



Cámara PIR inalámbrica

Manual de usuario



Prefacio

General

Este manual presenta la instalación, las funciones y las operaciones de la cámara PIR inalámbrica (en adelante, la "cámara PIR"). Lea atentamente antes de usar el dispositivo y guarde el manual en un lugar seguro para futuras consultas.

Modelo

DHI-ARD1731-W2; DHI-ARD1731-W2 (868)

Instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

Palabras de advertencia	Significado
 DANGER	Indica un peligro de alto 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 ayudarlo a resolver un problema o ahorrarle tiempo.
 NOTE	Proporciona información adicional como énfasis y complemento del texto.

Revisión histórica

Versión	Contenido de revisión	Tiempo de liberación
V1.0.2	Especificaciones técnicas actualizadas.	febrero 2023
V1.0.1	- Se agregó una versión de la aplicación y el concentrador DMSS. - Se agregó una nota de que el repetidor no admite la transmisión de imágenes desde la cámara PIR al concentrador.	agosto 2022
V1.0.0	Primer lanzamiento.	junio 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 manera que no cumpla con el manual.
- El manual se actualizará de acuerdo con las últimas leyes y reglamentos de las jurisdicciones relacionadas. Para obtener información detallada, consulte el manual del usuario en papel, use nuestro CD-ROM, escanee el código QR o visite nuestro sitio web oficial. El manual es solo para referencia. Se pueden encontrar ligeras diferencias entre la versión electrónica y la versión en papel.
- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto pueden dar lugar a que aparezcan algunas diferencias entre el producto real y el manual. Póngase en contacto con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria.
- Puede haber errores en la impresión o desviaciones en la descripción de las funciones, operaciones y datos técnicos. Si hay alguna duda o disputa, nos reservamos el derecho de dar una explicación final.
- Actualice el software del lector o pruebe con otro software del lector convencional si no se puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas registradas y nombres de compañías en el manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, póngase en contacto con el proveedor o con el servicio de atención al cliente si se produce algún problema durante el uso del dispositivo.
- Si hay alguna duda o controversia, nos reservamos el derecho de la explicación final.

Medidas de seguridad y advertencias importantes

Esta sección presenta contenido que cubre el manejo adecuado del dispositivo, la 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.....	I
Medidas de seguridad y advertencias importantes.....	III
1. Introducción.....	1
1.1 Resumen.....	1
1.2 Especificaciones técnicas.....	1
2 Lista de verificación.....	4
3 diseño.....	5
3.1 Apariencia.....	5
3.2 Dimensiones.....	6
4 Encendido.....	7
5 Adición de la cámara PIR al concentrador.....	9
6 Instalación.....	10
6.1 Campo de visión.....	10
6.2 Instalación de la cámara PIR.....	10
7 Configuración.....	12
7.1 Visualización del estado.....	12
7.2 Configuración de la cámara PIR.....	13
Apéndice 1 Recomendaciones sobre ciberseguridad.....	dieciséis

1. Introducción

1.1 Resumen

Con su cámara HD de 2 MP integrada y su sensor de imagen CMOS, la cámara PIR inalámbrica detecta intrusiones y captura instantáneas de alta definición. Es un detector de infrarrojos pasivo inalámbrico que envía instantáneas a través de la conexión Wi-Fi y Ethernet a su teléfono y ARC (central de alarma), para que las causas de las intrusiones se identifiquen de manera efectiva.

La cámara también tiene un diseño único para tomar instantáneas solo cuando ocurre una intrusión, lo que elimina la necesidad de instalar cámaras para monitorear constantemente las escenas. Diseñada para mantener a su familia y su empresa seguras, todo el proceso de transmisión de datos está encriptado y la cámara no obtiene su información privada de forma activa.

1.2 Especificaciones técnicas

Esta sección contiene las especificaciones técnicas de la cámara PIR. Consulte los que correspondan a su modelo.

Tabla 1-1 Especificaciones técnicas

Tipo	Parámetro	Descripción	
Video	Campo de visión	88° (H); 68° (V)	
	Tipo de imagen	jpeg	
	Resolución	1600 × 1200; 1280 × 960; 640 × 480; 320 × 240	
	Velocidad de detección	0,3 m/s-3 m/s (0,98 pies/s-9,84 pies/s)	
	Cuadros por segundo	2	
	Modo de iluminación	Luz infrarroja	
	Rango de iluminación	12 m (39,37 pies)	
	Interruptor día/noche	Color/Blanco y negro	
Función	Luz indicadora	1 × indicador de alarma verde	
	Botón	1 × interruptor de encendido	
	Actualización remota	Actualización en la nube	
	Detección de batería baja	Sí	
	Pantalla de nivel de batería	Sí	
	Manosear	alarma de manipulación	
	Intensidad de señal	Prueba de señal de RF Prueba de señal RF-HD	
	Frecuencia de carga	DHI-ARD1731-W2(868): 868,0 MHz-868,6 MHz	DHI-ARD1731-W2: 433,1 MHz-434,6 MHz

Tipo	Parámetro	Descripción	
	Distancia de comunicación	DHI-ARD1731-W2(868): RF: hasta 1600 m (5249,34 pies) en un espacio abierto RF-HD: hasta 300 m (984,25 pies) en un espacio abierto	DHI-ARD1731-W2: RF: hasta 1200 m (3937,01 pies) en un espacio abierto RF-HD: hasta 300 m (984,25 pies) en un espacio abierto
	Comunicación Mecanismo	bidireccional	
	Salto de frecuencia	Sí	
	Modo de encriptación	AES128	
General	Fuente de alimentación	CR123A× 3	
	Duración de la batería	4 años (si se activa dos veces por semana con una eficiencia de batería del 70 %)	
	Temperatura de funcionamiento	– 10 °C a +55 °C (+14 °F a +131 °F) (interior)	
	Humedad de funcionamiento	10%–90% (HR)	
	Dimensiones del producto	127,6 mm × 71,0 mm × 53,2 mm (5,02" × 2,80" × 2,09")	
	Dimensiones del embalaje	121,0 mm × 65,0 mm × 170,0 mm (4,76" × 2,56" × 6,69")	
	Peso neto	202 g (0,45 libras)	
	Peso bruto	333 g (0,73 libras)	
	Instalación	montaje en pared	
	Caja	PC + ABS	
	Certificaciones	EN 50131-1:2006 + A1:2009 + A2:2017 + A3:2020 EN 50131-2-2:2021 EN 50131-6:2017 EN 50131-5-3:2017 EN 50130-4:2011 + A1: 2014 (+) Grado de seguridad 2 Clase ambiental II CE	CE; FCC
técnica yo	Modo de detección	PIR	
	Sensibilidad	3 niveles ajustables	
	Rango de detección	12 m (39,37 pies) (86°) con una altura de instalación de 2,2 m (7,22 pies)	
	Velocidad de detección	0,3 m/s-3 m/s (0,98 pies/s-9,84 pies/s)	
	Nivel de inmunidad de mascotas	≤18 kg (39,68 libras)	
	Resistencia a la luz blanca Nivel	2000 lux	

Tipo	Parámetro	Descripción
	Digital bidireccional Temperatura Compensación	Sí
	Guión	Interior
	Corriente de funcionamiento	65 μ A
	Corriente de alarma	● Día: 170 mA (promedio); 800 mA (máx.) ● Noche: 230 mA (promedio); 2,8 A (máx.)

2 Lista de verificación

Figura 2-1 Lista de verificación

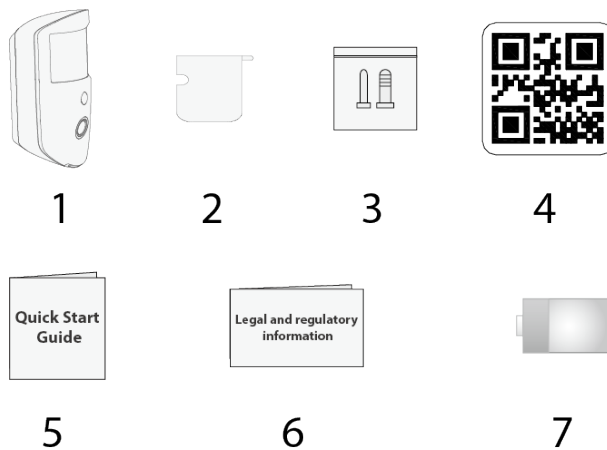


Tabla 2-1 Lista de verificación

No.	Nombre del artículo	Cantidad	No.	Nombre del artículo	Cantidad
1	Cámara PIR	1	5	Guía de inicio rápido	1
2	Adhesivo de doble cara cinta	1	6	Legal y regulatorio información	1
3	Paquete de tornillos	2	7	Batería	3
4	Código QR	1	-	-	-

3 diseño

3.1 Apariencia

Figura 3-1 Apariencia

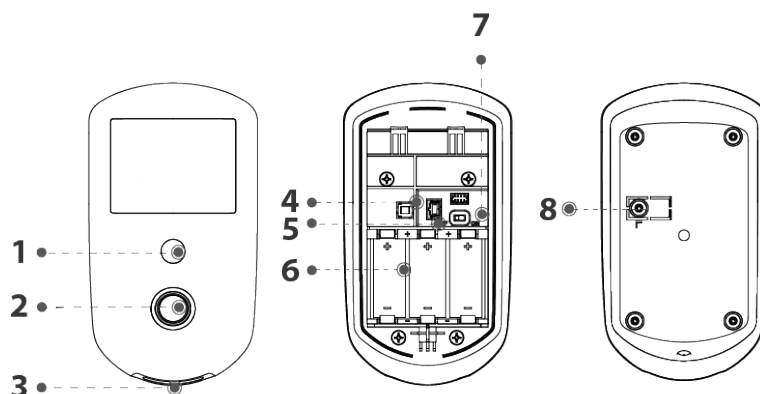
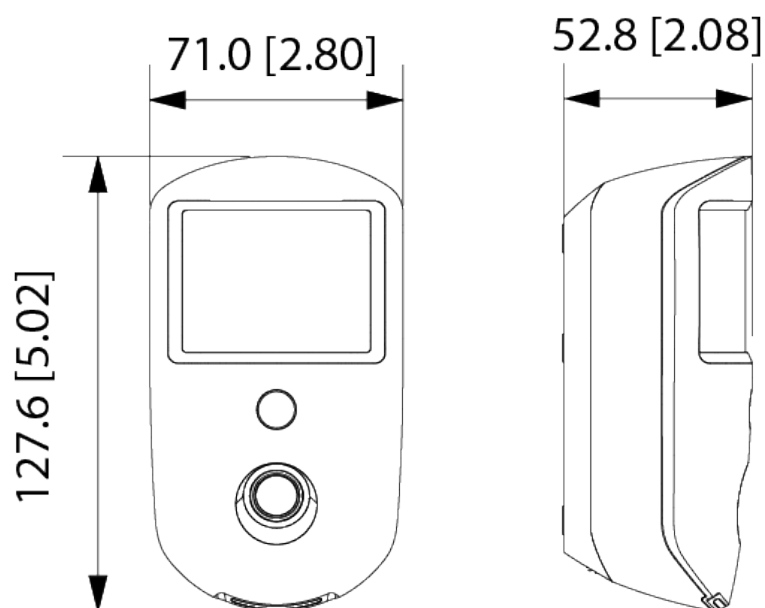


Tabla 3-1 Estructura

No.	Nombre	Descripción
1	luz infrarroja	Proporciona luz IR para entornos oscuros.
2	Cámara	Captura imágenes cuando se activa una alarma de intrusión.
3	Indicador	● Parpadea en verde rápidamente: modo de emparejamiento o modo de sensibilidad reducida. ● Verde fijo: se activó un evento de alarma. ● Verde fijo durante 2 segundos: Emparejamiento exitoso. ● Parpadea lentamente en verde durante 3 segundos: el emparejamiento falló.
4	Manibela de encendido	Cuando se suelta el interruptor de manipulación, se activará la alarma de manipulación.
5	Interruptor antisabotaje del soporte	(Opcional) Si se retira el soporte, se activará la alarma de manipulación.
6	Batería	Inserte las pilas para encender la cámara PIR.
7	Interruptor encendido / apagado	Encienda o apague la cámara PIR.
8	Contraportada	Si se abre la tapa trasera, se activará la alarma de manipulación.

3.2 Dimensiones

Figura 3-2 Dimensiones (mm [pulgadas])



4 Encendido

Paso 1 Afloje el tornillo para abrir la cámara PIR.

Figura 4-1 Afloje el tornillo

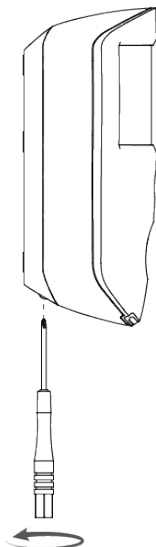


Figura 4-2 Abra la cámara PIR

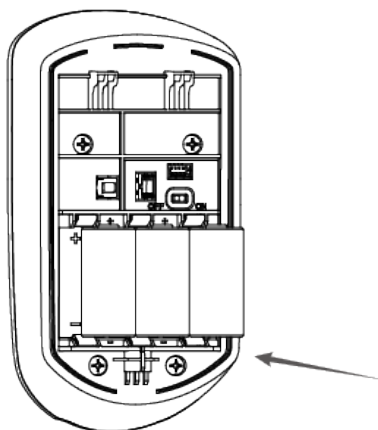


Paso 2 Inserte las pilas en la cámara PIR.



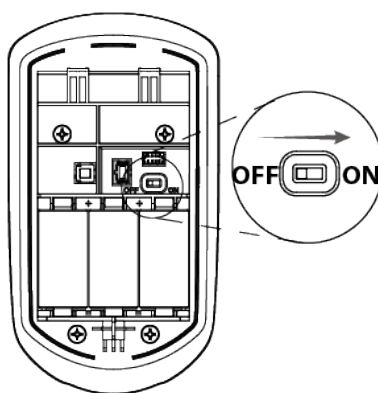
- Al insertar las baterías, asegúrese de que todas estén cargadas al mismo nivel.
- Al insertar las baterías, alinee los símbolos "+" de la batería con los del PIR-Cámara.

Figura 4-3 Inserte las pilas



Paso 3 Encienda la cámara PIR.

Figura 4-4 Encienda la cámara PIR



5 Adición de la cámara PIR al concentrador

Antes de conectar la cámara PIR 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 1.99 o posterior y que el concentrador sea V1.001.R.220625 o más tarde.
- Asegúrese de que ya haya creado una cuenta y agregado el hub a DMSS.
- 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 **Periférico** para agregar la cámara PIR. Grifo **+** para
- Paso 2 escanear el código QR en la parte inferior de la cámara PIR y luego toque **Próximo**. Grifo **Próximo** después
- Paso 3 de que se haya encontrado la cámara PIR.
- Etapa 4 Siga las instrucciones en pantalla y encienda la cámara PIR, y luego toque **Próximo**. Espere el
- Paso 5 emparejamiento.
- Paso 6 Personalice el nombre de la cámara PIR, seleccione el área y luego toque **Terminado**.

6 Instalación

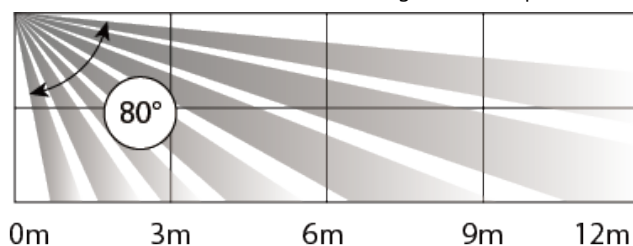
6.1 Campo de visión

El campo de visión de la cámara PIR se muestra a continuación.

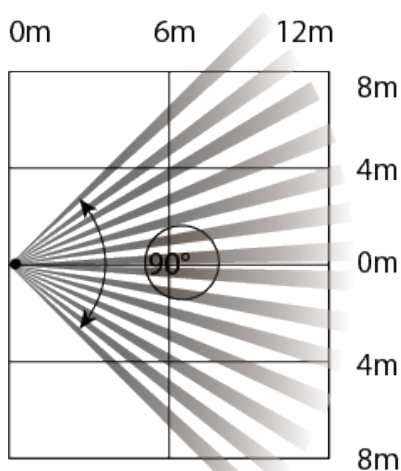


Al instalar y utilizar la cámara PIR, asegúrese de que no haya objetos que la oculten parcial o totalmente.
el campo de visión del detector.

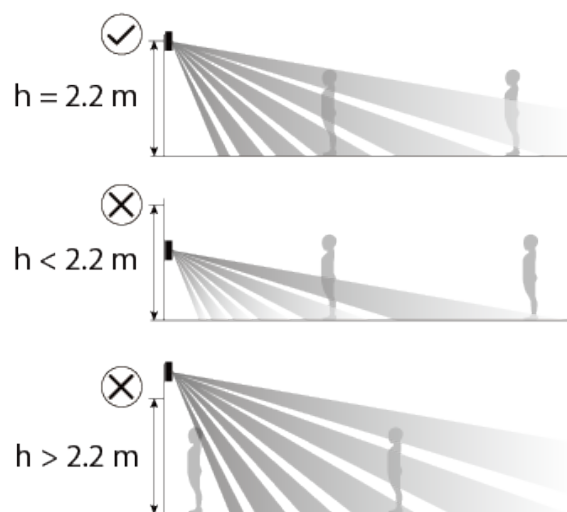
Figura 6-1 Campo de visión



a



b



c

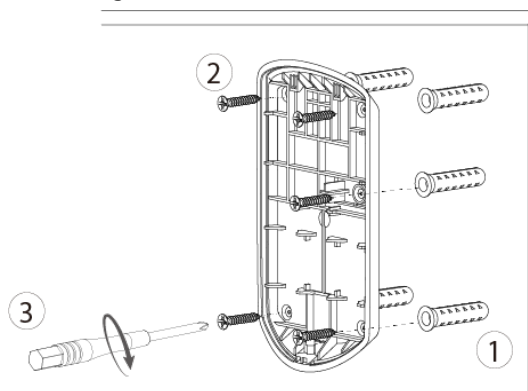
6.2 Instalación de la cámara PIR

Antes de la instalación, agregue la cámara PIR al concentrador y pruebe la intensidad de la señal y RF-HD.

Recomendamos instalar la cámara PIR en un lugar con una intensidad de señal de al menos 2 barras.

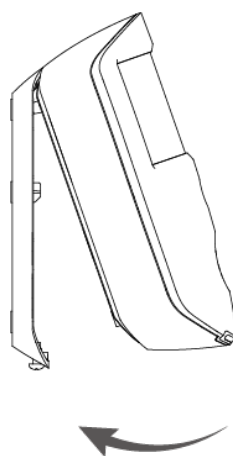
Paso 1 Perfore cuatro orificios en la pared de acuerdo con las posiciones de los orificios de la cámara PIR y luego coloque los pernos de expansión en los orificios.

Figura 6-2 Perforaciones



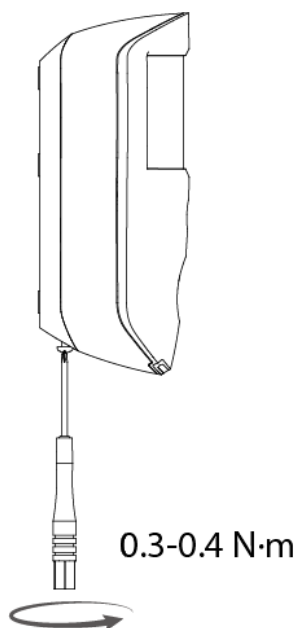
Paso 2 Cierre la cámara PIR.

Figura 6-3 Cierre la cámara PIR



Paso 3 Asegure la cámara PIR con un tornillo.

Figura 6-4 Asegure la cámara PIR con un tornillo



7 Configuración

Puede ver y editar información general de la cámara PIR.

7.1 Visualización del estado

En la pantalla del concentrador, seleccione una cámara PIR de la lista de periféricos y luego podrá ver el estado de la cámara PIR.

Tabla 7-1 Estado

Parámetro	Valor
Desactivar Temporalmente	El estado de si las funciones de la cámara PIR están habilitadas o deshabilitadas.   : Permitir.   : Solo deshabilite la alarma de sabotaje.   : Desactivar.
Temperatura	La temperatura del ambiente.
Intensidad de señal	La intensidad de la señal entre el concentrador y la cámara PIR.   : Bajo.   : Débil.   : Bien.   : Excelente.   : No.
Nivel de batería	El nivel de batería de la cámara PIR.   : Completamente cargado.   : Suficiente.   : Moderado.   : Insuficiente.   : Bajo.
Estado antimanipulación	El estado de manipulación de la cámara PIR, que reacciona al desprendimiento del cuerpo.
Estado en línea	Estado en línea y fuera de línea de la cámara PIR.   : En línea.   : Desconectado.
Introducción del tiempo de retraso	Tiempo de retardo de entrada.
Tiempo de retardo de salida	Tiempo de retardo de salida.
Estado de Zona de Protección 24 H	Estado activo de la zona de protección 24 h.   : Permitir.   : Desactivar.
Sensibilidad	Nivel de sensibilidad durante una alarma de choque.

Parámetro	Valor
transmitir a través Reloj de repetición	El estado de si la cámara PIR reenvía sus mensajes al concentrador a través del repetidor.  La cámara PIR no admite la función del repetidor (serie DHI-ARA43) para transmitir imágenes desde la cámara PIR al concentrador.
Versión del programa	La versión del programa de la cámara PIR.

7.2 Configuración de la cámara PIR

En la pantalla del concentrador, seleccione una cámara PIR de la lista de periféricos y luego toque  para configurar el parámetros de la cámara PIR.

Tabla 7-2 Descripción de parámetros

Parámetro	Descripción
Prueba de instantánea	Grifo Prueba de instantánea en la pantalla de la cámara PIR, y luego la cámara PIR tomará algunas instantáneas. Puede ver un mensaje de notificación en la lista de mensajes después.  Le recomendamos que utilice la función de prueba instantánea cuando instale la cámara PIR por primera vez. Esto le ayudará a encontrar las ubicaciones y los ángulos más adecuados.
Configuración del dispositivo	● Ver el nombre de la cámara PIR, el tipo, el SN y el modelo del dispositivo. ● Edite el nombre de la cámara PIR y luego toque Ahorrar para guardar la configuración.
Área	Seleccione el área a la que está asignada la cámara PIR.
Desactivar Temporalmente	Si envía comandos al centro de alarmas. ● Grifo Permitir, y luego la cámara PIR enviará comandos al concentrador. Permitir está configurado de forma predeterminada. ● Grifo Solo deshabilitar alarma de sabotaje, y luego el sistema solo ignorará los mensajes de alarma de manipulación. ● Grifo Desactivar, y luego la cámara PIR no enviará comandos al concentrador.

Parámetro	Descripción
Configuración de instantáneas	Configure el número de instantáneas que se pueden tomar a la vez, el intervalo y los parámetros de la imagen. ● Grifo Tiempos para tomar instantáneas y luego seleccione tiempos del 1 al 10. ● Grifo Intervalo de disparo y luego puede seleccionar 10, 30, 60 o 120 segundos. ● Grifo Resolución de imagen y cantidad y luego para la resolución de la imagen, puede seleccionar 1600 × 1200, 1280 × 960, 640 × 480 o 320 × 240. Para la cantidad de imágenes, puede seleccionar entre 1 y 20.  Para una resolución de imagen de 1600 × 1200, solo puede seleccionar entre 1 y 10 para la cantidad de imágenes.
Indicador LED	El indicador LED está habilitado de forma predeterminada. Para obtener detalles sobre el comportamiento del indicador, consulte "3.1 Apariencia".  Si el indicador LED está desactivado, el indicador LED permanecerá apagado independientemente de si la cámara PIR funciona normalmente o no.
Alarma de sobrecalentamiento	Habilitar el Alarma de sobrecalentamiento función, y luego la alarma se disparará cuando la temperatura del área donde está instalada la cámara PIR es más alta o más baja que la definida.
Zona de Protección 24H	● Si Zona de Protección 24H está habilitado, incluso el sistema está desarmado, la cámara PIR se puede armar y detecta movimiento. ● Si Zona de Protección 24H está deshabilitada, solo cuando el sistema está armado, la cámara PIR se puede armar y detecta movimiento. La cámara PIR no se armará inmediatamente, comenzará antes del final del intervalo de ping del detector concentrador (60 segundos por defecto).  Puede ir a la pantalla del hub para configurar el ping intervalo del hub-detector. Para obtener más información, consulte la del usuario manual del cubo.
Modo Hogar	Habilitar el Modo Hogar, y luego se armarán los periféricos seleccionados debajo del concentrador.
Modo de retraso en el modo de inicio	Habilitar el Modo de retraso en el modo de inicio, el periférico seleccionado debajo del concentrador se armará y la alarma no se activará hasta el final del tiempo de retraso personalizado.  solo habilitar Modo Hogar primera la Modo de retraso en Inicio Modo tomar efecto.

Parámetro	Descripción
Tiempo de retardo	El sistema le proporciona tiempo para salir o entrar en la zona de protección sin alarma. ● Tiempo de demora para ingresar al modo de armado: Cuando ingrese a la zona, si no desarma el sistema antes de que finalice el retraso, se activará una alarma.  Asegúrese de que el tiempo de demora para ingresar al modo de armado no supere los 45 segundos para cumplir con EN50131-1. ● Tiempo de retardo para salir del modo de armado: Cuando esté en la zona y arme el sistema, si no sale de la zona antes de que finalice el retraso, se activará una alarma. Puede seleccionar de 0 s a 120 s.  El modo de armado será efectivo después del tiempo de retardo.
Sensibilidad	● Ajuste el nivel de sensibilidad de la detección de movimiento. ● Seleccione entre bajo, medio y alto.
Enlace de sirena	Cuando se activa una alarma, los periféricos informarán los eventos de alarma al concentrador y alertarán con una sirena.
Detección de intensidad de señal	Pruebe la intensidad de la señal actual.
Prueba de detectores	Grifo Detección de inicio para probar el estado de la cámara PIR.
Prueba RF-HD	Grifo Detección de inicio para probar la intensidad de la señal para transmitir imágenes entre la cámara PIR y el concentrador.
Potencia de transmisión	● Seleccione entre alto, bajo y automático. ● Cuanto más altos son los niveles de potencia de transmisión, más transmisiones pueden viajar, pero aumenta el consumo de energía.  Si selecciona Bajo, la cámara PIR entrará en modo reducido Modo de sensibilidad.
Actualización en la nube	Actualizar en línea.
Borrar	Eliminar la cámara PIR.  Vaya a la pantalla central, seleccione la cámara PIR de la lista de periféricos y luego deslícese 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 un gabinete y una sala de computadoras especiales, e implemente un control de permisos de acceso y administración de claves bien hecho para evitar que el personal no autorizado realice contactos físicos, como dañar el hardware, la conexión no autorizada de un dispositivo extraíble (como un disco flash USB), puerto serie), etc.

2. Cambie las contraseñas regularmente

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

3. Establecer y actualizar contraseñas Restablecer información a tiempo

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

4. Habilitar bloqueo de cuenta

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

5. Cambiar HTTP predeterminado y otros puertos de servicio

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

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

6. Habilitar HTTPS

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

7. Enlace de dirección MAC

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

8. Asigne cuentas y privilegios de manera razonable

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

9. Deshabilite los servicios innecesarios y elija modos seguros

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

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

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

10. Transmisión encriptada de audio y video

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

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

11. Auditoría segura

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

12. Registro de red

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

13. Construir un entorno de red seguro

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

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

dispositivo.

Más información

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

ENABLING A SAFER SOCIETY AND SMARTER LIVING