

Monitor interior digital (Modelo G)

Guía de inicio rápido



Prefacio

General






Este manual presenta las operaciones básicas del monitor interior digital (en lo sucesivo, "VTH").

Modelos

- VTH no de 2 hilos compatible con Wi-Fi y PoE.
- VTH no de 2 hilos que solo admite PoE.
- VTH de 2 hilos que admite Wi-Fi.

Las instrucciones de seguridad

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

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

Revisión histórica

Versión	Contenido de revisión	Fecha de lanzamiento
V1.0.1	Optimización manual.	febrero 2022
V1.0.0	Primer lanzamiento.	noviembre 2021

Aviso de protección de privacidad

Como usuario del dispositivo o controlador de datos, puede recopilar datos personales de otros, como su rostro, huellas dactilares y número de matrícula. 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: Proporcionar una identificación clara y visible para informar a las personas sobre la existencia del área de vigilancia y proporcione la información de contacto requerida.

Sobre el Manual

- El manual es solo para referencia. Se pueden encontrar ligeras diferencias entre el manual y el producto.
- No somos responsables de las pérdidas sufridas debido a la operación del producto de manera que no cumpla con el manual.
- El manual se actualizará de acuerdo con las últimas leyes y reglamentos de las jurisdicciones relacionadas. Para obtener información detallada, consulte el manual del usuario en papel, use nuestro CD-ROM, escanee el código QR o visite nuestro sitio web oficial. El manual es solo para referencia. Se pueden encontrar ligeras diferencias entre la versión electrónica y la versión en papel.
- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto pueden dar lugar a que aparezcan 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.
- Puede haber errores en la impresión o desviaciones en la descripción de las funciones, operaciones y datos técnicos. Si hay alguna duda o disputa, nos reservamos el derecho de dar una 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 registradas y nombres de compañías en el manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, póngase en contacto con el proveedor o con el servicio de atención al cliente si se produce algún problema durante el uso del dispositivo.
- Si hay alguna duda o controversia, nos reservamos el derecho de la explicación final.

Medidas de seguridad y advertencias importantes

Esta sección presenta contenido que cubre el manejo adecuado del dispositivo, la prevención de riesgos y la prevención de daños a la propiedad. Lea atentamente antes de usar el dispositivo, cumpla con las pautas cuando lo use y guarde el manual en un lugar seguro para futuras consultas.

Requisitos de operación



- Compruebe si la fuente de alimentación es correcta antes de usar.
- No desconecte el cable de alimentación del lateral del dispositivo mientras el adaptador está encendido.
- Opere el dispositivo dentro del rango nominal de entrada y salida de energía.
- Transporte, use y almacene el dispositivo en condiciones de humedad y temperatura permitidas.
- No deje caer ni salpique líquido sobre el dispositivo y asegúrese de que no haya ningún objeto lleno de líquido sobre el dispositivo para evitar que el líquido fluya hacia él.
- No desmonte el dispositivo sin instrucción profesional.

requerimientos de instalación



WARNING

- No conecte el adaptador de corriente al dispositivo mientras el adaptador esté encendido.
- Cumpla estrictamente con el código y las normas locales de seguridad eléctrica. Asegúrese de que el voltaje ambiental sea estable y cumpla con los requisitos de suministro de energía del dispositivo.
- No conecte el dispositivo a dos o más tipos de fuentes de alimentación para evitar daños al dispositivo.
- El uso inadecuado de la batería puede provocar un incendio o una explosión.



- El personal que trabaje en alturas debe tomar todas las medidas necesarias para garantizar su seguridad personal, incluido el uso de casco y cinturones de seguridad.
- No coloque el dispositivo en un lugar expuesto a la luz solar o cerca de fuentes de calor.
- Mantenga el dispositivo alejado de la humedad, el polvo y el hollín.
- Instale el dispositivo en una superficie estable para evitar que se caiga.
- Instale el dispositivo en un lugar bien ventilado y no bloquee su ventilación.
- Utilice un adaptador o una fuente de alimentación de gabinete proporcionada por el fabricante.
- Utilice los cables de alimentación recomendados para la región y cumpla con las especificaciones de potencia nominal.
- Asegúrese de que la fuente de alimentación cumpla con los requisitos SELV (voltaje extrabajo de seguridad) y que el voltaje nominal cumpla con el estándar IEC60065, IEC60950-1 o IEC62368-1. Los requisitos de la fuente de alimentación están sujetos a la etiqueta del dispositivo.
- El dispositivo es un aparato eléctrico de clase I. Asegúrese de que la fuente de alimentación del dispositivo esté conectada a una toma de corriente con protección a tierra.

Tabla de contenido

Prefacio.....	I Medidas
de seguridad y advertencias importantes	III 1
Estructura	1
1.1 Panel frontal.....	1
1.2 Panel trasero (2 hilos)	2
1.3 Panel trasero (no de 2 hilos)	3
2 Instalación.....	4
2.1 Preparativos	4
2.2 Instalación en pared	4
3 Configuración de VTO.....	5
3.1 Herramienta de configuración	5
3.2 Inicialización.....	5
3.3 Configuración del número VTO	7
3.4 Configuración de parámetros de red	7
3.5 Configuración del servidor SIP	8
3.6 Configuración de número de llamada y llamada de grupo	9
3.7 Adición de VTO	10
3.8 Adición de número de habitación	11
4 Configuración VTH.....	13
4.1 Antes de comenzar	13
4.2 Configuración rápida.....	13
4.3 Configuración manual	dieciséis
4.3.1 Configuración de parámetros de red	dieciséis
4.3.2 Configuración del servidor SIP	17
4.3.3 Configuración de VTH.....	18
4.3.4 Configuración de VTO.....	19
5 Puesta en servicio.....	21
5.1 VTO llamando a VTH	21
5.2 Monitoreo de VTH VTO	21
Apéndice 1 Recomendaciones sobre ciberseguridad	23

1 Estructura

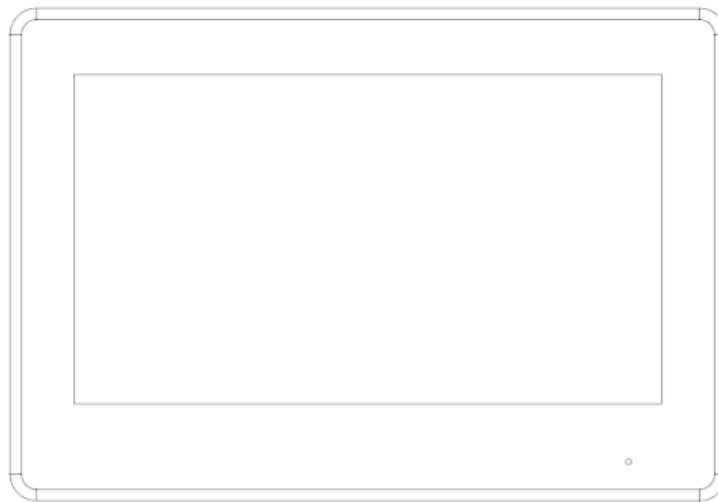
Los VTH tienen el mismo panel frontal pero difieren en los puertos del panel posterior. Algunos admiten 2 hilos y otros no.



Se pueden encontrar ligeras diferencias en los puertos del producto real.

1.1 Panel frontal

Figura 1-1 Panel frontal



1.2 Panel trasero (2 hilos)

Figura 1-2 Panel trasero para modelo de 2 hilos

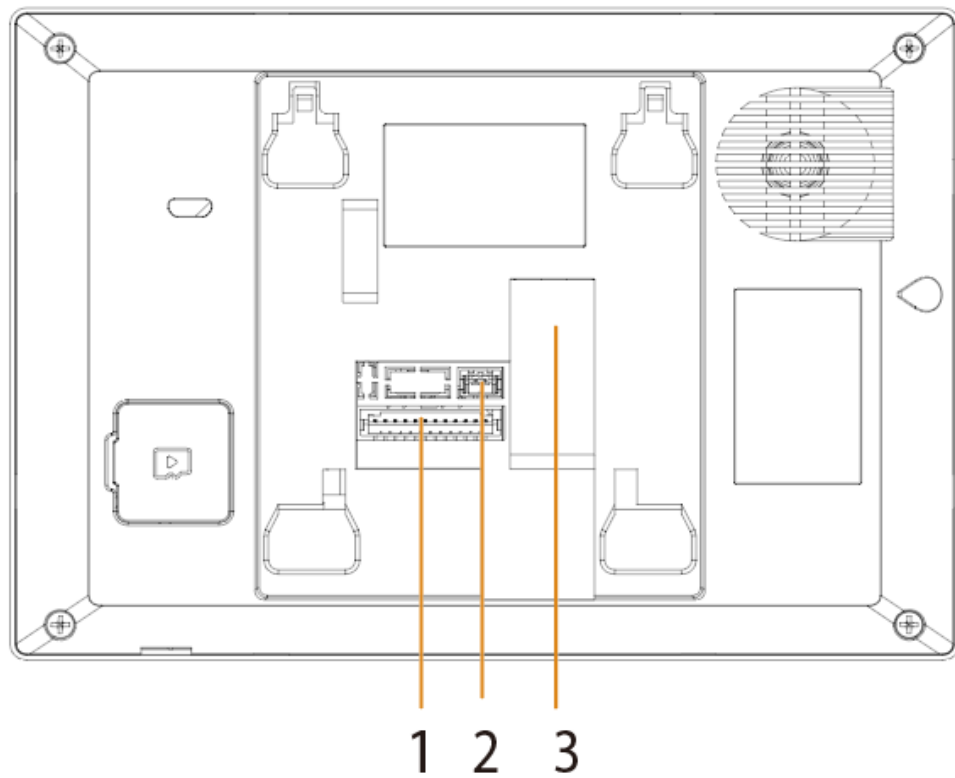


Tabla 1-1 Componentes

No.	Nombre
1	Puerto de alarma
2	puerto de 2 hilos
3	puerto de red

1.3 Panel trasero (no de 2 hilos)

Figura 1-3 Panel trasero para modelo sin 2 hilos

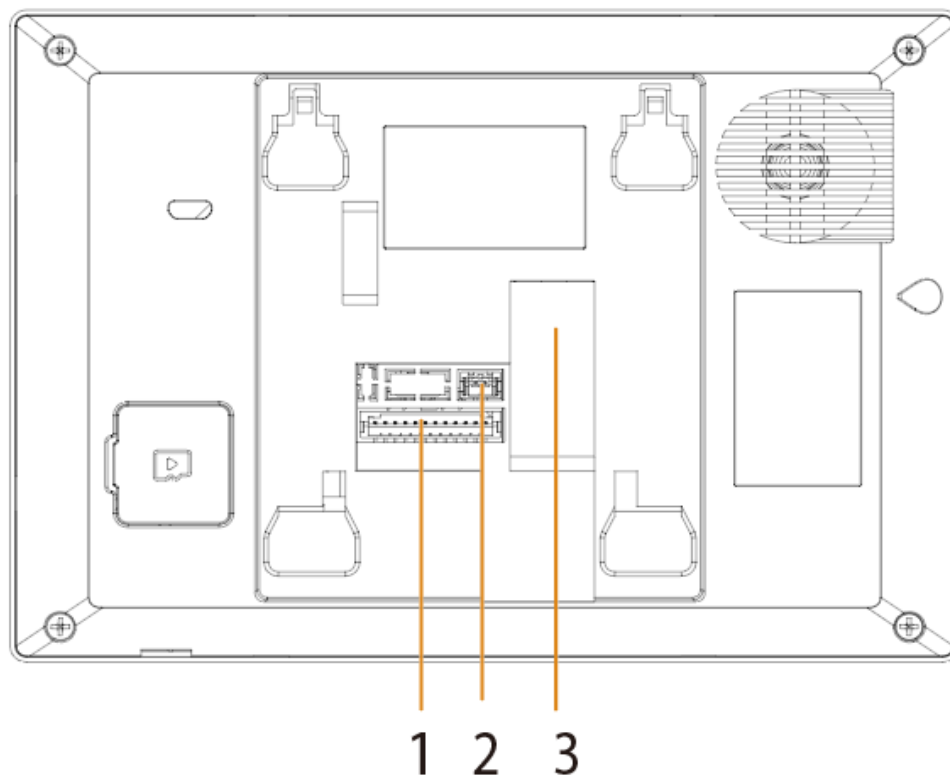


Tabla 1-2 Componentes

No.	Nombre
1	Puerto de alarma
2	Puerto de entrada de energía
3	puerto de red

2 Instalación

2.1 Preparativos



- No instale el VTH en un entorno hostil con condensación, alta temperatura, polvo, sustancia corrosiva y luz solar directa.
- En caso de anomalía después de encender el VTH, corte la fuente de alimentación de inmediato y desconecte el cable de red. Encienda después de solucionar problemas.
- La instalación debe ser realizada por equipos profesionales. No desmonte ni repare el dispositivo por usted mismo en caso de falla del dispositivo. Póngase en contacto con el servicio posventa si necesita ayuda.

2.2 Instalación en pared

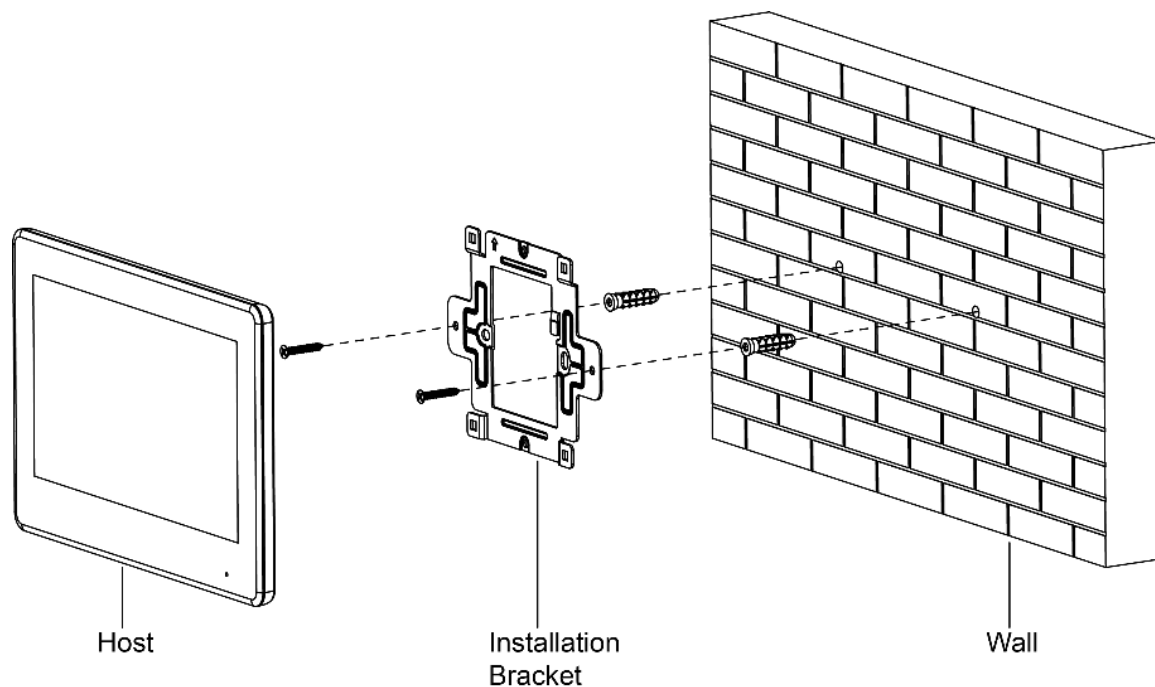
Instale directamente el VTH con un soporte en una pared, que es adecuado para todo tipo de dispositivos.

Paso 1 Taladre orificios en la pared de acuerdo con las posiciones de los orificios del soporte de instalación.

Paso 2 Fije el soporte de instalación en la pared con tornillos.

Paso 3 Coloque la parte superior del dispositivo en la parte superior del soporte de instalación y luego empuje la parte inferior del VTH.

Figura 2-1 Instalación en pared



3 Configuración de VTO

Este capítulo proporciona una configuración paso a paso del VTO. Siga las instrucciones a continuación para comenzar.



Las instantáneas son solo para referencia y se pueden encontrar ligeras diferencias en la página web real de el VTO dependiendo de su modelo.

3.1 Herramienta de configuración

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

3.2 Inicialización

Para iniciar sesión por primera vez, debe inicializar el VTO.

Paso 1 Encienda el VTO.

Paso 2 Vaya a la dirección IP predeterminada (192.168.1.108) del VTO en la barra de direcciones del navegador y luego presione la tecla Intro para ir a la página web del VTO.



● El nombre de usuario es administrador por defecto.

● Asegúrese de que la dirección IP de la PC esté en el mismo segmento de red que el VTO.

Paso 3 Sobre el **Inicialización del dispositivo** página, ingrese y confirme la contraseña, y luego haga clic en **Próximo**.



La contraseña debe constar de 8 a 32 caracteres que no estén en blanco y contener al menos dos tipos de los siguientes caracteres: mayúsculas, minúsculas, números y caracteres especiales (excepto " ; : &).

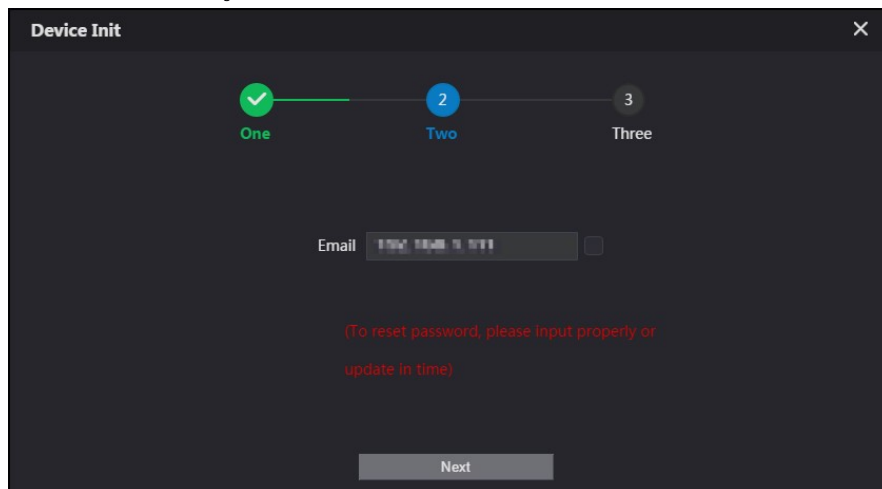
Figura 3-1 Inicialización del dispositivo

The screenshot shows a dark-themed 'Device Init' window. At the top, there's a progress indicator with three steps: '1 One', '2 Two', and '3 Three'. Step 1 is highlighted with a blue circle. Below the progress indicator, the 'Username' is set to 'admin'. There is a 'Password' field with a strength indicator showing 'Low', 'Middle', and 'High' options. Below the password field is a 'Confirm Password' field. At the bottom, there is a 'Next' button.

Etapas Etapa 4 Selecciona el **Correo electrónico** e ingrese la dirección de correo electrónico.

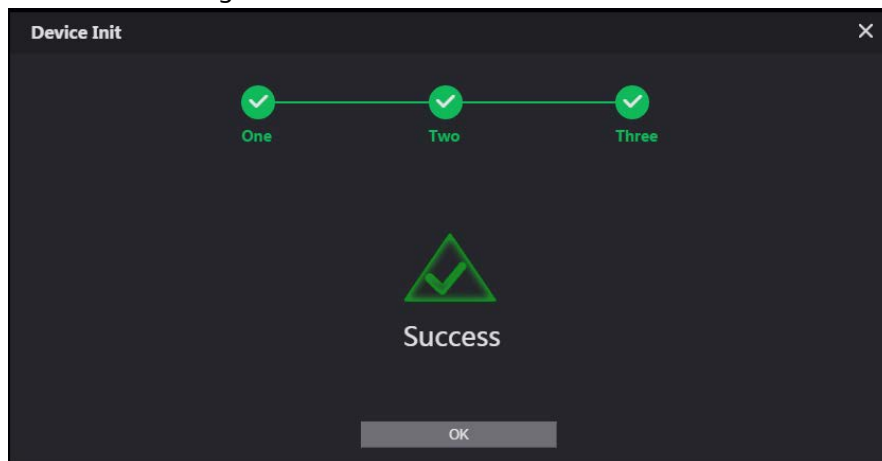
Esto le ayuda a restablecer su contraseña cuando la pierde o la olvida.

Figura 3-2 Establecer una dirección de correo electrónico



Paso 5 Hacer clic **Próximo**.

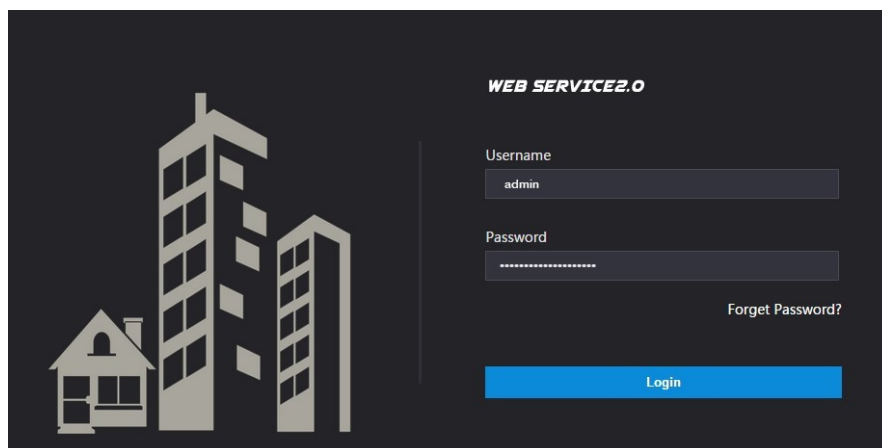
Figura 3-3 Inicialización exitosa



Paso 6 Hacer clic **OK**.

Ingrese el nombre de usuario (admin por defecto) y la nueva contraseña para iniciar sesión en la página web.

Figura 3-4 Página de inicio de sesión



3.3 Configuración del número VTO

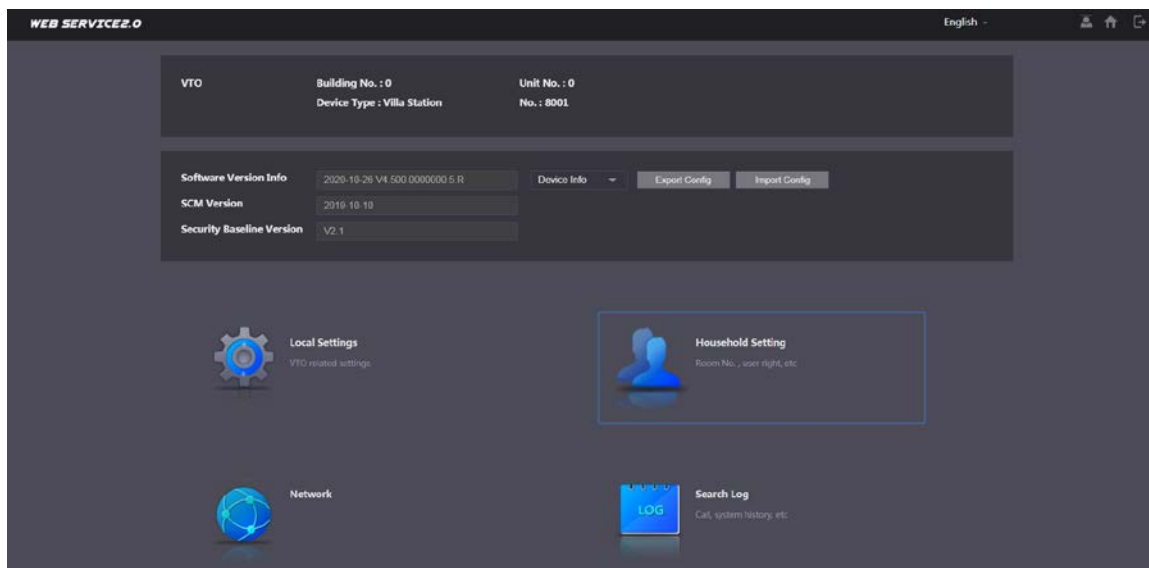
Se pueden usar números para distinguir cada VTO, y le recomendamos que lo configure de acuerdo con la unidad o el número de edificio.



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

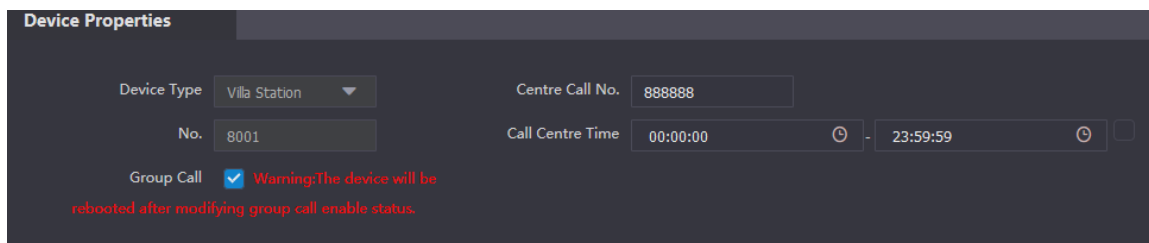
Paso 1 Inicie sesión en la página web de VTO.

Figura 3-5 Página de inicio



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

Figura 3-6 Propiedades del dispositivo

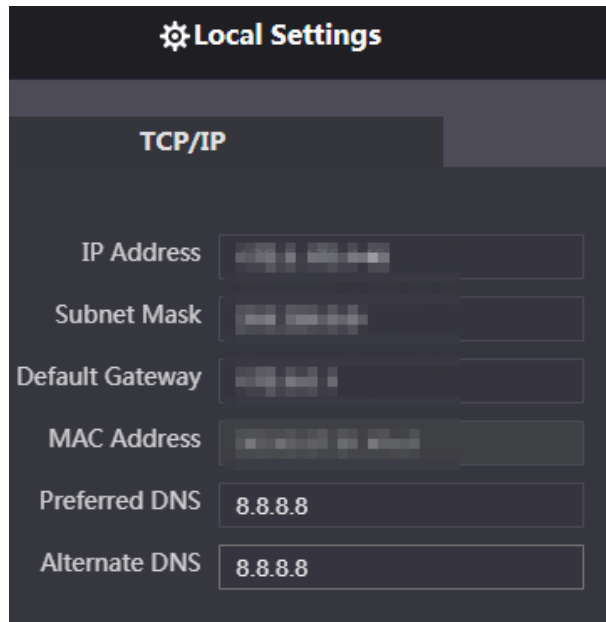


Paso 3 Introduzca el número en **No.** y luego haga clic en **Confirmar**.

3.4 Configuración de parámetros de red

Paso 1 Seleccione **Red > Básico**.

Figura 3-7 Información de TCP/IP



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

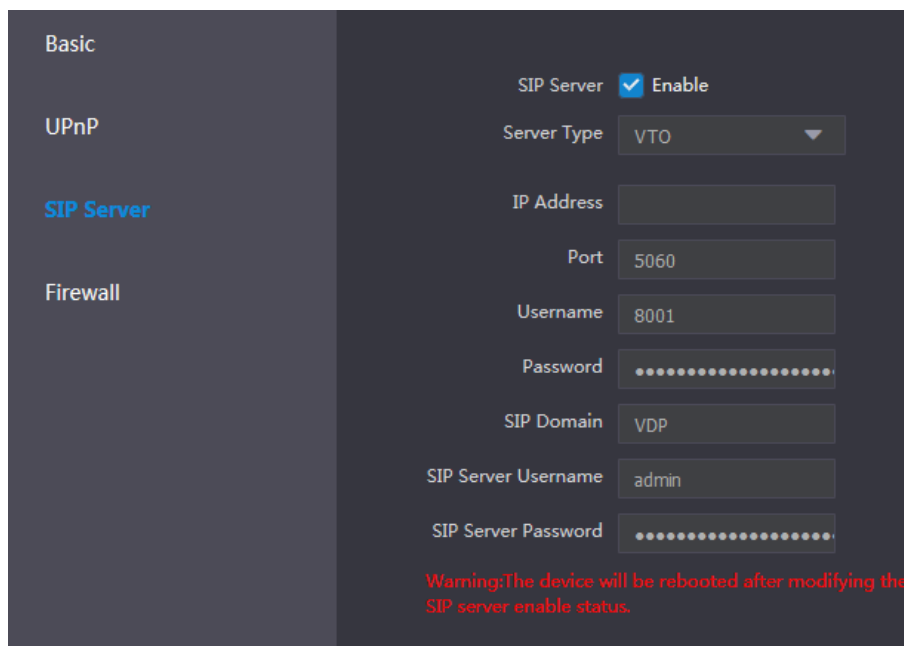
El VTO se reiniciará automáticamente. Debe agregar la dirección IP de su PC al mismo segmento de red que el VTO para iniciar sesión nuevamente.

3.5 Configuración del servidor SIP

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

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

Figura 3-8 Servidor SIP



Paso 2 Seleccione el tipo de servidor según sea necesario.

- Si el VTO actual funciona como servidor SIP, habilite **Servidor SIP** y luego haga clic en **Salvar**.

El VTO se reiniciará automáticamente y luego podrá agregar otros VTO y VTH a este VTO.



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

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

Tabla 3-1 Configuración del servidor SIP

Parámetro	Descripción
Dirección IP	La dirección IP del VTO que funciona como servidor SIP.
Puerto	- 5060 por defecto cuando VTO funciona como servidor SIP. 5080 por defecto cuando la plataforma funciona como servidor SIP.
Nombre de usuario	Déjalo como predeterminado.
Clave	
Dominio SIP	Déjalo como predeterminado.
Nombre de usuario del servidor SIP	Nombre de usuario y contraseña de inicio de sesión de la página web del servidor SIP.
Contraseña del servidor SIP	

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

3.6 Configuración de número de llamada y llamada de grupo

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

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

Figura 3-9 Propiedades del dispositivo

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

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



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

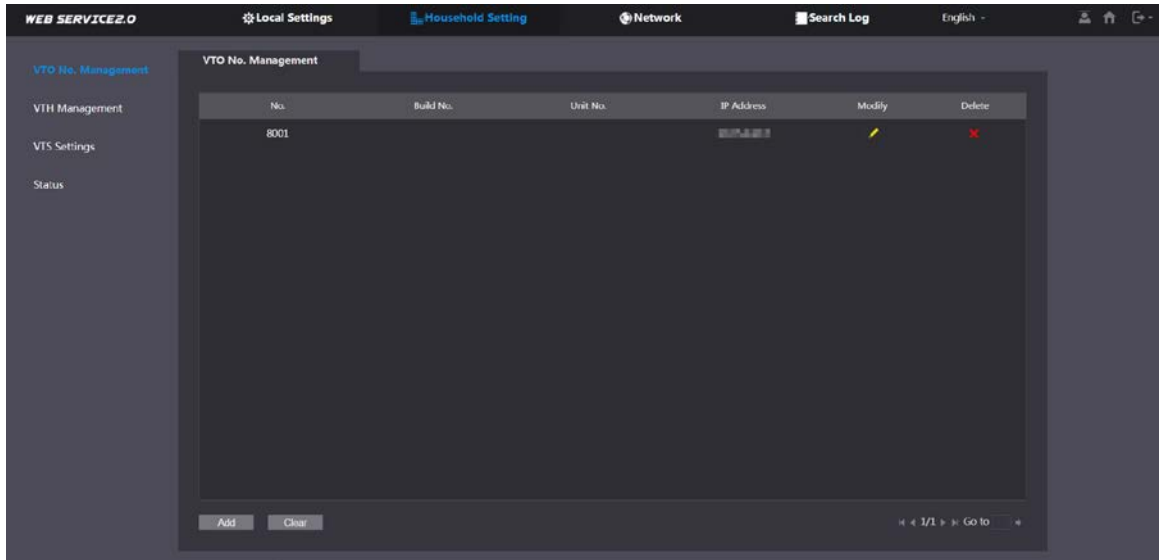
Paso 3 Inicie sesión en la página web del servidor SIP y luego seleccione **Configuración local > Básico**.

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

3.7 Adición de VTO

Puede agregar VTO al servidor SIP, y todos los VTO conectados al mismo servidor SIP pueden hacer videollamadas entre sí. Esta sección es aplicable cuando un VTO funciona como servidor SIP, y si está utilizando otros servidores como servidor SIP, consulte el manual correspondiente para la configuración detallada. **Paso 1** Inicie sesión en la página web del servidor SIP y luego seleccione **Configuración del hogar > Gestión del número de VTO**.

Figura 3-10 Gestión del número de VTO



Paso 2 Hacer clic **Agregar**.

Figura 3-11 Agregar VTO

Paso 3 Configure los parámetros.



Se debe agregar el servidor SIP.

Tabla 3-2 Agregar estaciones de puerta (VTO)

Parámetro	Descripción
No. de registro	número VTO.

Contraseña de registro	Mantenga el valor predeterminado.
construir no.	Disponible solo cuando otros servidores funcionan como servidor SIP.
Numero de unidad.	
Dirección IP	Dirección IP de VTO.
Nombre de usuario	Nombre de usuario y contraseña de inicio de sesión de la página web de VTO.
Clave	

Etapa 4 Hacer clic **Salvar**.

3.8 Agregar número de habitación

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



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

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

Figura 3-12 Gestión del número de habitación


Room No.	First Name	Last Name	Nick Name	Registration Mode	Modify
9901#0				public	
9901#1				public	
9901#2				public	
9901#3				public	
9901#4				public	
9901#5				public	
9901#6				public	
9901#7				public	
9901#8				public	
9901#9				public	

Paso 2 Hacer clic **Agregar**.

Figura 3-13 Agregar un número de habitación individual

Paso 3 Configurar la información de la habitación.

Tabla 3-3 Información de la habitación

Parámetro	Descripción
Primer nombre	Información utilizada para diferenciar cada habitación.
Apellido	
Apodo	
Habitación no.	<p>Número de habitación.</p>  <ul style="list-style-type: none"> - Cuando hay múltiples VTH, el número de habitación para el VTH principal debe terminar con #0, y los números de habitación para VTH de extensión con #1, #2... - Puede configurar hasta 9 VTH de extensión para un VTH principal.
Modo de registro	Seleccione público .
Contraseña registrada	Mantenga el valor predeterminado.

Etapa 4 Hacer clic **Salvar**.

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

4 Configuración VTH

Este capítulo presenta la configuración del VTH y cómo lograr la función de intercomunicador. Siga las instrucciones a continuación para comenzar.

4.1 Antes de comenzar

- Asegúrese de que no haya un circuito corto o abierto en el VTO y el VTH.
- Plan de IP y número (que funciona como un número de teléfono) para cada VTO y VTH. Asegúrese de que VTH y VTO estén en el segmento de red.

4.2 Configuración rápida

Para el inicio de sesión por primera vez, puede inicializar y configurar el VTH a través de la configuración rápida.



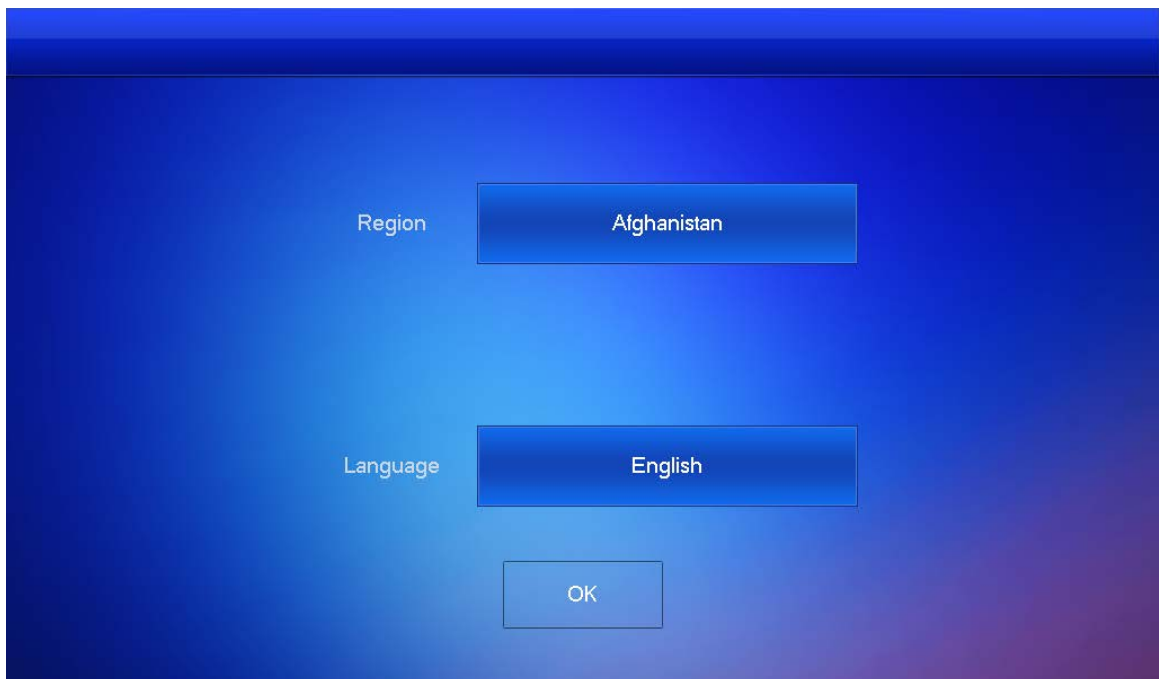
La configuración rápida le permite configurar los parámetros del VTO, VTH y el servidor SIP

En seguida. Si desea modificar los parámetros, consulte "4.3 Configuración manual".

Paso 1 Encienda el VTH.

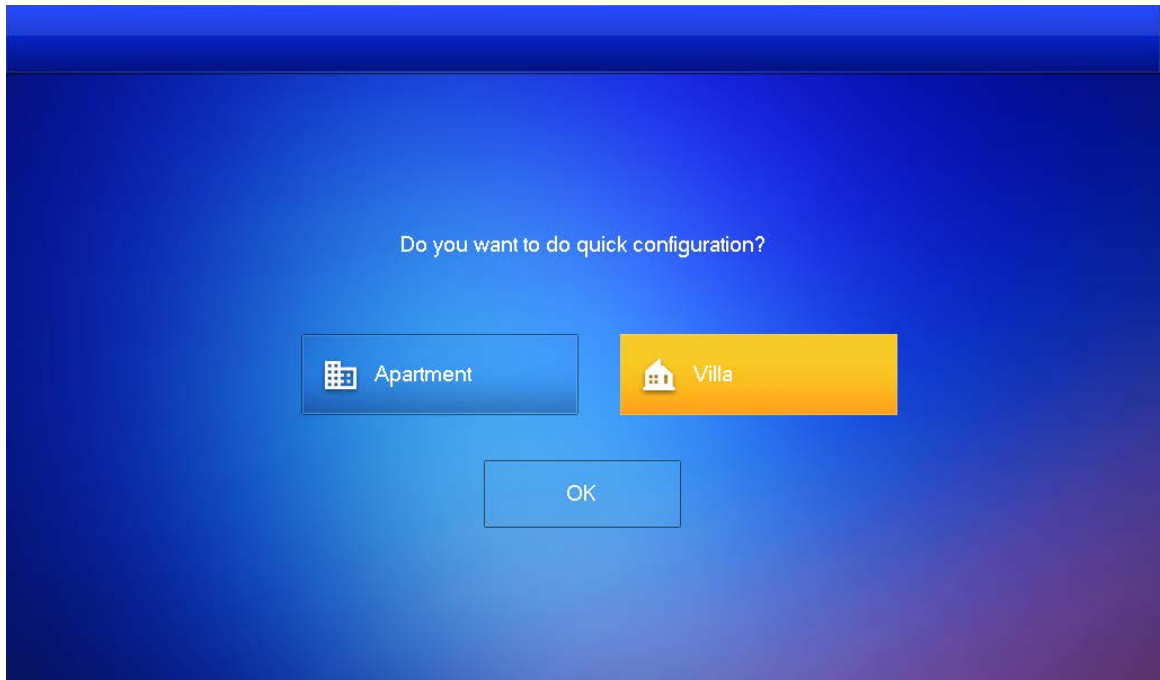
Paso 2 Seleccione una región y un idioma, y luego toque **OK**.

Figura 4-1 Región e idioma



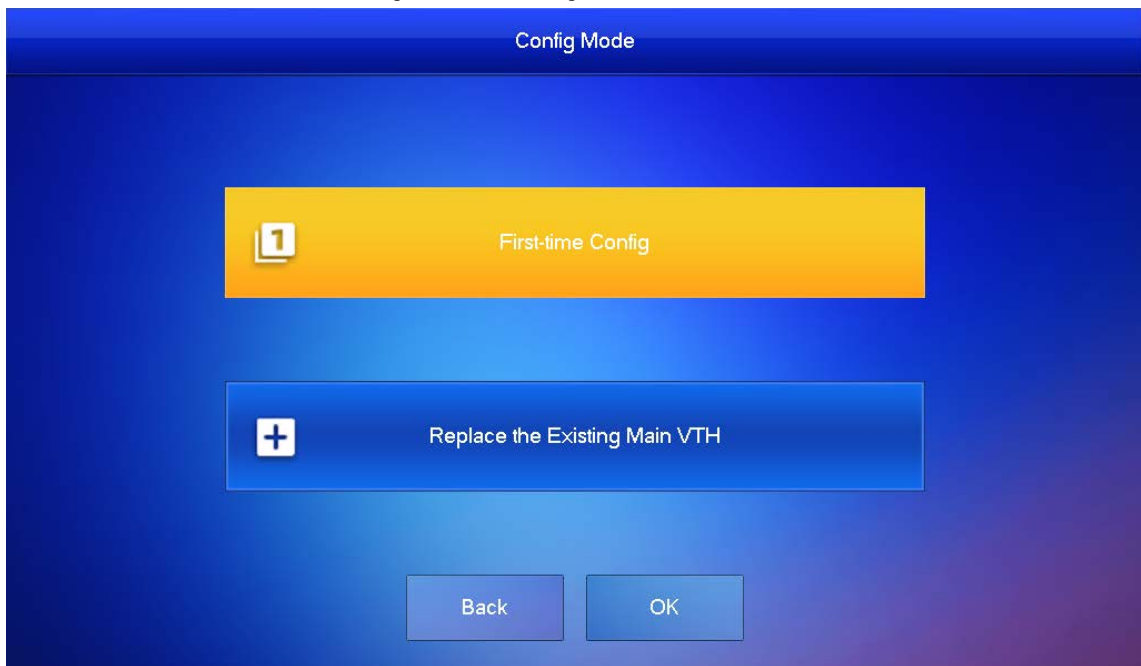
Paso 3 Establezca el tipo de configuración rápida como **Villay** luego toque **OK**.

Figura 4-2 Configuración rápida



Etapa 4 Seleccione **Configuración por primera vez** luego toque **OK**.

Figura 4-3 Modo de configuración



Paso 5 Seleccione **IP estática**, ingrese su IP de VTH planificada, máscara de red y puerta de enlace, y luego toque **Próximo**. Sobre el **Establecer contraseña VTH** pantalla, ingrese y confirme la contraseña, ingrese la dirección de correo electrónico y luego toque **Próximo**.

Figura 4-4 Establecer contraseña para VTH

STEP 2/5 Set VTH Password

Password 6 digits password

Confirm Pwd 6 digits password

Email This email is used to reset the password

Back Next

Paso 7 Sobre el **Establecer contraseña VTO** pantalla, ingrese la contraseña de VTO y confírmela, y luego toque **Próximo**.

Figura 4-5 Establecer contraseña para VTO

STEP 3/5 Set VTO Password

Password 8-32 characters password

Confirm PWD 8-32 characters password

Email This email is used to reset the password.

Back Next

Paso 8 Grifo **Inicializar** para completar la inicialización del VTO y el VTH principal, y luego toque **Próximo**. Debe asegurarse de que las direcciones IP de VTH y VTO estén en el mismo segmento de red. De lo contrario, VTH no puede obtener la información de VTO después de la configuración.

Figura 4-6 Inicializar los dispositivos

Device Type	SN	MAC	IP	Status	Operation
Local	000000000000000000			Uninitialized	Initialize
VTH	JLMB9AN0YT			Initialized	Initialize
VTH	0JAQKP6IIO			Initialized	Initialize
VTH	08:ed:ed:00:e6:89			Initialized	Initialize
VTO	20:19:10:10:17:35			Initialized	Initialize

1 2 3 4 5 6 >

Back Refresh Batch Initialization Next

Paso 9 Grifo **Configuración de una teclapa** para finalizar la configuración del VTO y VTH, así como del servidor SIP. La barra de estado le sugerirá si su configuración es exitosa.

4.3 Configuración manual

Puede configurar manualmente los parámetros que desea modificar.

4.3.1 Configuración de parámetros de red

Puede optar por conectar el VTH a la red a través de WLAN o LAN.

4.3.1.1 WLAN

Paso 1 Toque y mantenga **Ajuste** durante aproximadamente 3 segundos e ingrese la contraseña que configuró para el

Paso 2 VTH. Grifo **Red > WLAN**. Habilitar

Paso 3 OFF para ver todas las redes utilizables.

Etapas 4 Antes de conectarse a una red Wi-Fi, primero realice una de las siguientes acciones.

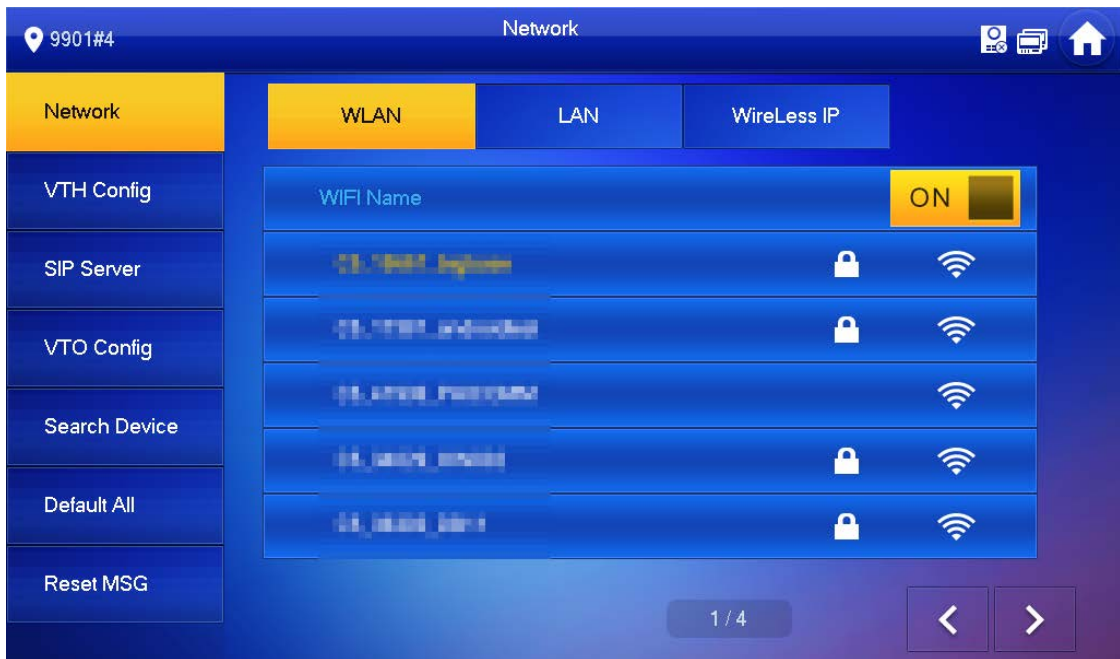
- Grifo **IP inalámbrica**, ingrese la IP local, la máscara de subred y la puerta de enlace que planea para el VTH, y luego toque **OK**. Grifo **IP inalámbrica**, toca automáticamente.
- OFF para habilitar la función DHCP para obtener información de IP



Para habilitar la función DHCP, utilice un enrutador con función DHCP.

Paso 5 Sobre el **WiFi** pantalla, toque el nombre de Wi-Fi y luego ingrese la contraseña para conectarse a la red.

Figura 4-7 WLAN



4.3.1.2 LAN

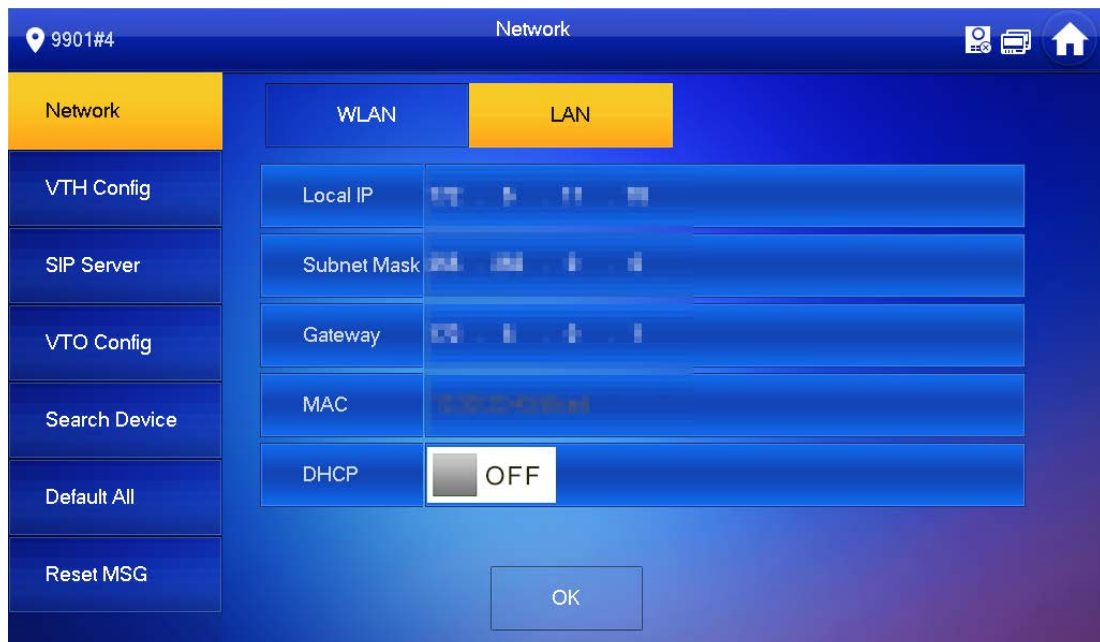
Paso 1 Toque y mantenga **Ajuste** durante aproximadamente 3 segundos e ingrese la contraseña que configuró para el

Paso 2 VTH. Grifo **Red** > **LAN**.

Paso 3 Ingrese la máscara de subred IP local y la puerta de enlace que planea para el VTH.

También puedes tocar OFF para habilitar la función DHCP para obtener información de IP automáticamente.

Figura 4-8 LAN



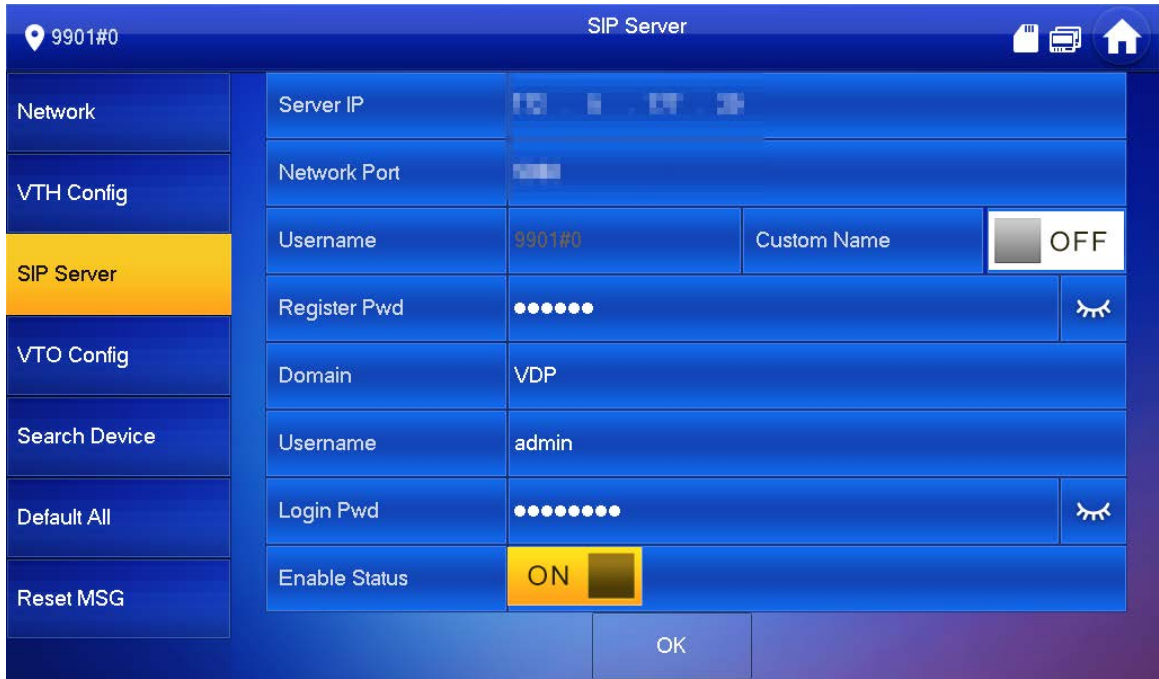
Etapa 4 Grifo **OK**.

4.3.2 Configuración del servidor SIP

Paso 1 Toque y mantenga **Ajuste** durante aproximadamente 3 segundos e ingrese la contraseña que configuró para el VTH.

Paso 2 Grifo **Servidor SIP**.

Figura 4-9 Servidor SIP



Paso 3 Configure los parámetros del servidor SIP.

Etapa 4 Colocar **Habilitar estado** para **ON**.

Paso 5 Grifo **OK**.

Tabla 4-1 Servidor SIP

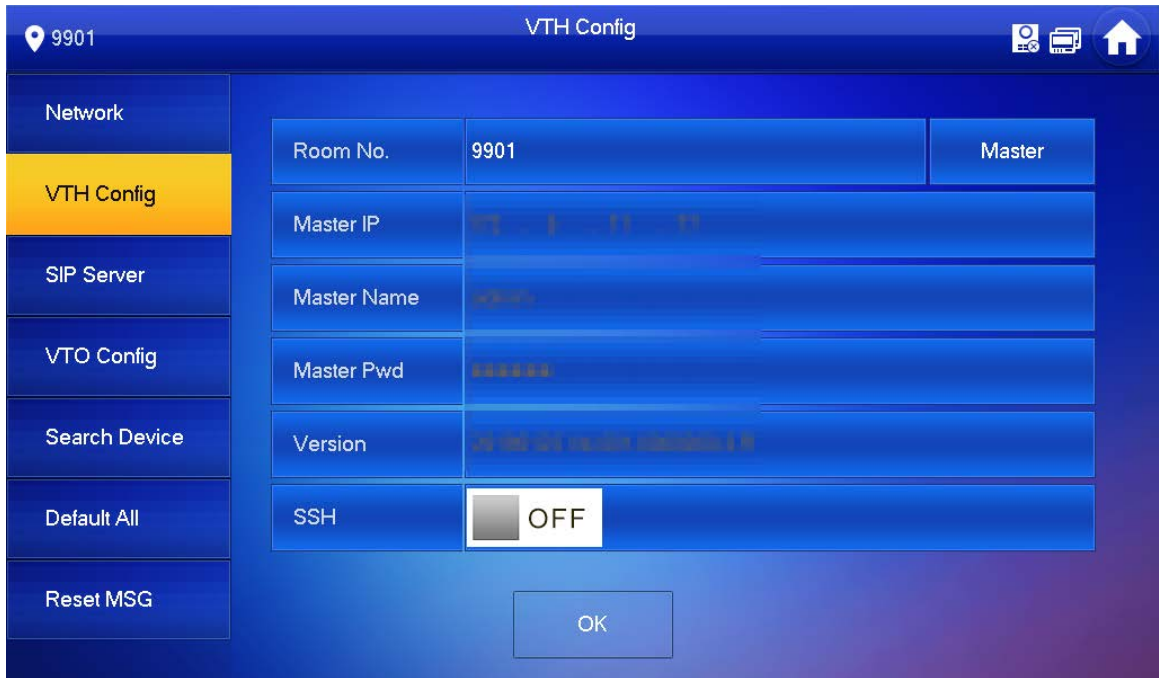
Parámetro	Descripción
Servidor IP	<ul style="list-style-type: none"> - Cuando la plataforma funciona como servidor SIP, la IP del servidor es la dirección IP de la plataforma. - Cuando VTO funciona como servidor SIP, la IP del servidor es la dirección IP de VTO.
Puerto de red	<ul style="list-style-type: none"> - Cuando la plataforma funciona como servidor SIP, el puerto de red es 5080. - Cuando VTO funciona como servidor SIP, el puerto de red es 5060.
Nombre de usuario	Déjalo como predeterminado.
Registrar Contraseña	
Dominio	Dominio de registro del servidor SIP, que puede ser nulo. Cuando VTO funciona como servidor SIP, el dominio de registro del servidor SIP es VDP.
Nombre de usuario	Nombre de usuario y contraseña para iniciar sesión en el servidor SIP.
Contraseña de inicio de sesión	

4.3.3 Configuración de VTH

Paso 1 Toque y mantenga **Ajuste** durante aproximadamente 3 segundos e ingrese la contraseña que configuró para el VTH. Grifo

Paso 2 **Configuración VTH**.

Figura 4-10 Configuración de VTH



Paso 3 Ingrese el número de habitación (como 9901 o 101#0).

Si hay una extensión VTH, el número de habitación debe terminar en #0. De lo contrario, no podrá conectarse a VTO.

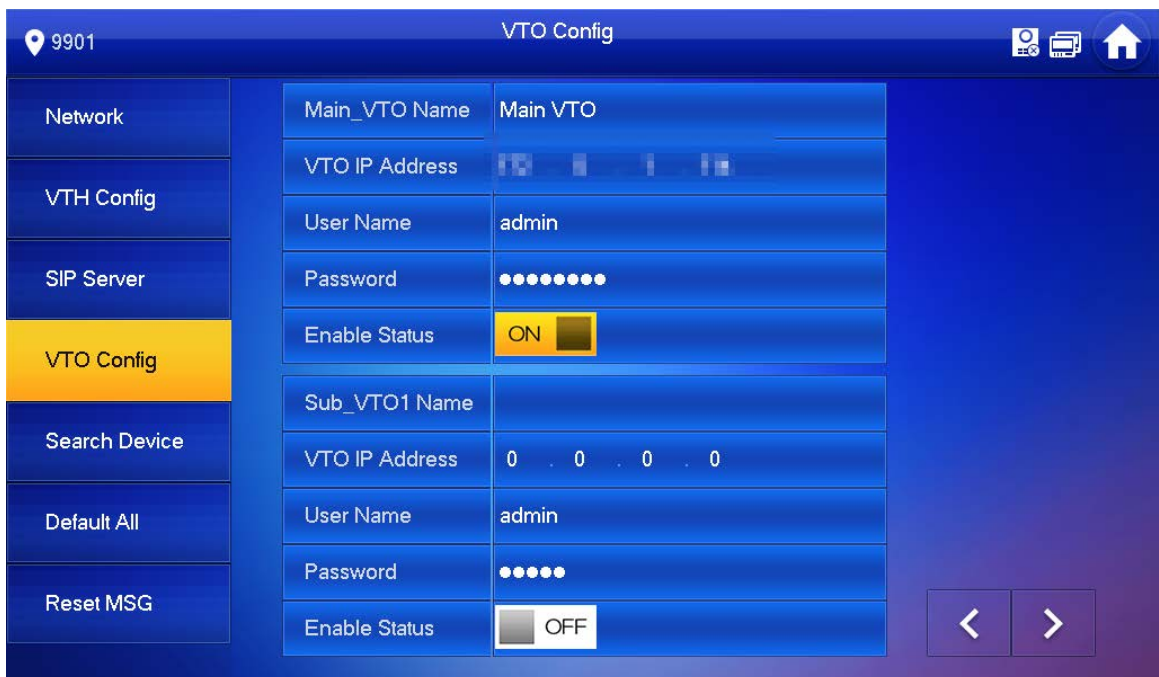
Etapa 4 Grifo **OK**.

4.3.4 Configuración de VTO

Paso 1 Toque y mantenga **Ajuste** durante aproximadamente 3 segundos e ingrese la contraseña que configuró para el VTH. Grifo

Paso 2 Configuración VTO.

Figura 4-11 Configuración de VTO



Paso 3 Añadir VTO.

4.3.4.2 Agregar VTO principal


Paso 1 Ingrese el nombre principal de VTO, la dirección IP de VTO, el nombre de usuario y la contraseña.

Paso 2 Colocar **Habilitar estado** para .

Paso 3 Compruebe si la configuración se ha realizado correctamente comprobando la barra de estado en la esquina superior derecha.

4.3.4.3 Adición de VTO secundario

Paso 1 Ingrese el nombre de VTO secundario, la dirección IP de VTO secundario, el nombre de usuario y la contraseña.

Paso 2 Colocar **Habilitar estado** para .

Paso 3 Compruebe si la configuración se ha realizado correctamente comprobando la barra de estado en la esquina superior derecha.

5 Puesta en marcha

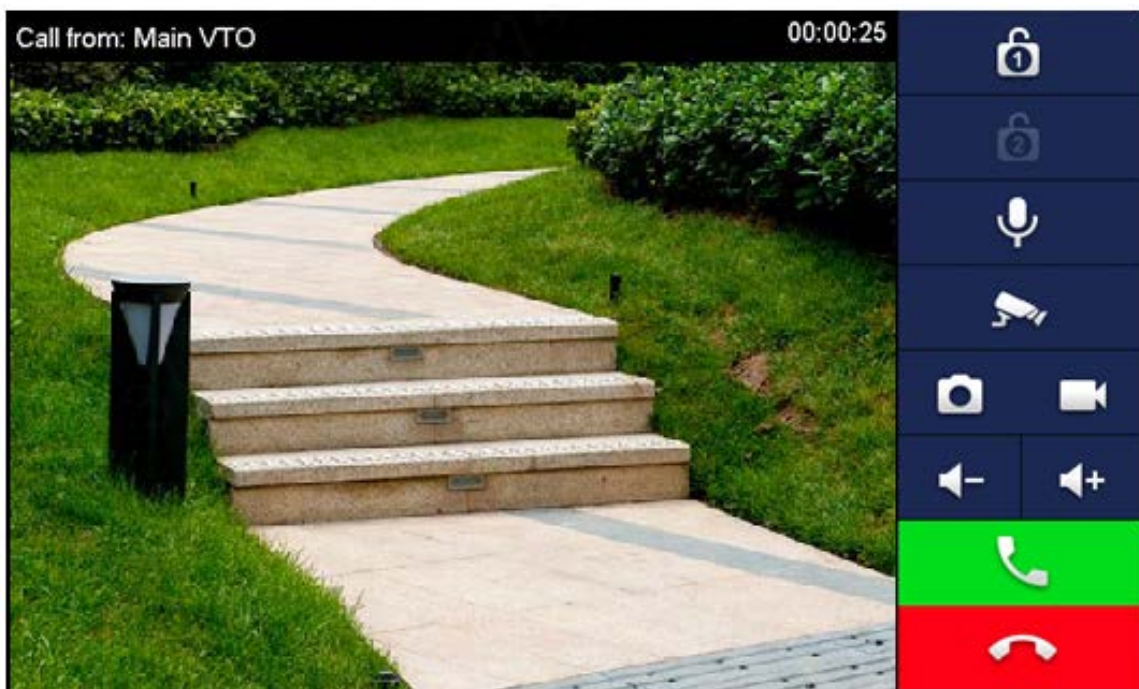
Después de completar la configuración básica, verifique si la función de intercomunicador puede funcionar.

5.1 VTO llamando a VTH

Paso 1 Marque un número de habitación en el VTO (por ejemplo, 9901).

Paso 2 Grifo  en el VTH para contestar la llamada.

Figura 5-1 Llamada VTH desde VTO



5.2 Monitoreo de VTH VTO

Un VTH puede monitorear VTO.

Paso 1 En la pantalla de inicio, seleccione **Supervisor > Puerta**.

Paso 2 Configure el VTO para ir a la página de monitoreo.

Paso 3 Toque el icono para ver el video VTO.



La siguiente figura significa que la tarjeta SD se ha insertado en VTH. Si la tarjeta SD no está insertado, los iconos de grabación e instantánea son grises.

Figura 5-2 Puerta

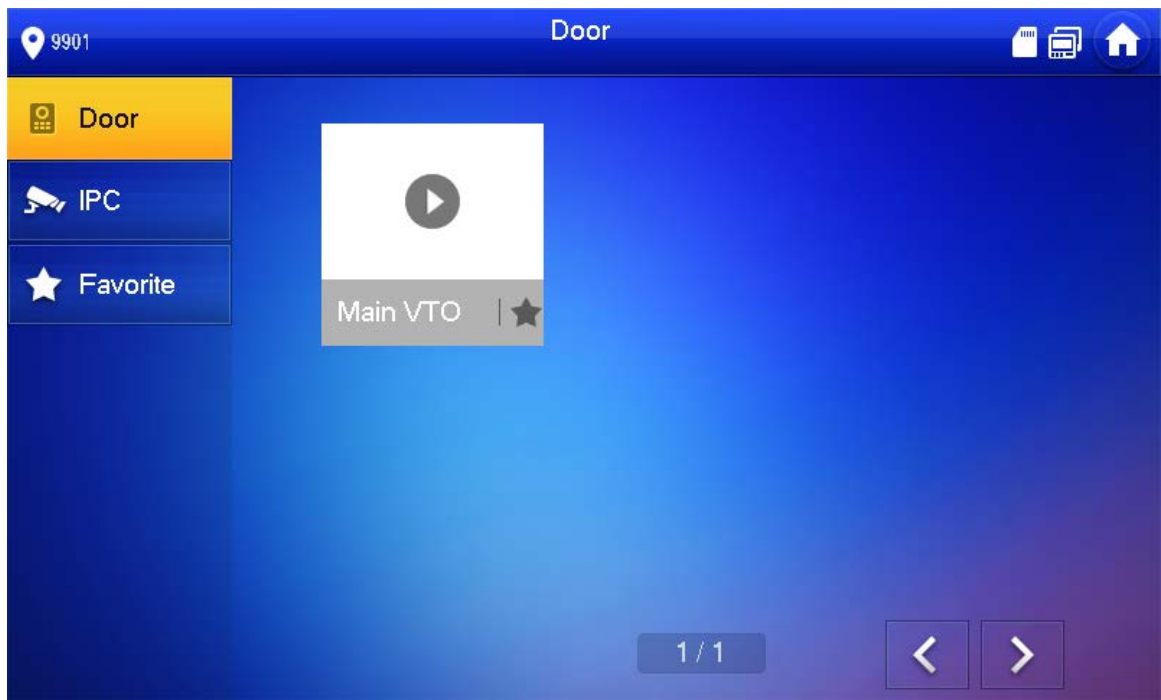
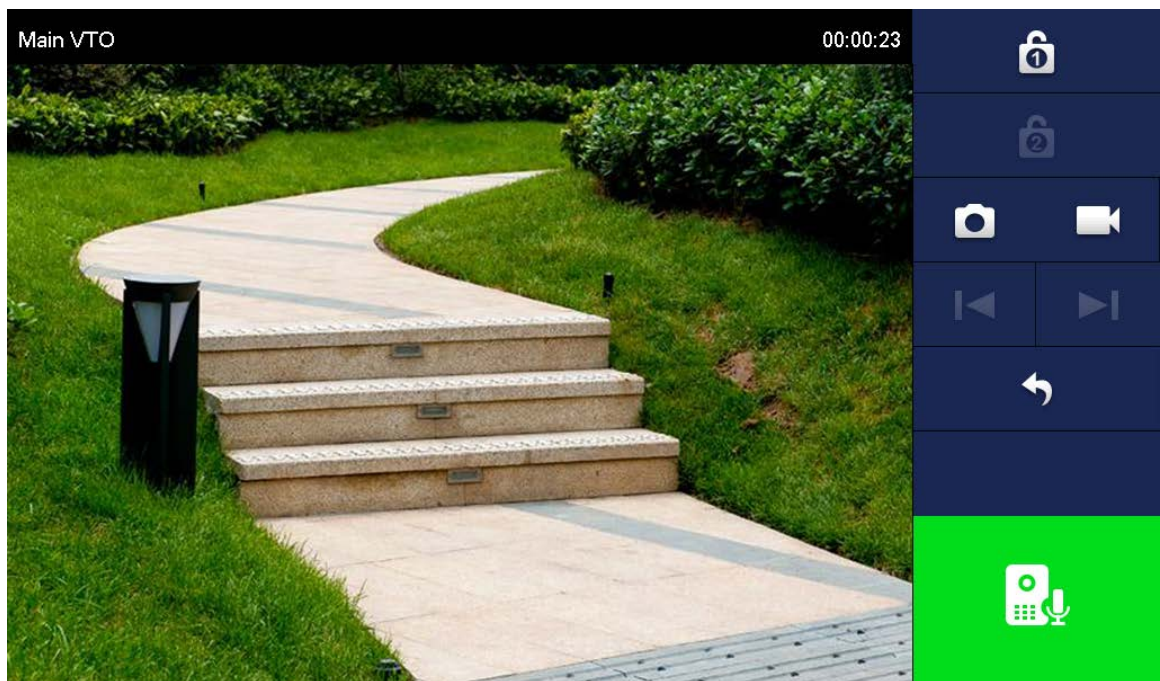


Figura 5-3 Dispositivo de monitoreo



Apéndice 1 Recomendaciones sobre ciberseguridad

Acciones obligatorias que se deben tomar para la seguridad básica de la red del

dispositivo: 1. Use contraseñas seguras

Consulte las siguientes sugerencias para establecer contraseñas:

- La longitud no debe ser inferior a 8 caracteres;
- Incluya al menos dos tipos de caracteres; los tipos de caracteres incluyen letras mayúsculas y minúsculas, números y símbolos;
- No contenga el nombre de la cuenta o el nombre de la cuenta en orden inverso; No utilice caracteres continuos, como 123, abc, etc.;
- No utilice caracteres superpuestos, como 111, aaa, etc.;

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

- De acuerdo con el procedimiento estándar en la industria tecnológica, recomendamos mantener actualizado el firmware de su dispositivo (como NVR, DVR, cámara IP, etc.) para garantizar que el sistema esté equipado con los últimos parches y correcciones de seguridad. Cuando el dispositivo está conectado a la red pública, se recomienda habilitar la función de "comprobación automática de actualizaciones" para obtener información oportuna de las actualizaciones de firmware lanzadas por el fabricante.
- Le sugerimos que descargue y utilice la última versión del software del cliente.

Recomendaciones "agradables de tener" para mejorar la seguridad de la red de su

dispositivo: 1. Protección física

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

2. Cambie las contraseñas regularmente

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

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

El dispositivo admite la función de restablecimiento de contraseña. Configure la información relacionada para restablecer la contraseña a tiempo, incluido el buzón del usuario final y las preguntas de protección de contraseña. Si la información cambia, modifíquela a tiempo. Al establecer preguntas de protección de contraseña, se sugiere no utilizar aquellas que se pueden adivinar fácilmente.

4. Habilitar bloqueo de cuenta

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

5. Cambiar HTTP predeterminado y otros puertos de servicio

Le sugerimos que cambie el HTTP predeterminado y otros puertos de servicio a cualquier conjunto de números entre 1024 y 65535, lo que reduce el riesgo de que personas ajenas puedan adivinar qué puertos está utilizando.

6. Habilitar HTTPS

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

7. Enlace de dirección MAC

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

8. Asigne cuentas y privilegios de manera razonable

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

9. Deshabilite los servicios innecesarios y elija modos seguros

Si no es necesario, se recomienda desactivar algunos servicios como SNMP, SMTP, UPnP, etc., para reducir los riesgos.

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

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

10. Transmisión encriptada de audio y video

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

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

11. Auditoría segura

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

12. Registro de red

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

13. Construya un entorno de red seguro

Para garantizar mejor la seguridad del dispositivo y reducir los posibles riesgos cibernéticos, recomendamos:

- Deshabilite la función de mapeo de puertos del enrutador para evitar el acceso directo a los dispositivos de intranet desde una red externa.
- La red debe dividirse y aislarse de acuerdo con las necesidades reales de la red. Si no hay requisitos de comunicación entre dos subredes, se sugiere usar VLAN, GAP de red y otras tecnologías para dividir la red, a fin de lograr el efecto de aislamiento de la red.
- Establezca el sistema de autenticación de acceso 802.1x para reducir el riesgo de acceso no autorizado a redes privadas.
- Habilite la función de filtrado de direcciones IP/MAC para limitar el rango de hosts que pueden acceder al dispositivo.