



AVISO DE FALLOS Y GESTIÓN DE ALARMAS INDUSTRIALES

AS1111

Manual de usuario

Dispositivo de supervisión de alarmas y notificación para montaje en cuadro ·
32 entradas digitales



Índice

1	Acerca de este manual	4
2	Acceso al panel	4
2.1	Abrir el panel	4
2.2	Inicio de sesión y PIN	4
2.3	Disposición de la pantalla y navegación	5
2.4	Roles y permisos	5
3	Dashboard	6
3.1	Entradas digitales	6
3.2	Alarm Summary y Quick Actions	6
3.3	System Status	7
4	Alarmas	7
4.1	Mensaje de notificación	7
4.2	Niveles de gravedad	7
4.3	Ciclo de vida de una alarma	7
4.4	Página Alarm Monitoring	8
4.5	Reconocer, silenciar y restablecer	8
4.6	Escalado (notificación escalonada)	9
5	Personas y canales de notificación	9
5.1	My account	9
5.2	Recibir notificaciones por Telegram	9
5.3	Horario laboral y gravedad mínima	10
5.4	Añadir personas (administrador)	10
5.5	Comportamiento de las notificaciones	10
5.6	Registro de notificaciones	10
6	Ajustes de entradas y alarmas (administrador)	10
6.1	Reglas	10
6.2	Opciones de alarma	11
6.3	Destinatarios y permiso de reconocimiento	11
6.4	Ajustes de escalado	11
6.5	Guardar y restablecer	12
7	Registro de eventos	12
8	Vista de planta	13
9	Cortes y página System	14
9.1	Comportamiento ante cortes	14

9.2	Mensajes de corte	14
9.3	Informe de cortes	14
9.4	Página System	15
10	Copia de seguridad de los ajustes (administrador)	15
11	Integración: ERP y software de mantenimiento (administrador, TI)	15
11.1	Webhook	15
11.2	Endpoints de lectura (REST)	16
11.3	Seguridad	17
12	Resumen de tareas del administrador	17
13	Preguntas frecuentes	18
14	Glosario	18

1 Acerca de este manual

Este manual está dirigido a los operadores, técnicos, jefes de turno y administradores que utilizan a diario el panel web del Alert SCADA AS1111. El montaje, el cableado, los ajustes de red y la configuración inicial del dispositivo se describen en la **Guía de instalación del AS1111**.

Algunas secciones son para todos (acceso al panel, supervisión de alarmas, reconocimiento, registro de eventos, My account). Las secciones que requieren permisos de configuración (personas, reglas de alarma, destinatarios, escalado, copia de seguridad, integración) llevan la indicación **administrador** en el título.

Seguridad de las personas

Alert SCADA es un dispositivo de **aviso de fallos**. **No sustituye a los sistemas de detección de incendios, detección de gases, seguridad de las personas ni a los sistemas de alarma exigidos por la ley**. La entrega de las notificaciones depende de la alimentación eléctrica, de internet y de servicios de terceros (Telegram, correo electrónico).

El panel puede cambiarse entre turco e inglés. En este manual, los nombres de páginas y botones se indican en inglés; el texto exacto en pantalla puede variar ligeramente. Las capturas de pantalla muestran la interfaz en turco y son ejemplos; los nombres de las entradas y de los dispositivos serán distintos en su instalación. Las pantallas del panel pueden mostrar el modelo como **ION8-1111**.

2 Acceso al panel

2.1 Abrir el panel

El panel es una página web; **no se instala ninguna aplicación**. En un teléfono, una tableta o un ordenador conectado a la red de la planta, abra el navegador y vaya a la dirección que le haya facilitado su administrador:

- **http://ion8-xxxxxx.local** o el nombre que su administrador haya dado al dispositivo (p. ej., **http://linea-prensa-2.local**), o
- la dirección IP del dispositivo (p. ej., **http://192.168.1.50**).

Ambas direcciones se muestran como enlaces que se pueden pulsar y copiar en la tarjeta WiFi de **Settings** y en la página **Notifications** → **WiFi**. La dirección **.local** no se abre en algunos teléfonos Android; en ese caso, utilice la dirección IP.

En el teléfono

El panel se adapta a la pantalla del teléfono; las tablas se muestran como tarjetas una debajo de otra. **Añada la página a la pantalla de inicio** desde el menú del navegador para abrirla con un solo toque.

Si el panel no se abre en absoluto mientras el teléfono está en el WiFi de la planta, es posible que el **aislamiento de clientes / red de invitados** esté activado en el router; comuníquelo a su administrador o a su equipo de TI. El panel se utiliza solo en la red de la planta; no está expuesto a internet.

2.2 Inicio de sesión y PIN

- Salvo que su administrador haya elegido otra cosa, el panel **puede consultarse sin iniciar sesión**. Para reconocer una alarma o cambiar un ajuste, utilice **Sign in** arriba a la derecha → seleccione su nombre → introduzca su **PIN**.
- El PIN es personal, tiene 4–6 cifras y se guarda en el dispositivo de forma no reversible.
- Tras 5 intentos con un PIN erróneo hay que esperar 5 minutos. Si no realiza ninguna acción durante 30 minutos, la sesión se cierra automáticamente.
- Con **Settings** → **View access**, el administrador puede exigir el inicio de sesión incluso para consultar el panel.

- Si olvida su PIN, su administrador le asigna uno nuevo. El PIN olvidado de un administrador se restablece con el código de recuperación propio del dispositivo (Guía de instalación).

2.3 Disposición de la pantalla y navegación

- El **menú** está agrupado por temas: Monitoring, Alarms, Management. En un teléfono, el menú se encuentra tras el botón ☰ de la parte superior izquierda.
- **Barra inferior en el teléfono:** las pestañas Home, Alarms, Plant, Events y Menu están siempre visibles.
- Fila **Related:** en la parte superior de cada página, lleva con un solo toque a las páginas que se utilizan junto con esa página (p. ej., Alarm Monitoring → Alarm Settings).
- **Barra superior:** el número de alarmas activas (🔔) se muestra en todas las páginas. El botón 🌐 cambia el idioma (turco / inglés) y el botón 🌙/☀️ alterna entre la vista clara y la oscura.
- **Barra de estado:** indica si el panel está conectado al dispositivo (**Connected** / **Disconnected**) y el tiempo de funcionamiento del dispositivo. Si muestra "Disconnected", la información en pantalla no está actualizada; compruebe su red y vuelva a cargar la página.
- **Detalles del canal:** toque una tarjeta de entrada en el Dashboard o el nombre de un canal en el Event Log: aparecen el estado actual, los eventos recientes y los botones **Full history** (Event Log filtrado por ese canal) / **Alarm setting**.
- **Cambios sin guardar:** si cambia un ajuste y pasa a otra página sin guardar, se le pregunta si desea guardar: **Save** o **Leave without saving**.

2.4 Roles y permisos

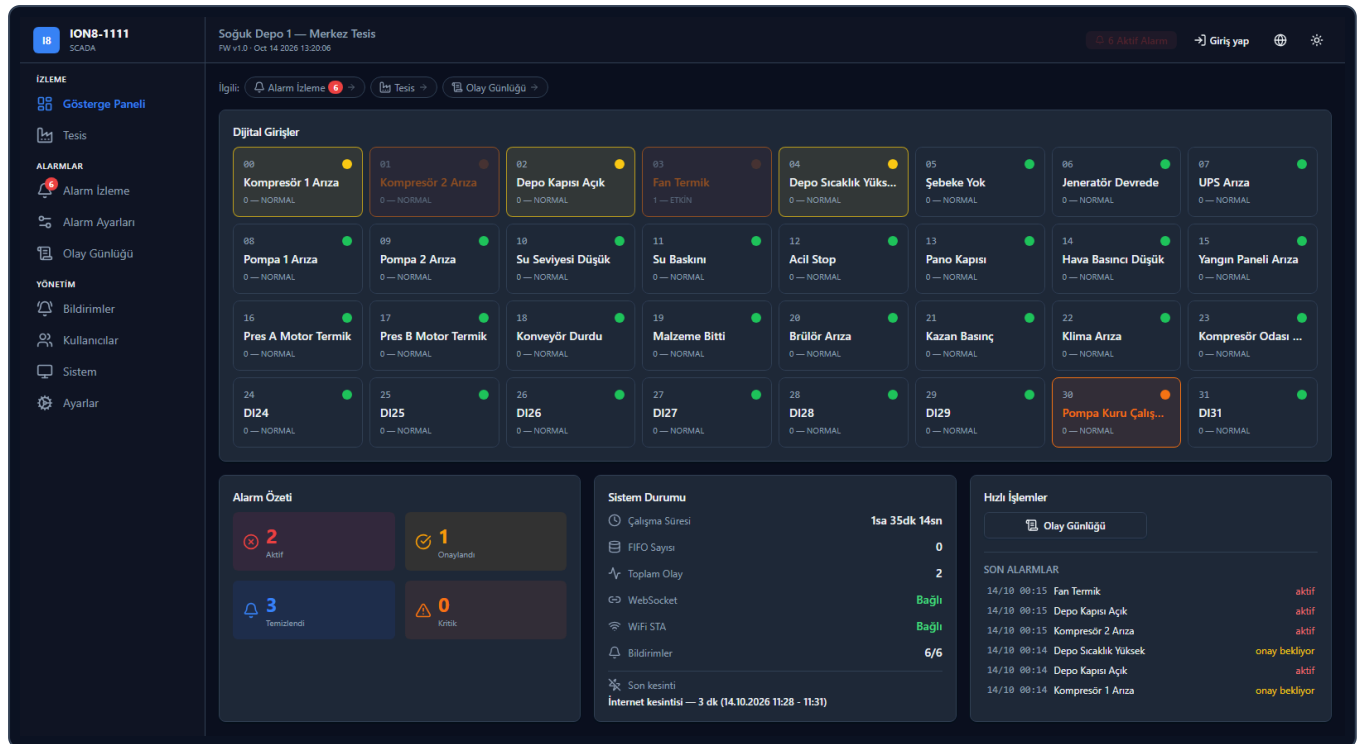
Cada persona tiene uno o varios **roles** (p. ej., Administrador, Jefe de turno, Técnico, Operador). Los permisos se asignan a los roles (**Users** → **Roles**). Pueden definirse hasta 32 personas y 16 roles.

Permiso (en el panel)	Permite
ACK	Reconocer alarmas
Silence	Silenciar temporalmente el sonido de la alarma / las notificaciones repetidas
Config	Reglas de alarma, destinatarios, ajustes del dispositivo y de notificación
Add user	Añadir y eliminar personas, asignar roles y PIN
Service (maintenance)	Ajustes de servicio y pantallas de diagnóstico; solo para el servicio técnico autorizado

Administrador completo = Config + Add user. Algunas acciones (cambiar el rol autorizado para reconocer, el informe de cortes, el restablecimiento de fábrica) solo puede realizarlas un administrador completo. El dispositivo no permite eliminar al último administrador; defina **al menos dos** administradores.

3 Dashboard

El Dashboard (panel de control) es la página de inicio del dispositivo: el estado actual de las 32 entradas, el resumen de alarmas, el estado del sistema y las últimas alarmas en una sola pantalla.



Dashboard (ordenador): 32 tarjetas de entrada, Alarm Summary, System Status y últimas alarmas (interfaz en turco)

3.1 Entradas digitales

Cada una de las 32 entradas se muestra como una tarjeta: número de entrada (00–31), nombre y texto del estado actual (p. ej., "Bomba en marcha"). **El color de la tarjeta indica el estado de alarma**, no si la entrada está a 0 o a 1:

Aspecto	Significado	Qué hacer
Rojo, intermitente	Alarma no reconocida	Compruebe la situación, reconozca la alarma
Rojo, fijo	Alarma reconocida, pero la condición persiste	Se apaga por sí sola cuando se elimina el fallo
Amarillo / naranja	Entrada de vuelta a la normalidad, pendiente de reconocimiento	Reconozca la alarma
Punto azul	Entrada a 1, sin alarma	—
Punto verde	Entrada a 0, sin alarma	—

Regla Both Edges

En las entradas que generan alarma "en cada cambio" (p. ej., notificación de puerta abierta / cerrada), la alarma es el propio cambio: termina cuando se reconoce. La tarjeta no permanece en rojo aunque la entrada siga a 1.

3.2 Alarm Summary y Quick Actions

- Alarm Summary:** el número de alarmas activas, reconocidas, de vuelta a la normalidad (pendientes de reconocimiento) y críticas.

- **Quick Actions: Acknowledge all, Silence, Reset, Event Log** (los botones aparecen según sus permisos).
- **Últimas alarmas:** las últimas alarmas y su estado (activa · pendiente de reconocimiento · reconocida · cerrada). Toque una fila para abrir el Event Log.

3.3 System Status

La conexión del panel con el dispositivo, el estado del WiFi de la planta y de las notificaciones, el tiempo de funcionamiento y **Last outage** (el último corte de suministro eléctrico o de internet, su duración y su intervalo horario). Un corte de internet en curso se muestra en rojo.

4 Alarmas

4.1 Mensaje de notificación

La alarma llega por el canal configurado para usted (Telegram y/o correo electrónico). Ejemplo (traducido a modo de ilustración):

[CRÍTICO] Línea de prensa 2 - Taller de soldadura
 Canal: Fallo bomba (DI30)
 Estado: Bomba parada
 Hora: 04.10.2026 14:32:07
 N.º de evento: 7629

El encabezado muestra el **nivel de gravedad**, seguido del nombre y la ubicación del dispositivo; debajo figuran la entrada, qué ha ocurrido, cuándo ha ocurrido y el número de evento. Las alarmas que llegan con pocos segundos de diferencia se agrupan en un solo mensaje ("3 alarmas ..."), para que su teléfono no se vea inundado de notificaciones.

4.2 Niveles de gravedad

A la alarma de cada entrada se le asigna uno de cuatro niveles de gravedad. La gravedad aparece en el encabezado de la notificación y en el panel; los ajustes de "gravedad mínima" y de horario laboral de las personas y el límite de repetición por minuto funcionan en función de ella.

Gravedad	En el encabezado de la notificación (panel en turco)	Límite de repetición (predeterminado, por minuto)
Info	[BILGI]	3
Warning	[UYARI]	3
Alarm	[ALARM]	3
Critical	[KRITIK]	Sin límite

Límite de repetición: si la misma entrada genera muchas alarmas en un minuto, las que exceden el límite no se envían (quedan en el registro). El administrador establece el límite por nivel de gravedad en **Notifications** → **General**; 0 = sin límite.

4.3 Ciclo de vida de una alarma

- 1 **Se produce la alarma:** se envía una notificación a las personas correspondientes y la tarjeta parpadea en rojo en el panel.
- 2 **Usted la reconoce:** así indica que se está ocupando del fallo. Se registran el nombre de la persona que reconoce y el tiempo de respuesta; las demás personas que recibieron la alarma reciben una notificación "acknowledged — Acknowledged by: su nombre" y se detiene el reenvío a niveles superiores (escalado).

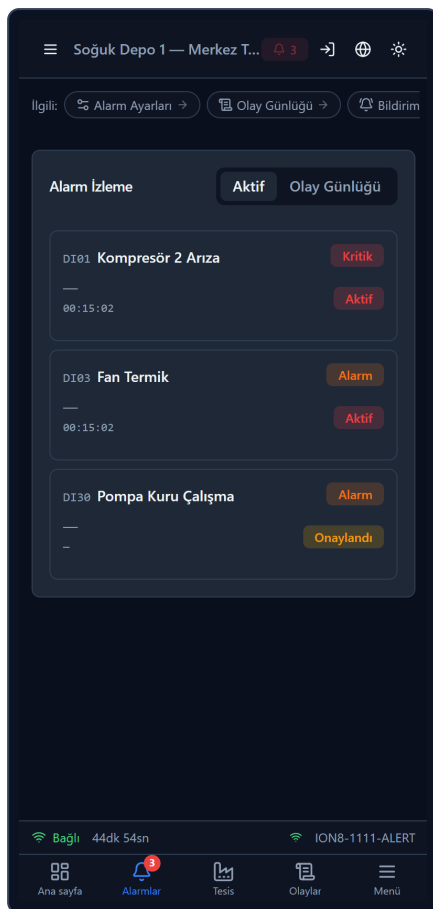
- 3 **La condición termina:** cuando la entrada vuelve a la normalidad, la alarma se cierra. Si está activado para la entrada, se envía una notificación **"back to normal — lasted X min"**.

Si la condición termina antes del reconocimiento, la alarma pasa a **"back to normal — awaiting acknowledgement"** y se cierra cuando se reconoce.

Alarmas no reconocidas

Una alarma no reconocida se notifica a **niveles superiores** (jefe de turno, responsable de mantenimiento) tras los tiempos establecidos por su administrador. Aunque la señal vuelva a la normalidad, una alarma no reconocida sigue escalando.

4.4 Página Alarm Monitoring



La pestaña **Active** muestra las alarmas pendientes de reconocimiento y las alarmas en curso (una tarjeta por entrada en el teléfono):

Campo	Significado
Channel / Name	Número de entrada (DI00–DI31) y nombre
Time	Hora en que se produjo la alarma
Message	Texto del cambio que inició la alarma
Severity	Info · Warning · Alarm · Critical
State	Active · Acknowledged · Back to normal — awaiting acknowledgement
Acknowledge	Botones de reconocimiento y silenciamiento

Botones en la parte superior de la página: **Acknowledge all · Silence · Reset · Test**. La pestaña **Event Log** muestra el historial en la misma página.

Alarm Monitoring (teléfono, interfaz en turco): una tarjeta por alarma

- **Cada alarma no reconocida ocupa una fila propia.** Por ejemplo, si una puerta se abrió y se cerró dos veces antes de reconocerse, cada cambio aparece en su propia fila, con su hora y su texto.
- El reconocimiento es **por entrada**: el botón **Acknowledge** de una entrada cierra a la vez todas las filas de esa entrada (junto al botón aparece una nota como "acknowledges 2 alarms together").
- **Test** (para personas autorizadas) genera una alarma de prueba para comprobar que el sistema funciona.

4.5 Reconocer, silenciar y restablecer

- **Reconocer:** el botón **Acknowledge** de la fila de la alarma (de su tarjeta en el teléfono) en la página Alarm Monitoring, o **Acknowledge all**. Si hay varios dispositivos en la misma instalación, también puede reconocer la alarma de otro dispositivo desde la página **Plant**.

- **Si no se muestra el botón Acknowledge:** no ha iniciado sesión, su rol no tiene el permiso de reconocimiento o solo un rol determinado puede reconocer la alarma de esa entrada. **Acknowledge all** solo reconoce las alarmas para las que usted tiene permiso e indica cuántas se han omitido.
- **Silence:** detiene temporalmente las notificaciones repetidas (requiere el permiso Silence). No cierra la alarma.
- **Reset:** las alarmas **enclavadas** (latched) persisten, aunque la señal se recupere, hasta que una persona autorizada las reconoce y pulsa **Reset**.

Los reconocimientos, silenciamientos y restablecimientos se anotan en el registro de eventos junto con quién los realizó.

4.6 Escalado (notificación escalonada)

Una alarma no reconocida se reenvía al nivel siguiente tras los tiempos establecidos. Cadena de ejemplo:

Paso	Cuándo	A quién (ejemplo)
Primera notificación	Cuando se produce la alarma	Operador
Nivel 1	Si no se reconoce, 10 min después	Jefe de turno
Nivel 2	Si no se reconoce, otros 10 min después	Responsable de mantenimiento
Nivel 3	Si no se reconoce, otros 10 min después	Director general

Los tiempos y las personas son ejemplos; el administrador configura la cadena según su organización (Sección 6.4).

- La cadena se detiene cuando la alarma se **reconoce**. En una entrada con reconocimiento automático, también se detiene cuando la señal vuelve a la normalidad.
- Con el reconocimiento automático desactivado, una alarma **no reconocida** sigue escalando aunque la señal vuelva a la normalidad.
- Se ejecuta una sola cadena por entrada: los cambios nuevos mientras el reconocimiento está pendiente no reinician la cadena.
- Sin internet, un paso de escalado no se pierde; se envía cuando se restablece la conexión.
- Las notificaciones "acknowledged" y "back to normal" se envían a **todos los niveles alcanzados** (no a la persona que reconoció la alarma).

5 Personas y canales de notificación

5.1 My account

Settings → **My account** (tras iniciar sesión). Cada persona solo puede cambiar sus propios datos:

- Nombre completo
- **Where notifications should reach me** (dónde quiero recibir las notificaciones): Telegram · E-mail · Panel
- ID de Telegram y dirección de correo electrónico
- **Send me alarms of at least this severity** (enviarme alarmas de al menos esta gravedad; p. ej., solo Alarm y Critical)
- **Working hours** (horario laboral)
- **Change PIN** (se requiere su PIN actual)

Solo el administrador puede cambiar su rol y los datos de las demás personas.

5.2 Recibir notificaciones por Telegram

Cada persona lo hace una sola vez, en su propio teléfono:

- 1 En Telegram, abra el **bot de notificación del dispositivo** (el enlace se muestra en la página My account y en el asistente de configuración) y pulse **Start**. Si no lo hace, el bot no podrá enviarle mensajes.
- 2 Abra @userinfobot y pulse **Start**; copie el número **Id** de la respuesta.
- 3 Pegue el número en el campo **Telegram ID** de My account y guarde.

La cuenta de notificación viene preparada con el dispositivo; Telegram no tiene coste ni suscripción. Las notificaciones por correo electrónico pueden llegar la primera vez a la carpeta de correo no deseado; añada la dirección del remitente a su lista de remitentes seguros.

5.3 Horario laboral y gravedad mínima

Se aplican a cada persona por separado:

- **Gravedad mínima:** las alarmas por debajo del nivel de gravedad seleccionado no se envían a esa persona (p. ej., el responsable de mantenimiento solo recibe Critical).
- **Horario laboral:** fuera del horario laboral, solo se envían las alarmas por encima del nivel de gravedad seleccionado. Por la noche solo le despertarán las alarmas importantes.

Estos ajustes filtran las notificaciones; las alarmas se siguen mostrando en el panel y en el registro de eventos.

5.4 Añadir personas (administrador)

Users → **People** → **Add person**: nombre completo, rol(es), PIN (si la persona va a iniciar sesión en el panel), canales de notificación (Telegram / E-mail / Panel), ID de Telegram, correo electrónico, gravedad mínima y horario laboral.

- Una persona recién añadida con ID de Telegram o dirección de correo electrónico que todavía no sea destinataria de ninguna entrada se añade automáticamente a los destinatarios de alarma de todas las entradas. Una persona que se elimine posteriormente de los destinatarios no vuelve a modificarse.
- Después de añadir una persona, envíe un mensaje de prueba desde **Notifications** → **Log** y compruebe que llega.

5.5 Comportamiento de las notificaciones

- **Envío agrupado:** las alarmas que llegan con pocos segundos de diferencia se agrupan en un solo mensaje.
- **Reintento:** una notificación que no pudo entregarse a una persona por un canal se reintenta solo para esa persona y ese canal (0–5 veces, Notifications → General).
- **Límite de repetición:** Sección 4.2.
- **Notificaciones del sistema:** dispositivo reiniciado (con la duración del corte de suministro), problema de conexión interna, problema de la tarjeta de almacenamiento, resumen de cortes de internet e informe de cortes. Se envían a los roles de alarma del sistema o, si no hay ninguno definido, a los roles con el permiso Config.

5.6 Registro de notificaciones

Notifications → **Log**: cada notificación enviada (alarma, escalado, reconocida, vuelta a la normalidad, sistema, prueba), a quién y por qué canal se envió, y el resultado. Para una notificación que no pudo enviarse, se muestra el **motivo** (el error devuelto por Telegram o por el servidor de correo electrónico, "sin internet" y similares). Toque una fila para ver el texto completo del mensaje.

6 Ajustes de entradas y alarmas (administrador)

6.1 Reglas

La página **Alarm Settings** → **Rules** tiene una fila por entrada (una tarjeta por entrada en el teléfono).

Ajuste	Descripción
Channel name	Nombre que se muestra en las notificaciones y en el panel (p. ej., "Bomba 1 Térmico")
Trigger	Disabled (no se supervisa) · Rising Edge (0→1 alarma, 1→0 vuelta a la normalidad) · Falling Edge (1→0 alarma, 0→1 vuelta a la normalidad) · Both Edges (cada cambio es una alarma y una notificación independientes)
Debounce (ms)	Filtrado de señal: un cambio no se tiene en cuenta hasta que la entrada ha permanecido estable durante este tiempo (0–10 000 ms). Filtra los rebotes de contacto y las interferencias breves
Severity	Info · Warning · Alarm · Critical
Texts	Textos de estado (para 0 y 1; se muestran debajo de la entrada en el panel) y mensajes de flanco (la línea "Estado:" de la notificación, p. ej., "Puerta abierta" / "Puerta cerrada")

6.2 Opciones de alarma

Opción	Descripción
Latched	La alarma persiste, aunque la señal vuelva a la normalidad, hasta que una persona autorizada la reconoce y la restablece
Auto-acknowledge	La alarma se cierra por sí sola cuando la señal vuelve a la normalidad; no se espera reconocimiento
Inverted Logic	Para contactos NC: la pérdida de la señal (incluida la rotura de un cable) es una alarma; su retorno es la normalidad
Log only	El evento se registra y se muestra en el panel; no se envía ninguna notificación
Back to normal	Se envía una notificación cuando la señal vuelve a la normalidad. "at least ... s": no se envía si la alarma duró menos de este tiempo (para entradas que se activan y desactivan con frecuencia)
Acknowledged notification	Cuando se reconoce la alarma, las demás personas que la recibieron reciben una notificación "acknowledged — by: ..."

Both Edges

Con esta regla, la alarma es el propio cambio: se cierra cuando se reconoce y no persiste aunque la entrada siga a 1. Cada cambio nuevo es una notificación independiente aunque el anterior no se haya reconocido; un solo reconocimiento los cierra todos.

6.3 Destinatarios y permiso de reconocimiento

En la tabla **Alarm Settings** → **Targets** se elige a **qué roles y personas** se envía la alarma de cada entrada.

La última columna de la tabla es el **rol autorizado para reconocer** (ACK role): solo las personas del rol seleccionado y los administradores completos pueden reconocer la alarma de esa entrada; por ejemplo, solo el equipo de mantenimiento puede reconocer la alarma de la caldera. "Everyone" = todas las personas con el permiso ACK. Solo un administrador completo puede cambiar el rol autorizado para reconocer.

6.4 Ajustes de escalado

El botón **Escalation** de la fila de la entrada en la página Targets:

- 1 Active el interruptor **Use escalation**. La **primera notificación** se envía cuando se produce la alarma (se rellena con los destinatarios de la entrada).

- 2 **Nivel 1:** establezca el tiempo "if not acknowledged, ... min after the previous step" (si no se reconoce, ... min después del paso anterior) y seleccione las personas (p. ej., Jefe de turno).
- 3 Con **Add level** puede añadir hasta dos niveles más: como máximo 4 pasos, incluida la primera notificación; como máximo 4 roles + 4 personas por paso.
- 4 Pulse **Save**. Para asignar la misma cadena a todas las entradas, utilice **Apply to all inputs** (se pulsa dos veces para confirmar).

6.5 Guardar y restablecer

- Los cambios en Alarm Settings se escriben en el dispositivo y pasan a ser permanentes al pulsar **Save**; no se pierden en un corte de suministro. Las filas modificadas se resaltan en amarillo y el botón indica cuántos canales han cambiado. **Undo** descarta los cambios no guardados.
- Reset alarm settings** restablece las reglas, los nombres y los textos de las 32 entradas; se conservan los usuarios, los ajustes de notificación y los destinatarios. Después del restablecimiento, **ninguna entrada genera alarmas**.

7 Registro de eventos

Todos los cambios de las entradas, las alarmas, los reconocimientos, los inicios de sesión en el panel y los cambios de ajustes se registran **con fecha y hora** y con quién los realizó. Los cortes de suministro eléctrico y de internet y los reinicios del dispositivo también se incluyen en el registro (página **Event Log**).

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

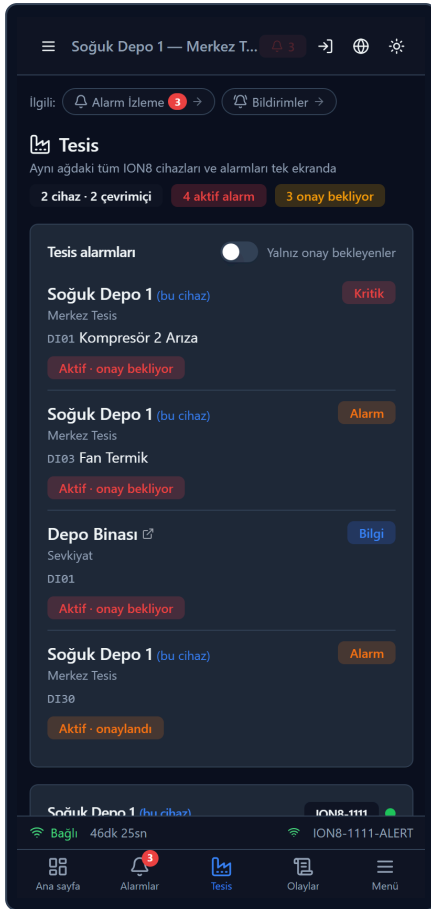
Event Log: quién reconoció, cuándo y al cabo de cuántos minutos (interfaz en turco)

- Filtrado:** utilice los botones **All** · **Last 1 hour** · **Last 24 hours** · **Last 7 days** de la parte superior y **Filter** para seleccionar un intervalo de fechas y consultar el pasado. Para el historial de un canal, toque el nombre del canal y seleccione **Full history**.
- Columnas:** hora, canal, flanco (↑ ascendente · ↓ descendente, reconocimiento, ajuste), mensaje, gravedad y número de evento.
- Las filas de alarma** muestran quién la reconoció, el tiempo de respuesta y cuánto duró la alarma ("▲ Awaiting acknowledgement" · "✓ Back to normal · lasted 12 min").
- En un teléfono, cada evento aparece en su propia tarjeta: nombre de la entrada, gravedad, sentido, hora y descripción.

La respuesta a "¿qué ha pasado durante la noche?" en el cambio de turno está aquí. Los registros pueden utilizarse como evidencia en análisis de fallos y auditorías.

8 Vista de planta

Si hay más de un dispositivo Alert SCADA en la misma red de planta (p. ej., un AS1111 en otra línea o un AS1122 con salidas), la página **Plant** los muestra todos en una sola pantalla.



Página Plant (teléfono, interfaz en turco)

Sección	Contenido
Fila superior	Cuántos dispositivos son visibles y cuántos están en línea; total de alarmas activas y no reconocidas en la planta
Plant alarms	Las alarmas de todos los dispositivos en una sola lista: dispositivo, entrada, gravedad, estado. El interruptor Awaiting acknowledgement only filtra la lista
Tarjetas de dispositivo	Nombre, ubicación, modelo, si está en línea y entradas de cada dispositivo (rojo/naranja = alarma, verde = activa). Open device page cambia al panel propio de ese dispositivo

Reconocer la alarma de otro dispositivo: el botón **Acknowledge** de la lista (necesita el permiso de reconocimiento). El reconocimiento se transmite a ese dispositivo y se registra a su nombre. Si la fila indica "remote acknowledgement off", el administrador de ese dispositivo ha desactivado el reconocimiento desde otros dispositivos: reconózcala en el panel propio de ese dispositivo. Si indica "device not visible", en este momento no es posible acceder al dispositivo.

- Si no se recibe nada de un dispositivo durante 6 segundos, se muestra "no connection". Si un dispositivo visto anteriormente deja de verse por completo durante 2 minutos, la página Plant muestra las posibles causas (dispositivo apagado, red distinta, aislamiento de clientes, contraseña de planta distinta).
- Para que los dispositivos se vean entre sí, todos deben estar en **la misma red WiFi de la planta** y tener introducida **la misma contraseña de planta** (administrador: **Plant** → **Plant settings**). No se necesita internet.
- Al tocar el nombre de otro dispositivo se abre el panel de ese dispositivo en una pestaña nueva; estos enlaces funcionan mientras el teléfono está en el WiFi de la planta.
- La página Plant no sustituye al panel propio de cada dispositivo: los ajustes y las reglas se cambian en el panel propio de cada dispositivo. Para accionar las salidas de un AS1122 con alarmas del AS1111, la regla se configura en el panel del AS1122.

9 Cortes y página System

9.1 Comportamiento ante cortes

Situación	Qué hace el dispositivo	Qué ve usted
Sin internet	Sigue supervisando y registrando las entradas; retiene las notificaciones	Cuando vuelve internet, el dispositivo verifica la conexión (hasta 90 s); las notificaciones retenidas llegan con una nota "... min delayed (no connection)", seguidas de un resumen del corte. Las notificaciones con más de 30 minutos de antigüedad no se envían y permanecen en el registro de eventos. No se envía ningún mensaje por interrupciones de menos de 1 minuto sin ninguna alarma entretanto
Corte de suministro eléctrico	No funciona y no puede supervisar las entradas. Los ajustes y los registros se conservan	Cuando vuelve la alimentación, una notificación "Device restarted: power outage ...". Las entradas que pasaron al estado de alarma durante el corte generan una alarma en el arranque
Falta el informe	—	Si el informe de cortes está activado, a la hora prevista llega un mensaje "system running" o un informe de cortes. Si no llega, compruebe la alimentación y la conexión a internet del dispositivo

El AS1111 dispone de un **reloj con batería de respaldo**: las horas de inicio y fin de un corte de suministro se registran correctamente incluso sin internet. Se recomienda una alimentación respaldada por SAI para una supervisión ininterrumpida.

9.2 Mensajes de corte

Ejemplos (traducidos a modo de ilustración):

Tras un corte de suministro eléctrico

Dispositivo reiniciado: corte de suministro ~10 min 45 s (21:00 - 21:11).
Las entradas no se supervisaron durante este tiempo.

Resumen de corte de internet

[SISTEMA] Línea de prensa 2 - Taller de soldadura
La conexión a internet estuvo caída 7 min (23:22 - 23:29). Se retuvieron 2 notificaciones durante el corte y se enviaron al restablecerse la conexión.

Informe de cortes

[INFORME DE CORTES] Línea de prensa 2 - Taller de soldadura
Informe de cortes (04.10 21:00 - 04.10 22:00)
1 corte:
- Internet: 1 h 26 min (04.10 20:59 - 22:26)
Total: sin corte de suministro, internet 1 h 26 min.

9.3 Informe de cortes

Notifications → **Outage report** (administrador completo): frecuencia del informe (cada hora ... cada semana), hora / día y destinatarios. Se informa de todos los cortes del periodo seleccionado; si no hubo ninguno, se envía un mensaje **"system running"** (sistema en funcionamiento). Este mensaje confirma con regularidad que el dispositivo funciona y puede comunicarse con usted: el silencio también es una señal. Valor predeterminado: desactivado.

9.4 Página System

La página **System** muestra la información de estado del dispositivo: memoria, WiFi, tarjeta de almacenamiento y estado de la conexión interna, y el **Boot history** (historial de arranques: el motivo de los últimos 16 arranques: corte de suministro / reinicio programado / error de software; tiempo de funcionamiento anterior). El historial de arranques no se borra con un restablecimiento de fábrica.

- **Restart device:** los ajustes se conservan; el panel queda desconectado durante aproximadamente 1 minuto.
- Cuando se ponga en contacto con el servicio técnico, adjunte una captura de pantalla de esta página.

10 Copia de seguridad de los ajustes (administrador)

Settings → Settings backup:

- **Download backup:** los roles, las personas, los destinatarios de alarma y el escalado, los nombres y textos de las entradas, los ajustes de notificación, el informe de cortes, el nombre del dispositivo y el ajuste de planta se guardan en un único archivo (.json). Opcional: los datos de contacto de las personas y el WiFi de la planta. **Los PIN nunca se incluyen en la copia de seguridad.**
- **Restore:** seleccione el archivo, marque las secciones una por una, **Restore selected**. Si el WiFi de la planta ya es el mismo, no se modifica. La copia de seguridad puede restaurarse en el mismo dispositivo o en uno nuevo; a las personas nuevas asígneles su PIN desde la página Users.

Archivo de copia de seguridad

El archivo de copia de seguridad puede contener la contraseña del WiFi y los datos de contacto de las personas. Guárdelo de forma segura. Haga una copia de seguridad antes de cambios importantes.

11 Integración: ERP y software de mantenimiento (administrador, TI)

Los eventos de Alert SCADA pueden transferirse de dos maneras a sistemas como ERP, CRM, software de mantenimiento / órdenes de trabajo o SCADA. Esta sección es un resumen; para conocer todos los campos y ejemplos, su equipo de TI puede solicitar la **Guía de integración** a support@ionia-automation.com.

Necesidad	Método	Dirección
Abrir una orden de trabajo / un registro cuando se produce una alarma; actualizarlo al reconocerla o al resolverse	Webhook	Dispositivo → su servidor (HTTP POST, JSON), en el momento del evento
Estado actual, eventos pasados y cortes en una pantalla o en un informe	Endpoints de lectura (REST)	Su software → dispositivo (HTTP GET, JSON)

La escritura de ajustes, el reconocimiento de alarmas o la adición de personas desde el exterior no forman parte de la integración; estas acciones solo se realizan en una sesión del panel protegida por PIN.

11.1 Webhook

Un webhook se configura en el dispositivo como si fuera una **persona**: allí donde se envían las alarmas, se envían también a la dirección del webhook con las mismas reglas.

- 1 **Users → People → Add person.** Nombre: p. ej., ERP. No le asigne PIN.
- 2 Entre los canales de notificación, marque solo **Webhook** e introduzca la dirección de su servidor en el campo **URL** (como máximo 127 caracteres).

- 3 Añada esta persona (o su rol) a los destinatarios de las entradas que se van a supervisar y, si es necesario, también a los niveles de escalado. Para enviarlo todo, deje la gravedad mínima en **Info** y el horario laboral vacío.
- 4 En la tarjeta **Settings** → **Integration (webhook)**, introduzca la dirección y pruébela con **Send**; en pantalla debe aparecer "Webhook OK 200".
- 5 Recomendado: en la misma tarjeta, active la firma con **Generate key**. La clave solo se muestra una vez; introdúzcala en su sistema receptor.

Propiedad	Valor
Petición	POST , Content-Type: application/json , UTF-8, un único objeto JSON
Dirección	http:// o https:// ; con HTTPS, el certificado del servidor se verifica con certificados raíz públicos (no se aceptan certificados autofirmados)
Tiempo de espera / éxito	10 segundos / el servidor debe devolver 2xx
En caso de fallo	La misma notificación se reintenta (0–5 veces); se retiene mientras no hay red y las que tienen más de 30 minutos no se envían
Tipo de evento (type)	alarm · escalation · ack · normal · system · test
Campos principales	device , location , channel (0–31), channel_name , state , severity (INFO ... CRITICAL), event_id , time , subject , text
Firma	HMAC-SHA256 opcional; la marca de tiempo y la firma se envían en cabeceras HTTP

Filtre los duplicados

Debido a los reintentos, el mismo evento puede llegar dos veces. En el lado receptor, filtre los duplicados mediante la combinación `channel + event_id + type` . Para recibir también las notificaciones del sistema, añada la persona del webhook a uno de los roles de alarma del sistema.

11.2 Endpoints de lectura (REST)

Dirección: `http://<device-address>/api/...` ; método `GET` , respuesta JSON. Asigne al dispositivo una dirección IP fija. Consulte como máximo cada 2 segundos, preferiblemente cada 5–10 segundos; para eventos en tiempo real, utilice el webhook.

Endpoint	Contenido
<code>/api/status</code>	Resumen del dispositivo: modelo, nombre, ubicación, tiempo de funcionamiento, número de alarmas activas, estado de la tarjeta de almacenamiento
<code>/api/alarm</code>	Entradas que no están en estado normal y su estado (activa · reconocida · de vuelta a la normalidad, pendiente de reconocimiento)
<code>/api/events?since=<n></code>	Eventos recientes; con <code>since</code> , solo los nuevos
<code>/api/outages</code>	Los últimos 32 cortes de suministro eléctrico / de internet y los últimos 16 arranques
<code>/api/device</code>	Modelo, nombre del dispositivo, ubicación
<code>/api/alarm/rules</code>	Nombre, tipo de disparo, gravedad y textos de estado de cada entrada

Endpoint	Contenido
/api/stats	Contadores diarios y contadores de envío de notificaciones
/api/peers	Otros dispositivos de la misma red y sus resúmenes de alarmas

Si View access está activado, los endpoints distintos de /api/status y /api/stats requieren una sesión; para la integración, defina una persona y un rol independientes con permisos solo de supervisión.

11.3 Seguridad

- El panel y los endpoints de lectura funcionan mediante **HTTP** sin cifrar. Utilice el dispositivo solo en una red de planta de confianza y no lo exponga a internet; para el acceso remoto, utilice una VPN.
- El cuerpo del webhook contiene nombres de personas e información de la instalación; si el servidor receptor está fuera de su red, utilice **HTTPS** y active la firma.

12 Resumen de tareas del administrador

Tarea	Dónde
Añadir / eliminar personas, asignar roles y PIN	Users → People
Editar los permisos de los roles	Users → Roles
Nombre de la entrada, condición de alarma, gravedad, textos, opciones	Alarm Settings → Rules
Quién recibe la alarma, escalado, rol autorizado para reconocer	Alarm Settings → Targets
Informe de cortes (frecuencia, destinatarios)	Notifications → Outage report
Registro de notificaciones, mensaje de prueba	Notifications → Log
Número de reintentos, límite de repetición	Notifications → General
WiFi de la planta, WiFi del dispositivo (ocultar / desactivar / contraseña)	Notifications → WiFi
Nombre y ubicación del dispositivo	Settings → Device name and location
Descargar / restaurar la copia de seguridad de los ajustes	Settings → Settings backup
Exigir inicio de sesión para consultar el panel	Settings → View access
Prueba del webhook y clave de firma	Settings → Integration (webhook)
Contraseña de planta, reconocimiento desde otros dispositivos	Plant → Plant settings
Reiniciar el dispositivo	System → Restart device
Código de recuperación, restablecimiento completo de fábrica	Settings (solo desde el WiFi del dispositivo)
Volver al asistente de configuración	Settings

Buenas prácticas:

- Defina al menos **dos** administradores; los administradores deben utilizar PIN de 6 cifras.
- Después de añadir una persona, envíe un mensaje de prueba y compruebe que llega.
- Descargue una **copia de seguridad de los ajustes** antes de cambios importantes.
- Active el informe de cortes: el mensaje "system running" es una confirmación periódica de que el dispositivo funciona correctamente.

13 Preguntas frecuentes

Pregunta	Respuesta
No recibo notificaciones	¿Está activado el canal en My account? ¿Ha pulsado Start en el bot de Telegram? Fuera del horario laboral no se envían las alarmas de gravedad baja. Su administrador puede ver el motivo en Notifications → Log.
No recibo correos electrónicos	Revise la carpeta de correo no deseado; añada la dirección del remitente a su lista de remitentes seguros.
He olvidado mi PIN	Su administrador establece un PIN nuevo en la página Users. El PIN de un administrador se restablece con el código de recuperación (Guía de instalación).
El panel no se abre	¿Está su teléfono en la red de la planta? Pruebe con la dirección IP en lugar de la dirección <code>.local</code> .
La pantalla muestra "Disconnected"	Su teléfono u ordenador no puede comunicarse con el dispositivo: compruebe su red y vuelva a cargar la página.
No veo el botón Acknowledge	Inicie sesión. Si sigue sin aparecer, su rol no tiene permiso para reconocer esa entrada.
La misma entrada genera alarmas con demasiada frecuencia	Puede que el contacto tenga rebotes o que la señal sea inestable. Su administrador puede ajustar el tiempo de filtrado de señal (Debounce).
La alarma está reconocida, pero la tarjeta sigue en rojo	La condición persiste (rojo fijo). Se apaga cuando se elimina el fallo.
¿Se pierden las alarmas si se cae internet?	No. La supervisión y el registro continúan; las notificaciones se envían cuando se restablece la conexión (excepto las de más de 30 minutos, que permanecen en el registro de eventos).
¿Y los ajustes tras un corte de suministro?	Los ajustes y los nombres de las entradas se conservan. Cuando el dispositivo arranca, informa de la duración del corte.
¿Qué significan las luces del dispositivo?	Verde = funcionamiento normal, amarillo (LED3) = conectado al WiFi de la planta, amarillo (LED2) = la tarjeta de almacenamiento funciona, rojo = error crítico. Detalles: Guía de instalación.
El otro dispositivo no aparece en la página Plant	¿Están ambos dispositivos en la misma red WiFi, son iguales las contraseñas de planta y está desactivado el aislamiento de clientes (red de invitados) en el router?
Nadie se despertó por una alarma nocturna	Revise los ajustes de escalado con su administrador; deben estar definidos los niveles superiores y los tiempos.
¿Tiene coste Telegram?	No. La cuenta de notificación viene preparada con el dispositivo; cada persona pulsa Start en el bot una sola vez.
¿Notificaciones por WhatsApp o SMS?	No en esta versión; los canales de notificación son Telegram, correo electrónico, webhook y el panel web.

14 Glosario

Término	Significado
Reconocimiento (ACK)	Confirmar que alguien se está ocupando de la alarma. Se registran la persona y el tiempo de respuesta, y el escalado se detiene
Escalado	Reenvío de una alarma no reconocida a niveles superiores tras los tiempos establecidos

Término	Significado
Destinatario (Target)	Los roles y las personas a los que se envía la alarma de una entrada
Rol	Grupo de personas al que se asignan permisos (p. ej., Jefe de turno)
Nivel de gravedad (Severity)	El nivel de la alarma: Info · Warning · Alarm · Critical
Disparo (Trigger)	El cambio que inicia la alarma: flanco ascendente (0→1), flanco descendente (1→0), ambos flancos
Debounce (filtrado de señal)	El tiempo que una entrada debe permanecer estable para que se tenga en cuenta un cambio
Contacto NO / NC	Contacto normalmente abierto / normalmente cerrado
Inverted Logic	Para contactos NC: la pérdida de la señal (incluida la rotura de un cable) se considera alarma
Alarma enclavada (Latched)	Alarma que persiste, aunque la señal se recupere, hasta que se reconoce y se restablece
Silence	Detener temporalmente las notificaciones repetidas; no cierra la alarma
Horario laboral	Las horas en las que una persona recibe notificaciones; fuera de ellas, solo las alarmas por encima del nivel de gravedad seleccionado
Envío agrupado	Envío en un solo mensaje de las alarmas que se producen en pocos segundos
Informe de cortes	Informe periódico de los cortes de suministro eléctrico y de internet; "system running" si no hubo ninguno
Contraseña de planta	Contraseña común introducida en todos los dispositivos de la misma red para que se reconozcan entre sí
WiFi del dispositivo	La red WiFi propia del dispositivo para la configuración y el mantenimiento
WiFi de la planta	La red con acceso a internet a la que se conecta el dispositivo para enviar notificaciones
Código de recuperación	Código propio del dispositivo que se utiliza para establecer un PIN de administrador nuevo si se ha olvidado
Webhook	Envío automático de eventos a su servidor mediante HTTP POST



Contacto

Ventas e información: info@ionia-automation.com
 Soporte técnico: support@ionia-automation.com
ionia-automation.com