Estación de puerta modular

Guía de inicio rápido

Versión 1.0.0

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 la estación de puerta modular (en adelante denominada "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

El suministro de energía se puede cortar solo después de que el dispositivo haya completado la actualización y se haya reiniciado.

Instrucciones de seguridad

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

Palabras de señal	Significado
PELIGRO	Indica un alto riesgo 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 ayudarle a resolver un problema o ahorrarle tiempo.
NOTA	Proporciona información adicional como énfasis y complemento al texto.

Historial de revisiones

Versión	Contenido de la revisión	Hora de lanzamiento
Versión 1.0.0	Primer lanzamiento.	Diciembre de 2020

Acerca del manual

- El manual es solo de referencia. Si existe alguna discrepancia entre el manual y el producto real, prevalecerá el producto real.
- No seremos responsables de ninguna pérdida causada por 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 existe alguna 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 provocar 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.
- Aún así, puede haber desviaciones en los datos técnicos, las funciones y la descripción de las operaciones, o errores en la impresión. Si tiene alguna duda o disputa, consulte nuestra explicación final.
- Actualice el software del lector o pruebe otro software de lectura convencional si no se puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas registradas y nombres de empresas en el manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, comuníquese con el proveedor o el servicio de atención al cliente si ocurre algún problema al utilizar el dispositivo.
- Si existe alguna incertidumbre 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 de usarlo para evitar peligros y pérdidas materiales. Siga estrictamente el manual durante la aplicación y consérvelo en un lugar adecuado para futuras consultas.

Requisitos de funcionamiento

- No exponga el dispositivo a la luz solar directa ni a fuentes de calor. No
- instale el dispositivo en un lugar húmedo o polvoriento.
- Instale el dispositivo en lugares estables de forma horizontal para evitar que se caiga.
- No deje que gotee ni salpique líquidos sobre el dispositivo ni coloque encima de él nada que contenga líquidos. Instale el
- dispositivo en lugares bien ventilados y no bloquee sus rejillas de ventilación.
- Utilice el dispositivo únicamente dentro del rango de entrada y salida
- nominales. No desmonte el dispositivo usted mismo.
- Transporte, utilice y almacene el dispositivo dentro del rango de humedad y temperatura permitidos.

Requisitos de energía

- Utilice cables eléctricos recomendados en su área y dentro de sus especificaciones nominales.
- Utilice una fuente de alimentación que cumpla con los requisitos de voltaje extra bajo de seguridad (SELV) y suministre energía con un voltaje nominal que cumpla con la norma de fuente de alimentación limitada de 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

Prólogo I
Medidas de seguridad y advertencias importantes ..... III 1
Descripción general 1
1.1 Introducción 1
1.2 Características 1
2 Estructura 2
2.1 Módulo de cámara 2
2.2 Módulo Indicador 3
2.3 Módulo de audio 4
2.4 Módulo de botones 5
2.5 Módulo de teclado (con Braille) 6
2.6 Módulo de tarjeta 6
2.7 Módulo de huellas dactilares 7
2.8 Módulo de visualización 7
2.9 Módulo en blanco 8
2.10 Conexión en cascada 8
3 Configuración y puesta en servicio 9
3.1 Procedimiento 9
3.2 Configuración de VTO 9
3.2.1 Inicialización 9
3.2.2 Configuración del número VTO 10
3.2.3 Configuración de parámetros de red 11
3.2.4 Configuración de servidores SIP 11
3.2.5 Adición de VTO 13
3.2.6 Agregar número de habitación 14
3.2.7 Configuración del módulo 17
3.3 Puesta en servicio 19
3.3.1 VTO llamando a VTH 19
3.3.2 Monitoreo VTH VTO 19
Appendix 1 Recomendaciones de ciberseguridad 21

1.1 Introducción

Puede construir el VTO modular con diferentes módulos, incluidos el módulo de cámara, el módulo indicador, el módulo de botones, el módulo de teclado, el módulo de tarjeta, el módulo de huellas dactilares, el módulo de audio y el módulo de pantalla. Los módulos de cámara y audio son indispensables y se pueden agregar otros 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 administración durante una emergencia.
- Desbloqueo: Tarjeta, huella dactilar, contraseña y desbloqueo remoto.
- Alarma: Alarma antimanipulación, alarma de contacto de puerta y alarma de desbloqueo por 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

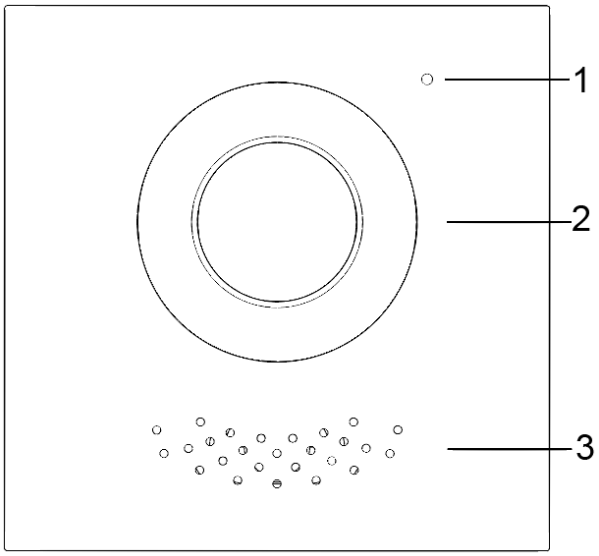


Tabla 2-1 Descripción del panel frontal

No.	Nombre
1	Micrófono
2	Cámara
3	Vocero

Figure 2-2 Panel trasero

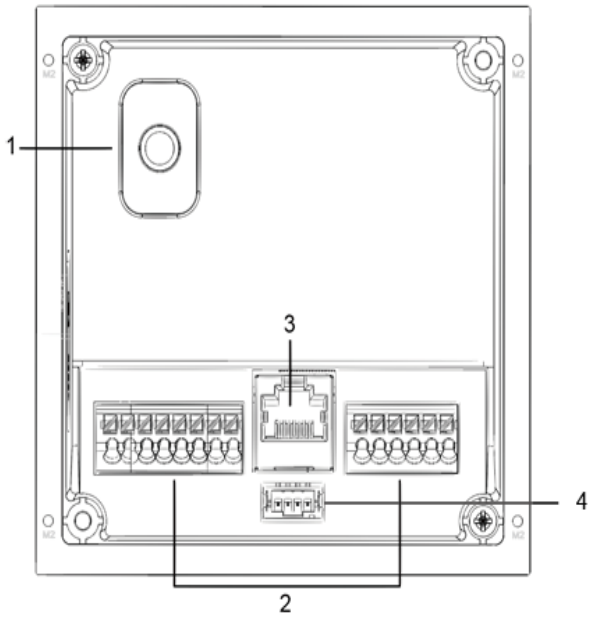


Tabla 2-2 Descripción del panel trasero

No.	Nombre	Descripción
1	Interruptor antimanipulación	Cuando el VTO se retira de la pared a la fuerza, se activará una alarma y la información de la alarma se enviará al centro de administración.
2	Puertos	Conectar a fuente de alimentación, cerradura de control eléctrico, cerradura solenoide y botón de salida.
3	Puerto Ethernet	Conectarse a los cables de red.
4	Puerto de conexión en cascada	Conectarse a otros módulos.

Figure 2-3 Descripción de los puertos

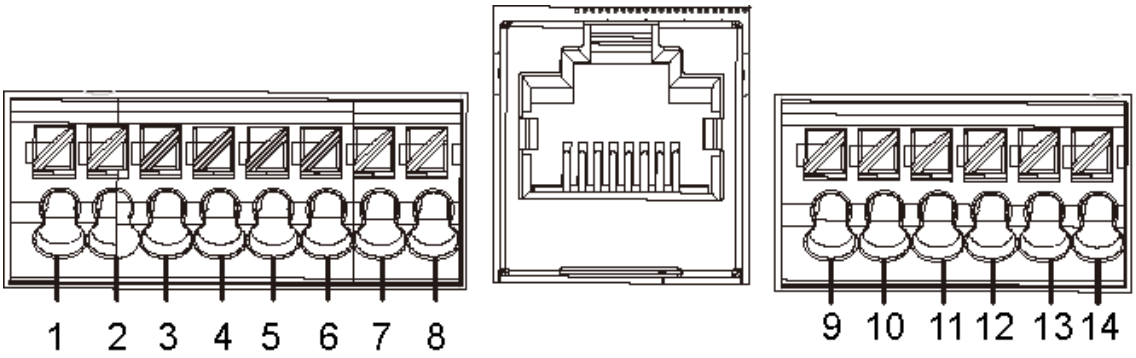


Tabla 2-3 Descripción del puerto

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

2.2 Módulo indicador

Figure 2-4 Panel frontal

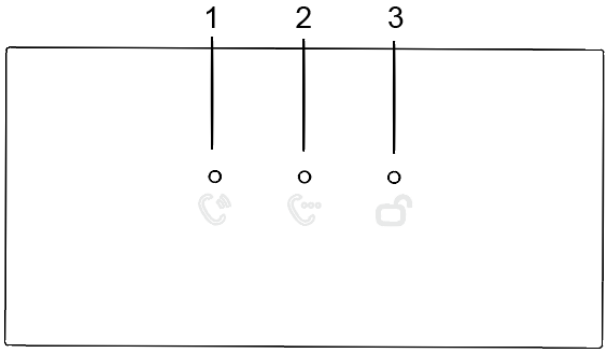


Tabla 2-4 Descripción del módulo indicador (1)

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

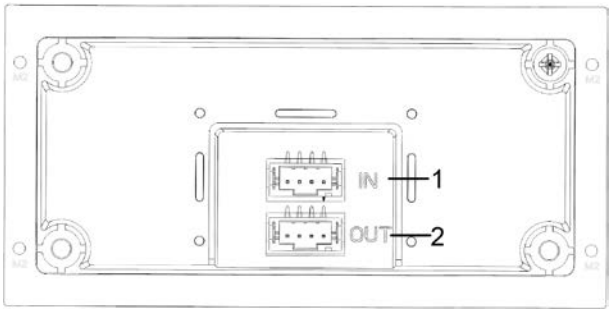


Tabla 2-5 Descripción del módulo indicador (2)

No.	Nombre	Descripción
1	Entrada en cascada	Conectarse 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

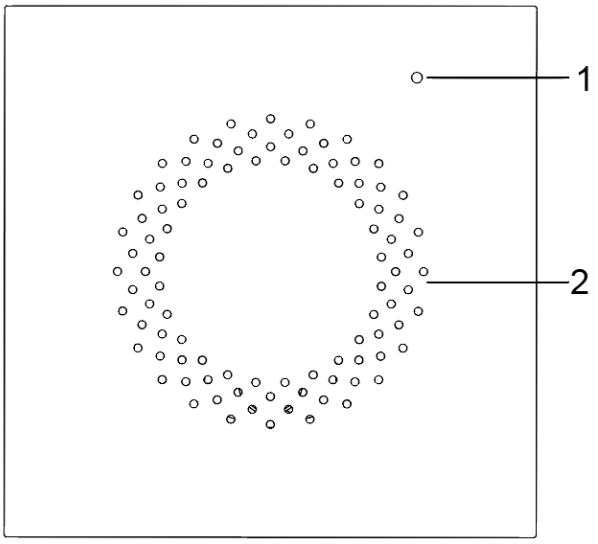


Tabla 2-6 Descripción del módulo de audio

No.	Nombre
1	Micrófono
2	Vocero

2.4 Módulo de botones

Hay módulos de un botón, de dos botones y de cinco botones con la misma función. Aquí tomamos como ejemplo el módulo de cinco botones.

Figure 2-7 Panel frontal del módulo de cinco botones

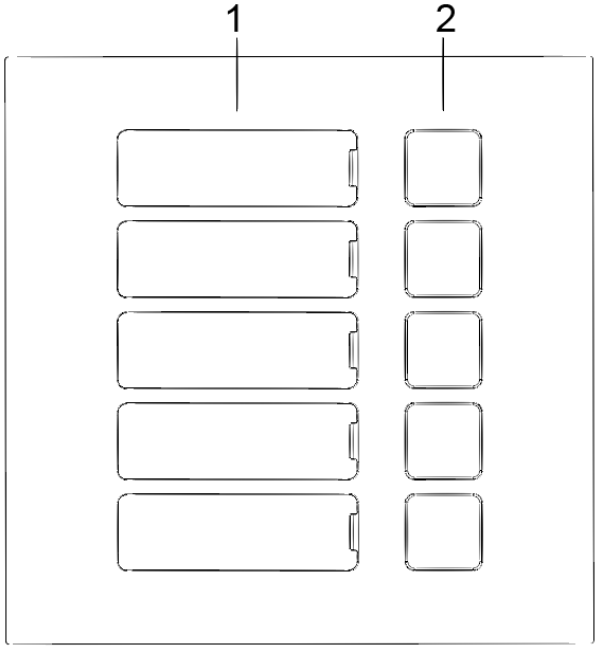


Tabla 2-7 Descripción del panel frontal

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

Figure 2-8 Panel trasero del módulo de cinco botones

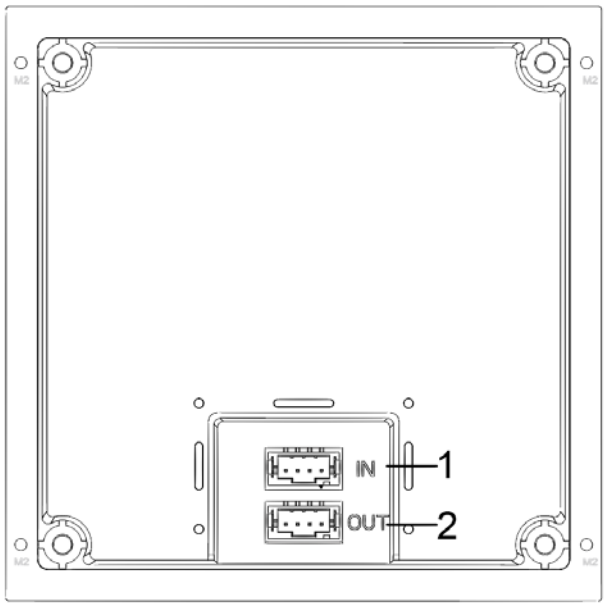


Tabla 2-8 Descripción del panel trasero

No.	Nombre
1	Entrada en cascada
2	Salida en cascada

2.5 Módulo de teclado (con Braille)

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

Figure 2-9 Módulo de teclado

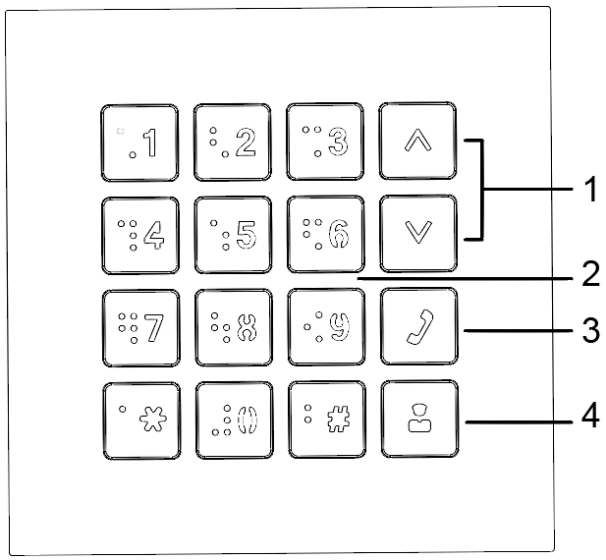


Tabla 2-9 Descripción del módulo de teclado

No.	Nombre	Descripción
1	Selección	—
2	Números	Introduzca la contraseña o los números VTH.
3	Llamar	Llamar a VTHs.
4	Centro de gestión de llamadas	—

2.6 Módulo de tarjeta

Desliza tu tarjeta cerca del ícono.

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

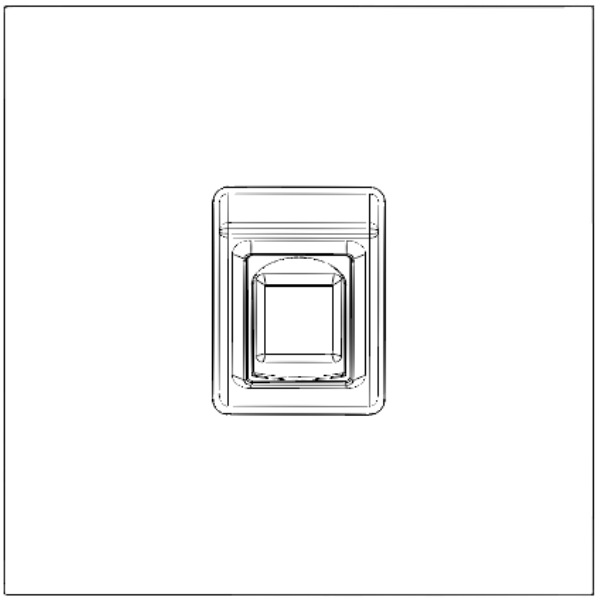
Figure 2-10 Módulo de tarjeta

2.7 Módulo de huellas dactilares

Recoge y verifica huellas dactilares.

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

Figure 2-11 Módulo de huellas dactilares

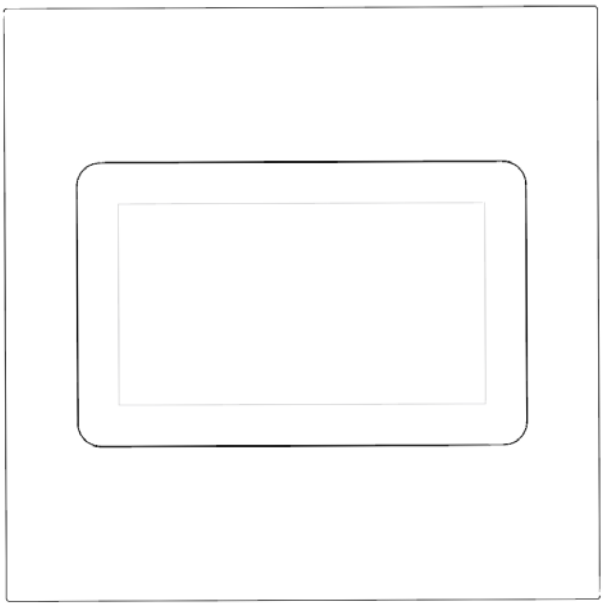


2.8 Módulo de visualización

Muestra información del usuario.

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

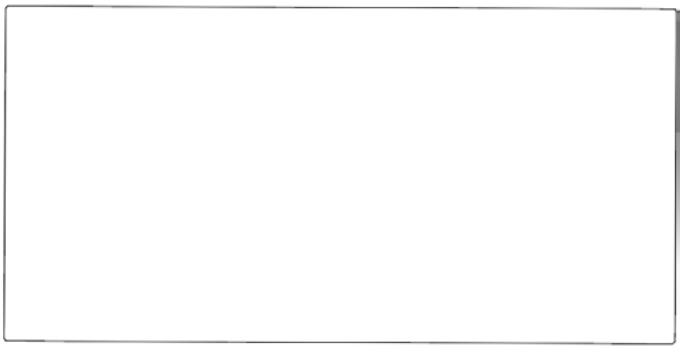
Figure 2-12 Módulo de visualización



2.9 Módulo en blanco

Para una mejor apariencia, utilice el módulo en blanco si hay espacio extra al colocar los módulos juntos.

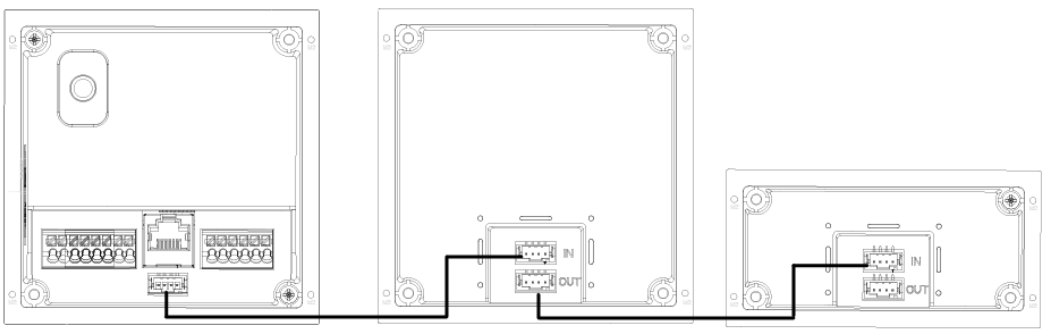
Figure 2-13 Módulo en blanco



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 haya configurado para el VTO. prevalecerán la interfaz y la función.

3.1 Procedimiento

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

Step 1 Planifique la dirección IP y el número de unidad/sala (funciona como un número de teléfono) para cada dispositivo.

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

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

Step 4 los ajustes sean 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, deberá crear una nueva contraseña para la interfaz web.

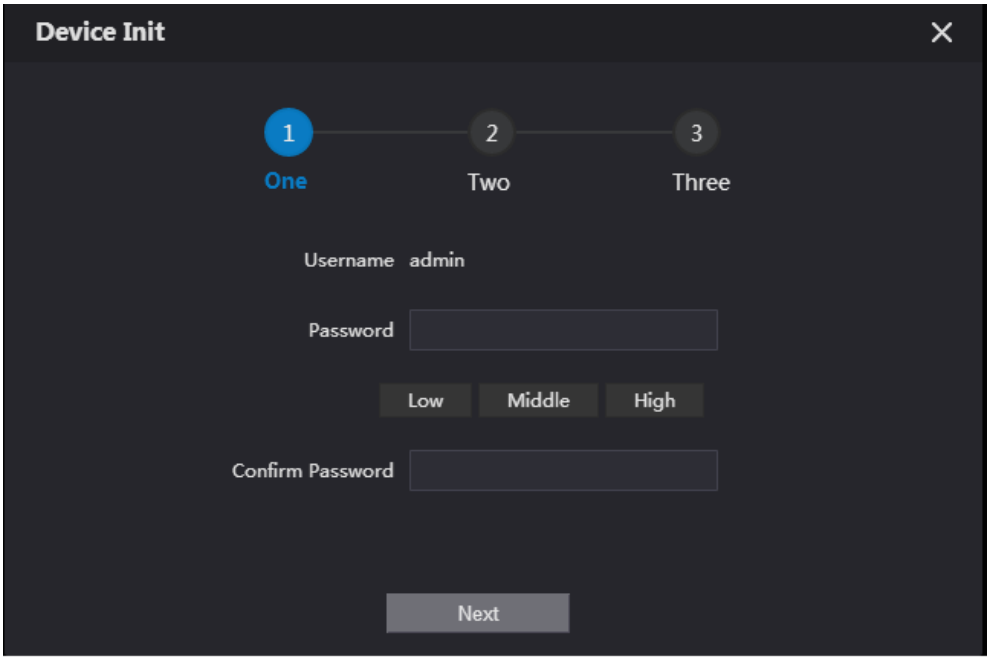
3.2.1 Inicialización

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, Recomendamos cambiar la dirección IP predeterminada (**Red > Básica**) para evitar conflictos.

Figure 3-1 Inicialización del dispositivo



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

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

Step 5 Haga clic en**DE ACUERDO**El sistema pasa a la interfaz de inicio de sesión.

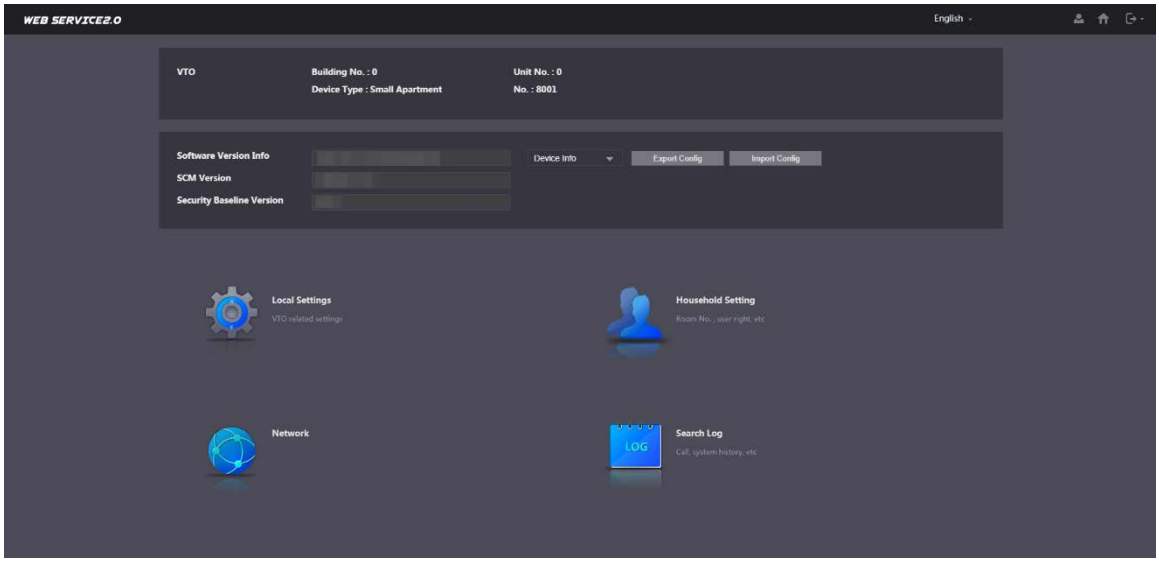
3.2.2 Configuración del número VTO

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 esté funcionando como servidor SIP. Un número VTO puede contiene 5 números como máximo y no puede ser el mismo que cualquier número de habitación.

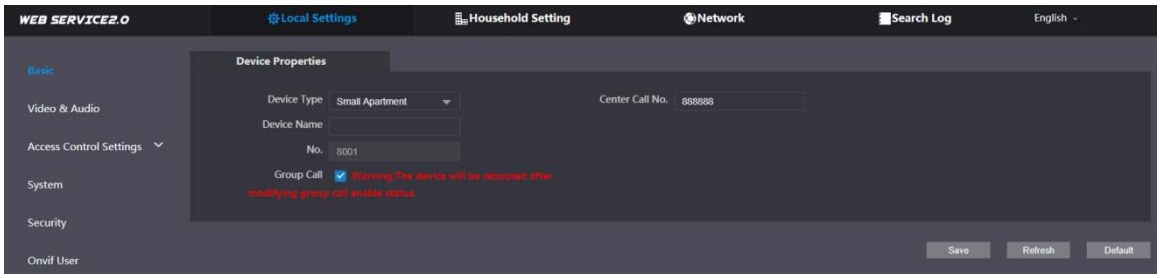
Step 1 Inicie sesión en la interfaz web de VTO.

Figure 3-2 Interfaz principal



Step 2 Seleccionar**Configuración local > Básica**.

Figure 3-3 Propiedades del dispositivo

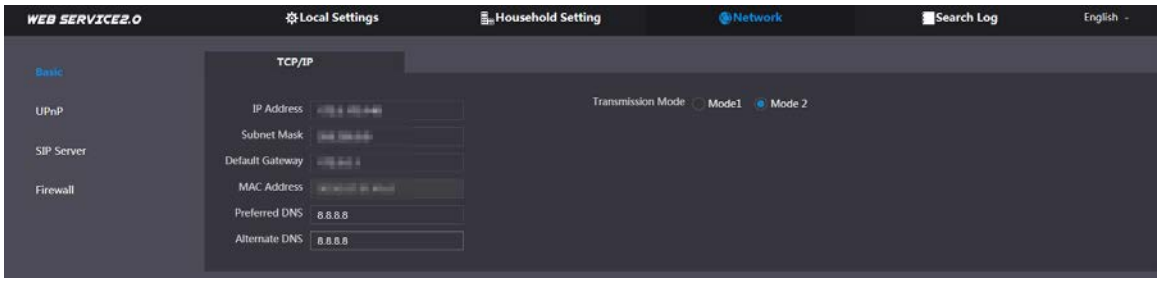


Step 3 Introduzca el número en**No.**y luego haga clic en**Ahorrar**.

3.2.3 Configuración de parámetros de red

Step 1 Seleccionar**Red > Básica**.

Figure 3-4 Información TCP/IP



Step 2 Introduzca los parámetros y haga clic**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

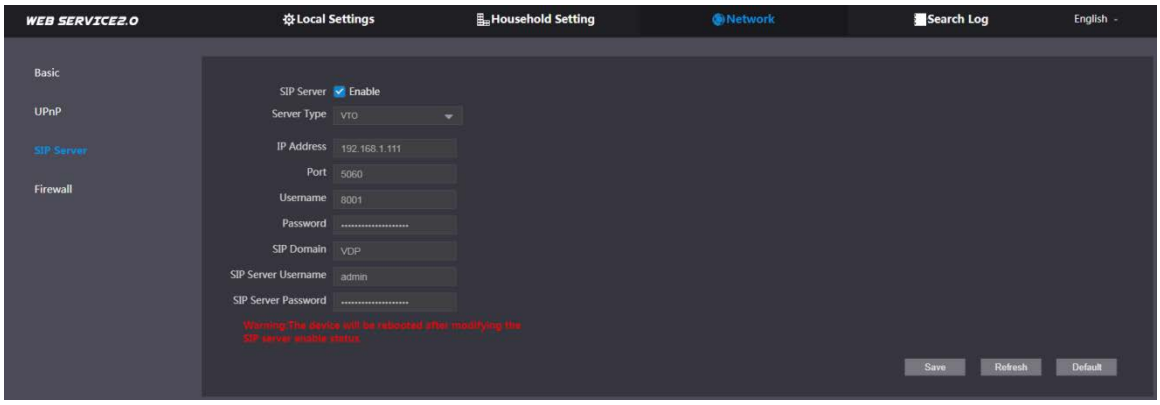
Cuando se conectan al mismo servidor SIP, todos los VTO y VTH pueden llamarse entre sí. Puede utilizar un VTO u otros servidores como servidor SIP.

- Si el VTO actual es el servidor SIP,**Edificio No.**y**Unidad No.**No se mostrará en el **Propiedades del dispositivo**interfaz.
- Si vas a**Configuración de red > Servidor SIP**, permitir**Servidor alternativo**y acceder a la web Interfaz de nuevo,**Edificio No.**y**Unidad No.**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 se aplica solo a un edificio.

1) Habilitar**Servidor SIP**.

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

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

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

- Plataforma (Express/DSS) como servidor SIP: esto se aplica a varios edificios o unidades. Si no tiene una plataforma, utilice un VTO como servidor SIP.

1) Deshabilitar**Servidor SIP**.

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

3) Configure 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 de forma predeterminada cuando VTO funciona como servidor SIP. 5080 de forma ● predeterminada cuando la plataforma funciona como servidor SIP.
Nombre de usuario/Contraseña	Mantenlo por defecto
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/ Contraseña	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 alternativa de VTS.	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 del VTS y el VTO se reiniciará.

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

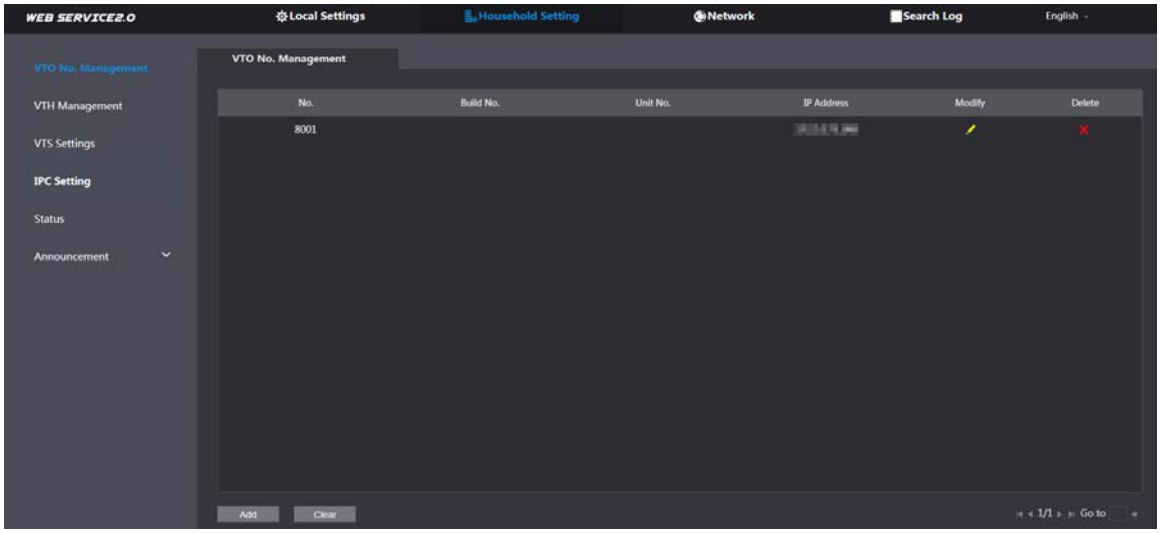
Cuando una plataforma funciona como servidor SIP, habilite**Edificio de apoyo**y**Unidad de apoyo**primero si Es necesario establecer el número del edificio y el número de unidad del edificio.

3.2.5 Agregar 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 es aplicable cuando 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.

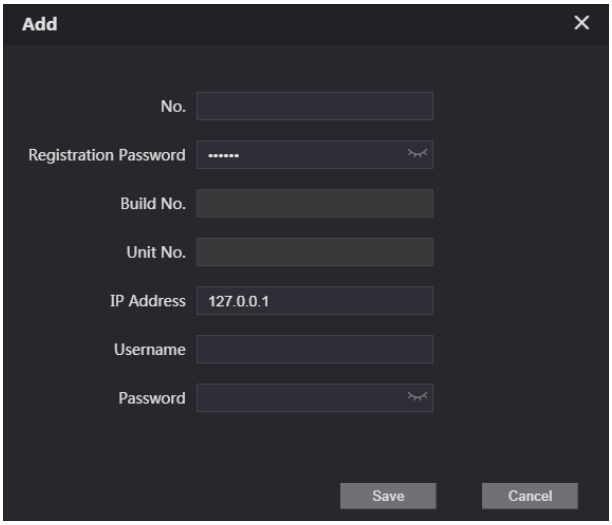
Step 1 Inicie sesión en la interfaz web del servidor SIP y luego seleccione**Configuración del hogar > Gestión de número de VTO**.

Figure 3-6 Gestión de números VTO



Step 2 Hacer clic**Agregar**.

Figure 3-7 Agregar VTO



Step 3 Configurar los parámetros.

Se debe agregar el servidor SIP.

Tabla 3-2 Agregar VTO

Parámetro	Descripción
Rec. Nro.	Número de VTO. Consulte "3.2.2 Configuración del número de VTO".
Registrar contraseña	Mantenlo por defecto
Número de compilación	Disponible solo cuando otros servidores funcionan como servidor SIP.
Unidad No.	
Dirección IP	Dirección IP VTO.
Nombre de usuario	Nombre de usuario y contraseña para iniciar sesión en la interfaz web de VTO.
Contraseña	

Step 4 Hacer clic**Ahorrar**.

3.2.6 Agregar número de habitación

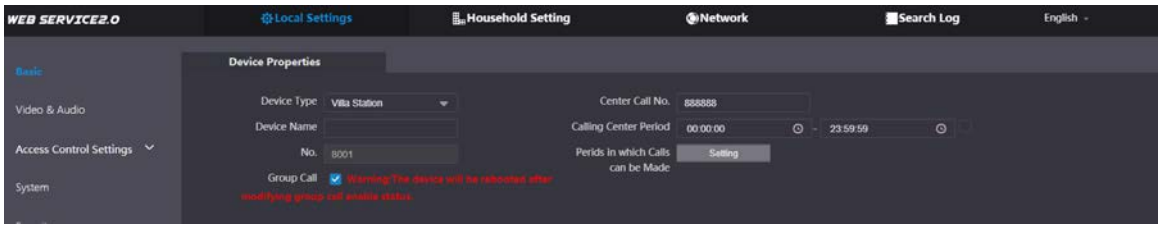
Puede agregar el número de habitación planificado al servidor SIP y luego configurar el número de habitación en los dispositivos VTH para conectarlos a la red. Esta sección es aplicable cuando el VTO funciona como servidor SIP y, si utiliza otros servidores como servidor SIP, consulte el manual correspondiente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

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

Utilizando el VTO en una Villa

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

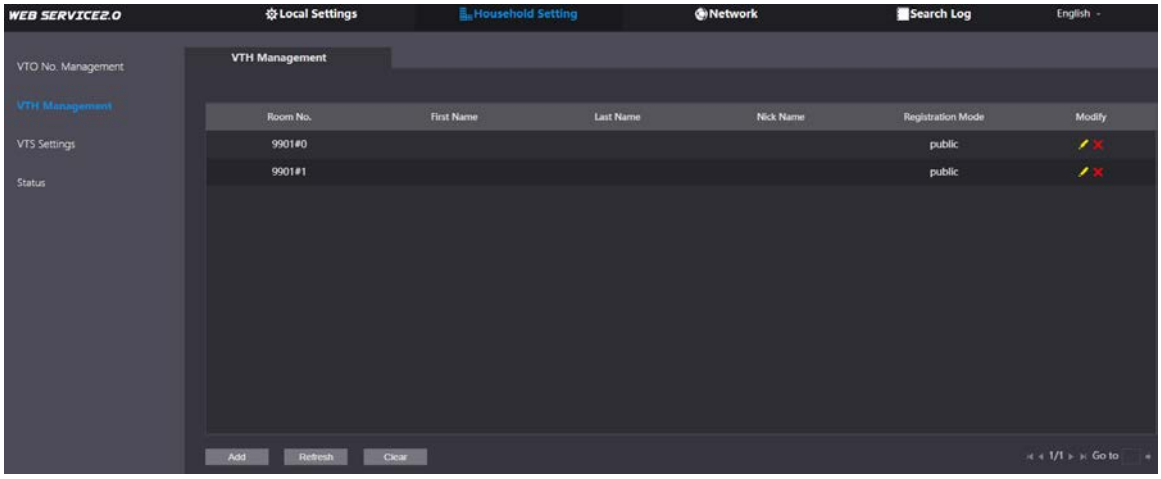
Figure 3-8 Propiedades del dispositivo



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

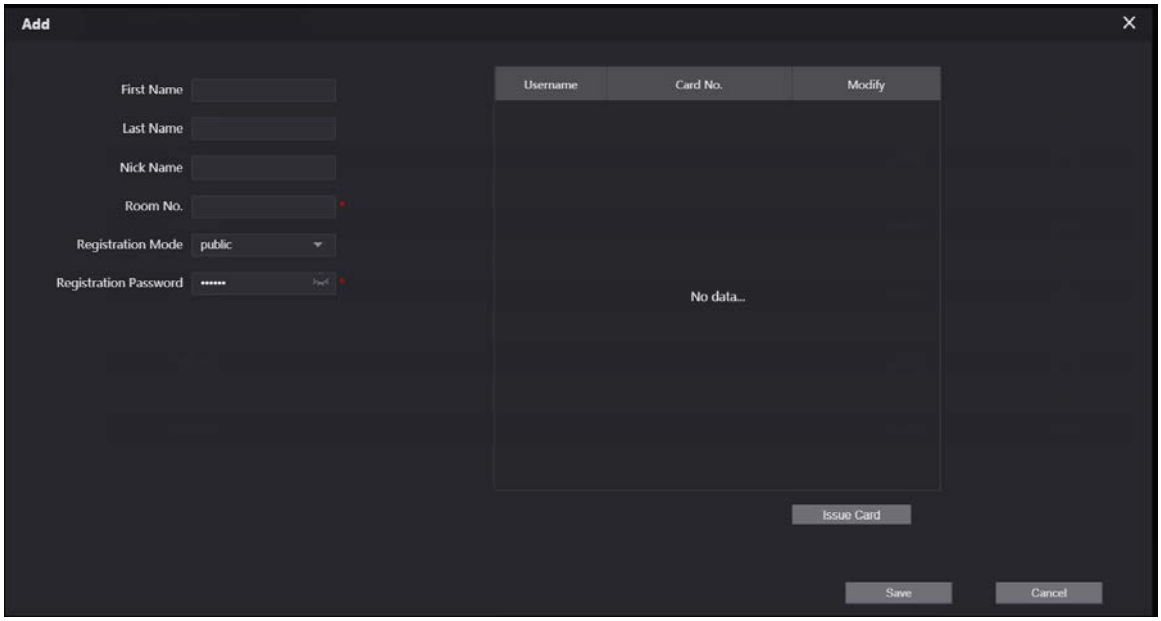
Step 3 **Ahorrar**. Seleccionar**Entorno doméstico > Gestión de VTH**.

Figure 3-9 Gestión de números de habitaciones



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
Nombre de pila	Información utilizada para diferenciar cada habitación.
Apellido	
Apodo	
Habitación N°	● Cuando hay varios VTH, el número de habitación del VTH principal debe terminar con #0 y los números de habitación de los VTH secundarios con #1, #2... ● Puedes tener hasta 10 VTH secundarios para un VTH principal.
Registro Tipo	Seleccionar**público**.
Registro Contraseña	Mantenlo por defecto

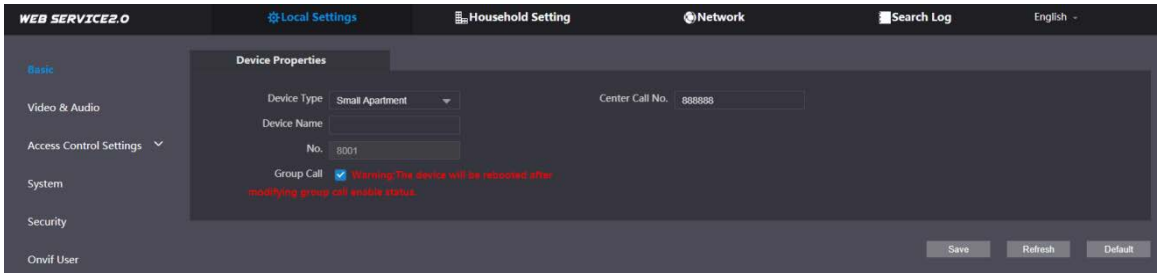
Step 6 Hacer clic**Ahorrar**.

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

Uso del VTO en un apartamento pequeño

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

Figure 3-11 Propiedades del dispositivo

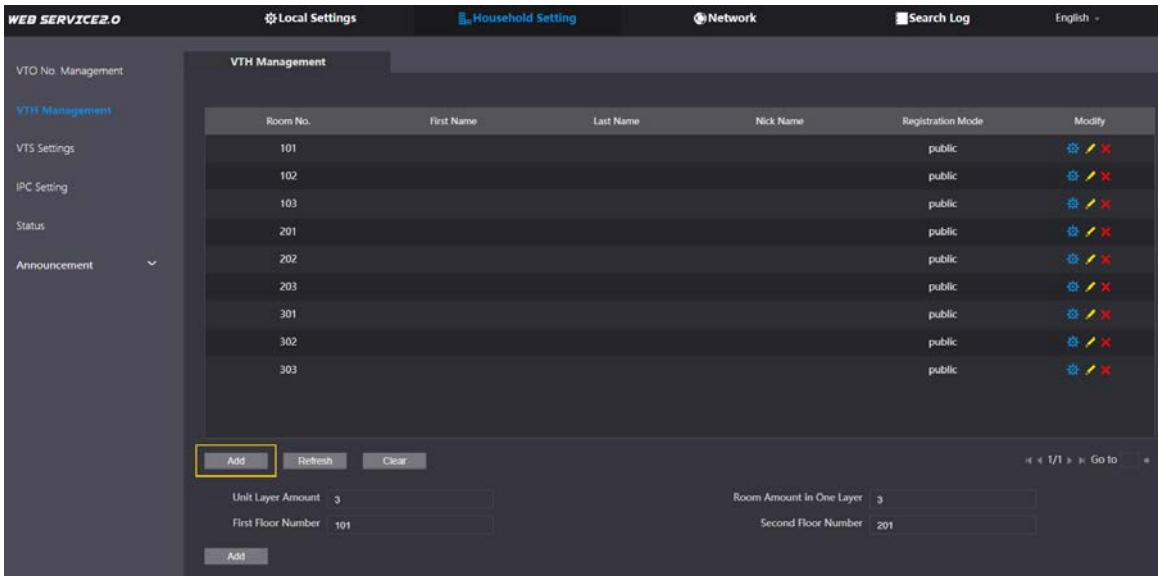


Step 2 Colocar**Tipo de dispositivo**a**Apartamento pequeño**y luego haga clic en**Ahorrar**.

Step 3 Seleccionar**Entorno doméstico > Gestión de VTH**Puede agregar un solo número de habitación o agregarlos en lotes.

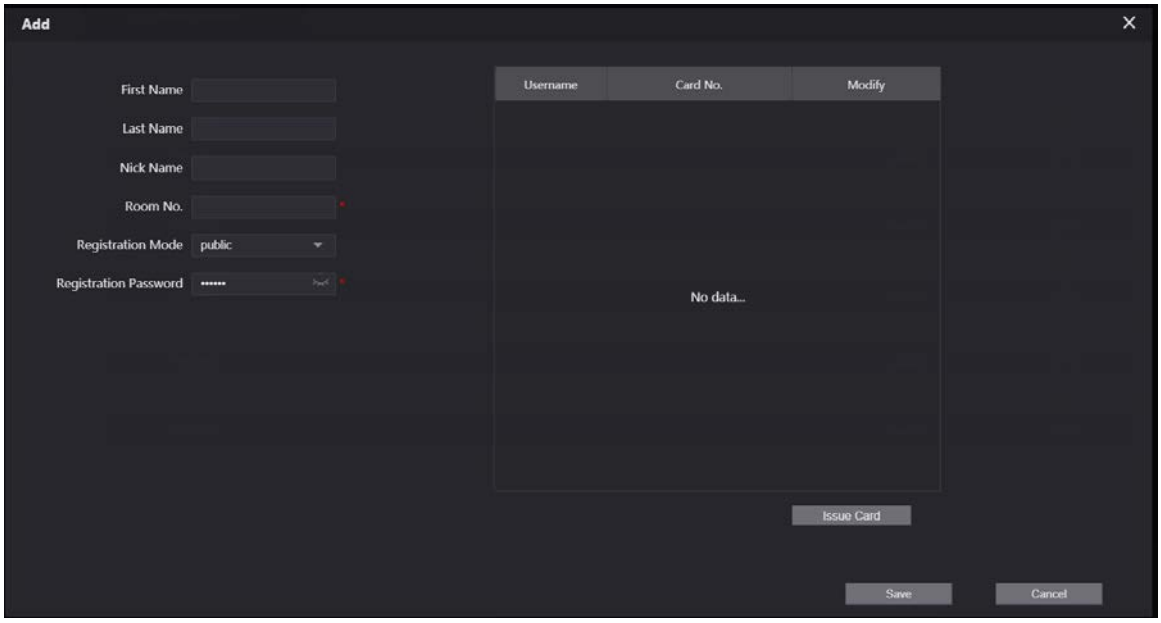
- Añade un número de habitación individual.

Figure 3-12 Añadir números de habitación



1) Haga clic**Agregar**.

Figure 3-13 Añadir un número de habitación individual

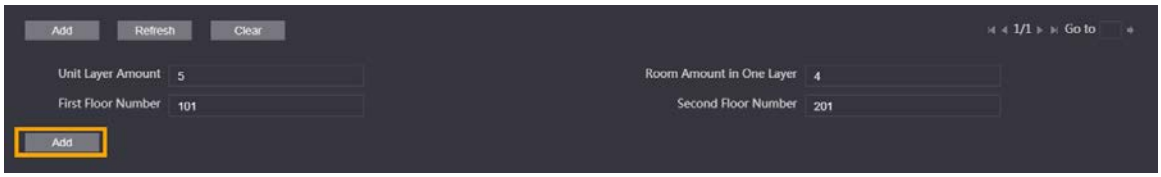


2) Configure la información de la izquierda. Consulte la Tabla 3-3 para obtener más detalles.

3) Haga clic**Ahorrar**.

- Agregar varios números de habitaciones.

Figure 3-14 Agregar números de habitaciones en lotes



1) Configurar la información.

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

2) Haga clic**Agregar**y luego haga clic en**Refrescar**Para ver el estado más reciente

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

3.2.7 Configuración del módulo

El módulo de cámara se agrega de manera 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: módulo de huellas dactilares, módulo de tarjeta y teclado. Módulo, puedes agregar solo uno de cada tipo. Para otros módulos, puedes agregar tantos como necesites.

3.2.7.1 Agregar módulos

Step 1 Seleccionar**Configuración local > Básica > Diseño de fachada**.

Figure 3-15 Disposición de la 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 Se ha añadido.

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

El orden debe ser de arriba hacia 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.

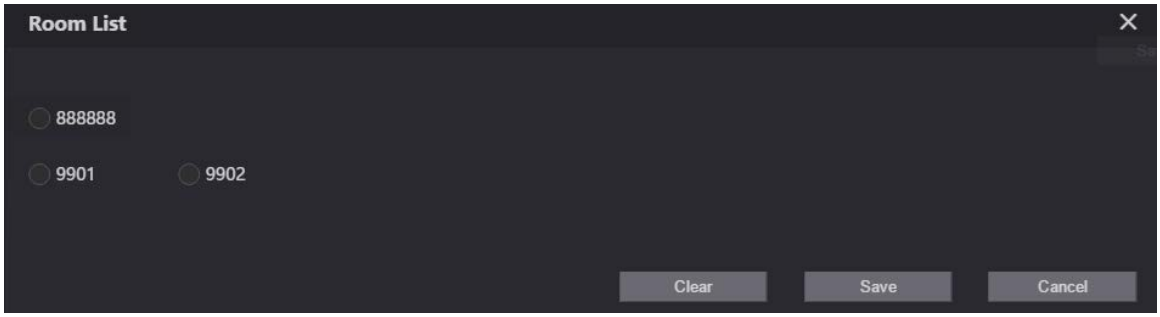
Step 1 Seleccionar**Configuración local > Básica > Diseño de fachada**.

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 servicio

3.3.1 VTO llamando a VTH

Step 1 Marque un número de habitación en el VTO.

Step 2 Prensa .

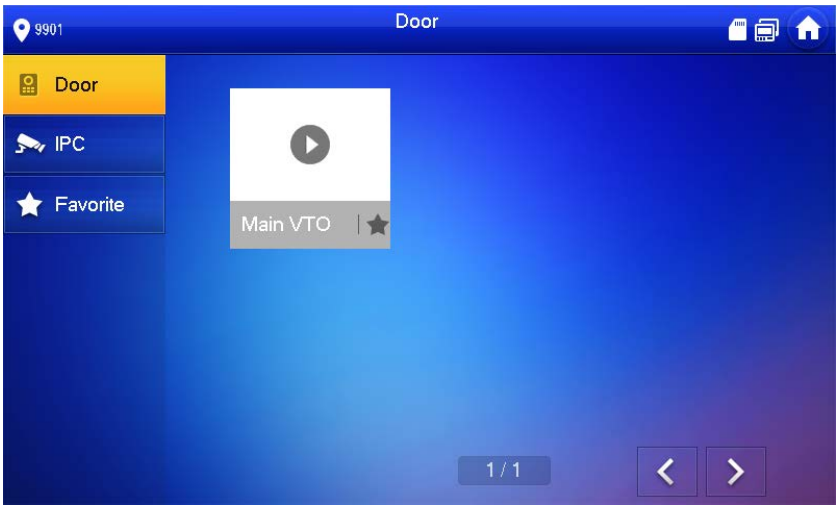
Step 3 Grifo en el VTH para responder al llamado.

Figure 3-19 Pantalla de llamada

3.3.2 Monitoreo de VTH VTO

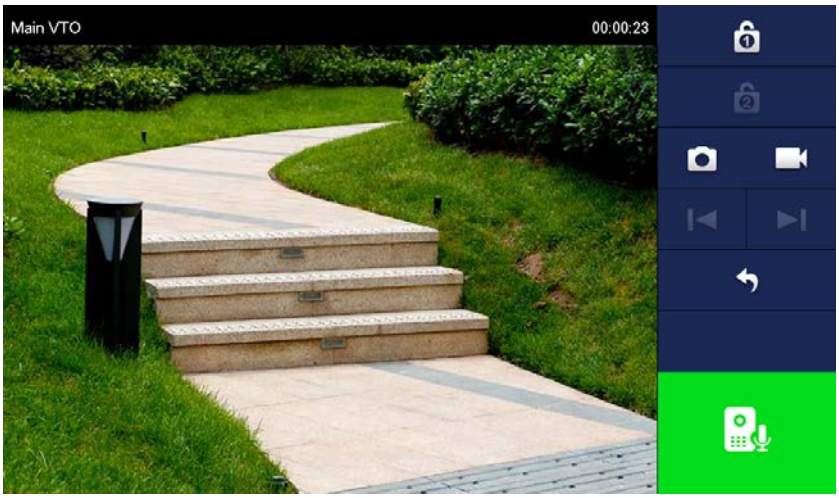
Step 1 En el VTH, seleccione**Monitor > Puerta**.

Figure 3-20 Puerta



Step 2 Seleccione el VTO que desea monitorear.

Figure 3-21 Vídeo de vigilancia



Appendix 1 Recomendaciones de ciberseguridad

La ciberseguridad es más que una palabra de moda: es algo que concierne a todos los dispositivos conectados a Internet. La videovigilancia IP no es inmune a los riesgos cibernéticos, pero tomar medidas básicas para proteger y fortalecer las redes y los dispositivos conectados los hará menos susceptibles a los ataques. A continuación, se ofrecen 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. 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 caracteres; los tipos de caracteres incluyen letras mayúsculas y minúsculas, números y símbolos;
- No contenga el nombre de la cuenta ni 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 esté conectado a la red pública, se recomienda habilitar la función de "comprobación automática de actualizaciones" para obtener información oportuna sobre las actualizaciones de firmware publicadas por el fabricante.
- Le sugerimos que descargue y utilice la última versión del software del cliente.

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

Le sugerimos que proteja físicamente el dispositivo, especialmente los dispositivos de almacenamiento. Por ejemplo, coloque el dispositivo en una sala de computadoras y un gabinete especiales e implemente un control de acceso y una gestión de claves bien hechos para evitar que personal no autorizado realice contactos físicos, como dañar el hardware, conectar sin autorización dispositivos extraíbles (como un disco flash USB, un puerto serial), etc.

2. Cambie las contraseñas periódicamente

Le sugerimos que cambie sus contraseñas periódicamente para reducir el riesgo de que sean adivinadas o descifradas.

3. Establezca y actualice la información de restablecimiento de contraseñas de manera oportuna

El dispositivo admite la función de restablecimiento de contraseña. Configure a tiempo la información relacionada con el restablecimiento de contraseña, incluido el buzón de correo del usuario final y las preguntas de protección de contraseña. Si la información cambia, modifíquela a tiempo. Al configurar las preguntas de protección de contraseña, se recomienda no utilizar aquellas que se puedan adivinar fácilmente.

4. Habilitar bloqueo de cuenta

La función de bloqueo de cuenta está activada 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, se bloqueará la cuenta correspondiente y la dirección IP de origen.

5. Cambiar el puerto 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 externas puedan adivinar qué puertos está utilizando.

6. Habilitar HTTPS

Le sugerimos que habilite HTTPS, para que pueda visitar el servicio web a través de un canal de comunicación seguro.

7. Vinculación de direcciones MAC

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

8. Asignar cuentas y privilegios de manera razonable

Según los requisitos comerciales y de gestión, agregue usuarios de manera razonable y asígneles un conjunto mínimo de permisos.

9. Desactivar servicios innecesarios y elegir 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 cifrado y autenticación seguras.
- SMTP: Elija TLS para acceder al servidor de buzón. FTP:
- Elija SFTP y configure contraseñas seguras.
- Punto de acceso AP: elija el modo de cifrado WPA2-PSK y configure contraseñas seguras.

10. Transmisión de audio y vídeo encriptados

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 que los datos de audio y video sean robados durante la transmisión.

Recordatorio: la transmisión cifrada provocará cierta pérdida en la eficiencia de transmisión.

11. Auditoría segura

- Comprobar usuarios en línea: le sugerimos que compruebe periódicamente los usuarios en línea para ver si el dispositivo ha iniciado sesión sin autorización.
- Comprobar el registro del dispositivo: al ver los registros, puede conocer las direcciones IP que se utilizaron 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 un período prolongado, se recomienda que habilite la función de registro de red para garantizar que los registros críticos se sincronicen con el servidor de registro de red para realizar el 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 la red externa.
- La red debe estar dividida y aislada de acuerdo con las necesidades reales de la red. Si no hay requisitos de comunicación entre dos subredes, se recomienda utilizar VLAN, GAP de red y otras tecnologías para dividir la red, a fin de lograr el efecto de aislamiento de la red.
- Establecer el sistema de autenticación de acceso 802.1x para reducir el riesgo de acceso no autorizado a redes privadas.
- Habilite la función de filtrado de direcciones IP/MAC para limitar el rango de hosts a los que se les permite acceder al dispositivo.