Estación de recolección de datos

Manual de usuario

V1.0.1

Prefacio

Las instrucciones de seguridad

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

Palabras de advertencia	Significado
PELIGRO	Indica un peligro de alto potencial que, si no se evita, provocará la muerte o lesiones graves.
ADVERTENCIA	Indica un peligro 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 revisión	Tiempo de liberación
V1.0.1	Actualizado "1.1 Introducción".	mayo 2021
V1.0.0	Primer lanzamiento.	marzo 2021

Medidas de seguridad y advertencias importantes

Este capítulo describe el contenido que cubre el manejo adecuado de la Estación de recopilación de datos (en lo sucesivo, "la Estación"), la prevención de riesgos y la prevención de daños a la propiedad. Lea este contenido detenidamente antes de utilizar la estación, respételos cuando la utilice y guarde bien el manual para futuras consultas.

Requisito de operación

- No coloque ni instale la Estación en un lugar expuesto a la luz solar o cerca de una fuente de calor.
- Mantenga la estación alejada de la humedad, el polvo o el hollín.
- Mantenga la Estación instalada horizontalmente en un lugar estable para evitar que se caiga.
- No deje caer ni salpique líquido sobre la estación y asegúrese de que no haya ningún objeto lleno de líquido sobre la estación para evitar que el líquido fluya hacia la estación.
- Instale la estación en un lugar bien ventilado y no bloquee la ventilación del escáner.
- Opere la estación dentro del rango nominal de entrada y salida de energía.
- No desmonte la estación.
- Transporte, use y almacene la Estación en las condiciones de humedad y temperatura permitidas.

Seguridad ELECTRICA

- Reemplácelas siempre con el mismo tipo de baterías.
- Utilice los cables de alimentación recomendados en la región y cumpla con la especificación de potencia nominal.
- Utilice el adaptador de corriente proporcionado con la Estación; de lo contrario, podría provocar lesiones personales y daños en el dispositivo.
- La fuente de alimentación debe cumplir con los requisitos de la norma de voltaje extra bajo de seguridad (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 fuente de alimentación está sujeto a la etiqueta del dispositivo.
- Conectar la Estación (estructura tipo I) a la toma de corriente con puesta a tierra de protección.
- El acoplador del aparato es un dispositivo de desconexión. Cuando use el acoplador, mantenga el ángulo para facilitar la operación.

Tabla de contenido

1.1 Introducción

Al trabajar con una cámara corporal, la Estación puede adquirir los datos de las cámaras corporales y cargarlas. La estación puede reconocer automáticamente y conectar la cámara corporal conectada a través del puerto USB. Al trabajar con la plataforma de centro móvil portátil, la estación puede autorizar la cámara corporal y adquirir automáticamente la evidencia electrónica (video, audio e instantánea). La estación contiene un módulo de control y un módulo de recopilación de datos. Un módulo de control puede admitir 4 módulos de recopilación de datos como máximo.

1.2 Características

- Recargue y recopile datos de un máximo de 32 cámaras corporales al mismo tiempo. Actualice
- las cámaras corporales de forma automática o manual.
- Cree automáticamente un archivo y luego guarde los datos electrónicos recopilados.
- Cargue automáticamente la evidencia a FTP o Portable Mobile Center Platform. Sincroniza
- automáticamente la hora.
- Cuando hay más de 1 módulo de recolección de datos, la Estación recolectará datos de la cámara corporal en los muelles fijos de cada módulo de recolección de datos en prioridad.
- Puede buscar, editar, transcodificar, reproducir, ver, eliminar y administrar todos los datos de la estación.

1.3 Apariencia del producto

1.3.1 Módulo de control

Figura 1-1 Panel frontal y panel posterior

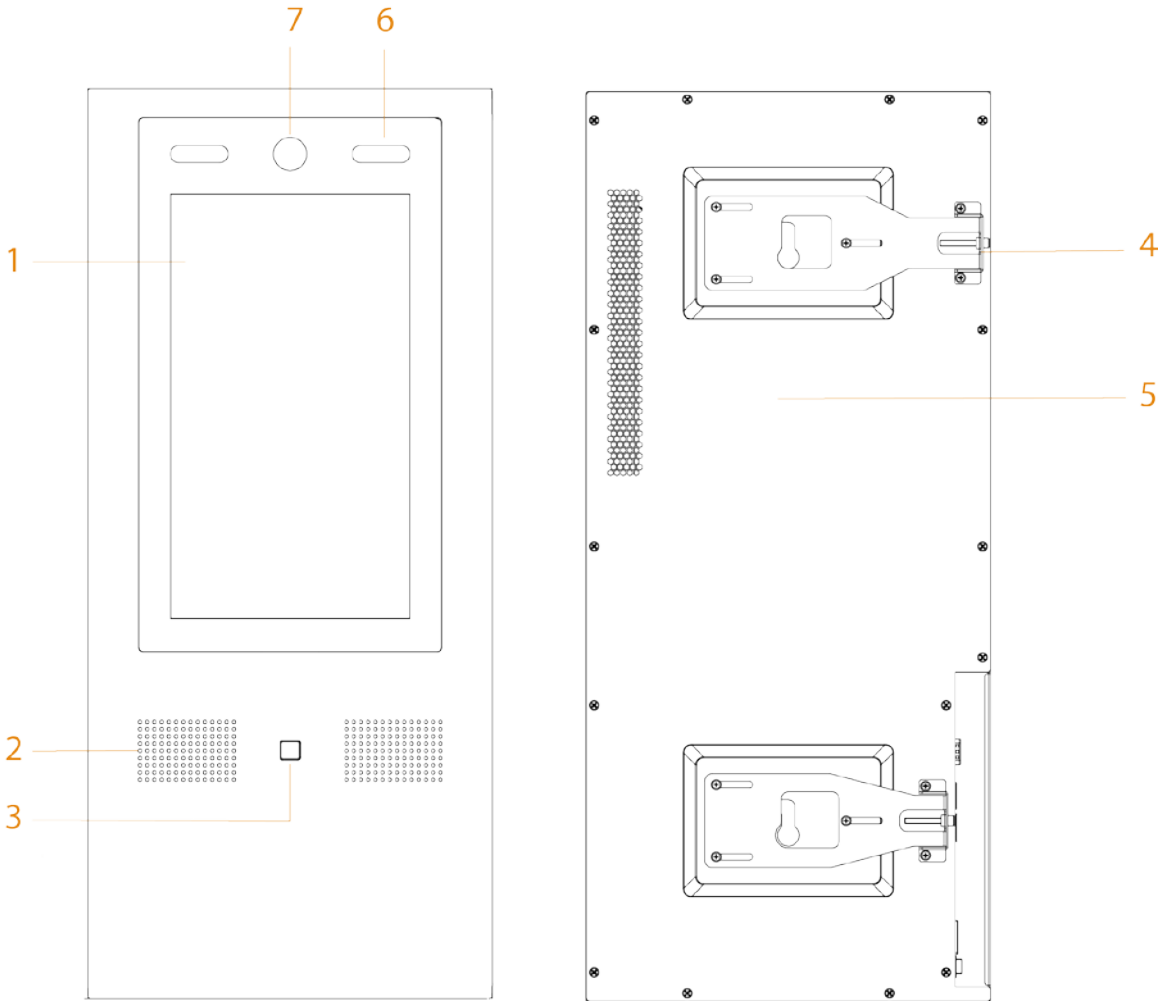


Figura 1-2 Panel lateral

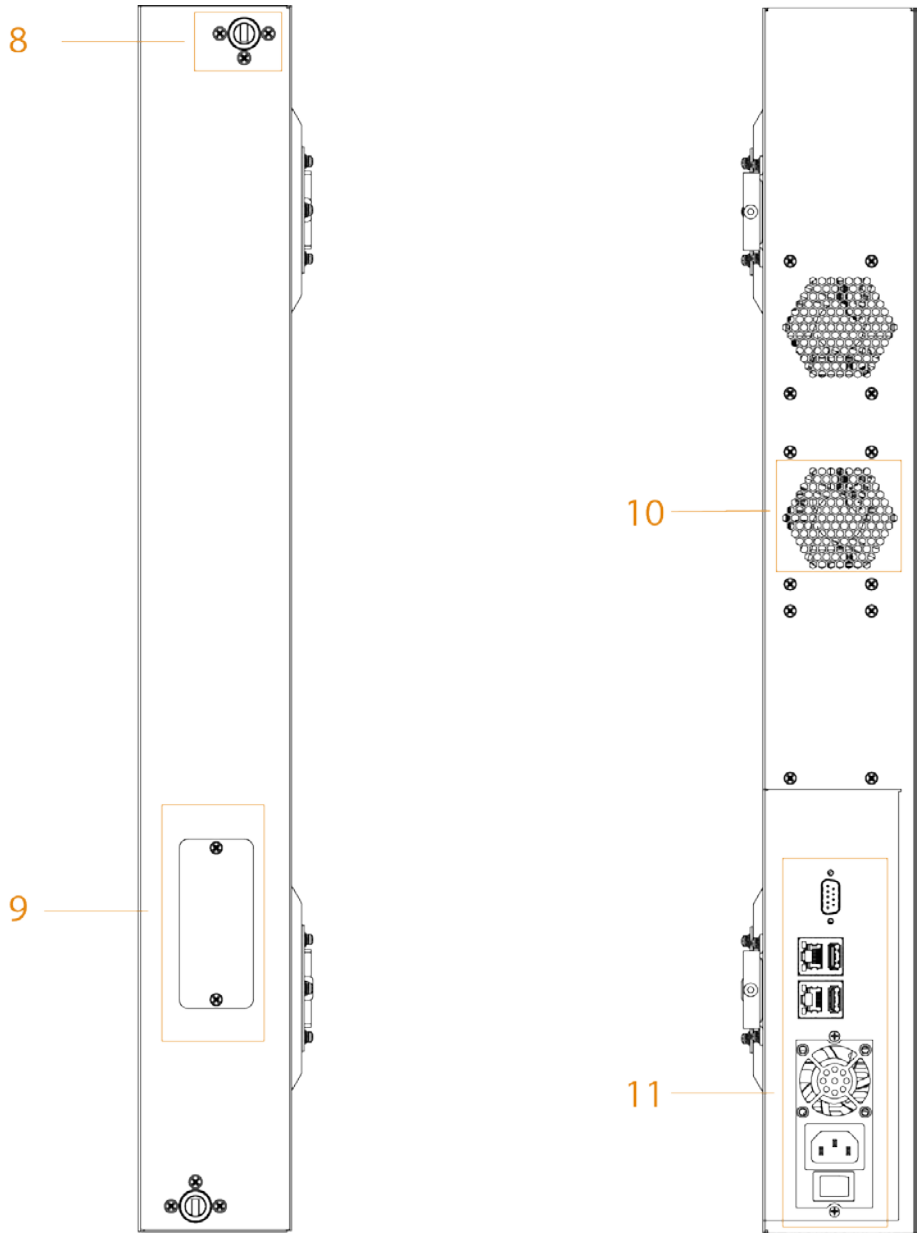


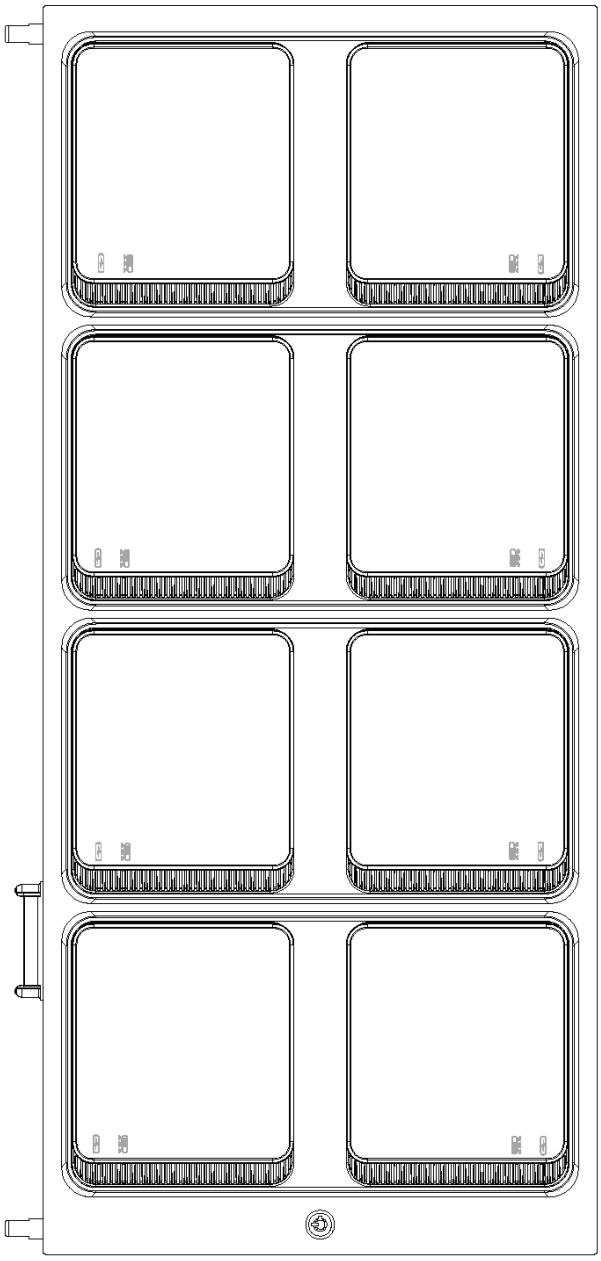
Tabla 1-1 Descripción de la apariencia

No.	Nombre	Descripción
1	Pantalla táctil	Pantalla táctil de 13,3 pulgadas.
2	Vocero	Salida de audio.
3	Sensor de huellas dactilares	Agregue datos de huellas dactilares o desbloquee por huellas dactilares. Se pueden agregar como máximo 3 huellas dactilares para cada usuario.
4	Tablero de ajuste	Retire el módulo de control cuando conecte el módulo de control y los módulos de recopilación de datos.
5	Cubierta trasera	—
6	luz blanca	- Proporciona luz adicional al reconocer rostros. Proporciona luz - adicional a la cámara en condiciones de oscuridad.
7	Cámara	Reconoce la información de la cara. Puede desbloquear la estación a través del reconocimiento facial.
8	carcasa del eje.	Conecta el módulo de control y los módulos de recopilación de datos. Uno está en la parte superior y el otro en la parte inferior.

No.	Nombre	Descripción
9	Conector.	Transfiere los datos del módulo de control y los módulos de recopilación de datos.
10	Disipación de calor agujero	—
11	Puertos	Incluye puerto de entrada de alimentación, puertos USB, puertos Ethernet y puerto RS-232. Para obtener más información, consulte la Tabla 1-2.

1.3.2 Aspecto de los módulos de recopilación de datos

Figura 1-3 Aspecto de los módulos de recopilación de datos



- Coloque cámaras corporales en los muelles para la recopilación de datos. Cuando hay más de 1 recogida de datos módulos, se recogerán primero los datos de las cámaras corporales en los dos muelles de la primera fila.
- Hay dos iconos debajo de un muelle: indica recarga; indica la recopilación de datos.
- Cuando no se puede abrir un muelle, puede abrirlo con la llave.

1.4 Descripción de los botones

Figura 1-4 Puertos

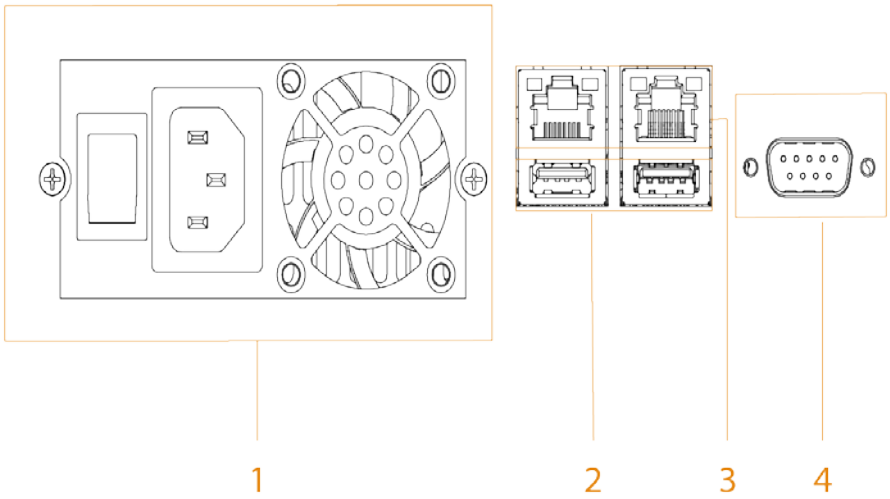


Tabla 1-2 Descripción del puerto

No.	Nombre	Descripción
1	Entrada de alimentación	Entradas de alimentación de CA de 100 V–240 V para la estación. Después de apagar la Estación, el ventilador funcionará durante un período para enfriar la Estación.
2	puertos USB	Conéctese a dispositivos de almacenamiento USB (USB2.0 y USB3.0), mouse y más.
3	ethernet	2 puertos Gigabit. Cuando usa dos puertos al mismo tiempo, solo un puerto puede obtener la puerta de enlace automáticamente. Para la otra tarjeta Ethernet, deshabilite la función de obtener la dirección IP automáticamente.
4	RS-232	Se utiliza para la depuración serial común, la configuración de direcciones IP y la transmisión de datos de serial transparente.

1.5 Encendido

La cubierta de la Estación tiene electricidad estática, lo que podría provocar una descarga eléctrica. Para evitar la electricidad choque, asegúrese de que la estación esté bien conectada a tierra.

Paso 1 Conecte el cable de alimentación y el cable de red.

Paso 2 Presiona el boton de poder.

Todo el proceso tomará un período de tiempo. Por favor sea paciente.

Conexión de 2 dispositivos

2.1 Conexión del módulo de control y el módulo de recopilación de datos

- Puede conectar 4 módulos de recopilación de datos al módulo de control como máximo.
- Para los detalles de instalación, consulte las instrucciones en el mapa de posicionamiento.

Paso 1 Fije el módulo de control en la pared.

Paso 2 Pegue el mapa de posicionamiento del módulo de recopilación de datos en la pared.

Paso 3 Fije el módulo de recopilación de datos de acuerdo con las instrucciones en el mapa de posicionamiento.

2.2 Conexión de la cámara corporal y el módulo de recopilación de datos

Después de iniciar la estación, conecte las cámaras corporales a la estación y luego podrá recopilar datos de las cámaras corporales y recargarlas.

Asegúrese de que la conexión de las cámaras corporales y el módulo de recopilación de datos sea correcta, y que el cuerpo las cámaras están colocadas en las ranuras correctamente. Si las cámaras corporales no se colocan correctamente en las ranuras, el las cámaras pueden caerse cuando se abren las bases o las bases no se pueden abrir.

Las ranuras están diseñadas exclusivamente para la cámara corporal MPT220 de forma predeterminada. Si quieres usarlos para Cámara corporal MPT210, use la ranura separada en el paquete de accesorios.

Paso 1 Abra la base a través de la pantalla táctil o la tecla y luego saque el cable de datos.

No tire violentamente del cable de datos. De lo contrario, podría dar como resultado un resorte no válido o un puerto que se afloja. conexión.

Figura 2-1 Saque el cable de datos (ranura MPT220)

Figura 2-2 Saque el cable de datos (ranura MPT210)

Paso 2 Conecte el cable de datos a la cámara corporal hasta que la estación muestre el cuadro de diálogo de conexión exitosa.

Figura 2-3 Dispositivo de conexión (ranura MPT220)

Figura 2-4 Dispositivo de conexión (ranura MPT210)

Paso 3 Después de la conexión, coloque la cámara corporal en la base y luego podrá recopilar datos y recargar la cámara corporal.

- Para la cámara corporal MPT220, inserte el dispositivo en la ranura.
- Para la cámara corporal MPT210, inserte el clip en la ranura. Solo cámara corporal MPT210 con el último clip se puede insertar en la ranura. Consulte la Figura 2-4.

Figura 2-5 Recopilación de datos (ranura MPT220)

Figura 2-6 Recopilación de datos (ranura MPT210)

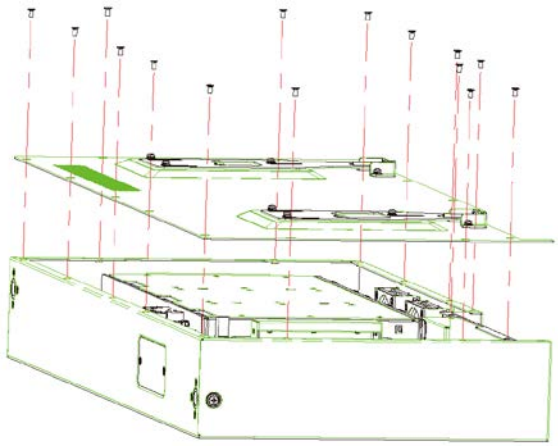
3 Instalación de disco duro

Puede instalar seis HDD 10T (unidades de disco duro).

- Para evitar espacio de almacenamiento insuficiente, se recomiendan discos duros de más de 2T.
- Para reducir la presión de escritura de cada HDD, le recomendamos que instale al menos 2 HDD con la misma capacidad de recogida de datos y recarga.

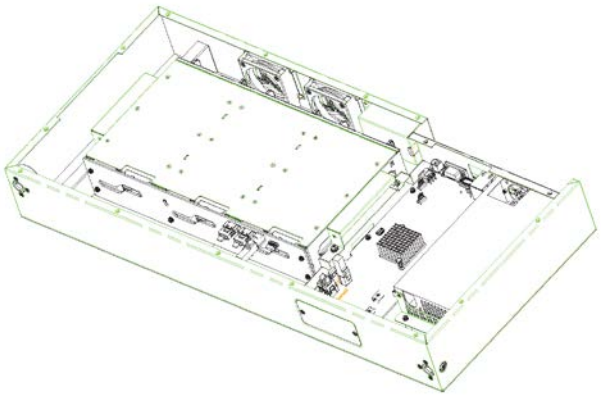
Paso 1 Afloje los tornillos de la cubierta trasera y luego retire la cubierta trasera.

Figura 3-1 Retire la cubierta trasera



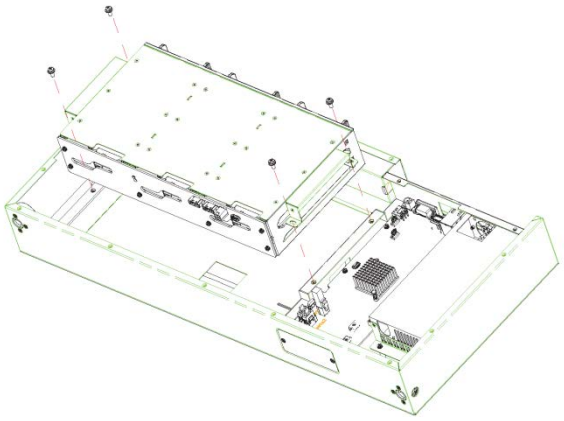
Paso 2 Desconecte los cables entre la placa principal y la placa HDD.

Figura 3-2 Cable suelto



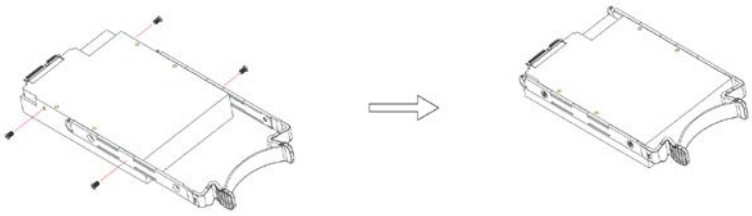
Paso 3 Afloje los cuatro tornillos fijos en la caja del disco duro y luego saque la caja.

Figura 3-3 Saque la caja del disco duro



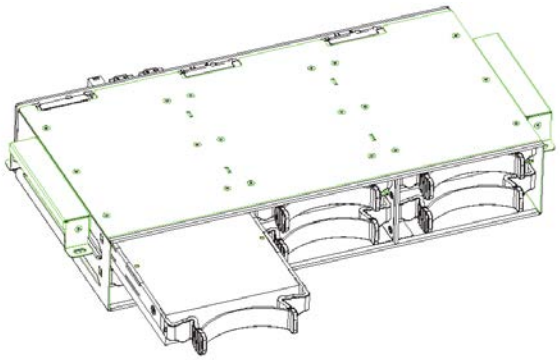
Paso 4 Arreglar discos duros.

Figura 3-4 Reparar HDD



Paso 5 Instalar discos duros. Empuje los HDD fijos en la caja HDD.

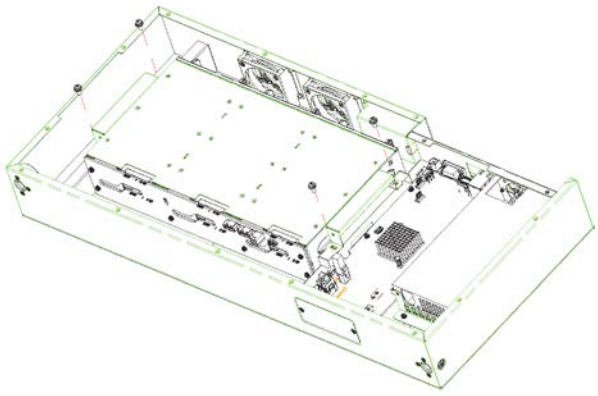
Figura 3-5 Instalar HDD



Empuje los discos duros en la dirección que muestran el puerto del disco duro y el puerto de la placa principal.

Paso 6 Fije la caja HDD en el chasis.

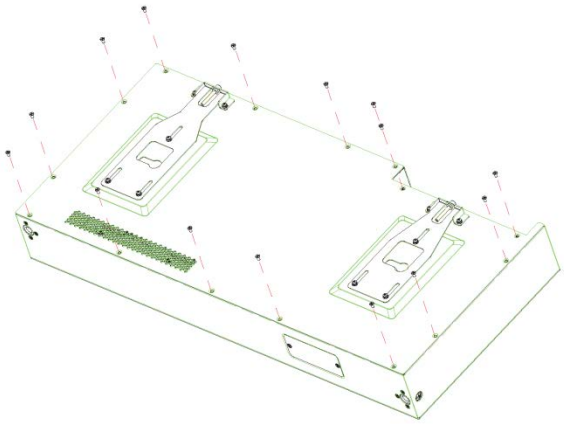
Figura 3-6 Instale la caja HDD



Paso 7 Conecte el cable entre la placa principal y la placa HDD. Arregla la

Paso 8 cubierta.

Figura 3-7 Fije la cubierta



4 Configuración y funcionamiento

4.1 Generalidades

Figura 4-1 Interfaz principal

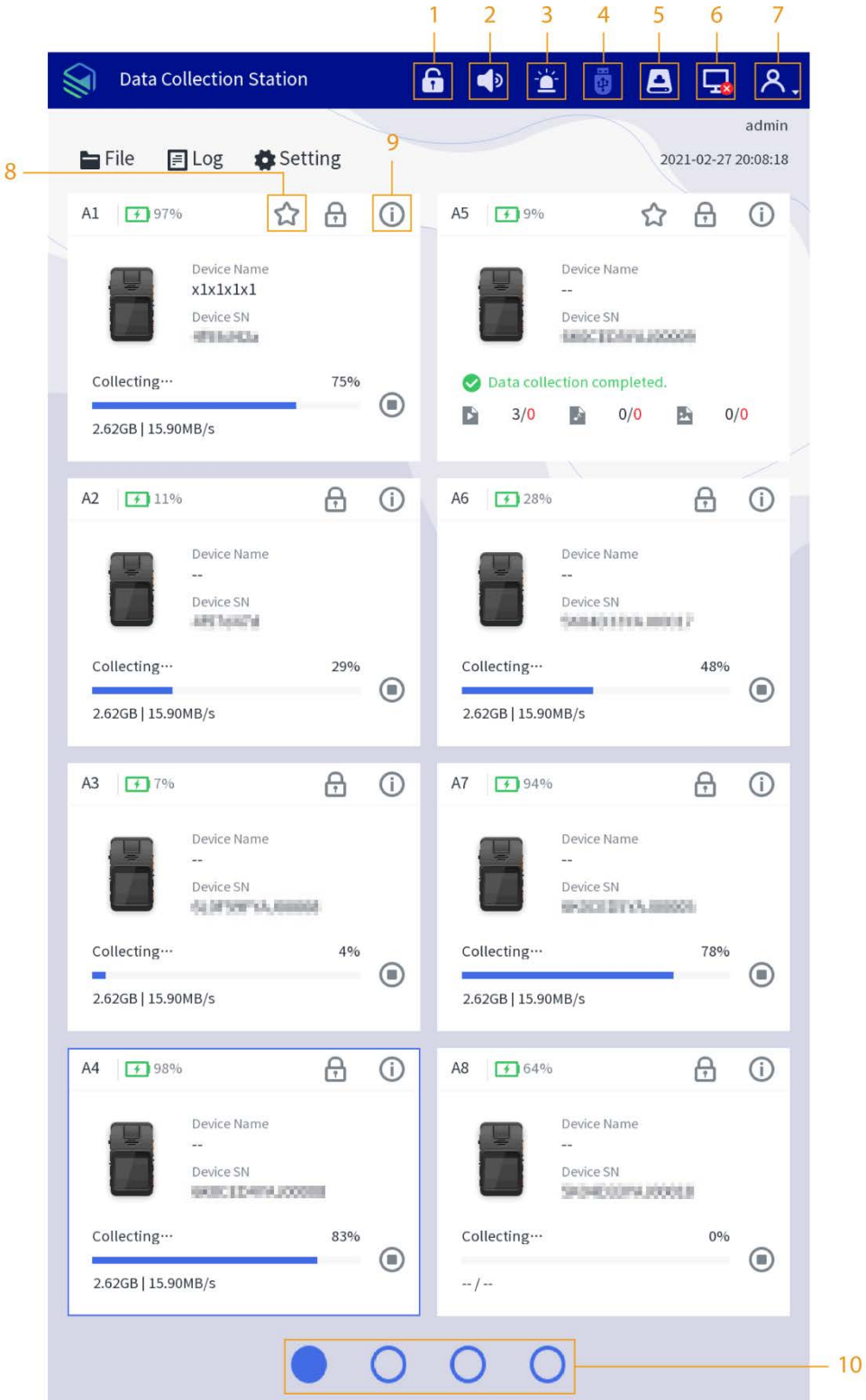


Tabla 4-1 Descripción de la interfaz principal

No.	Descripción
1	Desbloquee el muelle con un toque.
2	Alarma. Tóquelo y la melodía de la alarma se desactivará.
3	Pantalla de información de alarma. La luz roja parpadea cuando hay alarma.
4	Dispositivo de almacenamiento USB externo. Gris significa que no hay ningún dispositivo de almacenamiento USB conectado.
5	Ver la capacidad del disco duro.
6	: Indica que se está cargando un archivo; : Indica que no se está cargando ningún archivo.
7	Iniciar sesión, cerrar sesión, reiniciar, apagar y editar la información del usuario.
8	indica la recopilación de datos en prioridad, lo que puede mejorar la velocidad de recopilación del muelle correspondiente. Para habilitar esta función, debe conectar al menos dos módulos de recopilación de datos. Él La función es compatible con los dos muelles de la primera fila en cada módulo de recopilación de datos.
9	Ver métodos de actualización de la estación y cámaras corporales. Hacer clic**obligar a hacer cumplir**sobre el**Información del dispositivo**interfaz, ingrese el nombre del ejecutor y el ejecutor no, haga clic**Búsqueda**y, a continuación, seleccione el ejecutor que desea vincular.
10	Cambiar las interfaces de los módulos de recopilación de datos. Admite 4 interfaces como máximo.

4.1.1 Gestión de archivos

4.1.1.1 Colección de archivos

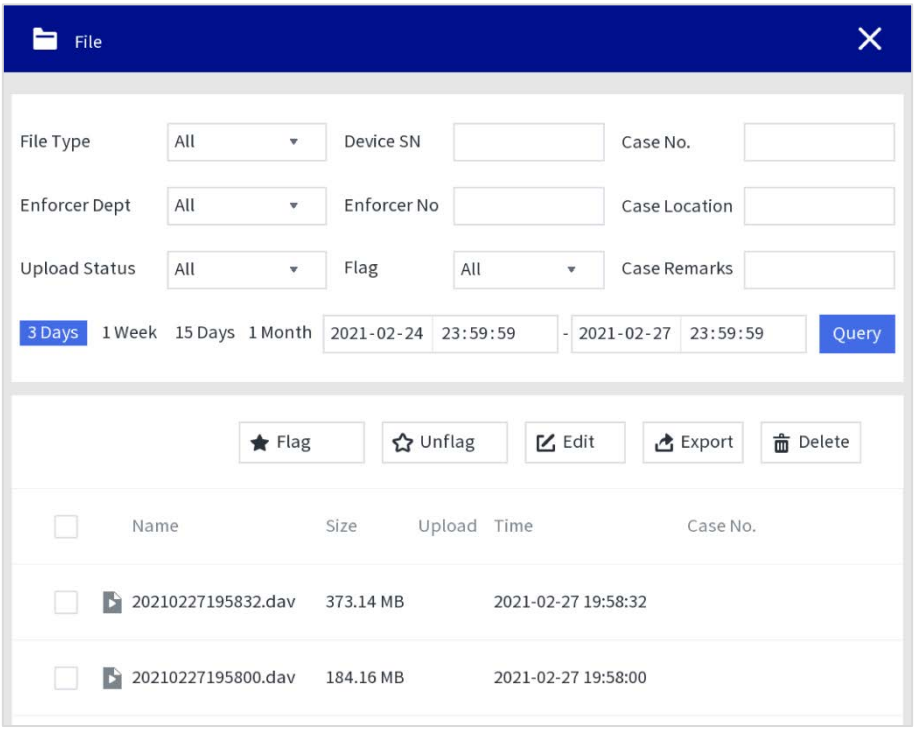
Después de recopilar los archivos de datos de las cámaras corporales, la Estación cargará los archivos en la plataforma de acuerdo con la configuración en**Almacenamiento**.

4.1.1.2 Búsqueda de archivos

Puede buscar archivos de video, archivos de audio e instantáneas de acuerdo con las condiciones configuradas, incluido el tipo de archivo, el departamento del ejecutor, el estado de carga, el número de serie del dispositivo, el número del ejecutor, la bandera, el número del caso, la ubicación del caso, los comentarios del caso, la hora de inicio y la finalización. tiempo.

El rango de tiempo máximo para la búsqueda de archivos es de 1 mes.

Figura 4-2 Búsqueda de archivos



4.1.1.3 Visualización de archivos

Haga doble clic en un archivo para ver los detalles y podrá realizar las operaciones de reproducción rápida, reproducción lenta, acercamiento o alejamiento.

No puede reproducir rápidamente o reproducir lentamente un archivo de audio en formato AMR.

4.1.2 Búsqueda de registro

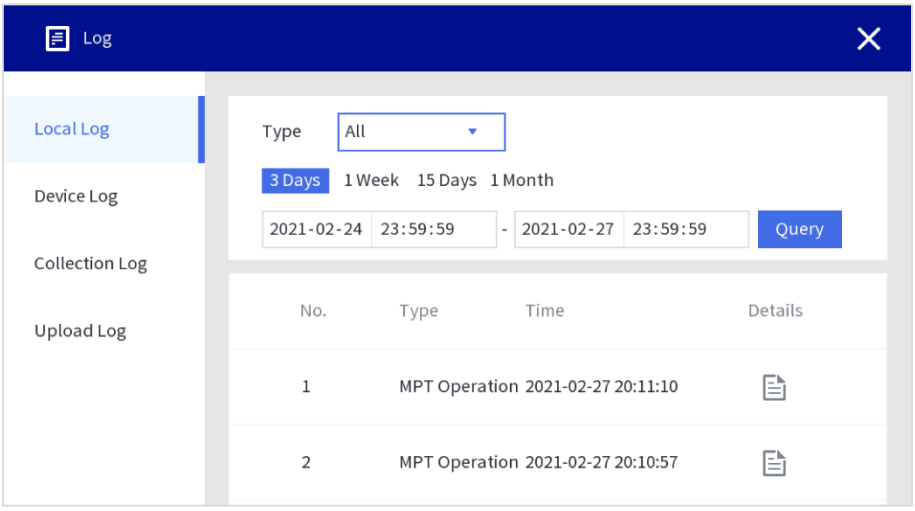
Puede ver registros locales, registros de dispositivos, registros de recopilación y registros de carga.

4.1.2.1 Registro local

Seleccione**Registro > Registro local**, seleccione el tipo de registro, ingrese la hora de inicio y la hora de finalización, y luego haga clic en**Consulta.**

El rango de tiempo máximo para la búsqueda de registros es de 1 mes.

Figura 4-3 Registro local

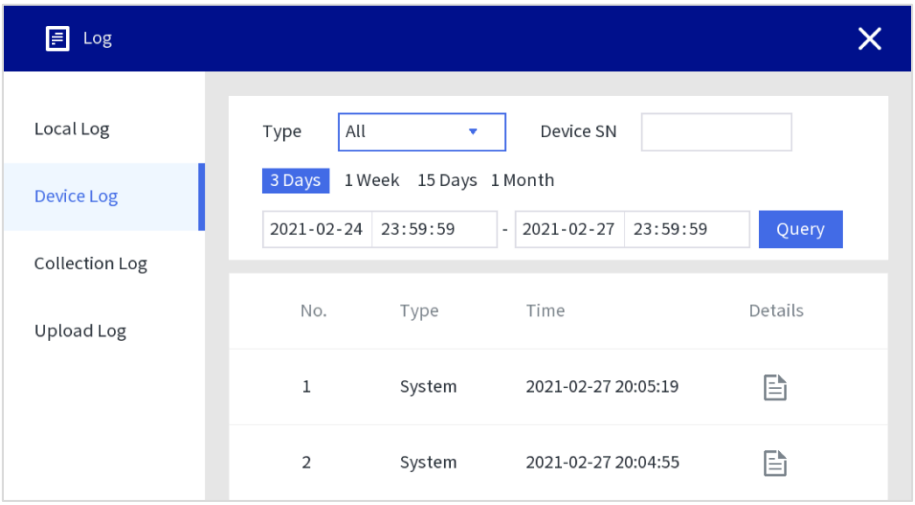


4.1.2.2 Registro del dispositivo

Seleccione**Registro > Registro del dispositivo**, seleccione el tipo de registro, ingrese el SN del dispositivo, la hora de inicio y la hora de finalización, y luego haga clic en **Consulta.**

El rango de tiempo máximo para la búsqueda de registros es de 1 mes.

Figura 4-4 Registro del dispositivo

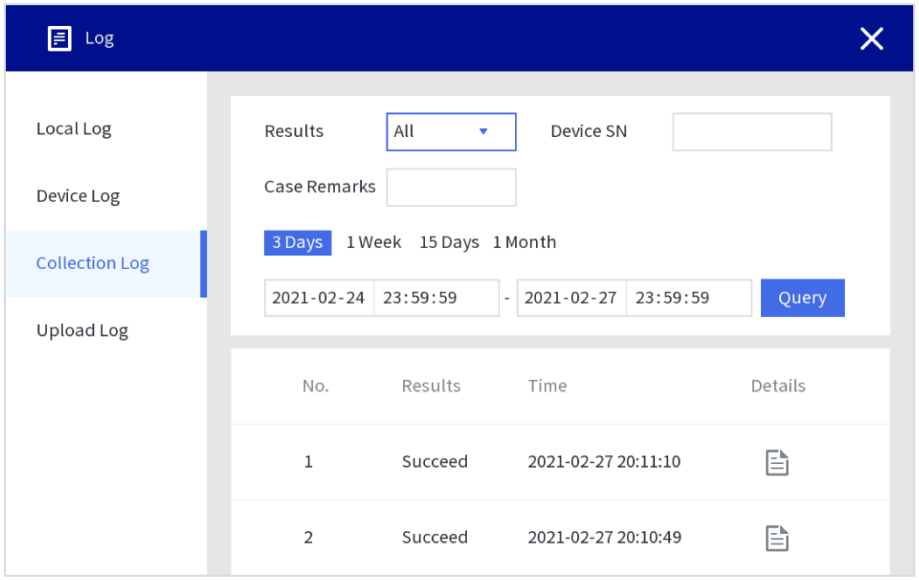


4.1.2.3 Registro de recopilación

Seleccione**Registro > Registro de recopilación**, seleccione los resultados, ingrese el SN del dispositivo, los comentarios del caso, la hora de inicio y la hora de finalización, y luego haga clic en**Consulta.**

El rango de tiempo máximo para la búsqueda de registros es de 1 mes.

Figura 4-5 Registro de recopilación

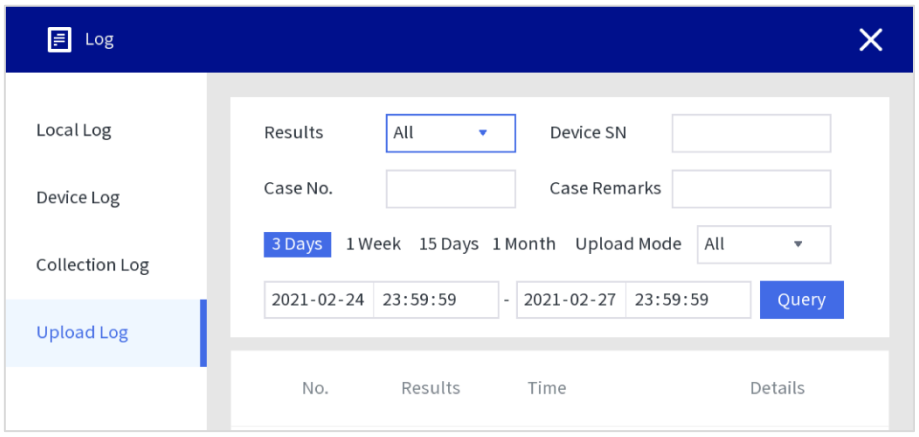


4.1.2.4 Cargar registro

Seleccione**Registro > Subir registro**, seleccione el resultado, ingrese el SN del dispositivo, el número de caso, los comentarios del caso, la hora de inicio y la hora de finalización, y luego haga clic en**Consulta.**

El rango de tiempo máximo para la búsqueda de registros es de 1 mes.

Figura 4-6 Registro de carga



4.1.3 Configuración local

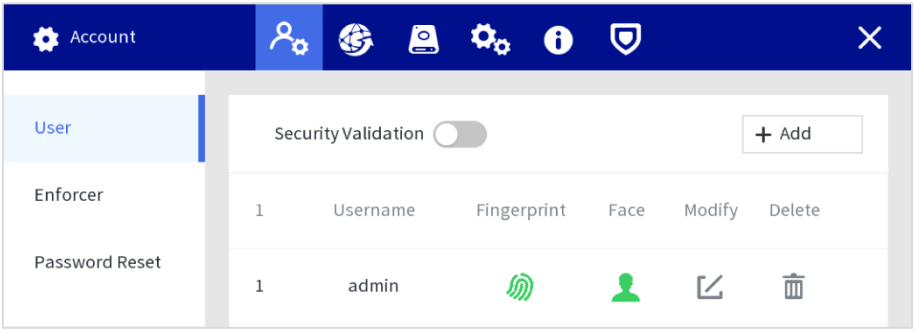
4.1.3.1 Usuario

El administrador puede agregar usuarios, eliminar usuarios y editar permisos de usuario según sea necesario.

4.1.3.1.1 Gestión de usuarios

Paso 1 Seleccione**Configuración > Cuenta > Usuario**.

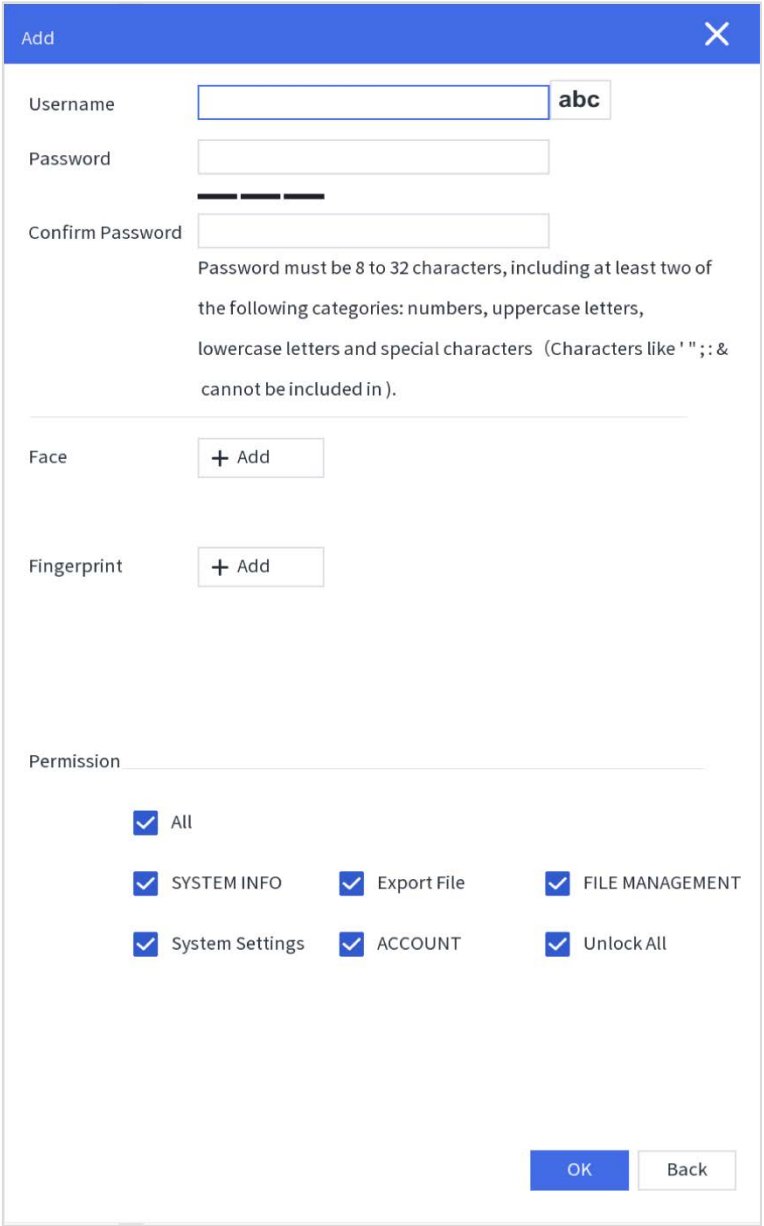
Figura 4-7 Gestión de usuarios



Paso 2 Hacer clic**Agregar**para agregar usuarios.

Puede agregar rostros y huellas dactilares, y configurar permisos de usuario. Todos los permisos están habilitados de forma predeterminada.

Figura 4-8 Agregar usuarios



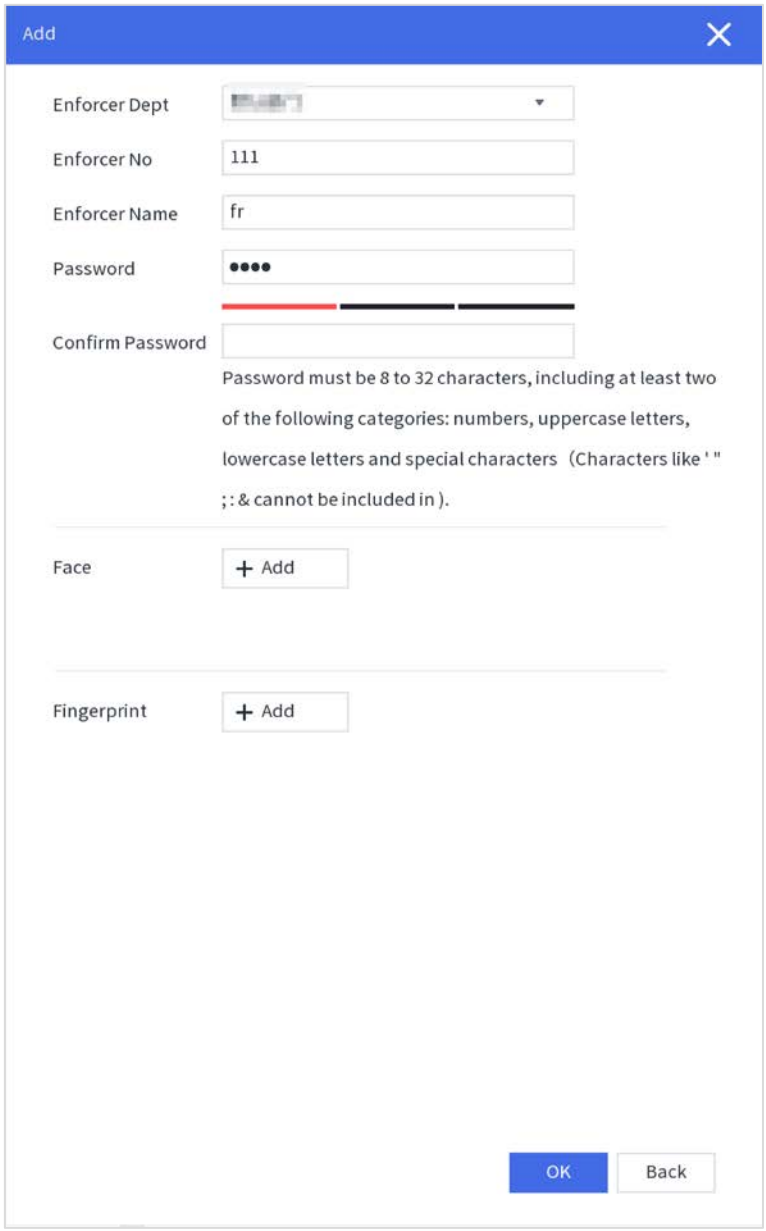
4.1.3.1.2 Gestión de ejecutores

Seleccione**Configuración > Cuenta > Enforcer**.

Agregar ejecutor

Hacer clic**Agregar**para agregar usuarios. Ingrese el departamento del ejecutor, el número del ejecutor, el nombre del ejecutor, la contraseña y confirme la contraseña, y agregue la cara y la huella digital según sea necesario.

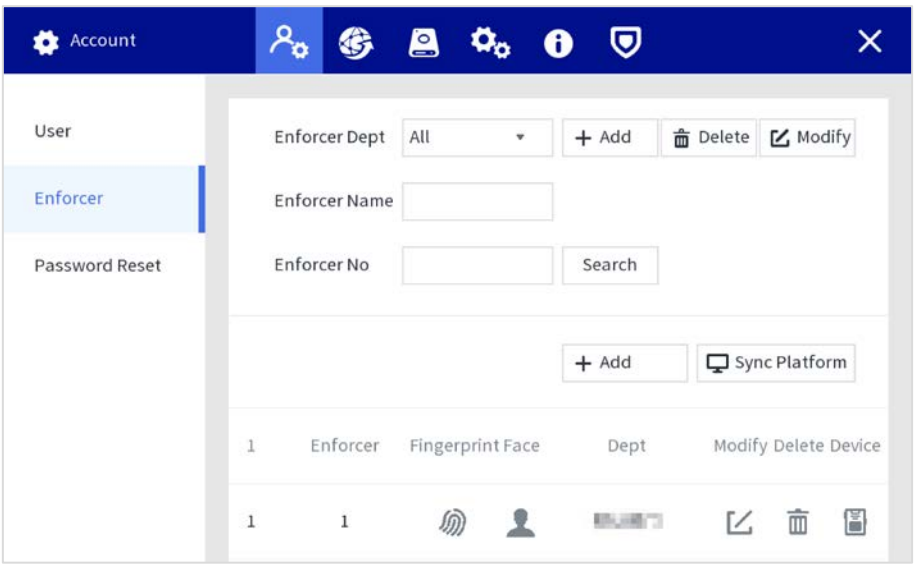
Figura 4-9 Agregar ejecutor



Buscando a Enforcer

Puede buscar al ejecutor a través del departamento del ejecutor, el nombre del ejecutor y el número del ejecutor.

Figura 4-10 Buscando ejecutor



4.1.3.1.3 Restablecimiento de contraseña

Habilite la función y podrá restablecer la contraseña haciendo clic en en la interfaz de inicio de sesión.

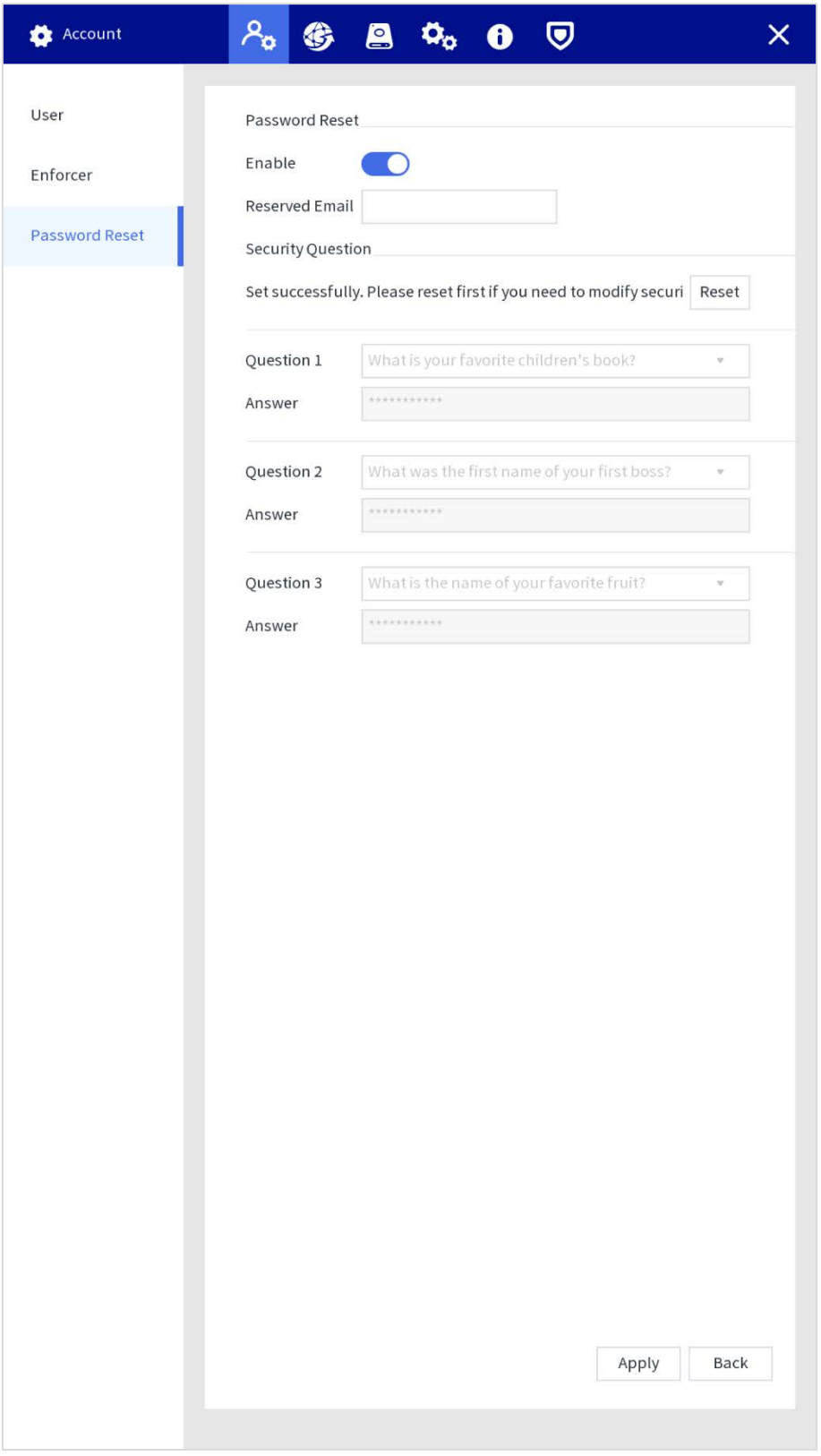
Paso 1 Seleccione**Configuración> Cuenta> Restablecimiento de contraseña**y habilite la función de restablecimiento de contraseña. Si la función no está habilitada, solo puede restablecer la contraseña reiniciando la Estación. Ingrese la

Paso 2 dirección de correo electrónico de recuperación y las preguntas de seguridad.

Si desea modificar la pregunta de seguridad después de una configuración exitosa, haga clic en**Reiniciar**primero. Hacer clic

Paso 3 **Aplicar**.

Figura 4-11 Restablecimiento de contraseña



4.1.3.2 Gestión de red

4.1.3.2.1 TCP/IP

Puede configurar la dirección IP y el servidor DNS (Sistema de nombres de dominio) y otra información de acuerdo con la planificación de la red.

Asegúrese de que al menos un puerto Ethernet se haya conectado a la red antes de configurar la dirección IP.

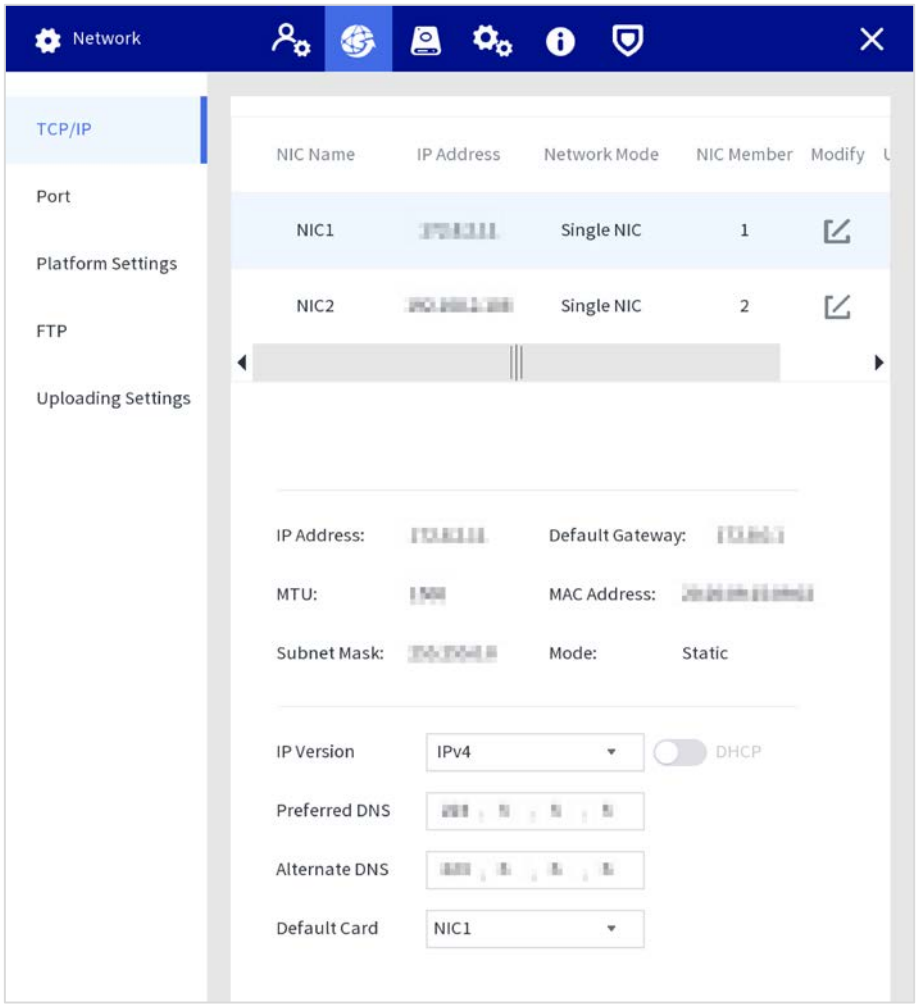
Paso 1 Seleccione**Configuración > Red > TCP/IP**.

Paso 2 Configure el parámetro de la tarjeta Ethernet.

1) Haga clic de la tarjeta Ethernet correspondiente.

2) Configure el parámetro de la tarjeta Ethernet.

Figura 4-12 Configuración de IP



Paso 3 Hacer clic**Aplicar**.

4.1.3.2.2 Puerto

Configura los números de puerto y el número máximo de usuarios (incluye web y plataforma) que puede conectarse al dispositivo simultáneamente.

Paso 1 Seleccione**Configuración > Red > Puerto**.

Paso 2 Configure el parámetro del puerto.

Figura 4-13 Configurar parámetro de puerto

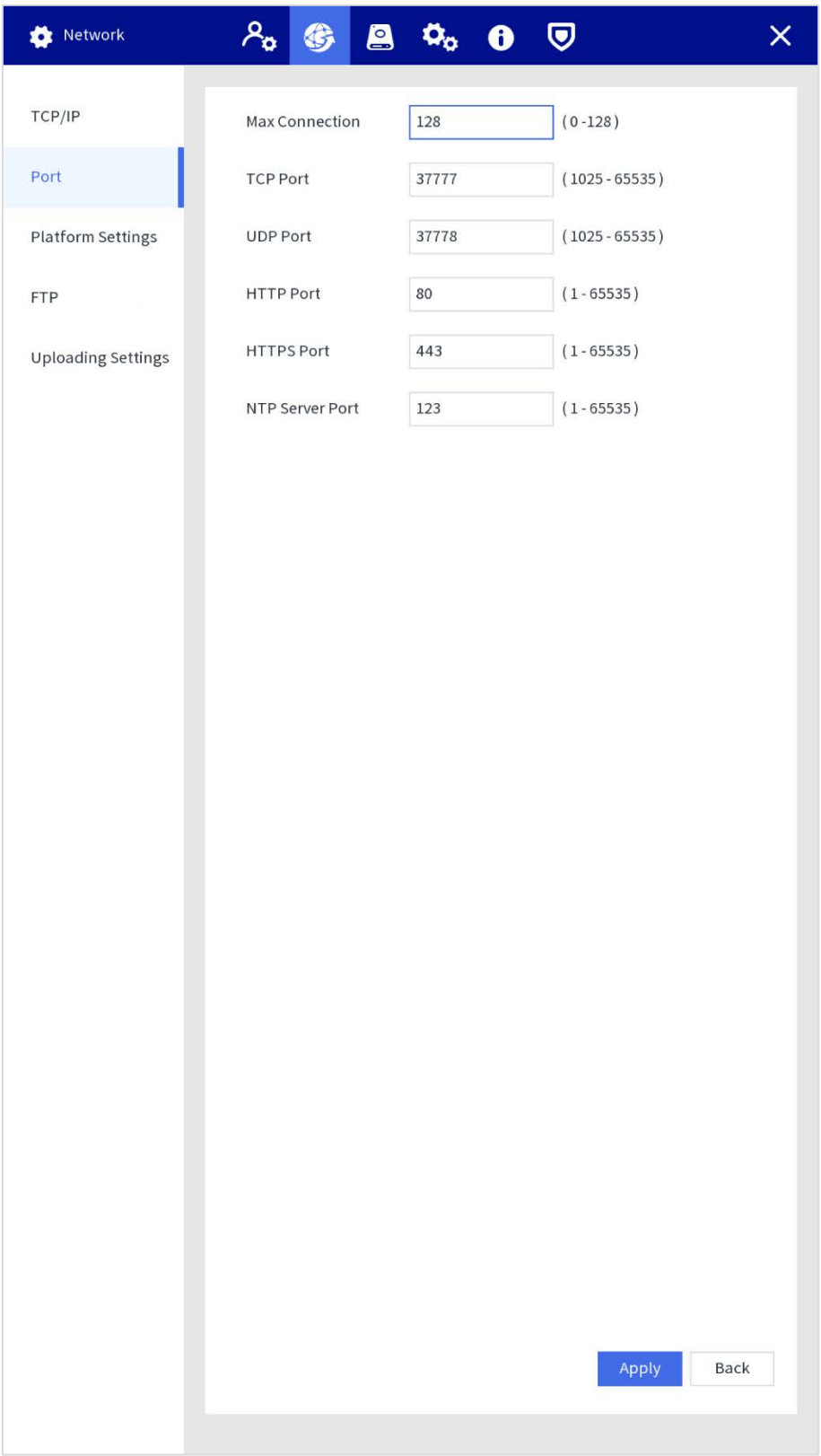


Tabla 4-2 Descripción de los parámetros del puerto

Parámetro	Descripción
Conexión máxima	Ingrese el número según sea necesario. Va de 0 a 128.
Puerto TCP	Ingrese el número según sea necesario. Es 37777 de forma predeterminada y varía de 1025 a 65535.

Parámetro	Descripción
El puerto UDP	Ingrese el número según sea necesario. Es 37778 de forma predeterminada y varía de 1025 a 65535.
Puerto HTTP	Ingrese el número según sea necesario. Es 80 por defecto y va de 1 a 65535. Si el valor que establece no es 80, agregue el número de puerto después de la dirección IP cuando utilice el navegador para iniciar sesión en el dispositivo.
Puerto HTTPS	Ingrese el número según sea necesario. Es 443 por defecto y va de 1 a 65535.
Puerto del servidor NTP	Ingrese el número según sea necesario. Es 123 por defecto y va de 1 a 65535.

Paso 3 Hacer clic**Aplicar**.

4.1.3.2.3 Configuración de la plataforma

Paso 1 Seleccione**Configuración > Red > Configuración de la plataforma**.

Paso 2 Seleccione**Ninguna**o**Centro móvil portátil**según sea necesario.

Figura 4-14 Configuración de la plataforma

Paso 3 Hacer clic**Aplicar**.

4.1.3.2.4 Configuración FTP

Configure el servidor FTP y luego podrá guardar videos, audios e instantáneas en el servidor FTP.

requisitos previos

Ha implementado un servidor FTP y ha creado un usuario con permiso de lectura y escritura.

El usuario FTP creado debe tener permiso de escritura; de lo contrario, la carga del archivo fallará.

Procedimiento

Paso 1 Seleccione**Configuración > Red > FTP**.

Paso 2 Habilite FTP, seleccione el tipo de FTP y luego configure los parámetros.

Puede seleccionar FTP o SFTP de la lista desplegable. Se recomienda SFTP para mejorar Seguridad de la red.

Figura 4-15 Configuración de FTP

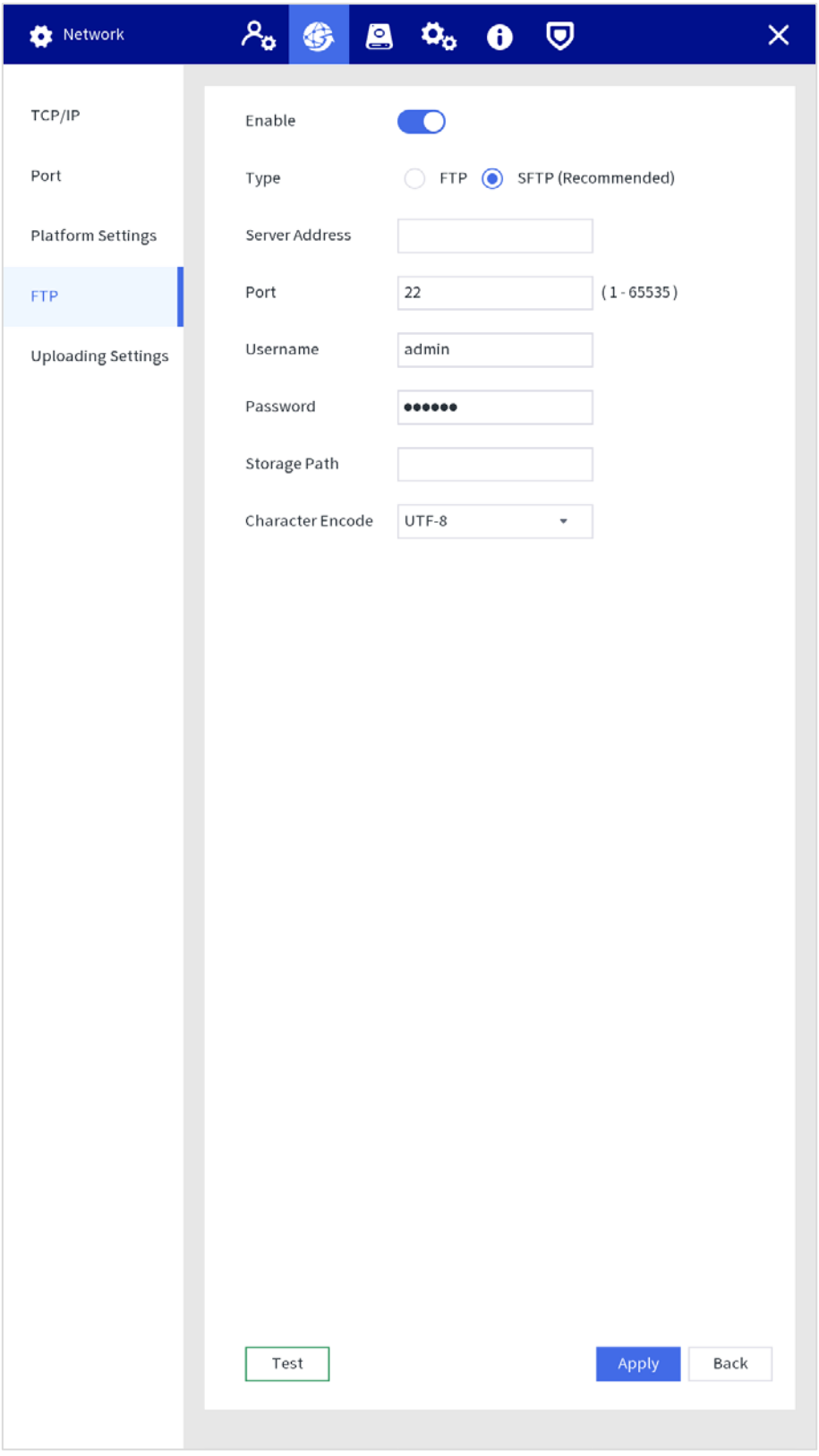


Tabla 4-3 Parámetros de FTP

Parámetro	Descripción
Dirección del servidor	La dirección IP del servidor FTP.
Puerto	El número de puerto del servidor FTP. El puerto predeterminado es 22 para SFTP y el puerto predeterminado es 21 para FTP

Parámetro	Descripción
Nombre de usuario Clave	El nombre de usuario y la contraseña para iniciar sesión en el servidor FTP.
Ruta de almacenamiento	La ruta de destino en el servidor FTP.  Crear carpeta en servidor FTP. - Si no ingresa el nombre del directorio remoto, el sistema crea automáticamente las carpetas de acuerdo con la IP y la hora. - Si ingresa el nombre del directorio remoto, el sistema crea primero la carpeta con el nombre ingresado en el directorio raíz de FTP y luego crea automáticamente las carpetas de acuerdo con la IP y la hora.
Codificación de caracteres	Admite UTF-8 y GB2312.  Cuando se muestran códigos desordenados en el servidor, cambie la codificación de caracteres.

Paso 3 Hacer clic**Aplicar**.

4.1.3.3 Gestión de almacenamiento

Puede administrar los recursos de almacenamiento (como el archivo de registro) y el espacio de almacenamiento. Para que sea fácil de usar y mejorar el uso del espacio de almacenamiento.

4.1.3.3.1 Básico

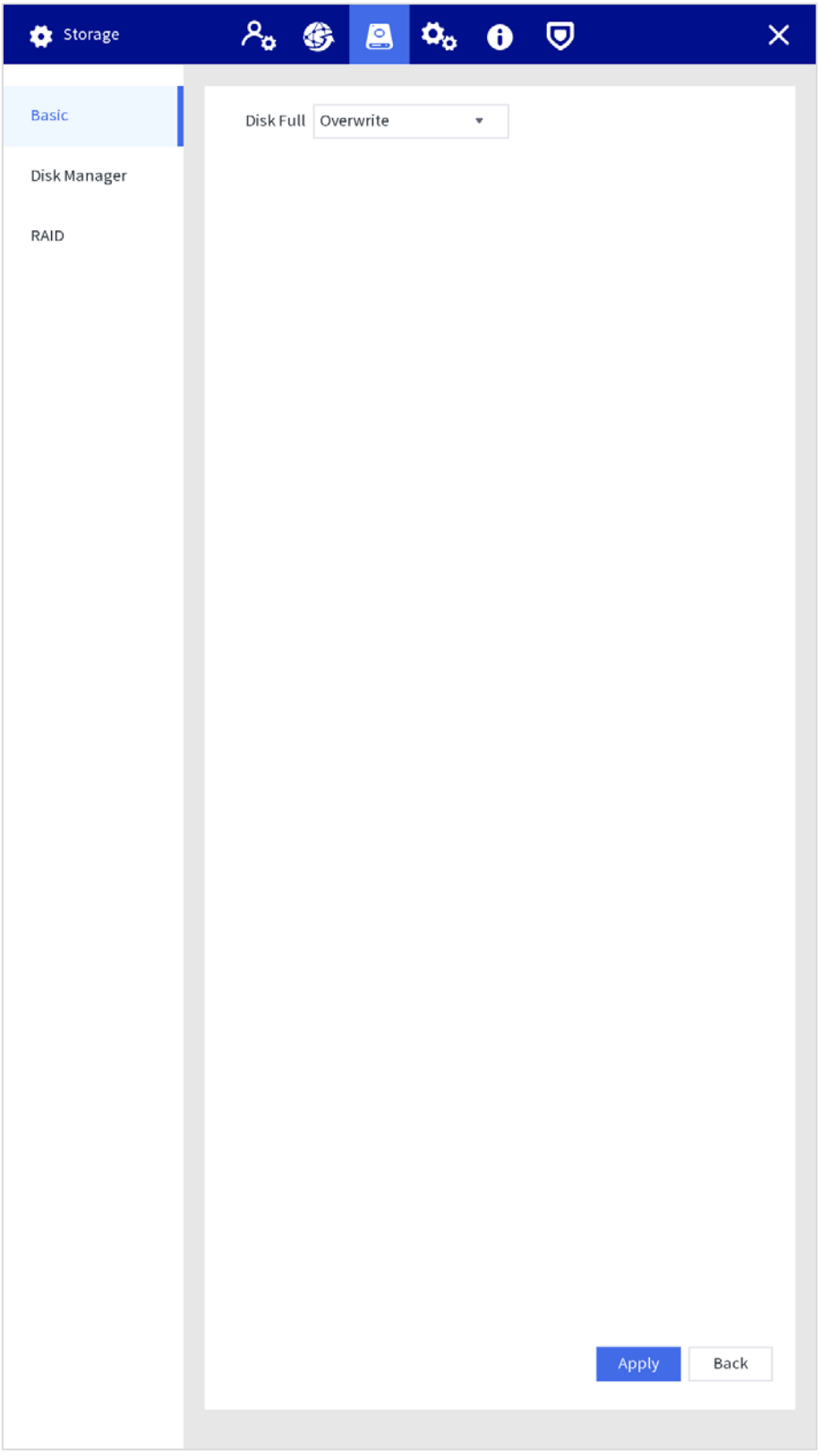
Paso 1 Seleccione**Configuración > Almacenamiento >**

Paso 2 **Básico**. Configurar parámetros.

Disco lleno: configure los ajustes para la situación en la que todos los discos de lectura/escritura estén llenos y no haya más discos libres.

- Seleccione**Detener registro**para detener la grabación.
- Seleccione**Sobrescribir**para sobrescribir los archivos de video grabados siempre desde la primera vez.

Figura 4-16 Configuración básica



Paso 3 Hacer clic**Aplicar**.

4.1.3.3.2 Administrador de discos

Puede ver la información del disco, formatear el disco y configurar el tipo de disco de acuerdo con la situación real. Paso 1 Seleccione **Configuración> Almacenamiento> Administrador de discos**.

Paso 2 Hacer clic  para ver los detalles.

Paso 3 (Opcional) Formatee un HDD.

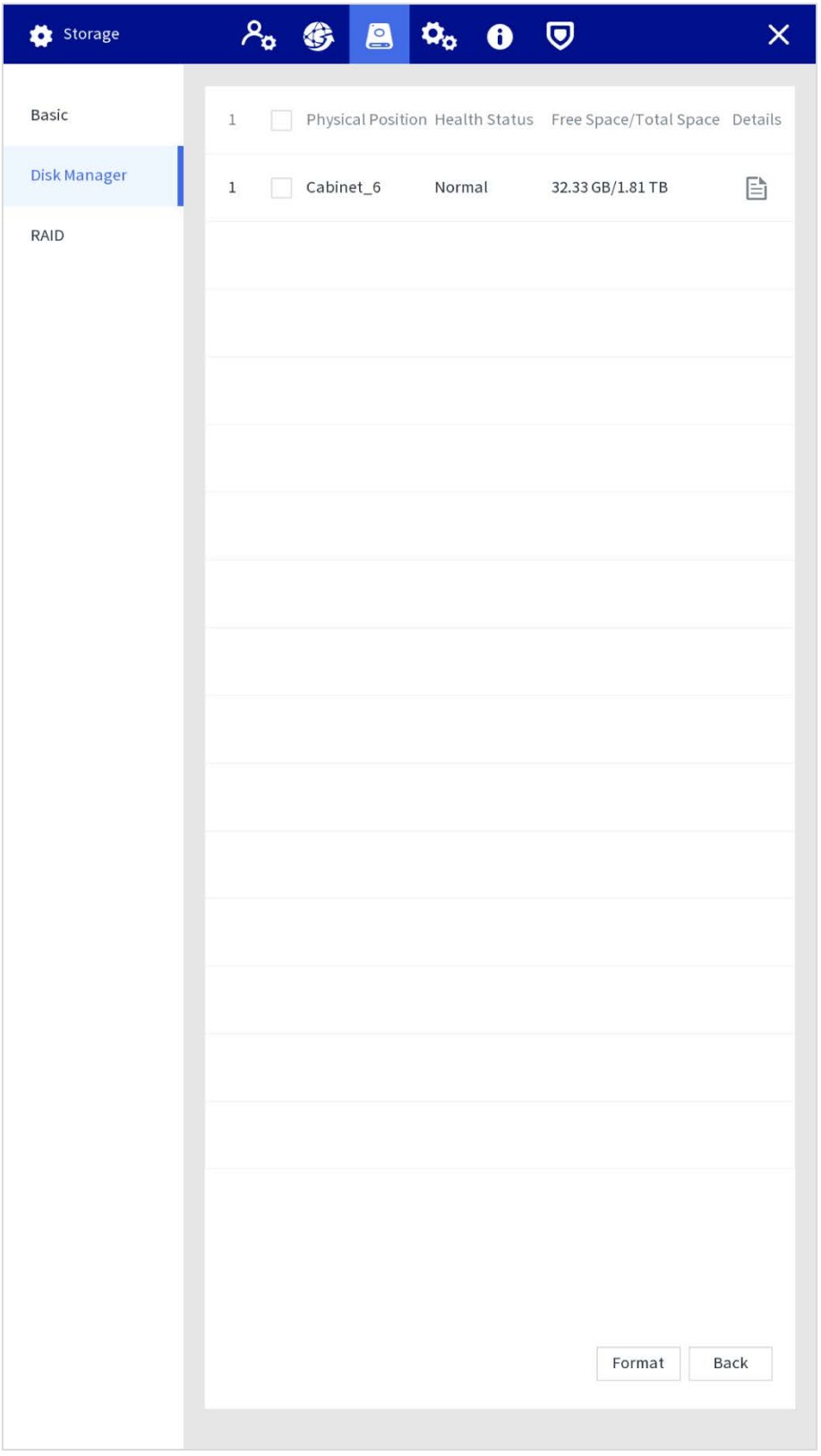
1) Seleccione un HDD y luego haga clic en**Formato**.

2) Haga clic**DE ACUERDO**.

3) Introduzca la contraseña de administrador y haga clic en**DE ACUERDO**. Se eliminan todos los datos del HDD.

Esta operación eliminará todos los datos del HDD, proceda con precaución.

Figura 4-17 Administrador de discos



4.1.3.3.3 RAID

RAID (matriz redundante de discos independientes) es una tecnología de virtualización de almacenamiento de datos que combina varios componentes físicos de HDD en una sola unidad lógica con el fin de redundancia de datos, mejora del rendimiento o ambos.

- La estación es compatible con RAID0, RAID1, RAID5, RAID10. Para más detalles, consulte el "Apéndice 1 Raid Introducción." Esta sección toma RAID 5 como ejemplo.
- Recomendamos implementar el disco RAID al comienzo de la configuración de RAID. Crear o eliminar RAID afectará los datos del dispositivo.

Configuración de RAID

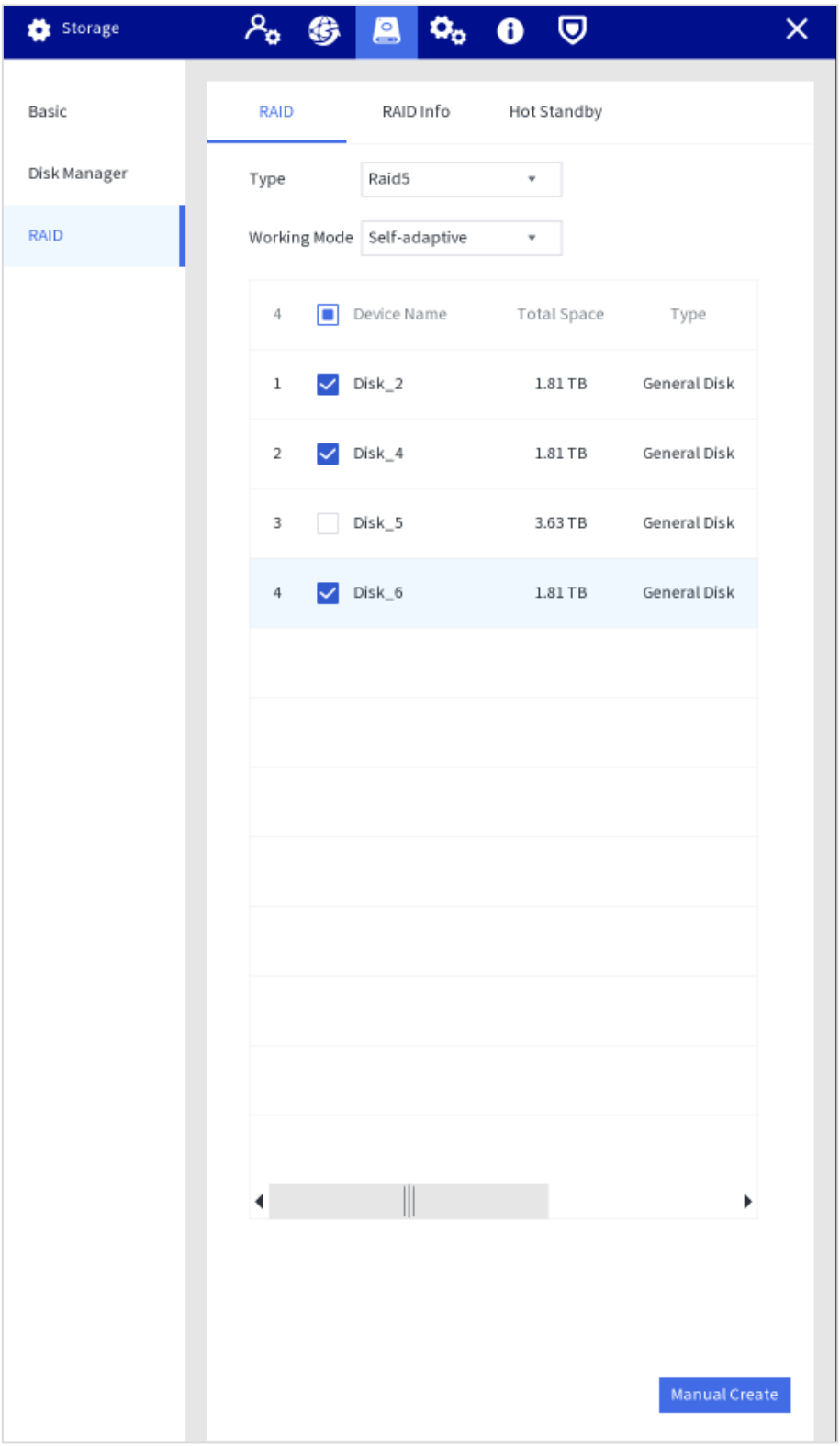
Paso 1 Seleccione**Configuración> Almacenamiento> RAID> RAID**.

Paso 2 Seleccione el tipo de RAID y el modo de trabajo.

Cuando selecciona RAID 5 en**Tipo**, puede configurar el modo de trabajo.

- Autoadaptable: el sistema puede ajustar automáticamente la velocidad de sincronización de RAID de acuerdo con la carga comercial actual. Cuando no hay ningún negocio externo en ejecución, la sincronización se realiza a alta velocidad. Cuando hay negocios externos en ejecución, la sincronización se realiza a baja velocidad.
- Sincronizar primero: los recursos se asignan primero a la sincronización de RAID.
- El negocio primero: los recursos se asignan primero al negocio.
- Equilibrio de carga: los recursos se asignan a la sincronización comercial y RAID por igual.

Figura 4-18 RAID



Paso 3 Seleccione el disco en el que desea crear RAID. Hacer clic

Paso 4 **Creación manual**. Hacer clic**Confirmar**.

Paso 5

Después de la autenticación, el RAID se crea correctamente y se muestra la información del nuevo RAID.

Figura 4-19 Crear RAID con éxito

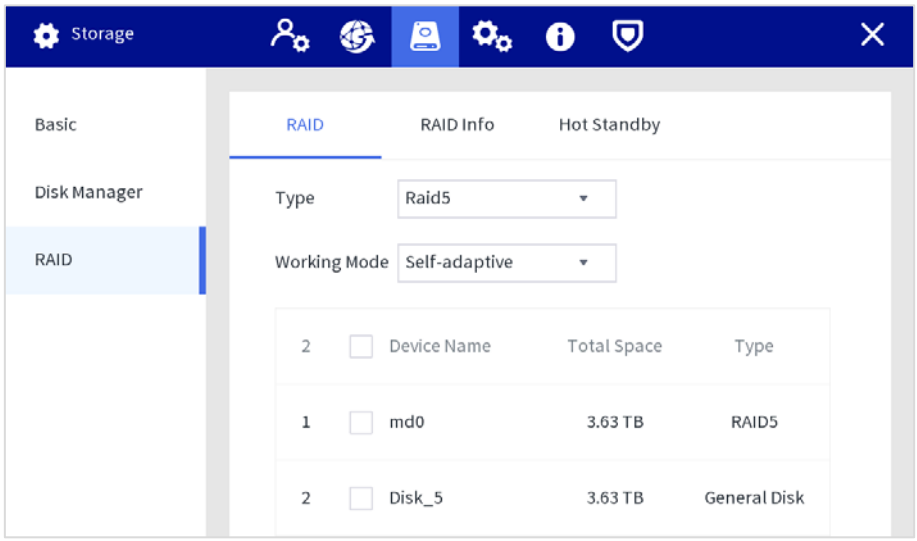


Figura 4-20 Visualización en el administrador de discos Se crea RAID (1)

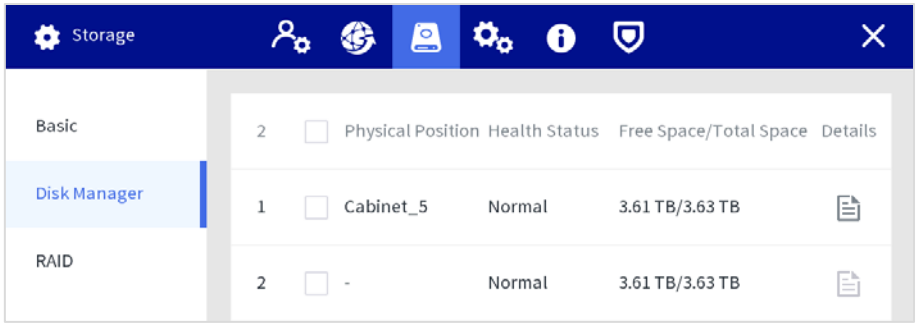
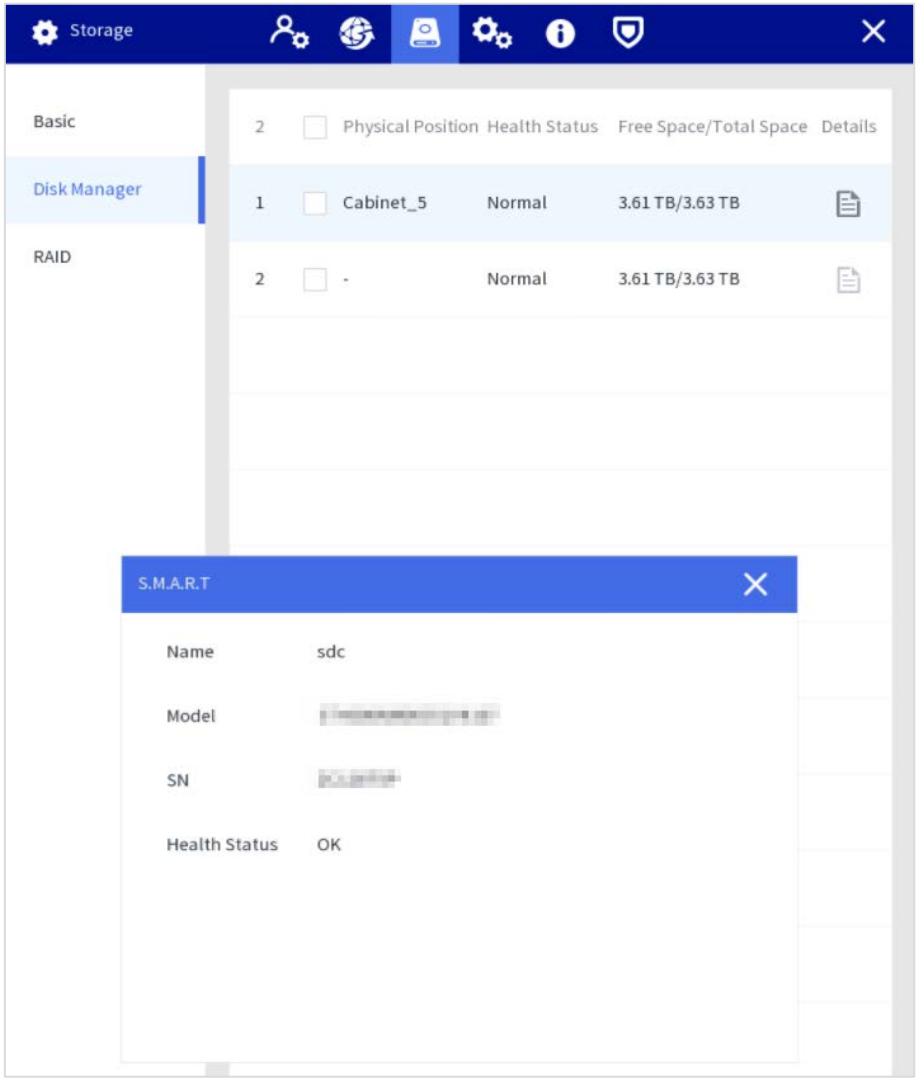


Figura 4-21 Visualización en el administrador de discos Se crea RAID (2)



Información RAID

Puede ver la información de RAID, incluido el nombre del dispositivo, el espacio total y el tipo.

Seleccione**Configuración > Almacenamiento > RAID > Información de RAID**y luego haga clic en RAID para ver los detalles.

Figura 4-22 Información de RAID

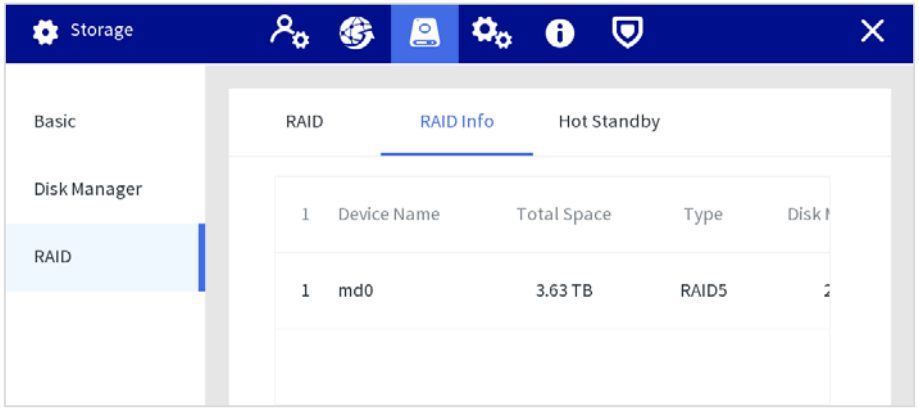
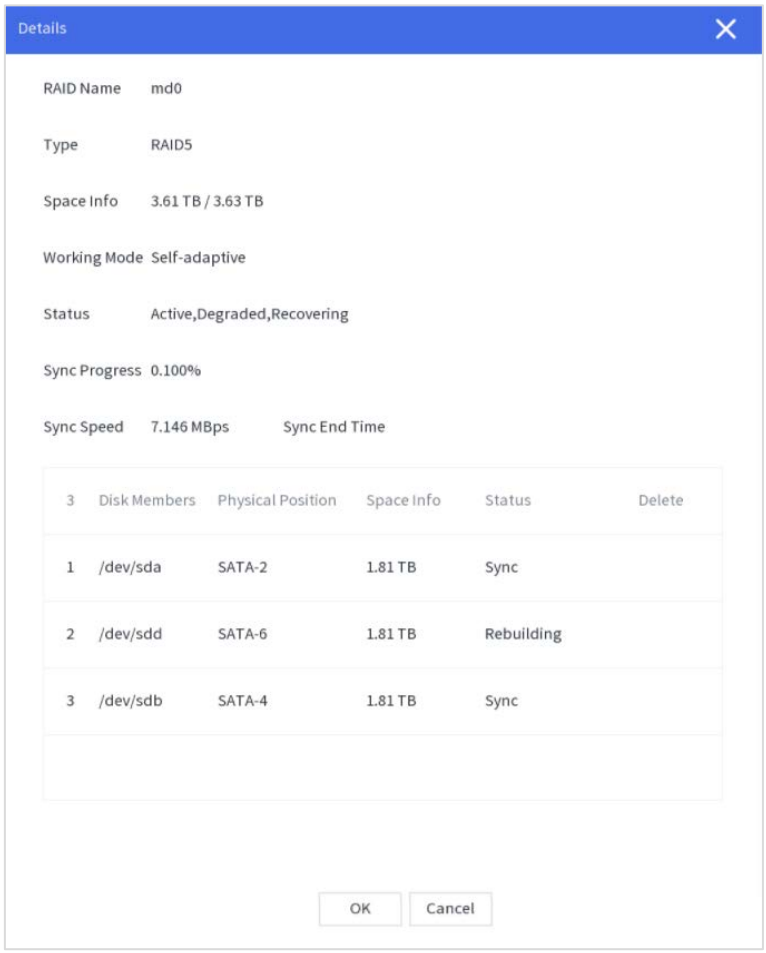


Figura 4-23 Detalles



Espera activa

Cuando una unidad de disco duro del grupo RAID tiene un problema, la unidad de disco duro de repuesto dinámico puede reemplazar la unidad de disco duro que no funciona correctamente. No hay riesgo de pérdida de datos y puede garantizar la confiabilidad del sistema de almacenamiento.

Paso 1 Seleccione**Configuración> Almacenamiento> RAID> Hot Standby**.

Paso 2 Seleccione el tipo de dispositivo y el grupo RAID que necesita agregar HDD de repuesto dinámico.

- Repuesto dinámico privado: seleccione un grupo RAID para agregar, y luego el disco duro se agregará al grupo RAID correspondiente y se utilizará como un disco duro de repuesto dinámico para el RAID.
- Hot standby global: es un HDD de repuesto dinámico para todos los grupos RAID en lugar de un grupo RAID específico.

Figura 4-24 Repuesto dinámico privado

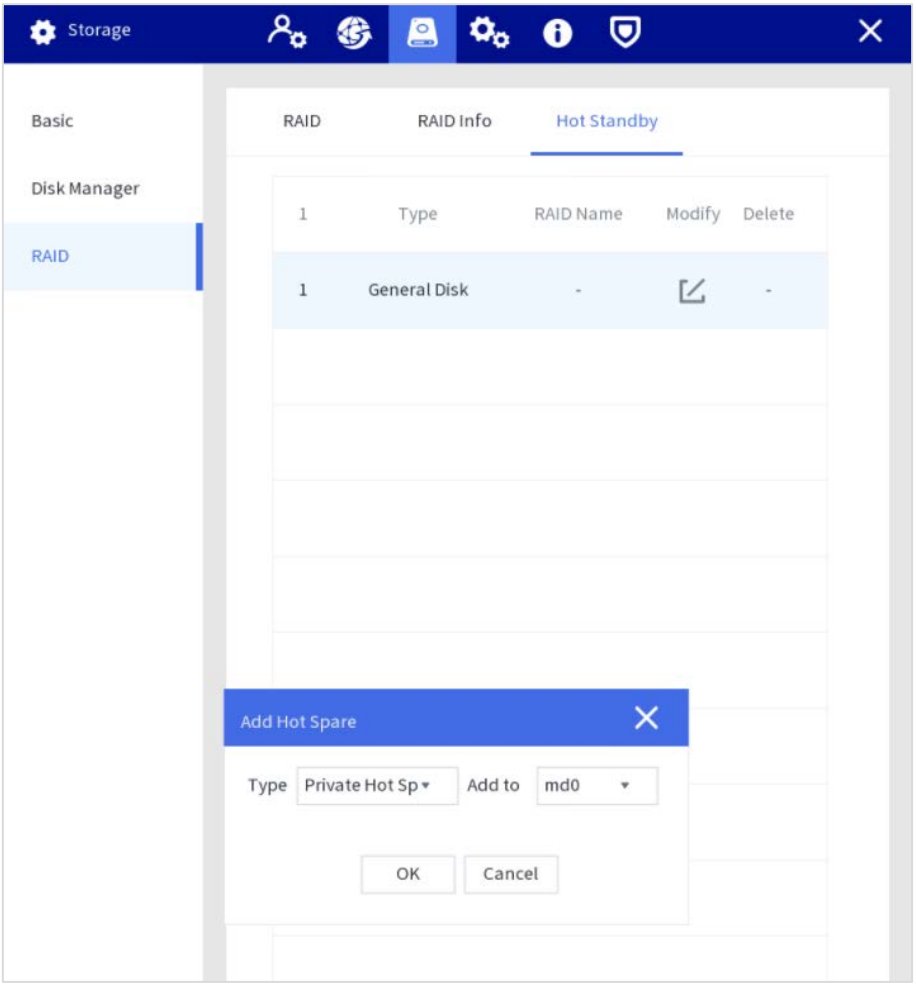
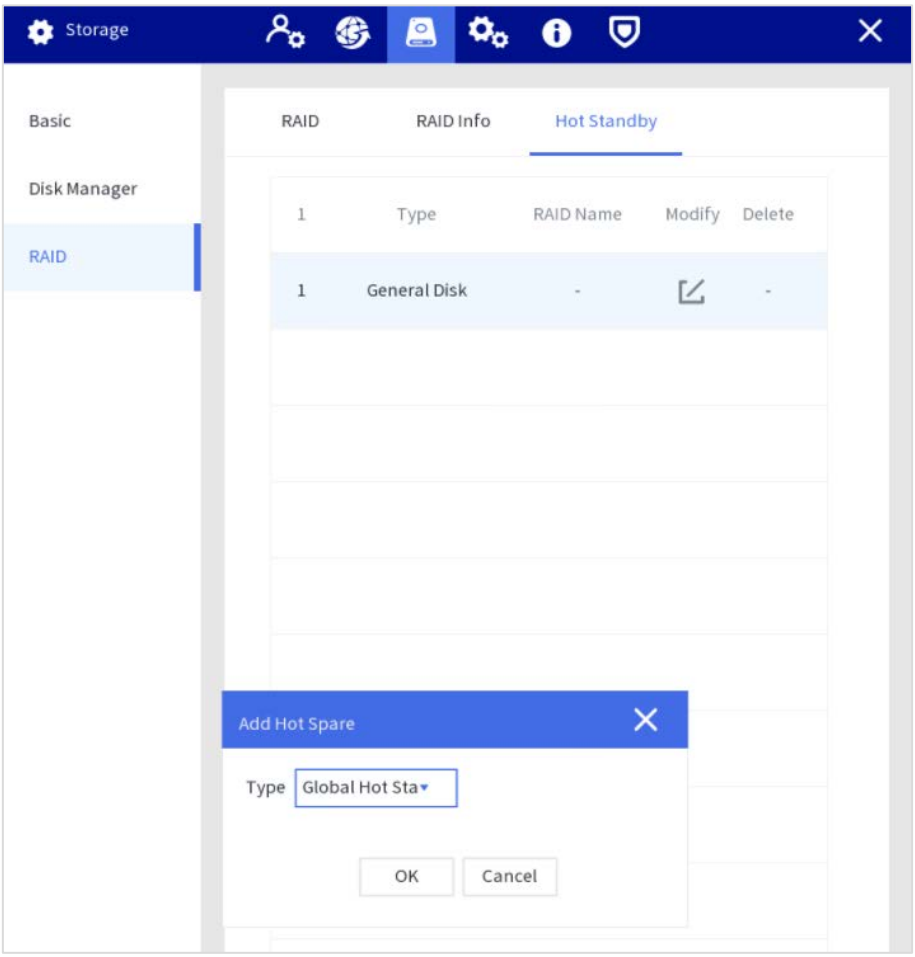


Figura 4-25 Espera activa global



Paso 3 Hacer clic**DE ACUERDO**.

Después de la autenticación, el modo de espera activo se crea correctamente.

Figura 4-26 Hot standby global

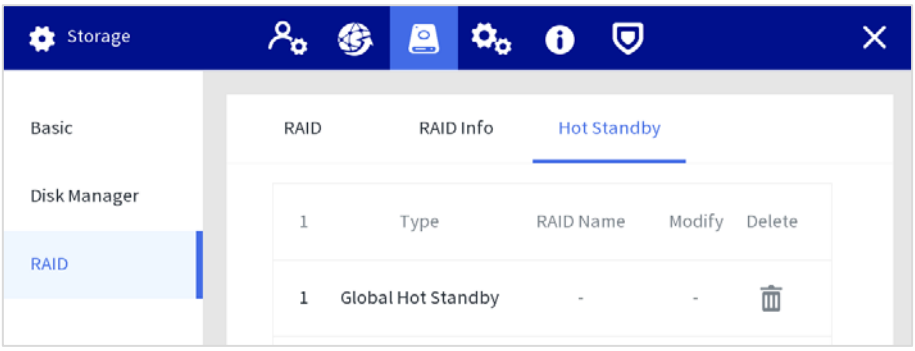
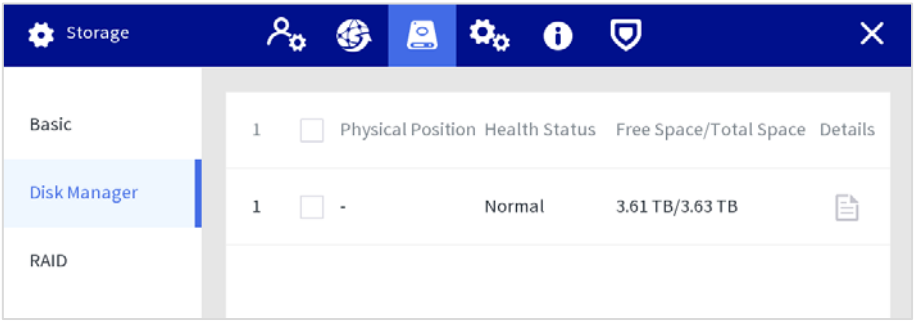


Figura 4-27 Visualización en el administrador de discos después de crear el modo de espera en caliente



4.1.3.4 Gestión del sistema

4.1.3.4.1 Configuración básica

Puede configurar el tiempo de apagado de la pantalla, el tiempo de cierre de sesión, el estándar de video y decidir si activar la alarma cuando se produce una desconexión de la red.

Figura 4-28 Configuración básica

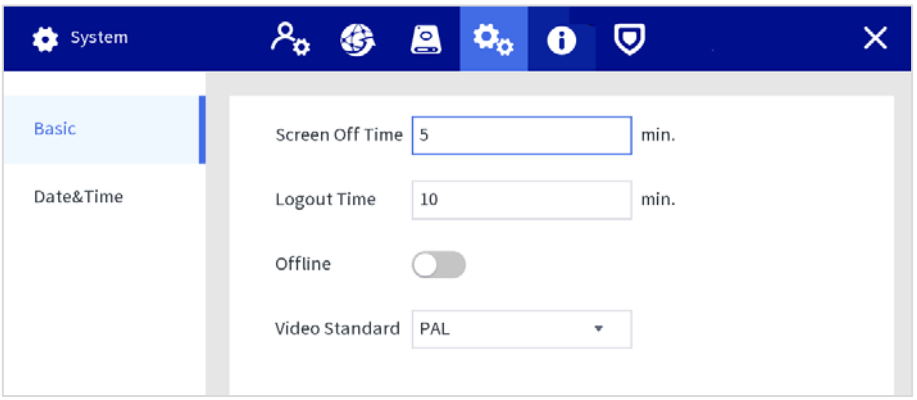


Tabla 4-4 Parámetros de fecha y hora

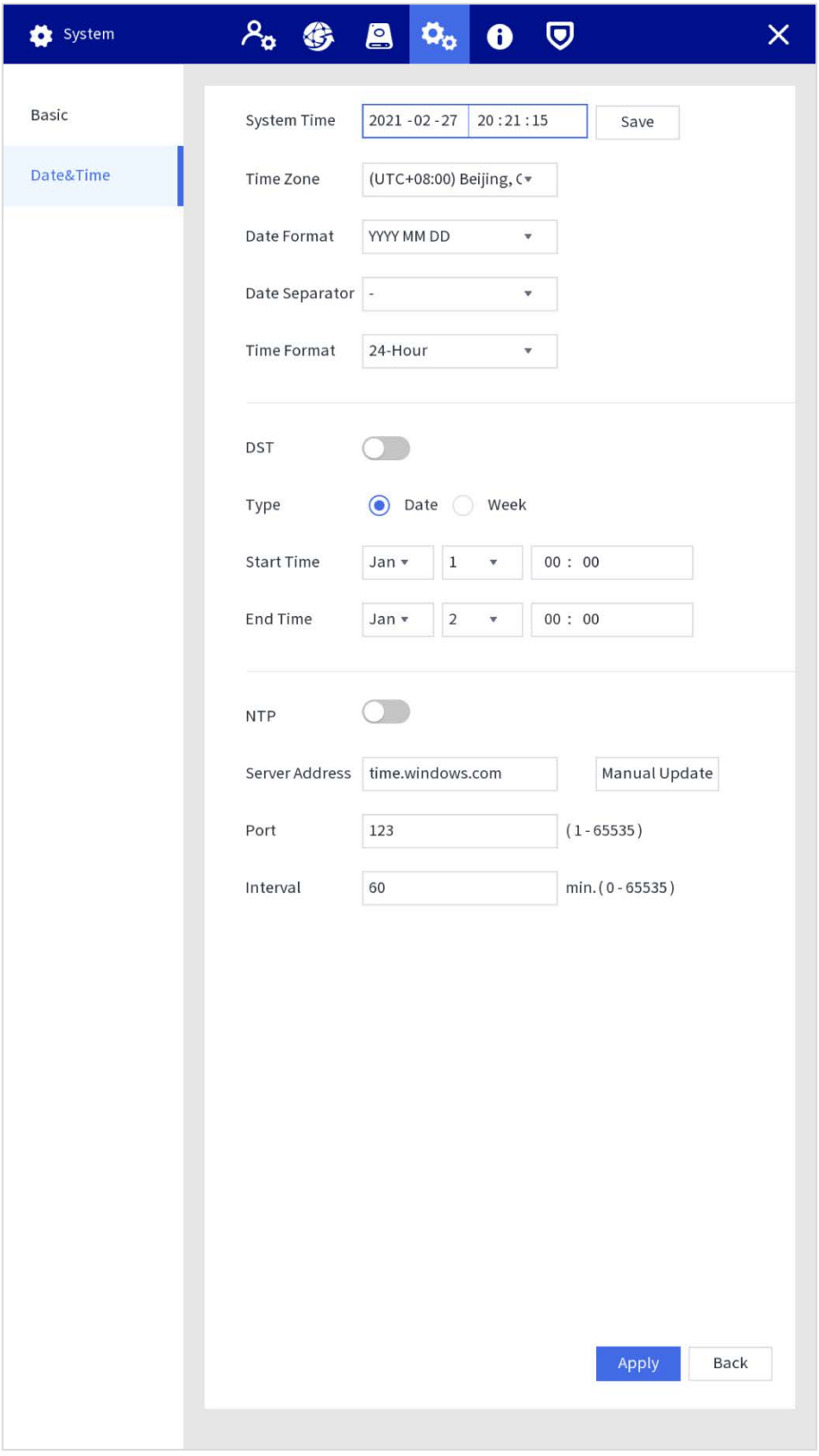
Parámetro	Descripción
Tiempo de apagado de pantalla	Configure el tiempo de apagado de la pantalla. Cuando no opere la Estación dentro del tiempo definido, la pantalla se apagará. Va de 0 a 60 minutos, y 0 significa que la pantalla siempre estará encendida. Para prolongar la vida útil de la pantalla LCD, le recomendamos que no establezca el tiempo en 0 minutos.
Hora de cierre de sesión	Establezca el intervalo de cierre de sesión automático. Cuando no opere la estación dentro del tiempo establecido, la estación se cerrará automáticamente. Después del cierre de sesión automático, debe iniciar sesión nuevamente para operar. Va de 0 a 60 minutos, y 0 significa que la estación no se desconectará. Para garantizar la seguridad de la cuenta de la Estación, le recomendamos que no establezca el tiempo en 0 minutos.
Desconectado	Cuando**Desconectado**está habilitado, se activará una alarma cuando se produzca una desconexión de la red en cualquier puerto Ethernet.
Estándar de vídeo	Seleccione el estándar de video de**CAMARADA**y**NTSC**. Reinicie la estación después de cambiar el estándar de video para que la configuración surta efecto.

4.1.3.4.2 Fecha y hora

Paso 1 Seleccione**Configuración> Sistema> Fecha y hora**.

En la misma red, si la hora de la cámara del cuerpo no coincide con la de la estación, no podrá ver ni reproducir videos. Puede configurar la hora manualmente o a través de NTP.

Figura 4-29 Fecha y hora



- Configurar la hora manualmente

  Establezca la hora, el formato y la zona horaria del sistema de acuerdo con la situación real.

Tabla 4-5 Parámetros de fecha y hora

Parámetro	Descripción
Hora del sistema	Configure la fecha y la hora del sistema del dispositivo. Hacer clic**Sincronizar PC**para sincronizar la hora con la PC desde donde inicia sesión en la interfaz web.
Zona horaria	Zona horaria del área actual.
Formato de fecha	Seleccione un formato de fecha de**AAA MM DD**,**MM DD AAAA**, y**DD MM AAAA**.
Separador de fecha	Seleccione un separador entre año, mes y fecha.
Formato de tiempo	Seleccione un formato de hora de**24 horas**y**12 horas**.
horario de verano	Cuando habilite el horario de verano, configure el tipo de horario de verano, la hora de inicio y la hora de finalización. DST es un sistema para estipular la hora local, con el fin de ahorrar energía. El horario de verano se aplica en algunos países o regiones. Habilite o deshabilite DST según sea necesario.

- Habilitar NTP

  Habilite NTP e ingrese la dirección del servidor, el puerto y el intervalo. Después de la configuración, el sistema ajusta la hora del dispositivo de acuerdo con la hora del servidor NTP.

  Intervalo se refiere al intervalo de tiempo en el que el dispositivo sincroniza la hora con el servidor NTP.

Paso 2 Hacer clic**Aplicar**.

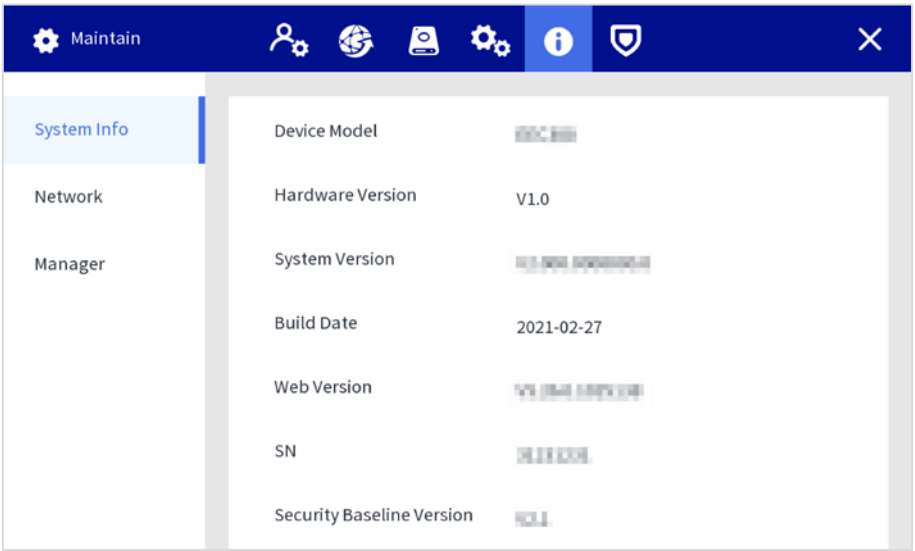
4.1.3.5 Gestión de Operación y Mantenimiento

4.1.3.5.1 Información del sistema

Puede ver el modelo del dispositivo, la versión de hardware, la versión del sistema y la versión web.

Seleccione**Configuración> Mantener> Información del sistema**.

Figura 4-30 Información del sistema



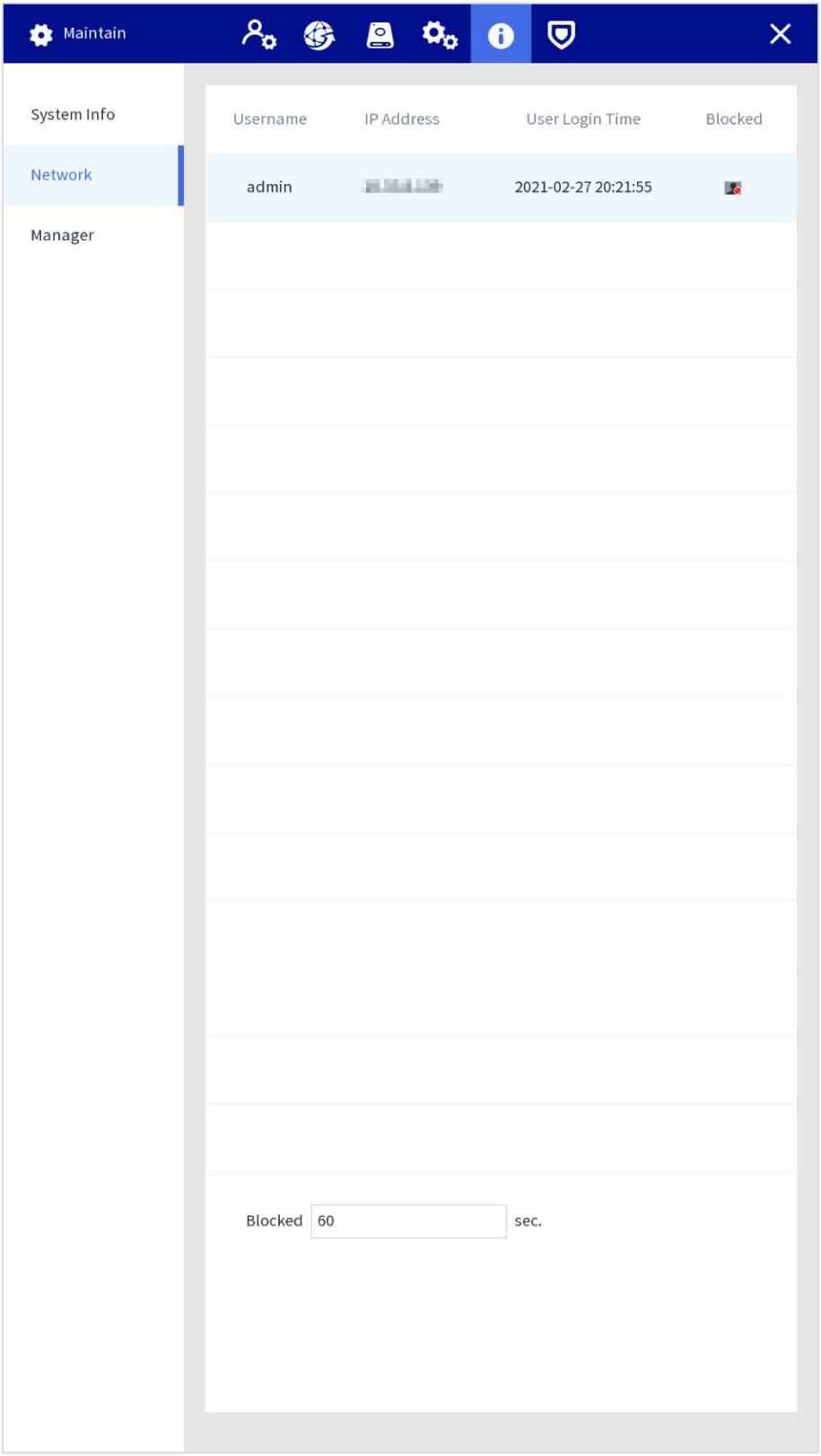
4.1.3.5.2 Red

Puede ver la información del usuario que está accediendo al dispositivo y la lista de usuarios se actualiza en tiempo real.

Seleccione**Configuración > Mantener > Red**.

Hacer clic  para bloquear a un determinado usuario por un período, y el tiempo de bloqueo se puede configurar hasta 65,535 segundos.

Figura 4-31 Información de red

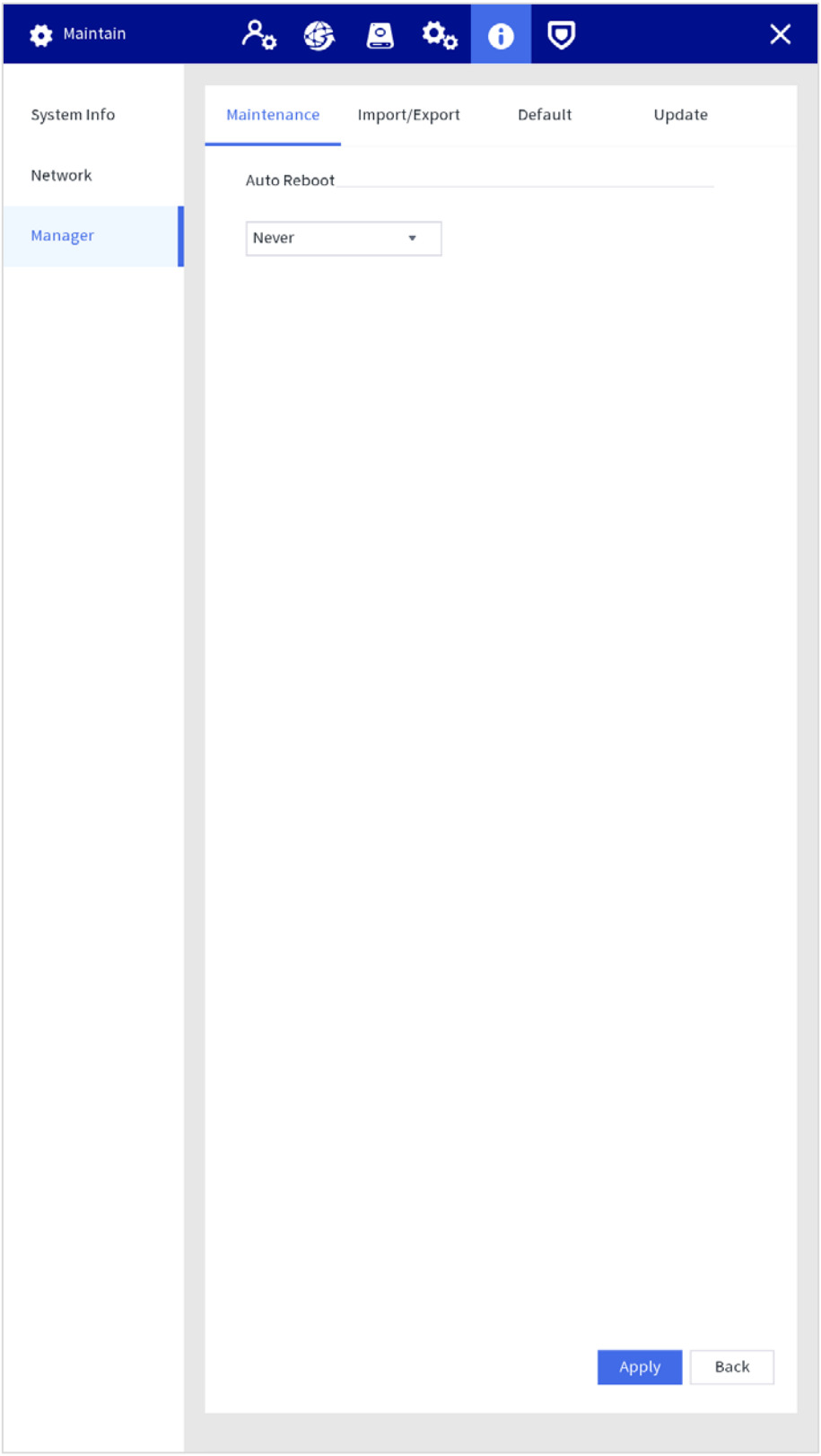


4.1.3.5.3 Mantener

Mantenimiento del dispositivo

Paso 1 Seleccione**Configuración > Mantener > Administrador > Mantenimiento**y, a continuación, establezca la fecha de mantenimiento.

Figura 4-32 Mantenimiento del dispositivo



Paso 2 Hacer clic**Aplicar**.

Importación y exportación

Exporte los datos del dispositivo y la información del usuario para la copia de seguridad. Cuando hay una excepción de dispositivo, puede importar los datos exportados para recuperar los datos.

Paso 1 Seleccione**Configuración > Mantener > Administrador > Importar/Exportar**.

Paso 2 Seleccione**Exportar**desde el**Tipo de operación**lista, seleccione el tipo de archivo y la ruta de almacenamiento según sea necesario, y luego ingrese la contraseña.

Paso 3 Hacer clic**Comienzo**.

Paso 4 (Opcional) Cuando haya una excepción de dispositivo, seleccione**Importar**desde el**Tipo de operación**lista, seleccione el tipo de archivo y la ruta de almacenamiento del archivo de configuración que se va a importar y, a continuación, introduzca la contraseña.

Paso 5 Hacer clic**Comienzo**.

Importe el archivo de configuración y luego reinicie la estación.

Figura 4-33 Configuración de exportación

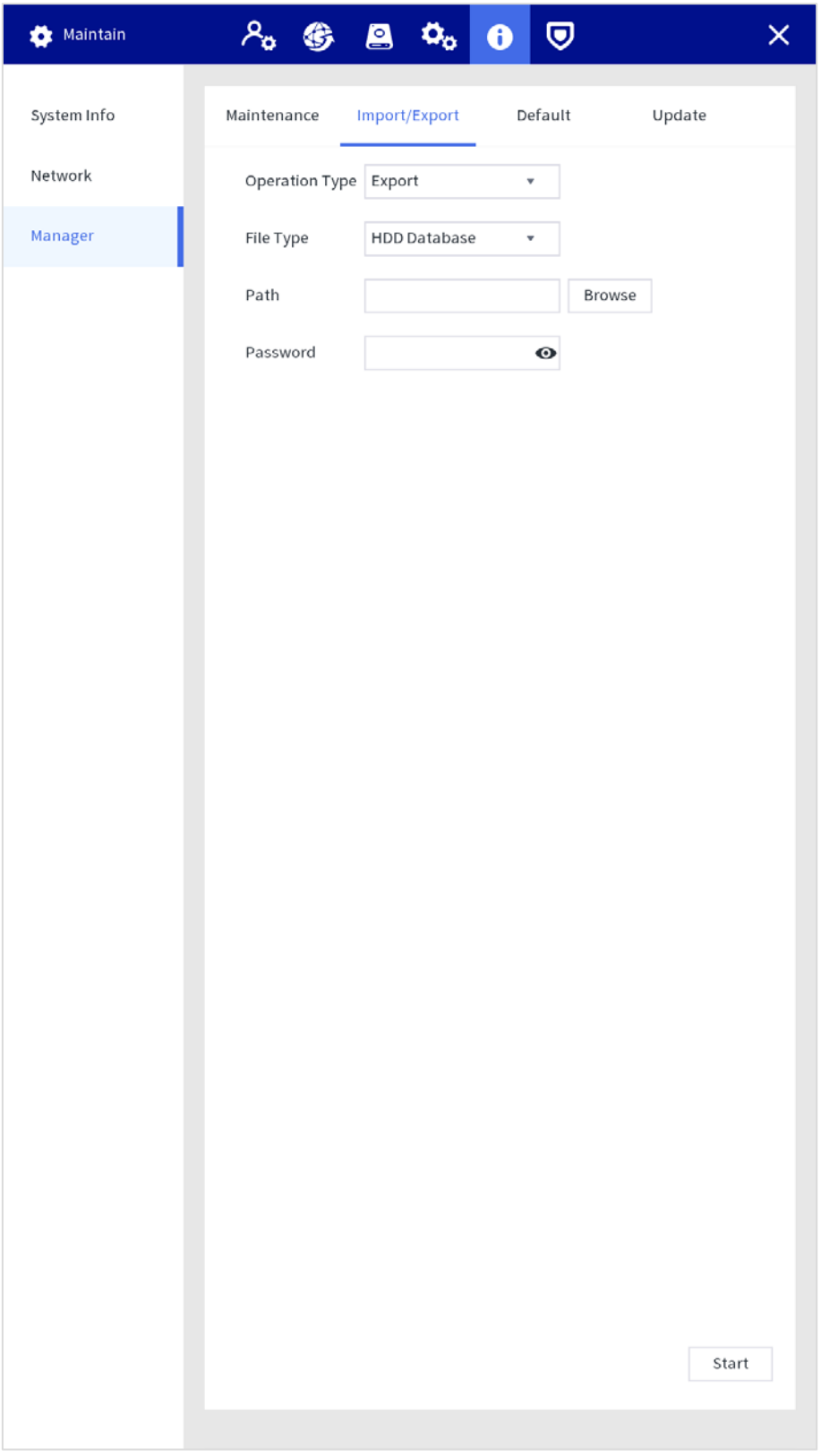
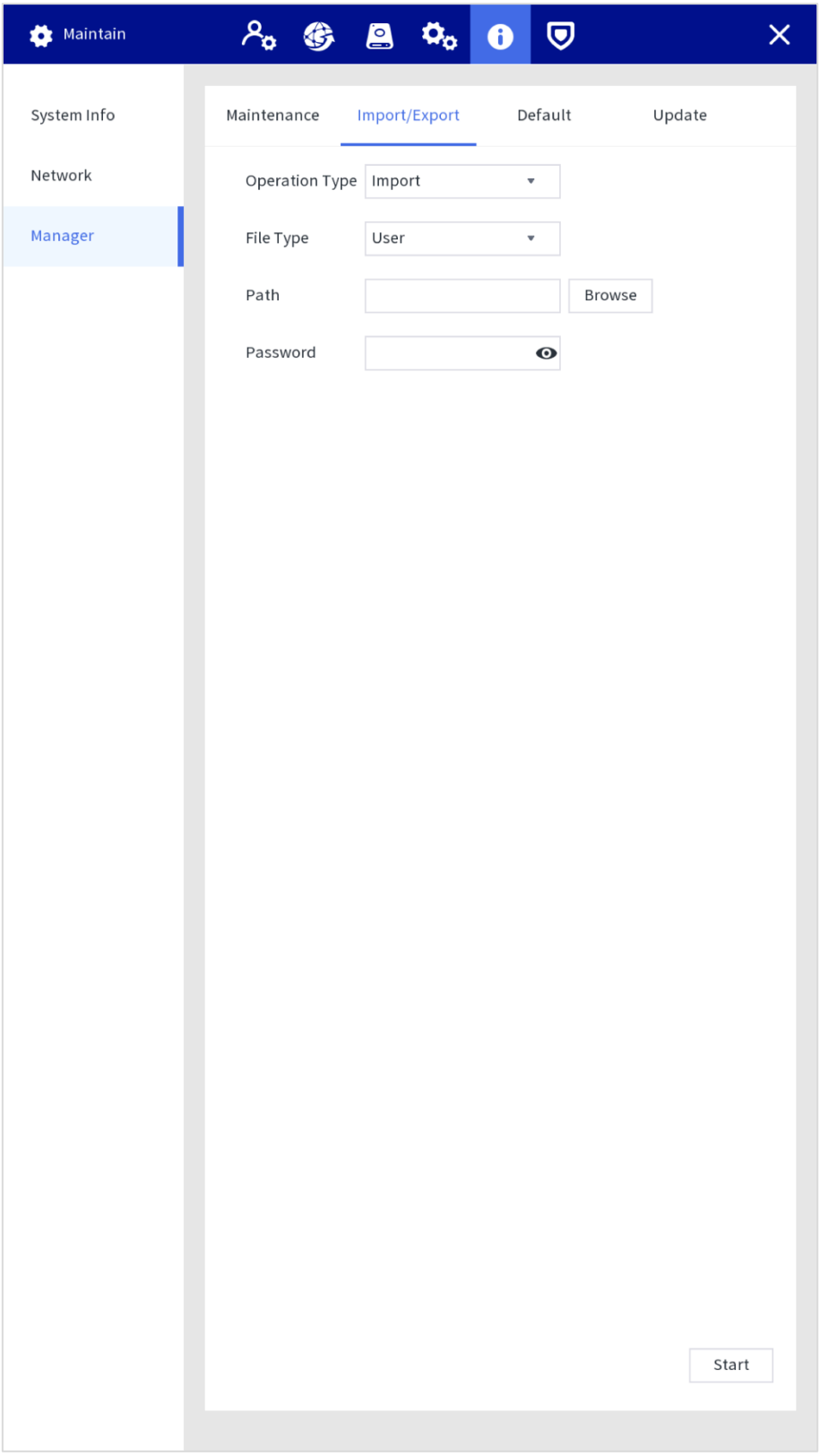


Figura 4-34 Importar configuración



Defecto

Cuando el sistema funcione lentamente y tenga errores de configuración, intente solucionar los problemas restaurando la configuración predeterminada.

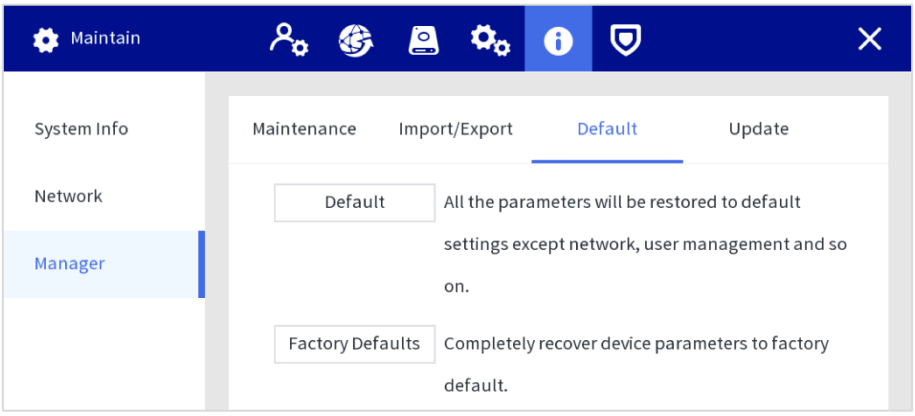
⚠

Hacer clic**Fallas de fábrica**, se eliminarán todas las configuraciones excepto los datos en el almacenamiento externo. Tú puede eliminar datos en un almacenamiento externo formateando los medios de almacenamiento y otros métodos.

Paso 1 Seleccione**Configuración > Mantener > Administrador > Predeterminado**.

Paso 2 Hacer clic**Defecto**o**Fallas de fábrica**según sea necesario.

Figura 4-35 Predeterminado



- Predeterminado: hacer clic**Defecto**, y los parámetros como excepto red, la administración de usuarios se restaurarán a la configuración predeterminada.
- Valor predeterminado de fábrica: haga clic en**Fallas de fábrica**y se muestra el cuadro de diálogo de sugerencias. Hacer clic**DE ACUERDO**. Todos los parámetros se restaurarán a la configuración predeterminada de fábrica.

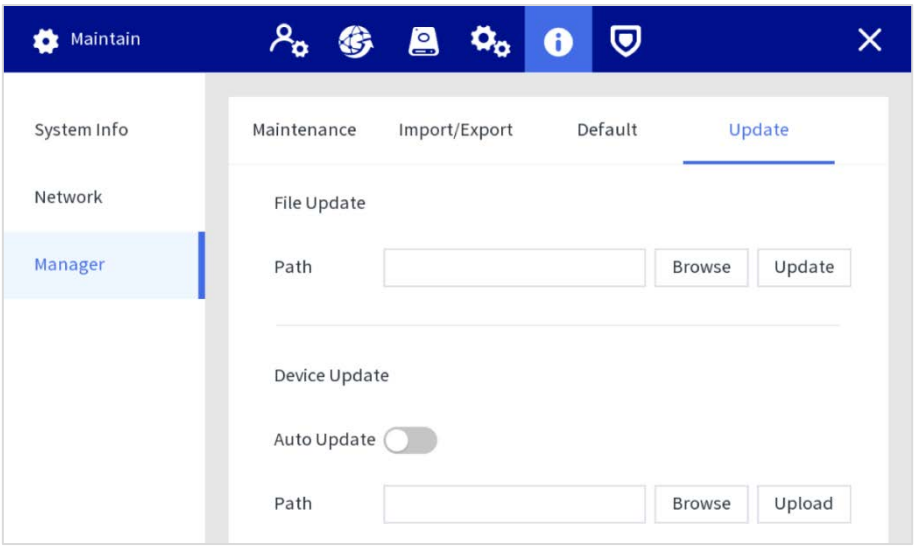
Actualización de la estación

Inserte una unidad flash USB con el archivo de actualización en formato bin y luego importe el archivo de actualización a la estación para actualizar la versión del sistema.

Paso 1 Seleccione**Configuración> Mantener> Administrador> Actualizar**.

Paso 2 Seleccione el archivo de actualización y luego haga clic en**Actualizar**.

Figura 4-36 Actualización



Actualización de la cámara corporal

Antes de actualizar, cargue los archivos de actualización a la Estación de acuerdo con los tipos de cámaras corporales.

- Actualización automática

Habilite la función de actualización automática. La cámara corporal detectará los archivos de actualización y se actualizará automáticamente después de acceder a la estación.

- Actualización manual

  Cuando la función de actualización automática esté deshabilitada, seleccione el archivo de actualización y luego haga clic en**Subir**para sube el archivo de la última versión. Hacer clic  en la interfaz principal y luego haga clic en el**Actualizar**pestaña para actualizar el dispositivo.

4.1.3.6 Seguridad

4.1.3.6.1 Estado de seguridad

Detecte el usuario y el servicio, y escanee los módulos de seguridad para verificar el estado de seguridad de la Estación. Cuando aparece una anomalía, puede procesarla a tiempo.

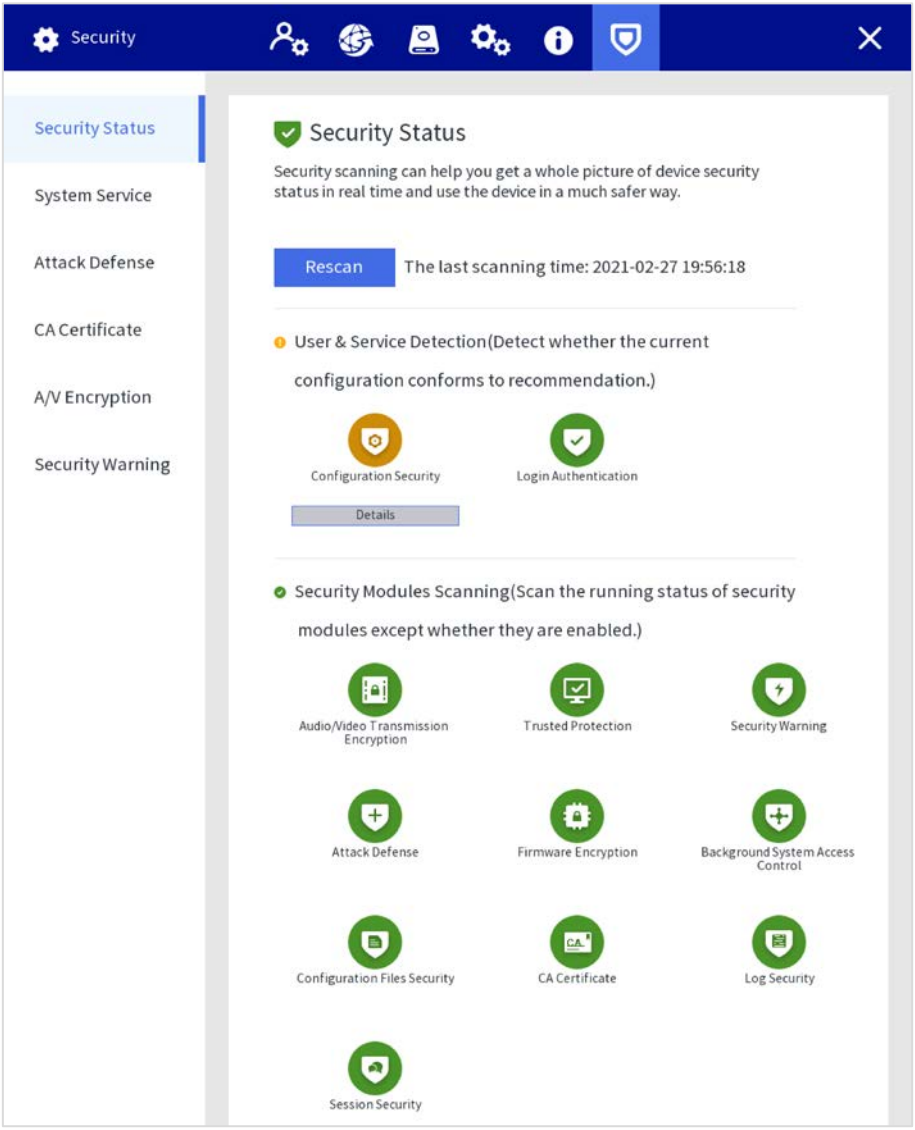
- Detección de usuarios y servicios: detecte la autenticación de inicio de sesión, el estado del usuario y la seguridad de la configuración para verificar si la configuración actual cumple con las recomendaciones.
- Escaneo de módulos de seguridad: Escanea el estado de funcionamiento de los módulos de seguridad, como la transmisión de audio/video, protección confiable, advertencia de seguridad y defensa contra ataques, no detecta cuando están habilitados.

Procedimiento

Paso 1 Seleccione**Configuración > Seguridad > Estado de seguridad**. Hacer clic**volver a**

Paso 2 **escanear**para escanear el estado de seguridad de la Estación.

Figura 4-37 Estado de seguridad



Resultados

Después de escanear, se mostrarán diferentes resultados con diferentes colores. El amarillo indica que los módulos de seguridad son anormales y el verde indica que los módulos de seguridad son normales.

Hacer clic**Detalles**para ver los detalles del resultado del escaneo.

- Hacer clic**Ignorar**para ignorar la excepción, y no se escaneará en el siguiente escaneo.

Hacer clic**Detección de reincorporación**, y la excepción se escaneará en el siguiente escaneo.

- Hacer clic**Optimizar**y se muestra la interfaz correspondiente, y puede editar la configuración para borrar la excepción.

4.1.3.6.2 Sistema

Servicio Básico

Paso 1 Seleccione**Configuración> Seguridad> Servicio del sistema> Servicios básicos**.

Paso 2 Configurar parámetros.

Figura 4-38 Servicios básicos

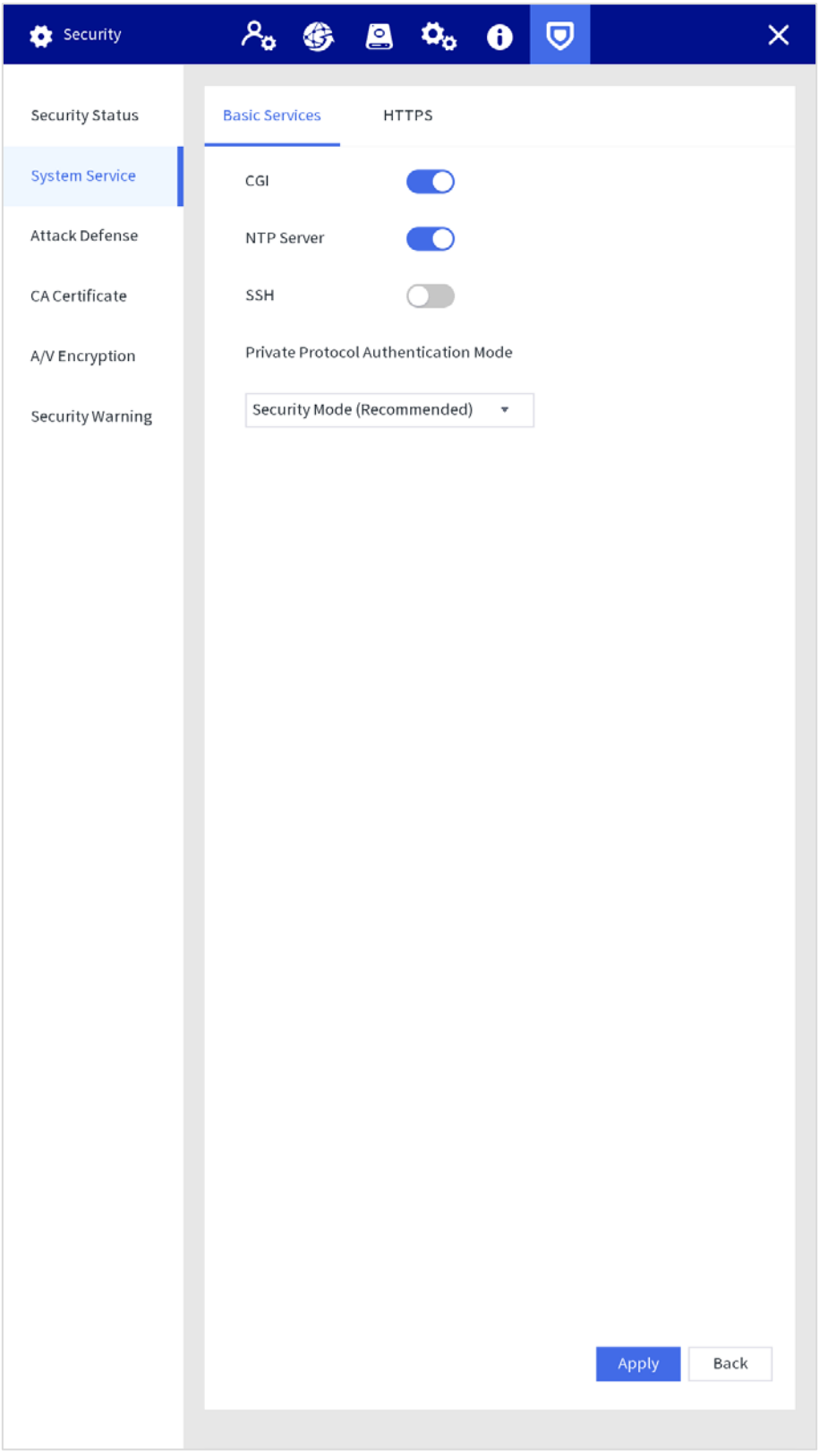


Tabla 4-6 Descripción de los parámetros básicos del servicio

Parámetro	Descripción
CGI	Habilite esta función y los dispositivos podrán acceder a la estación a través de este servicio. Está habilitado por defecto.
Servidor NTP	Después de habilitar esta función, la estación se utiliza como un servidor NTP, que se puede utilizar para sincronizar la hora de la cámara del cuerpo. Está habilitado por defecto.

Parámetro	Descripción
SSH	Puede habilitar la autenticación SSH para realizar la gestión de seguridad. Está habilitado por defecto.
Protocolo privado Autenticación Modo	Seleccione el modo de autenticación de protocolo privado para garantizar la seguridad del dispositivo al iniciar sesión.**modo de seguridad**es recomendado.

Paso 3 Hacer clic**Aplicar**.

HTTPS

Al crear un certificado de servidor, la PC puede iniciar sesión en el dispositivo mediante HTTPS para garantizar la seguridad de los datos de comunicación y proteger la información del usuario y la seguridad del dispositivo con medidas tecnológicas estables.

Le recomendamos el servicio HTTPS. Si el servicio está deshabilitado, puede haber riesgo de fuga de datos.

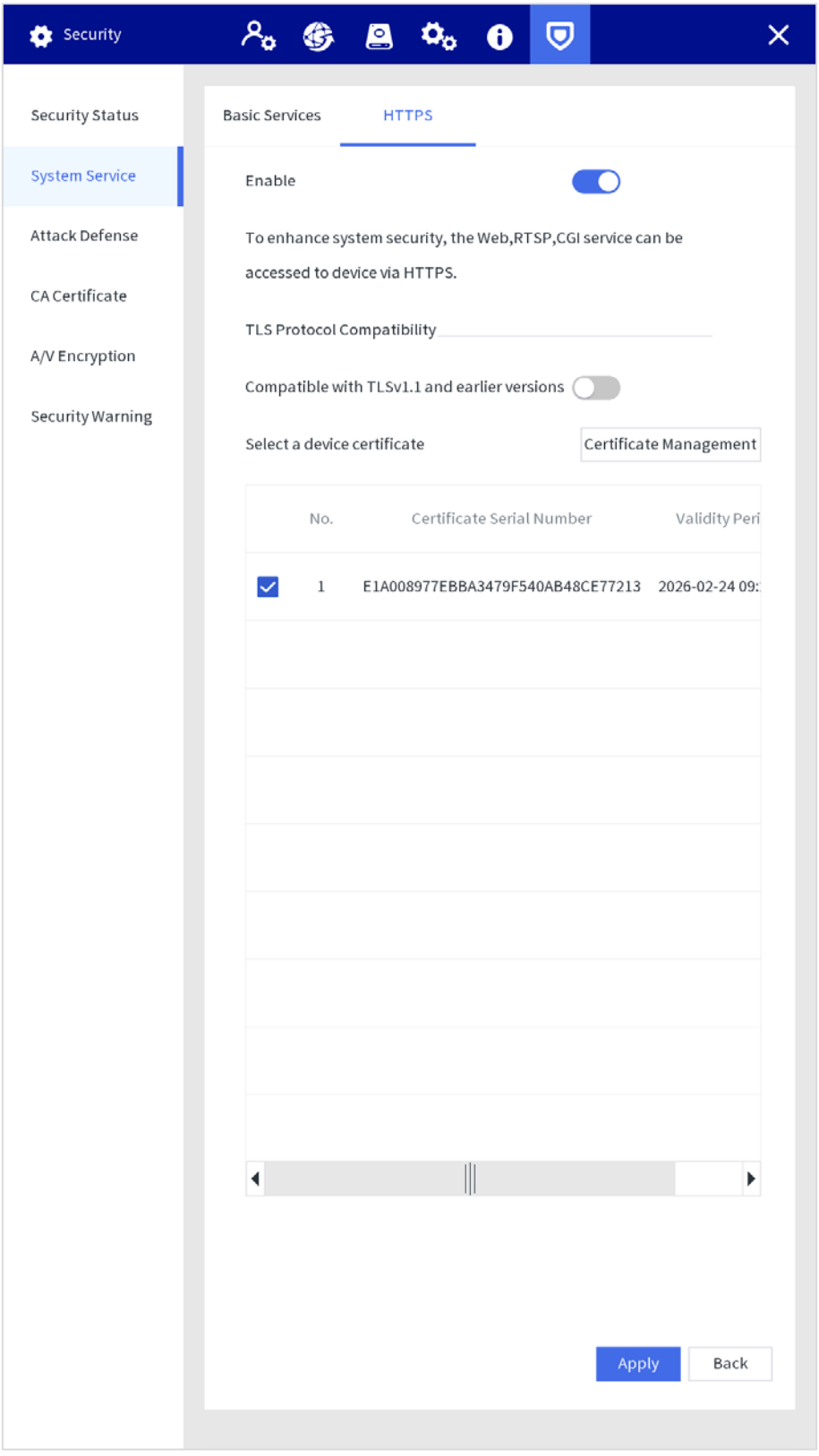
Procedimiento

Paso 1 Seleccione**Configuración > Seguridad > Centro de seguridad >**

Paso 2 **HTTPS**. Habilite HTTPS y luego seleccione la certificación.

Si no hay ningún certificado en la lista, haga clic en**Gestión de certificados**para importar un certificado.

Figura 4-39 HTTPS



Paso 3 (Opcional) Haga clic en junto a**Compatible con TLSv1.1 y versiones anteriores**para permitir la función de compatibilidad de protocolos.

Paso 4 Hacer clic**Aplicar**.

Resultados

Abra el navegador, ingrese https://*IP del dispositivo*:*Puerto*y, a continuación, presione la tecla Intro.

Puerto se refiere al número de puerto HTTPS. Si el puerto HTTPS es 443, simplemente ingrese https://IP del dispositivo.

4.1.3.6.3 Defensa de Ataque

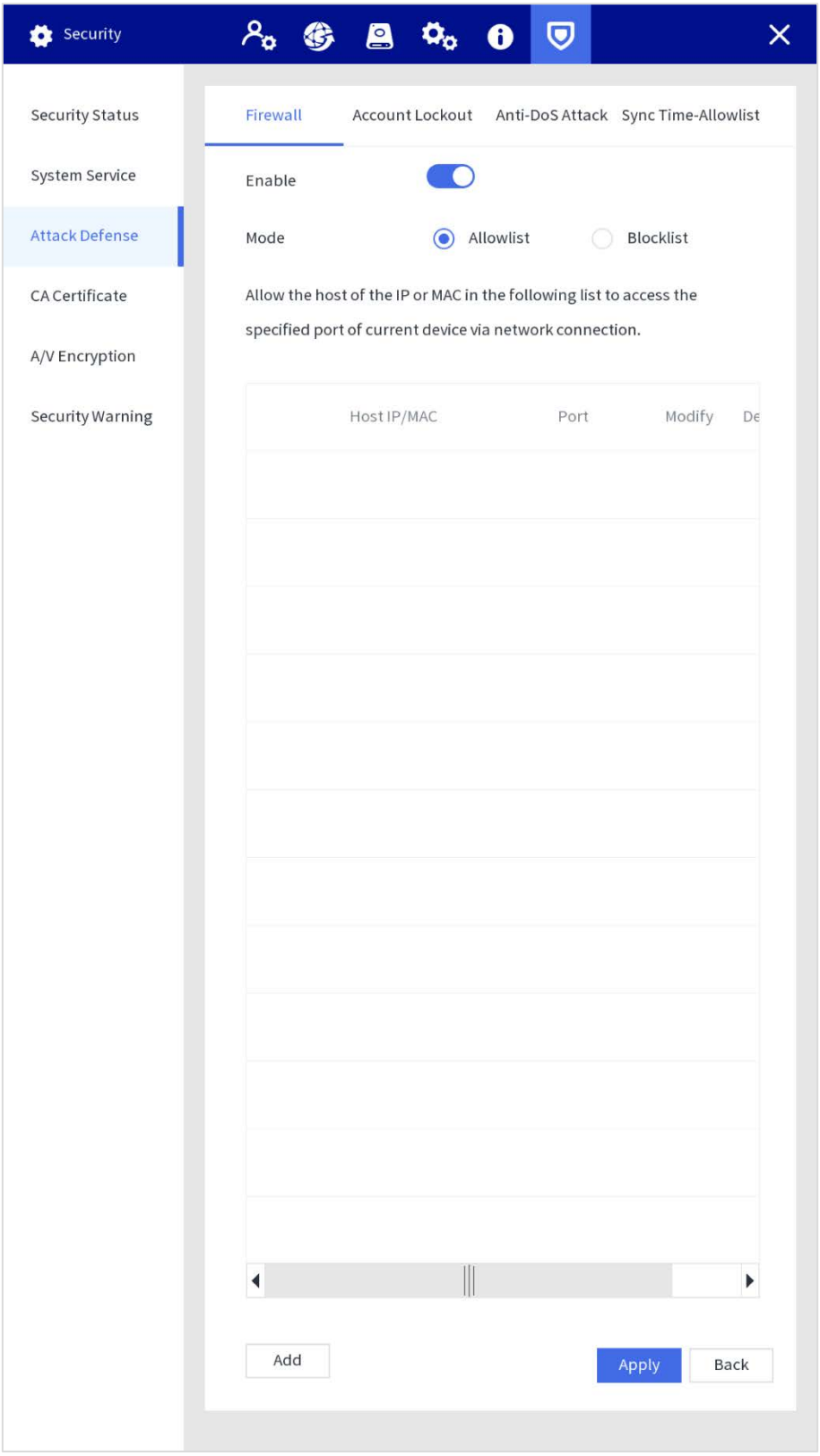
cortafuegos

Configure el firewall para limitar el acceso a la Estación.

Paso 1 Seleccione**Configuración > Seguridad > Defensa contra ataques >**

Paso 2 **Cortafuegos**. Habilite la función de cortafuegos.

Figura 4-40 Cortafuegos



Paso 3 Seleccione el modo de acceso.

La lista de permitidos y la lista de bloqueados no se pueden habilitar al mismo tiempo.

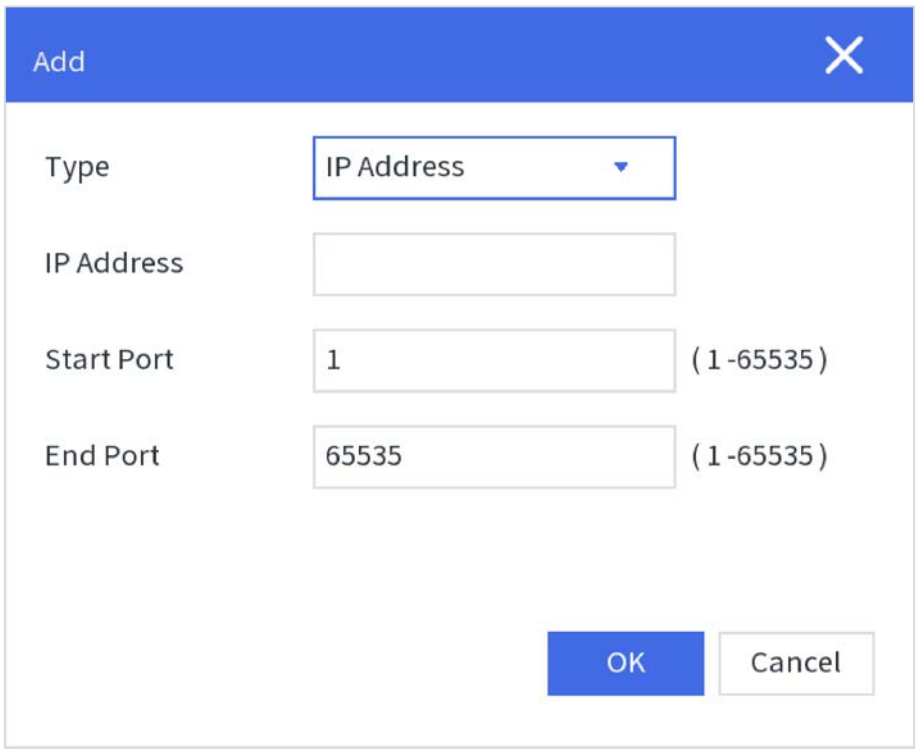
- Lista de permitidos: solo cuando la IP/MAC de su PC está en la lista de permitidos, puede acceder a la Estación. Lista
- de bloqueo: cuando la IP/MAC de su PC está en la lista de bloqueo, no puede acceder a la estación.

Paso 4 Agregue la dirección IP/MAC del host a la lista de permitidos o bloqueados.

1) Haga clic**Agregar**.

2) Ingrese la información del host IP según sea necesario.

Figura 4-41 Agregar lista de permitidos



3) Haga clic**DE ACUERDO**.

Paso 5 Hacer clic**Aplicar**.

Bloqueo de cuenta

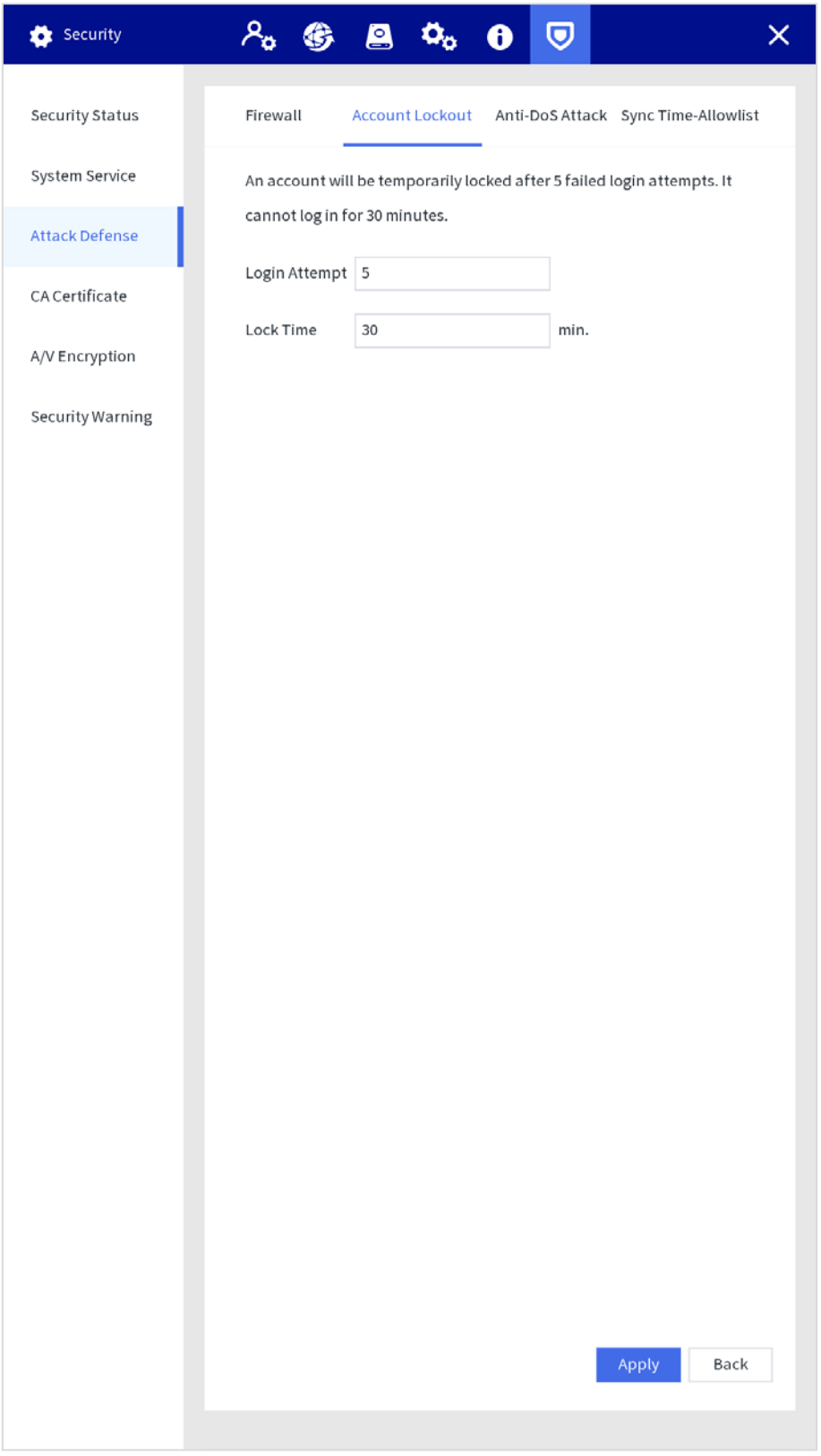
Si ingresa consecutivamente una contraseña incorrecta superior al valor configurado, la cuenta se bloqueará.

Paso 1 Seleccione**Configuración> Seguridad> Defensa contra ataques> Bloqueo de cuenta**.

Paso 2 Configurar parámetros.

- **Intento de inicio de sesión**: límite superior de intentos de inicio de sesión. Si ingresa consecutivamente una contraseña incorrecta superior al valor configurado, la cuenta se bloqueará.
- **Tiempo de bloqueo**: El período durante el cual no puede iniciar sesión después de que los intentos de inicio de sesión alcancen limite superior.

Figura 4-42 Bloqueo de cuenta



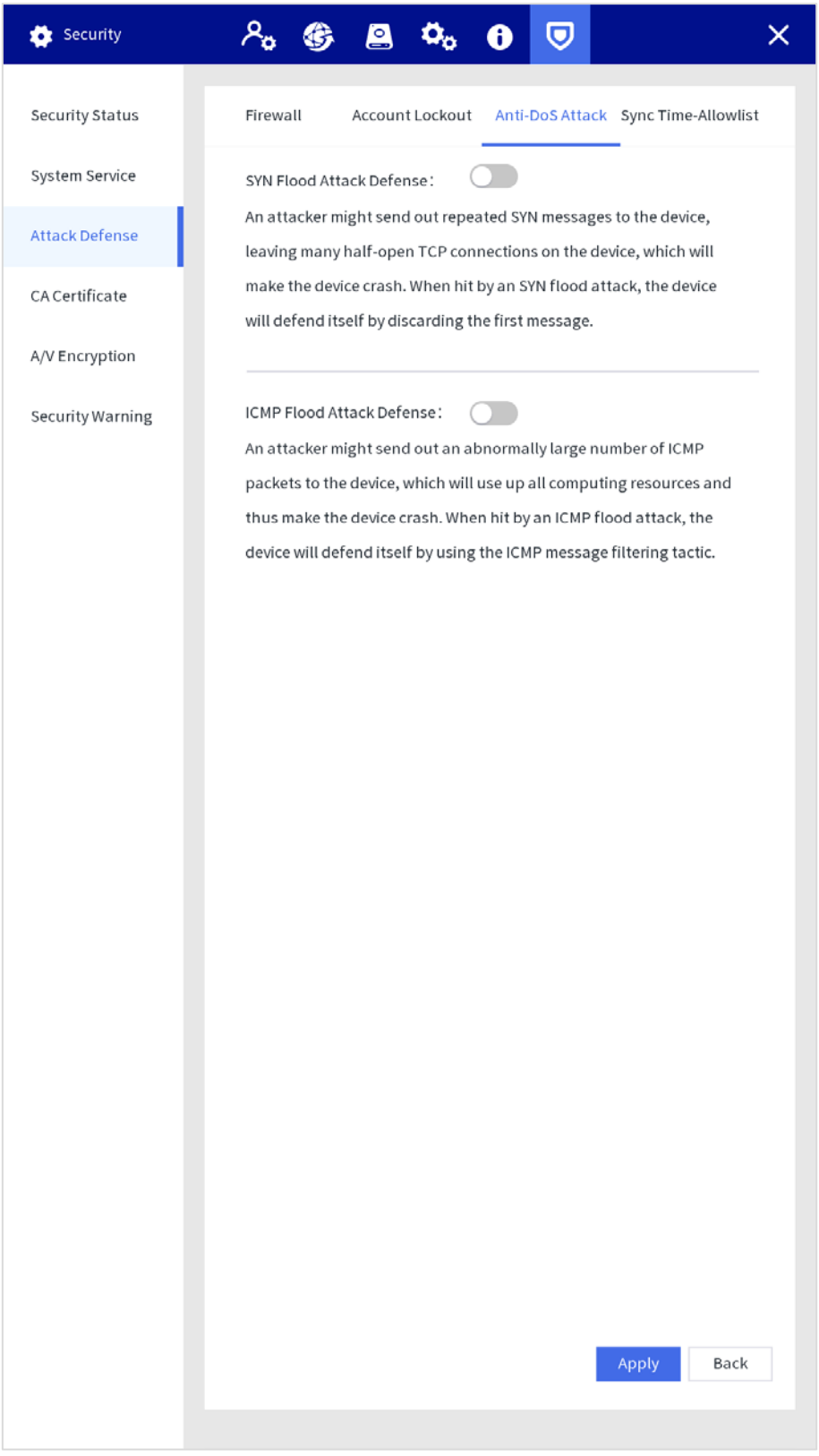
Paso 3 Hacer clic**Aplicar**.

Ataque Anti-DoS

Establezca el modo de defensa contra ataques para defender el dispositivo contra ataques Dos (denegación de servicio). Paso 1 Seleccione**Configuración > Seguridad > Defensa contra ataques > Ataque Anti-DoS**.

Paso 2 Puede habilitar SYN Flood Attack Defense y ICMP Flood Attack Defense para defender el dispositivo contra ataques Dos según sea necesario.

Figura 4-43 Ataque Anti-DoS



Paso 3 Hacer clic**Aplicar**.

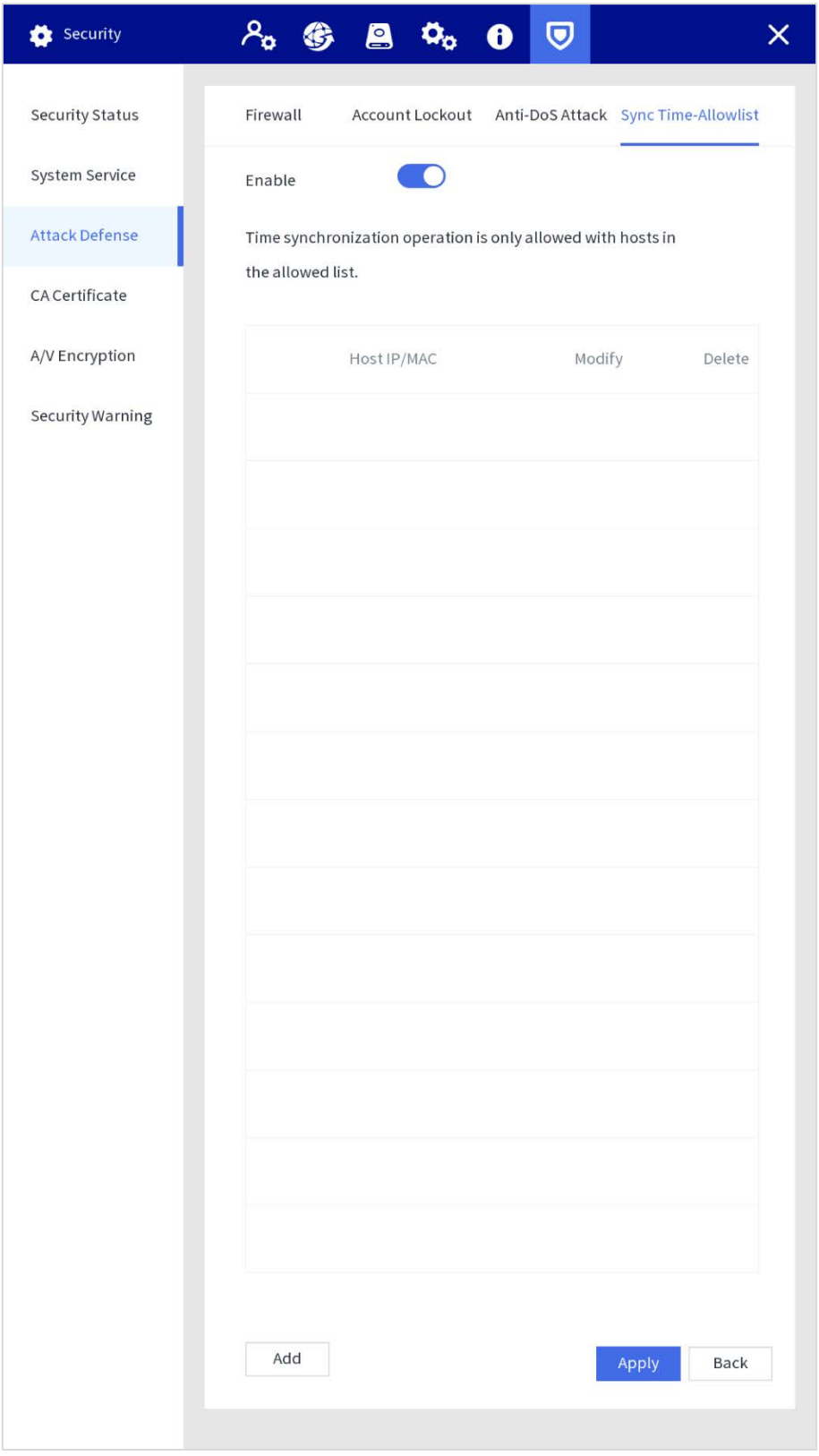
Tiempo de sincronización: lista de permitidos

Establezca la dirección IP de los hosts que pueden sincronizar y cambiar la hora del sistema, en caso de que varios hosts calibren la hora del sistema con la estación varias veces.

Paso 1 Seleccione**Configuración> Seguridad> Defensa contra ataques> Tiempo de sincronización-Lista permitida**.

Paso 2 Habilite la función de lista de permitidos de tiempo de sincronización.

Figura 4-44 Lista permitida de tiempo de sincronización



Paso 3 Hacer clic**Agregar**para agregar la IP/MAC del host de origen a través de la dirección IP o el segmento de IP.

Figura 4-45 Agregar dirección IP

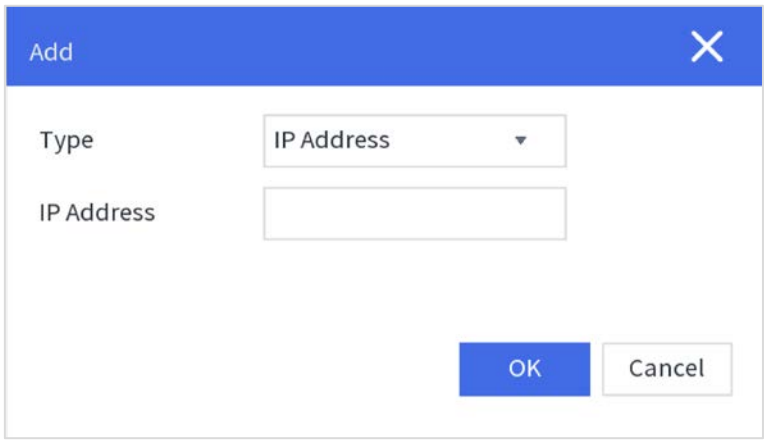
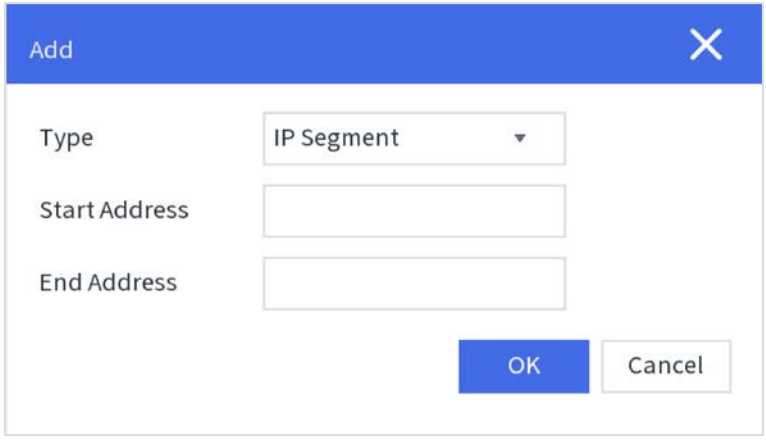


Figura 4-46 Segmento IP



Paso 4 Hacer clic**Aplicar**.

4.1.3.6.4 Certificado CA

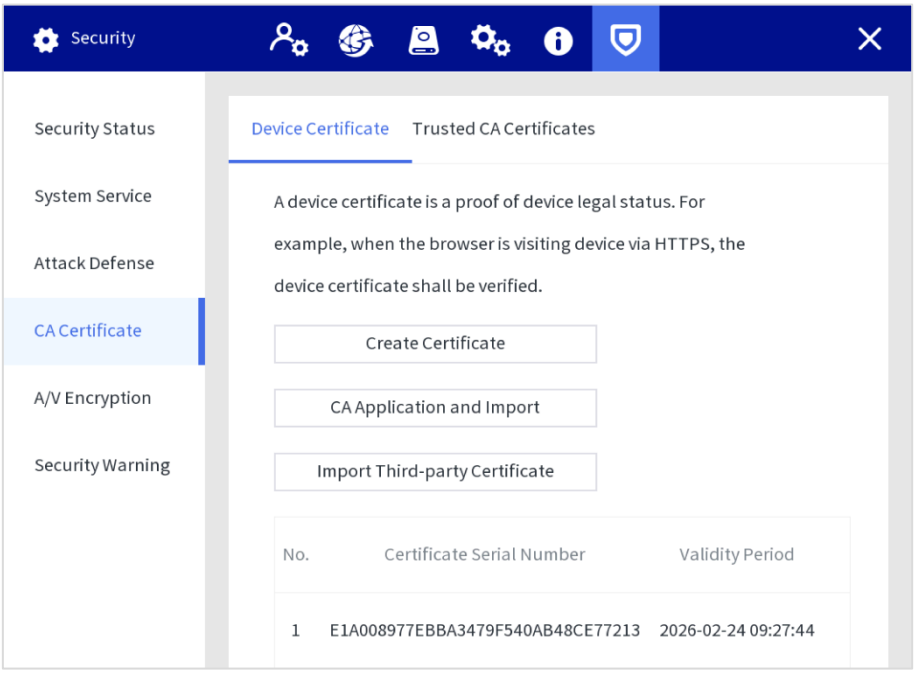
Cree un certificado o cargue un certificado autenticado y luego podrá iniciar sesión a través de HTTPS con el navegador web.

Creando certificado

Paso 1 Seleccione**Configuración> Seguridad> Certificado CA> Certificado de dispositivo**.

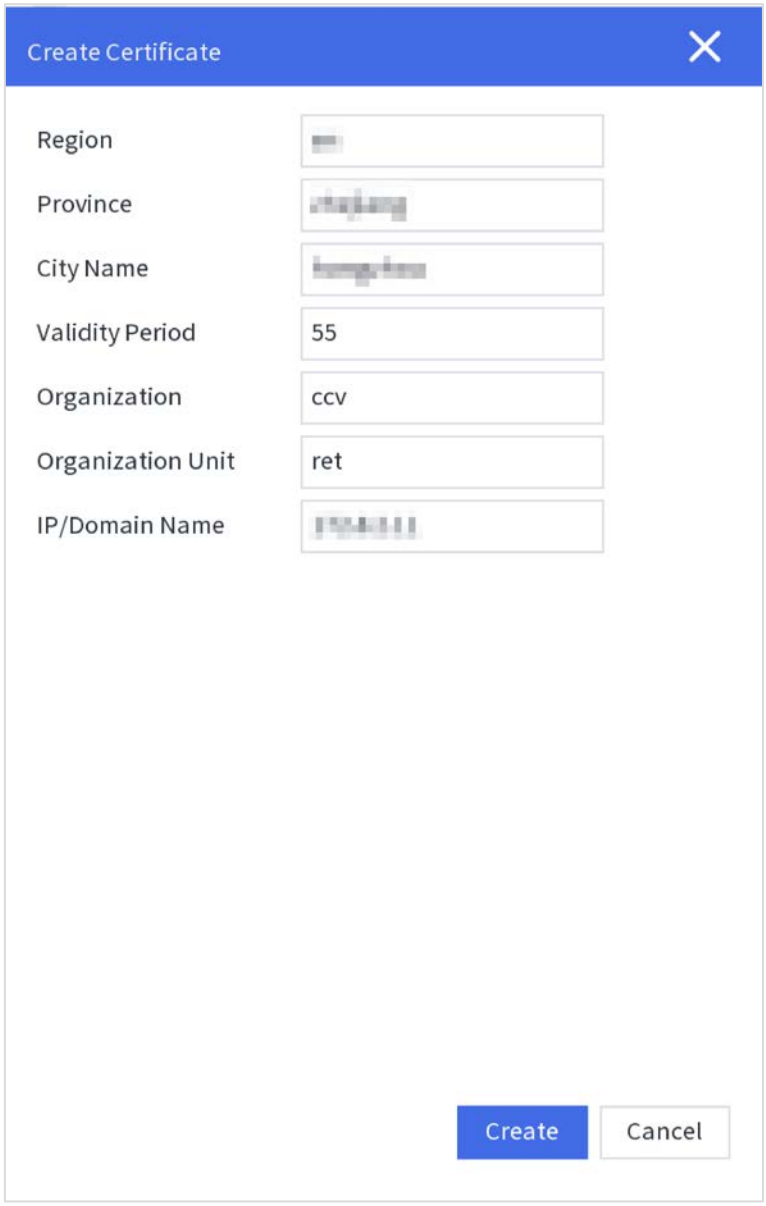
Paso 2 Hacer clic**Crear certificado**.

Figura 4-47 Certificado de dispositivo



Paso 3 Ingrese la información del certificado según sea necesario.

Figura 4-48 Crear certificado



Paso 4 Hacer clic**Crear**.

Una vez que el certificado se haya creado correctamente, puede ver el certificado creado en la **Certificado de dispositivo**interfaz.

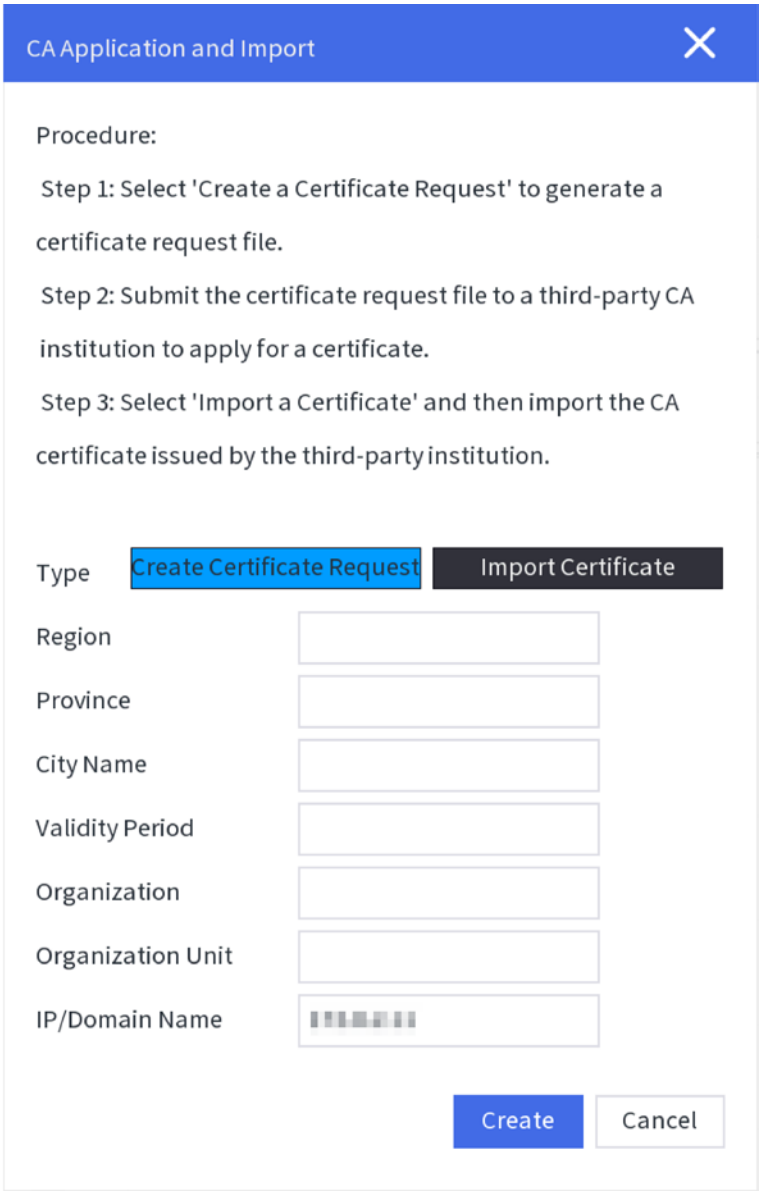
Solicitud e importación del certificado de CA

Paso 1 Seleccione**Configuración> Seguridad> Certificado CA> Certificado de dispositivo**.

Paso 2 Hacer clic**Solicitud e Importación de CA**.

Paso 3 Introduzca la información del certificado y haga clic en**Crear**para guardar el certificado en un dispositivo externo.

Figura 4-49 Solicitar e importar un certificado de CA



Paso 4 Solicite el certificado de CA de la autoridad de certificación de terceros.

Paso 5 Importar certificado CA.

1) Guarde el certificado de CA en una unidad flash USB y luego inserte la unidad en la estación.

2) Haga clic**Certificado de importación**sobre el**Solicitud e Importación de CA**interfaz.

3) Importe el certificado de acuerdo con las instrucciones de la pantalla.

Una vez que el certificado se haya importado correctamente, puede ver el certificado creado en la **Certificado de dispositivo**interfaz.

Importación de certificado de terceros

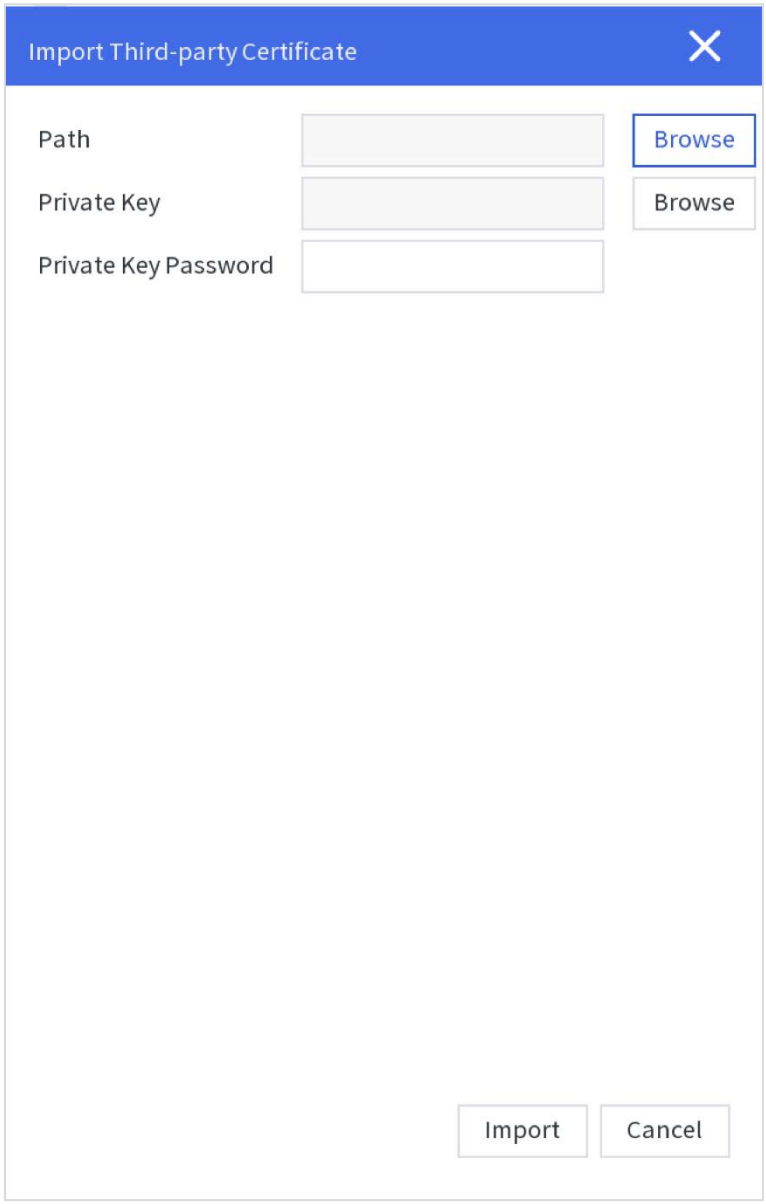
Guarde el certificado de terceros en una unidad flash USB y luego inserte la unidad en la estación.

Paso 1 Seleccione**Configuración> Seguridad> Certificado CA> Certificado de dispositivo**.

Paso 2 Hacer clic**Importar certificado de terceros**.

Paso 3 Seleccione el certificado y el archivo de clave privada e ingrese la contraseña de la clave privada.

Figura 4-50 Importar certificado de terceros



Paso 4 Hacer clic**Importar**.

Una vez que el certificado se haya importado correctamente, puede ver el certificado creado en la **Certificado de dispositivo**interfaz.

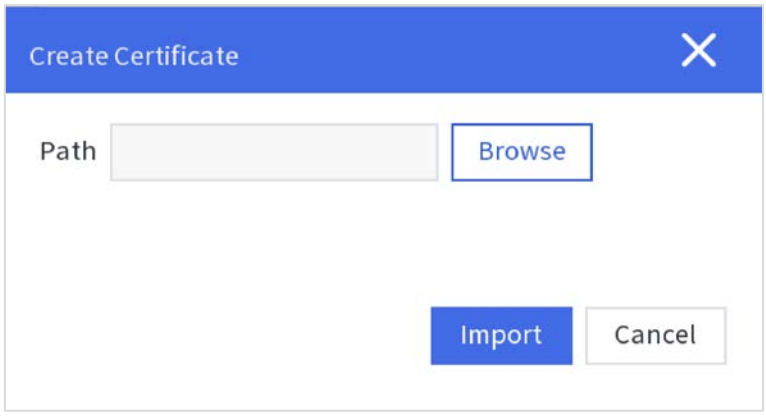
Instalación del certificado de CA de confianza

El certificado CA es un certificado digital de la identidad legal de la Estación. Por ejemplo, cuando la Estación accede a la LAN a través de 802.1x, se requiere el certificado CA.

Paso 1 Seleccione**Configuración > Seguridad > Certificado de CA > Certificado de CA de confianza**.

Paso 2 Hacer clic**Instalar certificado de confianza**.

Figura 4-51 Instalar certificado de CA de confianza



Paso 3 Hacer clic**Navegar**para seleccionar el certificado en la interfaz de solicitud y, a continuación, haga clic en**Importar**.

Una vez que el certificado se haya importado correctamente, puede ver el certificado creado en la **Certificado de dispositivo**interfaz.

4.1.3.6.5 Cifrado A/V

La estación admite el cifrado de audio y video durante la transmisión de datos.

Le recomendamos que habilite la función de cifrado A/V. Puede haber riesgo de seguridad si esta función está desactivado.

Paso 1 Seleccione**Configuración > Seguridad > Cifrado A/V**.

Paso 2 Configurar parámetros.

Figura 4-52 Cifrado A/V

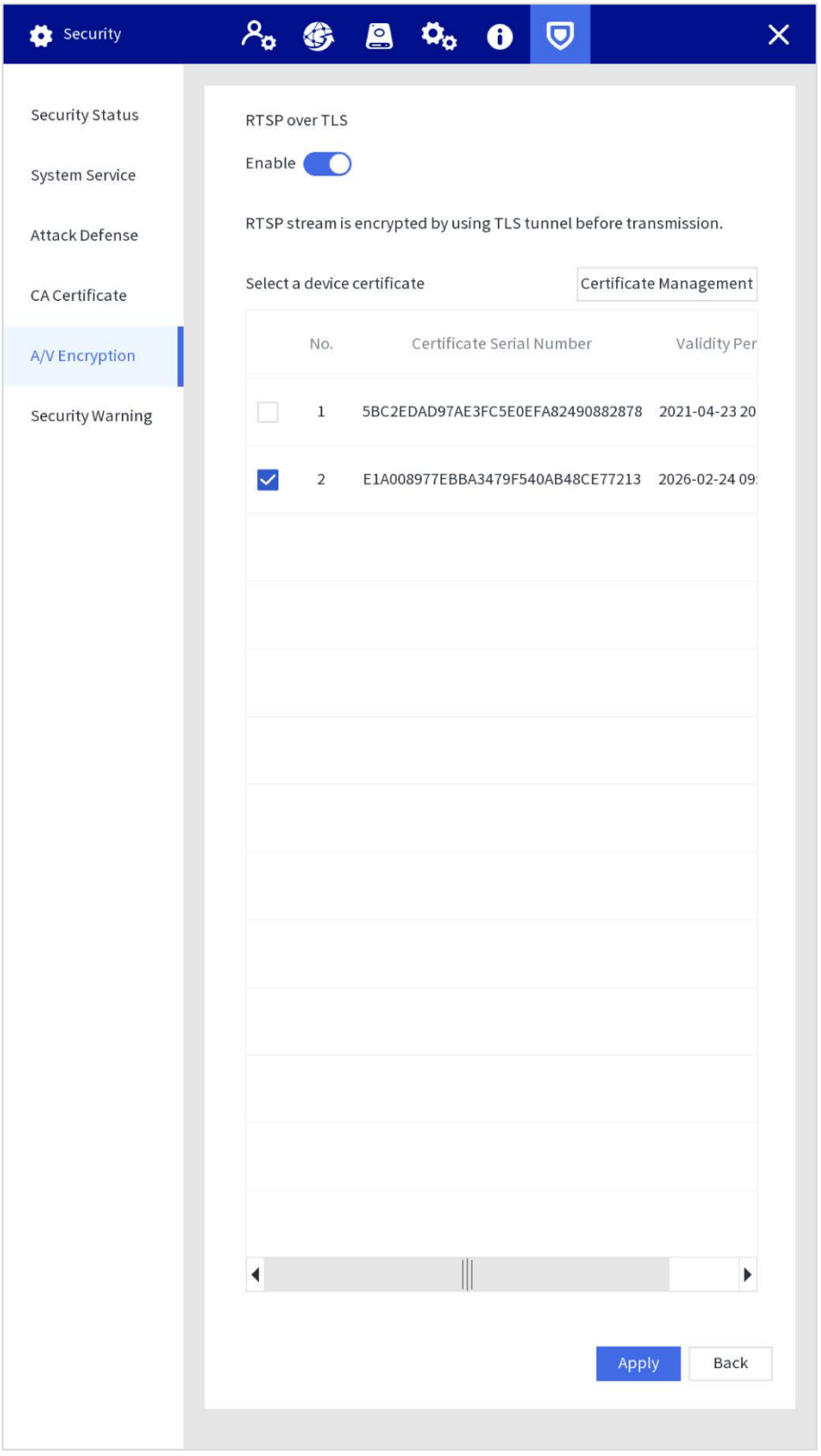


Tabla 4-7 Descripción de audio y video

Tipo de cifrado	Parámetro	Descripción
RTSP sobre TLS	Permitir	Habilita el cifrado de transmisión RTSP mediante TLS. Permitir**RTSP sobre TLS**y, a continuación, seleccione certificado en el **Seleccione un certificado de dispositivo**lista. Puede haber un riesgo de seguridad si RTSP sobre TLS está deshabilitado.
	Certificado administración	El certificado creado o importado se mostrará en la **Seleccione un certificado de dispositivo**y luego seleccione el certificado según sea necesario.

Paso 3 Hacer clic**Aplicar**.

4.1.3.6.6 Advertencia de seguridad

Excepcion de seguridad

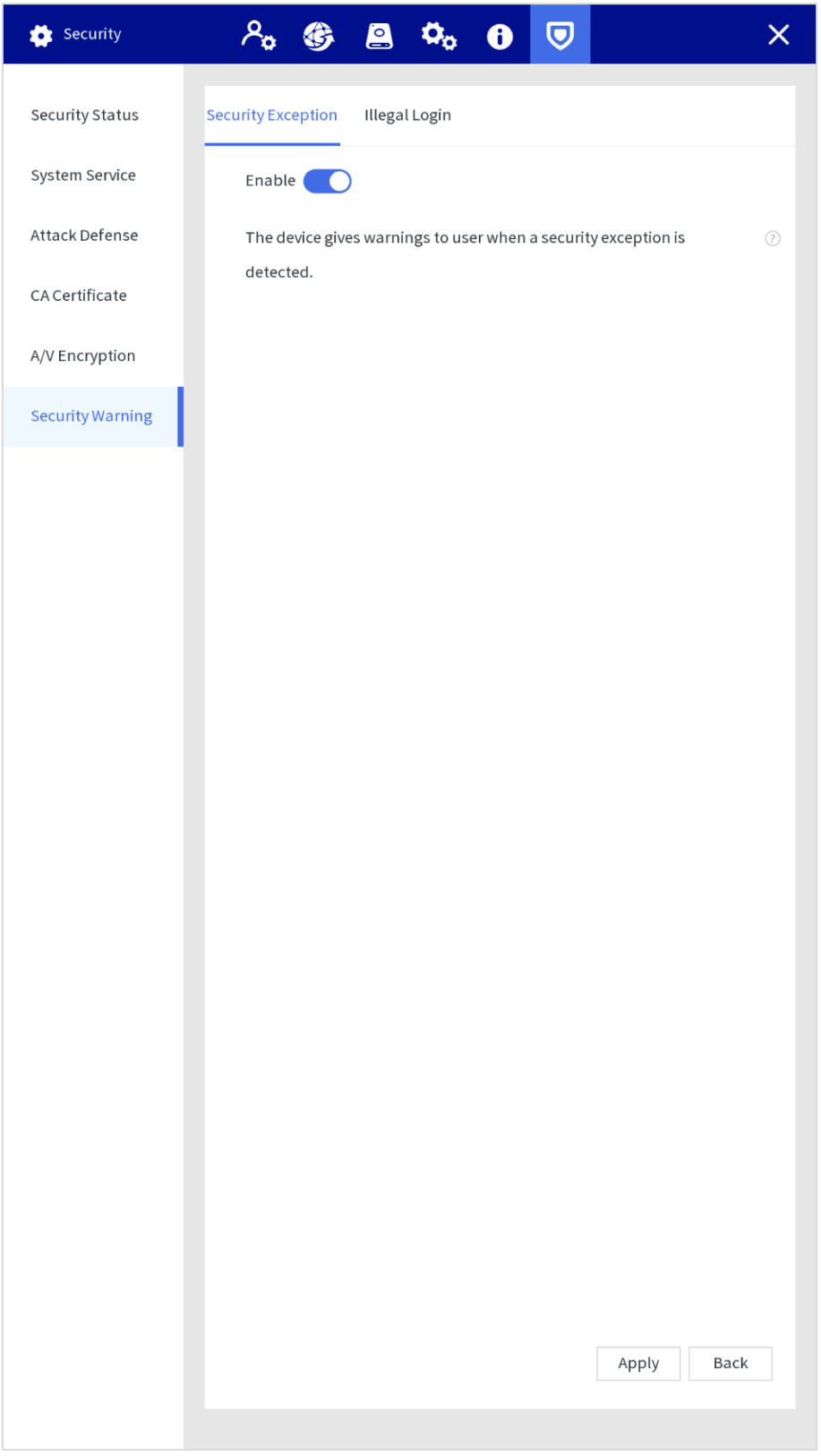
Inmediatamente después de detectar comportamientos anormales de seguridad, la Estación envía una advertencia de seguridad para recordar al usuario oportunamente.

Paso 1 Seleccione**Configuración> Seguridad> Advertencia de seguridad> Excepción de seguridad**.

Paso 2 Habilitar advertencia de seguridad**.**

Hacer clic para ver los detalles del evento de excepción de seguridad.

Figura 4-53 Excepción de seguridad



Paso 3 Hacer clic**Aplicar**.

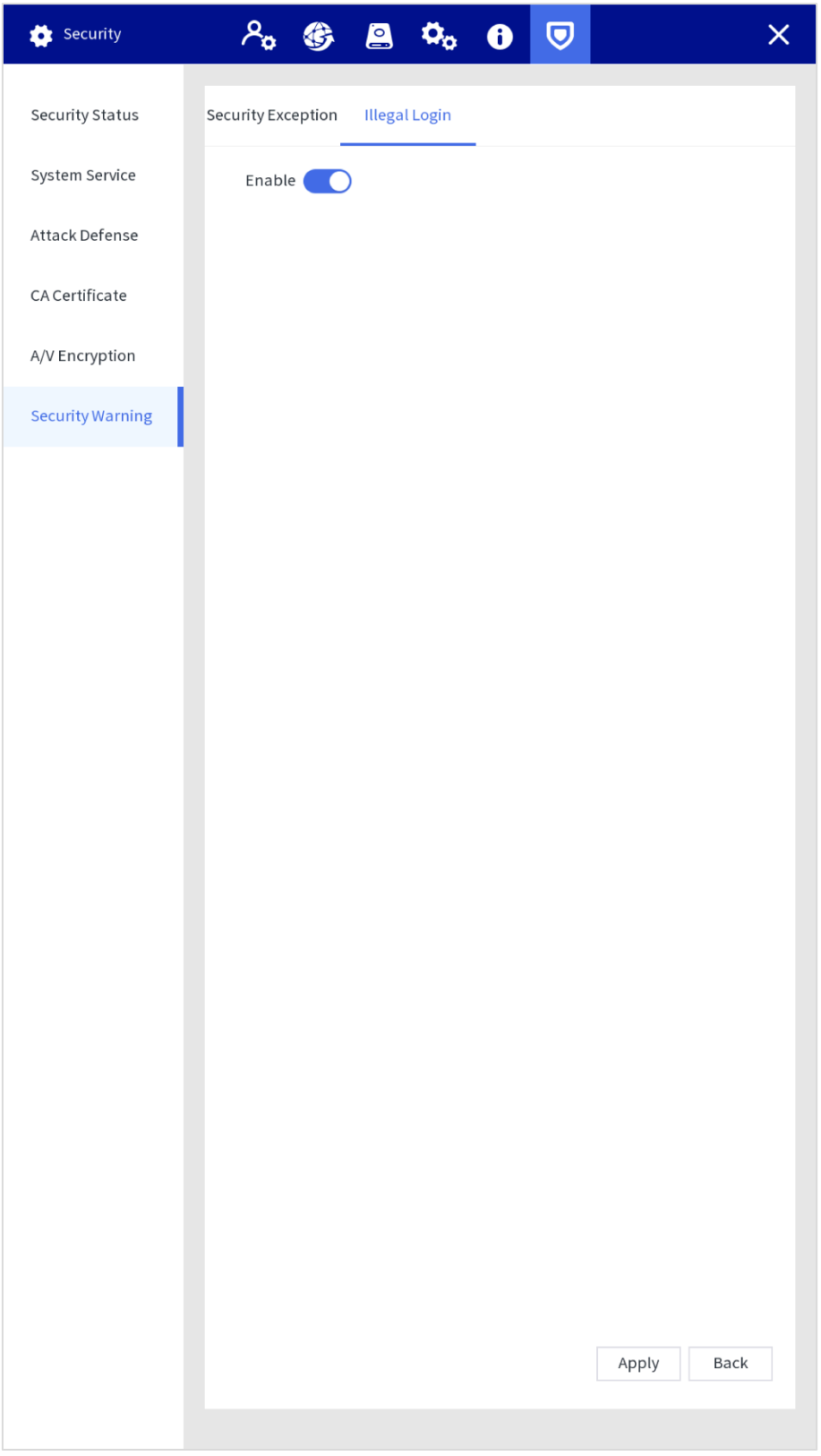
Inicio de sesión ilegal

Inmediatamente después de detectar un inicio de sesión no válido, el dispositivo envía una advertencia de seguridad para recordárselo al usuario a tiempo.

Paso 1 Seleccione**Configuración> Seguridad> Advertencia de seguridad> Inicio de sesión ilegal**.

Paso 2 Habilite la advertencia de inicio de sesión ilegal.

Figura 4-54 Inicio de sesión ilegal



Paso 3 Hacer clic**Aplicar**.

4.2 Configuración web

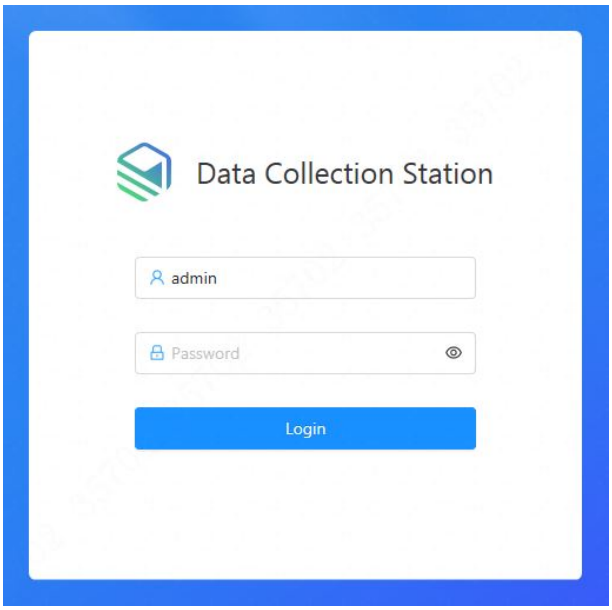
4.2.1 Iniciar sesión

No puede iniciar sesión en la estación a través de navegadores sin complementos.

Inicie sesión en la web de la Estación siguiendo los siguientes pasos.

Paso 1 Ingrese la dirección IP (192.168.1.108 para Ethernet 1 y 192.168.2.108 para Ethernet 2 de manera predeterminada) en la barra de direcciones del navegador IE y luego presione Entrar.

Figura 4-55 Inicio de sesión



Paso 2 Introduzca el nombre de usuario y la contraseña.

La cuenta de administrador es admin por defecto. Hacer

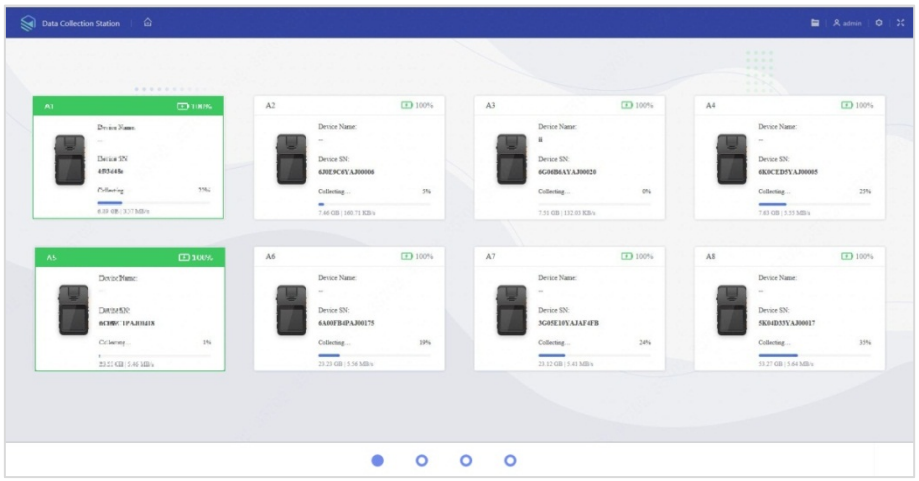
Paso 3 clic**Acceso.**

4.2.2 Gestión de archivos

4.2.2.1 Recopilación de archivos

Después de recopilar los archivos de datos de las cámaras corporales, la estación cargará los archivos en la plataforma o FTP de acuerdo con la configuración en**Almacenamiento**.

Figura 4-56 Carga de archivos

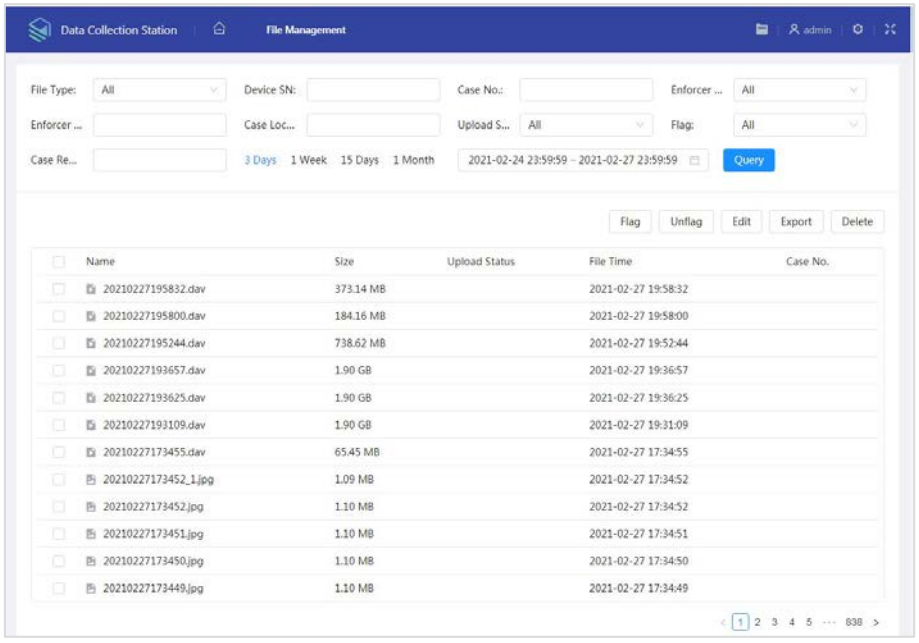


4.2.2.2 Búsqueda de archivos

Seleccione**Gestión de archivos**e ingrese el tipo de archivo, el departamento del ejecutor, el estado de carga, el SN del dispositivo, el número del ejecutor, la bandera, el número del caso, la ubicación del caso y los comentarios del caso, y puede buscar archivos de video, archivos de audio e instantáneas de acuerdo con las condiciones configuradas.

El rango de tiempo máximo para la búsqueda de archivos es de 1 mes.

Figura 4-57 Buscar archivos



4.2.2.3 Visualización de archivos

Haga doble clic en un archivo para ver los detalles y podrá realizar las operaciones de reproducción rápida, reproducción lenta, acercamiento o alejamiento.

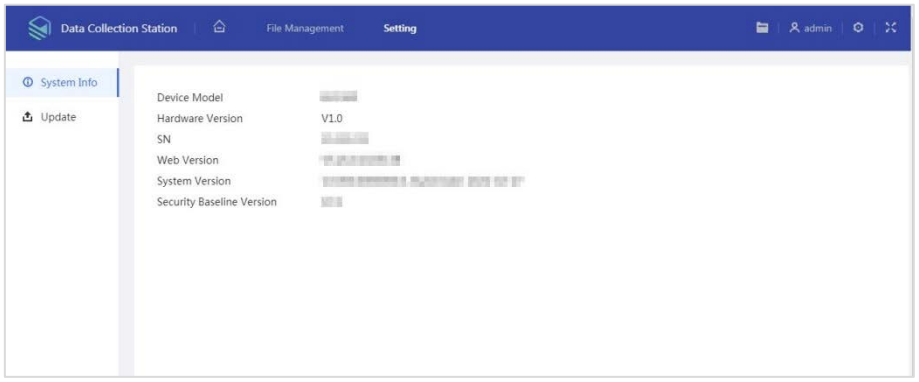
No puede reproducir rápidamente o reproducir lentamente un archivo de audio en formato AMR.

4.2.3 Configuración web

4.2.3.1 Información del sistema

Seleccione**Configuración > Información del sistema**y puede ver el modelo del dispositivo, la versión de hardware, el SN, la versión web, la versión del sistema y la versión de referencia de seguridad.

Figura 4-58 Información del sistema

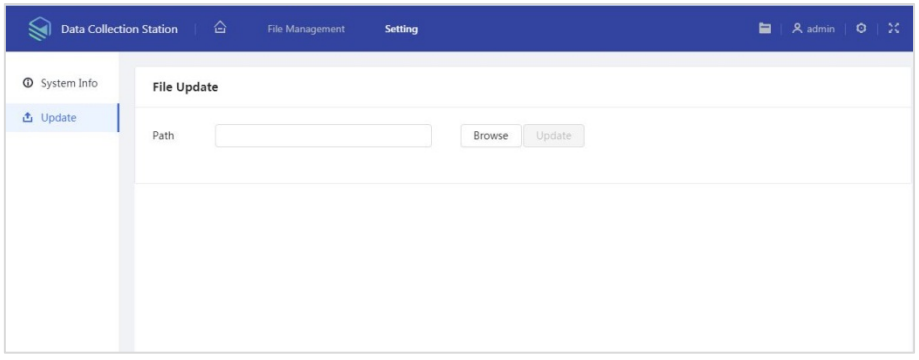


4.2.3.2 Actualizar

Seleccione**Configuración > Actualizar**, seleccione el archivo y luego haga clic en**Actualizar**.

- No desconecte la alimentación o la red, ni reinicie ni apague la Estación durante la actualización.
- Asegúrese de que el archivo de actualización sea correcto. Un archivo de actualización incorrecto puede provocar un error en el dispositivo.

Figura 4-59 Actualización



Apéndice 1 RAID

RAID es una abreviatura de matriz redundante de discos independientes. Consiste en combinar varios HDD independientes (HDD físicos) para formar un grupo de HDD (HDD lógico), para proporcionar un mayor rendimiento de almacenamiento y redundancia de datos.

Nivel RAID

En comparación con un HDD, RAID proporciona más capacidad de almacenamiento y redundancia de datos. Las diferentes matrices redundantes tienen diferentes niveles de RAID. Cada nivel de RAID tiene su propia protección de datos, disponibilidad de datos y grado de rendimiento.

Nivel RAID	Descripción	mín. HDD necesario
RAID 0	RAID 0 se llama creación de bandas. RAID 0 es para guardar la fragmentación continua de datos en varios discos duros. Puede procesar la lectura y escritura al mismo tiempo, por lo que su velocidad de lectura/escritura es N (N se refiere a la cantidad de HDD del RAID 0) veces más que un HDD. RAID 0 no tiene datos redundantes, por lo que un daño en el HDD puede provocar la pérdida de datos que no se pueden restaurar.	2
RAID 1	También se le llama espejo o espejo. Los datos de RAID 1 se escriben en dos o más HDD por igual, lo que garantiza la confiabilidad del sistema y los datos se pueden reparar. La velocidad de lectura de RAID 1 está casi cerca del volumen total de todos los discos duros. La velocidad de escritura está limitada por el HDD más lento. Al mismo tiempo, RAID 1 tiene la tasa de uso de HDD más baja. Es solo el 50%.	
RAID 5	RAID 5 es para guardar los datos y la información de verificación impar/par correspondiente en cada HDD del grupo RAID 5 y guardar la información de verificación y los datos correspondientes en diferentes HDD. Cuando se daña un HDD de RAID 5, el sistema puede usar los datos restantes y la información de verificación correspondiente para restaurar los datos dañados. No afecta la integridad de los datos.	3
RAID 6	Basado en RAID 5, RAID 6 agrega un HDD de verificación impar/par. Los dos sistemas pares/impares independientes adoptan algoritmos diferentes, la fiabilidad de los datos es muy alta. Incluso dos HDD se rompen al mismo tiempo, no hay riesgo de pérdida de datos. En comparación con RAID 5, RAID 6 necesita asignar un espacio de disco duro más grande para la información de verificación impar/par, por lo que su lectura/escritura es aún peor.	4
RAID 10	RAID 10 es una combinación de RAID 1 y RAID 0. Utiliza la alta velocidad extra eficiente de RAID 0 y la alta capacidad de protección y restauración de datos de RAID 1. Tiene un alto rendimiento de lectura/escritura y seguridad. Sin embargo, la eficiencia de uso de RAID 10 HDD es tan baja como RAID 1.	

Capacidad RAID

Consulte la hoja para obtener información sobre el espacio RAID.

capacidadN se refiere a la cantidad de mini HDD para crear el RAID correspondiente, que está sujeto a la valor en la interfaz web.

Parámetro	Espacio total del N HDD
RAID 10	(N/2) × min (capacidad N)
RAID 6	(N-2) × min (capacidad N)
RAID 5	(N-1) × min (capacidad N)
RAID 1	Min (capacidad N)
RAID 0	La cantidad total del grupo RAID actual

Apéndice 2 Recomendaciones sobre ciberseguridad

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

Acciones obligatorias que se deben tomar para la seguridad básica de la red del dispositivo: 1. Use contraseñas seguras

Consulte las siguientes sugerencias para establecer contraseñas:

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

2. Actualice el firmware y el software del cliente a tiempo

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

Recomendaciones "agradables de tener" para mejorar la seguridad de la red de su dispositivo: 1. Protección física

Le sugerimos que realice una protección física al dispositivo, especialmente a los dispositivos de almacenamiento. Por ejemplo, coloque el dispositivo en una sala y gabinete de computadoras especiales, e implemente un permiso de control de acceso y una administración de claves bien hechos para evitar que el personal no autorizado realice contactos físicos, como dañar el hardware, la conexión no autorizada de un dispositivo extraíble (como un disco flash USB). , puerto serie), etc.

2. Cambie las contraseñas regularmente

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

3. Establezca y actualice la información de restablecimiento de contraseñas a tiempo

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

4. Habilitar bloqueo de cuenta

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

5. Cambiar HTTP predeterminado y otros puertos de servicio

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

6. Habilitar HTTPS

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

7. Enlace de dirección MAC

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

8. Asigne cuentas y privilegios de manera razonable

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

9. Deshabilite los servicios innecesarios y elija modos seguros

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

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

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

10. Transmisión encriptada de audio y video

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

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

11. Auditoría segura

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

12. Registro de red

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

13. Construya un entorno de red seguro

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

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

- Habilite la función de filtrado de direcciones IP/MAC para limitar el rango de hosts que pueden acceder al dispositivo.