Grabador de video en red

Guía de inicio rápido

V1.0.1

Prefacio

General

Este manual presenta las funciones y operaciones de los dispositivos NVR (en adelante, "el Dispositivo").

Instrucciones de seguridad

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

Palabras de advertencia	Sentido
PRECAUCIÓN	Indica un riesgo potencial que, si no se evita, podría provocar daños a la propiedad, pérdida de datos, menor rendimiento o resultados impredecibles.
CONSEJOS	Proporciona métodos para ayudarlo a resolver un problema o ahorrarle tiempo.
NOTA	Proporciona información adicional como énfasis y complemento del texto.

Revisión histórica

No.	Versión	Contenido de la revisión	Tiempo de liberación
2	V1.0.1	• Se actualizó una figura en el Programa. • Seguridad eléctrica actualizada.	Septiembre de 2019
1	V1.0.0	Primer lanzamiento.	Julio de 2019

Acerca del manual

- El manual es solo para referencia. Si hay inconsistencia entre el manual y el producto real, prevalecerá el producto real.
- No nos hacemos 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 el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto pueden causar algunas diferencias entre el producto real y el manual. Póngase en contacto con el servicio de atención al cliente para obtener el programa más actualizado y la documentación complementaria. Todavía puede haber desviaciones en los datos técnicos, la
- descripción de funciones y operaciones, o errores en la impresión. Si tiene alguna duda o disputa, consulte nuestra explicación final. Actualice el software del lector o pruebe con otro software de lectura convencional si el manual (en PDF
-

formato) no se puede abrir.

- Todas las marcas comerciales, marcas comerciales registradas y los nombres de empresas que aparecen en el manual son propiedad de sus respectivos propietarios.
- Visite nuestro sitio web, comuníquese con el proveedor o con el servicio de atención al cliente si se produce algún problema al utilizar el dispositivo.
- Si hay alguna duda o controversia, consulte nuestra explicación final.

Advertencias y medidas de seguridad importantes

Gracias por adquirir nuestra grabadora de vídeo en red (NVR).

Este manual le ayudará a familiarizarse con nuestro NVR en poco tiempo. Lea el manual detenidamente antes de comenzar a utilizar su NVR y consérvelo correctamente para futuras consultas.

Requisito de funcionamiento

- Instale el dispositivo de front-end PoE en interiores. El dispositivo no
- es compatible con el montaje en pared.
- No coloque ni instale el dispositivo en un área expuesta a la luz solar directa o cerca de un dispositivo generador de calor.

- No instale el dispositivo en un área húmeda, polvorienta o fuliginosa.
- Mantenga su instalación horizontal, o instálelo en lugares estables, y evite que se caiga.
- No gotee ni salpique líquidos sobre el dispositivo; No coloque sobre el dispositivo nada lleno de líquido, para evitar que fluyan líquidos al dispositivo.
- Instale el dispositivo en lugares bien ventilados; no bloquee su abertura de ventilación. Utilice el dispositivo solo
- dentro del rango nominal de entrada y salida.
- No desmonte el dispositivo de forma arbitraria.
- Transporte, use y almacene el dispositivo dentro del rango permitido de humedad y temperatura.

Seguridad ELECTRICA

- El uso inadecuado de la batería puede provocar un incendio, una explosión o una inflamación. Al
- reemplazar la batería, asegúrese de utilizar el mismo modelo.
- Utilice los cables de alimentación recomendados en la región y cumpla con la especificación de potencia nominal.

- Use el adaptador de corriente provisto con el Dispositivo; de lo contrario, podría provocar lesiones personales y daños al dispositivo.

- La fuente de alimentación debe cumplir con los requisitos de la norma de seguridad de voltaje muy bajo (SELV) y suministrar energía con un voltaje nominal que cumpla con el requisito de fuente de alimentación limitada de acuerdo con IEC60950-1. Tenga en cuenta que el requisito de suministro de energía está sujeto a la etiqueta del dispositivo.

- Conecte el dispositivo (estructura tipo I) a la toma de corriente con toma de tierra de protección.
- El acoplador del aparato es un dispositivo de desconexión. Cuando utilice el acoplador, mantenga el ángulo para facilitar la operación.

Tabla de contenido

1 Inicio rápido

Las siguientes figuras son solo para referencia. El producto real prevalecerá.

Apague la alimentación antes de reemplazar el disco duro.

1.1 Comprobación de los componentes

Toda la instalación y las operaciones aquí deben cumplir con las normas locales de seguridad eléctrica. El dispositivo no admite el montaje en la pared con el panel frontal hacia abajo.

Cuando reciba el dispositivo, verifique la siguiente lista de verificación. Si alguno de los artículos falta o está dañado, comuníquese con el distribuidor local o el ingeniero de posventa de inmediato.

No.	Artículos		Requisito
1	Paquete	Apariencia	Ningún daño evidente.
		Materiales de embalaje	Sin posiciones rotas o distorsionadas que puedan ser causadas por golpes.
		Accesorios	No falta.
2	Etiquetas	Etiquetas en el dispositivo	• El modelo del dispositivo se ajusta a la orden de compra. • No roto. No rompa ni tire las etiquetas; de lo contrario, los servicios de garantía no están garantizados. Debe proporcionar el número de serie del producto cuando solicite el servicio postventa.
3	Dispositivo	Apariencia	Ningún daño evidente.
		Cables de datos, potencia cables, cables de ventilador, placa base	Sin conexión suelta. Si hay alguna conexión suelta, comuníquese con el servicio posventa de la empresa a tiempo.

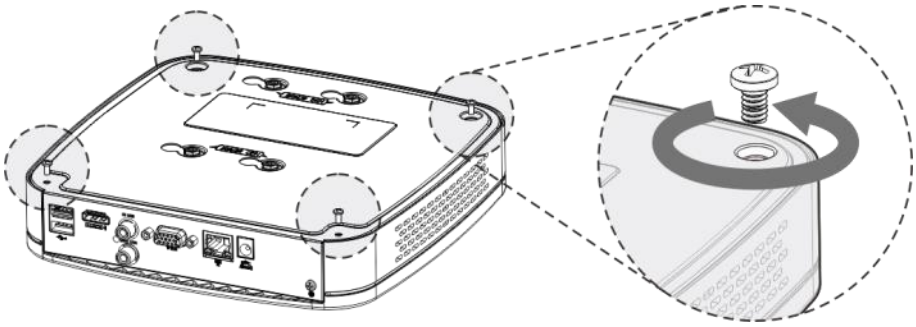
1.2 Instalación de HDD

1.2.1 INTELIGENTE 1U

Para la primera instalación, compruebe si el disco duro se ha instalado o no. Se recomienda utilizar HDD de nivel empresarial o de vigilancia. No se recomienda utilizar HDD de PC.

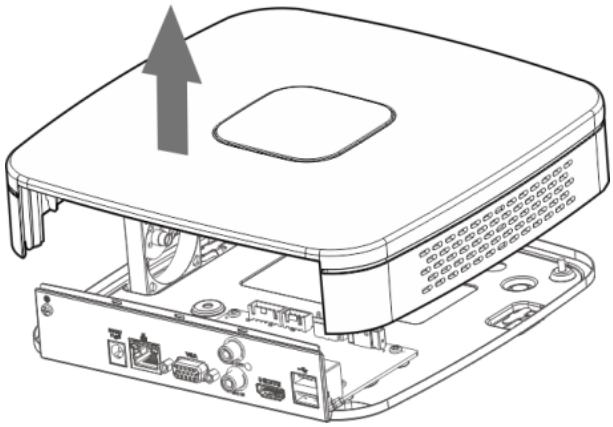
Paso 1 Dé la vuelta al dispositivo y retire los cuatro tornillos de fijación de la placa base del dispositivo.

Figura 1-1 Instalación de HDD (1)



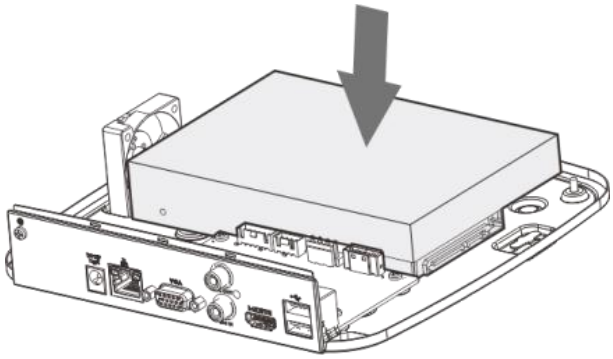
Paso 2 Retire la cubierta en la dirección que se muestra en la siguiente flecha.

Figura 1-2 Instalación de HDD (2)



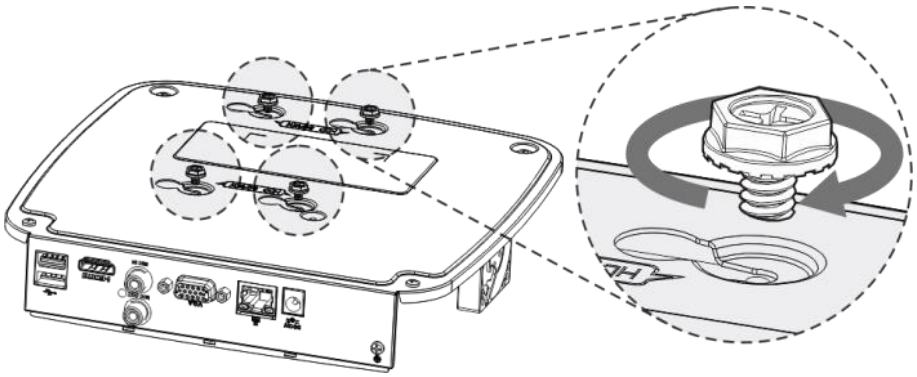
Paso 3 Haga coincidir los cuatro orificios de la placa base para colocar el disco duro.

Figura 1-3 Instalación de HDD (3)



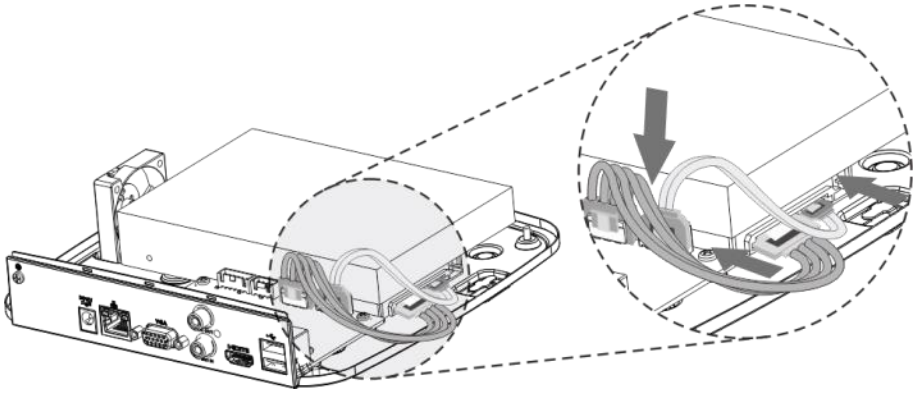
Paso 4 Coloque el dispositivo boca abajo, haga coincidir los tornillos con los orificios del disco duro y luego apriete ellos. El disco duro se fija al zócalo.

Figura 1-4 Instalación de HDD (4)



Paso 5 Conecte el cable de datos del disco duro y el cable de alimentación al dispositivo.

Figura 1-5 Instalación de HDD (5)



Paso 6 Vuelva a colocar la tapa y apriete los cuatro tornillos del zócalo para completar el instalación.

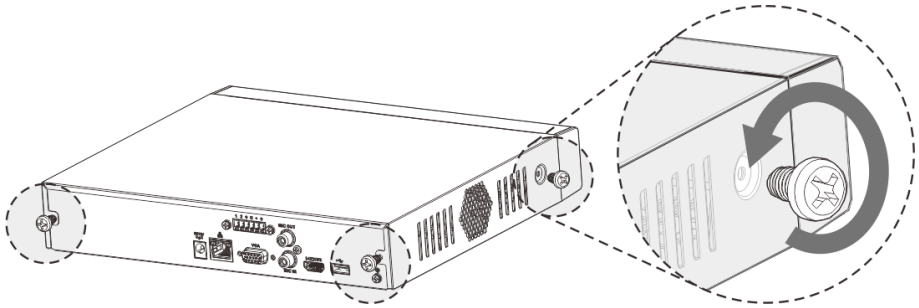
Figura 1-6 Instalación de HDD (6)

1.2.2 MINI 1U, COMPACTO 1U, 1U

Para la primera instalación, asegúrese de que el disco duro se haya instalado o no. Se recomienda utilizar HDD de nivel empresarial o de vigilancia. No se recomienda utilizar HDD de PC.

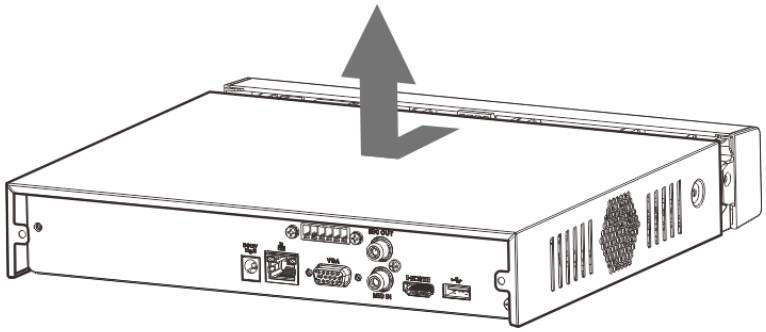
Paso 1 Quite los tornillos de fijación de la tapa (incluidos los dos tornillos del panel trasero y dos tornillos en los paneles izquierdo y derecho).

Figura 1-7 Instalación de HDD (1)



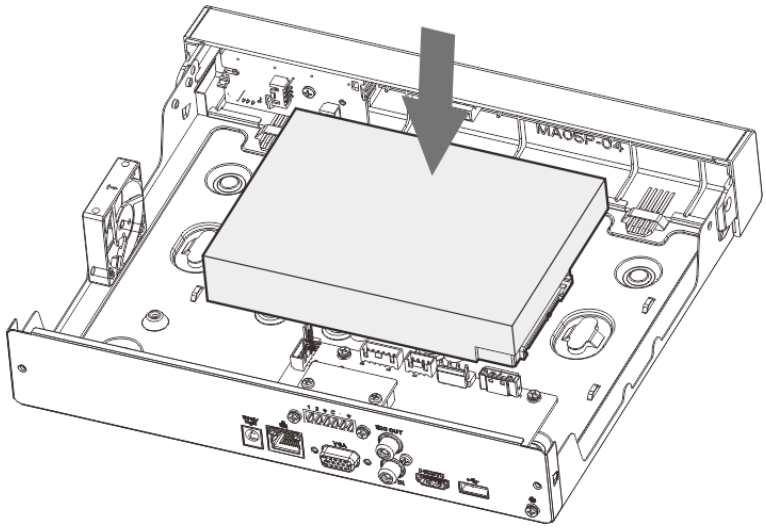
Paso 2 Retire la cubierta en la dirección que se muestra en la siguiente flecha.

Figura 1-8 Instalación de HDD (2)



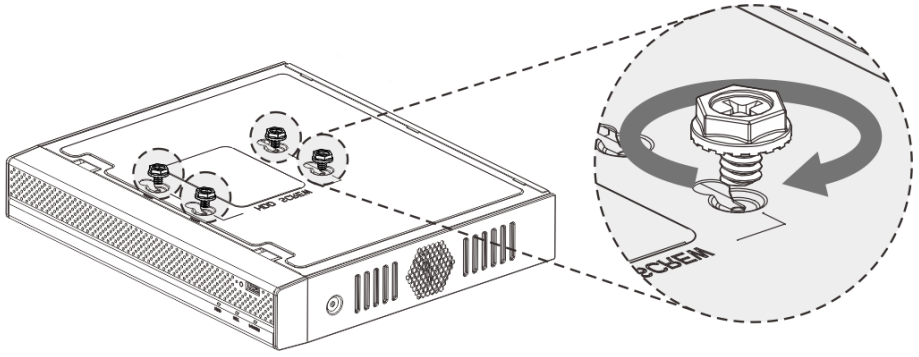
Paso 3 Haga coincidir los cuatro orificios de la placa base para colocar el disco duro.

Figura 1-9 Instalación de HDD (3)



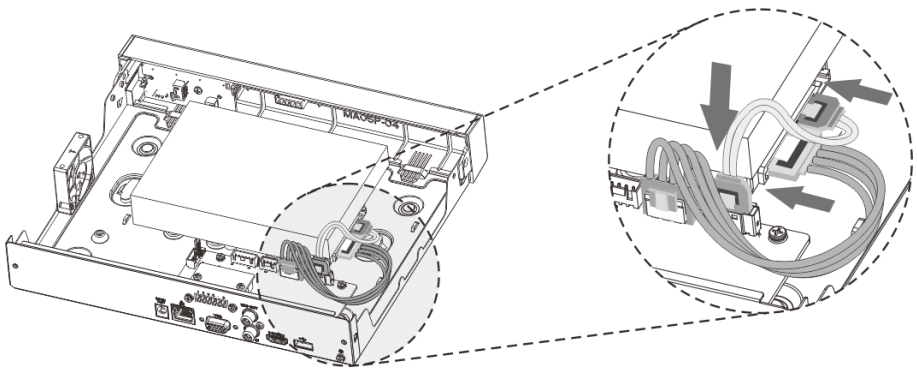
Paso 4 Coloque el dispositivo boca abajo, haga coincidir los tornillos con los orificios del disco duro y luego sujetarlos. El disco duro se fija al zócalo.

Figura 1-10 Instalación de HDD (4)



Paso 5 Conecte el cable de datos del disco duro y el cable de alimentación al dispositivo.

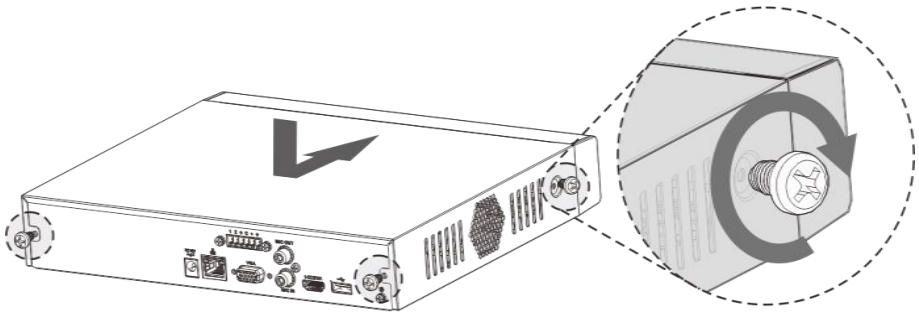
Figura 1-11 Instalación de HDD (5)



Paso 6 Vuelva a colocar la cubierta y apriete los tornillos del panel trasero y los paneles laterales

completar la instalación.

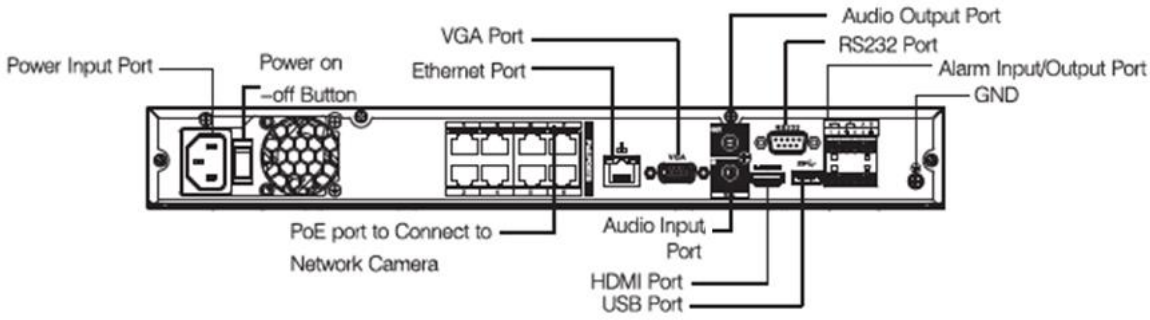
Figura 1-12 Instalación de HDD (6)



2 Conexión

La apariencia real puede ser diferente según el modelo que compró.

Figura 2-1 Conexión en serie 1U



- Verifique cuidadosamente los íconos en el panel posterior y consulte el producto real para obtener información detallada.
- Si el icono es DC 12V, entrada de potencia DC 12V. Si el icono es DC48V, entrada de alimentación DC 48V.

3 Configuraciones locales

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

3.1 Arrancar

Antes del arranque, asegúrese de:

- El voltaje de entrada nominal debe coincidir con el requisito de potencia del dispositivo. Asegúrese de que la conexión del cable de alimentación esté lista y luego presione el botón de encendido.
- Para la seguridad del dispositivo, primero conecte el dispositivo al adaptador de corriente y luego conéctelo a la toma de corriente.
- Utilice siempre la corriente estable. Se recomienda utilizar UPS.
- El dispositivo de algunas series no tiene el botón de encendido y apagado. Puede iniciar el dispositivo una vez que se conecte la alimentación.

Conecte el dispositivo al monitor, conéctelo a la toma de corriente y luego presione el botón de encendido para iniciar el dispositivo.

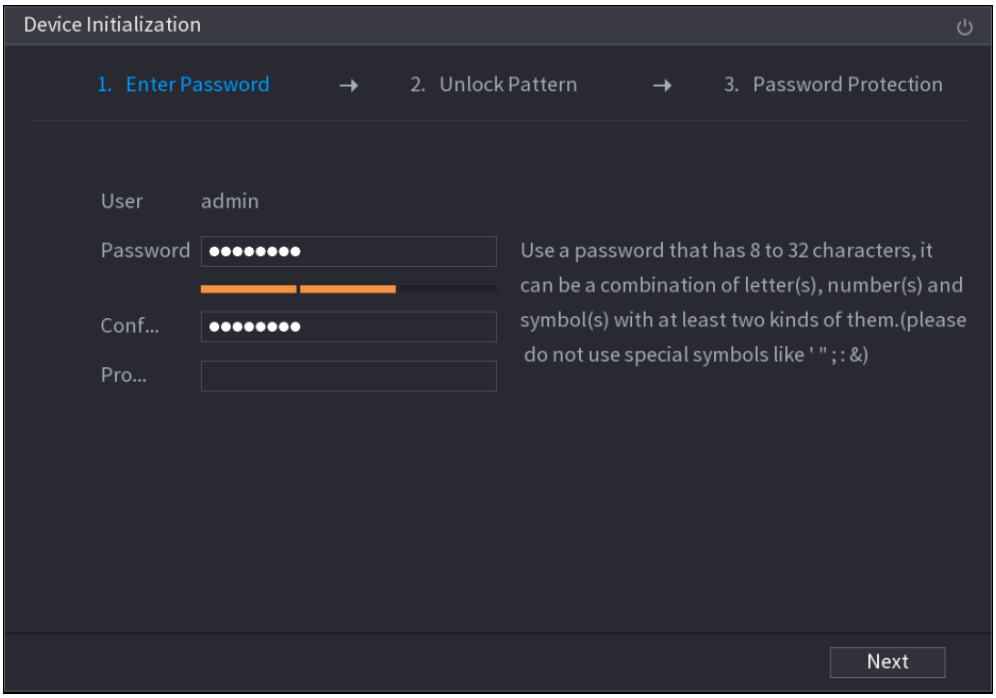
3.2 Inicialización del dispositivo

Al arrancar por primera vez, debe configurar la información de contraseña para **administración** (por defecto). Para garantizar la seguridad del dispositivo, mantenga correctamente la contraseña de inicio de sesión del administrador y modifíquela con regularidad.

Paso 1 Encienda el dispositivo.

los **Inicialización del dispositivo** se muestra la interfaz. Vea la Figura 3-1.

Figura 3-1 Ingrese la contraseña



Paso 2 Configure la información de la contraseña para admin. Para obtener más detalles, consulte la Tabla 3-1.

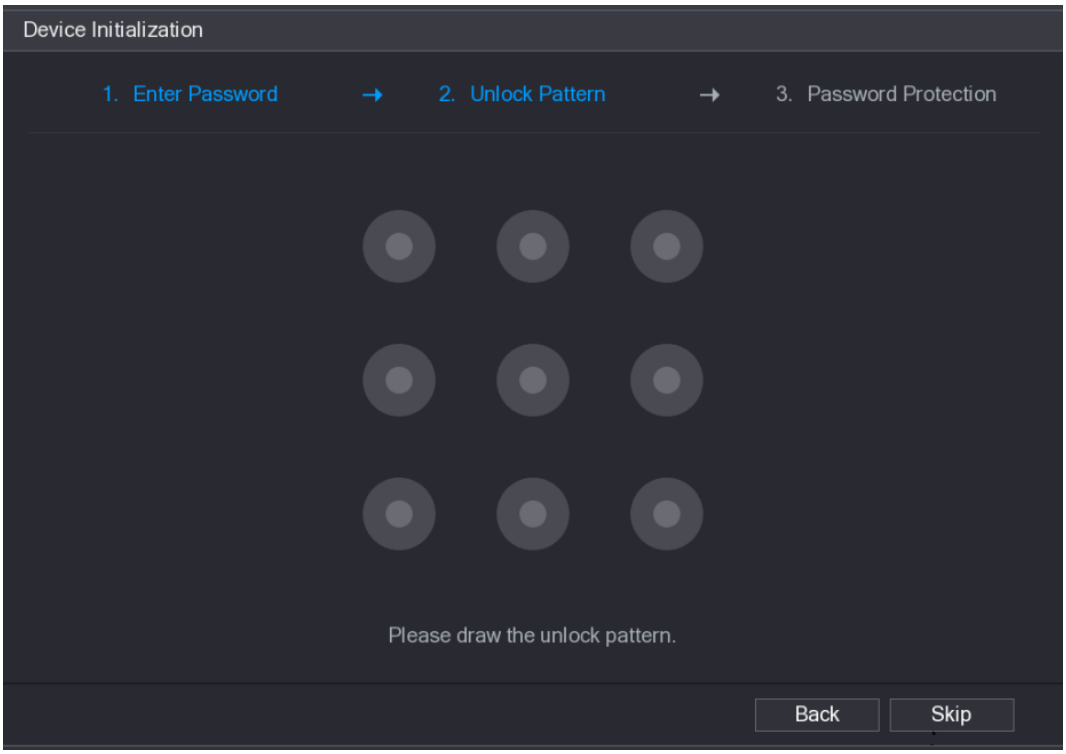
Tabla 3-1 Descripción de la información de contraseña

Parámetro	Descripción
Usuario	Por defecto, el usuario es **administración.**
Contraseña	En el **Contraseña** cuadro, ingrese la contraseña de administrador. La contraseña debe constar de 8 a 32 caracteres que no estén en blanco y contener al menos dos tipos de caracteres entre número, letra y carácter especial (excluyendo '";: &).
Confirmar contraseña	
Pregunta rápida	En el **Pregunta rápida** , ingrese la información que pueda recordarle la contraseña. En la interfaz de inicio de sesión, haga clic en , se mostrará el mensaje para ayudarlo restablecer la contraseña.

Paso 3 Haga clic en **Próximo.**

los **Patrón de desbloqueo** se muestra la interfaz de configuración. Vea la Figura 3-2.

Figura 3-2 Patrón de desbloqueo

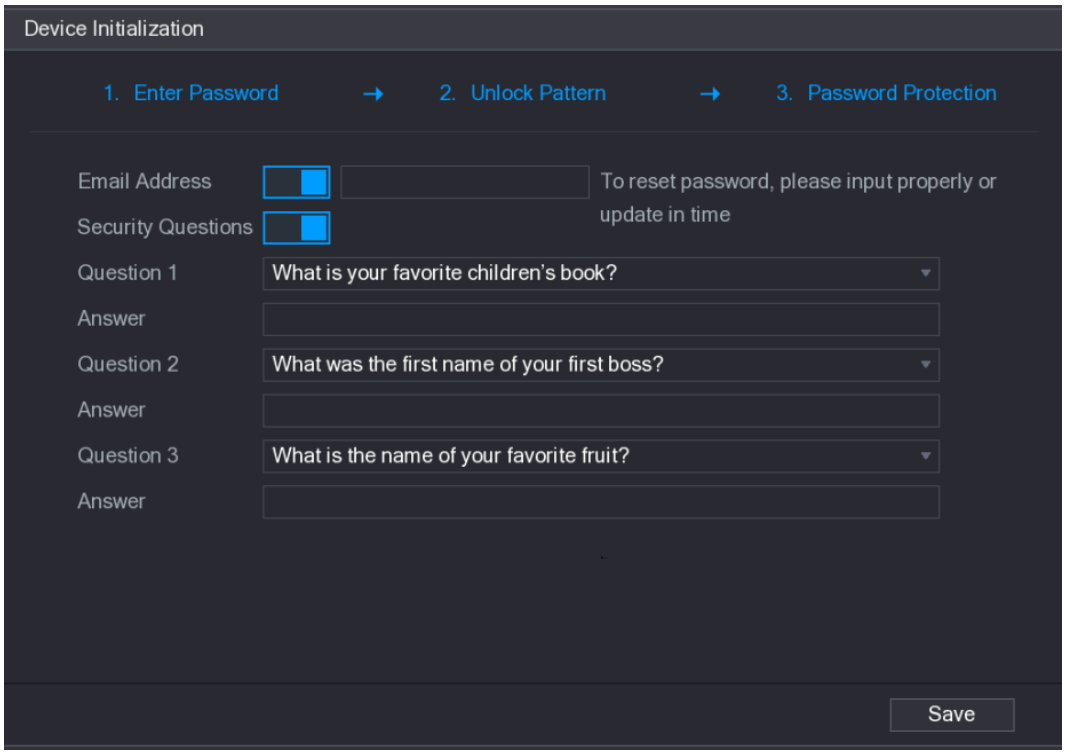


Paso 4 Dibuje un patrón de desbloqueo.

Después de configurar el patrón de desbloqueo, se muestra la interfaz de configuración de protección con contraseña. Vea la Figura 3-3.

- Una vez que haya configurado el patrón de desbloqueo, el sistema requerirá el patrón de desbloqueo como método de inicio de sesión predeterminado. Si omite esta configuración, ingrese la contraseña para iniciar sesión.
- Si no desea configurar el patrón de desbloqueo, haga clic en **Omitir.**

Figura 3-3 Protección por contraseña



Paso 5 Configure los parámetros de protección para la contraseña. Para obtener más detalles, consulte la Tabla 3-2.

- Después de la configuración, si olvidó la contraseña del usuario administrador, puede restablecer la contraseña a través de la dirección de correo electrónico reservada o preguntas de seguridad. Para obtener detalles sobre cómo restablecer la contraseña, consulte *Manual de usuario.*
- Si no desea configurar los ajustes, desactive las funciones de dirección de correo electrónico y preguntas de seguridad en la interfaz.

Tabla 3-2 Descripción del parámetro de protección por contraseña

Contraseña **Modo de protección**	**Descripción**
Dirección de correo electrónico	Ingrese la dirección de correo electrónico reservada. En el **Dirección de correo electrónico** , ingrese una dirección de correo electrónico para restablecer la contraseña. En caso de que haya olvidado la contraseña, ingrese el código de seguridad que obtendrá de esta dirección de correo electrónico reservada para restablecer la contraseña de administrador.
Seguridad Preguntas	Configure las preguntas y respuestas de seguridad. En caso de que haya olvidado la contraseña, ingresar las respuestas a las preguntas puede hacer que restablezca la contraseña.
Si desea configurar la función de correo electrónico o preguntas de seguridad más tarde o si desea cambiar las configuraciones, seleccione **Menú principal> CUENTA> USUARIO.**	

Paso 6 Haga clic en **Okay** para completar la configuración.

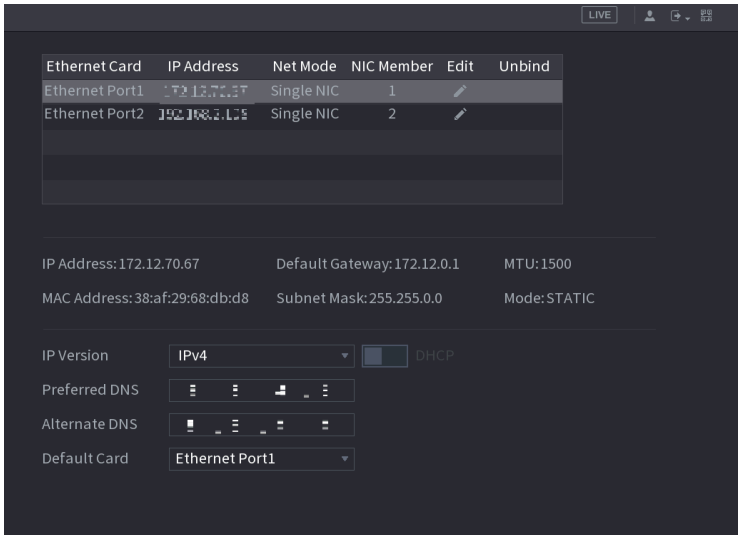
los **Asistente de inicio** se muestra la interfaz. Para obtener detalles sobre la configuración rápida durante el inicio, consulte *Manual de usuario.*

3.3 Modificar la dirección IP

Seleccione **Menú principal> RED> TCP / IP.** Se muestra la interfaz TCP / IP. Vea la Figura 3-4.

Hacer clic  para modificar la dirección IP de acuerdo con la situación real (la dirección IP predeterminada es 192.168.1.108).

Figura 3-4 TCP / IP



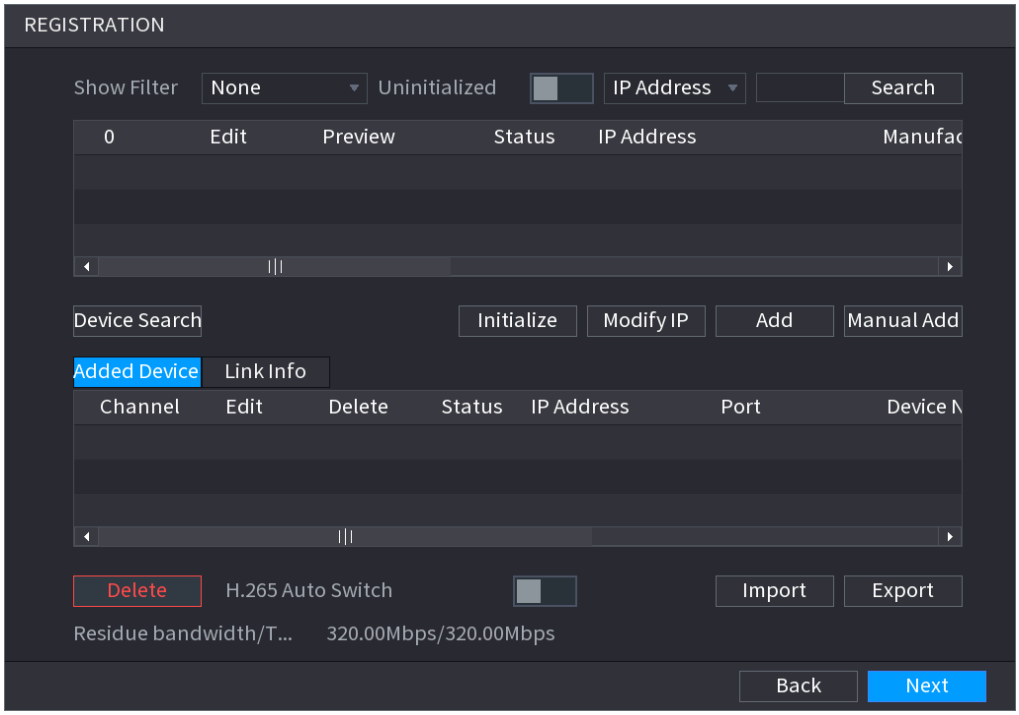
3.4 Registro

Seleccione **Menú principal> CÁMARA> Registro.** Se muestra la interfaz de registro. Vea la Figura 3-5.

Puede registrar dispositivos remotos de las siguientes dos formas:

- Hacer clic **Búsqueda de dispositivos.** En la lista de resultados, haga doble clic en el dispositivo remoto o seleccione la casilla de verificación frente al dispositivo y luego haga clic en **Añadir** para registrar el dispositivo remoto. Hacer clic **Agregar manual** e ingrese la dirección IP del dispositivo
- remoto para registrarlo.

Figura 3-5 Registro



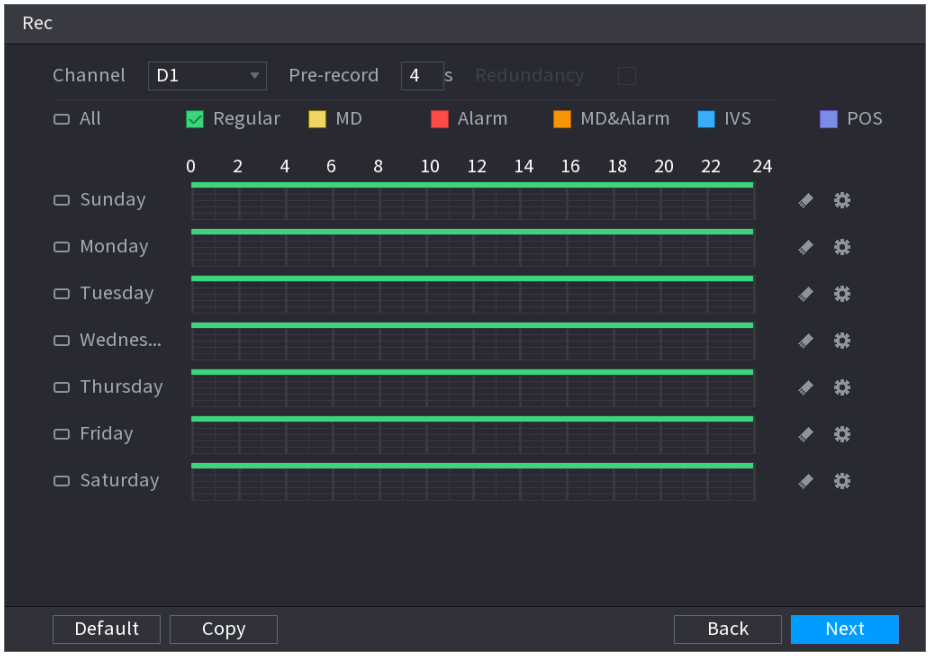
3,5 Calendario

Todos los canales tienen una grabación continua de 24 horas por defecto de fábrica. Puede personalizar el período de registro y el tipo de registro.

Paso 1 Seleccione **Menú principal> ALMACENAMIENTO> HORARIO> Rec.**

los **Rec** se muestra la interfaz. Vea la Figura 3-6.

Figura 3-6 Programación



Paso 2 Configure parámetros como canal, pregrabación, ANR y tipo de grabación.

- Después de configurar un HDD para que sea un disco redundante, seleccione el **Redundancia** casilla de verificación para realizar una copia de seguridad del archivo de video. Sirve para guardar archivos de video en diferentes HDD al mismo tiempo. Una vez que uno de los discos duros está dañado, todavía hay un archivo de respaldo en otro disco para garantizar la confiabilidad de los datos.

- Seleccione la casilla de verificación ANR para habilitar esta función. Cuando el IPC no tiene acceso a la red, sigue grabando y guarda los registros en la tarjeta SD. Una vez que se recupera la red, IPC transmite los registros durante la interrupción de la red al dispositivo NVR para garantizar la integridad de los registros.

Paso 3 Establezca el período de programación. Incluye dibujo y edición.

- Dibujo: Mantenga presionado el botón izquierdo del mouse y arrastre el mouse en la figura del tiempo para dibujar el período.
- Edición: haga clic en  para configurar el período y luego haga clic en **OKAY.**

Paso 4 Haga clic en **Aplicar** o **Okay** para guardar la configuración.

La programación de grabación configurada puede entrar en vigor solo cuando la función de grabación automática está habilitada. Para obtener detalles sobre cómo habilitar la grabación automática, consulte *Manual de usuario.*

3.6 Reproducción

Seleccione **Menú principal> Reproducción** o haga clic derecho en la interfaz de vista previa y seleccione **Buscar.** Se muestra la interfaz de búsqueda de registros. Vea la Figura 3-7.

Puede reproducir registros de acuerdo con el tipo de registro configurado, el tiempo de registro y el canal. Para obtener información detallada, consulte *Manual de usuario.*

Figura 3-7 Búsqueda de registros

3,7 Apagar

Hacer clic  en la esquina superior derecha y luego seleccione **Apagar.**

4 Operaciones web

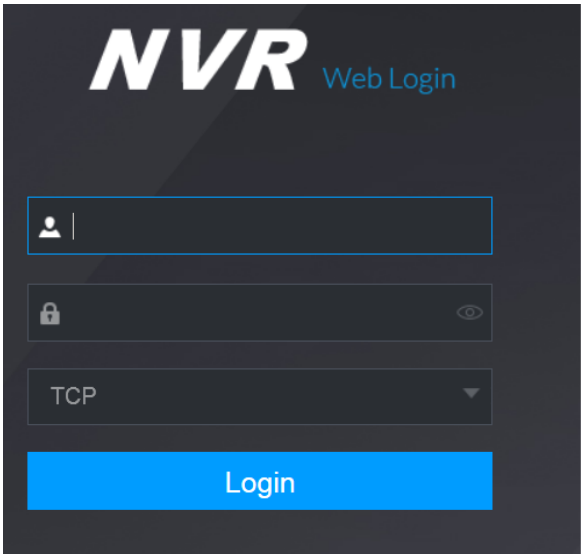
Si es la primera vez que inicia sesión en el dispositivo, primero debe inicializar el dispositivo. Para obtener información detallada, consulte *Manual de usuario.*

Paso 1 Abra el navegador e ingrese la dirección IP del dispositivo en la barra de direcciones. prensa

Introducir clave.

los **Iniciar sesión** se muestra la interfaz. Vea la Figura 4-1.

Figura 4-1 Inicio de sesión



Paso 2 Ingrese el nombre de usuario y la contraseña.

- El nombre de usuario predeterminado es admin y la contraseña de inicio de sesión es la que estableció en la inicialización del dispositivo. Para garantizar la seguridad del dispositivo, se recomienda modificar la contraseña de administrador con regularidad y mantenerla correctamente.
- Si olvidó la contraseña de inicio de sesión de administrador, haga clic en **Se te olvidó tu contraseña** para restablecerlo. Para obtener información detallada, consulte *Manual de usuario.*

Paso 3 Haga clic en **Iniciar sesión.**

los **Avance** se muestra la interfaz. En la interfaz web, puede realizar operaciones como configuración del sistema, administración de dispositivos y configuración de red. Para obtener más detalles, consulte

Manual de usuario.

- Cuando inicie sesión en la web por primera vez, instale el control de acuerdo con las indicaciones del sistema.

5 P2P

Paso 1 Escanee el código QR con el teléfono celular para descargar e instalar la aplicación móvil.

Puede obtener el código QR de la aplicación móvil y el código QR del SN del dispositivo de las dos formas siguientes:

- Inicie sesión en la interfaz local y seleccione **Menú principal> RED> P2P.**
- Inicie sesión en la interfaz web y seleccione **Menú principal> RED> TCP / IP> P2P.**

Figura 5-1 Código QR de la aplicación móvil

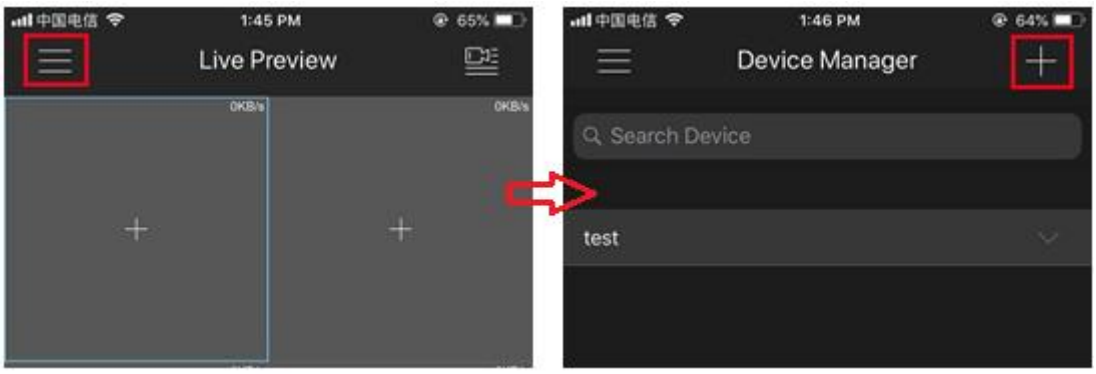
Paso 2 Registre el dispositivo en la aplicación móvil

Después de registrar el dispositivo correctamente, puede ver la pantalla del monitor en la aplicación del teléfono celular.

Las siguientes figuras son solo para referencia. El producto real prevalecerá. Para obtener información detallada, consulte *Manual de usuario.*

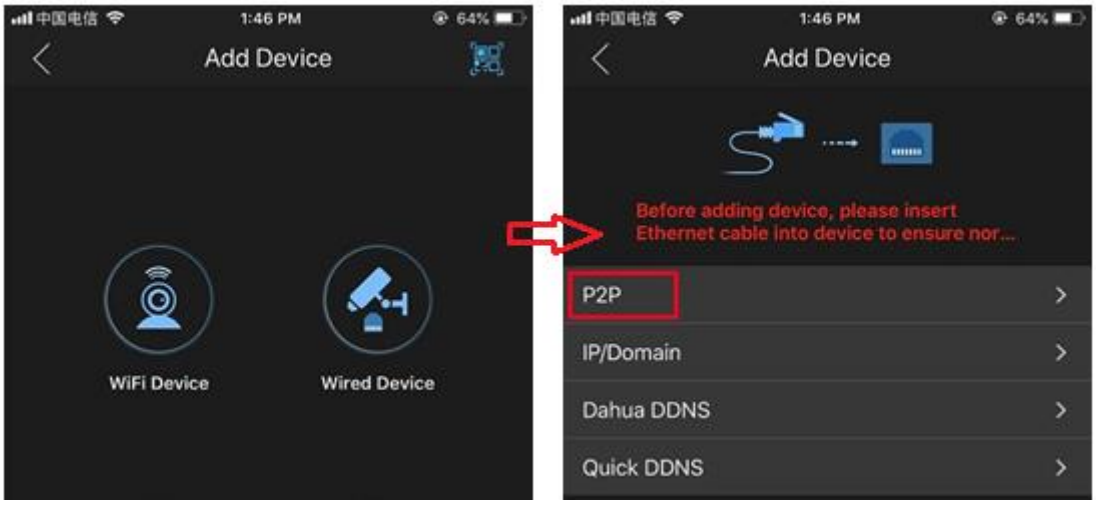
1) Toque  . Seleccione **Administrador de dispositivos,** y luego toque  . Vea la Figura 5-2.

Figura 5-2 P2P (1)



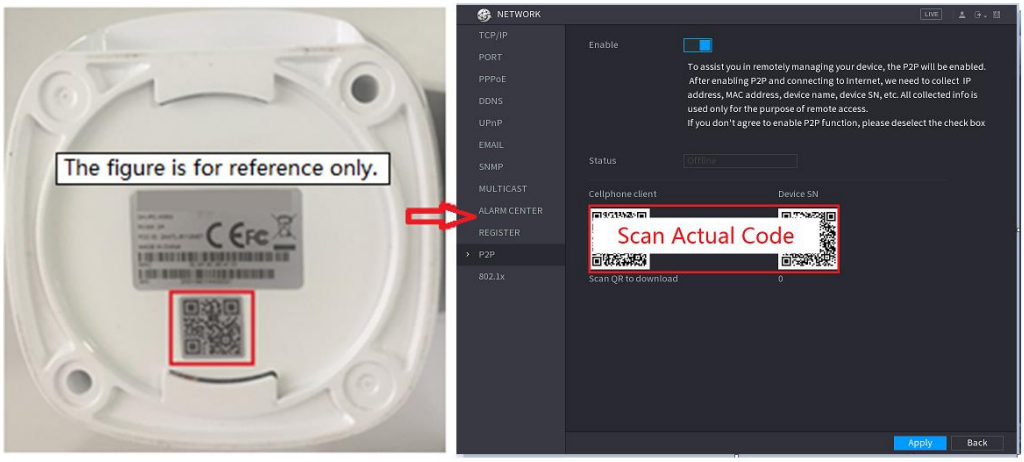
2) Toque el tipo de dispositivo correspondiente (**Dispositivo WiFi** o **Dispositivo cableado)** y luego toque **P2P** para registrar el dispositivo. Vea la Figura 5-3.

Figura 5-3 P2P (2)



3) Escanee la etiqueta del dispositivo o el SN del dispositivo en la interfaz local (**RED> P2P)** para registrar el dispositivo. Vea la Figura 5-4.

Figura 5-4 P2P (3)



4) Después de escanear, puede ver el SN del dispositivo. Hacer clic **Iniciar vista previa en vivo** y tu puedes ver imagen en vivo en el celular.

Apéndice 1 Recomendaciones de ciberseguridad

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

Acciones obligatorias que deben tomarse 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 contenga el nombre de la cuenta o el nombre de la cuenta en orden inverso; No utilice
- caracteres continuos, como 123, abc, etc .; No utilice caracteres superpuestos, como 111,
- aaa, etc .;

2. Actualice el firmware y el software 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 función de "búsqueda automática de actualizaciones" para obtener información oportuna de las actualizaciones de firmware publicadas por el fabricante.

- Le sugerimos que descargue y utilice la última versión del software 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 especial y gabinete, e implemente permisos de control de acceso bien hechos y administración de claves para evitar que el personal no autorizado lleve a cabo contactos físicos como daños en el hardware, conexión no autorizada de equipos extraíbles (como un disco flash USB , puerto serie), etc.

2. Cambie las contraseñas con regularidad

Le sugerimos que cambie las contraseñas con regularidad para reducir el riesgo de ser adivinado o descifrado.

3. Establecer y actualizar contraseñas Restablecer información a tiempo

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 las preguntas de protección por contraseña, se sugiere no utilizar aquellas que se puedan adivinar fácilmente.

4. Habilitar bloqueo de cuenta

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

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

   Le sugerimos que cambie el HTTP predeterminado y otros puertos de servicio en cualquier conjunto de números entre 1024 ~ 65535, reduciendo el riesgo de que personas externas puedan adivinar qué puertos está utilizando.

6. **Habilitar HTTPS**

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

7. **Habilitar lista blanca**

   Le sugerimos que habilite la función de lista blanca 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 blanca.

8. **Enlace de dirección MAC**

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

9. **Asignar cuentas y privilegios de forma 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 autenticación y de cifrado seguras.
    - SMTP: elija TLS para acceder al servidor de buzones de correo. FTP: elija
    - SFTP y configure contraseñas seguras.
    - Punto de acceso AP: elija el modo de cifrado WPA2-PSK y configure contraseñas seguras.

11. **Transmisión encriptada de audio y video**

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

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

12. **Auditoría segura**

    - Verificar usuarios en línea: le sugerimos que verifique a los usuarios en línea con regularidad para ver si el dispositivo está conectado 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 limitada capacidad de almacenamiento del equipo, el registro almacenado es limitado. Si necesita guardar el registro durante mucho tiempo, se recomienda que habilite la función de registro de red para asegurarse de 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:

    - Desactive la función de asignación de puertos del enrutador para evitar el acceso directo a los dispositivos de la intranet desde una red externa.

- La red debe dividirse y aislarse de acuerdo con las necesidades reales de la red. Si no hay requisitos de comunicación entre dos subredes, se sugiere utilizar VLAN, red GAP y otras tecnologías para dividir la red, a fin de lograr el efecto de aislamiento de la red.

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