CENTRAL CLOUD & FLEET MANUAL

GRID-EMS-SERVER Connection & Fleet Manual

Field Reference Guide for Pairing Edge GEMS Units to the Central Cloud Server, High-Frequency Telemetry Ingestion, and Remote Fleet Command Orchestration.

DOCUMENT REFERENCE
GEMS-MAN-SRV-2026

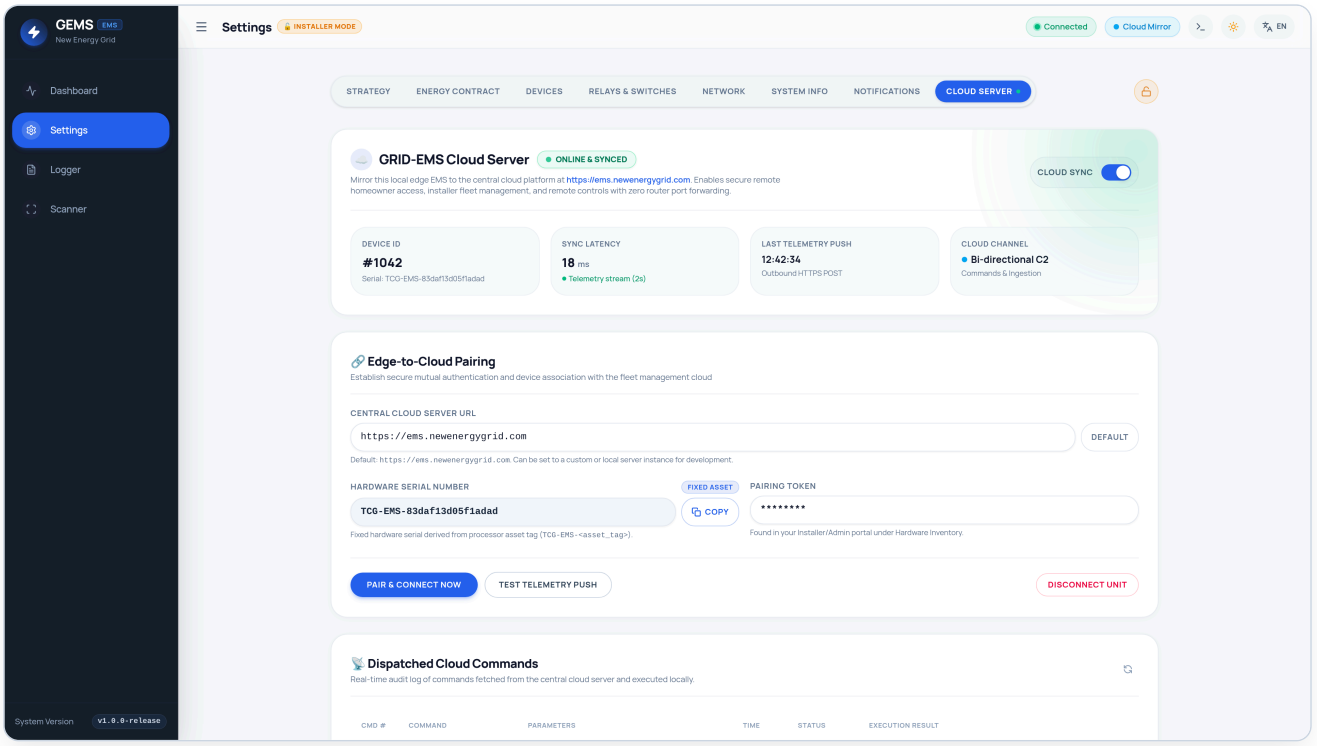
APPLICABLE RELEASE
v9.25.3-release (Official Tag)

CENTRAL CLOUD SERVICE
GRID-EMS-SERVER (v2.x Cloud Fleet API)

DEFAULT SERVER ENDPOINT
https://ems.newenergygrid.com

SECURITY ARCHITECTURE
Outbound-Only TLS 1.3 • Zero Router Port Forwarding

EDGE TARGET PLATFORM
Raspberry Pi 5 / 4 (ARM64 Linux)



© 2026 New Energy Grid • Confidential Field Reference

Manual Overview & Table of Contents

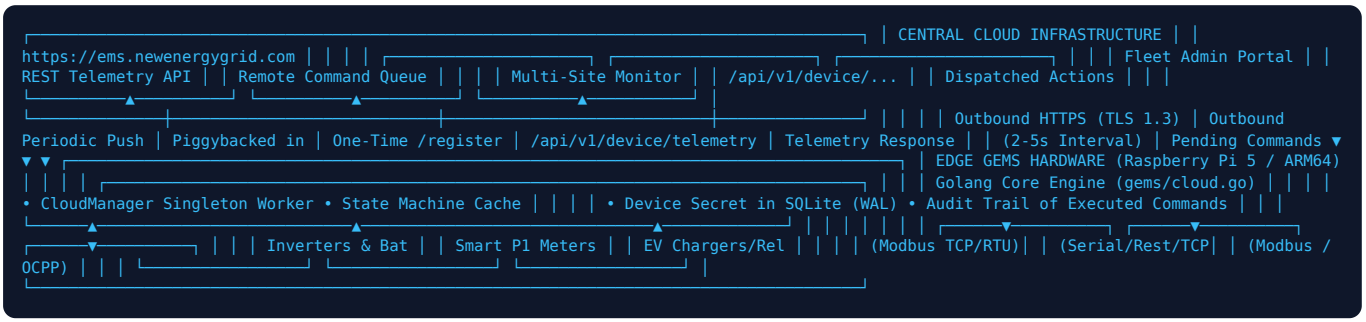
This manual provides electricians, solar installers, fleet operators, and system integrators with technical specifications and field procedures required to pair local edge GEMS installations with **GRID-EMS-SERVER**.

Section	Topic	Primary Audience
Section 1	Architecture & Communications Topology	Systems Engineers, Network Architects
Section 2	Network & Firewall Prerequisites	IT Administrators, On-Site Installers
Section 3	Pairing & Cryptographic Handshake Protocol	Field Commissioning Technicians
Section 4	Live Telemetry Ingestion Engine & Metrics Schema	Fleet Integrators, Software Engineers
Section 5	Remote Command Dispatch & Execution Engine	CPO Operators, Grid Aggregators
Section 6	UI Operation: Settings → Cloud Server Tab	Commissioners, Technical Support
Section 7	Security, Privacy & Edge Autonomy Guarantee	Data Compliance Officers, Security Teams
Section 8	Troubleshooting, Status Codes & Field Diagnostics	Service Technicians, Helpdesk Tier 2

> 💡 **Edge Autonomy & 100% Optional Cloud Connectivity**
>
> **Local-First Guarantee & Optional Integration:** GEMS is engineered from the ground up as a decentralized edge node. Connecting to **GRID-EMS-SERVER** is **possible and 100% optional**. All local control loops—including sub-second Modbus EV throttling, solar surplus divert, Flanders peak shaving, Netherlands smart saldering, battery arbitrage, and relay automation—execute with complete autonomy without any cloud or internet dependency. When paired, the cloud integration adds encrypted remote access, multi-site fleet management, and automated monitoring.

1. Architecture & Communications Topology

GEMS communicates with **GRID-EMS-SERVER** via an outbound-only polling and telemetry push pipeline. In this architecture, the edge controller initiates all connections over HTTPS, completely eliminating the need for inbound router ports, dynamic DNS services, or public IP addresses at the customer premises.



1.1 Core Architectural Principles

- **Zero Inbound Firewall Exposure:** Home and commercial routers do not require port forwarding, DMZ allocation, or UPnP. All communication is outbound HTTPS to port 443.
- **Telemetry Aggregation:** Every sync interval (configurable between 2s and 60s, default 5s), the edge engine collects real-time measurements across inverters, batteries, meters, EV chargers, heat pumps, and tariffs into a single JSON payload.
- **Piggybacked Remote Commands:** Rather than opening long-lived persistent inbound channels or requiring complex VPNs, the cloud server attaches any pending commands to the HTTP 200 response of the telemetry push. The edge controller executes the command and acknowledges status in the next request.
- **Sub-Millisecond Hardware Isolation:** The CloudManager goroutine runs decoupled from the local hardware polling workers. A slow WAN link or cloud downtime will never cause Modbus polling jitter or delay peak-shaving responses.

2. Network & Firewall Prerequisites

Before commissioning the cloud connection on site, verify that the local network meets the following outbound routing criteria:

Destination Host	Protocol	Port	Direction	Purpose
`ems.newenergygrid.com` (or custom server host)	HTTPS (TLS 1.2/1.3)	TCP 443	Outbound	Device registration, telemetry ingestion, remote command ack
Local DNS (e.g., `1.1.1.1`, `8.8.8.8`, Gateway)	DNS	UDP/TCP 53	Outbound	Host resolution of cloud server domain name
NTP Time Server (e.g., `pool.ntp.org`)	NTP	UDP 123	Outbound	System clock accuracy (required for valid TLS certificates & timestamps)

> ⚠️ **Corporate / Strict Guest VLAN Guidelines**
> If installing GEMS behind a strict corporate firewall, ensure that outbound HTTPS traffic to `ems.newenergygrid.com` is not subject to deep-packet SSL inspection (MITM proxying) unless the enterprise CA root certificate is installed into the Debian system trust store (`/usr/local/share/ca-certificates/`).

3. Pairing & Authentication Workflow

Pairing authorizes a physical GEMS edge device to push data to a specific tenant/site account within **GRID-EMS-SERVER**. Pairing uses a secure two-phase handshake.

3.1 Step-by-Step Pairing Workflow

1. **Acquire Pairing Token:** Log in to the central fleet management portal at `https://ems.newenergygrid.com`. Navigate to **Sites** → **Add New EMS Node** and copy the generated 16-character hardware pairing token (e.g., `PAIR-8821-X9K2`).
2. **Detect or Confirm Serial Number:** GEMS automatically extracts the persistent hardware serial number from the Raspberry Pi SoC via `/proc/cpuinfo` and prefixes it with `TCG-EMS-` (e.g., `TCG-EMS-83daf13d05f1adad` for asset tag `83daf13d05f1adad`). The Hardware Serial Number is permanently locked to the edge processor asset tag to maintain cryptographic hardware identity.
3. **Submit Credentials in GEMS UI:** Open GEMS Settings → **Cloud Server** tab. Paste the pairing token into the input field.
4. **Initiate Handshake:** Click **Pair & Connect Now**. The backend immediately dispatches the registration payload:

```
POST /api/v1/device/register HTTP/1.1
Host: ems.newenergygrid.com
Content-Type: application/json
User-Agent: GRID-EMS-Agent/9.4.0

{
  "serial_number": "TCG-EMS-83daf13d05f1adad",
  "pairing_token": "PAIR-8821-X9K2",
  "model": "GEMS v9.4 Pro",
  "firmware_version": "v9.4.2",
  "ip_local": "192.168.1.150"
}
```

Upon verifying that the pairing token is valid and unallocated, the server generates a permanent `device_id` and a high-entropy 256-bit `device_secret` token:

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "status": "ok",
  "device_id": 1042,
  "device_secret": "",
  "message": "Device paired successfully"
}
```

The GEMS engine securely commits the received `device_id` and `device_secret` into the local SQLite database (`site_settings` table). From this moment forward, the pairing token is retired, and all subsequent communications use the cryptographic device secret.

4. Live Telemetry Ingestion & Offline Store-and-Forward Buffer

Once paired, the `CloudManager` goroutine executes a background loop pushing telemetry at the configured sync interval. If home internet connectivity drops temporarily, GEMS buffers telemetry frames locally in a bounded SQLite store-and-forward queue (`cloud_telemetry_queue`, up to 10,000 snapshots at 60-second intervals) and replays them automatically once WAN connectivity returns. Every sync packet is formatted according to the standardized GRID-EMS-SERVER JSON schema:

```
POST /api/v1/device/telemetry HTTP/1.1
Host: ems.newenergygrid.com
Content-Type: application/json
X-Device-Secret: <YOUR_DEVICE_SECRET>
X-Device-Serial: TCG-EMS-83daf13d05f1adad
User-Agent: GRID-EMS-Agent/9.4.0

{
  "solar_power_watts": 4800,
  "grid_power_watts": -1450,
  "battery_power_watts": -1200,
  "battery_soc": 78.5,
  "battery_temperature": 24.2,
  "battery_health": 99.0,
  "home_consumption_watts": 850,
  "ev_power_watts": 1300,
  "ev_charging_mode": "eco",
  "ev_connected": 1,
  "ev_soc": 0.0,
  "heat_pump_watts": 1200,
  "heat_pump_state": "boost",
  "relay1_state": 1,
  "relay2_state": 0,
  "current_tariff_eur_kwh": 0.1245,
  "spot_price_eur_mwh": 80.0,
  "l1_current_amps": 6.3,
  "l2_current_amps": 0.0,
  "l3_current_amps": 0.0,
  "frequency_hz": 50.01,
  "voltage_v": 231.4,
  "solar_energy_today_kwh": 24.6,
  "grid_import_today_kwh": 2.1,
  "grid_export_today_kwh": 14.8,
  "home_energy_today_kwh": 11.4,
  "ev_energy_today_kwh": 6.8
}
```

5. Remote Command Dispatch & Execution

Central operators, installers, or virtual power plant (VPP) aggregators can send commands down to any edge unit via **GRID-EMS-SERVER**. When the edge pushes telemetry, the server attaches pending commands in the response payload:

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "status": "ok",
  "device_id": 1042,
  "server_time": "2026-09-07T17:19:55Z",
  "pending_commands": [
    {
      "id": 101,
      "command": "set_strategy_mode",
      "payload": {
        "mode": "flanders",
        "peak_limit_kw": 2.5
      }
    }
  ]
}
```

5.1 Supported Remote Command Catalog

Command Name	Payload Parameters	Edge Action Executed
`set_strategy_mode`	`mode`: string ("eco", "flanders", "dynamic", "zero_export"), `peak_limit_kw`: float	Updates active energy strategy and immediately applies Flanders capacity ceiling to EV and battery loops.
`set_battery_mode`	`device_id`: int, `mode`: string ("auto", "charge_grid", "discharge_grid", "hold")	Dispatches Modbus holding register commands to inverter to force battery charge or arbitrage discharge.
`throttle_ev_charger`	`device_id`: int, `max_current_a`: int (6 - 32)	Adjusts charging current limit via Modbus TCP register 5012 or OCPP `SetChargingProfile`.
`set_relay`	`relay_id`: int (1 or 2), `state`: int (0 or 1)	Actuates physical GPIO or smart HTTP relay (e.g. Shelly Pro 2) for heat pump SG-Ready or thermal boost.
`reboot`	`delay_sec`: int (default 5)	Executes graceful Linux system reboot (`sudo systemctl reboot`) after acknowledging command.

5.2 Command Acknowledgment & Audit Trail

Following local execution, GEMS acknowledges the result by posting to `/api/v1/device/commands/{id}/ack` with status (`executed` or `failed`) and execution notes. An audit log of all executed commands is displayed in real-time on the GEMS Cloud tab.

6. Step-by-Step UI Commissioning Guide

Field commissioning of the cloud connection requires less than two minutes in the GEMS Web UI:

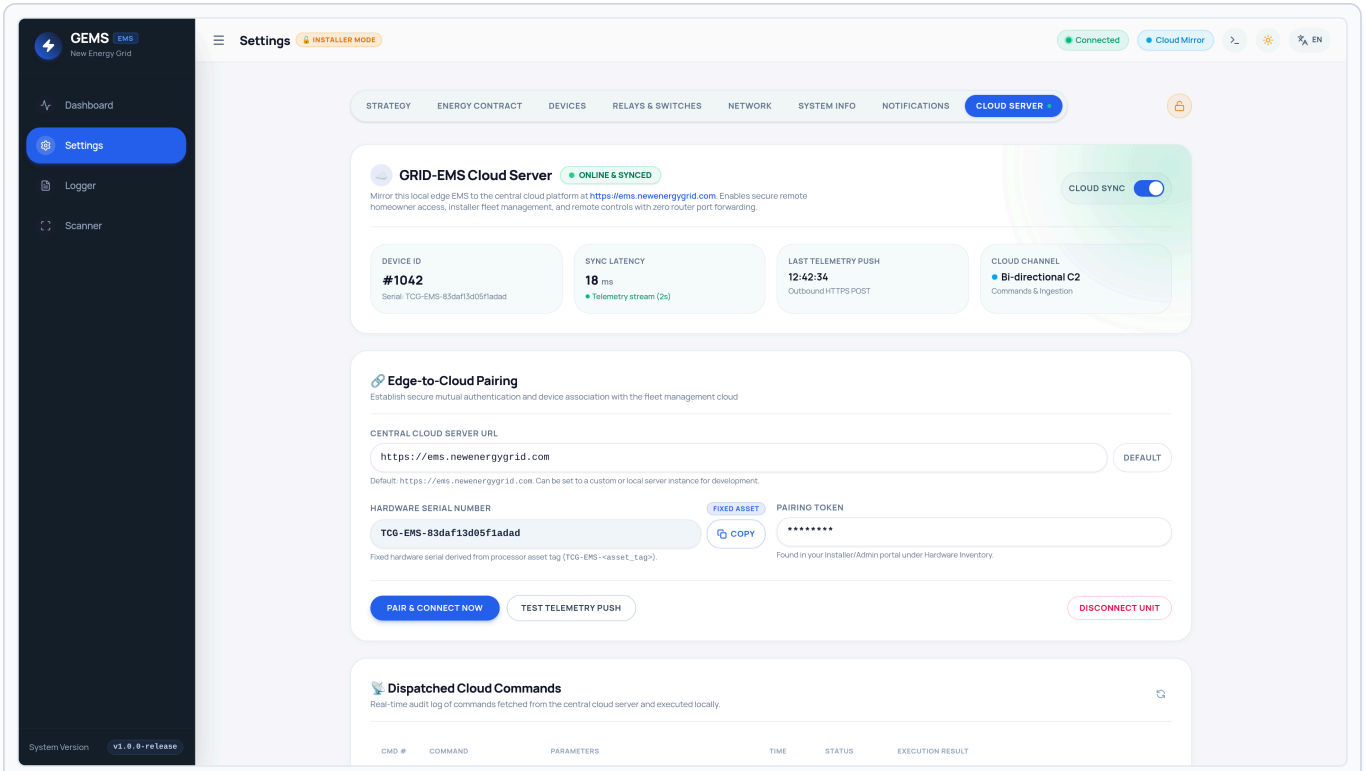


Figure 6.1: GEMS Central Cloud Settings — Showing active sync status, latency metrics, pairing fields, and audit log.

Step 1: Open Settings → Cloud Server

Open the GEMS dashboard in your browser (`http://<raspberry-pi-ip>`) and click **Settings** in the navigation sidebar. Select the **Cloud Server** tab from the horizontal tab strip.

Step 2: Enter Pairing Credentials

Verify that the **Central Cloud Server URL** is set to `https://ems.newenergygrid.com` (or enter your custom self-hosted endpoint). Paste your 16-character pairing token into the **Pairing Token** field.

Step 3: Pair and Test Connection

Click **Pair & Connect Now**. Once the card displays ● **ONLINE & SYNCED** with a green indicator, click **Test Telemetry Push** to verify end-to-end telemetry ingestion. The round-trip sync latency will be calculated and displayed (typically 15–30 ms).

7. Security, Privacy & Edge Autonomy Guarantee

7.1 Security Architecture

- **Cryptographic Secret Handshake:** All telemetry frames are authenticated using the unique `X-Device-Secret` header issued during registration. Replay attacks and spoofing are prevented by server-side timestamp validation.
- **Transport Layer Security:** All traffic strictly enforces TLS 1.3 encryption. Unencrypted HTTP traffic is rejected by the server.
- **No Inbound Port Vulnerabilities:** Because GEMS never opens an inbound public port, malicious internet scanners (e.g. Shodan) cannot detect or probe the device.

7.2 GDPR & Homeowner Privacy Compliance

In accordance with European privacy and data minimization directives (GDPR):

- **Zero Vehicle Tracking:** GEMS enforces strict directives prohibiting vehicle telematics, EV VIN storage, or driver RFID tracking. Only electrical metrics (charging power in Watts and pilot state) are transmitted.
- **Granular Disconnect:** The homeowner can click **Disconnect Unit** at any time in the UI, instantly terminating cloud communication and purging local device secrets.

8. Troubleshooting & Field Diagnostics

Reported Error / Status	Probable Root Cause	Recommended Field Resolution
Disconnected / Gray	Cloud Sync switch is toggled OFF or unit has not been paired.	Toggle the **Cloud Sync** switch to ON and click **Pair & Connect Now**.
`Handshake failed: dial tcp: lookup ...`	DNS resolution failure on Raspberry Pi local network adapter.	Verify gateway DNS settings. Test with `ping ems.newenergygrid.com` in Cockpit terminal (port 9090).
`HTTP 401 Unauthorized`	Device secret was invalidated or removed from the central portal.	GEMS automatically attempts re-registration. If token expired, generate a new token in the portal and re-pair.
`Telemetry push network error: timeout`	Local router is blocking outbound port 443 or internet bandwidth is saturated.	Verify router firewall rules. Ensure outbound TCP port 443 is unrestricted.
High Latency (> 500 ms)	Poor Wi-Fi signal or congested cellular 4G/5G backup router.	Connect Raspberry Pi via dedicated Cat6 Ethernet cable rather than Wi-Fi.

8.1 Live System Diagnostic Commands

Installers can monitor the live CloudManager daemon via SSH or the built-in Cockpit Web Terminal (Port 9090):

```
# Inspect live cloud synchronization logs
sudo journalctl -u gems -f | grep CloudManager

# Test DNS and outbound HTTPS connectivity directly from edge
curl -Iv https://ems.newenergygrid.com/api/status

# Verify edge site settings and stored cloud device ID
sqlite3 /var/lib/gems/gems.db "SELECT id, cloud_enabled, cloud_server_url, cloud_device_id, cloud_serial_number FROM site_settings WHE
```