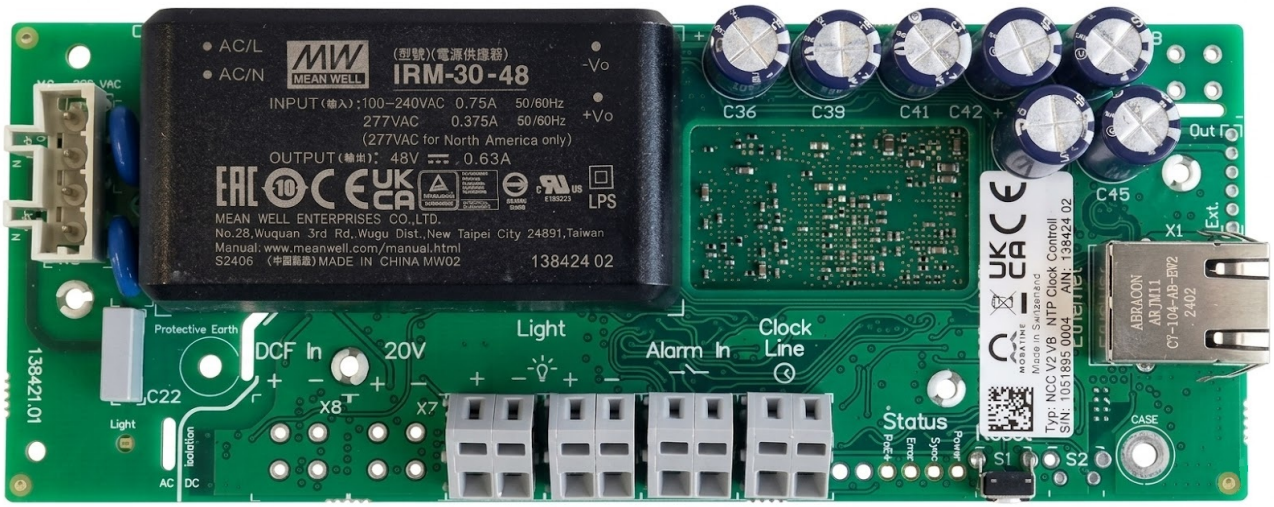
User Manual

NCC V2

Network Clock Controller V2



Scan the QR code or enter following URL to get the latest version:
https://www.mobatime.com/support/resources/

BE-801480.00 | 2026-08-10

Regulations and Certification

This product was developed and produced in accordance with the following EU directives:

EMC :
Electromagnetic compatibility directive 2014/30/EU

LVD :
Low voltage directive 2014/35/EU

RED :
Radio equipment directive 2014/53/EU

RoHS :
Restriction of the use of certain hazardous substances directive 2011/65/EU

REACH :
Chemical substances directive 1907/2006/EC

WEEE :
Waste electrical and electronic equipment directive 2012/19/EU

Railway Interop. :
Interoperability of the rail system within the European Union directive 2016/797/EU

Railway Safety :
Railway safety directive 2016/798/EU

See Conformity for the declaration of conformity of this specific product. This product may offer a CB test certificate for download at www.mobatime.com/support/resources/

CE

Important Notes

1. Please read and follow the safety information in this document before operating the product. We cannot guarantee that no accidents or damage will occur due to improper use of this product. Please use this product with care and operate at your own risk.
2. We are not liable for any direct or indirect damage caused by the use of this document or the said product.
3. This product must be connected and installed by a qualified electrician who is familiar with the relevant regulations (e.g. VDE).
4. The information in this document is subject to change without notice. The latest version of this document is available for download at www.mobatime.com/support/resources/ .
5. The product software is continuously being optimized and supplemented with new options. The latest firmware is available for download at www.mobatime.com/support/resources/ .
6. This Instruction Manual has been composed with the utmost care to explain all the details to ensure a safe and stable operation of this product. Nevertheless, if questions arise or any errors appear, feel free to contact support.
7. **MOBATIME Two Years Limited Product Warranty.** MOSER-BAER AG and BÜRK MOBATIME GmbH warrant MOBATIME branded hardware product contained in the original packaging against defects in materials and workmanship when used normally in accordance with MOBATIME's guidelines for a period of TWO YEARS from the date of original retail purchase by the end-user purchaser.

8. No part of this document or the said product may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from BÜRK MOBATIME GmbH, D-78026 VS-Schwenningen or MOSER-BAER AG - CH 3454 Sumiswald.

9.

Table of Contents

1 Safety

Read the safety sections carefully and follow all the instructions. This ensures safe and reliable operation of this device.

1.1. Instructions and Symbols

Symbols used throughout this document and their meaning are as follows:

A note or important information.

Answer to a possible question. Contact information.

Keep away from children and people with limited physical, sensory, or mental capacities.

Action needs to be taken.

Connect device to earth ground.

More information included in the manual.

Disconnect mains power before doing anything.

An example or a hint.

Additional references or information.

Attention of electrical shocks.

Surface may be hot.

Item is flammable.

A warning, be cautious.

Recyclable materials.

Do not put in trash.

1.2. General

For safety and licensing reasons, unauthorized modifications and/or changes to the product are prohibited. Maintenance, adjustments or repairs may only be carried out by the factory (copyright holder).

The product is not a toy; it does not belong in the hands of children. Mount or place the product so that it cannot be reached by children. Children may try to insert objects into the product. The product will not only be damaged, but there is also a risk of injury, as well as danger to life through electric shock.

Never open the housing of this product, for it poses mortal danger from electric shock or may even cause a fire.

Keep packaging such as plastic films away from children. There is the risk of suffocation if misused.

Use caution with the product, knocks, blows, or even falls from a low height can damage it.

In industrial facilities, the accident prevention regulations of the trade associations for electrical systems and equipment must be observed.

Do not use the product if it is damaged. It can be assumed that safe operation is no longer possible if:

- the product has visible damage;
- the product is not working properly (thick smoke or a burning smell, audible crackling noise, discoloration of the product or surrounding areas);
- the product was stored under adverse conditions;
- tough conditions during transport.

Improper handling of this product operated on the mains voltage can cause mortal danger from electric shock!

Interconnecting or combining equipment bearing a CE label does not inevitably result in a system that conforms with the safety regulations. Integrators will have to reassess the new product's compliance according to the locally valid directives. See section Conformity for more information on certification of this product.

1.3. Installation

This product must be connected and installed by a qualified electrician who is familiar with the relevant regulations (e.g. VDE).

Never plug the product into voltage/power supply immediately after it has been moved from cold into warm environment (e.g. during/after transport/unboxing). The resultant condensed water may damage the product or may cause electric shock.

Allow the product to reach the ambient temperature. Wait until the condensation has evaporated, this can take a few hours. Only then can the product be connected to the voltage/current supply and put into operation.

This product may have screw terminal with open electrical contacts. It is essential to ensure that the connection is made only when no voltage/current is applied. Secure the power supply to prevent accidental reconnection. Verify the absence of voltage using an appropriate meter.

The power supply line must be protected with a residual current circuit breaker (RCCB) with a trip current ≤ 30 mA.

Always connect earth ground to the device at the indicated protective earth terminal (PE or earth symbol indication).

Always unplug a power plug from the socket only at the intended gripping surface, pull the power plug not the cord from a power outlet. Wires may rip out and pose danger to life through electric shock.

Maintain sufficient cooling of the product according to its specifications.

1.4. Operation

- Use the product in the specified environment. Use outside of the specifications can damage the product and/or stop any operation
- The product may not be exposed to extreme temperatures, direct sunlight or strong vibrations. Protect the product from moisture, dust and dirt.

Operation in environments with excessive dust, flammable gases, vapours or solvents is not permitted. It may cause explosion or fire.

Depending on the cooling type and ambient temperature, the product housing may reach temperatures above 60 °C, which can burn the skin

- Do not overload the product. Note the input / output voltages and currents as well as output powers indicated on the product.
- Depending on the input currents and input voltages, suitable connecting cables with appropriate cable diameter must be used. Only use the plugs and connectors supplied in the original packaging with the product.

1.5. Maintenance and Cleaning

- If the product and/or the connecting cable is damaged, do not touch it: there is mortal danger from electric shock! First, turn off the power supply to all poles of the product (turn off associated circuit breaker or remove the fuse, then turn off GFCI). Verify the absence of voltage using an appropriate meter.
- For the end consumer, the product is maintenance free. Leave any maintenance to an expert. Repairs may only be done by the factory itself (copyright holder).
- For external cleaning one can use a clean, soft, dry cloth. Dust can be easily removed with a clean, soft brush and a vacuum cleaner

Unplug all poles of the product from the operating voltage before cleaning.

- Do not use aggressive chemicals or abrasive cleaners, as this may cause discoloration or even material changes.
- You can use cleaning / disinfection supplies on stainless steel frame for extra cleanliness.
- This product is equipped with fuses for protection against high voltage and high currents. Burned fuses may only be replaced by the factory itself (copyright owner).

Never bridge a fuse, it is a fire hazard and can cause a fatal electric shock.

Read the Troubleshooting section to find help to common mistakes, misbehavior and knows issues.

1.6. Disposing

At the end of its lifecycle, do not dispose of this device in the regular household rubbish. Return it to the supplier who will dispose of it correctly.

The user is lawfully obligated to return unusable batteries. **Disposal of used batteries through household waste is prohibited!** Batteries which contain dangerous substances are labelled with a picture of crossed out trash bin. The symbol means that this product may not be disposed through household waste. Unusable batteries can be returned free of charge at appropriate collection points of your waste disposal company or at shops that sell batteries. By doing so, you fulfil your legal responsibilities and help protect the environment.

This product was packed and stuffed with proper materials to protect it during transportation. Packaging materials can be recycled and should be disposed environmentally friendly.

2 Introduction

2.1. Product Description

The **Network Clock Controller V2** , abbreviated to **NCC V2** , acts as an interface between a computer network and MOBALine movements.

- **Secure and Reliable:** Features secure boot, encrypted storage, and signed firmware updates to ensure tamper-proof operation.
- **Integrated Illumination Control:** Built-in LED driver with fault detection and flexible control modes (manual operation, AC input-based switching or scheduled operation).
- **Intuitive Web Interface:** An easy-to-use graphical interface allows for straightforward configuration and management.
- **Advanced Monitoring:** Monitor device status and events with modern protocols such as Syslog and SNMPv3 (read-only access + traps).
- **Automation-Ready:** A standard RESTCONF API enables seamless integration into network management systems.
- **Automatic Device Discovery:** Supports SSDP for fast and effortless detection within the local network.
- **Accurate Time Synchronization:** Uses NTP to maintain precise and reliable timekeeping.
- **Flexible Network Configuration:** Supports DHCP for automatic IP address assignment.
- **Enhanced Security by Default:** Each device is shipped with a unique default password.

2.2. Scope of Delivery

Verify the shipment on arrival and report any missing items to the supplier within 14 days.

The package contains the following items:

- **NCC V2** - Network Clock Controller V2 in the selected variant
- 4-pole spring terminal (only for **NCC V2 AC** and **NCC V2 VB**)

2.3. Technical Specification

The following technical specifications apply. Refer to the Installation chapter for additional details.

- **General**
  - **Mechanical Dimensions** (W x D x H): 165 mm x 65 mm x 37 mm
  - **Weight** :
    - NCC V2: 60 g
    - NCC V2 AC: 150 g
    - NCC V2 VB: 180 g
  - **Temperature Range** : -30°C to +70°C
  - **Operating Altitude** : <4000m above sea level
  - **Relative Humidity** : 5 to 95% (non-condensing)
- **Synchronization**
  - **Synchronized** : typically < ±50ms
  - **Unsynchronized** : typically < ±2s after 24h

2.4. Compliance

2.4.1. EMC and Safety

- EN 61000-6-2 (industrial)
- EN 61000-6-4 (industrial)
- EN 50121-4 (railway)
- EN 62368-1 (safety)

2.4.2. Networking

Implemented LAN related standards are the following:

- RFC 2818 (HTTPS)
- RFC 5424 (Syslog)
- RFC 7950 (Yang)
- RFC 6020 (YANG model)
- RFC 6241 (Netconf)
- RFC 5905 (NTP)
- RFC 3414 (SNMPv3)

2.5. Terms and Definitions

The following terms and definitions apply to this device:

Permanently connected equipment :	Equipment that can only be connected to or disconnected from the mains supply using a tool.
Professional equipment :	Equipment intended for use in commercial, industrial, or trade environments and not intended for sale to the general public.
Class II equipment :	Equipment in which protection against electric shock is achieved through double insulation or reinforced insulation, without reliance on protective earthing.
Instructed person :	A person who has been instructed or supervised by a skilled person regarding potential energy sources and who is capable of responsibly using the provided safeguards and precautionary measures (for installation and operation of the device).
Skilled person :	A person with relevant education, training, or experience enabling them to identify hazards and take appropriate measures to reduce the risk of injury to themselves and others.
Fire enclosure :	Enclosure intended as a safeguard against the spread of fire from within the enclosure to outside the enclosure.

These terms may be used throughout this manual. All instructions must be followed to ensure safe operation of the device and user safety. As this device is classified as professional and permanently connected equipment, it may only be installed by a **skilled person** and operated by an **instructed person** . Normal operating conditions must be ensured and maintained at all times (see the Technical Specification section for details).

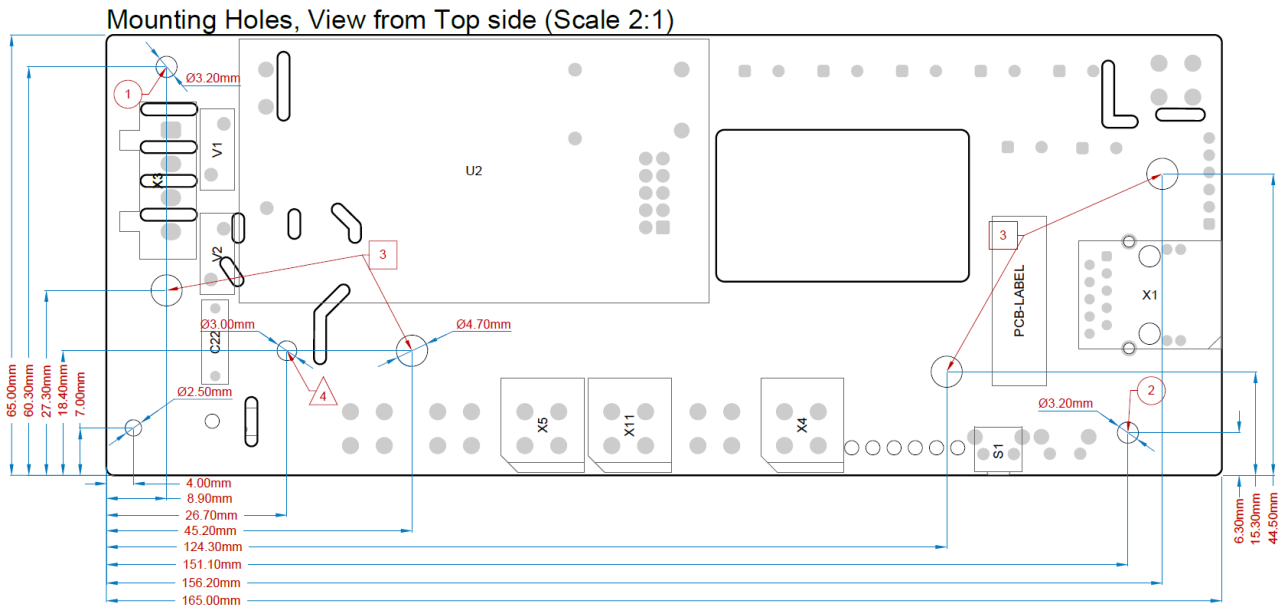
2.6. Abbreviations

The following abbreviations are used throughout this manual:

NTP :	Network Time Protocol
SNMP :	Simple Network Management Protocol
MIB :	Management Information Base
NMS :	Network Management System
MOBA :	Moser-Baer AG, Sumiswald
HTTP(S) :	Hypertext Transfer Protocol (Secure)
REST API :	Representational State Transfer Application Programming Interface
RESTCONF :	HTTP-based protocol defined in RFC 8040
YANG :	Data modeling language used with RESTCONF (defined in RFC 7950)
API :	Application Programming Interface
DHCP :	Dynamic Host Configuration Protocol
SLAAC :	Stateless Address Autoconfiguration
DNS :	Domain Name System
ICMP :	Internet Control Message Protocol
TLS :	Transport Layer Security
SSDP :	Simple Service Discovery Protocol
LLDP :	Link Layer Discovery Protocol

3 Installation

3.1. Mounting



- **(1) Main Mounting Hole** : Mechanical mounting point only; no electrical connection.
- **(2) Functional Earth (Ethernet)** : Electrical connection using a metal fastener. Required when a DCF receiver is used.
- **(3) Standoffs** : Support the PCB at multiple points to prevent flexing when cable terminals are accessed.
- **(4) Function Earth (EMC / Chassis)** : Electrical connection to the local chassis ground using a metal fastener.
  - **Class II Compliance** : The product is designed as a Class II (double-insulated) device and does not rely on a protective earth connection for electrical safety.
  - **Purpose** : This connection is utilized purely as a Function Earth (FE) path for internal EMC suppression capacitors (Y-capacitors). Connecting it to an earthed chassis or enclosure does not affect the safety class of the device but is recommended for optimal electromagnetic compatibility.

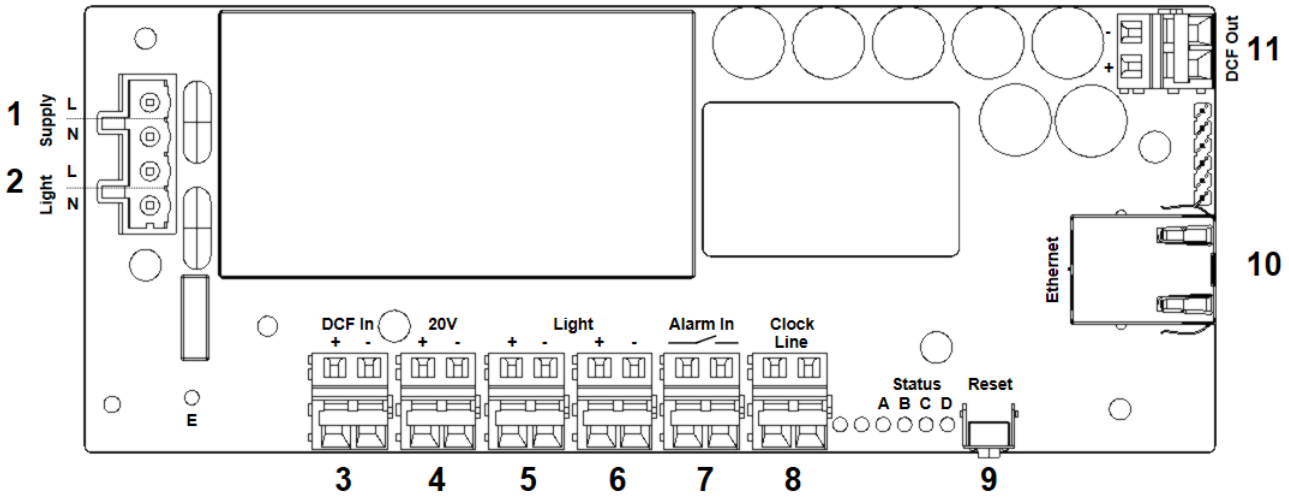
The device must only be installed by a **skilled person** , such as a qualified electrician, who is familiar with the relevant regulations.

This equipment is not suitable for use in locations where children are likely to be present.

The device must only be installed in a **fire enclosure** with protection against contact, dirt and water.

Disconnect all power sources - including the illumination switching input - before handling the PCB. Additionally, the *NCC V2 VB* may remain energized even after all external power sources are disconnected. After shutting down the device, wait at least one hour before handling it.

3.2. Interfaces and Variants



Three product variants are available, differing in feature set and interface availability. The following table summarizes these differences and the associated connections. Refer to the subsequent sections for detailed descriptions.

Label	Name	NCC V2	NCC V2 AC	NCC V2 VB
Ordering Information				
-	Ordering Number	138422	138423	138424
-	Spring Terminal Included	✗	✓	✓
Power Supply				
10	PoE / PoE+	✓	✓	✓
1	Mains	✗	✓	✓
-	Backup Supply	✗	✗	✓
Indicators / Controls				
9	Reset Button	✓	✓	✓
A-D	Status LEDs	✓	✓	✓
Inputs and Outputs				
10	Ethernet	✓	✓	✓
8	Clock Line	✓	✓	✓
5-6	Illumination	✓	✓	✓
7	Alarm Input	✗	✗	✓
2	LED Switching Input	✗	✓	✓
3, 4	DCF Input	✗	✗	✗
11	DCF Output	✗	✗	✗

3.2.1. Mains

Mains voltage connections are made using a 4-pole pluggable spring-clamp terminal block (WAGO 721 series). The LED switching input may be left unconnected if this function is not required. The maximum permissible conductor cross-section is 2.5 mm², and the insulation must be stripped to a length of 9-10 mm. All phase and neutral conductors shall be secured near the terminal block using cable ties.

Label	Connection Type	Nominal Voltage	Voltage Tolerance	Power Rating	Length	Description
1	Terminal Block	100-240 VAC 50 Hz	+/- 10%	30 W	N/A	Mains supply input that powers the device. **Recommended Fuse:** **3.15 A / slow-blow**
2	Terminal Block	100-240 VAC 50 Hz	+/- 10%	0.5 W	N/A	Switching input that can turn the LED illumination on an off. **Recommended Fuse:** **315 mA / fast-acting**

The external electrical installation must include an appropriate fuse and an all-pole mains switch for all mains connections.

Only use the original terminal block. We accept no responsibility for any damage to persons or property resulting from the use of plugs other than those provided, or from faulty or unsafe wiring.

Avoid stripping wires in a way that could lead to contact with other components. Make sure to attach strain reliefs to relieve the connection points of cables and lines from mechanical stress.

The power supply connection to the clock must be installed by a **skilled person** . National regulations must be followed.

Make sure all wires are disconnected from live voltage before handling them.

Power supply units may fail permanently if operated outside of the nominal voltage ratings.

3.2.2. Ethernet

The Ethernet connector (10) accepts standard Ethernet network cables. The device supports auto-negotiation for 10 Mbps and 100 Mbps operation, as well as Auto-MDIX.

Power over Ethernet (PoE and PoE+) is supported but not required, as the device can also be powered via an AC supply. When mains power is connected, PoE functionality is automatically disabled.

Label	Connection Type	Nominal Voltage	Voltage Tolerance	Power Rating	Length	Description
10	RJ45	0-57 V	+/- 10%	25.5 W	< 100 m	Ethernet connection with support for PoE or PoE+.

Power supply units may fail permanently if operated outside of the nominal voltage ratings.

3.2.3. Illumination Driver

The *NCC V2* can drive LED illumination rings for single-sided and double-sided clocks. Two separate connectors (5, 6) are provided to simplify installation and servicing; both connectors are internally connected to the same LED driver.

Label	Connection Type	Voltage	Current	Length	Description
5, 6	Terminal Block	0-24 V	0-700 mA	< 1 m	LED Driver Outputs.

The maximum available illumination power depends on the selected power source. When powered via PoE only, the maximum brightness may be limited (≈ 10 W with PoE, ≈ 16 W with PoE+ or mains power).

Under open-circuit conditions (no load connected), the output voltage may rise to up to 57 V. To prevent damage to the LEDs, connect or disconnect the illumination only when the device is powered off.

3.2.4. Clock Line Driver

The *NCC V2* clock line output (8) supplies power to, synchronizes, and monitors clock movements for both single-sided and double-sided clocks using MOBALine.

The connection is made using two conductors. Polarity is not relevant for operation; however, when two movements are connected and monitoring is required, one movement must be connected with reversed polarity.

Label	Connection Type	Voltage	Current	Length	Description
8	Terminal Block	20 V	0-100 mA	< 1 m	Clock Line Output.

3.2.5. Status LEDs

Device status is indicated by multiple LEDs.

Label	Name	Meaning
A	PoE+	PoE+ or AC power input is connected
B	Error	An error is active (e.g. short circuit on an output)
C	Sync	NCC V2 is synchronized
D	Power	NCC V2 is powered
E	Light	State of the illumination switching input (*AC/VB* only)

3.2.6. Reset Button

The reset button (9) allows the device to be rebooted or restored to factory settings. Press and hold the button for **5 seconds** to reboot the device, or for **20 seconds** to perform a factory reset.

For security reasons, the factory reset function can be disabled in the device configuration.

Never press the reset button during configuration changes or a firmware update.

3.2.7. Alarm Input

The alarm input can be connected to a normally open, potential-free switching contact. This input may be used, for example, for vandalism detection.

Label	Connection Type	Voltage	Current	Length	Description
7	Terminal Block	20 V	0-2 mA	< 1 m	Alarm Input.

3.2.8. Backup Supply

The NCC V2 VB variant includes an internal energy storage unit. In the event of a power failure, this backup supply ensures that connected analog clock movements are driven to the 12 o'clock position.

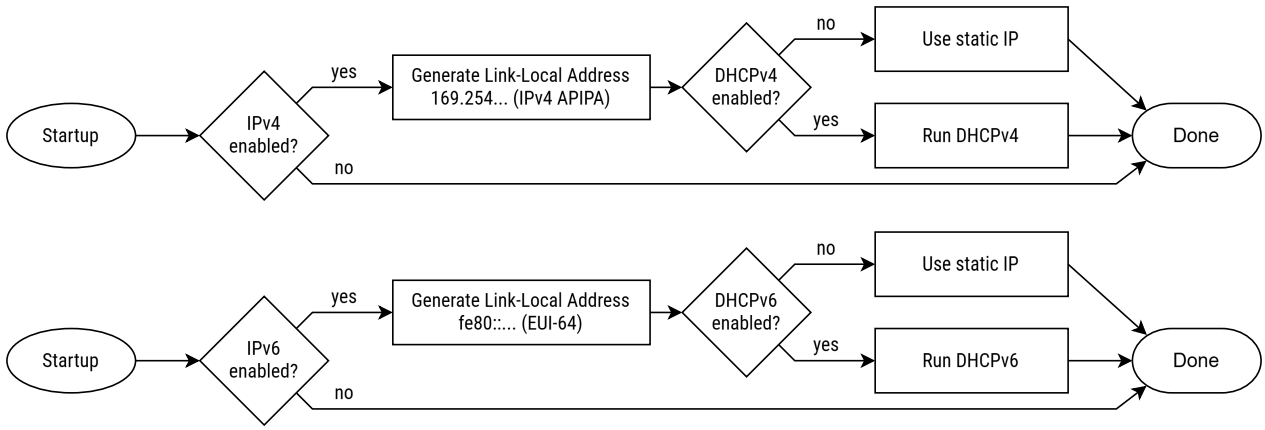
4 Commissioning

4.1. Discovery

This chapter describes ways of connecting to a device that uses the default settings. If the device is already configured, you can access the web interface simply by entering the IP address directly into the address bar of a web browser.

4.1.1. Default Device Behavior

If a DHCPv4 or DHCPv6 server is present in the network, the device will receive the correct network configuration upon startup. In case of an error or when no DHCP server is available, link-local IP addresses can be used. Because such addresses are never routed, the device will be unable to communicate with anything outside its local network segment, and a valid configuration will need to be applied manually. A client with a link-local address (e.g., 169.254.x.x or fe80::/10) might be needed to access the web interface until the device is properly configured.



The first startup takes longer than subsequent ones. It can take up to a minute until the device becomes reachable over the network.

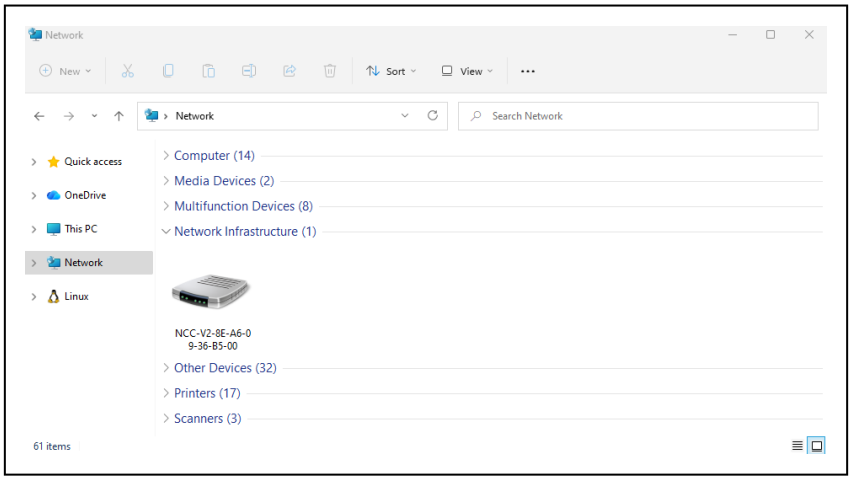
4.1.2. Determining the Device IP

There are multiple ways of discovering the device in the network.

If you are connecting to the device on a network **without a DHCP server** , your host computer must temporarily also use a **link-local** network address. Usually this works without modifying any settings, but under some circumstances, some temporary changes are needed. See Network FAQ for more details.

4.1.2.1. Using SSDP

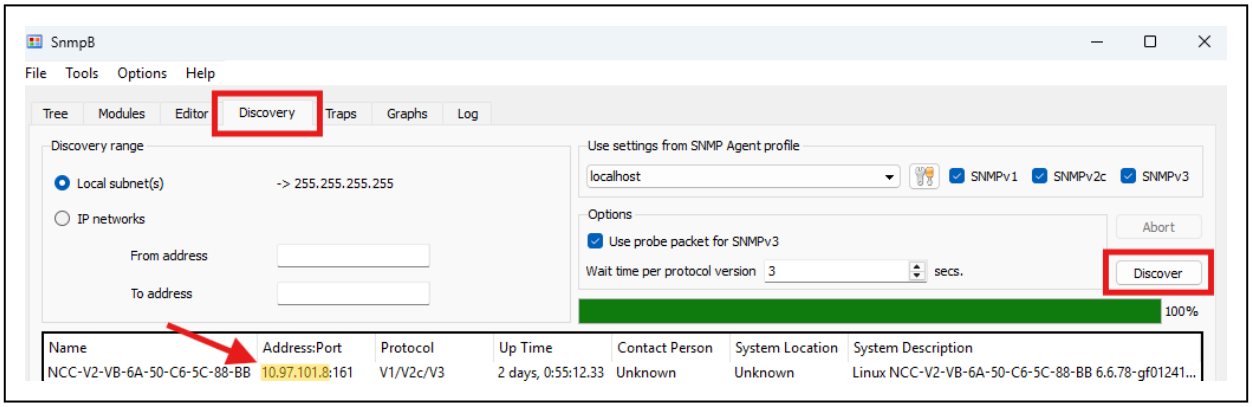
On Windows, open the file explorer and navigate to the `Network` section. The web interface is opened by double-clicking on the device:



On Linux, the `ssdp-scan` utility offers a similar way to discover devices.

4.1.2.2. Using SNMP

SNMPv2c is enabled by default. This allows the device to be discovered using an SNMP GET request broadcast. Most SNMP management tools support this discovery method. The screenshot below illustrates the process for the SNMPB software:



Once the device is detected, copy its IP address (without the port) into the address bar of a web browser and press **Enter** to open the web interface.

4.1.2.3. DHCP Server

If the network provides a DHCP server, there are two additional ways to discover the device. Details may vary depending on the DHCP server vendor. Refer to the server documentation for specifics.

- **Check the assignments** : The DHCP server maintains a list of currently assigned IP addresses, typically showing hostnames and IPs. The device's IP address can be identified from this list.
- **IP Assignment by MAC Address** : Most DHCP servers allow assigning a specific IP address to a device based on its MAC address. Using this method, a predefined IP can be assigned to the device.

Once the IP address is known, it can be accessed via a web browser.

4.1.2.4. IPv6 EUI-64

For IPv6, the device generates a link-local address using the **EUI-64** method, which derives it from the device's MAC address. This process is deterministic: if the MAC address is known, the link-local IPv6 address can be calculated. The MAC address is printed on a label on the device.

The example below illustrates the calculation manually, though it is usually easier to use an online EUI-64 calculator.

1. Device MAC address as printed on the label: `4E:D1:BA:A7:0F:40`
2. Split the address in half: `4ED1BA + A70F40`
3. Insert `FFFE` in between: `4ED1BA + FFFE + A70F40`
4. Arrange into groups of four hexadecimal digits: `4ED1:BAFF:FEA7:0F40`
5. Invert the 7th bit (second hex digit): `4CD1:BAFF:FEA7:0F40`
6. Add the link-local prefix `FE80::` to get the final address: `FE80::4CD1:BAFF:FEA7:0F40`

4.1.2.5. IP Scanner

The device IP address can also be discovered using an IP scanner. This method may take longer than the alternatives described above and is therefore not preferred.

If used, the scan should be limited to the IPv4 address range assigned by the DHCP server (if known, for example `192.168.0.0/8`) or to the IPv4 link-local range (`169.254.0.0/16`). Scanning IPv6 address ranges should be avoided due to the very large number of possible addresses.

4.2. Webinterface

The web interface is the primary method for accessing and configuring the device.

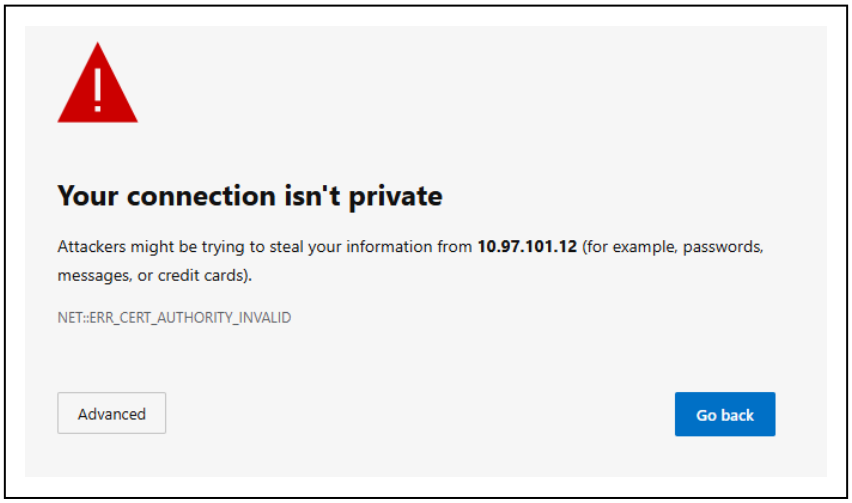
4.2.1. Connecting

To connect, enter the device's IP address into the address bar of a web browser. Do not include a port number. When using an IPv6 address, ensure that it is enclosed in square brackets.

- Example (IPv4): `10.97.101.15`
- Example (IPv6): `[FE80::4CD1:BAFF:FEA7:0F40]`

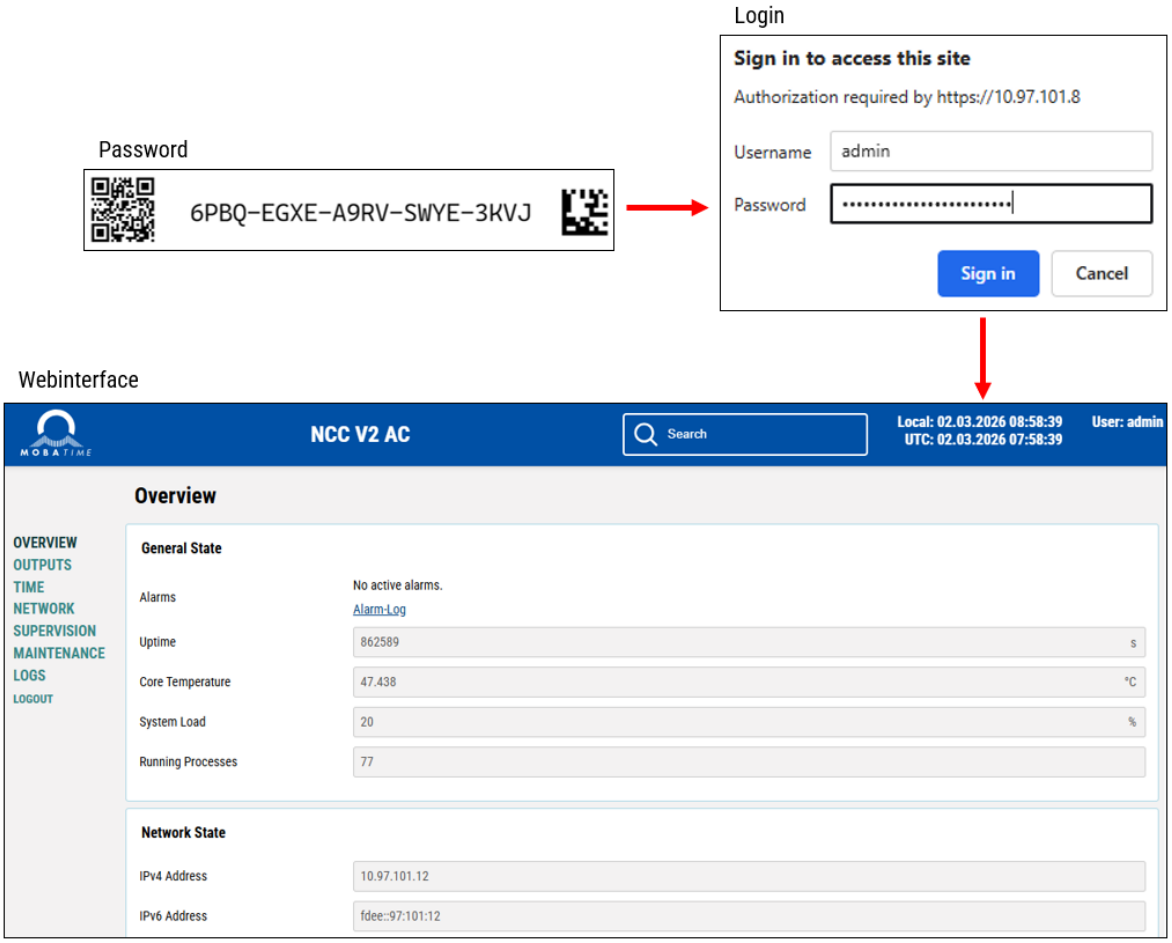
4.2.2. Initial Security Warning

Upon first opening the web interface the following error message is shown, which means that the browser does not trust the device's TLS certificate. This can be fixed by later configuring a trusted certificate as described in TLS Certificates . With a direct network connection to the device, it is usually reasonable to click on `Advanced` and proceed with commissioning despite this warning.



4.2.3. Login

A login window is then shown. Each device comes pre-configured with a unique password. This password is printed on a label on the device (example: *6PBQ-EGXE-A9RV-SWYE-3KVJ*):



Once logged in, the web interface is shown and it is now possible to configure the device.

After the first successful login, the default password must be changed immediately.

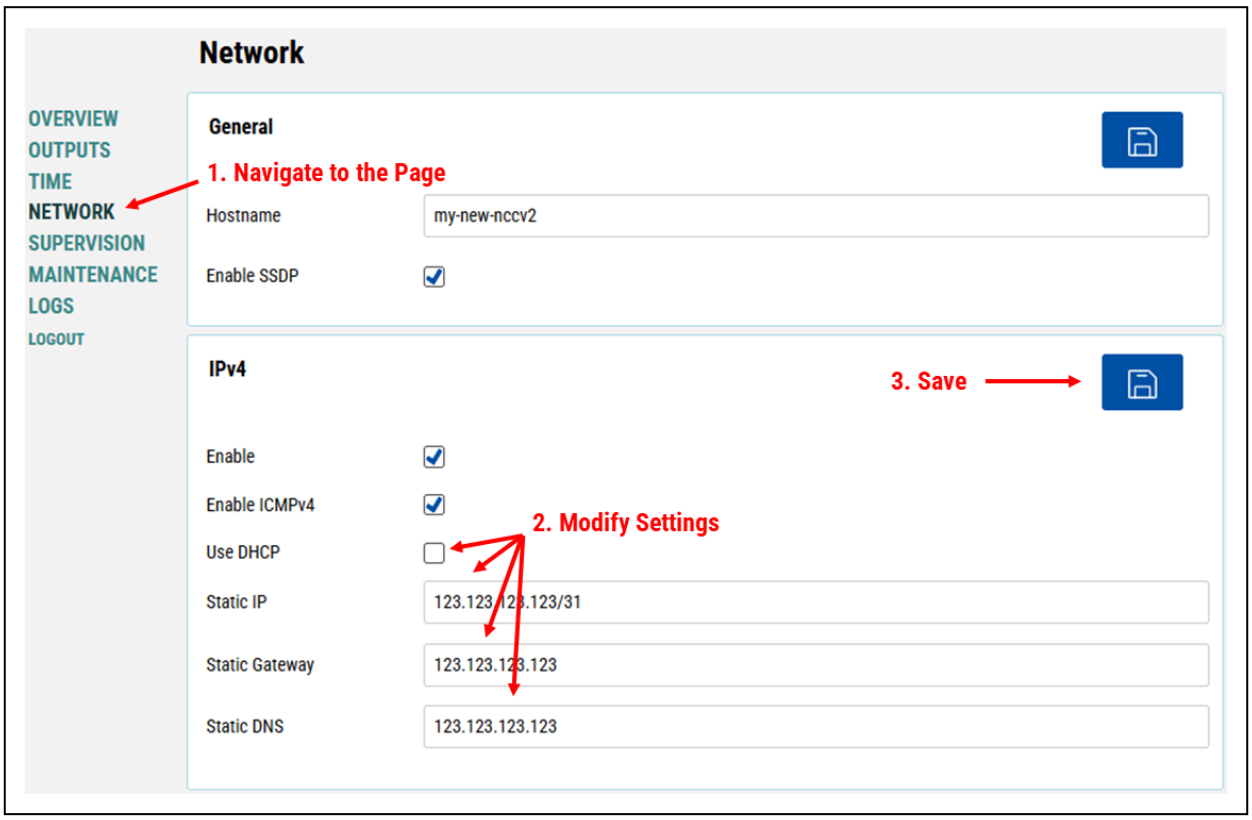
Use a secure password manager to store the administrator password. This enables the use of randomly generated, long, unique, and highly secure passwords.

If access to the administrator password is lost, a factory reset must be performed. If the factory reset function has been disabled, recovery is not possible.

4.2.4. Modifying Settings

One of the first configuration tasks is typically to adjust the network settings so that the device integrates into the existing network.

The general workflow for modifying the device configuration is shown below:



1. **Navigate to the relevant settings page.** There is also a search bar that will show all options related to a term.
2. **Modify the desired values.** Input fields that are not applicable are automatically hidden (for example, the static IP address fields when DHCP is enabled). Hovering over a setting displays additional help text.
3. **Save the configuration.**

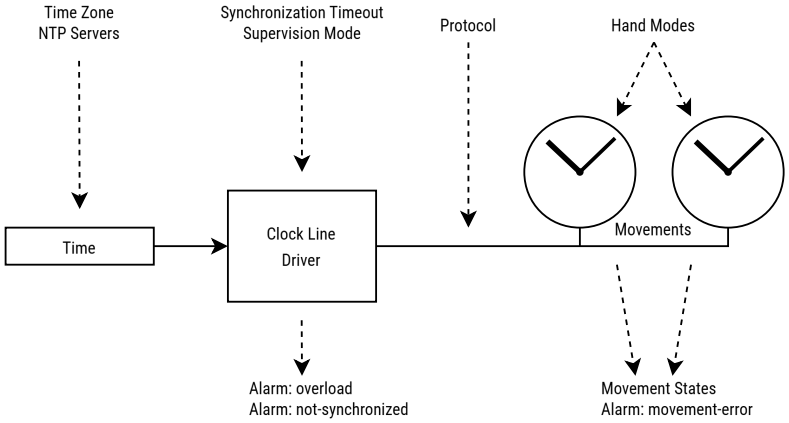
Refer to the next chapter for a detailed description of all available configuration parameters and actions.

Changing network settings may temporarily interrupt the connection. If the device's IP address changes, reconnect using the new IP address.

5 Management and Configuration

5.1. Clock Line

The clock line output is used to power and synchronize up to two MOBALine movements. It provides both time distribution and supervision of the connected movements.



To enable movement supervision and error detection, configure the Supervision parameter according to your setup: use single-sided for one movement or double-sided for two movements. You can also configure the behavior of the minute and second hands.

The Synchronization Timeout defines how long the movements continue running after time synchronization is lost. When this timeout expires, an alarm is raised and the movements are stopped at the 12:00 position.

This timeout operates independently of the NTP synchronization timeout (see NTP client settings). This allows early notification of time synchronization issues (for example, after 1 hour via NTP) while delaying visible clock stoppage (for example, after 24 hours on the clock line).

5.1.1. State

The State section shows the current status of the clock line and the connected movements.

Parameter	Example Values	Description
Alarm	not-synchronized	Alarms currently active on the clock line.
Clock 1, Clock 2	ok	Supervision state of the connected MOBALine movements. Valid states are **not-supervised** , **ok** and **error** . On single-sided configurations, **Clock 2** is always **not-supervised** .

The following alarms may be raised by the clock line:

Alarm	Meaning	Troubleshooting Tips
not-synchronized	The device is not synchronized to a time source, and the clock line may not receive valid time information.	Verify that the NTP client is enabled and configured correctly.
overload	The clock line is overloaded, for example due to a short circuit.	Inspect the physical installation. A damaged cable or movement may be causing a short.
movement-error	One or more movements connected to the line are reporting an error.	Ensure that movement supervision is configured correctly. If **double-sided** is selected, the device expects two connected movements.

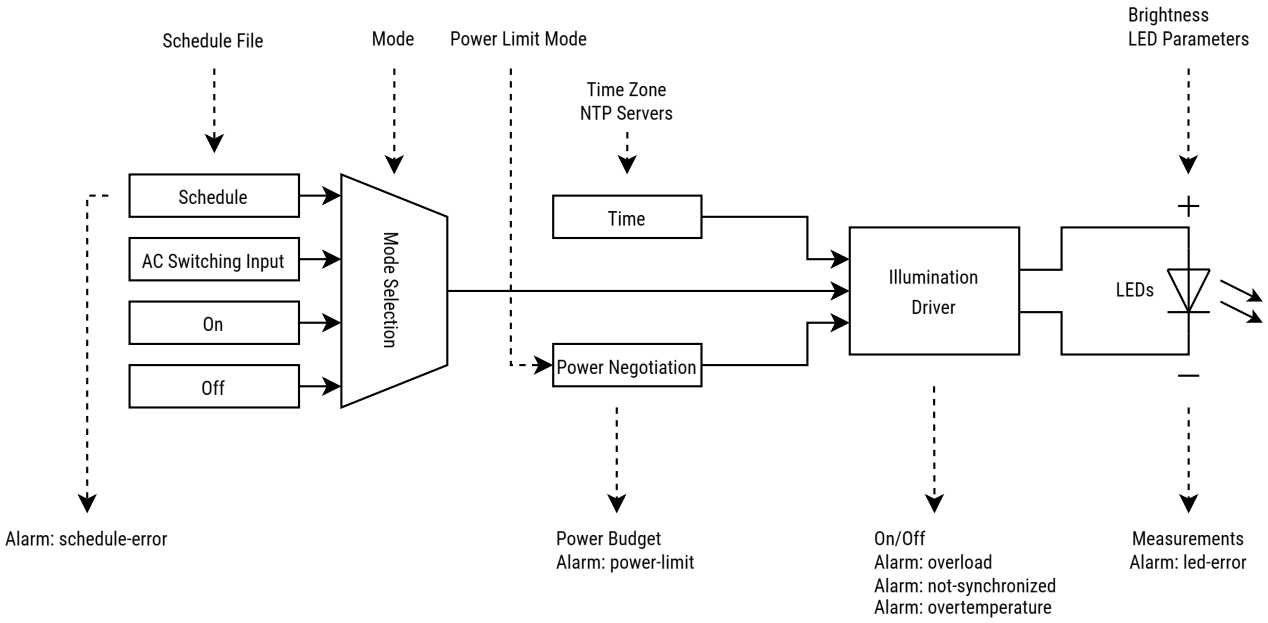
5.1.2. Configuration

Use these settings to control clock line operation, supervision, and movement behavior.

Parameters	Default Value	Description
Protocol	MOBALine	Time code used to power and synchronize the movements. Currently, only MOBALine is supported.
Mode	run	Operating mode of the line: - **run** (normal operation) - **stop** (no output voltage) - **12h** (move to 12h position) - **id** (for movement identification)
Supervision	off	Enables movement supervision. Options are **off** , **single-sided** (one movement), or **double-sided** (two movements).
Second Hand Mode	step	Defines the behavior of the second hand. Options are: - **step** - **continuous** - **continuous-with-stop** - **wobbling** - **wobbling-with-stop**
Minute Hand Mode	continuous	Defines the behavior of the minute hand. Options are: - **continuous** - **step** - **half-step**
Synchronization Timeout	86400	Time in seconds the clock line continues running after time synchronization is lost. When the timeout expires, the movements are moved to the 12:00 position.

5.2. Illumination

The NCC V2 can control and monitor the clock's illumination. Before enabling the illumination output, configure the **Maximum LED Current** and **Maximum LED Voltage** to match the specifications of the connected LED rings. This is essential to prevent damage to the LEDs. Once configured, you can select the desired brightness and operating mode.



Depending on the power source and the LEDs used, the maximum achievable brightness may be limited. This is handled automatically by the Power Limit setting:

- With a mains power connection, the full illumination power is available.
- With PoE+, the required power is automatically requested from the PoE+ switch.
- With PoE, the brightness is automatically limited to the available power budget.

The illumination output is automatically disabled if the internal device temperature exceeds approximately 60 °C.

5.2.1. State

The State section displays the current operating status and measured values of the illumination output.

Parameter	Example Values	Description
Alarm	not-synchronized	Alarms currently reported by the illumination driver.
On	true	Indicates whether the illumination output is currently enabled (true = on, false = off).
LED Voltage	21 V	Voltage measured across the LEDs.
LED Current	0.35 A	Current flowing through the LEDs.
LED Power	7.35 W	Power currently supplied to the LEDs.
Power Budget	13 W	Maximum power available to the illumination driver. The LED power cannot exceed this value.

The following alarms may be reported by the illumination subsystem:

Alarm	Meaning	Troubleshooting Tips
not-synchronized	The device is not synchronized to a time source, so scheduled illumination may not be accurate.	Verify that the NTP client is enabled and configured correctly.
led-error	The LED driver has detected an error, such as an open circuit or short circuit.	Check the LED wiring and verify the configured operating point.
overtemperature	The LED driver has been disabled due to excessive temperature.	Allow the device to cool down and ensure sufficient ventilation.
schedule-error	The configured illumination schedule is invalid.	Verify the schedule content and reload the file without modifications.
power-limit	The available power source cannot support the selected brightness level.	Reduce the brightness or verify the power limit and power source configuration.

5.2.2. Configuration

Use the following parameters to configure illumination behavior and limits.

Parameter	Default Value	Description
Mode	off	Sets the illumination operating mode: - **off** or **on** - **ac** (controlled by the AC input) - **schedule** (controlled by a week program)
Power Limit	auto	Determines how the power limit is applied. - **auto** selects the limit automatically based on the power source and LLDP communication. - **off** disables power limiting.
Brightness	50%	Sets the LED brightness as a percentage (0-100%) of the maximum available power.
Maximum LED Current	350 mA	Maximum output current of the LED driver, corresponding to 100% brightness. Valid range: 1-700 mA. Must match the connected LEDs.
Maximum LED Voltage	22 V	LED voltage at maximum current. The value is rounded up to the nearest volt.
Switching Schedule	N/A	Text-based switching schedule generated by the MOBA Switch Editor. Only active when **Mode** is set to **schedule** .

To avoid damage, the configured LED voltage and current must match the connected hardware. Incorrect settings may damage the LEDs or significantly reduce their lifespan.

Setting the power limit to **off** ignores the limits defined by the PoE standard. This option should only be used if auto does not behave as expected (for example, when using a special PoE injector). While disabling the power limit typically does not damage the device, it may cause a boot loop if the PoE switch detects an overload and cuts power. In this case, recovery is possible by temporarily disconnecting the LEDs from the NCC V2.

5.3. Time

5.3.1. General

The **Timezone** parameter defines the time zone used by the device. All time zones defined in the IANA time zone database are supported. For a complete list, see General FAQ .

5.3.2. NTP

The NTP client is the primary method used to synchronize the device time.

5.3.2.1. State

Parameter	Example Values	Description
Time Source	10.97.100.102	NTP server the device is currently synchronized with.
Reference Time	2026-02-10T09:26:17+0000	Most recently received time value.
Stratum	5	NTP stratum level of the device.
Accuracy	0.000432s	Estimated accuracy of the device time synchronization.
Drift	-0.340 PPM	Estimated clock drift of the device.

The following alarms may be raised by the NTP client:

Alarm	Meaning	Troubleshooting Tips
not-synchronized	The device does not have valid time information.	This alarm is expected immediately after startup and should clear within a few minutes. If it persists, verify the network configuration and the configured NTP servers.
sync-timeout	The device was previously synchronized but has not received new time information within the configured timeout period.	Synchronization was successful at least once but is no longer working. Verify device settings and check for external issues such as network problems or unavailable NTP servers.

5.3.2.2. Configuration

Parameters	Default Value	Description
Enable	true	Enables or disables automatic time synchronization via NTP.
Time Server 1-4	ntp.mobatime.com, ntp-public.mobatime.com, pool.ntp.org	NTP servers used to synchronize the device time.
Synchronization Timeout	3600s	Triggers an alarm if no time update is received within this period.

5.4. Network

The **Network** section configures how the device connects to the network and displays current state. Both IPv4 and IPv6 are supported.

5.4.1. State

The State section provides read-only information about the current network status and traffic statistics.

Parameter	Example Values	Description
IPv4 Address, IPv6 Address	10.97.101.8, fdee::97:101:8	Primary IPv4 and IPv6 addresses assigned to the network interface.
IPv6 DUID	00:01:...:88:bb	DHCPv6 Unique Identifier of the device.
Received Packets, Transmitted Packets	459836, 100655	Total number of network packets received and transmitted.
Received Bytes, Transmitted Bytes	61247116, 86387638	Total number of bytes received and transmitted.
Receive Errors, Transmit Errors	0, 0	Number of errors detected on the Ethernet link.

5.4.2. Configuration

Use these settings to define the device hostname, enable network discovery, and configure IPv4 and IPv6 connectivity.

Parameters	Default Value	Description
General		
Hostname	Product Name + MAC Address	Hostname of the device as used on the network.
Enable SSDP	true	Enables discovery of the device using SSDP / UPnP.
IPv4		
Enable	true	Enable IPv4 communication.
ICMPv4	true	Allows ICMPv4 echo requests (ping).
Use DHCP	true	If enabled, the device obtains its IPv4 address from a DHCP server. If disabled, the configured static values are used.
Static IP	N/A	Static IPv4 address used when DHCPv4 is disabled.
Static Gateway	N/A	IPv4 gateway used when DHCPv4 is disabled.
Static DNS	N/A	IPv4 DNS server used when DHCPv4 is disabled.
IPv6		
Enable	true	Enable IPv6 communication.
ICMPv6	true	Allows ICMPv6 echo requests (ping).
Use DHCP	true	If enabled, the device obtains its IPv6 address from a DHCP server. If disabled, the configured static values are used.
Static IP	N/A	Static IPv6 address used when DHCPv6 is disabled.
Static	N/A	IPv6 gateway used when DHCPv6 is disabled.
Static DNS	N/A	IPv6 DNS server used when DHCPv6 is disabled.

Changing network settings may temporarily interrupt the connection. If the device's IP address changes, reconnect using the new address.

IPv4 and IPv6 cannot be disabled at the same time.

Static IPv4 addresses must be entered using prefix notation (CIDR format). See Network FAQ for information on how prefix lengths correspond to subnet masks.

5.5. Supervision

5.5.1. Log Files

The device stores several types of log files that can be viewed on the **Logs** page in the web interface. These logs provide insight into system status, configuration changes, and user activity.

All log files are stored on the device in encrypted form. For security reasons, logs cannot be deleted or disabled by users and are only cleared during a factory reset. Log files are automatically compressed and rotated when they reach a defined size. For security-critical logs, the two previous log files are retained in compressed form.

5.5.1.1. Alarm Log

The alarm log records all changes in the device's alarm state. Alarms are either set (active) or cleared (inactive). Each entry includes a timestamp, the alarm identifier, and its current state.

Event	Example Log Message
System alarm set	2025-07-15T13:41:47.017909+00:00: alarm: 'system-restarted' set.
System alarm cleared	2025-07-15T13:42:23.830722+00:00: alarm: 'system-restarted' cleared.

5.5.1.2. Audit Log

The audit log tracks all user actions and configuration changes. This includes parameter modifications, authentication attempts, and administrative actions such as reboots, firmware updates, or factory resets.

Event	Example Log Message
Parameter change	2025-08-08T14:10:52.919901+00:00: audit: User 'maintainer' modified parameter '/ntp/enable'.
Failed login attempt	2025-08-08T14:11:19.000777+00:00: audit: User 'admin' failed to authenticate.
Initiated reboot	2025-08-08T14:15:12.157051+00:00: audit: User 'admin' started reboot.
Password change	2025-08-08T14:10:50.982835+00:00: audit: User 'maintainer' changed their password.
User management	2025-08-08T13:59:05.967640+00:00: audit: User 'maintainer' was enabled by 'admin'.
Started firmware update	2025-08-08T14:15:10.517462+00:00: audit: User 'admin' started firmware update.
Initiated factory reset	2025-08-08T14:15:14.200724+00:00: audit: User 'admin' started factory reset.

5.5.1.3. Web Access Log

The web access log records all HTTP requests handled by the device's web server.

Example Log Messages
2026-02-10T14:05:39.660362+00:00: nginx_access: 10.97.100.1 admin "GET /restconf/data HTTP/1.1" 200 15749
2026-02-10T14:06:08.019087+00:00: nginx_access: 10.97.100.20 admin "GET /restconf/data/ HTTP/2.0" 200 15728

Each log entry contains, in order: **timestamp** , **log source** , **client IP address** , **user** , **request method and URL** , **HTTP status code** , and **response size** .

5.5.1.4. Other

Additional files are available on the device, such as open-source license information or software self-test results. These files are provided for reference and typically do not require monitoring during normal operation.

5.5.2. Syslog

The device can forward log messages to a central server using the syslog protocol. To enable log forwarding, set **Enable** to **true** and configure the destination Server. The server can be specified as either an IP address or a hostname.

The following table provides an overview of the available configuration options.

Parameters	Default Value	Description
Enable	false	Enables or disables forwarding of log messages to a remote syslog server.
Protocol	UDP	Network protocol used to send log messages. Supported values are **UDP** and **TCP** .
Server, Port	0.0.0.0:514	IP address or hostname and port of the remote syslog server that receives the log messages.
Alarm Notifications	true	Sends log messages when alarms are raised or cleared.
Audit Log	false	Forwards audit log entries, such as configuration changes and login attempts.
Periodic Heartbeat	false	Periodically sends a status message containing the current device state.
Debug	false	Forwards the full debug log to the syslog server. Intended for remote troubleshooting.

The debug log is intended for troubleshooting and customer support and should normally remain disabled. It produces a high volume of messages, has no strictly defined format, and may include irrelevant or misleading entries. Error messages do not necessarily indicate an actual malfunction.

5.5.3. SNMP

The device supports discovery and monitoring using the Simple Network Management Protocol (SNMP). If SNMP is not required, it is recommended to disable it to reduce the attack surface.

A device-specific MIB file describing the alarm states can be downloaded from the website. In addition, standard SNMP MIBs are supported.

SNMPv2c does not use any encryption and is simple to set up. Once both sides are configured with the same community string, the protocol is ready to use. SNMPv3 offers authentication and encryption of traffic (typically called “auth” and “priv”). When using SNMPv3, user credentials must be created before access can be granted.

5.5.3.1. Read Access

Use the following settings to configure SNMP read access to the device.

Parameters	Default Value	Description
Protocol	v2c	SNMP version used for read access. Supported values are **off** , **v2c** and **v3** .
System Location, System Contact	Unknown	Informational fields reported by the device and displayed in network management systems.
Community String	public	SNMPv2c community string used for read access.
Security Level	N/A	Security level for SNMPv3 read access. Supported values are **no-auth-no-priv** (not recommended), **auth-no-priv** and **auth-priv** .
SNMPv3 User	N/A	Name of the SNMPv3 user used for read access.

5.5.3.2. Traps

SNMP traps are sent periodically and whenever an alarm becomes active or is cleared.

Parameters	Default Value	Description
Protocol	v2c	SNMP version used for traps. Supported values are **off** , **v2c** and **v3** .
SNMP Manager, Port	0.0.0.0:162	Address and port of the SNMP manager that receives the traps.
Interval	60s	Periodic trap interval. Set to 0 to send traps only when alarms change.
Community String	public	SNMPv2c community string used for traps.
Security Level	N/A	Security level for SNMPv3 trap delivery. Supported values are **no-auth-no-priv** (not recommended), **auth-no-priv** and **auth-priv** .
SNMPv3 User	N/A	Name of the SNMPv3 user used for trap delivery.

5.5.3.3. SNMPv3 User Management

The device provides basic user management for SNMPv3. Up to five SNMPv3 users can be configured simultaneously.

- **Add User** : Creates a new SNMPv3 user by specifying a username, authentication algorithm and password, and a privacy algorithm and password.
- **Clear Users** : Removes all SNMPv3 users from the device.

Configured users are displayed in the list of usernames. Changes may take a few seconds to become active. For security reasons, passwords are not stored in plain text and cannot be viewed or recovered after creation.

5.6. Access Control

The device can be fully configured and managed through the RESTCONF API. SNMP is available for monitoring purposes only and provides read-only access to device status information.

The device supports multiple user accounts with different permission levels. By default, only the admin account is enabled. It is preconfigured with a unique password printed on the device label.

If access to the admin account is lost (for example, due to a changed and forgotten password), the device can only be recovered by performing a factory reset using the physical reset button. A factory reset deletes all configuration settings and stored user data. For security reasons, the reset button can be disabled. If it is disabled and access credentials are lost, the device cannot be recovered. In such cases, it is impossible - even for the manufacturer - to access any of the stored data.

5.6.1. Roles

The RESTCONF interface supports the following user roles and associated permissions:

Action	admin	maintainer	operator	viewer
Enable / Disable Accounts	✓	✗	✗	✗
Set All Passwords	✓	✗	✗	✗
Change Own Password	✓	✓	✓	✓
Read State and Settings	✓	✓	✓	✓
Modify Device I/O Settings	✓	✓	✓	✗
Modify All Settings	✓	✓	✗	✗
Install Firmware Updates	✓	✓	✗	✗
Reboot	✓	✓	✓	✗
Factory Reset	✓	✗	✗	✗
Read Logs	✓	✓	✓	✓
Create Backups	✓	✓	✗	✗
Apply Backups	✓	✗	✗	✗

5.6.2. Management

User accounts are managed in the **User Management** section of the **Maintenance** page. The following actions are available:

- **Set Password** : Changes the password of the currently logged-in user.
- **Enable User Account** : Allows the admin to enable another user account and assign an initial password. The user can change this password after logging in. This function can also be used to reset a forgotten password.
- **Disable User Account** : Disables a specific user account, preventing the user from logging in and accessing the device.

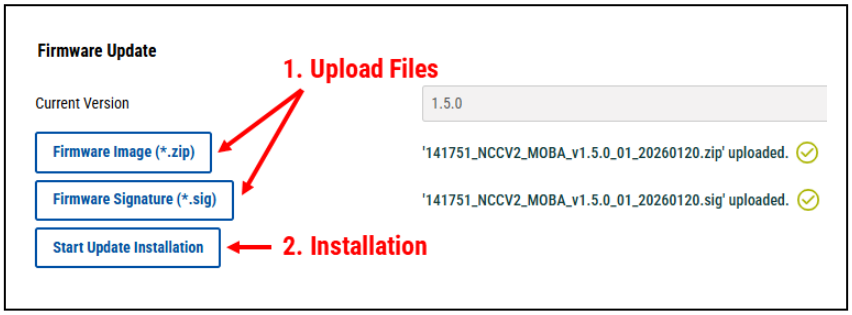
5.7. Maintenance

5.7.1. Firmware Update

Each firmware update consists of two files that must both be uploaded to the device:

- The firmware image (`.zip`)
- The signature (`.sig`)

To begin the update, navigate to the **Maintenance** tab and use the **File Upload** buttons to select the files from your computer. When each file is uploaded successfully, a green checkmark appears next to it. Once both files are uploaded, click **Start Update Installation** to begin the installation process.



The update process runs automatically. If the installation is successful, the device will reboot up to two times to complete the update. If an error occurs, an alarm is raised, and the device continues operating with the currently installed firmware version.

During a firmware update, do **not** reboot or cut power to the device.

The device verifies the integrity of the firmware update. Installation will fail if the firmware image has been modified. For instructions on manual verification, see Security FAQ .

For security reasons, installation of older firmware versions is not permitted (anti-rollback protection). The device will reject such updates.

5.7.2. Rebooting

Rebooting the device takes approximately one minute. A reboot can be used to restore the device to a clean operational state or to immediately apply certain changes that cannot easily be triggered externally. For example, rebooting forces the device to fully reinitialize its network interface, allowing it to immediately respond to changes in the network infrastructure (such as a modified IP address assignment from a DHCP server). Most configuration changes do not require a reboot to take effect.

Reboots are typically performed manually (for example, during troubleshooting) or automatically as part of another process (such as a firmware update).

5.7.3. Alarm Testing

The **Dummy Error** function provides a simple way to test supervision and alarm handling settings. This alarm can be manually enabled or disabled from the **Maintenance** page.

When enabled, the device treats the dummy error like a real fault condition. It is logged accordingly and reported through all configured notification mechanisms (for example, syslog).

The dummy error is a configuration parameter. It persists across reboots and is included in configuration backups. Once enabled, it remains active until it is manually disabled.

5.7.4. Factory Reset

A factory reset restores the device to its initial state and permanently deletes all user data, including configuration settings and log files.

A factory reset can be initiated in one of the following ways:

- Digitally, by an authenticated admin user
- Physically, using the reset button on the device

Factory resets via the physical reset button can be disabled using the **Allow Unauthenticated Factory Reset** option. In this context, *unauthenticated* means that anyone with physical access to the device can press the reset button and trigger a factory reset. For additional security considerations, refer to the Cyber Security chapter.

Only disable the factory reset button after verifying that the admin login is functional and the password is securely stored (for example, in a password manager). If the reset button is disabled and the admin credentials are lost, the device cannot be accessed or recovered, and all stored information will remain permanently inaccessible.

5.7.5. SSL Certificates

When accessing the device for the first time, your browser may display a security warning because the default TLS certificate is not trusted. To remove this warning, you can upload a custom TLS certificate issued by a trusted authority within your organization.

Certificates can be uploaded from the **Maintenance** page. You must provide:

- The TLS certificate (in PEM format)
- The corresponding private key (in PEM format)

You may either paste the contents directly into the provided text fields or upload the files from your computer. After a successful upload, the device will use the new certificate for all subsequent HTTPS connections.

For optimal performance, the use of Elliptic Curve Digital Signature Algorithm (ECDSA) certificates is recommended. ECDSA certificates provide comparable security to RSA certificates while requiring less computational overhead.

The device validates all uploaded certificates and will reject certificates that are malformed or that use unsupported cryptographic algorithms.

5.7.6. Backups

Backups allow you to restore the device configuration at a later time. For security reasons, backup files are encrypted using a user-defined password. This password is required when restoring the backup.

A backup includes:

- Device configuration
- Enabled user accounts and their credentials

A backup does **not** include log files or other runtime-generated data.

Create a Backup

1. Click **Create Backup** .
2. Enter an encryption password.
3. The encrypted backup file is automatically downloaded to your computer.

Restore from a Backup

1. Upload the backup file.
2. Click **Restore From Backup** .
3. Enter the correct decryption password.
4. The device restores the configuration and reboots automatically.

5.7.7. Support Package

A support package contains diagnostic and troubleshooting information that can be shared with customer support. The package is encrypted and can only be accessed using the specified encryption password.

Create a Support Package

1. Click **Create Support Package** .
2. Enter an encryption password.
3. The encrypted package is automatically created and downloaded to your computer.
4. Provide the package to customer support together with the decryption password.

The support package may include:

- Device configuration
- Log files
- Self-test results
- Network and routing information
- Salted password hashes of all enabled user accounts

The support package does not include highly sensitive information such as TLS/SSL private keys.

6 Cyber Security

Adhering to security best practices is essential for building a secure and reliable system. An effective security approach needs to consider all components of the infrastructure.

Smart network clocks and similar devices deserve particular attention. They are often installed in publicly accessible or remote locations and may be more exposed to physical or network-based attacks than core infrastructure components.

This chapter outlines common threat scenarios, explains how the device mitigates risks by design, and provides recommendations for additional protective measures.

Not all cybersecurity threats result from malicious attacks. For example, a forgotten password or an incorrectly configured output can also compromise system availability or security.

6.1. Protocols and Used Network Ports

The following table lists the network protocols and ports used by the device.

Port	Transport	Protocol	Can be Disabled	Comment
80	TCP	HTTP	✗	Redirects incoming requests to HTTPS. Not used for other services.
443	TCP	HTTPS	✗	Web interface, RESTCONF API, and file uploads.
123	UDP	NTP	✓	Time synchronization.
161, 162	UDP	SNMP	✓	SNMP read access (GET) and trap transmission.
1900	UDP, TCP	SSDP	✓	Service discovery.
1901	TCP	UPnP	✓	Provides device information for automatic discovery (e.g., Windows File Explorer).
57, 68	UDP	DHCPv4	✓	Automatic IPv4 address assignment.
546	UDP	DHCPv6	✓	Automatic IPv6 address assignment.
53, 853	UDP, TCP	DNS	✗	Name resolution
-	-	ICMP, ICMPv6	✓	Network diagnostics and error reporting.

Ports used by external services may differ from their default values (for example, syslog may use a port other than 514).

6.2. Security Checklist

The security of an installation can be improved by taking the following measures.

Many of these measures restrict functionality in order to improve security. For example, disabling ICMP prevents the device from responding to ping requests. While this may make troubleshooting more difficult for administrators, it also reduces network visibility for potential attackers.

Security always involves balancing operational convenience against risk exposure.

6.2.1. Reduce the Attack Surface

Minimize the number of accessible services and entry points:

- Disable unused network protocols (e.g., ICMPv4, ICMPv6, SSDP, SNMP, Syslog).
- Install firmware and security updates as soon as they become available.
- Protect physical network ports from unauthorized access.
- Replace the default TLS certificate with a trusted certificate issued by your organization.
- Use strong, unique passwords for all user accounts.
- Disable unused user accounts.
- Disable the physical factory reset button if appropriate.

6.2.2. Network Segmentation and Access Control

Limit the device's communication to only what is strictly necessary:

- Restrict outbound network access (e.g., allow communication only with required NTP servers or management systems).
- Do not expose the device directly to the public internet.
- Avoid configuring port forwarding to the device.
- Place the device in a dedicated VLAN or protected network segment where possible.

6.2.3. Monitoring and Incident Response

Ensure that suspicious activity can be detected and addressed quickly:

- Enable logging and forward logs to a central syslog server.
- Monitor network traffic for unusual behavior.
- Regularly review device logs and system status.
- Test supervision and alarm mechanisms (e.g., using the dummy error function).

6.3. Scenarios

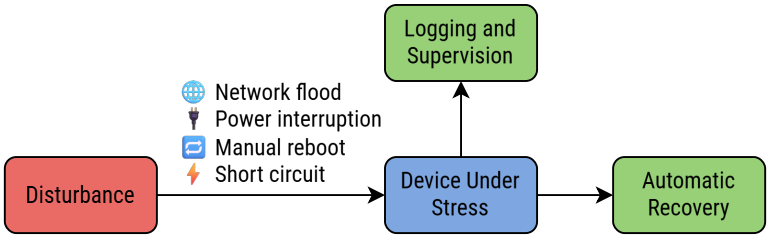
The following key threat scenarios were considered during the development of the device. For each scenario, a brief description is provided along with:

- The mitigation measures implemented in the device hardware and software design
- Recommended actions to take if suspicious activity or an attack is detected

This structured approach helps ensure that potential risks are understood and that appropriate preventive and corrective measures are in place.

6.3.1. Denial of Service (Temporary)

This scenario covers situations in which the device temporarily stops operating normally but does not leak sensitive information and does not suffer permanent damage. The effects are noticeable (for example, a clock stops or displays an incorrect time), but normal operation resumes automatically once the disturbance ends.



Realistic attack vectors include:

- Flooding the device with excessive network traffic
- Triggering a manual reboot (if physical access is available)
- Interrupting the power supply
- Overloading or short-circuiting a physical output

6.3.1.1. Implemented Measures

The primary defense mechanisms against temporary denial-of-service conditions are logging, supervision, and automatic recovery features.

- The device logs significant events (e.g., reboots) and abnormal conditions (e.g., high CPU load, short circuits, or hardware faults).
- Supervision mechanisms allow these events to be reported to monitoring systems.
- Built-in reliability features are designed to ensure that the device automatically returns to normal operation after transient faults or abnormal operating conditions.

These measures enable administrators to determine when an incident occurred and assess its impact.

6.3.1.2. Recommended Recovery Actions

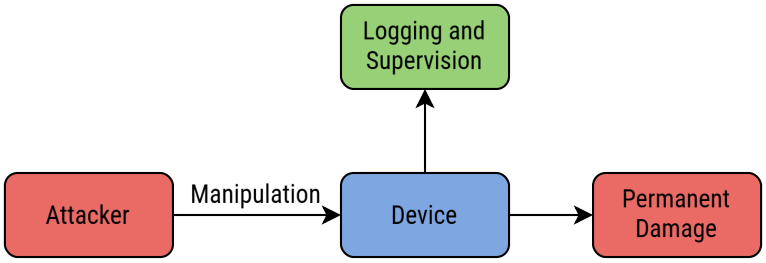
If a denial-of-service incident is suspected:

- Remove the attacker or the source of disruption from the network or physical environment.
- Identify the scope and duration of the incident.
- Verify that the device has returned to normal operation.
- Review logs and monitoring data for anomalies.
- Report any newly discovered vulnerabilities or attack patterns to the manufacturer.

This approach ensures both immediate recovery and continuous improvement of system security.

6.3.2. Denial of Service (Permanent)

A permanent denial-of-service occurs when an attacker destroys or irreversibly disables the device.



Possible causes include

- **Mechanical damage** : Physical damage that renders the device inoperable.
- **Electrical damage** : Intentional or accidental misuse (e.g., overvoltage, short circuits, reverse polarity) that damages internal components.
- **Theft** : Physical removal of the device from its installation site.
- **Misconfiguration or lost credentials** : Incorrect configuration or forgotten passwords that prevent access.
- **Software vulnerabilities** : Sophisticated attacks that leave the device in an unusable state.

6.3.2.1. Implemented Measures

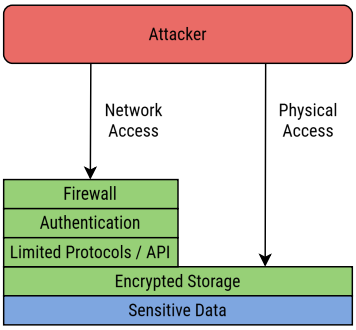
- **Continuous monitoring** : Dedicated “heartbeat” mechanisms (e.g., via syslog or SNMP) indicate whether the device is operating normally.
- **Electrical protection** : Inputs and outputs are protected against common faults such as overload.
- **Tamper detection** : In certain cases, the device intentionally stops operating if severe tampering is detected (e.g., installation of unofficial software; Secure Boot enforcement).
- **Reliability safeguards** : Built-in mechanisms prevent common configuration errors from causing permanent damage. For example, the device can automatically recover from failed firmware updates and reject invalid network settings.

6.3.2.2. Recommended Recovery Actions

- Analyze the incident and ensure there is no ongoing hazard (e.g., electrical damage).
- Attempt recovery where possible:
  - Inspect and remove any physical issues (e.g., damaged or shorted wiring).
  - Perform a factory reset to eliminate potential misconfigurations.
- If recovery is not possible, return the device to the manufacturer for further analysis.

6.3.3. Data Extraction

The goal of a data extraction attack is to gain unauthorized access to sensitive information stored on the device.



Data of interest may include:

- Login credentials (e.g., passwords)
- Log files (e.g., usage patterns, potential vulnerabilities)
- Device configuration and operational state
- Private keys and certificates
- Environmental information (e.g., network topology)

Possible attack methods include:

- Password guessing or brute-force attacks
- Exploitation of insecure protocols or configuration weaknesses
- Physical access to analyze memory contents
- Social engineering

6.3.3.1. Implemented Measures

- **Encryption at rest** : User data (configuration, logs, TLS certificates, etc.) is fully encrypted when the device is powered off.
- **Secure credential storage** : Passwords are never stored in plain text.
- **Software protection** : Firmware is encrypted to hinder reverse engineering and data extraction.
- **Access control** : Device access requires authentication.
- **Protocol control** : Optional protocols (e.g., ICMP, SSDP) can be disabled if not required.

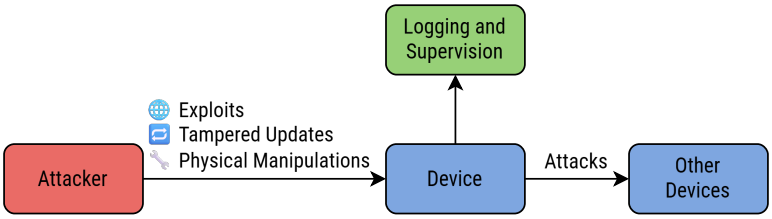
6.3.3.2. Recommended Recovery Actions

If data extraction is suspected:

- Assess the scope of the incident and identify compromised data.
- Mitigate further risk:
  - Revoke affected TLS certificates.
  - Change all potentially compromised passwords.
- Report the incident to the manufacturer.

6.3.4. Device Takeover

Device takeover refers to an attacker gaining control of the device and potentially executing malicious code.



Such attacks may aim to:

- Use the device as an entry point for broader network attacks.
- Enlist the device in a botnet to conduct distributed attacks.

Possible attack vectors include:

- Installing a tampered software update
- Exploiting software vulnerabilities
- Replacing the device entirely (e.g., unplugging it and installing a malicious substitute) when physical access is available

6.3.4.1. Implemented Measures

- **Security updates** : Known vulnerabilities are addressed through regular security updates. These should be installed promptly.
- **Defense in depth** : Multiple layers of protection are implemented:
  - **Secure software updates** : Only authenticated and untampered updates can be installed.
  - **Secure Boot** : If unauthorized software is detected (e.g., due to physical tampering), the device will not start.
  - **Firewall** : Unauthorized or unexpected connections are rejected.
- **Monitoring and logging** : Logs (e.g., web server access logs) provide evidence of potential tampering attempts.

6.3.4.2. Recommended Recovery Actions

- Immediately disconnect the device from the network.
- Analyze the system and assess the extent of the compromise.
- Revoke potentially affected TLS certificates and change all passwords.
- Report the incident to the manufacturer.

7 Frequently Asked Questions

The logout button doesn't work.

The logout function may not behave consistently across all web browsers. For example, some browsers (such as Firefox) may cache authentication credentials and automatically log the user in again after logout. In such cases, the saved credentials may need to be manually cleared.

Parts of the webinterface are in the wrong language.

Some elements of the web interface are automatically localized by the web browser. This may affect number formatting (e.g., decimal separators) and some browser-generated error messages (e.g., "value out of range").

How can the integrity of a firmware update be checked?

The device automatically rejects firmware updates that were tampered with. It does this by checking the uploaded image against the provided signature and a pre-shared public key. Using OpenSSL, it is possible to run this authenticity check on any computer. The check requires that the public key (*.pub*) is obtained from a trusted source:

```
# Example with authentic firmware
user@computer ~ $ openssl dgst -sha512 \
    -signature Firmware.sig \
    -verify Firmware.pub \
    Firmware.zip
Verified OK

# Example with manipulated firmware
user@computer ~ $ openssl dgst -sha512 \
    -signature Firmware.sig \
    -verify Firmware.pub \
    Firmware.zip
Verification failure
```

What are the supported time zones?

All current time zones defined in the IANA time zone database version 2025a are supported.

```
Abidjan, Accra, Addis_Ababa, Algiers, Asmara, Asmera, Bamako, Bangui, Banjul, Bissau,
Blantyre, Brazzaville, Bujumbura, Cairo, Casablanca, Ceuta, Conakry, Dakar, Dar_es_Salaam,
Djibouti, Douala, El_Aaiun, Freetown, Gaborone, Harare, Johannesburg, Juba, Kampala, Khartoum,
Kigali, Kinshasa, Lagos, Libreville, Lome, Luanda, Lubumbashi, Lusaka, Malabo, Maputo, Maseru,
Mbabane, Mogadishu, Monrovia, Nairobi, Ndjamena, Niamey, Nouakchott, Ouagadougou, Porto-Novo,
Sao_Tome, Timbuktu, Tripoli, Tunis, Windhoek, Adak, Anchorage, Anguilla, Antigua, Araguaina,
Argentina/Buenos_Aires, Argentina/Catamarca, Argentina/ComodRivadavia, Argentina/Cordoba,
Argentina/Jujuy, Argentina/La_Rioja, Argentina/Mendoza, Argentina/Rio_Gallegos, Argentina/
Salta, Argentina/San_Juan, Argentina/San_Luis, Argentina/Tucuman, Argentina/Ushuaia, Aruba,
Asuncion, Atikokan, Atka, Bahia, Bahia_Banderas, Barbados, Belem, Belize, Blanc-Sablon,
Boa_Vista, Bogota, Boise, Buenos_Aires, Cambridge_Bay, Campo_Grande, Cancun, Caracas,
Catamarca, Cayenne, Cayman, Chicago, Chihuahua, Ciudad_Juarez, Coral_Harbour, Cordoba,
Costa_Rica, Creston, Cuiaba, Curacao, Danmarkshavn, Dawson, Dawson_Creek, Denver, Detroit,
Dominica, Edmonton, Eirunepe, El_Salvador, Ensenada, Fort_Nelson, Fort_Wayne, Fortaleza,
Glace_Bay, Godthab, Goose_Bay, Grand_Turk, Grenada, Guadeloupe, Guatemala, Guayaquil, Guyana,
Halifax, Havana, Hermosillo, Indiana/Indianapolis, Indiana/Knox, Indiana/Marengo, Indiana/
Petersburg, Indiana/Tell_City, Indiana/Vevay, Indiana/Vincennes, Indiana/Winamac,
Indianapolis, Inuvik, Iqaluit, Jamaica, Jujuy, Juneau, Kentucky/Louisville, Kentucky/
Monticello, Knox_IN, Kralendijk, La_Paz, Lima, Los_Angeles, Louisville, Lower_Princes, Maceio,
Managua, Manaus, Marigot, Martinique, Matamoros, Mazatlan, Mendoza, Menominee, Merida,
Metlakatla, Mexico_City, Miquelon, Moncton, Monterrey, Montevideo, Montreal, Montserrat,
Nassau, New_York, Nipigon, Nome, Noronha, North_Dakota/Beulah, North_Dakota/Center,
North_Dakota/New_Salem, Nuuk, Ojinaga, Panama, Pangnirtung, Paramaribo, Phoenix,
Port-au-Prince, Port_of_Spain, Porto_Acre, Porto_Velho, Puerto_Rico, Punta_Arenas,
Rainy_River, Rankin_Inlet, Recife, Regina, Resolute, Rio_Branco, Rosario, Santa_Isabel,
Santarem, Santiago, Santo_Domingo, Sao_Paulo, Scoresbysund, Shiprock, Sitka, St_Barthelemy,
St_Johns, St_Kitts, St_Lucia, St_Thomas, St_Vincent, Swift_Current, Tegucigalpa, Thule,
Thunder_Bay, Tijuana, Toronto, Tortola, Vancouver, Virgin, Whitehorse, Winnipeg, Yakutat,
Yellowknife, Casey, Davis, DumontDUrville, Macquarie, Mawson, McMurdo, Palmer, Rothera,
South_Pole, Syowa, Troll, Vostok, Longyearbyen, Aden, Almaty, Amman, Anadyr, Aqtau, Aqtobe,
Ashgabat, Ashkhabad, Atyrau, Baghdad, Bahrain, Baku, Bangkok, Barnaul, Beirut, Bishkek,
Brunei, Calcutta, Chita, Choibalsan, Chongqing, Chungking, Colombo, Dacca, Damascus, Dhaka,
Dili, Dubai, Dushanbe, Famagusta, Gaza, Harbin, Hebron, Ho_Chi_Minh, Hong_Kong, Hovd, Irkutsk,
Istanbul, Jakarta, Jayapura, Jerusalem, Kabul, Kamchatka, Karachi, Kashgar, Kathmandu,
Katmandu, Khandyga, Kolkata, Krasnoyarsk, Kuala_Lumpur, Kuching, Kuwait, Macao, Macau,
Magadan, Makassar, Manila, Muscat, Nicosia, Novokuznetsk, Novosibirsk, Omsk, Oral, Phnom_Penh,
Pontianak, Pyongyang, Qatar, Qostanay, Qyzylorda, Rangoon, Riyadh, Saigon, Sakhalin,
Samarkand, Seoul, Shanghai, Singapore, Srednekolymsk, Taipei, Tashkent, Tbilisi, Tehran,
Tel_Aviv, Thimbu, Thimphu, Tokyo, Tomsk, Ujung_Pandang, Ulaanbaatar, Ulan_Bator, Urumqi,
Ust-Nera, Vientiane, Vladivostok, Yakutsk, Yangon, Yekaterinburg, Yerevan, Azores, Bermuda,
Canary, Cape_Verde, Faeroe, Faroe, Jan_Mayen, Madeira, Reykjavik, South_Georgia, St_Helena,
Stanley, ACT, Adelaide, Brisbane, Broken_Hill, Canberra, Currie, Darwin, Eucla, Hobart, LHI,
Lindeman, Lord_Howe, Melbourne, NSW, North, Perth, Queensland, South, Sydney, Tasmania,
Victoria, West, Yancowinna, Acre, DeNoronha, East, Atlantic, Central, Eastern, Mountain,
Newfoundland, Pacific, Saskatchewan, Yukon, Chile/Continental, Chile/EasterIsland, Greenwich,
UCT, UTC, Universal, Zulu, Amsterdam, Andorra, Astrakhan, Athens, Belfast, Belgrade, Berlin,
Bratislava, Brussels, Bucharest, Budapest, Busingen, Chisinau, Copenhagen, Dublin, Gibraltar,
Guernsey, Helsinki, Isle_of_Man, Jersey, Kaliningrad, Kiev, Kirov, Kyiv, Lisbon, Ljubljana,
London, Luxembourg, Madrid, Malta, Mariehamn, Minsk, Monaco, Moscow, Oslo, Paris, Podgorica,
Prague, Riga, Rome, Samara, San_Marino, Sarajevo, Saratov, Simferopol, Skopje, Sofia,
Stockholm, Tallinn, Tirane, Tiraspol, Ulyanovsk, Uzhgorod, Vaduz, Vatican, Vienna, Vilnius,
Volgograd, Warsaw, Zagreb, Zaporozhye, Zurich, Antananarivo, Chagos, Christmas, Cocos, Comoro,
Kerguelen, Mahe, Maldives, Mauritius, Mayotte, Reunion, Mexico/BajaNorte, Mexico/BajaSur,
Mexico/General, Apia, Auckland, Bougainville, Chatham, Chuuk, Easter, Efate, Enderbury,
Fakaofo, Fiji, Funafuti, Galapagos, Gambier, Guadalcanal, Guam, Honolulu, Johnston, Kanton,
Kiritimati, Kosrae, Kwajalein, Majuro, Marquesas, Midway, Nauru, Niue, Norfolk, Noumea,
Pago_Pago, Palau, Pitcairn, Pohnpei, Ponape, Port_Moresby, Rarotonga, Saipan, Samoa, Tahiti,
Tarawa, Tongatapu, Truk, Wake, Wallis, Yap, Alaska, Aleutian, Arizona, US/Central,
East-Indiana, US/Eastern, Hawaii, Indiana-Starke, Michigan, CET, CST6CDT, Cuba, EET, EST,
EST5EDT, Egypt, Eire, Factory, GB, GB-Eire, GMT, GMT+0, GMT-0, GMT0, HST, Hongkong, Iceland,
Iran, Israel, Japan, Libya, MET, MST, MST7MDT, NZ, NZ-CHAT, Navajo, PRC, PST8PDT, Poland,
Portugal, ROC, ROK, Turkey, W-SU, WET
```

Is it possible to access the device's API without the webinterface?

The device can be fully configured and monitored through its RESTCONF API. This is the same API used by the web interface and allows for easy integration into automation scripts and network management systems.

All API requests require HTTP Basic Authentication with a valid user account. When using a self-signed certificate, you may need to use an option like `--insecure` with tools like `curl` to bypass certificate validation (do not use this option in production!).

Example: Reading Settings and Status

```
# Request the NTP configuration and state from the device:
user@computer ~ $ curl -X GET -u "admin:password" \
    "https://192.168.0.39/restconf/data/network-slave-clock-common:ntp"
```

```
// Example Response
{
  "network-slave-clock-common:ntp": {
    "enable": true,
    "server1": "ntp.mobatime.com",
    "server2": "ntp-public.mobatime.com",
    "server3": "pool.ntp.org",
    "server4": "pool.ntp.org",
    "synchronized": true,
    "drift": "-0.283",
    "accuracy": "0.005249",
    "stratum": 3
  }
}
```

Example: Changing Configuration Parameters

```
# Send a PATCH request with a JSON payload containing the parameters you wish to change.
user@computer ~ $ curl -X PATCH -u "admin:password" \
  -H "Content-Type: application/yang-data+json" \
  -d '{"network-slave-clock-common:ntp": {"enable": false}}' \
  "https://192.168.0.39/restconf/data/network-slave-clock-common:ntp"
```

Example: Executing Commands

```
# Commands (RPCs) are executed by sending a POST request to the operations endpoint.
# Reboot the device
user@computer ~ $ curl -X POST -u "admin:password" \
  "https://192.168.0.39/restconf/operations/network-slave-clock-common:reboot"

# Change the admin password
user@computer ~ $ curl -X POST -u "admin:password" \
  -H "Content-Type: application/yang-data+json" \
  -d '{"network-slave-clock-common:input": {"password": "my_new_password"}}' \
  "https://192.168.0.39/restconf/operations/network-slave-clock-common:set-own-password"
```

How does the IPv4 prefix work? How can I set the IPv4 network mask?

The prefix notation is fully equivalent to classical network masks. See the following table for details:

Class	Prefix	Network mask	Usable hosts per subnet
-	/1	128.0.0.0	2,147,483,646
-	/2	192.0.0.0	1,073,741,822
-	/3	224.0.0.0	536,870,910
-	/4	240.0.0.0	268,435,454
-	/5	248.0.0.0	134,217,726
-	/6	252.0.0.0	67,108,862
-	/7	254.0.0.0	33,554,430
A	/8	255.0.0.0	16,777,214
A	/9	255.128.0.0	8,388,606
A	/10	255.192.0.0	4,194,302
A	/11	255.224.0.0	2,097,150
A	/12	255.240.0.0	1,048,574
A	/13	255.248.0.0	524,286
A	/14	255.252.0.0	262,142
A	/15	255.254.0.0	131,070
B	/16	255.255.0.0	65,534
B	/17	255.255.128.0	32,766
B	/18	255.255.192.0	16,382
B	/19	255.255.224.0	8,190
B	/20	255.255.240.0	4,094
B	/21	255.255.248.0	2,046
B	/22	255.255.252.0	1,022
B	/23	255.255.254.0	510
C	/24	255.255.255.0	254
C	/25	255.255.255.128	126
C	/26	255.255.255.192	62
C	/27	255.255.255.224	30
C	/28	255.255.255.240	14
C	/29	255.255.255.248	6
C	/30	255.255.255.252	2
C	/31	255.255.255.254	0

How to set a link-local IP address on Windows?

If the device is being provisioned on a network without a DHCP server, a link-local IP address is required. On Windows systems, a link-local address is assigned automatically. If connectivity issues occur, follow the steps below to eliminate common configuration problems:

1. **Enable DHCP on the network interface.**
   Since no DHCP server is present, the interface will automatically assign itself a link-local address.
2. **Reconnect the network cable.**
   Disconnect and reconnect the Ethernet cable to ensure the interface initializes with the updated settings.
3. **Disable other network interfaces.**
   Temporarily disable WLAN and any additional LAN interfaces. This prevents routing conflicts when multiple interfaces have link-local addresses.
4. **Verify the IP address assignment.**
   Open a command prompt and run `ipconfig` . Confirm that the interface has an address in the link-local range:
   - IPv4: 169.254.x.x
   - IPv6: fe80::…

```
C:\Users\...> ipconfig
...
Ethernet adapter:
...
Link-local IPv6 Address . . . . . : fe80::dfb4:...    <--- IPv6 link-local address
Autoconfiguration IPv4 Address. . : 169.254.95.33     <--- IPv4 link-local address
Subnet Mask . . . . . . . . . . . : 255.255.0.0
...
```

The device does not appear in Windows Explorer

The device announces itself using SSDP / UPnP. It will only appear in Windows Explorer if the following conditions are met:

1. The device and the computer can communicate (compatible network configuration).
2. Windows Network Discovery is enabled and active on the relevant network interface.

If the device is not displayed, follow these troubleshooting steps:

1. **Verify IP configuration.**
   Ensure the Windows computer has an IP address in the same subnet as the device. If no DHCP server is available, a link-local address is required for initial discovery.
2. **Disconnect other network interfaces.**
   Temporarily disable WLAN and any additional LAN connections to avoid routing conflicts.
3. **Disable special network settings.**
   Temporarily turn off non-default settings such as metered connection, data limits, or additional authentication mechanisms.
4. **Enable Network Discovery.**
   Check the current network profile type (Public, Private, or Domain) and enable Network Discovery for that specific profile.
5. **Check firewall settings.**
   Ensure that firewall rules are not blocking incoming or outgoing SSDP or UPnP traffic. Allow the required communication if necessary (for example “Network Discovery (SSDP-In)”).

Are there any command-line tools that can detect the device?

Yes. Many tools are either pre-installed on your system or available as free downloads that can detect the device.

Example: SSDP Discovery in Windows PowerShell

```
PS C:\Users\user> $ssdpFinder = New-Object -ComObject 'UPnP.UPnPDeviceFinder'
PS C:\Users\user> $ssdpFinder.FindByType('upnp:rootdevice', 0)
...
FriendlyName     : NCC-V2-VB-6A-50-C6-5C-88-BB
PresentationURL  : http://10.97.101.8/
ManufacturerName : Mobatime
...
```

Example: SSDP Discovery on Linux

```
user@computer ~ $ ssdp-scan
+ NCC-V2-VB-6A-50-C6-5C-88-BB              http://10.97.101.8/
+ NCC-V2-82-3B-56-C6-53-A6                 http://10.97.101.14/
...
```

MOBATIME

Headquarters/Production
Sales Worldwide

Tel. +41 34 432 46 46 | Fax +41 34 432 46 99
moserbaer@mobatime.com | www.mobatime.com

Sales Switzerland

MOBATIME AG | Stettbachstrasse 5 | CH-8600 Dübendorf
Tel. +41 44 802 75 75 | Fax +41 44 802 75 65
info-d@mobatime.ch | www.mobatime.ch

MOBATIME SA | En Budron H 20 | CH-1052 Le Mont-sur-Lausanne
Tél. +41 21 654 33 50 | Fax +41 21 654 33 69
info-f@mobatime.ch | www.mobatime.ch

Sales Germany/Austria

BÜRK MOBATIME GmbH
Postfach 3760 | D-78026 VS-Schwenningen
Steinkirchring 46 | D-78056 VS-Schwenningen
Tel. +49 7720 / 85 35 - 0 | Fax +49 7720 / 85 35 - 11
buerk@buerk-mobatime.de | www.buerk-mobatime.de