Estación de puerta modular

Guía de inicio rápido

V1.0.0

Prefacio

General

Este documento presenta principalmente la función del producto, la estructura, la conexión en red, el proceso de montaje, el proceso de depuración y las operaciones web de la estación de puerta modular (en lo sucesivo, "VTO").

Modelos

VTO4202F-MK, VTO4202F-MB1, VTO4202F-MB2, VTO4202F-MB5, VTO4202F-MR, VTO4202F-MS, VTO4202F-MF, VTO4202F-ML, VTO4202F-MA, VTO4202F-P y VTO4202F-P-S2.

Actualización del dispositivo

La fuente de alimentación se puede cortar solo después de que el dispositivo haya completado la actualización y se haya reiniciado.

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.
PUNTAS	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	Tiempo de liberación
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 VTO. Lea atentamente el manual antes del uso para evitar peligros y pérdidas materiales. Siga estrictamente el manual durante la aplicación y guárdelo adecuadamente para futuras consultas.

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 en lugares estables de forma horizontal para evitar que se caiga.
- No gotee ni salpique líquidos sobre el dispositivo, ni coloque sobre el dispositivo nada lleno de líquido.
- Instale el dispositivo en lugares bien ventilados 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

- Utilice cables eléctricos recomendados en su área y dentro de su especificación nominal.
- 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 la etiqueta 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

1.1 Introducción

Puede construir el VTO modular con diferentes módulos, incluido el módulo de cámara, el módulo de indicadores, el módulo de botones, el módulo de teclado, el módulo de tarjetas, el módulo de huellas dactilares, el módulo de audio y el módulo de visualización. Los módulos de cámara y audio son indispensables, y los demás se pueden agregar según sea necesario.

1.2 Características

- Videollamada: Realice videollamadas a monitores interiores (VTH).
- Llamada grupal: llame a varios VTH simultáneamente.
- Monitoreo de video: hasta 6 VTH pueden ver la imagen de monitoreo de este VTO al mismo tiempo.
- Llamada de emergencia: Llame al centro de gestión durante una emergencia.
- Desbloqueo: Tarjeta, huella, contraseña y desbloqueo remoto.
- Alarma: alarma antimanipulación, alarma de contacto de puerta y alarma de desbloqueo de contraseña de coacción. La información de la alarma se enviará al centro de gestión.
- Búsqueda de registros: registros de llamadas, registros de alarmas y registros de desbloqueo.

2 Estructura

2.1 Módulo de cámara

Figure 2-1 Panel frontal

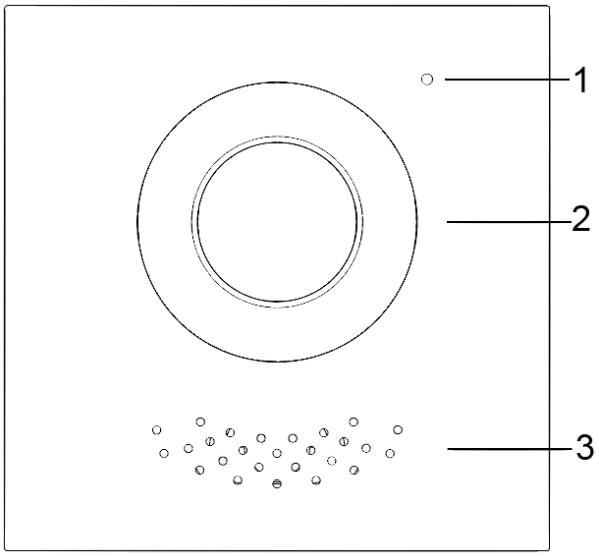


Tabla 2-1 Descripción del panel frontal

No.	Nombre
1	Micrófono
2	Cámara
3	Altavoz

Figure 2-2 Panel trasero

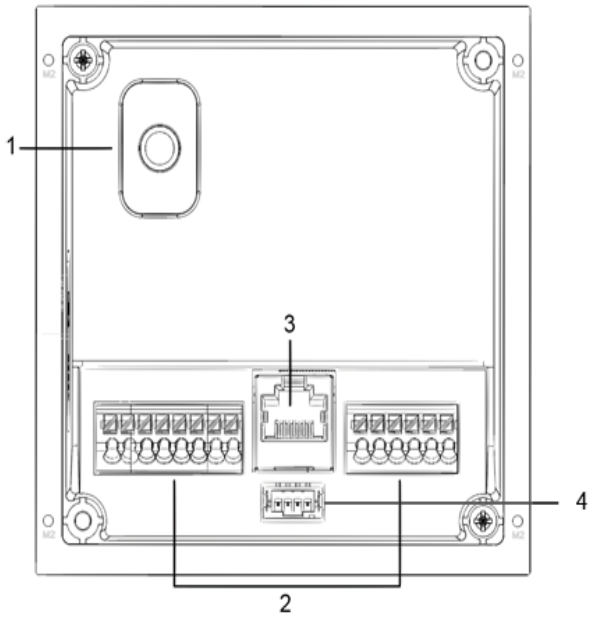


Tabla 2-2 Descripción del panel trasero

No.	Nombre	Descripción
1	Interruptor antimanipulación	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	Puertos	Conectar a la fuente de alimentación, bloqueo de control eléctrico, bloqueo de solenoide y botón de salida.
3	Puerto Ethernet	Conéctese a los cables de red.
4	Puerto de conexión en cascada	Conéctese a otros módulos.

Figure 2-3 Descripción de los puertos

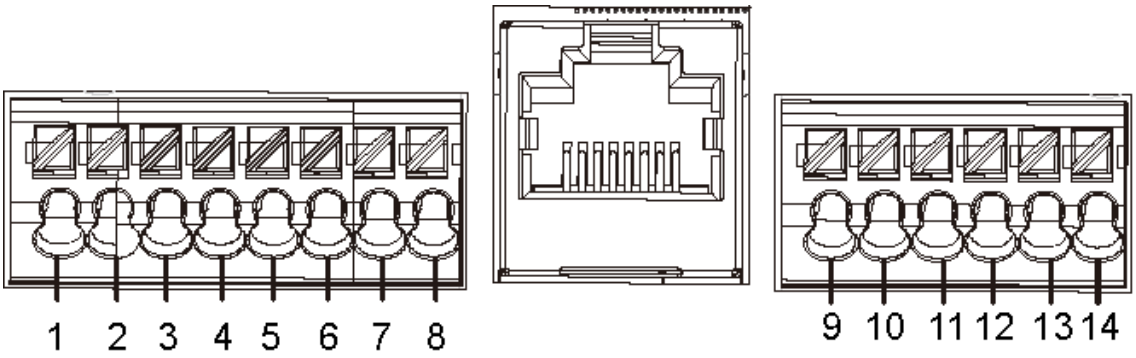


Tabla 2-3 Descripción del puerto

No.	Descripción	No.	Descripción
1	TIERRA	8	EOC1 (2 hilos – (GND) para un módulo de cámara de 2 hilos)
2	+ 12V_SALIDA	9	BOTÓN_PUERTA
3	RS-485_B	10	RETROALIMENTACIÓN DE LA PUERTA
4	RS-485_A	11	TIERRA
5	ALARMA_NO	12	PUERTA_NC
6	ALARMA_COM	13	PUERTA_COM
7	EOC2 (2 hilos +(48 V) para un módulo de cámara de 2 hilos)	14	PUERTA_NO

2.2 Módulo indicador

Figure 2-4 Panel frontal

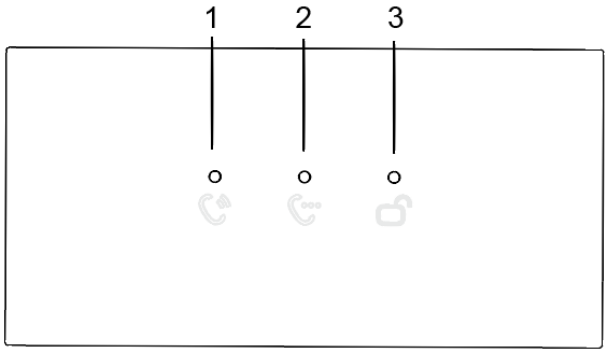


Tabla 2-4 Descripción del módulo indicador (1)

No.	Nombre	Descripción
1	Indicador de llamada	Estado de actividad.
2	Indicador de conversación	
3	Indicador de desbloqueo	

Figure 2-5 Panel trasero del módulo indicador

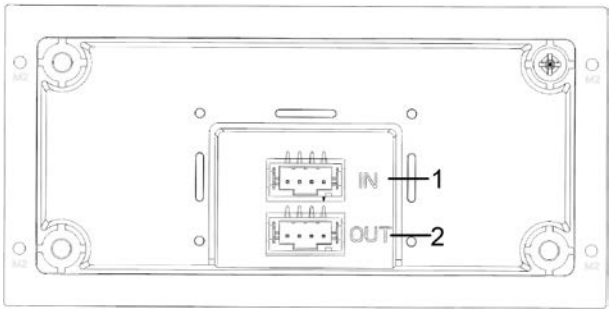


Tabla 2-5 Descripción del módulo indicador (2)

No.	Nombre	Descripción
1	Entrada en cascada	Conéctese a otros módulos.
2	Salida en cascada	

2.3 Módulo de audio

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

Figure 2-6 Módulo de audio

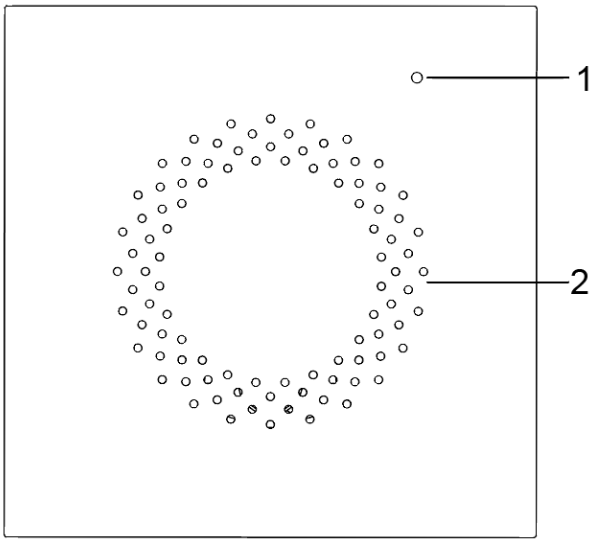


Tabla 2-6 Descripción del módulo de audio

No.	Nombre
1	Micrófono
2	Altavoz

2.4 Módulo de botones

El módulo de un botón, el módulo de dos botones y el módulo de cinco botones están disponibles con la misma función. Aquí tomamos el módulo de cinco botones como ejemplo.

Figure 2-7 Panel frontal del módulo de cinco botones

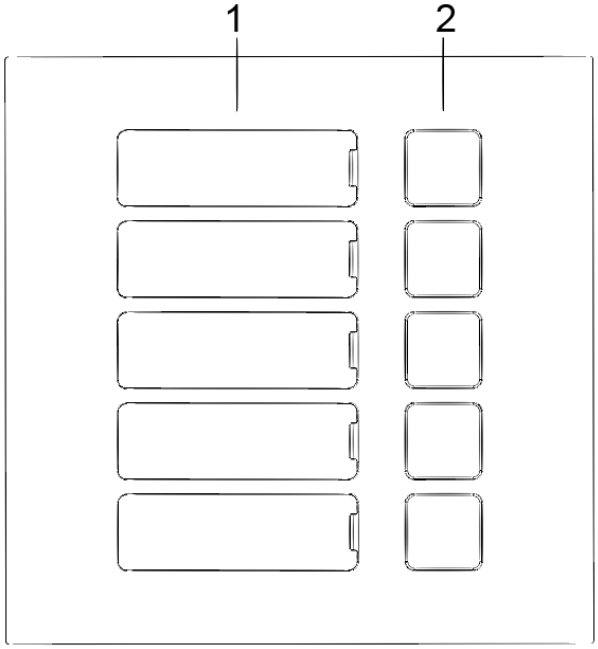


Tabla 2-7 Descripción del panel frontal

No.	Nombre	Descripción
1	Directorio de usuarios	Ponga tarjetas de identificación aquí.
2	Botones de llamada	Llame a otros VTH o al centro de gestión. Primero configure los parámetros relacionados en la interfaz web.

Figure 2-8 Panel trasero del módulo de cinco botones

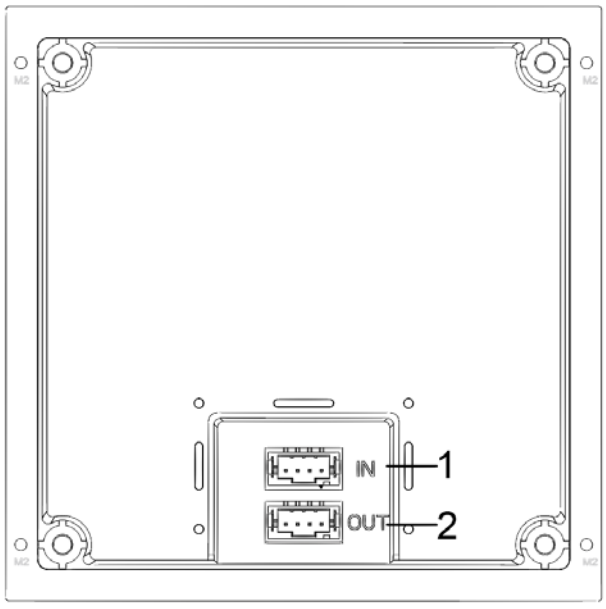


Tabla 2-8 Descripción del panel trasero

No.	Nombre
1	Entrada en cascada
2	Salida en cascada

2.5 Módulo de teclado (con Braille)

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

Figure 2-9 Módulo de teclado

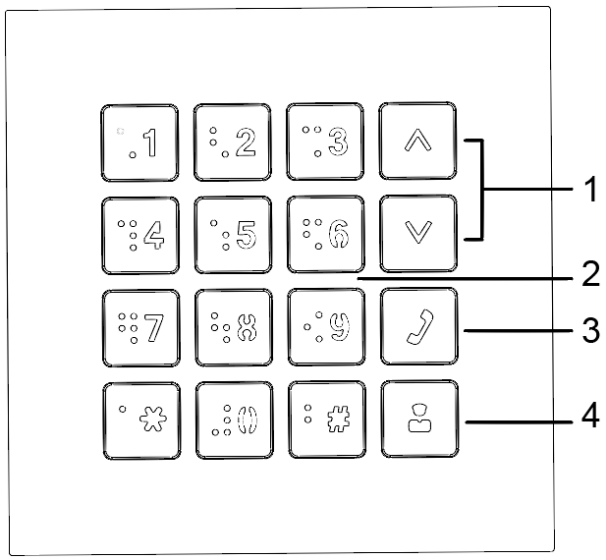


Tabla 2-9 Descripción del módulo de teclado

No.	Nombre	Descripción
1	Selección	—
2	Números	Ingrese la contraseña o los números VTH.
3	Llamar	Llame a los VTH.
4	centro de gestión de llamadas	—

2.6 Módulo de tarjeta

Pase su tarjeta cerca del icono.

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

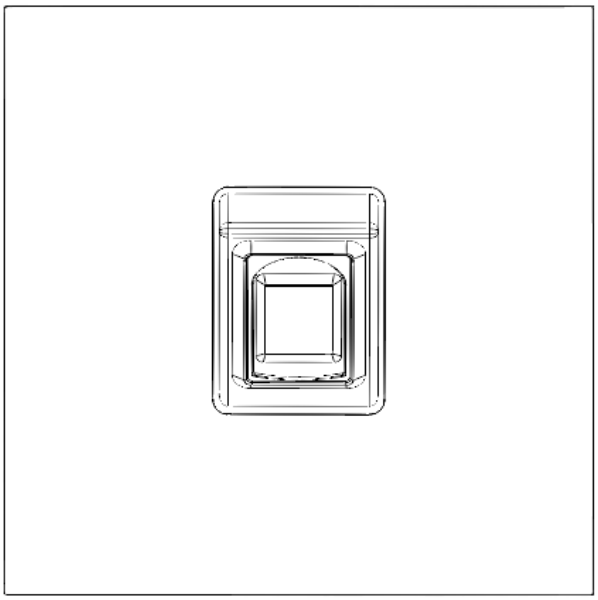
Figure 2-10 Módulo de tarjeta

2.7 Módulo de huellas dactilares

Recopila y verifica las huellas dactilares.

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

Figure 2-11 Módulo de huellas dactilares

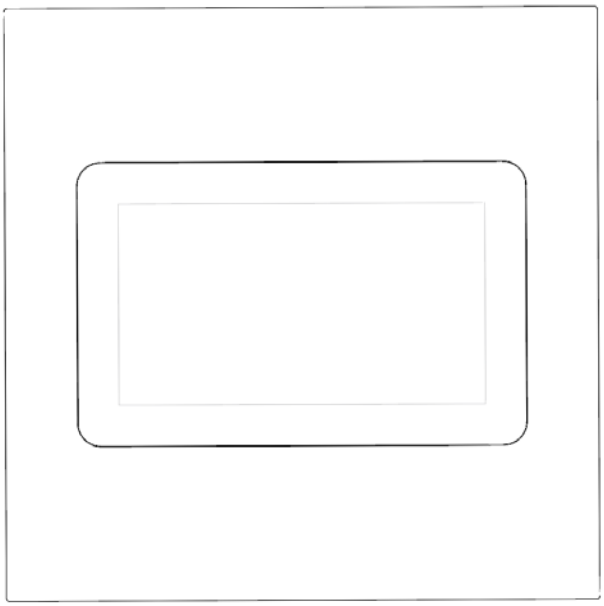


2.8 Módulo de pantalla

Muestra información del usuario.

Los paneles traseros del módulo de pantalla y el módulo de botones tienen diferentes posiciones de puertos, pero las funciones de los puertos son lo mismo.

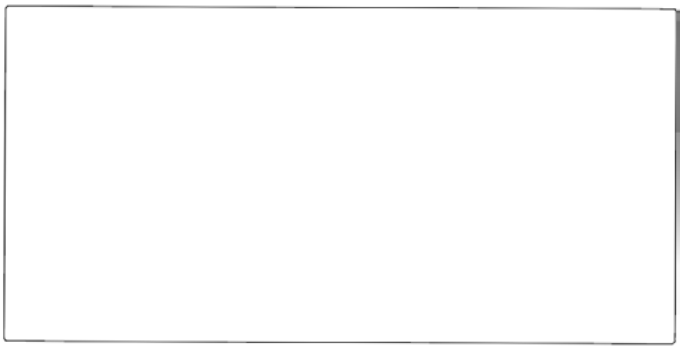
Figure 2-12 Módulo de visualización



2.9 Módulo en blanco

Para una mejor apariencia, use el módulo en blanco si hay un espacio adicional mientras coloca los módulos juntos.

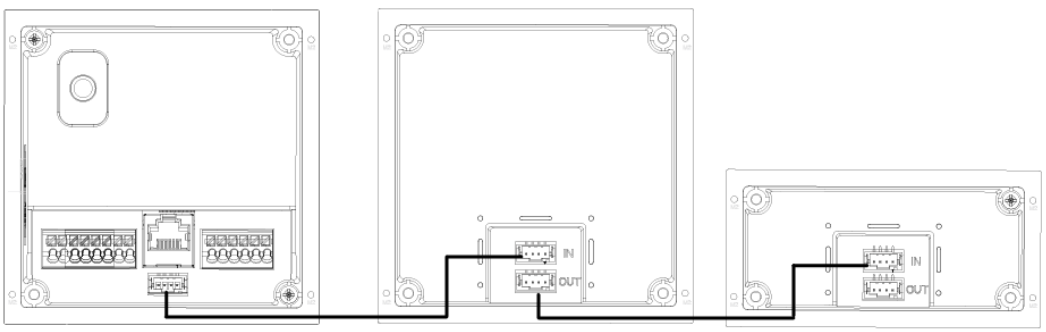
Figure 2-13 Módulo en blanco



2.10 Conexión en cascada

Se necesita una conexión en cascada para que todos los módulos funcionen juntos.

Figure 2-14 Ejemplo de conexión en cascada



3 Configuración y puesta en servicio

Este capítulo presenta las configuraciones básicas de los dispositivos VTO y VTH.

La interfaz y la función pueden variar según el tipo de dispositivo que configuró para el VTO. El actual la interfaz y la función prevalecerán.

3.1 Procedimiento

Antes de la configuración, asegúrese de que no haya un cortocircuito o un circuito abierto.

Step 1 IP del plan y número de unidad/habitación (funciona como un número de teléfono) para cada dispositivo.

Step 2 Configure el VTO. Consulte "3.2 Configuración de VTO".

Step 3 Configure el VTH. Consulte el manual del usuario de VTH. Compruebe si todos

Step 4 los ajustes son correctos. Consulte "3.3 Puesta en servicio".

3.2 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.

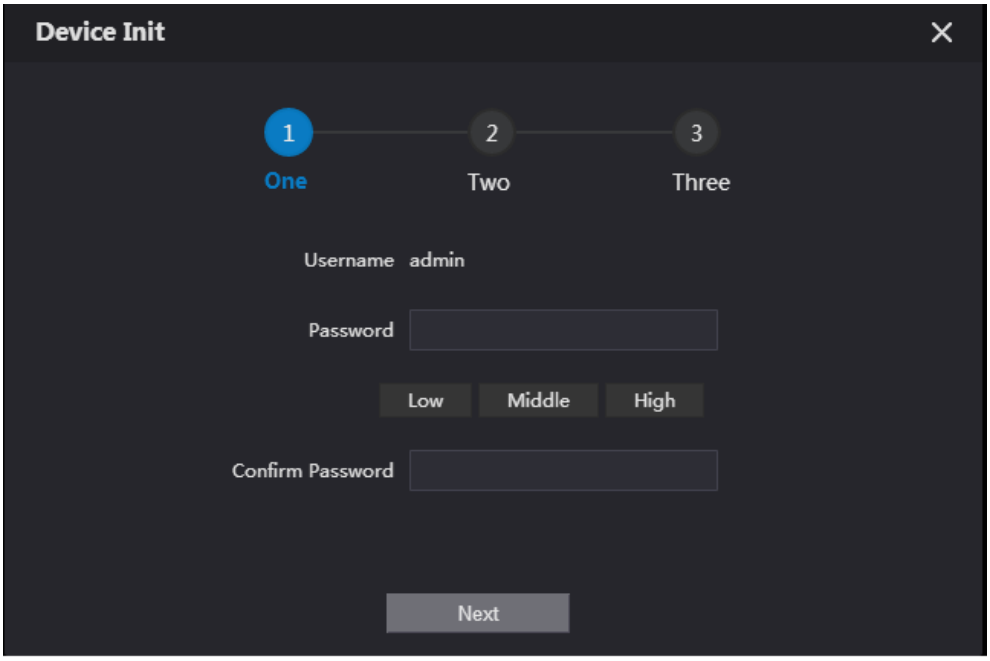
3.2.1 Inicialización

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 3-1 Inicialización del dispositivo



Step 3 Introduzca y confirme la contraseña y, a continuación, haga clic en**próximo**.

Step 4 Seleccione**Correo electrónico**, ingrese una dirección de correo electrónico para restablecer la contraseña y luego haga clic

Step 5 en**próximo**. Hacer clic**OK**. El sistema va a la interfaz de inicio de sesión.

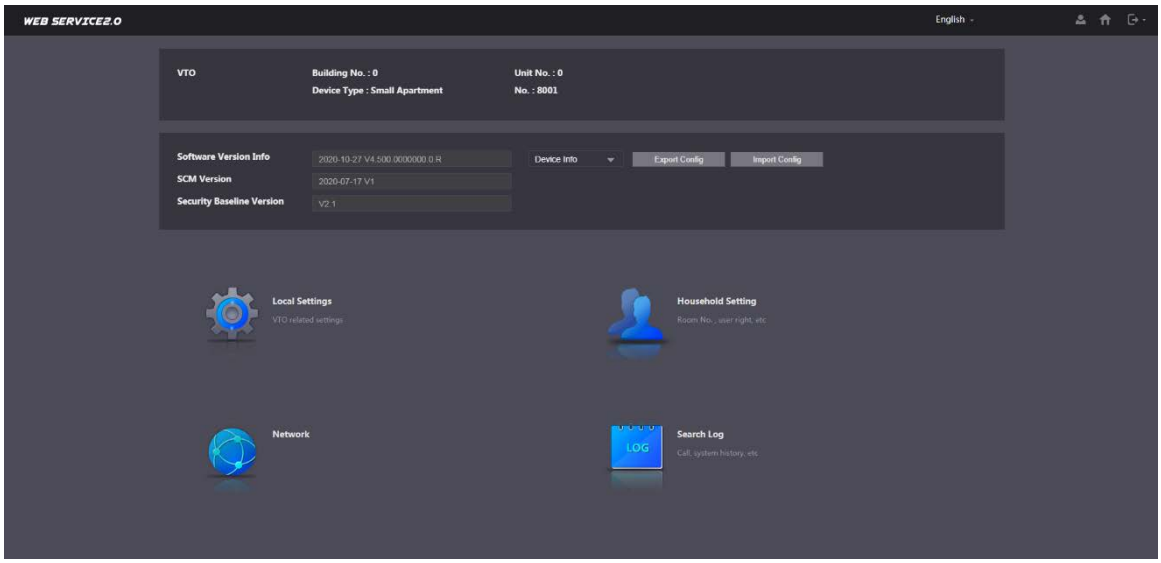
3.2.2 Configuración del número de VTO

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 5 números como máximo, y no puede ser el mismo con cualquier número de habitación.

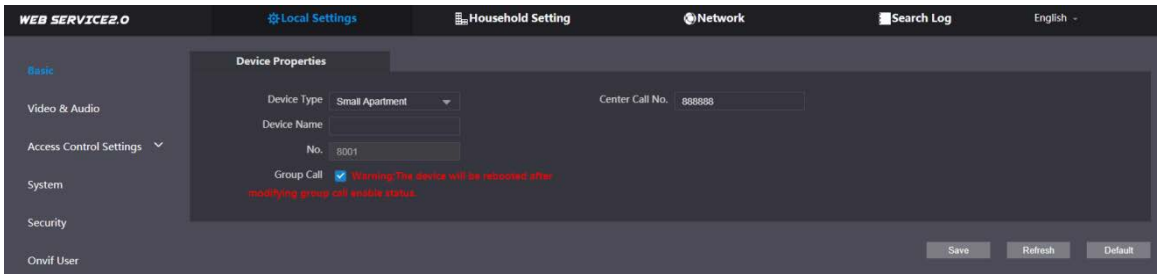
Step 1 Inicie sesión en la interfaz web de VTO.

Figure 3-2 Interfaz principal



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

Figure 3-3 Propiedades del dispositivo

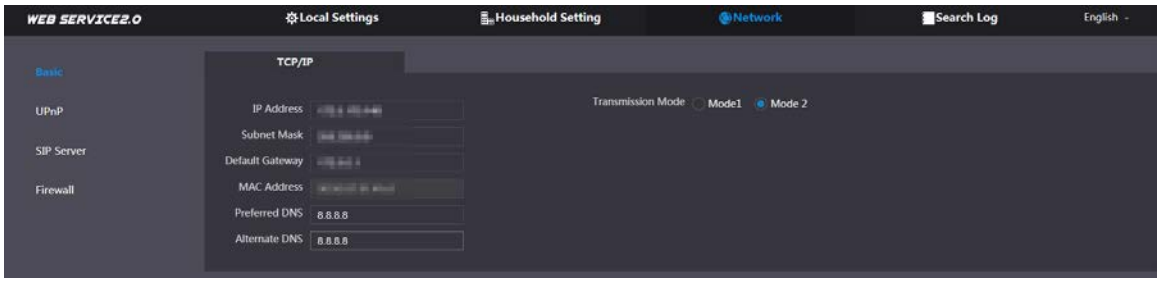


Step 3 Introduzca el número en**No.**y luego haga clic en**Ahorrar**.

3.2.3 Configuración de parámetros de red

Step 1 Seleccione**Red > Básico**.

Figure 3-4 Información TCP/IP



Step 2 Introduzca los parámetros y haga clic en**Ahorrar**.

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

3.2.4 Configuración de servidores SIP

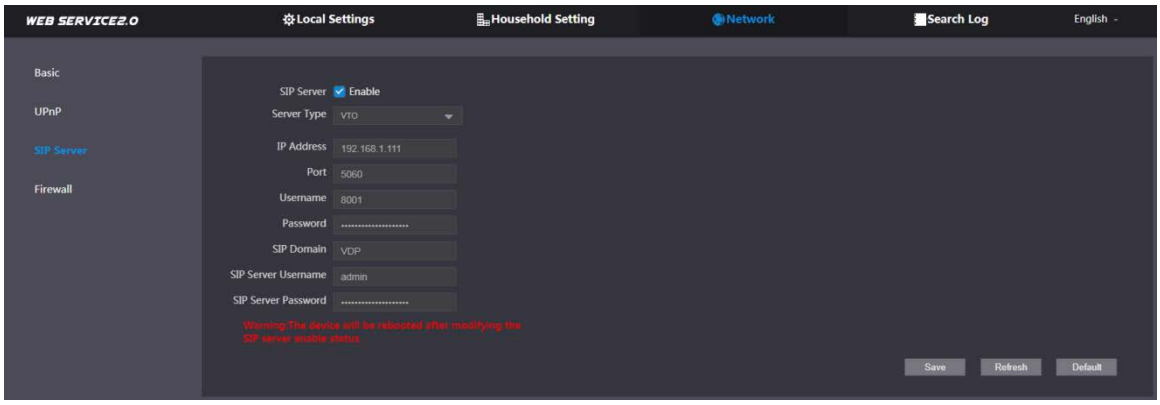
Cuando se conecta al mismo servidor SIP, todos los VTO y VTH pueden llamarse entre sí. Puede utilizar un VTO u otros servidores como servidor SIP.

- Si el VTO actual es el servidor SIP,**Edificio número.**y**Numero de unidad.**no se mostrará en la **Propiedades del dispositivo**interfaz.
- Si vas a**Configuración de red > Servidor SIP**, habilitar**Servidor alternativo**e inicia sesión en la web interfaz de nuevo,**Edificio número.**y**Numero de unidad.**se mostrará en el**Propiedades del dispositivo** interfaz.

Step 1 Inicie sesión en la interfaz web.

Step 2 Seleccione**Red > Servidor SIP**.

Figure 3-5 servidor SIP



Step 3 Seleccione un servidor SIP.

- VTO como servidor SIP: esto es aplicable a un solo edificio.

1) Habilitar**Servidor SIP**.

2) Seleccionar**Tipo de servidor**como**VTO**.

3) Configurar los parámetros. Consulte la Tabla 3-1.

4) Haga clic**Ahorrar**. El VTO se reiniciará automáticamente.

- Plataforma (Express/DSS) como servidor SIP: Esto es aplicable a múltiples edificios o unidades. Si no tiene una plataforma, use un VTO como servidor SIP.

1) Deshabilitar**Servidor SIP**.

2) Seleccionar**Tipo de servidor**a**Expreso/DSS**.

3) Configurar los parámetros.

Tabla 3-1 Descripción de los parámetros del servidor SIP

Parámetro	Descripción
Dirección IP	Dirección IP del servidor SIP. Si**Servidor alternativo**no está habilitado, el VTO no puede llamar al VTS.
Puerto	● 5060 por defecto cuando VTO funciona como servidor SIP. 5080 por ● defecto cuando la plataforma funciona como servidor SIP.
Usuario Contraseña	Manténgalo predeterminado.
Dominio SIP	● Debe ser VDP cuando VTO funciona como servidor SIP. ● Manténgalo nulo o predeterminado cuando la plataforma funcione como servidor SIP.
Nombre de usuario del servidor SIP/ Clave	Se utiliza para iniciar sesión en el servidor SIP.
Dirección IP alternativa	Dirección IP del servidor alternativo.
Nombre de usuario alternativo	Nombre de usuario y contraseña de inicio de sesión del servidor alternativo.
Contraseña alternativa	
Dirección IP VTS alternativa	Dirección IP del VTS alternativo.
Servidor alternativo	● Después de ingresar la dirección IP alternativa, el nombre de usuario, la contraseña y la dirección IP de VTS, debe habilitar**Servidor alternativo**. ● Después**Servidor alternativo**está habilitado, solo puede ingresar la dirección IP de VTS y el VTO se reiniciará.

Step 4 Hacer clic**OK**y el VTO se reiniciará automáticamente.

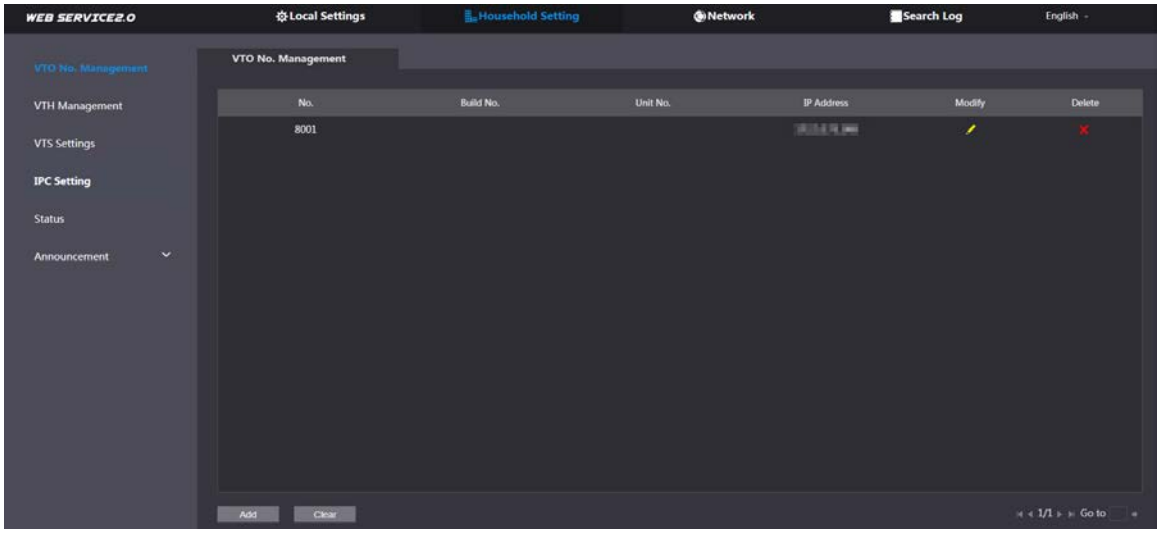
Cuando una plataforma funciona como servidor SIP, habilite**Edificio de apoyo**y**Unidad de Apoyo**primero si es necesario configurar el número de edificio y el número de unidad de edificio.

3.2.5 Agregar VTO

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

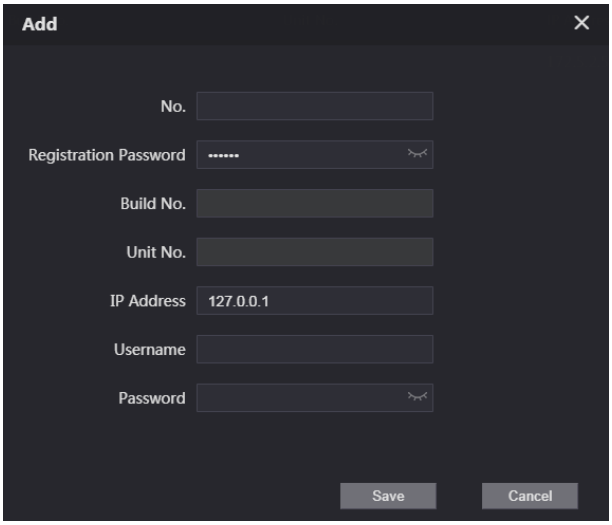
Step 1 Inicie sesión en la interfaz web del servidor SIP y luego seleccione**Configuración del hogar > Gestión del número de VTO**.

Figure 3-6 Gestión de números de VTO



Step 2 Hacer clic**Agregar**.

Figure 3-7 Agregar VTO



Step 3 Configure los parámetros.

Se debe agregar el servidor SIP.

Tabla 3-2 Agregar VTO

Parámetro	Descripción
No. de registro	número VTO. Consulte "3.2.2 Configuración del número de VTO".
Contraseña de registro	Manténgalo 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**Ahorrar**.

3.2.6 Agregar número de habitación

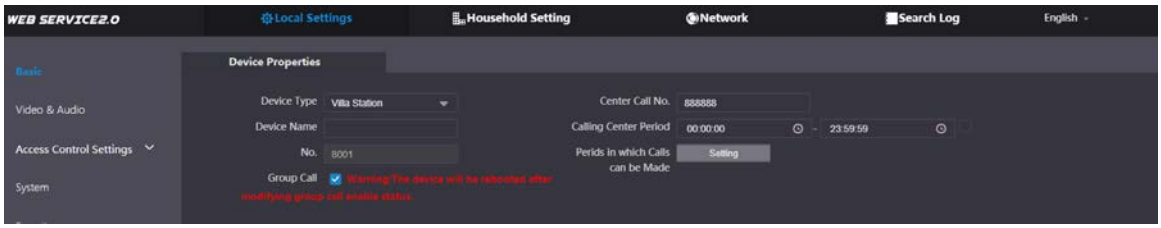
Puede agregar el número de habitación planificado al servidor SIP y luego configurar el número de habitación en los dispositivos VTH para conectarlos a la red. Esta sección es aplicable cuando el VTO funciona como servidor SIP, y si utiliza otros servidores como servidor SIP, consulte el manual correspondiente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

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

Usando el VTO en una Villa

Step 1 Inicie sesión en la interfaz web del servidor SIP y luego seleccione**Configuración local > Básico**.

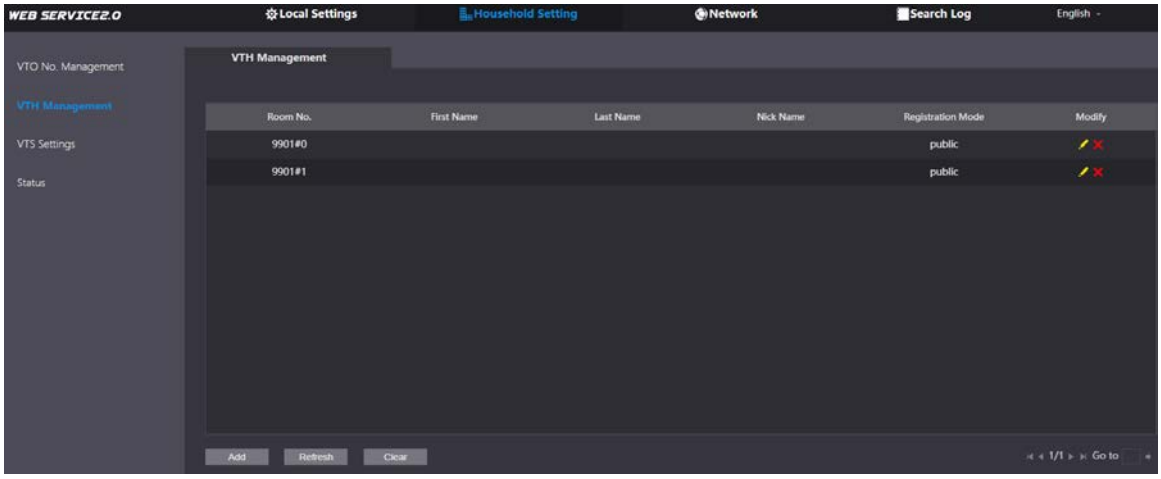
Figure 3-8 Propiedades del dispositivo



Step 2 Establecer**Tipo de dispositivo**a**Estación Villa**y luego haga clic en

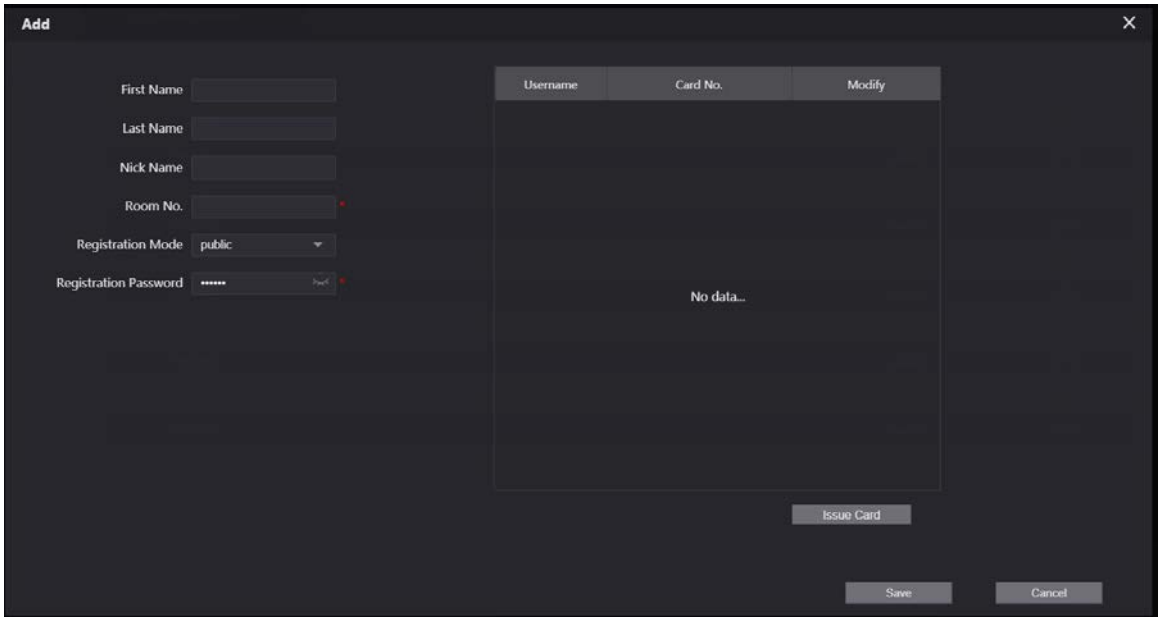
Step 3 **Ahorrar**. Seleccione**Configuración del hogar > Gestión de VTH**.

Figure 3-9 Gestión del número de habitación



Step 4 Hacer clic**Agregar**.

Figure 3-10 Añadir un número de habitación individual



Step 5 Configure la información de la izquierda.

Tabla 3-3 Información de la habitación

Parámetro	Descripción
Primer nombre Apellido Apodo	Información utilizada para diferenciar cada habitación.
Habitación no.	● Cuando hay múltiples VTH, el número de habitación para el VTH principal debe terminar en #0, y los números de habitación para los VTH secundarios en #1, #2... ● Puede tener hasta 10 VTH secundarios para un VTH principal.
Registro Escribe	Seleccione**público**.
Registro Clave	Manténgalo predeterminado.

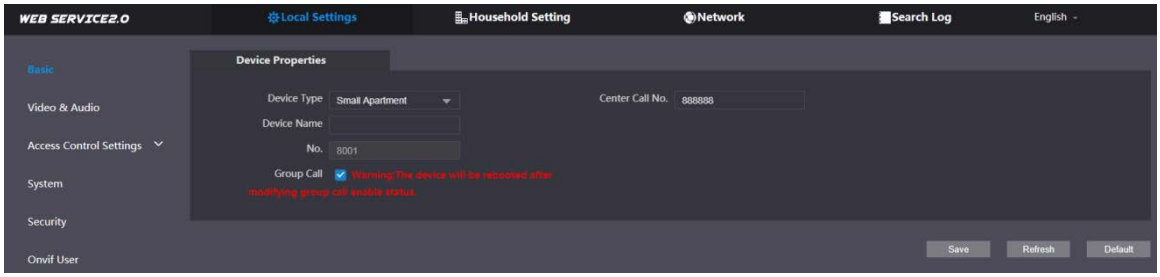
Step 6 Hacer clic**Ahorrar**.

- Hacer clic  o  para modificar o eliminar un número de habitación.
- Hacer clic**Claro**para borrar todos los números de habitación.

Usando el VTO en un apartamento pequeño

Step 1 Inicie sesión en la interfaz web del servidor SIP y luego seleccione**Configuración local > Básico**.

Figure 3-11 Propiedades del dispositivo

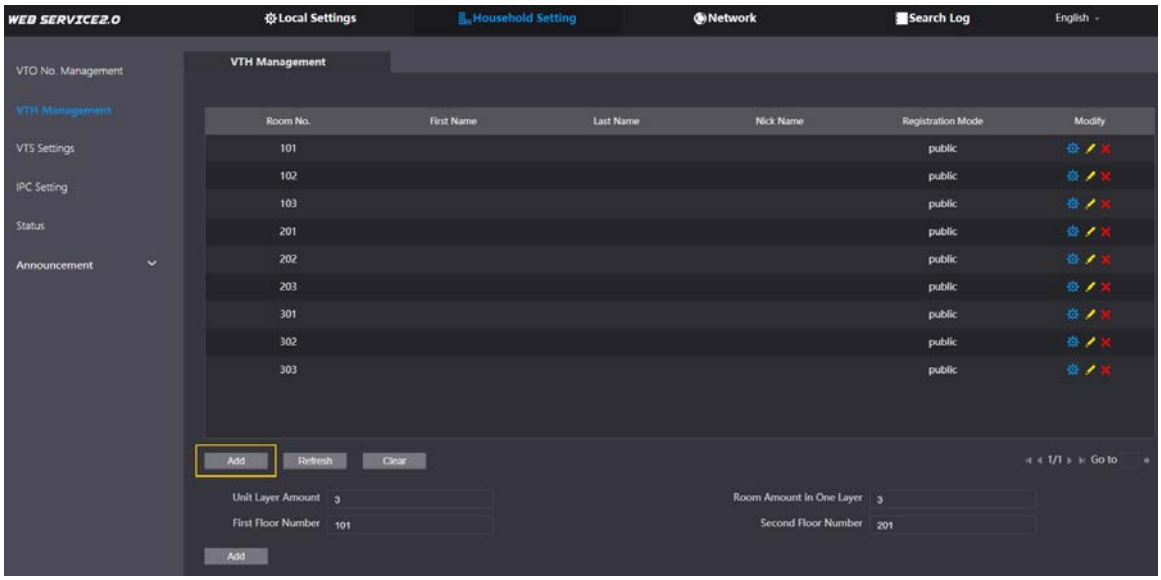


Step 2 Establecer**Tipo de dispositivo**a**Apartamento pequeño**y luego haga clic en**Ahorrar**.

Step 3 Seleccione**Configuración del hogar > Gestión de VTH**. Puede agregar un número de habitación individual o agregarlos en lotes.

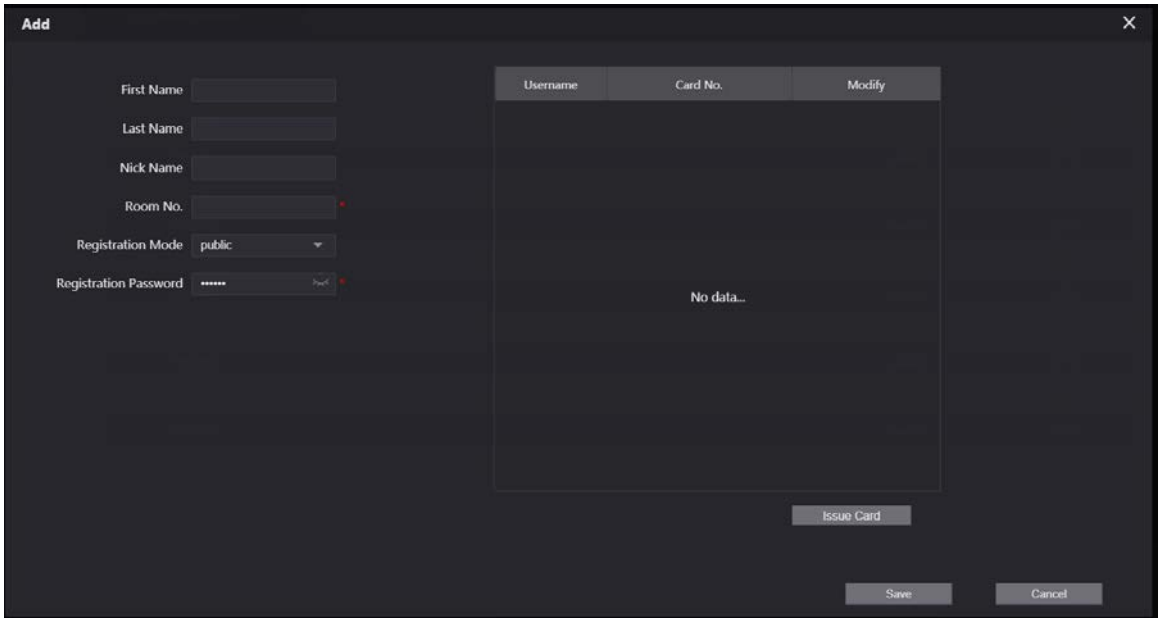
- Agregue un número de habitación individual.

Figure 3-12 Añadir números de habitación



1) Haga clic**Agregar**.

Figure 3-13 Añadir un número de habitación individual

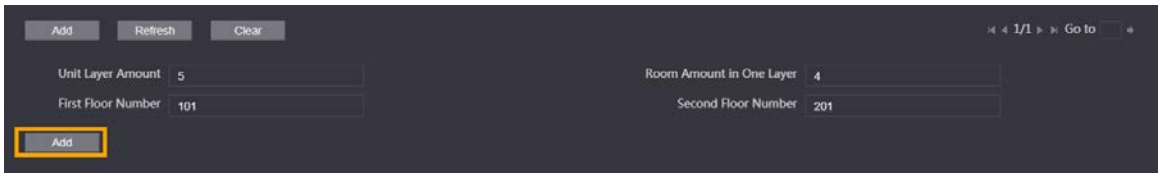


2) Configure la información de la izquierda. Consulte la Tabla 3-3 para obtener más detalles.

3) Haga clic**Ahorrar**.

- Agregue varios números de habitación.

Figure 3-14 Agregar números de habitación en lotes



1) Configurar la información.

- **Cantidad de capa de unidad**: El número de pisos en el apartamento. **Cantidad de**
- **habitación en una capa**: El número de habitaciones en un piso. **Número del**
- **primer piso**: El primer número de habitación en el primer piso. **Número del**
- **segundo piso**: El primer número de habitación en el segundo piso.

2) Haga clic**Agregar**y luego haga clic en**Actualizar**para ver el último estado

- Hacer clic  o  para modificar o eliminar un número de habitación.
- Hacer clic**Claro**para borrar todos los números de habitación.

3.2.7 Configuración del módulo

El módulo de la cámara se agrega de forma predeterminada. Todos los demás módulos deben agregarse en el diseño de la fachada antes de su uso.

El VTO puede tener hasta 9 módulos funcionales. Para módulo de huella dactilar, módulo de tarjeta y teclado módulo, puede agregar solo uno de cada tipo. Para otros módulos, puede agregar tantos como necesite.

3.2.7.1 Adición de módulos

Step 1 Seleccione**Configuración local > Básico > Diseño de fachada**.

Figure 3-15 Diseño de fachada

Step 2 Hacer clic  , se mostrarán los módulos disponibles.

El módulo de teclado, el módulo de tarjeta y el módulo de huellas dactilares no se mostrarán si tienen sido agregado

Step 3 Seleccione los módulos de acuerdo con el diseño real del VTO.

El orden debe ser de arriba a abajo y de izquierda a derecha.

Step 4 Hacer clic**Confirmar**y luego reinicie el navegador para aplicar los cambios.

3.2.7.2 Configuración de módulos

Debe configurar los números de habitación para el módulo de botones.

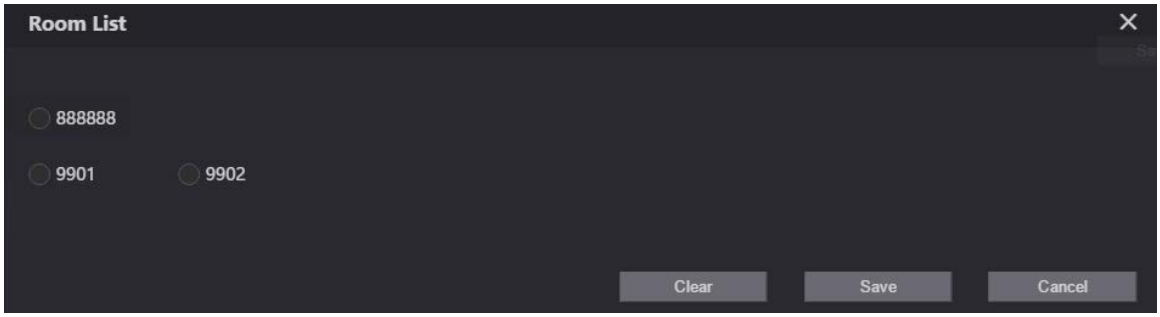
Step 1 Seleccione**Configuración local > Básico > Diseño de fachada**.

Figure 3-16 Configurar el módulo de botones

Step 2 Hacer clic  .

El número de habitación que se muestra en la interfaz corresponde al VTH agregado. "888888" es el número del centro de gestión.

Figure 3-17 Lista de habitaciones



Step 3 Seleccione el número de habitación y luego haga clic en**Ahorrar**.

Figure 3-18 Información del número de habitación

Step 4 Hacer clic**Confirmar**y luego reinicie el navegador para aplicar los cambios.

3.3 Puesta en marcha

3.3.1 VTO llamando a VTH

Step 1 Marque un número de habitación en el VTO.

Step 2 Prensa .

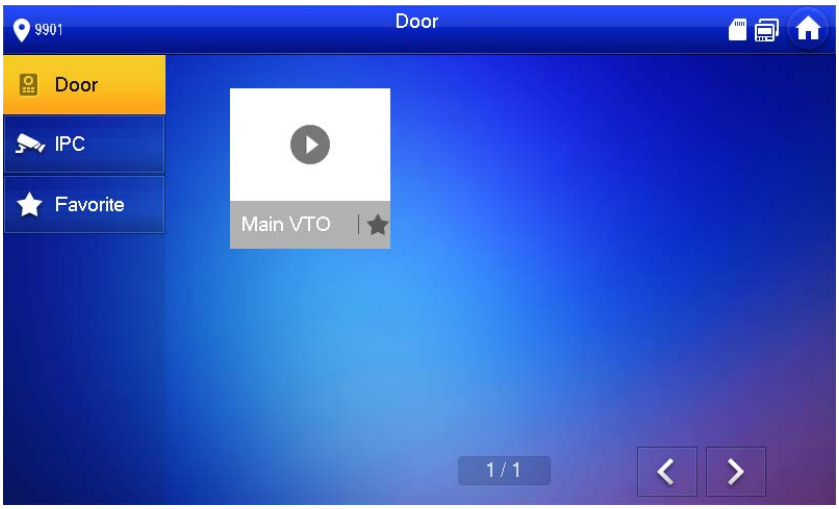
Step 3 Tocar en el VTH para contestar la llamada.

Figure 3-19 Pantalla de llamada

3.3.2 Monitoreo de VTH VTO

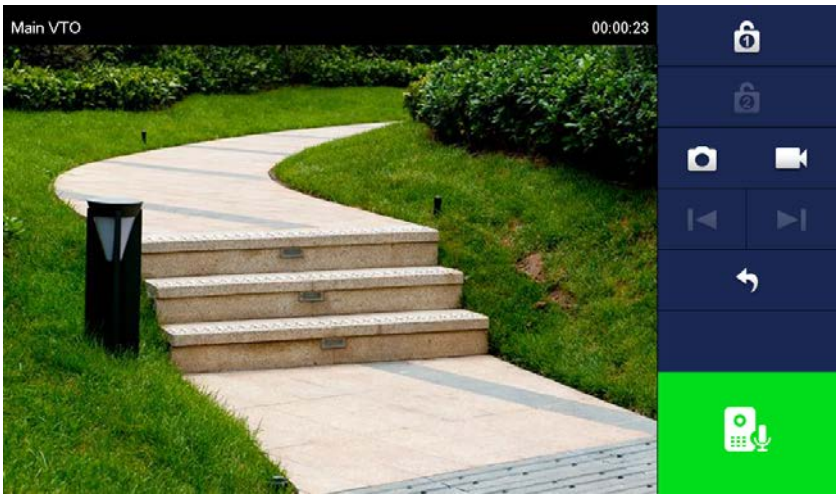
Step 1 En el VTH, seleccione**Supervisar > Puerta**.

Figure 3-20 Puerta



Step 2 Seleccione el VTO que desea monitorear.

Figure 3-21 Monitoreo de video



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 "verificación automática de actualizaciones" para obtener información oportuna de las actualizaciones de firmware lanzadas por el fabricante.
- Le sugerimos que descargue y utilice la última versión del software del cliente.

Recomendaciones "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.