

DATASHEET

Messaging & Notification

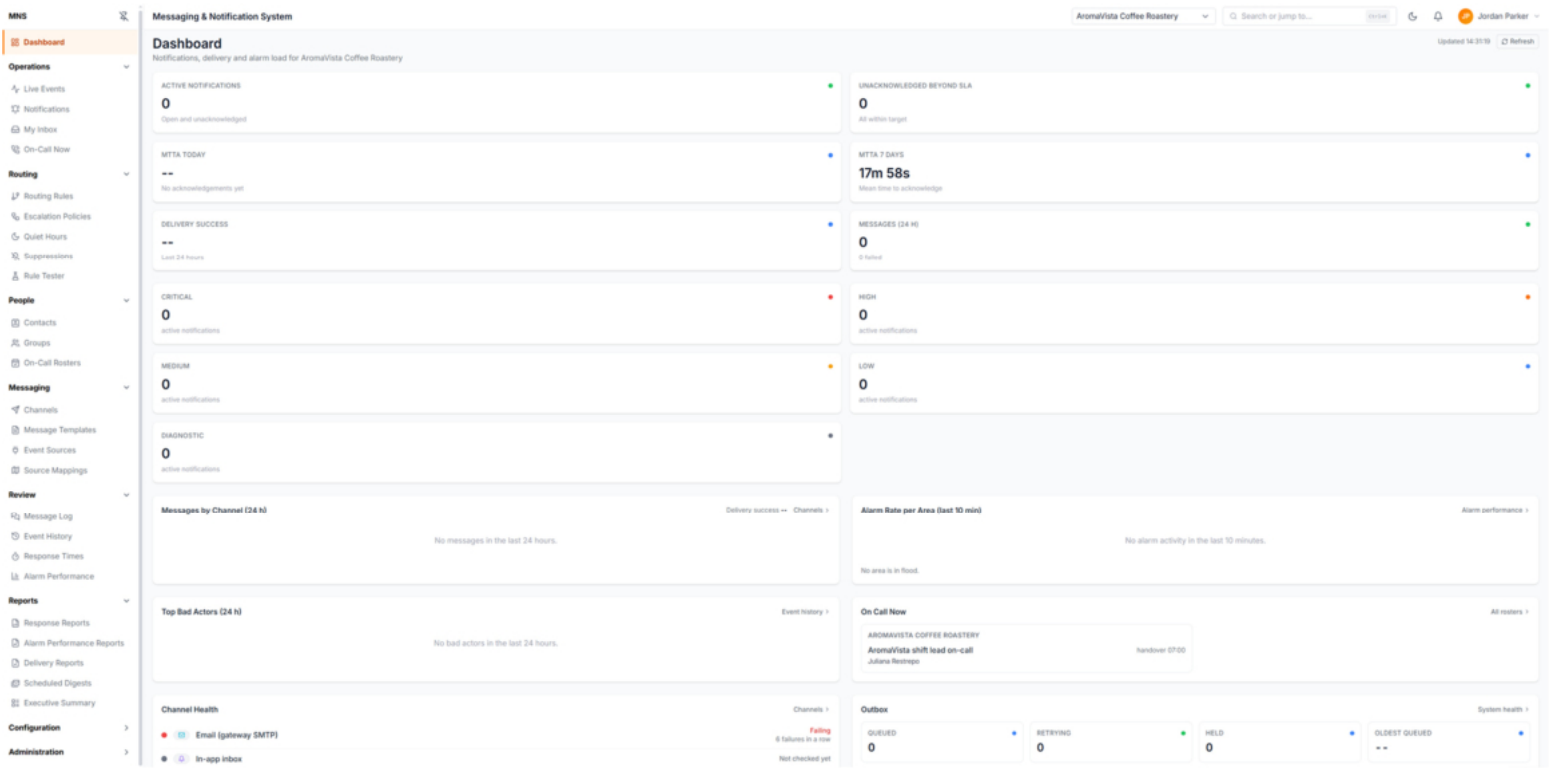
The right alert, to the right person, at the right time

A critical alarm that nobody acts on is an incident waiting to happen. In most plants, alarms stop at the SCADA screen: after-hours events wait for the next shift, email distribution lists go unread, and when something goes wrong there is no record of who was told, when, and who took ownership. LOGICAL SYSTEMS Messaging & Notification System (MNS) closes that gap - turning alarms and events from your automation systems into targeted, trackable notifications with full accountability from first alert to acknowledgement.

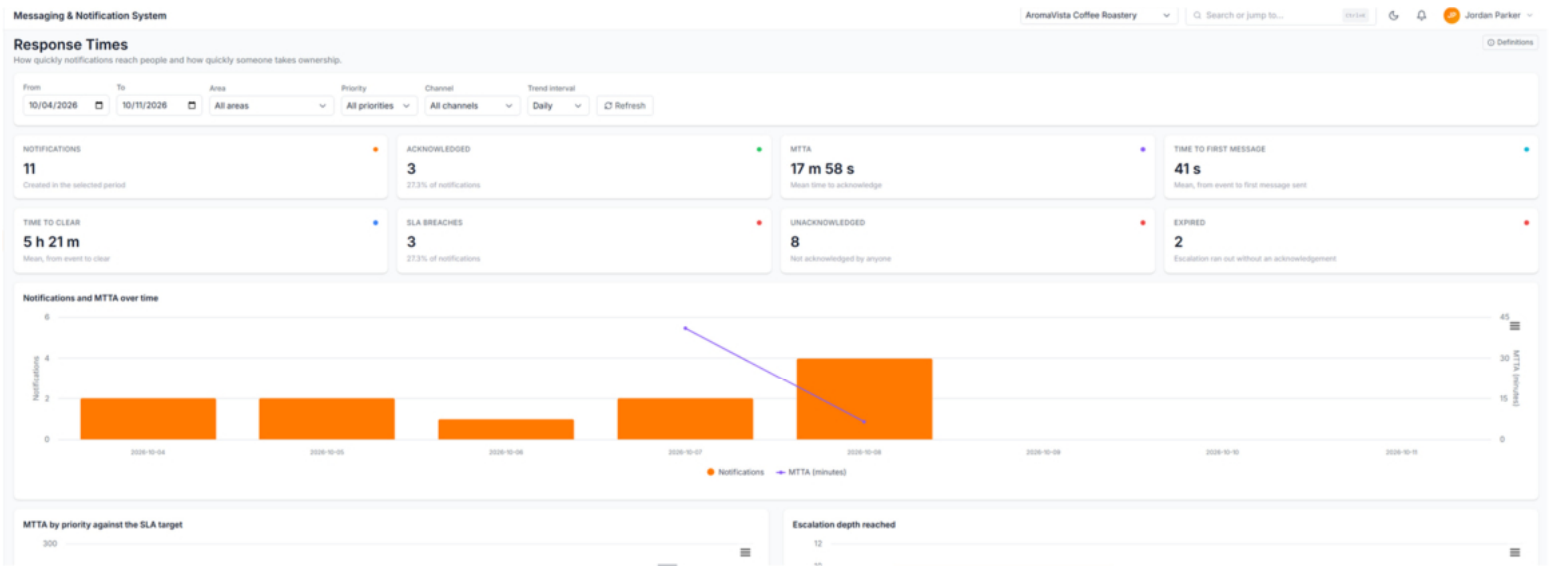
Built natively on the Inductive Automation® Ignition platform, MNS ingests Ignition alarms, events from LSA applications such as OEE, PFM, QMS, TMS, WMS, EMS and MM, and events from external systems through a simple REST notification contract. Every event is resolved against your ISA-95 plant model - site, area, line, machine - and routed through ordered rules that match source, priority, plant scope, shift and time window. Notifications reach people on the channels they actually use: email, SMS, Microsoft Teams, Slack, webhooks and the built-in in-app inbox. Escalation policies, on-call rosters with rotations and holiday cover, quiet hours and flood protection make sure the right person always takes ownership - without drowning anyone in noise.

MNS runs out of the box with an embedded database - no external database server required - and scales from a single gateway to a multi-site enterprise, with sites synchronized over the Ignition Gateway Network. Built-in analytics measure alarm load against ISA-18.2 / IEC 62682 guidance and response performance against your own SLA targets, so the same system that delivers your notifications also shows you how to improve them. Every message, delivery attempt and acknowledgement is logged, numbered and exportable, and role-based access control with a full audit trail keeps configuration changes as accountable as the notifications themselves.

From Plant Events to
Accountable Actions in Real Time



Live Notification KPIs: Active notifications, unacknowledged beyond SLA, response times, delivery success and message volume.
Priority Overview: Active notification counts by priority - Critical, High, Medium, Low and Diagnostic.
Channel Health & Outbox: Live health of every delivery channel with queued, retrying and held message counts.
On Call Now: Who is on call at every site right now, with the next handover time.



Closing the Notification Loop

Every alarm is end to end managed. Everything recorded, nothing dropped.

Capture

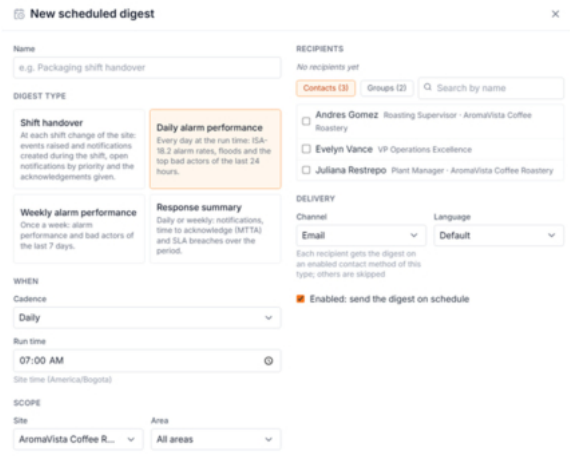
1. Ingest: Ignition alarms, LSA applications and external systems.
2. Scope: Events resolved to site, area, line and machine.

Deliver

3. Route: Ordered rules by source, priority, scope, shift and time.
4. Notify: Channel and language templates to people, groups and rosters.
5. Escalate: Stepped policies until someone acknowledges.

Learn

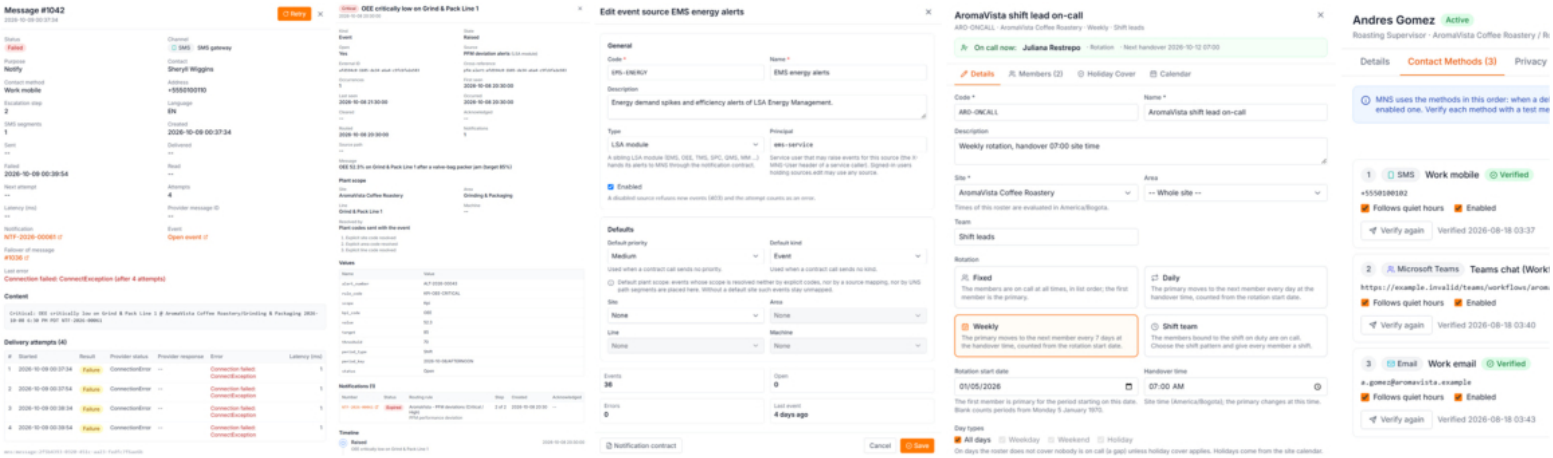
6. Acknowledge: One click from any channel, with response codes.
7. Review: Response times and ISA-18.2 alarm analytics.



Take Ownership

Of Every Alarm, on Every Shift

MNS makes ownership explicit. Routing rules are evaluated in a defined order and can be tested safely: the built-in Rule Tester replays any historical event or a sample event as a dry run, showing exactly which rules match and who would be notified right now - nothing is sent, nothing is recorded. Escalation policies notify step by step until someone acknowledges, with configurable delays, repeat cycles, expiry and automatic stop on acknowledgement or on event clear. Acknowledgements carry a response code - Acknowledged, Responding, Not my area, False alarm, No action required - and an optional comment, and MNS records who acknowledged, through which channel, and how long it took. Suppression is deliberate, never silent: operators can shelve a noisy source, engineers can schedule maintenance windows, and condition suppressions driven by live tag values mute expected alarms while a line is stopped - every suppressed event is recorded with its reason. Every notification carries a unique number and a complete timeline, *raised, routed, notified, escalated, acknowledged* and audit ready at any time.



Built for People

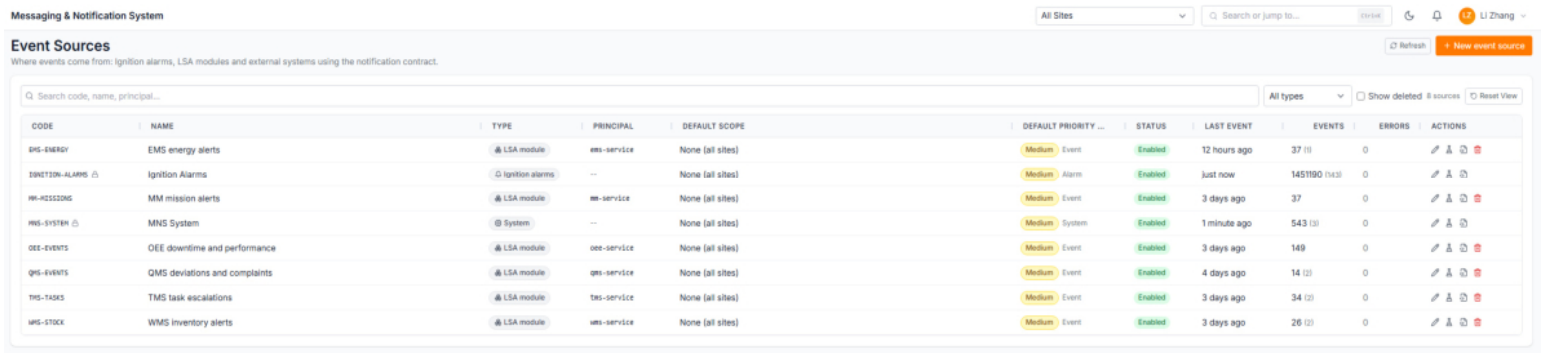
Who Keep Plants Running

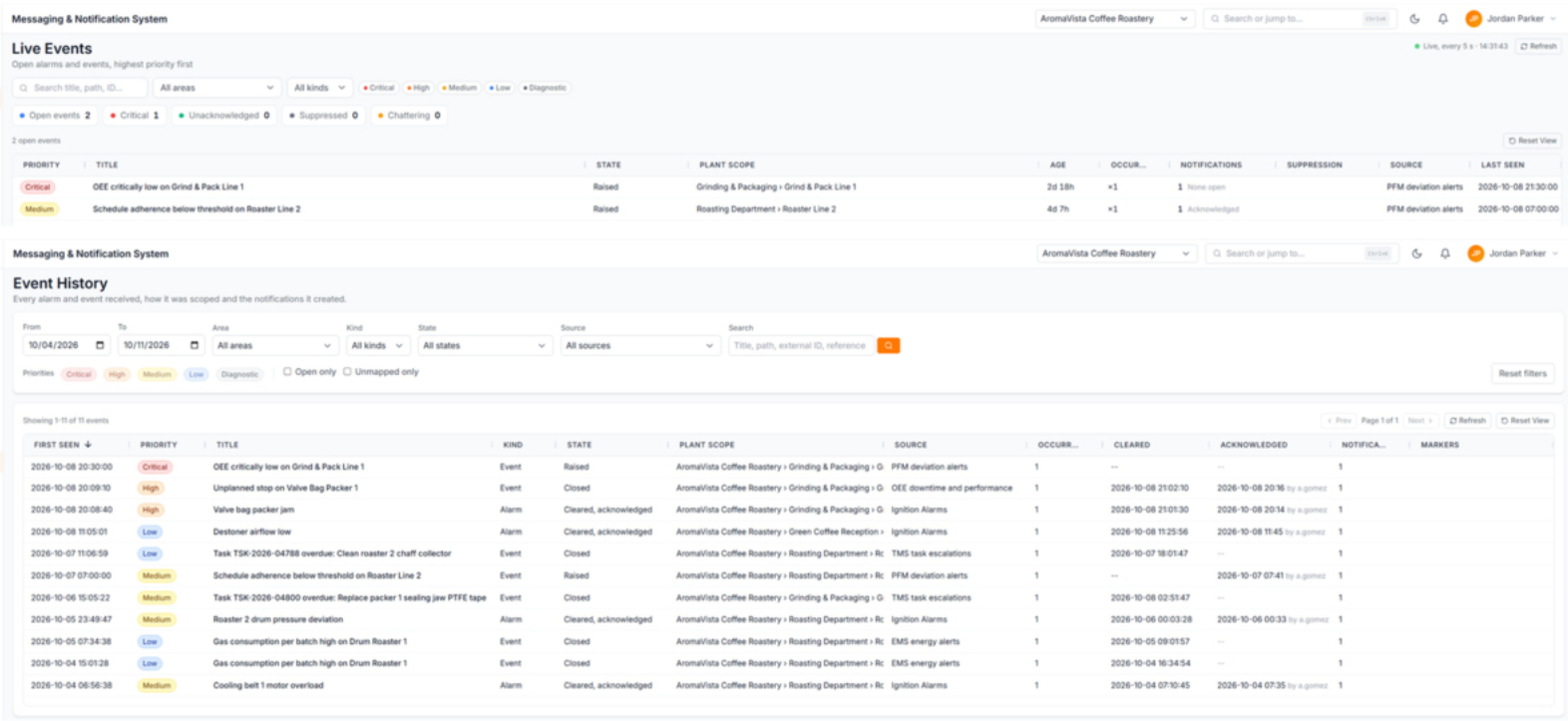
Notifications only work when they reach a person who can act. Every contact in MNS carries an ordered list of contact methods - if delivery fails on one method, MNS automatically fails over to the next, and each method can be verified with a test message so you know the address works before you depend on it. Contacts are grouped for broadcast (everyone at once) or sequential delivery (one at a time, waiting for an acknowledgement before notifying the next). On-call rosters cover every site, area or team with fixed, daily, weekly or shift-bound rotations, defined handover times, holiday cover and one-off stand-in overrides. Quiet hours hold lower-priority messages per person and deliver them as a single digest when the window ends - while critical alerts always break through. Per-contact language preferences and message template variants mean people are alerted in the language they work in.

MNS is the notification hub for the whole LSA application suite and beyond. Ignition alarms are ingested natively from the alarm pipeline. Sibling LSA applications - OEE downtime and performance, PFM deviation alerts, QMS deviations and complaints, TMS task escalations, WMS inventory alerts, EMS energy alerts and MM mission alerts - hand their events to MNS through the notification contract, and external systems use the same REST interface with per-source service principals. Acknowledgement callbacks flow back to the originating module, and unacknowledged notifications can automatically create tasks in TMS. Delivery channels cover email (SMTP), SMS gateways, Microsoft Teams, Slack, webhooks and the in-app inbox, each with health monitoring, rate limits and automatic retry with backoff.



Role-based access control with seven permission levels and site-level restrictions, a full audit trail, configurable themes and UI translations complete the enterprise picture. For multi-site estates, each site runs its own MNS instance and synchronizes configuration and history with a central gateway over the Ignition Gateway Network.





Key Features and Benefits

Features

- Native Ignition gateway module - no middleware, no separate server
- Multi-channel delivery: email, SMS, Microsoft Teams, Slack, webhooks, in-app inbox
- Automatic failover across a contact's methods and delivery channels
- Ordered routing rules by source, priority, plant scope, shift, day type and time window
- Stepped escalation policies with delays, repeats, reminders and expiry
- On-call rosters with fixed, daily, weekly and shift-bound rotations, holiday cover and stand-ins
- Quiet hours with automatic digests; critical alerts always break through
- Flood protection with per-recipient rate caps and summary messages
- Rule Tester: dry-run any event against live rules - nothing sent, nothing recorded

Benefits

- Faster response to critical events - the right person is alerted directly, on the channel they actually use
- No silently dropped alarms - every event, message and acknowledgement is recorded and numbered
- Less alarm fatigue - suppression, flood control and quiet hours cut noise without hiding critical alerts
- Clear accountability - who was notified, who acknowledged, how long it took, measured against SLA targets
- Alarm quality you can manage - bad actors, chattering and standing alarms surfaced against ISA-18.2 guidance
- Lower integration cost - one notification hub for Ignition alarms, LSA applications and external systems

Technical Requirements

System Requirements

Ignition® (8.1.+) Core Modules, Quad-core processor, 16 GB RAM, 10 GB free disk space

Supported Operating Systems

Windows Server 2019/2022/2025, Windows 10/11, macOS (X, 10.16+), Linux (Ubuntu, CentOS, RHEL)

Supported Protocols

MQTT, OPC UA / OPC DA, REST API (JSON Payloads)
Kafka (via connector), Snowflake (via pipeline, data bridge)

Supported Databases

Microsoft SQL Server, Oracle, MySQL, MariaDB, PostgreSQL, any database with JDBC driver

Supported Browsers

Chrome, Firefox, Safari, Microsoft Edge



LOGICAL SYSTEMS
AUTOMATION & INTEGRATION SERVICES
Specialists in Automation & Digitalization for Manufacturing Industries

Copyright © 2026 LOGICAL SYSTEMS and its subsidiaries. All rights reserved.
All product names mentioned are the trademarks of their respective holders.

www.logicalsystems.io | info@logicalsystems.io