DAMARK SOLUTIONS

Edge Gateway

Customer Onboarding & Activation Guide

PREPARED FOR	Beta customers and integrators deploying the Damark Edge Gateway
DOCUMENT TYPE	Visual onboarding procedure using real Portal and local gateway screens
STATUS	Internal beta draft — screenshots redacted
DATE	Generated June 17, 2026

HANDLING NOTICE — Screenshots in this guide have been blurred where emails, license tokens, activation tokens, remote keys, and gateway identifiers were visible. Review once more before public distribution.

ABOUT THIS GUIDE

Procedure overview

This guide walks a beta customer or integrator through the complete Edge Gateway flow: create a Portal account, verify email, generate a middleware license, run the local Edge Gateway, activate the gateway, configure local PLC or BACnet data and tags, exercise the local console for live status, command testing, auditing, and governance, and create a Remote Integration Client for external SCADA, HMI, or dashboard integration.

1	2	3	4	5
Workspace & Email Verification	**Licensing & Local Gateway**	**Cloud Registration & Activation**	**Device Configuration & Local Console**	**Remote Integration**
Steps 1–4	Steps 5–9	Steps 10–15	Steps 16–28	Steps 29–31

Before you begin

- A Windows 10/11 (x64) host machine to run the downloaded local Edge Gateway package.
- Network access from that host to the Damark Customer Gateway Portal.
- A work email address to create and verify the customer workspace.
- Local network or serial access to the PLC or BACnet devices being onboarded.
- A tag list (CSV, JSON, or controller export) for the PLCs or BACnet devices being onboarded.

HANDLING NOTICE — Screenshots in this guide have been blurred where emails, license tokens, activation tokens, remote keys, and gateway identifiers were visible. Review once more before public distribution.

PHASE 1 · WORKSPACE & EMAIL VERIFICATION

STEP 1 OF 31

Create a customer workspace

Open the Damark Customer Gateway Portal and create the customer account and workspace using the customer name, work email, password, company name, and workspace slug.

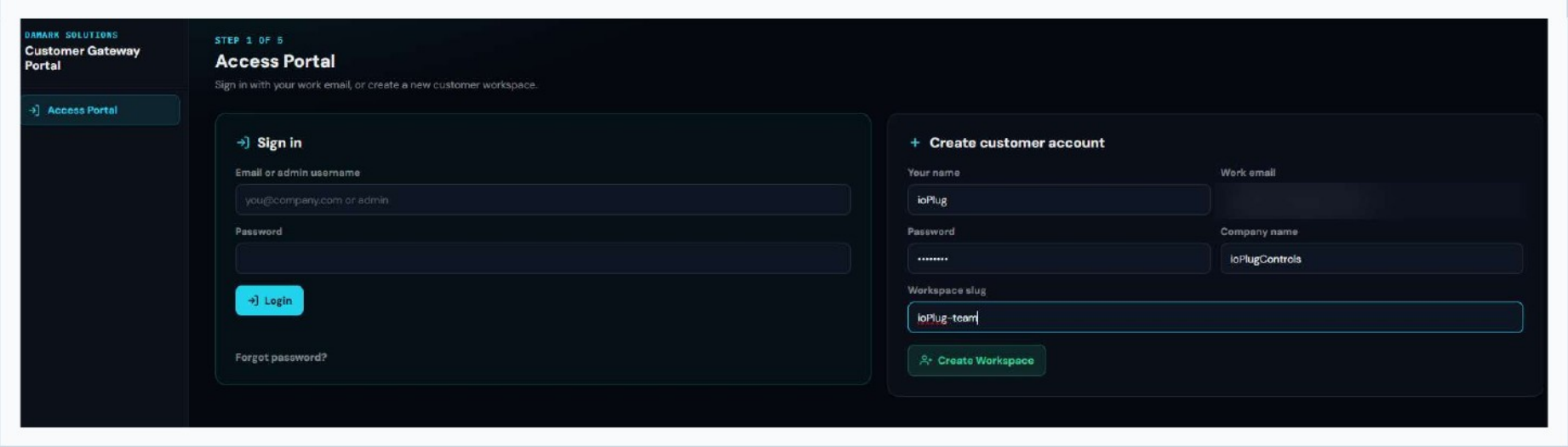

FIGURE 1 — *The Customer Gateway Portal sign-in and workspace creation screen.*

PHASE 1 · WORKSPACE & EMAIL VERIFICATION

STEP 2 OF 31

Verify email prompt

After the workspace is created, the Portal shows the email verification panel. The user should check their inbox and complete verification before signing in.

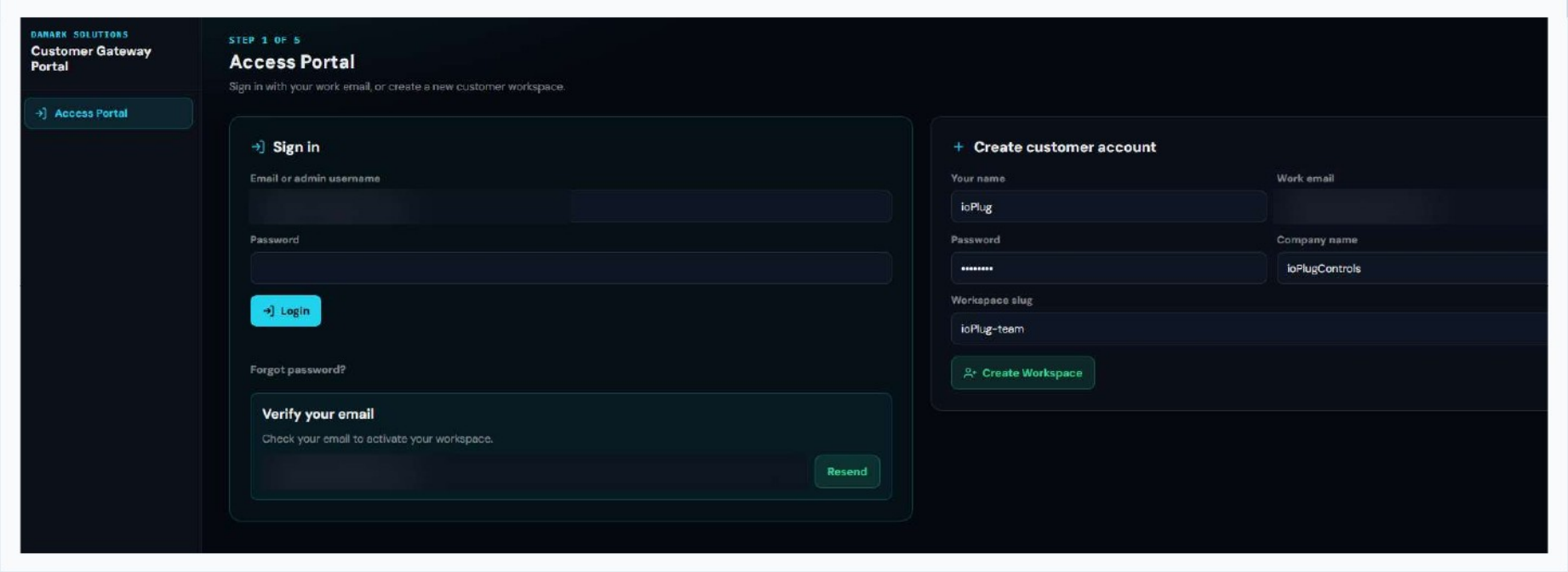

FIGURE 2 — *Workspace created — the Portal prompts for email verification before sign-in.*

Confirm the verification email

Open the Damark Solutions verification email and select Verify email address. The link expires, so this step should be completed promptly.

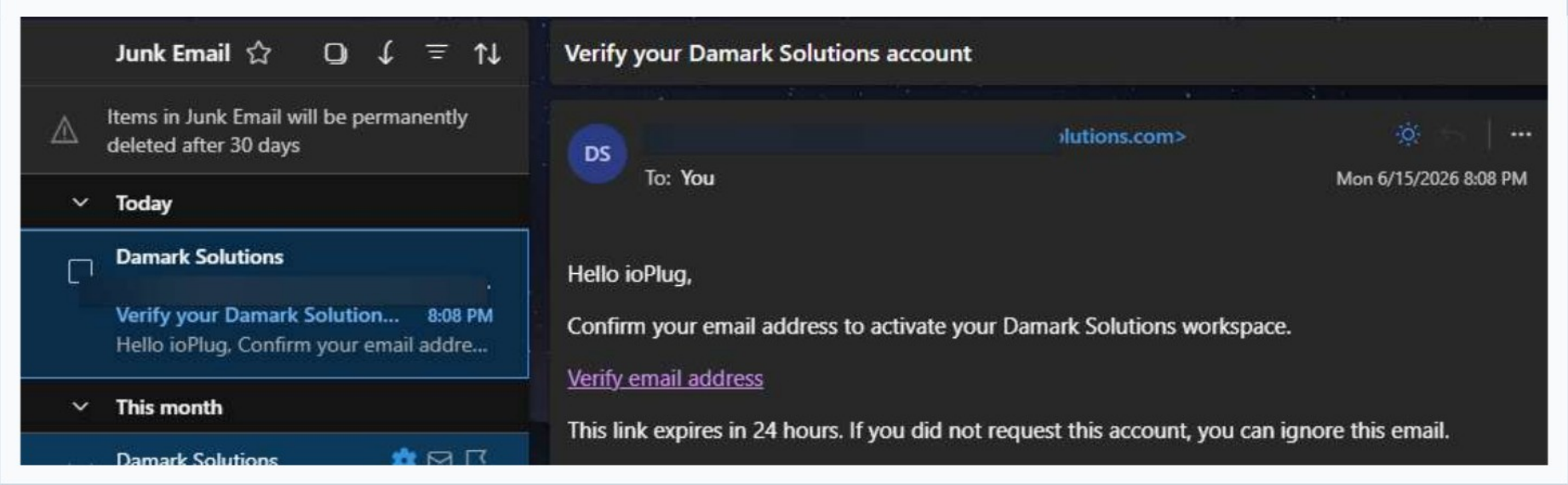

FIGURE 3 — *The verification email from Damark Solutions, with the Verify email address link.*

Email verified

The Portal confirms that the email is verified and the workspace trial is active. The user can now sign in.

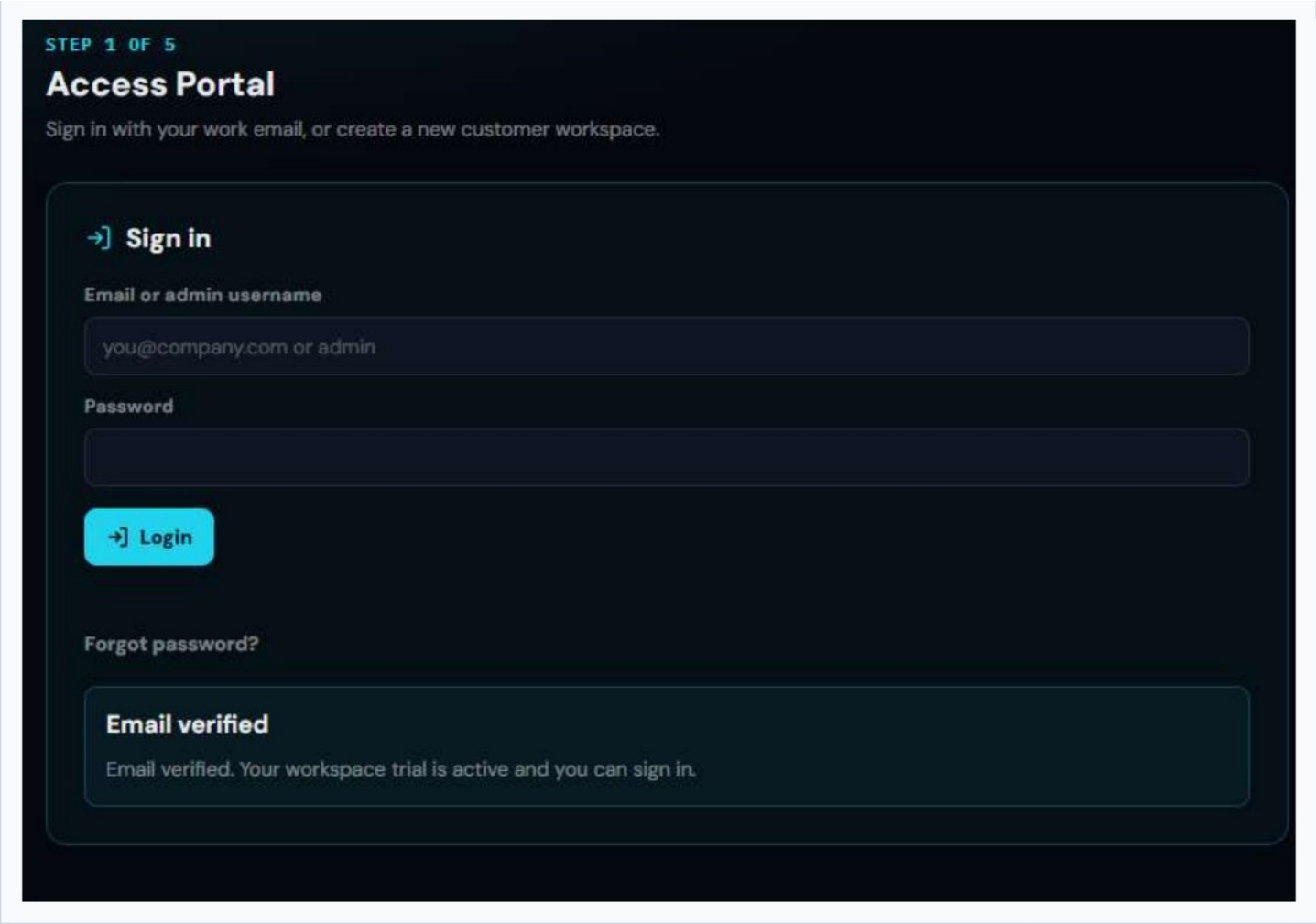

FIGURE 4 — *After verification, the Portal confirms the workspace trial is active.*

Generate a middleware license

Go to Users, choose the workspace user, and generate the middleware license token. This token controls local gateway login and beta access.

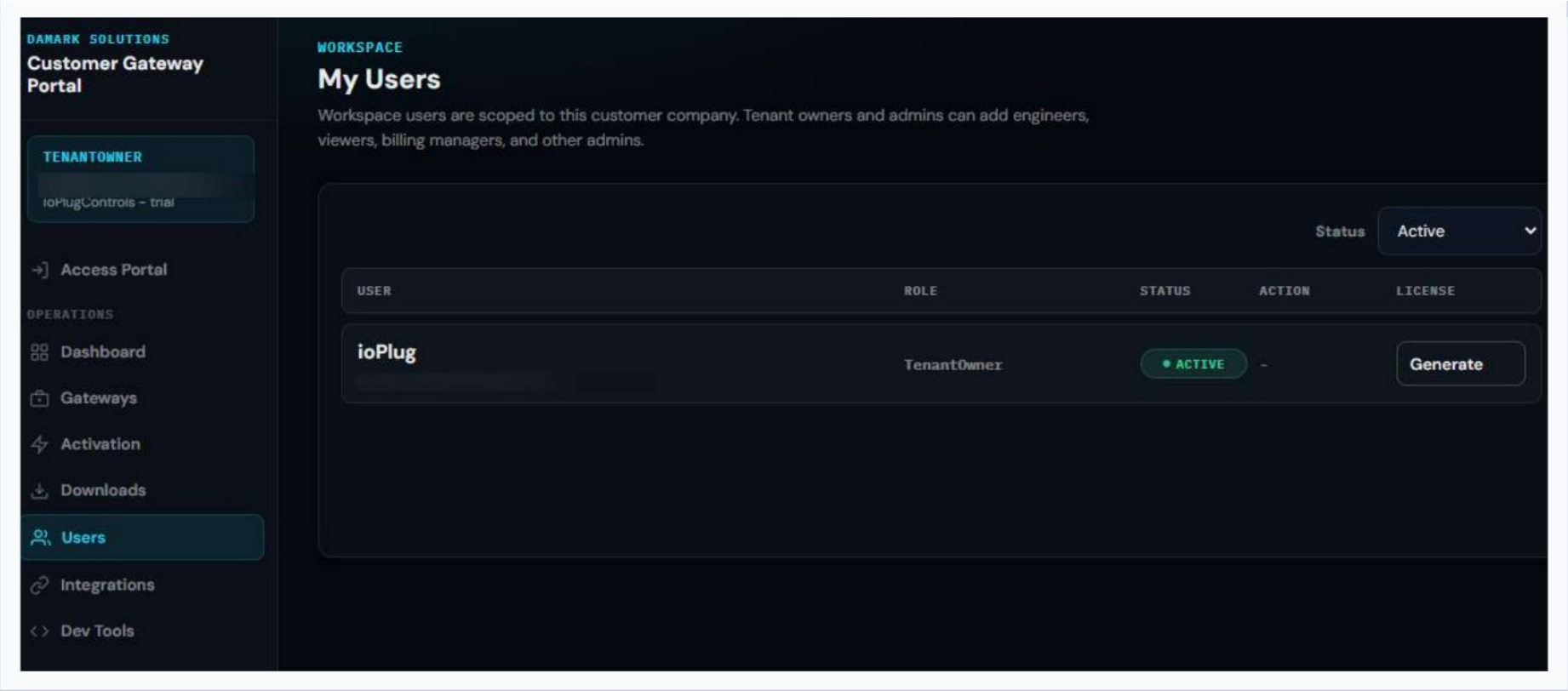

FIGURE 5 — *The Users panel, with Generate queued for the workspace owner's middleware license.*

SECURITY REMINDER — Copy secrets only into the intended local gateway or trusted client. Do not email, screenshot, or publish raw tokens.

Run the local Edge Gateway

Extract the downloaded ZIP package and run `PlcMiddleware.Host`. This starts the local gateway application.

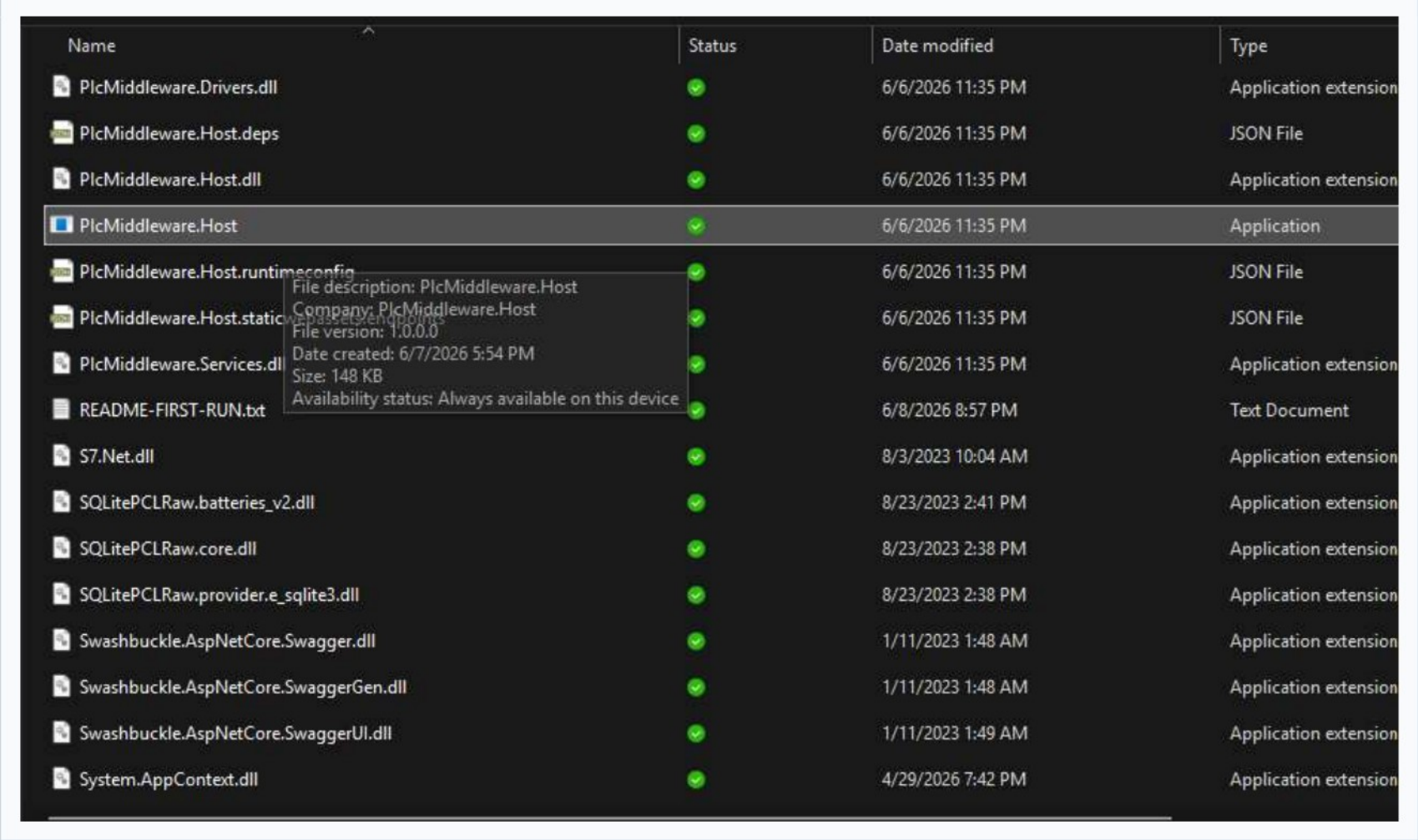

FIGURE 6 — *Windows File Explorer showing the extracted PlcMiddleware.Host package.*

Open the local gateway URL

Open the local gateway in the browser, typically `http://localhost:5000`.

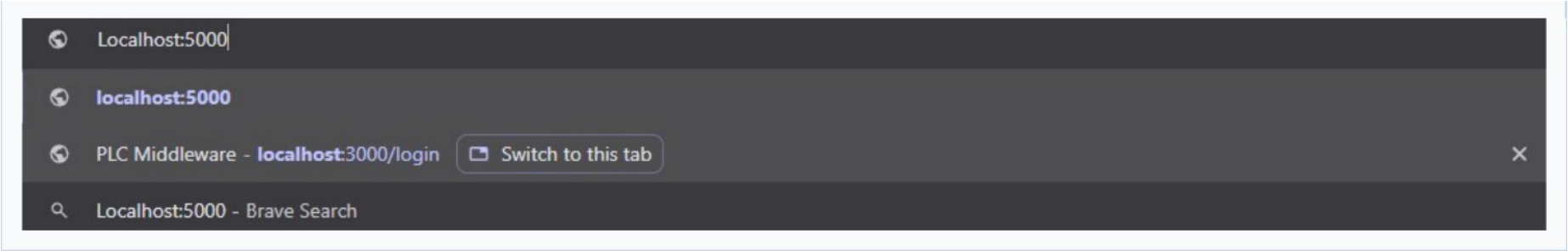

FIGURE 7 — *Opening the local gateway at http://localhost:5000 in the browser.*

Copy the license token

Copy the generated middleware license token from the Portal that starts as `dmg_xxxxx`. It is shown once and should be handled as a secret.

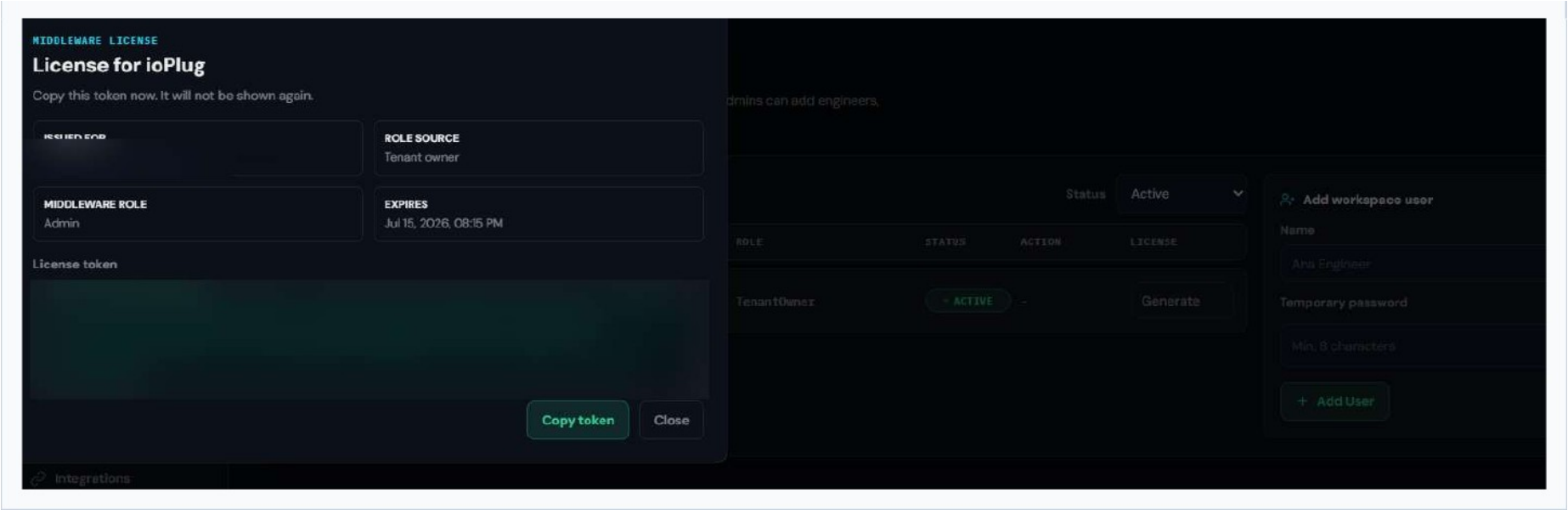

FIGURE 8 — *The one-time middleware license token, ready to copy into the local gateway.*

> **SECURITY REMINDER —** Copy secrets only into the intended local gateway or trusted client. Do not email, screenshot, or publish raw tokens.

Log in with the license

Paste the license token into the local Edge Gateway login page and select Login with License.

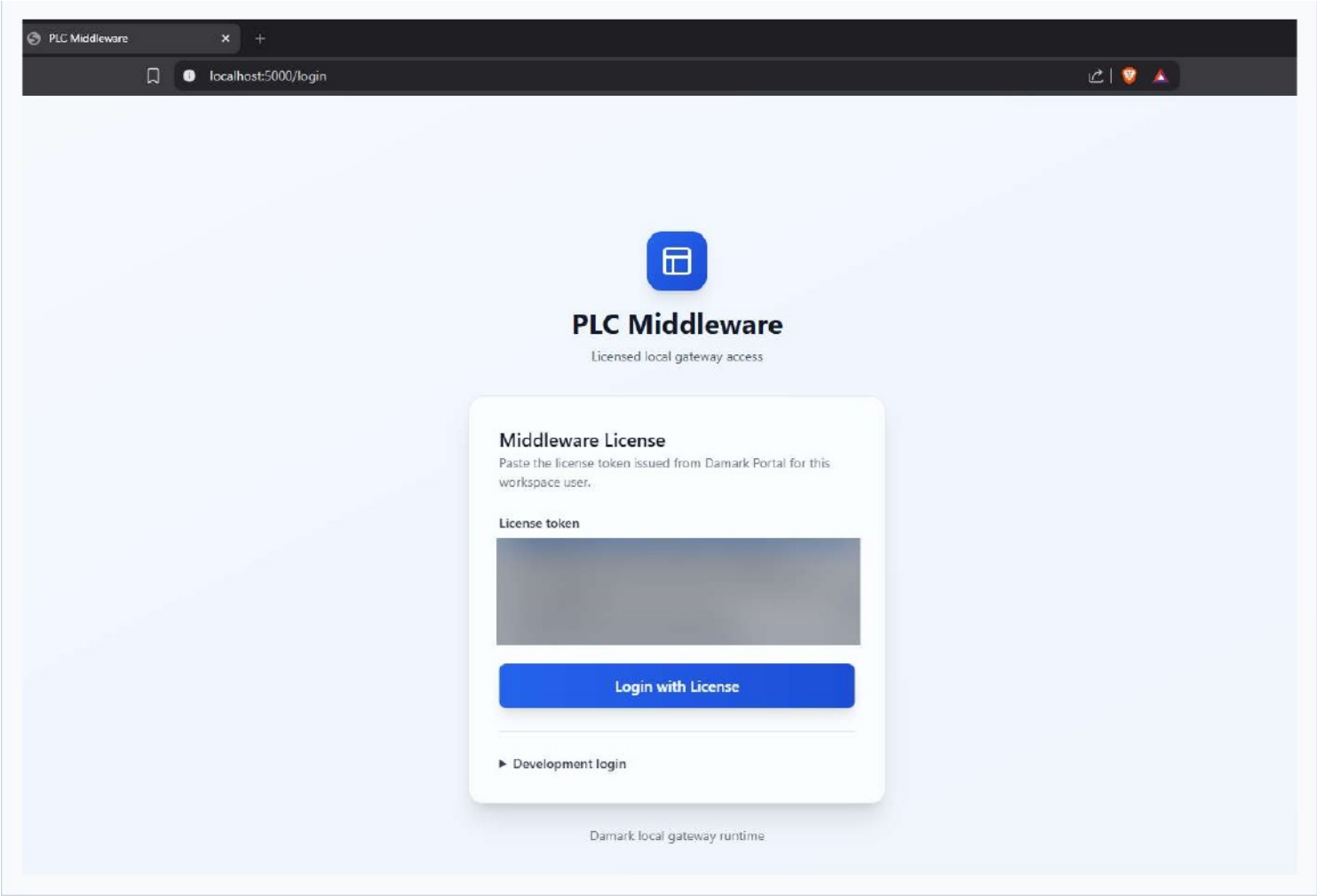

FIGURE 9 — *The local Edge Gateway login screen, ready to accept the license token.*

PHASE 3 · CLOUD REGISTRATION & ACTIVATION

STEP 10 OF 31

Register a cloud gateway record

In the Portal, register the gateway record that the local middleware will bind against.

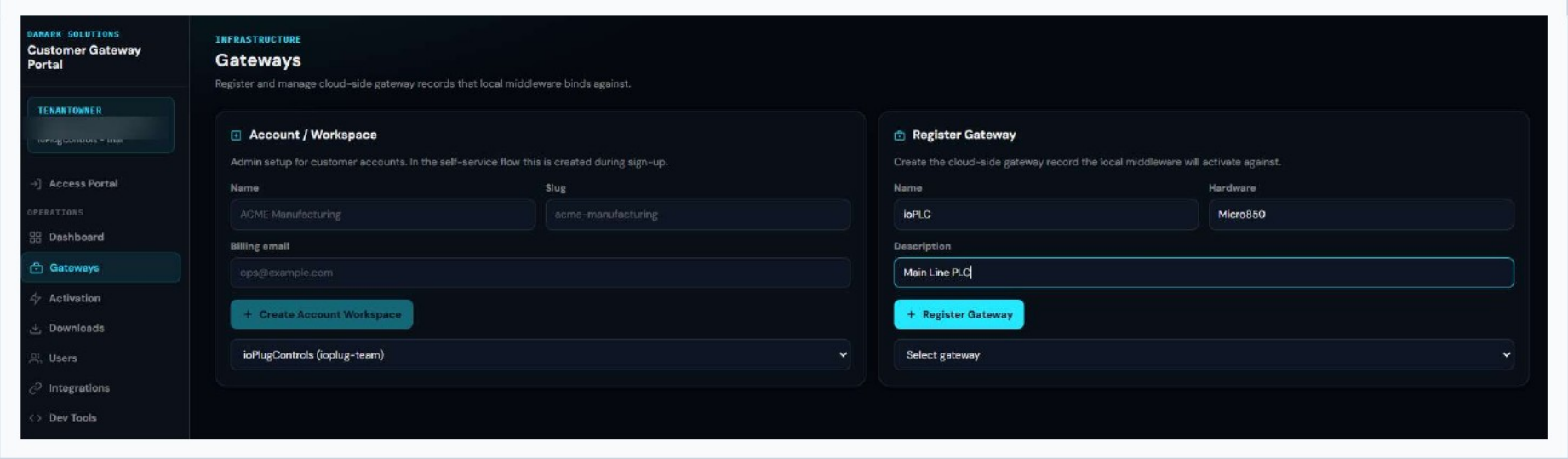

FIGURE 10 — *Registering the cloud-side gateway record that the local middleware will bind against.*

PHASE 3 · CLOUD REGISTRATION & ACTIVATION

STEP 11 OF 31

Review the gateway dashboard

The Portal dashboard shows the gateway in Draft state before activation and synchronization.

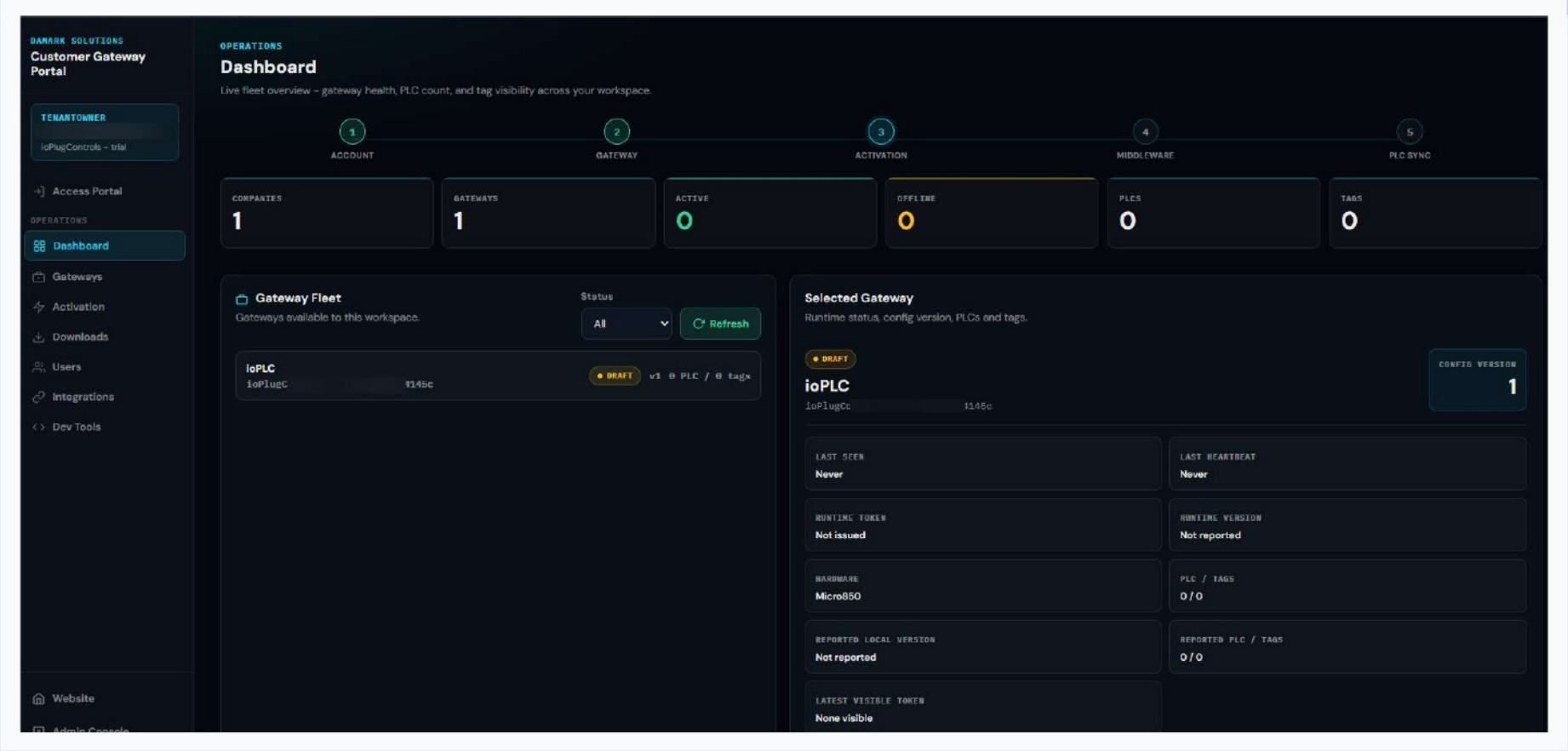

FIGURE 11 — *The Portal dashboard, with the new gateway showing in Draft state.*

Confirm selected gateway status

Use the Selected Gateway panel to inspect gateway details, runtime token status, heartbeat, PLC count, and tag visibility.

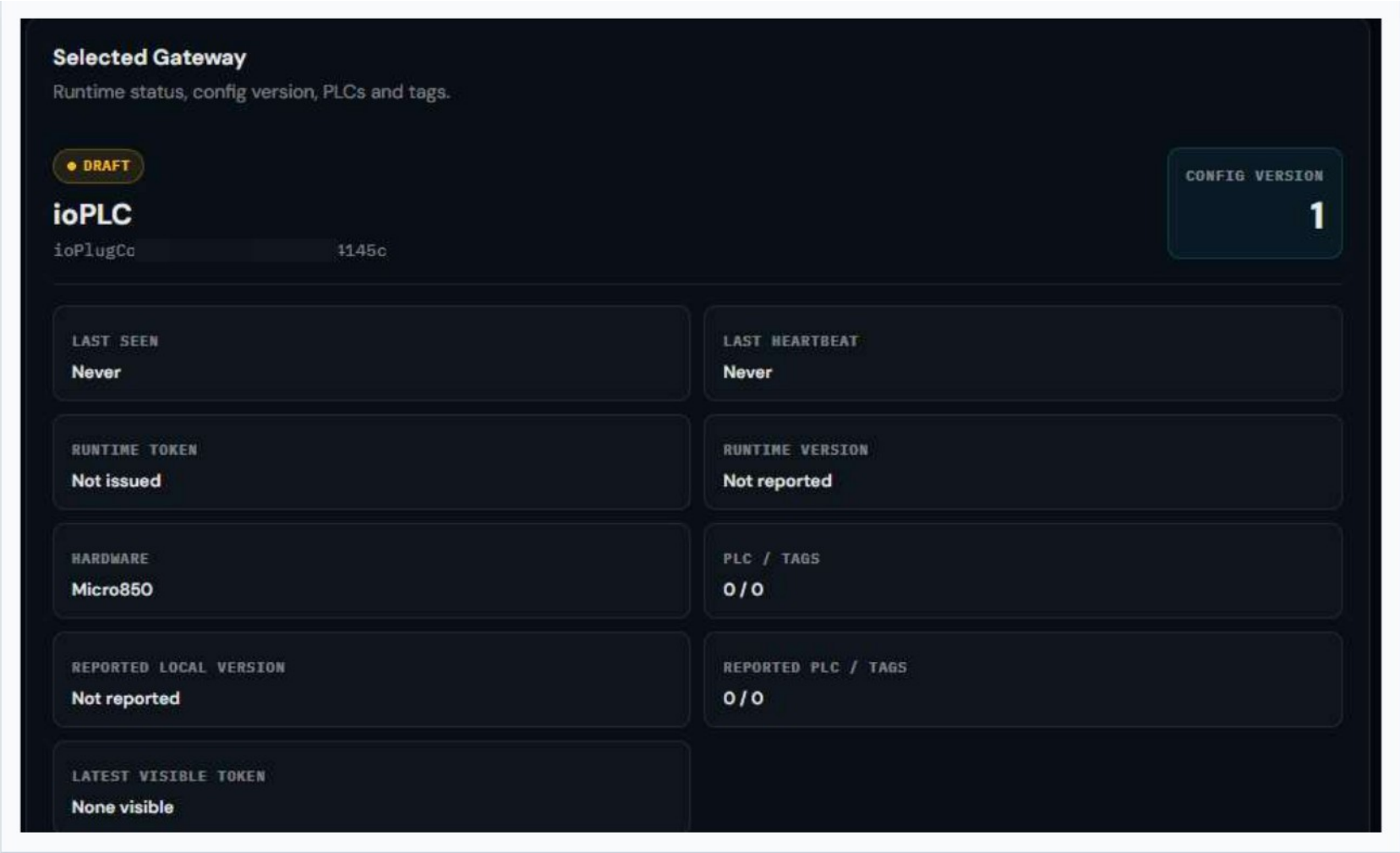

FIGURE 12 — *The Selected Gateway panel — runtime status, heartbeat, and tag counts at a glance.*

Create the activation package

Create an activation package in the Portal. Copy the activation token and config details for the local middleware binding step.

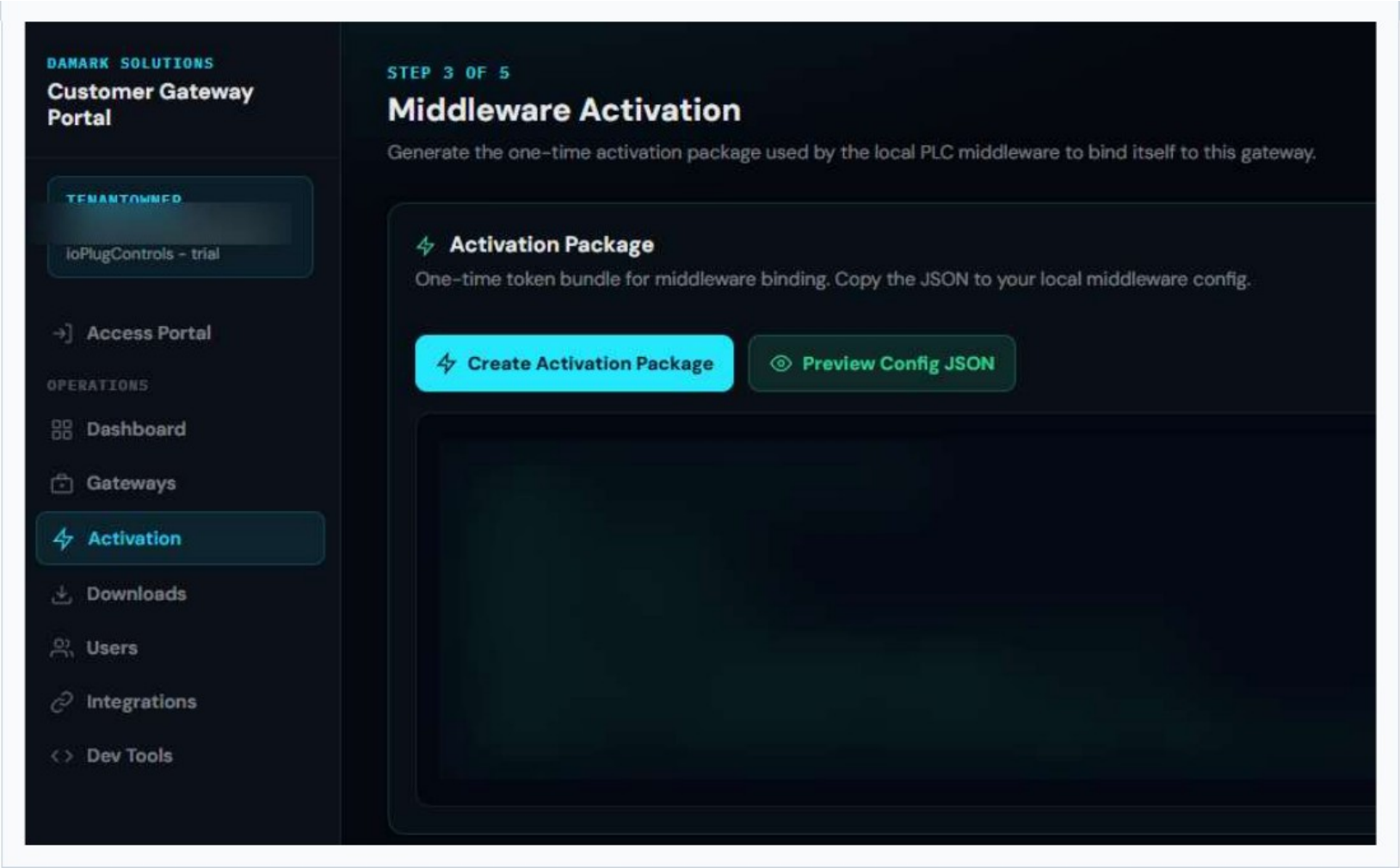

FIGURE 13 — *Generating the one-time activation package for the local middleware.*

SECURITY REMINDER — Copy secrets only into the intended local gateway or trusted client. Do not email, screenshot, or publish raw tokens.

Activate the local gateway

In the local Edge Gateway settings, enter the Portal URL and activation token, then activate the gateway.

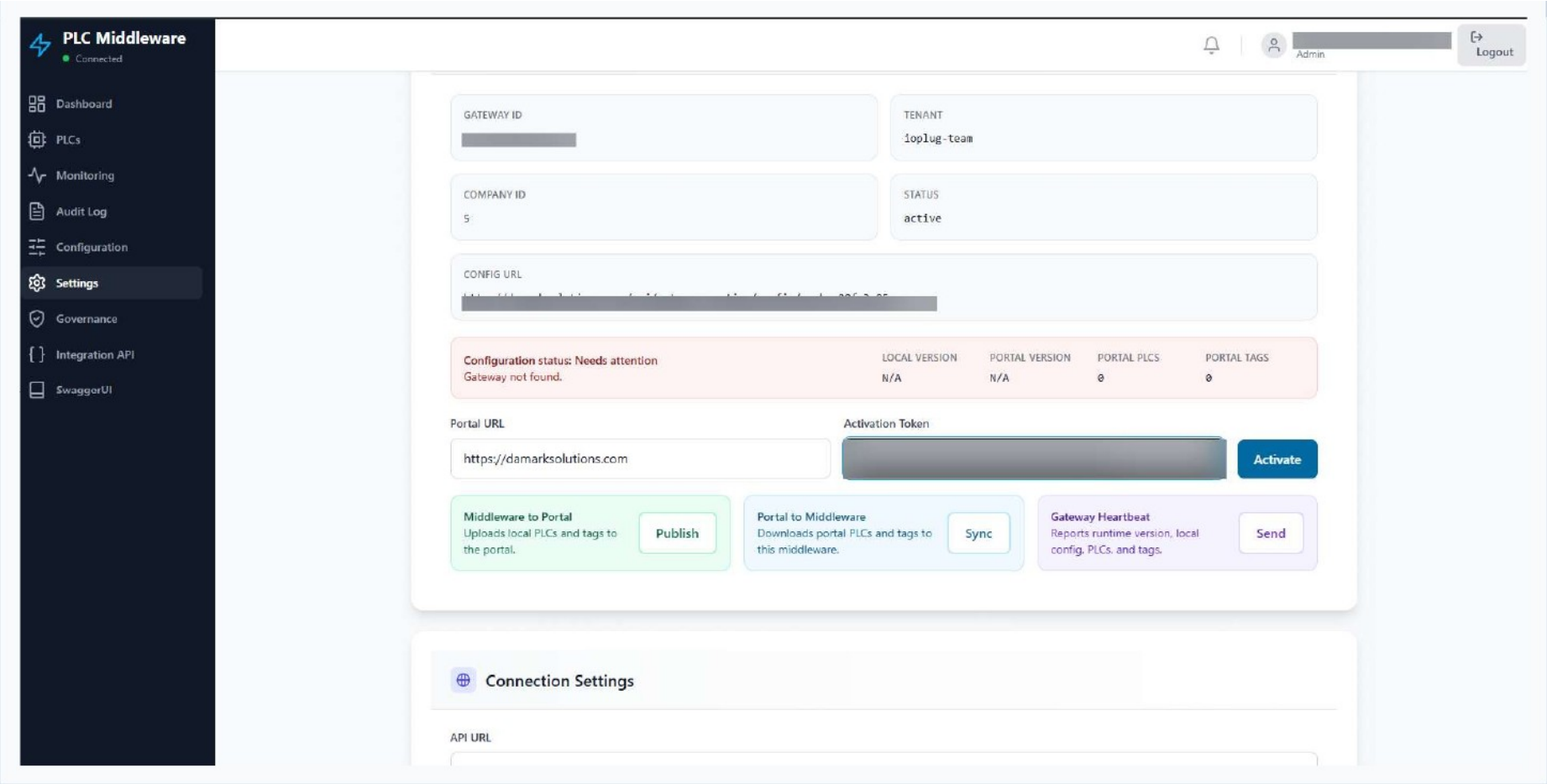

FIGURE 14 — *The local gateway Settings page, ready for the Portal URL and activation token.*

Confirm activation and sync state

After activation, the gateway reports success. If local and portal versions differ, sync first or force publish depending on the intended source of truth.

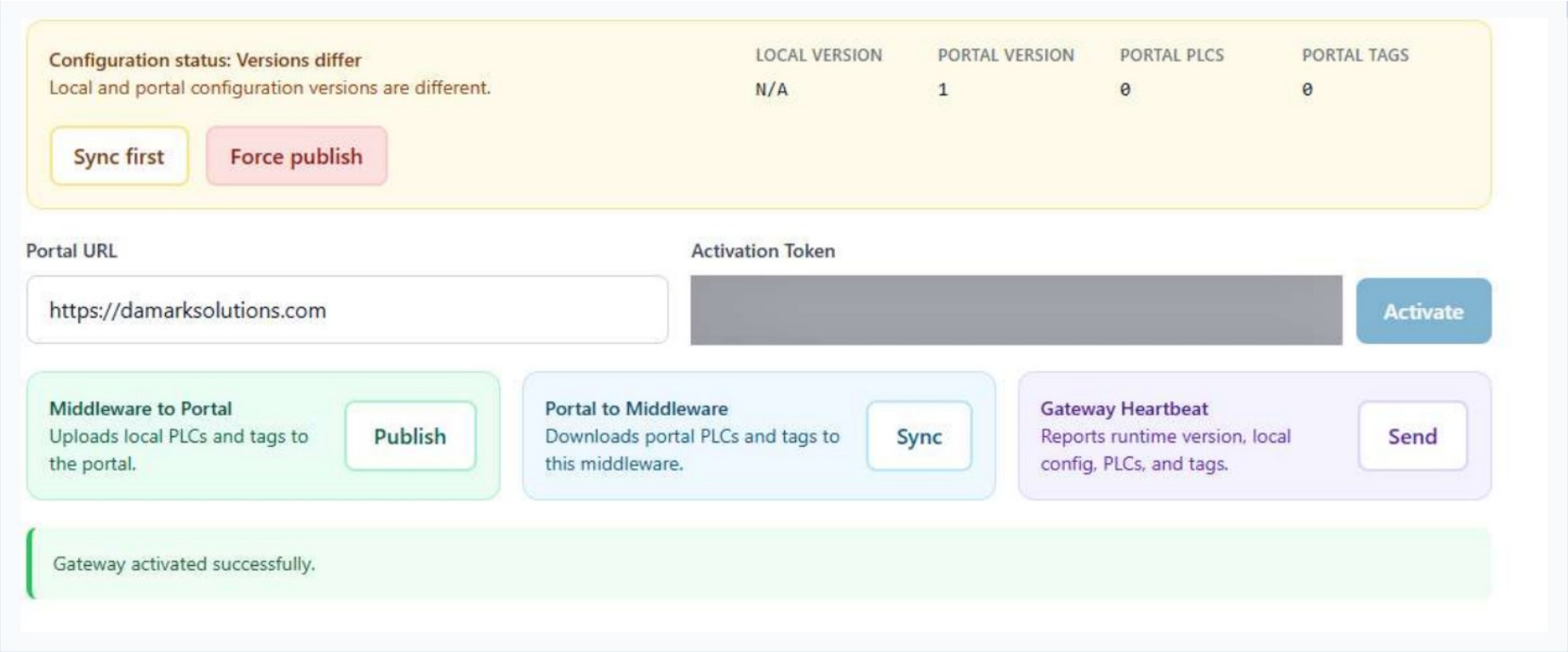

FIGURE 15 — *Activation complete — the gateway reports a successful sync.*

Configure PLCs or BACnet devices

Use the local Configuration page to add, edit, import, validate, and apply PLC and BACnet configuration.

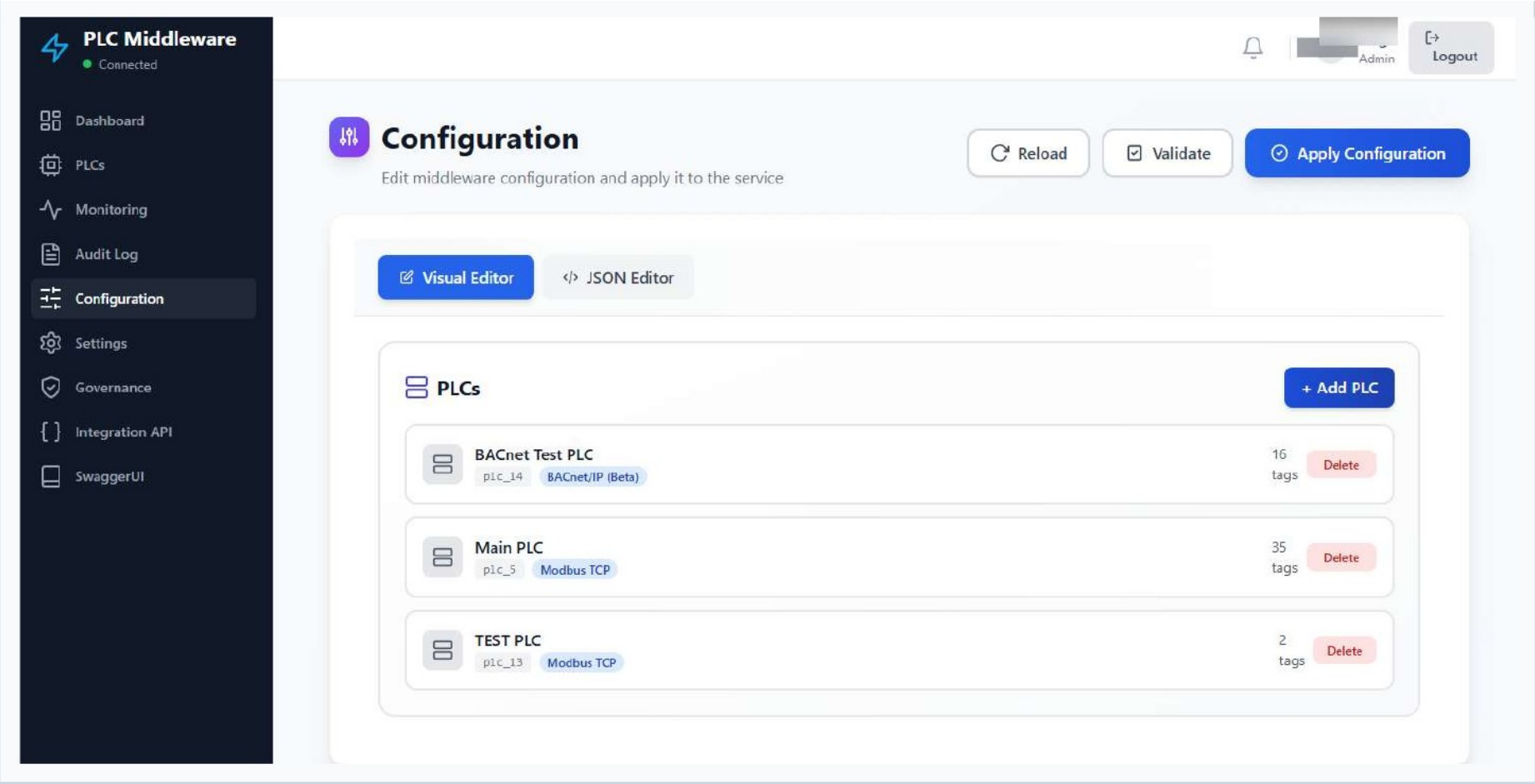

FIGURE 16 — *The Configuration page, listing PLC and BACnet devices bound to this gateway.*

Add a new PLC connection

From Configuration, select Add PLC and choose the protocol. For Modbus TCP, set the IP address, port, and timeout for the target controller.

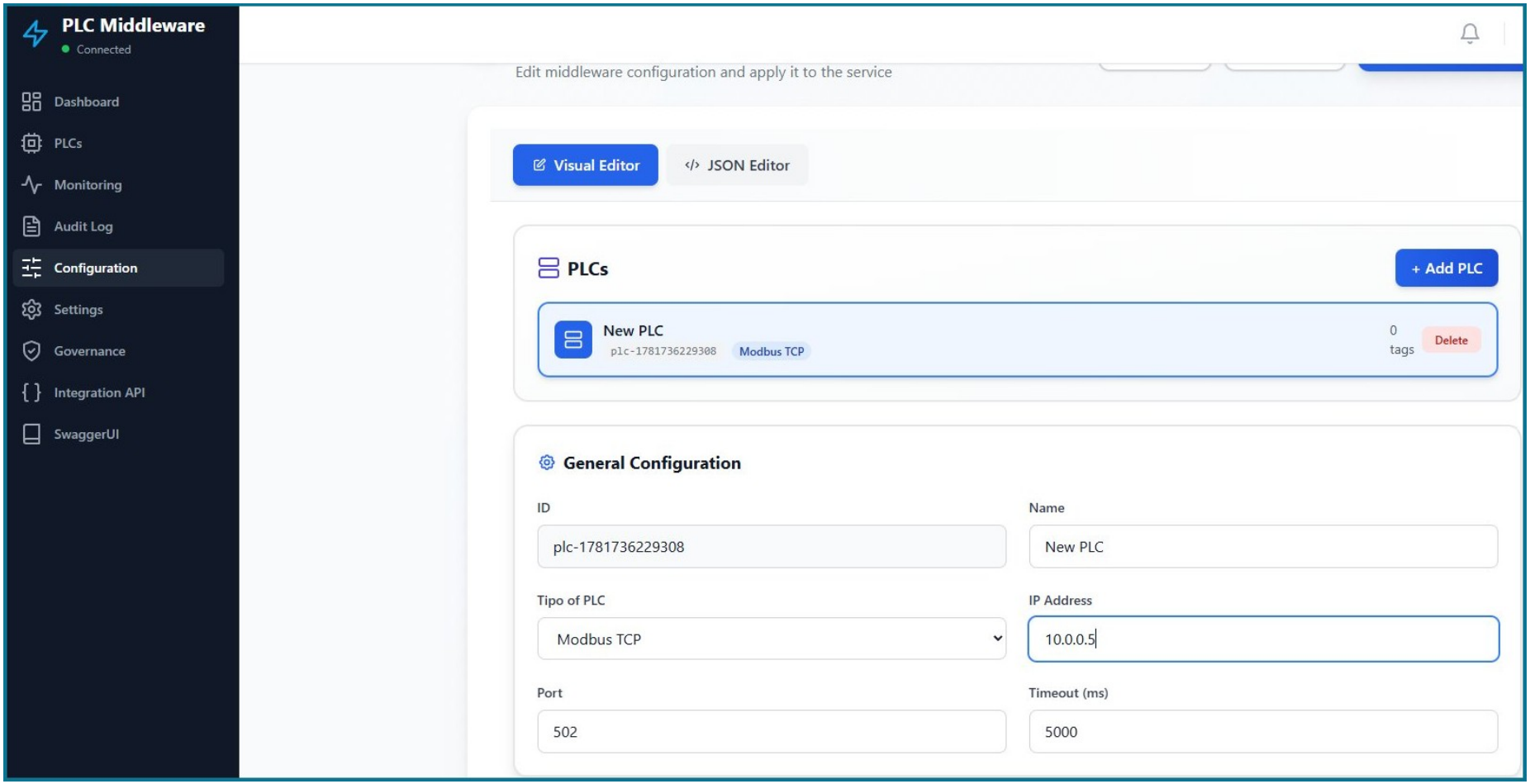

FIGURE 17 — *Adding a new Modbus TCP PLC connection, with IP address, port, and timeout.*

Import tags from CSV, JSON, or controller exports

Open Import Tags and paste CSV, JSON, CCW Modbus XML, TwinCAT XML, or BACnet EDE data. The Supported fields panel lists the required and optional columns, including governance and rate-limit fields.

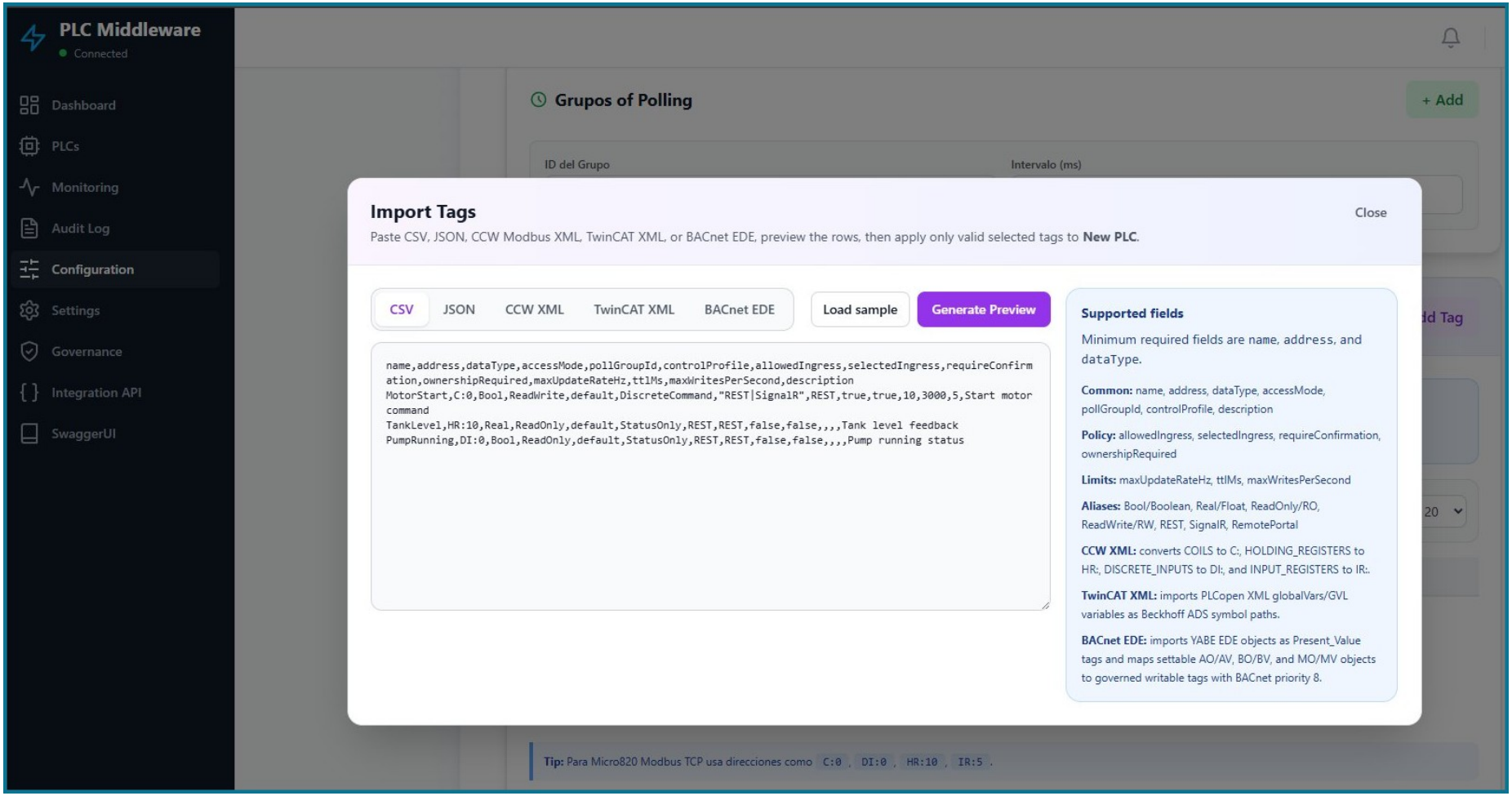

FIGURE 18 — *The Import Tags dialog, with a CSV sample and the supported-fields reference.*

Preview and select tags to apply

Generate Preview parses the pasted data and reports how many rows are valid. Review each row, adjust fields if needed, then choose which rows to apply to this PLC.

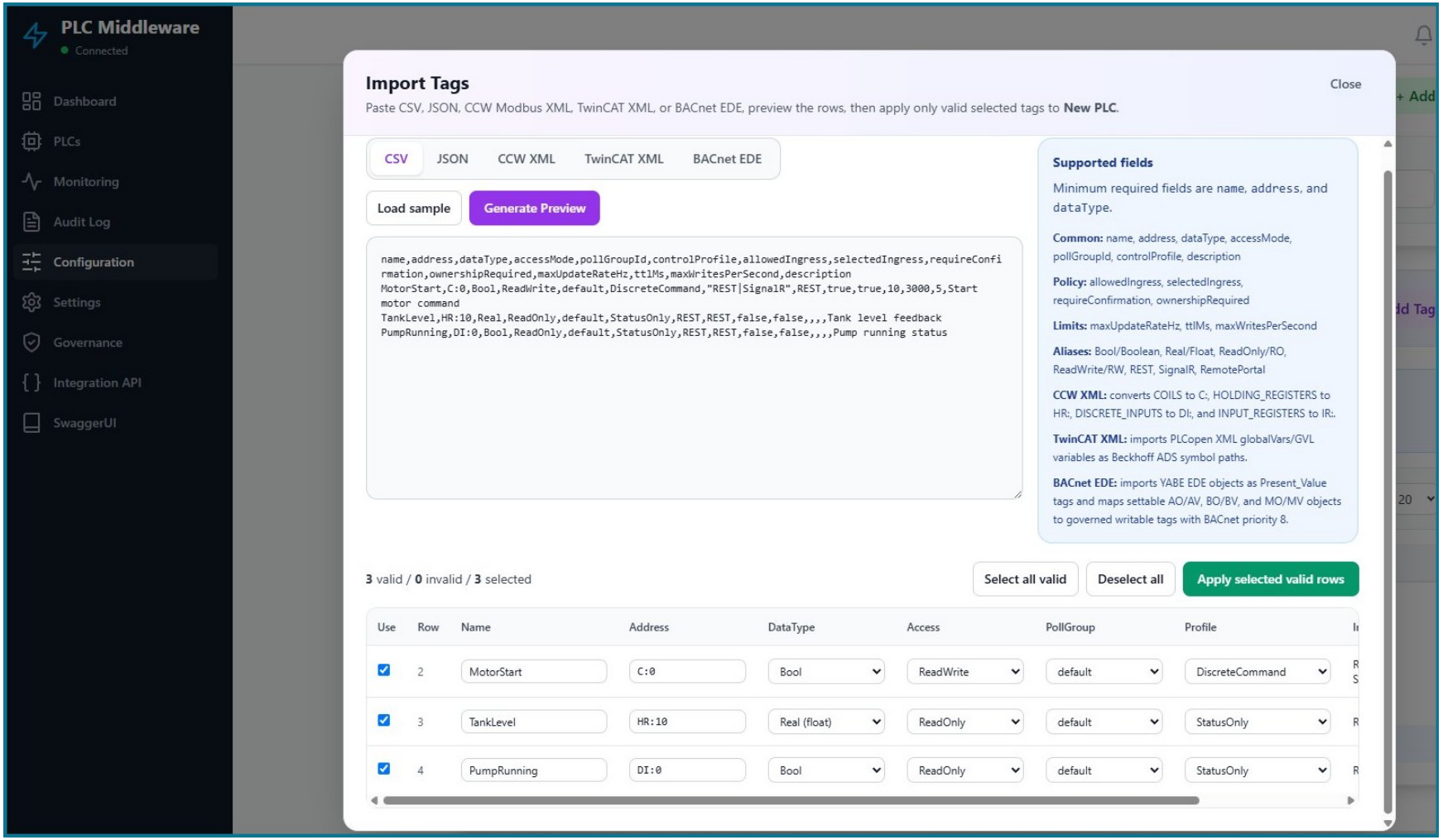

FIGURE 19 — *The import preview — three valid rows ready to apply to New PLC.*

Configure per-tag access and write policy

Each tag carries its own access mode, allowed ingress (REST, SignalR, or Remote Portal), confirmation and ownership requirements, and write-rate limits. The address guide clarifies Modbus coil, register, and reference-number conventions.

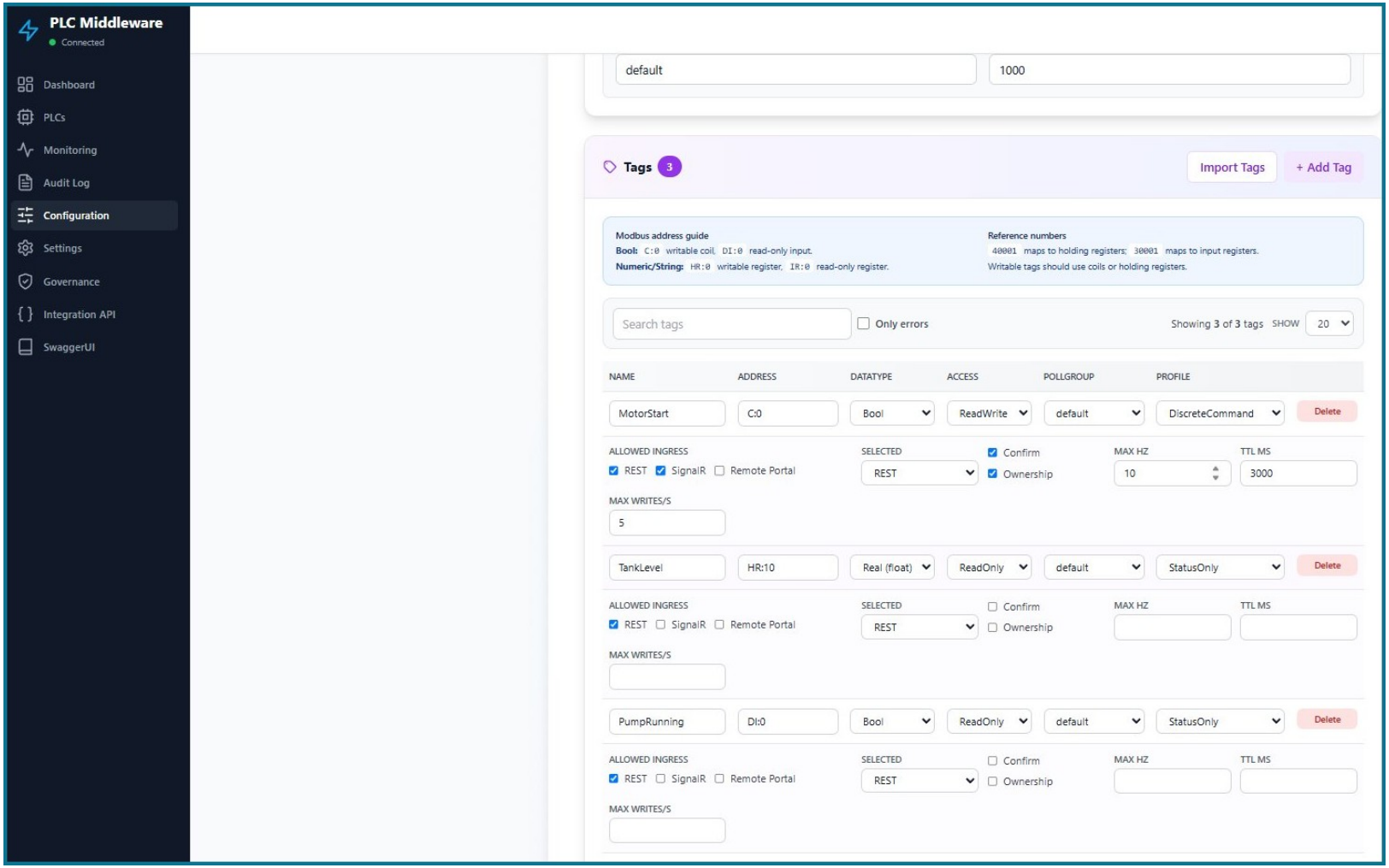

FIGURE 20 — *Tag-level governance fields — access mode, ingress, confirmation, ownership, and write-rate limits.*

Validate and apply the configuration

Validate checks the configuration before Apply Configuration pushes it live to the running service. The PLC list immediately reflects the new tag count.

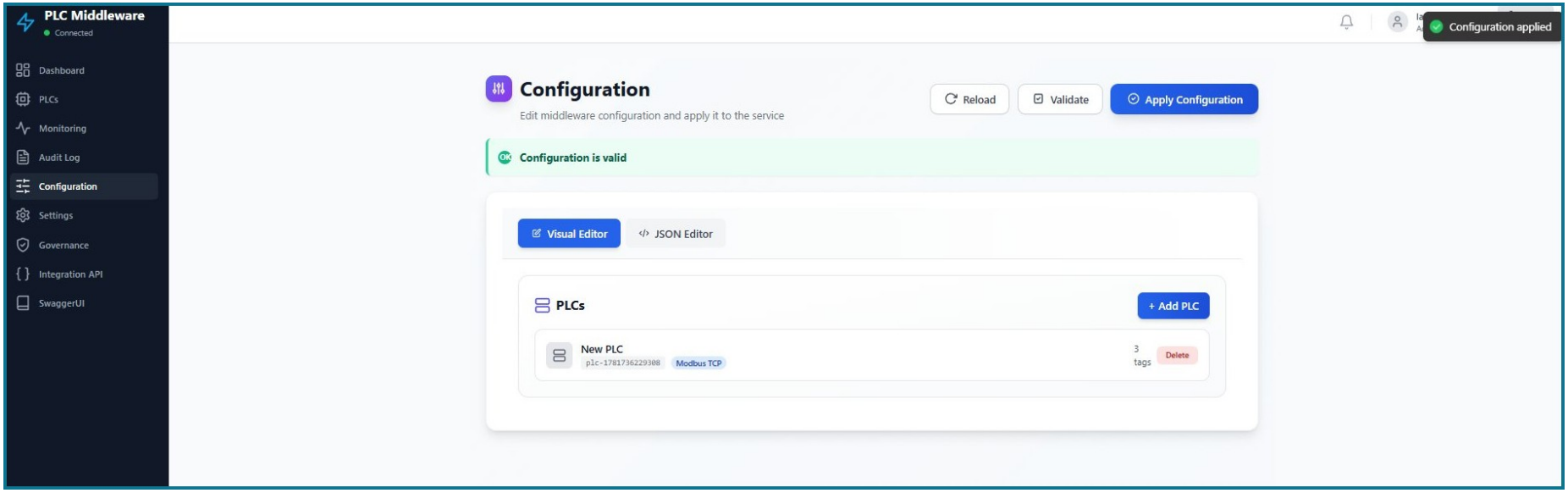

FIGURE 21 — *Configuration applied — New PLC now reports three tags.*

Monitor live PLC connection status

The PLCs page shows real-time connection state, address, tag and poll-group counts, and last-connection time for each configured device, with Test and Reconnect actions.

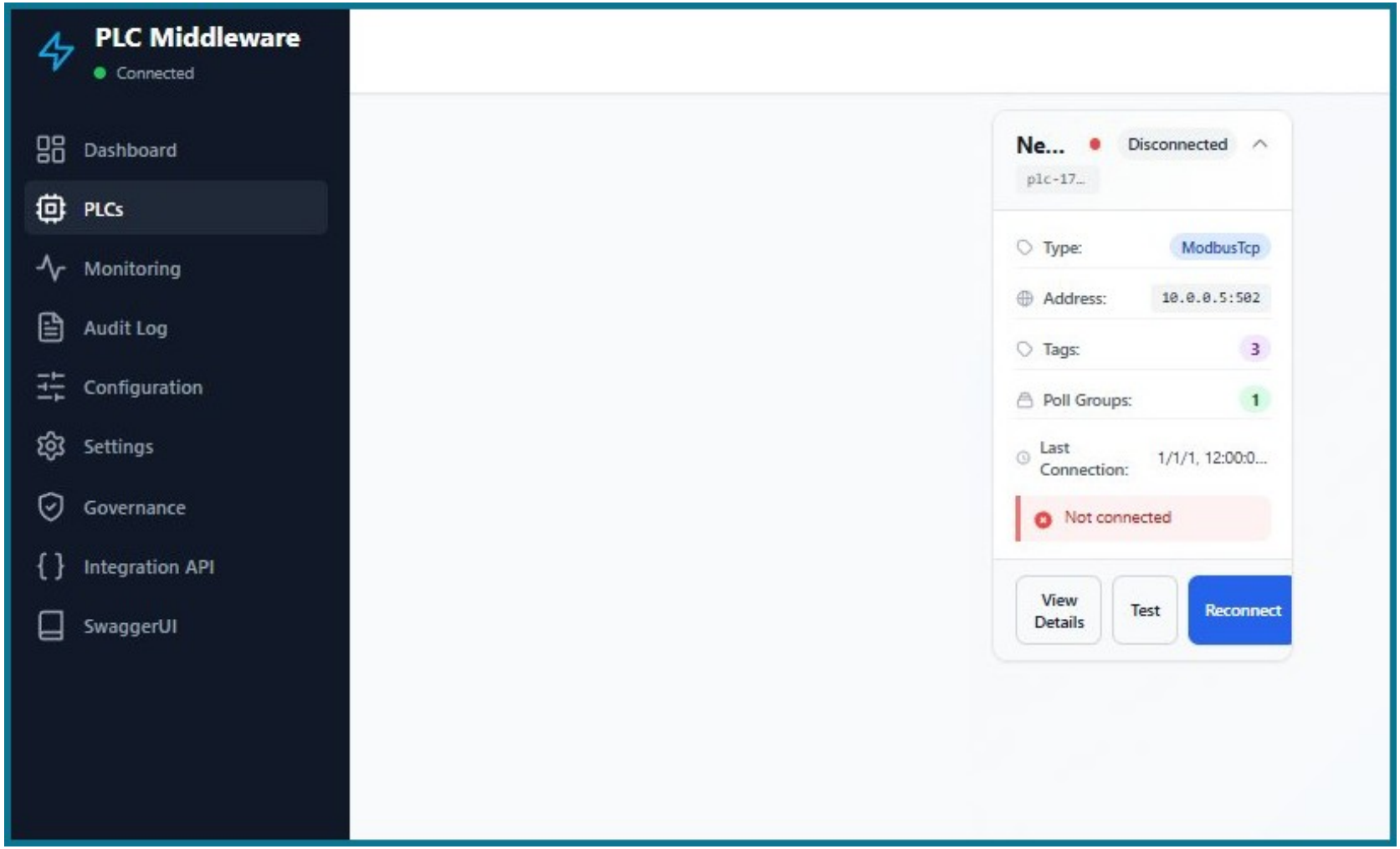

FIGURE 22 — *A PLC card showing a disconnected Modbus TCP device, ready to reconnect.*

Review the fleet dashboard

The Dashboard summarizes total, connected, and disconnected PLCs and tags across the gateway, and streams recent telemetry for the PLCs selected for display.

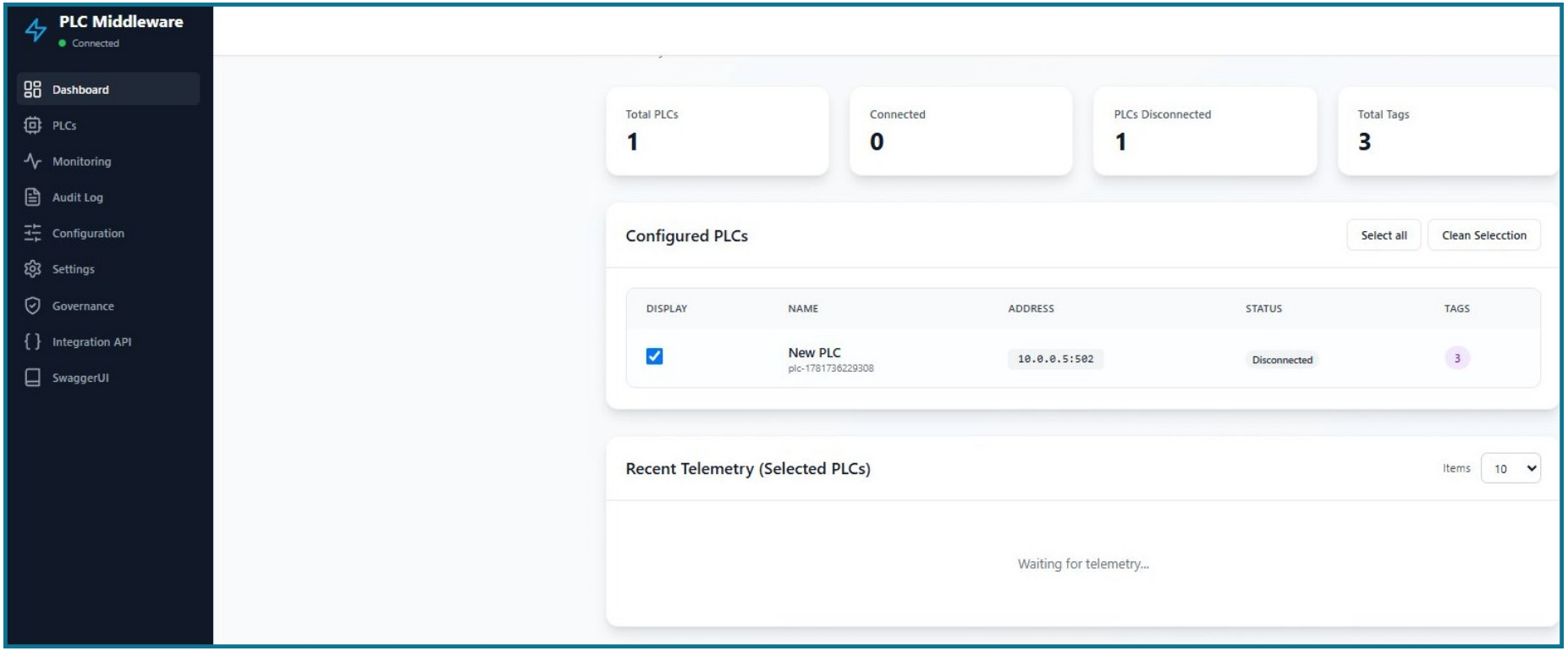

FIGURE 23 — *The Dashboard — fleet summary counters and the Recent Telemetry panel.*

Test writes from the Command Console

The Command Console lets an operator exercise a tag write over REST or SignalR before any external client does, with the exact payload — including the idempotency key — shown for review.

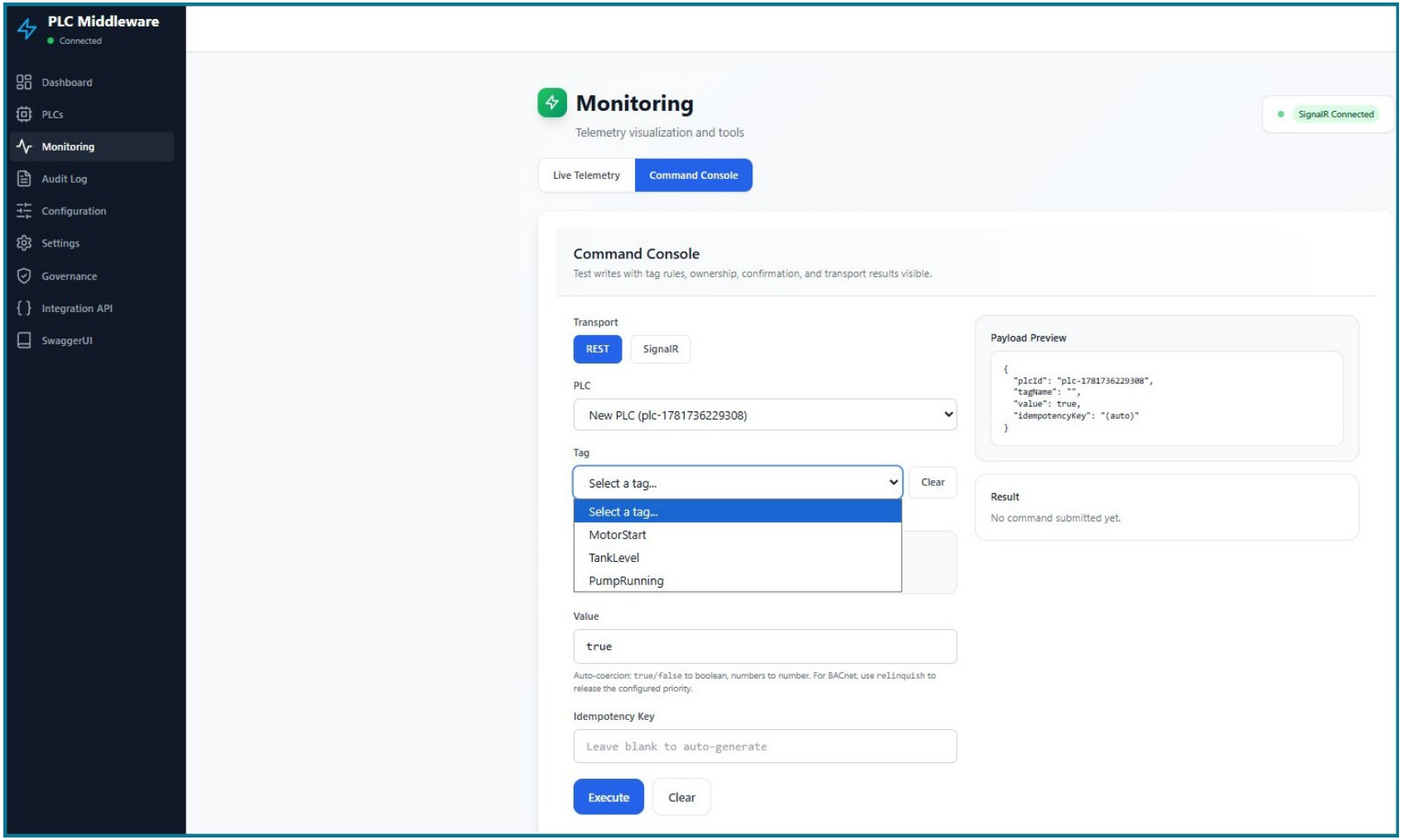

FIGURE 24 — *The Command Console, with a write queued for the MotorStart tag.*

OPERATIONAL REMINDER — Commands sent from the Console reach the real PLC if connected. Use a non-production controller or a safe test tag.

Review the command audit log

Every write — from the Command Console, REST, or SignalR — is recorded in the Audit Log with outcome and timing, and can be filtered by PLC, tag, status, or date range.

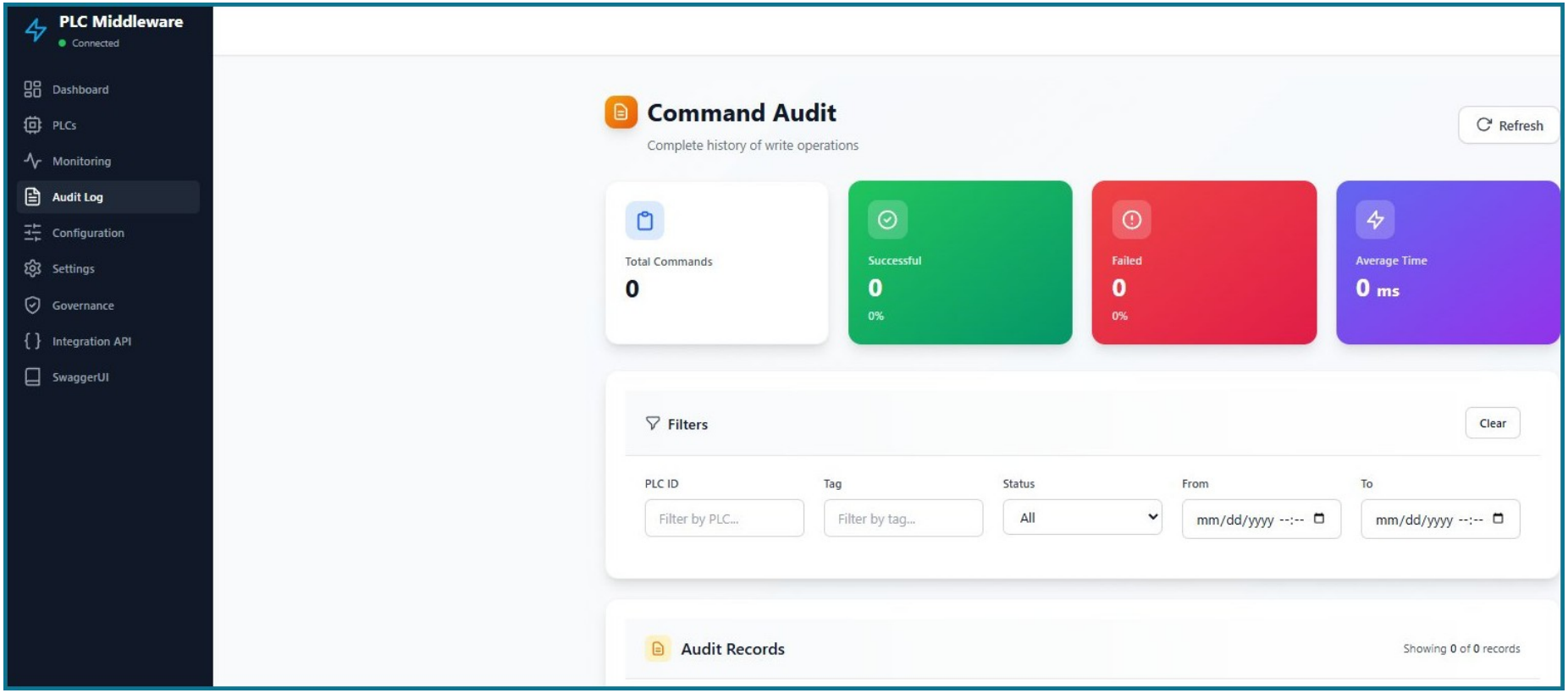

FIGURE 25 — *The Command Audit view, with success-rate and timing summaries and filterable records.*

Configure governance policies

Governance defines what each tag may do over REST versus SignalR, applies reusable safety templates, controls which client integrations may write, and manages ownership leases so two clients cannot fight over the same actuator.

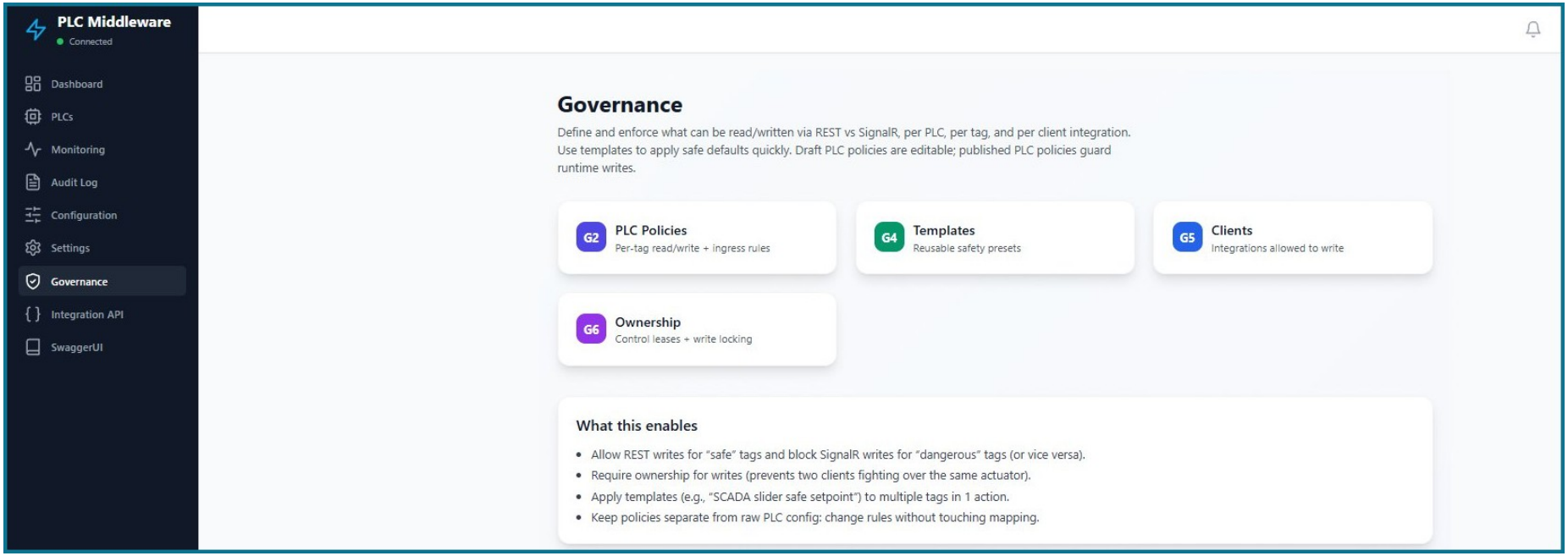

FIGURE 26 — *The Governance landing page — policies, templates, clients, and ownership.*

Set up the Integration API for external clients

The Integration API is the entry point for an external SCADA, HMI, or script. A client key passes four checks — client state, read/write scope, governance policy, and ownership or rate limits — before any read or write reaches a PLC.

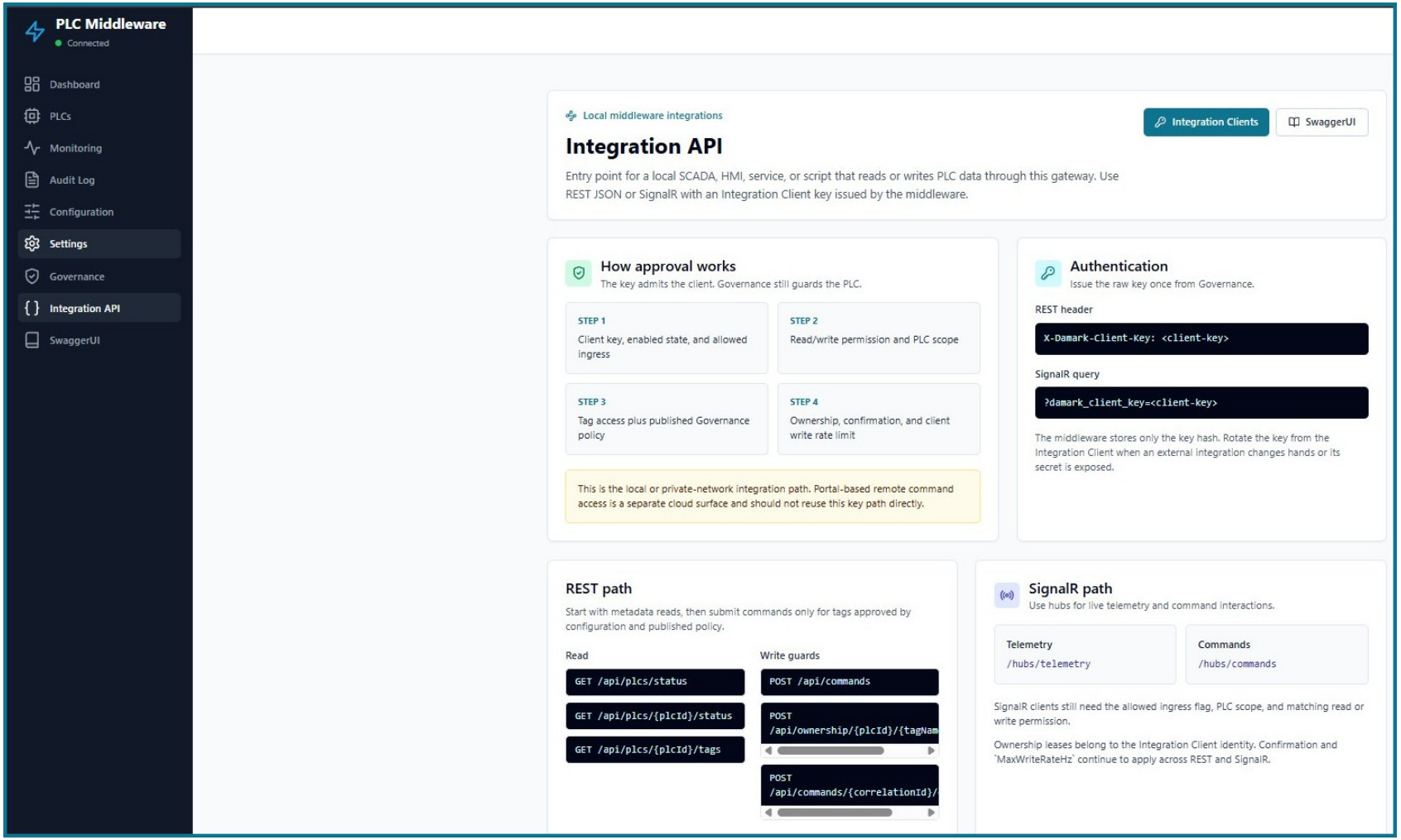

FIGURE 27 — *The Integration API reference — approval steps, authentication headers, and REST/SignalR paths.*

Explore the full API reference in SwaggerUI

SwaggerUI documents every endpoint exposed by the local gateway, grouped by area, and lets a developer authorize and try requests directly from the browser.

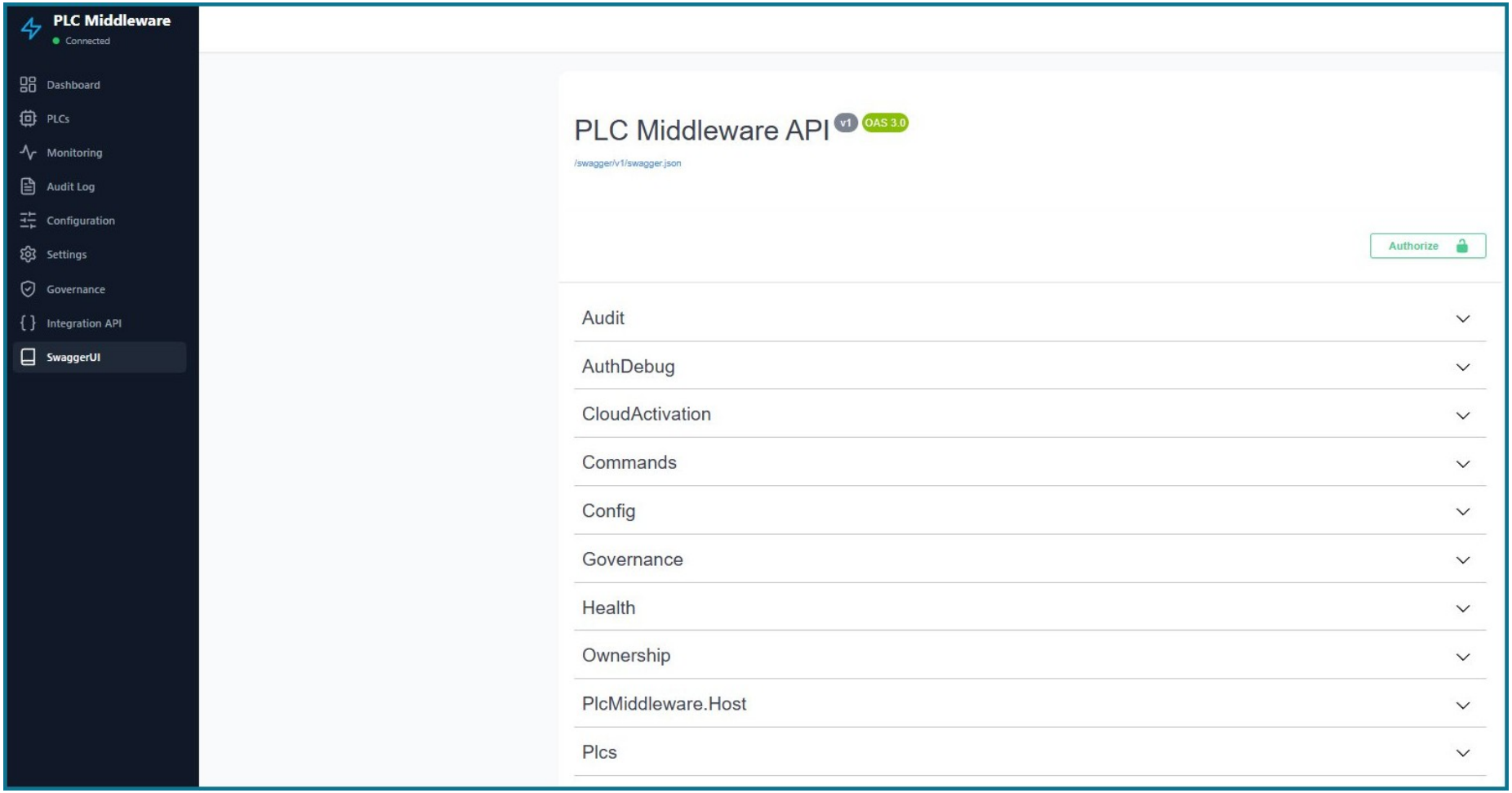

FIGURE 28 — *SwaggerUI — the local gateway's interactive API reference.*

Create a Remote Integration Client

In Portal Integrations, create a remote client, select the acting workspace user, enable the required access, and scope it to the gateway.

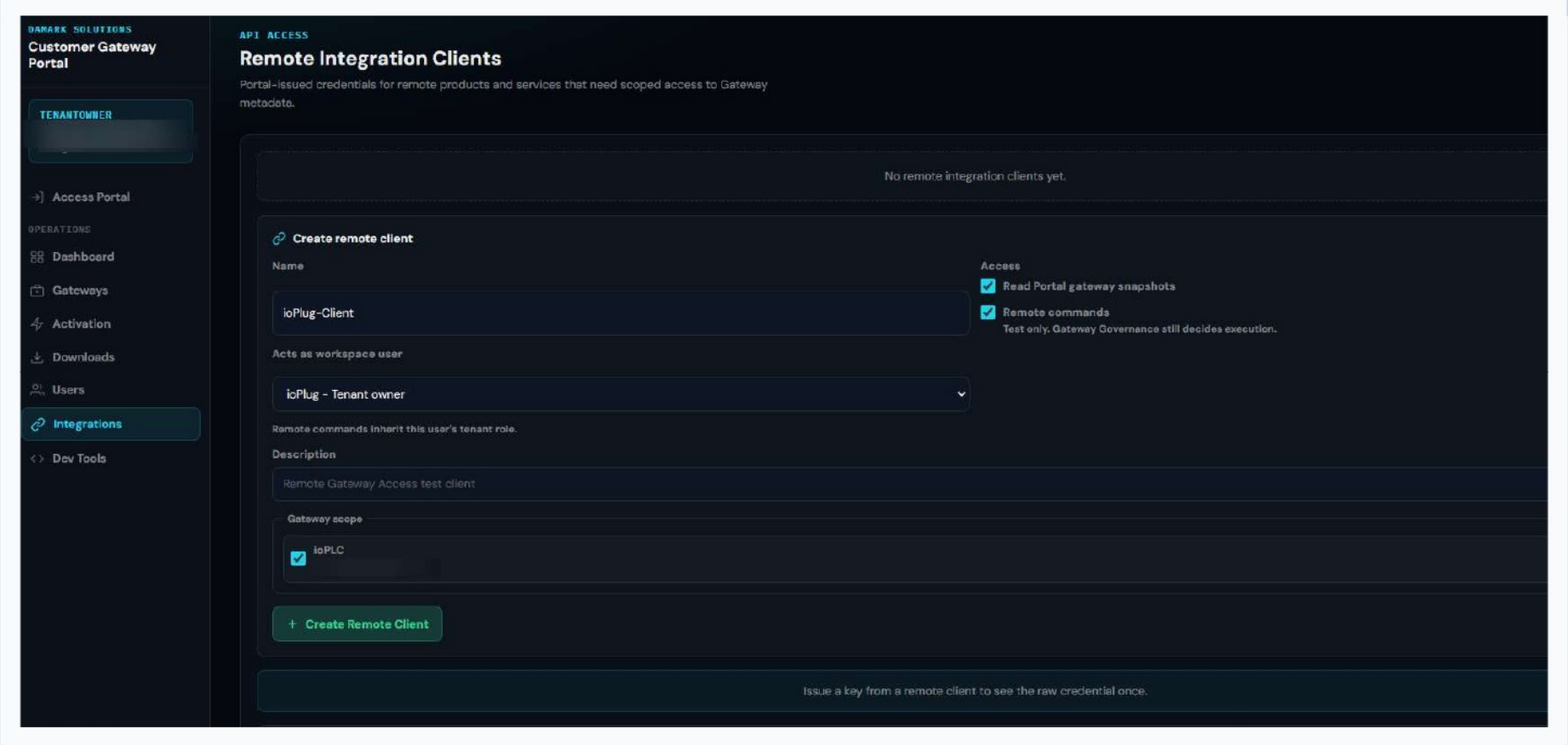

FIGURE 29 — *Creating a Remote Integration Client scoped to the ioPLC gateway.*

Issue the remote key

Issue a key for the Remote Integration Client. This key is used by external SCADA, HMI, and dashboard clients to connect through the Portal.

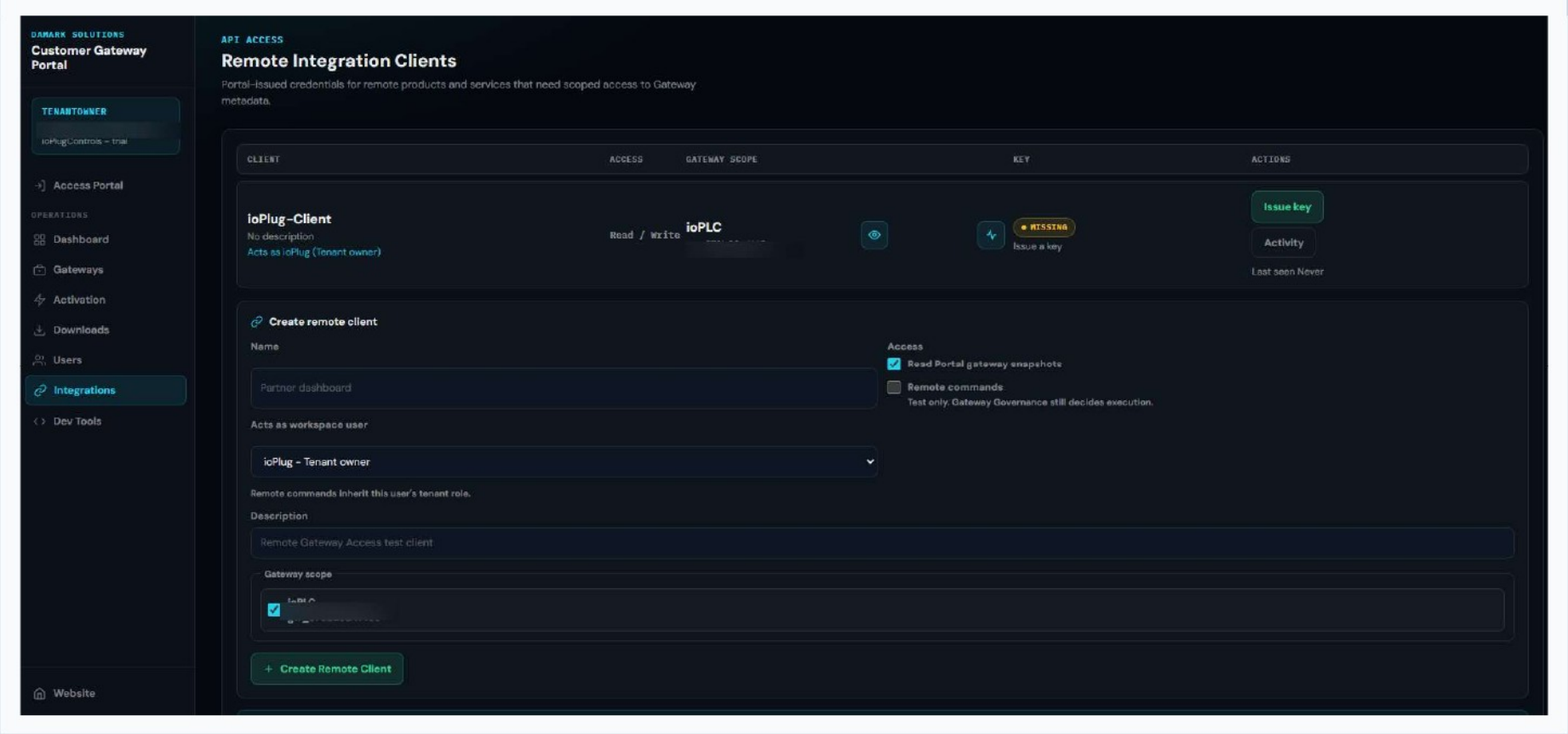

FIGURE 30 — *The Remote Integration Client, ready to issue its first access key.*

Store the remote client key securely

Copy the remote client key immediately. It is shown once, can be rotated or revoked, and should not be exposed publicly.

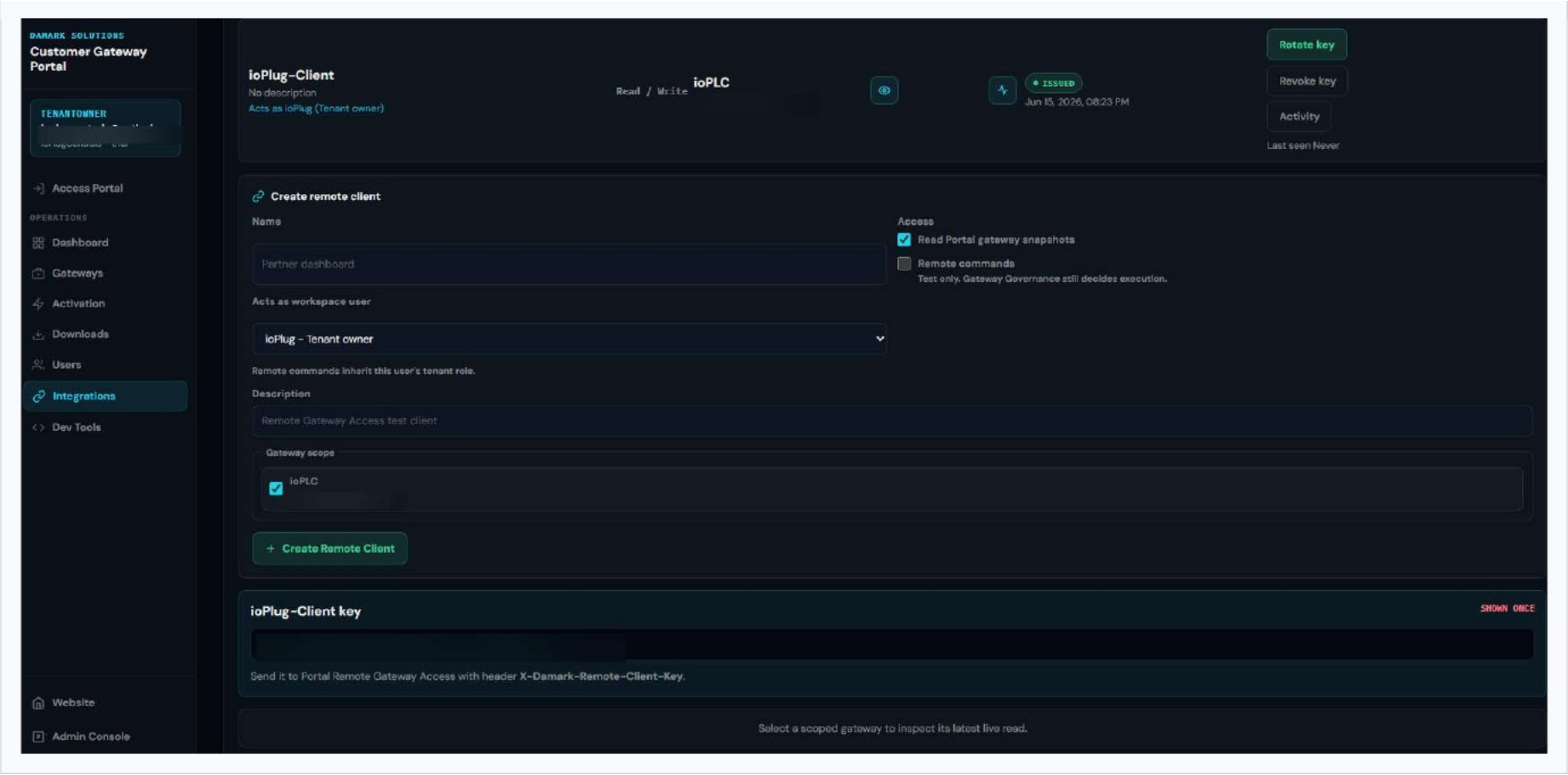

FIGURE 31 — *The one-time remote client key, shown once and ready to be stored securely.*

SECURITY REMINDER — Copy secrets only into the intended local gateway or trusted client. Do not email, screenshot, or publish raw tokens.

BEFORE YOU HAND OFF

Operational checklist

Confirm each item below before considering the onboarding complete or sharing this procedure outside the internal beta team.

PHASE 1 · WORKSPACE & EMAIL VERIFICATION

- ☐ Customer account is created and email is verified.

PHASE 2 · LICENSING & LOCAL GATEWAY

- ☐ Workspace user has an issued middleware license token.
- ☐ Local Edge Gateway starts and accepts the license token.

PHASE 3 · CLOUD REGISTRATION & ACTIVATION

- ☐ Cloud gateway record exists in the Portal.
- ☐ Activation package is generated and applied locally.
- ☐ Gateway activation succeeds and heartbeat/sync can be sent.

PHASE 4 · DEVICE CONFIGURATION & LOCAL CONSOLE

- ☐ PLC or BACnet configuration is validated and applied locally.
- ☐ Tags are imported or added with the correct address and data type.
- ☐ Tag-level access, ingress, and write-rate policies are reviewed.
- ☐ PLC connection status is confirmed from the PLCs view.
- ☐ Dashboard fleet summary and telemetry are reviewed.
- ☐ A test write is exercised and confirmed from the Command Console.
- ☐ The audit log reflects the test write.
- ☐ Governance policies (templates, clients, ownership) are configured as needed.
- ☐ Integration API authentication and endpoints are understood (REST, SignalR, SwaggerUI).

PHASE 5 · REMOTE INTEGRATION

- ☐ Remote Integration Client is scoped to the intended gateway.
- ☐ Remote key is issued, copied once, and stored securely.
- ☐ Screenshots are reviewed and redacted before sharing outside the internal beta team.