SEGNALAZIONE GUASTI E GESTIONE ALLARMI INDUSTRIALI

AS1122

Guida all'installazione

Dispositivo da quadro per monitoraggio allarmi, notifica e segnalazione in campo · 16 ingressi · 16 uscite

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

Indice

1 Informazioni sulla guida e sicurezza 4

1.1 Informazioni sulla guida 4

1.2 Istruzioni di sicurezza 4

2 Panoramica del prodotto 6

2.1 Che cosa fa l'AS1122 6

2.2 Dispositivo e pannello frontale 6

2.3 Etichetta del dispositivo 7

3 Montaggio 7

3.1 Scelta della posizione 7

3.2 Montaggio nel quadro 7

4 Collegamento elettrico 8

4.1 Regole generali 8

4.2 Alimentazione 8

4.3 Ingressi 8

4.4 Uscite 9

4.5 Prima di dare tensione 9

5 Primo avvio e procedura guidata di configurazione 10

5.1 Accensione 10

5.2 Connessione al WiFi del dispositivo 10

5.3 Procedura guidata di configurazione 10

5.4 Messaggio di prova 11

5.5 Codice di ripristino 11

6 Connessione di rete 12

6.1 WiFi dell'impianto 12

6.2 Accesso al pannello dalla rete dell'impianto 12

6.3 WiFi del dispositivo e relativa password 12

6.4 Requisiti IT e firewall 13

7 Persone e notifiche 15

7.1 Ruoli e permessi 15

7.2 Aggiunta di persone 15

7.3 Account di notifica e Telegram 15

7.4 E-mail 16

7.5 Destinatari ed escalation 16

7.6 Prova e registro degli invii 16

8 Messa in servizio degli ingressi 16

9 Messa in servizio delle uscite 17

9.1 Denominazione e prova manuale delle uscite 17

9.2 Prima regola di uscita 17

9.3 Prova in campo 18

10 Più dispositivi: Plant 18

11 Backup, ripristino delle impostazioni di fabbrica e recupero 19

11.1 Backup delle impostazioni 19

11.2 Ripristino delle impostazioni di fabbrica 19

11.3 Se si dimentica il PIN dell'amministratore 19

11.4 Se si dimentica la password del WiFi del dispositivo 20

11.5 Aggiornamento software 20

12 Pannello frontale: LED e pulsanti 20

12.1 LED di stato 20

12.2 Pulsanti 20

13 Risoluzione dei problemi 21

14 Dati tecnici (riepilogo) 22

15 Lista di controllo per la messa in servizio 23

16 Garanzia e assistenza 23

1 Informazioni sulla guida e sicurezza

1.1 Informazioni sulla guida

Questa guida è destinata al personale tecnico che monta Alert SCADA AS1122 nel quadro elettrico, esegue i collegamenti elettrici e completa la configurazione iniziale. L'uso quotidiano (monitoraggio degli allarmi, conferma, regole di uscita) è descritto nel **Manuale d'uso**.

Prodotto	Alert SCADA AS1122 — 16 ingressi digitali, 16 uscite digitali
Destinatari	Personale elettrico / di automazione che monta, cabla e mette in servizio il dispositivo; personale IT
Documenti correlati	Manuale d'uso · Scheda tecnica · Certificato di garanzia

In questa guida i nomi di menu, pagine e pulsanti del pannello sono indicati in **grassetto**, con la dicitura dell'interfaccia inglese (ad es. **Alarm Settings** → **Rules**). Il pannello è disponibile in turco e in inglese.

Riquadri di avviso utilizzati in questa guida:

Pericolo
La mancata osservanza può mettere in pericolo persone o cose.

Attenzione
La mancata osservanza può danneggiare il dispositivo o l'impianto, oppure un allarme può andare perso.

Nota
Informazioni che facilitano il lavoro.

1.2 Istruzioni di sicurezza

Sicurezza delle persone
Alert SCADA è un dispositivo di segnalazione guasti. **Non sostituisce i sistemi di rivelazione incendio, di rivelazione gas, di sicurezza delle persone o i sistemi di allarme obbligatori per legge** e non possiede le certificazioni di tali sistemi.

Le uscite dell'AS1122 servono **solo per avviso e segnalazione** (sirene, lampeggianti, colonne luminose, avvisatori acustici). Le uscite non sono un relè di sicurezza, un arresto di emergenza né un circuito di sicurezza macchina. **I circuiti di arresto di emergenza e di sicurezza delle persone restano nei rispettivi sistemi di sicurezza.**

- Il montaggio e il collegamento elettrico devono essere eseguiti da **personale elettrico qualificato** nel rispetto delle norme impiantistiche vigenti.
- Eseguire il cablaggio **solo in assenza di tensione**: l'alimentazione del dispositivo, la tensione di segnale sugli ingressi e l'alimentazione dei carichi collegati alle uscite devono essere tutte disinserite.
- I valori di alimentazione, ingressi e uscite non devono superare i limiti indicati in questa guida (Sezione 4 e Sezione 14).
- Montare il dispositivo **all'interno di un quadro elettrico asciutto e privo di polvere**.
- In caso di mancanza di alimentazione e di guasto interno del dispositivo, le uscite vengono **rilasciate (disattivate)**. La scelta, la protezione e il funzionamento sicuro delle apparecchiature collegate alle uscite sono responsabilità dell'utente.

- Il recapito delle notifiche dipende dall'alimentazione elettrica, dalla connessione internet e da servizi di terzi (Telegram, e-mail). Negli impianti critici, alimentare il dispositivo da una linea protetta da un **gruppo di continuità (UPS)** e valutare un canale di comunicazione di riserva.
- Non aprire l'involucro. Le parti interne non sono sostituibili dall'utente; l'apertura dell'involucro fa decadere la garanzia.

2 Panoramica del prodotto

2.1 Che cosa fa l'AS1122

L'AS1122 monitora costantemente 16 segnali a contatto nel quadro elettrico (guasto pompa, intervento del relè termico, porta, interruttore di livello, arresto macchina ecc.). Quando un segnale passa in stato di allarme, avvisa le persone interessate e, se lo si desidera, segnala in campo con una sirena, un lampeggiante o una colonna luminosa.

Monitora
16 ingressi digitali (DI00–DI15), scansione 1 ms. Contatti normalmente aperti e normalmente chiusi.

Avvisa
Più persone contemporaneamente tramite Telegram ed e-mail. Conferma (presa in carico), chi è intervenuto e quando, escalation degli allarmi non confermati.

Segnala in campo
16 uscite (DO00–DO15): sirene, lampeggianti, colonne luminose, avvisatori acustici. Una persona autorizzata le attiva e disattiva manualmente, oppure funzionano automaticamente con regole SE ... ALLORA senza programmazione.

Registra
Tutti gli eventi, le conferme e i comandi alle uscite con data, ora e persona. Interruzioni di alimentazione e di internet con la relativa durata.

Il dispositivo non è legato a un cloud: impostazioni e registrazioni restano all'interno del dispositivo. Internet viene usato solo per inviare le notifiche e sincronizzare l'orologio. Per la configurazione e l'uso non si installa alcuna app; è sufficiente il browser di uno smartphone, di un tablet o di un computer.

2.2 Dispositivo e pannello frontale

Pannello frontale: quattro LED di stato e tre pulsanti; i morsetti di collegamento si trovano sui bordi superiore e inferiore dell'involucro.

Parte	Descrizione
LED di stato (4)	Da sinistra a destra LED1 rosso, LED2 giallo, LED3 giallo, LED4 verde. Indicano che il dispositivo è in funzione, che è connesso al WiFi dell'impianto e lo stato di registrazione (Sezione 12)
Pulsanti (3)	Pulsante sinistro, centrale e destro. Per il riavvio senza computer (Sezione 12)
Morsetti	Morsettiere a vite: alimentazione, ingressi e uscite (Sezione 4)
Etichetta	Numero di serie, dati del WiFi del dispositivo e codici QR (Sezione 2.3)

2.3 Etichetta del dispositivo

Annotare i dati dell'etichetta prima dell'installazione; serviranno durante la configurazione e l'assistenza.

Voce	Esempio	Scopo
Numero di serie	`ION8-1122-YYAA-NNNN`	Registrazione di garanzia e assistenza
Nome WiFi del dispositivo	`ION8BOOT_xxxxxx`	Configurazione iniziale e connessione di manutenzione
Password WiFi del dispositivo	Stampata sull'etichetta	Prima connessione; **modificarla** dopo la configurazione (Sezione 6.3)
Indirizzo del pannello	`http://192.168.4.1`	Indirizzo del pannello con connessione al WiFi del dispositivo
Codici QR	**1** · **2** · QR piccolo	1: collega lo smartphone al WiFi del dispositivo · 2: apre il pannello nel browser · QR piccolo: numero di serie

> **Codice modello**
> Sull'etichetta del dispositivo e nell'angolo superiore del pannello il codice modello compare come **ION8-1122**; questo codice si riferisce ad Alert SCADA AS1122.

3 Montaggio

3.1 Scelta della posizione

- Montare il dispositivo **all'interno di un quadro elettrico asciutto e privo di polvere**. L'involucro offre una protezione parziale contro la polvere; non è protetto contro l'acqua.
- Il dispositivo si collega alla rete dell'impianto tramite **WiFi**. **Un armadio metallico attenua il segnale WiFi:** prima del montaggio, verificare con uno smartphone, a porta del quadro chiusa, che il WiFi dell'impianto sia sufficientemente forte all'interno del quadro. Se il segnale è debole, utilizzare un access point WiFi vicino al quadro.
- Scegliere una posizione in cui i LED e i pulsanti del pannello frontale siano ben visibili e facilmente raggiungibili all'apertura della porta del quadro.
- Lasciare spazio sufficiente davanti ai morsetti per il cablaggio.

3.2 Montaggio nel quadro

1. Fissare il dispositivo **con viti su una superficie piana** (piastra di montaggio del quadro). Sono presenti 4 fori di fissaggio da Ø3,8 mm; l'interasse dei fori è **80,4 × 104,1 mm**.
2. Serrare le viti senza forzare l'involucro.
3. Prima del cablaggio, verificare che il pannello frontale e i morsetti siano facilmente accessibili.

Dati meccanici	Valore
Montaggio	Fissaggio a vite su superficie piana, all'interno di un quadro elettrico
Fori di fissaggio	4 × Ø3,8 mm, interasse 80,4 × 104,1 mm
Dimensioni	115 × 114 × 45 mm (escluse alette di fissaggio e connettori)
Peso	250 g

4 Collegamento elettrico

4.1 Regole generali

Cablare in assenza di tensione

Eseguire tutti i collegamenti con l'alimentazione del dispositivo, la tensione di segnale degli ingressi e l'alimentazione dei carichi delle uscite **disinserite**. Non collegare né scollegare i morsetti con l'alimentazione inserita.

- I morsetti sono a vite. Applicare puntalini ai conduttori a trefoli; serrare le viti e verificare tirando leggermente il filo.
- Per quanto possibile, posare i cavi di segnale separati dai cavi di potenza.
- Durante il cablaggio annotare a quale canale corrisponde ciascun morsetto; al primo avvio si verificherà ogni ingresso e ogni uscita sul pannello (Sezione 8 e Sezione 9).

4.2 Alimentazione

Tensione di alimentazione	**24 V DC** nominale, campo di funzionamento **15–30 V DC**

- Alimentare il dispositivo dalla sorgente a 24 V DC presente nel quadro. Rispettare la polarità.
- Per un monitoraggio senza interruzioni, prelevare l'alimentazione da una linea **protetta da UPS**. In caso di mancanza di alimentazione il dispositivo non funziona, non può monitorare gli ingressi e tutte le uscite si disattivano; al ritorno dell'alimentazione segnala la durata dell'interruzione (Manuale d'uso).
- Se un'apparecchiatura di segnalazione collegata a un'uscita (ad es. una sirena) deve funzionare anche in caso di mancanza di alimentazione, alimentare sia il dispositivo sia tale apparecchiatura da una linea protetta da UPS.

4.3 Ingressi

Numero di ingressi	16 ingressi digitali (2 × 8), indicati sul pannello come **DI00 – DI15**
Tipo di ingresso	**PNP, 24 V DC**: l'ingresso diventa attivo (1) quando si applicano +24 V; almeno 15 V per l'1 logico
Isolamento	Isolamento ottico, 2500 V
Collegabili	Contatti puliti (contatto di relè, interruttore, pulsante), sensori con uscita PNP

- **Contatto pulito:** collegare un lato del contatto a 24 V DC e l'altro lato all'ingresso. Quando il contatto si chiude, l'ingresso diventa 1.
- **Contatto normalmente aperto (NO):** l'ingresso diventa 1 quando il contatto si chiude. Come condizione di allarme selezionare "Signal on (0→1)".
- **Contatto normalmente chiuso (NC):** l'ingresso è normalmente a 1; diventa 0 quando il contatto si apre o **il filo si interrompe**. Nei circuiti in cui anche un filo interrotto deve generare un allarme, utilizzare un contatto NC e l'opzione **Inverted Logic** (logica invertita) dell'ingresso (Sezione 8).

Ingressi non utilizzati

Impostare gli ingressi non utilizzati su **Disabled** (disabilitato) nel pannello (alla consegna tutti gli ingressi sono Disabled). In questo modo un ingresso flottante non genera allarmi dovuti a disturbi.

4.4 Uscite

Numero di uscite	16 uscite digitali (2 × 8), indicate sul pannello come **DO00 – DO15**
Tipo di uscita	Uscita a transistor di tipo sourcing (PNP); protetta contro sovracorrente e sovratemperatura
Tensione di uscita	Segue la tensione di alimentazione (con l'uscita attiva, la tensione di alimentazione è applicata al carico)
Corrente di uscita	Max. **100 mA** per uscita
Uso previsto	Avviso e segnalazione: sirene, lampeggianti, colonne luminose, avvisatori acustici, bobine di relè di interfaccia
All'avvio	Tutte le uscite si avviano disattivate
In caso di mancanza di alimentazione / guasto	Le uscite vengono rilasciate (disattivate)

- Quando è attiva, l'uscita applica la tensione di alimentazione al carico (sourcing). Collegare un lato del carico all'uscita e l'altro lato allo 0 V dell'alimentazione.
- Spie di segnalazione DC, bobine di relè di interfaccia e ingressi PLC / di segnale che assorbono **non più di 100 mA** possono essere collegati direttamente.
- Non collegare direttamente sirene, lampeggianti, colonne luminose o apparecchiature di segnalazione a 230 V AC **che assorbono una corrente maggiore**: pilotare con l'uscita un **relè di interfaccia o un contattore adeguato** e alimentare il carico tramite il contatto di tale relè.
- Scegliere le apparecchiature collegate in modo che rimangano in uno stato sicuro quando l'uscita è disattivata (mancanza di alimentazione, guasto del dispositivo, aggiornamento software). Non collegare a un'uscita dell'AS1122 un carico la cui disattivazione creerebbe un pericolo.

Le uscite non sono un circuito di sicurezza

Non utilizzare le uscite dell'AS1122 in circuiti di arresto di emergenza, di sicurezza macchina o di sicurezza delle persone. Tali circuiti restano nei rispettivi sistemi di sicurezza certificati. Le uscite dell'AS1122 servono solo per avviso e segnalazione.

4.5 Prima di dare tensione

✓	Verifica
☐	Tensione di alimentazione entro 15–30 V DC, polarità corretta
☐	Contatti di ingresso collegati ai canali corretti; tipo di contatto (NO / NC) annotato
☐	I carichi delle uscite non superano 100 mA; carichi maggiori tramite relè di interfaccia
☐	Le apparecchiature collegate sono sicure da disattivate; nessuna uscita collegata a un circuito di sicurezza
☐	Viti dei morsetti serrate, i fili non si sfilano se tirati

5 Primo avvio e procedura guidata di configurazione

5.1 Accensione

1. Verificare i collegamenti e dare tensione. All'avvio **tutte le uscite sono disattivate.**
2. I LED si accendono prima uno dopo l'altro, poi indicano lo stato (Sezione 12). Se durante il primo minuto il LED verde lampeggia lentamente, il dispositivo è ancora in fase di avvio; attendere.
3. Dopo circa **1 minuto** compare la rete WiFi propria del dispositivo (`ION8BOOT_xxxxxx`).

5.2 Connessione al WiFi del dispositivo

1. Scansionare con lo smartphone il **codice QR 1** sull'etichetta, oppure selezionare il **nome WiFi del dispositivo** dall'elenco WiFi dello smartphone / del computer. Inserire **la password stampata sull'etichetta**.
2. Sulla maggior parte degli smartphone, appena connessi compare la notifica **"Accedi alla rete"** e il pannello del dispositivo si apre automaticamente. Se lo smartphone avvisa "Nessuna connessione internet su questa rete", scegliere di **rimanere connessi**.
3. Se il pannello non si apre da solo, aprire **http://192.168.4.1** nel browser oppure scansionare il **codice QR 2** sull'etichetta.

> **Quando è attivo il WiFi del dispositivo?**
> Una volta che il dispositivo è connesso alla rete dell'impianto, il WiFi del dispositivo si disattiva per impostazione predefinita. Si riattiva per i primi 10 minuti dopo ogni accensione e quando si perde la rete dell'impianto (Sezione 6.3).

5.3 Procedura guidata di configurazione

Finché nel dispositivo non esiste un amministratore, il pannello si apre con la **procedura guidata di configurazione**. Ogni passo può essere saltato; si può tornare alla procedura guidata in seguito dalla pagina **Settings**. Fino al completamento della configurazione, nella barra superiore compare l'avviso "Setup not complete" (configurazione non completata).

Passo	Che cosa si fa	Raccomandazione
1. Amministratore	Nome e cognome e **PIN** (4–6 cifre)	PIN a 6 cifre per gli amministratori
2. Dispositivo	**Nome del dispositivo** e **ubicazione**; compaiono nell'intestazione di ogni notifica	Ad es. "Edificio Magazzino" / "Spedizioni"
3. WiFi dell'impianto	Rete con accesso a internet per le notifiche (solo **2,4 GHz**); anche l'orologio viene preso da internet	Sezione 6.1
4. Ingressi	Nome e condizione di allarme per gli ingressi utilizzati: Off · Signal on (0→1) · Signal off (1→0) · On every change	Impostazioni dettagliate nella Sezione 8
5. Destinatari delle notifiche	ID Telegram e/o indirizzo e-mail delle persone che riceveranno gli allarmi	Sezione 7
6. Messaggio di prova	Un messaggio di prova a ogni persona; rispondere alla domanda "Did it arrive?" (è arrivato?)	Sezione 5.4

Passo	Che cosa si fa	Raccomandazione
7. Fine	Riepilogo della configurazione e **codice di ripristino**	Annotare il codice e conservarlo in un luogo sicuro

Configurazione iniziale solo tramite il WiFi proprio del dispositivo

Finché non è definito un amministratore, le impostazioni non possono essere modificate dalla rete dell'impianto. Ciò impedisce che un'altra persona sulla rete prenda il controllo di un dispositivo non ancora configurato.

La procedura guidata non configura le uscite. Denominazione, prova e regole delle uscite sono descritte nella Sezione 9.

5.4 Messaggio di prova

Al passo 6 della procedura guidata viene inviato un messaggio di prova a ogni persona e viene chiesto se è arrivato. Per un canale che non ha recapitato il messaggio, seguire il suggerimento sullo schermo: per Telegram la persona deve aver premuto **Start** nel bot di notifica; per l'e-mail controllare la cartella della posta indesiderata (spam) (Sezione 7). Il messaggio di prova può essere inviato di nuovo in qualsiasi momento dalla pagina **Notifications** → **Log**.

5.5 Codice di ripristino

Ogni dispositivo ha un proprio **codice di ripristino** di 12 caratteri. Se il PIN dell'amministratore viene dimenticato, con questo codice si imposta un nuovo PIN (Sezione 11.3). Il codice non cambia nemmeno dopo un ripristino completo delle impostazioni di fabbrica.

- **Per visualizzarlo:** con connessione al WiFi del dispositivo, accedere come amministratore → **Settings** → **Recovery Code** → **Show code**.
- **Se un'altra persona è venuta a conoscenza del codice:** nello stesso punto, **Generate new code**; il vecchio codice non è più valido.

Conservare il codice di ripristino

Annotare il codice e conservarlo in un luogo sicuro insieme ai documenti del dispositivo. Se si perdono sia il codice sia il PIN dell'amministratore, l'unico modo per accedere al pannello come amministratore è un ripristino completo delle impostazioni di fabbrica.

6 Connessione di rete

6.1 WiFi dell'impianto

Per inviare notifiche e sincronizzare l'orologio, il dispositivo deve essere connesso a una rete WiFi con accesso a internet.

1. **Notifications** → **WiFi** (oppure il passo 3 della procedura guidata) → **Scan Networks** → selezionare la rete → inserire la password → **Connect**.
2. A connessione avvenuta, sullo schermo compare l'indirizzo del dispositivo nella rete dell'impianto; il LED3 (giallo) si accende.

> **Solo 2,4 GHz**
> Il dispositivo si connette solo a reti a **2,4 GHz**; i 5 GHz non sono supportati. Se il router usa lo stesso nome per 2,4 e 5 GHz e si verificano problemi di connessione, configurare un nome separato per i 2,4 GHz.

Se la rete salvata non viene trovata, il dispositivo riprova prima frequentemente, poi meno spesso (al massimo ogni 5 minuti).

6.2 Accesso al pannello dalla rete dell'impianto

Una volta che il dispositivo è connesso al WiFi dell'impianto, **due indirizzi** per raggiungere il pannello vengono mostrati come link cliccabili e copiabili: in **Notifications** → **WiFi** (scheda dello stato di connessione), nei passi WiFi e "Done" della procedura guidata e nella scheda **Settings** → **WiFi**. Da uno smartphone o da un computer sulla stessa rete:

- **http://ion8-xxxxxx.local** (oppure il nome assegnato, ad es. `http://magazzino.local`), oppure
- l'indirizzo IP del dispositivo (ad es. `http://192.168.1.50`).

Alcuni smartphone Android non riescono a risolvere i nomi `.local`; in tal caso utilizzare l'indirizzo IP.

Nome di rete del dispositivo (.local). Può essere modificato nella scheda **Notifications** → **WiFi** → **Network address**. Sono ammessi solo lettere minuscole, cifre e trattini (max. 32 caratteri; non può iniziare né terminare con un trattino). I caratteri turchi vengono convertiti automaticamente (ş→s). Se il campo resta vuoto, viene usato il nome automatico (`ion8-xxxxxx`). Non assegnare lo stesso nome a due dispositivi sulla stessa rete.

Indirizzo IP: Automatic / Static. L'impostazione predefinita è **Automatic** (l'indirizzo viene assegnato dal router e può cambiare nel tempo). Se si seleziona **Static IP**, inserire indirizzo IP, subnet mask, gateway e DNS; il pulsante "Use current address" compila i campi con l'indirizzo attuale. Al salvataggio il dispositivo verifica l'indirizzo sulla rete e non lo salva se è già in uso da un altro dispositivo. Il dispositivo ricontrolla l'indirizzo a ogni connessione: se l'indirizzo è in uso da un altro dispositivo o la rete è cambiata, passa da solo all'IP automatico e mostra un avviso nella parte superiore del pannello.

> **Consigliato**
> Configurare una **prenotazione DHCP** per il dispositivo sul router / server DHCP mantiene fisso l'indirizzo ed è il metodo più affidabile. Negli impianti con più dispositivi o con un'integrazione, assegnare a ogni dispositivo un indirizzo fisso.

6.3 WiFi del dispositivo e relativa password

In **Notifications** → **WiFi** → **Device WiFi** si sceglie il comportamento della rete WiFi propria del dispositivo:

Opzione	Comportamento
Off while connected to the plant network (predefinita)	Attiva per i primi 10 minuti dopo ogni accensione, in modalità di configurazione, mentre qualcuno è connesso al dispositivo e quando la rete dell'impianto è persa da oltre 30 secondi; disattivata negli altri casi
Always on	Il WiFi del dispositivo trasmette continuamente
Hidden	Il nome della rete non compare nell'elenco; chi conosce il nome può connettersi

Modificare la password del WiFi del dispositivo
La password sull'etichetta serve per la configurazione iniziale. **Modificarla sempre dopo la configurazione** e registrare la nuova password: **Notifications → WiFi → Device WiFi → Device WiFi password** (disponibile anche nel passo WiFi della procedura guidata). Finché la password non viene modificata, sul pannello compare un avviso.

- La password ha una lunghezza di 8–63 caratteri; sono ammessi solo lettere dell'alfabeto inglese, cifre e simboli. La password di fabbrica riportata sull'etichetta e le password facilmente indovinabili non vengono accettate.
- Se si modifica la password mentre si è connessi al WiFi del dispositivo, la connessione si interrompe dopo qualche secondo; riconnettersi con la nuova password.
- Se il computer continua a provare la vecchia password e mostra un errore, eseguire **Forget** (dimentica) sulla rete nell'elenco WiFi, quindi connettersi con la nuova password (sullo smartphone: dimentica / rimuovi rete).
- Se la password viene dimenticata: Sezione 11.4.

6.4 Requisiti IT e firewall

Il dispositivo effettua solo connessioni **in uscita**; non sono necessarie connessioni in ingresso verso il dispositivo (port forwarding).

Servizio	Destinazione	Porta
Notifica Telegram	api.telegram.org	TCP 443 (HTTPS)
Notifica e-mail	Server di invio (predefinito del produttore o server proprio)	TCP 465 (SSL)
Sincronizzazione dell'orologio	Server NTP	UDP 123
Risoluzione dei nomi	Server DNS della rete	UDP/TCP 53
Webhook (se utilizzato)	Server proprio	Porta indicata nell'indirizzo (HTTP / HTTPS)

Requisiti della rete locale. Per l'accesso al pannello da smartphone / computer e perché i dispositivi si vedano tra loro (pagina **Plant**, regole di uscita basate su un altro dispositivo):

- I dispositivi e gli smartphone / computer usati per aprire il pannello devono trovarsi sulla **stessa rete** (stesso router, stesso intervallo di indirizzi).
- Sul router / access point **l'isolamento dei client deve essere disattivato** (AP isolation, client isolation, "rete ospiti"). Se è attivo, il pannello non si apre dagli smartphone e i dispositivi non si vedono tra loro; le notifiche Telegram ed e-mail non sono interessate. In una rete aziendale, chiedere al reparto IT un'eccezione per i dispositivi Alert SCADA (l'indirizzo MAC del dispositivo è indicato nella pagina **Plant**).
- La comunicazione tra dispositivi avviene tramite broadcast locale **UDP 48230**; i broadcast locali non devono essere bloccati. I pacchetti sono firmati con la password d'impianto (Sezione 10).

- Per gli indirizzi `.local`, il traffico mDNS (UDP 5353) deve poter transitare sulla rete; in caso contrario, utilizzare l'indirizzo IP.

Non esporre il pannello su internet

Il pannello web utilizza HTTP non cifrato. Utilizzare il pannello solo su una **rete d'impianto affidabile**; non configurare il port forwarding. Se è necessario l'accesso remoto, utilizzare una VPN.

7 Persone e notifiche

7.1 Ruoli e permessi

- **Persona:** utente che può accedere al pannello con un PIN e/o riceve notifiche (max. **32** persone).
- **Ruolo:** gruppo di persone a cui vengono assegnati i permessi (max. **16** ruoli; ad es. Amministratore, Capoturno, Tecnico, Operatore). Gli allarmi vengono indirizzati a ruoli o a singole persone.

Nella pagina **Users** → **Roles**, a ogni ruolo vengono assegnati i seguenti permessi:

Nome nell'interfaccia	Consente
ACK	Confermare (prendere in carico) gli allarmi
Mute	Sospendere temporaneamente le notifiche ripetute di un allarme
Config	Regole di allarme, destinatari, impostazioni del dispositivo e delle notifiche; **comando manuale delle uscite**
Add user	Aggiungere / rimuovere persone, assegnare ruoli e PIN
Service (maintenance)	Impostazioni di assistenza — solo assistenza autorizzata

Amministratore completo = Config + Add user. Alcune operazioni (modifica del ruolo abilitato alla conferma, impostazioni del report interruzioni, ripristino delle impostazioni di fabbrica) possono essere eseguite solo da un amministratore completo.

> **Almeno due amministratori**
> Definire almeno **due** amministratori con PIN; gli amministratori dovrebbero usare PIN a 6 cifre. Il dispositivo non consente di eliminare l'ultimo amministratore.

7.2 Aggiunta di persone

Users → **People** → **Add person**: nome e cognome, ruolo/i, PIN (se la persona accederà al pannello), canali di notifica (Telegram / E-mail / Panel), ID Telegram, indirizzo e-mail, **gravità minima** (ad es. ricevere solo Critical) e **orario di lavoro** (fuori dall'orario di lavoro vengono inviati solo gli allarmi al di sopra della gravità selezionata).

- Il PIN ha 4–6 cifre ed è memorizzato nel dispositivo in forma non reversibile.
- Dopo 5 tentativi errati di inserimento del PIN, l'accesso per quella persona viene bloccato per 5 minuti. La sessione si chiude dopo 30 minuti di inattività.
- Ciascuno può modificare il proprio PIN, i dati Telegram / e-mail e l'orario di lavoro nella pagina **Settings** → **My Account**.

> **Nuove persone e destinatari degli allarmi**
> Una persona appena aggiunta, con ID Telegram o indirizzo e-mail, che non è ancora destinataria di alcun ingresso, viene aggiunta automaticamente ai destinatari degli allarmi di tutti gli ingressi. Una persona rimossa in seguito dai destinatari non viene più modificata.

7.3 Account di notifica e Telegram

Il dispositivo viene fornito **già pronto con l'account di notifica del produttore**: un bot di notifica Telegram e un mittente e-mail sono già configurati; non è necessario alcun account o abbonamento separato.

Per Telegram, ogni persona esegue una sola volta, sul proprio smartphone, quanto segue:

1. Apre **il bot di notifica del dispositivo** in Telegram e preme **Start**. Il link al bot è indicato nella procedura guidata e nella pagina **My Account**. Il bot non può inviare messaggi a una persona che non ha eseguito questo passo (regola di Telegram).

2. Ricava il proprio ID Telegram: ad es. apre **@userinfobot**, preme Start e copia il numero **Id** dalla risposta.

3. Inserisce il numero nel campo **Telegram ID** della persona (**Users** → **People**, oppure la persona stessa in **Settings** → **My Account**).

7.4 E-mail

Compilare il campo **e-mail** della persona e attivare il canale E-mail. I primi messaggi potrebbero finire nella cartella della posta indesiderata (spam); chiedere ai destinatari di aggiungere l'indirizzo del mittente all'elenco dei mittenti attendibili. Se si desidera utilizzare un proprio server e-mail, contattare l'assistenza autorizzata.

7.5 Destinatari ed escalation

- Nella tabella **Alarm Settings** → **Targets** si sceglie quali ruoli e persone ricevono l'allarme di ciascun ingresso.
- Un allarme non confermato viene inoltrato ai livelli superiori agli intervalli impostati nell'impostazione **Escalation** dell'ingresso: fino a **4 passi** inclusa la prima notifica, ciascun passo con fino a 4 ruoli + 4 persone. Esempio: Operatore (0 min) → Capoturno (+10 min) → Responsabile manutenzione (+20 min). Gli intervalli sono impostati dall'utente.
- Dettagli: Manuale d'uso, "Livelli di gravità, destinatari ed escalation".

7.6 Prova e registro degli invii

- **Notifications** → **Log**: inviare un messaggio di **prova** a ogni persona. Tutti gli invii, i relativi esiti ed eventuali cause di errore sono visualizzati qui.
- Una notifica che non è stato possibile recapitare a una persona su un canale viene ritentata solo per quella persona e quel canale (**Notifications** → **General**: numero di tentativi 0–5).

8 Messa in servizio degli ingressi

La pagina **Alarm Settings** → **Rules** contiene una riga per ciascun ingresso. Le modifiche vengono scritte nel dispositivo premendo **Save**.

1. Assegnare a ogni ingresso utilizzato un **Channel Name** (nome del canale) chiaro (ad es. "Guasto compressore 1"); questo nome compare nelle notifiche e sul pannello.

2. Selezionare il **Trigger**: **Rising Edge** per un contatto NO (allarme su 0→1); **Falling Edge**, oppure un contatto NC con **Inverted Logic**, se l'allarme è la perdita del segnale; **Both Edges** per gli ingressi che devono notificare aperto / chiuso. Lasciare gli ingressi non utilizzati su **Disabled**.

3. Selezionare la **Severity** (livello di gravità: Info · Warning · Alarm · Critical) e, se necessario, inserire un valore di **Debounce** (filtraggio del segnale, 0–10 000 ms).

4. Attivare ogni ingresso **fisicamente** in campo: verificare sul pannello che cambi il canale corretto nella direzione corretta e che la notifica arrivi.

Tutte le opzioni degli ingressi (allarme ritenuto, conferma automatica, notifica di ritorno alla normalità, testi) sono descritte nel Manuale d'uso.

9 Messa in servizio delle uscite

> **Prima di tutto la sicurezza in campo**
>
> Prima di provare le uscite, assicurarsi che l'azionamento delle apparecchiature collegate non metta in pericolo nessuno. Informare il personale in campo prima di provare sirene e lampeggianti.

9.1 Denominazione e prova manuale delle uscite

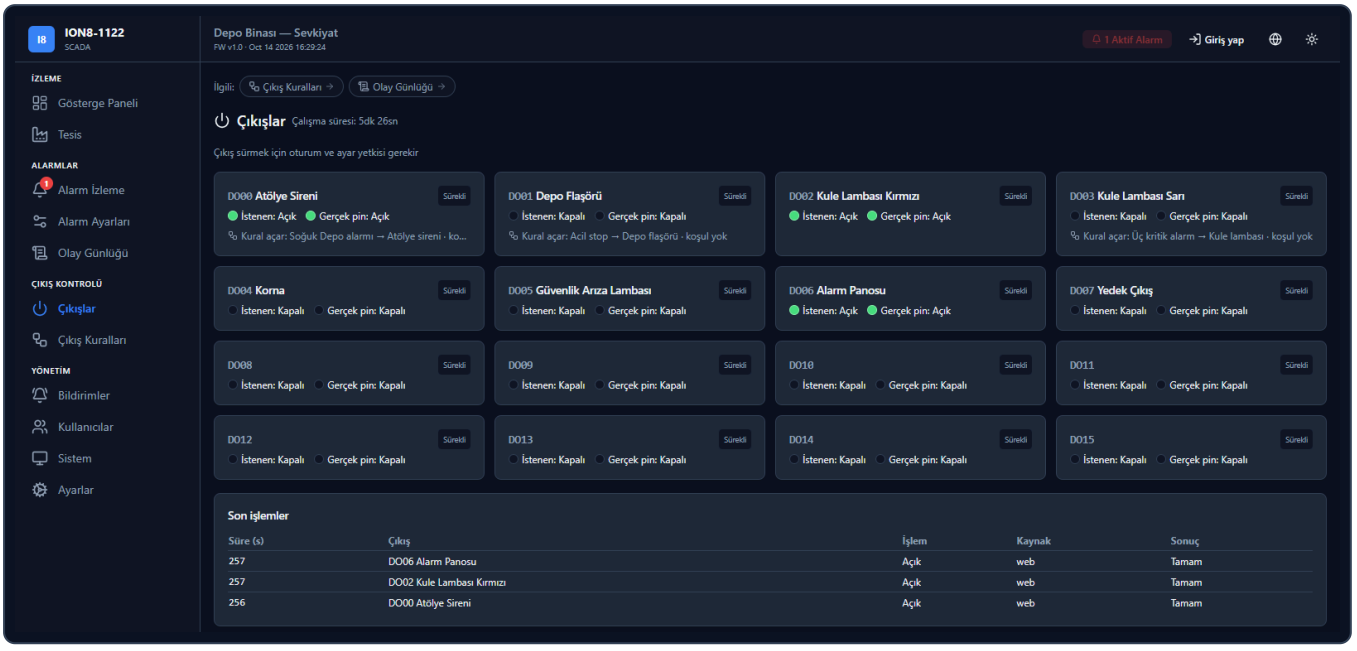
Per comandare le uscite è necessario aver effettuato l'accesso e il proprio ruolo deve avere il permesso **Config**.

1. Nella pagina **Outputs**, premere il pulsante ⚙ **Settings** di ogni uscita utilizzata e assegnarle un **Name** (ad es. "Sirena officina", "Lampeggiante magazzino").

2. Selezionare il **Mode**: **Continuous** (resta attiva finché non viene disattivata) oppure **Pulse** (resta attiva per un tempo impostato e poi si disattiva; ad es. un avvisatore acustico o un pulsante di reset). In modalità continua è possibile impostare per sicurezza un **Maximum on time** (tempo massimo di attivazione).

3. Provare l'uscita con **On / Off** (**Pulse** in modalità impulsiva). Ogni comando di attivazione richiede una conferma.

4. Verificare che gli stati **Requested** (richiesto) e **Actual pin** (stato effettivo del pin) sulla scheda coincidano e che in campo funzioni l'apparecchiatura corretta. Se differiscono, la scheda mostra un avviso; controllare il cablaggio.



Pagina Outputs (interfaccia in turco): nome, stato richiesto ed effettivo di ogni uscita, la regola che la controlla; in basso le operazioni recenti.

9.2 Prima regola di uscita

Perché le uscite funzionino automaticamente in base agli allarmi, le regole vengono impostate nella pagina **Output Rules** (è richiesto l'accesso come amministratore). Il modo più rapido è scegliere uno dei modelli predefiniti:

Modello	Che cosa fa
Unacknowledged alarm → siren	La sirena resta attiva finché un allarme è in attesa di conferma; si ferma alla conferma
Critical alarm → output	Uscita attiva finché è presente un allarme attivo di gravità Critical

Modello	Che cosa fa
Input → output	Uscita attiva finché un ingresso è attivo
Other device's alarm → output	Uscita locale attiva finché un altro dispositivo Alert SCADA dell'impianto ha un allarme

Leggere la riga **Summary** (riepilogo) della regola e premere **Save**. Tutte le opzioni delle regole sono descritte nel Manuale d'uso.

9.3 Prova in campo

Provare in campo ogni regola di uscita dopo averla impostata:

- Creare la condizione (ad es. attivare l'ingresso); verificare che l'uscita si attivi.
- Confermare l'allarme o far terminare la condizione; verificare che l'uscita si disattivi.
- Se esiste una regola di manutenzione / soppressione (KEEP OFF), verificare che l'uscita non si attivi mentre la regola è attiva.
- Provare una mancanza di alimentazione: spegnere e riaccendere il dispositivo; verificare che tutte le uscite si avviino disattivate e che le regole tornino poi a comandare le uscite in base alle condizioni.

10 Più dispositivi: Plant

Se sulla stessa rete dell'impianto sono presenti più dispositivi Alert SCADA (ad es. AS1111 e AS1122), la pagina **Plant** (impianto) li mostra tutti, con i relativi allarmi, in un'unica schermata. Un allarme su un dispositivo può comandare un'uscita di un altro AS1122 (ad es. un guasto nel magazzino accende la lampada nella portineria). Non sono necessari server né cloud; la comunicazione tra dispositivi funziona anche senza internet.

1. Collegare tutti i dispositivi alla **stessa rete WiFi dell'impianto**; assicurarsi che sul router **l'isolamento dei client sia disattivato** (Sezione 6.4).

2. Su ogni dispositivo, aprire **Plant → Plant settings** come amministratore e inserire **la stessa password d'impianto su tutti i dispositivi**. Finché la password non viene modificata, la pagina mostra l'avviso "Plant password is at factory value" (password d'impianto al valore di fabbrica).

3. Verificare nella pagina **Plant** che tutti i dispositivi risultino **online**.

- I dispositivi accettano solo pacchetti provenienti da dispositivi che conoscono la stessa password d'impianto.
- Se non si desidera che gli allarmi di questo dispositivo vengano confermati da altri dispositivi, disattivare la conferma da altri dispositivi in **Plant settings**.
- Se un dispositivo visto in precedenza non è più visibile da 2 minuti, la pagina **Plant** mostra un avviso e le possibili cause (dispositivo spento, rete diversa, isolamento dei client, password d'impianto diversa). Un dispositivo rimosso definitivamente viene eliminato con il pulsante **remove from list** nell'avviso.

11 Backup, ripristino delle impostazioni di fabbrica e recupero

11.1 Backup delle impostazioni

Settings → **Settings backup** (amministratore):

- **Download backup:** ruoli, persone, regole di allarme, destinatari ed escalation, nomi e testi degli ingressi, **impostazioni delle uscite e regole di uscita**, impostazioni di notifica, report interruzioni, nome del dispositivo e impostazioni dell'impianto vengono scaricati in un unico file `.json`. I dati di contatto delle persone e il WiFi dell'impianto sono inclusi solo se le relative caselle sono selezionate. **I PIN non vengono mai inclusi.**
- **Restore:** selezionare il file → selezionare le sezioni → **Restore selected**. Può essere usato anche in modalità di configurazione quando si configura un nuovo dispositivo; assegnare i PIN alle nuove persone nella pagina **Users**. Le regole di uscita che fanno riferimento a un altro dispositivo non vengono ripristinate se tale dispositivo non è presente in questo impianto.

> **Proteggere il file di backup**
> Il file di backup può contenere la password WiFi e i dati di contatto delle persone; conservarlo in modo sicuro. Eseguire un backup al termine della messa in servizio e prima di modifiche importanti.

11.2 Ripristino delle impostazioni di fabbrica

Operazione	Dove	Eliminato	Conservato
Reset delle impostazioni di allarme	**Alarm Settings**	Regole degli ingressi, nomi dei canali, testi, allarmi attivi	Persone, impostazioni di notifica, destinatari
Ripristino completo delle impostazioni di fabbrica	**Settings** (solo amministratore, solo dal WiFi del dispositivo)	Persone, PIN, ruoli, destinatari, impostazioni di notifica e WiFi, regole di allarme; facoltativamente il registro eventi. La password del WiFi del dispositivo torna a quella riportata sull'etichetta	Identità del dispositivo, software, codice di ripristino, nome del dispositivo

> **Dopo il reset delle impostazioni di allarme**
> Dopo il reset delle impostazioni di allarme **nessun ingresso genera allarmi**; configurare di nuovo gli ingressi.

> **Alla cessione del dispositivo o all'invio in assistenza**
> Eseguire prima un backup delle impostazioni, quindi un **ripristino completo delle impostazioni di fabbrica** con l'opzione **"Also delete event log"** (elimina anche il registro eventi) selezionata; i dati personali vengono cancellati dal dispositivo.

11.3 Se si dimentica il PIN dell'amministratore

1. Connettersi al WiFi del dispositivo (se necessario, spegnere e riaccendere il dispositivo e sfruttare i primi 10 minuti).
2. **Sign in** → **I forgot my PIN** → selezionare l'account dell'amministratore → inserire il **codice di ripristino** e il nuovo PIN.
3. Nessun'altra impostazione cambia; l'operazione viene scritta nel registro eventi (**Event Log**).

Il recupero non è possibile dalla rete dell'impianto (è richiesta la vicinanza fisica al dispositivo). Dopo 5 tentativi errati di inserimento del codice è prevista un'attesa di 5 minuti.

11.4 Se si dimentica la password del WiFi del dispositivo

- Se il dispositivo è connesso alla rete dell'impianto, accedere al pannello dalla rete dell'impianto come amministratore e impostare una nuova password in **Notifications → WiFi → Device WiFi**.
- Se il pannello non è raggiungibile né dalla rete dell'impianto né dal WiFi del dispositivo, contattare l'assistenza tecnica (support@ionia-automation.com); tenere a portata di mano il numero di serie.

11.5 Aggiornamento software

Gli aggiornamenti vengono eseguiti dall'**assistenza autorizzata** tramite il WiFi del dispositivo. I pacchetti sono firmati dal produttore; il dispositivo rifiuta pacchetti non firmati o danneggiati. Il nuovo software diventa definitivo solo dopo aver verificato che funzioni correttamente. **Durante l'aggiornamento tutte le uscite vengono rilasciate (disattivate)**; al riavvio del dispositivo le uscite vengono di nuovo comandate in base alle regole. Impostazioni e registrazioni vengono conservate durante l'aggiornamento.

12 Pannello frontale: LED e pulsanti

12.1 LED di stato

All'accensione o al riavvio del dispositivo, per alcuni secondi si accende solo il LED verde. Poi i LED si accendono uno dopo l'altro (circa 5 secondi) e quindi indicano lo stato:

LED	Colore	Acceso	Spento
LED4	Verde	Il dispositivo funziona correttamente	È presente un problema critico (vedere LED1)
LED3	Giallo	Il dispositivo è connesso al WiFi dell'impianto	WiFi dell'impianto assente o non configurato (le notifiche non vengono inviate)
LED2	Giallo	Scheda di memoria inserita e funzionante	Scheda di memoria assente o non leggibile
LED1	Rosso	**Errore critico**: i due processori del dispositivo non riescono a comunicare oppure la memoria è a un livello critico	Nessun errore critico

- Se durante il primo minuto dopo l'avvio il **LED verde lampeggia lentamente**, il dispositivo è ancora in fase di avvio; attendere.
- **Se il LED1 è acceso**, riavviare il dispositivo (Sezione 12.2). Se il problema persiste, contattare l'assistenza autorizzata.
- Mentre si esegue un'operazione con i pulsanti, i LED ne indicano l'avanzamento; al termine tornano alla visualizzazione dello stato.

12.2 Pulsanti

Operazione	Come	Risultato
Riavvio	Tenere premuto il **pulsante centrale per 10 secondi**	Il dispositivo si riavvia; le impostazioni vengono conservate. Le uscite si disattivano durante il riavvio

Il riavvio può essere eseguito anche dal pannello: **System → Restart device** (il pannello resta disconnesso per circa 1 minuto; le uscite si disattivano durante il riavvio). Il ripristino completo delle impostazioni di fabbrica si esegue dal pannello (Sezione 11.2).

13 Risoluzione dei problemi

Sintomo	Causa possibile	Soluzione
WiFi del dispositivo non visibile	Il dispositivo è connesso alla rete dell'impianto ed è in modalità "off while connected"	Spegnere e riaccendere il dispositivo; è visibile per i primi 10 minuti. Oppure accedere al pannello dalla rete dell'impianto
Il pannello non si apre dalla rete dell'impianto	Ci si trova su una rete diversa / il nome `.local` non viene risolto	Connettersi alla stessa rete; provare l'indirizzo IP
Connessi alla rete dell'impianto ma il pannello non si apre nemmeno con l'indirizzo IP	Isolamento dei client / rete ospiti sul router	Disattivare l'isolamento oppure collegare dispositivo e smartphone alla rete principale; in una rete aziendale chiedere al reparto IT un'eccezione (Sezione 6.4)
"Initial setup only from the device's own WiFi..."	Nessun amministratore definito	Connettersi tramite il WiFi del dispositivo e completare la procedura guidata
Non si connette al WiFi dell'impianto	Rete a 5 GHz, password errata, segnale debole	Selezionare una rete a 2,4 GHz; verificare la password; migliorare il segnale (armadio metallico)
Il messaggio Telegram non arriva	Bot non avviato, ID errato, canale disattivato	Sezione 7.3; verificare la causa dell'errore in **Notifications → Log**
L'e-mail non arriva	Cartella spam, indirizzo errato	Controllare la cartella spam e l'indirizzo; consultare il registro (**Log**)
Alcune persone non ricevono messaggi	Fuori orario di lavoro + gravità bassa; persona non tra i destinatari	Impostazione di orario di lavoro / gravità della persona e destinatari dell'ingresso
Un ingresso non genera mai allarmi	Ingresso Disabled, direzione di trigger errata, cablaggio	**Alarm Settings → Rules**; osservare lo stato dell'ingresso nella **Dashboard**
Lo stesso ingresso genera allarmi troppo spesso	Rimbalzo del contatto / disturbi	Aumentare il tempo di debounce; usare "Return to Normal — at least ... s"
Uscita indicata come attiva ma l'apparecchiatura non funziona	Cablaggio, alimentazione del carico, relè di interfaccia	Confrontare **Requested** e **Actual pin** sulla scheda; controllare il lato carico
Avviso "Requested and actual pin differ"	Problema nel circuito di uscita, sovraccarico	Controllare la corrente del carico (max. 100 mA); se persiste, contattare l'assistenza
"No connection to output modules"	Connessione interna del dispositivo persa; uscite rilasciate in stato sicuro	Riavviare il dispositivo; se non basta, contattare l'assistenza
"Module fault: DO0-7 / DO8-15"	Un modulo di uscita segnala un guasto	Contattare l'assistenza
Pagina **Plant**: "... device not seen for 2 minutes"	Dispositivo spento, rete diversa o isolamento dei client	Verificare una per una le cause indicate nell'avviso
Pagina **Plant**: "plant password ... differs"	Password d'impianto diverse sui dispositivi	Inserire la stessa password su tutti i dispositivi in **Plant → Plant settings**

Sintomo	Causa possibile	Soluzione
Il dispositivo si riavvia da solo	Problema di alimentazione	Controllare l'alimentazione; comunicare all'assistenza la causa indicata in **System → Boot history**
LED1 (rosso) acceso	Errore critico	Riavviare il dispositivo; se persiste, contattare l'assistenza
L'avviso "Setup not complete" non scompare	Manca l'amministratore, un destinatario delle notifiche o il WiFi dell'impianto	**Settings → Setup wizard**

Quando si contatta l'assistenza, tenere a portata di mano: il numero di serie, uno screenshot della pagina **System** e il momento in cui è iniziato il problema.

14 Dati tecnici (riepilogo)

Voce	Valore
Alimentazione	24 V DC nominale, 15–30 V DC
Ingressi digitali	16 (DI00–DI15); PNP, 24 V DC (1 logico ≥ 15 V); isolamento ottico, 2500 V
Scansione ingressi	1 ms; filtraggio del segnale 0–10 000 ms per ingresso
Uscite digitali	16 (DO00–DO15); transistor di tipo sourcing (PNP), la tensione di uscita segue l'alimentazione; max. 100 mA per uscita
Modalità delle uscite	Continua (tempo massimo di attivazione opzionale) · Impulsiva (durata impostata, frequenza limitata)
Stato sicuro delle uscite	Uscite disattivate all'avvio, durante gli aggiornamenti software, in caso di perdita della connessione interna e durante la mancanza di alimentazione
Regole di uscita	Fino a 16 regole; per regola 8 condizioni, 4 gruppi OR, 4 uscite
Comunicazione	WiFi 2,4 GHz 802.11 b/g/n (nessun 5 GHz); client sulla rete dell'impianto + access point proprio. Nessuna connessione Ethernet / cellulare
Notifica	Telegram · E-mail · Webhook · pannello web
Utenti	Fino a 32 persone, 16 ruoli; PIN a 4–6 cifre per persona
Orologio	Sincronizzato da internet (nessun orologio con batteria tampone)
Montaggio	Fissaggio a vite su superficie piana, all'interno di un quadro elettrico; 4 × Ø3,8 mm
Dimensioni / peso	115 × 114 × 45 mm / 250 g
Morsetti	Morsetti a vite
Involucro	Per montaggio all'interno di un quadro elettrico; protezione parziale contro la polvere, non protetto contro l'acqua
Garanzia	24 mesi dalla data della fattura

15 Lista di controllo per la messa in servizio

✓	Verifica
☐	Collegamenti di alimentazione, ingressi e uscite eseguiti; i carichi delle uscite non superano 100 mA
☐	Dati dell'etichetta (numero di serie, nome WiFi del dispositivo) registrati
☐	**Password del WiFi del dispositivo modificata**, nuova password registrata
☐	Amministratore creato; **secondo amministratore** definito
☐	Codice di ripristino conservato in un luogo sicuro
☐	Nome e ubicazione del dispositivo inseriti
☐	Connesso al WiFi dell'impianto; il pannello si apre dalla rete dell'impianto; al dispositivo è assegnato un indirizzo fisso
☐	Ingressi utilizzati denominati, ingressi non utilizzati su Disabled
☐	Ogni ingresso attivato **fisicamente**; canale corretto e direzione corretta verificati sul pannello
☐	Persone aggiunte; Start premuto nel bot Telegram; **messaggi di prova ricevuti**
☐	Destinatari e (se necessario) escalation impostati; un allarme confermato e la notifica "confermato" ricevuta
☐	Uscite denominate e provate manualmente; stato richiesto ed effettivo coincidono
☐	Regole di uscita impostate e **provate in campo** (attivazione, disattivazione, regole di soppressione)
☐	In caso di più dispositivi: stessa password d'impianto su tutti, tutti online nella pagina **Plant**
☐	(Consigliato) Report interruzioni attivato
☐	Backup delle impostazioni scaricato e consegnato alla direzione dell'impianto
☐	Manuale d'uso e indirizzo del pannello consegnati agli utenti

16 Garanzia e assistenza

- **Garanzia:** 24 mesi dalla data della fattura, contro difetti di materiale e di fabbricazione. La garanzia è registrata in base al numero di serie. Le condizioni sono riportate nel Certificato di garanzia fornito con il prodotto.
- Installazione e uso non conformi alle guide, valori di alimentazione / ingresso / uscita fuori dai limiti, sovratensioni, acqua, umidità, urti, apertura non autorizzata dell'involucro e interruzioni di servizi di terzi (internet, Telegram, e-mail) non sono coperti dalla garanzia.
- **Quando si richiede assistenza**, tenere a portata di mano: il numero di serie (etichetta del dispositivo), la fattura, una descrizione del guasto e, se possibile, uno screenshot della pagina **System**. Prima di inviare il dispositivo in assistenza, eseguire un backup delle impostazioni e un ripristino completo delle impostazioni di fabbrica.

Assistenza tecnica: **support@ionia-automation.com** · Vendite e informazioni: **info@ionia-automation.com** · **ionia-automation.com**

Contatti
Vendite e informazioni: info@ionia-automation.com
Assistenza tecnica: support@ionia-automation.com
ionia-automation.com