

VTO modular (VTO4202F-P)

Guía de inicio rápido

V1.0.1

Prefacio

General

Este documento presenta principalmente la función del producto, la estructura, la red, el proceso de montaje, el proceso de depuración y las operaciones web de VTO modular.

Modelos

VTO4202F-MK, VTO4202F-MB1, VTO4202F-MB2, VTO4202F-MB5, VTO4202F-MR, VTO4202F-MS,
VTO4202F-MF, VTO4202F-ML, VTO4202F-MA, VTO4202F-P

Actualización de dispositivo

No corte la fuente de alimentación durante la actualización del dispositivo. La fuente de alimentación se puede cortar solo después de que el dispositivo haya completado la actualización y se haya reiniciado.

Las instrucciones de seguridad

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

Palabras de advertencia	Sentido
 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 la revisión	Tiempo de liberación
V1.0.0	Primer lanzamiento.	Julio de 2019

Aviso de protección de privacidad

Como usuario del dispositivo o controlador de datos, puede recopilar datos personales de otras personas, como rostro, huellas dactilares, número de placa del automóvil, dirección de correo electrónico, número de teléfono, GPS, etc. 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, las siguientes: Proporcionar una identificación clara y visible para informar al sujeto de datos la existencia de un área de vigilancia y proporcionar información relacionada. contacto.

Acerca del manual

- El manual es solo para referencia. Si hay inconsistencia entre el manual y el producto real, prevalecerá el producto real.
- No nos hacemos responsables de ninguna pérdida causada por las operaciones que no cumplan con el manual. El manual se actualizará de acuerdo con las últimas leyes y regulaciones 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 actualizado y la documentación complementaria. Todavía puede haber desviaciones en los datos técnicos, la 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 de lectura convencional si no puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas comerciales registradas y los nombres de empresas que aparecen en el manual son propiedad de sus respectivos propietarios.
- Visite nuestro sitio web, comuníquese con el proveedor o con el servicio de atención al cliente si se produce algún problema al utilizar el dispositivo.
- Si hay alguna duda o controversia, consulte nuestra explicación final.

Advertencias y medidas de seguridad importantes

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

Requisito de funcionamiento

- No coloque ni instale el dispositivo en un área expuesta a la luz solar directa o cerca de un dispositivo generador de calor.
- No instale el dispositivo en un área húmeda, polvorienta o fuliginosa.
- Mantenga su instalación horizontal, o instálelo en lugares estables, y evite que se caiga.
- No gotee ni salpique líquidos sobre el dispositivo; No coloque sobre el dispositivo nada que contenga líquidos, para evitar que los líquidos fluyan hacia el dispositivo.
- Instale el dispositivo en lugares bien ventilados; no bloquee su abertura de ventilación. Utilice el dispositivo solo dentro del rango nominal de entrada y salida.
- No desmonte el dispositivo de forma arbitraria.
- Transporte, use y almacene el dispositivo dentro del rango permitido de humedad y temperatura.

Requisitos de energía

- El producto utilizará cables eléctricos (cables de alimentación) recomendados por esta área, que se utilizarán dentro de su especificación nominal.
- Utilice una fuente de alimentación que cumpla con los requisitos de SELV (voltaje de seguridad muy bajo) y suministre energía con un voltaje nominal que cumpla con la Fuente de energía limitada en IEC60950-1. Para conocer los requisitos específicos de la fuente de alimentación, consulte las etiquetas del dispositivo.
- El acoplador de electrodomésticos es un dispositivo de desconexión. Durante el uso normal, mantenga un ángulo que facilite la operación.

Tabla de contenido

Prólogo	YO Advertencias y
salvaguardias importantes	III 1 Resumen
.....	1
1.1 Introducción	1
1.2 Función	1
2 Estructura	2
2.1 Módulo de cámara.....	2
2.2 Módulo de luz indicadora	3
2.3 Módulo de audio	4
2.4 Módulo de botones	4
2.5 Módulo de teclado (con Braille)	6
2.6 Módulo de deslizamiento de tarjetas	6
2.7 Módulo de huellas dactilares	7
2.8 Módulo de visualización	7
2.9 Módulo en blanco	8
3 Instalación	9
3.1 Instalación en / en la pared	9
3.1.1 Instalación en la pared	9
3.1.2 Instalación en la pared	11
3.2 Montaje horizontal / vertical	12
3.2.1 Montaje horizontal	12
3.2.2 Montaje vertical	13
3.3 Conexión en cascada	13
4 Configuración	14
4.1 Proceso de configuración	14
4.2 Configurando VTO	14
4.2.1 Inicialización	14
4.2.2 Configuración del número VTO	15
4.2.3 Configuración de parámetros de red	dieciséis
4.2.4 Selección de servidores SIP	17
4.2.5 Agregar dispositivos VTO	20
4.2.6 Agregar número de habitación	21
4.2.7 Módulo de configuración	23
4.3 Verificación de la configuración	26
4.3.1 Llamar a VTH desde VTO	26
4.3.2 Haciendo Monitor desde VTH	27
Appendix 1 Recomendaciones de ciberseguridad	29

1.1 Introducción

El VTO modular consta de un módulo de cámara, un módulo de luz indicadora, un módulo de un botón, un módulo de dos botones, un módulo de cinco botones, un módulo de teclado, un módulo de deslizamiento de tarjetas, un módulo de huellas digitales, un módulo de audio y un módulo de pantalla. El módulo de cámara y el módulo de audio son indispensables, mientras que se pueden seleccionar otros módulos según sea necesario.

La combinación de VTO modular, VTH, VTS y plataforma crea un sistema de comunicación de voz / video.

1.2 Función

- Videollamada: realice videollamadas en el VTO modular con usuarios de VTH. Llamada grupal:
- llame a varios usuarios de VTH en un VTO simultáneamente.
- Ser monitoreado: los videos capturados por el VTO se pueden ver en tiempo real; Admite transmisión de video de 6 canales como máximo.
- Llamada de emergencia: presione la tecla para llamar al Centro en caso de una emergencia. Desbloqueo: Tarjeta,
- huella digital, contraseña y desbloqueo remoto.
- Alarma: admite alarma de manipulación, alarma de sensor de puerta y alarma de desbloqueo de contraseña de coacción. La información de alarma se puede enviar al Centro de gestión.
- Búsqueda de registros: se pueden buscar registros de llamadas, registros de alarma y registros de desbloqueo.

2 Estructura

2.1 Módulo de cámara

Figure 2-1 Módulo de cámara (panel frontal)

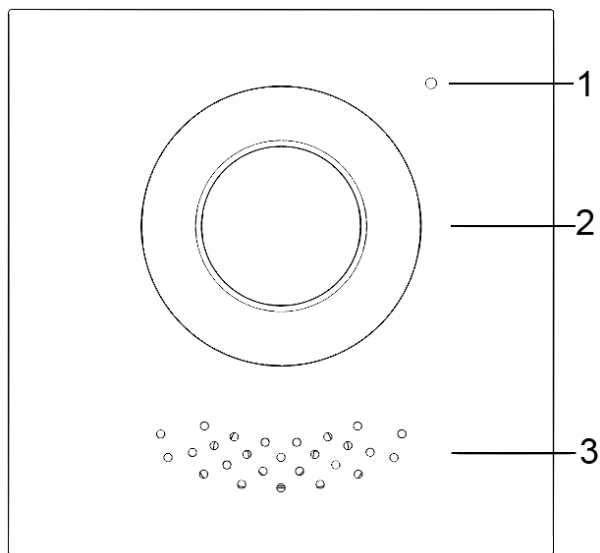


Tabla 2-1 Descripción del módulo de la cámara (panel frontal)

No.	Nombre	Descripción
1	Micrófono	Entrada de audio.
2	Cámara	Supervise el área frente a la puerta.
3	Altavoz	Salida de audio.

Figure 2-2 Módulo de cámara (panel trasero)

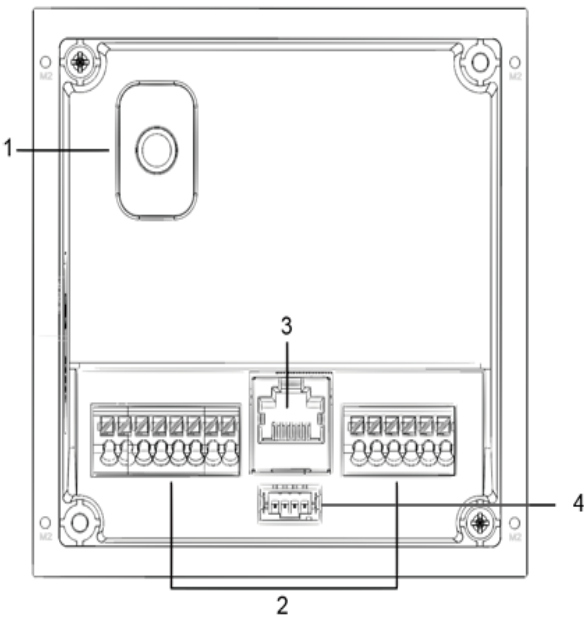
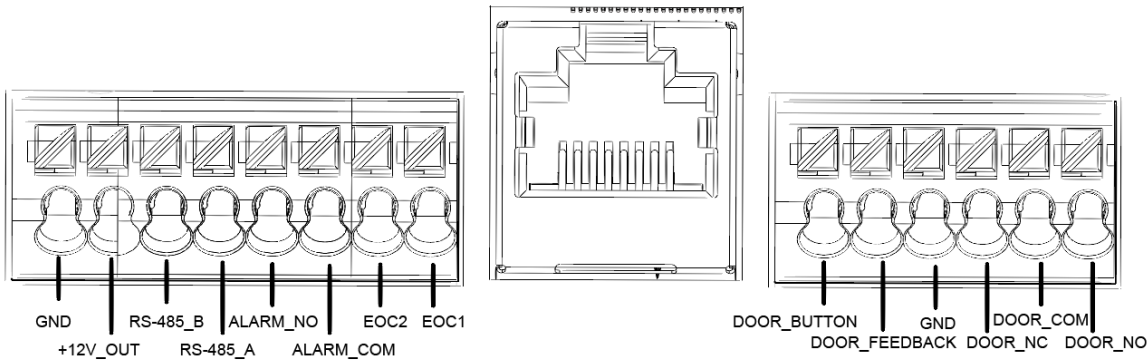


Tabla 2-2 Descripción del módulo de la cámara (panel posterior)

No.	Nombre	Descripción
1	Manosear cambiar	Cuando el VTO se separa a la fuerza de la pared, se emitirá un sonido de alarma y la información de alarma se enviará al centro de gestión.
2	Puerto de usuario	Proporcione un puerto de alimentación, un puerto de bloqueo, un puerto de retroalimentación del sensor de la puerta y un puerto de botón de salida para conectar la fuente de alimentación, el bloqueo de control eléctrico, el bloqueo del solenoide y el botón de salida. Vea la Figura 2-3.
3	Ethernet Puerto	Conectado a cables de red.
4	cascada conexión Puerto	 En caso de conexión en cascada de varios módulos, los módulos necesitan una conexión en cascada.

Figure 2-3 Puertos de usuario



2.2 Módulo de luz indicadora

Figure 2-4 Módulo de luz indicadora (panel frontal)

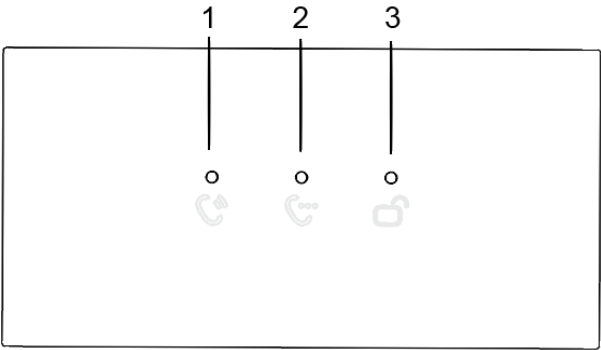


Tabla 2-3 Descripción del módulo de luz indicadora

No.	Nombre	Descripción
1	Indicador de llamada	Indique el estado de la llamada. Indique el
2	Indicador de conversación	estado de conversación. Indica el estado de
3	Indicador de desbloqueo	desbloqueo.

Figure 2-5 Módulo de luz indicadora (panel trasero)

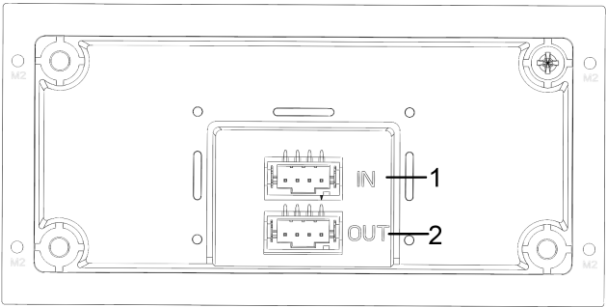


Tabla 2-4 Descripción del módulo de luz indicadora (panel trasero)

No.	Nombre	Descripción
1	Puerto de entrada en cascada	Conectado a otros módulos.
2	Puerto de salida en cascada	

2.3 Módulo de audio



El panel trasero del módulo de audio es el mismo que el panel trasero del módulo de la cámara.

Figure 2-6 Módulo de audio

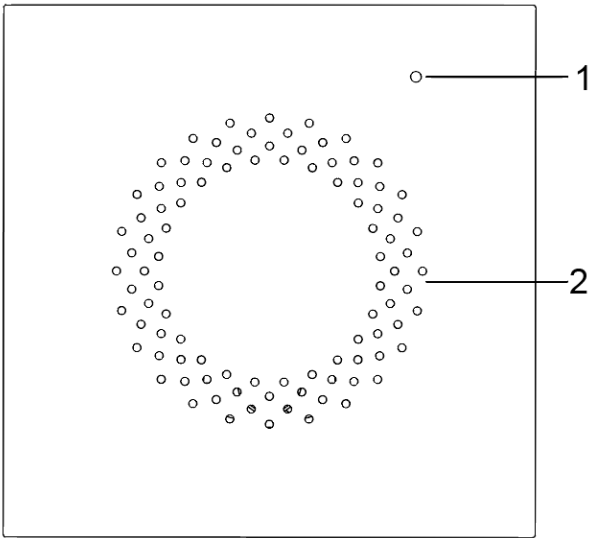


Tabla 2-5 Descripción del módulo de audio

No.	Nombre	Descripción
1	Micrófono	Entrada de audio.
2	Altavoz	Salida de audio.

2.4 Módulo de botones

El módulo de un botón, el módulo de dos botones y el módulo de cinco botones están disponibles. Sus funciones son las mismas, aunque la cantidad de botones es diferente.

Aquí se toma como ejemplo el módulo de cinco botones. Consulte la Figura 2-7 y la Tabla 2-6.

Figure 2-7 Módulo de cinco botones (panel frontal)

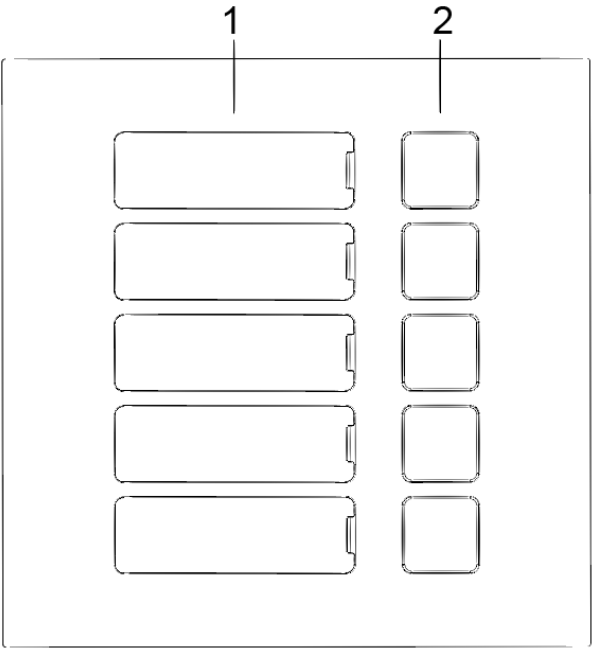


Tabla 2-6 Descripción del módulo de botones (panel frontal)

No.	Nombre	Descripción
1	Directorio de usuarios	Muestra la información del usuario según los botones.
2	Botón de llamada	Llame al VTH y llame al centro de administración (primero debe hacer consultas en la web).

Figure 2-8 Módulo de cinco botones (panel trasero)

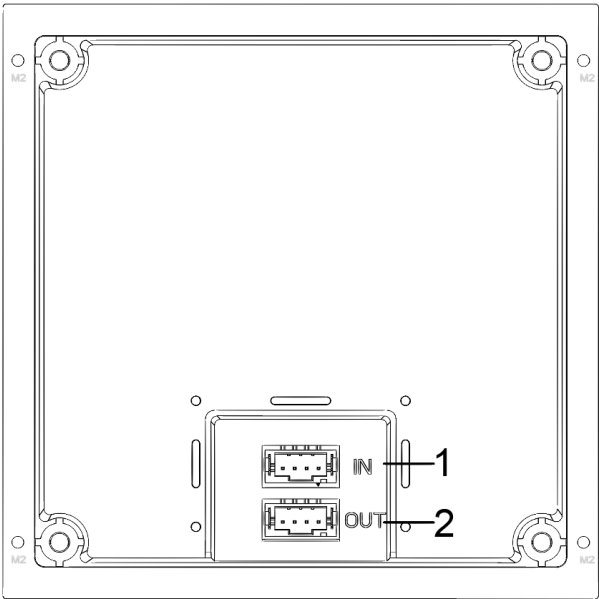


Tabla 2-7 Descripción del módulo de botones (panel posterior)

No.	Nombre	Descripción
1	Puerto de entrada en cascada	Conectado a otros módulos.
2	Puerto de salida en cascada	

2.5 Módulo de teclado (con Braille)



El panel trasero del módulo de teclado es el mismo que el panel trasero del módulo de botones.

Figure 2-9 Módulo de teclado

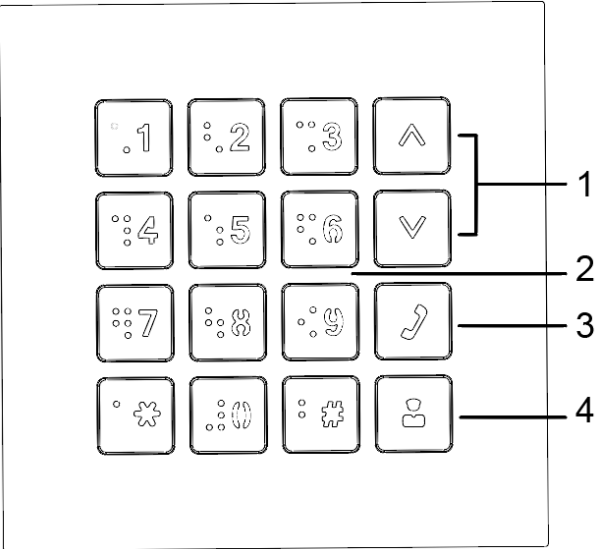


Tabla 2-8 Descripción del módulo de teclado

No.	Nombre	Descripción
1	Botones de selección	Presione los botones para seleccionar el elemento anterior o siguiente. Ingrese la
2	Botón numérico	contraseña y los nombres VTH. Por ejemplo, la contraseña de desbloqueo es 123456. Ingrese "# + 123456 + #". Presione el botón para iniciar una llamada a VTH.
3	Botón de llamada	
4	Centro de gestión de llamadas	Centro de gestión de llamadas.

2.6 Módulo de deslizamiento de tarjetas

Puede deslizar la tarjeta cerca del icono que se muestra en la Figura 2-10.



El panel trasero del módulo de deslizamiento de tarjetas es el mismo que el panel trasero del módulo de botones.

Figure 2-10 Módulo de deslizamiento de tarjetas (mm [pulgadas])



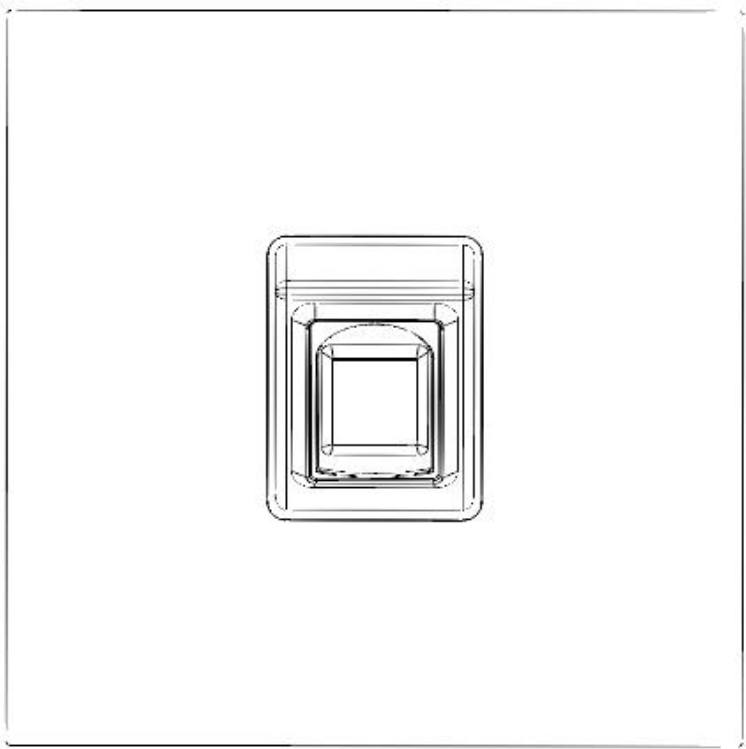
2.7 Módulo de huellas dactilares

El módulo es útil para recopilar huellas dactilares o desbloquear con huella dactilar.



Los paneles traseros del módulo de huellas dactilares y el módulo de botones tienen diferentes posiciones de puerto, pero las funciones del puerto son las mismas.

Figure 2-11 Módulo de huellas dactilares



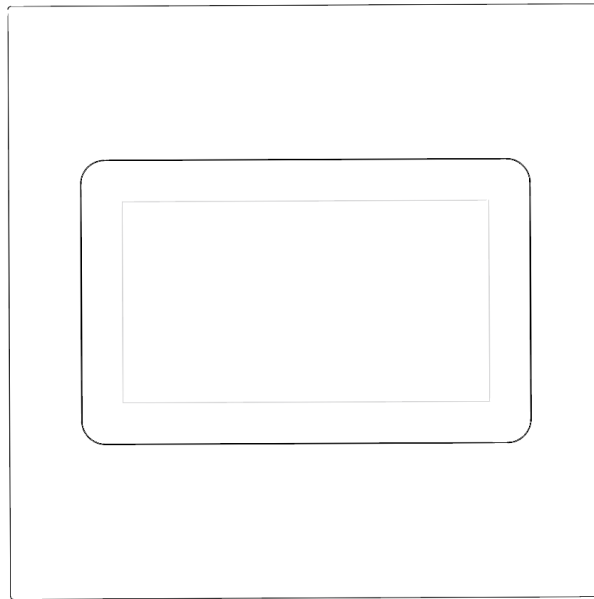
2.8 Módulo de visualización

El módulo de visualización se puede utilizar para mostrar información del usuario.



Los paneles traseros del módulo de visualización y el módulo de botones tienen diferentes posiciones de puerto, pero las funciones de puerto son las mismas.

Figure 2-12 Módulo de visualización



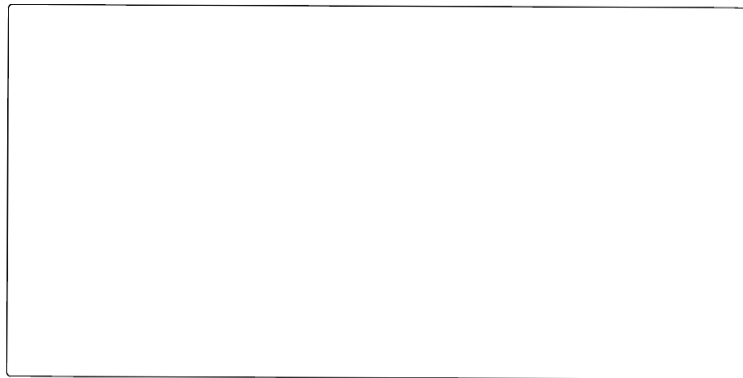
2.9 Módulo en blanco

El módulo en blanco se puede utilizar para una apariencia más atractiva cuando hay espacio adicional.



Los paneles traseros del módulo en blanco y el módulo de botones tienen diferentes posiciones de puerto, pero las funciones del puerto son las mismas.

Figure 2-13 Módulo en blanco



3 Instalación

El VTO modular admite el montaje de dos módulos y tres módulos, y puede montarlo horizontal o verticalmente. Dependiendo de las condiciones reales de la superficie de instalación, puede instalar el VTO en la pared o en la pared.

Esta sección toma el montaje de 3 módulos, por ejemplo.



- Las tarjetas de visita y la cubierta de la tarjeta se incluyen en el paquete de forma predeterminada.
- Al encender después del montaje, asegúrese de que todos los módulos estén conectados; de lo contrario, es posible que los módulos no funcionen normalmente.
- Antes de instalar la caja de montaje en superficie y la caja de montaje empotrada, los cables en la pared deben pasar por el soporte o la caja de montaje.

3.1 Instalación en la pared

3.1.1 Instalación en la pared

Step 1 Taladre orificios de acuerdo con las posiciones de los orificios de la caja de montaje y coloque el tubo de expansión en su lugar.

Step 2 Fije la caja de montaje a la pared con tornillos ST4 × 25. Fije el panel trasero en

Step 3 la caja de montaje con tornillos M2 × 8. Conecte los cables. Consulte "2

Step 4 Estructura".

Step 5 Fije los módulos en el panel trasero con tornillos M3 × 8.

Step 6 Aplique pegamento a los espacios entre la caja de montaje y la pared.

Step 7 Escriba el número de habitación o el nombre de usuario en la tarjeta de visita e insértelo en el directorio de usuarios.

Step 8 Aplique sellador de silicona en los espacios entre el dispositivo y la pared.

Figure 3-1 Aplicar sellador de silicona a los espacios

Apply silicone sealant to gaps between the device and the wall.

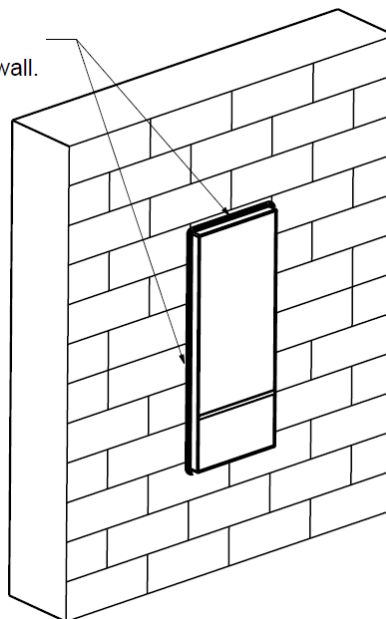
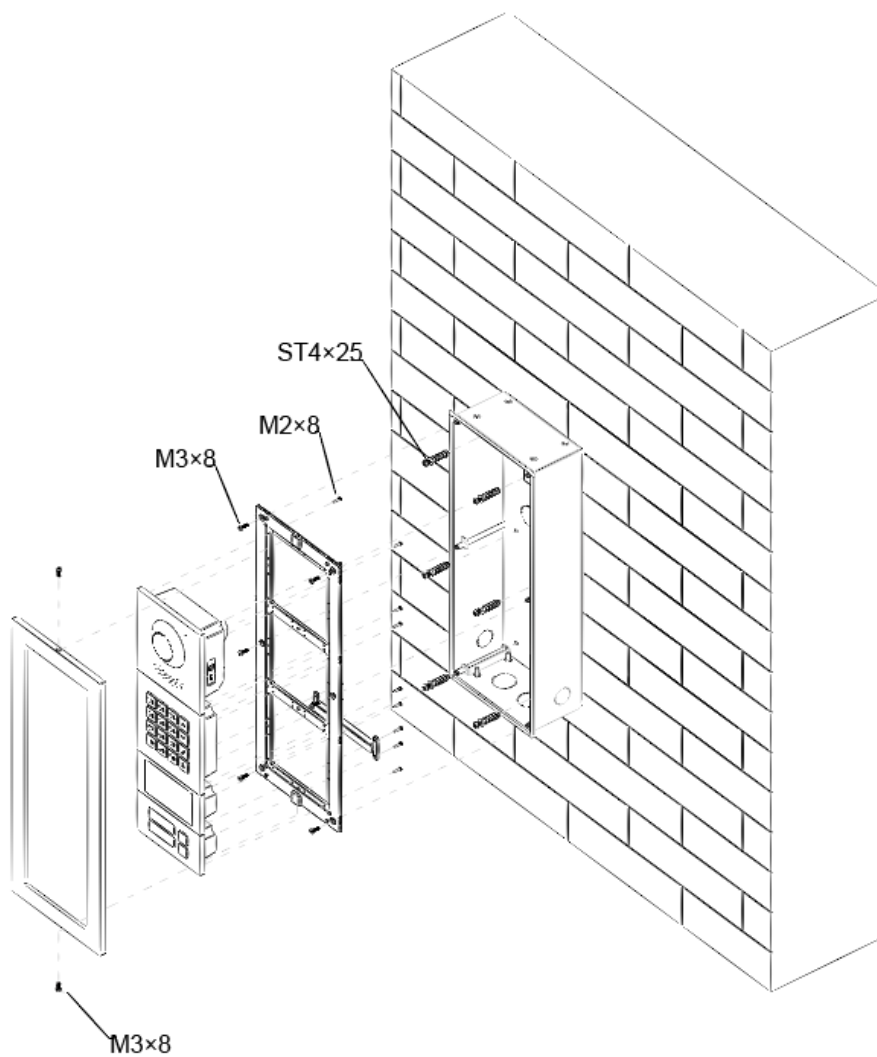


Figure 3-2 Instalación en la pared



3.1.2 Instalación en la pared

Step 1 Haz un agujero en la pared.



- Para el montaje de 2 módulos, la dimensión del orificio rectangular es de 126 mm × 226 mm a 128 mm × 228 mm.
- Para el montaje de 3 módulos, la dimensión del orificio rectangular es de 126 mm × 326 mm a 268 mm × 329 mm.

Step 2 Coloque la caja de montaje en la pared con tornillos ST4 × 25; asegúrese de que el borde de la caja se adhiera a la pared.

Step 3 Fije el panel trasero en la caja de montaje con tornillos M2 × 8. Conecte los

Step 4 cables. Consulte "2 Estructura".

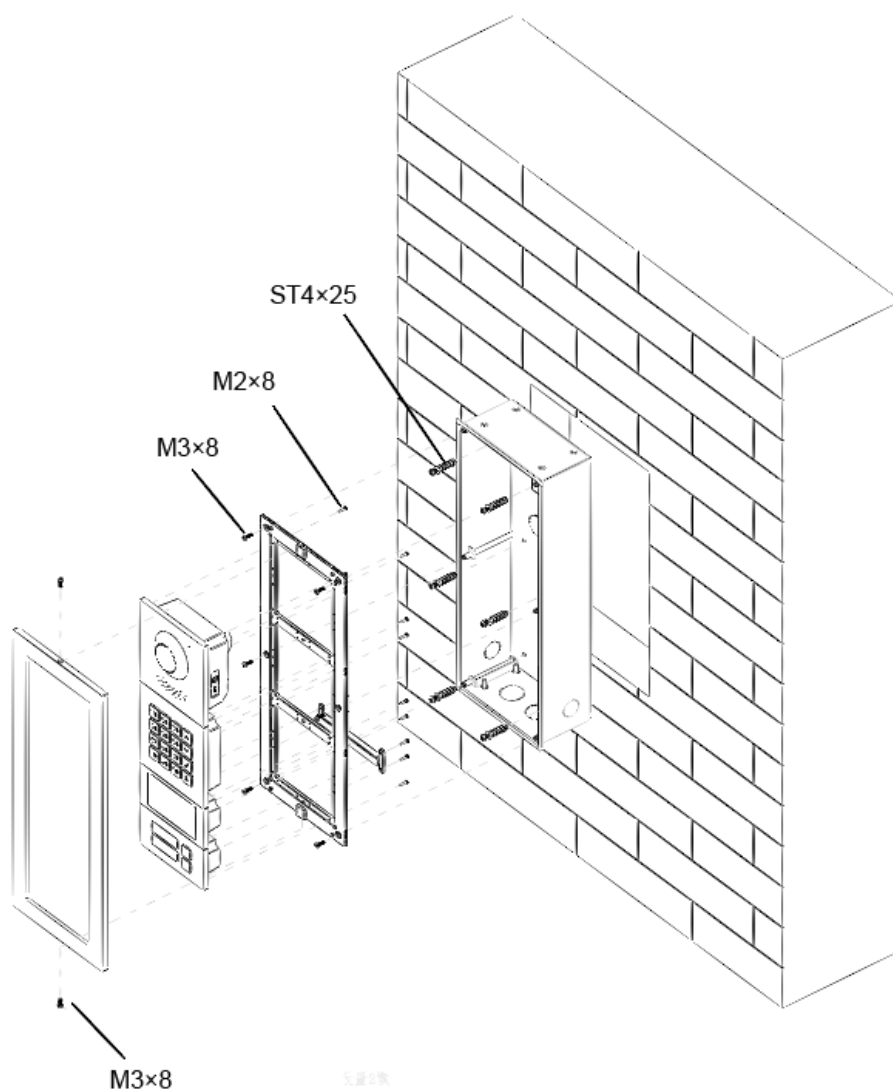
Step 5 Fije cada módulo en el panel trasero con tornillos M3 × 8.

Step 6 Aplique pegamento en los espacios entre el panel trasero, la caja de montaje y la pared.

Step 7 Escriba el número de habitación o el nombre de usuario en la tarjeta de visita e insértelo en el directorio de usuarios.

Step 8 Aplique sellador de silicona en los espacios entre el dispositivo y la pared.

Figure 3-3 Instalación en la pared



3.2 Montaje horizontal / vertical

3.2.1 Montaje horizontal

Figure 3-4 Montaje horizontal (1)

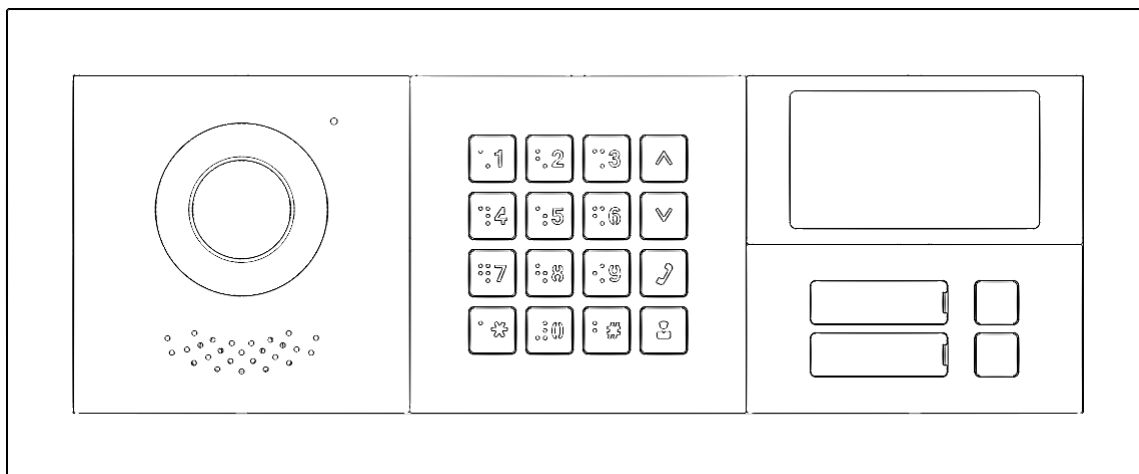
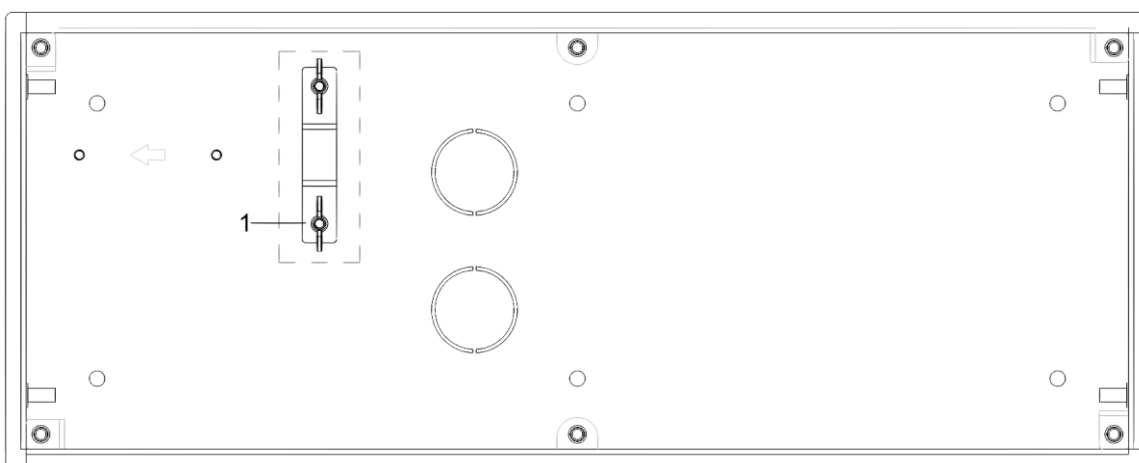


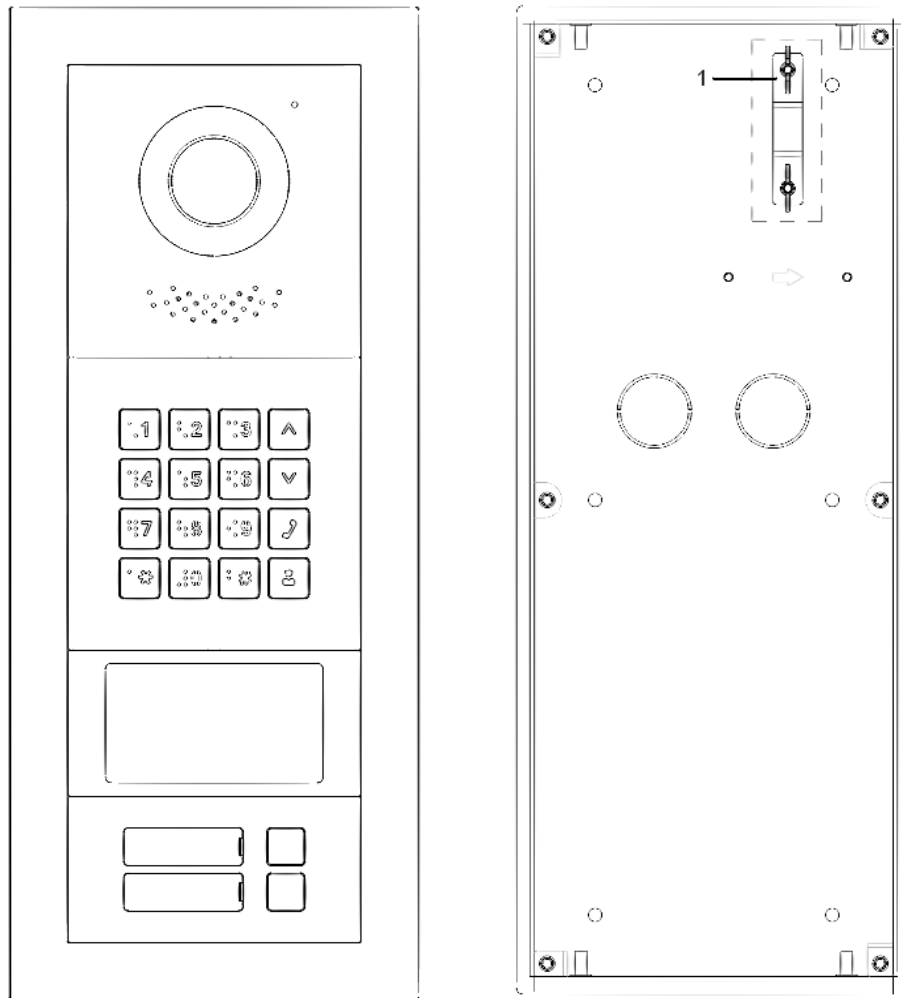
Figure 3-5 Montaje horizontal (2)



Cuando el VTO está montado horizontalmente, asegúrese de que el interruptor de sabotaje en el panel trasero (marcado con "1" en la Figura 3-4) esté retraído de modo que una vez que se desmonte el VTO, se suelte el interruptor de sabotaje y luego se activen las alarmas desencadenadas. La alarma seguirá sonando durante 15 segundos.

3.2.2 Montaje vertical

Figure 3-6 Ilustraciones de montaje vertical

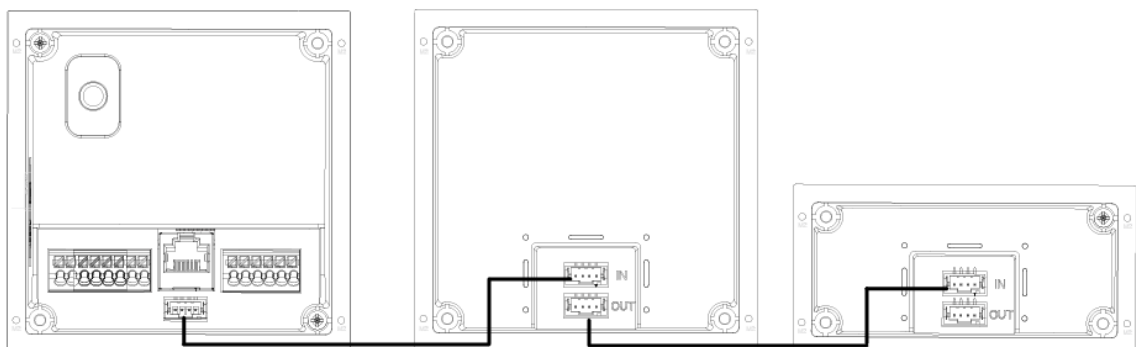


Cuando el VTO esté montado verticalmente, asegúrese de que el interruptor de sabotaje en el panel trasero (marcado con "1" en la Figura 3-5) esté retraído de modo que una vez que se desmonte el VTO, se suelte el interruptor de sabotaje y luego se activen las alarmas desencadenadas. La alarma seguirá sonando durante 15 segundos.

3.3 Conexión en cascada

Para que los módulos funcionen de forma colaborativa, se necesita una conexión en cascada. Vea un ejemplo de conexión en cascada en la Figura 3-7.

Figure 3-7 Conexión en cascada



4 Configuración

Este capítulo presenta cómo inicializar, conectar y realizar configuraciones primarias para los dispositivos VTO y VTH para realizar funciones básicas, incluida la administración, llamadas y monitoreo de dispositivos. Para una configuración más detallada, consulte el Manual del usuario.

4.1 Proceso de configuración



Antes de la configuración, verifique todos los dispositivos y asegúrese de que no haya cortocircuitos o circuitos abiertos en los circuitos.

Step 1 Planifique la dirección IP para cada dispositivo y también planifique el número de unidad y el número de habitación que necesita.

Step 2 Configure VTO. Consulte "4.2 Configuración de VTO".

- 1) Inicialice VTO. Consulte "4.2.1 Inicialización".
- 2) Configure el número VTO. Consulte "4.2.2 Configuración del número VTO".
- 3) Configure los parámetros de la red VTO. Consulte "4.2.3 Configuración de parámetros de red".
- 4) Configure el servidor SIP. Consulte "4.2.4 Selección de servidores SIP".
- 5) Agregue dispositivos VTO al servidor SIP. Consulte "4.2.5 Agregar dispositivos VTO".
- 6) Agregue el número de habitación al servidor SIP. Consulte "4.2.6 Agregar número de habitación". Configure VTH.

Step 3 Consulte el manual de usuario de VTH.

Step 4 Verifique la configuración. Consulte "4.3 Verificación de la configuración".

4.2 Configuración de VTO

Conecte el VTO a su PC con un cable de red y, para iniciar sesión por primera vez, debe crear una nueva contraseña para la interfaz web.

4.2.1 Inicialización

La dirección IP predeterminada de VTO es 192.168.1.108 y asegúrese de que la PC esté en el mismo segmento de red que VTO.

Step 1 Conecte el VTO a la fuente de alimentación y luego enciéndalo.

Step 2 Abra el navegador de Internet en la PC, luego ingrese la dirección IP predeterminada del VTO en la barra de direcciones y luego presione Enter.

los **Inicialización del dispositivo** se muestra la interfaz. Vea la Figura 4-1.

Figure 4-1 Inicialización del dispositivo

Device Init

1 One 2 Two 3 Three

Username admin

Password

Low Middle High

Confirm Password

Next

Step 3 Ingrese y confirme la contraseña, y luego haga clic en **Próximo**.

Se muestra la interfaz de configuración de correo electrónico.

Step 4 Seleccione el **Email** casilla de verificación y luego ingrese su dirección de correo electrónico. Esta dirección de correo electrónico se puede utilizar para restablecer la contraseña y se recomienda finalizar esta configuración. Hacer clic **Próximo**. La inicialización tuvo éxito. Hacer clic **OKAY**.

Step 5

Step 6

los **Iniciar sesión** se muestra la interfaz. Vea la Figura 4-2.

Figure 4-2 Iniciar sesión

WEB SERVICE2.0

Username

Password

Forgot Password?

Login

4.2.2 Configuración del número VTO

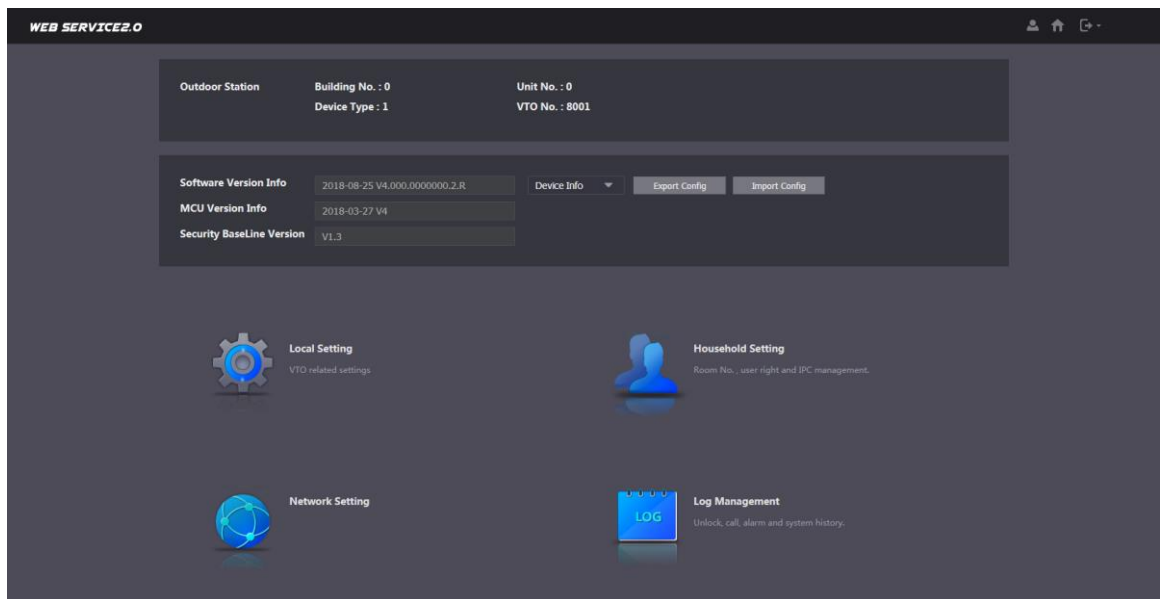
El número de VTO se puede utilizar para diferenciar cada VTO, y normalmente se configura según la unidad o el número de edificio.



- Puede cambiar el número de un VTO cuando no está funcionando como servidor SIP.
- El número VTO puede contener 5 números como máximo y no puede ser el mismo con ningún número de habitación.

Step 1 Inicie sesión en la interfaz web del VTO y luego se muestra la interfaz principal. Vea la Figura 4-3.

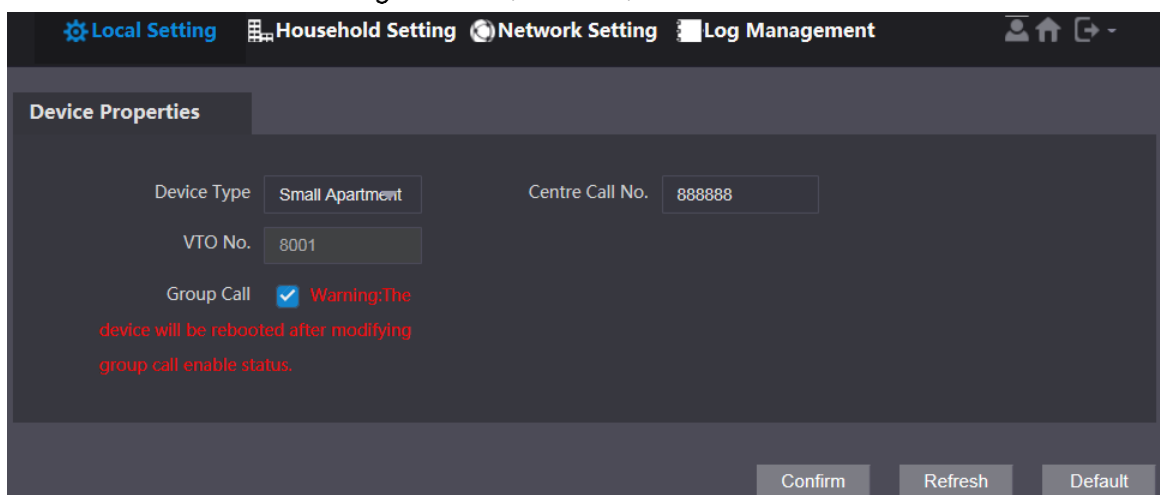
Figure 4-3 Interfaz principal



Step 2 Seleccione Configuración local> Básico.

Se muestran las propiedades del dispositivo. Vea la Figura 4-4.

Figure 4-4 Propiedades del dispositivo



Step 3 En el **VTO No.** cuadro de entrada, ingrese el número VTO que planeó para este VTO, y luego haga clic **Confirmar** ahorrar.

4.2.3 Configuración de parámetros de red

Step 1 Seleccione Configuración de red> Básico.

TCP / IP se muestra la interfaz. Vea la Figura 4-5.

Figure 4-5 Información de TCP / IP

The screenshot shows the 'Network Setting' page of the 'WEB SERVICE 2.0' interface. The 'TCP/IP' tab is selected. On the left, there are links for 'Basic', 'UPnP', 'SIP Server', and 'Firewall'. The main area contains the following configuration fields:

IP Addr.	
Subnet Mask	255.255.0.0
Gateway	
MAC Addr.	
Preferred DNS	8.8.8.8
Alternate DNS	8.8.8.8

Step 2 Ingrese los parámetros de red que planeó y luego haga clic en **Salvar**.

El VTO se reiniciará y deberá modificar la dirección IP de su PC al mismo segmento de red que el del VTO para iniciar sesión nuevamente.

4.2.4 Selección de servidores SIP

El Protocolo de inicio de sesión (SIP) se utiliza para señalar y controlar sesiones de comunicación multimedia en aplicaciones de llamadas de voz y video. Un servidor SIP es una aplicación que proporciona información o instrucciones a un agente de usuario.

- Cuando este VTO u otros VTO funcionan como servidor SIP, seleccione **VTO** desde el **Tipo de servidor** la lista desplegable. Se aplica a un escenario donde solo hay un edificio. Cuando la plataforma (Express / DSS) funciona como servidor SIP, seleccione **Express / DSS** desde el **Tipo de servidor** la lista desplegable. Se aplica a un escenario en el que hay varios edificios o varias unidades.



- Si el VTO que está operando es el servidor SIP, **Edificio número.** y **Numero de unidad.** no se mostrará en el **Propiedades del dispositivo** interfaz en **Configuración local> Básico**.
- Si seleccionó el **Habilitar** casilla de verificación del **Servidor alternativo** en **Configuración de red> Servidor SIP** y guarde la configuración, debe iniciar sesión en la interfaz web nuevamente, y **Edificio número.** y **Numero de unidad.** se mostrará en el **Propiedades del dispositivo** interfaz en **Configuración local> Básico**.

Step 3 Inicie sesión en la página web. En la página de inicio, seleccione **Configuración**

Step 4 **local> Básico**.

los **Propiedades del dispositivo** se muestra la interfaz, consulte la Figura 4-6.

Figure 4-6 Propiedades del dispositivo

- 1) Seleccionar **TCP / IP** desde el **Tipo de sistema** la lista desplegable.



El tipo de sistema predeterminado es un sistema analógico y debe cambiarse a TCP / IP. De lo contrario, no podrá conectarse al VTH.

- 2) Haga clic en **Okay** para guardar la configuración.

- 3) Reinicie el dispositivo manualmente o espere a que se reinicie automáticamente para que la configuración sea efectiva. Inicie sesión en la interfaz

Step 5

web nuevamente.

Step 6

Seleccione Configuración de red> Servidor SIP. los **Servidor SIP** se muestra la interfaz. Vea la Figura 4-7.

Figure 4-7 Servidor SIP (1)

Step 7

Seleccione un servidor SIP.

VTO como servidor SIP

Step 1

Seleccione **Habilitar** detrás **Servidor SIP**.

Step 2

Seleccione **VTO** desde el **Tipo de servidor** la lista desplegable. Configure los

Step 3

parámetros (consulte la Tabla 4-1 para obtener más detalles). Hacer clic **Salvar**.

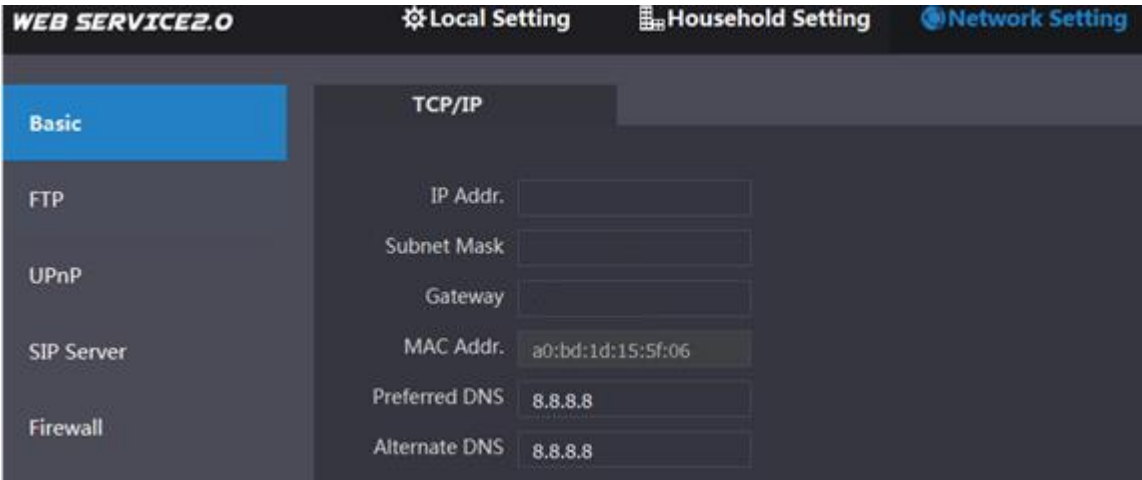
Step 4

El VTO se reiniciará automáticamente.

Plataforma (Express / DSS) como servidor SIP

Step 1 Seleccione Configuración de red> Servidor SIP. los **Servidor SIP** se muestra la interfaz. Vea la Figura 4-8.

Figure 4-8 Servidor SIP (2)



Step 2 Deshabilite el servidor SIP.

Step 3 Seleccione **Express / DSS** desde el **Tipo de servidor** la lista desplegable. Configure los

Step 4 parámetros de acuerdo con la Tabla 4-1.

Tabla 4-1 Descripción de los parámetros del servidor SIP

Parámetro	Descripción
Dirección IP	Dirección IP del servidor SIP.  Cuando la casilla de verificación Servidor alternativo no está seleccionada, se pueden ingresar la Dirección IP, el Nombre de usuario y la Contraseña, y no se puede llamar al VTS a través de VTO.
Puerto	● Es 5060 por defecto cuando otros VTO funcionan como servidor SIP. ● Es 5080 por defecto cuando la plataforma funciona como servidor SIP.
<u>Usuario Contraseña</u>	Utilice el valor predeterminado.
Dominio SIP	● Será VDP cuando otro VTO funcione como servidor SIP. ● Puede ser nulo o mantener el valor predeterminado cuando la plataforma funciona como servidor SIP.
Iniciar sesión Nombre de usuario / Contraseña	Nombre de usuario y contraseña para iniciar sesión en el servidor SIP.
IPAddr alternativo.	Dirección IP del servidor alternativo.
Nombre de usuario alternativo	Nombre de usuario y contraseña para iniciar sesión en el servidor alternativo.
Contraseña alternativa	
IP de VTS alternativa Dirección	Dirección IP del VTS alternativo.
Servidor alternativo	● Después de ingresar la dirección IP alternativa, el nombre de usuario, la contraseña y la dirección IP del VTS, debe

Parámetro	Descripción
	Selecciona el Habilitar casilla de verificación para habilitar el servidor alternativo. Después de haber seleccionado el Habilitar servidor alternativo casilla de verificación, solo puede ingresar la dirección IP del VTS y el VTO se reiniciará.

Step 5 Hacer clic **Okay** para guardar la configuración. El VTO se reiniciará automáticamente.



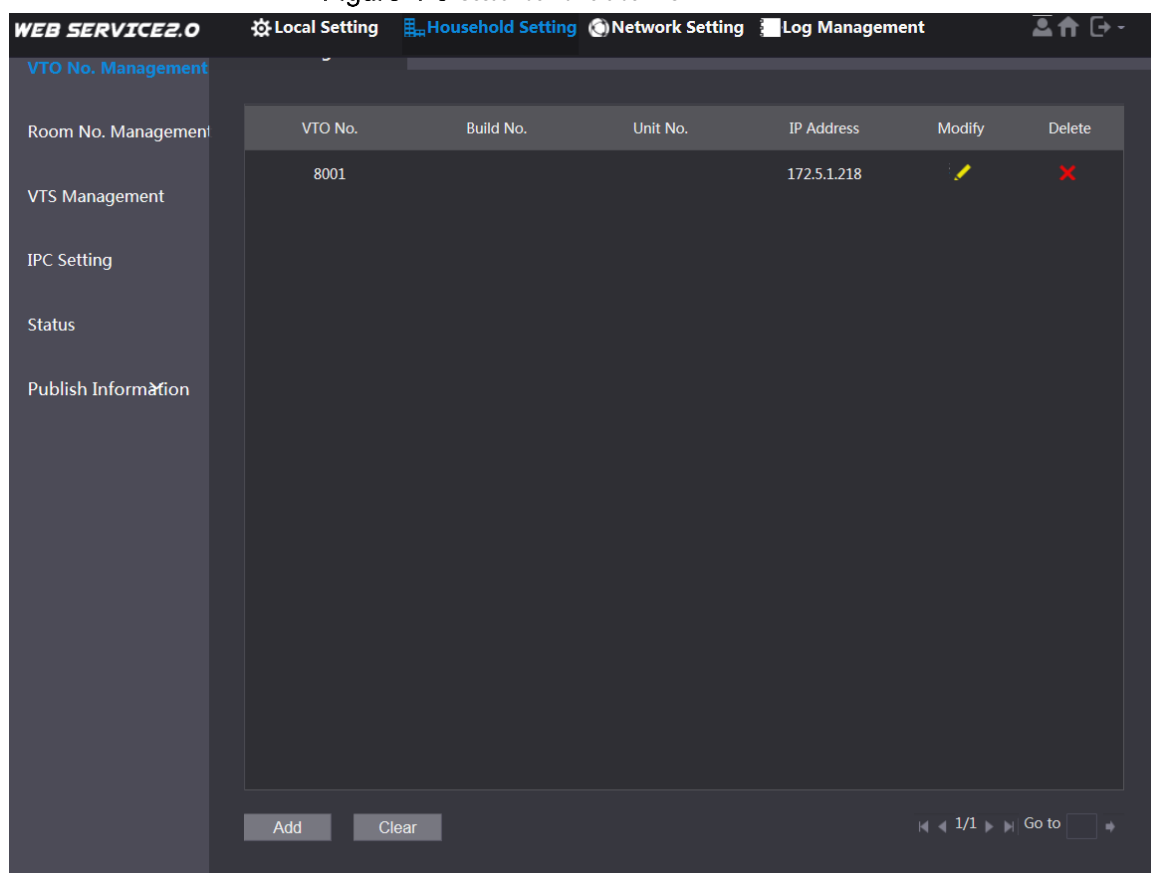
Cuando la plataforma funciona como servidor SIP, si es necesario configurar el número de edificio y el número de unidad de edificio, habilite **Edificio de apoyo** y **Unidad de apoyo** primero.

4.2.5 Agregar dispositivos VTO

Puede agregar dispositivos VTO al servidor SIP y todos los dispositivos VTO conectados al mismo servidor SIP pueden realizar videollamadas entre sí. Esta sección se aplica a la condición en la que un dispositivo VTO funciona como servidor SIP, y si está utilizando otros servidores como servidor SIP, consulte el manual correspondiente para obtener la configuración detallada.

Step 1 Inicie sesión en la interfaz web del servidor SIP y luego seleccione **Configuración del hogar > Gestión de número de VTO**.
los **VTO No. Gestión** se muestra la interfaz. Vea la Figura 4-9.

Figure 4-9 Gestión del número de VTO



Step 2 Hacer clic **Añadir**.

los **Añadir** se muestra la interfaz. Vea la Figura 4-10.

Figure 4-10 Agregar VTO

Step 3 Configure los parámetros y asegúrese de agregar el servidor SIP también. Consulte la Tabla 4-2.

Tabla 4-2 Configuración de VTO

Parámetro	Descripción
Rec No.	El número de VTO que configuró para el VTO de destino. Consulte los detalles en "4.2.2 Configuración del número VTO".
Registrar contraseña	Mantener el valor predeterminado.
Construir No.	Disponible solo cuando otros servidores funcionan como servidor SIP.
Numero de unidad.	
Dirección IP	La dirección IP del VTO de destino.
Nombre de usuario	El nombre de usuario y la contraseña para la interfaz web del VTO de destino.
Contraseña	

Step 4 Hacer clic **Salvar**.

4.2.6 Agregar número de habitación

Puede agregar el número de habitación planificado al servidor SIP y luego configurar el número de habitación en los dispositivos VTH para conectarlos a la red. Esta sección se aplica a la condición en la que un dispositivo VTO funciona como servidor SIP, y si utiliza otros servidores como servidor SIP, consulte el manual correspondiente para obtener la configuración detallada.



El número de habitación contiene como máximo 6 números o letras o sus combinaciones, y no puede ser igual a ningún número VTO.

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

los **Gestión de número de habitación** se muestra la interfaz. Vea la Figura 4-11.

Figure 4-11 Gestión de número de habitación

Room No.	First Name	Last Name	Nick Name	Register Type	Modify
1	1	1		home.null	
2	2	2		home.null	
3	3	3		home.null	
4	4	4		home.null	
5	5	5		home.null	
6	6	6		home.null	
7	7	7		home.null	
8	8	8		home.null	
9	9	9		home.null	
10	10	10		home.null	
11	11	11		home.null	

Unit Layer Amount: 5 Room Amount in One Layer: 4

First Floor Number: 101 Second Floor Number: 201

Step 2 Puede agregar un número de habitación individual o hacerlo por lotes.

- Agregar número de habitación individual

1) Haga clic en **Añadir**. Vea la Figura 4-11.

los **Añadir** se muestra la interfaz. Vea la Figura 4-12.

Figure 4-12 Agregar número de habitación individual

2) Configure la información de la habitación. Consulte la Tabla 4-3.

Tabla 4-3 Información de la habitación

Parámetro	Descripción
Nombre de pila	Ingresa la información que necesita para diferenciar cada habitación.
Apellido	

Parámetro	Descripción
Nombre de Nick	
Habitación no.	El número de habitación que planeaste.  - Si usa varios dispositivos VTH, el número de habitación del VTH maestro debe ser "número de habitación # 0", y el número de habitación de la extensión VTH debe ser "número de habitación # 1", "número de habitación # 2",..., " número de habitación # 99 ". - Puede tener 10 dispositivos VTH de extensión como máximo para un VTH maestro.
Seleccionar tipo de registro	público , y local está reservado para uso futuro. Registrarse
Contraseña	Mantenga el valor predeterminado.

3) Haga clic en **Salvar**.

Se muestra el número de habitación agregado. Hacer clic



para modificar la información de la habitación y haga clic en



para eliminar una habitación.

- Agregar número de habitación en lotes

1) Configure la Cantidad de capa de unidad, RoomAmount en una capa, Número de primer piso y Número de segundo piso de acuerdo con la condición real.

2) Haga clic en el **Añadir** en el fondo. Ver la Figura 4-13

Figure 4-13 Agregar en lote

Se muestran todos los números de habitación añadidos. Hacer clic **Actualizar** para ver el estado más reciente y haga clic en **Claro** para borrar todos los números de habitación.

4.2.7 Módulo de configuración

El módulo de la cámara está diseñado por defecto. Todos los demás módulos deben agregarse en el diseño de la fachada antes de su uso.

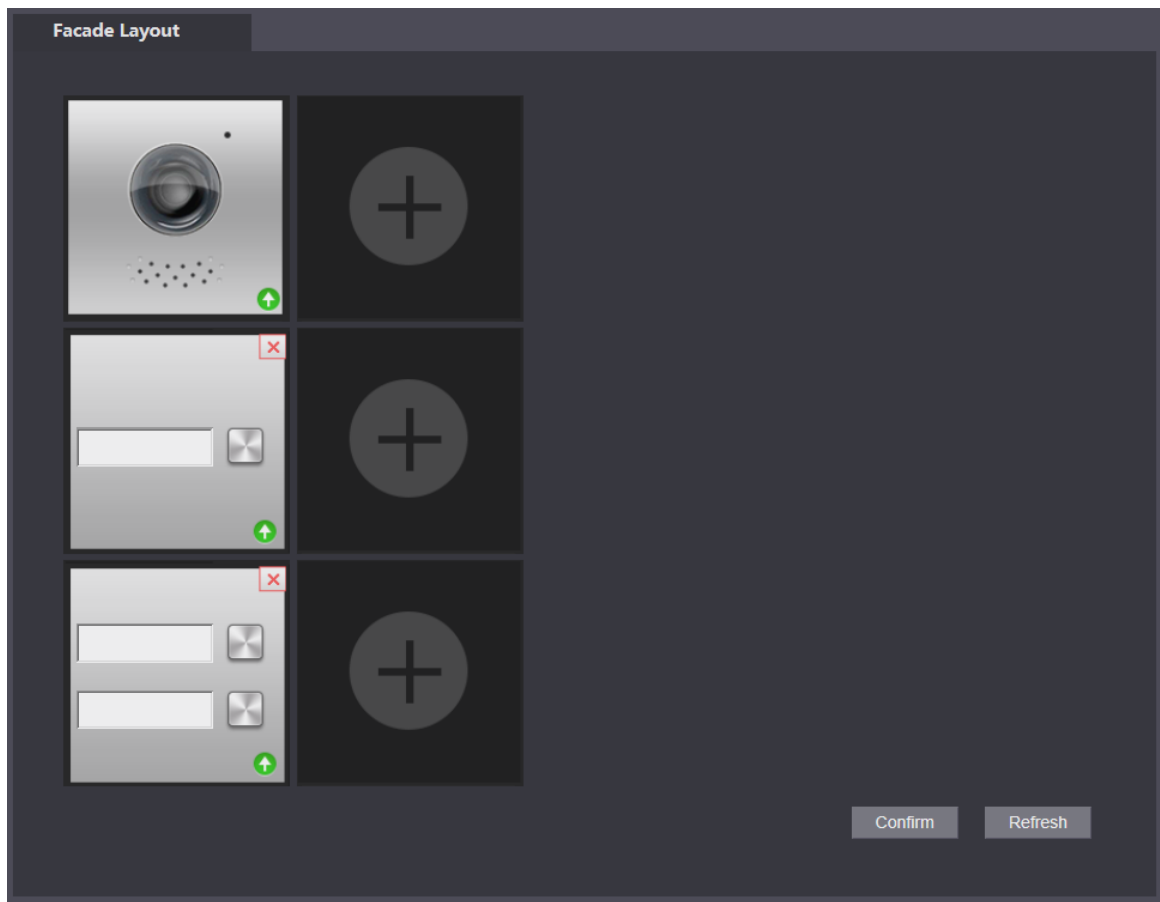


- Puede agregar 9 módulos como máximo a VTO4202F-MB1, VTO4202F-MB2, VTO4202F-MB5. Para los VTO de otros módulos, solo puede agregar un módulo.
- Para el módulo de huellas dactilares, el módulo de deslizamiento de tarjetas y el módulo de teclado, solo se puede agregar un módulo de cada tipo, respectivamente. Otros módulos se pueden combinar libremente.

4.2.7.1 Agregar módulos

Step 1 Seleccione Configuración local> Básico> Diseño de fachada. los **Disposición de la fachada** se muestra la interfaz. Vea la Figura 4-14.

Figure 4-14 Disposición de la fachada



Step 2

Hacer clic



El sistema muestra los módulos disponibles.



El módulo de teclado, el módulo de deslizamiento de tarjetas y el módulo de huellas dactilares no se mostrarán si se han agregado.

Step 3

Seleccione los módulos de acuerdo con el diseño real de VTO.



La posición de conexión real del dispositivo en la interfaz web es de arriba a abajo y de izquierda a derecha.

Admite agregar varios módulos al mismo tiempo y guardar las configuraciones. Hacer clic **Confirmar**, y luego

Step 4

reinicie el navegador para que las configuraciones sean efectivas.

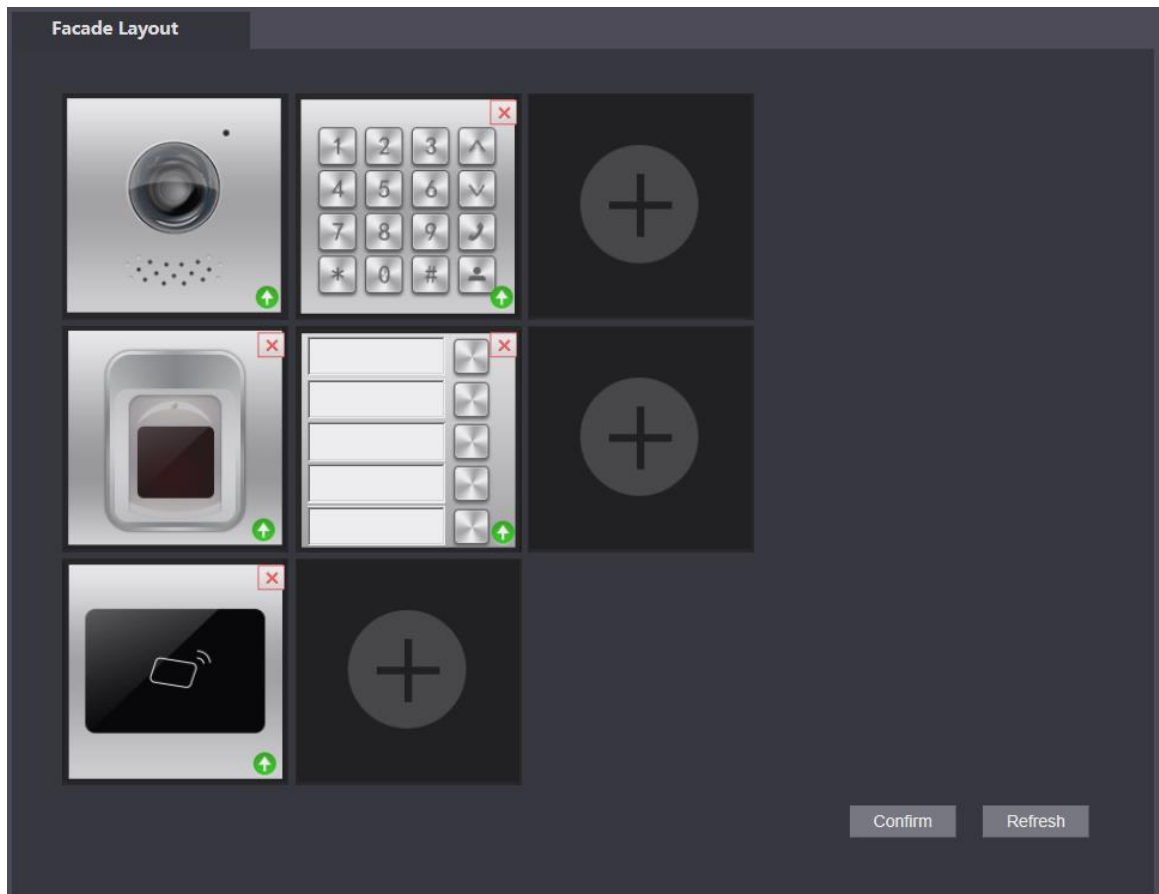
4.2.7.2 Configuración de módulos

Debe configurar las teclas de llamada para el módulo de botones y el módulo de la cámara respectivamente.

Step 1

Seleccione Configuración local> Básico> Diseño de fachada. los **Disposición de la fachada** se muestra la interfaz. Vea la Figura 4-15.

Figure 4-15 Establecer módulos



Step 2

Hacer clic

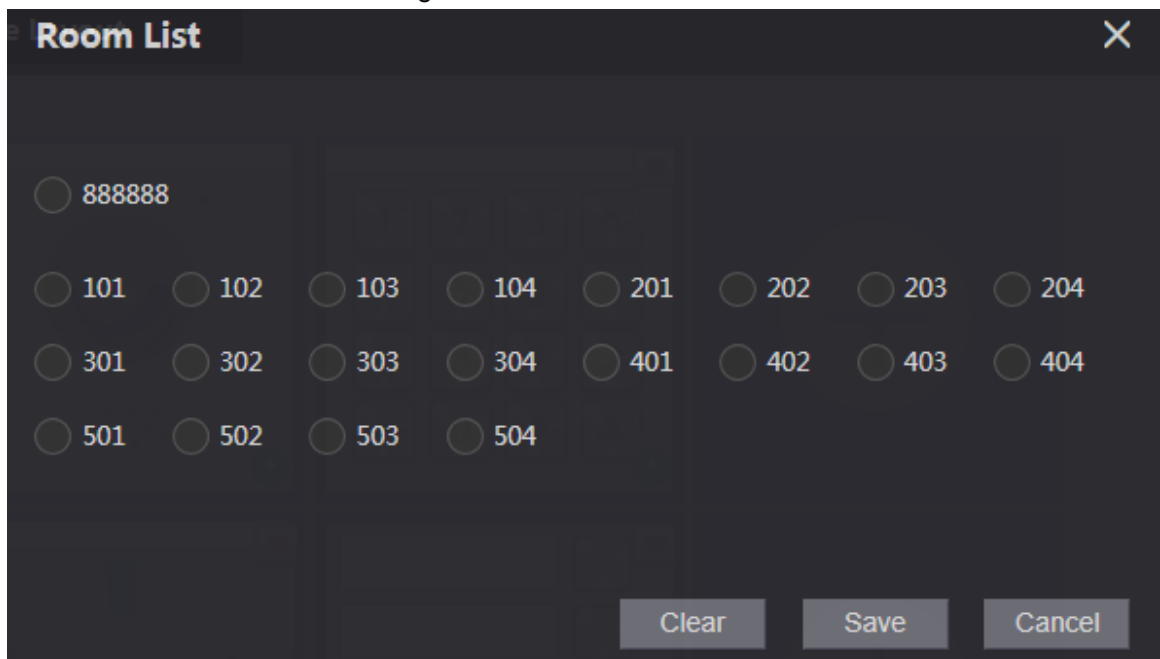


los **Lista de habitaciones** se muestra la interfaz. Vea la Figura 4-16.



La habitación no. que se muestra en la interfaz corresponde al VTH agregado. "888888" es el número de llamada del centro.

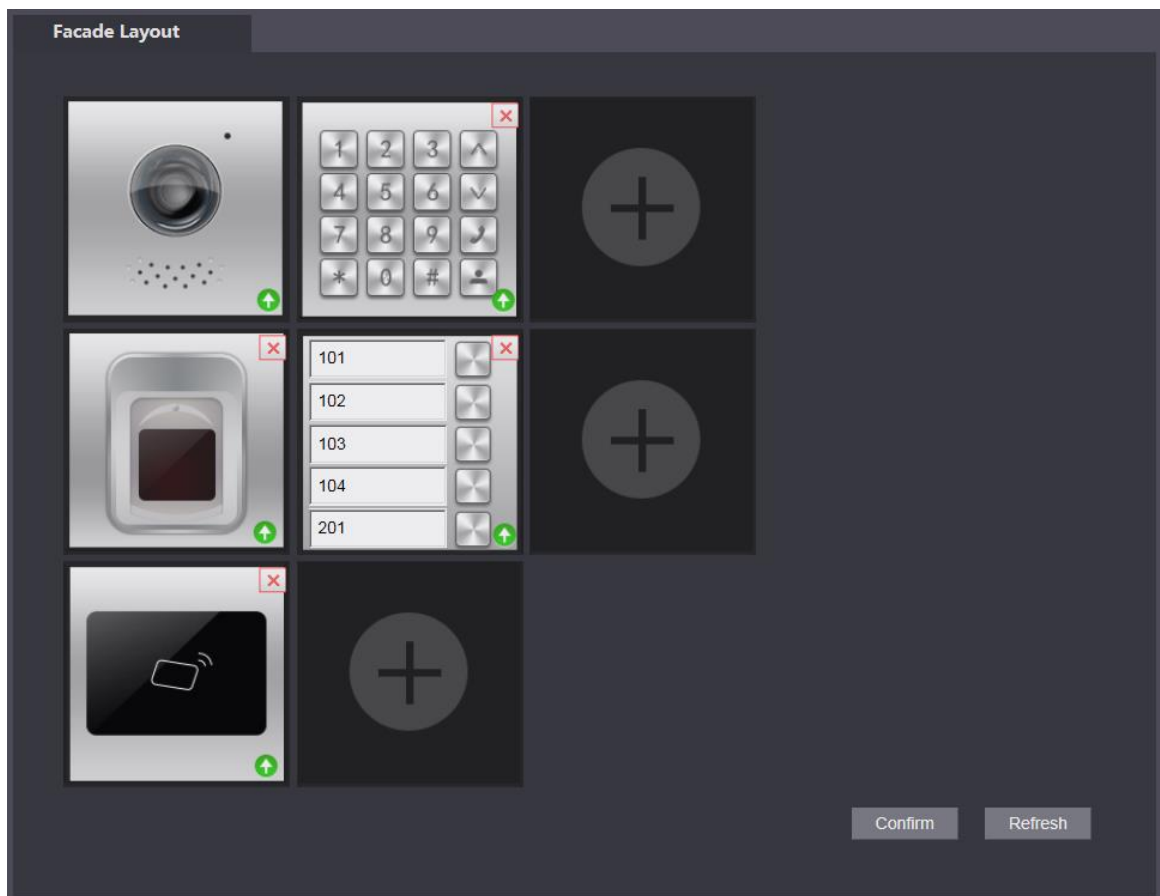
Figure 4-16 Lista de habitaciones



Step 3 Seleccione la habitación no. y haga clic en **Salvar**.

La interfaz muestra información sobre el número de habitación. Vea la Figura 4-17.

Figure 4-17 Información del número de habitación



Step 4 Hacer clic **Confirmar**, y luego reinicie el navegador para que las configuraciones sean efectivas. guardar la configuración.

4.3 Verificación de la configuración

4.3.1 Llamar a VTH desde VTO

Step 1 Marque el número de habitación en el VTO.

Step 2 prensa .

El VTO está llamando al VTH. Vea la Figura 4-18.

Figure 4-18 Pantalla de llamada

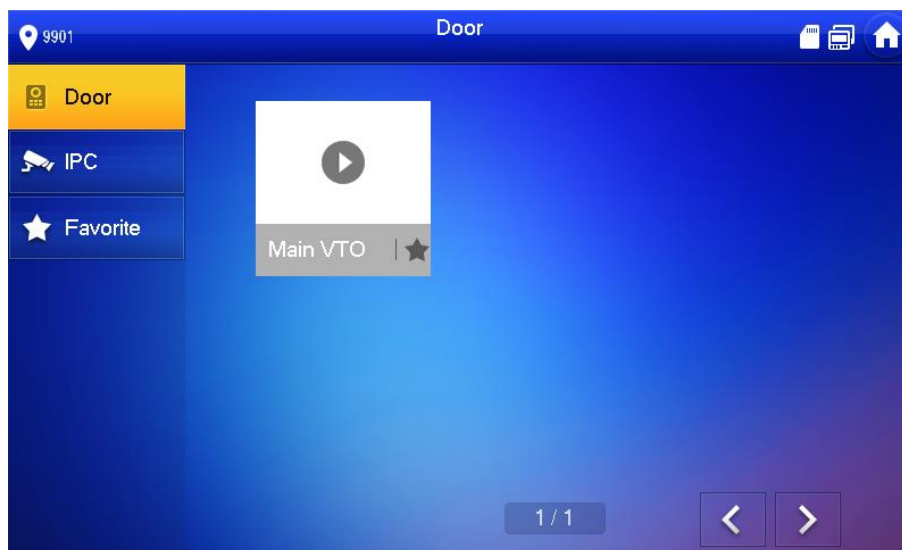


Step 3 Grifo  en el VTH para contestar la llamada.

4.3.2 Hacer monitor desde VTH

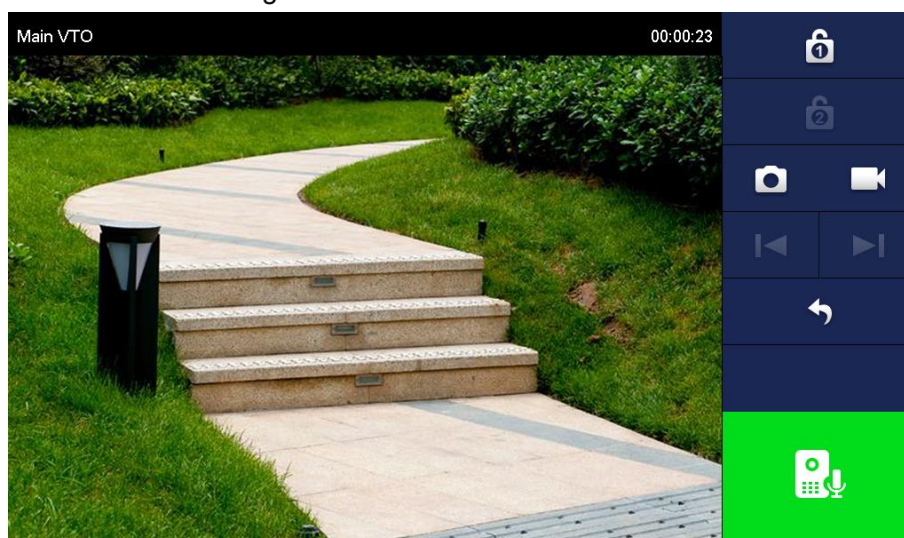
Step 1 En la interfaz principal del VTH, seleccione **Monitor> Puerta**.
los **Puerta** se muestra la interfaz. Vea la Figura 4-19.

Figure 4-19 Puerta



Step 2 Seleccione el VTO que necesita monitorear.
Aparece la pantalla del monitor. Vea la Figura 4-20.

Figure 4-20 Pantalla del monitor



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 muestran algunos consejos y recomendaciones sobre cómo crear un sistema de seguridad más seguro.

Acciones obligatorias que deben tomarse para la seguridad de la red de equipos básicos:

1. Utilice contraseñas seguras

Consulte las siguientes sugerencias para establecer contraseñas:

- La longitud no debe ser inferior a 8 caracteres;
- Incluya al menos dos tipos de personajes; 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 cliente a tiempo

- De acuerdo con el procedimiento estándar en la industria tecnológica, 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 "búsqueda automática de actualizaciones" para obtener información oportuna de las actualizaciones de firmware publicadas por el fabricante.
- Le sugerimos que descargue y utilice la última versión del software cliente.

Recomendaciones "Es bueno tener" para mejorar la seguridad de la red de su equipo:

1. Protección física

Le sugerimos que realice protección física a los equipos, especialmente a los dispositivos de almacenamiento. Por ejemplo, coloque el equipo en una sala de computadoras especial y gabinete, e implemente permisos de control de acceso bien hechos y administración de claves para evitar que el personal no autorizado lleve a cabo contactos físicos como daños en el hardware, conexión no autorizada de equipos 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 ser adivinado o descifrado.

3. Establecer y actualizar contraseñas Restablecer información a tiempo

El equipo 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 las preguntas de protección por contraseña, se sugiere no utilizar aquellas que se puedan 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 con la contraseña incorrecta varias veces, 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 en cualquier conjunto de números entre 1024 ~ 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, excepto aquellos con direcciones IP específicas, accedan al sistema. Por lo tanto, asegúrese de agregar la dirección IP de su computadora y la dirección IP del equipo adjunto a la lista blanca.

8. Enlace de dirección MAC

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

9. Asignar cuentas y privilegios de forma razonable

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

10. 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 contraseñas de autenticación y de cifrado seguras.
- 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.

11. Transmisión encriptada de audio y video

Si su contenido de datos de audio y video es muy importante o sensible, 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 provocará cierta pérdida en la eficiencia de transmisión.

12. Auditoría segura

- Verificar usuarios en línea: le sugerimos que verifique a los usuarios en línea con regularidad para ver si el dispositivo está conectado sin autorización.
- Verifique el registro del equipo: al ver los registros, puede conocer las direcciones IP que se utilizaron para iniciar sesión en sus dispositivos y sus operaciones clave.

13. Registro de red

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

14. Construya un entorno de red seguro

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

- Desactive la función de asignación de puertos del enrutador para evitar el acceso directo a los dispositivos de la 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 utilizar VLAN, red GAP 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.