Cámara ANPR inteligente

Manual de usuario

V1.0.0

Prefacio

General

El manual presenta la estructura e instalación de la cámara inteligente con acceso automático.
reconocimiento de matrículas (en adelante "la cámara").

Instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

Palabras de advertencia	Significado
DANGER	Indica un alto riesgo potencial que, si no se evita, provocará la muerte o lesiones graves.
CAUTION	Indica un riesgo potencial que, si no se evita, podría provocar daños a la propiedad, pérdida de datos, reducciones en el rendimiento o resultados impredecibles.
TIPS	Proporciona métodos para ayudarle a resolver un problema o ahorrar tiempo.
NOTE	Proporciona información adicional como complemento al texto.

Revisión histórica

Contenido de revisión	Tiempo de liberación	Contenido de revisión
V1.0.0	Primer lanzamiento.	octubre 2022

Aviso de protección de privacidad

Como usuario del dispositivo o controlador de datos, puede recopilar datos personales de otras personas, como su rostro, huellas dactilares y número de matrícula. Debe cumplir con las leyes y regulaciones locales de protección de la privacidad para proteger los derechos e intereses legítimos de otras personas mediante la implementación de medidas que incluyen, entre otras: Proporcionar una identificación clara y visible para informar a las personas sobre la existencia del área de vigilancia y proporcionar la información de contacto requerida.

Acerca del Manual

- El manual es sólo para referencia. Pueden encontrarse ligeras diferencias entre el manual y el producto.
- No somos responsables de las pérdidas incurridas debido a la operación del producto de maneras que no sean las cumplimiento del manual.
- El manual se actualizará de acuerdo con las últimas leyes y regulaciones de las jurisdicciones relacionadas. Para obtener información detallada, consulte el manual del usuario en papel, utilice nuestro CD-ROM, escanee el código QR o visite nuestro sitio web oficial. El manual es sólo para referencia. Es posible que se encuentren ligeras diferencias entre la versión electrónica y la versión en papel.
- Todos los diseños y software están sujetos a cambios sin previo aviso por escrito. Actualizaciones de Producto Podría dar lugar a que aparezcan algunas diferencias entre el producto real y el manual. Comuníquese con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria.
- Puede haber errores en la impresión o desviaciones en la descripción de las funciones, operaciones y datos técnicos. Si hay alguna duda o disputa, nos reservamos el derecho de dar una explicación final.
- Actualice el software del lector o pruebe otro software de lectura convencional si el manual (en PDF)

formato) no se puede abrir.

- Todas las marcas comerciales, marcas comerciales registradas y nombres de empresas que aparecen en el manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, comuníquese con el proveedor o con el servicio de atención al cliente si ocurre algún problema mientras utilizando el dispositivo.
- Si existe alguna incertidumbre o controversia, nos reservamos el derecho de dar una explicación final.

Salvaguardias y advertencias importantes

Esta sección presenta contenido que cubre el manejo adecuado del dispositivo, la prevención de riesgos y la prevención de daños a la propiedad. Lea atentamente antes de usar el dispositivo, cumpla con las pautas al usarlo y guarde el manual en un lugar seguro para consultarlo en el futuro.

Requisitos de transporte

Transporte el dispositivo en las condiciones permitidas de humedad y temperatura.

Requisitos de almacenamiento

Guarde el dispositivo en condiciones permitidas de humedad y temperatura.

requerimientos de instalación

- No conecte el adaptador de corriente al dispositivo mientras el adaptador esté encendido.
- Cumpla estrictamente con el código y las normas locales de seguridad eléctrica. Asegúrese de que el voltaje ambiental es estable y cumple con los requisitos de suministro de energía del dispositivo.
- No conecte el dispositivo a dos o más tipos de fuentes de alimentación para evitar daños al dispositivo.

- El personal que trabaja en alturas debe tomar todas las medidas necesarias para garantizar la seguridad personal, incluido el uso de casco y cinturones de seguridad.
- No coloque el dispositivo en un lugar expuesto a la luz solar o cerca de fuentes de calor.
- Mantenga el dispositivo alejado de la humedad, el polvo y el hollín.
- Coloque el dispositivo en un lugar bien ventilado y no bloquee su ventilación.
- Utilice un adaptador o fuente de alimentación del gabinete proporcionado por el fabricante.
- La fuente de alimentación debe cumplir con los requisitos de ES1 en el estándar IEC 62368-1 y no ser más alto que PS2. Tenga en cuenta que los requisitos de suministro de energía están sujetos a la etiqueta del dispositivo.
- El aparato es un aparato eléctrico de clase I. Asegúrese de que la fuente de alimentación del dispositivo esté conectado a una toma de corriente con protección a tierra.
- Se debe instalar un dispositivo de desconexión de emergencia durante la instalación y el cableado en un lugar fácilmente lugar accesible para cortes de energía de emergencia.
- Desconecte el dispositivo al instalar y conectar la lente.

Requisitos de operación

- Asegúrese de que la fuente de alimentación sea la correcta antes de su uso.
- No desenchufe el cable de alimentación en el costado del dispositivo mientras el adaptador esté encendido.
- Opere el dispositivo dentro del rango nominal de entrada y salida de energía.
- Utilice el dispositivo en condiciones permitidas de humedad y temperatura.
- No deje caer ni salpique líquido sobre el dispositivo y asegúrese de que no haya ningún objeto lleno de

líquido en el dispositivo para evitar que fluya líquido hacia él.

- No desmonte el dispositivo.
- No apunte el dispositivo hacia fuentes de luz intensa (como la luz de una lámpara y la luz del sol) cuando lo enfoque.
- No vibre, apriete ni sumerja el dispositivo en líquido durante el transporte, almacenamiento o instalación.
- No bloquee la ventilación cerca del dispositivo.
- Le recomendamos utilizar el dispositivo con un dispositivo de protección contra rayos para obtener una mayor protección contra los rayos. Para escenarios al aire libre, cumpla estrictamente con las normas de protección contra rayos.
- Conecte a tierra la parte de conexión a tierra funcional del dispositivo (cable de conexión a tierra o protector contra sobretensiones). para mejorar su confiabilidad. El dispositivo es un aparato eléctrico de clase I. Asegúrese de que la fuente de alimentación del dispositivo esté conectada a una toma de corriente con conexión a tierra de protección.
- El dispositivo debe usarse con la cubierta protectora para escenarios al aire libre para evitar el riesgo de daños por agua al dispositivo.
- Proteja el cable de línea y los cables para que no se pisen ni se aprieten, especialmente en los enchufes, tomas y el punto por donde salen del dispositivo.
- Modifique la contraseña predeterminada del dispositivo después de iniciar sesión por primera vez para evitar que el dispositivo sea robado.

Requisitos de mantenimiento

- Empaquetar el dispositivo con embalaje proporcionado por su fabricante o embalaje de la misma calidad. antes de devolverlo para su reparación.
- No toque el dispositivo fotosensible con las manos. Utilice un soplador de aire para limpiar el polvo y suciedad en la lente.
- Limpie la superficie del dispositivo con un paño suave y seco o un paño suave y limpio humedecido en agua neutra. detergente.
- Utilice los accesorios sugeridos por el fabricante. La instalación y el mantenimiento deben ser realizados por profesionales calificados.

Tabla de contenido

1. Introducción

1.1 Descripción general

La cámara adopta un algoritmo inteligente de aprendizaje profundo. Admite detección de vehículos, reconocimiento de matrículas, reconocimiento de logotipos, reconocimiento de modelos y reconocimiento de colores, y modos de codificación como como H.265.

La cámara consta de una carcasa protectora, un iluminador y una cámara HD inteligente. La cámara HD inteligente adopta CMOS de escaneo progresivo, que posee varias características como alta definición, baja iluminancia, alta velocidad de fotogramas y excelente reproducción del color.

La cámara se aplica ampliamente a la captura de vehículos y al reconocimiento de carreteras comunitarias, estacionamientos y otras vigilancias de entradas y salidas.

1.2 Características

Las funciones están disponibles en modos seleccionados y pueden diferir de la cámara real.

Gestión de permisos

- Cada grupo de usuarios posee permisos. Los permisos de un usuario no pueden exceder los permisos de su grupo.
- 2 niveles de usuario.
- Permiso de apertura de barrera y función de alarma de lista de bloqueo.
- Configuración de dispositivos y gestión de permisos a través de Ethernet.

Almacenamiento

- Almacena los datos de vídeo correspondientes en el servidor central según la configuración (como alarma y ajustes de sincronización).
- Los usuarios pueden grabar a través de la web según sus requisitos. El archivo de vídeo grabado será almacenado en la computadora donde se encuentra el cliente.
- Admite el intercambio en caliente local de la tarjeta de almacenamiento y el almacenamiento cuando se desconecta la red. Sobrescribe automáticamente las imágenes y los vídeos almacenados cuando la memoria se vuelve insuficiente.
- Almacena 1024 registros y control de permisos de usuario.
- Admite almacenamiento FTP y reabastecimiento automático de red (ANR).

Alarma

- Puede activar una alarma ante excepciones en el funcionamiento de la cámara a través de la red, como la tarjeta de memoria. daño.
- Algunos dispositivos pueden conectarse a varios periféricos de alarma para responder a una entrada de alarma externa en tiempo real (dentro de 200 ms). Puede manejar correctamente varias alarmas según el enlace predefinido por los usuarios y generar el mensaje de voz correspondiente (los usuarios pueden grabar la voz con anticipación).

Monitoreo de red

- Transmite datos de video de un solo canal comprimidos por el dispositivo al terminal de red y los hace reaparecer después de la descompresión a través de la red. Mantenga el retraso dentro de los 500 ms cuando se permita el ancho de banda.
- Admite un máximo de 10 usuarios en línea al mismo tiempo.
- Admite acceso al sistema y administración de dispositivos a través de la web.
- La transmisión de datos de vídeo adopta HTTP, TCP, UDP, MULTICAST y RTP/RTCP.

Captura y reconocimiento

- Reconocimiento de matrícula y otra información del vehículo, incluido el color, logotipo, modelo, y otras características del vehículo.
- Admite configurar información OSD y configurar la ubicación del canal y la imagen.
- Admite captura y codificación de imágenes. Admite el cifrado de marcas de agua de imágenes para evitar imágenes de ser manipuladas.
- Las imágenes capturadas pueden registrar automáticamente la hora, ubicación, matrícula, color del vehículo, y más.

Control periférico

- Control de periféricos: admite la configuración de varios protocolos de control de periféricos y páginas de conexión.
- Se conecta a dispositivos externos como detectores de vehículos, detectores de señales y más.

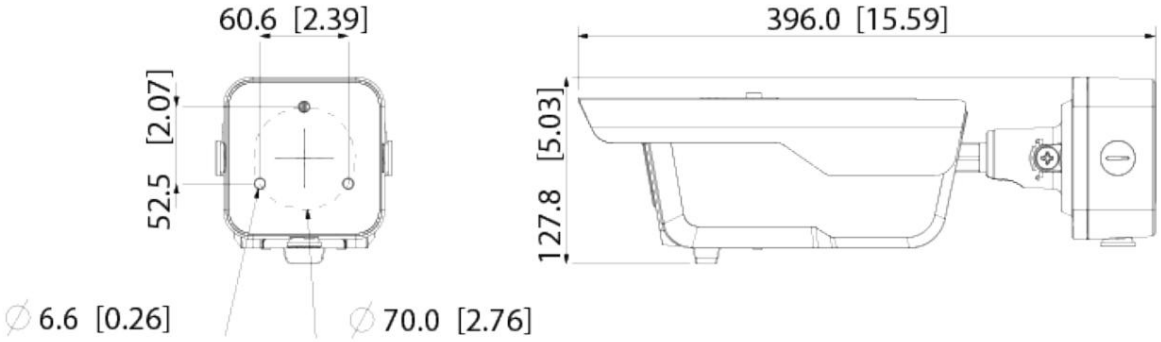
Ajuste automático

- Iris automático: ajusta automáticamente la apertura del iris a los cambios de luz a lo largo del día.
- Balance de blancos automático: muestra con precisión el color del objeto cuando cambian las condiciones de luz.
- Exposición automática: ajusta automáticamente la velocidad de obturación según el valor de exposición de la imagen medido por el sistema de medición y según la exposición del obturador y del iris configurada en los valores predeterminados de fábrica.
- Ganancia automática: aumenta automáticamente la sensibilidad de la cámara cuando la iluminancia es muy baja, mejorando Salida de señal de imagen para que la cámara pueda adquirir una imagen clara y brillante.

2 Estructura

2.1 Dimensiones

Figura 2-1 Dimensiones (mm [pulgadas])



2.2 Dispositivo completo

Figura 2-2 Estructura completa del dispositivo

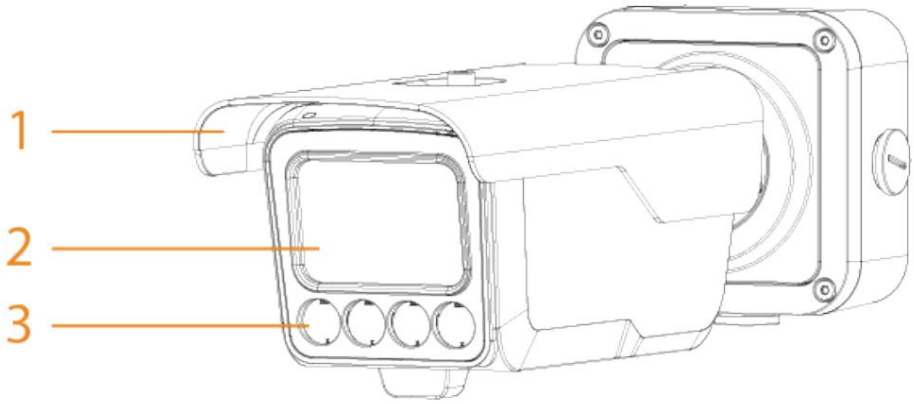


Tabla 2-1 Descripción de la estructura

No.	Descripción	No.	Descripción
1	Cubierta protectora	3	Iluminador
2	Lente	—	

2.3 Panel trasero

Figura 2-3 Estructura del panel inferior

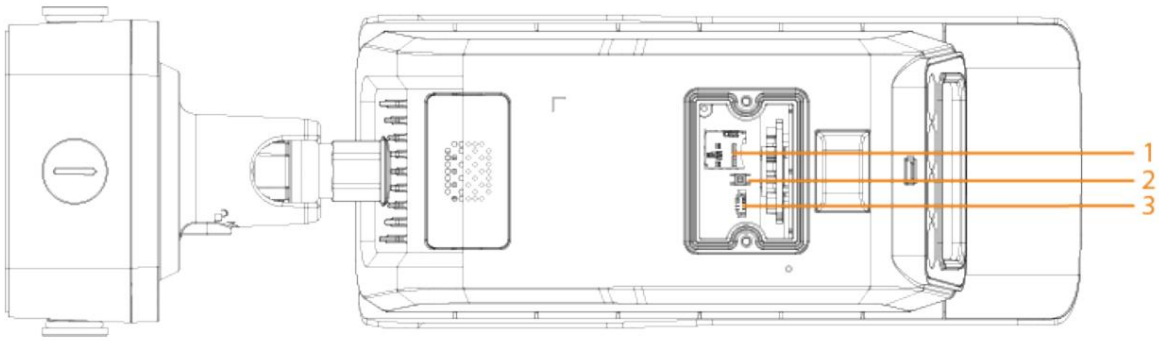


Tabla 2-2 Descripción del panel inferior

No.	Descripción	No.	Descripción
1	Ranura para una tarjeta SD	3	Puerto de depuración
2	Restablecimiento de hardware	—	

2.4 cables

Figura 2-4 Cables

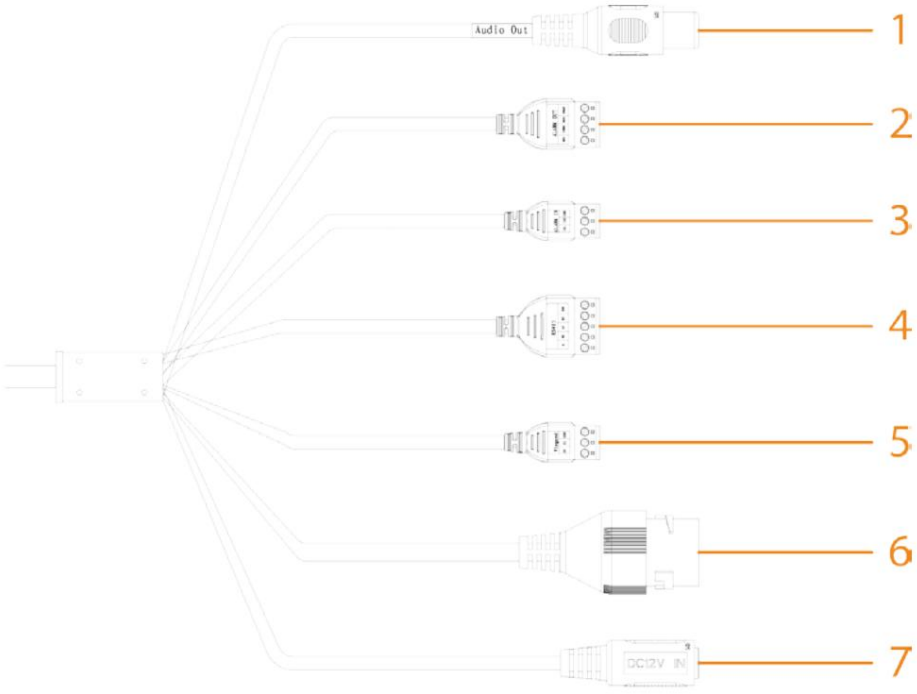


Tabla 2-3 Descripción del cable

No.	Función	Descripción
1	SALIDA DE AUDIO	La cámara envía una señal de audio a través de este puerto.
2	alarma	Salida de alarma, conexión a barrera y dispositivos de salida de alarma como luz de alarma.
3	Alarma en	Entrada de alarma, conexión a detector de vehículos, detector de infrarrojos, bucle de inducción y más.

No.	Función	Descripción
4	RS-485	Se conecta a pantallas y otros dispositivos externos.
5	Wiegand	Conecta y envía matrículas al controlador de acceso.
6	Y	Se conecta a una red. También admite fuente de alimentación PoE.
7	12 VCC	Se conecta a una fuente de alimentación de 12 VCC. ⚠ Se producirán daños en el dispositivo si la alimentación no se suministra correctamente.

3 Instalación

Las siguientes figuras de instalación son solo como referencia y pueden diferir del producto real.

3.1 Montaje en poste

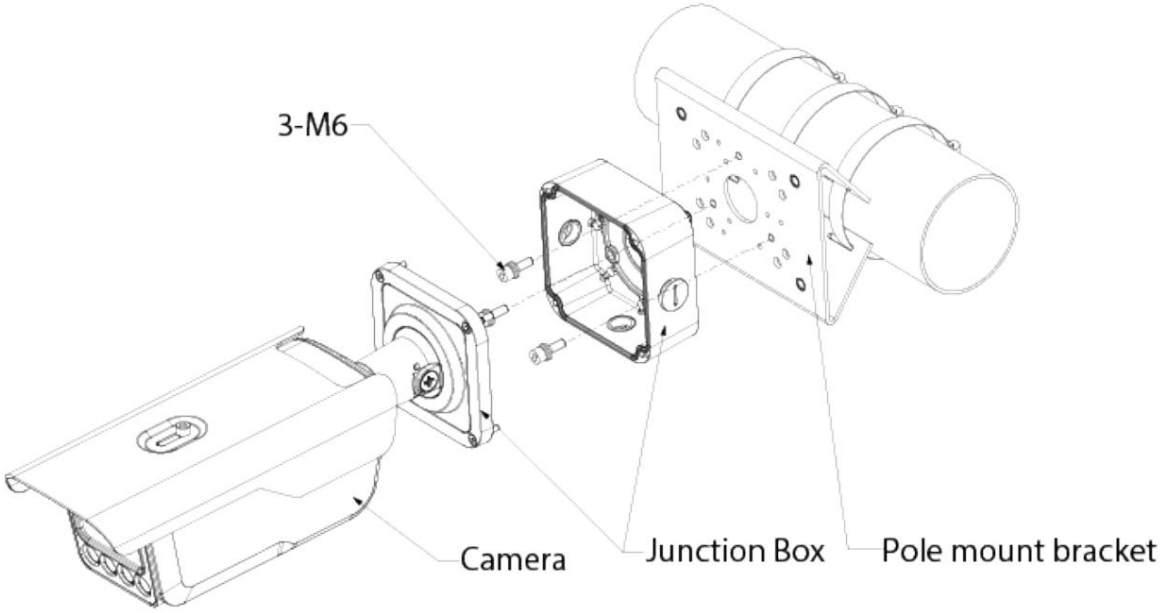
Procedimiento

Paso 1 Fije el soporte de montaje en poste al poste.

Paso 2 Utilice 3 tornillos M6 para fijar la caja de conexiones al soporte de montaje en poste.

Paso 3 Apriete los tornillos en el extremo de la cámara para fijarla a la caja de conexiones.

Figura 3-1 Montaje en poste



3.2 Montaje en pared

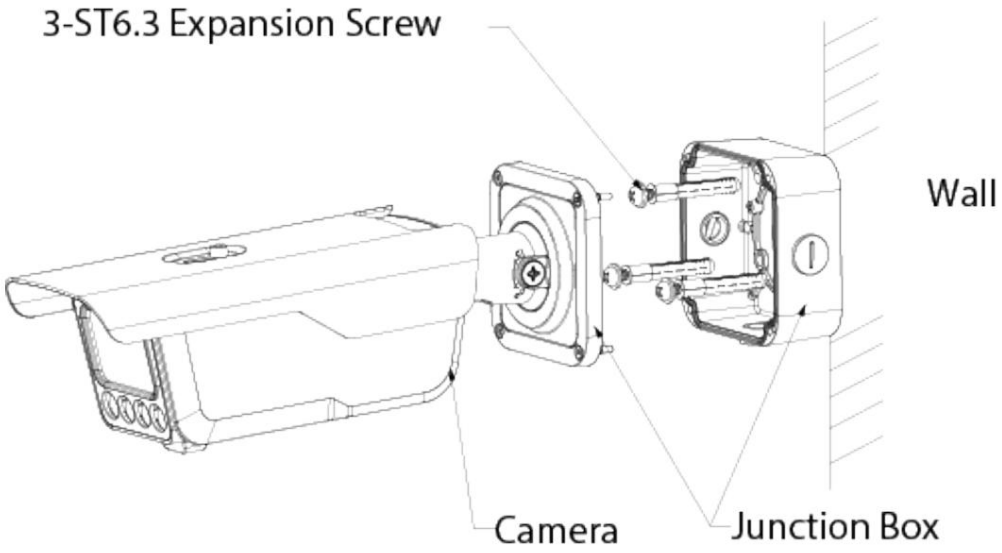
Procedimiento

Paso 1 Taladre agujeros en la pared de acuerdo con los agujeros de la caja de conexiones.

Paso 2 Utilice 3 tornillos de expansión ST6.3 para fijar la caja de conexiones a la pared.

Paso 3 Apriete los tornillos en el extremo de la cámara para fijarla a la caja de conexiones.

Figura 3-2 Montaje en pared



3.3 Montaje en techo

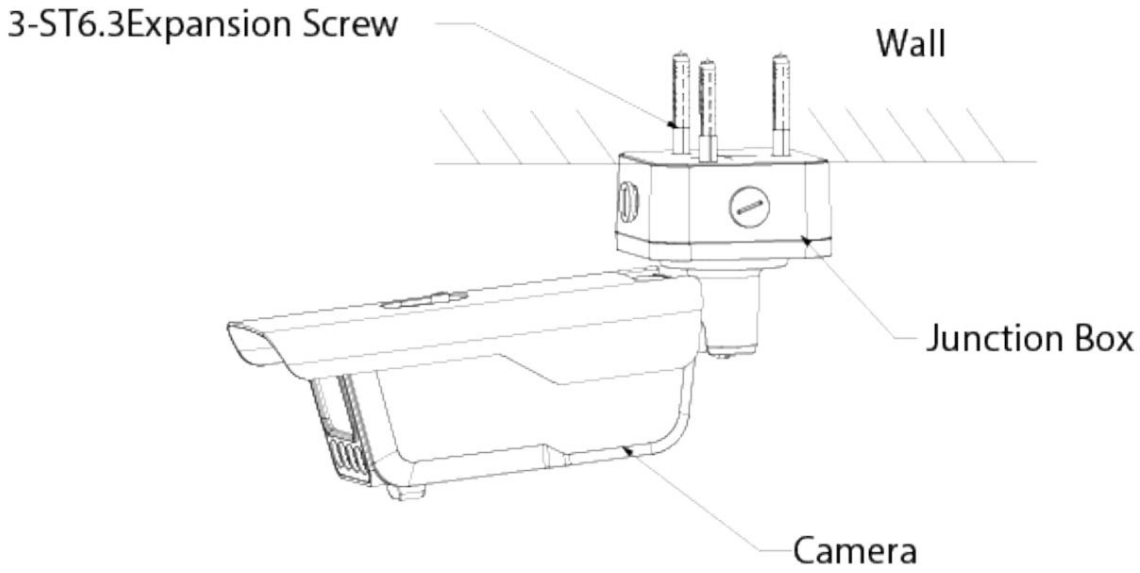
Procedimiento

Paso 1 Taladre agujeros en el techo de acuerdo con los agujeros de la caja de conexiones.

Paso 2 Utilice 3 tornillos de expansión ST6.3 para fijar la caja de conexiones al techo.

Paso 3 Apriete los tornillos en el extremo de la cámara para fijarla a la caja de conexiones.

Figura 3-3 Montaje en techo



Apéndice 1 Recomendaciones de ciberseguridad

Acciones obligatorias que se deben tomar para la seguridad básica de la red de dispositivos:

1. Utilice contraseñas seguras

Consulte las siguientes sugerencias para establecer contraseñas:

- La longitud no debe ser inferior a 8 caracteres.
- Incluir al menos dos tipos de personajes; Los tipos de caracteres incluyen letras mayúsculas y minúsculas, números y símbolos.
- No incluya 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.

2. Actualice el firmware y el software cliente a tiempo

- De acuerdo con el procedimiento estándar en la industria tecnológica, recomendamos mantener su dispositivo (como NVR, DVR, cámara IP, etc.) firmware actualizado 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 "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 "es bueno tener" para mejorar la seguridad de la red de su dispositivo:

1. Protección física

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

2. Cambie las contraseñas con regularidad

Le sugerimos que cambie las contraseñas con regularidad para reducir el riesgo de que las adivinen o las descifren.

3. Establecer y actualizar contraseñas Restablecer información oportuna

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 sobre protección de contraseña. Si la información cambia, modifíquela a tiempo. Al configurar preguntas de protección con contraseña, se sugiere no utilizar aquellas que puedan adivinarse fácilmente.

4. Habilite el bloqueo de cuenta

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

5. Cambie HTTP predeterminado y otros puertos de servicio

Le sugerimos que cambie 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. Habilite HTTPS

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

7. Vinculación de direcciones MAC

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

8. Asigne cuentas y privilegios de manera razonable

De acuerdo con los requisitos comerciales y de administración, agregue usuarios de manera razonable y asigne un

conjunto mínimo de permisos para ellos.

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 riesgos.

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

- SNMP: elija SNMP v3 y configure autenticación y contraseñas de cifrado seguras.
  contraseñas.
- SMTP: elija TLS para acceder al servidor de buzones de correo.
- FTP: elija SFTP y configure contraseñas seguras. • Punto de

acceso AP: elija el modo de cifrado WPA2-PSK y configure contraseñas seguras.

10. Transmisión cifrada de audio y vídeo

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

Recordatorio: la transmisión cifrada provocará cierta pérdida en la eficiencia de la transmisión.

11. Auditoría segura

- Verificar a los usuarios en línea: le sugerimos que verifique a los usuarios en línea con regularidad para ver si el dispositivo está
  iniciado sesión sin autorización.
- Verificar el registro del dispositivo: al ver los registros, puede conocer las direcciones IP que se utilizaron 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 un período prolongado, 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.

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 asignación de puertos del enrutador para evitar el acceso directo a los dispositivos de la intranet.
  desde la red externa.
- La red debe dividirse y aislarse según las necesidades reales de la red. Si
  No existen requisitos de comunicación entre dos subredes, se sugiere utilizar VLAN, Network GAP y otras tecnologías para dividir la red, a fin de lograr el efecto de aislamiento de la red.

- Establecer 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 a los que se les permite acceder al
  dispositivo.