Manual Powerstation TWO

Installation & Configuration

Version 1.0

06/08/24

Table of contents

Introduction

Welcome to the Powerstation TWO Manual. This document provides detailed instructions on how to configure and use the Powerstation TWO charging station, manufactured by Powerstation.

---

1. Quick Start

1.1 Intro

Configuring one or more charging stations.

Each charge point is equipped with a 4G modem for communication (recommended) with a backend or can communicate with a backend over a local network.

If there are multiple charging points that need to communicate with each other in a DLM (Dynamic Load Management), you will need:

- Separate UTP connection (STER connection, not daisy-chained) for each charger
- All connected to an unmanaged switch
- Power supply and protection per charging station (1 power cable can power both sockets of a Powerstation TWO)

A circuit breaker must be provided for each charger, from 16A to 63A. On a three-phase grid, 16A corresponds to 11kW, 63A to 44kW.

The charging station is able to statically distribute the power over all connectors. This means that the Master will set the total power made available for the charging island, and will distribute it according to supply and demand.

A dynamic distribution is also possible, provided that an extra kWh meter is added to the main board. In this way, the total power of the connection can be set, and the kWh meter will measure how much is being drawn. The balance will go to the charging island.

1.2 Charge point configuration without backend

1. Connect your laptop to the free config port of the Bender controller. (Are you not familiar with this? Then go to chapters 2 and 3).
2. Go to the Bender configuration page; http://192.168.123.123:81
3. Log in with username **operator** and password **yellow_zone**

There are now 2 ways to start charging, either Plug & Charge or by means of RFID Badge. This is up to the customer.

Plug & Charge	RFID Badge
Click on Authorization and set 'Free Charging' to **On/On**	Click on Whitelists
With Free Charging Mode, you have to choose No OCPP (since there is no backend)	Click on Add Item and badge with the desired charge card (on the RFID of the Master controller)
Click Save and Restart	If necessary, repeat the above step until all RFID badges have been read
	Click Save and Restart

1.3 Charge point configuration with backend

1.3.1 Connection via SIM (4G)

1. Insert the SIM card you received into the SIM slot of the controller.
2. Log in to the controller
3. In the menu on the left, click on Network
4. Enter the APN of the corresponding provider

E-Flux APN Username Password	m2m.services / /
Total Username Password	Wlapn.com g2m g2m
LMS Username Password	evc-net.apn / /

5. Click save
6. Click on backend and fill in the following details
    a. Connection: GSM
    b. OCPP Mode: OCPP-J 1.6
    c. Websocket JSON OCPP URL of the backend:

E-Flux	wss://ocpp.e-flux.nl/1.6/powerstation
Total	ws://evse.total-ev-charge.com:9999/ocpp/WebSocket
LMS	ws://ws-private.evc-net.com

7. Click save and restart
8. After reboot; Check the following:
    a. Connection State (Modem) APN session duration
    b. Connection State (Backend) Connected (send heartbeat in … seconds)

    If the above appears correctly and is filled in, the connection with the backend is good.

9. Register the charging station with the backend provider (OCPP ID, Serial number, ..)

Please note, depending on the provider, other adjustments may also be required to the settings. For Total, the RFID Tag Letter Case must also be in **Upper Case** . Check with the backend provider.

1.3.2 Connection via local network

1. Log in to the controller
2. In the menu on the left, click on Network
3. Connection Type: Ethernet
4. Backend Setting:
    a. OCPP Mode: OCPP-J 1.6
    b. Websocket JSON OCPP URL of the backend:

E-Flux	wss://ocpp.e-flux.nl/1.6/powerstation
Total	ws://evse.total-ev-charge.com:9999/ocpp/WebSocket
LMS	ws://ws-private.evc-net.com

5. Click save and restart
6. After reboot; Check the following:
    a. Connection State (Backend) Connected (send heartbeat in … seconds)
7. Register the charging station with the backend provider (OCPP ID, Serial number, ..)

1.4 DLM Master Configuration

Log in to the controller.

Under the Network tab

1. Show GSM settings
2. WAN Router on On
3. View LAN settings
4. Changing Ethernet Configuration Mode in DHCP Server
5. WLAN enabled on On
6. Save

Under tab Installation

1. Fill in **the current carrying capacity of the supply line** (Charging Station Installation Current Limit) – **Fuse**, circuit breaker value, etc.specific to the charge point.
2. Fill in phase rotation of the charging point correctly (Socket 1 and 2)
3. Save

Under tab Load Management

1. Operator Maximum Charging Current – Can be set for socket 1 (Max 32A)
2. Operator Maximum Charging Current (Connector 2) – Can be set for socket 2 (Max 32A)
3. Dynamic Load Management:

Dynamic Load Management DLM Master/Slave	DLM Master (With Internal Slave)
EVSE Sub-Distribution Limit	Value of the main fuse of the loading platform (in Ampere per phase)
Operator Sub-Distribution Limit	Equal to or lower as EVSE Sub-distribution limit (in Amps per phase)
Support for external kwh meter	If present, choose On, otherwise Off
Meter Configuration (Second)	Choose Used Meter
IP Secondary Meter Address	IP Address of the meter, please note that they must be in the same network. Note DHCP Server setting of Master if applicable
Main Distribution Limit	Value of the main fuse (Pay attention to location of kwh meter)
External meter location	Set correctly! Included is full consumption of the building
Minimum charging current	Standard at 7A (8A may be required for some cars)
Max charging current in case of disconnection	Defaults to 7A, if connection to Master is lost

4. Leave other values as they are
5. Click save and restart
6. Confirm that connection to all slaves is correct (check on Dashboard page)

Extra:

Bender controllers work by default in range 172.16.23.001 to .255. If the master is set up as DHCP Server, it will distribute leases in this range. Make sure that the external kWh meter has a fixed IP address in this range and set this correctly in the Load Management tab at Second Meter.

If you're connecting to a local network, keep an eye out for IP collisions! It is strongly recommended to always set up your own network for the charging stations. If you can't connect a backend via SIM (because it's underground, for example) it's best to set up your own network and install a 4G SIM modem in a place with reception and connect it to the unmanaged switch.

1.5 DLM Slave Configuration

Log in to the controller.

Under tab Installation

1. Fill in **the current carrying capacity of the supply line** (Charging Station Installation Current Limit) – **Fuse**, circuit breaker value, etc.specific to the charge point
2. Fill in phase rotation of the charging point correctly (Socket 1 and 2)
3. Save

Under tab Load Management

1. Operator Maximum Charging Current – Can be set for socket 1 (Max 32A)
2. Operator Maximum Charging Current (Connector 2) – Can be set for socket 2 (Max 32A)
3. Dynamic Load Management:

Dynamic Load Management DLM Master/Slave	DLM Slave (Master-Auto-Discovery)
Minimum charging current	Standard at 7A (8A may be required for some cars)
Max charging current in case of disconnection	Defaults to 7A, if connection to Master is lost

4. Leave other values as they are
5. Click save and restart

2. Access to Configuration Interface

USB access

Note: USB access should only be performed by a qualified electrician. Make sure you have Java installed on your laptop.

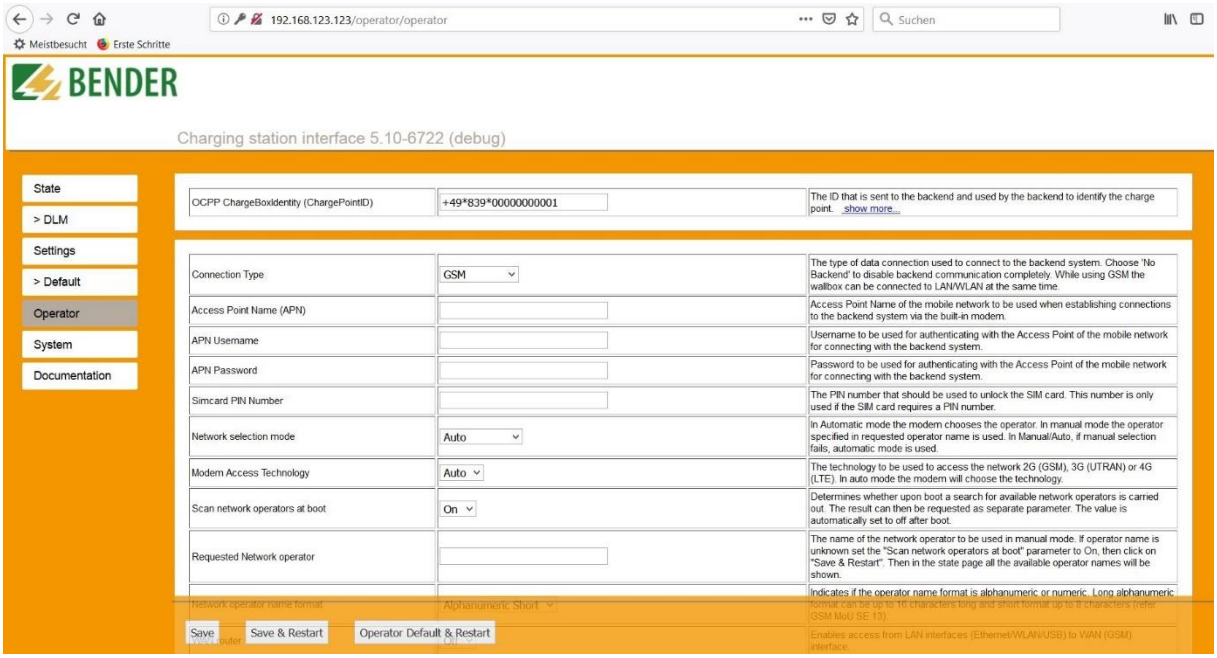
To establish a physical connection to the controller, a PC and a USB cable (with USB-A and Micro-USB-B connector) are required. Plug your cable's micro USB plug into the corresponding port on the controller, marked "CONFIG". Plug the other end of the cable into your PC. A so-called RNDIS (Remote Network Driver Interface Specification) network is simulated, which is automatically recognized in Linux and Mac operating systems.

For Windows, the driver "RNDIS/CDC Ethernet Gadget" must be installed. This is usually done automatically. If not, the driver can be installed manually from Control Panel.

1. Open the Control Panel.
2. Find the unknown device or "RNDIS/Ethernet Gadget" under "Other Devices".
3. Right-click and select "Update Drivers".
4. Select "Search My Computer for Drivers".
5. Select "Let me choose from a list of device drivers on my computer".
6. Uncheck "Show compatible hardware" and select "Microsoft Corporation".
7. Select "NDIS Compliant External Device" and confirm with "Next".

After installation, the charge controller will be recognized as a network adapter. Enter http://192.168.123.123/operator in your browser's address bar to access the configuration interface.

Legacy view of the configuration page:



Ethernet access

When accessing via Ethernet, enter the IP address of the charge controller into the Ethernet network instead of 192.168.123.123. If the controller receives an IP address from a DHCP server, you must find out the IP address of the DHCP server. With a static IP configuration, you use the configured static IP address. A permanent second static IP address is 192.168.124.123. Manually configure your PC to an IP address in the same range (e.g. 192.168.124.100 with subnet mask 255.255.255.0).

Access via Backend

Access through the backend uses the controller's OCPP interface. The backend sends GetConfiguration and ChangeConfiguration messages to read the configuration parameters.

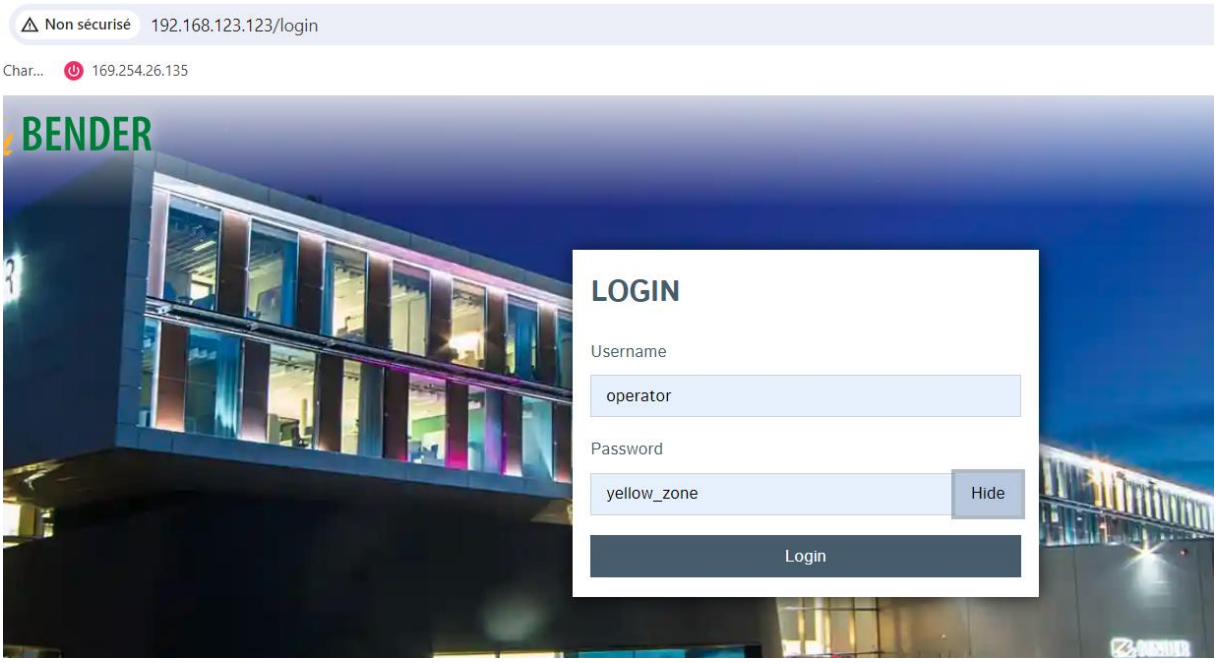
3. Access to Configuration Interface 2.0

To make changes to the controller's configuration, the web-based configuration interface must be accessed. Since firmware version 5.12, the configuration interface 2.0 has been available. The web interface can be accessed via WLAN, Ethernet, USB or mobile network interface.

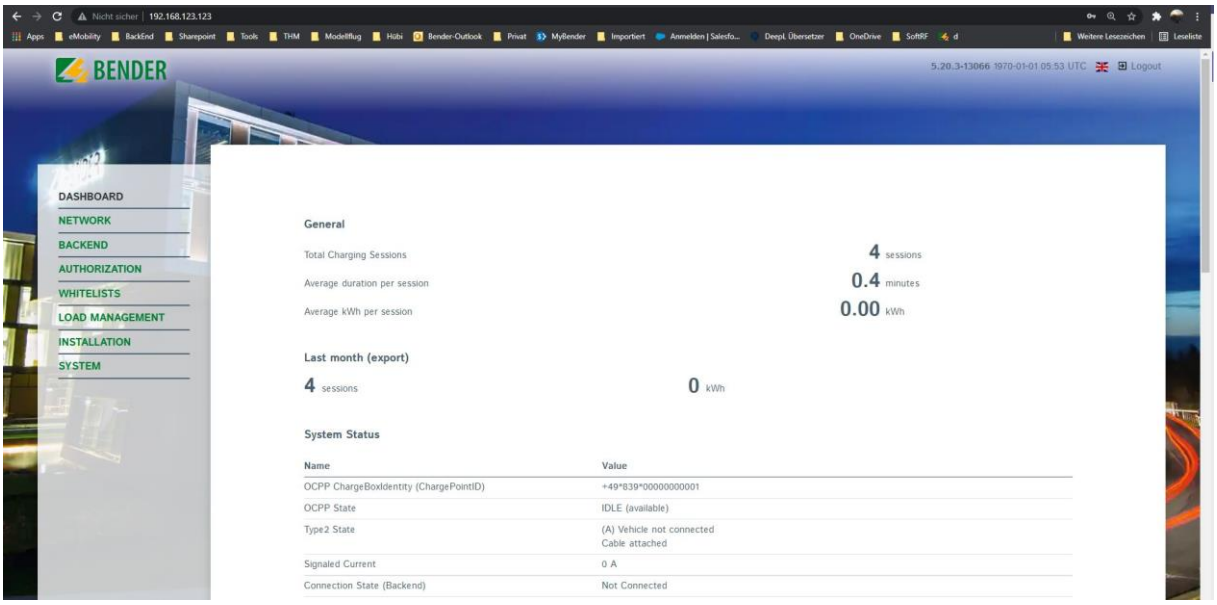
USB access

Make a physical connection using a USB cable. Plug the micro USB plug into the "CONFIG" port on the controller and the other end into your PC. Enter http://192.168.123.123/ in the address bar.

Username: operator
Password: yellow_zone



Interface 2.0 screen:



Access via Ethernet

Enter the IP address of the charge controller in the Ethernet network. If DHCP is used, you need to find out the IP address of the DHCP server. For a static IP configuration, use the configured static IP address 192.168.124.123.

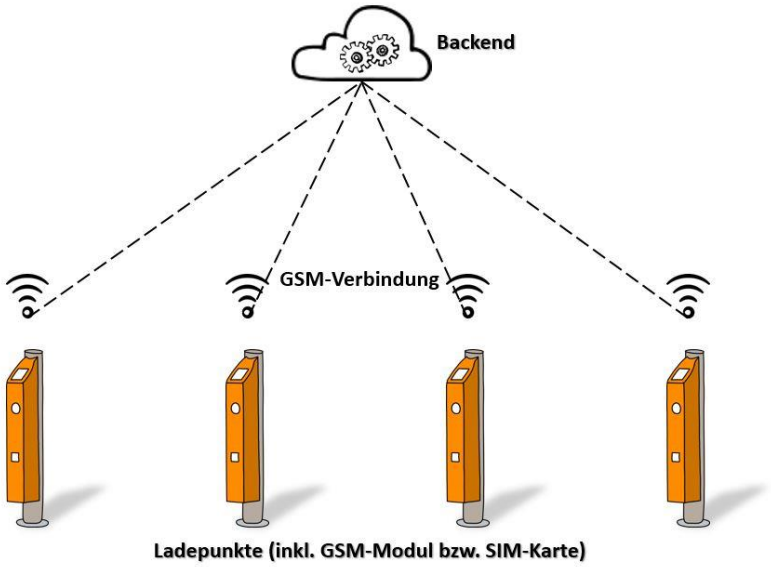
Access via Backend

Uses the controller's OCPP interface for configuration through the backend system.

4. Configuring Network Connections

3.1 GSM Network Connection

Configure the charge point to connect to the internet or private network via GSM. Make sure the controller has a GSM module and antenna, and the SIM card is inserted and activated.



5.29.4-13558 1

BACKEND

Connection

Connection Type	GSM

OCPP

OCPP ChargeBoxIdentity (ChargePointID)	ENOGEN22SB-JB-0017805
OCPP Mode	OCPP-J 1.6
WebSockets JSON OCPP URL of the Backend	ws://evse.total-ev-charge.com:9999/ocpp/WebSocket
Websockets proxy	
WebSockets keep-alive interval	60
HTTP Basic Authentication password	
Force Heartbeat request messages	On
Send informative StatusNotifications	On
Send error StatusNotifications	On
Send USB error StatusNotifications	Off
Strategy for StatusNotification state transitions	Occupied on Charging
Allow long get configuration keys	Off

Configuration parameters:

- Connection Type: GSM

- Access Point Name (APN): Provided by backend provider
- APN Username: Provided by backend provider
- APN Password: Provided by backend provider
- SIM Card PIN Number: Provided with the SIM card
- Only IoT sim is supported

Overview

Parameter	Value	Description
Connection	Cell phone	Indicates how the charge point connects to the backend
Access Point Name (APN)	See information from your provider	Backend Operator APN
APN Username	See information from your provider	
APN Password	See information from your provider	
SIM card PIN number	Comes with the SIM card	
Network Selection Mode	Car; Manual; Manual/Auto	Searches and connects automatically or manually
Scan Network Operators at Startup	Only relevant if Network Select Mode is not set to Auto	
Modem access technology	Car; 2G; 3G; 4G	Mobile communication standard for communication
Preferred Network Operator	Only relevant if Network Select Mode is not set to Auto	
Network Operator Name Format	Only relevant if Network Select Mode is not set to Auto	

Save changes with Save & Restart.

Example of settings for Totalenergies SIM card:

NETWORK

GSM

Show Modem Configuration	Show
Access Point Name (APN)	wlapn.com
APN Username	g2m
APN Password	g2m
SIM PIN	
Network selection mode	Auto
Modem Access Technology	Auto
Requested Network operator	
Network operator name format	Alphanumeric Short
WAN router	Off
MTU	

LAN

Show LAN Configuration	Hide

USB

Show USB Configuration	Hide

And corresponding back-end address:

5.29.4-13558 1

BACKEND

Connection

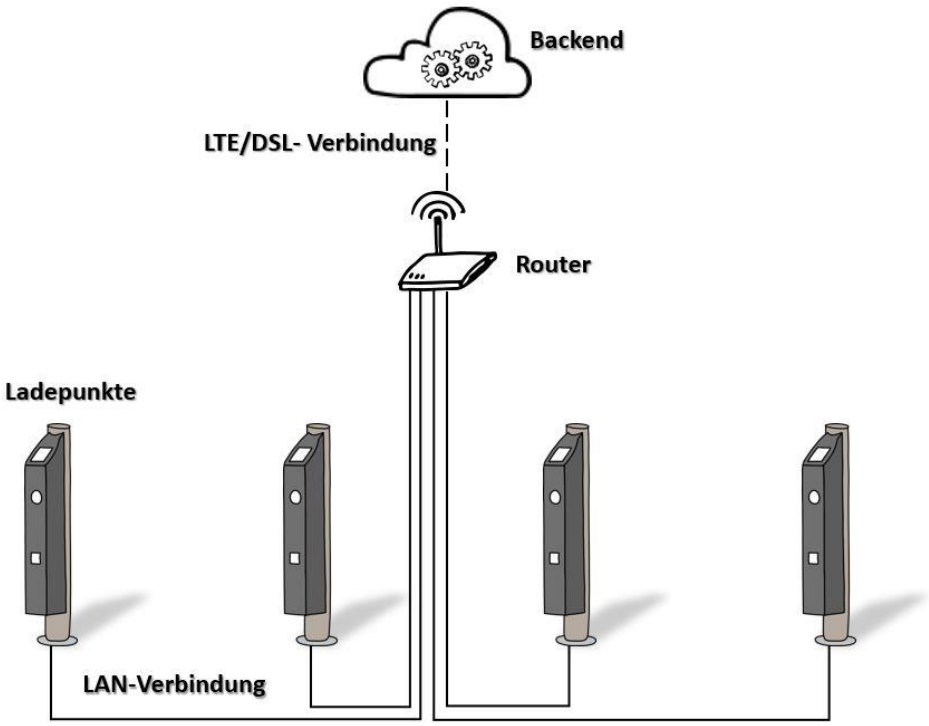
Connection Type	GSM

OCPP

OCPP ChargeBoxIdentity (ChargePointID)	ENOGEN22SB-JB-0017805
OCPP Mode	OCPP-J 1.6
WebSockets JSON OCPP URL of the Backend	ws://evse.total-ev-charge.com:9999/ocpp/WebSocket
Websockets proxy	
WebSockets keep-alive interval	60
HTTP Basic Authentication password	
Force Heartbeat request messages	On
Send informative StatusNotifications	On
Send error StatusNotifications	On
Send USB error StatusNotifications	Off
Strategy for StatusNotification state transitions	Occupied on Charging
Allow long get configuration keys	Off

3.2 LAN/Ethernet Network Connection

Integrate charge points into an existing local area network via Ethernet.



Configuration parameters:

- Connection Type: Ethernet
- Network Configuration Mode: Auto (DHCP Client) or Manual Configuration

Requirements

Your charge point has an Ethernet adapter

There is already a local wired network that is connected to the internet via a router

Your charge point is connected to your local network

Ethernet Network Configuration

Select "Connection Type" as "Ethernet".

The other settings are differentiated between automatic and manual configuration of the network, which you define under "Network configuration mode". Automatic configuration is performed using the so-called Dynamic Host Configuration Protocol (DHCP). The parameters are automatically assigned or defined by the server. Most routers offer this technology. However, some networks require a fixed assignment of the parameters. To do this, the manual mode

(Manual Configuration) must be selected. Before you configure the charge points accordingly, you must first determine whether the router on your local network supports or offers DHCP.

Note: Configuration as a DHCP server is not described here. This setting is used to configure a gateway (scenario 4).

Scenario 1: Auto DHCP Client

If your router automatically assigns IP addresses, select "Network Configuration Mode" as "Auto (DHCP Client)".

Parameter	Description
DHCP-client hostname	Hostname string
DHCP Client Request Repetitions	Number of connection attempts
DHCP Client Request Timeout	Timeout in seconds
DHCP Client Request Delay	Specified in seconds

Most of the time, you can directly accept the preset values of the four relevant parameters. You can also see the default values in the following image. Whether an ID and (if so) which ID should be entered in the DHCP client hostname field depends on your network. If necessary, contact the network administrator.

Save your entry with "Save & Restart".

Scenario 2: Manual Configuration

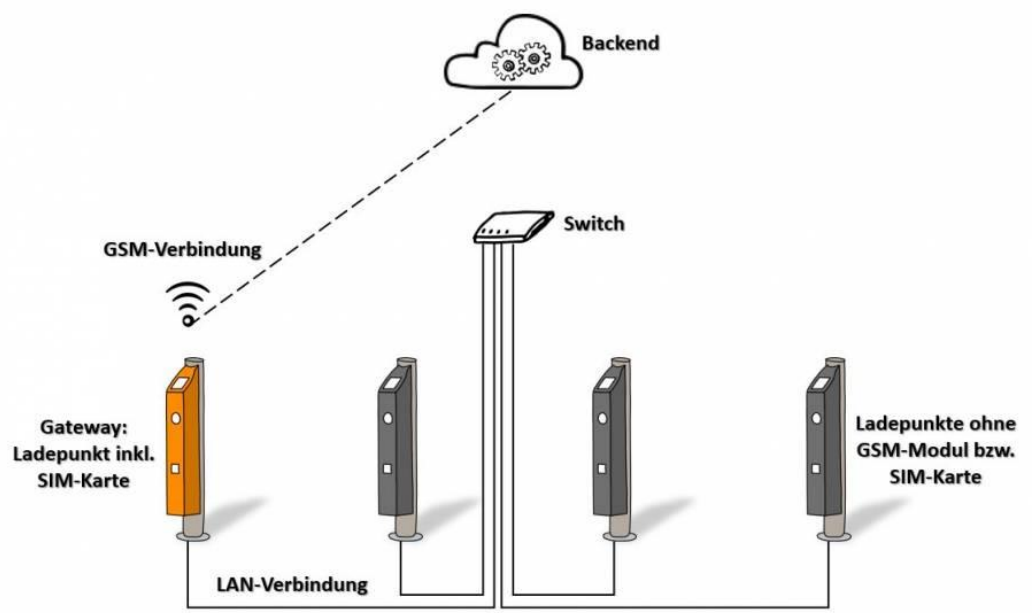
To integrate the charge point into an existing network where the router does not offer DHCP, select "Network Configuration Mode" as "Manual Configuration".

Parameter	Possible values	Description
Static Network Configuration IP	Usually: 192.168.xxx.xxx	Static LAN IP address of the charge point
Static Network Configuration Netmask	Usually: 255.255.255.0	Static LAN IP network masking of the charge point
Static Network Configuration Gateway	Usually: 192.168.xxx.1	IP address of the gateway/router
DNS Static Network Configuration		IP address of the server for name resolution

You have to enter the individual parameters yourself. To do this, contact your network administrator and ask for the individual parameters. Then enter the information in the appropriate fields and save your entry with "Save & Restart".

3.2 Gateway Configuration

Connect multiple charge points to the internet/backend via a gateway. The individual charging points are connected via Ethernet and a switch.



Configuration parameters:

- Connection type: GSM; Ethernet
- WAN Router: On
- Network Configuration Mode: Manual Configuration; Auto (DHCP Client); DHCP Server

Note: The WAN router and DLM master functions do not need to be configured on the same controller! It is therefore recommended to activate both functions on different controllers, so that in the event of a defect or malfunction, both functions do not fail at the same time.

Requirements

At least one charging point (gateway) has a GSM module and a SIM card

Physical connection of the charging points via Ethernet and switch is available and operational

Parameter	Mogelijke waarden	Beschrijving
Verbindingstype	GSM; Ethernet	
WAN-router	Aan; Uit	
Modus voor netwerkconfiguratie	Handmatige configuratie; Auto (DHCP-client); DHCP-server	Verschillende configuratietypes voor integratie in het netwerk
Statische netwerkconfiguratie IP		Vast IP-adres
Statische netwerkconfiguratie netmasker		Vast netwerkmaskeer
Statische netwerkconfiguratie gateway		Vast IP-adres van de gateway naar het internet
Statische netwerkconfiguratie DNS		Vast IP-adres van de server voor naamresolutie

Ethernet Network Configuration

The so-called gateway charging point is the charging point with a GSM module.

Scenario 1: Automatic Network Configuration

⇒ Available from firmware version 4.60 ⇐

With the automatic network configuration, it is possible for all charging points connected via Ethernet or WLAN to be automatically assigned an IP address/DNS and gateway using a built-in DHCP server. The DHCP server is then the controller on which the "Networking Configuration Mode" DHCP server is activated.

Note: If the charge points are given a randomly assigned IP address through the automatic network configuration, you will no longer be able to access a specific charge point via the Ethernet switch with a known IP address. If you use dynamic load management in conjunction with this configuration, there is a risk that the charge points will not receive IP addresses if the DHCP server fails, causing dynamic load management to malfunction. Depending on the configuration, no one will be able to load. It is therefore recommended that even if the DHCP server is enabled, you assign static IP addresses to the charge points. The advantage is that a laptop connected to the Ethernet switch is automatically given an IP address in the same network by the service technician. The DHCP server also plays an important role in name resolution (DNS relay) when connecting to a backend via GSM.

Configuration of the gateway charge point

1. Make a network connection via GSM. You can find instructions here.
2. Activate the WAN router by setting the parameter to "On".
3. Set the "Network Configuration Mode" parameter to "DHCP Server". This creates a new network for the other charging points, with the gateway acting as a router. All the

necessary parameters (such as the IP address) of the other charging points in the network are automatically assigned by the DHCP.

4. Save the settings with "Save & Restart".

As a DHCP server, the controller automatically accepts the following parameters:

- IP address: 172.16.23.1
- Network Masking (SubnetMask): 255.255.255.0
- Gateway: 172.16.23.1
- DNS (Domain Name Server): 172.16.23.1
- Range of IP addresses automatically assigned to the remaining charge points (clients): 172.16.23.100-172.16.23.254. This means that you can use the address range 172.16.23.2-172.16.23.99 for a static mapping.

Note: In older software versions (4.60 - 4.63), the IP address was 172.42.23.x instead of 172.16.23.x. Therefore, please check the software version before making any changes.

Configuration of the other charging points (clients)

As explained above, we do not recommend automatic configuration and recommend scenario 2: manual network configuration.

1. Set "Connection Type" to "Ethernet" throughout.
2. Deactivate WAN router for these charge points.
3. Set the "Networking Configuration Mode" parameter to "Auto (DHCP Client)". Also, make sure that there are no address conflicts in your network. Instructions on how to configure the relevant parameters can be found here.
4. Save the settings with "Save & Restart".

Scenario 2: Manual Network Configuration

The network parameters of the individual charging points are entered manually.

1. To avoid conflicts with the DHCP server, choose an IP address between 172.16.23.2 and 172.16.23.99.
2. The gateway and DNS server is the IP address of the DHCP server: 172.16.23.1.

4. Back-end connection

Here you can configure the type of communication between the charge point and the backend via the Open Charge Point Protocol (OCPP). The basic requirement for configuring the backend is that you have already set up an internet connection between the charge points and signed a contract with a backend provider. If you haven't configured a network yet, follow the instructions in the Network section.

Requirements

- Network connection is already configured
- A contractual relationship with a backend provider already exists
- The charge point is already registered or stored in the backend

Basic Scenario 1 Setting: OCPP-S 1.5/1.6 (SOAP)

Parameter	Range	Description
OCPP ChargeBoxIdentity (ChargePointID)	OCPP ChargeBoxIdentity	
OCPP Mode	OCPP-S 1.5; OCPP-S 1.6	
SOAP OCPP URL of Backend (Standard OCPP)	URL of the backend	URL of the backend. This is provided by your backend provider. Here you will find an overview of the URLs of different providers.
SSL mode as server	Encrypt only - No authentication; Allow expired certificate and skip host check; Skip host check; Allow expired certificate; Normal SSL Auth; No SSL, Plain HTTP	???
SOAP OCPP Server Port of ChargePoint	8090	Specify the port used for communication with the backend. Your backend provider will tell you the correct port. Here's a breakdown of the ports used by some carriers.
Backend Whitelist (SOAP)	List of IPs allowed to send requests to the charge point via SOAP	???
Mode for selecting the public address of the ChargePoint	Local device; Manual selection; Auto select; Teltonika RUTXXX	Manual selection: ... Address of "Public address of the charging point" is taken over; Automatic selection: ...

Configuration

1. Select OCPP Mode "OCPP 1.5" or "OCPP 1.6". The version depends on the backend to which your charge point needs to be connected.
2. Enter your backend address in the field. The URL must start with "http://" or "https://". Your provider will provide you with the address along with the contract documents. Here you will find an overview of some providers. SOAP OCPP URL of Backend (Standard OCPP)
3. Enter your OCPP ChargeBoxIdentity in the OCPP ChargeBoxIdentity (ChargePointID) field. This is usually sent to you by the backend operator. In some cases, you can set the ID yourself. However, it is important that the name is unique. In this case, we therefore recommend using the serial number of the charge point. It is important that the ID is already stored in the backend system.
4. In the SOAP OCPP Server Port or ChargePoint (Standard OCPP) field, enter the correct port.
5. Save your entry with "Save & Restart".

You can also make the following settings:

Mode for selecting the public address of the ChargePoint Here you can set which public address the charge point should accept.

- Local device: of the router?
- Manual select: The address you entered is accepted Public address of the ChargePoint.
- Auto select: Address is automatically assigned by an open internet service.
- Teltonika RUTXXX: Select this option if the charge point is connected to the Internet via a corresponding WAN router. This also requires WAN router password.

Scenario 2: OCPP-J 1.6 (JSON)

Parameter	Range	Description
OCPP ChargeBoxIdentity (ChargePointID)	ChargePointID	
OCPP Mode	OCPP-J 1.6	
WebSockets JSON OCPP URL of the Backend	Depends on the backend	The WS/WSS URL of the backend must be entered here. It should start with "ws:" or "wss:". Your provider will provide you with the URL. Here you will find an overview of some providers.
WebSockets keep-alive interval	Time in seconds (factory default: 0)	Disabled at zero

Configuration

1. Select OCPP Mode "OCPP-J 1.6".
2. Enter your charge point's ChargePoint ID in the OCPP ChargeBoxIdentity (ChargePointID) field.
3. Enter your backend address in the field. The URL should start with "ws:/" or "wss:/". Your provider will provide you with the address along with the contract documents. Here you will find an overview of some providers. WebSockets JSON OCPP URL of the Backend
4. Save your entry with "Save & Restart".

Under this WebSockets keep-alive interval field, you have the option to set a so-called "keep alive". Specific packets of a network protocol are exchanged at regular intervals between the actors in a network. The goal is to permanently test and maintain the network connection. You can enter the interval for exchanging packets in seconds here. If you enter zero seconds, this feature will be disabled. If a so-called "NAT router" is connected between the charge point and the backend, you must activate this function. Otherwise, the router may block the connection. If necessary, contact your system administrator or your mobile operator.

More settings Here you can make further settings for the communication between the charge points and the backend. These are largely independent of OCPP mode. Save your changes with "Save & Restart".

Restart transaction after power loss Determines whether the charging process should continue automatically with the same authentication parameters after a power failure and whether the data should be resent to the backend.

- On: The loading process continues with the same parameters –> no new authorization
- Off: The charging process is aborted -> the user needs to be reauthorized after the power failure

We generally recommend setting this to "On" or user complaints may occur.

Backend connection timeout: On the one hand, it corresponds to the waiting time in seconds for the charging station to receive a message from the backend before requesting the message again. On the other hand, it corresponds to the waiting time for choosing the mobile network and establishing the connection to the backend. If the mobile reception of the charging station is poor, a higher value is useful. On the other hand, a value that is too high leads to a long wait for the charge point to execute commands from the backend. This can lead to delays in operation. The factory default setting is 60s.

SSL Strictness as client Determination of the obligation to transfer data securely to the backend. The security levels range from no authentication to full authentication. Not every backend supports or requires encryption, so this parameter must be configured in consultation with the respective provider.

- Encrypt only - No authentication:
- Allow expired certificate and skip host check
- Skip host check

- Allow expired certificate
- Normal SSL Auth

We recommend... Please note that not every backend supports or requires encryption, so this parameter must be configured in consultation with the respective provider.

TCP Watchdog Timeout Specifies the number of seconds after which the charge point controller will automatically restart if a connection to the backend cannot be established. After the reboot, a new attempt is made to connect to the backend. Entering "0" will disable this option. The factory default setting is 10800s.

Display backend disconnect as error When activated, the LED status bar indicates to the user when the connection to the backend has been interrupted. Here you will find a list of the LED statuses of the charging point in Berlin. This function has been deactivated in the delivery state.

Send informative StatusNotifications Here you can specify whether purely informative status information (such as the measured temperature of the controller) should be sent to the backend.

Send error StatusNotifications Here you can specify whether error messages from the controller or charge point (e.g. if the actuator for securing the cable is defective) should be sent to the backend.

Send USB error StatusNotifications Here you can specify whether errors in communication via USB between controllers or charge points should be sent to the backend. Communication via USB usually only takes place with dual charging stations. See also Network.

Strategy for StatusNotification state transitions Here you can specify in which situation the charge point should be shown as "occupied" in the backend.

- "Occupied on Charging": The charge point is only shown as occupied when both a charging cable is connected and the authorization has been granted.
- "Occupied on Authorized/Plugged": one of the conditions is sufficient for the charge point to appear as occupied in the backend.

Preparing until state C (OCPP 1.6) Note: This setting is only relevant for OCPP 1.6. Determines when the status of the charging station jumps from "Preparing" to "Charging" in the backend.

- When 'On': Only when the car switches to charging status C (ready)
- If 'Off': Already when the car is in charging status B (vehicle detected)

Allow long get configuration keys

Next steps There are other important settings to consider when communicating between the charge point and the backend. You can find these in the Authorization section.

Overview of different backend providers Here you will find, among other things, the parameters for configuring the different providers.

Backend Provider	Access Point Name (APN)	APN Username	APN Password	OCPP Mode
TotalEnergies	wlapn.com	g2m	g2m	OCPP-J 1.6
Eflux	m2m.com			OCPP-J 1.6

Notification by e-mail (from SW version 5.30)

These parameters allow you to set up an email notification in case of errors that would also be reported to an OCPP backend. The email is sent in text format to a specific recipient.

You can find the necessary settings for username, password, SMTP server, port, etc. in your e-mail program. You can also specify a location for the charge point, which will be included in the email.

To be on the safe side, you may want to create your own email account just for the charge point, as the access data is stored on the charge controller. You can then forward the emails to your regular account.

The settings will only become active after the charge point has been restarted and the message (including the test button) can only then be used.

A test email can be sent using a test button. If it doesn't arrive in your inbox, check your SPAM folder and adjust the filter if necessary.

If the errors no longer exist, a notification will also be sent.

5. Authorization

5.1 Default parameters

Here you can configure all the parameters that control the authorization and authentication of users of the charging station.

`Vehicle connection timeout`

Once authorized, the user must plug the charging cable into the charging station within a defined period of time. If this is not the case, the authorization expires and the user must re-authenticate to recharge. You can set this period here. The default factory value is 45 seconds.

`Send Authorize for RemoteStart`

Here you can select whether the charge point should send an authorization message to the backend when a remote charging process is started (via RemoteStart message). You'll need to check with your backend provider about this setting. Some providers require this, while other backends require this feature to be deactivated.

`If in doubt allow charging`

Here you can specify how the charge point behaves when a user wants to authenticate and the RFID does not appear in any whitelist or cache and the request that is then sent to the backend cannot be answered. This may be the case, for example, if the internet connection is interrupted or the backend is not accessible.

- Off: The charging process will only start when the charge point receives feedback from the backend and the user is authorized. In extreme cases, this means that the user will not be able to charge.
- On: Here, the charging process is authorized even if there is no response from the backend. However, once this is done, the charging process can then be aborted.
- Immediate Plug-in: The charging process will begin immediately after the charging cable is plugged in. The user's RFID is not checked until the charging station has reconnected to the backend. If necessary, the charging process is then aborted. The difference with "On" is that here there is no need to present RFID at all when starting the charging process.

Note: If the charging station does not have a backend connection, this parameter must be set to "Off". Otherwise, anyone can use any RFID to charge permanently.

`Stop Transaction Mode`

Here you can select exactly how and when the charging transaction should be completed. This is particularly relevant if (among other things) charging time or parking time is charged.

- Normal: The cable is released and the transaction is stopped when the cable is removed from the car or the RFID used to authorize the charging process is presented again.
- Stop only by disconnecting: The transaction is only completely terminated when the cable is removed from the charging point.
- Only by RFID/RemoteStop: The charging process is not terminated until the authorized RFID is re-presented or a corresponding (remote stop) message is sent from the backend. Note: Removing the cable from the charge point does not end the transaction.
- Normal + Mode D + RCD Detected: This setting is essentially the same as normal mode. However, it is complemented by two cases in which the transaction is also terminated. Firstly, when the vehicle switches to the so-called charging mode D (see EN 62196 Type 2). This is the vehicle's way of indicating that the battery is "gassing out". However, the problem of outgassing does not occur with lithium-ion batteries, which is why charging mode D never occurs in practice. Second, when a fault current is detected and the residual current device (RCD) is tripped. This immediately cuts off the power supply. However, using this option requires the RCD to communicate with the controller and indicate when it has tripped. However, this is not the case with the Berlin charging point, for example.

`Lock Actuator only if authorized`

Here you can set when the cable should be secured or secured in the charging point by the actuator. It will then no longer be possible to pull out the charging cable.

- On: Only after successful authorization
- Off: Immediately after plugging in the charging cable

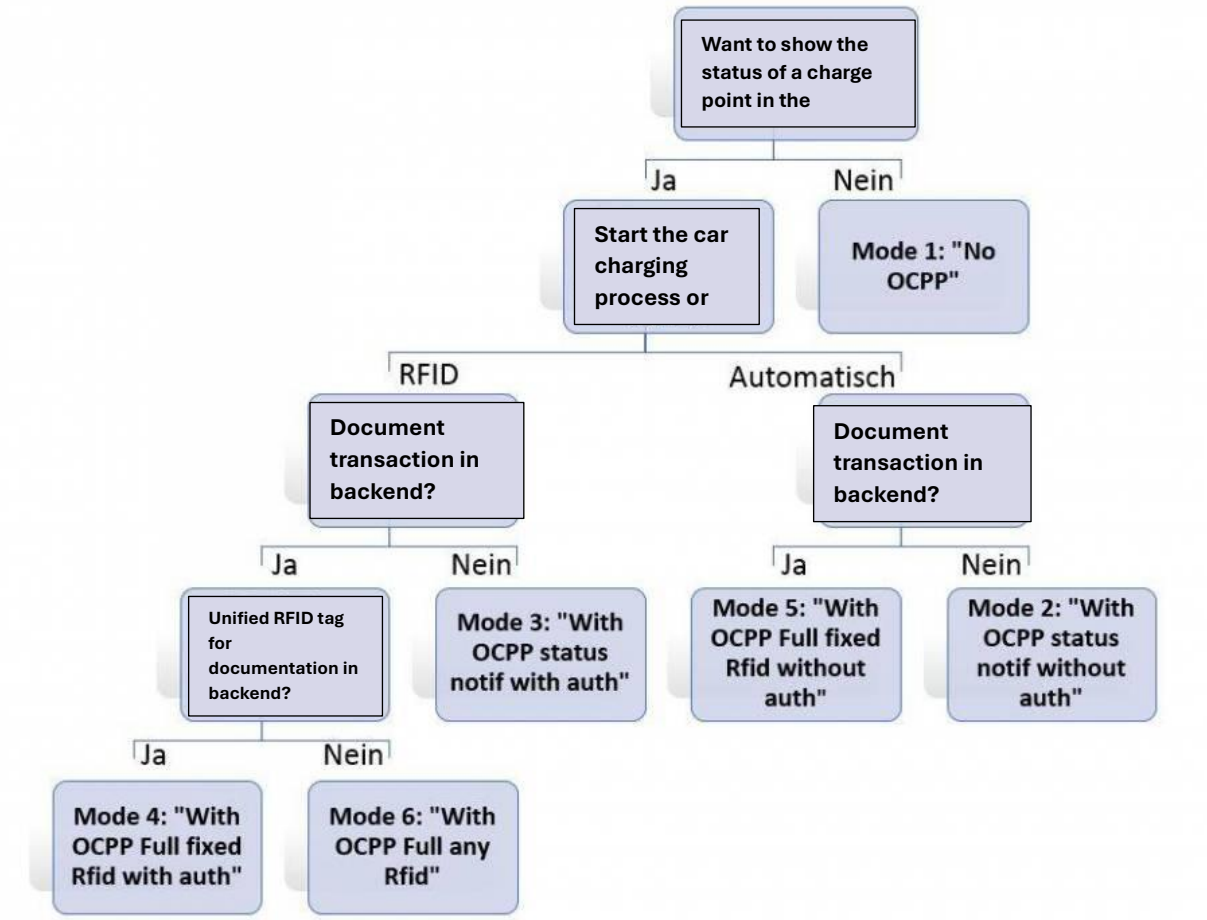
5.2 Free Charging

Free Charging describes a function in which basically anyone can charge at a charging point. So, the user group is not limited. In addition, charging does not incur any cost to the user. The CC613 controller offers 6 different variants for this.

Note: If you do not want free charging to be possible at your charging station, you must set the "Free Charging" parameter to "Off".

Overview

Parameter	Possible values	Description
FreeCharging	On; Off	Free Charging Turn on or off
Free Charging Mode	Mode 1; ... ; Mode 6	Choose one of the six available free charging modes
Rfid Tag for Free Charging with OCPP	Full, fixed RFID modes	RFID Tag Settings for Free Charging with OCPP



Configuration

Without backend

If your charging station does not have a backend connection, set the `Free Charging` parameter to "On" and select `Free Charging Mode` "No OCPP" (Mode 1).

Save your settings with "Save & Restart". After the restart, everyone can charge freely. The charging process will begin immediately after a connection to the car is established.

Potential users will not be able to see whether the charge point is free or occupied. It is not possible to evaluate the loading processes except by manually transferring the log files.

With backend

If your charge point has a backend connection, there are 5 different variants of free charging available. First, set the `Free Charging` parameter to "On". You can then select the desired variant. The image above will help you with the selection. **In contrast to the variant without a backend, the backend shows whether the charge point is occupied or free.**

First, the charge controller gives you the option to start and end the charging process with or without an RFID. In charging modes with "with authentication", a random RFID must be presented for charging - for example, the chip in the ID card is enough. This also means that the user cannot charge without an RFID. To finish the charging process, the same RFID must be presented again. However, in "without authentication" charging modes, no RFID needs to be presented for charging.

On the other hand, the charge controller offers several options for communication with the backend. If process-specific information is to be sent to the backend (e.g. start and stop transaction messages) and commands from the backend (e.g. remote stop) are to be allowed, then a so-called transaction ID is required. If this does not apply, the charge point will only send status messages. This applies to variants 2 and 3.

If a transaction ID is to be involved, you can also select whether to use the UID of the RFID (mode 6) or a unified ID, which should be specified in the `field Rfid Tag for Free Charging with OCPP Full, fixed rfid modes`. This will then be used for modes 4 and 5. In all other modes, this parameter can be ignored.

5.3 RFID Settings

List of compatible RFID cards:

- MIFARE Classic 1K/4K
- MIFARE Ultralight
- MIFARE Ultralight C
- MIFARE Plus S
- MIFARE Plus X
- MIFARE Plus SE
- MIFARE Plus EV2
- MIFARE DESFire
- MIFARE DESFire EV1
- MIFARE DESFire EV2
- MIFARE DESFire EV3
- MIFARE 2GO
- MIFARE SmartMX

One of the most important means of authentication at charging points is RFID (radio frequency identification) chips. This also includes NFC technology. These form the basis of all charging cards. The so-called UID (Unique Identification) of an RFID chip is central for identification. This is a unique code that represents the identity of a chip.

In this context, the CC613 controller offers two special functions in addition to free charging. To use the features, it is important that you know the UID of your RFID chips. One way to determine this is by reading it with an NFC-enabled mobile phone.

RFID Tag letter case

When reading the UID, the form of representation should always be taken into account. For our controller, the hexadecimal code must always be used. A distinction is made between uppercase and lowercase letters and between the normal and inverted byte order. When entering the UIDs, the form of representation must match the selection in the `RFID Tag letter case field`.

Example:

- Lower Case: 0a0e9b83
- Upper Case: 0A0E9B83
- Lower Case Reversed Byte Order: 839b0e0a
- Upper Case Reversed Byte Order: 839B0E0A

It's not always clear in which byte order the UIDs are specified. When in doubt, you should try both variants.

5.4 OCPP Whitelist

Description

The OCPP whitelist (also known as cache entry list or cache) is a type of local cache from the backend at the charge point. Here, all RFIDs from charge cards that have been approved by the backend are regularly transferred to the charge point. This is intended to ensure that the authorization of a charging process can take place even if the charge point is unable to connect to the backend. In addition, the authorization can be done much faster with the help of the cache.

If this option is deactivated, every time a request is made to the charge point (i.e. every time an RFID is presented to the RFID reader) a request is sent to the backend. The charging process will only be authorized when it is accepted.

Note: Deactivate the OCPP whitelist if you don't have a backend connection!

Configuration

To enable the OCPP whitelist, you need to set the `Enable OCPP whitelist` parameter (also Enable `cache`) to "On".

All UIDs released by the backend are then temporarily stored in the `List of entries in OCPP whitelist` (also in `List of entries in cache`). The intervals at which this list is updated depend on the respective backend.

Note: We recommend that you don't make any changes to this list, as they will be overwritten during the next sync. However, in certain cases, it may be helpful to delete the entire list. To do this, delete all songs from the list and save the change using "Save & Restart".

In the `OCPP whitelist expiry mode parameter`, you can select whether the charge point should autonomously delete cache entries if this is not done automatically by the backend.

- **End of epoch 2038 (default):** By default, the controller is configured to expire cache entry at the last possible date (December 31, 2038). In practice, this means that the local storage entries are never deleted by the controller itself. Changes to the cache are therefore made exclusively by the backend or manually.
- **One year from now**: The cache automatically expires one year after the last change.

5.5 Local Whitelist

Overview

The local whitelist (also known as fixed local list (FLL)) is a backend-independent list that is stored exclusively on the controller. UIDs included in this list are always authorized to load. No request is made to the backend.

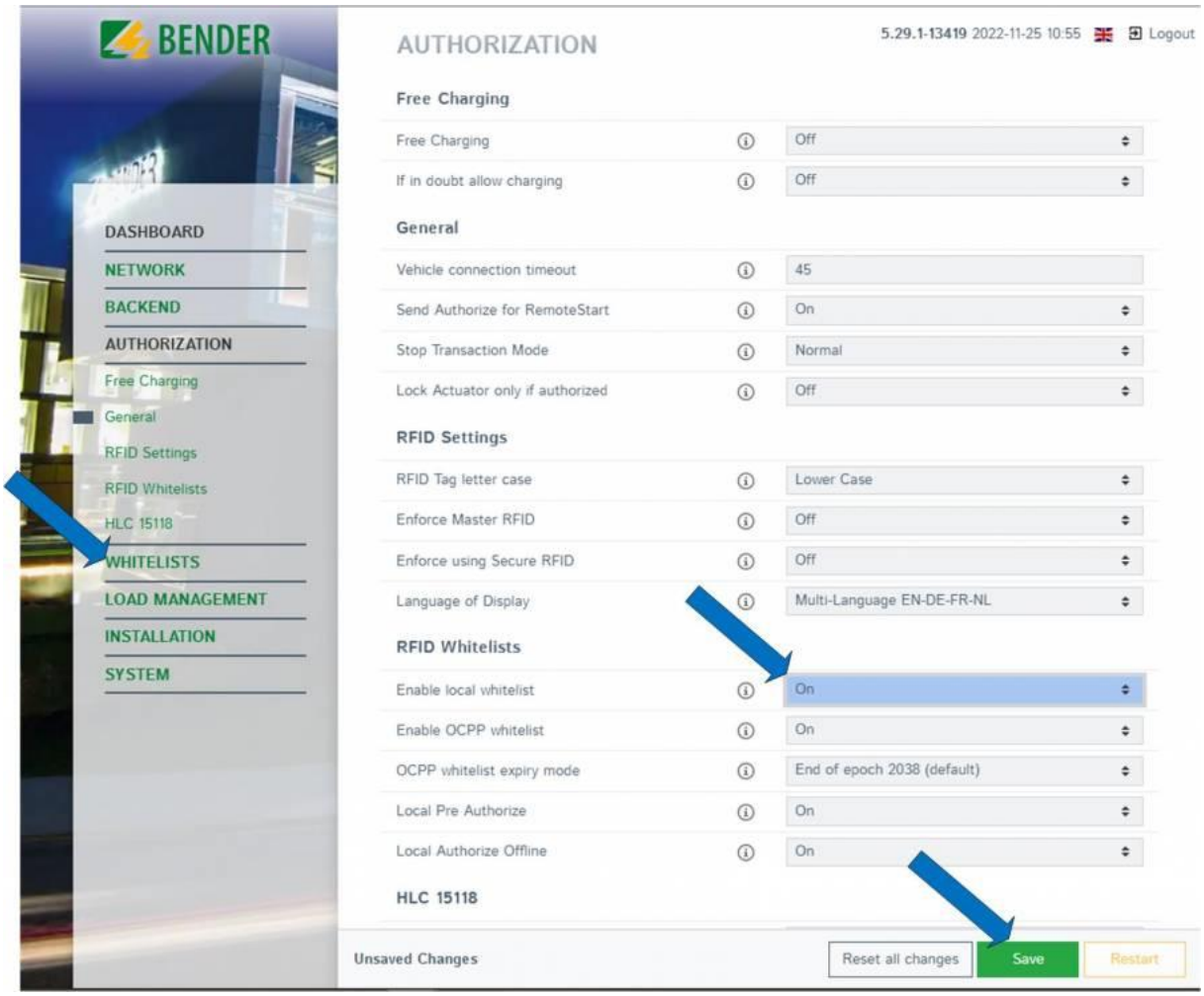
Configuration

To use this option, you must set the `Enable local whitelist` parameter (also known `as Enable fixed local list (FLL`)) to "On".

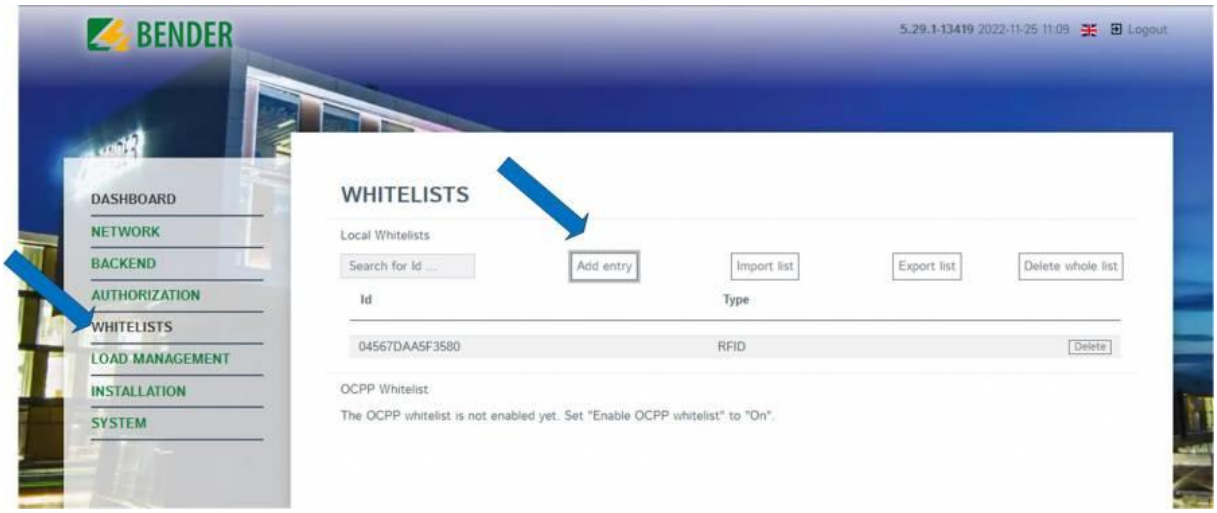
You can then enter all the UIDs you want in the List of entries in local whitelist. These must be separated by a colon. Make sure you are using the correct format (see Authorization).

Sample configuration in WebUI 2.0

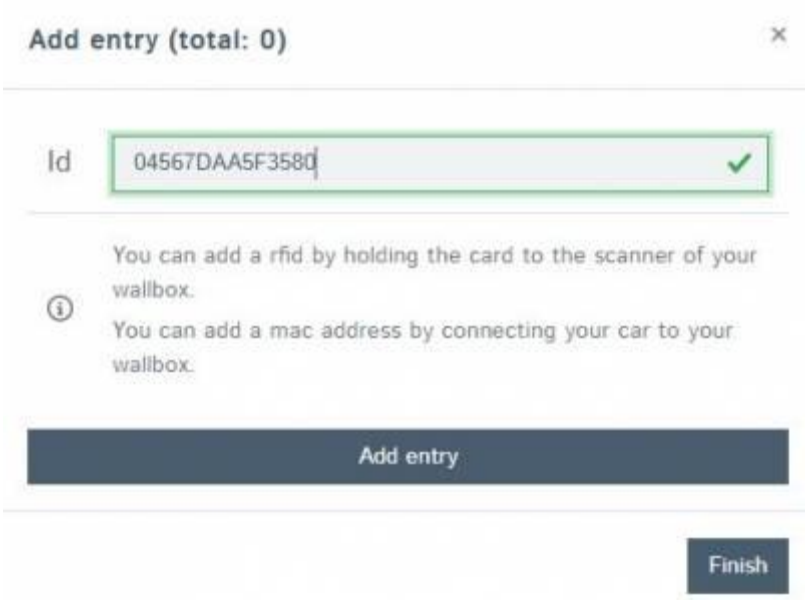
To activate the RFID local whitelist, the whitelist must be enabled in the "Authorization" submenu with the "Enable local whitelist" parameter. The "Whitelists" submenu will then appear in the left menu selection.



The menu selection will take you to the local whitelists. There you have the option to manage the entry within the whitelist. The list can be populated, exported, imported, or deleted using the function keys.

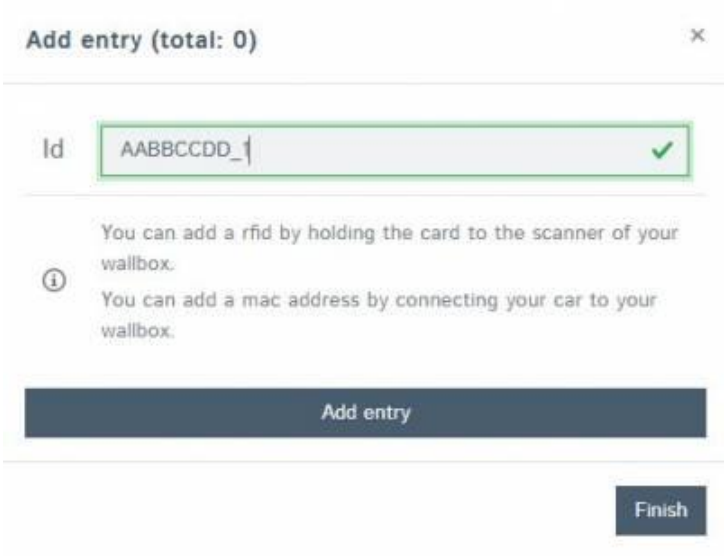


The "Add Input" button will open a new window and put the charge controller into RFID learning mode. This means that in this mode, all RFID tags can now be entered manually or read via RFID. To do this, the RFID tags can be held in front of the reader one by one. A newly read RFID tag is automatically added to the list. To complete the action, confirm the process by clicking the Finish button.



If there is a need to differentiate between access authorizations between two charge points (master/slave operation), a postfix for the assignment can be added to the RFID items. The

example shows an input that can only be authorized for charge point 1 (master), but is rejected at charge point 2 (slave).



6. Meaning of LEDs (RFID105/110/117)

The card reader recognizes and processes MiFARE-compatible RFID tokens (list of compatible RFID cards) in credit card format and as key fobs. The supported types include MiFARE Classic, DESFire EV1, DESFire EV2 and the copy-protected type DESFire EV2-J for EV charging.

Hold the RFID token against the card reader for at least 2 seconds to read it. The receiving antenna is installed directly behind the outlined circle. If the card is recognized, the integrated LED ring rotates.

The status LEDs have the following meanings:

Behavior	**Meaning**
GREEN Luminous	The charging point is ready and free to use.
YELLOW glow	The charge point is reserved for a user by the backend. The charge point completes the previous charging process. This can take up to 30 seconds.
WHITE rotating	The requested RFID card is requested from the backend. Please wait.
Flashing BLUE every half second	Charging card or access device has been accepted, charging process can be started.
Flashing BLUE every 2 seconds	The vehicle is loading.
GREEN-YELLOW-BLUE flashes five times	The offered charge card has been refused.
GREEN-YELLOW-BLUE flashes continuously	The charge point is not operational due to a technical error.
GREEN-YELLOW-BLUE clear	A software update is being performed on the charging station. The process takes up to 10 minutes.

7. Power Management & DLM Settings

7.1 Intro

All performance-related parameters are listed here. It also describes how **to set up Dynamic Load Management (DLM)** and ISO 15118 Powerline Communication (PLC). Please note that all parameters should only be changed by a qualified technician. In certain circumstances, improper configuration can create a fire hazard.

Installation

Operator Current Limit (A)

The "Operator Current Limit" is the maximum current in amperes that the charge point can supply. This value is indicated on the vehicle and must under no circumstances exceed the maximum current for which the charging point is designed. However, below this limit, the value can be freely chosen even during a charging process. This value should only be entered or changed by a specialist.

Remark

With this setting parameter, it is possible to "downgrade" existing hardware.

Example:

A charging station designed for 22 kW (three-phase, 32 A) can be converted to an 11 kW charging station by changing the "Operator Current Limit" parameter value. The maximum current supplied by the charging station for charging is limited to 16 A.

Power Source Voltage

The effective value (Root Mean Square - RMS) of the electrical voltage between a conductor and the neutral conductor that connects the charge point to the power supply must be entered here. The standard value of 230V AC applies to Central Europe. The value always refers to one phase. Therefore, 230V AC must be input, even for a three-phase connection. This value should only be entered or changed by a specialist.

Phases connected to the ChargePoint

Here you can select whether the charging point is operated single-phase or three-phase or is connected to the electricity grid.

- For a single-phase connection: you can choose between "Single-phase system" or "Single-phase system (IT ground)". IT grounding stands for a specific type of grounding (Isolé Terre).
- For a three-phase connection: always select "Three-phase system".

This value should only be entered or changed by a qualified technician.

7.2 Definition of Current Limits

Parameter	Menu	Description	Hardware configuration of the charging stations	Case 1: 1 EVSE	Case 2: 2 EVSE (Dual Power Supply)	Case 3: 2 EVSE (Single Power Supply)
Maximum current [A]	Manufacturer	The hardware current limit of the EVSE.	Set up via manufacturer role.	Available	Available	Available
Current carrying capacity of the supply line [A]	Manufacturer	The hardware power limit of a charging station with two sockets and one supply cable.	Set up via manufacturer role.	Not available	Not available	Available
Installation Current Limit [A]	Installer	The current limit of the installation.	Set via operator role.	Available per EVSE	Available per EVSE	Available for the complete charge point
Operator current limit [A]	Operator	The operator's power limit.	Set via operator role.	Available per EVSE	Available per EVSE	Available per EVSE

Explanation of the parameters:

- **Maximum current [A]**: The maximum current that the EVSE's hardware can handle, set by the manufacturer.
- **Current carrying capacity of the supply line [A]**: The maximum current carrying capacity of a charging station with two sockets and one supply cable, determined by the manufacturer.
- **Installation current limit [A]**: The maximum current limit set by the installer shall be equal to or lower than the manufacturer's limit in cases 1 and 2, and equal to or lower than the charging station limit in case 3.
- **Operator current limit [A]**: The current limit set by the operator must be equal to or lower than the installation limit.

7.3 Dual Charge Point with Single Power Line

Please note:

The single power line load balancing feature is only available from firmware 5.29.1 onwards and can be used in conjunction with the DLM algorithm.

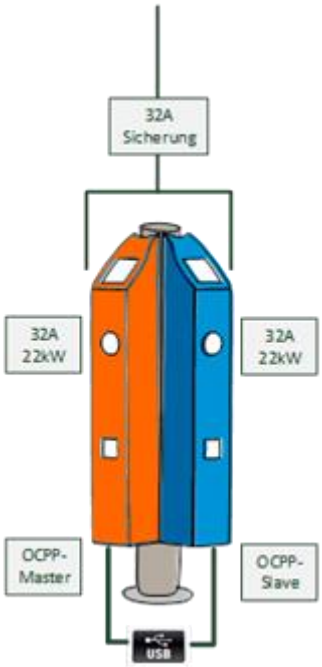
Example:

The double charging point may distribute a maximum of 22kW (32A). Each charge point can offer 22kW (32A) individually, but both charge points together may not offer more than 32A in total.

Sample Configuration

Parameter	Value	Description
Maximum current per charging point	32A	Each charging point can offer 32A individually.
Maximum Combined Current	32A	Both charging points together may not offer more than 32A.
Firmware Requirement	From version 5.29.1	The single power line load balancing feature is available from firmware version 5.29.1 and requires the DLM algorithm for optimal operation.

This configuration allows both charge points to make the best use of the available power, while preventing the total load from exceeding the 32A limit.



Requirements

The charging points operate in a master/slave configuration. See settings

Single Power Supply Configuration

The following settings must be done in the manufacturer menu on the legacy interface (WebUI 1.0):

1. Connect via USB:
    - Open the legacy interface via the URL: 192.168.123.123/legacy/manufacturer/manufacturer.
2. To adjust settings:
    - Make sure the settings are adjusted on both the master and slave controllers.
3. Save:
    - Save all changes.

Important: The above steps must be performed for both the master and slave controllers to ensure correct operation.

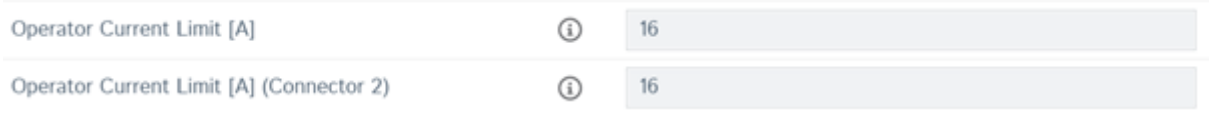
Master/Slave Modus	Master	Ein 'Master'-Controller übernimmt die Backend-Verbindung und kann Transaktionen auf den Slaves starten und stoppen. Der'Slave'-Controller verbindet sich mit einem Master als wäre dieser sein Backend. Einige andere Parameter werden beim Einschalten automatisch angepasst. WICHTIGER HINWEIS: Unterstützt wird aktuell ein Setup mit 1 Master und 1 Slave.
Ladestation mit einer Zuleitung	An	Diese Funktion schaltet eine Lastregelung zu, sofern beide Ladepunkte einer Doppel-Ladestation über eine gemeinsame Zuleitung versorgt werden.
Einstellungen 'Ladestation mit einer Zuleitung' sind für die Rolle Installateur zugänglich	An	Die Einstellung zu 'Ladestation mit einer Zuleitung' wird für die Rolle Installateur im WebUI 2.0 zugänglich.
Stromtragfähigkeit der Ladestation [A]	32	Durch die Verdrahtung und/oder Sicherungselemente vorgegebener maximaler Summenstrom der Ladestation in Ampere.

Next, switch to the WebUI 2.0

- Login via operator access
- Go to the WebUI 2.0 interface and log in with operator access
- Installation Menu
- Setting the maximum current carrying capacity of the power supply line

Be sure to observe and configure the phase rotations within the charging station to ensure optimal load distribution.

In the menu item Charging management, the operator can set the power limit for each charging point (1 and 2) separately.



7.3 ISO 15118 Configuration

The charge controller enables charging via the ISO 15118 (Power Line Communication) protocol. However, currently only a few vehicle models can communicate with the charge point via this standard.

Current settings

- Mode 1: Off → High level communication is disabled.
- Mode 2: On (Encouragement) → High level communication is enabled. Duty cycle of 5% is signaled for the first 2 seconds. After that, the nominal duty cycle is used.
- Mode 3: On (Offer) → High level communication is enabled. Only nominal duty cycle is used.
- Mode 4: On (Force) → High Level Communication is enabled. Duty cycle of 5% is always signaled.
- Mode 5: On (Ed2) → High level communication is enabled. HLC can begin at any time, regardless of the current duty cycle according to ISO 15118 Second Edition.

From Release 4.63

- Mode 1: Off → High level communication is disabled.
- Mode 3: On (Offer) → High level communication is enabled. Only nominal duty cycle is used.
- Mode 5: On (Ed2) → High level communication is enabled. HLC can begin at any time, regardless of the current duty cycle according to ISO 15118 Second Edition.

7.4 Dynamic Load Management (DLM)

The Dynamic Load Management (DLM) offers the possibility to optimally adjust the charging currents of multiple charging points to the available power. The DLM is designed as a local charging management system. The charging points are connected to each other via a network connection and are configured as required via their web interface.

There is no need for additional devices such as gateways, controllers, or interface adapters. This makes it easy to expand the load management. New charging points can be easily added and integrated into the network. In addition, all charging points that use the Bender controller can be deployed. This means that charging points from different manufacturers can also be used. The compatibility of the devices means that expansion is possible even after years without disrupting the existing technology.

Local charging management can also be integrated into existing or future energy management systems via standard interfaces such as EEBus, Modbus-TCP/IP or OCCP. This makes it easy to implement surplus charging on the PV system or integration into building/control technology. The backend operator can also intervene via OCPP communication. The CC613 supports OCPP smart charging profiles and also the so-called backend charging management, where the operator or CPO can intervene in addition to the local charging management.

Alternatively, local load management can also be supplemented with local load measurement. This is often required if the new charging infrastructure to be acquired is to be connected to the existing home connection of a building, for example, and the HAK is to be used jointly. However, the possible power reserves of the power connection for the charging infrastructure are usually not known. Or the power connection must be used optimally and not cause additional costs (peak shaving).

To do this, an (additional) energy meter is simply integrated into the charging point network via Modbus-TCP and included in the calculation of the currents.

Technical Requirements

The house connection, the supply line or the branch of a subdivision can be limiting factors for the charging current at charging points. This constraint initially represents the upper limit of the total flow to be distributed. Thus, in a subdivision at a charging point that has, for example, 32 amps (22 kW) available, only the following installations can be implemented without dynamic charging management:

Without charging management, the charge point would always reserve the maximum charging current. This means that every electric vehicle is guaranteed to be able to be charged at maximum current at all times throughout the entire charging process. Very few vehicles do this. A current of 32A is also not used for the entire charging or parking time that the vehicle is connected. But the maximum current of 32A is permanently reserved for the charging point when it is plugged into the LP.

Due to the constant supply of charging current, theoretically only one 22 kW charging point can be connected to the subdivision without exceeding the connected load. If the need for charging infrastructure increases, the subdivision should be expanded or renewed.

Load management can be used to solve the problems described above. Charging management can distribute the reserves of unused charging points to other charging points and allows the installation of charging points whose theoretical total output exceeds the actual available power of the power supply.

The currents are monitored with phase precision. This means that it takes into account whether the vehicle is charging on one or more stages. The phase rotation of the charging points in relation to each other is also taken into account. These special details make it possible to optimally distribute the available flows.

Operating Modes of Charge Management

Load management has different operating modes and options to optimize the load according to availability and consumption. Depending on how a system is set up, there are sometimes, in addition to the charging points, consumers that cannot be controlled (such as consumers in a building or house or business) and obviously affect the total amount of electricity available.

The most common configurations are therefore the following:

- Charge management without additional consumers (and therefore without external measurement)
- Charging management with additional, partly unknown, consumers and external metering

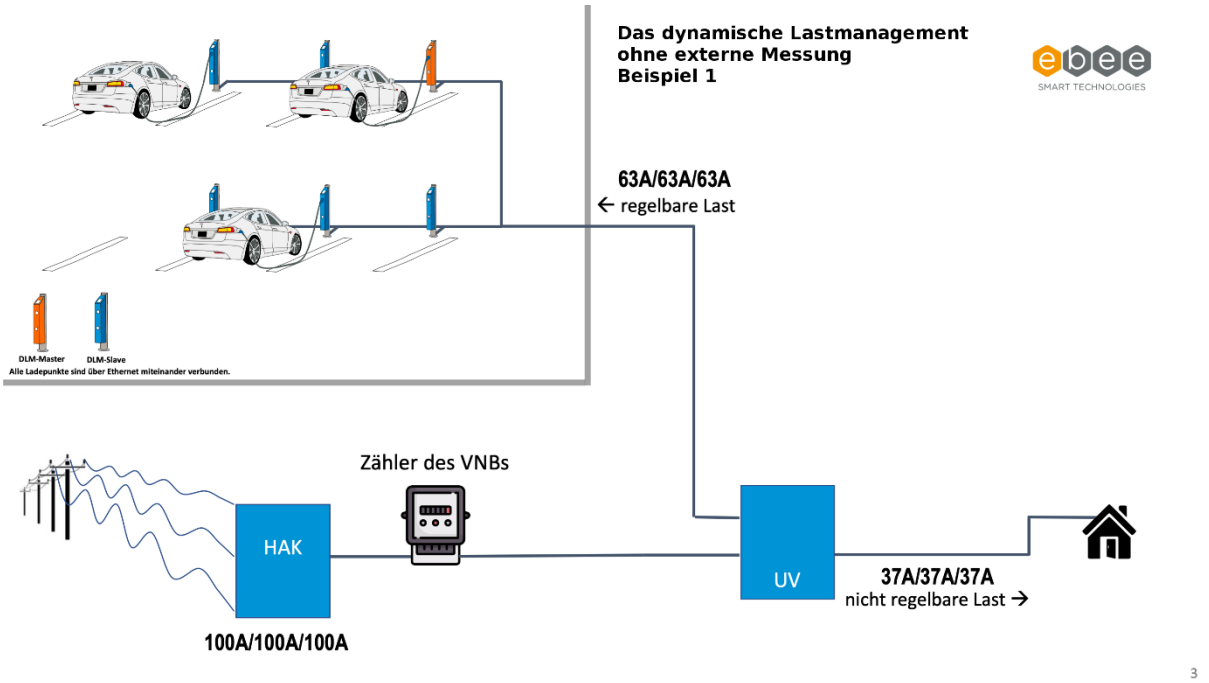
Both application cases must optimally distribute the charging currents and not exceed a definable load limit in order to avoid overloading.

7.4.1 Load management without external measurement

A fixed upper limit of the flow to be distributed is known and set. The charging management only needs the current charging currents of the charging points. A fixed current value (e.g. 63 A) is assigned to the group of charging points. The 63 A are distributed individually per phase at the charging points.

The following two scenarios illustrate where the use of such charging management makes sense:

- A 100 A connection provides a building and the charging infrastructure
    - The maximum load of the building is known, 37 amps (including reserve/margin) must be reserved for this.
      The remaining 63 A are allocated to the charging infrastructure via the DLM and distributed among the charging points by the charging management.
    - A charging station with 63 A
      There are no other consumers connected to this house connection except for the charging points.

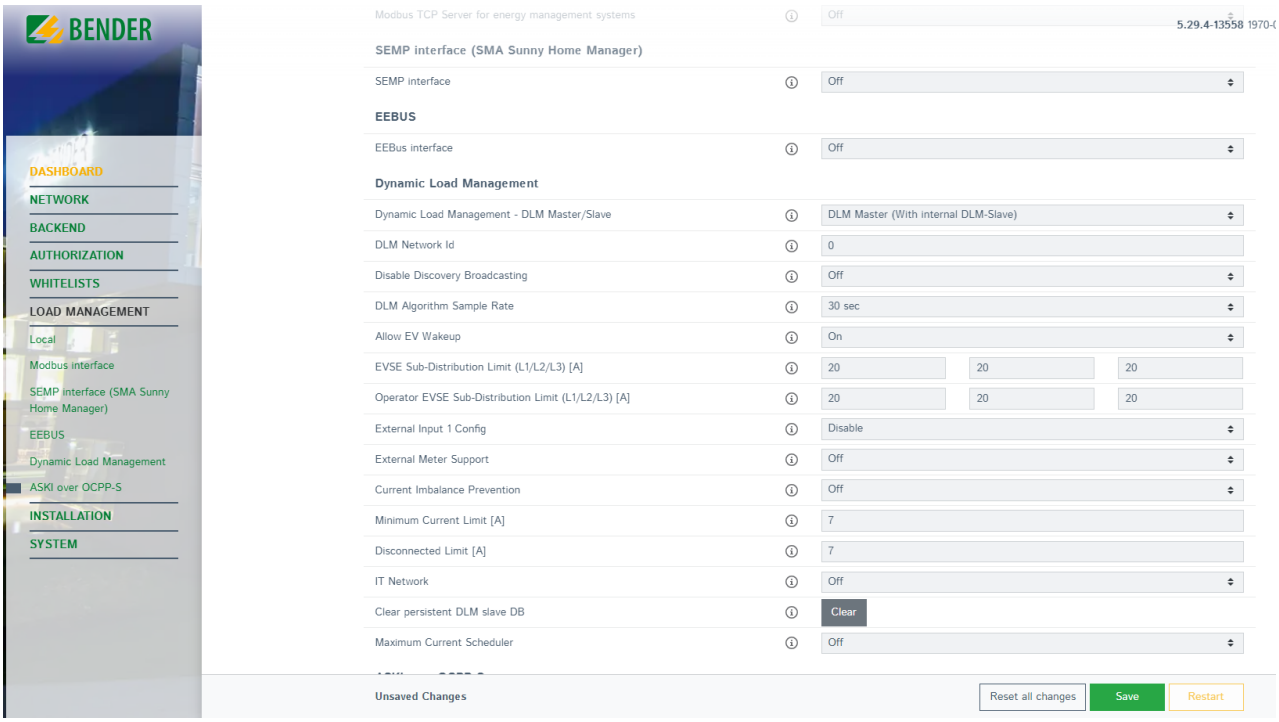


3

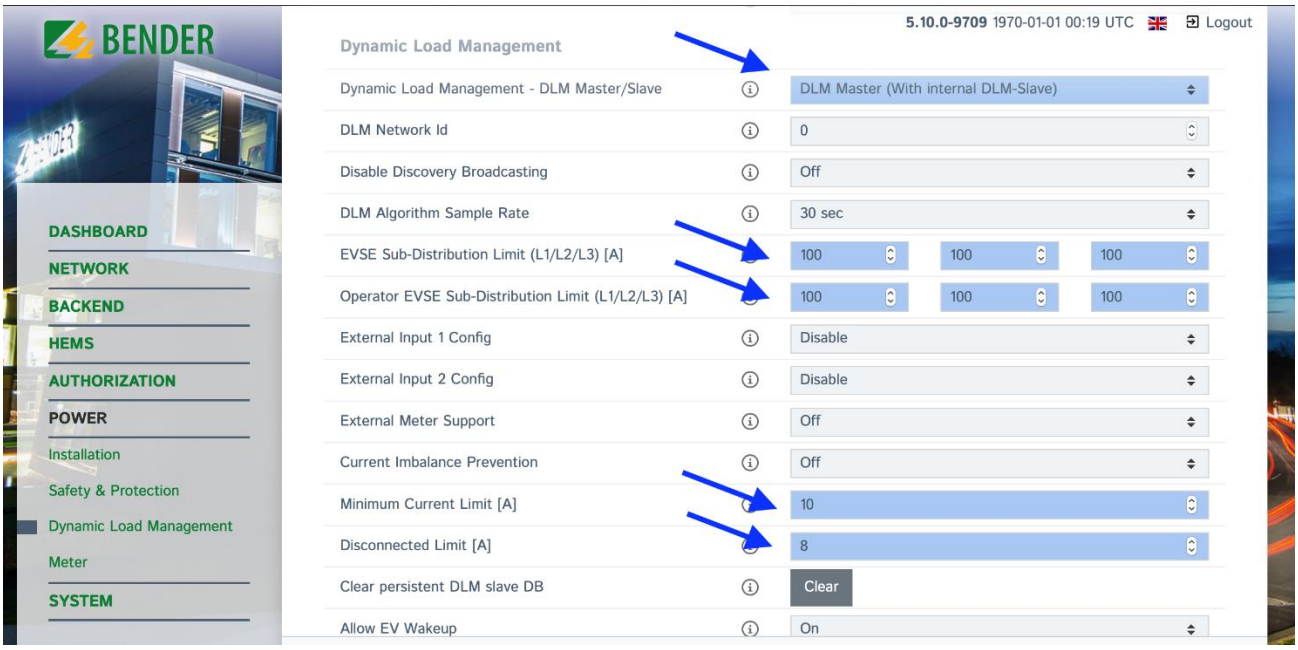
Configuration DLM Master with Internal Slave

Log in with at least `operator` rights.

1. Go to LOAD MANAGEMENT and set to DLM Master (With internal DLM-Slave).



2. Configure parameters
    1. EVSE Sub-Distribution Limit (L1/L2/L3) in A
    2. Operator EVSE Sub-Distribution Limit (L1/L2/L3) in A (may be the same as above)
    3. Minimum Current Limit in A. Usually 8A
    4. Disconnect Limit in A (when the connection to the Master is lost). Usually 8A
    5. Save & Restart



7.4.2 Load Management with External Measurement

The DLM needs to know the total load on the house connection, i.e. not only the current charging currents of the charging points, but also the current that is currently flowing through other consumers. This means that the total flow of electricity to be distributed to the charging points (LP) can be dynamically adjusted. The "consumption" of the building's electricity is not known and taxes are subject to change. The charging points or the DLM have to react to these sometimes spontaneous and uncontrollable load changes.

There are also often HAKs (house connection boxes) that, due to their design "on paper", would not allow the additional connection and operation of charging stations. No fixed power can be reserved for the charging technology. However, since the load on the building is not always the same, such reserves can be measured with a continuous power or load measurement on the HAK/room. These can be passed on to the charging stations via the DLM.

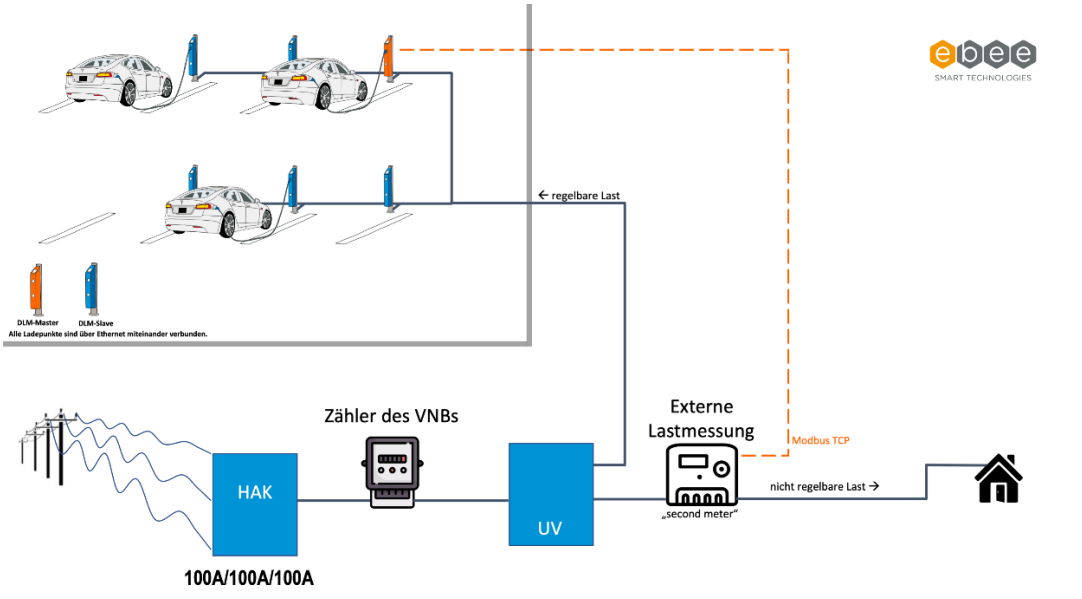
The charging current of an electric vehicle is adjustable and the maximum available charging current is specified to the vehicle by the charging point. The vehicle regulates its maximum charging current in accordance with this specification. Depending on the charging time and the charge level of the battery, the maximum possible power of the charging point, e.g. 11 kW or 22 kW, is rarely used. The charging management takes this into account and can therefore distribute the surplus to other charging points.

The additional meter required in this scenario can be installed directly behind the grid operator's meter (including EVSE sub-distribution) or in the sub-distribution behind the charging point branch (excluding EVSE sub-distribution). This also partly depends on the installation conditions or the structure of the installation. This means that the load of the additional consumers can be measured and taken into account in the calculation of the DLM.

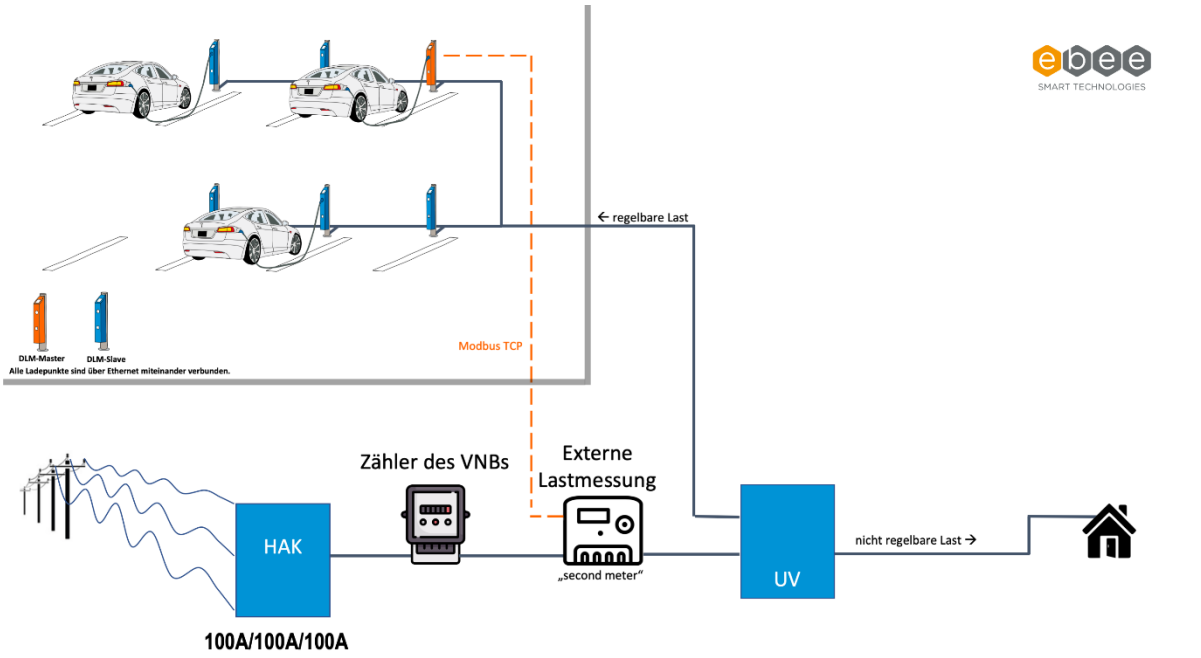
The following images are intended to illustrate the structure:

Load management with support of an external meter (DLM)

Excludes EVSE Subdistribution (Recommended Variant):



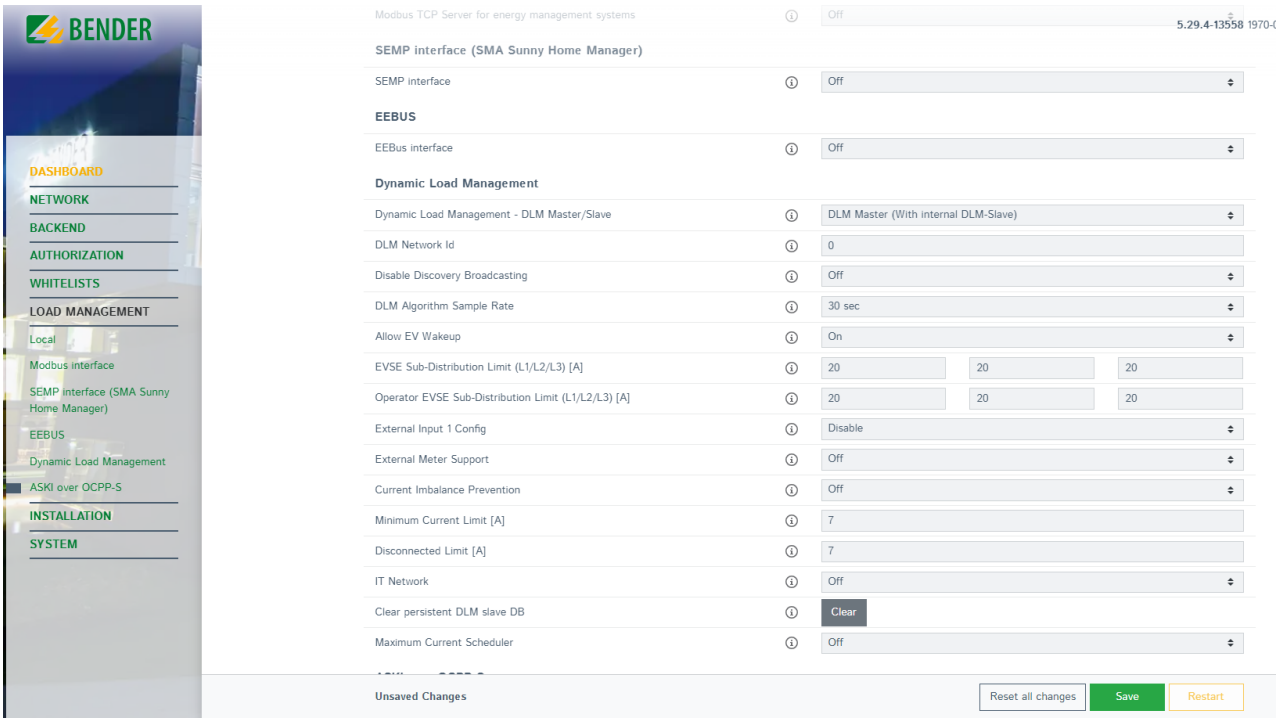
Including EVSE sub-distribution:



Configuration

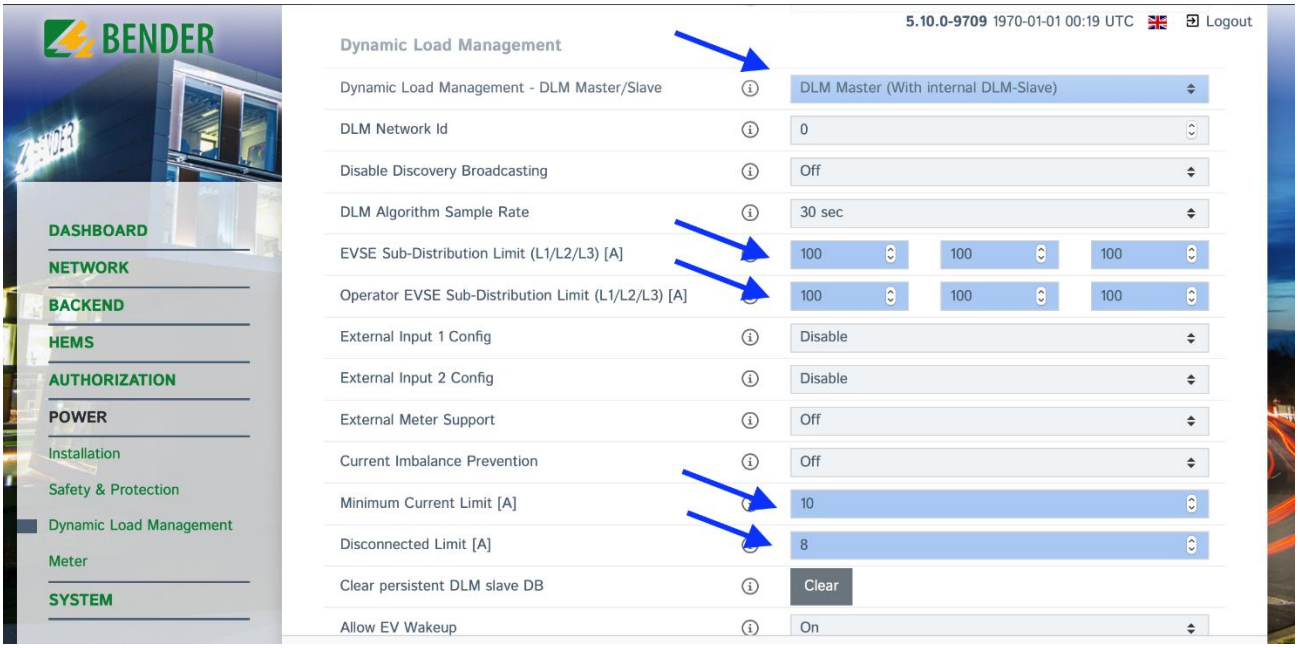
Log in with at least `operator` rights.

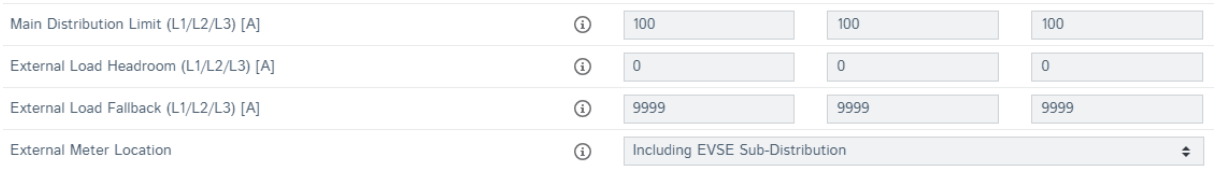
1. Go to LOAD MANAGEMENT and set to DLM Master (With internal DLM-Slave).



2. Configure parameters
    1. EVSE Sub-Distribution Limit (L1/L2/L3) in A

2. Operator EVSE Sub-Distribution Limit (L1/L2/L3) in A (may be the same as above)
3. Minimum Current Limit in A. Usually 8A
4. Disconnect Limit in A (when the connection to the Master is lost). Usually 8A
5. Turn on External Meter Support
6. There will be an extra field next to 'Meter Configuration (Second)', indicating the meter used. E.g. Modbus Siemens 7KM2200 (TCP)
7. Make sure that the IP address of the meter is in the same range as the networking of the charging stations
8. Set Main Distribution Limit (main connection, or the distribution board where the meter is located)
9. Indicate the placement of the meter at External Meter Location. Typically Including EVSE Sub-Distribution
10. Save & Restart





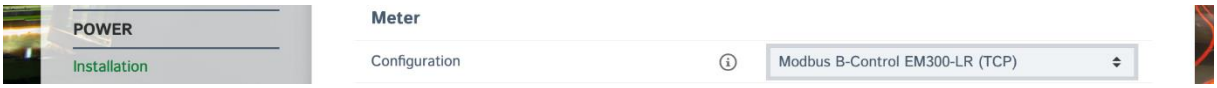
7.5 MODBUS TCP Meters

To perform this configuration, you must be logged in with at least operator rights.

1. Select a Modbus TCP meter type. These are marked with "(TCP)"

Or

Select the Charge Meter (OCPP Meter) under Configuration:



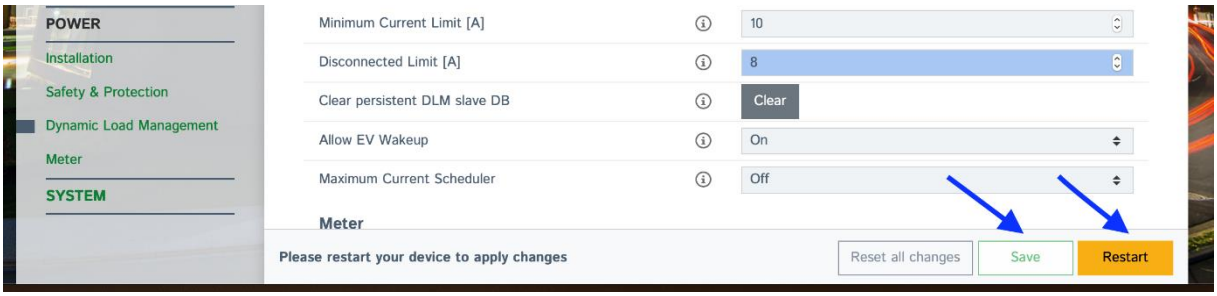
- Enter the IP address and the Modbus TCP port number of the meter.
- You can get this information from the display or manual of the meter you're using.

Or

The meter for the external measurement (Second Meter) under Meter Configuration (second):

- Enter the IP address and the Modbus TCP port number of the meter.
- You can get this information from the display or manual of the meter you're using.

2. Save configuration & restart.

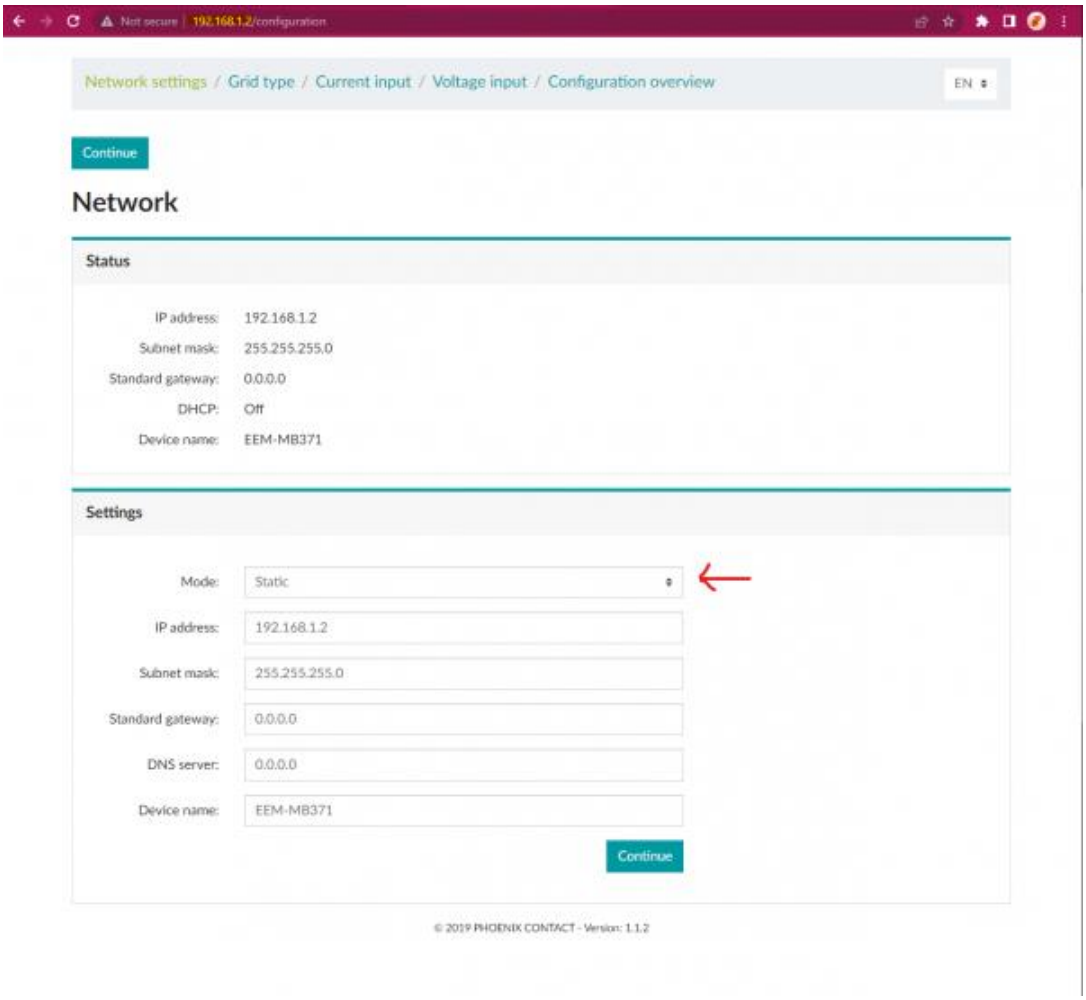


Phoenix Contact EEM-MB371

Please note that the Phoenix Contact EEM371/370 meters are equipped with a static IP address. To connect the energy meter to your local network, you need to configure it with the appropriate IP settings that are suitable for your LAN. You can reach the meter by adjusting the LAN settings

of your laptop to the standard range of your laptop. If you can reach the meter, adjust the IP address so that it is in the same range as the charging stations.

Open your preferred browser and navigate to http://192.168.1.2 or the meter's IP address. Click on the drop-down menu and set the mode to "Dynamic (DHCP)".



7.6 Phase-specific charging management

A rechargeable electric vehicle usually has a so-called "on-board charger". This charger, which is permanently installed in the car, is connected to a suitable charging point by a cable. The on-board charger is usually single-phase or three-phase. This means that in a three-phase network (three-phase current) either one phase or three phases are loaded.

The charging current communicated by the charging point always applies to all phases, regardless of whether the vehicle is charged on one or more phases.

Competitor load management systems often assume that all phases are always loaded equally, regardless of the actual load on each individual stage. This means that at a charging point where a vehicle charges single-phase at 1 x 16 amps, the remaining 2 phases are also reserved at 16 amps each, although the second and third stages are not actually loaded. The DLM has an automatic detection system to determine whether the connected vehicle is loading the network one-phase or three-phase. If it is a vehicle with a single-phase charger, the load is reserved only on the corresponding phase, the rest remains available for other vehicles. Every phase rotation is taken into account. For more information, see the "Phase Rotation" section.

7.7 DLM Master Errors

Failure of the DLM Master

Possible causes that lead to failure of the master's programme:

- Voltage drop on the charge controller running the DLM Master software.
- Connection error to the network (LAN, WLAN, GSM, USB) at the charging point in which the DLM Master is located.

Preventive measures

The above-mentioned events can be avoided by running the DLM Master software on a charge controller that is operated separately in a distribution box or in a network installation. This charging controller is then operated as a stand-alone variant and does not control a charging point. By running the power supply through the low-voltage distribution box or the network installation, the risk of power failure and the connection to the network is minimized.

In case of voltage drop

If the power supply of the charge controller in which the DLM Master software is running fails, the DLM slaves fall back to their individually set separate limit [A]. The charging currents then become static. In total, the separated limits of the DLM slaves must not exceed the value of the maximum available current.

A voltage drop at the charging point in which the DLM Master software runs can usually not occur due to a fault in the vehicle or due to poor operation by the charging customer in the case of charging points that comply with the calibration law. This is because the charge controller has a separate power supply. This means that the DLM Master software can continue to work even if an RCD/MCB (FI/LS) is activated by the vehicle.

In case of connection failure

If the network connection of the charge controller in which the DLM Master software is running is interrupted, the DLM slaves will react in a similar way to a voltage drop. Once the network connection is restored, the system will automatically recover and be controlled by the DLM Master again.

7.8 Phase Rotation

What does ChargePoint phase rotation mean?

Charging points are usually designed as single-phase or three-phase. This means that a car can charge at such charging points via the external line L1 (single-phase) or via the external lines L1, L2, L3 (three-phase). The phase position is always 120° to each other. To ensure that the charging management optimally distributes the charging current and avoids unbalanced loads, the information about the phase position or phase rotation must be set or communicated for each charging point. In order to better distribute the load, the phases are rotated in the subdivision.

Example:

Charge point 1

Charge point	Network
L1 ⇒	L1
L2 ⇒	L2
L3 ⇒	L3

Charge point 2

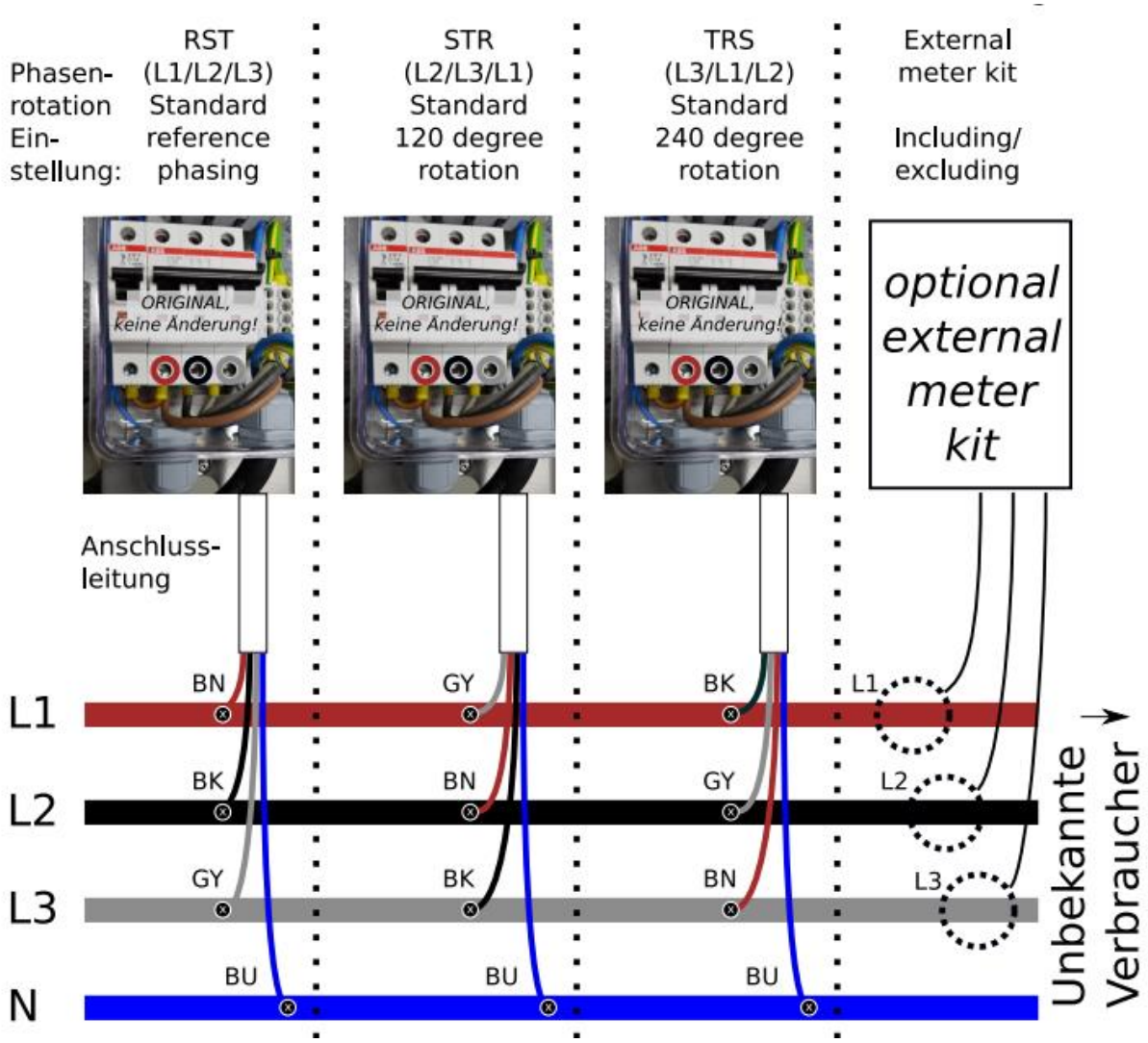
Charge point	Network
L1 ⇒	L2
L2 ⇒	L3
L3 ⇒	L1

Charge point 3

Charge point	Network
L1 ⇒	L3
L2 ⇒	L1
L3 ⇒	L2

This rotation is carried out in order to distribute the load caused by single-phase loading cars as evenly as possible across all phases.

The parameter "Phase rotation of the ChargePoint" is set in the charging point itself as intended by the installer for this charging point.


Phasen-
rotation
Ein-
stellung:
RST
(L1/L2/L3)
Standard
reference
phasing
STR
(L2/L3/L1)
Standard
120 degree
rotation
TRS
(L3/L1/L2)
Standard
240 degree
rotation
External
meter kit
Including/
excluding
ORIGINAL,
keine Änderung!
optional
external
meter
kit
Anschluss-
leitung
L1
L2
L3
N
BN
BK
GY
BU
Unbekannte
Verbraucher

8. Firmware Updates

Via Backend

Firmware updates are usually done automatically when connected to the backend.

Manual with Computer and USB Cable

Access to the controller's configuration interface. Under "System", select "Firmware Update", browse for the .deb file, and start the update. The process can take up to 15 minutes.

With USB stick

Make sure that the USB Firmware Update option is activated. Save the installation file in .deb format as sw_update.deb in the root directory of the USB flash drive. Insert the USB flash drive into the controller. The update is complete when the green "READY" LED flashes rapidly.

USB stick functions

Requirements

- A blank USB stick formatted with Windows fat32.
- A password file on the USB stick called USB_PASSWORD, with the operator password in plain text.

USB flash drive firmware update

Insert the USB stick into the controller and wait for the process to complete, indicated by the green "READY" LED flashing rapidly. The controller will restart automatically.

Reading log files via USB stick

Create an empty file called FIELD_ENGINEER in the root directory of the USB flash drive. Insert the stick into the controller, which will write all the log files and status information on the stick. The process is complete when the green "READY" LED flashes rapidly.

9. Error documentation

Provides a list and explanation of possible error messages and their solutions. This section is crucial for troubleshooting and maintaining operational efficiency.

Error code	Error activation message	Error resolution message	Transaction and charging is stopped	Notes	Corrective actions
groundFailure	Residual current detected via sensor	Residual current situation resolved	Yes	Internal RCMB device (yellow coil). This also detects DC residual current.	The safety mechanism is reset to its original state every time the cable is unplugged from the charging point. Otherwise, the error is automatically reset after a delay of 10 seconds if the EV was unplugged. In case the RCMB version is older than or equal to D0469, the delay is 15 minutes. If the problem persists, please check the yellow current transformer (coil) and its connection.
mode3Error	Vehicle signals error	Vehicle error resolved	No	Mode3 errors.	Disconnect EV and try again. If that doesn't help, follow EV's instructions.
mode3Error	Vehicle diode check failed - tamper detection	Vehicle with diode problem disconnected	Yes	Mode3 errors.	Disconnect EV and try again. If that doesn't help, follow EV's instructions.
aboutCurrentFailure	MCB or type 2 socket triggered	MCB type 2 reconnected	Yes		MCB needs to be re-armed, requires a maintenance visit.
aboutCurrentFailure	MCB or domestic socket triggered	MCB domestic socket reconnected	Yes		MCB needs to be re-armed, requires a maintenance visit.
groundFailure	RCD Fault	RCD reconnected	Yes	RCD device.	Up to a certain point this will be corrected automatically.

Error code	Error activation message	Error resolution message	Transaction and charging is stopped	Notes	Corrective actions
otherError	Surge Protection Device (SPD) tripped. Replace.	SPD triggered	No	External SPD device.	Surge Protection Devices (SPD) need to be replaced.
powerSwitchFailure	Contactor welded	Contactor weld resolved	Yes		Very likely requires a maintenance visit with high priority as it is an indication there might now be a properly disconnected socket when no plug is inserted.
otherError	Backend disconnected	Backend disconnected	No		
connectorLockFailure	Plug locking failed	Plug locking failed	No		Typically caused by not fully inserted plugs, unplugging and attempting to plug again in most cases resolves the problem.
connectorLockFailure	Type 2 actuator stuck, cannot unlock	Type 2 locking actuator recovered	Yes		A mechanical problem may require a maintenance visit. An Unlock Connector or Hard Reset triggers another attempt to unlock.
connectorLockFailure	Could not detect type 2 locking actuator	Type 2 locking actuator detected	Yes		A mechanical problem may require a maintenance visit. A hard reset triggers another attempt to redetect the actuator type.
powerMeterFailure	OCPP meter not communicating	OCPP meter communication recovered	Yes		

Error code	Error activation message	Error resolution message	Transaction and charging is stopped	Notes	Corrective actions
powerMeterFailure	External meter not communicating	External meter communication recovered	No		
readerFailure	RFID reader not communicating	RFID reader recovered	No		

10. Troubleshooting LED Indication

Step-by-step troubleshooting for common scenarios such as USB connection issues, driver installation issues, and network connection failures. This section uses diagnostic LEDs for fault indication and resolution.

Malfunction/error message	Possible cause(s)	Solution
Chargecard is not read	1. Incorrect "LED Type" Setting (Factory Reset)	Check the setting
	2. Incorrect setting "RFID - Slave" (factory reset)	
	3. Unsupported Card Type	
No backend connection when using a cellular or Ethernet connection	Configuration of the cellular or Ethernet interface is incorrect	Backend connection type set up correctly?
No backend connection when using an Ethernet connection	Ethernet connection interrupted	Examine:
	• Is the activity LED on the Ethernet switch 10K1 flashing of the Ethernet cable connected to the network?	

	• Is the Ethernet configuration in the Network section complete and correct?	
	• Are routers and switches functional?	
Backend Connection Cannot Be Established Despite Network Connection	Backend configuration incorrect or incomplete	Comparison of the set values OCPP mode, ChargeBoxIdentity, OCPP URL of the backend and any access passwords with the specifications of the backend operator.
Backend Connection Cannot Be Established Despite Network Connection	Backend not ready	Examine:
	• Backend online and operational?	
	• Charging station and device type created in the backend?	
Connection interruptions to the backend	Poor reception conditions	Different positioning of the charge point or use of an external router, if necessary change of network operator for roaming-capable SIM cards.
No display, LEDs completely off	No power supply, backup fuse, circuit breaker or RCD tripped.	If necessary, disconnect vehicles, visually inspect charging station, switch blown fuse back on.
LED flashes green/yellow/blue, energy meter without display	The charging point is not energized, e.g. because the residual current circuit breaker has been switched off.	• Marking vehicles
		• Switch the RCD back on
		• If the error occurs again, check if the charging contactors 7Q1 or 9Q1 are stuck and repair if necessary.
Error message immediately after connecting the vehicle	Charging socket locking actuator is jammed or dirty	Clean the actuator, lock and unlock it several times manually with the red lever, restart the charging point. If this doesn't help, replace the actuator.
Other Errors	Other cause	In the "System" / "Overview" menu, you can use the "Download Log Files" button to save a ZIP file with diagnostic data of the charging station. This file may be made available to device manufacturer technicians for diagnostic purposes.

11. Technical Specifications & Contact

Technical Specifications

- **Model:** Powerstation TWO
- **Network interfaces:** USB, Ethernet, GSM
- **Safety standards:** IEC 61851-1:2017 / IEC 61851-21-1:2017 / IEC 61851-21-2:2018 / ISO 17409:2015
- **Dimensions:** 1400x290x185mm (HxWxD)
- **Weight:** 27kg

Contact

For further assistance or technical support, please contact:

- **Phone:** +32 33 18 38 50
- **Email:** support@powerstation.be
- **Website:** powerstation.be

For immediate assistance with configuration or operational issues, please refer to the troubleshooting section of this manual or contact our technical support directly.