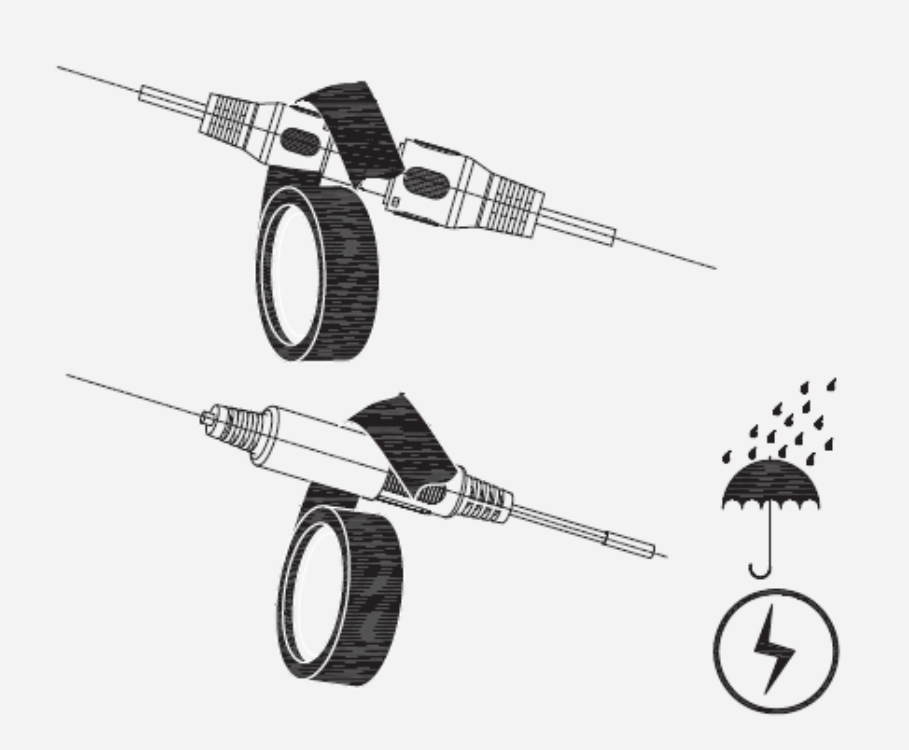
Cámara HDCVI

Manual de usuario

Medidas impermeables



13 Mantenimiento

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

Siga cuidadosamente las instrucciones de mantenimiento y mantenga una estricta adherencia.

Desmontaje y reemplazo del desecante

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

Mantenimiento de la lente y el protector de la lente

- La lente y el protector de la lente están cubiertos con una capa antirreflectante, que podría contaminarse o dañarse y provocar rayones en la lente o imágenes borrosas al tocarlas con polvo, grasa, huellas dactilares y otras sustancias similares.
- No toque el sensor de imagen (CCD o CMOS) directamente. El polvo y la suciedad se pueden eliminar con un soplador de aire o puede limpiar la lente suavemente 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 humedecido con un detergente suave.
- Para evitar posibles daños en el revestimiento del cuerpo del dispositivo que podrían causar una disminución del rendimiento, no utilice disolventes volátiles como alcohol, benceno, diluyentes, etc. para limpiar el cuerpo del dispositivo, ni tampoco se puede utilizar detergente abrasivo fuerte.

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;
- Incluir al menos dos tipos de caracteres: letras mayúsculas y minúsculas, números y símbolos; No
- contener 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 Cambiar contraseñas periódicamente

Se recomienda cambiar periódicamente la contraseña del dispositivo para reducir el riesgo de que la adivinen o la descifren.

1.3 Asignar cuentas y permisos adecuadamente

Agregue usuarios adecuadamente 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 mantenerlo habilitado para proteger la seguridad de la cuenta. Después de varios intentos fallidos de contraseña, la cuenta correspondiente y la dirección IP de origen se bloquearán.

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 de amenazas, si hay algún cambio en la información, modifíquela a tiempo. Al establecer preguntas de seguridad, se recomienda no utilizar respuestas fáciles de adivinar.

2. Configuración del servicio

2.1. Habilitar HTTPS

Se recomienda habilitar 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 cifrada para reducir el riesgo de que sus datos de audio y video sean interceptados durante la transmisión.

2.3 Desactivar servicios no esenciales y utilizar el modo seguro

Si no es necesario, se recomienda desactivar algunos servicios como SSH, SNMP, SMTP, UPnP, punto de acceso AP, 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 buzones.
- 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 que los actores de amenazas lo adivinen.

3. Configuración de red

3.1 Habilitar lista de permitidos

Se recomienda activar la función de lista de permitidos y solo permitir que IP en la lista de permitidos acceda 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 Enlace de dirección 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. Construya 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 asignación de puertos del enrutador para evitar el acceso directo a los dispositivos de la intranet desde la red externa.
- De acuerdo con las necesidades reales de la red, divida 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 y lograr el aislamiento de la red.
- Establecer un sistema de autenticación de acceso 802.1x para reducir el riesgo de acceso ilegal del terminal a la red privada.

4. Auditoría de seguridad

4.1 Verificar usuarios en línea

Se recomienda comprobar periódicamente a los usuarios en línea para identificar a los 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 mucho tiempo, se recomienda habilitar la función de registro de red para garantizar que los registros críticos estén sincronizados con el servidor de registro de red para su 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 actualización en línea, para obtener la información de actualización del 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 llevar a cabo 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 serie).