



INDUSTRIAL FAULT ALERTING AND ALARM MANAGEMENT

AS1122

Installation Guide

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



Contents

1	About this guide and safety	4
1.1	About this guide	4
1.2	Safety instructions	4
2	Product overview	5
2.1	What the AS1122 does	5
2.2	Device and front panel	5
2.3	Device label	6
3	Mounting	6
3.1	Choosing the location	6
3.2	Mounting in the panel	6
4	Electrical connection	7
4.1	General rules	7
4.2	Power supply	7
4.3	Inputs	7
4.4	Outputs	7
4.5	Before switching on	8
5	First start-up and setup wizard	9
5.1	Switching on	9
5.2	Connecting to the device WiFi	9
5.3	Setup wizard	9
5.4	Test message	10
5.5	Recovery code	10
6	Network connection	11
6.1	Plant WiFi	11
6.2	Accessing the panel from the plant network	11
6.3	Device WiFi and its password	11
6.4	IT and firewall requirements	12
7	People and notifications	13
7.1	Roles and permissions	13
7.2	Adding people	13
7.3	Notification account and Telegram	13
7.4	E-mail	14
7.5	Targets and escalation	14
7.6	Test and delivery log	14
8	Commissioning the inputs	14

9	Commissioning the outputs	15
9.1	Naming and testing the outputs by hand	15
9.2	First output rule	15
9.3	Field test	16
10	Several devices: Plant	16
11	Backup, factory reset and recovery	17
11.1	Settings backup	17
11.2	Factory reset	17
11.3	If the administrator PIN is forgotten	17
11.4	If the device WiFi password is forgotten	17
11.5	Software update	18
12	Front panel: LEDs and buttons	18
12.1	Status LEDs	18
12.2	Buttons	18
13	Troubleshooting	19
14	Technical data (summary)	20
15	Commissioning checklist	20
16	Warranty and support	21

1 About this guide and safety

1.1 About this guide

This guide is for the technical staff who mount the Alert SCADA AS1122 in the control panel, make the electrical connections and complete the initial setup. Day-to-day use (alarm monitoring, acknowledging, output rules) is described in the **User Manual**.

Product	Alert SCADA AS1122 — 16 digital inputs, 16 digital outputs
Intended for	Electrical / automation staff who mount, wire and commission the device; IT staff
Related documents	User Manual · Datasheet · Warranty Certificate

Menu, page and button names of the panel are shown in **bold** in this guide (e.g. **Alarm Settings** → **Rules**). The panel is available in Turkish and English.

Notice boxes used in this guide:

Danger

Ignoring this may endanger people or property.

Warning

Ignoring this may damage the device or the plant, or an alarm may be missed.

Note

Information that makes your work easier.

1.2 Safety instructions

Life safety

Alert SCADA is a fault alerting device. **It does not replace fire detection, gas detection, life-safety or legally required alarm systems** and does not hold the certifications of such systems.

The AS1122 outputs are **for warning and signalling only** (sirens, flashers, tower lights, horns). The outputs 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.**

- Mounting and electrical connection must be carried out by **authorised electrical personnel** in accordance with the applicable wiring regulations.
- Wire **only with the power off**: the device supply, the signal voltage on the inputs and the supply of the loads connected to the outputs must all be switched off.
- Supply, input and output values must not exceed the limits given in this guide (Section 4 and Section 14).
- Mount the device **inside a dry, dust-free control panel**.
- During a power failure and in the event of an internal device fault, the outputs are **released (switched off)**. The selection, protection and safe operation of the equipment connected to the outputs are the user's responsibility.
- Delivery of notifications depends on the power supply, the internet connection and third-party services (Telegram, e-mail). In critical plants, supply the device from a line backed by an **uninterruptible power supply (UPS)** and consider a backup communication path.
- Do not open the housing. The parts inside cannot be replaced by the user; opening the housing voids the warranty.

2 Product overview

2.1 What the AS1122 does

The AS1122 continuously monitors 16 contact signals in your control panel (pump fault, thermal overload trip, door, level switch, machine stop, etc.). When a signal goes into the alarm state, it notifies the people concerned and, if you wish, warns people on site with a siren, flasher or tower light.

Monitors

16 digital inputs (DI00–DI15), 1 ms scan. Normally open and normally closed contacts.

Notifies

Several people at once via Telegram and e-mail. Acknowledgement, who responded and when, and escalation of unacknowledged alarms.

Warns on site

16 outputs (DO00–DO15): sirens, flashers, tower lights, horns. An authorised person switches them on and off by hand, or they work automatically with no-code IF ... THEN rules.

Records

All events, acknowledgements and output commands with date, time and person. Power and internet outages with their duration.

The device is not tied to a cloud: settings and records stay inside the device. The internet is used only to send notifications and to synchronise the clock. No app is installed for setup or use; the browser on a phone, tablet or computer is all you need.

2.2 Device and front panel



Front panel: four status LEDs and three buttons; the connection terminals are on the top and bottom edges of the housing.

Part	Description
Status LEDs (4)	From left to right LED1 red, LED2 yellow, LED3 yellow, LED4 green. Show that the device is running, that it is connected to the plant WiFi, and the recording status (Section 12)
Buttons (3)	Left, middle and right button. For restarting without a computer (Section 12)
Terminals	Screw terminal blocks: supply, inputs and outputs (Section 4)
Label	Serial number, device WiFi details and QR codes (Section 2.3)

2.3 Device label

Note down the label details before installation; you will need them during setup and service.

Item	Example	Purpose
Serial number	ION8-1122-YYAA-NNNN	Warranty and service record
Device WiFi name	ION8B00T_XXXXXX	Initial setup and maintenance connection
Device WiFi password	Printed on the label	First connection; change it after setup (Section 6.3)
Panel address	http://192.168.4.1	Panel address while connected to the device WiFi
QR codes	1 · 2 · small QR	1: connects the phone to the device WiFi · 2: opens the panel in the browser · small QR: serial number

Model code

On the device label and in the top corner of the panel the model code appears as **ION8-1122**; this code refers to the Alert SCADA AS1122.

3 Mounting

3.1 Choosing the location

- Mount the device **inside a dry, dust-free control panel**. The housing offers partial protection against dust; it is not protected against water.
- The device connects to the plant network via **WiFi**. **A metal enclosure weakens the WiFi signal**: before mounting, check with a phone, with the enclosure door closed, that the plant WiFi is strong enough inside the enclosure. If the signal is weak, use a WiFi access point close to the enclosure.
- Choose a position where the front-panel LEDs and buttons can be seen and reached easily when the enclosure door is opened.
- Leave enough space in front of the terminals for wiring.

3.2 Mounting in the panel

- Mount the device **with screws on a flat surface** (panel mounting plate). There are 4 mounting holes of Ø3.8 mm; hole centres are **80.4 × 104.1 mm** apart.
- Tighten the screws without straining the housing.
- Before wiring, check that the front panel and the terminals are easy to reach.

Mechanical	Value
Mounting	Screw mounting on a flat surface, inside a control panel
Mounting holes	4 × Ø3.8 mm, centre-to-centre 80.4 × 104.1 mm
Dimensions	115 × 114 × 45 mm (excluding mounting lugs and connectors)
Weight	250 g

4 Electrical connection

4.1 General rules

Wire with the power off

Make all connections with the device supply, the input signal voltage and the supply of the output loads **switched off**. Do not connect or disconnect terminals while the supply is on.

- The terminals are screw terminals. Fit ferrules to stranded conductors; tighten the screws and check by pulling the wire gently.
- Route signal cables separately from power cables as far as possible.
- Note which terminal belongs to which channel as you wire; you will verify every input and output on the panel at first start-up (Section 8 and Section 9).

4.2 Power supply

Supply voltage	24 V DC nominal, operating range 15–30 V DC
----------------	---

- Supply the device from the 24 V DC source in the control panel. Observe the polarity.
- For uninterrupted monitoring, take the supply from a **UPS-backed** line. During a power failure the device does not operate, cannot monitor the inputs and all outputs switch off; when power returns it reports the duration of the outage (User Manual).
- If warning equipment connected to an output (e.g. a siren) must also work during a power failure, supply both the device and that equipment from a UPS-backed line.

4.3 Inputs

Number of inputs	16 digital inputs (2 × 8), shown on the panel as DI00 – DI15
Input type	PNP, 24 V DC : the input becomes active (1) when +24 V is applied; at least 15 V for logic 1
Isolation	Optically isolated, 2500 V
Can be connected	Dry contacts (relay contact, switch, push-button), sensors with PNP output

- **Dry contact**: connect one side of the contact to 24 V DC and the other side to the input. When the contact closes, the input becomes 1.
- **Normally open (NO) contact**: the input becomes 1 when the contact closes. Select "Signal on (0→1)" as the alarm condition.
- **Normally closed (NC) contact**: the input is normally 1; it becomes 0 when the contact opens or **the wire breaks**. In circuits where a broken wire must also raise an alarm, use an NC contact and the input's **Inverted Logic** option (Section 8).

Unused inputs

Set unused inputs to **Disabled** on the panel (all inputs are Disabled when shipped from the factory). This prevents a floating input from raising alarms due to interference.

4.4 Outputs

Number of outputs	16 digital outputs (2 × 8), shown on the panel as DO00 – DO15
-------------------	--

Output type	Sourcing (PNP) transistor output; protected against overcurrent and overtemperature
Output voltage	Follows the supply voltage (when the output is on, the supply voltage is applied to the load)
Output current	Max. 100 mA per output
Intended use	Warning and signalling: sirens, flashers, tower lights, horns, interposing relay coils
At start-up	All outputs start switched off
During a power failure / fault	Outputs are released (switched off)

- When on, the output applies the supply voltage to the load (sourcing). Connect one side of the load to the output and the other side to the 0 V of the supply.
- DC warning lamps, interposing relay coils and PLC / signal inputs drawing **no more than 100 mA** can be connected directly.
- Do not connect sirens, flashers, tower lights or 230 V AC warning equipment **drawing a higher current** directly: drive a **suitable interposing relay or contactor** from the output and supply the load through that relay's contact.
- Choose the connected equipment so that it stays in a safe state when the output is off (power failure, device fault, software update). Do not connect a load to an AS1122 output if switching it off would create a hazard.

The outputs are not a safety circuit

Do not use the AS1122 outputs in emergency stop, machine safety or life-safety circuits. These circuits stay in their own certified safety systems. The AS1122 outputs are for warning and signalling only.

4.5 Before switching on

✓	Check
☐	Supply voltage within 15–30 V DC, polarity correct
☐	Input contacts connected to the correct channels; contact type (NO / NC) noted
☐	Output loads do not exceed 100 mA; larger loads via interposing relays
☐	Connected equipment is safe when off; no output connected to a safety circuit
☐	Terminal screws tight, wires do not come out when pulled

5 First start-up and setup wizard

5.1 Switching on

- 1 Check the connections and switch on the power. At start-up **all outputs are off**.
- 2 The LEDs first light up one after another, then show the status (Section 12). If the green LED blinks slowly during the first minute, the device is still starting; wait.
- 3 After about **1 minute** the device's own WiFi network (`I0N8B00T_XXXXXX`) appears.

5.2 Connecting to the device WiFi

- 1 Scan **QR code 1** on the label with a phone, or select the **device WiFi name** from the WiFi list of the phone / computer. Enter **the password printed on the label**.
- 2 On most phones a **"Sign in to network"** notification appears as soon as you connect and the device panel opens automatically. If the phone warns "No internet on this network", choose **stay connected**.
- 3 If the panel does not open by itself, open **http://192.168.4.1** in the browser or scan **QR code 2** on the label.

When is the device WiFi on?

Once the device is connected to the plant network, the device WiFi switches off by default. It switches on again for the first 10 minutes after every power-up and when the plant network is lost (Section 6.3).

5.3 Setup wizard

As long as no administrator exists on the device, the panel opens with the **setup wizard**. Every step can be skipped; you can return to the wizard later from the **Settings** page. Until setup is complete, a "Setup not complete" warning is shown in the top bar.

Step	What you do	Recommendation
1. Administrator	Full name and PIN (4–6 digits)	6-digit PIN for administrators
2. Device	Device name and location ; shown in the header of every notification	E.g. "Warehouse Building" / "Dispatch"
3. Plant WiFi	Network with internet access for notifications (2.4 GHz only); the clock is also taken from the internet	Section 6.1
4. Inputs	Name and alarm condition for the inputs in use: Off · Signal on (0→1) · Signal off (1→0) · On every change	Detailed settings in Section 8
5. Notification recipients	Telegram ID and/or e-mail address of the people who will receive alarms	Section 7
6. Test message	A test message to each person; answer the "Did it arrive?" question	Section 5.4
7. Done	Setup summary and recovery code	Write the code down and keep it in a safe place

Initial setup only via the device's own WiFi

Settings cannot be changed from the plant network until an administrator is defined. This prevents someone else on the network from taking over a device that has not been set up.

The wizard does not configure the outputs. Naming, testing and rules for the outputs are described in Section 9.

5.4 Test message

In step 6 of the wizard, a test message is sent to each person and you are asked whether it arrived. For a channel that did not deliver, follow the hint on the screen: for Telegram the person must have pressed **Start** in the notification bot; for e-mail check the junk (spam) folder (Section 7). The test message can be sent again at any time from the **Notifications** → **Log** page.

5.5 Recovery code

Each device has its own 12-character **recovery code**. If the administrator PIN is forgotten, a new PIN is set with this code (Section 11.3). The code does not change even after a full factory reset.

- **To view it:** while connected to the device WiFi, sign in as administrator → **Settings** → **Recovery Code** → **Show code**.
- **If someone else has obtained the code:** in the same place, **Generate new code**; the old code becomes invalid.

Keep the recovery code

Write the code down and keep it in a safe place together with the device documents. If both the code and the administrator PIN are lost, the only way to sign in to the panel as administrator is a full factory reset.

6 Network connection

6.1 Plant WiFi

To send notifications and synchronise the clock, the device must be connected to a WiFi network with internet access.

- 1 **Notifications** → **WiFi** (or step 3 of the setup wizard) → **Scan Networks** → select the network → enter the password → **Connect**.
- 2 Once connected, the device's address on the plant network is shown on the screen; LED3 (yellow) lights up.

2.4 GHz only

The device connects only to **2.4 GHz** networks; 5 GHz is not supported. If your router uses the same name for 2.4 and 5 GHz and you have connection problems, set up a separate name for 2.4 GHz.

If the saved network cannot be found, the device retries at first frequently, then less often (at most every 5 minutes).

6.2 Accessing the panel from the plant network

Once the device is connected to the plant WiFi, **two addresses** for reaching the panel are shown as clickable and copyable links: **Notifications** → **WiFi** (connection status card), the WiFi and "Done" steps of the setup wizard, and the **Settings** → **WiFi** card. From a phone or computer on the same network:

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

Some Android phones cannot resolve **.local** names; in that case use the IP address.

Device network name (.local). Can be changed in the **Notifications** → **WiFi** → **Network address** card. Only lower-case letters, digits and hyphens are allowed (max. 32 characters; it cannot start or end with a hyphen). Turkish characters are converted automatically (ş→s). If left empty, the automatic name (**ion8-xxxxxx**) is used. Do not give two devices on the same network the same name.

IP address: Automatic / Static. The default is **Automatic** (the router assigns the address, which may change over time). If **Static IP** is selected, enter the IP address, subnet mask, gateway and DNS; the "Use current address" button fills in the fields with today's address. When saving, the device checks the network for the address and does not save it if another device is using it. The device checks the address again every time it connects: if the address is in use by another device or the network has changed, it switches to Automatic IP by itself and shows a warning at the top of the panel.

Recommended

Setting up a **DHCP reservation** for the device on the router / DHCP server keeps the address fixed and is the most reliable way. In plants with several devices or an integration, give every device a fixed address.

6.3 Device WiFi and its password

In **Notifications** → **WiFi** → **Device WiFi** you choose how the device's own WiFi network behaves:

Option	Behaviour
Off while connected to the plant network (default)	On for the first 10 minutes after every power-up, in setup mode, while someone is connected to the device, and when the plant network has been lost for more than 30 seconds; off at other times
Always on	The device WiFi broadcasts continuously

Option	Behaviour
Hidden	The network name does not appear in the list; anyone who knows the name can connect

Change the device WiFi password

The password on the label is for initial setup. **Always change it after setup** and record the new password:

Notifications → **WiFi** → **Device WiFi** → **Device WiFi password** (also available in the WiFi step of the setup wizard). A warning is shown on the panel until the password is changed.

- The password is 8–63 characters long; only English letters, digits and symbols are allowed. The factory password from the label and easily guessed passwords are not accepted.
- If you change the password while connected to the device WiFi, the connection drops after a few seconds; reconnect with the new password.
- If the computer keeps trying the old password and shows an error, **Forget** the network in the WiFi list, then connect with the new password (on a phone: forget / remove network).
- If the password is forgotten: Section 11.4.

6.4 IT and firewall requirements

The device only makes **outbound** connections; no inbound connections to the device (port forwarding) are needed.

Service	Destination	Port
Telegram notification	api.telegram.org	TCP 443 (HTTPS)
E-mail notification	Sending server (manufacturer default or your own server)	TCP 465 (SSL)
Clock synchronisation	NTP servers	UDP 123
Name resolution	Your network's DNS server	UDP/TCP 53
Webhook (if used)	Your server	Port in the address (HTTP / HTTPS)

Local network requirements. For access to the panel from phones / computers and for the devices to see each other (Plant page, output rules based on another device):

- The devices and the phones / computers used to open the panel must be on **the same network** (same router, same address range).
- **Client isolation must be off** on the router / access point (AP isolation, client isolation, "guest network"). If it is on, the panel does not open from phones and the devices cannot see each other; Telegram and e-mail notifications are not affected. On a corporate network, ask the IT team for an exception for the Alert SCADA devices (the device's MAC address is shown on the Plant page).
- Communication between devices uses **UDP 48230** local broadcast; local broadcasts must not be blocked. The packets are signed with the plant password (Section 10).
- For `.local` addresses, mDNS (UDP 5353) must pass on the network; if it does not, use the IP address.

Do not expose the panel to the internet

The web panel uses unencrypted HTTP. Use the panel only on a **trusted plant network**; do not set up port forwarding. If remote access is needed, use a VPN.

7 People and notifications

7.1 Roles and permissions

- **Person:** a user who can sign in to the panel with a PIN and/or receives notifications (max. **32** people).
- **Role:** a group of people to which permissions are given (max. **16** roles; e.g. Administrator, Shift supervisor, Technician, Operator). Alarms are routed to roles or to individual people.

On the **Users** → **Roles** page, each role is given the following permissions:

Name in the interface	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. Some operations (changing the acknowledging role, outage report settings, factory reset) can only be performed by a full administrator.

At least two administrators

Define at least **two** administrators with a PIN; administrators should use 6-digit PINs. The device does not allow the last administrator to be deleted.

7.2 Adding people

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 address, **minimum severity** (e.g. receive Critical only) and **working hours** (outside working hours, only alarms above the selected severity are sent).

- The PIN has 4–6 digits and is stored on the device in a non-reversible form.
- After 5 wrong PIN attempts, sign-in for that person is locked for 5 minutes. The session closes after 30 minutes of inactivity.
- Everyone can change their own PIN, Telegram / e-mail details and working hours on the **Settings** → **My Account** page.

New people and alarm targets

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 changed again.

7.3 Notification account and Telegram

The device comes **ready with the manufacturer's notification account:** a Telegram notification bot and an e-mail sender are already set up; no separate account or subscription is needed.

For Telegram, each person does the following once, on their own phone:

- 1 Opens **the device's notification bot** in Telegram and presses **Start**. The link to the bot is shown in the setup wizard and on the **My Account** page. The bot cannot send messages to a person who has not done this (Telegram rule).

- 2 Finds out their Telegram ID: e.g. opens **@userinfobot**, presses Start and copies the **Id** number from the reply.
- 3 Enters the number in the person's **Telegram ID** field (**Users** → **People**, or the person themselves in **Settings** → **My Account**).

7.4 E-mail

Fill in the person's **e-mail** field and switch the E-mail channel on. The first messages may land in the junk (spam) folder; ask the recipients to add the sender address to their safe senders list. If you want to use your own e-mail server, contact the authorised service.

7.5 Targets and escalation

- In the **Alarm Settings** → **Targets** table you choose which roles and people receive the alarm of each input.
- An unacknowledged alarm is forwarded to higher levels at the intervals set in the input's **Escalation** setting: up to **4 steps** including the first notification, each step with up to 4 roles + 4 people. Example: Operator (0 min) → Shift supervisor (+10 min) → Maintenance lead (+20 min). The intervals are your setting.
- Details: User Manual, "Severity, targets and escalation".

7.6 Test and delivery log

- **Notifications** → **Log**: send a **test** message to each person. All deliveries, their results and any error reasons are shown here.
- 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).

8 Commissioning the inputs

The **Alarm Settings** → **Rules** page has one row per input. Changes are written to the device when you press **Save**.

- 1 Give every input in use a clear **Channel Name** (e.g. "Compressor 1 Fault"); this name appears in notifications and on the panel.
- 2 Select the **Trigger: Rising Edge** for an NO contact (0→1 alarm); **Falling Edge**, or an NC contact with **Inverted Logic**, if loss of the signal is the alarm; **Both Edges** for inputs that should notify opened / closed. Leave unused inputs **Disabled**.
- 3 Select the **Severity** (Info · Warning · Alarm · Critical) and, if needed, enter a **Debounce** value (signal filtering, 0–10 000 ms).
- 4 Trigger every input **physically** on site: check on the panel that the correct channel changes in the correct direction and that the notification arrives.

All input options (latching alarm, auto-acknowledge, return-to-normal notification, texts) are described in the User Manual.

9 Commissioning the outputs

Site safety first

Before testing the outputs, make sure that operating the connected equipment will not endanger anyone. Inform the staff on site before testing sirens and flashers.

9.1 Naming and testing the outputs by hand

To operate the outputs you must be signed in and your role must have the **Config** permission.

- 1 On the **Outputs** page, press the **Settings** button of each output in use and give it a **Name** (e.g. "Workshop siren", "Warehouse flasher").
- 2 Select the **Mode: Continuous** (stays on until switched off) or **Pulse** (stays on for a set time and then switches off; e.g. a horn or a reset push-button). In continuous mode you can set a **Maximum on time** for safety.
- 3 Test the output with **On / Off (Pulse in pulse mode)**. Every switch-on command asks for confirmation.
- 4 Check that the **Requested** and **Actual pin** states on the card match and that the correct equipment operates on site. If they differ, the card shows a warning; check the wiring.

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 page (Turkish interface): name, requested and actual state of each output, the rule controlling it; recent operations below.

9.2 First output rule

For the outputs to work automatically according to alarms, rules are set up on the **Output Rules** page (administrator sign-in required). The quickest way is to pick one of the ready-made templates:

Template	What it does
Unacknowledged alarm → siren	The 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

Template	What it does
Other device's alarm → output	Output here on while another Alert SCADA device in the plant has an alarm

Read the rule's **Summary** line and press **Save**. All rule options are described in the User Manual.

9.3 Field test

Test every output rule on site after setting it up:

- Create the condition (e.g. trigger the input); check that the output switches on.
- Acknowledge the alarm or end the condition; check that the output switches off.
- If there is a maintenance / suppression rule (KEEP OFF), check that the output does not switch on while it is active.
- Test a power failure: switch the device off and on; check that all outputs start switched off and that the rules then drive the outputs again according to the conditions.

10 Several devices: Plant

If there are several Alert SCADA devices (e.g. AS1111 and AS1122) on the same plant network, the **Plant** page shows all of them and their alarms on one screen. An alarm on one device can drive an output of another AS1122 (e.g. a fault in the warehouse lights the lamp in the gatehouse). No server or cloud is needed; communication between devices also works without the internet.

- 1 Connect all devices to **the same plant WiFi network**; make sure **client isolation is off** on the router (Section 6.4).
- 2 On each device, open **Plant** → **Plant settings** as administrator and enter **the same plant password on all devices**. Until the password is changed, the page shows the warning "Plant password is at factory value".
- 3 Check on the Plant page that all devices are shown as **online**.
 - Devices only accept packets from devices that know the same plant password.
 - If you do not want this device's alarms to be acknowledged from other devices, switch off acknowledgement from other devices in **Plant settings**.
 - If a device that was seen before has not been seen for 2 minutes, the Plant page shows a warning and possible causes (device off, different network, client isolation, different plant password). A device that has been removed permanently is cleared with the **remove from list** button in the warning.

11 Backup, factory reset and recovery

11.1 Settings backup

Settings → **Settings backup** (administrator):

- **Download backup:** roles, people, alarm rules, targets and escalation, input names and texts, **output settings and output rules**, notification settings, outage report, device name and plant settings are downloaded into a single `.json` file. People's contact details and the plant WiFi are included only if the corresponding boxes are ticked. **PINs are never included.**
- **Restore:** select the file → tick the sections → **Restore selected**. Can also be used in setup mode when setting up a new device; give the new people their PINs on the **Users** page. Output rules referring to another device are not restored if that device is not in this plant.

Protect the backup file

The backup file may contain the WiFi password and people's contact details; store it securely. Take a backup at the end of commissioning and before important changes.

11.2 Factory reset

Operation	Where	Deleted	Kept
Reset alarm settings	Alarm Settings	Input rules, channel names, texts, active alarms	People, notification settings, targets
Full factory reset	Settings (administrator only, from the device WiFi only)	People, PINs, roles, targets, notification and WiFi settings, alarm rules; optionally the event log. The device WiFi password reverts to the one on the label	Device identity, software, recovery code, device name

After resetting the alarm settings

After the alarm settings are reset, **no input raises alarms**; set up the inputs again.

When handing over the device or sending it for service

First take a settings backup, then perform a **full factory reset** with **"Also delete event log"** ticked; personal data is deleted from the device.

11.3 If the administrator PIN is forgotten

- 1 Connect to the device WiFi (if needed, power-cycle the device and use the first 10 minutes).
- 2 **Sign in** → **I forgot my PIN** → select the administrator account → enter the **recovery code** and the new PIN.
- 3 No other settings change; the operation is written to the Event Log.

Recovery is not possible from the plant network (physical proximity to the device is required). After 5 wrong code attempts there is a 5-minute wait.

11.4 If the device WiFi password is forgotten

- If the device is connected to the plant network, sign in to the panel from the plant network as administrator and set a new password in **Notifications** → **WiFi** → **Device WiFi**.

- If the panel cannot be reached either from the plant network or from the device WiFi, contact technical support (support@ionia-automation.com); have the serial number ready.

11.5 Software update

Updates are carried out by **authorised service** over WiFi. Packages are signed by the manufacturer; the device rejects unsigned or corrupt packages. New software only becomes permanent after it has been verified to run correctly.

During the update all outputs are released (switched off); when the device restarts, the outputs are driven again according to the rules. Settings and records are kept during an update.

12 Front panel: LEDs and buttons

12.1 Status LEDs

When the device is powered up or restarted, only the green LED lights for a few seconds. Then the LEDs light up one after another (about 5 seconds) and then show the status:

LED	Colour	On	Off
LED4	Green	Device is running correctly	There is a critical problem (see LED1)
LED3	Yellow	Device is connected to the plant WiFi	No plant WiFi or not set up (notifications are not sent)
LED2	Yellow	Recording card fitted and working	No recording card or it cannot be read
LED1	Red	Critical error: the device's two processors cannot communicate or memory is at a critical level	No critical error

- If the **green LED blinks slowly** during the first minute after start-up, the device is still starting; wait.
- **If LED1 is on**, restart the device (Section 12.2). If it persists, contact authorised service.
- While an operation is performed with the buttons, the LEDs show its progress; when it finishes, they return to the status display.

12.2 Buttons

Operation	How	Result
Restart	Hold the middle button for 10 seconds	The device restarts; settings are kept. Outputs switch off during the restart

A restart can also be performed from the panel: **System** → **Restart device** (the panel is disconnected for about 1 minute; outputs switch off during the restart). A full factory reset is performed from the panel (Section 11.2).

13 Troubleshooting

Symptom	Possible cause	Solution
Device WiFi not visible	Device is connected to the plant network and in "off while connected" mode	Power-cycle the device; it is visible for the first 10 minutes. Or sign in to the panel from the plant network
Panel does not open from the plant network	You are on a different network / <code>.local</code> is not resolved	Be on the same network; try the IP address
Connected to the plant network but the panel does not open with the IP address either	Client isolation / guest network on the router	Switch isolation off or connect the device and the phone to the main network; on a corporate network ask IT for an exception (Section 6.4)
"Initial setup only from the device's own WiFi..."	No administrator defined	Connect via the device WiFi and complete the wizard
Does not connect to the plant WiFi	5 GHz network, wrong password, weak signal	Select a 2.4 GHz network; check the password; improve the signal (metal enclosure)
Telegram message does not arrive	Bot not started, wrong ID, channel off	Section 7.3; check the error reason in Notifications → Log
E-mail does not arrive	Spam folder, wrong address	Check the spam folder and the address; check the Log
Some people do not receive messages	Outside working hours + low severity; person not a target	The person's working hours / severity setting and the input's targets
An input never raises an alarm	Input Disabled, wrong trigger direction, wiring	Alarm Settings → Rules ; watch the input state on the Dashboard
The same input raises alarms too often	Contact bounce / interference	Increase the debounce time; use "Return to Normal — at least ... s"
Output shown on but the equipment does not work	Wiring, load supply, interposing relay	Compare Requested and Actual pin on the card; check the load side
"Requested and actual pin differ" warning	Problem in the output circuit, overload	Check the load current (max. 100 mA); if it persists, contact service
"No connection to output modules"	Internal device connection lost; outputs released to the safe side	Restart the device; if this does not help, contact service
"Module fault: DO0-7 / DO8-15"	An output module reports a fault	Contact service
Plant page: "... device not seen for 2 minutes"	Device off, different network or client isolation	Check the causes in the warning one by one
Plant page: "plant password ... differs"	Different plant passwords on the devices	Enter the same password on all devices in Plant → Plant settings
The device restarts by itself	Supply problem	Check the supply; pass the reason in System → Boot history on to service
LED1 (red) is on	Critical error	Restart the device; if it persists, contact service
"Setup not complete" warning does not go away	Administrator, notification recipient or plant WiFi missing	Settings → Setup wizard

When contacting service, have ready: the serial number, a screenshot of the **System** page and when the problem started.

14 Technical data (summary)

Item	Value
Supply	24 V DC nominal, 15–30 V DC
Digital inputs	16 (DI00–DI15); PNP, 24 V DC (logic 1 $\geq$ 15 V); optically isolated, 2500 V
Input scan	1 ms; signal filtering 0–10 000 ms per input
Digital outputs	16 (DO00–DO15); sourcing (PNP) transistor, output voltage follows the supply; max. 100 mA per output
Output modes	Continuous (optional maximum on time) · Pulse (set duration, rate-limited)
Output safe state	Outputs off at start-up, during software updates, on internal connection loss and during power failures
Output rules	Up to 16 rules; per rule 8 conditions, 4 OR groups, 4 outputs
Communication	WiFi 2.4 GHz 802.11 b/g/n (no 5 GHz); client on the plant network + own access point. No Ethernet / cellular
Notification	Telegram · E-mail · Webhook · web panel
Users	Up to 32 people, 16 roles; 4–6-digit PIN per person
Clock	Synchronised from the internet (no battery-backed clock)
Mounting	Screw mounting on a flat surface, inside a control panel; 4 × Ø3.8 mm
Dimensions / weight	115 × 114 × 45 mm / 250 g
Terminals	Screw terminals
Housing	For mounting inside a control panel; partial protection against dust, not protected against water
Warranty	24 months from the invoice date

15 Commissioning checklist

✓ Check
☐ Supply, input and output connections made; output loads do not exceed 100 mA
☐ Label details (serial number, device WiFi name) recorded
☐ Device WiFi password changed , new password recorded
☐ Administrator created; second administrator defined
☐ Recovery code kept in a safe place
☐ Device name and location entered
☐ Connected to the plant WiFi; panel opens from the plant network; device given a fixed address
☐ Inputs in use named, unused inputs Disabled
☐ Every input triggered physically ; correct channel and correct direction seen on the panel

✓ Check
☐ People added; Start pressed in the Telegram bot; test messages received
☐ Targets and (if needed) escalation set up; an alarm acknowledged and the "acknowledged" notification seen
☐ Outputs named and tested by hand; requested and actual state match
☐ Output rules set up and tested on site (switch-on, switch-off, suppression rules)
☐ If there are several devices: same plant password on all devices, all online on the Plant page
☐ (Recommended) Outage report switched on
☐ Settings backup downloaded and handed over to plant management
☐ Users given the User Manual and the panel address

16 Warranty and support

- **Warranty:** 24 months from the invoice date, against defects in materials and workmanship. The warranty is registered under the serial number. The terms are in the Warranty Certificate supplied with the product.
- Installation and use contrary to the guides, supply / input / output values outside the limits, overvoltage, water, humidity, impact, unauthorised opening of the housing and outages of third-party services (internet, Telegram, e-mail) are not covered by the warranty.
- **When requesting support,** have ready: the serial number (device label), the invoice, a description of the fault and, if possible, a screenshot of the **System** page. Before sending the device for service, take a settings backup and perform a full factory reset.

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



Contact

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