

Grabador de vídeo en red

Guía de inicio rápido








Prefacio

General

Esta guía de inicio rápido (en adelante, "el Manual") presenta las funciones y operaciones del dispositivo NVR (en adelante, "el NVR").

Instrucciones de seguridad

Las siguientes palabras de señalización categorizadas con significado definido pueden aparecer en el Manual.

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

Revisión histórica

Versión	Contenido de revisión	Tiempo de liberación
V1.0.0	Primer lanzamiento.	julio 2020

Aviso de protección de privacidad

Como usuario de NVR o controlador de datos, puede recopilar datos personales de otras personas, como rostro, huellas dactilares, número de placa del automóvil, dirección de correo electrónico, número de teléfono y GPS. Debe cumplir con las leyes y regulaciones locales de protección de la privacidad para proteger los derechos e intereses legítimos de otras personas mediante la implementación de medidas que incluyen, entre otras: proporcionar una identificación clara y visible para informar al interesado la existencia de un área de vigilancia y proporcionar información relacionada. contacto.

Acerca del Manual

- El Manual es sólo para referencia. Si hay inconsistencia entre el Manual y el producto real, prevalecerá el producto real.
- No somos responsables de ninguna pérdida causada por las operaciones que no cumplan con el Manual.
- El Manual se actualizará de acuerdo con las últimas leyes y regulaciones de las regiones relacionadas. Para obtener información detallada, consulte el manual en papel, el CD-ROM, el código QR o nuestro sitio web oficial. Si hay inconsistencia entre el manual en papel y la versión electrónica, prevalecerá la versión electrónica.
- Todos los diseños y software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto pueden causar algunas diferencias entre el producto real y el Manual. Contacta el

Servicio al cliente para obtener el programa más reciente y documentación complementaria.

- Aún así puede haber desviaciones en los datos técnicos, funciones y descripción de operaciones, o errores de impresión. Si hay alguna duda o disputa, consulte nuestra explicación final.
- Actualice el software del lector o pruebe otro software de lectura convencional si no se puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas comerciales registradas y nombres de empresas que aparecen en el Manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, comuníquese con el proveedor o con el servicio de atención al cliente si ocurre algún problema al usar el NVR.
- Si hay alguna incertidumbre o controversia, consulte nuestra explicación final.

Salvaguardias y advertencias importantes

La siguiente descripción es el método de aplicación correcto del NVR. Lea atentamente el manual antes de usarlo para evitar peligros y pérdidas de propiedad. Cumpla estrictamente con el Manual durante la aplicación y consérvelo adecuadamente después de leerlo.

Requisitos operativos

- Instale las cámaras PoE en interiores.
- No coloque ni instale el NVR en un área expuesta a la luz solar directa o cerca de dispositivos generadores de calor.
- No instale el NVR en un área húmeda, polvorienta o fuliginosa.
- Mantenga su instalación horizontal o instálelo en lugares estables y evite que se caiga.
- No gotee ni salpique líquidos sobre el NVR; No coloque sobre el NVR nada que esté lleno de líquidos para evitar que los líquidos fluyan hacia el NVR.
- Instale el NVR en lugares bien ventilados; no bloquee su abertura de ventilación.
- Utilice el NVR sólo dentro del rango nominal de entrada y salida.
- No desmonte el NVR arbitrariamente.
- Transporte, utilice y almacene el NVR dentro del rango de humedad y temperatura permitido.

requerimientos de energía

- Utilice baterías según los requisitos. De lo contrario, ¡puede haber riesgo de incendio, explosión o quemaduras en las baterías!
- Para reemplazar las baterías, sólo se pueden utilizar baterías del mismo tipo.
- **Deseche las baterías agotadas según las instrucciones.**
- Utilice cables eléctricos dentro de las especificaciones nominales recomendadas por las regulaciones locales.
- Utilice un adaptador de corriente estándar compatible con este NVR. De lo contrario, el usuario asumirá las lesiones personales resultantes o los daños al NVR.
- Utilice una fuente de alimentación que cumpla con los requisitos SELV (voltaje extra bajo de seguridad) y suministre energía con un voltaje nominal que cumpla con la fuente de alimentación limitada en IEC60950-1. Para conocer los requisitos específicos de la fuente de alimentación, consulte las etiquetas del dispositivo.
- Los productos con estructura de categoría I se conectarán a una toma de corriente de red, que está equipada con una conexión a tierra de protección.
- El acoplador del aparato es un dispositivo de desconexión. Durante el uso normal, mantenga un ángulo que facilite la operación.

Tabla de contenido

Prefacio.....	I
Salvaguardias y advertencias importantes.....	III 1
Operaciones Locales.....	1
1.1 Iniciar el NVR.....	1
1.2 Inicializando el NVR.....	1
1.3 Configuración de la red.....	4
1.4 Agregar cámara IP.....	6
1.4.1 Inicialización de la cámara IP.....	6
1.4.2 Agregar cámara IP por resultado de búsqueda.....	10
1.4.3 Agregar cámara IP manualmente.....	12
1.5 Configuración del cronograma de almacenamiento de videos grabados.....	15
1.6 Configuración de ajustes P2P.....	17
1.6.1 Habilitación de la función P2P.....	17
1.6.2 Agregar el NVR al cliente de teléfono inteligente.....	18
1.7 Detección de movimiento inteligente.....	19
1.8 Vista en vivo.....	21
1.9 Reproducción de grabación.....	23
2 Iniciar sesión en la web.....	25
Apéndice 1 Recomendaciones de ciberseguridad.....	26

1 Operaciones Locales



Se pueden encontrar ligeras diferencias en las interfaces de diferentes modelos. Las siguientes cifras son para solo referencia. El producto real prevalecerá.

1.1 Iniciar el NVR

Antes de iniciar el NVR, asegúrese de que:

- El voltaje de entrada nominal coincide con los requisitos de energía del NVR.
- La conexión del cable de alimentación está lista.
- Para la seguridad del dispositivo, primero conecte el NVR al adaptador de corriente y luego conéctelo a la toma de corriente.
- Utilice siempre corriente estable. Se recomienda utilizar UPS como fuente de energía.

1.2 Inicializando el NVR

Este tema muestra cómo inicializar el NVR antes de usarlo.

Información de contexto

Al iniciar por primera vez, debe configurar la información de contraseña para **administración** (por defecto). Para garantizar la seguridad del dispositivo, le recomendamos encarecidamente que guarde correctamente la contraseña de inicio de sesión y la modifique periódicamente.

Procedimiento

Paso 1 Encienda el NVR.

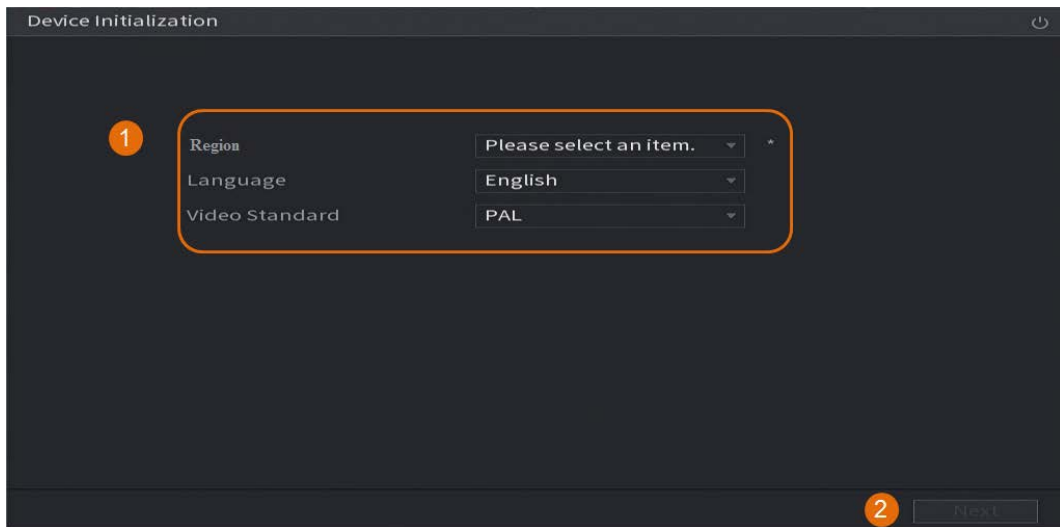
El sistema ingresa a la interfaz de inicialización del dispositivo.

Paso 2 En las listas desplegables, seleccione la región, el idioma y el estándar de video según sea necesario.



Puede cambiar estas configuraciones en las páginas de configuración del NVR después de la inicialización.

Figura 1-1 Establecer ubicación, idioma y estándar de video

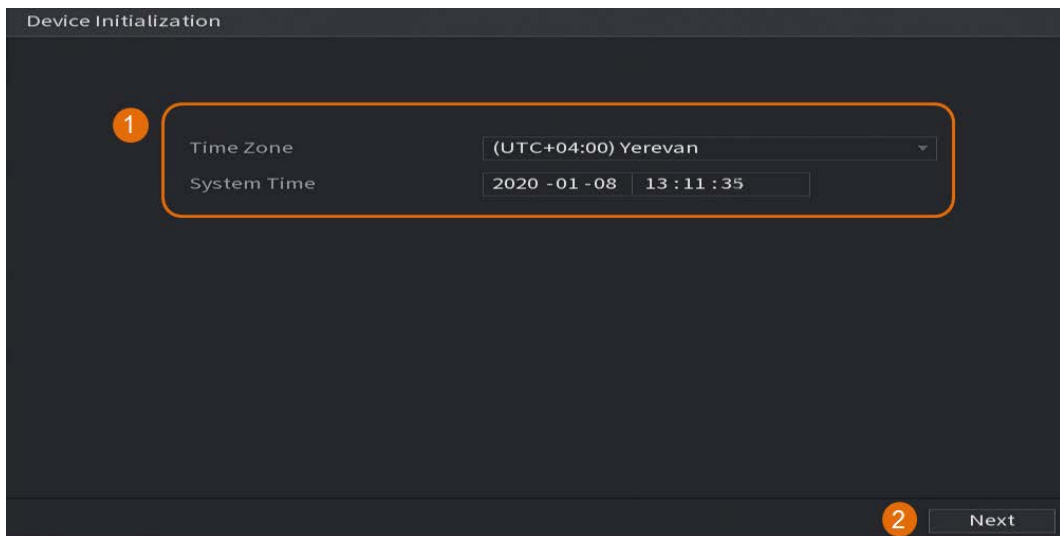


Paso 3 Hacer clic **Próximo**.

Etapa 4 Lea el Acuerdo de licencia de software y seleccione **He leído y acepto todos los términos**, y luego haga clic en **Próximo**.

Paso 5 Seleccione la zona horaria y configure la hora del sistema, y luego haga clic en **Próximo**.

Figura 1-2 Configurar la zona horaria y la hora del sistema



Paso 6 Configure la información de contraseña para el administrador del dispositivo y luego haga clic en **Próximo**.

Figura 1-3 Configurar la información de contraseña

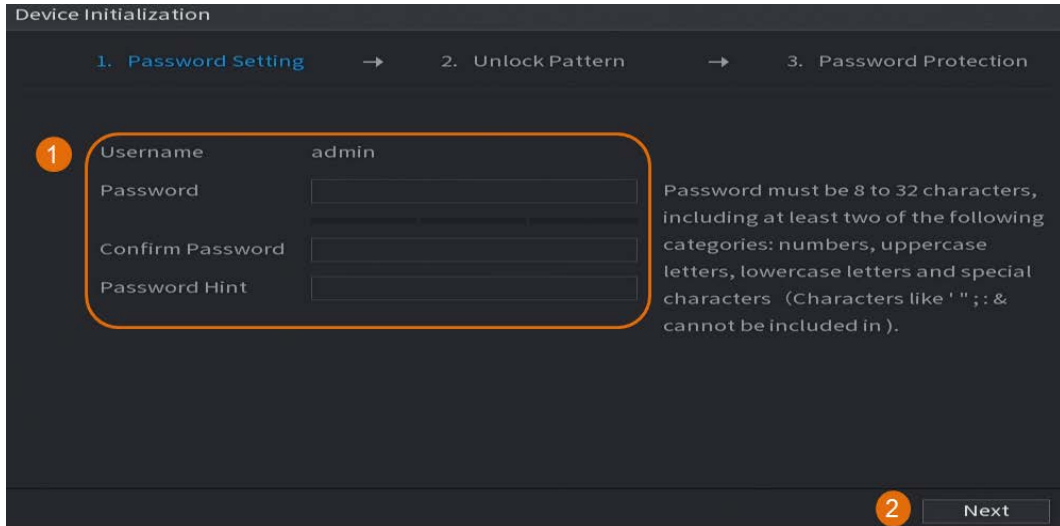



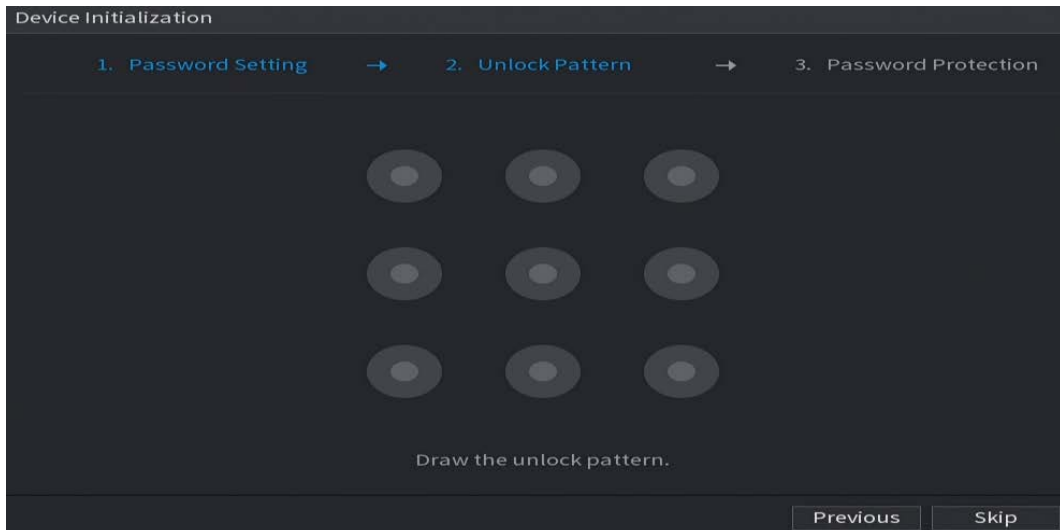


Tabla 1-1 Información de contraseña

Parámetro	Descripción
Nombre de usuario	Por defecto, el usuario es administración y no puedes cambiarlo.
Contraseña	Ingrese una nueva contraseña para el administrador del dispositivo en Contraseña y confirme la contraseña en el siguiente campo.
confirmar Contraseña	 La nueva contraseña se puede configurar desde 8 caracteres hasta 32 caracteres y contiene al menos dos tipos de números, letras y caracteres especiales (excluyendo "", "", ";", ":" y "&").
Pista de la contraseña	Ingrese una pregunta rápida que lo ayudará a recordar la contraseña de su dispositivo.  En la interfaz de inicio de sesión, haga clic en  y se mostrará el mensaje para ayudarlo a restablecer la contraseña.

Paso 7 (Opcional) Utilice el mouse para dibujar un patrón de desbloqueo y luego vuelva a dibujarlo para confirmarlo.

Figura 1-4 Dibujar un patrón de desbloqueo



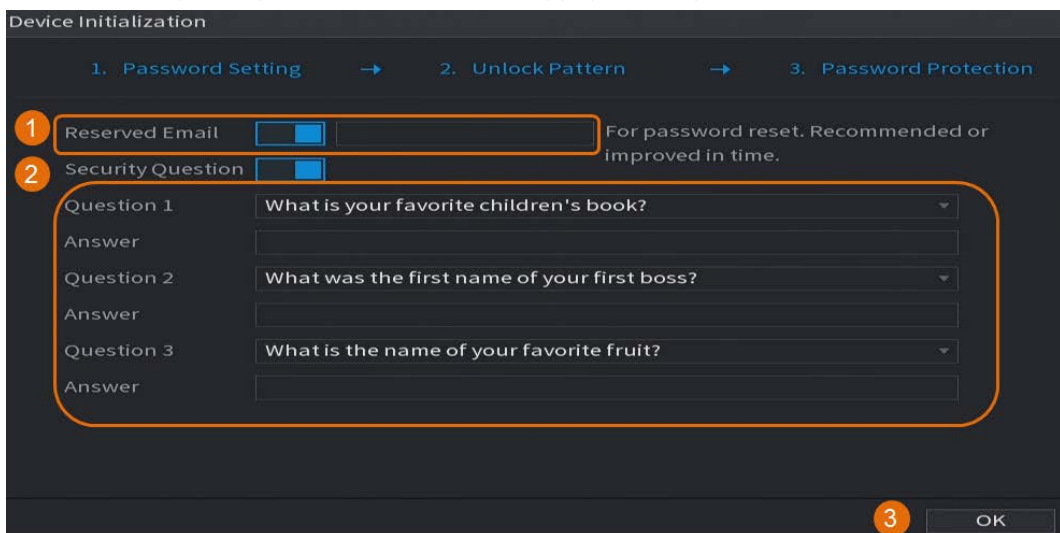
- El patrón que desea establecer debe cruzar al menos cuatro puntos.
- Si no desea configurar el patrón de desbloqueo, haga clic en **Saltar**.
- Una vez que haya configurado el patrón de desbloqueo, se utilizará como predeterminado método de autenticación. Si omite esta configuración, ingrese la contraseña para iniciar sesión.

Paso 8

(Opcional) Aplique el correo electrónico reservado y las preguntas de seguridad al NVR.

- Permitir **Correo electrónico reservado** e ingrese la dirección de correo electrónico.
- Permitir **Pregunta de seguridad** y seleccione preguntas de las listas desplegables para **Pregunta 1**, **Pregunta 2**, y **Pregunta 3** y luego ingrese las respuestas a esas preguntas.

Figura 1-5 Aplicar correo electrónico reservado y preguntas de seguridad



Paso 9

Hacer clic **DE ACUERDO**.

1.3 Configuración de la red

Puede configurar los ajustes básicos de la red, como el modo de red, la versión de IP y la dirección IP del NVR.

Paso 1 Seleccionar **Menú principal > RED > TCP/IP**.

Paso 2 Configurar parámetros.



También puede configurar los parámetros de red en el Asistente de inicio.

Figura 1-6 TCP/IP

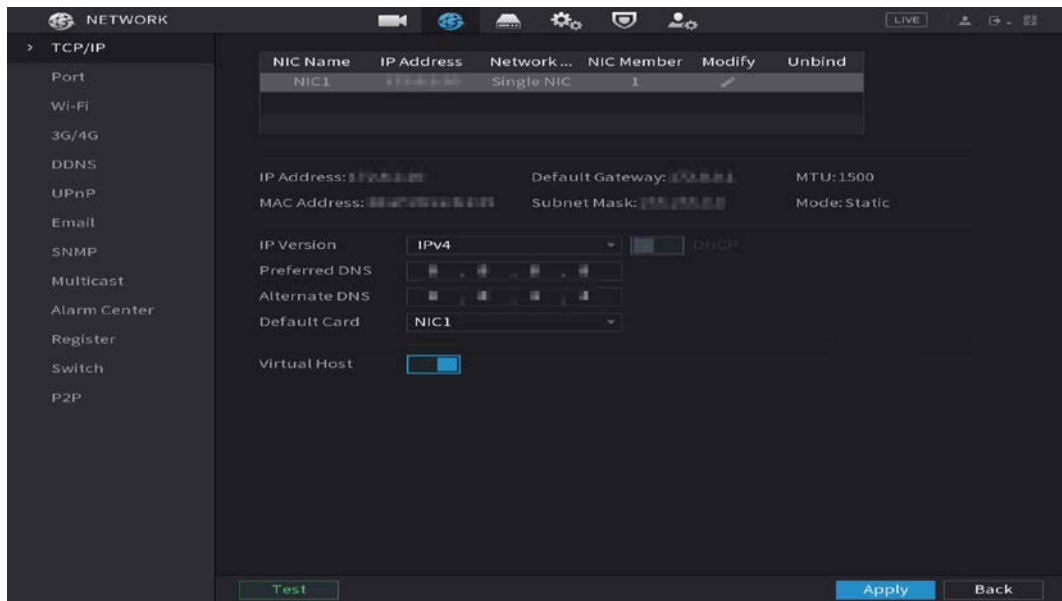



Tabla 1-2 Parámetros TCP/IP

Parámetro	Descripción
Versión IP	En el Versión IP lista, puede seleccionar IPv4 o IPv6 . Ambas versiones son compatibles para el acceso.
Dirección MAC	Muestra la dirección MAC del NVR.
DHCP	Habilite la función DHCP. La dirección IP, la máscara de subred y la puerta de enlace predeterminada no están disponibles para la configuración una vez que se habilita DHCP. <ul style="list-style-type: none"> ● Si DHCP es efectivo, la información obtenida se mostrará en el Dirección IP, Máscara de subred y Puerta de enlace predeterminada. De lo contrario, todos los valores muestran 0.0.0.0. ● Si la conexión PPPoE se realiza correctamente, la dirección IP, la máscara de subred, la puerta de enlace predeterminada y DHCP no estarán disponibles para la configuración.
Dirección IP	Ingrese la dirección IP y configure la máscara de subred correspondiente y la puerta de enlace predeterminada.  La dirección IP y la puerta de enlace predeterminada deben estar en la misma red segmento.
Máscara de subred	
Puerta de enlace predeterminada	
DNS preferido	Ingrese la dirección IP de DNS.
DNS alternativo	Ingrese la dirección IP del DNS alternativo.

Parámetro	Descripción
MTU	<p>Ingrese un valor para la tarjeta de red. El valor oscila entre 1280 bytes y 1500 bytes. El valor predeterminado es 1500.</p> <p>Los valores de MTU sugeridos son los siguientes.</p> <ul style="list-style-type: none"> ● 1500: El mayor valor del paquete de información Ethernet. Este valor normalmente se selecciona si no hay una conexión PPPoE o VPN, y también es el valor predeterminado de algunos enrutadores, adaptadores de red y conmutadores. ● 1492: Valor optimizado para PPPoE. ● 1468: Valor optimizado para DHCP. ● 1450: valor optimizado para VPN.
Prueba	Hacer clic Prueba para probar si la dirección IP ingresada y la puerta de enlace están interfundionando.

Paso 3 Hacer clic **DE ACUERDO**.

1.4 Agregar cámara IP

Puede agregar una cámara IP mediante el resultado de la búsqueda o ingresando manualmente la información de IP.



Las cámaras que desee agregar deben estar en la misma red que el NVR.

1.4.1 Inicialización de la cámara IP

El tema muestra cómo inicializar cámaras nuevas o las cámaras después de restaurar los valores predeterminados de fábrica.

Información de contexto

La cámara IP deberá inicializarse antes de conectarse a un NVR; de lo contrario, la conexión fallará. La inicialización cambiará la contraseña de inicio de sesión y la dirección IP de la cámara IP.



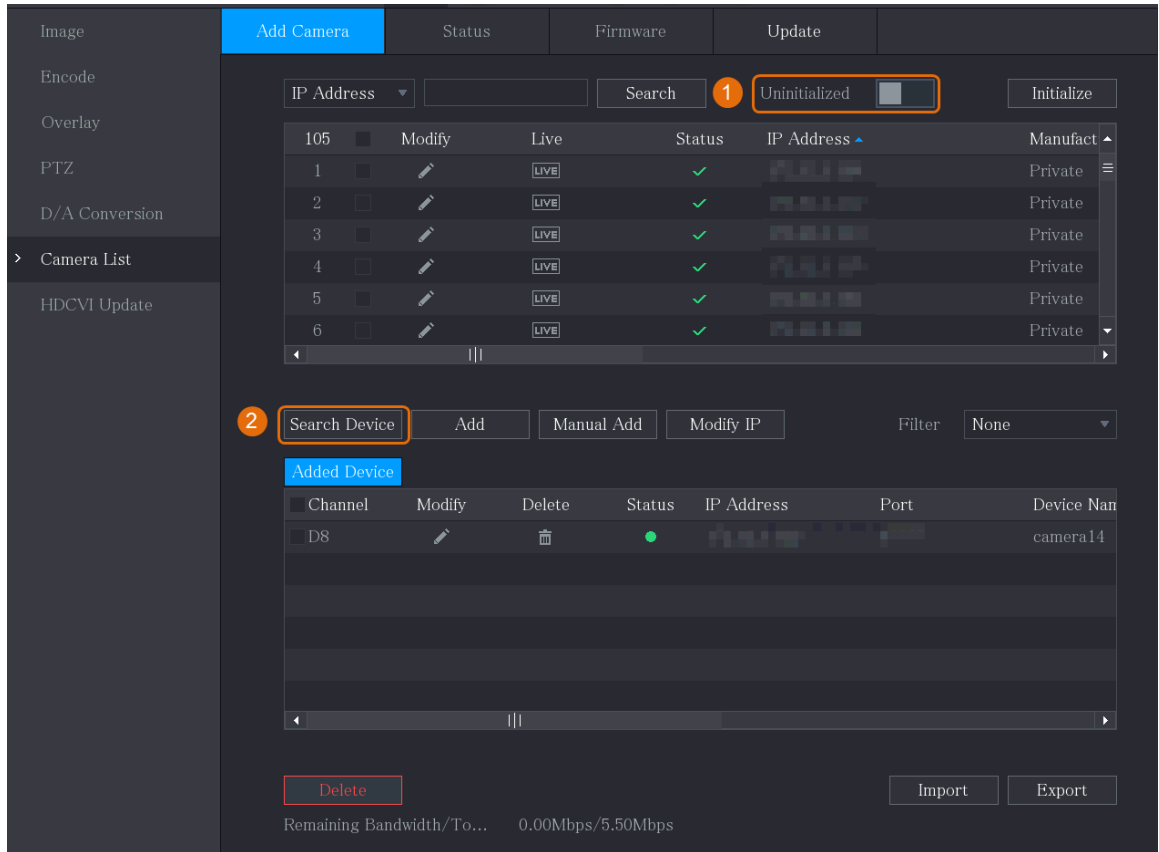
Cuando conecte una cámara al NVR a través del puerto PoE, el NVR inicializará automáticamente el cámara. Y la cámara adopta la contraseña y la información de correo electrónico del NVR de forma predeterminada.

Procedimiento

Paso 1 Seleccionar **Menú principal > Cámara > Lista de cámaras > Agregar cámara**.

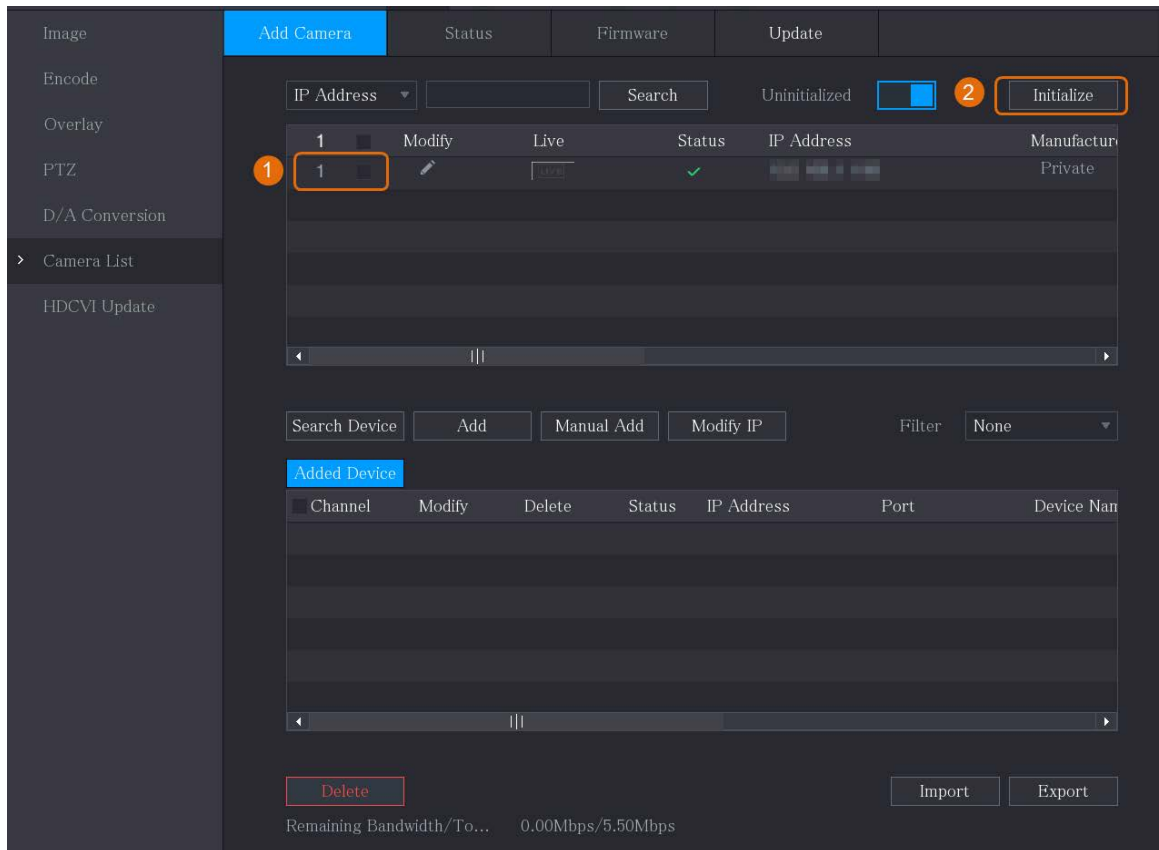
Paso 2 Permitir **No inicializado** y luego haga clic en **Dispositivo de búsqueda**.

Figura 1-7 Buscar dispositivo no inicializado



Paso 3 Seleccione la cámara que desea inicializar y luego haga clic en **Inicializar**.

Figura 1-8 Inicializar la cámara



Etapa 4 Aplique la contraseña y la información de correo electrónico a la cámara IP.

- Utilice la configuración del NVR.

1. Seleccione **Usando la contraseña actual del dispositivo y la información de correo electrónico.**



Esta casilla de verificación está seleccionada por defecto.

Figura 1-9 Aplicar la configuración del dispositivo

Enter Password

1 Using current device password and email info.

2 Next

2. Haga clic **Próximo.**

● Establezca manualmente la contraseña y la información de correo electrónico.

1. Cancele **Usando la contraseña actual del dispositivo y la información de correo electrónico.**

Figura 1-10 Establecer contraseña

Enter Password

1 Using current device password and email info.

2

User	admin
Password	<input type="password"/>
Confirm Password	<input type="password"/>

Use a password that has 8 to 32 characters, it can be a combination of letter(s), number(s) and symbol(s) with at least two kinds of them.(please do not use special symbols like ' ; : &)

3 Next

2. Establecer contraseña.

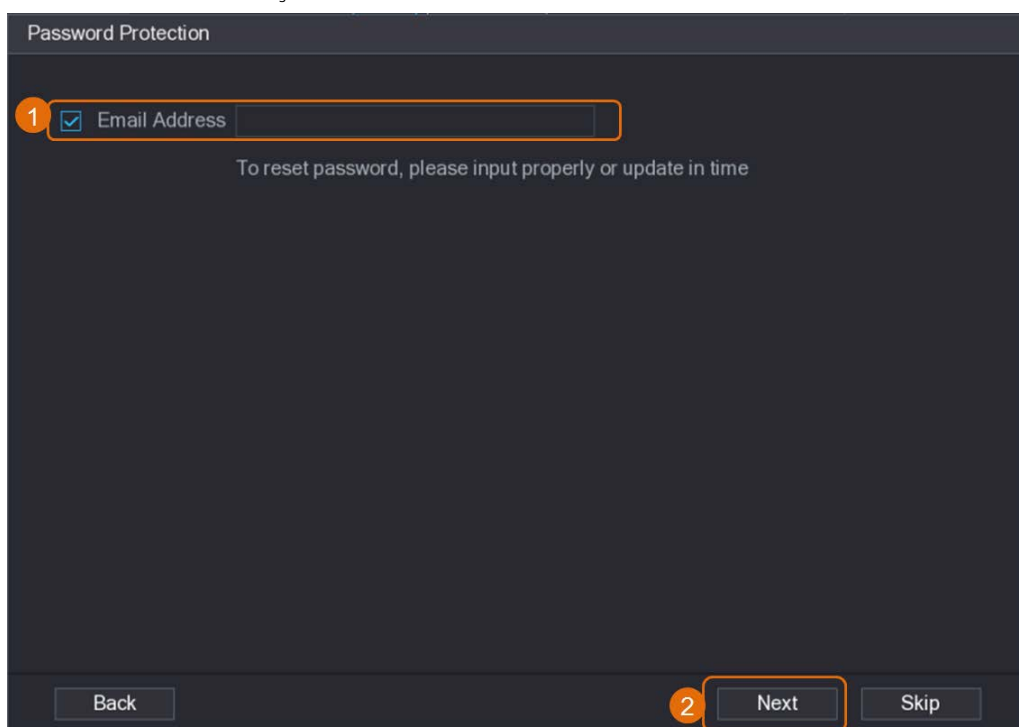
Tabla 1-3 Contraseña

Parámetro	Descripción
Usuario	El valor predeterminado es administración no se puede cambiar.
Contraseña	La nueva contraseña se puede configurar de 8 a 32 caracteres y contiene al menos dos tipos de números, letras y caracteres especiales (excluyendo " " , " " , " " , " " , " " y "&").
confirmar Contraseña	Ingrese una contraseña segura de acuerdo con la indicación de la barra de seguridad de la contraseña.

3. Haga clic **Próximo**.

4. Ingrese una dirección de correo electrónico y haga clic **Próximo**.

Figura 1-11 Establecer información de correo electrónico



Paso 5 Configure la dirección IP de la cámara.

- Seleccionar **DHCP** si hay un servidor DHCP implementado.
- Seleccionar **Estático** y luego ingrese la dirección IP, la máscara de subred, la puerta de enlace predeterminada y el valor incremental.



Establezca el valor incremental cuando necesite cambiar las direcciones IP de varias cámaras de una sola vez. El NVR agregará gradualmente el valor a la cuarta sección de la IP dirección cuando asigne direcciones IP para esas cámaras.

Figura 1-12 Configurar la dirección IP

The screenshot shows a 'NETWORK' configuration window. At the top, it says 'Checked Device No.: 1'. There are two radio buttons: 'DHCP' (unselected) and 'STATIC' (selected). Below these are three input fields for 'IP Address', 'Subnet Mask', and 'Default Gateway', each with a small grid icon. To the right of the IP Address field is an 'Incremental Value' field with the number '1'. At the bottom of the window are three buttons: 'Back', 'Next', and 'Skip'.

- Paso 6** Hacer clic **Próximo**.
Espere de 1 a 2 minutos para que se complete la inicialización.
- Paso 7** Hacer clic **Finalizado**.

1.4.2 Agregar cámara IP por resultado de búsqueda

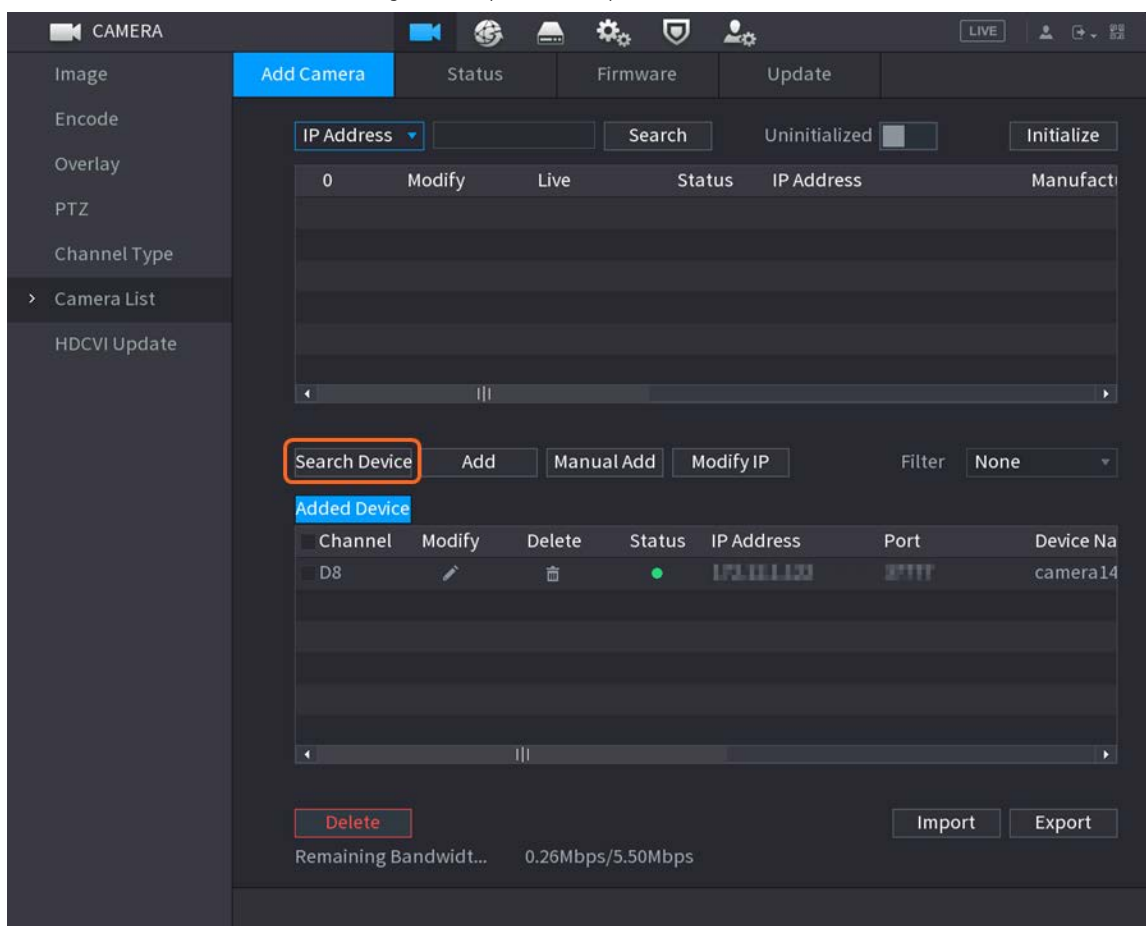
Requisitos previos

Asegúrese de que las cámaras que desea agregar ya se hayan inicializado y conectado a la red correcta.

Procedimiento

- Paso 1** Seleccionar **Menú principal > CÁMARA > Lista de cámaras > Agregar cámara**. Hacer clic
- Paso 2** **Dispositivo de búsqueda**.

Figura 1-13 Dispositivo de búsqueda



Paso 3 Agregue cámaras IP.

- Agregar haciendo doble clic: haga doble clic en la cámara de destino para agregarla a la lista.



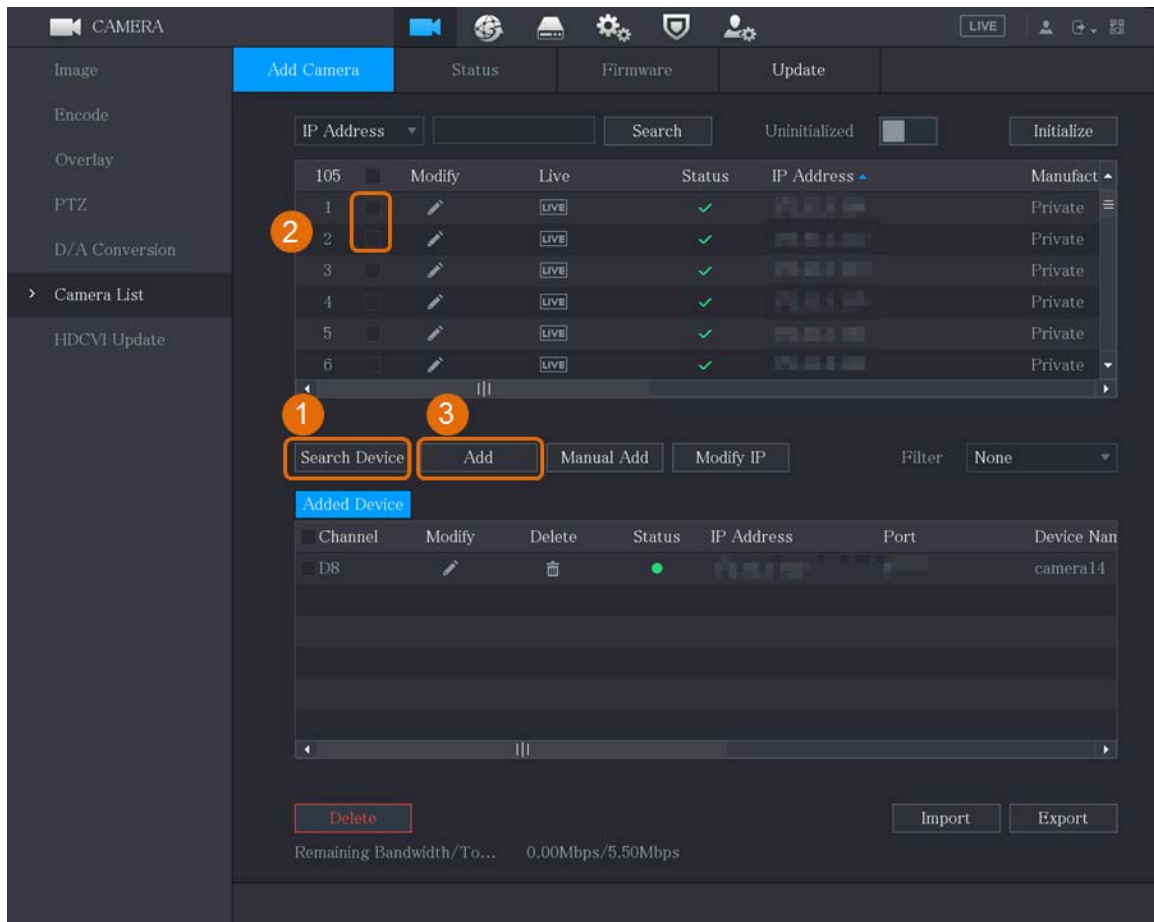
Puede agregar solo una cámara por resultado de búsqueda a la vez.

- Agregar mediante casilla de verificación: seleccione la casilla de verificación de la cámara de destino y luego haga clic en **Agregar** para agregarlo a la lista.



Puede seleccionar más de una casilla de verificación y agregar cámaras en lotes.

Figura 1-14 Agregar cámara IP por resultado de búsqueda



Resultado

- Si el estado de la cámara agregada es verde (), indica que la cámara se agregó correctamente al (NVR).
- Si el estado de la cámara agregada es rojo (), indica fallo de conexión entre la cámara y el NVR. Verifique los parámetros de la cámara, como contraseña, protocolo y número de canal, y luego intente agregarlos nuevamente.

1.4.3 Agregar cámara IP manualmente

Puede agregar una cámara IP mediante información de IP al mismo tiempo.

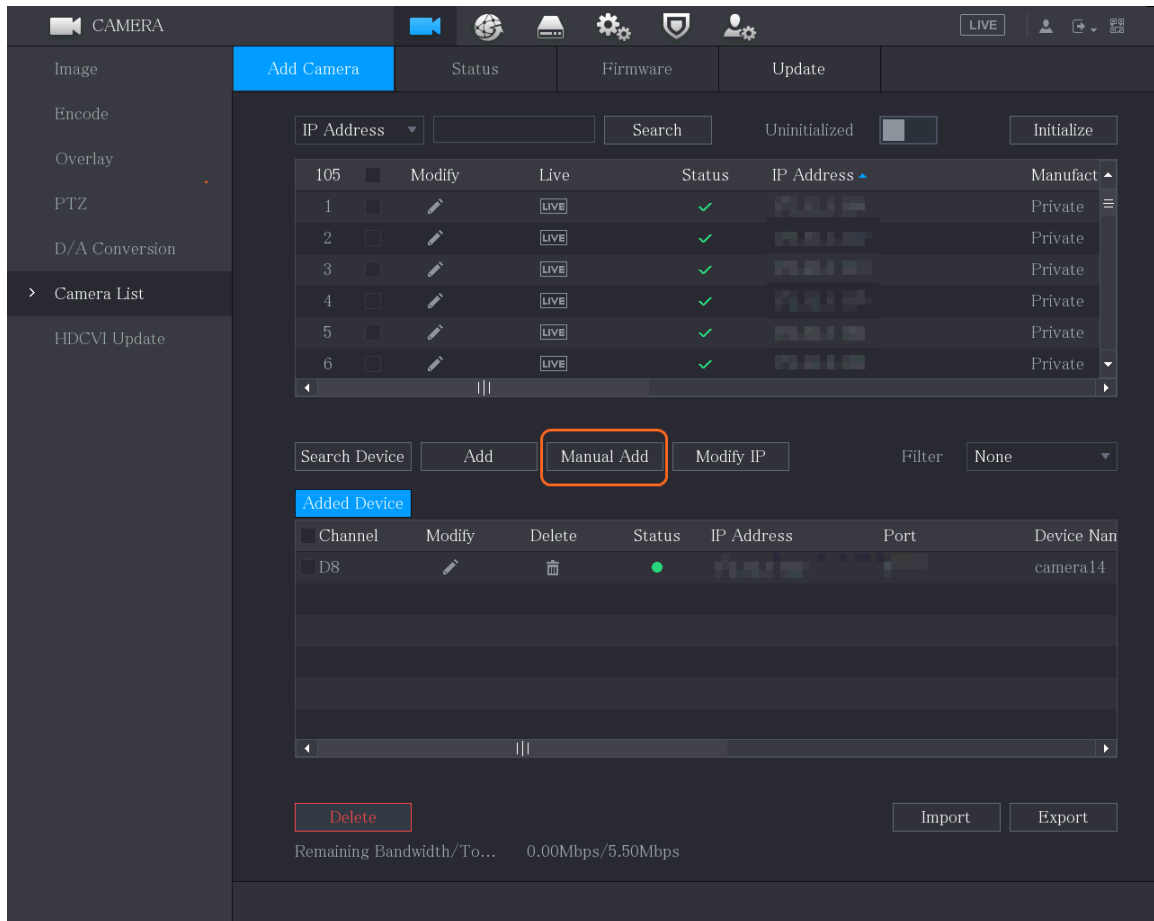
Requisitos previos

Asegúrese de que las cámaras que desea agregar ya se hayan inicializado y conectado a la red correcta.

Procedimiento

- Paso 1** Seleccionar **Menú principal > CÁMARA > Lista de cámaras > Agregar cámara**. Hacer clic
- Paso 2** **Agregar manualmente**.

Figura 1-15 Agregar manualmente



Paso 3 En el **Agregar manualmente** cuadro de diálogo, configure los parámetros.

Figura 1-16 Configurar parámetros de adición manual


The screenshot shows a 'Manual Add' configuration window with the following fields and values:

- Channel: D8
- Manufacturer: ONVIF
- IP Address: [Redacted]
- RTSP Port: Self-adaptive
- HTTP Port: 80
- Username: admin
- Password: [Redacted]
- Total Channels: [Redacted]
- Remote CH No.: D1
- Decode Strategy: General
- Encryption: Auto, TCP, UDP, MULTICAST

Buttons: Connect, Setting, OK, Cancel.

Tabla 1-4 Parámetros de adición manual

Parámetro	Descripción
Canal	Desde el Canal En la lista desplegable, seleccione el canal que desea usar en el NVR para conectar el dispositivo remoto.
Fabricante	Desde el Fabricante lista desplegable, seleccione el fabricante del dispositivo remoto.
Dirección IP	En el Dirección IP , ingrese la dirección IP de la cámara IP. Cambie el valor predeterminado (192.168.0.0) al que el sistema no puede conectarse.
Puerto RTSP	El valor predeterminado es 554. Puede cambiar el valor según sea necesario.
Puerto HTTP	El valor predeterminado es 80. Puede cambiar el valor según sea necesario. Si ingresa otro valor, por ejemplo, 70, entonces deberá ingresar 70 después de la dirección IP al iniciar sesión en el NVR mediante el navegador.
Puerto TCP	El valor predeterminado es 37777. Puede cambiar el valor según sea necesario.
Nombre de usuario	Ingrese el nombre de usuario del dispositivo remoto.
Contraseña	Ingrese la contraseña del usuario para el dispositivo remoto.
Número de canal remoto	Ingrese el número del canal remoto del dispositivo remoto que desea agregar.
Estrategia de decodificador	En el Estrategia de decodificador lista, seleccione Por defecto , Tiempo real , o Fluido según sea necesario.

Parámetro	Descripción
Tipo de protocolo	<ul style="list-style-type: none"> ● Si la cámara IP se agrega a través de un protocolo privado, seleccione tcp. ● Si la cámara IP se agrega a través del protocolo ONVIF, seleccione Auto, tcp, UDP, o MULTIDIFUSIÓN. ● Si la cámara IP se agrega a través de otros fabricantes, seleccione tcp o UDP.
Cifrado	<p>Si la cámara IP se agrega a través del protocolo ONVIF, habilitar la Cifrado. La casilla de verificación proporcionará protección de cifrado a los datos que se transmiten.</p>  <p>Para utilizar esta función, la función HTTPS debe estar habilitada para la cámara IP remota.</p>

Etapa 4 Hacer clic **DE ACUERDO**.

1.5 Configuración del cronograma de almacenamiento de videos grabados

De forma predeterminada, todas las cámaras graban videos continuamente las 24 horas del día. Puede modificar la configuración según sea necesario.



También puede configurar el programa de almacenamiento en el Asistente de inicio.

Procedimiento


Paso 1 Seleccionar **Menú principal > ALMACENAMIENTO > Cronograma > Registro**.

Figura 1-17 Programa de registro



Paso 2 Configurar parámetros.

Tabla 1-5 Parámetros de registro

Parámetro	Descripción
Canal	Desde el Canal lista desplegable, seleccione el canal para cambiar la configuración de grabación de video.
Enlatar	En el Enlatar , establezca el tiempo para capturar video adicional que ocurre antes de un evento para proporcionar contexto a una grabación. Rango de valores: 0 a 30 s.
Redundancia	<p>Permite a los usuarios configurar uno de los discos duros como disco duro redundante para guardar los archivos grabados en diferentes discos duros. En caso de falla del disco duro, puede encontrar la grabación de respaldo en el disco duro redundante.</p> <ul style="list-style-type: none"> ● Seleccionar Menú principal > ALMACENAMIENTO > Administrador de discos y luego configure un HDD como HDD redundante. ● Seleccionar Menú principal > ALMACENAMIENTO > Cronograma > Registro y luego seleccione el Redundancia casilla de verificación. <ul style="list-style-type: none"> ◇ Si el canal seleccionado no está grabando, la función de redundancia entrará en vigor la próxima vez que grabe sin importar si selecciona la casilla de verificación o no. ◇ Si el canal seleccionado está grabando, los archivos grabados actualmente se empaquetarán y luego comenzarán a grabar de acuerdo con el nuevo horario. <p></p> <ul style="list-style-type: none"> ● Esta función está disponible en modelos selectos. ● El disco duro redundante solo realiza copias de seguridad de los videos grabados, pero no de las instantáneas.
Tipo de evento	<p>Seleccione la casilla de verificación de los tipos de eventos.</p> <ul style="list-style-type: none"> ● General: Grabación general significa que el NVR graba todos los videos durante el período de tiempo especificado. La grabación general está representada por el color verde. ● Movimiento: Grabación de movimiento significa que el NVR graba video solo cuando se activa la detección de movimiento. La grabación de movimiento está representada por el color amarillo. ● Alarma: La grabación de alarma significa que el NVR graba video cuando se activa una alarma. La grabación de alarma está representada por el color rojo. ● MAMÁ: La grabación de fusiones y adquisiciones combina la grabación de movimiento y la grabación de alarma. El dispositivo graba video cuando se activa la detección de movimiento o cualquier alarma. El registro de fusiones y adquisiciones está representado por el color naranja. ● Inteligente: La grabación inteligente significa que el NVR graba video cuando se activa la detección inteligente. La grabación inteligente está representada por el color azul. ● punto de venta: La grabación de POS significa que el NVR graba video cuando se utiliza la máquina POS para realizar un pago. La grabación POS está representada por el color violeta.
Período	Define un período durante el cual la configuración de grabación configurada está activa. El sistema sólo activa la alarma en el período definido.

Parámetro	Descripción
Copiar a	Hacer clic Copiar a para copiar la configuración a otros canales.

Paso 3 Establezca el horario dibujando o editando.

- Dibujo: Mantenga presionado el botón izquierdo del mouse y arrastre el mouse para dibujar el período.
- Edición: Haga clic para configurar el período y luego haga clic en **DE ACUERDO**. Hacer clic **Aplicar**.

Etapa 4 clic **Aplicar**.



El programa de grabación configurado puede entrar en vigor sólo cuando la función de grabación automática está activada. Para obtener detalles sobre cómo habilitar la grabación automática, consulte el Manual del usuario.

1.6 Configuración de ajustes P2P

Puede utilizar el código QR para conectar un teléfono inteligente al NVR para su gestión.



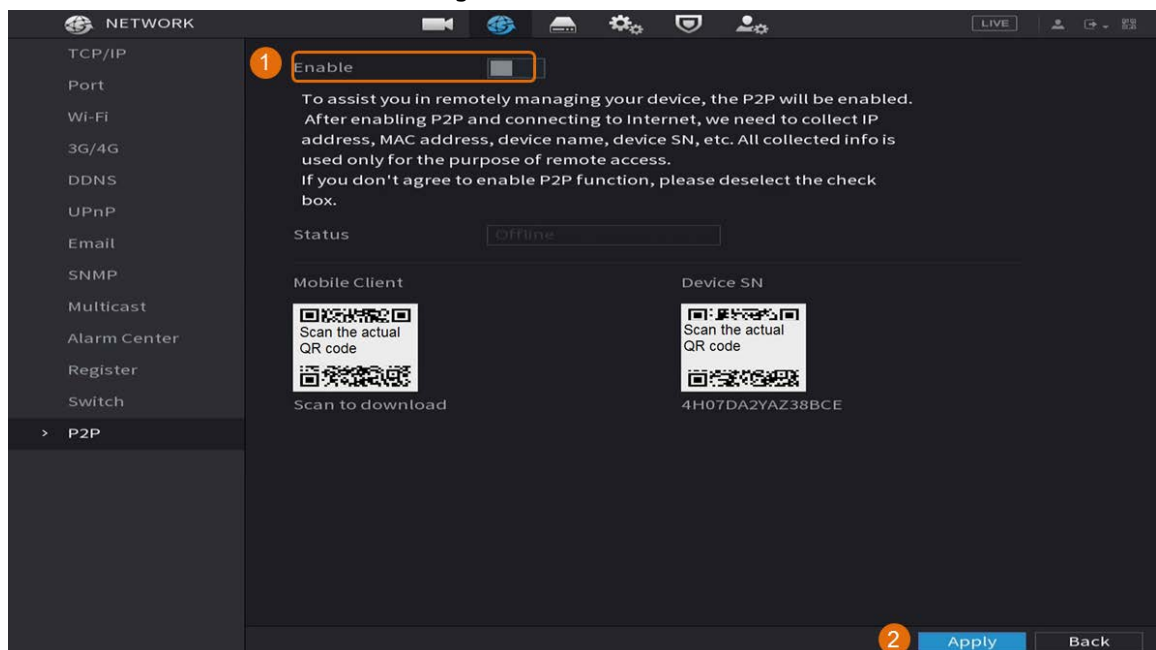
Asegúrese de que el NVR esté conectado a Internet y, en caso afirmativo, en el **Estado** caja del P2P interfaz, muestra **En línea**.

1.6.1 Habilitación de la función P2P

Debe ingresar a la interfaz P2P para habilitar la función P2P y escanear el código QR para descargar la aplicación del teléfono inteligente.

Paso 1 Seleccionar **Menú principal > RED > P2P**.

Figura 1-18 P2P




Paso 2 Hacer clic **Permitir** para habilitar la función P2P.

Paso 3 Hacer clic **Aplicar**

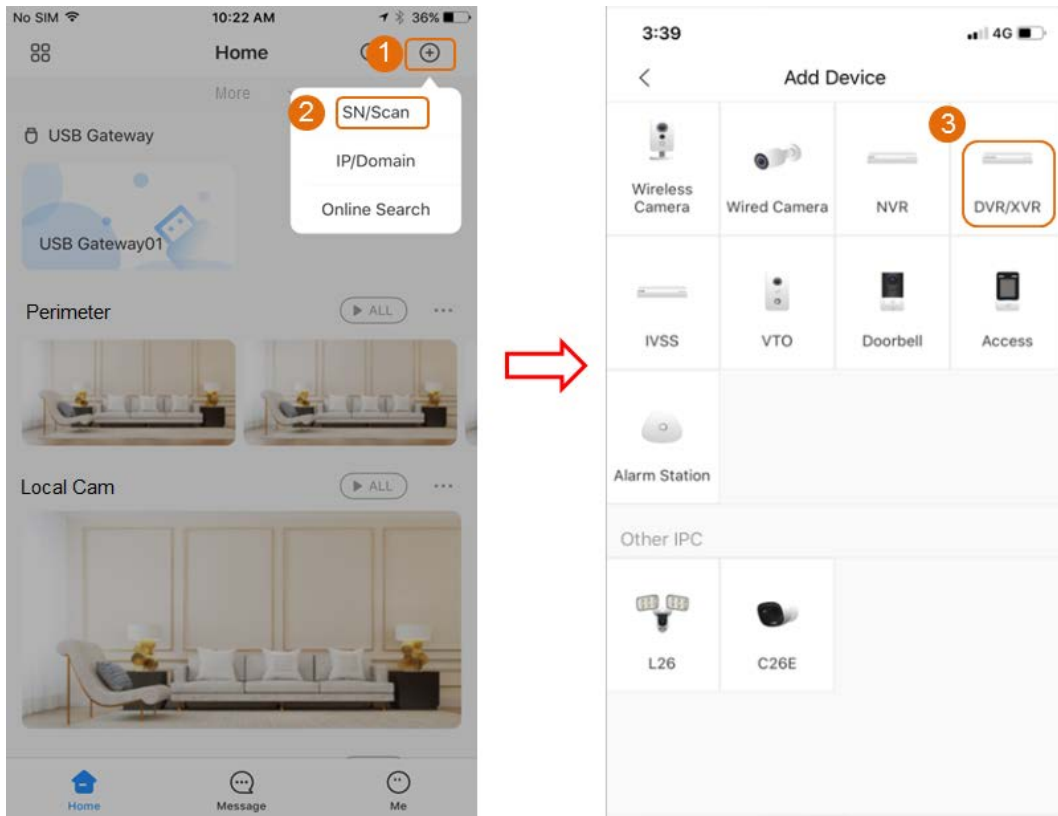
1.6.2 Agregar el NVR al cliente de teléfono inteligente

Este tema toma la adición del NVR al cliente de teléfono inteligente como ejemplo para la administración de teléfonos inteligentes.

Paso 1 Abra la aplicación y toque .

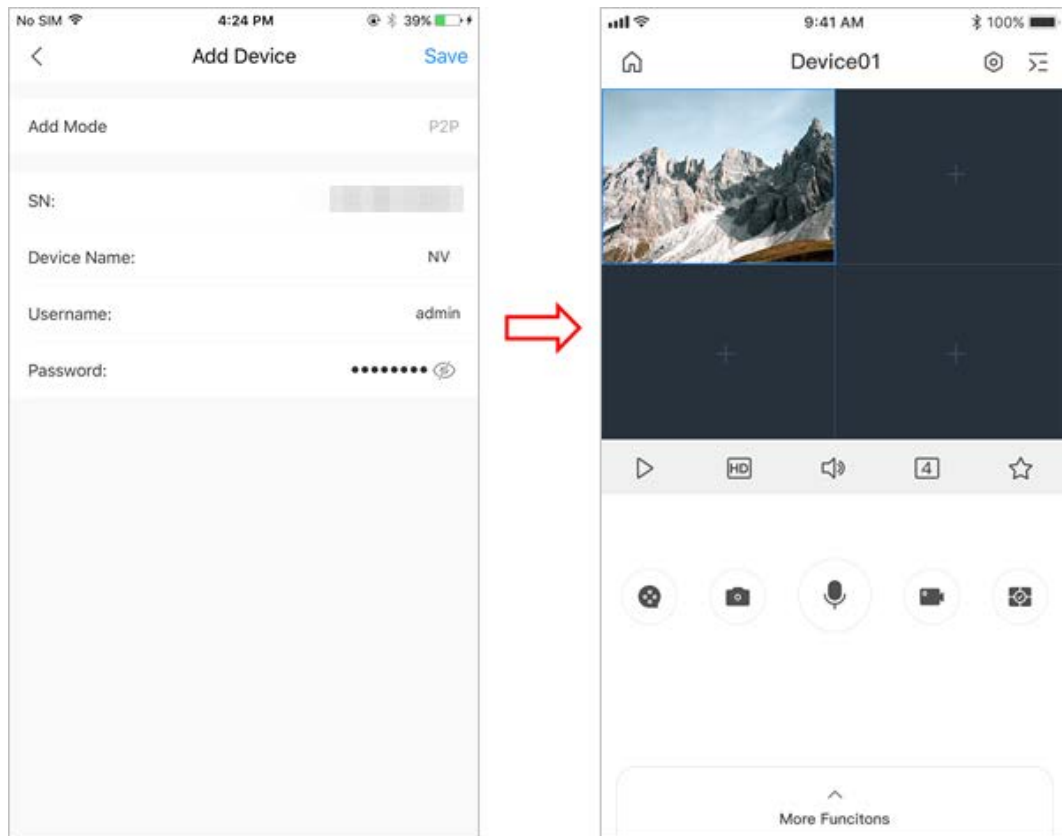
Paso 2 Seleccione **SN/escanear**.

Figura 1-19 Agregar dispositivo



Paso 3 Seleccione, ingrese un nombre y contraseña para el NVR y luego toque **Ahorrar**.

Figura 1-20 Iniciar vista en vivo



1.7 Detección de movimiento inteligente

Este tema muestra cómo configurar la detección de movimiento inteligente (SMD).

Información de contexto

La Detección de Movimiento Inteligente (SMD) es una función de monitoreo ideal para áreas poco pobladas donde desea una alerta de personas o vehículos en cualquier lugar de la escena sin tener que establecer reglas ni trazar líneas.

Procedimiento

Paso 1 Seleccionar **Menú principal > AI > Parámetro > SMD**.

Figura 1-21 SMD


The screenshot shows a configuration window for SMD linkage. The settings are as follows:







- Channel: D1 (dropdown)
- Enable: (checkbox)
- Sensitivity: Medium (dropdown)
- Effective Target: Human, Motor Vehicle
- Schedule: Setting (button)
- Anti-Dither: 0 sec. (input)
- Alarm-out Port: Setting (button)
- Post-Alarm: 0 sec. (input)
- Show Message: (checkbox)
- Report Alarm: (checkbox)
- Send Email: (checkbox)
- Record Channel: Setting (button)
- PTZ Linkage: Setting (button)
- Post-Record: 10 sec. (input)
- Tour: Setting (button)
- Picture Storage: (checkbox)
- Buzzer: (checkbox)
- Log: (checkbox)
- Alarm Tone: None (dropdown)

SMD linkage configuration synchronizes with MD linkage configuration.

Paso 2 Seleccione y habilite un canal y luego configure los parámetros.

Tabla 1-6

Parámetro	Descripción
Sensibilidad	Cuanto mayor sea el valor, más fácil será activar una alarma. Pero al mismo tiempo puede producirse una falsa alarma. Se recomienda el valor predeterminado.
Objetivo efectivo	Elija humano, vehículo motorizado o ambos.
Cronograma	Configure el periodo y en el rango horario establecido se vinculará el elemento de configuración correspondiente para iniciar la alarma.
Anti-vacilación	Indica el tiempo transcurrido desde el final de la detección de movimiento hasta el final de la acción de vinculación de la alarma. El rango es de 0 a 600 segundos.
Puerto de salida de alarma	El dispositivo de alarma (como luces, sirenas, etc.) está conectado al puerto de salida de alarma. Cuando ocurre una alarma, el dispositivo NVR transmite la información de la alarma al dispositivo de alarma.
Post-alarma	Cuando finaliza la alarma, la alarma se extiende por un periodo de tiempo. El rango de tiempo es de 0 segundos a 300 segundos.
Mostrar mensaje	Marque la casilla para habilitar un mensaje emergente en su PC host local.
Reportar alarma	<p>Seleccione la casilla de verificación. Cuando ocurre una alarma, el dispositivo NVR carga una señal de alarma a la red (incluida la central de alarmas).</p> <p></p> <ul style="list-style-type: none"> ● Esta función está disponible en modelos selectos. ● Primero debe configurar la central de alarmas.

Parámetro	Descripción
Enviar correo electrónico	<p>Seleccione la casilla de verificación. Cuando ocurre una alarma, el dispositivo NVR envía un correo electrónico al buzón configurado para notificar al usuario.</p>  <p>Primero debes configurar el correo electrónico.</p>
Canal de grabación	<p>Seleccione la casilla de verificación y seleccione el canal de grabación necesario (admite múltiples opciones). Cuando ocurre una alarma, el dispositivo NVR activa el canal para grabar.</p>  <p>Primero debe habilitar la grabación inteligente y la grabación automática.</p>
Post-grabación	<p>Al finalizar la alarma, la grabación se extiende por un período de tiempo. El rango de tiempo es de 10 segundos a 300 segundos.</p>
Enlace PTZ	<p>Seleccione la casilla de verificación y haga clic en Configuración para seleccionar el canal y la acción PTZ. Cuando ocurre una alarma, el dispositivo NVR asocia el canal para realizar la acción PTZ correspondiente. Por ejemplo, active el PTZ en el canal uno para girar al punto preestablecido X.</p>  <ul style="list-style-type: none"> ● La alarma Tripwire admite activar solo el punto preestablecido PTZ. ● Primero debe configurar las acciones PTZ correspondientes.
Recorrido	<p>Seleccione la casilla de verificación y seleccione el canal para el recorrido. Cuando ocurre una alarma, la interfaz local del dispositivo NVR muestra la pantalla del canal seleccionado.</p>  <ul style="list-style-type: none"> ● Primero debe configurar el intervalo de tiempo y el modo del recorrido. ● Una vez finalizado el recorrido, la interfaz de vista previa se restaura al modo de pantalla dividida antes del recorrido.
Almacenamiento de imágenes	<p>Seleccione la casilla de verificación Instantánea para tomar una instantánea del canal seleccionado.</p>  <p>Para utilizar esta función, seleccione Menú principal > CÁMARA > Codificar > Instantánea, seleccionar Evento en Tipolista.</p>
Zumbador	<p>Seleccione la casilla de verificación para activar el timbre cuando ocurra una alarma.</p>
Tono de alarma	<p>Marque la casilla y luego seleccione el archivo de audio correspondiente de la lista desplegable. El sistema reproduce el archivo de audio cuando ocurre la alarma.</p>  <p>Primero debe agregar un archivo de audio.</p>

Paso 3 Hacer clic **Aplicar**.

1.8 Vista en vivo

Después de iniciar sesión, el sistema pasa al modo de visualización en vivo de múltiples canales de forma predeterminada. Podrás visualizar el vídeo de seguimiento de cada canal. Tenga en cuenta que el número de ventanas mostradas puede variar según el modelo.

modelar.

Para ingresar a la pantalla de visualización en vivo desde otras interfaces, haga clic en



en la parte superior derecha de la pantalla.

Figura 1-22 Vista en vivo



Pantalla de visualización en vivo

Puede ver el vídeo en vivo de las cámaras conectadas a través de cada canal en la pantalla.

- De forma predeterminada, la hora del sistema, el nombre del canal y el número del canal se muestran en cada ventana de canal. Esta configuración se puede configurar seleccionando **Menú principal > CÁMARA > Cubrir > Cubrir**.
- La cifra en la esquina inferior derecha representa el número de canal. Si se cambia la posición del canal o se modifica el nombre del canal, puede reconocer el número del canal por esta cifra y luego realizar operaciones como consulta de grabación y reproducción.

Para conocer los iconos que se muestran en cada canal, consulte la Tabla 1-7.

Tabla 1-7 Descripción del icono

Icono	Descripción
	Se está grabando vídeo.
	La detección de movimiento ocurre en la escena.
	Se detecta pérdida de vídeo.
	La monitorización de canales está bloqueada.

1.9 Reproducción de grabación

Para reproducir una grabación, puede seleccionar **Menú principal > Reproducción** haga clic derecho en la interfaz de visualización en vivo y seleccione **Buscar**.

Figura 1-23 Interfaz principal de reproducción



Para obtener detalles sobre las instrucciones en la interfaz principal de reproducción, consulte *Manual de usuario*.

Reproducción instantánea

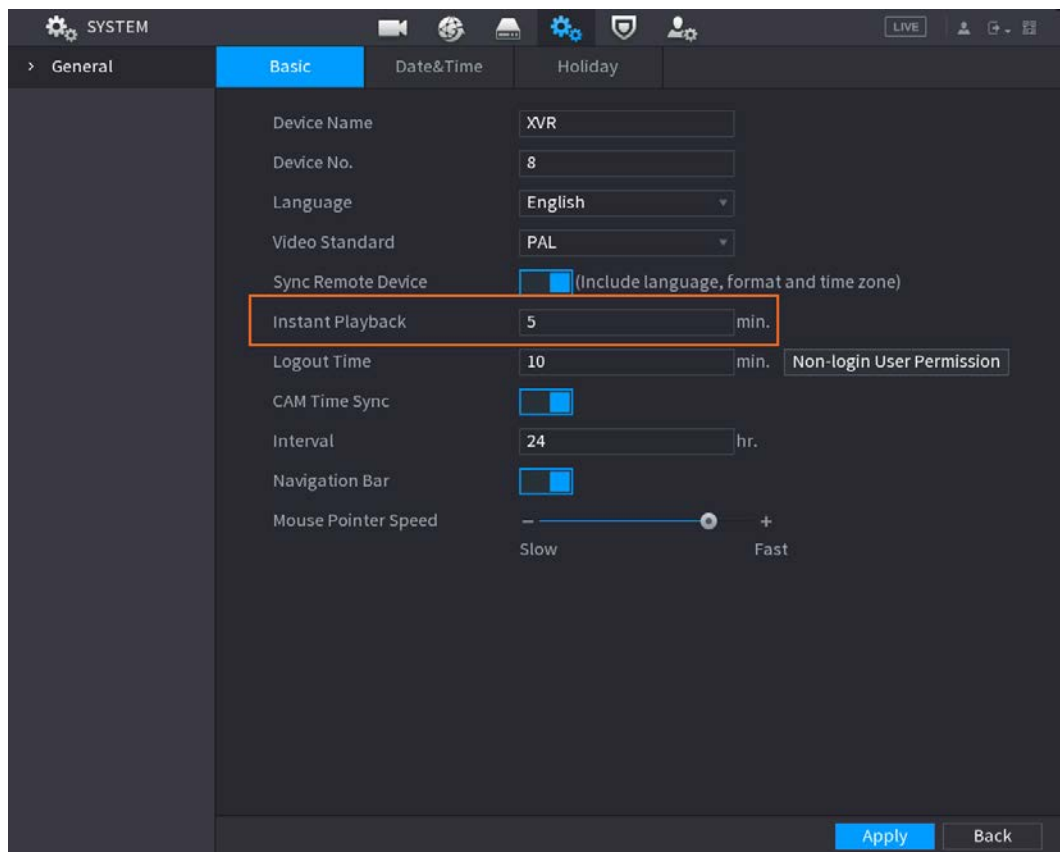
Puede reproducir los 5 minutos anteriores a 60 minutos del vídeo grabado.

Al hacer clic en **Se** muestra la interfaz de reproducción instantánea. La reproducción instantánea tiene las siguientes características:

- Mueve el control deslizante para elegir la hora a la que quieres empezar a jugar.
- Reproducir, pausar y cerrar la reproducción.
- La información como el nombre del canal y el ícono de estado de grabación están ocultos durante la reproducción instantánea y no se mostrarán hasta que se salga.
- Durante la reproducción, no se permite el cambio de diseño de división de pantalla.

Para cambiar el tiempo de reproducción, seleccione **Menú principal > SISTEMA > General > Básico**, en el **Juego instantáneo**, ingrese el tiempo que desea reproducir.

Figura 1-24 Establecer tiempo de reproducción instantánea



Reproducción de búsqueda inteligente

Durante la reproducción, puede analizar un área determinada para determinar si se produjo algún evento de detección de movimiento. El sistema mostrará las imágenes con eventos de movimiento del video grabado.



Esta función es sólo para algunos productos de la serie.

Para utilizar la función de búsqueda inteligente, debe habilitar la detección de movimiento para el canal seleccionando **Menú principal > ALARMA > Detección de vídeo > Detección de movimiento**.

2 Iniciar sesión en la web

La web proporciona la mayoría de las funciones en la GUI local. Puede iniciar sesión en la web para administrar el NVR según sea necesario.

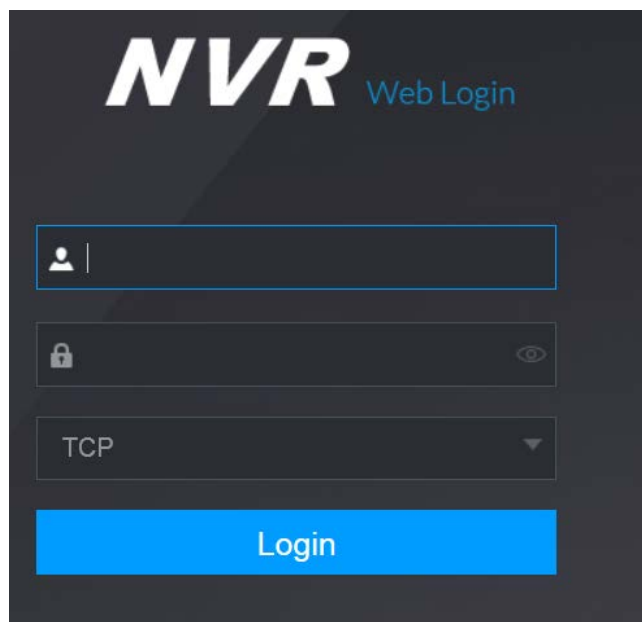



Se pueden encontrar ligeras diferencias en las interfaces de diferentes modelos. Las siguientes cifras son para solo referencia. El producto real prevalecerá.

Procedimiento

- Paso 1** Abra el navegador e ingrese la dirección IP del NVR y luego presione la tecla Enter. Ingrese el nombre de usuario y la contraseña.
- Paso 2**

Figura 2-1 Iniciar sesión



- La cuenta de administrador predeterminada es **administración**. La contraseña es la que estaba configurado durante la configuración inicial. Para proteger su cuenta, se recomienda mantener la contraseña correctamente y cámbiela periódicamente.
- Hacer clic  para mostrar la contraseña.

- Paso 3** Hacer clic **Acceso**.

Apéndice 1 Recomendaciones de ciberseguridad

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

Acciones obligatorias a tomar para la seguridad de la red de equipos básicos:

1. Utilice contraseñas seguras

Consulte las siguientes sugerencias para establecer contraseñas:

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

2. Actualice el firmware y el software cliente a tiempo

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

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

1. Protección física

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

2. Cambie las contraseñas con regularidad

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

3. Establecer y actualizar contraseñas Restablecer información oportuna

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

4. Habilite el bloqueo de cuenta

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

5. Cambie HTTP predeterminado y otros puertos de servicio

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

6. Habilite HTTPS

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

7. Habilitar la lista de permitidos

Le sugerimos que habilite la función de lista permitida para evitar que todos, excepto aquellos con direcciones IP específicas, accedan al sistema. Por lo tanto, asegúrese de agregar la dirección IP de su computadora y la dirección IP del equipo adjunto a la lista de permitidos.

8. Vinculación de direcciones MAC

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

9. Asigne cuentas y privilegios de manera razonable

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

10. Deshabilite los servicios innecesarios y elija modos seguros

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

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

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

11. Transmisión cifrada de audio y vídeo

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

Recordatorio: la transmisión cifrada provocará cierta pérdida en la eficiencia de la transmisión.

12. Auditoría segura

- **Verifique a los usuarios en línea:** le sugerimos que verifique a los usuarios en línea con regularidad para ver si el NVR ha iniciado sesión sin autorización.
- **Verifique el registro del equipo:** al ver los registros, puede conocer las direcciones IP que se utilizaron para iniciar sesión en sus dispositivos y sus operaciones clave.

13. Registro de red

Debido a la capacidad de almacenamiento limitada del equipo, el registro almacenado es limitado. Si necesita guardar el registro durante un período prolongado, se recomienda habilitar la función de registro de red para garantizar que los registros críticos estén sincronizados con el servidor de registro de red para su seguimiento.

14. Construya un entorno de red seguro

Para garantizar mejor la seguridad de los equipos y reducir los posibles riesgos cibernéticos, recomendamos:

- **Deshabilite la función de asignación de puertos del enrutador** para evitar el acceso directo a los dispositivos de la intranet desde la red externa.
- **La red debe dividirse y aislarse según las necesidades reales de la red.** Si no hay requisitos de comunicación entre dos subredes, se sugiere utilizar VLAN, red GAP y otras tecnologías para particionar la red, a fin de lograr el

efecto de aislamiento de la red.

- Establezca el sistema de autenticación de acceso 802.1x para reducir el riesgo de acceso no autorizado a redes privadas.

15. Se recomienda que habilite el firewall de su dispositivo o la función de lista de bloqueo y lista de permitidos para reducir el riesgo de que su dispositivo pueda ser atacado.