

ThermalDIAG - API Integration Overview

Public overview of integration capabilities, the security model, and supported use cases.

Document type	API Integration Overview	API contract	External API Contract V1
Version	1.0	Date	2026-08-31
Status	Public information		
Author	JC-Technology GmbH		

Contents

- | | |
|-----------------------------|---|
| 1. Purpose and audience | 5. Data conventions |
| 2. Integration model | 6. Security and operation |
| 3. Authentication and roles | 7. Deliberate limits of External Integration V1 |
| 4. Supported data areas | 8. Detailed documentation and approval |
-

1. Purpose and audience

ThermalDIAG is a locally operated application for the combined monitoring and documentation of thermal, electrical, mechanical, and digital plant conditions. Its authenticated REST API allows approved external systems to read selected operational information and initiate clearly limited workflows.

This overview is intended for technical decision makers, system integrators, and IT/OT owners. It describes the available integration areas without disclosing internal implementation details, complete data models, or concrete endpoint paths. Authorized integration partners can receive a separate technical integration guide when required.

2. Integration model

The primary external interface is an HTTP-based REST API on the relevant ThermalDIAG installation. ThermalDIAG remains the system of record for project structure, measurements, incidents, tickets, and evidence. External clients operate only within the approved project scope and the role assigned to them.

Typical integrations include:

- forwarding a compact plant or project status to a supervisory system;
- retrieving current measurements and historical time series;
- displaying incidents, event histories, and frozen evidence;
- connecting the ticket workflow to maintenance processes;
- retrieving snapshots and reports for technical documentation;
- controlled operational actions by explicitly authorized users.

The API is not a safety controller and does not replace a PLC, protective device, or professionally approved plant control logic.

3. Authentication and roles

Every API access uses a dedicated ThermalDIAG user. A technical client requests an API token and subsequently sends it as a bearer token. Credentials and tokens must not be stored in source code, configuration repositories, screenshots, or logs.

The authorization model follows the principle of least privilege:

- `viewer`: read-only monitoring of selected summaries;
- `technician`: technical diagnostics and work on assigned tickets;
- `operator`: incident handling and approved operational changes;
- `admin`: customer-side administration and supervision;
- `supervisor`: reserved service and approval role.

An external client should always receive the narrowest role sufficient for its purpose. Write access remains subject to object state, project scope, and workflow rules in addition to the role check.

4. Supported data areas

The External Integration V1 contract covers selected authenticated functions from the following areas:

- projects, project status, and dashboard summaries;
- locations, devices, and regions of interest (ROIs);
- current measurements and historical series;
- incident timelines, details, events, and trigger evidence;
- tickets, entries, checklists, measurements, and attachments;
- snapshots, snapshot jobs, and printable reports;
- selected role-dependent incident and ticket workflows.

Internal UI, administration, maintenance, deletion, rule editing, and Analytics publishing interfaces are outside the publicly described integration scope.

5. Data conventions

API timestamps are transferred as ISO 8601 datetime values. Storage and data exchange are UTC-based; local display follows the configured project time zone. External systems must not parse formatted UI timestamps.

Temperature values are supplied through the API in degrees Celsius. Fahrenheit is a display or report conversion only. IDs are stable technical references, but must never be treated as a replacement for authorization checks.

Responses use structured JSON data. Files such as snapshots, attachments, and reports are provided through authenticated file or report responses.

6. Security and operation

The API is intended to operate inside a controlled customer environment. When traffic crosses networks that are not fully trusted, TLS, restrictive firewall or VPN access, and an explicit client identity are required. A ThermalDIAG installation should not be exposed directly to the internet without controlled protection.

Recommended operating rules:

- one dedicated user per integration;
- grant only the required role and project scope;
- store tokens securely and renew them regularly;
- do not retry write requests blindly;
- log errors, timeouts, and ambiguous results;

- record interface and ThermalDIAG versions during acceptance;
- run a defined integration smoke test after updates.

7. Deliberate limits of External Integration V1

External Integration V1 is intentionally REST-based. The current contract does not include:

- MQTT or OPC UA;
- a ThermalDIAG-side Modbus TCP server;
- Modbus RTU or general PLC register mapping;
- bidirectional PLC command processing;
- freely configurable webhook actions;
- a public anonymous monitoring API;
- general service accounts or permanently valid API keys.

Simple industrial signals may be implemented per project through approved rule actions and available device outputs. This is not a general data bus or safety control interface.

8. Detailed documentation and approval

The separate REST API Integration Guide contains the supported endpoint paths, roles, parameters, response models, and tested examples. It is supplied on a version-specific basis to authorized customers and integration partners.

Before a production integration, the parties define:

1. target system and intended use of the data;
2. required projects and data areas;
3. user role and token lifetime;
4. network route, TLS, and firewall rules;
5. permitted read and write workflows;
6. error handling, acceptance test, and version maintenance.

Integration contact: office@jc-technology.at