INDUSTRIAL FAULT ALERTING AND ALARM MANAGEMENT

AS1111

User Manual

Panel-mounted alarm monitoring and notification device · 32 digital inputs

October 2026 · Rev. 1.0
ionia Automation Technologies · ionia-automation.com

Contents

1 About this manual 4

2 Panel access 4

2.1 Opening the panel 4

2.2 Signing in and PIN 4

2.3 Screen layout and navigation 5

2.4 Roles and permissions 5

3 Dashboard 6

3.1 Digital inputs 6

3.2 Alarm Summary and Quick Actions 6

3.3 System Status 7

4 Alarms 7

4.1 Notification message 7

4.2 Severity levels 7

4.3 Alarm life cycle 7

4.4 Alarm Monitoring page 8

4.5 Acknowledging, silencing and resetting 8

4.6 Escalation (stepped notification) 9

5 People and notification channels 9

5.1 My account 9

5.2 Receiving notifications on Telegram 9

5.3 Working hours and minimum severity 10

5.4 Adding people (administrator) 10

5.5 Notification behaviour 10

5.6 Notification log 10

6 Input and alarm settings (administrator) 10

6.1 Rules 10

6.2 Alarm options 11

6.3 Targets and acknowledge permission 11

6.4 Escalation settings 11

6.5 Saving and resetting 11

7 Event Log 12

8 Plant view 12

9 Outages and System page 14

9.1 Outage behaviour 14

9.2 Outage messages 14
9.3 Outage report 14
9.4 System page 14
10 Settings backup (administrator) 15
11 Integration: ERP and maintenance software (administrator, IT) 15
11.1 Webhook 15
11.2 Read endpoints (REST) 16
11.3 Security 17
12 Administrator tasks at a glance 17
13 Frequently asked questions 17
14 Glossary 18

1 About this manual

This manual is for the operators, technicians, shift supervisors and administrators who use the web panel of the Alert SCADA AS1111 every day. Mounting, wiring, network settings and initial setup of the device are described in the **AS1111 Installation Guide**.

Some sections are for everyone (panel access, alarm monitoring, acknowledgement, event log, My account). Sections that need configuration rights (people, alarm rules, targets, escalation, backup, integration) are marked **administrator** in the heading.

> **Life safety**
> Alert SCADA is a **fault alerting** device. **It does not replace fire detection, gas detection, life-safety or legally required alarm systems.** Delivery of notifications depends on power, the internet and third-party services (Telegram, e-mail).

The panel can be switched between Turkish and English. Page and button names are given here in English; the exact wording on screen may differ slightly. Screenshots show the Turkish interface and are examples; input and device names will be different in your plant. The panel screens may show the model as `ION8-1111`.

2 Panel access

2.1 Opening the panel

The panel is a web page; **no app is installed**. On a phone, tablet or computer connected to the plant network, open the browser and go to the address given by your administrator:

- **http://ion8-xxxxxx.local** or the name your administrator gave the device (e.g. `http://press-line-2.local`), or
- the device's IP address (e.g. `http://192.168.1.50`).

Both addresses are shown as clickable, copyable links on the WiFi card under **Settings** and on the **Notifications → WiFi** page. The `.local` address does not open on some Android phones; in that case use the IP address.

> **On a phone**
> The panel adapts to the phone screen; tables are shown as cards one below the other. **Add the page to your home screen** from the browser menu so it opens with a single tap.

If the panel does not open at all while the phone is on the plant WiFi, **client isolation / guest network** may be enabled on the router; tell your administrator or IT team. The panel is used only on the plant network; it is not exposed to the internet.

2.2 Signing in and PIN

- Unless your administrator has chosen otherwise, the panel **can be viewed without signing in**. To acknowledge an alarm or change a setting, use **Sign in** at the top right → select your name → enter your **PIN**.
- The PIN is personal, has 4–6 digits and is stored on the device in a non-reversible form.
- After 5 wrong PIN attempts you must wait 5 minutes. If you do nothing for 30 minutes, you are signed out automatically.
- With **Settings → View access**, the administrator can require sign-in just to view the panel.
- If you forget your PIN, your administrator gives you a new one. A forgotten administrator PIN is reset with the device's own recovery code (Installation Guide).

2.3 Screen layout and navigation

- The **menu** is grouped by topic: Monitoring, Alarms, Management. On a phone the menu is behind the ☰ button at the top left.
- **Bottom bar on a phone:** the Home, Alarms, Plant, Events and Menu tabs are always visible.
- **Related** row: at the top of every page, takes you with one tap to the pages used together with that page (e.g. Alarm Monitoring → Alarm Settings).
- **Top bar:** the number of active alarms (🔔) is shown on every page. The 🌐 button switches the language (Turkish / English), the ☀/☾ button switches between light and dark view.
- **Status bar:** whether the panel is connected to the device (**Connected** / **Disconnected**) and the device uptime. If it shows "Disconnected", the information on screen is not up to date; check your network and reload the page.
- **Channel details:** tap an input card on the Dashboard or a channel name in the Event Log: the current state, recent events and the **Full history** (Event Log filtered to that channel) / **Alarm setting** buttons appear.
- **Unsaved changes:** if you change a setting and move to another page without saving, you are asked whether to save: **Save** or **Leave without saving**.

2.4 Roles and permissions

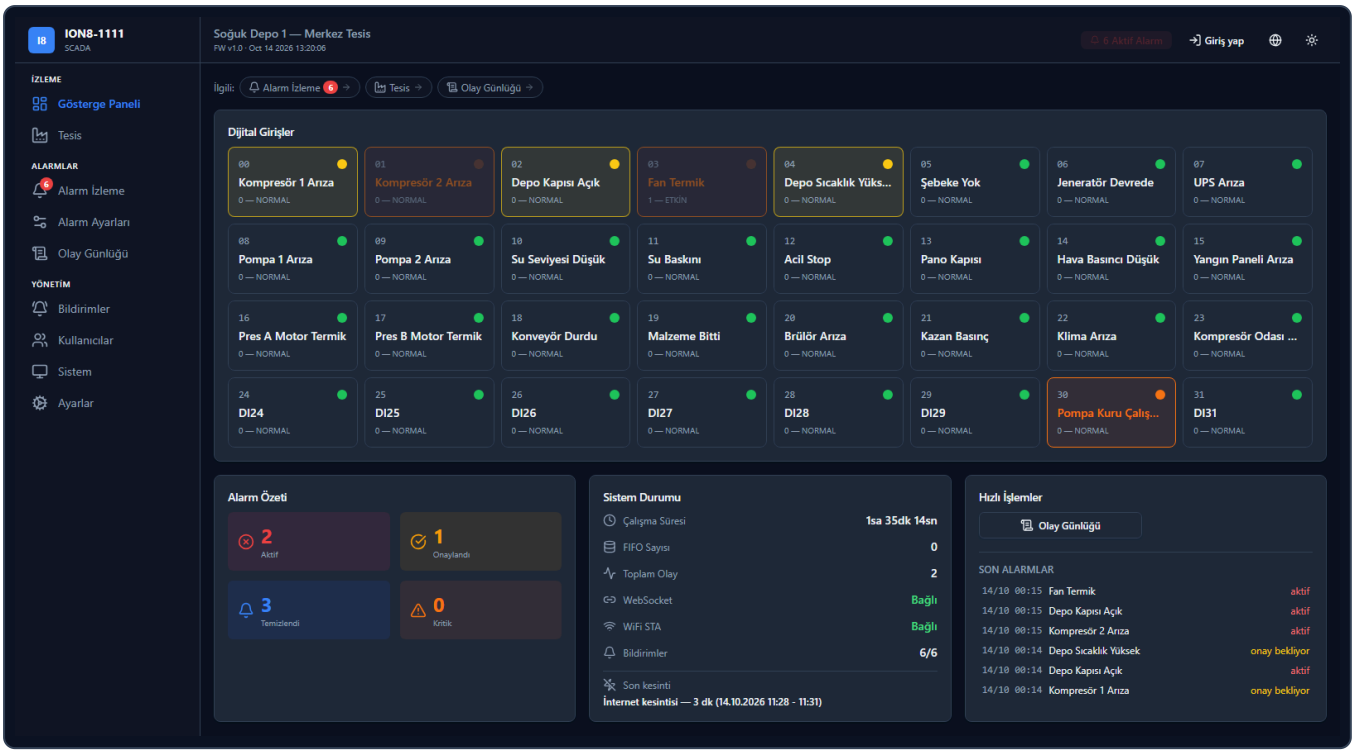
Each person has one or more **roles** (e.g. Administrator, Shift Supervisor, Technician, Operator). Permissions are given to roles (**Users** → **Roles**). Up to 32 people and 16 roles can be defined.

Permission (in the panel)	Allows
ACK	Acknowledging alarms
Silence	Temporarily silencing the alarm sound / repeat notifications
Config	Alarm rules, targets, device and notification settings
Add user	Adding and deleting people, assigning roles and PINs
Service (maintenance)	Service settings and diagnostic screens; for authorised service only

Full administrator = Config + Add user. Some actions (changing the acknowledging role, outage report, factory reset) can only be done by a full administrator. The device does not allow the last administrator to be deleted; define **at least two** administrators.

3 Dashboard

The Dashboard is the device's home page: the current state of the 32 inputs, the alarm summary, the system health and the latest alarms on one screen.



Dashboard (computer): 32 input cards, Alarm Summary, System Status and Latest alarms (Turkish interface)

3.1 Digital inputs

Each of the 32 inputs is shown as a card: input number (00–31), name and current state text (e.g. "Pump running"). **The card colour shows the alarm state**, not whether the input is 0 or 1:

Appearance	Meaning	What to do
`Red, flashing`	Unacknowledged alarm	Check the situation, **acknowledge**
`Red, steady`	Alarm acknowledged but the condition persists	Goes out by itself when the fault is cleared
`Yellow / orange`	Input back to normal, awaiting acknowledgement	Acknowledge
`Blue dot`	Input 1, no alarm	—
`Green dot`	Input 0, no alarm	—

> **Both Edges rule**
> For inputs that alarm "on every change" (e.g. door opened / closed notification), the alarm is the change itself: it ends when acknowledged. The card does not stay red even if the input stays at 1.

3.2 Alarm Summary and Quick Actions

- **Alarm Summary:** the number of active, acknowledged, back-to-normal (awaiting acknowledgement) and critical alarms.
- **Quick Actions: Acknowledge all**, **Silence**, **Reset**, **Event Log** (buttons appear according to your permissions).

- **Latest alarms:** the latest alarms and their states (active · awaiting acknowledgement · acknowledged · closed). Tap a row to open the Event Log.

3.3 System Status

The panel's connection to the device, plant WiFi and notification status, uptime and **Last outage** (the last power or internet outage, its duration and time range). An ongoing internet outage is shown in red.

4 Alarms

4.1 Notification message

An alarm arrives on the channel set up for you (Telegram and/or e-mail). Example (translated for illustration):

```
[CRITICAL] Press Line 2 - Welding Shop
Channel: Pump Fault (DI30)
State: Pump stopped
Time: 04.10.2026 14:32:07
Event no: 7629
```

The header shows the **severity**, followed by the device name and location; below are the input, what happened, when it happened and the event number. Alarms arriving within a few seconds are combined into one message ("3 alarms ..."), so your phone is not flooded with notifications.

4.2 Severity levels

Each input's alarm is given one of four severity levels. The severity appears in the notification header and in the panel; people's "minimum severity" and working-hours settings and the per-minute repeat limit work according to it.

Severity	In the notification header (Turkish panel)	Repeat limit (default, per minute)
Info	[BILGI]	3
Warning	[UYARI]	3
Alarm	[ALARM]	3
Critical	[KRITIK]	Unlimited

Repeat limit: if the same input raises many alarms within one minute, the excess is not sent (it stays in the record). The administrator sets the limit per severity under **Notifications → General**; 0 = unlimited.

4.3 Alarm life cycle

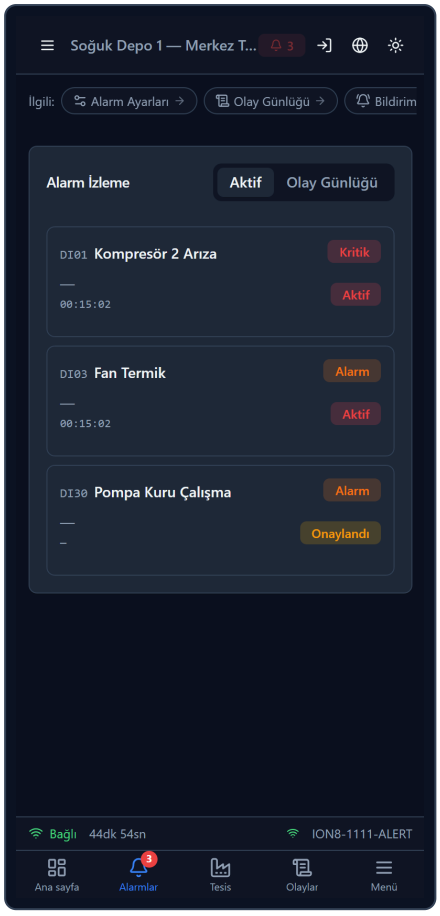
1. **The alarm occurs:** a notification goes to the relevant people and the card flashes red in the panel.
2. **You acknowledge it:** this says you are dealing with the fault. The name of the person acknowledging and the response time are recorded; the other people who received the alarm get an **"acknowledged — Acknowledged by: your name"** notification and forwarding to higher levels (escalation) stops.
3. **The condition ends:** when the input returns to normal, the alarm closes. If enabled for the input, a **"back to normal — lasted X min"** notification is sent.

If the condition ends before acknowledgement, the alarm changes to **"back to normal — awaiting acknowledgement"** and closes when acknowledged.

Unacknowledged alarms

An unacknowledged alarm is reported to **higher levels** (shift supervisor, maintenance manager) after the times set by your administrator. Even if the signal returns to normal, an unacknowledged alarm continues to escalate.

4.4 Alarm Monitoring page



Alarm Monitoring (phone, Turkish interface): one card per alarm

The **Active** tab lists alarms awaiting acknowledgement and ongoing alarms (one card per input on a phone):

Field	Meaning
Channel / Name	Input number (DI00–DI31) and name
Time	Time the alarm occurred
Message	Text of the change that started the alarm
Severity	Info · Warning · Alarm · Critical
State	Active · Acknowledged · Back to normal — awaiting acknowledgement
Acknowledge	Acknowledge and silence buttons

Buttons at the top of the page: **Acknowledge all** · **Silence** · **Reset** · **Test**. The **Event Log** tab switches to the history on the same page.

- **Each unacknowledged alarm is a separate row.** For example, if a door was opened and closed twice before being acknowledged, each change appears on its own row with its own time and text.
- Acknowledgement is **per input:** an input's **Acknowledge** button closes all of that input's rows together (a note such as "acknowledges 2 alarms together" appears next to the button).
- **Test** (for authorised people) generates a test alarm to check that the system is working.

4.5 Acknowledging, silencing and resetting

- **Acknowledge:** the **Acknowledge** button in the alarm's row (its card on a phone) on the Alarm Monitoring page, or **Acknowledge all**. If there are several devices in the same plant, you can also acknowledge another device's alarm from the **Plant** page.
- **If the Acknowledge button is not shown:** you have not signed in, your role does not have the acknowledge permission, or only a specific role may acknowledge that input's alarm. **Acknowledge all** only acknowledges the alarms you are permitted to, and tells you how many were skipped.
- **Silence:** temporarily stops repeat notifications (requires the Silence permission). It does not close the alarm.
- **Reset: latched** alarms persist, even if the signal recovers, until an authorised person acknowledges them and presses **Reset**.

Acknowledging, silencing and resetting are written to the Event Log together with who did them.

4.6 Escalation (stepped notification)

An unacknowledged alarm is forwarded to the next level after the set times. Example chain:

Step	When	To whom (example)
First notification	When the alarm occurs	Operator
Level 1	If not acknowledged, 10 min later	Shift supervisor
Level 2	If not acknowledged, another 10 min later	Maintenance manager
Level 3	If not acknowledged, another 10 min later	General manager

The times and people are examples; the administrator builds the chain to suit your organisation (Section 6.4).

- The chain stops when the alarm is **acknowledged**. For an input with auto-acknowledge, it also stops when the signal returns to normal.
- With auto-acknowledge off, an **unacknowledged** alarm keeps escalating even if the signal returns to normal.
- One chain runs per input: new changes while acknowledgement is pending do not restart the chain.
- Without internet, an escalation step is not lost; it is sent when the connection returns.
- "Acknowledged" and "back to normal" notifications go to **all levels reached** (not to the person who acknowledged).

5 People and notification channels

5.1 My account

Settings → **My account** (after signing in). Everyone can change only their own details:

- Full name
- **Where notifications should reach me:** Telegram · E-mail · Panel
- Telegram ID and e-mail address
- **Send me alarms of at least this severity** (e.g. Alarm and Critical only)
- **Working hours**
- **Change PIN** (your current PIN is required)

Only the administrator can change your role and other people's details.

5.2 Receiving notifications on Telegram

Each person does this once, on their own phone:

1. In Telegram, open the **device's notification bot** (the link is shown on the My account page and in the setup wizard) and press **Start**. If you do not, the bot cannot send you messages.
2. Open **@userinfobot** and press **Start**; copy the **Id** number from the reply.
3. Paste the number into the **Telegram ID** field on My account and save.

The notification account comes ready with the device; there is no fee or subscription for Telegram. E-mail notifications may land in the spam folder the first time; add the sender address to your safe senders list.

5.3 Working hours and minimum severity

Applied to each person separately:

- **Minimum severity:** alarms below the selected severity are not sent to that person (e.g. the maintenance manager receives Critical only).
- **Working hours:** outside working hours, only alarms above the selected severity are sent. At night you are woken only for important alarms.

These settings filter notifications; the alarms are still shown in the panel and in the Event Log.

5.4 Adding people (administrator)

Users → People → Add person: full name, role(s), PIN (if the person will sign in to the panel), notification channels (Telegram / E-mail / Panel), Telegram ID, e-mail, minimum severity and working hours.

- A newly added person with a Telegram ID or e-mail address who is not yet a target of any input is automatically added to the alarm targets of all inputs. A person later removed from the targets is not touched again.
- After adding a person, send a test message from **Notifications → Log** and check that it arrives.

5.5 Notification behaviour

- **Grouped sending:** alarms arriving within a few seconds are combined into one message.
- **Retry:** a notification that could not be delivered to a person on one channel is retried only for that person and channel (0–5 times, Notifications → General).
- **Repeat limit:** Section 4.2.
- **System notifications:** device restarted (with the power outage duration), internal connection problem, storage card problem, internet outage summary and outage report. These go to the system alarm roles or, if none are defined, to roles with the Config permission.

5.6 Notification log

Notifications → Log: every notification sent (alarm, escalation, acknowledged, back to normal, system, test), to whom and on which channel it went, and the result. For a notification that could not be sent, the **reason** is shown (the error returned by Telegram or the e-mail server, "no internet" and similar). Tap a row to see the full message text.

6 Input and alarm settings (administrator)

6.1 Rules

The **Alarm Settings → Rules** page has one row per input (one card per input on a phone).

Setting	Description
Channel name	Name shown in notifications and in the panel (e.g. "Pump 1 Thermal")
Trigger	**Disabled** (not monitored) · **Rising Edge** (0→1 alarm, 1→0 back to normal) · **Falling Edge** (1→0 alarm, 0→1 back to normal) · **Both Edges** (each change is a separate alarm and notification)
Debounce (ms)	Signal filtering: a change is not counted until the input has been stable for this time (0–10,000 ms). Filters contact chatter and short interference
Severity	Info · Warning · Alarm · Critical
Texts	State texts (for 0 and 1; shown below the input in the panel) and edge messages (the "State:" line in the notification, e.g. "Door opened" / "Door closed")

6.2 Alarm options

Option	Description
Latched	The alarm persists, even if the signal returns to normal, until an authorised person acknowledges and resets it
Auto-acknowledge	The alarm closes by itself when the signal returns to normal; no acknowledgement is awaited
Inverted Logic	For NC contacts: **loss** of the signal (including a broken cable) is an alarm, its return is normal
Log only	The event is recorded and shown in the panel; no notification is sent
Back to normal	A notification is sent when the signal returns to normal. "at least ... s": not sent if the alarm lasted less than this time (for inputs that switch on and off often)
Acknowledged notification	When the alarm is acknowledged, the other people who received it get an "acknowledged — by: ..." notification

> **Both Edges**
> With this rule, the alarm is the change itself: it closes when acknowledged and does not persist even if the input stays at 1. Each new change is a separate notification even if the previous one has not been acknowledged; one acknowledgement closes them all.

6.3 Targets and acknowledge permission

In the **Alarm Settings** → **Targets** table you choose **which roles and people** each input's alarm goes to.

The last column of the table is the **acknowledging role** (ACK role): only people in the selected role and full administrators may acknowledge that input's alarm; for example, only the maintenance team may acknowledge the boiler alarm. "Everyone" = everyone with the ACK permission. Only a full administrator can change the acknowledging role.

6.4 Escalation settings

The **Escalation** button in the input's row on the Targets page:

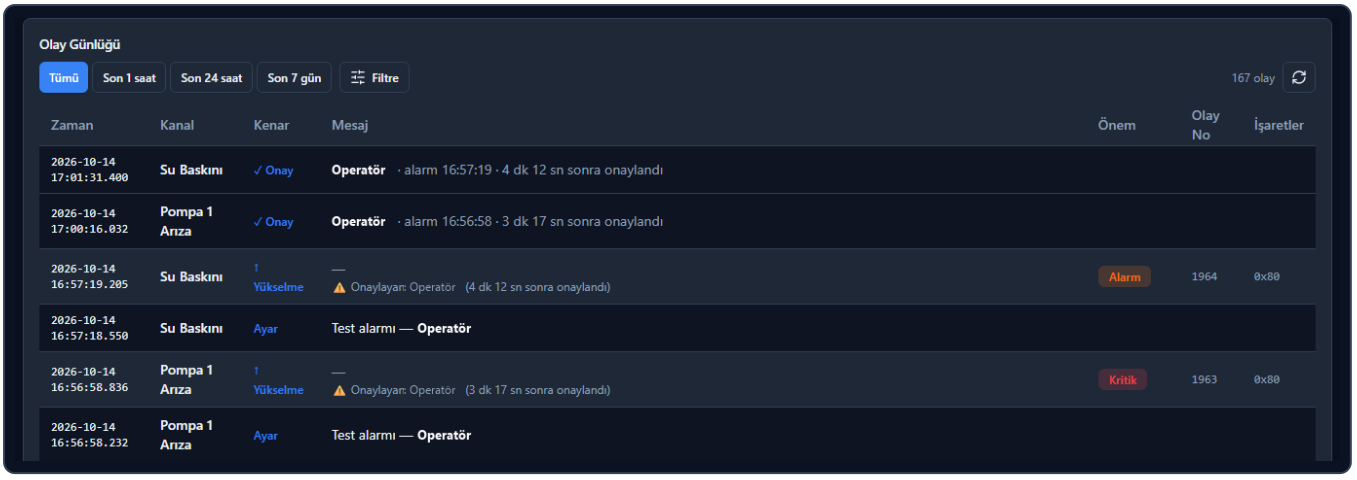
1. Turn on the **Use escalation** switch. The **first notification** goes out when the alarm occurs (filled from the input's targets).
2. **Level 1:** set the "if not acknowledged, ... min after the previous step" time and select the people (e.g. Shift Supervisor).
3. Use **Add level** to add up to two more levels: at most 4 steps including the first notification; at most 4 roles + 4 people per step.
4. Press **Save**. To give the same chain to all inputs, use **Apply to all inputs** (pressed twice to confirm).

6.5 Saving and resetting

- Changes in Alarm Settings are written to the device and become permanent when you press **Save**; they are not lost in a power cut. Changed rows are highlighted in yellow and the button shows how many channels have changed. **Undo** discards unsaved changes.
- **Reset alarm settings** resets the rules, names and texts of all 32 inputs; users, notification settings and targets are kept. After the reset, **no input raises an alarm**.

7 Event Log

All input changes, alarms, acknowledgements, panel sign-ins and setting changes are recorded **with date and time** and who made them. Power and internet outages and device restarts are also included in the log.



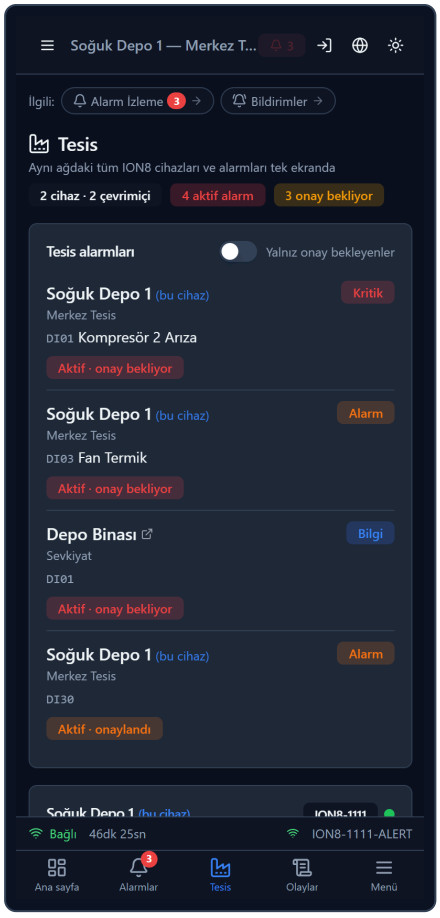
Event Log: who acknowledged, when, and after how many minutes (Turkish interface)

- **Filtering:** use the **All · Last 1 hour · Last 24 hours · Last 7 days** buttons at the top and **Filter** to select a date range and look back in time. For the history of one channel, tap the channel name and select **Full history**.
- **Columns:** time, channel, edge (↑ rising · ↓ falling, acknowledgement, setting), message, severity and event number.
- **Alarm rows** show who acknowledged, the response time and how long the alarm lasted ("⚠ Awaiting acknowledgement" · "✓ Back to normal · lasted 12 min").
- On a phone, each event appears on its own card: input name, severity, direction, time and description.

The answer to "what happened during the night?" at shift change is here. The records can be used as evidence in fault analysis and audits.

8 Plant view

If there is more than one Alert SCADA device on the same plant network (e.g. an AS1111 on another line or an AS1122 with outputs), the **Plant** page shows all of them on one screen.



Plant page (phone, Turkish interface)

Section	Content
Top row	How many devices are visible and how many are online; total active and unacknowledged alarms in the plant
Plant alarms	The alarms of all devices in one list: device, input, severity, state. The **Awaiting acknowledgement only** switch filters the list
Device cards	Each device's name, location, model, whether it is online, and its inputs (red/orange = alarm, green = active). **Open device page** switches to that device's own panel

Acknowledging another device's alarm: the **Acknowledge** button in the list (you need the acknowledge permission). The acknowledgement is passed to that device and recorded under your name. If the row says "remote acknowledgement off", that device's administrator has disabled acknowledgement from other devices: acknowledge it in that device's own panel. If it says "device not visible", the device cannot be reached at the moment.

- If nothing is heard from a device for 6 seconds, "no connection" is shown. If a previously seen device is not seen at all for 2 minutes, the Plant page shows the possible causes (device off, different network, client isolation, different plant password).
- For the devices to see each other, all must be on **the same plant WiFi network** and have **the same plant password** entered (administrator: **Plant → Plant settings**). No internet is needed.
- Tapping another device's name opens that device's panel in a new tab; these links work while the phone is on the plant WiFi.
- The Plant page does not replace each device's own panel: settings and rules are changed in each device's own panel. To drive an AS1122's outputs from AS1111 alarms, the rule is set up in the AS1122's panel.

9 Outages and System page

9.1 Outage behaviour

Situation	What the device does	What you see
Internet down	Keeps monitoring and recording the inputs; holds notifications	When the internet returns, the device verifies the connection (up to 90 s); held notifications arrive with a "... min delayed (no connection)" note, followed by an outage summary. Notifications **older than 30 minutes** are not sent and remain in the Event Log. No message is sent for drop-outs shorter than 1 minute with no alarm in between
Power cut	Does not run and cannot monitor the inputs. Settings and records are kept	When power returns, a "Device restarted: power outage ..." notification. Inputs that went into the alarm state during the outage raise an alarm at start-up
Report missing	—	If the outage report is enabled, a "system running" message or an outage report arrives at the expected time. If not, check the device's power and internet connection

The AS1111 has a **battery-backed clock**: the start and end times of a power cut are recorded correctly even without internet. A UPS-backed supply is recommended for uninterrupted monitoring.

9.2 Outage messages

Examples (translated for illustration):

After a power cut

```
Device restarted: power outage ~10 min 45 s (21:00 - 21:11).
Inputs were not monitored during this time.
```

Internet outage summary

```
[SYSTEM] Press Line 2 - Welding Shop
Internet connection was down for 7 min (23:22 - 23:29). 2 notifications were held
during the outage and sent when the connection returned.
```

Outage report

```
[OUTAGE REPORT] Press Line 2 - Welding Shop
Outage report (04.10 21:00 - 04.10 22:00)
1 outage:
- Internet: 1 h 26 min (04.10 20:59 - 22:26)
Total: no power outage, internet 1 h 26 min.
```

9.3 Outage report

Notifications → Outage report (full administrator): report frequency (hourly ... weekly), time / day and recipients. All outages in the selected period are reported; if there were none, a **"system running"** message is sent. This message regularly confirms that the device is working and can reach you: silence also tells you something. Default: off.

9.4 System page

The **System** page shows the device's health information: memory, WiFi, storage card and internal connection status, and the **Boot history** (the reason for the last 16 start-ups: power outage / planned restart / software error; previous

uptime). The boot history is not deleted by a factory reset.

- **Restart device:** settings are kept; the panel is disconnected for about 1 minute.
- When contacting service, include a screenshot of this page.

10 Settings backup (administrator)

Settings → Settings backup:

- **Download backup:** roles, people, alarm targets and escalation, input names and texts, notification settings, outage report, device name and plant setting are saved to a single file (`.json`). Optional: people's contact details and the plant WiFi. **PINs are never included in the backup.**
- **Restore:** select the file, tick the sections one by one, **Restore selected**. If the plant WiFi is already the same, it is not changed. The backup can be restored to the same or a new device; give new people their PIN from the Users page.

> **Backup file**
> The backup file may contain the WiFi password and people's contact details. Store it securely. Make a backup before major changes.

11 Integration: ERP and maintenance software (administrator, IT)

Alert SCADA events can be passed to systems such as ERP, CRM, maintenance / work-order software or SCADA in two ways. This section is a summary; for all fields and examples, your IT team can request the **Integration Guide** from support@ionia-automation.com.

Need	Method	Direction
Open a work order / record when an alarm occurs; update it when acknowledged or cleared	**Webhook**	Device → your server (HTTP POST, JSON), as the event happens
Current status, past events and outages on a display or in a report	**Read endpoints (REST)**	Your software → device (HTTP GET, JSON)

Writing settings, acknowledging alarms or adding people from outside are not part of the integration; these are done only in a PIN-protected panel session.

11.1 Webhook

A webhook is set up on the device like a **person**: wherever alarms go, they also go to the webhook address under the same rules.

1. **Users → People → Add person**. Name: e.g. `ERP`. Do not give it a PIN.
2. Among the notification channels, tick only **Webhook** and enter your server's address in the **URL** field (at most 127 characters).
3. Add this person (or its role) to the targets of the inputs to be monitored; if needed, to the escalation levels too. To send everything, leave the minimum severity at **Info** and the working hours empty.
4. On the **Settings → Integration (webhook)** card, enter the address and test it with **Send**; "Webhook OK 200" should appear on screen.

5 Recommended: on the same card, enable signing with **Generate key**. The key is shown only once; enter it in your receiving system.

Property	Value
Request	`POST`, `Content-Type: application/json`, UTF-8, a single JSON object
Address	`http://` or `https://`; with HTTPS the server certificate is verified against public root certificates (self-signed certificates are not accepted)
Timeout / success	10 seconds / the server must return **2xx**
On failure	The same notification is retried (0–5 times); held while there is no network, those older than 30 minutes are not sent
Event type (`type`)	`alarm` · `escalation` · `ack` · `normal` · `system` · `test`
Main fields	`device`, `location`, `channel` (0–31), `channel_name`, `state`, `severity` (`INFO` … `CRITICAL`), `event_id`, `time`, `subject`, `text`
Signature	Optional HMAC-SHA256; timestamp and signature are sent in HTTP headers

Filter out duplicates

Because of retries, the same event may arrive twice. On the receiving side, filter duplicates using the combination `channel` + `event_id` + `type`. To receive system notifications too, add the webhook person to one of the system alarm roles.

11.2 Read endpoints (REST)

Address: `http://<device-address>/api/...`; method `GET`, response JSON. Give the device a fixed IP address. Poll at most every 2 seconds, preferably every 5–10 seconds; use the webhook for real-time events.

Endpoint	Content
`/api/status`	Device summary: model, name, location, uptime, number of active alarms, storage card status
`/api/alarms`	Inputs not in the normal state and their states (active · acknowledged · back to normal, awaiting acknowledgement)
`/api/events?since=<n>`	Recent events; with `since`, only new ones
`/api/outages`	The last 32 power / internet outages and the last 16 start-ups
`/api/device`	Model, device name, location
`/api/alarm/rules`	Each input's name, trigger type, severity and state texts
`/api/stats`	Daily counters and notification sending counters
`/api/peers`	Other devices on the same network and their alarm summaries

If View access is enabled, endpoints other than `/api/status` and `/api/stats` require a session; for integration, define a separate person and role with monitoring rights only.

11.3 Security

- The panel and the read endpoints run over unencrypted **HTTP**. Use the device only on a trusted plant network and do not expose it to the internet; use a VPN for remote access.
- The webhook body contains people's names and plant information; if the receiving server is outside your network, use **HTTPS** and enable signing.

12 Administrator tasks at a glance

Task	Where
Add / remove people, assign roles and PINs	Users → People
Edit role permissions	Users → Roles
Input name, alarm condition, severity, texts, options	Alarm Settings → Rules
Who receives the alarm, escalation, acknowledging role	Alarm Settings → Targets
Outage report (frequency, recipients)	Notifications → Outage report
Notification log, test message	Notifications → Log
Number of retries, repeat limit	Notifications → General
Plant WiFi, device WiFi (hide / switch off / password)	Notifications → WiFi
Device name and location	Settings → Device name and location
Download / restore settings backup	Settings → Settings backup
Require sign-in to view the panel	Settings → View access
Webhook test and signing key	Settings → Integration (webhook)
Plant password, acknowledgement from other devices	Plant → Plant settings
Restart the device	System → Restart device
Recovery code, full factory reset	Settings (from the device WiFi only)
Return to the setup wizard	Settings

Good practice:

- Define at least **two** administrators; administrators should use 6-digit PINs.
- After adding a person, send a test message and check that it arrives.
- Download a **settings backup** before major changes.
- Enable the outage report: the "system running" message is regular confirmation that the device is working properly.

13 Frequently asked questions

Question	Answer
I receive no notifications	Is the channel enabled in My account? Did you press Start in the Telegram bot? Outside working hours, low-severity alarms are not sent. Your administrator can see the reason in Notifications → Log.
I receive no e-mails	Check the spam folder; add the sender address to your safe senders list.

Question	Answer
I forgot my PIN	Your administrator sets a new PIN on the Users page. An administrator PIN is reset with the recovery code (Installation Guide).
The panel does not open	Is your phone on the plant network? Try the IP address instead of the `.local` address.
The screen shows "Disconnected"	Your phone or computer cannot reach the device: check your network and reload the page.
I cannot see the Acknowledge button	Sign in. If it is still missing, your role is not allowed to acknowledge that input.
The same input alarms too often	The contact may chatter or the signal may be unstable. Your administrator can adjust the signal filtering time (Debounce).
The alarm is acknowledged but the card is red	The condition persists (steady red). It goes out when the fault is cleared.
Are alarms lost if the internet goes down?	No. Monitoring and recording continue; notifications are sent when the connection returns (except those older than 30 minutes, which remain in the Event Log).
Settings after a power cut?	Settings and input names are kept. When the device starts, it reports the outage duration.
What do the lights on the device mean?	Green = running normally, yellow (LED3) = connected to the plant WiFi, yellow (LED2) = storage card working, red = critical error. Details: Installation Guide.
The other device does not appear on the Plant page	Are both devices on the same WiFi network, are the plant passwords the same, and is client isolation (guest network) off on the router?
Nobody woke up for an alarm at night	Review the escalation settings with your administrator; higher levels and times must be defined.
Does Telegram cost anything?	No. The notification account comes ready with the device; each person presses Start in the bot once.
Notifications via WhatsApp or SMS?	Not in this version; the notification channels are Telegram, e-mail, webhook and the web panel.

14 Glossary

Term	Meaning
Acknowledge (ACK)	Confirming that the alarm is being dealt with. The person and response time are recorded and escalation stops
Escalation	Forwarding an unacknowledged alarm to higher levels after set times
Target	The roles and people an input's alarm goes to
Role	A group of people to which permissions are given (e.g. Shift Supervisor)
Severity	The level of the alarm: Info · Warning · Alarm · Critical
Trigger	The change that starts the alarm: rising edge (0→1), falling edge (1→0), both edges
Debounce (signal filtering)	The time an input must stay stable for a change to be counted
NO / NC contact	Normally open / normally closed contact
Inverted Logic	For NC contacts: loss of the signal (including a broken cable) counts as an alarm

Term	Meaning
Latched alarm	An alarm that persists, even if the signal recovers, until acknowledged and reset
Silence	Temporarily stopping repeat notifications; does not close the alarm
Working hours	The hours a person receives notifications; outside them only alarms above the selected severity
Grouped sending	Sending alarms that occur within a few seconds in one message
Outage report	A regular report of power and internet outages; "system running" if there were none
Plant password	Common password entered on all devices on the same network so they recognise each other
Device WiFi	The device's own WiFi network for setup and maintenance
Plant WiFi	The network with internet access that the device joins to send notifications
Recovery code	Device-specific code used to set a new administrator PIN if it is forgotten
Webhook	Automatic sending of events to your server by HTTP POST

Contact
Sales and information: info@ionia-automation.com
Technical support: support@ionia-automation.com
ionia-automation.com