User Manual
go-e Portal

V 1.0

Content

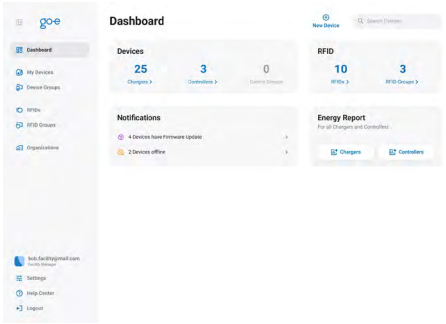
Discover the go-e YouTube Channel

Here you can find HOW-TO videos and product videos. Our videos are available with subtitles in different languages!

portal.go-e.com

1. Service Description

Your All-in-One Platform for Managing EV Charging



portal.go-e.com is a powerful, user-friendly platform built for charge point owners who demand full control, seamless confi guration, and scalable management of their electric vehicle (EV) charging infrastructure. Whether you're an individual user or operating a commercial charging network, the go-e Portal empowers you to deliver a premium charging experience – while simplifying operations and support.

Effortless Configuration & Maintenance
From fleet setup to ongoing updates, confi gure and maintain your charge points in minutes. The go-e Portal off ers intuitive tools that ensure quick deployment and easy management – without technical complexity.

Granular Energy Monitoring & Reporting
Get precise insights into your charging activity. Monitor energy consumption per session, RFID, or groups of devices with detailed reports that support operational efficiency.

Advanced Access Control
Assign specific access rights to users and groups - whether for public use, employee fleets, or private households. Control who can charge, when, and how, all from a single dashboard.

Built for Fleet Expansion & System Integration
As your fl eet grows, go-e grows with you. The portal is designed to support flexible expansion and seamless integration into third-party systems:

Multiple Connectivity Options

- **OCPP (Open Charge Point Protocol)** for smart network integration
- **MQTT** for custom IoT applications and real-time control
- **Digital Inputs** for local energy management and automation
- **APIs** for integrating with backend systems and apps
- **Modbus TCP** via Ethernet and TCP/IP for communication

Scalable Fleet Management

Configure, group, manage access (via RFIDs) and monitor hundreds of chargers with ease – ideal for businesses scaling their EV infrastructure over time.

Supports Consumer & Business Applications
Whether you're a homeowner managing a single charger, or a business running a large-scale network, the go-e Portal scales with you. Fleet management, public access, workplace charging—it's all in one place.

The go-e Portal is more than just a dashboard—it's the digital backbone for a cleaner, smarter mobility future. Whether you're electrifying your home, workplace, or public infrastructure, go-e gives you the tools to scale, support, and succeed.

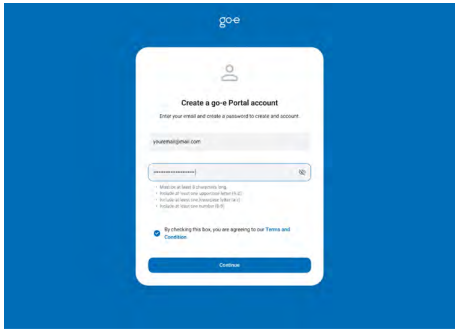
Get started today at portal.go-e.com

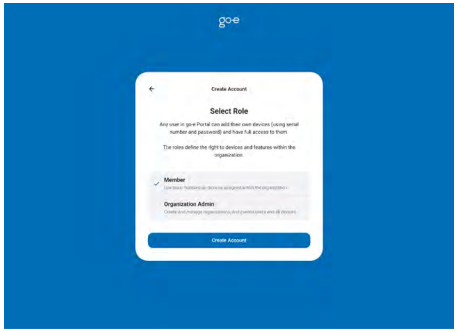
Your

go-e team

2. Functionalities

Account



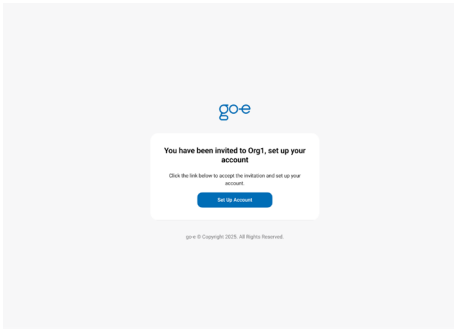


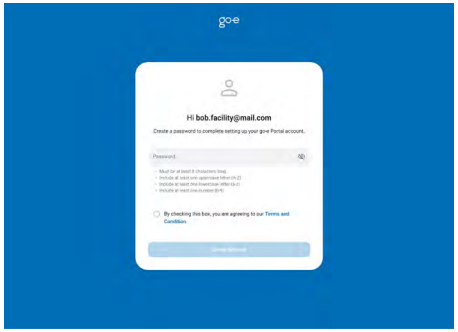
Self-Registration
From the login page, users can choose to create a new account. To register, a valid email address must be provided as the username, and a password must be set. Users must also agree to the Terms & Conditions to continue.

Next, users are prompted to select a role – **Organization Admin** or **Member**.

This selection determines whether they can create new organizations within the Portal. It does not restrict users from becoming an admin of an existing organization.

After completing registration, users will receive a confirmation email. They must verify their email address before logging in for the first time.



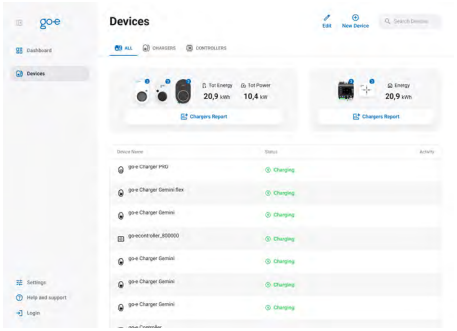


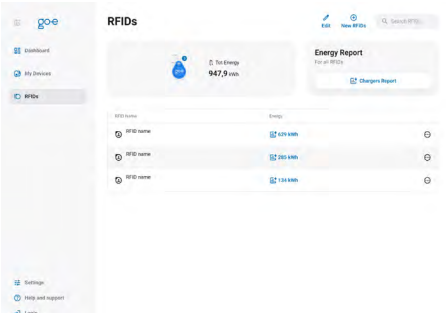
Invitation Based Registration

A user is invited to join an Organization via their email address. They receive an invitation link, and by clicking it, they're guided to set a password to complete their account setup (if not already registered in the Portal). No additional information is needed—once the password is set, the user gains access to the Portal with the role and device access assigned by the Organization Admin.

2. Functionalities

Account

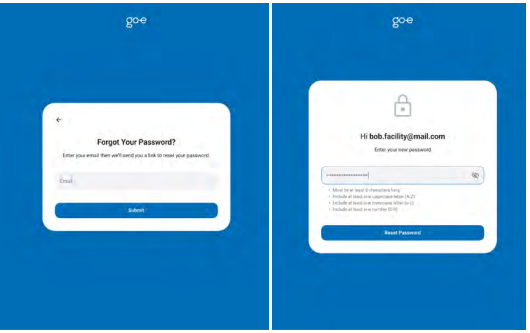




Anonymous access
The Portal can also be accessed without an account, off ering a limited set of functionalities. On the login screen, users can click “Use without Account” to proceed.

In this mode, users can add devices using their Serial Number and Password to fully operate them. Reports can be generated for individual or multiple devices, and RFID chips can be added. RFID pairing is only available for authenticated devices. Features such as Organizations and device grouping are not available in Anonymous access.

Devices and their data are cached in the browser, meaning they remain visible and accessible until the browser cache is cleared.



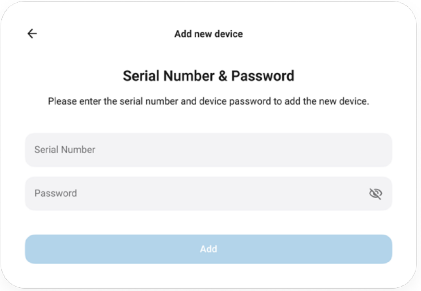
Recover password
If you’ve lost or forgotten your password, you can reset it from the main login page by entering your registered email address. A password reset link will be sent to your email, allowing you to set a new password and regain access to your account.

Add & Access devices

Note: Devices must be **online** (connected via LTE, Wi-Fi, or Ethernet) to be added to the Portal or operated remotely. Ensure the device is connected before proceeding.

Important: Older models without LTE or Ethernet (e.g., first-generation Gemini, Homefi x, or Home Plus) require commissioning via the app, as they do not have a Device Password by default. **Unfortunately, very old devices with version numbers V1 and V2 cannot be added to the Portal.**

Newer models (e.g., Gemini 2.0, CORE, and PRO) can connect automatically via LTE or Ethernet when powered on and begin operating with factory default settings. These defaults – such as grid parameters for chargers – may vary depending on the device model. While commissioning is not strictly required to start operating the device, it is strongly recommended to review and adjust these settings as needed.



Devices can appear in the Portal in two ways:

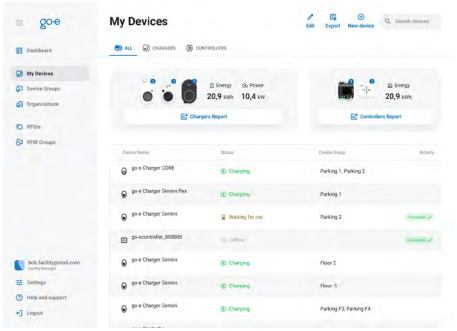
Manual Addition via Serial Number and Device Password (Accessible from the top-right corner of the Portal)

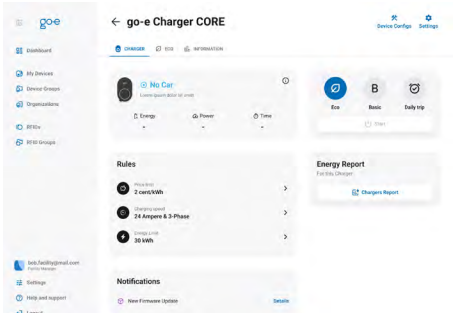
Users can add devices by entering the Serial Number and Device Password – found on the Reset Card (for Chargers) or Data Card (for Controllers). Once added, the device will appear under My Devices, and the user will have full control, regardless of their assigned role.

Assignment through an Organization
Devices can also be assigned to users within an Organization. These devices appear under the Organizations section. Access rights in this context are determined by the user‘s role within the organization. To access the full functionalities, users can still enter the device serial number and password – this will also list the device under My Devices, while it remains visible in the Organization view.

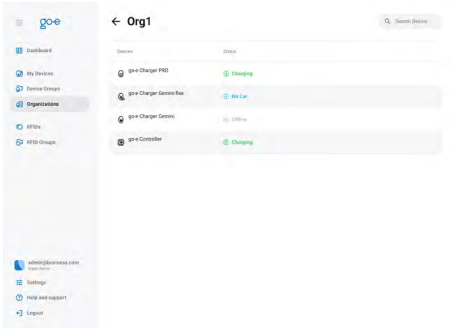
2. Functionalities

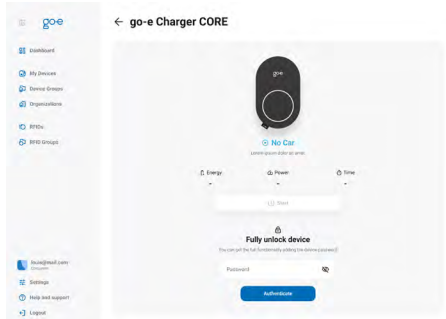
Add & Access devices





Authenticated devices
Devices added using the Serial Number and Device Password, or assigned devices that have been fully accessed with the password, will appear under My Devices. These devices can be fully operated by the user - typically intended for device owners or admins.



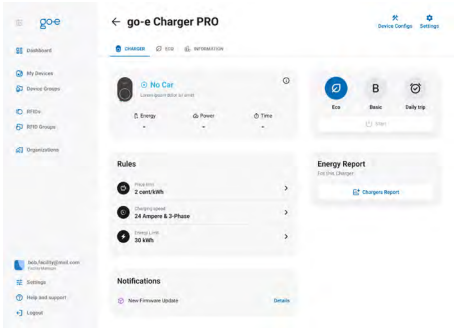


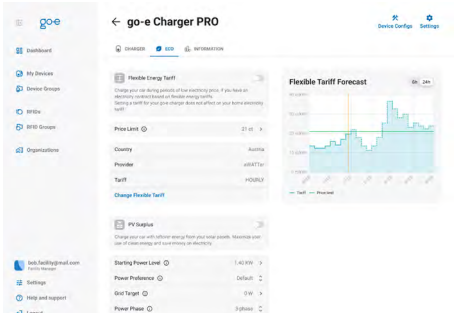
Assigned devices
Devices assigned through an Organization are visible under the Organizations section and access is managed based on the user's role within the organization. These devices can only be unassigned or removed by an Organization Admin.

To access the full set of functionalities, users enter the Device Serial Number and Password – this will also add the device to My Devices, while it remains listed under the organization.

2. Functionalities

Single device





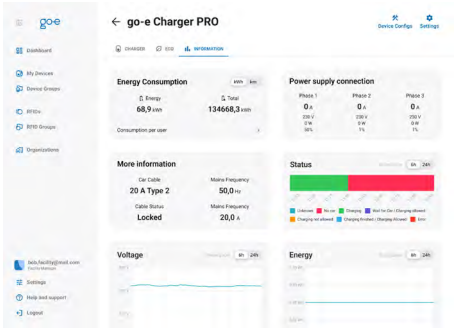
Charger

Main page
Based on the user's **role**, a core set of functionalities is available to operate the charger. These include:

- **Start/Stop charging**
- Setting **charging rules** (e.g., Energy Limits, Flexible tariff price limit, Charging Speed)
- Switching between **charging modes**
- Access to **reporting**
- Managing **notifications**

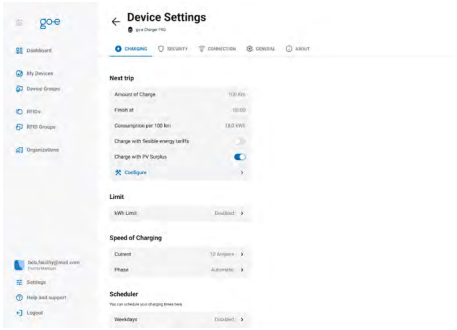
Eco Tab
Based on the user's role, additional settings may be available, including:

- **Energy tariff parameters** such as
  - **Country**
  - **Provider or Zone**
  - **Price limits**
- **Access to photovoltaic-related functionalities**, such as enabling solar charging modes or managing PV integration settings



Informations
Based on the user's **role**, access may be granted to **charger analytics** covering the past **6 to 24 hours**. These insights include:

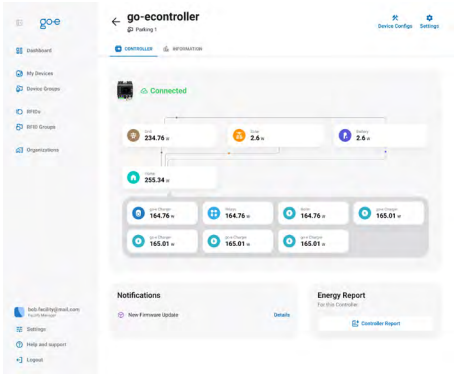
- **Status changes**
- **Temperature**
- **Voltage**
- **Energy consumption**
- Other key performance indicators

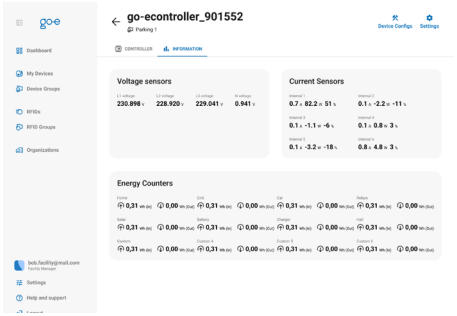


Settings
Based on the user's role, access to extended settings for individual chargers may be available. These settings allow for deeper confi guration and customization of the charger's behavior and operational parameters.

2. Functionalities

Single device





Controller

Main page
Based on the user's role, access to the controller includes:

- Energy Flows and status updates
- Reporting features
- Notifications

Informations
Based on the user's role, live data from controller-related sensors and energy metrics are available for monitoring.

Settings
Based on the user's role, access to extended settings for individual controllers may be granted, allowing advanced confi guration and management options.

RFIDs

RFID cards or tags can be used to securely start charging sessions on EV chargers. When RFID authentication is enabled, only recognized and paired RFIDs will be allowed to initiate charging. This ensures controlled access to the charger – ideal for private, shared, or commercial use.

Depending on the confi guration, RFID authentication can be managed in two modes – Cloud and Local – depending on the use case and connectivity of the charger.

Cloud RFIDs

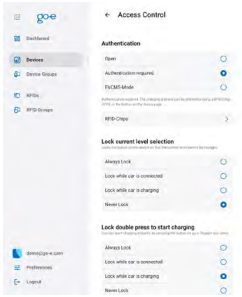
- No limit on the number of RFIDs that can be paired.
- Require the device to be online to function.
- Can be paired directly from the Portal (in the RFID section) on authenticated devices.
- Do not require physical confi rmation at the charger to pair.
- Ideal for dynamic environments with many users or frequent changes.

Local RFIDs

- Limited to 10 RFIDs, stored in the charger's local memory.
- Work even if the charger is offline.
- Must be paired physically at the charger (requires RFID tag to be tapped and confirmed).
- Can be paired in the charger's settings (via Portal or app) when physically near the charger.
- Useful for offline scenarios or simple access control.

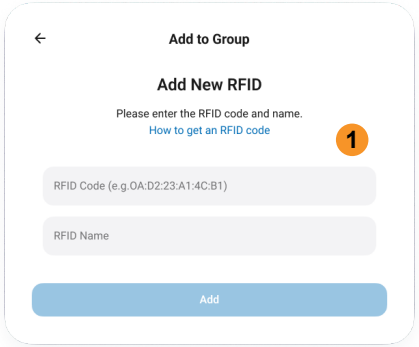
2. Functionalities

RFIDs



Enabling the Mode
To configure the authentication mode:

- Go to Settings > Security > Access Control > Authentication
- Choose one of the following:
  - Open – No authentication
  - Authentication Required – Uses Local RFIDs
  - Cloud Authentication – Enables Cloud RFIDs

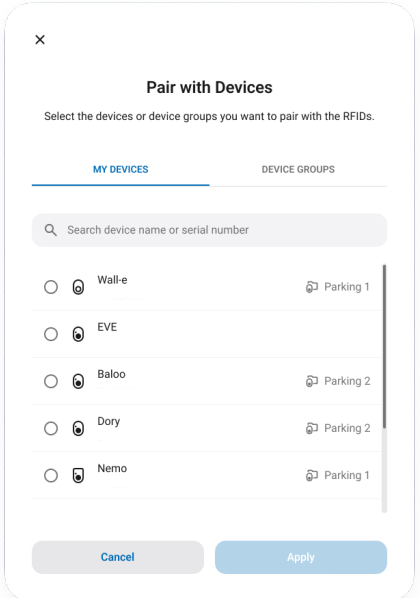


Add RFIDs
RFIDs can be added by simply entering the RFID serial number 1. Users can give a custom name to each RFID, which will be linked to their account. The same RFID code can be associated with multiple accounts, each with a diff erent given name.

By default, RFIDs display the consumption accrued from the start of the current month. For more detailed insights, users can generate a dedicated RFID report.

Consumption data is visible to any user who has added the RFID to their account, regardless of their role.

1 An RFID serial number – also known as a Unique Identifi er (UID) or Electronic Product Code (EPC) – is a unique code assigned to each RFID tag. It identifi es the tag and the item it's attached to, even among identical products. The serial number can be read using any compatible RFID reader, including some smartphone apps. It typically appears in a format like 00:00:00:00:00:00:00:00.

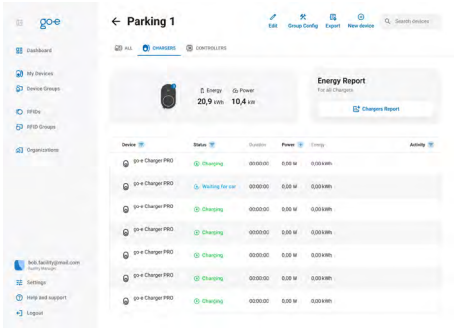


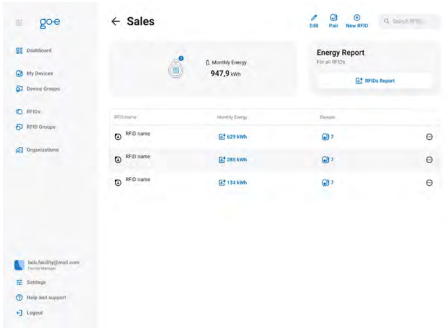
Assign device
Users can pair a Cloud RFID with a device only if they have full access to that device or have Organization Admin rights. Members who already have assigned devices cannot pair the RFID with those devices.

RFIDs can be paired with a single device, a selection of devices, or an entire device group.

2. Functionalities

Groups





Devices
Devices can be grouped together for various purposes, such as by location, business unit, or shared confi gurations and parameters. A single device can belong to multiple groups. Only authenticated devices can be included in groups.

Groups are linked to individual user accounts, meaning the same device can belong to diff erent groups for diff erent users, and each user can only see their own device groups.

Energy reports can be generated directly within a group, covering all devices in that group.

RFIDs
RFIDs can be grouped for various purposes, such as personas, business units, or locations. A single RFID can belong to multiple groups. Groups are linked to individual user accounts, so the same RFID may be in diff erent groups for diff erent users.

Energy reports can be generated easily within each group, covering all RFIDs included.

Configure Devices

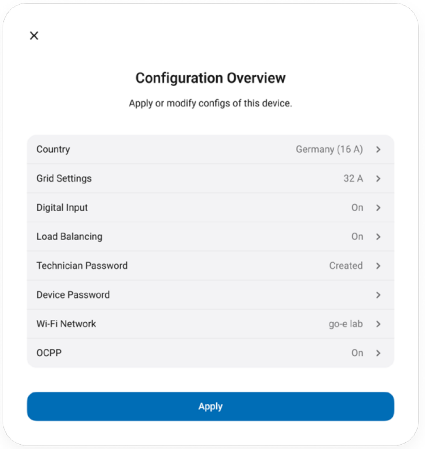
Configuration Note: Only authenticated devices can receive and apply confi gurations. If a device is offl ine, the confi guration will be queued and automatically applied once the device comes online.

- Queued configurations can be manually deleted any time.
- If the device does not reconnect within 7 days, the configuration will be automatically canceled.

Devices can be bulk configured with common settings such as:

- Country
- Grid settings
- Device password
- Technician password
- Digital input
- Wi-Fi/Network parameters
- OCPP
- Load Balancing

These configurations can be applied to a single device, a selection of devices, or an entire device group.

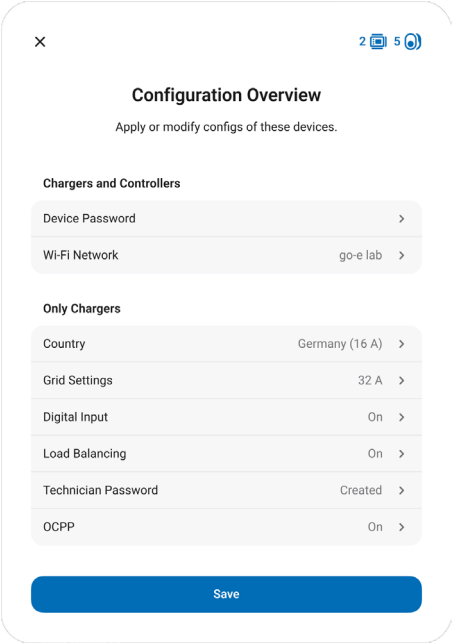


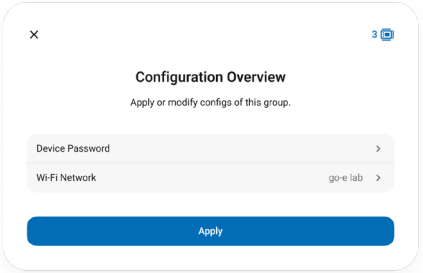
Single
Configuring a single device offers access to more detailed parameters, as some settings are specific to each device. For example, Network configurations, OCPP, and Load balancing settings are fully available when configuring an individual device.

In contrast, when configuring a group or a selection of devices, the available settings are more limited to those that can be commonly applied across multiple devices.

2. Functionalities

Configure Devices





Charger vs Controller
Controllers have a limited set of configurable parameters, primarily Device Password and Network settings.

When both controllers and chargers are selected for configuration, these common settings can be applied to both device types.

Consumption Report

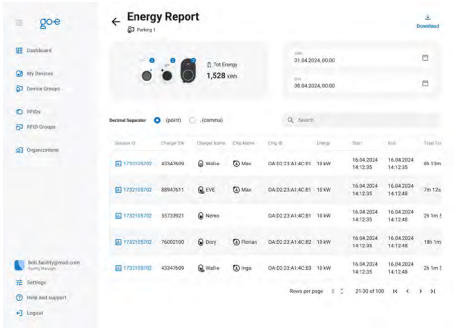
The Portal allows users to create custom energy consumption reports for specific time periods, covering chargers, controllers, and RFIDs. Reports can be generated for a single device, a selection of devices, or an entire device group.

By default, the reporting period runs from the beginning of the current month to the current day. Users can also choose the decimal separator (comma or point) before generating the report.

Consumption Reports Note:
Reports can be generated even for offline devices. Charging sessions are stored in the backend and synced every 8 hours, so a new session will appear in the report after the next scheduled backend update.

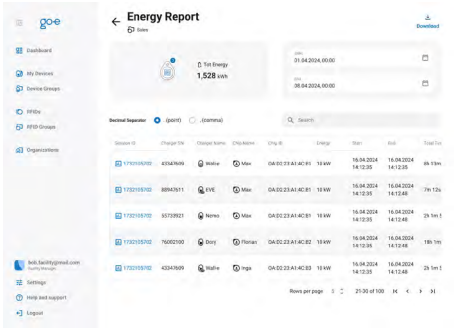
2. Functionalities

Consumption Report

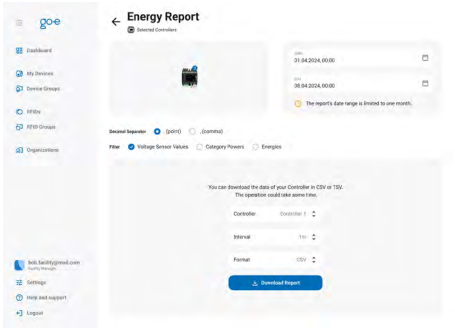


Charger & RFIDs
Chargers and RFID reports include the following information:

- Session ID
- Charger serial number
- Charger name
- RFID (Chip) name
- RFID (Chip) ID
- Total energy consumed
- Session start and stop times
- Total active charging time

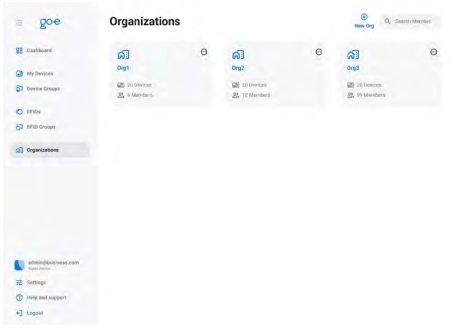


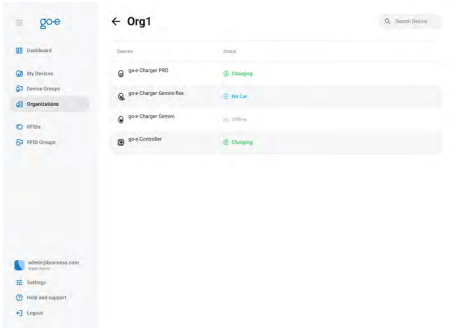
Each session can be expanded to reveal detailed technical information. Reports can be downloaded in CSV, TSV, or PDF formats.



Controller
Controller reports can only be generated for individual devices due to the detailed nature of the data.
The maximum report period is limited to one month. Users can customize the report by setting intervals and applying specific filters. Reports are available for download in CSV and TSV formats.

Organizations





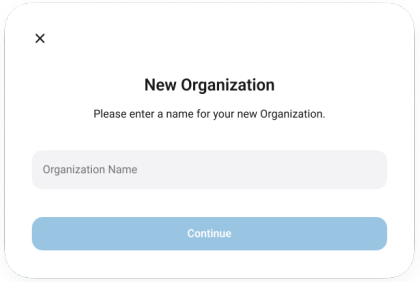
Organizations are designed to simplify user access management across multiple devices. They provide an ideal solution for companies with shared chargers, allowing administrators to restrict functionalities and editing rights based on each user's role.

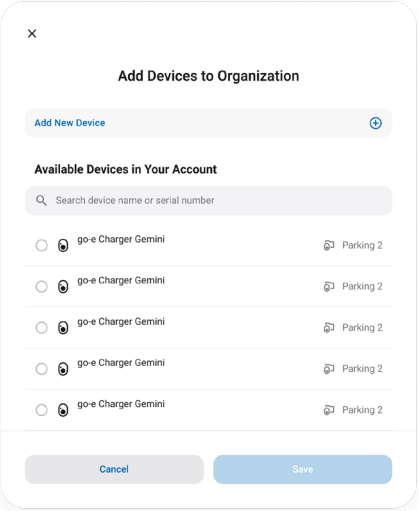
Roles

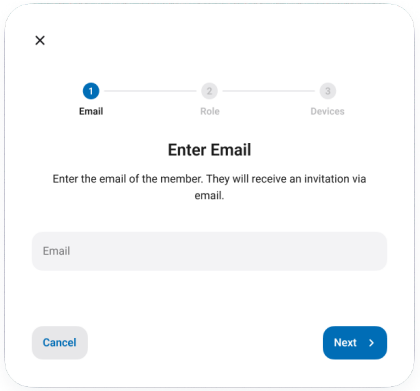
- Organization Admin: Can create and manage organizations, control user access, and have full control over all devices within the organization.
- Member: Can use basic features on devices assigned to them within the organization.

2. Functionalities

Organizations







Create / Manage
An **Organization Admin** can create and fully manage organizations. They have theability to add or remove authenticated devices from their account to the organization.

Members can be added to the organization and assigned to specific devices, including both chargers and controllers.

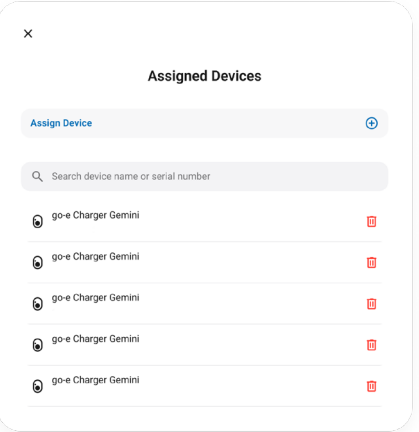
A user can belong to multiple organizations and hold different roles in each – for example, a Member in one organization and an Organization Admin in another.

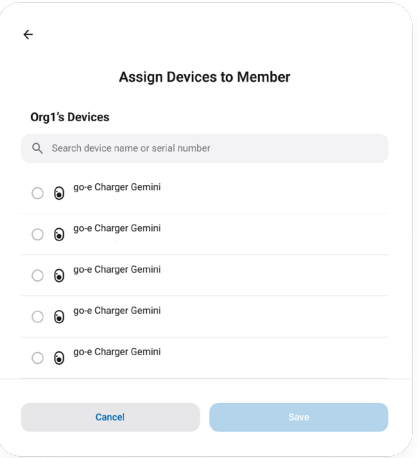
Invite
Users can be invited to join an organization via email. If they don't already have an
account, they will be prompted to create one by setting a password to access the portal.

Assign devices
Devices added to an organization can be assigned or unassigned to individual members or groups of members. Members will see these devices in the Organization section with limited information. By entering the device password, members can access the full set of functionalities.

Organization Admins automatically have all organization devices assigned and authenticated, granting them full functionality by default.

Devices can belong to multiple organizations simultaneously.





3. Use Cases Examples

Use case 1: Single Owner (Consumer)

Scenario
A single EV owner uses the Portal to manage their personal charger at home. They add their device by entering its Serial Number and Device Password, gaining full control over the charger's settings and usage.

The owner can monitor charging sessions, set energy limits, configure tariffs, and generate detailed reports. They also manage their own RFIDs for easy authentication and track consumption seamlessly – all from their personal account without the complexity of organizational roles or multiple users.

Key Role
A private individual who owns one or more chargers and RFIDs for personal use. This user manages their devices independently without any organizational structure.

Access & Authentication:
- The user creates an account by registering with a valid email and password, agreeing to Terms & Conditions, and confirming their email via a verification link.
- The user logs into the Portal and accesses their devices through My Devices.

Device Management:
- The user adds chargers and controllers by entering the device's Serial Number and Device Password (found on the Reset or Data Card).
- Devices added this way appear in My Devices, giving the user full control over them, regardless of role.
- The user can add RFIDs (to enable charging only with authentication, e.g. in shared spaces, like a condo parking lot) by entering the RFID code and assigning custom names. RFID is then paired with the charger.
- The user can configure device settings like country, grid settings, passwords, and network parameters on single devices, selections, or groups.

Functionality & Features:
- The user can fully operate chargers, including starting and stopping charging sessions, setting charging rules (energy limits, Flexible tariff price limit, charging speed), and selecting charging modes.
- The user can configure energy tariff parameters (country, provider, price limits) and access photovoltaic-related functionalities if applicable.
- Access to live data and analytics for the last 6-24 hours of charger usage (status changes, temperature, voltage, energy) is available.
- The user has access to basic and extended settings for single devices, including network configurations, OCPP, and load balancing (usually done by a technician).

Reporting:
- The user can generate custom energy consumption reports for the charger or RFIDs over specific time periods.
- Reports default to the current month but can be customized with different date ranges and decimal separators.
- Chargers and RFID reports include session details such as session ID, charger serial number, chip name and ID, total energy, start/stop times, and total active charging time, with detailed technical information available.

Anonymous Access:
- The user can also operate devices without logging in by using the "Use without Account" feature, which allows adding devices via Serial Number and Password for full device control.
- Device data in Anonymous mode is cached locally in the browser until cleared.

Password Management:
- In case of forgotten passwords, the user can reset it by submitting their registered email on the authentication page and receiving a reset link.

3. Use Cases Examples

Use case 2: On-site charging (Shared devices in an Office Parking Lot)

Scenario
An organization has installed multiple EV chargers in its office parking lot. These chargers are shared among employees. Access and functionality are managed by a Fleet Manager (Organization Admin), who controls which users (employees) can use which chargers and what level of access they have.

Key Roles
Fleet Manager (Organization Admin):
- Manages the organization account in the Portal.
- Adds, assigns, and configures chargers.
- Controls user access and role-based permissions.

Employees (Members):
- Use the chargers assigned to them within the organization.
- Have limited access based on their Member role (e.g., charging, basic settings, reporting).

Step-by-Step Workflow

1. Setup
- The Fleet Manager creates an Organization in the Portal.
- Devices (chargers and controllers) are authenticated by adding them using their Serial Number and Device Password.
- These authenticated devices are added to the Organization and are automatically available to the Fleet Manager with full access.

2. User Management
- Employees are invited via email to join the Organization.
- If an employee doesn't have an existing account, they set up one by creating a password. Each employee is added as a Member and assigned specific chargers they're allowed to use.

3. Access & Usage
- Employees access their assigned chargers under the Organization section.
- By default, Members have limited functionality (e.g., start/stop charging, view basic info).
- If needed, employees can fully control a charger by entering the Device Password (if permitted).

4. RFID Management
- Employees can add their own RFID chips to their accounts by entering the RFID code and giving a name.
- RFIDs can then be paired to specific chargers or charger groups by the Fleet Manager.
- Each employee can view energy consumption tied to their own RFID chip.

5. Device Grouping
- The Fleet Manager groups chargers by location (e.g., „Basement Parking", „Front Lot") or user type (e.g., „Executives", „Visitors").
- This simplifies bulk configuration and reporting.

6. Configuration
- The Fleet Manager configures common settings (Network, Device passwords, etc.) for all chargers or specific groups.
- Device configuration allows advanced features like OCPP setup, Load Balancing, and Wi-Fi settings.

7. Reporting
- Energy consumption reports can be generated per charger, RFID, device group, and RFID group.
- Members can view their own session history via RFID reports.
- The Fleet Manager can export reports in CSV, TSV or PDF formats, choosing custom time ranges and decimal separators.

3. Use Cases Examples

Use case 3: Chargers configuration and maintenance (installers)

Scenario
A professional installer is tasked with setting up and configuring several EV chargers at a customer location (e.g., office, public parking, or commercial fleet depot). The installer needs to quickly onboard, configure, and test multiple chargers, ensuring correct network setup, grid settings, and operational readiness.

Key Role
Installer / Technician (Authenticated User or Temporary Access):
- Does not necessarily belong to the final organization but may use their own account or temporary credentials.
- Has device-level access via Serial Number and Device Password.
- Operates mainly through the „My Devices“ section.

Step-by-Step Workflow

1. Accessing the Portal
- The installer either logs into their own Portal account or uses the “Use without Account” option for temporary setup.
- Devices are added by entering the Serial Number and Device Password, granting full control.

2. Bulk Onboarding
- All chargers on-site are added to “My Devices” using the serial number and password.
- Devices remain visible and controllable until the browser cache is cleared (in Anonymous mode) or permanently if authenticated.

3. Initial Configuration
The installer performs initial setup:
- Country & Grid settings
- Device Passwords and Technician Passwords
- Digital Input configurations
- Wi-Fi / Network Parameters

These settings can be applied:
- Individually (for fine-tuned setups)
- On a selection of devices (for common configurations)
- To device groups (e.g., all chargers in the same parking row)

4. Advanced Configuration (Single Device Mode)
When configuring a single charger, the installer can access:
- Full network settings (SSID, IP settings, etc.)
- OCPP endpoint configuration
- Load Balancing parameters
- Extended diagnostics and error reporting

5. Testing & Validation
- The installer starts and stops charging sessions to ensure functionality.
- Checks live metrics (voltage, temperature, energy flow) for verification.
- Optionally pairs an RFID to test user authentication and tracking.

6. Hand-off to Organization
After installation, the installer:
- Transfers the device to the customer’s organization (if applicable).
- Provides the Device Password to the Organization Admin for future control.
- Optionally invites the admin to create an account and to let him assign devices.

7. Ongoing Maintenance
If required, the installer can return later and re-authenticate using the Serial Number and Password to:
- Update firmware
- Reconfigure settings
- Troubleshoot network or operational issues

3. Use Cases Examples

Use case 4: Charging on demand (Hotel)

Scenario
A hotel offers EV charging services to its guests as an added amenity. To ensure a frictionless experience, guests do not need to create an account or interact with the Portal. Instead, they are given (or allowed to use) an RFID chip to authenticate and use a charger. The hotel uses the Portal to track usage and generate reports for billing purposes.

Key Roles
Hotel Guest:
• No portal account required
• Uses a temporary RFID to access chargers
Hotel Front-Desk / Fleet Manager:
• Prepares and issues RFID chips
• Manages chargers in the Portal under a dedicated "Hotel" organization
• Generates consumption reports to bill guests

Step-by-Step Workflow

1. Hotel Setup
• The Fleet Manager authenticates all on-site chargers by adding them (Serial Number + Device Password) to the "Hotel" organization.
• Chargers are grouped (e.g., "Underground Parking," "Front Parking") for easy management.
• A pool of RFID chips is created in the Portal and pre-paired with the Hotel's chargers.

2. Guest Check-In
• At arrival, the front desk hands the guest one of the RFID chips – no account creation or password is needed. The guest proceeds to the charging area.

3. Guest Charging
• The guest taps their RFID at the charger to start a session
• The charger reads the RFID, authenticates it against the Hotel's organization list, and begins charging.
• Live status, session start/stop times, and energy consumption are handled by the charger; no portal login is needed for the guest.

4. Session Tracking & Reporting
• Each charging session is automatically tagged with the guest's RFID ID.
• Hotel staff can generate an RFID-based report covering all sessions for any time period, specifically in this case for the duration of the guest stay.
• Reports include Session ID, Charger serial number, RFID ID, total energy, start/stop times, and active charging duration.

5. Guest Check-Out & Billing
• The Hotel Fleet Manager exports the RFID report in CSV, TSV, or PDF format.
• Consumption costs are applied to the guest's final bill. The hotel collects payment based on the detailed usage report.
• RFID chips are then returned to the pool for reuse by future guests.

4. Contact and support

Do you still have questions about the go-e Charger?

You can find helpful answers concerning the most frequently asked questions, help for technical problems and troubleshooting on:
www.go-e.com

If you cannot find an answer to your question in this guide, on our website or in the app, please feel free to contact us:

Support

go-e GmbH

Satellitenstraße 1
9560 Feldkirchen
AUSTRIA

support@go-e.com

+43 4276 62400

www.go-e.com