



SEGNALAZIONE GUASTI E GESTIONE ALLARMI INDUSTRIALI

AS1111

Manuale d'uso

Dispositivo da quadro per monitoraggio e notifica allarmi · 32 ingressi digitali



Indice

1	Informazioni su questo manuale	4
2	Accesso al pannello	4
2.1	Apertura del pannello	4
2.2	Accesso e PIN	4
2.3	Struttura dello schermo e navigazione	5
2.4	Ruoli e permessi	5
3	Dashboard	6
3.1	Ingressi digitali	6
3.2	Alarm Summary e Quick Actions	6
3.3	System Status	7
4	Allarmi	7
4.1	Messaggio di notifica	7
4.2	Livelli di gravità	7
4.3	Ciclo di vita dell'allarme	7
4.4	Pagina Alarm Monitoring	8
4.5	Conferma, tacitazione e reset	8
4.6	Escalation (notifica a livelli)	9
5	Persone e canali di notifica	9
5.1	My account	9
5.2	Ricevere le notifiche su Telegram	9
5.3	Orario di lavoro e gravità minima	10
5.4	Aggiunta di persone (amministratore)	10
5.5	Comportamento delle notifiche	10
5.6	Registro notifiche	10
6	Impostazioni di ingressi e allarmi (amministratore)	10
6.1	Regole	10
6.2	Opzioni di allarme	11
6.3	Destinatari e permesso di conferma	11
6.4	Impostazioni di escalation	11
6.5	Salvataggio e reset	12
7	Registro eventi (Event Log)	12
8	Vista impianto	13
9	Interruzioni e pagina System	14
9.1	Comportamento in caso di interruzione	14

9.2	Messaggi di interruzione	14
9.3	Report interruzioni	14
9.4	Pagina System	15
10	Backup delle impostazioni (amministratore)	15
11	Integrazione: ERP e software di manutenzione (amministratore, IT)	15
11.1	Webhook	15
11.2	Endpoint di lettura (REST)	16
11.3	Sicurezza	17
12	Attività dell'amministratore in sintesi	17
13	Domande frequenti	18
14	Glossario	18

1 Informazioni su questo manuale

Questo manuale è destinato a operatori, tecnici, capituono e amministratori che utilizzano ogni giorno il pannello web dell'Alert SCADA AS1111. Montaggio, cablaggio, impostazioni di rete e configurazione iniziale del dispositivo sono descritti nella **Guida all'installazione AS1111**.

Alcune sezioni sono destinate a tutti (accesso al pannello, monitoraggio degli allarmi, conferma, registro eventi, My account). Le sezioni che richiedono permessi di configurazione (persone, regole di allarme, destinatari, escalation, backup, integrazione) sono contrassegnate nel titolo con **amministratore**.

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 di allarme obbligatori per legge**. Il recapito delle notifiche dipende dall'alimentazione elettrica, da internet e da servizi di terzi (Telegram, e-mail).

Il pannello può essere impostato in turco o in inglese. I nomi di pagine e pulsanti sono riportati qui come appaiono nell'interfaccia inglese; la dicitura esatta sullo schermo può differire leggermente. Le schermate mostrano l'interfaccia in turco e sono esempi; i nomi degli ingressi e dei dispositivi nel vostro impianto saranno diversi. Le schermate del pannello possono indicare il modello come **ION8-1111**.

2 Accesso al pannello

2.1 Apertura del pannello

Il pannello è una pagina web; **non si installa alcuna app**. Su uno smartphone, tablet o computer collegato alla rete dell'impianto, aprire il browser e digitare l'indirizzo fornito dall'amministratore:

- **<http://ion8-xxxxxx.local>** oppure il nome che l'amministratore ha assegnato al dispositivo (ad es. **<http://linea-presse-2.local>**), oppure
- l'indirizzo IP del dispositivo (ad es. **<http://192.168.1.50>**).

Entrambi gli indirizzi sono mostrati come link cliccabili e copiabili nella scheda WiFi in **Settings** e nella pagina **Notifications** → **WiFi**. Su alcuni smartphone Android l'indirizzo **.local** non si apre; in tal caso utilizzare l'indirizzo IP.

Sullo smartphone

Il pannello si adatta allo schermo dello smartphone; le tabelle vengono mostrate come schede una sotto l'altra. **Aggiungere la pagina alla schermata Home** dal menu del browser, così si apre con un solo tocco.

Se il pannello non si apre affatto mentre lo smartphone è collegato alla WiFi dell'impianto, sul router potrebbe essere attivo l'**isolamento dei client / rete ospiti**; informare l'amministratore o il reparto IT. Il pannello si utilizza solo nella rete dell'impianto; non è esposto a internet.

2.2 Accesso e PIN

- Salvo diversa scelta dell'amministratore, il pannello **può essere consultato senza accesso**. Per confermare un allarme o modificare un'impostazione, usare **Sign in** in alto a destra → selezionare il proprio nome → inserire il proprio **PIN**.
- Il PIN è personale, ha 4–6 cifre ed è memorizzato nel dispositivo in forma non reversibile.
- Dopo 5 tentativi errati con il PIN occorre attendere 5 minuti. In caso di inattività per 30 minuti, la sessione viene chiusa automaticamente.
- Con **Settings** → **View access** l'amministratore può richiedere l'accesso anche solo per consultare il pannello.

- Se si dimentica il PIN, l'amministratore ne assegna uno nuovo. Un PIN dell'amministratore dimenticato si reimposta con il codice di ripristino del dispositivo (Guida all'installazione).

2.3 Struttura dello schermo e navigazione

- Il **menu** è raggruppato per argomento: Monitoring, Alarms, Management. Sullo smartphone il menu si trova dietro il pulsante  in alto a sinistra.
- **Barra inferiore sullo smartphone:** le schede Home, Alarms, Plant, Events e Menu sono sempre visibili.
- Riga **Related** (correlati): in cima a ogni pagina, porta con un tocco alle pagine utilizzate insieme a quella pagina (ad es. Alarm Monitoring → Alarm Settings).
- **Barra superiore:** il numero di allarmi attivi () è visibile in ogni pagina. Il pulsante  cambia la lingua (turco / inglese), il pulsante  alterna la visualizzazione chiara e scura.
- **Barra di stato:** indica se il pannello è collegato al dispositivo (**Connected** / **Disconnected**) e il tempo di funzionamento del dispositivo. Se compare "Disconnected", le informazioni sullo schermo non sono aggiornate; verificare la rete e ricaricare la pagina.
- **Dettagli del canale:** toccare una scheda di ingresso nella Dashboard o il nome di un canale nell'Event Log: compaiono lo stato attuale, gli ultimi eventi e i pulsanti **Full history** (Event Log filtrato su quel canale) / **Alarm setting**.
- **Modifiche non salvate:** se si modifica un'impostazione e si passa a un'altra pagina senza salvare, viene chiesto se salvare: **Save** oppure **Leave without saving**.

2.4 Ruoli e permessi

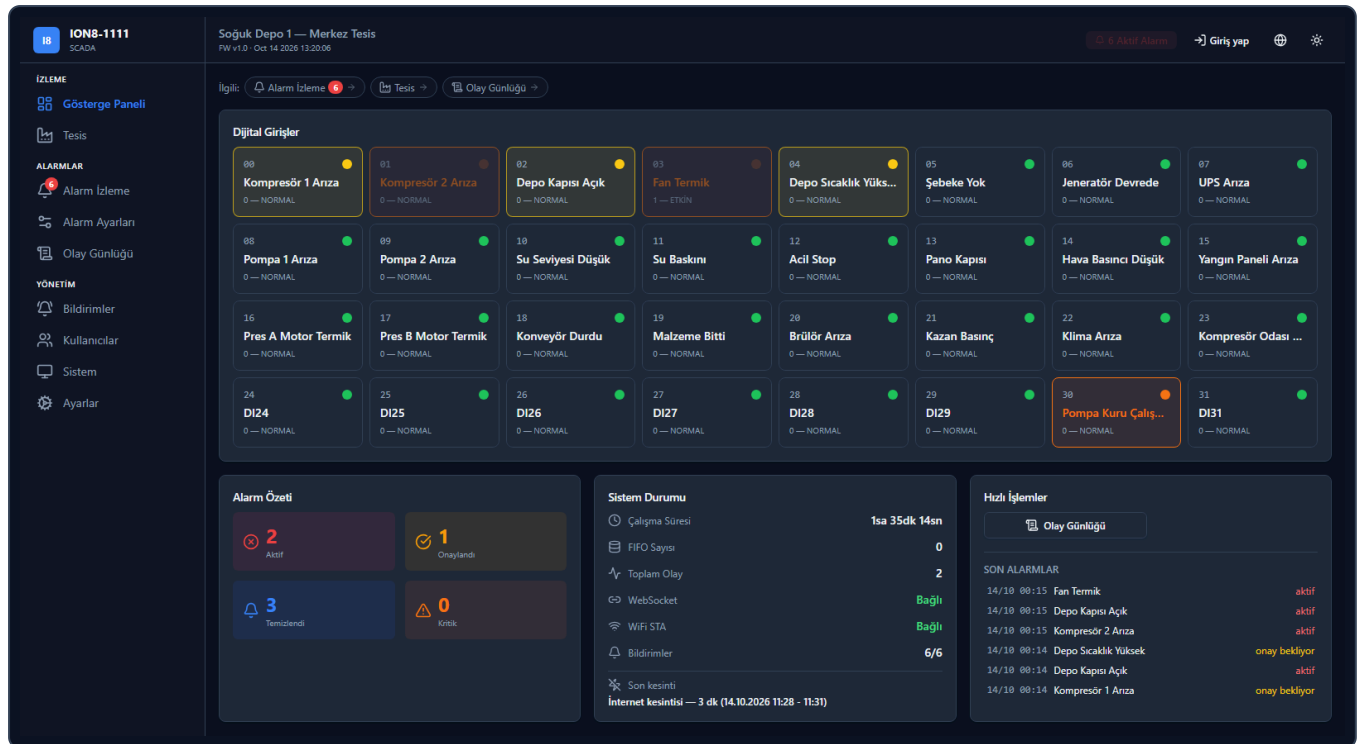
Ogni persona ha uno o più **ruoli** (ad es. Amministratore, Capoturno, Tecnico, Operatore). I permessi vengono assegnati ai ruoli (**Users** → **Roles**). È possibile definire fino a 32 persone e 16 ruoli.

Permesso (nel pannello)	Consente
ACK	Confermare gli allarmi
Silence	Tacitare temporaneamente il suono dell'allarme / le notifiche ripetute
Config	Regole di allarme, destinatari, impostazioni del dispositivo e delle notifiche
Add user	Aggiungere ed eliminare persone, assegnare ruoli e PIN
Service (maintenance)	Impostazioni di assistenza e schermate di diagnostica; solo per l'assistenza autorizzata

Amministratore completo = Config + Add user. Alcune operazioni (modifica del ruolo autorizzato alla conferma, report interruzioni, ripristino delle impostazioni di fabbrica) possono essere eseguite solo da un amministratore completo. Il dispositivo non consente di eliminare l'ultimo amministratore; definire **almeno due** amministratori.

3 Dashboard

La Dashboard è la pagina iniziale del dispositivo: stato attuale dei 32 ingressi, riepilogo degli allarmi, stato di salute del sistema e ultimi allarmi in un'unica schermata.



Dashboard (computer): 32 schede degli ingressi, Alarm Summary, System Status e Latest alarms (interfaccia in turco)

3.1 Ingressi digitali

Ciascuno dei 32 ingressi è rappresentato da una scheda: numero dell'ingresso (00–31), nome e testo dello stato attuale (ad es. "Pompa in funzione"). **Il colore della scheda indica lo stato di allarme**, non se l'ingresso è 0 o 1:

Aspetto	Significato	Cosa fare
Rosso, lampeggiante	Allarme non confermato	Verificare la situazione, confermare
Rosso, fisso	Allarme confermato ma la condizione persiste	Si spegne da solo quando il guasto è eliminato
Giallo / arancione	Ingresso tornato alla normalità, in attesa di conferma	Confermare
Punto blu	Ingresso 1, nessun allarme	—
Punto verde	Ingresso 0, nessun allarme	—

Regola Both Edges

Per gli ingressi che generano un allarme "a ogni variazione" (ad es. notifica di porta aperta / chiusa), l'allarme è la variazione stessa: termina con la conferma. La scheda non resta rossa anche se l'ingresso rimane a 1.

3.2 Alarm Summary e Quick Actions

- Alarm Summary** (riepilogo allarmi): numero di allarmi attivi, confermati, tornati alla normalità (in attesa di conferma) e critici.

- **Quick Actions** (azioni rapide): **Acknowledge all, Silence, Reset, Event Log** (i pulsanti compaiono in base ai propri permessi).
- **Latest alarms** (ultimi allarmi): gli allarmi più recenti e il loro stato (attivo · in attesa di conferma · confermato · chiuso). Toccando una riga si apre l'Event Log.

3.3 System Status

Collegamento del pannello al dispositivo, stato della WiFi dell'impianto e delle notifiche, tempo di funzionamento e **Last outage** (ultima interruzione di alimentazione o di internet, durata e intervallo orario). Un'interruzione di internet in corso è mostrata in rosso.

4 Allarmi

4.1 Messaggio di notifica

Un allarme arriva sul canale configurato per voi (Telegram e/o e-mail). Esempio (tradotto a titolo illustrativo):

```
[CRITICO] Linea Presse 2 - Reparto Saldatura
Canale: Guasto pompa (DI30)
Stato: Pompa ferma
Ora: 04.10.2026 14:32:07
Evento n.: 7629
```

L'intestazione riporta il **livello di gravità**, seguito dal nome e dall'ubicazione del dispositivo; sotto sono indicati l'ingresso, che cosa è accaduto, quando è accaduto e il numero dell'evento. Gli allarmi che arrivano a pochi secondi l'uno dall'altro vengono riuniti in un unico messaggio ("3 allarmi ..."), così lo smartphone non viene sommerso di notifiche.

4.2 Livelli di gravità

All'allarme di ogni ingresso viene assegnato uno dei quattro livelli di gravità: Info (informazione), Warning (avviso), Alarm (allarme), Critical (critico). La gravità compare nell'intestazione della notifica e nel pannello; le impostazioni "gravità minima" e orario di lavoro delle persone e il limite di ripetizione al minuto funzionano in base ad essa.

Gravità	Nell'intestazione della notifica (pannello in turco)	Limite di ripetizione (predefinito, al minuto)
Info	[BILGI]	3
Warning	[UYARI]	3
Alarm	[ALARM]	3
Critical	[KRITIK]	Illimitato

Limite di ripetizione: se lo stesso ingresso genera molti allarmi entro un minuto, quelli in eccesso non vengono inviati (restano nella registrazione). L'amministratore imposta il limite per ogni livello di gravità in **Notifications** → **General**; 0 = illimitato.

4.3 Ciclo di vita dell'allarme

- 1 **L'allarme si verifica:** una notifica raggiunge le persone interessate e nel pannello la scheda lampeggia in rosso.
- 2 **Lo confermate (presa in carico):** indicate così che vi state occupando del guasto. Il nome di chi conferma e il tempo di reazione vengono registrati; le altre persone che hanno ricevuto l'allarme ricevono la notifica "**acknowledged — Acknowledged by: vostro nome**" (confermato da) e l'inoltro ai livelli superiori (escalation) si interrompe.

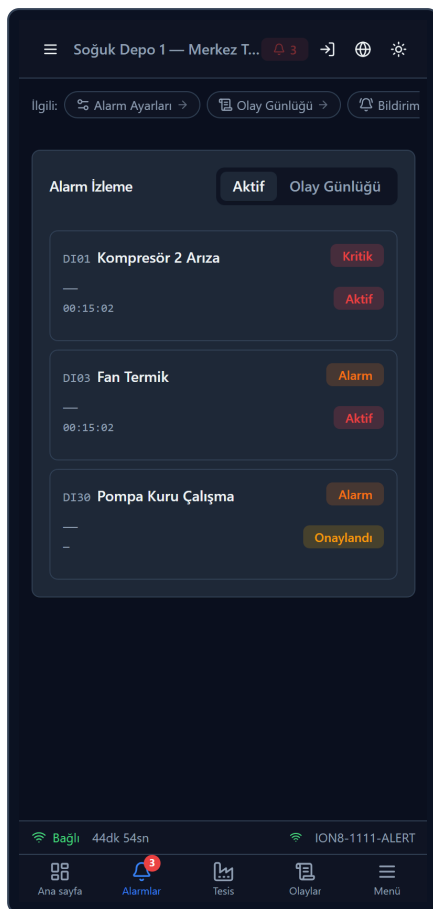
- 3 **La condizione termina:** quando l'ingresso torna alla normalità, l'allarme si chiude. Se attivata per l'ingresso, viene inviata una notifica **"back to normal — lasted X min"** (tornato alla normalità — durata X min).

Se la condizione termina prima della conferma, l'allarme passa allo stato **"back to normal — awaiting acknowledgement"** (tornato alla normalità — in attesa di conferma) e si chiude con la conferma.

Allarmi non confermati

Un allarme non confermato viene segnalato ai **livelli superiori** (capoturno, responsabile manutenzione) dopo i tempi impostati dall'amministratore. Anche se il segnale torna alla normalità, un allarme non confermato continua l'escalation.

4.4 Pagina Alarm Monitoring



La scheda **Active** elenca gli allarmi in attesa di conferma e quelli in corso (sullo smartphone una scheda per ogni ingresso):

Campo	Significato
Canale / Nome	Numero dell'ingresso (DI00–DI31) e nome
Ora	Ora in cui si è verificato l'allarme
Messaggio	Testo della variazione che ha avviato l'allarme
Gravità	Info · Warning · Alarm · Critical
Stato	Active · Acknowledged · Back to normal — awaiting acknowledgement
Conferma	Pulsanti di conferma e tacitazione

Pulsanti in cima alla pagina: **Acknowledge all** · **Silence** · **Reset** · **Test**. La scheda **Event Log** passa allo storico nella stessa pagina.

Alarm Monitoring (smartphone, interfaccia in turco): una scheda per ogni allarme

- **Ogni allarme non confermato è una riga separata.** Ad esempio, se una porta è stata aperta e chiusa due volte prima della conferma, ogni variazione compare su una propria riga con la propria ora e il proprio testo.
- La conferma è **per ingresso**: il pulsante **Acknowledge** di un ingresso chiude insieme tutte le righe di quell'ingresso (accanto al pulsante compare un'indicazione come "acknowledges 2 alarms together").
- **Test** (per le persone autorizzate) genera un allarme di prova per verificare che il sistema funzioni.

4.5 Conferma, tacitazione e reset

- **Conferma:** il pulsante **Acknowledge** nella riga dell'allarme (nella sua scheda sullo smartphone) della pagina Alarm Monitoring, oppure **Acknowledge all**. Se nello stesso impianto sono presenti più dispositivi, è possibile confermare l'allarme di un altro dispositivo anche dalla pagina **Plant**.

- **Se il pulsante Acknowledge non compare:** non si è effettuato l'accesso, il proprio ruolo non ha il permesso di conferma, oppure l'allarme di quell'ingresso può essere confermato solo da un ruolo specifico. **Acknowledge all** conferma solo gli allarmi per cui si dispone del permesso e indica quanti sono stati saltati.
- **Silence:** interrompe temporaneamente le notifiche ripetute (richiede il permesso Silence). Non chiude l'allarme.
- **Reset:** gli allarmi **ritenuti** (latched) persistono, anche se il segnale si ripristina, finché una persona autorizzata non li conferma e preme **Reset**.

Conferme, tacitazioni e reset vengono scritti nell'Event Log insieme al nome di chi li ha eseguiti.

4.6 Escalation (notifica a livelli)

Un allarme non confermato viene inoltrato al livello successivo dopo i tempi impostati. Esempio di catena:

Fase	Quando	A chi (esempio)
Prima notifica	Al verificarsi dell'allarme	Operatore
Livello 1	Se non confermato, dopo 10 min	Capoturno
Livello 2	Se non confermato, dopo altri 10 min	Responsabile manutenzione
Livello 3	Se non confermato, dopo altri 10 min	Direttore generale

Tempi e persone sono esempi; l'amministratore costruisce la catena in base alla vostra organizzazione (Sezione 6.4).

- La catena si interrompe quando l'allarme viene **confermato**. Per un ingresso con conferma automatica, si interrompe anche quando il segnale torna alla normalità.
- Con la conferma automatica disattivata, un allarme **non confermato** continua l'escalation anche se il segnale torna alla normalità.
- Per ogni ingresso è attiva una sola catena: nuove variazioni durante l'attesa della conferma non riavviano la catena.
- In assenza di internet, una fase di escalation non va persa; viene inviata al ritorno della connessione.
- Le notifiche "acknowledged" (confermato) e "back to normal" (tornato alla normalità) vengono inviate a **tutti i livelli raggiunti** (non alla persona che ha confermato).

5 Persone e canali di notifica

5.1 My account

Settings → **My account** (dopo l'accesso). Ciascuno può modificare solo i propri dati:

- Nome e cognome
- **Where notifications should reach me** (dove ricevere le notifiche): Telegram · E-mail · Panel
- ID Telegram e indirizzo e-mail
- **Send me alarms of at least this severity** (gravità minima degli allarmi ricevuti; ad es. solo Alarm e Critical)
- **Working hours** (orario di lavoro)
- **Change PIN** (viene richiesto il PIN attuale)

Solo l'amministratore può modificare il vostro ruolo e i dati delle altre persone.

5.2 Ricevere le notifiche su Telegram

Ogni persona esegue questa operazione una sola volta, sul proprio smartphone:

- 1 In Telegram aprire il **bot di notifica del dispositivo** (il link è riportato nella pagina My account e nella procedura guidata di configurazione) e premere **Start** (Avvia). In caso contrario, il bot non può inviarvi messaggi.

- 2 Aprire @userinfobot e premere **Start**; copiare il numero **Id** dalla risposta.
- 3 Incollare il numero nel campo **Telegram ID** in My account e salvare.

L'account di notifica è fornito pronto con il dispositivo; per Telegram non sono previsti costi né abbonamenti. Le notifiche e-mail possono finire nella cartella spam la prima volta; aggiungere l'indirizzo del mittente all'elenco dei mittenti attendibili.

5.3 Orario di lavoro e gravità minima

Si applicano a ogni persona separatamente:

- **Gravità minima:** gli allarmi al di sotto del livello di gravità selezionato non vengono inviati a quella persona (ad es. il responsabile manutenzione riceve solo Critical).
- **Orario di lavoro:** al di fuori dell'orario di lavoro vengono inviati solo gli allarmi al di sopra del livello di gravità selezionato. Di notte si viene svegliati solo per gli allarmi importanti.

Queste impostazioni filtrano le notifiche; gli allarmi restano comunque visibili nel pannello e nell'Event Log.

5.4 Aggiunta di persone (amministratore)

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, e-mail, gravità minima e orario di lavoro.

- 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.
- Dopo aver aggiunto una persona, inviare un messaggio di prova da **Notifications** → **Log** e verificare che arrivi.

5.5 Comportamento delle notifiche

- **Invio raggruppato:** gli allarmi che arrivano a pochi secondi l'uno dall'altro vengono riuniti in un unico messaggio.
- **Nuovo tentativo:** una notifica che non è stato possibile recapitare a una persona su un canale viene ritentata solo per quella persona e quel canale (0–5 volte, Notifications → General).
- **Limite di ripetizione:** Sezione 4.2.
- **Notifiche di sistema:** dispositivo riavviato (con la durata dell'interruzione di alimentazione), problema di connessione interna, problema della scheda di memoria, riepilogo dell'interruzione di internet e report interruzioni. Vengono inviate ai ruoli di allarme di sistema oppure, se non ne sono definiti, ai ruoli con il permesso Config.

5.6 Registro notifiche

Notifications → **Log**: ogni notifica inviata (allarme, escalation, conferma, ritorno alla normalità, sistema, prova), a chi e su quale canale è stata inviata e con quale esito. Per una notifica che non è stato possibile inviare, viene indicato il **motivo** (l'errore restituito da Telegram o dal server di posta, "no internet" e simili). Toccando una riga si visualizza il testo completo del messaggio.

6 Impostazioni di ingressi e allarmi (amministratore)

6.1 Regole

La pagina **Alarm Settings** → **Rules** ha una riga per ogni ingresso (sullo smartphone una scheda per ogni ingresso).

Impostazione	Descrizione
Channel name	Nome mostrato nelle notifiche e nel pannello (ad es. "Pompa 1 Termico")
Trigger	Disabled (non monitorato) · Rising Edge (fronte di salita: 0→1 allarme, 1→0 ritorno alla normalità) · Falling Edge (fronte di discesa: 1→0 allarme, 0→1 ritorno alla normalità) · Both Edges (entrambi i fronti: ogni variazione è un allarme e una notifica separati)
Debounce (ms)	Filtraggio del segnale: una variazione non viene considerata finché l'ingresso non è rimasto stabile per questo tempo (0–10.000 ms). Filtra i rimbalzi dei contatti e i disturbi brevi
Severity	Info · Warning · Alarm · Critical
Texts	Testi di stato (per 0 e 1; mostrati sotto l'ingresso nel pannello) e messaggi di fronte (la riga "Stato:" nella notifica, ad es. "Porta aperta" / "Porta chiusa")

6.2 Opzioni di allarme

Opzione	Descrizione
Latched	Allarme ritenuto: persiste, anche se il segnale torna alla normalità, finché una persona autorizzata non lo conferma e lo resetta
Auto-acknowledge	Conferma automatica: l'allarme si chiude da solo quando il segnale torna alla normalità; non si attende alcuna conferma
Inverted Logic	Logica invertita, per contatti NC: la scomparsa del segnale (compresa l'interruzione del cavo) è un allarme, il suo ritorno è la normalità
Log only	Solo registrazione: l'evento viene registrato e mostrato nel pannello; non viene inviata alcuna notifica
Back to normal	Viene inviata una notifica quando il segnale torna alla normalità. "at least ... s" (almeno ... s): non viene inviata se l'allarme è durato meno di questo tempo (per ingressi che si attivano e disattivano spesso)
Acknowledged notification	Quando l'allarme viene confermato, le altre persone che lo hanno ricevuto ricevono una notifica "acknowledged — by: ..." (confermato da)

Both Edges

Con questa regola l'allarme è la variazione stessa: si chiude con la conferma e non persiste anche se l'ingresso rimane a 1. Ogni nuova variazione è una notifica separata anche se la precedente non è stata confermata; una sola conferma le chiude tutte.

6.3 Destinatari e permesso di conferma

Nella tabella **Alarm Settings** → **Targets** si sceglie a **quali ruoli e persone** viene inviato l'allarme di ogni ingresso.

L'ultima colonna della tabella è il **ruolo autorizzato alla conferma** (ACK role): solo le persone del ruolo selezionato e gli amministratori completi possono confermare l'allarme di quell'ingresso; ad esempio, solo la squadra di manutenzione può confermare l'allarme della caldaia. "Everyone" (tutti) = tutti coloro che hanno il permesso ACK. Solo un amministratore completo può modificare il ruolo autorizzato alla conferma.

6.4 Impostazioni di escalation

Il pulsante **Escalation** nella riga dell'ingresso nella pagina Targets:

- 1 Attivare l'interruttore **Use escalation**. La **prima notifica** viene inviata al verificarsi dell'allarme (compilata con i destinatari dell'ingresso).

- 2 **Livello 1:** impostare il tempo "se non confermato, ... min dopo la fase precedente" e selezionare le persone (ad es. Capoturno).
- 3 Con **Add level** aggiungere fino a due ulteriori livelli: al massimo 4 fasi compresa la prima notifica; al massimo 4 ruoli + 4 persone per fase.
- 4 Premere **Save**. Per assegnare la stessa catena a tutti gli ingressi, utilizzare **Apply to all inputs** (da premere due volte per conferma).

6.5 Salvataggio e reset

- Le modifiche in Alarm Settings vengono scritte nel dispositivo e diventano permanenti quando si preme **Save**; non vanno perse in caso di interruzione di corrente. Le righe modificate sono evidenziate in giallo e il pulsante indica quanti canali sono stati modificati. **Undo** annulla le modifiche non salvate.
- Reset alarm settings** reimposta regole, nomi e testi di tutti i 32 ingressi; utenti, impostazioni di notifica e destinatari vengono conservati. Dopo il reset **nessun ingresso genera allarmi**.

7 Registro eventi (Event Log)

Tutte le variazioni degli ingressi, gli allarmi, le conferme, gli accessi al pannello e le modifiche delle impostazioni vengono registrati **con data e ora** e con il nome di chi li ha eseguiti. Anche le interruzioni di alimentazione e di internet e i riavvii del dispositivo sono inclusi nel registro.

Zaman	Kanal	Kenar	Mesaj	Önem	Olay No	İşaretler
2026-10-14 17:01:31.400	Su Baskını	✓ Onay	Operatör · alarm 16:57:19 · 4 dk 12 sn sonra onaylandı			
2026-10-14 17:00:16.032	Pompa 1 Arıza	✓ Onay	Operatör · alarm 16:56:58 · 3 dk 17 sn sonra onaylandı			
2026-10-14 16:57:19.205	Su Baskını	↑ Yükselme	Onaylayan: Operatör (4 dk 12 sn sonra onaylandı)	Alarm	1964	0x80
2026-10-14 16:57:18.550	Su Baskını	Ayar	Test alarmı — Operatör			
2026-10-14 16:56:58.836	Pompa 1 Arıza	↑ Yükselme	Onaylayan: Operatör (3 dk 17 sn sonra onaylandı)	Kritik	1963	0x80
2026-10-14 16:56:58.232	Pompa 1 Arıza	Ayar	Test alarmı — Operatör			

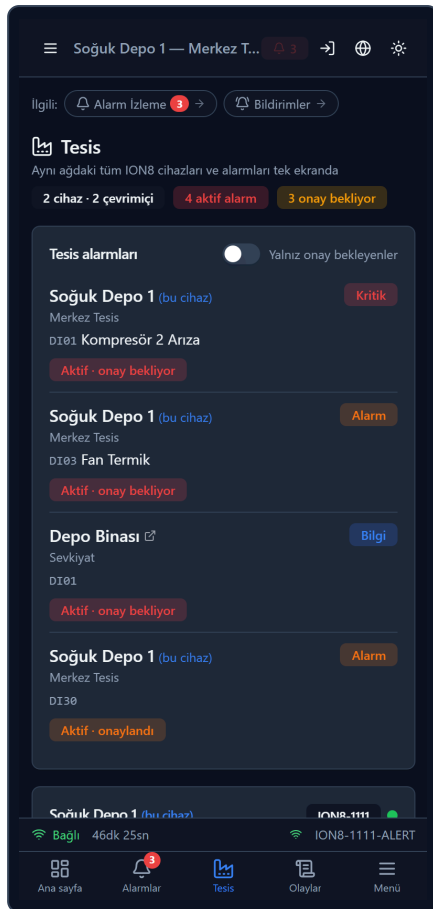
Event Log: chi ha confermato, quando e dopo quanti minuti (interfaccia in turco)

- Filtraggio:** utilizzare i pulsanti **All · Last 1 hour · Last 24 hours · Last 7 days** in alto e **Filter** per selezionare un intervallo di date e consultare lo storico. Per lo storico di un singolo canale, toccare il nome del canale e selezionare **Full history**.
- Colonne:** ora, canale, fronte (↑ salita · ↓ discesa, conferma, impostazione), messaggio, gravità e numero dell'evento.
- Le **righe di allarme** mostrano chi ha confermato, il tempo di reazione e la durata dell'allarme ("⚠ Awaiting acknowledgement" · "✓ Back to normal · lasted 12 min").
- Sullo smartphone ogni evento compare in una propria scheda: nome dell'ingresso, gravità, direzione, ora e descrizione.

La risposta alla domanda "che cosa è successo durante la notte?" al cambio turno si trova qui. Le registrazioni possono essere utilizzate come prova nell'analisi dei guasti e negli audit.

8 Vista impianto

Se nella stessa rete d'impianto sono presenti più dispositivi Alert SCADA (ad es. un AS1111 su un'altra linea o un AS1122 con uscite), la pagina **Plant** li mostra tutti in un'unica schermata.



Pagina Plant (smartphone, interfaccia in turco)

Sezione	Contenuto
Riga superiore	Quanti dispositivi sono visibili e quanti sono online; totale degli allarmi attivi e non confermati nell'impianto
Plant alarms	Gli allarmi di tutti i dispositivi in un unico elenco: dispositivo, ingresso, gravità, stato. L'interruttore Awaiting acknowledgement only filtra l'elenco
Schede dei dispositivi	Nome, ubicazione, modello di ogni dispositivo, se è online, e i suoi ingressi (rosso/arancione = allarme, verde = attivo). Open device page passa al pannello di quel dispositivo

Confermare l'allarme di un altro dispositivo: pulsante **Acknowledge** nell'elenco (è necessario il permesso di conferma). La conferma viene trasmessa a quel dispositivo e registrata a vostro nome. Se la riga indica "remote acknowledgement off", l'amministratore di quel dispositivo ha disattivato la conferma da altri dispositivi: confermare l'allarme nel pannello di quel dispositivo. Se indica "device not visible", al momento il dispositivo non è raggiungibile.

- Se da un dispositivo non arriva alcun segnale per 6 secondi, viene mostrato "no connection". Se un dispositivo visto in precedenza non è più visibile per 2 minuti, la pagina Plant mostra le possibili cause (dispositivo spento, rete diversa, isolamento dei client, password d'impianto diversa).
- Affinché i dispositivi si vedano a vicenda, tutti devono trovarsi **nella stessa rete WiFi dell'impianto** e avere inserita **la stessa password d'impianto** (amministratore: **Plant** → **Plant settings**). Internet non è necessario.
- Toccando il nome di un altro dispositivo, il suo pannello si apre in una nuova scheda del browser; questi link funzionano mentre lo smartphone è collegato alla WiFi dell'impianto.
- La pagina Plant non sostituisce il pannello di ciascun dispositivo: impostazioni e regole si modificano nel pannello di ogni dispositivo. Per comandare le uscite di un AS1122 con gli allarmi dell'AS1111, la regola si imposta nel pannello dell'AS1122.

9 Interruzioni e pagina System

9.1 Comportamento in caso di interruzione

Situazione	Cosa fa il dispositivo	Cosa si vede
Internet assente	Continua a monitorare e registrare gli ingressi; trattiene le notifiche	Al ritorno di internet il dispositivo verifica la connessione (fino a 90 s); le notifiche trattenute arrivano con l'annotazione "... min in ritardo (nessuna connessione)", seguite da un riepilogo dell'interruzione. Le notifiche più vecchie di 30 minuti non vengono inviate e restano nell'Event Log. Per interruzioni inferiori a 1 minuto senza allarmi nel frattempo non viene inviato alcun messaggio
Interruzione di corrente	Non funziona e non può monitorare gli ingressi. Impostazioni e registrazioni vengono conservate	Al ritorno della tensione, una notifica "Dispositivo riavviato: interruzione di corrente ...". Gli ingressi passati in stato di allarme durante l'interruzione generano un allarme all'avvio
Report mancante	—	Se il report interruzioni è attivo, all'ora prevista arriva un messaggio "sistema in funzione" o un report interruzioni. In caso contrario, verificare l'alimentazione e la connessione internet del dispositivo

L'AS1111 dispone di un **orologio con batteria tampone**: l'ora di inizio e di fine di un'interruzione di corrente viene registrata correttamente anche senza internet. Per un monitoraggio senza interruzioni si consiglia un'alimentazione protetta da UPS.

9.2 Messaggi di interruzione

Esempi (tradotti a titolo illustrativo):

Dopo un'interruzione di corrente

```
Dispositivo riavviato: interruzione di corrente ~10 min 45 s (21:00 - 21:11).
In questo intervallo gli ingressi non sono stati monitorati.
```

Riepilogo dell'interruzione di internet

```
[SISTEMA] Linea Presse 2 - Reparto Saldatura
Connessione internet assente per 7 min (23:22 - 23:29). 2 notifiche sono state trattenute
durante l'interruzione e inviate al ritorno della connessione.
```

Report interruzioni

```
[REPORT INTERRUZIONI] Linea Presse 2 - Reparto Saldatura
Report interruzioni (04.10 21:00 - 04.10 22:00)
1 interruzione:
- Internet: 1 h 26 min (04.10 20:59 - 22:26)
Totale: nessuna interruzione di corrente, internet 1 h 26 min.
```

9.3 Report interruzioni

Notifications → **Outage report** (amministratore completo): frequenza del report (ogni ora ... ogni settimana), ora / giorno e destinatari. Vengono riportate tutte le interruzioni del periodo selezionato; se non ce ne sono state, viene inviato un messaggio **"sistema in funzione"**. Questo messaggio conferma regolarmente che il dispositivo funziona e può raggiungervi: anche il silenzio è un'informazione. Impostazione predefinita: disattivato.

9.4 Pagina System

La pagina **System** mostra le informazioni sullo stato di salute del dispositivo: memoria, WiFi, scheda di memoria e stato della connessione interna, e la **Boot history** (cronologia avvii: motivo degli ultimi 16 avvii — interruzione di corrente / riavvio pianificato / errore software; tempo di funzionamento precedente). La cronologia avvii non viene cancellata dal ripristino delle impostazioni di fabbrica.

- **Restart device:** le impostazioni vengono conservate; il pannello resta disconnesso per circa 1 minuto.
- Quando si contatta l'assistenza, allegare una schermata di questa pagina.

10 Backup delle impostazioni (amministratore)

Settings → Settings backup:

- **Download backup:** ruoli, persone, destinatari degli allarmi ed escalation, nomi e testi degli ingressi, impostazioni di notifica, report interruzioni, nome del dispositivo e impostazione d'impianto vengono salvati in un unico file (.json). Facoltativi: dati di contatto delle persone e WiFi dell'impianto. **I PIN non vengono mai inclusi nel backup.**
- **Restore:** selezionare il file, spuntare le sezioni una per una, **Restore selected**. Se la WiFi dell'impianto è già la stessa, non viene modificata. Il backup può essere ripristinato sullo stesso dispositivo o su uno nuovo; assegnare il PIN alle nuove persone dalla pagina Users.

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 prima di modifiche importanti.

11 Integrazione: ERP e software di manutenzione (amministratore, IT)

Gli eventi di Alert SCADA possono essere trasmessi in due modi a sistemi come ERP, CRM, software di manutenzione / ordini di lavoro o SCADA. Questa sezione è un riepilogo; per tutti i campi e gli esempi, il vostro reparto IT può richiedere la **Guida all'integrazione** a support@ionia-automation.com.

Esigenza	Metodo	Direzione
Aprire un ordine di lavoro / una registrazione al verificarsi di un allarme; aggiornarlo alla conferma o alla risoluzione	Webhook	Dispositivo → vostro server (HTTP POST, JSON), nel momento dell'evento
Stato attuale, eventi passati e interruzioni su un display o in un report	Endpoint di lettura (REST)	Vostro software → dispositivo (HTTP GET, JSON)

Scrivere impostazioni, confermare allarmi o aggiungere persone dall'esterno non fa parte dell'integrazione; queste operazioni si eseguono solo in una sessione del pannello protetta da PIN.

11.1 Webhook

Un webhook si configura sul dispositivo come una **persona**: ovunque vadano gli allarmi, vengono inviati anche all'indirizzo del webhook con le stesse regole.

- 1 **Users → People → Add person.** Nome: ad es. **ERP**. Non assegnare un PIN.
- 2 Tra i canali di notifica spuntare solo **Webhook** e inserire l'indirizzo del vostro server nel campo **URL** (al massimo 127 caratteri).

- 3 Aggiungere questa persona (o il suo ruolo) ai destinatari degli ingressi da monitorare; se necessario, anche ai livelli di escalation. Per inviare tutto, lasciare la gravità minima su **Info** e l'orario di lavoro vuoto.
- 4 Nella scheda **Settings** → **Integration (webhook)** inserire l'indirizzo e provarlo con **Send**; sullo schermo deve comparire "Webhook OK 200".
- 5 Consigliato: nella stessa scheda attivare la firma con **Generate key**. La chiave viene mostrata una sola volta; inserirla nel sistema ricevente.

Proprietà	Valore
Richiesta	POST, Content-Type: application/json, UTF-8, un singolo oggetto JSON
Indirizzo	http:// o https:// ; con HTTPS il certificato del server viene verificato rispetto ai certificati radice pubblici (i certificati autofirmati non sono accettati)
Timeout / esito positivo	10 secondi / il server deve restituire 2xx
In caso di errore	La stessa notifica viene ritentata (0–5 volte); in assenza di rete viene trattenuta, quelle più vecchie di 30 minuti non vengono inviate
Tipo di evento (type)	alarm · escalation · ack · normal · system · test
Campi principali	device, location, channel (0–31), channel_name, state, severity (INFO ... CRITICAL), event_id, time, subject, text
Firma	HMAC-SHA256 facoltativa; marca temporale e firma vengono inviate negli header HTTP

Filtrare i duplicati

A causa dei nuovi tentativi, lo stesso evento può arrivare due volte. Sul lato ricevente, filtrare i duplicati tramite la combinazione `channel + event_id + type`. Per ricevere anche le notifiche di sistema, aggiungere la persona webhook a uno dei ruoli di allarme di sistema.

11.2 Endpoint di lettura (REST)

Indirizzo: `http://<indirizzo-dispositivo>/api/...`; metodo GET, risposta JSON. Assegnare al dispositivo un indirizzo IP fisso. Interrogare al massimo ogni 2 secondi, preferibilmente ogni 5–10 secondi; per gli eventi in tempo reale utilizzare il webhook.

Endpoint	Contenuto
/api/status	Riepilogo del dispositivo: modello, nome, ubicazione, tempo di funzionamento, numero di allarmi attivi, stato della scheda di memoria
/api/alarms	Ingressi non in stato normale e relativo stato (attivo · confermato · tornato alla normalità, in attesa di conferma)
/api/events?since=<n>	Eventi recenti; con <code>since</code> , solo quelli nuovi
/api/outages	Le ultime 32 interruzioni di corrente / internet e gli ultimi 16 avvii
/api/device	Modello, nome del dispositivo, ubicazione
/api/alarm/rules	Nome, tipo di trigger, gravità e testi di stato di ogni ingresso
/api/stats	Contatori giornalieri e contatori di invio delle notifiche

Endpoint	Contenuto
/api/peers	Altri dispositivi nella stessa rete e relativi riepiloghi degli allarmi

Se View access è attivo, gli endpoint diversi da /api/status e /api/stats richiedono una sessione; per l'integrazione, definire una persona e un ruolo separati con soli permessi di monitoraggio.

11.3 Sicurezza

- Il pannello e gli endpoint di lettura funzionano tramite **HTTP** non cifrato. Utilizzare il dispositivo solo in una rete d'impianto affidabile e non esporlo a internet; per l'accesso remoto utilizzare una VPN.
- Il corpo del webhook contiene nomi di persone e informazioni sull'impianto; se il server ricevente si trova al di fuori della vostra rete, utilizzare **HTTPS** e attivare la firma.

12 Attività dell'amministratore in sintesi

Attività	Dove
Aggiungere / rimuovere persone, assegnare ruoli e PIN	Users → People
Modificare i permessi dei ruoli	Users → Roles
Nome dell'ingresso, condizione di allarme, gravità, testi, opzioni	Alarm Settings → Rules
Chi riceve l'allarme, escalation, ruolo autorizzato alla conferma	Alarm Settings → Targets
Report interruzioni (frequenza, destinatari)	Notifications → Outage report
Registro notifiche, messaggio di prova	Notifications → Log
Numero di tentativi, limite di ripetizione	Notifications → General
WiFi dell'impianto, WiFi del dispositivo (nascondere / spegnere / password)	Notifications → WiFi
Nome e ubicazione del dispositivo	Settings → Device name and location
Scaricare / ripristinare il backup delle impostazioni	Settings → Settings backup
Richiedere l'accesso per consultare il pannello	Settings → View access
Prova del webhook e chiave di firma	Settings → Integration (webhook)
Password d'impianto, conferma da altri dispositivi	Plant → Plant settings
Riavviare il dispositivo	System → Restart device
Codice di ripristino, ripristino completo delle impostazioni di fabbrica	Settings (solo dalla WiFi del dispositivo)
Tornare alla procedura guidata di configurazione	Settings

Buone pratiche:

- Definire almeno **due** amministratori; gli amministratori dovrebbero utilizzare PIN a 6 cifre.
- Dopo aver aggiunto una persona, inviare un messaggio di prova e verificare che arrivi.
- Scaricare un **backup delle impostazioni** prima di modifiche importanti.
- Attivare il report interruzioni: il messaggio "sistema in funzione" conferma regolarmente che il dispositivo funziona correttamente.

13 Domande frequenti

Domanda	Risposta
Non ricevo notifiche	Il canale è attivo in My account? È stato premuto Start nel bot Telegram? Fuori dall'orario di lavoro gli allarmi di bassa gravità non vengono inviati. L'amministratore può vedere il motivo in Notifications → Log.
Non ricevo e-mail	Controllare la cartella spam; aggiungere l'indirizzo del mittente all'elenco dei mittenti attendibili.
Ho dimenticato il PIN	L'amministratore imposta un nuovo PIN nella pagina Users. Il PIN di un amministratore si reimposta con il codice di ripristino (Guida all'installazione).
Il pannello non si apre	Lo smartphone è collegato alla rete dell'impianto? Provare l'indirizzo IP invece dell'indirizzo <code>.local</code> .
Sullo schermo compare "Disconnected"	Lo smartphone o il computer non raggiunge il dispositivo: verificare la rete e ricaricare la pagina.
Non vedo il pulsante Acknowledge	Effettuare l'accesso. Se continua a mancare, il vostro ruolo non è autorizzato a confermare quell'ingresso.
Lo stesso ingresso genera allarmi troppo spesso	Il contatto potrebbe avere rimbalzi o il segnale potrebbe essere instabile. L'amministratore può regolare il tempo di filtraggio del segnale (Debounce).
L'allarme è confermato ma la scheda è rossa	La condizione persiste (rosso fisso). La scheda si spegne quando il guasto è eliminato.
Se internet si interrompe, gli allarmi vanno persi?	No. Monitoraggio e registrazione continuano; le notifiche vengono inviate al ritorno della connessione (tranne quelle più vecchie di 30 minuti, che restano nell'Event Log).
Le impostazioni dopo un'interruzione di corrente?	Impostazioni e nomi degli ingressi vengono conservati. All'avvio il dispositivo segnala la durata dell'interruzione.
Che cosa indicano le spie del dispositivo?	Verde = funzionamento regolare, giallo (LED3) = collegato alla WiFi dell'impianto, giallo (LED2) = scheda di memoria funzionante, rosso = errore critico. Dettagli: Guida all'installazione.
L'altro dispositivo non compare nella pagina Plant	Entrambi i dispositivi sono nella stessa rete WiFi, le password d'impianto sono uguali e l'isolamento dei client (rete ospiti) sul router è disattivato?
Di notte nessuno si è svegliato per un allarme	Rivedere le impostazioni di escalation con l'amministratore; devono essere definiti livelli superiori e tempi.
Telegram ha un costo?	No. L'account di notifica è fornito pronto con il dispositivo; ogni persona preme Start nel bot una volta.
Notifiche tramite WhatsApp o SMS?	Non in questa versione; i canali di notifica sono Telegram, e-mail, webhook e il pannello web.

14 Glossario

Termine	Significato
Conferma (ACK)	Presa in carico: conferma che ci si sta occupando dell'allarme. Vengono registrati la persona e il tempo di reazione e l'escalation si interrompe
Escalation	Inoltro di un allarme non confermato ai livelli superiori dopo tempi stabiliti
Destinatario (Target)	I ruoli e le persone a cui viene inviato l'allarme di un ingresso

Termine	Significato
Ruolo	Gruppo di persone a cui vengono assegnati i permessi (ad es. Capoturno)
Livello di gravità (Severity)	Il livello dell'allarme: Info · Warning · Alarm · Critical
Trigger	La variazione che avvia l'allarme: fronte di salita (0→1), fronte di discesa (1→0), entrambi i fronti
Debounce (filtraggio del segnale)	Il tempo per cui un ingresso deve restare stabile affinché una variazione venga considerata
Contatto NO / NC	Contatto normalmente aperto / normalmente chiuso
Inverted Logic (logica invertita)	Per contatti NC: la scomparsa del segnale (compresa l'interruzione del cavo) è considerata un allarme
Allarme ritenuto (Latched)	Allarme che persiste, anche se il segnale si ripristina, finché non viene confermato e resettato
Tacitazione (Silence)	Interruzione temporanea delle notifiche ripetute; non chiude l'allarme
Orario di lavoro	Le ore in cui una persona riceve le notifiche; al di fuori, solo gli allarmi al di sopra del livello di gravità selezionato
Invio raggruppato	Invio in un unico messaggio degli allarmi che si verificano a pochi secondi l'uno dall'altro
Report interruzioni	Report periodico delle interruzioni di corrente e di internet; "sistema in funzione" se non ce ne sono state
Password d'impianto	Password comune inserita su tutti i dispositivi della stessa rete affinché si riconoscano tra loro
WiFi del dispositivo	La rete WiFi propria del dispositivo, per configurazione e manutenzione
WiFi dell'impianto	La rete con accesso a internet a cui il dispositivo si collega per inviare le notifiche
Codice di ripristino	Codice specifico del dispositivo utilizzato per impostare un nuovo PIN dell'amministratore in caso di smarrimento
Webhook	Invio automatico degli eventi al vostro server tramite HTTP POST



Contatti

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