Testing Phase Notice: Eve Control is currently in a testing phase. We advise connecting only chargers that you or your partners have easy local access to, so they can be reconfigured on-site in case of unexpected behaviour. Please also note that this documentation is still in its validation phase and may contain errors.

Documentation Update: Sections in red were added or rewritten in this release. They reflect significant application changes — in particular the new **Add Device** flow on the Charging Stations page and the new self-service **Primary Backoffice** connection model. Sections shown in the default colour are unchanged. See `CHANGELOG.txt` for the full list of changes.

Eve Control User Guide

This guide walks you through the essential processes for managing your Alfen charging infrastructure using the Eve Control platform at **control.alfen.com**.

REWRITTEN

1. Connect a Charger to Eve Control

Before you can claim and manage a charger in Eve Control, the charger must be configured to connect to the Eve Control OCPP server. There are two ways to do this: using local installation tooling at the charger, or remotely via OCPP settings in your current backoffice.

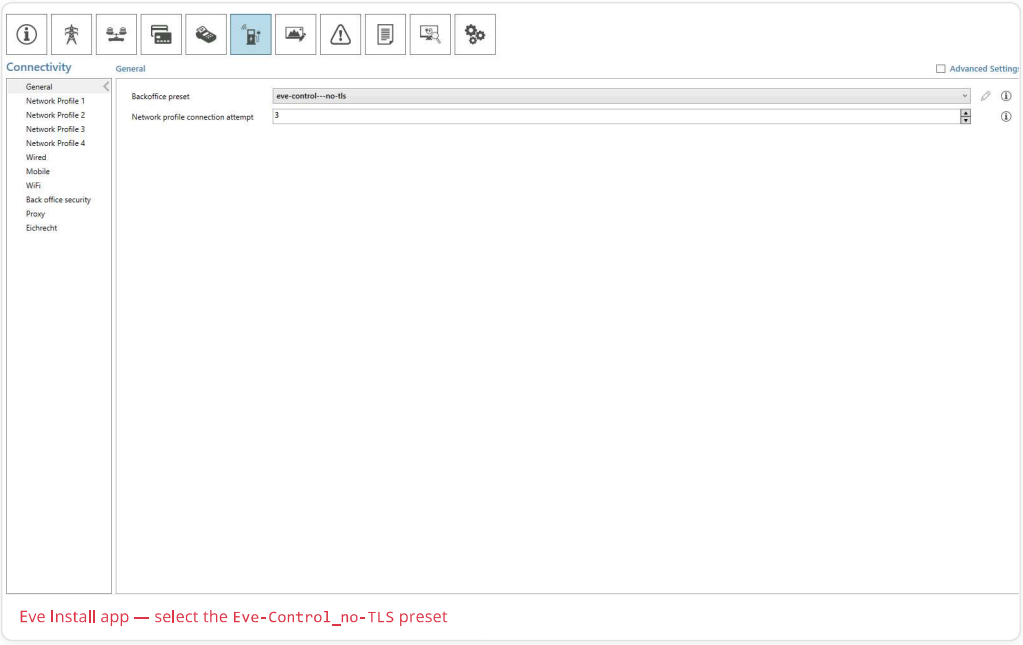
Option A: Via Local Installation Tooling

1 Connect to the Charger

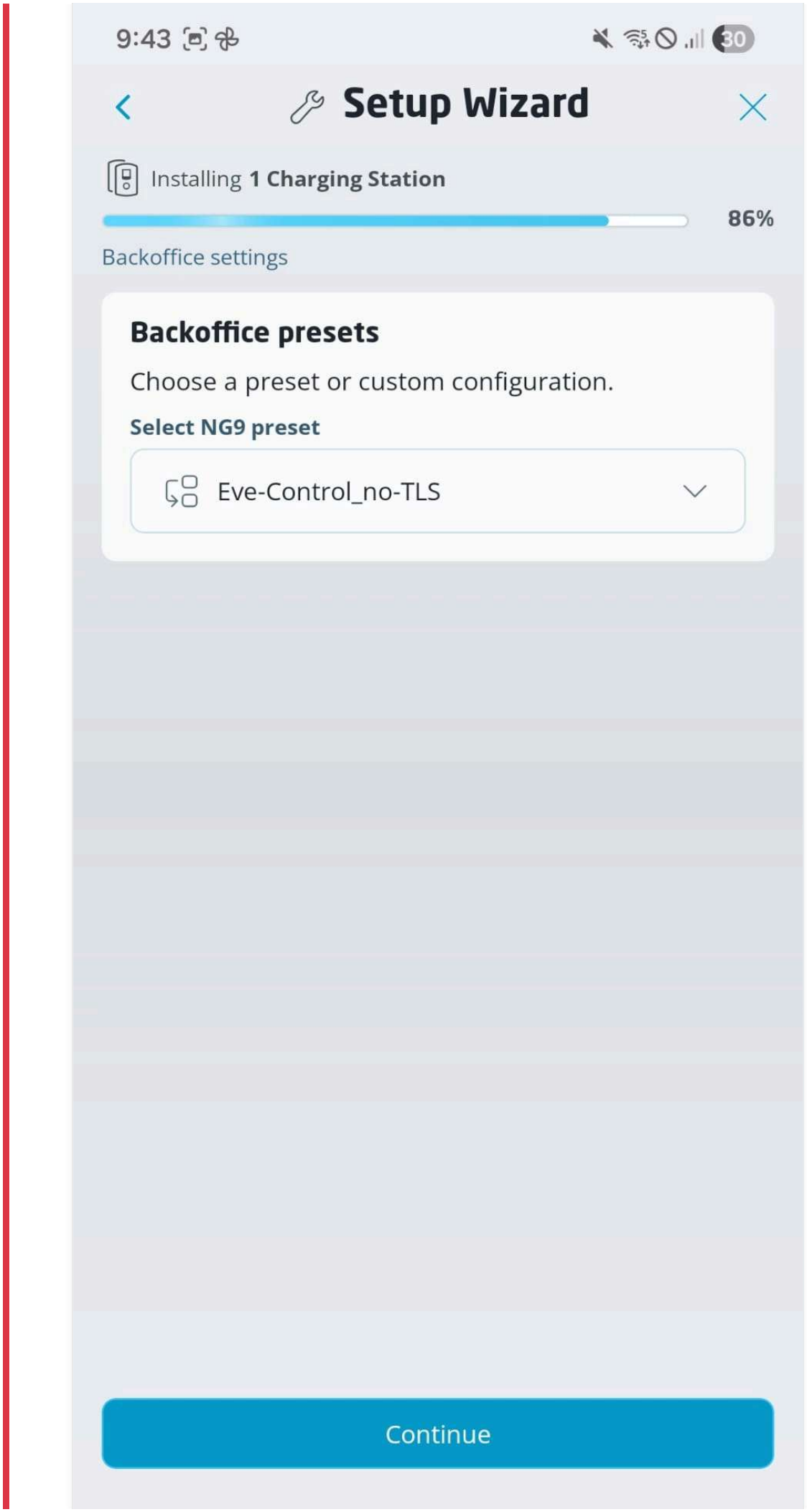
Use the **ACE Service Installer**, **MyEve**, or the new **Eve Install** app to connect to the charger locally.

2 Select the Eve Control Preset and Reboot

In the installation tool, select the **Eve Control** preset. The preset is called `eve-control---no tls` in ACE Service Installer and `Eve-Control_no-TLS` in Eve Install. This automatically configures the charger's OCPP settings to point to the Eve Control server. Then **reboot** the charger to apply the new configuration.



Eve Install app — select the `Eve-Control_no-TLS` preset


9:43
Setup Wizard
Installing 1 Charging Station
86%
Backoffice settings
Backoffice presets
Choose a preset or custom configuration.
Select NG9 preset
Eve-Control_no-TLS
Continue

ACE Service Installer — select the `eve-control---no tls` preset

> **Tip:** This is the recommended approach for initial installations. The preset takes care of all OCPP settings automatically.

Option B: Remotely via OCPP (Current Backoffice)

1 ### Configure a Backoffice Network Profile for Eve Control

In your current backoffice, set an available **BackofficeNetworkProfile** to the following value. For example, if your current backoffice uses BackofficeNetworkProfile1, configure BackofficeNetworkProfile2:

```
ocppVersion{OCPP16}ocppCsmsUrl{ws://ocpp.alfen.com/}messageTimeout{10}securityProfile{0}ocppInterface{Wired0}
```

2 ### For SIM-Connected Chargers (Optional)

If the chargers connect via SIM and the SIM is **not** in a private APN, you can use the wireless profile instead. (Chargers on a private APN cannot reach

```
ocppVersion{OCPP16}ocppCsmsUrl{ws://ocpp.alfen.com/}messageTimeout{30}securityProfile{0}ocppInterface{Wireless0}apn{YOURSIMAPN}apnUs
```

In case of using an **Alfen / ICU Connect SIM card**, use the following configuration instead:

```
ocppVersion{OCPP16}ocppCsmsUrl{ws://ocpp.alfen.com/}messageTimeout{30}securityProfile{0}ocppInterface{Wireless0}apn{alfen.m2m}apnUse
```

3 ### Set the Network Configuration Priority

Set the OCPP parameter `NetworkConfigurationPriority` to prioritize the Eve Control profile. For example, if Eve Control is in BackofficeNetworkProfile**2** and your current backoffice is in BackofficeNetworkProfile**1**, set the value to `2,1`.

4 ### Reboot the Charger

Send a reboot command to the charger from your current backoffice. After rebooting, the charger will connect to Eve Control.

5 ### Perform a Security Firmware Update

Once the charger is online in Eve Control, perform a **security firmware update** to switch the charger from insecure WebSocket (`ws://`) to secure WebSocket (`wss://`) connectivity. See section 10: Changing to Secure WebSocket Connectivity for detailed instructions.

> **Important:** After the charger connects to Eve Control, you can optionally reconnect it to your existing backoffice *through* Eve Control using the **Backoffice** tab on the charger page (see section 9: Connect a Primary Backoffice). This way Eve Control acts as an intermediary, and you retain visibility and control through both systems.

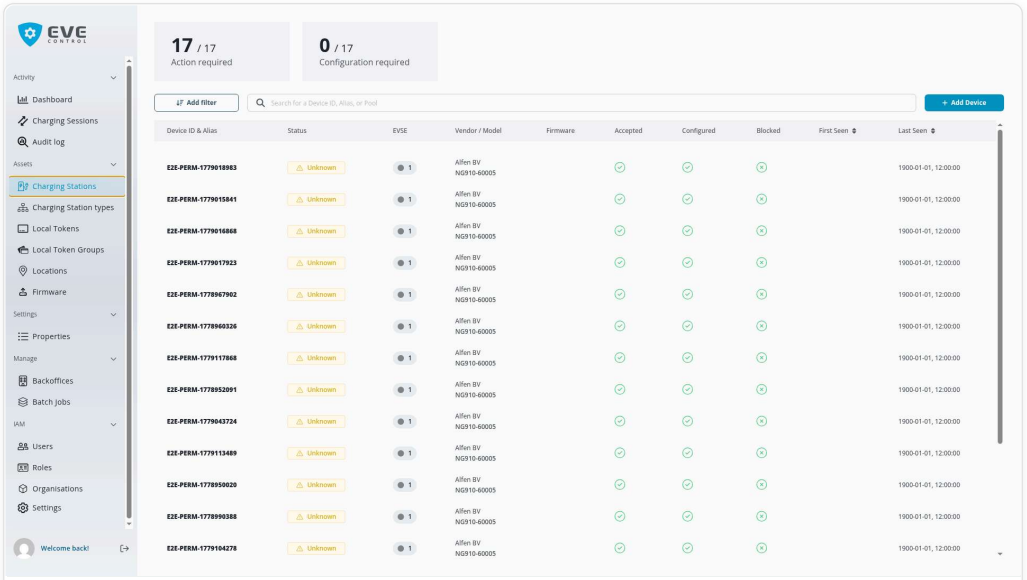
REWRITTEN

2. Add a Device

Adding a charger to Eve Control happens through the **Add Device** button on the Charging Stations page. After you enter the charger ID, the platform looks up the device and shows the appropriate follow-up form depending on whether the charger is already known to the platform.

1 Navigate to Charging Stations

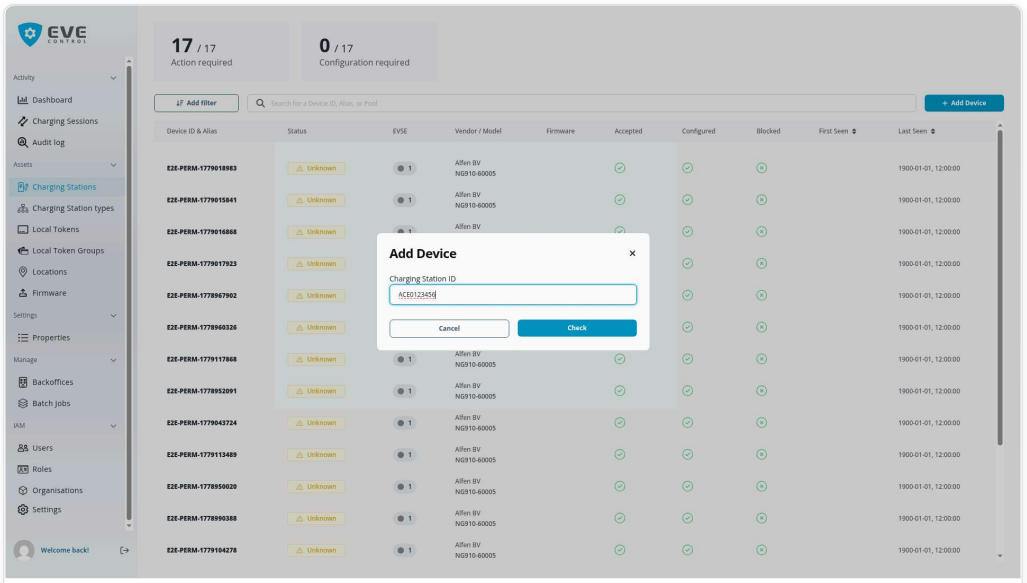
Click **Charging Stations** in the left sidebar to open the charging stations overview page, then click the **Add Device** button at the top of the list.



The Charging Stations overview page — the “Add Device” button is at the top right

2 Enter the Charging Station ID and click Check

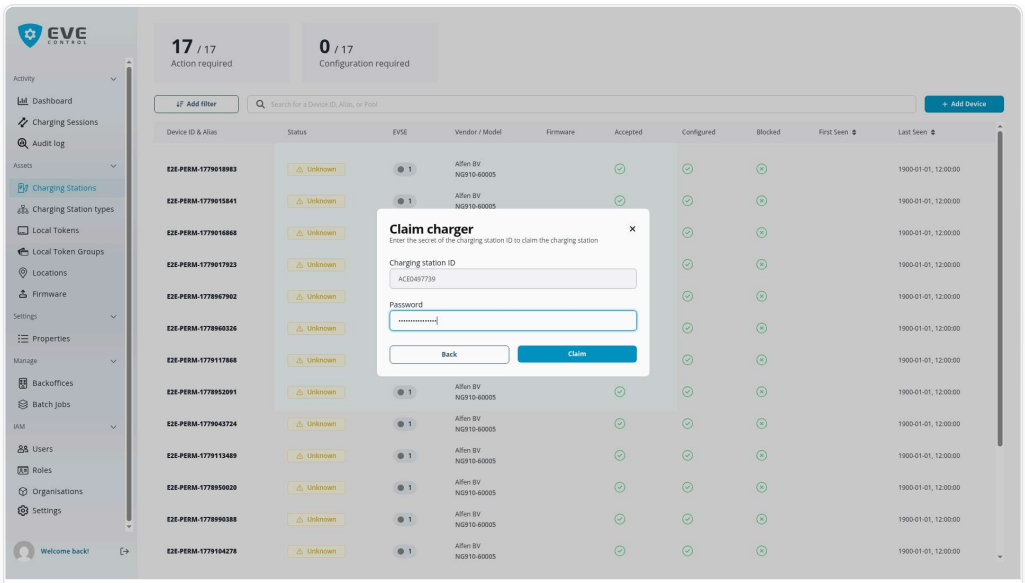
Type the charger’s **OCPP Identifier** — the identifier with which the charger communicates to the backoffice — into the field and click **Check**. This is not necessarily the serial number: the OCPP Identifier may have been changed after purchase. Eve Control looks up the device and presents the correct next step.



The Add Device dialog — enter the Charging Station ID and click Check

3a Outcome — Claim form (charger already exists in Eve Control)

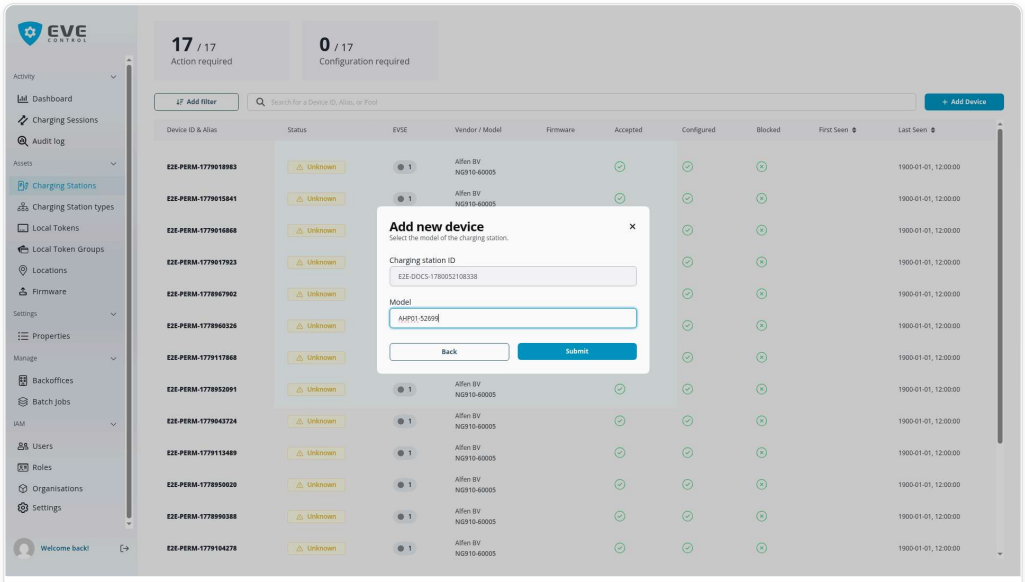
If the device already exists in Eve Control, a **Claim** form appears. Enter the **default charger password** from the charger password flyer and click **Claim**. After a successful claim, the charger appears in your Charging Stations list.



The Claim form — appears for devices that already exist in Eve Control

3b Outcome — Create form (charger not yet registered)

If the device is not yet registered in Eve Control — because the OCPP Identification Number in the charging station has been changed after purchasing — a **Create new device** form appears. Pick the correct **Model** from the searchable list and click **Submit**. This registers the charging station so it can connect to the platform.



The Create form — appears when the device is not yet known to the platform

3c Outcome — Already claimed

If the device is already owned by your organisation, you will see an **Already Claimed** message — the charger is already in your Charging Stations list and no further action is needed.

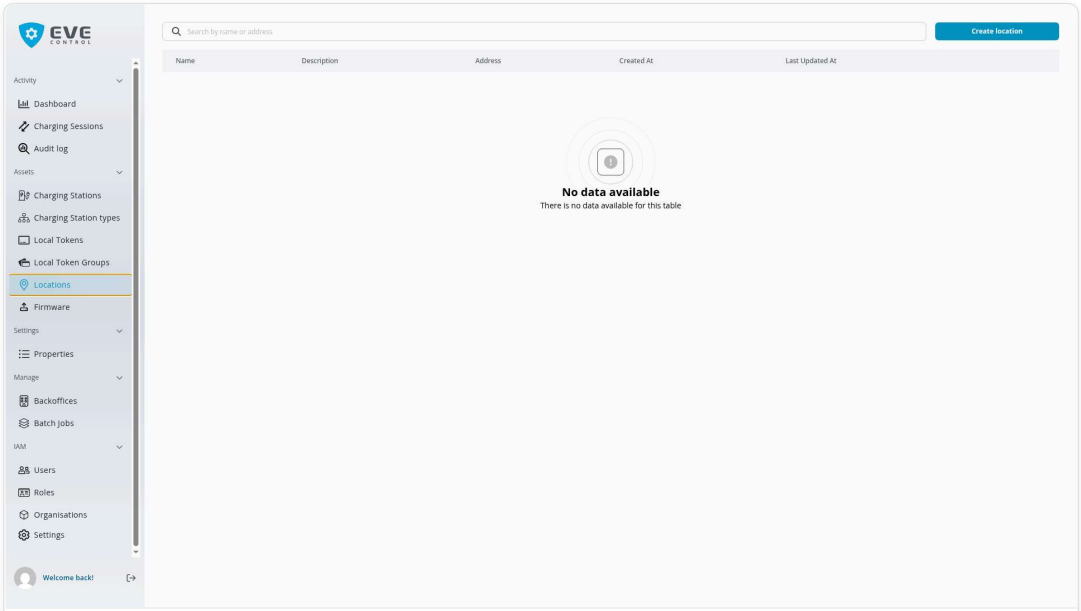
> **Tip:** Always use the charger's **OCPP Identifier** — the identifier with which the charger is communicating to the backoffice. This is not necessarily the serial number; the OCPP Identifier may have been changed after purchasing the device. The default charger password is printed on the charger label or included in the delivery paperwork.

3. Create a Location

Locations let you group chargers by physical site. Creating a location is required before you can assign chargers and manage access through token groups.

1 ### Navigate to Locations

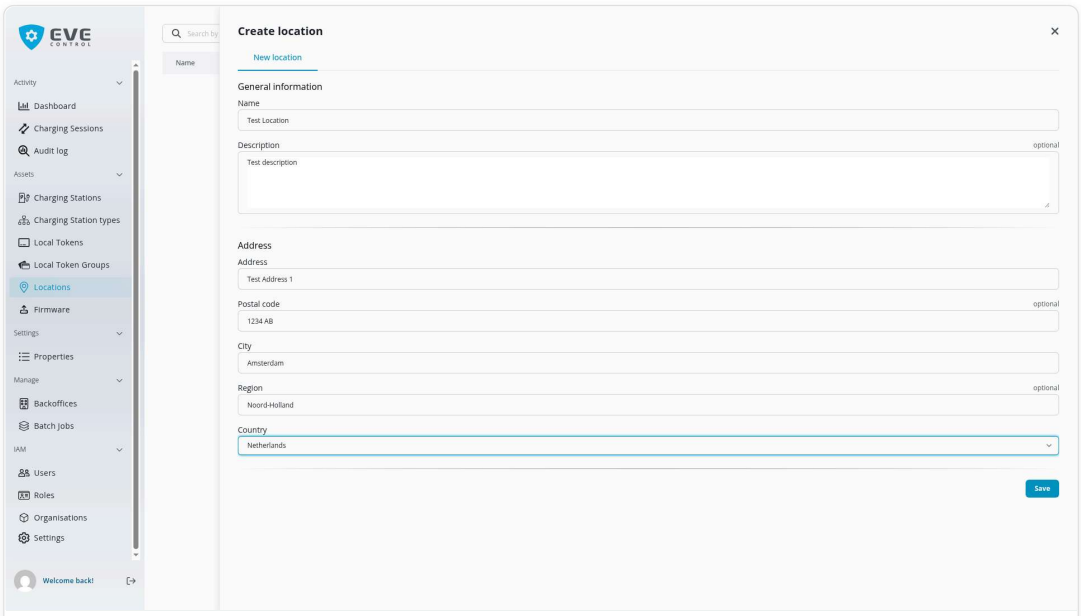
Click **Locations** in the left sidebar.



The Locations page before any locations are created

2 ### Fill in the Location Details

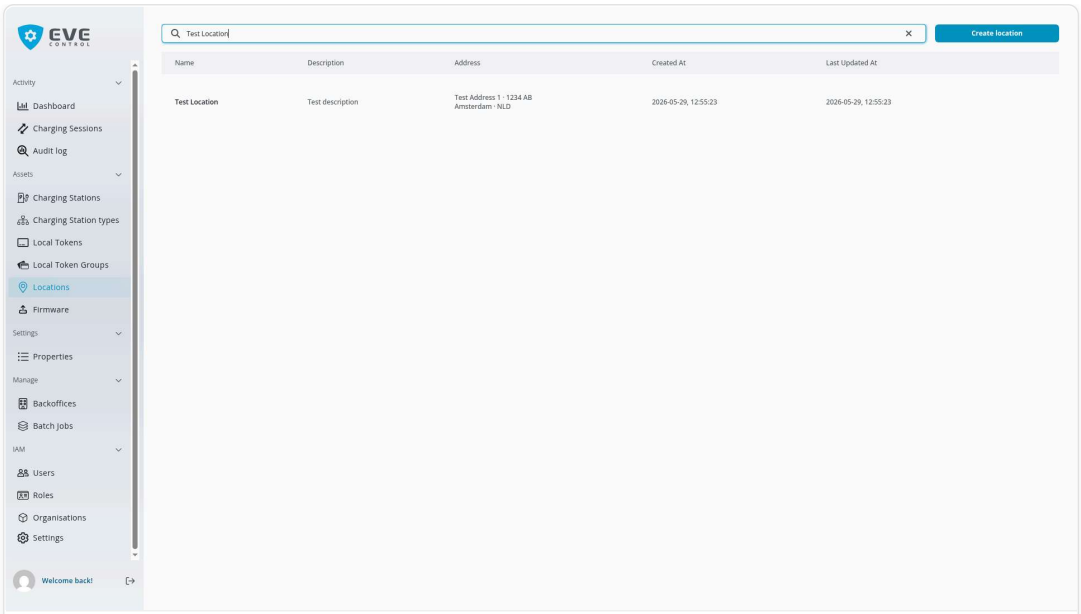
Click the **Create** button and fill in the location form: name, description, address, postal code, city, region, and country. Then click **Save**.



The location creation form with all fields filled in

3 ### Verify the Location

After saving, the new location appears in the locations list.



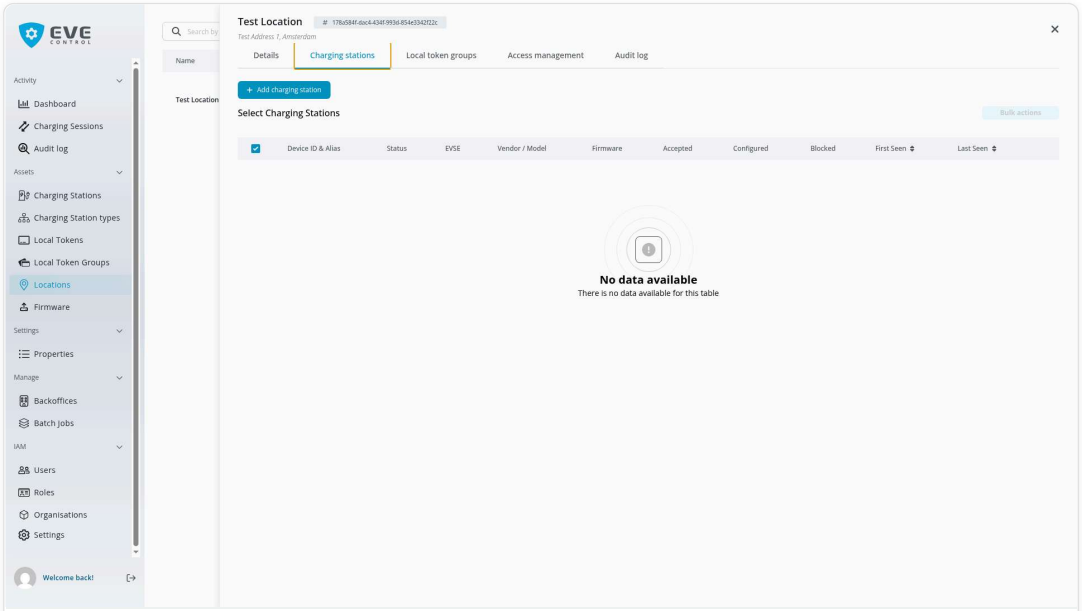
The new location now appears in the list

4. Add a Charging Station to a Location

Assigning a charger to a location enables location-based access control using token groups. A charger must be claimed first.

1 ### Open the Location and go to Charging Stations

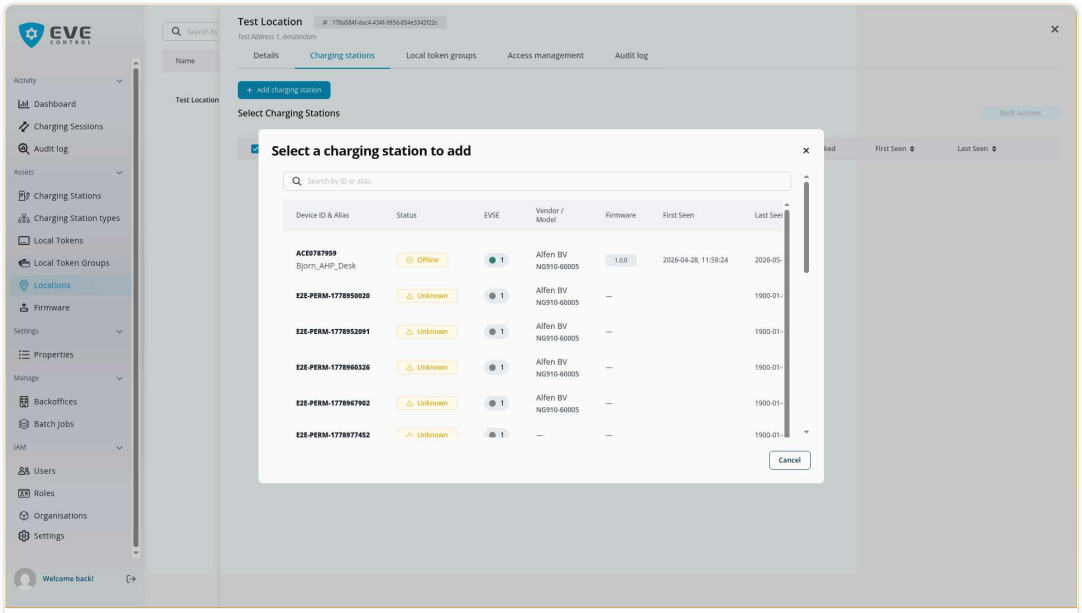
Navigate to **Locations**, click on the location you want, then select the **Charging stations** tab.



The Charging stations tab of a location (no chargers assigned yet)

2 ### Select a Charger

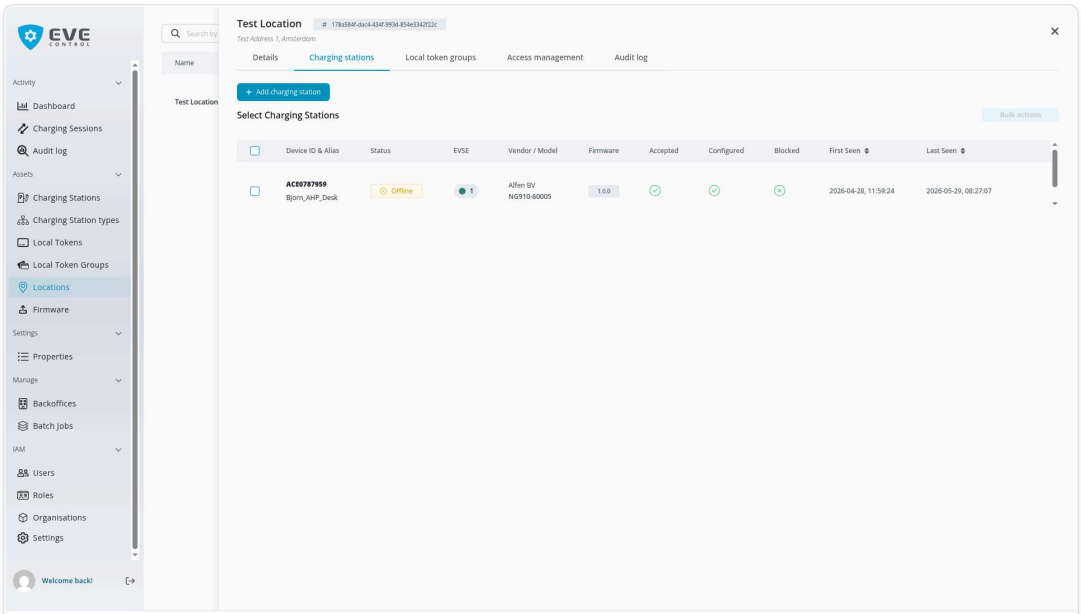
Click **Add charging station**. A list of available (unassigned) chargers appears. Click on the charger you want to add.



Selecting a charger to add to this location

3 ### Confirm

The charger now appears in the location's charging stations list.



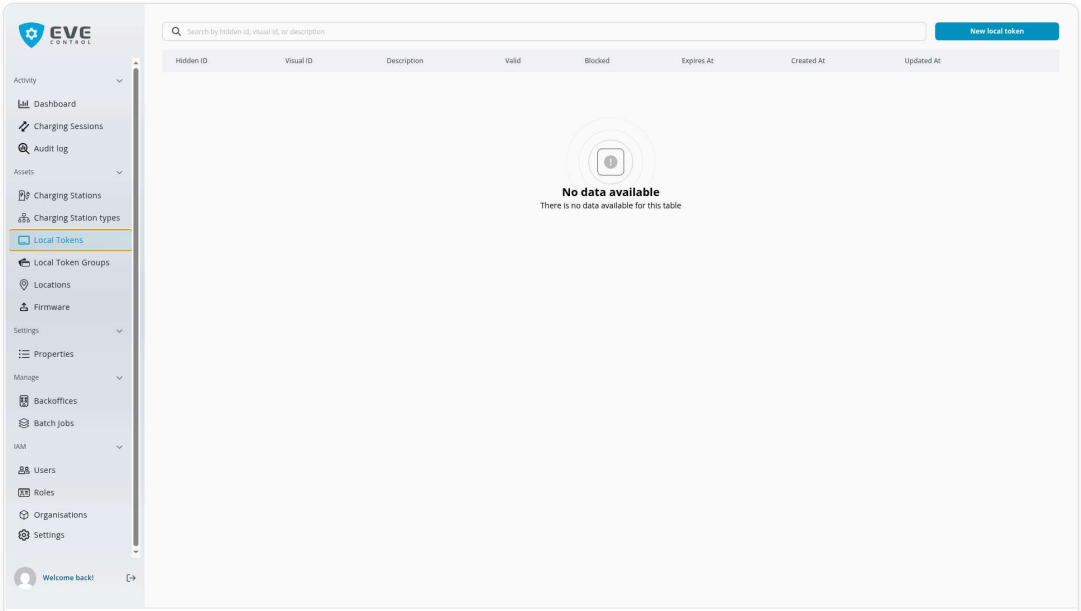
The charger is now assigned to this location

5. Create a Local Token

A local token represents a charge card or RFID tag. You create tokens to manage which cards are allowed to start charging sessions on your chargers.

1 ### Navigate to Local Tokens

Click **Local tokens** in the left sidebar.



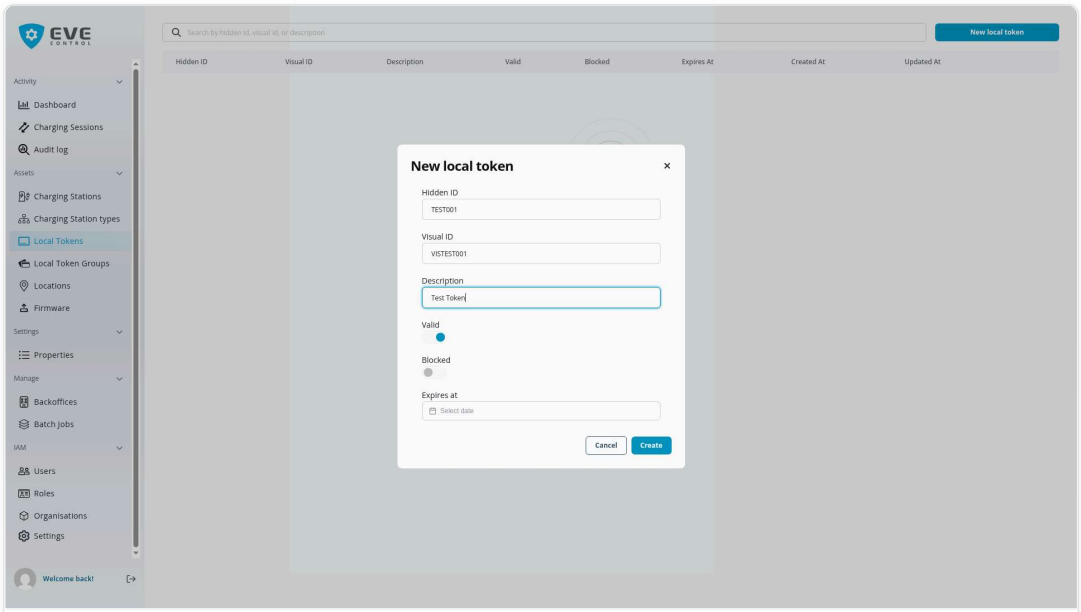
The Local Tokens page

2 ### Fill in Token Details

Click **Create** and fill in the form:

- **Hidden ID –** the internal UID of the charge card. See section 18: Finding a Card's Hidden ID for how to obtain this value.
- **Visual ID –** the number printed visibly on the card
- **Description –** a friendly name for the token (e.g. the card holder's name)

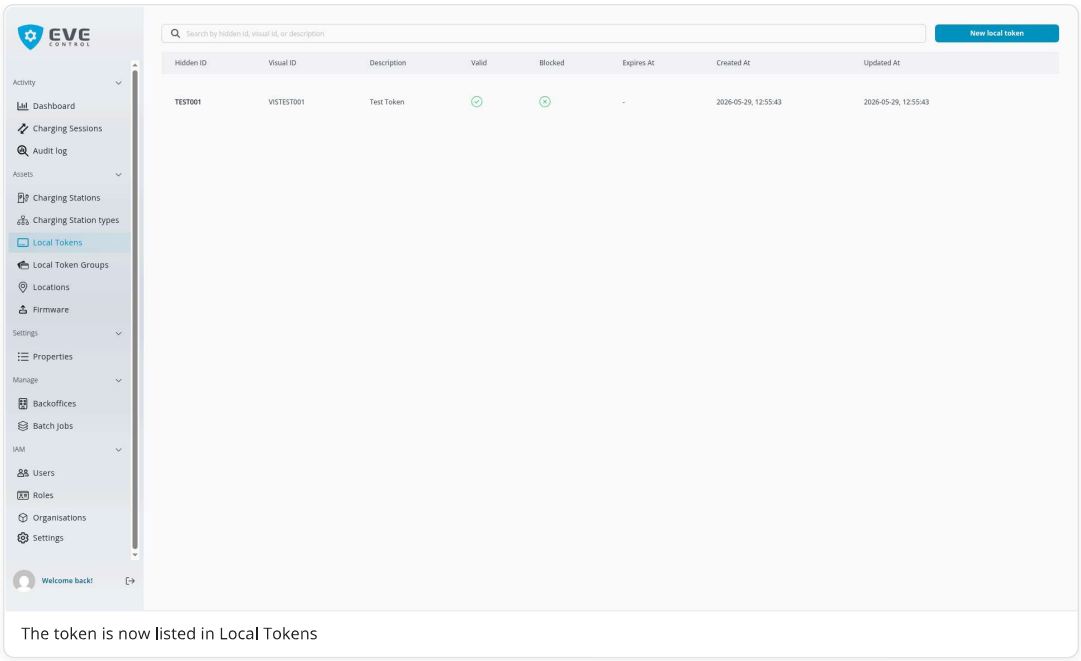
Then click **Create**.



The token creation form with all fields filled in

3 ### Verify the Token

The new token appears in the list.



The token is now listed in Local Tokens

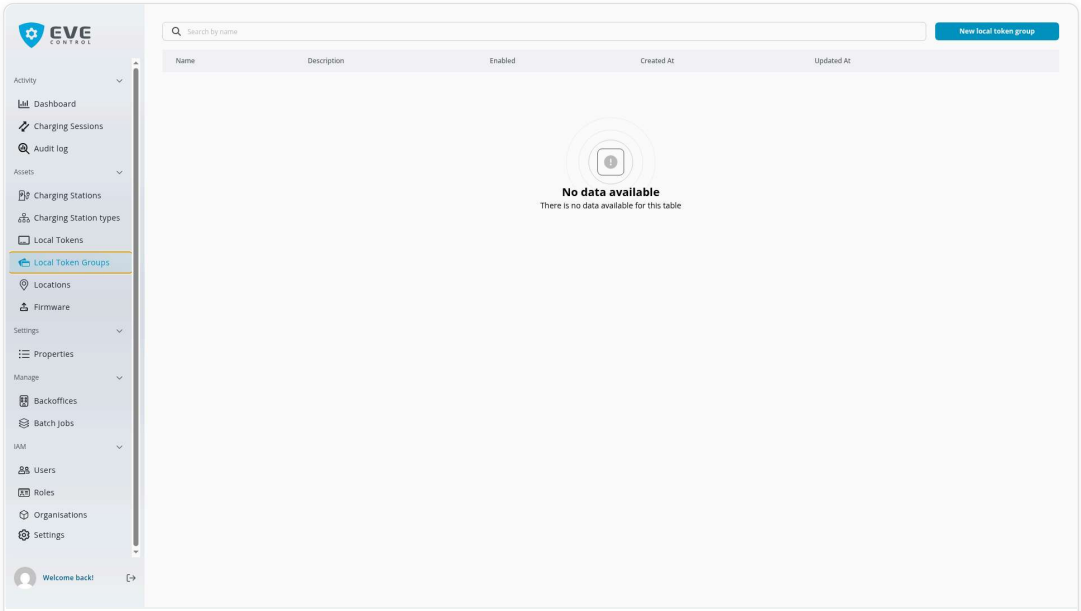
Note: A newly created token is *valid* and *not blocked* by default. However, it will not authorize charging until it is given access to a charger — either directly or through a token group linked to a location.

6. Create a Local Token Group

Token groups let you manage charging access for multiple tokens at once. Instead of granting each token individual charger access, you add tokens to a group and link the group to a location.

1 ### Navigate to Local Token Groups

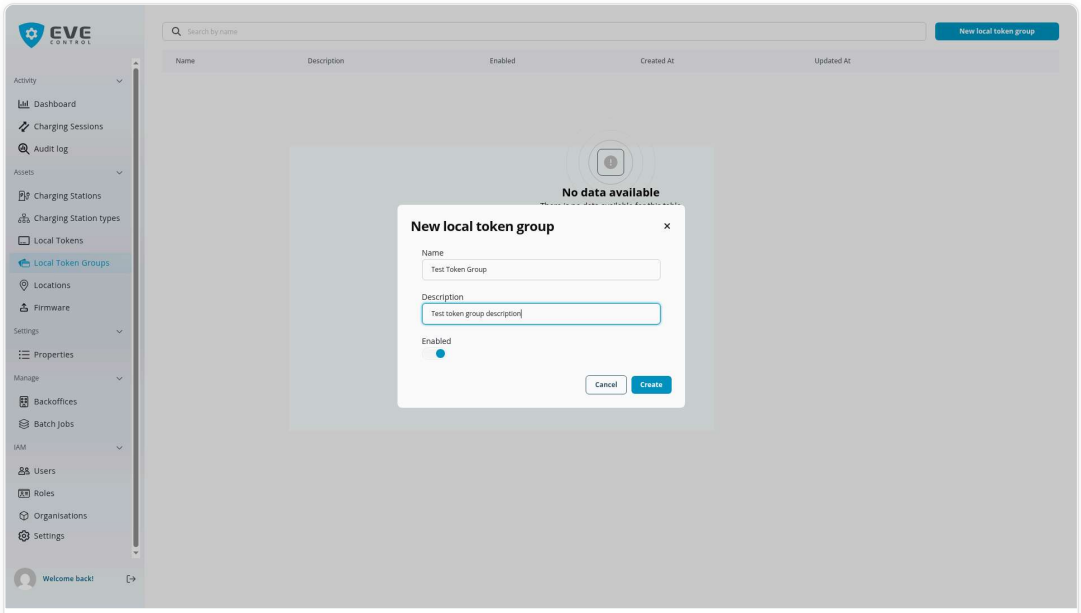
Click **Local token groups** in the left sidebar.



The Local Token Groups page

2 ### Fill in Group Details

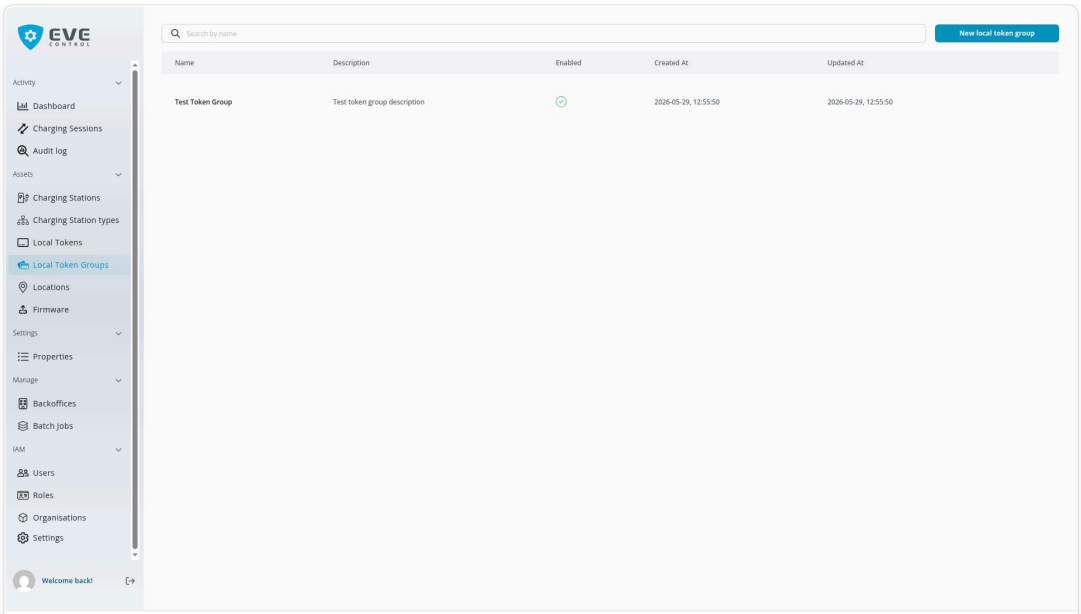
Click **Create** and enter a **name** and **description** for the group, then click **Create**.



The token group creation form

3 ### Verify the Token Group

The new group appears in the list.



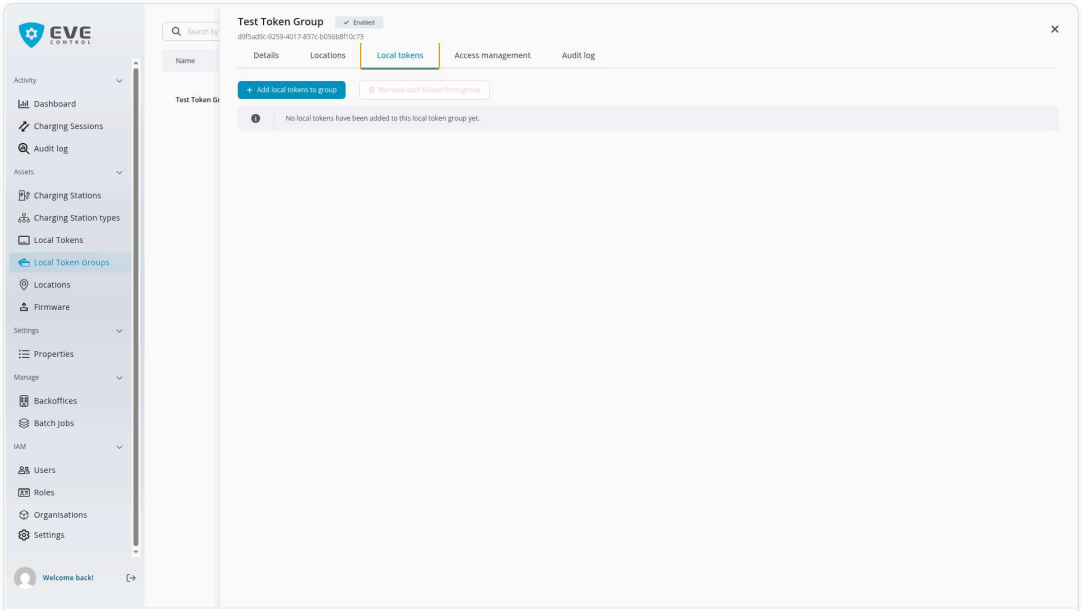
The token group is now listed

7. Add a Token to a Token Group

Adding tokens to a group allows them to inherit the group's location access. All tokens in a group can charge at every location linked to that group.

1 ### Open the Token Group

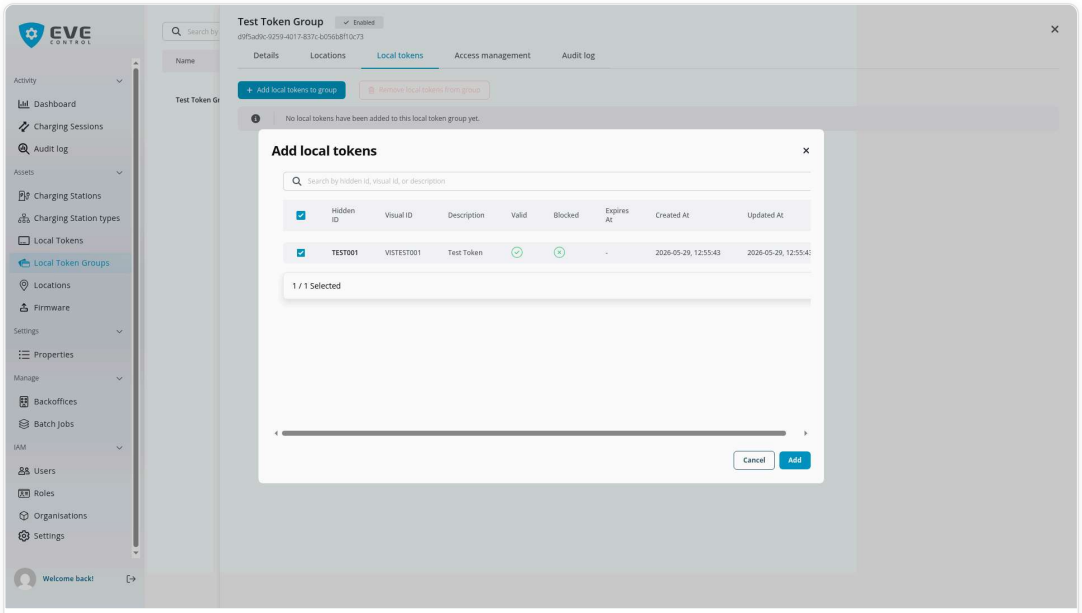
Navigate to **Local token groups** and click on the group. Then select the **Local tokens** tab.



The Local tokens tab of a token group (no tokens added yet)

2 ### Select Tokens to Add

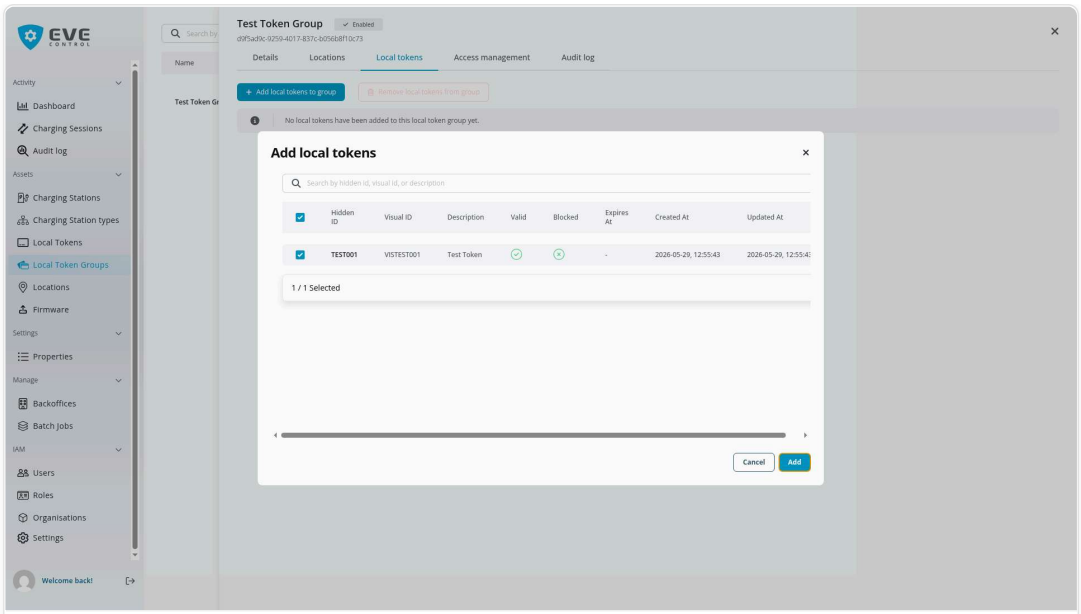
Click **Add local tokens to group**. Check the boxes next to the tokens you want to add, then click the confirm button.



Selecting tokens to add to the group

3 ### Confirm

The selected tokens now appear in the group.



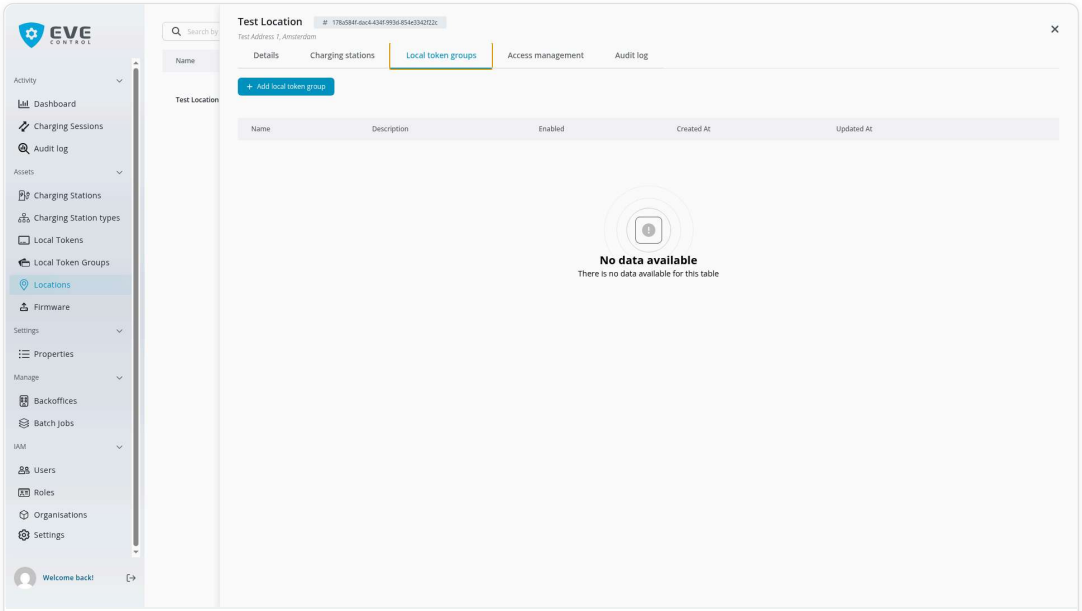
The token is now part of this group

8. Add a Token Group to a Location

Linking a token group to a location grants all tokens in that group permission to charge at every charging station assigned to that location. This is the final step to enable charging access.

1 ### Open the Location and go to Local Token Groups

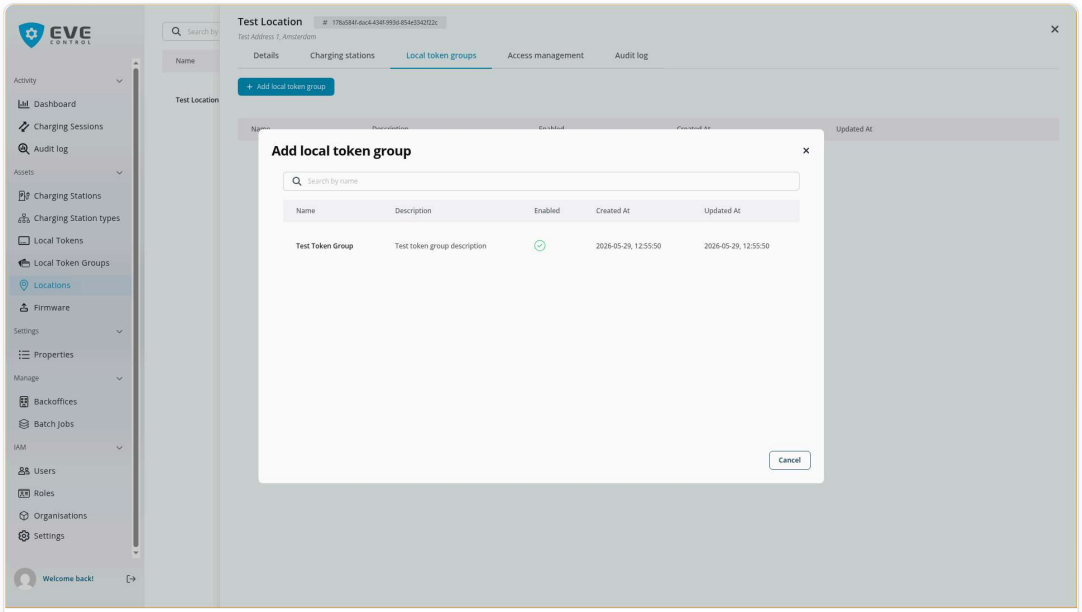
Navigate to **Locations**, click on the location, then select the **Local token groups** tab.



The Local token groups tab of a location (no groups linked yet)

2 ### Select a Token Group

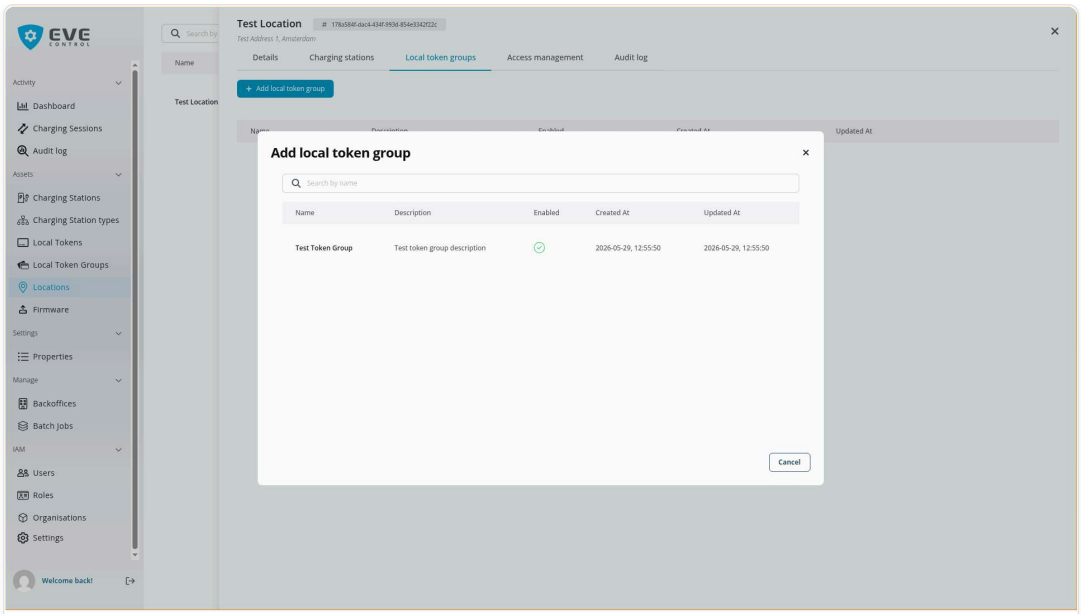
Click **Add local token group**. Select the group you want to link and confirm.



Selecting a token group to link to this location

3 ### Confirm

The token group now appears linked to the location. All tokens in this group can now charge at this location's charging stations.



The token group is now linked to this location

> **Access chain:** Token → Token Group → Location → Charging Station. A token can charge at a station if: (1) the token is in a group, (2) the group is linked to a location, and (3) the charger is assigned to that location.

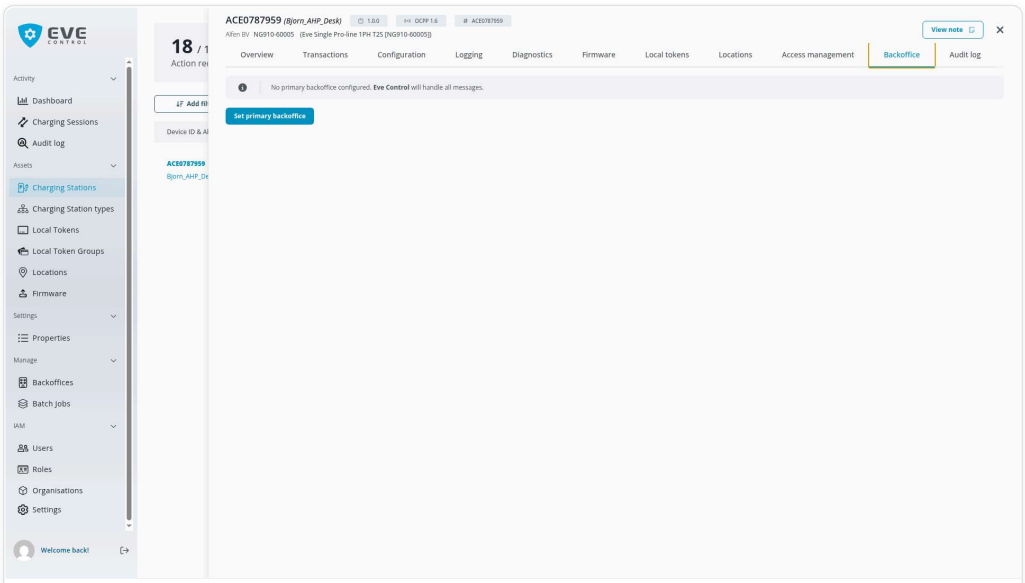
REWRITTEN

9. Connect a Primary Backoffice

Every charger you claim is automatically connected to Eve Control — that connection is not shown in the Backoffice tab and you cannot remove it. If you also want to forward the charger's OCPP traffic to a third-party Charge Point Management System (CPMS), you can connect **one additional backoffice**: the **primary backoffice**. The primary backoffice is responsible for authorising charge cards, handling transactions, and other CPMS operations, while Eve Control continues to provide visibility and management.

1 Open the Charger's Backoffice Tab

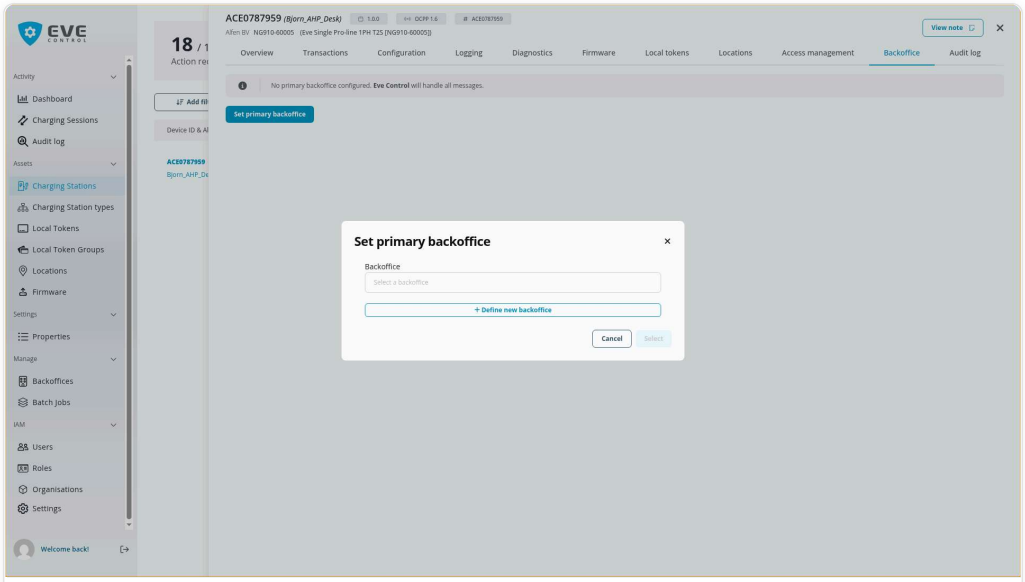
Navigate to **Charging Stations**, click on the charger, then select the **Backoffice** tab. If no primary backoffice has been set, the tab is empty.



The Backoffice tab when no primary backoffice has been set yet

2 Click "Set primary backoffice"

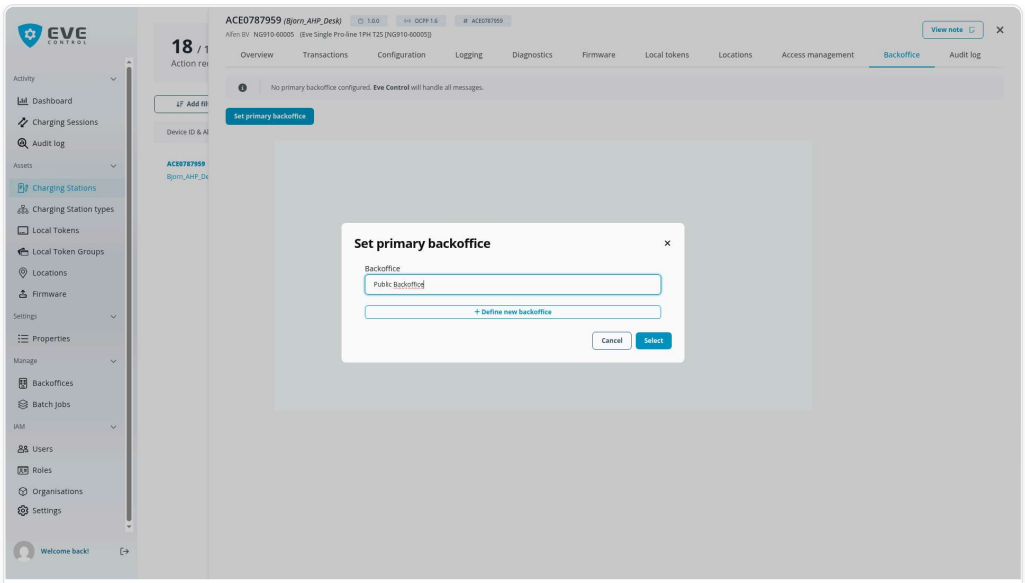
Click the **Set primary backoffice** button. A dialog opens with a dropdown showing every backoffice you have access to (your organisation's own private backoffices, and any public backoffices Alfen has published). The dropdown also contains a special entry **Define new backoffice...**.



The "Set primary backoffice" dialog

3a Option A — Pick an existing backoffice

Choose a backoffice from the dropdown (for example a public CPMS published by Alfen or one you previously created) and click **Select**. The charger will start forwarding traffic to that system.

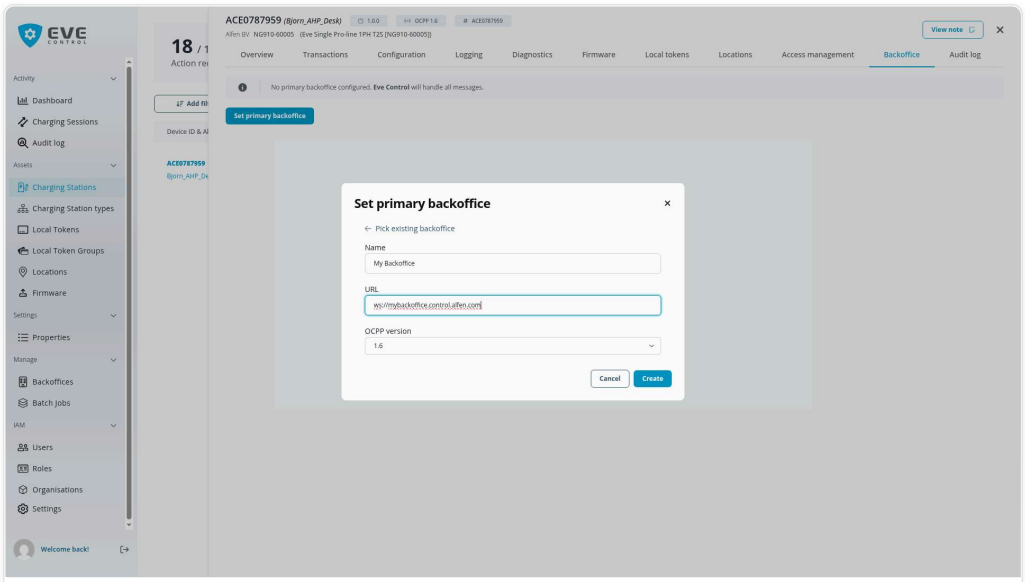


Selecting an existing backoffice from the dropdown

3b

Option B — Define a new backoffice (self-service)

If your CPMS is not in the dropdown, select **Define new backoffice…**. Fill in a **Name** and the **URL** of the new backoffice (for example `ws://your-cpms.example.com/` or the `wss://` equivalent for TLS), then click **Create**. The backoffice is added to your organisation's list *and* connected to this charger as the primary.



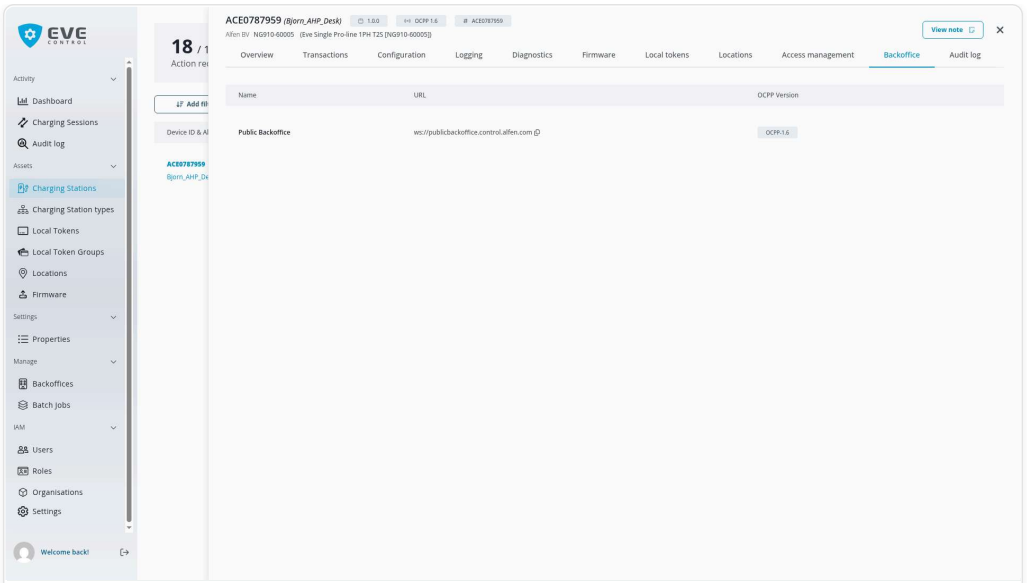
Self-service definition of a new private backoffice

Backoffices you create this way are *private to your organisation* and can be reused for other chargers you own.

4

Verify the Connection

The chosen backoffice now appears in the Backoffice tab. To swap it for a different one, remove the current entry (trash icon, confirm by typing `delete`) and repeat the steps above.



The chosen backoffice is now linked as primary

Only one primary at a time: A charger can be linked to at most one other backoffice. If you want to change to a different CPMS, remove the current primary first. Eve Control's own connection to the charger continues to work in parallel and is not affected.

REWRITTEN

10. Changing to Secure WebSocket Connectivity

By default, migrated chargers connect to Eve Control using an insecure WebSocket connection (`ws://`). To upgrade to a secure connection (`wss://`), you need to perform a security firmware update that installs the required TLS root certificate and updates the OCPP connection URL.

1 Verify the Charger is Online

Navigate to **Charging Stations** and confirm that the charger you want to update is online and connected to Eve Control.

2 Initiate the Security Firmware Update

Open the charger's detail page and navigate to the **Firmware** tab.

Make sure you select the security update that corresponds to your charger's platform and your type of connection. For example, for an NG9 charger connected by LAN cable, select **"NG9 Wired Security Update"** from the list.

Select the security update matching your charger's platform and connection type

Start the security firmware update. This update installs the root certificate required for TLS and reconfigures the charger's OCPP connection from `ws://ocpp.alfen.com/` to `wss://ocpp.alfen.com/`.

3 Wait for the Update to Complete

The charger will download and apply the security firmware update, then reboot automatically. After the reboot, it will reconnect to Eve Control using the secure `wss://` connection.

4 Verify the Secure Connection

Once the charger is back online, confirm that the connection is now using `wss://`. You can verify this in the charger's **Logging** tab or configuration details.

> **Why WSS?** Secure WebSocket (`wss://`) encrypts all communication between the charger and Eve Control using TLS, protecting against eavesdropping and tampering. This is the recommended configuration for production deployments.

REWRITTEN

11. Understanding the Data Model

Eve Control organises your charging infrastructure around a set of core entities. Understanding how they relate to each other is key to managing your setup effectively.

Core Entities

1. ### Organisation

   The top-level container. Every user, charger, location, token, and token group belongs to one or multiple organisations. Organisations are fully isolated from each other — you cannot see or manage another organisation's data unless access is explicitly granted on entity level.

2. ### Charging Station

   A physical Alfen EV charger connected to Eve Control via OCPP. Each charger is identified in Eve Control by its **OCPP Identifier** — the identifier with which the charger communicates to the backoffice. This is not necessarily the serial number, as the OCPP Identifier may have been changed after purchase. Chargers can be assigned to locations and have tokens linked to them for charging access.

3. ### Location

   A physical site (parking garage, office, housing complex) where one or more chargers are installed. Locations have a name, address, and other details. Token groups are linked to locations to grant access to all chargers at that site.

4. ### Local Token

   Represents a charge card (RFID tag). Each token has a Hidden ID (the chip UID), a Visual ID (printed on the card), and a description. Tokens can be valid or invalid, and blocked or unblocked.

5. ### Local Token Group

   A collection of tokens that share the same charging access. Instead of granting each token individual access, you place tokens in a group and link the group to locations. Token groups can be enabled or disabled.

How They Connect

Entities are linked through many-to-many relationships:

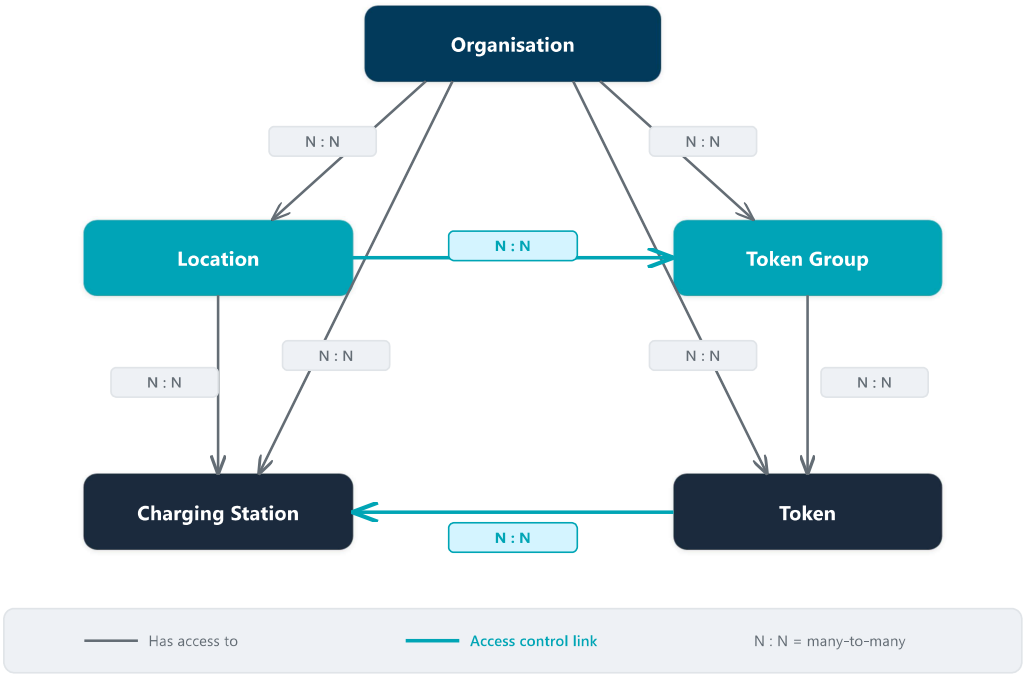
- A **charger** can be assigned to one or more **locations**
- A **location** can have multiple **chargers** and multiple **token groups**
- A **token group** can be linked to multiple **locations** and contain multiple **tokens**
- A **token** can belong to multiple **token groups** and have direct access to specific **chargers**

> **See the next section** for detailed entity relationship diagrams showing how these entities connect.

12. Entity Relationships

The diagram below shows how the five core entities relate to each other. The highlighted links are the key access control relationships.

Overview Diagram



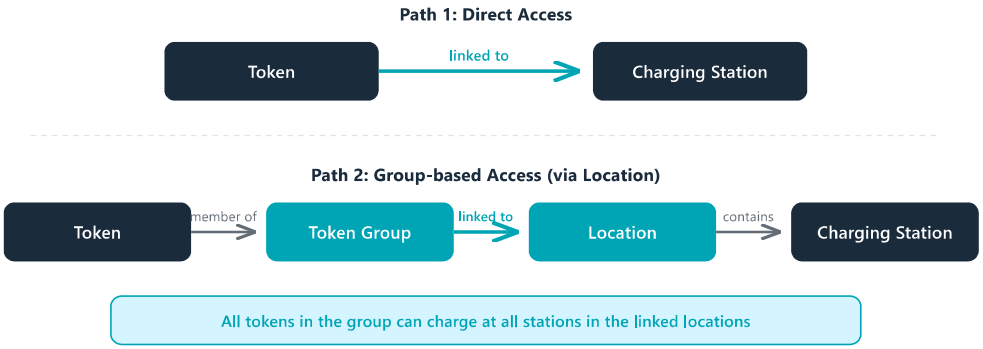
All Entity Relationships

Entity A	Relation	Entity B	Description
Organisation	N : N	Location	One or more organisations can have access to one or more locations.
Organisation	N : N	Charging Station	One or more organisations can have access to one or more charging stations.
Organisation	N : N	Token Group	One or more organisations can have access to one or more token groups.
Organisation	N : N	Token	One or more organisations can have access to one or more tokens.
Location	N : N	Charging Station	A location groups one or more charging stations by physical site. A charging station can belong to multiple locations.
Location	N : N	Token Group	A token group can be linked to one or more locations. All tokens in the group gain access to all charging stations at those locations. This is the primary mechanism for group-based access control.
Token Group	N : N	Token	A token group contains one or more tokens. A token can belong to multiple groups. The token's effective access is the union of all locations linked to all its groups.
Token	N : N	Charging Station	A token can be directly linked to one or more charging stations. This is the direct access mechanism (as opposed to group-based access via token groups and locations).

> **Note:** Token Groups cannot be linked directly to Charging Stations. To grant a group of tokens access to chargers, link the Token Group to a Location that contains those chargers.

Access Control: Two Paths

A token can gain access to a charging station through two distinct paths:



13. Access Control

There are two ways a charge card (token) can be authorised to start a session at a charger. You can use either or both methods.

Path 1: Direct Access

A token is added directly to a charger's local token list. This is the simplest approach and works well for a small number of chargers and tokens.

> **Direct access chain:** Token → Charging Station

You can set this up from either direction:

- From the **charger**: Open the charger, go to *Local tokens* tab, and add tokens
- From the **token**: Open the token, go to *Charging stations* tab, and add chargers

Path 2: Location-Based Access (via Token Groups)

Tokens are placed in a group, and the group is linked to a location that contains chargers. This is the scalable approach — ideal when managing many tokens and chargers.

> **Location-based access chain:** Token → Token Group → Location → Charging Station
>
> A token can charge at a station if: (1) the token is in a group, (2) the group is linked to a location, and (3) the charger is assigned to that location.

You can manage these links from either direction:

- Link token groups to locations from the **location** page (*Local token groups* tab) or from the **token group** page (*Locations* tab)
- Add tokens to groups from the **token group** page (*Local tokens* tab)
- Add chargers to locations from the **location** page (*Charging stations* tab) or from the **charger** page (*Locations* tab)

All Conditions for Charging

For a charge card to successfully start a charging session, **all** of the following must be true:

1. The card is registered as a **Local Token** in Eve Control
2. The token is **valid** (not invalidated)
3. The token is **not blocked**
4. The token has **access to the charger** via either direct access or a token group
5. If using a token group: the group must be **enabled**

14. Charger Operations

Each charging station has a detail page with multiple tabs for different operations. Here is an overview of what you can do from each tab.

Overview Tab

The default tab shows general charger information and provides quick actions:

- **Reboot —** sends a remote reset command to the charger. Verify in the Logging tab.
- **Unlock Connector —** remotely unlocks the charger's connector (e.g. to release a stuck cable). Look for "Unlocked" in the Logging tab.
- **Remote Start Transaction —** starts a charging session for a specific token. Enter the token UID, click Start.
- **Remote Stop Transaction —** stops an active charging session.

Backoffice Tab UPDATED

Manage the charger's primary backoffice connection. Eve Control is always connected and is no longer shown here. A charger can have at most one additional backoffice (the primary) which handles authorisation and transactions. See section 9: Connect a Primary Backoffice for the full step-by-step instructions, including the self-service flow for adding a new private backoffice.

Configuration Tab

View and modify the charger's OCPP configuration parameters (key-value pairs):

- **Filter —** use the search field to find a parameter by name
- **Edit —** click the edit icon next to a parameter to change its value, then click Save
- **Add variable —** create a new configuration parameter

> **Key parameters:**
>
> - `AuthorizeRemoteTxRequests` — when True, remote start transactions require token authorisation; when False, remote starts are accepted without checking the token
> - `AuthorizationCacheEnabled` — enables or disables the local authorisation cache on the charger

Logging Tab

A real-time log of all OCPP messages between the charger and Eve Control. This is your primary tool for verifying that operations have succeeded. Each row shows the message type, direction (Request/Response), and result.

Security Tab

Controls which token authorisation profiles are active on the charger. Profiles can be dragged between the "Active" and "Available" lists:

- **local-token-group —** enables location-based access via token groups. If this profile is removed from the active list, tokens with group-based access can no longer charge at this charger.

Diagnostics Tab

Request diagnostic data from the charger:

1. Select a date range using the calendar picker
2. Click **Send request**
3. Wait for the charger to process and upload the data (this may take 20 seconds or more)
4. Check the **Logging** tab for a `DiagnosticsStatusNotification` with status `Uploaded`

Firmware Tab

Update the charger's firmware:

1. Click **Select** to open the firmware selection dialog
2. Choose a firmware version from the list (only versions your organisation has been granted access to are shown)
3. Click **Update** to initiate the firmware update

4. Check the Logging tab for firmware status notifications (e.g. `Downloading`, `Installed`)

Local Tokens Tab

Manage which tokens have direct access to this charger. You can add tokens individually or remove them. This is the "direct access" method described in section 12.

Locations Tab

View and manage which locations this charger is assigned to. You can add the charger to a location or remove it.

15. Token & Group Lifecycle

Tokens and token groups have states that control whether they can authorise charging. Managing these states is how you control access over time.

Token States

Each token has two independent state flags:

State	Default	Actions	Effect When Negative
Valid	Yes (on creation)	Validate / Invalidate	Token cannot charge anywhere
Blocked	No (on creation)	Block / Unblock	Token cannot charge anywhere

To manage these states: navigate to **Local tokens**, click on the token to open its detail panel, and use the corresponding buttons.

> **Tip:** Both Valid and Not Blocked are required for a token to work. Invalidating is typically used when a card is permanently deactivated, while blocking is a temporary measure (e.g. a lost card that might be found again).

Token Group States

State	Default	Actions	Effect When Disabled
Enabled	Yes (on creation)	Enable / Disable token group	All tokens in this group lose their location-based access through this group

Disabling a group is a quick way to revoke access for an entire set of tokens without deleting or modifying individual tokens. Re-enabling the group restores access instantly.

Deleting Tokens and Groups

- **Deleting a token —** permanently removes the token. It can no longer authorise charging anywhere. Requires typing "delete" to confirm.
- **Deleting a token group —** permanently removes the group. All tokens that were in the group lose the location-based access the group provided. The tokens themselves are not deleted and any direct charger access they have is unaffected.

16. Revoking Charging Access

There are many ways to revoke a token's ability to charge, each with a different scope and impact.

Action	Scope	Reversible?
Invalidate token	Single token — cannot charge anywhere	Yes (Validate)
Block token	Single token — cannot charge anywhere	Yes (Unblock)
Disable token group	All tokens in the group — lose group-based access	Yes (Enable)
Remove token from group	Single token — loses this group's access	Yes (re-add)
Unlink group from location	All tokens in group — lose access to that location's chargers	Yes (re-link)
Remove charger from location	All group-based access to that charger through the location	Yes (re-add)
Remove token from charger	Single token — loses direct access to that charger	Yes (re-add)
Delete token group	All tokens in group — lose all group-based access	No (permanent)
Delete token	Token is permanently removed	No (permanent)

> **Recommendation:** Use *blocking* for temporary suspensions and *invalidating* or *deleting* for permanent deactivation. Use *disabling a group* to quickly suspend access for an entire set of users.

17. Organisation Isolation

Eve Control enforces strict data isolation between organisations. Each organisation operates as an independent tenant.

1 ### What You Can See

As an organisation user, you can only see and manage entities that belong to your own organisation: your chargers, locations, tokens, token groups, and fellow organisation users.

2 ### What You Cannot See

You cannot view tokens, token groups, locations, or chargers from other organisations. Navigating to the **Organisations** page as a regular user will show a "Not allowed" message.

3 ### User Access Requirements UPDATED

A user must meet two conditions to use Eve Control:

- Be placed in an **organisation** (users not in any organisation see "Not allowed")
- Have at least one **role** in that organisation. Users in an organisation but without a role are redirected to the **Request Access** page where they can ask the organisation admin for a role — see section 20. They are not blocked with a "Not allowed" page.

18. Finding the Hidden ID of a Charge Card

The **Hidden ID** (also called UID or token ID) is the internal identifier stored on a charge card's RFID chip. It is required when creating a Local Token in Eve Control. Unlike the Visual ID printed on the card, the Hidden ID is not directly visible. Below are several methods to find it.

Option A: Swipe the Card on a Charging Station and Read the Logs

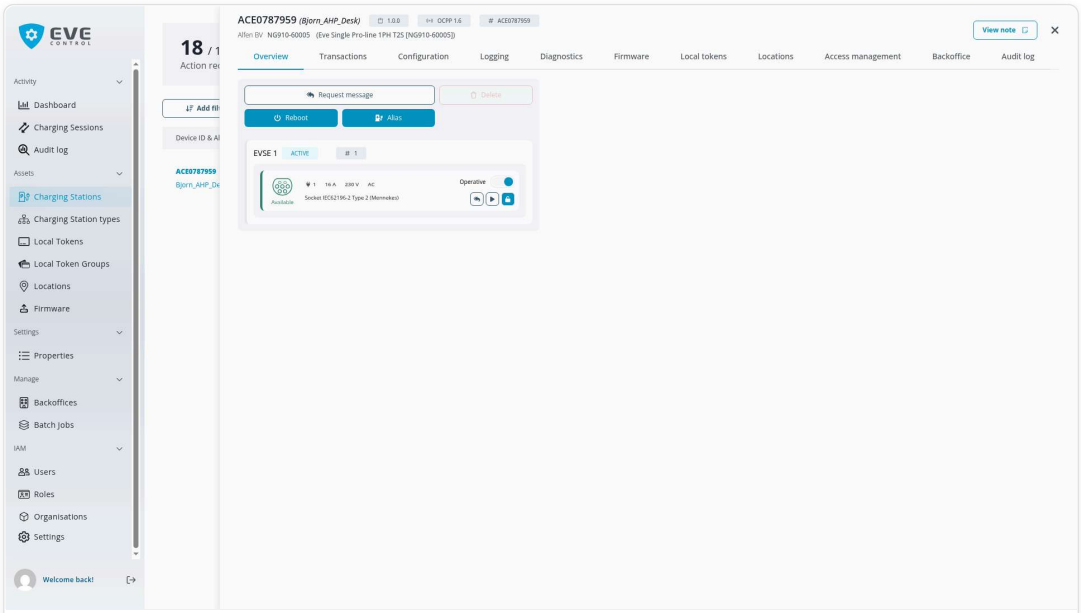
This is the most convenient method if the charger is already connected to Eve Control. The charger sends an `Authorize` request containing the card's Hidden ID whenever a card is swiped — even if the card is not yet registered.

1 Swipe the RFID Card

Go to the charging station and swipe (or hold) the RFID card on the card reader. The charger will send an `Authorize` request to Eve Control. It does not matter whether the authorization succeeds or fails — the card's identifier is included in the request either way.

2 Open the Charging Station in Eve Control

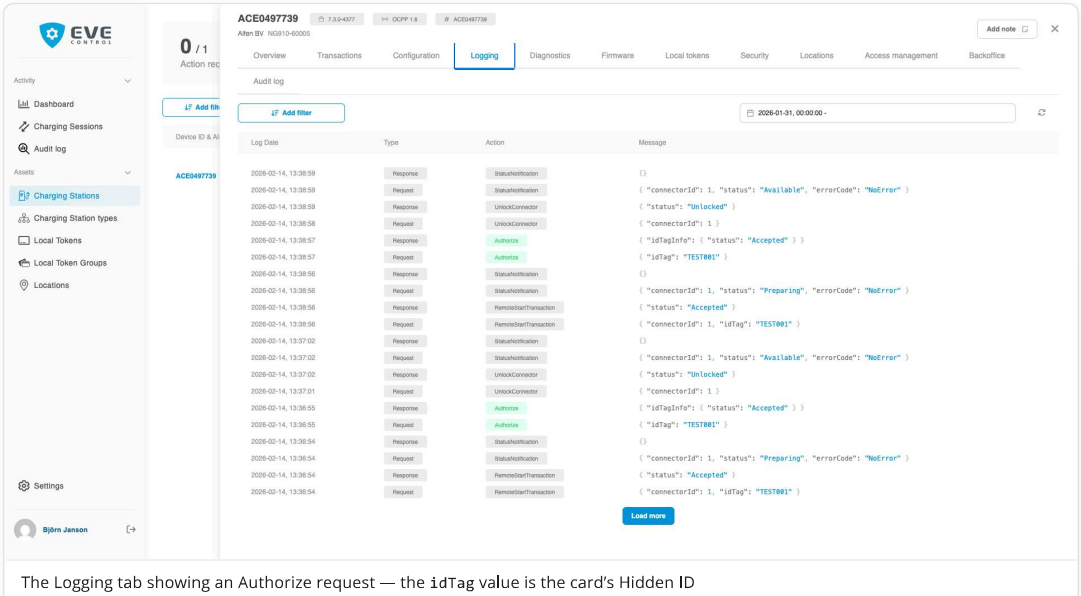
Navigate to **Charging Stations** in the sidebar and click on the charger where you swiped the card.



The charging station's Overview page

3 Go to the Logging Tab and Find the idTag

Click the **Logging** tab. Look for an `Authorize` request in the log entries. The `idTag` field in this message is the card's **Hidden ID**. Copy this value and use it when creating the Local Token.



The Logging tab showing an Authorize request — the `idTag` value is the card's Hidden ID

> **Tip:** The authorization result will show "Invalid" if the card is not yet registered — this is expected. The `idTag` value is still visible in the request regardless of the authorization result.

Option B: Check the Card's Packaging or Documentation

Some charge card suppliers print the UID on the card's packaging, on an accompanying sticker, or in the delivery documentation. Check any materials that came with the card.

Option C: Use a USB NFC/RFID Reader

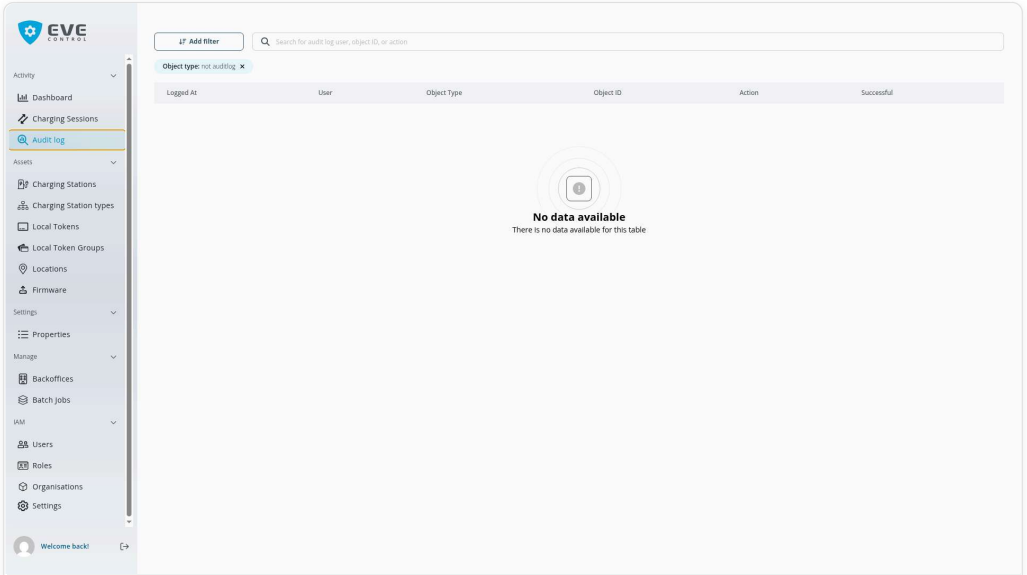
A dedicated and compatible USB NFC/RFID reader (e.g. an ACR122U) connected to a computer can read the card's UID. This is useful when registering many cards in bulk, as the UID is typically output as text that can be copied directly.

NEW 19. Audit Logs

The **Audit Logs** page records who did what inside your organisation. Use it to investigate when a token was blocked, when a charger was assigned to a location, when a role was changed, and many other administrative events. Audit logs are scoped to your organisation — you cannot see events from other organisations.

1 Open the Audit Logs page

Click **Audit Logs** in the left sidebar. The page shows a chronological table of recent events with columns for timestamp, actor, object type, object, and action.



The Audit Logs page

2 Filter the log

Use the **search field** at the top of the page to filter by free text — for example a charger ID (`SIMCHARGER`), a location name, or a token UID. You can also use the object-type filter to narrow down to a single category (chargers, locations, tokens, users, roles, etc.).

3 Open an event for details

Click any row in the table to open a detail panel on the right showing the full event payload — before/after values, the actor, the IP address, and the API endpoint that recorded the event. This is useful for confirming exactly what was changed.

> **What is audited?** CRUD on chargers, locations, tokens, token groups, users, roles, and organisations; access-grant changes; role assignment; and most other management operations. Charging session start/stop events are *not* audit log entries — those are visible in the Charging Sessions page.

REWRITTEN

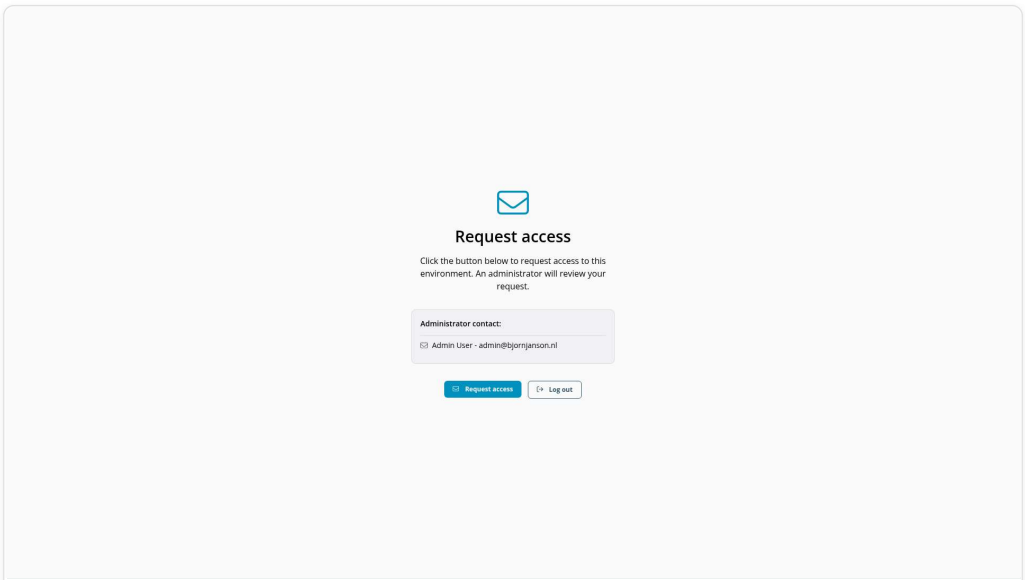
20. Request Access Flow

When a user belongs to an organisation but has not been given a role yet, they cannot use the application. Instead, after they log in they land on a dedicated **Request Access** page. This is the flow for new users joining an organisation that already exists in Eve Control.

For the requesting user

1 Log in for the first time

After you sign up, if your organisation already exists in Eve Control you will be redirected to `/request-access` automatically when you log in. Trying to navigate to other pages (Locations, Charging Stations, Dashboard) will send you back here until you have a role.



The Request Access page that pending users see after login

2 Submit an access request

The page shows the name of your organisation and a button to submit an access request. After clicking it, the page updates to show that a request is pending. Wait for your organisation admin to review it.

For the organisation admin

1 See pending requests

Pending requests appear in the **Users** page of your organisation. Users awaiting a role are highlighted; you can also see them on the organisation's user list.

2 Approve by assigning a role

Open the user and edit their roles — assign at least one organisation role (e.g. **Organisation User**, **Organisation Technician**, or **Organisation Admin**). The next time the user logs in they will land on the dashboard instead of the Request Access page.

3 Deny by removing the user

If you do not want to grant access, remove the user from the organisation. The user can no longer log in to the organisation and can be re-added later if needed.

NEW 21. Organisation Onboarding

All existing Alfen customers and contacts have been synchronised to Eve Control and are in an **onboarding state**. No admin has been designated yet. Any user in the organisation who logs in is guided through a flow to collectively elect the organisation admin(s). This ensures that the organisation itself decides who takes administrative control.

1 **Log in during onboarding state**

When a user from an organisation in onboarding state logs in, they are redirected to a dedicated screen rather than the dashboard. The screen explains the situation and invites the user to nominate one or more organisation admins.

2 **Select the organisation admin(s)**

The user selects one or more colleagues from the list of users in the organisation to become the Organisation Admin(s). The selection is submitted, and the chosen users are immediately granted the Organisation Admin role.

3 **All users in the organisation are notified**

After the admin selection is submitted, **every user in the organisation** receives a notification informing them of the decision — who was chosen as admin and by whom. Each user has the option to **revoke** the selection if they believe it was made in error. Once the onboarding state is resolved, all users land on the dashboard on their next login.

> **Note:** All existing Alfen customers and contacts have been synchronised to Eve Control and placed in onboarding state automatically. If your organisation is stuck in onboarding state or you have not received a notification you expected, contact Alfen support.

NEW 22. Users & Roles

Permissions in Eve Control are granted through **roles**. A role is a named bundle of permissions; a user gets capabilities by being assigned roles within your organisation. Eve Control ships with three built-in organisation roles, which cover the needs of most setups.

The built-in roles

- **Organisation Admin —** full access inside the organisation: manages users, approves access requests, claims chargers, and manages locations, tokens, token groups, and primary backoffices.
- **Organisation Technician —** operational access: onboards chargers, edits configuration, requests diagnostics, runs firmware updates.
- **Organisation User —** read access for everyday users: sees chargers, locations, and charging sessions.

Assign or change a user's roles

As an Organisation Admin, open the **Users** page in the sidebar to see the users in your organisation. Open a user's detail page, click the edit icon next to the role section, pick one or more roles from the multiselect, and submit. This is also how you approve a pending access request (see section 20): assigning a role moves the user from the Request Access page to the dashboard on their next login.

NEW 23. Self-Registration

New users can sign up to Eve Control on their own through the Azure AD B2C login page. What happens after sign-up depends on whether your organisation already exists in Eve Control.

1 Sign up

On the Eve Control login screen, click **Sign up**. Provide an email address and create a password. Azure AD B2C handles verification (email confirmation) and password policy.

2 Create your organisation and start using

If your organisation does not exist in Eve Control yet, you create it as part of onboarding and become its first Organisation Admin. You can start using Eve Control straight away — claim chargers, create locations, manage tokens, and invite colleagues.

3 If your organisation already exists

If an organisation matching your details already exists and it **has an Organisation Admin**, you will see a **Request Access** button. Clicking it sends an access request to that admin, who can approve it by assigning you a role (see section 20). On your next login after approval, you land on the dashboard.

If the organisation already exists but **does not have an Organisation Admin** yet, you will instead see a message asking you to **contact Alfen support** so access can be set up for you.

> **Password reset:** The Azure AD B2C login page offers a self-service password reset link. This does not affect the user's organisation or role — only their authentication credentials.

NEW 24. Charging Sessions

The **Charging Sessions** page (sidebar) shows ongoing and historical charging sessions across all chargers you have access to. Use it to investigate energy delivered, session duration, idTag (token) used, and connector status. The page is read-only — to stop an ongoing session, go to the charger's Overview tab and use the Remote Stop Transaction button.

Key columns

- **Started / Stopped timestamps** — when the session began and ended (empty if still ongoing).
- **Charging station** — the ID of the charger.
- **Connector** — the socket number used on multi-socket chargers.
- **idTag** — the token (Hidden ID) that authorised the session.
- **Energy delivered (kWh)** — how much energy was transferred.

Download transactions

Click **Download** to export sessions to a file. The dialog offers presets (e.g. *Last month*) or a custom date range. The export includes session metadata and meter values and is suitable for billing reconciliation.

Sessions vs Transactions

A *session* is the user-facing "plug-in to unplug" experience. A *transaction* is the OCPP `StartTransaction`…`StopTransaction` pair inside it. A single session can contain multiple transactions if the charger restarted or briefly lost connection. The Charging Sessions page collapses transactions into sessions by default.

NEW 25. Firmware Management

Eve Control can push firmware updates to chargers over OCPP. When a firmware version is available to your organisation, you can apply it to individual chargers from the charger's **Firmware** tab.

Apply firmware to a charger

- Open the target charger and switch to the **Firmware** tab.
- Click **Select** to choose from the firmwares available to your organisation.
- Click **Update**. The charger downloads the firmware, applies it, and reboots.
- Watch the **Logging** tab for `FirmwareStatusNotification` messages (`Downloading`, `Downloaded`, `Installing`, `Installed`).

> **Security firmware update:** For chargers that were migrated remotely via OCPP (Option B in section 1), the security firmware update is what switches the OCPP connection from `ws://` to `wss://`. See section 10.

NEW 26. Cross-Organisation Access

By default, every entity (charger, location, token, token group) belongs to one organisation and is invisible to others. When two organisations need to collaborate — for example a fleet operator that manages chargers installed at a customer site — the owning organisation can **grant access** to specific entities. This section explains how cross-org access works.

Grant access to another organisation

The owning organisation grants *shared* access. Open the entity, switch to the **Access management** tab, click **Grant Access**, search for the other organisation, and confirm. The other organisation can now see and operate on the entity. To remove access, use the trash icon next to the granted organisation.

> **Granting access to a location shares its chargers too:** When you grant another organisation access to a **location**, that organisation automatically also gains access to all chargers placed at that location. You do not need to share each charger individually.

What is shared

Sharing is per entity. **Chargers, locations, tokens, and token groups can all be shared** with another organisation. If you grant access to a single charger, the other organisation sees only that charger — not your other chargers, locations, or tokens unless those are also explicitly shared. The exception is locations: sharing a location also shares every charger placed at it. Granting access always keeps the original owner — the other organisation gets shared visibility, not ownership.

REWRITTEN

Questions & Answers

Common questions about Eve Control concepts and operations.

- Q What is a Location? ▸
- Q What is a Local Token? ▸
- Q What is a Local Token Group? ▸
- Q How do I make sure a charge card can charge? ▸
- Q What is a Backoffice connection? UPDATED ▸
- Q What does “primary backoffice” mean? NEW ▸
- Q Can I add my own backoffice if it’s not in the list? NEW ▸
- Q How do I remove a charging station from a location? ▸
- Q How do I block or unblock a token? ▸
- Q How do I validate or invalidate a token? ▸
- Q How do I enable or disable a token group? ▸
- Q What happens if I delete a token group? ▸
- Q Can one token be in multiple token groups? ▸
- Q Can one token group be linked to multiple locations? ▸
- Q How do I check if a token has charging access? ▸
- Q What is OCPP? ▸
- Q How do I view charger logs? ▸
- Q What is the difference between WS and WSS? ▸
- Q Why do remotely migrated chargers initially connect via WS instead of WSS? ▸

- How do I switch a charger from WS to WSS?
- Do chargers connected via local installation tooling also need a security firmware update?
- What is the difference between direct access and location-based access?
- What happens to a user without an organisation or roles? UPDATED
- How do I unlock a charger's connector remotely?
- How do I change an OCPP configuration parameter on a charger?
- How do I download diagnostics from a charger?
- What are the available user roles? UPDATED
- What does the Security tab on a charger do?
- How do I find the Hidden ID of an RFID charge card?
- How do I add a brand-new charger that does not exist in the platform yet? NEW
- Can I connect a charger to more than one third-party backoffice? NEW
- Where do I see who changed what? NEW

Roadmap & Versions

Eve Control is continuously evolving. Below is the planned feature roadmap across upcoming versions. Functionalities are released continuously and independently of the version milestones to deliver value as fast as possible.

Version 1 **Remote Serviceability** Live

Remote (self-service) serviceability — Full asset management platform

- Connect to the platform via OCPP
- Connect primary backoffice to the charger via Eve Control
- Basic access management without automated financial settlement of transactions
- Export transactions
- Optional Connectivity as a Service via Alfen SIM card
- Temporary remote connectivity for service cases
- (Multi) Firmware update

Version 2 **Improved Flows**

Simplifying onboarding, service and configuration flows

- Remote Diagnostics viewer for troubleshooting & validation
- SCN management (Monitoring, configuring)
- Streamlined asset management transfer
- Remote Load Balancing configuration
- Improved action-based dashboarding
- Chatbot integration
- Improved bulk commands and actions
- Simplified logo upload
- Onboarding flow from account creation to charger live
- Configure charging profiles

Version 3 **Decrease Installation Time**

Decreasing installation time while increasing first time right

- Prepare Installations, one-click local roll-out with Eve Install
- Simplified token onboarding when Eve Control is primary backoffice
- Centralized configuration management
- Easy charger license overview and purchasing

Version 4 **Advanced Service**

- AI based troubleshooting, auto provide solution steps based on charger diagnostics

Version 5 **One Digital Ecosystem**

Seamless integration with Eve Install

Account based charger access configuring who has local charger access

Collect Site Acceptance Test reporting

Temporary service connectivity via Eve Install

Store Eve Install configuration recovery points

Seamless Eve Control onboarding on Eve Install

Version 6 **Smart Energy Services**

3rd party smart charging (OCPP or OCPI)

SCN prioritized load balancing

Price-optimized charging

Note: Functionalities will be released continuously and independently of above-mentioned versions to add value as fast as possible.

Disclaimer: This roadmap is an indication of planned development direction. Based on customer feedback and changing priorities, the scope and order of features may change. We cannot guarantee that all listed functionality will be delivered as described.