Botón de pánico inalámbrico

Manual de usuario

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V2.0.0

Prefacio

General

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

Modelo

DHI-ARD822-W2 (868); DHI-ARD822-W2

Las instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

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

Historial de evisiones

Versión	Contenido de revisión	Tiempo de liberación
V2.0.0	Se agregaron notas de reemplazo de batería.	abril 2022
V1.0.0	Primer lanzamiento.	marzo 2022

Aviso de protección de privacidad

Como usuario del dispositivo o controlador de datos, puede recopilar datos personales de otros, como su rostro, huellas dactilares y número de matrícula. Debe cumplir con las leyes y regulaciones locales de protección de la privacidad para proteger los derechos e intereses legítimos de otras personas mediante la implementación de medidas que incluyen, entre otras: Proporcionar una identificación clara y visible para informar a las personas sobre la existencia del área de vigilancia y proporcione la información de contacto requerida.

Sobre el Manual

- El manual es solo para referencia. Se pueden encontrar ligeras diferencias entre el manual y el producto.
- No somos responsables de las pérdidas sufridas debido a la operación del producto de maneras que no están en

cumplimiento del manual.

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

Medidas de seguridad y advertencias importantes

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

Requisitos de operación

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

requerimientos de instalación

WARNING

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

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

Tabla de contenido

Prefacio.....yo

Medidas de seguridad y advertencias importantes.....III

1. Introducción.....1

1.1 Resumen.....1

1.2 Especificaciones técnicas.....1

2 Lista de verificación.....3

3 Apariencia.....4

4 Agregar el botón al concentrador.....5

5 Instalación.....6

6 Configuración.....7

6.1 Visualización del estado.....7

6.2 Configuración del botón.....7

Apéndice 1 Recomendaciones sobre ciberseguridad.....9

1. Introducción

1.1 Resumen

El botón de pánico inalámbrico es un transmisor de botón inalámbrico que envía una señal de alarma de pánico al centro del sistema de seguridad de alarma. Con solo presionar el botón, las señales de alarma y los eventos se envían a la compañía de monitoreo para garantizar una respuesta rápida y mantenerlo actualizado a través de la aplicación DMSS. Es adecuado para usar con seguridad en hogares, bancos y más. También es fácil de transportar.

1.2 Especificaciones técnicas

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

Tabla 1-1 Especificaciones técnicas

Tipo	Parámetro	Descripción	
Función	Luz indicadora	1 para múltiples estados (emparejamiento, comunicación y más)	
	Botón	2	
	Actualización remota	Actualización en la nube	
	Intensidad de señal Detección	Sí	
	Detección de batería baja	Sí	
	Pantalla de nivel de batería	Muestra el nivel de batería en la aplicación	
Inalámbrico	Frecuencia de carga	DHI-ARD822-W2 (868): 868,0 MHz–868,6 MHz	DHI-ARD822-W2: 433,1 MHz–434,6 MHz
	Comunicación Distancia	DHI-ARD822-W2 (868): Hasta 1.400 m (4.593,18 pies) en un espacio abierto	DHI-ARD822-W2: Hasta 1.300 m (4.065,09 pies) en un espacio abierto
	El consumo de energía	Límite 14 mW	
	Comunicación Mecanismo	bidireccional	
	Modo de encriptación	AES128	
	Salto de frecuencia	Sí	
General	Operando Temperatura	– 10 °C a +55 °C (+14 °F a +131 °F) (interior)	
	Humedad de funcionamiento	10%–90% (HR)	
	Duración de la batería	5 años (si se usa dos veces por semana)	
	Dimensiones del producto	55 mm × 36 mm × 14,2 mm (2,17" × 1,42" × 0,56") (Largo × Ancho × Alto)	

Tipo	Parámetro	Descripción	
	Dimensiones del embalaje	95 mm× 59,5 mm× 30,5 mm (3,74" × 2,34" × 1,20") (Largo × Ancho × Alto)	
	Instalación	Montaje en pared; Mano	
	Peso neto	18 g (0,04 libras)	
	Peso bruto	48 g (0,11 libras)	
	Certificaciones	DHI-ARD822-W2 (868): CE	DHI-ARD822-W2: CE; FCC
	Caja	PC + ABS	
	Proteccion	IP54	
Técnico	Corriente de funcionamiento	28mA	
	Modo de prueba	Sí	

2 Lista de verificación

Figura 2-1 Lista de verificación

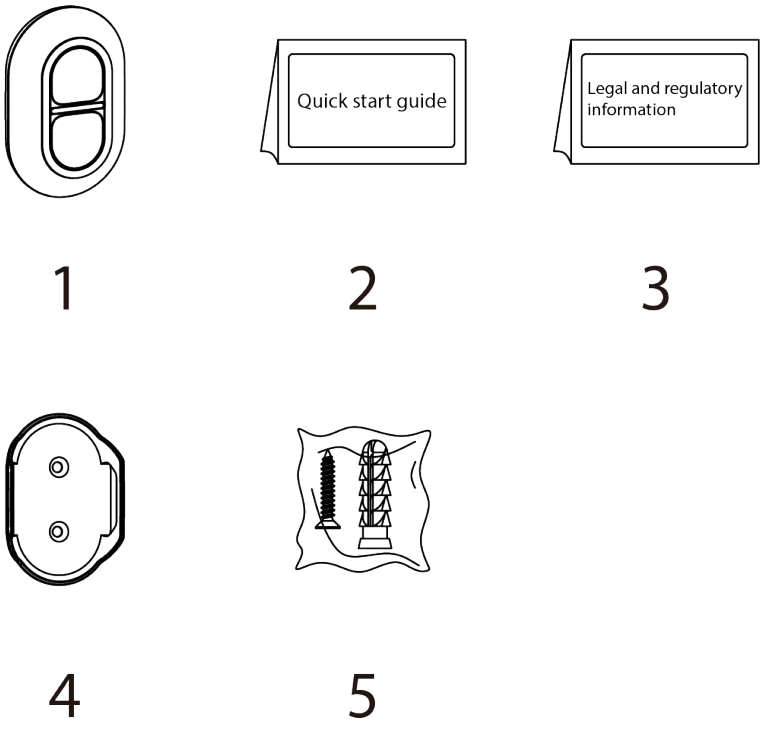


Tabla 2-1 Lista de verificación

No.	Nombre del árticulo	Cantidad	No.	Nombre del árticulo	Cantidad
1	Botón de pánico	1	4	Soporte (opcional)	1
2	Guía de inicio rápido	1	5	Paquete de tornillos (Opcional)	1
3	Legal y regulatorio información	1	—	—	—

3 Apariencia

Figura 3-1 Apariencia

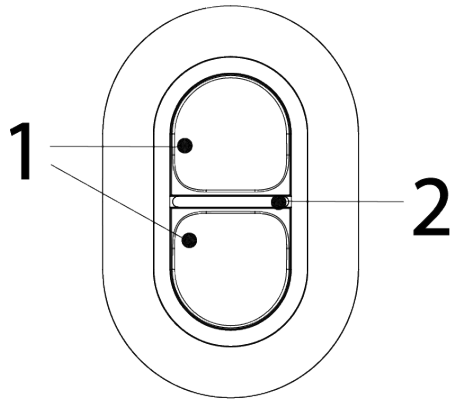


Tabla 3-1 Estructura

No.	Nombre	Descripción
1	Botón	● Mantenga presionados ambos botones al mismo tiempo durante 8 segundos, y luego el sistema ingresa al modo de emparejamiento. ◇ Parpadea en verde rápidamente: Emparejamiento. ◇ Verde fijo durante 2 segundos: Emparejamiento exitoso. ◇ Parpadea lentamente en verde durante 3 segundos: el emparejamiento falló. ● En el estado normal, presione ambos botones juntos una vez y luego el botón envía mensajes de alarma al concentrador. ◇ Parpadea en verde una vez: enviando mensajes al concentrador. ◇ Parpadea en verde durante 0,5 segundos: mensajes enviados correctamente al hub. ◇ Parpadea en rojo durante 0,5 segundos: Error al enviar mensajes al concentrador. ● En el modo de protección contra pulsaciones accidentales, mantenga presionados ambos botones durante 2 segundos y luego suene la alarma. los mensajes se enviarán al concentrador. El estado del indicador en el modo de protección contra pulsaciones accidentales es el mismo que el del estado normal. Asegúrate de haber habilitado la pulsación accidental función de protección en la aplicación DMSS.
2	Indicador	

4 Agregar el botón al concentrador

Antes de conectarlo al concentrador, instale la aplicación DMSS en su teléfono. Este manual utiliza iOS como ejemplo.

- Asegúrese de que la versión de la aplicación DMSS sea 1.98 o posterior y que el concentrador esté V1.001.0000000.7.R.220106 o posterior.
- Asegúrese de que el concentrador tenga una conexión a Internet estable.
- Asegúrese de que el concentrador esté desarmado.

Paso 1 Vaya a la pantalla del concentrador y luego toque 

para agregar el botón.

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

Paso 3 **próximo**después de que se haya encontrado el botón.

Paso 4 Siga las instrucciones en pantalla y cambie el botón a encendido, y luego toque**próximo**. Espera el

Paso 5 emparejamiento.

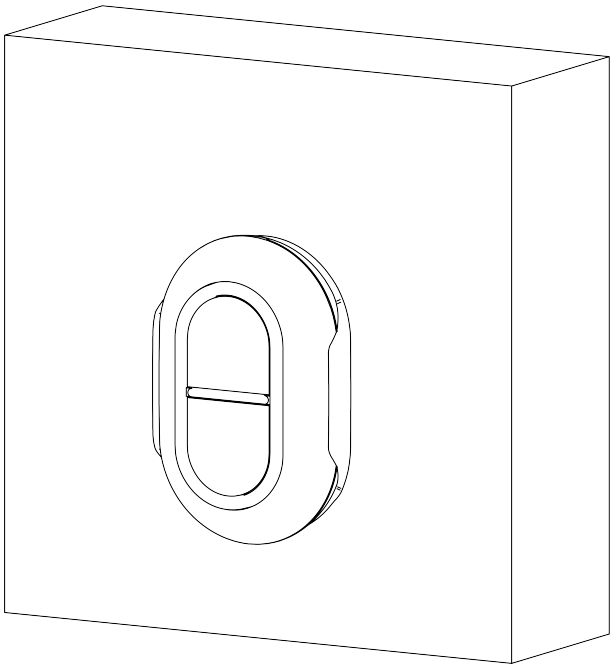
Paso 6 Personalice el nombre del botón, seleccione el área y luego toque**Terminado**.

5 Instalación

Antes de la instalación, agregue el botón al concentrador y verifique la intensidad de la señal del lugar de instalación. Recomendamos instalar el botón en un lugar con una intensidad de señal de al menos 2 barras. El botón es compatible con montaje en pared y se puede sujetar con la mano. Esta sección utiliza el montaje en pared como ejemplo.

Necesitas comprar un soporte para instalar el botón.

Figura 5-1 Instalación



Paso 1 Taladre 2 agujeros en la pared de acuerdo con las posiciones de los agujeros del soporte.

Paso 2 Coloque los pernos de expansión en los agujeros.

Paso 3 Alinee los orificios para tornillos en el soporte con los pernos de expansión y luego fije el soporte con tornillos.

Paso 4 Fije el botón al soporte.

- Si la batería está agotada, debe reemplazarla.
- Antes de insertar la batería nueva, asegúrese de presionar los botones primero o espere 30 segundos después de sacar el viejo.

6 Configuración

Puede ver y editar la información general del botón.

6.1 Visualización del estado

En la pantalla del concentrador, seleccione un botón de la lista de accesorios y luego podrá ver el estado del botón.

Tabla 6-1 Estado

Parámetro	Valor
Desactivar Temporalmente	El estado de si las funciones del repetidor están habilitadas o deshabilitadas. ● : Permitir. ● : Solo deshabilite la alarma de sabotaje. ● : Desactivar. La función solo está disponible cuando la versión de la aplicación DMSS es 1.96 o posterior, el concentrador es V1.001.0000000.6.R.211215 o posterior, y el botón es V1.000.0000001.0.R.20211203 o posterior.
Nivel de bateria	El nivel de batería del botón. ● : Completamente cargado. ● : Suficiente. ● : Moderado. ● : Insuficiente. ● : Bajo.
Modo de operación	El modo de trabajo del botón.
Brillo LED	El brillo de las luces LED.
Protección de prensa accidental	El estado de si la función de protección contra pulsaciones accidentales está habilitada o deshabilitada.
Transmitir a través del repetidor	El estado de si el botón reenvía mensajes de accesorios al concentrador a través del repetidor. La función solo está disponible cuando la versión de la aplicación DMSS es 1.96 o posterior, el concentrador es V1.001.0000000.6.R.211215 o posterior y el botón es V1.000.0000001.0.R.20211203 o posterior.
Versión del programa	La versión del programa del botón.

6.2 Configuración del botón

En la pantalla del concentrador, seleccione un botón de la lista de accesorios y luego toque para configurar el

parámetros del botón.

Tabla 6-2 Descripción del parámetro del botón de pánico

Parámetro	Descripción
Configuración del dispositivo	● 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	Seleccione el área a la que está asignado el botón.
Desactivar Temporalmente	Si envía información del sensor al centro de alarmas. ● Tocar**Permitir**, y luego el botón enviará mensajes de alarma al concentrador.**Permitir** está configurado de forma predeterminada. ● Tocar**Desactivar**, y luego el botón no enviará mensajes de alarma al concentrador.
Enlace de sirena	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 vincularán los eventos.
Canal de vídeo	Seleccione el canal de video según sea necesario.
Brillo LED	Configura el brillo de las luces LED. Puede seleccionar de **Apagado**, **Bajo**y**Alto**.
Protección de prensa accidental	Permitir**Protección de prensa accidental**para evitar la activación de operaciones no deseadas al presionar accidentalmente el botón. ● **Apagado**: deshabilite la función de protección contra pulsaciones accidentales. ● **Presione y mantenga**: Seleccione**Presione y mantenga**para habilitar la función de protección contra pulsaciones accidentales. Una vez habilitado, debe mantener presionados ambos botones para enviar mensajes de alarma al concentrador.
Detección de intensidad de señal	Pruebe la intensidad de la señal actual.
Prueba de botón	Detectar si el botón funciona.
Actualización en la nube	Actualizar en línea.
Borrar	Eliminar el botón.  Vaya a la pantalla del concentrador, seleccione el accesorio de la lista y luego desliza el dedo hacia la izquierda para eliminarlo.

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 de Dahua sobre cómo crear un sistema de seguridad más seguro.

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

1.**Utilice contraseñas seguras**

Consulte las siguientes sugerencias para establecer contraseñas:

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

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

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

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

1.Protección Física

Le sugerimos que realice una protección física al dispositivo, especialmente a los dispositivos de almacenamiento. Por ejemplo, coloque el dispositivo en 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.**Establecer y actualizar contraseñas Restablecer información a tiempo**

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

4.**Habilitar bloqueo de cuenta**

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

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

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

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

6.**Habilitar HTTPS**

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

7.**Enlace de dirección MAC**

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

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

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

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

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

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

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

10**Transmisión encriptada de audio y video**

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

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

11**Auditoría segura**

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

12**Registro de red**

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

13**Construir un entorno de red seguro**

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

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

dispositivo.

Más información

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

ENABLING A SAFER SOCIETY AND SMARTER LIVING

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