Centro de alarmas

Manual del usuario

ZHEJIANG DAHUA VISIÓN TECNOLOGÍA CO.LTD.

Versión 2.0.3

Prefacio

General

Este manual presenta la instalación, las funciones y el funcionamiento del concentrador de alarmas (en adelante, el "concentrador"). Lea atentamente antes de utilizar el dispositivo y guarde el manual para futuras consultas.

Instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

Palabras de señal	Significado
DANGER	Indica un alto riesgo potencial 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, menor rendimiento o resultados impredecibles.
TIPS	Proporciona métodos para ayudarle a resolver un problema o ahorrarle tiempo.
NOTE	Proporciona información adicional como énfasis y complemento al texto.

Historial de revisiones

Versión	Versión del software	Contenido de la revisión	Liberar Tiempo
Versión 2.0.3	V1.001.0000007.0.R.231016	• Se agregaron PIN, datos de roaming, usuario del teclado, retraso en caso de falla de energía principal y selección de idioma del concentrador. • Se actualizaron los códigos de eventos de SIA y los eventos de falla de armado y descripción.	Noviembre 2023
Versión 2.0.2	V1.001.0000006.0.R.230714	• Se agregó configuración de IPC y configuración de enlace de alarma-video. • Códigos de eventos SIA actualizados. • Se agregó la categoría ATS: SP2/DP2 en la especificación técnica.	Agosto 2023

Versión	Versión del software	Contenido de la revisión	Liberar Tiempo
Versión 2.0.1	—	• Función de configuración básica del dispositivo actualizada. • Función de estado de visualización actualizada. • Se actualizó la configuración de la función hub. • Función de configuración de red cableada actualizada.	Abril de 2023
Versión 2.0.0	—	• Se agregaron configuraciones de red. • Se agregaron eventos de falla de armado y descripciones. • Se agregaron códigos y descripciones de eventos de SIA.	Noviembre 2022
Versión 1.1.0	—	• Se agregaron operaciones en la aplicación COS Pro y DMSS. • Se agregó gestión de usuarios. • Imágenes actualizadas. • Descripciones actualizadas de los parámetros.	Febrero 2022
Versión 1.0.0	—	Primer lanzamiento.	Octubre 2021

Aviso de protección de la privacidad

Como usuario del dispositivo o responsable del tratamiento 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 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 de la existencia del área de vigilancia y proporcionar la información de contacto requerida.

Acerca del manual

- El manual es solo de referencia. Pueden 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 de acuerdo con las últimas leyes y regulaciones de las jurisdicciones relacionadas. Para obtener información detallada, consulte el manual del usuario en papel, utilice nuestro CD-ROM, escanee el código QR o visite nuestro sitio web oficial. El manual es solo para referencia. Pueden encontrarse 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 provocar 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 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 explicación final.
- 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 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 al usarlo.

Requisitos de funcionamiento

- 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 los líquidos salpiquen o goteen sobre el dispositivo. Asegúrese de que no haya objetos que contengan líquido sobre el dispositivo para evitar que los líquidos fluyan hacia él.
- 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 se ajuste a los requisitos de energía del dispositivo.
- No conecte el dispositivo a más de una fuente de alimentación, ya que podría dañarse.

- 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.
- Utilice el adaptador de corriente o la fuente de alimentación del estuche proporcionado por el fabricante del dispositivo.
- La fuente de alimentación debe cumplir con los requisitos de ES1 en la norma 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 conexión a tierra de protección.

Tabla de contenido

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, el ingreso o el intento de ingreso 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. Consulta las que correspondan a tu modelo.

Tabla 1-1 Especificaciones técnicas

Tipo	Parámetro	Descripción
Puerto	Red	1 puerto Ethernet autoadaptativo RJ-45 10 M/100 M
	GSM	SIM única (GSM:900/1800 MHz); SIM dual con modo de espera único
	LTE	SIM única (GSM: 900/1800 MHz, WCDMA: B1/B5/B8, LTE-FDD: B1/B3/B5/B7/B8/B20, LTE-TDD:B38/B40/B41); SIM dual con modo de espera único
	Batería	Puerto de batería de 12 V
	Luz indicadora	1 para estados múltiples (alarma, armado, desarmado, conexión en red y mal funcionamiento)
	Botón	1 × reinicio, 1 × encendido, 1 × AP
	Zumbador	Incorporado
	Manosear	1 puerto de manipulación de caja para el panel de control de alarma
Función	Notificación por SMS	Alarma SMS (hasta 5 números de teléfono) Sólo disponible en modelos 2G y 4G.
	Llamada telefónica Notificación	Sí (hasta 5 números de teléfono) Sólo disponible en modelos 2G y 4G.
	Enlace de vídeo	Sí
	Protocolo de red	TCP/IP, incluidos PPTP, L2TP, DHCP, UPNP y NTP
	Actualización remota	Actualización de la nube
	Configuración Método	Aplicación
	Armar y desarmar Método	Aplicación, teclado, llavero, agenda

Tipo	Parámetro	Descripción	
	Número de Periféricos	Máx. 150 periféricos inalámbricos (8 cámaras PIR, 6 sirenas, 4 repetidores, 8 teclados, 64 llaveros inalámbricos, 256 tarjetas MIFARE One (8 tarjetas por usuario de teclado))	
	Área	32 áreas (habitaciones)	
	Usuarios	33 usuarios de la aplicación (31 usuarios generales, 1 usuario administrador y 1 instalador) y 32 usuarios del teclado	
	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 batería	
	Registros de eventos	Máximo 5000	
	Falla de energía Protección para Configurado Parámetros	Sí	
	Gestión de usuarios	Máximo 8 usuarios: 1 instalador, 1 administrador, 6 usuarios generales	
	Consulta	Búsqueda de mensajes push, estado del dispositivo y versión del programa. Detección de la intensidad de la señal.	
De radiofrecuencia	Frecuencia portadora	DHI-ARC3000H-FW2 (868)/ DHI-ARC3000H-GW2 (868)/ DHI-ARC3000H-W2 (868): 868,0 MHz–868,6 MHz	DHI-ARC3000H-FW2/DHI-ARC3000H-GW2/DHI-ARC3000H-W2: 433,1 MHz–434,6 MHz
	Comunicación Distancia	DHI-ARC3000H-FW2 (868)/ DHI-ARC3000H-GW2 (868)/ DHI-ARC3000H-W2 (868): Hasta 2.000 m (6.561,68 pies) en espacio abierto	DHI-ARC3000H-FW2/DHI-ARC3000H-GW2/DHI-ARC3000H-W2: Hasta 1.200 m (3.937,01 pies) en espacio abierto
	Transmisión Fuerza	DHI-ARC3000H-FW2 (868)/ DHI-ARC3000H-GW2 (868)/ DHI-ARC3000H-W2 (868): Límite 25 mW	DHI-ARC3000H-FW2/DHI-ARC3000H-GW2/DHI-ARC3000H-W2: Límite 10 mW
	Comunicación Mecanismo	De dos vías	
	Modo de cifrado	AES128	
	Frecuencia Saltando	Sí	
	Interferencia de RF 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	2,4 g	
Fuerza Suministrar	Tipo de PS	Tipo A	

Tipo	Parámetro	Descripción
	Energía principal	12 VCC, 1,5 A
	Capacidad de la batería	2x 3,6 V/2150 mAh
	Batería en espera	Hasta 12 h Cuando se cumplen las siguientes condiciones, el tiempo de espera puede alcanzar las 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
	Corriente máx. disponible	3,5 A
	Fuerza Consumo	Máx. 15 W
	Actual Consumo	Normal: 220 mA; alarma: 300 mA
	Batería baja Umbral de batería	3,5 VCC
	Restauración de batería Límite	3,7 VCC
	Voltaje de liberación	< 3,358 V
	Recarga de batería Tiempo	80% aprox. 15 h
Audio y Video	Entrada de vídeo	IPC de 4 canales (solo recibe y reenvía eventos de alarma de IPC y videos de alarma correspondientes)
ARCO Señalización	Categoría ATS	DP2/SP2 (LAN/Wi-Fi y GPRS/4G)
	Reconocimiento Operación	Pasar por
	Protocolos	SIA-DC09
	Primario Ruta de transmisión	LAN/Wi-Fi (N.º 50136-2)
	Secundario Ruta de transmisión	GPRS/4G
	Notificación Equipo	C/E/F

Tipo	Parámetro	Descripción	
Certificaciones		DHI-ARC3000H-FW2 (868)/ DHI-ARC3000H-GW2 (868)/ DHI-ARC3000H-W2 (868): ES 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 Categoría ATS: SP2/DP2 CE	DHI-ARC3000H-FW2/DHI-ARC3000H-GW2/DHI-ARC3000H-W2: Comisión Federal de Comunicaciones (FCC) CE

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 checks marcados comunicación dispositivos
SP4	3 minutos	Encriptado		√	√	Solo uno de los dos checks marcados comunicación dispositivos
SP5	Años 90	Encriptado		√	√	Solo uno de los dos checks marcados comunicación dispositivos
DP1	25 horas	Estándar	√	√	√	Sólo dos de los tres están marcados comunicación dispositivos
DP2	30 minutos	Estándar	√	√	√	Sólo dos de los tres están marcados comunicación dispositivos

COMIÓ **Categoría**	**Informes** **Tiempo**	**Protocolos**	**Dispositivos de comunicación**			**Comunicación** **Dispositivo a utilizar**
			PSTN	**2G/3G**	**Propiedad intelectual**	
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 solo 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 notificación: El tiempo de notificación se establece en función del estándar de cada nivel de rendimiento. El tiempo de notificación es el tiempo máximo disponible para notificar cuando falla un dispositivo de transmisión de alarma. Los dispositivos de transmisión de alarma cumplen este requisito informando periódicamente su estado a través de 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 están cifrados 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 cuáles dispositivos de comunicación se utilizarán en función de la categoría ATE.

Tabla 1-3 Especificaciones técnicas

Especificaciones técnicas	**Descripción**
Clasificación ACE	Tipo A
Clase de medio ambiente	II
Voltaje de suministro	12 VCC, 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% (humedad relativa)
Peso neto	0,38 kg (0,84 libras)
Peso bruto	0,8 kg (1,76 libras)
Caja	PC + ABS

1.3 Lista de verificación

Revise el paquete de acuerdo con la siguiente lista de verificación. Si encuentra algún daño o pérdida, comuníquese con el servicio de atención al cliente.

Figura 1-1 Lista de verificación

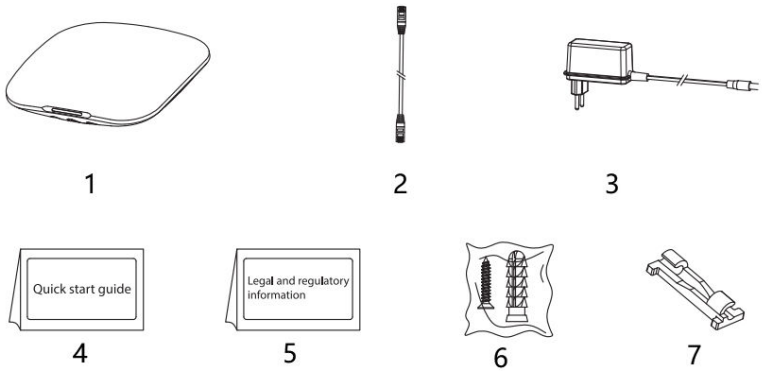


Tabla 1-4 Lista de verificación

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

2 Diseño

2.1 Apariencia

Figura 2-1 Apariencia

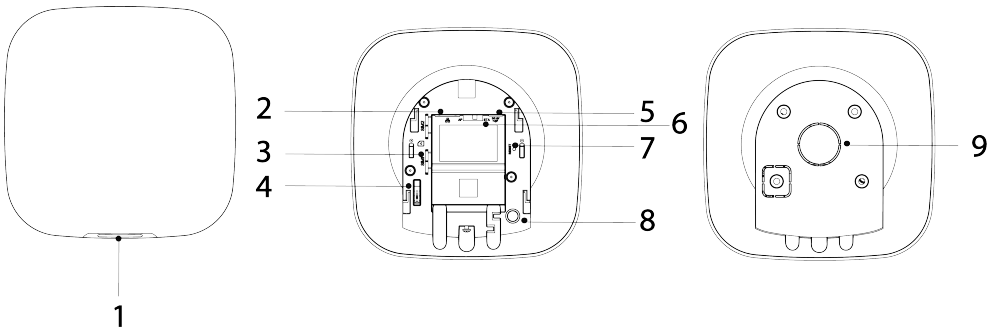


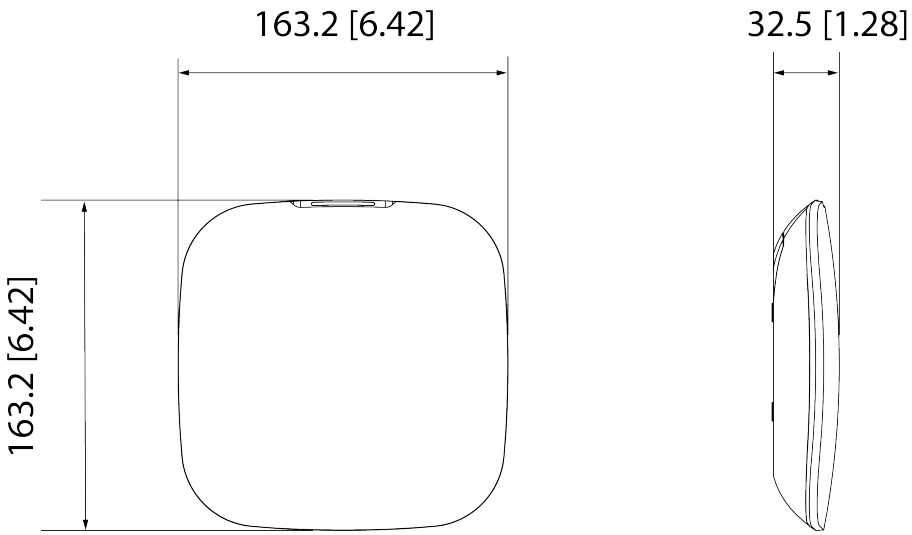
Tabla 2-1 Estructura

No.	Nombre	Descripción
1	Indicador	● Parpadea lentamente en verde: modo de sensibilidad reducida. ● Parpadea en verde: el concentrador comienza a funcionar. ● Amarillo sólido: No se pudo conectar a la nube. ● Verde sólido: modo 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 del 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 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 dos tarjetas SIM 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 complete la configuración de la red. ● La función SIM solo está disponible en modelos seleccionados.
4	Botón de manipulación	Cuando se suelta el interruptor antimanipulación, se activará la alarma antimanipulación.
5	Toma de cable de alimentación	Inserte el cable de alimentación.
6	AP	Encienda el 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	Botón de encendido y 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 Puesta en marcha

3.1 Usuarios

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

Nivel de acceso del usuario

Tabla 3-1 Nivel de acceso del usuario

Usuario	Nivel de acceso
Usuario administrador de DMSS	L2
Usuario general de DMSS	L2
Instalador	Nivel 3

- Instalador: los instaladores brindan 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 recibir permisos como configuración del dispositivo 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 la configuración del dispositivo y la 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: 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 negocio

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

Figura 3-1 Flujo de negocio (usuario DMSS)

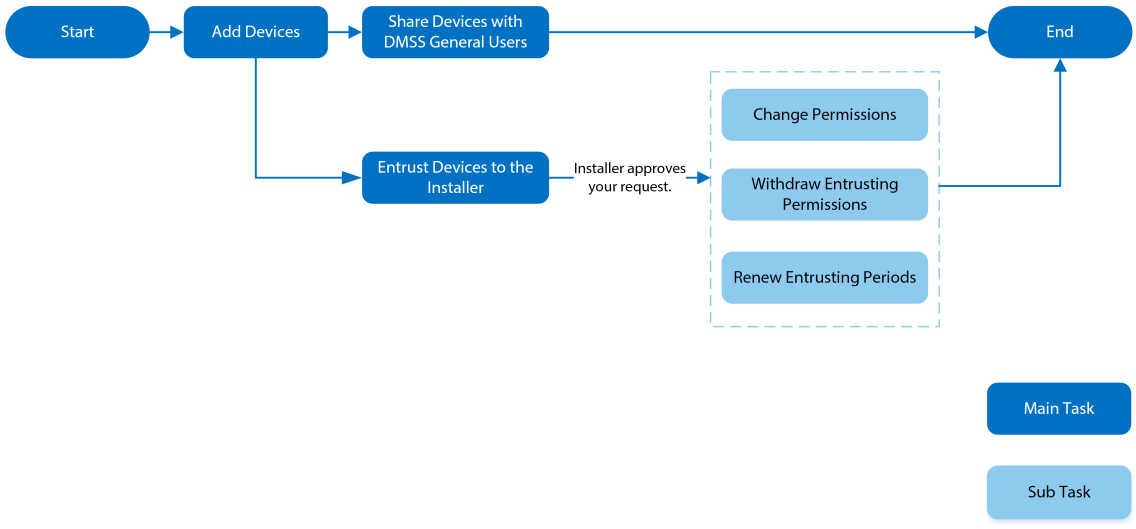
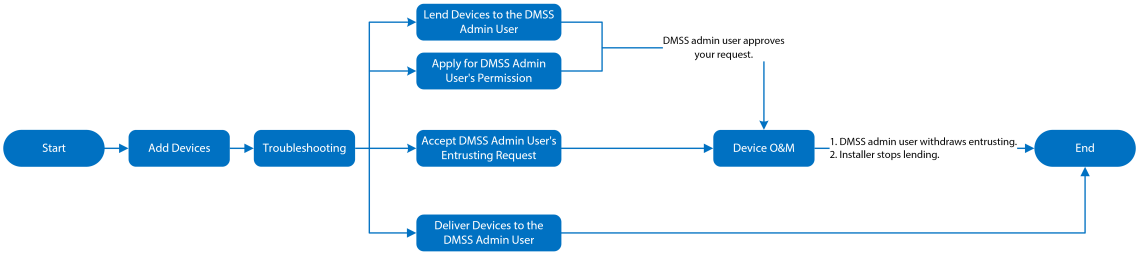


Figura 3-2 Flujo de negocio (Instalador)



3.2 Proceso de operación

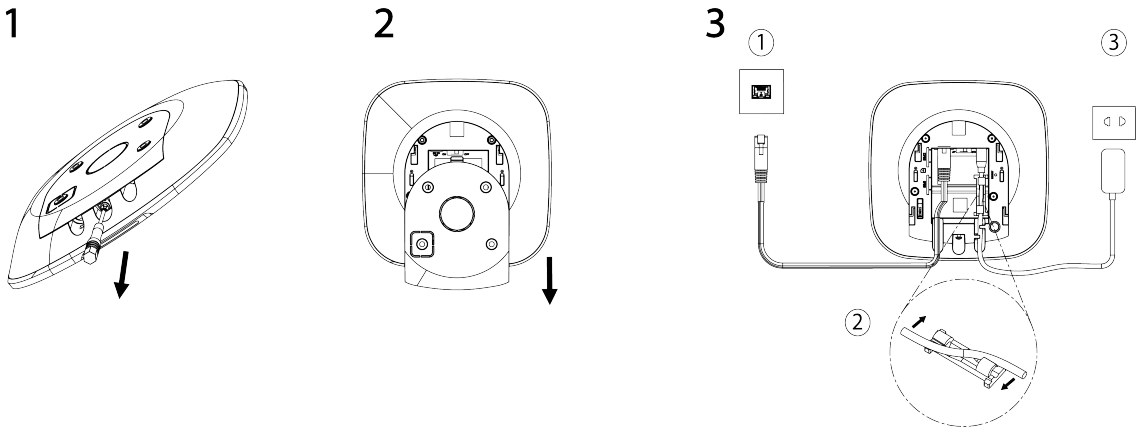
Siga los procedimientos a continuación para encender el sistema de alarma inalámbrico.

Figura 3-3 Proceso de operación

Encender

Conecte el concentrador a Ethernet y enciéndalo.

Figura 3-4 Encendido



Agregar dispositivos

1. Agregue el concentrador a la aplicación DoLynk Care y DMSS.
2. Añade los periféricos al concentrador.

Instalación del concentrador

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

- 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.

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 agujeros.
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.

Configurando el Hub

Configure el concentrador en la aplicación DoLynk Care y DMSS.

Activación del sistema de alarma

Puede utilizar el teclado, el llavero y la aplicación para armar el sistema. Después de enviar un comando de armado a la aplicación DoLynk Care y DMSS, el sistema comprobará el estado del sistema. Si el sistema tiene una falla, deberá elegir si desea armarlo a la fuerza. Para obtener detalles sobre los periféricos, consulte el manual del usuario del dispositivo correspondiente.

4 operaciones de Dolynk Care para instaladores

La aplicación Dolynk Care está diseñada para ayudar a los instaladores brindándoles servicios profesionales de operación y mantenimiento para los usuarios finales. Ofrece funciones que incluyen administración del sitio, administración del funcionamiento y el estado del dispositivo, revisión de la confianza del dispositivo y más. Para obtener más detalles, consulte *Manual del usuario de la aplicación Dolynk Care*.

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

4.1 Iniciar sesión en Dolynk Care

Para utilizar el dispositivo por primera vez, es necesario crear una cuenta. Este manual de usuario utiliza como ejemplo las operaciones en iOS.

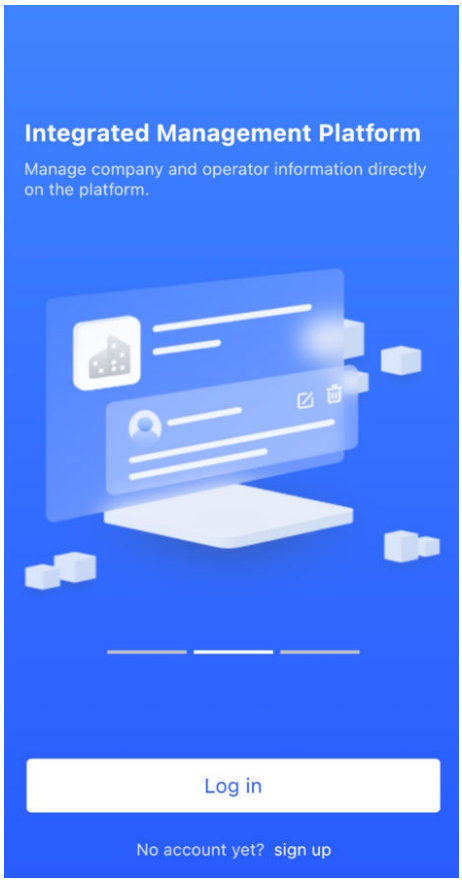
Procedimiento

Paso 1 Busque Dolynk Care en App Store para descargar la aplicación.

Para los usuarios de Android, pueden ir a Google Play para buscar la aplicación.

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

Figura 4-1 Iniciar sesión



Paso 3 Crear una cuenta.

1. En el**Acceso**pantalla, toque**¿Aún no tienes cuenta? Regístrate**.
2. En el**Registro**Pantalla, complete la información de los campos requeridos.
   - **nombre de empresa**:Introduzca el nombre de su empresa.
   - **Dirección del país**:Seleccione el país/área, provincia/estado y ciudad de su empresa.
   - **DIRECCIÓN**:Introduzca la dirección detallada de su empresa.
   - **Código de invitación**:Ingrese el código de invitación, que puede obtenerse del distribuidor o representante de ventas.
   - **Correo electrónico**:Introduzca su dirección de correo electrónico.
   - **Contraseña**:Introduzca la contraseña.
   - **Código de verificación**:Grifo**Enviar**, revise 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**Acuerdo de usuario**y luego seleccione el**He leído y acepto la Política de privacidad y el Acuerdo de usuario.**caja.
4. Toque**Registro**,y luego la aplicación vuelve a la**Acceso**pantalla. Ingrese su

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

- Para los nuevos clientes, se necesita la aprobación de la solicitud de cuenta. Recibirá un correo electrónico de aprobación de cuenta en un plazo de entre 1 y 3 días. Después de eso, podrá iniciar sesión en la aplicación con su cuenta.
- Algunos clientes afiliados no necesitan aprobación para registrarse en una cuenta de Dolynk Care. Pueden iniciar sesión directamente en la aplicación después del registro.

4.2 Agregar dispositivos

Los instaladores pueden agregar dispositivos a la aplicación Dolynk Care para su administración y mantenimiento. Antes de agregar dispositivos, asegúrese de que estén conectados a la red y a la alimentación. Puede agregar dispositivos de alarma, incluidos concentradores y varios periféricos, a la aplicación.

4.2.1 Agregar el Hub

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 esté conectado a la alimentación y a la red.
- Asegúrese de que su teléfono tenga habilitada la función Wi-Fi.

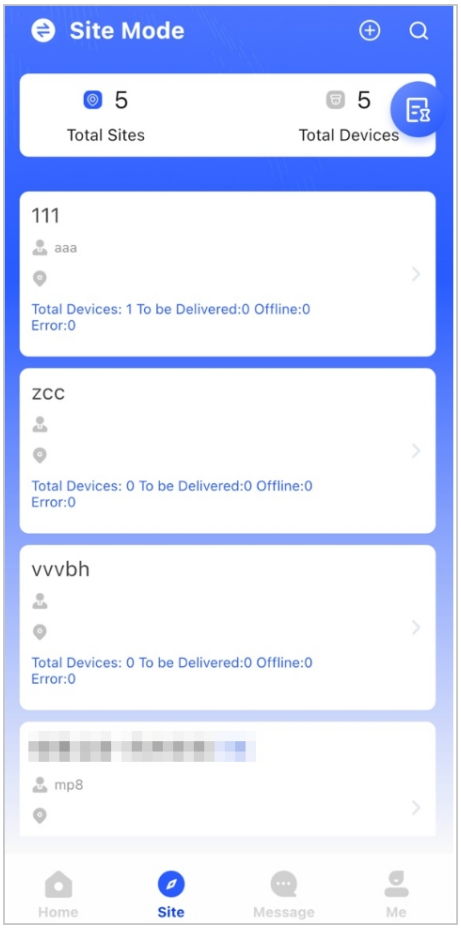
4.2.1.1 Agregar por SN o Código QR

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

Procedimiento

Paso 1 En el**Hogar**Pantalla, toque para ir a la**Sitio**pantalla.

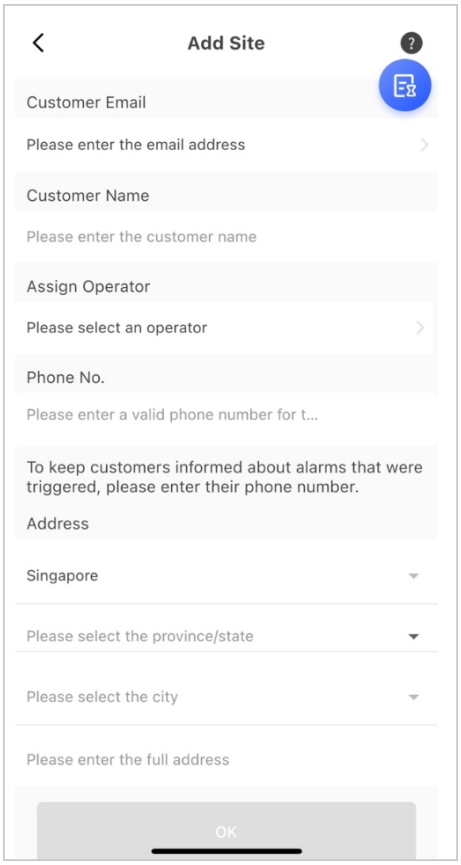
Figura 4-2 Sitio



Paso 2 Grifo para agregar un nuevo sitio.

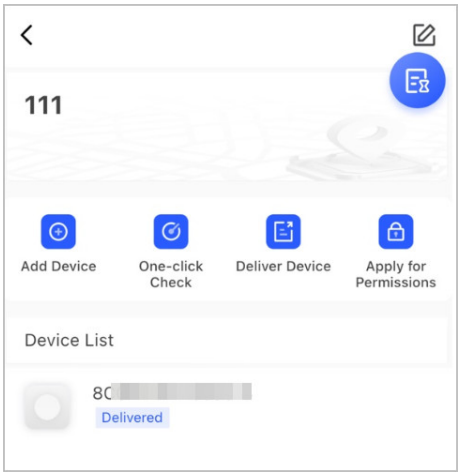
Ingrese la información del sitio y luego toque**DE ACUERDO**para crear el sitio.

Figura 4-3 Agregar sitio



Paso 3 En el**Sitio**pantalla que se creó, toque**Agregar dispositivo**.

Figura 4-4 Agregar dispositivo



Paso 4 Escanee el código QR del dispositivo o toque**Agregar manualmente**para ingresar manualmente el número de serie del dispositivo.

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

Paso 6 En el**Agregar dispositivo**Pantalla, seleccione un tipo de dispositivo.

Paso 7 Conéctese a una red inalámbrica o cableada.

- **Inalámbrico**

1. Toque**Inalámbrico**en la esquina superior derecha y luego**Inalámbrico**se convierte en**Con cable**.
2. Ingrese la contraseña de la red Wi-Fi a la 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.

- **Con cable**

1. Toque**Con cable**en la esquina superior derecha y luego**Con cable**se convierte en**Inalámbrico**.
2. Conecte el dispositivo a la alimentación y a la red y, a continuación, 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 mediante búsqueda LAN

Puedes buscar dispositivos y agregarlos. Asegúrate de que tu teléfono y los dispositivos estén conectados a la misma red.

Procedimiento

Paso 1 En el**Hogar**pantalla, toque para**Sitio**pantalla. Seleccione un sitio y

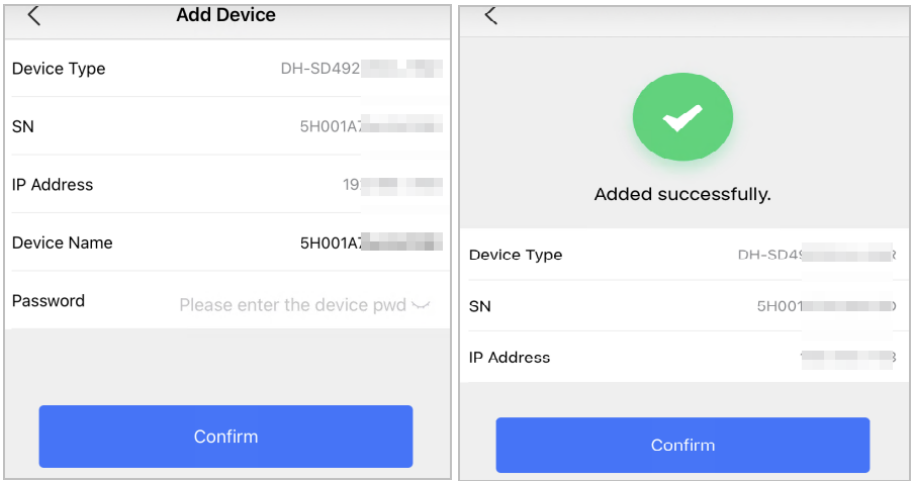
Paso 2 toque**Agregar dispositivo**para agregar un dispositivo.

Figura 4-5 Agregar un dispositivo

Paso 3 Grifo**Búsqueda en LAN**.

Paso 4 En**Agregar dispositivo**pantalla, ingrese la contraseña del dispositivo y luego toque**Confirmar**.

Figura 4-6 Confirmar para agregar un dispositivo



4.2.2 Agregar periféricos

Puede agregar varios periféricos al concentrador. En esta sección se utiliza un detector de puertas como ejemplo. Para obtener más información sobre cómo agregar periféricos, consulte los manuales de usuario de los respectivos periféricos.

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

Procedimiento

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.

Paso 2 Grifo**Próximo**.

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

Paso 4 Espere el emparejamiento.

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

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

4.3 Gestión de usuarios

4.3.1 Agregar 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.

Información de contexto

Según las certificaciones EN50131, el usuario administrador de DMSS no tiene permiso para configurar el dispositivo cuando los instaladores le prestan el concentrador o cuando le confían el concentrador al instalador.

4.3.1.1 Préstamo del dispositivo a los usuarios administradores del DMSS

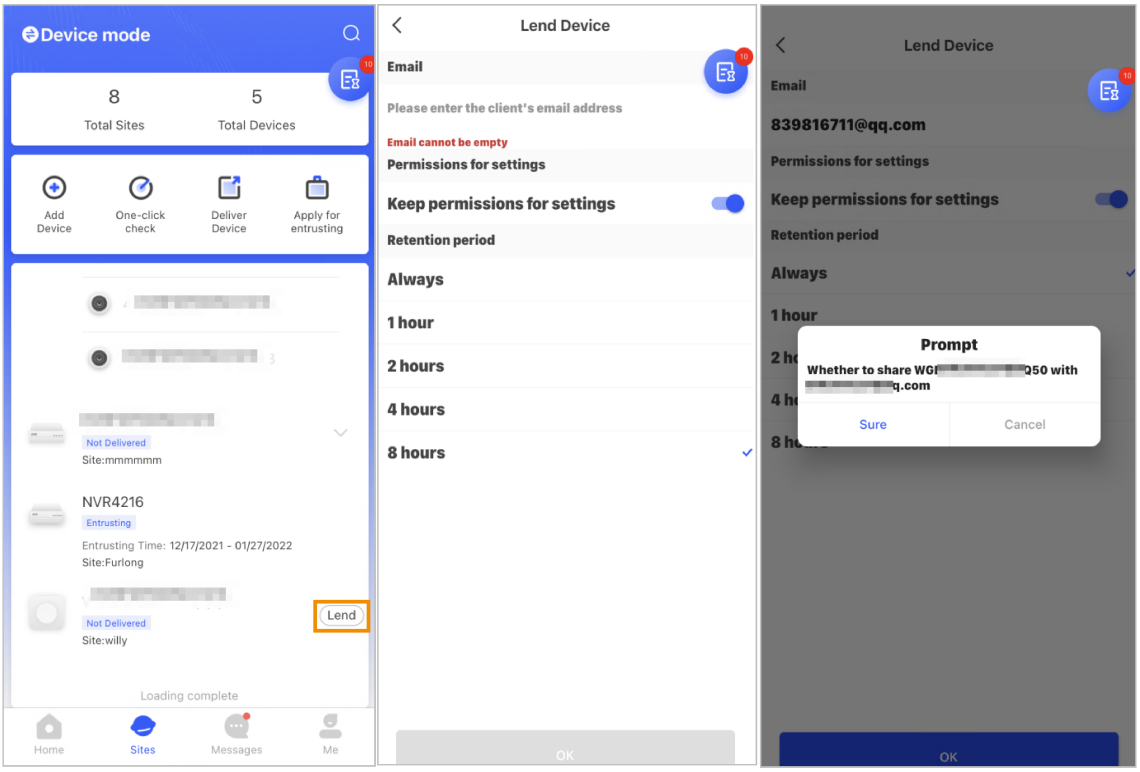
Según las certificaciones EN50131, el instalador puede prestar el concentrador al usuario administrador de DMSS. Luego, el instalador debe solicitar permisos al usuario administrador de DMSS, como configuración del dispositivo, operaciones de armado y desarmado y administración de usuarios.

Asegúrese de que el hub no haya sido agregado por otras cuentas.

Procedimiento

Paso 1 En el**Hogar**pantalla, toque y luego va a**Sitio**pantalla.

Figura 4-7 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 centro, ingrese el correo

Paso 4 electrónico del usuario administrador de DMSS.

Paso 5 Permitir**Permisos de configuración de reserva**y seleccione el tiempo de retención.

Paso 6 Toque**Confirmar**.

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

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

4.3.1.2 Aceptación de solicitudes de encargo

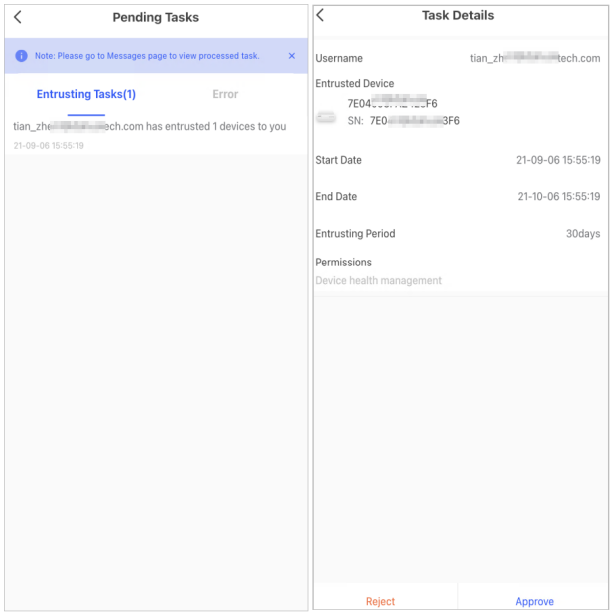
El instalador puede aceptar la solicitud de encomienda del usuario administrador de DMSS para proporcionar servicios de operación y mantenimiento a los usuarios.

Procedimiento

Paso 1 En el**Hogar**pantalla, seleccionar**Tarea pendiente**>**Revisión de confianza**.

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

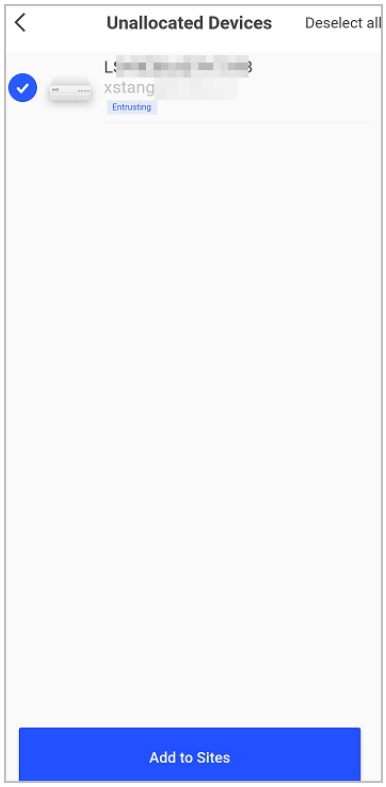
Figura 4-8 Manejar la encomienda de tareas



- Para aprobar

  1. Toque**Aprobar**,y luego va a la**Dispositivos no asignados**pantalla.
  2. Seleccione los dispositivos que desea asignar o toque**Seleccionar todo**,y luego toca**Agregar a sitios**.

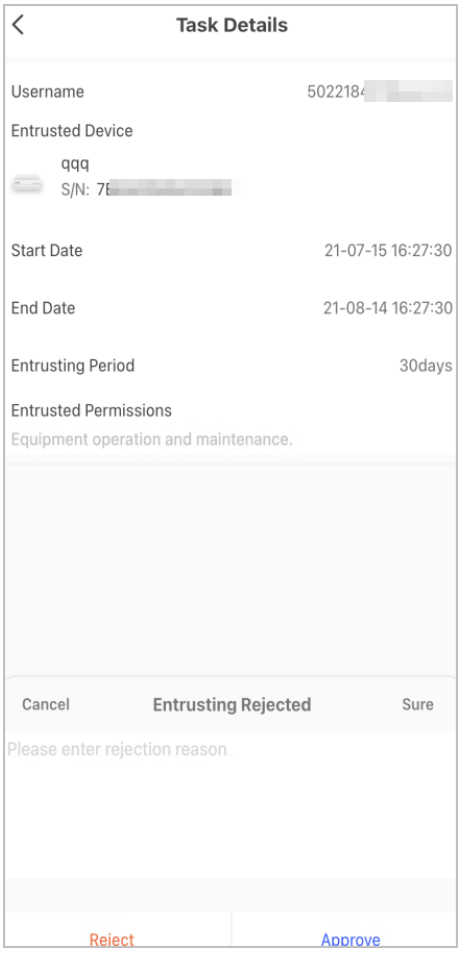
Figura 4-9 Agregar dispositivo a sitios



3. En el**Sitios**pantalla, seleccione un sitio o agregue un nuevo sitio.
4. Toque**DE ACUERDO**para confirmar mover este dispositivo al sitio seleccionado.

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

Figura 4-10 Rechazar



4.3.2 Eliminación de usuarios

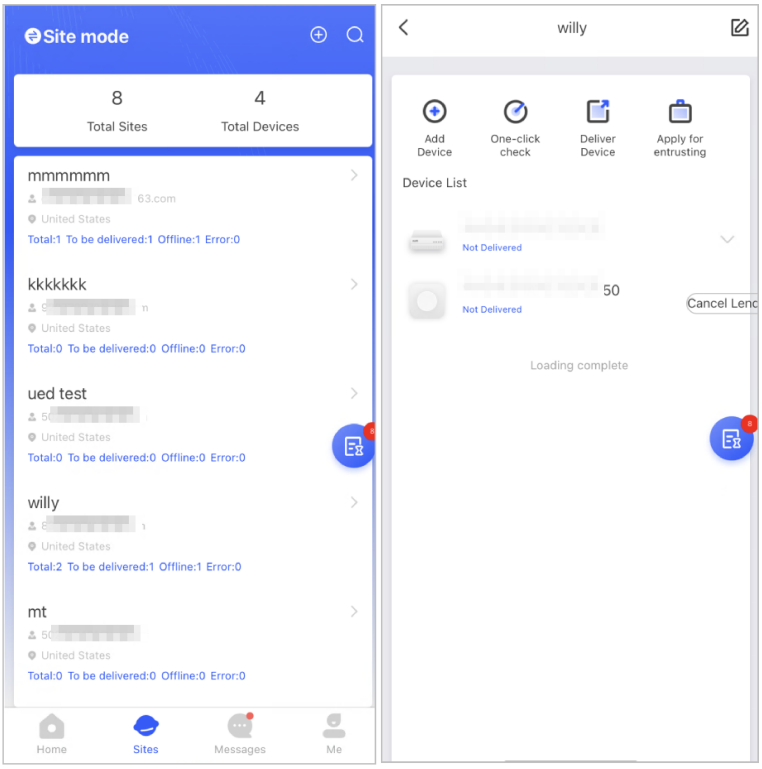
4.3.2.1 Cancelación del préstamo de dispositivos

Para el instalador, puede eliminar usuarios administradores de DMSS cancelando la opción de prestarles el centro.

Procedimiento

Paso 1 En el**Hogar**pantalla, toque y luego va a**Sitio**pantalla.

Figura 4-11 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 presta al usuario administrador de DMSS, luego seleccione el concentrador y luego toque**Cancelar préstamo**.

El mensaje se enviará a la cuenta de usuario administrador de DMSS, y el usuario administrador de DMSS podrá leer 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 los usuarios generales de DMSS.

Procedimiento

Paso 1 En el**Hogar**pantalla, toque y luego va a**Sitio**pantalla.

Paso 2 Toque en la esquina superior izquierda para cambiar a**Modo de dispositivo**En la lista de

Paso 3 dispositivos, seleccione el dispositivo según sea necesario.

Paso 4 En la pantalla central, toque y luego toque**Borrar**para eliminar el dispositivo.

4.4 Solicitud de permiso de usuario administrador de DMSS

Los instaladores pueden agregar el concentrador directamente a la aplicación Dolynk Care para brindar servicios de operación y mantenimiento del dispositivo a los usuarios administradores de DMSS. Tienen permisos limitados en el tiempo, incluida la configuración del dispositivo y la administración de usuarios, y deben volver a solicitar el permiso cuando vence.

Procedimiento

Paso 1 En el**Hogar**pantalla, toque , y luego va a**Sitio**pantalla.

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

Paso 3 En la lista de dispositivos, seleccione el dispositivo según sea necesario.

Paso 4 En el**Centro**pantalla, seleccione > **Configuración del concentrador**, toque cualquier parámetro que desee configurar y luego aparecerá un mensaje emergente para recordarle que debe solicitar permisos al usuario administrador de DMSS.

Paso 5 Grifo**Seguro**.

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

Paso 7 En el pantalla, toque**Mensaje personal**para ver los mensajes para ver si el DMSS El usuario administrador aceptó asignarle permisos.

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

4.5 Entrega de dispositivos al usuario administrador de DMSS

Después de instalar y configurar los dispositivos, puede enviarlos al usuario administrador de DMSS. No es posible enviar dispositivos desconectados o encomendados.

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

Procedimiento

Paso 1 En el**Hogar**pantalla, toque , y luego va a**Sitio**pantalla.

Paso 2 Grifo en la 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.

Paso 4 Toca y luego va a**Entregar dispositivos**pantalla.

No se podrán 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 pudieron ser entregados al usuario administrador de DMSS, vaya a**Fallido**Pantalla para entregar de nuevo.

Si los clientes utilizan una cuenta de Imou, sus dispositivos no se entregarán correctamente y aparecerá un mensaje en la pantalla.**Hogar**Pantalla que indica que la cuenta no tiene

el permiso. Solicite al cliente que actualice la cuenta en la aplicación DMSS. Para obtener más detalles, consulte *Manual del usuario de la aplicación DMSS*.

4.6 Operación y mantenimiento del estado del dispositivo

Los instaladores pueden proporcionar servicios de mantenimiento operativo y del estado del dispositivo, como verificar el estado de los dispositivos, configurarlos de forma remota y corregir errores.

4.6.1 Comprobación del estado de salud del dispositivo

Puede comprobar el estado en línea y fuera de línea de los dispositivos en tiempo real, y comprobar el estado de salud de los dispositivos de uno en uno o en lotes. En esta sección se utiliza el control en lotes como ejemplo.

Información de contexto

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.

Procedimiento

Paso 1 En el**Hogar**pantalla, toque , y luego va a**Sitio**pantalla.

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

Paso 3 Grifo .

Paso 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**.

No se pueden verificar los dispositivos fuera de línea.

4.6.2 Configuraciones básicas del dispositivo

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

Procedimiento

Paso 1 En el**Hogar**pantalla, toque ir a la**Sitio**pantalla.

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

Paso 3 En la lista de dispositivos, seleccione el dispositivo según sea necesario.

Paso 4 En la pantalla central, toque para ver y editar información general del dispositivo.

Tabla 4-1 Descripción de parámetros

Parámetro	Descripción
Estado del centro	Para obtener más detalles, consulte "4.6.2.2 Configuración del concentrador".
Configuración del concentrador	Para obtener más detalles, consulte "4.6.2.1 Estado de visualización".

Parámetro	Descripción
Configuración de red	Grifo**Configuración de 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.
Uso compartido de dispositivos	Grifo**Uso compartido de dispositivos**para compartir el estado del hub con los demás usuarios.
Actualización de la nube	Actualización en línea. No se permite la actualización cuando el concentrador está en estado armado o el nivel de batería es bajo.
Registros	Registros de dispositivos y aplicaciones. ● Registro del dispositivo: Seleccionar**Registro**>**Registro del dispositivo**para ver los registros de alarmas del dispositivo. También puedes tocar el**Registro del dispositivo**Pantalla para enviar registros de alarmas al correo electrónico vinculado. ● Registro de aplicaciones: Seleccionar**Registro**>**Registro de la aplicación**para ver los registros de alarmas del Dolynk Cuidado. También puedes tocar el**Registro de la aplicación**Pantalla para enviar registros de alarmas al correo electrónico vinculado.
Manual del usuario	Grifo**Manual del usuario**para obtener el manual del usuario del concentrador de alarma.

4.6.2.1 Estado de visualización

En el**Centro**pantalla, seleccionar > **Estado del centro**para ver el estado del hub.

Tabla 4-2 Estado

Parámetro	Descripción
Intensidad de la señal GMS/LTE	La intensidad de la señal de la red móvil para la tarjeta SIM activa. ● :Ultra bajo. ● : Bajo. ● : Moderado. ● : Alto. ● : No.

Parámetro	Descripción
Intensidad de la señal de Wi-Fi	Estado de la conexión a Internet del hub vía Wi-Fi. Para una mayor fiabilidad, recomendamos instalar el hub en lugares con una intensidad de señal de al menos 2 barras. ● :Ultra bajo. ● : Bajo. ● : Moderado. ● : Alto. ● : No.
Nivel de batería	Mostrar la electricidad restante de la batería. ● :Completamente cargado. ● : Suficiente. ● : Moderado. ● :Insuficiente.
Anti-manipulación	El modo de manipulación del periférico, que reacciona al desprendimiento del cuerpo.
Estado de la alimentación principal	Mostrar el estado de energía principal.
Estado de la conexión GSM/LTE	Estado de la conexión a Internet del hub a través de tarjeta SIM, Wi-Fi y Ethernet. ● :Conectado. ● :Desconectado.
Estado de la conexión Wi-Fi	
Estado de la 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. ● :No tiene tarjeta SIM.
Versión del programa	La versión del programa del hub.

4.6.2.2 Configuración del concentrador

En el**Centro**pantalla, seleccionar > **Configuración del concentrador**para configurar los parámetros del hub.

Tabla 4-3 Descripción de los parámetros del concentrador

Parámetro	Descripción
Administrador de usuarios	Puede agregar, modificar o eliminar usuarios del teclado cuando esté desarmado. ● **Agregar usuarios**:Grifo Para agregar un usuario, ingrese su nombre de usuario. contraseña y contraseña de coacción, y luego seleccione los permisos de armado y desarmado para la sala. ◇ La contraseña y el código de coacción deben tener entre 4 y 6 ◇ dígitos. El código de coacción es opcional. ◇ Se pueden crear hasta 32 usuarios. El primer usuario creado es el administrador de forma predeterminada. Todos los permisos están disponibles para ellos. ● **Eliminar usuario**:Seleccione el usuario y luego deslícese hacia la izquierda para eliminarlo. El usuario administrador debe ser el último en ser eliminado. ● **Modificación de la información del usuario**:Toque el usuario que necesita editar y luego podrá modificar la información del usuario, incluido el nombre de usuario, el código de acceso, el código de coacción y el permiso de armado y desarmado en la página de información del usuario. ● **Agregar tarjeta**:Grifo En la esquina superior derecha del usuario. Página de información para agregar una tarjeta para el usuario. Presione cualquier tecla para activar el teclado y luego coloque la tarjeta cerca del área de deslizamiento de tarjetas del teclado para ingresar al proceso de vinculación en 30 segundos. Si la información de la tarjeta se reconoce correctamente, el ID de la tarjeta se mostrará en la página de información del usuario y, a continuación, el teclado emitirá un pitido. Después de guardar las configuraciones, la tarjeta tendrá los permisos del usuario. Se pueden vincular hasta 8 tarjetas a un usuario. ● **Borrar tarjeta**:Seleccione la tarjeta y luego deslícela hacia la izquierda para eliminarla.
Armamento global/ Encantador	Arme o desarme todos los detectores en todas las áreas con un solo toque.
Programar armado/ Encantador	Armar o desarmar las áreas por horario. ● **Área**:Seleccione el área en la que opera el hub. ● **Configuración de comando**:Seleccione un modo armado según sea necesario tocando **Hogar**,**Lejos**, o**Desarmar**. ● **Tiempo**:Seleccione el período de tiempo en el que opera el hub. ● **Repetir**:Copiar el cronograma de armado o desarmado. ● **Armado a la fuerza**:Puede armar el sistema cuando ocurren errores en las zonas.
Configuración del tono de llamada	El tono de llamada al entrar o salir del modo de armado.

Parámetro	Descripción
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. ● 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.
Número de teléfono Gestión	GrifoAgregarEn la esquina superior derecha de la página, agregue un número de teléfono para recibir el evento y luego seleccione el tipo de evento que necesita enviar SMS. Los tipos de eventos incluyen alarma, falla, operación y si la alarma está vinculada al teléfono. Después de agregarlo, puede deslizar hacia la izquierda para probar las llamadas telefónicas y los mensajes SMS para verificar si el número de teléfono actual es válido. También puede 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	GrifoComenzarpara probar el estado de los periféricos que se conectan al concentrador en diferentes áreas y luego toqueDetenerpara 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.
Servicio en la nube Conexión	Establezca el intervalo de ping entre el servidor y el concentrador en un rango de 150 a 900 segundos (150 segundos de forma predeterminada). Si D-cloud detecta que el tiempo de desconexión 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.

Parámetro	Descripción
Latido del corazón	Configure el intervalo de ping del detector del concentrador. Los ajustes determinan 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**: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 no entregados para determinar la falla de 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 se detectará y se informará del estado fuera de línea de 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 de sirena para manipulación	● **Enlace de sirena para manipulación**:En el estado de armado, cuando el**Enlace de sirena 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 en el estado de desarmado. Está deshabilitado de manera predeterminada. Después de habilitar**Siempre activo**, cuando el **Enlace de sirena para manipulación**está habilitado, el concentrador vinculará el sonido de la alarma tanto en el estado de armado como de desarmado. Esto no cumple con las certificaciones EN50131-1.
Comprobación de la integridad del sistema	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. ● 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 durante 1 segundo, el indicador de armado y desarmado parpadea en verde durante 2 segundos y luego vuelve al estado normal.
CMS	Ingrese la dirección IP, el puerto y el ID del dispositivo y luego podrá registrar el concentrador en DSS Pro o Converter.

Parámetro	Descripción
Centro de alarmas	Permitir**Estación de Monitoreo**y luego configure los parámetros del protocolo SIA para el centro de recepción de alarmas (ARC). ● **Dirección IP preferida**:Introduzca la dirección IP y el número de puerto del ARC. ● **Dirección IP alternativa**:Introduzca la dirección IP alternativa y el número de puerto del ARC.  ◇ Los mensajes se enviarán a la dirección IP alternativa solo cuando la dirección IP preferida no pueda recibir el mensaje. ◇ Si**Intervalo de latidos del corazón**está habilitado, el sistema juzgará si enviar el mensaje a la dirección IP preferida o alternativa. ● **Protocolo IP**:Seleccionar**Protocolo de control de tráfico**por defecto. ● **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 significa**Intervalo de latidos del corazón**está deshabilitado. ● **Cuenta central**:Ingrese el número de cuenta creado por el ARC, que se utilizará para identificar el concentrador cuando este envíe información al ARC. ● **Encriptación**:El concentrador utiliza un formato de cifrado para la seguridad de la información cuando configura el ARC.**AES128**Está configurado de forma predeterminada. ● **Subir evento**:Toque junto a un evento para cargarlo. ◇ **Alarma**:Mensaje de alarma. ◇ **Error**:Fallo 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. ● **Prueba de comunicación**:Soportes**Prueba manual**y**Prueba programada**. ◇ **Prueba manual**:Pruebe manualmente si los parámetros de los centros de alarma preferidos y alternativos son normales. Si la prueba es exitosa, el centro puede recibir el evento de prueba. ◇ **Prueba programada**:La prueba programada está deshabilitada por error. Después de habilitarla, el concentrador informa periódicamente sobre el evento de prueba periódica.

Parámetro	Descripción
Comprobación de fallos	• **Falla de alimentación principal**:Está habilitado de manera predeterminada. Después de deshabilitarlo, cuando falla la alimentación principal del concentrador, este no lo indicará ni notificará. • **Manipulación del concentrador de alarma**:Está habilitado de forma predeterminada. Después de deshabilitarlo, cuando la tapa del concentrador esté abierta, el concentrador no indicará ni notificará nada. • **Conexiones a la plataforma en la nube**:Está habilitado de forma predeterminada. Después de deshabilitarlo, cuando la conexión entre el concentrador y la plataforma en la nube sea anormal, el concentrador no lo indicará ni notificará. • **Detección de errores en redes cableadas y Wi-Fi**:Está habilitado de forma predeterminada. Después de deshabilitarlo, cuando falla la red cableada y el wifi del concentrador, el concentrador no lo indicará ni notificará. • **Interferencia de RF**:Está habilitado de manera predeterminada. Después de deshabilitarlo, cuando el concentrador detecta interferencias de RF, no lo indica ni notifica, pero el evento se puede ver en el registro. La desactivación de cualquiera de estas funciones provocará que el sistema no cumpla con la norma EN50131-1 y no se enviarán los mensajes de error relacionados con la función deshabilitada.

4.6.3 Visualización de evaluaciones

Después de configurar los dispositivos de forma remota y de haber corregido los errores, los clientes evaluarán el desempeño de los operadores en la corrección de errores y el mantenimiento del estado del dispositivo. La cuenta de administrador puede ver detalles sobre los errores, como el tipo de error, la hora en que se produjo, las sugerencias y la operación, el nombre del operador y las calificaciones.

Procedimiento

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

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 solución de errores y la calificación.

4.6.4 Corrección de errores

Puede corregir errores después de comprobar dispositivos anormales. Los errores se detectan de dos formas: mediante informes automáticos de dispositivos y comprobación manual.

Procedimiento

Paso 1 En el**Hogar**pantalla, seleccionar**Tarea pendiente**>**Corrección de errores**En la

Paso 2 lista de errores, toque una tarea de error y luego toque**Iniciar procesamiento**.

Paso 3 Corrija el error según las sugerencias.

Paso 4 Grifo**Error corregido**Si se soluciona el error, esperar a que el cliente lo confirme.

Se notificará a los clientes el estado de la solución de los errores. Si confirman que el error se ha solucionado, se les solicitará que evalúen el servicio.

5 Operaciones del DMSS para usuarios finales

La aplicación DMSS ofrece servicios de vigilancia de seguridad profesionales para usuarios finales. Los usuarios administradores de DMSS pueden compartir el concentrador con usuarios generales de DMSS y confiarlo a una empresa. Los periféricos que vienen con el concentrador se pueden compartir y confiar al mismo tiempo. 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.

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.

Asegúrese de haber instalado la última versión de la aplicación.

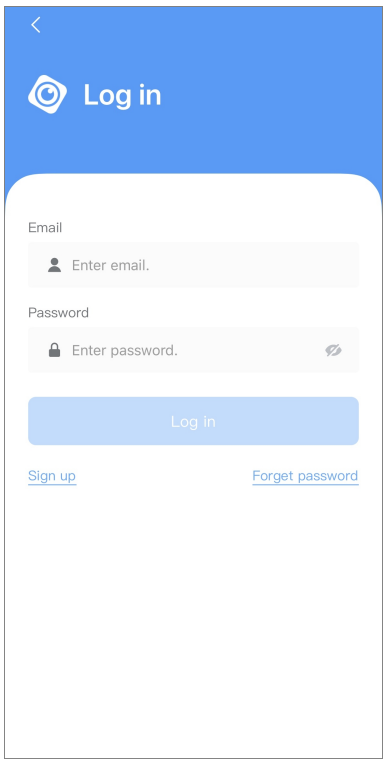
Procedimiento

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.

Figura 5-1 Inicio de sesión



Paso 3 Crear una cuenta.

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

2. Ingrese su dirección de correo electrónico y contraseña.

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

3. Lea el**Acuerdo de usuario**y**política de privacidad**y luego seleccione el**He leído y aceptó**caja.

4. 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, el código de verificación dejará de ser válido.

5. Toque**DE ACUERDO**.

Paso 4 En el**Acceso**pantalla, ingrese su correo electrónico y contraseña, y luego toque**Acceso**.

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

5.2 Agregar dispositivos

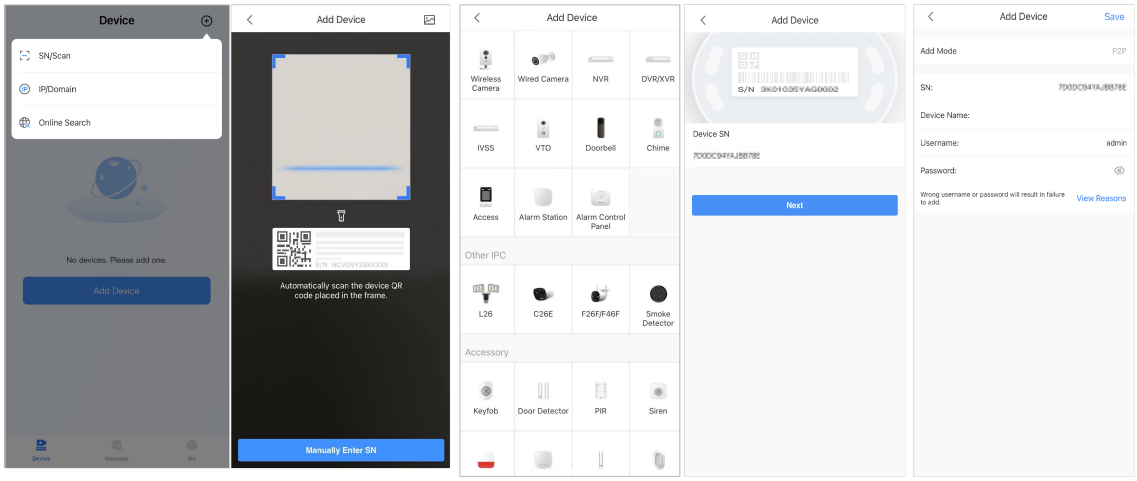
Para los usuarios finales, puede agregar dispositivos de alarma a la aplicación DMSS.

5.2.1 Agregar el Hub

Procedimiento

Paso 1 En el**Dispositivo**pantalla, toque y luego seleccione**SN/Escaneo**.

Figura 5-2 Agregar por código SN/QR



Paso 2 Agregar un dispositivo.

- Escanee directamente el código QR del dispositivo o toque e importe la imagen del código QR para agregar un dispositivo.
- Grifo**Ingresar SN manualmente**y luego ingrese el número de serie del dispositivo para agregar un dispositivo manualmente.

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

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

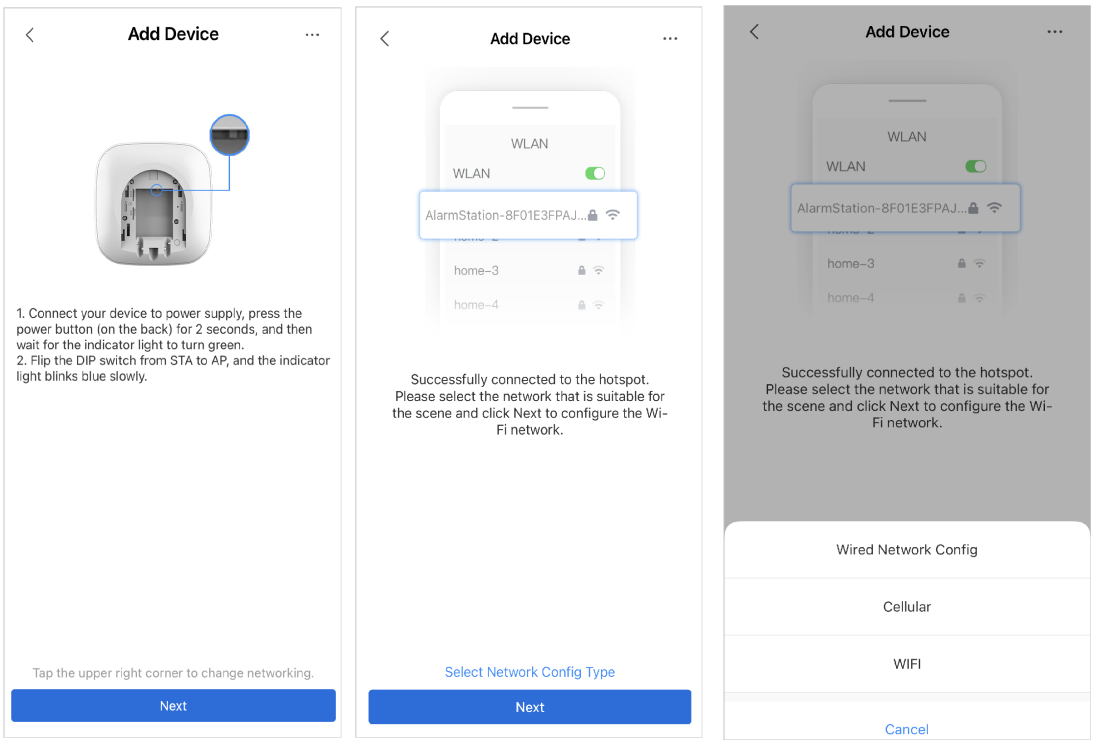
Paso 4 En el**Agregar dispositivo**pantalla, personalice el nombre del dispositivo, ingrese el nombre de usuario y la contraseña del dispositivo y luego toque**Ahorrar**.

Paso 5 Configurar los ajustes de red.

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, la máscara de subred, la puerta de enlace, el DNS y la dirección MAC.
- Celular: Configure el APN, modo de autenticación, nombre de usuario, contraseña, número de marcación, datos de roaming y PIN de la tarjeta SIM.
- Wi-Fi: seleccione una red Wi-Fi y luego ingrese la contraseña para conectarse a ella.

Figura 5-3 Configurar tipos de red



5.2.2 Agregar periféricos

Para los usuarios finales, puede agregar varios periféricos al concentrador. Las operaciones para agregar periféricos en DMSS son las mismas que en la aplicación Dolynk Care. Para obtener más información, consulte "4.2.2 Agregar periféricos".

5.2.3 Adición de IPC

Añade IPC al centro.

Prerrequisitos

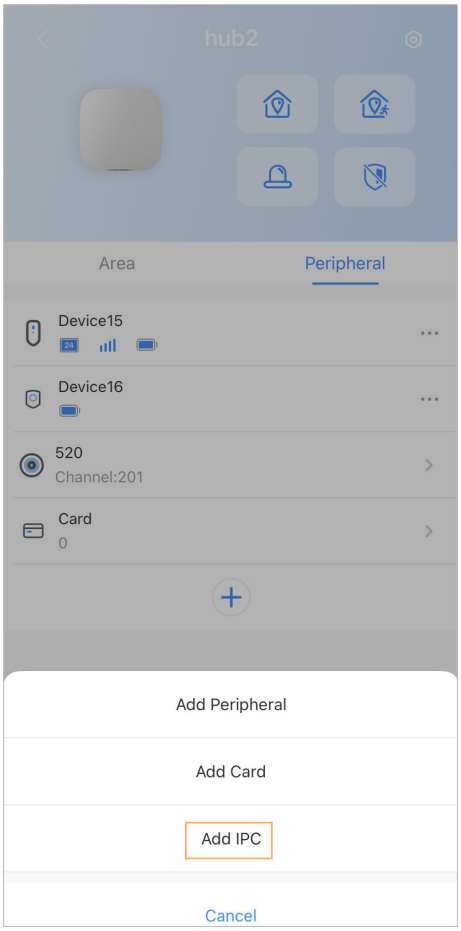
Asegúrese de que la versión de la aplicación DMSS sea 1.99.500 o posterior, y que el concentrador sea V1.001.0000006.0.R. 230714 o posterior.

Procedimiento

Paso 1 En la pantalla central, toque**Periférico**,y luego toca**+**.

Paso 2 Seleccionar**Añadir IPC**.

Figura 5-4 Agregar IPC

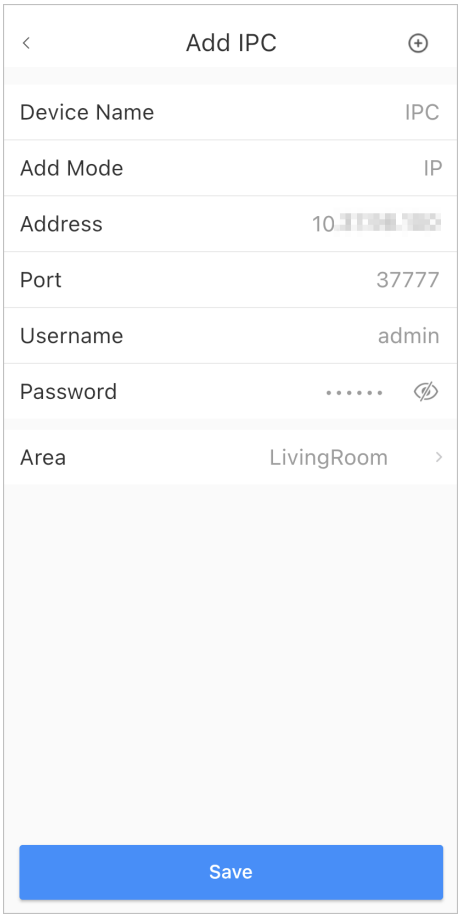


Paso 3 Añade un IPC al hub.

- 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.
  2. Toque**Ahorrar**.

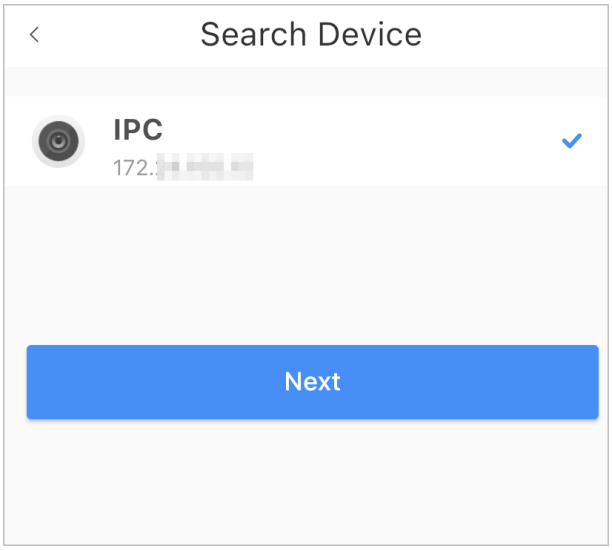
Figura 5-5 Agregar manualmente



- Búsqueda en línea:

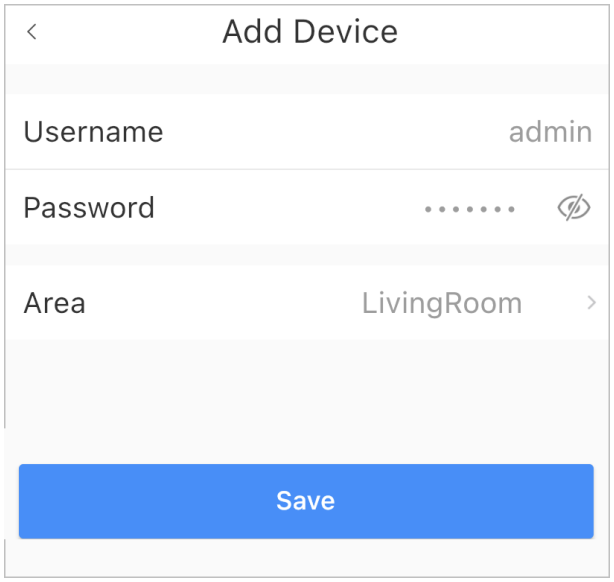
1. Toque para buscar el IPC en el mismo segmento de red.

Figura 5-6 Búsqueda en línea



2. Toque**Próximo**.
3. Ingrese la contraseña del IPC y seleccione el área donde está asignado el IPC, y luego toque**Ahorrar**.

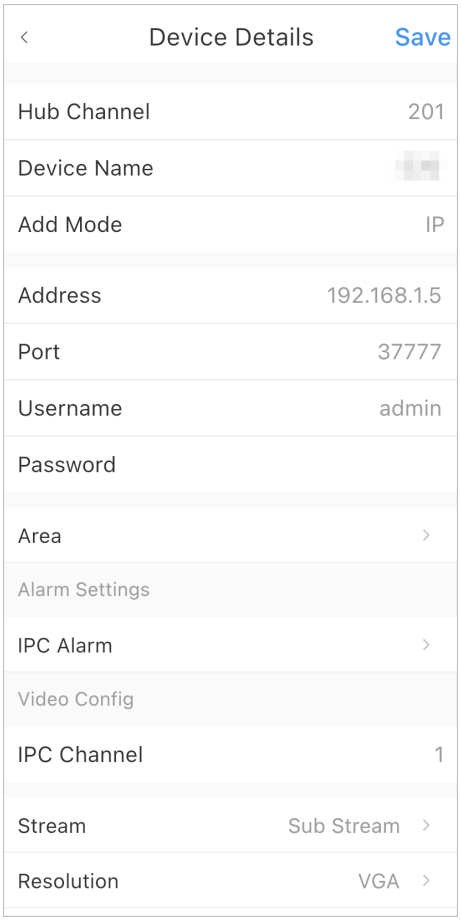
Figura 5-7 Ingresar contraseña



Operaciones relacionadas

En el**Detalles del dispositivo**pantalla, configure los parámetros del IPC.

Figura 5-8 Configuración de IPC



5.3 Configuración de la vinculación de alarmas por vídeo

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

Prerrequisitos

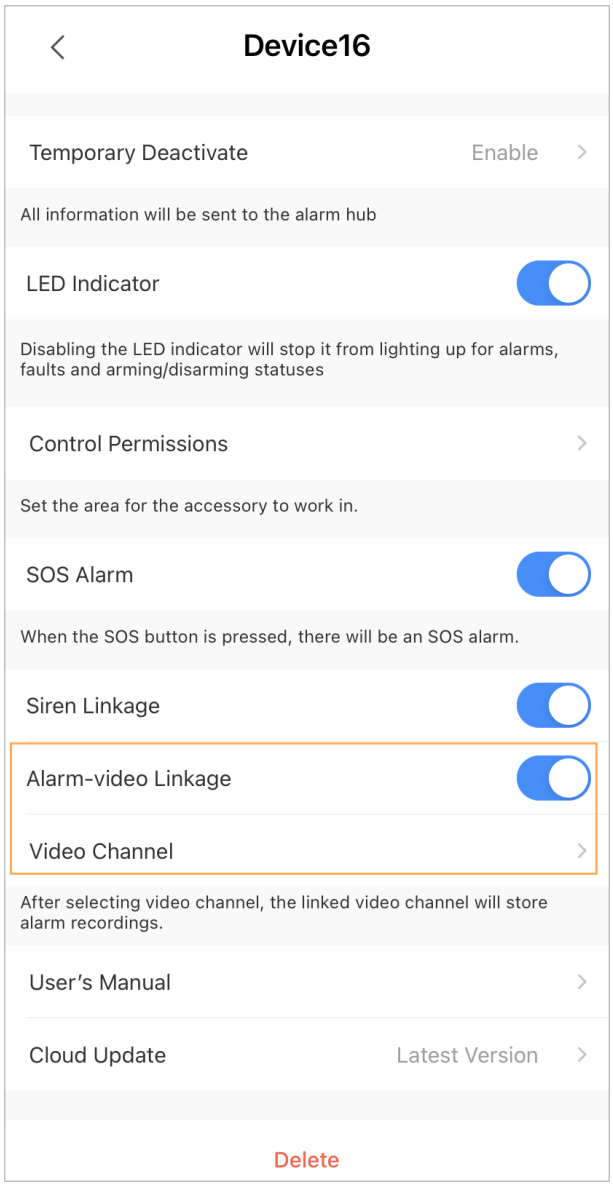
- Asegúrese de que el concentrador esté armado antes de configurar el enlace de alarma-video.
- Asegúrese de haber agregado periféricos al concentrador.

Procedimiento

Paso 1 En la pantalla del concentrador, seleccione un periférico en el**Periférico**lista y luego toque en el **Detalles del dispositivo**Pantalla para configurar los parámetros.

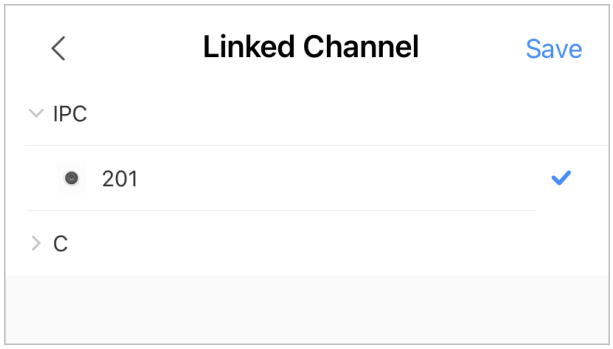
Paso 2 Permitir**Enlace de alarma y vídeo**,y luego seleccione**Canal de video**.

Figura 5-9 Pantalla de configuración



Paso 3 Seleccione un canal de vídeo de la**Canal vinculado**lista y toque**Ahorrar**.

Figura 5-10 Canal vinculado



5.4 Configuración general del concentrador

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

Procedimiento

Paso 1 En la pantalla del centro, toque ir a**Detalles del dispositivo**pantalla.

Tabla 5-1 Descripción de parámetros

Parámetro	Descripción
Estado del centro	Ver el estado del hub.
Configuración del concentrador	Configurar parámetros del hub.
Retardo por falla de la fuente de alimentación principal	Establezca el tiempo de retardo para que todos los dispositivos del sistema activen funciones cuando se desconecta la fuente de alimentación principal.
Indicador LED	Habilite la función para que el indicador LED del hub pueda funcionar.
Configuración de red	Grifo**Configuración de 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.
Uso compartido de dispositivos	Grifo**Uso compartido de dispositivos**para compartir el estado del hub con los demás usuarios.
Idiomas del dispositivo	Seleccione el idioma para el hub entre inglés, español, árabe, danés, francés, italiano y turco.
Confianza del dispositivo	Confíe los dispositivos a proveedores de servicios para que realicen servicios de operación de alarma para usted.
Manual del usuario	Grifo**Manual del usuario**para obtener el manual del usuario del concentrador de alarma.
Actualización de la nube	Actualización en línea. No se permite la actualización cuando el concentrador está en estado armado o el nivel de batería es bajo.

Parámetro	Descripción
Registros	Registros de dispositivos y aplicaciones. ● Registro del dispositivo: Seleccionar**Registro**>**Registro del dispositivo**para ver los registros de alarmas del dispositivo. También puedes tocar el**Registro del dispositivo**Pantalla para enviar registros de alarmas al correo electrónico vinculado. ● Registro de aplicaciones: Seleccionar**Registro**>**Registro de la aplicación**para ver los registros de alarmas de DoLynk Cuidado. También puedes tocar el**Registro de la aplicación**Pantalla para enviar registros de alarmas al correo electrónico vinculado.

5.4.1 Visualización del estado del concentrador

En el**Centro**pantalla, seleccionar > **Estado del centro**para ver el estado del hub.

Tabla 5-2 Estado

Parámetro	Descripción
Intensidad de la señal GMS/LTE	La intensidad de la señal de la red móvil para la tarjeta SIM activa. ● :Ultra bajo. ● : Bajo. ● : Moderado. ● : Alto. ● : No.
Intensidad de la señal de Wi-Fi	Estado de la conexión a Internet del hub vía Wi-Fi. Para una mayor fiabilidad, recomendamos instalar el hub en lugares con una intensidad de señal de al menos 2 barras. ● :Ultra bajo. ● : Bajo. ● : Moderado. ● : Alto. ● : No.
Nivel de batería	Mostrar la electricidad restante de la batería. ● :Completamente cargado. ● : Suficiente. ● : Moderado. ● :Insuficiente.
Anti-manipulación	El modo de manipulación del periférico, que reacciona al desprendimiento del cuerpo.
Estado de la alimentación principal	Mostrar el estado de energía principal.

Parámetro	Descripción
Estado de la conexión GSM/LTE	Estado de la conexión a Internet del hub a través de tarjeta SIM, Wi-Fi y Ethernet. ● :Conectado. ● :Desconectado.
Estado de la conexión Wi-Fi	
Estado de la conexión del cable de red	
Tarjeta SIM	Estado de conexión de la tarjeta SIM. ● :La tarjeta SIM 1 está activa. ● :La tarjeta SIM 2 está activa. ● :No tiene tarjeta SIM.
Estado de la tarjeta SIM	Esta barra de estado solo es compatible cuando hay una tarjeta SIM insertada en el concentrador. ● :La tarjeta SIM está desbloqueada. ● :La tarjeta SIM está bloqueada.
Versión del programa	La versión del programa del hub.

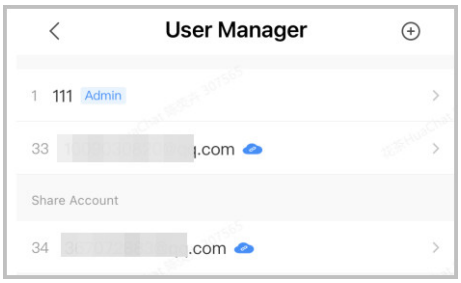
5.4.2 Configuración del concentrador

Procedimiento

Paso 1 En el**Centro**pantalla, toque .

Paso 2 Ver y editar información general del hub.

Tabla 5-3 Descripción de los parámetros del concentrador

Parámetro	Descripción
Administrador de usuarios	Puede agregar, modificar o eliminar usuarios del teclado cuando esté desarmado. ● **Agregar usuarios**:Grifo Para agregar un usuario, ingrese su nombre de usuario y el teclado. código (de 4 a 6 dígitos) y código de acceso de coacción (opcional) y luego seleccione los permisos de armado y desarmado para 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 de manera predeterminada y tiene todos los permisos disponibles. ◇ DMSS crea automáticamente un usuario de teclado cada vez que se agrega un dispositivo por primera vez. El número de secuencia de usuarios de teclado creados por el sistema comienza automáticamente desde 33 y tiene un ícono junto a su cuenta. ◇ Se creará automáticamente un usuario de teclado para los usuarios compartidos. Figura 5-11 Agregar usuario del teclado  ● **Eliminar usuario**:Seleccione el usuario y luego deslícese hacia la izquierda para eliminarlo. El usuario administrador debe ser el último en ser eliminado. ● **Modificación de la información del usuario**:Toque el usuario que necesita editar y luego podrá modificar la información del usuario, incluido el nombre de usuario, el código de acceso, el código de coacción y el permiso de armado y desarmado en la página de información del usuario. ● **Agregar tarjeta**:Grifo En la esquina superior derecha del usuario. Página de información para agregar una tarjeta para el usuario. Presione cualquier tecla para activar el teclado y luego coloque la tarjeta cerca del área de deslizamiento de tarjetas del teclado para ingresar al proceso de vinculación en 30 segundos. Si la información de la tarjeta se reconoce correctamente, el ID de la tarjeta se mostrará en la página de información del usuario y, a continuación, el teclado emitirá un pitido. Después de guardar las configuraciones, la tarjeta tendrá los permisos del usuario. Se pueden vincular hasta 8 tarjetas a un usuario. ● **Borrar tarjeta**:Seleccione la tarjeta y luego deslícela hacia la izquierda para eliminarla.
Armamento global/ Encantador	Arme o desarme todos los detectores en todas las áreas con un solo toque.

Parámetro	Descripción
Programar armado/ Encantador	Armar o desarmar las áreas por horario. ● **Área**:Seleccione el área en la que opera el hub. ● **Configuración de comando**:Seleccione un modo armado según sea necesario tocando **Hogar**,**Lejos**, o**Desarmar**. ● **Tiempo**:Seleccione el período de tiempo en el que opera el hub. ● **Repetir**:Copiar el cronograma de armado o desarmado. ● **Armado a la fuerza**:Puede armar el sistema cuando ocurren errores en las zonas.
Configuración del tono de llamada	El tono de llamada al entrar o salir del modo de armado.
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. ● 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.
Número de teléfono Gestión	GrifoAgregarEn la esquina superior derecha de la página, agregue un número de teléfono para recibir el evento y luego seleccione el tipo de evento que necesita enviar SMS. Los tipos de eventos incluyen alarma, falla, operación y si la alarma está vinculada al teléfono. Después de agregarlo, puede deslizar hacia la izquierda para probar las llamadas telefónicas y los mensajes SMS para verificar si el número de teléfono actual es válido. También puede 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	GrifoComenzarpara probar el estado de los periféricos que se conectan al concentrador en diferentes áreas y luego toqueDetenerpara completar la detección.
Sensibilidad reducida Modo	PermitirModo 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.
Servicio en la nube Conexión	Establezca el intervalo de ping entre el servidor y el concentrador en un rango de 150 a 900 segundos (150 segundos de forma predeterminada). Si D-cloud detecta que el tiempo de desconexión 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.

Parámetro	Descripción
Latido del corazón	Configure el intervalo de ping del detector del concentrador. Los ajustes determinan 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**: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 no entregados para determinar la falla de 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 se detectará y se informará del estado fuera de línea de 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 de sirena para manipulación	● **Enlace de sirena para manipulación**:En el estado de armado, cuando el**Enlace de sirena 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 en el estado de desarmado. Está deshabilitado de manera predeterminada. Después de habilitar**Siempre activo**, cuando el**Enlace de sirena para manipulación**está habilitado, el concentrador vinculará el sonido de la alarma tanto en el estado de armado como de desarmado. Esto no cumple con las certificaciones EN50131-1.
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. ● 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 durante 1 segundo, el indicador de armado y desarmado parpadea en verde durante 2 segundos y luego vuelve al estado normal.
CMS	Ingrese la dirección IP, el puerto y el ID del dispositivo y luego podrá registrar el concentrador en DSS Pro o Converter.

Parámetro	Descripción
Recibir alarma Central	Habilite la función y luego configure los parámetros del protocolo SIA para el centro de recepción de alarmas (ARC). ● **Nombre de dominio/IP preferido**:Introduzca la dirección IP/dominio y el número de puerto del ARC. ● **Nombre de dominio/IP alternativo**:Introduzca la dirección IP/dominio alternativo y el número de puerto del ARC. ◇ Los mensajes se enviarán a la dirección IP/dominio alternativo solo cuando la dirección IP preferida no pueda recibir el mensaje. ◇ Si**Intervalo de latidos del corazón**está habilitado, el sistema juzgará si enviar el mensaje a la dirección IP preferida o alternativa. ● **Protocolo IP**:Seleccionar**Protocolo de control de tráfico**por defecto. ● **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 significa**Intervalo de latidos del corazón**está deshabilitado. ● **Cuenta central**:Ingrese el número de cuenta creado por el ARC, que se utilizará para identificar el concentrador cuando este envíe información al ARC. ● **Periodo de recarga**:Seleccione el período de recarga de la lista. ● **Encriptación**:El concentrador utiliza un formato de cifrado para la seguridad de la información cuando configura el ARC.**AES128**Está configurado de forma predeterminada. ● **Subir eventos**:Toque junto a un evento para cargarlo. ◇ **Alarma**:Mensaje de alarma. ◇ **Defectos**:Fallo de energía, bajo voltaje de la batería, manipulación y fuera de línea. ◇ **Eventos**: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. ● **Prueba de comunicación**:Soportes**Prueba manual**y**Prueba programada**. ◇ **Prueba manual**:Pruebe manualmente si los parámetros de los centros de alarma preferidos y alternativos son normales. Si la prueba es exitosa, el centro puede recibir el evento de prueba. ◇ **Prueba programada**:La prueba programada está deshabilitada por error. Después de habilitarla, el concentrador informa periódicamente sobre el evento de prueba periódica.

Parámetro	Descripción
Comprobación de fallos	• **Falla de alimentación principal**:Está habilitado de manera predeterminada. Después de deshabilitarlo, cuando falla la alimentación principal del concentrador, este no lo indicará ni notificará. • **Manipulación del concentrador de alarma**:Está habilitado de forma predeterminada. Después de deshabilitarlo, cuando la tapa del concentrador esté abierta, el concentrador no indicará ni notificará nada. • **Conexiones a la plataforma en la nube**:Está habilitado de forma predeterminada. Después de deshabilitarlo, cuando la conexión entre el concentrador y la plataforma en la nube sea anormal, el concentrador no lo indicará ni notificará. • **Errores de red cableada y Wi-Fi**:Está habilitado de forma predeterminada. Después de deshabilitarlo, cuando falla la red cableada y el wifi del concentrador, el concentrador no lo indicará ni notificará. • **Errores de la red celular**:Está habilitado de manera predeterminada. Después de deshabilitarlo, cuando falla la red celular del concentrador, este no lo indicará ni notificará. • **Interferencia de RF**:Está habilitado de manera predeterminada. Después de deshabilitarlo, cuando el concentrador detecta interferencias de RF, no lo indica ni notifica, pero el evento se puede ver en el registro. La desactivación de cualquiera de estas funciones provocará que el sistema no cumpla con la norma EN50131-1 y no se enviarán los mensajes de error relacionados con la función deshabilitada.

5.5 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.

5.5.1 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 5-4 Descripción de los parámetros de la red cableada

Parámetro	Descripción
DHCP	Cuando hay un servidor DHCP en la red, puede habilitarlo **DHCP**y 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	
Puerta	
Sistema de nombres de dominio	
DNS2	
Dirección MAC	

5.5.2 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.

5.5.3 Configuración celular

Procedimiento

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

Paso 2 Configurar parámetros celulares.

Tabla 5-5 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**Establecer el celular como prioridad Al seleccionar la red.
Tarjeta SIM 1 Tarjeta SIM 2	• Admite dos tarjetas SIM y modo de espera único. • Las tarjetas SIM permiten que el concentrador utilice datos celulares y envíe notificaciones de alarma.
APN	El nombre del punto de acceso (APN) es el nombre de la configuración que su dispositivo lee para configurar una conexión para la puerta de enlace entre la red celular de su operador e Internet pública.
Modo de autenticación	Modo de autenticación de la red celular.
Nombre de usuario Contraseña	El nombre de usuario y la contraseña de la red celular.
Marcar número	El número al que debe llamar el concentrador.
Datos de itinerancia	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.
ALFILER	Introduzca el PIN de las tarjetas SIM para proteger la privacidad cuando sea necesario. Está prohibido introducir el código PIN cuando la tarjeta SIM está desbloqueada. Bloquéela cuando desee introducir el PIN.

5.6 Gestión de usuarios

5.6.1 Agregar usuario

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

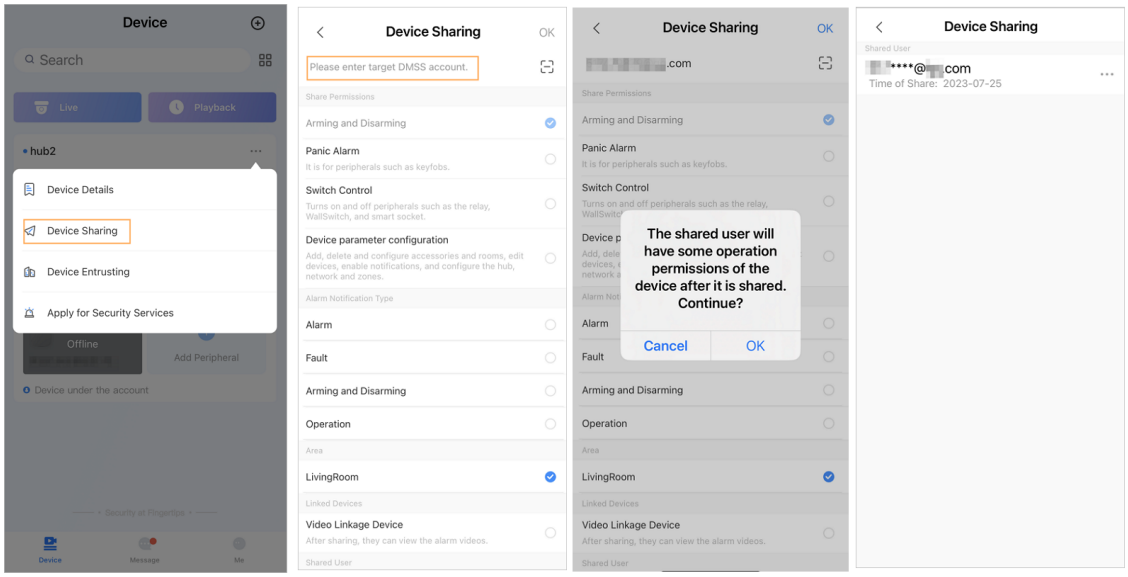
5.6.1.1 Agregar usuario general de DMSS

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 en > **Dispositivo** **Intercambio**como ejemplo.

Procedimiento

Paso 1 En el**Dispositivo**pantalla, toque junto a un dispositivo y luego toque**Uso compartido de dispositivos**

Figura 5-12 Compartir dispositivo



Paso 2 En el**Uso compartido de 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**Uso compartido de dispositivos**pantalla.

5.6.1.2 Agregar instalador

Para los usuarios administradores de DMSS, puede agregar instaladores confiándoles dispositivos. Puede confiarles dispositivos a los instaladores uno por uno o en lotes.

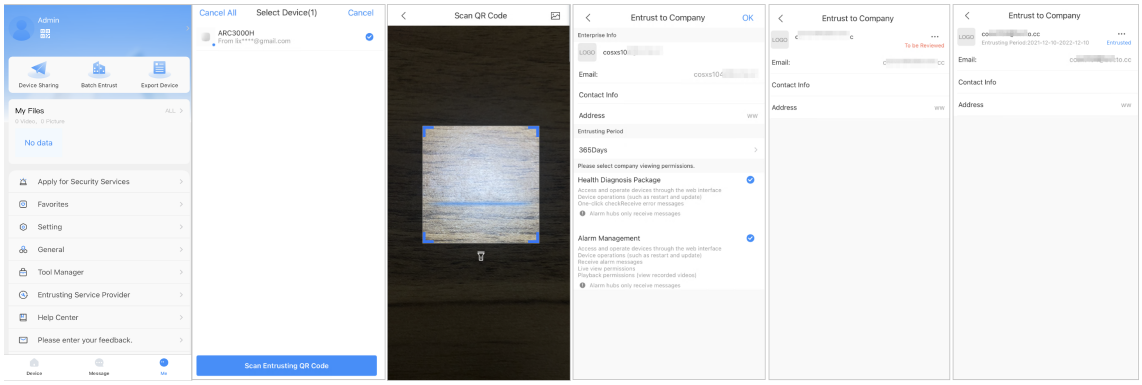
5.6.1.2.1 Confianza de dispositivos en lotes

Puede confiar dispositivos a una empresa en lotes.

Procedimiento

Paso 1 Seleccionar**A mí**>**Encomienda por lotes**.

Figura 5-13 Confiar dispositivos en lotes



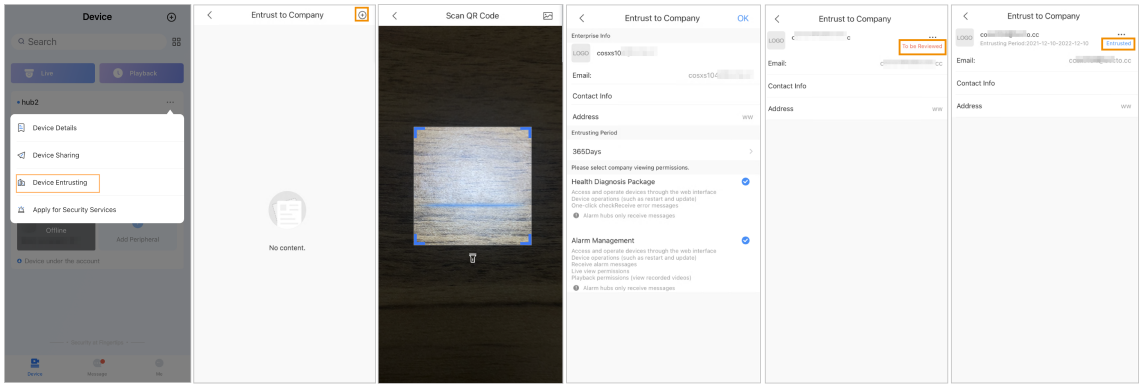
Paso 2 En el**Seleccionar dispositivo**En la pantalla, seleccione los dispositivos que desea confiar y, a continuación, confíelos a la empresa. El proceso para confiar varios dispositivos es el mismo que para confiar un solo dispositivo.

5.6.1.2.2 Confianza de dispositivos uno por uno

Procedimiento

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

Figura 5-14 Confiar un dispositivo



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

Puedes solicitar a los instaladores sus códigos QR.

Paso 3 En el**Confiar 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 del instalador.

Paso 4 Ver detalles de encomienda en el**Confiar a la empresa**pantalla.

Cuando se confía 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**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**.

5.6.2 Eliminación de usuario

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

5.6.2.1 Cancelación del uso compartido del dispositivo

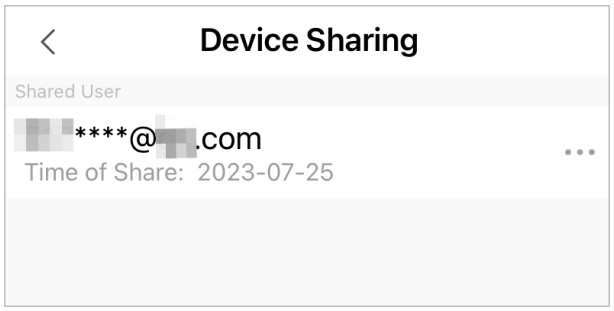
Para los usuarios administradores de DMSS, puede eliminar usuarios generales de DMSS cancelando el uso compartido de dispositivos con ellos en el**Uso compartido de dispositivos**Pantalla. Esta sección utiliza la ruta del > **Uso compartido de dispositivos**como un ejemplo.

Procedimiento

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

Paso 2 En la lista de cuentas de la**Uso compartido de dispositivos**pantalla, seleccione una cuenta y toque .

Figura 5-15 Usuario compartido



Paso 3 Seleccionar**Cancelar compartir**,y luego toca**DE ACUERDO**para cancelar el compartir.

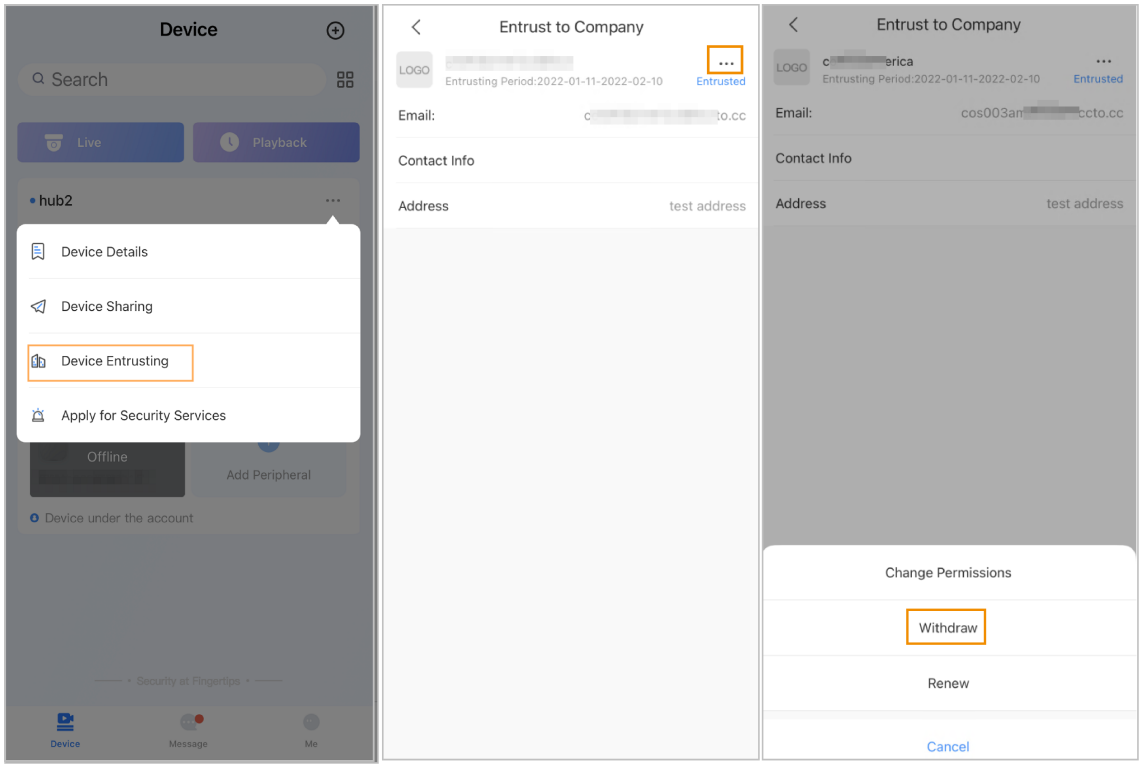
5.6.2.2 Cancelación de la Confianza de la Aplicación

Para los usuarios administradores de DMSS, pueden eliminar un instalador cancelando la aplicación que lo confió.

Procedimiento

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

Figura 5-16 Retirar solicitud de encomienda



Paso 2 En el**Confianza del dispositivo**pantalla, seleccionar ••• > **Retirar**y luego toque**DE ACUERDO**.

Se enviará un mensaje a la cuenta del instalador. Una vez que el instalador lea el mensaje y apruebe su solicitud de cancelación de la aplicación de confianza en Dolynk Care, su aplicación se cancelará.

5.6.2.3 Eliminación de dispositivo

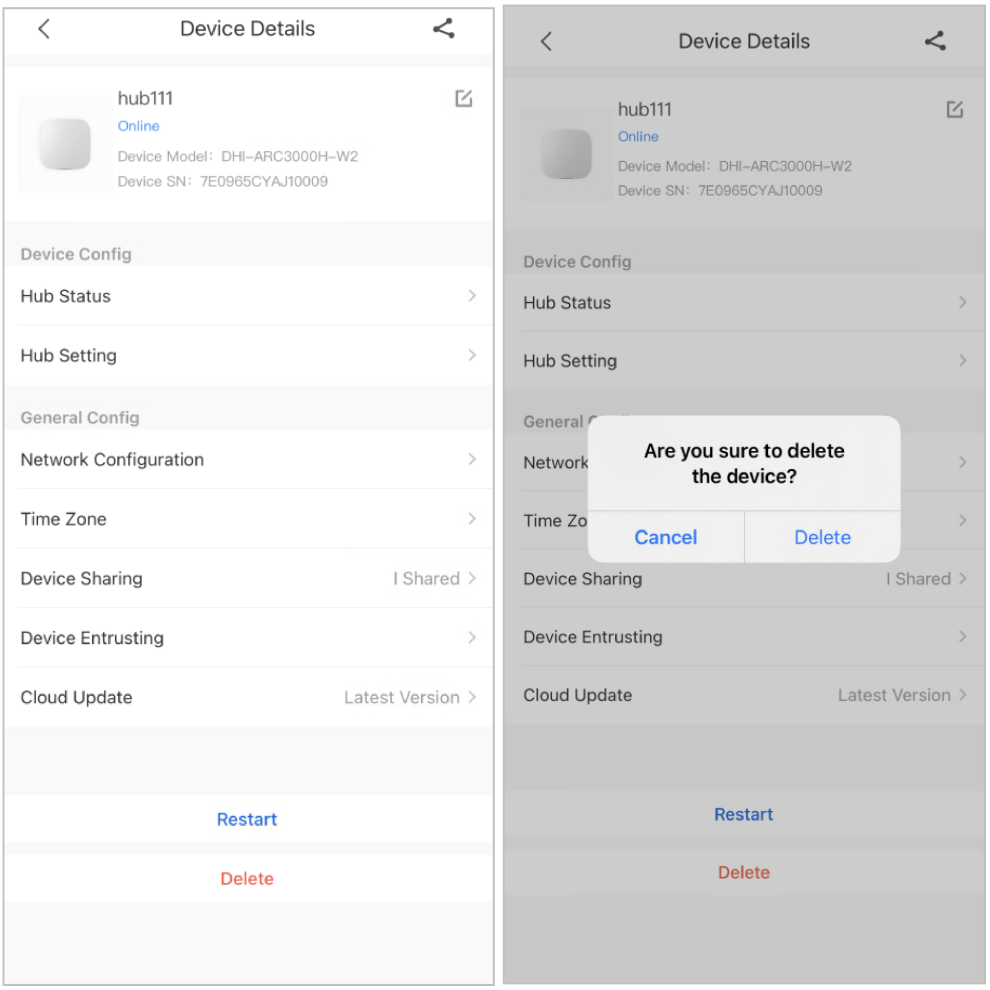
Para los usuarios administradores de DMSS, puede eliminar tanto a los instaladores como a los usuarios generales de DMSS eliminando los dispositivos.

El usuario administrador de DMSS no puede eliminar un instalador si los dispositivos son compartidos por el instalador.

Procedimiento

Paso 1 En el**Dispositivo**pantalla, seleccionar ••• > **Detalles del dispositivo**.

Figura 5-17 Eliminar el dispositivo



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

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

6 Operaciones generales

El usuario de nivel 2 o 3 tiene permiso para armar y desarmar el sistema. En esta sección se 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 contexto

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 obtener más información sobre cómo agregar los periféricos, consulte el manual del usuario del dispositivo correspondiente.

Paso 2 Armar y desarmar 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 cronograma.

6.1 Armado y desarmado individual

Puede armar y desarmar los detectores en una sola área.

Procedimiento

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**: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**:Apagar el sistema de seguridad. Lo opuesto a armarlo.
- **desactivar**:Cerrar la pantalla actual.

6.2 Armado y desarme global

Prerrequisitos

Asegúrese de haber habilitado la**Armado y desarme global**Función. En la pantalla central, seleccione  >**Configuración del concentrador**y luego habilitar**Armado y desarme global**.

Información de contexto

Puede armar y desarmar los detectores en todas las áreas.

Procedimiento

Paso 1 Vaya a la pantalla central.

Paso 2 Seleccione 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 individual" 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 llavero y el teclado correspondientes.

6.4 Armado y desarmado programado

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

Procedimiento

Paso 1 En la pantalla central, seleccione > **Configuración del concentrador**>**Armado/desarmado programado**.

Paso 2 En el**Armado/desarmado programado**pantalla, toque**Agregar**y 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 comando**:Seleccione de**Hogar**,**Lejos**, y**Desarmar**.
- **Tiempo**:Establecer un tiempo de armado.

  Para aplicar el tiempo de armado a otros días, toque**Repetir**y selecciona los días que desees.
- **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 (periféricos)

No.	Razón	Descripción
1	Pérdida de módulo	El periférico estaba desconectado.
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	exAbierto	La cubierta posterior del dispositivo externo estaba abierta.
6	Manosear	Se activó la alarma de manipulación periférica.
7	Batería baja	Se detectó batería baja en el dispositivo.
8	Pérdida de potencia primaria	Se detectó una falla en la alimentación principal del periférico.
9	Pérdida de batería	Se detectó una falla en la batería.
10	Sobrevoltaje	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 hub 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 una falla en la 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 en la red celular	Se detectó una falla en la ruta de transmisión de alarma (falla de la red celular).
11	Falla 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 de eventos y descripción de SIA

Apéndice Tabla 2-1 Códigos de eventos SIA y descripción

No.	Evento	Código CID	Descripción
1	Movimiento detectado	130	Alarma antirrobo.
		133	Alarma (segura) 24 horas.
		134	Alarma de entrada/salida.
2	Acción de apertura Detectado/Cerrando Acción detectada	130	Alarma antirrobo.
		133	Alarma (segura) 24 horas.
		134	Alarma de entrada/salida.
3	El contacto externo fue Abierto/Externo El contacto fue cerrado	130	Alarma antirrobo.
		133	Alarma (segura) 24 horas.
		134	Alarma de entrada/salida.
4	Alarma de coacción	121	Alarma de coacción.
5	El botón de pánico era Apretado	122	Alarma de pánico (silenciosa).
		123	Alarma de pánico (audible).
6	Alarma de intrusión	130	Alarma antirrobo.
		133	Alarma (segura) 24 horas.
		134	Alarma de entrada/salida.
7	Alarma de incendios	110	Alarma de incendios.
8	Fuga de gas detectada	151	Alarma de gas detectado.
9	Botón de alarma médica Fue presionado	100	Alarma médica.
10	El botón de atraco era Apretado	122	Alarma de pánico (silenciosa).
		123	Alarma de pánico (audible).
11	Detectada rotura de cristal	130	Alarma antirrobo.
		133	Alarma (segura) 24 horas.
		134	Alarma de entrada/salida.
12	Inclinación detectada	130	Alarma antirrobo.
		133	Alarma (segura) 24 horas.
		134	Alarma de entrada/salida.
13	Choque detectado	130	Alarma antirrobo.
		133	Alarma (segura) 24 horas.
		134	Alarma de entrada/salida.
14	Alarma de cable trampa/ Alarma de trampa detenida	131	Alarma perimetral

No.	Evento	Código CID	Descripción
15	Se abrió la tapa del panel de control/Panel de control La tapa estaba cerrada	137	Manosear.
16	La tapa periférica era Tapa abierta/periférica Estaba cerrado	137	Manipulación del sensor.
17	La tapa externa era Tapa abierta/externa Estaba cerrado	137	Manipulación del sensor.
18	Fuga de agua detectada / Fuga de agua detenida	154	Fuga de agua.
19	Batería baja/batería Nivel restaurado	302	Batería baja del sistema.
20	Falla de la batería/Batería Restaurado	311	Batería faltante/muerta.
21	Falla de alimentación principal/ Se restableció la energía principal	301	Pérdida de CA.
22	Interferencia de RF	344	Detección de interferencias en el receptor de RF.
23	Transmisión de alarma Fallo del sistema/Restaurado	350	Problemas de comunicación.
24	Transmisión de alarma Ruta: Red cableada/Wi- Falla de Fi/Restaurado	350	Problemas de comunicación.
25	Transmisión de alarma Ruta: Red celular Falla/Restaurado	350	Problemas de comunicación.
26	Conexión periférica Perdido/Periférico Conexión restaurada	355	Pérdida de supervisión - RF.
27	El centro está desconectado/el centro está en línea	356	Pérdida de la votación central
28	Batería periférica baja/Nivel de batería periférica restaurado	302	Batería baja del sistema.
29	Batería periférica Batería periférica/falla restaurada	311	Batería faltante/muerta.
30	Alimentación principal periférica Falla/Energía principal periférica restablecida	301	Pérdida de CA.
31	Conexión RF-HD Falló/RF-HD Conexión restaurada	354	Fallo en la comunicación del evento.

No.	Evento	Código CID	Descripción
32	Dispositivo bloqueado y Desbloqueado	501	Deshabilitar lector de acceso.
33	Protección contra sobretensiones Activado/Sobrevoltaje Protección restaurada	319	Sobretensión en la fuente de alimentación.
34	Protección contra sobrecorriente Sobrecorriente activada Protección restaurada	312	Sobrecorriente en la fuente de alimentación.
35	Protección contra sobrecalentamiento Activado/Sobrecalentamiento Protección restaurada	318	Sobrecalentamiento de la fuente de alimentación.
36	Temperatura alta/ Temperatura normal	158	Alta temperatura.
37	Baja temperatura/ Temperatura normal	159	Baja temperatura.
38	Armado	400 (aplicación)	Abrir/Cerrar.
		401 (Teclado numérico)	O/C por usuario.
		403 (Programado armamento)	A/C automático.
		407 (Llavero)	Armado/desarmado remoto.
		408	Brazo rápido.
		409	Interruptor de llave O/C
39	Desarmado	400 (aplicación)	Abrir/Cerrar.
		401 (Teclado numérico)	O/C por usuario.
		403 (Programado armamento)	A/C automático.
		407 (Llavero)	Armado/desarmado remoto.
		409	Interruptor de llave O/C
40	Modo hogar activado	441	QUEDA armada.
		442	Interruptor de llave armado STAY
41	Armado fallido	454 (Fallo de armado)	No se pudo cerrar.
		455 (Armado programado) falla)	Falló el autoarmado.
		457 (Fallo de armado con retardo de salida)	Error de salida (usuario).
42	Armado con fallas	450	Excepción O/C.
43	Temporalmente Desactivado/ Reactivado	502	Desactivado temporalmente.

No.	Evento	Código CID	Descripción
44	Deshabilitado temporalmente Notificaciones para el Tapa/Habilitado Notificaciones para la tapa	503	Desactivado temporalmente.
45	El informe de prueba fue Activado manualmente	601	Informe de prueba de disparo manual.
46	Informe de prueba periódica	602	Informe de prueba periódica.

Apéndice 3 Recomendaciones de ciberseguridad

La ciberseguridad es más que una palabra de moda: es algo que concierne a todos los dispositivos 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 conectados los hará menos susceptibles a los ataques. A continuación, se ofrecen algunos consejos y recomendaciones de Dahua sobre cómo crear un sistema de seguridad más seguro.

Acciones obligatorias a 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 ni 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 esté conectado a la red pública, se recomienda habilitar la función de "comprobación automática de actualizaciones" para obtener información oportuna sobre las actualizaciones de firmware publicadas por el fabricante.
- Le sugerimos que descargue y utilice la última versión del software del cliente.

Recomendaciones “deseables de tener” para mejorar la seguridad de la red de su dispositivo:

1.Protección física

Le sugerimos que proteja físicamente el dispositivo, especialmente los dispositivos de almacenamiento. Por ejemplo, coloque el dispositivo en una sala de computadoras y un gabinete especiales e implemente un control de acceso y una gestión de claves bien hechos para evitar que personal no autorizado realice contactos físicos, como dañar el hardware, conectar sin autorización dispositivos extraíbles (como un disco flash USB, un puerto serial), etc.

2.**Cambie las contraseñas periódicamente**

Le sugerimos que cambie sus contraseñas periódicamente para reducir el riesgo de que sean adivinadas o descifradas.

3.**Establecer y actualizar contraseñas Restablecer información oportunamente**

El dispositivo admite la función de restablecimiento de contraseña. Configure a tiempo la información relacionada con el restablecimiento de contraseña, incluido el buzón de correo del usuario final y las preguntas de protección de contraseña. Si la información cambia, modifíquela a tiempo. Al configurar las preguntas de protección de contraseña, se recomienda no utilizar aquellas que se puedan adivinar fácilmente.

4.**Habilitar bloqueo de cuenta**

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

5.**Cambiar el puerto 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 y 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 pueda visitar el servicio web a través de un canal de comunicación seguro.

7.**Vinculación 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 ARP.

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

Según los requisitos comerciales y de gestión, agregue usuarios de manera razonable y asígneles un conjunto mínimo de permisos.

9.**Desactivar servicios innecesarios y elegir modos seguros**

Si no es necesario, se recomienda desactivar algunos servicios como SNMP, SMTP, UPnP, etc., para reducir 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 autenticación seguras.
- SMTP: elija TLS para acceder al servidor de buzón.
- FTP: elija SFTP y configure contraseñas seguras.
- Punto de acceso AP: elija el modo de cifrado WPA2-PSK y configure contraseñas seguras.

10.**Transmisión de audio y vídeo encriptados**

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 que los datos de audio y video sean robados durante la transmisión.

Recordatorio: la transmisión cifrada provocará cierta pérdida en la eficiencia de transmisión.

11.**Auditoría segura**

- Comprobar usuarios en línea: le sugerimos que compruebe periódicamente los usuarios en línea para ver si el dispositivo ha iniciado sesión sin autorización.
- Comprobar el registro del dispositivo: al ver los registros, puede conocer las direcciones IP que se utilizaron 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 un período prolongado, se recomienda que habilite la función de registro de red para garantizar que los registros críticos se sincronicen con el servidor de registro de red para realizar el 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 la red externa.
- La red debe estar dividida y aislada de acuerdo con las necesidades reales de la red. Si no hay requisitos de comunicación entre dos subredes, se recomienda utilizar VLAN, GAP de red y otras tecnologías para dividir la red, a fin de lograr el efecto de aislamiento de la red.
- Establecer 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 a los que se les permite acceder al 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 últimas recomendaciones de seguridad.

ENABLING A SAFER SOCIETY AND SMARTER 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