Grabador de video en red AI

Guía de inicio rápido

V1.0.0

Prefacio

General

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

Las instrucciones de seguridad

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

Palabras de advertencia	Sentido
PELIGRO	Indica un alto riesgo potencial que, si no se evita, provocará la muerte o lesiones graves.
ADVERTENCIA	Indica un riesgo potencial medio o bajo que, si no se evita, podría provocar lesiones leves o moderadas.
PRECAUCIÓN	Indica un riesgo potencial que, si no se evita, podría provocar daños a la propiedad, pérdida de datos, 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

Versión	Contenido de la revisión	Tiempo de liberación
V1.0.0	Primer lanzamiento.	Julio de 2019

Aviso de protección de privacidad

Como usuario del dispositivo o controlador de datos, puede recopilar datos personales de otros, como rostro, huellas dactilares, número de placa del automóvil, dirección de correo electrónico, número de teléfono, GPS, etc. 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 sujeto de los datos la existencia de un área de vigilancia contacto.

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 ocasionada 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 no puede abrir el manual (en
- formato PDF).

- 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, póngase en contacto 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

La siguiente descripción es el método de aplicación correcto del dispositivo. Lea el manual detenidamente antes de usarlo para evitar peligros y pérdidas materiales. Cumpla estrictamente con el manual durante la aplicación y consérvelo correctamente después de leerlo.

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.

Requisitos de energía

- Asegúrese de utilizar el tipo de batería designado. De lo contrario, podría haber riesgo de explosión. Asegúrese de utilizar baterías
- de acuerdo con los requisitos. De lo contrario, puede provocar un incendio,
  Riesgos de explosión o quemaduras de las baterías.
- Para reemplazar las baterías, solo se puede usar el mismo tipo de baterías.
- Asegúrese de desechar las baterías agotadas de acuerdo con las instrucciones.
- El producto utilizará cables eléctricos (cables de alimentación) recomendados por esta área, que se utilizarán dentro de su especificación nominal.
- Asegúrese de utilizar un adaptador de corriente estándar que coincida con este dispositivo. De lo contrario, el usuario deberá asumir las lesiones personales resultantes o daños al Dispositivo.
- Utilice una fuente de alimentación que cumpla con los requisitos de SELV (voltaje de seguridad muy bajo) y suministre energía con un voltaje nominal que cumpla con la Fuente de energía 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 la toma de salida de la red eléctrica, que está equipada con conexión a tierra de protección.
- El acoplador de electrodomésticos es un dispositivo de desconexión. Durante el uso normal, mantenga un ángulo que facilite la operación.

Tabla de contenido

1 Comprobación de los componentes

Toda la instalación y las operaciones aquí deben cumplir con las normas locales de seguridad eléctrica.

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.

Elementos de verificación de secuencia			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 llame al servicio posventa.
3	Dispositivo	Apariencia	Ningún daño evidente.
		Cables de datos, potencia cables, cables de ventilador, placa base	No hay conexión suelta. Si hay alguno suelto, póngase en contacto con el servicio posventa de la empresa a tiempo.

2 Instalación de HDD

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

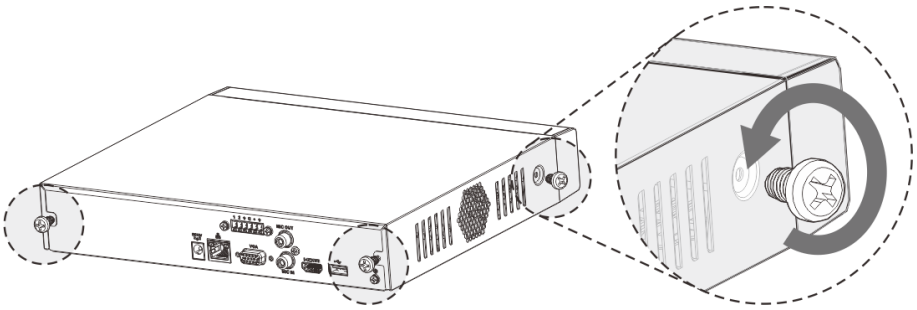
Apague la alimentación antes de reemplazar el disco duro.

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

2.1 1 disco duro

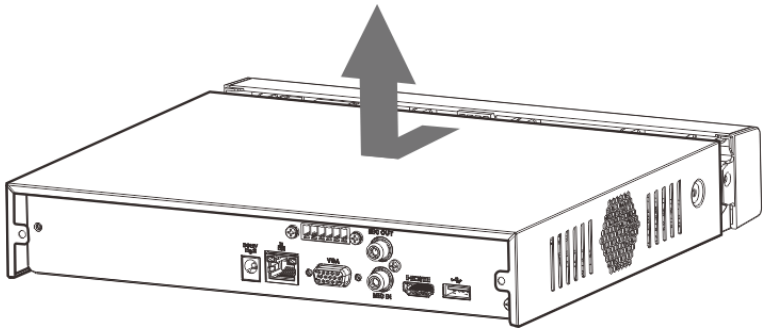
Paso 1 Quite los tornillos de fijación de la tapa de la carcasa (incluidos los dos tornillos del panel trasero y dos tornillos en los paneles izquierdo y derecho).

Figura 2-1 Instalación de HDD (1)



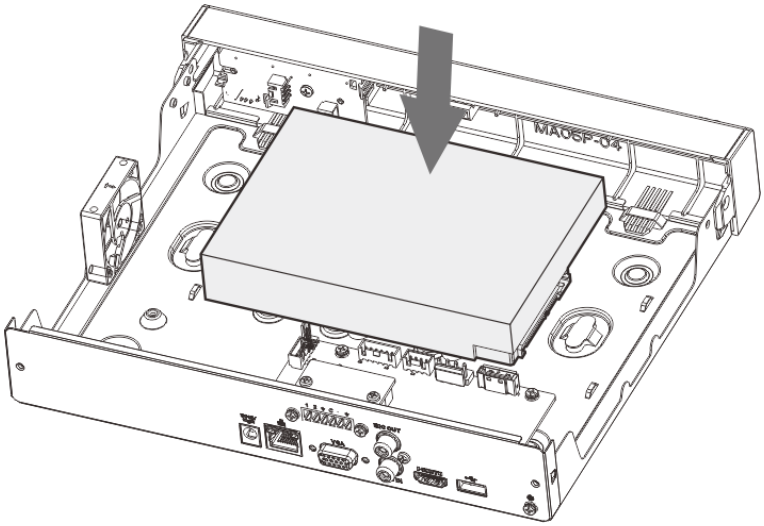
Paso 2 Retire la tapa de la carcasa en la dirección que se muestra en la siguiente flecha.

Figura 2-2 Instalación de HDD (2)



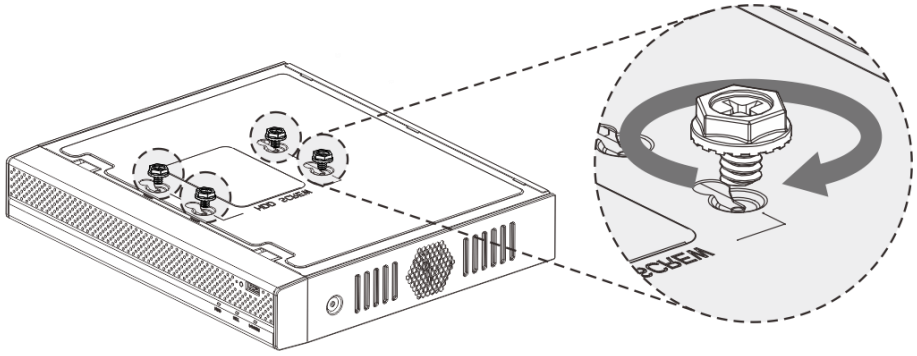
Paso 3 Haga coincidir los cuatro orificios de la placa base para colocar el disco duro.

Figura 2-3 Instalación de HDD (3)



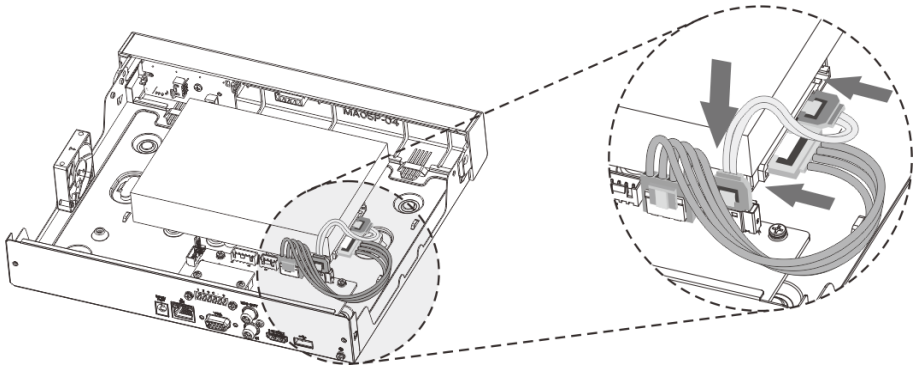
Paso 4 Coloque el dispositivo boca abajo, haga coincidir los tornillos con los orificios del disco duro y luego sujetarlos. El disco duro se fija al zócalo.

Figura 2-4 Instalación de HDD (4)



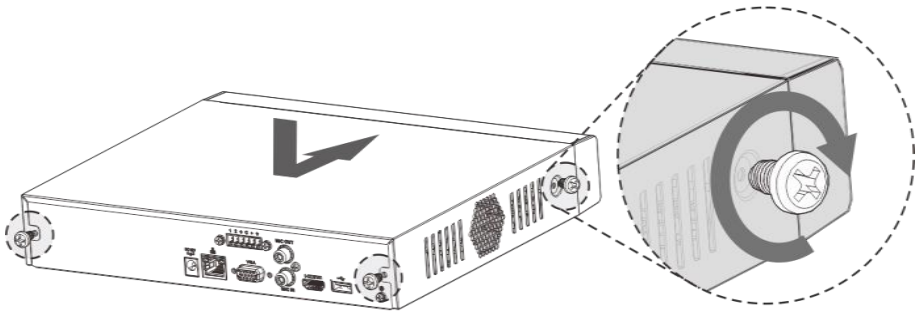
Paso 5 Conecte el cable de datos del disco duro y el cable de alimentación al dispositivo.

Figura 2-5 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.

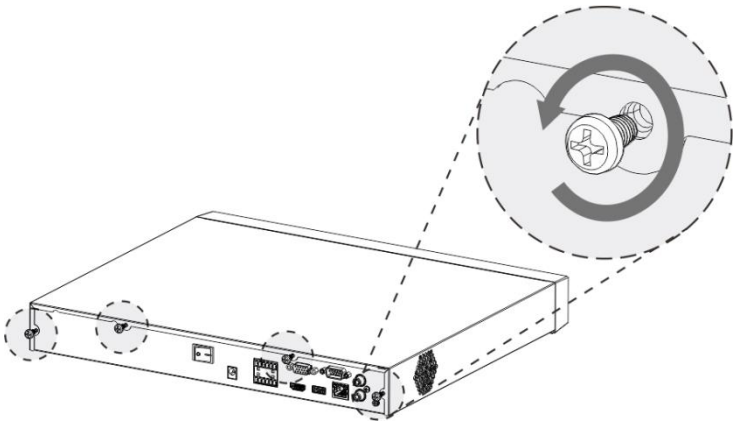
Figura 2-6 Instalación de HDD (6)



2.2 2 HDD

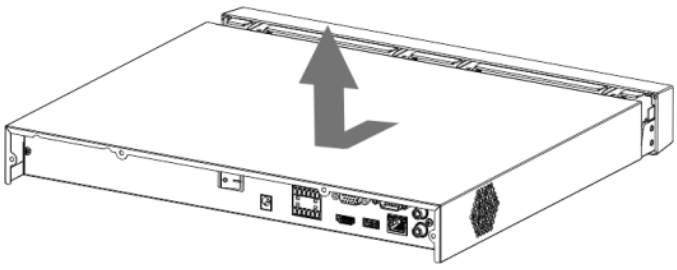
Paso 1 Quite los cuatro tornillos de fijación del panel trasero.

Figura 2-7 Instalación de HDD (1)



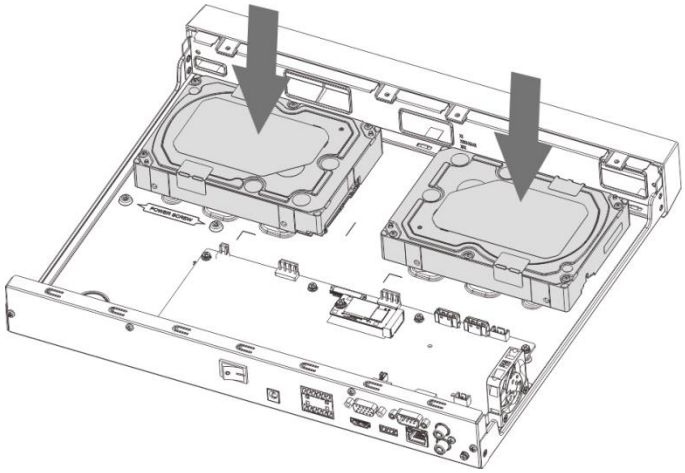
Paso 2 Retire la tapa de la carcasa en la dirección que se muestra en la siguiente flecha.

Figura 2-8 Instalación de HDD (2)



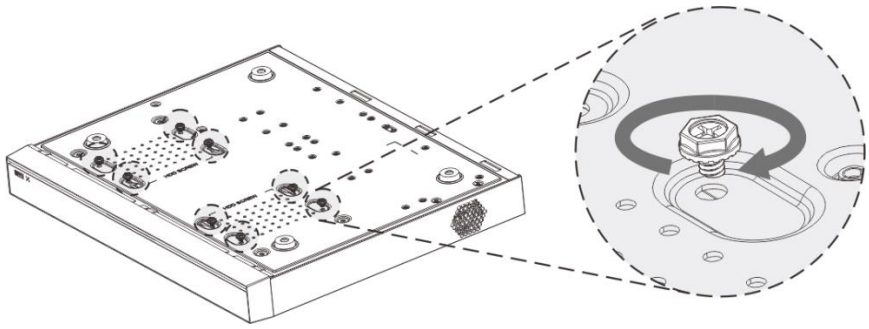
Paso 3 Haga coincidir los cuatro orificios de la placa base para colocar el disco duro.

Figura 2-9 Instalación de HDD (3)



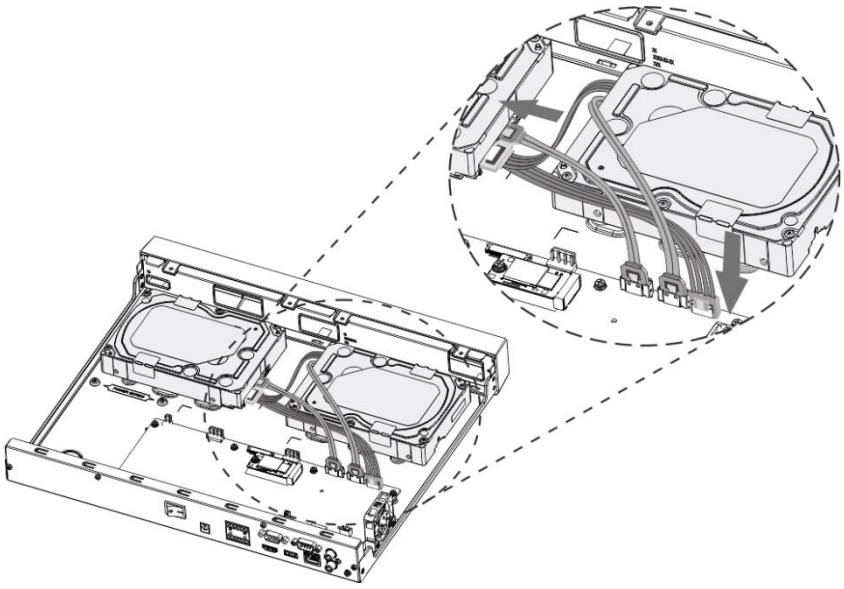
Paso 4 Coloque el dispositivo boca abajo, haga coincidir los tornillos con los orificios del disco duro y luego sujetarlos. El disco duro se fija al zócalo.

Figura 2-10 Instalación de HDD (4)



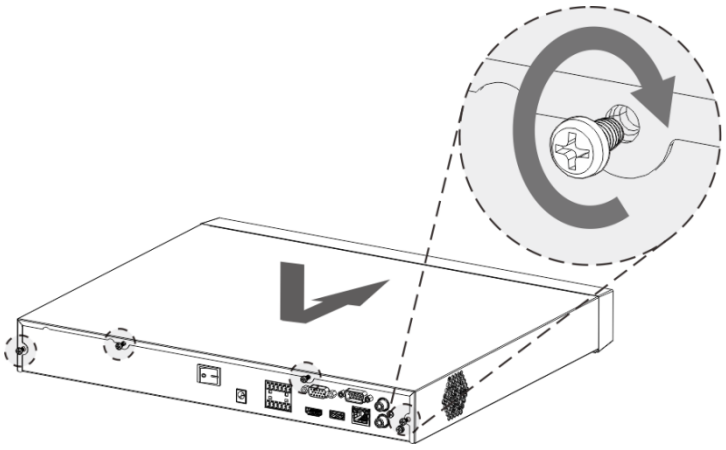
Paso 5 Conecte el cable de datos del disco duro y el cable de alimentación al dispositivo.

Figura 2-11 Instalación de HDD (5)



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

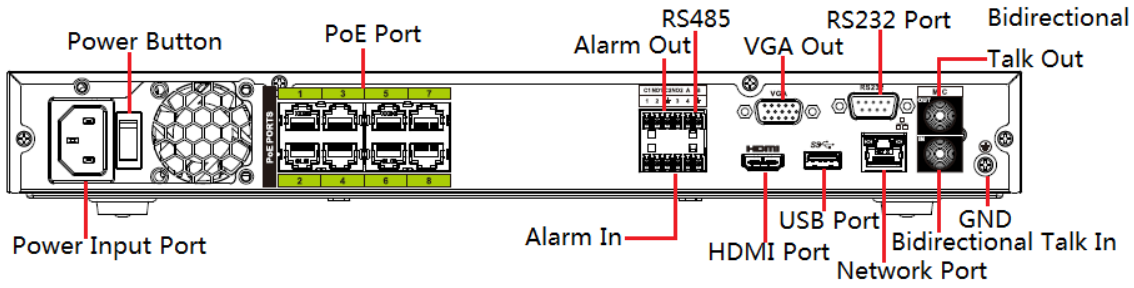
Figura 2-12 Instalación de HDD (6)



3 Conexión

La siguiente figura es solo para referencia. El producto real regirá. Para obtener más detalles, consulte *Manual de usuario.*

Figura 3-1 Ejemplo de conexión



4 Operaciones de GUI

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

4.1 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 encienda 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.

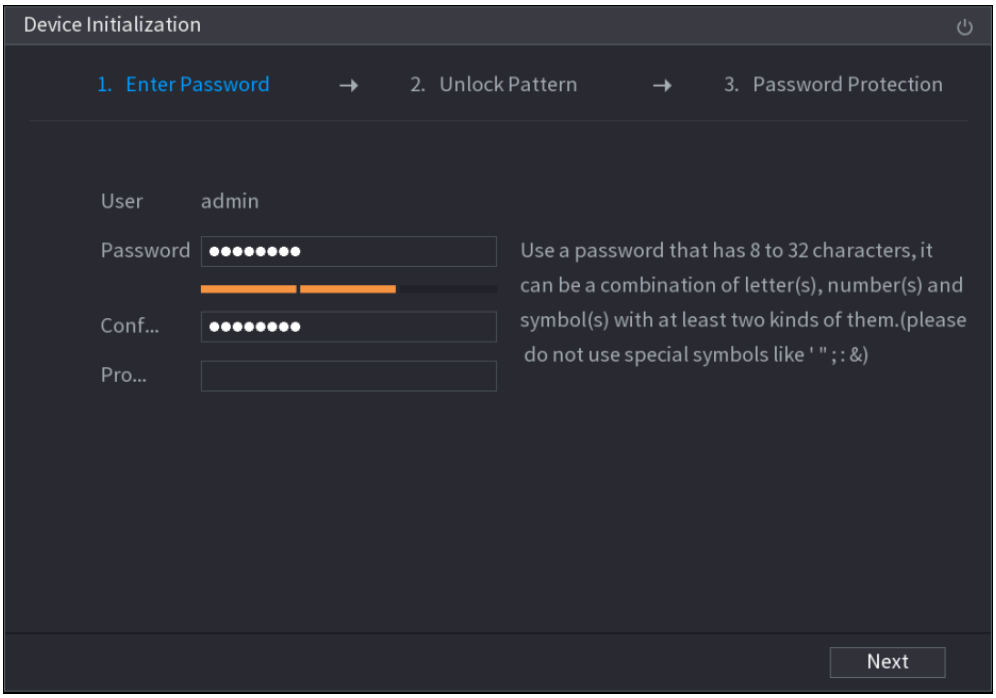
4.2 Inicialización del dispositivo

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 4-1.

Figura 4-1 Ingrese la contraseña



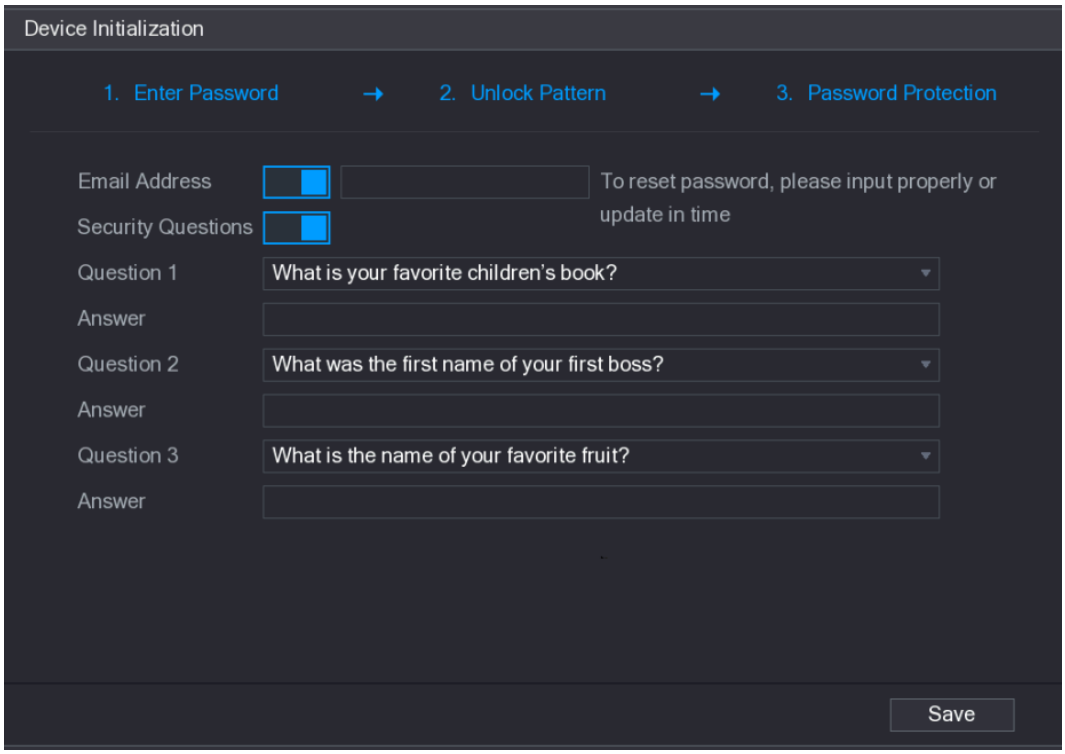
Paso 2 Configure la contraseña, confirme la contraseña y luego ingrese la pregunta inicial. La contraseña se puede establecer de 8 a 32 caracteres y contener al menos dos tipos de números, letras y caracteres especiales (excluyendo '"', '"' "," ; "," : "y" & "). Se recomienda para establecer una contraseña de alta seguridad de acuerdo con el mensaje. Configure el patrón de desbloqueo o haga clic en **Omitir.**

Paso 3

Después de configurar el patrón de desbloqueo, se muestra la interfaz de configuración de protección con contraseña. Vea la Figura 4-2.

- 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.

Figura 4-2 Protección por contraseña



Paso 4 Configure la protección por contraseña. Para obtener más detalles, consulte la Tabla 4-1.

- 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 4-1 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 5 Haga clic en **Okay** para completar la configuración.

los **Asistente de inicio** se muestra la interfaz. Para obtener más detalles, consulte *Manual de usuario.*

4.3 Modificar la dirección IP

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

Se muestra la interfaz TCP / IP. Vea la Figura 4-3.

Paso 2 Haga clic en  .

los **Editar** se muestra la interfaz. Vea la Figura 4-4.

Paso 3 Modifique la dirección IP de acuerdo con el plan de red real (la dirección IP predeterminada es 192.168.1.108).

Figura 4-3 TCP / IP

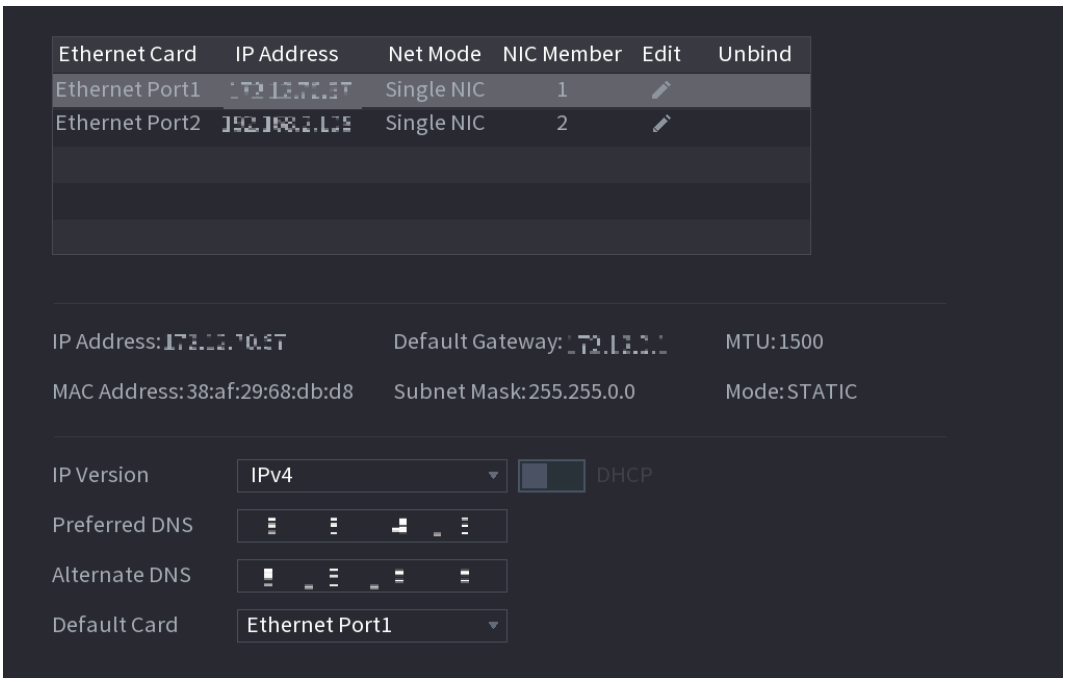
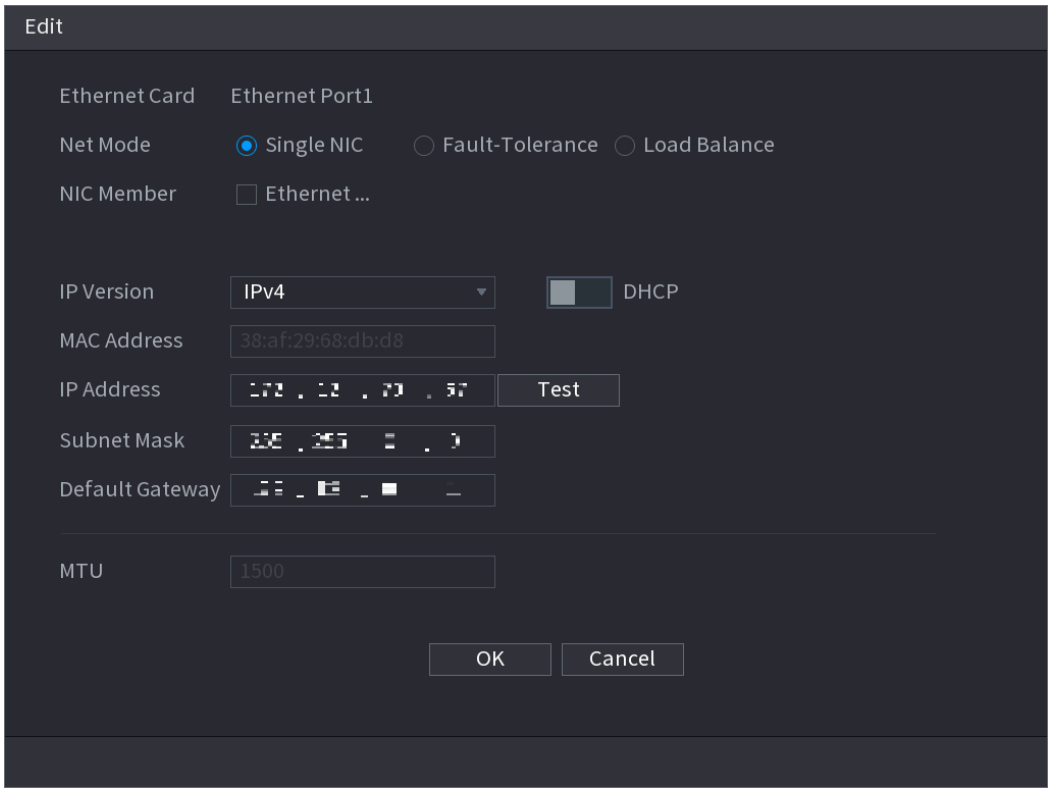


Figura 4-4 Editar



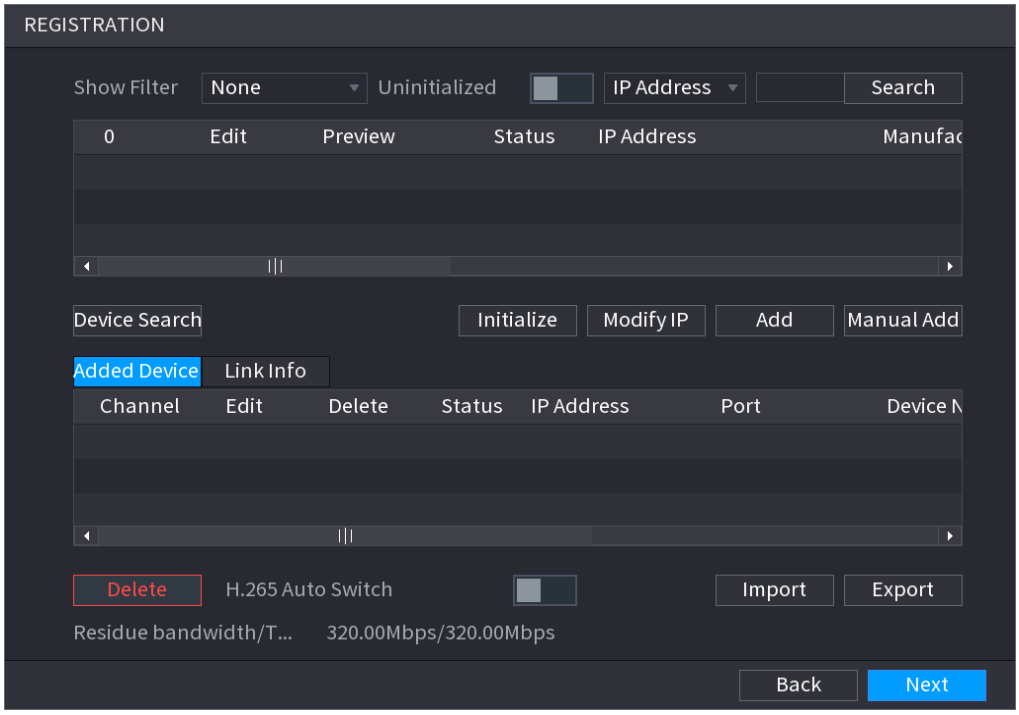
4.4 Registro de cámara

Seleccione **Menú principal> CÁMARA> Registro.** los **Registro** se muestra la interfaz. Vea la Figura 4-5.

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 4-5 Registro

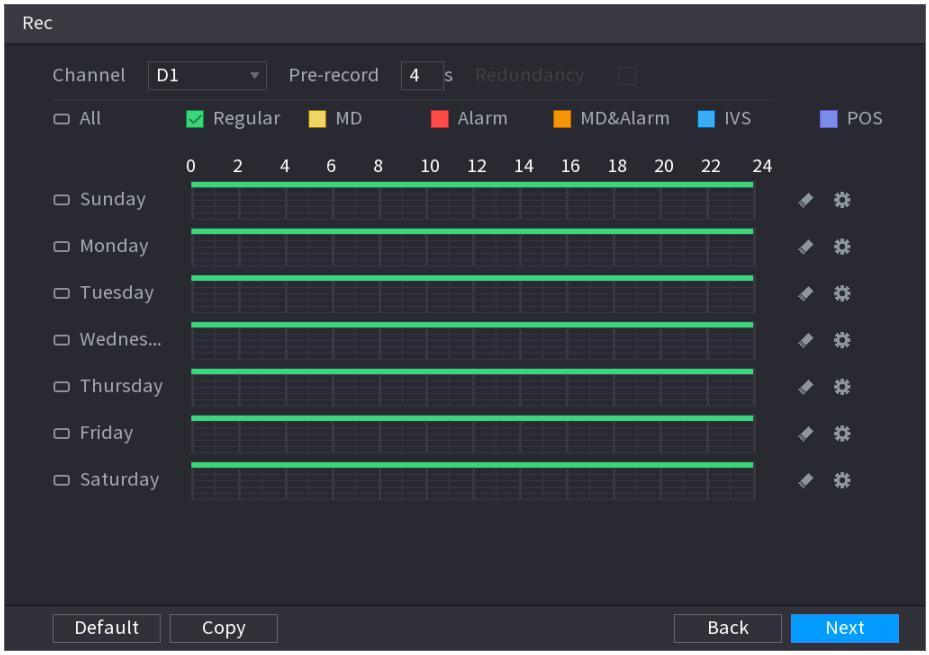


4.5 Calendario

Seleccione **Menú principal> ALMACENAMIENTO> HORARIO> Rec.** los **Rec** se muestra la interfaz. Vea la Figura 4-6.

De acuerdo con las necesidades reales, arrastre el mouse en la figura de tiempo para dibujar el período o haga clic para configurar el tiempo de registro.

Figura 4-6 Programación



4.6 Reproducción de grabación

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 4-7.

El sistema puede reproducir registros de acuerdo con los criterios de selección, como el tipo de registro, el tiempo de registro y el canal.

Figura 4-7 Búsqueda de registros

4.7 Apagar

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

5 Operaciones web

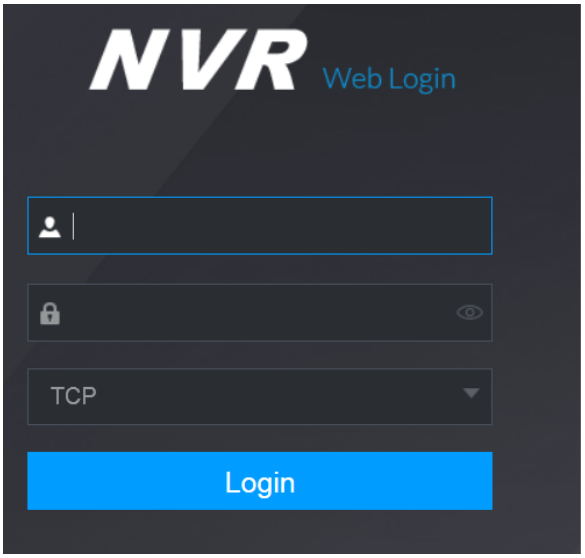
Si es la primera vez que inicia sesión en el dispositivo, primero debe inicializar el dispositivo. Para obtener información detallada, consulte *Manual de usuario.*

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 5-1.

Figura 5-1 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.

6 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.**

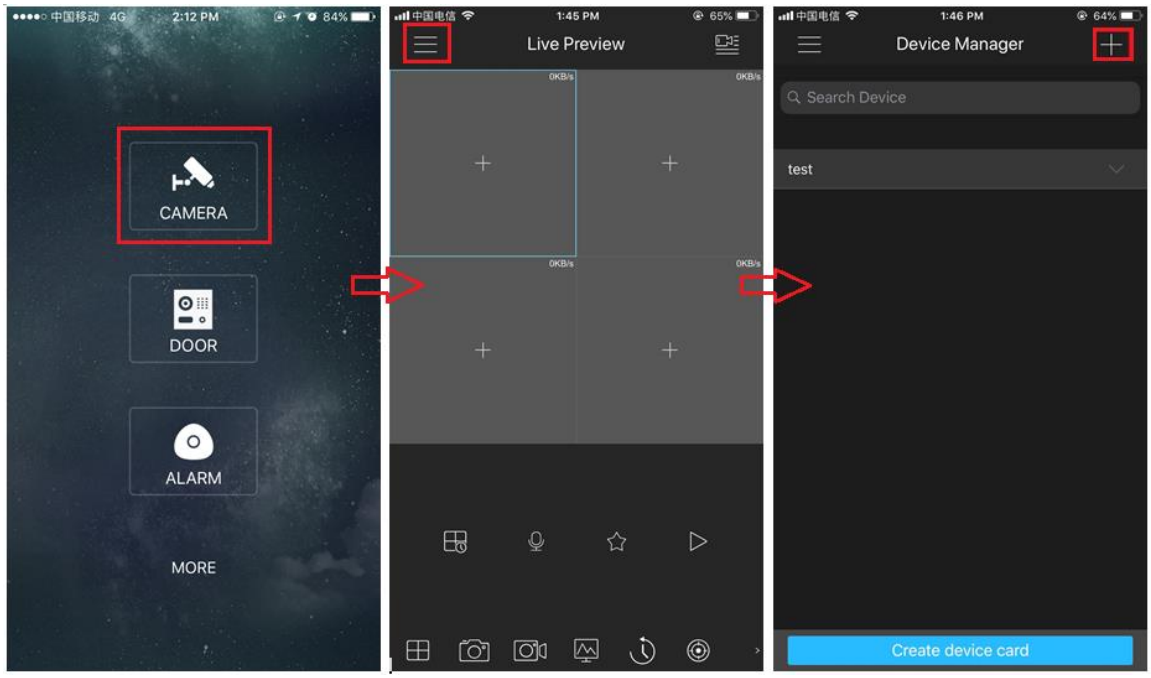
Figura 6-1 Código QR de la aplicación móvil

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 móvil.

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

Figura 6-2 Administrador de dispositivos



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.