

Konfigurationsanleitung

Für die Konfiguration Ihrer Ladestationen steht Ihnen das Technagon Webinterface zur Verfügung. Um Ihnen den Einstieg zu erleichtern, haben wir folgende Anleitung mit allgemeinen Informationen zum Webinterface und den Konfigurationsmöglichkeiten erstellt.

Inhaltsverzeichnis

1. WebUI	2
1.1 Webinterface	2
1.2 Admin	3
1.3 Dashboard	5
1.4 Network	5
1.5 Communication	7
1.6 Station	8
1.7 User Management	11
1.8 Software	16
2. OCPP-Keys	17
2.1 Quellen	17
2.2 Features	17
2.3 Konfiguration	22
3. OCPP Errors	25

1. WebUI

Voraussetzung für die funktionierende USB-Kommunikation mit dem Technagon PC sind Windows 11, MAC OS oder Linux.

Bei Windows 10 wird das Gerät zwar erkannt, der benötigte Treiber zur USB-Kommunikation mit dem Technagon PC jedoch nicht automatisch installiert.

Mögliche Fehlerbilder sind:

- Anmeldung im Web-Interface nicht möglich
- Browser bricht nach einer Weile ab

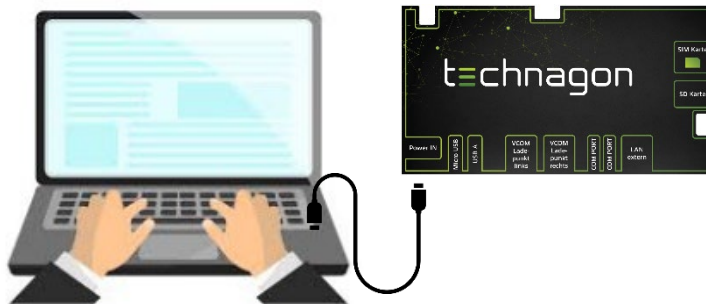
Um dies zu vermeiden, führen Sie bitte eine manuelle Treiberinstallation durch. Diese wird in folgender Anleitung beschrieben:

<https://technagon.de/wp-content/uploads/2023/07/Anleitung-Windows-10-Treiberinstallation-USB-Netzwerk.pdf>

1.1 Webinterface

Konfiguration der Anlage

Zur Konfiguration der Anlage steht Ihnen ein Web-Interface zur Verfügung. Verbinden Sie dazu einen Laptop mit einem aktuellen Web-Browser per microUSB-Kabel an die USB-Schnittstelle des Technagon PCs. Kontrollieren Sie, ob die Netzwerkeinstellungen Ihrer LAN Schnittstelle am Laptop auf DHCP stehen.



Melden Sie sich wie folgt am Web-Interface an:

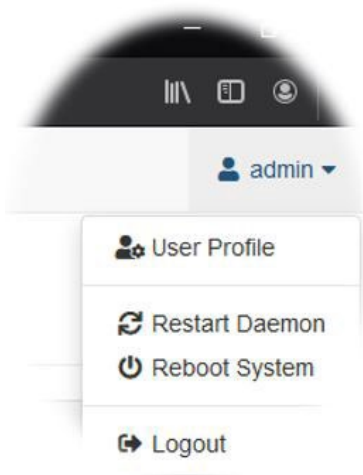
URL: `https://192.168.32.1`
 User: `admin`
 Password: `„Seriennummer der Anlage“`

Log In



1.2 Admin

Im Menüpunkt „admin“, der sich rechts oben befindet, hat man die Möglichkeit, Benutzereinstellungen vorzunehmen oder die Ladesäule bzw. den Daemon neu zu starten.



User Profile

Hier erhält der Benutzer die Möglichkeit, das Passwort zur Anmeldung am Web-Interface zu ändern:

Old Password: „Seriennummer der Anlage“
 New Password: „Gewünschtes Passwort“
 New Password (Repeat): „Gewünschtes Passwort wiederholen“

Change Password

Password

Old Password

New Password

New Password (Repeat)

Save

Advanced Settings

If unsure set to default

Show advanced settings

Default

HINWEIS

Es ist nicht möglich, das Passwort auf seinen Ursprung zurückzusetzen.

Des Weiteren lässt sich hier die Benutzereinstellung von „Default“ auf „Expert“ ändern. Dadurch gibt es in dem Punkt „User Management - Authentication“ weitere Einstellmöglichkeiten. Außerdem erscheint unter „Software“ ein Upload-Balken. Dies wird in den jeweiligen Kapiteln noch separat behandelt.

Restart Daemon

Bietet die Möglichkeit, den Client neu zu starten. Der Vorgang dauert nur wenige Sekunden.

Reboot System

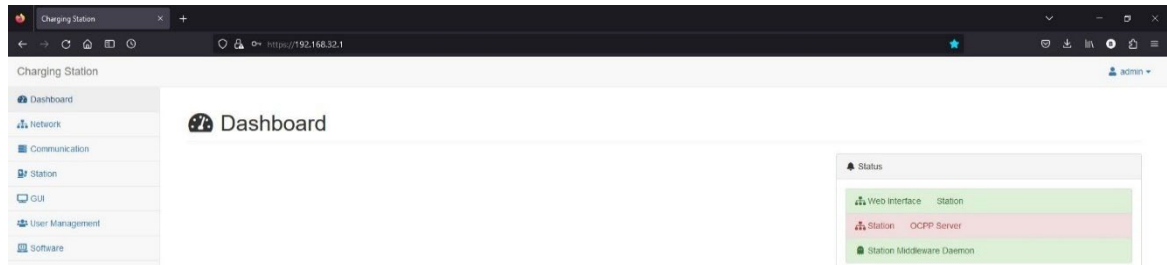
Die Ladesäule führt einen Neustart durch. Nicht nur der PC, sondern auch die Ladecontroller werden mit dieser Funktion neu gestartet.

Logout

Der Benutzer kann sich aus der WebUI ausloggen und die Anmeldeseite (Log In) wird wieder angezeigt.

1.3 Dashboard

Unter diesem Menüpunkt erhält der Benutzer Informationen über den Status des Systems. In diesem Beispiel besteht keine Verbindung zu einem OCPP-Backend-Server.



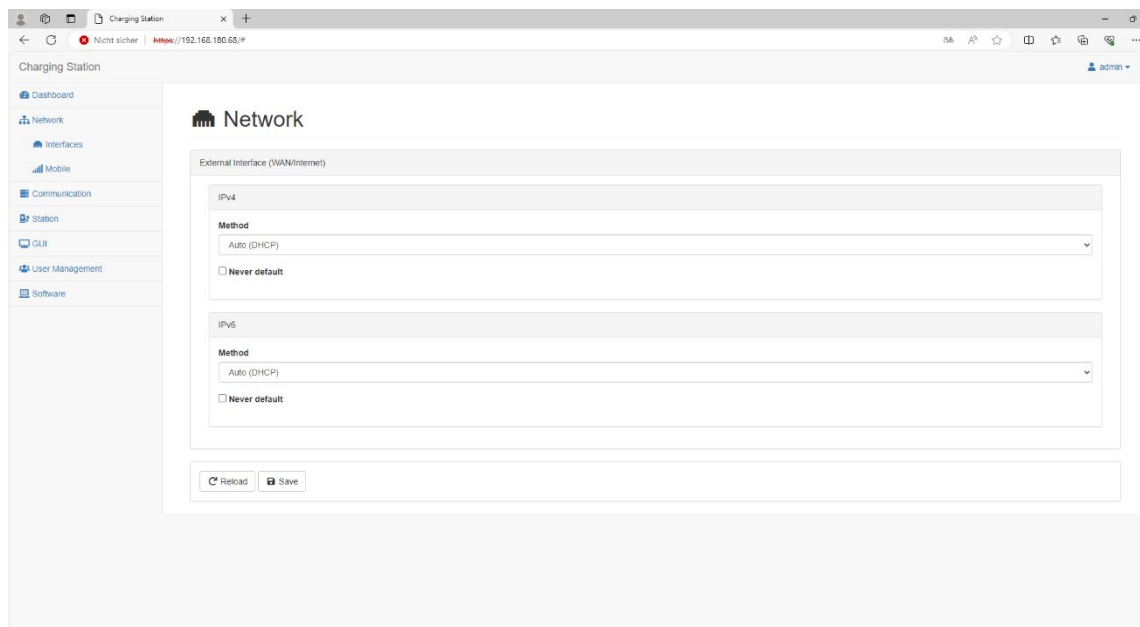
HINWEIS

Manche Einstellungen müssen nach Änderung gespeichert werden. Einige Einstellungen sind eventuell erst nach einem Neustart der Anlage oder des Clients aktiv. Einige Einstellungen sind sicherheitsrelevante Einstellungen und können das System „unsicher“ machen. Sollten Einstellungen geändert werden, welche die Sicherheit gefährden, ist unbedingt eine Freigabe vom Kunden erforderlich!

1.4 Network

Interface

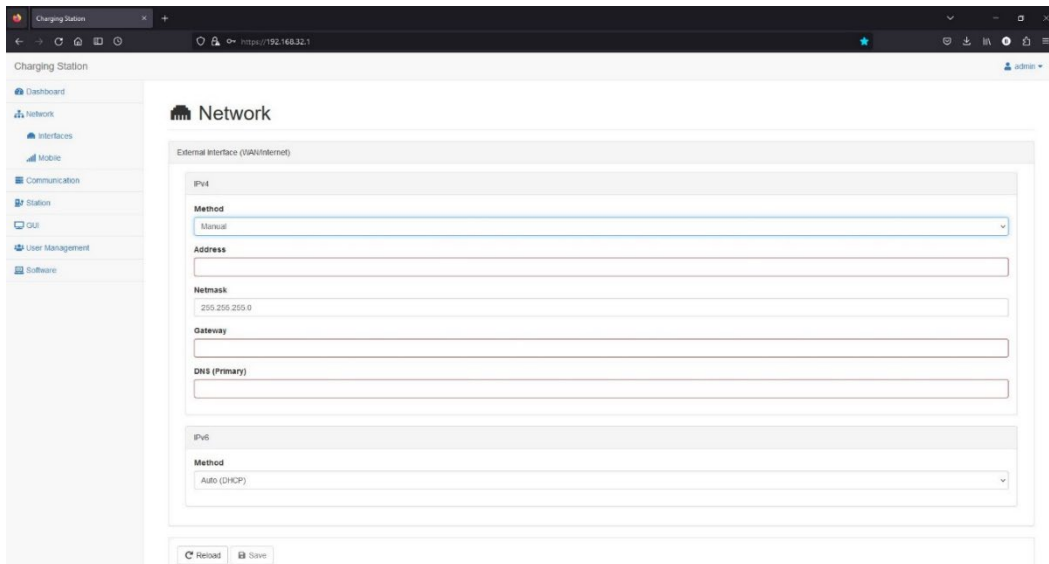
Unter „Interface (WAN/Internet)“ kann die Netzwerkkonfiguration für die Internetanbindung zum OCPP-Backend vorgenommen werden. Standardmäßig ist hier „Auto (DHCP)“ gesetzt und die Einstellungen werden automatisch vorgenommen.



Ist der Haken bei „Never default“ gesetzt, wird die OCPP Verbindung immer über Mobilfunk bevorzugt. Diese Funktion wird zum Beispiel benötigt, wenn eine OCPP-Backendverbindung

per Mobilfunkmodem und eine Lastmanagement-Verbindung per Modbus TCP bzw. LAN-Anbindung genutzt werden möchte.

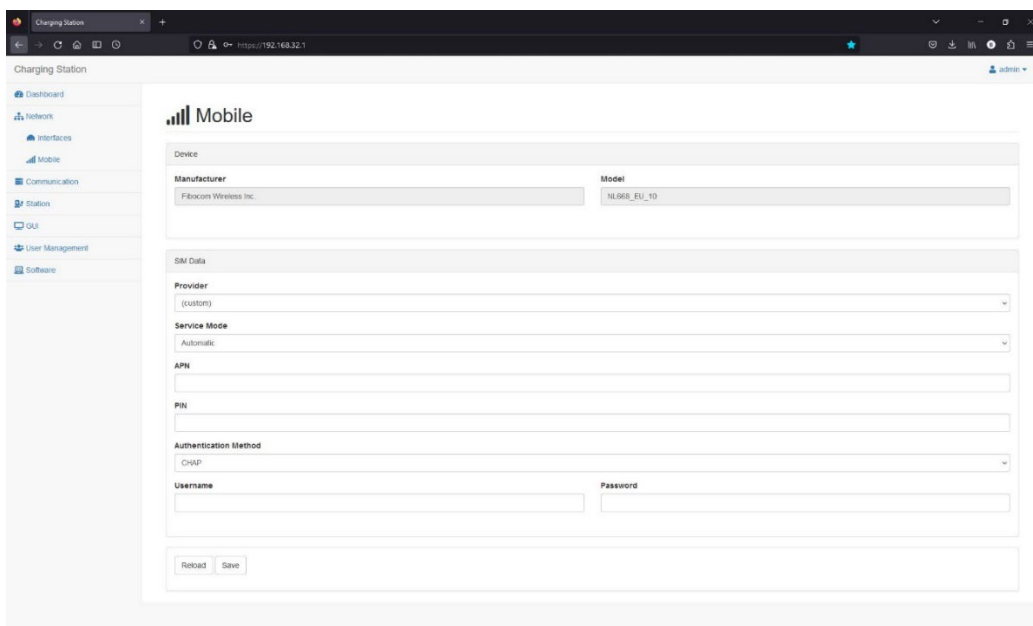
Wird die Einstellung „Auto (DHCP)“ verändert, hat man die Möglichkeit eine feste IP zu vergeben. Unterstützt wird IPv4 und IPv6.



Mobile

Der Benutzer hat die Möglichkeit, Einstellungen zur Mobilfunkverbindung vorzunehmen (nur bei Anlagen mit Modem).

Informationen zur verbauten Hardware werden unter dem Punkt „Device“ angezeigt (im Beispiel das Modem „Fibocom NL668“). Hier können keine Einstellungen vorgenommen werden.

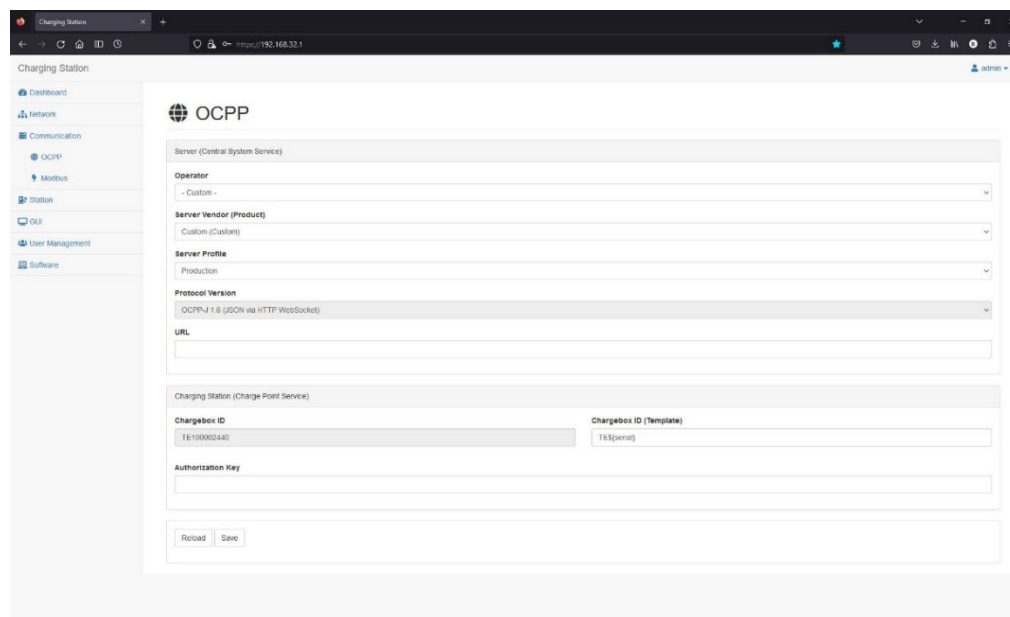


Hier können Einstellungen zur SIM-Karte vorgenommen werden.

1.5 Communication

OCPP

Hier können Einstellungen zur Verbindung zum Backend vorgenommen werden. Stellt man unter „Operator“ statt „(custom)“ ein vorinstalliertes und passendes Kundenprofil (z.B. „Factory settings“) ein, so müssen ansonsten keine Einstellungen vorgenommen werden. Wird als Profil „(custom)“ ausgewählt, kann man alle Einstellungen („Server Vendor“, „Server Profile“ und „URL“) zum Backend an die eigenen Bedürfnisse anpassen. Die „Protocol Version“ ist nicht veränderbar und immer auf „OCPP-J 1.6 (JSON via HTTP WebSocket)“ eingestellt, da OCPP 1.5 nicht mehr unterstützt wird.



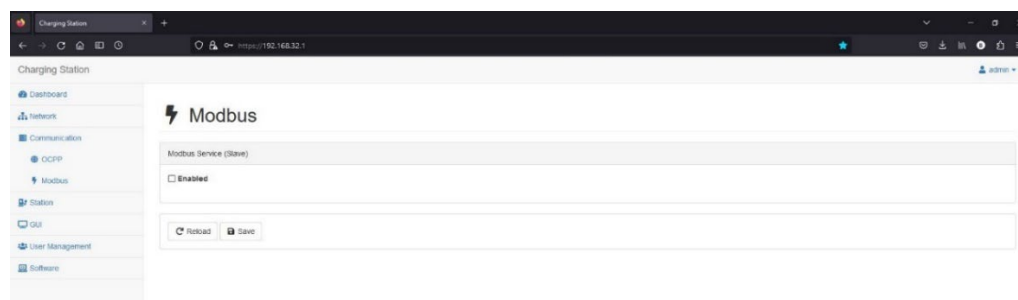
Unter „Chargebox ID“ kann keine Änderung vorgenommen werden. Sie wird automatisch aus der Seriennummer des Gerätes generiert. Jedoch kann unter „Chargebox ID (Template)“ vorgegeben werden, wie sich die Ladesäule am Backend zu melden hat.

Falls benötigt, kann hier auch noch ein „Authorization Key“ zur Anmeldung festgelegt werden.

Modbus (Lastmanagement Stufe 3)

Auf der Ladesäule läuft dauerhaft ein Modbus-Server. Die Verbindung zu diesem Server kann hier aktiviert bzw. deaktiviert werden. Das Modbus-Protokoll hierzu finden Sie unter folgendem Link:

<https://technagon.info/index.php/s/axy48yoZtSbgFzE>



Lastmanagement Stufe 2

Um das Lastmanagement zu aktivieren, führen Sie folgende Schritte durch:

1. LoadManagement aktivieren (enable)
2. Ladesäulen zuordnen (1x Masterstation auswählen, alle anderen als Slave definieren)
3. Cluster Limit in Ampere eingeben
4. Speichern.

LoadManagement Service

Enabled

Mode: master

Cluster Limit (A): 80

#	Name	Address	Limit (A)	Allocated (A)
1	200000246-1		32	32
2	200000246-2		0	0
3	200000388-1		0	0
4	200000388-2		0	0
5	200000317-1	192.168.180.68	0	0
6	200000317-2	192.168.180.68	32	32

Buttons: Reload, Save

* Bedeutung Kronen-Symbol: Master-Ladestation

HINWEIS

Diese Einstellung steht nur in einem funktionierenden Netzwerk zur Verfügung!

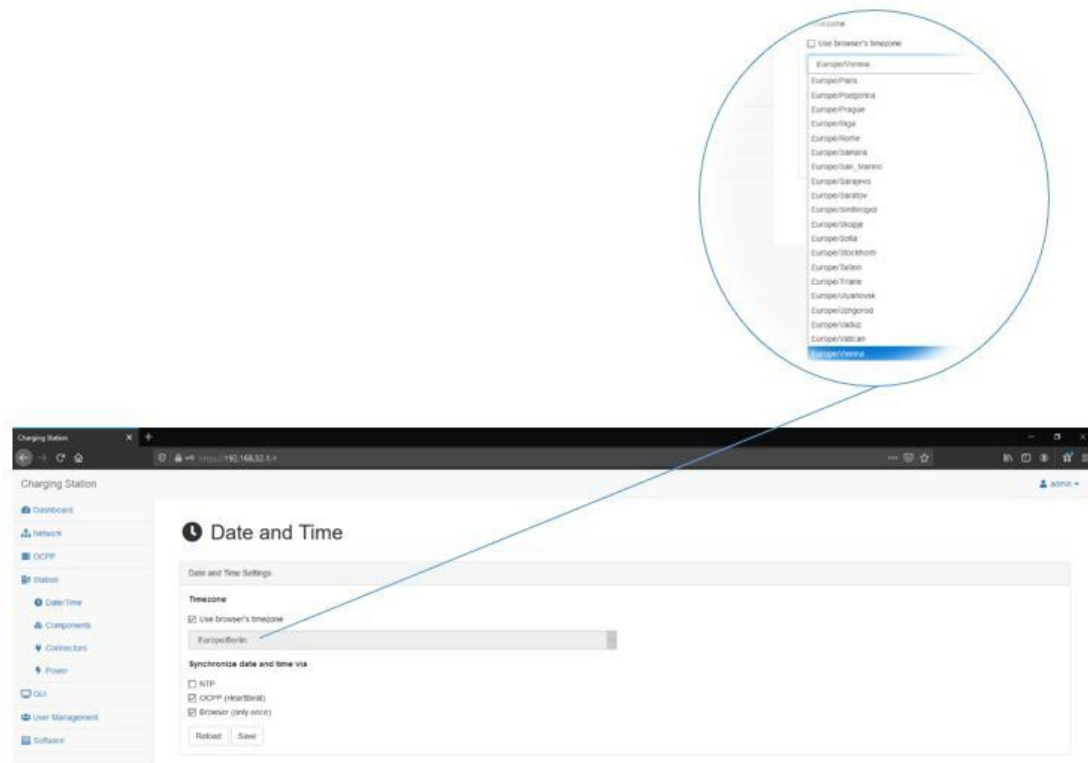
1.6 Station

Date/Time

Hier kann der Benutzer das Datum/die Uhrzeit für die Ladesäule festlegen. Dazu gibt es mehrere Möglichkeiten:

Use browser's timezone (ON): Datum/Uhrzeit wird vom verwendeten Browser übernommen

Use browser's timezone (OFF): Die Zeitzone kann manuell durch Auswahl aus der Liste festgelegt werden.



HINWEIS

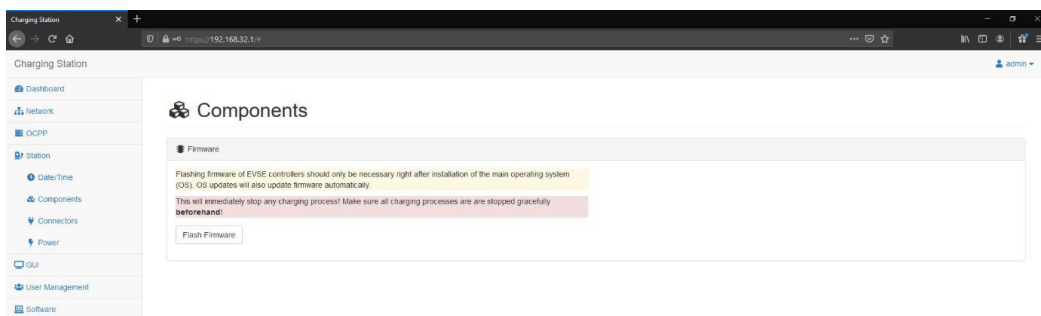
Bitte achten Sie darauf, dass die „Timezone“ dem entsprechenden Aufstellort angepasst ist.

Synchronisiert kann das Datum/die Uhrzeit werden durch:

- NTP: Synchronisierung über Internet-Verbindung (SIM-Karte)
- OCPP (HeartBeat): Synchronisierung über das Backend (bei jedem HeartBeat)
- Browser (only once): Synchronisierung über den Web-Browser (wird nur einmal durchgeführt!)

Components

Über den Button „Flash Firmware“ kann ein Flashen der Ladecontroller manuell angestoßen werden. Diese Funktion findet Anwendung nach einer Neuinstallation oder Update des Betriebssystems.

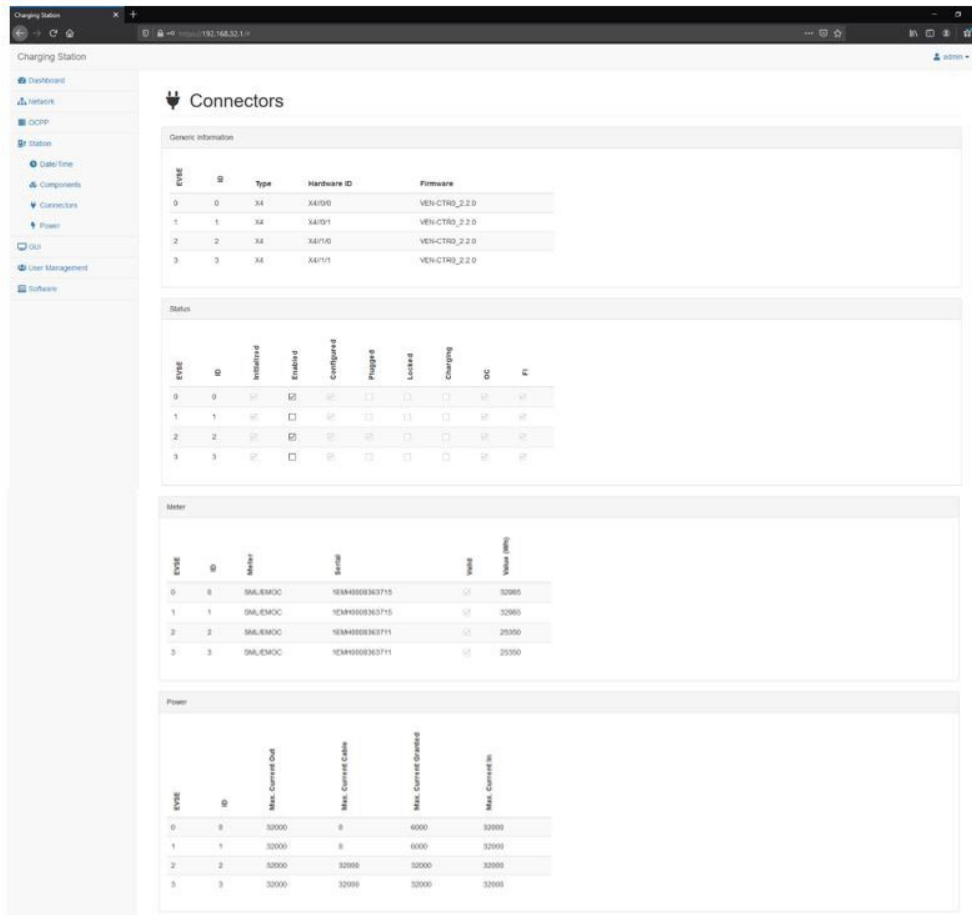


HINWEIS

Bestehende Ladevorgänge müssen vorab abgebrochen werden.

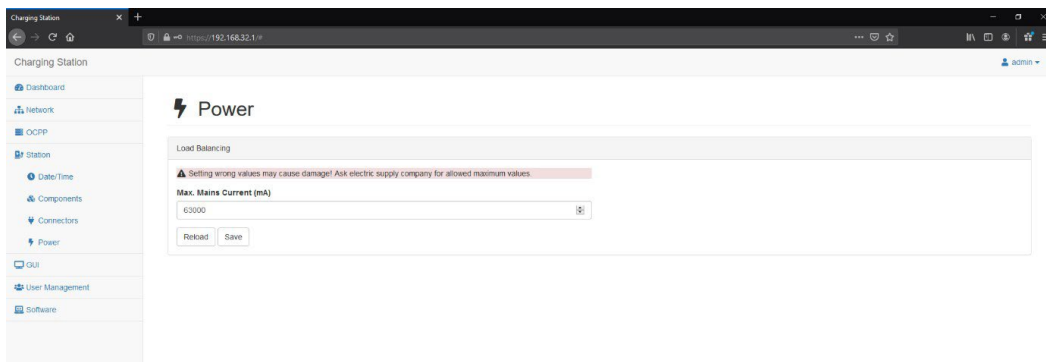
Connectors

Auf dieser Seite kann sich der Benutzer alle Informationen über die Ladecontroller, Zähler und den Ladestrom anzeigen lassen.



Power | Lastmanagement Stufe 1

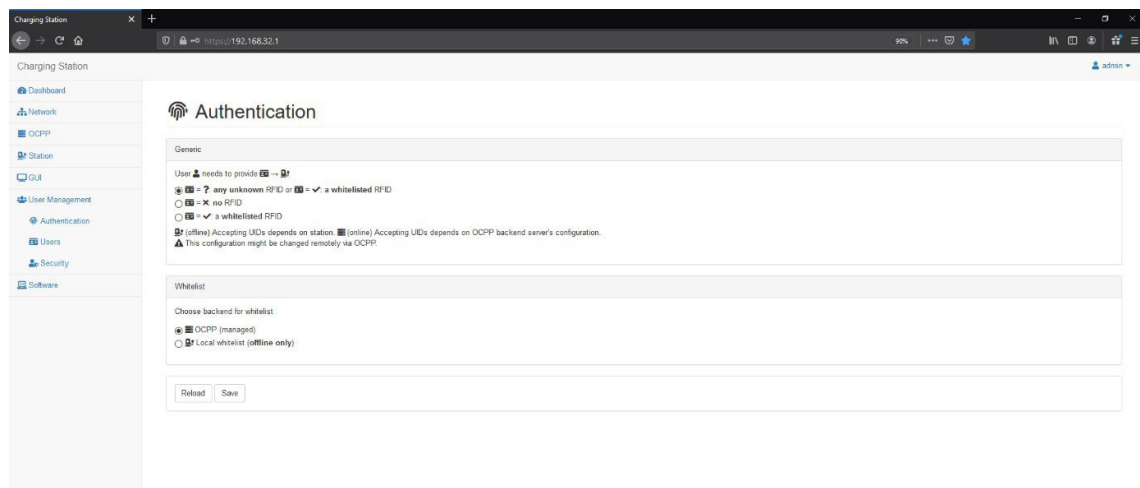
Im Idealfall stehen der Ladestation 63.000 mA zur Verfügung. Jeder Ladepunkt kann also mit 22 kW laden. Sollte eine Reduzierung erforderlich sein, kann hier die gesamte Anschlussleistung der Ladestation begrenzt werden. Die Leistung wird dann an den ersten Ladevorgang voll abgegeben; sollte ein zweiter Ladevorgang gestartet werden, wird die zur Verfügung stehende Energie halbiert.



1.7 User Management

Authentication

Hier können Einstellungen zur Authentifizierung an der Ladesäule vorgenommen werden.



Unter „Generic“ wird die Art der Authentifizierung bezüglich der RFID-Karte ausgewählt:

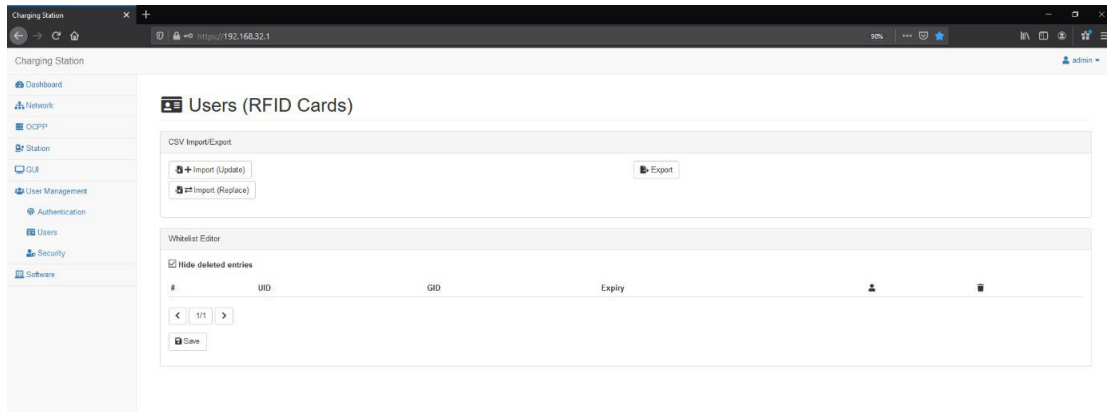
- any unknown RFID or a whitelisted RFID:
 - Ladesäule online: Abgleich gegen Whitelist im Backend
 - Ladesäule offline: Jede RFID-Karte wird akzeptiert
- no RFID: Laden ist ohne RFID-Karte möglich. Wichtig hierbei ist, dass die Dummy-RFID im Backend freigeschaltet ist. Diese wird dann bei jedem Ladevorgang vom Backend autorisiert. Im Experten-Modus kann hier die Dummy-RFID unter dem Punkt „Reader“ vorgegeben werden.
- a whitelisted RFID: In der Regel sind alle Technagon-Ladesäulen auf „a whitelisted RFID“ voreingestellt. Der RFID-Tag bei der Authentifizierung wird zuerst in der lokalen Whitelist, anschließend im Backend abgefragt.

Unter „Whitelist“ wird der Speicherort der RFID-Karten festgelegt. Mögliche Einstellungen sind hier:

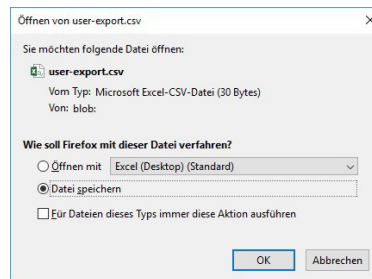
- OCPP (managed): Backend
- Local whitelist (offline only): Lokale Whitelist

Users

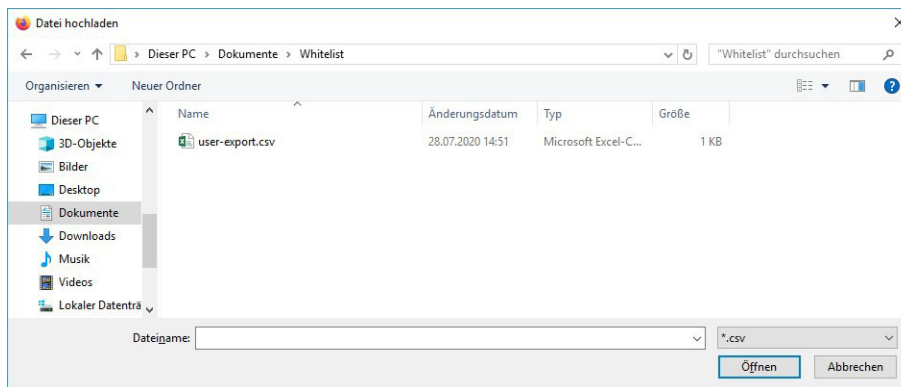
In diesem Menüpunkt kann eine lokale Whitelist für die Ladesäule angelegt werden. Um die lokale Whitelist verwenden zu können, muss vorher unter „User Management – Authentication“ die Einstellung „a whitelisted RFID“ ausgewählt werden und die Ladesäule vom Backend getrennt sein.



Über den Button „Export“ kann die bestehende Whitelist heruntergeladen werden.



Über den Button „Import (Update)“ kann eine geänderte Whitelist hochgeladen und an die bestehende Whitelist angehängt werden.



Über den Button „Import (Replace)“ kann eine geänderte Whitelist hochgeladen werden, die dann die bestehende Whitelist ersetzt.

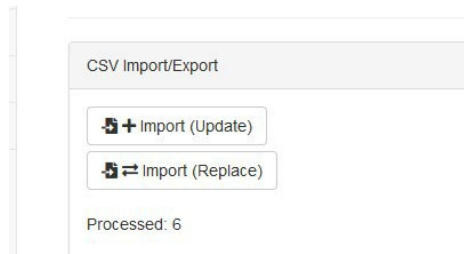
Eine externe Bearbeitung funktioniert folgendermaßen:

1. Nach dem Download über den Export-Button kann die CSV-Datei mit Microsoft Excel oder einem CSV-Editor geöffnet werden.
2. Der Aufbau dieser Datei ist immer derselbe:
 - Im Header (erste Zeile) muss immer folgendes stehen: **UID,GID,Expiry,Authorization**
 - Ab der zweiten Zeile werden RFID-Karten angelegt (immer eine Karte pro Zeile)

- Aufbau einer Zeile (der komplette Text wird in eine einzige Zelle eingegeben):
- Zuerst wird der RFID-Tag angegeben
- Anschließend zwei Komma
- Als nächstes kann der Ablauf einer Karte in folgendem Format angegeben werden (Expiry): 2020-01-01T12:00:00
- Abschließend wird die Autorisierung angegeben. Möglich sind hier: **accepted** und **blocked**
- Hinweis: Insgesamt sind bis zu 1000 Einträge möglich.
- Beispiel:

	A	B	C	D
1	UID,GID,Expiry,Authorization			
2	aec78085,,,accepted			
3	ae36959e,,,accepted			
4	0488dd2a561d80,,,blocked			
5	4b13b318,,2021-02-17T12:00:00,accepted			
6	d2006c8e,,,accepted			
7				

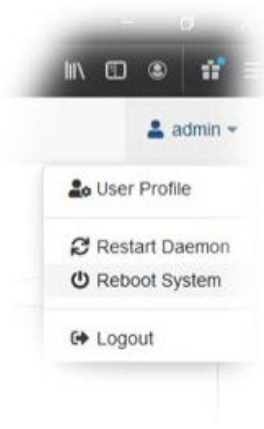
3. Nach dem Anlegen der Whitelist muss diese gespeichert und anschließend wieder in der WebUI importiert werden (wahlweise an die bestehende Whitelist anhängen mit **Import (Update)** oder diese ersetzen mit **Import (Replace)**).
4. Daraufhin werden die Einträge in der Whitelist übernommen und unter den Buttons zum Importieren wird neben **Processed** angezeigt, wie viele Zeilen der CSV-Datei bearbeitet wurden (der Header wird hier mitgezählt).



5. Durch einen Klick auf den Button **Save** wird der ganze Vorgang gespeichert.
6. Durch den Haken bei **Hide deleted entries** lassen sich gelöschte Einträge wieder sichtbar machen. Dies funktioniert jedoch nur solange kein Neustart an der Ladesäule durchgeführt wurde.



- Während eines Reboots werden die Einträge auf die Ladesäule übernommen. Also sollte zum Schluss der Änderungen immer ein Neustart (**admin – Reboot System**) und anschließend ein Test der angelegten RFID-Karten durchgeführt werden.

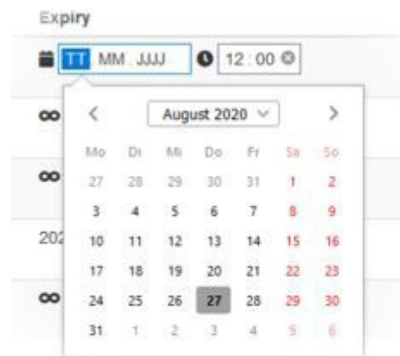


Eine interne Bearbeitung im Whitelist-Editor des WebUI funktioniert folgendermaßen:

- Klickt man auf eine UID, so kann man diese bearbeiten und verändern:



- Ebenso kann das Ablaufdatum/die Ablaufuhrzeit verändert werden. Das Datum wird aus einem Kalender ausgewählt, während die Uhrzeit per Hand eingegeben werden



muss:

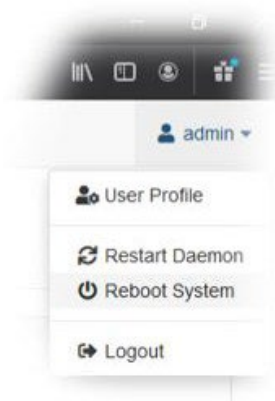
- Mit den Buttons rechts können bei allen Einträgen die Berechtigungen gesteuert werden. Indem man auf die Buttons klickt, kann man die gewünschte Einstellung für den jeweiligen Eintrag vornehmen:



- Mögliche Einstellungen sind:
 - Der RFID-Tag wird akzeptiert
 - Der RFID-Tag wird blockiert
 - Der RFID-Tag soll gelöscht werden
 - Ein gelöschter RFID-Tag soll wiederhergestellt werden
- Über die Pfeiltasten unten kann zwischen den einzelnen Seiten geblättert werden. Pro Seite werden 10 Einträge angezeigt.

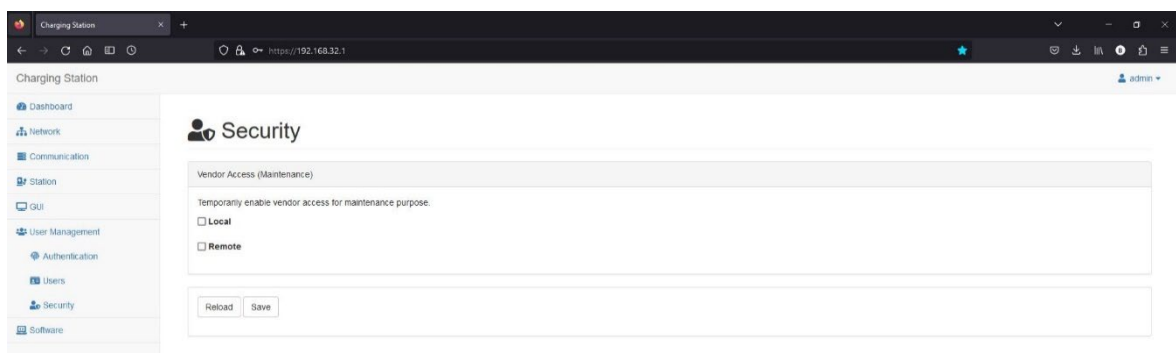


- Nach einer Änderung muss diese immer über den **Save**-Button abgespeichert werden.
- Während eines Reboots werden die Einträge auf die Ladesäule übernommen. Also sollte zum Schluss der Änderungen immer ein Neustart (**admin – Reboot System**) und anschließend ein Test der angelegten RFID-Karten durchgeführt werden.



Security

Hier kann der Zugang auf das Betriebssystem freigeschaltet werden. Diese Funktion sollte nur auf Anweisung des Herstellers verwendet werden, da ansonsten möglicherweise die Garantie erlischt.



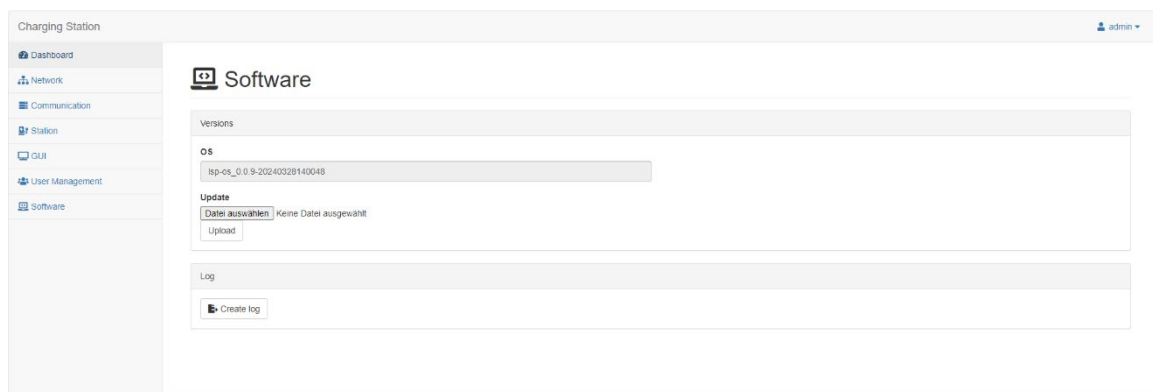
1.8 Software

Unter „Versions“ bei OS wird der aktuelle Softwarestand des Systems angezeigt.

Unter **Update** ist es ab der Softwareversion **Technagon OS-2.3 (0.0.9)** möglich, ein Update über das Webinterface durchzuführen. Hierzu sind folgende Schritte durchzuführen.

1. **Datei auswählen** klicken und eine beliebige Software-Version im Explorer auswählen.
2. Software durch einen Klick auf **Upload** an die Ladestation schicken.
3. Nun wird das Update durchgeführt, dies kann bis zu 10 Minuten dauern.
4. Durch Neuladen der Weboberfläche (F5) kann nach den 10 Minuten überprüft werden, ob das Update erfolgreich war. Hierbei wird unter **OS** die neue SW-Version angezeigt.

Außerdem können ab der Softwareversion **Technagon OS-2.3 (0.0.9)** auch die Logfiles der Ladestation über das Webinterface heruntergeladen werden. Hierzu einfach den Button **Create log** Klicken. Dieser Vorgang kann ein paar Minuten dauern. Anschließend wird das Log im Downloadbereich des Browsers abgelegt.



2. OCPP-Keys

2.1 Quellen

Weitere Informationen zum Thema OCPP findet man auf der Homepage von [Open Charge Alliance](https://www.openchargealliance.org/) (<https://www.openchargealliance.org/>).

Die OCPP-Spezifikation kann dort kostenlos heruntergeladen werden (<https://www.openchargealliance.org/downloads/>).

Hier sind alle Befehle und Nachrichten noch genauer erklärt.

2.2 Features

CPS ↔ CSS	OCPP	FIELD NAME	PARAMETERS/ RANGE	MANDATORY / OPTIONAL	SUPPORTED
→	Authorize.req	IdTag	Card Id	M	Yes
←	Authorize.conf	IdTagInfo		M	Yes
		- status	Accepted, Blocked, Expired, Invalid, ConcurrentTx	M	Yes
		- expiryDate	ISO 8601 date time	O	Yes
		- parentIdTag		O	No
→	BootNotification.req	chargeBoxSerialNumber	empty	O	Yes
		chargePointModel	Model	M	Yes
		chargePointSerialNumber	Serialnumber	O	Yes
		chargePointVendor	"Technagon GmbH"	M	Yes
		firmwareVersion	Isp-os-0.0.10	O	Yes
		iccid	89883030000045459887	O	Yes
		imsi	206018037157525	O	Yes
		meterSerialNumber		O	No
		meterType		O	No
←	BootNotification.conf	currentTime	ISO 8601 date time	M	Yes
		interval	180	M	Yes
		status	Accepted, Pending, Rejected	M	Yes
→	CancelReservation.req	reservationId	1234	M	Yes
←	CancelReservation.conf	status	Accepted, Rejected	M	Yes
→	ChangeAvailability.req	connectorId	0,1,2	M	Yes
		type	Inoperative, Operative	M	Yes

→	ChangeAvailability.conf	status	Accepted, Rejected	M	Yes
←	ChangeConfiguration.req	key	Key	M	Yes
		value	Value	M	Yes
→	ChangeConfiguration.conf	status	Accepted, Rejected, Not Supported	M	Yes
←	ClearCache.req				Yes
→	ClearCache.conf	status	Accepted, Rejected	M	Yes
←	ClearChargingProfile.req	id	123	O	Yes
		connectorId	0,1,2	O	No
		chargingProfilePurpose	ChargePointMaxProfile, TxDefaultProfile, TxProfile	O	No
		stackLevel	12	O	No
→	ClearChargingProfile.conf	status	Accepted, Unknown	M	Yes
→	DataTransfer.req	vendorId	generalConfiguration	M	Yes
		messageId	setMeterConfiguration	O	Yes
		data	ASDFGH	O	Yes
←	DataTransfer.conf	status	Accepted, Rejected, UnknownMessageId, UnknownVendorId	M	Yes
→	DiagnosticsStatusNotification.req	status	Idle, Uploaded, Upload-Failed	M	Yes
←	DiagnosticsStatusNotification.conf				
→	FirmwareStatusNotification.req	status	Download, Downloaded, Installed, InstallationFailed	M	Yes
←	FirmwareStatusNotification.conf				
←	GetCompositeSchedule.req	connectorId	0,1,2	M	No
		duration	240	M	No
		chargingRateUnit	A, W	O	No
→	GetCompositeSchedule.conf	status	Rejected	M	No
		connectorId	0,1,2	O	No
		scheduleStart	ISO 8601 date time	O	No
		chargingSchedule	Loadmanagement	O	No
←	GetConfiguration.req	key	key1, key2	O	Yes

→	GetConfiguration.conf	configurationKey	key1, key2	O	Yes
		unknownKey	key3, key4	O	Yes
←	GetDiagnostics.req	location	ftp://my.server/path /	M	Yes
		retries	3	O	No
		retryInterval	180	O	No
		startTime	ISO 8601 date time	O	No
		stopTime	ISO 8601 date time	O	No
→	GetDiagnostics.conf	fileName	serial.tar.gz	O	Yes
←	GetLocalListVersion.req				
→	GetLocalListVersion.conf	listVersion	12	M	Yes
→	Heartbeat.req				
←	Heartbeat.conf	currentTime	ISO 8601 date time	M	Yes
→	MeterValues.req	connectorId	1,2	M	Yes
		transactionId	5678	O	Yes
		meterValue		M	Yes
		- timestamp	ISO 8601 date time	M	Yes
		- sampledValue		M	Yes
		- value	234.56	M	Yes
		- context	Sample.Periodic, Transaction.Begin, Transaction.End	O	Yes
		- format	Raw, SignedData	O	Yes
		- measurand	Energy.Active.Import.Register, Power.Active.Import, Current.Offered, Current.Import.L1, Current.Import.L2, Current.Import.L3, Power.Offered, Voltage	O	Yes
		- phase		O	No
		- location	Outlet	O	No
		- unit	Wh	O	No
←	MeterValues.conf				
←	RemoteStartTransaction.req	connectorId	1,2	M	Yes
		idTag	Card Id	M	Yes
		chargingProfile	Loadmanagement	O	Yes
→	RemoteStartTransaction.conf	status	Accepted, Rejected	M	Yes

←	RemoteStopTransaction.req	transactionId	8345	M	Yes
→	RemoteStopTransaction.conf	status	Accepted, Rejected	M	Yes
←	ReserveNow.req	connectorId	1,2	M	Yes
		expiryDate	ISO 8601 date time	M	Yes
		idTag	Card Id	M	Yes
		parentIdTag		O	No
		reservationId	2345	M	Yes
→	ReserveNow.conf	status	Accepted, Occupied, Rejected	M	Yes
←	Reset.req	type	Hard, Soft	M	Yes
→	Reset.conf	status	Accepted, Rejected	M	Yes
←	SendLocalList.req	listVersion	12	M	Yes
		localAuthorizationList		O	Yes
		– idTag	Card Id	M	Yes
		– IdTagInfo		O	Yes
		— status	Accepted, Blocked, Expired, Invalid, ConcurrentTx	M	Yes
		— expiryDate	ISO 8601 date time	O	Yes
		— parentIdTag		O	Yes
		updateType	Differential, Full	M	Yes
→	SendLocalList.conf	status	Accepted, Failed, VersionMismatch	M	Yes
←	SetChargingProfile.req	connectorId	0,1,2	M	Yes
		csChargingProfiles	Loadmanagement	M	Yes
→	SetChargingProfile.conf	status	Accepted, Rejected	M	Yes
→	StartTransaction.req	connectorId	1,2	M	Yes
		idTag	Card Id	M	Yes
		meterStart	4567	M	Yes
		reservationId	367	O	Yes
		timestamp	ISO 8601 date time	M	Yes
←	StartTransaction.conf	idTagInfo		M	Yes
		– status	Accepted, Blocked, Expired, Invalid, ConcurrentTx	M	Yes
		– expiryDate	ISO 8601 date time	O	Yes
		– parentIdTag		O	Yes
		transactionId	538	M	Yes

→	StatusNotification.req	connectorId	0,1,2	M	Yes
		errorCode	ConnectorLockFailure, EVCommunicationError, GroundFailure, InternalError, NoError, OtherError, OverCurrentFailure, OverVoltage, PowerMeterFailure, WeakSignal	M	Yes
		info	text	O	Yes
		status	Available, Preparing, Charging, SuspendedEVSE, SuspendedEV, Finishing, Reserved, Un- available, Faulted	M	Yes
		timestamp	ISO 8601 date time	M	Yes
		vendorId	Company	O	Yes
		vendorErrorCode	RegulatoryComplianceFailure	O	Yes
←		StatusNotification.conf			
→	StopTransaction.req	idTag	Card Id	O	Yes
		meterStop	5854	M	Yes
		timestamp	ISO 8601 date time	M	Yes
		transactionId	456	M	Yes
		reason	EVDisconnected, HardReset, Local, Other, Remote, SoftReset, UnlockCommand	O	Yes
		transactionData		O	Yes
←	StopTransaction.conf	idTagInfo		O	Yes
		- status	Accepted, Blocked, Expired, Invalid, ConcurrentTx	M	Yes
		- expiryDate	ISO 8601 date time	O	Yes
		- parentIdTag		O	Yes
←	TriggerMessage.req	requestedMessage	BootNotification, HeartBeat, MeterValues, StatusNotification	M	Yes
		connectorId	1,2	O	Yes
→	TriggerMessage.conf	status	Accepted, Rejected, NotImplemented	M	Yes

←	UnlockConnector.req	connectorId	[1,2]	M	Yes
→	UnlockConnector.conf	status	Unlocked, UnlockFailed, NotSupported	M	Yes
←	UpdateFirmware.req	location	ftp://my.server/firmware-file	M	Yes
		retries	3	O	No
		retrieveDate	ISO 8601 date time	M	No
		retryInterval	180	O	No
→	UpdateFirmware.conf				
←	StopTransaction.conf	idTagInfo		O	Yes

2.3 Konfiguration

- read
- ← write
- ↔ read + write

NAME	ACCESS	DESCRIPTION
/hw/auth/device/Dummy/allowStop	↔	End charging by button press in Plug&Charge-Mode (everyone could unplug the cable)
/hw/auth/device/Dummy/enabled	↔	Plug&Charge-Mode (Online free charge)
/hw/auth/device/Dummy/id/value	↔	Dummy-RFID-Tag für Plug&Charge-Mode
/hw/connectors/<connector-id>/data	→	Meters data (voltage / current)
/hw/connectors/<connector-id>/meter/key	→	Meters Public key (GSWML)
/hw/connectors/1/evseld /hw/connectors/2/evseld	→	Show EVSE-ID on 4,3" display
/hw/connectors/1/evseLabel /hw/connectors/2/evseLabel	→	Show Chargingpoint number on 4,3" display (for Credit card terminal)
/Gui/Operator/Contact/phone	→	Show Support-Hotline on 4,3" display
/Price/1/adhoc /Price/2/adhoc	←	Show adhoc price and QR-code on 4,3" display Further information and a whitepaper you can find at: https://technagon.de/dynamic-qr-code/
/Network/Gateway/Device/Connection/signal	→	Mobile signal level
/ocpp/chargeBoxIdentity	↔	OCPP charge box identity of the station
/ocpp/stopTransactionsOnReset	↔	Stop charging transaction at OCPP reset
/power/station/mainsMaxCurrent	↔	Max. current (mA) station may draw from power grid
/Product/ActivationCode	←	Used to pass product activation codes to station
/Product/Features/	→	Path prefix for enabled product features (see ActivationCode)
/Safety/Ovp/failed	→	Over current protection activated. Replace recommended.

<code>/Security/enableLocalVendorAccess</code>	↔	Enable access to local linux terminal.
<code>/Security/enableRemoteVendorAccess</code>	↔	Enable ssh/opensvpn access.
<code>/WebUi/password/reset</code>	←	set stations webui password (write only!)
<code>AllowOfflineTxForUnknownId</code>	↔	see OCPP 1.6 Spec
<code>AuthIdLegicPrime</code>	↔	Pattern for Legic Prime Authentication.
<code>AuthIdLegicAdvant</code>	↔	Pattern for Legic Advant Authentication.
<code>AuthorizationCacheEnabled</code>	↔	Cache is enabled when at least one of AuthorizationCacheEnabled or LocalAuthListEnabled is true
<code>AuthorizationKey</code>	↔	BasicAuth authorization key.
<code>ChargeProfileMaxStackLevel</code>	→	see OCPP 1.6 Spec
<code>ChargingProfileStackPerConnector</code>	↔	Stack per connector in TxProfile
<code>ChargingScheduleAllowedChargingRateUnit</code>	→	see OCPP 1.6 Spec
<code>ChargingScheduleMaxPeriods</code>	→	see OCPP 1.6 Spec
<code>ConnectionTimeOut</code>	↔	see OCPP 1.6 Spec
<code>ConnectorPhaseRotationMaxLength</code>	→	see OCPP 1.6 Spec
<code>ConnectorSwitch3to1PhaseSupported</code>	→	see OCPP 1.6 Spec
<code>CurrentDateTime</code>	→	see OCPP 1.6 Spec
<code>GetConfigurationMaxKeys</code>	→	see OCPP 1.6 Spec
<code>GiroEStaticToken</code>	↔	Giro-e related
<code>HeartbeatInterval</code>	↔	see OCPP 1.6 Spec
<code>LocalAuthListEnabled</code>	↔	See AuthorizationCacheEnabled
<code>LocalAuthListMaxLength</code>	→	see OCPP 1.6 Spec
<code>LocalAuthorizeOffline</code>	↔	see OCPP 1.6 Spec
<code>LocalPreAuthorize</code>	↔	see OCPP 1.6 Spec
<code>MaxChargingProfilesInstalled</code>	→	see OCPP 1.6 Spec
<code>MeterValuesAlignedDataMaxLength</code>	→	see OCPP 1.6 Spec
<code>MeterValueSampleInterval</code>	↔	see OCPP 1.6 Spec
<code>MeterValuesSampledData</code>	↔	see OCPP 1.6 Spec
<code>MeterValuesSampledDataMaxLength</code>	→	see OCPP 1.6 Spec
<code>NumberOfConnectors</code>	→	see OCPP 1.6 Spec
<code>PreAuthorize</code>	↔	Preauthorize method to use (giro-e, <empty>)
<code>ReserveConnectorZeroSupported</code>	→	see OCPP 1.6 Spec
<code>SendLocalListMaxLength</code>	→	see OCPP 1.6 Spec

StopTransactionOnEVSideDisconnect	↔	Accepts true only (Eichrecht)
StopTxnAlignedDataMaxLength	→	see OCPP 1.6 Spec
StopTxnSampledData	↔	see OCPP 1.6 Spec
StopTxnSampledDataMaxLength	→	see OCPP 1.6 Spec
StopTxOnReset	↔	Whether to stop charging on reset (use true for OCPP 1.6 compliance)
SupportedFeatureProfiles	→	see OCPP 1.6 Spec
SupportedFeatureProfilesMaxLength	→	see OCPP 1.6 Spec
SupportedFileTransferProtocols	→	see OCPP 1.6 Spec
TimeSource	↔	Time source - NTP or HeartBeat
TimeZone	↔	Time zone
TransactionMessageAttempts	↔	Setting ins ignored (Eichrecht)
UnlockConnectorOnEVSideDisconnect	↔	Accepts true only
WebSocketPingInterval	↔	see OCPP 1.6 Spec

3. OCPP Errors

ID	BESCHREIBUNG
0	Die ganze Station oder eine Komponente, welche zur ganzen Station gehört.
1, 2	Ein bestimmter EVSE Connector.

ID	ERROR	INFO	STATUS	TOPPER
0	WeakSignal	Schlechter Empfang über das Mobilfunknetz	Verfügbar	
0	OverVoltageProtectionFailure	Überspannungsschutz ist nicht mehr sichergestellt	Verfügbar	
0	RegulatoryComplianceFailure	GSWML: Problem mit der SD-Karte	Fehlerhaft	x7 blinken
n	EVSECommunicationError	Fehler am Fahrzeug	Fehlerhaft	x1 blinken
0	ReaderFailure	Kein gültiger RFIDReader wurde gefunden	Verfügbar	
n	PowerMeterFailure	Fehler bei der Kommunikation zum Zähler	Fehlerhaft	x6 blinken
0	UnderVoltage	Phasenausfall: min. 1 Phase fehlt	Fehlerhaft	
n	OverCurrentFailure	Die Überstromsicherung hat ausgelöst	Fehlerhaft	x3 blinken
n	GroundFailure	RCD hat ausgelöst	Fehlerhaft	x4 blinken
n	ConnectorLockFailure	Stecker Verriegelung defekt oder Ladekabel nicht sauber angesteckt	Fehlerhaft	x5 blinken
n	PowerSwitchFailure	Schützkleber	Fehlerhaft	x2 blinken
n	EVCommunicationError	Fehler am Fahrzeug	Fehlerhaft	x1 blinken