



# Grabadora de vídeo en red

Manual de usuario

## Información legal

### Acerca de este documento

- Este documento incluye instrucciones para el uso y manejo del producto. Las imágenes, gráficos y demás información que se incluye a continuación son solo descriptivas y explicativas. • La información contenida en este documento está sujeta a cambios sin previo aviso debido a actualizaciones de firmware u otros motivos. Consulte la versión más reciente del documento en el sitio web de Hikvision ( <https://www.hikvision.com>) ). Salvo acuerdo en contrario, Hangzhou Hikvision Digital Technology Co., Ltd. o sus filiales (en adelante, «Hikvision») no ofrecen garantías, expresas ni implícitas.
- Utilice el Documento con la orientación y asistencia de profesionales capacitados en apoyando el Producto.

### Acerca de este producto

- Este producto solo puede disfrutar del soporte de servicio posventa en el país o región donde se encuentra. Se realiza la compra.
- Si el producto que elige es un producto de video, escanee el siguiente código QR para obtenerlo. “Iniciativas sobre el uso de productos de vídeo” y léalo con atención.



### Reconocimiento de los derechos de propiedad intelectual

- Hikvision posee los derechos de autor y/o patentes relacionados con la tecnología incorporada en el Productos descritos en este Documento, que pueden incluir licencias obtenidas de terceros. • Cualquier parte del Documento, incluyendo texto, imágenes, gráficos, etc., pertenece a Hikvision. Ninguna parte de este Documento puede ser extractada, copiada, traducida o modificada, total o parcialmente, por ningún medio sin permiso escrito. y otras marcas comerciales y logotipos de
- **HIKVISION** Hikvision son propiedad de Hikvision en varias jurisdicciones. •

Otras marcas comerciales y logotipos mencionados son propiedad de sus respectivos dueños.

- **HDMI**™ Los términos HDMI y HDMI High-Definition Multimedia Interface, y el logotipo HDMI son marcas comerciales o marcas comerciales registradas de HDMI Licensing Administrator, Inc. en los Estados Unidos y otros países.

## AVISO LEGAL

- EN LA MEDIDA MÁXIMA PERMITIDA POR LA LEY APLICABLE, ESTE DOCUMENTO Y LA

EL PRODUCTO DESCRITO, CON SU HARDWARE, SOFTWARE Y FIRMWARE, SE PROPORCIONA "TAL CUAL" Y "CON TODOS SUS FALLOS Y ERRORES". HIKVISION NO OFRECE GARANTÍAS, EXPRESAS O IMPLÍCITAS, INCLUYENDO, SIN LIMITACIÓN, LAS DE COMERCIABILIDAD, CALIDAD SATISFACTORIA O IDONEIDAD PARA UN PROPÓSITO PARTICULAR. EL USO DEL PRODUCTO POR SU PARTE ES BAJO SU PROPIA RESPONSABILIDAD.

EN NINGÚN CASO HIKVISION SERÁ RESPONSABLE ANTE USTED POR DAÑOS ESPECIALES, DERIVADOS, INCIDENTALES O INDIRECTOS, INCLUYENDO, ENTRE OTROS, DAÑOS POR PÉRDIDA DE BENEFICIOS COMERCIALES, INTERRUPCIÓN DE NEGOCIOS O PÉRDIDA DE DATOS, CORRUPCIÓN DE SISTEMAS O PÉRDIDA DE DOCUMENTACIÓN, YA SEA CON BASE EN INCUMPLIMIENTO DE CONTRATO, AGRAVIO (INCLUIDA LA NEGLIGENCIA), RESPONSABILIDAD DEL PRODUCTO O DE OTRO MODO, EN RELACIÓN CON EL USO DEL PRODUCTO, INCLUSO SI HIKVISION HA SIDO ADVERTIDO DE LA POSIBILIDAD DE DICHOS DAÑOS O PÉRDIDAS.

- USTED RECONOCE QUE LA NATURALEZA DE INTERNET CONLLEVA RIESGOS DE SEGURIDAD INHERENTES, Y HIKVISION NO ASUMIRÁ NINGUNA RESPONSABILIDAD POR FUNCIONAMIENTO ANORMAL, FUGA DE PRIVACIDAD U OTROS DAÑOS RESULTANTES DE UN ATAQUE CIBERNÉTICO, UN ATAQUE DE HACKERS, UNA INFECCIÓN DE VIRUS U OTROS RIESGOS DE SEGURIDAD DE INTERNET; SIN EMBARGO, HIKVISION PROPORCIONARÁ SOPORTE TÉCNICO OPORTUNO SI ES NECESARIO.
- USTED ACEPTA UTILIZAR ESTE PRODUCTO EN CUMPLIMIENTO CON TODAS LAS LEYES APLICABLES Y ES EL ÚNICO RESPONSABLE DE ASEGURARSE DE QUE SU USO SE AJUSTE A LA LEY APLICABLE.

ESPECIALMENTE, USTED ES RESPONSABLE DE USAR ESTE PRODUCTO DE FORMA QUE NO INFRINJA LOS DERECHOS DE TERCEROS, INCLUYENDO, SIN LIMITACIÓN, LOS DERECHOS DE PUBLICIDAD, DERECHOS DE PROPIEDAD INTELECTUAL O PROTECCIÓN DE DATOS Y OTROS DERECHOS DE PRIVACIDAD. NO DEBERÁ UTILIZAR ESTE PRODUCTO PARA NINGÚN USO FINAL PROHIBIDO, INCLUYENDO EL DESARROLLO O LA PRODUCCIÓN DE ARMAS DE DESTRUCCIÓN MASIVA, EL DESARROLLO O LA PRODUCCIÓN DE ARMAS QUÍMICAS O BIOLÓGICAS, CUALQUIER ACTIVIDAD EN EL CONTEXTO RELACIONADO CON CUALQUIER EXPLOSIVO NUCLEAR O CICLO DE COMBUSTIBLE NUCLEAR INSEGURO, O EN APOYO DE ABUSOS DE LOS DERECHOS HUMANOS.

- EN CASO DE CONFLICTO ENTRE ESTE DOCUMENTO Y LA LEY APLICABLE, LA LO ÚLTIMO PREVALECE.

© Hangzhou Hikvision Digital Technology Co., Ltd. Todos los derechos reservados.

## Información regulatoria

### Información de la FCC

Tenga en cuenta que los cambios o modificaciones no aprobados expresamente por la parte responsable del cumplimiento podrían anular la autoridad del usuario para operar el equipo.

Cumplimiento de la FCC: Este equipo ha sido probado y cumple con los límites establecidos en la parte 15 de las Normas de la FCC. Estos límites están diseñados para proporcionar una protección razonable contra interferencias perjudiciales en una instalación residencial. Este equipo genera, utiliza y puede radiar energía de radiofrecuencia y, si no se instala y utiliza de acuerdo con las instrucciones, puede causar interferencias perjudiciales en las comunicaciones por radio. Sin embargo, no se garantiza que no se produzcan interferencias en una instalación en particular. Si este equipo causa interferencias perjudiciales en la recepción de radio o televisión, lo cual se puede determinar encendiendo y apagando el equipo, se recomienda al usuario que intente corregir la interferencia mediante una o más de las siguientes medidas: • Reorientar o reubicar la antena receptora. • Aumentar la separación entre el equipo y el receptor. •

Conectar el equipo a una

toma de corriente en un circuito diferente al que está

conectado el receptor.

conectado.

• Consulte al distribuidor o a un técnico de radio/TV experimentado para obtener ayuda.

Condiciones de la

FCC: Este dispositivo cumple con la sección 15 de las Normas de la FCC. Su funcionamiento está sujeto a las dos condiciones

siguientes: • Este dispositivo no puede causar interferencias

perjudiciales. • Este dispositivo debe aceptar cualquier interferencia recibida, incluidas las que puedan causar un funcionamiento no deseado.

### Declaración de conformidad de la UE



Este producto y, si corresponde, también los accesorios suministrados están marcados con "CE" y, por lo tanto, cumplen con las normas europeas armonizadas aplicables enumeradas en la Directiva EMC 2014/30/UE, la Directiva LVD 2014/35/UE y la Directiva RoHS 2011/65/UE.



2012/19/UE (Directiva RAEE): Los productos marcados con este símbolo no pueden desecharse como residuos municipales sin clasificar en la Unión Europea. Para un reciclaje adecuado, devuelva este producto a su proveedor local.



Compre equipos nuevos equivalentes o deséchelos en los puntos de recogida designados. Para más información, consulte: <http://www.recyclethis.info> .

Reglamento (UE) 2023/1542 (Reglamento sobre baterías): Este producto contiene una batería y cumple con el Reglamento (UE) 2023/1542. La batería no puede desecharse como residuo municipal sin clasificar en la Unión Europea. Consulte la documentación del producto para obtener información específica sobre la batería. La batería está marcada con este símbolo, que puede incluir letras que indican cadmio (Cd) o plomo (Pb). Para un reciclaje adecuado, devuelva la batería a su proveedor o a un punto de recogida designado. Para más información, visite: <http://www.recyclethis.info> .

## Modelo aplicable

Este manual es aplicable a los siguientes modelos, pero no todas las funciones de este manual son válidas. compatible con cada modelo.

Tabla 1-1 Modelo aplicable

Serie	Modelo
DS-7600NI-I2	DS-7608NI-I2
	DS-7616NI-I2
	DS-7632NI-I2
DS-7600NI-I2/P	DS-7608NI-I2/8P
	DS-7616NI-I2/16P
	DS-7632NI-I2/16P
DS-7700NI-I4	DS-7708NI-I4
	DS-7716NI-I4
	DS-7732NI-I4
DS-7700NI-I4/P	DS-7708NI-I4/8P
	DS-7716NI-I4/16P
	DS-7732NI-I4/16P
	DS-7732NI-I4/24P
DS-7600NI-M1/P	DS-7604NI-M1/4P
DS-7608NI-M2	DS-7608NI-M2
	DS-7616NI-M2
	DS-7632NI-M2
DS-7600NI-M2/P	DS-7608NI-M2/8P
	DS-7616NI-M2/16P
DS-7700NI-M4	DS-7716NI-M4
	DS-7732NI-M4
	DS-7764NI-M4
DS-7700NI-M4/P	DS-7708NI-M4/8P

Serie	Modelo
	DS-7716NI-M4/16P
	DS-7732NI-M4/16P
	DS-7732NI-M4/24P
DS-9600NI-M8	DS-9616NI-M8
	DS-9632NI-M8
	DS-9664NI-M8
	DS-96128NI-M8
DS-9600NI-M8/R	DS-9616NI-M8/R
	DS-9632NI-M8/R
	DS-9664NI-M8/R
	DS-96128NI-M8/R
DS-9600NI-M16	DS-9616NI-M16
	DS-9632NI-M16
	DS-9664NI-M16
	DS-96128NI-M16
DS-9600NI-M16/R	DS-9616NI-M16/R
	DS-9632NI-M16/R
	DS-9664NI-M16/R
	DS-96128NI-M16/R
DS-7600NXI-M2/P/VPro	DS-7608NXI-M2/8P/VPro
	DS-7616NXI-M2/16P/VPro
DS-7600NXI-M2/VPro	DS-7608NXI-M2/VPro
	DS-7616NXI-M2/VPro
DS-7700NXI-M4/VPro	DS-7716NXI-M4/VPro
	DS-7732NXI-M4/VPro
DS-7700NXI-M4/16P/VPro	DS-7716NXI-M4/16P/VPro
	DS-7732NXI-M4/16P/VPro
DS-8600NI-M16	DS-86128NI-M16

Serie	Modelo
DS-9600NXI-M8/VPro	DS-9616NXI-M8/VPro
	DS-9632NXI-M8/VPro
	DS-9664NXI-M8/VPro
	DS-96128NXI-M8/VPro
DS-9600NXI-M8R/VPro	DS-9616NXI-M8R/VPro
	DS-9632NXI-M8R/VPro
	DS-9664NXI-M8R/VPro
	DS-96128NXI-M8R/VPro
DS-9600NXI-M16/VPro	DS-9632NXI-M16/VPro
	DS-9664NXI-M16/VPro
	DS-96128NXI-M16/VPro
DS-9600NXI-M16R/VPro	DS-9632NXI-M16R/VPro
	DS-9664NXI-M16R/VPro
	DS-96128NXI-M16R/VPro
DS-7600NXI-I2/S	DS-7608NXI-I2/S
	DS-7616NXI-I2/S
	DS-7632NXI-I2/S
DS-7600NXI-I2/P/S	DS-7608NXI-I2/8P/S
	DS-7616NXI-I2/16P/S
	DS-7632NXI-I2/16P/S
DS-7700NXI-I4/S	DS-7716NXI-I4/S
	DS-7732NXI-I4/S
DS-7700NXI-I4/P/S	DS-7716NXI-I4/16P/S
	DS-7732NXI-I4/16P/S
DS-8600NXI-I8/S	DS-8616NXI-I8/S
	DS-8632NXI-I8/S
	DS-8664NXI-I8/S
DS-8600NXI-I8/24P/S	DS-8632NXI-I8/24P/S




Serie	Modelo
DS-9600NXI-I8/S	DS-9616NXI-I8/S
	DS-9632NXI-I8/S
	DS-9664NXI-I8/S
DS-96000NI-H16R	DS-96256NI-H16R
	DS-96256NI-H16R/LCD
DS-96000NI-H20R	DS-96128NI-H20R
	DS-96128NI-H20R/LCD
	DS-96256NI-H20R
	DS-96256NI-H20R/LCD
DS-96000NI-H30R	DS-96128NI-H30R
	DS-96128NI-H30R/LCD
	DS-96256NI-H30R
	DS-96256NI-H30R/LCD
DS-9600NI-G8R	DS-9632NI-G8R
iDS-6700NXI-M1/X	iDS-6704NXI-M1/X
	iDS-6708NXI-M1/X
	iDS-6716NXI-M1/X
iDS-7600NXI-M1/X	iDS-7608NXI-M1/X
	iDS-7616NXI-M1/X
iDS-7600NXI-M2/X	iDS-7608NXI-M2/X
	iDS-7616NXI-M2/X
	iDS-7632NXI-M2/X
iDS-7600NXI-M2/P/X	iDS-7608NXI-M2/8P/X
	iDS-7616NXI-M2/16P/X
iDS-7700NXI-M4/X	iDS-7716NXI-M4/X
	iDS-7732NXI-M4/X
iDS-7700NXI-M4/16P/X	iDS-7716NXI-M4/16P/X
	iDS-7732NXI-M4/16P/X

Serie	Modelo
iDS-9632NXI-M8/X	iDS-9632NXI-M8/X
	iDS-9664NXI-M8/X
	iDS-96128NXI-M8/X
iDS-9600NXI-M8R/X	iDS-9632NXI-M8R/X
	iDS-9664NXI-M8R/X
	iDS-96128NXI-M8R/X
iDS-9600NXI-M16/X	iDS-9632NXI-M16/X
	iDS-9664NXI-M16/X
iDS-9600NXI-M16R/X	iDS-9632NXI-M16R/X
	iDS-9664NXI-M16R/X
iDS-96000NXI-H16R	iDS-96064NXI-H16R
	iDS-96128NXI-H16R
	iDS-96128NXI-H16R/LCD
iDS-96000NXI-H24R	iDS-96128NXI-H24R
	iDS-96128NXI-H24R/LCD
	iDS-96256NXI-H24R
	iDS-96256NXI-H24R/LCD
DS-7600NXI-I2/VPro	DS-7608NXI-I2/VPro
	DS-7616NXI-I2/VPro
	DS-7632NXI-I2/VPro
DS-7600NXI-I2/16P/VPro	DS-7632NXI-I2/16P/VPro
	DS-7616NXI-I2/16P/VPro
DS-7700NXI-I4/16P/VPro	DS-7716NXI-I4/16P/VPro
	DS-7732NXI-I4/16P/VPro
DS-7700NXI-I4/VPro	DS-7716NXI-I4/VPro
	DS-7732NXI-I4/VPro
DS-7600NXI-I2/8P/VPro	DS-7608NXI-I2/8P/VPro
DS-9600NXI-I16R/VPro	DS-9632NXI-I16R/VPro

Serie	Modelo
	DS-9664NXI-I16R/VPro
DS-9600NXI-I16/VPro	DS-9632NXI-I16/VPro
	DS-9664NXI-I16/VPro
DS-9600NXI-I8R/VPro	DS-9616NXI-I8R/VPro
	DS-9632NXI-I8R/VPro
	DS-9664NXI-I8R/VPro
DS-9600NXI-I8/VPro	DS-9616NXI-I8/VPro
	DS-9632NXI-I8/VPro
	DS-9664NXI-I8/VPro
DS-8600NXI-I8/VPro	DS-8616NXI-I8/VPro
	DS-8632NXI-I8/VPro
	DS-8664NXI-I8/VPro

## Instrucciones de seguridad

- La configuración adecuada de todas las contraseñas y otras configuraciones de seguridad es responsabilidad del instalador y/o usuario final.
- En el uso del producto, debe cumplir estrictamente con las normas de seguridad eléctrica de la nación y la región.
- Conecte firmemente el enchufe a la toma de corriente. No conecte varios dispositivos a la misma toma. Adaptador. Apague el dispositivo antes de conectar y desconectar accesorios y periféricos. • ¡Peligro de descarga eléctrica! Desconecte todas las fuentes de alimentación antes de realizar tareas de mantenimiento. • El equipo debe estar conectado a una toma de corriente con toma de tierra. • La toma de corriente debe estar instalada cerca del dispositivo y ser fácilmente accesible.
- El dispositivo con terminales de  indicando tensión peligrosa, el cableado externo conectado a la señalización requiere la instalación por parte de una persona cualificada.
- Nunca coloque el dispositivo en una ubicación inestable. El dispositivo podría caerse y causar lesiones personales graves, lesiones o muerte.
- El voltaje de entrada debe cumplir con el SELV (voltaje extra bajo de seguridad) y el LPS (voltaje de potencia limitado). Fuente de alimentación) según la norma IEC62368. • ¡Corriente de contacto alta! Conecte a tierra antes de conectar a la fuente de alimentación. • Si el dispositivo emite humo, olor o ruido, apáguelo inmediatamente y desenchúfelo. cable y luego comuníquese con el centro de servicio.
- Utilice el dispositivo junto con un SAI y, si es posible, utilice el disco duro recomendado por el fabricante. • Este equipo no es apto para su uso en lugares con alta probabilidad de niños. • PRECAUCIÓN: Riesgo de explosión si se sustituye la batería por una de tipo incorrecto. • No ingiera la batería. ¡Peligro de quemaduras químicas! • Este producto contiene una batería de tipo botón. Si se ingiere la batería, puede causar quemaduras internas graves en tan solo 2 horas e incluso la muerte.
- El reemplazo incorrecto de la batería por un tipo incorrecto puede anular una protección (por ejemplo, por ejemplo, en el caso de algunos tipos de baterías de litio).
- No arroje la batería al fuego ni a un horno caliente, ni la aplaste ni la corte mecánicamente. lo que podría provocar una explosión.
- No deje la batería en un entorno con una temperatura extremadamente alta, ya que podría provocar una explosión o la fuga de líquido o gas inflamable. • No someta la batería a una presión de aire extremadamente baja, ya que podría provocar una explosión o la fuga de líquido o gas inflamable. Fuga de líquido o gas inflamable. • Deseche las baterías usadas según las instrucciones. • Mantenga las partes del cuerpo alejadas de las aspas y los motores del ventilador. Desconecte la fuente de alimentación durante servicio.
- Mantenga las partes del cuerpo alejadas de los motores. Desconecte la fuente de alimentación durante el mantenimiento. • Utilice únicamente fuentes de alimentación del mismo modelo que el original o fuentes de alimentación LPS con el mismo voltaje y corriente eléctrica.

## Consejos preventivos y de precaución

Antes de conectar y operar su dispositivo, tenga en cuenta los siguientes consejos:

- El dispositivo está diseñado solo para uso en interiores. Instálelo en un entorno bien ventilado y sin polvo.  
sin líquidos.

Asegúrese de que la grabadora esté bien sujeta a un estante o estantería. Los golpes o sacudidas fuertes que sufra la grabadora por caídas pueden dañar sus delicados componentes electrónicos. El dispositivo no debe exponerse a goteos ni salpicaduras de agua, ni colocarse sobre él objetos que contengan líquido, como jarrones.

No coloque fuentes de llamas abiertas, como velas encendidas, sobre el dispositivo. No obstruya la ventilación cubriendo las aberturas con objetos como periódicos, manteles o cortinas. Nunca bloquee las aberturas colocando el dispositivo sobre una cama, un sofá, una alfombra u otra superficie similar.

- Para ciertos modelos, asegúrese de que el cableado de los terminales sea correcto para la conexión a una fuente de alimentación de CA. • Para ciertos modelos, el equipo ha sido diseñado y, cuando es necesario, modificado para la conexión.  
a un sistema de distribución de energía de TI.

-  Identifica el soporte de la batería en sí e identifica la posición de la(s) celda(s) dentro del soporte de la batería.

- + identifica el/los terminal(es) positivo(s) del dispositivo que se utiliza con corriente continua o que la genera, y - identifica el/los terminal(es) negativo(s) del dispositivo que se utiliza con corriente continua o que la genera.  
actual.

- Si el dispositivo ha estado apagado o colocado durante un tiempo prolongado, es posible que su batería de botón o moneda se agote.  
Sin energía.

- Cuando la batería de la moneda/botón se agota, la hora del sistema puede ser incorrecta.  
Contacte con el servicio posventa para sustituir la batería.



- Mantenga una distancia mínima de 200 mm (7,87 pulgadas) alrededor del equipo para una ventilación adecuada. • En ciertos modelos, asegúrese de que el cableado de los terminales sea correcto para la conexión a una fuente de alimentación de CA. • No toque los bordes ni las esquinas afilados. • Cuando el dispositivo funcione a más de 45 °C (113 °F), o la temperatura de su disco duro en SMART supere el valor indicado, asegúrese de que el dispositivo esté funcionando en un entorno fresco o reemplace el(los) HDD para que la temperatura del HDD en SMART sea inferior al valor indicado.

- Coloque un protector contra sobretensiones en la abertura de entrada del dispositivo en condiciones especiales, como en la cima de una montaña, una torre de hierro o un bosque.

- No toque los componentes expuestos (como los contactos metálicos de las entradas) y espere al menos 5 minutos, ya que podría quedar electricidad después de apagar el dispositivo. • El puerto USB del equipo se utiliza

únicamente para conectar un ratón, teclado, memoria USB o adaptador Wi-Fi. La corriente del dispositivo conectado no debe superar los 0,1 A.

- El puerto serie del dispositivo se utiliza únicamente para depuración. • Si el puerto de salida de alimentación del dispositivo no cumple con la fuente de alimentación limitada, el dispositivo conectado alimentado por este puerto deberá estar equipado con una carcasa resistente al fuego. • Si el dispositivo incluye un adaptador de corriente, utilice únicamente el adaptador incluido.

- Para el dispositivo con pegatina o  , preste atención a las siguientes precauciones: **PRECAUCIÓN: Caliente**  
¡No tocar las piezas! Podría quemarse los dedos al manipularlas. Espere media hora después de apagar el aparato antes de manipularlas.
- Si es necesario instalar el dispositivo en la pared o en el techo,
  1. Instale el dispositivo de acuerdo con las instrucciones de este manual.
  2. Para evitar lesiones, este dispositivo debe estar firmemente fijado a la superficie de instalación.  
de acuerdo con las instrucciones de instalación.
- Bajo temperaturas de trabajo elevadas (40 °C (104 °F) a 55 °C (131 °F)), la potencia de algunos  
Los adaptadores pueden disminuir.
- Asegúrese de que la alimentación esté desconectada antes de cablear, instalar o desmontar el  
dispositivo.
- Si necesita cablear el dispositivo usted mismo, seleccione el cable correspondiente para suministrar energía.  
Según los parámetros eléctricos indicados en el dispositivo. Pele el cable con un pelacables estándar en el punto  
correspondiente. Para evitar consecuencias graves, la longitud del cable pelado debe ser la adecuada y los conductores  
no deben quedar expuestos. • Si el dispositivo emite humo, olor o ruido,  
apáguelo inmediatamente, desenchufe el cable de alimentación y contacte con el centro de servicio.




## Convención de contenido

Para simplificar la descripción, lea las siguientes convenciones.

- El término grabador o dispositivo se refiere principalmente a una grabadora de video.
- El término dispositivo IP se refiere principalmente a una cámara de red (cámara IP), un domo IP (domo de velocidad), un DVS (cámara digital) Servidor de video), o NVS (Servidor de video en red).
- Canal se refiere principalmente al canal de video en la grabadora de video.

## Convenciones de símbolos

Los símbolos que pueden encontrarse en este documento se definen a continuación.

Símbolo	Descripción
 Peligro	Indica una situación peligrosa que, si no se evita, provocará o podría provocar la muerte o lesiones graves.
 Precaución	Indica una situación potencialmente peligrosa que, si no se evita, podría provocar daños en el equipo, pérdida de datos, degradación del rendimiento o resultados inesperados.
 Nota	Proporciona información adicional para enfatizar o complementar puntos importantes del texto principal.






## Descripción del indicador y la interfaz

### Descripción del indicador del panel frontal

Los indicadores en el panel frontal indican diferentes estados de funcionamiento de su dispositivo.

Tabla 1-1 Descripción del indicador común


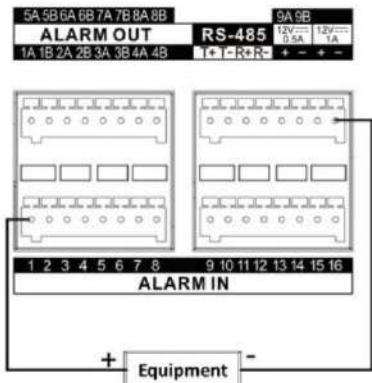
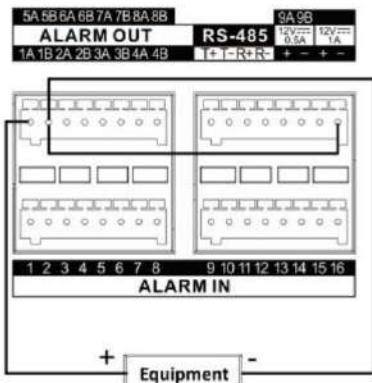
Indicador	Descripción
	El indicador se enciende cuando el dispositivo está encendido.
	El indicador parpadea cuando se leen o escriben datos en el disco duro.
	El indicador parpadea cuando la conexión de red funciona correctamente.

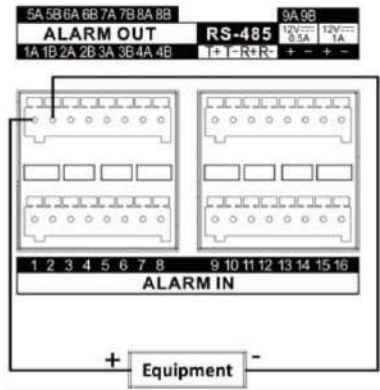

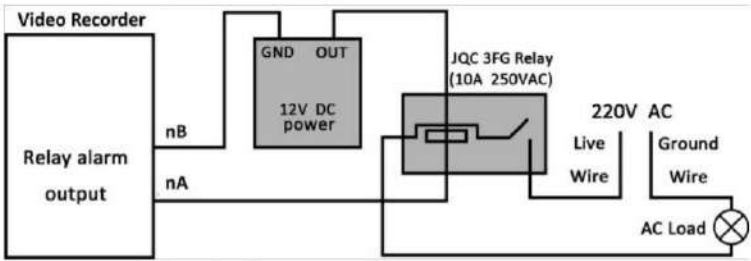
### Descripción de la interfaz

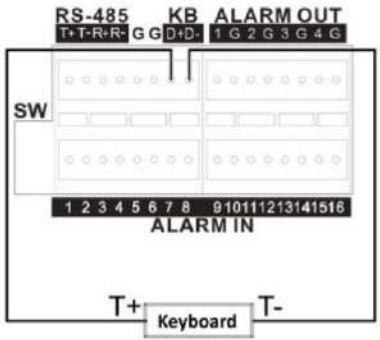
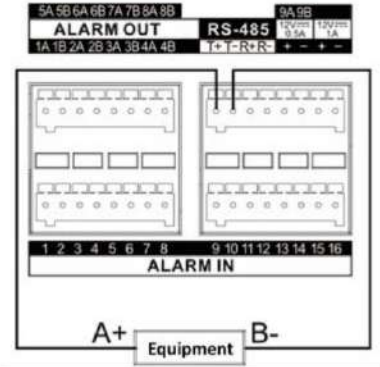
Las interfaces del panel varían según el modelo. Consulte la siguiente tabla para conocer las interfaces comunes. descripción.

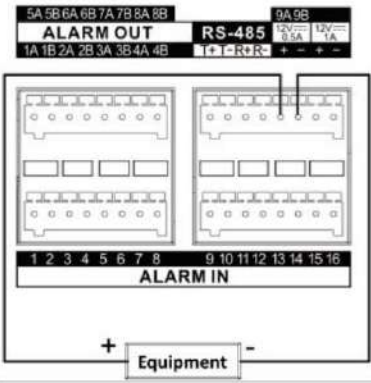
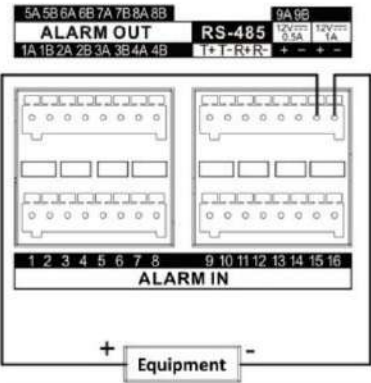
Tabla 1-2 Descripción del indicador común

Artículo	Descripción
VIDEO EN	Interfaz BNC para Turbo HD y entrada de video analógico.
SALIDA DE VIDEO	Conector BNC para salida de vídeo.
ENTRADA DE AUDIO	Conector RCA para entrada de audio.
SALIDA DE AUDIO	Conector RCA para salida de audio.
ENTRADA DE LÍNEA	Conector RCA para entrada de audio bidireccional.
USB	Interfaz de bus serie universal (USB) para dispositivo adicional.
VGA	Conector DB15 para salida de vídeo local y visualización de menú.
HDMI	Interfaz HDMI para salida de vídeo.
RS-485	Interfaz serial RS-485 para unidad de giro e inclinación, domo de velocidad, etc.
RS-232	Interfaz RS-232 para configuración de parámetros, o canal transparente.
LAN	Interfaz Ethernet autoadaptativa RJ-45.
eSATA	Interfaz de almacenamiento y expansión para grabación o respaldo.
Tierra	Suelo.

Artículo	Descripción
Interruptor de encendido	Interruptor para encender/apagar el dispositivo.
Fuente de alimentación	Fuente de alimentación de 100 a 240 VCA, 48 VCC o 12 VCC.
Tarjeta USIM	Ranura para tarjeta UIM/SIM.
	Interfaz de antena SMA.
ALARMA EN	<p>La entrada de alarma recibe la señal de entrada de alarma. El terminal positivo del equipo (+) debe conectarse a un número y el terminal negativo del equipo (-) debe conectarse a “-“ o “G”.</p> <p>Utilice el siguiente diagrama como ejemplo de conexión para la entrada de alarma.</p> 
ALARMA FUERA	<p>La salida de alarma envía una señal de alarma.</p> <p>Cuando un equipo utiliza alimentación de CC, su terminal positivo (+) debe Conéctese a un número con “A”, y su terminal negativo (-) debe ser Conéctese al número correspondiente con “B”, y luego conéctese a “-“ o “G”. Utilice el siguiente diagrama como ejemplo de conexión de salida de alarma para CC. equipo.</p> 

Artículo	Descripción
	<p>Cuando un equipo utiliza alimentación de CA, su terminal positivo (+) debe conectarse a un número con "A", y su terminal negativo (-) debe conectarse al número correspondiente con "B".</p> <p>Utilice el siguiente diagrama como ejemplo de conexión de salida de alarma para equipos de CA.</p>  <p> <b>Nota</b></p> <p>Debido a que el voltaje de carga de CA puede ser alto, utilice un relé externo por seguridad.</p> <p>Utilice el siguiente diagrama como referencia.</p>  <p><b>Note:</b> n represents a number in nA or nB, n can be 1 to 9.</p>
KB	<p>KB representa el teclado. Conecte «D+» y «D-» a «T+» y «T-», respectivamente.</p> <p>Utilice el siguiente diagrama como referencia.</p>

Artículo	Descripción
	
RS-485	<p>RS-485 es una especificación eléctrica de un sistema multipunto semidúplex de dos cables.</p> <p>Conexión en serie. Conecte "T+" y "T-" a "A+" y "B-", respectivamente.</p> <p>Utilice el siguiente diagrama como referencia.</p> 
Control 12V/ 12V== 0.5A	<p>Salida de alimentación controlable de 12 VCC y 0,5/1 A para dispositivo de alarma externo.</p> <p>La energía se encenderá cuando se active la salida de alarma correspondiente.</p> <p>Utilice el siguiente diagrama como referencia.</p>

Artículo	Descripción
	
12 V CC/ 12V $\overline{\text{---}}$ 1A	<p>Proporciona una salida de potencia de 12 VCC y 1 A.</p> <p>Utilice el siguiente diagrama como referencia.</p> 

## Instalación del disco duro

Si su dispositivo no admite el intercambio en caliente de discos duros, desconéctelo de la alimentación antes de instalar un disco duro (HDD). Para esta instalación, utilice un HDD recomendado por el fabricante.

Escanee el código QR a continuación para ver videos de instalación de HDD.



Figura 1-1 Instalación del disco duro

## Instalación del soporte

La instalación del soporte se aplica cuando es necesario quitar la cubierta del dispositivo e instalar el disco duro en el soporte interno.

### Pasos

1. Afloje los tornillos de la parte posterior y empuje la cubierta hacia atrás para quitarla.

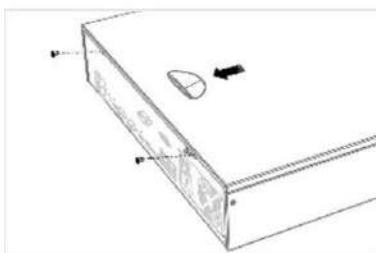


Figura 1-2 Retire la cubierta

2. Fije el disco duro en el soporte con tornillos.



Nota

Desinstale primero el soporte de la capa superior antes de instalar el disco duro en el soporte de la capa inferior.

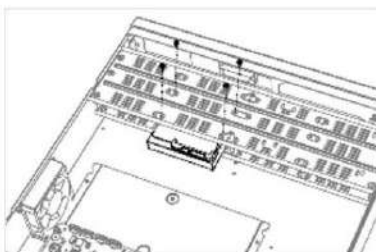


Figura 1-3 Reparación del disco duro

3. Conecte el cable de datos y el cable de alimentación.

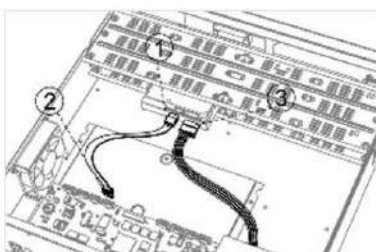


Figura 1-4 Conectar el cable



Nota

Puede repetir los pasos anteriores para instalar otros discos duros.

4. Vuelva a instalar la cubierta del dispositivo y apriete los tornillos.

### Instalación enchufable y extraíble del panel frontal

La instalación mediante conector y extracción del panel frontal se aplica cuando necesita abrir el panel frontal del dispositivo con una llave e instalar el disco duro.

Pasos

1. Fije las orejas de montaje al disco duro con tornillos.

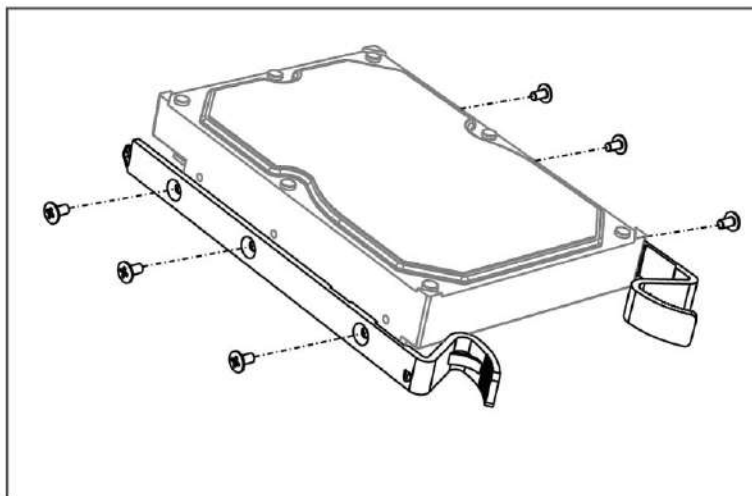


Figura 1-5 Fije las orejas de montaje al disco duro

2. Desbloquee el panel frontal con la llave adjunta y presione los botones en ambos lados del panel frontal. panel para abrirlo.

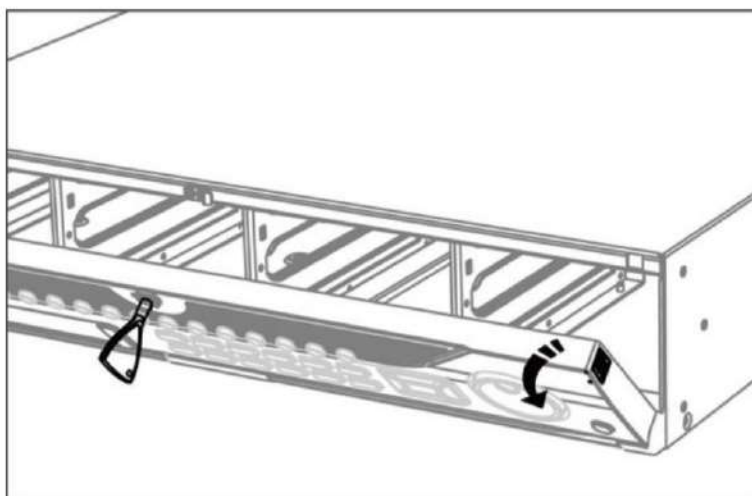


Figura 1-6 Panel frontal abierto

3. Inserte el disco duro hasta que quede firmemente fijado.



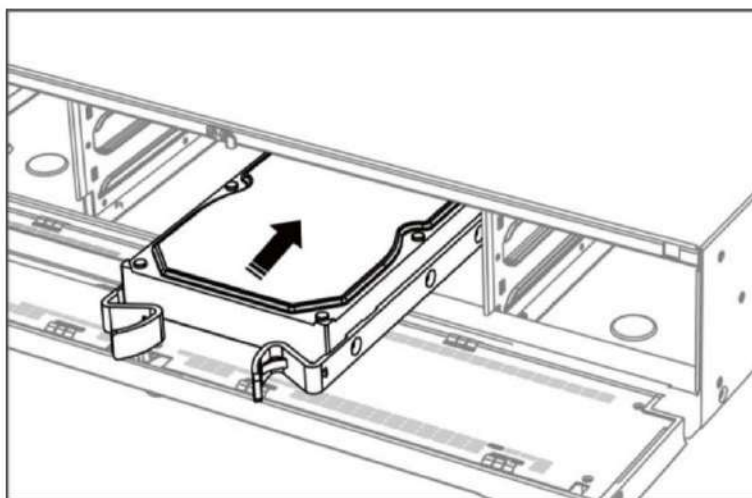


Figura 1-7 Insertar disco duro

4. Opcional: repita los pasos anteriores para instalar otros discos duros.
5. Cierre el panel frontal y bloquéelo con la llave.

#### Instalación de la caja del disco duro

La instalación de la carcasa del disco duro se refiere al método en el que usted instala el disco duro en la carcasa y luego conecta la carcasa del disco duro en la ranura.

##### Pasos

1. Desbloquee el panel frontal con la llave del panel.
2. Extraiga el panel frontal del dispositivo y colóquelo un poco por encima del mango izquierdo.



Nota

El ángulo entre el panel frontal y el dispositivo debe ser inferior a 10°.

3. Presione el botón azul para levantar el asa, sosténgala y saque la carcasa del disco duro.  
la ranura.
4. Fije el disco duro en la carcasa del mismo.
  - 1) Coloque un disco duro en la caja. La interfaz SATA debe estar orientada hacia la parte inferior de la caja.
  - 2) Ajuste la posición del disco duro. Asegúrese de que la parte trasera del disco duro esté alineada con la parte inferior.
  - 3) Utilice un destornillador para fijar los cuatro tornillos en los orificios de ambos lados.

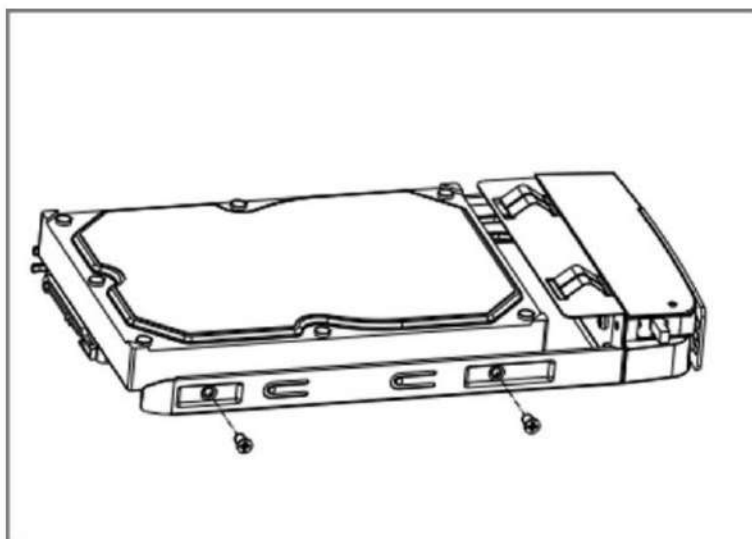


Figura 1-8 Reparación del disco duro

5. Empuje la carcasa del disco duro nuevamente dentro de la ranura.

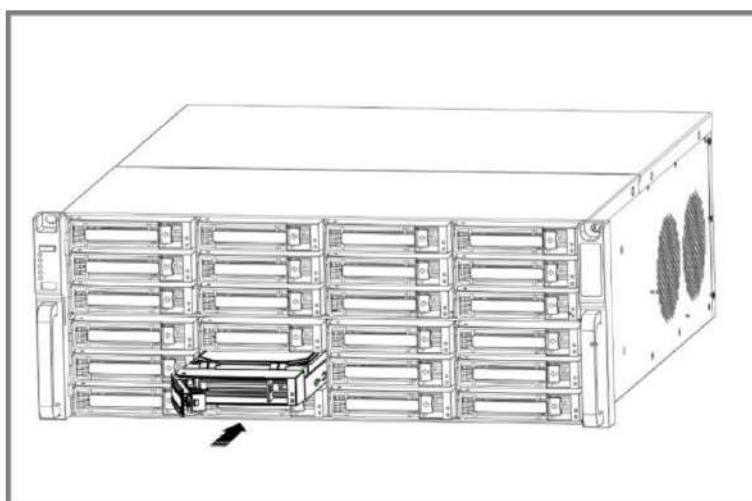


Figura 1-9 Inserte la carcasa del disco duro en la ranura

6. Presione la manija hasta oír un clic. Así se fija la carcasa del disco duro. Repita los pasos anteriores para instalarlo.

El resto de cajas de disco duro.

7. Cierre el panel frontal y bloquéelo con la llave del panel.

## Instalación fija en la parte inferior

La instalación fija en la parte inferior se aplica cuando necesita instalar y fijar el disco duro en la parte inferior del dispositivo.

### Pasos

1. Retire la cubierta del dispositivo aflojando los tornillos de los paneles.

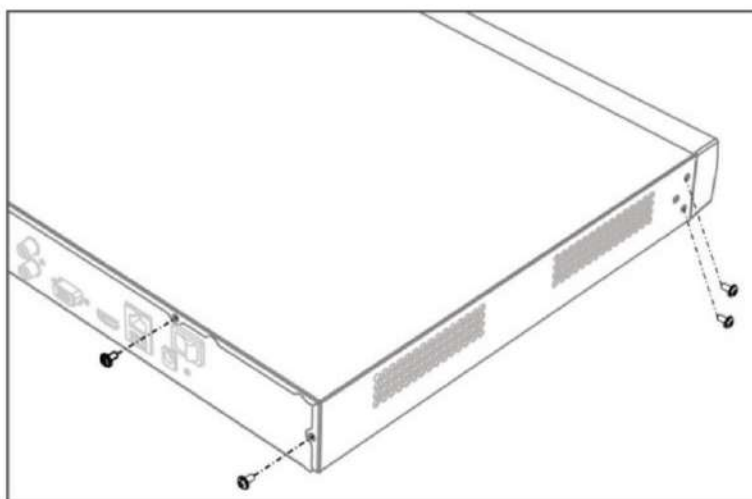


Figura 1-10 Retire la cubierta 2.

Conecte el cable de datos y el cable de alimentación.

- 1) Conecte un extremo del cable de datos a la placa base del dispositivo.
- 2) Conecte el otro extremo del cable de datos al disco duro.
- 3) Conecte un extremo del cable de alimentación al disco duro.
- 4) Conecte el otro extremo del cable de alimentación a la placa base del dispositivo.

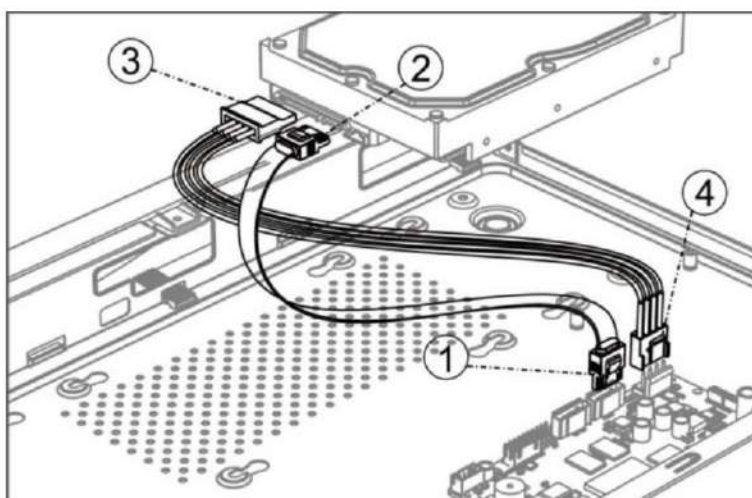


Figura 1-11 Conexión de cables

3. Configure el dispositivo, haga coincidir las roscas de los tornillos del HDD con los orificios reservados en la parte inferior del dispositivo y fije el disco duro con tornillos.

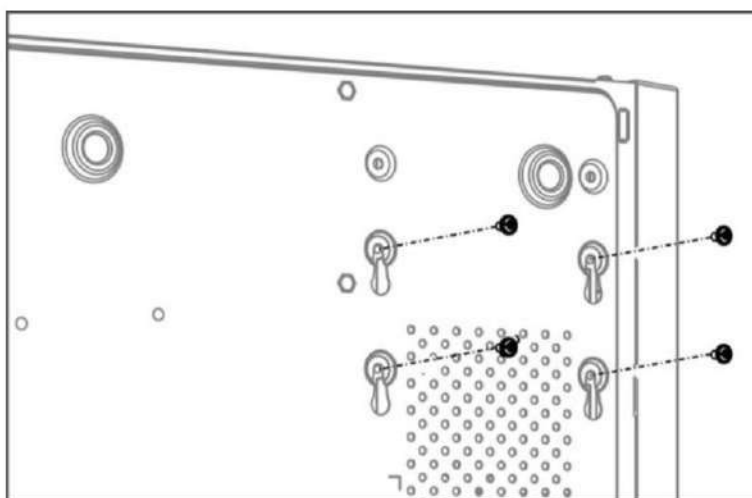


Figura 1-12 Fije el HDD a la parte inferior del dispositivo

4. Opcional: repita los pasos anteriores para instalar otros discos duros.
5. Vuelva a instalar la cubierta del dispositivo y apriete los tornillos.

## Reemplazo de batería de tipo moneda/botón

La batería de botón o moneda debe reemplazarse cuando el dispositivo haya estado apagado o no se haya colocado en su lugar durante un período prolongado y la hora del sistema sea incorrecta.

Antes de comenzar

Apague su dispositivo.

Pasos

1. Retire la cubierta del chasis del dispositivo.
2. Busque la batería de botón/moneda en la placa base.
3. Coloque el pulgar fuera de la ranura de la batería y, con el dedo índice, empuje suavemente el resorte de contacto positivo hacia afuera. La batería saldrá automáticamente.

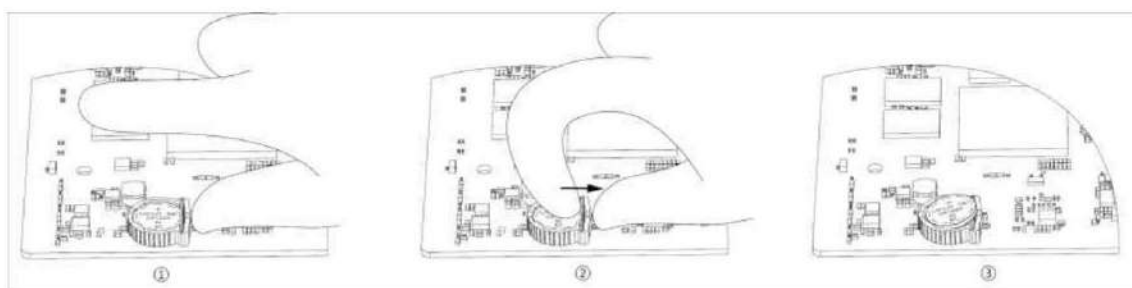


Figura 1-1 Retire la batería



Nota

- Debe usar guantes antiestáticos al retirar la batería.
- Si el resorte se deforma debido a una fuerza excesiva al empujar hacia afuera, es necesario Vuelva a ajustarlo a su posición original antes de insertar la batería.

4. Inserte la batería en diagonal hacia el lado con el punto de encaje de plástico en la ranura de la batería y luego presione la batería cerca del resorte de contacto positivo para encajarla debajo del resorte.

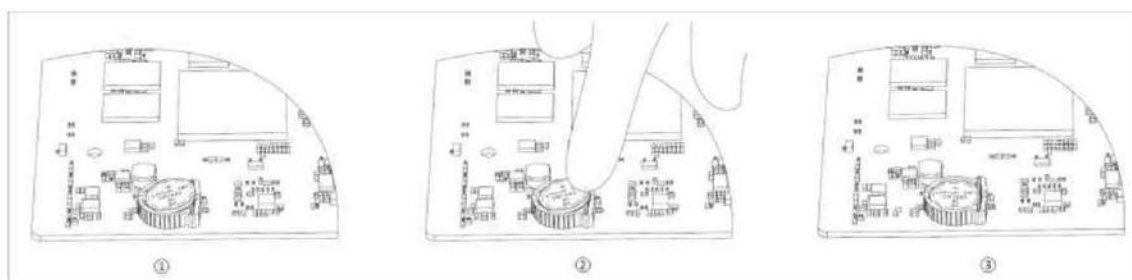


Figura 1-2 Reemplazo de la batería



Nota

Debes usar guantes antiestáticos al reemplazar la batería.

---

5. Vuelva a instalar la cubierta del chasis del dispositivo.

Qué hacer a

continuación Si la hora del sistema es incorrecta, vaya a configurar la hora.

## Contenido

Capítulo 1 Activar a través del menú local .....	1
Capítulo 2 Iniciar sesión en su dispositivo .....	3
Capítulo 3 Interfaz de usuario Introducción .....	4
Capítulo 4 Configuración de red .....	6
4.1 Configuración de parámetros de red .....	6
4.1.1 Configurar TCP/IP .....	6
4.1.2 Configurar DDNS .....	7
4.1.3 Configurar PPPoE .....	8
4.1.4 Configurar multidifusión .....	9
4.2 Configuración de acceso a la plataforma .....	9
4.2.1 Configurar Hik-Connect .....	9
4.2.2 Configurar OTAP .....	11
4.2.3 Configurar ISUP .....	12
4.2.4 Configurar el servicio SDK .....	13
4.2.5 Habilitar ISAPI .....	14
4.2.6 Configurar ONVIF .....	14
4.2.7 Configurar el servidor de registros .....	15
4.3 Configuración del servicio de red .....	16
4.3.1 Configurar HTTP(S) .....	16
4.3.2 Configurar RTSP .....	17
4.3.3 Configurar WebSocket(s) .....	18
4.3.4 Configurar la asignación de puertos (NAT) .....	18
4.3.5 Configurar IoT .....	20
Capítulo 5 Gestión de usuarios .....	21
Capítulo 6 Acceso al dispositivo .....	22
6.1 Acceder al dispositivo de vídeo .....	22

6.1.1 Agregar cámara de red en línea buscada automáticamente .....	22
6.1.2 Agregar cámara de red manualmente .....	23
6.1.3 Agregar cámara de red a través de PoE .....	24
6.1.4 Agregar cámara con energía solar a través del protocolo OTAP .....	24
6.1.5 Agregar cámara de red mediante protocolo personalizado .....	25
6.1.6 Agregar cámara de red a través del archivo de configuración de la cámara .....	26
6.2 Agregar dispositivo de control de acceso .....	26
6.3 Agregar panel de control de seguridad .....	27
6.4 Agregar dispositivo de audio .....	27
6.5 Agregar dispositivo POS .....	27
6.6 Gestión de canales .....	29
Capítulo 7 Agrupación de dispositivos .....	30
Capítulo 8 Configuración del dispositivo de video o audio .....	31
8.1 Habilitar el acceso a la transmisión H.265 .....	31
8.2 Configurar los ajustes de pantalla .....	31
8.3 Configurar parámetros de vídeo .....	32
8.4 Configurar máscara de privacidad .....	32
8.5 Configurar la protección de la privacidad .....	33
8.6 Configurar parámetros de audio .....	35
8.7 Configurar el servicio OTAP .....	35
8.8 Configuración de lotes .....	36
8.9 Configurar la interfaz PoE (Alimentación a través de Ethernet) .....	37
Capítulo 9 Gestión del almacenamiento .....	38
9.1 Administrar el disco duro .....	38
9.2 Configuración RAID .....	38
9.2.1 Crear una matriz de discos .....	39
9.2.2 Reconstruir matriz .....	41
9.2.3 Eliminar matriz .....	41



9.2.4 Ver información del firmware .....	41
9.3 Configurar el modo de almacenamiento .....	42
9.4 Configurar otros parámetros de almacenamiento .....	42
9.5 Administrar unidad flash USB .....	43
Capítulo 10 Configuración de programación .....	44
10.1 Configurar plantilla de programación .....	44
10.2 Configurar la programación de grabación .....	46
10.3 Configurar la programación de captura de imágenes .....	48
10.4 Configurar la grabación de audio .....	50
Capítulo 11 Vista en vivo .....	51
11.1 Configurar el diseño de la vista en vivo .....	51
11.2 Introducción a la GUI .....	51
11.3 Control PTZ .....	53
Capítulo 12 Reproducción .....	54
12.1 Introducción a la GUI .....	54
12.2 Reproducción normal .....	55
12.3 Reproducción de eventos .....	56
12.4 Reproducción de cortes .....	57
12.5 Reproducción de subperíodos .....	57
Capítulo 13 Centro de eventos .....	59
13.1 Configuración de eventos .....	59
13.1.1 Evento básico/genérico .....	59
13.1.2 Protección perimetral .....	61
13.1.3 Evento de comportamiento anormal .....	72
13.1.4 Evento objetivo .....	75
13.1.5 Detección de cámara térmica .....	77
13.1.6 Evento de entrada de alarma .....	78
13.1.7 Evento de análisis de audio .....	80

13.2 Configuración de vinculación .....	82
13.3 Configuración de desarmado .....	84
13.4 Configuración de lotes .....	85
13.5 Búsqueda de eventos .....	86
13.6 Ver alarmas .....	87
Capítulo 14 Búsqueda y copia de seguridad .....	88
Capítulo 15 AcuSeek .....	90
Capítulo 16 AcuSearch .....	93
Capítulo 17 Configuraciones inteligentes .....	95
17.1 Gestión de algoritmos .....	95
17.2 Estado del motor .....	95
17.3 Gestión del plan de tareas .....	95
17.4 Gestión de bibliotecas de listas .....	96
17.4.1 Agregar una biblioteca de listas .....	96
17.4.2 Subir imágenes de rostros a la biblioteca .....	96
17.5 Configuraciones de autoaprendizaje .....	97
17.5.1 Gestión de tareas de autoaprendizaje .....	97
17.5.2 Gestión de modelos .....	98
17.5.3 Estado inteligente .....	98
Capítulo 18 Centro de aplicaciones .....	99
18.1 Detección de personas y vehículos .....	99
18.2 Registro de personas .....	99
18.2.1 Agregar tarea de check-in .....	100
18.2.2 Búsqueda de registros de check-in .....	101
18.3 Informe estadístico .....	101
Capítulo 19 Configuración de parámetros del sistema .....	103
Capítulo 20 Copia de seguridad del dispositivo de repuesto activo .....	105
20.1 Establecer el dispositivo de trabajo .....	105

20.2 Establecer dispositivo de repuesto dinámico .....	105
Capítulo 21 Configurar evento de excepción .....	107
Capítulo 22 Ver información del sistema .....	109
Capítulo 23 Mantenimiento del sistema .....	110
23.1 Reinicio programado .....	110
23.2 Dispositivo de actualización .....	110
23.3 Copia de seguridad y restauración .....	110
23.4 Información de registro .....	111
23.5 Configurar el servidor de registros .....	111
23.6 Herramientas de mantenimiento .....	111
23.7 Configuración de apagado suave .....	112
Capítulo 24 Gestión de la seguridad .....	114
24.1 Filtro de direcciones .....	114
24.2 Cifrado de transmisión .....	114
24.3 Seleccionar la versión de TLS .....	114
Capítulo 25 Apéndice .....	115
25.1 Lista de adaptadores de corriente aplicables .....	115
25.2 Glosario .....	116
25.3 Preguntas frecuentes .....	117
25.3.1 ¿Por qué hay una parte de los canales que muestra “Sin recursos” o se vuelve negra la pantalla? ¿Vista en vivo multipantalla? .....	117
25.3.2 ¿Por qué la grabadora de video notifica una contraseña riesgosa después de agregar una cámara de red? .....	118
25.3.3 ¿Por qué la grabadora de video notifica que el tipo de transmisión no es compatible? .....	118
25.3.4 ¿Cómo confirmar que la grabadora de video está usando H.265 para grabar video? .....	118
25.3.5 ¿Por qué el grabador de video notifica un conflicto de IP? .....	118
25.3.6 ¿Por qué la imagen se bloquea al reproducirla con cámaras de un solo canal o de varios canales? .....	119
25.3.7 ¿Por qué el dispositivo no puede controlar la cámara PTZ a través de coaxitron? .....	119

25.3.8 ¿Por qué el PTZ parece no responder a través de RS-485? .....	119
25.3.9 ¿Por qué la calidad del sonido del vídeo no es buena? .....	119
25.4 Notificación de gas corrosivo .....	120

## Capítulo 1 Activar a través del menú local

Para acceder por primera vez, debe establecer una contraseña de administrador para activar el dispositivo. No se permite realizar ninguna operación antes de la activación. También puede activar el dispositivo mediante un navegador web, SADP o un software cliente.

Antes de comenzar

Asegúrese de que su dispositivo esté conectado a un monitor y un mouse.

Pasos

1. Encienda su dispositivo.
2. Configure la región o los parámetros DST (horario de verano).
3. Seleccione un idioma del sistema.
4. Ingrese la contraseña de administrador dos veces.



Precaución

Le recomendamos encarecidamente que cree una contraseña segura de su elección (utilizando un mínimo de 8 caracteres, incluidos al menos tres tipos de las siguientes categorías: letras mayúsculas, letras minúsculas, números y caracteres especiales) para aumentar la seguridad de su producto.

Y le recomendamos que cambie su contraseña periódicamente, especialmente en el sistema de alta seguridad, cambiar la contraseña mensualmente o semanalmente puede proteger mejor su producto.

---

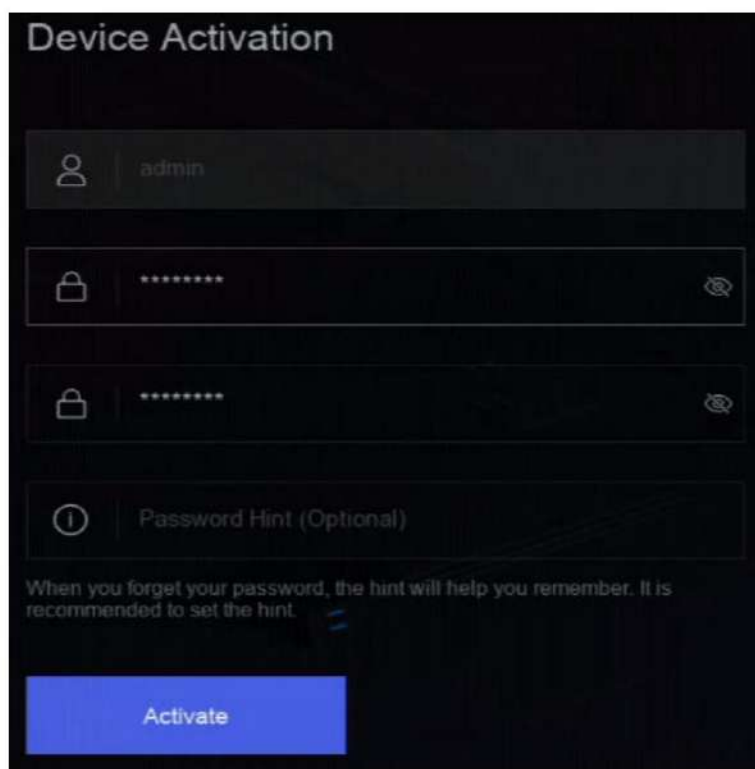


Figura 1-1 Activar a través del menú local

5. Opcional: Introduce una pista de contraseña. Te ayudará a recordarla si la olvidas.

6. Haga clic en Activar.



Nota

Una vez activado el dispositivo, deberás conservar correctamente la contraseña.

---

7. Opcional: Dibuja un patrón de desbloqueo.

8. Configure al menos un método de recuperación de contraseña.

Qué hacer a

continuación Siga el asistente para configurar los parámetros básicos.

## Capítulo 2 Inicie sesión en su dispositivo

Debe iniciar sesión en su dispositivo antes de operar el menú y otras funciones.

Antes de comenzar

Asegúrese de que su dispositivo esté activado.

Pasos

1. Encienda su dispositivo.
2. Haga clic derecho para mostrar el menú de acceso directo.
3. Seleccione un elemento según sea necesario. Por ejemplo, seleccione Salir de pantalla completa y automáticamente...  
Ingrese a la interfaz de inicio de sesión.

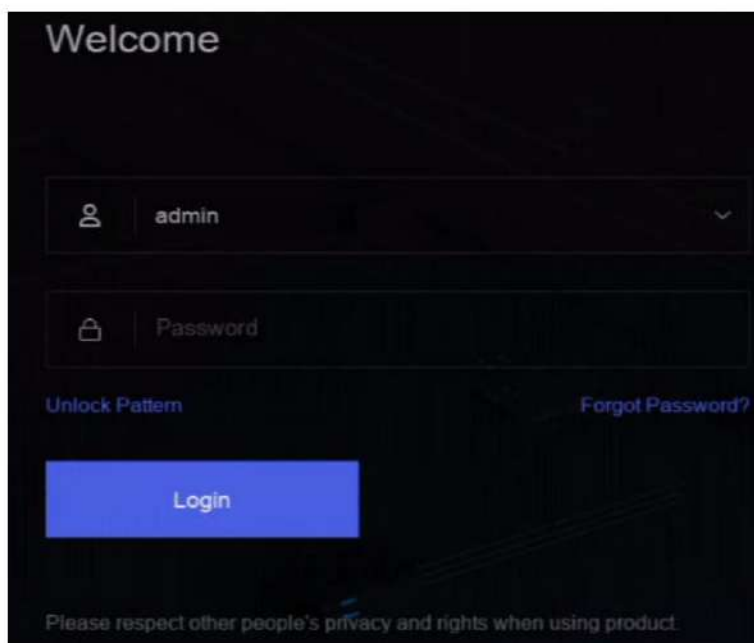


Figura 2-1 Inicio de sesión

4. Utilice el patrón de desbloqueo para iniciar sesión o haga clic en Iniciar sesión con contraseña para iniciar sesión con nombre de usuario y contraseña.



Nota

- El patrón de desbloqueo solo está disponible para el usuario administrador.
- Si olvida su patrón de desbloqueo o contraseña de inicio de sesión, haga clic en Olvidar contraseña en la contraseña.

Interfaz de inicio de sesión para restablecer su contraseña o utilice la pista de contraseña para recordarla.

---

## Capítulo 3 Interfaz de usuario Introducción

El dispositivo accederá a la interfaz de visualización en vivo después de encenderlo. Haga clic derecho y seleccione " Salir de pantalla completa" en el menú contextual.



Figura 3-1 Página de funciones principales

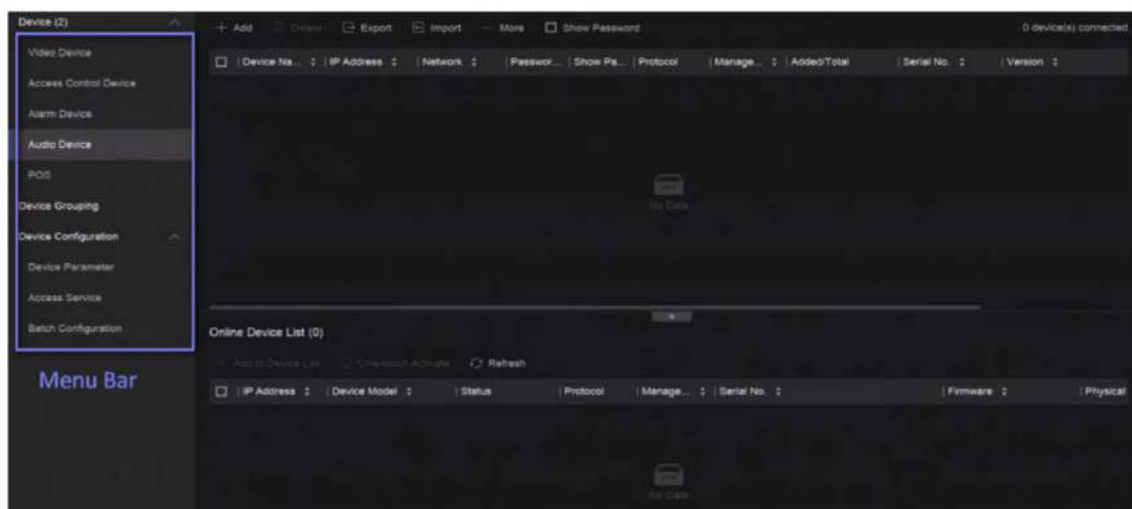








Figura 3-2 Ejemplo de barra de menú





Figura 3-3 Ejemplo de detección de personas y vehículos del centro de aplicaciones

Tabla 3-1 Introducción a la interfaz

Nombre de la interfaz	Introducción
Barra de tareas	<p>Las aplicaciones abiertas se listan en la barra de tareas. Puedes moverlas y cerrarlas. cada pestaña de la aplicación.</p> <p>Introducción del icono:</p> <ul style="list-style-type: none"><li>•  :Menú principal.</li><li>•  Centro de eventos. Se pueden buscar y visualizar las alarmas de eventos.</li><li>•  :El progreso de descarga de cada tarea de descarga se puede ver aquí.</li><li>•  :Apague, cierre sesión o reinicie su dispositivo.</li></ul>
Lista de aplicaciones	Aquí se muestran todas las aplicaciones. Puedes hacer clic en una para configurarla.
Barra de navegación	Haga clic para configurar cada función del sistema.
Barra de menú	<p>Aquí se enumeran los elementos configurables de cada aplicación.</p> <p> Nota</p> <p>Para las aplicaciones en el Centro de aplicaciones, puede hacer clic en  , o haga clic derecho para mostrar la barra de menú.</p>

## Capítulo 4 Configuración de red

Los parámetros de red, las configuraciones de acceso a la plataforma y los servicios de red son configurables.

### 4.1 Configuración de parámetros de red

Debe configurar los parámetros de red antes de utilizar funciones que requieran acceso a la red.

#### 4.1.1 Configurar TCP/IP

El protocolo TCP/IP debe estar configurado correctamente antes de operar la grabadora de video a través de la red o acceder a dispositivos de red.

Pasos

1. Vaya a Sistema → Configuración del sistema → Red → Red → TCP/IP .

The screenshot shows a web-based configuration interface for TCP/IP settings. It includes sections for 'Working Mode' with options for NIC selection, type, and DHCP status, and 'DNS Server Settings' with options for auto-obtaining DNS servers and specifying preferred/alternate servers. A 'Main NIC' dropdown is also present. A 'Save' button is at the bottom.

Figura 4-1 Configuración de TCP/

IP 2. Configure el modo de trabajo y seleccione NIC.

Multidirección

Los parámetros de las dos tarjetas NIC se pueden configurar de forma independiente. Puede seleccionar LAN1 o LAN2 en el campo "Tipo de NIC". Puede seleccionar una tarjeta NIC como ruta predeterminada. El sistema se conectará a la extranet y los datos se reenviarán a través de la ruta predeterminada.

Tolerancia a fallos de red

Las dos tarjetas NIC usan la misma dirección IP, y puede configurar la NIC principal como LAN1 o LAN2. De esta forma, si falla una tarjeta NIC, el grabador de video habilitará automáticamente la otra tarjeta NIC de reserva para garantizar el correcto funcionamiento del sistema.



Nota

El modo de trabajo solo está disponible para ciertos modelos.

---

### 3. Configurar los parámetros de red.

#### - IPv4

##### DHCP

Si el servidor DHCP está disponible, puede habilitar DHCP para obtener automáticamente una dirección IP y otras configuraciones de red de ese servidor.

Unidad de transmisión máxima (MTU)

La unidad de transmisión máxima (MTU) es el tamaño de la unidad de datos del protocolo de capa de red más grande que se puede comunicar en una sola transacción de red.

Obtener automáticamente el servidor DNS

Si DHCP está habilitado, puede marcar la opción Obtener servidor DNS automáticamente para obtener el servidor DNS preferido y el servidor DNS alternativo.

#### - IPv6

##### Anuncio de enrutador

Si el enrutador de la red admite IPv6, se recomienda utilizar este modo como predeterminado.

##### Auto

Si hay un dispositivo DHCPv6 en la red, se recomienda utilizar este modo

##### Configuración manual Debe

utilizar este modo si va a ingresar manualmente los parámetros IPv6.

### 4. Haga clic en Guardar.

## 4.1.2 Configurar DDNS

El servidor de nombres de dominio dinámico (DDNS) asigna direcciones IP de usuarios dinámicos a un nombre de dominio fijo servidor.

#### Antes de comenzar

Asegúrese de haber registrado los servicios DynDNS, PeanutHull y NO-IP con su ISP.

#### Pasos

1. Vaya a Sistema → Configuración del sistema → Red → Red → DDNS .

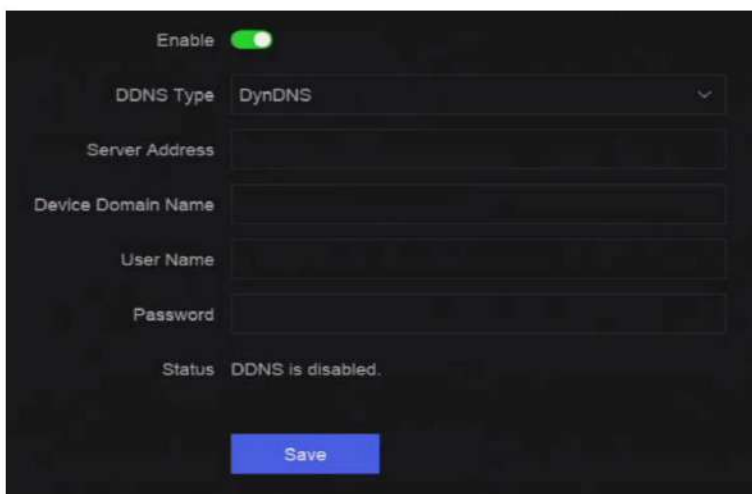


Figura 4-2 DDNS

2. Activar Habilitar.
3. Seleccione un tipo de DDNS.
4. Establezca parámetros, incluida la dirección del servicio, el nombre de dominio, etc.
5. Haga clic en Guardar.

### 4.1.3 Configurar PPPoE

Si el dispositivo está conectado a Internet mediante PPPoE, deberá configurar el nombre de usuario y la contraseña correspondientes. Para obtener más información sobre el servicio PPPoE, póngase en contacto con su proveedor de servicios de Internet.

Pasos

1. Vaya a Sistema → Configuración del sistema → Red → Red → PPPoE .

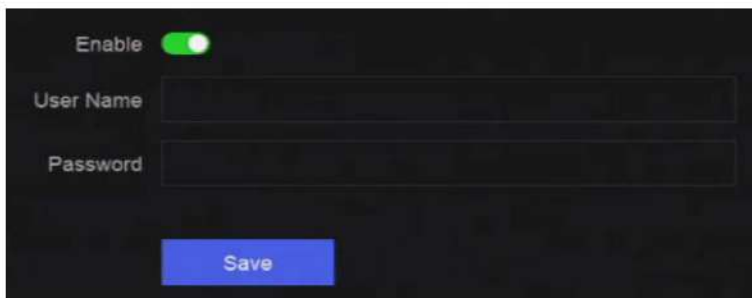


Figura 4-3 PPPoE

2. Activar Habilitar.
3. Ingrese el nombre de usuario y la contraseña.
4. Haga clic en Guardar.

Qué hacer a continuación

Vaya a Sistema → Mantenimiento del sistema → Información de ejecución → Estado de la red para ver el estado de PPPoE.

#### 4.1.4 Configurar multidifusión

Se puede configurar la multidifusión para habilitar la visualización en vivo para cámaras que excedan el número máximo permitido a través de la red.

Pasos

1. Vaya a Sistema → Configuración del sistema → Red → Red → Otro .
2. Establecer parámetros de multidifusión .



Nota

- Al agregar un dispositivo a través de un cliente de seguridad de video en red, la dirección IP del grupo de multidifusión debe ser la misma que la dirección IP de multidifusión del dispositivo.
- Para IPv4, cubre IP de clase D que van desde 224.0.0.0 a 239.255.255.255 y es  
Se recomienda usar una dirección IP entre 239.252.0.0 y 239.255.255.255. Al agregar un dispositivo al software CMS, la dirección de multidifusión debe ser la misma que la del dispositivo.

- 
3. Haga clic en Guardar.

#### 4.2 Configuración de acceso a la plataforma

##### 4.2.1 Configurar Hik-Connect

Hik-Connect ofrece una aplicación de teléfono móvil y un servicio de plataforma para acceder y administrar su grabadora de video, lo que le permite obtener un acceso remoto conveniente al sistema de seguridad de video.

Pasos

1. Vaya a Sistema → Configuración del sistema → Red → Hik-Connect.

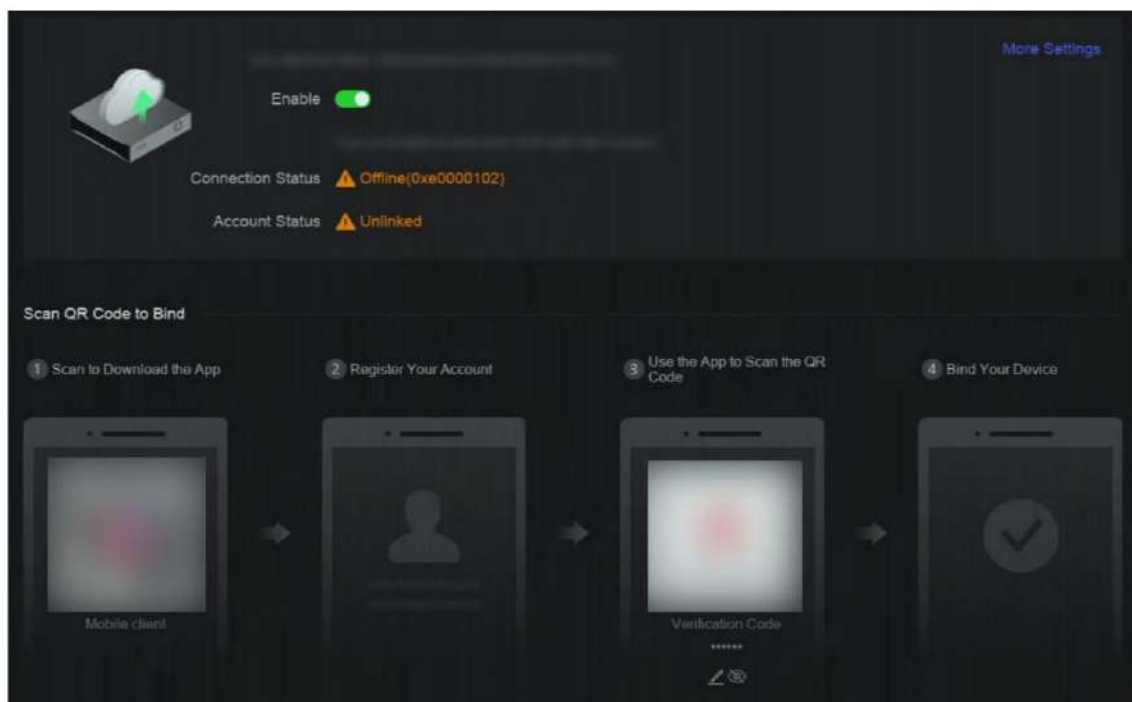


Figura 4-4 Hik-Connect

2. Active Habilitar y aparecerán los términos del servicio.
3. Acepte los términos del servicio.
4. Descargue la aplicación Hik-Connect.
  - Utilice un teléfono inteligente para escanear el código QR y descargue la aplicación Hik-Connect.
  - Descargue la aplicación desde <https://appstore.hikvision.com>.



Figura 4-5 Descargar Hik-Connect 5. Registre

- una cuenta en la aplicación.
6. Opcional: haga clic en Más configuraciones para habilitar el cifrado de transmisión, la sincronización de tiempo de plataforma y la transmisión de tasa de bits adaptable, o editar la dirección IP del servidor.
- Cifrado de transmisión

Es necesario ingresar un código de verificación en el acceso remoto y la vista en vivo después de habilitar esta función.

Sincronización de hora de

la plataforma El dispositivo sincronizará la hora con Hik-Connect en lugar del servidor NTP.

Transmisión de tasa de bits adaptativa

Cuando el entorno de red es deficiente, el dispositivo ajustará automáticamente la tasa de bits del video para garantizar la fluidez de reproducción.

Dirección IP del servidor

La dirección IP del servidor Hik-Connect.

7. Haga clic  para establecer el código de verificación.

8. Utilice la aplicación Hik-Connect para escanear el código QR del dispositivo y vincularlo con su cuenta Hik-Connect.



Nota

Si el dispositivo ya está vinculado a una cuenta, puede hacer clic en Desenlazar para desvincularlo de la cuenta actual.

---

Resultado

• Si su dispositivo está conectado con Hik-Connect, el estado de la conexión será En línea. • Si su dispositivo está vinculado con una cuenta Hik-Connect, el estado de la cuenta será Vinculado.

Qué hacer a

continuación Puede acceder a su grabadora de vídeo a través de Hik-Connect.

### 4.2.2 Configurar OTAP

OTAP (Protocolo de Acceso a Objetos Abiertos) es un estándar integrado unificado y un modo push-pull del protocolo de Hikvision en redes públicas y privadas. Una vez habilitado OTAP, otras aplicaciones podrán visualizar videos de forma remota a través de este protocolo.

Antes de comenzar

Asegúrese de que la red de su dispositivo sea accesible a través de OTAP.

Pasos

1. Vaya a Sistema → Configuración del sistema → Red → Acceso a la plataforma → OTAP .

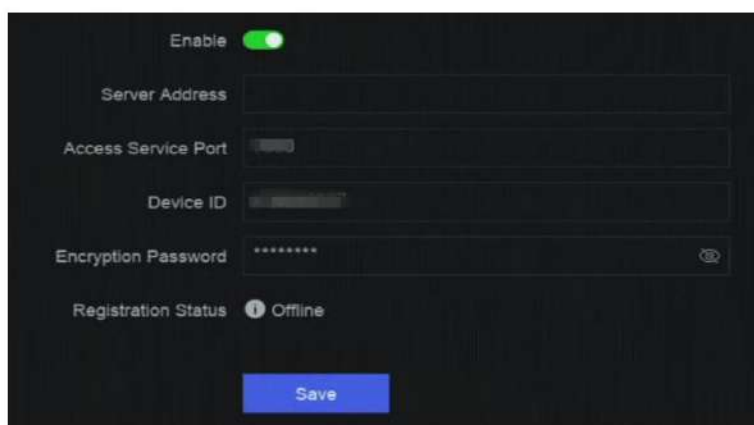


Figura 4-6 OTAP

2. Activa OTAP.
3. Establezca los parámetros.
4. Haga clic en Guardar.

### 4.2.3 Configurar ISUP

ISUP (Protocolo de enlace ascendente de seguridad inteligente) proporciona API, archivos de biblioteca y comandos para que la plataforma de terceros acceda a dispositivos como NVR, domos de velocidad, DVR, cámaras de red, NVR móviles, dispositivos móviles, dispositivos de decodificación, etc. Con este protocolo, la plataforma de terceros puede realizar funciones como visualización en vivo, reproducción, audio bidireccional, control PTZ, etc.

#### Pasos

1. Vaya a Sistema → CX → Configuración del sistema → Red → Acceso a la plataforma → ISUP .

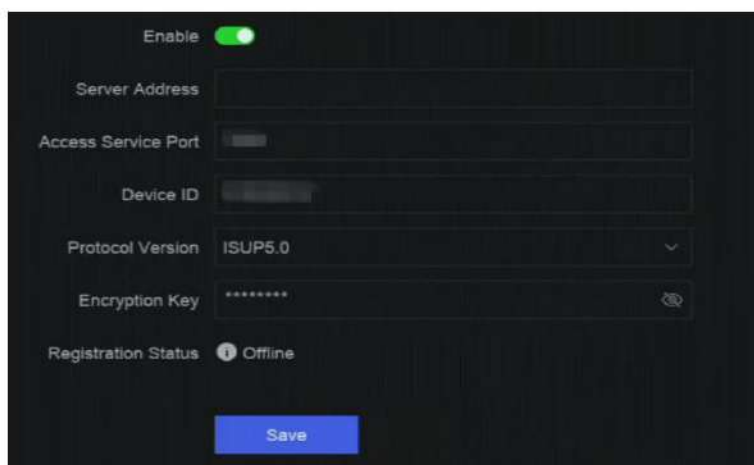


Figura 4-7 ISUP

2. Activar Habilitar.





### Nota

Si ISUP está habilitado, el acceso a Hik-Connect se deshabilitará automáticamente.

---

### 3. Establezca los parámetros relacionados.

#### Dirección del servidor

La dirección IP del servidor de la plataforma.

#### Puerto del servidor de acceso

El puerto del servidor de la plataforma varía de 1024 a 65535. El puerto real lo proporcionará la plataforma.

#### ID del dispositivo

La identificación del dispositivo será proporcionada por la plataforma.

#### Versión del protocolo

Versión del protocolo ISUP, solo está disponible ISUP 5.0.

#### Clave de cifrado

Se requiere una contraseña de cifrado al usar la versión ISUP V5.0. Esta proporciona una comunicación más segura entre el dispositivo y la plataforma. Introdúzcala para la verificación después de registrar el dispositivo en la plataforma ISUP. No puede estar vacía ni contener "ABCDEF".

### 4. Haga clic en Guardar.

Puede ver el estado del registro (en línea o fuera de línea) después de reiniciar el dispositivo.

## 4.2.4 Configurar el servicio SDK

El servicio SDK (Kit de Desarrollo de Software) se utiliza para que socios externos integren diferentes funciones. El servicio SDK mejorado adopta el protocolo TLS, lo que proporciona una transmisión de datos más segura.

#### Pasos

1. Vaya a Sistema → Configuración del sistema → Red → Acceso a la plataforma → SDK.

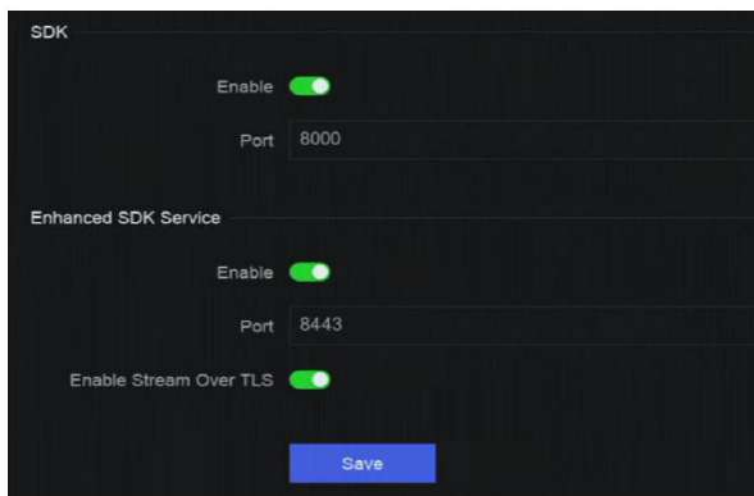


Figura 4-8 Servicio SDK

2. Configure el SDK y el servicio SDK mejorado según sus necesidades.



Nota

El puerto para el servicio SDK mejorado es 8443 de forma predeterminada.

---

3. Opcional: Habilite la transmisión por TLS. La tecnología de cifrado de transmisión por TLS proporciona más servicio de transmisión de flujo seguro.
4. Haga clic en Guardar.

## 4.2.5 Habilitar ISAPI

ISAPI (Interfaz de programación de aplicaciones de servidor de Internet) es un protocolo abierto basado en HTTP, que puede realizar la comunicación entre los dispositivos del sistema (por ejemplo, cámara de red, NVR, etc.).

Vaya a Sistema → Configuración del sistema → Red → Acceso a la plataforma → ISAPI para habilitar la función.

## 4.2.6 Configurar ONVIF

El protocolo ONVIF permite la conexión con cámaras de terceros. Las cuentas de usuario añadidas tienen permiso para conectar otros dispositivos mediante el protocolo ONVIF.

Pasos

1. Vaya a Sistema → CX → Configuración del sistema → Red → Acceso a la plataforma → ONVIF .

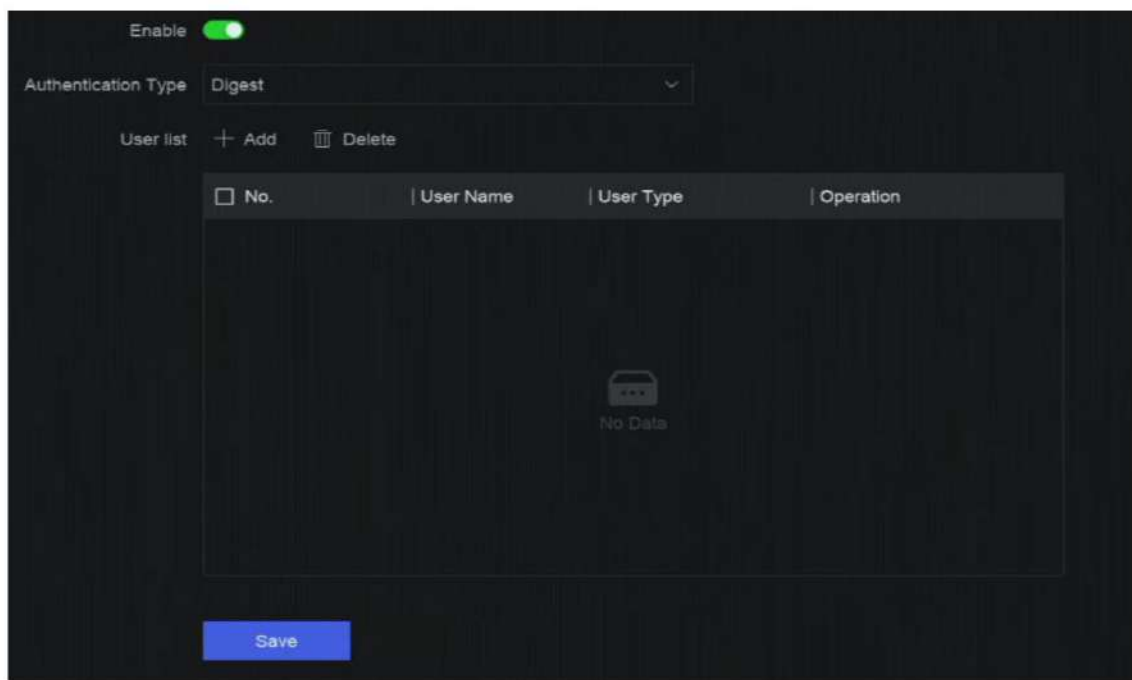


Figura 4-9 ONVIF

2. Activar Habilitar.
3. Seleccione un tipo de autenticación.
4. Haga clic en Agregar para agregar un usuario.
5. Establezca el nombre de usuario y la contraseña.



#### Precaución

Le recomendamos encarecidamente que cree una contraseña segura de su elección (con un mínimo de 8 caracteres, incluyendo al menos tres de las siguientes categorías: mayúsculas, minúsculas, números y caracteres especiales) para aumentar la seguridad de su producto. Le recomendamos que restablezca su contraseña periódicamente, especialmente en el sistema de alta seguridad. Restablecerla mensual o semanalmente protege mejor su producto. 6. Haga clic en Guardar.

---

#### 4.2.7 Configurar el servidor de registro

Los registros se pueden cargar al servidor de registros para realizar copias de seguridad.

##### Pasos

1. Vaya a Sistema → Configuración del sistema → Red → Acceso a la plataforma → Servidor de registros.

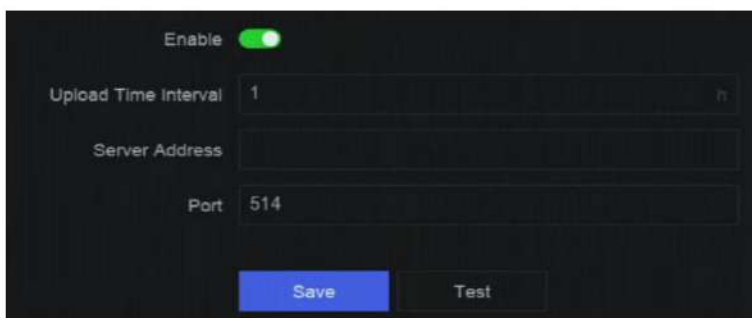


Figura 4-10 Servidor de registro

2. Activar Habilitar.
3. Configure el intervalo de tiempo de carga, la dirección IP del servidor y el puerto.
4. Opcional: haga clic en Probar para comprobar si los parámetros son válidos.
5. Haga clic en Guardar.

## 4.3 Configuración del servicio de red

### 4.3.1 Configurar HTTP(S)

Los puertos HTTP (Protocolo de transferencia de hipertexto) y HTTPS (Protocolo seguro de transferencia de hipertexto) se utilizan para el acceso remoto a través del navegador web. El protocolo HTTPS permite la transmisión cifrada y la autenticación de identidad, lo que mejora la seguridad del acceso remoto.

#### Pasos

1. Vaya a Sistema → Configuración del sistema → Red → Servicio de red → HTTP(S).

HTTP

Enable ☒

\* Port 80

HTTPS

Enable ☒

Ensure the client TLS version is enabled. [TLS Settings](#)

\* Port 443

Enable HTTPS Browsing ☐

HTTP/HTTPS Authentication

Authentication Type Digest

Digest Algorithm MD5

Authentication type and digest algorithm are valid for both HTTP and HTTPS.

Save

Figura 4-11 HTTP(S)

2. Opcional: activa HTTP o HTTPS.
3. Ver o editar el puerto HTTP o HTTPS.
4. Configure la autenticación HTTP/HTTPS.

#### Tipo de autenticación

Se pueden seleccionar dos tipos de autenticación, por razones de seguridad, se recomienda seleccionar Digest como tipo de autenticación.

#### Algoritmo de resumen

Los algoritmos de resumen se basan en HTTP/HTTPS y se utilizan principalmente para la autenticación de resumen de la autenticación de usuarios.

5. Haga clic en Guardar.

### 4.3.2 Configurar RTSP

RTSP (Protocolo de Transmisión en Tiempo Real) es un protocolo de control de red diseñado para controlar servidores de transmisión multimedia. Puede proteger específicamente los datos de transmisión de la visualización en vivo configurando la autenticación RTSP.

#### Pasos

1. Vaya a Sistema → Configuración del sistema → Red → Servicio de red → RTSP .



Figura 4-12 RTSP

2. Establecer parámetros.

Puerto

El puerto es 554 por defecto.

Tipo de autenticación

Se pueden seleccionar dos tipos de autenticación. Si selecciona Digest, solo la solicitud con autenticación Digest podrá acceder a la transmisión de vídeo por RTSP a través de la dirección IP. Por seguridad, se recomienda seleccionar Digest como tipo de autenticación.

Algoritmo de resumen RTSP

El algoritmo de resumen RTSP se basa en RTSP, es un algoritmo para la autenticación de resumen de la autenticación del usuario.

3. Haga clic en Guardar.

### 4.3.3 Configurar WebSocket(s)

El protocolo WebSocket, basado en TCP, proporciona comunicación full-duplex entre navegadores web y servidores. Permite iniciar una sesión de comunicación interactiva bidireccional.

Pasos

1. Vaya a Sistema → Configuración del sistema → Red → Servicio de red → WebSocket(s) .
2. Activar Habilitar.
3. Establecer puerto.
4. Haga clic en Guardar.

### 4.3.4 Configurar la asignación de puertos (NAT)

Se ofrecen dos métodos para el mapeo de puertos y el acceso remoto a través de la red multisegmento: UPnP™ (Universal Plug and Play) y mapeo manual. UPnP™ permite que el dispositivo detecte sin problemas la presencia de otros dispositivos en la red y establezca servicios de red funcionales para compartir datos, comunicaciones, etc. Puede usar la función UPnP™ para permitir la conexión rápida del dispositivo a la WAN a través de un enrutador sin mapeo de puertos.

Antes de comenzar:

Si desea habilitar la función UPnP™ del dispositivo, debe habilitarla en el enrutador al que está conectado. Si el modo de red del dispositivo está configurado como multidireccional, su ruta predeterminada debe estar en el mismo segmento de red que la dirección IP LAN del enrutador.

Pasos

1. Vaya a Sistema → Configuración del sistema → Red → Servicio de red → NAT

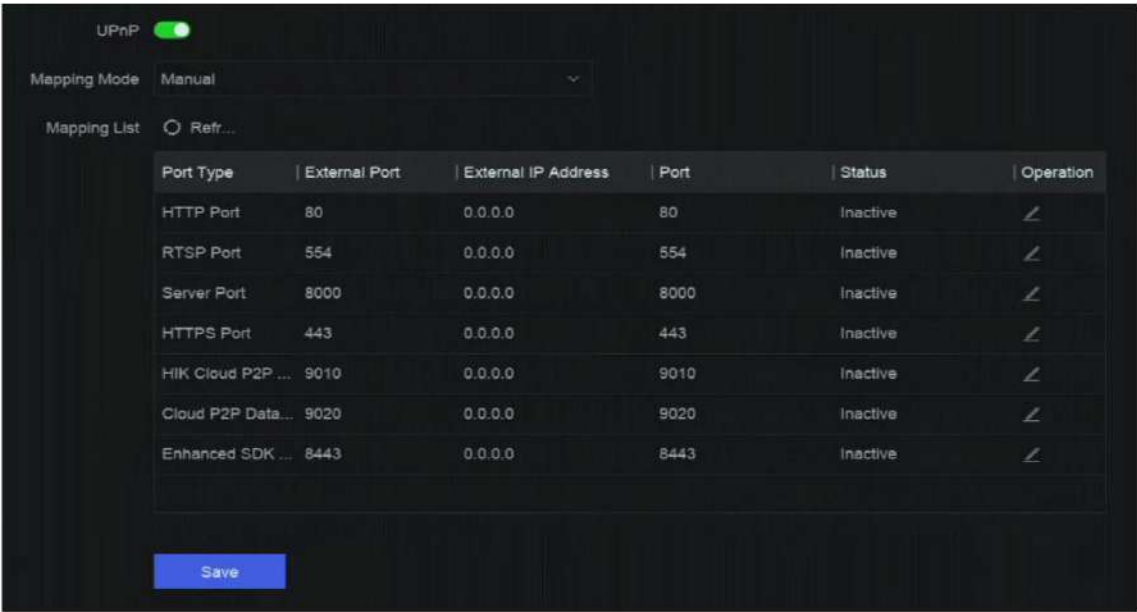


Figura 4-13 Mapeo de puertos (NAT)

2. Activar Habilitar.


3. Establecer el modo de mapeo.

Auto

Los elementos de mapeo de puertos son de solo lectura y los puertos externos son configurados automáticamente por el enrutador.

Manual

Puede editar manualmente el puerto externo.

4. Si el modo de mapeo está seleccionado como Manual, haga clic  para editar los puertos correspondientes.



- Nota
- El valor del número de puerto RTSP debe ser 554 o entre 1024 y 65535, mientras que el  
El valor de los demás puertos debe estar entre 1 y 65535 y ser diferente. Si se configuran varios dispositivos UPnP™ en el mismo enrutador, el número de puerto de cada dispositivo debe ser único. • Puerto externo indica el número de puerto interno para la asignación de puertos en el enrutador.

5. Haga clic en Guardar.

Qué hacer a

continuación Ingrese a la página de configuración del servidor virtual del enrutador, luego complete el espacio en blanco del puerto de origen interno/externo con el valor del puerto interno/externo y otros contenidos requeridos.

### 4.3.5 Configurar IoT

Puede configurar el puerto de red a través del cual el NVR recibirá alarmas de un panel de control de seguridad.

Vaya a Sistema → Configuración del sistema → Red → Servicio de red → IoT para habilitar la función y configurar el número de puerto.



Nota

El número de puerto que configure aquí debe ser el mismo que el puerto de envío de alarma en el panel de control de seguridad.

---



## Capítulo 5 Gestión de usuarios



Hay una cuenta predeterminada para el administrador. El nombre de usuario del administrador es admin. El administrador tiene permiso para agregar, eliminar y editar usuarios. Los usuarios invitados y operadores solo tienen permisos limitados.

Vaya a Sistema → Configuración del sistema → Administración de usuarios .



Figura 5-1 Gestión de usuarios

Tabla 5-1 Descripción de iconos/botones

Icono/Botón	Descripción
	Establecer la seguridad de la cuenta.
Agregar	Agregar un nuevo usuario invitado u operador.
	Eliminar el usuario seleccionado.



Nota

Antes de realizar la operación, debe confirmar la contraseña de administrador.

## Capítulo 6 Acceso al dispositivo

La grabadora de video puede acceder a varios tipos de dispositivos, como cámaras de red, dispositivos de control de acceso y dispositivos de alarma. Consulte el dispositivo para conocer la capacidad de acceso de su grabadora de video.

### 6.1 Acceder al dispositivo de vídeo

Hay varias formas de acceder a un dispositivo de vídeo.

#### 6.1.1 Agregar cámara de red en línea buscada automáticamente

Es posible buscar y agregar automáticamente cámaras de red en el mismo segmento de red al dispositivo.

Pasos

1. Vaya a Sistema → Acceso al dispositivo → Dispositivo → Dispositivo de video → Lista de dispositivos en línea .
2. Seleccione el/los dispositivo(s) de la lista.

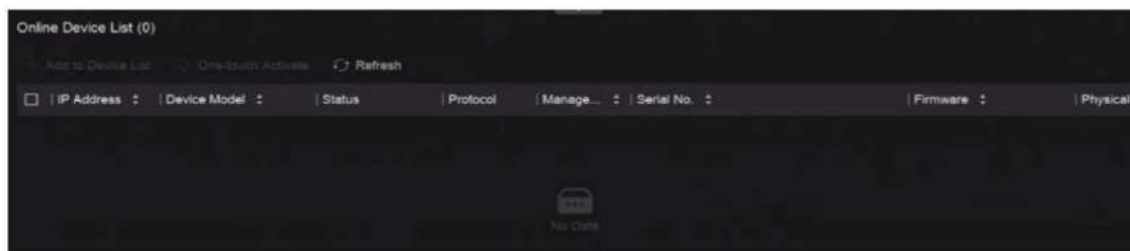


Figura 6-1 Agregar cámara de red en línea buscada automáticamente

3. Haga clic en Agregar a la lista de dispositivos.



Nota

El dispositivo usará una contraseña predeterminada para agregar cámaras de red. Asegúrese de que la contraseña de la cámara coincida con la predeterminada. Esta contraseña se puede configurar en Más → Configuración de contraseña predeterminada. Si las cámaras de red buscadas no están activadas, el dispositivo usará una contraseña predeterminada para activar y agregar las cámaras de red inactivas. Esta contraseña se puede configurar en Más → Configuración de contraseña predeterminada.

- Cuando se agrega correctamente una cámara de red, su estado será En línea. • Puede hacer clic en el nombre del dispositivo para agregar sus parámetros.

## 6.1.2 Agregar cámara de red manualmente

Agregue manualmente las cámaras de red a su grabadora de video.

Antes de empezar

- Asegúrese de que su cámara de red esté en el mismo segmento de red que su grabadora de video. • Asegúrese de que la conexión de red sea válida y correcta.
- Asegúrese de que la cámara de red esté activada.

Pasos

1. Vaya a Sistema → Acceso al dispositivo → Dispositivo → Dispositivo de video .

The screenshot shows a web interface for adding a network camera. The 'Add Device' window contains an empty table for online devices. Below the table, there are input fields for IP Address, Device Name, Protocol, Management Port, User Name, Password, and Transfer Protocol. A 'Test' button is next to the IP Address field. A checkbox for 'Use Channel Default Password' is also present.

Figura 6-2 Agregar cámara de red manualmente

2. Haga clic en Agregar.

3. Ingrese los parámetros de la cámara de red.

Usar la contraseña predeterminada del canal

Si está habilitado, la grabadora de video agregará la cámara con la contraseña predeterminada del canal establecido.

Más configuraciones

Puede habilitar la función Verificar certificado para verificar la cámara con un certificado. El certificado es una forma de identificación que proporciona una autenticación más segura. Para usar esta función, primero debe importar el certificado de la cámara de red al dispositivo.

4. Opcional: haga clic en Continuar para agregar para agregar otras cámaras de red.

5. Haga clic en Agregar.

### 6.1.3 Agregar cámara de red a través de PoE

Se puede conectar una cámara de red PoE (Alimentación a través de Ethernet) directamente a su dispositivo a través de la interfaz PoE en el panel trasero.

Después de usar un cable de red para conectar una cámara de red PoE a su dispositivo, deberá configurar la interfaz PoE correspondiente.

Consulte " Configurar la interfaz PoE (Alimentación a través de Ethernet)" para obtener más información.

### 6.1.4 Agregar cámara con energía solar a través del protocolo OTAP

Se pueden agregar cámaras con energía solar a su dispositivo a través del protocolo OTAP.

Antes de comenzar

Asegúrese de que la red entre su dispositivo y la cámara con energía solar sea accesible a través del protocolo OTAP.

Introduzca aquí el contexto de su tarea (opcional).

Pasos

1. Vaya a Sistema → Acceso al dispositivo → Configuración del dispositivo → Servicio de acceso → Servicio OTAP.
2. Activar Habilitar.
3. Configure el puerto del servidor OTAP y la clave de cifrado.
4. Opcional: Habilite la función de agregar cámara IP automáticamente. Una vez configurados los parámetros OTAP del dispositivo, las cámaras de red recién firmadas (mediante el protocolo OTAP) se agregarán automáticamente a su dispositivo.
5. Configure los parámetros del protocolo OTAP de la cámara solar a través del navegador web. Consulte

Consulte el manual del usuario de la cámara para obtener más detalles.



Nota

Los parámetros del protocolo OTAP de la cámara con energía solar deberán ser los mismos que los del dispositivo.

- 
6. Agregue cámaras alimentadas por energía solar a su dispositivo.
    - Si ha habilitado Agregar cámara IP automáticamente, las cámaras de red recién firmadas (a través de OTAP El protocolo se agregará automáticamente a su dispositivo.
    - Seleccione la(s) cámara(s) con energía solar de la Lista de dispositivos en línea y haga clic en Agregar rápidamente.
  7. Haga clic en Agregar en Sistema → Acceso al dispositivo → Dispositivo → Dispositivo de vídeo, seleccione Protocolo como OTAP y

Haga clic en Agregar.

¿Qué hacer a continuación?

- Después de agregar una cámara con energía solar a su dispositivo, puede activarla, ver la carga de su batería, ver su video en vivo, configurar sus parámetros a través del navegador web, etc.
- Configure la función ANR (Reposición automática de red) para la cámara. Consulte [Configurar grabación Cronograma](#).

### 6.1.5 Agregar cámara de red mediante un protocolo personalizado

Para las cámaras de red que no utilizan protocolos estándar, puede configurar protocolos personalizados para añadirlos. El sistema ofrece ocho protocolos personalizados.

Antes de empezar

- Asegúrese de que la cámara de red admita la transmisión RTSP.
- Prepare la URL (Localizador uniforme de recursos) para obtener la transmisión principal o secundaria de cámaras de red.

Pasos

1. Vaya a Sistema → Acceso al dispositivo → Dispositivo → Dispositivo de video.
2. Haga clic en Más → Administración de protocolos personalizados o en Agregar → Administración de protocolos.

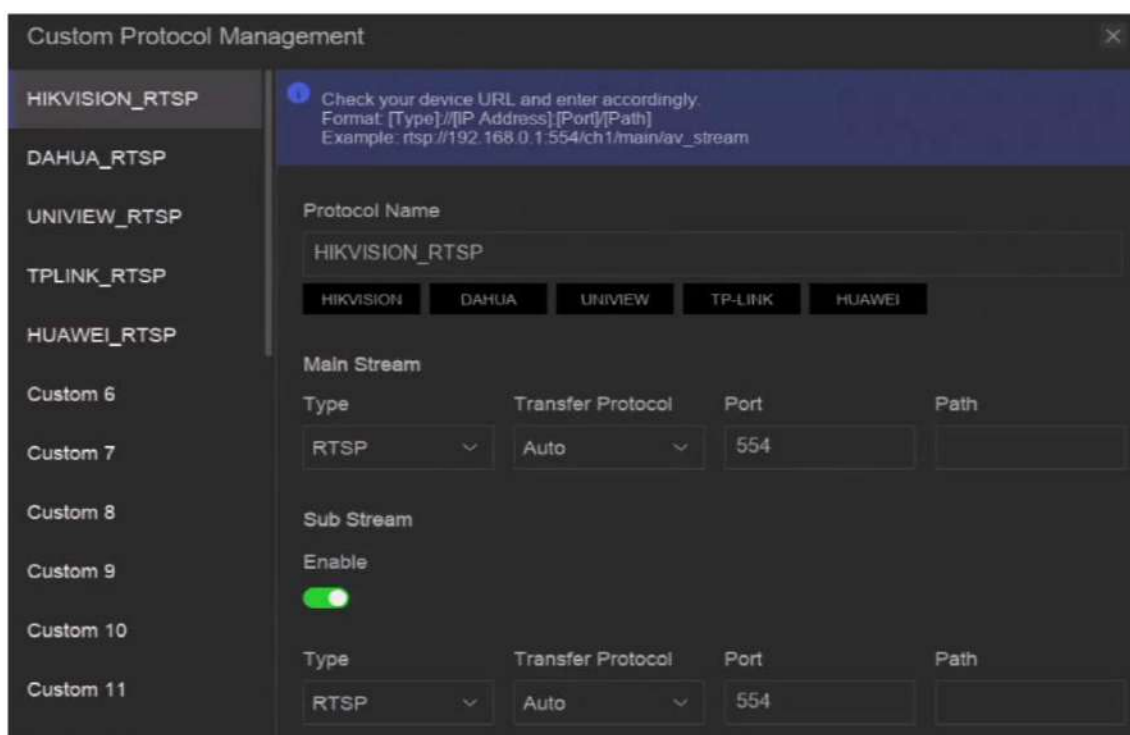


Figura 6-3 Agregar cámara de red mediante protocolo personalizado

3. Seleccione un tipo de protocolo en el lado izquierdo.
4. Establecer parámetros del protocolo.

### Tipo

La cámara de red que adopta un protocolo personalizado debe admitir la transmisión a través de RTSP estándar.

### Protocolo de transferencia

Se pueden seleccionar 3 tipos, incluidos Automático, UDP y RTP sobre RTSP.

### Puerto

El puerto para transmisión RTSP, su valor predeterminado es 554.

### Camino

Contacte al fabricante de la cámara de red para obtener la URL para obtener la transmisión principal y la subtransmisión. El formato general es [Tipo]://[Dirección IP]:[Puerto]/[Ruta del recurso]; por ejemplo, rtsp://192.168.0.1:554/ch1/main/av\_stream.



### Nota

- El nombre y la ruta del protocolo se pueden generar automáticamente si hace clic en un nombre de marca a continuación  
Nombre del protocolo.
- Puede desactivar la transmisión secundaria si la cámara no admite la transmisión secundaria o no es necesario  
Utilice la subtransmisión.

---

5. Haga clic en Aceptar.

6. Haga clic en Agregar en Sistema → Acceso al dispositivo → Dispositivo → Dispositivo de video para agregar manualmente una red cámara.

## 6.1.6 Agregar cámara de red a través del archivo de configuración de la cámara

Se puede exportar la información de las cámaras de red añadidas, incluyendo la dirección IP, el puerto, la contraseña del administrador, etc.

El archivo de configuración de la cámara exportado se puede editar en su ordenador. Tras la edición, también se puede importar a otros dispositivos para añadir las cámaras.

### Antes de comenzar

Conecte su grabadora de video a una unidad flash USB que contenga el archivo de configuración de la cámara.

### Pasos

1. Vaya a Sistema → Acceso al dispositivo → Dispositivo → Dispositivo de video .
2. Haga clic en Importar para importar el archivo de configuración en la unidad flash USB.
3. Establezca la ruta de la carpeta.
4. Haga clic en Confirmar.

## 6.2 Agregar dispositivo de control de acceso


Se pueden agregar dispositivos de control de acceso a su grabadora de vídeo.

El proceso de adición es similar con Access Video Device .

---

### 6.3 Agregar panel de control de seguridad

#### Pasos

1. Vaya a Sistema → Acceso al dispositivo → Dispositivo → Panel de control de seguridad .
2. Haga clic en Agregar.
3. Opcional: seleccione un protocolo.
4. Ingrese la dirección IP, el nombre y el puerto de servicio IoT del dispositivo.
5. Opcional: seleccione un protocolo de transferencia si selecciona OPTEx como tipo de protocolo.
6. Opcional: haga clic en  columna Operación para configurar los parámetros OSD, incluida la codificación de caracteres, el modo de superposición, el tamaño de fuente, etc.



#### Nota

El canal vinculado no se puede editar. Para editarlo, vaya a Centro de eventos → Configuración de eventos → Configuración de eventos → Evento del panel de control de seguridad .

---

La información OSD que haya configurado se mostrará en la imagen de video.

### 6.4 Agregar dispositivo de audio

Se pueden agregar dispositivos de audio a su grabadora de video, como parlantes IP y micrófonos.

El proceso de adición es similar con Access Video Device . Si conecta canales de video con un altavoz IP, este podría usarse para transmisión de voz. Si conecta canales de video con un micrófono, este se usaría como entrada de audio de los canales de video conectados para la grabación de video.

### 6.5 Agregar dispositivo POS

Se puede conectar una máquina/servidor POS a ciertos modelos de dispositivo. El dispositivo puede recibir mensajes de transacción de la máquina/servidor POS, superponerlos en la imagen de video y activar alarmas de eventos POS.

#### Pasos

1. Vaya a Sistema → Acceso al dispositivo → Dispositivo → POS .
2. Haga clic en Agregar para agregar un dispositivo POS.

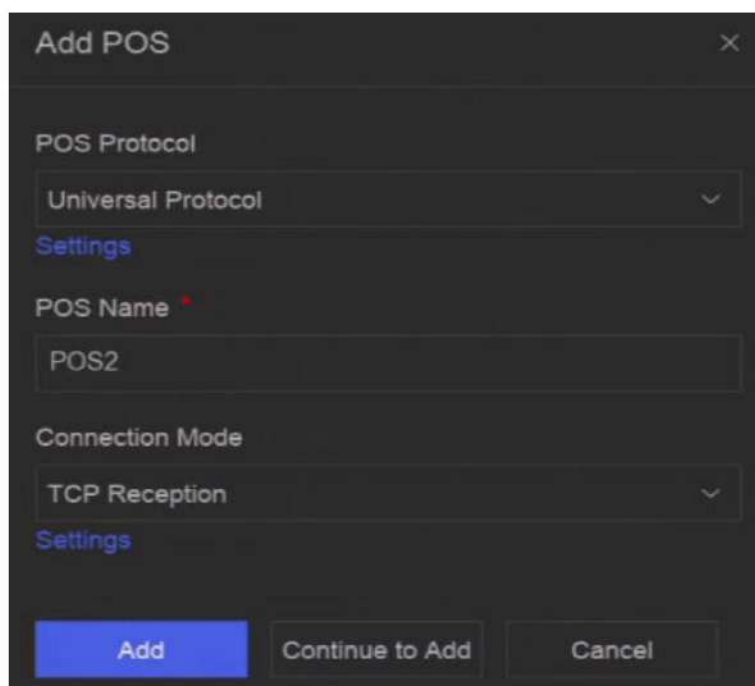


Figura 6-4 Agregar dispositivo POS

3. Configure los parámetros del dispositivo POS.

Protocolo POS

Protocolo Universal

Puede configurar el identificador de línea inicial, el salto de línea y el final de línea para los caracteres de superposición POS, así como la distinción entre mayúsculas y minúsculas. También puede comprobar opcionalmente el identificador de filtrado y el protocolo XML.

EPSON

Las etiquetas de línea de inicio y final fijas se utilizan para el protocolo EPSON.

CRA

Las etiquetas de línea fijas de inicio y fin se utilizan para el protocolo AVE. Se admiten conexiones de puerto serie y puerto serie virtual.

NÚCLEO

Las etiquetas de línea fijas de inicio y fin se utilizan para el protocolo AVE. Se admiten conexiones de puerto serie y puerto serie virtual. El protocolo NUCLEUS debe utilizarse en la comunicación de conexión RS-232.

Modo de conexión

Conexión TCP

Al utilizar una conexión TCP, el puerto debe configurarse entre 1 y 65535, y el puerto para cada máquina POS debe ser único.



#### Conexión UDP

Al utilizar una conexión UDP, el puerto debe configurarse entre 1 y 65535, y el puerto para cada máquina POS debe ser único.

#### Conexión USB a RS-232

Configure los parámetros del puerto del convertidor USB a RS-232, incluido el número de serie del puerto, la velocidad en baudios, el bit de datos, el bit de parada y la paridad.

#### Conexión RS-232

Conecte el dispositivo y la máquina POS a través de RS-232.

#### Conexión de multidifusión

Al conectar el dispositivo y la máquina POS a través del protocolo Multicast, configure la dirección y el puerto de multidifusión.

#### Conexión Sniff

Conecte el dispositivo y el TPV mediante Sniff. Configure las direcciones de origen y destino.

4. Haga clic en Agregar.



Nota

Después de agregar un dispositivo POS, puede hacer clic en Operación para configurar la superposición de texto de POS.

---

## 6.6 Gestión de canales

Tras agregar un dispositivo de video, puede ver su número y nombre de canal, así como administrar sus parámetros. Esta función se utiliza principalmente para dispositivos de video con más de un canal.

Vaya a Sistema → Acceso al dispositivo → Canal para administrar los canales de los dispositivos de video.

## Capítulo 7 Agrupación de dispositivos

Los dispositivos agregados se pueden clasificar en diferentes grupos personalizados.

Pasos

1. Vaya a Sistema → Acceso al dispositivo → Agrupación de dispositivos .

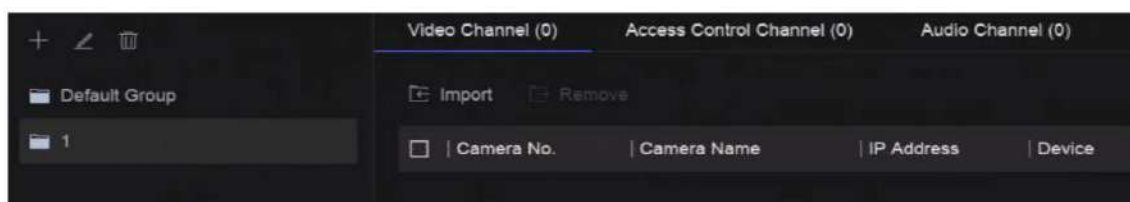





Figura 7-1 Agrupación de dispositivos

2. Haga clic en  para agregar un grupo.



Nota

Después de agregar un grupo, puede hacer clic en  para editarlo o  para eliminarlo.

3. Haga clic en Importar para agregar canales al grupo seleccionado.

## Capítulo 8 Configuración del dispositivo de video o audio

Puede configurar el dispositivo de vídeo o audio agregado, como máscara de privacidad, parámetros de imagen, etc.

### 8.1 Habilitar el acceso a la transmisión H.265

El dispositivo puede cambiar automáticamente a la transmisión H.265 de la cámara IP (que admite el formato de video H.265) para el acceso inicial.

#### Pasos

1. Vaya a Sistema → Acceso al dispositivo → Dispositivo → Dispositivo de video .
2. Haga clic en Más → Cambiar automáticamente a H.265 .
3. Habilite esta función.
4. Haga clic en Guardar.

### 8.2 Configurar los ajustes de pantalla

Configure la OSD (visualización en pantalla), la configuración de la imagen, la configuración de la exposición, la configuración del cambio día/noche, etc.

Vaya a Sistema → Acceso al dispositivo → Configuración del dispositivo → Parámetros del dispositivo → Dispositivo de vídeo → Configuración de pantalla. Seleccione una cámara y configure los parámetros que desee.

#### Configuración OSD

Configure los ajustes OSD (visualización en pantalla) de la cámara, incluida la fecha/hora, el nombre de la cámara, etc.

#### Configuración de imagen

Personalice los parámetros de la imagen, incluido el brillo, el contraste y la saturación para la vista en vivo y el efecto de grabación.

#### Tiempo de exposición

Ajuste el tiempo de exposición de la cámara (de 1/10000 a 1 s). Un valor de exposición mayor produce una imagen más brillante.

#### Interruptor día/noche

La cámara se puede configurar en modo diurno, nocturno o con cambio automático según las condiciones de iluminación del entorno.

Retroiluminación: Configure el amplio rango dinámico (WDR) de la cámara (de 0 a 100). Cuando la iluminación ambiental y el objeto presenten grandes diferencias de brillo, debe configurar el valor WDR.

#### Mejora de la imagen

Para mejorar al máximo el contraste de la imagen.

### 8.3 Configurar parámetros de vídeo

Los parámetros de video afectarían la imagen de visualización en vivo y el archivo de grabación.

Vaya a Sistema → Acceso al dispositivo → Configuración del dispositivo → Parámetros del dispositivo → Dispositivo de vídeo → Parámetros de vídeo. Seleccione una cámara y configure los parámetros según sus preferencias.

#### Corriente principal

La transmisión principal se refiere a la transmisión principal que afecta los datos grabados en el disco duro y determina directamente la calidad del video y el tamaño de la imagen. A diferencia de la transmisión secundaria, la transmisión principal proporciona un video de mayor calidad con mayor resolución y velocidad de fotogramas.

#### Subflujo

Sub-stream es un códec secundario que se ejecuta junto con el principal. Permite reducir el ancho de banda de internet saliente sin sacrificar la calidad de la grabación directa. Sub-stream suele usarse exclusivamente en aplicaciones de smartphones para ver vídeo en directo. Los usuarios con velocidades de internet limitadas pueden beneficiarse al máximo de esta configuración.

#### Resolución

La resolución de imagen mide el nivel de detalle que puede contener una imagen digital. A mayor resolución, mayor nivel de detalle.

La resolución se puede especificar como el número de columnas de píxeles (ancho) por el número de filas de píxeles (alto), por ejemplo, 1024 × 768.

#### Tipo de tasa de

bits. La tasa de bits (en kbit/s o Mbit/s) suele denominarse velocidad, pero en realidad define la cantidad de bits por unidad de tiempo, no la distancia por unidad de tiempo. Existen dos tipos: variable y constante.

#### Velocidad de fotogramas

Se refiere al número de fotogramas capturados por segundo. Una mayor velocidad de fotogramas es ventajosa cuando hay movimiento en la transmisión de vídeo, ya que mantiene la calidad de la imagen en todo momento.

#### Intervalo de fotograma I

El I-Frame, también conocido como intraimagen, es el primer fotograma de cada GOP (tecnología de compresión de vídeo de MPEG). Se puede visualizar como imágenes después de la compresión. El intervalo de I-Frame es la cantidad de fotogramas entre dos I-Frames consecutivos.

### 8.4 Configurar la máscara de privacidad

La máscara de privacidad protege la privacidad personal al ocultar partes de la imagen de la vista en vivo o la grabación con un área enmascarada.

#### Pasos

1. Vaya a Sistema → Acceso al dispositivo → Configuración del dispositivo → Parámetros del dispositivo → Dispositivo de video → Máscara de privacidad.

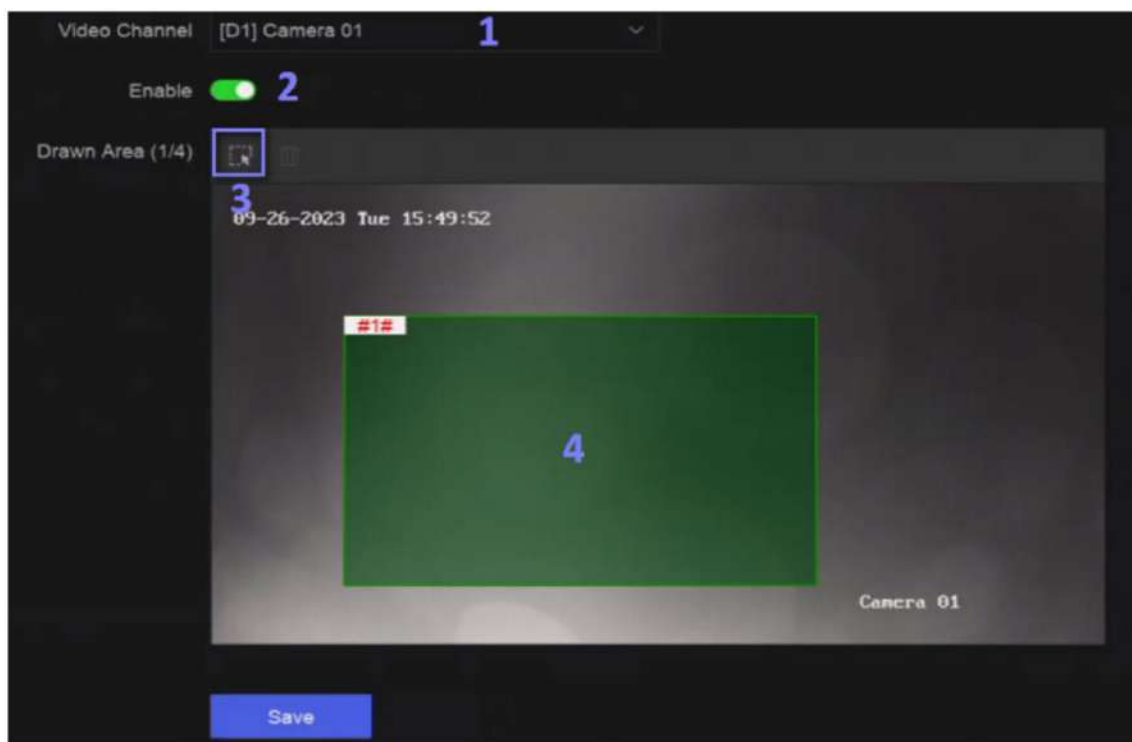


Figura 8-1 Máscara de privacidad

2. Seleccione una cámara.
3. Activar Habilitar.
4. Dibuje áreas de máscara en la ventana de vista previa. Estas áreas se marcarán con marcos de diferentes colores.



Nota

Se pueden configurar hasta 4 áreas de máscara de privacidad y se puede ajustar el tamaño de cada área.

---

5. Haga clic en Guardar.

## 8.5 Configurar la protección de la privacidad

Esta función permite oscurecer o desenfocar automáticamente áreas específicas (incluidos rostros y cuerpos humanos y vehículos) en las imágenes de video para proteger la privacidad personal o la información confidencial.

#### Antes de comenzar

Esta función debe ser compatible con la cámara.

#### Pasos

1. Vaya a Sistema → Acceso al dispositivo → Configuración del dispositivo → Parámetros del dispositivo → Dispositivo de video → Protección de la privacidad .

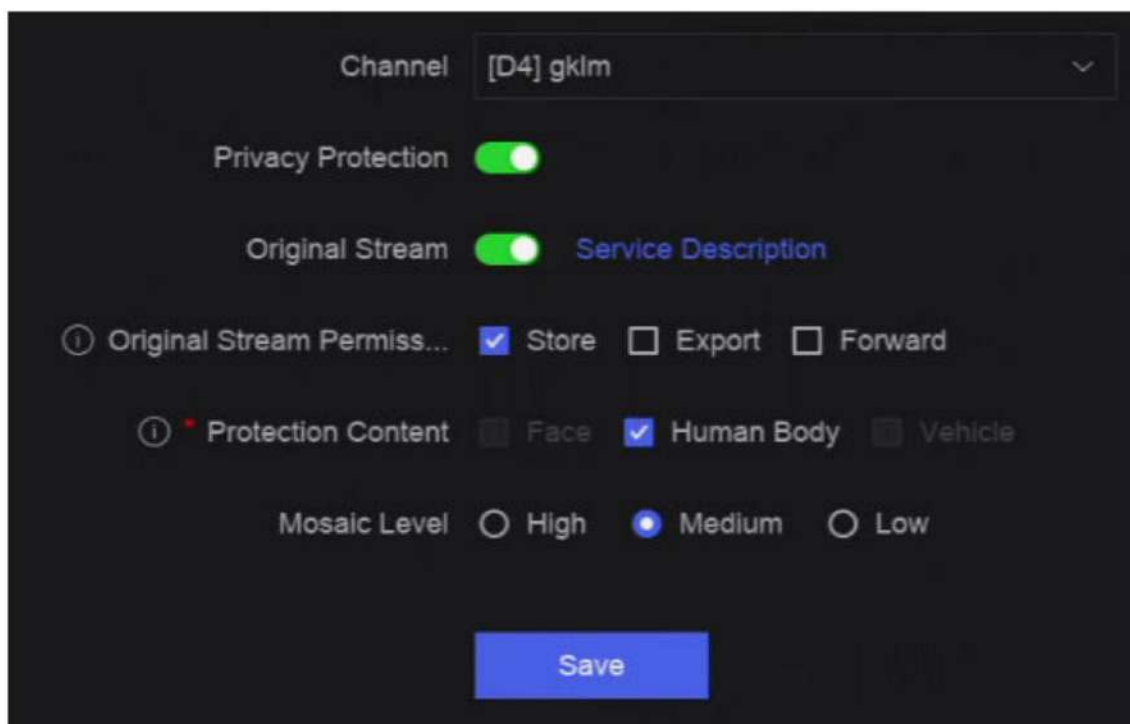


Figura 8-2 Protección de la privacidad

2. Seleccione una cámara.
3. Habilite la protección de privacidad.
4. Opcional: habilite la transmisión original y configure el permiso de transmisión.



#### Nota

Transmisión original significa transmisión de video sin mosaico.

---

#### Almacenar

La transmisión original se puede almacenar. Almacenar la transmisión original consumirá más espacio de almacenamiento o reducirá el tiempo de grabación del canal. La tasa de bits de la transmisión original es la misma que la de la cámara, que no es configurable.

#### Exportar

La transmisión original del canal se puede exportar.

#### Adelante

La transmisión original se puede reenviar.



### Nota

Debes verificar el permiso de la tienda antes de verificar los permisos de exportación y/o reenvío.

5. Establecer contenido de protección. El contenido de protección seleccionado se verá borroso durante la vista en vivo y reproducción.
6. Ajuste el nivel de mosaico. Cuanto más alto sea el nivel, más borrosa será la imagen.
7. Haga clic en Guardar.

## 8.6 Configurar parámetros de audio

Tras agregar un dispositivo de audio, puede configurar sus parámetros en Sistema → Acceso al dispositivo → Configuración del dispositivo → Parámetros del dispositivo → Dispositivo de audio. Por ejemplo, si agrega un altavoz IP, puede configurar su nombre, volumen de salida de audio y calidad de audio.

## 8.7 Configurar el servicio OTAP

OTAP (Protocolo de Acceso a Objetos Abiertos) es un estándar integrado unificado y un modo push-pull del protocolo de Hikvision en redes públicas y privadas. Una vez habilitado OTAP, otras aplicaciones podrán visualizar videos de forma remota a través de este protocolo.

Antes de comenzar

Asegúrese de que la red de su dispositivo sea accesible a través del protocolo OTAP.

Pasos

1. Vaya a Sistema → Acceso al dispositivo → Configuración del dispositivo → Servicio de acceso → Servicio OTAP.

Figura 8-3 Configurar el servicio OTAP

- 2. Activar Habilitar.
- 3. Establezca los parámetros.
- 4. Haga clic en Guardar.

## 8.8 Configuración por lotes

Los dispositivos conectados se pueden configurar en un lote.

Pasos 1.

Vaya a Sistema → Acceso al dispositivo → Configuración del dispositivo → Configuración por lotes .

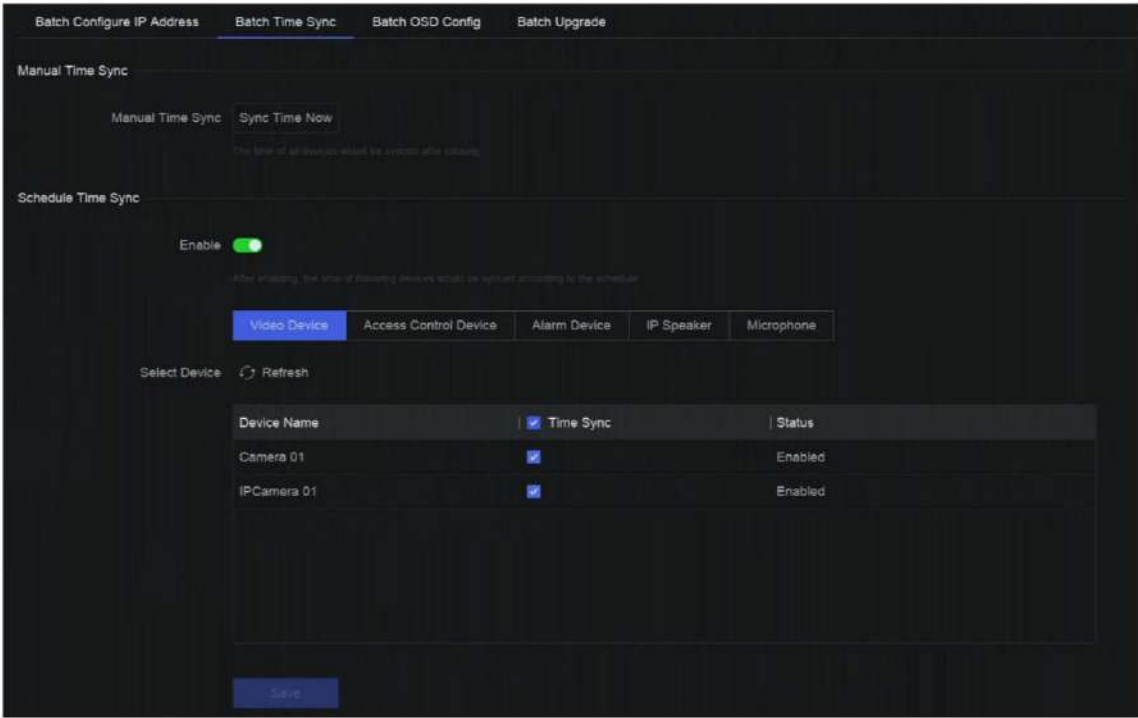


Figura 8-4 Configuración por lotes 2. Configure la

dirección IP, la sincronización horaria, el OSD o actualice el firmware según sus deseos.

### Sincronización horaria manual

Haga clic en Sincronizar hora ahora para sincronizar manualmente la hora de todos los dispositivos conectados. Esta operación es solo para... una vez.

### Programar sincronización horaria

La grabadora sincronizará la hora de los dispositivos seleccionados según un cronograma fijo.

- 3. Para configurar la dirección IP y sincronizar la hora, haga clic en Guardar.



## 8.9 Configurar la interfaz PoE (Alimentación a través de Ethernet)

Las interfaces PoE permiten que el dispositivo transfiera energía eléctrica y datos a los dispositivos PoE conectados. Además, la interfaz PoE es compatible con la función Plug and Play. El número de dispositivos PoE conectables varía según el modelo. Si desactiva una interfaz PoE, también puede usarla para conectarse a un dispositivo en línea.

Antes de comenzar

Asegúrese de que su NVR admita la función PoE.

Pasos

1. Vaya a Sistema → Acceso al dispositivo → Configuración del dispositivo → PoE.
2. Habilite la función Plug-and-Play de las interfaces PoE según sus necesidades.
3. Seleccione el tipo de dispositivo como Altavoz IP o Cámara.
4. Si se utiliza una interfaz PoE para conectar una cámara PoE, seleccione la distancia de conexión de la red cable.

Larga distancia

Transmisiones de red de larga distancia (100 a 300 metros) a través de interfaz PoE.

Corta distancia

Transmisión de red de corta distancia (< 100 metros) a través de interfaz PoE.



Nota

- Las interfaces PoE están habilitadas con el modo de corta distancia de forma predeterminada. • El ancho de banda de la cámara IP conectada al PoE se realiza mediante un cable de red largo (de 100 a 300 metros). no puede exceder los 6 MP.
  - La longitud máxima permitida del cable de red puede ser inferior a 300 metros dependiendo de la IP. Modelos de cámaras y materiales de cables.
  - Cuando la distancia de transmisión alcance de 100 a 250 metros, deberá utilizar el CAT5E o CAT6 Cable de red para conectar con la interfaz PoE.
  - Cuando la distancia de transmisión alcance los 250 a 300 metros, deberá utilizar la red CAT6 Cable para conectar con la interfaz PoE.
- 

5. Haga clic en Guardar.

Qué hacer a

continuación Cuando los dispositivos PoE están conectados, puede ver el estado y la energía de cada interfaz PoE.

## Capítulo 9 Gestión del almacenamiento

### 9.1 Administrar el disco duro


Es necesario inicializar un disco duro (HDD) recién instalado antes de usarlo. Puede formatearlo, reparar la base de datos y consultar su estado a través de la interfaz de administración de HDD.

Antes de comenzar

Asegúrese de que el disco duro esté instalado correctamente en su dispositivo.

Pasos 1.

Vaya a Sistema → Administración de almacenamiento → Disco duro de almacenamiento → Disco duro de almacenamiento



HDD No.	Free Space (GB)	Capacity (GB)	Status	Type	Property	Operation
1	166	466	Sleeping	Local	R/W	
3	3685	3726	Sleeping	Local	R/W	
5	3685	3726	Sleeping	Local	R/W	

Figura 9-1 Administrar HDD

2. Opcional: Realice las siguientes operaciones según su deseo.

Agregar red	Agregue un NAS o IP SAN.
Disco duro	
Formato	Formatear el disco duro seleccionado.
Reparar	Reparar la base de datos reconstruirá todas las bases de datos. Esto podría ayudar a mejorar la velocidad del sistema después de la actualización.
Base de datos	



#### Nota

- La reparación de la base de datos reconstruirá todas las bases de datos. Los datos existentes no se verán afectados, pero las funciones de búsqueda y reproducción locales no estarán disponibles durante el proceso. Puede acceder a ellas de forma remota mediante un navegador web, software cliente, etc.
- No extraiga la unidad ni apague el dispositivo durante el proceso.



Quitar/cargar el disco duro.

### 9.2 Configuración RAID

Una matriz de discos es una tecnología de virtualización de almacenamiento de datos que combina varias unidades de disco físicas en una sola unidad lógica. También conocida como "RAID", una matriz almacena datos en varios discos duros para proporcionar suficiente redundancia y permitir la recuperación de datos si falla un disco. Los datos se distribuyen.

a través de las unidades de una de varias maneras llamadas "niveles RAID", según la redundancia y el rendimiento requeridos.



### Precaución

RAID requiere discos duros de nivel empresarial.

Las funciones de esta sección solo están disponibles para ciertos modelos. Se recomienda usar discos duros del mismo modelo y capacidad.

Hay dos maneras de crear un RAID. Para la creación con un solo toque, el tipo de RAID predeterminado es RAID 5. Para la creación manual, se pueden configurar RAID 0, RAID 1, RAID 5, RAID 6 y RAID 10.

Tabla 9-1 Requisitos de HDD para cada tipo de RAID

Tipo de RAID	Número requerido de discos duros
RAID0	≥2
RAID1	2
RAID 5	≥3
RAID 6	≥4
RAID10	4 u 8



### Nota

• La función solo está disponible para ciertos modelos. • Cuando ocurre un evento de excepción de matriz, las acciones de vinculación correspondientes se pueden configurar en Sistema → Configuración del sistema → Excepción .

### 9.2.1 Crear una matriz de discos

Se puede crear una matriz de discos después de habilitar el modo de matriz.

#### Antes de empezar

• El modo de almacenamiento está configurado en Cuota en Sistema → Administración de almacenamiento → Modo de almacenamiento . • Hay suficientes discos duros correctamente instalados en el dispositivo. Y los discos duros para la creación de matrices son AI o nivel empresarial.

#### Pasos

1. Vaya a Sistema → Administración de almacenamiento → Disco duro de almacenamiento → Administración de matriz .
2. Haga clic en Habilitar modo de matriz o habilite el modo de matriz.

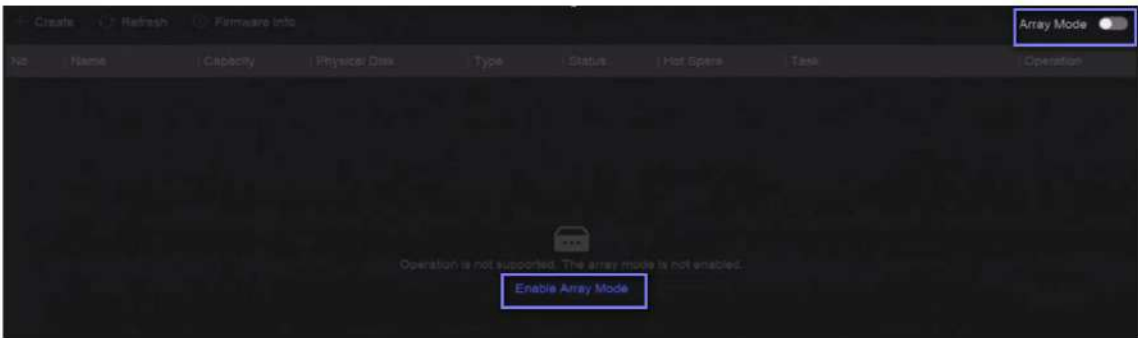


Figura 9-2 Habilitar RAID

- 3. Espere a que el dispositivo se reinicie.
- 4. Vaya a Sistema → Administración de almacenamiento → Disco duro de almacenamiento → Administración de matrices nuevamente.

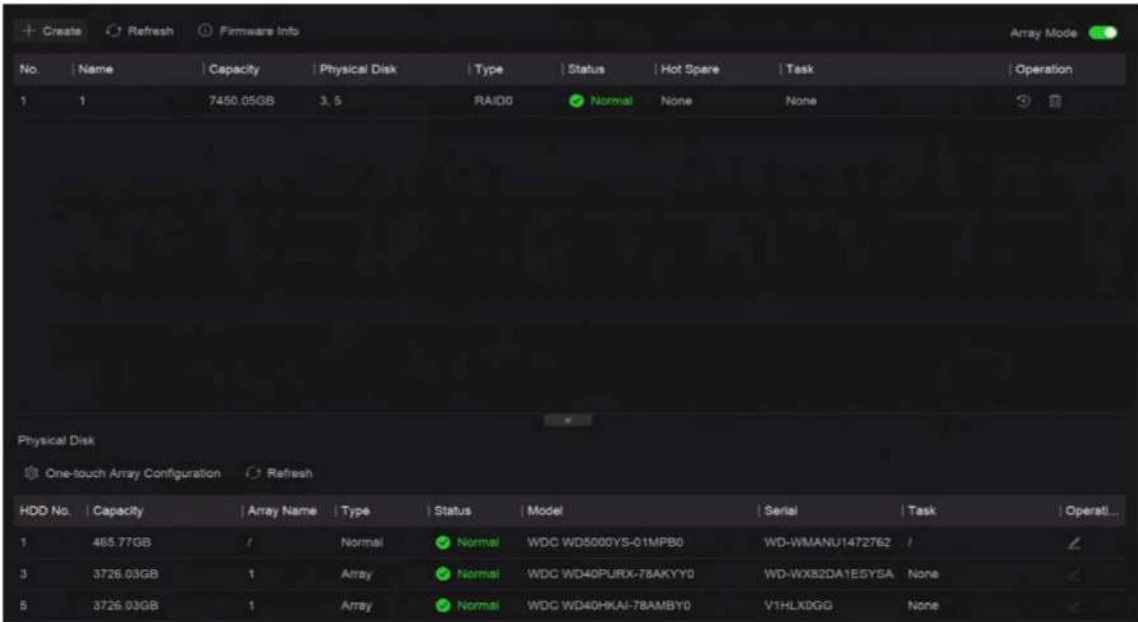


Figura 9-3 Gestión de matrices

- 5. Crea una matriz.

Método de creación	Descripción
Matriz de un solo toque	Haga clic en Configuración de matriz de un toque.
Configuración	<div><div></div><div>Nota</div></div> <p>De forma predeterminada, el tipo de matriz creado mediante la configuración de un toque es RAID 5.</p>
Creación manual	Haga clic en Crear para crear manualmente una matriz RAID 0, RAID 1, RAID 5, RAID 6 o RAID 10.



### 9.2.2 Reconstruir matriz

El estado del array incluye: Funcional, Degradado y Fuera de línea. Para garantizar la alta seguridad y confiabilidad de los datos almacenados en un array, realice un mantenimiento inmediato y adecuado del array según su estado.


#### Pasos

1. Vaya a Sistema → Administración de almacenamiento → Disco duro de almacenamiento → Administración de matriz .
2. Reconstruir una matriz.

Tabla 9-2 Método de reconstrucción

Método de reconstrucción	Descripción
Reconstrucción automática	<p>Debe haber un disco de repuesto en caliente en la matriz, y su capacidad no debe ser menor que la del disco con la capacidad mínima de la matriz. Haga clic en la columna Operación , debajo de Disco , para configurar un disco de repuesto en caliente.</p> <p>Cuando un disco duro de la matriz no funciona, se activará el disco de repuesto activo y la matriz se reconstruirá automáticamente.</p> <p> Nota</p> <p>Una vez finalizada la reconstrucción automática, se recomienda instalar otro HDD y configurarlo como disco de repuesto activo.</p>
Reconstrucción manual	<p>Si no hay discos de repuesto en caliente en la matriz, deberá reconstruir la matriz manualmente.</p> <p>Vaya a Sistema → Administración de almacenamiento → HDD de almacenamiento → Administración de matriz y seleccione el disco de repuesto activo en la lista para reconstruirlo.</p>

### 9.2.3 Eliminar matriz

Vaya a Sistema → Administración de almacenamiento → HDD de almacenamiento para hacer  para eliminar la matriz seleccionada.

### 9.2.4 Ver información del firmware

Puede ver la información del firmware de la matriz y configurar la velocidad de la tarea en segundo plano.

Antes de comenzar

Asegúrese de que la matriz de discos esté habilitada.

Pasos

1. Vaya a Sistema → Administración de almacenamiento → Disco duro de almacenamiento → Administración de matriz .
2. Haga clic en Información del firmware.
3. Opcional: Establecer la velocidad de la tarea en segundo plano.

### 9.3 Configurar el modo de almacenamiento

Pasos

1. Vaya a Sistema → Administración de almacenamiento → Modo de almacenamiento .

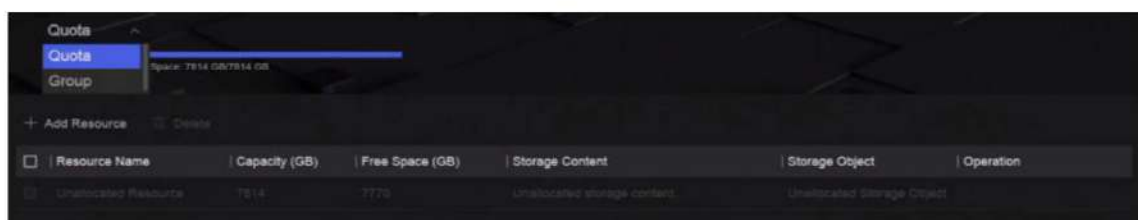


Figura 9-4 Modo de almacenamiento

2. Seleccione Cuota o Grupo.

Cuota

Cada cámara o dispositivo de audio se puede configurar con una cuota asignada para almacenar vídeos, imágenes o audios.

Grupo:

Se pueden gestionar varios discos duros en grupos. Se puede grabar vídeo de canales específicos en un grupo de discos duros específico mediante la configuración del disco duro.

3. Establezca los parámetros correspondientes. •


Cuota: Asignar espacio para objetos de almacenamiento. • Grupo:

Vincular canales a grupos de HDD.

### 9.4 Configurar otros parámetros de almacenamiento

Vaya a Sistema → Administración de almacenamiento → Configuración avanzada .

Tabla 9-3 Descripción de parámetros

Nombre del parámetro	Descripción
HDD durmiendo	Seleccione un modo para los discos duros. Modo de rendimiento, Modo equilibrado y Se pueden seleccionar los modos de ahorro de energía .
Sobrescritura	Cuando el disco duro esté lleno, continuará escribiendo nuevos archivos eliminándolos. archivos más antiguos
Guardar datos VCA de la cámara	Después de guardar los datos VCA de la cámara en su dispositivo, podrá búscalo en el centro de eventos.
Duración máxima por vídeo	Es la duración de cada archivo de vídeo cuando se exportan vídeos desde el dispositivo.
Etiqueta de vídeo posterior a la grabación	<p>Después de agregar una etiqueta a un video, es el tiempo que establece para grabar después de la hora programada</p> <p> Nota</p> <ul style="list-style-type: none"> <li>• Puede hacer clic durante la vista en vivo o la reproducción para agregar una etiqueta.</li> <li>• Para buscar videos por etiqueta, vaya a → Copia de seguridad → Por etiqueta.</li> </ul>
eSATA	Para dispositivos con interfaz eSATA en el panel trasero.
Uso	Establecer el uso de eSATA.

## 9.5 Administrar unidad flash USB

Después de insertar una unidad flash USB en su dispositivo, puede ver su capacidad de almacenamiento restante, gestionar su contenido o formatearlo.

Cuando se conecta una unidad flash USB a su dispositivo por primera vez, se pueden realizar operaciones breves

Se realizaron varias acciones, como la actualización y la copia de seguridad del dispositivo. Mientras tanto, se mostrará un nuevo icono en la esquina superior derecha.



## Capítulo 10 Configuración de programación

El dispositivo seguirá el cronograma para almacenar archivos en el disco.

### 10.1 Configurar plantilla de programación

Una vez configurada una plantilla de programación, puedes usarla como programación de grabación.

Pasos

1. Vaya a Sistema → Configuración del sistema → Configuración de plantilla → Programación de vacaciones .
2. Haga clic en Agregar.

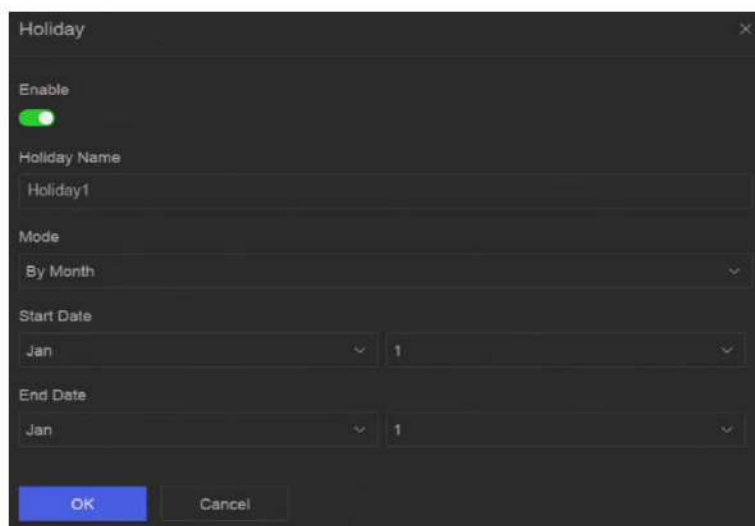


Figura 10-1 Agregar vacaciones

3. Activar Habilitar.
4. Configurar las vacaciones.



Nota

Una vez configurados los días festivos, podrá establecer el cronograma de días festivos de forma independiente.

El horario de vacaciones tiene mayor prioridad que el horario normal (de lunes a domingo).

---

5. Establecer programación de almacenamiento.
  - 1) Haga clic en Programación de almacenamiento.
  - 2) Seleccione un nombre para la plantilla.



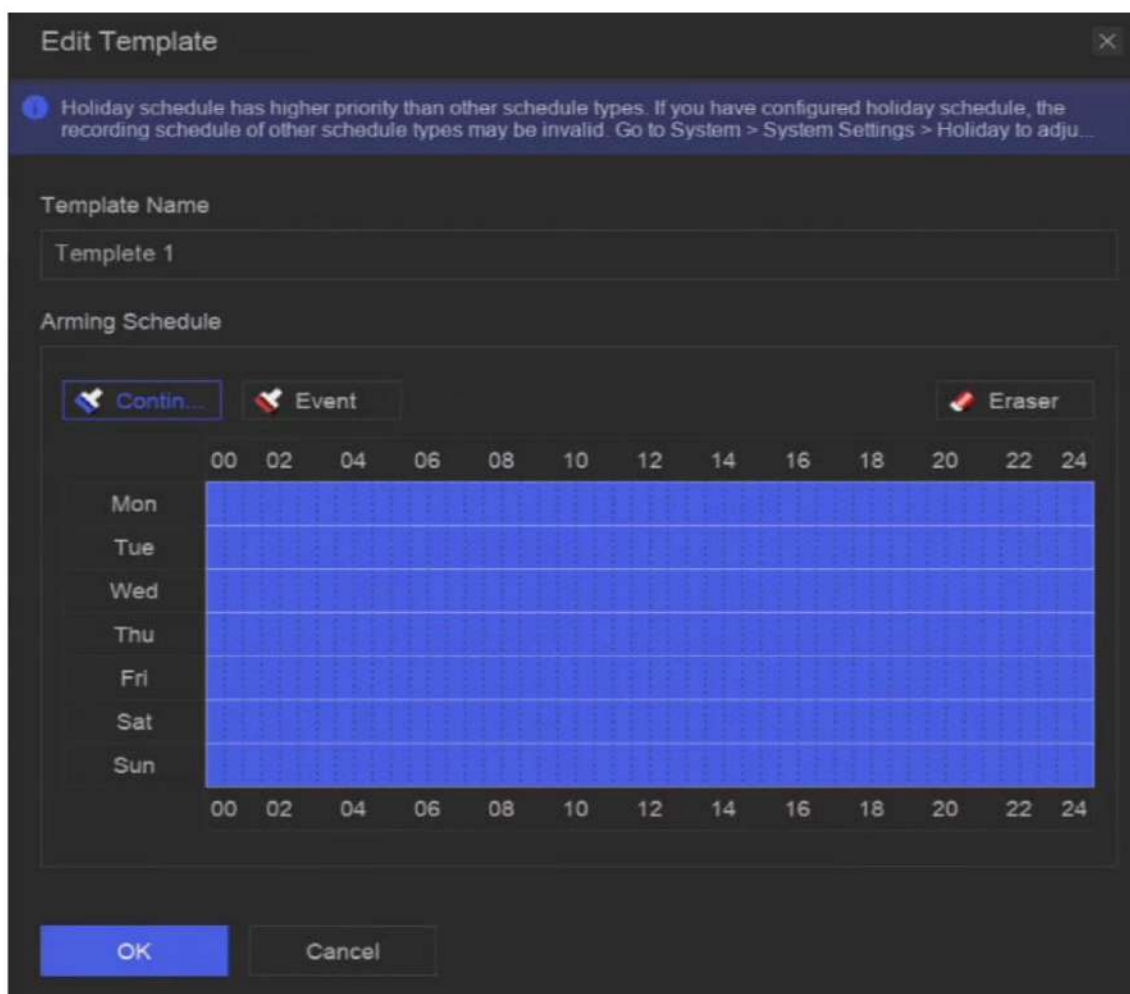


Figura 10-2 Editar plantilla 3)

Seleccione un tipo de grabación. Por ejemplo, Evento.

4) Arrastre el cursor sobre la barra de tiempo para dibujar la programación.



Nota

- Después de mover el cursor en la barra de tiempo, también puede hacer clic
- Puede hacer clic en Borrador para borrar la programación.

00:00-24:00



para establecer una hora específica



Nota

También puede hacer clic en Configurar plantilla para configurar la plantilla en Sistema → Administración de almacenamiento → Programación de almacenamiento → Grabación de video / Captura de imágenes / Grabación de audio .

6. Haga clic en Aceptar.

## 10.2 Configurar la programación de grabación

La cámara iniciará o detendrá automáticamente la grabación según el programa de grabación configurado.

### Pasos

1. Vaya a Sistema → Administración de almacenamiento → Programación de almacenamiento → Grabación de video .

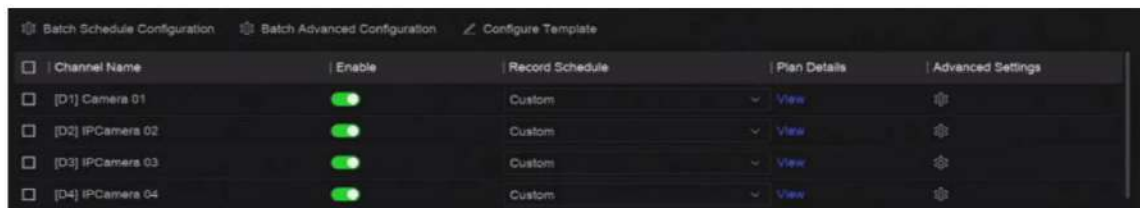


Figura 10-3 Configuración de grabación de video

2. Active Habilitar para una cámara.
3. Seleccione un tipo de programación.



### Nota

Si configura la Programación de grabación como Personalizada, puede arrastrar el cursor sobre la barra de tiempo para configurar la programación de grabación personalizada o mover el cursor sobre la barra de tiempo y **00:00-24:00** para establecer una hora específica hacer clic en programar.

4. Haga clic en Ver para ver el cronograma.



Figura 10-4 Ver programación



5. Opcional: haga clic  Configuración avanzada para configurar otros parámetros avanzados.

Tabla 10-1 Descripción de parámetros avanzados

Parámetro	Descripción
Grabar audio	<p>Habilitar o deshabilitar la grabación de audio.</p> <p> Nota</p> <p>El canal deberá tener función de audio, o tener conectado un dispositivo de audio.</p>
ANR	<p>ANR (Reposición automática de red) puede habilitar automáticamente la tarjeta SD de la cámara de red para guardar el video en caso de desconexión de la red y puede sincronizar datos después de que se recupere la red.</p>
Enlazar	<p>La hora que configuraste para grabar antes de la hora o evento programado. Por ejemplo, si una alarma activa la grabación a las 10:00, y configuras el tiempo de pregrabación en 5 segundos, la cámara graba a las 9:59:55.</p>

Parámetro	Descripción
Post-registro	El tiempo que configuras para grabar después del evento o la hora programada. Por ejemplo, si una alarma activa la grabación a las 11:00, y configuras un tiempo posterior a la grabación de 5 segundos, se graba hasta las 11:00:05.
Tipo de flujo	Para la transmisión principal, la resolución suele ser mayor. Para la transmisión secundaria, se puede grabar durante más tiempo con el mismo espacio de almacenamiento, pero la resolución será baja. Para la transmisión dual, el dispositivo graba tanto la transmisión principal como la secundaria.
Vídeo/Imagen Tiempo vencido	El tiempo de caducidad es el periodo que un archivo debe conservarse en el disco duro. Al alcanzarse este plazo, el archivo se eliminará. Si se establece en 0, el archivo no se eliminará. El tiempo real de conservación del archivo depende de la capacidad del disco duro.

6. Opcional: Seleccione canales en la lista y utilice Configuración de programación por lotes y Lote avanzado

Configuración para configurar canales en un lote.

7. Haga clic en Guardar.

### 10.3 Configurar la programación de captura de imágenes

El dispositivo capturaría automáticamente imágenes en vivo según el cronograma.

Pasos

1. Vaya a Sistema → Administración de almacenamiento → Programación de almacenamiento → Captura de imágenes .

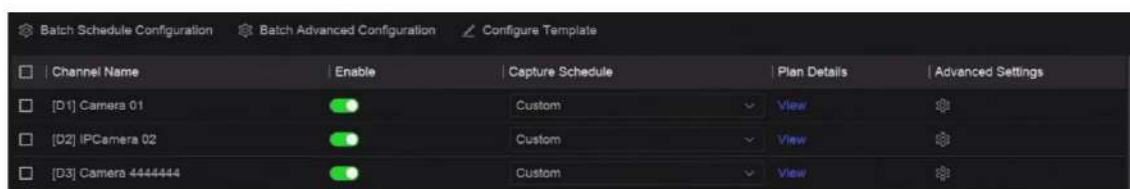


Figura 10-5 Configuración de captura de imágenes

2. Active Habilitar para una cámara.

3. Seleccione un tipo de programación.



Nota

Si configura la Programación de captura como Personalizada, puede arrastrar el cursor en la barra de tiempo para configurar la programación de captura de imágenes personalizada o mover el cursor en la barra de tiempo y hacer clic en la **00:00-24:00** para establecer la programación de tiempo especificada.

4. Haga clic en Ver para ver el cronograma.



Figura 10-6 Ver programación

5. Haga clic en Configuración avanzada para establecer parámetros de imagen avanzados.

Tabla 10-2 Descripción de parámetros avanzados

Parámetro	Descripción
Retraso de captura	La duración de la captura de imágenes.
Resolución	Establezca la resolución de la imagen a capturar.
Calidad de la imagen	Configure la calidad de imagen en baja, media o alta. Alta calidad de imagen. requiere más espacio de almacenamiento.
Intervalo	El intervalo de tiempo de captura de cada imagen en vivo.

6. Opcional: Seleccione canales en la lista y utilice Configuración de programación por lotes y Lote avanzado

Configuración para configurar canales en un lote.

7. Haga clic en Guardar.

## 10.4 Configurar la grabación de audio


El dispositivo grabará audios automáticamente según el cronograma de grabación configurado.

### Pasos

1. Vaya a Sistema → Administración de almacenamiento → Programación de almacenamiento → Grabación de audio .
2. Active **Habilitar para un canal**.
3. Seleccione un tipo de programación.



### Nota

Si configura la Programación de grabación como Personalizada, puede arrastrar el cursor sobre la barra de tiempo para configurar la programación de grabación personalizada o mover el cursor sobre la barra de tiempo y  para establecer una hora específica hacer clic en programar.

4. Haga clic en Ver para ver el cronograma.
5. Opcional: haga clic en Configuración avanzada para configurar otros parámetros avanzados.

Tabla 10-3 Descripción de parámetros avanzados

Parámetro	Descripción
Enlazar	La hora que configuraste para grabar antes de la hora o evento programado. Por ejemplo, si una alarma activa la grabación a las 10:00, y configuras el tiempo de pregrabación en 5 segundos, el canal graba a las 9:59:55.
Post-registro	El tiempo que configuras para grabar después del evento o la hora programada. Por ejemplo, si una alarma activa la grabación a las 11:00, y configuras un tiempo posterior a la grabación de 5 segundos, se graba hasta las 11:00:05.

6. Opcional: Seleccione canales en la lista y utilice Configuración de programación por lotes y Lote avanzado Configuración para configurar canales en un lote.
7. Haga clic en Guardar.

## Capítulo 11 Vista en vivo

### 11.1 Configurar el diseño de la vista en vivo

La vista en vivo muestra la imagen de video de cada cámara en tiempo real.

Pasos

1. Vaya a Vista en vivo.
2. Haga clic en la esquina inferior derecha.
3. Seleccione un tipo de división de ventana o haga clic en Personalizar para personalizar un nuevo tipo según su deseo.
4. Mueva el cursor a Vista predeterminada en Vista.
5. Haga clic en el lado derecho de Ver.
6. Siga las instrucciones para ajustar la interfaz de salida de la imagen en vivo. Además de las dos opciones mencionadas en la interfaz de usuario, puede arrastrar un canal de una ventana a otra.
7. Haga clic en .

### 11.2 Introducción a la GUI

Puede ver imágenes en vivo, reproducir audio en vivo, capturar imágenes, realizar reproducción instantánea, etc.

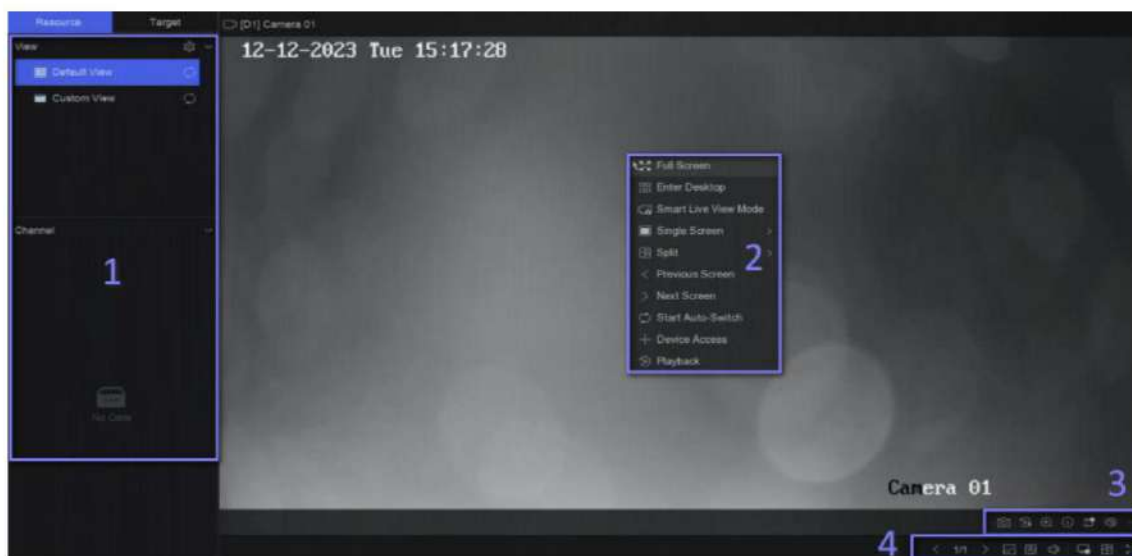


Figura 11-1 Vista en vivo (Tipo 1)

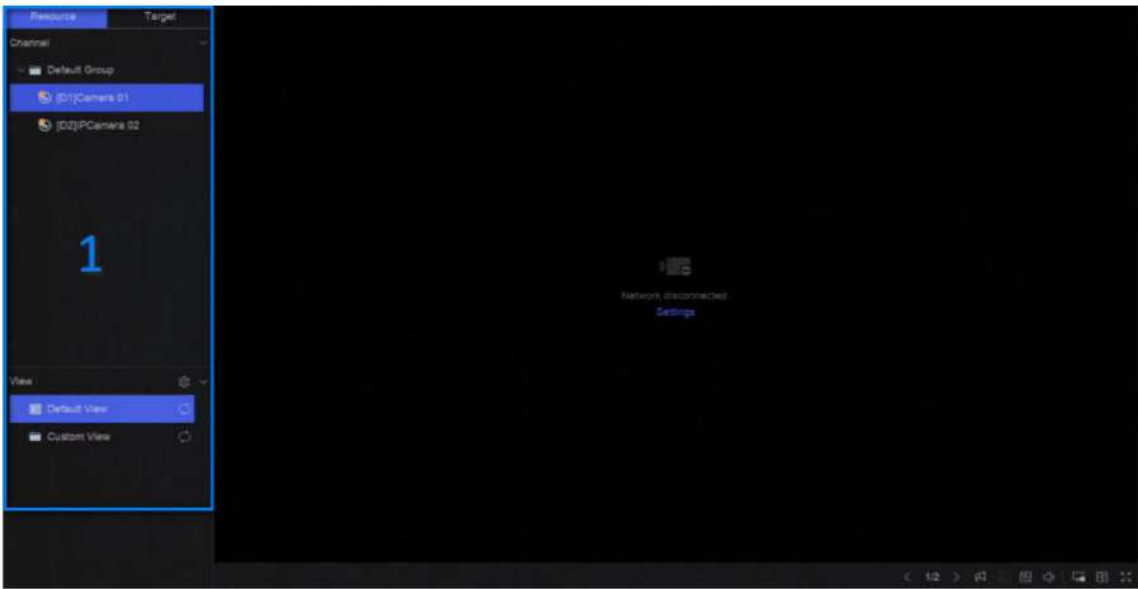





Figura 11-2 Vista en vivo (Tipo 2)

Tabla 11-1 Descripción de la interfaz

No.	Descripción
1	Lista de canales, panel de control PTZ y lista de detección de objetivos. Si selecciona un canal de la lista, el dispositivo lo redirigirá a la ventana correspondiente. Si hace clic en Objetivo, podrá ver los resultados de la detección de objetivos en vivo en la lista y configurar los ajustes correspondientes.
2	Menú contextual del botón derecho. Aparecerá al hacer clic derecho con el cursor en el área de la imagen.
3	Barra de herramientas de canal. <ul style="list-style-type: none"><li>Haga clic  para agregar una etiqueta y acceder al canal. Después de agregarla, puede ir a  de seguridad → Por etiqueta para buscar videos por etiqueta.</li><li>Puede seleccionar  para mostrar información de VCA para mostrar la regla marcos.</li></ul>
4	Barra de herramientas de vista en vivo. Aquí se pueden realizar funciones como transmisión de voz, visualización de información VCA y conmutación de salida .





Nota

- Puede desplazarse hacia arriba o hacia abajo con el mouse para pasar a la pantalla anterior o siguiente.
- Si ocurre una excepción en la visualización de la imagen del canal, la ventana correspondiente mostrará el mensaje de error y puede hacer clic directamente en el texto (en color azul) para editar la configuración del dispositivo.

## 11.3 Control PTZ

PTZ son las siglas de Pan, Tilt y Zoom. Al agregar una cámara PTZ a su dispositivo, este podrá girar a la izquierda y a la derecha, inclinar hacia arriba y hacia abajo, y acercar y alejar la imagen.

Seleccione una cámara PTZ y expanda el menú de control PTZ en la esquina inferior izquierda.

Tabla 11-2 Operación PTZ

Tarea	Descripción	Operación
Programar	Los ajustes preestablecidos registran la posición PTZ y el estado del zoom, enfoque, iris, etc. Puede llamar a un ajuste preestablecido para mover rápidamente la cámara a la posición predefinida.	<p>Establecer un ajuste</p> <p>preestablecido: 1. Seleccione un ajuste preestablecido.</p> <p>2. Utilice los botones de dirección para ajustar la imagen.</p> <p>3. Haga clic  .</p>
		<p>Llamar a un ajuste preestablecido: haga clic  en  .</p>
Patrulla	Se pueden configurar las patrullas para mover el PTZ a puntos clave y permanecer allí durante un tiempo determinado antes de pasar al siguiente punto clave. Los puntos clave corresponden a los ajustes preestablecidos.	<p>Establecer una patrulla: 1. Seleccione una patrulla.</p> <p>2. Haga clic  .</p> <p>en 3. Agregar ajustes preestablecidos para la patrulla.</p> <p>4. Haga clic en Aceptar.</p>
		<p>Llamar a una patrulla: haga clic  en  .</p>
Patrón	Se pueden configurar patrones grabando el movimiento del PTZ. Puedes activar el patrón para que el PTZ se mueva según la ruta predefinida.	<p>Establecer un patrón:</p> <p>1. Haga  .</p> <p>clic 2. Utilice los botones de dirección para ajustar la imagen, el dispositivo grabará el movimiento.</p>
		<p>3. Detener la grabación.</p> <p>Llamar a un patrón: haga clic  en  .</p>



Nota

Si no se puede utilizar el panel PTZ, haga clic para verificar la configuración. .

## Capítulo 12 Reproducción

### 12.1 Introducción a la GUI

Puede reproducir archivos de vídeo o audio.

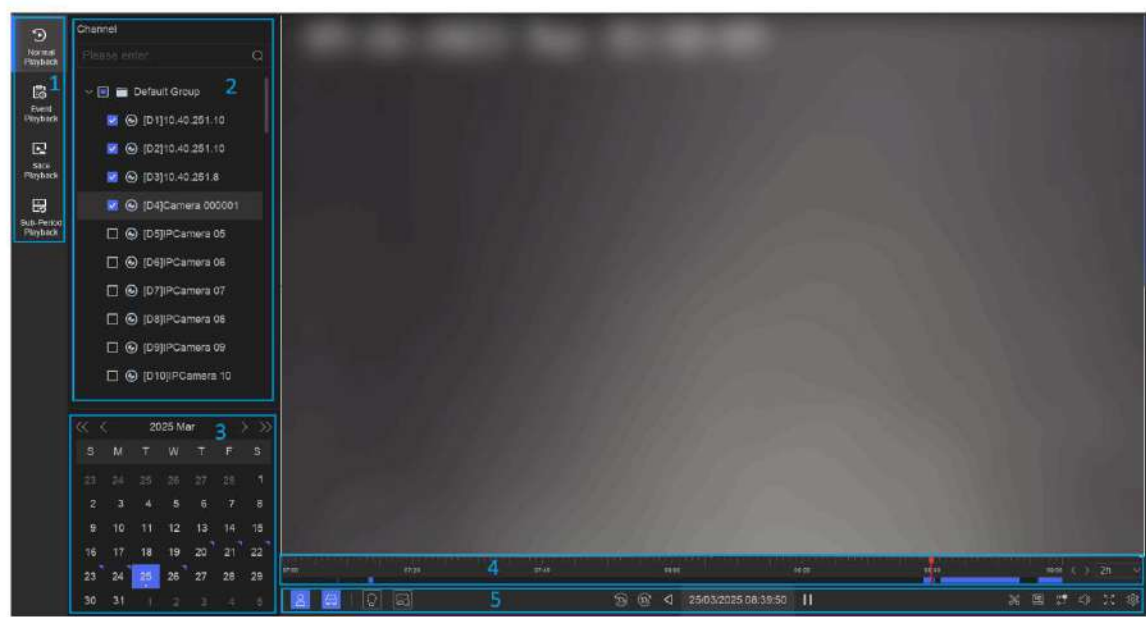









Figura 12-1 Reproducción

Tabla 12-1 Descripción de la interfaz

No.	Descripción
1	Área para seleccionar el tipo de reproducción.
2	Lista de canales.
3	Calendario para selección de hora.
4	<div>Línea de tiempo de reproducción.</div> <ul style="list-style-type: none"><li>• Coloque el cursor en la línea de tiempo, arrastre la línea de tiempo hacia posición hasta un tiempo determinado.</li><li>• El período marcado con barra azul contiene video. Barra roja Indica que el video en el período es un video de evento.</li><li>• Desplácese hacia arriba o hacia abajo para acercar o alejar la línea de tiempo.</li></ul>
5	Barra de herramientas de reproducción.

No.	Descripción
	<ul style="list-style-type: none"> <li>• Haga clic en  (Búsqueda inteligente) y siga las sugerencias emergentes para crear una regla de evento y buscar vídeos que puedan activarla. El funcionamiento es similar al de la función Dual-VCA.</li> <li>• Haga clic para  ejecutar la función AcuSearch. Consulte AcuSearch para obtener más información.</li> <li>• Haga clic en  / para  mostrar vídeos que contienen imágenes de personas. vehículo.</li> </ul> <p> Nota</p> <p>Para usar esta función, asegúrese de haber configurado el Objetivo de detección como Humano o Vehículo para ciertos tipos de eventos. • Haga clic en  Seleccione canales y configure la hora de inicio y finalización para recortar el video en los canales seleccionados dentro de un periodo de tiempo específico. • Haga clic en  para configurar la estrategia de reproducción de video normal y video inteligente (el video que contiene datos inteligentes).</p>

## 12.2 Reproducción normal

Reproduce videos de un canal. En algunos dispositivos, se puede permitir la reproducción sincronizada de varios canales.

### Pasos

1. Vaya a Reproducción → 
2. Seleccione el/los canal(es) en la lista del lado izquierdo.



Nota

Reproducción de grupo: seleccione un grupo de la lista y se podrán reproducir los canales del grupo.

3. Seleccione una fecha en el calendario.




Nota

El triángulo azul en la esquina de la fecha del calendario indica que hay videos disponibles.

4. Opcional: Realizar más operaciones.

Captura  Haga clic para capturar imágenes durante la reproducción.

Zoom digital Haga clic para  ampliar una parte determinada de la imagen de vídeo.



Haz clic para añadir una etiqueta al canal. Después de añadirla, puedes ir a Copia de seguridad → Por etiqueta para buscar vídeos por etiqueta.



Haz clic para bloquear el video. Una vez bloqueado, no se sobrescribirá.

Después de bloquear, puede ir a Copia de seguridad → Por etiqueta para buscar videos por bloqueo.

VCA dual

Selecciona → VCA dual para buscar vídeos que puedan activar la regla de evento correspondiente. Consulte los pasos de configuración de eventos para obtener más información sobre cada tipo de evento.



Nota

Para utilizar esta función, vaya a Configuración → Acceso al dispositivo → Configuración del dispositivo → Parámetros del dispositivo → Información de pantalla en Scream para activar Habilitar VCA dual a través del navegador web y vaya a Sistema → Administración de almacenamiento → Configuración avanzada para activar Guardar datos VCA de la cámara a través de la interfaz GUI local.

Mostrar VCA

Información

Puede seleccionar Mostrar información de VCA para mostrar los marcos de reglas.

Desactivar

Si la protección de privacidad está activada, la imagen puede contener mosaicos. Puede seleccionar →

Privacidad

Mostrar protección de privacidad para ver el vídeo original (sin mosaicos) si el permiso de almacenamiento de la protección de privacidad también está activado.

Protección

Consulte Configurar protección de privacidad para obtener detalles sobre la función de protección de privacidad.

### 12.3 Reproducción de eventos

Cuando selecciona el modo de reproducción de eventos, el sistema analizará y marcará los videos que contienen información de detección de movimiento, detección de cruce de línea o detección de intrusión.

Antes de empezar

- Asegúrese de que la cámara tenga habilitado el VCA dual. Puede habilitarlo a través del navegador web de la cámara.

Interfaz en Configuración → Vídeo/Audio → Información de visualización en Stream .

- Asegúrese de que su grabadora de video tenga habilitada la opción Guardar datos VCA de la cámara en Administración de almacenamiento → Configuración avanzada .

Pasos

1. Seleccione Reproducción →
2. Seleccione una fecha en el calendario.



Nota


El triángulo azul en la esquina de la fecha del calendario indica que hay videos disponibles.

3. Haga clic  → VCA dual en la esquina inferior derecha de la imagen de reproducción para seleccionar un tipo de evento. Consulte

Los pasos de configuración del evento para obtener detalles de cada tipo de evento.

4. Haga clic en Buscar.

Los videos que cumplan con el requisito de la regla de detección se marcarán en rojo.

5. Haga clic  para configurar la reproducción de video normal y video inteligente (el video que contiene datos inteligentes) estrategia.



Nota


Si no se utiliza Dual-VCA , los segmentos rojos en la barra de progreso significan que los videos inteligentes son generados por el evento original.

---

### 12.4 Reproducción de cortes

Divida el vídeo en partes y reproduzcalas.

Pasos

1. Vaya a Reproducción → . 
2. Seleccione una cámara de la lista de cámaras.
3. Seleccione una fecha en el calendario.
4. Haga clic en Buscar.


El vídeo recuperado se dividirá en fragmentos de una hora para su reproducción.

5. Opcional: seleccione un segmento de una hora y haga clic en  dividirlo en fragmentos de un minuto para su reproducción.

### 12.5 Reproducción de subperíodos

Los archivos de vídeo se pueden reproducir en varios subperíodos simultáneamente en la pantalla.

Pasos

1. Vaya a Reproducción → . 
2. Seleccione una cámara.
3. Establezca la hora de inicio y la hora de finalización.
4. Haga clic en Buscar.

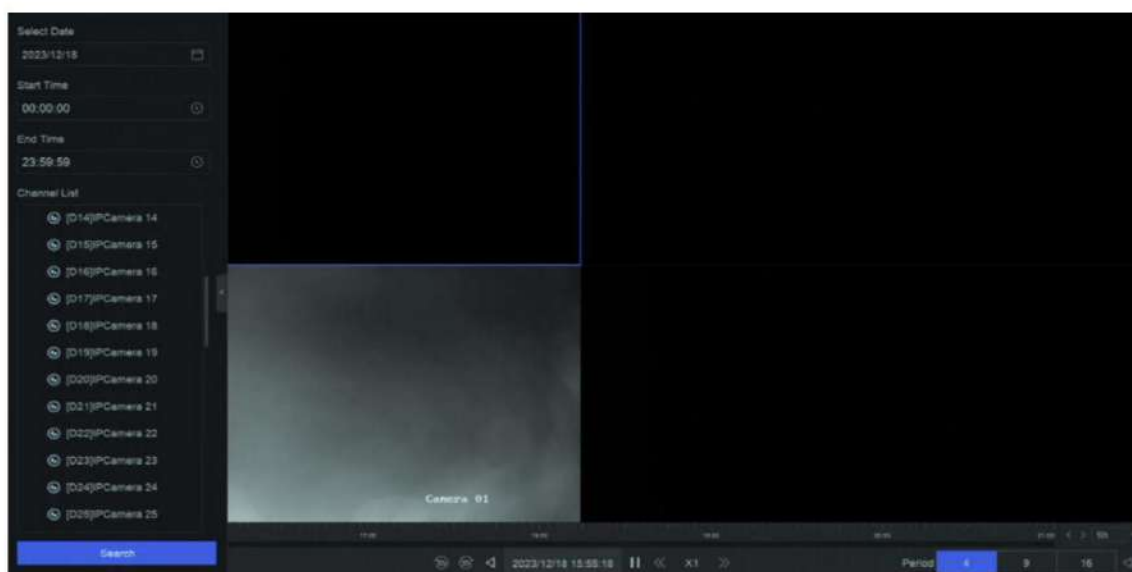


Figura 12-2 Reproducción de subperíodos

5. Seleccione el período en la esquina inferior derecha, por ejemplo, 4.



#### Nota

Según el número definido de pantallas divididas, los archivos de video de la fecha seleccionada se pueden dividir en segmentos promedio para su reproducción. Por ejemplo, si hay archivos de video entre las 16:00 y las 22:00, y se selecciona el modo de visualización en 6 pantallas, se pueden reproducir simultáneamente durante una hora en cada pantalla.

---

## Capítulo 13 Centro de eventos

### 13.1 Configuración de eventos

#### 13.1.1 Evento básico/genérico

##### Pasos


1. Vaya a Centro de eventos →  Configuración de eventos → Evento básico / Evento genérico .
2. Seleccione un canal.
3. Seleccione un tipo de evento.
4. Activar Habilitar.
5. Haga clic en Configuración de reglas para establecer la regla.

Tabla 13-1 Evento normal

Nombre del evento	Descripción del evento	Configuración de reglas	
Movimiento Detección	La detección de movimiento detecta los objetos en movimiento en el área monitoreada.	<p>Utilice la barra de herramientas en la parte superior de la imagen para dibujar el área de detección.</p> <ul style="list-style-type: none"> <li>• IA por NVR: El NVR analizará los eventos de detección de movimiento. El dispositivo puede analizar videos que contengan personas y vehículos.</li> </ul> <p>Solo el objetivo del tipo seleccionado (humano o vehículo) activará las alarmas, lo que puede reducir las falsas alarmas causadas por otros objetos. • IA por cámara: La</p> <p>El evento de detección de movimiento será analizado por cámara.</p> <ul style="list-style-type: none"> <li>• Objetivo de detección: Se pueden seleccionar humanos y vehículos , además de falsas alarmas, solo el</li> </ul>	La sensibilidad permite calibrar la facilidad con la que el movimiento puede activar la alarma. Un valor más alto aumenta la facilidad con la que se activa la detección de movimiento.

Nombre del evento	Descripción del evento	Configuración de reglas	
		Los objetivos seleccionados pueden activar alarmas.	
Video Manipulación Detección	La detección de manipulación de video activa una alarma cuando se cubre la lente de la cámara y toma medidas de respuesta de alarma.	Utilice la barra de herramientas en la parte superior de la imagen para dibujar el área de detección.	
Pérdida de vídeo Detección	La detección de pérdida de video detecta la pérdida de video de un canal y toma medidas de respuesta de alarma.	-	
Audio Excepción Detección	La detección de excepciones de audio detecta sonidos anormales en la escena, como un aumento o disminución repentino en la intensidad del sonido.	-	
Desenfoque Detección	Se puede detectar el desenfoque de la imagen causado por el desenfoque de la lente.	-	
Repentino Escena Cambiar Detección	La detección de cambio de escena detecta el cambio del entorno de seguridad de video afectado por factores externos, como la rotación intencional de la cámara.	-	

6. Haga clic en Programación de armado para seleccionar un tipo de programación de armado.




Nota

Si configura el Programa de armado como Personalizado, puede arrastrar el cursor sobre la barra de tiempo para configurar un programa de armado personalizado o mover el cursor sobre la barra de tiempo y **00:00-24:00** para establecer una hora específica hacer clic en programar.

7. Haga clic en Método de vinculación para configurar los métodos de vinculación.



Tabla 13-2 Descripción del método de vinculación

Método de vinculación	Descripción
Notificar a Vigilancia Centro	El dispositivo puede enviar una señal de excepción o alarma al host de alarma remoto cuando ocurre un evento. El host de alarma se refiere al PC con el software cliente instalado (p. ej., iVMS-4200, iVMS-5200).
Ventana emergente de alarma	Cuando se activa una alarma, el monitor local muestra la alarma ventana emergente.
Zumbador	Cuando se detecta una alarma, el zumbador emitirá un pitido audible.
Enviar correo electrónico	El sistema puede enviar un correo electrónico con información de alarma a uno o más usuarios cuando se detecta una alarma.
Salida de alarma	La salida de alarma puede activarse mediante la entrada de alarma, detección de movimiento, detección de manipulación de video, detección de rostro, detección de cruce de línea y cualquier otro evento.
Registro	<p>Cuando se detecta una alarma, el canal seleccionado grabará videos.</p> <p> <b>Nota</b></p> <p>La programación de grabación de video debe estar habilitada para el canal; de lo contrario, la vinculación no será válida. Puede configurar la programación de grabación de video en Sistema → Administración de almacenamiento → Programación de almacenamiento → Grabación de video .</p>

8. Haga clic en Guardar.

### 13.1.2 Protección perimetral

Los eventos de protección perimetral incluyen detección de cruce de línea, detección de intrusión, detección de ingreso a la región y detección de salida de la región.

#### Configurar la detección de cruce de línea

La detección de cruce de línea detecta personas, vehículos y objetos que cruzan una línea virtual definida. La dirección de detección puede configurarse como bidireccional, de izquierda a derecha o de derecha a izquierda.

##### Pasos



**Nota**

Una parte de los siguientes pasos solo están disponibles para ciertos modelos de NVR o cámaras.

1. Vaya a Centro de eventos →  Configuración de eventos → Protección perimetral.

2. Seleccione una cámara.
3. Opcional: Activar el análisis secundario. El motor del dispositivo correspondiente analizará este evento por segunda vez para reducir las falsas alarmas.



Nota

Al menos un motor del dispositivo debe ejecutar el algoritmo de Análisis secundario para protección perimetral . Puede hacer clic en Asignar motor en el lado derecho para asignar el motor rápidamente, o ir a Sistema → Configuraciones inteligentes → Configuración de algoritmo → Administración de algoritmo para habilitar el algoritmo de Análisis secundario para protección perimetral .

4. Opcional: Activa la IA por NVR. El motor del dispositivo correspondiente analizará el video y... Las cámaras solo transmiten flujo de video.



Nota

Al menos un motor del dispositivo debe ejecutar el algoritmo de Protección Perimetral . Puede hacer clic en "Asignar motor" a la derecha para asignarlo rápidamente o ir a Sistema → Configuración inteligente → Configuración del algoritmo → Administración del algoritmo para habilitar el algoritmo de Protección Perimetral .

5. Seleccione Cruce de línea.
6. Activar Habilitar.

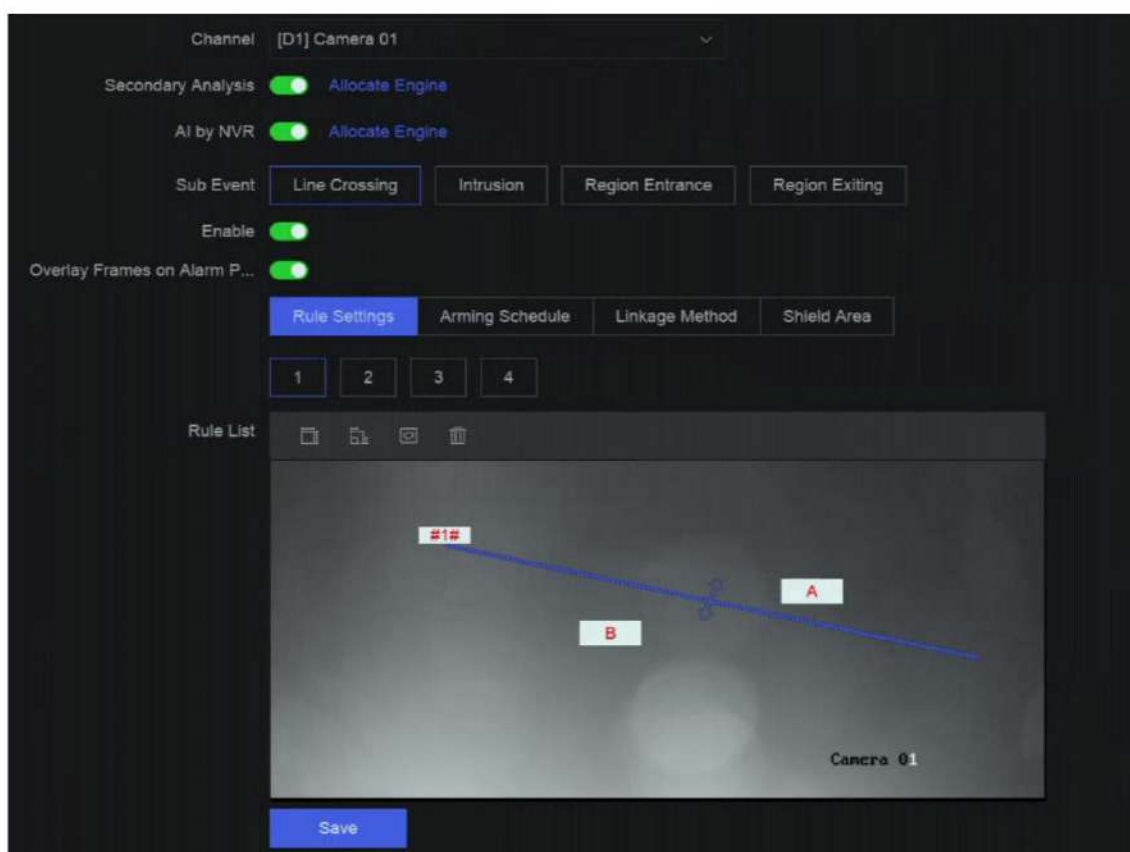



Figura 13-1 Detección de cruce de línea

7. Haga clic en Configuración de reglas para detectar reglas.

1) Seleccione un número de regla. Por ejemplo, seleccione 1.

2) Haga  , y haga clic en la imagen dos veces respectivamente para dibujar el punto de inicio y el punto final de clic en la línea de detección.

3) Establecer dirección, sensibilidad, objetivo de detección y confianza del objetivo.

A<->B

Solo se muestra la flecha en el lado B. Cuando un objeto cruza la línea configurada en ambas direcciones, se puede detectar y se activan las alarmas.

A->B

Sólo se puede detectar el objeto que cruza la línea configurada desde el lado A al lado B.

B->A

Sólo se puede detectar el objeto que cruza la línea configurada desde el lado B al lado A.

Sensibilidad

Cuanto mayor sea el valor, más fácilmente se podrá activar la alarma de detección.


Objetivo de detección

Seleccione el objetivo de detección como humano o vehículo para descartar las alarmas que no se activan por personas o vehículos. El objetivo de detección solo está disponible para ciertos modelos.

Confianza en el objetivo

Se utiliza para indicar el nivel de certeza o confiabilidad en la detección de eventos de cruce de línea.

Establecer niveles de confianza más altos garantiza que solo las detecciones altamente confiables activen eventos, lo que reduce las falsas alarmas.


4) Opcional: Haga clic en  para dibujar el tamaño máximo o mínimo. Solo los objetivos que cumplen con el tamaño . El requisito puede activar alarmas.

5) Opcional: Repita los pasos anteriores para dibujar más reglas. Se admiten hasta 4 reglas.

8. Haga clic en Programación de armado para seleccionar un tipo de programación de armado.




Nota

Si configura el Programa de armado como Personalizado, puede arrastrar el cursor sobre la barra de tiempo para configurar un programa de armado personalizado o mover el cursor sobre la barra de tiempo y  para establecer una hora específica hacer clic en programar.

9. Haga clic en Método de vinculación para configurar los métodos de vinculación.

Tabla 13-3 Descripción del método de vinculación

Método de vinculación	Descripción
Notificar a Vigilancia Centro	El dispositivo puede enviar una señal de excepción o alarma al host de alarma remoto cuando ocurre un evento. El host de alarma se refiere al PC con el software cliente instalado (p. ej., iVMS-4200, iVMS-5200).
Ventana emergente de alarma	Cuando se activa una alarma, el monitor local muestra la alarma ventana emergente.

Método de vinculación	Descripción
Zumbador	Cuando se detecta una alarma, el zumbador emitirá un pitido audible.
Enviar correo electrónico	El sistema puede enviar un correo electrónico con información de alarma a uno o más usuarios cuando se detecta una alarma.
Salida de alarma	La salida de alarma puede activarse mediante la entrada de alarma, detección de movimiento, detección de manipulación de video, detección de rostro, detección de cruce de línea y cualquier otro evento.
Registro	<p>Cuando se detecta una alarma, el canal seleccionado grabará videos.</p> <p> <b>Nota</b></p> <p>La programación de grabación de video debe estar habilitada para el canal; de lo contrario, la vinculación no será válida. Puede configurar la programación de grabación de video en Sistema → Administración de almacenamiento → Programación de almacenamiento → Grabación de video .</p>

10. Opcional: Configure el Área de Protección cuando la IA por NVR esté habilitada. Una vez configurada el área de protección, el dispositivo no analizará el comportamiento del objetivo en el área, por lo que los eventos de protección perimetral no se activarán dentro del área.

11. Haga clic en Guardar.

Qué hacer a

continuación Puede ir a Vista en vivo y hacer clic en Objetivo para ver las alarmas en tiempo real.

## Configurar la detección de intrusiones

La función de detección de intrusiones detecta personas, vehículos u otros objetos que entran y merodean en una zona virtual predefinida. Se pueden tomar medidas específicas cuando se activa una alarma.

Pasos



**Nota**

Una parte de los siguientes pasos solo están disponibles para ciertos modelos de NVR o cámaras.

1. Vaya a Centro de eventos → Configuración de eventos → Protección perimetral.
2. Seleccione una cámara.
3. Opcional: Activar el análisis secundario. El motor del dispositivo correspondiente analizará este evento. por segunda vez para reducir las falsas alarmas.



## Nota

Al menos un motor del dispositivo debe ejecutar el algoritmo de Análisis secundario para protección perimetral .

Puede hacer clic en Asignar motor en el lado derecho para asignar el motor rápidamente, o ir a Sistema → Configuraciones inteligentes → Configuración de algoritmo → Administración de algoritmo para habilitar el algoritmo de Análisis secundario para protección perimetral .

4. Opcional: Activa la IA por NVR. El motor del dispositivo correspondiente analizará el video y...

Las cámaras solo transmiten flujo de video.



## Nota

Al menos un motor del dispositivo debe ejecutar el algoritmo de Protección Perimetral . Puede hacer clic en "Asignar motor" a la derecha para asignarlo rápidamente o ir a Sistema → Configuración inteligente → Configuración del algoritmo → Administración del algoritmo para habilitar el algoritmo de Protección Perimetral .

5. Seleccione Intrusión.

6. Activar Habilitar.

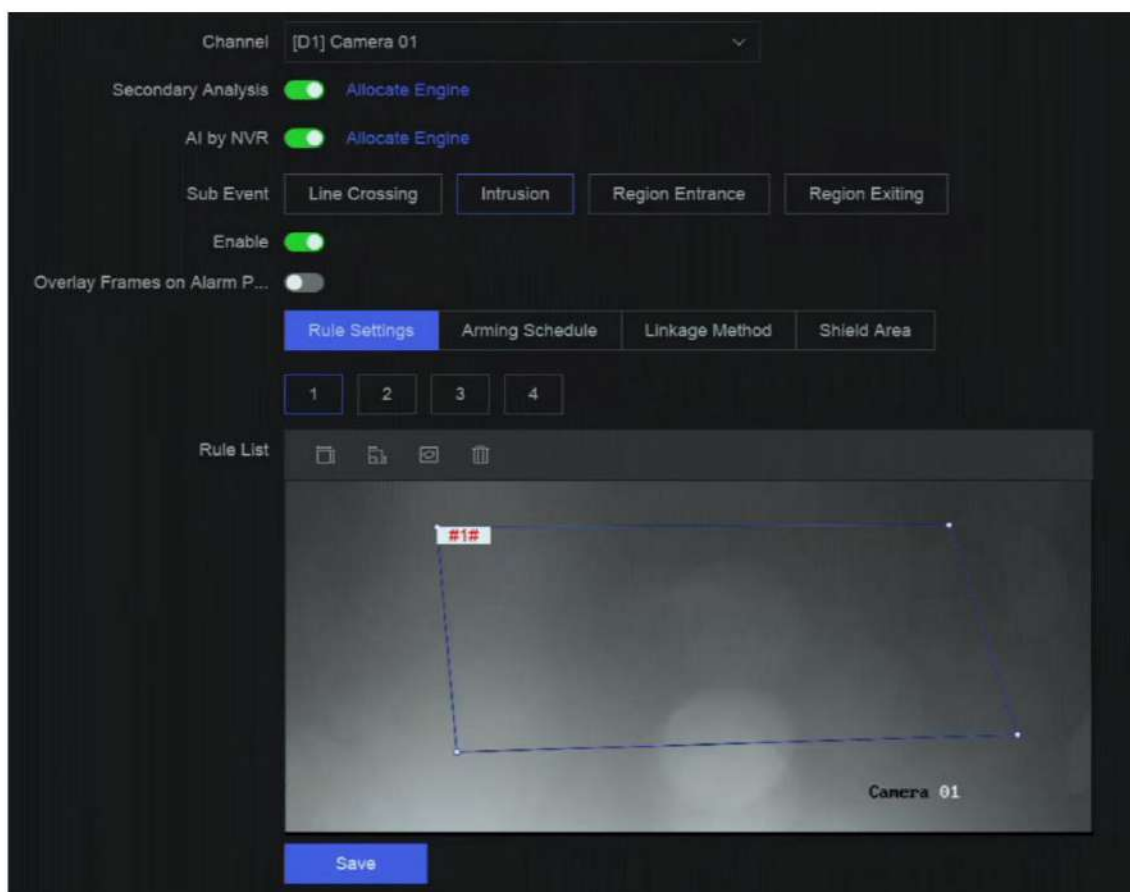



Figura 13-2 Detección de intrusiones

7. Haga clic en Configuración de reglas para detectar reglas.

- 1) Seleccione un número de regla. Por ejemplo, seleccione 1.

2) Haga  , y haga clic en la imagen 4 veces respectivamente para dibujar cada punto de un cuadrilátero o clic en el área decagonal.

3) Establezca el umbral de tiempo, la sensibilidad, el objetivo de detección y la confianza del objetivo.

### Umbral de tiempo

El tiempo que un objeto permanece en la zona. Cuando el tiempo que el objeto permanece en el área de detección definida supera el umbral, el dispositivo activará una alarma.

### Sensibilidad


Cuanto mayor sea el valor, más fácilmente se podrá activar la alarma de detección.

### Objetivo de detección

Seleccione el objetivo de detección como humano o vehículo para descartar las alarmas que no se activan por personas o vehículos. El objetivo de detección solo está disponible para ciertos modelos.

### Confianza en el objetivo

Se utiliza para indicar el nivel de certeza o fiabilidad en la detección de eventos de intrusión. Establecer niveles de confianza más altos garantiza que solo las detecciones altamente fiables activen eventos, lo que reduce las falsas alarmas.

4) Opcional: Haga clic en  para dibujar el tamaño máximo o mínimo. Solo los objetivos que cumplen con el tamaño .


El requisito puede activar alarmas.

5) Opcional: Repita los pasos anteriores para dibujar más reglas. Se admiten hasta 4 reglas.

8. Haga clic en Programación de armado para seleccionar un tipo de programación de armado.




### Nota

Si configura el Programa de armado como Personalizado, puede arrastrar el cursor sobre la barra de tiempo para configurar un programa de armado personalizado o mover el cursor sobre la barra de tiempo y  para establecer una hora específica hacer clic en programar.

9. Haga clic en Método de vinculación para configurar los métodos de vinculación.

Tabla 13-4 Descripción del método de vinculación

Método de vinculación	Descripción
Notificar a Vigilancia Centro	El dispositivo puede enviar una señal de excepción o alarma al host de alarma remoto cuando ocurre un evento. El host de alarma se refiere al PC con el software cliente instalado (p. ej., iVMS-4200, iVMS-5200).
Ventana emergente de alarma	Cuando se activa una alarma, el monitor local muestra la alarma ventana emergente.
Zumbador	Cuando se detecta una alarma, el zumbador emitirá un pitido audible.
Enviar correo electrónico	El sistema puede enviar un correo electrónico con información de alarma a uno o más usuarios cuando se detecta una alarma.

Método de vinculación	Descripción
Salida de alarma	La salida de alarma puede activarse mediante la entrada de alarma, detección de movimiento, detección de manipulación de video, detección de rostro, detección de cruce de línea y cualquier otro evento.
Registro	<p>Cuando se detecta una alarma, el canal seleccionado grabará videos.</p> <p> <b>Nota</b></p> <p>La programación de grabación de video debe estar habilitada para el canal; de lo contrario, la vinculación no será válida. Puede configurar la programación de grabación de video en Sistema → Administración de almacenamiento → Programación de almacenamiento → Grabación de video .</p>

10. Opcional: Configure el Área de Protección cuando la IA por NVR esté habilitada. Una vez configurada el área de protección, el dispositivo no analizará el comportamiento del objetivo en el área, por lo que los eventos de protección perimetral no se activarán dentro del área.

11. Haga clic en Guardar.

Qué hacer a

continuación Puede ir a Vista en vivo y hacer clic en Objetivo para ver las alarmas en tiempo real.

## Configurar la detección de entrada a la región

La detección de entrada a la región detecta objetos que ingresan a una región virtual predefinida.

Pasos



**Nota**

Una parte de los siguientes pasos solo están disponibles para ciertos modelos de NVR o cámaras.

1. Vaya a Centro de eventos → Configuración de eventos → Protección perimetral.
2. Seleccione una cámara.
3. Opcional: Activar el análisis secundario. El motor del dispositivo correspondiente analizará este evento. por segunda vez para reducir las falsas alarmas.



**Nota**

Al menos un motor del dispositivo debe ejecutar el algoritmo de Análisis secundario para protección perimetral .

Puede hacer clic en Asignar motor en el lado derecho para asignar el motor rápidamente, o ir a Sistema → Configuraciones inteligentes → Configuración de algoritmo → Administración de algoritmo para habilitar el algoritmo de Análisis secundario para protección perimetral .

4. Opcional: Activa la IA por NVR. El motor del dispositivo correspondiente analizará el video y...  
Las cámaras solo transmiten flujo de video.



Nota

Al menos un motor del dispositivo debe ejecutar el algoritmo de Protección Perimetral . Puede hacer clic en "Asignar motor" a la derecha para asignarlo rápidamente o ir a Sistema → Configuración inteligente → Configuración del algoritmo → Administración del algoritmo para habilitar el algoritmo de Protección Perimetral .

5. Seleccione Entrada Región.

6. Activar Habilitar.

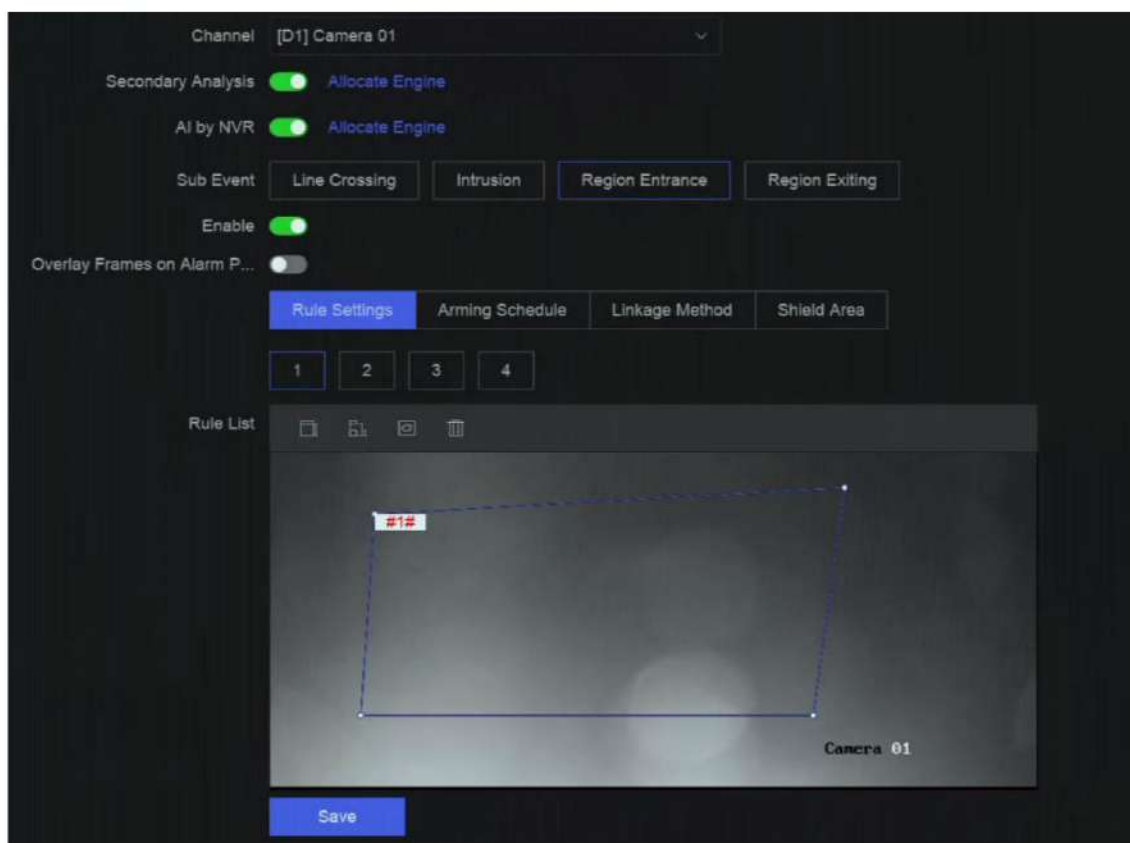


Figura 13-3 Detección de entrada a la región

7. Haga clic en Configuración de reglas para detectar reglas.

1) Seleccione un número de regla. Por ejemplo, seleccione 1.

2) Haga clic y haga clic en la imagen 4 veces respectivamente para dibujar cada punto de un área cuadrilátera o decagonal.

3) Establezca la sensibilidad, el objetivo de detección y la confianza del objetivo.

Sensibilidad

Cuanto mayor sea el valor, más fácilmente se podrá activar la alarma de detección.

Objetivo de detección

Seleccione el objetivo de detección como humano o vehículo para descartar las alarmas que no se activan por personas o vehículos. El objetivo de detección solo está disponible para ciertos modelos.



## Confianza en el objetivo

Se utiliza para indicar el nivel de certeza o confiabilidad en la detección de eventos de entrada a la región.

Establecer niveles de confianza más altos garantiza que solo las detecciones altamente confiables activen eventos, lo que reduce las falsas alarmas.

4) Opcional: Repita los pasos anteriores para dibujar más reglas. Se admiten hasta 4 reglas.

8. Haga clic en Programación de armado para seleccionar un tipo de programación de armado.



Nota

Si configura el Programa de armado como Personalizado, puede arrastrar el cursor sobre la barra de tiempo para configurar un

programa de armado personalizado o mover el cursor sobre la barra de tiempo y

00:00-24:00




para establecer una hora específica

hacer clic en programar.

9. Haga clic en Método de vinculación para configurar los métodos de vinculación.

Tabla 13-5 Descripción del método de vinculación

Método de vinculación	Descripción
Notificar a Vigilancia Centro	El dispositivo puede enviar una señal de excepción o alarma al host de alarma remoto cuando ocurre un evento. El host de alarma se refiere al PC con el software cliente instalado (p. ej., iVMS-4200, iVMS-5200).
Ventana emergente de alarma	Cuando se activa una alarma, el monitor local muestra la alarma ventana emergente.
Zumbador	Cuando se detecta una alarma, el zumbador emitirá un pitido audible.
Enviar correo electrónico	El sistema puede enviar un correo electrónico con información de alarma a uno o más usuarios cuando se detecta una alarma.
Salida de alarma	La salida de alarma puede activarse mediante la entrada de alarma, detección de movimiento, detección de manipulación de video, detección de rostro, detección de cruce de línea y cualquier otro evento.
Registro	<p>Cuando se detecta una alarma, el canal seleccionado grabará videos.</p> <p> Nota</p> <p>La programación de grabación de video debe estar habilitada para el canal; de lo contrario, la vinculación no será válida. Puede configurar la programación de grabación de video en Sistema → Administración de almacenamiento → Programación de almacenamiento → Grabación de video .</p>

10. Opcional: Configure el Área de Protección cuando la IA por NVR esté habilitada. Una vez configurada el área de protección, el dispositivo no analizará el comportamiento del objetivo en el área, por lo que los eventos de protección perimetral no se activarán dentro del área.

11. Haga clic en Guardar.

Qué hacer a

continuación Puede ir a Vista en vivo y hacer clic en Objetivo para ver las alarmas en tiempo real.

### Configurar la detección de salida de la región

La detección de salida de región detecta objetos que salen de una región virtual predefinida.

#### Pasos


---



Nota

Una parte de los siguientes pasos solo están disponibles para ciertos modelos de NVR o cámaras.

---

1. Vaya a Centro de eventos →  Configuración de eventos → Protección perimetral.
  2. Seleccione una cámara.
  3. Opcional: Activar el análisis secundario. El motor del dispositivo correspondiente analizará este evento.  
por segunda vez para reducir las falsas alarmas.
- 



Nota

Al menos un motor del dispositivo debe ejecutar el algoritmo de Análisis secundario para protección perimetral .

Puede hacer clic en Asignar motor en el lado derecho para asignar el motor rápidamente, o ir a Sistema → Configuraciones inteligentes → Configuración de algoritmo → Administración de algoritmo para habilitar el algoritmo de Análisis secundario para protección perimetral .

---

4. Opcional: Activa la IA por NVR. El motor del dispositivo correspondiente analizará el video y...  
Las cámaras solo transmiten flujo de video.
- 



Nota

Al menos un motor del dispositivo debe ejecutar el algoritmo de Protección Perimetral . Puede hacer clic en "Asignar motor" a la derecha para asignarlo rápidamente o ir a Sistema → Configuración inteligente → Configuración del algoritmo → Administración del algoritmo para habilitar el algoritmo de Protección Perimetral .

---

5. Seleccione Región Saliendo.
6. Activar Habilitar.

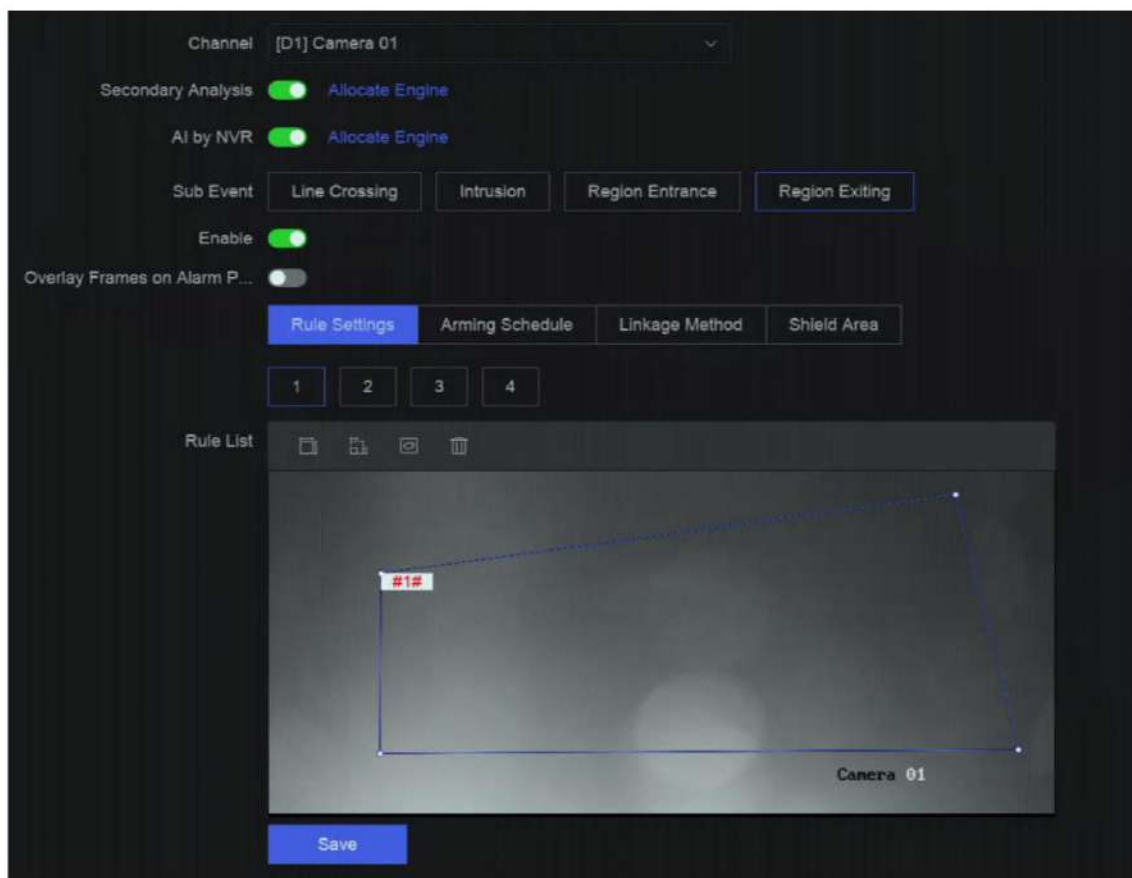


Figura 13-4 Región que sale de la detección 7. Haga clic

en Configuración de reglas para configurar las reglas de detección.

- 1) Seleccione un número de regla. Por ejemplo, seleccione 1.
- 2) Haga clic en la imagen 4 veces respectivamente para dibujar cada punto de un área cuadrilátera o decagonal.

- 3) Establezca la sensibilidad, el objetivo de detección y la confianza del objetivo.

#### Sensibilidad

Cuanto mayor sea el valor, más fácilmente se podrá activar la alarma de detección.

#### Objetivo de detección

Seleccione el objetivo de detección como humano o vehículo para descartar las alarmas que no se activan por personas o vehículos. El objetivo de detección solo está disponible para ciertos modelos.

#### Confianza en el objetivo

Se utiliza para indicar el nivel de certeza o confiabilidad en la detección de eventos de salida de la región.


Establecer niveles de confianza más altos garantiza que solo las detecciones altamente confiables activen eventos, lo que reduce las falsas alarmas.

- 4) Opcional: Repita los pasos anteriores para dibujar más reglas. Se admiten hasta 4 reglas.

8. Haga clic en Programación de armado para seleccionar un tipo de programación de armado.




## Nota

Si configura el Programa de armado como Personalizado, puede arrastrar el cursor sobre la barra de tiempo para configurar un programa de armado personalizado o mover el cursor sobre la barra de tiempo y  para establecer una hora específica hacer clic en programar.

9. Haga clic en Método de vinculación para configurar los métodos de vinculación.

Tabla 13-6 Descripción del método de vinculación

Método de vinculación	Descripción
Notificar a Vigilancia Centro	El dispositivo puede enviar una señal de excepción o alarma al host de alarma remoto cuando ocurre un evento. El host de alarma se refiere al PC con el software cliente instalado (p. ej., iVMS-4200, iVMS-5200).
Ventana emergente de alarma	Cuando se activa una alarma, el monitor local muestra la alarma ventana emergente.
Zumbador	Cuando se detecta una alarma, el zumbador emitirá un pitido audible.
Enviar correo electrónico	El sistema puede enviar un correo electrónico con información de alarma a uno o más usuarios cuando se detecta una alarma.
Salida de alarma	La salida de alarma puede activarse mediante la entrada de alarma, detección de movimiento, detección de manipulación de video, detección de rostro, detección de cruce de línea y cualquier otro evento.
Registro	<p>Cuando se detecta una alarma, el canal seleccionado grabará videos.</p> <p> Nota</p> <p>La programación de grabación de video debe estar habilitada para el canal; de lo contrario, la vinculación no será válida. Puede configurar la programación de grabación de video en Sistema → Administración de almacenamiento → Programación de almacenamiento → Grabación de video .</p>

10. Opcional: Configure el Área de Protección cuando la IA por NVR esté habilitada. Una vez configurada el área de protección, el dispositivo no analizará el comportamiento del objetivo en el área, por lo que los eventos de protección perimetral no se activarán dentro del área.

11. Haga clic en Guardar.

Qué hacer a continuación

Puede ir a Vista en vivo y hacer clic en Objetivo para ver las alarmas en tiempo real.

### 13.1.3 Evento de comportamiento anormal

Antes de comenzar

Asegúrese de que la cámara admita esta función.

Pasos

1. Vaya a Centro de eventos → Configuración de eventos → Evento de comportamiento anormal .
2. Seleccione una cámara.
3. Seleccione un tipo de evento.
4. Activar Habilitar.
5. Haga clic en Configuración de reglas para establecer la regla.

Tabla 13-7 Eventos de comportamiento anormal

Nombre del evento	Descripción del evento	Configuración de reglas
Merodeando Detección	La detección de merodeo se utiliza para detectar si un objetivo permanece dentro de un área específica durante más tiempo que el tiempo establecido y activar la alarma para las acciones vinculadas.	<p>a. Seleccione un número de regla.</p> <p>b. Utilice la barra de herramientas en la parte superior de la imagen para dibujar la línea de detección.</p> <p>c. Establecer umbral de tiempo y sensibilidad.</p> <p>Umbral de tiempo</p> <p>Tiempo que el objetivo permanece en la región. Si el valor es 10, se activa una alarma después de que el objetivo permanezca en la región durante 10 s. Rango: [1-10].</p> <p>Sensibilidad:</p> <p>Similitud de la imagen de fondo con el objeto. Cuanto mayor sea el valor, más fácilmente se activará la alarma de detección. d. Opcional: Repita los pasos anteriores para configurar otro.</p>
Aparcamiento Detección	La detección de estacionamiento se utiliza para detectar violaciones de estacionamiento en el área, aplicable en autopistas y calles de un solo sentido.	
Desesperado equipaje Detección	La detección de equipaje desatendido detecta los objetos abandonados en una región predefinida, como equipaje, carteras, materiales peligrosos, etc., y se pueden tomar una serie de acciones cuando se activa la alarma.	
Objeto Eliminación Detección	La función de detección de eliminación de objetos detecta los objetos eliminados de una región predefinida, como las exhibiciones en exhibición, y se pueden tomar una serie de acciones cuando se activa la alarma.	
Movimiento rápido Detección	La detección de movimiento rápido se utiliza para detectar carreras y persecuciones sospechosas, exceso de velocidad y movimientos rápidos. Activará una alarma cuando un objeto se mueva rápidamente y enviará una notificación al host de armado para que...	

Nombre del evento	Descripción del evento	Configuración de reglas
	que se puedan tomar con antelación las medidas necesarias.	
Gente Reunión Detección	La detección de reuniones de personas se utiliza para detectar si la densidad de cuerpos humanos dentro de un área específica excede el valor establecido y activa la alarma para las acciones vinculadas.	a. Seleccione un número de regla. b. Use la barra de herramientas en la parte superior de la imagen para dibujar la línea de detección. c. Establezca el porcentaje. El porcentaje representa la densidad de cuerpos humanos dentro del área. Si supera el valor umbral, el dispositivo activará la alarma.  d. Opcional: repita los pasos anteriores para configurar otro.

6. Haga clic en Programación de armado para seleccionar un tipo de programación de armado.




#### Nota

Si configura el Programa de armado como Personalizado, puede arrastrar el cursor sobre la barra de tiempo para configurar un programa de armado personalizado o mover el cursor sobre la barra de tiempo y **00:00-24:00** para establecer una hora específica hacer clic en programar.

7. Haga clic en Método de vinculación para configurar los métodos de vinculación.

Tabla 13-8 Descripción del método de vinculación

Método de vinculación	Descripción
Notificar a Vigilancia Centro	El dispositivo puede enviar una señal de excepción o alarma al host de alarma remoto cuando ocurre un evento. El host de alarma se refiere al PC con el software cliente instalado (p. ej., iVMS-4200, iVMS-5200).
Ventana emergente de alarma	Cuando se activa una alarma, el monitor local muestra la alarma ventana emergente.
Zumbador	Cuando se detecta una alarma, el zumbador emitirá un pitido audible.
Enviar correo electrónico	El sistema puede enviar un correo electrónico con información de alarma a uno o más usuarios cuando se detecta una alarma.
Salida de alarma	La salida de alarma puede activarse mediante la entrada de alarma, detección de movimiento, detección de manipulación de video, detección de rostro, detección de cruce de línea y cualquier otro evento.
Registro	Cuando se detecta una alarma, el canal seleccionado grabará videos.

Método de vinculación	Descripción
	 Nota <p>La programación de grabación de video debe estar habilitada para el canal; de lo contrario, la vinculación no será válida. Puede configurar la programación de grabación de video en Sistema → Administración de almacenamiento → Programación de almacenamiento → Grabación de video .</p>


8. Haga clic en Guardar.

### 13.1.4 Evento objetivo

Antes de comenzar

Asegúrese de que la cámara conectada admita esta función o que el motor del dispositivo haya habilitado el algoritmo de Reconocimiento de objetivos o Estructuración de video en Centro de eventos → Configuración de eventos → Configuraciones inteligentes → Configuración de algoritmo → Administración de algoritmos .

Pasos

1. Vaya a Centro de eventos →  Configuración de eventos → Evento de destino .
2. Seleccione una cámara.
3. Seleccione un evento.
4. Activar Habilitar.
5. Establecer reglas para el evento.

Nombre del evento	Descripción del evento	Configuración de reglas
Captura de Rostros:	La captura de rostros detecta y captura los rostros que aparecen en la escena. Se pueden activar acciones de vinculación al detectar un rostro humano.	-
Imagen de la cara Comparación	La función compara las imágenes de rostros detectados con la biblioteca de listas especificada. Se activa una alarma cuando la comparación es exitosa.	<ul style="list-style-type: none"> <li>• Admite la configuración de la calificación de objetivos. Cara La comparación de imágenes comienza cuando el grado del objetivo cumple con los requisitos de comparación (la distancia entre pupilas es mayor que el umbral configurado y el ángulo de inclinación y el ángulo de panorámica son menores que los umbrales configurados).</li> <li>• Admite la configuración de avisos para errores y comparaciones sucesivas.</li> </ul>

Nombre del evento	Descripción del evento	Configuración de reglas
Extraño Detección	Las caras que no estén en la lista de la biblioteca y que aparezcan en el vídeo se identificarán como extraños.	<ul style="list-style-type: none"> <li>• Admite la configuración de la calificación de objetivos. Cara La comparación de imágenes comienza cuando el grado del objetivo cumple con los requisitos de comparación (la distancia de la pupila es mayor que el umbral configurado y el ángulo de inclinación y el ángulo de panorámica son menores que los umbrales configurados).</li> <li>• Admite la configuración de la solicitud para Detectar extraños.</li> </ul>
Objetivo múltiple Tipo Detección	La detección de múltiples objetivos permite que el dispositivo detecte rostros, cuerpos humanos y vehículos simultáneamente en un escena.	-

6. Haga clic en Programación de armado para seleccionar un tipo de programación de armado.



Nota


Si configura el Programa de armado como Personalizado, puede arrastrar el cursor sobre la barra de tiempo para configurar un programa de armado personalizado o mover el cursor sobre la barra de tiempo y **00:00-24:00** para establecer una hora específica hacer clic en programar.

7. Haga clic en Método de vinculación para configurar los métodos de vinculación.

Tabla 13-9 Descripción del método de vinculación

Método de vinculación	Descripción
Notificar a Vigilancia Centro	El dispositivo puede enviar una señal de excepción o alarma al host de alarma remoto cuando ocurre un evento. El host de alarma se refiere al PC con el software cliente instalado (p. ej., iVMS-4200, iVMS-5200).
Ventana emergente de alarma	Cuando se activa una alarma, el monitor local muestra la alarma ventana emergente.
Zumbador	Cuando se detecta una alarma, el zumbador emitirá un pitido audible.
Enviar correo electrónico	El sistema puede enviar un correo electrónico con información de alarma a uno o más usuarios cuando se detecta una alarma.
Salida de alarma	La salida de alarma puede activarse mediante la entrada de alarma, detección de movimiento, detección de manipulación de video, detección de rostro, detección de cruce de línea y cualquier otro evento.
Registro	Cuando se detecta una alarma, el canal seleccionado grabará videos.



Método de vinculación	Descripción
	 <b>Nota</b> La programación de grabación de video debe estar habilitada para el canal; de lo contrario, la vinculación no será válida. Puede configurar la programación de grabación de video en Sistema → Administración de almacenamiento → Programación de almacenamiento → Grabación de video .

8. Haga clic en Guardar.

### 13.1.5 Detección de cámara térmica

El NVR admite los modos de detección de eventos de las cámaras de red térmicas: detección de fuego y humo, detección de temperatura, detección de diferencia de temperatura, etc.

Antes de comenzar

Agregue la cámara de red térmica a su dispositivo y asegúrese de que la cámara esté activada.

Pasos


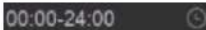
1. Vaya a Centro de eventos →  Configuración de eventos → Evento térmico .
2. Seleccione una cámara.
3. Seleccione un tipo de evento.
4. Activar Habilitar.
5. Haga clic en Configuración de reglas para establecer la regla.

Tabla 13-10 Eventos térmicos

Nombre del evento	Descripción del evento
Detección de incendios	Se activará una alarma cuando se detecte fuego en el área de armado.
Detección de temperatura	Se activará una alarma cuando la temperatura supere el valor umbral.
Protección perimetral	Los eventos de protección perimetral incluyen detección de cruce de línea, detección de intrusión, detección de ingreso a la región y detección de salida de la región.


6. Haga clic en Programación de armado para seleccionar un tipo de programación de armado.



Si configura el Programa de armado como Personalizado, puede arrastrar el cursor sobre la barra de tiempo para configurar un programa de armado personalizado o mover el cursor sobre la barra de tiempo y  para establecer una hora específica hacer clic en programar.

7. Haga clic en Método de vinculación para configurar los métodos de vinculación.

Tabla 13-11 Descripción del método de vinculación


Método de vinculación	Descripción
Notificar a Vigilancia Centro	El dispositivo puede enviar una señal de excepción o alarma al host de alarma remoto cuando ocurre un evento. El host de alarma se refiere al PC con el software cliente instalado (p. ej., iVMS-4200, iVMS-5200).
Ventana emergente de alarma	Cuando se activa una alarma, el monitor local muestra la alarma ventana emergente.
Zumbador	Cuando se detecta una alarma, el zumbador emitirá un pitido audible.
Enviar correo electrónico	El sistema puede enviar un correo electrónico con información de alarma a uno o más usuarios cuando se detecta una alarma.
Salida de alarma	La salida de alarma puede activarse mediante la entrada de alarma, detección de movimiento, detección de manipulación de video, detección de rostro, detección de cruce de línea y cualquier otro evento.
Registro	<p>Cuando se detecta una alarma, el canal seleccionado grabará videos.</p> <p> <b>Nota</b></p> <p>La programación de grabación de video debe estar habilitada para el canal; de lo contrario, la vinculación no será válida. Puede configurar la programación de grabación de video en Sistema → Administración de almacenamiento → Programación de almacenamiento → Grabación de video .</p>

8. Haga clic en Guardar.

### 13.1.6 Evento de entrada de alarma

Establecer la acción de manejo de una alarma de sensor externo.

#### Pasos

1. Vaya a Centro de eventos →  Configuración de eventos → Evento de entrada de alarma .
2. Seleccione un nombre de entrada de alarma.

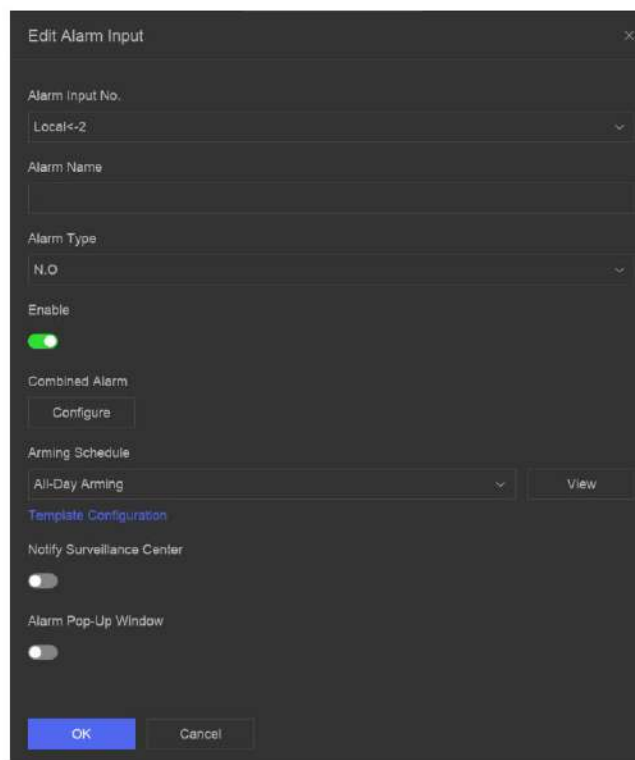


Figura 13-5 Configurar entrada de alarma



#### Nota

Por ejemplo, Local<-1 representa que el número de entrada de alarma en el panel trasero del dispositivo es 1.

---

3. Editar el nombre de la alarma.

4. Establecer el tipo de alarma.

NO

Cuando los contactos están en estado natural y sin energía, si dos contactos están apagados, entonces pueden llamarse normalmente abiertos.

CONTINUAR DEL SIGUIENTE

Cuando los contactos están en estado natural y sin energía, si se conducen dos contactos, entonces se pueden llamar normalmente cerrados.

5. Activar Habilitar.

6. Opcional: si selecciona Local<-1 en el Paso 2, seleccione el método de procesamiento.

- Seleccione la entrada de alarma de proceso y luego podrá configurar el programa de armado y la vinculación correspondientes. métodos, etc.



#### Nota

Las operaciones a continuación están todas disponibles cuando selecciona este método de procesamiento.

---

- Seleccione Desarme rápido y luego se deshabilitarán los métodos de vinculación de todos los eventos.

7. Haga clic en Configurar para configurar la alarma combinada.

1) Seleccione un canal.

2) Seleccione eventos de alarma combinados, como detección de movimiento y detección de manipulación de video.


3) Haga clic en Aceptar.

La alarma combinada se activará cuando reciba alarmas tanto de la entrada de alarma como de los eventos.

8. Haga clic en Programación de armado para seleccionar un tipo de programación de armado.




Nota

Si configura el Programa de armado como Personalizado, puede arrastrar el cursor sobre la barra de tiempo para configurar un programa de armado personalizado o mover el cursor sobre la barra de tiempo y  para establecer una hora específica hacer clic en programar.

9. Haga clic en Método de vinculación para configurar los métodos de vinculación.

Tabla 13-12 Descripción del método de vinculación

Método de vinculación	Descripción
Notificar a Vigilancia Centro	El dispositivo puede enviar una señal de excepción o alarma al host de alarma remoto cuando ocurre un evento. El host de alarma se refiere al PC con el software cliente instalado (p. ej., iVMS-4200, iVMS-5200).
Ventana emergente de alarma	Cuando se activa una alarma, el monitor local muestra la alarma ventana emergente.
Zumbador	Cuando se detecta una alarma, el zumbador emitirá un pitido audible.
Enviar correo electrónico	El sistema puede enviar un correo electrónico con información de alarma a uno o más usuarios cuando se detecta una alarma.
Salida de alarma	La salida de alarma puede activarse mediante la entrada de alarma, detección de movimiento, detección de manipulación de video, detección de rostro, detección de cruce de línea y cualquier otro evento.
Registro	<p>Cuando se detecta una alarma, el canal seleccionado grabará videos.</p> <p> Nota</p> <p>La programación de grabación de video debe estar habilitada para el canal; de lo contrario, la vinculación no será válida. Puede configurar la programación de grabación de video en Sistema → Administración de almacenamiento → Programación de almacenamiento → Grabación de video .</p>

10. Haga clic en Guardar.

### 13.1.7 Evento de análisis de audio

Pasos

1. Vaya a Centro de eventos →  Configuración de eventos → Análisis de audio .

2. Seleccione un canal.
3. Seleccione un tipo de evento.
4. Activar Habilitar.
5. Haga clic en Configuración de reglas para establecer la regla.

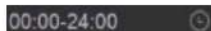
Tabla 13-13 Evento de análisis de audio

Nombre del evento	Descripción del evento	Configuración de reglas
Audio Excepción Detección	La detección de excepciones de audio detecta sonidos anormales en la escena, como un aumento o disminución repentinos del sonido de intensidad.	<p>Detección de aumento repentino de la intensidad del sonido</p> <p>Detecta un aumento brusco del sonido en la escena.</p> <p>Detección de disminución repentina de la intensidad del sonido</p> <p>Detecta una caída brusca de sonido en la escena.</p> <p>Sensibilidad</p> <p>Cuanto mayor sea el valor, más fácil será activar la alarma de detección.</p> <p>Umbral de intensidad del sonido</p> <p>Puede filtrar el sonido ambiental. Cuanto más alto sea el sonido ambiental, mayor será el valor. Ajústelo según el entorno.</p>

6. Haga clic en Programación de armado para seleccionar un tipo de programación de armado.




Nota

Si configura el Programa de armado como Personalizado, puede arrastrar el cursor sobre la barra de tiempo para configurar un programa de armado personalizado o mover el cursor sobre la barra de tiempo y  para establecer una hora específica hacer clic en programar.

7. Haga clic en Método de vinculación para configurar los métodos de vinculación.

Tabla 13-14 Descripción del método de vinculación

Método de vinculación	Descripción
Notificar a Vigilancia Centro	El dispositivo puede enviar una señal de excepción o alarma al host de alarma remoto cuando ocurre un evento. El host de alarma se refiere al PC con el software cliente instalado (p. ej., iVMS-4200, iVMS-5200).
Ventana emergente de alarma	Cuando se activa una alarma, el monitor local muestra la alarma ventana emergente.
Zumbador	Cuando se detecta una alarma, el zumbador emitirá un pitido audible.
Enviar correo electrónico	El sistema puede enviar un correo electrónico con información de alarma a uno o más usuarios cuando se detecta una alarma.

Método de vinculación	Descripción
Salida de alarma	La salida de alarma se puede activar mediante la entrada de alarma, movimiento Detección, detección de manipulación de vídeo, detección de rostros, cruce de línea detección y cualquier otro evento.
Registro	<p>Cuando se detecta una alarma, el canal seleccionado grabará vídeos.</p> <p> <b>Nota</b></p> <p>Se habilitará la programación de grabación de vídeo para el canal, De lo contrario, este enlace no sería válido. Puede ir a Sistema → Gestión de almacenamiento → Programación de almacenamiento → Grabación de vídeo a Configurar la programación de grabación de vídeo.</p>

8. Haga clic en Guardar.

## 13.2 Configuración de enlace

Configurar parámetros para vinculaciones de eventos.

### Pasos

- Vaya a Centro de eventos → Configuración de eventos → Configuración de vinculación o Sistema → Evento Configuración → Configuración de eventos → Configuración de vinculación.
- Haga clic en Correo electrónico para configurar los parámetros de correo electrónico.

Tabla 13-15 Vinculación de correo electrónico

Artículo	Descripción
Autenticación del servidor	Habilítelo si el servidor SMTP requiere autenticación de usuario y Introduzca el nombre de usuario y la contraseña correspondiente.
Servidor SMTP	La dirección IP del servidor SMTP o el nombre de host (por ejemplo, smtp.263xmail.com).
Puerto SMTP	El puerto SMTP. El puerto TCP/IP predeterminado para SMTP es el 25.
Habilitar SSL/TLS	Habilite SSL/TLS si el servidor SMTP tiene el requisito.
Remitente	El nombre del remitente.
Dirección del remitente	La dirección del remitente.
Seleccionar receptores	Seleccione el receptor. Se pueden configurar hasta 3 receptores.
Imagen adjunta	Enviar correo electrónico con imágenes de alarma adjuntas.

Artículo	Descripción
Habilitar 3 imágenes adjuntas para la protección perimetral	Cuando se activa un evento de protección perimetral, el dispositivo enviará un correo electrónico con 3 imágenes de alarma adjuntas.
Intervalo	El intervalo de tiempo para capturar las imágenes adjuntas.

### Nota

Si está utilizando una cuenta de correo electrónico de Outlook, configure el Tipo de correo electrónico como Outlook y haga clic en Ayuda en el lado derecho para leer las instrucciones de configuración; luego siga los pasos en la interfaz para completar la configuración.

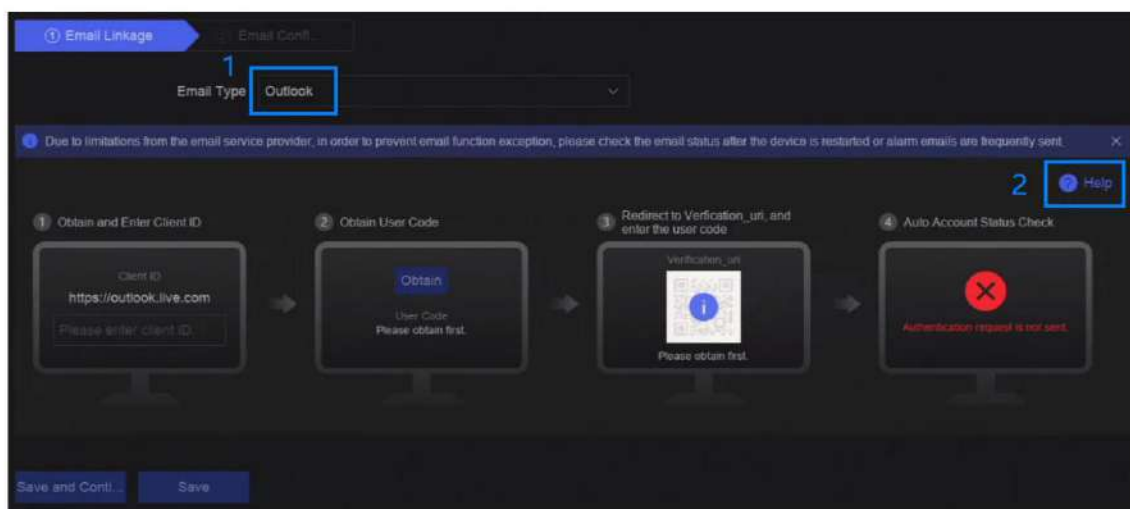


Figura 13-6 Configuración de correo electrónico de Outlook

- Haga clic en Administración de audio para administrar los archivos de audio para la vinculación de alarmas.

### Nota

Hay 3 archivos de audio predeterminados en la lista que no se pueden eliminar. Puedes importar archivos de audio desde una unidad USB. Los archivos deben estar en formato AAC o MP3 y su tamaño no debe superar los 1 MB.

- Si ha conectado altavoces IP, haga clic en Altavoz IP para importar archivos de audio a los altavoces IP seleccionados para la vinculación de la alarma.

### Nota

- Esta acción de vinculación solo está disponible para algunos tipos de eventos.
- El archivo de audio cargado debe estar en formato MP3, WAV o ACC, y el tamaño del archivo debe ser menor de 1 MB.

- Haga clic en Salida de alarma para configurar los parámetros de salida de alarma.



#### Nota

- Haga clic en el nombre de cada salida de alarma para editarla. • El número de salida de alarma coincide con el del panel trasero del dispositivo. Por ejemplo, Local->1 significa la salida de alarma n.º 1 en el panel trasero del dispositivo.

#### Demora

La duración de la señal de alarma.

#### Estado de alarma

Haga clic en el disparador para cambiar el estado.

6. Si ha conectado cámaras de audio y luz, haga clic en Configuración de audio y luz de la cámara para configurar los parámetros de luz intermitente y altavoz de la cámara para la vinculación de la alarma.



#### Nota

Esta acción de vinculación solo está disponible para algunos tipos de eventos.

7. Si ha conectado paneles de control de seguridad, haga clic en Panel de control de seguridad para configurar parámetros que incluyen dirección IP y número de puerto.

## 13.3 Configuración de desarmado

Después de configurar una plantilla de desarme, puede usarla para desarmar canales en un lote.

Los canales que tienen habilitada la opción Permitir desarmado no activarán los elementos de vinculación de alarma según la plantilla de desarmado.

#### Pasos

1. Vaya a Centro de eventos → Configuración de eventos → Configuración de vínculo o Sistema → Configuración de eventos → Configuración de eventos → Configuración de vínculo.



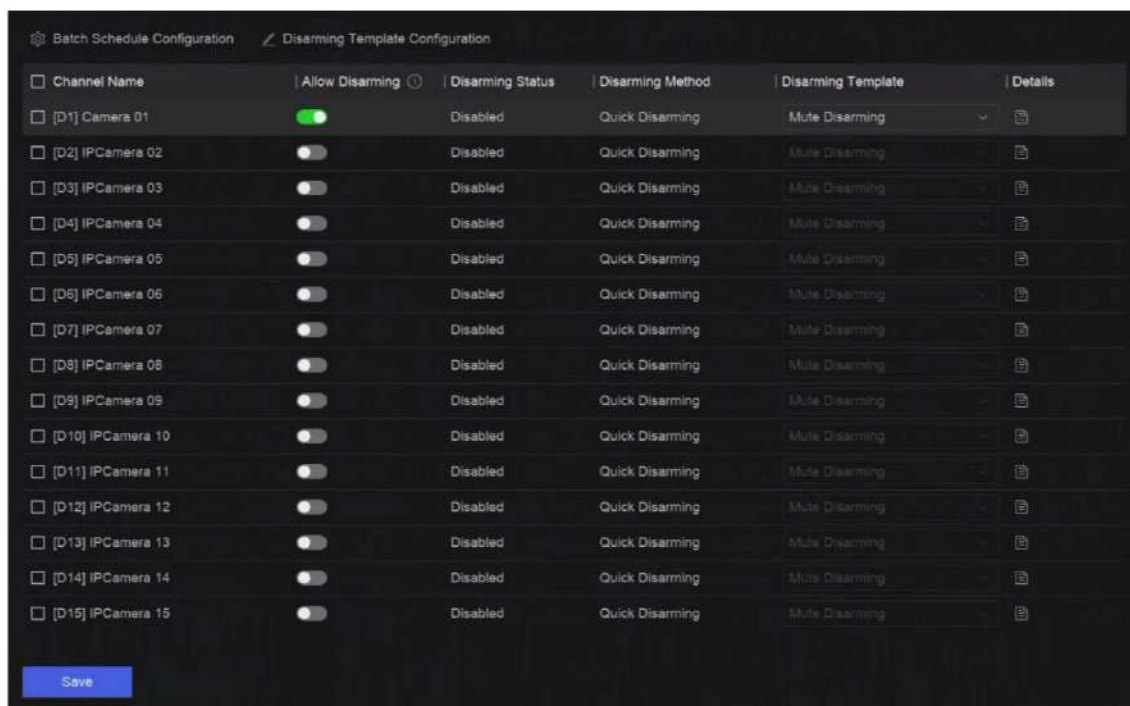


Figura 13-7 Configuración de desarme 2. Seleccione

los canales que tienen permiso para desarmar.

3. Haga clic en Configuración de programación por lotes.

4. Activar/Habilitar .

5. Seleccione la plantilla de desarme. Solo hay dos tipos disponibles.



Nota

Actualmente, solo hay dos tipos de plantillas disponibles y no se pueden configurar los parámetros de cada una.

6. Haga clic en Aceptar.

## 13.4 Configuración por lotes

Los eventos listados y la acción de vinculación correspondiente de Notify Surveillance Center se pueden habilitar o deshabilitar por lotes desde Centro de Eventos → Configuración de Eventos → Configuración de Lotes desde Sistema → Configuración de Eventos → Configuración de Eventos → Configuración de Lotes. Después de habilitar un evento, haga clic en "Ir a Configuración de Eventos" para establecer las reglas.

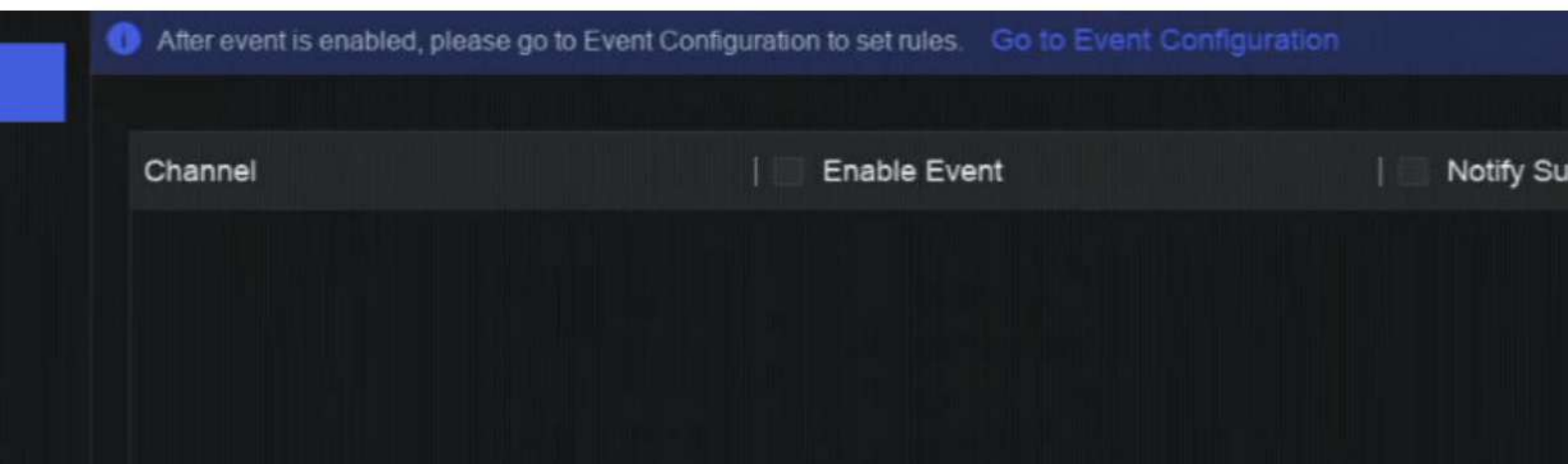


Figura 13-8 Configuración del lote

### 13.5 Búsqueda de eventos

Puede buscar archivos de eventos como vídeos e imágenes según la condición de búsqueda.

Pasos

1. Vaya a Centro de eventos → .

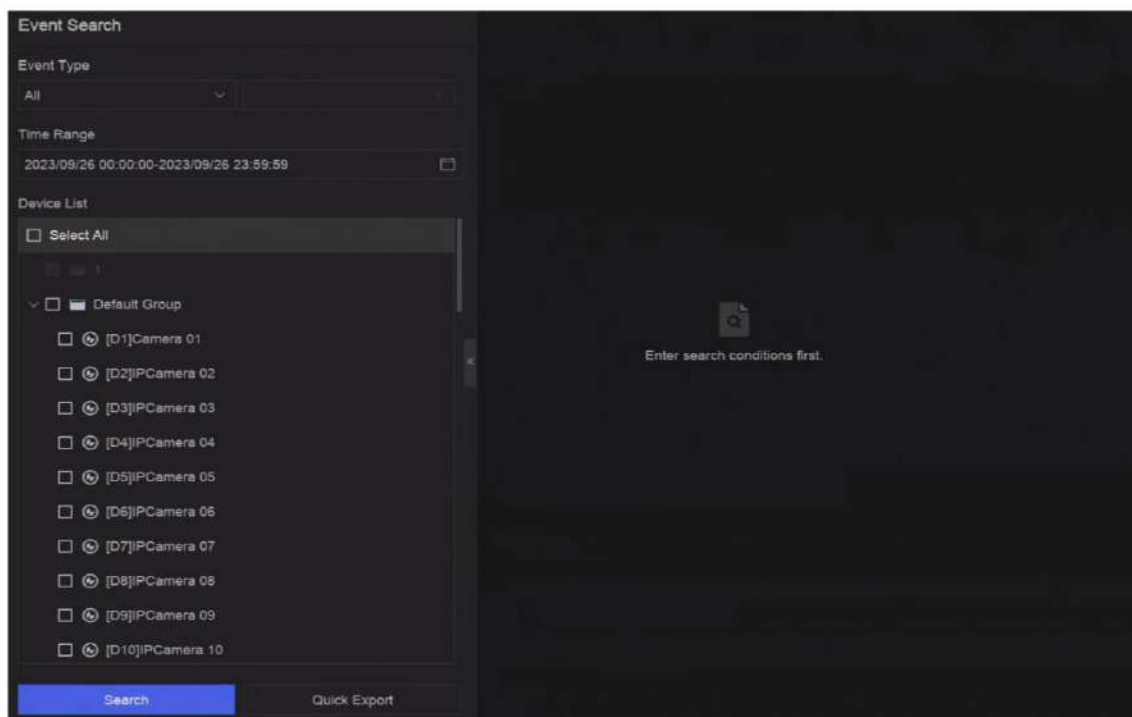


Figura 13-9 Búsqueda de eventos

2. Especifique las condiciones detalladas, incluido el tipo de evento, la hora, el canal, etc.

3. Haga clic en Buscar.

El dispositivo mostrará los resultados de la búsqueda de los canales seleccionados.


Qué hacer a continuación

Seleccione los elementos de la lista de resultados y expórtelos para realizar una copia de seguridad.

## 13.6 Ver alarmas

Puede ver vídeos e imágenes de alarmas en tiempo real y reproducirlos.

Pasos

1. Vaya a Centro de eventos → 

2. Haga clic en Alarma en tiempo real.

3. Seleccione la alarma de la lista.

Si hay demasiadas alarmas, haga clic en Filtrar para buscar y encontrar la alarma.

4. Haga clic en Reproducir y se reproducirá el video de la grabación de la alarma.

5. Vea las imágenes de la alarma a la derecha. Se mostrará el número de imágenes disponibles.

## Capítulo 14 Búsqueda y copia de seguridad

Puede buscar archivos según diferentes condiciones de búsqueda, incluido el tipo de archivo, el tipo de evento, la hora, la etiqueta, etc. Los resultados de la búsqueda se pueden exportar a otro dispositivo, como una unidad flash USB.

Antes de comenzar

Asegúrese de que el disco duro esté instalado correctamente y que los parámetros de grabación estén configurados adecuadamente.

Pasos 1.

Vaya a Copia de seguridad.

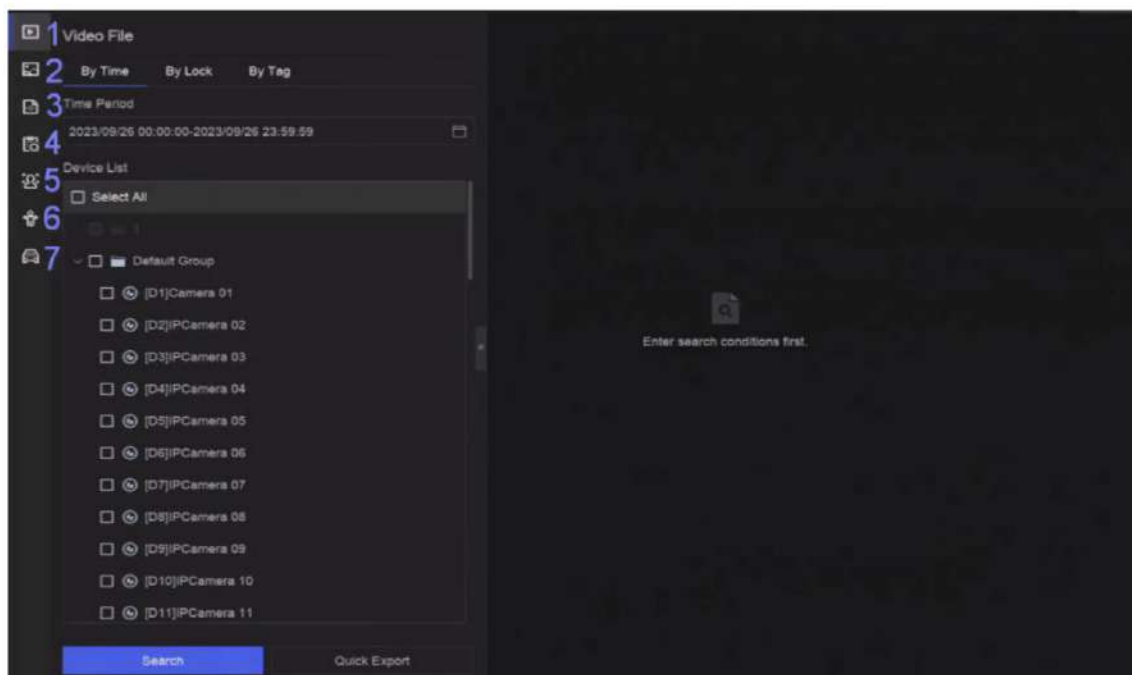


Figura 14-1 Búsqueda y copia de seguridad

2. Elija un método de búsqueda según su preferencia en el lado izquierdo; se admiten 7 tipos.



Nota

Las condiciones de búsqueda variarán según el método de búsqueda seleccionado.

---

3. Establezca las condiciones de búsqueda.

4. Haga clic en Buscar.



Figura 14-2 Resultado de la búsqueda

5. Opcional: Realice las siguientes operaciones.

- 1 Haga clic para seleccionar un archivo.
- 2 Haga clic para bloquear un archivo. Una vez bloqueado, no se sobrescribirá.
- 3 Haga clic para exportar un archivo.
- 4 Utilice la barra de herramientas en la parte superior para filtrar los resultados por canal.
- 5 Utilice la barra de herramientas en la parte superior para cambiar el efecto de visualización.
- 6 Vaya a diferentes páginas de resultados.
- 7 Expande o contrae la interfaz. Tras seleccionar un vídeo de la lista de resultados, podrás reproducirlo rápidamente.

6. Inserte una unidad flash USB en el dispositivo para realizar una copia de seguridad.

7. Exporte archivos a la unidad flash USB.

- Seleccione los archivos en la lista de resultados y haga clic en Exportar.
- Haga clic en Exportar todo para exportar todos los archivos.

## Capítulo 15 AcuSeek

AcuSeek permite la recuperación eficiente y precisa de las imágenes y videoclips deseados simplemente ingresando descripciones de texto relevantes.

Antes de empezar

- Asegúrese de haber agregado la cámara compatible con AcuSeek y de haber configurado la grabación. Horario para la cámara.

Asegúrese de haber configurado el motor AcuSearch. Consulte AcuSearch . \_\_\_\_\_

Pasos

1. Vaya a Centro de eventos → Configuración de eventos → Configuración inteligente → Gestión de algoritmos → Búsqueda inteligente , Seleccione AcuSeek y verifique el análisis de objetivos para los canales correspondientes.

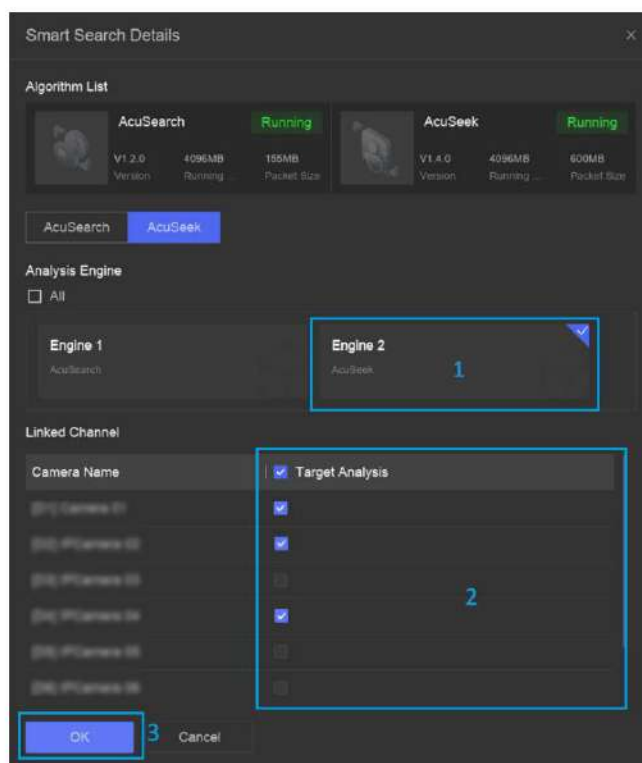


Figura 15-1 Configurar el motor AcuSeek

2. En la página principal de la GUI, haga clic en AcuSeek y configure las condiciones según las necesidades reales.

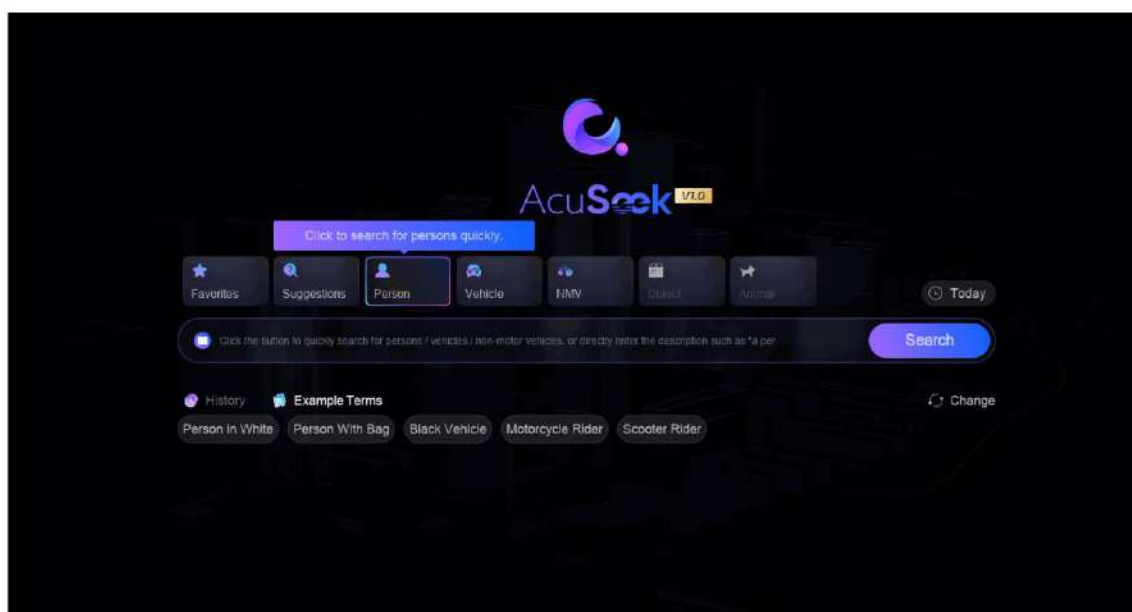


Figura 15-2 Establecer condiciones de búsqueda

- (Recomendado) Haga clic en Sugerencias, Persona, Vehículo o NMV y seleccione una de las condiciones predefinidas. Al buscar personas y vehículos, puede seleccionar condiciones de varios aspectos. Por ejemplo, puede buscar a una persona con una camiseta amarilla, pantalones azules y sombrero.

- Introduzca la condición en el cuadro de búsqueda.

- Haga clic en Favoritos para seleccionar condiciones de Favoritos.

Puede hacer clic en Personalizar para agregar términos a Favoritos.

- Haga clic en Hoy y defina el tiempo (3 días, 7 días, Personalizado) para la búsqueda.

- Haga clic en una condición de búsqueda del historial o un término de ejemplo debajo del cuadro de búsqueda. Puede hacer clic en el icono de estrella para agregar una condición de búsqueda del historial a Favoritos.

3. Haga clic en Buscar para ver los resultados de la búsqueda y realizar más operaciones según la figura. abajo.

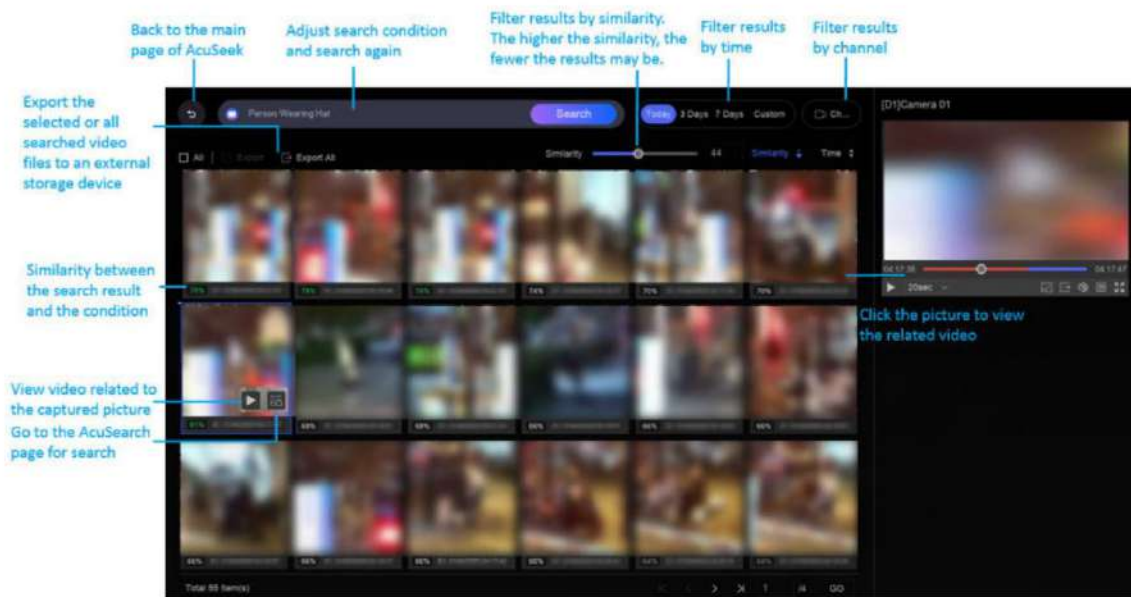


Figura 15-3 Resultados de AcuSeek




## Capítulo 16 AcuSearch

La función AcuSearch primero extrae imágenes de un rostro o cuerpo humano de una escena de video durante la visualización en vivo o la reproducción, luego compara la imagen extraída con videos grabados y, finalmente, encuentra los videos que contienen el objetivo.

Antes de comenzar



Asegúrese de que su dispositivo o cámara admita esta función.


Pasos

1. Vaya a Sistema → Configuración inteligente → Configuración de algoritmo → Administración de algoritmos para habilitar el algoritmo AcuSearch.
  - IA por cámara: la cámara realizará el análisis de AcuSearch.
  - IA por NVR: El dispositivo realizará el análisis de AcuSearch y se requieren recursos del motor.  
para análisis.
2. Vaya a Vista en vivo o Reproducción y haga clic en el  esquina inferior izquierda durante la reproducción del video.



Nota

- Si los objetivos son difíciles de encontrar durante la reproducción, se recomienda utilizar la Búsqueda inteligente (  ) a encontrar escenas que contengan objetivos.
- El rostro y el cuerpo humanos se enmarcarán con diferentes colores. • Después de hacer clic, también puede  arrastrar el cursor sobre la imagen para enmarcar manualmente un objetivo o ajustar manualmente el área del marco.

- 
3. Haga clic  del objetivo seleccionado.

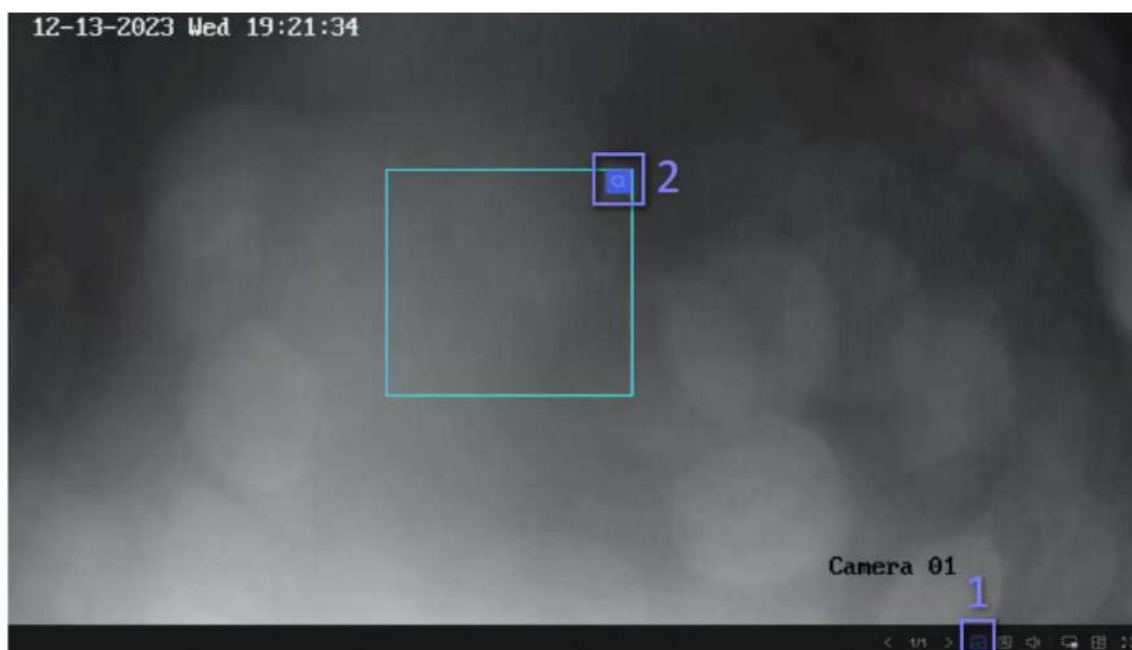


Figura 16-1 AcuSearch

Si se encuentran videos comparados, el dispositivo redireccionará a la interfaz de AcuSearch.

4. Ver los resultados de la búsqueda.

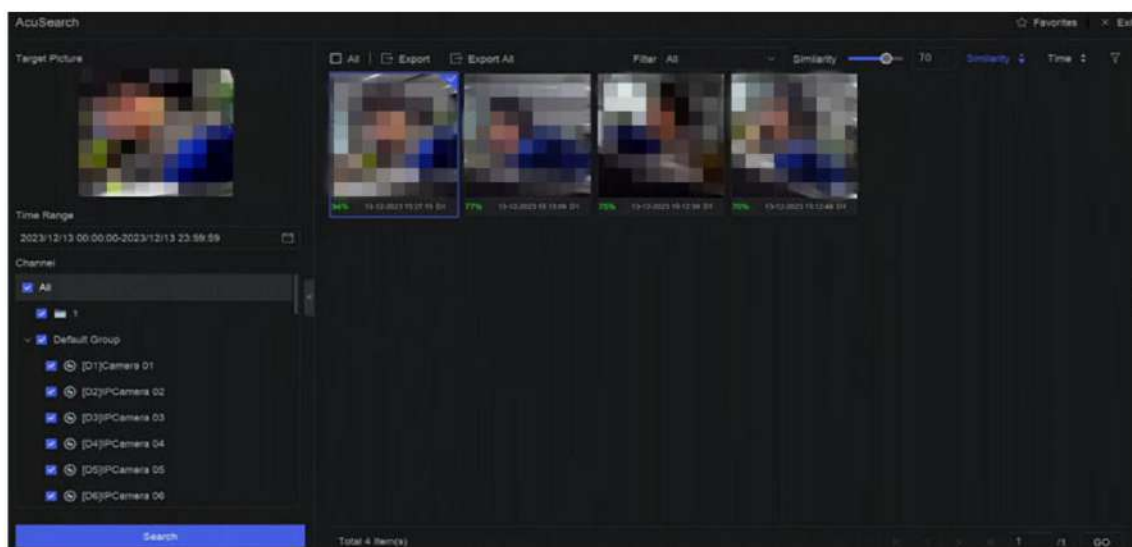


Figura 16-2 Resultado de AcuSearch

5. Opcional: Si los resultados no son los deseados, puede ajustar parámetros como el rango de tiempo, el canal o Similitud para buscar de nuevo.
6. Opcional: Seleccione un elemento de la lista de resultados; el vídeo correspondiente se reproducirá a la derecha, marcado en rojo. Puede hacer clic en los iconos de la barra de herramientas para realizar funciones.

## Capítulo 17 Configuraciones inteligentes

### 17.1 Gestión de algoritmos

Los motores de dispositivos utilizan algoritmos para analizar diferentes funciones inteligentes. Una función inteligente se podrá utilizar tras asignar el algoritmo correspondiente a un motor.

Vaya a Sistema → Configuración de eventos → Configuración de eventos → Configuración inteligente → Gestión de algoritmos o Centro de eventos → Configuración de eventos → Configuración inteligente → Gestión de algoritmos. Se mostrarán los algoritmos disponibles y podrá hacer clic en el algoritmo que desee para vincular los motores.

Para ciertos modelos que admiten el algoritmo AcuSearch, puede elegir la cámara (AI by Camera) o NVR (AI by NVR) para ejecutar el algoritmo AcuSearch.

### 17.2 Estado del motor

Puede ver el estado del motor, incluido el estado de funcionamiento, la temperatura y el nombre del algoritmo.

Vaya a Sistema → Configuración de eventos → Configuración de eventos → Ajustes inteligentes → Estado del motor o Centro de eventos → Configuración de eventos → Ajustes inteligentes → Estado del motor. Si necesita cambiar el algoritmo, consulte Administración de algoritmos .

---

### 17.3 Gestión del plan de tareas

Puede ver el estado de la tarea en la configuración de tareas. Los resultados del análisis inteligente se utilizan para filtrar las imágenes al buscar imágenes de cuerpos humanos y vehículos.

Vaya a Sistema → Configuración de eventos → Configuración de eventos → Ajustes inteligentes → Gestión de planes de tareas o Centro de eventos → Configuración de eventos → Ajustes inteligentes → Gestión de planes de tareas. Para la comparación de objetivos en tiempo real, puede ver el progreso diario.

El estado de la tarea incluye principalmente tres condiciones: Deshabilitado, En espera y Habilitado.

Desactivado

No hay ninguna tarea de análisis habilitada en la cámara.

Espera

La tarea de análisis de la cámara está habilitada. El dispositivo está esperando para analizar los datos.

Activado

La tarea de análisis de la cámara está habilitada y el dispositivo está analizando los datos de la cámara.

## 17.4 Gestión de bibliotecas de listas

La biblioteca de listas se utiliza principalmente para almacenar y comparar imágenes de objetivos. La biblioteca de desconocidos se utiliza para almacenar imágenes de desconocidos y no se puede eliminar.

### 17.4.1 Agregar una biblioteca de listas

#### Pasos

1. Vaya a Sistema → Configuración de eventos → Configuración de eventos → Archivo de datos → Biblioteca de listas o Centro de eventos → Configuración de eventos → Archivo de datos → Biblioteca de listas.
2. Haga clic en Agregar.
3. Ingrese el nombre de la biblioteca.
4. Haga clic en Confirmar.



#### Nota

- Después de una biblioteca de lista, puede mover el cursor sobre la biblioteca para editarla o eliminarla.
  - Puede hacer clic en Eliminar en lote para eliminar las bibliotecas seleccionadas o borrar todas las imágenes en el grupo seleccionado. bibliotecas.
- 

### 17.4.2 Subir imágenes de rostros a la biblioteca

La comparación de imágenes de destino se basa en las imágenes de destino de la biblioteca. Puede cargar una sola imagen de destino o importar varias a la biblioteca.

#### Antes de empezar

- Asegúrese de que el formato de la imagen sea JPEG o JPG.
- Importe todas las imágenes a un dispositivo de respaldo con anticipación.


#### Pasos

1. Haga doble clic en una biblioteca de listas.
2. Opcional: Haga clic en "Etiqueta personalizada" para agregar etiquetas a las imágenes. Puede editar la etiqueta como desee, por ejemplo, información personal, organización, puesto, etc.
3. Haga clic en Agregar o Importar.
4. Importar imagen(es).

- Añadir: Haz clic para subir una imagen a la vez. Si la imagen tiene varios objetivos, debes elegir uno.

- Importar: Se pueden importar varias imágenes a la vez. El dispositivo usará el nombre del archivo como nombre de la imagen y dejará los demás atributos vacíos, o importará archivos de imagen según las reglas especificadas. Si una imagen tiene varios objetivos, el dispositivo seleccionará el objetivo central por defecto.

5. Opcional: Realice las siguientes operaciones.

Eliminar imágenes de la biblioteca	<ul style="list-style-type: none"><li>• Seleccione una imagen y elimínela. •</li></ul> Seleccione las imágenes y haga clic en Eliminar por lotes para eliminar la selección. unos.
Buscar imágenes en el Biblioteca	 Hacer clic en la barra de herramientas para buscar imágenes.
Copiar imágenes a Otra biblioteca	Seleccione imágenes y haga clic en Copiar a para copiar las imágenes cargadas de la biblioteca actual a otra biblioteca.
Editar imágenes	Haga clic en el nombre de la imagen y edite sus atributos.
Exportar imágenes	Seleccione imágenes y haga clic en Exportar para exportarlas a una unidad flash USB.

### 17.5 Configuraciones de autoaprendizaje

La tecnología de autoaprendizaje optimiza la precisión del algoritmo y requiere una mínima intervención manual del usuario. Al activarse, el dispositivo recopila automáticamente información sobre falsas alarmas y la utiliza para entrenar y optimizar constantemente el algoritmo correspondiente.

Vaya a Sistema → Configuración de eventos → Configuración de eventos → Configuración inteligente → Gestión de algoritmos o Centro de eventos → Configuración de eventos → Configuración inteligente → Gestión de algoritmos para habilitar el algoritmo de autoaprendizaje .



#### Nota

- Solo algunos modelos admiten esta función. • Actualmente, la función de autoaprendizaje solo se puede implementar para eventos de protección perimetral. • Si su dispositivo solo tiene un motor, debe desactivar la IA del NVR y la cámara debe analizar los objetivos de detección. Si su dispositivo solo tiene dos o más motores, puede activar la IA del NVR y usar un motor para analizar los objetivos de detección, y luego usar otro para ejecutar el algoritmo de autoaprendizaje.

---

#### 17.5.1 Gestión de tareas de autoaprendizaje

Una vez ejecutado el algoritmo de autoaprendizaje, también se debe habilitar la tarea de autoaprendizaje.

Vaya a Sistema → Configuración de eventos → Configuración de eventos → Autoaprendizaje → Administración de tareas o Centro de eventos → Configuración de eventos → Autoaprendizaje → Administración de tareas para habilitar la tarea.

Se listará la tarea disponible y podrás ver su estado y la barra de progreso. La recopilación de material tardará bastante tiempo.

Al completar la tarea, el algoritmo de autoaprendizaje se actualizará automáticamente. Puede hacer clic en " Actualizar configuración automáticamente" para configurar la hora de actualización.



Nota

- Cuando el algoritmo de autoaprendizaje no esté disponible para eventos de protección perimetral cuando El algoritmo se está actualizando.
  - El entrenamiento de fuerza solo se utiliza para el soporte técnico.
- 

## 17.5.2 Gestión de modelos

Puede configurar la versión del modelo del algoritmo de autoaprendizaje según sus necesidades.

Vaya a Sistema → Configuración de eventos → Configuración de eventos → Autoaprendizaje → Gestión de modelos o Centro de eventos → Configuración de eventos → Autoaprendizaje → Gestión de modelos para configurar la versión del modelo.

Restaurar a la versión anterior

Restaurar el modelo a la versión anterior a ésta.

Restaurar a la versión predeterminada

Restaurar el modelo a la versión predeterminada de fábrica.

## 17.5.3 Estado inteligente

Puede ver el estado de rendimiento del algoritmo de autoaprendizaje de cada canal en Sistema → Configuración de eventos → Configuración de eventos → Autoaprendizaje → Estado inteligente o Centro de eventos → Configuración de eventos → Autoaprendizaje → Estado inteligente.

## Capítulo 18 Centro de aplicaciones

### 18.1 Detección de personas y vehículos

La información humana y del vehículo se mostrará para el canal seleccionado en tiempo real.


La detección de personas y vehículos debe configurarse con antelación. Vaya al Centro de eventos → par configurarlo.



Figura 18-1 Detección de personas y vehículos

Tabla 18-1 Descripción de detección de personas y vehículos

No.	Descripción
1	Menú de acceso directo del botón derecho.
2	Configuración de detección de personas y vehículos. Puede configurar el diseño, el aviso de comparación exitosa y los canales de recursos.
3	Entrar/salir de pantalla completa.

### 18.2 Check-in de personas

Una vez agregadas las tareas de check-in, puedes ver la información de check-in en vivo y buscar resultados de check-in.

### 18.2.1 Agregar tarea de check-in

Antes de iniciar el check-in de personas es necesario configurar adecuadamente la tarea correspondiente.

Antes de empezar


- Una cámara para el registro de personas está conectada correctamente. •

Vaya a Sistema → Configuración inteligente → Configuración de algoritmo → Gestión de algoritmo .

Asignar reconocimiento de objetivos a al menos un motor.

- La biblioteca de listas para la comparación de check-in está configurada correctamente. Consulte [Agregar una biblioteca de listas](#) para detalles.

Pasos

1. Haga clic en Registro de persona .
2. Haga clic derecho para mostrar el menú en el lado izquierdo.
3. Haga clic  .
- en 4. Haga clic en Agregar.

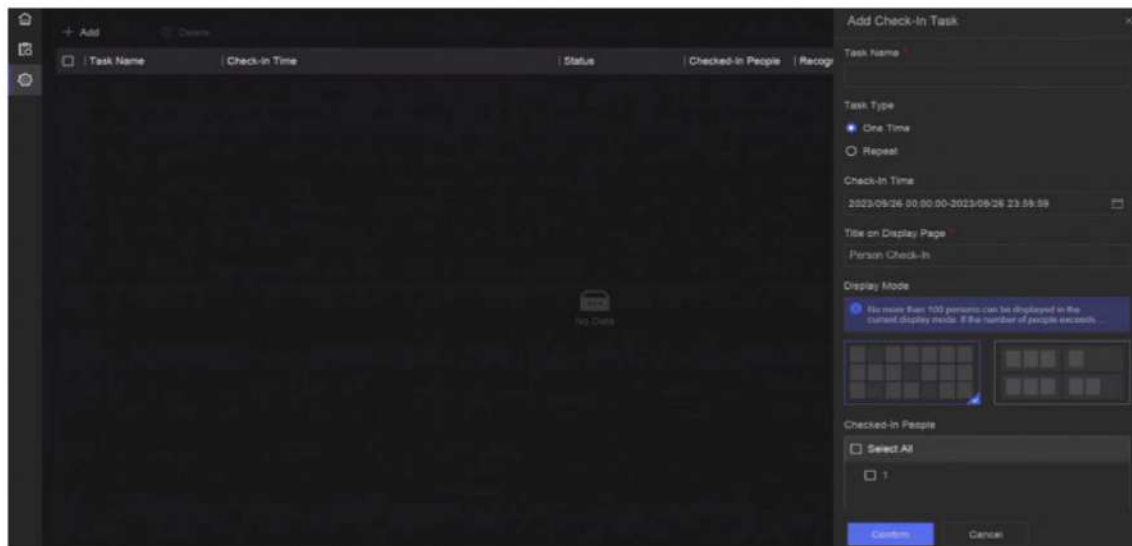


Figura 18-2 Agregar tarea de check-in

5. Establecer tarea.

Una sola vez

La tarea se utilizará una sola vez.

Repetir

La tarea se utilizará y repetirá varias veces.

6. Configure otros parámetros, incluido el nombre de la tarea, la hora de registro, el canal de reconocimiento, etc.

7. Haga clic en Confirmar.




## 18.2.2 Buscar registros de check-in

Una vez configuradas las tareas de check-in, puedes buscar los registros por día o mes.

Antes de comenzar

Asegúrese de que las tareas de registro estén configuradas.

Pasos

1. Vaya a Registro de personas .
2. Haga clic derecho para mostrar el menú en el lado izquierdo.
3. Haga clic  .

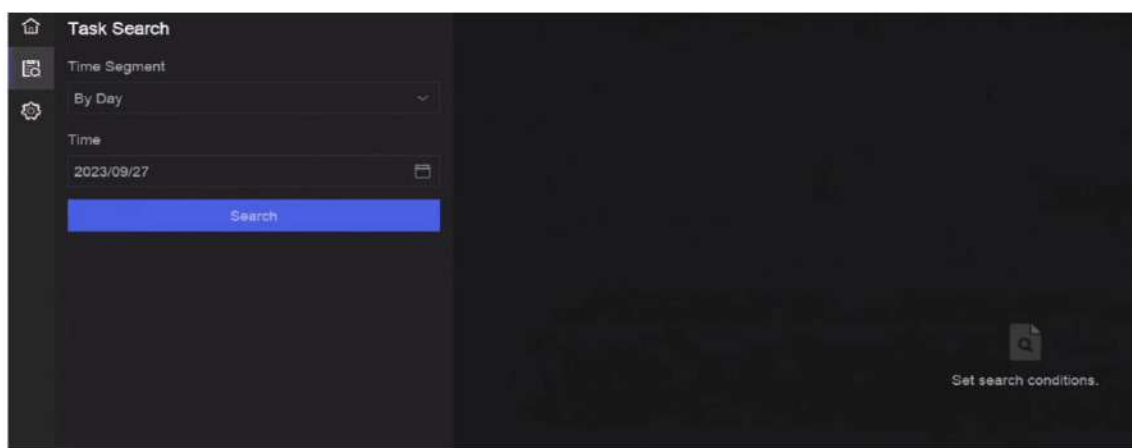


Figura 18-3 Búsqueda de registros de check-in


4. Establecer la hora.


5. Haga clic en Buscar.

## 18.3 Informe estadístico

Puede ver informes de recuento de personas y mapas de calor.

Tabla 18-2 Introducción al informe estadístico

Función Nombre	Icono	Condición	Descripción
Gente Cálculo		<ul style="list-style-type: none"><li>• La función debe ser compatible con la cámara IP conectada. Por ejemplo, un conteo de personas.</li></ul>	El conteo de personas calcula la cantidad de personas que entran o salen de un área determinada configurada y crea informes diarios/semanales/mensuales/anuales para su análisis.

Función Nombre	Icono	Condición	Descripción
		<p>La cámara está conectada a su dispositivo.</p> <ul style="list-style-type: none"> <li>• Los datos estadísticos de la cámara se pueden almacenar en el disco duro del dispositivo.</li> </ul>	
Mapa de calor		<ul style="list-style-type: none"> <li>• La función debe ser compatible con la cámara IP conectada. • Los datos estadísticos de la cámara se pueden almacenar en el disco duro del dispositivo.</li> </ul>	<p>Un mapa de calor es una representación gráfica de datos. Esta función se utiliza para analizar cuántas personas visitaron y se alojaron en un lugar específico. área.</p>

## Capítulo 19 Configuración de parámetros del sistema

Los parámetros del sistema incluyen el nombre del dispositivo, la región, la hora, el tiempo de bloqueo de la pantalla, el idioma, etc.

Vaya a Sistema → Configuración del sistema → Configuración del sistema para configurar el parámetro.

Tabla 19-1 Descripción de parámetros

Tipo	Nombre del parámetro	Descripción
Información básica	Tiempo de bloqueo de pantalla	La pantalla se bloqueará cuando el cursor no se mueva durante el tiempo especificado.
	Vista en vivo Permiso en Pantalla de bloqueo	Una vez bloqueada la pantalla, el dispositivo reproducirá la imagen en vivo de las cámaras que tengan este permiso.
Región y hora Configuración	Bloqueo de zona horaria	Se requiere la contraseña de administrador para esta operación. Una vez bloqueada la zona horaria, la información de la zona horaria del dispositivo no se puede modificar de forma remota desde otras plataformas o interfaces, como la interfaz web a través del navegador.  Solo puede bloquear o desbloquear la zona horaria a través de la interfaz GUI local.
	Modo de sincronización horaria	<ul style="list-style-type: none"> <li>• Sincronización horaria NTP: Puede seleccionar la sincronización horaria NTP y configurar el servidor NTP, el puerto del servidor NTP, el puerto del cliente NTP y el intervalo. El intervalo es el intervalo de tiempo entre dos acciones de sincronización dentro del servidor NTP. Si el dispositivo está conectado a una red pública, debe usar un servidor NTP con función de sincronización horaria, como las direcciones de servidor listadas para su selección. Si el dispositivo está configurado en una red personalizada, se puede usar software NTP para establecer un servidor NTP para la sincronización horaria.</li> <li>• Sincronización horaria manual: Configure manualmente la hora del sistema.</li> <li>• Sincronización horaria del servidor Hik-Connect: El dispositivo sincronizará la hora con Hik-Connect en lugar del servidor NTP.</li> <li>• Sincronización horaria del servidor Guarding Vision: el dispositivo sincronizará la hora con Guarding Vision en lugar del servidor NTP.</li> </ul>
	Horario de verano	El horario de verano (DST) se refiere al período del año en que los relojes se adelantan un día. En algunas zonas del mundo, esto genera más horas de sol por la noche durante los meses más cálidos.

Tipo	Nombre del parámetro	Descripción
		Adelantamos nuestros relojes un cierto período (depende en el sesgo de DST que configure) al comienzo del horario de verano, y moverlos hacia atrás en el mismo período cuando volvamos a hora estándar (ST).
Salida del menú	Puerto auxiliar Cambio automático	Cuando dos o más monitores están conectados a la parte trasera Panel, uno de ellos puede convertirse en la salida auxiliar que no pueden acceder al menú principal. Imágenes en el auxiliar Las ventanas de salida cambiarán automáticamente a la siguiente unos según el intervalo.
Canal cero	-	El canal cero, conocido como canal virtual, puede mostrar en vivo imágenes de todos los canales del dispositivo, lo que permite guardar ancho de banda para la transmisión.
RS-232	Uso	Consola  Después de conectarlo a la PC con un convertidor, la PC puede configurarse Los parámetros del dispositivo.  Canal transparente  Se conecta directamente a un dispositivo serial. La PC puede Acceder de forma remota al dispositivo serial a través de la red.

## Capítulo 20 Copia de seguridad del dispositivo de repuesto activo

Las grabadoras de video pueden formar un sistema de reserva activa N+M. El sistema consta de varias grabadoras de video en funcionamiento y al menos una de reserva activa. Cuando una grabadora de video en funcionamiento falla, la de reserva activa entra en funcionamiento, lo que aumenta la fiabilidad del sistema. Se requiere una conexión bidireccional, como se muestra en la figura a continuación, entre las grabadoras de video de reserva activa y las grabadoras de video en funcionamiento.



Figura 20-1 Construir un sistema de repuesto activo



### Nota

- Se permiten hasta 32 dispositivos en funcionamiento y 32 dispositivos de repuesto dinámico. • Se recomienda usar todos los dispositivos en un mismo modelo para garantizar la compatibilidad. Contacte a su distribuidor para obtener más información.  
Detalles de los modelos que admiten la función de repuesto activo.
  - Solo ciertos modelos admiten esta función.
- 

### 20.1 Establecer dispositivo de trabajo

#### Pasos

1. Vaya a Sistema → Administración del sistema → N+M Hot Spare .
2. Establezca el modo de trabajo como modo normal.
3. Activar Habilitar.
4. Haga clic en Guardar.
5. Opcional: Ver la dirección IP del dispositivo de repuesto activo y el estado de funcionamiento del dispositivo de repuesto activo.

### 20.2 Establecer dispositivo de repuesto activo

El dispositivo de repuesto activo se hará cargo de las tareas del dispositivo en funcionamiento cuando este falle.

#### Pasos

1. Vaya a Sistema → Administración del sistema → N+M Hot Spare .
2. Establezca el modo de trabajo como modo de repuesto activo.
3. Haga clic en Guardar. Su dispositivo se reiniciará automáticamente.



### Nota

- La conexión de la cámara se desactivará cuando el dispositivo funcione en modo de repuesto activo. • Se recomienda encarecidamente restaurar los valores predeterminados del dispositivo después de cambiar el modo de trabajo de repuesto activo. dispositivos de repuesto al modo normal para garantizar el funcionamiento normal después.

---

4. Vaya a Sistema → Administración del sistema → N+M Hot Spare nuevamente.

5. Agregue dispositivos que funcionen al sistema de repuesto activo.

6. Agregue dispositivos de repuesto activo al sistema de repuesto activo.

7. Haga clic en Guardar.

## Capítulo 21 Configurar evento de excepción

Los eventos de excepción se pueden configurar para tomar la sugerencia del evento en la interfaz de vista en vivo y activar la salida de alarma y acciones de vinculación.

Pasos

1. Vaya a Sistema → Configuración del sistema → Excepción .

Main Type Exception: HDD Exception

HDD Full

Notify Surveillance Center: ☐

Send Email: ☐ [Configure Email](#)

Buzzer: ☒

Alarm Output: ☐ Select All [Configure Alarm Output](#)

- ☐ Local->1
- ☐ Local->2
- ☐ Local->3
- ☐ Local->4
- ☐ Local->5
- ☐ Local->6
- ☐ Local->7
- ☐ Local->8

Save

Figura 21-1 Configuración de eventos de excepción



2. Seleccione el tipo de excepción.
3. Configure los métodos de vinculación.

Tabla 21-1 Descripción del enlace

Método de vinculación	Descripción
Notificar a Vigilancia Centro	El dispositivo puede enviar una señal de excepción o alarma al host de alarma remoto cuando ocurre un evento. El host de alarma se refiere al PC con el software cliente instalado (p. ej., iVMS-4200, iVMS-5200).
Zumbador	Cuando se detecta una alarma, el zumbador emitirá un pitido audible.
Enviar correo electrónico	El sistema puede enviar un correo electrónico con información de alarma a uno o más usuarios cuando se detecta una alarma.
Salida de alarma	La salida de alarma puede activarse mediante la entrada de alarma, detección de movimiento, detección de manipulación de video, detección de rostro, detección de cruce de línea y cualquier otro evento.



Nota

Cuando ocurren eventos de excepción,  en la esquina superior derecha se notificará y usted podrá hacer clic para ver .

---

4. Haga clic en Guardar.



## Capítulo 22 Ver información del sistema

Vaya a Sistema → Mantenimiento del sistema → Información en ejecución → Información del sistema para ver la información del sistema, incluida información de grabación de video, información del disco duro, información de red, información de transmisión de vista en vivo o reproducción de video, información de diagnóstico de sincronización de tiempo, etc.

Si ocurre una excepción del dispositivo, por ejemplo, cuando ocurre una excepción de sincronización de hora y la batería RTC (pila de botón o moneda) está sin energía, puede afectar la grabación o reproducción de video; resuelva la excepción lo antes posible.

## Capítulo 23 Mantenimiento del sistema

Las funciones de mantenimiento del sistema incluyen búsqueda de registros, reinicio programado, actualización, etc.

### 23.1 Reinicio programado

El dispositivo se reiniciará automáticamente según lo programado.

Vaya a Sistema → Mantenimiento del sistema → Mantenimiento → Programar reinicio para habilitar la función y configurar la programación de reinicio.

### 23.2 Dispositivo de actualización

El sistema del dispositivo se puede actualizar con una unidad flash USB local, un servidor FTP remoto, etc.

Vaya a Sistema → Mantenimiento del sistema → Mantenimiento → Actualizar para actualizar su dispositivo.

### 23.3 Copia de seguridad y restauración

Vaya a Sistema → Mantenimiento del sistema → Mantenimiento → Copia de seguridad y restauración para restaurar o realizar una copia de seguridad de los parámetros del sistema.

#### Importar/Exportar archivo de configuración

Los archivos de configuración del dispositivo se pueden exportar a un dispositivo local para realizar una copia de seguridad, y los archivos de configuración de un dispositivo se pueden importar a varios dispositivos si se deben configurar con los mismos parámetros.

#### Restauración simple

Restaura todos los parámetros, excepto la red (incluida la dirección IP, la máscara de subred, la puerta de enlace, la MTU, el modo de trabajo de la NIC, la ruta predeterminada, el puerto del servidor, etc.) y los parámetros de la cuenta de usuario, a la configuración predeterminada de fábrica.

#### Valores predeterminados

de fábrica Restaura todos los parámetros a la configuración predeterminada de fábrica.

#### Restaurar a inactivo

Restaurar el dispositivo al estado inactivo y deje todas las configuraciones sin cambios excepto la restauración del usuario. cuentas.

### 23.4 Información de registro

Vaya a Sistema → Mantenimiento del sistema → Mantenimiento → Registro para buscar y exportar información de registro.

#### Configuración de tiempo vencido

Cuando el disco de registro esté lleno, los registros que excedan el período se sobrescribirán.

### 23.5 Configurar el servidor de registros

Puede cargar registros del sistema al servidor para realizar copias de seguridad.

#### Pasos

1. Vaya a Sistema → CX → Configuración del sistema → Red → Red → Servidor de registro .
2. Activar Habilitar.
3. Configure la hora de carga, la dirección IP del servidor y el puerto.
4. Opcional: haga clic en Probar para comprobar si los parámetros son válidos.
5. Haga clic en Guardar.

### 23.6 Herramientas de mantenimiento

Se proporcionan múltiples herramientas para el mantenimiento del sistema, como detección SMART y detección de sectores defectuosos.

#### Antes de comenzar

Asegúrese de que el disco duro esté instalado correctamente.

#### Pasos

1. Vaya a Sistema → Mantenimiento del sistema → Mantenimiento → Herramientas de mantenimiento .
2. Seleccione herramientas según sus necesidades.

Tabla 23-1 Descripción de la herramienta

Nombre de la herramienta	Descripción
Datos de red Escucha	La monitorización de datos de red es el proceso de revisar, analizar y gestionar los datos de red para detectar cualquier anomalía o proceso que pueda afectar el rendimiento, la disponibilidad o la seguridad de la red.
Ping de captura de paquetes de red	La prueba de ping se utiliza para detectar si la dirección IP de destino es accesible.  Captura de paquetes NIC

Nombre de la herramienta	Descripción
	Después de que la grabadora acceda a la red, puede usar una unidad flash USB para capturar y exportar paquetes de red.
Detección del estado del disco duro	Puede ver el estado de un disco duro Seagate de 4 TB a 8 TB generado después del 1 de octubre de 2017. Utilice esta función para solucionar problemas del disco duro. La Detección de Estado muestra el estado del disco duro con mayor detalle que la función SMART.
Detección SMART	SMART (Tecnología de Automonitoreo, Análisis y Reporte) son sistemas de monitoreo de HDD para detectar varios indicadores de confiabilidad con la esperanza de anticipar fallas.
Detección de sectores defectuosos	Cuando un disco duro contiene demasiados sectores defectuosos, se recomienda reemplazarlo; de lo contrario, se pueden perder archivos en el disco duro.
Clon de disco duro	Copiar los datos de un HDD a otro a través de la interfaz eSATA.



Nota

Se recomienda utilizar herramientas de mantenimiento con la ayuda del soporte técnico.

## 23.7 Configuración de apagado suave

La función de apagado suave solo está disponible para dispositivos con salidas de alarma POWER-AC (excepción de alimentación de CA), POWER-UPS (excepción de SAI) y POWER-UPSL (baja potencia del SAI) (en el panel principal). El dispositivo puede recibir y registrar estas alarmas. Cuando se activan las alarmas POWER-AC y POWER-UPSL, el dispositivo se apaga automáticamente según el tiempo preestablecido. Si no se activa ninguna de las alarmas, el dispositivo se enciende automáticamente.

### Pasos

1. Vaya a Sistema → Mantenimiento del sistema → Mantenimiento → Configuración de apagado suave.

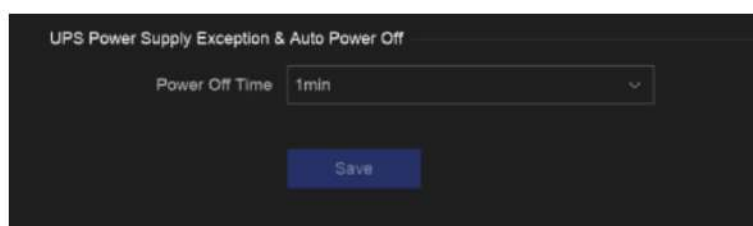


Figura 23-1 Configuración de apagado suave 2.

Configure el tiempo de apagado. El dispositivo se apagará automáticamente después del tiempo preestablecido cuando se activan las alarmas correspondientes.

3. Haga clic en Guardar.

**Ejemplo**

Por ejemplo, si el tiempo de apagado se establece en 1 minuto, cuando se activan las alarmas POWER-AC (excepción de energía de CA) y POWER-UPSL (baja energía de UPS), el dispositivo se apagará automáticamente después de 1 minuto.

## Capítulo 24 Gestión de la seguridad

### 24.1 Filtro de direcciones

El filtro de direcciones decide si permitir o prohibir que una dirección IP/MAC específica acceda a su dispositivo.

Antes de comenzar

Inicie sesión con la cuenta de administrador.

Pasos

1. Vaya a Sistema → Mantenimiento del sistema → Administración de seguridad → Filtro de direcciones .
2. Activar Habilitar.
3. Configure el tipo de filtrado. Elija entre filtrar por dirección IP o dirección MAC.
4. Configure el tipo de restricción. El mecanismo del dispositivo permitirá o prohibirá el acceso a direcciones IP/MAC específicas.
5. Opcional: Configurar lista de restricciones. Puede agregar, editar o eliminar direcciones.
6. Haga clic en Guardar.

### 24.2 Cifrado de transmisión

Después de habilitar el cifrado de transmisión, se requerirá una clave de cifrado para la visualización en vivo remota, la reproducción remota y los videos descargados.

Pasos

1. Vaya a Sistema → Mantenimiento del sistema → Administración de seguridad → Cifrado de transmisión .
2. Activar Habilitar.
3. Establecer clave de cifrado.



Nota

La clave de cifrado de la transmisión se sincroniza con el código de verificación del servicio Hik-Connect. Tras activar el código de cifrado, la transmisión de Hik-Connect se cifrará de forma forzada.

---

4. Haga clic en Guardar.

### 24.3 Seleccionar la versión de TLS

La configuración de TLS será efectiva para HTTP y el servicio SDK mejorado. Esto proporciona un servicio de transmisión de flujo más seguro. Vaya a Sistema → Mantenimiento del sistema → Administración de seguridad → TLS para seleccionar la versión de TLS.

## Capítulo 25 Apéndice

### 25.1 Lista de adaptadores de corriente aplicables

Utilice únicamente los adaptadores de corriente que se enumeran a continuación.

Modelo de adaptador de corriente	Presupuesto	Fabricante
ADS-26FSG-12 12024EPG	12 V, 2 A	Shenzhen Honor Electronic Co., Limitado.
MSA-Z3330IC12.0-48W-Q	12 V, 3,33 A	Tecnología de suministro de energía Moso Compañía, Ltd.
MSA-C1500IC12.0-18P-DE	12 V, 1,5 A	0000201935 Tecnología MOSO Compañía, Ltd.
ADS-25FSG-12 12018GPG	CE, 100 a 240 V CA, 12 V, 1,5 A, 18 W, $\Phi 5,5 \times 2,1 \times 10$	0000200174 Shenzhen Honor Compañía electrónica, Ltd.
MSA-C1500IC12.0-18P-US	12 V, 1,5 A	0000201935 Tecnología MOSO Compañía, Ltd.
TS-A018-120015AD	100 a 240 VCA, 12 V, 1,5 A, 18 Ancho, $\Phi 5,5 \times 2,1 \times 10$	0000200878 Transacción de Shenzhen Tecnologías Co., Ltd.
MSA-C2000IC12.0-24P-DE	12 V, 2 A	0000201935 Tecnología MOSO Compañía, Ltd.
ADS-24S-12 1224GPG	CE, 100 a 240 V CA, 12 V, 2 A, 24 W, $\Phi 2,1$	0000200174 Shenzhen Honor Compañía electrónica, Ltd.
MSA-C2000IC12.0-24P-US	EE. UU., 12 V, 2 A	0000201935 Tecnología MOSO Compañía, Ltd.
ADS-26FSG-12 12024EPCU	EE. UU., 12 V, 2 A	0000200174 Shenzhen Honor Compañía electrónica, Ltd.
KPL-040F-VI	12 V, 3,33 A, 40 W	0000203078 Pozo de canal Tecnología Co., Ltd.
MSA-Z3330IC12.0-48W-Q	12 V, 3,33 A	0000201935 Tecnología MOSO Compañía, Ltd.
MSP-Z1360IC48.0-65W	48 V, 1,36 A	0000201935 Tecnología MOSO Compañía, Ltd.
KPL-050S-II	48 V, 1,04 A	0000203078 Pozo de canal Tecnología Co., Ltd.

## 25.2 Glosario

### Doble flujo

La transmisión dual es una tecnología que permite grabar video de alta resolución localmente y transmitir una transmisión de menor resolución por la red. El DVR genera ambas transmisiones: la principal tiene una resolución máxima de 1080p y la secundaria, una resolución máxima de CIF.

### DVR

Acrónimo de Grabadora de Video Digital. Una DVR es un dispositivo capaz de recibir señales de video de cámaras analógicas, comprimirlas y almacenarlas en sus discos duros.

### Disco duro

Acrónimo de unidad de disco duro. Medio de almacenamiento que almacena datos codificados digitalmente en discos con superficies magnéticas.

### DHCP

El Protocolo de configuración dinámica de host (DHCP) es un protocolo de aplicación de red utilizado por los dispositivos (clientes DHCP) para obtener información de configuración para la operación en una red de Protocolo de Internet.

### HTTP

Acrónimo de Protocolo de Transferencia de Hipertexto. Protocolo para transferir solicitudes e información de hipertexto entre servidores y navegadores a través de una red.

### PPPoE

PPPoE, Protocolo Punto a Punto sobre Ethernet, es un protocolo de red para encapsular tramas del Protocolo Punto a Punto (PPP) dentro de tramas Ethernet. Se utiliza principalmente con servicios ADSL, donde los usuarios individuales se conectan al transceptor ADSL (módem) a través de Ethernet, y en redes Metro Ethernet simples.

### DDNS

El DNS dinámico es un método, protocolo o servicio de red que proporciona la capacidad a un dispositivo en red, como un enrutador o un sistema informático que utiliza el conjunto de protocolos de Internet, de notificar a un servidor de nombres de dominio para cambiar, en tiempo real (ad-hoc), la configuración DNS activa de sus nombres de host configurados, direcciones u otra información almacenada en DNS.

### DVR híbrido

Un DVR híbrido es una combinación de un DVR y un NVR.

---

Acrónimo de Network Time Protocol (Protocolo de Tiempo de Red). Protocolo diseñado para sincronizar los relojes de las computadoras en una red.

### NTSC



Acrónimo de Comité Nacional del Sistema de Televisión. NTSC es un estándar de televisión analógica utilizado en países como Estados Unidos y Japón. Cada fotograma de una señal NTSC contiene 525 líneas de escaneo a 60 Hz.

Continúa en el capítulo 25.3

Siglas de Network Video Recorder (Grabador de Vídeo en Red). Un NVR puede ser un sistema integrado o basado en PC que se utiliza para la gestión y el almacenamiento centralizados de cámaras IP, domos IP y otros DVR.

CAMARADA

Acrónimo de Phase Alternating Line (Línea de Fase Alterna). PAL es otro estándar de vídeo utilizado en sistemas de televisión abierta en gran parte del mundo. La señal PAL contiene 625 líneas de escaneo a 50 Hz.

PTZ

Acrónimo de Pan, Tilt, Zoom. Las cámaras PTZ son sistemas accionados por motor que permiten que la cámara se mueva horizontal y verticalmente, verticalmente, hacia arriba y hacia abajo, y acerque y aleje el zoom.

USB

Acrónimo de Universal Serial Bus. USB es un estándar de bus serie plug-and-play para interconectar dispositivos a una computadora host.

## 25.3 Preguntas frecuentes

25.3.1 ¿Por qué hay una parte de los canales que muestra “Sin recursos” o se vuelve negra la pantalla en la vista en vivo de múltiples pantallas?

### Razón

1. La resolución de la subtransmisión o la configuración de la tasa de bits no son adecuadas.
2. Error en la conexión de la subtransmisión.

### Solución

1. Vaya a Cámara → Parámetros de video → Subtransmisión . Seleccione el canal y baje el volumen.

Resolución y tasa de bits máxima (la resolución debe ser menor a 720p, la tasa de bits máxima debe ser menor a 2048 Kbps).



Nota

Si su grabadora de video le informa que no admite esta función, puede iniciar sesión en la cámara y ajustar los parámetros de video a través del navegador web.

2. Configure correctamente la resolución de la subtransmisión y la tasa de bits máxima (la resolución debe ser inferior a 720p, la tasa de bits máxima debe ser inferior a 2048 Kbps), luego elimine el canal y agréguelo nuevamente.

### 25.3.2 ¿Por qué la grabadora de video notifica una contraseña riesgosa después de agregar una cámara de red?

#### Razón

La contraseña de la cámara es demasiado débil.

#### Solución

Cambiar la contraseña de la cámara.



#### Advertencia

Le recomendamos encarecidamente que cree una contraseña segura de su elección (con un mínimo de 8 caracteres, incluyendo al menos tres de las siguientes categorías: mayúsculas, minúsculas, números y caracteres especiales) para aumentar la seguridad de su producto. También le recomendamos que restablezca su contraseña periódicamente, especialmente en el sistema de alta seguridad. Restablecerla mensual o semanalmente le ayudará a proteger mejor su producto.

---

### 25.3.3 ¿Por qué el grabador de video notifica que el tipo de transmisión no es compatible?

#### Razón

El formato de codificación de la cámara no coincide con el de la grabadora de vídeo.

#### Solución

Si la cámara utiliza H.265/MJPEG para la codificación, pero la grabadora de video no admite H.265/MJPEG, cambie el formato de codificación de la cámara al mismo que el de la grabadora de video.

### 25.3.4 ¿Cómo confirmar que la grabadora de video está usando H.265 para grabar video?

#### Solución

Compruebe si el tipo de codificación en la barra de herramientas de vista en vivo es H.265.

### 25.3.5 ¿Por qué el grabador de video notifica conflicto de IP?

#### Razón

La grabadora de vídeo utiliza la misma dirección IP que otros dispositivos.

#### Solución

Cambie la dirección IP de la grabadora de video. Asegúrese de que no coincida con la de otros dispositivos.

### 25.3.6 ¿Por qué la imagen se bloquea al reproducirla con cámaras de un solo canal o de varios canales?

#### Razón

Excepción de lectura/escritura de HDD.

#### Solución

Exporta el video y reproducélo en otros dispositivos. Si se reproduce correctamente en otro dispositivo, cambia el disco duro y vuelve a intentarlo.

### 25.3.7 ¿Por qué el dispositivo no puede controlar la cámara PTZ a través de coaxitron?

#### Razón

1. La cámara no es compatible con coaxitron.
2. El protocolo coaxitron es incorrecto.
3. La señal se ve afectada por el transceptor óptico de vídeo.

#### Solución

1. Asegúrese de que la señal de entrada de video sea HDTVl y que la cámara admita coaxitron.
2. Asegúrese de que los parámetros del protocolo coaxitron sean correctos, como la velocidad en baudios y la dirección.
3. Retire el transceptor óptico de vídeo y vuelva a intentarlo.

### 25.3.8 ¿Por qué el PTZ parece no responder a través de RS-485?

#### Razón

1. El cable RS-485 no está conectado correctamente.
2. La interfaz RS-485 está rota.
3. El protocolo de control no es correcto.

#### Solución

1. Compruebe si el cable RS-485 está conectado correctamente.
2. Cambie la interfaz RS-485 y vuelva a intentarlo.
3. Asegúrese de que el protocolo de control sea Pelco.

### 25.3.9 ¿Por qué la calidad del sonido del vídeo no es buena?

## Razón

1. El dispositivo de entrada de audio no tiene un buen efecto en la recopilación de sonido.
2. Interferencia en la transmisión.
3. El parámetro de audio no está configurado correctamente.

## Solución

1. Compruebe si el dispositivo de entrada de audio funciona correctamente. Puede cambiarlo.  
y vuelve a intentarlo.
2. Verifique la línea de transmisión de audio. Asegúrese de que todas las líneas estén bien conectadas o soldadas y que no haya interferencia electromagnética.
3. Ajuste el volumen del audio según el entorno y el dispositivo de entrada de audio.

## 25.4 Notificación de gas corrosivo

En salas que no sean de centro de datos, se recomienda que el límite de concentración de gas corrosivo cumpla con requisitos de la sustancia química activa de nivel 3C2 en IEC 60721-3-3:2002.

Tabla 25-1 Límite de concentración de gas corrosivo

Categoría de gas corrosivo	Valor promedio (mg/m <sup>3</sup> )	Valor máximo (mg/m <sup>3</sup> )
SO <sub>2</sub> (dióxido de azufre)	0.3	1.0
H <sub>2</sub> S (sulfuro de hidrógeno)	0.1	0.5
Cl <sub>2</sub> (cloro)	0.1	0.3
HCl (cloruro de hidrógeno)	0.1	0.5
HF (fluoruro de hidrógeno)	0.01	0.03
NH <sub>3</sub> (amoníaco)	1.0	3.0
O <sub>3</sub> (Ozono)	0.05	0.1
NO <sub>x</sub> (Óxidos de nitrógeno)	0.5	1.0



Nota

- Los valores promedio en la tabla anterior son límites de control típicos para gases corrosivos en la máquina.  
Ambiente ambiente. En general, no se recomienda que la concentración de gases corrosivos superar el valor medio.
- El valor máximo se refiere al valor límite o pico. La duración del gas corrosivo  
La concentración para alcanzar el valor máximo no debe exceder los 30 minutos diarios.

Tabla 25-2 Categorías y fuentes comunes de gases corrosivos

Categoría	Fuentes primarias
H <sub>2</sub> S (sulfuro de hidrógeno)	Emisiones geotérmicas, actividad microbiana, fabricación de petróleo, corrosión de la madera, tratamiento de aguas residuales, etc.
SO <sub>2</sub> (dióxido de azufre), SO <sub>3</sub> (azufre Trióxido)	Combustión de carbón, productos derivados del petróleo, gases de escape de automóviles, fundición de minerales, fabricación de ácido sulfúrico, combustión de tabaco, etc.
S (Azufre)	Talleres de fundición, fabricación de azufre, etc.
HF (fluoruro de hidrógeno)	Fabricación de fertilizantes, fabricación de aluminio, fabricación de cerámica, fabricación de acero, fabricación de equipos electrónicos, combustión de minerales, etc.
NO <sub>x</sub> (Óxidos de nitrógeno)	Escape de automóviles, combustión de petróleo, actividad microbiana, industria química, etc.
NH <sub>3</sub> (amoníaco)	Actividad microbiana, aguas residuales, fabricación de fertilizantes, emisiones geotérmicas, etc.
CO (monóxido de carbono)	Combustión, escape de automóviles, actividad microbiana, descomposición de árboles, etc.
Cl <sub>2</sub> (cloro), ClO <sub>2</sub> (cloro Dióxido)	Fabricación de cloro, fabricación de aluminio, fabricación de zinc, descomposición de residuos, etc.
HCl (cloruro de hidrógeno)	Escapes de automóviles, combustión, incendios forestales, combustión de polímeros en procesos marinos, etc.
HBr (ácido bromhídrico), HI (Ácido yodhídrico)	Escape de automóviles, etc.
O <sub>3</sub> (Ozono)	Procesos ópticos atmosféricos (incluidos principalmente óxido nítrico y peróxido de hidrógeno), etc.
C <sub>n</sub> H <sub>n</sub> (alcano)	Escapes de automóviles, quema de tabaco, desechos animales, aguas residuales, descomposición de árboles, etc.



See Far, Go Further

[www.rosarioseguridad.com.ar](http://www.rosarioseguridad.com.ar)

✉ [ventas@rosarioseguridad.com.ar](mailto:ventas@rosarioseguridad.com.ar)

☎ +54 9 341 6708000

☎ +54 9 341 6799822

📷 [rosarioseguridadok](https://www.instagram.com/rosarioseguridadok)

📺 Rosario Seguridad

📘 Rosario Seguridad

Grupo Instaladores

📘 <https://www.facebook.com/groups/591852618012744/>

☎ +54 9 341 6591429

☎ +54 9 341 4577532

Avenida Pellegrini 4820-Presidente Perón 3998 - Rosario - Santa Fe - Argentina