Centro de alarmas

Manual de usuario

ZHEJIANG DAHUA VISIÓN TECNOLOGÍA CO.LTD. V2.0.3

Prefacio

General

Este manual presenta la instalación, funciones y operaciones del centro de alarma (en adelante, el "centro"). Lea atentamente antes de usar el dispositivo y guarde el manual en un lugar seguro para consultarlo en el futuro.

Instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

Palabras de advertencia	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 del texto.

Revisión histórica

Versión	Versión del software	Contenido de revisión	Liberar Tiempo
V2.0.3	V1.001.0000007.0.R.231016	• Se agregó PIN, datos de roaming, usuario del teclado, retraso en la falla de energía principal y selección de idioma del concentrador. • Se actualizaron los códigos de eventos SIA y los eventos de falla de armado y descripción.	Noviembre 2023
V2.0.2	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 categoría ATS: SP2/DP2 en la especificación técnica.	Agosto 2023

Versión	Versión del software	Contenido de revisión	Liberar Tiempo
V2.0.1	—	• 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 2023
V2.0.0	—	• Configuraciones de red agregadas. • Se agregaron descripciones y eventos de falla de armado. • Se agregaron códigos y descripciones de eventos SIA.	Noviembre 2022
V1.1.0	—	• Se agregaron operaciones en la aplicación COS Pro y DMSS. • Gestión de usuarios agregada. • Imágenes actualizadas. • Descripciones actualizadas de los parámetros.	Febrero 2022
V1.0.0	—	Primer lanzamiento.	Octubre 2021

Aviso de protección de privacidad

Como usuario del dispositivo o controlador de datos, puede recopilar datos personales de 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 sobre la existencia del área de vigilancia y proporcionar la información de contacto requerida.

Acerca del Manual

- El manual es sólo para referencia. Pueden encontrarse ligeras diferencias entre el manual y el producto.
- No somos responsables de las pérdidas incurridas debido a la operación del producto de manera que no cumpla con el manual.
- El manual se actualizará de acuerdo con las últimas leyes y 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 sólo para referencia. Es posible que se encuentren ligeras diferencias entre la versión electrónica y la versión en papel.
- Todos los diseños y software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones de productos pueden provocar que aparezcan algunas diferencias entre el producto real y el manual. Comuníquese con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria.
- Pueden existir errores en la impresión o desviaciones en la descripción de las funciones, operaciones y datos técnicos. Si hay alguna duda o disputa, nos reservamos el derecho de dar una explicación final.
- Actualice el software del lector o pruebe otro software de lectura convencional si no se puede abrir el manual (en formato PDF).

- Todas las marcas comerciales, marcas comerciales registradas y nombres de empresas que aparecen en este manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, comuníquese con el proveedor o con 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 dar una explicación final.

Salvaguardias 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 operación

- 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 las condiciones permitidas de humedad y temperatura.
- Evite que los líquidos salpiquen o goteen sobre el dispositivo. Asegúrese de que no haya objetos llenos de líquido encima del dispositivo para evitar que fluyan líquidos hacia él.
- No desmonte el dispositivo.

requerimientos de instalación

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

- Observe todos los procedimientos de seguridad y use el equipo de protección requerido proporcionado para su uso mientras trabaja en alturas.
- No exponga el dispositivo a la luz solar directa ni a fuentes de calor.
- No instale el dispositivo en lugares húmedos, polvorientos o con humo.
- Instale el dispositivo en un lugar bien ventilado y no bloquee el ventilador del dispositivo.
- Utilice el adaptador de corriente o la fuente de alimentación del estuche proporcionada por el fabricante del dispositivo.
- La fuente de alimentación debe cumplir con los requisitos de ES1 en el estándar IEC 62368-1 y no ser superior a PS2. Tenga en cuenta que los requisitos de suministro de energía están sujetos a la etiqueta del dispositivo.
- Conecte los aparatos eléctricos de clase I a una toma de corriente con protección a tierra.

Tabla de contenido

1. Introducción

1.1 Descripción general

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

1.2 Especificaciones técnicas

Esta sección contiene las especificaciones técnicas del dispositivo. Consulte los que corresponden a su 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); Modo de espera único con doble SIM
	LTE	SIM única (GSM: 900/1800 MHz, WCDMA: B1/B5/B8, LTE-FDD: B1/B3/B5/B7/B8/B20, LTE-TDD:B38/B40/B41); Modo de espera único con doble SIM
	Batería	Puerto de batería de 12 V
	Luz indicadora	1 para múltiples estados (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) Solo disponible en modelos 2G y 4G.
	Llamada telefónica Notificación	Sí (hasta 5 números de teléfono) Solo 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 en la nube
	Configuración Método	Aplicación
	Armar y desarmar Método	Aplicación, teclado, llavero, horario

Tipo	Parámetro	Descripción	
	Número de Periféricos	Máx. 150 periféricos inalámbricos (8 cámaras PIR, 6 sirenas, 4 repetidores, 8 teclados, 64 mandos inalámbricos, 256 tarjetas MIFARE One (8 tarjetas por usuario de teclado))	
	Área	32 áreas (habitaciones)	
	Usuarios	33 usuarios de aplicaciones (31 usuarios generales, 1 usuario administrador y 1 instalador) y 32 usuarios de teclado	
	Fuerza Gestión	Cambio automático 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 fallo de voltaje de la batería.	
	Registros de eventos	Máx. 5000	
	Fallo de alimentación Protección para Configurado Parámetros	Sí	
	Gestión de usuarios	Máx. 8 usuarios: 1 instalador, 1 administrador, 6 usuarios generales	
	Consulta	Búsqueda de mensajes push, estado del dispositivo y versión del programa. Detectando la intensidad de la señal.	
RF	Frecuencia de carga	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-ARCO3000H-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 un espacio abierto	DHI-ARC3000H-FW2/DHI-ARC3000H-GW2/DHI-ARCO3000H-W2: Hasta 1.200 m (3.937,01 pies) en un espacio abierto
	Transmisión Fuerza	DHI-ARC3000H-FW2 (868)/ DHI-ARC3000H-GW2 (868)/ DHI-ARC3000H-W2 (868): Límite de 25 mW	DHI-ARC3000H-FW2/DHI-ARC3000H-GW2/DHI-ARCO3000H-W2: Límite de 10 mW
	Comunicación Mecanismo	bidireccional	
	Modo de encriptación	AES128	
	Frecuencia Saltando	Sí	
	Interferencia de radiofrecuencia Detección	Para una detección de 60 segundos, si la interferencia dura más de 30 segundos, el sistema informa la información de interferencia de RF.	
	Wifi	2,4G	
Fuerza Suministrar	Tipo de PS	Escribe un	

Tipo	Parámetro	Descripción
	Poder principal	12 VCC, 1,5 A
	Capacidad de la batería	2x 3,6 V/2150 mAh
	Batería en espera	Hasta 12h Cuando se cumplen las siguientes condiciones, el tiempo de espera puede llegar a 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
	Máx. actual disponible	3,5 A
	Fuerza Consumo	Máx. 15W
	Actual Consumo	Normal: 220 mA; alarma: 300 mA
	Bateria BAJA Umbral de batería	3,5 VCC
	Restauración de batería Límite	3,7 VCC
	Voltaje de liberación	< 3,358 voltios
	Recarga de batería Tiempo	80% aprox. 15 horas
Audio y Video	Entrada de video	IPC de 4 canales (simplemente obtenga y reenvíe eventos de alarma de IPC y los videos de alarma correspondientes)
ARCO Señalización	Categoría ETA	DP2/SP2 (LAN/WiFi y GPRS/4G)
	Reconocimiento Operación	Pasar por
	Protocolos	SIA-DC09
	Primario Ruta de transmisión	LAN/Wi-Fi (NO 50136-2)
	Secundario Ruta de transmisión	GPRS/4G
	Notificación Equipo	C/E/F

Tipo	Parámetro	Descripción	
Certificaciones		DHI-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-ARCO3000H-W2: FCC CE

Tabla 1-2 Categoría ATE

COMIÓ Categoría	Informes Tiempo	Protocolos	Dispositivos de comunicación			Comunicación Dispositivo a utilizar
			PSTN	2G/3G	IP	
SP2	25 horas	Estándar	√			El cheque marcado comunicación dispositivo
SP3	30 minutos	Estándar		√	√	Sólo uno de los dos check marcado comunicación dispositivos
SP4	3 minutos	cifrado		√	√	Sólo uno de los dos check marcado comunicación dispositivos
SP5	90s	cifrado		√	√	Sólo uno de los dos check marcado comunicación dispositivos
DP1	25 horas	Estándar	√	√	√	Sólo dos de los tres cheques marcados comunicación dispositivos
DP2	30 minutos	Estándar	√	√	√	Sólo dos de los tres cheques marcados comunicación dispositivos

COMIÓ Categoría	Informes Tiempo	Protocolos	Dispositivos de comunicación			Comunicación Dispositivo a utilizar
			PSTN	2G/3G	IP	
DP3	3 minutos	cifrado		√	√	los dos cheque marcado comunicación dispositivos
DP4	90s	cifrado		√	√	los dos cheque marcado comunicación dispositivos

ATE: Equipo de transmisión de alarma.

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

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

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

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

Dispositivos de comunicación: Dispositivos de comunicación implementados.

Dispositivos de comunicación que se utilizarán: indica la cantidad y qué dispositivos de comunicación se utilizarán según la categoría ATE.

Tabla 1-3 Especificaciones técnicas

Especificación técnica	Descripción
Clasificación ACE	Escribe un
Clase ambiental	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% (HR)
Peso neto	0,38 kg (0,84 libras)
Peso bruto	0,8 kg (1,76 libras)
Caja	PC + ABS

1.3 Lista de verificación

Verifique el paquete de acuerdo con la siguiente lista de verificación. Si encuentra algo dañado o perdido, comuníquese con el servicio de atención al cliente.

Figura 1-1 Lista de verificación

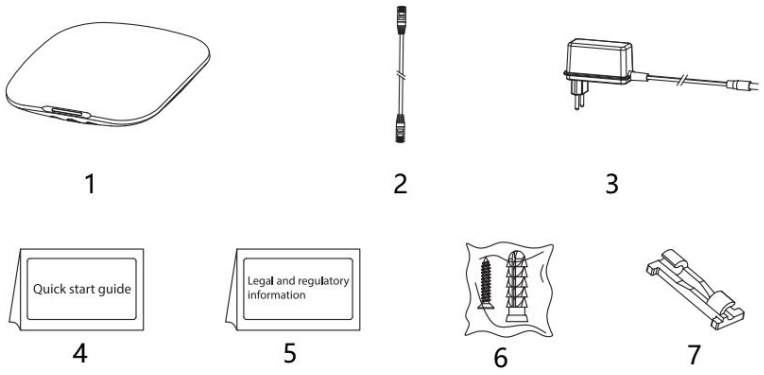


Tabla 1-4 Lista de verificación

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

2 Diseño

2.1 Apariencia

Figura 2-1 Apariencia

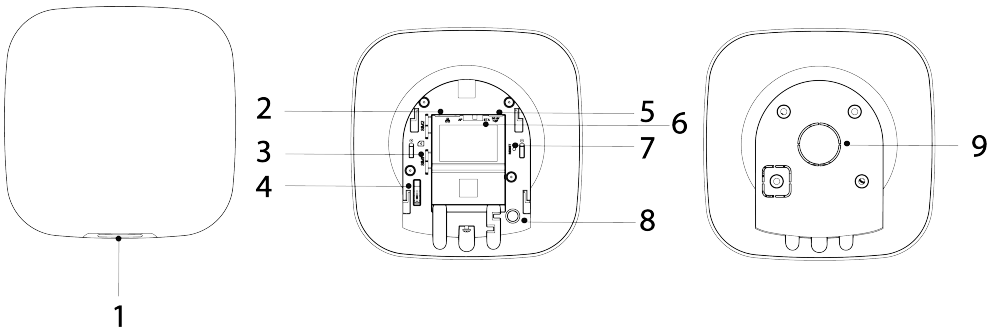


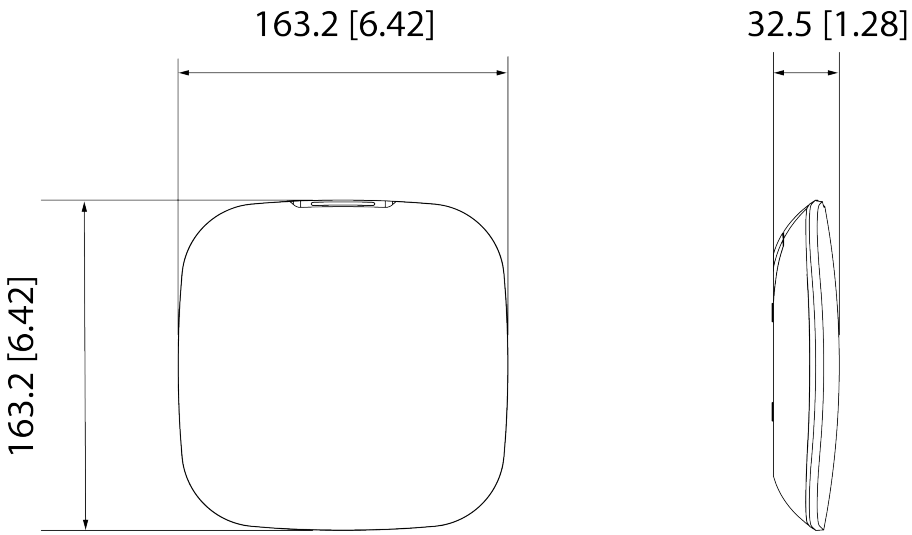
Tabla 2-1 Estructura

No.	Nombre	Descripción
1	Indicador	● Parpadea en verde lentamente: modo de sensibilidad reducida. ● Parpadea en verde: el concentrador comienza a funcionar. ● Amarillo fijo: no se pudo conectar a la nube. ● Verde fijo: modo desarmado. ● Azul fijo: modo de armado. ● Parpadea en rojo: se activó un evento de alarma. ● Parpadea en amarillo: Se ha detectado una avería. ● Parpadea en azul: ejecutando la configuración de AP o el concentrador se está emparejando con periféricos. ● Parpadea rápidamente en azul: Modo de emisión de tarjeta.
2	Toma de cable Ethernet	Conecte el concentrador a Ethernet.
3	Ranura para micro SIM 1/2	Instale la tarjeta principal en la primera ranura y la tarjeta de respaldo en la segunda ranura. ● Admite tarjetas SIM duales y modo de espera único. ● Las tarjetas SIM permiten que el concentrador utilice datos móviles y envíe notificaciones de alarma. ● Las tarjetas SIM no funcionarán hasta que se haya completado la configuración de la red. ● La función SIM solo está disponible en modelos selectos.
4	Botón de manipulación	Cuando se suelta el interruptor de manipulación, se activará la alarma de manipulación.
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	Boton de encendido / apagado	Mantenga presionado el botón durante 2 segundos para encender o apagar el concentrador.
9	Contraportada	Si se abre la cubierta trasera, se activará la alarma de manipulación.

2.2 Dimensiones

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



3 inicio

3.1 Usuarios

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

Nivel de acceso de usuario

Tabla 3-1 Nivel de acceso de usuario

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

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

Flujo de negocios

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

Figura 3-1 Flujo de negocios (usuario DMSS)

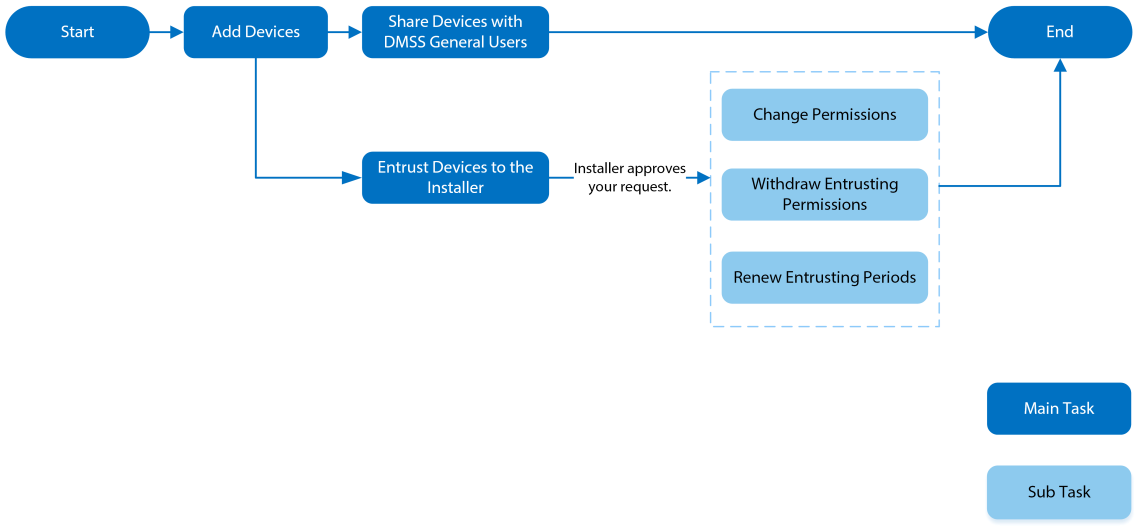
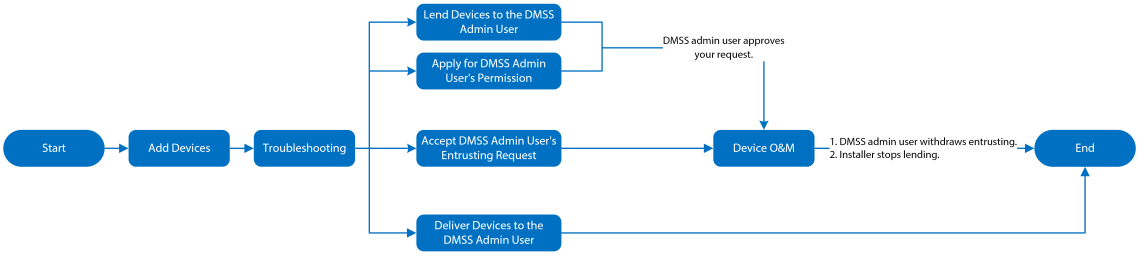


Figura 3-2 Flujo de negocios (instalador)



3.2 Proceso de operación

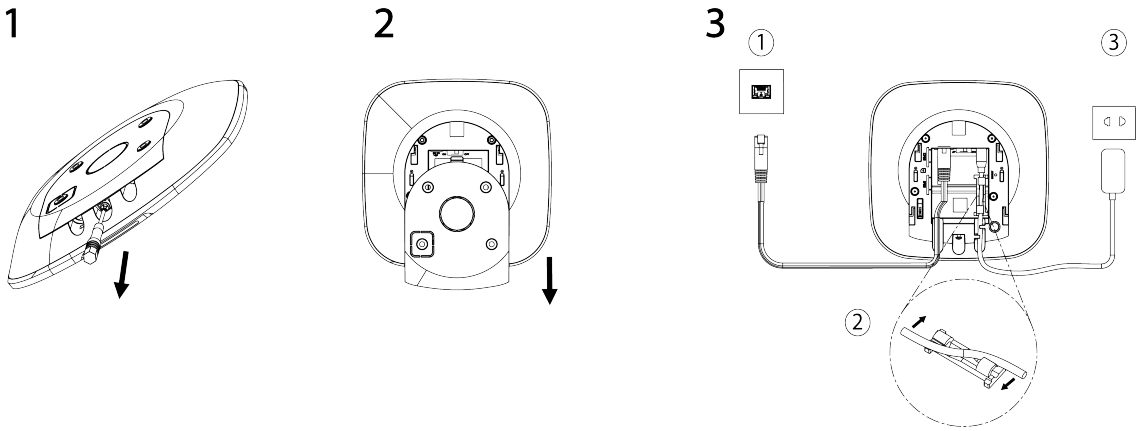
Siga los procedimientos a continuación para encender el sistema de alarma inalámbrico.

Figura 3-3 Proceso de operación

Encendido

Conecte el concentrador a Ethernet y enciéndalo.

Figura 3-4 Encendido



Agregar dispositivos

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

Instalación del concentrador

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

- Al aire libre.
- Lugares cercanos a objetos metálicos que provoquen atenuación y blindaje de la señal de radio.
- Lugares con señal GSM débil.

- Lugares cercanos a fuentes de interferencias de radio que se encuentren a menos de 1 metro de distancia del router y de 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 para los tornillos y luego taladrelos en la placa de montaje.
2. Coloque los pernos de expansión en los orificios.
3. Fije la placa de montaje a la pared y luego alinee los orificios para tornillos de la placa con los pernos de expansión.
4. Fije la placa de montaje con tornillos autorroscantes ST4 × 25 mm.
5. Coloque el centro de la alarma en la placa de montaje de arriba a abajo.
6. Fije el centro de la alarma y la placa de montaje con tornillos de cabeza avellanada M3 × 8 mm.

Configurar el concentrador

Configure el concentrador en la aplicación DoLynk Care y DMSS.

Armando el sistema de alarma

Puede usar el teclado, el control remoto y la aplicación para armar su sistema. Después de enviar un comando de armado a la aplicación DoLynk Care y DMSS, el sistema verificará el estado del sistema. Si el sistema tiene una falla, deberá elegir si desea forzar el armado. Para obtener detalles sobre los periféricos, consulte el manual de 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. Proporciona funciones que incluyen administración del sitio, administración del funcionamiento y del estado del dispositivo, revisión de confianza del dispositivo y más. Para más detalles, consulte*Manual del usuario de la aplicación Dolynk Care*.

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

4.1 Iniciar sesión en Dolynk Care

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

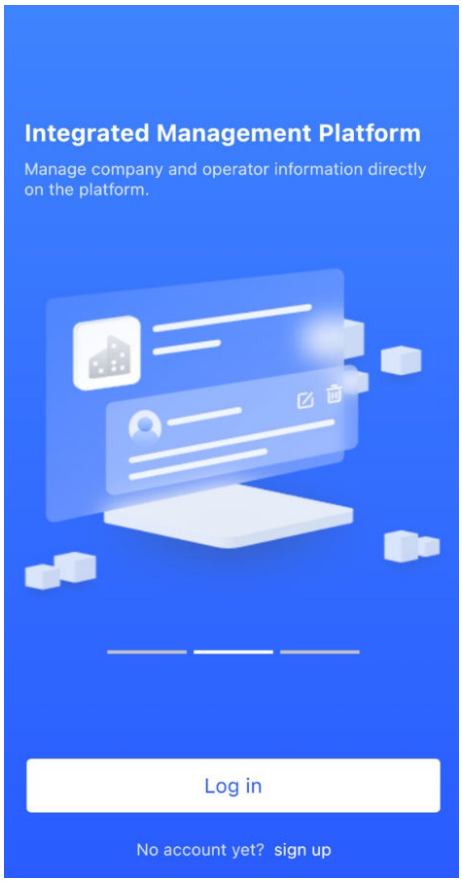
Procedimiento

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

Los usuarios de Android pueden ir a Google Play para buscar la aplicación.

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

Figura 4-1 Iniciar sesión



Paso 3 Crea una cuenta.

1. Sobre el**Acceso**pantalla, toque**¿No tienes cuenta aún? inscribirse**.
2. Sobre 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**:Ingrese la dirección detallada de su empresa.
   - **código de invitación**:Ingrese el código de invitación, que puede obtener del revendedor o representante de ventas.
   - **Correo electrónico**:Ingrese su dirección de correo electrónico.
   - **Contraseña**:Introducir la contraseña.
   - **Código de verificación**:Grifo**Enviar**, marque su casilla de correo electrónico para recibir un código de verificación y luego ingrese el código en**Código de verificación**.
3. Lee el**política de privacidad**y**Acuerdo del 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 regresa al**Acceso**pantalla. Ingrese su

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

- Para nuevos clientes, se necesita la aprobación de la solicitud de cuenta. Pasarán entre 1 y 3 días para recibir un correo electrónico de aprobación de la cuenta. Después de eso, puedes iniciar sesión en la aplicación con tu cuenta.
- Algunos clientes afiliados no necesitan ser aprobados para registrarse y obtener 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 el dispositivo esté conectado a la corriente y a la red. Puede agregar dispositivos de alarma, incluidos concentradores y múltiples periféricos, a la aplicación.

4.2.1 Agregar el concentrador

El concentrador se puede agregar en**Modo 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.

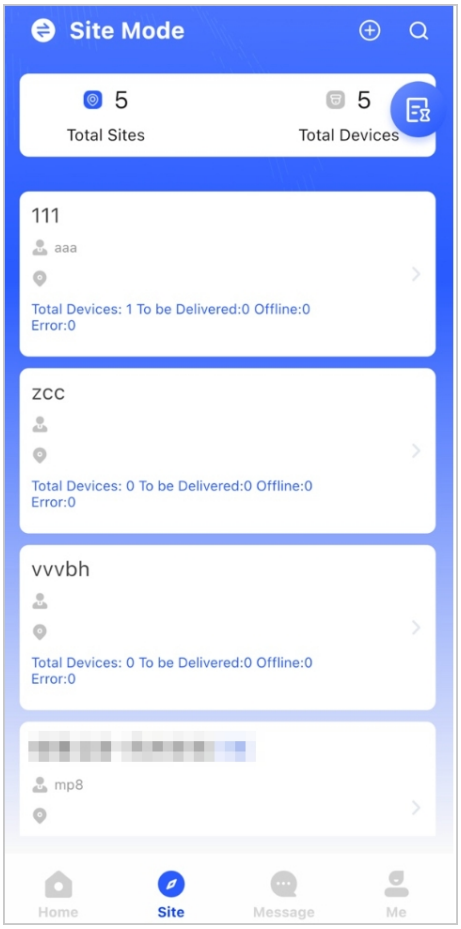
4.2.1.1 Agregar por SN o Código QR

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 Sobre el**Hogar**pantalla, toque para ir a la**Sitio**pantalla.

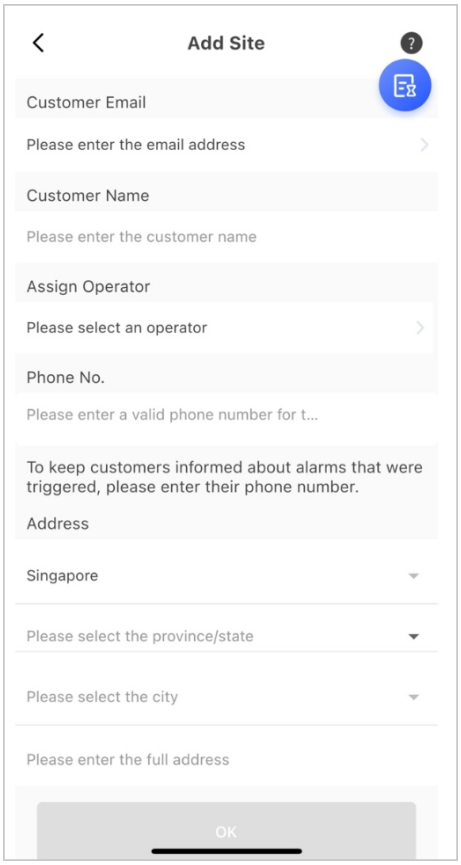
Figura 4-2 Sitio



Paso 2 Grifo para agregar un nuevo sitio.

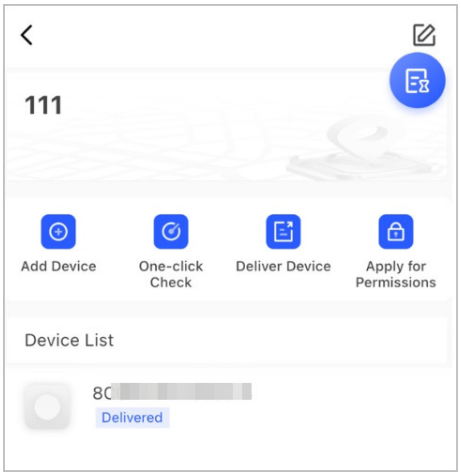
Ingrese la información del sitio y luego toque**DE ACUERDO**para crear el sitio.

Figura 4-3 Agregar sitio



Paso 3 Sobre el**Sitio**pantalla que se creó, toque**Añadir dispositivo**.

Figura 4-4 Agregar dispositivo



Etapa 4 Escanea el código QR del dispositivo o toca**Agregar manualmente**para ingresar manualmente el SN del dispositivo.

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

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

Paso 7 dispositivo. Conéctese a una red inalámbrica o por cable.

- **Inalámbrico**

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

- **cableado**

1. Toque**cableado**en la esquina superior derecha y luego**cableado**se convierte**Inalámbrico**.
2. Conecte el dispositivo a la corriente y a la red, y luego toque**Próximo**.

Si falla, repita los procedimientos anteriores.

Paso 8 Si el concentrador que está agregando no está inicializado, ingrese la contraseña, 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

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

Procedimiento

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

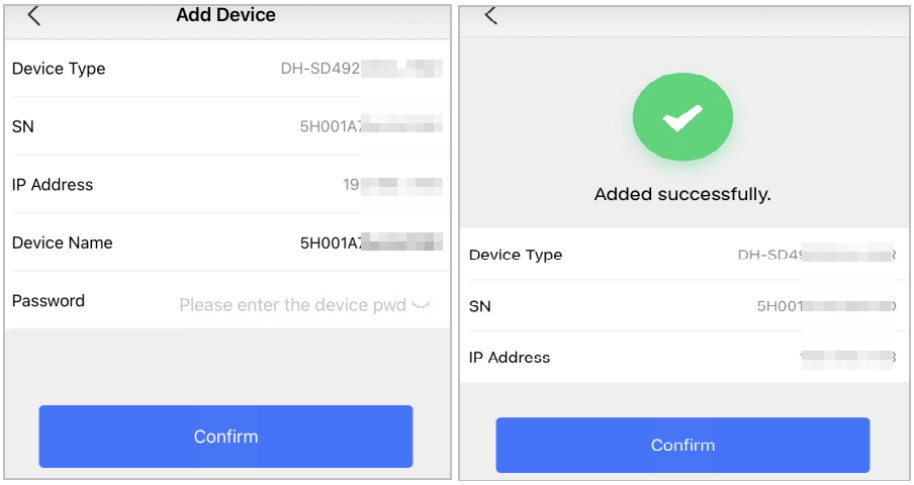
Paso 2 toque**Añadir dispositivo**para agregar un dispositivo.

Figura 4-5 Agregar un dispositivo

Paso 3 Grifo**Búsqueda de LAN**.

Etapa 4 En**Añadir 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. La sección utiliza el detector de puertas como ejemplo. Para obtener detalles sobre cómo agregar periféricos, consulte los manuales de usuario de los respectivos periféricos.

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

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 que aparecen en pantalla, active el detector de puerta y luego toque**Próximo**para agregarlo al centro.

Etapa 4 Espere el emparejamiento.

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

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

4.3 Administrar 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

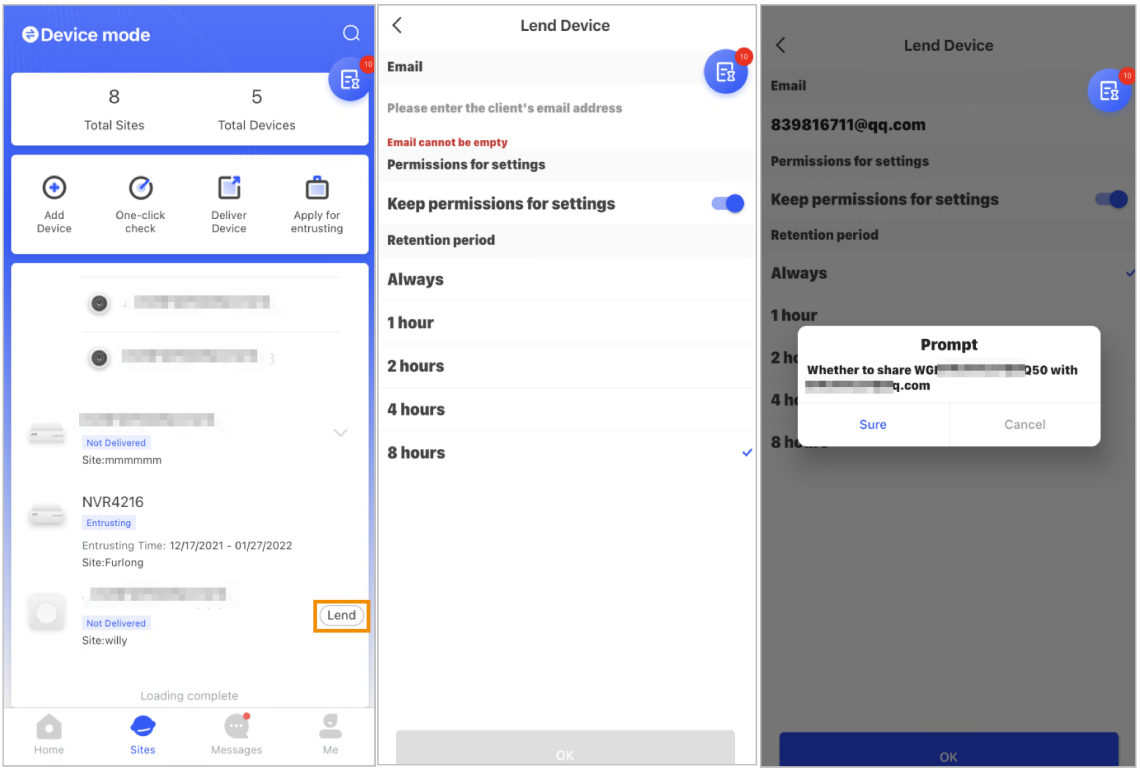
Según las certificaciones EN50131, el instalador puede prestar el concentrador al usuario administrador de DMSS. Luego, el instalador debe solicitar permisos del usuario administrador de DMSS, como configuración del dispositivo, operaciones de armado y desarmado y administración de usuarios.

Asegúrese de que otras cuentas no hayan agregado el centro.

Procedimiento

Paso 1 Sobre el**Hogar**pantalla, toque y luego irá 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

Etapa 4 electrónico del usuario administrador de DMSS.

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

Paso 6 **Confirmar**.

Paso 7 Sobre el pantalla, toque**Mensaje personal**, puede ver mensajes para ver si el El usuario administrador de DMSS acordó aceptar su solicitud para compartir con ellos.

Se enviará un mensaje compartido 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 Aceptar solicitudes de encomienda

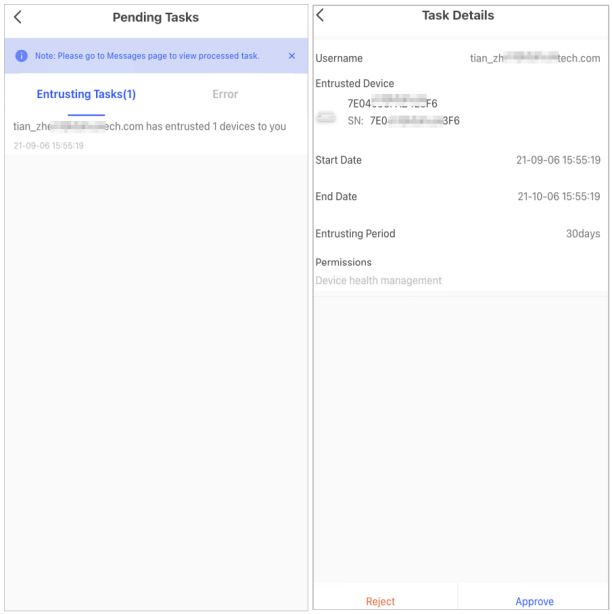
El instalador puede aceptar la solicitud de encomienda del usuario administrador de DMSS para proporcionar servicios de operación y mantenimiento a los usuarios.

Procedimiento

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

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

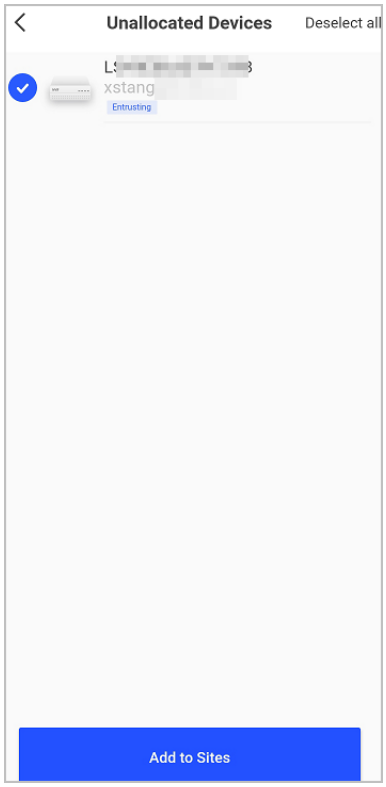
Figura 4-8 Manejar tareas de encomienda



- Aprobar

  1. Toque**Aprobar**,y luego va al**Dispositivos no asignados**pantalla.
  2. Seleccione los dispositivos que se asignarán o toque**Seleccionar todo**,y luego toque**Agregar a sitios**.

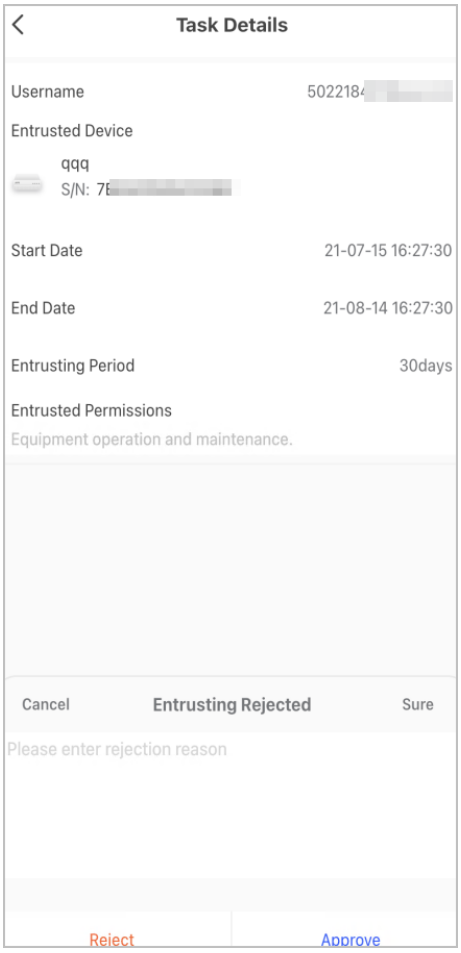
Figura 4-9 Agregar dispositivo a sitios



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

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

Figura 4-10 Rechazar



4.3.2 Eliminar usuarios

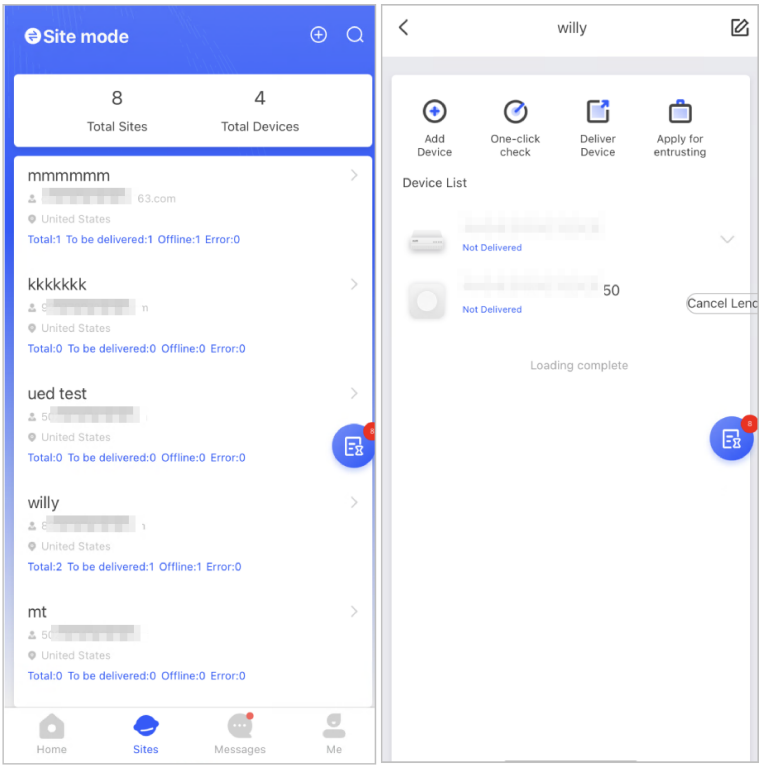
4.3.2.1 Cancelación del préstamo de los dispositivos

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

Procedimiento

Paso 1 Sobre el**Hogar**pantalla, toque y luego irá 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 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 centro 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 Sobre el**Hogar**pantalla, toque y luego irá 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.

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

4.4 Solicitud del permiso del usuario administrador de DMSS

Para los instaladores, pueden agregar el centro directamente a la aplicación Dolynk Care para proporcionar servicios de operación y mantenimiento del dispositivo para los usuarios administradores de DMSS. Tiene permisos por tiempo limitado, incluida la configuración del dispositivo y la administración de usuarios, y debe volver a solicitar el permiso cuando caduque.

Procedimiento

Paso 1 Sobre 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.

Etapa 4 Sobre 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 Sobre el pantalla, toque**Mensaje personal**para ver 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 entregarlos al usuario administrador de DMSS. Los dispositivos confiados y sin conexión no se pueden entregar.

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

Procedimiento

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

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

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

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

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

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

Si los clientes utilizan la cuenta Imou, sus dispositivos no se entregarán correctamente. Y aparecerá un mensaje en el**Hogar**pantalla indicando que la cuenta no tiene

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

4.6 Operación y mantenimiento del estado del dispositivo

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

4.6.1 Comprobación del estado del dispositivo

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

Información de contexto

Las configuraciones para estos se pueden encontrar en**Modo 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 Sobre 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 .

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

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

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

Los dispositivos sin conexión no se pueden verificar.

4.6.2 Configuraciones básicas del dispositivo

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

Procedimiento

Paso 1 Sobre el**Hogar**pantalla, toque ir al**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.

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

Tabla 4-1 Descripción del parámetro

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

Parámetro	Descripción
configuración de la red	Grifo**configuración de la red**para ver la información de su red actual.
Zona horaria	Grifo**Zona horaria**para seleccionar su zona horaria y habilite el horario de verano (DST) si es necesario. ● **Zona horaria**:Seleccione la zona horaria en la que opera el centro. ● **horario de verano**:Seleccione la fecha o semana y luego seleccione la hora de inicio y la hora de finalización.
Compartir dispositivo	Grifo**Compartir dispositivo**para compartir el estado del hub con los demás usuarios.
Actualización en 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 alarma al correo electrónico vinculado. ● Registro de aplicaciones: Seleccionar**Registro**>**Registro de aplicaciones**para ver los registros de alarmas del Dolynk Cuidado. También puedes tocar el**Registro de aplicaciones**pantalla para enviar registros de alarma al correo electrónico vinculado.
Manual de usuario	Grifo**Manual de usuario**para obtener el manual del usuario del centro de alarma.

4.6.2.1 Estado de visualización

Sobre el**Centro**pantalla, seleccione > **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 Wi-Fi	Estado de la conexión a Internet del hub a través de Wi-Fi. Para una mayor confiabilidad, recomendamos instalar el concentrador en lugares con una intensidad de señal de al menos 2 barras. ● : Ultra bajo. ● : Bajo. ● : Moderado. ● : Alto. ● : No.
Nivel de bateria	Muestra la electricidad restante de la batería. ● : Completamente cargado. ● : Suficiente. ● : Moderado. ● : Insuficiente.
Antimanipulación	El modo de manipulación del periférico, que reacciona al desprendimiento del cuerpo.
Estado de energía principal	Muestra el estado de la energía principal.
Estado de conexión GSM/LTE	Estado de la conexión a Internet del hub mediante tarjeta SIM, Wi-Fi y Ethernet. ● : Conectado. ● : Desconectado.
Estado de la conexión Wi-Fi	
Estado de conexión del cable de red	
Estado de la tarjeta SIM	Estado de conexión de la tarjeta SIM. ● : La tarjeta SIM 1 está activa. ● : La tarjeta SIM 2 está activa. ● : Sin tarjeta SIM.
Versión del programa	La versión del programa del hub.

4.6.2.2 Configurar el concentrador

Sobre el**Centro**pantalla, seleccione > **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 está desarmado. ● **Agregar usuarios**:Grifo para agregar un usuario. Ingrese su nombre de usuario, código de acceso y código de acceso de coacción, y luego seleccione los permisos de armado y desarmado para la sala. ◇ El código de acceso y el código de coacción deben tener entre 4 y 6 ◇ dígitos. La contraseña de coacción es opcional. ◇ Se pueden crear hasta 32 usuarios. El primer usuario creado es el usuario administrador de forma predeterminada. Todos los permisos están disponibles para ellos. ● **Eliminando usuario**:Seleccione el usuario y luego deslice el dedo hacia la izquierda para eliminarlo. El usuario administrador debe ser el último en ser eliminado. ● **Modificar 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 la tarjeta del teclado para ingresar al proceso de vinculación dentro de 30 segundos. Si la información de la tarjeta se reconoce correctamente, la identificación de la tarjeta se mostrará en la página de información del usuario y luego el teclado emitirá un pitido. Luego de guardar las configuraciones, la tarjeta tendrá los permisos de usuario. Se pueden vincular hasta 8 tarjetas a un usuario. ● **Eliminar tarjeta**:Seleccione la tarjeta y luego deslícela hacia la izquierda para eliminarla.
Armado global/ Encantador	Arma o desarma todos los detectores en todas las áreas con un solo toque.
Programar armado/ Encantador	Armar o desarmar las áreas según cronograma. ● **Área**:Seleccione el área en la que opera el centro. ● **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 centro. ● **Repetir**:Copie el cronograma de armado o desarmado. ● **Armado a la fuerza**:Puede armar el sistema cuando ocurren errores en las zonas.
Configuración de tono de llamada	El tono de llamada al entrar o salir del modo de armado.

Parámetro	Descripción
Indicador LED	**Indicador LED**está habilitado de forma predeterminada. ● Si**Indicador LED**está desactivado, 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	Grifo**Agregar**en la esquina superior derecha de la página para agregar 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 agregar, puede deslizar hacia la izquierda para probar llamadas telefónicas y mensajes SMS para verificar si el número de teléfono actual es válido. También puedes deslizar hacia la izquierda para eliminar el número de teléfono móvil. Toque el número de teléfono para ingresar a la página de edición del número de teléfono y luego podrá editar el número y seleccionar el tipo de evento que necesita enviar SMS. Sólo los dispositivos 2G/4G admiten esta función.
Modo de prueba	Grifo**Comenzar**para probar el estado de los periféricos que se conectan al concentrador en diferentes áreas y luego toque**Detener**para completar la detección.
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 de almacenamiento en la nube Conexión	Establezca el intervalo de ping del servidor-concentrador en un rango de 150 a 900 segundos (150 segundos de forma predeterminada). Si D-cloud detecta que la duración sin conexión del hub excede los 150 segundos, informará el estado del hub 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 de concentrador. La configuración determina la frecuencia con la que el concentrador se comunica con los periféricos y la rapidez con la que se detecta la pérdida de conexión. ● **Intervalo de ping del detector**:La frecuencia de los periféricos conectados operados por el concentrador está configurada en el rango de 12 segundos a 300 segundos (60 segundos de forma predeterminada). 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 el error 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 e informará el 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.
Sirena de enlace para manipulación	● **Sirena de enlace para manipulación**:En el estado de armamento, cuando el**Sirena de enlace para manipulación**está habilitado, el concentrador vinculará el sonido de la alarma. La sirena alertará 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 forma predeterminada. Después de habilitar**Siempre activo**, cuando el **Sirena de enlace para manipulación**está habilitado, el concentrador vinculará el sonido de la alarma tanto en el estado de armado como de desarmado. Esto no cumple con las certificaciones EN50131-1.
Verificación de 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, incidentes de manipulación y conectividad. Si se detectan errores, se mostrarán advertencias. ● Para el llavero, el indicador parpadea en verde y luego se vuelve rojo. ● Para la aplicación, aparece un mensaje de alarma. ● Para el teclado, 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 la ID del dispositivo, y luego podrá registrar el concentrador en DSS Pro o Converter.

Parámetro	Descripción
Centro de alarma	Permitir**Estación de monitoreo**y luego configure los parámetros del protocolo SIA para el centro receptor de alarmas (CRA). ● **Dirección IP preferida**:Ingrese la dirección IP y el número de puerto del ARC. ● **Dirección IP alternativa**:Ingrese 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**está habilitado, el sistema juzgará si desea enviar el mensaje a la dirección IP preferida o alternativa. ● **Protocolo IP**:Seleccionar**tcp**por defecto. ● **Intervalo de latidos**:Configure el intervalo de latidos con un rango de 0 segundos a 24 horas (60 segundos de forma predeterminada). 0 segundos significa**Intervalo de latidos**está desactivado. ● **cuenta central**:Ingrese el número de cuenta creado por el ARC, que se utilizará para identificar el centro cuando el centro envíe información al ARC. ● **Cifrado**: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 las centrales de alarma preferidas y alternativas son normales. Si la prueba es exitosa, el centro puede recibir el evento de prueba. ◇ **Prueba programada**:La prueba programada está deshabilitada por falla. Después de habilitarlo, el centro informa periódicamente los eventos de prueba.

Parámetro	Descripción
Verificación de fallas	• **Falla de energía principal**:Está habilitado de forma predeterminada. Después de la desactivación, cuando falla la alimentación principal del concentrador, el concentrador no indicará ni notificará. • **Sabotaje del centro de alarma**:Está habilitado de forma predeterminada. Después de la desactivación, cuando la tapa del concentrador está abierta, el concentrador no indicará ni notificará. • **Conexiones a la plataforma en la nube**:Está habilitado de forma predeterminada. Después de la deshabilitación, cuando la conexión entre el concentrador y la plataforma en la nube es anormal, el concentrador no indicará ni notificará. • **Detección de errores de red cableada y Wi-Fi**:Está habilitado de forma predeterminada. Después de la desactivación, cuando la red cableada y Wi-Fi del concentrador fallan, el concentrador no indicará ni notificará. • **Interferencia de RF**:Está habilitado de forma predeterminada. Después de la desactivación, cuando el concentrador detecta una interferencia de RF, no lo indicará ni notificará, pero el evento se puede ver en el registro. Deshabilitar cualquiera de estas funciones hará que el sistema no cumpla con EN50131-1 y no se enviarán mensajes de error relacionados con la función deshabilitada.

4.6.3 Ver evaluaciones

Después de configurar los dispositivos de forma remota y corregir 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 errores como el tipo de error, la hora a la que ocurrió el error, sugerencias y operación, el nombre del operador y calificaciones.

Procedimiento

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

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

4.6.4 Corrección de errores

Puede corregir errores después de verificar los dispositivos anormales. Los errores se encuentran de dos maneras, incluidos los informes automáticos del dispositivo y la verificación manual.

Procedimiento

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

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

Paso 3 **procesamiento**. Corrija el error según las sugerencias.

Etapa 4 Grifo**Error solucionado**si el error se solucionó y luego espere a que el cliente lo confirme.

Se notificará a los clientes sobre el estado de corrección de errores. Si confirman que el error se ha solucionado, se les pedirá que evalúen el servicio.

5 operaciones DMSS para usuarios finales

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

Las figuras son sólo como 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.

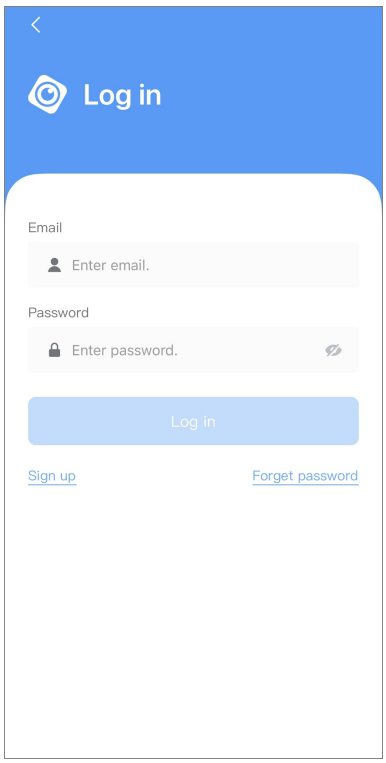
Procedimiento

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 Iniciar sesión



Paso 3 Crea una cuenta.

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

2. Ingrese su dirección de correo electrónico y contraseña.

Grifo para mostrar la contraseña y el icono se convertirá .

3. Lee el**Acuerdo del Usuario**y**política de privacidad**y luego seleccione el**He leído y acepto**caja.

4. Toque**Obtener código de verificación**, verifique su casilla de correo electrónico para obtener el código de verificación y luego ingrese el código.

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**.

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

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

5.2 Agregar dispositivos

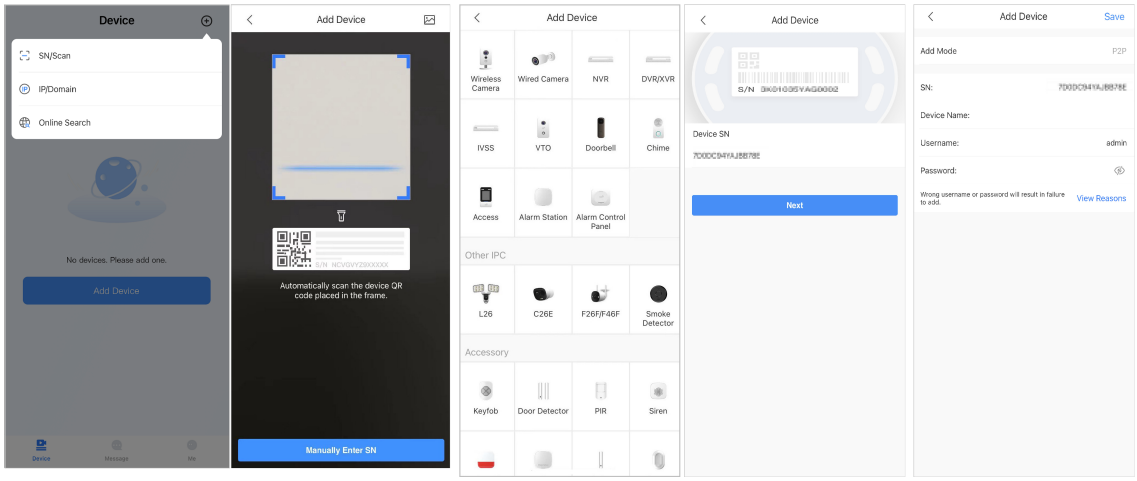
Para los usuarios finales, puede agregar dispositivos de alarma a la aplicación DMSS.

5.2.1 Agregar el concentrador

Procedimiento

Paso 1 Sobre el**Dispositivo**pantalla, toque y luego seleccione**SN/escanear**.

Figura 5-2 Agregar por código SN/QR



Paso 2 Agrega un dispositivo.

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

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

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

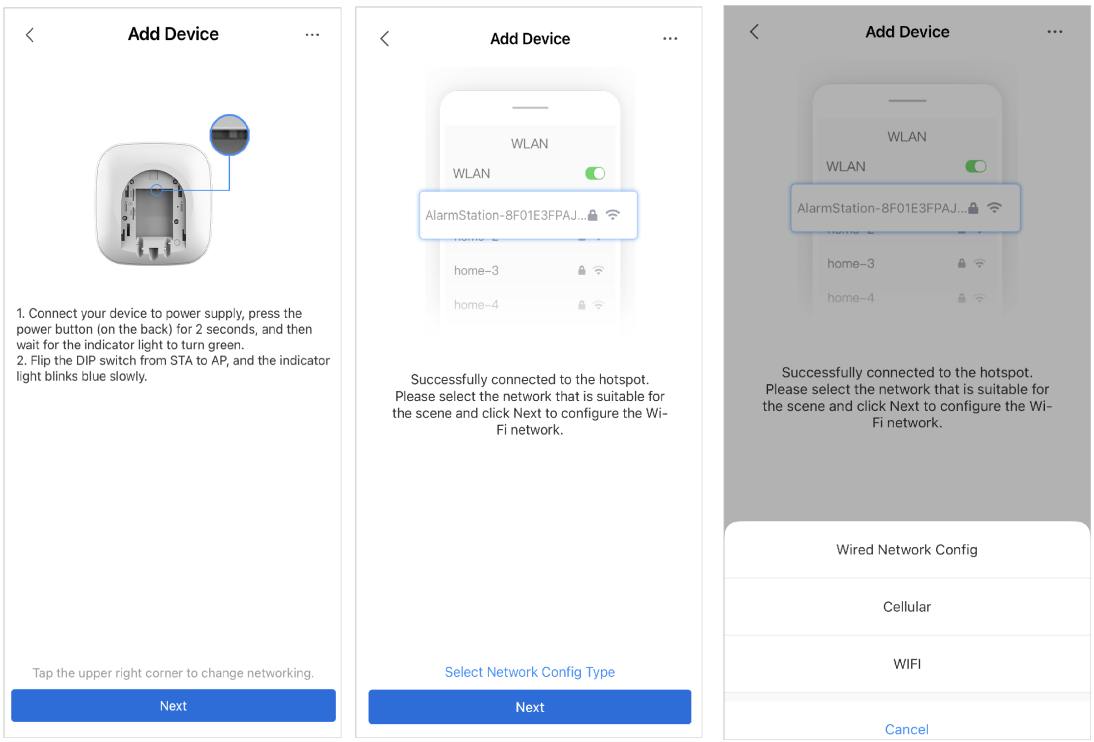
Etapa 4 Sobre el**Añadir dispositivo**pantalla, personalice el nombre del dispositivo, ingrese el nombre de usuario y la contraseña del dispositivo y luego toque**Ahorrar**.

Paso 5 Configurar los ajustes de red.

1. Sobre el**Añadir dispositivo**,grifo**Próximo**para unirse al punto de acceso del centro.
2. Cuando la conexión se establezca exitosamente, toque**Seleccione 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, la dirección DNS y MAC.
- Celular: Configura 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 periférico

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 Agregar IPC

Agregue IPC al centro.

Requisitos previos

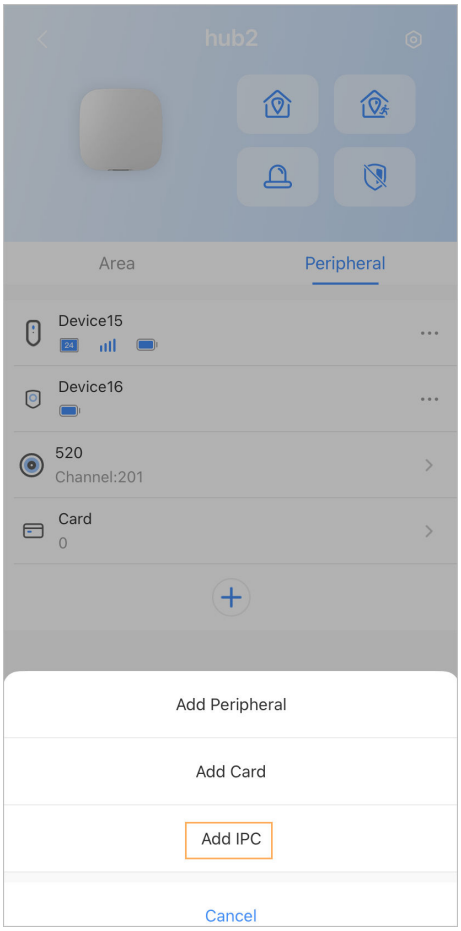
Asegúrese de que la versión de la aplicación DMSS sea 1.99.500 o posterior y que el concentrador sea V1.001.0000006.0.R. 230714 o posterior.

Procedimiento

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

Paso 2 Seleccionar**Agregar IPC**.

Figura 5-4 Agregar IPC

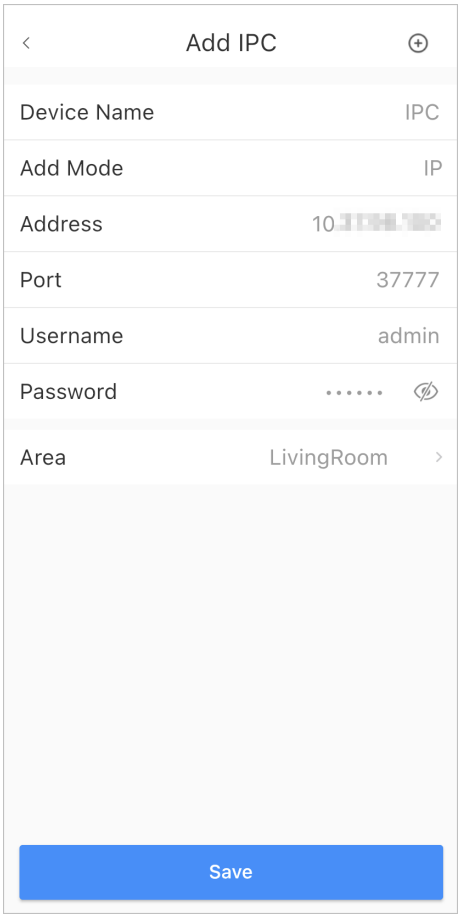


Paso 3 Agregue un IPC al concentrador.

- Agregar manualmente:

  1. Configure el nombre del dispositivo, la dirección IP del IPC, el número de puerto, el nombre de usuario y la contraseña del IPC, y seleccione el área donde está asignado el IPC.
  2. Toque**Ahorrar**.

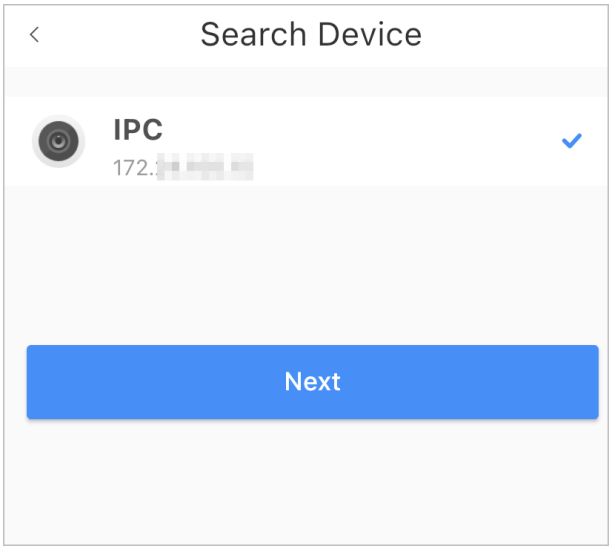
Figura 5-5 Agregar manualmente



- Búsqueda en línea:

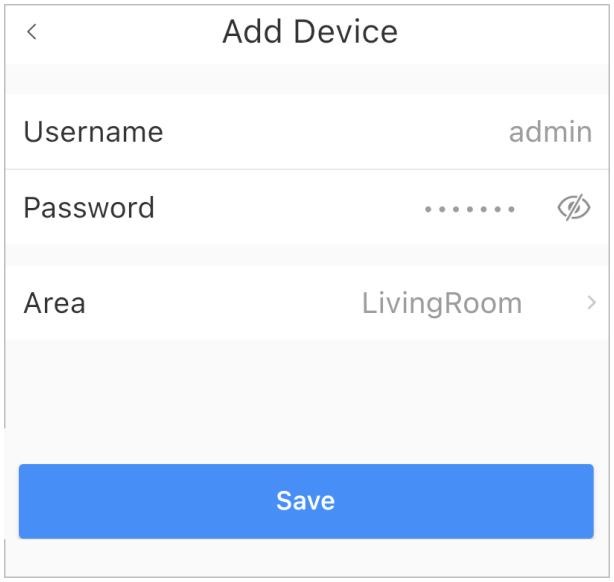
1. Toque para buscar el IPC en el mismo segmento de red.

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**.

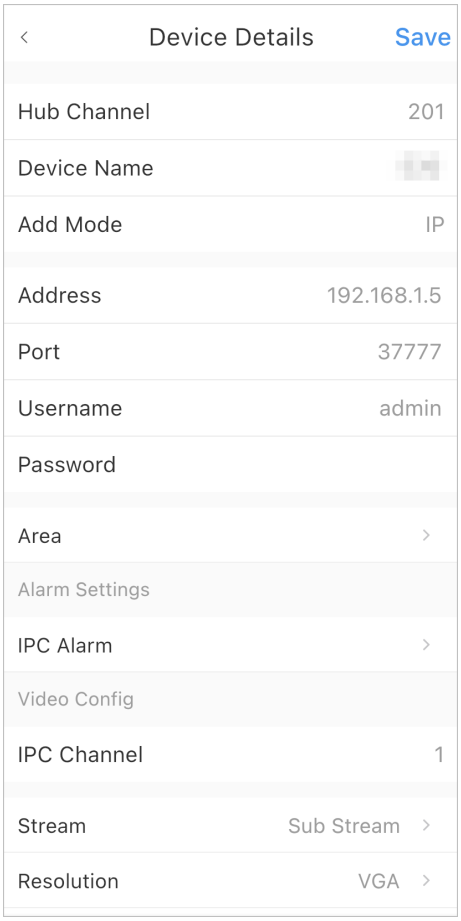
Figura 5-7 Ingresar contraseña



Operaciones relacionadas

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

Figura 5-8 Configuración de IPC



5.3 Configuración del vídeo de vinculación de alarma

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

Requisitos previos

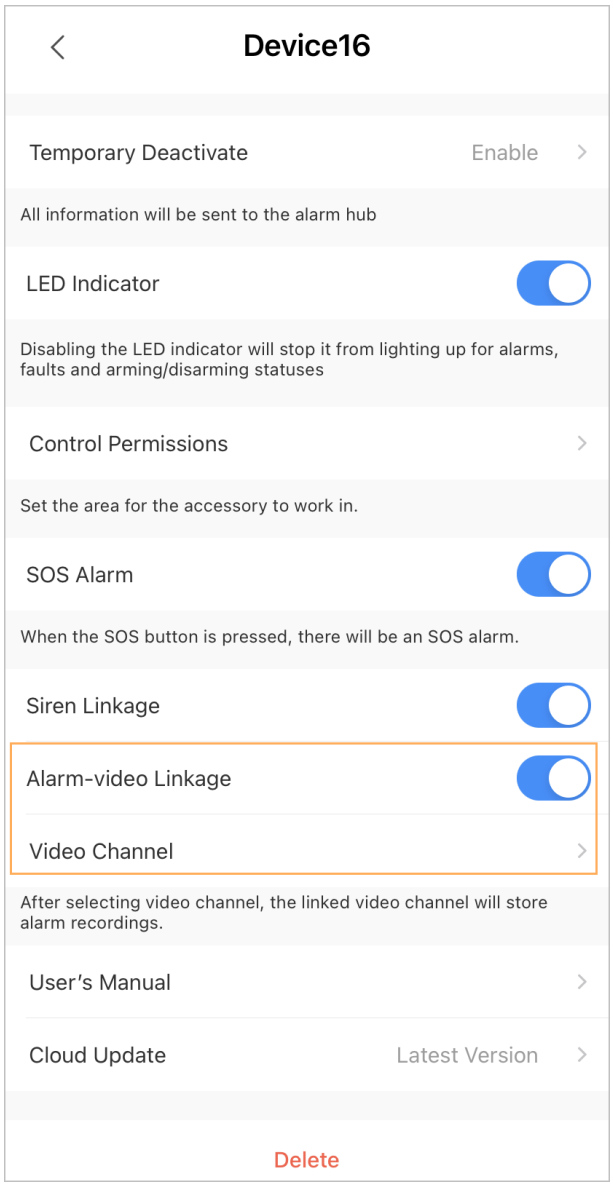
- Asegúrese de que el concentrador esté armado antes de configurar el enlace de alarma y video.
- Asegúrese de haber agregado periféricos al concentrador.

Procedimiento

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

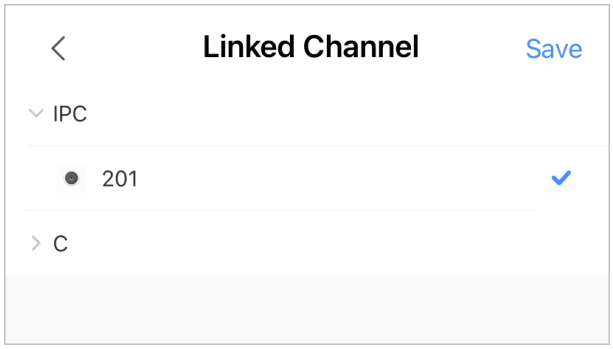
Paso 2 Permitir**Enlace alarma-vídeo**,y luego seleccione**Canal de vídeo**.

Figura 5-9 Pantalla de configuración



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

Figura 5-10 Canal vinculado



5.4 Configuración general del concentrador

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

Procedimiento

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

Tabla 5-1 Descripción del parámetro

Parámetro	Descripción
Estado del centro	Ver el estado del centro.
Configuración del concentrador	Configure los parámetros del hub.
Retardo de falla de energía principal	Configure 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 concentrador pueda funcionar.
configuración de la red	Grifo**configuración de la red**para ver la información de su red actual.
Zona horaria	Grifo**Zona horaria**para seleccionar su zona horaria y habilite el horario de verano (DST) si es necesario. ● **Zona horaria**:Seleccione la zona horaria en la que opera el centro. ● **horario de verano**:Seleccione la fecha o semana y luego seleccione la hora de inicio y la hora de finalización.
Compartir dispositivo	Grifo**Compartir dispositivo**para compartir el estado del hub con los demás usuarios.
Idiomas del dispositivo	Seleccione el idioma del centro entre inglés, español, árabe, danés, francés, italiano y Turquía.
Confianza del dispositivo	Confíe los dispositivos a proveedores de servicios para que realicen los servicios de operación de alarma por usted.
Manual de usuario	Grifo**Manual de usuario**para obtener el manual del usuario del centro de alarma.
Actualización en 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 alarma al correo electrónico vinculado. ● Registro de aplicaciones: Seleccionar**Registro**>**Registro de aplicaciones**para ver los registros de alarmas de DoLynk Cuidado. También puedes tocar el**Registro de aplicaciones**pantalla para enviar registros de alarma al correo electrónico vinculado.

5.4.1 Visualización del estado del concentrador

Sobre el**Centro**pantalla, seleccione > **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 Wi-Fi	Estado de la conexión a Internet del hub a través de Wi-Fi. Para una mayor confiabilidad, recomendamos instalar el concentrador en lugares con una intensidad de señal de al menos 2 barras. ● : Ultra bajo. ● : Bajo. ● : Moderado. ● : Alto. ● : No.
Nivel de bateria	Muestra la electricidad restante de la batería. ● : Completamente cargado. ● : Suficiente. ● : Moderado. ● : Insuficiente.
Antimanipulación	El modo de manipulación del periférico, que reacciona al desprendimiento del cuerpo.
Estado de energía principal	Muestra el estado de la energía principal.

Parámetro	Descripción
Estado de conexión GSM/LTE	Estado de la conexión a Internet del hub mediante tarjeta SIM, Wi-Fi y Ethernet. ● : Conectado. ● : Desconectado.
Estado de la conexión Wi-Fi	
Estado de 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. ● : Sin tarjeta SIM.
Estado de la tarjeta SIM	Esta barra de estado solo se admite 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.

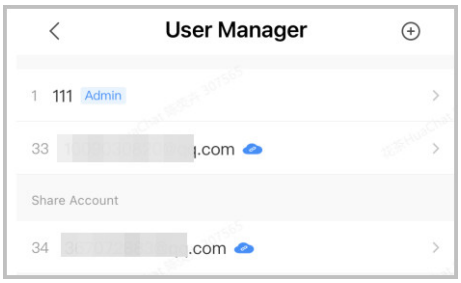
5.4.2 Configuración del concentrador

Procedimiento

Paso 1 Sobre 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 está desarmado. ● **Agregar usuarios**:Grifo para agregar un usuario. Ingrese su nombre de usuario, 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 sala. ◇ Se permiten hasta 64 usuarios de teclado (32 usuarios agregados manualmente y 32 usuarios creados automáticamente). El primer usuario creado manualmente es el usuario administrador de forma predeterminada y todos los permisos están disponibles para él. ◇ DMSS crea automáticamente un usuario de teclado cada vez que se agrega un dispositivo por primera vez. El número de secuencia de usuarios del teclado creado por el sistema comienza automáticamente desde 33 y tiene un icono junto a su cuenta. ◇ Se creará automáticamente un usuario de teclado para usuarios compartidos. Figura 5-11 Agregar usuario del teclado  ● **Eliminando usuario**:Seleccione el usuario y luego deslice el dedo hacia la izquierda para eliminarlo. El usuario administrador debe ser el último en ser eliminado. ● **Modificar 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 la tarjeta del teclado para ingresar al proceso de vinculación dentro de 30 segundos. Si la información de la tarjeta se reconoce correctamente, la identificación de la tarjeta se mostrará en la página de información del usuario y luego el teclado emitirá un pitido. Luego de guardar las configuraciones, la tarjeta tendrá los permisos de usuario. Se pueden vincular hasta 8 tarjetas a un usuario. ● **Eliminar tarjeta**:Seleccione la tarjeta y luego deslícela hacia la izquierda para eliminarla.
Armado global/ Encantador	Arma o desarma todos los detectores en todas las áreas con un solo toque.

Parámetro	Descripción
Programar armado/ Encantador	Armar o desarmar las áreas según cronograma. ● **Área**:Seleccione el área en la que opera el centro. ● **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 centro. ● **Repetir**:Copie el cronograma de armado o desarmado. ● **Armado a la fuerza**:Puede armar el sistema cuando ocurren errores en las zonas.
Configuración de tono de llamada	El tono de llamada al entrar o salir del modo de armado.
Indicador LED	**Indicador LED**está habilitado de forma predeterminada. ● Si**Indicador LED**está desactivado, 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 para agregar 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 agregar, puede deslizar hacia la izquierda para probar llamadas telefónicas y mensajes SMS para verificar si el número de teléfono actual es válido. También puedes deslizar hacia la izquierda para eliminar el número de teléfono móvil. Toque el número de teléfono para ingresar a la página de edición del número de teléfono y luego podrá editar el número y seleccionar el tipo de evento que necesita enviar SMS. Sólo los dispositivos 2G/4G admiten esta función.
Modo de prueba	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 de almacenamiento en la nube Conexión	Establezca el intervalo de ping del servidor-concentrador en un rango de 150 a 900 segundos (150 segundos de forma predeterminada). Si D-cloud detecta que la duración sin conexión del hub excede los 150 segundos, informará el estado del hub 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 de concentrador. La configuración determina la frecuencia con la que el concentrador se comunica con los periféricos y la rapidez con la que se detecta la pérdida de conexión. ● **Intervalo de ping del detector**:La frecuencia de los periféricos conectados operados por el concentrador está configurada en el rango de 12 segundos a 300 segundos (60 segundos de forma predeterminada). 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 el error 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 e informará el 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.
Sirena de enlace para manipulación	● **Sirena de enlace para manipulación**:En el estado de armamento, cuando el**Sirena de enlace para manipulación**está habilitado, el concentrador vinculará el sonido de la alarma. La sirena alertará 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 forma predeterminada. Después de habilitar**Siempre activo**, cuando el**Sirena de enlace para manipulación**está habilitado, el concentrador vinculará el sonido de la alarma tanto en el estado de armado como de desarmado. 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, incidentes de manipulación y conectividad. Si se detectan errores, se mostrarán advertencias. ● Para el llavero, el indicador parpadea en verde y luego se vuelve rojo. ● Para la aplicación, aparece un mensaje de alarma. ● Para el teclado, 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 la ID del dispositivo, y luego podrá registrar el concentrador en DSS Pro o Converter.

Parámetro	Descripción
Recepción de alarma Central	Habilite la función y luego configure los parámetros del protocolo SIA para la central receptora de alarmas (CRA). ● **IP preferida/nombre de dominio**:Ingrese la dirección IP/dominio y el número de puerto del ARC. ● **IP alternativa/nombre de dominio**:Ingrese la dirección IP/dominio alternativa y el número de puerto del ARC.  ◇ Los mensajes se enviarán a la dirección IP/dominio alternativa solo cuando la dirección IP preferida no pueda recibir el mensaje. ◇ Si**Intervalo de latidos**está habilitado, el sistema juzgará si desea enviar el mensaje a la dirección IP preferida o alternativa. ● **Protocolo IP**:Seleccionar**tcp**por defecto. ● **Intervalo de latidos del corazón**:Configure el intervalo de latidos con un rango de 0 segundos a 24 horas (60 segundos de forma predeterminada).  0 segundos significa**Intervalo de latidos**está desactivado. ● **Cuenta Central**:Ingrese el número de cuenta creado por el ARC, que se utilizará para identificar el centro cuando el centro envíe información al ARC. ● **Período de recarga**:Seleccione el período de recarga de la lista. ● **Cifrado**: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. ◇ **Fallos**: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 las centrales de alarma preferidas y alternativas son normales. Si la prueba es exitosa, el centro puede recibir el evento de prueba. ◇ **Prueba programada**:La prueba programada está deshabilitada por falla. Después de habilitarlo, el centro informa periódicamente los eventos de prueba.

Parámetro	Descripción
Verificación de fallas	• **Falla de energía principal**:Está habilitado de forma predeterminada. Después de la desactivación, cuando falla la alimentación principal del concentrador, el concentrador no indicará ni notificará. • **Sabotaje del centro de alarma**:Está habilitado de forma predeterminada. Después de la desactivación, cuando la tapa del concentrador está abierta, el concentrador no indicará ni notificará. • **Conexiones a la plataforma en la nube**:Está habilitado de forma predeterminada. Después de la deshabilitación, cuando la conexión entre el concentrador y la plataforma en la nube es anormal, el concentrador no indicará ni notificará. • **Errores de red cableada y Wi-Fi**:Está habilitado de forma predeterminada. Después de la desactivación, cuando la red cableada y Wi-Fi del concentrador fallan, el concentrador no indicará ni notificará. • **Errores de red celular**:Está habilitado de forma predeterminada. Después de la desactivación, cuando falla la red celular del concentrador, el concentrador no indicará ni notificará. • **Interferencia de RF**:Está habilitado de forma predeterminada. Después de la desactivación, cuando el concentrador detecta una interferencia de RF, no lo indicará ni notificará, pero el evento se puede ver en el registro. Deshabilitar cualquiera de estas funciones hará que el sistema no cumpla con EN50131-1 y no se enviarán mensajes de error relacionados con la función deshabilitada.

5.5 Configuración de red

Sobre el**Configuración general**del**Detalles del dispositivo**pantalla, toque**configuración de la red**y luego podrá 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 la red**>**Configuración de red cableada**

Paso 2 . Configure 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 habilitar **DHCP**y luego el concentrador obtiene una dirección IP dinámica automáticamente.
Dirección IP	Configure la dirección IP manualmente: configure la dirección IP, la máscara de subred, la puerta de enlace predeterminada, la dirección DNS y MAC manualmente para el concentrador.
Máscara de subred	
Puerta	
DNS	
DNS 2	
Dirección MAC	

5.5.2 Configuración de la red Wi-Fi

Procedimiento

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

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

5.5.3 Configuración celular

Procedimiento

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

Paso 2 Configurar parámetros celulares.

Tabla 5-5 Descripción de los parámetros celulares

Parámetro	Descripción
Celular	Grifo al lado de**Celular**para habilitar el celular.
Prioridad	Grifo al lado de**Prioridad**para establecer el celular como prioridad al seleccionar la red.
Tarjeta SIM 1 tarjeta SIM 2	• Admite tarjetas SIM duales y modo de espera único. • Las tarjetas SIM permiten que el concentrador utilice datos móviles y envíe notificaciones de alarma.
APN	El nombre del punto de acceso (APN) es el nombre de la configuración que lee su dispositivo para configurar una conexión para la puerta de enlace entre la red celular de su proveedor y la Internet pública.
Modo de autenticación	Modo de autenticación de la red celular.
Nombre de usuario Contraseña	El nombre de usuario y contraseña de la red celular.
Marque el número	El número al que debe llamar el centro.
Datos en 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.
Reiniciar las estadísticas	Restablezca el uso de datos móviles para reiniciar el conteo.
ALFILER	Ingrese el PIN de las tarjetas SIM para proteger la privacidad cuando sea necesario. Está prohibido ingresar el código PIN cuando el estado de la tarjeta SIM está desbloqueado. Bloquéelo cuando desee ingresar el PIN.

5.6 Administrar usuarios

5.6.1 Agregar usuario

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

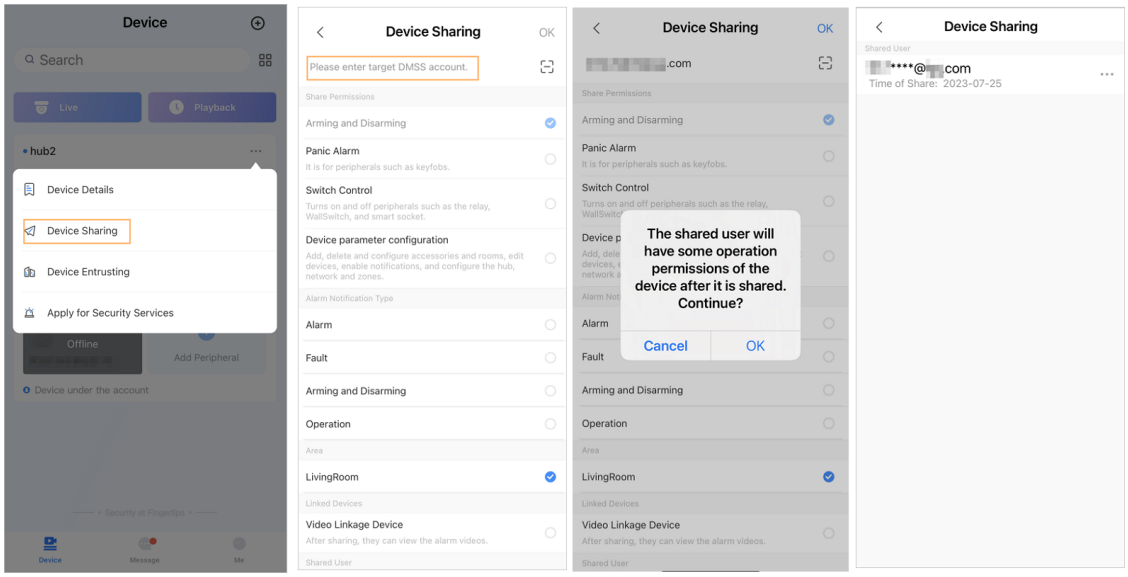
5.6.1.1 Agregar usuario general de DMSS

Puedes ir a > **Detalles del dispositivo**> ,o > **Detalles del dispositivo**>**Compartir dispositivo**para compartir el dispositivo. Estos métodos son similares. Esta sección utiliza dispositivos compartidos en > **Dispositivo** **Intercambio**como ejemplo.

Procedimiento

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

Figura 5-12 Compartir dispositivo



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

Paso 3 Seleccione permisos de dispositivo para usuarios según sus necesidades reales. Grifo**DE**

Etapa 4 **ACUERDO**.

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

5.6.1.2 Agregar instalador

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

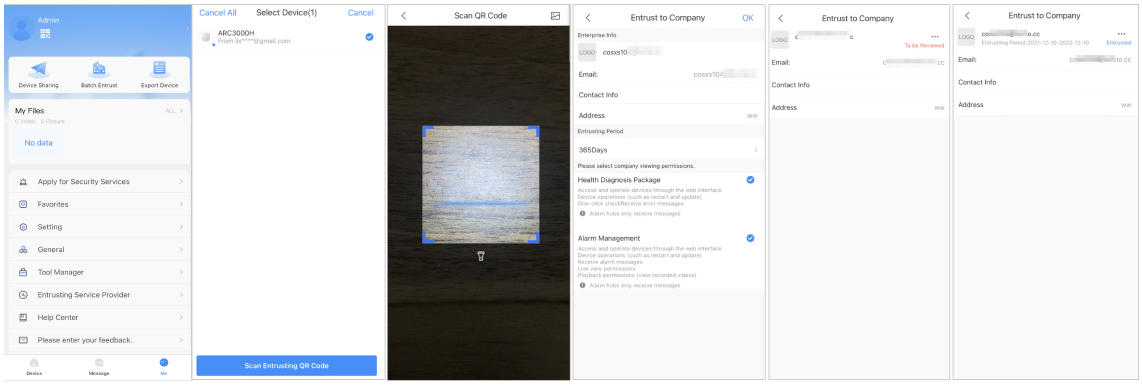
5.6.1.2.1 Confiar dispositivos en lotes

Puede confiar dispositivos a una empresa en lotes.

Procedimiento

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

Figura 5-13 Entrust dispositivos en lotes



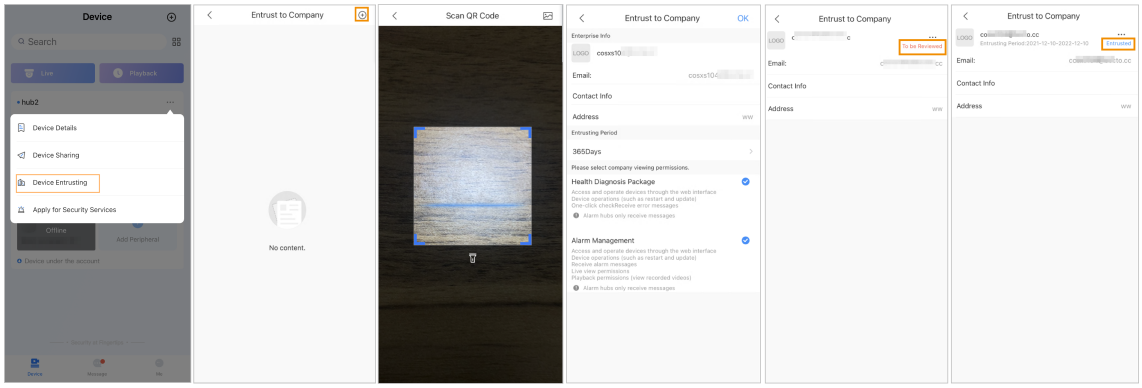
Paso 2 Sobre el**Seleccione el dispositivo**pantalla, seleccione los dispositivos que se van a confiar y luego confíelos a la empresa. El proceso para confiar varios dispositivos es el mismo que confiar un solo dispositivo.

5.6.1.2.2 Confiar dispositivos uno por uno

Procedimiento

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

Figura 5-14 Confiar un dispositivo



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

Puede solicitar a los instaladores sus códigos QR.

Paso 3 Sobre el**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 empresarial se reconocerá automáticamente después de escanear el código QR del instalador.

Etapa 4 Ver detalles de confianza en el**Confiar a la empresa**pantalla.

Cuando se le ha confiado con éxito,**Para ser revisado**cambiará a**Entregado**.

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

Operaciones relacionadas

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

5.6.2 Eliminar usuario

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

5.6.2.1 Cancelar el uso compartido de dispositivos

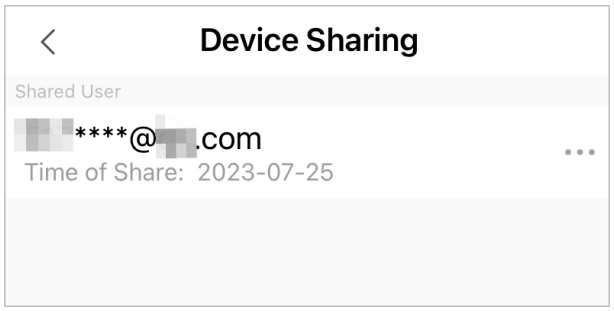
Para el usuario administrador de DMSS, puede eliminar usuarios generales de DMSS cancelando el uso compartido de los dispositivos con ellos en el**Compartir dispositivo**pantalla. Esta sección utiliza la ruta del > **Compartir dispositivo**como un ejemplo.

Procedimiento

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

Paso 2 En la lista de cuentas del**Compartir dispositivo**pantalla, seleccione una cuenta y toque .

Figura 5-15 Usuario compartido



Paso 3 Seleccionar**Cancelar compartir**,y luego toque**DE ACUERDO**para cancelar el uso compartido.

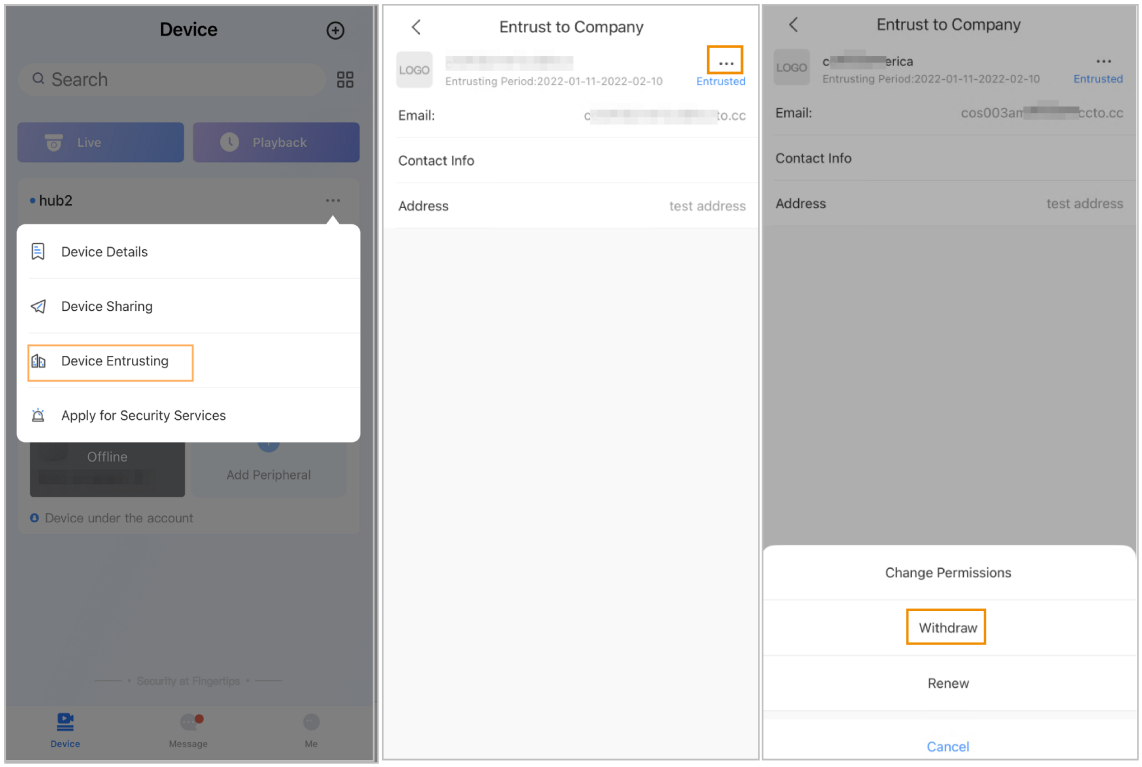
5.6.2.2 Cancelación del encargo de la aplicación

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

Procedimiento

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

Figura 5-16 Retirar la solicitud de encomienda



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

Se enviará un mensaje a la cuenta del instalador. Después de que el instalador lea el mensaje y apruebe su solicitud para cancelar la solicitud de confianza en Dolynk Care, su solicitud será cancelada.

5.6.2.3 Eliminación de dispositivo

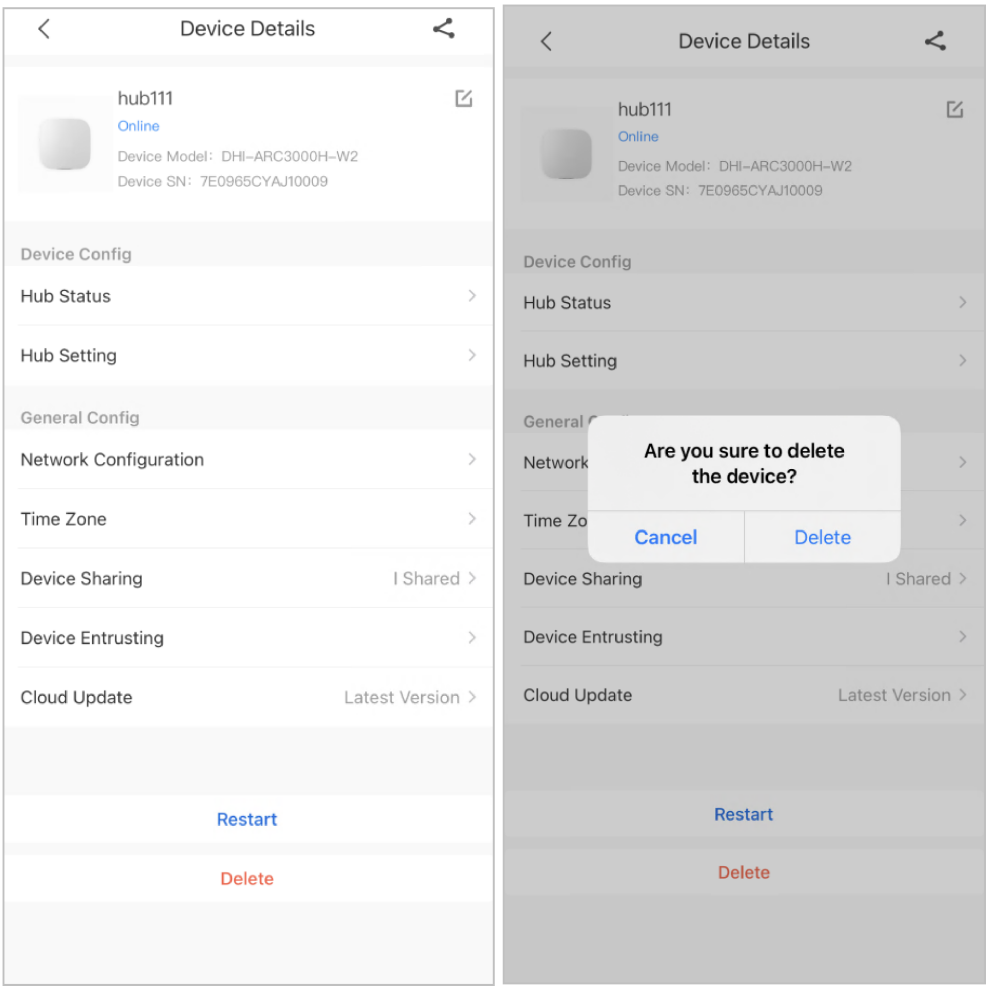
Para el usuario administrador de DMSS, puede eliminar tanto los instaladores como los usuarios generales de DMSS eliminando dispositivos.

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

Procedimiento

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

Figura 5-17 Eliminar el dispositivo



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

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

6 Operaciones Generales

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

Requisitos previos

- Asegúrese de haber agregado un concentrador antes de realizar las 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 y desarmar y configurar dispositivos de alarma.

Procedimiento

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

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

- Armado y Desarmado Único: Arma y desarma los detectores en una sola área.
- Armado y Desarmado Global: Arma y desarma 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: armar y desarmar los detectores según lo programado.

6.1 Armado y Desarmado Único

Puedes 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**:Apague el sistema de seguridad. Lo contrario de armarse.
- **desactivar**:Cierra la pantalla actual.

6.2 Armado y Desarme Global

Requisitos previos

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

Información de contexto

Puedes armar y desarmar los detectores en todas las áreas.

Procedimiento

Paso 1 Vaya a la pantalla del centro.

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

6.3 Armado y Desarmado Manual

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

- Para armar y desarmar los detectores en un solo área o en todas las áreas, consulte "6.1 Armado y desarmado único" y "6.2 Armado y desarmado global".
- Para operar a través del mando y el teclado, primero debe asignar los permisos de control de las áreas al mando y al teclado. Para obtener más información, consulte el manual del usuario del mando y teclado correspondientes.

6.4 Armado y Desarmado Programado

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

Procedimiento

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

Paso 2 Sobre el**Armado/Desarmado programado**pantalla, toque**Agregar**y luego configurar planes de armado.

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

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

Apéndice 1 Eventos de falla de armado y Descripción

Apéndice Tabla 1-1 Descripción y eventos de falla de armado (periféricos)

No.	Razón	Descripción
1	Pérdida de módulo	El periférico estaba desconectado.
2	error de corazon	No se han enviado paquetes de latidos durante más de 18 minutos.
3	Alarma	Alarma (24 horas).
4	Abierto	La tapa trasera del dispositivo estaba abierta.
5	exabierto	La tapa trasera del dispositivo externo estaba abierta.
6	Manosear	Se activó la alarma de manipulación periférica.
7	Batería baja	Se detectó batería baja del dispositivo.
8	PriPowerLoss	Se detectó un fallo de alimentación principal periférico.
9	Pérdida de batería	Se detectó falla de batería.
10	Sobretensión	Se detectó sobretensión.
11	Sobrecorriente	Se detectó sobrecorriente.
12	Sobrecalentar	Se detectó sobrecalentamiento.
13	Alarma de incendios	Se activó la alarma de incendio.
14	Alarma Médica	Se activó la alarma médica.
15	Alarma SOS	Se activó la alarma SOS.
dieciséis	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 retención	Se activó la alarma de pánico.

Apéndice Tabla 1-2 Descripción y eventos de falla de armado (hub)

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 centro de alarmas.
3	Error de conexión del servidor	El centro estaba fuera de línea.
4	Error de conexión del servidor SIA	Hay un error con la conexión entre el hub y la central receptora de alarmas SIA.
5	Batería baja	Se detectó batería baja.
6	Pérdida principal	Se detectó un fallo de alimentación principal.
7	Pérdida de batería	Se detectó falla de batería.

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

Apéndice 2 Códigos y descripción de eventos SIA

Apéndice Tabla 2-1 Códigos y descripción de eventos SIA

No.	Evento	Código CID	Descripción
1	Movimiento detectado	130	Alarma de robo.
		133	Alarma las 24 horas (segura).
		134	Alarma de Entrada/Salida.
2	Acción de apertura Detectado/Cerrando Acción detectada	130	Alarma de robo.
		133	Alarma las 24 horas (segura).
		134	Alarma de Entrada/Salida.
3	El contacto externo fue Abierto/Externo El contacto fue cerrado	130	Alarma de robo.
		133	Alarma las 24 horas (segura).
		134	Alarma de Entrada/Salida.
4	Alarma de coacción	121	Alarma de coacción.
5	El botón de pánico estaba Presionado	122	Alarma de Pánico (Silencio).
		123	Alarma de pánico (audible).
6	Alarma de intrusión	130	Alarma de robo.
		133	Alarma las 24 horas (segura).
		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 retención estaba Presionado	122	Alarma de Pánico (Silencio).
		123	Alarma de pánico (audible).
11	Rotura de vidrio detectada	130	Alarma de robo.
		133	Alarma las 24 horas (segura).
		134	Alarma de Entrada/Salida.
12	Inclinación detectada	130	Alarma de robo.
		133	Alarma las 24 horas (segura).
		134	Alarma de Entrada/Salida.
13	Choque detectado	130	Alarma de robo.
		133	Alarma las 24 horas (segura).
		134	Alarma de Entrada/Salida.
14	Alarma de cable trampa/ Alarma de cable trampa detenida	131	Alarma perimetral

No.	Evento	Código CID	Descripción
15	La tapa del panel de control estaba abierta/Panel de control La tapa estaba cerrada	137	Manosear.
dieciséis	La tapa periférica estaba Tapa abierta/periférica estaba cerrado	137	Sabotaje del sensor.
17	La tapa externa fue Tapa abierta/externa estaba cerrado	137	Sabotaje 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	Fallo de batería/batería Restaurado	311	Batería faltante/agotada.
21	Fallo de energía principal/ Energía principal restaurada	301	Pérdida de CA.
22	Interferencia de RF	344	Detección de atasco en el receptor RF.
23	Transmisión de alarma Fallo del sistema/restablecido	350	Problemas de comunicación.
24	Transmisión de alarma Ruta: Red cableada/Wi- Fallo de Fi/restablecido	350	Problemas de comunicación.
25	Transmisión de alarma Ruta: red celular Fallo/Restaurado	350	Problemas de comunicación.
26	Conexión periférica Perdido/Periférico Conexión restaurada	355	Pérdida de supervisión - RF.
27	Hub está fuera de línea/Hub está en línea	356	Pérdida de las encuestas centrales
28	Batería baja del periférico/ Nivel de batería del periférico restaurado	302	Batería baja del sistema.
29	Batería periférica Fallo/batería periférica restaurada	311	Batería faltante/agotada.
30	Alimentación principal periférica Fallo/alimentación principal periférica restaurada	301	Pérdida de CA.
31	Conexión RF-HD Fallido/RF-HD Conexión restaurada	354	Falla en comunicar el evento.

No.	Evento	Código CID	Descripción
32	Dispositivo bloqueado y desbloqueado	501	Inhabilitación del lector de acceso.
33	Proteccion al sobrevoltaje Activado/Sobretensión Protección restaurada	319	Sobretensión en la fuente de alimentación.
34	Protección contra la sobretensión Sobrecorriente activada Protección restaurada	312	Sobrecorriente en la fuente de alimentación.
35	Protección contra el sobrecalentamiento Activado/Sobrecalentamiento Protección restaurada	318	Sobrecalentamiento de la fuente de alimentación.
36	Alta temperatura/ Temperatura normal	158	Alta temperatura.
37	Baja temperatura/ Temperatura normal	159	Baja temperatura.
38	Armado	400 (aplicación)	Abierto cerrado.
		401 (teclado)	O/C por usuario.
		403 (programado armamento)	A/C automático.
		407 (llavero)	Armado/desarmado remoto.
		408	Brazo rápido.
		409	A/C del interruptor de llave
39	Desarmado	400 (aplicación)	Abierto cerrado.
		401 (teclado)	O/C por usuario.
		403 (programado armamento)	A/C automático.
		407 (llavero)	Armado/desarmado remoto.
		409	A/C del interruptor de llave
40	Modo Hogar activado	441	Armado QUÉDATE.
		442	Interruptor de llave armado EN CASA
41	Armado fallido	454 (fallo de armado)	No se pudo cerrar.
		455 (armado programado falla)	Falló el armado automático.
		457 (fallo de armado del 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	Desactivado 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 periódico	602	Informe de prueba periódico.

Apéndice 3 Recomendaciones de ciberseguridad

La ciberseguridad es más que una simple palabra de moda: es algo que pertenece 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 presentan algunos consejos y recomendaciones de Dahua sobre cómo crear un sistema de seguridad más seguro.

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

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 personajes; Los tipos de caracteres incluyen letras mayúsculas y minúsculas, números y símbolos.
- No incluya 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 está conectado a la red pública, se recomienda habilitar la función “verificación automática de actualizaciones” para obtener información oportuna de las actualizaciones de firmware lanzadas por el fabricante.
- Le sugerimos que descargue y utilice la última versión del software del cliente.

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

1.Protección física

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

2.**Cambie las contraseñas con regularidad**

Le sugerimos que cambie las contraseñas con regularidad para reducir el riesgo de que las adivinen o las descifren.

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

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

4.**Habilitar bloqueo de cuenta**

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

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

Le sugerimos que cambie HTTP predeterminado y otros puertos de servicio a cualquier conjunto de números entre 1024 y 65535, lo que reduce el riesgo de que personas ajenas puedan adivinar qué puertos está utilizando.

6.**Habilitar HTTPS**

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

7.**Enlace de dirección MAC**

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

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

De acuerdo con los requisitos comerciales y de administración, agregue usuarios de manera razonable y asígneles un conjunto mínimo de permisos.

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

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

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

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

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

Si el contenido de sus datos de audio y video es muy importante o confidencial, le recomendamos que utilice la función de transmisión cifrada 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 la transmisión.

11.**Auditoría segura**

- Verifique los usuarios en línea: le sugerimos que verifique a los usuarios en línea con regularidad para ver si el dispositivo inició sesión sin autorización.
- Verifique 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 habilitar la función de registro de red para garantizar que los registros críticos estén sincronizados con el servidor de registro de red para su seguimiento.

13.**Construya un entorno de red seguro**

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

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

Más información

Visite el centro de respuesta a emergencias de seguridad del sitio web oficial de Dahua para obtener 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