Centro de alarmas

Manual de usuario

ZHEJIANG DAHUA VISION TECHNOLOGY CO.LTD. V2.0.0

Prefacio

General

Este manual presenta la instalación, las funciones y las operaciones del concentrador de alarma (en lo sucesivo, el "concentrador"). Lea atentamente antes de usar el dispositivo y guarde el manual en un lugar seguro para futuras consultas.

Instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

Palabras de advertencia	Significado
PELIGRO	Indica un peligro de alto potencial que, si no se evita, provocará la muerte o lesiones graves.
ADVERTENCIA	Indica un peligro potencial medio o bajo que, si no se evita, podría provocar lesiones leves o moderadas.
PRECAUCIÓN	Indica un riesgo potencial que, si no se evita, podría provocar daños a la propiedad, pérdida de datos, menor rendimiento o resultados impredecibles.
CONSEJOS	Proporciona métodos para ayudarlo a resolver un problema o ahorrarle tiempo.
NOTA	Proporciona información adicional como énfasis y complemento del texto.

Revisión histórica

Versión	Contenido de revisión	Tiempo de liberación
V2.0.0	● Configuraciones de red añadidas. ● Se agregaron eventos y descripciones de fallas de armado. ● Se agregaron códigos y descripciones de eventos SIA.	noviembre 2022
V1.1.0	● Se agregaron operaciones en la aplicación COS Pro y DMSS. ● Gestión de usuarios añadida. ● Imágenes actualizadas. ● Se actualizaron las descripciones de los parámetros.	febrero 2022
V1.0.0	Primer lanzamiento.	octubre 2021

Aviso de protección de privacidad

Como usuario del dispositivo o controlador de datos, puede recopilar datos personales de otros, como su rostro, huellas dactilares y número de matrícula. Debe cumplir con las leyes y regulaciones 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 proporcione la información de contacto requerida.

Sobre el Manual

- El manual es solo para referencia. Se pueden encontrar ligeras diferencias entre el manual y el producto.
- No somos responsables de las pérdidas sufridas debido a la operación del producto de manera que no cumpla con el manual.
- El manual se actualizará de acuerdo con las últimas leyes y reglamentos de las jurisdicciones relacionadas. Para obtener información detallada, consulte el manual del usuario en papel, use nuestro CD-ROM, escanee el código QR o visite nuestro sitio web oficial. El manual es solo para referencia. Se pueden encontrar ligeras diferencias entre la versión electrónica y la versión en papel.
- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto pueden dar lugar a que aparezcan algunas diferencias entre el producto real y el manual. Póngase en contacto con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria.
- Puede haber errores en la impresión o desviaciones en la descripción de las funciones, operaciones y datos técnicos. Si hay alguna duda o disputa, nos reservamos el derecho de dar una explicación final.
- Actualice el software del lector o pruebe con otro software del lector convencional si no se puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas registradas y nombres de compañías en el manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, póngase en contacto con el proveedor o con el servicio de atención al cliente si se produce algún problema durante el uso del dispositivo.
- Si hay alguna duda o controversia, nos reservamos el derecho de la explicación final.

Medidas de seguridad y advertencias importantes

Esta sección presenta contenido que cubre el manejo adecuado del dispositivo, la prevención de riesgos y la prevención de daños a la propiedad. Lea atentamente antes de usar el dispositivo y cumpla con las pautas cuando lo use.

Requisitos de operación

- Asegúrese de que la fuente de alimentación del dispositivo funcione correctamente antes de su uso.
- No extraiga el cable de alimentación del dispositivo mientras esté encendido.
- Utilice el dispositivo únicamente dentro del rango de potencia nominal.
- Transporte, use y almacene el dispositivo en condiciones de humedad y temperatura permitidas.
- Evite que los líquidos salpiquen o goteen sobre el dispositivo. Asegúrese de que no haya objetos llenos de líquido encima del dispositivo para evitar que fluyan líquidos hacia él.
- No desmonte el dispositivo.

requerimientos de instalación

WARNING

- Conecte el dispositivo al adaptador antes de encenderlo.
- Cumpla estrictamente con las normas locales de seguridad eléctrica y asegúrese de que el voltaje en el área sea constante y cumpla con los requisitos de energía del dispositivo.
- No conecte el dispositivo a más de una fuente de alimentación. De lo contrario, el dispositivo podría dañarse.

- Observe todos los procedimientos de seguridad y use el equipo de protección requerido proporcionado 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.
- Utilice el adaptador de corriente o la fuente de alimentación de la carcasa proporcionada por el fabricante del dispositivo.
- La fuente de alimentación debe cumplir con los requisitos de ES1 en el estándar IEC 62368-1 y no ser superior a PS2. Tenga en cuenta que los requisitos de la fuente de alimentación están sujetos a la etiqueta del dispositivo.
- Conecte los aparatos eléctricos de clase I a una toma de corriente con puesta a tierra de protección.

Tabla de contenido

1. Introducción

1.1 Resumen

El concentrador de alarma es un dispositivo central en el sistema de seguridad, que controla el funcionamiento de todos los accesorios 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 luego alertará a los usuarios.

1.2 Especificaciones técnicas

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

Tabla 1-1 Especificaciones técnicas

Tipo	Parámetro	Descripción
Puerto	Red	1 puerto Ethernet autoadaptable RJ-45 10 M/100 M
	G/M	SIM única (GSM: 900/1800 MHz); Modo de espera único de doble SIM
	LTE	SIM única (GSM: 900/1800 MHz, WCDMA: B1/B5/B8, LTE-FDD: B1/B3/B5/ B7/B8/B20, LTE-TDD:B38/B40/B41); Modo de espera único de doble SIM
	Batería	puerto de batería de 12 V
	Luz indicadora	1 para múltiples estados (alarma, armado, desarmado, red y mal funcionamiento)
	Botón	1 × reinicio, 1 × encendido, 1 × AP
	Zumbador	Incorporado
	Manosear	1 puerto de tamper de caja para el panel de control de alarma
Función	Notificación SMS	SMS de alarma (hasta 5 números de teléfono) Solo disponible en modelos seleccionados.
	Llamada telefónica Notificación	Sí (hasta 5 números de teléfono) Solo disponible en modelos seleccionados.
	Enlace de vídeo	Sí
	Protocolo de red	TCP/IP, incluidos PPTP, L2TP, DHCP, UPNP y NTP
	Actualización remota	Actualización en la nube
	Configuración Método	aplicación
	Armar y Desarmar Método	Aplicación, teclado, llavero, horario

Tipo	Parámetro	Descripción	
	Número de Periféricos	máx. Periféricos inalámbricos de 150 canales (6 sirenas, 64 llaveros inalámbricos, 4 repetidores y 8 teclados)	
	Área	32 áreas (habitaciones)	
	Fuerza Gestión	Conmutación automática entre la fuente de alimentación principal y la fuente de alimentación de almacenamiento	
		Alarma por pérdida de energía principal	
		Alarma por pérdida de batería y falla de voltaje de la batería	
	Registros de eventos	máx. 400	
	Fallo de alimentación Protección para Configurado Parámetros	Sí	
	Usuario Gestión	máx. 8 usuarios: 1 instalador, 1 administrador, 6 usuarios generales	
	Consulta	Búsqueda de mensajes push, estado del dispositivo y versión del programa. Detección de la fuerza de la señal.	
RF	Frecuencia de carga	DHI-ARA3000H-FW2 (868)/DHI-ARA3000H-GW2 (868)/DHI-ARA3000H-W2 (868): 868,0 MHz–868,6 MHz	DHI-ARA3000H-FW2/DHI-ARA3000H-GW2/DHI-ARA3000H-W2: 433,1 MHz–434,6 MHz
	Comunicación Distancia	DHI-ARA3000H-FW2 (868)/DHI-ARA3000H-GW2 (868)/DHI-ARA3000H-W2 (868): Hasta 2000 m (6561,68 pies) en un espacio abierto	DHI-ARA3000H-FW2/DHI-ARA3000H-GW2/DHI-ARA3000H-W2: Hasta 1.200 m (3.937,01 pies) en un espacio abierto
	Transmisión Fuerza	DHI-ARA3000H-FW2 (868)/DHI-ARA3000H-GW2 (868)/DHI-ARA3000H-W2 (868): Límite 25 mW	DHI-ARA3000H-FW2/DHI-ARA3000H-GW2/DHI-ARA3000H-W2: Límite 10 mW
	Comunicación Mecanismo	bidireccional	
	Modo de encriptación	AES128	
	Frecuencia Saltando	Sí	
	Interferencia de radiofrecuencia Detección	Para una detección de 60 segundos, si la interferencia dura más de 30 segundos, el sistema informa la información de interferencia de RF.	
	Wifi	2,4G	
Fuerza Suministrar	Tipo de PS	Escribe un	
	Poder principal	12 V CC, 1,5 A	
	Capacidad de la batería	2x 3,6 V/2150 mAh	

Tipo	Parámetro	Descripción
	Batería en espera	Hasta 12h Cuando se cumplen las siguientes condiciones, el tiempo de espera puede llegar a 12 h: ● Se conecta con Wi-Fi, GPRS/3G/4G. ● Se conecta a ARC y el intervalo de latidos es de 1800 segundos. ● Se conecta a 8 entradas y 1 sirena. ● Se conecta a la nube.
	Tipo de Batería	Tipo de batería: Polímero de iones de litio recargable incorporado; modelo de batería: 18650
	máx. actual disponible	3,5A
	Fuerza Consumo	máx. 15W
	Actual Consumo	normal: 220mA; alarma: 300mA
	Bateria BAJA Umbral de batería	3,5 VCC
	Restaurar batería Límite	3,7 VCC
	Voltaje de liberación	＜3.358V
	Recarga de batería Tiempo	80% aprox. 15 horas
ARCO Señalización	Categoría ATS	DP2/SP2 (LAN/Wi-Fi y GPRS/4G)
	Reconocemento Operación	Pasar por
	protocolos	SIA-DC09
	Primario Ruta de transmisión	LAN/Wi-Fi (Nº 50136-2)
	Secundario Ruta de transmisión	GPRS/4G
	Notificación Equipo	C/E/F

Tipo	Parámetro	Descripción	
Certificaciones		DHI-ARA3000H-FW2 (868)/DHI-ARA3000H-GW2 (868)/DHI-ARA3000H-W2 (868): EN 50131-1:2006+A1:2009+A2:2017+A3:2020 EN 50131-3:2009 EN 50131-6:2017 EN 50131-5-3:2017 EN 50131-10: 2014 EN 50136-2: 2013 Grado de seguridad 2 Clase ambiental II CE	DHI-ARA3000H-FW2/DHI-ARA3000H-GW2/DHI-ARA3000H-W2: FCC CE

Tabla 1-2 Categoría ATE

COMIÓ Categoría	Informes Tiempo	protocolos	Dispositivos de comunicación			Comunicación Dispositivo a utilizar
			RTPC	2G/3G	IP	
SP2	25 horas	Estándar	√			El cheque marcado comunicación dispositivo
SP3	30 minutos	Estándar		√	√	Solo uno de los dos marcados comunicación dispositivos
SP4	3 minutos	encriptado		√	√	Solo uno de los dos marcados comunicación dispositivos
SP5	90s	encriptado		√	√	Solo uno de los dos marcados comunicación dispositivos
DP1	25 horas	Estándar	√	√	√	Solo dos de los tres marcados comunicación dispositivos
DP2	30 minutos	Estándar	√	√	√	Solo dos de los tres marcados comunicación dispositivos
DP3	3 minutos	encriptado		√	√	los dos chequean marcado comunicación dispositivos

COMIÓ **Categoría**	**Informes** **Tiempo**	**protocolos**	**Dispositivos de comunicación**			**Comunicación** **Dispositivo a utilizar**
			RTPC	**2G/3G**	**IP**	
DP4	90s	encriptado		√	√	los dos chequean marcado comunicación dispositivos

ATE: Equipo de transmisión de alarmas.

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 presentación de informes: El tiempo de presentación de informes se prescribe en función del estándar de cada nivel de desempeño. El tiempo de notificación es el tiempo máximo disponible para informar cuando falla un dispositivo de transmisión de alarma. Los dispositivos de transmisión de alarmas cumplen con este requisito informando regularmente su estado a través de una función de prueba simbólica específica.

Protocolos: Indica el nivel de seguridad de los protocolos a utilizar para la notificación de fallas. Los protocolos estándar y los protocolos de voz están encriptados. Los protocolos de alta seguridad se cifran con una clave de cifrado AES de 128 bits o AES de 256 bits.

Dispositivos de comunicación: Dispositivos de comunicación implementados.

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

Tabla 1-3 Especificaciones técnicas

Especificación técnica	**Descripción**
Clasificación ACE	Escribe un
Clase ambiental	Yo
Voltaje de suministro	12 V CC, 1,5 A
Dimensiones del producto	163,0 mm × 163,0 mm × 32,0 mm (6,42" × 6,42" × 1,26")
Dimensiones del embalaje	219,0 mm × 187,0 mm × 91,0 mm (8,62" × 7,36" × 3,58")
Temperatura de funcionamiento	– 10 °C a +50 °C (+14 °F a +122 °F) – 10 °C a +40 °C (+14 °F a 104 °F) (temperatura certificada)
Humedad	10%–90% (HR)
Peso neto	0,38 kg (0,84 libras)
Peso bruto	0,8 kg (1,76 libras)
Caja	PC + ABS

1.3 Lista de verificación

Verifique el paquete de acuerdo con la siguiente lista de verificación. Si encuentra algo dañado o perdido,

Contactar Servicio al Cliente.

Figura 1-1 Lista de verificación

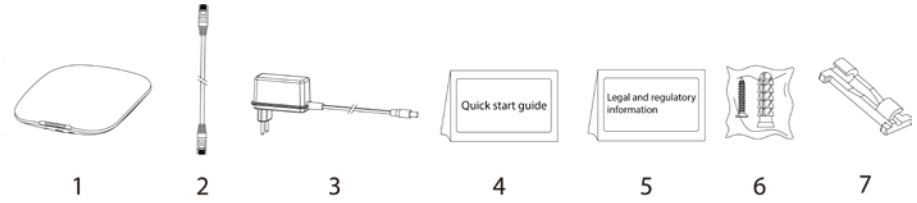


Tabla 1-4 Lista de verificación

No.	Nombre del árticulo	Cantidad	No.	Nombre del árticulo	Cantidad
1	Centro de alarma	1	5	Legal y regulatorio información	1
2	Cable	1	6	Paquete de tornillos	1
3	Adaptador	1	7	Clip de abrazadera de fijación de cable	1
4	Guía de inicio rápido	1	—	—	—

2 diseño

2.1 Apariencia

Figura 2-1 Apariencia

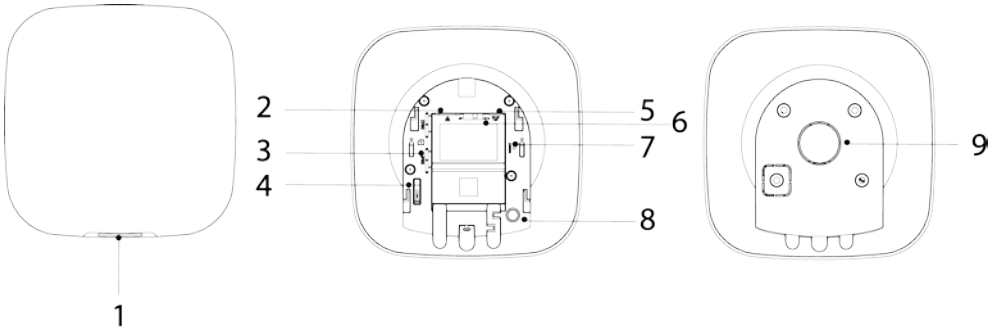


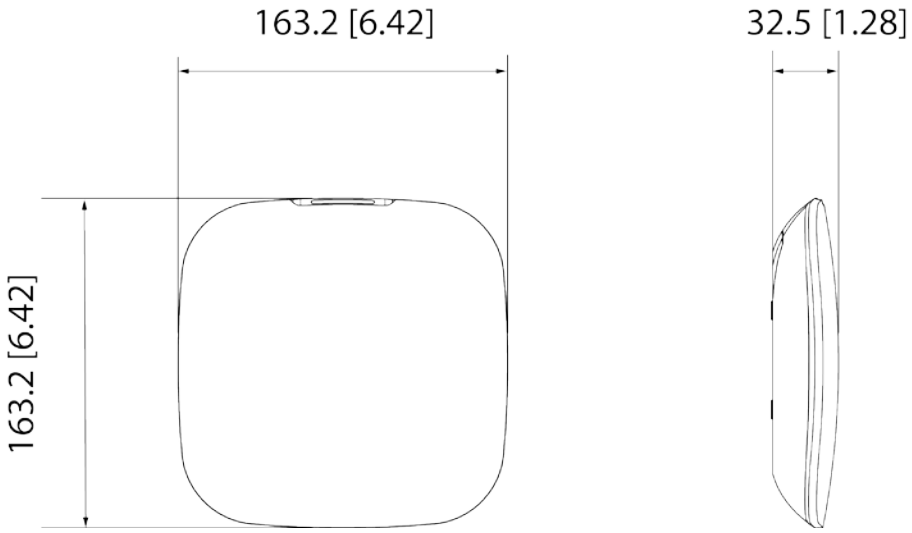
Tabla 2-1 Estructura

No.	Nombre	Descripción
1	Indicador	● Parpadea lentamente en verde: modo de sensibilidad reducida. ● Parpadea en verde: el concentrador comienza a funcionar. ● Amarillo fijo: no se pudo conectar a la nube. ● Verde continuo: modo de desarmado. ● Azul continuo: modo de armado. ● Parpadea en rojo: se activó el evento de alarma. ● Parpadea en amarillo: Detectado 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	Toma de cable Ethernet	Conecte el concentrador a la Ethernet.
3	Ranura para micro SIM 1/2	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 use datos móviles y envíe notificaciones de alarma. ● Las tarjetas SIM no funcionarán hasta que la configuración de la red haya finalizado. sido completado ● La función SIM solo está disponible en modelos seleccionados.
4	Botón de sabotaje	Cuando se suelta el interruptor de manipulación, se activará la alarma de manipulación.
5	Enchufe del cable de alimentación	Inserte el cable de alimentación.
6	punto de acceso	Encienda AP, el teléfono se conectará al punto de acceso desde el concentrador y luego sincronizará el nombre de usuario y la contraseña de Wi-Fi con el concentrador.

No.	Nombre	Descripción
7	Botón de reinicio	Mantenga presionado el botón durante 10 segundos para reiniciar el concentrador y restaurar la configuración predeterminada de fábrica.
8	Boton de encendido / apagado	Mantenga presionado el botón durante 2 segundos para encender o apagar el concentrador.
9	Contraportada	Si se abre la tapa trasera, se activará la alarma de manipulación.

2.2 Dimensiones

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



3 Inicio

3.1 Usuarios

Los usuarios solo se pueden crear en la aplicación DMSS y COS Pro. Clasifique a los usuarios en diferentes roles para que puedan tener diferentes niveles de acceso para operar los dispositivos.

Nivel de acceso de usuario

Tabla 3-1 Nivel de acceso de usuario

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

- Instalador: Los instaladores brindan a los usuarios finales servicios de operación y mantenimiento. Este rol debe solicitar permisos del usuario final (usuario administrador de DMSS) para operar el dispositivo. Pueden recibir permisos como configuración de dispositivos y administración de usuarios.
- Usuario administrador de DMSS: el usuario administrador sería un usuario final. Este rol no se puede modificar y tiene permisos, como configuración de dispositivos y administración de usuarios. Los usuarios administradores de DMSS no tienen permiso para configurar el dispositivo cuando los instaladores les prestan el concentrador o cuando confían el concentrador al instalador.
- Usuario general de DMSS: estos son usuarios con los que un usuario 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 encomienda y uso compartido en la aplicación DMSS y COS Pro. Los instaladores y los usuarios finales pueden seguir el proceso para compartir y confiar dispositivos.

Figura 3-1 Flujo comercial (usuario de DMSS)

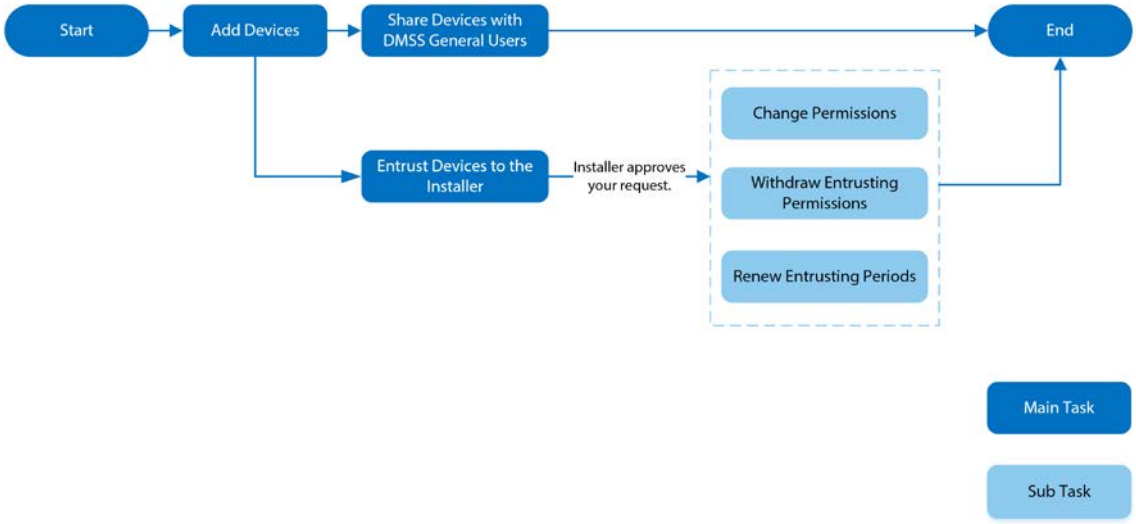
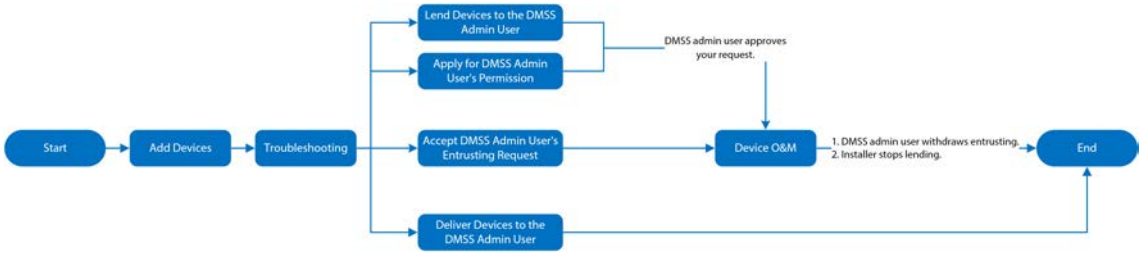


Figura 3-2 Flujo comercial (Instalador)



3.2 Proceso de Operación

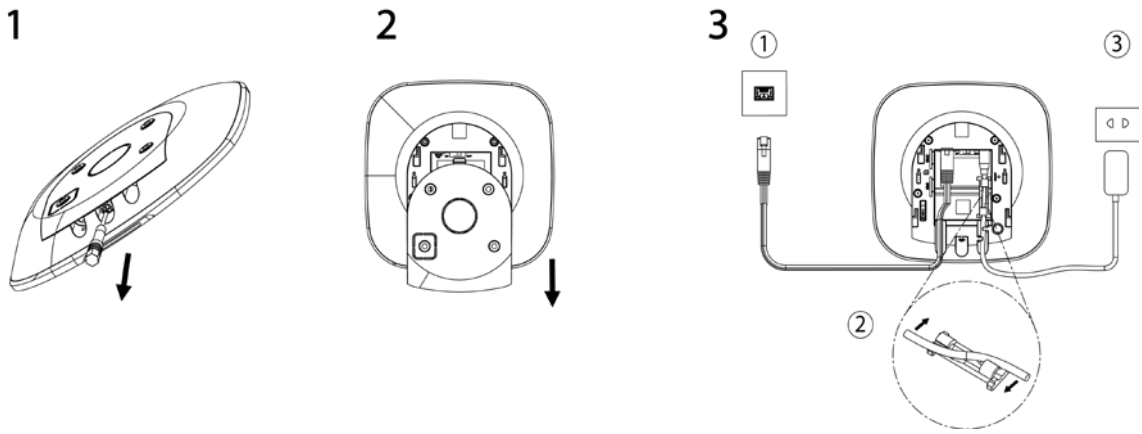
Siga los procedimientos a continuación para encender el sistema de alarma inalámbrico.

Figura 3-3 Proceso de operación

Encendido

Conecte el concentrador a Ethernet y encienda el concentrador.

Figura 3-4 Encendido



Adición de dispositivos

1. Agregue el concentrador a la aplicación COS Pro y DMSS. Para obtener más información, consulte "4.2 Adición de dispositivos" y "5.2 Adición de dispositivos".
2. Agregue los accesorios al cubo. Para obtener más información, consulte "4.2.2 Adición de accesorios" y "5.2.2 Adición de accesorios".

Instalación del concentrador

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

- Al aire libre.
- Lugares próximos a objetos metálicos que provoquen atenuación y apantallamiento de la señal de radio.
- Lugares con una señal GSM débil.
- Lugares próximos a fuentes de interferencias de radio que estén a menos de 1 metro del router y de los cables de alimentación.
- Lugares donde la temperatura y la humedad excedan los límites permitidos.

Figura 3-5 Instalación

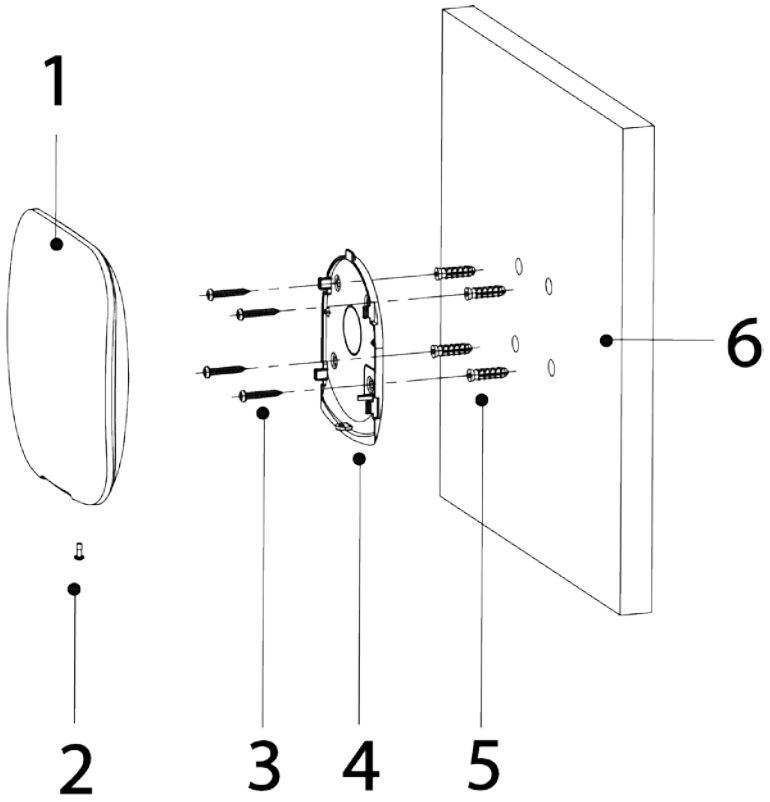


Tabla 3-2 Elementos de instalación

No.	Nombre del árticulo	No.	Nombre del árticulo
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 para los tornillos y, a continuación, taladre en la placa de montaje.
2. Coloque los pernos de expansión en los orificios.
3. Fije la placa de montaje a la pared y luego alinee los orificios para tornillos de 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 cubo de la alarma y la placa de montaje con tornillos de cabeza avellanada M3 × 8 mm.

Configuración del concentrador

Configure el concentrador en la aplicación COS Pro y DMSS. Para obtener más información, consulte "4.6.2 Configuraciones básicas del dispositivo".

Armar el sistema de alarma

Puede usar el teclado, el control remoto y la aplicación para armar su sistema. Después de enviar un comando de armado a la aplicación COS Pro y DMSS, el sistema verificará el estado del sistema. Si el sistema tiene una falla, deberá elegir si forzar el armado. Para obtener detalles sobre cómo armar y desarmar el sistema, consulte "6 Operaciones generales". Para obtener detalles sobre los accesorios, consulte el manual de usuario del dispositivo correspondiente.

4 Operaciones COS Pro para instaladores

La aplicación COS Pro está diseñada para ayudar a los instaladores al brindar servicios profesionales de operación y mantenimiento para los usuarios finales. Proporciona funciones que incluyen la administración del sitio, la operación y la administración del estado del dispositivo, la revisión de la confianza del dispositivo y más. Para más detalles, consulte*COS Pro App_Manual del usuario*.

Las cifras son solo de referencia y pueden diferir de la interfaz real.

4.1 Iniciar sesión en COS Pro

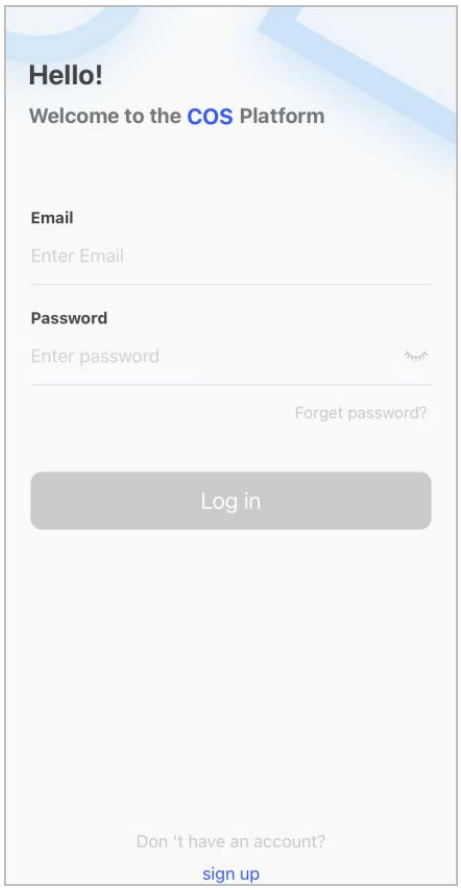
Para el uso por primera vez, debe crear una cuenta. Este manual de usuario utiliza las operaciones en iOS como ejemplo.

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

Para usuarios de Android, puede ir a Google Play para descargar COS Pro.

Paso 2 En su teléfono, toque para iniciar la aplicación.

Figura 4-1 Inicio de sesión



Paso 3 Crea una cuenta.

1. En el**Acceso**pantalla, toque**inscribirse**.
2. En el**Registro**pantalla, complete la información de los campos requeridos.

Si el país/región que selecciona es de América del Norte, entonces el**Número de registro del distribuidor**aparecerá en el**Registro**pantalla. Para todos los demás países y regiones, **nombre de empresa**aparecerá.

- **Correo electrónico**: Introduzca su dirección de correo electrónico.
- **País/Región**: Seleccione el país/región, provincia/estado y ciudad de su empresa.
- **DIRECCIÓN**: Introduzca la dirección detallada de su empresa.
- **nombre de empresa**: Introduzca el nombre de su empresa.
- **Número de registro del distribuidor**: Introduzca el número de registro del distribuidor.

  Para clientes en América del Norte, ingrese el número de registro del distribuidor.
- **código de invitación**: Ingrese el código de invitación, que se puede obtener del invitador.
- **Contraseña**y**confirmar Contraseña**: Introduzca la contraseña y confírmela de nuevo.
- **Código de verificación**: Grifo**Enviar**, marque su casilla de correo electrónico para recibir un código de verificación y luego ingrese el código en**Código de verificación**.

3. Lea el**política de privacidad**y**Protocolo de servicio**y, a continuación, seleccione el**He leído y acepto la Política de Privacidad y el Protocolo de Servicio**caja.
4. Toque**Registro**, y luego la aplicación vuelve a la**Acceso**pantalla. Ingrese su

Etapa 4 dirección de correo electrónico y contraseña, y luego toque**Acceso**.

- Para nuevos clientes, se necesita la aprobación de la solicitud de cuenta. Tomará de 1 a 3 días recibir un correo electrónico de aprobación de la cuenta. Después de eso, puede iniciar sesión en la aplicación con su cuenta.
- Algunos clientes afiliados no necesitan aprobación para registrarse en una cuenta COS Pro. Pueden iniciar sesión directamente en la aplicación después del registro.

4.2 Adición de dispositivos

Para los instaladores, puede agregar dispositivos a la aplicación COS Pro para administración y mantenimiento. Antes de agregar dispositivos, asegúrese de que el dispositivo esté conectado a la alimentación y a la red. Puede agregar dispositivos de alarma, incluidos concentradores y múltiples accesorios a la aplicación.

4.2.1 Agregar el concentrador

El concentrador se puede agregar en**Modo de sitio**o**modo de dispositivo**. Si agrega dispositivos en el**modo de dispositivo**, primero debe seleccionar un sitio. Las operaciones para estos dos modos son similares. Esta sección utiliza configuraciones en**modo de dispositivo**como ejemplo.

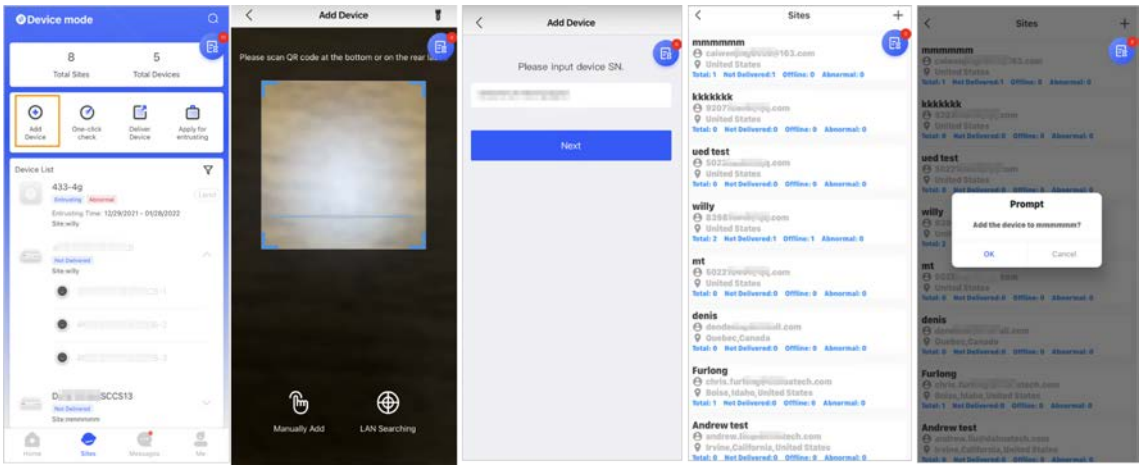
- Antes de agregar el concentrador, asegúrese de que el concentrador esté conectado a la alimentación y a la red.
- Asegúrese de que su teléfono tenga habilitada la función Wi-Fi.

4.2.1.1 Adición por código SN/QR

Puede agregar el concentrador escaneando el código QR del dispositivo o ingresando manualmente el SN del dispositivo en la red inalámbrica o cableada.

Paso 1 Sobre el**Hogar**pantalla, toque , y luego va a**Sitios**pantalla.

Figura 4-2 Agregar un dispositivo



Paso 2 Grifo en la esquina superior izquierda para cambiar a**modo de dispositivo**. para

Paso 3 Grifo agregar un dispositivo.

Etapa 4 Escanee el código QR del dispositivo o toque**Agregar manualmente**para ingresar manualmente el SN del dispositivo.

Paso 5 Seleccione un sitio y luego toque**DE ACUERDO**.

Paso 6 Sobre el**Añadir dispositivo**pantalla, seleccione un tipo de

Paso 7 dispositivo. Conéctese a una red inalámbrica o cableada.

- **Inalámbrico**

1) Toca**Inalámbrico**en la esquina superior derecha y luego**Inalámbrico**se convierte**cableado**.

2) Ingrese la contraseña para el Wi-Fi al que está conectado su teléfono y luego toque **Conectar**.

3) Siga las instrucciones en pantalla y luego toque**Próximo**.

4) Espere el emparejamiento.

Si falla, repita los procedimientos anteriores.

- **cableado**

1) Toca**cableado**en la esquina superior derecha y luego**cableado**se convierte**Inalámbrico**.

2) Conecte el dispositivo a la alimentación y a la red, y luego toque**Próximo**.

Si falla, repita los procedimientos anteriores.

Paso 8 Si el concentrador que está agregando no está inicializado, ingrese la contraseña y confírmela nuevamente, y luego toque**Inicializar el dispositivo**para completar la inicialización.

Paso 9 Grifo**Terminado**y luego podrá ver el dispositivo en la lista de dispositivos.

4.2.1.2 Agregar a través de la configuración de AP

Puede agregar el concentrador a través de la configuración de AP.

Paso 1 Sobre el**Hogar**pantalla, toque , y luego va a**Sitios**pantalla.

Paso 2 Toque en la esquina superior izquierda para cambiar a**modo de dispositivo**. para

Paso 3 Grifo agregar un dispositivo.

Figura 4-3 Agregar un dispositivo

Etapa 4 Escanee el código QR del dispositivo o toque**Agregar manualmente**para ingresar manualmente el SN del

Paso 5 dispositivo. Sobre el**Añadir dispositivo**pantalla, seleccione**Estación de alarma**.

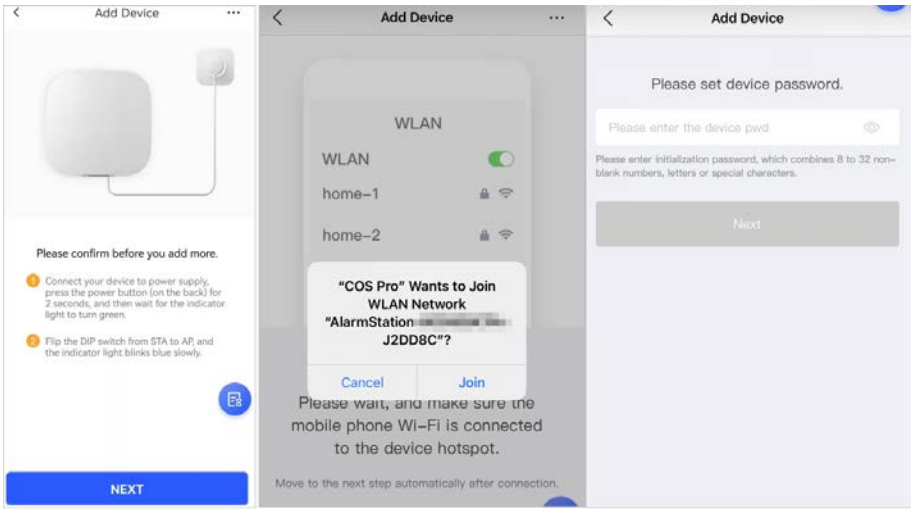
Figura 4-4 Seleccionar estación de alarma

Paso 6 Siga las instrucciones en pantalla y mueva el interruptor DIP de STA a AP. Grifo**Unirse**para

Paso 7 conectarse al punto de acceso del dispositivo.

Paso 8 Establezca la contraseña del dispositivo para inicializar el dispositivo y luego toque**Próximo**.

Figura 4-5 Agregar a través de la configuración de AP



Paso 9 Conéctese a la red. 1)

Seleccione WiFi.

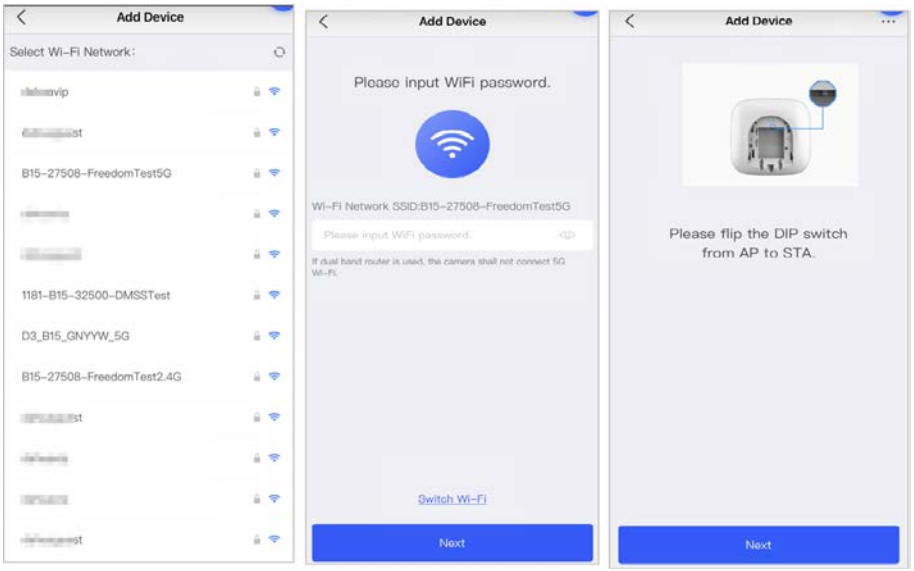
Asegúrese de que su teléfono y el dispositivo estén conectados a la misma red.

2) Ingrese la contraseña de Wi-Fi y luego toque**Próximo**.

3) Mueva el interruptor DIP de AP a STA y luego toque**Próximo**.

4) Espere a que el dispositivo complete la configuración de la red.

Figura 4-6 Conectarse a la red



Paso 10 Grifo**Terminado**.

4.2.1.3 Adición mediante búsqueda LAN

Puede buscar dispositivos y agregarlos. Asegúrese de que su teléfono y los dispositivos estén conectados a la misma red.

Paso 1 Sobre el**Hogar**pantalla, toque , y luego va a**Sitios**pantalla.

Paso 2 Toque en la esquina superior izquierda para cambiar a**modo de dispositivo**. para

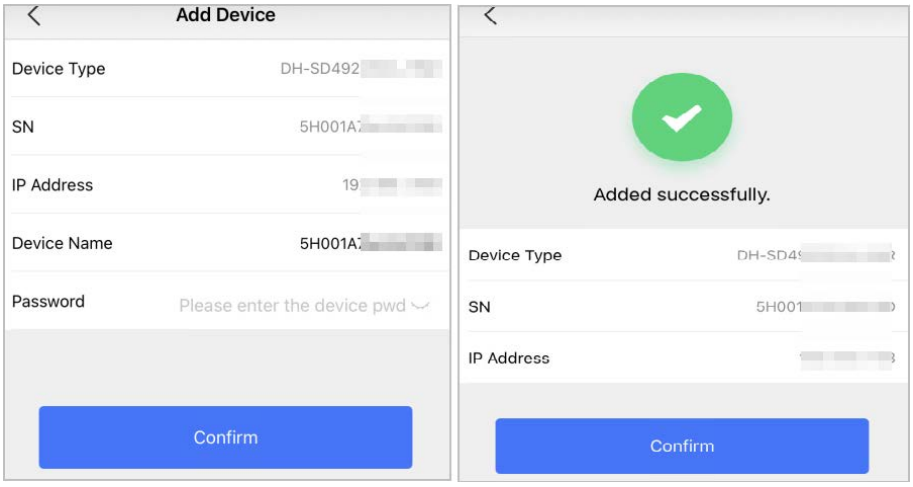
Paso 3 Grifo agregar un dispositivo.

Figura 4-7 Agregar un dispositivo

Etapa 4 Grifo**Búsqueda de LAN**.

Paso 5 En**Añadir dispositivo**pantalla, ingrese la contraseña del dispositivo y luego toque**Confirmar**.

Figura 4-8 Confirmar para agregar un dispositivo



4.2.2 Adición de accesorios

Puede agregar múltiples accesorios en el centro. La sección utiliza el detector de puerta como ejemplo. Para obtener detalles sobre cómo agregar accesorios, consulte los manuales de usuario de los accesorios respectivos.

Se pueden agregar hasta 6 sirenas, 64 llaveros, 4 repetidores y 8 teclados a un concentrador.

Paso 1 En la pantalla central, toque la parte en la esquina superior derecha y luego escanee el código QR en la inferior del detector de puerta. Grifo

Paso 2 **Próximo**.

Paso 3 Siga las instrucciones en pantalla y encienda el detector de puerta y luego toque**Próximo**para agregarlo al concentrador.

Etapa 4 Espera el emparejamiento.

Paso 5 Personalice el nombre del detector de puerta y seleccione el área, y luego toque**Terminado**.

- Eliminar el accesorio: vaya a la pantalla del concentrador, seleccione el accesorio de la lista y luego desliza el dedo hacia la izquierda para eliminarlo.
- Se pueden crear hasta 32 áreas en un concentrador.

4.3 Gestión de usuarios

4.3.1 Adición de usuarios administradores de DMSS

Para el instalador, puede agregar usuarios administradores de DMSS compartiendo dispositivos de confianza con ellos o aceptando su solicitud de confianza.

El usuario administrador de DMSS no tiene permiso para configurar el dispositivo cuando los instaladores prestan el hub a ellos, o cuando confían el hub al instalador.

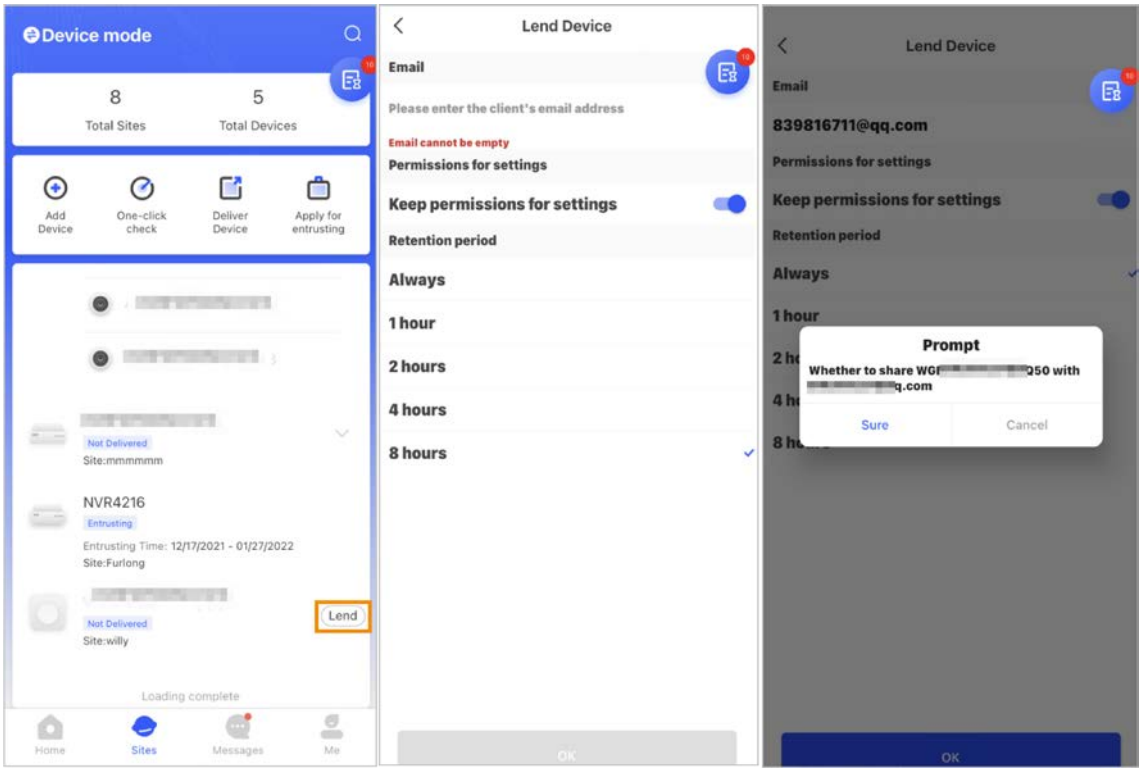
4.3.1.1 Préstamo del dispositivo a los usuarios administradores de DMSS

El instalador puede prestar el concentrador al usuario administrador de DMSS. Posteriormente, el instalador debe solicitar permisos del usuario administrador de DMSS, como la configuración del dispositivo, las operaciones de armado y desarmado y la administración de usuarios.

Asegúrese de que otras cuentas no hayan agregado el concentrador.

Paso 1 Sobre el**Hogar**pantalla, toque , y luego va a**Sitios**pantalla.

Figura 4-9 Prestar el concentrador al usuario administrador de DMSS



Paso 2 Grifo en la esquina superior izquierda para cambiar a**modo de dispositivo**.

Paso 3 En la lista de dispositivos, seleccione un concentrador, toque**Prestar**en la esquina derecha del cubo. Ingrese el correo

Etapa 4 electrónico del usuario administrador de DMSS.

Paso 5 Permitir**Reservar permisos de configuración**y seleccione el tiempo de retención. Grifo

Paso 6 **Confirmar**.

Paso 7 En la pantalla, toque**Mensaje personal**, puede ver los mensajes para ver si el usuario administrador de DMSS aceptó su solicitud para compartir con ellos.

Se enviará un mensaje para compartir a la cuenta de usuario administrador de DMSS, y el usuario administrador de DMSS puede leer el mensaje en la aplicación DMSS.

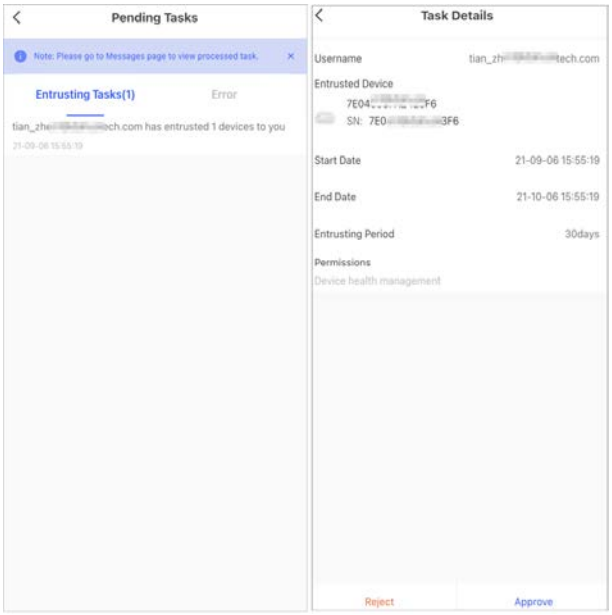
4.3.1.2 Aceptación de solicitudes de confianza

El instalador puede aceptar la solicitud de confianza del usuario administrador de DMSS.

Paso 1 Sobre el**Hogar**pantalla, seleccione**Tarea pendiente**>**Encomendar revisión**.

Paso 2 Sobre el**Tarea pendiente**pantalla, seleccione una tarea para ver los detalles de la tarea y manejar las aplicaciones de confianza.

Figura 4-10 Manejar tareas de encomienda

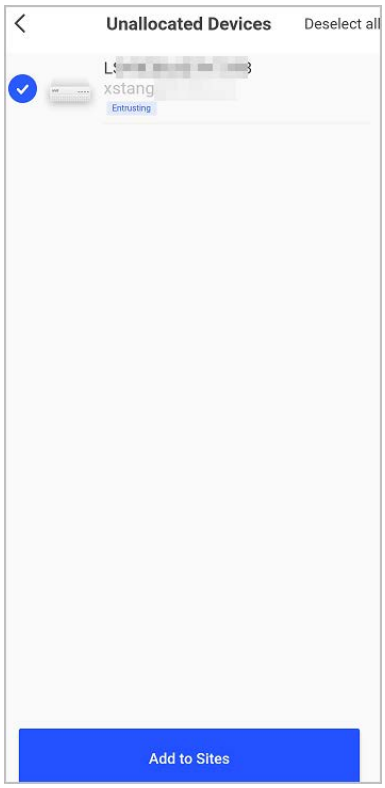


- Aprobar

1) Toca**Aprobar**, y luego va a la**Dispositivos no asignados**pantalla.

2) Seleccione los dispositivos que se asignarán o toque**Seleccionar todo**y luego toque**Agregar a sitios**.

Figura 4-11 Agregar dispositivo a sitios

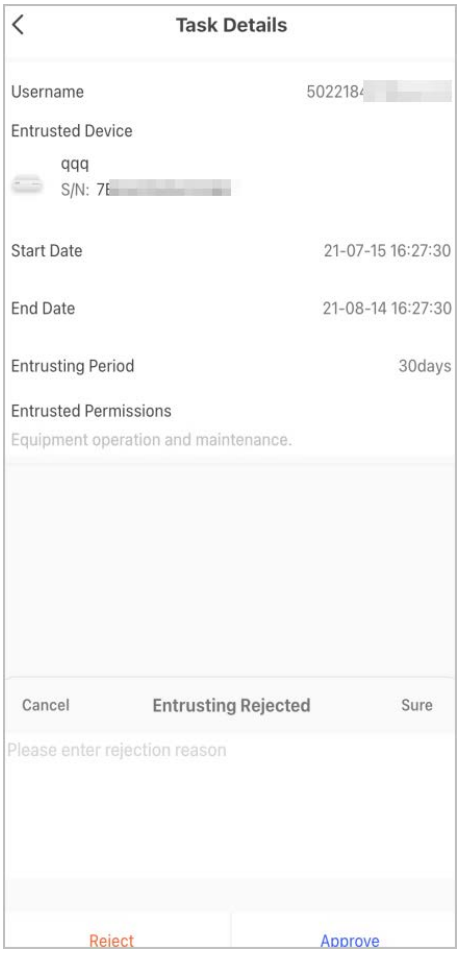


3) En el**Sitios**pantalla, seleccione un sitio o agregue un nuevo sitio.

4) Toca**DE ACUERDO**para confirmar mover este dispositivo al sitio seleccionado.

- Para rechazar: toca**Rechazar**, ingrese los motivos del rechazo y luego toque**Seguro**.

Figura 4-12 Rechazar



4.3.2 Eliminación de usuarios

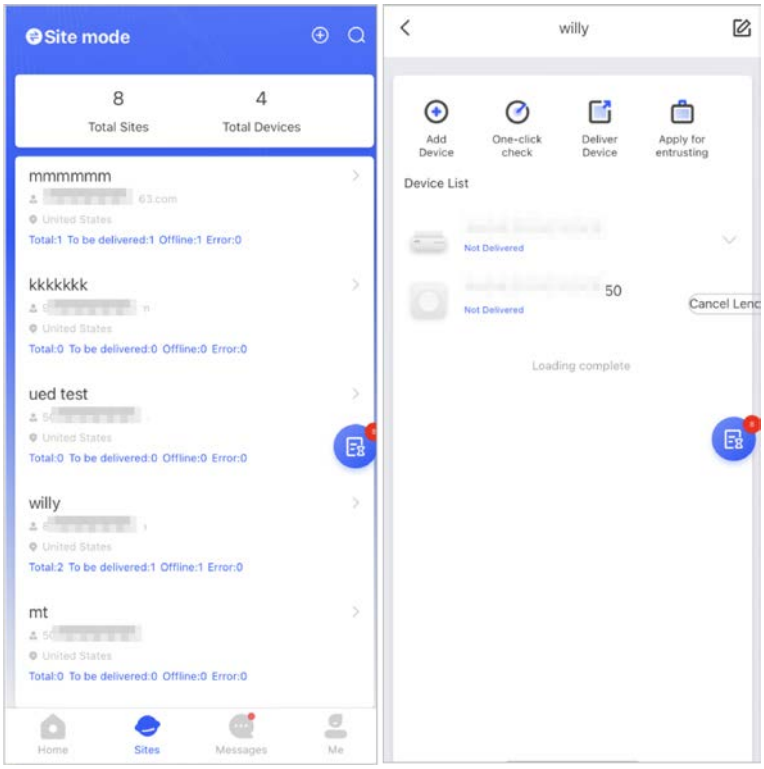
Para el instalador, puede eliminar un usuario cancelando el préstamo de los dispositivos al usuario administrador de DMSS o eliminando los dispositivos.

4.3.2.1 Cancelación para prestar los dispositivos

Para el instalador, puede eliminar a los usuarios administradores de DMSS cancelando para prestarles el concentrador.

Paso 1 Sobre el**Hogar**pantalla, toque , y luego va a**Sitios**pantalla.

Figura 4-13 Prestar el concentrador al usuario administrador de DMSS



Paso 2 Grifo en la esquina superior izquierda para cambiar a**Modo de sitio**.

Paso 3 En la lista de sitios, seleccione el sitio con el dispositivo que le prestó al usuario administrador de DMSS, luego seleccione el concentrador y luego toque**Cancelar Prestar**.

El mensaje se enviará a la cuenta de usuario administrador de DMSS, y el usuario administrador de DMSS puede lea el mensaje en la aplicación DMSS.

4.3.2.2 Eliminación de dispositivos

Para el instalador, puede eliminar usuarios administradores de DMSS eliminando dispositivos.

- Asegúrese de que el instalador haya cancelado el préstamo de los dispositivos al usuario administrador de DMSS.
- El instalador puede eliminar todos los usuarios de DMSS si el usuario administrador de DMSS ha compartido los dispositivos con el DMSS. usuarios generales.

Paso 1 Sobre el**Hogar**pantalla, toque , y luego va a**Sitios**pantalla. Toque en la esquina

Paso 2 superior izquierda para cambiar a**modo de dispositivo**. En la lista de dispositivos,

Paso 3 seleccione el dispositivo según sea necesario.

Etapa 4 En la pantalla del concentrador, toque y luego toque**Borrar**para eliminar el dispositivo.

4.4 Solicitud de permiso de usuario administrador de DMSS

Para los instaladores, puede agregar el concentrador directamente a la aplicación COS Pro para proporcionar servicios de operación y mantenimiento del dispositivo para los usuarios administradores de DMSS. Tiene permisos por tiempo limitado, incluidos

configuración del dispositivo y administración de usuarios, y debe volver a solicitar el permiso al vencimiento. Paso 1 Sobre el**Hogar**pantalla, toque , y luego va a**Sitios**pantalla. Toque en la esquina

Paso 2 superior izquierda para cambiar a**modo de dispositivo**. En la lista de dispositivos,

Paso 3 seleccione el dispositivo según sea necesario.

Etapa 4 Sobre el**Centro**pantalla, seleccione > **Configuración del concentrador**, toque cualquier parámetro que desee configurar y luego aparecerá un mensaje para recordarle que solicite permisos del usuario administrador de DMSS.

Paso 5 Grifo**Seguro**.

Paso 6 Seleccione las horas de permiso y luego toque**Confirmar**.

Paso 7 En la pantalla, toque**Mensaje personal**para ver los mensajes y ver si el usuario administrador de DMSS accedió a asignarle permisos.

Se enviará un mensaje de solicitud a la cuenta de usuario administrador de DMSS, y el usuario administrador de DMSS puede leer el mensaje en la aplicación DMSS.

4.5 Entrega de dispositivos al usuario administrador de DMSS

Después de depurar los dispositivos, puede entregarlos al usuario administrador de DMSS. Los dispositivos sin conexión y en confianza no se pueden entregar.

Los requisitos de las certificaciones En50131 no se cumplirán si el instalador entrega el concentrador a un DMSS usuario administrador.

Paso 1 Sobre el**Hogar**pantalla, toque , y luego va a**Sitios**pantalla. Toque en la

Paso 2 esquina superior izquierda para cambiar a**Modo de sitio**.

Paso 3 En la lista de sitios, seleccione un sitio con dispositivos que deben entregarse al usuario administrador de DMSS.

Etapa 4 Toque y luego va a**Entregar dispositivos**pantalla.

No se pueden entregar más de 5 dispositivos a la vez.

Paso 5 Ingrese los correos electrónicos del usuario administrador de DMSS y luego toque**Seguro**para ver los resultados de la entrega. Para los dispositivos que no se entregaron al usuario administrador de DMSS, vaya a la**Fallido**pantalla para entregar de nuevo.

Si los clientes están utilizando la cuenta de Imou, sus dispositivos no se entregarán correctamente. Y aparecerá un mensaje en la**Hogar**pantalla que indica que la cuenta no tiene la permiso. Pídale al cliente que actualice la cuenta en la aplicación DMSS. Para detalles, ver*Manual del usuario de la aplicación DMSS.*

4.6 Funcionamiento y mantenimiento del estado del dispositivo

Los instaladores pueden proporcionar servicios de mantenimiento de la operación y el estado del dispositivo, como verificar la

estado de salud de los dispositivos, configuración remota de dispositivos y corrección de errores.

4.6.1 Comprobación del estado de salud del dispositivo

Puede verificar el estado en línea y fuera de línea de los dispositivos en tiempo real y verificar el estado de salud de los dispositivos uno a la vez o en lotes. Esta sección utiliza el registro de lotes como ejemplo.

Las configuraciones para estos se pueden encontrar en**Modo de sitio**y**modo de dispositivo**. Las operaciones para estos dos modos son similares. Esta sección utiliza configuraciones en**modo de dispositivo**como ejemplo. Paso 1

Sobre el**Hogar**pantalla, toque , y luego va a**Sitios**pantalla.

Paso 2 Toque en la esquina superior izquierda para cambiar a**modo de dispositivo**.

Paso 3 Grifo .

Etapa 4 Seleccione los dispositivos que desea verificar y luego toque**X dispositivos seleccionados. Iniciar comprobación de estado**.

Para seleccionar todos los dispositivos, toque**Seleccionar todo**.

Paso 5 Vea los resultados de la verificación y luego toque**DE ACUERDO**.

Los dispositivos sin conexión no se pueden comprobar.

4.6.2 Configuraciones básicas del dispositivo

Después de agregar dispositivos, incluido el concentrador de alarmas y los accesorios, puede ver y editar la información general del dispositivo.

Paso 1 Sobre el**Hogar**pantalla, toque , y luego va a**Sitios**pantalla. Toque en la esquina

Paso 2 superior izquierda para cambiar a**modo de dispositivo**. En la lista de dispositivos,

Paso 3 seleccione el dispositivo según sea necesario.

Etapa 4 En la pantalla del concentrador, toque para ver y editar información general en el dispositivo.

Tabla 4-1 Descripción de parámetros

Parámetro	Descripción
Configuración del dispositivo	● Ver el nombre, el tipo y el SN del dispositivo. ● Edite el nombre del dispositivo y luego toque**Ahorrar**para guardar la configuración.
Estado del concentrador	Para obtener más información, consulte "4.6.2.2 Configuración del concentrador".
Configuración del concentrador	Para obtener más información, consulte "4.6.2.1 Visualización del estado".
Zona horaria	Grifo**Zona horaria**para seleccionar su zona horaria y habilite DST (horario de verano) si es necesario. ● **Zona horaria**: Seleccione la zona horaria en la que opera el concentrador. ● **horario de verano**: seleccione la fecha o la semana y, a continuación, seleccione la hora de inicio y la hora de finalización.
configuración de la red	Grifo**configuración de la red**para ver la información de su red actual.

Parámetro	Descripción
Uso compartido de dispositivos	Grifo**Uso compartido de dispositivos**para compartir el estado del concentrador con los demás usuarios. Para obtener más información, consulte "4.3.1.1 Préstamo del dispositivo a los usuarios administradores de DMSS".
Actualización en la nube	Actualizar en línea. La actualización no está permitida cuando el concentrador está en estado armado o el nivel de la batería es bajo.
Registro	Registros de dispositivos y aplicaciones. ● Registro del dispositivo: Seleccionar**Registro**>**registro del dispositivo**para ver los registros de alarmas del dispositivo. También puede tocar en el**registro del dispositivo**pantalla para enviar registros de alarma al correo electrónico vinculado. ● Registro de la aplicación: Seleccionar**Registro**>**registro de la aplicación**para ver los registros de alarmas del COS Pro. También puedes tocar sobre el**registro de la aplicación**pantalla para enviar registros de alarmas a el correo electrónico vinculado.

4.6.2.1 Estado de visualización

Sobre el**Centro**pantalla, seleccione > **Estado del concentrador**para ver el estado del concentrador.

Tabla 4-2 Estado

Parámetro	Descripción
Intensidad de la señal GSM	La intensidad de la señal de la red móvil para la tarjeta SIM activa. ● : Ultra bajo. ● : Bajo. ● : Moderado. ● : Alto. ● : No.
Intensidad de la señal Wi-Fi	Estado de la conexión a Internet del concentrador a través de Wi-Fi. Para una mayor confiabilidad, recomendamos instalar el concentrador en lugares con una intensidad de señal de al menos 2 barras. ● : Ultra bajo. ● : Bajo. ● : Moderado. ● : Alto. ● : No.
Almacenamiento de batería	Muestra la electricidad restante de la batería. ● : Completamente cargado. ● : Suficiente. ● : Moderado. ● : Insuficiente.
Antimanipulación	El modo de manipulación del accesorio, que reacciona al desprendimiento del cuerpo.
Estado de alimentación principal	Muestra el estado de la alimentación principal.

Parámetro	Descripción
Estado de conexión GSM	Estado de la conexión a Internet del concentrador a través de la tarjeta SIM, Wi-Fi y Ethernet. ● : Conectado. ● : Desconectado.
Estado de la conexión wifi	
Estado de conexión del cable de red	
Estado de la tarjeta SIM	Estado de conexión de la tarjeta SIM. ● : la tarjeta SIM 1 está activa. ● : la tarjeta SIM 2 está activa. ● : Sin tarjeta SIM.
Versión del programa	La versión del programa del concentrador.

4.6.2.2 Configuración del concentrador

Sobre el**Centro**pantalla, seleccione > **Configuración del concentrador**para configurar los parámetros del concentrador.

Tabla 4-3 Descripción de los parámetros del concentrador

Parámetro	Descripción
Global Armar/Desarmar	Arma o desarma todos los detectores en todas las áreas con un solo toque.
Cronograma Armar/Desarmar	Armar o desarmar las áreas por horario. ● **Área**: Seleccione el área en la que opera el concentrador. ● **Configuración de comandos**: Seleccione un modo armado según sea necesario tocando **Hogar**,**Lejos**, o**Desarmar**. ● **Tiempo**: Seleccione el período de tiempo en el que opera el concentrador. ● **Repetir**: Copie el horario de armado o desarmado. ● **Armado forzado**: Puede armar el sistema cuando ocurren errores en las zonas.
Configuración de tono de llamada	El tono de llamada al entrar o salir del modo de armado.
Indicador LED	**Indicador LED**está habilitado de forma predeterminada. Para obtener detalles sobre el comportamiento del indicador, consulte "2.1 Apariencia". ● Si**Indicador LED**está deshabilitado, el indicador LED permanecerá apagado independientemente de si el concentrador está funcionando normalmente o no. ● La función solo está disponible cuando la versión de la aplicación DMSS es 1.96 o posterior, y el concentrador es V1.001.0000000.4.R.211014 o posterior.
Modo de prueba	Grifo**Comenzar**para probar el estado de los accesorios que se conectan al concentrador en diferentes áreas, y luego toque**Detener**para completar la detección.
Sensibilidad reducida Modo	Permitir**Modo de sensibilidad reducida**, y luego se reducirá la potencia de transmisión del concentrador. La función solo está disponible cuando la versión de la aplicación DMSS es 1.97 o posterior, y el concentrador es V1.001.0000000.6.R.211215 o posterior.

Parámetro	Descripción
Servicio de almacenamiento en la nube Conexión	Establezca el intervalo de ping del concentrador del servidor con un rango de 150 a 900 segundos (150 segundos de forma predeterminada). Si D-cloud detecta que la duración fuera de línea del concentrador supera los 150 segundos, informará el estado del concentrador al usuario a través de la aplicación. La función solo está disponible cuando la versión de la aplicación DMSS es 1.96 o posterior, y el concentrador es V1.001.0000000.6.R.211215 o posterior.
Latido del corazón	Configure el intervalo de ping del concentrador-detector. La configuración determina la frecuencia con la que el concentrador se comunica con los accesorios y la rapidez con la que se detecta la pérdida de conexión. ● **Intervalo de ping del detector**: La frecuencia de los accesorios conectados operados por el concentrador está configurada 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 no entregados para determinar fallas en la conexión**: Se configura un contador de paquetes no entregados en el rango de 3 a 60 (15 paquetes por defecto). ◇ Cuanto menor sea el número, con mayor frecuencia el estado sin conexión de accesorios es detectado e informado. ◇ Si el concentrador pierde constantemente la conexión con los accesorios y no puede detectar sus latidos definidos, informará su estado fuera de línea al sistema.
Antimanipulación Vocero	Alerta con sirena si la tapa trasera de accesorios y hub está abierta.
Integridad del sistema Controlar	Cuando está habilitado, el concentrador verifica el estado de todos los detectores antes de armarlos, como el nivel de carga de la batería, los incidentes de manipulación y la conectividad. Si se detectan errores, se mostrarán advertencias. ● Para el llavero, el indicador parpadea en verde y luego se vuelve rojo. ● Para la aplicación, aparece un mensaje de alarma. ● Para el teclado, suena durante 1 segundo, el armado y desarmado El indicador parpadea en verde durante 2 segundos y luego cambia a la estado normal
CMS	Ingrese la dirección IP, el puerto y la ID del dispositivo, y luego puede registrar el concentrador en D-cloud. La función solo está disponible cuando la versión de la aplicación DMSS es 1.96 o posterior, y el concentrador es V1.001.0000000.6.R.211215 o posterior.

Parámetro	Descripción
Estación de monitoreo	Permitir**Estación de monitoreo**y luego configure los parámetros del protocolo SIA para el centro de recepción de alarmas (CRA). ● **Dirección IP preferida**: Ingrese la dirección IP y el número de puerto del CRA. ● **Dirección IP alternativa**: Ingrese la dirección IP alternativa y el número de puerto del CRA. ◇ Los mensajes se enviarán a la dirección IP alternativa solo cuando la dirección IP preferida no recibe el mensaje. ◇ Si**Intervalo de latido**está habilitado, el sistema decidirá si enviar el mensaje a la dirección IP preferida o alternativa. ● **Protocolo IP**: Seleccionar**TCP**por defecto. ● **Intervalo de latido**: establezca el intervalo de latidos del corazón con un rango de 0 segundos a 24 horas (60 segundos de forma predeterminada). 0 segundos significa**Intervalo de latido**está desactivado. ● **cuenta central**: Ingrese el número de cuenta que creó el CRA, que se utilizará para identificar el concentrador cuando el concentrador envíe información al CRA. ● **Cifrado**: El concentrador utiliza un formato de cifrado para la seguridad de la información cuando configura el CRA.**AES128**está configurado de forma predeterminada. ● **Subir evento**: Grifo junto a un evento para cargarlo. ◇ **Alarma**: Mensaje de alarma. ◇ **Error**: falla de energía, bajo voltaje de la batería, manipulación y fuera de línea. ◇ **Evento**: prohibir el uso de periféricos, agregar o eliminar periféricos y agregar o eliminar usuarios. ◇ **Armar/Desarmar**: Notificaciones de mensajes de armado y desarmado del sistema.

4.6.3 Corrección de errores

Puede corregir errores después de verificar los dispositivos anormales. Los errores se encuentran de dos maneras, incluido el informe automático del dispositivo y la verificación manual.

Paso 1 Sobre el**Hogar**pantalla, seleccione**Tarea pendiente**>**Corrección de errores**. En la

Paso 2 lista de errores, toque una tarea de error y luego toque**Empezar a procesar**.

Paso 3 Solucione el error de acuerdo con las sugerencias.

Etapa 4 Grifo**Error arreglado**si el error está solucionado, y luego esperar a que el cliente lo confirme.

Los clientes serán notificados del estado de corrección de errores. Si confirman que el error ha arreglado, se les pedirá que evalúen el servicio.

4.6.4 Visualización de evaluaciones

Después de configurar los dispositivos de forma remota y corregir los errores, los clientes evaluarán cómo los operadores se desempeñaron en la reparación de errores y el mantenimiento de la salud del dispositivo. La cuenta de administrador puede ver detalles sobre errores como el tipo de error, la hora en que ocurrió el error, sugerencias y operación, el nombre del operador y calificaciones.

Paso 1 En pantalla, toque**Notificación de errores**.

Paso 2 En la lista de mensajes, toque un mensaje para ver los detalles del mensaje, incluido el nombre de usuario del cliente, el nombre de usuario del operador, los detalles del dispositivo, los detalles del error, los detalles de la corrección del error y la calificación.

5 Operaciones de DMSS para usuarios finales

La aplicación DMSS brinda servicios profesionales de vigilancia de seguridad para usuarios finales. Para los usuarios administradores de DMSS, puede compartir el concentrador con hasta 6 usuarios generales de DMSS y confiarlo a una empresa. Los accesorios que vienen con el concentrador se pueden compartir y confiar al mismo tiempo. Para compartir y confiar el centro usted mismo, debe instalar la última versión de la aplicación DMSS.

Las cifras son solo de referencia y pueden diferir de la interfaz real.

5.1 Iniciar sesión en DMSS

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

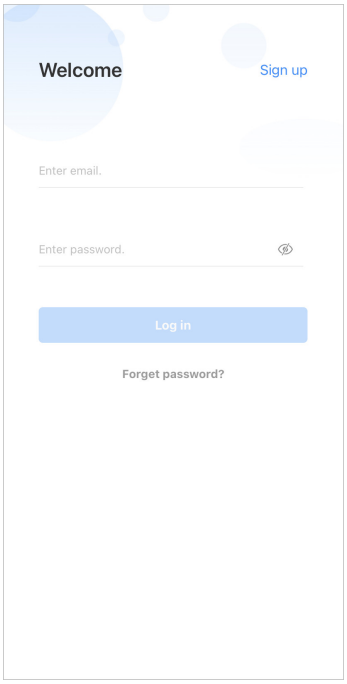
Asegúrate de haber instalado la última versión de la aplicación.

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

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

Paso 2 En su teléfono, toque para iniciar la aplicación.

Figura 5-1 Inicio de sesión



Paso 3 Crea una cuenta.

1) En el**Acceso**pantalla, toque**Inscribirse**.

2) Introduzca su dirección de correo electrónico y contraseña.

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

3) Leer el**Acuerdo del Usuario**y**política de privacidad**y, a continuación, seleccione el**He leído y acepto**caja.

4) Toca**Obtener código de verificación**, busque en su casilla de correo electrónico el código de verificación y, a continuación, introdúzcalo.

Use el código de verificación dentro de los 60 segundos de haberlo recibido. De lo contrario, el código de verificación dejará de ser válido.

5) Toca**DE ACUERDO**.

Etapa 4 Sobre el**Acceso**pantalla, ingrese su correo electrónico y contraseña, y luego toque**Acceso**.

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

5.2 Adición de dispositivos

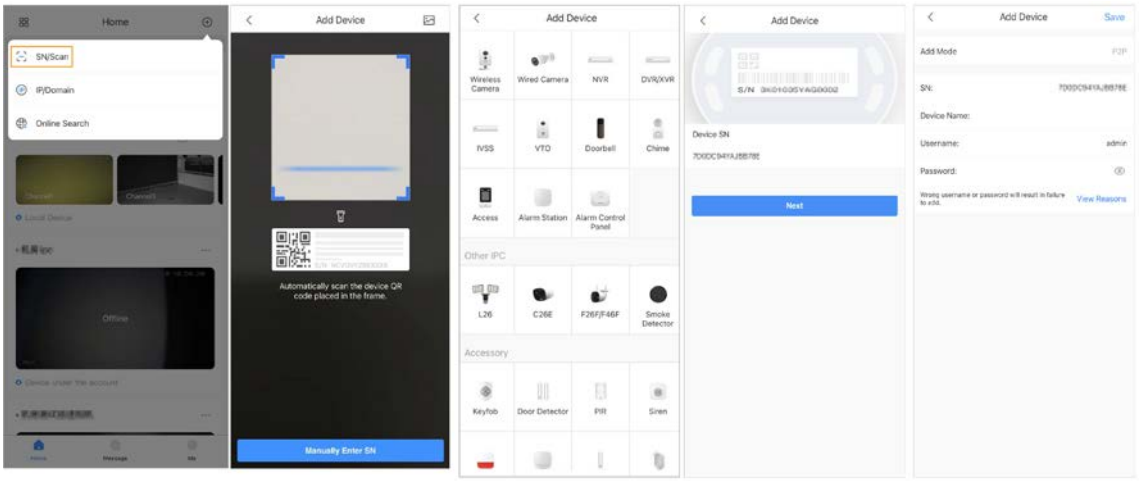
Para los usuarios finales, puede agregar dispositivos de alarma a la aplicación DMSS.

5.2.1 Agregar el concentrador

Puede agregar el concentrador ingresando manualmente el SN del dispositivo y escaneando el código QR. Paso 1

Sobre el**Hogar**pantalla, toque y luego seleccione**NS/escaneo**.

Figura 5-2 Agregar por código SN/QR



Paso 2 Agrega 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 manualmente el NS**y luego ingrese el SN del dispositivo para agregar manualmente un dispositivo.

Paso 3 Seleccione el tipo de dispositivo y luego toque**Próximo**.

Grifo**Próximo**si el sistema identifica el tipo de dispositivo automáticamente.

Etapa 4 Sobre el**Añadir dispositivo**pantalla, personalice el nombre del dispositivo, ingrese el nombre de usuario y la contraseña del dispositivo, y luego toque**Ahorrar**.

5.2.2 Adición de accesorios

Para los usuarios finales, puede agregar múltiples accesorios al hub. Las operaciones para agregar accesorios en DMSS son las mismas que en COS Pro. Para obtener más información, consulte "4.2.2 Adición de accesorios".

5.3 Configuración general del concentrador

5.3.1 Configuración del concentrador

Sobre el**Detalles del dispositivo**pantalla, toque , y luego puede ver y editar la información general del centro. La información general del dispositivo que se muestra en la aplicación DMSS es la misma que en la aplicación COS Pro. Para obtener más información, consulte "4.6.2 Configuraciones básicas del dispositivo".

5.3.2 Configuración de red

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

5.3.2.1 Configuración de red cableada

Paso 1 Seleccionar**Configuración de la red**>**Configuración de red cableada**

Paso 2 . Configure los parámetros de conexión de la red cableada.

Tabla 5-1 Descripción de los parámetros de la red cableada

Parámetro	Descripción
DHCP	Cuando hay un servidor DHCP en la red, puede habilitar **DHCP**, y luego el concentrador obtiene la dirección IP dinámica automáticamente.
Dirección IP	Configure la dirección IP manualmente: Configure la dirección IP, la máscara de subred, la puerta de enlace predeterminada y el DNS manualmente para el concentrador.
Máscara de subred	
Centro de alarmas	
DNS	
DNS 2	

5.3.2.2 Configuración de la red Wi-Fi

Paso 1 Seleccionar**Configuración de la red**>**Configuración de la red wifi**.

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

5.3.2.3 Configuración celular

Paso 1 Seleccionar**Configuración de la red**>**Celular**.

Paso 2 Configurar parámetros celulares.

Tabla 5-2 Descripción de los parámetros celulares

Parámetro	Descripción
Celular	Grifo al lado de**Celular**para habilitar el celular.
Prioridad	Grifo al lado de**Prioridad**para establecer el celular como la prioridad al seleccionar la red.
tarjeta SIM 1	• Admite tarjetas SIM duales y modo de espera único. • Las tarjetas SIM permiten que el concentrador use datos móviles 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 proveedor y la Internet pública.
Modo de autenticación	Modo de autenticación de la red celular.
Nombre de usuario	El nombre de usuario y la contraseña de la red celular.
Contraseña	
Marque el número	El número al que debe llamar el concentrador.
Uso de datos móviles	Ver el uso de los datos móviles.
Reiniciar las estadísticas	Restablezca el uso de datos móviles para reiniciar el conteo.

5.4 Gestión de usuarios

5.4.1 Adición de usuarios

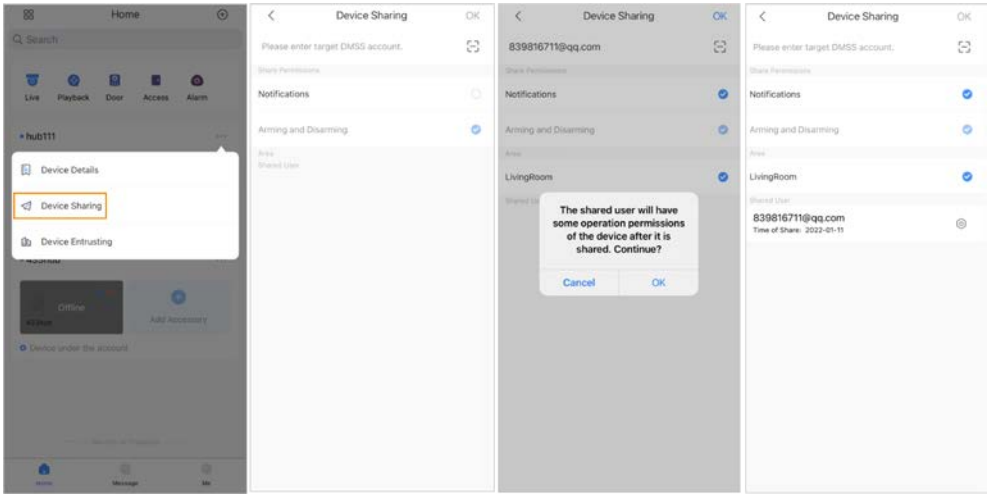
Para los usuarios administradores de DMSS, puede agregar instaladores y usuarios generales de DMSS.

5.4.1.1 Adición de usuarios generales de DMSS

Puede compartir dispositivos con hasta 6 usuarios generales de DMSS. Puedes ir a > **Detalles del dispositivo**> , o > **Detalles del dispositivo**>**Uso compartido de dispositivos**para compartir el dispositivo. Estos métodos son similares. Esta sección utiliza dispositivos compartidos > **Uso compartido de dispositivos** como ejemplo.

Paso 1 Sobre el**Hogar**pantalla, toque junto a un dispositivo y luego toque**Uso compartido de dispositivos**.

Figura 5-3 Compartir dispositivo



Paso 2 Sobre el**Uso compartido de dispositivos**pantalla, comparta el dispositivo con el usuario ingresando su cuenta DMSS o escaneando su código QR.

Paso 3 Seleccione los permisos del dispositivo para los usuarios en función de su necesidad real. Grifo**DE**

Etapa 4 **ACUERDO**.

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

5.4.1.2 Adición de instaladores

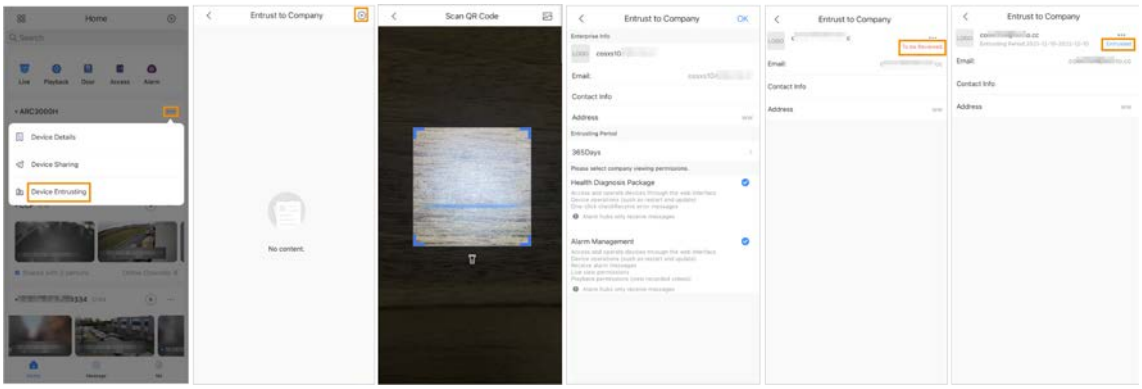
Para los usuarios administradores de DMSS, puede agregar instaladores confiándoles dispositivos. Puede confiar los dispositivos al instalador uno por uno o en lotes.

5.4.1.2.1 Dispositivo de confianza uno por uno

Procedimiento

Paso 1 Sobre el**Hogar**pantalla, toque ••• junto a un dispositivo y luego toque**Confiar dispositivo**.

Figura 5-4 Confiar un dispositivo



Paso 2 Sobre el**Encomendar a la empresa**pantalla, toque ⊕ , y luego escanee el código QR correspondiente de el instalador, o toque e importe la imagen del código QR para confiar el dispositivo al instalador.

Puede solicitar a los instaladores sus códigos QR.

Paso 3 Sobre el**Encomendar a la empresa**pantalla, seleccione los períodos de confianza y los permisos de visualización de la empresa, y luego toque**DE ACUERDO**.

- Debe seleccionar al menos un permiso de visualización de**Paquete de Diagnóstico de Salud**y **Gestión de alarmas**.
- La información de la empresa se reconocerá automáticamente después de escanear el código QR de el instalador

Etapa 4 Ver detalles de encomienda en el**Encomendar a la empresa**pantalla.

Cuando se encomienda con éxito,**Para ser revisado**cambiará a**Entregado**.

Después de que se haya enviado con éxito una solicitud de confianza, aparecerá un mensaje en la**Hogar** pantalla. Debe esperar una respuesta del instalador, que se mostrará en la **A mí**>**Buzón**>**Personal**pantalla.

Operaciones relacionadas

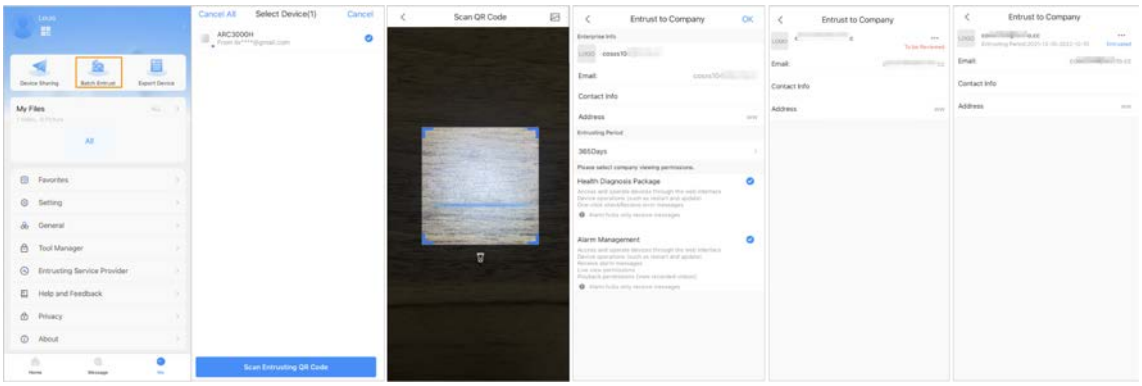
- Para cambiar los permisos, vaya a la**Encomendar a la empresa**pantalla y luego toque **Cambiar permisos**.
- Para retirar los permisos de encomienda, vaya a la**Encomendar a la empresa**pantalla y luego toque **Retirar**.
- Para renovar los periodos de encomienda, vaya a la**Encomendar a la empresa**pantalla y luego toque**Renovar**.

5.4.1.2.2 Confiar dispositivos en lotes

Puede confiar dispositivos a una empresa en lotes.

Paso 1 Sobre el**Hogar**pantalla, seleccione**A mí**>**Encomienda por lotes**.

Figura 5-5 Confiar dispositivos en lotes



Paso 2 Sobre el**Seleccione el dispositivo**pantalla, seleccione los dispositivos a confiar y luego confíelos a la empresa. El proceso para confiar varios dispositivos es el mismo que confiar un solo dispositivo. Para obtener más información, consulte "5.4.1.2.1 Dispositivo de confianza uno por uno".

5.4.2 Eliminación de usuarios

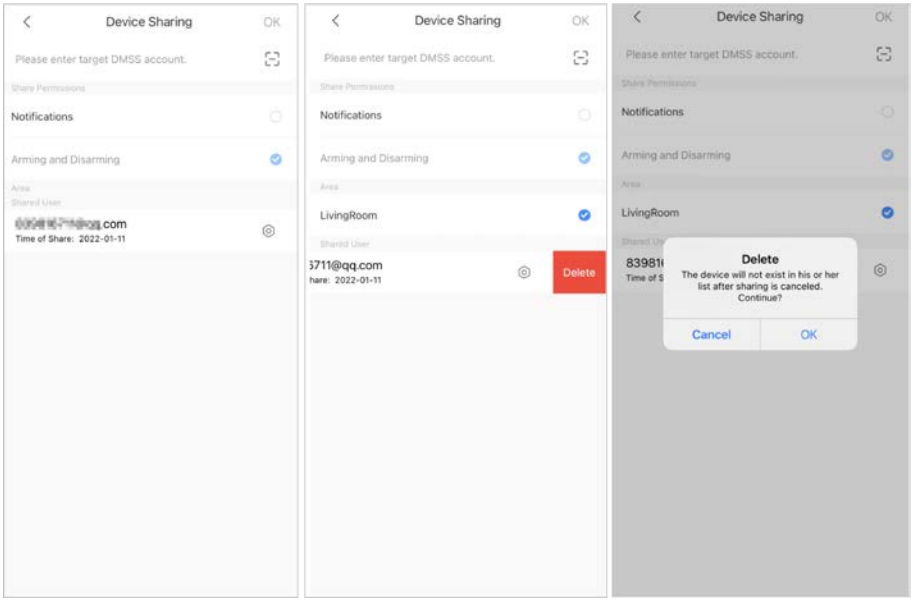
Para los usuarios administradores de DMSS, puede eliminar tanto los instaladores como los usuarios generales de DMSS.

5.4.2.1 Cancelación para compartir los dispositivos

Para el usuario administrador de DMSS, puede eliminar los usuarios generales de DMSS cancelando para compartir los dispositivos con ellos en el**Uso compartido de dispositivos**pantalla. Para obtener detalles sobre cómo ir a**Uso compartido de dispositivos**pantalla, consulte "5.4.1.1 Adición de usuarios generales de DMSS". Esta sección utiliza métodos en > **Uso compartido de dispositivos**como un ejemplo.

Paso 1 Sobre el**Hogar**pantalla, toque junto a un dispositivo y luego toque**Uso compartido de dispositivos**.

Figura 5-6 Compartir dispositivo



Paso 2 En la lista de cuentas del**Uso compartido de dispositivos**pantalla, seleccione una cuenta, deslice el bloque hacia la izquierda y luego toque**Borrar**. Grifo**DE ACUERDO**para cancelar el uso compartido.

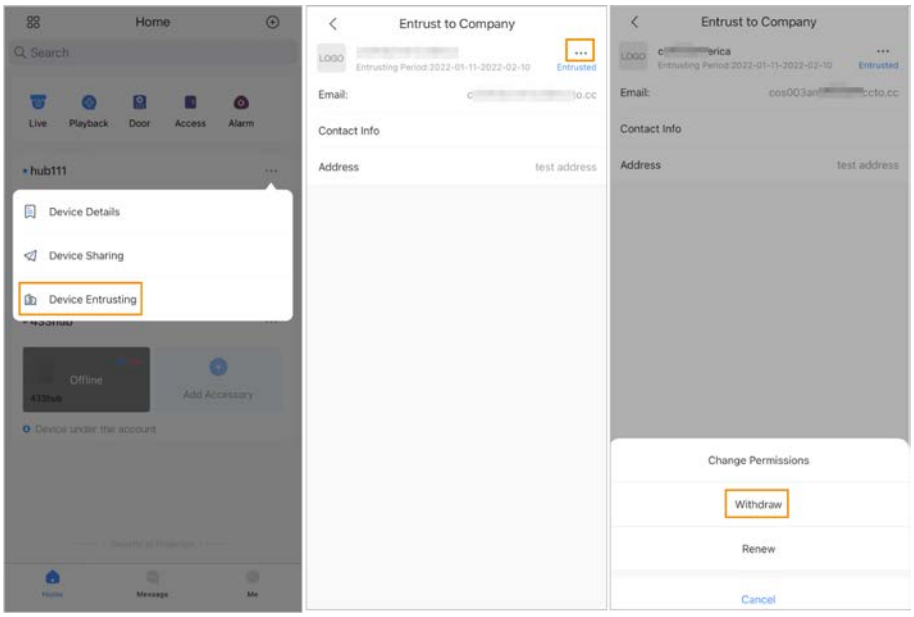
Paso 3

5.4.2.2 Cancelación de la Solicitud de Encomienda

Para los usuarios administradores de DMSS, puede eliminar un instalador cancelando la aplicación de confianza. Paso 1

Sobre el**Hogar**pantalla, toque junto a un dispositivo y luego toque**Confiar dispositivo**.

Figura 5-7 Retirar solicitud de confianza



Paso 2 Sobre el**Confiar dispositivo**pantalla, seleccione > **Retirar**y luego toque**DE ACUERDO**.

Se enviará un mensaje a la cuenta del instalador. Después de que el instalador lea el mensaje y aprueba su solicitud para cancelar la solicitud de encomienda en COS Pro, su la solicitud será cancelada.

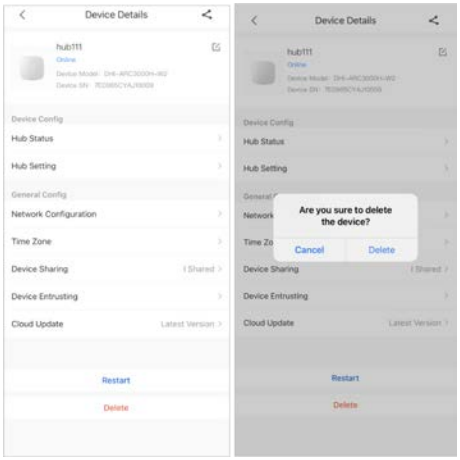
5.4.2.3 Eliminación de dispositivos

Para el usuario administrador de DMSS, puede eliminar tanto los instaladores como los usuarios generales de DMSS eliminando dispositivos.

El usuario administrador de DMSS no puede eliminar un instalador si el instalador comparte los dispositivos.

Paso 1 Sobre el**Hogar**pantalla, seleccione > **Detalles del dispositivo**.

Figura 5-8 Eliminar el dispositivo



Paso 2 Sobre el**Detalles del dispositivo**pantalla, toque**Borrar**.

Paso 3 Grifo**Borrar**para eliminar los dispositivos.

6 Operaciones Generales

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

requisitos previos

- 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 contexto

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

Procedimiento

Paso 1 En la pantalla central, toque**Accesorio**para agregar los accesorios. Para obtener detalles sobre cómo agregar los accesorios, consulte el manual del usuario del dispositivo correspondiente.

Paso 2 Armar y desarmar los detectores en una sola área o en todas las áreas mediante operaciones manuales o programadas.

- Armado y Desarmado Único: Armar y desarmar los detectores en una sola área. Para obtener más información, consulte "6.1 Armado y desarmado sencillos".
- Armado y Desarmado Global: Arma y desarma los detectores en todas las áreas. Para obtener más información, consulte "6.2 Armado y desarmado global".
- Armado y desarmado manual: Armar el sistema de seguridad a través de la aplicación DMSS, teclado o llavero.
- Programar Armado y Desarmado: Armar y desarmar los detectores por horario. Para obtener más información, consulte "6.4 Armado y desarmado programados".

6.1 Armado y desarmado individual

Puede armar y desarmar los detectores en una sola área.

Paso 1 En la pantalla central, toque**Área**.

Paso 2 Toque un área y luego seleccione entre**Hogar**,**Lejos**,**Desarmar**, y**Desactivar**en la ventana emergente.

- **Hogar**: Un modo de armado que le permite armar el sistema cuando está dentro del área del sistema de alarma.
- **Lejos**: Arme el sistema cuando abandone el área del sistema de alarma.
- **Desarmar**: Apague el sistema de seguridad. Lo contrario de armar.
- **Desactivar**: Cierra la pantalla actual.

6.2 Armado y Desarmado Global

requisitos previos

Asegúrese de haber habilitado el**Armado/Desarmado Global**función. En la pantalla del concentrador, seleccione > **Configuración del concentrador**y luego habilite**Armado/Desarmado Global**.

Información de contexto

Puede armar y desarmar los detectores en todas las áreas.

Procedimiento

Paso 1 Vaya a la pantalla del concentrador.

Paso 2 Seleccionar de**Hogar**,**Lejos**, y**Desarmar**en la pantalla superior.

6.3 Armado y Desarmado Manual

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

- Para armar y desarmar los detectores en una sola área o en todas las áreas, consulte "6.1 Armado y Desarmado Único" y "6.2 Armado y Desarmado Global".
- Para operar a través del llavero y el teclado, primero debe asignar los permisos de control de las áreas al llavero y al teclado. Para obtener más información, consulte el manual del usuario del mando a distancia y el teclado correspondientes.

6.4 Armado y Desarmado Programado

Puede establecer un horario para armar y desarmar los detectores. Puede configurar planes de armado, incluido el área de armado, los modos y los períodos.

Paso 1 En la pantalla del concentrador, seleccione > **Configuración del concentrador**>**Armado/Desarmado Programado**.

Paso 2 Sobre el**Armado/Desarmado Programado**pantalla, toque**Agregar**y luego configure los planes de armado.

- **Nombre**: personalice un nombre para los planes de armado.
- **Área**: seleccione una o varias áreas que desee armar.
- **Configuración de comandos**: Seleccionar de**Hogar**,**Lejos**, y**Desarmar**.
- **Tiempo**: Configure un tiempo de armado.

  Para aplicar el tiempo de armado a otros días, toque**Repetir**y seleccione los días que desee.
- **Armado Forzado**: Seleccione según sea necesario.

Apéndice 1 Eventos de falla de armado y Descripción

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

No.	Razón	Descripción
1	Pérdida de módulo	El accesorio estaba fuera de línea.
2	Error del 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	exAbierto	La tapa trasera del dispositivo externo estaba abierta.
6	Manosear	Se activó la alarma de manipulación de accesorios.
7	Batería baja	Se detectó batería baja del dispositivo.
8	PriPowerLoss	Se detectó una falla de energía principal accesoria.
9	Pérdida de batería	Se detectó una falla en la batería.
10	Sobretensión	Se detectó sobretensión.
11	sobrecorriente	Se detectó sobrecorriente.
12	Sobrecalentar	Se detectó sobrecalentamiento.
13	Alarma de incendios	Se activó la alarma de incendio.
14	MédicoAlarma	Se disparó la alarma médica.
15	Alarma SOSA	Se activó la alarma SOS.
dieciséis	alarma de pánico	Se activó la alarma de pánico.
17	Alarma de gas	Se disparó la alarma de fuga de gas.
18	Alarma de intrusión	Se disparó 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 (concentrador)

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 alarmas.
3	Error de conexión del servidor	El concentrador 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 de alimentación principal.
7	Pérdida de batería	Se detectó una falla en la batería.

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

Apéndice 2 Códigos de eventos SIA y descripción

Apéndice Tabla 2-1 Códigos de eventos SIA y descripción

No.	Evento	Código CID	Descripción
1	Alarma de movimiento	130 133 134	130: Alarma de robo. 133: alarma de 24 horas (caja fuerte). 134: Alarma de Entrada/Salida.
2	Alarma detectora de puerta Restaurar	130 133 134	130: Alarma de robo. 133: alarma de 24 horas (caja fuerte). 134: Alarma de Entrada/Salida.
3	Alarma de entrada externa Restaurar	130 133 134	130: Alarma de robo. 133: alarma de 24 horas (caja fuerte). 134: Alarma de Entrada/Salida.
4	alarma de coacción	121	Alarma de coacción.
5	Alarma SOS	120	Alarma de pánico.
6	Alarma de intrusión	130 133 134	130: Alarma de robo. 133: alarma de 24 horas (caja fuerte). 134: Alarma de Entrada/Salida.
7	Alarma de incendios	110	Alarma de incendios.
8	Alarma de fuga de gas	151	Alarma de gas detectado.
9	alarma medica	100	Alarma Médica.
10	Alarma de atraco	120	Alarma de pánico.
11	Manipulación del controlador Resuelto	137	Manosear.
12	Manipulación de periféricos Resuelto	383	Manipulación de sensores.
13	Dispositivo externo Manipulación resuelta	383	Manipulación de sensores.
14	Voltaje de la batería restaurado	302	Batería baja del sistema.
15	Recuperación de fallas de batería	311	Batería faltante/muerta.
dieciséis	Energía restaurada	301	Pérdida de CA.
17	Interferencia de RF	344	Detección de atascos en el receptor de RF.
18	Transmisión de alarma Fallo del sistema restaurado	350	Problema de comunicación.
19	Transmisión de alarma Fallo de ruta Errores restaurados/Wi-Fi Recuperación	350	Problema de comunicación.

No.	Evento	Código CID	Descripción
20	Transmisión de alarma Fallo de ruta Restaurado/Inalámbrico Errores de red Recuperación	350	Problema de comunicación.
21	Periférico No Conectado Restaurado	381	Pérdida de supervisión - RF.
22	Periférico Bajo Alarma de batería Recuperación	302	Batería baja del sistema.
23	Batería periférica Recuperación de fallas	311	Batería faltante/muerta.
24	Periférico Principal Fallo de alimentación restaurado	301	Pérdida de CA.
25	Fallo de RF-HD restaurado	354	Evento de falta de comunicación.
26	Dispositivo bloqueado y desbloqueado	501	Acceder al lector deshabilitado.
27	Sobretensión Protección restaurada	319	Sobretensión de la fuente de alimentación.
28	sobrecorriente Protección restaurada	312	Sobrecorriente de la fuente de alimentación.
29	Protección contra el sobrecalentamiento restaurado	318	Sobrecalentamiento de la fuente de alimentación.
30	Alta temperatura Alarma restaurada	158	Alta temperatura.
31	Baja temperatura Alarma restaurada	159	Baja temperatura.
32	Brazo	400 (aplicación) 401 (teclado) 403 (Programado armamento) 407 (mando a distancia) 408 (armado global)	400: Abrir/Cerrar. 401: O/C por usuario. 403: A/C automático. 407: Armado/desarmado remoto. 408: Armado rápido.
33	Desarmar	400 (aplicación) 401 (teclado) 403 (Programado armamento) 407 (mando a distancia) 408 (Sin contraseña armamento)	400 Abrir/Cerrar. 401 O/C por usuario. 403 A/C automático. 407 Armado/desarmado remoto. 408 Armado rápido.
34	Armado en casa	441	ESTANCIA armada.

No.	Evento	Código CID	Descripción
35	Fallo de armado	454 (fallo de armado) 455 (Programado falla de armado) 457 (Retardo de salida falla de armado)	454 Error al cerrar. 455 Autoarmado fallido. 457 Error de salida (usuario).
36	Armado Forzado	450	Excepción O/C.
37	Deshabilitar periférico Recuperación	502	Temporalmente desactivado.
38	Solo deshabilitar sabotaje Recuperación de alarma	503	Desactivado temporalmente.
39	Informe de prueba manual	601	Informe de prueba de disparo manual.

Apéndice 3 Recomendaciones sobre ciberseguridad

La ciberseguridad es más que una palabra de moda: es algo que pertenece a todos los dispositivos que están conectados a Internet. La videovigilancia IP no es inmune a los riesgos cibernéticos, pero tomar medidas básicas para proteger y fortalecer las redes y los dispositivos en red los hará menos susceptibles a los ataques. A continuación se presentan algunos consejos y recomendaciones de Dahua sobre cómo crear un sistema de seguridad más seguro.

Acciones obligatorias que se deben tomar para la seguridad básica de la red del dispositivo:

1.**Utilice contraseñas seguras**

Consulte las siguientes sugerencias para establecer contraseñas:

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

2.**Actualice el firmware y el software del cliente a tiempo**

- De acuerdo con el procedimiento estándar en la industria tecnológica, recomendamos mantener actualizado el firmware de su dispositivo (como NVR, DVR, cámara IP, etc.) para garantizar que el sistema esté equipado con los últimos parches y correcciones de seguridad. Cuando el dispositivo está conectado a la red pública, se recomienda habilitar la función de "comprobación automática de actualizaciones" para obtener información oportuna de las actualizaciones de firmware lanzadas por el fabricante.
- Le sugerimos que descargue y utilice la última versión del software del cliente.

Recomendaciones "agradables de tener" para mejorar la seguridad de la red de su dispositivo:

1.Protección Física

Le sugerimos que realice una protección física al dispositivo, especialmente a los dispositivos de almacenamiento. Por ejemplo, coloque el dispositivo en un gabinete y una sala de computadoras especiales, e implemente un control de permisos de acceso y administración de claves bien hecho para evitar que el personal no autorizado realice contactos físicos, como dañar el hardware, la conexión no autorizada de un dispositivo extraíble (como un disco flash USB). , puerto serie), etc.

2.**Cambie las contraseñas regularmente**

Le sugerimos que cambie las contraseñas regularmente para reducir el riesgo de ser adivinadas o descifradas.

3.**Establecer y actualizar contraseñas Restablecer información a tiempo**

El dispositivo admite la función de restablecimiento de contraseña. Configure la información relacionada para restablecer la contraseña a tiempo, incluido el buzón del usuario final y las preguntas de protección de contraseña. Si la información cambia, modifíquela a tiempo. Al establecer preguntas de protección de contraseña, se sugiere no utilizar aquellas que se pueden adivinar fácilmente.

4.**Habilitar bloqueo de cuenta**

La función de bloqueo de cuenta está habilitada de forma predeterminada y le recomendamos que la mantenga activada para garantizar la seguridad de la cuenta. Si un atacante intenta iniciar sesión varias veces con la contraseña incorrecta, la cuenta correspondiente y la dirección IP de origen se bloquearán.

5.**Cambiar HTTP predeterminado y otros puertos de servicio**

Le sugerimos que cambie el HTTP predeterminado y otros puertos de servicio a cualquier conjunto de números entre

1024–65535, lo que reduce el riesgo de que personas externas puedan adivinar qué puertos está utilizando.

6.**Habilitar HTTPS**

Le sugerimos que habilite HTTPS, para que visite el servicio web a través de un canal de comunicación seguro.

7.**Enlace de dirección MAC**

Le recomendamos vincular la dirección IP y MAC de la puerta de enlace al dispositivo, reduciendo así el riesgo de suplantación de identidad ARP.

8.**Asigne cuentas y privilegios de manera razonable**

De acuerdo con los requisitos comerciales y de gestión, agregue usuarios razonablemente y asígneles un conjunto mínimo de permisos.

9.**Deshabilite los servicios innecesarios y elija modos seguros**

Si no es necesario, se recomienda desactivar algunos servicios como SNMP, SMTP, UPnP, etc., para reducir los riesgos.

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

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

10**Transmisión encriptada de audio y video**

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

Recordatorio: la transmisión encriptada causará cierta pérdida en la eficiencia de la transmisión.

11**Auditoría segura**

- Verifique a los usuarios en línea: le sugerimos que verifique a los usuarios en línea regularmente para ver si el dispositivo está conectado sin autorización.
- Verifique el registro del dispositivo: al ver los registros, puede conocer las direcciones IP que se usaron para iniciar sesión en sus dispositivos y sus operaciones clave.

12**Registro de red**

Debido a la capacidad de almacenamiento limitada del dispositivo, el registro almacenado es limitado. Si necesita guardar el registro durante mucho tiempo, se recomienda habilitar la función de registro de red para asegurarse de que los registros críticos se sincronizan con el servidor de registro de red para su seguimiento.

13**Construir un entorno de red seguro**

Para garantizar mejor la seguridad del dispositivo y reducir los posibles riesgos cibernéticos, recomendamos:

- Deshabilite la función de mapeo de puertos del enrutador para evitar el acceso directo a los dispositivos de intranet desde una red externa.
- La red debe dividirse y aislarse de acuerdo con las necesidades reales de la red. Si no hay requisitos de comunicación entre dos subredes, se sugiere usar VLAN, GAP de red y otras tecnologías para dividir la red, a fin de lograr el efecto de aislamiento de la red.
- Establezca el sistema de autenticación de acceso 802.1x para reducir el riesgo de acceso no autorizado a redes privadas.
- Habilite la función de filtrado de direcciones IP/MAC para limitar el rango de hosts que pueden acceder a la

dispositivo.

Más información

Visite el centro de respuesta a emergencias de seguridad del sitio web oficial de Dahua para conocer los anuncios de seguridad y las recomendaciones de seguridad más recientes.

ENABLING A SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No.1199 Bin'an Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053
Email: overseas@dahuatech.com | Fax: +86-571-87688815 | Tel: +86-571-87688883