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**.

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

2 Check Firmware (NG9 Chargers Only)

If the charger is an **NG9 model**, first perform a firmware update to a version that contains the required root certificate for connecting to Eve Control. Without this certificate, the charger cannot establish a secure connection.

3 Select the Eve Control Preset and Reboot

In the installation tool, select the **Eve Control** preset. This automatically configures the charger's OCPP settings to point to the Eve Control server. Then **reboot** the charger to apply the new configuration.

> **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)

If you want to migrate a charger that is already connected to another backoffice, you can configure it remotely via OCPP. **For now, only do this for chargers that you can easily access and connect to with the Service Installer**, in case you need to troubleshoot.

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 Eve

```
ocppVersion{OCPP16}ocppCsmsUrl{ws://ocpp.alfen.com/}messageTimeout{15}securityProfile{0}ocppInterface{Wireless0}apn{YOURSIMAP
```

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.

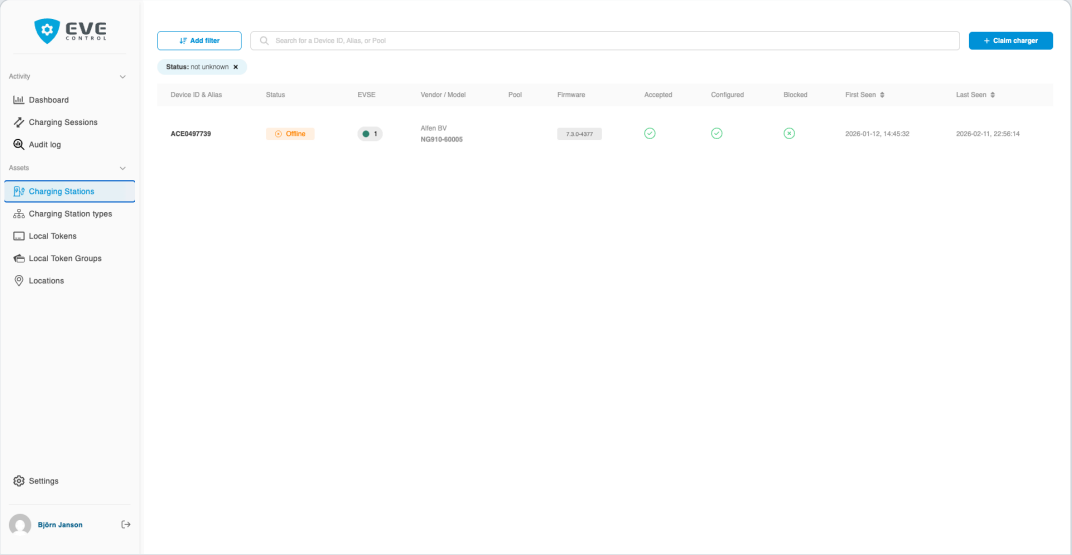
> **Important:** After the charger connects to Eve Control, you can optionally reconnect it to your existing backoffice *through* Eve Control using the **Backoffice** tab on the charger page (see section 9: Backoffice Forwarding). This way Eve Control acts as an intermediary, and you retain visibility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

2. Claim a Charging Station

Before you can manage a charger in Eve Control, you need to claim it using the charger's serial number and default charger password. These can be found on the label inside the charger or in the delivery documentation.

1 Navigate to Charging Stations

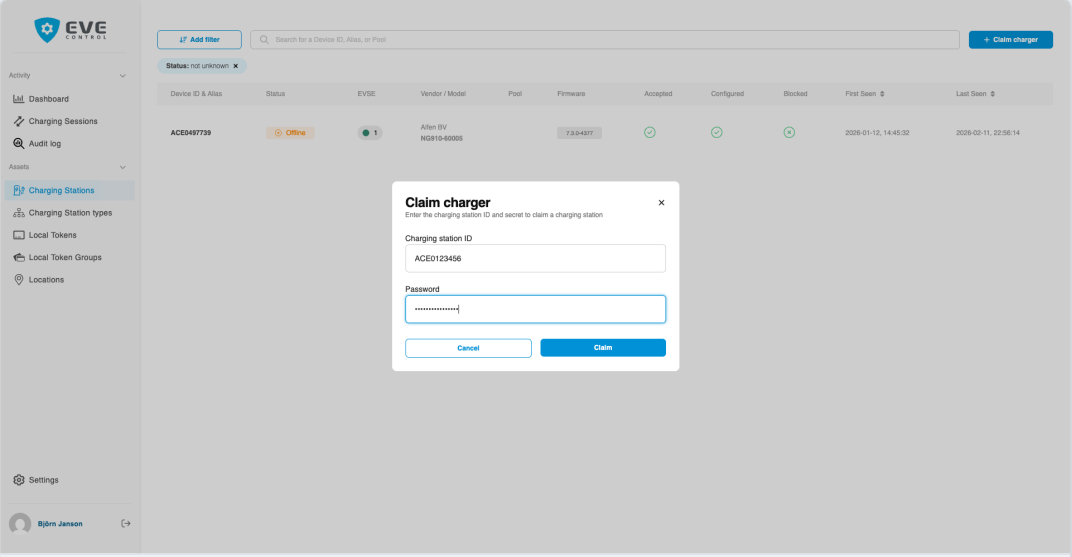
Click **Charging Stations** in the left sidebar to open the charging stations overview page.



The Charging Stations overview page

2 Open the Claim Dialog

Click the **Claim Charging Station** button. Enter the charger's **serial number** (e.g. ACE0123456) and the **default charger password** from the charger password flyer, then click **Claim**.



The claim dialog with serial number and password fields

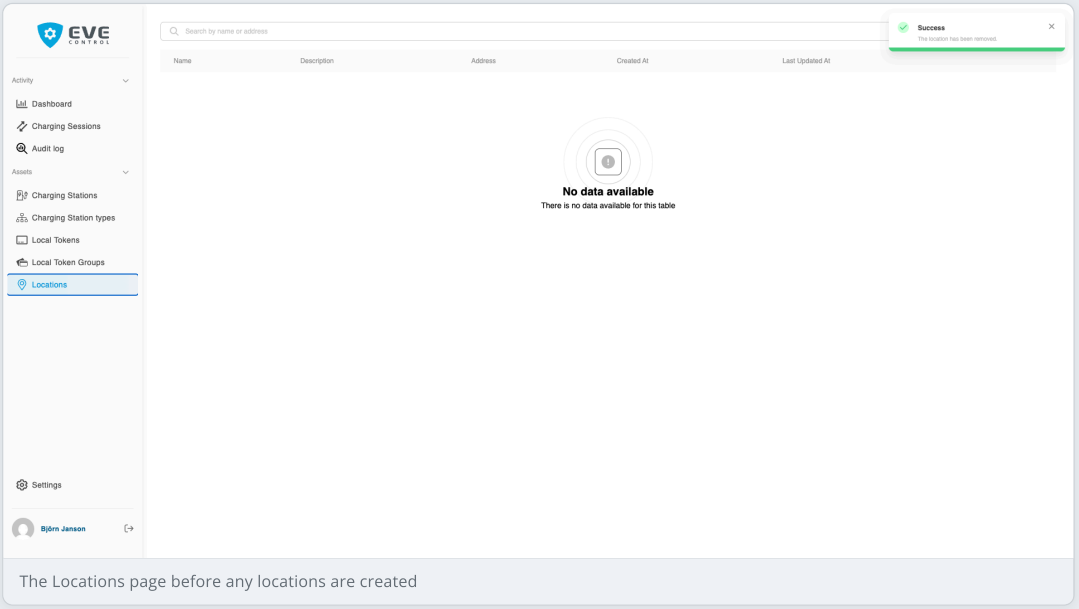
> **Tip:** The serial number starts with "ACE" followed by digits. The default charger password is printed on the charger label or included in the delivery paperwork. After claiming, the charger will appear in your Charging Stations list.

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

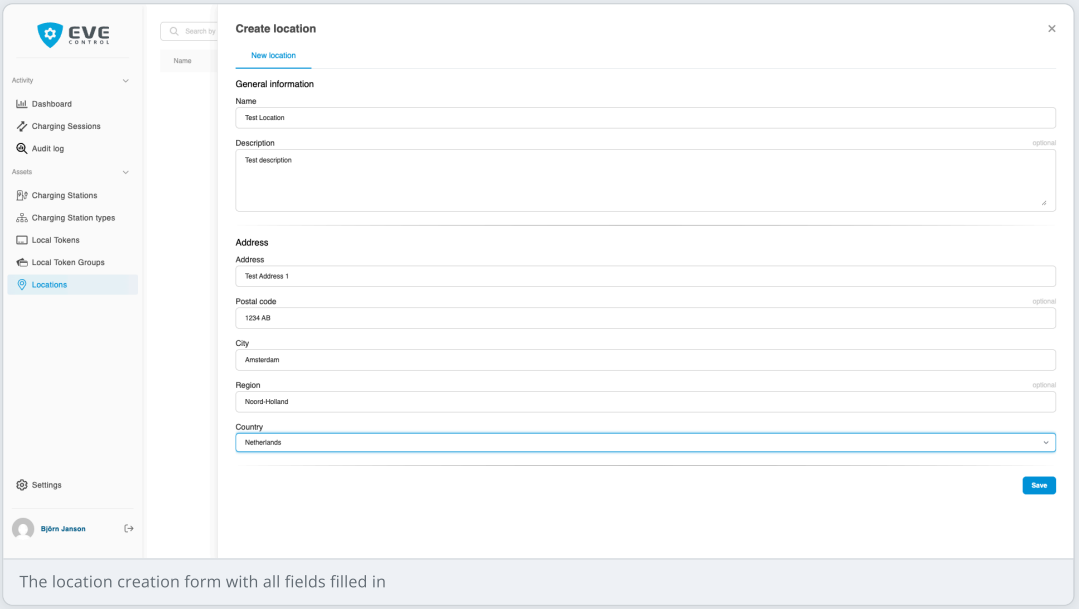
Click **Locations** in the left sidebar.



The Locations page before any locations are created

2 Fill in the Location Details

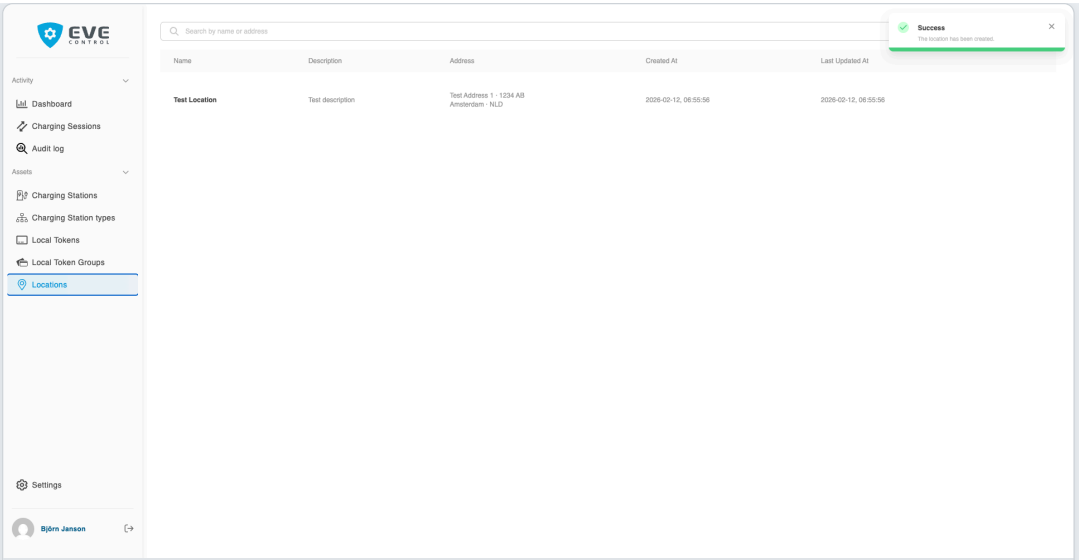
Click the **Create** button and fill in the location form: name, description, address, postal code, city, region, and country. Then click **Save**.



The location creation form with all fields filled in

3 Verify the Location

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



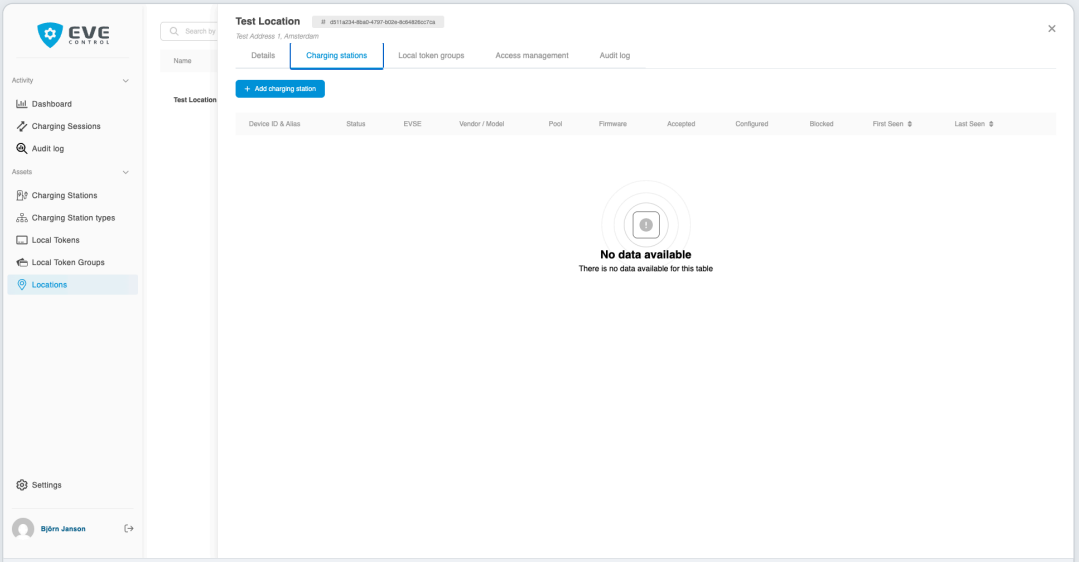
The new location now appears in the list

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

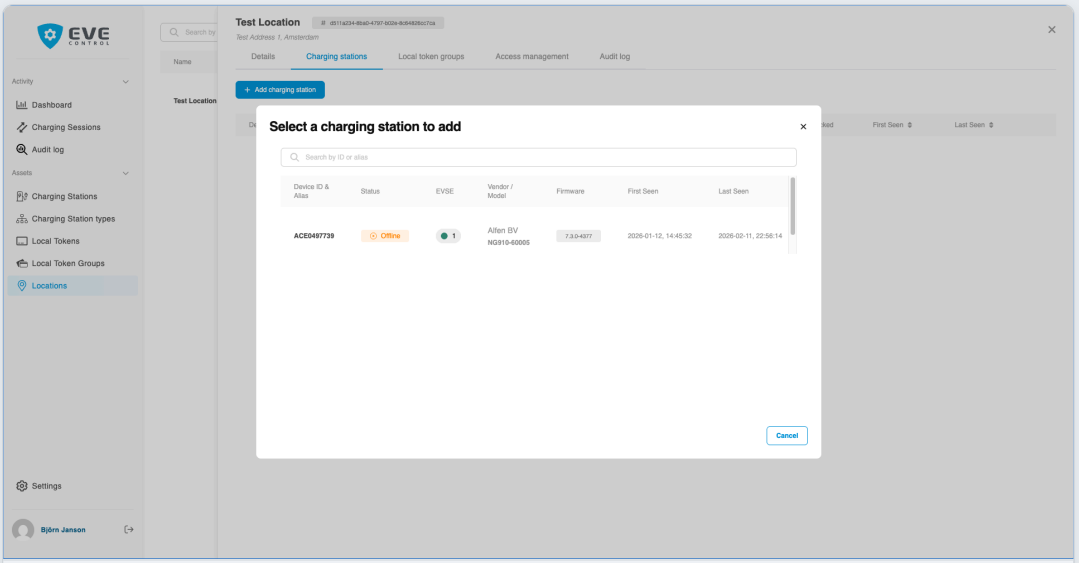
Navigate to **Locations**, click on the location you want, then select the **Charging stations** tab.



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

2 Select a Charger

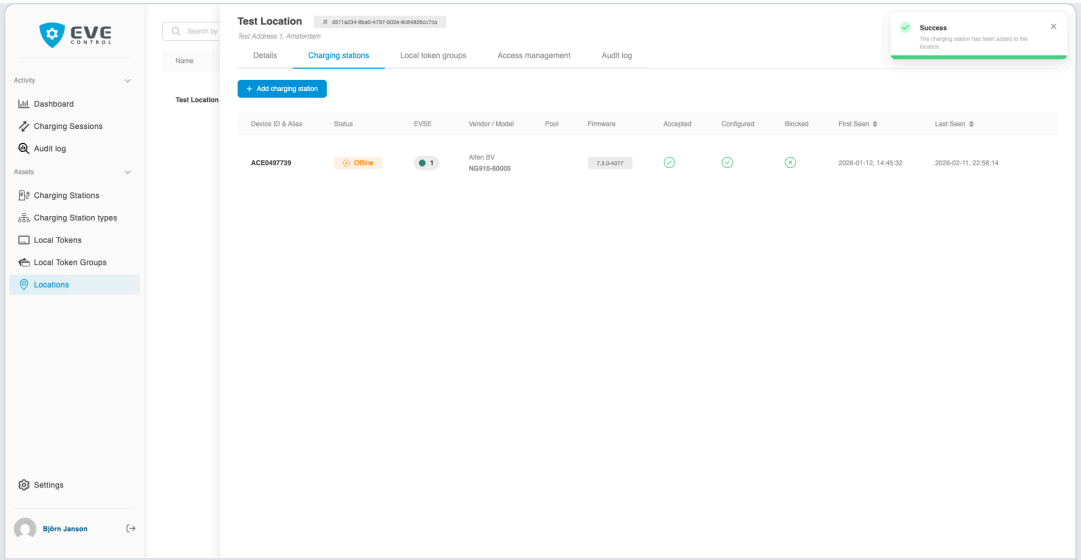
Click **Add charging station**. A list of available (unassigned) chargers appears. Click on the charger you want to add.



Selecting a charger to add to this location

3 Confirm

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



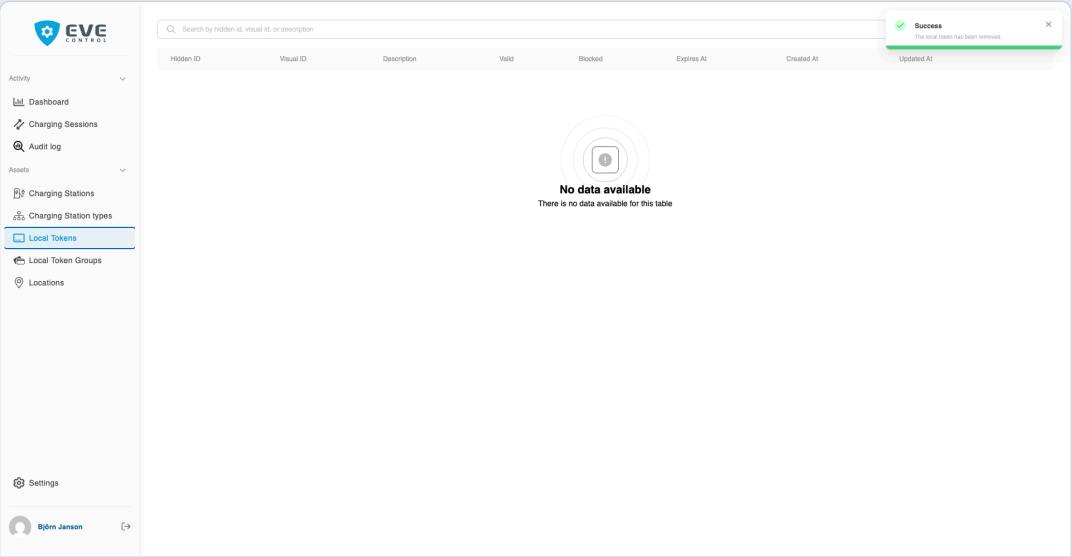
The charger is now assigned to this location

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.



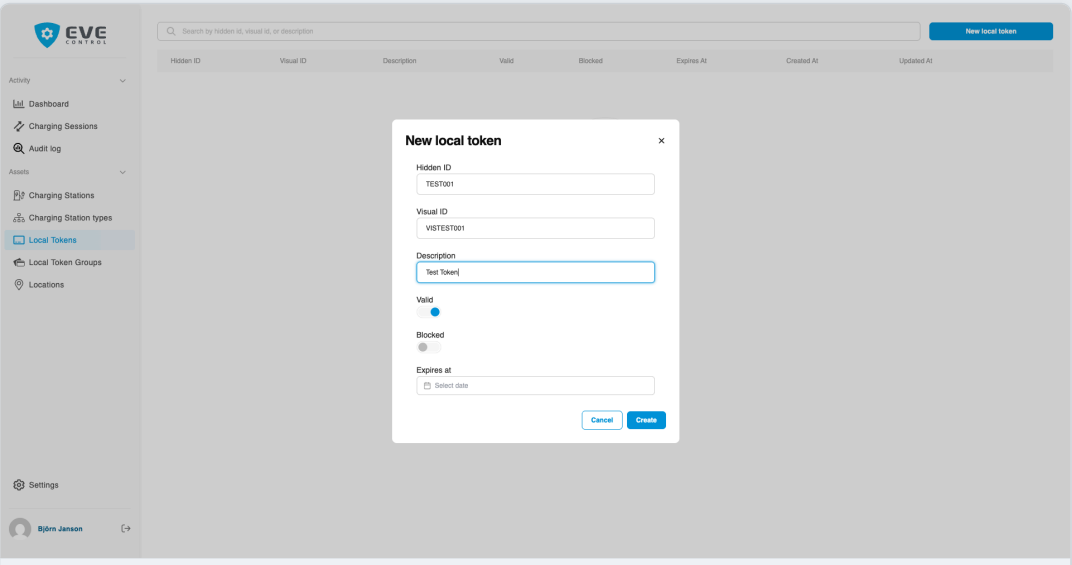
The Local Tokens page

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)

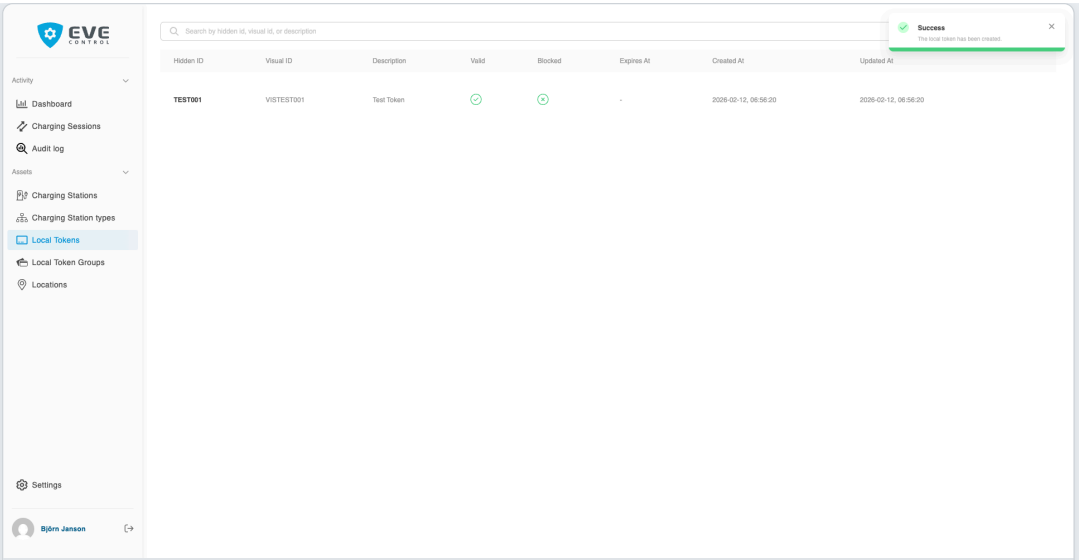
Then click **Create**.



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

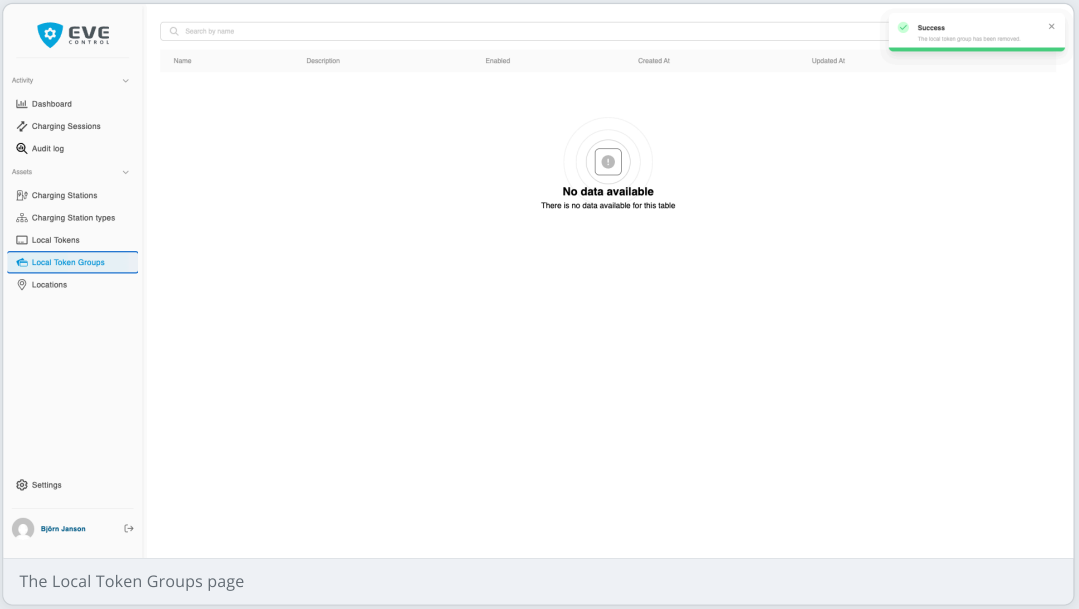
Note: A newly created token is *valid* and *not blocked* by default. However, it will not authorize charging until it is given access to a charger — either directly or through a token group linked to a location.

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

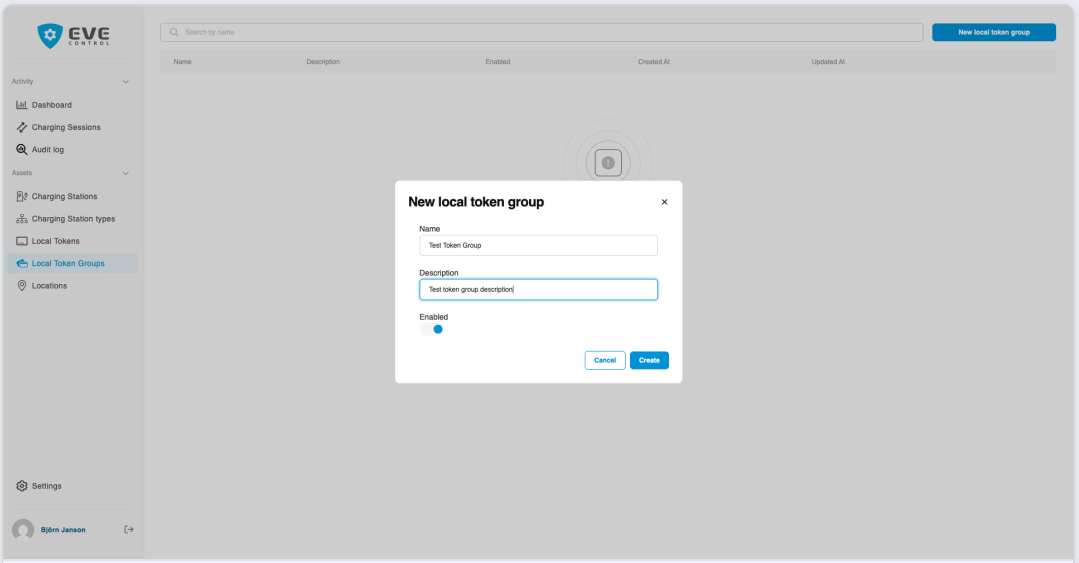
Click **Local token groups** in the left sidebar.



The Local Token Groups page

2 Fill in Group Details

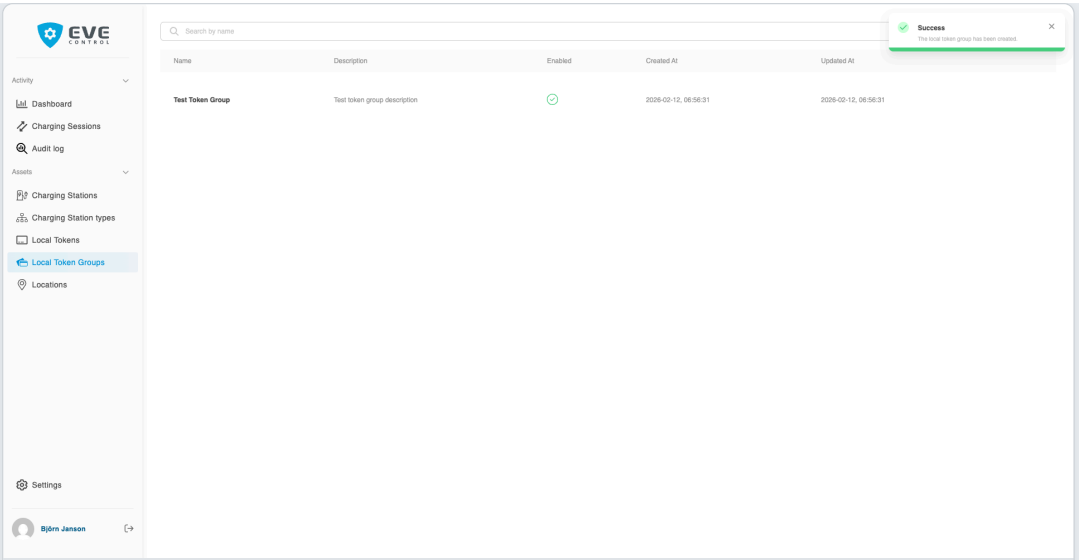
Click **Create** and enter a **name** and **description** for the group, then click **Create**.



The token group creation form

3 Verify the Token Group

The new group appears in the list.



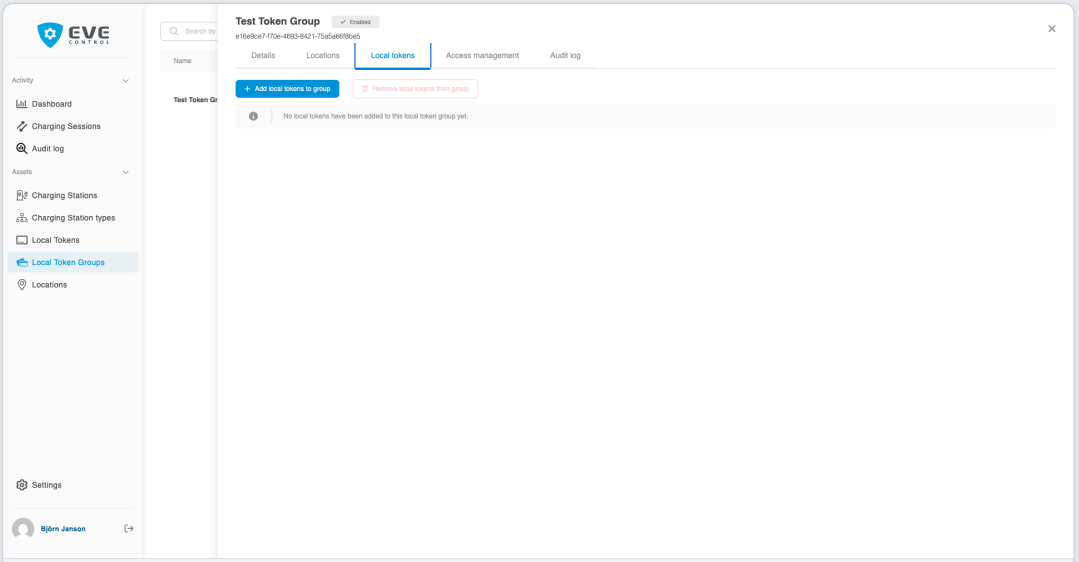
The token group is now listed

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

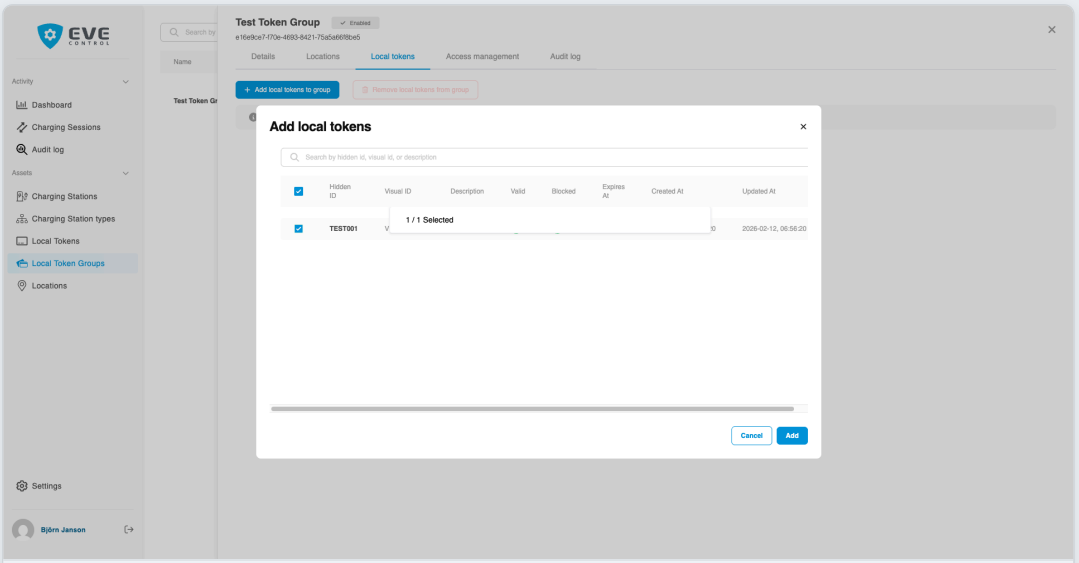
Navigate to **Local token groups** and click on the group. Then select the **Local tokens** tab.



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

2 Select Tokens to Add

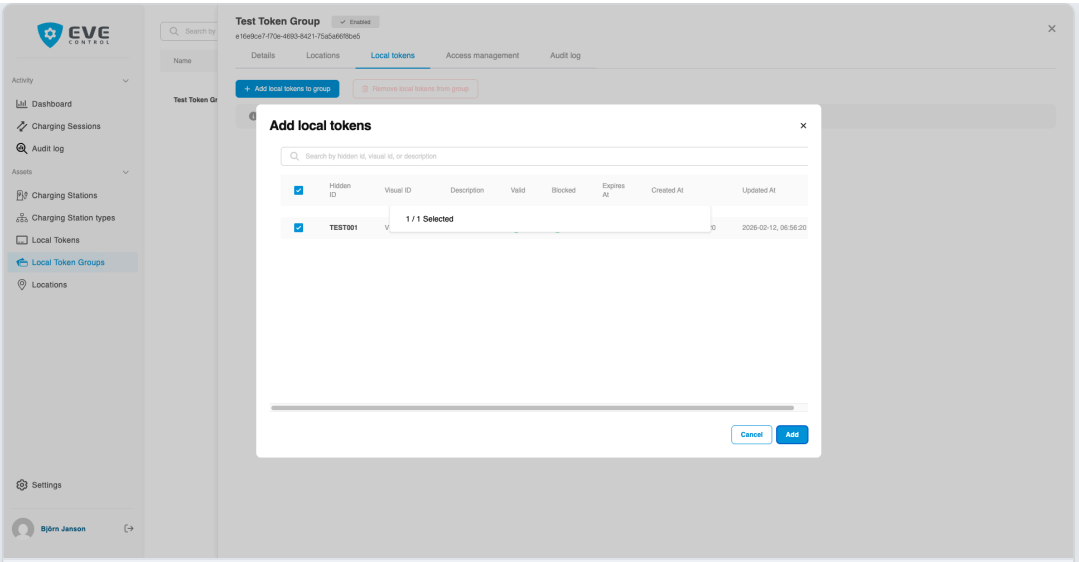
Click **Add local tokens to group**. Check the boxes next to the tokens you want to add, then click the confirm button.



Selecting tokens to add to the group

3 Confirm

The selected tokens now appear in the group.



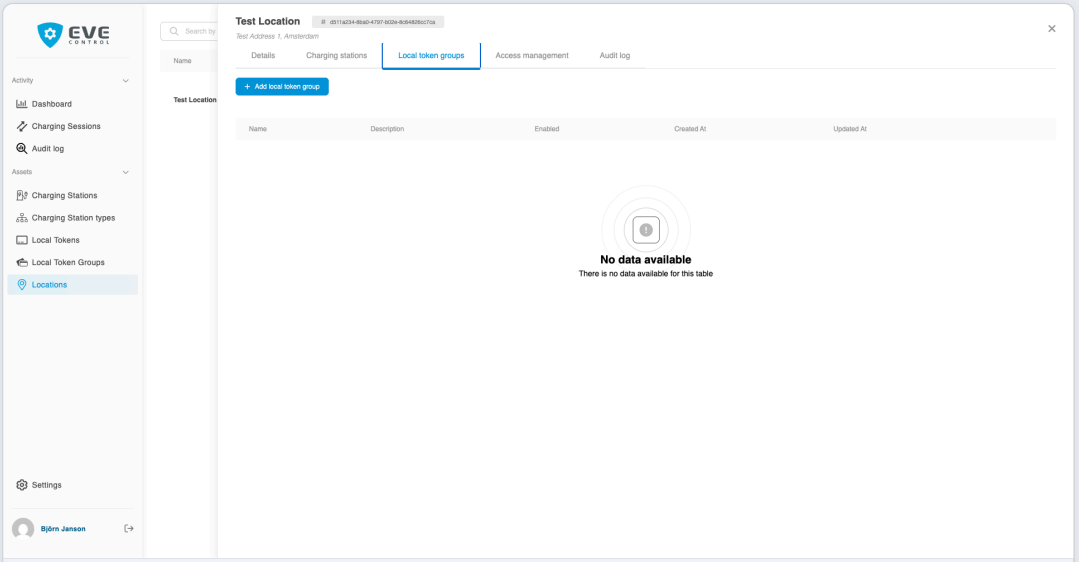
The token is now part of this group

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

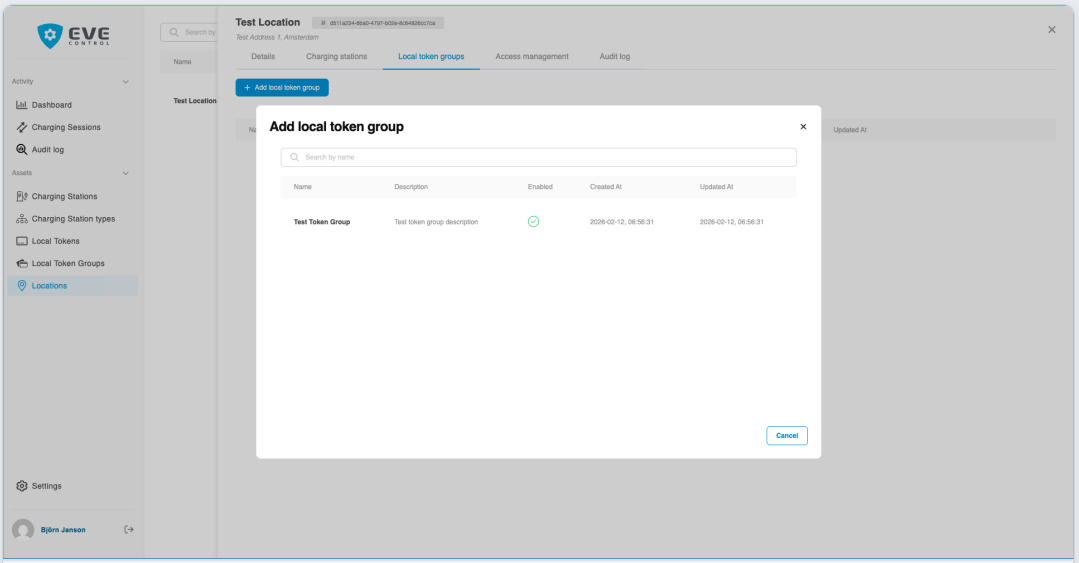
Navigate to **Locations**, click on the location, then select the **Local token groups** tab.



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

2 Select a Token Group

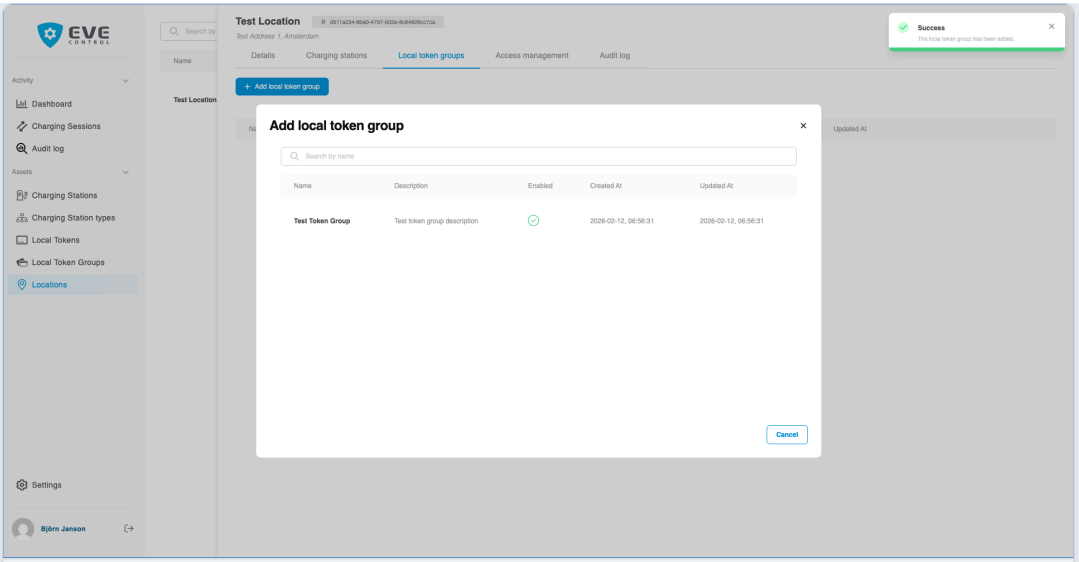
Click **Add local token group**. Select the group you want to link and confirm.



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.

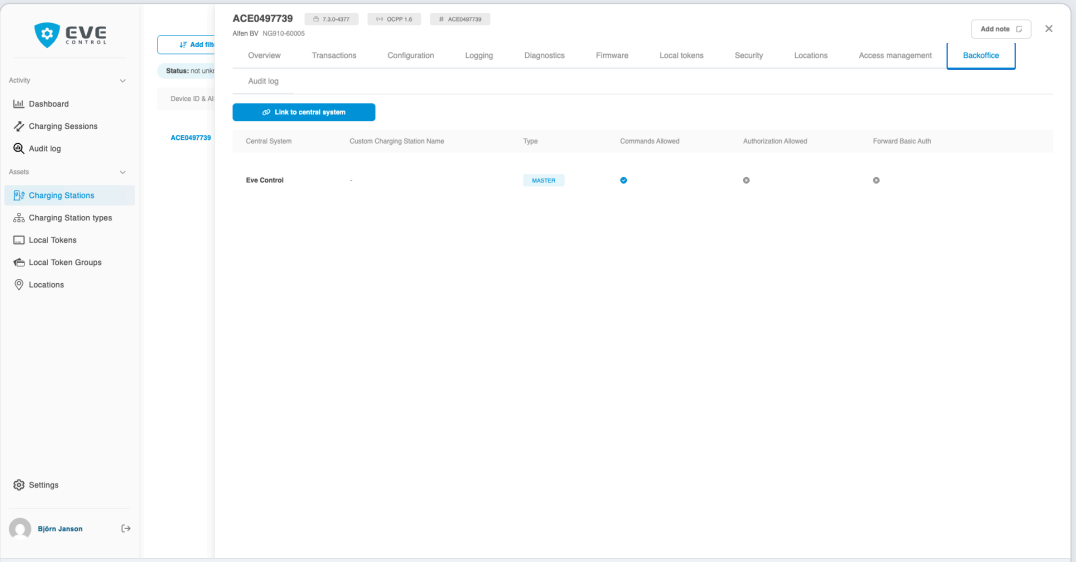
9. Forward to Primary Backoffice

> **Note:** This functionality will change before go-live to not having set Eve Control to READONLY anymore. Users will also be able to add a custom backoffice connection self-service

If you use a third-party Charge Point Management System (CPMS) as your primary backoffice, you can configure Eve Control to forward charger communication to that system. Eve Control then operates in READONLY mode.

1 Open the Charger's Backoffice Tab

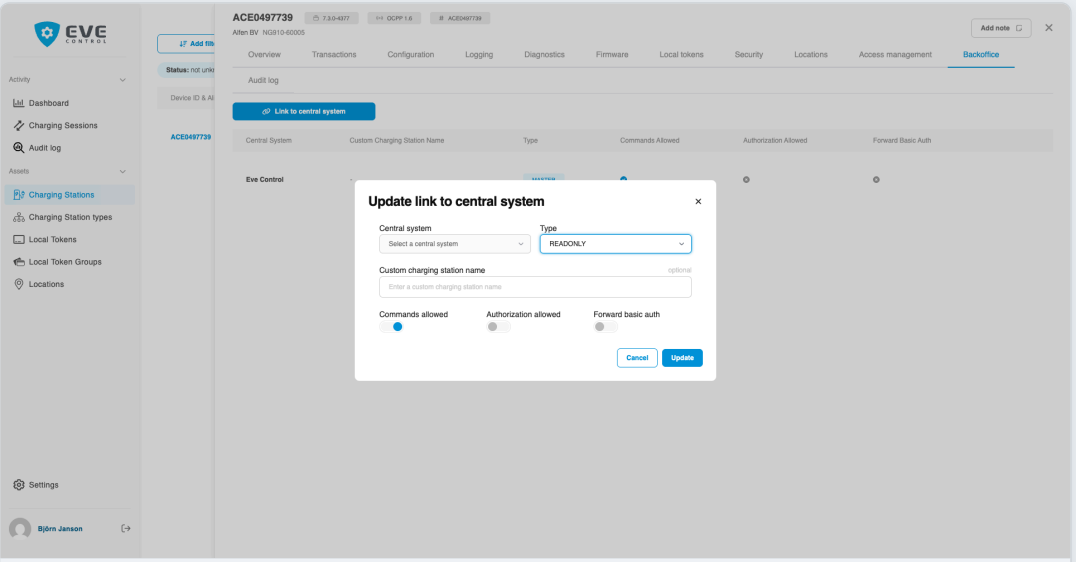
Navigate to **Charging Stations**, click on the charger, then select the **Backoffice** tab. By default, Eve Control is listed as MASTER.



The Backoffice tab showing Eve Control as MASTER

2 Change Eve Control to READONLY

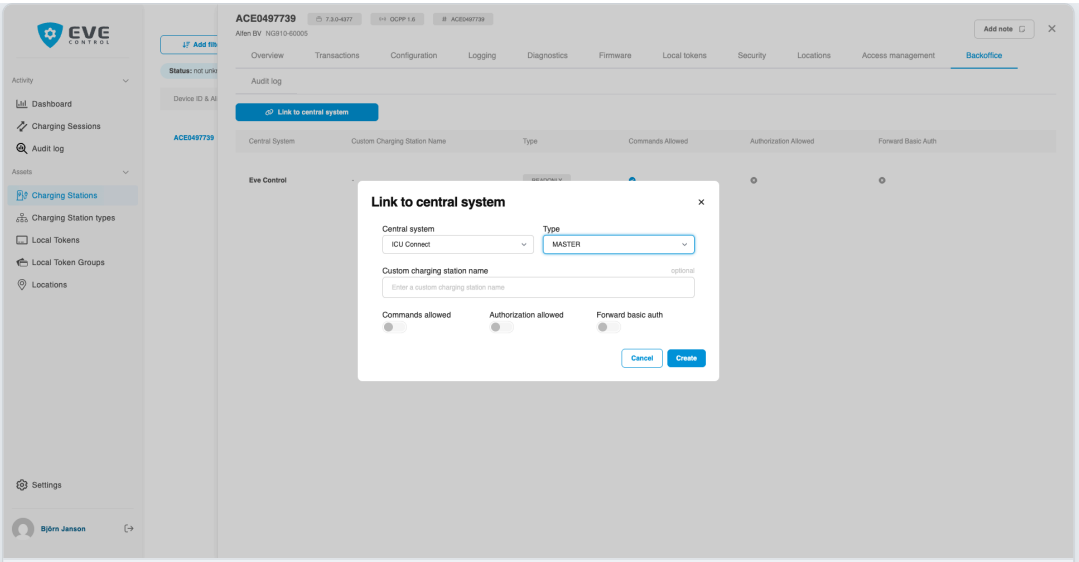
Click the edit icon next to Eve Control. Change the type from MASTER to **READONLY** and click **Update**.



Changing Eve Control from MASTER to READONLY

3 Link Your Primary Backoffice

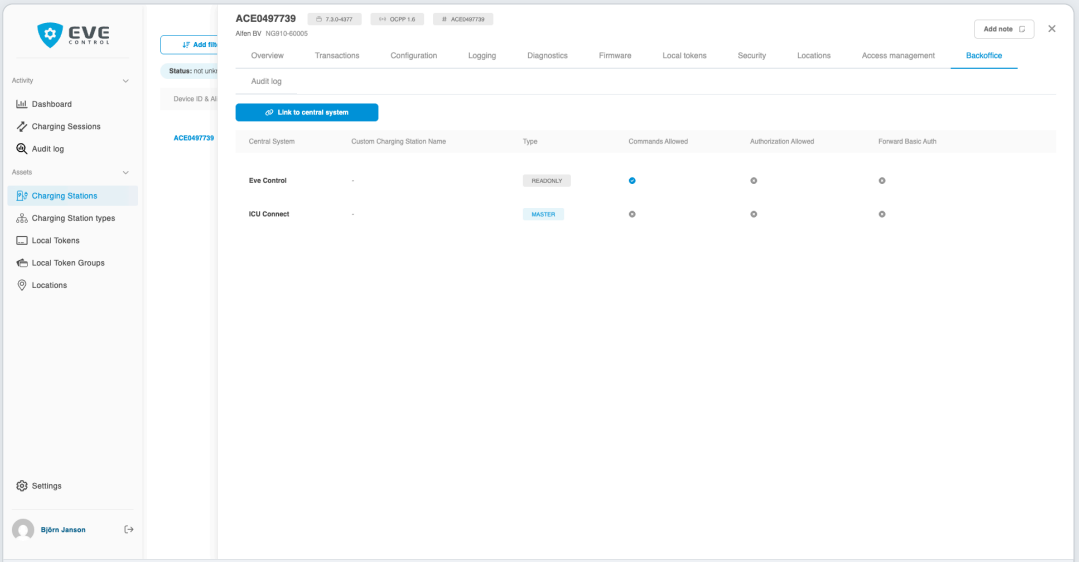
Click **Link to central system**. Select your primary backoffice system (e.g. ICU Connect), set the type to **MASTER**, and click **Create**.



Linking to a primary backoffice system as MASTER

4 Verify the Configuration

Both backoffice connections are now visible: Eve Control as READONLY and your primary system as MASTER.



Eve Control (READONLY) and the primary backoffice (MASTER) are both connected

MASTER vs READONLY: The MASTER backoffice controls the charger — it can start/stop sessions, manage tokens, and send configuration. READONLY only receives data and status updates. A charger can have at most one MASTER connection.

10. Changing to Secure WebSocket Connectivity

By default, chargers migrated via OCPP (Option B in section 1) 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. 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.

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 by its serial number (e.g. ACE0497739). 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:

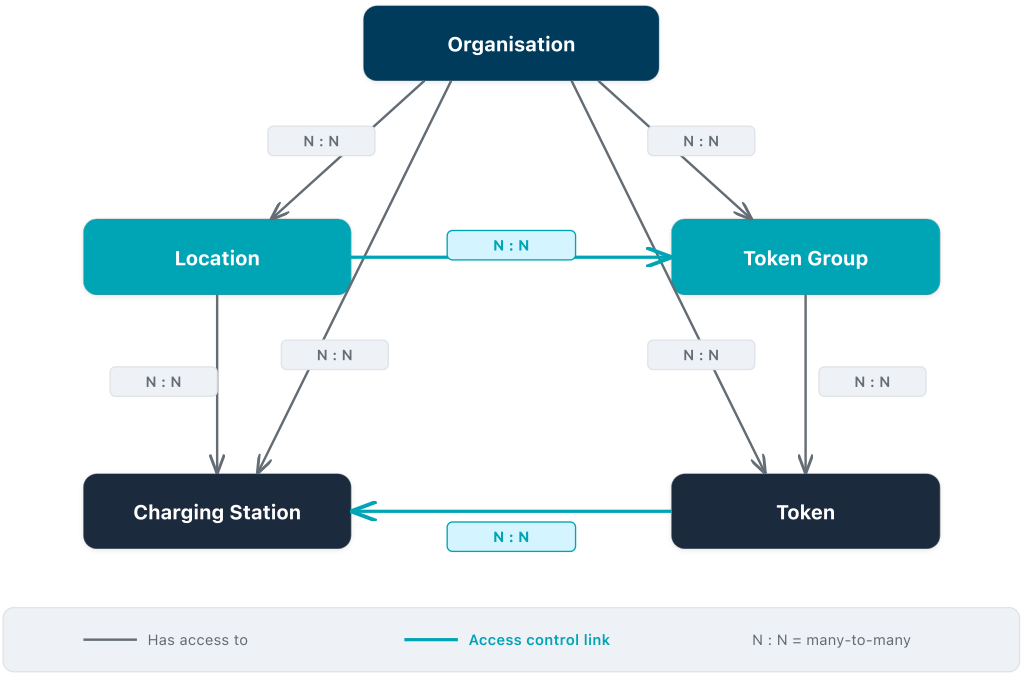
- A **charger** can be assigned to one or more **locations**
- A **location** can have multiple **chargers** and multiple **token groups**
- A **token group** can be linked to multiple **locations** and contain multiple **tokens**
- A **token** can belong to multiple **token groups** and have direct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



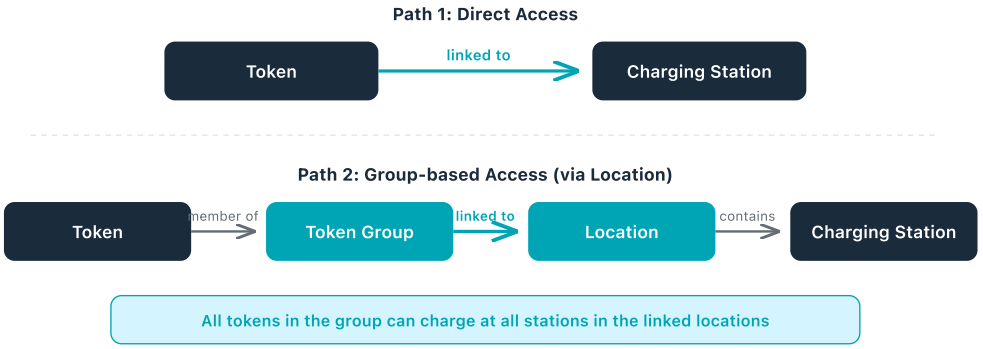
All Entity Relationships

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

Manage the charger's OCPP backoffice connections. See section 9 for details on configuring primary backoffice forwarding.

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

   A user must meet two conditions to access Eve Control:

   - Be placed in an **organisation** (users not in an organisation see "Not allowed")
   - Have at least one **role** assigned (users without roles see "Not allowed")

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

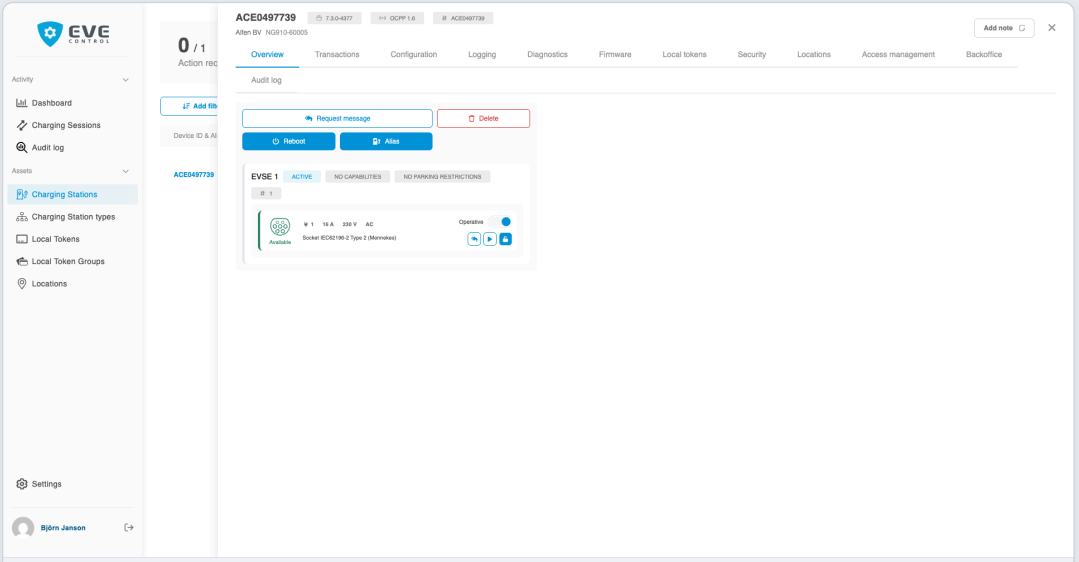
This is the most convenient method if the charger is already connected to Eve Control. The charger sends an `Authorize` request containing the card's Hidden ID whenever a card is swiped — even if the card is not yet registered.

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

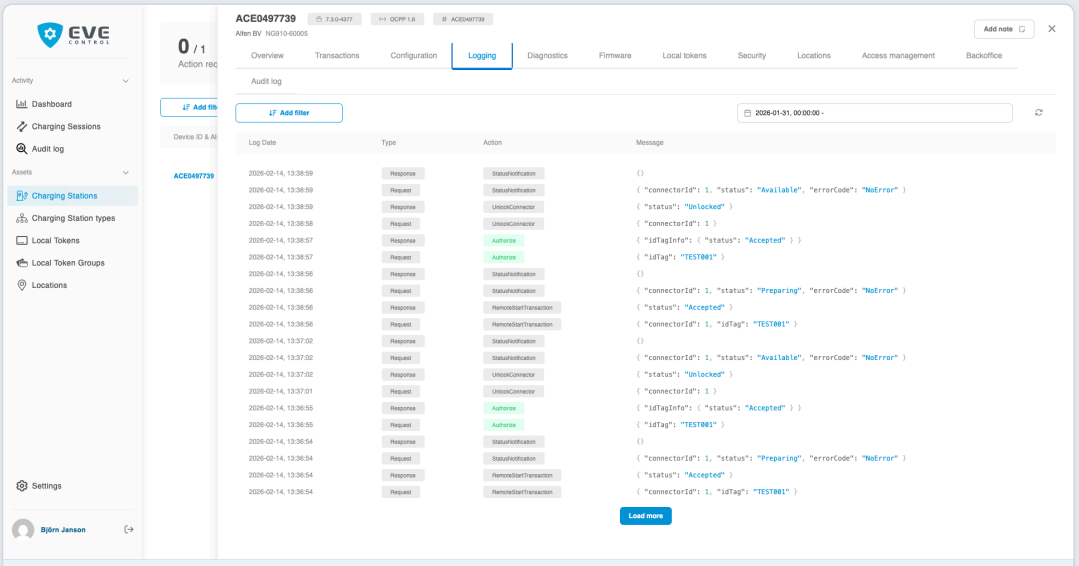
Navigate to **Charging Stations** in the sidebar and click on the charger where you swiped the card.



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.

Questions & Answers

Common questions about Eve Control concepts and operations.

Q What is a Location?

A **Location** represents a physical site where one or more charging stations are installed — for example, a parking garage, office building, or housing complex. Locations are used to:

- Group charging stations by physical site
- Manage charging access via token groups (a token group linked to a location grants access to all chargers at that location)
- Organize your fleet geographically

Each location has a name, address, and other details. Charging stations must be assigned to a location for token-group-based access control to work.

Q What is a Local Token?

A **Local Token** represents a charge card (RFID tag) registered in Eve Control. Each token has:

- **Hidden ID (UID)** – the internal identifier stored on the card's chip, used for authentication
- **Visual ID** – the number printed on the card
- **Description** – a human-readable label (e.g. the cardholder's name)

Tokens can be *valid/invalid* and *blocked/unblocked*. A token must be valid and not blocked to authorize charging. Tokens can be given charging access either directly (per charger) or through token groups (per location).

Q What is a Local Token Group?

A **Local Token Group** is a collection of tokens that share the same charging access. Instead of configuring access for each token individually, you:

1. Create a token group
2. Add tokens to the group
3. Link the group to one or more locations

All tokens in the group can then charge at all stations in those locations. Groups can be *enabled* or *disabled* — disabling a group instantly revokes access for all tokens in it.

Q How do I make sure a charge card can charge?

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

- The card is registered as a **Local Token** in Eve Control
- The token is **valid** (not invalidated)
- The token is **not blocked**
- The token has **access to the charger**, either:
  - Directly: the token is added to the charger's local token list, or
  - Via group: the token is in a **token group** that is linked to a **location** containing the charger
- If using a token group: the group is **enabled**

Q What is a Backoffice connection?

A **Backoffice connection** is the link between a charging station and a Charge Point Management System (CPMS) over the OCPP protocol. Eve Control acts as a backoffice by default when you claim a charger. You can also connect the charger to a third-party backoffice system (like ICU Connect, has-to-be, or others) for billing, roaming, or other advanced features.

Q

What is the difference between MASTER and READONLY backoffice?

- **MASTER** – the primary backoffice that controls the charger. It can authorize tokens, start/stop sessions, change configuration, and send firmware updates. A charger can have only one MASTER.
- **READONLY** – receives status updates and data from the charger but cannot send commands. Use this when you want Eve Control to monitor the charger while a third-party system manages it.

When forwarding to a primary backoffice, set Eve Control to READONLY and the external system to MASTER.

Q How do I remove a charging station from a location?

Open the charger's detail page, go to the **Locations** tab, and click the trash icon next to the location. Confirm by typing the required text. Alternatively, open the location, go to the **Charging stations** tab, and remove the charger from there.

Q How do I block or unblock a token?

Navigate to **Local tokens**, click on the token to open its detail panel. You will see the **Blocked** status. Click the **Block** or **Unblock** button and confirm. A blocked token cannot start charging sessions, even if it has access to a charger.

Q How do I validate or invalidate a token?

Navigate to **Local tokens**, click on the token to open its detail panel. You will see the **Valid** status. Click the **Validate** or **Invalidate** button and confirm. An invalidated token cannot authorize charging. Newly created tokens are valid by default.

Q How do I enable or disable a token group?

Navigate to **Local token groups**, click on the group to open its detail panel. You will see the **Enabled** status. Click **Enable token group** or **Disable token group** and confirm. When a group is disabled, none of the tokens in it can charge via that group's location links.

Q What happens if I delete a token group?

Deleting a token group removes it permanently. All tokens that were in the group lose the location-based access that the group provided. The tokens themselves are *not* deleted — they remain in your token list but will no longer have access through that group. If those tokens also have direct charger access, that access is not affected.

Q Can one token be in multiple token groups?

Yes. A token can belong to multiple token groups. Its effective access is the **union** of all locations linked to all groups it belongs to. For example, if a token is in Group A (linked to Location 1) and Group B (linked to Location 2), it can charge at both locations.

Q Can one token group be linked to multiple locations?

Yes. A token group can be linked to multiple locations. All tokens in the group will have access to all chargers at every linked location.

Q How do I check if a token has charging access?

Navigate to **Local tokens**, click on the token, then go to the **Charging stations** tab. This shows all chargers the token has direct access to. To check group-based access, look at the **Local token groups** tab to see which groups

the token belongs to, then check which locations each group is linked to.

Q What is OCPP?

OCPP (Open Charge Point Protocol) is the industry-standard communication protocol between charging stations and backoffice systems. Alfen chargers use OCPP to communicate with Eve Control (and other CPMS platforms). OCPP handles authentication, session management, configuration, firmware updates, and diagnostics. Eve Control supports OCPP 1.6.

Q How do I view charger logs?

Navigate to **Charging Stations**, click on a charger, then select the **Logging** tab. This shows all OCPP messages between the charger and Eve Control in real time, including authorization requests, session events, configuration changes, and status notifications.

Q What is the difference between WS and WSS?

- **WS (`ws://`)** – an unencrypted WebSocket connection. Data between the charger and Eve Control is sent in plain text, which means it can potentially be intercepted or tampered with.
- **WSS (`wss://`)** – a secure WebSocket connection encrypted with TLS (the same technology used for HTTPS). All communication is protected against eavesdropping and tampering.

WSS is the recommended protocol for production use. WS is only used as an initial connection method when migrating chargers remotely via OCPP, because the charger may not yet have the required TLS root certificate.

Q Why do remotely migrated chargers initially connect via WS instead of WSS?

When migrating a charger remotely via OCPP from another backoffice (Option B in section 1), the charger may not yet have the TLS root certificate needed to establish a secure `wss://` connection to Eve Control. Using `ws://` allows the charger to connect initially so that a **security firmware update** can be performed through Eve Control to install the certificate and switch to `wss://`.

Q How do I switch a charger from WS to WSS?

Perform a **security firmware update** via the charger's **Firmware** tab in Eve Control. This update installs the required TLS root certificate and automatically reconfigures the charger's OCPP connection URL from `ws://ocpp.alfen.com/` to `wss://ocpp.alfen.com/`. The charger will reboot and reconnect securely. See section 10 for step-by-step instructions.

Q Do chargers connected via local installation tooling also need a security firmware update?

No. When you connect a charger using the **Service Installer**, **MyEve**, or **Eve Install** app with the Eve Control preset (Option A in section 1), the charger is configured to use `wss://` from the start. The security firmware update is only needed for chargers that were migrated remotely via OCPP using an initial `ws://` connection.

Q What is the difference between direct access and location-based access?

- **Direct access** — you link a token directly to a charging station. Simple but requires managing each token-charger pair individually.
- **Location-based access** — you place tokens in a group, link the group to a location, and assign chargers to that location. More scalable: adding a new charger to the location automatically gives all tokens in linked groups access to it.

You can use both methods simultaneously. A token can have direct access to some chargers and group-based access to others.

Q What happens to a user without an organisation or roles?

A user who is not placed in any organisation, or who is in an organisation but has no roles assigned, will see a "Not allowed" page when they log in. They cannot access any part of the application. An administrator must assign the user to an organisation and grant at least one role before they can use Eve Control.

Q How do I unlock a charger's connector remotely?

Navigate to **Charging Stations**, click on the charger, and click the unlock icon on the Overview tab. Confirm the action. You can verify it worked by going to the **Logging** tab and checking for an `UnlockConnector` message with the result "Unlocked".

Q How do I change an OCPP configuration parameter on a charger?

Open the charger's detail page and go to the **Configuration** tab. Use the filter field to find the parameter, then click the edit icon to change its value. After saving, check the **Logging** tab to verify the change was accepted by the charger. You can also add entirely new parameters using the "Add variable" button.

Q How do I download diagnostics from a charger?

Open the charger's detail page and go to the **Diagnostics** tab. Select a date range using the calendar picker, then click **Send request**. The charger will process the request and upload the diagnostics. This may take 20 seconds or more. Check the Logging tab for a `DiagnosticsStatusNotification` with status "Uploaded" to confirm completion.

Q What are the available user roles?

Eve Control has three organisation roles:

- **Administrator** — full access to all features, including user management and organisation settings
- **Technician** — access to charger management, diagnostics, and configuration
- **End-User** — basic access for viewing chargers and charging sessions

Role assignment is managed by organisation administrators.

Q What does the Security tab on a charger do?

The **Security** tab controls which token authorisation profiles are active on the charger. For example, the `local-token-group` profile enables location-based access via token groups. You can drag profiles between "Active" and "Available" lists. Removing `local-token-group` from the active list means tokens with group-based access can no longer charge at that charger, even if all other conditions are met.

Q How do I find the Hidden ID of an RFID charge card?

The **Hidden ID** (also called UID or token ID) is the internal identifier stored on the 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. There are several ways to find it. See section 18: Finding the Hidden ID of a Charge Card for detailed step-by-step instructions with screenshots.

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.