Smart OCPP Broker

Onboarding Guide

Welcome! This guide walks you through the information we need to connect your charging infrastructure to Pleevi's Smart OCPP Broker. The broker acts as a proxy between your charging stations and your existing CPMS. We use this to identify the driver (for the driver application). If you opted for smart charging without a local controller, this is also how we send the schedules to the charging poles.

1. Current CPMS WebSocket URL

We need the WebSocket endpoint of your current Charging Point Management System (CPMS). This is the URL your charging stations currently connect to via OCPP. The Pleevi broker will proxy all OCPP messages through to this endpoint, ensuring full transparency with your existing platform.

CPMS WebSocket URL	*e.g. wss://cpms.example.com/ocpp*

Typically this is a `wss://` (secure WebSocket) or `ws://` URL provided by your CPMS vendor.

2. OCPP Security Profile & Credentials

OCPP 2.0.1 defines three security profiles with increasing levels of protection. Please indicate which profile is configured on your charging stations and provide the corresponding credentials and certificates. This allows us to correctly set up the broker's connection to your stations.

Security Profile in Use (see below)	*e.g. Profile 2 (TLS + Basic Auth)*

OCPP Version (optional)	*e.g. OCPP 1.6J / OCPP 2.0.1*

ℹ️ **Only fill in the section that matches your profile**

Each profile below first explains how authentication works, then asks for the specific credentials we need. If you're unsure which profile or certificates are in use, let us know. We'll help you set this up. If possible already send us a screenshot of the OCPP configuration view of the charging station.

Profile 0

No Authentication (ws://)

The charging station connects to the CPMS over an unencrypted WebSocket (ws://) without any authentication. There is no password and no TLS encryption. This is common on simple or older charging stations that rely on network-level security (e.g. a private APN or local network).

What we need for Profile 0:

Charging station has access to the internet	*Can the charging station reach the internet directly, or is it behind a firewall/NAT?*

Profile 1

Basic Authentication — Unsecured Transport (ws://)

Communication runs over an unencrypted WebSocket (ws://) connection. The charging station authenticates to the CPMS using an HTTP Basic Auth password sent during the WebSocket upgrade. Because traffic is not encrypted, this profile is only suitable for trusted/private networks or when a VPN tunnel is in place between stations and the CPMS. It is deprecated in most modern deployments.

What we need for Profile 1:

VPN (if applicable)	*If stations connect via VPN or the CPMS is behind a VPN, provide more details on the setup.*

Charging station has access to the internet	*Can the charging station reach the internet directly, or is it behind a firewall/NAT?*

Profile 2

TLS with Basic Authentication (wss://)

Communication is encrypted using TLS 1.2 or higher (wss://). During the TLS handshake, the CPMS presents a server certificate which the charging station validates against a trusted CA root. After the secure channel is established, the station authenticates with an HTTP Basic Auth password. This profile protects against eavesdropping and man-in-the-middle attacks while remaining straightforward to manage.

What we need for Profile 2:

Custom CA Root Certificate	*Do you use a custom CA Root Certificate? If not sure, indicate so.*

VPN (if applicable)	*If stations connect via VPN or the CPMS is behind a VPN, provide more details on the setup.*

Charging station has access to the internet	*Can the charging station reach the internet directly, or is it behind a firewall/NAT?*

Profile 3

Mutual TLS — Client-Side Certificates (wss://)

The highest security level. Both the CPMS and the charging station exchange and verify TLS certificates (mutual TLS / mTLS). This eliminates password-based authentication entirely. Each station holds a unique client certificate that acts as its identity. The CPMS verifies this certificate against a trusted CA before allowing communication. Provides message integrity and non-repudiation.

ℹ️ Onboarding meeting required

Due to the complexity of mutual TLS configuration, we will schedule a dedicated onboarding meeting to walk through the certificate setup together. Please reach out to your Pleevi contact or email support@pleevi.ai to arrange this.

3. Driver List

Please provide a CSV file containing the drivers that should be authorized through the Smart OCPP Broker. Each driver should have an email address and one or more badge IDs (RFID tokens). Multiple badge IDs for a single driver can be separated by commas within the same field. This list is required for identifying the user in the broker, if authorisation is activated via the CPMS, the CPMS will remain in charge of authentication.

Expected CSV Format

Email	Badge ID(s)
john.doe@example.com	BADGE001, BADGE002
jane.smith@example.com	BADGE003
...	...

File format: UTF-8 encoded CSV with headers `email` and `badge_ids`. Send the file as an attachment alongside this completed guide.

4. What Happens Next?

ℹ️ New WebSocket URL

After receiving and processing the information above, we will provision your environment in the

> Pleevi platform and provide you with a new WebSocket URL.
>
> This new URL should be configured on your charging stations in place of the current CPMS WebSocket URL. All OCPP communication will then flow through the Pleevi Smart OCPP Broker, which proxies messages to your original CPMS.
>
> Your existing CPMS will continue to receive all OCPP messages as before — no changes are needed on the CPMS side.

Questions? Reach out to your Pleevi contact or email us at support@pleevi.ai.