



Llavero inalámbrico

Manual de usuario



Prefacio

General

Este manual presenta las funciones y operaciones del llavero inalámbrico (en lo sucesivo, "el llavero").

Las instrucciones de seguridad

Las siguientes palabras de advertencia categorizadas con un significado definido pueden aparecer en el manual.

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

Revisión histórica

Versión	Contenido de revisión	Tiempo de liberación
V1.0.0	Primer lanzamiento.	enero 2021

Sobre el Manual

- El manual es solo para referencia. Si hay inconsistencia entre el manual y el producto real, prevalecerá el producto real.
- No somos responsables de ninguna pérdida causada por las operaciones que no cumplen con el manual.
- El manual se actualizaría de acuerdo con las últimas leyes y reglamentos de las regiones relacionadas. Para obtener información detallada, consulte el manual en papel, el CD-ROM, el código QR o nuestro sitio web oficial. Si hay inconsistencia entre el manual en papel y la versión electrónica, prevalecerá la versión electrónica.
- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto pueden causar algunas diferencias entre el producto real y el manual. Póngase en contacto con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria.
- Todavía puede haber desviación en los datos técnicos, descripción de funciones y operaciones, o errores en la impresión. Si tiene alguna duda o disputa, consulte nuestra explicación final.
- Actualice el software del lector o pruebe con otro software del lector convencional si no se puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas comerciales registradas y los nombres de compañías en el manual son propiedad

de sus respectivos dueños.

- Visite nuestro sitio web, comuníquese con el proveedor o el servicio al cliente si ocurre algún problema al usar el dispositivo.
- Si hay alguna duda o controversia, consulte nuestra explicación final.

Medidas de seguridad y advertencias importantes

La siguiente descripción es la aplicación correcta del dispositivo. Lea atentamente el manual antes de usarlo para evitar peligros y pérdidas de propiedad. Siga estrictamente el manual durante la aplicación y consérvelo correctamente después de leerlo.

Requisitos operativos

- No coloque ni instale el dispositivo en un área expuesta a la luz solar directa o cerca de un dispositivo generador de calor.
- No instale el dispositivo en un área húmeda, polvorienta o fuliginosa.
- Mantenga su instalación horizontal, o instálelo en lugares estables, y evite que se caiga.
- No gotee ni salpique líquidos sobre el dispositivo; no coloque en el dispositivo nada lleno de líquidos para evitar que los líquidos fluyan hacia el dispositivo.
- Instale el dispositivo en lugares bien ventilados; no bloquee su abertura de ventilación.
- Use el dispositivo solo dentro del rango nominal de entrada y salida.
- No desmonte el dispositivo arbitrariamente.
- Transporte, use y almacene el dispositivo dentro del rango permitido de humedad y temperatura.
- No coloque el concentrador en lugares cercanos a fuentes de interferencia de radio, como objetos metálicos.

Requisitos de energía

- Use baterías de acuerdo con los requisitos; de lo contrario, podría provocar un incendio, una explosión o quemar las baterías.
- Para reemplazar las baterías, use el mismo tipo de baterías.
- Utilice los cables eléctricos (cables de alimentación) recomendados por esta área, que deberán utilizarse dentro de su especificación nominal.
- Utilice un adaptador de corriente estándar compatible con este dispositivo. De lo contrario, el usuario debe asumir las lesiones personales o daños al dispositivo resultantes.
- Utilice una fuente de alimentación que cumpla con los requisitos SELV (voltaje extra bajo de seguridad) y suministre energía con un voltaje nominal que cumpla con la fuente de alimentación limitada en IEC60950-1. Para conocer los requisitos específicos de la fuente de alimentación, consulte las etiquetas de los dispositivos.
- Los productos con estructura de categoría I se conectarán a la toma de salida de la red eléctrica, que está equipada con protección a tierra.
- El acoplador de electrodomésticos es un dispositivo de desconexión. Durante el uso normal, mantenga un ángulo que facilite la operación.
- Utilice los accesorios regulados por el fabricante. El dispositivo debe ser instalado y mantenido por profesionales.

Tabla de contenido

Prefacio.....	yo
Medidas de seguridad y advertencias importantes.....	III
1. Introducción.....	1
2 Lista de verificación.....	2
3 diseño.....	3
3.1 Apariencia.....	3
3.2 Tecla de función.....	3
4 Conexión al concentrador.....	5
5 Configuración del mando a distancia.....	6
5.1 Configuración del llavero.....	6
5.2 Visualización del estado del llavero.....	6
6 Uso del mando a distancia.....	8
Apéndice 1 Recomendaciones sobre ciberseguridad.....	9

1. Introducción

El llavero inalámbrico es un control remoto en miniatura que se conecta al concentrador y controla el sistema de alarma de su hogar. Funciona enviando señales de comunicación inalámbrica al sistema de alarma, el cual reconocerá la señal y luego realizará la función que se le asigne al área.

2 Lista de verificación

Verifique el paquete de acuerdo con la siguiente lista de verificación. Si el dispositivo se daña o se pierde, comuníquese con el servicio posventa.

Figura 2-1 Lista de verificación

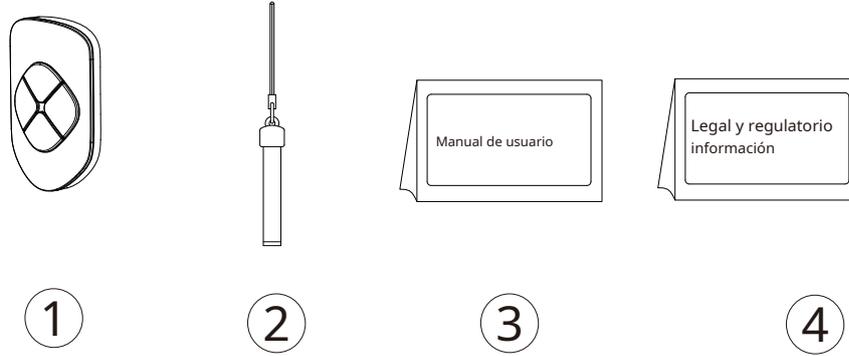


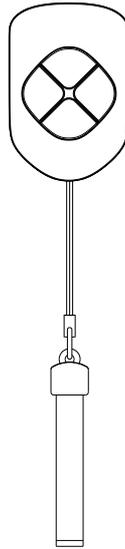
Tabla 2-1 Lista de verificación

No.	Nombre del artículo	Cantidad
1	Llavero inalámbrico	1
2	Cuerda	1
3	Manual de usuario	1
4	Información legal y regulatoria	1

3 diseño

3.1 Apariencia

Figura 3-1 Apariencia



3.2 Botón de función

Figura 3-2 Botón de función

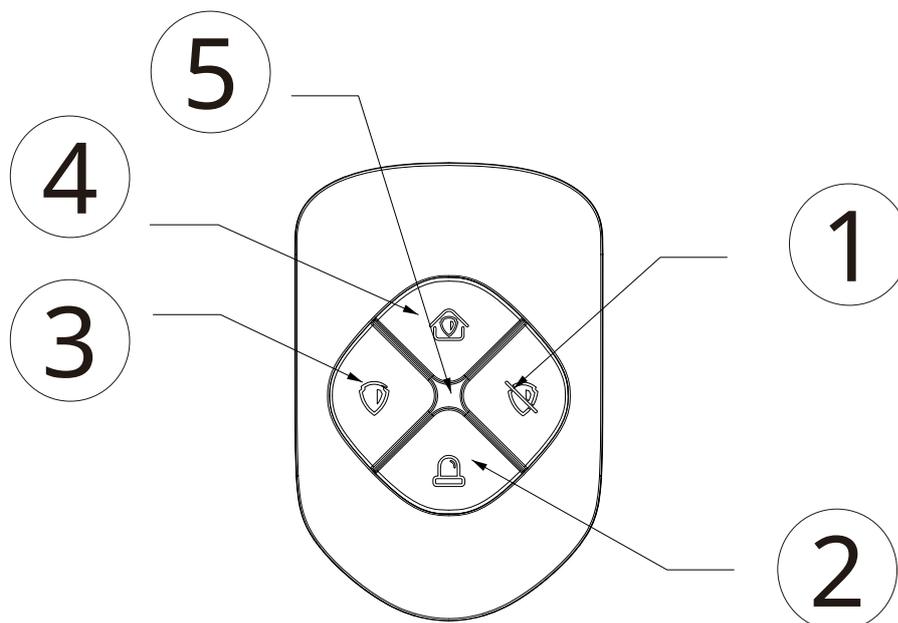


Tabla 3-1 Descripción del botón de función

No.	Nombre	Descripción
1	Botón de desarmado	Presione el botón una vez para desarmar el sistema.
2	llamada de socorro	Presione el botón de pánico y luego el llavero enviará una señal de alarma al sistema de alarma.
3	botón de armado	Presione el botón una vez para armar el sistema.
4	modo hogar	Presione el modo de inicio y luego se armarán los accesorios seleccionados.
5	Indicador	<ul style="list-style-type: none">● Parpadea en verde rápidamente: modo de emparejamiento.● Verde fijo: Normal.● Rojo fijo: el llavero está fuera de línea.● Primero parpadea en verde y luego cambia a rojo: la conexión con el concentrador falló.

4 Conexión al concentrador

Antes de la conexión con el concentrador, instale la aplicación DMSS en su teléfono. Asegúrese de haber instalado la última versión de la aplicación. Las interfaces y funciones pueden variar con diferentes dispositivos agregados, y prevalecerá la interfaz real. Este manual toma iOS como ejemplo.



- Asegúrese de que ya ha creado una cuenta y ha agregado un concentrador a la aplicación.
- Asegúrese de que el concentrador tenga una conexión a Internet estable.
- Asegúrese de que el concentrador esté desarmado.

Paso 1 Vaya a la interfaz del concentrador y luego toque  para agregar el llavero.

Paso 2 Toque  para escanear el código QR en la parte inferior del llavero y luego toque **próximo**. Tocar

Paso 3 **próximo** después de que se haya encontrado el llavero. Siga las instrucciones en pantalla y presione

Paso 4 **próximo**.  y  una vez al mismo tiempo, y luego toque

Paso 5 Espera el emparejamiento.

Paso 6 Personalice el nombre del llavero y luego toque **Terminado**.

5 Configuración del mando a distancia

Puede ver y editar información general del llavero.

5.1 Configuración del llavero

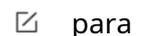
Sobre el **Centro**interfaz, seleccione el llavero según sea necesario de la lista de accesorios, y luego puede configurar los parámetros del llavero.

Tabla 5-1 Descripción del parámetro del llavero

Parámetro	Descripción
Configuración del dispositivo	<ul style="list-style-type: none"> ● Ver el nombre del dispositivo, el tipo, el SN y el modelo del dispositivo. ● Edite el nombre del dispositivo y luego toque Guardar para guardar la configuración.
Área	<ul style="list-style-type: none"> ● Ver el área existente. ● Agregue el área que desea armar y luego toque Guardar para guardar la configuración.
Permisos de control	Seleccione el área sobre la cual el llavero tiene permisos de control.
Alarma SOS	Si está habilitado, los mensajes de alarma SOS se enviarán cuando se detecte un evento de alarma.
Vinculación alarma-altavoz	Cuando se activa una alarma, los accesorios informarán los eventos de alarma al concentrador y alertarán con una sirena.
Vinculación alarma-video	Cuando se activa una alarma, los accesorios informarán los eventos de alarma al concentrador y luego se vincularán con videos.
Canal de vídeo	Seleccione el canal de video según sea necesario.
Actualización en la nube	Actualizar en línea.
Borrar	<p>Eliminar el accesorio en línea.</p>  <p>Ve a la Centrointerfaz, seleccione el accesorio de la lista y luego desliza el dedo hacia la izquierda para eliminarlo.</p>

5.2 Visualización del estado del llavero

Sobre el **Centro**interfaz, seleccione el llavero según sea necesario de la lista de accesorios y luego presione la



para

pestaña para ver el estado del llavero.

Tabla 5-2 Estado

Parámetro	Descripción
Nivel de batería	El nivel de batería del llavero.   : Completamente cargado.   : Suficiente.   : Moderado.   : Insuficiente.
Estado SOS	El estado de la alarma SOS.
Versión del programa	La versión del programa del llavero.

6 Uso del mando a distancia

La distancia máxima de conexión entre el llavero y el concentrador es de 1.500 metros. Esta distancia se reduce con paredes, pisos insertados y cualquier objeto que obstaculice la transmisión de la señal.

Después de agregar los accesorios en el concentrador, puede operar en el llavero.

- Presionar  y  una vez al mismo tiempo para conectarse con el concentrador.
- Presionar  una vez para habilitar el modo Ausente y luego se armarán todos los accesorios en el área.



Presionar  dos veces si el **Comprobación de integridad del sistema** está habilitado en el concentrador.

- Presionar  una vez para habilitar el modo hogar, y luego los accesorios seleccionados en el área serán armado.
- Presionar  una vez para habilitar el modo desarmado, y luego todos los accesorios en el área serán desarmado.
- Presionar  una vez para habilitar SOS.

Apéndice 1 Recomendaciones sobre ciberseguridad

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

Acciones obligatorias que se deben tomar para la seguridad básica de la red del dispositivo: 1. Use contraseñas seguras

Consulte las siguientes sugerencias para establecer contraseñas:

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

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

- De acuerdo con el procedimiento estándar en la industria tecnológica, recomendamos mantener actualizado el firmware de su dispositivo (como NVR, DVR, cámara IP, etc.) para garantizar que el sistema esté equipado con los últimos parches y correcciones de seguridad. Cuando el dispositivo está conectado a la red pública, se recomienda habilitar la función de "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 "agradables de tener" para mejorar la seguridad de la red de su dispositivo:

1. Protección Física

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

2. Cambie las contraseñas regularmente

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

3. Establezca y actualice la información de restablecimiento de contraseñas a tiempo

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

4. Habilitar bloqueo de cuenta

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

5. Cambiar HTTP predeterminado y otros puertos de servicio

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

6. Habilitar HTTPS

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

7. Enlace de dirección MAC

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

8. Asigne cuentas y privilegios de manera razonable

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

9. Deshabilite los servicios innecesarios y elija modos seguros

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

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

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

10. Transmisión encriptada de audio y video

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

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

11. Auditoría segura

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

12. Registro de red

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

13. Construya un entorno de red seguro

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

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

ENABLING A SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No.1199 Bin'an Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053

Email: overseas@dahuatech.com | Fax: +86-571-87688815 | Tel: +86-571-87688883