

Estación de puerta de villa (versión 4.5)

Guía de inicio rápido



Prefacio

General

Este manual presenta la estructura, el proceso de montaje y la configuración básica de la estación de puerta villa (en lo sucesivo, "VTO").

Las instrucciones de seguridad

Las siguientes palabras de advertencia categorizadas con un significado definido pueden aparecer en el manual.

Palabras de advertencia	Sentido
 PELIGRO	Indica un peligro de alto potencial que, si no se evita, provocará la muerte o lesiones graves.
 ADVERTENCIA	Indica un peligro potencial medio o bajo que, si no se evita, podría provocar lesiones leves o moderadas.
 PRECAUCIÓN	Indica un riesgo potencial que, si no se evita, podría provocar daños a la propiedad, pérdida de datos, menor rendimiento o resultados impredecibles.
 CONSEJOS	Proporciona métodos para ayudarlo a resolver un problema o ahorrarle tiempo.
 NOTA	Proporciona información adicional como énfasis y complemento del texto.

Revisión histórica

Versión	Contenido de revisión	Fecha de lanzamiento
V1.0.0	Primer lanzamiento.	diciembre 2020

Sobre el Manual

- El manual es solo para referencia. Si hay inconsistencia entre el manual y el producto real, prevalecerá el producto real.
- No somos responsables de ninguna pérdida causada por las operaciones que no cumplen con el manual. El manual se actualizaría de acuerdo con las últimas leyes y reglamentos de las regiones relacionadas. Para obtener información detallada, consulte el manual en papel, el CD-ROM, el código QR o nuestro sitio web oficial. Si hay inconsistencia entre el manual en papel y la versión electrónica, prevalecerá la versión electrónica.
- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto pueden causar algunas diferencias entre el producto real y el manual. Póngase en contacto con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria.
- Todavía puede haber desviación en los datos técnicos, descripción de funciones y operaciones, o errores en la impresión. Si tiene alguna duda o disputa, consulte nuestra explicación final.

- Actualice el software del lector o pruebe con otro software del lector convencional si no se puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas comerciales registradas y nombres de compañías en el manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, comuníquese con el proveedor o el servicio al cliente si ocurre algún problema al usar el dispositivo.
- Si hay alguna duda o controversia, consulte nuestra explicación final.

Medidas de seguridad y advertencias importantes

La siguiente descripción es el método de aplicación correcto del dispositivo. Lea atentamente el manual antes de usarlo para evitar peligros y pérdidas de propiedad. Siga estrictamente el manual durante la aplicación y consérvelo correctamente después de leerlo.

Requisitos operativos

- No exponga el dispositivo a la luz solar directa ni a una fuente de calor.
- No instale el dispositivo en un área húmeda o polvorienta.
- Instale el dispositivo horizontalmente en lugares estables y evite que se caiga.
- No gotee ni salpique líquidos sobre el dispositivo, ni coloque sobre el dispositivo ningún objeto lleno de líquido.
- Instale el dispositivo en un lugar bien ventilado y no bloquee su ventilación.
- Use el dispositivo solo dentro del rango nominal de entrada y salida. No desmonte el dispositivo usted mismo.
- Transporte, use y almacene el dispositivo dentro del rango permitido de humedad y temperatura.

requerimientos de energía

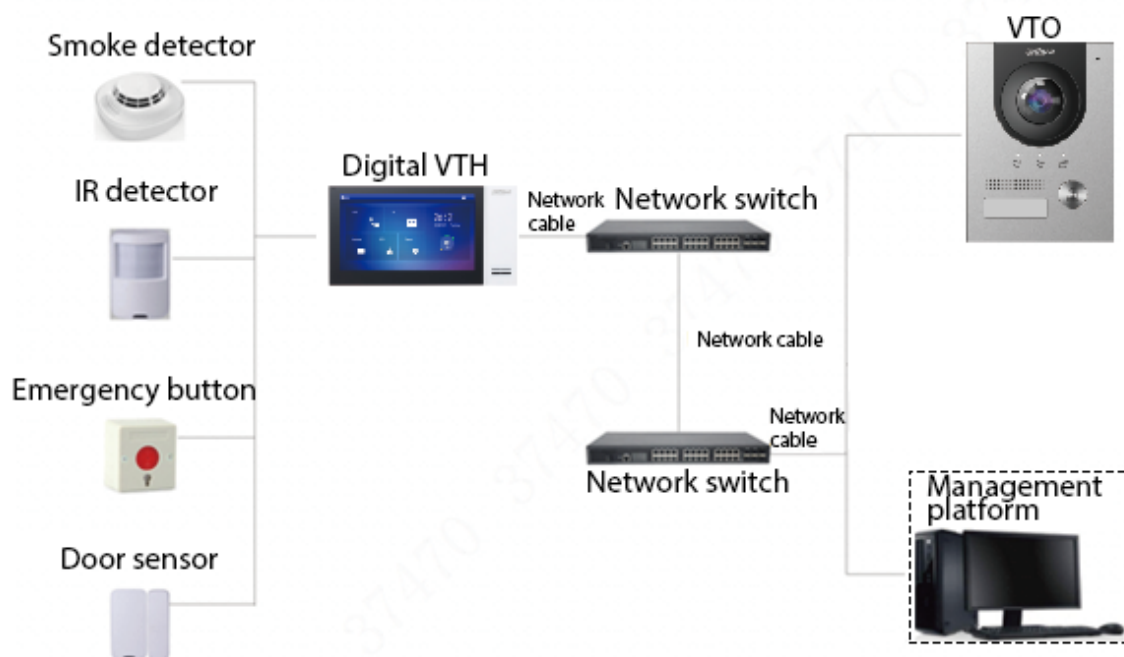
- El producto debe utilizar cables eléctricos que cumplan con los requisitos locales.
- Utilice una fuente de alimentación que cumpla con los requisitos SELV (voltaje extra bajo de seguridad) y suministre energía con un voltaje nominal que cumpla con la fuente de alimentación limitada en IEC60950-1. Para conocer los requisitos específicos de la fuente de alimentación, consulte las etiquetas de los dispositivos.
- El acoplador de electrodomésticos es un dispositivo de desconexión. Durante el uso normal, mantenga un ángulo que facilite la operación.

Tabla de contenido

Prefacio.....	I Medidas
de seguridad y advertencias importantes	III 1
Diagrama de red	1
2 Apariencia.....	2
2.1 VTO2101E-P.....	2
2.1.1 Panel frontal	2
2.1.2 Panel trasero	3
2.2 VTO2202F-P-S2/VTO2202F-P/VTO2202F/VTO2201F-P.....	4
2.2.1 Panel frontal	4
2.2.2 Panel trasero	5
2.3 VTO2111D-P-S2/VTO1101D-P	6
2.3.1 Panel frontal	6
2.3.2 Panel trasero	7
2.4 VTO3211D-P-S2.....	8
2.4.1 Panel frontal	8
2.4.2 Panel trasero	9
2.5 VTO3221E-P.....	10
2.5.1 Panel frontal	10
2.5.2 Panel trasero	11
2.6 VTO2211G-P/VTO1201G-P.....	12
2.6.1 Panel frontal	12
2.6.2 Panel trasero	13
3 Instalación.....	15
4 Configuración	dieciséis
4.1 Procedimiento.....	dieciséis
4.2 Herramienta de configuración	dieciséis
4.3 Configuración de VTO.....	dieciséis
4.3.1 Inicialización	dieciséis
4.3.2 Configuración del número VTO	17
4.3.3 Configuración de parámetros de red	18
4.3.4 Configuración del servidor SIP	19
4.3.5 Configuración de número de llamada y llamada de grupo.....	20
4.3.6 Adición de VTO	20
4.3.7 Adición de número de habitación.....	21
4.4 Puesta en marcha.....	23
4.4.1 VTO llamando a VTH	23
4.4.2 Monitoreo de VTH VTO.....	23
5 EasyViewer Plus	25
Appendix 1 Recomendaciones de ciberseguridad	26

1 diagrama de red

Figure 1-1 Diagrama de Red



En ciertas aplicaciones, como una villa, el Centro de gestión/Plataforma suele ser innecesario.

2 Apariencia

2.1 VTO2101E-P

2.1.1 Panel frontal

Figure 2-1 VTO2101E-P

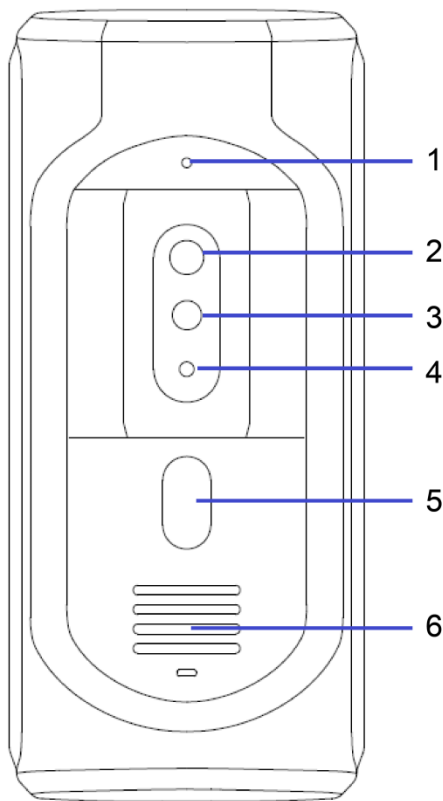


Tabla 2-1 Descripción del panel frontal

No.	Nombre	Descripción
1	Micrófono	—
2	Cámara	—
3	Luz de iluminación IR	Proporciona luz IR adicional para la cámara cuando está oscuro.
4	Sensor de luz	Detecta la condición de iluminación ambiental.
5	Botón de llamada	Llame a los VTH o al centro de gestión.
6	Altavoz	—

2.1.2 Panel trasero

Figure 2-2 VTO2101E-P

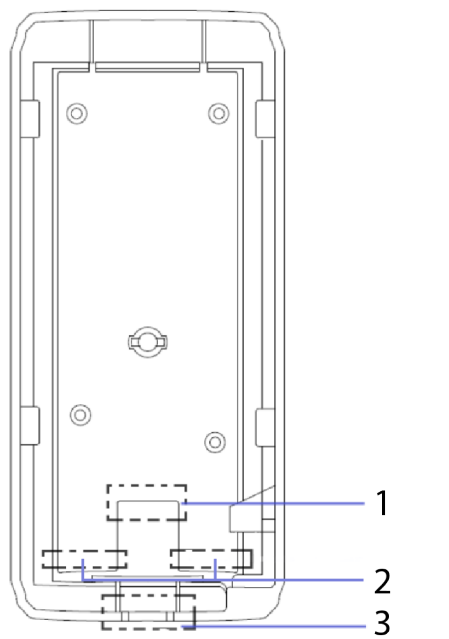


Tabla 2-2 Descripción del panel trasero

No.	Nombre	Descripción
1	puerto de red	Se conecta al cable de red.
2	Puertos RS-485	Consulte la figura y la tabla a continuación.
3	Salida de cables	Pase los cables aquí.

Figure 2-3 Conexión de cable

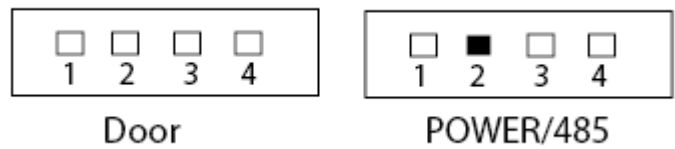


Tabla 2-3 Descripción del puerto

PUERTA		POTENCIA/485	
No.	Nombre	No.	Nombre
1	NO	1	+ 12V
2	CAROLINA DEL NORTE	2	TIERRA
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

Figure 2-4 Panel frontal

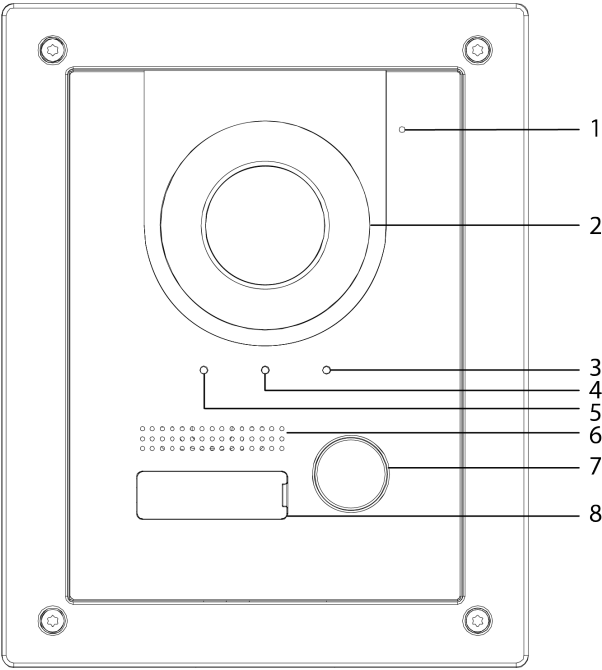


Tabla 2-4 Descripción del panel frontal

No.	Nombre	Descripción
1	Micrófono	—
2	Cámara	—
3	Indicador	Encendido: Puerta desbloqueada.
4		Encendido: En una llamada.
5		Encendido: llamando.
6	Altavoz	—
7	Botón de llamada	Llame a otros VTH o al centro de gestión.
8	Etiqueta de nombre	Nombre de host.

2.2.2 Panel trasero

Figure 2-5 Panel trasero

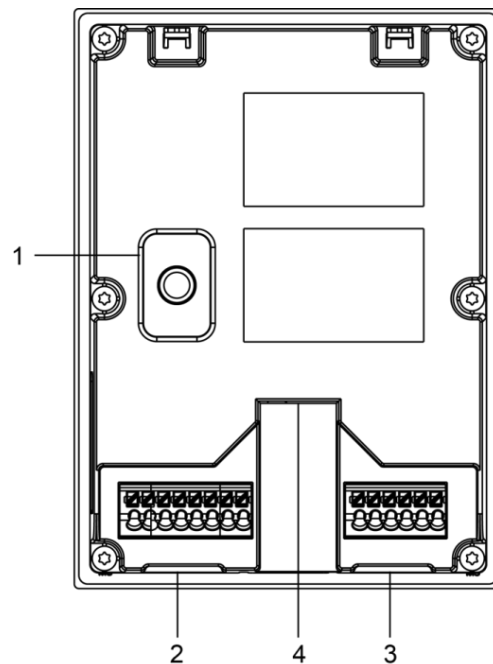


Tabla 2-5 Descripción del panel trasero

NO	Nombre	Descripción
1	Antimanipulación cambiar	Cuando el VTO se quita de la pared a la fuerza, se activará una alarma y la información de la alarma se enviará al centro de gestión.
2	Puerto	De izquierda a derecha: TIERRA + 12V_SALIDA RS485_B RS485_A ALARMA_NO ALARMA_COM VTO2202F-P-S2: 2 hilos + (48 V); VTO2202F-P y VTO2202F: EOC1 (+12 V); VTO2201F: +24V. VTO2202F-P-S2: 2 hilos - (GND); VTO2202F-P y VTO2202F: EOC2 (GND); VTO2201F: TIERRA.
3		De izquierda a derecha: DOOR_BUTTON PUERTA_FB TIERRA PUERTA_NC PUERTA_COM PUERTA_NO
4	Puerto Ethernet	Se conecta a la red con un cable Ethernet.  Solo los modelos con "P" admiten PoE.

2.3 VTO2111D-P-S2/VTO1101D-P

2.3.1 Panel frontal

Figure 2-6 Panel frontal

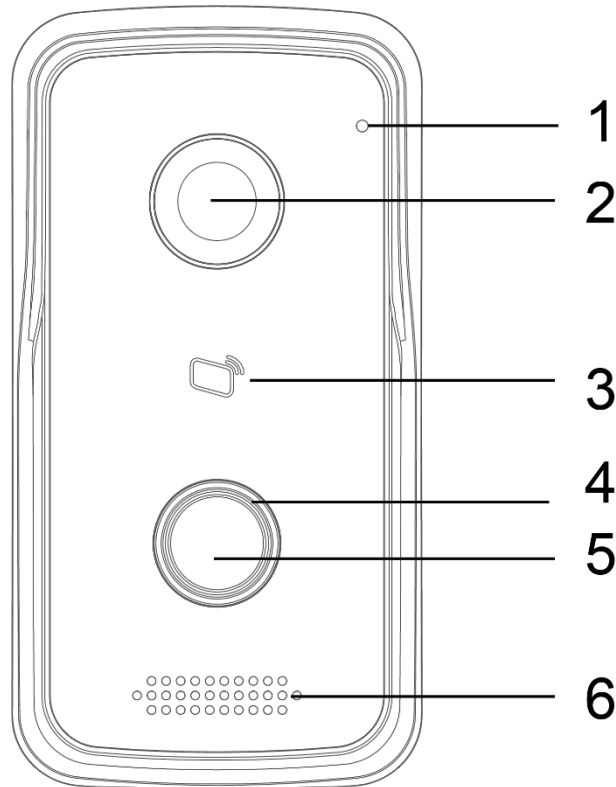


Tabla 2-6 Descripción del panel frontal

No.	Nombre	Descripción
1	Micrófono	—
2	Cámara	—
3	Área de lectura de tarjetas	Deslice para desbloquear o emitir la tarjeta.
4	Indicador	● Azul fijo: modo de espera. ● Parpadea en azul: llamando o no hay red.
5	Botón de llamada	Llame a los VTH o al centro de gestión.
6	Altavoz	—

2.3.2 Panel trasero

Figure 2-7 Panel trasero

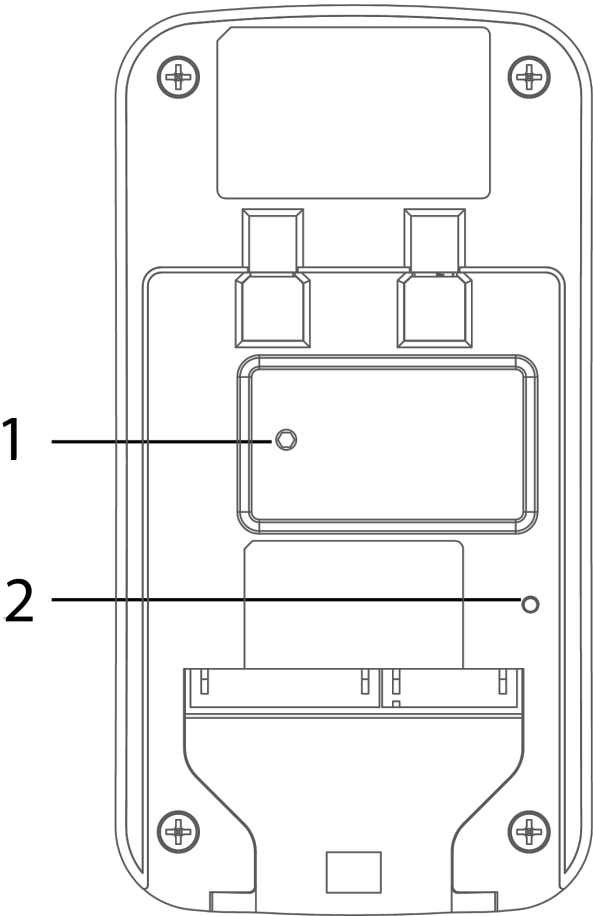


Tabla 2-7 Descripción del panel trasero

No.	Nombre	Descripción
1	Antimanipulación cambiar	Cuando el VTO se quita de la pared a la fuerza, se activará una alarma y la información de la alarma se enviará al centro de gestión.
2	REINICIAR	Manténgalo presionado durante 10 segundos para restablecer todas las configuraciones.

Figure 2-8 Conexión de cable

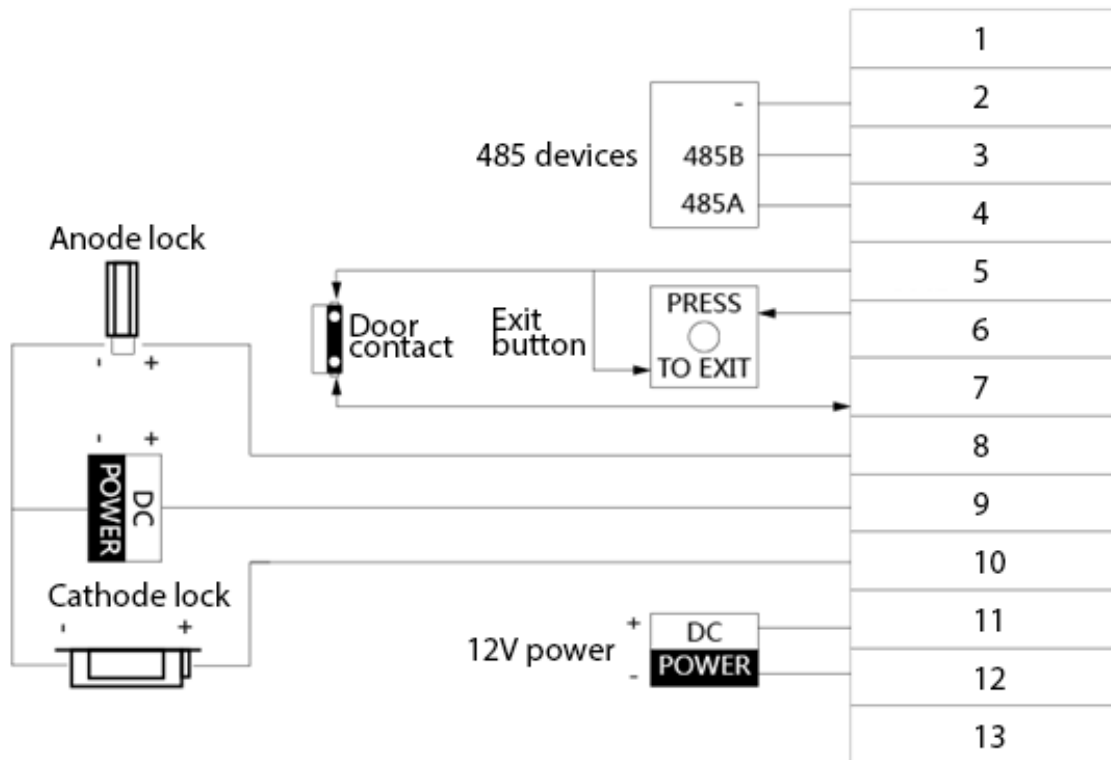


Tabla 2-8 Descripción del puerto

No.	Descripción	No.	Descripción
1	N / A	8	CAROLINA DEL NORTE
2	TIERRA	9	COM
3	485_B	10	NO
4	485_A	11	TIERRA
5	TIERRA	12	12V
6	DESBLOQUEAR	13	NETO
7	REALIMENTACIÓN	—	—

2.4 VTO3211D-P-S2

2.4.1 Panel frontal

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

Figure 2-9 VTO3211D-P4-S2

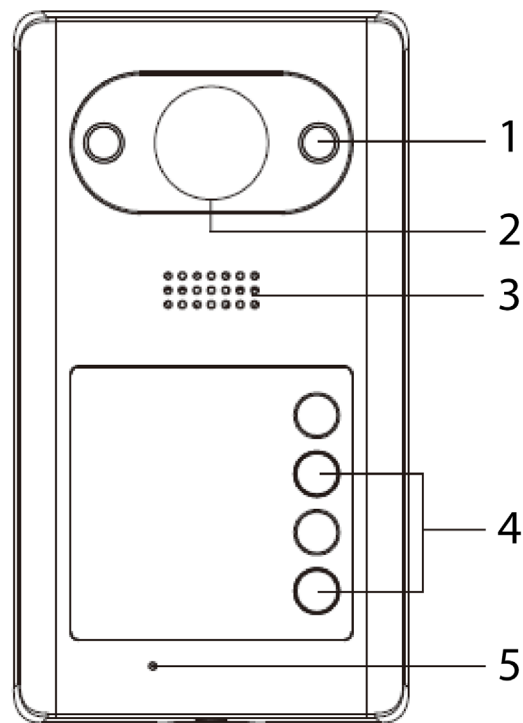


Tabla 2-9 Descripción del panel frontal

No.	Nombre	Descripción
1	iluminador de infrarrojos	Proporciona luz IR adicional para la cámara cuando está oscuro.
2	Cámara	—
3	Altavoz	—
4	Botón de llamada	Llame a los VTH o al centro de gestión.
5	Micrófono	—

2.4.2 Panel trasero

Figure 2-10 VTO3211D-P4

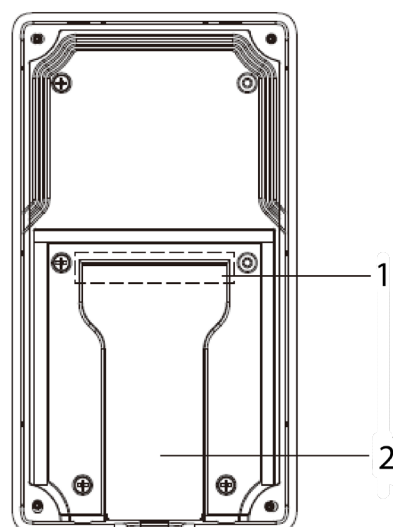


Tabla 2-10 Descripción del panel trasero

No.	Nombre	Descripción
1	Puertos de cable	Consulte la figura y la tabla a continuación.
2	Salida de cables	Pase los cables aquí.

Figure 2-11 Conexión de cable

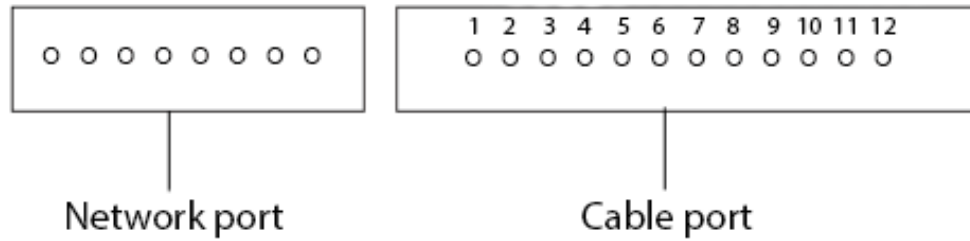


Tabla 2-11 Descripción del puerto de cable

No.	Nombre	No.	Nombre
1	ALM_COM	7	ALIMENTACIÓN DE LA PUERTA
2	ALM_NO	8	PUERTA_NC
3	ALM_IN	9	PUERTA_COM
4	RS485B	10	PUERTA_NO
5	RS485A	11	TIERRA
6	PUERTA ABIERTA	12	CC 12V

2.5 VTO3221E-P

2.5.1 Panel frontal

Figure 2-12 Panel frontal

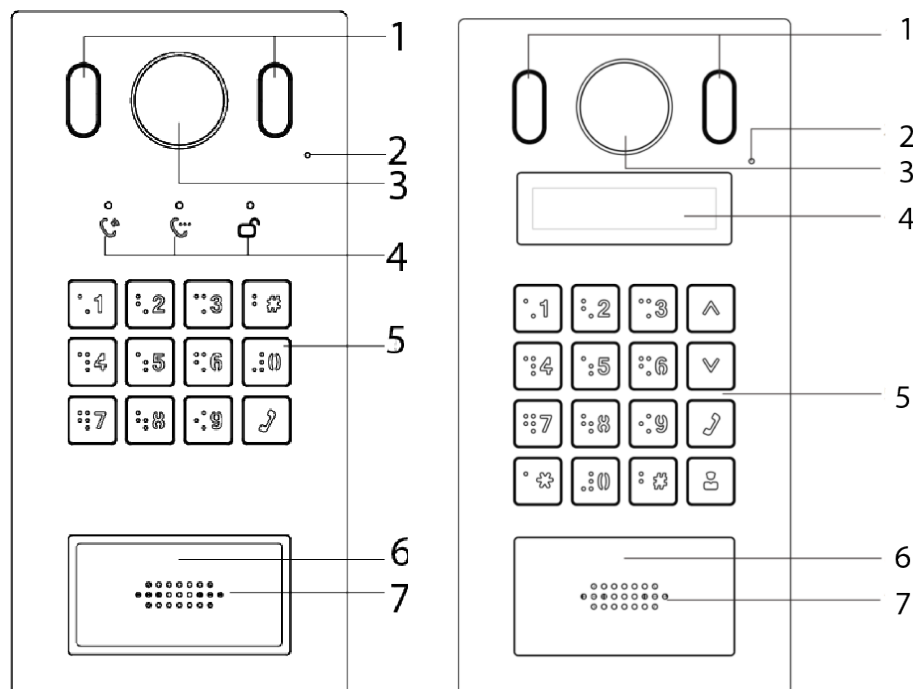


Tabla 2-12 Descripción del panel frontal

No.	Nombre	Descripción
1	Iluminador	Proporciona luz adicional para la cámara cuando está oscuro.
2	Micrófono	—
3	Cámara	—
4	Indicadores	Muestra el estado de llamadas, conversaciones y desbloqueo.
5	teclado	—
6	Área de lectura de tarjetas	Pase una tarjeta aquí para desbloquear la puerta.
7	Altavoz	—

2.5.2 Panel trasero

Figure 2-13 VTO3221E-P

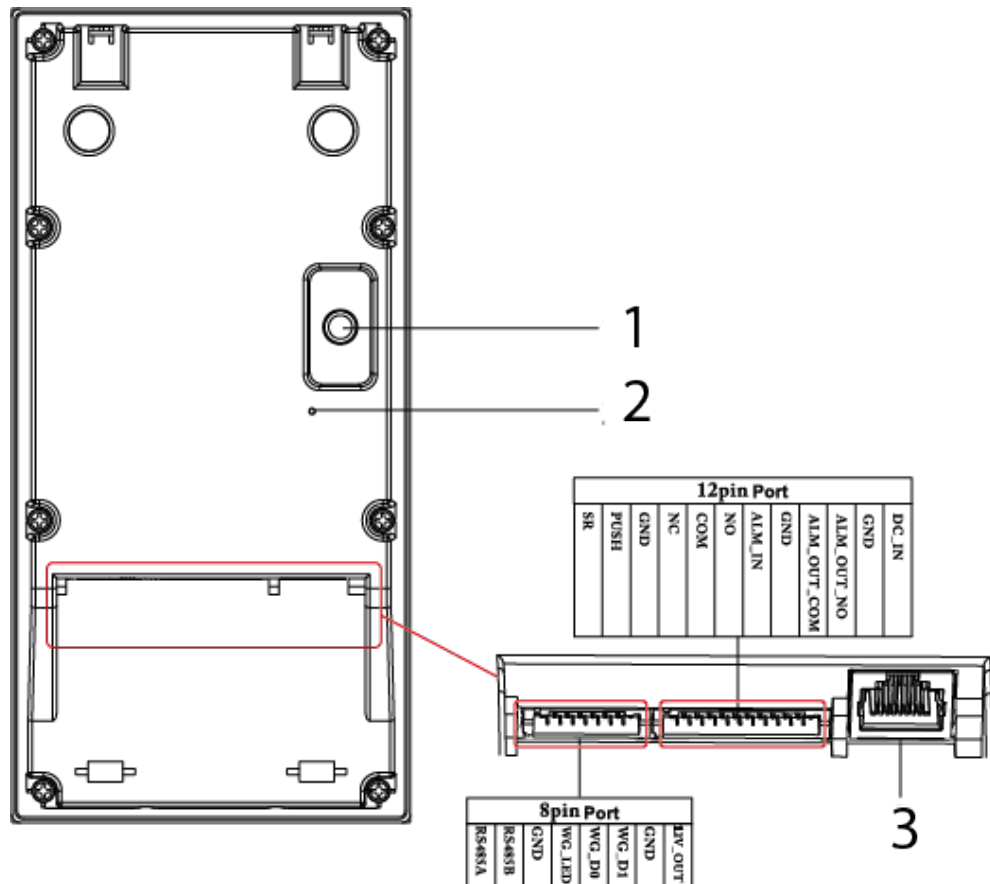


Tabla 2-13 Descripción del panel trasero

No.	Nombre	Descripción
1	Antimanipulación cambiar	Cuando el VTO se quita de la pared a la fuerza, se activará una alarma y la información de la alarma se enviará al centro de gestión.
2	Botón de reinicio	Manténgalo presionado durante 10 s para restablecer todas las configuraciones.
3	Puerto Ethernet	Se conecta al cable Ethernet.

2.6 VTO2211G-P/VTO1201G-P

2.6.1 Panel frontal

Figure 2-14 Panel frontal de VTO2211G/VTO1201G

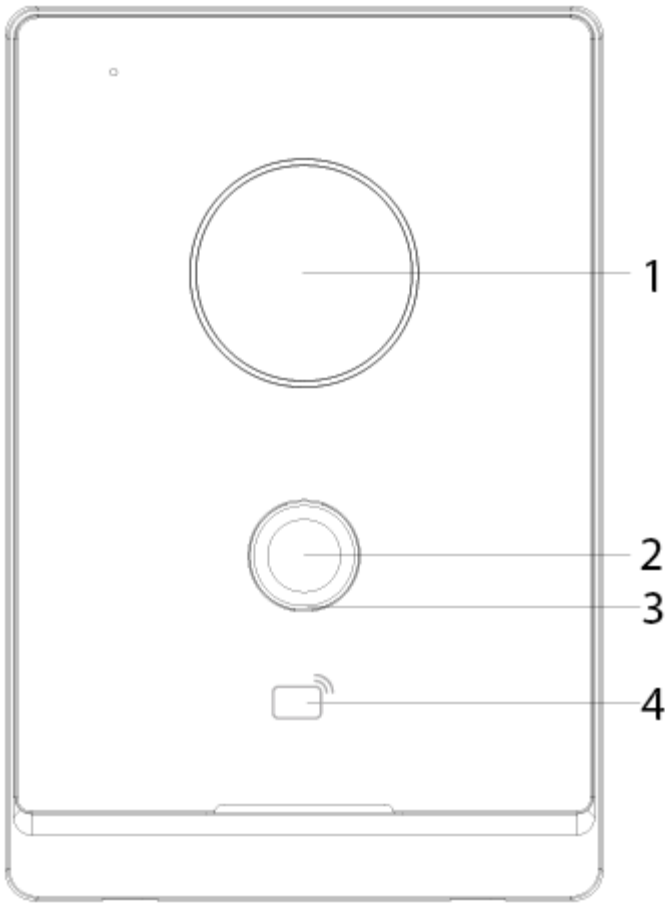


Tabla 2-14 Descripción del panel frontal

No.	Nombre	Descripción
1	Cámara	—
2	Botón de llamada	Llame a los VTH o al centro de gestión.
3	Indicador	● Apagado: el dispositivo está en modo de espera. ● Verde continuo: haciendo una llamada. ● Azul sólido: en una llamada. ● Amarillo-verde: puerta desbloqueada por VTH mientras el VTO está haciendo una llamada. Rojo-azul: puerta desbloqueada por VTH cuando el VTO está en una llamada. ● Respiración azul: Red desconectada.
4	lectura de cartas área	Pase una tarjeta aquí para desbloquear la puerta (solo para VTO2211G-P).

2.6.2 Panel trasero

Figure 2-15 Panel trasero de VTO2211G-P/VTO1201G-P

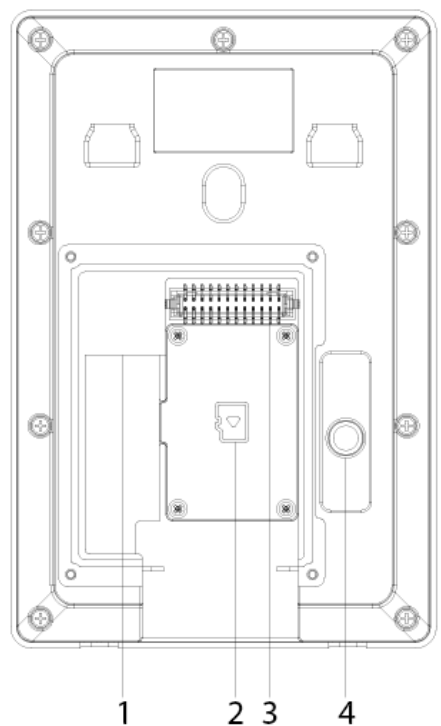
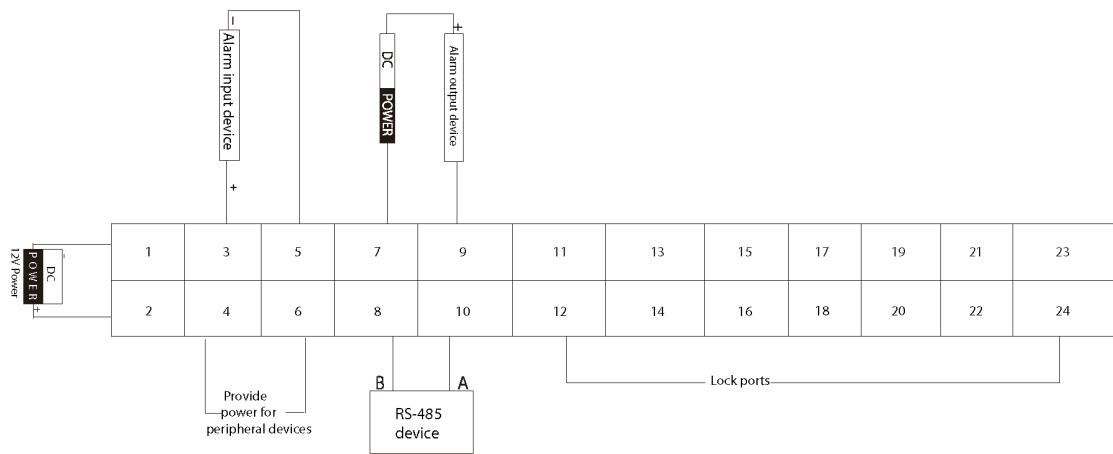


Tabla 2-15 Descripción del panel trasero

No.	Descripción	No.	Descripción
1	puerto de red	3	Puertos
2	tapa de la tarjeta SD	4	Interruptor antimanipulación

Figure 2-16 Conexión de cable VTO2211G-P



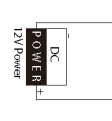
Los puertos 12, 14, 16, 18, 20, 22 y 24 se utilizan para conectarse a las cerraduras.

Tabla 2-16 Descripción del puerto

No.	Nombre	No.	Nombre
1	DC EN-	13	No disponible
2	DC_IN+	14	PUERTA1_COM

No.	Nombre	No.	Nombre
3	ALARMA_EN	15	No disponible
4	+ 12V_SALIDA	dieciséis	PUERTA1_NO
5	TIERRA	17	No disponible
6	TIERRA	18	TIERRA
7	ALARMA_NO	19	No disponible
8	RS485B	20	PUERTA1_FB
9	ALARMA_COM	21	No disponible
10	RS485A	22	TIERRA
11	No disponible	23	No disponible
12	PUERTA1_NC	24	PUERTA1_PUSH

Figure 2-17 Conexión de cable VTO1201G-P

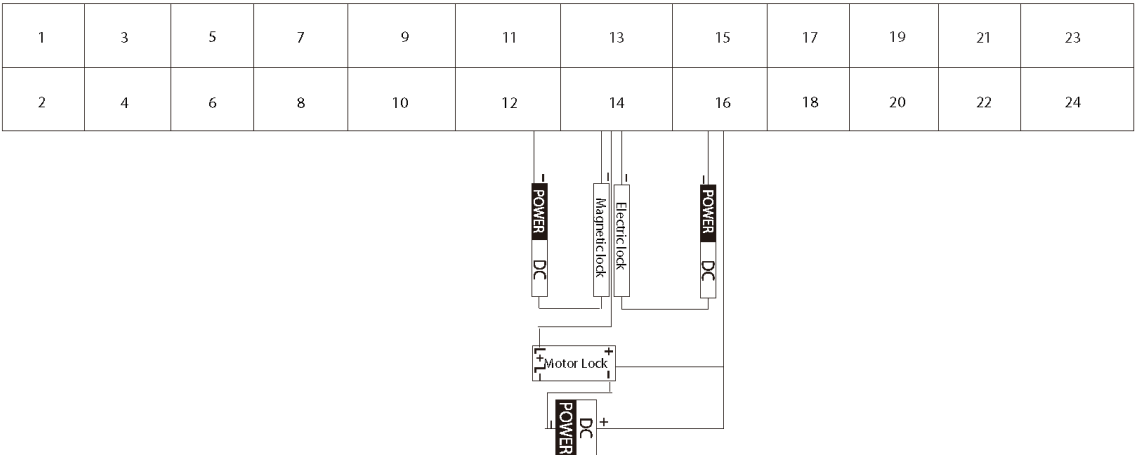


1	3	5	7	9	11	13	15	17	19	21	23
2	4	6	8	10	12	14	16	18	20	22	24

Tabla 2-17 Descripción del puerto

No.	Nombre
1	DC EN-
2	DC_IN+
3-24	función reservada

Figure 2-18 Conexión de cable de bloqueo

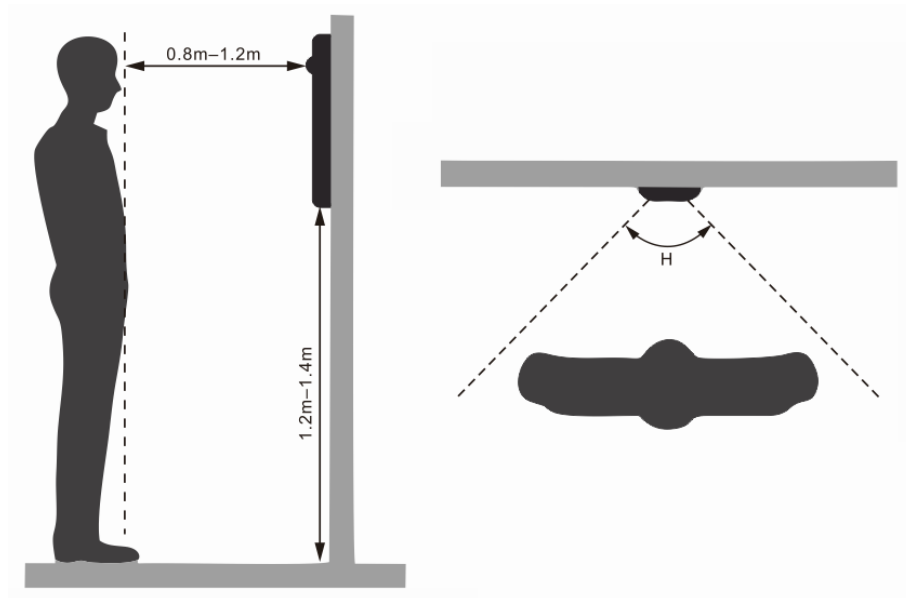


Puede conectar una cerradura magnética o una cerradura eléctrica según sea necesario. Consulte la figura anterior para conocer las reglas de conexión del puerto.

3 Instalación

- La instalación y configuración debe ser realizada por equipos profesionales. Póngase en contacto con el soporte técnico si necesita reparar el dispositivo.
- Consulte la figura a continuación para conocer la posición de instalación. El ángulo de visión horizontal del dispositivo varía según los modelos, y el rostro humano debe apuntar al centro del dispositivo.

Figure 3-1 Posición de instalación



4 Configuración

Este capítulo presenta las configuraciones básicas de los dispositivos VTO y VTH. Consulte el manual del usuario para obtener más detalles.



Las interfaces pueden variar según la versión del software. Prevalecerá la interfaz real.

4.1 Procedimiento



Antes de la configuración, verifique cada dispositivo y asegúrese de que no haya cortocircuito o circuito abierto.

- Step 1** Plan de IP y número (funciona como un número de teléfono) para cada dispositivo.
- Step 2** Configure el VTO. Consulte "4.3 Configuración de VTO".
- Step 3** Configure el VTH. Consulte el manual del usuario de VTH. Compruebe si todos los
- Step 4** ajustes son correctos. Consulte "4.4 Puesta en servicio".

4.2 Herramienta de configuración

Puede descargar la herramienta de configuración "VDPCConfig" y usarla para configurar y actualizar varios dispositivos. Para más detalles, consulte el manual de usuario correspondiente.

4.3 Configuración de VTO

Conecte el VTO a su PC con un cable de red y, para el primer uso, debe crear una nueva contraseña de inicio de sesión para la interfaz web.

4.3.1 Inicialización

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

- Step 1** Encienda el VTO.
- Step 2** Vaya a la dirección IP del VTO en el navegador.



Para iniciar sesión por primera vez, ingrese la IP predeterminada (192.168.1.108). Si tiene varios VTO, nosotros recomendamos cambiar la dirección IP predeterminada (**Red > Básico**) para evitar conflictos.

Figure 4-1 Inicialización del dispositivo

Device Init

1 2 3
One Two Three

Username admin

Password

Low Middle High

Confirm Password

Next

- Step 3** Ingrese y confirme su nueva contraseña, y luego haga clic en **Próximo**. Seleccione **Correo electrónico** e ingrese la dirección de correo electrónico para restablecer la contraseña. Hacer clic **Próximo** y luego haga clic en **OK** para ir a la interfaz de inicio de sesión.

Figure 4-2 Interfaz de inicio de sesión

WEB SERVICE 2.0

Username

Password

Forget Password?

Login

4.3.2 Configuración del número de VTO

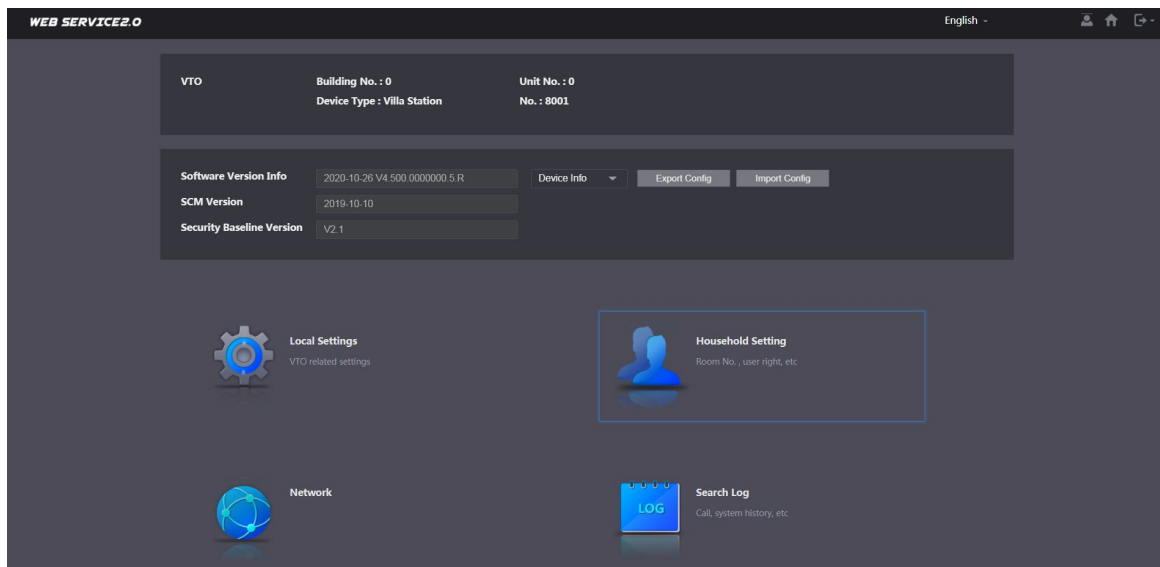
Se pueden usar números para distinguir cada VTO, y recomendamos configurarlo según el número de unidad o edificio.



- Puede cambiar el número de un VTO cuando no funciona como servidor SIP.
- Un número VTO puede contener hasta 5 números y no puede ser el mismo que cualquier número de habitación.

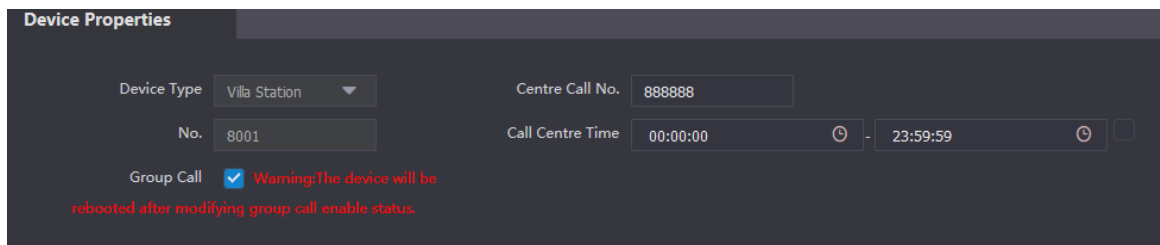
Step 1 Inicie sesión en la interfaz web de VTO.

Figure 4-3 Interfaz principal



Step 2 Seleccione **Configuración local > Básico**.

Figure 4-4 Propiedades del dispositivo

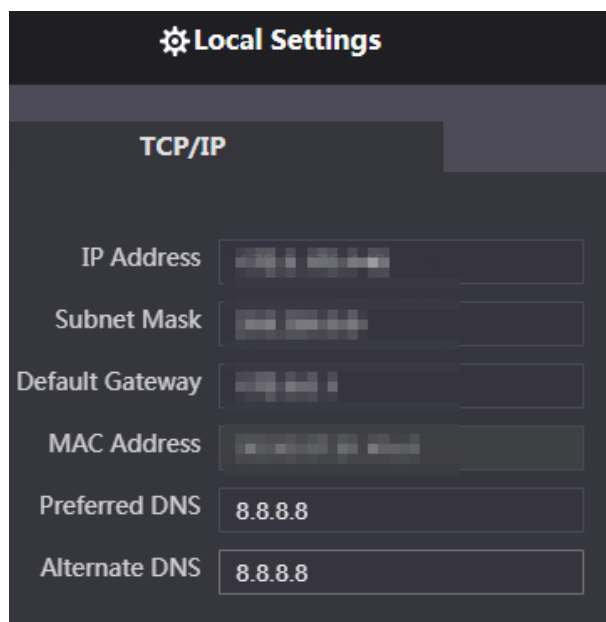


Step 3 Introduzca el número en **No.** y luego haga clic en **Confirmar**.

4.3.3 Configuración de parámetros de red

Step 1 Seleccione **Red > Básico**.

Figure 4-5 Información TCP/IP



Step 2 Ingrese cada parámetro y luego haga clic en **Salvar**.

El VTO se reiniciará automáticamente. Debe agregar la dirección IP de su PC al mismo segmento de red que el VTO para iniciar sesión nuevamente.

4.3.4 Configuración del 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.

Step 1 Seleccione **Red > Servidor SIP**.

Figure 4-6 servidor SIP

Step 2 Seleccione el tipo de servidor según sea necesario.

- Si el VTO actual funciona como servidor SIP, habilite **Servidor SIP** y luego haga clic en **Salvar**. El VTO se reiniciará automáticamente y luego podrá agregar otros VTO y VTH a este VTO. Consulte "4.3.6 Agregar VTO y 4.3.7 Agregar número de habitación".



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

- Si otros VTO funcionan como servidor SIP, configure **Tipo de servidor** como VTO, y luego 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 VTO funciona como servidor SIP. 5080 por ● defecto cuando la plataforma funciona como servidor SIP.
Nombre de usuario	Mantenga el valor predeterminado.
Clave	
Dominio 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 **Tipo de servidor** según sea necesario y, a continuación, consulte el manual correspondiente para obtener más información.

4.3.5 Configuración de número de llamada y llamada de grupo

Para marcar y llamar a un VTO, debe configurar el número de llamada en cada VTO que funciona como número de teléfono.

Step 1 Seleccione **Configuración local > Básico**.

Figure 4-7 Propiedades del dispositivo

Step 2 En el **No.** cuadro de entrada, ingrese el número de habitación al que necesita llamar y luego haga clic en **Confirmar** ahorrar. Repita esta operación en cada interfaz web de estación de puerta de villa (VTO).

En el servidor SIP, puede habilitar la función de llamada grupal. Al llamar a un VTH principal, todas las extensiones VTH también recibirán la llamada.



El VTO se reiniciará después de habilitar o deshabilitar la función de llamada grupal.

Step 3 Inicie sesión en la interfaz web del servidor SIP y luego seleccione **Configuración local > Básico**.

Step 4 Habilitar **Llamada de grupo**, haga clic **Confirmar**, y luego el VTO se reiniciará.

4.3.6 Adición de VTO

Puede agregar VTO al servidor SIP, y todos los VTO conectados al mismo servidor SIP pueden hacer videollamadas entre sí. Esta sección es aplicable cuando un VTO funciona como servidor SIP, y si está utilizando otros servidores como servidor SIP, consulte el manual correspondiente para la configuración detallada.

Step 1 Inicie sesión en la interfaz web del servidor SIP y luego seleccione **Configuración del hogar > Gestión del número de VTO**.

Figure 4-8 Gestión de número de VTO

Step 2 Hacer clic **Agregar**.

Figure 4-9 Agregar VTO

Step 3 Configure los parámetros.



Se debe agregar el servidor SIP.

Tabla 4-2 Agregar estaciones de puerta (VTO)

Parámetro	Descripción
No. de registro	número VTO. Consulte "4.3.2 Configuración del número de VTO".
Contraseña de registro	Mantenga el valor predeterminado.
construir no.	Disponible solo cuando otros servidores funcionan como servidor SIP.
Numero de unidad.	
Dirección IP	Dirección IP de VTO.
Nombre de usuario	Nombre de usuario y contraseña de inicio de sesión de la interfaz web de VTO.
Clave	

Step 4 Hacer clic **Salvar**.

4.3.7 Agregar número de habitación

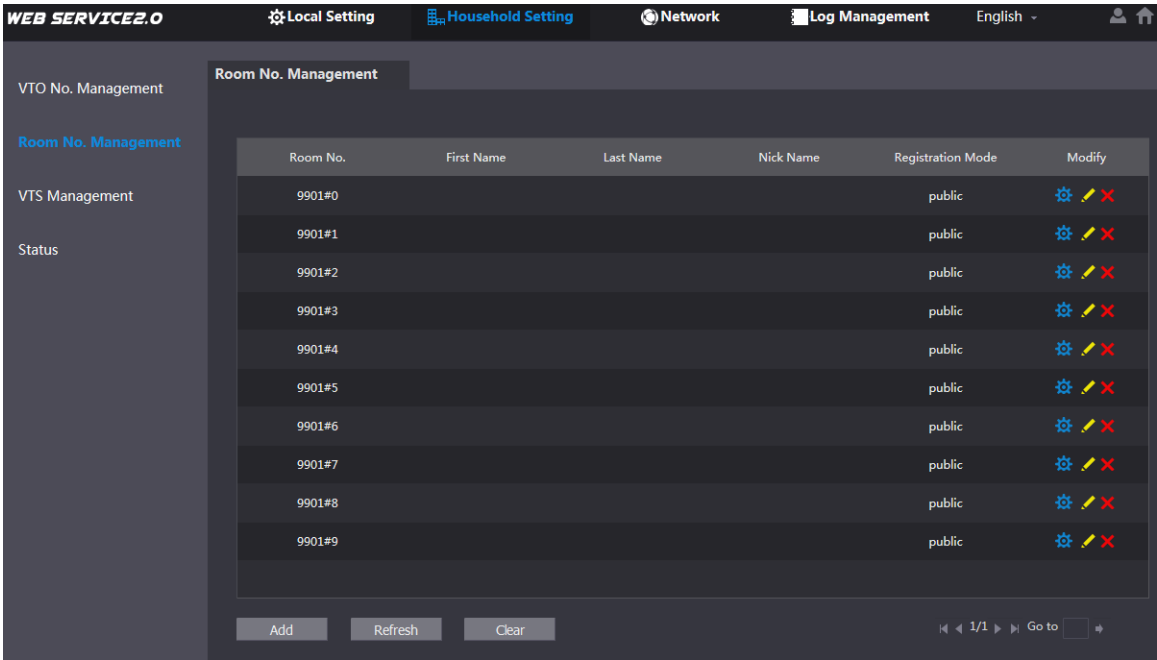
Puede agregar números de habitación al servidor SIP y luego configurar el número de habitación en los VTH para conectarlos a la red. Esta sección es aplicable cuando un VTO funciona como servidor SIP, y si utiliza otros servidores como servidor SIP, consulte el manual correspondiente para la configuración detallada.



El número de habitación puede contener 6 dígitos de números o letras o su combinación como máximo, y no puede ser igual a ningún número de VTO.

Step 1 Inicie sesión en la interfaz web del servidor SIP y luego seleccione **Configuración del hogar > Gestión del número de habitación**.

Figure 4-10 Gestión del número de habitación



Step 2 Hacer clic **Agregar**.

Figure 4-11 Añadir un número de habitación individual

Add

First Name

Last Name

Nick Name

Room No.

Registration Mode

public

Registered Password

Username

Card No.

Modify

No data...

Issue Card

Save

Cancel

Step 3 Configurar la información de la habitación.

Tabla 4-3 Información de la habitación

Parámetro	Descripción
Primer nombre	Información utilizada para diferenciar cada habitación.
Apellido	
Apodo	
Habitación no.	Número de habitación.

Parámetro	Descripción
	 - Cuando hay múltiples VTH, el número de habitación para el VTH principal debe terminar con #0, y los números de habitación para VTH de extensión con #1, #2... - Puede configurar hasta 9 VTH de extensión para un VTH principal.
Modo de registro	Seleccione público .
Contraseña registrada	Mantenga el valor predeterminado.

Step 4 Hacer clic **Salvar**.

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

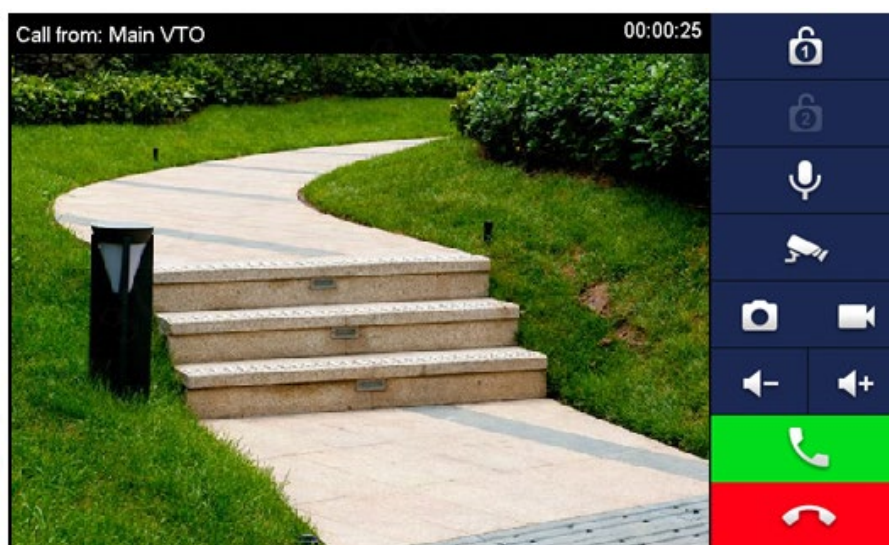
4.4 Puesta en marcha

4.4.1 VTO llamando a VTH

Step 1 Marque un número de habitación en el VTO.

Step 2 Grifo  en el VTH para contestar la llamada.

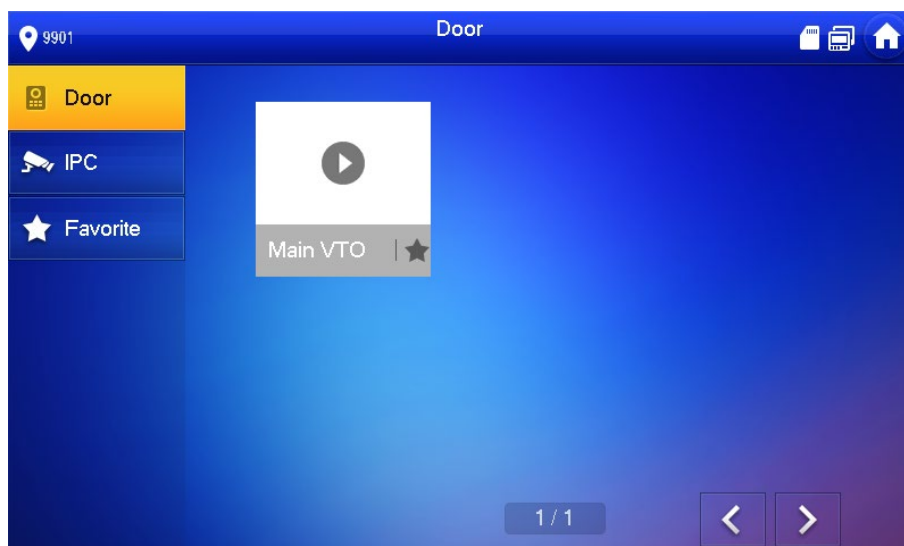
Figure 4-12 Pantalla de llamada



4.4.2 Monitoreo de VTH VTO

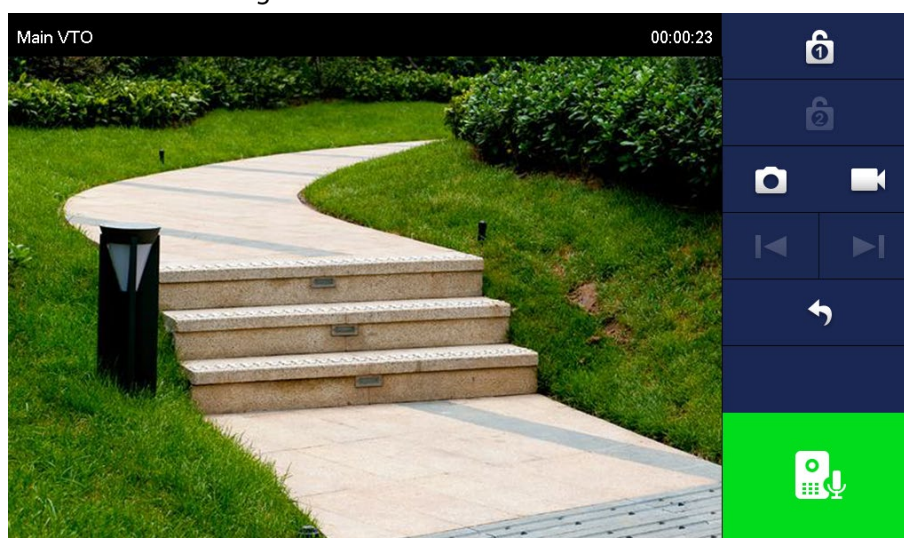
Step 1 En la interfaz principal del VTH, seleccione **Supervisar > Puerta**.

Figure 4-13 Puerta



Step 2 Seleccione un VTO.

Figure 4-14 Monitoreo de video



5 EasyViewer Plus

EasyViewer Plus (en adelante, la "aplicación") le permite administrar dispositivos, reproducir videos, desbloquear puertas y más.

Antes de agregar el VTO a la aplicación, debe conectar el VTO al enrutador a través de Wi-Fi, o conectar el VTO al enrutador usando un interruptor y luego cambiar manualmente la dirección IP del VTO a la misma red que el enrutador si DHCP no es compatible.

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

Appendix 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 en 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.

Acciones obligatorias que se deben tomar para la seguridad básica de la red del dispositivo: 1. Use contraseñas seguras

Consulte las siguientes sugerencias para establecer contraseñas:

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

2. Actualice el firmware y el software del cliente a tiempo

- De acuerdo con el procedimiento estándar en la industria tecnológica, 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 oportuna de las actualizaciones de firmware lanzadas por el fabricante.
- Le sugerimos que descargue y utilice la última versión del software del cliente.

Recomendaciones "agradables de tener" para mejorar la seguridad de la red de su dispositivo: 1. Protección física

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

2. Cambie las contraseñas regularmente

Le sugerimos que cambie las contraseñas regularmente para reducir el riesgo de ser adivinadas o descifradas.

3. Establezca y actualice la información de restablecimiento de contraseñas a tiempo

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 de protección de contraseña. Si la información cambia, modifíquela a tiempo. Al establecer preguntas de protección de contraseña, se sugiere no utilizar aquellas que se pueden adivinar fácilmente.

4. Habilitar bloqueo de cuenta

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

5. Cambiar HTTP predeterminado y otros puertos de servicio

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

8. Asigne cuentas y privilegios de manera razonable

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

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 los riesgos.

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

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

10. Transmisión encriptada de audio y video

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

Recordatorio: la transmisión encriptada causará cierta pérdida en la eficiencia de la transmisión.

11. Auditoría segura

- Verifique a los usuarios en línea: le sugerimos que verifique a los usuarios en línea regularmente para ver si el dispositivo está conectado sin autorización.
- Verifique el registro del dispositivo: al ver los registros, puede conocer las direcciones IP que se usaron 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, se recomienda habilitar la función de registro de red para asegurarse de que los registros críticos se sincronizan 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 mapeo de puertos del enrutador para evitar el acceso directo a los dispositivos de intranet desde una red externa.
- La red debe dividirse y aislarse de acuerdo con las necesidades reales de la red. Si no hay requisitos de comunicación entre dos subredes, se sugiere usar VLAN, GAP de red y otras tecnologías para dividir la red, a fin de lograr el efecto de aislamiento de la red.
- Establezca 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 que pueden acceder al dispositivo.