.

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**

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

Actions

**Start**
Starts the pairing window during the selected timeframe or until it is stopped.
Time countdown is displayed.

**Stop**
Stops the pairing window.
Trusted remote certificates

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

- Used for
- Issued by
- Issued to
- Valid from
- Expiration

In case a certificate expires, the connection with the client will be lost. If this happens, the user will have recreate the connection and associated certificates.

- Status — valid, expires soon, or expired

Actions

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

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

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

**Edit**
Gives access to a summary of the certificate.

### 2.4.8 Email

Email sending configuration

For examples on email sending configuration see the **Servicing the Network Management Module>>>Subscribing to a set of alarms for email notification** section.
Email sending configuration table
The table shows all the email sending configuration and includes the following details:

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

Actions

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

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

Edit
Press the pen icon to edit email sending configuration and access to the following settings:

- Active
- **Configuration name**
- **Email address**
- **Notify on events** – Severity level/Attach logs/Exceptions on events notification
- **Periodic report** – Active/Recurrence/Starting/Topic selection – Card/Devices
Edit email sending configuration

Active: Yes
Configuration name: Configuration #1
Email address: Myname@email.com

⚠ Notify on events (Enabled)
Active: Yes

On card events
<table>
<thead>
<tr>
<th>Severity</th>
<th>Subscribe</th>
<th>Attach logs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warning</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Info</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

On device events
<table>
<thead>
<tr>
<th>Severity</th>
<th>Subscribe</th>
<th>Attach logs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warning</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Info</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Exceptions on events notification

Always notify events with code 🟢

Never notify events with code 🟢

Periodic report (Enabled)
Active: Yes
Recurrence: Every Day
Starting:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Subscribe</th>
<th>Attach logs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Card</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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
- Sender address
- Secure SMTP connection
- Verify certificate authority
- SMTP server authentication

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

- Save and test server configuration

Default settings parameters and limitations

For details on default parameters and limitations, see the Information>>Default settings parameters section.

2.4.9 My preferences

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 Settings>>Users>>LDAP-Users preferences section.
Profile

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.

If you have the administrator’s rights, you can press the **pen logo** to edit user profile and update the following information:

- Full name
- Email
- Phone
- Organization

Temperature

- °C (Celsius)
- °F (Fareinheit)
Date format

- YYYY-MM-DD
- DD-MM-YYYY
- DD.MM.YYYY
- DD/MM/YYYY
- MM/DD/YYYY
- DD MM YYYY

Time format

- hh:mm:ss (24h)
- hh:mm:ss (12h)

Language

- German
- English
- Spanish
Default settings parameters and limitations

For details on default parameters and limitations, see the Information>>>Default settings parameters section.

2.5 Meters

2.5.1 Power

Main utility

<table>
<thead>
<tr>
<th>FREQUENCY</th>
<th>VOLTAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 Hz</td>
<td>0 V</td>
</tr>
<tr>
<td>50 Hz</td>
<td>243.7 V</td>
</tr>
<tr>
<td>70 Hz</td>
<td>294 V</td>
</tr>
</tbody>
</table>

Output

<table>
<thead>
<tr>
<th>FREQUENCY</th>
<th>VOLTAGE</th>
<th>POWER</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 Hz</td>
<td>230.3 V</td>
<td>0 W</td>
</tr>
<tr>
<td>50 Hz</td>
<td>250.78 V</td>
<td>1500 W</td>
</tr>
</tbody>
</table>

Displays the product input and output measures.

The numbers on the right side of a gauge show the scale. They do not indicate allowed or observed minimum or maximum levels.

Input

- Frequency (Hz)
- Voltage (V)

Output

- Frequency (Hz)
- Voltage (V)
- Power (W)
- Current (A)
2.5.2 Measure logs

Configuration

This log configuration allows to define the log acquisition frequency.

Measure logs

Press the Download measures button to download the log file.

If available, possible measures are listed below:

- Input Voltage (V)
- Input Frequency (Hz)
- Bypass Voltage (V)
- Bypass Frequency (Hz)
- Output Voltage (V)
- Output Frequency (Hz)
- Output Current (A)
- Output Apparent Power (VA)
- Output Active Power (W)
- Output Power Factor
- Output Percent Load (%)
- Battery Voltage (V)
- Battery Capacity (%)
- Battery Remaining Time (s)

Default settings parameters and limitations

For details on default parameters and limitations, see the Information>>>Default settings parameters section
2.6 Controls

2.6.1 UPS

<table>
<thead>
<tr>
<th>Status</th>
<th>Commands</th>
<th>Pending action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entire UPS</td>
<td>On Protected</td>
<td>Switch ON</td>
</tr>
<tr>
<td>Battery test</td>
<td>Pass</td>
<td>Quick test</td>
</tr>
</tbody>
</table>

Entire UPS

Controls are displayed for the entire UPS, and not for specific outlet options or battery test.

The table in this section displays UPS or battery status, the associated commands (on/off and battery test), and the pending action.

Status
Reflects the current mode of the UPS. The following is a list of potential table values that are displayed based on the UPS topology.

- On — Protected/Not protected
- Off — Not powered/Not protected

Commands
A set of commands are available and activated when one of the following buttons is pressed. A confirmation window appears.

- Safe OFF
This will shut off the load. Protected applications will be safely powered down.

This control is available only if the status is not OFF and if there are no active commands running.

- Safe reboot
This will shut off and then switch ON the load. Protected applications will be safely powered down.

This control is available only if the status is not OFF and if there are no active commands running.

- Switch ON
This will switch ON the load or turn ON the online UPS.

This control is available when the status is OFF, if there are no active commands running and if the Online UPS is on bypass.

Pending action
Displays the delay before shutdown and delays before startup.

Battery test

Status
Battery test status reflects the last completed battery test result, as well as its critical status (color) and completion time.

- Pass
- Warning
Controls

- Fail
- Unknown

Commands
Quick test and Advanced test buttons are disabled if a battery test is already in progress or scheduled.
The Abort button is enabled only when a test is in progress or scheduled.

Pending action
The pending action reflects the battery test status.
- None
- Scheduled
- In progress
- Aborted
- Done

2.6.2 Outlets

<table>
<thead>
<tr>
<th>Status</th>
<th>Commands</th>
<th>Pending action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group 1 — ON</td>
<td>Switch ON</td>
<td>Safe OFF</td>
</tr>
<tr>
<td></td>
<td>Safe reboot</td>
<td></td>
</tr>
<tr>
<td>Group 2 — ON</td>
<td>Switch ON</td>
<td>Safe OFF</td>
</tr>
<tr>
<td></td>
<td>Safe reboot</td>
<td></td>
</tr>
</tbody>
</table>

Group 1/ Group 2
Load segmentations allow, battery runtime to remain on essential equipment and automatically power down non-priority equipment during an extended power outage.

This feature is also used for remote reboot and the sequential start of servers in order to restrict inrush currents.

Status
It reflects the current outlet status.
- On — Protected/Not protected
- Off — Not powered

Commands
A set of commands are available and activated when one of the following buttons is pressed. A confirmation window appears.

- Safe OFF
This will shut off the load connected to the associated load segment. Protected applications are safely powered down.
This control is available only if the status is not OFF and if there are no active commands running.

- Safe reboot
This will power down and then switch ON the load connected to the associated load segment. Protected applications are safely powered down.
This control is available only if the status is not OFF and if there are no active commands running.

- Switch ON
This will switch ON the load connected to the associated load segment.
This control is available when status is OFF and if there are no active commands running.

Pending action
Displays the delay before shutdown and delay before startup.

2.7 Protection

2.7.1 Scheduled shutdowns

Use Scheduled Shutdowns to turn off either the UPS or individual load segments at a specific day and time.

This feature is used for saving energy by turning off equipment outside of office hours or to enhance cybersecurity by powering down network equipment.

If server shutdown scenarios are defined for any of the connected servers or appliances, they will be triggered before the corresponding outlets are turned off as configured in shutdown settings.

Scheduled shutdowns table

<table>
<thead>
<tr>
<th>Recurrence</th>
<th>Load segment</th>
<th>Shutdown time</th>
<th>Restart time</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Once</td>
<td>Primary</td>
<td>04/22/2018 09:44:08 EST</td>
<td>04/24/2018 09:44:08 EST</td>
<td>Active</td>
</tr>
<tr>
<td>Every day</td>
<td>Group 1</td>
<td>04/05/2018 09:44:08 EST</td>
<td>10/05/2018 09:44:08 EST</td>
<td>Active</td>
</tr>
<tr>
<td>Every week</td>
<td>Group 2</td>
<td>11/21/2018 09:44:08 EST</td>
<td>11/28/2018 09:44:08 EST</td>
<td>Active</td>
</tr>
</tbody>
</table>

The table displays the scheduled shutdowns and includes the following details.

- **Active** – Yes/No
- **Recurrence** – Once/Every day/Every week
- **Load segment** – Primary/Group 1/Group 2
- **Shutdown** – Date/Time
- **Restart** – Date/Time

Actions

**New**
Press the New button to create a scheduled shutdown.

**Remove**
Select a schedule shutdown and press the Remove button to delete the scheduled shutdown.

**Edit**
Press the pen icon to edit schedule shutdown and to access the settings.
2.7.2 Agent list

Pairing with shutdown agents

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.

Authentication and encryption of connections between the UPS network module and shutdown agents is based on matching certificates. Automated pairing of shutdown agents and UPS network modules is recommended in case the installation is done manually in a secure and trusted network, and when certificates cannot be created in other ways.

During the selected timeframe, new agent connections to the Network Module are automatically trusted and accepted. After automatic acceptance, make sure that all listed agents belong to your infrastructure. If not, access may be revoked using the Delete button.

For maximum security, Eaton recommend following one of the two methods on the certificate settings page:
- import client certificates manually.
- generate trusted certificate for both clients and Network Module using your own PKI.

Actions

Start
Starts the pairing window for the selected timeframe or until it is stopped.
Time countdown is displayed.

Stop
Stops the pairing window.

Agent list table

The table displays the IPP agent list that is connected to the Network Module and includes the following details:

- Name
- Address
- Version of the Agent
- Power source (Policy)
- Delay (in s)
- OS shutdown duration (in s)
- Status
- Communication
• In service | Protected
• In service | Not protected
• Stopping | Protected
• Stopped | Protected

• Communication
  • Connected | yyyy/mm/dd hh:mm:ss
  • Lost | yyyy/mm/dd hh:mm:ss

Actions

Delete

1. When the agent is connected, the Delete function will not work correctly because the agent will keep on trying to reconnect.

So connect to the software, remove the Network module from the Software nodes list (in the nodes list, right click on the Network module and click remove nodes).

When communication with the agent is lost, agent can be deleted by using the Delete button.

Select an agent and press the Delete button to delete the agent.

2.7.3 Agent settings

Agent shutdown sequence timing

<table>
<thead>
<tr>
<th>Primary</th>
<th>Name</th>
<th>Delay (s)</th>
<th>OS shutdown duration (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td></td>
<td></td>
<td>120</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Group 1</th>
<th>Name</th>
<th>Delay (s)</th>
<th>OS shutdown duration (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td></td>
<td></td>
<td>120</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Group 2</th>
<th>Name</th>
<th>Delay (s)</th>
<th>OS shutdown duration (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td></td>
<td></td>
<td>120</td>
</tr>
</tbody>
</table>

All agents that are connected to the Network Module are displayed in tables by power sources.

• Primary
• Group 1
• Group 2
The 'local agent' setting is used for setting for example a minimum shutdown duration, or a power down delay for a load segment that has no registered shutdown agents. One use case would be a load segment that powers network equipment that needs to stay on while servers and storage perform their orderly shutdown.

The tables include the following details:

- Name
- Delay (in s)
- OS shutdown duration (in s)

**Actions**

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

**Set OS shutdown duration**
Select and directly change the setting in the table and then **Save**.

**Examples**

Examples below show the impact of agent settings on the shutdown sequence for an ordered shutdown or an immediate shutdown.

<table>
<thead>
<tr>
<th>Agent settings examples</th>
<th>Sequential shutdown</th>
<th>Immediate shutdown</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td><strong>Delay (s)</strong></td>
<td><strong>OS shutdown duration (s)</strong></td>
</tr>
<tr>
<td>Local</td>
<td>120</td>
<td>120</td>
</tr>
<tr>
<td>Agent 1</td>
<td>10</td>
<td>60</td>
</tr>
<tr>
<td>Agent 2</td>
<td>60</td>
<td>60</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td><strong>Delay (s)</strong></td>
<td><strong>OS shutdown duration (s)</strong></td>
</tr>
<tr>
<td>Local</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Agent 1</td>
<td>60</td>
<td>60</td>
</tr>
<tr>
<td>Agent 2</td>
<td>60</td>
<td>60</td>
</tr>
</tbody>
</table>

**Note:**
The trigger in the diagram is the moment when the shutdown sequence starts and it is defined in the power outage policy section for each power source.

### 2.7.4 Power outage policy

These setting are in conjunction with the shutdown agents and control how the network module directs the shutdown of protected servers and appliances. It gives the possibility to prioritize and schedule shutdown actions so that the IT system is powered down in the correct order. For example, applications first, database servers next, and storage last. It is also possible to turn off some outlets to reduce power consumption and get longer battery runtime for the most important devices.

For examples on Powering down applications see the Servicing the Network Management Module >> Powering down/up applications examples section.
On power outage

<table>
<thead>
<tr>
<th>Power Source</th>
<th>Policy</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary</td>
<td>Maximize availability policy</td>
<td>by ending the shutdown sequence 30s before the end of backup time</td>
</tr>
<tr>
<td>Group 1</td>
<td>Load shedding policy</td>
<td>by starting the shutdown sequence</td>
</tr>
<tr>
<td></td>
<td>when on battery for 120s</td>
<td>OR</td>
</tr>
<tr>
<td></td>
<td>when the battery capacity is under 0%</td>
<td></td>
</tr>
<tr>
<td>Group 2</td>
<td>Load shedding policy</td>
<td>by starting the shutdown sequence</td>
</tr>
<tr>
<td></td>
<td>when on battery for 120s</td>
<td>OR</td>
</tr>
<tr>
<td></td>
<td>when the battery capacity is under 0%</td>
<td></td>
</tr>
</tbody>
</table>

Policies are set per power source (outlet groups) if they are present in the UPS.

Enable/Disable
For each power source, the shutdown policy can be enabled or disabled with check-boxes.
When disabled, the policy will be greyed out.

Set the policy
The available policies for shutdown are listed below from preset to customized settings:

**Preset policies**
- Maximize availability — To end the shutdown 30s before the end of backup time.
- Immediate graceful shutdown — To start the shutdown after 30s of backup time.

**Custom policies**
When there are several conditions to start the shutdown sequence, the shutdown sequence will start as soon as one of the conditions is reached.
- Load shedding — To start the shutdown when on battery for the set time in (s) or when battery capacity reaches the set capacity in (%). When disabled, the condition is greyed out.
- Custom — Same as load shedding but with 2 additional options:
  - to end the shutdown after the set time in (s) before the end of backup time.
  - to start shutdown after the set time in (s) before the end of backup time.
Protection

⚠️ When primary shuts OFF, both group1 and group 2 shut OFF immediately.
So if Primary is set to one of the following:

- Immediate graceful shutdown — groups policies should be restricted to immediate graceful shutdown.
- Load shedding — groups policies should avoid Maximize availability.

On custom policy, if the 2 checkboxes are unchecked, only the last condition is taken into account.

Settings examples
All the following examples are using below agents settings.

- **Example 1: Maximize availability policy**

  ![Maximize availability policy diagram](image)
• Example 2: Immediate graceful shutdown policy

• Example 3: Load shedding policy
Protection

Settings #2

Example 4: Custom policy

Settings #1
On low battery warning

In some cases, like a renewed power failure or failed battery, the capacity is much lower than anticipated. The UPS gives a Low battery warning when there is 2 - 3 minutes of estimated runtime left, depending on the UPS and its settings. This time is typically enough for shutting down a server, but does not allow sophisticated sequential shutdown schemes.

The Low battery policy is intended for these cases.

When utility comes back

These settings define the restart sequence when utility comes back. For example, this allows sequential startup of the IT system so that network and storage devices are connected to 'Primary' and start up immediately. After a delay database servers in Group1 are powered up, and then application and web servers in Group 2 are powered up. This startup would ensure that necessary services would be available for each layer when needed. A sequential startup will also help avoid a peak power draw in the beginning.
Options
- Keep shutdown sequence running until the end, and then restart (forced reboot).
- Wait until UPS battery capacity exceeds a set percentage value in (%), and then automatically restart the UPS.
  - Then restart Group 1 after a set time in (s).
  - Then restart Group 2 after a set time in (s).

Enable/Disable
Each option listed above can be enabled or disabled with check-boxes.
When disabled, the option will be greyed out.

2.8 Card

2.8.1 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.

Identification
- System name
- Product
- Physical name
- Vendor
- UUID
- Part number
- Serial number
- Hardware version
- Location
- Contact

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

2.8.2 System logs

Press the Download System Logs button to select the log files to download.
2.8.3 Administration

Network module firmware

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

Firmware information

- **Status**
  - Uploading
  - Invalid
  - Valid
  - Pending reboot
  - Active

- **Version**
  - Displays the associated firmware version.

- **Release date**
  - Displays the release date of the firmware.
  - For better performance, security, and optimized features, Eaton recommends to upgrade the Network Module regularly.

- **Installation date**
  - Displays when the firmware was installed in the Network Module.
Activation date
Displays when the firmware was activated in the Network Module.

Upgrade the Network Module firmware
During the upgrade process, the Network Module does not monitor the UPS Product 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. 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 UPS Network Module automatically restarts.

   **Network module is rebooting**

   Please wait a minute while the network module is restarting.

   Note that depending on your configuration the network module may restart with a different IP address.

   ! **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 Alarm section.

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.
2. A confirmation message displays, click Sanitize to confirm.
Reboot
Reboot means restarting the network module operating system.

To reboot the Network Module:
1. Click **Reboot**.
2. A confirmation message displays, click **Continue** to confirm, the reboot time will take approximately less than 2min.

Communication Lost and Communication recovered may appear in the Alarm section.

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.
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. None of the network module users or network informations are extracted.

To download the maintenance report file:

1. Click Download report.
2. A confirmation message displays, Maintenance report file successfully downloaded.

Settings

Allow to save and restore the Network module settings.

Save

Below settings are not saved:

- User accounts (user settings, passwords, preferences)
- Protection agents (agent list, agent settings)
- SNMPv3 authentication and privacy keys
- Sensor settings (commissioning, alarm configuration)
To save the Network module settings:

1. Click on **Save**
2. Select the settings to exclude
3. Click on **Continue**

**Restore**

Restoring settings may result in the Network module reboot.

To restore the Network module settings:

1. Click on **Restore**
2. Select the settings to exclude.
3. Click on **Continue**
4. Click again on **Continue** to confirm

2.8.4 Commissioning (sensors)

Sensors commissioning 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

<table>
<thead>
<tr>
<th>Polarity set</th>
<th>Current state</th>
<th>Dry contact status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normally open</td>
<td>open</td>
<td></td>
</tr>
<tr>
<td>Normally open</td>
<td>closed</td>
<td></td>
</tr>
<tr>
<td>Normally closed</td>
<td>closed</td>
<td></td>
</tr>
<tr>
<td>Normally closed</td>
<td>open</td>
<td></td>
</tr>
</tbody>
</table>

- **Communication** – Connected/Lost with dates

### Actions

**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.

**Delete**

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

⚠️ When a sensor is deleted, all the commissioning informations are deleted.

**Define offsets**

Select the sensors.

Press the **Define offset** button to adjust the temperature and humidity offsets of the selected sensors.

Extend the temperature or humidity section.

Set the offsets in the cell, temperatures and humidities will be updated accordingly.

Press the **Save** button when done.
Deactivated humidities or temperatures are not displayed.
Press the pen logo to edit sensor communication information and 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)

Press **Save** after modifications.

**Note:**

If the UPS provides temperature compensated battery charging option, see the *Servicing the EMP>>>Using the EMP for temperature compensated battery charging* section

### 2.9 Sensors

#### 2.9.1 Status (sensors)

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

#### Temperature table

<table>
<thead>
<tr>
<th>Name</th>
<th>Location</th>
<th>Current</th>
<th>Communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMPRT1H1C2 @2-T1</td>
<td>Lab_TOP</td>
<td>23.0°C</td>
<td>Connected</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Date: 06/22/2016 19:57:02 CEST</strong></td>
</tr>
<tr>
<td>EMPRT1H1C2 @1-S-T1</td>
<td>Lab_MIDDLE</td>
<td>23.4°C</td>
<td>Lost</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Date: 06/27/2016 08:19:27 CEST</strong></td>
</tr>
<tr>
<td>EMPRT1H1C2 @24-T1</td>
<td>Lab_BOTTOM</td>
<td>23.0°C</td>
<td>Connected</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Date: 06/22/2016 19:57:02 CEST</strong></td>
</tr>
</tbody>
</table>

The table shows the following information for each sensors.

- Name
- Location
- Current temperature
- Communication – Connected/Lost with dates

#### Humidity table

<table>
<thead>
<tr>
<th>Name</th>
<th>Location</th>
<th>Current</th>
<th>Communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMPRT1H1C2 @2-H1</td>
<td>Lab_TOP</td>
<td>37.0%</td>
<td>Connected</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Date: 06/22/2016 19:57:02 CEST</strong></td>
</tr>
</tbody>
</table>

The table shows the following information for each sensors.

- Name
- Location
- Current humidity
- Communication – Connected/Lost with dates
Dry contacts table

<table>
<thead>
<tr>
<th>Name</th>
<th>Location</th>
<th>Status</th>
<th>Communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lab_FRONT_DOOR</td>
<td>Lab_TOP</td>
<td></td>
<td>Connected</td>
</tr>
<tr>
<td>Lab_REAR_DOOR</td>
<td>Lab_TOP</td>
<td></td>
<td>Connected</td>
</tr>
</tbody>
</table>

The table shows the following information for dry contacts.

- Name
- Status
- Status with date

<table>
<thead>
<tr>
<th>Polarity set</th>
<th>Current state</th>
<th>Dry contact status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normally open</td>
<td>open</td>
<td></td>
</tr>
<tr>
<td>Normally open</td>
<td>closed</td>
<td></td>
</tr>
<tr>
<td>Normally closed</td>
<td>closed</td>
<td></td>
</tr>
<tr>
<td>Normally closed</td>
<td>open</td>
<td></td>
</tr>
</tbody>
</table>

- Communication – Connected/Lost with dates

2.9.2 Alarm configuration (sensors)

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

Temperature

<table>
<thead>
<tr>
<th>Name</th>
<th>Location</th>
<th>Enabled</th>
<th>Low critical</th>
<th>Low warning</th>
<th>Measure</th>
<th>High warning</th>
<th>High critical</th>
<th>Hysteresis</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMDT1H1C2 @2-T1</td>
<td>Lab_TOP</td>
<td></td>
<td>10</td>
<td>15</td>
<td>22.4°C</td>
<td>55</td>
<td>55</td>
<td>1</td>
</tr>
<tr>
<td>EMDT1H1C2 @1-T1</td>
<td>Lab_MIDDLE</td>
<td></td>
<td>10</td>
<td>15</td>
<td>22.4°C</td>
<td>55</td>
<td>55</td>
<td>1</td>
</tr>
<tr>
<td>EMDT1H1C2 @24-T1</td>
<td>Lab_BOTTOM</td>
<td></td>
<td>10</td>
<td>15</td>
<td>22.0°C</td>
<td>55</td>
<td>55</td>
<td>1</td>
</tr>
</tbody>
</table>

The table shows the following information and settings for each sensors.

- Name
- Enabled – yes/no
- Low critical threshold – xx°C or xx°F
- Low warning threshold – xx°C or xx°F
- Current temperature
- High warning threshold – xx°C or xx°F
• High critical threshold – xx°C or xx°F
• Hysteresis – x°C or x°F

Actions

Set Enabled
Select and directly change the setting in the table and then Save.
When disabled, no alarm will be sent.

Set alarm threshold
Select and directly 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.

Set Hysteresis
Select and directly 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.

Humidity

<table>
<thead>
<tr>
<th>Name</th>
<th>Location</th>
<th>Enabled</th>
<th>Low critical</th>
<th>Low warning</th>
<th>Measure</th>
<th>High warning</th>
<th>High critical</th>
<th>Hysteresis</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMPOT HQ/C @3-H1</td>
<td>Lab TOP</td>
<td>yes</td>
<td>10</td>
<td>20</td>
<td>27.5%</td>
<td>60</td>
<td>70</td>
<td>1</td>
</tr>
</tbody>
</table>

The table shows the following information and settings for each sensors.

• Name
• Enabled – yes/no
• Low critical threshold – xx%
• Low warning threshold – xx%
• Current humidity
• High warning threshold – xx%
• High critical threshold – xx%
• Hysteresis – x%

Actions

Set Enabled
Select and directly change the setting in the table and then Save.
When disabled, no alarm will be sent.

Set alarm threshold
Select and directly 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.

Set Hysteresis
Select and directly 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.
Dry contacts

<table>
<thead>
<tr>
<th>Name</th>
<th>Location</th>
<th>Enabled</th>
<th>Alarm severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lab_FRONT_DOOR</td>
<td>Lab_TOP</td>
<td>x</td>
<td>info</td>
</tr>
<tr>
<td>Lab_REAR_DOOR</td>
<td>Lab_TOP</td>
<td>x</td>
<td>info</td>
</tr>
</tbody>
</table>

The table shows the following settings for each dry contacts.

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

Actions

Set Enabled
Select and directly change the setting in the table and then Save.
When disabled, no alarm will be sent.

Set alarm severity
Select and directly change the setting in the table and then Save.
Dry contacts alarm will be sent at the selected level.

Default settings parameters and limitations

For details on default parameters and limitations, see the Information>>>Default settings parameters section

2.9.3 Information (sensors)

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

EMPDT1H1C2 @1

- Physical name Eaton EMPDT1 H1C2
- Vendor Eaton
- Part number EMPDT1H1C2
- Firmware version 01.02.0009
- UUID c9fe1f8af0b0d0db7f624e754b6e9c
- Serial number GB13j28274
- Location -
2.10 Legal information (footer)

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

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

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

2.10.3 Availability of source code
Provides the way to obtain the source code of open source components that are made available by their licensors.
2.11 Contextual help and full documentation

2.11.1 Access to contextual help

Press ? icon on the top right side of the page to access the contextual help.

Contextual help can be closed by pressing the X icon on the top right of the page.

Search feature is indexed, but when inside the contextual help section it won't search in the full documentation.

To get better results when searching, search inside the full documentation.

2.11.2 Access to full documentation

Press ? icon on the top right side of the page to access the contextual help.

In the contextual help section, press the Full documentation button on the top right to access the full documentation in a new window.

You can then navigate into below sections:

- Contextual help
- Servicing the Network Management Module
- Securing the Network Management Module
- Information
- Troubleshooting
3 Servicing the Network Management Module

3.1 Unpacking the Network module

The network module will include the following:

- Network module
- Quickstart
- USB AM to Micro USB/M/5P 5ft Cable

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.

3.2 Installing the Network Module

3.2.1 Mounting the Network Module

It is not necessary to power down the UPS before installing the Network Module.

Required tools: No. 2 Phillips screwdriver.

The Network Module is hot-swappable. Inserting and/or extracting the Network Module from the communication slot of the product has no effect on the output.

1. Remove the two screws securing the option slot cover plate and store the plate for possible future use.

2. Install the Network Module along the alignment channels in the option slot. Secure the Network Module using the two screws you removed in step 1.

3. If the product is powered up, you can verify that the Network Module is seated properly and communicating with the product by checking that the Status ON LED flashes green after 2 minutes.
3.2.2 Accessing the web interface through Network

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.

Accessing the web interface

1. On a network computer, launch a supported web browser. The browser window appears.
2. In the Address/Location field, enter: `https://xxx.xxx.xxx.xxx`, where `xxx.xxx.xxx.xxx` is the static IP address of the Network Module. The log in screen appears.
3. Enter the user name in the User Name field. The default user name is `admin`.
4. Enter the password in the Password field. The default password is `admin`. The password must be changed at first login.
5. Click **Sign In**. The Network Module web interface appears.

3.2.3 Finding and setting the IP address

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

Read from the device LCD

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

1. 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.

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 Settings>>>Network>>>IPV4.
• Read the IPv4 settings.

Your network is not equipped with a BOOTP/DHCP server

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 Settings>>>Network>>>IPV4.
• Select Manual (Static IP).
• Input the following information:
  IPv4 Address
  Subnet Mask
  Default Gateway
• Save the changes.

3.2.4 Accessing the web interface through RNDIS

Connecting the configuration cable
1. Connect the Micro-B to USB cable to a USB connector on the host computer.
2. Connect the cable to the Settings connector on the Network Module.

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

Web interface access through RNDIS

Configuring the RNDIS

Automatic configuration

1. 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.

Manual configuration
1. In case Windows® OS fails to find driver automatically, go to the Windows control panel>Network and sharing center>Local area connection
2. Right click on the RNDIS local area connection and select Properties.

4. Then enter the configuration as below and validate (IP = 169.254.0.150 and mask = 255.255.255.0), click OK, then click on Close.

![Image of Internet Protocol Version 4 (TCP/IPv4) Properties]

Accessing the web interface
1. Be sure that the UPS is powered on.

2. On the host computer, download the RNDIS_Serial.zip file from the website [www.powerquality.eaton.com/Support/](http://www.powerquality.eaton.com/Support/) and extract it.

For more information, navigate to [Accessing to the latest Network Module firmware/driver section](#).

3. Launch setProxy.bat to add 169.254.* in proxy’s exceptions list, if needed.

4. Launch a supported browser, the browser window appears.

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.

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

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

8. Click **Sign In**. The Network Module local web interface appears.
3.2.5 Accessing the card through serial terminal emulation

Connecting the configuration cable

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

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

Manual configuration of the serial connection

1. On the host computer, download the RNDIS_Serial.zip file from the website www.powerquality.eaton.com/Support/ and extract it.
2. Plug the USB cable and go to Windows® Device Manager.
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.

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.
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.

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

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

7. The installation is successful when the COM port number is displayed for the Gadget Serial device in the Windows® Device Manager.
Accessing the card through Serial
Use the console and get access to the card, refer to CLI section to get command instructions.

3.2.6 Configuring the UPS Network Module settings
Use Eaton UPS Network Module web interface to configure the UPS Network Module.
Main web interface menus are described below:

<table>
<thead>
<tr>
<th>Menu</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home page</td>
<td>Overview of the UPS/Module status (Synoptic, Alarm, Meters, Load segments, ...).</td>
</tr>
<tr>
<td>Module settings</td>
<td>Date&amp;Time, Users, Alerts, Network, Protocols, System logs, My Preferences, ...).</td>
</tr>
<tr>
<td>List of Alarms</td>
<td>Date, time and description.</td>
</tr>
<tr>
<td>Power quality</td>
<td>Meters.</td>
</tr>
<tr>
<td>Entire UPS Control</td>
<td>Battery test, Load Segments control.</td>
</tr>
<tr>
<td>Scheduled Shutdown</td>
<td>Protected Application, Agents Settings, Power Outage Policy.</td>
</tr>
</tbody>
</table>
3.3 Configuring/Commissioning/Testing LDAP

3.3.1 Commissioning

Refer to the section Contextual Help>>>Settings>>>Users to get help on the configuration.

Configuring connection to LDAP database

This step configures the LDAP client of the network module in order 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 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).

Typical request parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>OpenLDAP</th>
<th>Active Directory™ with POSIX account activated</th>
<th>Active Directory™</th>
</tr>
</thead>
<tbody>
<tr>
<td>User base DN</td>
<td>ou=users, dc=example, dc=com</td>
<td>ou=users, dc=example, dc=com</td>
<td>ou=users, dc=example, dc=com</td>
</tr>
<tr>
<td>User name attribute</td>
<td>uid</td>
<td>uid</td>
<td>sAMAccountName</td>
</tr>
<tr>
<td>UID attribute</td>
<td>uidNumber</td>
<td>uidNumber</td>
<td>objectSid:S-1-5-xx-yy-zz (domain SID)</td>
</tr>
<tr>
<td>Group base DN</td>
<td>ou=groups, dc=example, dc=com</td>
<td>ou=groups, dc=example, dc=com</td>
<td>ou=groups, dc=example, dc=com</td>
</tr>
<tr>
<td>Group name attribute</td>
<td>gid</td>
<td>gid</td>
<td>sAMAccountName</td>
</tr>
<tr>
<td>GID attribute</td>
<td>gidNumber</td>
<td>gidNumber</td>
<td>objectSid:S-1-5-xx-yy-zz (domain SID)</td>
</tr>
</tbody>
</table>

Testing connection to LDAP database

Refer to the section Information>>>CLI>>>ldap-test to get help on the CLI command.

To test connection to the LDAP database:
1. Connect to the CLI.
2. Launch `ldap-test --checkusername` command.
3. In case of error, use the `verbose` option of the command to investigate the reason.

### 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 5 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.

### Testing profile mapping

Refer to the section Information>>>CLI>>>ldap-test to get help on the CLI command.

To test LDAP users profile mapping:
1. Connect to the CLI.
2. Launch `ldap-test --checkmappedgroups` command.
3. This command will verify each mapped group exists in the LDAP base and will display the associated local profile.
4. In case of error, use the `verbose` option of the command to investigate the reason.

### Define LDAP users preferences

This step configures the users preferences to apply to all LDAP users.

#### 3.3.2 Testing LDAP authentication

Refer to the section Information>>>CLI>>>ldap-test to get help on the CLI command.

1. Connect to the CLI.
2. Launch `ldap-test --checkuserauth` command.
3. This command will verify an LDAP user can authenticate using his username and password and will display its local profile.
4. In case of error, use the `verbose` option of the command to investigate the reason

### 3.3.3 Limitations

- If the same username exists in both local and LDAP databases, the behaviour 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 users preferences are common to all LDAP users.
- LDAP users cannot change their password through the Network Module.

### 3.4 Pairing agent to the Network Module

Authentication and encryption of connections between the UPS network module and shutdown agents is based on matching certificates.
3.4.1 Pairing with automatic acceptance (recommended if done in a secure and trusted network)

Pairing with automatic acceptance of shutdown agents and UPS network modules is recommended in case the installation is done in a secure and trusted network, and when certificates cannot be created in other ways.

**STEP 1:** Action on the Network Module

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 static 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 **Sign In**. The Network Module web interface appears.

2. Navigate to Protection/Agents list page

3. In the Pairing with shutdown agents section, select the time to accept new agents and press the **Start** button and the press **Continue**. During the selected timeframe, new agent connections to the Network Module are automatically trusted and accepted.

**STEP 2:** Action on the agent while the time to accepts new agents is running on the Network Module

1. Connect to the web interface of the agent

2. Detect the UPS Network Module with a **Quick scan**, **Range scan** or an **Address(es) scan**.

3. Right-click on the UPS Network Module when discovered and then **Add** a power source, **Configure** it, and **Save** it.

**STEP 3:** Action on the Network Module

1. Make sure all listed agents in the card (Protection/Agents list) belong to your infrastructure, if not, access may be revoked using the **Delete** button.

2. If the time for pairing still runs, you can stop it. Press **Stop** in the Pairing with shutdown agents section.

**Note:** After that stage, the agent creates a client certificate. The power source could show a communication loss since the current client certificate is not trusted by the Network Module.

3.4.2 Pairing with manual acceptance (maximum security)

Manual pairing provides the maximum security.

**STEP 1:** Action on the agent

1. Connect to the web interface of the agent

2. Detect the UPS Network Module with a **Quick scan**, **Range scan** or an **Address(es) scan**.

3. Define the power source

   **Note:** After that stage, the agent creates a client certificate. The power source could show a communication loss since the current client certificate is not trusted by the Network Module.

4. Copy the agent certificate file **client.pem** that is located in the folder

**STEP 2:** Action on the Network Module

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 static 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 Sign In. The Network Module web interface appears.

2. Navigate to Settings/Certificate page

3. In the Trusted remote certificates section, click Import, select Protected applications (MQTT) and then click on CONTINUE

4. Select the client.pem file previously saved, click Open. Communication with the agent is restored.

3.5 Powering down/up applications (examples)

3.5.1 Powering down IT system in a specific order

Target
Powering down applications first (when on battery for 30s), database servers next (3min after the applications), and storage last (as late as possible).

Step 1: Installation setup

Objective
Use load segmentation provided by the UPS to independently control the power supply of each IT equipment categories (Applications, Database servers, Storage).

It also allows IT equipment to sequentially restart on utility recovery (Restart sequentially the IT equipment on utility recovery).

Resulting setup
UPS provides outlets (Group 1 and Group 2) and a primary output.

⚠️ When primary shuts OFF, both group 1 and group 2 shut OFF immediately.

Connections to UPS are done as described below:

• Group 1: Applications
Powering down/up applications (examples)

- Group 2: Database servers
  - Primary: Storage

Step 2: Agent settings

Objective
Ensure IT solution is shutdown gracefully.

Resulting setup
1. Install IPP Software on each servers (Application, Database servers, Storage) and register the UPS load segment as power source:
   - Applications: Group 1
   - Database servers: Group 2
   - Storage: Entire UPS

2. Pair agent to the Network Module (Pairing agent to the Network Module).
   When done, each servers appears in the Agent list.

3. Navigate to Protection/Agent settings page.

   For examples of Agent settings, see the Agent settings examples section.

4. Set the OS shutdown duration to the time needed for your server to shutdown gracefully.
   This will make sure IPP shuts down your servers before the load segment is powered down.
   As a result, it will define the overall shutdown sequence duration for each load segments.

Step 3: Power outage policy settings

Objective
Use load segment policies to define shutdown sequencing.

Resulting setup
1. Navigate to Protection/Power outage policy page of the Network Module

   For examples of Power outage policy, see the following sections:
   - Maximize availability policy example
   - Immediate graceful shutdown policy example
   - Load shedding policy examples
   - Custom policy examples

2. Enable policies of Primary, Group 1 and Group 2.

3. Set Primary to: maximize availability policy.
Powering down/up applications (examples)

Storage is the last one to power down, its availability is maximized and its shutdown will end 30s before the end of backup time.

4. Set Group 1 and Group 2 to: **load shedding policy**.

   Applications must shutdown first so Group 1 has been set to start shutdown when on battery for 30s.
   
   Servers must shutdown second so Group 2 has been set to start shutdown when on battery for 210s, so 3min after the applications.

### 3.5.2 Powering down non-priority equipment first

**Target**

Powering down non-priority equipment first (immediately) and keep battery power for critical equipment.

Powering down critical equipment 3min before the end of backup time.
Step 1: Installation setup

Objective
Use load segmentation provided by the UPS to independently control the power supply of each IT equipment categories (Applications, Database servers, Storage).

Load segmentation also allows IT equipment to restart sequentially on utility recovery. (Restart sequentially the IT equipment on utility recovery).

Resulting setup
UPS provides outlets (Group 1 and Group 2) and a primary output.

⚠️ When primary shuts OFF, both group 1 and group 2 shut OFF immediately.

Connections can be done as described below:
- Group 2: non-priority equipment
- Group 1: critical equipment
- Primary: critical equipment

Step 2: Agent settings

Objective
Ensure IT solution is shutdown gracefully.

Resulting setup
1. Install IPP Software on each servers (Application, Database servers, Storage) and register the UPS load segment as power source:
   - Critical equipment: Group 1
   - Non-priority equipment: Group 2
   - Critical equipment: Entire UPS

2. Pair agent to the Network Module (Pairing agent to the Network Module).
   When done, each servers appears in the Agent list.

3. Navigate to Protection/Agent settings page

⚠️ For examples of Agent settings, see the Agent settings examples sections.

4. Set the OS shutdown duration to the time needed for your server to shutdown gracefully.
   This will make sure IPP shutdowns your servers before the load segment is powered down.
   As a result, it will define the overall shutdown sequence duration for each load segments.

Step 3: Power outage policy settings

Objective
Use load segment policies to define shutdown sequencing.

Resulting setup
1. Navigate to Protection/Power outage policy page on the Network Module
2. Enable policies of Primary, Group 1 and Group 2.

3. Set Primary and Group 1 to: **custom policy** and set it to end shutdown sequence 180s before the end of backup time.

4. Set Group 2 to: **immediate graceful shutdown policy**.

Critical equipment is the last one to power down, their availability will be maximized and their shutdown will end 180s before the end of backup time.

Non-priority equipment immediately shuts down when on battery for 10s to keep battery power for critical equipment.
3.5.3 Restart sequentially the IT equipment on utility recovery

Target
Restart the storage first (right after utility recovery), database servers next (2min after utility recovery) and applications last (3min after utility recovery).

Step 1: Installation setup

Objective
Use load segmentation provided by the UPS to independently control the power supply of each IT equipment categories (Applications, Database servers, Storage).
This will allow to restart sequentially the IT equipment on utility recovery.

Resulting setup
UPS provides outlets (Group 1 and Group 2) and a primary output.

⚠️ When utility recovers, primary starts immediately.

Connections to UPS can be done as described below:
- Group 1: Applications
- Group 2: Database servers
- Primary: Storage

Step 2: Power outage policy settings

Objective
Use load segment restart settings to define restart sequencing.

Resulting setup
1. Navigate to Protection/Power outage policy page and to the When utility comes back section.
When utility comes back:

- Keep shutdown sequence running until the end and then restart (forced reboot)
- Automatically restart the UPS when battery capacity exceeds

Then Group 1 after 120s
Then Group 2 after 60s

2. Enable the "Keep shutdown sequence running until the end and then restart (forced reboot)".
3. Enable the "Automatically restart the UPS when battery capacity exceeds" and set it to 0%.
   The storage will restart first, right after utility recovery without waiting the battery capacity to exceed a % limit.
4. Set Then Group 1 after to 120s.
   The database servers will restart 120s after the utility recovery.
5. Set Then Group 2 after to 60s.
   The database servers will restart 180s after the utility recovery.

3.6 Checking the current firmware version of the Network Module

Current firmware of the Network Module can be accessed in:
- The footer: Version: x.xx.x
- The Card menu: Card>>>System information>>>FW information: Firmware version x.xx.x
- The Card menu: Card>>>Administration>>>Network module firmware: Active FW version x.xx.x

3.7 Accessing to the latest Network Module firmware/driver/script

Download the latest Eaton Network Module firmware, driver or script from the Eaton website www.powerquality.eaton.com/Support/.

3.8 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

3.8.1 Web interface
To upgrade the Network module through the Web interface, refer to the section: Firmware upgrade through the Web interface.

3.8.2 Shell script

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
```

### 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:

```
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
```

3.8.3 Example:

```
$ ./install_updatePackage.sh -u admin -p <mypassword> -f FW_Update.tar -i <cardIpAddress> -r
```
3.9 Changing the RTC battery cell

1. Access the Network Module, and then disconnect the Network cable, if needed.
2. Unscrew the Network Module and remove it from the slot.
3. Locate the RTC battery cell located on the back of the Network Module.

4. Get a new battery cell (CR1220 type).

5. Replace the battery cell, the positive mark (+) should be visible when inserting it.
6. Replace the Network Module and secure the screw, reconnect the Network cable if it was unplugged during the operation.

7. Connect the Network Module and set the date and time. For more information, see the Date & Time section.
3.10 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 to implement 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 Date and Time section.

3.11 Synchronizing the time of the Network Module and the UPS

This section is valid only when the UPS can manage date and time (refer to the UPS user manual for confirmation).

The Network Module use UTC time and manage the time zone and the DST.
The UPS manage only the local time.

3.11.1 Automatic time synchronization

Everyday at 5 a.m
The UPS time (local time) is synchronized with the Network Module.

If the Network Module time is lost
The Network Module and the UPS time is synchronized with the oldest time between the last know Network Module time and the UPS time.

3.11.2 Manual time synchronization

From the Network Module
On the Network Module, navigate to Settings>>>Date & Time section and update the time.
The UPS time (local time) is directly synchronized with the Network Module.

From the UPS

When the time is updated on the UPS, it is not synchronized on the Network Module.

3.12 Changing the language of the web pages

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

1. Navigate to Settings>>>My preferences>>>Language.
2. Select the language, and then press the Save button.
3.13 Resetting username and password

1. Navigate to Settings>>>Users.
2. Press the pen icon ℹ️ 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.

3.14 Recovering main administrator password

To reset the main administrator password:

1. Access the Network Module, disconnect the Network cable, if needed.
2. Unscrew the Network Module and remove it from the slot.
3. Locate the RESET switch that is located on the back of the Network Module.
4. Peel off the protection:

5. Change the position of switch number 3, this change is detected during power ON and the reset will be applied:

   Case 1:
3.15 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 Settings>>>Network>>>IPV4.
2. Select Manual (Static IP).
3. Input the following information:
   - IPv4 Address
   - Subnet Mask
   - Default Gateway
4. Save the changes.

3.16 Reading product (UPS) information in a simple way

3.16.1 Web page

The product information is located in the Home page, specifically with the Details button on the top of the diagram and in the Meters menu.

3.17 Subscribing to a set of alarms for email notification

3.17.1 Example #1: subscribing only to one alarm (load unprotected)

Follow the steps below:

1. Navigate to Settings>>>Email>>>Email sending configuration.
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)
4. Press **Save**, the table will show the new configuration.

Logs will be attached by default in that example even if there is no subscription on card or device events.
3.17.2 Example #2: subscribing to all Critical alarms and some specific Warnings

Follow the steps below:

1. Navigate to Settings>>>Email>>>Email sending configuration.

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)
Add email sending configuration

Active: Yes
Configuration name: ALL Critical and User account Warning notification
Email address: myaddress@mycompany.com

Notify on events *(Disabled)*
Active: No

On card events

<table>
<thead>
<tr>
<th>Severity</th>
<th>Subscribe</th>
<th>Attach logs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Warning</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Info</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

On device events

<table>
<thead>
<tr>
<th>Severity</th>
<th>Subscribe</th>
<th>Attach logs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Warning</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Info</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Exceptions on events notification

Always notify events with code ✔

0800700.0800900

4. Press **Save**, the table will show the new configuration.
4 Securing the Network Management Module

4.1 Cybersecurity considerations for electrical distribution systems

4.1.1 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.

4.1.2 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.

4.1.3 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

4.1.4 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.
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

4.1.5 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.”
4.1.6 Designing for the threat vectors

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 preestablished 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.

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.
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.
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

4.1.7 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

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.

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.
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.

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.

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
Cybersecurity considerations for electrical distribution systems

- People and processes
- Network security
- Host security
- Applications security (both internally developed and commercially off-the-shelf (COTS))

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.

4.1.8 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.

4.1.9 Terms and definitions

| DMZ | 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. |
| Encryption | The process of transforming plain or clear text using an algorithm to make it unreadable to anyone except those possessing special knowledge. |
| ICS | A device or set of device that manage, command, direct, or regulate the behavior of other devices or systems. |
| Protocol | A set of standard rules for data representation, signaling, authentication, and error detection required to send information over a communications channel |
4.1.10 Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>COTS</td>
<td>Commercially Off-the-Shelf</td>
</tr>
<tr>
<td>DMZ</td>
<td>Demilitarized Zone</td>
</tr>
<tr>
<td>DOS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>HMI</td>
<td>Human Machine Interface</td>
</tr>
<tr>
<td>ICS</td>
<td>Industrial Control Systems</td>
</tr>
<tr>
<td>ICS-CERT</td>
<td>Industrial Control Systems - Cyber EmergencyResponse Team</td>
</tr>
<tr>
<td>IDPS</td>
<td>Intrusion Detection and Prevention Systems</td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection Systems</td>
</tr>
<tr>
<td>IPS</td>
<td>Intrusion Prevention Systems</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>NVD</td>
<td>National Vulnerability Database</td>
</tr>
<tr>
<td>OSI</td>
<td>Open System Interconnection</td>
</tr>
<tr>
<td>PLC</td>
<td>Programmable Logic Controller</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control and Data Acquisition</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>SIEM</td>
<td>Security Information and Event Management</td>
</tr>
<tr>
<td>USB</td>
<td>Universal Serial Bus</td>
</tr>
</tbody>
</table>

4.1.11 References


4.2 Cybersecurity recommended secure hardening guidelines

4.2.1 Introduction
This Network module has been designed with Cybersecurity as an important consideration. Number of Cybersecurity features are now offered in the product which if implemented as per the recommendations in this section would minimize Cybersecurity risk to the Network module. This section “secure configuration” or “hardening” guidelines provide information to the users to securely deploy and maintain their product to adequately minimize the cybersecurity risks to their system.

Eaton is committed to minimizing the Cybersecurity risk in its products and deploys cybersecurity best practices and latest cybersecurity technologies in its products and solutions; making them more secure, reliable and competitive for our customers. Eaton also offers Cybersecurity Best Practices whitepapers to its customers that can be referenced at www.eaton.com/cybersecurity

4.2.2 Secure configuration guidelines

Asset identification and Inventory
Keeping track of all the devices in the system is a pre-requisite for effective management of Cybersecurity of a system. Ensure you maintain an inventory of all the components in your system in a manner in which you uniquely identify each component. To facilitate this Network module supports the following identifying information - manufacturer, type, serial number, f/w version number, and location.

Network Module identification and its firmware information
It can be retrieved by navigating to Card>>>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

Communication settings
It can be retrieved by navigating to Settings>>>Network

LAN
- Link status
- MAC address

The COPY TO CLIPBOARD button will copy the information to the clipboard.
Cybersecurity recommended secure hardening guidelines

Securing the Network Management Module

- Configuration

**IPV4**
- Status
- Mode
- Address
- Netmask
- Gateway

**Domain**
- Mode
- FQDN
- Primary DNS
- Secondary DNS

**IPV6**
- Status
- Mode
- Addresses

**UPS details**
It can be retrieved by navigating to **Home>>>Details**

**Details**
- Name
- Model
- P/N
- S/N
- Location
- FW version

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

**Physical Protection**
Industrial Control Protocols don’t offer cryptographic protections at protocol level, at physical ports and at controller mode switches leaving them exposed to Cybersecurity risk. Physical security is an important layer of defense in such cases. Network module is designed with the consideration that it would be deployed and operated in a physically secure location.

- Physical access to cabinets and/or enclosures containing Network module and the associated system should be restricted, monitored and logged at all times.
- Physical access to the communication lines should be restricted to prevent any attempts of wiretapping, sabotage. It’s a best practice to use metal conduits for the communication lines running between one cabinet to another cabinet.
- Attacker with unauthorized physical access to the device could cause serious disruption of the device functionality. A combination of physical access controls to the location should be used, such as locks, card readers, and/or guards etc.
- Network module supports the following physical access ports, controller mode switches and USB ports: RJ45, USB A, USB Micro-B. Access to them need to be restricted.
- Do not connect unauthorized USB device or SD card for any operation (e.g. Firmware upgrade, Configuration change and Boot application change).
- Before connecting any portable device through USB or SD card slot, scan the device for malwares and virus.

**Authorization and Access Control**
It is extremely important to securely configure the logical access mechanisms provided in Network module to safeguard the device from unauthorized access. Eaton recommends that the available access control mechanisms be used properly to ensure that access to the system is restricted to legitimate users only. And, such users are restricted to only the privilege levels necessary to complete their job roles/functions.
Cybersecurity recommended secure hardening guidelines

- Ensure default credentials are changed upon first login. Network module should not be commissioned for production with Default credentials; it’s a serious Cybersecurity flaw as the default credentials are published in the manuals.
- No password sharing – Make sure each user gets his/her own password for that desired functionality vs. sharing the passwords. Security monitoring features of Network module are created with the view of each user having his/her own unique password. Security controls will be weakened as soon as the users start sharing the password.
- Restrict administrative privileges - Threat actors are increasingly focused on gaining control of legitimate credentials, especially those associated with highly privileged accounts. Limit privileges to only those needed for a user’s duties.
- Perform periodic account maintenance (remove unused accounts).
- Change passwords and other system access credentials whenever there is a personnel change.
- Use client certificates along with username and password as additional security measure.

Description of the User management in the Network Module:

- User and profiles management: (Navigate to Settings>>>Users)
  - Add users
  - 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 page.
  - Follow embedded help for instructions on how to edit a user account.

- Server and client certificate configuration: (Navigate to Settings>>>Certificate)
  - Follow embedded help for instructions on how to configure it.

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 SNMP v1 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

Network Security

Network module provides network access to facilitate communication with other devices in the systems and configuration. But this capability could open up a big security hole if it’s not configured securely.

Eaton recommends segmentation of networks into logical enclaves and restrict the communication to host-to-host paths. This helps protect sensitive information and critical services and limits damage from network perimeter breaches. At a minimum, a utility Industrial Control Systems network should be segmented into a three-tiered architecture (as recommended by NIST SP800-82[R3]) for better security control.

Deploy adequate network protection devices like Firewalls, Intrusion Detection / Protection devices,

Please find detailed information about various Network level protection strategies in Eaton Cybersecurity Considerations for Electrical Distribution Systems [R1]. Use the below information for configuring the firewalls to allow needed access 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. Instructions are available in the Contextual help>>>Settings>>>SNMP.

Logging and Event Management

Best Practices

- Eaton recommends that all remote interactive sessions are encrypted, logged, and monitored including all administrative and maintenance activities.
- Ensure that logs are backed up, retain the backups for a minimum of 3 months or as per organization’s security policy.
- Perform log review at a minimum every 15 days.
- Navigate to Information>>>List of events codes to get log information and how to export it.

Secure Maintenance

Best Practices

Apply Firmware updates and patches regularly

Due to increasing Cyber Attacks on Industrial Control Systems, Eaton implements a comprehensive patch and update process for its products. Users are encouraged to maintain a consistent process to promptly monitor for fresh firmware updates, implement patching and updates as and when required or released.

- 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 - http://eaton.com/cybersecurity and patch through www.powerquality.eaton.com/Support/.

Conduct regular Cybersecurity risk analyses of the organization/system.

Eaton has worked with third-party security firms to perform system audits, both as part of a specific customer’s deployment and within Eaton’s own development cycle process. Eaton can provide guidance and support to your organization’s effort to perform regular cybersecurity audits or assessments.

Plan for Business Continuity / Cybersecurity Disaster Recovery

It’s a Cybersecurity best practice for organizations to plan for Business continuity. Establish an OT Business Continuity plan, periodically review and, where possible, exercise the established continuity plans. Make sure offsite backups include

- Backup of the latest f/w copy of Network module. Make it a part of SOP to update the backup copy as soon as the latest f/w is updated on Network module.
- Backup of the most current configurations.
- Documentation of the most current User List.
- Save and store securely the current configurations of the device.

4.2.3 References

[R1] Cybersecurity Considerations for Electrical Distribution Systems (WP152002EN):
http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf

[R2] Cybersecurity Best Practices Checklist Reminder (WP910003EN):
http://www.cooperindustries.com/content/dam/public/powersystems/resources/library/1100_EAS/WP910003EN.pdf

https://ics-cert.us-cert.gov/Standards-and-References

[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/SP/nistspecialpublication800-41r1.pdf
4.3 Configuring user permissions through profiles

The user profile can be defined when creating a new user or changed when modifying an existing one. Refer to the section Users in the settings.

4.4 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.

Sanitization erases all the data (user name and password, certificates, keys, settings, logs...).

To sanitize the Network Module refer to: Sanitization
5 Servicing the EMP

5.1 Description and features

The optional Environmental Monitoring Probe (EMP) 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).

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, magnets, 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 ±2°C.
- The EMP measures relative humidity from 10% to 90% with an accuracy of ±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).

5.2 Unpacking the EMP

The sensor will include the following:

- EMPDT1H1C2 sensor
- Dry contact terminal block
- Quickstart
- USB to RS485 converter
- RJ45 female to female connector
- 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.
5.3 Installing the EMP

5.3.1 Defining EMPs address and termination

Manual addressing

Address must be defined before the EMP power-up otherwise the changes won't be taken into account. Do not set all the 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.

Example: manual addressing of 3 EMPs connected to the Network-M2

Green LED of the TO DEVICE RJ45 connector shows if the EMP is powered by the Network module.

5.3.2 Mounting the EMP

The EMP includes magnets, cable ties slots and keyholes to enable multiple ways of mounting it on your installation.
Bottom mounting capabilities:
- magnets
- keyholes
- tie wraps
- nylon fastener

Side mounting
- magnets
- tie wraps

Rack mounting with keyhole example
To mount the EMP on the rack, use the supplied screw, washer and nut. Then, mount the EMP on the screw and tighten it.

Rack mounting with tie wraps example
To mount the EMP on the door of the rack, use the supplied cable ties.
### Bottom mounting

To mount the EMP on the wall close to the rack, use the supplied screw and screw anchor. Then, mount the EMP on the screw and tighten it.

### Side mounting

- **Wall mounting with screws example**
  
  To mount the EMP on the wall close to the rack, use the supplied screw and screw anchor. Then, mount the EMP on the screw and tighten it.

- **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.
5.3.3 Cabling the first EMP to the device

Connecting the EMP to the device USB port

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 (example: Network-M2)

Steps
1. Connect one end of the Ethernet cable to the RJ-45 connector on the EMP (FROM DEVICE), then connect the other end of the cable to the RJ45 female/female connector.
2. Connect the RJ45 connector of the USB to RS485 converter to the other end of the RJ45 female/female connector.
3. Connect the USB connector of the USB to RS485 converter cable to the Network-Module USB connector.

Example: EMP connection to the Network-M2

Cut nylon fastener and stick it on the EMP bottom on the location highlighted below, this will prevent to interfere with the EMP data acquisition parts.
5.3.4 Daisy chaining 3 EMPs

Material needed:

- First EMP connected to the device (refer to previous section)
- Additional EMPs
- 2 x Ethernet cable (not supplied).
- Device (example: Network-M2)

Steps

1. Connect one end of the Ethernet cable to the RJ-45 connector on the first EMP (TO SENSORS), then connect the other end of the cable to the RJ45 connector of the second EMP (FROM DEVICE).

2. Connect one end of the Ethernet cable to the RJ-45 connector on the second EMP (TO SENSORS), then connect the other end of the cable to the RJ45 connector of the third EMP (FROM DEVICE).

3. Refer to next section for the EMPs addressing in daisy chain.

Example: connection to the Network-M2

5.3.5 Connecting an external contact device

To connect an external device to the EMP:

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.

2. Tighten the corresponding tightening screws on top of the EMP to secure the wires.
5.4 Commissioning the EMP

5.4.1 On the Network-M2 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 **Sign In**. The Network Module web interface appears.

**STEP 2:** Navigate to Cards/Commissioning page

**STEP 3:** Proceed to the commissioning (refer to the contextual help for details: Cards>>>Commissioning (Sensors)
- 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.

The Sensor button on the left bar also appears, this will be reviewed on STEP4.

- 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: Sensors>>>Alarm configuration)
- Click on the **Sensors** menu that has just appeared on the left bar after the EMP discovery.
- Select the **Alarm configuration** page.
- Enable or disable alarms.
- Define thresholds, hysteresis and severity of temperature, humidity and dry contacts alarms.

5.5 Using the EMP for temperature compensated battery charging

This section applies only to UPS that provides temperature compensated battery charging option.
Address must be defined before the EMP is powered up; otherwise the changes won’t be taken into account.
Do not set all the Modbus address to 0, otherwise the EMP will not be detected.
Define a unique address for all the EMPs in the daisy-chain.
Set the RS485 termination (TER) to 1 on the last EMP of the daisy chain. On other EMPs this should be set to 0.

5.5.1 Addressing the EMP
Set the address 31 to the sensor dedicated to the battery room temperature:
- Set all the Modbus address switches to 1 to set the EMP to the address 31 as indicated on the picture below:

![Modbus Address Diagram]

5.5.2 Commissioning the EMP
Refer to the section Commissioning the EMP.

5.5.3 Enabling temperature compensated battery charging in the UPS

⚠️ The temperature compensated battery charging feature needs to be enabled in the UPS.

To enable the temperature compensated battery charging, refer to the UPS user manual.
6 Information

6.1 Front panel connectors and LED indicators

<table>
<thead>
<tr>
<th>Nbr</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Network connector</td>
<td>Ethernet port</td>
</tr>
<tr>
<td>2</td>
<td>Network speed LED</td>
<td>Flashing green sequences:&lt;br&gt;• 1 flash — Port operating at 10Mbps&lt;br&gt;• 2 flashes — Port operating at 100Mbps&lt;br&gt;• 3 flashes — Port operating at 1Gbps</td>
</tr>
<tr>
<td>3</td>
<td>Network link/activity LED</td>
<td>• Off — UPS Network Module is not connected to the network.&lt;br&gt;• Solid yellow — UPS Network Module is connected to the network, but no activity detected.&lt;br&gt;• Flashing yellow — UPS Network Module is connected to the network and sending or receiving data.</td>
</tr>
<tr>
<td>4</td>
<td>AUX connector</td>
<td>For Network Module accessories only.&lt;br&gt;<strong>Do not use for general power supply or USB charger.</strong></td>
</tr>
<tr>
<td>5</td>
<td>Restart button</td>
<td>Ball point pen or equivalent will be needed to restart:&lt;br&gt;• Short press (&lt;6s) — Safe software restart (firmware safely shutdown before restart).&lt;br&gt;• Long press (&gt;9s) — Forced hardware restart.</td>
</tr>
<tr>
<td>6</td>
<td>ON LED</td>
<td>Flashing green — Network Module is operating normally.</td>
</tr>
<tr>
<td>7</td>
<td>Warning LED</td>
<td>Solid red — Network Module is in error state.</td>
</tr>
</tbody>
</table>
8. Boot LEDs
Solid green and flashing red — Network Module is starting boot sequence.

9. Settings/UPS data connector
Configuration port.
Access to Network Module’s web interface through RNDIS (Emulated Network port).
Access to the Network Module console through Serial (Emulated Serial port).

6.2 Default settings parameters

6.2.1 Settings

General

<table>
<thead>
<tr>
<th>Default setting</th>
<th>Possible parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location — empty</td>
<td>Location — 31 characters maximum</td>
</tr>
<tr>
<td>Contact — empty</td>
<td>Contact — 255 characters maximum</td>
</tr>
<tr>
<td>System name — empty</td>
<td>System name — 255 characters maximum</td>
</tr>
</tbody>
</table>

Date & Time

<table>
<thead>
<tr>
<th>Default setting</th>
<th>Possible parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode — Manual (Time zone: Europe/Paris)</td>
<td>Mode — Manual (Time zone: selection on map/Date) / Dynamic (NTP)</td>
</tr>
</tbody>
</table>

Users

<table>
<thead>
<tr>
<th>Default setting</th>
<th>Possible parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum length — enabled (8)</td>
<td>Minimum length — enable (6-32)/disable</td>
</tr>
<tr>
<td>Minimum upper case — enabled (1)</td>
<td>Minimum upper case — enable (0-32)/disable</td>
</tr>
<tr>
<td>Minimum lower case — enabled (1)</td>
<td>Minimum lower case — enable (0-32)/disable</td>
</tr>
<tr>
<td>Minimum digit — enabled (1)</td>
<td>Minimum digit — enable (0-32)/disable</td>
</tr>
<tr>
<td>Special character — enabled (1)</td>
<td>Special character — enable (0-32)/disable</td>
</tr>
<tr>
<td>Password expires after — disabled</td>
<td>Password expires after — disable/enable (1-99999)</td>
</tr>
<tr>
<td>Main administrator password never expires — disabled</td>
<td>Main administrator password never expires — disable/enable</td>
</tr>
<tr>
<td>Block account when invalid password is entered after — disabled</td>
<td>Block account when invalid password is entered after — disable/enable (1-99)</td>
</tr>
<tr>
<td>Main administrator account never blocks — disabled</td>
<td>Main administrator account never blocks — disable/enable</td>
</tr>
</tbody>
</table>
### Session expiration
<table>
<thead>
<tr>
<th>No activity timeout — 60 minutes</th>
<th>No activity timeout — 1-60 minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session lease time — 120 minutes</td>
<td>Session lease time — 60-720 minutes</td>
</tr>
</tbody>
</table>

### Local users
<table>
<thead>
<tr>
<th>1 user only:</th>
<th>10 users maximum:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Active — Yes</td>
<td>• Active — Yes/No</td>
</tr>
<tr>
<td>• Profile — Administrator</td>
<td>• Profile — Administrator/Viewer</td>
</tr>
<tr>
<td>• Username — admin</td>
<td>• Username — 255 characters maximum</td>
</tr>
<tr>
<td>• Full Name — blank</td>
<td>• Full Name — 128 characters maximum</td>
</tr>
<tr>
<td>• Email — blank</td>
<td>• Email — 128 characters maximum</td>
</tr>
<tr>
<td>• Phone — blank</td>
<td>• Phone — 64 characters maximum</td>
</tr>
<tr>
<td>• Organization — blank</td>
<td>• Organization — 128 characters maximum</td>
</tr>
</tbody>
</table>

### LDAP
<table>
<thead>
<tr>
<th>Configure</th>
<th>Configure</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Active – No</td>
<td>• Active – No/yes</td>
</tr>
<tr>
<td>• Security SSL – SSL</td>
<td>• Security SSL – None/Start TLS/SSL</td>
</tr>
<tr>
<td>Verify server certificate – enabled</td>
<td>Verify server certificate – disabled/enabled</td>
</tr>
<tr>
<td>• Primary server Name – Primary</td>
<td>• Primary server Name – 128 characters maximum</td>
</tr>
<tr>
<td>Hostname – blank</td>
<td>Hostname – 128 characters maximum</td>
</tr>
<tr>
<td>Port – 636</td>
<td>Port – x-xxx</td>
</tr>
<tr>
<td>• Secondary server Name – blank</td>
<td>• Secondary server Name – 128 characters maximum</td>
</tr>
<tr>
<td>Hostname – blank</td>
<td>Hostname – 128 characters maximum</td>
</tr>
<tr>
<td>Port – blank</td>
<td>Port – x-xxx</td>
</tr>
<tr>
<td>• Credentials Anonymous search bind – disabled</td>
<td>• Credentials Anonymous search bind – disabled/enabled</td>
</tr>
<tr>
<td>Search user DN – blank</td>
<td>Search user DN – 1024 characters maximum</td>
</tr>
<tr>
<td>Password – blank</td>
<td>Password – 128 characters maximum</td>
</tr>
<tr>
<td>• Search base Search base DN – dc=example,dc=com</td>
<td>• Search base Search base DN – 1024 characters maximum</td>
</tr>
<tr>
<td>• Request parameters User base DN – ou=people,dc=example,dc=com</td>
<td>• Request parameters User base DN – 1024 characters maximum</td>
</tr>
<tr>
<td>User name attribute – uid</td>
<td>User name attribute – 1024 characters maximum</td>
</tr>
<tr>
<td>UID attribute – uidNumber</td>
<td>UID attribute – 1024 characters maximum</td>
</tr>
<tr>
<td>Group base DN – ou=group,dc=example,dc=com</td>
<td>Group base DN – 1024 characters maximum</td>
</tr>
<tr>
<td>Group name attribute – gid</td>
<td>Group name attribute – 1024 characters maximum</td>
</tr>
<tr>
<td>GID attribute – gidNumber</td>
<td>GID attribute – 1024 characters maximum</td>
</tr>
<tr>
<td>Profile mapping – no mapping</td>
<td>Profile mapping – up to 5 remote groups mapped to local profiles</td>
</tr>
</tbody>
</table>

### Users preferences
| Language – English | German/English/Spanish/French/Italian/Japanese/Simplified Chinese/Traditional Chinese |
| Temperature unit – °C (Celsius) | °C (Celsius)/°F (Fahrenheit) |
| Date format – MM-DD-YYYY | MM-DD-YYYY / YYY-MM-DD / DD-MM-YYYY / DD.MM.YYYY / DD/MM/YYYY / DD MM YYYY |
| Time format – hh:mm:ss (24h) | hh:mm:ss (24h) / hh:mm:ss (12h) |
### Default settings parameters

#### Network

<table>
<thead>
<tr>
<th>Default setting</th>
<th>Possible parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LAN</strong></td>
<td></td>
</tr>
<tr>
<td>Configuration — Auto negotiation</td>
<td>Configuration — Auto negotiation - 10Mbps - Half duplex - 10Mbps - Full duplex - 100Mbps - Half duplex - 100Mbps - Full duplex - 1.0 Gbps - Full duplex</td>
</tr>
<tr>
<td><strong>IPV4</strong></td>
<td></td>
</tr>
<tr>
<td>Mode — Dynamic (DHCP)</td>
<td>Mode — DHCP/Manual (IP address/Netmask/Gateway)</td>
</tr>
<tr>
<td><strong>Domain</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Domain configuration (more) : | Domain configuration (more) :
  • Hostname — ups-[MAC address]
  • Mode — DHCP |
  • Hostname — 128 characters maximum
  • Mode : DHCP/Manual (Domain name/Primary DNS/Secondary DNS) |
| **IPV6**        |                     |
| Enable — checked | Enable — enable/disable |
| IPV6 details (more) : | IPV6 details (more) :
  • Mode — Router |
  • Mode — Router/Manual (Address/Prefix/Gateway) |

#### Protocols

<table>
<thead>
<tr>
<th>Default setting</th>
<th>Possible parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HTTPS</strong></td>
<td></td>
</tr>
<tr>
<td>Port — 443</td>
<td>Port — x-xxx</td>
</tr>
</tbody>
</table>

Information – 128
<table>
<thead>
<tr>
<th>Default setting</th>
<th>Possible parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SNMP</strong></td>
<td></td>
</tr>
<tr>
<td>Enable — disabled</td>
<td>Enable — disable/enable</td>
</tr>
<tr>
<td>Port — 161</td>
<td>Port — x-xxx</td>
</tr>
<tr>
<td>SNMP V1 — disabled</td>
<td>SNMP V1 — disable/enable</td>
</tr>
<tr>
<td>• Community #1 — public</td>
<td>• Community #1 — 128 characters maximum</td>
</tr>
<tr>
<td></td>
<td>Active — No</td>
</tr>
<tr>
<td></td>
<td>Access — Read only</td>
</tr>
<tr>
<td>• Community #2 — private</td>
<td>• Community #2 — 128 characters maximum</td>
</tr>
<tr>
<td></td>
<td>Active — No</td>
</tr>
<tr>
<td></td>
<td>Access — Read/Write</td>
</tr>
<tr>
<td>SNMP V3 — enabled</td>
<td>SNMP V3 — disable/enable</td>
</tr>
<tr>
<td>• User #1 — readonly</td>
<td>• User #1 — 32 characters maximum</td>
</tr>
<tr>
<td></td>
<td>Active — No</td>
</tr>
<tr>
<td></td>
<td>Access — Read only</td>
</tr>
<tr>
<td></td>
<td>Authentication — Auth (SHA-1)</td>
</tr>
<tr>
<td></td>
<td>Password — empty</td>
</tr>
<tr>
<td></td>
<td>Confirm password — empty</td>
</tr>
<tr>
<td></td>
<td>Privacy — Secured - AES</td>
</tr>
<tr>
<td></td>
<td>Key — empty</td>
</tr>
<tr>
<td></td>
<td>Confirm key — empty</td>
</tr>
<tr>
<td>• User#2 — readwrite</td>
<td>• User#2 — 32 characters maximum</td>
</tr>
<tr>
<td></td>
<td>Active — No</td>
</tr>
<tr>
<td></td>
<td>Access — Read/Write</td>
</tr>
<tr>
<td></td>
<td>Authentication — Auth (SHA-1)</td>
</tr>
<tr>
<td></td>
<td>Password — empty</td>
</tr>
<tr>
<td></td>
<td>Confirm password — empty</td>
</tr>
<tr>
<td></td>
<td>Privacy — Secured - AES</td>
</tr>
<tr>
<td></td>
<td>Key — 128 characters maximum</td>
</tr>
<tr>
<td></td>
<td>Confirm key — 128 characters maximum</td>
</tr>
<tr>
<td><strong>Trap receivers</strong></td>
<td></td>
</tr>
<tr>
<td>No trap</td>
<td>Active — No/Yes</td>
</tr>
<tr>
<td></td>
<td>Application name — 128 characters maximum</td>
</tr>
<tr>
<td></td>
<td>Hostname or IP address — 128 characters maximum</td>
</tr>
<tr>
<td></td>
<td>Port — x-xxx</td>
</tr>
<tr>
<td></td>
<td>Protocol — V1</td>
</tr>
<tr>
<td></td>
<td>Trap community — 128 characters maximum</td>
</tr>
</tbody>
</table>
## Default settings parameters

### Email

<table>
<thead>
<tr>
<th>Default setting</th>
<th>Possible parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Email sending configuration</strong></td>
<td>5 configurations maximum</td>
</tr>
<tr>
<td>No email</td>
<td>Active — No/Yes</td>
</tr>
<tr>
<td>Configuration name — 128 characters maximum</td>
<td>Email address — 128 characters maximum</td>
</tr>
<tr>
<td>Notify on events</td>
<td>• Notify on events</td>
</tr>
<tr>
<td>Active — No/Yes</td>
<td>• Notify on events</td>
</tr>
<tr>
<td>On card events — Subscribe/Attach logs (Critical/Warning/Info)</td>
<td>On devices events — Subscribe/Attach logs (Critical/Warning/Info)</td>
</tr>
<tr>
<td>Exceptions on events notification — Always notify events with code/Never notify events with code</td>
<td></td>
</tr>
<tr>
<td>Periodic report</td>
<td>• Periodic report</td>
</tr>
<tr>
<td>Active — No/Yes</td>
<td>• Periodic report</td>
</tr>
<tr>
<td>Recurrence — Every day/Every week/Every month</td>
<td>Starting – Date and time</td>
</tr>
<tr>
<td>Topic – Subscribe/Attach logs (Card/Devices)</td>
<td>Email configuration</td>
</tr>
<tr>
<td>Sender – text field/list of customization key words</td>
<td>Subject – text field/list of customization key words</td>
</tr>
</tbody>
</table>

### SMTP

<table>
<thead>
<tr>
<th>Default setting</th>
<th>Possible parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server IP/Hostname — blank</td>
<td>Server IP/Hostname — 128 characters maximum</td>
</tr>
<tr>
<td>SMTP server authentication — disabled</td>
<td>SMTP server authentication — disable/enable</td>
</tr>
<tr>
<td>Port — 25</td>
<td>Port — x-xxx</td>
</tr>
<tr>
<td>Sender address — <a href="mailto:ups@networkcard.com">ups@networkcard.com</a></td>
<td>Sender address — 128 characters maximum</td>
</tr>
<tr>
<td>Secure SMTP connection — enabled</td>
<td>Secure SMTP connection — enable/disable</td>
</tr>
<tr>
<td>Verify certificate authority — disabled</td>
<td>Verify certificate authority — disable/enable</td>
</tr>
</tbody>
</table>

### My preferences

<table>
<thead>
<tr>
<th>Default setting</th>
<th>Possible parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Profile</strong></td>
<td>Edit user:</td>
</tr>
<tr>
<td>Edit user:</td>
<td>• Full name — 128 characters maximum</td>
</tr>
<tr>
<td>• Email — blank</td>
<td>• Email — 128 characters maximum</td>
</tr>
<tr>
<td>• Phone — blank</td>
<td>• Phone — 64 characters maximum</td>
</tr>
<tr>
<td>• Organization — blank</td>
<td>• Organization — 128 characters maximum</td>
</tr>
<tr>
<td><strong>Temperature</strong></td>
<td>°C (Celsius) / °F (Fahrenheit)</td>
</tr>
<tr>
<td><strong>Date format</strong></td>
<td>MM-DD-YYYY / YYYY-MM-DD / DD-MM-YYYY / DD.MM.YYY / DD/MM/YYYY / DD MM YYYY</td>
</tr>
<tr>
<td><strong>Time format</strong></td>
<td>hh:mm:ss (24h) / hh:mm:ss (12h)</td>
</tr>
<tr>
<td>Language</td>
<td>English</td>
</tr>
<tr>
<td>----------</td>
<td>---------</td>
</tr>
<tr>
<td>Language</td>
<td>German/English/Spanish/French/Italian/Japanese/Simplified Chinese/Traditional Chinese</td>
</tr>
</tbody>
</table>

### 6.2.2 Meters

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Default setting</th>
<th>Possible parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Log measures every — 60s</td>
<td>Log measures every — 3600s maximum</td>
</tr>
</tbody>
</table>

### 6.2.3 Sensors alarm configuration

<table>
<thead>
<tr>
<th>Temperature</th>
<th>Default setting</th>
<th>Possible parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Enabled — No</td>
<td>Enabled — No/Yes</td>
</tr>
<tr>
<td></td>
<td>Low critical – 0°C/32°F</td>
<td>low critical&lt;low warning&lt;high warning&lt;high critical</td>
</tr>
<tr>
<td></td>
<td>Low warning – 10°C/50°F</td>
<td></td>
</tr>
<tr>
<td></td>
<td>High warning – 70°C/158°F</td>
<td></td>
</tr>
<tr>
<td></td>
<td>High critical – 80°C/176°F</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Humidity</th>
<th>Default setting</th>
<th>Possible parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Enabled — No</td>
<td>Enabled — No/Yes</td>
</tr>
<tr>
<td></td>
<td>Low critical – 10%</td>
<td>0%&lt;low critical&lt;low warning&lt;high warning&lt;high critical&lt;100%</td>
</tr>
<tr>
<td></td>
<td>Low warning – 20%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>High warning – 80%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>High critical – 90%</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Dry contacts</th>
<th>Default setting</th>
<th>Possible parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Enabled — No</td>
<td>Enabled — No/Yes</td>
</tr>
<tr>
<td></td>
<td>Alarm severity – Warning</td>
<td>Alarm severity – Info/Warning/Critical</td>
</tr>
</tbody>
</table>
# 6.3 Specifications/Technical characteristics

<table>
<thead>
<tr>
<th><strong>Physical characteristics</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Dimensions (wxdxh)</td>
<td>132 x 66 x 42 mm</td>
</tr>
<tr>
<td>Weight</td>
<td>70 g</td>
</tr>
<tr>
<td>RoHS</td>
<td>100% compatible</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Storage</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage temperature</td>
<td>-25°C to 70°C (14°F to 158°F)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Ambient conditions</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating temperature</td>
<td>0°C to 70°C (32°F to 158°F)</td>
</tr>
<tr>
<td>Relative humidity</td>
<td>5%-95%, noncondensing</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Module performance</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Module input power</td>
<td>5V-12V ±5%</td>
</tr>
<tr>
<td>AUX output power</td>
<td>5V ±5%</td>
</tr>
<tr>
<td>Date/Time backup</td>
<td>CR1220 battery coin cell</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Functions</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Languages</td>
<td>English, French, Italian, German, Spanish, Japanese</td>
</tr>
<tr>
<td>Alarms/Log</td>
<td>Email, SNMP trap, web interface / Log on events</td>
</tr>
<tr>
<td>Network</td>
<td>Gigabit ETHERNET, 10/100/1000Mb/s, auto negotiation, HTTP 1.1, SNMP V1, SNMP V3, NTP, SMTP, DHCP</td>
</tr>
<tr>
<td>Security</td>
<td>Restricted to TLS 1.2</td>
</tr>
<tr>
<td>Supported MIBs</td>
<td>*See below for a detailed list</td>
</tr>
<tr>
<td>Browsers</td>
<td>Internet Explorer, Google Chrome, Firefox, Safari</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Settings (default values)</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>IP network</td>
<td>DHCP enabled</td>
</tr>
<tr>
<td>Port</td>
<td>443 (https), 22 (ssh), 161 (snmp), 162 (snmp trap), 25 (smtp), 8883 (mqtts), 123 (ntp), 5353 (mdns-sd), 80 (http)</td>
</tr>
<tr>
<td>Web interface access control</td>
<td>User name: admin</td>
</tr>
<tr>
<td>Settings/UPS data connector</td>
<td>USB RNDIS Apipa compatible</td>
</tr>
</tbody>
</table>
6.4 List of event codes

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

6.5 Alarm log codes

To retrieve Alarm logs, navigate to Alarm section and press the Download alarms button.

### 6.5.1 Critical

<table>
<thead>
<tr>
<th>Code</th>
<th>Severity</th>
<th>Active message</th>
<th>Non active message</th>
<th>Advice</th>
</tr>
</thead>
<tbody>
<tr>
<td>002</td>
<td>Critical</td>
<td>Internal failure</td>
<td>End of internal failure</td>
<td>Service required</td>
</tr>
<tr>
<td>004</td>
<td>Critical</td>
<td>Temperature alarm</td>
<td>Temperature OK</td>
<td>Check air conditioner</td>
</tr>
<tr>
<td>007</td>
<td>Critical</td>
<td>Fan fault</td>
<td>Fan OK</td>
<td>Service required</td>
</tr>
<tr>
<td>00F</td>
<td>Critical</td>
<td>Parallel UPS not compatible</td>
<td>Parallel UPS compatibility OK</td>
<td>Service required</td>
</tr>
<tr>
<td>010</td>
<td>Critical</td>
<td>UPS power supply fault</td>
<td>UPS power supply OK</td>
<td>Service required</td>
</tr>
<tr>
<td>011</td>
<td>Critical</td>
<td>Parallel UPS protection lost</td>
<td>Parallel UPS protection OK</td>
<td>Reduce output load</td>
</tr>
<tr>
<td>012</td>
<td>Critical</td>
<td>Parallel UPS measure inconsistent</td>
<td>Parallel UPS measure OK</td>
<td>Service required</td>
</tr>
<tr>
<td>100</td>
<td>Critical</td>
<td>Rectifier fuse fault</td>
<td>Rectifier fuse OK</td>
<td>Service required</td>
</tr>
<tr>
<td>105</td>
<td>Critical</td>
<td>Input AC module failure</td>
<td>Input AC module OK</td>
<td>Service required</td>
</tr>
<tr>
<td>110</td>
<td>Critical</td>
<td>Building alarm (through dry contact)</td>
<td>Building alarm OK</td>
<td>-</td>
</tr>
<tr>
<td>11F</td>
<td>Critical</td>
<td>Building alarm (through Network module)</td>
<td>Building alarm OK</td>
<td>-</td>
</tr>
<tr>
<td>202</td>
<td>Critical</td>
<td>Bypass thermal overload</td>
<td>Bypass thermal OK</td>
<td>Reduce output load</td>
</tr>
<tr>
<td>203</td>
<td>Critical</td>
<td>Bypass temperature alarm</td>
<td>Bypass temperature OK</td>
<td>Check air conditioner</td>
</tr>
<tr>
<td>207</td>
<td>Critical</td>
<td>Bypass AC module failure</td>
<td>Bypass AC module OK</td>
<td>-</td>
</tr>
<tr>
<td>208</td>
<td>Critical</td>
<td>Bypass overload</td>
<td>No bypass overload</td>
<td>-</td>
</tr>
<tr>
<td>305</td>
<td>Critical</td>
<td>Rectifier failure</td>
<td>Rectifier OK</td>
<td>Service required</td>
</tr>
<tr>
<td>306</td>
<td>Critical</td>
<td>Rectifier overload</td>
<td>Rectifier OK</td>
<td>Reduce output load</td>
</tr>
<tr>
<td>308</td>
<td>Critical</td>
<td>Rectifier short circuit</td>
<td>Rectifier OK</td>
<td>Reduce output load</td>
</tr>
<tr>
<td>Code</td>
<td>Critical Event</td>
<td>Status</td>
<td>Action</td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>--------------------------------</td>
<td>-----------------</td>
<td>-------------------------------</td>
<td></td>
</tr>
<tr>
<td>400</td>
<td>DCDC converter failure</td>
<td>DCDC converter OK</td>
<td>Service required</td>
<td></td>
</tr>
<tr>
<td>500</td>
<td>Battery charger fault</td>
<td>Battery charger OK</td>
<td>Service required</td>
<td></td>
</tr>
<tr>
<td>600</td>
<td>Battery fuse fault</td>
<td>Battery fuse OK</td>
<td>Service required</td>
<td></td>
</tr>
<tr>
<td>602</td>
<td>Battery fuse fault</td>
<td>Battery fuse OK</td>
<td>Service required</td>
<td></td>
</tr>
<tr>
<td>604</td>
<td>Battery low</td>
<td>Battery OK</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>607</td>
<td>Battery test failed</td>
<td>Battery test OK</td>
<td>Check battery</td>
<td></td>
</tr>
<tr>
<td>60D</td>
<td>No battery</td>
<td>Battery present</td>
<td>Check battery</td>
<td></td>
</tr>
<tr>
<td>700</td>
<td>Inverter limitation</td>
<td>No current limitation</td>
<td>Reduce output load</td>
<td></td>
</tr>
<tr>
<td>701</td>
<td>Inverter fuse fault</td>
<td>Inverter fuse OK</td>
<td>Service required</td>
<td></td>
</tr>
<tr>
<td>704</td>
<td>Inverter internal failure</td>
<td>UPS OK</td>
<td>Service required</td>
<td></td>
</tr>
<tr>
<td>705</td>
<td>Inverter overload</td>
<td>No power overload</td>
<td>Reduce output load</td>
<td></td>
</tr>
<tr>
<td>706</td>
<td>Temperature alarm</td>
<td>Temperature OK</td>
<td>Check air conditioner</td>
<td></td>
</tr>
<tr>
<td>70A</td>
<td>Inverter thermal overload</td>
<td>No power overload</td>
<td>Reduce output load</td>
<td></td>
</tr>
<tr>
<td>70B</td>
<td>Inverter short circuit</td>
<td>End of inverter short circuit</td>
<td>Service required</td>
<td></td>
</tr>
<tr>
<td>802</td>
<td>Shutdown imminent</td>
<td>Shutdown canceled</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>805</td>
<td>Output short circuit</td>
<td>Output OK</td>
<td>Reduce output load</td>
<td></td>
</tr>
<tr>
<td>806</td>
<td>Emergency power OFF</td>
<td>No emergency OFF</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>811</td>
<td>Parallel negative power</td>
<td>Parallel power OK</td>
<td>Reduce output load</td>
<td></td>
</tr>
<tr>
<td>814</td>
<td>Firmware watchdog reset</td>
<td>Firmware watchdog OK</td>
<td>Service required</td>
<td></td>
</tr>
<tr>
<td>815</td>
<td>Calibration fault</td>
<td>Calibration OK</td>
<td>Service required</td>
<td></td>
</tr>
<tr>
<td>81E</td>
<td>Load unprotected</td>
<td>Load protected</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>900</td>
<td>Maintenance bypass</td>
<td>Not on maintenance bypass</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>1201</td>
<td>Temperature is critically low</td>
<td>Temperature is back to low</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>1204</td>
<td>Temperature is critically high</td>
<td>Temperature is back to high</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>1211</td>
<td>Humidity is critically low</td>
<td>Humidity is back to low</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>1214</td>
<td>Humidity is critically high</td>
<td>Humidity is back to high</td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>
### 6.5.2 Warning

<table>
<thead>
<tr>
<th>Code</th>
<th>Severity</th>
<th>Active message</th>
<th>Non active message</th>
<th>Advice</th>
</tr>
</thead>
<tbody>
<tr>
<td>001</td>
<td>Warning</td>
<td>On battery</td>
<td>No more on battery</td>
<td>-</td>
</tr>
<tr>
<td>00B</td>
<td>Warning</td>
<td>Parallel UPS redundancy lost</td>
<td>Parallel UPS redundancy OK</td>
<td>Reduce output load</td>
</tr>
<tr>
<td>00E</td>
<td>Warning</td>
<td>Parallel UPS communication lost</td>
<td>Parallel UPS communication OK</td>
<td>Service required</td>
</tr>
<tr>
<td>103</td>
<td>Warning</td>
<td>Utility breaker open</td>
<td>Utility breaker closed</td>
<td>-</td>
</tr>
<tr>
<td>104</td>
<td>Warning</td>
<td>Input AC frequency out of range</td>
<td>Input AC frequency in range</td>
<td>-</td>
</tr>
<tr>
<td>106</td>
<td>Warning</td>
<td>Input AC not present</td>
<td>Input AC present</td>
<td>-</td>
</tr>
<tr>
<td>107</td>
<td>Warning</td>
<td>Input bad wiring</td>
<td>Input wiring OK</td>
<td>Check input wiring</td>
</tr>
<tr>
<td>108</td>
<td>Warning</td>
<td>Input AC voltage out of range (⁻)</td>
<td>Input AC voltage in range</td>
<td>-</td>
</tr>
<tr>
<td>109</td>
<td>Warning</td>
<td>Input AC voltage out of range (⁺)</td>
<td>Input AC voltage in range</td>
<td>-</td>
</tr>
<tr>
<td>10A</td>
<td>Warning</td>
<td>Input AC unbalanced</td>
<td>End of input AC unbalanced</td>
<td>-</td>
</tr>
<tr>
<td>200</td>
<td>Warning</td>
<td>Bypass phase out range</td>
<td>Bypass phase in range</td>
<td>-</td>
</tr>
<tr>
<td>201</td>
<td>Warning</td>
<td>Bypass not available</td>
<td>Bypass available</td>
<td>Service required</td>
</tr>
<tr>
<td>204</td>
<td>Warning</td>
<td>Bypass breaker open</td>
<td>Bypass breaker closed</td>
<td>-</td>
</tr>
<tr>
<td>205</td>
<td>Warning</td>
<td>Bypass mode</td>
<td>No more on bypass</td>
<td>-</td>
</tr>
<tr>
<td>206</td>
<td>Warning</td>
<td>Bypass frequency out of range</td>
<td>Bypass frequency in range</td>
<td>-</td>
</tr>
<tr>
<td>209</td>
<td>Warning</td>
<td>Bypass voltage out of range</td>
<td>Bypass voltage in range</td>
<td>-</td>
</tr>
<tr>
<td>20A</td>
<td>Warning</td>
<td>Bypass AC over voltage</td>
<td>End of bypass AC over voltage</td>
<td>-</td>
</tr>
<tr>
<td>20B</td>
<td>Warning</td>
<td>Bypass AC under voltage</td>
<td>End of bypass AC under voltage</td>
<td>-</td>
</tr>
<tr>
<td>20C</td>
<td>Warning</td>
<td>Bypass bad wiring</td>
<td>Bypass wiring OK</td>
<td>Check bypass wiring</td>
</tr>
<tr>
<td>300</td>
<td>Warning</td>
<td>DC bus + too high</td>
<td>DC bus + voltage OK</td>
<td>Service required</td>
</tr>
<tr>
<td>301</td>
<td>Warning</td>
<td>DC bus - too high</td>
<td>DC bus - voltage OK</td>
<td>Service required</td>
</tr>
<tr>
<td>302</td>
<td>Warning</td>
<td>DC bus + too low</td>
<td>DC bus + voltage OK</td>
<td>Service required</td>
</tr>
<tr>
<td>303</td>
<td>Warning</td>
<td>DC bus - too low</td>
<td>DC bus - voltage OK</td>
<td>Service required</td>
</tr>
<tr>
<td>Code</td>
<td>Alarm Type</td>
<td>Condition 1</td>
<td>Condition 2</td>
<td>Action</td>
</tr>
<tr>
<td>------</td>
<td>---------------------</td>
<td>-----------------------</td>
<td>-----------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>304</td>
<td>Warning</td>
<td>DC bus unbalanced</td>
<td>DC bus OK</td>
<td>Service required</td>
</tr>
<tr>
<td>501</td>
<td>Warning</td>
<td>Charger temperature alarm</td>
<td>Charger temperature OK</td>
<td>Service required</td>
</tr>
<tr>
<td>502</td>
<td>Warning</td>
<td>Max charger voltage</td>
<td>Charger voltage OK</td>
<td>Service required</td>
</tr>
<tr>
<td>503</td>
<td>Warning</td>
<td>Min charger voltage</td>
<td>Charger voltage OK</td>
<td>Service required</td>
</tr>
<tr>
<td>603</td>
<td>Warning</td>
<td>Battery discharging</td>
<td>End of UPS battery discharge</td>
<td>-</td>
</tr>
<tr>
<td>605</td>
<td>Warning</td>
<td>Battery temperature alarm</td>
<td>Battery temperature OK</td>
<td>Service required</td>
</tr>
<tr>
<td>606</td>
<td>Warning</td>
<td>Battery breaker open</td>
<td>Battery breaker closed</td>
<td>Service required</td>
</tr>
<tr>
<td>610</td>
<td>Warning</td>
<td>Battery low voltage</td>
<td>Battery OK</td>
<td>Check battery</td>
</tr>
<tr>
<td>613</td>
<td>Warning</td>
<td>Battery voltage too high</td>
<td>Battery voltage OK</td>
<td>-</td>
</tr>
<tr>
<td>70C</td>
<td>Warning</td>
<td>Inverter voltage too low</td>
<td>Inverter voltage OK</td>
<td>Service required</td>
</tr>
<tr>
<td>70D</td>
<td>Warning</td>
<td>Inverter voltage too high</td>
<td>Inverter voltage OK</td>
<td>Service required</td>
</tr>
<tr>
<td>801</td>
<td>Warning</td>
<td>Load not powered</td>
<td>Load powered</td>
<td>-</td>
</tr>
<tr>
<td>803</td>
<td>Warning</td>
<td>Output breaker open</td>
<td>Output breaker closed</td>
<td>-</td>
</tr>
<tr>
<td>808</td>
<td>Warning</td>
<td>Power overload</td>
<td>No power overload</td>
<td>Reduce output load</td>
</tr>
<tr>
<td>80D</td>
<td>Warning</td>
<td>Internal configuration failure</td>
<td>Internal configuration OK</td>
<td>Service required</td>
</tr>
<tr>
<td>80E</td>
<td>Warning</td>
<td>Overload pre-alarm</td>
<td>No overload pre-alarm</td>
<td>Reduce output load</td>
</tr>
<tr>
<td>810</td>
<td>Warning</td>
<td>Overload alarm</td>
<td>No overload</td>
<td>Reduce output load</td>
</tr>
<tr>
<td>816</td>
<td>Warning</td>
<td>Compatibility failure</td>
<td>Compatibility OK</td>
<td>Service required</td>
</tr>
<tr>
<td>817</td>
<td>Warning</td>
<td>Output over current</td>
<td>No output over current</td>
<td>Reduce output load</td>
</tr>
<tr>
<td>818</td>
<td>Warning</td>
<td>Output frequency out of range</td>
<td>Output frequency in range</td>
<td>Service required</td>
</tr>
<tr>
<td>819</td>
<td>Warning</td>
<td>Output voltage too high</td>
<td>Output voltage OK</td>
<td>Service required</td>
</tr>
<tr>
<td>81A</td>
<td>Warning</td>
<td>Output voltage too low</td>
<td>Output voltage OK</td>
<td>Service required</td>
</tr>
<tr>
<td>81B</td>
<td>Warning</td>
<td>UPS Shutoff requested</td>
<td>End of UPS shutoff requested</td>
<td>Service required</td>
</tr>
<tr>
<td>81D</td>
<td>Warning</td>
<td>Load not powered</td>
<td>Load protected</td>
<td>-</td>
</tr>
<tr>
<td>901</td>
<td>Warning</td>
<td>Maintenance bypass breaker closed</td>
<td>Maintenance bypass breaker open</td>
<td>-</td>
</tr>
<tr>
<td>B00</td>
<td>Warning</td>
<td>End of warranty</td>
<td>End of warranty cleared</td>
<td>-</td>
</tr>
<tr>
<td>Code</td>
<td>Severity</td>
<td>Active message</td>
<td>Non active message</td>
<td>Advice</td>
</tr>
<tr>
<td>------</td>
<td>----------</td>
<td>----------------</td>
<td>--------------------</td>
<td>--------</td>
</tr>
<tr>
<td>B01</td>
<td>Warning</td>
<td>Batteries are aging. Consider replacement</td>
<td>Batteries aging condition cleared</td>
<td>-</td>
</tr>
<tr>
<td>1032</td>
<td>Warning</td>
<td>Protection: immediate shutdown in progress</td>
<td>Protection: immediate shutdown completed</td>
<td>-</td>
</tr>
<tr>
<td>1053</td>
<td>Warning</td>
<td>Protection: communication lost with Agent</td>
<td>Protection: communication recovered with Agent</td>
<td>-</td>
</tr>
<tr>
<td>1200</td>
<td>Warning</td>
<td>Communication lost ((with EMP))</td>
<td>Communication recovered ((with EMP))</td>
<td>-</td>
</tr>
<tr>
<td>1202</td>
<td>Warning</td>
<td>Temperature is low ((EMP))</td>
<td>Temperature is back to normal ((EMP))</td>
<td>-</td>
</tr>
<tr>
<td>1203</td>
<td>Warning</td>
<td>Temperature is high ((EMP))</td>
<td>Temperature is back to normal ((EMP))</td>
<td>-</td>
</tr>
<tr>
<td>1212</td>
<td>Warning</td>
<td>Humidity is low ((EMP))</td>
<td>Humidity is back to normal ((EMP))</td>
<td>-</td>
</tr>
<tr>
<td>1213</td>
<td>Warning</td>
<td>Humidity is high ((EMP))</td>
<td>Humidity is back to normal ((EMP))</td>
<td>-</td>
</tr>
</tbody>
</table>

6.5.3 Info

<table>
<thead>
<tr>
<th>Code</th>
<th>Severity</th>
<th>Active message</th>
<th>Non active message</th>
<th>Advice</th>
</tr>
</thead>
<tbody>
<tr>
<td>005</td>
<td>Info</td>
<td>Communication lost ((with UPS))</td>
<td>Communication recovered ((with UPS))</td>
<td>Service required</td>
</tr>
<tr>
<td>009</td>
<td>Info</td>
<td>On high efficiency</td>
<td>High efficiency disabled</td>
<td>-</td>
</tr>
<tr>
<td>013</td>
<td>Info</td>
<td>Upgrading: limited communication</td>
<td>End of upgrade mode</td>
<td>-</td>
</tr>
<tr>
<td>101</td>
<td>Info</td>
<td>On AVR ((Boost))</td>
<td>End of AVR ((Boost))</td>
<td>-</td>
</tr>
<tr>
<td>102</td>
<td>Info</td>
<td>On AVR ((Buck))</td>
<td>End of AVR ((Buck))</td>
<td>-</td>
</tr>
<tr>
<td>A00</td>
<td>Info</td>
<td>Group 1 is OFF</td>
<td>Group 1 is ON</td>
<td>-</td>
</tr>
<tr>
<td>A01</td>
<td>Info</td>
<td>Group 2 is OFF</td>
<td>Group 2 is ON</td>
<td>-</td>
</tr>
<tr>
<td>A0F</td>
<td>Info</td>
<td>Group is OFF</td>
<td>Group is ON</td>
<td>-</td>
</tr>
<tr>
<td>1016</td>
<td>Info</td>
<td>Protection: sequential shutdown scheduled</td>
<td>Protection: sequential shutdown canceled</td>
<td>-</td>
</tr>
<tr>
<td>1017</td>
<td>Info</td>
<td>Protection: sequential shutdown in progress</td>
<td>Protection: sequential shutdown completed</td>
<td>-</td>
</tr>
<tr>
<td>1100</td>
<td>Info</td>
<td>Schedule: shutdown date reached</td>
<td>Schedule: shutdown initiated</td>
<td>-</td>
</tr>
</tbody>
</table>
### Alarm log codes

<table>
<thead>
<tr>
<th>Code</th>
<th>Severity</th>
<th>Active message</th>
<th>Non active message</th>
<th>Advice</th>
</tr>
</thead>
<tbody>
<tr>
<td>1101</td>
<td>Info</td>
<td>Schedule: restart date reached</td>
<td>Schedule: restart initiated</td>
<td>-</td>
</tr>
<tr>
<td>1300</td>
<td>Info</td>
<td>No UPS connected</td>
<td>Communication recovered (with UPS)</td>
<td>-</td>
</tr>
<tr>
<td>1301</td>
<td>Info</td>
<td>UPS not supported</td>
<td>Communication recovered (with UPS)</td>
<td>-</td>
</tr>
</tbody>
</table>

#### 6.5.4 With settable severity

<table>
<thead>
<tr>
<th>Code</th>
<th>Severity</th>
<th>Active message</th>
<th>Non active message</th>
<th>Advice</th>
</tr>
</thead>
<tbody>
<tr>
<td>1221</td>
<td>Settable</td>
<td>Contact is active <em>(EMP)</em></td>
<td>Contact is back to normal <em>(EMP)</em></td>
<td>-</td>
</tr>
</tbody>
</table>
### 6.6 System log codes

To retrieve System logs, navigate to Card>>>System logs section and press the **Download System logs** button.

#### 6.6.1 Critical

<table>
<thead>
<tr>
<th>Code</th>
<th>Severity</th>
<th>Log message</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>0801000</td>
<td>Alert</td>
<td>User account - admin password reset to default</td>
<td>logAccount.csv</td>
</tr>
<tr>
<td>0E00400</td>
<td>Critical</td>
<td>The [selfsign/PKI] signed certificate of the &lt;service&gt; server is not valid</td>
<td>logSystem.csv</td>
</tr>
<tr>
<td>0A00700</td>
<td>Error</td>
<td>Network module file system integrity corrupted &lt;f/w: xx.yy.zzzz&gt;</td>
<td>logUpdate.csv</td>
</tr>
</tbody>
</table>

#### 6.6.2 Warning

<table>
<thead>
<tr>
<th>Code</th>
<th>Severity</th>
<th>Log message</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>0A00200</td>
<td>Warning</td>
<td>Network module upgrade failed &lt;f/w: xx.yy.zzzz&gt;</td>
<td>logUpdate.csv</td>
</tr>
<tr>
<td>0A00A00</td>
<td>Warning</td>
<td>Network module bootloader upgrade failed &lt;f/w: xx.yy.zzzz&gt;</td>
<td>logUpdate.csv</td>
</tr>
<tr>
<td>0B00500</td>
<td>Warning</td>
<td>RTC battery cell low</td>
<td>logSystem.csv</td>
</tr>
<tr>
<td>0E00200</td>
<td>Warning</td>
<td>New [self/PKI] signed certificate [generated/imported] for &lt;service&gt; server</td>
<td>logSystem.csv</td>
</tr>
<tr>
<td>0E00300</td>
<td>Warning</td>
<td>The [self/PKI] signed certificate of the &lt;service&gt; server will expire in &lt;X&gt; days</td>
<td>logSystem.csv</td>
</tr>
<tr>
<td>0800700</td>
<td>Warning</td>
<td>User account - password expired</td>
<td>logAccount.csv</td>
</tr>
<tr>
<td>0800900</td>
<td>Warning</td>
<td>User account - locked</td>
<td>logAccount.csv</td>
</tr>
</tbody>
</table>

#### 6.6.3 Info

<table>
<thead>
<tr>
<th>Code</th>
<th>Severity</th>
<th>Log message</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>0300D00</td>
<td>Notice</td>
<td>User action - sanitization launched</td>
<td>logSystem.csv</td>
</tr>
<tr>
<td>0A00500</td>
<td>Notice</td>
<td>Network module sanitized</td>
<td>logUpdate.csv</td>
</tr>
<tr>
<td>0A00900</td>
<td>Notice</td>
<td>Network module bootloader upgrade success &lt;f/w: xx.yy.zzzz&gt;</td>
<td>logUpdate.csv</td>
</tr>
<tr>
<td>0A00B00</td>
<td>Notice</td>
<td>Network module bootloader upgrade started &lt;f/w: xx.yy.zzzz&gt;</td>
<td>logUpdate.csv</td>
</tr>
<tr>
<td>0A00C00</td>
<td>Notice</td>
<td>Periodic system integrity check started</td>
<td>logUpdate.csv</td>
</tr>
<tr>
<td>0B00100</td>
<td>Notice</td>
<td>Time manually changed</td>
<td>logSystem.csv</td>
</tr>
<tr>
<td>Code</td>
<td>Type</td>
<td>Description</td>
<td>File</td>
</tr>
<tr>
<td>----------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>0B00700</td>
<td>Notice</td>
<td>NTP server not available &lt;NTP server address&gt;</td>
<td>logSystem.csv</td>
</tr>
<tr>
<td>0900100</td>
<td>Notice</td>
<td>Session - opened</td>
<td>logSession.csv</td>
</tr>
<tr>
<td>0900200</td>
<td>Notice</td>
<td>Session - closed</td>
<td>logSession.csv</td>
</tr>
<tr>
<td>0900300</td>
<td>Notice</td>
<td>Session - invalid token</td>
<td>logSession.csv</td>
</tr>
<tr>
<td>0900400</td>
<td>Notice</td>
<td>Session - authentication failed</td>
<td>logSession.csv</td>
</tr>
<tr>
<td>0300F00</td>
<td>Notice</td>
<td>User action - network module admin password reset switch activated</td>
<td>logSystem.csv</td>
</tr>
<tr>
<td>0E00500</td>
<td>Notice</td>
<td>[Certificate authority/ Client certificate] &lt;id&gt; is added for &lt;service&gt;</td>
<td>logSystem.csv</td>
</tr>
<tr>
<td>0E00600</td>
<td>Notice</td>
<td>[Certificate authority/ Client certificate] &lt;id&gt; is revoked for &lt;service&gt;</td>
<td>logSystem.csv</td>
</tr>
<tr>
<td>0800100</td>
<td>Notice</td>
<td>User account - created &lt;user account id&gt;</td>
<td>logAccount.csv</td>
</tr>
<tr>
<td>0800200</td>
<td>Notice</td>
<td>User account - deleted &lt;user account id&gt;</td>
<td>logAccount.csv</td>
</tr>
<tr>
<td>0800400</td>
<td>Notice</td>
<td>User account - name changed &lt;user account id&gt;</td>
<td>logAccount.csv</td>
</tr>
<tr>
<td>0800600</td>
<td>Notice</td>
<td>User account - password changed</td>
<td>logAccount.csv</td>
</tr>
<tr>
<td>0800800</td>
<td>Notice</td>
<td>User account - password reset &lt;user account id&gt;</td>
<td>logAccount.csv</td>
</tr>
<tr>
<td>0800A00</td>
<td>Notice</td>
<td>User account - unlocked</td>
<td>logAccount.csv</td>
</tr>
<tr>
<td>0800B00</td>
<td>Notice</td>
<td>User account - activated &lt;user account id&gt;</td>
<td>logAccount.csv</td>
</tr>
<tr>
<td>0800C00</td>
<td>Notice</td>
<td>User account - deactivated &lt;user account id&gt;</td>
<td>logAccount.csv</td>
</tr>
<tr>
<td>0800D00</td>
<td>Notice</td>
<td>User account - password rules changed</td>
<td>logAccount.csv</td>
</tr>
<tr>
<td>0800E00</td>
<td>Notice</td>
<td>User account - password expiration changed</td>
<td>logAccount.csv</td>
</tr>
<tr>
<td>0800F00</td>
<td>Notice</td>
<td>User account - session expiration changed</td>
<td>logAccount.csv</td>
</tr>
<tr>
<td>0900D00</td>
<td>Notice</td>
<td>&lt;user&gt; connected into interactive CLI with session id XXXXXX</td>
<td>logSession.csv</td>
</tr>
<tr>
<td>0900E00</td>
<td>Notice</td>
<td>&lt;user&gt; disconnected from interactive CLI with session id XXXXXX</td>
<td>logSession.csv</td>
</tr>
<tr>
<td>0900F00</td>
<td>Notice</td>
<td>&lt;user&gt; doesn’t have access to CLI - CLI session id XXXXXX</td>
<td>logSession.csv</td>
</tr>
<tr>
<td>0901000</td>
<td>Notice</td>
<td>&lt;user&gt; connected and executes remote command &lt;command&gt; into the CLI - CLI session id XXXXXX</td>
<td>logSession.csv</td>
</tr>
<tr>
<td>0901100</td>
<td>Notice</td>
<td>&lt;user&gt; finished executing remote command &lt;command&gt; into the CLI - CLI session id XXXXXX</td>
<td>logSession.csv</td>
</tr>
<tr>
<td>0901200</td>
<td>Notice</td>
<td>&lt;user&gt; connection rejected - CLI session id XXXXXX</td>
<td>logSession.csv</td>
</tr>
<tr>
<td>0901300</td>
<td>Notice</td>
<td>&lt;user&gt; disconnected from interactive CLI with session id XXXXXX due to session timeout</td>
<td>logSession.csv</td>
</tr>
<tr>
<td>Log Code</td>
<td>Type</td>
<td>Description</td>
<td>File</td>
</tr>
<tr>
<td>----------</td>
<td>-------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>0901400</td>
<td>Notice</td>
<td><code>&lt;user&gt;</code> disconnected from interactive CLI with session id XXXXXX due to concurrent connection with session id XXXXXX</td>
<td>logSession.csv</td>
</tr>
<tr>
<td>0A00100</td>
<td>Info</td>
<td>Network module upgrade success <code>&lt;f/w: xx.yy.zzzz&gt;</code></td>
<td>logUpdate.csv</td>
</tr>
<tr>
<td>0A00300</td>
<td>Info</td>
<td>Network module upgrade started</td>
<td>logUpdate.csv</td>
</tr>
<tr>
<td>0A00600</td>
<td>Info</td>
<td>Network module file system integrity OK <code>&lt;f/w: xx.yy.zzzz&gt;</code></td>
<td>logUpdate.csv</td>
</tr>
<tr>
<td>0B00300</td>
<td>Info</td>
<td>Time with NTP synchronized</td>
<td>logSystem.csv</td>
</tr>
<tr>
<td>0B00600</td>
<td>Info</td>
<td>Time settings changed</td>
<td>logSystem.csv</td>
</tr>
<tr>
<td>0B01100</td>
<td>Info</td>
<td>Time reset to last known date: &quot;date&quot;</td>
<td>logSystem.csv</td>
</tr>
</tbody>
</table>
6.7 SNMP trap oid

6.7.1 Eaton XupsMIB trap oid and message:

<table>
<thead>
<tr>
<th>Trap oid:</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>.1.3.6.1.4.1.534.1.11.4.1.0.x</td>
<td></td>
</tr>
<tr>
<td>.1.3.6.1.4.1.534.1.11.4.1.0.3</td>
<td>Battery discharging</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.534.1.11.4.1.0.4</td>
<td>Battery low</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.534.1.11.4.1.0.5</td>
<td>No more on battery</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.534.1.11.4.1.0.6</td>
<td>Battery OK</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.534.1.11.4.1.0.7</td>
<td>Power overload</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.534.1.11.4.1.0.8</td>
<td>Internal failure</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.534.1.11.4.1.0.10</td>
<td>Inverter internal failure</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.534.1.11.4.1.0.11</td>
<td>Bypass mode</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.534.1.11.4.1.0.12</td>
<td>Bypass not available</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.534.1.11.4.1.0.13</td>
<td>Load not powered</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.534.1.11.4.1.0.14</td>
<td>On battery</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.534.1.11.4.1.0.15</td>
<td>Building alarm through input dry contact</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.534.1.11.4.1.0.16</td>
<td>Shutdown imminent</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.534.1.11.4.1.0.17</td>
<td>No more on bypass</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.534.1.11.4.1.0.20</td>
<td>Breaker open</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.534.1.11.4.1.0.23</td>
<td>Battery test failed</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.534.1.11.4.1.0.26</td>
<td>Communication lost</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.534.1.11.4.1.0.30</td>
<td>Sensor contact is active</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.534.1.11.4.1.0.31</td>
<td>Sensor contact back to normal</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.534.1.11.4.1.0.32</td>
<td>Parallel UPS redundancy lost</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.534.1.11.4.1.0.33</td>
<td>Temperature alarm</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.534.1.11.4.1.0.34</td>
<td>Battery charger fault</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.534.1.11.4.1.0.35</td>
<td>Fan fault</td>
</tr>
<tr>
<td>.1.3.6.1.4.1.534.1.11.4.1.0.36</td>
<td>Fuse fault</td>
</tr>
</tbody>
</table>
6.8 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.

### 6.8.1 Commands available

You can see this list anytime by typing in the CLI:

```
?
```

### 6.8.2 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 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)

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

Help
"role-system-info-viewer"

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

-<OPTION>, --help display help page
-<OPTION>, --lan display Link status and MAC address
-<OPTION>, --ipv4 display IPv4 Mode, Address, Netmask and Gateway
-<OPTION>, --ipv6 display IPv6 Mode, Addresses and Gateway
-<OPTION>, --domain display Domain mode, FQDN, Primary and Secondary DNS

"role-system-manager"
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>
      dhcp
-f, --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
    - disable IPv6
-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 Adress, 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 Adress, Netmask and Gateway
   netconf -i manual 192.168.0.1 255.255.255.0 192.168.0.2
-> Disable IPv6
   netconf -6 disable

6.8.4 reboot
Reboots the card.

Help

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

6.8.5 sanitize
Sanitize command to return card to factory reset configuration.

Help

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

6.8.6 time
Command used to display or change time and date.

Help

"system-info-viewer"

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

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

"system-info-admin"
CLI Information – 147

Usage: time [OPTION]...
Display time and date, change time and date.
- h, --help display help page
- p, --print display date and time in YYYYMMDDhhmss format
- s, --set <mode>
  Mode values:
  - set date and time (format YYYYMMDDhhmss)
    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

6.8.7 save_configuration | restore_configuration

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-formated standard input.

Examples of usage

Save over SSH: sshpass -p $PASSWORD ssh $USER@$CARD_ADDRESS save_configuration > $FILE
Restore over SSH: cat $FILE | sshpass -p $PASSWORD ssh $USER@$CARD_ADDRESS restore_configuration

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
- $FILE is a path to the JSON file (on your host computer) where the configuration is saved or restored.

6.8.8 maintenance

Creates a maintenance report file which may be handed to the technical support.
Help

6.8.9 get release info
Displays certain basic information related to the firmware release.

get release info
-d Get current release date
-s Get current release sha1
-t Get current release time
-v Get current release version number

6.8.10 logout
Logout the current user.

logout

6.8.11 history
Displays recent commands executed on the card.

history

6.8.12 ping
Ping utility is 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

6.8.13 ssh-keygen

Command used for generating the ssh keys.

Help

$ssh-keygen

-h, --help Display help
<cr> Renew SSH keys

6.8.14 traceroute

Traceroute utility for checking the configuration of the network.

Help

$traceroute

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

6.8.15 ldap-test

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 (optionnal)
  --secondary     Force the test to use secondary server (optionnal)
  -v,--verbose    Print the exchanges with LDAP server (optionnal)
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 (optionnal)
  -s,--secondary  Force the test to use secondary server (optionnal)
  -v,--verbose    Print the exchanges with LDAP server (optionnal)
ldap-test --checkmappedgroups [--primary|--secondary] [-v]
Check LDAP mapping
  -p,--primary    Force the test to use primary server (optionnal)
  -s,--secondary  Force the test to use secondary server (optionnal)
  -v,--verbose    Print the exchanges with LDAP server (optionnal)

Quick guide for testing:

In case of issue with LDAP configuration, we recommand 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>

6.9 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.

6.9.1 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. Eaton reserves the right to charge minimal administrative costs,
in compliance with the terms of the underlying open source licenses, when the situation requires.
6.9.2 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,

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.

6.9.3 Notice for our proprietary (i.e. non-Open source) elements

Copyright © 2017 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.
6.10 Acronyms and abbreviations

**AC**: Alternating current.

**AVR**: Automatic Voltage Regulation provides stable voltage to keep equipment running in the optimal range.

**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.

**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

**GID**: Group Identifier is a numeric value used to represent a specific group (LDAP).

**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 UPS from a browser-based management console. Administrators can monitor, manage, and control a single UPS locally and remotely. A familiar browser interface provides secure access to the UPS Administrator Software and UPS 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).

**kVA**: kilovolt-ampere

**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.

**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 a cryptographic protocol that provides 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.

**UPS**: An uninterruptible power supply is an electrical apparatus that provides emergency power to a load when the input power source or mains power fails.

A UPS is typically used to protect hardware such as computers, data centers, telecommunication equipment or other electrical equipment where an unexpected power disruption could cause injuries, fatalities, serious business disruption or data loss.
7 Troubleshooting

7.1 Action not allowed in Control/Schedule/Power outage policy

7.1.1 Symptom
Below message is displayed when you access the Control, Schedule or Power outage policy page.

This action is not allowed by the UPS.
To enable it, please refer to the user manual of the UPS and its instructions on how to configure the UPS settings and allow remote commands.

7.1.2 Possible Cause
1- Remote commands are not allowed due to the UPS configuration (see the action below)
2- The UPS does not support remote commands.

7.1.3 Action
Refer to the UPS user manual and its instruction on how to configure the UPS settings and allow remote commands.
Example: UPS menu Settings>>>ON/OFF settings>>>Remote command>>>Enable.

7.2 Client server is not restarting

7.2.1 Symptom
Utility power has been restored, the UPS and its load segments are powered on, but the Client server does not restart.

7.2.2 Possible Cause
The “Automatic Power ON” server setup setting might be disabled.

7.2.3 Action
In the server system BIOS, change the setting for Automatic Power ON to "Enabled".

7.3 EMP detection fails at discovery stage

In the Network Module, in Card>>>Commissioning, EMPs are missing in the Sensor commissioning table.

7.3.1 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.
How do I log in if I forgot my password?

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

7.4.1 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 Recovering main administrator password.

7.5 IPP is not able to communicate with the Network module

7.5.1 Symptoms

- In the Network Module, in Protection>>>Agents list>>>Agents list, agent is showing "Lost" as a status.
- In the Network Module, in Settings>>>Certificates>>>Trusted remote certificates, the status of the Protected applications (MQTT) is showing "Not valid yet".
- IPP shows "The authentication has failed", "The notifications reception encountered error".
7.5.2 Possible cause

The IPP certificate is not yet valid for the Network Module.

Certificates of IPP and the Network Module are not matching so that authentication and encryption of connections between the Network Module and the shutdown agents is not working.

7.5.3 Setup

IPP is started.

Network module is connected to the UPS and to the network.

7.5.4 Action #1

Check if the IPP certificate validity for the Network Module.

**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 static 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 **Sign In**. The Network Module web interface appears.

**STEP 2:** Navigate to **Settings/Certificates** page

**STEP 3:** In the **Trusted remote certificates** section, check the status of the Protected applications (MQTT).

If it is "Valid" go to Action#2 STEP 2, if it is "Not yet valid", time of the need to be synchronized with IPP.

**STEP 4:** Synchronize the time of the Network Module with IPP and check that the status of the Protected applications (MQTT) is now valid.

Communication will then recover, if not go to Action#2 STEP 2.

7.5.5 Action #2

Pair agent to the Network Module with automatic acceptance (recommended in case the installation is done in a secure and trusted network).

For manual pairing (maximum security), go to **Servicing the Network Management Module***>>>Pairing agent to the Network Module* section and then go to STEP 2, item 1.

**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 static 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 **Sign In**. The Network Module web interface appears.

**STEP 2:** Navigate to **Protection/Agents list** page.

**STEP 3:** In the **Pairing with shutdown agents** section, select the time to accept new agents and press the **Start** button and **Continue**. During the selected timeframe, new agent connections to the Network Module are automatically trusted and accepted.

**STEP 4:** Action on the agent (IPP) while the time to accepts new agents is running on the Network Module.
Remove the Network module certificate file(s) *.0 that is (are) located in the folder Eaton\IntelligentPowerProtector\configs\tls.

7.6 LDAP configuration/commissioning is not working

Refer to the section Servicing the Network Management Module>>>Commissioning/Testing LDAP.

7.7 Password change in My preferences is not working

7.7.1 Symptoms
The password change shows "Invalid credentials" when I try to change my password in My preferences menu.

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

7.7.3 Action
Let one day between your last password change and retry.

7.8 UPS Network Module fails to boot after upgrading the firmware

7.8.1 Possible Cause
The IP address has changed.

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

7.8.2 Action
Recover the IP address and connect to the card.

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

7.9.1 Symptom
After an upgrade:

- The Web interface is not up to date
- New features of the new FW are not displayed

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.