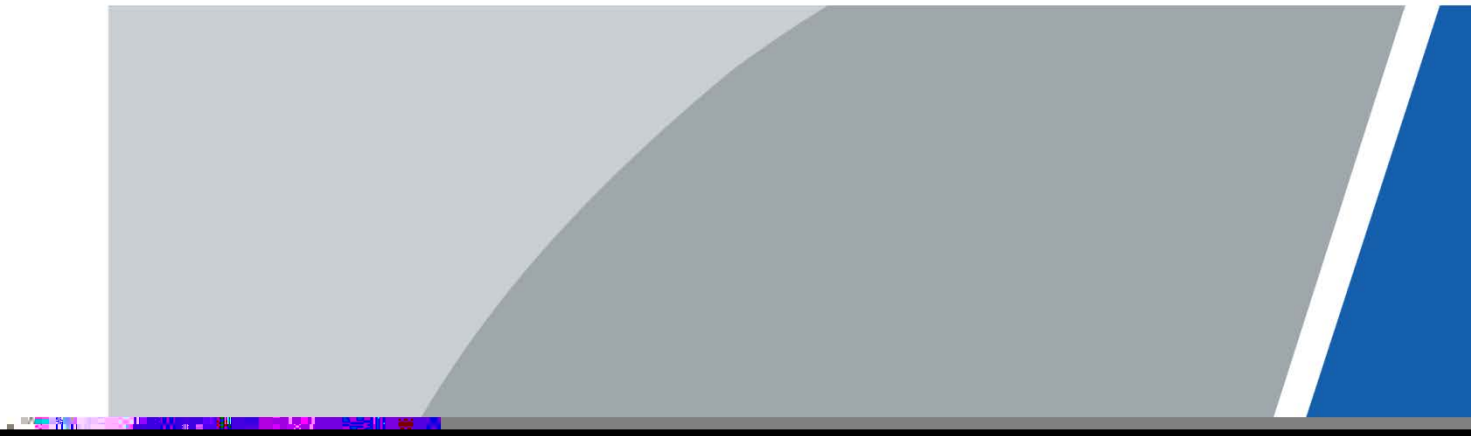
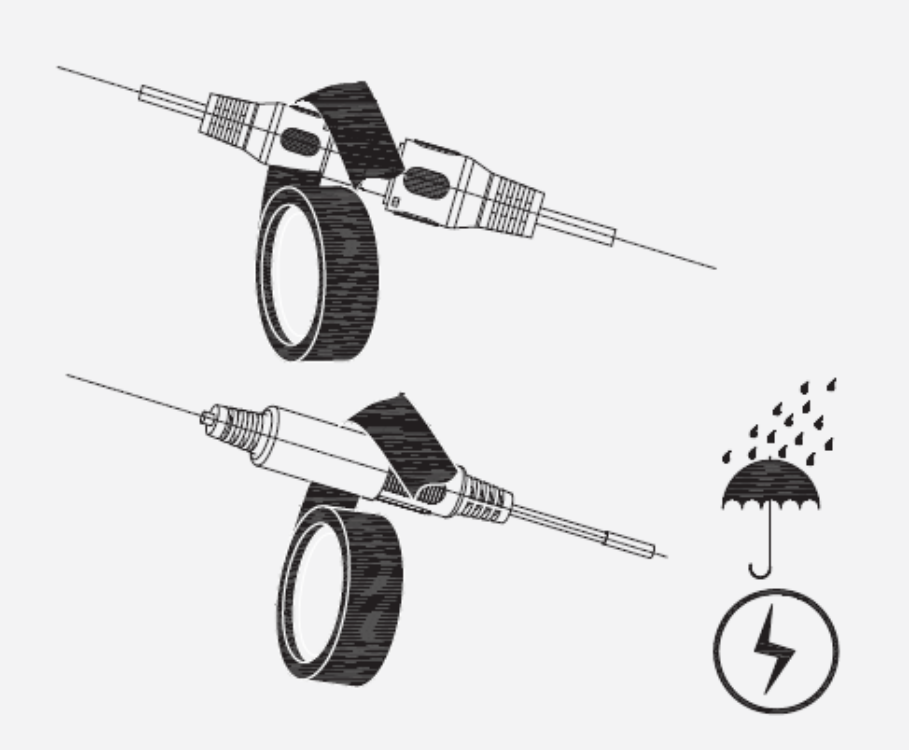
Cámara HDCVI

Manual del usuario





13 Mantenimiento

Para mantener la calidad de la imagen y el correcto funcionamiento del dispositivo, lea las

Siga cuidadosamente las instrucciones de mantenimiento y manténgalas estrictamente.

Desmontaje y sustitución del desecante

- Siga cuidadosamente las instrucciones del manual al realizar cualquier operación de desmontaje del dispositivo; de lo contrario, podría causar fugas de agua o mala calidad de imagen debido a un desmontaje no profesional.
- Comuníquese con el servicio posventa para reemplazar el desecante si encuentra niebla condensada en la lente después de desempacar o cuando el desecante se vuelve verde. (No todos los modelos incluyen el desecante).

Mantenimiento de la lente y del protector de la lente

- La lente y el protector de lente están cubiertos con un revestimiento antirreflejo, que podría contaminarse o dañarse y provocar rayones en la lente o imágenes borrosas al entrar en contacto con polvo, grasa, huellas dactilares y otras sustancias similares.
- No toque directamente el sensor de imagen (CCD o CMOS). El polvo y la suciedad se pueden eliminar con un soplador de aire o puede limpiar la lente con cuidado con un paño suave humedecido con alcohol.

Mantenimiento del cuerpo del dispositivo

- El cuerpo del dispositivo se puede limpiar con un paño suave y seco, que también se puede utilizar para eliminar manchas difíciles si se humedece con un detergente suave.
- Para evitar posibles daños en el revestimiento del cuerpo del dispositivo que podrían causar una disminución del rendimiento, no utilice solventes volátiles como alcohol, benceno, diluyentes, etc. para limpiar el cuerpo del dispositivo, ni tampoco se pueden utilizar detergentes fuertes y abrasivos.

Recomendación de seguridad

1. Gestión de cuentas

1.1Utilice contraseñas complejas

Consulte las siguientes sugerencias para establecer contraseñas:

- La longitud no debe ser inferior a 8 caracteres;
- Incluya al menos dos tipos de caracteres: 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 repetidos, como 111, aaa, etc.

1.2 Cambie las contraseñas periódicamente

Se recomienda cambiar periódicamente la contraseña del dispositivo para reducir el riesgo de que sea adivinada o descifrada.

1.3 Asignar cuentas y permisos de forma adecuada

Agregue usuarios de forma adecuada según los requisitos de servicio y administración y asigne conjuntos de permisos mínimos a los usuarios.

1.4 Habilitar la función de bloqueo de cuenta

La función de bloqueo de cuenta está habilitada de forma predeterminada. Se recomienda mantenerla habilitada para proteger la seguridad de la cuenta. Después de varios intentos fallidos de ingresar la contraseña, se bloquearán la cuenta correspondiente y la dirección IP de origen.

1.5 Establecer y actualizar la información de restablecimiento de contraseña de manera oportuna

Nuestro dispositivo admite la función de restablecimiento de contraseña. Para reducir el riesgo de que esta función sea utilizada por actores maliciosos, si hay algún cambio en la información, modifíquela a tiempo. Al configurar las preguntas de seguridad, se recomienda no utilizar respuestas fáciles de adivinar.

2. Configuración del servicio

2.1. Habilitar HTTPS

Se recomienda que habilite HTTPS para acceder a servicios web a través de canales seguros.

2.2 Transmisión cifrada de audio y vídeo

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

2.3 Desactiva los servicios no esenciales y utiliza el modo seguro

Si no es necesario, se recomienda desactivar algunos servicios como SSH, SNMP, SMTP, UPnP, AP hotspot, etc., para reducir las superficies de ataque.

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

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

2.4 Cambiar HTTP y otros puertos de servicio predeterminados

Se recomienda cambiar el puerto predeterminado de HTTP y otros servicios a cualquier puerto entre 1024 y 65535 para reducir el riesgo de ser adivinado por actores de amenazas.

3. Configuración de red

3.1 Habilitar lista de permitidos

Se recomienda activar la función de lista de permitidos y permitir que solo las direcciones IP de la lista de permitidos accedan al dispositivo. Por lo tanto, asegúrese de agregar la dirección IP de su computadora y la dirección IP del dispositivo compatible a la lista de permitidos.

3.2 Vinculación de direcciones MAC

Se recomienda vincular la dirección IP de la puerta de enlace a la dirección MAC del dispositivo para reducir el riesgo de suplantación de ARP.

3.3. Construir un entorno de red seguro

Para garantizar mejor la seguridad de los dispositivos y reducir los posibles riesgos cibernéticos, se recomienda lo siguiente:

- Deshabilite la función de mapeo de puertos del enrutador para evitar el acceso directo a los dispositivos de intranet desde la red externa.
- De acuerdo con las necesidades reales de la red, particione la red: si no hay demanda de comunicación entre las dos subredes, se recomienda utilizar VLAN, puerta de enlace y otros métodos para particionar la red para lograr el aislamiento de la red.
- Establecer un sistema de autenticación de acceso 802.1x para reducir el riesgo de acceso ilegal a terminales de la red privada.

4. Auditoría de seguridad

4.1 Verificar usuarios en línea

Se recomienda revisar periódicamente a los usuarios en línea para identificar usuarios ilegales.

4.2 Verificar el registro del dispositivo

Al ver los registros, puede obtener información sobre las direcciones IP que intentan iniciar sesión en el dispositivo y las operaciones clave de los usuarios registrados.

4.3 Configurar el registro de red

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

5. Seguridad del software

5.1 Actualizar el firmware a tiempo

De acuerdo con las especificaciones operativas estándar de la industria, el firmware de los dispositivos debe actualizarse a la última versión a tiempo para garantizar que el dispositivo tenga las últimas funciones y seguridad. Si el dispositivo está conectado a la red pública, se recomienda habilitar la función de detección automática de actualizaciones en línea, para obtener la información de actualización de firmware publicada por el fabricante de manera oportuna.

5.2 Actualizar el software del cliente a tiempo

Se recomienda descargar y utilizar el software de cliente más reciente.

6. Protección física

Se recomienda realizar protección física para los dispositivos (especialmente los dispositivos de almacenamiento), como colocar el dispositivo en una sala de máquinas y un gabinete dedicados, y tener control de acceso y administración de claves para evitar que personal no autorizado dañe el hardware y otros equipos periféricos (por ejemplo, disco flash USB, puerto serial).