



**AX PRO**

User Manual

# Información legal

© 2022 Hangzhou Hikvision Digital Technology Co., Ltd. Todos los derechos reservados.

## Acerca de este manual

El Manual incluye instrucciones para el uso y manejo del Producto. Las imágenes, los gráficos, las imágenes y toda la demás información que se incluye a continuación son solo para descripción y explicación. La información contenida en el Manual está sujeta a cambios, sin previo aviso, debido a actualizaciones de firmware u otras razones. Encuentre la última versión de este Manual en el sitio web de Hikvision (<https://www.hikvision.com/>).

Utilice este Manual con la orientación y la asistencia de profesionales capacitados en el soporte del Producto.

## Marcas registradas

**HIKVISION** y otras marcas comerciales y logotipos de Hikvision son propiedad de Hikvision en varias jurisdicciones.

Otras marcas comerciales y logotipos mencionados son propiedad de sus respectivos dueños.

### Descargo de responsabilidad

EN LA MEDIDA MÁXIMA PERMITIDA POR LA LEY APLICABLE, ESTE MANUAL Y EL PRODUCTO DESCRITO, CON SU HARDWARE, SOFTWARE Y FIRMWARE, SE PROPORCIONAN "TAL CUAL" Y "CON TODOS LOS FALLOS Y ERRORES". HIKVISION NO OFRECE GARANTÍAS, EXPRESAS O IMPLÍCITAS, INCLUYENDO SIN LIMITACIÓN, COMERCIALIZACIÓN, CALIDAD SATISFACTORIA O IDONEIDAD PARA UN PROPÓSITO EN PARTICULAR. EL USO DEL PRODUCTO POR SU PARTE ES BAJO SU PROPIO RIESGO. EN NINGÚN CASO

¿HIKVISION SERÁ RESPONSABLE ANTE USTED POR CUALQUIER DAÑO ESPECIAL, CONSECUENTE, INCIDENTAL O INDIRECTO, INCLUYENDO, ENTRE OTROS, DAÑOS POR PÉRDIDA DE BENEFICIOS COMERCIALES, INTERRUPCIÓN COMERCIAL O PÉRDIDA DE DATOS, CORRUPCIÓN DE SISTEMAS O PÉRDIDA DE DOCUMENTACIÓN, YA SEA BASADO EN INCUMPLIMIENTO DE CONTRATO, AGRAVIO (INCLUIDA LA NEGLIGENCIA), RESPONSABILIDAD DEL PRODUCTO O DE CUALQUIER OTRO TIPO, EN RELACIÓN CON EL USO DEL PRODUCTO, INCLUSO SI HIKVISION HA SIDO ADVERTIDO DE LA POSIBILIDAD DE DICHOS DAÑOS O PÉRDIDAS.

USTED RECONOCE QUE LA NATURALEZA DE INTERNET PROPORCIONA RIESGOS DE SEGURIDAD INHERENTES, Y HIKVISION NO ASUMIRÁ NINGUNA RESPONSABILIDAD POR EL FUNCIONAMIENTO ANORMAL, LA FUGA DE PRIVACIDAD U OTROS DAÑOS RESULTANTES DE ATAQUE CIBERNÉTICO, ATAQUE DE HACKER, INSPECCIÓN DE VIRUS U OTROS RIESGOS DE SEGURIDAD DE INTERNET; SIN EMBARGO, HIKVISION PROPORCIONARÁ SOPORTE TÉCNICO OPORTUNO SI ES NECESARIO.

USTED ACEPTA UTILIZAR ESTE PRODUCTO DE ACUERDO CON TODAS LAS LEYES APLICABLES, Y USTED ESTÁ EL ÚNICO RESPONSABLE DE GARANTIZAR QUE SU USO SE CONFORME A LA LEGISLACIÓN APLICABLE.

ESPECIALMENTE, USTED ES RESPONSABLE, DE UTILIZAR ESTE PRODUCTO DE UNA MANERA QUE NO INFRINGA LOS DERECHOS DE TERCEROS, INCLUYENDO SIN LIMITACIÓN, DERECHOS DE PUBLICIDAD, DERECHOS DE PROPIEDAD INTELECTUAL O DE PROTECCIÓN DE DATOS Y OTROS DERECHOS DE PRIVACIDAD.

NO UTILIZARÁ ESTE PRODUCTO PARA CUALQUIER USO FINAL PROHIBIDO, INCLUYENDO EL DESARROLLO O LA PRODUCCIÓN DE ARMAS DE DESTRUCCIÓN MASIVA, EL DESARROLLO O

PRODUCCIÓN DE ARMAS QUÍMICAS O BIOLÓGICAS, CUALQUIER ACTIVIDAD EN EL CONTEXTO RELACIONADA CON UN CICLO DE COMBUSTIBLE NUCLEAR EXPLOSIVO O INSEGURO, O EN APOYO A ABUSOS DE LOS DERECHOS HUMANOS.

EN CASO DE CONFLICTO ENTRE ESTE MANUAL Y LA LEY APLICABLE, ESTA PREVALECE.

**Protección de Datos**

Durante el uso del dispositivo, se recopilarán, almacenarán y procesarán datos personales. Para proteger los datos, el desarrollo de los dispositivos Hikvision incorpora principios de privacidad por diseño. Por ejemplo, para dispositivos con funciones de reconocimiento facial, los datos biométricos se almacenan en su dispositivo con un método de encriptación; para el dispositivo de huellas dactilares, solo se guardará la plantilla de huellas dactilares, que es imposible reconstruir una imagen de huellas dactilares.

Como controlador de datos, se le recomienda recopilar, almacenar, procesar y transferir datos de acuerdo con las leyes y regulaciones de protección de datos aplicables, lo que incluye, entre otros, la realización de controles de seguridad para salvaguardar los datos personales, como la implementación de controles de seguridad físicos y administrativos razonables. realizar revisiones y evaluaciones periódicas de la eficacia de sus controles de seguridad.

## Convenciones de símbolos

Los símbolos que se pueden encontrar en este documento se definen a continuación.

Símbolo	Descripción
 <b>Peligro</b>	Indica una situación peligrosa que, si no se evita, provocará o podría provocar la muerte o lesiones graves.
 <b>Precaución</b>	Indica una situación potencialmente peligrosa que, si no se evita, podría provocar daños en el equipo, pérdida de datos, degradación del rendimiento o resultados inesperados.
 <b>Nota</b>	Proporciona información adicional para enfatizar o complementar puntos importantes del texto principal.

### **Nota**

- Actualice el firmware a la última versión.
- Para los instaladores, se recomienda instalar y mantener dispositivos a través de Hik-ProConnect.

## Información reglamentaria

EN 50131-1:2006+A1:2009+A2:2017

Grado de seguridad (SG): 2

EN 50131-3:2009

Clase ambiental (CE): II

EN 50131-6:2017

DP2

EN 50131-5-3:2017

Certificado por KIWA

EN 50131-10: 2014



EN 50136-2: 2013

 **Nota** El etiquetado de conformidad con EN50131 debe eliminarse si se utilizan configuraciones no conformes.

### Declaración de conformidad de la UE

	<p>Este producto y, si corresponde, los accesorios suministrados también están marcados con "CE" y cumplen, por lo tanto, con las normas europeas armonizadas aplicables enumeradas en la Directiva EMC. 2014/30/EU, Directiva RE 2014/53/EU, la Directiva RoHS 2011/65/UE</p>
	<p>2012/19/EU (directiva WEEE): Los productos marcados con este símbolo no pueden eliminarse como residuos municipales sin clasificar en la Unión Europea. Para un reciclaje adecuado, devuelva este producto a su proveedor local al comprar un equipo nuevo equivalente, o deséchelo en los puntos de recolección designados. Para obtener más información, consulte: <a href="http://www.recyclethis.info">www.recyclethis.info</a></p>
	<p>2006/66/EC (directiva sobre baterías): Este producto contiene una batería que no se puede desechar como residuo municipal sin clasificar en la Unión Europea. Consulte la documentación del producto para obtener información específica sobre la batería. La batería está marcada con este símbolo, que puede incluir letras para indicar cadmio (Cd), plomo (Pb) o mercurio (Hg). Para un reciclaje adecuado, devuelva la batería a su proveedor o a un punto de recogida designado. Para obtener más información, consulte: <a href="http://www.recyclethis.info">www.recyclethis.info</a></p>

	<p>Advertencia</p> <p>Este es un producto de clase A. En un entorno doméstico, este producto puede causar interferencias de radio, en cuyo caso el usuario deberá tomar las medidas adecuadas.</p>
	<p>Información de la FCC</p> <p>Tenga en cuenta que los cambios o modificaciones no aprobados expresamente por la parte responsable del cumplimiento podrían anular la autoridad del usuario para operar el equipo.</p> <p>Cumplimiento con la FCC: este equipo ha sido probado y se ha determinado que cumple con los límites para un dispositivo digital de Clase B, de conformidad con la parte 15 de las Reglas de la FCC. Estos límites están diseñados para brindar una protección razonable contra interferencias dañinas en una instalación residencial. Este equipo genera, usa y puede irradiar energía de radiofrecuencia y, si no se instala y usa de acuerdo con las instrucciones, puede causar interferencias dañinas en las comunicaciones por radio. Sin embargo, no hay garantía de que no se produzcan interferencias en una instalación en particular. Si este equipo causa interferencias dañinas en la recepción de radio o televisión, lo cual se puede determinar apagando y encendiendo el equipo, se recomienda al usuario que intente corregir la interferencia mediante una o más de las siguientes medidas:</p> <ul style="list-style-type: none"> <li>-Reorientar o reubicar la antena receptora.</li> <li>-Aumente la separación entre el equipo y el receptor.</li> <li>—Conectar el equipo a una toma de un circuito diferente al que está conectado el receptor.</li> <li>—Consulte al distribuidor oa un técnico experimentado en radio/TV para obtener ayuda.</li> </ul> <p>Este equipo debe instalarse y operarse con una distancia mínima de 20 cm entre el radiador y su cuerpo.</p> <p>Condiciones de la FCC</p> <p>Este dispositivo cumple con la parte 15 de las normas de la FCC. La operación está sujeta a las siguientes dos condiciones:</p> <ol style="list-style-type: none"> <li>1. Es posible que este dispositivo no cause interferencias dañinas.</li> <li>2. Este dispositivo debe aceptar cualquier interferencia recibida, incluida la interferencia que pueda provocar un funcionamiento no deseado.</li> </ol>

# Contenido

<b>Capítulo 1 Instrucciones de instalación .....</b>	<b>9</b>
<b>1.1 Escena típica .....</b>	<b>9</b>
1.2 Precaución.....	9
1.3 Preguntas frecuentes sobre la instalación.....	10
<b>Capítulo 2 Introducción .....</b>	<b>11</b>
Descripción <b>del sistema</b> .....	11
<b>Capítulo 3 Arranque.....</b>	<b>14</b>
<b>3.1 Gestión de Autoridades .....</b>	<b>14</b>
3.2 Activación .....	15
<b>3.2.1 Activación local .....</b>	<b>15</b>
3.2.2 Activación con LAN/SIM(4G/GPRS) .....	dieciséis
3.2.3 Activación con Wi-Fi .....	17
3.3 Desvincular el dispositivo .....	24
3.3.1 Desvincular el dispositivo de su propia cuenta.....	24
3.3.2 Desvincular el dispositivo de otra cuenta.....	24
<b>Capítulo 4 Administración de usuarios .....</b>	<b>27</b>
4.1 Gestión de usuarios.....	27
4.1.1 Invitar al administrador .....	27
4.1.2 Cancelar el acceso del instalador.....	28
4.1.3 Añadir un Operador.....	29
4.1.4 Eliminar un Operador .....	30
4.1.5 Deshabilitar el servicio Hik-Connect .....	31
4.1.6 Invitar al instalador .....	31
4.2 Entradas de acceso .....	31
<b>Capítulo 5 Configuración .....</b>	<b>33</b>
5.1 Configuración con Hik-Proconnect.....	33
5.1.1 Usar la APLICACIÓN Hik-Proconnect .....	33
5.1.2 Usar el portal Hik-ProConnect .....	55
5.2 Configuración con Hik-Connect .....	59

---

<b>5.3 Configuración con el cliente web .....</b>	<b>84</b>
5.3.1 Configuración del sistema .....	85
5.3.2 Gestión de dispositivos .....	96
5.3.3 Gestión de permisos .....	108
5.3.4 Gestión de vídeo.....	110
5.3.5 Configuración de área .....	112
5.3.6 Ajustes de comunicación.....	112
5.3.7 Mantenimiento .....	126
5.3.8 Estado de verificación .....	131
<b>5.4 Informe a CRA (Centro Receptor de Alarmas) .....</b>	<b>132</b>
Configurar ATS en el Transceptor del Centro de Recepción .....	132
Configurar ATS en el Transceptor del Panel .....	133
Prueba de señalización .....	134
<b>Capítulo 6 Operaciones generales .....</b>	<b>136</b>
6.1 Armado .....	136
6.2 Desarmar.....	137
6.3 Control SMS .....	137
<b>A. Solución de problemas .....</b>	<b>138</b>
A.1 Fallo de comunicación .....	138
A.1.1 Conflicto de IP .....	138
A.1.2 La página web no es accesible .....	138
A.1.3 Hik-Connect está fuera de línea .....	138
A.1.4 La cámara de red se cae con frecuencia.....	138
A.1.5 Error al agregar el dispositivo en la aplicación .....	138
A.1.6 La información de la alarma no se transmite a APP/4200/ Centro de alarmas.....	139
A.2 Exclusión Mutua de Funciones .....	139
A.2.1 No se puede ingresar al modo de registro .....	139
A.3 Fallo de zona .....	139
A.3.1 La zona está fuera de línea .....	139
A.3.2 Zona a prueba de manipulaciones .....	139
A.3.3 Zona Activada/Falla.....	139

---

<b>A.4 Problemas durante el armado</b> .....	140
<b>A.4.1 Falla en el Armado (Cuando el armado forzado no está habilitado)</b> .....	140
<b>A.5 Falla Operacional</b> .....	140
<b>A.5.1 No se pudo ingresar al modo de prueba</b> .....	140
<b>A.5.2 La operación de borrado de alarmas en el panel no produce el informe de borrado de alarmas</b> .....	140
<b>A.6 Fallo en la entrega del correo</b> .....	140
<b>A.6.1 Error al enviar correo de prueba</b> .....	140
<b>A.6.2 Error al enviar el correo durante el uso</b> .....	141
<b>A.6.3 Error al enviar correos a Gmail</b> .....	141
<b>A.6.4 Error al enviar correos a QQ o Foxmail</b> .....	141
<b>A.6.5 Error al enviar correos a Yahoo</b> .....	141
<b>A.6.6 Configuración de correo</b> .....	142
<b>B. Tipos de entrada</b> .....	143
<b>C. Tipos de salida</b> .....	146
<b>D. Tipos de eventos</b> .....	147
<b>E. Niveles de acceso</b> .....	148
<b>F. Señalización</b> .....	150
<b>Detección de fallas ATP/ATS</b> .....	150
<b>Categoría ATS</b> .....	150
<b>G. Código SIA y CID</b> .....	151
<b>H. Matriz de Comunicación y Comando de Operación</b> .....	164
<b>I. Tipos de zonas de detectores</b> .....	165

# Capítulo 1 Instrucciones de instalación

## 1.1 Escena típica



Ubicación de instalación típica de los dispositivos: 1. Panel de control AX PRO

2. Repetidor 3.

Detector PIR

4. Sonda

5. Detector magnético

## 1.2 Precaución

1. Evite instalar el dispositivo en superficies metálicas.

2. Evite colocar el dispositivo directamente en el suelo.

3. No se permite envolver el dispositivo en metal.

4. Evite las obstrucciones en un radio de 50 cm alrededor del dispositivo, excepto la superficie de instalación.

5. El repetidor debe instalarse entre el panel de control y el periférico.

6. Verifique la intensidad de la señal antes de la instalación y se recomienda instalar el dispositivo en la ubicación del indicador verde. (No envuelva el detector con las manos cuando compruebe la intensidad de la señal).

7. Se recomienda la instalación vertical de los dispositivos.

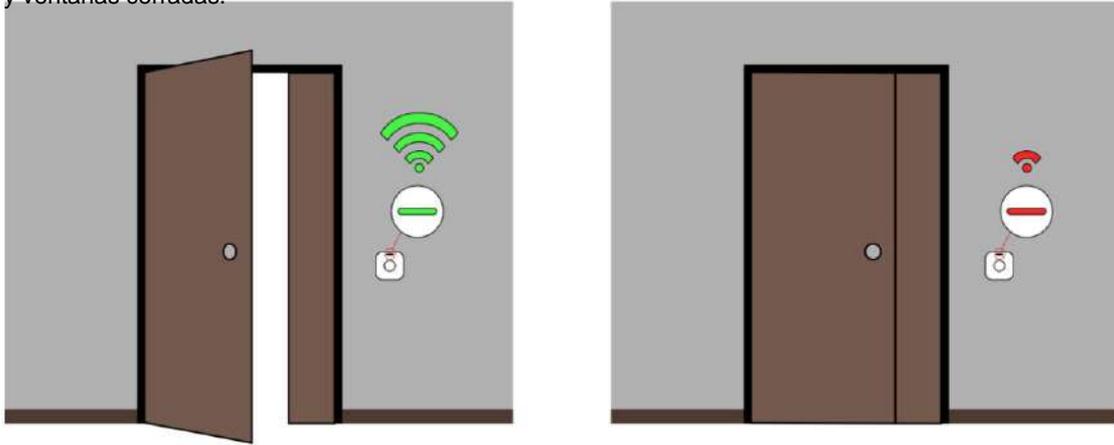
### 1.3 Preguntas frecuentes sobre la instalación

#### Pregunta 1:

¿Por qué la señal es normal durante la instalación, pero peor en el uso real?

#### Respuesta:

compruebe si el entorno de trabajo cambia durante la instalación y el uso real. Como la obstrucción causada por puertas y ventanas cerradas.



#### Pregunta 2:

Una vez completada la instalación, el periférico está fuera de línea.

#### Responder:

- Ajuste la posición del panel de control y compruebe si la intensidad de la señal es adecuada para instalación.
- Instale un repetidor entre el periférico fuera de línea y el panel de control.
- Verifique si instalar los dispositivos de acuerdo con las precauciones.

## Capítulo 2 Introducción

### Descripción del sistema

AX PRO es un sistema de alarma inalámbrico diseñado para proteger las instalaciones requeridas para una protección adecuada contra la alarma de intrusión. Admite LAN/Wi-Fi como red de transmisión principal. El sistema es aplicable a los escenarios de mercado, tienda, casa, fábrica, almacén, oficina, etc.

- Innovadora tecnología inalámbrica bidireccional Tri-X.
- Comunicación bidireccional con cifrado AES-128.
- El espectro ensanchado por salto de frecuencia (FHSS) se usa para evitar interferencias, para evitar escuchas ilegales y para permitir comunicaciones de acceso múltiple por división de código (CDMA).
- Guía de voz para alerta de alarma, indicación de estado del sistema, aviso de operación, etc.
- Configuración a través de cliente web, cliente móvil y Convergence Cloud.
- Empuja la notificación de alarma a través de mensajes o llamadas telefónicas.
- Ve videos de vida de Hik-Connect y clips de video de alarma a través de correos electrónicos, Hik-ProConnect y Hik Conectar.
- Sube informes de alarmas a CRA.
- Protocolo SIA-DC09 y admite formato de datos Contact ID y SIA.
- Batería de respaldo de litio de 4520 mAh con 12 H de duración en espera.

---

 **Nota**

ISUP5.0: un protocolo de Internet de privacidad que se utiliza para acceder a la plataforma de terceros, que admite la carga de informes de alarma, la gestión de AXE PRO y la carga de videos cortos.

La priorización del mensaje y las indicaciones son las mismas. El AXPRO carga mensajes y da indicaciones sincrónicamente.

---

---

 **Nota**

Protocolo estándar DC-09:

ADM-CID: el método de presentación de datos de DC-09 es CID, que no está encriptado y solo para cargar informes de alarma.

\*ADC-CID: el método de presentación de datos de DC-09 es CID, que está encriptado y solo para cargar informes de alarma.

SIA-DCS: el método de presentación de datos de DC-09 es DCS (también llamado protocolo SIA), que no está encriptado y solo para cargar informes de alarma.

\*SIA-DCS: el método de presentación de datos de DC-09 es DCS (también llamado protocolo SIA), que está encriptado y solo para cargar informes de alarma.

---

### Instrucción RSSI para periféricos

Con respecto a EN 50131-5-3 4.2.2 Requisito de inmunidad a la atenuación.

Intensidad de señal	RSSI Valor	Indicación	Observación
Fuerte	>120	Verde Listo	para instalar
Medio	81 a 120	Amarillo OK	para instalar
Débil	60 a 80	Rojo	No se recomienda instalar, pero puede funcionar
Inválido	0 a 59	Rojo (parpadeo) No	se puede instalar correctamente, no puede funcionar con normalidad

 **Nota**

Instale periféricos solo si la intensidad de la señal es superior a 80. Para obtener un sistema mucho mejor, instálo a 120 o más.

### Opciones de notificación de AX PRO

El AX PRO es adecuado para los siguientes requisitos de notificación junto con las sirenas requeridas

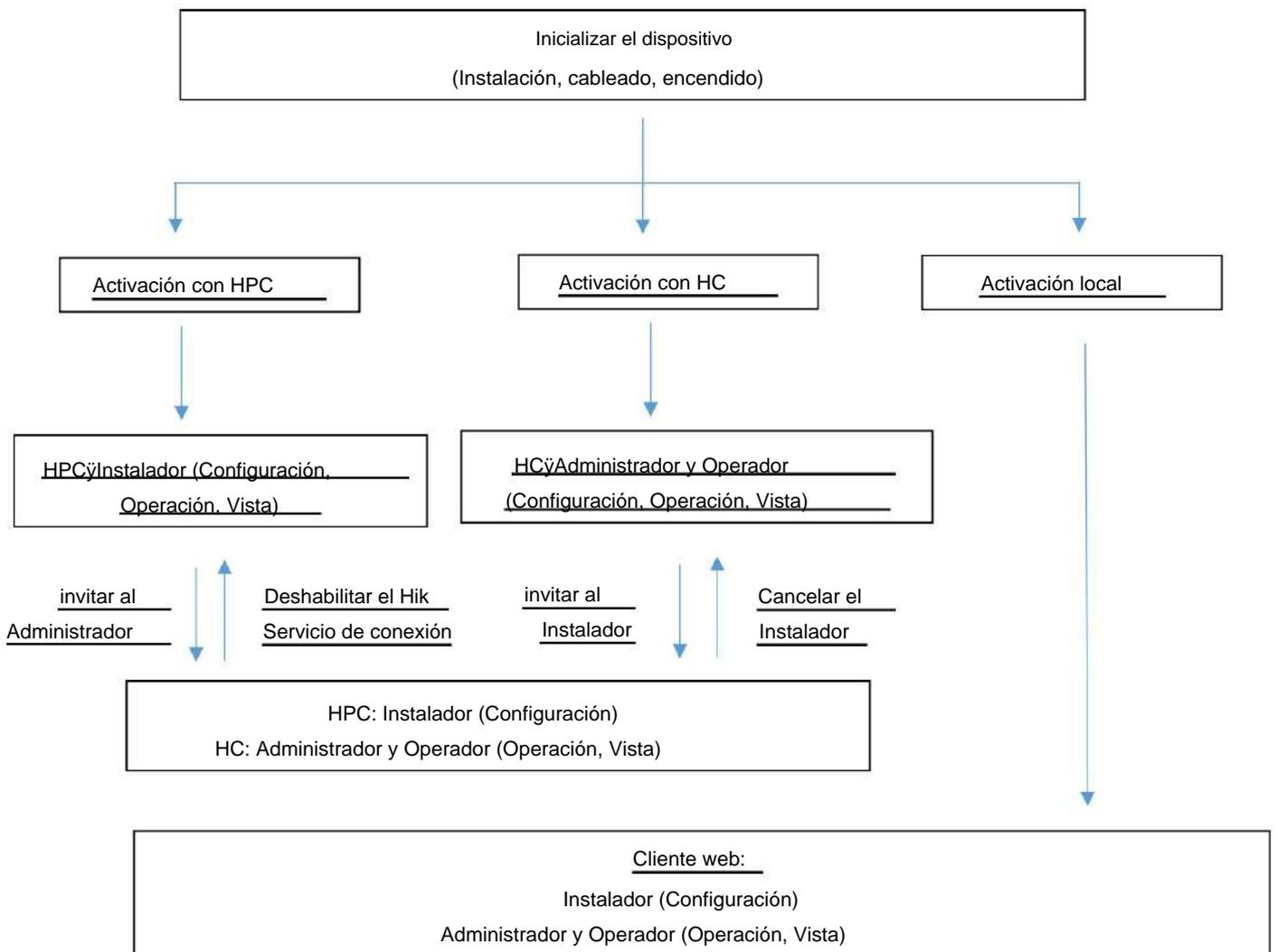
Notificación equipo	YO Y HAS Grado 2		
	Opciones		
	C	mi	F
autoalimentado WD audible	2	1	Opcional
ATS	DP1	Opcional	DP2

## Capítulo 3 Puesta en marcha

### 3.1 Gestión de autoridad

Puede usar un navegador web, HPC (Hik-ProConnect, APP) o HC (Hik-Connect, APP) para activar el dispositivo. Después de la activación, puede administrar el dispositivo transfiriendo permisos entre aplicaciones.

También puede usar la cuenta y la contraseña de todas las cuentas para iniciar sesión en el cliente WEB para configurar el dispositivo.



Para obtener más información, consulte el **Capítulo 4 Gestión de usuarios**.

## 3.2 Activación

Mientras inicia el dispositivo con Hik-ProConnect o Hik-Connect, el AX PRO siempre debe agregarse primero a una cuenta de instalador. La cuenta del instalador invitará y transferirá la propiedad a la cuenta del administrador más tarde después de finalizar toda la configuración y prueba iniciales. Siga los pasos a continuación para inicializar el sistema de alarma inalámbrico.

Puede activar el dispositivo por Wi-Fi, LAN o SIM (4G/GPRS).

También puede activar el dispositivo a través de SADP o navegador web.

### 3.2.1 Activación local Busque la

dirección IP del dispositivo a través del software SADP y active el dispositivo a través de SADP o navegador web.

#### Antes de que empieces

Obtenga el software SADP del sitio web oficial (<http://www.hikvision.com/>) e instálelo de acuerdo con las indicaciones.

El dispositivo y la computadora que ejecuta la herramienta SADP deben pertenecer al mismo segmento de red.

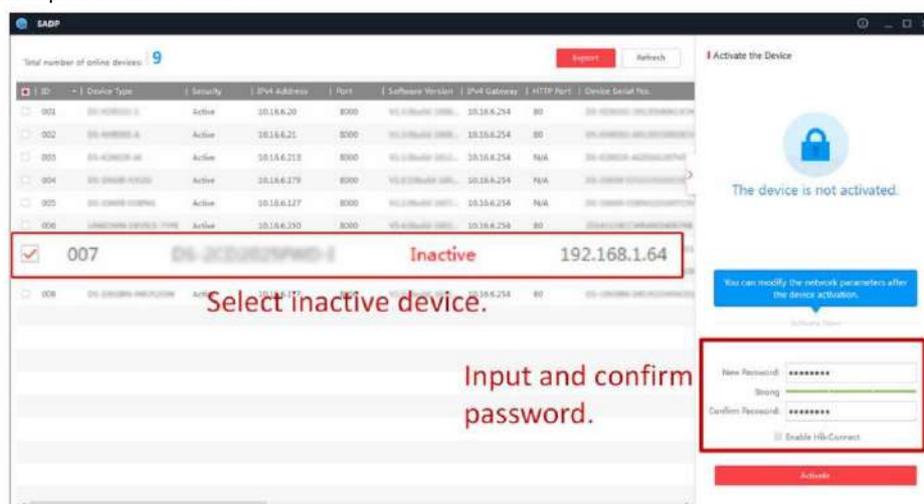
#### Pasos

1. Asegúrese de que el dispositivo y la computadora estén en el mismo segmento de red.
2. Abra el software SADP y busque dispositivos en línea.
3. Busque la dirección IP del dispositivo en SADP.

#### Active el dispositivo a través de SADP 4.

Seleccione su dispositivo en la lista de dispositivos en línea.

5. Ingrese la nueva contraseña (contraseña de administrador) y confirme la contraseña.
6. Haga clic en **Activar** para iniciar la activación.



7. El estado del dispositivo pasa a ser **Activo** después de una activación exitosa.

#### Activar el dispositivo a través del cliente web

4. Introduzca la dirección IP en la barra de direcciones del navegador.

5. El sistema abrirá automáticamente la ventana de activación. Siga las indicaciones para crear una contraseña de activación para la cuenta de administrador.

6. Utilice la contraseña para iniciar sesión.

---

 **Nota**

- Después de la activación, si el administrador no habilita el instalador, el administrador posee todos los permisos de configuración en el cliente web; si el instalador local o el instalador en la nube (en la aplicación) está habilitado e inicia sesión en el cliente web, el administrador local pierde los permisos de configuración y los permisos de configuración se transfieren al instalador local/instalador en la nube.
  - Cuando existe el instalador en la nube, el administrador de la nube no tiene permiso de configuración.
  - Si el panel de control no recibe la cuenta emitida por la nube, puede usar las cuentas de administrador e instalador local como de costumbre. Si el panel de control recibe la cuenta HC/HPC de la nube, sobrescribirá directamente la cuenta del administrador/instalador local, y la nube correspondiente heredará y sincronizará los datos generados por el administrador/instalador local.  
cuenta.
- 

### 3.2.2 Activación con LAN/SIM(4G/GPRS)

#### Paso 1 Crear un sitio (Solo para HPC)

Descargue Hik-ProConnect e inicie sesión con la cuenta del instalador.

Un sitio es el lugar donde se desplegó el sistema de alarma. Cree un sitio donde se pueda agregar el dispositivo con su nombre y dirección del sitio. El propietario del sitio sería un usuario final, generalmente considerado como administrador.

#### Paso 2 Conéctese a la red.

Conecte el dispositivo a Ethernet con LAN o SIM y encienda el dispositivo.

---

 **Nota**

- Mientras el dispositivo está encendido, el LED de encendido se vuelve verde.
  - Una vez que el dispositivo se haya conectado a la red, asegúrese  El indicador LED se vuelve verde. de que la tarjeta SIM que inserte pueda conectarse a la red.
- 

#### Paso 3 Agregar dispositivo

1. Abra el sitio. (Solo para HPC)

---

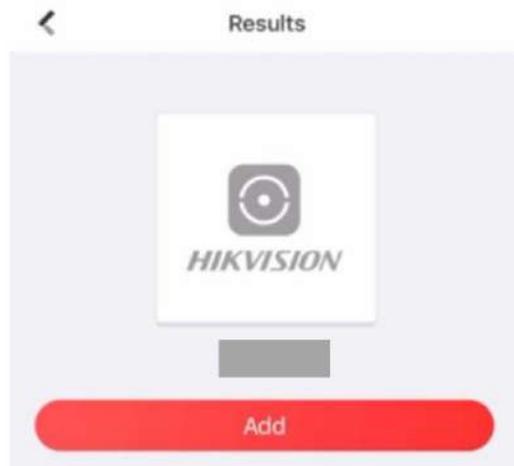
 **Nota**

Si bien inicializa el dispositivo con Hik-Connect, no es necesario que cree un sitio primero.

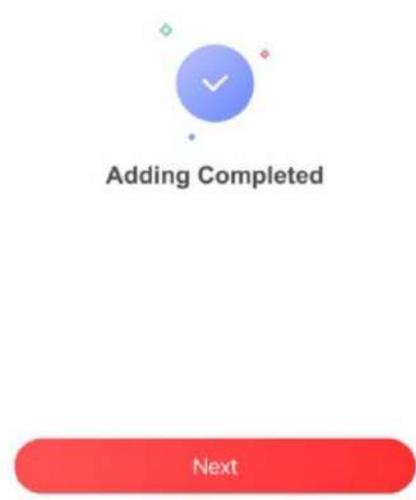
---

2. Toque + y escanee el código QR en la etiqueta del panel.

3. Toque **Agregar**.



4. Toque **Siguiente**. Puede editar los parámetros del dispositivo o saltar para usarlo directamente.



El panel de control se agregará al sitio (HPC) creado y administrado por la cuenta del instalador, lo que también significa que la cuenta del instalador se creó en el panel.

El instalador ahora puede realizar la configuración y las pruebas del panel antes de implementarlo. Tanto el servicio Hik ProConnect/Hik-Connect como el cliente web local pueden iniciar sesión con la cuenta del instalador de Hik ProConnect/Hik-Connect.

---

 **Nota**

Si bien inicializa el dispositivo con Hik-connect, no es necesario que cree un sitio primero. Descargue e inicie sesión en la aplicación y agregue el dispositivo escaneando el código QR o ingrese el número de serie del dispositivo.

---

### 3.2.3 Activación con Wi-Fi

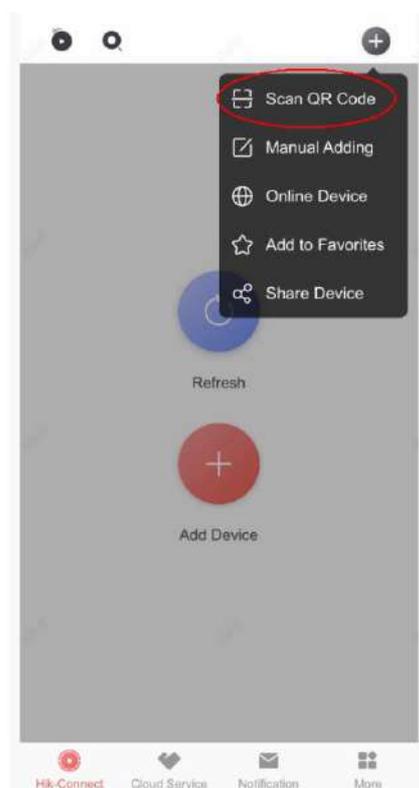
### Paso 1 Crear un sitio (Solo para HPC)

Descargue Hik-ProConnect e inicie sesión con la cuenta del instalador.

Un sitio es el lugar donde se desplegó el sistema de alarma. Cree un sitio donde se pueda agregar el dispositivo con su nombre y dirección del sitio. El propietario del sitio sería un usuario final, generalmente considerado como administrador.

### Paso 2 Configure la red en la aplicación

1. Descargue Hik-Connect/Hik-ProConnect e inicie sesión.
2. Encienda el AX PRO.
3. Conecte su teléfono a la red Wi-Fi de su hogar. Asegúrese de que este Wi-Fi pueda acceder a Internet normalmente y que la señal sea estable.
4. Abra el HC o HPC, haga clic en + y seleccione **Escanear código QR**.



5. Escanee el código QR en la parte posterior del panel de control y espere el resultado.



6. Toque **Siguiente**.

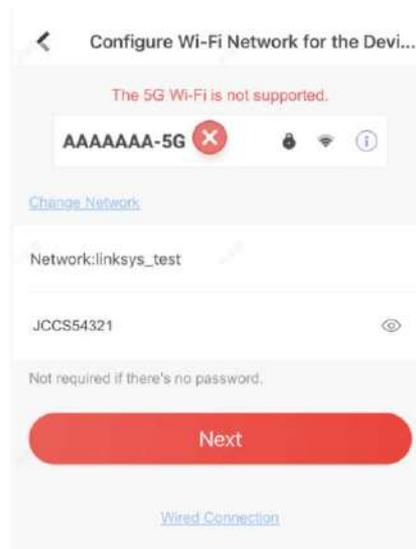
7. Toque **Conexión inalámbrica**.



8. Verifique que el dispositivo esté iniciado. Y luego toque **Siguiente**.



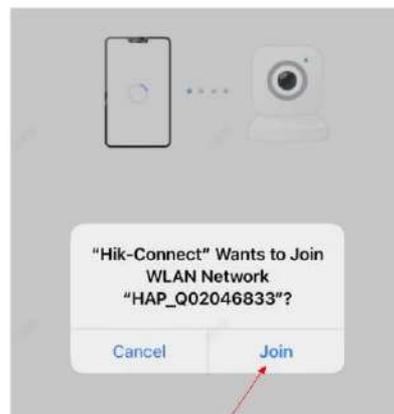
9. La aplicación completará automáticamente en la página el WiFi doméstico utilizado actualmente por el teléfono móvil, como se muestra en la figura a continuación. Después de confirmar la contraseña de WiFi, toque **Siguiente**.



10. Toque **Conectarse a una red**.



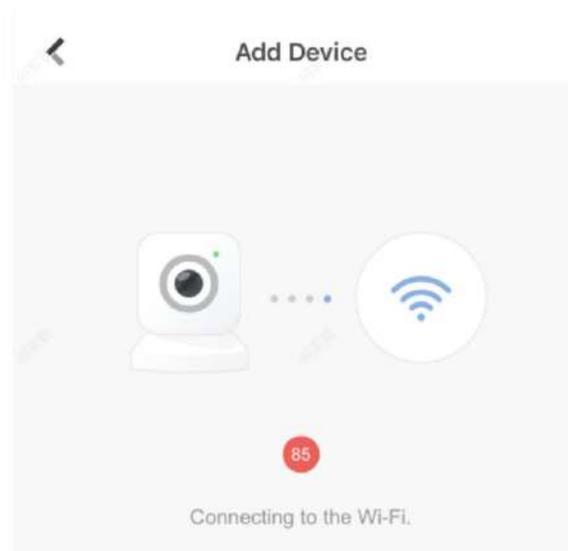
11. Toque **Unirse**. El teléfono móvil desconectará el Wi-Fi de casa. Después de interactuar la información con el panel de control, el teléfono móvil volverá automáticamente al Wi-Fi doméstico.



Como se muestra en la figura anterior, durante la interacción de la información, el Wi-Fi se conectó al teléfono móvil llamado "HAP\_serial number" (número de serie AX PRO)

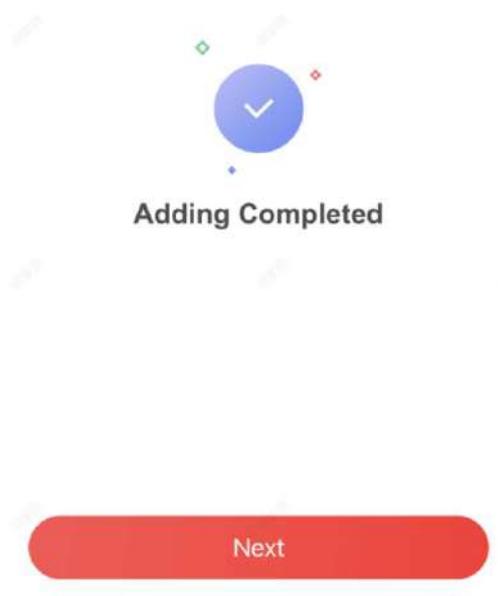


12. Después de que el panel de control emita "Salir del modo de punto de acceso", aparecerá la siguiente página.

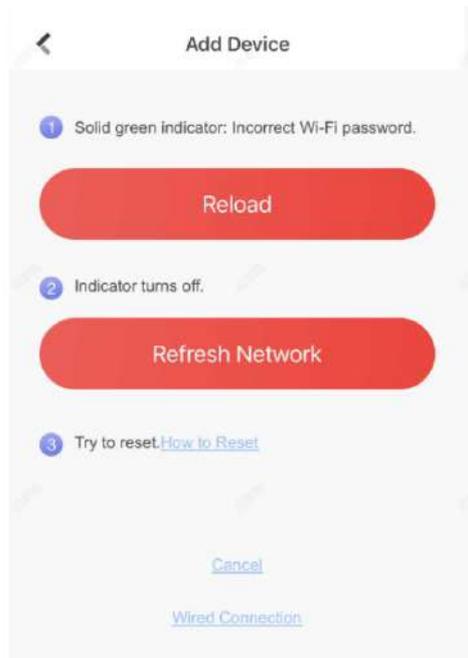


13. Espere a que el dispositivo se una al WiFi doméstico e inicie sesión en EZVIZ Cloud.

(1) Cuando la señal WiFi del hogar sea buena, el panel de control iniciará sesión correctamente en EZVIZ Cloud y completará el enlace antes de que finalice la cuenta regresiva.



(2) Cuando la señal Wi-Fi doméstica es inestable, es posible que el panel de control no esté conectado al EZVIZ Cloud antes de que finalice la cuenta atrás y aparecerá la siguiente página:



Si se asegura de que la contraseña del Wi-Fi doméstico sea correcta y la calidad sea buena, toque **Actualizar red**, el panel de control ingresará una nueva cuenta regresiva. Puedes esperar la conexión.

Si desea cambiar el Wi-Fi doméstico, primero debe cambiar el Wi-Fi doméstico conectado al teléfono móvil, luego presione el botón **RESET** en la parte posterior del panel de control (marcado en la figura a continuación). Después de escuchar la voz de "Ingresar al modo de punto de acceso", toque **Recargar**. La interfaz retrocederá a paso 9, puede configurar la red nuevamente.



---

 **Nota**

Una vez conectado el dispositivo a la red, el



El indicador LED se vuelve verde.

---

### 3.3 Desvincular el dispositivo

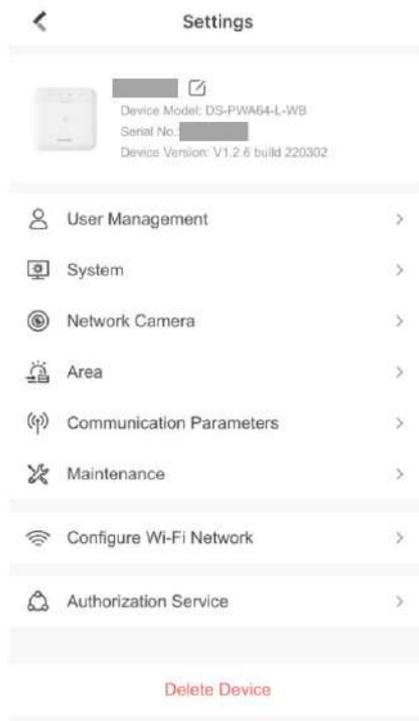
#### 3.3.1 Desvincular el dispositivo de su propia cuenta

Cuando el dispositivo está vinculado a su propia cuenta, puede eliminarlo directamente.

1. En la página de la lista de dispositivos, toque el AX PRO y luego inicie sesión en el dispositivo (si es necesario) para ingresar a la página.

2. Toque .

3. Toque **Eliminar dispositivo**.



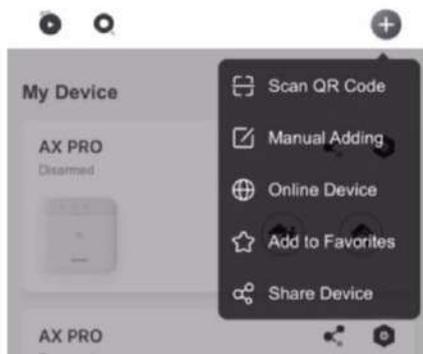
#### 3.3.2 Desvincular el dispositivo de otra cuenta

Asegúrese de que el panel de control esté en sus manos.

El teléfono y el dispositivo están en el mismo segmento de red.

1. Abra HC/HPC y toque +.

2. Toque **Escanear código QR**.



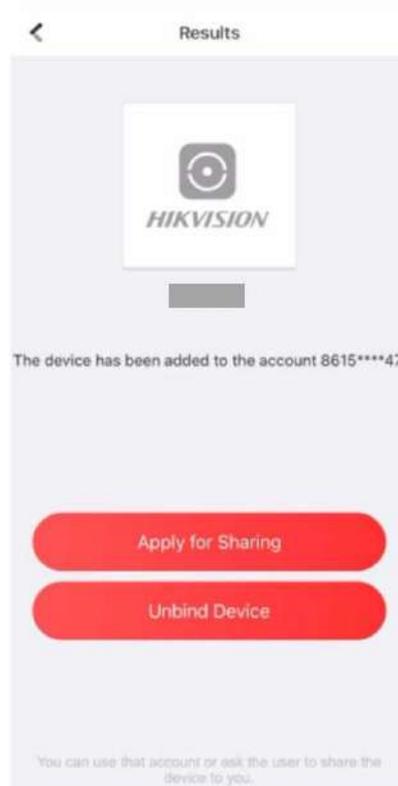
3. Escanea el código QR en la etiqueta del dispositivo.



4. Presione el botón **RESET** dos veces rápidamente en la parte posterior del dispositivo.



5. Toque **Desvincular dispositivo**.



5. Ingrese el código de verificación y toque **Finalizar**.



El dispositivo está desvinculado de la cuenta. Puedes agregarlo a tu cuenta ahora.

## Capítulo 4 Gestión de usuarios

### 4.1 Gestión de usuarios

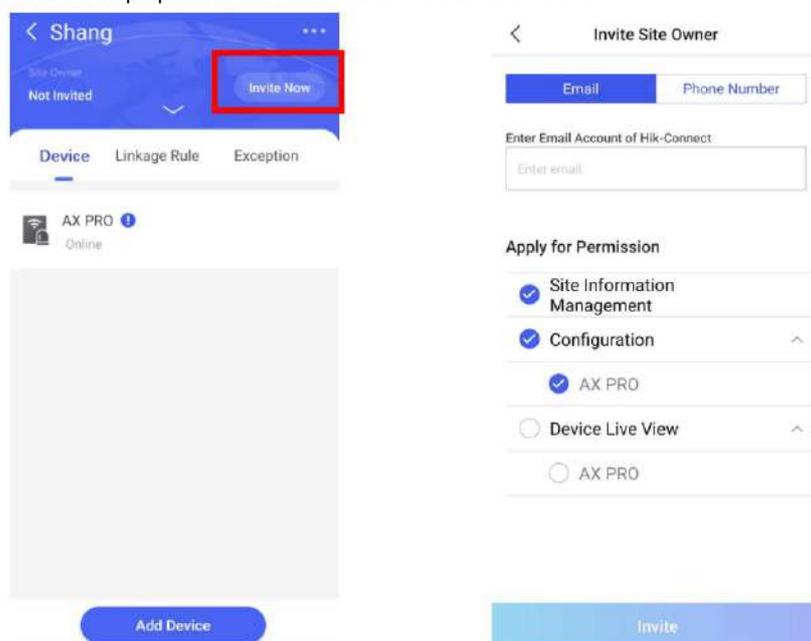


#### Nota

- Los usuarios se pueden crear en clientes.
- El nombre y la contraseña del usuario de la red (cliente web y usuario de la aplicación) pueden tener entre 1 y 32 caracteres y de 8 a 16 caracteres.

#### 4.1.1 Invitar al administrador

El administrador era conocido como propietario del sitio en Hik-ProConnect Service.



Una vez finalizada la configuración inicial, el instalador invitará al propietario del sitio y solicitará el permiso de administración del sitio y configuración del dispositivo desde la cuenta del administrador. La cuenta de administrador sería una cuenta de usuario final en el servicio Hik-Connect.

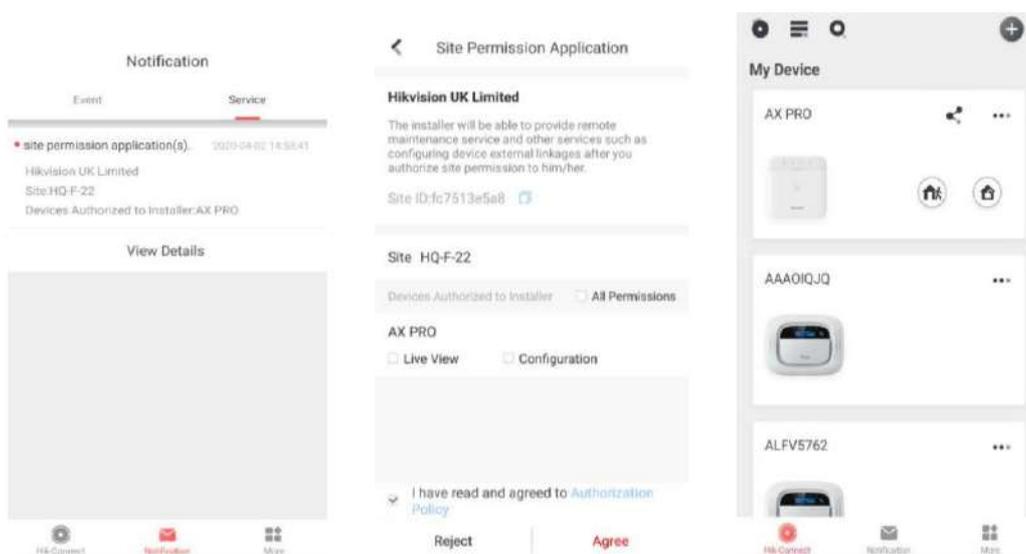
1. Presione el botón **"Invitar ahora"** e ingrese la cuenta de correo electrónico o el número de teléfono para transferir la propiedad del sitio al administrador. Al mismo tiempo, el instalador aplicará los permisos del propietario del sitio, como configuración y administración.
2. **Opcional:** marque **Permitirme desactivar el servicio Hik-Connect**.

**Nota**

- Si la casilla de verificación está marcada, después de entregar el Sitio a su cliente y su cliente aprueba la solicitud, puede desactivar el servicio Hik-Connect para los dispositivos que alquile a su cliente sin su autorización. Si el servicio Hik-Connect está deshabilitado, su cliente no puede operar en estos dispositivos a través del cliente móvil de Hik-Connect.

3. Abra la aplicación Hik-Connect e inicie sesión con la cuenta de administrador. La solicitud de servicio del instalador se recibirá en la página de notificación. Abra el detalle de la notificación para aceptar el servicio de instalación y los permisos de configuración. El panel de control y otros dispositivos en el sitio se mostrarán en su lista de dispositivos.

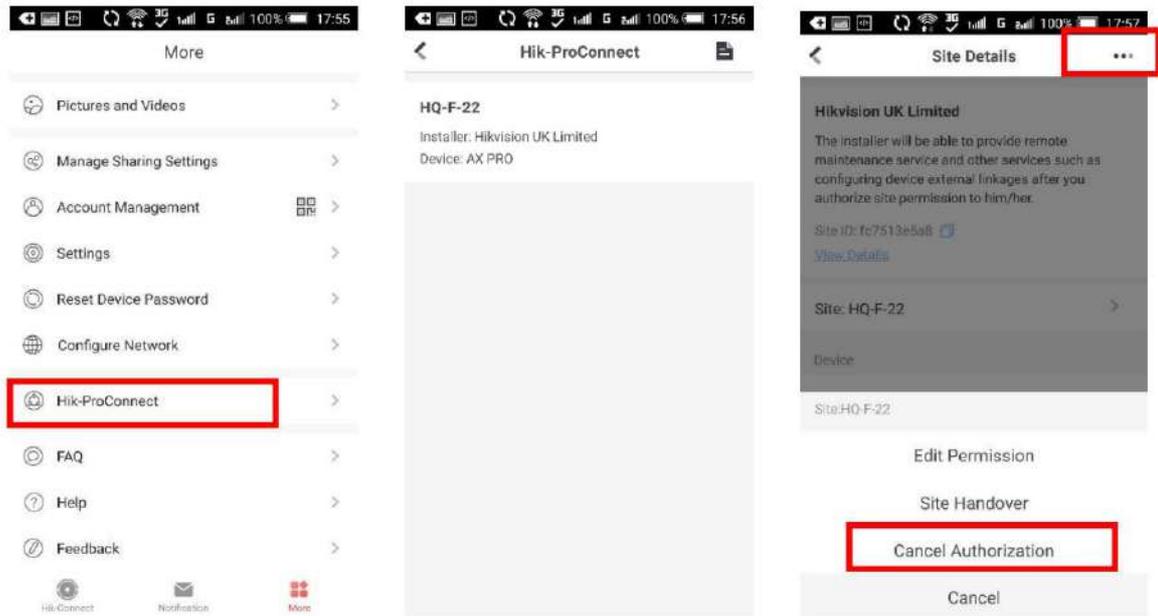
La cuenta de administrador se agregará al panel de control, que podría usarse para iniciar sesión en la aplicación Hik Connect y el cliente web local.



#### 4.1.2 Cancelar el acceso del instalador

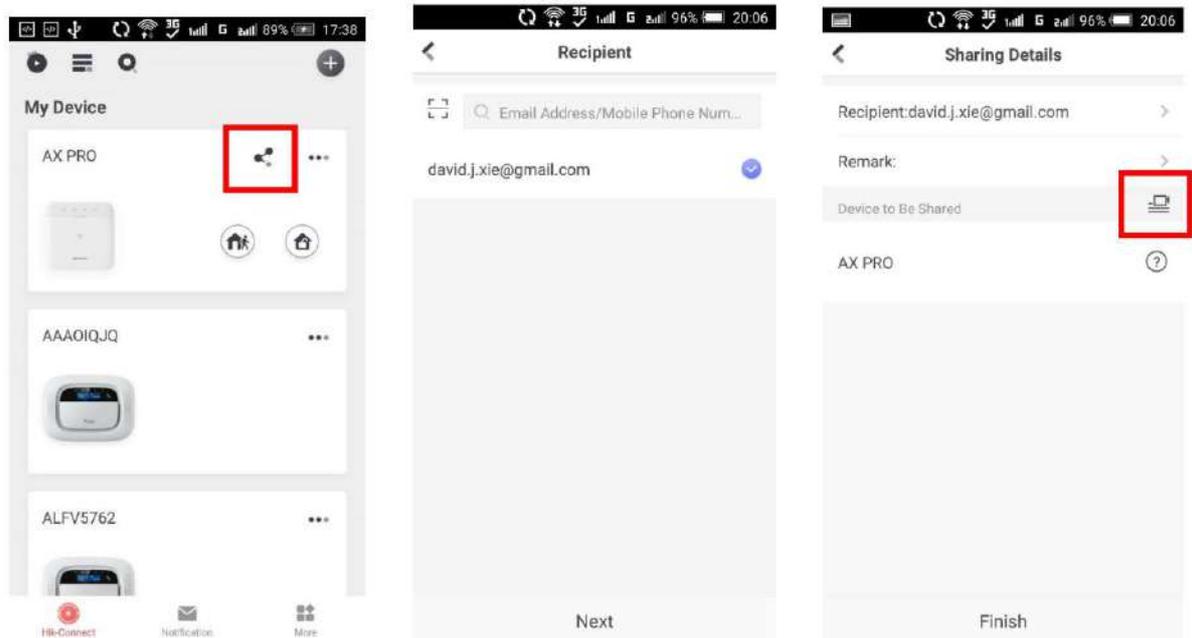
El administrador puede cancelar la autorización de acceso del instalador.

1. Ingrese a la página **Más** y toque **Hik-ProConnect**. Todos los sitios administrados por Hik-ProConnect El servicio se enumeran en la página.
2. Toque el botón de opción en la esquina superior derecha de la página de detalles del sitio y toque **Cancelar autorización** en el menú emergente.
3. Confirme la operación y se cancelará la autorización del instalador. Una vez cancelada la autorización, el instalador deberá volver a aplicarla si hubiera algún requisito de acceso.



### 4.1.3 Agregar un Operador

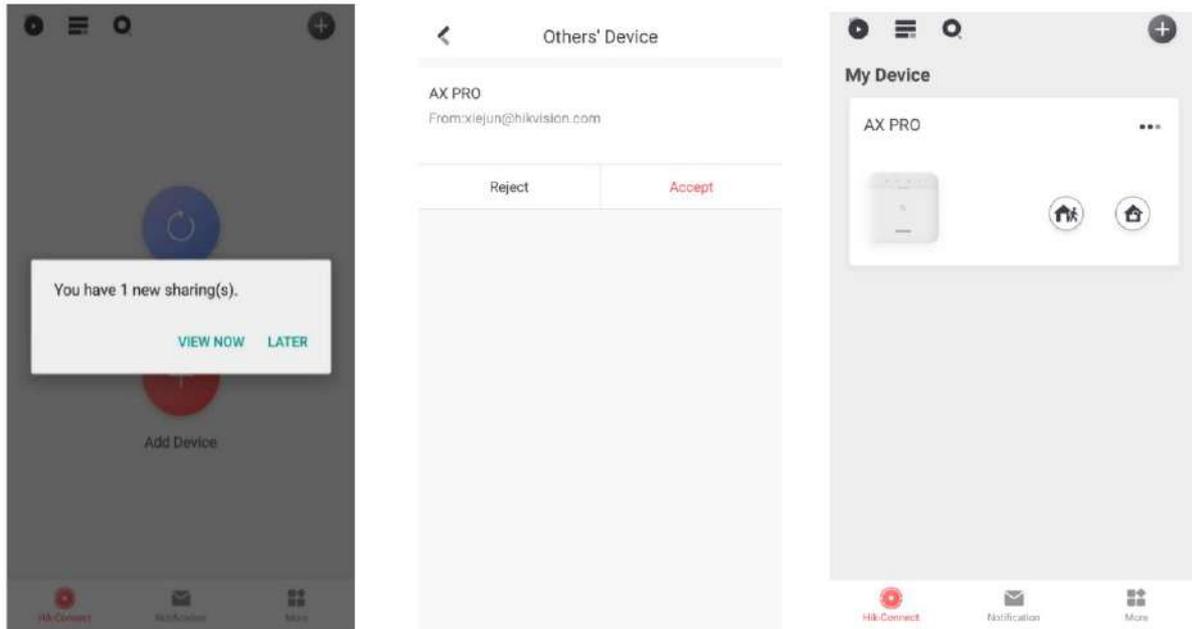
El administrador puede compartir el dispositivo con otros operadores.



1. Toque el  (botón compartir) en la lista de dispositivos.

2. Ingrese la cuenta Hik-Connect del operador.

El administrador también puede seleccionar qué dispositivo compartir.



Se enviará un mensaje compartido a la cuenta del operador, y el operador puede leer el mensaje en la aplicación Hik-Connect.

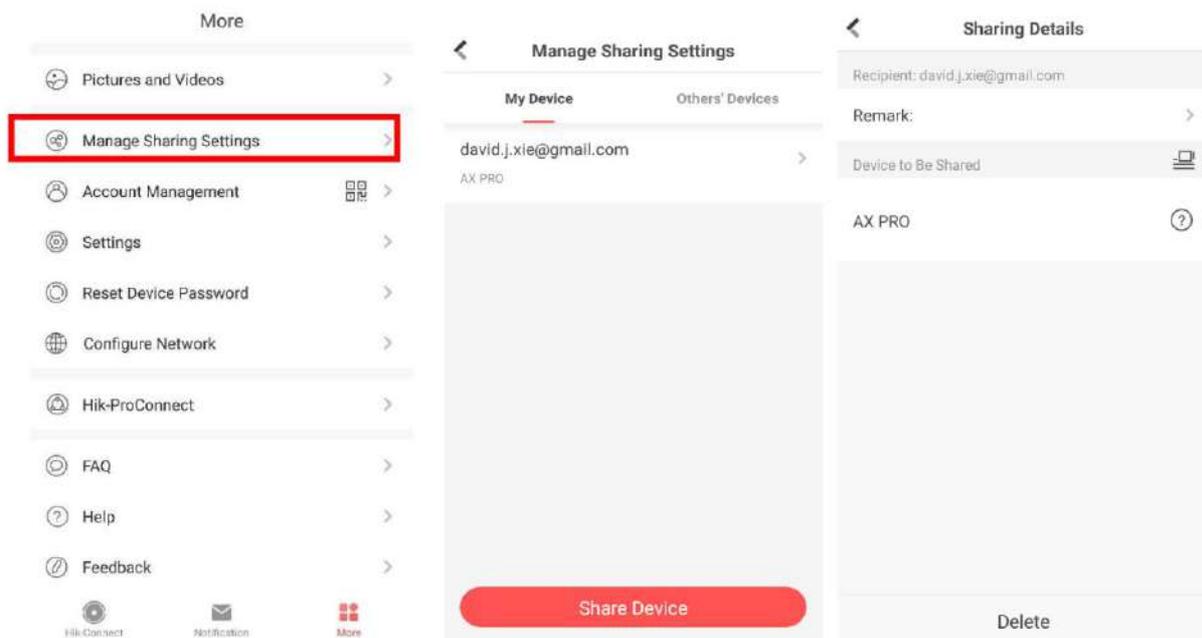
3. Acepte la invitación y el dispositivo aparecerá en la lista de dispositivos.

La cuenta del operador se agregará al panel de control, que podría usarse para iniciar sesión en la aplicación Hik Connect y el cliente web local.

#### 4.1.4 Eliminar un Operador

El usuario administrador puede eliminar un operador.

1. Ingrese a la página **Más** y toque **Administrar configuración de uso compartido**.
2. Elimine el operador seleccionado o elimínelo del dispositivo.



## 4.1.5 Deshabilitar el servicio Hik-Connect



- El sitio debe ser un sitio de alquiler.
- El instalador del lado de HPC debe marcar **Permitirme deshabilitar el servicio Hik-Connect** cuando invitar al administrador y al administrador del lado HC también acepta esta opción.

Puede ir a la pestaña **Dispositivo** para deshabilitar el servicio Hik-Connect para un dispositivo o todos los dispositivos en este Sitio tocando o desactivando el interruptor del servicio Hik-Connect. También puede eliminar los dispositivos de la cuenta Hik-Connect de su cliente sin

## 4.1.6 Invitar al instalador

1. En HC, toque  en la lista de dispositivos



2. Toque **Compartir con el instalador** e ingrese la dirección de correo electrónico.
3. Toque **Aceptar**.
4. Toque **Compartir con el instalador** y **Compartir código QR**
5. En HPC, seleccione un sitio y toque **Agregar dispositivo**.
6. Escanea el código QR.
7. En HC, el usuario recibirá una solicitud de autorización del dispositivo. Vaya a la página de la aplicación y toque **Aceptar**.
8. Vaya a **Servicio en la nube** y **Autorización de dispositivos** y **Autorizar más dispositivos**
9. Seleccione dispositivos y permisos.
10. Toque **Aceptar** y los dispositivos se autorizarán al instalador y se agregarán al sitio.

## 4.2 Entradas de acceso

Al instalador ya los operadores del AXPRO se les asignaron diferentes niveles de acceso que definen las funciones del sistema que puede realizar un usuario individual. Se proporcionan varias entradas de usuario para

diferentes roles de usuario con un nivel de acceso particular.

### **Entradas de acceso para instaladores (nivel de acceso 3)**

#### **ÿ Servicio Hik-ProConnect**

Hik-ProConnect es un servicio para instaladores que se utiliza para administrar los sistemas de alarma de los clientes ubicados en varios sitios de forma remota. Los paneles de control se pueden agregar a una cuenta de instalador en el servicio Hik-ProConnect y se pueden administrar en los sitios.

#### **ÿ Cliente web local**

Visite la dirección IP del dispositivo que se puede encontrar con la herramienta SADP. El instalador puede iniciar sesión con la cuenta de servicio Hik-ProConnect después de agregar el panel.

#### **ÿ Otras entradas**

Los PIN y las etiquetas del teclado también se pueden asignar con el usuario del instalador en un nivel de acceso particular para realizar operaciones esenciales.

### **Entradas de acceso para el administrador y los operadores (nivel de acceso 2)**

#### **ÿ Servicio Hik-Connect**

El servicio Hik-Connect se puede utilizar para que los usuarios finales accedan y administren los dispositivos.

#### **ÿ Cliente web local (para el administrador)**

Tan pronto como se agregó el panel a la cuenta de usuario final en el servicio Hik-Connect, la cuenta de Hik Connect se puede usar para iniciar sesión en la compilación del cliente web.

Los operadores no pueden iniciar sesión en el cliente web.

#### **ÿ Otras entradas**

Los PIN y las etiquetas del teclado también se pueden asignar con el usuario final en un nivel de acceso particular para realizar operaciones esenciales.

# Capítulo 5 Configuración

## 5.1 Configuración con Hik-Proconnect

### 5.1.1 Usar la aplicación Hik-Proconnect

El instalador puede usar Hik-Proconnect para configurar el AX PRO, como activación, inscripción de dispositivos, etc.

#### Descargue e inicie sesión en Hik-ProConnect

Descargue el cliente móvil Hik-ProConnect e inicie sesión en el cliente antes de operar el AX PRO.

##### Pasos

1. Descargue el cliente móvil Hik-ProConnect.
2. Opcional: Registre una nueva cuenta si es la primera vez que usa el cliente móvil Hik-ProConnect.



- Para obtener más información, consulte *el Manual del usuario de Hik-ProConnect Mobile Client*.
  - Necesita un código de invitación para registrarse. Por favor pregunte a los soportes técnicos.
- 

3. Ejecute e inicie sesión en el cliente.

#### Agregar AX PRO al cliente móvil

Agregue AX PRO al cliente móvil antes de otras operaciones.

##### Pasos

1. Encienda el AX PRO.
2. Cree o busque un sitio.
  - Toque +, establezca el nombre del sitio, la zona horaria, la dirección, la ciudad, el estado/provincia/región y toque **Aceptar** para crear un sitio.
  - Ingrese el nombre del sitio en el área de búsqueda y toque el **ícono** de búsqueda para buscar un sitio.
3. Toque **Agregar dispositivo**.
  - Toque **Escanear código QR** para ingresar a la página Escanear código QR. Escanee el código QR en el AXE PRO.



Normalmente, el código QR está impreso en la etiqueta pegada en la tapa trasera del AXE PRO.

---

Toque **Adición manual** para ingresar a la página Agregar dispositivo. Ingrese el número de serie del dispositivo y el código de verificación para agregar el dispositivo.

4. Active el **dispositivo**.

## Agregar periférico al AX PRO

Agregue periférico al AX PRO.

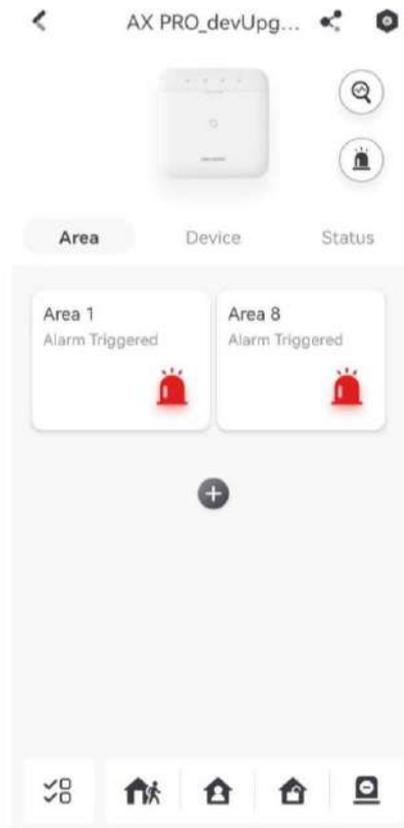
### Pasos

1. Seleccione un sitio.
2. Seleccione un dispositivo de control (AX PRO).
3. Toque el ícono + .
  - Escanea el código QR en el periférico.
  - Tocar  para entrar en la página Entrada manual. Ingrese el número de serie del dispositivo y seleccione el dispositivo escriba para agregar el dispositivo.

### Página principal

Puede ver fallas, armar y desarmar áreas, ver el estado del dispositivo, etc.

En la página de la lista de dispositivos, toque el AX PRO y luego inicie sesión en el dispositivo (si es necesario) para ingresar a la página.



### Activar la alarma

Tocar  para seleccionar Alarma de **pánico audible** o Alarma de **pánico silenciosa**.

### Ver fallas

Tocar  para ver fallas.

### Gerencia de Área

Toque **+** para agregar un área.

Toque Área para ingresar a la página de administración del área. Consulte **Establecer horario de armado/desarmado** para obtener más detalles.

### Armar/Desarmar el Área

Arma o desarma el área manualmente como desees.

En la página de la lista de dispositivos, toque el AX PRO y luego inicie sesión en el dispositivo (si es necesario) para ingresar al Área página.

### Operaciones para una sola área



- **Armado Ausente:** Pulse  para armar lejos una sola área. Cuando todas las personas en el área de detección salir, active el modo Ausente para armar todas las zonas en el área después del tiempo de permanencia definido.
- **Armado En Casa:** Pulse  para armar una sola área. Cuando todas las personas permanezcan dentro del área de detección, active el modo Permanecer para armar todo el conjunto de detección de robo perimetral en todas las zonas de todos. áreas

### Operaciones para áreas múltiples



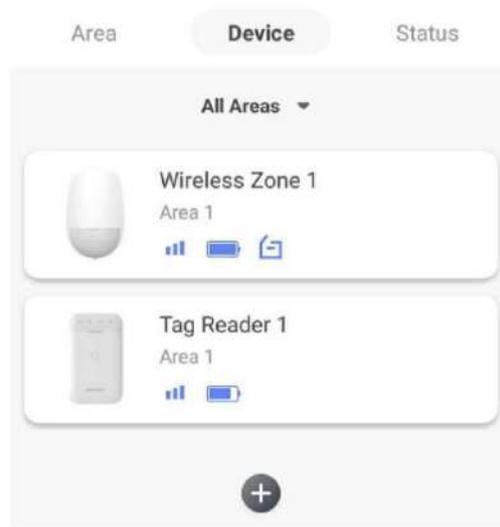
- **Seleccionar áreas:** toca  para seleccionar las áreas que desea operar. Si no selecciona áreas, siguiendo las operaciones surtirán efecto para todas las áreas.
- **Armado Ausente:** Pulse  para armar áreas seleccionadas. Cuando todas las personas en el área de detección se vayan, active el modo Ausente para armar todas las zonas en todas las áreas después del tiempo de permanencia definido.
- **Armado En Casa:** Pulse  Para quedarte armar todas las áreas. Cuando las personas permanezcan dentro del área de detección, active el modo Permanecer para armar toda la detección de robo perimetral (como detector perimetral, contactos magnéticos, detector de cortina en el balcón) configurada en todas las zonas de todas las áreas. Mientras tanto, los detectores dentro del área de detección se omiten (como los detectores PIR). Gente

puede moverse dentro del área y la alarma no se activará.

- **Desarmar:** toque  para desarmar todas las áreas. En el modo Desarmado, todas las zonas de todas las áreas no activan la alarma, sin importar si los eventos de alarma ocurren o no.
- **Alarma silenciosa:** toque  hasta alarmas silenciosas para todas las áreas.

## Gestión de zonas

1. Toque **Dispositivo** para ver las zonas vinculadas.



2. Toque + para agregar una nueva zona.
3. Toque una zona para ingresar a la página de administración. Puede ver el estado del dispositivo (por ejemplo, temperatura, estado de la batería, fuerza única, etc.).
4. Toque en la esquina superior derecha para ingresar a la página de configuración de zona.
5. Seleccione un tipo de zona.

Puede ver los tipos de zona configurables para varios detectores a través de **1. Tipos de zona de detector.**

### Zona instantánea

Este tipo de zona activará inmediatamente un evento de alarma cuando esté armada.

### Zona de retraso

**-Retraso de salida:** El retraso de salida le proporciona tiempo para salir de la zona sin alarma.

El armado con fallas está habilitado: primero debe confirmar las fallas y luego la zona está en proceso de armado. Si la zona de retardo se activa dentro del tiempo de retardo de salida pero se restablece antes de que finalice el tiempo, la alarma no se activará y la zona se armará.

El armado con fallas está deshabilitado: Armado inmediato. Si la zona de retardo se activa dentro del tiempo de retardo de salida pero se restablece antes de que finalice el tiempo, la alarma no se activará.

**-Retraso de entrada:** el retraso de entrada le proporciona tiempo para ingresar a la zona para desarmar el sistema sin alarma.

Después de la activación, si la zona no se desarma o silencia antes de que finalice el tiempo de retardo de entrada, la zona emitirá una alarma.

**-Tiempo de Retardo de Armado Parcial:** El armado Parcial usa el Tiempo de Retardo de Armado Parcial para la cuenta regresiva.

El sistema da un tiempo de retardo de entrada/salida cuando se arma o se vuelve a entrar. Por lo general, se utiliza en la ruta de entrada/salida (p. ej., puerta principal/entrada principal), que es una ruta clave para armar/desarmar a través del teclado operativo para los usuarios.



• Puede establecer 2 duraciones de tiempo diferentes en **Opciones del sistema** y **Programación y temporizador**.

• Asegúrese de que el temporizador no supere los 45 segundos para cumplir con EN50131-1.

• Puede configurar el tiempo de retardo de armado en casa para la zona de retardo.

---

### Zona de pánico

Zona activa de 24 horas, esté armada o no. Informe de alarma de pánico después de la activación. Suele utilizarse en los locales equipados con botón de pánico, detector de humo y detector de rotura de cristales.

### alarma medica

Zona activa de 24 horas, esté armada o no. Informe de alarma médica después de la activación.

### Zona de fuego

Zona activa de 24 horas, esté armada o no. Informe de alarma de incendio después de la activación.

### Zona de Gas

Zona activa de 24 horas, esté armada o no. Informe de alarma de gas después de la activación.

### Zona de seguimiento

La zona actúa como zona retardada cuando detecta un evento de activación durante el retardo de entrada del sistema, mientras que actúa como zona instantánea en caso contrario.

### Zona de interruptor de llave

**-Por tiempo de disparo:** cambie el estado de armado y desarmado después de cada disparo. Por ejemplo, en el estado desarmado, si la zona se activa, el área vinculada se armará. Active la zona nuevamente y el área se desarmará.

**-Por estado de zona:** debe elegir armar o desarmar el área vinculada después de que se active la zona.

En el caso de la alarma de manipulación, la operación de armado y desarmado no se activará.

### Zona deshabilitada

Zona deshabilitada ignorando cualquier evento de alarma. Por lo general, se utiliza para desactivar detectores defectuosos.

### Zona 24 horas

La zona se activa todo el tiempo con salida de sonido/luz cuando ocurre la alarma, ya sea que esté armada o no. Por lo general, se usa en áreas con riesgo de incendio equipadas con detectores de humo y sensores de temperatura.

#### Zona de tiempo de espera

La zona se activa todo el tiempo. Cuando esta zona se haya activado o restaurado y exceda el tiempo establecido, se generará una alarma.

Se puede utilizar en lugares equipados con contactos magnéticos que requieren acceso pero solo por un período corto (por ejemplo, la puerta de la caja de la boca de incendios u otra puerta de la caja de seguridad externa).

**-Alarma de zona no activada:** Si la zona no se activa durante el tiempo establecido, se activará la alarma.

**-Alarma en Zona Activada:** Si la zona se activa durante el tiempo establecido, emitirá una alarma.

**-Período de tiempo de reintento:** establezca el período de tiempo de espera.

6. Habilite **Zona cruzada, Alarma silenciosa, etc.** según sus necesidades reales.



#### Nota

Algunas zonas no admiten la función. Consulte la zona real para configurar la función.

---

#### Modo armado

Si la zona es una zona pública (la zona pertenece a más de un área), puede configurar el modo de armado.

**Y:** Cuando todas las áreas enlazadas estén armadas, la zona se armará. Cuando cualquiera de las áreas vinculadas se desarma, la zona se desarmará.

**O:** Cuando cualquiera de las áreas enlazadas esté armada, la zona se armará. Cuando todas las áreas vinculadas estén desarmadas, la zona se desarmará. Cuando la zona está en alarma, las áreas desarmadas vinculadas con la zona no se pueden armar.

#### Bypass de Armado Parcial

La zona se anulará automáticamente en el armado En Casa.

#### Zona cruzada

**PD6662 no está habilitado:** debe configurar el intervalo de tiempo combinado.

Cuando se activa la primera zona, el sistema comenzará a cronometrar después de que se restablezca la zona. Si la segunda zona se activa dentro del tiempo establecido, ambas zonas darán alarmas. De lo contrario, no se activará ninguna alarma.

Si la primera zona no se restablece, ambas zonas darán alarmas cuando se active la segunda zona, independientemente de si ha transcurrido el tiempo establecido.

**PD6662 está habilitado:** debe configurar el intervalo de tiempo combinado.

La primera zona dará una alarma cuando se active. Si la primera zona no se restablece y la segunda zona se activa, el sistema informará la confirmación de la alarma.

Si se restablece la primera zona, el sistema comenzará a cronometrar. Si la segunda zona se activa dentro del tiempo establecido, el sistema informará la confirmación de la alarma.

Si se restablece la primera zona, el sistema comenzará a cronometrar. Si la segunda zona no se activa dentro del tiempo establecido, no se reportará ninguna información.

#### Prohibir anular al armar

Una vez habilitado, no puede anular zonas al armar.

#### Repicar

Habilitar el timbre. Normalmente se utiliza para detectores magnéticos de puertas.

#### **alarma silenciosa**

Después de habilitarse, cuando se activa una alarma, solo se cargará el informe y no se emitirá ningún sonido.

#### **Doble golpe**

Después de habilitarlo, se puede configurar el intervalo de tiempo. Si el mismo detector se activa dos veces o de forma continua en un período de tiempo, se activará la alarma.

#### **Tiempo de retardo de sirena**

La sirena se activará inmediatamente (0s) o después del tiempo establecido.

#### **Salida de la puerta final**

Solo los contactos magnéticos tienen esta opción.

Después de habilitar, cuando el usuario use teclados o lectores de etiquetas para armar:

-Armar con fallas está habilitado: Durante la cuenta regresiva de armado, si el contacto magnético se activa y luego se restablece, el proceso de armado terminará inmediatamente después.

restaurando, y el armado está completo.

- Armar con fallas está deshabilitado: si el contacto magnético se activa y luego se restablece, el área enlazada arma inmediatamente la zona retardada.

#### **Activaciones de Límite Swinger (Zona Cableada)**

Cuando el número de veces que se activa el detector de infrarrojos supera el valor establecido, la alarma ya no se activará. (Excepto alarmas antienmascaramiento).

#### **Zona Dual (Zona Cableada)**

Después de habilitado, cuando el transmisor múltiple detecta que todo el circuito de zona de la zona local y la zona extendida está en circuito abierto, ambas zonas activan alarmas de tapa abierta.

## **Gestión de usuarios**

Los instaladores (usuario de Hik-ProConnect) pueden gestionar usuarios. Si es el administrador, puede agregar, editar y eliminar usuarios, y asignar diferentes permisos a los usuarios recién agregados.

### **Pasos**



Hay cuatro tipos de usuarios para el AX PRO, incluido el administrador (o propietario), el operador y el instalador (o instalador). Los diferentes tipos de usuarios tienen diferentes permisos para acceder a la funcionalidad de AX PRO.

- 
1. Ingrese al sitio, toque AX PRO y luego inicie sesión en el dispositivo (si es necesario) para ingresar a AX PRO página.
  2. Toque **Siguiente** para invitar al usuario.

---

 **Nota**

El destinatario debe aceptar la invitación.

---

3. Toque  **Administración de usuarios** y **Usuario**.
4. Toque un usuario para ingresar a la página de administración de usuarios.
5. Opcional: Realice las siguientes operaciones si es necesario.

**Permiso de usuario**

Puede tocar el usuario de destino en la lista de usuarios y luego tocar **Editar icono** para establecer los permisos autorizados para el usuario de destino.

---

 **Nota**

Solo el administrador puede hacer tal operación.

---

**Establecer áreas vinculadas**

Si el usuario objetivo es un operador, toque el usuario objetivo en la lista de usuarios y luego toque **Áreas vinculadas** para establecer el área vinculada al usuario objetivo.

---

 **Nota**

Solo el administrador puede hacer tal operación.

---

**Cambiar teclado  
Clave**

Si el usuario de destino es un administrador, un instalador o un operador, puede tocar el usuario de destino en la lista de usuarios y luego tocar **Cambiar contraseña del teclado** para establecer la contraseña del teclado para el usuario de destino.

**Cambiar coacción  
Clave**

Si el usuario objetivo es un administrador o un operador, puede tocar el usuario objetivo en la lista de usuarios y luego tocar **Cambiar contraseña de coacción** para establecer la contraseña de coacción para el usuario objetivo.

---

 **Nota**

Si está bajo coacción, puede ingresar el código de coacción en el teclado para armar y desarmar áreas y cargar una alarma de coacción.

---

**Control de automatización** Un administrador, un instalador o un operador pueden controlar el relé módulo, interruptor de pared y enchufe inteligente.

---

 **Nota**

- Los elementos de configuración y los permisos de usuario variarán según el tipo de usuario.
  - Puede ver tarjetas/etiquetas vinculadas y llaveros del usuario, pero no tiene permiso para hacerlo configurarlos.
-

## Gestión de tarjetas/etiquetas

Después de agregar tarjetas/etiquetas al AX PRO inalámbrico, puede deslizar la tarjeta/etiqueta para armar o desarmar todos los detectores agregados a áreas específicas del AX PRO y silenciar las alarmas.



El ID/PIN de la etiqueta es un número entero de 32 bits y la variante podría ser 42949672956.

---

### Pasos

1. Ingrese al sitio, toque el AXE PRO y luego inicie sesión en el dispositivo (si es necesario) para ingresar a la página.
2. Toque y **Administración de usuarios** y **Tarjeta/Etiqueta** para ingresar a la página Tarjeta/Etiqueta.
3. Toque + para agregar una etiqueta.
4. Cuando escuche el mensaje de voz "Swipe Tag", debe presentar la etiqueta en la etiqueta AXE PRO  
área de presentación. •  
Al escuchar un pitido, se reconoce la etiqueta. • La etiqueta se mostrará en la  
página de etiquetas.
5. Opcional: toque una etiqueta para ingresar a la página de configuración.
6. Toque **Editar icono** para editar el nombre de la etiqueta.



• Si inicia sesión como instalador, omite este paso. La edición del nombre de la etiqueta solo está disponible para el administrador. • El nombre debe contener de 1 a 32 caracteres.

---

7. Deslice **Activar etiqueta**.
8. Seleccione un usuario vinculado.
9. Seleccione el tipo de etiqueta



Diferentes usuarios vinculados tienen diferentes permisos de etiqueta.

---

### Etiqueta de operación

Puede deslizar la etiqueta para armar o desarmar.

### Etiqueta de

**patrulla** Cuando pase la etiqueta, el sistema cargará un registro.

10. Opcional: toque **Eliminar** para eliminar la etiqueta.

## Información del dispositivo

Puede cambiar el idioma y seleccionar la zona horaria.

### Pasos

1. En la página de la lista de dispositivos, toque AX PRO y luego inicie sesión en el dispositivo (si es necesario) para ingresar el página.
2. Toque **Sistema** y **Configuración** para ingresar a la página.
3. Seleccione el idioma y la zona horaria del dispositivo.
4. Habilite DST según sus necesidades.

horario de verano

El horario de verano (también llamado horario de verano) es la práctica de adelantar los relojes durante los meses más claros para que las noches tengan más luz del día y las mañanas menos.

## Gestión del sistema

### Pasos

1. En la página de la lista de dispositivos, toque AX PRO y luego inicie sesión en el dispositivo (si es necesario) para ingresar el página.
2. Toque **Sistema** y **Opciones del sistema** y **Administración** del sistema para ingresar a la página.

### Armado automático forzado

Después de habilitarse, cuando comienza el armado automático temporizado, si hay fallas activas en una zona, la zona se anulará automáticamente.

Puede ir a **Sistema** y **Opciones** de sistema y **Horario y hora** para configurar el horario de armado/desarmado automático y las áreas vinculadas.



Debe desactivar Armar con fallas en la página Opciones de armar. O la función de Armado automático forzado/Armado forzado no puede ser válida.

---

### Armado Forzado

Después de habilitarse, cuando comienza el armado manual, si hay fallas activas en una zona, la zona se omitirá automáticamente.

Puede usar llaveros, etiquetas y teclados para armar zonas o armar zonas manualmente en la aplicación. Se pueden seleccionar áreas individuales, múltiples o todas para armar.



Debe desactivar Armar con fallas en la página Opciones de armar. O la función de Armado automático forzado/Armado forzado no puede ser válida.

---

### Informe de estado del sistema

Si la opción está habilitada, el dispositivo cargará el informe a la nube (para APP) y ARC automáticamente cuando se cambie el estado de AX PRO.

### **Mensaje de voz**

Si la opción está habilitada, el AX PRO habilitará el mensaje de voz.

- Indicaciones de falla al armar: Indicaciones de voz de fallas al armar.
- Indicaciones de falla cuando está armado: Indicaciones de voz de fallas cuando el sistema está armado.
- Avisos de fallas al desarmar: aviso de voz de fallas al desarmar
- Indicaciones de falla cuando está desarmado: Indicaciones de voz de fallas cuando el sistema está desarmado.
- Indicaciones de voz en alarma: Indicaciones de voz de fallas cuando se activa una alarma.

### **Volumen del sistema**

El rango de volumen del sistema disponible es de 0 a 10.

### **Alarma audible de sabotaje**

Mientras está habilitado, el sistema alertará con un zumbador para la alarma de manipulación. Independientemente de si está habilitado o no, la alarma de manipulación normalmente se enviará a la nube (para APP) y ARC.

### **Botón de bloqueo del panel**

Todas las funciones de AX PRO se congelarán después de que se habilite. Esta función solo puede ser habilitada por usuarios con permiso de instalador.

### **Duración de la alarma**

Establezca un mensaje de voz de alarma vinculado que dure el tiempo.

### **Pérdida de supervisión inalámbrica**

Los detectores y periféricos cuyos tiempos de pérdida de latido superen el valor establecido se mostrarán como fuera de línea.

### **Anular al rearmar**

Mientras está habilitado, después de anular el detector, si se restauran sus fallas y se arma el área enlazada, el detector se armará automáticamente.

### **El LED de falla permanece encendido cuando**

está armado Cuando el sistema está armado, el indicador de falla siempre está encendido.

#### **Armar LED permanecer encendido**

El LED de brazo está siempre encendido.

### **Indicador Hik-Connect**

Habilite el indicador HC.

### **Restauración del detector de movimiento**

Los detectores de movimiento incluyen todos los detectores PIR.

- Desactivar: Sin restauración automática.
- Inmediatamente después de la alarma: los detectores de movimiento se restauran automáticamente inmediatamente después de la alarma e informan a Cloud (para APP) y ARC.
- Después de desarmar: los detectores de movimiento se restauran automáticamente después de desarmar e informan a la nube (para APP) y ARC

### **Ajustes de sensibilidad de interferencia**

El dispositivo detectará la interferencia de RF y enviará mensajes cuando la interferencia de RF interfiera con la comunicación. Puede ajustar la sensibilidad de detección.

#### **Modo de ahorro de energía**

Mientras está habilitado, la fuente de alimentación principal está apagada, Wi-Fi entra en bajo consumo de energía, 4G se cierra, falla la lectura de etiquetas, LED apagado y aviso de voz apagado.

#### **Restablecimiento del detector de humo**

Solo para la zona cableada de la central M2H, que está configurada como detector de humo.

#### **Habilitar PD6662**

Habilitar el estándar PD6662. Las funciones que no cumplan con el estándar no tendrán efecto.

#### **Verificación de fallas**

La verificación de fallas aquí es solo para el panel de control en el estado normal.

El sistema determina si verificar las fallas enumeradas en la página. El sistema sólo comprobará el fallo que esté seleccionado.

#### **Pasos**

1. En la página de la lista de dispositivos, toque el AX PRO y luego inicie sesión en el dispositivo (si es necesario) para ingresar el página.
2. Toque y **Sistema** y **Opciones del sistema** y **Verificación de fallas del sistema** para ingresar a la página.

#### **Detectar la desconexión de la cámara de red**

Esta opción solo aparece si se ha agregado una cámara a AX PRO.

Si la opción está habilitada, cuando la cámara de red vinculada se desconecte, se activará una alarma. El tiempo de retraso de la detección de la desconexión de la cámara de red es el mismo que el de la LAN.

#### **Comprobación de pérdida de batería**

Si la opción está habilitada, cuando la batería del panel esté desconectada, el dispositivo cargará eventos.

#### **Comprobación de batería baja**

Si la opción está habilitada, cuando la batería del panel está en estado de batería baja, el dispositivo cargará eventos.

#### **LAN perdida**

Si la opción está habilitada, cuando la red cableada esté desconectada o con otras fallas, la alarma se disparará.

**-Retraso de pérdida de LAN:** si la red vuelve a la normalidad dentro de la duración del retraso, no se informará ninguna falla.

#### **Wi-Fi perdido**

Si la opción está habilitada, cuando el Wi-Fi esté desconectado o con otras fallas, la alarma se disparará.

**-Retraso de pérdida de WiFi:** si la red vuelve a la normalidad dentro de la duración del retraso, no se informará ninguna falla.

### **Celular Perdido**

Si la opción está habilitada, cuando la red de datos celular esté desconectada o con otras fallas, la alarma se disparará.

**-Retraso de pérdida de celular:** si la red vuelve a la normalidad dentro de la duración del retraso, no se informará ninguna falla.

### **Pérdida de alimentación de red del panel**

Si la opción está habilitada, se activará una alarma cuando se desconecte el suministro principal del panel de control.

### **Retardo de pérdida de alimentación de red del panel**

El sistema verifica la falla después de la duración de tiempo configurada después del apagado de CA.

Para cumplir con la norma EN 50131-3, la duración del tiempo de verificación debe ser de 10 s.

### **Opciones de armado**

Esta función es para todo el sistema de alarma, para informar al usuario del estado actual del sistema antes de armarlo. Si está habilitado, habrá un aviso de falla y un proceso de confirmación para los lectores de etiquetas, teclados, llaveros y la aplicación. Si no está habilitado, no habrá detección de fallas antes de armar.

### **Pasos**

1. En la página de la lista de dispositivos, toque AX PRO y luego inicie sesión en el dispositivo (si es necesario) para ingresar el página.
2. Toque **Sistema** y **Opciones del sistema** y **Opciones** de armado para ingresar a la página.

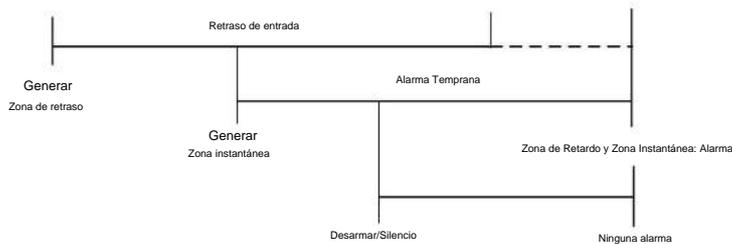
Puede configurar los siguientes parámetros:

### **Armar con falla**

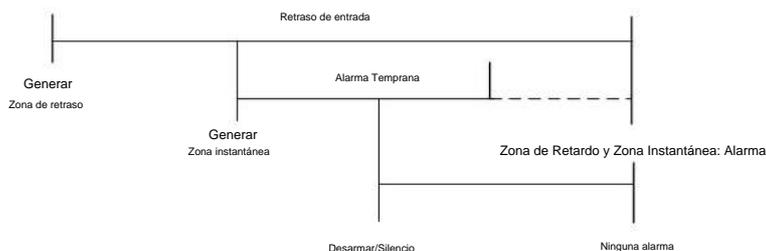
Verifique las fallas en la lista Habilitar armado con fallas, y el dispositivo no detendrá el procedimiento de armado cuando ocurran fallas.

### **Alarma**

**temprana** Primero se activa una zona de retraso y el área se encuentra en la etapa de "Retraso de entrada". Durante el período de tiempo de retardo, se activa una zona instantánea (solo para la primera zona instantánea activada). En este momento, el área entra en la etapa de alarma temprana. Hay alarma de voz del panel de control y alarma sonora local, pero no se envía ningún mensaje de alarma. Si la zona se desarma o se silencia antes de que finalicen la alarma temprana y el retardo de entrada, no se informará el mensaje de alarma. De lo contrario, tanto la zona retardada como la zona instantánea activarán la alarma.



O



3. Toque **Guardar**.

## Modo de inscripción

### Pasos

1. En la página de la lista de dispositivos, toque AX PRO y luego inicie sesión en el dispositivo (si es necesario) para ingresar el página.
2. Toque **Sistema** y **Opciones del sistema** y **Modo de inscripción** para ingresar a la página.
3. Toque **Entrar en el modo de inscripción**. Puede inscribir el periférico activándolo.

## Cámara de red

### Agregar cámaras al AX PRO

#### Pasos

1. En el sitio, toque AX PRO y luego inicie sesión en el dispositivo (si es necesario).
2. Toque **Cámara de red** y **Canal** de cámara de red para ingresar a la página.
3. Toque **Agregar canal**.
4. Introduzca la dirección IP, el puerto, el nombre de usuario y la contraseña de la cámara.
5. Toque **Guardar icono**.
6. Opcional: toca **Editar** o **Eliminar** para editar o eliminar la cámara seleccionada.

## Establecer parámetros de vídeo

### Pasos

1. En el sitio, toque AX PRO y luego inicie sesión en el dispositivo (si es necesario).
2. Toque y **Cámara de red** y **Configuración de vídeo de evento** para ingresar a la página.
3. Seleccione una cámara y configure los parámetros de vídeo.

#### Tipo de

transmisión Transmisión principal: se utiliza en la grabación y la vista previa de alta definición, tiene una alta resolución, tasa de codificación y calidad de imagen.

Sub-Stream: se utiliza para transmitir imágenes de red y obtener una vista previa como una transmisión de vídeo con características de menor resolución, tasa de bits y calidad de imagen.

#### Tipo de tasa de

**bits** Seleccione el tipo de tasa de bits como constante o variable.

#### Resolución

Seleccione la resolución de la salida de vídeo.

#### tasa de bits

El valor más alto corresponde a la calidad de vídeo más alta, pero se requiere un mejor ancho de banda.

#### Antes de la alarma

El tiempo de grabación antes de la alarma.

#### Después de la alarma

La duración del tiempo de grabación después de la alarma.

## Establecer horario de armado/desarmado

### Pasos

1. En la página de la lista de dispositivos, toque AX PRO y luego inicie sesión en el dispositivo (si es necesario) para ingresar el página.
2. Toque y **Área** para ingresar a la página.
3. Toque un área de la lista, habilite el área y seleccione los dispositivos vinculados.
4. Establecer parámetros:

#### Armado automático

Permita que el área se arme automáticamente en un punto de tiempo específico.

#### Tiempo de armado automático

Configure el horario para que el área se arme automáticamente.

#### Desarmado automático

Permita que el área se desarme automáticamente en un punto de tiempo específico.

#### Tiempo de desarme automático

Configure el horario para que el área se desarme automáticamente.

#### Indicación de sonido de autoarmado

Después de desactivarlo, el zumbador no emitirá un pitido antes del armado automático.

#### Tarde para desarmar

Habilite el dispositivo para enviar una notificación al teléfono o tableta para recordarle al usuario que debe desarmar el área cuando el área todavía está armada después de un punto de tiempo específico.



Debe habilitar la función Notificación de administración del panel en el Cliente web de **Parámetros de comunicación** y **Comunicación de eventos** antes de habilitar la función Tarde para desarmar.

---

#### Tiempo de retraso para desarmar

Establezca el punto de tiempo mencionado en **Tarde para desarmar**.

#### Excepción de fin de semana

Si está habilitado, **Auto Armado**, **Auto Desarmado** y **Tarde para Desarmar** están deshabilitados durante el fin de semana.

#### Vacaciones exceptuadas

Habilite la función y la zona no se armará/desarmará en las vacaciones. Debe configurar el programa de vacaciones después de habilitarlo.



Se pueden configurar hasta 6 grupos de vacaciones.

---

## Comunicación

### Red cableada

#### Pasos

1. En el sitio, toque AX PRO y luego inicie sesión en el dispositivo (si es necesario).
2. Toque y **Parámetros de comunicación** y **Red cableada** para ingresar a la página.
3. Configure los parámetros.
  - Configuración automática: habilite **DHCP** y configure el puerto HTTP.
  - Configuración manual: **DHCP** deshabilitado y configuración **de dirección IP, máscara de subred, dirección de puerta de enlace, DNS Dirección del servidor**.
4. **Opcional:** configure la dirección del servidor DNS correcta si el dispositivo necesita visitar el servidor Hik-Connect a través de un nombre de dominio.
5. Haga clic en **Guardar**.

## Configuración wifi

### Pasos

1. En el sitio, toque AX PRO y luego inicie sesión en el dispositivo (si es necesario).
2. Toque y **Parámetros de comunicación** y **Configuración Wi-Fi** para ingresar a la página.
3. Toque un Wi-Fi para conectarse en la lista.

## Red de datos móviles

### Pasos

1. En el sitio, toque AX PRO y luego inicie sesión en el dispositivo (si es necesario).
2. Toque y **Parámetros de comunicación** y **Configuración de red de datos móviles** para ingresar a la página.
3. Habilite **la red de datos móviles**.
4. Toque para seleccionar una tarjeta SIM. Toque **Configuración de parámetros** y **Editar icono** y configure los parámetros incluyendo el nombre de usuario, contraseña de acceso, APN, MTU y código PIN.
5. Toque **Guardar icono**.
6. Habilite **el límite de uso de datos**.
7. Edite **los datos utilizados este mes** y **los datos limitados por mes**.

### Número de acceso

Introduzca el número de marcación del operador.



Solo el usuario de la tarjeta SIM de la red privada necesita ingresar el número de acceso.

---

### Nombre de usuario

Pregúntele al operador de red e ingrese el nombre de usuario.

### Contraseña de acceso

Pregúntele al operador de red e ingrese la contraseña.

### APN

Pídale al operador de red que obtenga la información de APN e ingrese la información de APN.

### Datos limitados por mes

Puede habilitar la función y establecer el umbral de datos cada mes. Si el uso de datos supera el umbral configurado, se activará una alarma y se cargará en el centro de alarmas y el cliente móvil.

### Datos utilizados este mes

Los datos utilizados se acumularán y se mostrarán en este cuadro de texto.

## Notificaciones push

Cuando se activa una alarma, si desea enviar la notificación de alarma al teléfono móvil, debe

puede establecer los parámetros de envío de notificaciones.

#### **Pasos**

1. En el sitio, toque AX PRO y luego inicie sesión en el dispositivo (si es necesario).
2. Toque y **Parámetros de comunicación** y **Notificación(es) automática(s)** para ingresar a la página.
3. Habilite la notificación de destino.

#### **Alarma de zona/tapa abierta** El

dispositivo enviará notificaciones cuando se active la alarma de zona o cuando se active o restablezca la tapa de zona abierta.



#### **Nota**

Debe configurar el tiempo de intervalo de filtrado de eventos para las llamadas telefónicas.

---

#### **Tapa de periféricos abierta**

El dispositivo enviará notificaciones cuando se active o restablezca la tapa abierta de cualquier periférico.

#### **Tapa del panel abierta**

El dispositivo enviará notificaciones cuando la tapa del panel de control se abra o se restablezca.

#### **Alarma de pánico**

El dispositivo enviará notificaciones cuando se active o restablezca la alarma de pánico por zonas, teclados o llaveros.

#### **alarma medica**

El dispositivo enviará notificaciones cuando se active la alarma médica.

#### **Alarma de incendios**

El dispositivo enviará notificaciones cuando se active la alarma de incendio.

#### **alarma de gas**

El dispositivo enviará notificaciones cuando se active la alarma de gas.

#### **Estado del panel**

El dispositivo enviará notificaciones cuando cambie el estado del sistema del panel de control.

#### **Estado de zona**

El dispositivo enviará notificaciones cuando se cambie el estado de la zona.

#### **Estado de los periféricos**

El dispositivo enviará notificaciones cuando se cambie el estado de cualquier periférico.

#### **Operación del panel**

El dispositivo enviará notificaciones cuando el usuario opere el AX PRO.

#### **Evento de alarma inteligente**

El dispositivo enviará notificaciones cuando se active la alarma en las cámaras térmicas.

#### **Establecer alarma de emergencia (en la aplicación)**

Los eventos seleccionados serán notificados como emergencia mientras que el evento no seleccionado no se mostrará en la página.

5. Toque **Llamada telefónica y SMS**.

6. Toque **+ Agregar número de teléfono** para ingresar el número de teléfono.

7. Toque el número de teléfono agregado para habilitar **Llamadas telefónicas y SMS** según sus necesidades.

(Para llamadas telefónicas) Establecer números de llamadas.

(Para SMS) Establecer permiso de armado, permiso de desarmado y permiso de borrado de alarma para áreas

#### **Mensaje común**

Puede ingresar el contenido del mensaje. Cuando se active la alarma, su contenido personalizado se agregará al comienzo del mensaje enviado por el sistema.

#### **Voz común**

Puede importar un nuevo audio. Cuando se active la alarma, su voz personalizada se agregará al comienzo del contenido del teléfono marcado por el sistema. También puede tocar **Borrar** para eliminar audios



#### **Nota**

Solo se admite el formato WAV, hasta 512 KB y 15 s.

---

10. Revisa las notificaciones.

### **Centro de recepción de alarmas (CRA)**

Puede configurar los parámetros del centro de recepción de alarmas y todas las alarmas se enviarán al centro de alarmas configurado.

#### **Pasos**

1. En el sitio, toque **AX PRO** y luego inicie sesión en el dispositivo (si es necesario).
2. Toque **Parámetros de comunicación y Centro de recepción de alarmas (CRA)** para ingresar a la página.
3. Seleccione un CRA y actívelo.

#### **Tipo de protocolo**

Seleccione el Tipo de protocolo como ADM-CID, ISUP, SIA-DCS, \*SIA-DCS, \*ADM-CID, CSV-IP, Módulo FSK o Módulo RDC para configurar el modo de carga.

#### **Verificación de intrusos como servicio**

Cuando el panel de control cargue la información de la alarma, devolverá la dirección de la imagen y el video para que usted los vea.

#### **Compañías**

Seleccione la empresa de soporte como Ninguna, Hungría-Empresa receptora de múltiples alarmas o Francés

Empresa Receptora de Alarmas.

#### **Tipo de dirección**

Seleccione el Tipo de dirección como Dirección IP y Nombre de dominio. Ingrese la dirección del servidor/nombre de dominio, número de puerto y código de cuenta.

#### **Modo de transmisión**

Seleccione el Modo de transmisión como TCP o UDP. UDP es recomendado por el estándar SIA DC-09.

#### **Período de tiempo de espera de reintento**

Después del tiempo seleccionado, el sistema volverá a intentar transmitir.

#### **intentos**

Establezca el número de reintentos.

#### **Opción de sondeo**

Establezca la tasa de sondeo con un rango de 10 a 3888000 segundos. El sistema informará la falla si el tiempo supera el límite. El estado del dispositivo se mostrará como fuera de línea.

#### **Prueba periódica**

Después de habilitarlo, puede configurar el intervalo de tiempo, configurando la frecuencia con la que se envía un evento de prueba al CRA para garantizar la conexión.

#### **GMT**

Habilite la hora del meridiano de Greenwich.

### **Configuración del servicio en la nube**

#### **Pasos**

1. En el sitio, toque AX PRO y luego inicie sesión en el dispositivo (si es necesario).
2. Toque y **Parámetros de comunicación** **Configuración del servicio en la nube** para ingresar a la página.
3. Seleccione el **modo de comunicación**.

#### **Red alámbrica y prioridad Wi-Fi**

El orden de prioridad de conexión de mayor a menor es: red cableada, Wi-Fi, red de datos móviles.

#### **Con cable y Wi-Fi**

El sistema seleccionará primero la red cableada. Si no se detecta una red cableada, seleccionará la red Wi-Fi.

#### **Red de datos móviles**

El sistema seleccionará solo la red de datos móviles.

4. Habilite **la prueba periódica**. Ingrese el intervalo de prueba periódica.
5. Toque **Guardar**.

#### Notificación por correo electrónico

##### Pasos

1. En el sitio, toque AX PRO y luego inicie sesión en el dispositivo (si es necesario).
2. Toque **Parámetros de comunicación** y **Notificación por correo electrónico** para ingresar a la página.
3. Habilitar **correo electrónico 1**.
4. Introduzca el nombre del remitente, la dirección de correo electrónico del remitente, la dirección del servidor SMTP, el puerto SMTP, el nombre de usuario y clave.



##### Nota

Se recomienda utilizar Gmail y Hotmail para el envío de correos.

Solo si la zona está vinculada con una cámara de red, el correo electrónico de alarma se adjuntará con el video de alarma.

---

5. Seleccione el tipo de cifrado como **Ninguno, SSL o TLS**.
6. Habilite **la autenticación del servidor**.
7. Ingrese el nombre del destinatario y la dirección de correo electrónico del destinatario. Toque **Probar la dirección de correo electrónico del receptor** para probar si la dirección de correo electrónico es correcta.
8. Toque **Guardar**.
9. Opcional: configure el **correo electrónico 2** en el mismo orden. Puede elegir si configurar el correo electrónico 2 como buzón de respaldo.



##### Nota

Las reseñas de videos y fotos se enviarán a ambos buzones. Si el Correo electrónico 2 está configurado como un buzón de respaldo, el sistema enviará correos electrónicos al Correo electrónico 2 solo si el Correo electrónico 1 no se recibe.

---

#### Configuración FTP

##### Pasos

1. En el sitio, toque AX PRO y luego inicie sesión en el dispositivo (si es necesario).
2. Toque **Parámetros de comunicación** y **Configuración de FTP** para ingresar a la página.
3. Seleccione **FTP preferido** o **FTP alternativo** y habilite FTP.
4. Configurar los parámetros de FTP

##### Tipo FTP

Configure el tipo de FTP como preferido o alternativo.

##### Tipo de protocolo

FTP y SFTP son seleccionables. La carga de archivos se cifra mediante el protocolo SFTP.

#### **Dirección y puerto del servidor**

La dirección del servidor FTP y el puerto correspondiente.

#### **Nombre de usuario y contraseña/Anonimato**

El usuario de FTP debe tener permiso para cargar imágenes. Si el servidor FTP admite la carga de imágenes por parte de usuarios anónimos, puede habilitar Anónimo para ocultar la información de su dispositivo durante la carga.

#### **Estructura del directorio**

La ruta de guardado de las instantáneas en el servidor FTP.

4. Toque **Guardar**.

## **NAT**

Universal Plug and Play (UPnP™) es una arquitectura de red que proporciona compatibilidad entre equipos de red, software y otros dispositivos de hardware. El protocolo UPnP permite que los dispositivos se conecten sin problemas y simplifica la implementación de redes en entornos domésticos y corporativos.

Habilite la función UPnP, y no necesita configurar la asignación de puertos para cada puerto, y el dispositivo está conectado a la red de área amplia a través del enrutador.

#### **Pasos**

1. En el sitio, toque AX PRO y luego inicie sesión en el dispositivo (si es necesario).
2. Toque **Parámetros de comunicación** y **NAT** para ingresar a la página.
3. Arrastre el control deslizante para habilitar UPnP.
4. **Opcional:** Seleccione el tipo de asignación como **Manual** para establecer el puerto HTTP y el puerto de servicio.
5. Haga clic en **Guardar** para completar la configuración .

#### **Servicio de intercomunicación**

Puede configurar el servicio de intercomunicación para una sirena de intercomunicación.

#### **Antes de que empieces**

Primero debe registrar un zumbador de intercomunicador.

Solo se puede configurar una sirena como sirena de intercomunicación.

#### **Pasos**

1. Toque **Comunicación** y **Servicio de intercomunicador** para ingresar a la página.
2. Deslice para habilitar la función.
3. Configure el tipo de intercomunicador.

#### **SORBO**

El panel de control utilizará el servidor ARC y SIP.

#### **Receptor IP Pro**

El panel de control usará el servicio en la nube del usuario.

4. Seleccione una sonda y toque **Guardar**.

## Mantenimiento del dispositivo

### Prueba de paseo

#### Pasos

1. En el sitio, toque AX PRO y luego inicie sesión en el dispositivo (si es necesario).
2. Toque  **Mantenimiento** y **Mantenimiento del dispositivo** para ingresar a la página de mantenimiento.
3. Toque **Prueba** y toque **Iniciar prueba de paseo** para comprobar si el dispositivo funciona correctamente o no.

#### Mantenimiento

1. En el sitio, toque AX PRO y luego inicie sesión en el dispositivo (si es necesario).
2. Toque  **Mantenimiento** y **Mantenimiento**.

##### Alarma de manipulación en el inicio de sesión de HPC

Si está habilitado, se activará una alarma cuando el dispositivo sea manipulado después de iniciar sesión en HPC.

#### Reiniciar dispositivo

El AX PRO se reiniciará.

##### Tronco

Ver registros de dispositivos.

### Actualización de dispositivo

#### Pasos

1. En el sitio, toque AX PRO y luego inicie sesión en el dispositivo (si es necesario).
2. Toque  **Mantenimiento** y **Actualización de dispositivo** para actualizar el panel de control, o toque  **Mantenimiento** y **Actualización** de detectores y periféricos para actualizar detectores y periféricos.

### Recopilación de registros remotos

#### Pasos

1. En el sitio, toque AX PRO y luego inicie sesión en el dispositivo (si es necesario).
2. Toque  **Mantenimiento** y **Recopilación de registros remotos** para habilitar la función.

Recopilación de registros remotos es para obtener registros relacionados con el dispositivo. Cuando esto esté habilitado, nuestro soporte técnico podrá recopilar registros relacionados con el dispositivo de forma remota y cargarlos en nuestro servidor para solucionar problemas. Puede establecer el período de validez de acuerdo con las necesidades reales. Esta función se desactivará después del período de validez establecido.

## 5.1.2 Usar el portal Hik-ProConnect

Para el panel de control de seguridad AX PRO, puede realizar operaciones que incluyen armar/desarmar área,

silenciar alarma, anular zona, etc., y configurar remotamente el panel de control en el Portal. También puede solicitar un PIN (requerido para actualizar el firmware de AX PRO) y cambiar el idioma de AX PRO.

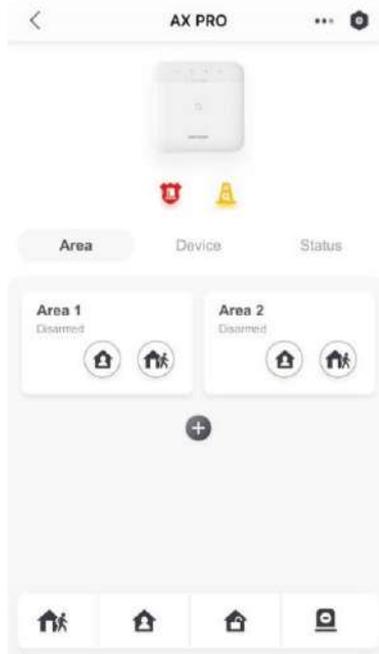
Haga clic en  **Sitio** para ingresar a la página de lista de sitios y luego haga clic en el nombre de un sitio para ingresar a la página de detalles del sitio.

## Operar remotamente AX PRO

Haga clic en AX PRO para abrir el panel de operaciones. Y puede realizar las siguientes operaciones.

**Tabla 4-3 Descripción de la operación**

Operación	Descripción
Armar En Casa un Área Específica	Seleccione la pestaña <b>Área</b> y luego haga clic en <b>Armado En Casa</b> para armar en casa el área.
Armar Ausente un Área Específica	Seleccione la pestaña <b>Área</b> y luego haga clic en <b>Armado Ausente</b> .
Desarmar un área específica	Seleccione la pestaña <b>Área</b> y luego haga clic en <b>Desarmar</b> .
Armado En Casa Múltiples Áreas	Seleccione la pestaña <b>Área</b> y, a continuación, seleccione áreas y haga clic en  .
Armar Ausente Múltiples Áreas	Seleccione la pestaña <b>Área</b> y, a continuación, seleccione áreas y haga clic en  .
Desarmar áreas múltiples	Seleccione la pestaña <b>Área</b> y, a continuación, seleccione áreas y haga clic en  .
Silenciar alarmas de múltiples Áreas	Seleccione la pestaña <b>Área</b> y, a continuación, seleccione áreas y haga clic en  .
Filtrar dispositivo periférico por Área	Seleccione la pestaña <b>Dispositivo</b> y luego haga clic  y seleccione un área para en mostrar solo los dispositivos periféricos vinculados al área seleccionada, o seleccione <b>Todo</b> para mostrar todos los dispositivos periféricos vinculados a todos los áreas
Relé de control	Seleccione la pestaña <b>Dispositivo</b> , y luego seleccione un expansor de salida inalámbrica para mostrar las sirenas vinculadas a él, y luego seleccione sirena(s) para habilitarlas/deshabilitarlas.
Zona de anulación	Seleccione la pestaña <b>Dispositivo</b> y, a continuación, seleccione una zona (es decir, un detector) y encienda el interruptor <b>Anular</b> para anular la zona.



### Configurar AX PRO de forma remota

Puedes hacer clic  para ingresar a la página web del panel de control de seguridad para configurar el dispositivo.

---

#### Nota

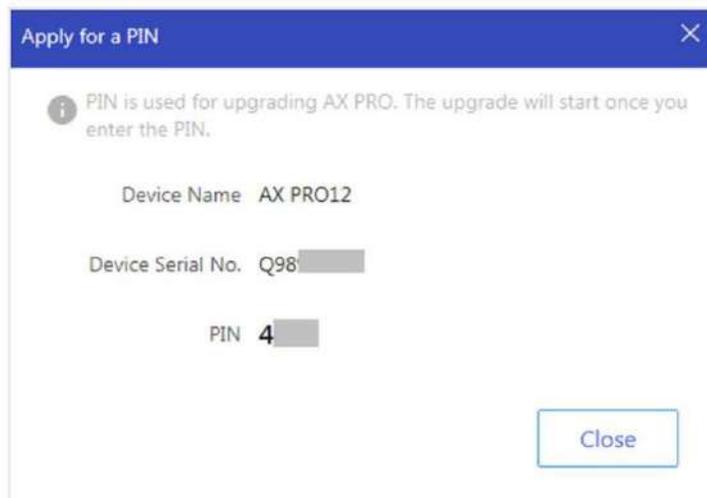
Para obtener detalles sobre la configuración del panel de control de seguridad, consulte el manual de usuario del dispositivo.

---

### Solicitar un PIN

Puedes hacer clic  y para  abrir la ventana Solicitar un PIN y, a continuación, aparecerá el código PIN.

desplegado.



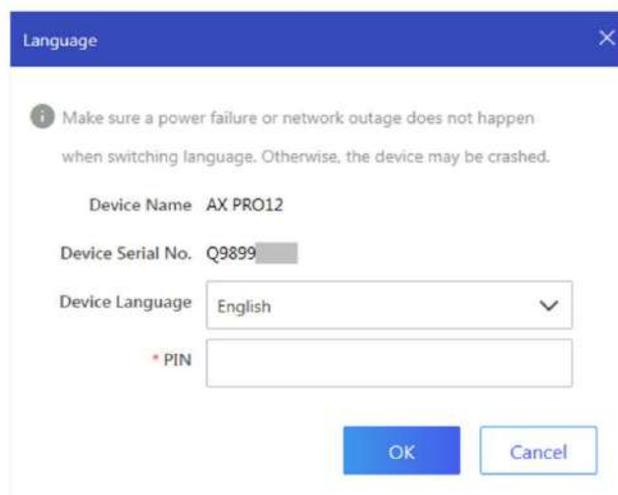
## Cambiar idioma



Nota

Debería haber solicitado un PIN.

Puede hacer clic  y  para abrir la ventana Idioma, y luego configure el idioma del dispositivo y en introducir el PIN.

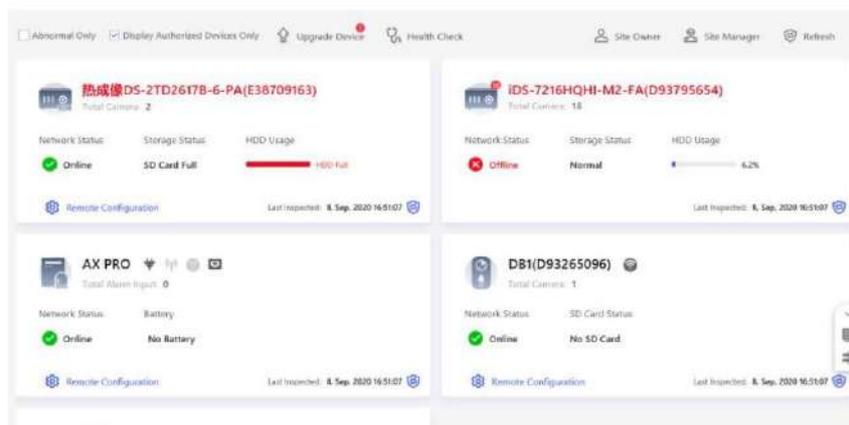


## Vigilancia de la salud

1. Ingrese al sitio web del portal Hik-ProConnect y haga clic en **Monitoreo de salud** y **Estado de salud** para ingresar .

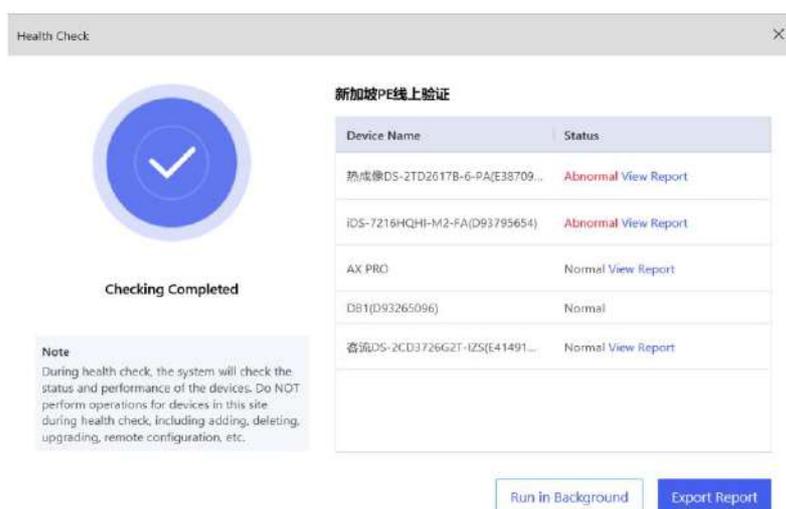
la página.

2. Seleccione un sitio.



3. Haga clic en **Comprobación de estado** y haga clic en **Comprobar ahora**.

Cuando se completa la verificación, puede ver el estado y los informes de los dispositivos. También puede exportar el informe.



4. Haga clic en  para obtener el último estado del dispositivo.

## 5.2 Configuración con Hik-Connect

El operador puede usar Hik-Connect para controlar el dispositivo, como la operación general de armado/desarmado y la gestión de usuarios, etc.

## Descargue e inicie sesión en el cliente móvil

Descargue el cliente móvil Hik-Connect e inicie sesión en el cliente antes de operar el AX PRO.

### Pasos

1. Descargue el cliente móvil Hik-Connect.
2. Opcional: Registre una nueva cuenta si es la primera vez que usa el cliente móvil Hik-Connect.



Para obtener más información, consulte *el Manual del usuario de Hik-Connect Mobile Client*.

---

3. Ejecute e inicie sesión en el cliente.

## Agregar AX PRO al cliente móvil

Agregue un AX PRO al cliente móvil antes de otras operaciones.

### Pasos

1. Encienda el AX PRO.
  2. Seleccione el tipo de adición.
- Toque **+** y **Escanear código QR** para ingresar a la página Escanear código QR. Escanee el código QR en el AXE PRO.



Normalmente, el código QR está impreso en la etiqueta pegada en la tapa trasera del AXE PRO.

---

Toque **+** y **Adición manual** para ingresar a la página Agregar dispositivo. Ingrese el número de serie del dispositivo con el tipo de adición de dominio Hik Connect.

3. Toque  para buscar el dispositivo.
4. Toque **Agregar** en la página de resultados.
5. Ingrese el código de verificación y toque **Aceptar**.
6. Después de completar la adición, ingrese el alias del dispositivo y toque **Guardar**.
7. Opcional: toque y **Eliminar dispositivo** para eliminar el dispositivo.
8. Opcional: toca y para  el nombre del dispositivo.

## Agregar periférico al AX PRO

Agregue periférico al AX PRO.

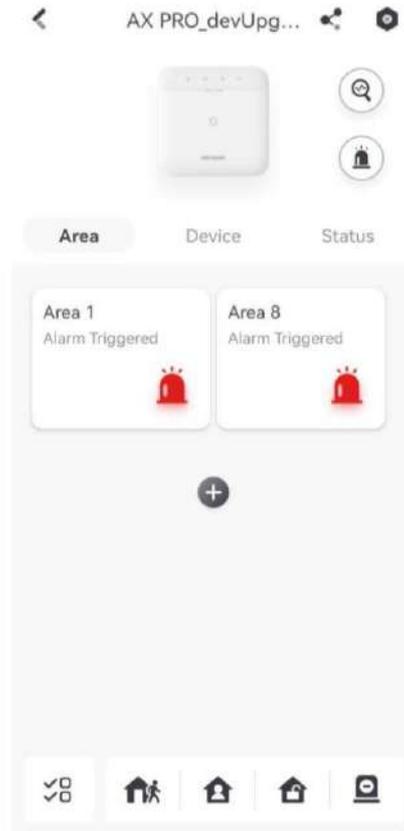
### Pasos

1. Seleccione un dispositivo de control (AX PRO).
2. Toque **+**
  - Toque **Escanear código QR** para ingresar a la página Escanear código QR. Escanea el código QR en el periférico.
  - Tocar  para entrar en la página Entrada manual. Ingrese el número de serie del dispositivo y seleccione el dispositivo escriba para agregar el dispositivo.

### Página principal

Puede ver fallas, armar y desarmar áreas, ver el estado del dispositivo, etc.

En la página de la lista de dispositivos, toque el AX PRO y luego inicie sesión en el dispositivo (si es necesario) para ingresar el página.



### Activar la alarma

Tocar  para seleccionar Alarma de **pánico audible** o Alarma de **pánico silenciosa**.

### Ver fallas

Tocar  para ver fallas.

### Gerencia de Área

Toque **+** para agregar un área.

Toque **Área** para ingresar a la página de administración del área. Se refiere a [área de administración](#) para detalles.

### Armar/Desarmar el Área

Arma o desarma el área manualmente como desees.

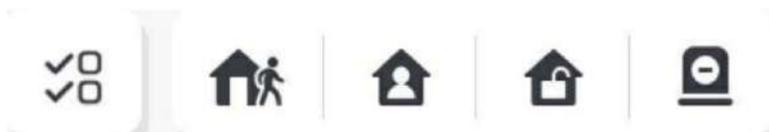
En la página de la lista de dispositivos, toque el AX PRO y luego inicie sesión en el dispositivo (si es necesario) para ingresar al Área página.

### Operaciones para una sola área



- **Armado Ausente:** Pulse  para armar lejos una sola área. Cuando todas las personas en el área de detección salir, active el modo Ausente para armar todas las zonas en el área después del tiempo de permanencia definido.
- **Armado En Casa:** Pulse  para armar una sola área. Cuando todas las personas permanezcan dentro del área de detección, active el modo Permanecer para armar todo el conjunto de detección de robo perimetral en todas las zonas de todos. áreas

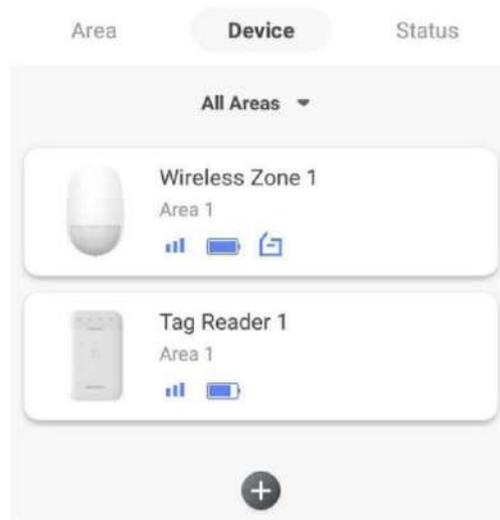
### Operaciones para áreas múltiples



- **Seleccionar áreas:** toque  para seleccionar las áreas que desea operar. Si no selecciona áreas, siguiendo las operaciones surtirán efecto para todas las áreas.
- **Armado Ausente:** Pulse  para armar áreas seleccionadas. Cuando todas las personas en el área de detección se vayan, active el modo Ausente para armar todas las zonas en todas las áreas después del tiempo de permanencia definido.
- **Armado En Casa:** Pulse  Para quedarte armar todas las áreas. Cuando las personas permanezcan dentro del área de detección, active el modo Permanecer para armar toda la detección de robo perimetral (como detector perimetral, contactos magnéticos, detector de cortina en el balcón) configurada en todas las zonas de todas las áreas. Mientras tanto, los detectores dentro del área de detección se omiten (como los detectores PIR). Las personas pueden moverse dentro del área y la alarma no se activará.
- **Desarmar:** toque  para desarmar todas las áreas. En el modo Desarmado, todas las zonas de todas las áreas no activar la alarma, sin importar si los eventos de alarma ocurren o no.
- **Alarma silenciosa:** toque  hasta alarmas silenciosas para todas las áreas.

## Gestión de zonas

1. Toque **Dispositivo** para ver las zonas vinculadas.



2. Toque + para agregar una nueva zona.
3. Toque una zona para ingresar a la página de administración. Puede ver el estado del dispositivo (por ejemplo, temperatura, estado de la batería, fuerza única, etc.). en la esquina
4. Toque  superior derecha para ingresar a la página de configuración de zona.
5. Seleccione un tipo de zona.

Puede ver los tipos de zona configurables para varios detectores a través de **1. Tipos de zona de detector.**

#### **Zona instantánea**

Este tipo de zona activará inmediatamente un evento de alarma cuando esté armado.

#### **Zona de retraso**

**-Retraso de salida:** El retraso de salida le proporciona tiempo para salir de la zona sin alarma.

El armado con fallas está habilitado: primero debe confirmar las fallas y luego la zona está en proceso de armado. Si la zona de retardo se activa dentro del tiempo de retardo de salida pero se restablece antes de que finalice el tiempo, la alarma no se activará y la zona se armará.

El armado con fallas está deshabilitado: Armado inmediato. Si la zona de retardo se activa dentro del tiempo de retardo de salida pero se restablece antes de que finalice el tiempo, la alarma no se activará.

**-Retraso de entrada:** el retraso de entrada le proporciona tiempo para ingresar a la zona para desarmar el sistema sin alarma.

Después de la activación, si la zona no se desarma o silencia antes de que finalice el tiempo de retardo de entrada, la zona emitirá una alarma.

**-Tiempo de Retardo de Armado Parcial:** El armado Parcial usa el Tiempo de Retardo de Armado Parcial para la cuenta regresiva.

El sistema da un tiempo de retardo de entrada/salida cuando se arma o se vuelve a entrar. Por lo general, se utiliza en la ruta de entrada/salida (p. ej., puerta principal/entrada principal), que es una ruta clave para armar/desarmar a través del teclado operativo para los usuarios.



**Nota**

• Puede establecer 2 duraciones de tiempo diferentes en **Opciones del sistema** y **Programación y temporizador**.

• Asegúrese de que el temporizador no supere los 45 segundos para cumplir con EN50131-1.

• Puede configurar el tiempo de retardo de armado en casa para la zona de retardo.

---

**Zona de pánico**

Zona activa de 24 horas, esté armada o no. Informe de alarma de pánico después de la activación. Suele utilizarse en los locales equipados con botón de pánico, detector de humo y detector de rotura de cristales.

**alarma medica**

Zona activa de 24 horas, esté armada o no. Informe de alarma médica después de la activación.

**Zona de fuego**

Zona activa de 24 horas, esté armada o no. Informe de alarma de incendio después de la activación.

**Zona de Gas**

Zona activa de 24 horas, esté armada o no. Informe de alarma de gas después de la activación.

**Zona de seguimiento**

La zona actúa como zona retardada cuando detecta un evento de activación durante el retardo de entrada del sistema, mientras que actúa como zona instantánea en caso contrario.

**Zona de interruptor de llave**

**-Por tiempo de disparo:** cambie el estado de armado y desarmado después de cada disparo. Por ejemplo, en el estado desarmado, si la zona se activa, el área vinculada se armará. Active la zona nuevamente y el área se desarmará.

**-Por estado de zona:** debe elegir armar o desarmar el área vinculada después de que se active la zona.

En el caso de la alarma de manipulación, la operación de armado y desarmado no se activará.

**Zona deshabilitada**

Zona deshabilitada ignorando cualquier evento de alarma. Por lo general, se utiliza para desactivar detectores defectuosos.

**Zona 24 horas**

La zona se activa todo el tiempo con salida de sonido/luz cuando ocurre la alarma, ya sea que esté armada o no. Por lo general, se usa en áreas con riesgo de incendio equipadas con detectores de humo y sensores de temperatura.

**Zona de tiempo de espera**

La zona se activa todo el tiempo. Cuando esta zona se haya activado o restaurado y exceda el tiempo establecido, se generará una alarma.

Se puede utilizar en lugares equipados con contactos magnéticos que requieren acceso pero solo por un período corto (por ejemplo, la puerta de la caja de la boca de incendios u otra puerta de la caja de seguridad externa).

**-Alarma de zona no activada:** Si la zona no se activa durante el tiempo establecido, se activará la alarma.

**-Alarma en Zona Activada:** Si la zona se activa durante el tiempo establecido, emitirá una alarma.

-Período de tiempo de reintento: establezca el período de tiempo de espera.

6. Habilite **Zona cruzada, Alarma silenciosa, etc.** según sus necesidades reales.



**Nota**

Algunas zonas no admiten la función. Consulte la zona real para configurar la función.

---

### **Modo armado**

Si la zona es una zona pública (la zona pertenece a más de un área), puede configurar el modo de armado.

**Y:** Cuando todas las áreas enlazadas estén armadas, la zona se armará. Cuando cualquiera de las áreas vinculadas se desarma, la zona se desarmará.

**O:** Cuando cualquiera de las áreas enlazadas esté armada, la zona se armará. Cuando todas las áreas vinculadas estén desarmadas, la zona se desarmará. Cuando la zona está en alarma, las áreas desarmadas vinculadas con la zona no se pueden armar.

### **Bypass de Armado Parcial**

La zona se anulará automáticamente en el armado En Casa.

### **Zona cruzada**

**PD6662 no está habilitado:** debe configurar el intervalo de tiempo combinado.

Cuando se activa la primera zona, el sistema comenzará a cronometrar después de que se restablezca la zona. Si la segunda zona se activa dentro del tiempo establecido, ambas zonas darán alarmas. De lo contrario, no se activará ninguna alarma.

Si la primera zona no se restablece, ambas zonas darán alarmas cuando se active la segunda zona, independientemente de si ha transcurrido el tiempo establecido.

**PD6662 está habilitado:** debe configurar el intervalo de tiempo combinado.

La primera zona dará una alarma cuando se active. Si la primera zona no se restablece y la segunda zona se activa, el sistema informará la confirmación de la alarma.

Si se restablece la primera zona, el sistema comenzará a cronometrar. Si la segunda zona se activa dentro del tiempo establecido, el sistema informará la confirmación de la alarma.

Si se restablece la primera zona, el sistema comenzará a cronometrar. Si la segunda zona no se activa dentro del tiempo establecido, no se reportará ninguna información.

### **Prohibir anular al armar**

Una vez habilitado, no puede anular zonas al armar.

### **Repicar**

Habilitar el timbre. Normalmente se utiliza para detectores magnéticos de puertas.

### **alarma silenciosa**

Después de habilitarse, cuando se activa una alarma, solo se cargará el informe y no se emitirá ningún sonido.

### **Doble golpe**

Después de habilitarlo, se puede configurar el intervalo de tiempo. Si el mismo detector se activa dos veces o

continuamente en un período de tiempo, la alarma se activará.

#### **Tiempo de retardo de sirena**

La sirena se activará inmediatamente (0s) o después del tiempo establecido.

#### **Salida de la puerta final**

Solo los contactos magnéticos tienen esta opción.

Después de habilitar, cuando el usuario use teclados o lectores de etiquetas para armar:

-Armar con fallas está habilitado: Durante la cuenta regresiva de armado, si el contacto magnético se activa y luego se restablece, el proceso de armado terminará inmediatamente después.

restaurando, y el armado está completo.

- Armar con fallas está deshabilitado: si el contacto magnético se activa y luego se restablece, el área enlazada arma inmediatamente la zona retardada.

#### **Activaciones de Límite Swinger (Zona Cableada)**

Cuando el número de veces que se activa el detector de infrarrojos supera el valor establecido, la alarma ya no se activará. (Excepto alarmas antienmascaramiento).

#### **Zona Dual (Zona Cableada)**

Después de habilitado, cuando el transmisor múltiple detecta que todo el circuito de zona de la zona local y la zona extendida está en circuito abierto, ambas zonas activan alarmas de tapa abierta.

7. Si es necesario, vincular una PIRCAM o una cámara para la zona.

8. Haga clic en **Aceptar**.

#### **Ver el estado de**

Toque **Estado** para ver el estado de los periféricos.

#### **Zona de anulación**

Cuando el área está armada, puede anular una zona en particular como desee.

#### **Antes de que empieces**

Vincule un detector a la zona.

#### **Pasos**

1. En la página de la lista de dispositivos, toque AX PRO y luego inicie sesión en el dispositivo (si es necesario) para ingresar el página de área.
2. Toque **Dispositivo**.
3. Toque una zona en la pestaña Dispositivo.
4. Toque para ingresar a la página Configuración.
5. Habilite **Anular** y la zona estará en el estado de anulación.

#### **Estado de omisión**

El detector de la zona no detecta nada y no recibirá ninguna alarma del zona.

## Gestión de usuarios

El administrador y los instaladores pueden gestionar usuarios. Si es el administrador, puede agregar, editar y eliminar usuarios, y asignar diferentes permisos a los usuarios recién agregados.

### Pasos



Hay cuatro tipos de usuarios para el AX PRO, incluido el administrador (o propietario), el operador y el instalador (o instalador). Los diferentes tipos de usuarios tienen diferentes permisos para acceder a la funcionalidad de AX PRO.

---

1. En la página de la lista de dispositivos, toque el AX PRO y luego inicie sesión en el dispositivo (si es necesario) para ingresar el Página AX PRO.
2. Toque para ingresar a la página del destinatario.
3. Seleccione un usuario para invitar.
  - Escanea el código QR para invitar a un usuario.
  - Ingrese la dirección de correo electrónico/número de teléfono móvil para invitar a un usuario.
  - Seleccione un usuario de la lista.
4. Pulse en **Siguiente** para invitar al usuario.



El destinatario debe aceptar la invitación.

---

5. Toque y **Administración de usuarios** y **Usuario**.
6. Toque un usuario para ingresar a la página de información del usuario.
7. Opcional: Realice las siguientes operaciones si es necesario.

#### Permiso de usuario

Puede tocar el usuario de destino en la lista de usuarios y luego tocar los permisos autorizados para el usuario de destino.



Solo el administrador puede hacer tal operación.

---

#### Establecer áreas vinculadas

Si el usuario objetivo es un operador, toque el usuario objetivo en la lista de usuarios y luego toque **Áreas vinculadas** para establecer el área vinculada al usuario objetivo.



Solo el administrador puede hacer tal operación.

---

#### Cambiar teclado Clave

Si el usuario de destino es un administrador, un instalador o un operador, puede tocar el usuario de destino en la lista de usuarios y luego tocar **Cambiar teclado**

**Contraseña** para establecer la contraseña del teclado para el usuario de destino.

---

 **Nota**

La contraseña (código PIN) puede tener de 4 a 6 dígitos. No se permite ningún número, con diferencias de 10.000 a 100.000, y sin límite de combinación de dígitos.

Después de agregar un teclado, puede agregar el código PIN (contraseña del teclado) en el menú de usuario. Cuando haga clic en el cuadro de entrada, habrá una indicación que muestra que se permiten de 4 a 6 números. Esto es lo mismo para cada usuario

---

**Cambiar coacción  
Clave**

Si el usuario de destino es un administrador o un operador, puede tocar el usuario de destino en la lista de usuarios y luego tocar **Cambiar contraseña de coacción** para establecer la contraseña de coacción para el usuario de destino.

---

 **Nota**

Si está bajo coacción, puede ingresar el código de coacción en el teclado para armar y desarmar áreas y cargar una alarma de coacción.

---

**Control de automatización** Un administrador, un instalador o un operador pueden controlar el relé módulo, interruptor de pared y enchufe inteligente.

---

 **Nota**

- Los elementos de configuración y los permisos de usuario variarán según el tipo de usuario.
  - Puede ver la Tarjeta/Etiqueta vinculada y el Llavero inalámbrico del usuario, pero no tiene permiso para configurarlos.
- 

8. Opcional: (Solo para el administrador) Haga clic en + para agregar un usuario.

## Gestión de tarjetas/etiquetas

Después de agregar tarjetas/etiquetas al AX PRO inalámbrico, puede deslizar la tarjeta/etiqueta para armar o desarmar todos los detectores agregados a áreas específicas del AX PRO y silenciar las alarmas.

---

 **Nota**

El ID/PIN de la etiqueta es un número entero de 32 bits y la variante podría ser 42949672956.

---

### Pasos

1. Ingrese al sitio, toque el AXE PRO y luego inicie sesión en el dispositivo (si es necesario) para ingresar a la página.
2. Toque  **Administración de usuarios** y **Tarjeta/Etiqueta** para ingresar a la página Tarjeta/Etiqueta.

3. Toque + para agregar una etiqueta.
4. Cuando escuche el mensaje de voz "Swipe Tag", debe presentar la etiqueta en la etiqueta AXE PRO  
área de presentación. •  
Al escuchar un pitido, se reconoce la etiqueta. • La etiqueta se mostrará en la página  
de etiquetas.
5. Opcional: toque una etiqueta para ingresar a la página de configuración.
6. Toque **Editar icono** para editar el nombre de la etiqueta.



• Si inicia sesión como instalador, omite este paso. La edición del nombre de la etiqueta solo está disponible para el administrador. • El nombre debe contener de 1 a 32 caracteres.

---

7. Deslice **Activar etiqueta**.
8. Seleccione un usuario vinculado.
9. Seleccione el tipo de etiqueta



Diferentes usuarios vinculados tienen diferentes permisos de etiqueta.

---

#### Etiqueta de operación

Puede deslizar la etiqueta para armar o desarmar.

#### Etiqueta de

**patrulla** Cuando pase la etiqueta, el sistema cargará un registro.

10. Opcional: toque **Eliminar** para eliminar la etiqueta.

## Información del dispositivo

Puede cambiar el idioma y seleccionar la zona horaria.

#### Pasos

1. En la página de la lista de dispositivos, toque AX PRO y luego inicie sesión en el dispositivo (si es necesario) para ingresar el  
página.
2. Toque **Sistema y Configuración** para ingresar a la página.
3. Seleccione el idioma y la zona horaria del dispositivo.
4. Habilite DST según sus necesidades.

horario de verano

El horario de verano (también llamado horario de verano) es la práctica de adelantar los relojes durante los meses más claros para que las noches tengan más luz del día y las mañanas menos.

## Gestión del sistema

### Pasos

1. En la página de la lista de dispositivos, toque AX PRO y luego inicie sesión en el dispositivo (si es necesario) para ingresar el página.
2. Toque **Sistema** y **Opciones del sistema** y **Administración** del sistema para ingresar a la página.

### Armado automático forzado

Después de habilitarse, cuando comienza el armado automático temporizado, si hay fallas activas en una zona, la zona se anulará automáticamente.

Puede ir a **Sistema** y **Opciones** de sistema y **Horario y hora** para configurar el horario de armado/desarmado automático y las áreas vinculadas.



#### Nota

Debe desactivar Armar con fallas en la página Opciones de armar. O la función de Armado automático forzado/Armado forzado no puede ser válida.

---

### Armado Forzado

Después de habilitarse, cuando comienza el armado manual, si hay fallas activas en una zona, la zona se omitirá automáticamente.

Puede usar llaveros, etiquetas y teclados para armar zonas o armar zonas manualmente en la aplicación. Se pueden seleccionar áreas individuales, múltiples o todas para armar.



#### Nota

Debe desactivar Armar con fallas en la página Opciones de armar. O la función de Armado automático forzado/Armado forzado no puede ser válida.

---

### Informe de estado del sistema

Si la opción está habilitada, el dispositivo cargará el informe a la nube (para APP) y ARC automáticamente cuando se cambie el estado de AX PRO.

### Mensaje de voz

Si la opción está habilitada, el AX PRO habilitará el mensaje de voz.

-Indicaciones de falla al armar: Indicaciones de voz de fallas al armar.

-Indicaciones de falla cuando está armado: Indicaciones de voz de fallas cuando el sistema está armado.

-Avisos de fallas al desarmar: aviso de voz de fallas al desarmar

-Indicaciones de falla cuando está desarmado: Indicaciones de voz de fallas cuando el sistema está desarmado.

-Indicaciones de voz en alarma: Indicaciones de voz de fallas cuando se activa una alarma.

### Volumen del sistema

El rango de volumen del sistema disponible es de 0 a 10.

### Alarma audible de sabotaje

Mientras está habilitado, el sistema alertará con un zumbador para la alarma de manipulación. Independientemente de si

está habilitado o no, la alarma de manipulación normalmente se enviará a la nube (para APP) y ARC.

#### **Botón de bloqueo del panel**

Todas las funciones de AX PRO se congelarán después de que se habilite. Esta función solo puede ser habilitada por usuarios con permiso de instalador.

#### **Duración de la alarma**

Establezca un mensaje de voz de alarma vinculado que dure el tiempo.

#### **Pérdida de supervisión inalámbrica**

Los detectores y periféricos cuyos tiempos de pérdida de latido superen el valor establecido se mostrarán como fuera de línea.

#### **Anular al rearmar**

Mientras está habilitado, después de anular el detector, si se restauran sus fallas y se arma el área enlazada, el detector se armará automáticamente.

#### **El LED de falla permanece encendido cuando**

está armado Cuando el sistema está armado, el indicador de falla siempre está encendido.

#### **Armar LED permanecer encendido**

El LED de brazo está siempre encendido.

#### **Indicador Hik-Connect**

Habilite el indicador HC.

#### **Restauración del detector de movimiento**

Los detectores de movimiento incluyen todos los detectores PIR.

-Desactivar: Sin restauración automática.

-Inmediatamente después de la alarma: los detectores de movimiento se restauran automáticamente inmediatamente después de la alarma e informan a Cloud (para APP) y ARC.

-Después de desarmar: los detectores de movimiento se restauran automáticamente después de desarmar e informan a la nube (para APP) y ARC

#### **Ajustes de sensibilidad de interferencia**

El dispositivo detectará la interferencia de RF y enviará mensajes cuando la interferencia de RF interfiera con la comunicación. Puede ajustar la sensibilidad de detección.

#### **Modo de ahorro de energía**

Mientras está habilitado, la fuente de alimentación principal está apagada, Wi-Fi entra en bajo consumo de energía, 4G se cierra, falla la lectura de etiquetas, LED apagado y aviso de voz apagado.

#### **Restablecimiento del detector de humo**

Solo para la zona cableada de la central M2H, que está configurada como detector de humo.

#### **Habilitar PD6662**

Habilitar el estándar PD6662. Las funciones que no cumplan con el estándar no tendrán efecto.

## Verificación de fallas

La verificación de fallas aquí es solo para el panel de control en el estado normal.

El sistema determina si verificar las fallas enumeradas en la página. El sistema sólo comprobará el fallo que esté seleccionado.

## Pasos

1. En la página de la lista de dispositivos, toque AX PRO y luego inicie sesión en el dispositivo (si es necesario) para ingresar el página.
2. Toque **Sistema** y **Opciones del sistema** y **Verificación de fallas del sistema** para ingresar a la página.

## Detectar la desconexión de la cámara de red

Esta opción solo aparece si se ha agregado una cámara a AX PRO.

Si la opción está habilitada, cuando la cámara de red vinculada se desconecte, se activará una alarma. El tiempo de retraso de la detección de la desconexión de la cámara de red es el mismo que el de la LAN.

## Comprobación de pérdida de batería

Si la opción está habilitada, cuando la batería del panel esté desconectada, el dispositivo cargará eventos.

## Comprobación de batería baja

Si la opción está habilitada, cuando la batería del panel está en estado de batería baja, el dispositivo cargará eventos.

## LAN perdida

Si la opción está habilitada, cuando la red cableada esté desconectada o con otras fallas, la alarma se disparará.

**-Retraso de pérdida de LAN:** si la red vuelve a la normalidad dentro de la duración del retraso, no se informará ninguna falla.

## Wi-Fi perdido

Si la opción está habilitada, cuando el Wi-Fi esté desconectado o con otras fallas, la alarma se disparará.

**-Retraso de pérdida de WiFi:** si la red vuelve a la normalidad dentro de la duración del retraso, no se informará ninguna falla.

## Celular Perdido

Si la opción está habilitada, cuando la red de datos celular esté desconectada o con otras fallas, la alarma se disparará.

**-Retraso de pérdida de celular:** si la red vuelve a la normalidad dentro de la duración del retraso, no se informará ninguna falla.

## Pérdida de alimentación de red del panel

Si la opción está habilitada, se activará una alarma cuando se desconecte el suministro principal del panel de control.

## Retardo de pérdida de energía de la red

**eléctrica del panel** El sistema verifica la falla después de la duración de tiempo configurada después del apagado de CA.

Para cumplir con la norma EN 50131-3, la duración del tiempo de verificación debe ser de 10 s.

### Opciones de armado

Esta función es para todo el sistema de alarma, para informar al usuario del estado actual del sistema antes de armarlo. Si está habilitado, habrá un aviso de falla y un proceso de confirmación para los lectores de etiquetas, teclados, llaveros y la aplicación. Si no está habilitado, no habrá detección de fallas antes de armar.

#### Pasos

1. En la página de la lista de dispositivos, toque AX PRO y luego inicie sesión en el dispositivo (si es necesario) para ingresar el página.
2. Toque **Sistema** y **Opciones del sistema** y **Opciones de armado** para ingresar a la página.

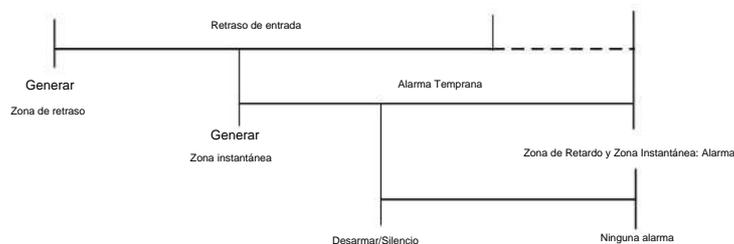
Puede configurar los siguientes parámetros:

#### Armar con falla

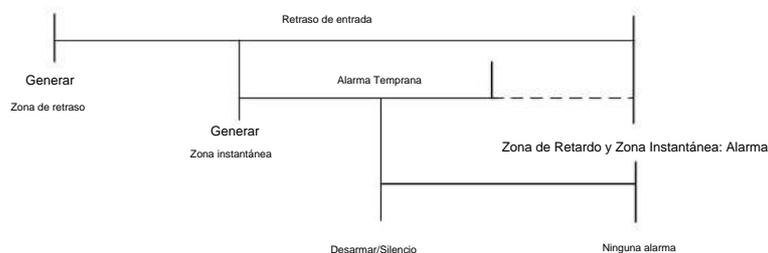
Verifique las fallas en la lista Habilitar armado con fallas, y el dispositivo no detendrá el procedimiento de armado cuando ocurran fallas.

#### Alarma Temprana

Primero se activa una zona de retraso y el área se encuentra en la etapa de "Retraso de entrada". Durante el período de tiempo de retardo, se activa una zona instantánea. En este momento, el área entra en la etapa de alarma temprana (solo para la primera zona instantánea activada). Hay alarma de voz del panel de control y alarma sonora local, pero no se envía ningún mensaje de alarma. Si la zona se desarma o se silencia antes de que finalicen la alarma temprana y el retardo de entrada, no se informará el mensaje de alarma. De lo contrario, tanto la zona retardada como la zona instantánea activarán la alarma.



O



3. Toque **Guardar**.

## Modo de inscripción

### Pasos

1. En la página de la lista de dispositivos, toque AX PRO y luego inicie sesión en el dispositivo (si es necesario) para ingresar el página.
2. Toque **Sistema** y **Opciones del sistema** y **Modo de inscripción** para ingresar a la página.
3. Toque **Entrar en el modo de inscripción**. Puede inscribir el periférico activándolo.

## Cámara de red

### Agregar cámaras al AX PRO

#### Pasos

1. En el sitio, toque AX PRO y luego inicie sesión en el dispositivo (si es necesario).
2. Toque **Cámara de red** y **Canal** de cámara de red para ingresar a la página.
3. Toque **Agregar canal**.
4. Introduzca la dirección IP, el puerto, el nombre de usuario y la contraseña de la cámara.
5. Toque **Guardar icono**.
6. Opcional: toca **Editar** o **Eliminar** para editar o eliminar la cámara seleccionada.

### Establecer parámetros de vídeo

#### Pasos

1. En el sitio, toque AX PRO y luego inicie sesión en el dispositivo (si es necesario).
2. Toque **Cámara de red** y **Configuración de vídeo de evento** para ingresar a la página.
3. Seleccione una cámara y configure los parámetros de vídeo.

#### Tipo de transmisión

Transmisión principal: se utiliza en la grabación y la vista previa de alta definición, tiene una alta resolución, tasa de codificación y calidad de imagen.

Sub-Stream: se utiliza para transmitir imágenes de red y obtener una vista previa como una transmisión de vídeo con características de menor resolución, tasa de bits y calidad de imagen.

#### Tipo de tasa de

**bits** Seleccione el tipo de tasa de bits como constante o variable.

#### Resolución

Seleccione la resolución de la salida de vídeo.

#### tasa de bits

El valor más alto corresponde a la calidad de vídeo más alta, pero se requiere un mejor ancho de banda.

#### Antes de la alarma

El tiempo de grabación antes de la alarma.

#### Después de la alarma

La duración del tiempo de grabación después de la alarma.

## Establecer horario de armado/desarmado

### Pasos

1. En la página de la lista de dispositivos, toque AX PRO y luego inicie sesión en el dispositivo (si es necesario) para ingresar el página.
2. Toque  para ingresar a la página.
3. Toque un área de la lista, habilite el área y seleccione los dispositivos vinculados.
4. Establecer parámetros:

#### Armado automático

Permita que el área se arme automáticamente en un punto de tiempo específico.

#### Tiempo de armado automático

Configure el horario para que el área se arme automáticamente.

#### Desarmado automático

Permita que el área se desarme automáticamente en un punto de tiempo específico.

#### Tiempo de desarme automático

Configure el horario para que el área se desarme automáticamente.

#### Indicación de sonido de autoarmado

Después de desactivarlo, el zumbador no emitirá un pitido antes del armado automático.

#### Tarde para desarmar

Habilite el dispositivo para enviar una notificación al teléfono o tableta para recordarle al usuario que debe desarmar el área cuando el área todavía está armada después de un punto de tiempo específico.



Debe habilitar la función Notificación de administración del panel en el Cliente web de **Parámetros de comunicación y Comunicación de eventos** antes de habilitar la función Tarde para desarmar.

---

#### Tiempo de retraso para desarmar

Establezca el punto de tiempo mencionado en **Tarde para desarmar**.

#### Excepción de fin de semana

Si está habilitado, **Auto Armado**, **Auto Desarmado** y **Tarde para Desarmar** están deshabilitados durante el fin de semana.

#### Vacaciones exceptuadas

Habilite la función y la zona no se armará/desarmará en las vacaciones. Debe configurar el programa de vacaciones después de habilitarlo.



Se pueden configurar hasta 6 grupos de vacaciones.

---

## Comunicación

### Red cableada

#### Pasos

1. En el sitio, toque AX PRO y luego inicie sesión en el dispositivo (si es necesario).
2. Toque **Parámetros de comunicación** y **Red cableada** para ingresar a la página.
3. Configure los parámetros.
  - Configuración automática: habilite **DHCP** y configure el puerto HTTP.
  - Configuración manual: **DHCP** deshabilitado y configuración **de dirección IP, máscara de subred, dirección de puerta de enlace, DNS Dirección del servidor.**
4. **Opcional:** configure la dirección del servidor DNS correcta si el dispositivo necesita visitar el servidor Hik-Connect a través de un nombre de dominio.
5. Haga clic en **Guardar**.

### Configuración wifi

#### Pasos

1. En el sitio, toque AX PRO y luego inicie sesión en el dispositivo (si es necesario).
2. Toque **Parámetros de comunicación** y **Configuración Wi-Fi** para ingresar a la página.
3. Toque un Wi-Fi para conectarse en la lista.

### Red de datos móviles

#### Pasos

1. En el sitio, toque AX PRO y luego inicie sesión en el dispositivo (si es necesario).
2. Toque **Parámetros de comunicación** y **Configuración de red de datos móviles** para ingresar a la página.
3. Habilite **la red de datos móviles.**
4. Toque para seleccionar una tarjeta SIM. Toque **Configuración de parámetros** y **Editar icono** y configure los parámetros incluyendo el nombre de usuario, contraseña de acceso, APN, MTU y código PIN.
5. Toque **Guardar icono.**
6. Habilite **el límite de uso de datos.**
7. Edite **los datos utilizados este mes** y **los datos limitados por mes.**

#### Número de acceso

Introduzca el número de marcación del operador.

---



Solo el usuario de la tarjeta SIM de la red privada necesita ingresar el número de acceso.

---

#### Nombre de usuario

Pregúntele al operador de red e ingrese el nombre de usuario.

#### Contraseña de acceso

Pregúntele al operador de red e ingrese la contraseña.

#### APN

Pídale al operador de red que obtenga la información de APN e ingrese la información de APN.

#### Datos limitados por mes

Puede habilitar la función y establecer el umbral de datos cada mes. Si el uso de datos supera el umbral configurado, se activará una alarma y se cargará en el centro de alarmas y el cliente móvil.

#### Datos utilizados este mes

Los datos utilizados se acumularán y se mostrarán en este cuadro de texto.

### Notificaciones push

Cuando se activa una alarma, si desea enviar la notificación de alarma al teléfono móvil, puede configurar los parámetros de notificación automática.

#### Pasos

1. En el sitio, toque AX PRO y luego inicie sesión en el dispositivo (si es necesario).
2. Toque  **Parámetros de comunicación** y **Notificación(es) automática(s)** para ingresar a la página.
3. Habilite la notificación de destino.

#### Alarma de zona/tapa abierta

El dispositivo enviará notificaciones cuando se active la alarma de zona o cuando se active o restablezca la tapa de la zona abierta.



Debe configurar el tiempo de intervalo de filtrado de eventos para las llamadas telefónicas.

---

#### Tapa de periféricos abierta

El dispositivo enviará notificaciones cuando se active o restablezca la tapa abierta de cualquier periférico.

#### Tapa del panel abierta

El dispositivo enviará notificaciones cuando la tapa del panel de control se abra o se restablezca.

#### Alarma de pánico

El dispositivo enviará notificaciones cuando se active o restablezca la alarma de pánico por zonas, teclados o llaveros.

#### alarma medica

El dispositivo enviará notificaciones cuando se active la alarma médica.

#### Alarma de incendios

El dispositivo enviará notificaciones cuando se active la alarma de incendio.

#### alarma de gas

El dispositivo enviará notificaciones cuando se active la alarma de gas.

#### Estado del panel

El dispositivo enviará notificaciones cuando cambie el estado del sistema del panel de control.

#### Estado de zona

El dispositivo enviará notificaciones cuando se cambie el estado de la zona.

#### Estado de los periféricos

El dispositivo enviará notificaciones cuando se cambie el estado de cualquier periférico.

#### Operación del panel

El dispositivo enviará notificaciones cuando el usuario opere el AX PRO.

#### Evento de alarma inteligente

El dispositivo enviará notificaciones cuando se active la alarma en las cámaras térmicas.

#### Establecer alarma de emergencia (en la aplicación)

Los eventos seleccionados serán notificados como emergencia mientras que el evento no seleccionado no se mostrará en la página.

5. Toque **Llamada telefónica y SMS**.
6. Toque **+ Agregar número de teléfono** para ingresar el número de teléfono.
7. Toque el número de teléfono agregado para habilitar **Llamadas telefónicas y SMS** según sus necesidades.  
(Para llamadas telefónicas) Establecer números de llamadas.  
(Para SMS) Establecer permiso de armado, permiso de desarmado y permiso de borrado de alarma para áreas

#### Mensaje común

Puede ingresar el contenido del mensaje. Cuando se active la alarma, su contenido personalizado se agregará al comienzo del mensaje enviado por el sistema.

#### Voz común

Puede importar un nuevo audio. Cuando se active la alarma, su voz personalizada se agregará al comienzo del contenido del teléfono marcado por el sistema. También puede tocar Borrar para eliminar audios



#### Nota

Solo se admite el formato WAV, hasta 512 KB y 15 s.

---

10. Revisa las notificaciones.

## Centro de recepción de alarmas (CRA)

Puede configurar los parámetros del centro de recepción de alarmas y todas las alarmas se enviarán al centro de alarmas configurado.

### Pasos

1. En el sitio, toque AX PRO y luego inicie sesión en el dispositivo (si es necesario).
2. Toque y **Parámetros de comunicación** y **Centro de recepción de alarmas (CRA)** para ingresar a la página.
3. Seleccione un CRA y actívelo.

#### Tipo de protocolo

Seleccione el Tipo de protocolo como ADM-CID, ISUP, SIA-DCS, \*SIA-DCS, \*ADM-CID, CSV-IP, Módulo FSK o Módulo RDC para configurar el modo de carga.

#### Verificación de intrusos como servicio

Cuando el panel de control cargue la información de la alarma, devolverá la dirección de la imagen y el video para que usted los vea.

#### Compañías

Seleccione la empresa de asistencia como Ninguna, Empresa receptora de múltiples alarmas húngara o Empresa receptora de alarmas francesa.

#### Tipo de dirección

Seleccione el Tipo de dirección como Dirección IP y Nombre de dominio. Ingrese la dirección del servidor/nombre de dominio, número de puerto y código de cuenta.

#### Modo de transmisión

Seleccione el Modo de transmisión como TCP o UDP. UDP es recomendado por el estándar SIA DC-09.

#### Período de tiempo de espera de reintento

Después del tiempo seleccionado, el sistema volverá a intentar transmitir.

#### intentos

Establezca el número de reintentos.

#### Opción de sondeo

Establezca la tasa de sondeo con un rango de 10 a 3888000 segundos. El sistema informará la falla si el tiempo supera el límite. El estado del dispositivo se mostrará como fuera de línea.

#### Prueba periódica

Después de habilitarlo, puede configurar el intervalo de tiempo, configurando la frecuencia con la que se envía un evento de prueba al CRA para garantizar la conexión.

## GMT

Habilite la hora del meridiano de Greenwich.

## Configuración del servicio en la nube

### Pasos

1. En el sitio, toque AX PRO y luego inicie sesión en el dispositivo (si es necesario).
2. Toque  **Parámetros de comunicación** y **Configuración del servicio en la nube** para ingresar a la página.
3. Seleccione el **modo de comunicación**.

### Red alámbrica y prioridad Wi-Fi

El orden de prioridad de conexión de mayor a menor es: red cableada, Wi-Fi, red de datos móviles.

### Con cable y Wi-Fi

El sistema seleccionará primero la red cableada. Si no se detecta una red cableada, seleccionará la red Wi-Fi.

### Red de datos móviles

El sistema seleccionará solo la red de datos móviles.

4. Habilite **la prueba periódica**. Ingrese el intervalo de prueba periódica.
5. Toque **Guardar**.

## Notificación por correo electrónico

### Pasos

1. En el sitio, toque AX PRO y luego inicie sesión en el dispositivo (si es necesario).
2. Toque  **Parámetros de comunicación** y **Notificación por correo electrónico** para ingresar a la página.
3. Habilitar **correo electrónico 1**.
4. Introduzca el nombre del remitente, la dirección de correo electrónico del remitente, la dirección del servidor SMTP, el puerto SMTP, el nombre de usuario y clave.



Se recomienda utilizar Gmail y Hotmail para el envío de correos.

Solo si la zona está vinculada con una cámara de red, el correo electrónico de alarma se adjuntará con el video de alarma.

---

5. Seleccione el tipo de cifrado como **Ninguno, SSL o TLS**.
6. Habilite **la autenticación del servidor**.
7. Ingrese el nombre del destinatario y la dirección de correo electrónico del destinatario. Toque **Probar la dirección de correo electrónico del receptor** para probar si la dirección de correo electrónico es correcta.
8. Toque **Guardar**.
9. Opcional: configure el **correo electrónico 2** en el mismo orden. Puede elegir si configurar el correo electrónico 2 como buzón de respaldo.



Las reseñas de videos y fotos se enviarán a ambos buzones. Si el Correo electrónico 2 está configurado como un buzón de respaldo, el sistema enviará correos electrónicos al Correo electrónico 2 solo si el Correo electrónico 1 no se recibe.

---

## Configuración FTP

### Pasos

1. En el sitio, toque AX PRO y luego inicie sesión en el dispositivo (si es necesario).
2. Toque **Parámetros de comunicación** y **Configuración de FTP** para ingresar a la página.
3. Seleccione **FTP preferido** o **FTP alternativo** y habilite FTP.
4. Configurar los parámetros de FTP

### Tipo FTP

Configure el tipo de FTP como preferido o alternativo.

### Tipo de protocolo

FTP y SFTP son seleccionables. La carga de archivos se cifra mediante el protocolo SFTP.

### Dirección y puerto del servidor

La dirección del servidor FTP y el puerto correspondiente.

### Nombre de usuario y contraseña/Anonimato

El usuario de FTP debe tener permiso para cargar imágenes. Si el servidor FTP admite la carga de imágenes por parte de usuarios anónimos, puede habilitar Anónimo para ocultar la información de su dispositivo durante la carga.

### Estructura del directorio

La ruta de guardado de las instantáneas en el servidor FTP.

4. Toque **Guardar**.

## NAT

Universal Plug and Play (UPnP™) es una arquitectura de red que proporciona compatibilidad entre equipos de red, software y otros dispositivos de hardware. El protocolo UPnP permite que los dispositivos se conecten sin problemas y simplifica la implementación de redes en entornos domésticos y corporativos.

Habilite la función UPnP, y no necesita configurar la asignación de puertos para cada puerto, y el dispositivo está conectado a la red de área amplia a través del enrutador.

### Pasos

1. En el sitio, toque AX PRO y luego inicie sesión en el dispositivo (si es necesario).
2. Toque **Parámetros de comunicación** y **NAT** para ingresar a la página.
3. Arrastre el control deslizante para habilitar UPnP.

4. **Opcional:** Seleccione el tipo de asignación como **Manual** para establecer el puerto HTTP y el puerto de servicio.
5. Haga clic en **Guardar** para completar la configuración .

### Servicio de intercomunicación

Puede configurar el servicio de intercomunicación para una sirena de intercomunicación.

#### Antes de que empieces

Primero debe registrar un zumbador de intercomunicador.

Solo se puede configurar una sirena como sirena de intercomunicación.

#### Pasos

1. Toque **Comunicación** y **Servicio de intercomunicador** para ingresar a la página.
2. Deslice para habilitar la función.
3. Configure el tipo de intercomunicador.

SORBO

El panel de control utilizará el servidor ARC y SIP.

#### Receptor IP Pro

El panel de control usará el servicio en la nube del usuario.

4. Seleccione una sonda y toque **Guardar**.

### Mantenimiento del dispositivo

Puede reiniciar el dispositivo.

#### Pasos

1. En el sitio, toque AX PRO y luego inicie sesión en el dispositivo (si es necesario).
2. Toque **Mantenimiento** y **Reiniciar dispositivo**, para entrar en la página de mantenimiento.  
El AX PRO se reiniciará.
3. Toque **Mantenimiento** y **Actualización de dispositivo** para actualizar el panel de control, o toque **Mantenimiento** y **Actualización** de detectores y periféricos para actualizar detectores y periféricos.
4. Opcional: Toque **Mantenimiento** y **Recopilación de registros remotos** para habilitar la función.

Recopilación de registros remotos es para obtener registros relacionados con el dispositivo. Cuando esto está habilitado, nuestro soporte técnico podrá recopilar registros relacionados con el dispositivo de forma remota y cargarlos en nuestro servidor para solucionar problemas. Puede establecer el período de validez de acuerdo con las necesidades reales. Esta función se desactivará después del período de validez establecido.

## Conexión wifi

Puede hacer que el AX PRO se conecte a Wi-Fi a través de la aplicación.

### Pasos

1. En la página de la lista de dispositivos, toque AX PRO y luego inicie sesión en el dispositivo (si es necesario) para ingresar el página.
2. Toque y **Configurar red Wi-Fi**.
3. Siga las instrucciones de la página y cambie el AX PRO al modo AP. Presiona **Siguiente**.
4. Seleccione un Wi-Fi estable para que el dispositivo se conecte.
5. Regrese a la página de configuración para ingresar la contraseña de Wi-Fi y toque **Siguiente**.
6. Toque **Conectarse a una red** y espere la conexión.

Una vez completada la conexión, el AX PRO le indicará que salga del modo AP y cambie automáticamente al modo STA.

## Comprobar notificación de alarma

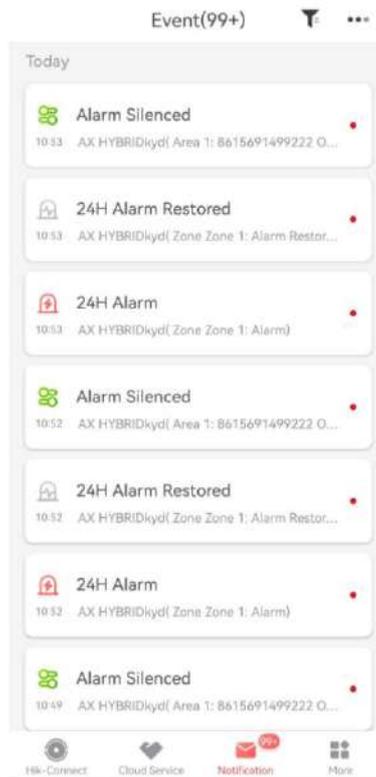
Cuando se active una alarma, recibirá una notificación de alarma. Puede consultar la información de la alarma desde el cliente móvil.

### Antes de que empieces

- Asegúrese de haber vinculado una zona con un detector.
- Asegúrese de que la zona no esté anulada.
- Asegúrese de no haber habilitado la función de zona silenciosa.

### Pasos

1. Toque **Notificación** en el cliente móvil para ingresar a la página.  
Todas las notificaciones de alarma se enumeran en la página Notificación.
2. Seleccione una alarma y podrá ver los detalles de la alarma.



3. **Opcional:** si la zona tiene una cámara vinculada, puede ver la reproducción cuando se active la alarma motivado.

4. **Opcional:** toca  para buscar eventos por fechas o dispositivos.

## 5.3 Configuración con el cliente web

### Pasos

1. Conecte el dispositivo a la red Ethernet.
2. Busque la dirección IP del dispositivo a través del software cliente y el software SADP.
3. Introduzca la dirección IP buscada en la barra de direcciones.
4. Utilice el nombre de usuario y la contraseña de activación para iniciar sesión.



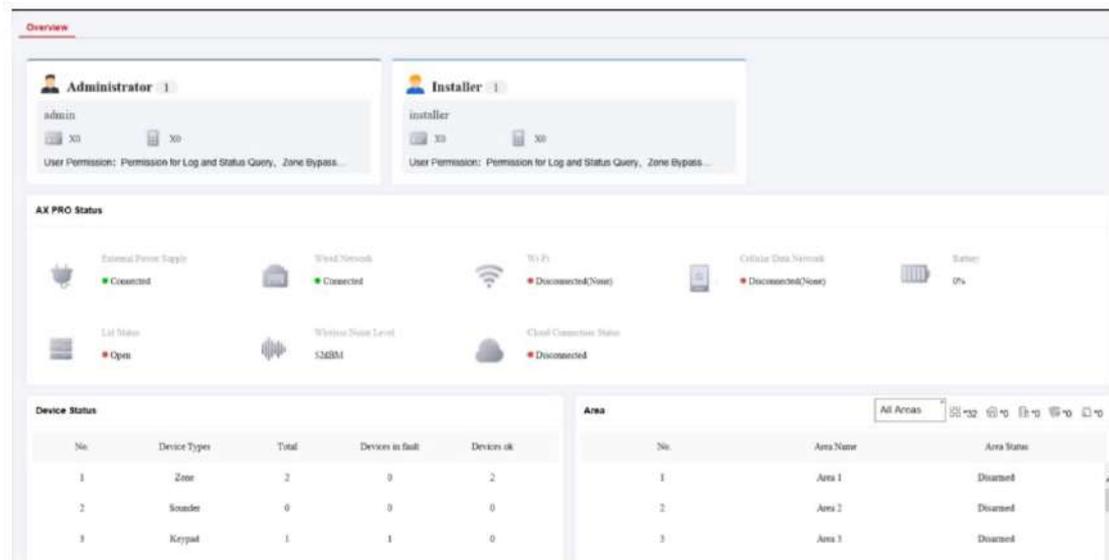
### Nota

ÿ Solo el administrador y el instalador pueden iniciar sesión en el cliente web.

ÿ El nombre de usuario y la contraseña son los mismos cuando se activa a través de Hik-Connect o Hik ProConectar.

---

Puede ver el estado del usuario, del dispositivo y del área en la página de información general.



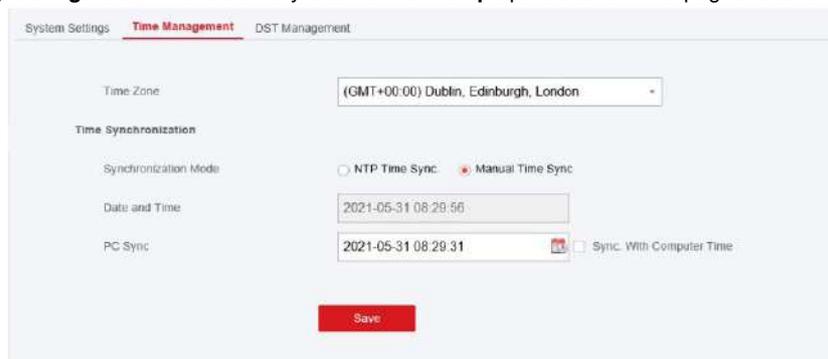
### 5.3.1 Configuración del sistema

#### Ajustes de hora

Puede configurar la zona horaria del dispositivo, sincronizar la hora del dispositivo y configurar el horario de verano. El dispositivo admite sincronización de tiempo a través del servidor **Hik-Connect**.

#### Gestión del tiempo

Haga clic en **Sistema** y **Configuración del sistema** y **Gestión del tiempo** para acceder a la página Gestión del tiempo.



Puede seleccionar una zona horaria de la lista desplegable.

Puede sincronizar la hora del dispositivo manualmente con NTP. Marque la casilla de verificación de **NTP Time Sync.**, ingrese la dirección del servidor y el número de puerto, y configure el intervalo de sincronización.

Puede sincronizar la hora del dispositivo manualmente. O marque **Sincronizar. con Computer Time** para sincronizar la hora del dispositivo con la hora de la computadora.

---

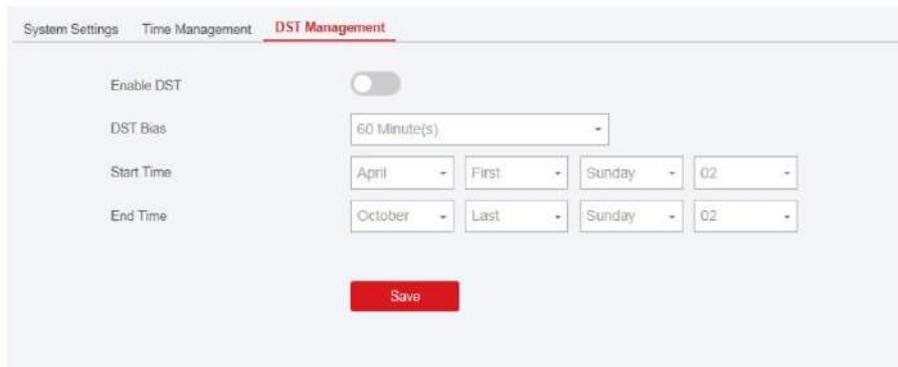
#### Nota

Mientras sincroniza la hora manualmente o con la hora de la computadora, el sistema registra el registro "Sincronización SDK".

---

### Administración de DST Haga

clic en **Sistema** y **Configuración del sistema** y **Administración de DST** para ingresar a la página de Administración de tiempo.

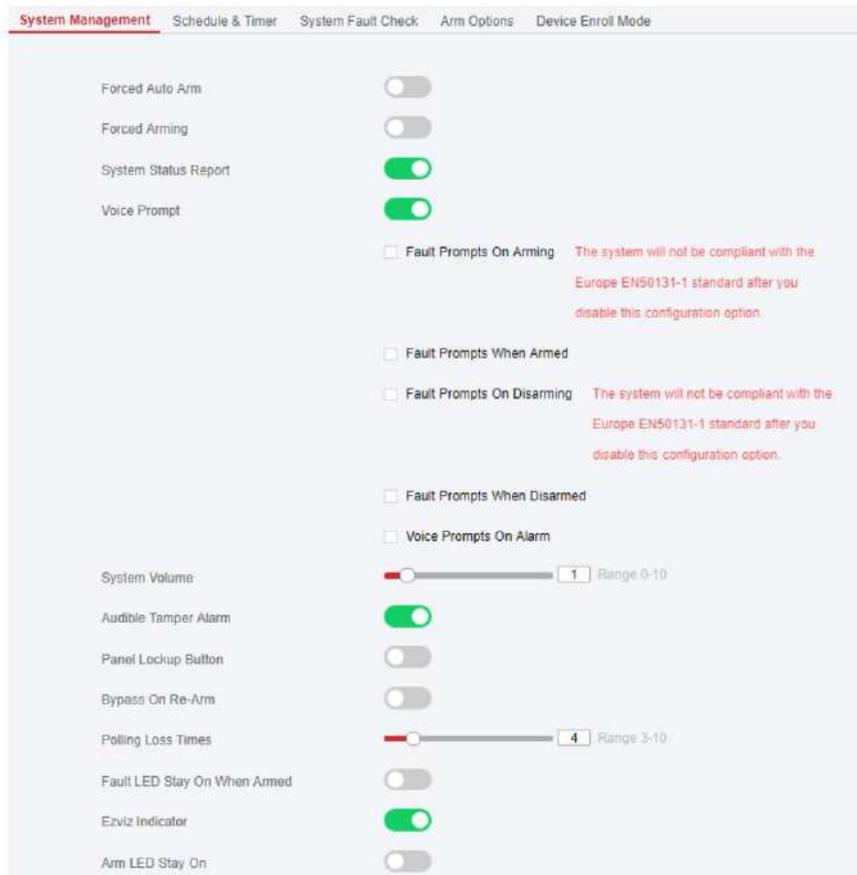


Puede habilitar el horario de verano y configurar el sesgo del horario de verano, la hora de inicio del horario de verano y la hora de finalización del horario de verano.

## Gestión del sistema

Configure las opciones de autoridad.

Haga clic en **Sistema** y **Opciones del sistema** y **Administración** del sistema para ingresar a la página.



### Armado automático forzado

Después de habilitarse, cuando comienza el armado automático temporizado, si hay fallas activas en una zona, la zona se anulará automáticamente.

Puede ir a **Sistema** y **Opciones** de sistema y **Horario y hora** para configurar el horario de armado/desarmado automático y las áreas vinculadas.

---

 **Nota**

Debe desactivar Armar con fallas en la página Opciones de armar. O la función de Armado automático forzado/  
Armado forzado no puede ser válida.

---

### **Armado Forzado**

Después de habilitarse, cuando comienza el armado manual, si hay fallas activas en una zona, la zona se omitirá automáticamente.

Puede usar llaveros, etiquetas y teclados para armar zonas o armar zonas manualmente en la aplicación. Se pueden seleccionar áreas individuales, múltiples o todas para armar.

---

 **Nota**

Debe desactivar Armar con fallas en la página Opciones de armar. O la función de Armado automático forzado/  
Armado forzado no puede ser válida.

---

### **Informe de estado del sistema**

Si la opción está habilitada, el dispositivo cargará el informe a la nube (para APP) y ARC automáticamente cuando se cambie el estado de AX PRO.

### **Mensaje de voz**

Si la opción está habilitada, el AX PRO habilitará el mensaje de voz.

-Indicaciones de falla al armar: Indicaciones de voz de fallas al armar.

-Indicaciones de falla cuando está armado: Indicaciones de voz de fallas cuando el sistema está armado.

-Avisos de fallas al desarmar: aviso de voz de fallas al desarmar

-Indicaciones de falla cuando está desarmado: Indicaciones de voz de fallas cuando el sistema está desarmado.

-Indicaciones de voz en alarma: Indicaciones de voz de fallas cuando se activa una alarma.

### **Volumen del sistema**

El rango de volumen del sistema disponible es de 0 a 10.

### **Alarma audible de sabotaje**

Mientras está habilitado, el sistema alertará con un zumbador para la alarma de manipulación. Independientemente de si está habilitado o no, la alarma de manipulación normalmente se enviará a la nube (para APP) y ARC.

### **Botón de bloqueo del panel**

Todas las funciones de AX PRO se congelarán después de que se habilite. Esta función solo puede ser habilitada por usuarios con permiso de instalador.

### **Anular al rearmar**

Mientras está habilitado, después de anular el detector, si se restauran sus fallas y se arma el área enlazada, el detector se armará automáticamente.

#### **Tiempos de pérdida de sondeo**

Establezca el número máximo de veces para la pérdida de sondeo de periféricos y detectores. El sistema informará la falla si el tiempo supera el límite.

El estado de estos periféricos y detectores se mostrará como fuera de línea.

#### **El LED de falla permanece encendido cuando está armado**

Cuando el sistema está armado, el indicador de falla siempre está encendido.

#### **Indicador Ezviz**

Habilite el indicador Ezviz.

#### **Armar LED permanecer encendido**

El LED de brazo está siempre encendido.

#### **Restauración del detector de movimiento**

Los detectores de movimiento incluyen todos los detectores PIR.

-Desactivar: Sin restauración automática.

-Inmediatamente después de la alarma: los detectores de movimiento se restauran automáticamente inmediatamente después de la alarma e informan a Cloud (para APP) y ARC.

-Después de desarmar: los detectores de movimiento se restauran automáticamente después de desarmar e informan a la nube (para APP) y ARC

#### **Ajustes de sensibilidad de interferencia**

El dispositivo detectará la interferencia de RF y enviará mensajes cuando la interferencia de RF interfiera con la comunicación. Puede ajustar la sensibilidad de detección.

#### **Modo de ahorro de energía**

Mientras está habilitado, la fuente de alimentación principal está apagada, Wi-Fi entra en bajo consumo de energía, 4G se cierra, falla la lectura de etiquetas, LED apagado y aviso de voz apagado.

#### **Restablecimiento del detector de humo**

Solo para la zona cableada de la central M2H, que está configurada como detector de humo.

#### **Habilitar PD6662**

Habilitar el estándar PD6662. Las funciones que no cumplan con el estándar no tendrán efecto.

## **Ajustes de horario y temporizador**

Puede configurar el horario de la alarma. La zona se armará/desarmará según el horario configurado.

#### **Pasos**

1. Haga clic en **Sistema** y **Opciones del sistema** y **Programación y temporizador** para ingresar a la página Programación y temporizador.

System Management **Schedule & Timer** System Fault Check Arm Options Device Enroll Mode

Area: Area1

Enable auto Arm:

Time: 00:00

Enable auto Disarm:

Time: 00:00

Late to Disarm:

Time: 00:00

Weekend Exception:

Holiday Exception:

Auto Arm Sound Prompt:

Panel Alarm Duration: 90 s

Save

2. Seleccione un área.

3. Establezca los siguientes parámetros según las necesidades reales.

#### Habilitar Armado Automático

Habilite la función y establezca la hora de inicio del armado. La zona se armará según el tiempo configurado.

---

#### Nota

- El tiempo de autoarmado y el tiempo de autodesarmado no pueden ser iguales.
  - El zumbador suena lentamente 2 minutos antes de que comience el armado automático y suena rápido 1 minuto antes de que comience el armado automático.
  - Puede seleccionar habilitar el armado forzado en la página Opciones del sistema. Mientras la función esté habilitada, el sistema estará armado independientemente de la falla.
- 

#### Habilitar desarme automático

Habilite la función y configure la hora de inicio del desarmado. La zona se desarmará según el tiempo configurado.

---

#### Nota

- El tiempo de autoarmado y el tiempo de autodesarmado no pueden ser iguales.
- 

#### Tarde para desarmar

Habilite la función y ajuste la hora. Si la alarma se activa después del tiempo configurado, la persona se considerará retrasada.



Debe habilitar la función Notificación de administración del panel en **Parámetros de comunicación** y **Comunicación de eventos** antes de habilitar la función Tarde para desarmar.

---

#### Excepción de fin de semana

Habilite la función y la zona no se armará en el fin de semana.

#### Excepción de vacaciones

Habilite la función y la zona no se armará/desarmará en las vacaciones. Debe configurar el programa de vacaciones después de habilitarlo.

---



Se pueden configurar hasta 6 grupos de vacaciones.

---

#### Aviso de sonido de armado automático

Después de desactivarlo, el zumbador no emitirá un pitido antes del armado automático.

#### Duración de la alarma del panel

El tiempo de duración de la alarma del panel.

---



El rango de duración de tiempo disponible es de 10 s a 900 s.

---

5. Haga clic en **Guardar**.

#### Verificación de fallas

La verificación de fallas aquí es solo para el panel de control en el estado normal.

El sistema determina si verificar las fallas enumeradas en la página. El sistema sólo comprobará el fallo que esté seleccionado.

Haga clic en **Sistema** y **Opciones del sistema** y **Verificación de fallas del sistema** para ingresar a la página.

Panel Battery Lost	<input checked="" type="checkbox"/>
Panel Low Battery	<input checked="" type="checkbox"/>
LAN Lost	<input checked="" type="checkbox"/>
LAN Lost Delay	<input type="text" value="180"/> s
WiFi Lost	<input checked="" type="checkbox"/>
WiFi Lost Delay	<input type="text" value="180"/> s
Cellular Lost	<input checked="" type="checkbox"/>
Cellular Lost Delay	<input type="text" value="180"/> s
Panel Mains Power Lost	<input checked="" type="checkbox"/>
Panel Mains Power Loss Delay	<input type="text" value="10"/> s

Save

### Detectar la desconexión de la cámara de red

Esta opción solo aparece si se ha agregado una cámara a AX PRO.

Si la opción está habilitada, cuando la cámara de red vinculada se desconecte, se activará una alarma. El tiempo de retraso de la detección de la desconexión de la cámara de red es el mismo que el de la LAN.

### Batería del panel perdida

Si la opción está habilitada, cuando la batería esté desconectada, el dispositivo cargará eventos.

### Panel de batería baja

Si la opción está habilitada, cuando la batería está en estado de batería baja, el dispositivo cargará eventos.

### LAN perdida

Si la opción está habilitada, cuando la red cableada esté desconectada o con otras fallas, la alarma se disparará.

**-Retraso de pérdida de LAN:** si la red vuelve a la normalidad dentro de la duración del retraso, no se informará ninguna falla.

### Wi-Fi perdido

Si la opción está habilitada, cuando el Wi-Fi esté desconectado o con otras fallas, la alarma se disparará.

**-Retraso de pérdida de Wi-Fi:** si la red vuelve a la normalidad dentro de la duración del retraso, no se informará ninguna falla.

### Celular Perdido

Si la opción está habilitada, cuando la red de datos celular esté desconectada o con otras fallas, la alarma se disparará.

**-Retraso de pérdida de celular:** si la red vuelve a la normalidad dentro de la duración del retraso, no se informará ninguna falla.

### Pérdida de alimentación principal del panel

Si la opción está habilitada, se activará una alarma cuando se desconecte el suministro principal del panel de control.

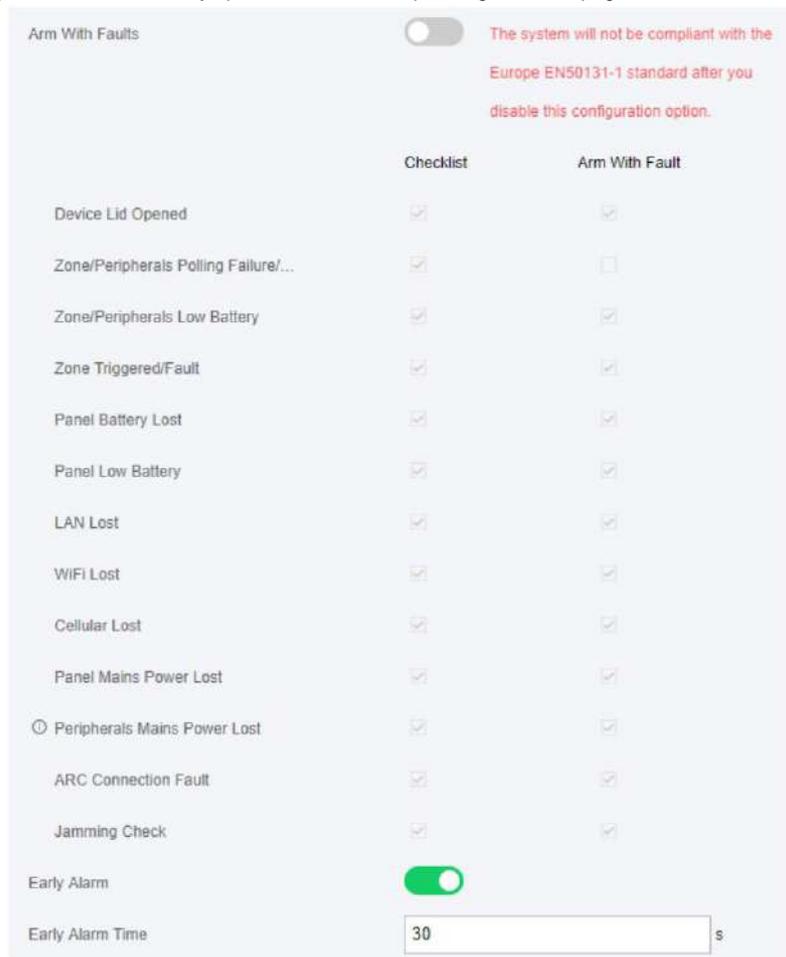
**Retardo de pérdida de energía principal del panel**

El sistema verifica la falla después de la duración de tiempo configurada después del apagado de CA.  
 Para cumplir con la norma EN 50131-3, la duración del tiempo de verificación debe ser de 10 s.

**Opciones de armado**

Esta función es para todo el sistema de alarma, para informar al usuario del estado actual del sistema antes de armarlo. Si está habilitado, habrá un aviso de falla y un proceso de confirmación para los lectores de etiquetas, teclados, llaveros y APP. Si no está habilitado, no habrá detección de fallas antes de armar.

Haga clic en **Sistema** y **Opciones del sistema** y Opciones de **armado** para ingresar a la página.



Puede configurar los siguientes parámetros:

**Armar con fallas**

Verifique las fallas en la lista Armar con fallas y el dispositivo no detendrá el proceso de armado cuando ocurran fallas.

**Lista de verificación de fallas**

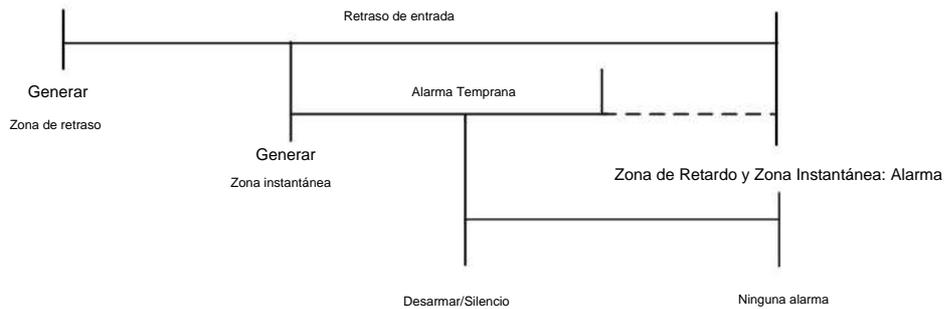
El sistema verificará si el dispositivo tiene las fallas en la lista de verificación durante el proceso de armado.

### Alarma Temprana

Primero se activa una zona de retraso y el área se encuentra en la etapa de "Retraso de entrada". Durante el período de tiempo de retardo, se activa una zona instantánea. En este momento, el área entra en la etapa de alarma temprana (solo para la primera zona instantánea activada). Hay alarma de voz del panel de control y alarma sonora local, pero no se envía ningún mensaje de alarma. Si la zona se desarma o se silencia antes de que finalicen la alarma temprana y el retardo de entrada, no se informará el mensaje de alarma. De lo contrario, tanto la zona retardada como la zona instantánea activarán la alarma.

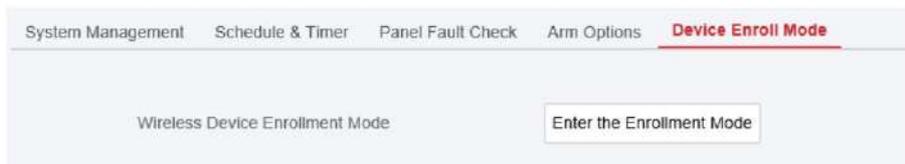


O



### Modo de inscripción de dispositivos

Haga clic en Ingresar al modo de inscripción para que el panel ingrese al modo de inscripción.



### Configuraciones de seguridad

#### Configuración SSH

Habilite o deshabilite SSH (Secure Shell) según sus necesidades reales.

Haga clic en **Sistema** y **Seguridad del sistema** y **Configuración de SSH** para ingresar a la página de Configuración de SSH y puede

habilitar o deshabilitar la función SSH.



### Bloqueo de la configuración del usuario

El dispositivo se bloqueará 90 s después de 3 intentos de credencial fallidos (se puede configurar en Tiempo de reintento antes del bloqueo automático) en un minuto.

Puede ver el usuario bloqueado o desbloquear un usuario y establecer la duración del bloqueo del usuario.

---

#### Nota

Para cumplir con el requisito de EN, el sistema solo registrará el mismo registro 3 veces de forma continua.

---

### Pasos

1. Haga clic en **Sistema y Seguridad del sistema y Intentos de bloqueo de usuario** para ingresar a la Configuración de bloqueo de usuario página.

2. Configure los siguientes parámetros.

#### Veces de reintento antes del bloqueo automático

Si el usuario ingresa continuamente la contraseña incorrecta por más de las veces configuradas, la cuenta se bloqueará.

---

#### Nota

El administrador tiene dos intentos más que el valor configurado.

---

#### Tiempo de bloqueo automático

Establece la duración del bloqueo cuando la cuenta está bloqueada.



La duración de bloqueo disponible es de 5s a 1800s.

---

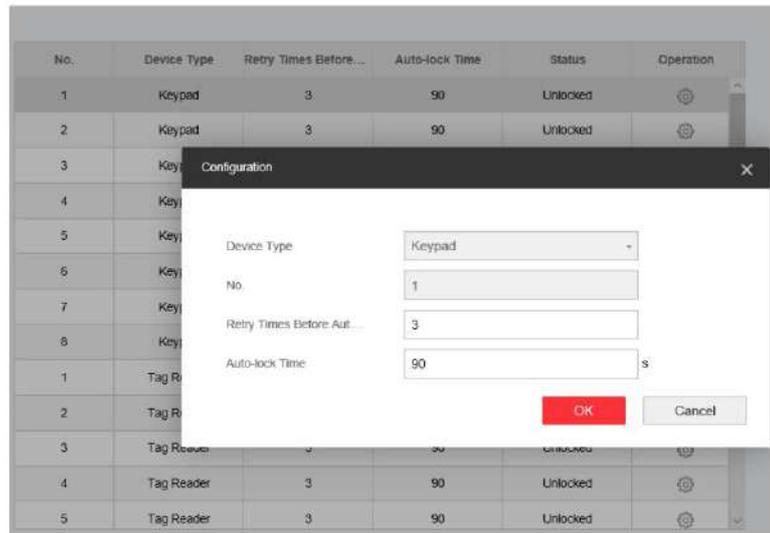
- Haga clic en  para desbloquear la cuenta o haga clic en **Desbloquear todo** para desbloquear todos los usuarios bloqueados en la lista.
- Haga clic en **Guardar**.

#### Configuración de bloqueo del módulo

Establezca los parámetros de bloqueo del módulo, incluido el número máximo de intentos fallidos y la duración del bloqueo. El módulo se bloqueará por la duración del tiempo programado, una vez que la autenticación del módulo haya fallado por la cantidad de tiempos configurados.

#### Pasos

- Haga clic en **Sistema** y **Seguridad del sistema** y **Configuración de bloqueo del módulo** para ingresar a la Configuración de bloqueo del módulo.  
página.



- Seleccione un módulo de la lista y haga clic en . Establezca los siguientes parámetros del módulo seleccionado.

#### Veces de reintento antes del bloqueo automático

Si un usuario continuamente intenta autenticar una contraseña por más de los intentos configurados permitidos, el teclado se bloqueará por la duración programada.

#### Tiempo de bloqueo automático

Establece la duración del bloqueo cuando el teclado está bloqueado. Después de la duración configurada, el teclado se desbloqueará.

- Haga clic en **Aceptar**.

## 5.3.2 Gestión de dispositivos

Puede administrar los periféricos registrados, incluidos el detector, la sirena, el teclado, etc. en esta sección.

### Zona

Puede establecer los parámetros de la zona en la página de la zona.

#### Pasos

1. Haga clic en **Dispositivo** y **Zona** para ingresar a la página Zona.

Zone	Device Number	Name	Main Device	Channel No	Device Types	Silent Alarm	Chime	Linked Camera	Operation
1	3	Wireless Zone 1	/	/	Instant	Disable	Disable	/	  
2	4	Wireless Zone 2	/	/	Instant	Disable	Disable	/	  

2. Seleccione una zona y haga clic en  para ingresar a la página Configuración de zona.

Zone Settings
✕

Detector Type Wireless PIR-Glass Break Detector ▾

Zone Type Instant ▾

Stay Arm Bypass

Forbid Bypass on Arming

Chime

Silent Alarm

Sounder Delay Time 0 ▾ s

Double Knock

Cross Zone None ▾

Link Pircam Not Link ▾

Link Camera Not Link ▾

OK
Cancel

3. Edite el nombre de la zona.

4. Verifique las áreas vinculadas.



#### Nota

• Solo se enumerarán las áreas habilitadas.

• El periférico recién agregado está vinculado al área 1 de forma predeterminada.

---

5. Seleccione un tipo de zona.

Puede ver los tipos de zona configurables para varios detectores a través de **I. Tipos de zona de detector.**

#### Zona instantánea

Este tipo de zona activará inmediatamente un evento de alarma cuando esté armada.

#### Zona de retraso

**-Retardo de salida:** el Retardo de salida le proporciona tiempo para salir de la zona sin alarma.

El armado con fallas está habilitado: primero debe confirmar las fallas y luego la zona está en proceso de armado. Si la zona de retardo se activa dentro del tiempo de retardo de salida pero se restablece antes de que finalice el tiempo, la alarma no se activará y la zona se armará.

El armado con fallas está deshabilitado: Armado inmediato. Si la zona de retardo se activa dentro del tiempo de retardo de salida pero se restablece antes de que finalice el tiempo, la alarma no se activará.

**-Retraso de entrada:** el retraso de entrada le proporciona tiempo para ingresar a la zona para desarmar el sistema sin alarma.

Después de la activación, si la zona no se desarma o silencia antes de que finalice el tiempo de retardo de entrada, la zona emitirá una alarma.

**-Tiempo de Retardo de Armado Parcial:** El armado Parcial usa el Tiempo de Retardo de Armado Parcial para la cuenta regresiva.

El sistema da un tiempo de retardo de entrada/salida cuando se arma o se vuelve a entrar. Por lo general, se utiliza en la ruta de entrada/salida (p. ej., puerta principal/entrada principal), que es una ruta clave para armar/desarmar a través del teclado operativo para los usuarios.



#### Nota

• Puede establecer 2 duraciones de tiempo diferentes en **Opciones del sistema** y **Programación y temporizador**.

• Asegúrese de que el temporizador no supere los 45 segundos para cumplir con EN50131-1.

• Puede configurar el tiempo de retardo de armado en casa para la zona de retardo.

---

#### Zona de pánico

Zona activa de 24 horas, esté armada o no. Informe de alarma de pánico después de la activación. Suele utilizarse en los locales equipados con botón de pánico, detector de humo y detector de rotura de cristales.

#### alarma medica

Zona activa de 24 horas, esté armada o no. Informe de alarma médica después de la activación.

#### Zona de fuego

Zona activa de 24 horas, esté armada o no. Informe de alarma de incendio después de la activación.

#### Zona de Gas

Zona activa de 24 horas, esté armada o no. Informe de alarma de gas después de la activación.

#### Zona de seguimiento

La zona actúa como zona retardada cuando detecta un evento de activación durante el retardo de entrada del sistema, mientras que actúa como zona instantánea en caso contrario.

#### Zona de interruptor de llave

**-Por tiempo de disparo:** cambie el estado de armado y desarmado después de cada disparo. Por ejemplo, en el estado desarmado, si la zona se activa, el área vinculada se armará. Active la zona nuevamente y el área se desarmará.

**-Por estado de zona:** debe elegir armar o desarmar el área vinculada después de que la zona esté

motivado.

En el caso de la alarma de manipulación, la operación de armado y desarmado no se activará.

#### **Zona deshabilitada**

Zona deshabilitada ignorando cualquier evento de alarma. Por lo general, se utiliza para desactivar detectores defectuosos.

#### **Zona 24 horas**

La zona se activa todo el tiempo con salida de sonido/luz cuando ocurre la alarma, ya sea que esté armada o no. Por lo general, se usa en áreas con riesgo de incendio equipadas con detectores de humo y sensores de temperatura.

#### **Zona de tiempo de espera**

La zona se activa todo el tiempo. Cuando esta zona se haya activado o restaurado y exceda el tiempo establecido, se generará una alarma.

Se puede utilizar en lugares equipados con contactos magnéticos que requieren acceso pero solo por un período corto (por ejemplo, la puerta de la caja de la boca de incendios u otra puerta de la caja de seguridad externa).

**-Alarma de zona no activada:** Si la zona no se activa durante el tiempo establecido, se activará la alarma.

**-Alarma en Zona Activada:** Si la zona se activa durante el tiempo establecido, emitirá una alarma.

**-Período de tiempo de reintento:** establezca el período de tiempo de espera.

6. Habilite **Zona cruzada, Alarma silenciosa, etc.** según sus necesidades reales.



#### **Nota**

Algunas zonas no admiten la función. Consulte la zona real para configurar la función.

---

#### **Modo armado**

Si la zona es una zona pública (la zona pertenece a más de un área), puede configurar el modo de armado.

**Y:** Cuando todas las áreas enlazadas estén armadas, la zona se armará. Cuando cualquiera de las áreas vinculadas se desarma, la zona se desarmará.

**O:** Cuando cualquiera de las áreas enlazadas esté armada, la zona se armará. Cuando todas las áreas vinculadas estén desarmadas, la zona se desarmará. Cuando la zona está en alarma, las áreas desarmadas vinculadas con la zona no se pueden armar.

#### **Bypass de Armado Parcial**

La zona se anulará automáticamente en el armado En Casa.

#### **Zona cruzada**

**PD6662 no está habilitado:** debe configurar el intervalo de tiempo combinado.

Cuando se activa la primera zona, el sistema comenzará a cronometrar después de que se restablezca la zona. Si la segunda zona se activa dentro del tiempo establecido, ambas zonas darán alarmas. De lo contrario, no se activará ninguna alarma.

Si la primera zona no se restablece, ambas zonas darán alarmas cuando se active la segunda zona, independientemente de si ha transcurrido el tiempo establecido.

**PD6662 está habilitado:** debe configurar el intervalo de tiempo combinado.

La primera zona dará una alarma cuando se active. Si la primera zona no se restablece y la

se activa la segunda zona, el sistema informará la confirmación de la alarma.

Si se restablece la primera zona, el sistema comenzará a cronometrar. Si la segunda zona se activa dentro del tiempo establecido, el sistema informará la confirmación de la alarma.

Si se restablece la primera zona, el sistema comenzará a cronometrar. Si la segunda zona no se activa dentro del tiempo establecido, no se reportará ninguna información.

#### **Prohibir anular al armar**

Una vez habilitado, no puede anular zonas al armar.

#### **Repicar**

Habilitar el timbre. Normalmente se utiliza para detectores magnéticos de puertas.

#### **alarma silenciosa**

Después de habilitarse, cuando se activa una alarma, solo se cargará el informe y no se emitirá ningún sonido.

#### **Doble golpe**

Después de habilitarlo, se puede configurar el intervalo de tiempo. Si el mismo detector se activa dos veces o de forma continua en un período de tiempo, se activará la alarma.

#### **Tiempo de retardo de sirena**

La sirena se activará inmediatamente (0s) o después del tiempo establecido.

#### **Salida de la puerta final**

Solo los contactos magnéticos tienen esta opción.

Después de habilitar, cuando el usuario use teclados o lectores de etiquetas para armar:

-Armar con fallas está habilitado: Durante la cuenta regresiva de armado, si el contacto magnético se activa y luego se restablece, el proceso de armado terminará inmediatamente después.

restaurando, y el armado está completo.

- Armar con fallas está deshabilitado: si el contacto magnético se activa y luego se restablece, el área enlazada arma inmediatamente la zona retardada.

#### **Activaciones de Límite Swinger (Zona Cableada)**

Cuando el número de veces que se activa el detector de infrarrojos supera el valor establecido, la alarma ya no se activará. (Excepto alarmas antienmascaramiento).

#### **Zona Dual (Zona Cableada)**

Después de habilitado, cuando el transmisor múltiple detecta que todo el circuito de zona de la zona local y la zona extendida está en circuito abierto, ambas zonas activan alarmas de tapa abierta.

7. Si es necesario, vincular una PIRCAM o una cámara para la zona.

8. Haga clic en **Aceptar**.



Después de agregar el transmisor, puede hacer clic en **Dispositivo** y **Zona** y **Inscribir** para agregar una zona cableada. Seleccione el **Modo** de relación como Alámbrico, la **Fuente del dispositivo** como Transmisor único o múltiple, el Canal y haga clic en **Aceptar**.

Después de configurar la zona, puede ingresar a **Mantenimiento** y Estado del **dispositivo** y Estado de la **zona** para ver el estado de la zona.

9. **Opcional:** haga clic en **Dispositivo** y **Zona** y haga clic en Configuración del detector. Puede configurar los parámetros del detector.

Detector Settings

LED

Swinger Limit Activations 3

Polling Rate 5min

OK Cancel

## sonda

La sirena se asocia al AX PRO a través del módulo receptor inalámbrico, y la sirena inalámbrica de 868 Mhz se puede asociar al AX PRO híbrido a través del receptor inalámbrico que se encuentra en la dirección 9.

### Pasos

1. Haga clic en **Dispositivo** y **Sonda** para acceder a la página Sonda.
2. Haga clic  para ingresar a la página Configuración de sonda.

Sounder Settings

Alarm Volume: 2

Alarm Duration: 90 s

Alarm Strobe Flash:

Alarm Buzzer:

Lid Open When Disarmed:

Arm/Disarm Indicator:

Arm/Disarm Buzzer:

Chime Indication:

Buzzer Indicate on Delay Zone:

Intercom Service:

Intercom Duration: 10 min

Polling Rate: 5 min

OK Cancel

3. Configure el nombre de la alarma, el volumen y la duración.



El rango de volumen de alarma disponible es de 0 a 3 (la función varía según el modelo de dispositivo).

El rango de duración de alarma disponible es de 10 a 900 s.

---

4. Seleccione el área vinculada.



¡ Solo se enumerarán las áreas habilitadas.

¡ El periférico recién agregado está vinculado al área 1 de forma predeterminada.

---

5. Seleccione para habilitar la configuración.

**Flash estroboscópico de alarma**

Habilitar luz estroboscópica de alarma.

**Zumbador de alarma**

Activar zumbador de alarma.

**Tapa abierta cuando está desarmado**

Cuando el área enlazada está desarmada, hay una alarma de tapa abierta activada por un periférico, y también se activará la sirena.

#### Indicador de armado/desarmado

Habilitar el indicador LED de armado/desarmado.

#### Activar/desactivar zumbador

Activar alarma de armado/desarmado.

#### Indicador de timbre

Habilitar timbre.

#### Indicador de zumbador en la zona de retardo

Cuando el retraso de entrada o salida del área, además del panel de control, la sirena también emitirá una alarma.

#### Servicio de intercomunicación

Habilitar el servicio de intercomunicación. Solo una sirena puede habilitar esta función.

6. Establezca la **Tasa de sondeo**.

7. Si es necesario, habilite **Registrar sonda inalámbrica**.

8. Haga clic en **Aceptar**.



Después de configurar la sirena, puede hacer clic en **Mantenimiento** y Estado del **dispositivo** y Estado de la **sirena** para ver el estado de la sonda.

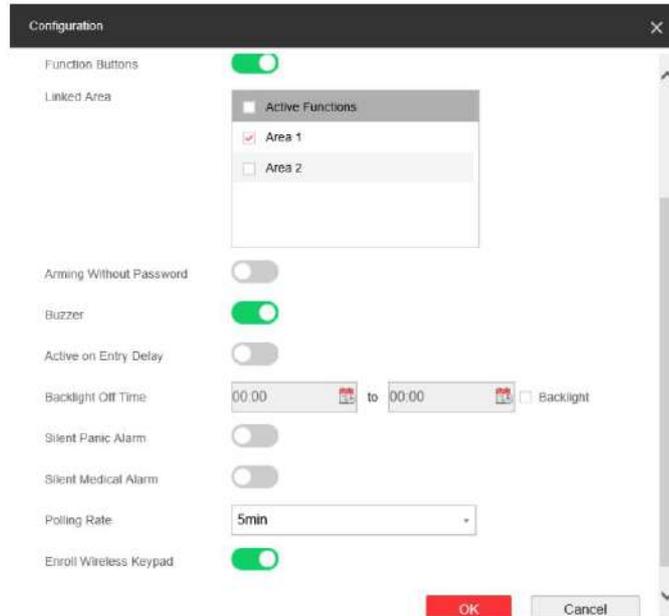
---

## teclado

Puede establecer los parámetros del teclado que está registrado en el AX PRO.

#### Pasos

1. Haga clic en **Dispositivo** y **Teclado** para ingresar a la página.
2. Haga clic  para ingresar a la página de configuración del teclado.



3. Configure el nombre del teclado.
4. Habilite la función de zumbador, alarma de pánico silenciosa, alarma médica silenciosa y botón del teclado.
5. Habilite la función de armado sin contraseña y activo en retardo de entrada.
6. Marque la casilla de verificación **Habilitar** de Tiempo de apagado de la luz de fondo y configure la duración de la luz apagada.
7. Establezca la tasa de sondeo.
8. Seleccione el área vinculada del teclado.

---

 **Nota**

ÿ Solo se enumerarán las áreas habilitadas. ÿ El periférico recién agregado está vinculado al área 1 de forma predeterminada.

---

9. Configure si desea cancelar o no el registro del teclado. Si el enlace está habilitado, el dispositivo ser borrado
10. Haga clic en **Aceptar**.

---

 **Nota**

• Después de configurar el teclado, puede hacer clic en **Mantenimiento** ÿ Estado del **dispositivo** ÿ Estado del **teclado** .  
para ver el estado del teclado. • Puede configurar la contraseña del teclado en la página de **Usuario** ÿ **Gestión de usuarios** ÿ **Operación**.

---

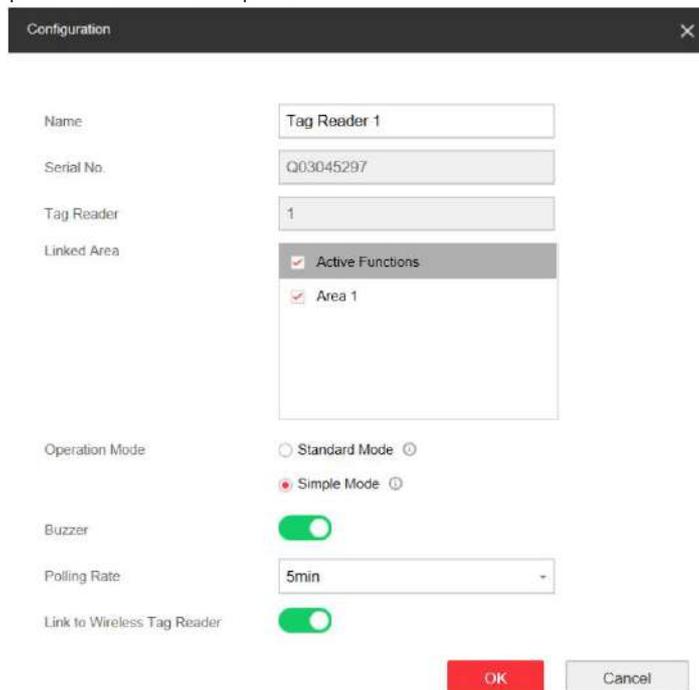
## Lector de etiquetas

Puede establecer los parámetros del lector de etiquetas.

### Pasos

1. Haga clic en **Dispositivo** ÿ **Lector de etiquetas** para ingresar a la página.
2. Haga clic en **Inscribirse**, ingrese el número de serie para agregar un lector de etiquetas.

3. Haga clic en  para editar los parámetros del lector de etiquetas.



4. Edite el nombre del dispositivo.

5. Verifique las áreas vinculadas.

6. Seleccione el modo de operación.

#### Modo estandar

La selección de área y la confirmación de fallas son compatibles al deslizar la etiqueta para armar o desarmar.

#### Modo simple

Sin selección de área y confirmación de falla al deslizar la etiqueta para armar o desarmar.

7. Elija si habilitar el **zumbador**. Después de desactivar el zumbador, no habrá ningún pitido cuando deslizando la etiqueta.

8. Establecer **tasa de sondeo**.

9. **Opcional:** habilite el **enlace al lector de etiquetas inalámbrico**.

10. Haga clic en **Aceptar**.

## Automatización

Puede configurar los parámetros de las salidas de relé que están registradas en el AX PRO.

#### Pasos

1. Haga clic en **Dispositivo** y **Automatización** para ingresar a la página.

2. Haga clic en **Inscribir**, ingrese el número de serie y seleccione el tipo de dispositivo para agregar un dispositivo de salida de relé.

3. Haga clic en  para editar la información del relé.

ÿ Configure el nombre del dispositivo de salida de relé.

ÿ Seleccione el área vinculada para la salida.

### Nota

ÿ Solo se enumerarán las áreas habilitadas.

ÿ El periférico recién agregado está vinculado al área 1 de forma predeterminada.

ÿ La función varía según los diferentes tipos de relé

ÿ Configure el estado del original como Normalmente cerrado o Normalmente abierto.

ÿ Configure el evento para que se active.

ÿ Configure la activación después de ser activado.

ÿ Establezca si vincular o no al dispositivo de salida de relé. Si el enlace está habilitado, el dispositivo será eliminado

### Reloj de repetición

El repetidor puede amplificar señales entre el panel de control y los periféricos.

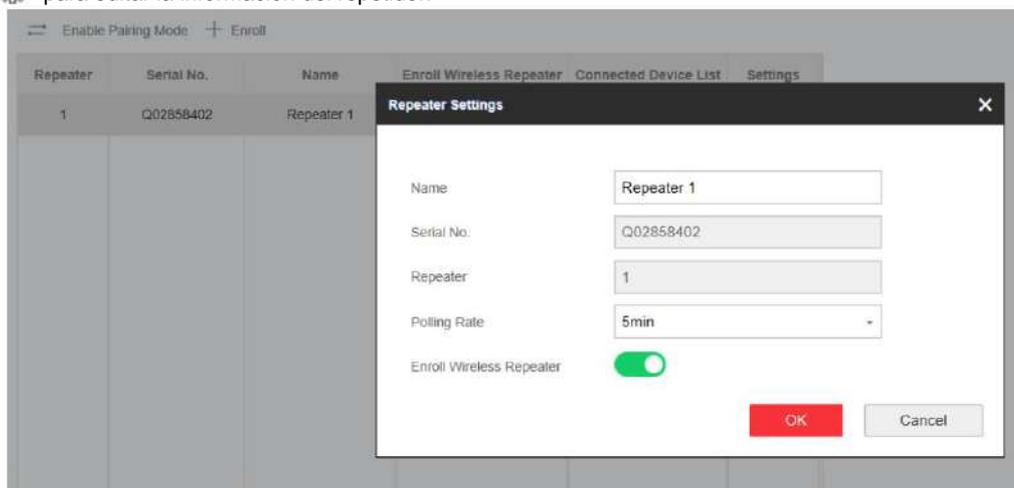
### Pasos

1. Haga clic en **Dispositivo** ÿ **Repetidor** para ingresar a la página.
2. Haga clic en **Inscribir**, ingrese el número de serie y seleccione el tipo de dispositivo para agregar un repetidor.
3. Haga clic en **Entrar en modo** de emparejamiento para que el repetidor entre en el modo de emparejamiento de dispositivos.

4. Cuando la distancia entre el periférico y el panel de control es grande, el repetidor se puede utilizar como estación de transferencia para el emparejamiento. El modo de emparejamiento dura 3 minutos y no se puede interrumpir. Después de que el emparejamiento sea exitoso, se mostrará una lista de dispositivos conectados.



5. Haga clic en  para editar la información del repetidor.

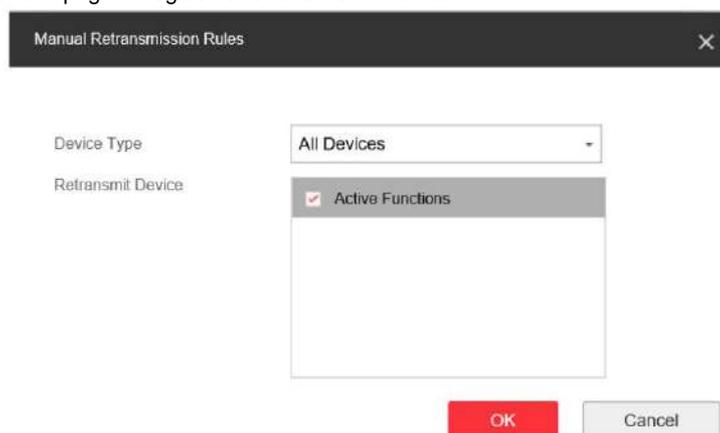


• Configure el nombre del repetidor.

• Configure la tasa de sondeo del repetidor.

• Configure si cancelar o no la inscripción del repetidor. Si el enlace está habilitado, el dispositivo será borrado.

6. Haga clic en  para ingresar a la página Reglas de retransmisión manual.



• Seleccione el **tipo de dispositivo**.

• Comprobar **funciones activas**.

ÿ Haga clic en **Aceptar**, luego los dispositivos se pueden retransmitir manualmente.

## Transmisor

Puede configurar los parámetros del transmisor.

### Pasos

1. Haga clic en **Dispositivo** ÿ **Transmisor** para ingresar a la página.
2. Haga clic en **Inscribir**, ingrese el número de serie y seleccione el modelo de dispositivo para agregar un transmisor.
3. Haga clic **para** editar la información del transmisor.

Parameter Setting

Transmitter: 1

Name: Multi Transmitter 1

Serial No.: Q86860014

Polling Rate: 5min

Linked Area:

Active Functions:

- Area 1
- Area 2

Enroll Wireless Transmi...

OK Cancel

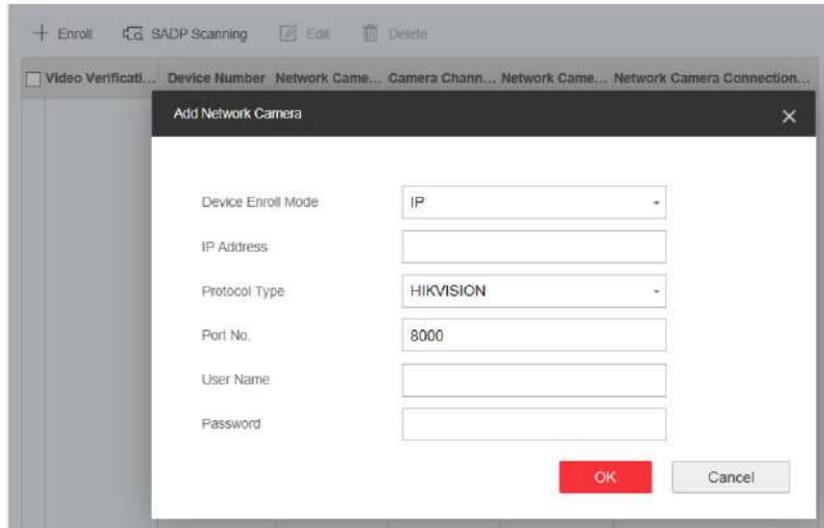
4. Configure el nombre del transmisor.
5. Establezca la tasa de sondeo del transmisor.
6. Habilite **Registrar transmisión inalámbrica**.
7. Haga clic en **Aceptar**.

## Cámara de red

Puede agregar cámaras de red en el sistema.

### Pasos

1. Haga clic en **Dispositivo** ÿ **Cámara de red** para ingresar a la página de administración de cámaras de red.



2. Haga clic en **Registrar** e ingrese la información básica de la cámara, como la dirección IP y el número de puerto, y seleccione el tipo de protocolo.

3. Introduzca el nombre de usuario y la contraseña de la cámara.

#### Escaneo SADP

Escanee todas las cámaras de red en la misma LAN. Aparecerá una lista después de escanear. Puede verificar directamente para agregar cámaras en la lista.

4. Haga clic en **Aceptar**.

5. **Opcional:** haga clic en **Editar** o **Eliminar** para editar o eliminar la cámara seleccionada.

## 5.3.3 Gestión de permisos

### Agregar/Editar/Eliminar llavero

Puede agregar un mando a distancia al AX PRO y puede controlar el AX PRO a través del mando a distancia. También puede editar la información del llavero o eliminar el llavero del AX PRO.

#### Pasos

1. Haga clic en **Dispositivo** y **Llavero** para ingresar a la página de Administración de llaveros.

2. Haga clic en **Inscribir** y presione cualquier tecla en el control remoto.

3. Establezca los parámetros del llavero.

#### Nombre

Personaliza un nombre para el llavero.

#### Configuración de permisos

Marque diferentes elementos para asignar permisos.

#### Configuración de tecla única

Seleccione de la lista desplegable para configurar las funciones de la tecla I y la tecla II

### Configuración de teclas de combinación

Seleccione de la lista desplegable para configurar las funciones de las teclas de combinación.

4. Haga clic en **Aceptar**.

5. Opcional: haga clic  para editar la información del llavero.

en 6. Opcional: elimine un único mando o marque varios mandos y haga clic en **Eliminar** para eliminar los mandos en lote.



La comunicación de dispositivos inalámbricos como llaveros fue identificada por el número SN, que será encriptado durante la transmisión. El número SN iba del carácter Q a la Z y le seguían 8 dígitos, como Q02235774. Permitiendo un número máximo de 100,000,000 (10 a la potencia de 8 [dígitos]).

---

### Añadir/Editar/Eliminar etiqueta

Puede agregar una etiqueta al AX PRO y puede usar la etiqueta para armar/desarmar la zona. También puede editar la información de la etiqueta o eliminar la etiqueta del AX PRO.



La comunicación de la etiqueta se identificó mediante el número SN, que se cifrará durante la transmisión. El número SN estaba a la cabeza con 32 dígitos, y se pueden identificar como máximo 4,294,967,296 números SN.

---

### Pasos

1. Haga clic en **Dispositivo** y **Etiqueta** para ingresar a la página de administración.
2. Haga clic en **Inscribirse** y coloque una etiqueta en el área de etiquetas del AXE PRO.
3. Personalice un nombre para la etiqueta en la ventana emergente.
4. Seleccione el tipo de etiqueta y el área vinculada a la etiqueta.
5. Seleccione el permiso para la etiqueta.



Debe asignar al menos un permiso para la etiqueta.

---

6. Haga clic en **Aceptar** y la información de la etiqueta se mostrará en la lista.



La etiqueta admite al menos 20y000 números de serie.

---

7. Opcional: haga clic en  puede cambiar el nombre de la etiqueta.

8. Opcional: elimine una sola etiqueta o marque varias etiquetas y haga clic en **Eliminar** para eliminar etiquetas en lote.

## 5.3.4 Gestión de vídeos

Puede agregar dos cámaras de red al AX PRO y vincular la cámara con la zona seleccionada para el monitoreo de video. También puede recibir y ver el video del evento a través del cliente y el correo electrónico.

### Agregar cámaras al AX PRO

#### Pasos

1. Haga clic en **Dispositivo** y **Cámara de red** para ingresar a la página de administración de cámaras de red.

2. Haga clic en **Registrar** e ingrese la información básica de la cámara, como la dirección IP y el número de puerto, y seleccione el tipo de protocolo.
3. Introduzca el nombre de usuario y la contraseña de la cámara.

#### Escaneo SADP

Escanee todas las cámaras de red en la misma LAN. Aparecerá una lista después de escanear. Puede verificar directamente para agregar cámaras en la lista.

4. Haga clic en **Aceptar**.

5. **Opcional:** haga clic en **Editar** o **Eliminar** para editar o eliminar la cámara seleccionada.

### Vincular una cámara con la zona

#### Pasos

1. Haga clic en **Dispositivo** y **Zona** para ingresar a la página de configuración.
2. Seleccione una zona en la que desee incluir monitoreo de video y haga clic en 3. Seleccione 

#### Vincular cámara.

4. Haga clic en **Aceptar**.



Solo si la zona está vinculada con una cámara de red, el correo electrónico de alarma se adjuntará con el video de alarma.

---

## Establecer parámetros de vídeo

### Pasos

1. Haga clic en **Dispositivo** y **Cámara de red** y **Parámetros de video** para ingresar a la página.

2. Seleccione una cámara y configure los parámetros de video.

#### Tipo de

transmisión Transmisión principal: se utiliza en la grabación y la vista previa de alta definición, tiene una alta resolución, tasa de codificación y calidad de imagen.

Sub-Stream: se utiliza para transmitir imágenes de red y obtener una vista previa como una transmisión de video con características de menor resolución, tasa de bits y calidad de imagen.

#### Tipo de tasa de bits

Seleccione el tipo de tasa de bits como constante o variable.

#### Resolución

Seleccione la resolución de la salida de video.

#### Bitrate de vídeo

El valor más alto corresponde a la calidad de video más alta, pero se requiere un mejor ancho de banda.

#### Post-grabación/Pre-grabación

Configure el tiempo de grabación de video antes y después de la alarma.

### 5.3.5 Configuración de área

#### Ajustes básicos

Puede vincular zonas al área seleccionada.

##### Pasos

1. Haga clic en **Área** y **Configuración básica** para ingresar a la página.
2. Seleccione un área.
3. Marque **Habilitar**.
4. Haga clic en **Editar zona vinculada** y **Editar periférico vinculado** para comprobar las zonas o periféricos vinculados.
5. Haga clic en **Guardar** para completar la configuración.

### 5.3.6 Configuración de comunicación

#### Red cableada

Puede configurar la dirección IP del dispositivo y otros parámetros de red.

##### Pasos

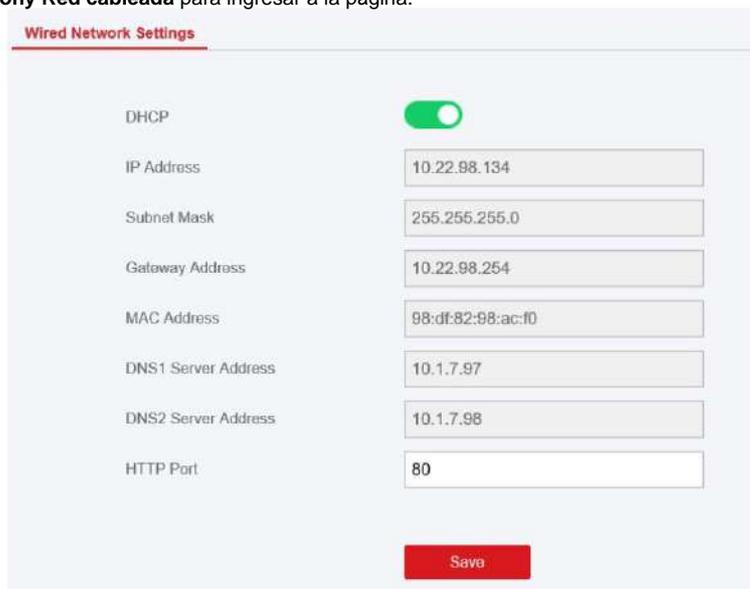


Nota

Las funciones variaron según el modelo del dispositivo.

---

1. Haga clic en **Comunicación** y **Red cableada** para ingresar a la página.



DHCP	<input checked="" type="checkbox"/>
IP Address	<input type="text" value="10.22.98.134"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Gateway Address	<input type="text" value="10.22.98.254"/>
MAC Address	<input type="text" value="98:df:82:98:ac:f0"/>
DNS1 Server Address	<input type="text" value="10.1.7.97"/>
DNS2 Server Address	<input type="text" value="10.1.7.98"/>
HTTP Port	<input type="text" value="80"/>

Save

2. Configure los parámetros.

– Configuración automática: habilite **DHCP** y configure el puerto HTTP.

– Configuración manual: **DHCP** deshabilitado y configuración de **dirección IP, máscara de subred, dirección de puerta de enlace, DNS Dirección del servidor.**

3. **Opcional:** configure la dirección del servidor DNS correcta si el dispositivo necesita visitar el servidor Hik-Connect a través de un nombre de dominio.

4. Haga clic en **Guardar**.

## Wifi

Puede configurar los parámetros de Wi-Fi si hay redes Wi-Fi seguras y confiables cerca.

### Pasos

1. Haga clic en **Comunicación** y **Wi-Fi** para ingresar a la página de Wi-Fi.

**Wi-Fi Settings** WLAN

Status of STA/AP Switch

Switch Mode: STA Mode

Wi-Fi

SSID Wi-Fi: TP-LINK\_96D6

Wi-Fi Password:

Encryption Mode: WPA2-personal

Network List

Name	Channel...	Signal S...	Encryption Mode	Operation
TP-LINK_96D6	1	70	WPA2-personal	Disconnect
TP-LINK_DD63	11	70	WPA2-personal	Connect
HIK-Office	6	70	WPA2-personal	Connect
linksys_test	8	61	WPA2-personal	Connect
HUAWEI-0404LN	6	58	WPA2-personal	Connect
OPPO Reno	5	58	WPA2-personal	Connect
HAP_Q12345678	11	54	WPA2-personal	Connect

2. Conéctese a una red Wi-Fi.

– Conexión manual: ingrese el **SSID Wi-Fi** y la **contraseña de Wi-Fi**, seleccione **Modo de cifrado** y haga clic en **Ahorrar**.

– Seleccionar de la lista de redes: seleccione una red Wi-Fi de destino de la lista de redes. Haga clic en **Conectar** e ingrese Contraseña de Wi-Fi y haga clic en **Conectar**.

3. Haga clic en **WLAN** para ingresar a la página WLAN.

Wi-Fi Settings **WLAN**

DHCP

IP Address

Subnet Mask

Gateway Address

MAC Address

DNS1 Server Address

DNS2 Server Address

4. Establezca la **dirección IP**, la **máscara de subred**, la dirección de la **puerta de enlace** y la **dirección del servidor DNS**.



**Nota**

Si habilita DHCP, el dispositivo obtendrá los parámetros de Wi-Fi automáticamente.

---

5. Haga clic en **Guardar**.

## Red de datos móviles

Configure los parámetros de la red celular si inserta una tarjeta SIM dentro del dispositivo. Mediante el uso de la red celular, el dispositivo puede cargar notificaciones de alarma al centro de alarmas.

### Antes de que empieces

Inserte una tarjeta SIM en la ranura para tarjeta SIM del dispositivo.

### Pasos

1. Haga clic en **Comunicación** y **Red de datos móviles** para acceder a la configuración de la red de datos móviles.  
página.

Cellular Data Network Settings

Enable

**SIM Card1**

Access Number   
For accessing private network, you need to enter the accessing number.

User Name

Access Password

APN

MTU

PIN Code

Data Usage Limit

Data Used This Month  M

Data Limited per Month  M

Network Connection Test

**SIM Card2**

Access Number   
For accessing private network, you need to enter the accessing number.

User Name

---

 **Nota**

Solo el usuario de la tarjeta SIM de la red privada necesita ingresar el número de acceso.

---

2. Habilite la función.
3. Configure los parámetros de la red de datos móviles.

**Número de acceso**

Introduzca el número de marcación del operador.

---

 **Nota**

Solo el usuario de la tarjeta SIM de la red privada necesita ingresar el número de acceso.

---

**Nombre de usuario**

Pregúntele al operador de red e ingrese el nombre de usuario.

**Contraseña de acceso**

Pregúntele al operador de red e ingrese la contraseña.

**APN**

Pídale al operador de red que obtenga la información de APN e ingrese la información de APN.

**Límite de uso de datos**

Puede habilitar la función y establecer el umbral de datos cada mes. Si el uso de datos supera el umbral configurado, se activará una alarma y se cargará en el centro de alarmas y el cliente móvil.

#### Datos utilizados este mes

Los datos utilizados se acumularán y se mostrarán en este cuadro de texto.

#### Prueba de conexión de red

Haga clic en Detección para comprobar el estado de la conexión de red.

4. Haga clic en **Guardar**.

### Centro de alarma

Puede configurar los parámetros del centro de alarmas y todas las alarmas se enviarán a la alarma configurada centro.

#### Pasos

1. Haga clic en **Comunicación** y **Centro de recepción de alarmas** para ingresar a la página Centro de recepción de alarmas.

The screenshot shows the configuration interface for the alarm center (ARC1). It includes the following fields and controls:

- Enable:** A green toggle switch is turned on.
- Protocol Type:** A dropdown menu set to 'ADM-CID'.
- GMT:** A green toggle switch is turned on.
- Address Type (Alarm Receiver Server):** A dropdown menu set to 'IP'.
- Server Address (Alarm Receiver Server):** A text input field containing '0.0.0.0'.
- Port No. (Alarm Receiver Server):** A text input field containing '0'.
- Account Code:** An empty text input field.
- Transmission Mode:** A dropdown menu set to 'TCP'.
- Impulse Counting Time:** A text input field containing '20' with a 's' unit indicator.
- Attempts:** A text input field containing '3'.
- Polling Rate:** A text input field with a 's' unit indicator and an 'Enable' checkbox.
- Periodic Test:** A grey toggle switch is turned off.
- Companies:** A dropdown menu set to 'None'.
- Intruder Verification as a Service:** A grey toggle switch is turned off.

A red 'Save' button is located at the bottom center of the configuration area.

2. Seleccione el **CRA** como **1** o **2** para la configuración y deslice el control deslizante para habilitar la alarma seleccionada centro receptor.

---

#### Nota

Solo si el centro receptor de alarmas 1 (ARC1) está habilitado, puede configurar el centro receptor de alarmas 2 como el **canal de respaldo** y editar los parámetros del canal.

---

3. Seleccione el **tipo de protocolo** como **ADM-CID, ISUP, SIA-DCS, \*SIA-DCS, \*ADM-CID, CSV-IP, FSK**

**Módulo, Módulo RDC** o **Módulo IDS** para configurar el modo de carga.

---

 **Nota**

Protocolo estándar DC-09

ADM-CID: el método de presentación de datos de DC-09 es CID, que no está encriptado y solo para cargar informes de alarma.

\*ADM-CID: el método de presentación de datos de DC-09 es CID, que está encriptado y solo para cargar informes de alarma.

SIA-DCS: el método de presentación de datos de DC-09 es DCS (también llamado protocolo SIA), que no está encriptado y solo para cargar informes de alarma.

\*SIA-DCS: el método de presentación de datos de DC-09 es DCS (también llamado protocolo SIA), que está encriptado y solo para cargar informes de alarma.

---

**ADM-CID** o **SIA-DCS**: debe seleccionar el **tipo de receptor de alarma** como **IP** o **nombre de dominio** e ingresar la dirección IP, el número de puerto, el código de cuenta, el tiempo de conteo de impulsos, los intentos y la tasa de sondeo.

**Verificación de intrusos como servicio**

Cuando el panel de control cargue la información de la alarma, devolverá la dirección de la imagen y el video para que usted los vea.

---

 **Nota**

Establezca la tasa de sondeo con un rango de 10 a 3888000 segundos.

---

**ISUP, CSV-IP, FSK y RDC**: no es necesario configurar los parámetros del protocolo.

**IDS**: Debe ingresar el código de cuenta.

**\*SIA-DCS** o **\*ADM-CID** Debe seleccionar el **tipo de receptor de alarma** como **IP** o **nombre de dominio** e ingresar la dirección IP, el número de puerto, el código de cuenta, el tiempo de conteo de impulsos, los intentos, la tasa de sondeo, la aritmética de cifrado, la longitud de la contraseña y el secreto llave.

---

 **Nota**

Establezca la tasa de sondeo con un rango de 10 a 3888000 segundos.

---

4. Haga clic en **Guardar**.

## Use PIRCAM para cargar imágenes o videos

Puede habilitar la función PIRCAM para cargar imágenes o videos.

1. Subir fotos

Puede elegir cargar de 1 a 20 imágenes.

(1) Haga clic en **Comunicación** y **Centro de recepción de alarmas** para ingresar a la página.

(2) Deslice el control deslizante para habilitar el centro receptor de alarmas seleccionado.

(3) Seleccione el **Tipo de protocolo** como **SIA-DCS**.

(4) Seleccione las **Empresas** como **Empresa Receptora de Alarmas Francesa**.

(5) Haga clic en **Guardar**.

Destination IP or Host Name	URL	Protocol	Port	Test
0.0.0.0	/	HTTP	80	Test
0.0.0.0	/	HTTP	80	Test

(6) Configure los parámetros de SMTP o FTP.

Configure los parámetros de SMTP: haga clic en

**Comunicación y Notificación por correo electrónico.**

Habilite **los eventos de verificación de video** y configure los parámetros correspondientes. Para obtener más información, consulte Notificación por correo electrónico. Haga clic en **Guardar**.

Configure los parámetros de FTP: haga clic en

**Comunicación y FTP** para ingresar a la página Configuración de FTP.

Deslice el control deslizante para habilitar FTP y establezca los parámetros correspondientes. Para obtener más información, consulte FTP.

Haga clic en **Guardar**.

FTP Settings

FTP Type: Preferred FTP

Enable FTP:

Address Type: IP

FTP Server:

Port No.: 21

Protocol Type: FTP

Enable Anonymity:

User Name:

Password:

Directory Structure: Save in Root Directory

Parent Directory: Custom

Secondary Directory: Custom

Save

## 2. Subir vídeos

En esta condición, cuando la PIRCAM esté configurada para capturar más de dos imágenes, se cargarán videos.

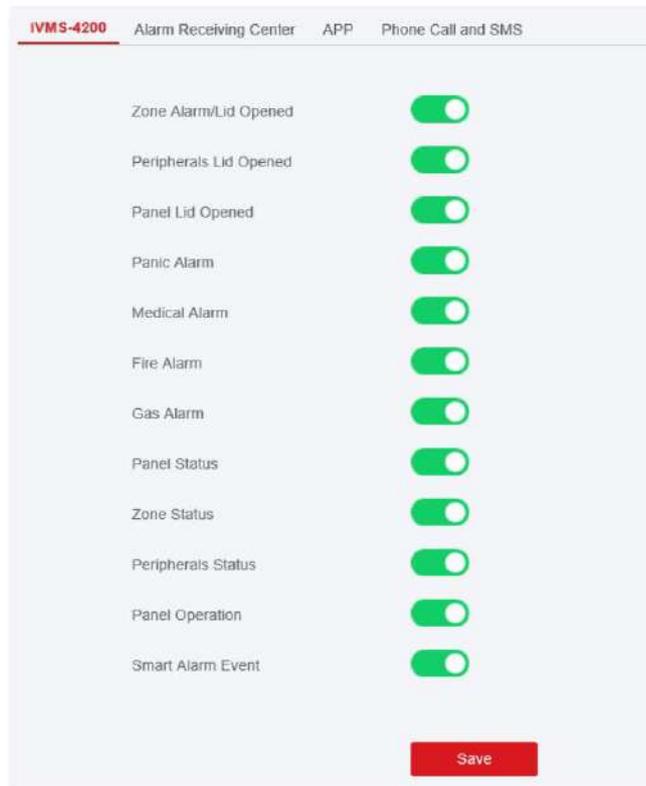
- (1) Haga clic en **Comunicación** y **Centro de recepción de alarmas** para ingresar a la página.
- (2) Deslice el control deslizante para habilitar el centro receptor de alarmas seleccionado.
- (3) Seleccione el **Tipo de protocolo** como **SIA-DCS**.
- (4) Haga clic en **Guardar**.
- (5) Configure los parámetros SMTP o FTP de la misma manera que Subir fotos.

## Empuje de notificación

Cuando se activa una alarma, si desea enviar la notificación de alarma al cliente, al centro de alarmas, a la nube o al teléfono móvil, puede configurar los parámetros de notificación automática.

### Pasos

1. Haga clic en **Comunicación** y **Notificación de tipos de eventos**.



2. Habilite la notificación de destino.

#### **Alarma de zona/tapa abierta**

El dispositivo enviará notificaciones cuando se active la alarma de la zona (en el cliente web, el cliente de software o el cliente móvil) o cuando se active o restablezca la alarma de los periféricos de la zona.

#### **Tapa de periféricos abierta**

El dispositivo enviará notificaciones cuando se active o restablezca la alarma de tapa abierta de cualquier periférico.

#### **Tapa del panel abierta**

El dispositivo enviará notificaciones cuando se active o restablezca la alarma de tapa abierta del panel de control.

#### **Alarma de pánico**

El dispositivo enviará notificaciones cuando se active o restablezca la alarma de pánico en los teclados o llaveros.

#### **alarma medica**

El dispositivo enviará notificaciones cuando se active la alarma médica en los teclados.

#### **Alarma de incendios**

El dispositivo enviará notificaciones cuando se active la alarma de incendio en los teclados o cuando un usuario presione la tecla de alarma de incendio en el teclado.

#### alarma de gas

El dispositivo enviará notificaciones cuando se active la alarma de gas en los teclados.

#### Estado del panel

El dispositivo enviará notificaciones cuando cambie el estado del sistema del panel de control.

#### Estado de zona

El dispositivo enviará notificaciones cuando se cambie el estado de cualquier zona.

#### Estado de los periféricos

El dispositivo enviará notificaciones cuando se cambie el estado de cualquier periférico.

#### Operación del panel

El dispositivo enviará notificaciones cuando el usuario opere el panel de control.

#### Evento de alarma inteligente

El dispositivo enviará notificaciones cuando se active la alarma en las cámaras de red.

3. Para el **Centro de recepción de alarmas**, debe seleccionar el número del centro antes de la configuración.

4. Para la **aplicación**, debe verificar si es una alarma importante.

#### Alarma importante

Cuando la aplicación está en modo silencioso, los elementos de pulsación configurados como alarma importante seguirán reproduciendo las indicaciones de voz correspondientes. Las alarmas de incendio, médicas y de pánico están configuradas como alarmas importantes de manera predeterminada.

Event	Enabled	Important Alarm
Zone Alarm/Lid Opened	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Peripherals Lid Opened	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Panel Lid Opened	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Panic Alarm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Medical Alarm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Fire Alarm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Gas Alarm	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Smart Alarm Event	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Panel Status	<input checked="" type="checkbox"/>	
Zone Status	<input checked="" type="checkbox"/>	
Peripherals Status	<input checked="" type="checkbox"/>	
Panel Operation	<input checked="" type="checkbox"/>	

Save

5. **Opcional:** si desea enviar las notificaciones de alarma al cliente móvil, debe configurar **Teléfono**

**Parámetros de llamadas y SMS .**

- (1) Configure el **índice de teléfonos** móviles y el **número de teléfono móvil**.
- (2) Verifique la **llamada de voz** en la página del **teléfono** .
- (3) Seleccione el tiempo de **intervalo de filtrado** y el **número de llamadas**.
- (4) Comprobar **SMS** en la página de **mensajes** .
- (5) Seleccione áreas que tengan permiso para armar, desarmar o borrar alarmas.

**Sugerencia general**

Puede importar **Common Voice**. Cuando se active la alarma, su voz personalizada se agregará al comienzo del contenido del teléfono marcado por el sistema.

---

 **Nota**

Solo se admite el formato WAV, hasta 512 KB y 15 s.

---

Puede ingresar **Mensaje común**. Cuando se active la alarma, su contenido personalizado se agregará al comienzo del mensaje enviado por el sistema.

6. Haga clic en **Guardar**.



Para notificación de teléfono móvil:  
y Debe presionar y Se requiere \* para terminar la llamada.  
agregar el código de control al ingresar el número de teléfono móvil.

---

#### Servicio de almacenamiento en la nube

Si desea registrar el dispositivo en el cliente móvil para la configuración remota, debe configurar los parámetros de registro del cliente móvil.

#### Antes de que empieces

- Conectar el dispositivo a la red a través de una conexión por cable, una conexión de acceso telefónico o Wi-Fi conexión.
- Configure la dirección IP del dispositivo, la máscara de subred, la puerta de enlace y el servidor DNS en la LAN.

#### Pasos

1. Haga clic en **Comunicación y Servicio en la nube** para ingresar a la página Configuración de registro de Hik-Connect.

The screenshot shows the 'Cloud Service Settings' interface. It includes a 'Register to Hik-Connect' checkbox which is checked. The 'Hik-Connect Connection Status' is 'Online'. The 'Custom Server Address' toggle is turned off. The 'Server Address' field is masked with a checkered pattern. The 'Communication Mode' is set to 'Wired Network & Wi-Fi Priority'. The 'Verification Code' field is masked with asterisks, with a note below stating: 'The code should contain 6 to 12 characters (it is recommended to be more than 8 characters and the combination of numeric and letter)'. The 'Periodic Test' toggle is turned on, and the 'Periodic Test Interval' is set to 60 seconds. A red 'Save' button is located at the bottom of the settings panel.

2. Marque **Registrarse en Hik-Connect**.



De forma predeterminada, el servicio Hik-Connect del dispositivo está habilitado.

---

Puede ver el estado del dispositivo en el servidor de Hik-Connect ([www.hik-connect.com](http://www.hik-connect.com)).

3. Habilite **la dirección del servidor personalizado**.

La dirección del servidor ya se muestra en el cuadro de texto Dirección del servidor.

4. Seleccione un modo de comunicación de la lista desplegable de acuerdo con el método de comunicación del dispositivo actual.

#### **Prioridad de red alámbrica y Wi-Fi** El orden

de prioridad de conexión de mayor a menor es: red alámbrica, Wi-Fi, red de datos móviles.

#### **Con cable y Wi-Fi**

El sistema seleccionará primero la red cableada. Si no se detecta una red cableada, seleccionará la red Wi-Fi.

#### **Red de datos móviles**

El sistema seleccionará solo la red de datos móviles.

5. Opcional: cambie el código de verificación.



- De forma predeterminada, el código de verificación se muestra en el cuadro de texto.
  - El código de verificación debe contener de 6 a 12 letras o dígitos. Por razones de seguridad, un 8- Se sugiere una contraseña de caracteres que contenga dos o más de los siguientes tipos de caracteres: mayúsculas, minúsculas y dígitos.
- 

6. Habilite **la prueba periódica**. Ingrese el intervalo de prueba periódica.

7. Haga clic en **Guardar**.

#### **Notificación por correo electrónico**

Puede enviar el video o evento de alarma al correo electrónico configurado.

#### **Pasos**

1. Haga clic en **Comunicación y Notificación por correo electrónico** para ingresar a la página.
2. Seleccione y active **Correo electrónico 1**.
3. Habilite **los eventos de verificación de video y la autenticación del servidor**.
4. Introduzca la información del remitente.



Se recomienda utilizar Gmail y Hotmail para el envío de correos.  
Solo si la zona está vinculada con una cámara de red, el correo electrónico de alarma se adjuntará con el video de alarma.

---

5. Ingrese la información del receptor.
6. Haga clic en **Prueba de dirección del receptor** y asegúrese de que la dirección sea correcta.
7. Haga clic en **Guardar**.
8. Opcional: configure el **correo electrónico 2** en el mismo orden. Puede elegir si configurar el correo electrónico 2 como buzón de respaldo.

 **Nota**

Las reseñas de videos y fotos se enviarán a ambos buzones. Si el Correo electrónico 2 está configurado como un buzón de respaldo, el sistema enviará correos electrónicos al Correo electrónico 2 solo si el Correo electrónico 1 no se recibe.

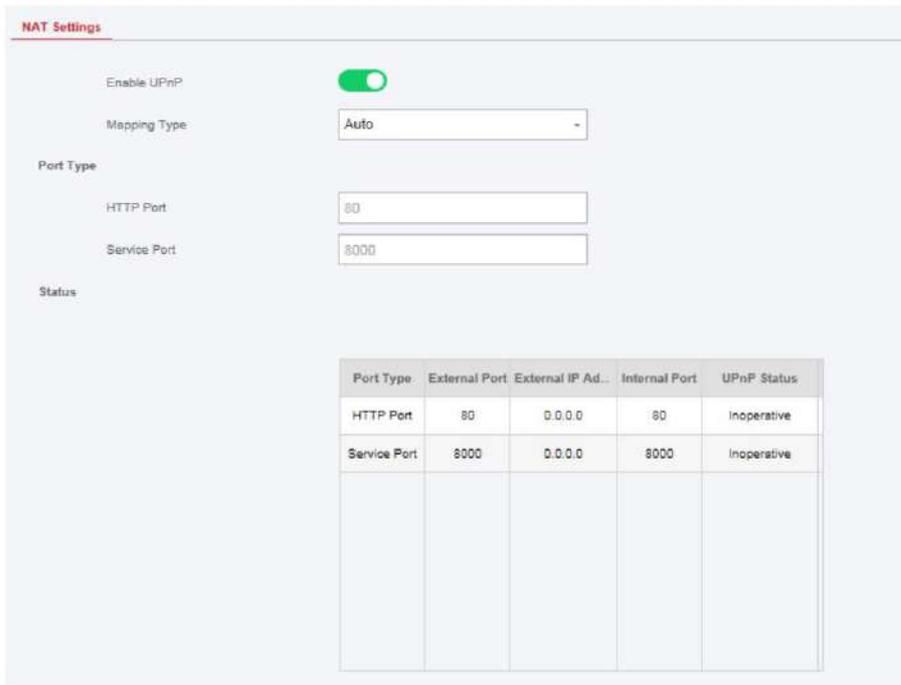
## NAT

Universal Plug and Play (UPnP™) es una arquitectura de red que proporciona compatibilidad entre equipos de red, software y otros dispositivos de hardware. El protocolo UPnP permite que los dispositivos se conecten sin problemas y simplifica la implementación de redes en entornos domésticos y corporativos.

Habilite la función UPnP, y no necesita configurar la asignación de puertos para cada puerto, y el dispositivo está conectado a la red de área amplia a través del enrutador.

### Pasos

1. Haga clic en **Comunicación** y **NAT** para ingresar a la página.



The screenshot shows the 'NAT Settings' page. It includes a toggle for 'Enable UPnP' which is turned on. Below it, 'Mapping Type' is set to 'Auto'. Under the 'Port Type' section, 'HTTP Port' is set to 80 and 'Service Port' is set to 8000. At the bottom, there is a table with the following data:

Port Type	External Port	External IP Ad...	Internal Port	UPnP Status
HTTP Port	80	0.0.0.0	80	Inoperative
Service Port	8000	0.0.0.0	8000	Inoperative

2. Arrastre el control deslizante para habilitar UPnP.
3. **Opcional:** Seleccione el tipo de asignación como **Manual** y establezca el puerto HTTP y el puerto de servicio.
4. Haga clic en **Guardar** para completar la configuración .

## FTP

Puede configurar el servidor FTP para guardar video de alarma.

### Pasos

1. Haga clic en **Comunicación** y **FTP** para ingresar a la página.

## 2. Configurar los parámetros de FTP

### Tipo FTP

Configure el tipo de FTP como preferido o alternativo.

### Tipo de protocolo

FTP y SFTP son seleccionables. La carga de archivos se cifra mediante el protocolo SFTP.

### Servidor FTP y número de puerto

La dirección del servidor FTP y el puerto correspondiente.

### Nombre de usuario y contraseña

El usuario de FTP debe tener permiso para cargar imágenes. Si el servidor FTP admite la carga de imágenes por parte de usuarios anónimos, puede marcar Anónimo para ocultar la información de su dispositivo durante la carga.

### Estructura del directorio

La ruta de guardado de las instantáneas en el servidor FTP.

## Servicio de intercomunicación

Puede configurar el servicio de intercomunicación para una sirena de intercomunicación.

### Antes de que empieces

Primero debe registrar un zumbador de intercomunicador.

Solo se puede configurar una sirena como sirena de intercomunicación.

### Pasos

1. Haga clic en **Comunicación** y **Servicio de intercomunicación** para ingresar a la página.
2. Deslice para habilitar la función.
3. Configure el tipo de intercomunicador.

SORBO

El panel de control utilizará el servidor ARC y SIP.

### Receptor IP Pro

El panel de control usará el servicio en la nube del usuario.

4. Seleccione una sonda y haga clic en **Guardar**.

## 5.3.7 Mantenimiento

### Información del dispositivo

Puede ver el nombre del dispositivo y otra información.

Haga clic en **Mantenimiento y Información del dispositivo** para ingresar a la página.

Puede ver el modelo del dispositivo, el número de serie del dispositivo, la versión de firmware del dispositivo, la versión web o hacer clic en **Acerca de** y **Ver licencias** para ver las licencias de software de origen.

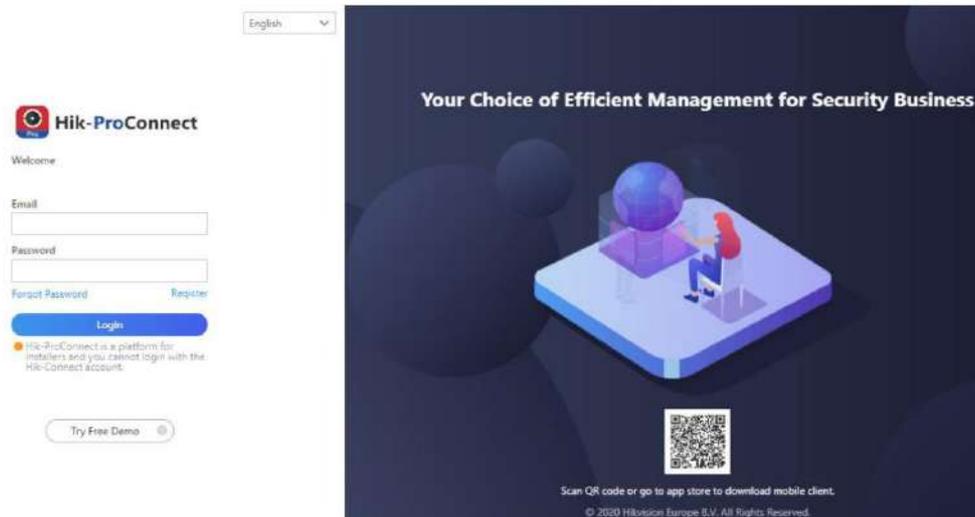
Puede ir a **Sistema y Configuración** del sistema para cambiar el nombre del dispositivo.

### Actualización de dispositivo

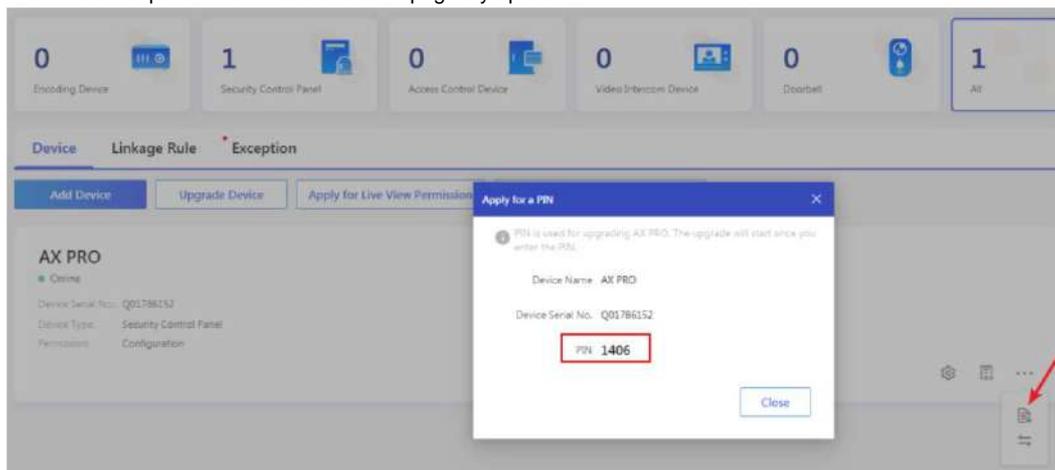
### Obtener PIN de fabricación

Para actualizar el dispositivo, se necesita un PIN de fabricación para la autenticación. El PIN de fabricación solo puede obtenerse del servicio Hik-ProConnect, lo que significa que el instalador, autorizado por el administrador en el nivel de acceso 2, ha autorizado el acceso en el nivel 4. El PIN de fabricación solo puede funcionar una vez.

### y Obtener PIN del servicio Hik-ProConnect



Inicie sesión con la cuenta del instalador e ingrese a la página del dispositivo que desea actualizar. Hacer clic **Menú Más** en la parte inferior derecha de la página y aplica un PIN.



### ¿ Obtenga el PIN del soporte técnico de HIKVISION

Es mejor usar el escritorio remoto para acceder al cliente web local del panel de control. El PIN se autorizará de acuerdo con el procedimiento estándar de soporte técnico.

### Actualización de firmware

#### ¿ Actualización del panel de control: 1.

Haga clic en **Mantenimiento** ¿ Actualización del **dispositivo** ¿ **Actualización del panel de control** para ingresar a la página.

2. Haga clic en **Ver** para encontrar el archivo de firmware con el nombre digicap.dav.

3. Haga clic en **Actualizar** para completar. ¿

#### **Actualización de detectores y periféricos:** 1. Haga

clic en **Mantenimiento** ¿ **Actualización de dispositivos** ¿ **Actualización de detectores y periféricos** para ingresar a la página.

2. Seleccione el Tipo de actualización y el Periférico.

3. Haga clic en **Ver** para buscar el archivo de actualización del firmware.

4. Haga clic en **Actualizar** para completar.



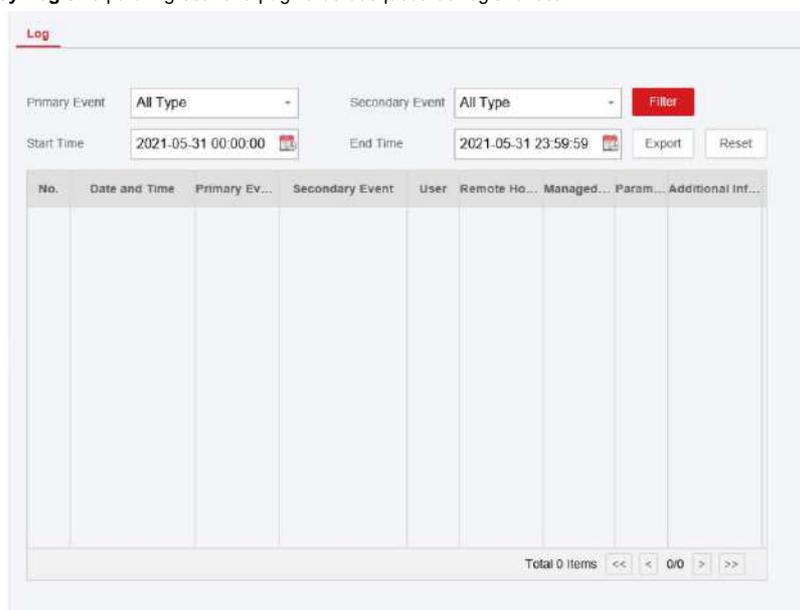
Tanto los usuarios como la información de configuración se conservarán después de que finalice la actualización.

---

### Búsqueda de registro local

Puede buscar el registro en el dispositivo.

Haga clic en **Mantenimiento** ¿ **Registro** para ingresar a la página de búsqueda de registro local.



Seleccione un evento principal y un evento secundario de la lista desplegable, establezca la hora de inicio y finalización del registro y haga clic en **Filtrar**. Toda la información de registro filtrada se mostrará en la lista.

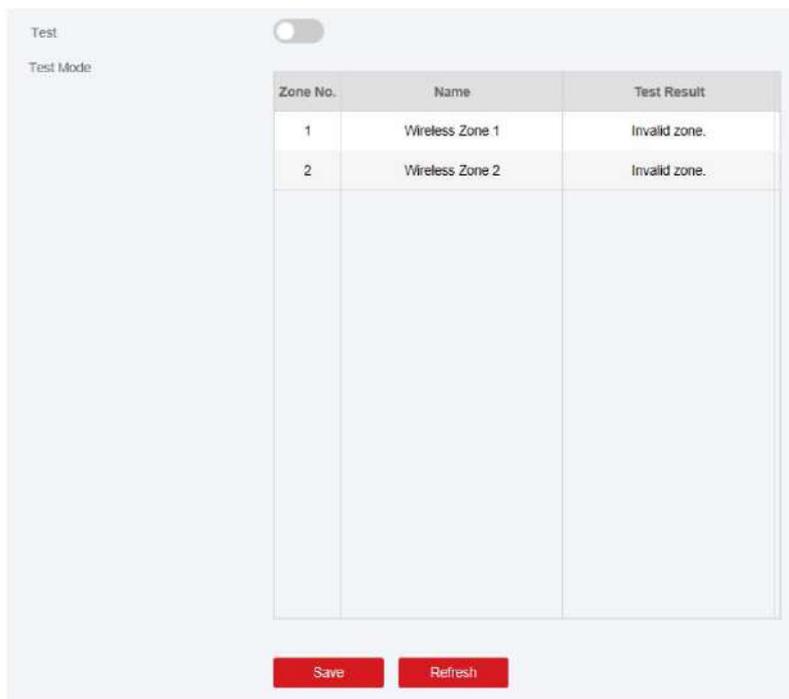
También puede hacer clic en **Restablecer** para restablecer todas las condiciones de búsqueda.

## Prueba

El AX PRO admite la función de prueba de caminata.

## Pasos

1. Ingrese a **Mantenimiento** y **Mantenimiento del dispositivo** y **Prueba** para habilitar la función.



The screenshot shows a web interface for testing. At the top, there is a 'Test' label and a toggle switch. Below it, the text 'Test Mode' is visible. The main part of the interface is a table with three columns: 'Zone No.', 'Name', and 'Test Result'. The table contains two rows of data. Below the table, there are two red buttons labeled 'Save' and 'Refresh'.

Zone No.	Name	Test Result
1	Wireless Zone 1	Invalid zone.
2	Wireless Zone 2	Invalid zone.

### Nota

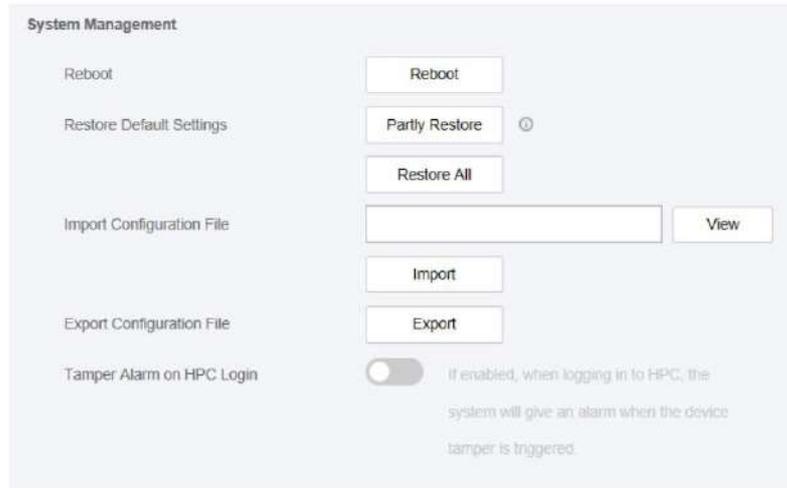
Solo cuando todos los detectores están sin fallas, puede ingresar al modo PRUEBA.

2. Habilite **Prueba** para iniciar la prueba de paseo.
3. Haga clic en **Guardar** para completar la configuración.
4. Activar el detector en cada zona.
5. Verifique el resultado de la prueba.

## Mantenimiento del sistema

Puede reiniciar el dispositivo, restaurar la configuración predeterminada, importar/exportar el archivo de configuración o actualizar el dispositivo de forma remota.

Seleccione el dispositivo y haga clic en el  software del cliente, o ingrese la dirección IP del dispositivo en la barra de direcciones del navegador web. Haga clic en **Mantenimiento** y **Mantenimiento del dispositivo** y **Mantenimiento** para ingresar a la página Actualización y mantenimiento.



### Reiniciar

Haga clic en **Reiniciar** para reiniciar el dispositivo.

### Restaurar la configuración predeterminada

Haga clic en **Restaurar parcialmente** para restaurar todos los parámetros excepto la información de la zona horaria del dispositivo, los parámetros del usuario, la red cableada, la red Wi-Fi, la información del detector de información de HC, la información del detector registrado en la zona y la información del periférico inalámbrico registrado a los valores predeterminados.

Haga clic en **Restaurar todo** para restaurar todos los parámetros a la configuración de fábrica.

### Importar archivo de configuración

Haga clic en **Ver** para seleccionar el archivo de configuración de la PC y haga clic en **Importar archivo de configuración** para importar los parámetros de configuración al dispositivo. La importación del archivo de configuración requiere ingresar la contraseña establecida en el momento de la exportación.

### Exportar archivo de configuración

Haga clic en **Exportar archivo de configuración** para exportar los parámetros de configuración del dispositivo a la PC.

La exportación del archivo de configuración requiere el uso de una contraseña para el cifrado del archivo.

### Alarma de manipulación en el inicio de sesión de HPC

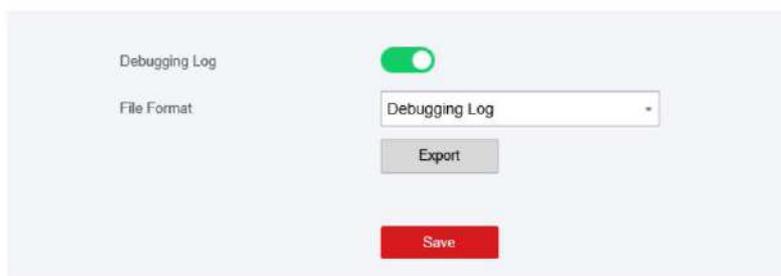
Una vez habilitada esta función, la alarma de tapa abierta del dispositivo (alarma de manipulación) entra en vigor cuando el instalador inicia sesión. (De forma predeterminada, la alarma de tapa abierta (alarma de manipulación) no tiene efecto cuando el instalador inicia sesión).

### Exportar archivo

Puede exportar el archivo de depuración a la PC.

#### Pasos 1.

Haga clic en **Mantenimiento y Mantenimiento del dispositivo** y **Exportar archivo** para ingresar a la página.



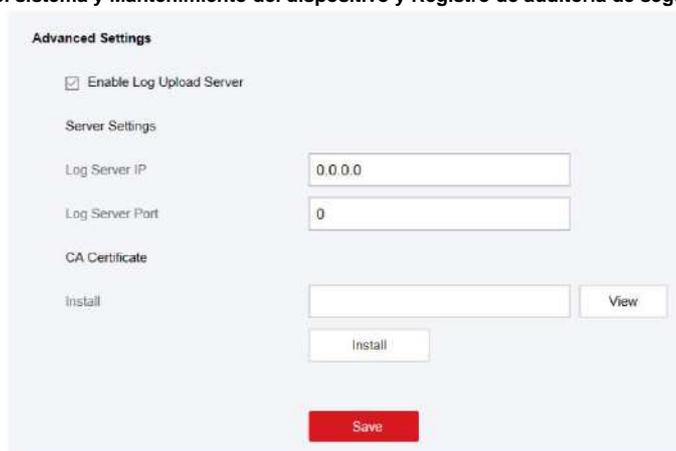
2. Deslice para habilitar la función.
3. Haga clic en **Exportar** para guardar el archivo de depuración en la PC.

### Registro de auditoría de seguridad

Puede agregar el servidor de auditoría de seguridad al sistema. El dispositivo cargará registros web en el servidor.

### Pasos

2. Haga clic en **Mantenimiento del sistema** y **Mantenimiento del dispositivo** y **Registro de auditoría de seguridad** para ingresar a la página.



3. Marque **Habilitar servidor de carga de registros**.
4. Introduzca la IP y el puerto del servidor de registro.
5. Haga clic en **Ver** para seleccionar un certificado.



Se permiten los formatos ca.crt, ca-chan.crt, private.txt.

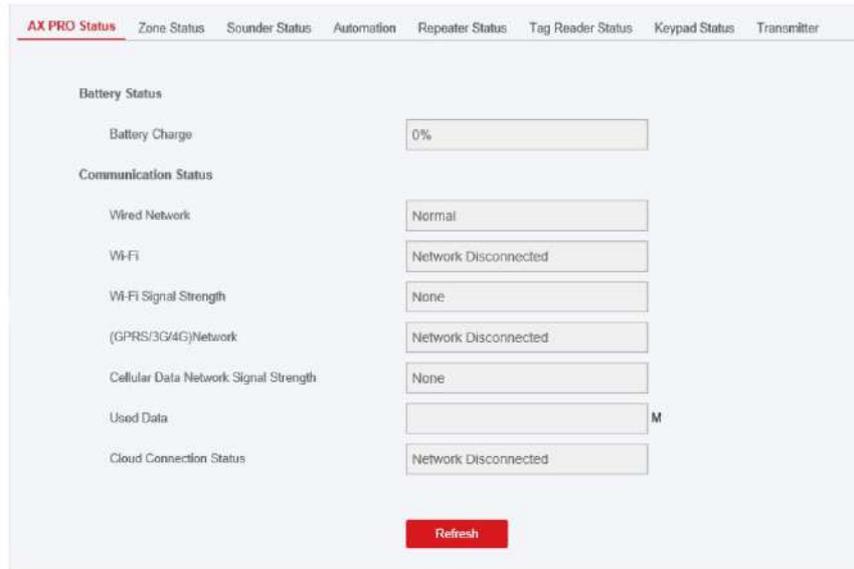
---

6. Haga clic en **Instalar**.
7. Haga clic en **Guardar**.

## 5.3.8 Comprobar estado

Después de configurar la zona, el repetidor y otros parámetros, puede ver su estado.

Haga clic en **Mantenimiento** y **Estado del dispositivo**. Puede ver el estado del panel de control AX PRO, zona, sirena, automatización, repetidor, teclado, lector de etiquetas, llavero y transmisor.



## 5.4 Informe a CRA (Centro Receptor de Alarmas)

El panel de control inalámbrico AX PRO está diseñado con un transceptor integrado siguiendo la guía de EN 50131-10 y EN 50136-2. La categoría DP2 se proporciona con una interfaz de red principal de LAN/WiFi y una interfaz de red secundaria de GPRS o 3G/4G LTE. El ATS (sistema de transmisión de alarmas) está diseñado para usar siempre la interfaz de red LAN/Wi-Fi cuando esté disponible para ahorrar el uso de datos móviles.

La interfaz de red secundaria proporciona resiliencia y confiabilidad durante fallas en el suministro eléctrico.

### Configurar ATS en el transceptor del centro de recepción

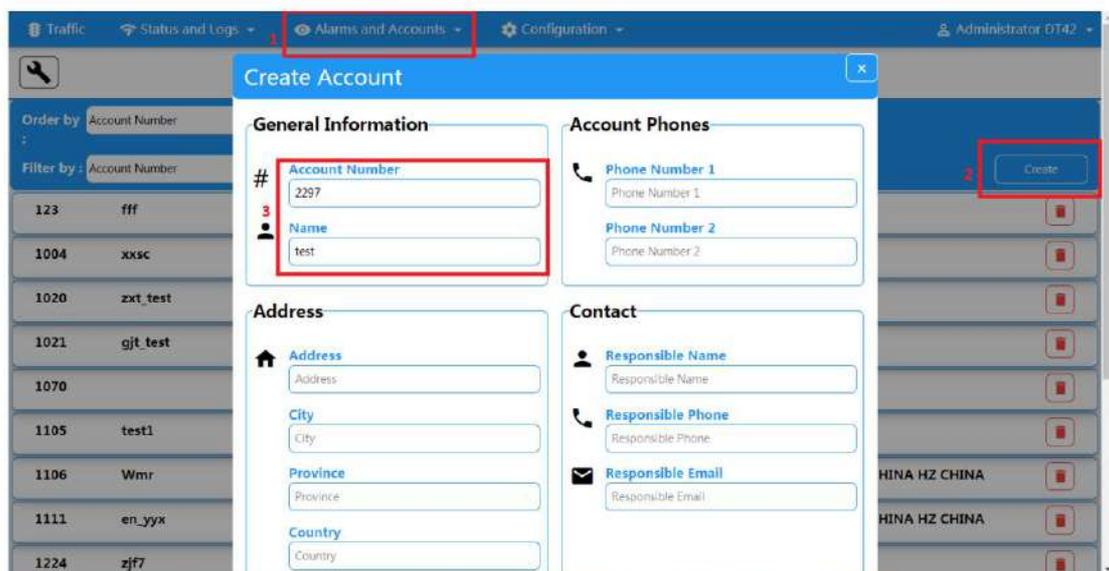
**Pasos:**

1. Inicie sesión en el cliente web del receptor de alarma.
2. Haga clic en **Configuración y Recepción de IP** y cree un servidor de recepción como se muestra a continuación.



3. Haga clic en **Alarmas y cuentas y Gestión de cuentas** y asigne una cuenta para el panel como

mostrar a continuación.



## Configurar ATS en el Transceptor del Panel

### Pasos:

1. Inicie sesión con la cuenta del instalador desde el cliente web local.
2. Haga clic en **Comunicación y Centro de recepción de alarmas (CRA)** y habilite el **Centro de recepción de alarmas 1**.

Alarm Receiver Center1

Enable

Protocol Type

Address Type

Server Address

Port No.

Account Code

Transmission Mode

Impulse Counting Time  s

Attempts

Polling Rate    Enable

Encryption Arithmetic

Password Length

Secret Key

ÿ = Configuración de protocolo =

#### Tipo de protocolo

- ADM-CID
- SIA-DCS
- \*ADM-CID
- Token \*SIA-

DCS Select admitido por el receptor en el CRA. Elija el token con la marca "\*" para

mejorar la seguridad de las comunicaciones.

ÿ = Configuración del servidor =

ÿ	<b>Tipo de dirección</b> — PI - Nombre de dominio
ÿ	<b>Dirección del servidor</b> <b>Nombre de dominio</b>
ÿ	número de puerto Ingrese la dirección IP o el nombre de dominio por el cual se puede llegar al transceptor del centro de recepción. Número de puerto de entrada del servidor proporcionado por el ARC

ÿ = Configuración de cuenta =

ÿ	<b>Código de cuenta</b> Ingrese la cuenta asignada provista por el CRA.
---	--

ÿ = Configuración del protocolo SIA DC-09 =

ÿ	<b>Modo de transmisión</b> —TCP — UDP Tanto TCP como UDP son compatibles para la transmisión. UDP es recomendado por el estándar SIA DC-09.
ÿ	<b>Ajuste de conexión</b> <ul style="list-style-type: none"> <li>• <b>Tiempo de conteo de impulsos</b> <small>Período de tiempo de espera de reintento</small>                      Configure el período de tiempo de espera para que el receptor responda. La retransmisión se organizará si el transceptor del centro de recepción está fuera de tiempo.</li> <li>• <b>intentos</b>                      Configure el número máximo de intentos de retransmisión.</li> <li>• <b>Tasa de sondeo</b>                      Configure el intervalo entre 2 sondeos en vivo si está activado.</li> </ul>
ÿ	<b>Configuración de cifrado</b> <ul style="list-style-type: none"> <li>• <b>Aritmética de cifrado</b>                      — AES</li> <li>• <b>Longitud de la contraseña</b>                      — 128                      — 192                      — 256</li> <li>• <b>Secreto</b> <small>Llave</small>                      Configure la longitud de la clave de cifrado e ingrese la clave proporcionada por el ARC.</li> </ul>

Prueba de señalización

Active una alarma de pánico desde el panel de control.

Inicie sesión en el receptor. Haga clic en **Tráfico** para revisar todos los mensajes recibidos.

The screenshot displays a web interface for managing traffic. At the top, there is a navigation bar with the following items: 'Traffic' (highlighted with a red box), 'Status and Logs', 'Alarms and Accounts', and 'Configuration'. The user is logged in as 'Administrator DT42'. The main heading is 'Traffic', with a 'Refresh in 16' indicator. Below this, there are controls for 'Order by' (set to 'Reception Time') and sorting options 'Ascendant' and 'Descendant'. A 'Filter by' section is set to 'Event ID' with a search input field and a '+' button. A table of events is shown below, with the first row highlighted by a red box:

Event 580777	Account : 2297	Zone : 1	Description : Panic Alarm / 001	Partition : 01	Receiver # : 1	2020-03-28 12:01:42	Code : E120	Line # : 0
--------------	----------------	----------	---------------------------------	----------------	----------------	---------------------	-------------	------------

The second row of the table shows 'Event 580776' with a timestamp of '2020-03-28 12:01:36'.

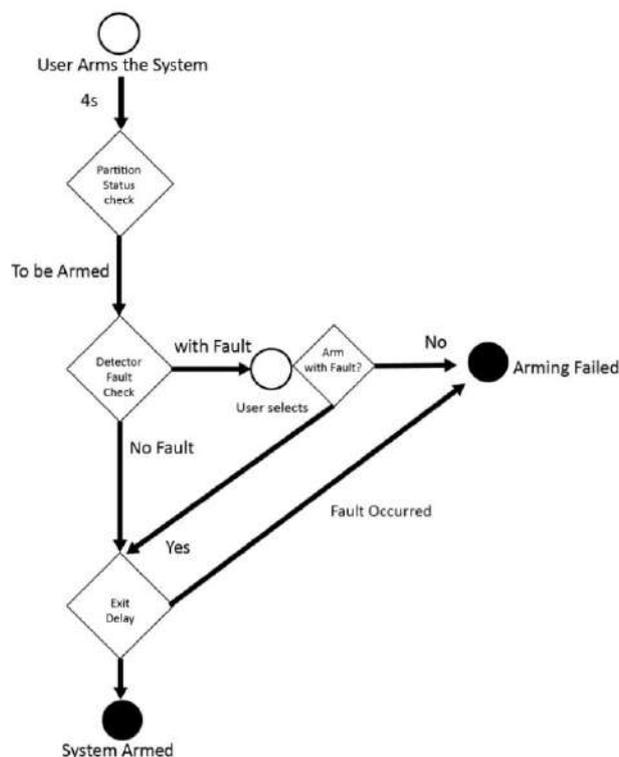
## Capítulo 6 Operaciones generales

### 6.1 Armado

Puede usar el teclado, el llavero, la etiqueta, el software del cliente, el cliente móvil para armar su sistema.

Después de enviar el comando de armado a AX PRO, el sistema verificará el estado del detector. Si el detector falla, deberá elegir si desea armar el sistema con falla.

Mientras el sistema está armado, el AX PRO indicará el resultado en 5 segundos y cargará el informe de armado.



#### Nivel de acceso de Armado

El usuario en el nivel 2 o 3 tiene permiso para armar o armar parcialmente el sistema.

#### Indicación de armado

El indicador de armado/desarmado se mantiene azul fijo durante 5 s.

#### Motivo de la falla de armado

- Detector de intrusión activado (excepto el detector en la ruta de salida).
- Dispositivo de alarma de pánico activado.
- Ocurrió una alarma de manipulación.
- Excepción de comunicación
- Excepción de la fuente de alimentación principal

- Excepción de batería de respaldo
- Fallo de recepción de alarma • Fallo de sirena • Batería baja del llavero • Otros

#### **Armado con falla** Mientras

el armado se detiene con falla, el usuario en el nivel 2 tiene permiso para armar el sistema con falla (armado forzado).

El armado forzado solo tiene efecto en la operación de armado actual.  
La operación de armado forzado se registrará en el registro de eventos.

## **6.2 Desarmado**

Puede desarmar el sistema con teclado, llavero, etiqueta, software de cliente o cliente móvil.

#### **Indicación de desarmado** El

indicador de armado/desarmado parpadea durante 30 segundos mientras el usuario desarma con éxito el sistema a través de la ruta de entrada/salida.

El sistema informará el resultado del desarmado después de que se complete la operación.

#### **Duración del retraso de**

**entrada** Asegúrese de que el temporizador no supere los 45 segundos para cumplir con EN50131-1.

#### **Alarma temprana**

Si la primera zona instantánea se activa cuando el AX PRO está en el estado de retardo de entrada, el AX PRO luego ingresa al modo de alarma temprana.

La duración de la alarma temprana se puede configurar (> 30 s).

El AX PRO informará la alarma solo si el evento de alarma dura más que la duración de la alarma temprana con la adición del retraso de entrada.

## **6.3 Control SMS**

Puede controlar el sistema de seguridad con SMS, y el comando se muestra a continuación.

Formato de SMS para Armar/Desarmar/Silenciar alarma:

{Comando} + {Tipo de operación} + {Objetivo}

Comando: 2 dígitos, 00- Desarmado, 01- Armado Ausente, 02- Armado Presente, 03- Silenciar alarma Tipo de operación: 1- Área Operación Objetivo: No más de 3 dígitos, 0- Operación para todas las áreas, 1- Operación para área 1(zona1), y el resto se puede deducir por analogía.

## A. Resolución de problemas

### A.1 Fallo de comunicación

#### A.1.1 Conflicto de IP

Descripción de la falla:

la IP que el panel adquirió o configuró automáticamente es la misma que la de otros dispositivos, lo que genera conflictos de IP.

Solución:

busque la IP disponible actual a través de ping. Cambie la dirección IP y vuelva a iniciar sesión.

#### A.1.2 La página web no es accesible

Descripción de la falla:

Use el navegador para acceder a las páginas web y muestre Inaccesible.

Soluciones:

1. Verifique si el cable de red está suelto y si la red del panel es anormal.
2. El puerto del panel ha sido modificado. Agregue un puerto a la dirección web para obtener más acceso.

#### A.1.3 Hik-Connect está fuera de línea

Descripción de la falla:

La página web muestra que el Hik-Connect está fuera de línea.

Solución:

La configuración de red del panel es un error, no se puede acceder a la extranet.

#### A.1.4 La cámara de red se cae con frecuencia

Descripción de la falla:

El sistema informa múltiples registros de eventos de desconexión y conexión de IPC.

Solución:

Verifique si la comunicación de red o la vista en vivo de la cámara es adecuada.

#### A.1.5 No se pudo agregar el dispositivo en la aplicación

Descripción de la falla:

cuando se usa la aplicación para agregar dispositivos, se le indica que el dispositivo no se pudo agregar, no se pudo encontrar el dispositivo, etc.

Solución:

Verifique la página web: si Hik-Connect está fuera de línea.

## **A.1.6 La información de alarma no se transmite a APP/4200/Centro de alarmas**

Descripción de la falla:

después de que se activa la alarma, el centro de alarma app/4200/ no recibe el mensaje de alarma.

Solución:

"Mensaje push" - "alarma y aviso a prueba de manipulaciones" no está habilitado. Debe habilitar el "aviso de alarma y protección contra manipulaciones".

## **A.2 Exclusión Mutua de Funciones**

### **A.2.1 No se puede ingresar al modo de registro**

Descripción de la falla:

Haga clic en la tecla de función del panel y la tecla de aviso no es válida.

Solución: El

panel está en modo "Punto de acceso". Cambie el panel al modo "estación" y luego intente ingresar nuevamente al modo de registro.

## **A.3 Fallo de zona**

### **A.3.1 La zona está fuera de línea**

Descripción de la falla:

Ver el estado de las zonas que se muestra fuera de línea.

Solución:

Compruebe si el detector informa de subtensión. Reemplace la batería del detector

### **A.3.2 Zona a prueba de manipulaciones**

Descripción de la falla:

Ver el estado de las zonas que se muestra a prueba de manipulaciones.

Solución:

Hacer un botón a prueba de manipulaciones del detector holden.

### **A.3.3 Zona Activada/Fallo**

Descripción de la falla:

Ver el estado de las zonas que muestra activado/fallo.

Solución:

Restablezca el detector.

## **A.4 Problemas durante el armado**

### **A.4.1 Falla en el Armado (Cuando el armado forzado no está habilitado)**

Descripción de la falla:

Cuando el panel se está armando, falla el armado rápido.

Solución:

El panel no habilita el "armado forzado", y cuando hay una falla en la zona, el armado fallará. Active la habilitación de "armado forzado" o restaure la zona al estado normal.

## **A.5 Falla Operacional**

### **A.5.1 No se pudo ingresar al modo de prueba**

Descripción de la falla:

No se pudo habilitar el modo de prueba, lo que indica "Una falla en la zona".

Solución:

El estado de la zona, el estado de la alarma o la alimentación de la zona es anormal.

### **A.5.2 La operación de borrado de alarmas en el panel no produce el informe de borrado de alarmas**

Descripción de la falla:

La operación de borrado de alarma en el panel no produce el informe de borrado de alarma.

Solución:

En ausencia de alarma, no se cargará ningún informe para la limpieza del brazo.

## **A.6 Error de entrega de correo**

### **A.6.1 Error al enviar correo de prueba**

Descripción de la falla:

cuando configure la información del correo, haga clic en "probar bandeja de entrada" y la prueba fallará.

Solución:

Configuración incorrecta de los parámetros del buzón. Edite la información de configuración del buzón, como se muestra en la tabla 1/1.

## A.6.2 Error al enviar correo durante el uso

Descripción de la falla:

Compruebe el registro de excepciones del panel. Hay un "error de envío de correo".

Solución:

El servidor de buzones tiene acceso restringido. Inicie sesión en el buzón para ver si está bloqueado.

## A.6.3 Error al enviar correos a Gmail

Descripción de la falla:

El buzón del destinatario es Gmail. Haga clic en "Probar bandeja de entrada" y la prueba de solicitud falla.

1. Google evita que los usuarios accedan a Gmail mediante aplicaciones/dispositivos que no cumplan con sus estándares de seguridad.

Solución:

Inicie sesión en el sitio web (<https://www.google.com/settings/security/lesssecureapps>) y "comience a usar el acceso de la aplicación que no es lo suficientemente seguro". El dispositivo puede enviar correos normalmente.

2. Gmail no elimina la autenticación CAPTCHA.

Solución: haga clic en el enlace a continuación y luego haga clic en

"continuar" (<https://accounts.google.com/b/0/displayunlockcaptcha>).

## A.6.4 Error al enviar correos a QQ o Foxmail

Descripción de la falla:

El buzón del receptor es QQ o foxmail. Haga clic en "Probar bandeja de entrada" y la prueba de solicitud falla.

1. Cuenta o contraseña incorrecta de QQ.

Solución:

la contraseña requerida para el inicio de sesión de la cuenta QQ no es la contraseña utilizada para el inicio de sesión normal. La ruta específica es: Ingrese la cuenta de correo electrónico y dispositivo y cuenta y para generar el código de autorización y use el código de autorización como contraseña de inicio de sesión.

2. Se necesita permiso de inicio de sesión SMTP para abrir.

## A.6.5 Error al enviar correos a Yahoo

Descripción de la falla:

El buzón del receptor es yahoo. Haga clic en "probar bandeja de entrada" y la prueba de aviso falla.

1. El nivel de seguridad del buzón es demasiado alto.

Solución:

Vaya a su cuenta de correo y active "inicio de sesión menos seguro".

## A.6.6 Configuración de correo

Tabla A-1 Configuración de correo

Tipo de correo	Servidor de correo	Puerto SMTP	Protocolos compatibles
Gmail	smtp.gmail.com	587	TLS/STARTTLS (TLS)
panorama	smtp.office365.com	587	STARTTLS (TLS)
Hotmail	smtp.office365.com	587	STARTTLS (TLS)
qq	smtp.qq.com	587	STARTTLS (TLSv1.2)
yahoo	smtp.mail.yahoo.com 587		STARTTLS (TLSv1.2)
126	smtp.126.com	465	SSL/TLS
Siná	smtp.sina.com	25/465/587	SSL/TLS/STARTTLS (SSL/TLS)



**Nota**

Sobre la configuración del correo:

- Puerto SMTP Predeterminado para usar el puerto 25 sin encriptación, o usar el puerto 465 si se usa SSL/TLS.  
El puerto 587 se utiliza principalmente para el modo de protocolo STARTTLS.  
El modo de protocolo STARTTLS que se suele utilizar de forma predeterminada al seleccionar TLS.
- Nombre de usuario El nombre de usuario de Outlook y Hotmail requiere nombres completos, y otros correos electrónicos requieren un prefijo antes de @.

## B. Tipos de entrada

Tabla B-1 Tipos de entrada

Tipos de entrada	Operaciones
Zona instantánea	<p>El sistema emitirá una alarma inmediatamente cuando detecte un evento de activación después de que el sistema esté armado.</p> <p>Respuesta audible Activar el sonido del sistema y la sirena.</p> <p>Indicación de voz: alarma de zona X.</p>
Zona perimetral	<p>El sistema emitirá una alarma inmediatamente cuando detecte un evento de activación después de que el sistema esté armado.</p> <p>Respuesta audible: active el sonido del sistema y la sirena.</p> <p>Hay un intervalo configurable entre alarma y sirena salida, que le permite comprobar la alarma y cancelar la salida de sirena durante el intervalo.</p> <p>Indicación de voz: alarma perimetral de la zona X.</p>
Zona Retrasada	<p>El sistema le proporciona tiempo para salir o entrar en el área de defensa sin alarma.</p> <p>Respuesta audible: active el sonido del sistema y la sirena.</p> <p>Indicación de voz: alarma de zona X.</p>
Zona de seguimiento	<p>La zona actúa como zona retardada cuando detecta un evento de activación durante el retardo de entrada del sistema, mientras que actúa como zona instantánea en caso contrario.</p> <p>Respuesta audible: active el sonido del sistema y la sirena.</p> <p>Indicación de voz: alarma de seguimiento de zona X.</p>
Zona de silencio 24H	<p>La zona se activa todo el tiempo sin ningún sonido/sirena salida cuando se produce la alarma.</p> <p>Respuesta audible: No hay sonido del sistema (mensaje de voz o sirena).</p>
Zona de pánico	<p>La zona se activa todo el tiempo.</p> <p>Respuesta audible: active el sonido del sistema y la sirena.</p> <p>Indicación de voz: alarma de pánico de la zona X.</p>
Zona de fuego	<p>La zona se activa todo el tiempo con salida de sonido/sirena cuando ocurre la alarma.</p>

Tipos de entrada	Operaciones
	<p>Respuesta audible: active el sonido del sistema y la sirena.</p> <p>Indicación de voz: alarma de incendio de la zona X.</p>
Zona de Gas	<p>La zona se activa todo el tiempo con salida de sonido/sirena cuando ocurre la alarma.</p> <p>Respuesta audible: active el sonido del sistema y la sirena.</p> <p>Indicación de voz: alarma de gas de la zona X.</p>
Zona Médica	<p>La zona se activa todo el tiempo con un pitido de confirmación cuando ocurre la alarma.</p> <p>Respuesta audible: active el sonido del sistema y la sirena.</p> <p>Indicación de voz: alarma médica de la zona X.</p>
Zona de tiempo de espera	<p>La zona se activa todo el tiempo. El tipo de zona se usa para monitorear e informar el estado "ACTIVO" de una zona, pero solo informará y alarmará este estado después de que haya expirado el tiempo programado (1 a 599) segundos.</p>
Zona deshabilitada	<p>Las alarmas no se activarán cuando la zona se active o se altere.</p> <p>Respuesta audible: No hay sonido del sistema (mensaje de voz o sirena).</p>
Zona virtual (teclado/mando)	<p>El sistema emitirá una alarma inmediatamente cuando detecte un evento de activación después de que el sistema esté armado.</p> <p>Respuesta audible: active el sonido del sistema y la sirena.</p> <p>Aviso de voz: el zumbador emite un pitido.</p>
Alarma de manipulación	<p>El sistema emitirá una alarma inmediatamente cuando detecte un evento de activación después de que el sistema esté armado.</p> <p>Respuesta audible: active el sonido del sistema y la sirena.</p> <p>Indicación de voz: Zona X manipulada.</p>
Enlace	<p>Activa el dispositivo vinculado cuando ocurre un evento.</p> <p>Por ejemplo, los relés vinculados del expansor de salida se habilitarán cuando el AX PRO esté armado.</p>
Brazo	<p>Cuando está armado: Indicación de voz por falla. Puede manejar la falla de acuerdo con el mensaje de voz. • Sistema de sonido para armar con Tag o llavero. • Aviso de voz por falla.</p> <p>Puede manejar la falla de acuerdo con el mensaje de voz.</p>

Se muestra el evento de falla en el cliente. Puede manejar la falla a través del software del cliente o del cliente móvil.

Aviso de voz: Armado/Armado fallido.

## C. Tipos de salida

Tabla C-1 Tipos de salida

Tipos de salida	Activo	Restaurar
Armamento	Armar el AXE PRO	Después del retardo de salida configurado
Encantador	Desarmar el AXE PRO	Después del retardo de salida configurado
Alarma	Cuando ocurre un evento de alarma. La salida de alarma se activará después del retardo de salida/entrada configurado.	Después del retardo de salida configurado, desarmar el AX PRO o silenciar la alarma
Enlace de zona	Cuando ocurre un evento de alarma, el relé vinculado emitirá una señal de alarma.	Después de la duración de salida configurada
Manual de operación	Habilitar relés manualmente	Durante el tiempo de activación o desactivar los relés manualmente

## D. Tipos de eventos

Tabla D-1 Tipos de eventos

Tipos de eventos	Disfraz	Predeterminado 1 (notificación de alarma)	Predeterminado 2 (cliente)	Predeterminado 3 (cliente móvil)	Predeterminado 4 (teléfono) (cliente móvil) (opción de alarmas 1/2)
alarma y Manosear	x/ÿ	ÿ	ÿ	ÿ	ÿ
Seguridad vital Evento	x/ÿ	ÿ	ÿ	ÿ	ÿ
Estado del sistema	x/ÿ	ÿ	x	x	x
Panel administración	x/ÿ	ÿ	x	x	x

## E. Niveles de acceso

Nivel	Descripción
1	Acceso por cualquier persona; por ejemplo, el público en general.
2	Acceso de usuario por un operador y administrador; por ejemplo clientes (usuarios de sistemas).
3	Acceso de usuario por un instalador; por ejemplo un profesional de una empresa de alarmas.

**Tabla E-1 Permiso del Nivel de Acceso**

Función	Permiso		
	1	2	3
Armamento	No	Sí	Sí
Encantador	No	Sí	Sí
Restauración/borrado de alarma	No	Sí	Sí
Acceso al modo de prueba de paseo	No	Sí	Sí
Anular (zona)/Deshabilitar/Forzar armado	No	Sí	Sí
Agregar/Cambiar código de verificación	No	Sí	Sí
Adición/edición de usuario de nivel 2 y Código de verificación	No	Sí	Sí
Adición/edición de datos de configuración	No	No	Sí
Sustitución de software y firmware	No	No	No

### Nota

<sup>a</sup> Por la condición de estar acreditado por usuario en nivel 2. <sup>b</sup> Por la condición de estar acreditado por usuario en nivel 2 y nivel 3. <sup>d</sup> Los usuarios sólo pueden editar su propio código de usuario.

- El nivel de usuario 2 puede asignar el permiso de inicio de sesión del controlador al nivel de usuario 3 en el página de configuración.
- El nivel de usuario 2 debe asignar permisos al nivel de usuario 3 si el nivel de usuario 3 desea iniciar sesión. el controlador de forma remota.
- Cuando se omite el controlador, el nivel de usuario 3 puede iniciar sesión en el controlador sin la asignación de permisos del nivel de usuario 2.

- Cuando se omite el controlador, el nivel de usuario 3 puede iniciar sesión en el controlador sin la asignación de permisos del nivel de usuario 2.
- El nivel de usuario 4 puede iniciar sesión en el controlador solo cuando el nivel de usuario 2 o el nivel 3 ha asignado permisos al nivel de usuario 4.

## F. Señalización

### DetECCIÓN DE FALLAS ATP/ATS

Las fallas de ATP (ruta de transmisión de alarma) se detectarán cuando la interfaz de red del panel de control se desconecte o la ruta de transmisión al transceptor del centro de recepción ubicado en ARC se bloquee en algún punto intermedio. Se informará una falla ATS (Sistema de transmisión de alarmas) cuando se detecten fallas ATP en ambas rutas de transmisión.

La restauración de ATP se detectará tan pronto como se conecte la interfaz de red y se restablezca la ruta de transmisión al transceptor del centro de recepción. La restauración de ATS se informará cuando se detecte la restauración de ATP de cualquier ruta de transmisión.

El rendimiento de temporización de la detección de fallas y restauraciones de ATP se muestra en la siguiente tabla.

	Transmisor	Tiempo máximo de detección
Falla/restauración ATP primaria	LAN/Wi-Fi	10 min
Falla/restauración de ATP secundaria	GPRS	60 minutos
	3G/4G LTE	20 min (cuando falló el ATP primario)

La señalización siempre se transmitirá desde la ATP primaria cuando esté operativa. De lo contrario, se cambiará automáticamente a la ruta de transmisión secundaria que esté operativa en ese momento. Los eventos de falla y restauración de ATP primarios y secundarios se informarán al CRA cuando quede un ATP para trabajar. También se registrarán en la memoria de registro obligatoria con capacidad de 1000 registros asignados en el almacenamiento de memoria flash no volátil, así como el registro de fallas ATS. El detalle de los informes y registros se enumeran en la siguiente tabla.

	Código de evento al señalar	Descripción del registro de eventos
Falla/restauración ATP primaria	E351/R351	Ruta LAN fallida/Recuperación de ruta LAN
Falla/restauración de ATP secundaria	E352/R352	Ruta de red móvil fallida/Ruta de red móvil Recuperación
Fallo/restauración de ATS	N / A	ATS falló
Fallo/restauración de la interfaz de red principal	E351/R351	Ruta LAN fallida/Recuperación de ruta LAN
Fallo/restauración de la interfaz de red secundaria	E352/R352	Ruta de red móvil fallida/Ruta de red móvil Recuperación

### Categoría ATS

La categoría ATS de AXPRO es DP2. Mientras la central receptora de alarmas esté habilitada. El panel de control cargará el informe de alarma al centro receptor a través de la ruta principal (LAN o Wi-Fi) o la ruta de respaldo (3G/4G). Si el panel de control está correctamente conectado a la red LAN o Wi-Fi, la ruta principal se selecciona como ruta de transmisión. Si falla la conexión de la ruta principal, la ruta se cambiará a 3G/4G. Y si se restaura la conexión de la ruta principal, la ruta volverá a cambiarse a LAN o Wi-Fi. El panel de control verifica el estado de la conexión continuamente y genera fallas de transmisión de registros para cualquiera de las rutas. Si bien ambas rutas no son válidas, el panel de control determina la falla del ATS.

## G. Código SIA y CID



**Nota**

El siguiente código es para transmitir desde el panel de control de seguridad al CRA a través del protocolo DC09.

**Tabla G-1 Código SIA y CID**

Código SIA	Código CID	Descripción	Información del escenario
MAMÁ	1100	alarma medica	Esta alarma de zona es a menudo se usa para activar el botón de emergencia
mh	3100	Alarma médica restaurada	
----- (Gotera de agua Detector: WA)	1130 (Gotera de agua Detector: 1154)	alarma de robo	1103 (código hik) detector de fugas de agua instantáneo alarma 1130 (código hik) alarma de robo Se utiliza para la activación de la alarma de retardo en la zona de retardo de la fuga de agua detector
BH (Gotera de agua Detector: WH)	3130 (Gotera de agua Detector: 3154)	Alarma de robo restaurada	
FA (Detector de calor: KA)	1111 (Detector de calor: 1114)	Alarma de incendios	
FH (Detector de calor: KH)	3111 (Detector de calor: 3114)	Alarma de incendio restaurada	
DECRAH	1121	Alarma de coacción	
DECRAH	1122	Alarma de pánico silenciosa	
S.S	3122	Alarma de pánico silenciosa restaurada	
-----	1123	Alarma de pánico audible	
CH	3123	Alarma de pánico audible restaurada	

Código SIA	Código CID	Descripción	Información del escenario
	1130	Alarma de tiempo de espera	Alarma de tiempo de espera de zona
BH	3130	Alarma de tiempo de espera restaurada	
Panikaria	1120	Alarma de pánico silenciosa	1122 (código hik) 24H alarma silenciosa, 1127 (código hik) alarma de pánico silenciosa
Panikaria	1120	Alarma de pánico audible	1123 (código hik) 24H alarma audible 1129 (código hik) alarma de pánico
PH	3120	Alarma de pánico audible restaurada	
	1130	alarma de robo	
BH	3130	Alarma de robo restaurada	
	1131	Perímetro violado	
BH	3131	Perímetro restaurado	
ANUNCIO	1132	Alarma de robo interior	
CK	3132	Alarma de robo interior restaurado	
(Gotera de agua Detector: WA)	1130 (Gotera de agua Detector: 1154)	Alarma 24H	Alarma auxiliar de 24 horas/Alarma de vibración de 24 horas (reservado)
BH (Gotera de agua Detector: WH)	3130 (Gotera de agua Detector: 3154)	Alarma 24H Restaurada	
(Gotera de agua Detector: WA)	1130 (Gotera de agua Detector: 1154)	alarma de robo	
BH (Gotera de agua Detector: WH)	3130 (Gotera de agua Detector: 3154)	Alarma de robo restaurada	
	1137	tapa abierta	
TR	3137	Tapa restaurada	
BV	1139	Alarma confirmada	Usado cuando el La opción PD6662 es

Código SIA	Código CID	Descripción	Información del escenario
			activado
B/N	3139	Restauración de alarma confirmada	
FA	1142	Alarma de cortocircuito de BUS	Para el panel de control
CN	3142	BUS Cortocircuito Restaurado	
	1144	Módulo externo Desconectado	Se desmontó la sonda detectora de señal triple
TR	3144	Módulo externo conectado	
AG	1148	Alarma de movimiento del dispositivo	Para el panel de control (reservado)
CO	3148	Alarma de movimiento del dispositivo restaurado	
	1149	Alarma de enmascaramiento	Activado cuando el detector está bloqueado
BH	3149	Alarma de enmascaramiento restaurada	
Georgia	1162	Alarma de fuga de gas	Gas: monóxido de carbono (CO)
GH	3162	Alarma de fuga de gas restaurada	
Ah	1207	Zona de alerta temprana	Usado para alarma temprana de zona
PC	3207	Zona de alerta temprana Despedido	
A	1301	Pérdida de alimentación de red	
Arkansas	3301	Red eléctrica restaurada	
YouTube	1302	Batería BAJA	
AÑO	3302	Voltaje de la batería restaurado	
ZY	1305	Restablecer los valores predeterminados	Para el panel de control
YM Falta la batería del transmisor Rango de identificación: 301 -	1311 Falta la batería del transmisor Rango de identificación: 301 -	Batería desconectada	falta de batería del panel de control
AÑO Falta la batería del transmisor	3311 Falta la batería del transmisor	Batería reconectada	

Código SIA	Código CID	Descripción	Información del escenario
Rango de identificación: 301 -	Rango de identificación: 301 -		
YI	1312	Protección contra la sobretensión Motivado	Activado cuando la corriente está sobrecargada
YJ	3312	Protección contra la sobretensión restaurado	
YP	1319	Protección al sobrevoltaje Motivado	Activado cuando el voltaje está sobrecargado
YQ	3319	Protección al sobrevoltaje restaurado	
AI	1333	Excepción de expansor	Alarma anormal del expansor
CQ	3333	Expansor restaurado	
A.J.	1336	Impresora desconectada	
RC	3336	Impresora conectada	
XT	1384	Batería BAJA	
XR	3384	Voltaje de la batería restaurado	
		Expansor de Baja Tensión	
		Voltaje normal del expansor	
YP	1301	Pérdida de alimentación de red	Pérdida de alimentación de CA del repetidor
YQ	3301	Red eléctrica restaurada	
YM	1311	Batería desconectada	Falta la batería del repetidor
AÑO	3311	Batería reconectada	
TA (El número de serie del módulo de salida comienza en 1, el del teclado comienza en 101, el del lector de etiquetas comienza en 201)	1144 (El número de serie del módulo de salida comienza en 1, el del teclado comienza en 101, el del lector de etiquetas comienza en 201)	tapa abierta	1341 (código hik) para expansor 1343 (código hik) para repetidor inalámbrico 1344 (código hik) para sonda inalámbrica 1346 (código hik) para periférico inalámbrico 1383 (código hik) para sensor de zona

Código SIA	Código CID	Descripción	Información del escenario
TR (El número de serie del módulo de salida comienza en 1, el del teclado comienza en 101, el del lector de etiquetas comienza en 201)	3144 (El número de serie del módulo de salida comienza en 1, el del teclado comienza en 101, el del lector de etiquetas comienza en 201)	Tapa restaurada	
YP transmisor de CA pérdida de potencia Rango de identificación: 301 ~ Alimentación de CA de la sirena Pérdida Rango de identificación: 202 ~	1301 transmisor de CA pérdida de potencia Rango de identificación: 301 ~ Alimentación de CA de la sirena Pérdida Rango de identificación: 202 ~	Pérdida de alimentación de CA del expansor	para expansor
YQ transmisor de CA pérdida de potencia Rango de identificación: 301 ~ Alimentación de CA de la sirena Pérdida Rango de identificación: 202 ~	3301 transmisor de CA pérdida de potencia Rango de identificación: 301 ~ Alimentación de CA de la sirena Pérdida Rango de identificación: 202 ~	Pérdida de alimentación de CA del expansor restaurado	
SG	1381	Dispositivo sin conexión	
XC	3381	Dispositivo restaurado	
XT (El número de serie del módulo de salida comienza desde 1, del teclado comienza desde 101, del lector de etiquetas comienza desde 201, del transmisor comienza desde 301)	1384 (El número de serie del módulo de salida comienza desde 1, del teclado comienza desde 101, del lector de etiquetas comienza desde 201, del transmisor comienza desde 301)	Batería BAJA	1337 (código hik) Bajo voltaje del repetidor 1347 (código hik) Subtensión de periféricos inalámbricos
XR (El número de serie del módulo de salida comienza en 1, el del teclado comienza en 101, el del lector de etiquetas comienza en 201, el del transmisor comienza en 301)	3384 (El número de serie del módulo de salida comienza en 1, el del teclado comienza en 101, el del lector de etiquetas comienza en 201, el del transmisor comienza en 301)	Voltaje de la batería restaurado	

Código SIA	Código CID	Descripción	Información del escenario
XL (El número de serie del módulo de salida comienza en 1, el del teclado comienza en 101, el del lector de etiquetas comienza en 201, el del transmisor comienza en 301)	1381 (El número de serie del módulo de salida comienza en 1, el del teclado comienza en 101, el del lector de etiquetas comienza en 201, el del transmisor comienza en 301)	Dispositivo sin conexión	
XC (El número de serie del módulo de salida comienza en 1, el del teclado comienza en 101, el del lector de etiquetas comienza en 201, del transmisor comienza desde 301)	3381 (El número de serie del módulo de salida comienza en 1, el del teclado comienza en 101, el del lector de etiquetas comienza en 201, del transmisor comienza desde 301)	Dispositivo restaurado	
LT	1351	Fallo de la ruta de señalización principal	Fallo de ATP del canal principal
LR	3351	Ruta de señalización principal restaurado	
LT	1352	Fallo de ruta de señalización de respaldo	Fallo de ATP del canal de respaldo
LR	3352	Ruta de señalización de respaldo restaurado	
SOY	1354	Línea telefónica desconectada	
CU	3354	Línea telefónica conectada	
PIE	1380	Fallo del sensor del detector	
F.J.	3380	Fallo del sensor del detector restaurado	
UN	1382	Fallo Supervisión BUS	Módulo BUS de expansión desconectado
CV	3382	Restablecimiento de la supervisión del AUTOBÚS	
		Alarma de circuito abierto de zona	El detector NC es motivado
		Alarma de cortocircuito de zona	NO se activa el detector

Código SIA	Código CID	Descripción	Información del escenario
OP	1401	Desarmado	
CL	3401	Armado	
OA	1403	Desarmado automático	
California	3403	Armado automático	
zona de casa	1406	Alarma silenciada	por área
CW	3408	Armado instantáneo	
CS	1409	Desarmado de zona con interruptor de llave	
zona grande	3409	Armado de zona con interruptor de llave	
Patron Hogar	3441	Armado en modo hogar	
CX	3442	Armado Forzado	
		Activar salida por programación	
		Desactivar la salida por programación	
Conectividad	1452	Tarde para desarmar	Se usa cuando configura el armado tardío del área
CD	1455	Autoarmado fallido	
		Error al encender la salida	Error al encender el relé
		No se pudo apagar la salida	
		Desarmado automático fallido	
		Cambio de red	
modo de copia	1570	anulado	
QU	3570	Derivación restaurada	
Australia	1574	Omisión de grupo	
CZ	3574	Omisión de grupo restaurada	
AV	1601	Prueba de informe manual	
PR	1602	Prueba de informe periódico	
TS	1607	Prueba de paseo habilitada	
TE	3607	Prueba de paseo deshabilitada	
AW	1617	Prueba de conexión telefónica	
LB	1627	Modo de programación	

Código SIA	Código CID	Descripción	Información del escenario
LX	1628	Salir de Programación	
-----	1131	Detección de intrusos	
BH	3131	Detección de intrusos restaurada	
-----	1131	Alarma de zona cruzada	
BH	3131	Alarma de zona cruzada restaurada	
		alarma infrarroja	
		Alarma PIR restaurada	
SÍ	1775	Aumento repentino del sonido Alarma de intensidad	
Delaware	3775	Aumento repentino del sonido Alarma de intensidad restaurada	
Arizona	1776	Disminución repentina del sonido Alarma de intensidad	
DF	3776	Disminución repentina del sonido Alarma de intensidad restaurada	
		Fallo de entrada de audio	
		Entrada de audio restaurada	
-----	1131	Alarma de cruce de línea	
BH	3131	Alarma de cruce de línea restaurada	
-----	1134	Detección de entrada de región	
FA	1112	Alarma de fuente de fuego	
FH	3112	Alarma de fuente de fuego restaurada	
Kansas	1158	Prealarma de alta temperatura	
CR	3158	Prealarma de alta temperatura restaurado	
1159	ZS	Prealarma de baja temperatura	
ZR	3159	Prealarma de baja temperatura restaurado	
ka	1158	Alarma de alta temperatura	
KH	3158	Alarma de alta temperatura restaurado	

Código SIA	Código CID	Descripción	Información del escenario
ES	1159	Alarma de temperatura baja	
Z H	3159	Alarma de temperatura baja restaurado	
EE, UU.	1134	Detección de salida de región	
PA (El número de usuario del teclado comienza desde 101, el del llavero comienza desde 901)	1120 (El número de usuario del teclado comienza desde 101, el del llavero comienza desde 901)	Alarma de pánico audible	
FA	1110	Alarma de incendio con teclado/control remoto	
		Robo de teclado/control remoto Alarma	
CI	1454	Armado fallido	
MAMÁ	1100	Teclado/Mando a distancia Médico Alarma	
no sé	1501	Teclado bloqueado	
HACER	3501	Teclado desbloqueado	
		Alarma de ausencia	
SER	1910	Teclado Desconectado	
DH	3910	Teclado conectado	
BF	1911	Relé KBUS desconectado	
DI	3911	Relé KBUS conectado	
		KBUS GP/K desconectado	
		KBUS GP/K conectado	
		KBUS MN/K Desconectado	
		KBUS MN/K conectado	
no sé	1501	Lector de etiquetas bloqueado	
HACER	3501	Lector de etiquetas desbloqueado	
BD	1865	Etiqueta no registrada	
SG	1381	Dispositivo sin conexión	
XC	3381	Dispositivo restaurado	

Código SIA	Código CID	Descripción	Información del escenario
XT	1384	Batería BAJA	
XR	3384	Voltaje de la batería restaurado	
XL (El número de serie del módulo de salida comienza en 1, el del teclado comienza en 101, el del lector de etiquetas comienza en 201)	1381 (El número de serie del módulo de salida comienza en 1, el del teclado comienza en 101, el del lector de etiquetas comienza en 201)	Dispositivo sin conexión	
XC (El número de serie del módulo de salida comienza en 1, el del teclado comienza en 101, el del lector de etiquetas comienza en 201)	3381 (El número de serie del módulo de salida comienza en 1, el del teclado comienza en 101, el del lector de etiquetas comienza en 201)	Dispositivo restaurado	
SG	1381	Dispositivo sin conexión	
XC	3381	Dispositivo restaurado	
BI	1918	Fallo del transmisor de radar	
DL	3918	Transmisor de radar restaurado	
XT	1384	Batería BAJA	
XR	3384	Voltaje de la batería restaurado	
	1350	Fallo celular	
NR	3350	Celular Restaurado	
	1350	Excepción de tarjeta SIM	
NR	3350	Tarjeta SIM restaurada	
	1350	Fallo de red	
NR	3350	Red restaurada	
XQ	1344	Interferencia detectada	
XH	3344	Atasco restaurado	
	1350	Límite de datos Alcanzado	
XT	1384	Batería BAJA	
XR	3384	Voltaje de la batería restaurado	

Código SIA	Código CID	Descripción	Información del escenario
	1350	Dirección IP ya utilizada	
NR	3350	Dirección IP normal	
	1350	Fallo de red	
NR	3350	Red restaurada	
	1131	Alarma de detección de movimiento Empezado	
BH	3131	Alarma de detección de movimiento Detenido	
BJ	1941	Dispositivo bloqueado	
MD	3941	Alarma de bloqueo de dispositivo restaurado	
		Pérdida de señal de vídeo	
		Señal de video restaurada	
		Formato de entrada/salida Sin par	
		Formato de entrada/salida restaurado	
		Excepción de entrada de video	
		Entrada de video restaurada	
		Disco duro completo	
		Disco duro libre	
		Excepción de disco duro	
		disco duro restaurado	
		No se pudo cargar la imagen	
BQ	1948	Envío de correo electrónico fallido	
BR	1949	Cámara de red Desconectado	
SD	3949	Cámara de red conectada	
		Comprobación de impuestos	
		Publicar respuesta	
BU	1962	Consultoría de alarmas contra incendios	

Código SIA	Código CID	Descripción	Información del escenario
DT	3962	Consulta de alarma contra incendios	
BV	1963	Consultoría de alarmas de coacción	
DU	3963	Consultoría de alarmas de coacción Sobre	
B/N	1964	Alarma médica de emergencia Consultante	
VD	3964	Alarma médica de emergencia consultando sobre	
DW	3250	Firma de patrulla	
BX	1970	Consulta AUTOBÚS	
POR	1971	Registro de AUTOBÚS	
BZ	1973	Desarmado de Zona Única	
DX	3973	Armado de Zona Única	
California	1974	Alarma de zona única borrada	
CB	1306	Dispositivo eliminado	
DY	3306	Dispositivo inscrito	
CC	1976	Consulta de trabajo	
DZ	3976	Consultoría de Negocios	
CD	1306	Dispositivo eliminado	
EE. UU.	3306	Dispositivo inscrito	
CE	1306	Dispositivo eliminado	
EB	3306	Dispositivo inscrito	
FC	1306	Dispositivo eliminado	
CE	3306	Dispositivo inscrito	
C.G.	1306 (El número de serie del módulo de salida comienza en 1, el del teclado comienza en 101, el del lector de etiquetas comienza en 201, el del transmisor comienza en 301)	Dispositivo eliminado	

Código SIA	Código CID	Descripción	Información del escenario
	3306 (El número de serie del módulo de salida comienza en 1, el del teclado comienza en 101, el del lector de etiquetas comienza en 201, el del transmisor comienza en 301)	Dispositivo inscrito	
JA	1461	Contraseña incorrecta	El teclado ingresó una contraseña de operación incorrecta
	1350	Dispositivo sin conexión	
YM	1311	Agotamiento de energía	

## H. Matriz de Comunicación y Comando de Operación

Escanee el código QR para la matriz de comunicación y el comando de operación



Matriz de comunicación AXPRO Comando de operación AXPRO

### Declaración de privacidad del usuario

- El comando debug o zhimakaimen se usa para controlar el acceso al sistema de archivos para garantizar seguridad del dispositivo. Para obtener este permiso, puede ponerse en contacto con el soporte técnico.
- El dispositivo tiene administrador, instalador, mantenimiento, cuenta de operador. Puede usar estas cuentas para acceder y configurar el dispositivo.

### Información de privacidad del usuario Descripción

Clave	La contraseña de la cuenta del dispositivo, utilizada para iniciar sesión en el dispositivo.
Nombre de usuario	El nombre de usuario de la cuenta del dispositivo, que se utiliza para iniciar sesión en el dispositivo.
IP del dispositivo y puerto	La IP y el puerto del dispositivo se utilizan para admitir la comunicación del servicio de red. Para obtener más información, consulte <i>Matriz de comunicación</i> .
Tronco	Se utiliza para registrar información como el estado operativo del dispositivo y los registros de operación.
Información de la base de datos	Se utiliza para registrar información.

## I. Tipos de zonas de detectores

Esta tabla es aplicable a los detectores de la versión 1.2.7, para mostrar los tipos de zona configurables de varios detectores.

Detector	Tipo de zona disponible
Detector PIR inalámbrico	Instantáneo/Retraso/Seguimiento/Tiempo de espera/24 horas/Deshabilitado
Detector inalámbrico DT	Instantáneo/Retraso/Seguimiento/Tiempo de espera/24 horas/Deshabilitado
Contacto magnético inalámbrico	Instantáneo/Retraso/Seguimiento/24 horas/Pánico/Tiempo de espera/ Interruptor de llave/Deshabilitado
Botón de emergencia inalámbrico	Pánico/Zona Médica/desactivado
Detector exterior	Instantáneo/Retraso/Seguimiento/Tiempo de espera/24 horas/Deshabilitado
cámara infrarroja	Instantáneo/Retraso/Seguimiento/24 horas/Deshabilitado
Detector de temperatura y humedad	Instantáneo/Retraso/24 Horas/Deshabilitado
Detector inalámbrico de rotura de cristales	Instantáneo/Retraso/Seguimiento/24 horas/Deshabilitado
Detector de humo inalámbrico	Incendio/Discapacitado
Detector inalámbrico de fugas de agua	Instantáneo/Retraso/24 Horas/Deshabilitado
Detector de calor inalámbrico	Incendio/Discapacitado
Detector inalámbrico de CO	Gas/Discapacitados



www.rosarioseguridad.com.ar

 [ventas@rosarioseguridad.com.ar](mailto:ventas@rosarioseguridad.com.ar)

  +54 9 341 6708000

  +54 9 341 6799822

 [rosarioseguridadok](https://www.instagram.com/rosarioseguridadok)

 [Rosario Seguridad](https://www.youtube.com/RosarioSeguridad)

 [Rosario Seguridad](https://www.facebook.com/RosarioSeguridad)

Grupo Instaladores

 <https://www.facebook.com/groups/591852618012744/>

  +54 9 341 6591429

  +54 9 341 4577532

Avenida Pellegrini 4820 - Presidente Perón 3998 - Rosario - Santa Fe - Argentina

