# Gerente de MPT

## Manual del usuario

# Prefacio

Este manual presenta las funciones y operaciones del cliente de PC MPT Manager (en adelante denominado "el cliente").

Instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

| Palabras de señal | Significado |
|---|---|
| DANGER | Indica un peligro potencial alto que, si no se evita, provocará la muerte o lesiones graves. |
| WARNING | Indica un peligro potencial medio o bajo que, si no se evita, podría provocar lesiones leves o moderadas. |
| TIPS | Proporciona métodos para ayudarle a resolver un problema o ahorrar tiempo. |
| NOTE | Proporciona información adicional como complemento al texto. |

Historial de revisiones

| Versión | Contenido de la revisión | Hora de lanzamiento |
|---|---|---|
| Versión 1.0.0 | Primer lanzamiento. | Junio de 2025 |

Aviso de protección de la privacidad

Como usuario del dispositivo o responsable del tratamiento de datos, podría recopilar datos personales de terceros, como su rostro, audio, huellas dactilares y número de matrícula. Debe cumplir con las leyes y normativas 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 a las personas sobre la existencia del área de vigilancia y proporcionar la información de contacto requerida.

## Acerca del manual

- Este manual es solo de referencia. Podrían existir ligeras diferencias entre el manual y el producto.
- No seremos responsables de pérdidas ocasionadas por el uso del producto de formas que no cumplan con el manual.
- El manual se actualizará según las últimas leyes y regulaciones de las jurisdicciones pertinentes. Para obtener información detallada, consulte el manual de usuario impreso, utilice nuestro CD-ROM, escanee el código QR o visite nuestro sitio web oficial. Este manual es solo de referencia. Podrían existir ligeras diferencias entre la versión electrónica y la versión impresa.
- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto podrían generar diferencias entre el producto real y el manual. Para obtener el programa más reciente y la documentación complementaria, póngase en contacto con el servicio de atención al cliente.
- Podría haber errores de impresión o desviaciones en la descripción de las funciones, operaciones y datos técnicos. En caso de duda o controversia, nos reservamos el derecho de ofrecer una explicación definitiva.

- Actualice el software del lector o pruebe otro software de lectura convencional si no se puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas registradas y nombres de empresas en el manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, comuníquese con el proveedor o el servicio de atención al cliente si ocurre algún problema durante el uso del dispositivo.
- Si existe alguna incertidumbre o controversia, nos reservamos el derecho de explicación final.

# Tabla de contenido

# 1 Descripción general

MPT Manager, un software cliente para ordenador, ofrece servicios como copias de seguridad de exportación de audio y vídeo, exportación de registros y actualización de dispositivos, compatible con dispositivos portátiles como el MPT320, la cámara corporal N1, etc. Este manual toma como ejemplo el MPT230.

Antes de utilizar el software, asegúrese de que los controladores de Android estén instalados en su computadora y de que pueda reconocer correctamente el dispositivo individual.

# 2 Configuraciones básicas

## 2.1 Conexión del dispositivo

Procedimiento

Paso 1 Instalar el Administrador MPT.

Siga las instrucciones del sistema y haga clic**Próximo**Hasta que se complete la instalación. Después, aparecerá un icono de acceso directo a MPT Manager en el escritorio de su computadora.

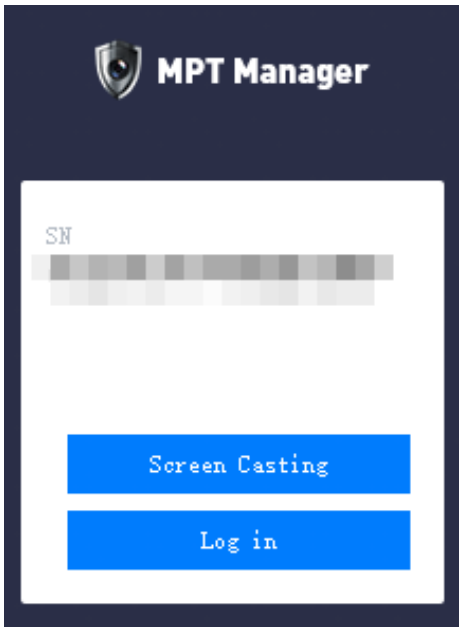
Paso 2 Inicie el dispositivo y luego conéctelo a su computadora a través del cable USB.

Paso 3 Haga doble clic 

En el escritorio, haga clic en**Acceso**para ingresar la contraseña del dispositivo y luego haga clic en **DE ACUERDO**.

Cuando la computadora detecte el dispositivo, mostrará el número de serie del dispositivo en el lado izquierdo.

Figura 2-1 Iniciar sesión en MPT Manager

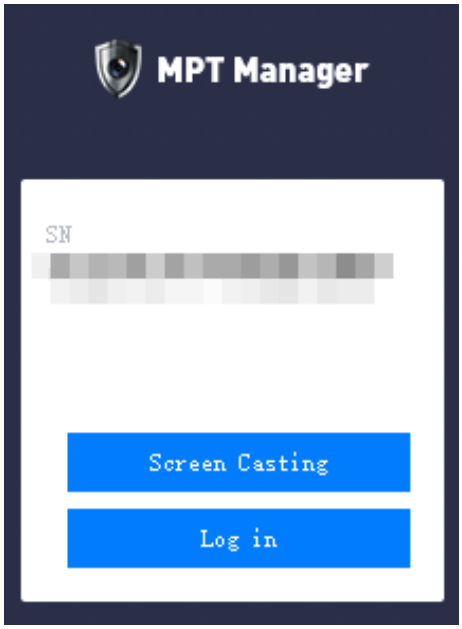



## 2.2 Transmisión de pantalla

Puede realizar una transmisión de pantalla para el MPT 230 y la cámara corporal N1 en su computadora.

Después de conectar el dispositivo a la computadora, haga clic en**Transmisión de pantalla**proyectar la interfaz del dispositivo en la computadora, permitiendo el control remoto del dispositivo a través de la computadora.

Figura 2-2 Iniciar sesión en MPT Manager




El inicio de sesión del dispositivo y la transmisión de pantalla no se pueden habilitar al mismo tiempo.

## 2.3 Administración de dispositivos

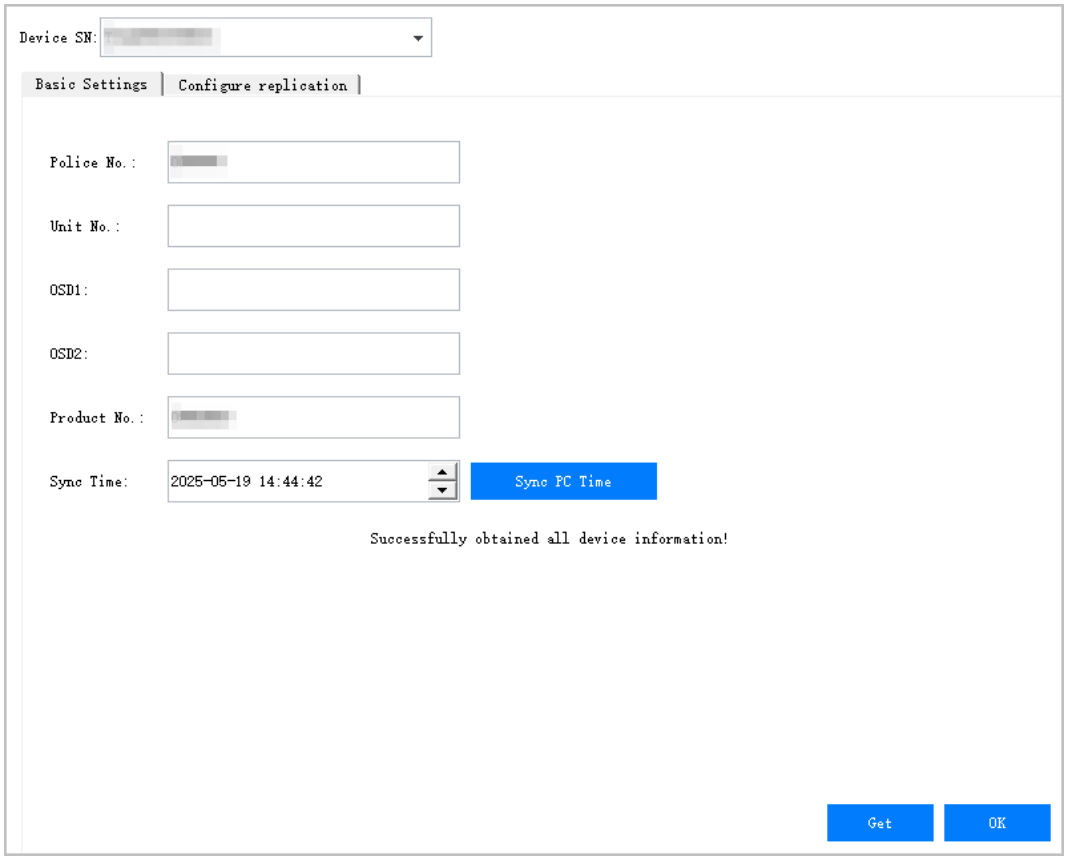
Procedimiento

Paso 1 Después de conectar el dispositivo a la computadora e iniciar sesión en el Administrador MPT, haga clic en**Configuración**

Paso 2 Seleccione el número de serie del dispositivo correspondiente en la lista desplegable para seleccionar el dispositivo. En el

Paso 3 **Configuración básica**pestaña, haga clic**Conseguir**para obtener la información del dispositivo.

Figura 2-3 Administración de dispositivos




Hacer clic**Sincronizar la hora del PC**para sincronizar la hora del dispositivo con la hora de la computadora.

## 2.4 Replicación de dispositivos

Puede copiar las configuraciones de registro y codificación activas, pero el ID de registro se ha reemplazado con el mismo valor y debe ajustarlo manualmente.

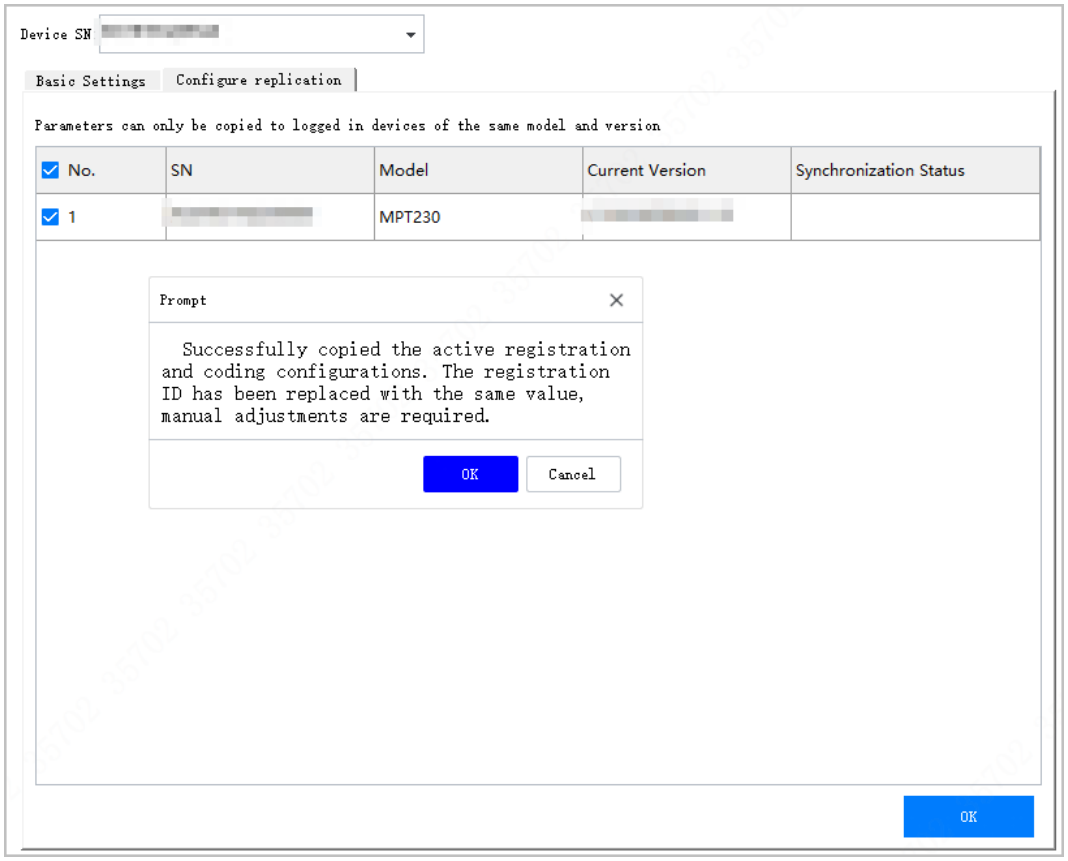
Procedimiento

Paso 1 Conecte al menos dos dispositivos MPT a la computadora y luego seleccione**Configuración**>**Configurar la replicación**para ingresar a la página de replicación.

Los parámetros solo se pueden copiar a dispositivos conectados del mismo modelo y versión.

Paso 2 Seleccione el dispositivo al que desea copiar información en la lista y haga clic**DE ACUERDO**en la ventana emergente.

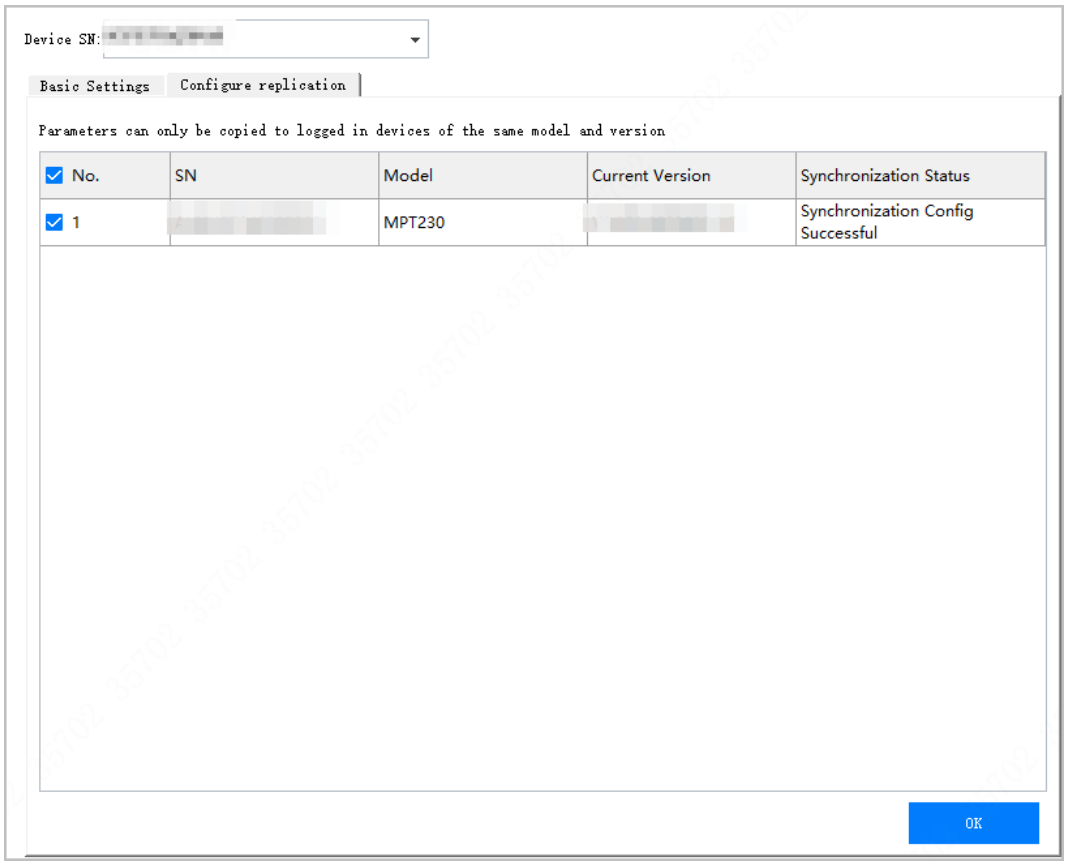
Figura 2-4 Replicar la configuración




Resultados

El estado de sincronización indica "**Configuración de sincronización exitosa**".

Figura 2-5 Mensaje de éxito

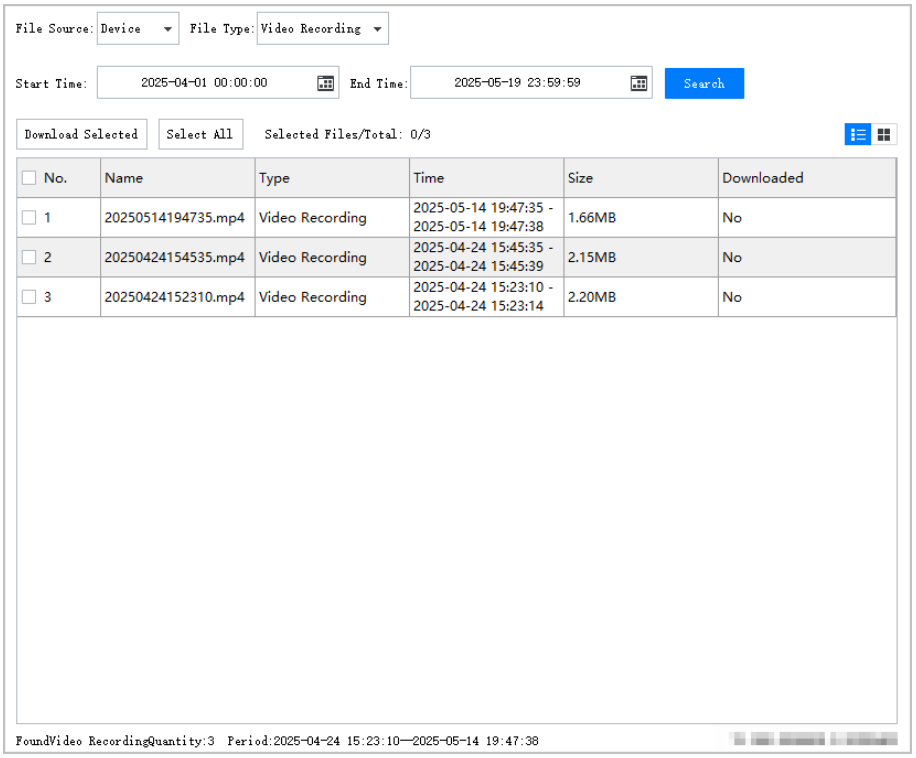


## Copia de seguridad de exportación de 3 archivos

Puede realizar una copia de seguridad de los archivos de los dispositivos conectados copiándolos o cortándolos.

1. Después de conectar el dispositivo a la computadora e iniciar sesión en el Administrador MPT, haga clic en**Archivo**.

Figura 3-1 Copia de seguridad de la exportación de archivos




2. Haga clic en la esquina superior derecha para configurar los ajustes de administración de almacenamiento y luego hacer clic**DE ACUERDO**.

Figura 3-2 Gestión de almacenamiento

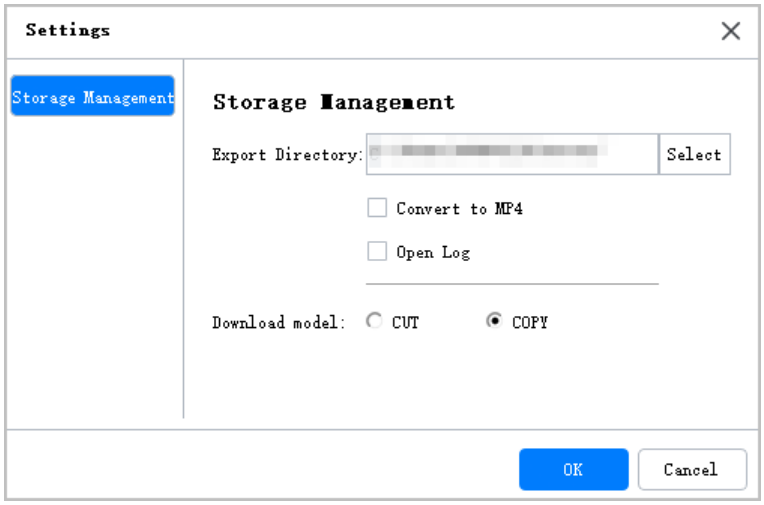


Tabla 3-1 Descripción de los parámetros de gestión de almacenamiento

| Parámetro | Descripción |
| --- | --- |
| Directorio de exportación | Seleccione la ubicación en su computadora donde desea realizar la copia de seguridad. |
| Convertir a MP4 | Si realiza una copia de seguridad de un vídeo, al seleccionar esta opción se convertirá automáticamente al formato MP4. |
| Abrir registro | Si lo selecciona, el proceso de copia de seguridad abrirá automáticamente los registros. |
| Descargar modelo | • **CORTAR**:El proceso de copia de seguridad eliminará los archivos del dispositivo automáticamente.<br>• **COPIAR**:El proceso de copia de seguridad no eliminará los archivos del dispositivo. |

3. Seleccione la fuente del archivo, el tipo de archivo, la hora de inicio y la hora de finalización y, a continuación, haga clic en**Buscar**.

4. Seleccione los archivos que desea respaldar y haga clic en**Descargar Seleccionado**para descargarlos en la computadora.

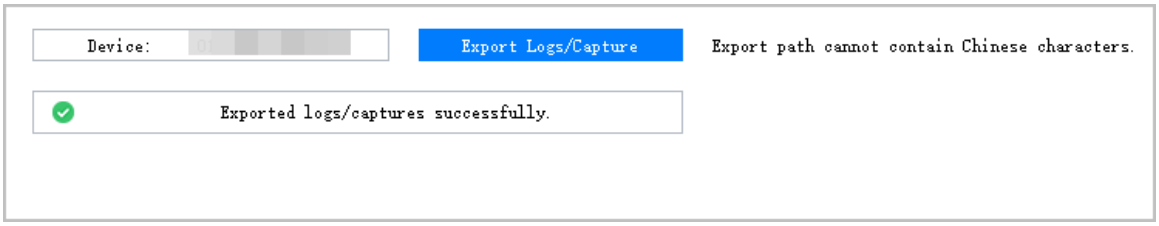
Hacer clic**Seleccionar todo**para seleccionar todos los archivos en el resultado de la búsqueda.

# 4 Exportación de registros y captura de paquetes

Puede exportar registros y realizar capturas de paquetes para el dispositivo.

1. Después de conectar el dispositivo a la computadora e iniciar sesión en el Administrador MPT, haga clic en**Registro**.

Figura 4-1 Exportación y captura de registros




2. Haga clic**Exportar registros/capturar**para iniciar el proceso.

Cuando este proceso sea exitoso, aparecerá un mensaje**Registros/capturas exportados exitosamente**.

# 5 Actualización del dispositivo

Puede actualizar el dispositivo a través de MPT Manager.

1. Después de conectar el dispositivo a la computadora e iniciar sesión en el Administrador MPT, haga clic en**Mejora**.
2. Haga clic**Mejora**para ingresar a la página de actualización y seleccionar el modo de actualización de la lista desplegable.

Figura 5-1 Actualización del dispositivo

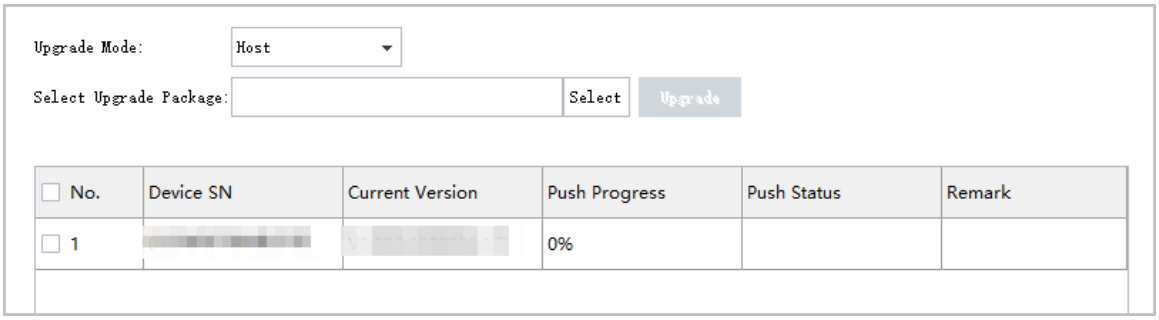
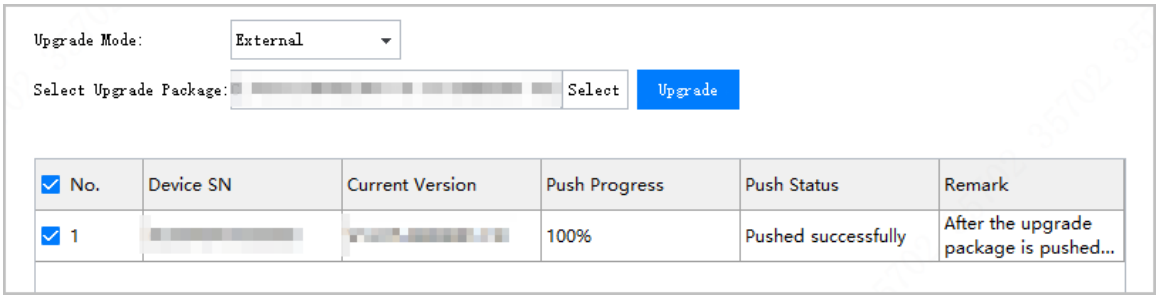



Figura 5-2 Estado de envío exitoso




3. Haga clic**Seleccionar**para seleccionar el paquete de actualización y hacer clic**Mejora**.
4. Seleccione el dispositivo y haga clic**Mejora**.

   El progreso de envío llega al 100% cuando el paquete de actualización se envía exitosamente al dispositivo.

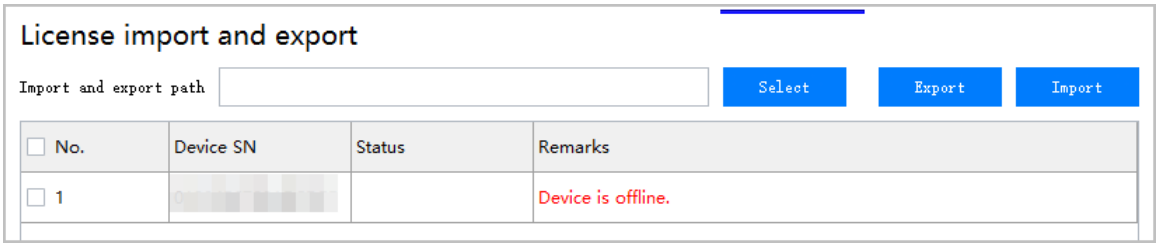
# 6 Licencia de Importación y Exportación

Puede importar y exportar la licencia del dispositivo.

1. Después de conectar el dispositivo a la computadora e iniciar sesión en el Administrador MPT, haga clic en**Licencia**.
2. Licencia de Importación y Exportación.

- Importar la licencia del dispositivo: Haga clic en**Seleccionar**Para seleccionar la ruta de importación de la licencia, haga clic en los dispositivos en los que desea realizar operaciones y, a continuación, haga clic en**Importar**.
- Exportar la licencia del dispositivo: Haga clic en**Seleccionar**Para seleccionar la ruta de exportación de la licencia, haga clic en los dispositivos en los que desea realizar operaciones y, a continuación, haga clic en**Exportar**.

Figura 6-1 Importación y exportación de licencias



# Apéndice 1 Recomendación de seguridad

## 1.Gestión de cuentas

a.**Utilice contraseñas seguras**

- 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 ni el nombre de la cuenta en orden inverso.
- No utilice caracteres continuos, como 123, abc, etc.
- No utilice caracteres superpuestos, como 111, aaa, etc.

b.**Cambiar la contraseña periódicamente**

Se recomienda cambiar las contraseñas periódicamente para reducir el riesgo de que sean adivinadas o descifradas.

do.**Asignar cuentas y permisos de manera razonable**

Según las necesidades del negocio y de gestión, agregue razonablemente nuevos usuarios y asígneles razonablemente un conjunto mínimo de permisos.

d.**Habilitar bloqueo de cuenta**

La función de bloqueo de cuenta está activada por defecto y se recomienda mantenerla 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.

mi.**Establecer y actualizar contraseñas Restablecer información oportunamente**

La plataforma admite la función de restablecimiento de contraseña. Para reducir el riesgo de ataques, configure la información necesaria para el restablecimiento de contraseña a tiempo. Si la información cambia, modifíquela a tiempo. Al configurar preguntas de protección de contraseña, se recomienda no usar preguntas fáciles de adivinar.

F.**Habilitar la vinculación de cuentas IP/MAC**

Se recomienda habilitar el mecanismo de vinculación de IP/MAC de cuentas para mejorar aún más la seguridad del acceso.

## 2.Configuración del servicio

a.**Habilitar HTTPS**

Se sugiere habilitar HTTPS, para poder visitar el servicio web a través de un canal de comunicación seguro.

b.**Desactivar servicios innecesarios y elegir modos seguros**

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

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

- SMTP: elija TLS para acceder al servidor de buzón.
- FTP: elija SFTP y configure contraseñas seguras.

## 3.Configuración de red

a.**Habilitar lista de permitidos del firewall**

Se recomienda habilitar la lista de permitidos 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 del equipo correspondiente a la lista de permitidos.

b.**Aislamiento de red**

La red debe aislarse mediante la partición de la red de videovigilancia y la red de la oficina en el conmutador y el enrutador en diferentes VLAN. Esto evita que los atacantes usen la red de la oficina para lanzar ataques de pivote en la red de videovigilancia.

4.**Auditoría de seguridad**

a.**Comprobar usuarios en línea**

Se recomienda verificar periódicamente a los usuarios en línea para identificar si hay usuarios ilegales que inician sesión.

b.**Ver el registro de la plataforma**

Al ver el registro, puede obtener la información de IP del intento de iniciar sesión en la plataforma y la información de operación clave del usuario que inició sesión.

## 5.**Protección física**

Se recomienda proteger físicamente el dispositivo que tenga instalada la plataforma. Por ejemplo, colóquelo en una sala de computadoras y un gabinete especiales, e implemente un control de acceso y una gestión de claves rigurosos para evitar que personal no autorizado realice contactos físicos, como dañar el hardware.

6.**Seguridad perimetral**

Se sugiere implementar productos de seguridad perimetral y tomar las medidas necesarias, como acceso autorizado, control de acceso y prevención de intrusiones para proteger la seguridad de la plataforma de software.