

ThermalDIAG - Panoramica dell'integrazione API

Panoramica pubblica delle possibilità di integrazione, del modello di sicurezza e dei casi d'uso supportati.

Tipo	Panoramica integrazione API	Contratto API	External API Contract V1
Versione	1.0	Data	2026-08-31
Stato	Informazione pubblica		
Autore	JC-Technology GmbH		

Indice

- | | |
|---------------------------|---|
| 1. Scopo e destinatari | 6. Sicurezza ed esercizio |
| 2. Modello d'integrazione | 7. Limiti intenzionali di External Integration V1 |
| 3. Autenticazione e ruoli | 8. Documentazione dettagliata e approvazione |
| 4. Aree dati supportate | |
| 5. Convenzioni dei dati | |
-

1. Scopo e destinatari

ThermalDIAG è un'applicazione locale per il monitoraggio e la documentazione congiunti delle condizioni termiche, elettriche, meccaniche e digitali di un impianto. La sua API REST autenticata consente ai sistemi esterni autorizzati di leggere informazioni operative selezionate e di avviare flussi di lavoro chiaramente delimitati.

Questa panoramica è destinata a responsabili tecnici, integratori di sistema e referenti IT/OT. Descrive le aree d'integrazione disponibili senza divulgare dettagli implementativi interni, modelli dati completi o percorsi endpoint concreti. Se necessario, i partner d'integrazione autorizzati possono ricevere una guida tecnica separata.

2. Modello d'integrazione

L'interfaccia esterna principale è un'API REST basata su HTTP presente nella relativa installazione ThermalDIAG. ThermalDIAG rimane il sistema di riferimento per struttura dei progetti, misure, incidenti, ticket ed evidenze. I client esterni operano esclusivamente nell'ambito dei progetti autorizzati e del ruolo assegnato.

Le integrazioni tipiche comprendono:

- trasmissione di uno stato sintetico dell'impianto o del progetto a un sistema superiore;
- acquisizione di misure correnti e serie storiche;
- visualizzazione di incidenti, cronologie degli eventi ed evidenze congelate;
- collegamento del workflow dei ticket ai processi di manutenzione;
- acquisizione di snapshot e report per la documentazione tecnica;
- operazioni controllate da parte di utenti esplicitamente autorizzati.

L'API non è un controllore di sicurezza e non sostituisce un PLC, un dispositivo di protezione o una logica d'impianto approvata professionalmente.

3. Autenticazione e ruoli

Ogni accesso API utilizza un utente ThermalDIAG dedicato. Un client tecnico richiede un token API e lo invia successivamente come bearer token. Credenziali e token non devono essere memorizzati nel codice sorgente, nei repository di configurazione, negli screenshot o nei log.

Il modello di autorizzazione applica il principio del privilegio minimo:

- `viewer`: monitoraggio in sola lettura di riepiloghi selezionati;
- `technician`: diagnostica tecnica e lavoro sui ticket assegnati;
- `operator`: gestione degli incidenti e modifiche operative autorizzate;

- `admin`: amministrazione e supervisione lato cliente;
- `supervisor`: ruolo riservato per assistenza e approvazione.

A un client esterno deve essere assegnato sempre il ruolo più limitato sufficiente allo scopo. Oltre al ruolo, gli accessi in scrittura restano vincolati allo stato dell'oggetto, al progetto e alle regole del workflow.

4. Aree dati supportate

Il contratto External Integration V1 comprende funzioni autenticate selezionate nelle seguenti aree:

- progetti, stato del progetto e riepiloghi dashboard;
- Locations, dispositivi e regioni di interesse (ROI);
- misure correnti e serie storiche;
- Timeline degli incidenti, dettagli, eventi ed evidenze di trigger;
- ticket, voci, checklist, misure e allegati;
- snapshot, job snapshot e report stampabili;
- workflow selezionati di incidenti e ticket dipendenti dal ruolo.

Le interfacce interne per UI, amministrazione, manutenzione, cancellazione, modifica delle regole e publishing di Analytics non fanno parte dell'ambito d'integrazione descritto pubblicamente.

5. Convenzioni dei dati

I timestamp API sono trasmessi come valori datetime ISO 8601. La memorizzazione e lo scambio dati sono basati su UTC; la visualizzazione locale segue il fuso orario configurato per il progetto. I sistemi esterni non devono analizzare i timestamp formattati dell'interfaccia utente.

Le temperature sono fornite tramite API in gradi Celsius. Fahrenheit è solo una conversione di visualizzazione o report. Gli ID sono riferimenti tecnici stabili, ma non devono mai sostituire i controlli di autorizzazione.

Le risposte utilizzano dati JSON strutturati. File come snapshot, allegati e report sono forniti tramite risposte file o report autenticate.

6. Sicurezza ed esercizio

L'API è prevista all'interno di un ambiente cliente controllato. Se il traffico attraversa reti non completamente affidabili, sono necessari TLS, accessi restrittivi tramite firewall o VPN e un'identità client esplicita. Un'installazione ThermalDIAG non deve essere esposta direttamente a Internet senza una protezione controllata.

Regole operative consigliate:

- un utente dedicato per ogni integrazione;

- assegnazione del solo ruolo e ambito progetto necessari;
- memorizzazione sicura e rinnovo regolare dei token;
- nessuna ripetizione automatica e indiscriminata delle richieste in scrittura;
- registrazione di errori, timeout e risultati ambigui;
- registrazione delle versioni di interfaccia e ThermalDIAG in fase di collaudo;
- smoke test definito dell'integrazione dopo ogni aggiornamento.

7. Limiti intenzionali di External Integration V1

External Integration V1 è intenzionalmente basata su REST. Il contratto attuale non comprende:

- MQTT o OPC UA;
- un server Modbus TCP lato ThermalDIAG;
- Modbus RTU o una mappatura generale dei registri PLC;
- elaborazione bidirezionale dei comandi PLC;
- azioni webhook liberamente configurabili;
- un'API di monitoraggio pubblica e anonima;
- service account generici o chiavi API con validità permanente.

Segnali industriali semplici possono essere realizzati per il singolo progetto tramite azioni di regola approvate e uscite disponibili dei dispositivi. Non si tratta di un bus dati generale né di un'interfaccia di comando di sicurezza.

8. Documentazione dettagliata e approvazione

La Guida all'integrazione API REST separata contiene i percorsi endpoint supportati, i ruoli, i parametri, i modelli di risposta e gli esempi verificati. Viene fornita in relazione a una versione specifica a clienti e partner d'integrazione autorizzati.

Prima dell'integrazione in produzione vengono definiti congiuntamente:

1. sistema destinatario e utilizzo previsto dei dati;
2. progetti e aree dati necessari;
3. ruolo utente e durata del token;
4. percorso di rete, TLS e regole firewall;
5. flussi di lettura e scrittura consentiti;
6. gestione degli errori, test di accettazione e manutenzione delle versioni.

Contatto per le integrazioni: office@jc-technology.at