Videoportero para Villas (VTO) (VTO2111DPS2)

Guía de inicio rápido

V1.0.0

Prólogo

General

Este manual presenta la estructura y la configuración básica del videoportero (VTO).

Instrucciones de seguridad

En el manual pueden aparecer las siguientes palabras de señalización clasificadas con significado definido.

Palabras de señalización	Significado
 **ADVERTENCIA**	Indica un riesgo de potencial medio o bajo que, de no evitarse, podría ocasionar lesiones leves o moderadas.
 **PRECAUCIÓN**	Indica un riesgo potencial que, de no evitarse, podría ocasionar daños en la propiedad, pérdida de datos, bajo rendimiento u otro resultado impredecible.
 **NOTA**	Proporciona información adicional como énfasis o complemento al texto.

Historial de revisión

Versión	Contenido de la revisión	Fecha de lanzamiento
V1.0.0	Primera edición	Marzo de 2020

Acerca del manual

- El manual es solo una referencia. Si detecta alguna discrepancia entre el manual y el producto real, el producto real prevalecerá.
- No aceptaremos ninguna responsabilidad por las pérdidas producidas por el uso del dispositivo sin seguir las indicaciones del manual.
- El manual debería ser actualizado de acuerdo con las últimas leyes y normas de las regiones relacionadas. Para ver más información, consulte el manual impreso, el CD-ROM, el código QR o nuestra página web oficial. En caso de existir una discrepancia entre el manual impreso y la versión electrónica, prevalecerá la versión electrónica.
- Todos los diseños y el software aquí incluidos están sujetos a cambios sin aviso previo por escrito. Las actualizaciones del producto podrían ocasionar discrepancias entre el producto real y el manual. Contacte con el servicio de atención al cliente solicitando el programa actualizado y la documentación suplementaria.
- Aun así podría haber alguna desviación en los datos técnicos, funciones y descripción de las operaciones, o errores de impresión. En caso de duda o disputa, consulte nuestra explicación final.
- Actualice el software del lector o intente con otro software lector convencional en el caso de que no pueda abrir el manual (en formato PDF).

- Todas las marcas comerciales, marcas comerciales registradas y nombres de empresas en el manual pertenecen a sus respectivos propietarios.
- Visite nuestra página web, contacte con su vendedor o con el servicio de atención al cliente si tiene problemas al usar el dispositivo.
- Si hubiera incertidumbres o controversias, consulte nuestra explicación final.

Advertencias y precauciones de seguridad importantes

La siguiente descripción es el método de aplicación correcto del dispositivo. Lea detenidamente el manual antes de usarlo para evitar los peligros y la pérdida de propiedad. Cumpla estrictamente con el manual durante la aplicación y guárdelo correctamente después de leerlo.

Requisitos de funcionamiento

- No coloque ni instale el dispositivo en un lugar expuesto a la luz directa del sol o cerca de otro dispositivo que genere calor.
- No instale el dispositivo en una zona húmeda, polvorienta o muy oscura.
- Mantenga su instalación horizontal o instálela en lugares estables y evite que se caiga.
- No vierta ni salpique líquidos sobre el dispositivo, ni coloque encima ningún objeto lleno de líquido, con el objeto de evitar que los líquidos penetren en el dispositivo.
- Instale el dispositivo en un lugar bien ventilado y no bloquee sus ranuras de ventilación.
- Use el dispositivo únicamente dentro del rango de voltaje nominal, tanto de entrada como de salida.
- No desmonte el dispositivo arbitrariamente.
- Transporte, utilice y guarde el dispositivo conforme a los límites permitidos de humedad y temperatura.

Requisitos de alimentación

- El producto utiliza los cables eléctricos (cables de alimentación) homologados para la región en la que se usará el dispositivo.
- Utilice una fuente de alimentación que cumpla con los requisitos SELV (baja tensión de seguridad) y suministre la alimentación eléctrica con una tensión nominal que se ajuste a la fuente de alimentación limitada de la norma IEC60950-1. Para conocer los requisitos específicos de la fuente de alimentación, consulte las etiquetas del dispositivo.
- El acoplador del aparato es un dispositivo de desconexión. Durante el uso normal, mantenga un ángulo que facilite su funcionamiento.

Índice de contenidos

1 Introducción

Después de abrir y desembalar la caja, compruebe que el videoportero no presenta daños y que están todos los accesorios (videoportero, guía de inicio rápido y paquete de tornillería).

Figura 1-1 Apariencia

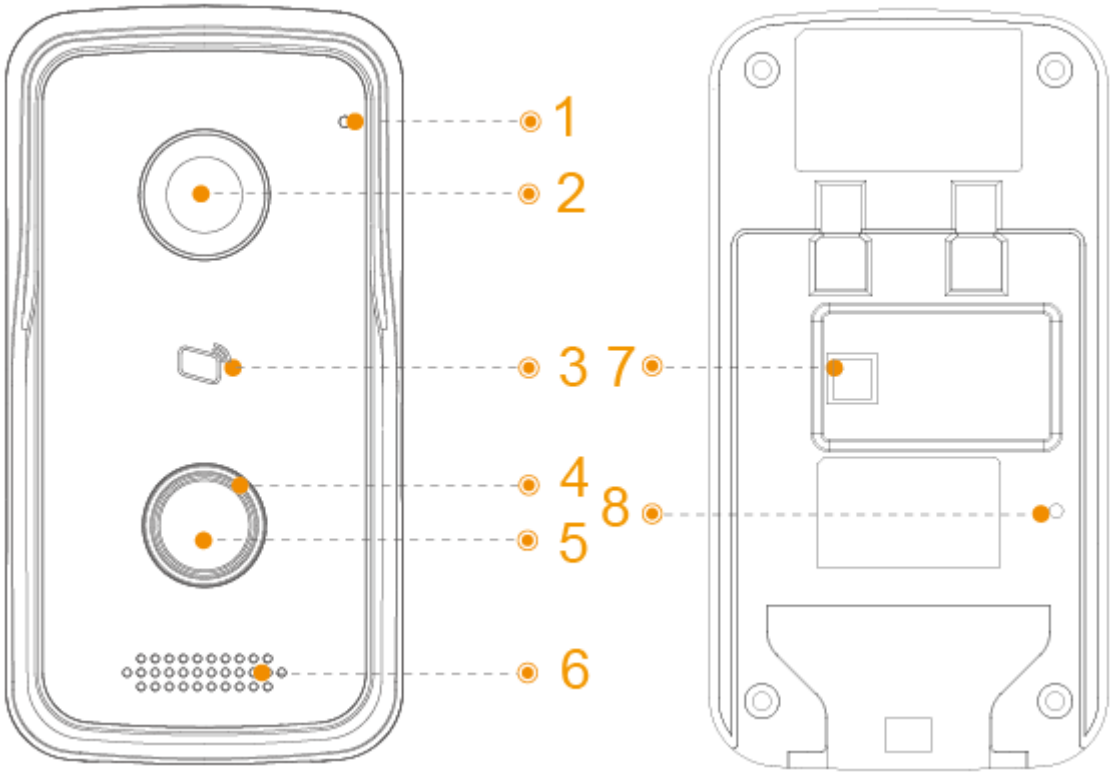

Tabla 1-1Descripción de los puertos

Núm.	Nombre	Núm.	Nombre
1	Micrófono	5	Botón de llamada
2	Cámara	6	Altavoz
3	Lector de tarjetas de acceso	7	Interruptor anti-sabotaje
4	Luz indicadora	8	Restablecer

2 Instalación de la aplicación y dispositivo de adición

Escanee el siguiente código QR para descargar e instalar la aplicación.

Figure 2-1

Antes de agregar el videoportero (VTO) al gDMSS Plus, debe modificar la dirección IP del videoportero (VTO), asegurarse de que el videoportero(VTO) y el router estén conectados a la misma red, y conectar el videoportero (VTO) a la fuente de alimentación.

En su móvil toque ,y, a continuación, siga las instrucciones en pantalla hasta que aparezca la interfaz de selección de región.

Seleccione una región.

Toque Listo en la esquina superior derecha de la interfaz.

Aparecerá la interfaz En directo.

Directo

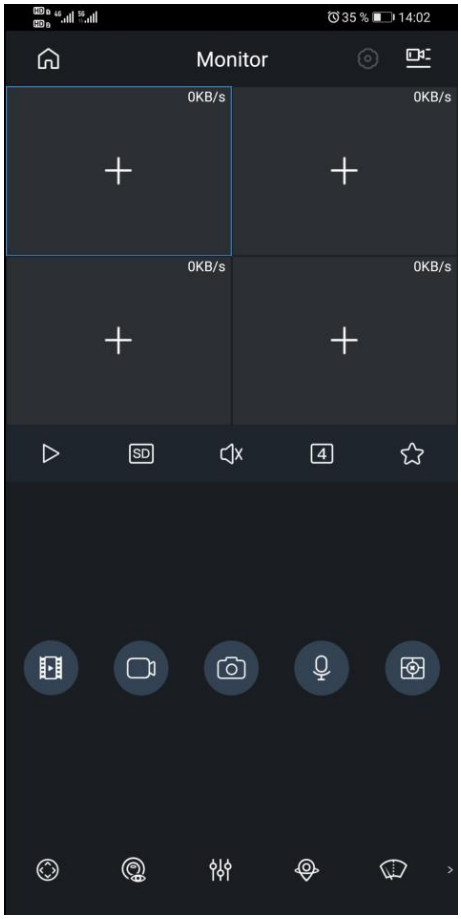

Figure 2-2

Toque en la esquina superior izquierda de la interfaz En directo.

Aparecerá la interfaz Hogar.

Hogar

Figure 2-3

Toque en la interfaz Hogar.

Aparecerá la interfaz del Administrador de dispositivos.

Toque en la esquina superior izquierda de la interfaz Administrador de dispositivos.

Administrador de dispositivos

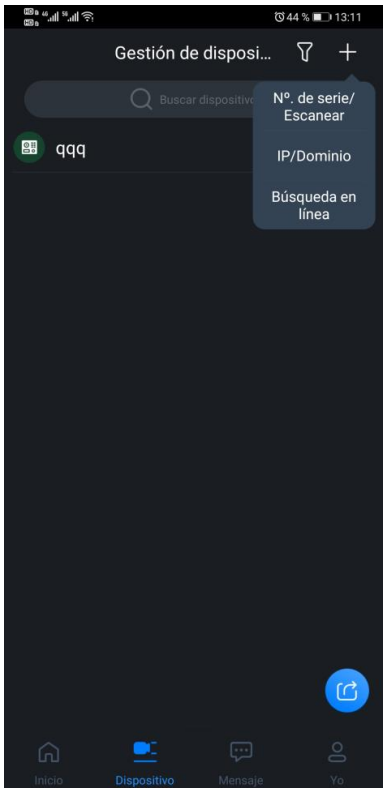

Figure 2-4

Añadir a través de una red por cable

Toque IP/Dominio.

Aparecerá la interfaz para añadir dispositivos.

Añadir dispositivo

Figure 2-5

Toque VTO en la interfaz Agregar dispositivo.

Aparecerá la interfaz para añadir dispositivos.

Añadir dispositivo

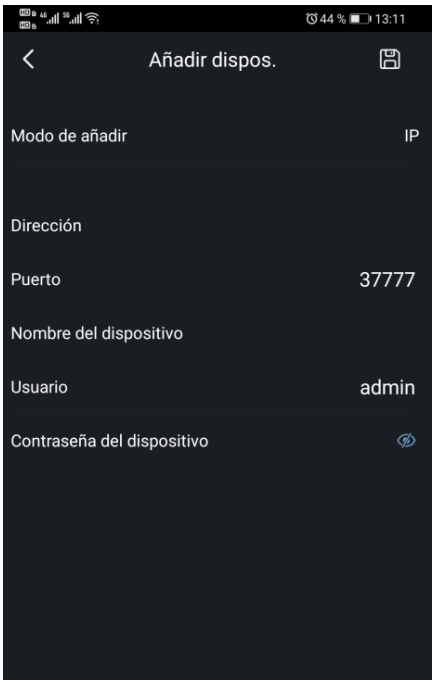

Figure 2-6

Introduzca la dirección (dirección IP del videoportero (VTO)), nombre del dispositivo y contraseña del dispositivo.

Pulse en .

Se ha añadido el videoportero (VTO). Puede ver vídeos grabados por el videoportero (VTO), llamar al videoportero (VTO), desbloquear puertas cuando hay una llamada desde el videoportero (VTO) y mucho más.

Puerta

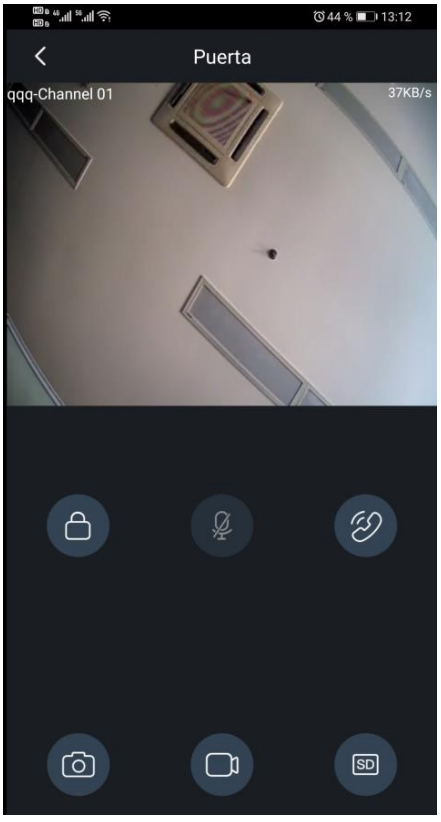

Figure 2-7

Appendix 1 Preguntas frecuentes

1. **El dispositivo no funciona con normalidad.**
   Reinicie el dispositivo con los parámetros de fábrica y vuélvalos a configurar.
2. **¿Cómo reinicio el dispositivo con los parámetros de fábrica?**
   Mantenga pulsado el botón restablecer durante 10 s.
3. **El dispositivo no está conectado.**
   Si la luz indicadora permanece parpadeando en azul, quiere decir que el dispositivo no está en línea. Compruebe la conexión de red. Si la conexión de red es normal, reinicie el dispositivo con los parámetros de fábrica y vuélvalos a configurar.

Appendix 2 Recomendaciones de 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 conectados a la 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.

Medidas obligatorias que debe tomar para la seguridad de la red del equipo básico:

1. **Usar contraseñas seguras**

   Consulte las siguientes sugerencias para establecer contraseñas:

   - La longitud no puede ser inferior a 8 caracteres;
   - Incluya al menos dos tipos de caracteres: letras mayúsculas y minúsculas, números y símbolos;
   - No utilice el nombre de la cuenta o el nombre de la cuenta al revés;
   - No utilice caracteres continuos, como 123, abc, etc.;
   - No utilice caracteres repetidos continuos, como 111, aaa, etc.;

2. **Actualizar el firmware y el software cliente puntualmente**

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

Medidas recomendadas para mejorar la seguridad de la red de su equipo:

1. **Protección física**

   Le sugerimos que proteja físicamente su equipo, especialmente los dispositivos de almacenamiento. Por ejemplo, coloque el equipo en una sala y armario especiales para ordenadores e implemente un correcto permiso de control de acceso y una administración de claves para evitar que el personal no autorizado pueda acceder físicamente al equipo y dañar el hardware, conectarse sin autorización a equipos extraíbles (como un disco flash USB, un puerto serie), etc.

2. **Cambiar contraseñas periódicamente**

   Le sugerimos que cambie las contraseñas periódicamente para reducir el riesgo de que puedan adivinarse o descifrarse.

3. **Establecer y actualizar puntualmente la información de restablecimiento de contraseñas**

   El equipo admite la función de restablecimiento de contraseña. Configure la información relacionada para restablecer la contraseña puntualmente, incluyendo las preguntas de protección de contraseña y la dirección electrónica del usuario final. Si la información cambia, modifíquela inmediatamente. Al establecer las preguntas de protección de la contraseña, le sugerimos que no utilice las que se puedan adivinar fácilmente.

4. **Habilitar bloqueo de cuenta**

   La función de bloqueo de cuenta está habilitada de manera predeterminada, y le recomendamos que la mantenga 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.

5. **Cambiar HTTP y otros puertos de servicio predeterminados**

   Le sugerimos que cambie el HTTP y otros puertos de servicio predeterminados a cualquier serie de números entre 1024 y 65535, reduciendo el riesgo de que personas externas 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. **Habilitar lista blanca**

   Le sugerimos que habilite la función de lista blanca para evitar que todos, salvo aquellos con direcciones IP especificadas, puedan acceder al sistema. Por lo tanto, asegúrese de agregar la dirección IP de su ordenador y la dirección IP del equipo acompañante a la lista blanca.

8. **Enlace de dirección MAC**

   Le recomendamos que enlace la dirección IP y MAC de la puerta de enlace al equipo, reduciendo el riesgo de redireccionamiento de ARP.

9. **Asignar cuentas y privilegios razonablemente**

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

10. **Inhabilitar servicios innecesarios y elegir modos seguros**

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

    Si son necesarios, se recomienda encarecidamente que utilice modos seguros, incluyendo, entre otros, los siguientes servicios:

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

11. **Transmisión cifrada de audio y vídeo**

    Si su contenido de datos de audio y vídeo es muy importante o sensible, le recomendamos que utilice la función de transmisión cifrada para reducir el riesgo de robo de datos de audio y vídeo durante la transmisión.

    Recuerde: la transmisión cifrada causará alguna pérdida en la eficiencia de la transmisión.

12. **Auditoría segura**

    - Comprobar usuarios en línea: le sugerimos que compruebe los usuarios en línea periódicamente para ver si alguien se ha conectado al dispositivo sin autorización.
    - Verificar registro del equipo: Al consultar los registros, puede conocer las direcciones IP que se han utilizado para iniciar sesión en sus dispositivos y sus operaciones clave.

13. **Registro de red**

Debido a la capacidad de almacenamiento limitada del equipo, el registro almacenado es limitado. Si necesita guardar el registro durante mucho tiempo, le recomendamos que habilite la función de registro de red para asegurarse de que los registros importantes estén sincronizados con el servidor de registro de red para su seguimiento.

14. Crear un entorno de red seguro

Para garantizar mejor la seguridad de los equipos y reducir los posibles riesgos cibernéticos, le recomendamos:

- Inhabilitar la función de asignación de puertos del enrutador para evitar el acceso directo a los dispositivos de la Intranet desde una red externa.
- Particionar y aislar la red según las necesidades reales de la red. Si no hay requisitos de comunicación entre dos subredes, le sugerimos que utilice VLAN, GAP de red y otras tecnologías para particionar 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 las redes privadas.
- Es recomendable tener activado el cortafuegos de su dispositivo o las funciones de lista negra y lista blanca (no autorizados/autorizados) para reducir el riesgo de que su dispositivo pueda ser atacado.