



INDUSTRIAL FAULT ALERTING AND ALARM MANAGEMENT

AS1122

User Manual

Panel-mounted alarm monitoring, notification and on-site warning device ·
16 inputs · 16 outputs



October 2026 · Rev. 1.0

ionia Automation Technologies · ionia-automation.com

Contents

1	Getting started	4
1.1	About this manual	4
1.2	Accessing the panel	4
1.3	Using a phone	4
1.4	Menu and pages	4
1.5	Language, appearance and connection status	5
2	Sign-in, PIN and roles	5
2.1	Signing in	5
2.2	Roles and permissions	5
2.3	View access	5
2.4	My Account	5
3	Dashboard	6
3.1	Input cards	6
3.2	Plant and Outputs summary	6
3.3	Alarm Summary, Quick Actions, System Status	6
4	When an alarm occurs	6
4.1	Notification	6
4.2	Alarm life cycle	7
4.3	Acknowledging	7
4.4	Muting and resetting	8
5	Alarm Monitoring page	8
6	Severity, targets and escalation	8
6.1	Severity levels	8
6.2	Targets	8
6.3	Escalation chain	8
6.4	Acknowledging role	9
6.5	Working hours and minimum severity	9
7	People and notification channels	9
7.1	People	9
7.2	Telegram	9
7.3	E-mail	10
7.4	Notification behaviour	10
7.5	Delivery log	10
8	Inputs: name, condition and filtering	10
8.1	Input settings	10

8.2	Options	10
8.3	Resetting the alarm settings	11
9	Outputs	12
9.1	Output card	12
9.2	Switching on and off by hand	12
9.3	Recent operations (audit trail)	13
9.4	Output settings (⌘ Settings)	13
9.5	Output warnings	13
10	Output rules	14
10.1	Ready-made templates	14
10.2	Setting up a rule	14
10.3	Several conditions: AND, OR, NOT	15
10.4	Another device's alarm	15
10.5	Suppression and maintenance rules: KEEP OFF	15
10.6	Delays	15
10.7	Rule list and states	15
10.8	Rule examples	16
11	Output safety behaviour	16
12	Event Log	17
13	Plant view	17
14	System, backup and administrator tasks	18
14.1	System page	18
14.2	Settings backup	19
14.3	Administrator tasks: where?	19
15	Outages	20
16	Integration	21
16.1	Webhook	21
16.2	Read endpoints	22
16.3	Security	22
17	Frequently asked questions	22
18	Glossary	23

1 Getting started

1.1 About this manual

This manual is for the operators, technicians, shift supervisors and administrators who use the web panel of the Alert SCADA AS1122 every day. Mounting, wiring and initial setup of the device are described in the **Installation Guide**.

The AS1122 monitors **16 digital inputs**, raises alarms and notifies people. It drives its **16 outputs** by hand or automatically with the **output rules** you define: e.g. the workshop siren sounds while there is an unacknowledged alarm, or a fault in another building lights the flasher here.

Life safety

Alert SCADA is a fault alerting device; it does not replace fire detection, gas detection, life-safety or legally required alarm systems. The AS1122 outputs are **for warning and signalling only**; they are not a safety relay, an emergency stop or a machine safety circuit. Emergency stop and life-safety circuits stay in their own safety systems.

Menu, page and button names of the panel are shown in **bold** in this manual. Screenshots are from the Turkish interface.

1.2 Accessing the panel

Open the browser on a phone, tablet or computer connected to the plant network and enter the address given by your administrator:

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

No app needs to be installed. Both addresses are shown as clickable and copyable links in the **Settings** → **WiFi** card and on the **Notifications** → **WiFi** page. The `.local` address does not open on some Android phones; in that case use the IP address.

If the panel does not open

If the panel does not open at all while your phone is connected to the plant WiFi, **client isolation / guest network** may be switched on in the router. Tell your administrator or the IT team.

1.3 Using a phone

- The panel adapts to the phone screen; on a phone, tables are shown as cards one below the other.
- The menu is behind the ☰ button at the top left. The bar at the bottom of the screen always shows the **Home**, **Alarms**, **Plant**, **Outputs** and **Menu** tabs.
- **Add the page to the home screen** from the browser menu; it then opens with one tap.

1.4 Menu and pages

The menu is grouped by topic:

Group	Pages
Monitoring	Dashboard · Plant
Alarms	Alarm Monitoring · Alarm Settings · Event Log
Output control	Outputs · Output Rules
Management	Notifications · Users · System · Settings

- The **Related** row at the top of each page takes you with one tap to the pages used together with it (e.g. **Alarm Monitoring** → **Alarm Settings**).
- In Alarm Monitoring, the  icon next to a channel name (with the settings permission) opens and highlights that channel in Alarm Settings.
- On the Outputs page, tapping the name of the rule that controls an output highlights that rule in Output Rules.

1.5 Language, appearance and connection status

- The panel is available in **Turkish** and **English** (the  button at the top right). The  button switches between light and dark appearance.
- The bottom bar shows whether the panel is connected to the device (**Connected** / **Disconnected**) and the device uptime. The panel updates live; if it says "Disconnected", the information on the screen is not current.
- **Unsaved changes:** if you change a setting that has a Save button and move to another page without saving, you are asked "There are unsaved changes. Save them?": **Save** or **Leave without saving**. If you close the dialog, you stay on the page.

2 Sign-in, PIN and roles

2.1 Signing in

Unless your administrator has chosen otherwise, the panel can be **viewed** without signing in. To acknowledge alarms, operate outputs or change settings, use **Sign in** at the top right → select your name → enter your **PIN**.

- The PIN has 4–6 digits; it is stored on the device in a non-reversible form.
- After 5 wrong PIN attempts you must wait 5 minutes.
- If you are inactive for 30 minutes, the session closes automatically.
- If you forget your PIN, your administrator sets a new one on the **Users** page. The administrator PIN is renewed with the recovery code (Installation Guide).

2.2 Roles and permissions

People are assigned to roles; permissions are given to roles. Example roles: Administrator, Shift supervisor, Technician, Operator. Up to 32 people and 16 roles can be defined.

Permission	Allows
ACK	Acknowledging alarms
Mute	Temporarily stopping repeat notifications of an alarm
Config	Alarm rules, targets, device and notification settings; operating the outputs by hand
Add user	Adding / removing people, assigning roles and PINs
Service (maintenance)	Service settings — authorised service only

Full administrator = Config + Add user. Adding and changing output rules, changing the acknowledging role, setting up the outage report and factory reset are administrator tasks only.

2.3 View access

By default the panel can be viewed without signing in (a PIN is always required to change settings). If the administrator switches on **Settings** → **View Access**, signing in is also required to view the panel.

2.4 My Account

Settings → **My Account** (after signing in). You can only change your own details:

- Full name
- **Where should notifications 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:** outside working hours, only alarms above the severity you select are sent
- **Change PIN** (your current PIN is required)

3 Dashboard

3.1 Input cards

Each of the 16 inputs is shown as a card: input number (00–15), its name and the current state text (e.g. "Compressor running"). **The colour of the card shows the alarm state**, not whether the input is 0 or 1:

Appearance	Meaning	What to do
Red, blinking	Unacknowledged alarm	Check the situation, acknowledge
Red, steady	Alarm acknowledged but the condition persists	Goes off by itself when the fault is cleared
Yellow / orange	Input returned to normal, waiting for acknowledgement	Acknowledge
Blue dot	Input 1, no alarm	—
Green dot	Input 0, no alarm	—

Both Edges inputs

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

Channel details: tap an input card. The current state, recent events, the output rules using this input, and the **Full history** (Event Log filtered to that channel) / **Alarm setting** buttons open.

3.2 Plant and Outputs summary

- **Plant:** how many Alert SCADA devices on the same network are online and how many active and unacknowledged alarms there are in the plant. **Open** → Plant page (Section 13).
- **Outputs:** the current state of the 16 outputs (green = on) and how many output rules are defined / running. Tap the link to open Output Rules.

3.3 Alarm Summary, Quick Actions, System Status

- **Alarm Summary:** numbers of active, acknowledged, returned-to-normal (waiting for acknowledgement) and critical alarms.
- **Quick Actions:** **Acknowledge All**, **Mute**, **Reset**, **Event Log**; below them **Recent alarms**.
- **System Status:** the panel's connection to the device, notification (plant WiFi) status, uptime and **Last outage** (the last power or internet outage, its duration and time span; an ongoing internet outage is shown in red).

4 When an alarm occurs

4.1 Notification

The alarm arrives through the channel set up for you (Telegram and/or e-mail):

```
[KRITIK] Warehouse Building - Dispatch  
Kanal: Compressor Fault (DI03)  
Durum: Compressor stopped  
Zaman: 04.10.2026 14:32:07  
Olay no: 7629
```

The header shows the **severity** (BILGI · UYARI · ALARM · KRITIK = Info · Warning · Alarm · Critical), the device name and location; below are the input, what happened and when. The examples in this manual show the Turkish message labels: Kanal = Channel, Durum = State, Zaman = Time, Olay no = Event no. Alarms arriving within a few seconds are combined into one message ("3 alarms ...").

4.2 Alarm life cycle

Stage	What happens
1. Alarm occurs	The people concerned are notified; the card blinks red on the panel. If defined, an output rule runs (e.g. siren)
2. Acknowledged	You indicate that 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" notification; forwarding to higher levels (escalation) stops. A siren tied to the "unacknowledged alarm" condition stops
3. Condition ends	The input returns to normal. If enabled for the input, a "returned to normal — lasted X min" notification arrives
4. Closed	The alarm closes when it has been acknowledged and its condition has ended

If the condition ends before acknowledgement, the alarm goes to **"Returned to normal — waiting for acknowledgement"** and closes when acknowledged.

An unacknowledged alarm goes to higher levels

An unacknowledged alarm is reported to **higher levels** (e.g. shift supervisor, maintenance lead) at the intervals set by your administrator. Even if the signal returns to normal, an unacknowledged alarm continues to go to the higher levels.

Example "acknowledged" notification (to the other people who received the alarm; not to the person who acknowledged):

```
[ONAYLANDI] Warehouse Building - Dispatch  
Kanal: Compressor Fault (DI03)  
Onaylayan: Shift supervisor  
Alarm başlangıcı: 14:32:07  
Tepki süresi: 1 dk 11 sn  
Durum: Giriş hâlâ alarm konumunda  
Zaman: 04.10.2026 14:33:18
```

ONAYLANDI = Acknowledged, Onaylayan = Acknowledged by, Alarm başlangıcı = Alarm start, Tepki süresi = Response time, "Giriş hâlâ alarm konumunda" = Input still in alarm position.

4.3 Acknowledging

- The **Acknowledge** button in the alarm's row (on a phone, its card) on the **Alarm Monitoring** page, or Dashboard → **Acknowledge All**. An alarm of another Alert SCADA device can be acknowledged from the **Plant** page (Section 13).

- If the acknowledge button is not shown: you are not signed in, your role does not have the acknowledge permission, or the alarm of that input can only be acknowledged by a specific role.
- **Acknowledge All** acknowledges only the alarms you are permitted to acknowledge and tells you how many were skipped.

4.4 Muting and resetting

- **Mute:** temporarily stops repeat notifications of the alarm (Mute permission required). It does not close the alarm.
- **Reset:** **latching** alarms persist, even if the signal recovers, until an authorised person acknowledges them and presses **Reset**.

5 Alarm Monitoring page

The **Active** tab lists alarms waiting for acknowledgement and ongoing alarms (on a phone, each alarm is a card):

Item	Meaning
Channel / Name	Input number (DI00–DI15) and name
Time	Time the alarm occurred
Message	Text of the change that started the alarm (e.g. "Door opened")
Severity	Info · Warning · Alarm · Critical
State	Active · Acknowledged · Returned to normal — waiting for acknowledgement
Acknowledge	Acknowledge and mute buttons

- **Each unacknowledged alarm is a separate row;** acknowledgement, however, is **per input**: the **Acknowledge** button of an input closes all rows of that input together.
- Buttons at the top of the page: **Acknowledge All** · **Mute** · **Reset** · **Test** (test alarm for an authorised person).

6 Severity, targets and escalation

6.1 Severity levels

Every input has a severity. The severity appears in the notification header; people's "minimum severity" and working hours settings and the severity filter of output rules work on it.

Severity	Typical use
Info	Events for the record and for information (e.g. generator running)
Warning	Situations that need attention soon (e.g. door left open)
Alarm	Fault that requires intervention (e.g. fan thermal overload tripped)
Critical	Fault that requires immediate intervention (e.g. compressor stopped)

6.2 Targets

In the **Alarm Settings** → **Targets** table you choose **which roles and people** receive the alarm of each input (Config permission). 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 targets of all inputs.

6.3 Escalation chain

Forwards an unacknowledged alarm to higher levels at set intervals. The **Escalation** button in the input's row:

- 1 Switch on **Use escalation**. The **first notification** is sent at the time of the alarm (filled in from the input's targets).
- 2 **Level 1**: "if not acknowledged, ... min after the previous step" → e.g. Shift supervisor.
- 3 Add up to 3 more levels with **Add level** (4 steps including the first notification; each step with up to 4 roles + 4 people).
- 4 **Save**. To give all inputs the same chain, use **Apply to all inputs** (press twice to confirm).

Example chain: Operator (0 min) → Shift supervisor (+10 min) → Maintenance lead (+20 min) → Plant manager (+30 min).

- The chain stops when the alarm is **acknowledged**. For an auto-acknowledged input it also stops when the signal returns to normal.
- With auto-acknowledge off, an **unacknowledged** alarm continues to go to higher levels even if the signal returns to normal.
- One chain runs per input: new changes arriving while acknowledgement is pending do not restart the chain.
- No level is lost while there is no internet; it is sent when the connection returns.
- "Acknowledged" and "returned to normal" notifications go to **all levels reached** (not to the person who acknowledged).

6.4 Acknowledging role

The last column of the Targets table: the alarm of that input can be acknowledged **only by people in the selected role** and by full administrators. "Everyone" = everyone with the ACK permission. Only a full administrator can change this column.

6.5 Working hours and minimum severity

Set separately for each person (**Users** → **People**, or by the person themselves in **My Account**):

- **Minimum severity**: the person only receives alarms of this severity and above (e.g. plant manager Critical only).
- **Working hours**: outside working hours, only alarms above the selected severity are sent; nobody is woken up at night for minor events.

7 People and notification channels

7.1 People

Users → **People** → **Add person** (Add user permission): 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 person can receive notifications only (without a PIN) or only sign in to the panel.

7.2 Telegram

The device comes ready with the manufacturer's notification account; no separate account or subscription is needed. Each person, once:

- 1 Opens **the device's notification bot** in Telegram and presses **Start**. The link is shown on the **My Account** page and in the setup wizard. The bot cannot send messages to a person who has not done this.
- 2 Finds out their Telegram ID: e.g. opens **@userinfobot**, presses **Start** and copies the **Id** number from the reply.

- 3 Pastes the number into the **Telegram ID** field in **My Account** and saves.

7.3 E-mail

Enter the person's e-mail address and switch the E-mail channel on. The first messages may land in the junk (spam) folder; add the sender address to the safe senders list.

7.4 Notification behaviour

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

7.5 Delivery log

Notifications → **Log:** every notification sent, to whom and through which channel, and the result. For a notification that could not be delivered, the **reason** is given; tap the row to see the full text of the message. **Test** messages can also be sent to each person from here.

8 Inputs: name, condition and filtering

The **Alarm Settings** → **Rules** page has one row per input (Config permission). Changes in the table are written to the device and become permanent when you press **Save**; changed rows are shown in yellow and the button shows how many channels have changed. **Undo** discards unsaved changes.

8.1 Input settings

Setting	Description
Channel Name	Name shown in notifications and on the panel (e.g. "Pump 1 Thermal")
Trigger	Disabled (not monitored) · Rising Edge (0→1 alarm, 1→0 returns to normal) · Falling Edge (1→0 alarm, 0→1 returns to normal) · Both Edges (every 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 bounce and short interference
Severity	Info · Warning · Alarm · Critical
Texts	State texts (for 0 and 1; shown under the input on the panel) and edge messages (the "State:" line in the notification, e.g. "Door opened" / "Door closed")

8.2 Options

Option	Description
Latching	The alarm persists, even if the signal returns to normal, until an authorised person acknowledges and resets it (for signals such as emergency stop or thermal overload)
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 is the alarm, its return is normal. A broken wire also raises an alarm
Log Only	The event is recorded and shown on the panel; no notification is sent

Option	Description
Return 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 frequently)
Acknowledged Notification	When the alarm is acknowledged, the other people who received it get an "acknowledged — by: ..." notification

Both Edges

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

8.3 Resetting the alarm settings

The **Reset Alarm Settings** button resets the rules, names and texts of the 16 inputs; users, notification settings and targets are kept. After the reset, **no input raises alarms**.

9 Outputs

The **Outputs** page shows the 16 outputs (**D000–D015**) and lets you operate them by hand.

The screenshot shows the ION8-1122 SCADA interface. The left sidebar contains navigation options: İzleme (Monitoring), Tesis (Facility), ALARMLAR (Alarms), ÇIKIŞ KONTROLÜ (Output Control), and YÖNETİM (Management). The main area displays the 'Çıkışlar' (Outputs) section. It shows 16 output cards, each with a requested state (İstenen) and an actual state (Gerçek pin). Below the cards is a table of recent operations (Son işlemler).

Süre (s)	Çıkış	İşlem	Kaynak	Sonuç
257	D006 Alarm Panosu	Açık	web	Tamam
257	D002 Kule Lambası Kırmızı	Açık	web	Tamam
256	D000 Atölye Sireni	Açık	web	Tamam

Outputs (Turkish interface): outputs that are on are green; each card shows the requested and actual state and the rule controlling the output; recent operations below.

9.1 Output card

Item / button	Meaning
D003 · name	Output number and the name you gave it (e.g. "Tower Light Yellow")
Continuous / Pulse	Output mode (Section 9.4)
Requested	The state the device requests from the output (On / Off)
Actual pin	The actual state read back from the output. If it differs from the requested state, the card shows a warning ("Requested and actual pin differ")
Rule switches on: ...	The output rule and condition that can switch this output on
On / Off	Switches an output in continuous mode on / off
Pulse	Switches an output in pulse mode on for the set time and releases it
Time remaining	For a timed output, the time left until it switches off
Rate limit: new pulse in ... s	The pulse limit has been reached; a pulse can be given again when the time has elapsed

9.2 Switching on and off by hand

Before giving a command

The outputs operate equipment on site such as sirens, flashers and horns. Before giving a command, make sure the site is safe.

- To operate outputs you must be **signed in** and your role must have the **Config** permission. Without the permission, the buttons are not shown.

- Every **switch-on / pulse** command asks for confirmation. The **Off** command is always accepted.
- The **Release all** button switches all outputs off (asks for confirmation).
- If you switch an output used by an output rule (shown with a blue frame on the Output Rules page) on or off by hand, **your manual command takes effect**; the rule takes control of the output again the next time its own condition changes (e.g. when a new alarm arrives or an alarm is acknowledged). For example, if an operator switches the siren off by hand, the rule does not switch it on again until a new event occurs.

9.3 Recent operations (audit trail)

The **Recent operations** list shows the time, the output, the operation (On / Off / Pulse), the **source** (panel, rule...) and the result of every output command. Output commands are recorded with who / when: you can always see later who switched which output on or off, and when.

9.4 Output settings (⚙ Settings)

Setting	Description
Name	Name shown on the panel, in rules and in records (e.g. "Workshop siren", "Warehouse flasher")
Mode	Continuous: stays on until switched off · Pulse: stays on for the set time and switches off by itself (horn, door release, reset push-button)
Pulse duration (ms)	On time in pulse mode
Maximum on time (s)	Safety limit in continuous mode: when this time has elapsed, the output switches off by itself. 0 = unlimited
On connection loss	If the connection to the output module inside the device is lost: Release (default, output switches off) · Hold (output stays in its last state; can only be selected in continuous mode without a time limit)
Rate limit: count / window (s)	In pulse mode, the maximum number of pulses within a given time (default 3 in 600 s). So that a faulty rule or a wrong press cannot keep the equipment running

Recommendation for sirens

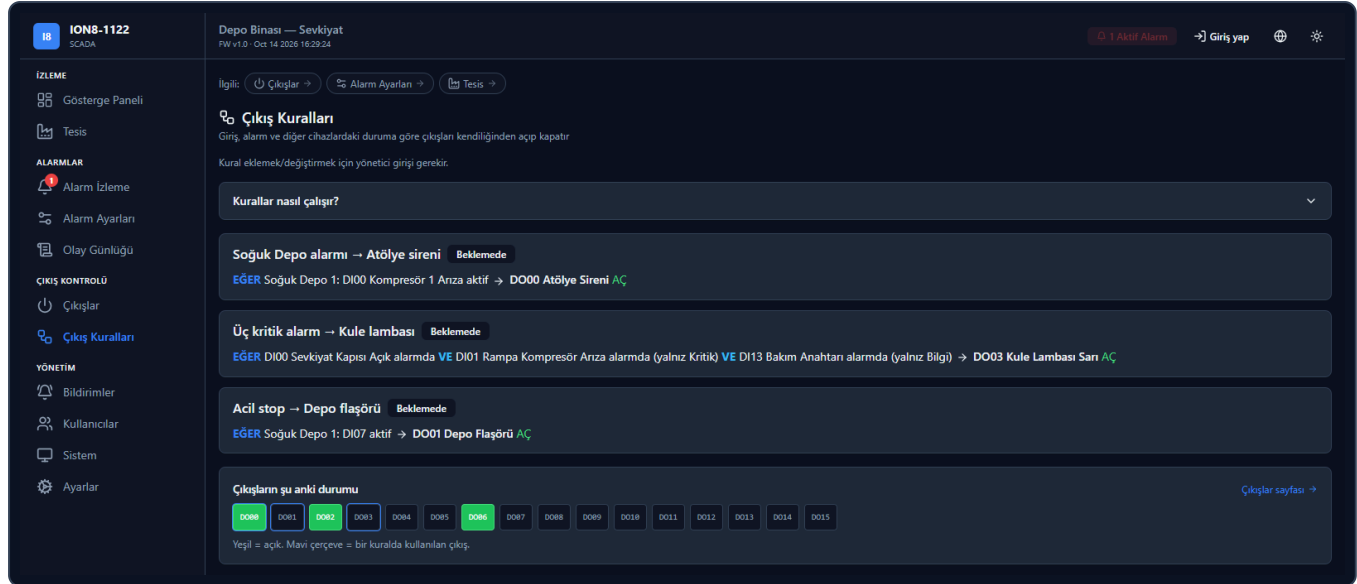
Give sirens and horns in continuous mode a **Maximum on time** (e.g. a few minutes). Then the siren does not sound forever even if nobody can respond; the alarm notification and escalation continue.

9.5 Output warnings

Warning	Meaning and action
Requested and actual pin differ	The output did not reach the requested state. Check the load and the wiring; if it persists, contact service
No connection to output modules	The connection to the output module inside the device has been lost; the outputs have been released to the safe side. If it persists, restart the device; if this does not help, inform service
Software updating — outputs released to the safe side	Authorised service is updating the software; when the device restarts, the outputs are driven again according to the rules
Module fault: D00-7 / D08-15	An output module reports a fault; inform service

10 Output rules

Output rules switch outputs on and off **automatically** according to inputs, alarms and other Alert SCADA devices in the plant. No code or PLC program is needed: a rule reads like a plain sentence, **IF ... THEN**. Adding and changing rules requires an administrator sign-in.



Output Rules (Turkish interface): each rule reads as a plain sentence; below, the current state of the outputs (green = on, blue frame = output used in a rule).

10.1 Ready-made templates

You can pick one of the ready-made templates at the bottom of the page and edit it:

Template	What it does
Unacknowledged alarm → siren	The selected output (siren) stays on while an alarm is waiting for acknowledgement; it stops when acknowledged
Critical alarm → output	Output on while there is an active alarm of Critical severity
Input → output	Output on while an input is active (mirrors the input to the output)
Other device's alarm → output	Output here on while another Alert SCADA device in the plant has an alarm (e.g. a fault in another building lights a lamp here)

10.2 Setting up a rule

- 1 **New rule** → **Rule name** (e.g. "Compressor fault → workshop siren") and **Enabled**.
- 2 **IF** — add one or more conditions (table below).
- 3 **THEN** — select the output and what to do: **ON** or **KEEP OFF**.
- 4 Enter the **delays** if needed (Section 10.6).
- 5 Read the **Summary** line (e.g. "IF DI03 in alarm, at least Alarm → ON DO00 (if it lasts 5 s)") → **Save**.
- 6 **Test the rule on site**: create the condition, check that the output switches on and that it switches off when the condition ends.

Condition	Meaning
Alarm present	Active alarm on the selected input (or on any input)
Unacknowledged alarm present	Lasts until the alarm is acknowledged; the condition is met even after the alarm has ended if it has not been acknowledged
Input active	Selected input is 1
Alarm on other device	Alarm on the selected input of the selected Alert SCADA device in the plant
Other device's input active	The selected input of the other device is 1

Severity filter: limits an alarm condition to alarms of a given severity (e.g. *any severity*, *at least Alarm* = Alarm and Critical, or one specific severity only).

10.3 Several conditions: AND, OR, NOT

- **Add AND condition:** all conditions in the same group must be met. Example: "if three critical alarms are present at once, light the tower lamp".
- **Add OR group:** any one of the groups is enough. Example: "sound the siren if compressor 1 **or** compressor 2 has a fault".
- **not:** inverts the condition. Example: "door open **and** night-mode switch **not** active".

10.4 Another device's alarm

An alarm on one device can drive an output of an AS1122 on the same plant network: without running a cable, a fault in the warehouse lights the lamp in the gatehouse. Both devices must see each other on the Plant page (same network, same plant password; Section 13).

If messages stop arriving

A condition based on another device counts as not met if no message has arrived from that device for **6 seconds**. This way the output does not stay stuck on when the connection is lost.

10.5 Suppression and maintenance rules: KEEP OFF

If **KEEP OFF (block)** is selected in the **THEN** part, the rule suppresses all other rules that want to switch this output on, as long as its condition is met. Example: "the siren must not sound while the maintenance switch is on". If one rule says **ON** for an output and another says **KEEP OFF**, **KEEP OFF** wins.

10.6 Delays

- **Condition must last at least ... seconds:** short pulses do not switch the output on (e.g. the siren sounds only if the alarm lasts 5 seconds).
- **Stay on for ... seconds after the condition ends:** e.g. the flasher stays on for another 30 seconds after the alarm ends.

Both delays are at most 3600 seconds.

10.7 Rule list and states

State	Meaning
Running	The rule is switching the output on right now
Waiting for delay	The condition is met; waiting for the delay to elapse
Idle	The condition is not met

State	Meaning
Off	The rule is not enabled

In the **Current state of the outputs** row at the bottom of the page, green = on and a blue frame = output used in a rule.

Limits: up to **16 rules**; per rule up to 8 conditions, 4 OR groups and 4 outputs; up to 4 different other devices across all rules. Rule and output settings are permanent; they are not lost when the power fails.

10.8 Rule examples

Need	Rule
Sound the workshop siren if the compressor fails; stop it when acknowledged	IF DI03 unacknowledged alarm present → ON DO00 Workshop siren
Light the tower lamp if three critical alarms are present at once	IF DI00 alarm AND DI01 alarm AND DI02 alarm (Critical only) → ON DO03 Tower lamp
The siren must not sound during maintenance	IF DI13 Maintenance switch input active → KEEP OFF DO00 Workshop siren
A fault in the cold store lights the flasher in dispatch	IF alarm on other device (Cold Store 1, DI00) → ON DO01 Warehouse flasher
Short contacts must not sound the siren	Delay: condition must last at least 5 s

11 Output safety behaviour

The AS1122 outputs are designed to be safe: an output only switches on with an authorised and current command.

All off at start-up

When the device starts, all outputs start switched off; the rules then drive the outputs again according to the conditions. Outputs switched on by hand start switched off.

Off command always works

The Off command and Release all are never rejected.

Safe state on a problem

If the internal device connection is lost, during a software update and during a power failure, the outputs are released (switched off); they do not stay stuck on.

No endless siren

Maximum on time, pulse rate limit and the 6-second rule for other devices; every operation is recorded.

Situation	What the outputs do
Device starting (first power-up, restart)	All outputs start switched off; the rules drive them again according to the conditions
Off / Release all command	Always accepted
Internal connection to the output module lost	The output is released (switched off). Only a continuous output without a time limit set to Hold stays in its last state. When the connection returns, the output does not switch on by itself
Software update	All outputs are released; after the restart they are driven according to the rules
Power failure	The device does not operate; all outputs switch off. Settings and rules are kept

Situation	What the outputs do
No message from another device for 6 s	The condition based on that device counts as not met; the output does not stay on
Maximum on time of a continuous output elapsed	The output switches off by itself
Pulse rate limit reached	No new pulse until the window has elapsed
One rule says ON, another KEEP OFF	KEEP OFF wins

The outputs are not a safety circuit

The safe behaviour of the outputs is intended to prevent warning equipment from operating by itself; it is not a safety function. Emergency stop and life-safety circuits stay in their own safety systems. During a power failure the outputs are off: if the warning equipment must also work during an outage, supply the device and the equipment from a **UPS-backed line**.

12 Event Log

- All input changes, alarms, acknowledgements, panel sign-ins and settings changes are recorded **with date and time** and who made them.
- Alarm rows show the person who acknowledged, the response time and how long the alarm lasted.
- Power and internet outages and device restarts are also included in the log.
- Use the buttons at the top to select **All** · **Last 1 hour** · **Last 24 hours** · **Last 7 days**; filter with **Filter**. Tap a channel name to open the details of that channel.

Olay Günlüğü						
<div> Tümü Son 1 saat Son 24 saat Son 7 gün Filtre </div>				167 olay		
Zaman	Kanal	Kenar	Mesaj	Önem	Olay No	İşaretler
2026-10-14 17:01:31.400	Su Baskını	✓ Onay	Operatör · alarm 16:57:19 · 4 dk 12 sn sonra onaylandı			
2026-10-14 17:00:16.032	Pompa 1 Arıza	✓ Onay	Operatör · alarm 16:56:58 · 3 dk 17 sn sonra onaylandı			
2026-10-14 16:57:19.205	Su Baskını	↑ Yükselme	▲ Onaylayan: Operatör (4 dk 12 sn sonra onaylandı)	Alarm	1964	0x80
2026-10-14 16:57:18.550	Su Baskını	Ayar	Test alarmı — Operatör			
2026-10-14 16:56:58.836	Pompa 1 Arıza	↑ Yükselme	▲ Onaylayan: Operatör (3 dk 17 sn sonra onaylandı)	Kritik	1963	0x80
2026-10-14 16:56:58.232	Pompa 1 Arıza	Ayar	Test alarmı — Operatör			

Event Log (Turkish interface): alarm, acknowledgement and settings events, with the person who acknowledged and the response time.

Recording card

If a recording card is fitted and working in the device (LED2 on the front panel is on), the history is stored permanently and you can look back by selecting a date. Without a recording card, the log is kept only while the device is running; recent events are deleted on restart (alarms, notifications and settings are not affected).

13 Plant view

If there are several Alert SCADA devices (AS1111, AS1122) on the same plant network, the **Plant** page shows all of them on one screen.

The screenshot displays the ION8-1122 SCADA interface. The top bar shows the system name 'Depo Binası — Sevkiyat' and the version 'FW v1.0 - Oct 14 2026 16:29:24'. The left sidebar contains navigation options: İzleme (Monitoring), Tesis (Facility), Alarmlar (Alarms), Çıkış Kontrolü (Output Control), and Yönetim (Management). The main area shows a list of alarms for 'Tesis alarmları'. The list includes columns for Cihaz (Device), Giriş (Input), Önem (Severity), and Durum (Status). Below the list, there are two device cards: 'Depo Binası (bu cihaz)' and 'Soğuk Depo 1'. Each card shows a status bar with '1 aktif alarm' and '1 onay bekliyor', a grid of input/output status, and a 'Çıkışlar (yeşil = açık)' section.

Plant (Turkish interface): the alarms of all devices in one list; below, a card for each device with its inputs and outputs.

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 Unacknowledged only switch filters the list
Device cards	Name, location and model of each device, whether it is online; its inputs and outputs. 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). If it says "remote acknowledgement off", the administrator of that device has disabled acknowledgement from other devices; if it says "device not visible", the device cannot be reached at the moment.
- The links on the device cards work while the phone or computer is on the plant network.
- For the devices to see each other, all of them must be connected to **the same plant WiFi network, client isolation must be off** on the router, and **the same plant password** must be entered on all of them (administrator: **Plant** → **Plant settings**).
- If a device that was seen before has not been seen for **2 minutes**, the page shows a warning and possible causes (device off, different network, client isolation); if packets arrive but the plant password differs, it says so separately. A device that has been removed permanently is cleared with the **remove from list** button in the warning.

14 System, backup and administrator tasks

14.1 System page

The **System** page shows the device status: uptime, WiFi connection, memory, the status of internal device connections and the **Boot history** (the cause of the last 16 start-ups — power outage, planned restart or software error — the previous uptime and start-up times; not deleted by a factory reset).

Restart device: settings are kept; the panel is disconnected for about 1 minute; the outputs switch off during the restart and are then driven again according to the rules. Attach a screenshot of this page when contacting service.

14.2 Settings backup

Settings → Settings backup (administrator):

- **Download backup:** roles, people, alarm targets and escalation, input names and texts, **output settings and output rules**, notification settings, outage report, device name and plant settings are downloaded into one file. Optional: people's contact details and the plant WiFi. **PINs are never included in the backup.**
- **Restore:** you can select the sections one by one. Rules referring to another device are not restored if that device is not in this plant. You can also load the same configuration into a new device.

Take a backup before important changes; store the file securely (it may contain contact details and the WiFi password).

14.3 Administrator tasks: where?

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
Output name, mode, times, behaviour on connection loss	Outputs → ⚙ Settings
Output rules	Output Rules
Outage report (frequency, recipients)	Notifications → Outage report
Notification delivery log, test message	Notifications → Log
Plant WiFi, device WiFi (hide / 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; Installation Guide)
Return to the setup wizard	Settings

Good practice:

- Define at least **two** administrators; administrators should use 6-digit PINs.
- Change the plant password during setup and enter the same one on all devices.
- **Test every output rule on site** after setting it up.
- Download a **settings backup** before important changes.

15 Outages

Situation	What the device does	What you see
Internet down	Continues to monitor the inputs, run the output rules and record; holds back notifications. Communication with other Alert SCADA devices on the same network (Plant, rules based on other devices) also works without the internet	When the internet returns, the held notifications arrive with a "... min delayed" note, followed by an "Internet was down for X min..." summary. Notifications older than 30 minutes are not sent (the events remain in the Event Log)
Power failure	Does not operate; inputs are not monitored, outputs switch off . Settings, rules and input names are kept	When power returns, the device starts and the output rules drive the outputs again according to the conditions. A "Device restarted: power outage ~X min ... Inputs were not monitored during this time." notification arrives. Inputs that went into the alarm state during the outage raise an alarm at start-up
Report did not arrive	—	If the outage report is on, a "system running" message or an outage report arrives at the expected time. If not, check the device's power and internet connection

- When the internet returns, the device checks that the internet is really available (at most 90 seconds), then sends the held notifications. No message is sent for interruptions shorter than 1 minute with no alarm in between.

Clock

The AS1122 has no battery-backed clock; the time is taken from the internet. After a power failure, the device waits for the time from the internet (at most 3 minutes) so that it can report the outage duration. If there is no internet, the start-up notification is sent without the duration once the internet returns.

Outage report (Notifications → Outage report, full administrator): select the report frequency (hourly ... weekly), time / day and recipients. All power and internet outages in the selected period are reported; if there was no outage, a **"system running"** message is sent. This message regularly confirms that the device is running and can reach you. Default: off.

UPS recommendation

During a power failure the device cannot monitor the inputs and the outputs are off. For uninterrupted monitoring and warning, supply the device and the warning equipment from a **UPS-backed line**.

16 Integration

AS1122 events can be passed to your own software (ERP, CRM, maintenance / work order system, SCADA, display) in two ways. This section is an overview; detailed integration information for your IT team can be requested from technical support.

Need	Method	Direction
Open a work order in the ERP / a record in the CRM when an alarm occurs, update it when acknowledged / ended	Webhook	Device → your server (HTTP POST, JSON)
Current status on a display or in a report	Read endpoints	Your software → device (HTTP GET, JSON)
Event history, outage history, state of outputs and rules	Read endpoints	Your software → device

Writing settings from outside, **operating outputs**, acknowledging alarms or adding people are not part of the integration; these are done only from the web panel with a PIN-protected user session. If outputs need to switch according to a condition, use the device's own **Output Rules**.

16.1 Webhook

The webhook is defined 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 a PIN (it will not sign in to the panel).
- 2** Tick only **Webhook** among the notification channels; enter your server's address in the **URL** field (max. 127 characters).
- 3** Add the person or their role to the targets of the inputs to be monitored (**Alarm Settings → Targets**). To send everything, leave the minimum severity at **Info** and the working hours empty.
- 4** Test with **Send** after entering the address in the **Settings → Integration (webhook)** card; the screen should show "Webhook OK 200".
- 5** For signing (recommended), use **Create key** in the same card. The key is shown **only once**; enter it in your receiving system.

Request	POST, Content-Type: application/json, UTF-8 JSON body
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; your server must return a 2xx status code
Failure	The same notification is retried for this person and channel (0–5 times). The same event may arrive twice: de-duplicate with <code>channel + event_id + type</code>
Event types (type)	alarm · escalation · ack · normal · system · test
Main fields	device, location, channel (0–15), channel_name, state, severity (INFO · WARNING · ALARM · CRITICAL), event_id, time, subject, text

Signature (optional)	HMAC-SHA256; the timestamp and signature arrive in request headers. The receiver verifies them over the raw body
No internet / network	The notification is held and sent when the connection returns; held notifications older than 30 minutes are not sent

To also receive system notifications (device restarted, internet outage summary, outage report), add the webhook person to one of the system alarm roles.

16.2 Read endpoints

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

Endpoint	Content
<code>/api/status</code>	Device summary: model, name, location, serial number, uptime, number of active alarms
<code>/api/alarms</code>	Inputs that are not normal and their alarm states
<code>/api/events?since=</code>	Recent events; only new ones with <code>since</code>
<code>/api/outages</code>	Last 32 power / internet outages and last 16 start-ups
<code>/api/do</code>	Requested and actual state of the outputs, modes, remaining times, module faults
<code>/api/logic</code>	List of output rules and their current state
<code>/api/device</code> · <code>/api/alarm/rules</code> · <code>/api/stats</code> · <code>/api/peers</code>	Device information · input names and rules · daily counters · other devices in the plant

If **View Access** is on, all endpoints except `/api/status` and `/api/stats` require a PIN-based session. For the integration, define a separate person and role with monitoring rights only.

16.3 Security

- The web panel and the read endpoints use **HTTP** (unencrypted). Use the device only on a trusted plant network and do not expose it to the internet (no port forwarding). If remote access is needed, use a VPN.
- The webhook body contains people's names and plant information. If the receiving server is outside the plant, use an **HTTPS** address and switch on webhook signing.

17 Frequently asked questions

Question	Answer
I do not receive notifications	Is the channel switched on 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
The output buttons are not shown	Sign in; your role must have the Config permission
I switched an output on and it switched off by itself a few seconds later	The output is in pulse mode or its maximum on time has elapsed; or the condition of the rule controlling the output changed in the meantime (blue frame on Output Rules)
Pulse not possible: "Rate limit"	The number of pulses allowed in the set time has been reached; wait for the time shown on the card or ask the administrator to change the limit

Question	Answer
A rule does not work	Is the rule Enabled ? If its state is "Waiting for delay", the delay has not elapsed. Is there another rule blocking the same output (KEEP OFF)?
The alarm was acknowledged but the siren is still sounding	The siren rule may be tied to "Alarm present" rather than "Unacknowledged alarm present": it sounds as long as the alarm condition lasts. Review the rule with your administrator
I switched the siren off by hand; will the rule switch it on again?	Not immediately. The rule takes control of the output again the next time its condition changes (new alarm or acknowledgement)
A condition based on another device does not work	Is that device shown on the Plant page? Same network, same plant password and client isolation off on the router are required
Will the siren sound if the internet is down?	Yes. Input monitoring, output rules and rules between devices on the same network also work without the internet; only notifications are held back
What happens after a power failure?	Settings, rules and names are kept; outputs start switched off and are driven again according to the rules. Outputs you switched on by hand start switched off
I forgot my PIN	Your administrator sets a new PIN on the Users page. The administrator PIN is renewed 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 <code>.local</code> address
What do the lights on the device mean?	Green (LED4) = running correctly · yellow LED3 = connected to the plant WiFi · yellow LED2 = recording card working · red LED1 = critical error. Details: Installation Guide
Can I use it instead of a fire / gas alarm system?	No. Alert SCADA is a fault alerting device; it does not replace life-safety systems. The outputs are for warning and signalling only

18 Glossary

Term	Meaning
Input (DI)	Monitored contact signal; DI00–DI15
Output (DO)	Output driving warning equipment such as a siren, flasher or lamp; DO00–DO15
Acknowledgement (ACK)	A person indicating that they are dealing with an alarm; their name and response time are recorded
Escalation	Forwarding an unacknowledged alarm to higher levels at set intervals
Severity	Level of the alarm: Info · Warning · Alarm · Critical
Latching alarm	Alarm that persists, even if the signal recovers, until acknowledged and reset
Debounce (signal filtering)	Time the input must stay stable so that short bounce and interference do not raise alarms
Inverted Logic	For NC contacts: loss of the signal counts as the alarm
Continuous / Pulse mode	The output stays on until switched off / stays on for a set time and switches off
Requested / Actual pin	The state the device requests from the output / the actual state read back from the output
Output rule	IF ... THEN rule that drives an output according to a condition
KEEP OFF	Rule that prevents an output from switching on as long as its condition is met (e.g. maintenance)

Term	Meaning
Plant	Page showing all Alert SCADA devices on the same network together
Plant password	Common password entered on all devices of a plant so that they recognise each other
Webhook	Automatic sending of events to your server (HTTP POST, JSON)
Recovery code	Device-specific code for setting a new PIN when the administrator PIN is forgotten



Contact

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