Videoportero (Versión 4.5)

Guía de inicio rápido

V1.0.0

Prólogo

General

Este manual presenta la estructura, el proceso de montaje y la configuración básica del videoportero (en adelante «VTO»).

Instrucciones de seguridad

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

Palabras de señalización	Significado
PELIGRO	Indica un riesgo altamente potencial que, de no evitarse, provocará lesiones graves o incluso la muerte.
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.
CONSEJOS	Proporciona métodos para ayudarle a solucionar un problema o ahorrar tiempo.
NOTA	Proporciona información adicional como énfasis o complemento al texto.

Historial de revisión

Versión	Contenido de la revisión	Fecha de lanzamiento
V1.0.0	Primer lanzamiento.	Diciembre 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 existe alguna incertidumbre o duda, 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 exponga el dispositivo a la luz solar directa ni a fuentes de calor.
- No instale el dispositivo en una zona húmeda o polvorienta.
- Instale el dispositivo de forma horizontal en lugares estables y evite que se caiga.
- No salpique ni deje gotear líquidos sobre el dispositivo; no coloque sobre el dispositivo nada que contenga líquidos.
- Instale el dispositivo en un lugar bien ventilado y no bloquee su ventilación.
- Use el dispositivo únicamente dentro del rango de voltaje nominal, tanto de entrada como de salida.
- No desmonte el dispositivo usted mismo.
- Transporte, utilice y guarde el dispositivo conforme a los límites permitidos de humedad y temperatura.

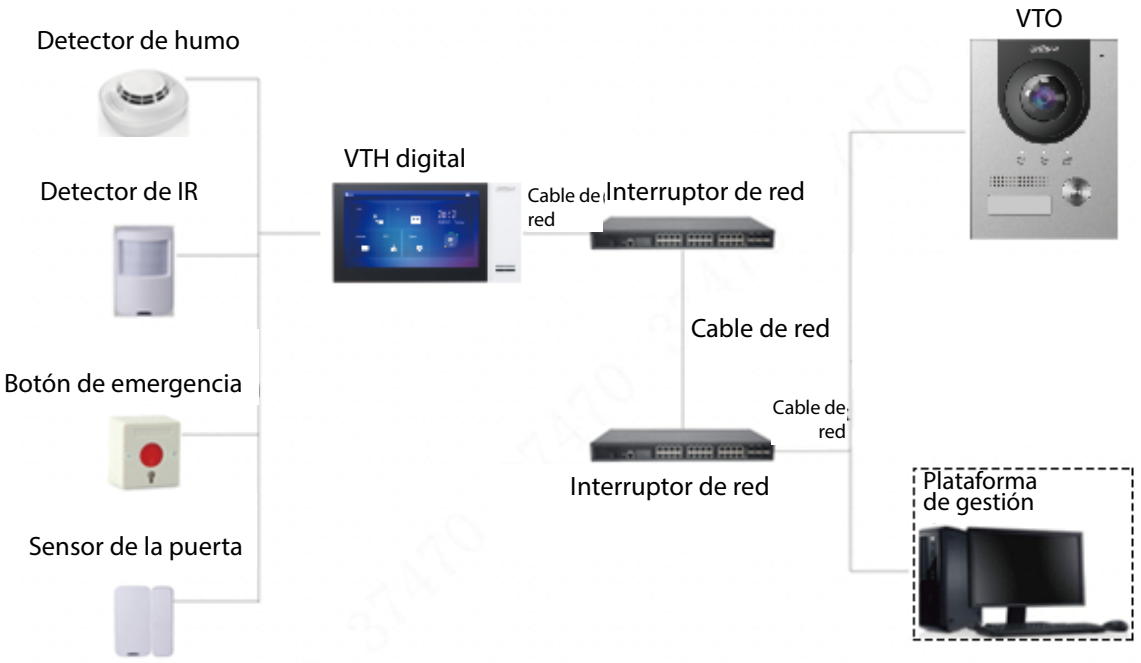
Requisitos de alimentación

- El producto debe utilizar cableado eléctrico que cumpla los requisitos locales.
- Utilice una fuente de alimentación que cumpla con ES1 pero que no exceda los límites de PS2 establecidos en IEC 62368-1. 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 Diagrama de red

Figura 1-1 Diagrama de red



En determinadas aplicaciones, como la casa, el/la Centro/Plataforma de gestión suele ser innecesario/a.

2 Apariencia

2.1 VTO2101E-P

2.1.1 Panel frontal

Figura 2-1 VTO2101E-P

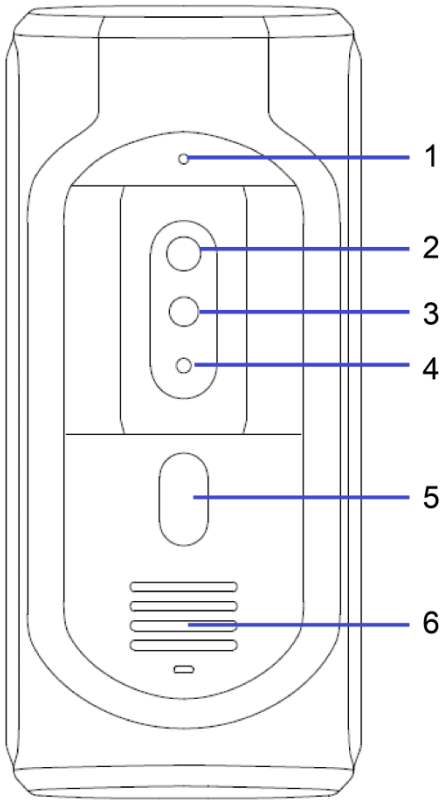


Tabla 2-1 Descripción del panel frontal

Núm.	Nombre	Descripción
1	Micrófono	—
2	Cámara	—
3	Luz de iluminación IR	Proporciona luz IR adicional a la cámara cuando está oscuro.
4	Sensor de luz	Detecta condiciones de iluminación ambiental.
5	Botón de llamada	Llame a los monitores internos (VTH) o al centro de gestión.
6	Altavoz	—

2.1.2 Panel trasero

Figura 2-2 VTO2101E-P

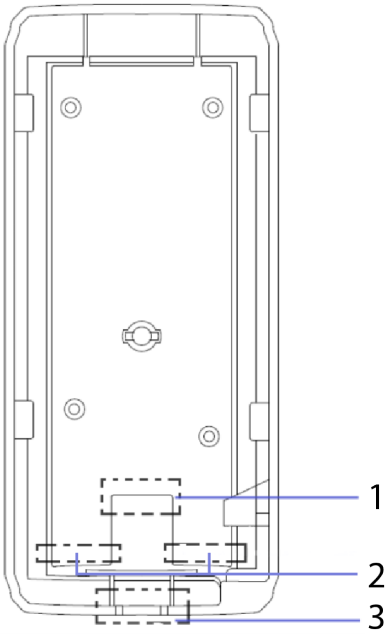
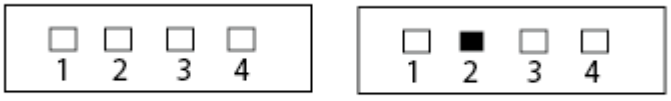


Tabla 2-2 Descripción del panel trasero

Núm.	Nombre	Descripción
1	Puerto de red	Se conecta al cable de red.
2	Puertos RS-485	Consulte la figura y la tabla siguientes.
3	Salida del cableado	Coloque el cableado aquí.

Figura 2-3 Conexión del cable



Puerta ENCENDIDO/485

Tabla 2-3 Descripción del puerto

PUERTA		ENCENDIDO/485	
Núm.	**Nombre**	**Núm.**	**Nombre**
1	NO	1	+12 V
2	NC	2	GND
3	COM	3	RS-485A
4	ENTRADA DE ALARMA o Desbloquear (predeterminado)	4	RS-485B

2.2 VTO2202F-P-S2/VTO2202F-P/VTO2202F/VTO2201F-P

2.2.1 Panel frontal

Figura 2-4 Panel frontal

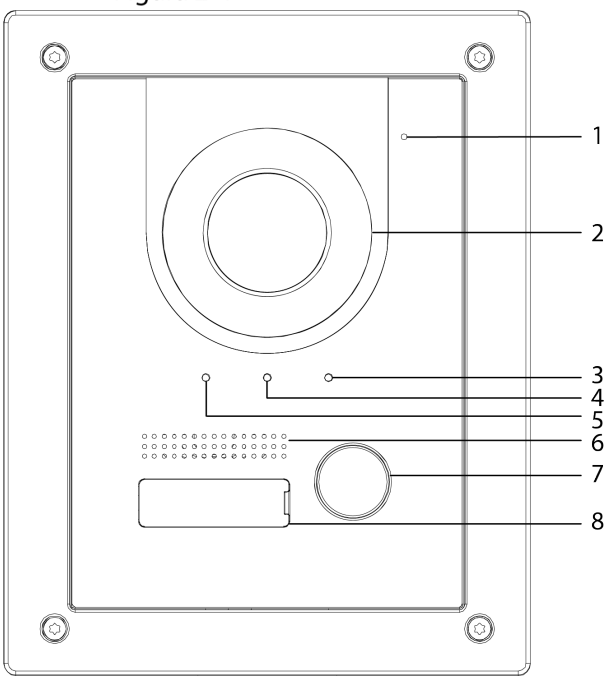


Tabla 2-4 Descripción del panel frontal

Núm.	Nombre	Descripción
1	Micrófono	—
2	Cámara	—
3	Indicador	Encendido: Puerta bloqueada.
4		Encendido: En una llamada.
5		Encendido: Llamando.
6	Altavoz	—
7	Botón de llamada	Llame a los monitores internos (VTH) o al centro de gestión.
8	Etiqueta de nombre	Nombre del host.

2.2.2 Panel trasero

Figura 2-5 Panel trasero

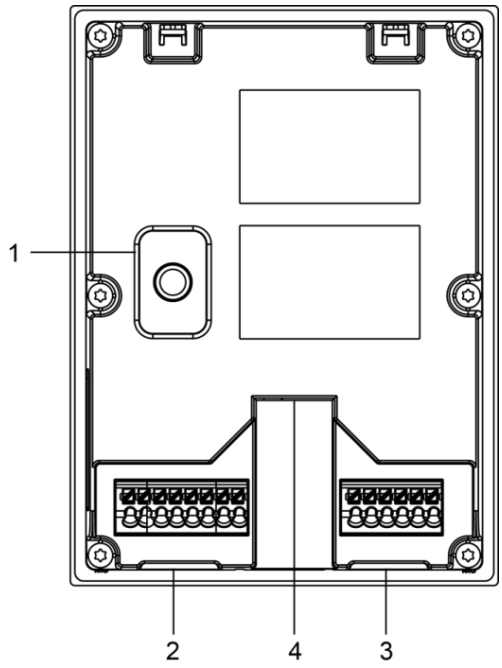


Tabla 2-5 Descripción del panel trasero

NA	Nombre	Descripción
1	Interruptor contra manipulaciones	Cuando el VTO se retira de la pared por medio de la fuerza, se activará una alarma y la información de la misma se enviará al centro de gestión.
2	Puerto	De izquierda a derecha: GND +12V_OUT RS485_B RS485_A ALARM_NO ALARM_COM VTO2202F-P-S2: 2-hilos + (48V); VTO2202F-P y VTO2202F: EOC1 (+12V); VTO2201F: + 24V. VTO2202F-P-S2: 2-hilos - (GND); VTO2202F-P y VTO2202F: EOC2 (GND); VTO2201F: GND.
3		De izquierda a derecha: DOOR_BUTTON DOOR_FB GND DOOR_NC DOOR_COM DOOR_NO
4	Puerto Ethernet	Se conecta a la red con el cable Ethernet. Solo los modelos con «P» admiten PoE.

2.3 VTO2111D-P-S2/VTO1101D-P

2.3.1 Panel frontal

Figura 2-6 Panel frontal

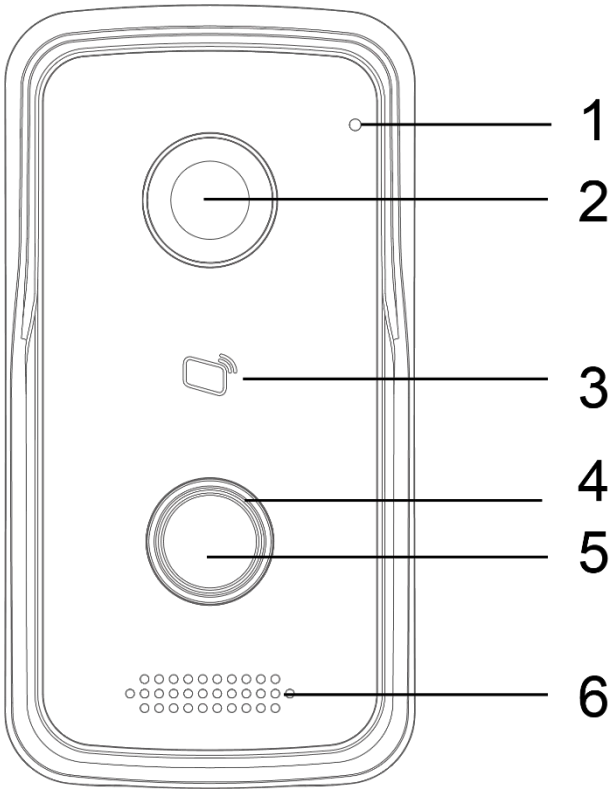


Tabla 2-6 Descripción del panel frontal

Núm.	Nombre	Descripción
1	Micrófono	—
2	Cámara	—
3	Área de lectura de tarjetas	Deslizar para desbloquear o emitir la tarjeta.
4	Indicador	• Azul fijo: modo de espera. • Parpadeo de color azul: llamando o sin red.
5	Botón de llamada	Llame a los monitores internos (VTH) o al centro de gestión.
6	Altavoz	—

2.3.2 Panel trasero

Figura 2-7 Panel trasero

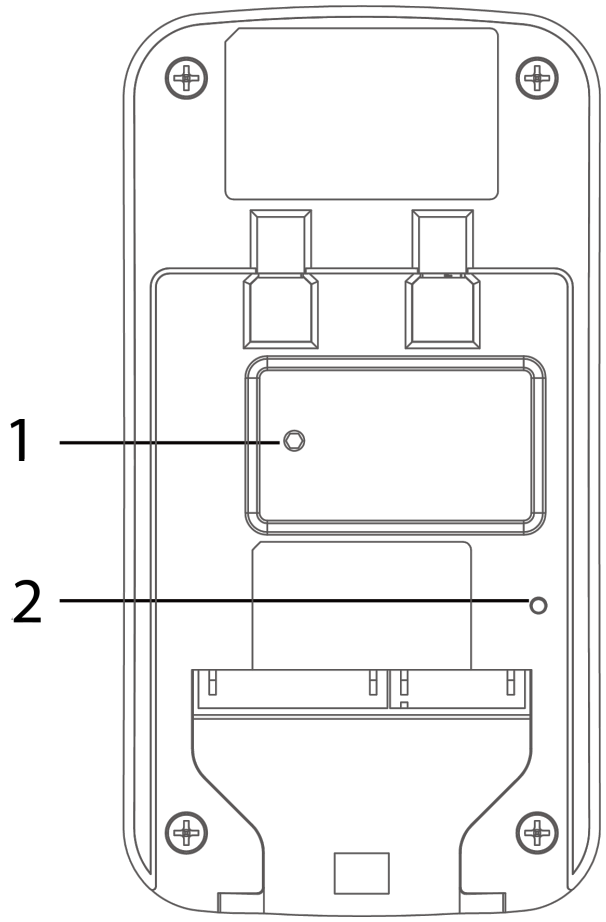


Tabla 2-7 Descripción del panel trasero

Núm.	Nombre	Descripción
1	Interruptor contra manipulaciones	Cuando el VTO se retira de la pared por medio de la fuerza, se activará una alarma y la información de la misma se enviará al centro de gestión.
2	REINICIAR	Mantenga pulsado durante 10 segundos para restablecer todos los ajustes.

Figura 2-8 Conexión del cable

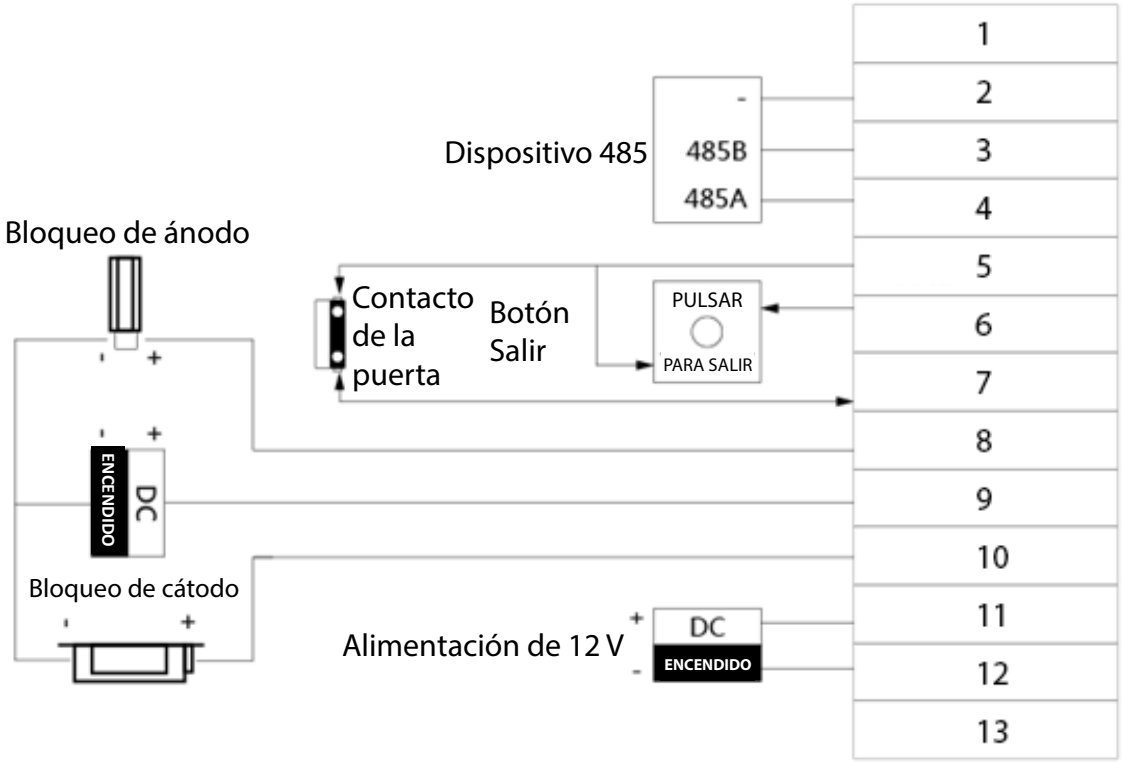


Tabla 2-8 Descripción del puerto

Núm.	Descripción	Núm.	Descripción
1	N/A	8	NC
2	GND	9	COM
3	485_B	10	NO
4	485_A	11	GND
5	GND	12	12V
6	DESBLOQ	13	RED
7	COMENTARIOS	—	—

2.4 VTO3211D-P-S2

2.4.1 Panel frontal

El número de botones en el panel frontal varía según los modelos. El VTO3211D-P-S2 tiene un botón, el VTO3211D-P2-S2 tiene dos botones y el VTO3211D-P4-S2 tiene cuatro botones. Aquí tomamos el VTO3211D-P4-S2 como ejemplo.

Figura 2-9 VTO3211D-P4-S2

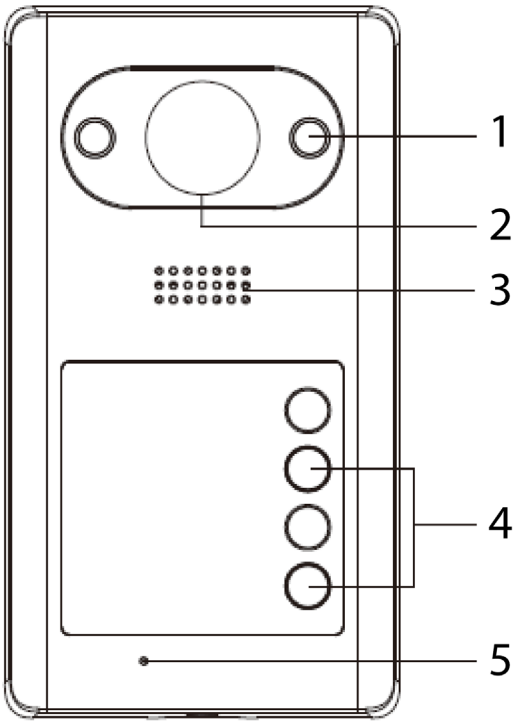


Tabla 2-9 Descripción del panel frontal

Núm.	Nombre	Descripción
1	Iluminador IR	Proporciona luz IR adicional a la cámara cuando está oscuro.
2	Cámara	—
3	Altavoz	—
4	Botón de llamada	Llame a los monitores internos (VTH) o al centro de gestión.
5	Micrófono	—

2.4.2 Panel trasero

Figura 2-10 VTO3211D-P4

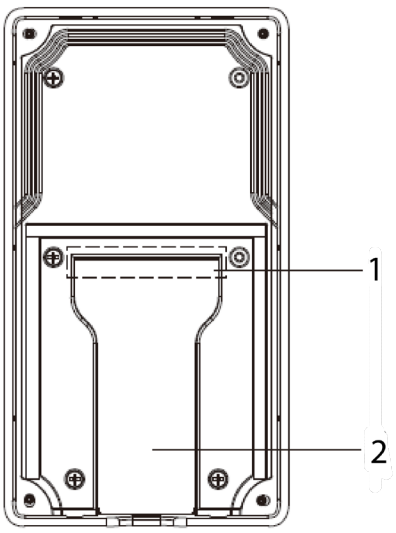


Tabla 2-10 Descripción del panel trasero

Núm.	Nombre	Descripción
1	Puertos de cable	Consulte la figura y la tabla siguientes.
2	Salida del cableado	Coloque el cableado aquí.

Figura 2-11 Conexión del cable

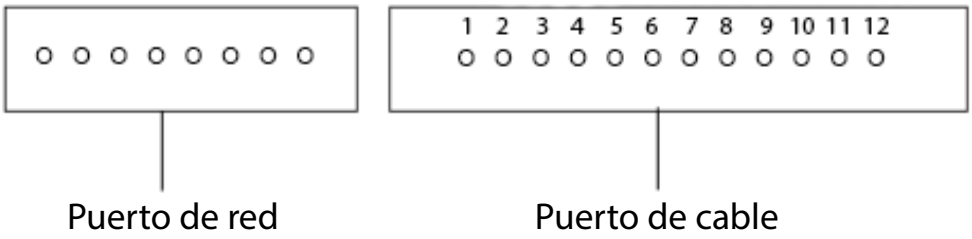


Tabla 2-11 Descripción del puerto para cables

Núm.	Nombre	Núm.	Nombre
1	ALM_COM	7	DOOR_FEED
2	ALM_NO	8	DOOR_NC
3	ALM_IN	9	DOOR_COM
4	RS485B	10	DOOR_NO
5	RS485A	11	GND
6	DOOR_OPEN	12	DC 12V

2.5 VTO3221E-P

2.5.1 Panel frontal

Figura 2-12 Panel frontal

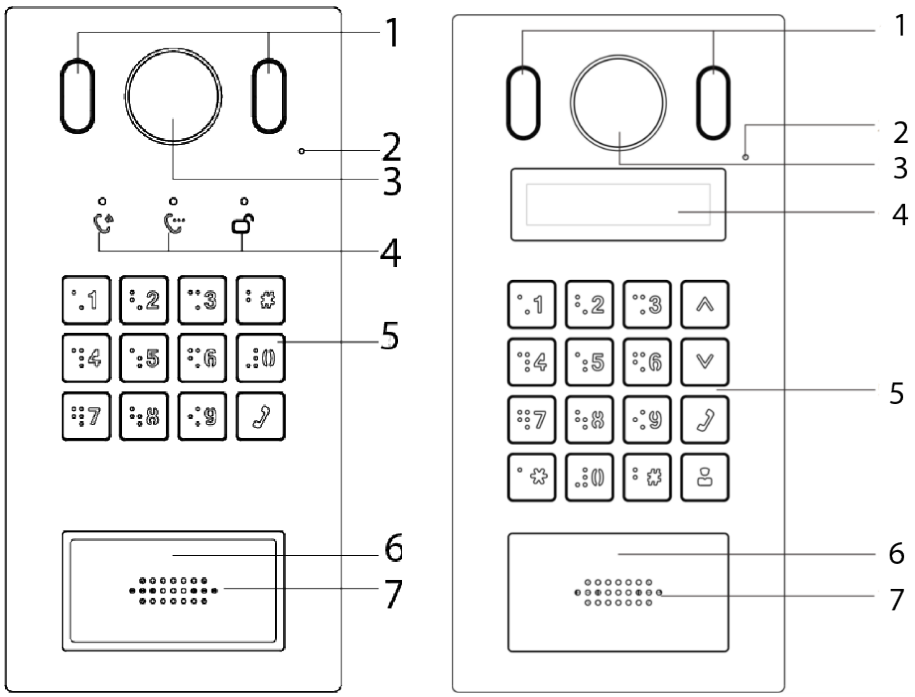


Tabla 2-12 Descripción del panel frontal

Núm.	Nombre	Descripción
1	Iluminador	Proporciona luz adicional a la cámara cuando está oscuro.
2	Micrófono	—
3	Cámara	—
4	Indicadores	Muestra el estado al llamar, hablar y desbloquear.
5	Teclado	—
6	Área de lectura de tarjetas	Pase una tarjeta aquí para abrir la puerta.
7	Altavoz	—

2.5.2 Panel trasero

Figura 2-13 VTO3221E-P

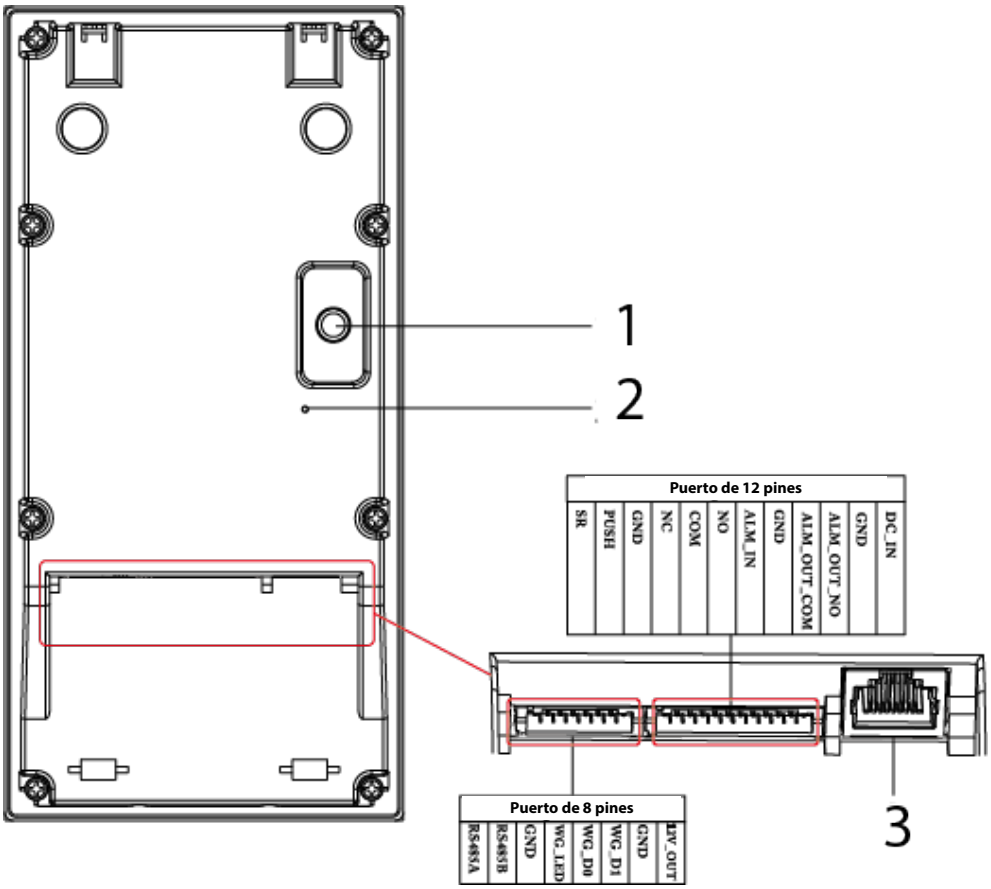


Tabla 2-13 Descripción del panel trasero

Núm.	Nombre	Descripción
1	Interruptor contra manipulaciones	Cuando el VTO se retira de la pared por medio de la fuerza, se activará una alarma y la información de la misma se enviará al centro de gestión.
2	Botón de reinicio	Mantenga pulsado durante 10 segundos para restablecer todos los ajustes.
3	Puerto Ethernet	Se conecta al cable de Ethernet.

2.6 VTO2211G-P/VTO1201G-P

2.6.1 Panel frontal

Figura 2-14 Panel delantero del VTO2211G/VTO1201G

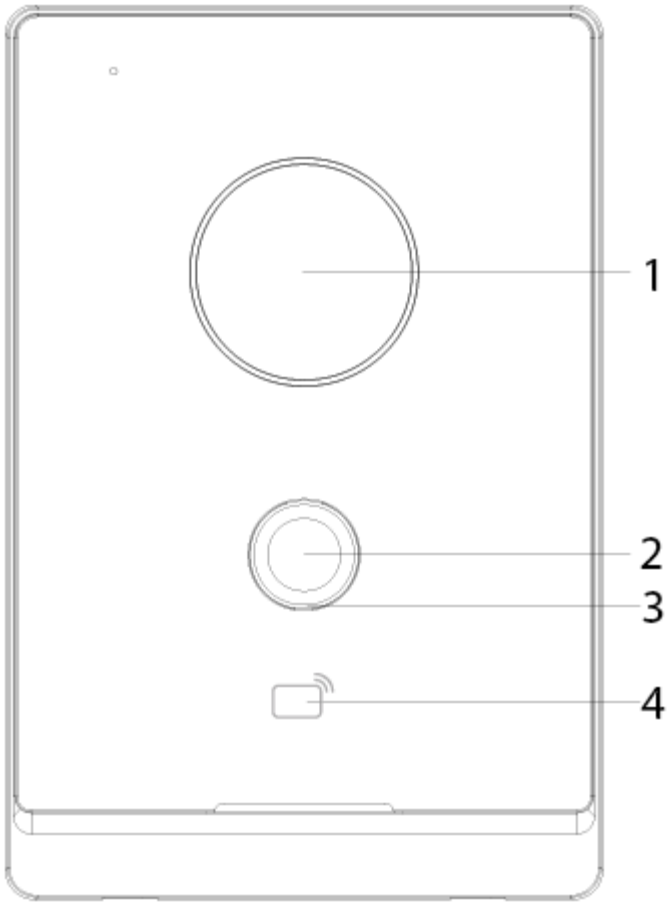


Tabla 2-14 Descripción del panel frontal

Núm.	Nombre	Descripción
1	Cámara	—
2	Botón de llamada	Llame a los monitores internos (VTH) o al centro de gestión.
3	Indicador	● Desactivado: el dispositivo está en modo de espera. ● Verde fijo: haciendo una llamada. ● Azul fijo: En una llamada. ● Amarillo-verde: puerta desbloqueada por el VTH mientras el VTO hace una llamada. ● Rojo-azul: puerta desbloqueada por el VTH cuando el VTO hace una llamada. ● Azul: red desconectada.
4	Área de lectura de tarjetas	Pase una tarjeta aquí para abrir la puerta (solo para el VTO2211G-P).

2.6.2 Panel trasero

Figura 2-15 Panel trasero del VTO2211G-P/VTO1201G-P

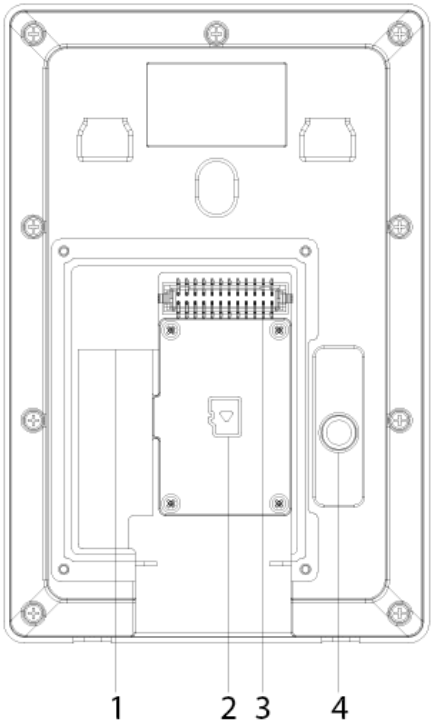
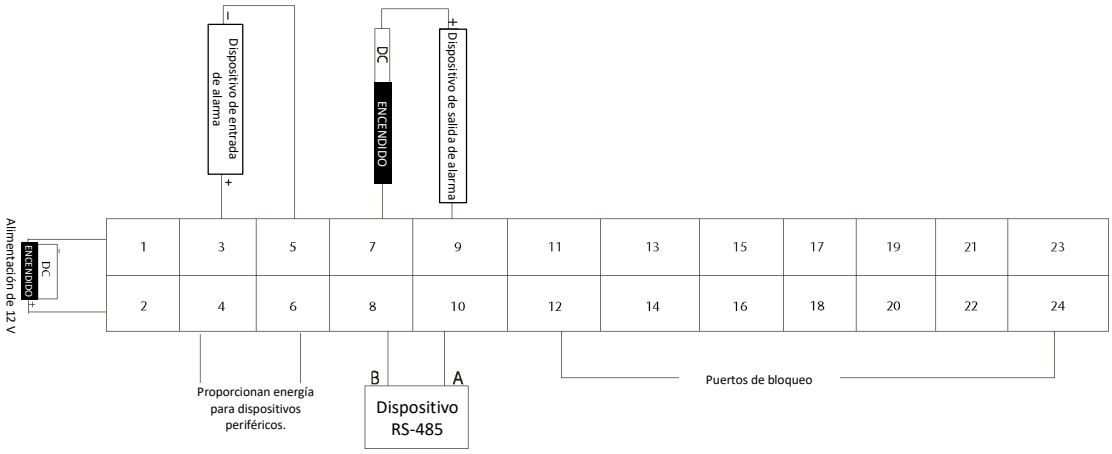


Tabla 2-15 Descripción del panel trasero

Núm.	Descripción	Núm.	Descripción
1	Puerto de red	3	Puertos
2	Cubierta de la tarjeta SD	4	Interruptor contra manipulaciones

Figura 2-16 Conexión de cable del VTO2211G-P



Los puertos 12, 14, 16, 18, 20, 22 y 24 se utilizan para conectarse a las cerraduras.

Tabla 2-16 Descripción del puerto

Núm.	Nombre	Núm.	Nombre
1	DC_IN-	13	No disponible
2	DC_IN+	14	DOOR1_COM

Núm.	Nombre	Núm.	Nombre
3	ALARM_IN	15	No disponible
4	+12V_OUT	16	DOOR1_NO
5	GND	17	No disponible
6	GND	18	GND
7	ALARM_NO	19	No disponible
8	RS485B	20	DOOR1_FB
9	ALARM_COM	21	No disponible
10	RS485A	22	GND
11	No disponible	23	No disponible
12	DOOR1_NC	24	DOOR1_PUSH

Figura 2-17 Conexión de cable del VTO1201G-P

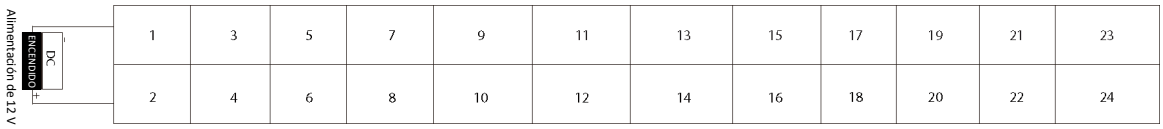
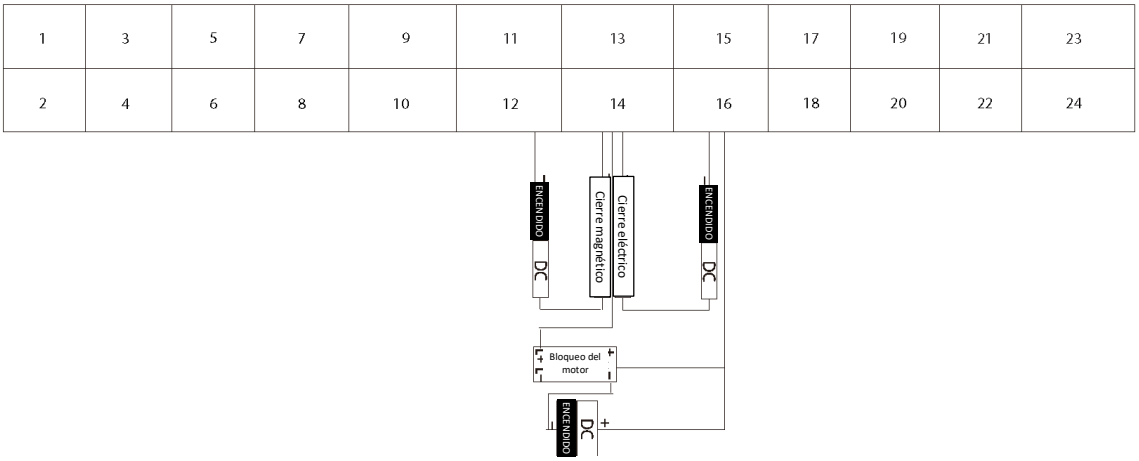


Tabla 2-17 Descripción del puerto

Núm.	Nombre
1	DC_IN-
2	DC_IN+
3-24	Función reservada

Figura 2-18 Conexión de cable

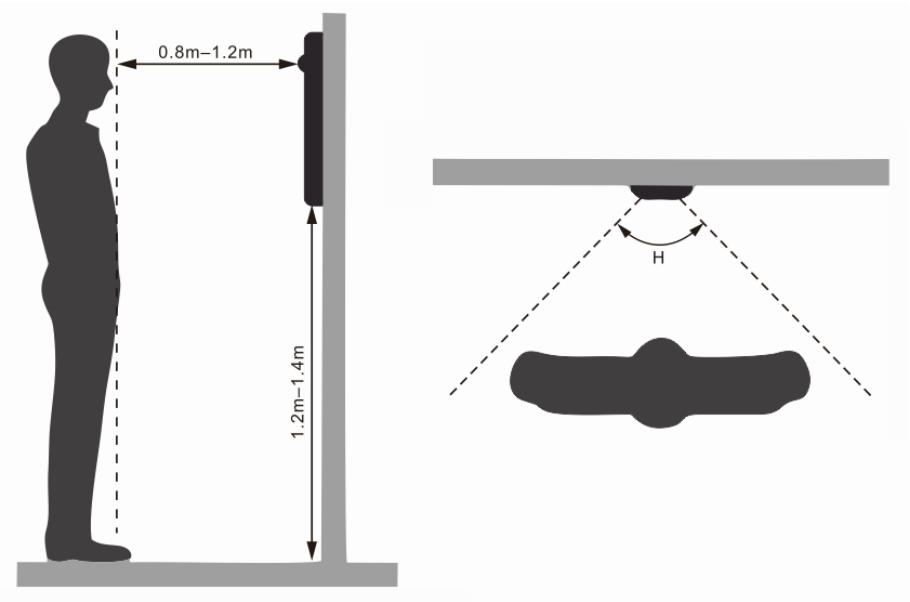


Puede conectar una cerradura magnética o una cerradura eléctrica según sea necesario. Consulte la figura anterior para conocer las reglas de conexión de puertos.

3 Instalación

- La instalación y la configuración se deben realizar por equipos profesionales. Póngase en contacto con la asistencia técnica si necesita reparar el dispositivo.
- Consulte la figura siguiente para conocer la posición de instalación. El ángulo de visión horizontal del dispositivo varía según el modelo, y la cara de la persona debe apuntar al centro del dispositivo.

Figura 3-1 Posición de instalación



4 Configuración

Este capítulo se centra en las configuraciones básicas de los dispositivos VTO y VTH. Consulte el manual del usuario para obtener más información.

Las interfaces pueden variar según la versión del software. La pantalla real prevalecerá.

4.1 Procedimiento

Antes de la configuración, compruebe los dispositivos y asegúrese de que no existan cortocircuitos o circuitos abiertos.

Paso 1: Planifique la IP y el número (funciona como un número de teléfono) para cada dispositivo.

Paso 2: Configure el VTO. Consulte "Configuración del VTO".

Paso 3: Configure el VTH. Consulte el manual del usuario del VTH.

Paso 4: Compruebe que todos los ajustes sean correctos. Consulte «4.4 Puesta en servicio».

4.2 Herramienta de configuración

Puede descargar la herramienta de configuración «VDPConfig» y utilizarla para configurar y actualizar varios dispositivos. Para más información, consulte el manual del usuario correspondiente.

4.3 Configuración del VTO

Conecte el VTO al PC con un cable de red y, la primera vez, deberá crear una nueva contraseña de inicio para la interfaz web.

4.3.1 Inicialización

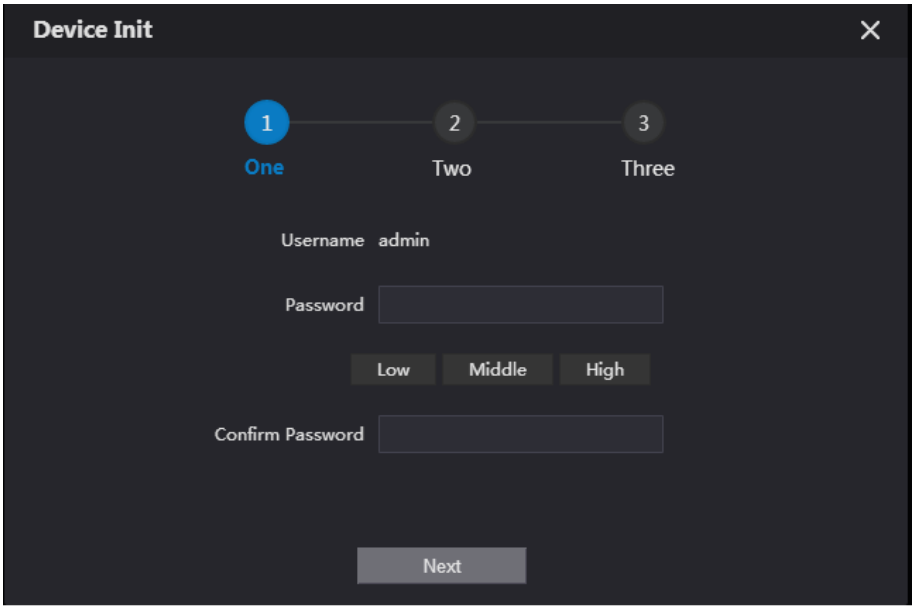
Asegúrese de que el PC esté en el mismo segmento de red.

Paso 1: Encienda el VTO.

Paso 2: Vaya a la dirección IP del VTO en el navegador.

- Para iniciar sesión por primera vez, introduzca la IP predeterminada (192.168.1.108). Si dispone de varios VTO, le recomendamos que cambie la dirección IP predeterminada en **Red > Básico** para evitar conflictos.

Figura 4-1 Inicio del dispositivo



Paso 3: Ingrese y confirme su nueva contraseña y, a continuación, haga clic en **Siguiente**.

Paso 4: Seleccione **Correo electrónico** e introduzca la dirección de correo electrónico que usará si necesita restablecer la contraseña.

Paso 5: Haga clic en **Siguiente**, y haga clic en **Aceptar** para a la interfaz de inicio de sesión.

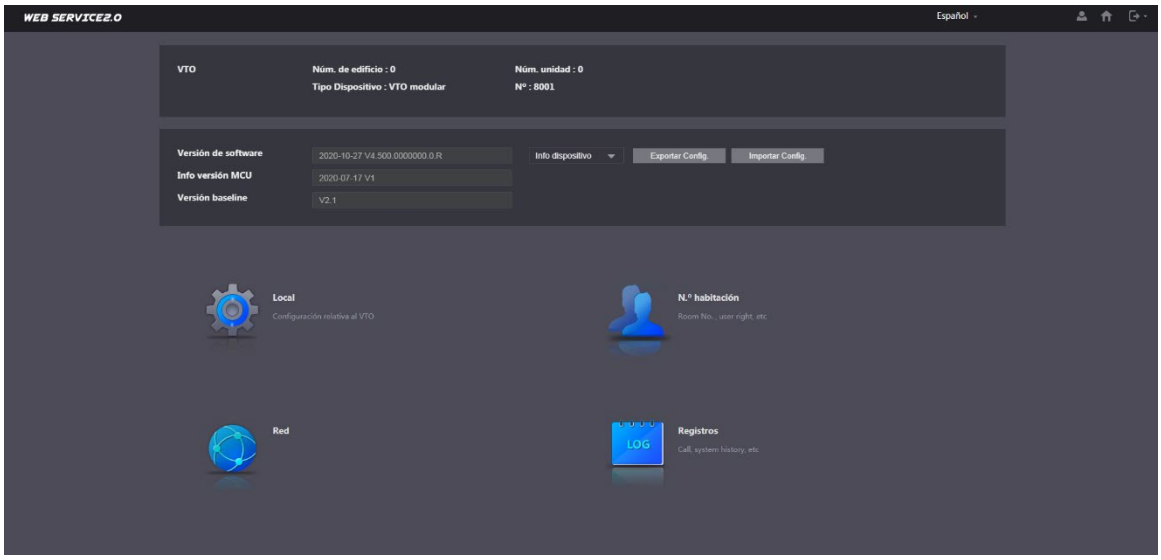
4.3.2 Configuración del número de VTO

Se pueden usar números para distinguir cada VTO, y recomendamos configurarlo según la unidad o el número de edificio.

- Puede cambiar el número de un VTO cuando NO funcione como servidor SIP.
- El número de VTO puede incluir 5 números como máximo, y no puede ser el mismo que el de otro número de habitación.

Paso 1: Inicie sesión en la interfaz web del VTO.

Figura 4-2 Interfaz principal



Paso 2: Seleccione **Local > Configuración básica**.

Figura 4-3 Propiedades del dispositivo

Paso 3: Ingrese el número en **Núm.** y, a continuación, haga clic en **Confirmar**.

4.3.3 Configuración de los parámetros de red

Paso 1: Seleccione **Red > Básico**.

Figura 4-4 Información TCP/IP

Paso 2: Introduzca cada parámetro y seguidamente haga clic en **Guardar**.

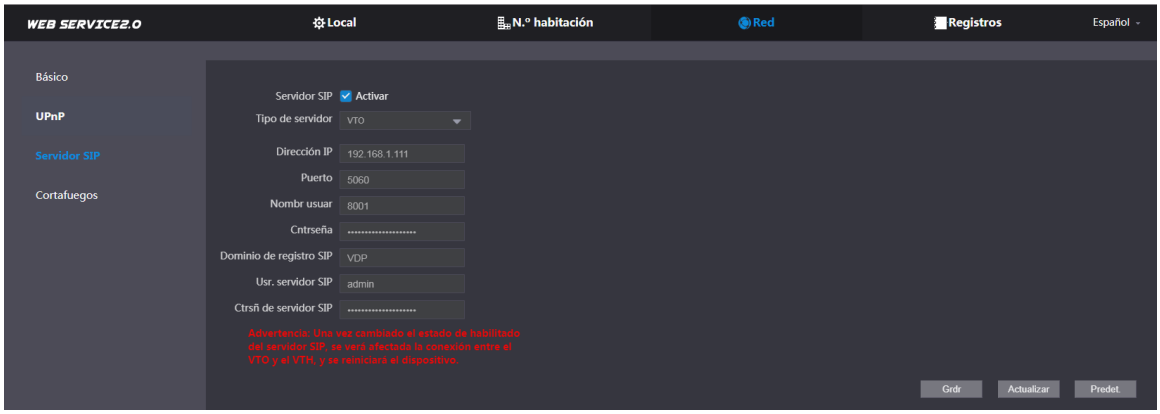
El VTO se reiniciará automáticamente. Deberá añadir la dirección IP de su PC en el mismo segmento de red que el VTO para iniciar sesión nuevamente.

4.3.4 Configuración de servidor SIP

Cuando se conecta al mismo servidor SIP, todos los VTO y VTH pueden llamarse entre sí. Puede utilizar un VTO u otros servidores como servidor SIP.

Paso 1: Seleccione **Red>Servidor SIP**.

Figura 4-5 Servidor SIP



Paso 2: Seleccione el tipo de servidor según sea necesario.

- Si el VTO funciona como servidor SIP, habilite el **Servidor SIP** y, a continuación, haga clic en **Guardar**.

  El VTO se reiniciará automáticamente y luego podrá añadir otros VTO y VTH a este VTO. Consulte "4.3.6 Añadir los VTO y 4.3.7 Adición de número de habitación".

Si el VTO actual no funciona como servidor SIP, no habilite el **Servidor SIP**. De lo contrario, la conexión con este VTO no funcionará correctamente.

- Si otros VTO funcionan como servidor SIP, configure el **Tipo de servidor** como VTO y, a continuación, configure los parámetros.

Tabla 4-1 Configuración del servidor SIP

Parámetro	Descripción
Dirección IP	La dirección IP del VTO que funciona como servidor SIP.
Puerto	● 5060 por defecto cuando el VTO funciona como servidor SIP. ● 5080 por defecto cuando la plataforma funciona como servidor SIP.
Nombre de usuario	Conserve el valor predeterminado.
Contraseña	
Dominio de SIP	VDP.
Nombre de usuario del servidor SIP	Nombre de usuario y contraseña de inicio de sesión de la interfaz web del servidor SIP.
Contraseña del servidor SIP	

- Si otros servidores funcionan como servidor SIP, configure el **Tipo de servidor** según sea necesario y, a continuación, consulte el manual correspondiente para obtener más información.

4.3.5 Configurar el número de llamada y llamada de grupo

Para marcar y llamar a un VTO, debe configurar el número de llamada en todos los VTO que funcionen como número de teléfono.

Paso 1: Seleccione **Local > Configuración básica**.

Figura 4-6 Propiedades del dispositivo

Paso 2: En el cuadro de entrada de **Número**, introduzca el número de habitación al que necesita llamar y seguidamente haga clic en **Confirmar** para guardar. Repita esta operación en cada interfaz web del VTO.

En el servidor SIP, puede habilitar la función de llamada de grupo. Al llamar a un VTH principal, el resto de VTH también recibirán la llamada.

- Puede cambiar el número del VTO cuando no funciona como servidor SIP.
- El VTO se reiniciará después de habilitar o deshabilitar la función de llamada de grupo.

Paso 3: Inicie sesión en la interfaz web del servidor SIP y, a continuación, seleccione **Local > Configuración básica**.

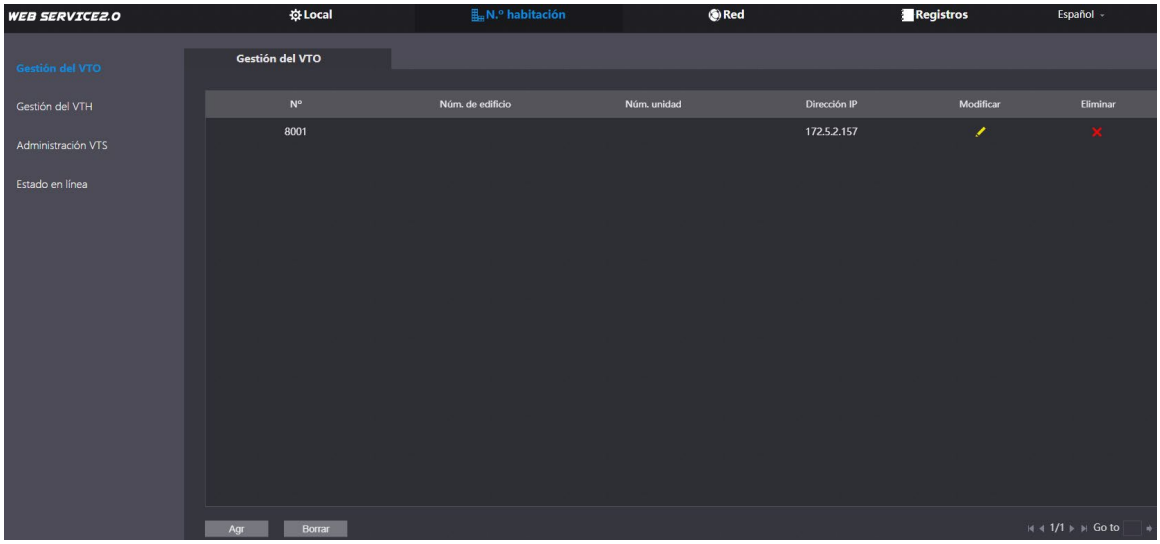
Paso 4: Habilite la **Llamada de grupo**, haga clic en **Confirmar** y seguidamente, el VTO se reiniciará.

4.3.6 Añadir los VTO

Puede añadir VTO al servidor SIP para que todos los VTO conectados al mismo servidor SIP puedan hacer videollamadas entre sí. Esta sección se aplica siempre cuando un videoportero (VTO) funciona como servidor SIP, y si utiliza otros servidores como servidor SIP, consulte el manual correspondiente para obtener una configuración detallada.

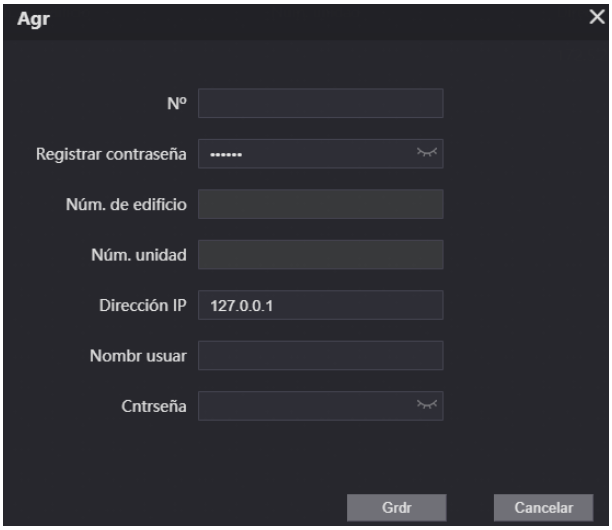
Paso 1: Inicie sesión en la interfaz web del servidor SIP y, a continuación, seleccione **Configuración del hogar> Gestión de Núm. VTO**.

Figura 4-7 Gestión de Núm. VTO



Paso 2: Haga clic sobre **Añadir**.

Figura 4-8 Añada el VTO



Paso 3: Configure los parámetros.

- Se debe añadir el servidor SIP.

Tabla 4-2 Añadir videoporteros (VTO)

Parámetro	Descripción
N.º regis.	Número de VTO. Consulte «4.3.2 Configuración del número de VTO».
Contraseña de registro	Conserve el valor predeterminado.
Núm. edificio	Disponible solo cuando otros servidores funcionan como servidor SIP.
N.º de unidad	

Dirección IP	Dirección IP del VTO.
Nombre de usuario	Nombre de usuario y contraseña de inicio de sesión de la interfaz web del VTO.
Contraseña	

Paso 4: Haga clic en **Guardar** (Save).

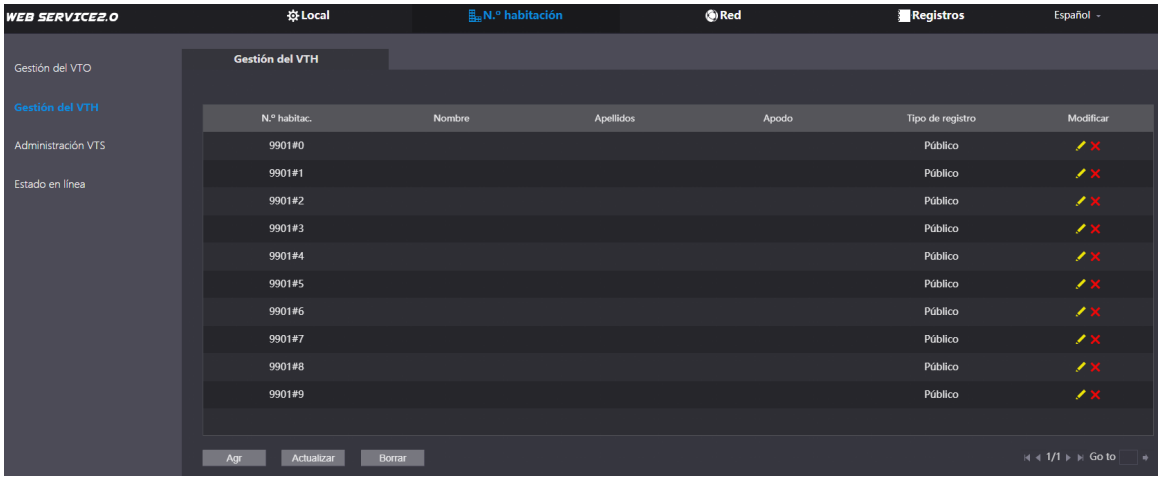
4.3.7 Adición de número de habitación

Puede añadir el número de habitación al servidor SIP y luego configurar el número de habitación en los VTH para conectarlos a la red. Esta sección se aplica siempre cuando un videoportero (VTO) funciona como servidor SIP, y si utiliza otros servidores como servidor SIP, consulte el manual correspondiente para obtener una configuración detallada.

El número de habitación puede contener, como máximo, 6 números o letras o una combinación de ellos y no puede ser un número de VTO.

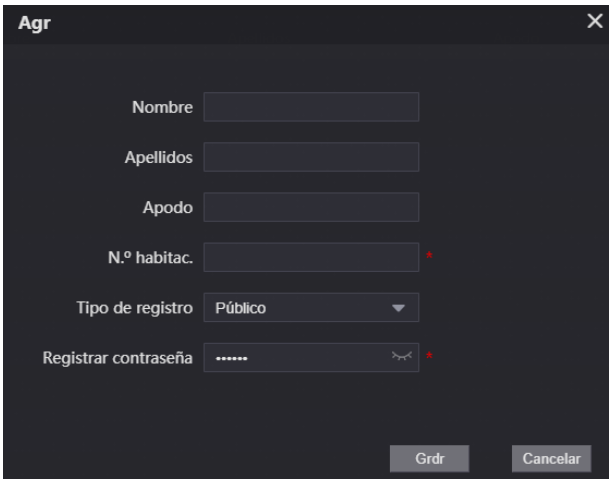
Paso 1: Inicie sesión en la interfaz web del servidor SIP y, a continuación, seleccione **Configuración del hogar> Gestión del n.º de habitación**.

Figura 4-9 Gestión de número de habitación



Paso 2: Haga clic sobre **Añadir**.

Figura 4-10 Añadir un número de habitación



Paso 3: Configure la información de la habitación.

Tabla 4-3 Información de la habitación

Parámetro	Descripción
Nombre	Información utilizada para diferenciar cada habitación.
Apellidos	
Nombre de usuario	
N.º de habitación	Número de habitación. ● Cuando hay varios VTH, el número de habitación para el VTH principal debe terminar en #0, y los números de habitación para las extensiones VTH en #1, #2… ● Puede configurar hasta 9 VTH secundarios para un VTH principal.
Modo de registro	Seleccione **público**.
Clave de seguridad registrada	Conserve el valor predeterminado.

Paso 4: Haga clic en **Guardar** (Save).

Haga clic en para modificar la información de la habitación, y haga clic en para eliminar la habitación.

4.4 Puesta en servicio

4.4.1 Llamada del VTO al VTH

Paso 1: Marque el número de habitación en el VTO.

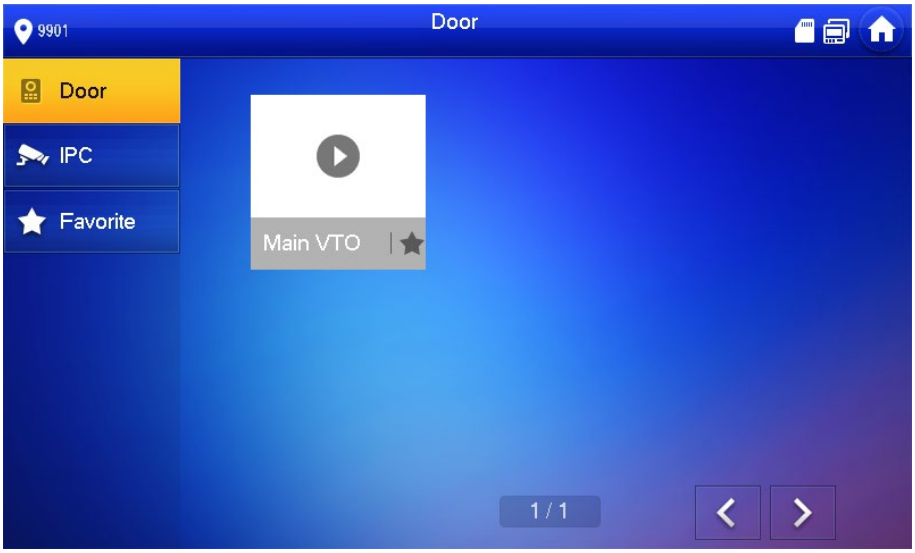
Paso 2: Pulse en el VTH para responder la llamada.

Figura 4-11 Pantalla de llamada

4.4.2 Monitorización del VTO desde el VTH

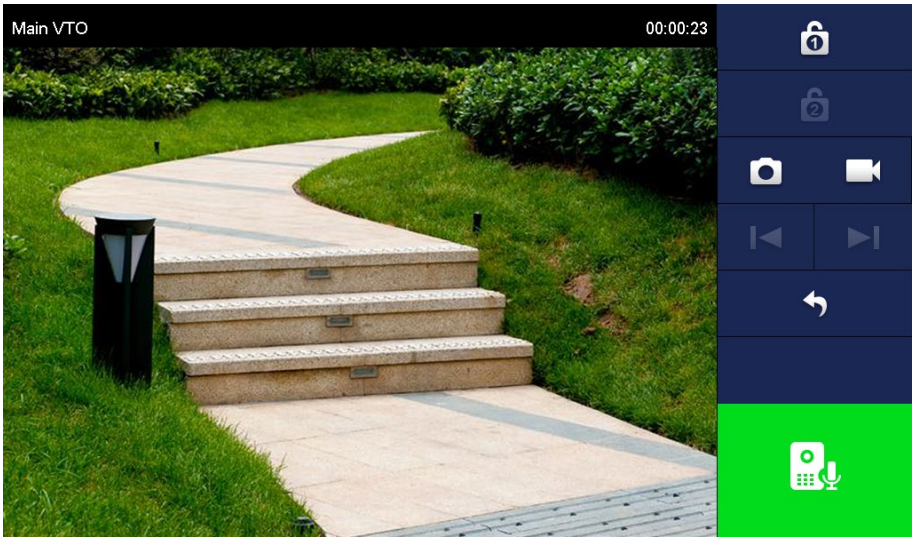
Paso 1: En la interfaz principal del VTH, seleccione **Monitor> Puerta**.

Figura 4-12 Puerta



Paso 2: Seleccionar un VTO.

Figura 4-13 Vídeo de monitorización



5 EasyViewer Plus

La aplicación EasyViewer Plus (en lo sucesivo, la «aplicación») le permite administrar dispositivos, reproducir vídeos, desbloquear puertas y mucho más.

Antes de añadir el VTO a la aplicación, debe conectar el VTO al router a través de Wi-Fi, o conectar el VTO al router usando un «switch» y, a continuación, cambiar manualmente la dirección IP del VTO a la misma red que el router si el DHCP no es compatible.

Descargue la aplicación en la tienda de aplicaciones de su smartphone. En la aplicación, seleccione **Configuración > Ayuda y comentarios** para ver instrucciones de cada función.

Apéndice 1 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 dispositivo 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 dispositivo (como NVR, DVR, cámara IP, etc.) 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 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 dispositivo:

1. **Protección física**

   Le sugerimos que proteja físicamente su dispositivo, especialmente los dispositivos de almacenamiento. Por ejemplo, coloque el dispositivo 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 dispositivos 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 dispositivo 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. **Enlace de dirección MAC**

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

8. **Asignar cuentas y privilegios razonablemente**

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

9. **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.

10. **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.

11. **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 dispositivo: Al consultar los registros, puede conocer las direcciones IP que se han utilizado 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 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.

13. Crear un entorno de red seguro

Para garantizar mejor la seguridad de los dispositivos 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.
- Habilitar la función de filtrado de direcciones IP/MAC para limitar el rango de hosts permitidos para acceder al dispositivo.