



Centro de alarmas 2

Manual de usuario



Prefacio

General

Este manual presenta la instalación, las funciones y el funcionamiento del concentrador de alarma 2 (en adelante, el "concentrador"). Lea atentamente antes de usar el dispositivo y conserve este manual para futuras consultas.

Instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

Palabras de señal	Significado
 DANGER	Indica un peligro potencial alto que, si no se evita, provocará la muerte o lesiones graves.
 WARNING	Indica un peligro potencial medio o bajo que, si no se evita, podría provocar lesiones leves o moderadas.
 CAUTION	Indica un riesgo potencial que, si no se evita, podría provocar daños a la propiedad, pérdida de datos, reducciones en el rendimiento o resultados impredecibles.
 ESD	Dispositivos sensibles a la electroestática. Indica un dispositivo que es sensible a la descarga electrostática.
 ELECTRIC SHOCK	Indica alto voltaje peligroso. Tenga cuidado de no entrar en contacto con la electricidad.
 LASER RADIATION	Indica un peligro de radiación láser. Tenga cuidado de evitar la exposición a un rayo láser.
 TIPS	Proporciona métodos para ayudarle a resolver un problema o ahorrar tiempo.
 NOTE	Proporciona información adicional como complemento al texto.

Historial de revisiones

Versión	Contenido de la revisión	Hora de lanzamiento
V1.1.3	Se agregaron nuevas funciones y se revisaron los parámetros técnicos.	Octubre de 2025
Versión 1.1.2	Se agregaron nuevas funciones y se revisaron los códigos de eventos SIA.	Diciembre 2024
Versión 1.1.1	Parámetros técnicos revisados.	Junio de 2024
Versión 1.1.0	Configuración del concentrador revisada.	Abril de 2024
Versión 1.0.0	Primer lanzamiento.	Diciembre 2023

Aviso de protección de la privacidad

Como usuario del dispositivo o controlador de datos, es posible que recopile datos personales de otras personas, como su rostro,

Audio, huellas dactilares y número de matrícula. Debe cumplir con las leyes y normativas locales de protección de la privacidad para proteger los derechos e intereses legítimos de otras personas mediante la implementación de medidas que incluyen, entre otras: proporcionar una identificación clara y visible para informar a las personas sobre la existencia del área de vigilancia y proporcionar la información de contacto requerida.

Acerca del manual

- Este manual es solo de referencia. Podrían existir ligeras diferencias entre el manual y el producto.
- No seremos responsables de pérdidas ocasionadas por el uso del producto de formas que no cumplan con el manual.
- El manual se actualizará según las últimas leyes y regulaciones de las jurisdicciones pertinentes. Para obtener información detallada, consulte el manual de usuario impreso, utilice nuestro CD-ROM, escanee el código QR o visite nuestro sitio web oficial. Este manual es solo de referencia. Podrían existir ligeras diferencias entre la versión electrónica y la versión impresa.
- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto podrían generar diferencias entre el producto real y el manual. Para obtener el programa más reciente y la documentación complementaria, póngase en contacto con el servicio de atención al cliente.
- Podría haber errores de impresión o desviaciones en la descripción de las funciones, operaciones y datos técnicos. En caso de duda o controversia, nos reservamos el derecho de ofrecer una explicación definitiva.
- Actualice el software del lector o pruebe otro software de lectura convencional si no se puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas registradas y nombres de empresas en el manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, comuníquese con el proveedor o el servicio de atención al cliente si ocurre algún problema durante el uso del dispositivo.
- Si existe alguna incertidumbre o controversia, nos reservamos el derecho de explicación final.

Medidas de seguridad y advertencias importantes

Esta sección presenta información sobre el manejo adecuado del dispositivo, la prevención de riesgos y la prevención de daños materiales. Lea atentamente antes de usar el dispositivo y siga las instrucciones al usarlo.

Requisitos de operación



El dispositivo o el control remoto contienen pilas de botón. No ingiera las pilas debido a al riesgo de quemaduras químicas.

Resultado posible: La ingestión de una pila de botón puede provocar quemaduras internas graves y la muerte en un plazo de 2 horas.

Medidas preventivas (incluidas, entre otras):

- Mantenga las baterías nuevas y usadas fuera del alcance de los niños.
- Si el compartimento de la batería no está bien cerrado, deje de utilizar el producto inmediatamente y manténgalo fuera del alcance de los niños.
- Busque atención médica inmediata si cree que una batería fue ingerida o insertada dentro de cualquier parte del cuerpo.



- Asegúrese de que la fuente de alimentación del dispositivo funcione correctamente antes de usarlo.
- No desconecte el cable de alimentación del dispositivo mientras esté encendido.
- Utilice el dispositivo únicamente dentro del rango de potencia nominal.
- Transporte, utilice y almacene el dispositivo en condiciones de humedad y temperatura permitidas.
- Evite que el dispositivo se salpique o gotee con líquidos. Asegúrese de que no haya objetos con líquido sobre el dispositivo para evitar que entren líquidos.
- No desmonte el dispositivo.

Requisitos de instalación



- Conecte el dispositivo al adaptador antes de encenderlo.
- Cumpla estrictamente las normas de seguridad eléctrica locales y asegúrese de que el voltaje en el área sea estable y cumpla con los requisitos de energía del dispositivo.
- No conecte el dispositivo a más de una fuente de alimentación. De lo contrario, podría dañarse.
- Siga los requisitos eléctricos para alimentar el dispositivo.
 - ◇ Los siguientes son los requisitos para seleccionar un adaptador de corriente.
 - La fuente de alimentación debe cumplir con los requisitos de las normas IEC 60950-1 e IEC 62368-1.
 - El voltaje debe cumplir con los requisitos de SELV (voltaje extra bajo de seguridad) y no exceder los estándares ES-1.

- Cuando la potencia del dispositivo no supere los 100 W, la fuente de alimentación debe cumplir los requisitos de LPS y no ser superior a PS2.
- ◇ Recomendamos utilizar el adaptador de corriente proporcionado con el dispositivo.
- ◇ Al seleccionar el adaptador de corriente, los requisitos de suministro de energía (como el voltaje nominal) están sujetos a la etiqueta del dispositivo.



- Observe todos los procedimientos de seguridad y use el equipo de protección requerido provisto para su uso mientras trabaja en alturas.
- No exponga el dispositivo a la luz solar directa ni a fuentes de calor.
- No instale el dispositivo en lugares húmedos, polvorientos o con humo.
- Instale el dispositivo en un lugar bien ventilado y no bloquee el ventilador del dispositivo.
- Conecte los aparatos eléctricos de clase I a una toma de corriente con conexión a tierra de protección.

Tabla de contenido

Prefacio.....	I
Medidas de seguridad y advertencias importantes.....	III
1 Introducción.....	1
1.1 Descripción general.....	1
1.2 Especificaciones técnicas.....	1
1.3 Lista de verificación.....	6
2 Diseño.....	8
2.1 Apariencia.....	8
2.2 Dimensiones.....	9
3 Puesta en marcha.....	10
3.1 Usuarios.....	10
3.2 Proceso de operación.....	11
4 Operaciones DMSS para usuarios finales.....	14
4.1 Registrarse e iniciar sesión en DMSS.....	14
4.2 Agregar dispositivos.....	16
4.2.1 Agregar el Hub.....	16
4.2.2 Agregar periféricos.....	17
4.2.3 Adición de IPC.....	19
4.2.4 Agregar módulo de expansión.....	24
4.3 Configuración de la vinculación de alarmas de vídeo.....	25
4.4 Configuración general del concentrador.....	26
4.4.1 Visualización del estado del concentrador.....	27
4.4.2 Configuración de los parámetros del concentrador.....	29
4.5 Configuración de red.....	36
4.5.1 Configuración de red cableada.....	36
4.5.2 Configuración de la red Wi-Fi.....	37
4.5.3 Configuración celular.....	37
4.6 Administración de dispositivos.....	38
4.6.1 Confianza de dispositivos.....	38
4.6.1.1 Confianza de dispositivos en lotes.....	38
4.6.1.2 Confianza de dispositivos uno por uno.....	39
4.6.2 Compartir dispositivos.....	41
4.6.3 Desvinculación de dispositivos.....	42
4.7 Gestión de áreas.....	42
4.7.1 Agregar área.....	42

4.7.2 Establecer el área como área pública.....	43
4.7.3 Configuración del modo de mantenimiento.....	44
5 Operaciones generales.....	45
5.1 Armado y desarmado único.....	45
5.2 Armado y desarme global.....	46
5.3 Armado y desarmado manual.....	47
5.4 Armado y desarmado programado.....	47
5.5 Armado y desarmado controlados por SMS.....	48
Apéndice 1 Eventos de falla de armado y descripción.....	50
Apéndice 2 Códigos y descripción de eventos de SIA.....	52
Apéndice 3 Compromiso y recomendación de seguridad.....	57

1 Introducción

1.1 Descripción general

El concentrador de alarmas es un dispositivo central del sistema de seguridad que controla el funcionamiento de todos los periféricos conectados. Si el sistema de seguridad detecta la presencia, entrada o intento de entrada de un intruso en el área armada, el concentrador recibirá las señales de alarma de los detectores y alertará a los usuarios.

1.2 Especificaciones técnicas

Esta sección contiene las especificaciones técnicas del dispositivo. Consulte las que correspondan a su modelo.

Tabla 1-1 Especificaciones técnicas

Tipo	Parámetro	Descripción
Puerto	Entrada de alarma	64 canales ampliables
	Salida de alarma	64 canales ampliables
	Inalámbrico Periférico	150 periféricos (incluidos dispositivos inalámbricos y con cable): específicamente, hasta 64 llaveros inalámbricos hasta 8 teclados inalámbricos hasta 6 sirenas inalámbricas (incluidas 4 sirenas de intercomunicador) hasta 4 repetidores inalámbricos Hasta 64 cámaras PIR inalámbricas (incluidas cámaras PIR para interiores, cámaras PIR para exteriores y detectores de triple tecnología) hasta 16 transmisores de E/S múltiples Hasta 16 módulos expansores RS-485 (incluidos expansores de entrada y de salida)
	Área	32 áreas (habitaciones)
	Modo de red	Ethernet, Wi-Fi y red celular (admite la instalación de dos tarjetas SIM. Solo se puede habilitar una tarjeta a la vez)
	Puerto de red	1 puerto Ethernet RJ-45, 10 Mbps/100 Mbps.
	Acumulador	Una batería de litio recargable de 4.750 mAh incorporada.
Video y audio	Entrada de vídeo	hasta 8 IPC a bordo
	Salida de audio	1 canal
	Control de volumen	Sí
	Transmisión de voz	Teléfono y altavoz local
Función	Luz indicadora	El indicador indica el estado de las alarmas, el armado y desarmado, la conexión de red y la falla del dispositivo.

Tipo	Parámetro	Descripción		
	Botón	Incluye un botón de reinicio, un botón de voltaje y un botón de cambio de AP.		
	SMS	Sí (hasta 12 números de teléfono)		
	Llamada telefónica	Sí (hasta 12 números de teléfono)		
	Enlace de vídeo	Sí		
	Caché sin conexión	Almacena hasta 50 mensajes de alarma.		
	Armar y desarmar Método	App, teclado, control remoto, tarjeta, SMS, armado y desarmado programado.		
	Actualización remota	Actualización de la nube		
	Batería baja Detección	Sí		
	Usuario Gestión	33 usuarios de la aplicación (31 usuarios generales, 1 usuario administrador y 1 instalador) y 32 usuarios del teclado		
	Registros	Hasta 5.000 entradas		
	Transmisión Protocolo	SIA, SoftGuard		
Inalámbrico	Frecuencia portadora	DHI-ARC3800H-FW2(868)/DHI-ARC3800H-FW2: 868,0 MHz– 868,6 MHz	DHI-ARC3800H-FW2/DHI-ARC3800H-W2: 433,1 MHz– 434,6 MHz	DHI-ARC3800H-FW2(915)/DHI-ARC3800H-W2 (915): 915 MHz-928 MHz
	Transmisor Potencia (EIRP)	DHI-ARC3800H-FW2(868)/DHI-ARC3800H-FW2: Límite de 25 mW	DHI-ARC3800H-FW2/DHI-ARC3800H-W2: Límite de 10 mW	DHI-ARC3800H-FW2(915)/DHI-ARC3800H-W2(915): Límite de 1W
	Comunicación Mecanismo	Bidireccional		
	Comunicación Distancia	DHI-ARC3800H-FW2(868)/DHI-ARC3800H-FW2: Hasta 2.000 m (6,561.68 pies) en un espacio abierto	DHI-ARC3800H-FW2/DHI-ARC3800H-W2: Hasta 1.200 m (3.937,01 pies) en un espacio abierto	DHI-ARC3800H-FW2(915)/DHI-ARC3800H-W2(915): Hasta 2.000 m (6,561.68 pies) en un espacio abierto
	Modo de cifrado	AES128		
	Frecuencia Saltando	Sí		
General	Idioma	Compatible con 17 idiomas: árabe, checo, danés, neerlandés, inglés, francés, alemán, italiano, portugués (Europa), ruso, español (Latinoamérica), español (Europa), turco, eslovaco, polaco, griego y búlgaro. El idioma predeterminado es inglés.		

Tipo	Parámetro	Descripción
	Fuente de alimentación	100–240 VCA, 50/60 Hz
	Tiempo de espera	La batería dura hasta 12 horas cuando está completamente cargada y está dentro de las siguientes condiciones: Está conectado al Wi-Fi, su ID está conectado a la central receptora de alarmas, el intervalo de latidos es de 1.800 segundos y está conectado a 8 periféricos y la nube.
	Fuerza Consumo	220 VCA 80 mA (máx.) 220 VCA 40 mA (en espera)
	Operante Temperatura	Cuando la batería no se está cargando: -10 °C a +55 °C (+14 °F a + 131 °F) Cuando la batería se está cargando: 0 °C a +45 °C (+32 °F a + 113 °F)
	Operante Humedad	10%–90% (HR)
	Producto Dimensiones	174,8 mm × 174,8 mm × 38,3 mm (6,88" × 6,88" × 1,51") (largo × ancho × alto)
	Peso neto	510 g (1,12 libras)
	Peso bruto	860 g (1,90 libras)
	Instalación	Admite instalación en pared y en escritorio.
	Material de la carcasa	PC + ABS

Tipo	Parámetro	Descripción		
	Certificaciones	DHI-ARC3800H-FW2(868)/ DHI-ARC3800H-W2(868): EN 50131-1:2006+A1:2009 + A2:2017+A3:2020 EN 50131-3:2009 EN 50131-6:2017+A1:2021 EN 50131-5-3:2017 EN 50131-10:2014 EN 50136-2:2013+A1:2023 Grado de seguridad 2 (IMQ-SISTEMI DE SEGURIDAD) Ambiental Clase II Categoría ATS: SP2/DP2 CE  Proceso de dar un título IMQ-SISTEMI DI SICUREZZA es obligatorio administrar sistema con Aplicación DMSS para nivel de acceso 2, y DoLynK Cuidado del acceso nivel 3	DHI-ARC3800H-FW2/ DHI-ARC3800H-W2: CE	DHI-ARC3800H-FW2(915)/DHI-ARC3800H-W2(915): /
	Anticorrosión Nivel	Protección básica *Los productos están diseñados para uso general y son aplicables incluso en áreas sin requisitos específicos de protección anticorrosión.		

Tipo	Parámetro	Descripción
	Almacenamiento Temperatura	- 10 °C a +55 °C (+14 °F a +131 °F)
	Humedad de almacenamiento	10%-90% (HR)
	Embalaje Dimensiones	254 mm × 211 mm × 61 mm (10,00" × 8,31" × 2,40") (largo × ancho × alto), independiente en la caja interior 524 mm × 508 mm × 442 mm (20,63" × 20,00" × 17,40") (largo × ancho × alto), estuche protector
Wifi	Estándar Wi-Fi	IEEE 802.11b/g/n
	Frecuencia de Wi-Fi Rango	2400-2483,5 MHz
	Energía Wi-Fi Transmisión	≤20 dBm a 2400-2483,5 MHz
Celular Red	Red celular Estándar	Estándar de red celular
	Rango de frecuencia	UE: 4G: LTE FDD: B1/B3/B7/B8/B20/B28A; LTE TDD: B38/B40/B41; 3G: WCDMA: B1/B8; 2G: GSM: 1.800/900 MHz;
	Transmisor Potencia (EIRP)	4G: Clase de potencia 3: 23 dBm ± 2 dB 3G: Clase de potencia 3: 24 dBm + 1/-3 dB 2G: Clase de potencia 0: 30 dBm ± 3 dB (GSM900) Clase de potencia 5: 33 dBm ± 3 dB (GSM1800)

Tabla 1-2 Categoría ATE

COMIÓ Categoría	Informes Tiempo	Protocolos	Dispositivos de comunicación			Comunicación Dispositivo a utilizar
			PSTN	2G/3G	Propiedad intelectual	
SP2	25 horas	Estándar	√			El cheque marcado comunicación dispositivo
SP3	30 minutos	Estándar		√	√	Solo uno de los dos está marcado comunicación dispositivos
SP4	3 minutos	Encriptado		√	√	Solo uno de los dos está marcado comunicación dispositivos

COMIÓ Categoría	Informes Tiempo	Protocolos	Dispositivos de comunicación			Comunicación Dispositivo a utilizar
			PSTN	2G/3G	Propiedad intelectual	
SP5	Años 90	Encriptado		✓	✓	Solo uno de los dos está marcado comunicación dispositivos
DP1	25 horas	Estándar	✓	✓	✓	Sólo dos de los tres marcas de verificación comunicación dispositivos
DP2	30 minutos	Estándar	✓	✓	✓	Sólo dos de los tres marcas de verificación comunicación dispositivos
DP3	3 minutos	Encriptado		✓	✓	Los dos cheques marcado comunicación dispositivos
DP4	Años 90	Encriptado		✓	✓	Los dos cheques marcado comunicación dispositivos

ATE: Equipo de transmisión de alarma.

SPx (Single Path): Valor que indica el nivel de rendimiento alcanzado por un único dispositivo de comunicación, según la norma EN 50136-1.

DPx (Double Path): Valor que indica el nivel de rendimiento alcanzado por una combinación de dos dispositivos de comunicación, según la norma EN 50136-1.

Tiempo de reporte: El tiempo de reporte se establece según el estándar de cada nivel de rendimiento. El tiempo de reporte es el tiempo máximo disponible para informar cuando falla un dispositivo de transmisión de alarma. Los dispositivos de transmisión de alarma cumplen este requisito informando periódicamente su estado mediante una función de prueba simbólica específica.

Protocolos: Indica el nivel de seguridad de los protocolos que se utilizarán para la notificación de fallos. Los protocolos estándar y de voz están cifrados. Los protocolos de alta seguridad se cifran con una clave AES de 128 o 256 bits.

Dispositivos de comunicación: Dispositivos de comunicación implementados.

Dispositivos de comunicación a utilizar: Indica el número y cuáles dispositivos de comunicación se utilizarán en función de la categoría ATE.

SP2: LAN/WiFi usando la NUBE, Aplicación DMSS (tiempo de informe predeterminado 150") o ARCO tiempo de presentación de informes mín. 25 h);

DP2: primaria LAN/WiFi usando la NUBE, Aplicación DMSS (tiempo de informe predeterminado 150") o ARCO tiempo de reporte mín. 30 min) y secundaria GPRS/4G usando la NUBE Aplicación DMSS (tiempo de informe predeterminado 150") o ARCO tiempo de informe mín. 30 min)/

1.3 Lista de verificación

Revise el paquete con la siguiente lista. Si alguno de los artículos está dañado o falta, comuníquese con

servicio al cliente.

Figura 1-1 Lista de verificación

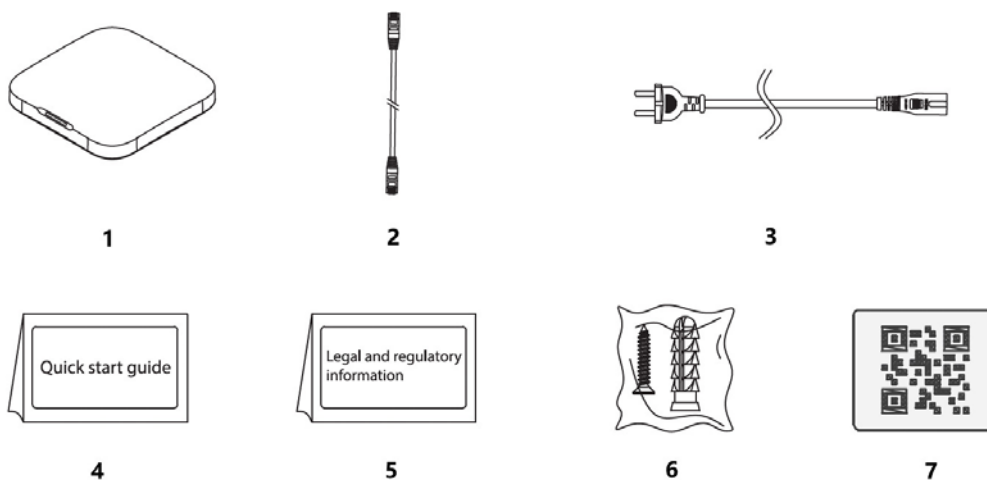


Tabla 1-3 Lista de verificación

No.	Nombre del artículo	Cantidad	No.	Nombre del artículo	Cantidad
1	Centro de alarmas 2	1	5	Legal y regulatorio información	1
2	Cable	1	6	Paquete de tornillos	2
3	Adaptador	1	7	Código QR	1
4	Guía de inicio rápido	1	—	—	—

2 Diseño

2.1 Apariencia

Figura 2-1 Apariencia

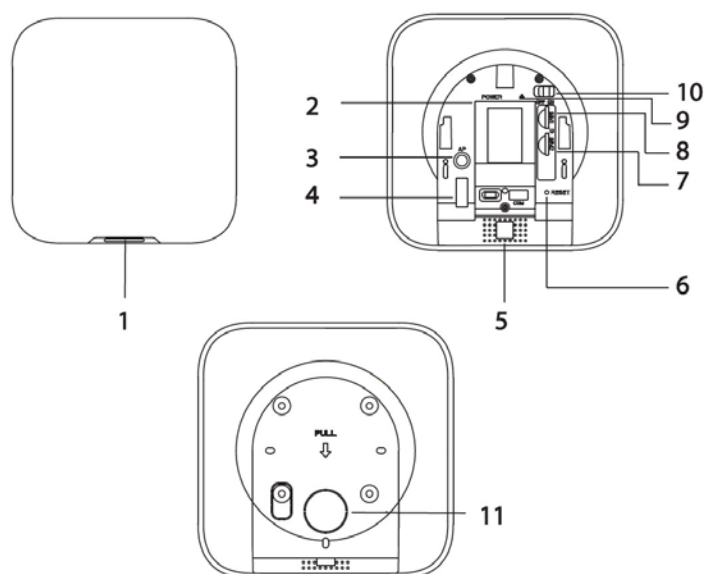


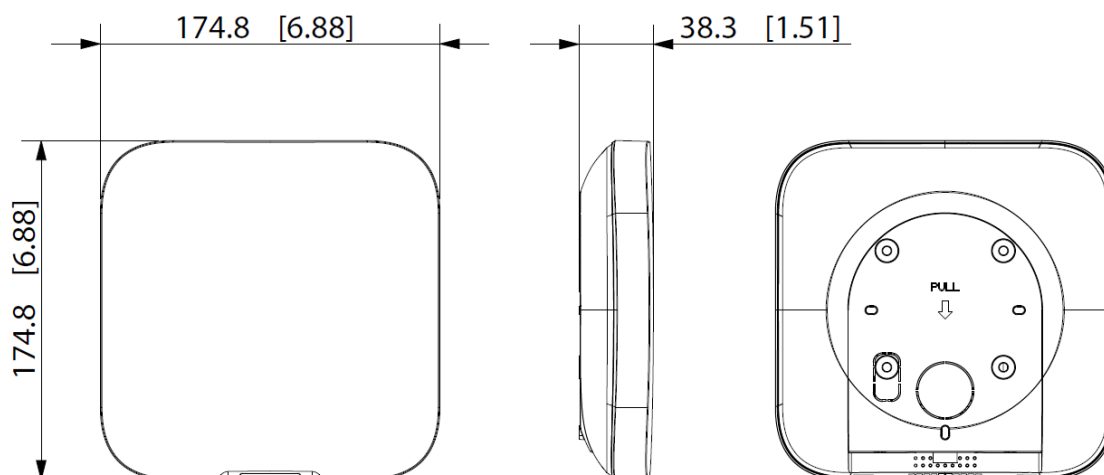
Tabla 2-1 Estructura

No.	Nombre	Descripción
1	Indicador	● Parpadea lentamente en verde: modo de sensibilidad reducida. ● Parpadea en verde: el concentrador comienza a funcionar. ● Amarillo sólido: Error en la conexión a la nube. ● Verde sólido: modo de desarmado. ● Azul sólido: modo de armado. ● Parpadea en rojo: se activó un evento de alarma. ● Parpadea en amarillo: se detectó un mal funcionamiento. ● Parpadea en azul: se está ejecutando la configuración de AP o el concentrador se está emparejando con periféricos. ● Parpadea rápidamente en azul: modo de emisión de tarjeta.
2	Puerto de alimentación	Conectar a la fuente de alimentación.
3	Botón AP	Mantenga presionado el botón durante 2 segundos para activar la función AP. El teléfono se conectará al punto de acceso desde el concentrador y sincronizará el nombre de usuario y la contraseña de Wi-Fi con el concentrador. También puede desactivar el AP manteniendo presionado el botón durante 2 segundos cuando esté habilitado.
4	Interruptor de seguridad	Cuando se suelta el interruptor antimanipulación, se activará la alarma antimanipulación.
5	Vocero	Generar sonido.

No.	Nombre	Descripción
6	Botón de reinicio	Mantenga presionado el botón durante 10 segundos para reiniciar el concentrador y restaurar la configuración predeterminada de fábrica.
7	Ranura para SIM 2	Instale la tarjeta principal en la primera ranura y la tarjeta de reserva en la segunda ranura. ● Admite tarjetas SIM duales y modo de espera único. ● Las tarjetas SIM permiten que el concentrador utilice datos celulares y envíe notificaciones de alarma.  ● Las tarjetas SIM no funcionarán hasta que se haya configurado la red. se ha completado ● La función SIM solo está disponible en modelos seleccionados.
8	Ranura para SIM 1	
9	Toma de cable Ethernet	Conecte el concentrador a Ethernet.
10	Interruptor de encendido	Encender o apagar el concentrador.
11	Contraportada	Si se abre la tapa trasera, se activará la alarma antimanipulación.

2.2 Dimensiones

Figura 2-2 Dimensiones (Unidad: mm [pulgadas])



3 Puesta en marcha

3.1 Usuarios

Los usuarios solo se pueden crear en la aplicación DMSS. Clasifique a los usuarios en diferentes roles para que tengan distintos niveles de acceso para operar los dispositivos.

Para la Certificación IMQ-SISTEMI DI SICUREZZA es obligatorio gestionar el sistema con APP DMSS para el nivel de acceso 2, y DoLynk Care para el nivel de acceso 3.

Nivel de acceso de usuario

Tabla 3-1 Nivel de acceso del usuario

Usuario	Nivel de acceso
Usuario administrador de DMSS	L2
Usuario general del DMSS	L2
Instalador	L3

- Instalador: Los instaladores proporcionan servicios de operación y mantenimiento a los usuarios finales. Este rol debe solicitar permisos al usuario final (usuario administrador de DMSS) para operar el dispositivo. Pueden obtener permisos como la configuración del dispositivo y la gestión de usuarios.
- Usuario administrador de DMSS: El usuario administrador sería un usuario final. Este rol no se puede modificar y tiene permisos, como la configuración del dispositivo y la gestión de usuarios. Los usuarios administradores de DMSS no tienen permiso para configurar el dispositivo cuando los instaladores les prestan el concentrador ni cuando se lo confían.
- Usuario general de DMSS: Son usuarios con quienes un administrador de DMSS comparte dispositivos a través de la aplicación DMSS. Este rol se puede modificar y solo tiene permisos básicos, como ver el estado del dispositivo y armar y desarmar salas.

Flujo de negocios

A continuación se muestra el proceso de encomendar y compartir dispositivos en la aplicación DMSS. Los instaladores y usuarios finales pueden seguir el proceso para compartir y encomendar dispositivos.

Figura 3-1 Flujo de negocio (usuario DMSS)

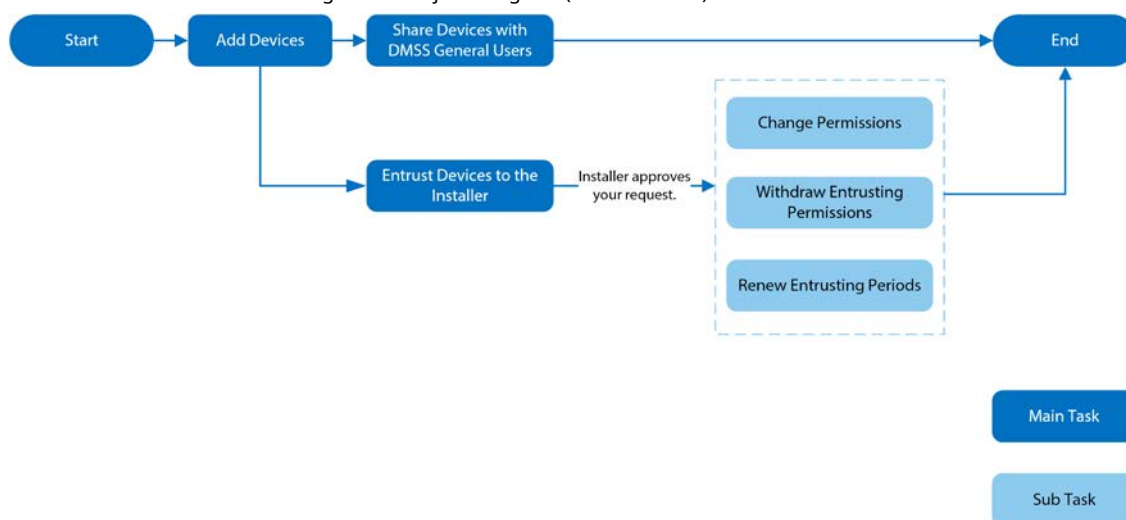
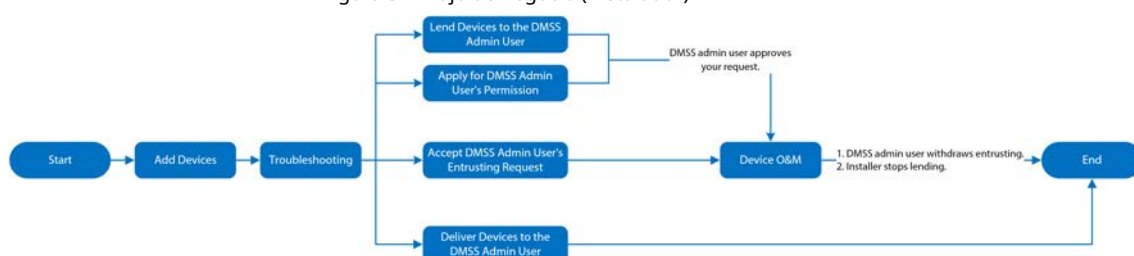


Figura 3-2 Flujo de negocio (Instalador)



3.2 Proceso de operación

Siga los procedimientos a continuación para encender el sistema de alarma inalámbrico.

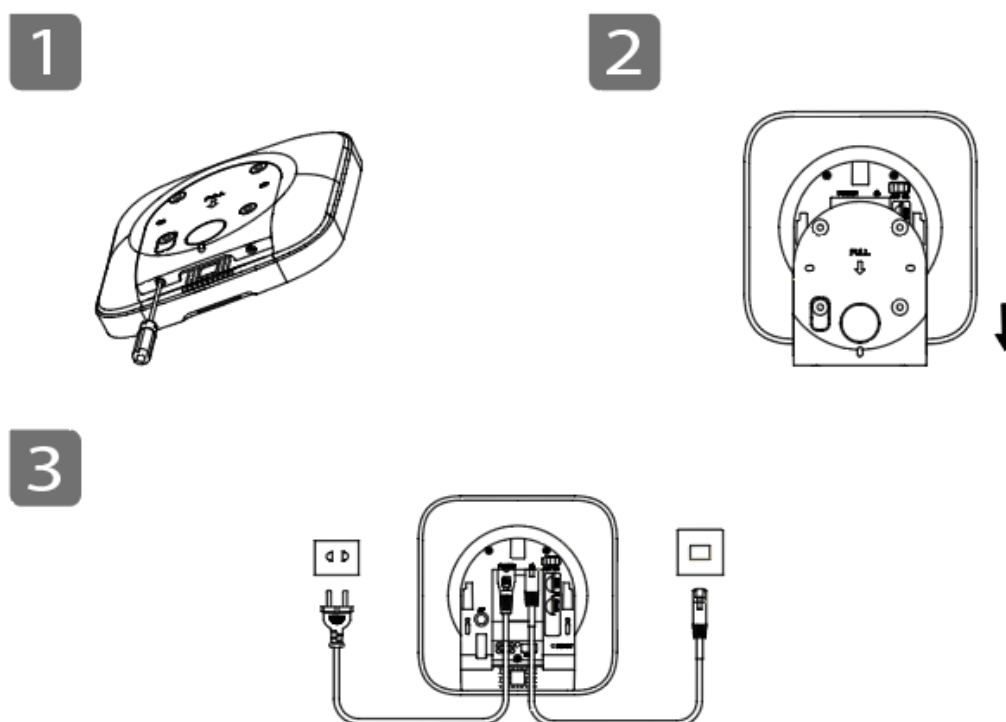
Figura 3-3 Proceso de operación



Encendido

Conecte el concentrador a Ethernet y enciéndalo.

Figura 3-4 Encendido



Agregar dispositivos

1. Agregue el concentrador a la aplicación DMSS.
2. Agregue los periféricos al concentrador.

Instalación del concentrador

Recomendamos usar tornillos de expansión para instalar el concentrador. No lo coloque en las siguientes zonas:

- Al aire libre.
- Lugares cercanos a objetos metálicos que provoquen atenuación y apantallamiento de la señal de radio.
- **Lugares con señal GSM débil.**
- Lugares cercanos a fuentes de interferencia de radio que estén a menos de 1 metro del enrutador y los cables de alimentación.
- Lugares donde la temperatura y la humedad superan los límites permitidos.

Figura 3-5 Instalación

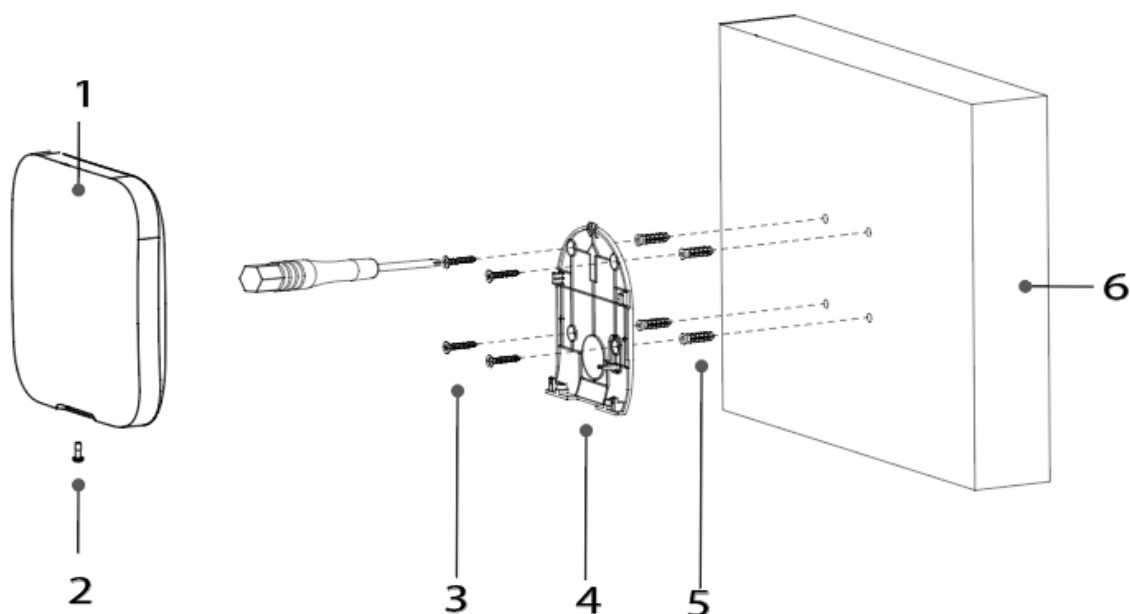


Tabla 3-2 Elementos de instalación

No.	Nombre del artículo	No.	Nombre del artículo
1	Centro	4	Placa de montaje
2	Tornillo de cabeza avellanada M3 × 8 mm	5	Perno de expansión
3	Tornillo autorroscante ST4 × 25 mm	6	Muro

1. Confirme la posición de los orificios de los tornillos y luego perforelos en la placa de montaje.
2. Coloque los pernos de expansión en los orificios.
3. Coloque la placa de montaje en la pared y luego alinee los orificios de los tornillos en la placa con los pernos de expansión.
4. Fije la placa de montaje con tornillos autorroscantes ST4 × 25 mm.
5. Coloque el concentrador de alarma en la placa de montaje de arriba a abajo.
6. Fije el concentrador de alarma y la placa de montaje con tornillos de cabeza avellanada M3 × 8 mm.

Configuración del concentrador

Configure el concentrador en la aplicación DMSS.

Activación del sistema de alarma

Puede usar el teclado, el mando a distancia y la app para armar el sistema. Tras enviar un comando de armado a la app DMSS, el sistema comprobará su estado. Si el sistema presenta una falla, deberá decidir si desea armarlo a la fuerza. Para obtener más información sobre los periféricos, consulte el manual del usuario del dispositivo correspondiente.

4 Operaciones DMSS para usuarios finales

La aplicación DMSS ofrece servicios profesionales de vigilancia de seguridad para usuarios finales. Los usuarios administradores de DMSS pueden compartir el concentrador con usuarios generales de DMSS y confiarlo a una sola empresa. Los periféricos incluidos con el concentrador se pueden compartir y confiar simultáneamente. Para compartir y confiar el concentrador usted mismo, debe instalar la última versión de la aplicación DMSS.



Las figuras son sólo de referencia y pueden diferir de la interfaz real.

4.1 Registrarse e iniciar sesión en DMSS

El sistema de seguridad se configura y controla mediante la app DMSS. Puede acceder a ella en iOS y Android. Esta sección utiliza las operaciones en iOS como ejemplo.



Asegúrese de tener instalada la última versión de la aplicación.

Procedimiento

Paso 1 Busque DMSS en la tienda de aplicaciones y luego descargue la aplicación.



Para los usuarios de Android, pueden ir a Google Play para descargar DMSS.

Paso 2 En tu teléfono, toca  para iniciar la aplicación.

Paso 3 Crear una cuenta.

- 1) Toque **Inscribirse**.
- 2) Seleccione un país o región de la lista.
- 3) Ingrese el correo electrónico y contraseña para el registro.



Grifo  para mostrar la contraseña y el icono se convertirá en .

4) Seleccione el **He leído y acepto el Acuerdo de registro de DMSS, la Política de privacidad y la Política de privacidad de DoLynk Pass**.

5) Toque **Obtener código de verificación**, revise su casilla de correo electrónico en busca del código de verificación y luego introdúzcalo.

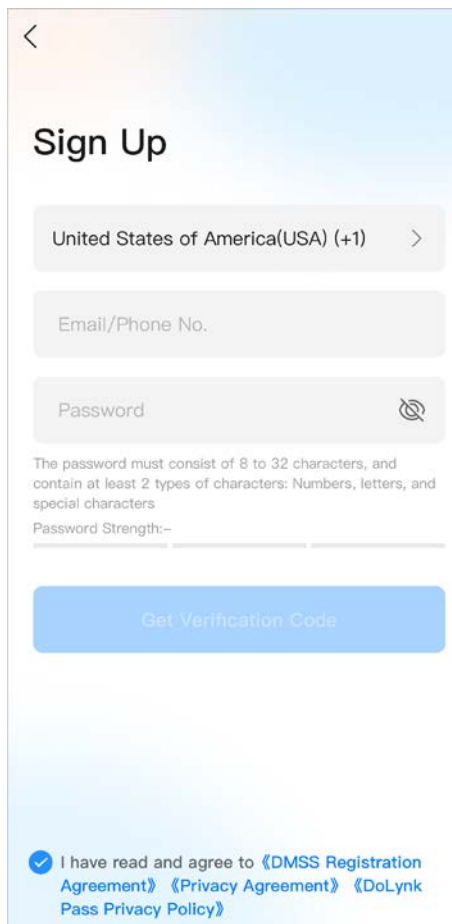


Utilice el código de verificación dentro de los 60 segundos posteriores a su recepción. De lo contrario, la verificación...

El código dejará de ser válido.

6) Toque **DE ACUERDO**.

Figura 4-1 Registrarse



Sign Up

United States of America(USA) (+1) >

Email/Phone No.

Password 

The password must consist of 8 to 32 characters, and contain at least 2 types of characters: Numbers, letters, and special characters

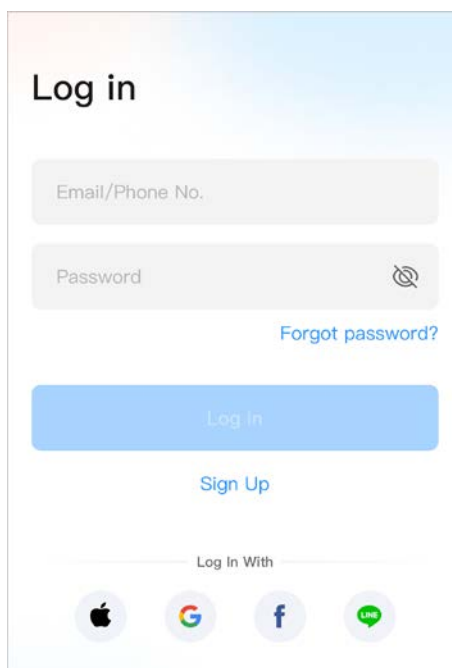
Password Strength:--

Get Verification Code

☒ I have read and agree to [《DMSS Registration Agreement》](#) [《Privacy Agreement》](#) [《DoLynk Pass Privacy Policy》](#)

Paso 4 Regresar a la **Acceso** pantalla, ingrese su correo electrónico y contraseña, y luego toque **Acceso**.

Figura 4-2 Inicio de sesión



Log in

Email/Phone No.

Password 

[Forgot password?](#)

Log In

[Sign Up](#)

Log In With



Puede modificar la contraseña en el **A mí** > **Gestión de cuentas** > **Modificar contraseña**.

4.2 Agregar dispositivos

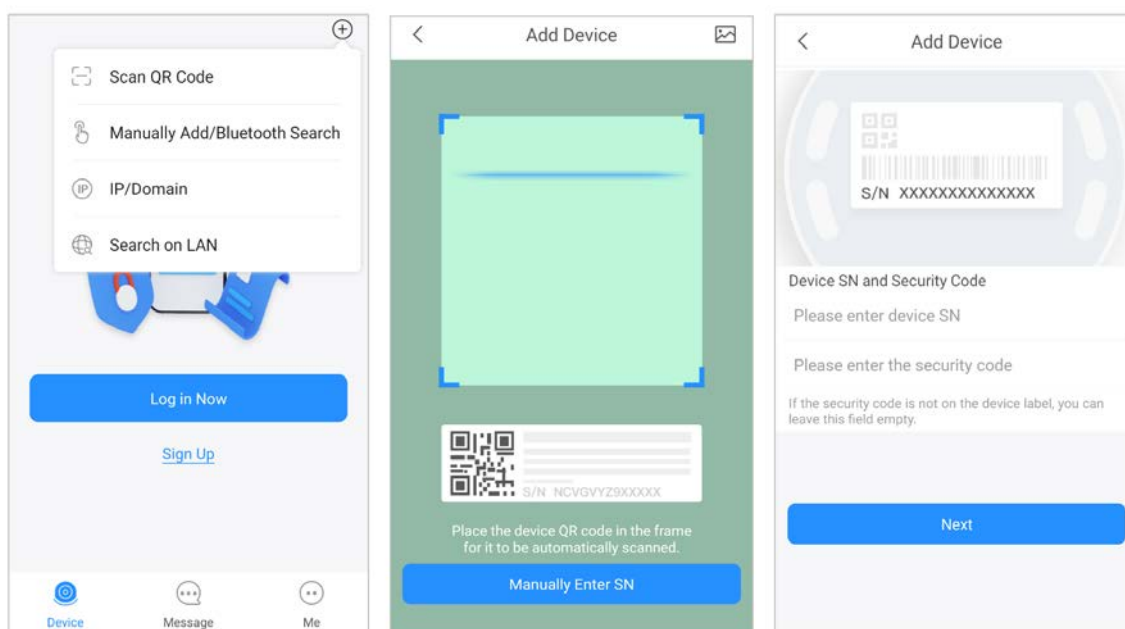
Para los usuarios finales, puede agregar dispositivos de alarma a la aplicación DMSS.

4.2.1 Agregar el Hub

Procedimiento

Paso 1 En el **Dispositivo** pantalla, toque , y luego seleccione **Escanear código QR**.

Figura 4-3 Agregar por código QR



Paso 2 Agregar un dispositivo.

- Escanee el código QR del dispositivo directamente o toque el  e importe la imagen del código QR para agregar un dispositivo.
- **Grifo Introducir SN manualmente** Ingrese el número de serie del dispositivo para agregarlo manualmente. Seleccione el tipo de dispositivo y toque **Próximo**.

Paso 3



Grifo Próximo Si el sistema identifica automáticamente el tipo de dispositivo.

Paso 4 En el **Agregar dispositivo** pantalla, personalice el nombre del dispositivo, ingrese el nombre de usuario y la contraseña del dispositivo y luego toque **Ahorrar**. Configurar los ajustes de red.

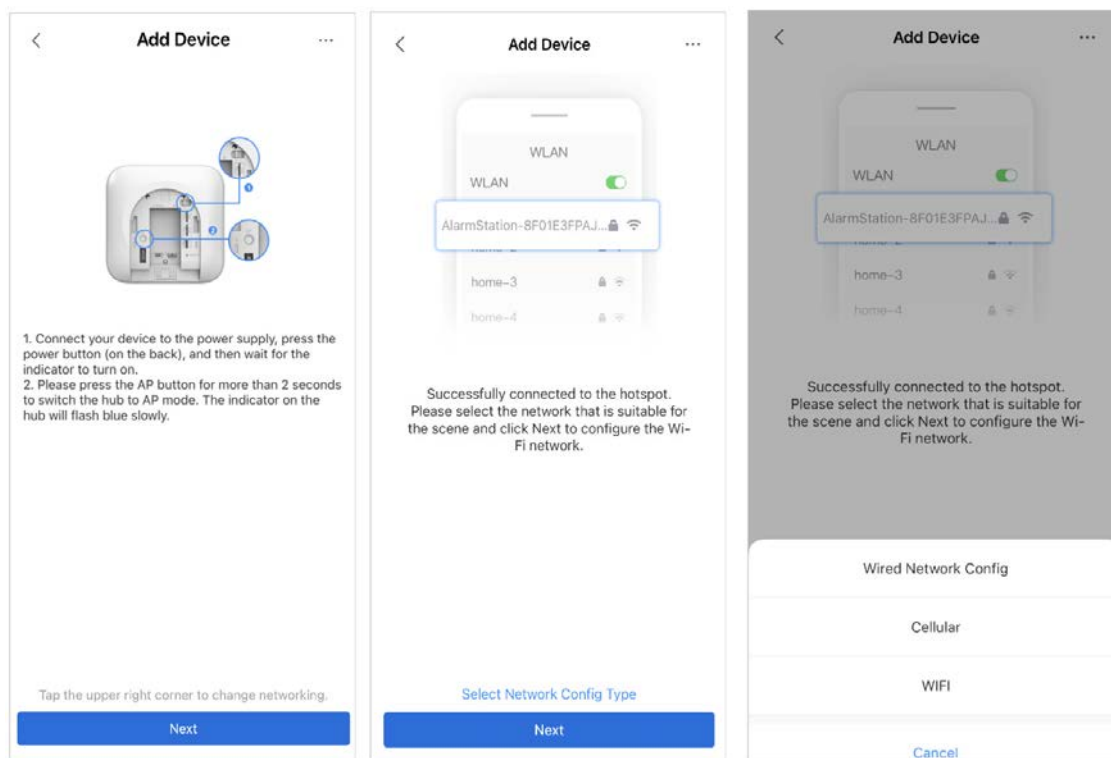
Paso 5

- 1) En el **Agregar dispositivo**, grifo **Próximo** para unirse al punto de acceso del hub.
- 2) Cuando la conexión se haya establecido correctamente, toque **Seleccionar el tipo de configuración de red**.
- 3) Seleccione los tipos de red que desea configurar.
- Red cableada: habilite la función DHCP o ingrese manualmente la dirección IP y la máscara de subred.

puerta de enlace, DNS y dirección MAC.

- Celular: Configure el APN, modo de autorización, nombre de usuario, contraseña, número de marcación, datos de roaming para la tarjeta SIM.
- Wi-Fi: seleccione una red Wi-Fi y luego ingrese la contraseña para conectarse a ella.

Figura 4-4 Configurar tipos de red

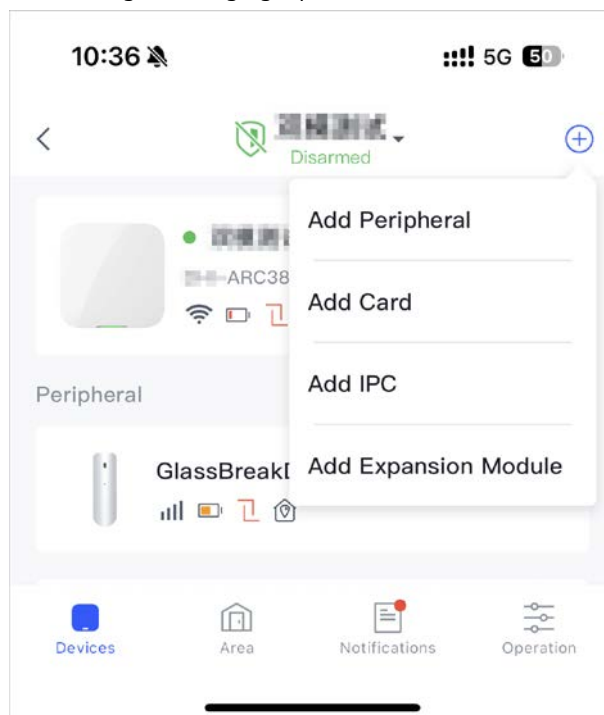


4.2.2 Agregar periféricos

Puede agregar varios periféricos al concentrador. Para obtener más información sobre cómo agregarlos, consulte los manuales de usuario de cada uno.

Ir a la **Dispositivos** pantalla del concentrador y luego seleccione  > **Agregar periférico**.

Figura 4-5 Agregar periférico



Agregar uno por uno

1. Escanee el código QR en la parte inferior del dispositivo y luego toque **Próximo**.
También puede ingresar el número de serie del periférico tocando **SN**, seleccione una imagen de código QR de **Mis archivos** para agregar los periféricos.
2. Siga las instrucciones en pantalla y encienda el dispositivo, luego toque **Próximo**.
3. Espere el emparejamiento.
4. Personalice el nombre del dispositivo, seleccione el área y luego toque **Terminado**.

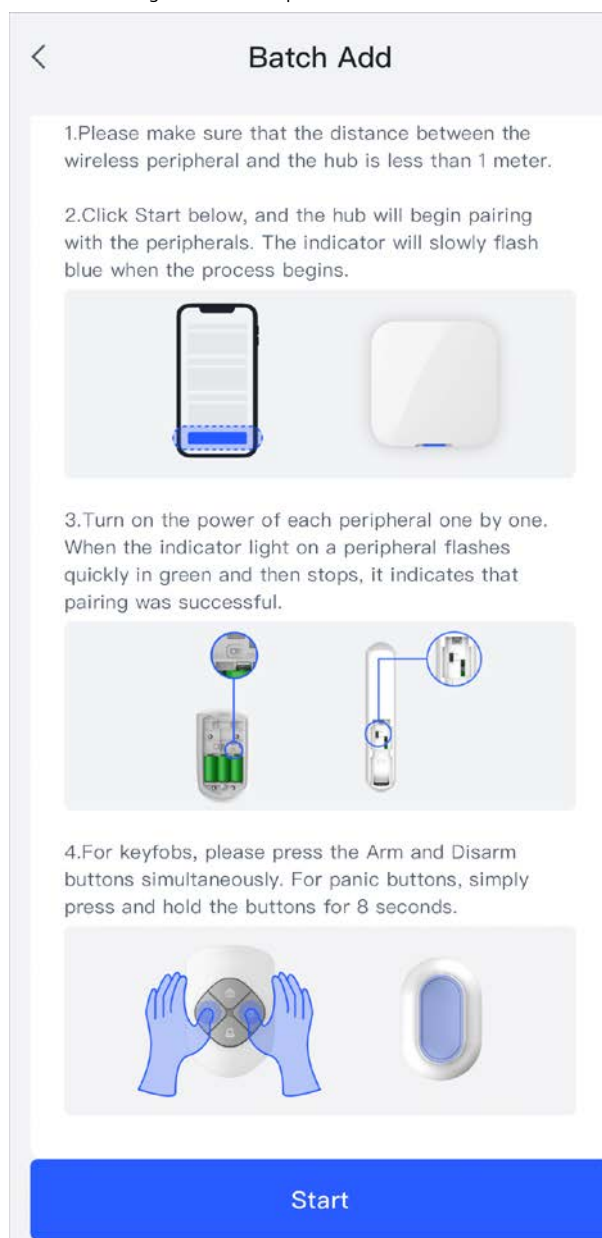
Agregar en lotes

Grifo **Bach Añadir**, y luego toque **Comenzar** para iniciar el emparejamiento.



- Asegúrese de que la distancia entre los periféricos y el concentrador sea inferior a 1 metro.
- Encienda el periférico. Cuando la luz indicadora del periférico parpadee rápidamente en Verde y luego se apaga, lo que indica que el emparejamiento se realizó correctamente. Repita este paso para agregar periféricos. uno por uno. Tenga cuidado de no encender los periféricos a la vez.
- Para llaveros, presione el **Brazo y Desarmar**. Presione simultáneamente los botones para iniciar el emparejamiento. Para evitar el pánico Botones, mantenga presionado el botón durante 8 segundos para ir al modo de emparejamiento.

Figura 4-6 Adición por lotes



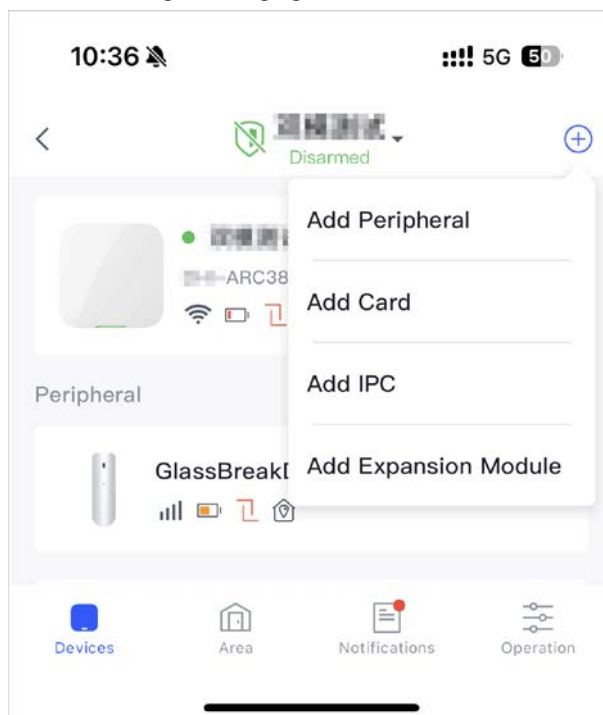
4.2.3 Adición de IPC

Añade IPC al concentrador.

Procedimiento

Paso 1 Ir a la **Dispositivos** pantalla del concentrador y luego seleccione > **Añadir IPC**.

Figura 4-7 Agregar IPC



Paso 2

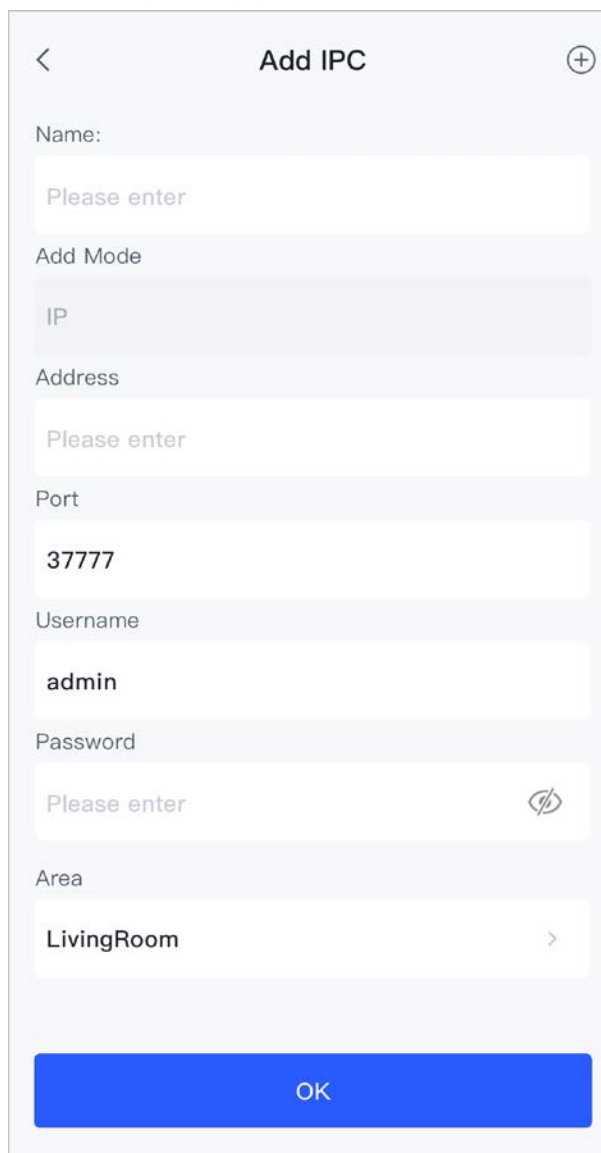
Añade un IPC al concentrador.



Agregar manualmente:

1. Configure el nombre del dispositivo, la dirección IP del IPC, el número de puerto, el nombre de usuario y la contraseña del IPC, y seleccione el área donde está asignado el IPC y luego toque **DE ACUERDO**.

Figura 4-8 Agregar manualmente

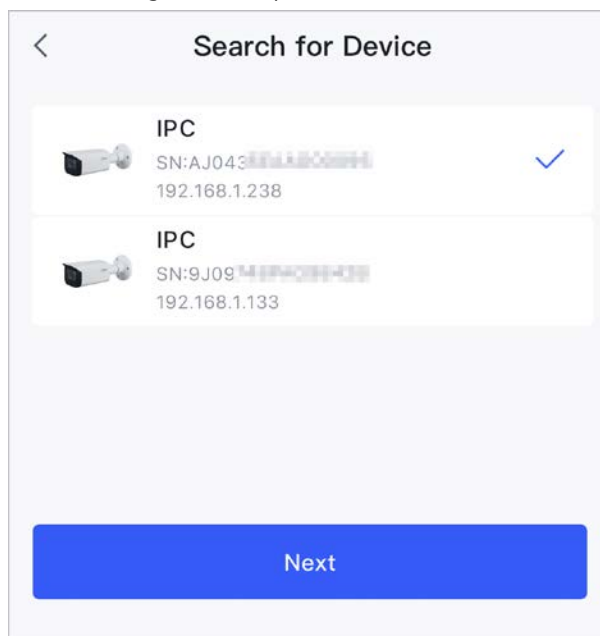


2. Seleccione el canal del IPC y luego toque **DE ACUERDO**.

● Búsqueda en línea:

1. Toque  y seleccione **Buscar en LAN** para buscar el IPC en la misma red segmento.

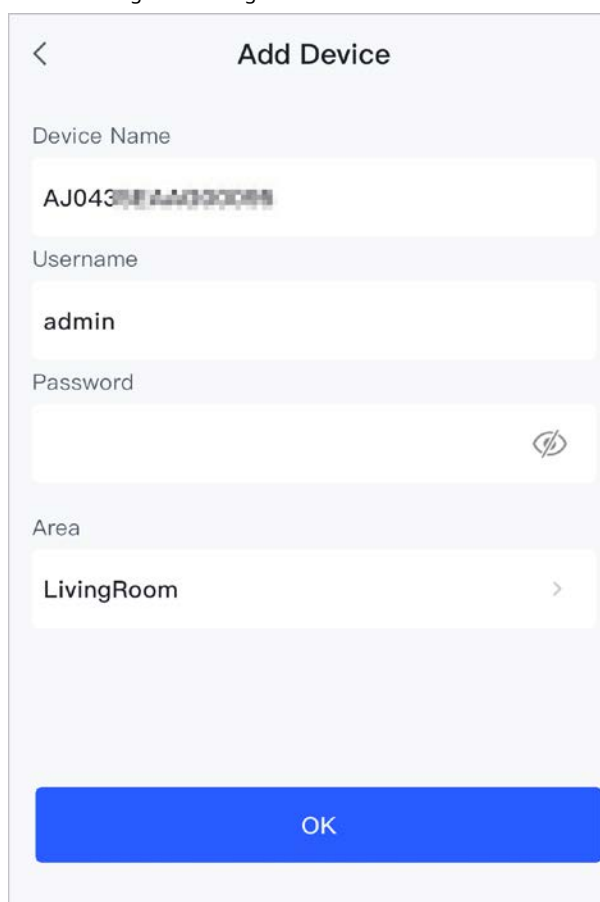
Figura 4-9 Búsqueda en línea



2. Toque **Próximo**.

3. Ingrese la contraseña del IPC y seleccione el área donde está asignado el IPC, luego toque **DE ACUERDO**.

Figura 4-10 Ingresar contraseña



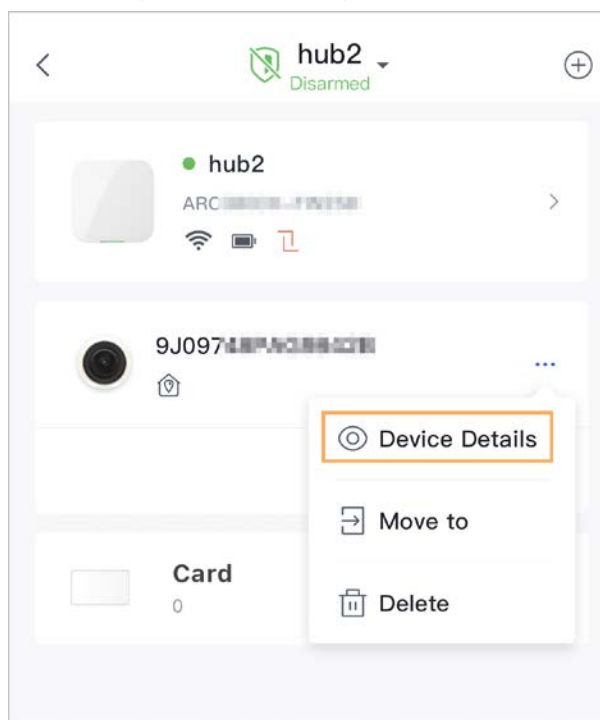
4. Seleccione el canal del IPC y luego toque **DE ACUERDO**.

Operaciones relacionadas

Puede configurar los parámetros del IPC agregado. 1.

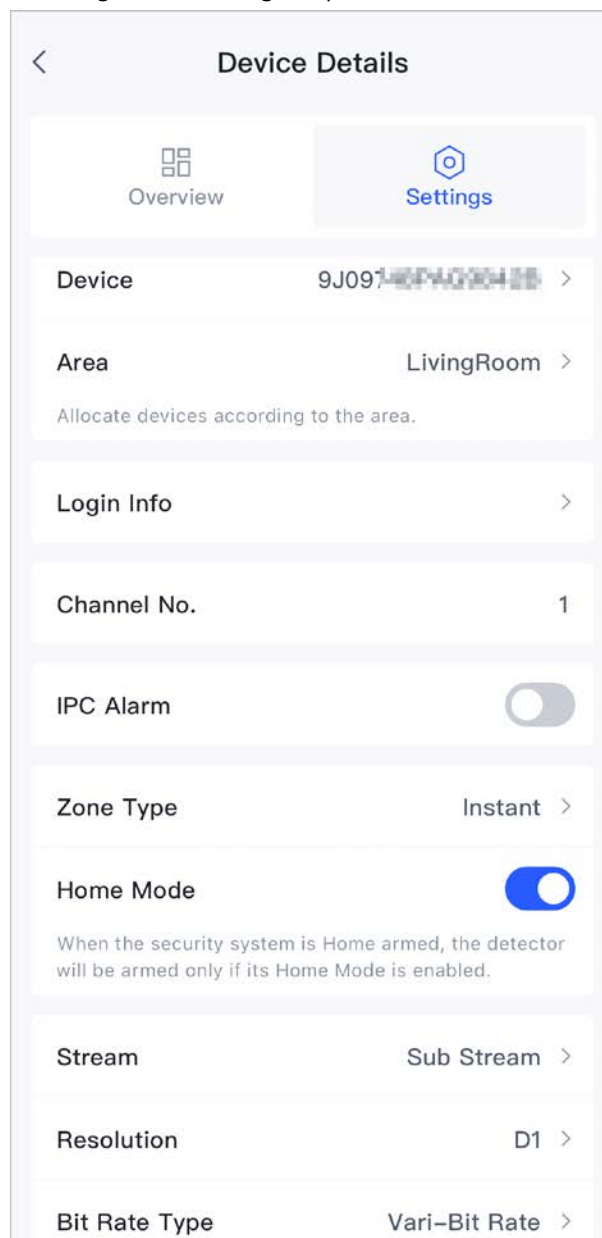
Seleccione **Detalles del dispositivo** del IPC.

Figura 4-11 Detalles del dispositivo



2. Seleccionar **Ajustes** para configurar los parámetros del IPC.

Figura 4-12 Configurar parámetros

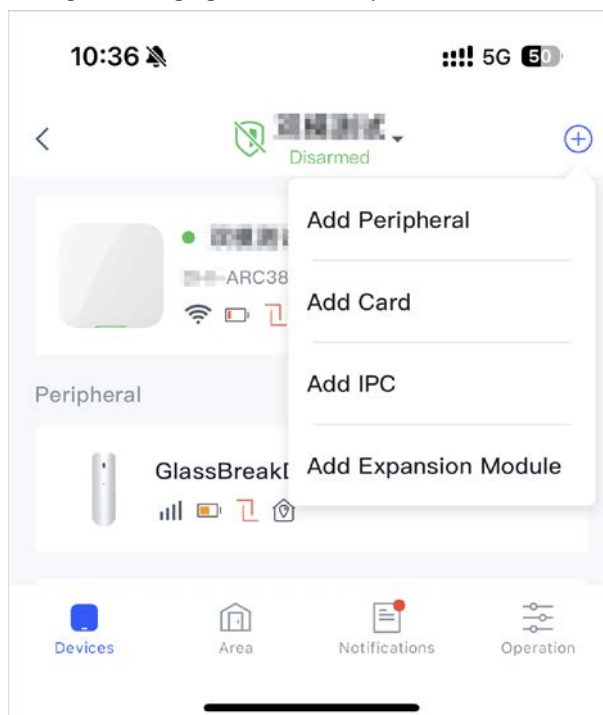


4.2.4 Agregar módulo de expansión

Procedimiento

Paso 1 Ir a la **Dispositivos** pantalla del concentrador y luego seleccione  > **Agregar módulo de expansión.**

Figura 4-13 Agregar módulo de expansión



Paso 2 Grifo **Comenzar** para agregar el módulo de expansión.

Asegúrese de haber conectado el bus RS-485 del módulo de expansión al concentrador, configure una dirección única usando su interruptor DIP y luego enciéndalo.

4.3 Configuración de la vinculación de alarmas de vídeo

Configure la vinculación de alarma para periféricos para que pueda ver videoclips cuando se active la alarma.

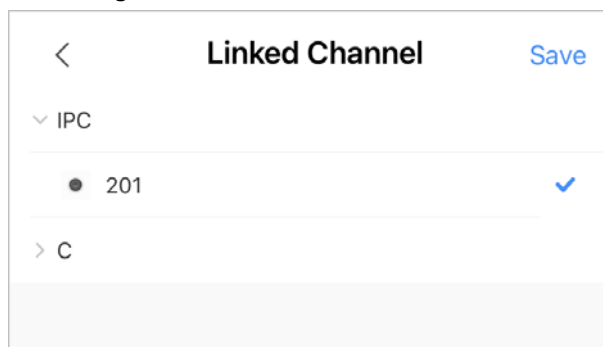
Prerrequisitos

- Asegúrese de que el concentrador esté armado antes de configurar la vinculación de alarma y video.
- Asegúrese de haber agregado periféricos al concentrador.

Procedimiento

- Paso 1** En el **Dispositivo** En la pantalla del concentrador, seleccione un periférico y luego vaya a **Detalles del dispositivo** > **Ajustes** para configurar los parámetros.
- Paso 2** Permitir **Vinculación de alarma y vídeo**, y luego seleccione **Canal de vídeo**.
- Paso 3** Seleccione un canal de vídeo de la **Canal vinculado** lista y toque **Ahorrar**.

Figura 4-14 Canal vinculado



4.4 Configuración general del concentrador

Puede ver y editar información básica del dispositivo.

Procedimiento

Paso 1 En la pantalla del centro, toque **Ajustes** para ver los detalles del dispositivo.

Tabla 4-1 Descripción de parámetros

Parámetro	Descripción
Dispositivo	● Ver nombre, tipo, SN y modelo del dispositivo del concentrador. ● Edite el nombre del dispositivo y luego toque Ahorrar para guardar la configuración.
Configuración del concentrador	Configurar parámetros del concentrador.
Red	Grifo Red para ver su información de red actual.
Huso horario	Grifo Huso horario para seleccionar su zona horaria y habilitar el horario de verano (DST) si es necesario. ● Huso horario: Seleccione la zona horaria en la que opera el hub. ● Horario de verano: Seleccione la fecha o semana y luego seleccione la hora de inicio y la hora de finalización.
Idioma	Seleccione el idioma de enlace para los mensajes de voz. Disponible en 18 idiomas: árabe, checo, danés, neerlandés, inglés, francés, alemán, italiano, portugués (Europa), ruso, español (Latinoamérica), español (Europa), turco, eslovaco, polaco, griego, búlgaro y estonio. El inglés está configurado por defecto.
Manual del usuario	Grifo Manual del usuario para obtener el manual del usuario del concentrador de alarma.
Actualización de firmware	Actualización en línea.  No se permite la actualización cuando el concentrador está en estado armado o el nivel de batería es bajo.

Parámetro	Descripción
Ver registros	Ver registros del dispositivo y de la aplicación. - Registro del dispositivo: Seleccionar Ver registros > Registro del dispositivo para ver los registros de alarmas de el dispositivo. También puedes tocar el Registro del dispositivo Pantalla para enviar registros de alarmas al correo electrónico vinculado. - Registro de aplicaciones: Seleccionar Ver registros > Registro de la aplicación para ver los registros de alarmas. También puede tocar el Registro de la aplicación Pantalla para enviar registros de alarmas al correo electrónico vinculado.
Recopilar registros	Recopilar registros del dispositivo y la aplicación.

4.4.1 Visualización del estado del concentrador

Descripción del icono del concentrador

Se explica el significado de los iconos del detector de puerta. Puede verlos en la pantalla central.

Tabla 4-2 Descripción del icono del dispositivo

Parámetro	Icono	Descripción
Intensidad de la señal LTE		Ultra débil
		Débil
		Bien
		Excelente
		Sin señal
Intensidad de la señal Wi-Fi		Ultra débil
		Débil
		Bien
		Excelente
		Sin señal
Tarjeta SIM		La tarjeta SIM 1 está activa.
		La tarjeta SIM 2 está activa.
		Sin tarjeta SIM.
		La tarjeta SIM está desbloqueada.
		La tarjeta SIM está bloqueada.
Nivel de batería		100%
		80%
		60%

Parámetro	Icono	Descripción
		40%
		20%

Descripción del estado del concentrador de alarmas

En el **Dispositivos** En la pantalla del concentrador, seleccione un concentrador y luego seleccione **Descripción general** **Estado** para ver la información y el estado del concentrador.

Tabla 4-3 Descripción general

Parámetro	Descripción
Información básica	Muestra la información básica del concentrador.
Estado en línea	Muestra el estado en línea del concentrador.
Tipo	Muestra el tipo de dispositivo.
SN	Muestra el número de serie del concentrador.
Modelo	Muestra el modelo del dispositivo del concentrador.

Tabla 4-4 Estado

Parámetro	Descripción
Intensidad de la señal LTE	La intensidad de la señal de la red móvil para la tarjeta SIM activa.
Intensidad de la señal Wi-Fi	Estado de la conexión a internet del concentrador vía Wi-Fi. Para mayor fiabilidad, recomendamos instalar el concentrador en lugares con una intensidad de señal de al menos 2 barras.
Nivel de batería	Muestra la electricidad restante de la batería en forma de porcentaje.
Manosear	Muestra el estado antimanipulación del concentrador. Los tipos incluyen: ● Abierto ● Desconectado
Alimentación externa	Muestra el estado de la conexión de alimentación externa. Los tipos incluyen: ● Conectado ● Desconectado
GSM	Muestra el estado GSM del concentrador. Los tipos incluyen: ● Conectado ● Desconectado
Wifi	Muestra el estado de Wi-Fi del concentrador. Los tipos incluyen: ● Conectado ● Desconectado
Ethernet	Muestra el estado de Ethernet del concentrador. Los tipos incluyen: ● Conectado ● Desconectado

Parámetro	Descripción
Tarjeta SIM	Muestra el estado de conexión de la tarjeta SIM. Los tipos incluyen: ● Tarjeta SIM 1 ● Tarjeta SIM 2 ● Ninguno ● Bloqueado (esta barra de estado solo es compatible cuando hay una tarjeta SIM insertada en el concentrador).
Arc1Primary	Muestra el estado de conexión de los centros de recepción de alarmas 1 y 2. Los tipos incluyen: ● Conectado ● Desconectado.
Arc1Secundario	
Arc2Primary	
Arc2Secunary	
Versión de firmware	La versión del programa del concentrador.

4.4.2 Configuración de los parámetros del concentrador

Procedimiento

Paso 1 En el **Dispositivos** Pantalla del hub, seleccione el hub.

Paso 2 Seleccionar **Ajustes > Configuración del concentrador** para ver y editar información general del centro.

Tabla 4-5 Descripción de los parámetros del concentrador

Parámetro	Descripción
Respaldo Configuración	Si este concentrador está dañado, puedes transferir sus parámetros y configuraciones periféricas a otro concentrador. Después de habilitarlo, se realizará una copia de seguridad periódica de la configuración del concentrador.

Parámetro	Descripción
Administrador de usuarios	Puede agregar, modificar o eliminar usuarios de la aplicación o del teclado cuando esté desarmado. ● Usuario del teclado: Grifo Agregar Para agregar un usuario del teclado, ingrese el nombre de usuario, el código de operación (de 4 a 6 dígitos) y la contraseña de emergencia (opcional). Luego, seleccione los permisos de armado y desarmado de la habitación.  ◇ Se permiten hasta 64 usuarios del teclado (32 usuarios agregados manualmente y 32 usuarios creados automáticamente). El primer usuario creado manualmente es el Usuario administrador por defecto. Tiene todos los permisos disponibles. ◇ DMSS crea automáticamente un usuario de teclado cada vez que se activa un dispositivo. Se agregó por primera vez. El número de secuencia de usuarios del teclado creado por el sistema comienza automáticamente desde 33 y tiene un ícono junto a...  a su cuenta. ◇ Se creará automáticamente un usuario de teclado para los usuarios compartidos. ● Usuario de la aplicación: Seleccione el usuario para modificar sus permisos, incluidos SOS, control de interruptor, derivación, notificación, código de teclado, instantánea y video de alarma.  Seleccionar Compartir dispositivos, ingrese la cuenta DMSS con la que se compartirá el dispositivo y seleccione los permisos para la cuenta.
Alarma SOS	Configure los tipos de alarma SOS, incluida la alarma de pánico, el enlace a la sirena, la alarma médica, la alarma médica y la alarma de incendio. Después de la configuración, toque LLAMADA DE SOCORRO en el Operación Pantalla del concentrador para activar la alarma. Al seleccionar varios tipos de alarma, una ventana emergente le recuerda que debe seleccionar una alarma para activarla en ese momento.
Instalador	Confíe en los proveedores de servicios. Toque Confianto, ingrese la cuenta del proveedor de servicios, el período de confianza y seleccione los dispositivos a confiar, seleccione He leído y acepto el Acuerdo de usuario, y luego toque Próximo.
Global Armado/Desarmado eng	Arme o desarme todos los detectores en todas las áreas con un toque.
Programado Armado/Desarmado eng	Armar o desarmar las áreas por horario. ● Área: Seleccione el área en la que opera el hub. ● Configuración de comandos: Seleccione un modo armado según sea necesario tocando Hogar, Lejos, o Desarmar. ● Punto de tiempo: Seleccione el período de tiempo en el que opera el hub. ● Repetir: Seleccione el(los) día(s) de la semana como período de repetición. ● Armado forzado: Puede armar el sistema cuando ocurren errores en las zonas.

Parámetro	Descripción
Configuración de sonido	● Volumen: Seleccione el volumen de la alarma. ● Sonido de alarma/manipulación: Habilite la función para que haya sonido cuando ocurra la alarma o el evento de manipulación. ● Duración del sonido de la alarma: Configure la duración del sonido. ● Reproducir sonido para el tiempo de retardo y el armado/desarmado: Habilite la función para que el tono de llamada se aplique en estos escenarios. ● Área: Seleccione el área donde se aplicarán los ajustes de sonido. Puede seleccionar Todas las áreas Luego, puedes acceder a los permisos de todas las áreas del centro. O puedes seleccionar solo las áreas que desees.
Indicador LED	Indicador LED Está habilitado de forma predeterminada.  Si Indicador LED está deshabilitado, el indicador LED permanecerá apagado independientemente de si el concentrador está funcionando normalmente o no.
Intercomunicador Servicio	Permitir Servicio de intercomunicación para lograr la función. ● Límite de tiempo de intercomunicación: Cuando se activa una alarma, se pueden iniciar los servicios de intercomunicación dentro del intervalo de tiempo configurado. Una vez transcurrido el tiempo, no se puede iniciar una nueva sesión de intercomunicación.  La duración de cada sesión de intercomunicación no puede ser superior a 20 minutos. ● Intercomunicador: ◇ Intercomunicador de la aplicación: Intercomunicador entre la sirena y la aplicación DMSS. Seleccione la sirena asignada a diferentes áreas o seleccione No vincular. ◇ Intercomunicador SIP: Intercomunicador entre la sirena y la plataforma de terceros. ○ Seleccione la sirena para el intercomunicador. Se admite la selección filtrada por sirena y área. ○ Configuración del servidor SIP: Nombre de usuario/Contraseña: Sujeto a configuración en terceros plataforma. Dirección del servidor SIP: Ingrese la dirección IP de la plataforma de terceros. Puerto del servidor SIP/Puerto local: Sea coherente con el número de puerto de la plataforma de terceros. plataforma del partido Estado de registro: muestra el estado si el SIP está configurado o no.

Parámetro	Descripción
Número de teléfono Gestión	● Sonido personalizado: Configure el sonido personalizado y se reproducirá un sonido adicional durante la llamada si se activa una alarma. ● VoLTE: Habilite la función, el concentrador puede realizar llamadas y enviar SMS utilizando el servicio IMS, mientras que desactive la función, el concentrador solo puede enviar SMS y realizar llamadas a través de redes GSM. ● Número de teléfono: Grifo Agregar En la esquina superior derecha de la página, añada un número de teléfono para recibir el evento y, a continuación, seleccione el tipo de evento que requiere el envío de SMS. Los tipos de evento incluyen alarma, fallo, funcionamiento y si la alarma está vinculada al teléfono. Después de agregarlo, puedes deslizar hacia la izquierda para probar las llamadas y los SMS y verificar si el número actual es válido. También puedes deslizar hacia la izquierda para eliminar el número de teléfono móvil. Toque el número de teléfono para ingresar a la página de edición del número de teléfono y luego podrá editar el número y seleccionar el tipo de evento que necesita enviar SMS.  Sólo los dispositivos 2G/4G admiten esta función.
Modo de prueba	Grifo Comenzar para probar el estado de los periféricos que se conectan al concentrador en diferentes áreas y luego toque Detener para completar la detección.
Reducido Sensibilidad Modo	Permitir Modo de sensibilidad reducida y luego se reducirá la potencia de transmisión del concentrador.
Importar Configuración	Puede transferir la configuración de un concentrador a otro del mismo modelo. Tras la importación, las relaciones de encomienda, préstamo o servicios de seguridad existentes no se conservarán. Proceda con precaución.  Debes habilitar Configuración de respaldo antes de importar la configuración.
Servicio en la nube Conexión	Establezca el intervalo de ping entre el servidor y el concentrador entre 150 y 900 segundos (150 segundos por defecto). Si D-cloud detecta que el tiempo de desconexión del concentrador supera los 150 segundos, informará al usuario sobre su estado a través de la aplicación.

Parámetro	Descripción
Latido del corazón	Configure el intervalo de ping del detector del concentrador. Esta configuración determina la frecuencia con la que el concentrador se comunica con los periféricos y la rapidez con la que se detecta la pérdida de conexión. ● Intervalo de ping del detector (s): La frecuencia de los periféricos conectados operados por el concentrador se configura en el rango de 12 segundos a 300 segundos (60 segundos por defecto).  Cuanto más corto sea el intervalo de ping del detector, más corta será la vida útil de la batería. ● Número de paquetes descartados: Se configura un contador de paquetes no entregados en el rango de 3 a 60 (15 paquetes por defecto).  ◇ Cuanto menor sea el número, más frecuentemente se mostrará el estado fuera de línea. Se detectan y se informan los periféricos. ◇ Si el concentrador pierde constantemente la conexión con los periféricos y no puede detectar sus latidos definidos, informará su estado fuera de línea al sistema.
Enlace Sirena para Manosear	● Sirena de enlace para manipulación: En el estado de armado, cuando el Sirena de enlace para manipulación está habilitado, el concentrador vinculará el sonido de la alarma.  La sirena avisará cuando las tapas del concentrador y los periféricos estén abiertas. ● Siempre activo: Configure si desea vincular el sonido de la alarma durante el desarmado. Está deshabilitado por defecto. Después de habilitarlo Siempre activo, cuando el Sirena de enlace para manipulación está habilitado, el concentrador vinculará el sonido de la alarma tanto en el estado de armado como de desarmado.  ◇ El enmascaramiento de las detecciones se gestiona como condiciones de falla, no es WD activo permitido en condiciones no establecidas. ◇ Esto no cumple con las certificaciones EN50131-1.
Sistema Comprobación de integridad	Al habilitar esta función, el concentrador verifica si el sistema actual presenta anomalías durante el armado. Si las presenta, se impedirá el armado. Los elementos verificados incluyen brazo con fallas, falla de energía principal, retraso de falla de energía principal, manipulación del concentrador de alarma, conexión a la plataforma en la nube, error de red cableada, error de Wi-Fi, error de red celular, interferencia de RF y conexión ARC.  ● En el caso del llavero, el indicador parpadea en verde y luego se vuelve rojo. ● Para la aplicación, aparece un mensaje de alarma. ● Para el teclado, emite un pitido de 1 segundo, el indicador de armado y desarmado parpadea en verde durante 2 segundos y luego vuelve al estado normal.

Parámetro	Descripción
DSS	Ingresa la IP/dominio, el puerto y el ID del dispositivo y luego podrá registrar el concentrador en DSS Pro o Converter.

Parámetro	Descripción
Alarma Recepción Centro	SeleccionarCentro receptor de alarmas 1oCentro receptor de alarmas 2Vaya a la pantalla de configuración correspondiente. Active la función y configure los parámetros. ● Protocolo de comunicación:Seleccionar deSIA-DC-09(SIA-DCS),SIA-DC-09(ADM-CID),SIA-DC-09(ADM-CID México),Protector suaveyPrivado. ● Dirección IP preferida/Nombre de dominio/Puerto:Ingrese la dirección IP/dominio y el número de puerto del ARC. ● Dirección IP alternativa/nombre de dominio/puerto:Ingrese la dirección IP/dominio alternativa y el número de puerto del ARC.  ◇ Los mensajes se enviarán a la dirección IP/dominio alternativo solo cuando La dirección IP preferida no puede recibir el mensaje. ◇ SiIntervalo de latidos del corazónestá habilitado, el sistema juzgará si enviar el mensaje a la dirección IP preferida o alternativa. ● Protocolo IP: SeleccionarTCPpor defecto. ● Conexión corta: Habilitado por defecto. El concentrador cambiará a la comunicación de enlace corto TCP con la central receptora de alarmas. La conexión entre ambos se establece solo al enviar eventos (incluidos eventos de latido y de prueba). La conexión se cierra tras una transmisión exitosa o si falla (tiempo de espera agotado o falta de respuesta). ● Intervalo de latidos del corazón:Establezca el intervalo de latidos con un rango de 0 segundos a 24 horas (60 segundos por defecto).  0 segundos significaIntervalo de latidos del corazónestá deshabilitado. ● Cuenta Central:Ingrese el número de cuenta creado por el ARC, que se utilizará para identificar el concentrador cuando éste envíe información al ARC. ● Cifrado:El concentrador utiliza un formato de cifrado para la seguridad de la información cuando configura el ARC.AES128Está configurado de forma predeterminada. ● Periodo de recarga:Seleccione el período de recarga de la lista. ● Subir eventos:Toca  a un evento para cargarlo. ◇ Alarma:Mensaje de alarma. ◇ Restaurar informe de alarma:Seleccionar deInmediatamenteyAl desarmar. ◇ Error:Fallo de energía, bajo voltaje de la batería, manipulación y fuera de línea. ◇ Operación:Operación realizada en el sistema. ◇ Armado/Desarmado:Notificaciones de mensajes de armado y desarmado del sistema. ◇ Campo extendido: Habilitado por defecto. Si está desactivado, los mensajes de eventos reportados mediante el protocolo SIA solo incluyen URLs de imágenes y videos, y excluyen todos los campos extendidos (por ejemplo, los campos I y R).

Parámetro	Descripción
	● Verificación de vídeo:Envía imágenes y vídeos de alarma al centro de recepción de alarmas. ● Prioridad de eventos de alarmaTras su activación, el dispositivo informa inmediatamente de los mensajes de alarma cuando se activa. Una vez preparadas las imágenes y los vídeos de la alarma, enviará otro informe con una URL donde se almacenen las imágenes y los vídeos.  Sólo cuando Verificación de vídeo está habilitado, Prioridad de eventos de alarma se muestra en la pantalla. ● Prueba de comunicación:Soportes Prueba manual y Prueba programada. ◇ Prueba manualPruebe manualmente si los parámetros de las centrales de alarma preferidas y alternativas son normales. Si la prueba es exitosa, la central puede recibir el evento de prueba. ◇ Prueba programadaLa prueba programada está deshabilitada por error. Tras habilitarla, el concentrador informa periódicamente sobre eventos de prueba. Puede configurar el periodo de informe automático. El periodo predeterminado es de 24 horas. SP2:LAN/WiFi usando la NUBE, APP DMSS (tiempo de informe predeterminado 150") o tiempo de informe ARC mín. 25 h); DP2: Primaria LAN/WiFi usando la NUBE, Aplicación DMSS(tiempo de informe predeterminado 150") o tiempo de informe ARC mínimo 30 min) y secundario GPRS/4G usando la NUBE Aplicación DMSS(tiempo de informe predeterminado 150") o ARC tiempo de reporte min. 30 min).

4.5 Configuración de red

En el **Configuración general** del **Detalles del dispositivo** pantalla, toque **Configuración de red** y luego puede seleccionar la red para el concentrador: red cableada, red inalámbrica o red celular.

4.5.1 Configuración de red cableada

Procedimiento

- Paso 1** Seleccionar **Configuración de red** > **Configuración de red cableada**.
- Paso 2** Configurar los parámetros de conexión de red cableada.

Tabla 4-6 Descripción de los parámetros de la red cableada

Parámetro	Descripción
DHCP	Cuando hay un servidor DHCP en la red, puede habilitarlo DHCP luego el concentrador obtiene automáticamente una dirección IP dinámica.
Dirección IP	Configurar la dirección IP manualmente: configure manualmente la dirección IP, la máscara de subred, la puerta de enlace predeterminada, el DNS y la dirección MAC para el concentrador.
Máscara de subred	

Parámetro	Descripción
Puerta	
DNS	
DNS 2	
Dirección MAC	

4.5.2 Configuración de la red Wi-Fi

Procedimiento

- Paso 1** Seleccionar **Configuración de red > Configuración de red Wi-Fi**.
- Paso 2** Seleccione una red Wi-Fi disponible en el área y luego ingrese la contraseña de la red para conectarse a la red.

4.5.3 Configuración celular

Procedimiento

- Paso 1** Seleccionar **Configuración de red > Celular**.
- Paso 2** Configurar parámetros celulares.

Tabla 4-7 Descripción de los parámetros celulares

Parámetro	Descripción
Celular	Grifo  Al lado de la Celular para habilitar el celular.
Prioridad	Grifo  Al lado de la Prioridad Para establecer el celular como prioridad Al seleccionar la red.
Tarjeta SIM 1	● Admite dos tarjetas SIM y modo de espera único. ● Las tarjetas SIM permiten que el concentrador utilice datos celulares y envíe notificaciones de alarma.
Tarjeta SIM 2	
APN	El nombre del punto de acceso (APN) es el nombre de la configuración que lee su dispositivo para configurar una conexión para la puerta de enlace entre la red celular de su operador e Internet público.
Modo de autorización	Modo de autenticación de la red celular.
Nombre de usuario	El nombre de usuario y la contraseña de la red celular.
Contraseña	
Número de marcación	El número al que debe llamar el concentrador.
Datos de roaming	Habilite la función cuando viaje fuera de la región de cobertura para acceder a la conexión a Internet.
Uso de datos móviles	Ver el uso de los datos móviles.
Restablecer estadísticas	Restablezca el uso de datos móviles para reiniciar el conteo.

Parámetro	Descripción
ALFILER	Admite ingresar el PIN de SIM 1 y SIM 2 respectivamente para proteger la privacidad cuando sea necesario.  Está prohibido introducir el código PIN cuando la tarjeta SIM esté desbloqueada. Bloquéela cuando desee introducir el PIN.

4.6 Administración de dispositivos

4.6.1 Confianza de dispositivos

Los usuarios administradores de DMSS pueden agregar instaladores confiándoles dispositivos. Pueden confiarles dispositivos uno por uno o por lotes.

4.6.1.1 Confianza de dispositivos en lotes

Puede confiar dispositivos al proveedor de servicios en lotes.

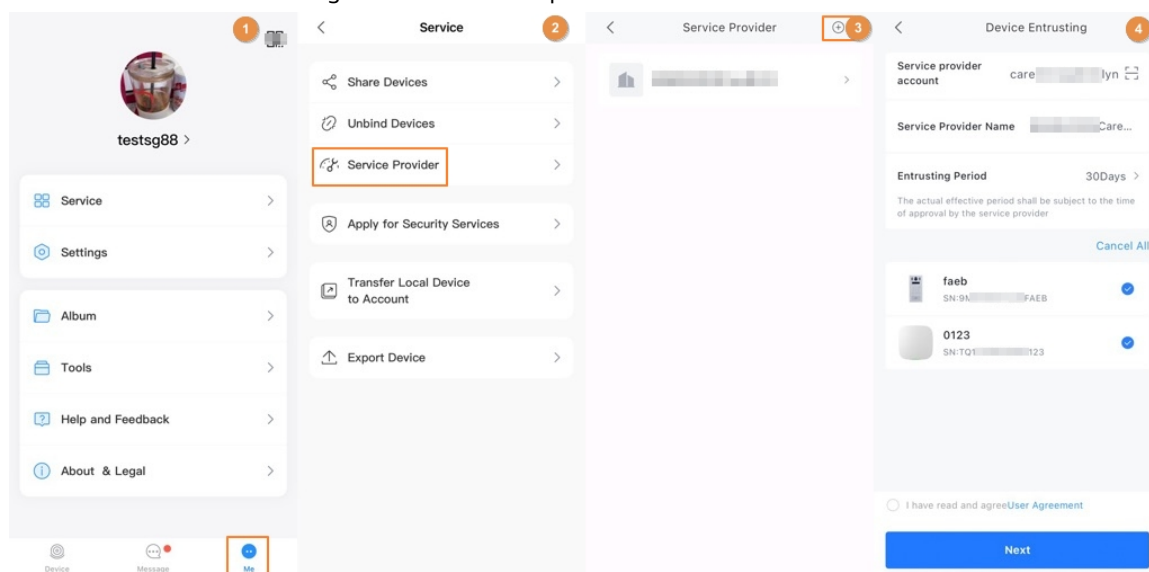
Prerrequisitos

Usted se ha vinculado con un proveedor de servicios.

Procedimiento

- Paso 1** En el **Dispositivo** pantalla, seleccionar **A mí** > **Servicio** > **Proveedor de servicios**, y luego toque .
- Paso 2** En el **Confianza de dispositivos** Pantalla, confirme la información del proveedor de servicios vinculado, o también puede tocar para  escanear el código QR del proveedor de servicios.
- Paso 3** Seleccione los dispositivos que desea confiar y confíelos a DoLynk Care. El proceso para confiar varios dispositivos es el mismo que para confiar uno solo.

Figura 4-15 Confiar dispositivos en lotes



4.6.1.2 Confianza de dispositivos uno por uno

Puede confiar un dispositivo a usuarios de DoLynk Care. Puede configurar los permisos de confianza.

Prerrequisitos

Usted se ha vinculado con un proveedor de servicios.

Procedimiento

- Paso 1** En el **Dispositivo** pantalla, toque  junto a un dispositivo y luego toque **Confianza de dispositivos**.
- Paso 2** En el **Confiar** Pantalla, confirme la información del proveedor de servicios vinculado, o también puede tocar para  escanear el código QR correspondiente del instalador.
- Paso 3** Seleccione los períodos de confianza y los permisos y luego toque **DE ACUERDO**.

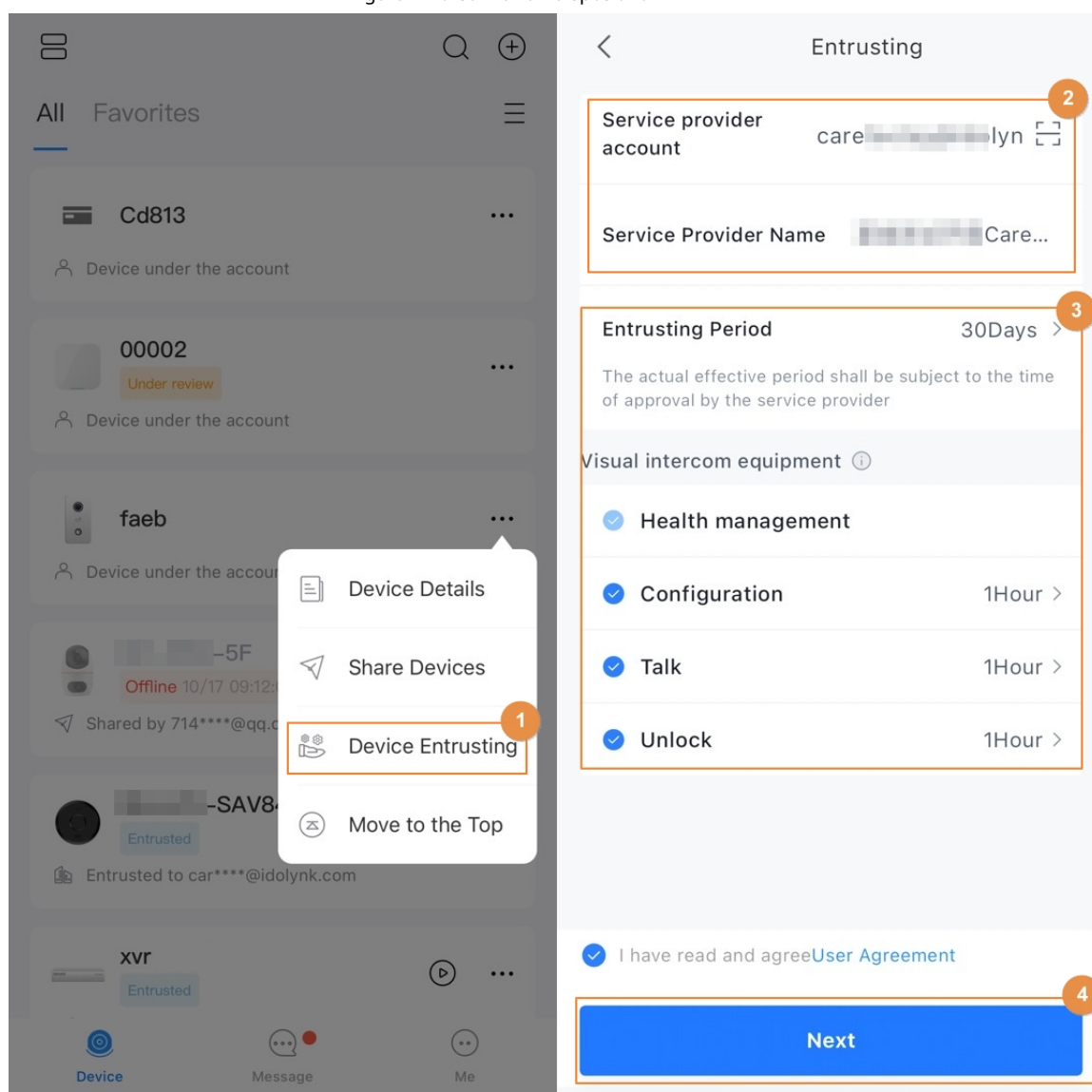
Tabla 4-8 Instrucción de permisos

Permiso	Descripción	Nota
Salud Gestión	Seleccione de forma predeterminada, lo que no se puede cancelar, incluidos los permisos para verificación de estado con un solo clic, informe de errores, corrección de errores, estadísticas de datos e informe de estado.	—
Dispositivos de vídeo	Puede solicitar permisos de configuración del dispositivo, video en vivo y reproducción. ● Permiso de configuración: incluye reiniciar y actualizar el dispositivo, formatear la tarjeta SD y complemento de configuración. ● Vídeo en vivo y reproducción: vea el vídeo en vivo, reproduzca las grabaciones y el permiso de vídeo del complemento.	Tu puedes elegir temporario permisos, tales como 1 hora o 4 horas, u optar por autorización Durante todo el período de encomienda. Por ejemplo, si el período de encomienda es 30 días, tendrás la permisos para el 30 días completos duración.
Dispositivos de alarma	Puede solicitar permisos de configuración y funcionamiento del dispositivo. ● Permiso de configuración: incluye agregar, eliminar y configurar los periféricos, agregar, eliminar y configurar las salas, editar la información del dispositivo, configurar la red y la zona horaria del dispositivo, actualizar el dispositivo, agregar y eliminar usuarios, cambiar la contraseña del dispositivo y vincularlo con la cuenta del convertidor. ● Permiso de operación: Incluye armado o desarmado (incluido SOS), prueba del concentrador de alarma y periféricos, y control de salida de alarma (enchufe, interruptor y relé).	

Permiso	Descripción	Nota
Video Interconexión Dispositivos	Puede solicitar permisos de configuración y funcionamiento del dispositivo. ● Permisos de configuración: Incluye transmisión de red, configuración SIP y mantenimiento del dispositivo. ● Permisos de operación: Incluyendo hablar y abrir puertas.	

Paso 4 Leer y seleccionar **He leído y acepto el Acuerdo de usuario**, y luego toque **Próximo**.

Figura 4-16 Confiar un dispositivo



Resultado

Puede ver el estado de la encomienda en la pantalla de la lista de dispositivos. Una vez encomendada correctamente, el estado del dispositivo cambia de **En revisión** a **Encomendando a ******.



Después de enviar con éxito una solicitud de confianza, aparecerá un mensaje en la **Hogar** pantalla.

Debe esperar una respuesta del instalador, que se mostrará en la **Mensaje**>

Buzón>Información personal.

Operaciones relacionadas

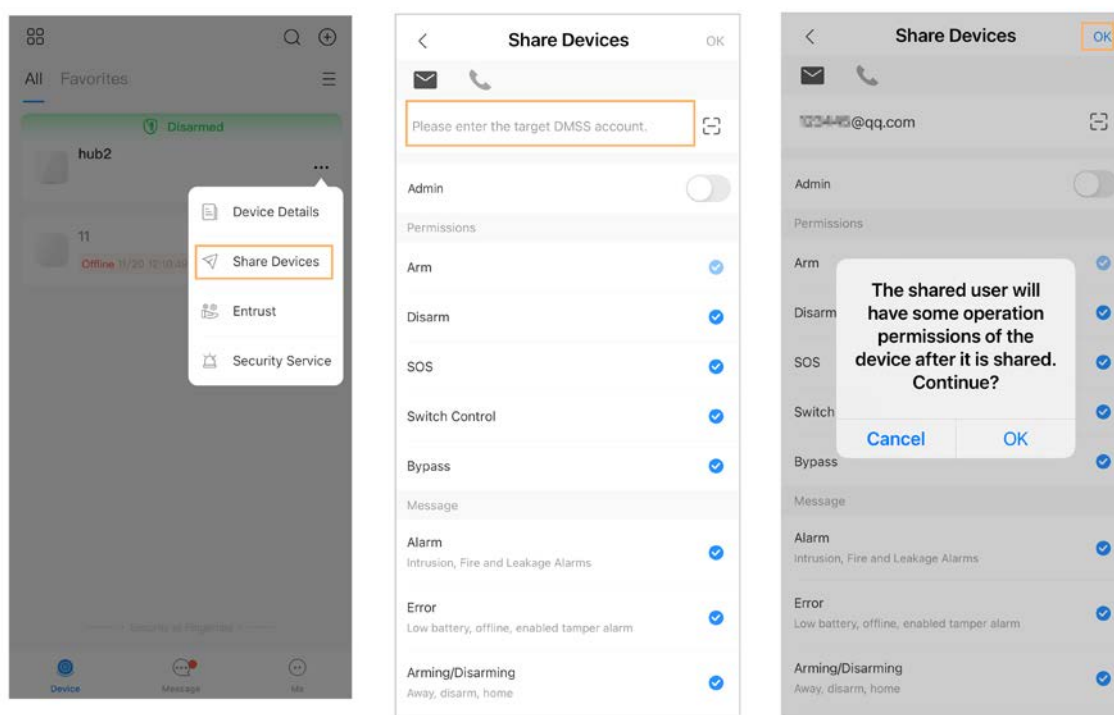
- Para cambiar los permisos, vaya a la **Confiar a la empresa** pantalla y luego toque **Cambiar permisos**.
- Para retirar los permisos de confianza, vaya a la **Confiar a la empresa** pantalla y luego toque **Retirar**.
- Para renovar los períodos de encomienda, acceda a la **Confiar a la empresa** pantalla y luego toque **Renovar**.

4.6.2 Compartir dispositivos

Procedimiento

Paso 1 En el **Dispositivo** pantalla, toque  junto a un dispositivo y luego toque **Compartir dispositivos**.

Figura 4-17 Dispositivo compartido



Paso 2 En el **Compartir dispositivos** pantalla, comparta el dispositivo con el usuario ingresando a su cuenta DMSS o escaneando su código QR.

Paso 3 Seleccione los permisos del dispositivo para los usuarios según sus necesidades reales. Toque **DE**

Paso 4 **ACUERDO.**

La cuenta con la que compartiste el dispositivo aparecerá en la **Usuario compartido** sección de la **Compartir dispositivos** pantalla.

4.6.3 Desvinculación de dispositivos

Al agregar el dispositivo, si ya estaba vinculado a otra cuenta, puede desvincularlo primero. Luego, podrá agregarlo correctamente.

Procedimiento

Paso 1 Seleccionar **A mí>Servicio>Desvincular dispositivos**.

Paso 2 Escanee el código QR o introduzca manualmente el número de serie del dispositivo. Existen dos métodos:

- Solicitud de desvinculación:
 1. El sistema muestra el código de autorización. Siga las instrucciones en pantalla para cargar las imágenes necesarias.
 2. El sistema verifica la información enviada. Una vez que el sistema la haya verificado correctamente, se podrá desvincular el dispositivo.
- Desvincular con contraseña del dispositivo: si tiene la contraseña del dispositivo, puede ingresarla para desvincularlo.



El dispositivo debe estar en línea. Si olvidó la contraseña o la contraseña es incorrecta, Puede solicitar desvincular el dispositivo.

4.7 Gestión de áreas

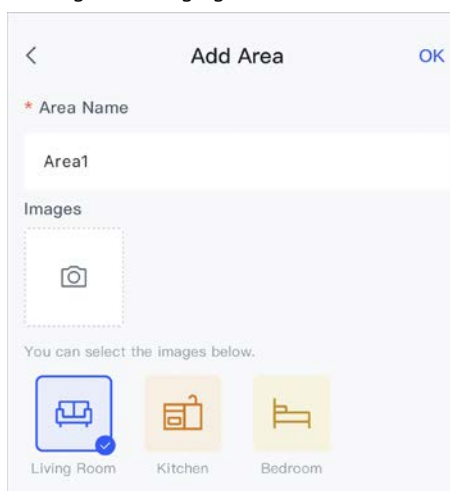
4.7.1 Agregar área

Procedimiento

Paso 1 En el **Área** Pantalla del concentrador, toque **+** En la esquina superior derecha, para agregar

Paso 2 áreas. Configure el área, seleccione la imagen y luego toque **DE ACUERDO**.

Figura 4-18 Agregar área



4.7.2 Establecer el área como área pública

Establezca el área como área pública y luego podrá vincularse a otras áreas.

Información de fondo

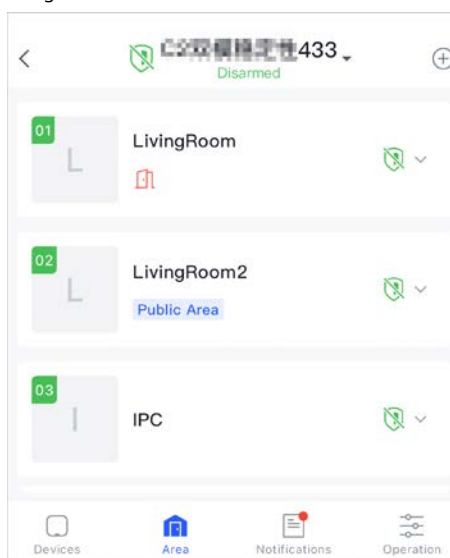
Un área pública debe tener conexión con al menos otras 2 áreas.

- Si todas las áreas vinculadas están armadas, el área pública se armará automáticamente.
- Si alguna de las áreas vinculadas está desarmada, el área pública se desarmará automáticamente.

Procedimiento

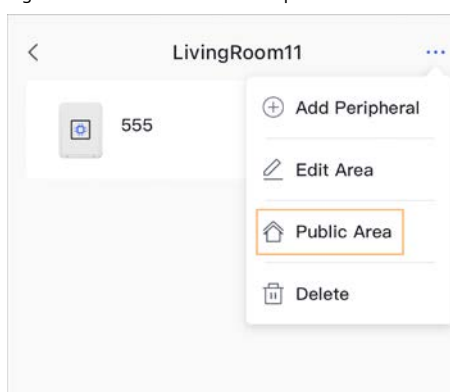
Paso 1 En el **Área** Pantalla del hub, seleccione un área para ir a su pantalla de detalles.

Figura 4-19 Seleccionar un área



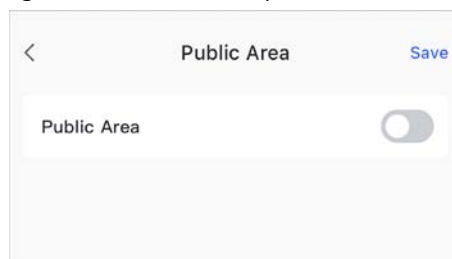
Paso 2 Grifo...en la esquina superior derecha y luego toque **Área pública**.

Figura 4-20 Establecer como área pública



Paso 3 Permitir **Área pública**, y luego toque **Ahorrar**.

Figura 4-21 Habilitar área pública

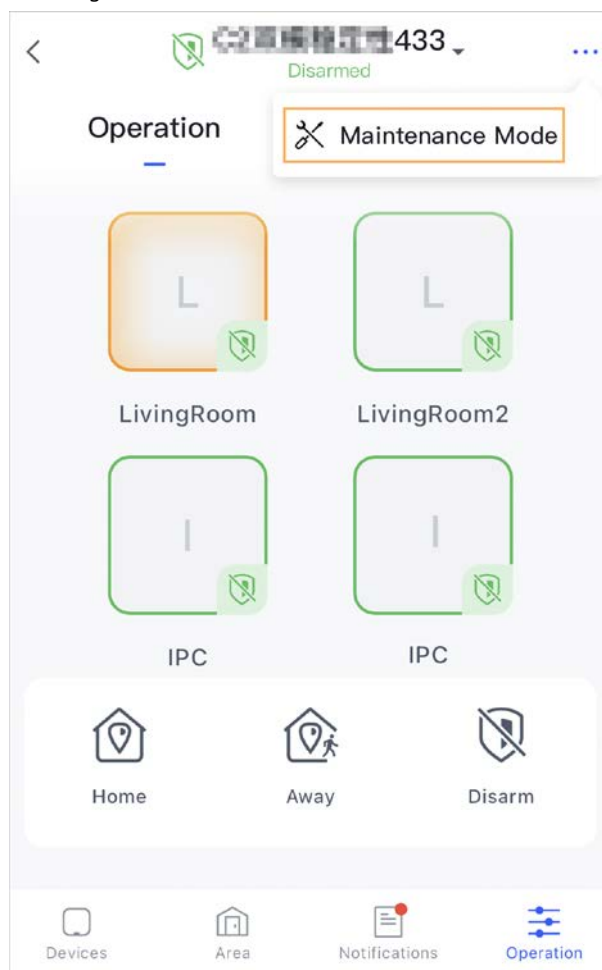


4.7.3 Configuración del modo de mantenimiento

El modo de mantenimiento está diseñado para el mantenimiento y las actualizaciones de los dispositivos. En este modo, el sistema suspende todos los informes de alarmas y fallos a las áreas para evitar notificaciones innecesarias durante las tareas de mantenimiento.

En el **Operación** pantalla, toque... en la esquina superior derecha y luego toque **Modo de mantenimiento**.

Figura 4-22 Modo de mantenimiento



5 Operaciones generales

El usuario de nivel 2 o 3 tiene permiso para armar y desarmar el sistema. Esta sección utiliza como ejemplo la operación del usuario final en DMSS.

Prerrequisitos

- Asegúrese de haber agregado un concentrador antes de realizar configuraciones.
- Asegúrese de que el concentrador tenga una conexión a Internet estable.
- Asegúrese de que el concentrador esté desarmado.

Información de fondo

Puede administrar concentradores y periféricos de alarma y realizar operaciones como armar, desarmar y configurar dispositivos de alarma.

Procedimiento

- Paso 1** En la pantalla central, toque **Periférico** Para agregar los periféricos. Para más detalles sobre cómo agregarlos, consulte el manual del usuario del dispositivo correspondiente.
- Paso 2** Arme y desarme los detectores de una sola área o de todas las áreas mediante operaciones manuales o programadas.
- Armado y desarmado único: arme y desarme los detectores en una sola área.
 - Armado y Desarmado Global: Arme y desarme los detectores en todas las áreas.
 - Armado y desarmado manual: arme el sistema de seguridad a través de la aplicación DMSS, el teclado o el llavero.
 - Programar armado y desarmado: arme y desarme los detectores según programación.

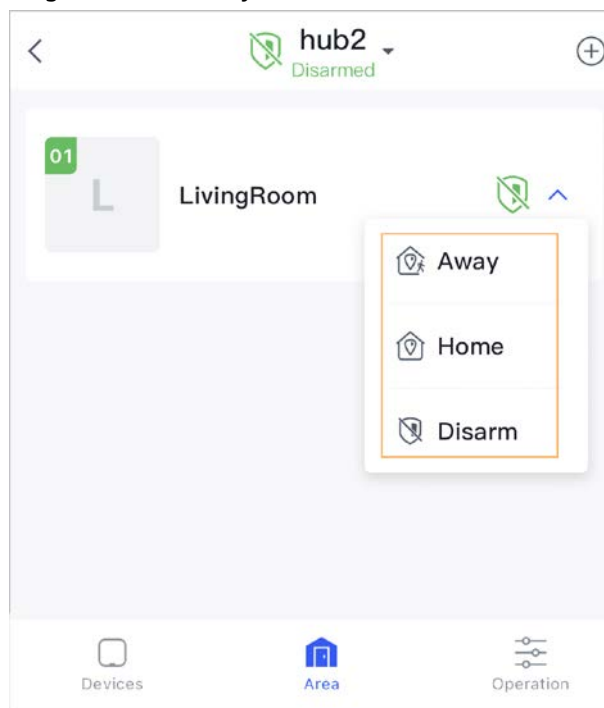
5.1 Armado y desarmado único

Puede armar y desarmar los detectores en una sola área.

Procedimiento

- Paso 1** En la pantalla central, toque **Área**.
- Paso 2** Toque junto a un área y luego seleccione entre **Hogar**, **Lejos**, **Desarmar**.
- **Hogar**: Arme el sistema cuando esté dentro del área del sistema de alarma.
 - **Lejos**: Arme el sistema cuando abandone el área del sistema de alarma.
 - **Desarmar**: Apaga el sistema de seguridad. Lo opuesto a armarlo.

Figura 5-1 Armado y desarmado único



5.2 Armado y desarme global

Puede armar y desarmar los detectores en todas las áreas.

Prerrequisitos

Asegúrese de tener habilitada la **Armado/desarmado global** función.

Procedimiento

- Paso 1 En el **Operación** Pantalla del concentrador, seleccione entre **Hogar**, **Lejos** Para armar globalmente los detectores. Toque **Desarmar**
- Paso 2 Para desarmar globalmente los detectores. Toque **LLAMADA DE SOCORRO** para activar alarmas.
- Paso 3

Figura 5-2 Armado y desarmado global



5.3 Armado y desarmado manual

Puede activar el sistema de seguridad a través de la aplicación DMSS o del llavero.

- Para armar y desarmar los detectores en una sola área o en todas las áreas, consulte "Armado y desarmado individual" y "Armado y desarmado global".
- Para operar con el mando y el teclado, primero debe asignarles los permisos de control de las áreas. Para más información, consulte el manual del usuario del mando y el teclado correspondientes.

5.4 Armado y desarmado programado

Puede configurar un horario para armar y desarmar detectores. Puede configurar planes de armado, incluyendo

Área de armado, modos y periodos.

Procedimiento

Paso 1 En la pantalla del centro, seleccione **Detalles del dispositivo** > **Ajustes** > **Configuración del concentrador**.

Paso 2 Seleccione **Armado/desarmado programado** pantalla, toque **Agregar** luego configurar los planes de armado.

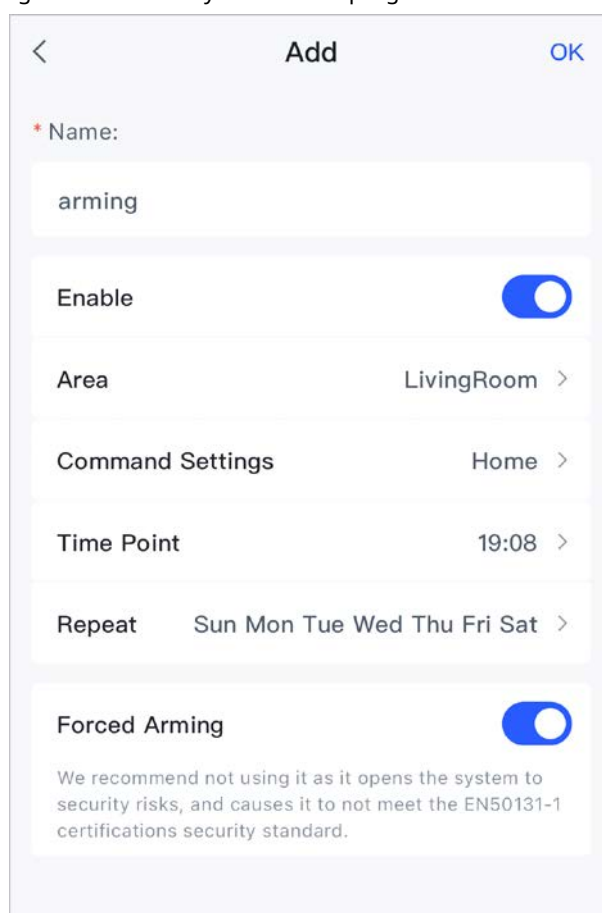
- **Nombre:** Personaliza un nombre para los planes de armado.
- **Área:** Seleccione una o varias áreas que desee armar.
- **Configuración de comandos:** Seleccione de **Hogar**, **Lejos**, y **Desarmar**.
- **Tiempo:** Establecer una hora de armado.



Para aplicar el tiempo de armado a otros días, toque **Repetir** y seleccione los días que desees.

- **Armado forzado:** Seleccione según sea necesario.

Figura 5-3 Armado y desarmado programado



< Add OK

* Name: arming

Enable ☒

Area LivingRoom >

Command Settings Home >

Time Point 19:08 >

Repeat Sun Mon Tue Wed Thu Fri Sat >

Forced Arming ☒

We recommend not using it as it opens the system to security risks, and causes it to not meet the EN50131-1 certifications security standard.

Paso 3 Grifo **DE ACUERDO**.

5.5 Armado y desarmado controlados por SMS

Envíe comandos para armar o desarmar la habitación donde se encuentra el concentrador mediante los números de teléfono registrados en el sistema de gestión telefónica. Los números no registrados no tienen permisos de operación. Formato de comando: [comando]*[número de habitación de 1 a 2 dígitos]

Comandos específicos:

- 01: Brazo

- 11: Brazo forzado
- 02: Desarmar
- 03: Brazo en casa
- 13: Brazo forzado en casa

Número de habitación:

- Formato de dos dígitos (compatible con un solo dígito).
- 0 o 00: Armado global.

Respuesta:

- Éxito: El sistema indica "El armado fue exitoso".
- Error: El sistema indica "Error de armado, el sistema tiene una falla" o "Comando ilegal".



- Para los dos comandos de armado forzado 11 y 13, el comando de armado forzado se envía en el Inicio. Si el armado es exitoso sin fallas, se enviará un mensaje de armado exitoso. Si el armado es exitoso con una falla, se enviará el mensaje de armado con una falla.
- Para la autenticación de coincidencia de números de teléfono, ya que el número de teléfono que recibe el SMS no tiene código de país, el número de teléfono se compara de atrás hacia adelante y todos son coincidentes con el número más corto. Los números con menos de 6 dígitos se ignoran. Si el número al recibir el SMS o el número configurado contiene '+', se convierte a 0 para el número de teléfono verificación coincidente.

Apéndice 1 Eventos de falla de armado y Descripción

Apéndice Tabla 1-1 Eventos de falla de armado y descripción (periféricos)

No.	Razón	Descripción
1	Pérdida de módulo	El periférico estaba fuera de línea.
2	Error de corazón	No se han enviado paquetes de latidos durante más de 18 minutos.
3	Alarma	Alarma (24 horas).
4	Abierto	La tapa trasera del dispositivo estaba abierta.
5	exOpen	La cubierta posterior del dispositivo externo estaba abierta.
6	Manosear	Se activó la alarma de manipulación periférica.
7	Batería baja	Se detectó batería baja del dispositivo.
8	Pérdida de potencia primaria	Se detectó un fallo en la alimentación principal periférica.
9	Pérdida de batería	Se detectó falla de batería.
10	Sobretensión	Se detectó sobretensión.
11	Sobrecorriente	Se detectó sobrecorriente.
12	Sobrecalentar	Se detectó sobrecalentamiento.
13	Alarma de incendio	Se activó la alarma de incendio.
14	Alarma médica	Se activó la alarma médica.
15	Alarma SOS	Se activó la alarma SOS.
16	Alarma de pánico	Se activó la alarma de pánico.
17	Alarma de gas	Se activó la alarma de fuga de gas.
18	Alarma de intrusión	Se activó la alarma de intrusión.
19	Alarma de atraco	Se activó la alarma de pánico.

Apéndice Tabla 1-2 Eventos de falla de armado y descripción (centro)

No.	Razón	Descripción
1	Alerta de SOS	La alarma de pánico se puede activar a través de la aplicación DMSS.
2	Manosear	Se activó la alarma de manipulación del concentrador de alarma.
3	Error de conexión al servidor	El centro estaba fuera de línea.
4	Error de conexión de SIAServer	Hay un error con la conexión entre el concentrador y el centro de recepción de alarmas SIA.
5	Batería baja	Se detectó batería baja.
6	Pérdida principal	Se detectó un fallo en la alimentación principal.
7	Pérdida de batería	Se detectó falla de batería.

No.	Razón	Descripción
8	Sin GSM	Se detectaron errores en el módulo 2G/4G.
9	Falla del ATS	Se detectó una falla en el sistema de transmisión de alarma.
10	Falla ATP de la red celular	Se detectó una falla en la ruta de transmisión de alarma (falla de la red celular).
11	Fallo de ATP en red cableada/ Wi-Fi	Se detectó una falla en la ruta de transmisión de alarma (falla de red inalámbrica o Wi-Fi).
12	Modo AP	Se detectó una falla en el modo AP.

Apéndice 2 Códigos y descripción de eventos de SIA

Apéndice Tabla 2-1 Códigos y descripción de eventos SIA

No.	Evento	Código original	SIA Código	Descripción
1	Alarma médica	1100	MAMÁ	Se presionó el botón de alarma médica
2	Alarma médica Interrumpido	3100	MH	Se restauró el botón de alarma médica
3	Alarma de incendios	1110	FA	Alarma de incendios
4	Alarma de incendio detenida	3110	FH	Alarma de incendio detenida
5	Alarma de coacción	1121	JA	Alarma de coacción
6	Alarma de pánico silenciosa	1122	JA	Se presionó el botón de pánico El botón de asalto era Apretado
7	Alarma de pánico silenciosa Interrumpido	3122	S.S	Se restauró el botón de pánico El botón de asalto era Restaurado
8	Alarma de pánico audible	1123	Pensilvania	Se presionó el botón de pánico El botón de asalto era Apretado
9	Alarma de pánico audible Interrumpido	3123	PH	Se restauró el botón de pánico El botón de asalto era Restaurado
10	Alarma antirrobo	1130	licenciado en Letras	Movimiento detectado Acción de apertura detectada El contacto externo fue Abierto Alarma de intrusión Rotura de cristal detectada Inclinación detectada Choque detectado

No.	Evento	Código original	SIA Código	Descripción
11	Alarma antirrobo Interrumpido	3130	BR	Movimiento detenido Acción de cierre detectada El contacto externo fue Cerrado Alarma de intrusión detenida El vidrio dejó de romperse Dejó de inclinarse El choque se detuvo
12	Alarma perimetral	1131	licenciado en Letras	Alarma de cable trampa
13	Alarma perimetral Interrumpido	3131	BR	Alarma de cable trampa detenida
14	Alarma de 24 horas	1133	licenciado en Letras	Movimiento detectado Acción de apertura detectada El contacto externo fue Abierto Rotura de cristal detectada Inclinación detectada Choque detectado
15	Alarma de 24 horas Interrumpido	3133	BR	Movimiento detenido Acción de cierre detectada El contacto externo fue Cerrado Alarma de intrusión detenida El vidrio dejó de romperse Dejó de inclinarse El choque se detuvo
16	Alarma de entrada o salida	1134	licenciado en Letras	Movimiento detectado Acción de apertura detectada El contacto externo fue Abierto Rotura de cristal detectada Inclinación detectada Choque detectado

No.	Evento	Código original	SIA Código	Descripción
17	Alarma de entrada o salida detenida	3134	BR	Movimiento detenido Acción de cierre detectada El contacto externo fue Cerrado Alarma de intrusión detenida El vidrio dejó de romperse Dejó de inclinarse El choque se detuvo
18	La tapa se abrió	1137	ejército de reserva	La tapa se abrió Se abrió la tapa externa y el dispositivo se movió
19	La tapa estaba cerrada	3137	TR	La tapa estaba cerrada La tapa externa estaba cerrada y el dispositivo dejó de moverse
20	Módulo de expansión Se desconectó	1143	EM	El módulo de la cámara es Conectado
21	Módulo de expansión Estaba conectado	3143	ES	Módulo de cámara fue Desconectado
22	Alarma de enmascaramiento	1149	ejército de reserva	Alarma de enmascaramiento
23	Alarma de enmascaramiento Interrumpido	3149	TR	Alarma de enmascaramiento detenida
24	Fuga de gas	1151	Georgia	Fuga de gas detectada
25	Fuga de gas detenida	3151	GH	Fuga de gas detenida
26	Fuga de agua	1154	Washington	Fuga de agua detectada
27	Fuga de agua Interrumpido	3154	WH	Fuga de agua detenida
28	Temperatura alta	1158	KA	Temperatura alta
29	Temperatura normal	3158	KH	Temperatura normal
30	Baja temperatura	1159	ZA	Baja temperatura
31	Temperatura normal	3159	ZH	Temperatura normal
32	Falla de alimentación principal	1301	EN	Falla de alimentación principal
33	Energía principal restaurada	3301	Arkansas	Energía principal restaurada
34	Batería baja	1302	YouTube	Batería baja
35	Nivel de batería restaurado	3302	Año	Nivel de batería restaurado
36	Fallo de la batería	1311	YM	Fallo de la batería
37	Batería restaurada	3311	Año	Batería restaurada
38	Sobrecorriente Protección activada	1312	YI	Protección contra sobrecorriente Motivado

No.	Evento	Código original	SIA Código	Descripción
39	Sobrecorriente Protección restaurada	3312	YJ	Protección contra sobrecorriente Restaurado
40	Protección contra sobrecalentamiento Motivado	1318	KA	Protección contra sobrecalentamiento Motivado
41	Protección contra sobrecalentamiento Restaurado	3318	KH	Protección contra sobrecalentamiento Restaurado
42	Sobretensión Protección activada	1319	YP	Protección contra sobretensión Motivado
43	Sobretensión Protección restaurada	3319	YQ	Protección contra sobretensión Restaurado
44	Interferencia de RF	1344	XQ	Interferencia de RF
45	Falla del ATS	1350	Nuevo Testamento	Falla del ATS Fallo de red cableada Fallo de Wi-Fi Fallo de la red celular
46	ATS restaurado	3350	NR	ATS restaurado Red cableada restaurada Wi-Fi restaurado Red celular restaurada
47	Comunicación Falla	1354	YS	Conexión RF-HD fallida
48	Comunicación Restaurado	3354	Sí, sí	Conexión RF-HD restaurada
49	El dispositivo inalámbrico era Desconectado	1355	SG	Conexión perdida
50	El dispositivo inalámbrico era Conectado	3355	Campo a través	Conexión restaurada
51	Bucle de protección en cortocircuito	1372	QT	Bucle de protección en cortocircuito
52	Se arregló el cortocircuito bucle de protección	3372	Código QR	Arreglado el cortocircuito Bucle de protección
53	Fallo del sensor	1380	COMO	Fallo del sensor
54	Sensor restaurado	3380	UN	Falla del sensor restaurada
55	Desarmado por APP	1400	Cuota de mercado	Armado
56	Armado por APP	3400	CQ	Desarmado
57	Desarmado por teclado	1401	OP	Armado
58	Armado por teclado	3401	CL	Desarmado
59	Desarmado por horario	1403	OA	Armado
60	Armado por horario	3403	California	Desarmado

No.	Evento	Código original	SIA Código	Descripción
61	Cancelar	1406	ANTES DE CRISTO	Cancelar
62	Desarmado por llavero	1407	Sistema operativo	Armado
63	Armado por llavero	3407	CS	Desarmado
64	Armado rápidamente	3408	CS	Armado
65	Desarmado por Interruptor de llave	1409	Sistema operativo	Armado
66	Armado por KeySwitich	3409	CS	Desarmado
67	Modo Inicio Activado	3441	Países Bajos	Modo Inicio Activado
68	Modo Inicio Activado por Interruptor de llave	3442	Países Bajos	Modo Inicio Activado
69	Armado con fallas	3450	CF	Armado con fallas
70	Armado fallido	1454	CI	Armado fallido
71	Armado fallido Por horario	1455	CD	Armado fallido
72	Error de salida	1457	EA	Armado fallido
73	Dispositivo bloqueado	1501	DK	Dispositivo bloqueado
74	Dispositivo desbloqueado	3501	HACER	Dispositivo desbloqueado
75	Dispositivo desactivado	1502	Mariscal de campo	Desactivado permanentemente
76	Dispositivo reactivado	3502	QU	Periférico reactivado Periférico
77	Manipulación deshabilitada	1503	tuberculosis	Tapa desactivada permanentemente
78	Tamper habilitado	3503	TU	Tapa habilitada
79	Dispositivo omitido	1570	Mariscal de campo	Pasado por alto
80	Bypass del dispositivo Restaurado	3570	QU	No pasado por alto
81	Tamper anulado	1578	tuberculosis	Señal de manipulación anulada
82	Anulación de manipulación Restaurado	3578	TU	Señal de manipulación no anulada
83	Prueba de activación manual Informe	1601	RX	Informe de prueba
84	Informe de prueba periódica	1602	RP	Informe de prueba periódica
Nulo	Latido del corazón	Nulo	Nulo	Latido del corazón reportado por Dispositivo

Apéndice 3 Compromiso de seguridad y Recomendación

Dahua Vision Technology Co., Ltd. (en adelante, "Dahua") concede gran importancia a la ciberseguridad y la protección de la privacidad, y continúa invirtiendo fondos especiales para mejorar integralmente la concienciación y las capacidades de seguridad de los empleados de Dahua y brindar la seguridad adecuada a sus productos. Dahua ha establecido un equipo de seguridad profesional para brindar control y empoderamiento de seguridad durante todo el ciclo de vida del producto: diseño, desarrollo, pruebas, producción, entrega y mantenimiento. Siguiendo el principio de minimizar la recopilación de datos y los servicios, prohibir la implantación de puertas traseras y eliminar servicios innecesarios e inseguros (como Telnet), los productos Dahua siguen introduciendo tecnologías de seguridad innovadoras y se esfuerzan por mejorar las capacidades de garantía de seguridad del producto, proporcionando a los usuarios de todo el mundo alarmas de seguridad y servicios de respuesta a incidentes de seguridad 24/7 para proteger mejor sus derechos e intereses de seguridad. Asimismo, Dahua anima a los usuarios, socios, proveedores, agencias gubernamentales, organizaciones del sector e investigadores independientes a informar a Dahua PSIRT sobre cualquier riesgo o vulnerabilidad potencial que detecten en los dispositivos Dahua. Para conocer los métodos de informe específicos, consulte la sección de ciberseguridad del sitio web oficial de Dahua.

La seguridad del producto requiere no solo la atención y el esfuerzo continuos de los fabricantes en I+D, producción y entrega, sino también la participación activa de los usuarios, quienes pueden contribuir a mejorar el entorno y los métodos de uso del producto, a fin de garantizar su seguridad una vez puesto en uso. Por ello, recomendamos a los usuarios que utilicen el dispositivo de forma segura, incluyendo, entre otras cosas:

Gestión de cuentas

1. Utilice contraseñas complejas

Consulte las siguientes sugerencias para establecer contraseñas:

- La longitud no debe ser inferior a 8 caracteres;
- Incluya al menos dos tipos de caracteres: letras mayúsculas y minúsculas, números y símbolos;
- No contenga el nombre de la cuenta ni el nombre de la cuenta en orden inverso;
- No utilice caracteres continuos, como 123, abc, etc.;
- No utilice caracteres repetidos, como 111, aaa, etc.

2. Cambie las contraseñas periódicamente

Se recomienda cambiar periódicamente la contraseña del dispositivo para reducir el riesgo de que sea adivinada o descifrada.

3. Asignar cuentas y permisos de forma adecuada

Agregue usuarios de forma adecuada según los requisitos de servicio y administración y asigne conjuntos de permisos mínimos a los usuarios.

4. Habilitar la función de bloqueo de cuenta

La función de bloqueo de cuenta está habilitada por defecto. Se recomienda mantenerla habilitada para proteger la seguridad de la cuenta. Tras varios intentos fallidos de contraseña, la cuenta y la dirección IP de origen correspondientes se bloquearán.

5. Establecer y actualizar la información de restablecimiento de contraseña de manera oportuna

El dispositivo Dahua admite la función de restablecimiento de contraseña. Para reducir el riesgo de que esta función sea utilizada por cibercriminales, si se produce algún cambio en la información, modifíquela a tiempo. Al configurar las preguntas de seguridad, se recomienda no usar respuestas fáciles de adivinar.

Configuración del servicio

1. Habilitar HTTPS

Se recomienda habilitar HTTPS para acceder a los servicios web a través de canales seguros.

2. Transmisión cifrada de audio y vídeo

Si el contenido de sus datos de audio y video es muy importante o confidencial, le recomendamos utilizar la función de transmisión encriptada para reducir el riesgo de que sus datos de audio y video sean interceptados durante la transmisión.

3. Desactiva los servicios no esenciales y utiliza el modo seguro

Si no es necesario, se recomienda desactivar algunos servicios como SSH, SNMP, SMTP, UPnP, AP hotspot, etc., para reducir las superficies de ataque.

Si es necesario, se recomienda encarecidamente elegir modos seguros, incluidos, entre otros, los siguientes servicios:

- SNMP: elija SNMP v3 y configure contraseñas de autenticación y cifrado seguras.
- SMTP: elija TLS para acceder al servidor de buzón.
- FTP: elija SFTP y configure contraseñas complejas.
- Punto de acceso AP: elija el modo de cifrado WPA2-PSK y configure contraseñas complejas.

4. Cambiar HTTP y otros puertos de servicio predeterminados

Se recomienda cambiar el puerto predeterminado de HTTP y otros servicios a cualquier puerto entre 1024 y 65535 para reducir el riesgo de ser adivinado por actores de amenazas.

Configuración de red

1. Habilitar lista de permitidos

Se recomienda activar la lista de permitidos y permitir que solo las IP de esta lista accedan al dispositivo. Por lo tanto, asegúrese de agregar la dirección IP de su computadora y la del dispositivo compatible a la lista de permitidos.

2. Vinculación de direcciones MAC

Se recomienda vincular la dirección IP de la puerta de enlace a la dirección MAC del dispositivo para reducir el riesgo de suplantación de ARP.

3. Construir un entorno de red seguro

Para garantizar mejor la seguridad de los dispositivos y reducir los posibles riesgos cibernéticos, se recomienda lo siguiente:

- Deshabilite la función de mapeo de puertos del enrutador para evitar el acceso directo a los dispositivos de intranet desde la red externa;
- De acuerdo con las necesidades reales de la red, divida la red: si no hay demanda de comunicación entre las dos subredes, se recomienda utilizar VLAN, puerta de enlace y otros métodos para particionar la red para lograr el aislamiento de la red;
- Establecer un sistema de autenticación de acceso 802.1x para reducir el riesgo de acceso ilegal a terminales de la red privada.

Auditoría de seguridad

1. Comprobar usuarios en línea

Se recomienda revisar periódicamente a los usuarios en línea para identificar usuarios ilegales.

2. Comprobar el registro del dispositivo

Al ver los registros, puede obtener información sobre las direcciones IP que intentan iniciar sesión en el dispositivo y las operaciones clave de los usuarios registrados.

3. Configurar el registro de red

Debido a la capacidad de almacenamiento limitada de los dispositivos, el registro almacenado es limitado. Si necesita guardar el registro durante un periodo prolongado, se recomienda habilitar la función de registro de red para garantizar que los registros críticos se sincronicen con el servidor de registro de red para su seguimiento.

Seguridad del software

1. Actualizar el firmware a tiempo

Según las especificaciones operativas estándar de la industria, el firmware de los dispositivos debe actualizarse a la última versión oportunamente para garantizar que cuenten con las funciones y la seguridad más recientes. Si el dispositivo está conectado a la red pública, se recomienda habilitar la función de detección automática de actualizaciones en línea para obtener la información de actualización de firmware publicada por el fabricante de manera oportuna.

2. Actualizar el software del cliente a tiempo

Le recomendamos que descargue y utilice el software de cliente más reciente.

Protección física

Se recomienda realizar protección física para los dispositivos (especialmente los dispositivos de almacenamiento), como colocar el dispositivo en una sala de máquinas y un gabinete dedicados, y tener control de acceso y administración de claves para evitar que personal no autorizado dañe el hardware y otros equipos periféricos (por ejemplo, disco flash USB, puerto serial).

ENABLING A SMARTER SOCIETY AND BETTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053

Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188