



INDUSTRIAL FAULT ALERTING AND ALARM MANAGEMENT

AS1111

Installation Guide

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



Contents

1	About this guide	4
1.1	Safety instructions	4
2	Product overview	4
2.1	What it does	4
2.2	What's in the box	5
2.3	Front panel	5
2.4	Device label	5
3	Mounting and electrical connection	6
3.1	Mounting	6
3.2	Power supply	6
3.3	Inputs	6
4	Network connection	7
4.1	Device WiFi	7
4.2	Plant WiFi	8
4.3	Accessing the panel from the plant network	8
4.4	IT and firewall requirements	8
5	First start-up and setup wizard	9
5.1	Powering up	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	Notification contacts	10
6.1	Notification account	10
6.2	Adding people	11
6.3	Telegram	11
6.4	E-mail	11
6.5	Notification log and retries	11
7	Configuring and testing inputs	11
8	Multiple devices: Plant view	12
9	Maintenance	13
9.1	Settings backup and restore	13
9.2	Factory reset	13
9.3	If the administrator PIN is forgotten	13

9.4	If the device WiFi password is forgotten	13
9.5	Software updates	14
9.6	Storage card	14
10	Front panel: lights and buttons	14
10.1	Status lights	14
10.2	Buttons	14
11	Troubleshooting	15
12	Technical data	16
13	Commissioning checklist	17
14	Warranty and support	17

1 About this guide

This guide is for the technical staff who mount the Alert SCADA AS1111 in the control panel, make the electrical connections and complete the initial setup. Day-to-day use of the device (alarm monitoring, acknowledgement, people, alarm rules, event log) is described in the **AS1111 User Manual**.

The following signs are used in this guide:

Danger

If ignored, people may be harmed.

Warning

If ignored, the device or the plant may be damaged, or an alarm may be missed.

Note

Information that makes your work easier.

The web 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.

The device label, the serial number and the device's network names carry the product family's technical code **ION8** (e.g. serial number ION8-1111-...). The panel screens may also show the model as ION8-1111.

1.1 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. For systems such as a fire alarm panel, only the fault output may be monitored, for information purposes.

- Mounting and electrical connection must be carried out by **qualified electrical personnel** in accordance with the applicable wiring regulations.
- Wiring is done only with the **power switched off**. Supply and input voltages must not exceed the limits given in this guide (Section 12).
- Mount the device **inside a dry, dust-free control panel**.
- 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 (including the storage card) cannot be replaced by the user; opening the housing voids the warranty.

2 Product overview

2.1 What it does

The AS1111 continuously monitors **up to 32 contact signals** in your plant (pump fault, thermal overload trip, door, level switch, pressure switch, machine stop, emergency stop, UPS and generator signals). When a signal enters the alarm state, the device:

Notifies

Sends the alarm to the people you define via Telegram and/or e-mail and, if required, to your ERP or maintenance software.

Waits for acknowledgement

Shows the alarm in the web panel. An authorised person acknowledges it; the name and response time are recorded.

Escalates

Forwards an unacknowledged alarm to the next level (shift supervisor, maintenance manager) after the times you set.

Records

Logs every event with date and time and reports power and internet outages.

The device is not connected 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; a browser on a phone, tablet or computer is enough.

The AS1111 has **no outputs**. To drive a siren, beacon or stack light, use the **AS1122** model of the same family (16 digital inputs + 16 digital outputs). If there is an AS1122 in the same plant, alarms from the AS1111 can also drive the AS1122's outputs (Section 8).

2.2 What's in the box

- AS1111 device (internal storage card fitted and ready)
- Quick Start card
- Warranty Certificate

2.3 Front panel



AS1111 front: four status LEDs, three buttons and terminal blocks

The front has **four status lights (LEDs)** and **three buttons** (a middle button and two side buttons). Anyone who opens the panel door can see from the lights that the device is running, connected to the plant network and recording.

LED	Colour	When lit
LED4	Green	Device running normally
LED3	Yellow	Connected to the plant WiFi
LED2	Yellow	Storage card working
LED1	Red	Critical error

The buttons allow a restart and a full factory reset without a computer. Details: Section 10.

Signal and supply wiring is connected to the **pluggable screw terminals** on the top and bottom edges of the device.

2.4 Device label

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

Item	Example	Purpose
Serial number	ION8-1111-2610-0001	Warranty and service record
Device WiFi name	ION8B00T_xxxxxx	Initial setup and maintenance connection

Item	Example	Purpose
Device WiFi password	Printed on the label	Factory password; change it during setup (Section 4.1)
Panel address	<code>http://192.168.4.1</code>	Panel address while connected to the device WiFi
QR codes	1 Connect to WiFi · 2 Open panel · small code: serial no.	1: connects the phone to the device WiFi; 2: opens the panel in the browser

Label information

The factory password on the label can be read by anyone with physical access to the device. Change the device WiFi password as soon as setup is complete and keep the new password in a safe place.

3 Mounting and electrical connection

3.1 Mounting

- The device is **screwed onto a flat surface inside the control panel**: 4 holes of Ø3.8 mm, hole centres 80.4 × 104.1 mm apart. The housing measures 115 × 114 × 45 mm (excluding mounting lugs and connectors).
- Leave enough space above and below the device for cable entry and for unplugging the pluggable terminals.
- The device communicates over WiFi. **A metal enclosure weakens the WiFi signal**: before installation, check with a phone that the plant WiFi is strong enough inside the panel. If necessary, use a WiFi access point close to the panel.

3.2 Power supply

Item	Value
Supply voltage	24 V DC nominal, operating range 15–30 V DC
Terminals	Pluggable, 5.08 mm pitch; conductor cross-section 0.2–2.5 mm²

- Take the supply from the 24 V DC power supply in the panel; check the polarity before connecting.
- For uninterrupted monitoring, the supply should come from a **UPS-backed line**. During a power cut the device does not run and cannot monitor its inputs; when power returns it reports the outage duration (Section 9 and User Manual).

Warning

Plug in or remove terminals only with the power off. Voltages above 30 V DC can damage the device.

3.3 Inputs

The AS1111 has **32 digital inputs**, arranged in four terminal blocks of 8 (A, B, C, D from left to right) and numbered **DI00 – DI31** in the panel.

Item	Value
Input type	PNP, 24 V DC : the input becomes 1 when +24 V is applied (at least 15 V for logic 1)
Isolation	Optically isolated inputs, 2500 V
Suitable for	Dry contacts, relay contacts, switches, PNP-output sensors
Scan	1 ms; per-input adjustable signal filtering 0–10,000 ms

A dry contact is wired between +24 V and the input terminal: when the contact closes, +24 V reaches the input and the input becomes 1.

- **Normally open (NO)** contact: the input becomes 1 when the contact closes. Suitable for contacts that close on a fault (e.g. a thermal overload fault contact, a flood contact).
- **Normally closed (NC)** contact: the input becomes 0 when the contact opens **or the cable breaks**. In circuits where a broken cable must also raise an alarm, use an NC contact and the **Inverted Logic** option in the panel.

Example signal	Contact	Alarm condition in the panel
Pump thermal overload fault	NO (closes on fault)	On signal (0→1)
Level switch: water level low	NC (normally closed)	On signal loss (1→0) or Inverted Logic
Panel door opened / closed	NO or NC	On every change
Emergency stop pressed	NC	On signal loss (1→0) or Inverted Logic

Unused inputs

Set unused inputs to **Disabled** in the panel so that a floating input does not cause spurious alarms. All inputs are Disabled when the device leaves the factory.

After wiring, trigger each input in turn and check that the correct channel changes in the correct direction in the panel (Section 7).

4 Network connection

The AS1111 uses two WiFi networks: the **device WiFi** it broadcasts itself, for setup and maintenance, and the **plant WiFi** it joins to send notifications. There is no Ethernet or cellular connection. At sites without WiFi (e.g. a pumping station), a 4G router can be installed on site.

4.1 Device WiFi

The device broadcasts its own WiFi network under the name printed on the label (ION8B00T_XXXXXX). Initial setup can only be done from this network.

Its behaviour is selected under **Notifications** → **WiFi** → **Device WiFi**:

Option	Behaviour
Off while connected to the plant network (default)	On for the first 10 minutes after each power-up, in setup mode, while someone is connected to it, and when the plant network has been lost for more than 30 seconds; off at other times
Always on	The device WiFi broadcasts continuously
Hidden	The network name does not appear in the list; anyone who knows the name can connect

Change the device WiFi password. The factory password is printed on the label and must be changed after setup: **Notifications** → **WiFi** → **Device WiFi** → **Device WiFi password** (also available in the WiFi step of the setup wizard).

- The password has 8–63 characters, using only English letters, digits and symbols. The factory password and 12345678 are not accepted. A warning is shown in the panel until the password is changed.
- If you change it while connected to the device WiFi, the connection drops after 3 seconds; reconnect with the new password.
- If the computer keeps trying the old password, **forget** the network in the WiFi list, then connect with the new password (on a phone: forget / remove network).
- Record the new password. If it is forgotten: Section 9.4.

4.2 Plant WiFi

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

- 1 Open **Notifications** → **WiFi** (or the WiFi step of the setup wizard).
- 2 Press **Scan networks**, select the network, enter the password and press **Connect**.
- 3 Once connected, the device's address on the plant network is shown on screen; note it down.

2.4 GHz only

The device connects only to **2.4 GHz** (802.11 b/g/n) 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, first frequently and then at longer intervals (at most every 5 minutes).

4.3 Accessing the panel from the plant network

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

- **http://ion8-xxxxxx.local** (or the name you assigned, e.g. **http://press-line-2.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.

Network name (.local). Changed on the **Network address** card under Notifications → WiFi. Only lowercase letters, digits and hyphens are allowed (at most 32 characters; it cannot start or end with a hyphen). Turkish characters are converted as you type (ş → s). If left empty, an automatic name 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 the fields with the current address. When saving, the device checks whether the address is already used by another device on the network and does not save it if it is. If the address is later taken by another device or the network changes, the device switches back to Automatic IP by itself and shows a warning at the top of the panel.

Recommendation

The most reliable way to keep the address fixed is a **DHCP reservation** for the device on the router or DHCP server.

4.4 IT and firewall requirements

The device only makes **outbound** connections. No inbound connections or port forwarding are required.

Service	Destination	Port
Telegram notification	api.telegram.org	TCP 443 (HTTPS)
E-mail notification	Sending server	TCP 465 (SSL)
Time synchronisation	NTP servers	UDP 123
Name resolution	Your network's DNS server	UDP/TCP 53

Local network requirements. For access to the panel from phones and computers and for devices to see each other (Plant page):

- The devices and the phones or 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 or access point (AP isolation, client isolation, "guest network"). If it is on, the panel cannot be opened from a phone and the devices cannot see each other; Telegram and e-mail notifications are not affected. On a corporate network, ask your IT team for an exception for the devices (the device's MAC address is shown on the Plant page).
- Device-to-device communication uses local broadcast (**UDP 48230**); local broadcasts must not be blocked.
- `.local` addresses require mDNS (**UDP 5353**) on the network; otherwise use the IP address.

Do not expose the panel to the internet

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

5 First start-up and setup wizard

5.1 Powering up

- 1 Check the supply and input wiring, then switch on the power.
- 2 For a few seconds only the green LED is lit, then the LEDs light up in sequence (about 5 seconds).
- 3 After about **40 seconds** the device's own WiFi network (`ION8B00T_XXXXXX`) appears.

5.2 Connecting to the device WiFi

- 1 Scan **QR code 1** on the label with the phone camera, or select the **device WiFi name** from the label in the WiFi list and 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 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.

Note

By default, the device WiFi switches off once the device is connected to the plant network. It comes back on for the first 10 minutes after each power-up and whenever the plant network is lost (Section 4.1).

5.3 Setup wizard

As long as the device has no administrator, 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 completed" 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. "Press Line 2" / "Welding Shop"
3. Plant WiFi	2.4 GHz network with internet access; device WiFi password	Section 4
4. Inputs	Name and alarm condition for the inputs in use: Off · On signal (0→1) · On signal loss (1→0) · On every change	Unused inputs Off
5. Notification contacts	Telegram ID and/or e-mail address of the people who receive alarms	Section 6
6. Test message	Test message to each person; answer the "Did it arrive?" question	Section 5.4
7. Finish	Setup summary, panel addresses and recovery code	Write down the code and keep it safe

Initial setup only from the device WiFi

Without an administrator, settings cannot be changed from the plant network. This prevents a device that has not been set up from being taken over by someone else on the network.

5.4 Test message

In step 6 of the wizard a test message is sent to each person and you are asked "Did it arrive?". For a channel that did not deliver, follow the hint on screen; the most common causes are not pressing **Start** in the bot on Telegram, a wrongly entered Telegram ID, and e-mail ending up in the spam folder (Section 6).

After setup you can also send a test message to each person from **Notifications** → **Log**.

5.5 Recovery code

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

- **To view it:** while connected to the device WiFi, sign in as administrator → **Settings** → **Recovery code** → **Show code**.
- **If the code has been compromised:** in the same place, **Generate new code**; the old code becomes invalid.
- How to use it: Section 9.3.

Warning

Write down the recovery code and keep it in a safe place, separate from the device. Anyone with the code and physical access to the device can reset the administrator PIN.

6 Notification contacts

6.1 Notification account

The device comes **ready with the manufacturer's notification account**: a Telegram notification bot and an e-mail sender are already set up. You do not need to open an account or pay a subscription. The sender name of the e-mails is your device name. If you want to use your own e-mail server, contact authorised service.

6.2 Adding people

Users → **People** → **Add person** (administrator):

- Full name and role(s)
- PIN (if the person will sign in to the panel)
- Notification channels: **Telegram** · **E-mail** · **Panel**
- Telegram ID and/or e-mail address
- **Minimum severity** (e.g. receive Critical only) and **working hours** (outside working hours only alarms above the selected severity are sent)

Up to 32 people and 16 roles can be defined. Roles, permissions and alarm targets are described in the User Manual.

Note

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.

6.3 Telegram

Done once per person, on the person's own phone:

- 1 Open the **device's notification bot** using the link under **Settings** → **My account** → **Telegram** in the panel (or the link in the setup wizard) and press **Start**. The bot cannot send messages to anyone who has not done this (Telegram rule).
- 2 In Telegram, open **@userinfobot** and press **Start**; copy the **Id** number from the reply.
- 3 Enter the number in the person's **Telegram ID** field (Users → People; or the person themselves under Settings → My account).

6.4 E-mail

Fill in the person's **e-mail** field and enable the E-mail channel. The first messages may land in the spam folder; ask recipients to add the sender address to their safe senders list.

6.5 Notification log and retries

- **Notifications** → **Log**: every notification sent, its recipient, channel and result, and the error reason if it could not be sent. Test messages are also sent from here.
- A notification that could not be delivered to a person on one channel is retried only for that person and channel (Notifications → General: number of retries 0–5). It appears in the log as e.g. "[retry 1]".

7 Configuring and testing inputs

The wizard only sets a name and an alarm condition for each input. Detailed settings are on the **Alarm Settings** → **Rules** page (severity, signal filtering, state texts, latched alarm, auto-acknowledge, inverted logic, back-to-normal notification). They are all described in the User Manual. During commissioning, do at least the following:

- Give every input in use a name that is clear on site (e.g. "Pump 1 Thermal"); set unused ones to **Disabled**.
- Enable **Inverted Logic** for inputs with NC contacts.
- Increase the **Debounce** (signal filtering) time for contacts that chatter (float switch, pressure switch).
- Set the **severity** (Info · Warning · Alarm · Critical) of each alarm.
- In the **Alarm Settings** → **Targets** table, set who receives each alarm and, if needed, the escalation.
- Press **Save** after making changes; changes in Alarm Settings are not written to the device until Save is pressed.

Physical test. Trigger each input on site, one by one (close / open the contact). Check in the panel that the correct channel changes in the correct direction and that the notification reaches the right people. Acknowledge one alarm and check that the other people receive the "acknowledged" notification.

8 Multiple devices: 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 panel's **Plant** page shows all of them and their alarms on one screen. An authorised person can also acknowledge another device's alarm from here. No server, cloud or internet connection is needed for this.

For the devices to see each other:

- 1 Connect all devices to **the same plant WiFi network**; make sure client isolation (guest network) is off on the router (Section 4.4).
- 2 On each device, as administrator, enter **the same plant password** under **Plant → Plant settings**. Communication between devices is signed with this password; devices only listen to devices that know the same password.
- 3 If required, enable or disable **acknowledgement from other devices** in the same section.

If a previously seen device is not seen at all for **2 minutes**, the Plant 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. For a device that has been removed permanently, the administrator uses the **remove from list** button in the warning.

Together with an AS1122. If there is an AS1122 in the same plant, alarms from the AS1111 can be used as conditions in the AS1122's output rules; for example, a fault in the warehouse switches on a lamp in the security gatehouse. Output rules are set in the AS1122's own panel (AS1122 manuals).

The screenshot shows the ION8-1122 SCADA interface. The top bar indicates 'Depo Binası — Sevkiyat' and 'FW v1.0 Oct 14 2026 16:29:24'. The left sidebar contains navigation options: İzleme, Gösterge Paneli, Tesis, ALARMLAR, ÇIKIŞ KONTROLÜ, and YÖNETİM. The main area displays 'Tesis alarmları' for 'Depo Binası' and 'Soğuk Depo 1'. The alarms are listed in a table with columns: Cihaz, Giriş, Önem, and Durum. The status bar at the top right shows '0.1 Aktif Alarm' and 'Giriş yap'. The bottom section shows a detailed view of the 'Depo Binası' and 'Soğuk Depo 1' devices, including their status and a list of active alarms.

Cihaz	Giriş	Önem	Durum
Soğuk Depo 1	D100 Kompresör 1 Arıza	Kritik	Aktif - onay bekliyor
Soğuk Depo 1	D101 Kompresör 2 Arıza	Kritik	Aktif - onay bekliyor
Soğuk Depo 1	D104	Kritik	Aktif - onay bekliyor
Soğuk Depo 1	D103 Fan Termik	Alarm	Aktif - onay bekliyor
Soğuk Depo 1	D102 Depo Kapısı Açık	Uyarı	Aktif - onay bekliyor
Depo Binası (bu cihaz)	D101	Bilgi	Aktif - onay bekliyor
Soğuk Depo 1	D130	Alarm	Aktif - onaylandı

Plant page: two devices on the same network (an AS1111 and an AS1122) and all alarms on one screen (example, Turkish interface)

9 Maintenance

9.1 Settings backup and restore

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

- **Download backup:** roles, people, alarm rules and targets (including escalation), input names and texts, notification settings, outage report, device name and plant setting are saved to 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.** If the plant WiFi is already the same, it is not changed. It can also be used in setup mode when setting up a new device; give new people their PIN from the Users page.

A settings backup is also the easiest way to set up the same configuration on many devices quickly.

Backup file

The backup file may contain the WiFi password and people's contact details. Store it securely. Make a backup before major changes; at the end of commissioning, hand the backup over to the customer.

9.2 Factory reset

Action	Where	Deleted	Kept
Reset alarm settings	Alarm Settings	Rules, input names, texts, active alarms	People, notification settings, targets
Full factory reset	Settings (administrator only, from the device WiFi only) or the buttons (Section 10)	People, PINs, roles, targets, notification and WiFi settings, alarm rules; optionally the event log. The device WiFi password returns to the factory password	Device identity, software, recovery code, device name

After the alarm settings are reset, **no input raises an alarm**; configure the inputs again.

Handing over or sending for service

Before handing the device over to another site or sending it for service, first make a settings backup, then perform a **full factory reset** and tick "**Also delete event log**"; personal data is erased from the device.

9.3 If the administrator PIN is forgotten

- 1 Connect to the device WiFi (if necessary, switch the device off and on again and use the first 10 minutes).
- 2 In the panel: **Sign in** → **Forgot my PIN** → select the administrator account → enter the **recovery code** and the new PIN.
- 3 No other settings change; the action 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 you must wait 5 minutes. The administrator resets other people's PINs on the Users page.

9.4 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 and set a new password under **Notifications** → **WiFi** → **Device WiFi** (administrator). If the panel cannot be reached at all, perform a **full**

factory reset with the buttons (Section 10); the password returns to the factory password and setup must be done again.

9.5 Software updates

Software updates are carried out by **authorised service** via the device WiFi. Update packages are signed by the manufacturer; the device rejects unsigned or corrupted packages. New software only becomes permanent once it has been verified to run correctly; if there is a problem, the device switches to its recovery partition. Settings and records are kept during an update.

9.6 Storage card

The event history and notification log are kept on the storage card (microSD) inside the device; the card is not removed by the user. Settings and people's details are also stored in the device's internal memory. If there is a problem with the card, the device sends a system notification, the yellow LED2 goes out and the status is shown on the System page; in this case, contact service.

10 Front panel: lights and buttons

10.1 Status lights

When the device is powered up or restarted, only the green LED is lit for a few seconds (this is normal). Then the LEDs light up in sequence (about 5 seconds) and then show the status:

LED	Colour	When lit	When off
LED4	Green	Device running normally	There is a critical problem (see LED1)
LED3	Yellow	Device connected to the plant WiFi	No plant WiFi or not set up (notifications are not sent)
LED2	Yellow	Storage card fitted and working	Storage card cannot be read (event log cannot be written)
LED1	Red	Critical error: internal connection problem or memory at a critical level	No critical error

- If the **green LED flashes slowly** during the first minute after power-up, the device is still starting; wait.
- **If LED1 is lit**, restart the device (middle button for 10 seconds). If it persists, contact authorised service.
- While a button action is in progress, the LEDs show its progress; when it ends they return to the status display.
- Authorised service can run an LED and button test from the panel; when the test ends, or after 10 minutes, the LEDs show the status again.

10.2 Buttons

Action	How	Result
Restart	Hold the middle button for 10 seconds. The LEDs fill up one by one, flash during the last second, then stay lit → release the button	The device restarts; settings are kept . Releasing before 10 seconds cancels the action
Full factory reset	1) Hold both side buttons together for 10 seconds; release when all four LEDs stay lit. 2) While the LEDs flash rapidly, press the middle button 3 times within 6 seconds	The device returns to full factory settings (the event log is kept) and restarts. The device WiFi password returns to the factory password. Repeat the setup (Section 5)

If any step is done incorrectly (released too early, time exceeded, another button pressed), the action is cancelled and no settings change. The device can also be restarted from the panel: **System** → **Restart device** (the panel is

disconnected for about 1 minute).

11 Troubleshooting

Symptom	Possible cause	Remedy
Device WiFi not visible	Connected to the plant network and in "off while connected" mode	Switch the device off and on; 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, or the <code>.local</code> name is not resolved	Use the same network; try the IP address (addresses under Notifications → WiFi)
Device is on the plant network but the panel does not open via the IP address either	Client isolation / guest network on the router	Turn isolation off or connect the device and the phone to the main network; on a corporate network, ask IT for an exception (Section 4.4)
"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)
No Telegram messages	Start not pressed in the bot, wrong ID, channel disabled	Section 6.3; check the error reason in Notifications → Log
No e-mails	Spam folder, wrong address	Check the spam folder and the address; check the Log
Some people do not receive messages	Outside working hours and low severity; person not a target	Check the person's working hours and severity setting and the input's targets
An input never raises an alarm	Input Disabled, alarm condition reversed, wiring	Alarm Settings → Rules; trigger the input and watch its state on the Dashboard
The same input alarms too often	Contact chatter, interference	Increase the debounce time; use "Back to normal – at least ... s"
Plant page shows "... device not seen for 2 minutes"	Device off, different network or client isolation	Check the causes in the warning one by one; if the device has been removed, remove from list
Plant page shows "plant password ... not the same"	Different plant passwords on the devices	Enter the same password on all devices under Plant → Plant settings
Device restarts by itself	Supply problem	Check the supply; pass the reason in System → Boot history to service
Red LED1 is lit	Critical error	Restart with the middle button; if it persists, contact service
"Setup not completed" warning does not go away	Administrator, notification contact 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 began.

12 Technical data

Item	Value
Model	Alert SCADA AS1111 — fault alerting and alarm notification device
Digital inputs	32 (DI00–DI31), four blocks of 8; PNP, 24 V DC; optically isolated (2500 V)
Scan / signal filtering	1 ms / 0–10,000 ms per input
Outputs	None (outputs: AS1122)
Supply	24 V DC nominal, 15–30 V DC
Terminals	Pluggable screw terminals, 5.08 mm; 0.2–2.5 mm ²
Communication	WiFi 2.4 GHz 802.11 b/g/n (plant network + the device's own network); no 5 GHz, Ethernet or cellular
Notification	Telegram · E-mail (SSL, port 465) · Webhook (HTTP/HTTPS POST, JSON) · web panel
Web panel	In the browser (phone, tablet, PC); Turkish / English; no app to install
Users	Up to 32 people, 16 roles; personal 4–6-digit PIN
Escalation	Up to 4 steps (including the first notification), 4 roles + 4 people per step
Recording	Internal storage card (event history, notification log); outage record and boot history
Clock	Battery-backed real-time clock; synchronised from the internet
Mounting	Inside the panel, screwed to a flat surface; 4 × Ø3.8 mm, hole spacing 80.4 × 104.1 mm
Dimensions	115 × 114 × 45 mm (excluding mounting lugs and connectors)
Enclosure	For installation inside a control panel; partial protection against dust
Warranty	24 months from the invoice date

Default values

Item	Factory setting
Device WiFi	ION8B00T_XXXXXX ; password on the label (change during setup); panel http://192.168.4.1
Device WiFi mode	Off while connected to the plant network
Address from the plant network	http://ion8-xxxxxx.local or IP (Automatic)
Web panel	HTTP, port 80; Turkish / English; can be viewed without signing in
Alarm rules	All inputs Disabled
Outage report	Off
Repeat limit (per minute)	Info 3 · Warning 3 · Alarm 3 · Critical unlimited
Session / logout	Sign-out after 30 min of inactivity · 5 min lockout after 5 wrong PINs

13 Commissioning checklist

✓	Check
☐	Supply and input wiring done, power on, green LED lit
☐	Label details (serial no., device WiFi name) recorded
☐	Device WiFi password changed , new password recorded
☐	Administrator created; second administrator defined
☐	Recovery code stored in a safe place
☐	Device name and location entered
☐	Connected to the plant WiFi (yellow LED3 lit); panel opens from the plant network; address fixed
☐	Inputs in use named, unused inputs Disabled
☐	Every input physically triggered; correct channel and direction seen in the panel
☐	People added; Start pressed in the Telegram bot; test messages received
☐	Targets and (if needed) escalation set; one alarm acknowledged and the "acknowledged" notification seen
☐	(Several devices) Same plant password on all devices; all devices visible on the Plant page
☐	(Recommended) Outage report enabled
☐	Settings backup downloaded and handed over to the customer
☐	Users given the User Manual and the panel address

14 Warranty and support

- **Warranty:** 24 months from the invoice date, against defects in material and workmanship. The warranty is recorded against the device's serial number. Terms and exclusions are given in the **Warranty Certificate** supplied with the device.
- **Examples of exclusions:** installation or use contrary to the manuals, use outside the supply and input limits, overvoltage, lightning, water, humidity, dust and impact, unauthorised opening of the housing, unauthorised repair or software installation, interruptions of third-party services (internet, Telegram, e-mail).
- **When requesting support**, have ready the serial number, the invoice, a description of the fault and, if possible, a screenshot of the **System** page. Before sending the device for service, make a settings backup and perform a full factory reset (with "Also delete event log" ticked).

Indirect damage that may result from a notification not arriving or arriving late, and the limitation of liability, are explained in the Warranty Certificate.

For technical questions, write to **support@ionia-automation.com**; for sales and general information, to **info@ionia-automation.com**.



Contact

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