Estación de puerta de villa

Manual de usuario

V1.0.1

Prefacio

General

Este manual presenta la instalación, funciones y operaciones del dispositivo de estación de puerta de villa (en adelante, "el VTO"). Lea atentamente antes de usar el dispositivo y guarde el manual en un lugar seguro para consultarlo en el futuro.

Instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

Palabras de advertencia	Significado
DANGER	Indica un alto riesgo potencial que, si no se evita, provocará la muerte o lesiones graves.
WARNING	Indica un peligro potencial medio o bajo que, si no se evita, podría provocar lesiones leves o moderadas.
CAUTION	Indica un riesgo potencial que, si no se evita, podría provocar daños a la propiedad, pérdida de datos, reducciones en el rendimiento o resultados impredecibles.
TIPS	Proporciona métodos para ayudarle a resolver un problema o ahorrar tiempo.
NOTE	Proporciona información adicional como complemento al texto.

Revisión histórica

Versión	Contenido de revisión	Fecha de lanzamiento
V1.0.1	Estructura añadida.	diciembre 2023
V1.0.0	Primer lanzamiento.	agosto 2023

Aviso de protección de privacidad

Como usuario del dispositivo o controlador de datos, puede recopilar datos personales de otras personas, como su rostro, audio, 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 proporcionar la información de contacto requerida.

Acerca del Manual

- El manual es sólo para referencia. Pueden encontrarse ligeras diferencias entre el manual y el producto.

- No somos responsables de las pérdidas incurridas 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 regulaciones de las jurisdicciones relacionadas. Para obtener información detallada, consulte el manual del usuario en papel, utilice nuestro CD-ROM, escanee el código QR o visite nuestro sitio web oficial. El manual es sólo para referencia. Es posible que se encuentren ligeras diferencias entre la versión electrónica y la versión en papel.
- Todos los diseños y software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones de productos pueden provocar que aparezcan algunas diferencias entre el producto real y el manual. Comuníquese con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria.
- Pueden existir 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 otro software de lectura convencional si no se puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas comerciales registradas y nombres de empresas que aparecen en este manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, comuníquese con el proveedor o con el servicio de atención al cliente si ocurre algún problema durante el uso del dispositivo.
- Si existe alguna incertidumbre o controversia, nos reservamos el derecho de dar una explicación final.

Salvaguardias 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 y cumpla con las pautas al usarlo.

Requisitos de operación

- Compruebe si la fuente de alimentación es correcta antes de su uso.
- No desenchufe el cable de alimentación en el costado del dispositivo mientras el adaptador esté encendido.
- Opere el dispositivo dentro del rango nominal de entrada y salida de energía.
- Transporte, utilice y almacene el dispositivo en las condiciones permitidas de humedad y temperatura.
- Si el dispositivo permanece apagado durante más de un mes, debe colocarse en su paquete original y sellarse. Asegúrese de mantenerlo alejado de la humedad y guárdelo en las condiciones permitidas de humedad y temperatura.
- 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

- 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 podría provocar un incendio o una explosión.

- El personal que trabaja en alturas debe tomar todas las medidas necesarias para garantizar la 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 sobre 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 fuente de alimentación de gabinete proporcionado por el fabricante.
- Utilice los cables de alimentación recomendados para la región y cumplan con las especificaciones de potencia nominal.
- La fuente de alimentación debe cumplir con los requisitos de ES1 en el estándar IEC 62368-1 y no ser superior a PS2. Tenga en cuenta que los requisitos de suministro de energía 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 conexión a tierra de protección.

Tabla de contenido

Prefacio..... I Medidas de seguridad y advertencias importantes..... III 1 Estructura.....1
1.1 Estación de puerta de villa (varios botones)..... 1
1.1.1 Panel frontal..... 1
1.1.2 Panel trasero..... 2
1.2 Estación de puerta de villa (botón único).....2
1.2.1 Serie R..... 2
1.2.2 Serie D.....5
1.2.3 Serie G..... 8
1.3 Modelo de botón..... 10
1.3.1 Panel frontal.....10
1.3.2 Panel trasero..... 11
2 Inicializando el VTO.....13
2.1 Internet..... 13
2.2 APLICACIÓN DMSS..... 13
3 Iniciar sesión y restablecer la contraseña..... 17
3.1 Iniciar sesión..... 17
3.2 Restablecer la contraseña..... 17
4 Página de inicio..... 18
5 Asistente de configuración..... 19
5.1 Configuración como servidor SIP..... 19
5.2 No configurar como servidor SIP.....20
6 Configuración del dispositivo local.....21
6.1 Configuraciones básicas..... 21
6.1.1 Estación de puerta de villa..... 21
6.1.2 Segunda Estación de Confirmación..... 23
6.2 Control de acceso.....25
6.2.1 Configuración..... 25
6.2.2 RS-485..... 26
6.3 Diseño..... 27
7 Sistema..... 30
7.1 Vídeo.....30
7.2 Audio.....32
7.3 Tiempo..... 33
7.4 Usuario ONVIF..... 35
7.5 Configuración..... 36

7.6 Mantenimiento.....36
7.7 Actualización.....37
7.8 Información Legal..... 37
7.9 Información del sistema..... 37
8 Configuración del dispositivo..... 39
8.1 Gestión del nº de VTO..... 39
8.2 Gestión de VTH..... 40
8.3 Gestión del VTS.....41
9 Gestión de personas..... 43
10 Configuración de red..... 46
10.1 TCP/IP.....46
10.2 Puerto..... 47
10.3 Servidor SIP..... 47
10.4 Segunda estación de confirmación en cascada..... 51
10.5 Servicio de almacenamiento en la nube..... 52
10.6 UPnP..... 52
10.6.1 Habilitación de servicios UPnP..... 53
10.6.2 Agregar servicios UPnP.....53
10.7 Wifi..... 55
10.8 Servicios basicos..... 55
11 Gestión de registros.....58
11.1 Historial de llamadas..... 58
11.2 Registros de alarmas..... 58
11.3 Desbloquear registros..... 59
11.4 Registro..... 59
12 Gestión de seguridad..... 61
12.1 Estado de seguridad..... 61
12.2 Servicio del sistema..... 61
12.3 Defensa de ataque.....62
12.3.1 Cortafuegos.....62
12.3.2 Bloqueo de cuenta.....63
12.3.3 Ataque Anti-DoS..... 64
12.4 Certificado CA..... 64
12.5 Cifrado de vídeo..... sesenta y cinco
12.6 Advertencia de seguridad..... sesenta y cinco
Configuración del modelo de 13 botones..... 67
13.1 Conexión de cables.....67
13.2 Configuración VTH.....68
Apéndice 1 Recomendaciones de ciberseguridad..... 70

1 estructura

1.1 Estación de puerta de villa (varios botones)

1.1.1 Panel frontal

Figura 1-1 Panel frontal

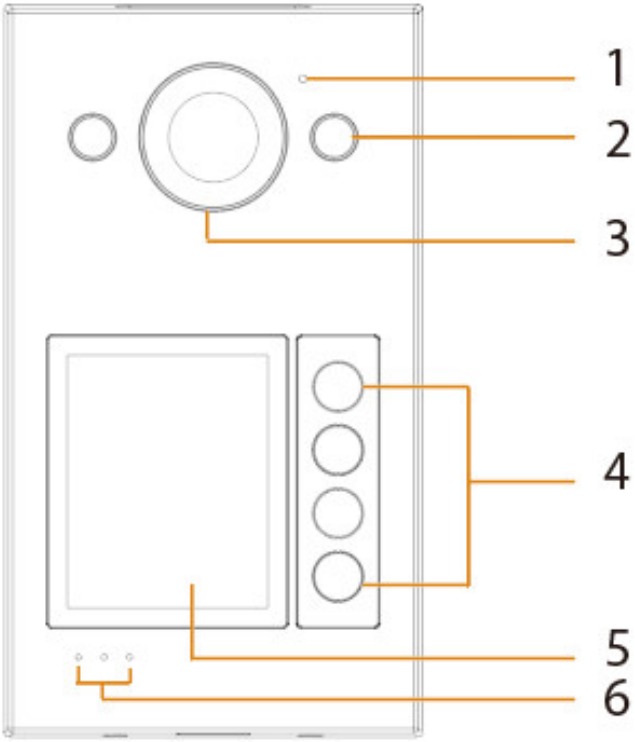


Tabla 1-1 Componentes

No.	Nombre	Función
1	micrófono	Entrada de audio.
2	Iluminador	Proporciona una luz constante para enfocar más fácilmente un sujeto en un entorno oscuro.
3	Cámara	Capture imágenes o grabe vídeos para el VTO.
4	Botones de llamada	Llame al VTH.
5	Área para pasar tarjetas	Pase las tarjetas registradas para desbloquear las puertas.
6	Indicadores	De izquierda a derecha: ● Timbre: VTO está llamando al VTH. ● Hablando: VTO está hablando con VTH. ● Desbloqueo: Desbloqueo de VTO exitoso.

1.1.2 Panel trasero

Los puertos funcionales pueden diferir según los modelos reales.

Figura 1-2 Panel trasero

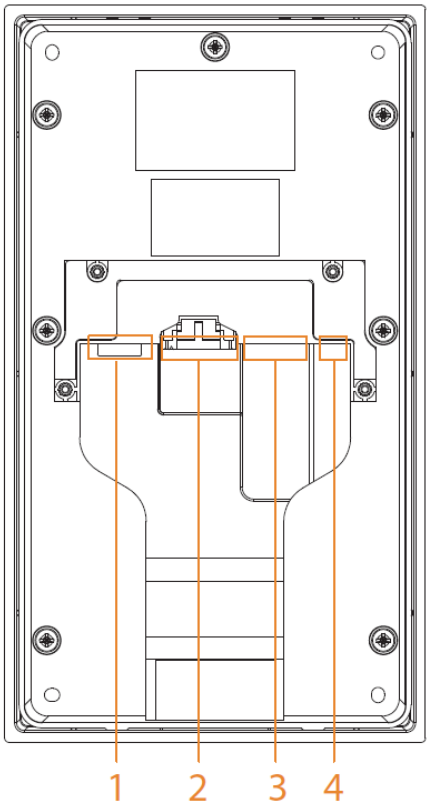


Tabla 1-2 Componentes

No.	Nombre	Función
1	ranura para tarjetas SD	Se utiliza para insertar una tarjeta SD para poder almacenar información de datos, como imágenes y vídeos.
2	Puertos funcionales	Puerto de alarma, puerto de detector de puerta, puerto 485, puerto de alimentación, etc.
3	Puerto de red	Puerto de red RJ-485 para conectarse a la red.
4	Botón de reinicio	Mantenga presionado el botón durante varios segundos para restablecer la configuración de fábrica.

1.2 Estación de puerta de villa (un solo botón)

1.2.1 Serie R

1.2.1.1 Panel frontal

El tamaño y la apariencia pueden variar según los modelos de producto.

Figura 1-3 Panel frontal

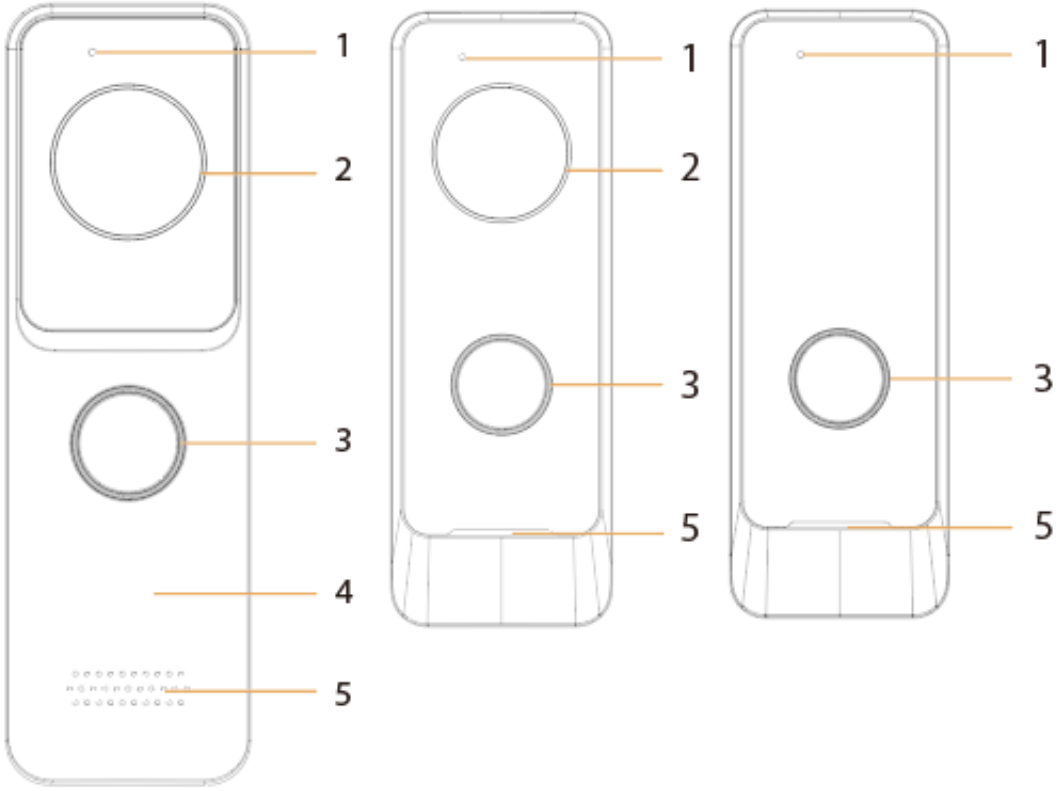


Tabla 1-3 Componentes

No.	Nombre	Función
1	micrófono	Entrada de audio.
2	Cámara	Capture imágenes o grabe vídeos para el VTO.
3	Botón de llamada	Llame al VTH.
4	Área para pasar tarjetas	Pase las tarjetas registradas para desbloquear las puertas. La función de deslizar la tarjeta solo está disponible en modelos selectos.
5	Vocero	Salida de audio.

1.2.1.2 Panel trasero

Los puertos funcionales pueden diferir según el modelo. A continuación se muestran dos modelos utilizados como ejemplos.

Figura 1-4 Panel trasero (1)

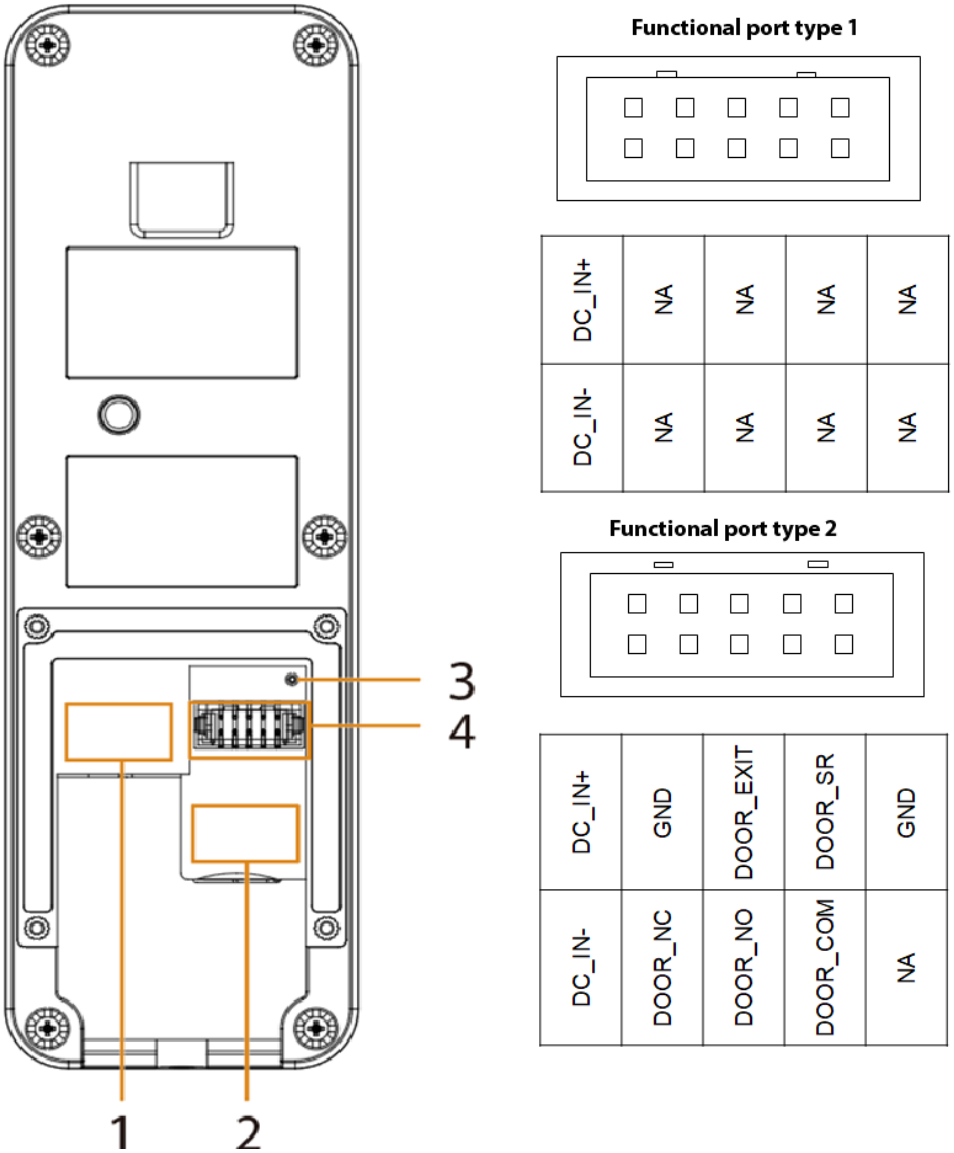


Tabla 1-4 Componentes

No.	Nombre	Función
1	Puerto de red	Se conecta a la red.
2	ranura para tarjetas SD	Inserte la tarjeta SD para poder almacenar información de datos, como imágenes y videos.
3	Botón de reinicio	Mantenga presionado el botón durante varios segundos para restablecer la configuración de fábrica.
4	Puertos funcionales	● Tipo 1: El puerto funcional solo tiene un puerto de entrada de energía para conectarse a la fuente de alimentación. ● Tipo 2: El puerto funcional incluye un puerto de entrada de energía y un puerto detector de puerta.

Figura 1-5 Panel trasero (2)

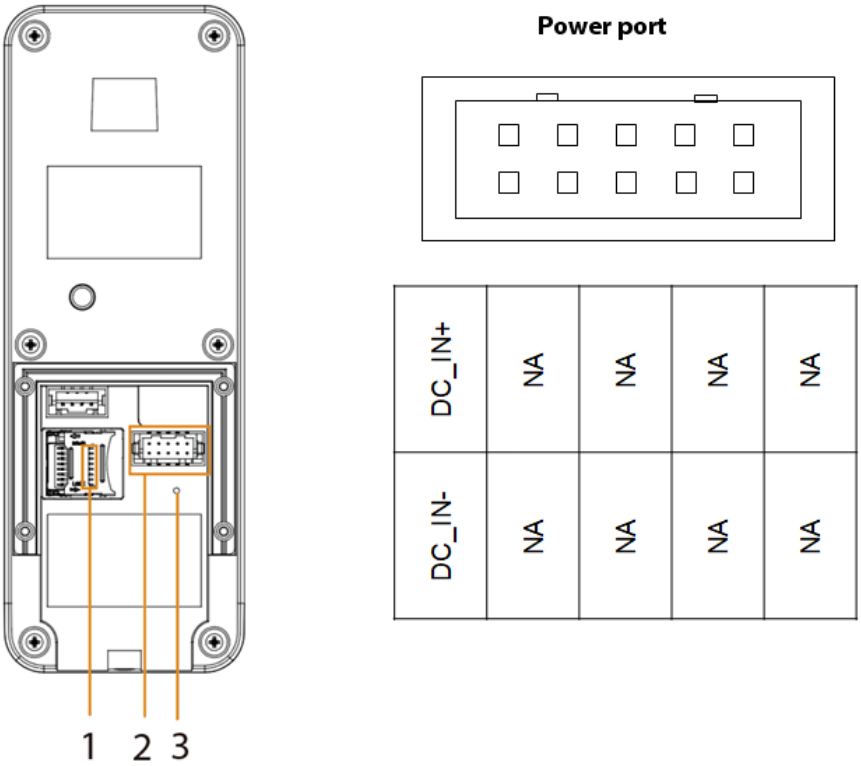


Tabla 1-5 Componentes

No.	Nombre	Función
1	ranura para tarjetas SD	Inserte la tarjeta SD para poder almacenar información de datos, como imágenes y videos.
2	Puerto de alimentación	Se conecta a la fuente de alimentación.
3	Botón de reinicio	Mantenga presionado el botón durante varios segundos para restablecer la configuración de fábrica.

1.2.2 Serie D

1.2.2.1 Panel frontal

Figura 1-6 Panel frontal

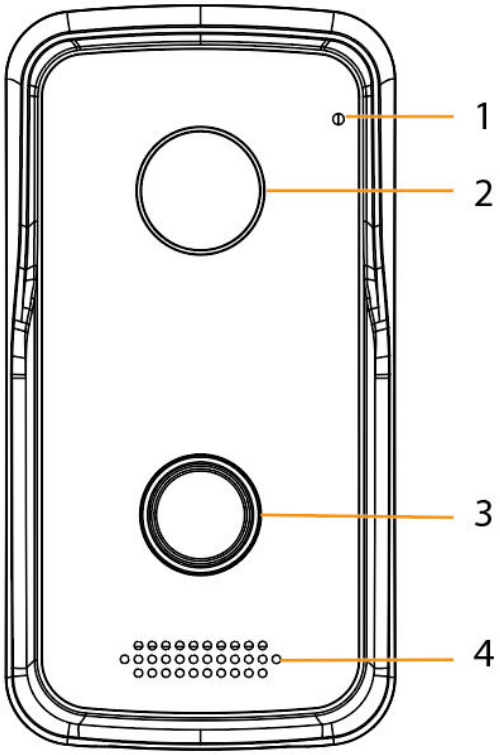


Tabla 1-6 Componentes

No.	Nombre	Función
1	micrófono	Entrada de audio.
2	Cámara	Capture imágenes o grabe vídeos para el VTO.
3	Botón de llamada	Llame al VTH.
4	Vocero	Salida de audio.

1.2.2.2 Panel trasero

Figura 1-7 Panel trasero

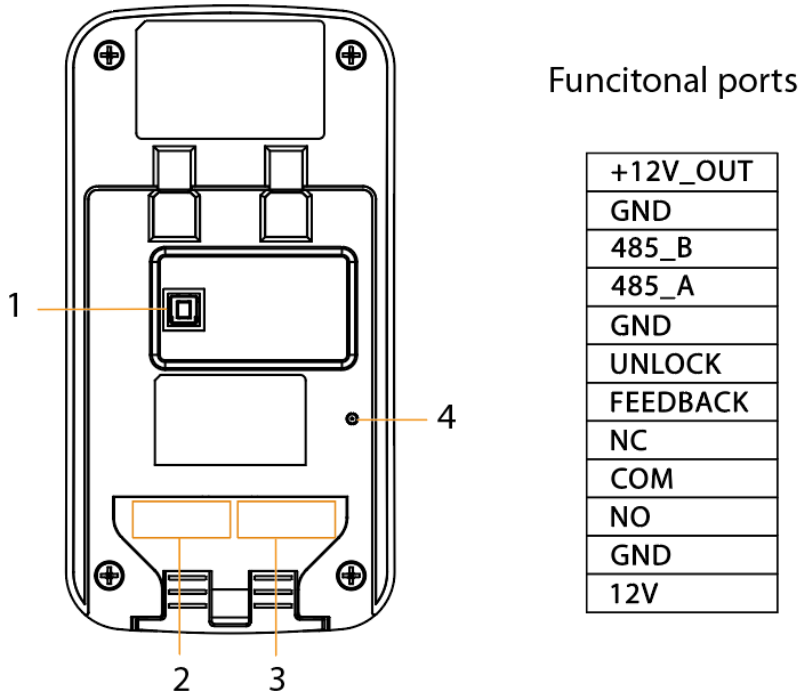


Tabla 1-7 Componentes

No.	Nombre	Función
1	Botón de manipulación	● Después de retirar el dispositivo instalado de la pared u otros lugares, el dispositivo emitirá un pitido y se generará el registro de alarma. ● Dentro de los 5 minutos posteriores a que se enciende el dispositivo, si presiona el botón de manipulación 5 veces en 8 segundos, el dispositivo emite un pitido y elimina la información de la cuenta. Se generará el registro de alarma.
2	Puertos funcionales	Puerto de alarma, puerto detector de puerta, puerto 485, puerto de alimentación y más.
3	Puerto de red	Se conecta a la red.
4	Botón de reinicio	Mantenga presionado el botón durante varios segundos para restablecer la configuración de fábrica.

1.2.3 Serie G

1.2.3.1 Panel frontal

Figura 1-8 Panel frontal

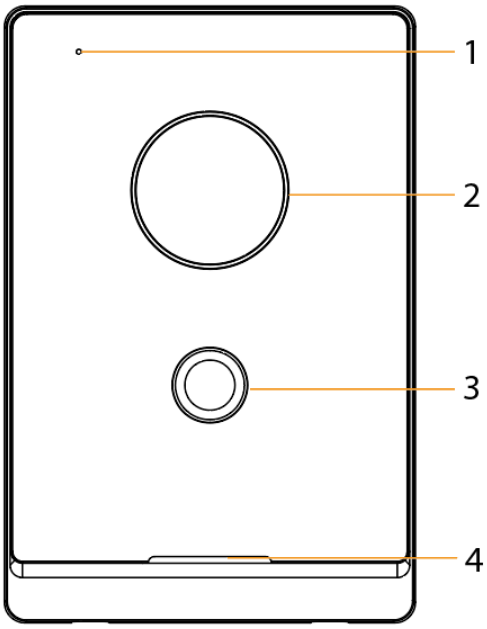


Tabla 1-8 Componentes

No.	Nombre	Función
1	micrófono	Entrada de audio.
2	Cámara	Capture imágenes o grabe vídeos para el VTO.
3	Botón de llamada	Llame al VTH. El botón muestra diferentes colores en diferentes estados. ● En espera: sin luz. ● Llamada no contestada: Verde fijo. ● Llamada respondida: Azul fijo. ● Desbloquear cuando el dispositivo está en estado de espera: Rojo. ● Desbloquear cuando no se responde la llamada: Parpadea en verde, amarillo y luego verde. ● Desbloquear después de responder la llamada: parpadea en azul, rosa y luego azul. ● Red desconectada: Luz de respiración verde.
4	Vocero	Salida de audio.

1.2.3.2 Panel trasero

Figura 1-9 Panel trasero

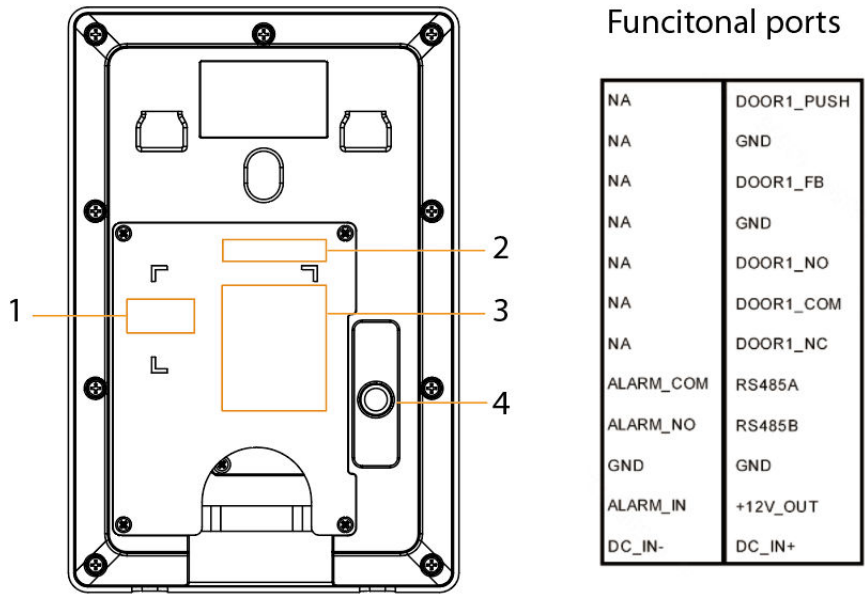


Tabla 1-9 Componentes

No.	Nombre	Función
1	Puerto de red	Se conecta a la red.
2	Puertos funcionales	Puerto de alarma, puerto de detector de puerta, puerto 485, puerto de alimentación, etc.
3	ranura para tarjetas SD	Inserte la tarjeta SD para poder almacenar información de datos, como imágenes y videos.
4	Botón de manipulación	• Después de retirar el dispositivo instalado de la pared u otros lugares, el dispositivo emitirá un pitido y se generará el registro de alarma. • Dentro de los 5 minutos posteriores a que se enciende el dispositivo, si presiona el botón de manipulación 5 veces en 8 segundos, el dispositivo emite un pitido y elimina la información de la cuenta. Se generará el registro de alarma.

1.3 Modelo de botón

1.3.1 Panel frontal

Figura 1-10 Panel frontal

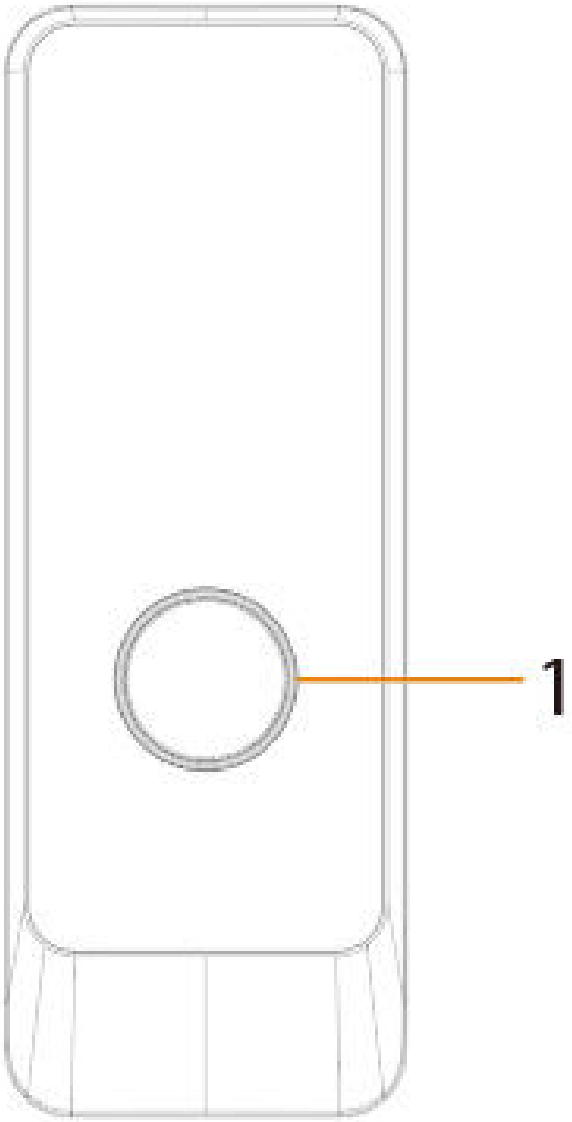


Tabla 1-10 Componentes

No.	Nombre	Función
1	presiona el botón	El modelo de botón se puede conectar al VTH. Presione el botón en el modelo y el VTH recibe una señal de alarma.

1.3.2 Panel trasero

Figura 1-11 Panel trasero

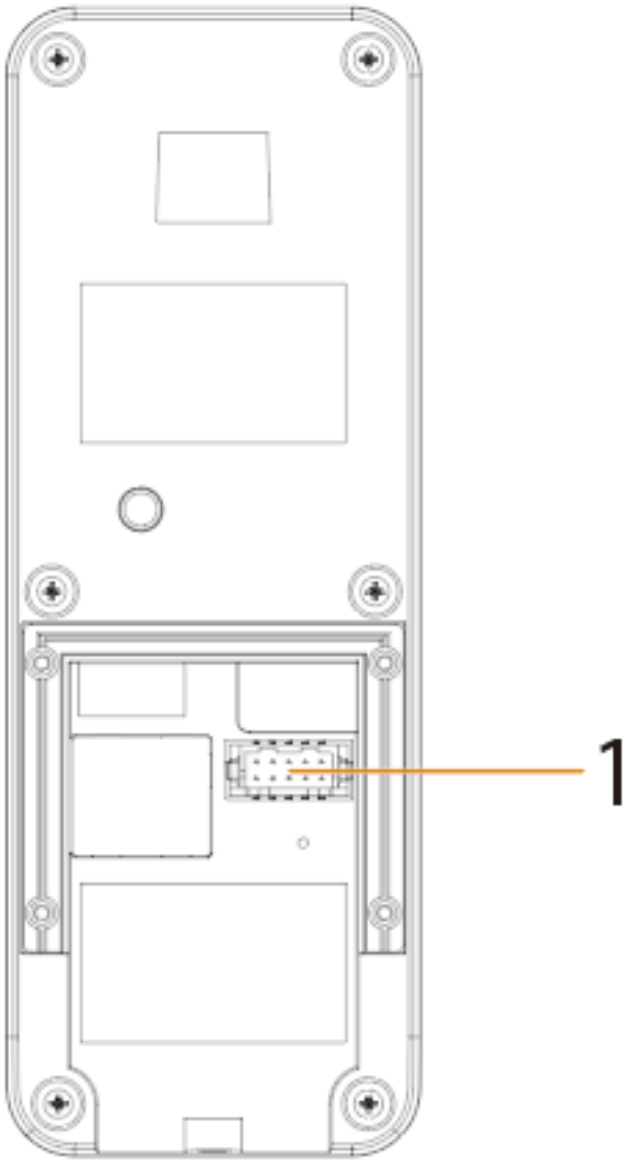
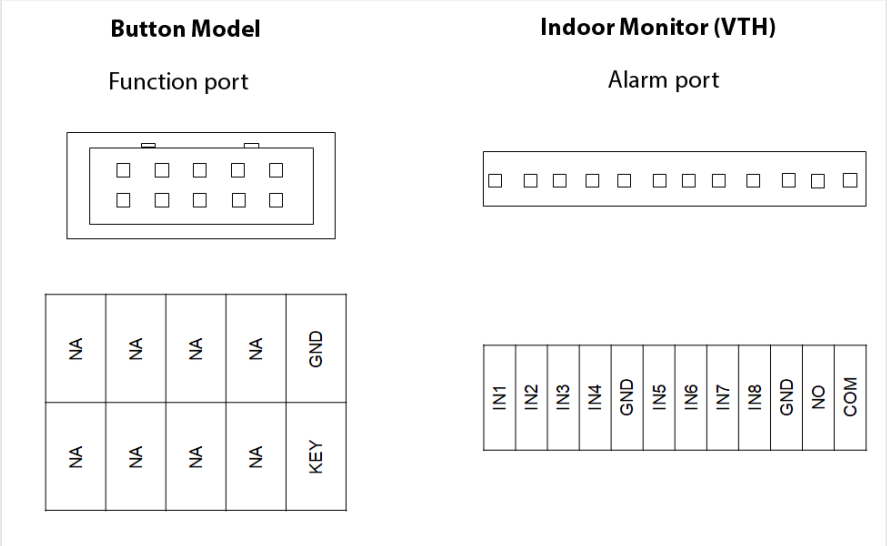


Tabla 1-11 Componentes

No.	Nombre	Función
1	Puerto funcional	Se utiliza para entrada de alarma.

Figura 1-12 Conexión de cables



Conecte el puerto KEY del modelo de botón a cualquiera de los puertos de entrada de alarma del monitor interior (VTH) con un hilo de cable. Después de eso, toque**Configuración**>**Alarma**>**Zona cableada**en el VTH y configure el**Tipo**del puerto de entrada de alarma que eligió conectar al puerto KEY como**Timbre de la puerta**.

2 Inicializando el VTO

2.1 Web

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

Procedimiento

Paso 1 Encienda el VTO.

Paso 2 Vaya a la dirección IP predeterminada (192.168.1.108) del VTO.

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

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

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

Etapa 4 Selecciona el**Correo electrónico**casilla de verificación e ingrese una dirección de correo electrónico para restablecer la contraseña. Hacer clic

Paso 5 **Próximo**.

Paso 6 Hacer clic**DE ACUERDO**para ir a la página de inicio de sesión.

Paso 7 Ingrese el nombre de usuario (admin por defecto) y la contraseña para iniciar sesión en la página web.

2.2 APLICACIÓN DMSS

Si su modelo solo admite conexión Wi-Fi a la red, solo puede inicializar el VTO en la aplicación DMSS. Para conocer el funcionamiento detallado de la aplicación, consulte su manual de usuario.

Requisitos previos

Ha descargado el DMSS en APP Store (iOS) o Google Play (Android), ha creado una cuenta e iniciado sesión en la aplicación.

Procedimiento

Paso 1 Encienda el VTO.

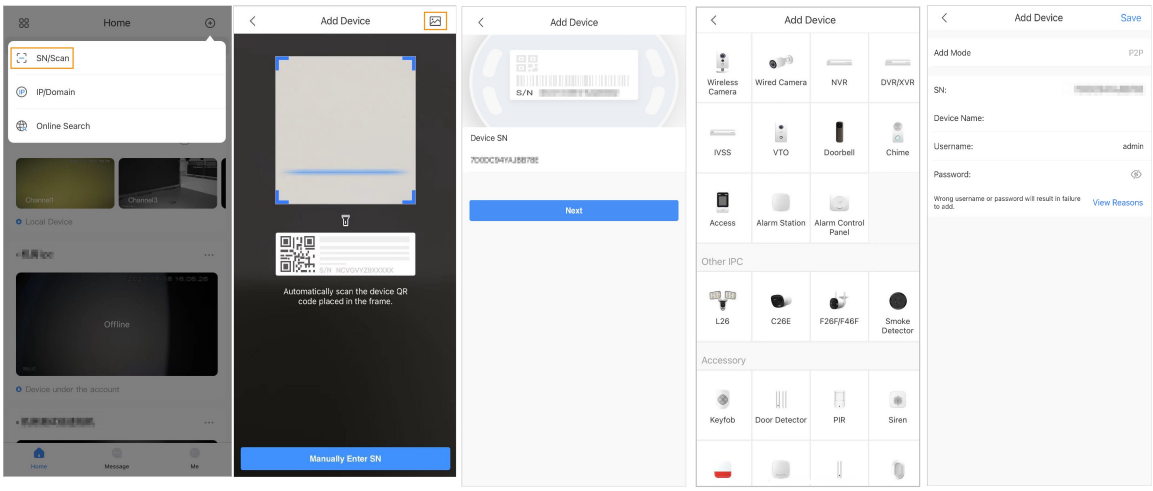
Paso 2 Habilite el punto de acceso en el VTO presionando y manteniendo presionado el botón de llamada en el VTO hasta que escuche el mensaje de voz.

La función de punto de acceso es para permitirle conectar el VTO a la red a través de**configuración de punto de acceso**en la aplicación.

Paso 3 Agregue el VTO a la aplicación DMSS.

1. Sobre el**Hogar**pantalla, toque y luego seleccione**SN/escanear**.
2. Agregue un VTO.
3. Puede agregar escaneando el código QR en el panel trasero del VTO.
4. El número SN del VTO aparece automáticamente y luego toque**Próximo**.
5. Seleccione el tipo de dispositivo como**VTO**y luego aparece la información del dispositivo.
6. Toque**Ver razones**.

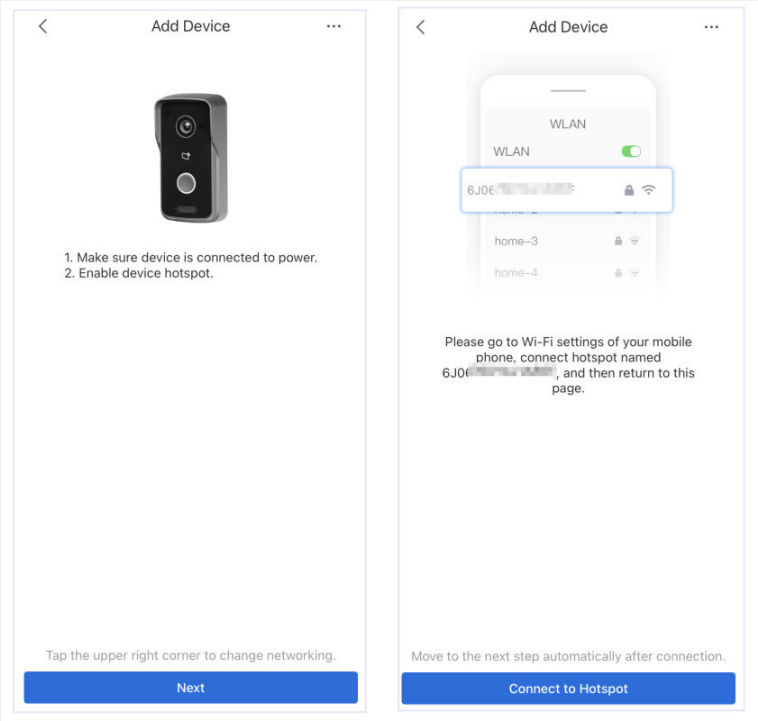
Figura 2-1 Agregar VTO a DMSS



7. Configure la red cambiando la red a**Configuración de punto de acceso**,y luego toque**Próximo**.
8. Conecte su teléfono al punto de acceso que acaba de habilitar en el VTO.

- El nombre del punto de acceso es el número SN de su VTO.
- La página actual pasará al siguiente paso automáticamente después de la conexión.

Figura 2-2 Configuración de AP

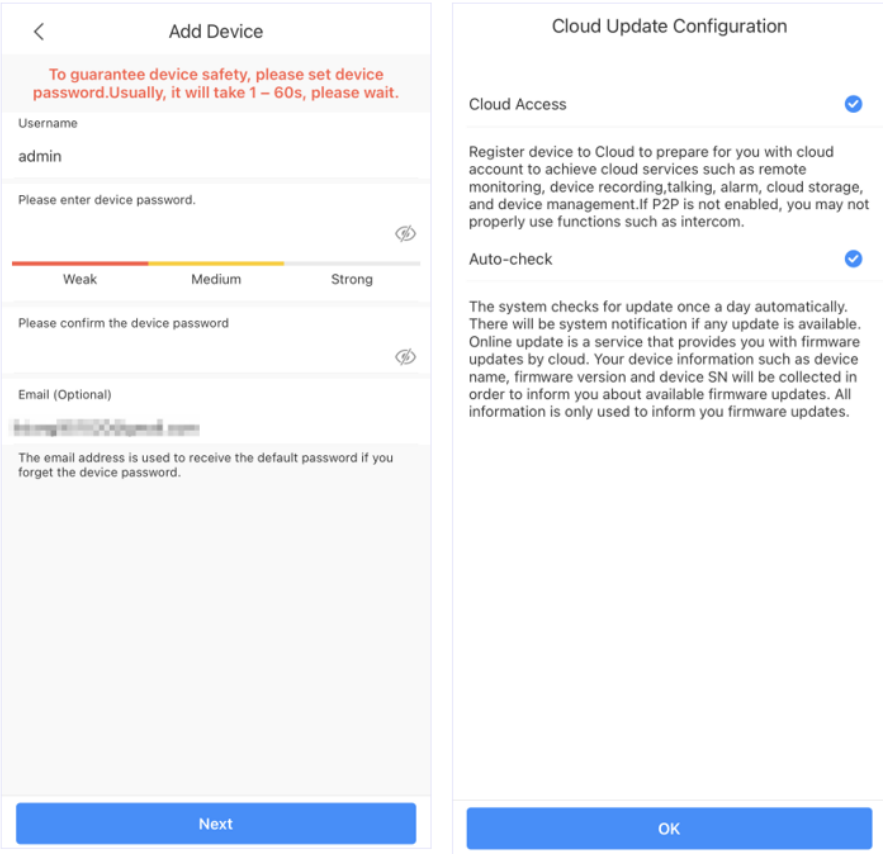


Etapa 4 Complete la inicialización según las instrucciones de la aplicación.

1. Ingrese la contraseña que planeó para el VTO, confírmela y luego toque**Próximo**.
2. Seleccione**Acceso a la nube**y**Verificación automática**y luego toque**DE ACUERDO**.

El proceso de inicialización está completo.

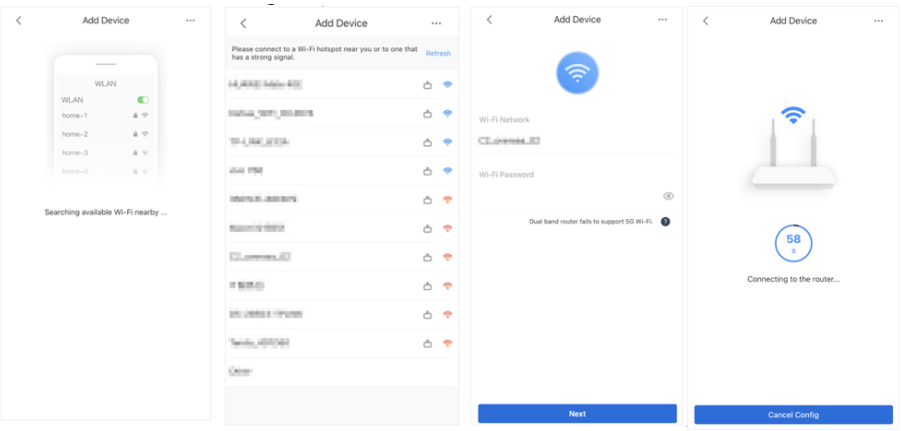
Figura 2-3 Inicialización



Paso 5 Conecte el VTO a la red a través de Wi-Fi.

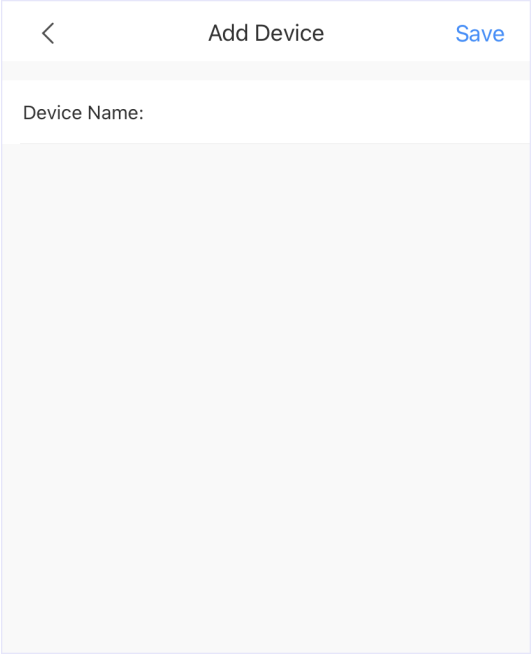
1. Seleccione una red Wi-Fi disponible.
2. Ingrese la contraseña y toque**Próximo**. Espere a que el VTO se conecte al enrutador.

Figura 2-4 Conexión Wi-Fi



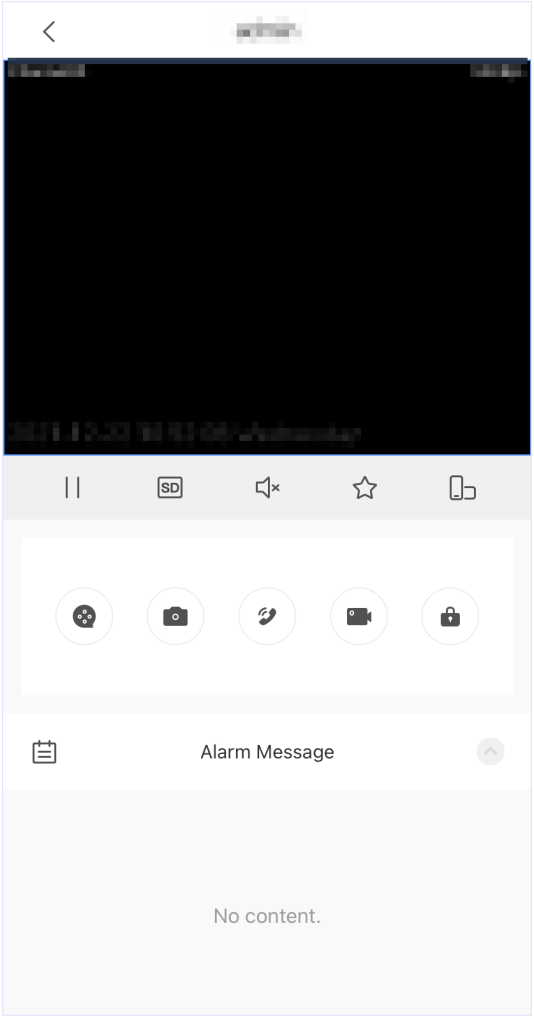
Paso 6 Configure el nombre del dispositivo y luego toque**Ahorrar**.

Figura 2-5 Configurar el nombre del dispositivo



Paso 7 Vea el vídeo de seguimiento desde la cámara del VTO.

Figura 2-6 Monitorear



3 Iniciar sesión y restablecer la contraseña

3.1 Iniciar sesión

Antes de iniciar sesión, asegúrese de que la computadora esté en el mismo segmento de red que el VTO.

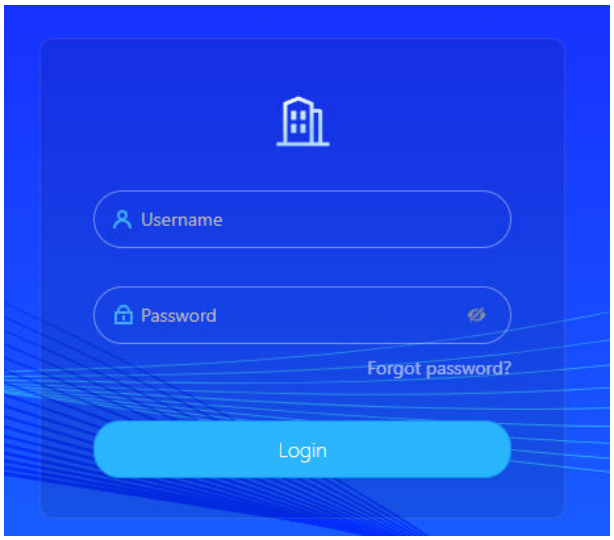
Procedimiento

Paso 1 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, le recomendamos que cambie la dirección IP predeterminada para evitar conflictos.

Paso 2 Ingresar**administración**como nombre de usuario, ingrese la contraseña que estableció durante la inicialización y luego haga clic en**Acceso**.

Figura 3-1 Iniciar sesión



3.2 Restablecer contraseña

Procedimiento

Paso 1 En la página de inicio de sesión, haga clic en**¿Has olvidado tu contraseña?**,y luego haga clic

Paso 2 **Próximo**. Escanee el código QR y obtendrá una cadena de números y letras.

Paso 3 Envíe la cadena a la cuenta de correo electrónico que se muestra en la página y luego el código de seguridad se enviará a la dirección de correo electrónico configurada durante la inicialización.

Etapa 4 Ingrese el código de seguridad en el cuadro de entrada y luego haga clic en**Próximo**.

- Si no configuró una dirección de correo electrónico durante la inicialización, comuníquese con su proveedor o servicio al cliente para obtener ayuda.
- El código de seguridad será válido sólo durante 24 horas después de su recepción.
- Si ingresa el código de seguridad incorrecto 5 veces consecutivas, su cuenta se bloqueará durante 5 minutos.

Paso 5 Ingrese y confirme la nueva contraseña y luego haga clic en**DE ACUERDO**.

4 Página de inicio

Figura 4-1 Página de inicio

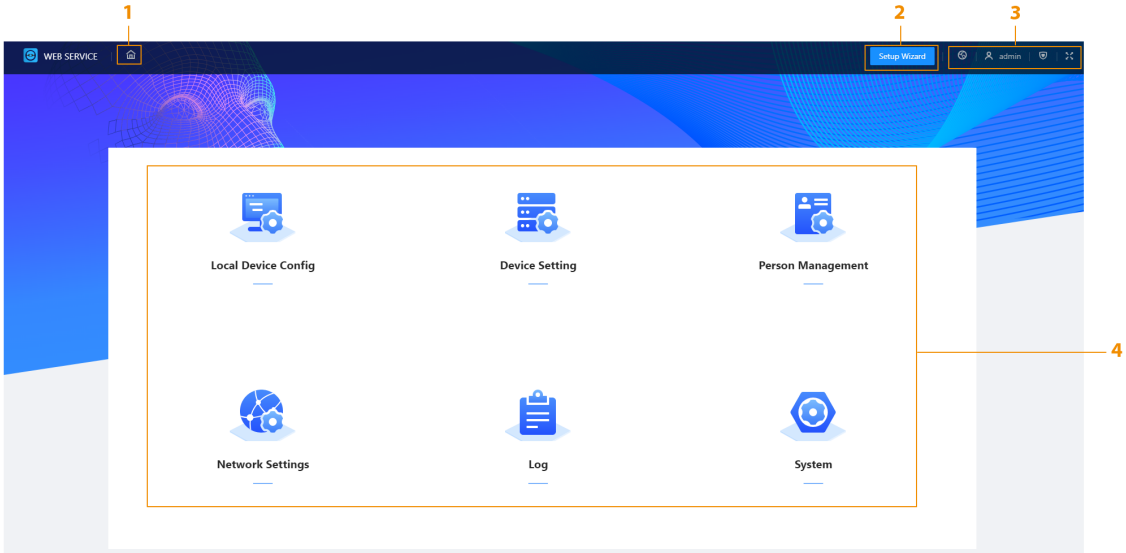


Tabla 4-1 Introducción a la página de inicio

No.	Función	Descripción
1	Botón de inicio	Vuelve a la página de inicio.
2	Asistente de configuración	Configure el servidor SIP de VTO.
3	Barra de navegación	• : Cambiar idioma de la página web del VTO. • admin: cambie la contraseña, cierre sesión en el dispositivo actual, reinicie el sistema y restaure el dispositivo a la configuración de fábrica. • : vea y configure los ajustes de seguridad. • : vea la página web en modo de pantalla completa.
4	función VTO	Diferentes áreas funcionales de la VTO.

5 Asistente de configuración

A través del asistente de configuración, puede finalizar el proceso de agregar VTO/VTH y especificar cualquier VTO como servidor SIP. También puede cancelar su estado de funcionamiento como servidor SIP.

5.1 Configuración como servidor SIP

Configure el VTO como servidor SIP.

Requisitos previos

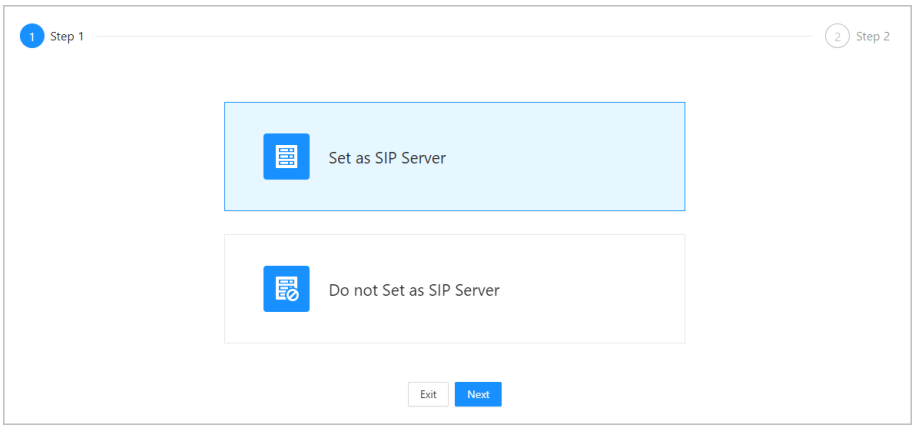
Ha agregado VTO en la página web. Si no, puedes agregarlos**Establecer como servidor SIP**página o en el **Configuración del dispositivo**sección.

Procedimiento

Paso 1 Inicie sesión en la página web de la VTO.

Paso 2 Seleccionar**Asistente de configuración**>**Establecer como servidor SIP**y luego haga clic en**Próximo**.

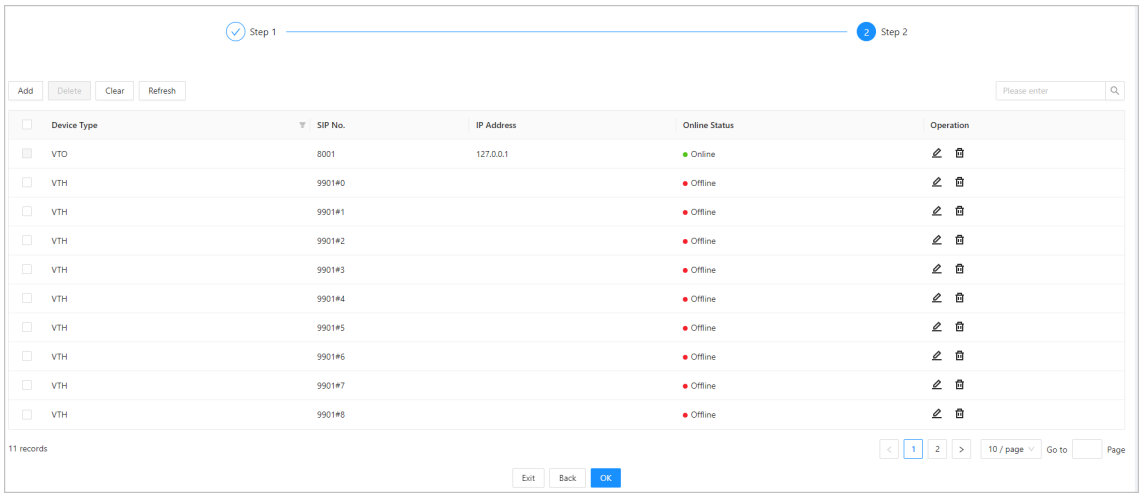
Figura 5-1 Establecer como servidor SIP



Paso 3 Seleccione el VTO que se configurará como servidor SIP y luego haga clic en**DE ACUERDO**.

También puedes hacer clic**Agregar**para agregar VTO si no ha tenido uno que funcione como servidor SIP.

Figura 5-2 Seleccione el servidor SIP



5.2 No configurar como servidor SIP

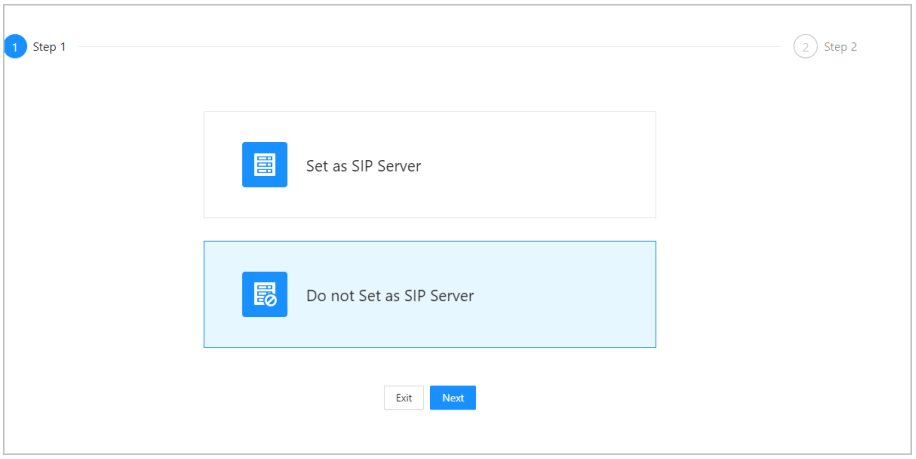
Si desea cambiar el servidor SIP, debe eliminar el actual de la lista.

Procedimiento

Paso 1 Inicie sesión en la página web de la VTO.

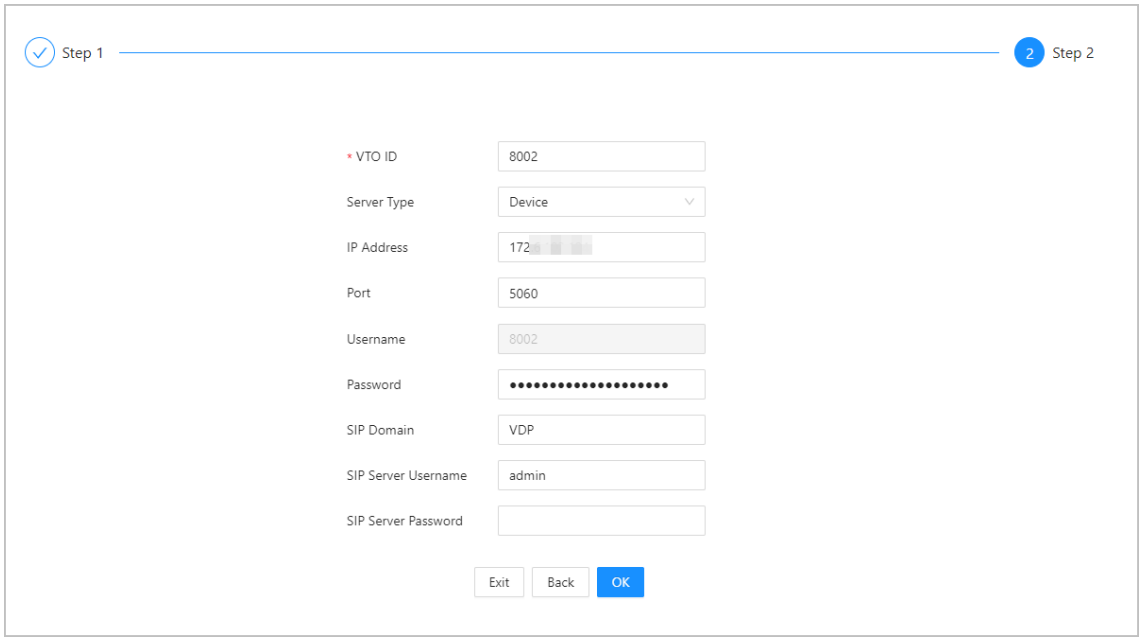
Paso 2 Seleccionar**Asistente de configuración**>**No configurar como servidor SIP**y luego haga clic en**Próximo**.

Figura 5-3 No configurar como servidor SIP



Paso 3 Configure la información del VTO que no desea configurar como servidor SIP y luego haga clic en**DE ACUERDO**.

Figura 5-4 Configurar información



6 Configuración del dispositivo local

Este capítulo presenta la configuración detallada del VTO.

Se pueden encontrar ligeras diferencias en diferentes modelos.

6.1 Configuraciones básicas

Configure los ajustes básicos del dispositivo.

6.1.1 Estación de puerta de villa

Procedimiento

Paso 1 Seleccionar**Configuración del dispositivo local**>**Ajustes**

Paso 2 **básicos**. Configure los parámetros.

Figura 6-1 Configuración básica (estación Villa)

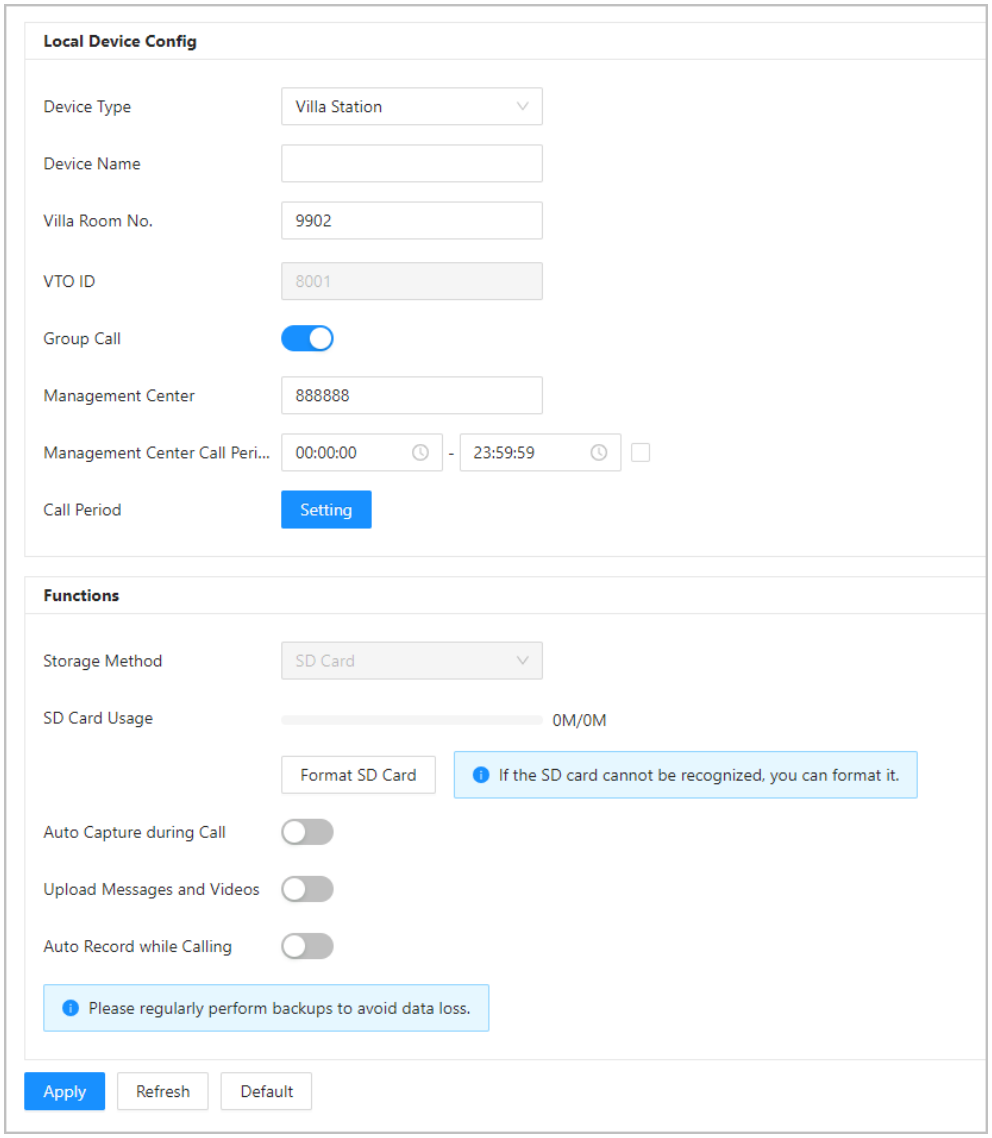


Tabla 6-1 Descripción de parámetros básicos

Parámetro	Descripción
Tipo de dispositivo	Seleccionar**Estación Villa**.
Nombre del dispositivo	Cuando otros dispositivos estén monitoreando este VTO, el nombre del dispositivo aparecerá en la imagen de monitoreo.
Habitación Villa No.	Número de habitación VTH. Se utiliza para llamar a VTH.
ID de VTO	Se utiliza para diferenciar cada VTO y le recomendamos configurarlo según la unidad o el número de edificio, y luego puede agregar VTO al servidor SIP utilizando sus números. El número no se puede cambiar cuando el VTO actúa como servidor SIP.
Centro de Gestión	888888 de forma predeterminada.

Parámetro	Descripción
Período de llamada del centro de gestión	Configure el período de tiempo en el que el VTO puede llamar al centro de gestión y luego habilite la función.
Llamada grupal	Habilítelo en el VTO que funciona como servidor SIP, y cuando un VTH principal reciba una llamada, todos los VTH de extensión también recibirán la llamada.
Período de llamada	El período de tiempo en el que el VTO llama a otros dispositivos no está limitado. Hacer clic**Configuración**para configurar el periodo de llamada en un día/ semana.
Método de almacenamiento	Tarjeta SD por defecto.
Uso de la tarjeta SD	Muestra la capacidad total y utilizada de la tarjeta SD. Puedes hacer clic **Formatear tarjeta SD**para eliminar todos los datos de la tarjeta SD.
Captura automática durante la llamada	Tome una instantánea y guárdela en la tarjeta SD del VTO cuando el VTO esté llamando.
Subir mensajes y vídeos	Cuando está habilitado: ● Si se inserta una tarjeta SD tanto en el VTH como en el VTO, el mensaje de video se guardará tanto en las tarjetas SD del VTH como en el VTO. ● Si solo se inserta una tarjeta SD en el VTH o el VTO, el mensaje de video se guardará solo en la tarjeta SD del VTH o el VTO. ● Si no se inserta ninguna tarjeta SD en el VTH o VTO, no se guardará ningún mensaje de video.
Grabación automática durante una llamada	Realice una grabación cuando el VTO esté en una llamada y guárdela en la tarjeta SD del VTO.

Paso 3 Hacer clic**Aplicar**.

6.1.2 Segunda Estación de Confirmación

Procedimiento

Paso 1 Seleccionar**Configuración del dispositivo local**>**Ajustes**

Paso 2 **básicos**. Configure los parámetros.

Figura 6-2 Configuración básica (segunda estación de confirmación)

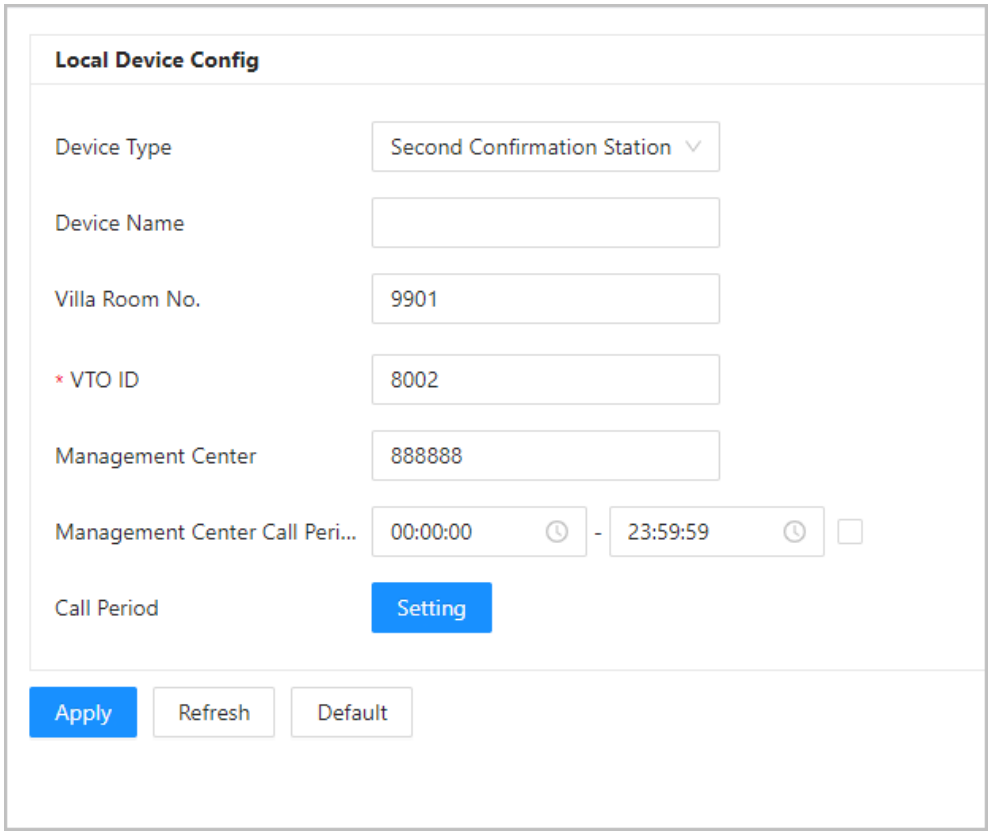


Tabla 6-2 Descripción de parámetros básicos

Parámetro	Descripción
Tipo de dispositivo	Seleccionar**Segunda Estación de Confirmación**.
Nombre del dispositivo	Cuando otros dispositivos estén monitoreando este VTO, el nombre del dispositivo aparecerá en la imagen de monitoreo.
Habitación Villa No.	Número de habitación VTH. Se utiliza para llamar a VTH.
ID de VTO	Se utiliza para diferenciar cada VTO y le recomendamos configurarlo según la unidad o el número de edificio, y luego puede agregar VTO al servidor SIP utilizando sus números. El número no se puede cambiar cuando el VTO actúa como servidor SIP.
Centro de Gestión	888888 de forma predeterminada.
Período de llamada del centro de gestión	Configura la hora si solo deseas recibir llamadas de VTH durante un período específico y luego habilita la función.
Período de llamada	Hacer clic**Configuración**para configurar el periodo de llamada en un día/semana.

Paso 3 Hacer clic**Aplicar**.

6.2 Control de acceso

Las diferentes series de modelos tienen variadas funciones de control de acceso. A continuación se muestra el ejemplo de configuración del modelo serie Q.

6.2.1 Configuración

Procedimiento

Paso 1 Seleccionar**Configuración del dispositivo local**>**Control de acceso**>

Paso 2 **configuración**. Configure los parámetros.

Figura 6-3 Control de acceso

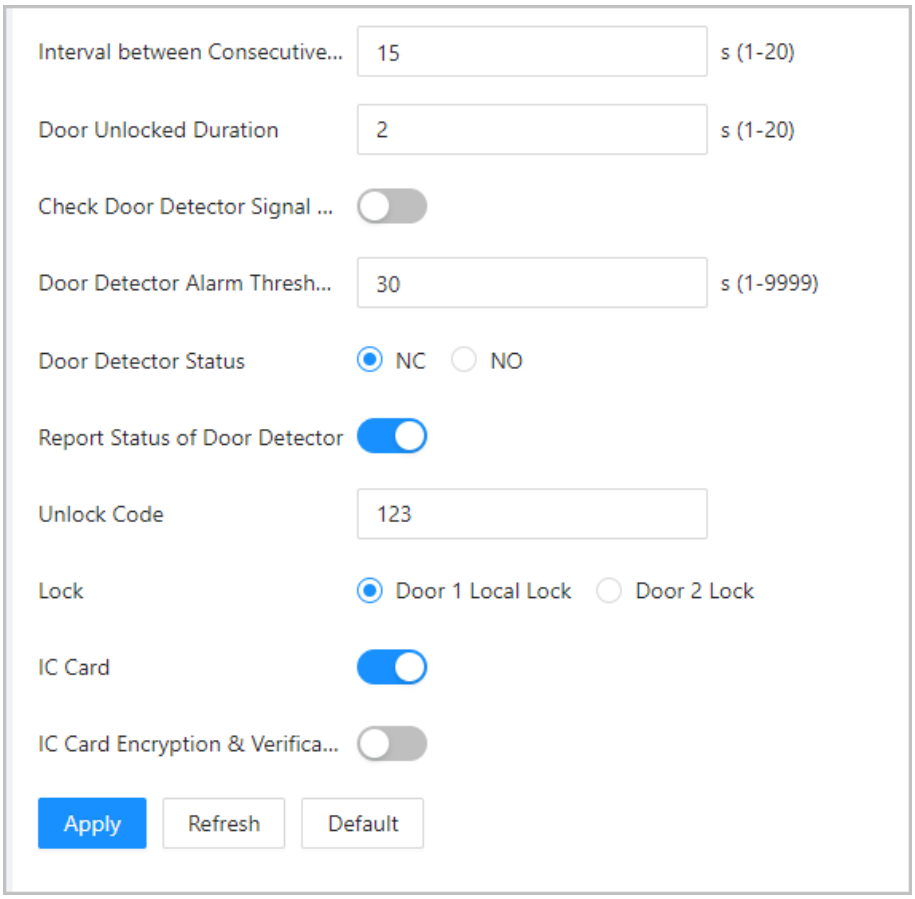


Tabla 6-3 Descripción de los parámetros de control de acceso

Parámetro	Descripción
Intervalo entre desbloqueos consecutivos	La puerta sólo se podrá volver a desbloquear después de ese intervalo.
Duración de la puerta desbloqueada	El tiempo durante el cual la cerradura permanece abierta.
Verifique la señal del detector de puerta antes de cerrar	Habilite la función según sus necesidades.
Umbral de alarma del detector de puerta	El umbral de tiempo en el que se activa la alarma del detector de puerta.

Parámetro	Descripción
Estado del detector de puerta	● **CAROLINA DEL NORTE**:Normalmente cerrado. ● **NO**:Normalmente abierto.
Informe del estado del detector de puerta	Sincronice el estado del sensor de puerta con los monitores interiores (VTH).
Código de desbloqueo	Puede conectar un teléfono de terceros, como un teléfono SIP, al VTO y usar el código para abrir la puerta de forma remota.
Cerrar	● **Cerradura local de la puerta 1**: Bloqueo local. ● **Cerradura de la puerta 2**: 485 cerradura. Seleccione el tipo de bloqueo para desbloquear el bloqueo que seleccione.
Tarjeta IC	Habilite la función para que los usuarios puedan deslizar tarjetas para desbloquear la puerta.
Cifrado y verificación de tarjetas IC	Habilite la función para que el cifrado y la verificación de la tarjeta IC surtan efecto.

Paso 3 Hacer clic**Aplicar**.

6.2.2 RS-485

Procedimiento

Paso 1 Seleccionar**Configuración del dispositivo local**>**Control de acceso**>**RS-485**.

Paso 2 Configura los parámetros de la cerradura conectada a través del puerto RS-485.

Figura 6-4 RS-485

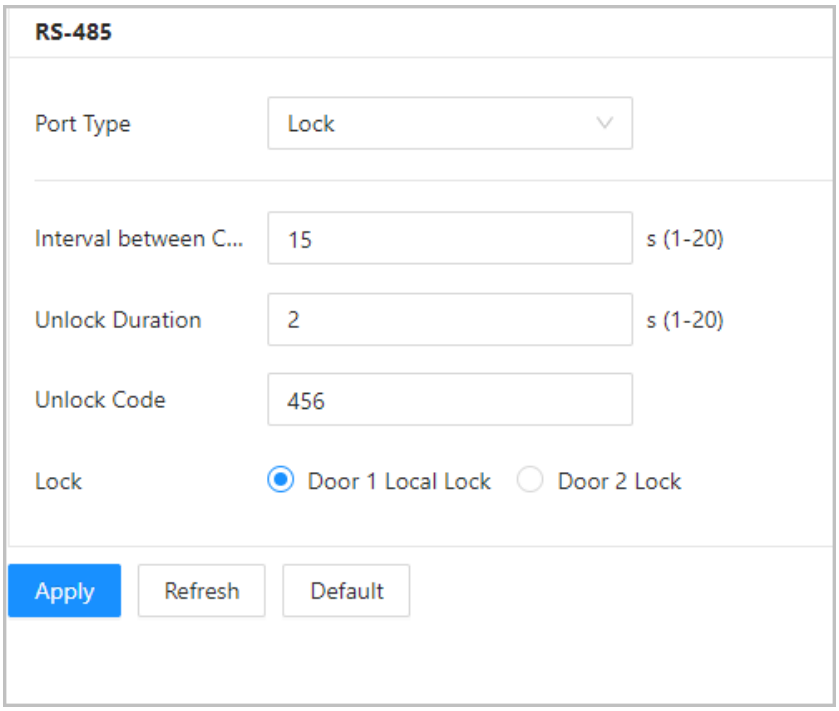


Tabla 6-4 Descripción de RS-485

Parámetro	Descripción
Tipo de puerto	**Cerrar**por defecto.

Parámetro	Descripción
Intervalo entre desbloqueos consecutivos	La puerta sólo se podrá volver a desbloquear después de ese intervalo.
Duración del desbloqueo	El tiempo durante el cual la cerradura permanece abierta.
Código de desbloqueo	Puede conectar un teléfono de terceros, como un teléfono SIP, al VTO y usar el comando para abrir la puerta de forma remota. El comando predeterminado es 456.
Cerrar	Selecciona el**Cerrar**escriba para desbloquear el bloqueo que seleccione. ● **Cerradura local de la puerta 1**: Bloqueo local. ● **Cerradura de la puerta 2**: 485 cerradura.

Paso 3 Hacer clic**Aplicar**.

6.3 Diseño

Esta función solo está disponible para la serie Q con múltiples botones (1 botón, 2 botones y 4 botones). A continuación se muestra un ejemplo de configuración para el VTO que tiene un botón instalado en su dispositivo.

Procedimiento

Paso 1 Inicie sesión en la página web de la VTO. Seleccionar

Paso 2 **Configuración del dispositivo local**>**Disposición**.

Paso 3 Haga clic en las placas de identificación al lado de donde instaló los botones y luego seleccione el número de habitación en la lista.**Módulo**quieres unir. Por ejemplo, 9901, 9902, 9903 y 9904.

- Primero debe configurar el número de habitación. De lo contrario, no tendrá ningún número de habitación para seleccionar en la lista de módulos. Los números de habitación VTH están configurados en**Configuración del dispositivo**. Para obtener más información, consulte "8.2 Gestión de VTH".
- Debe configurar el número de habitación según la posición de instalación de los botones. Por ejemplo, si solo ha instalado un botón al lado de la primera placa de identificación, deberá hacer clic en el módulo de la primera placa de identificación para configurar el número de habitación en la página web. Si ha instalado un botón al lado de la cuarta placa de identificación, deberá hacer clic en el módulo de la cuarta placa de identificación para configurar el número de habitación en la página web. Mantenga la regla de configuración anterior cuando instale 2 botones o 4 botones en el VTO y configure los números de habitación correspondientes en la página web.

Figura 6-5 Instalación del cuarto botón

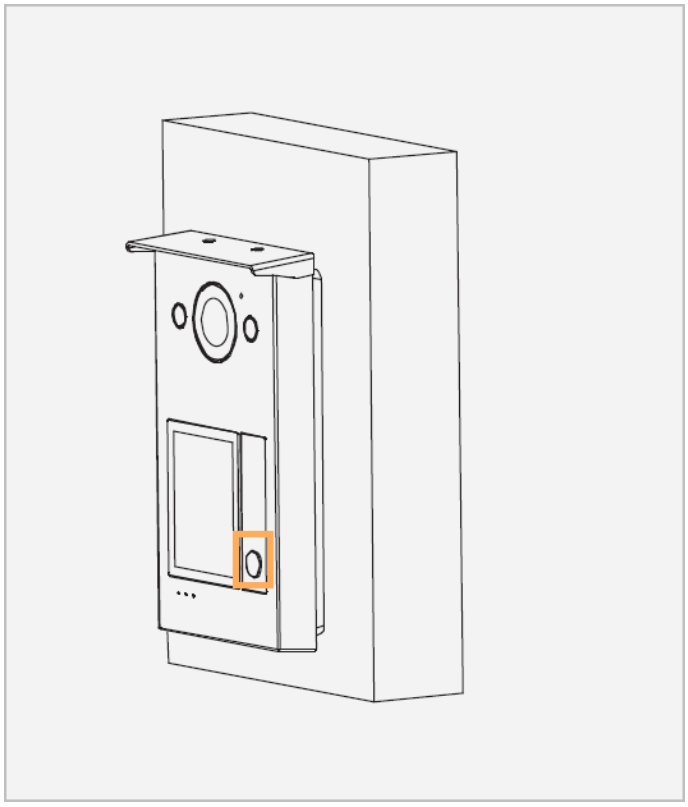
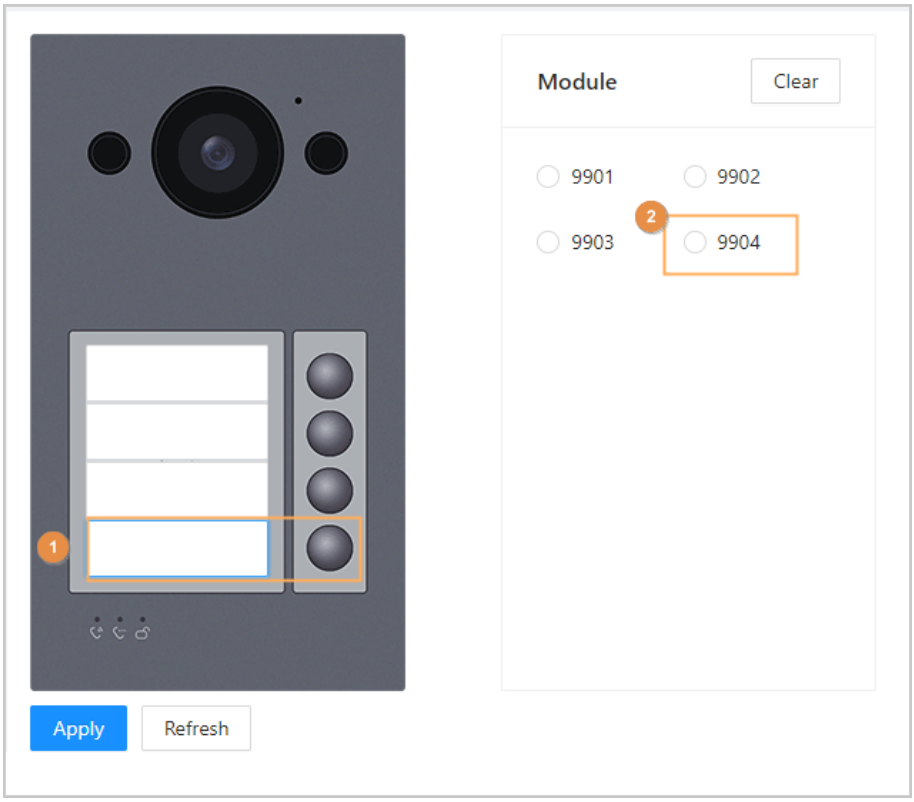
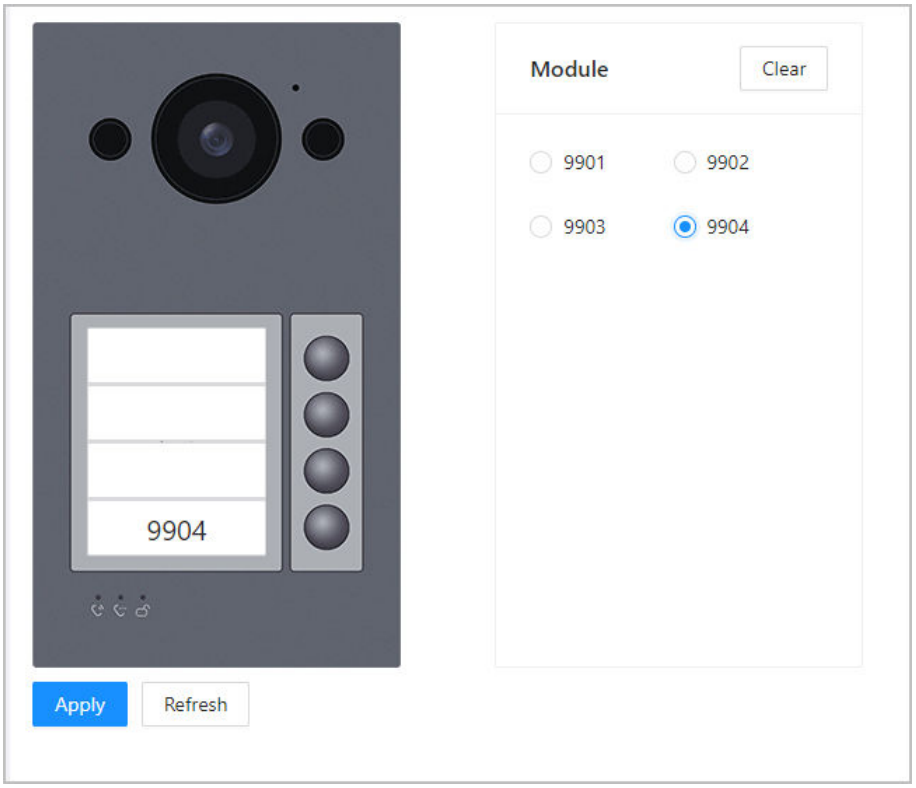


Figura 6-6 Configurar la cuarta placa de identificación (1)



Etapa 4 Hacer clic**Aplicar**para guardar el número de habitación seleccionado.

Figura 6-7 Configurar la cuarta placa de identificación



Paso 5 Si desea vincular los números de las habitaciones cuando instala 2 botones o 4 botones para el VTO, repita del Paso 3 al Paso 4 hasta que haya configurado todos los números de las habitaciones.

7 sistema

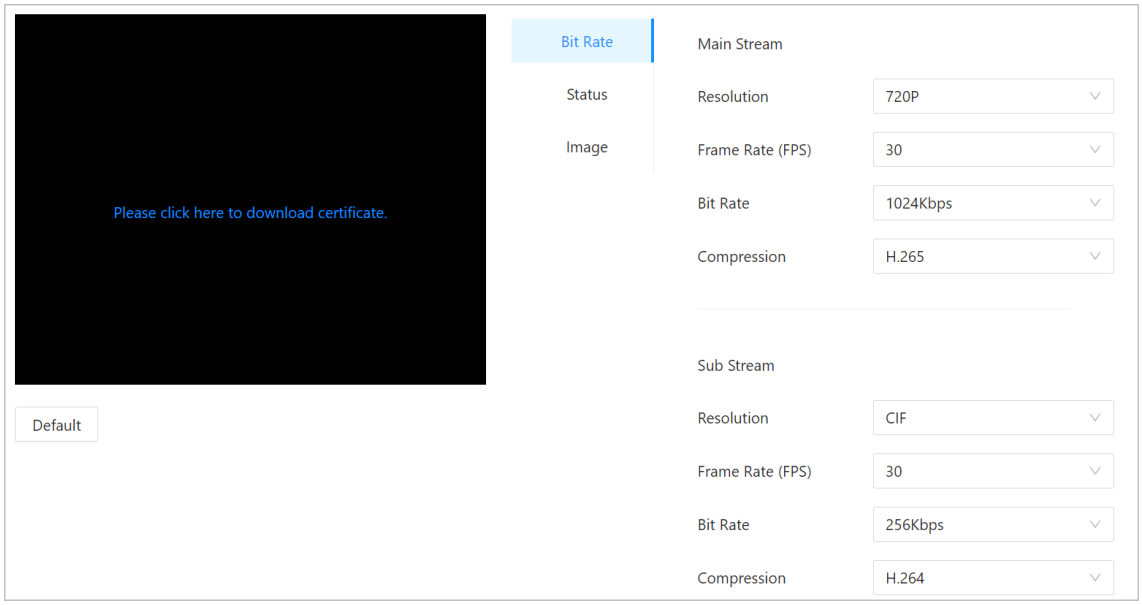
Vídeo 7.1

Configurar el formato y calidad de vídeo y audio del VTO.

Procedimiento

Paso 1 Seleccionar**Sistema**>**Video**.

Figura 7-1 Vídeo



Paso 2 Configure los parámetros, que entrarán en vigor tras el cambio.

Tabla 7-1 Descripción del parámetro de vídeo

Parámetro		Descripción
Tasa de bits	Resolución (principal Arroyo)	• **720P**:1280 × 720. • **WVGA**:800 × 480. • **D1**:704 × 576. • **CIF**:352 × 288.
	Velocidad de fotogramas (FPS) (transmisión principal)	• Si selecciona el**Estándar de vídeo**como**CAMARADA**: El rango es de 1 a 25. • Si selecciona el**Estándar de vídeo**como**NTSC**: El rango es de 1 a 30). Cuanto mayor sea el valor, más fluido será el vídeo, pero requerirá más ancho de banda.
	Tasa de bits (transmisión principal)	Incluye 768 Kbps, 896 Kbps, 1024 Kbps, 1,25 Mbps, 1,5 Mbps, 1,75 Mbps, 2 Mbps y 4 Mbps y más. Cuanto mayor sea el valor, mejor será la calidad del vídeo, pero requiere más ancho de banda.

Parámetro		Descripción
	Compresión (principal Arroyo)	H.264. H.265. En comparación con H.264, H.265 requiere un ancho de banda menor.
	Resolución (subtransmisión)	● **1080P**:1920 × 1080. ● **WVGA**:800 × 480. ● **QVGA**:320 × 240. ● **D1**:704 × 576. ● **CIF**:352 × 288.
	Velocidad de fotogramas (FPS) (subtransmisión)	El rango es de 1 a 25. Cuanto mayor sea el valor, más fluido será el vídeo, pero requiere más ancho de banda.
	Velocidad de bits (subtransmisión)	Incluye 224 Kbps, 256 Kbps, 320 Kbps, 384 Kbps, 448 Kbps, 512 Kbps, 640 Kbps, 768 Kbps. Cuanto mayor sea el valor, mejor será la calidad del vídeo, pero requiere más ancho de banda.
	Compresión (Sub Arroyo)	H.264. H.265.
Estado	Modo escena	Seleccionar de**Auto**,**Desactivar**,**Soleado**y**Noche**.**Auto**está seleccionado de forma predeterminada.
	Modo de compensación	● **BLC**:Compensación de luz de fondo. Mejora la claridad del objetivo en la imagen. ● **WDR**:Amplio rango dinámico. Mejore el brillo de las áreas oscuras y reduzca el brillo de las áreas brillantes para mejorar la imagen. ● **CHL**:Alta compensación de luz. Reduzca el brillo de los puntos fuertes para mejorar la imagen general. ● **Desactivar**: No utilice ningún modo de compensación.
	Día/Noche	Seleccionar de**Color**,**Auto**y**B/N**.
	Estándar de vídeo	Seleccionar**CAMARADA**o**NTSC**según tu zona.
Imagen	Brillo	Cuanto mayor sea el valor, más brillante será la imagen.
	Contraste	Valor mayor para mayor contraste entre áreas brillantes y oscuras.
	Matiz	Haz que el color sea más brillante o más oscuro. El valor predeterminado lo establece el sensor de luz y recomendamos mantenerlo predeterminado.
	Saturación	Cuanto mayor sea el valor, más denso será el color.

Parámetro		Descripción
	Gama	Cambia el brillo de la imagen y mejora el rango dinámico de la imagen de forma no lineal. Cuanto mayor sea el valor, más brillante será la imagen. Esta función está disponible en modelos selectos.
	Espejo	Muestre la imagen con los lados izquierdo y derecho invertidos.
	Voltear	Muestre la imagen al revés.
	Tiempo de visualización	Muestra la hora y fecha actuales en la imagen de vídeo.

7.2 Audio

Procedimiento

Paso 1 Seleccionar**Sistema**>**Video**.

Paso 2 Configure los parámetros, que entrarán en vigor tras el cambio.

Figura 7-2 Audio

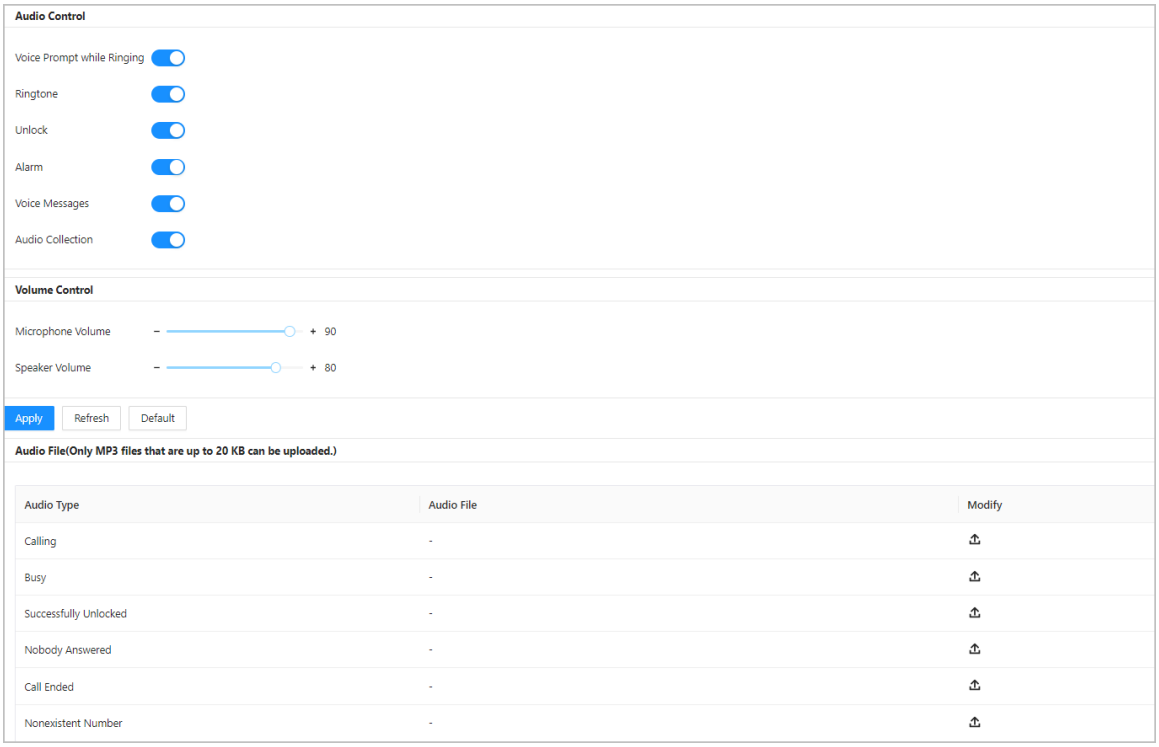


Tabla 7-2 Descripción de los parámetros de audio

Parámetro		Descripción
control de audio	Aviso de voz mientras suena	Activa o desactiva cada tipo de sonido.
	Tono de llamada	
	Alarma	

Parámetro		Descripción
	Mensajes de voz	
	desbloquear	
	Colección de audios	
Control del volumen	Volumen del micrófono	Ajusta el volumen.
	Volumen del altavoz	

Paso 3 Hacer clic**Aplicar**.

Etapa 4 (Opcional) Cargue el archivo de audio haciendo clic junto al tipo de audio correspondiente (incluyendo llamadas, ocupado, desbloqueado exitosamente, nadie respondió, llamada finalizada y número inexistente).

Sólo se pueden cargar archivos MP3 de hasta 20 KB.

7.3 Tiempo

Configure la zona horaria y los parámetros de horario de verano.

Procedimiento

Paso 1 Seleccionar**Sistema**>**Tiempo**.

Paso 2 Configure la hora y la zona horaria y el horario de verano.

Figura 7-3 Hora

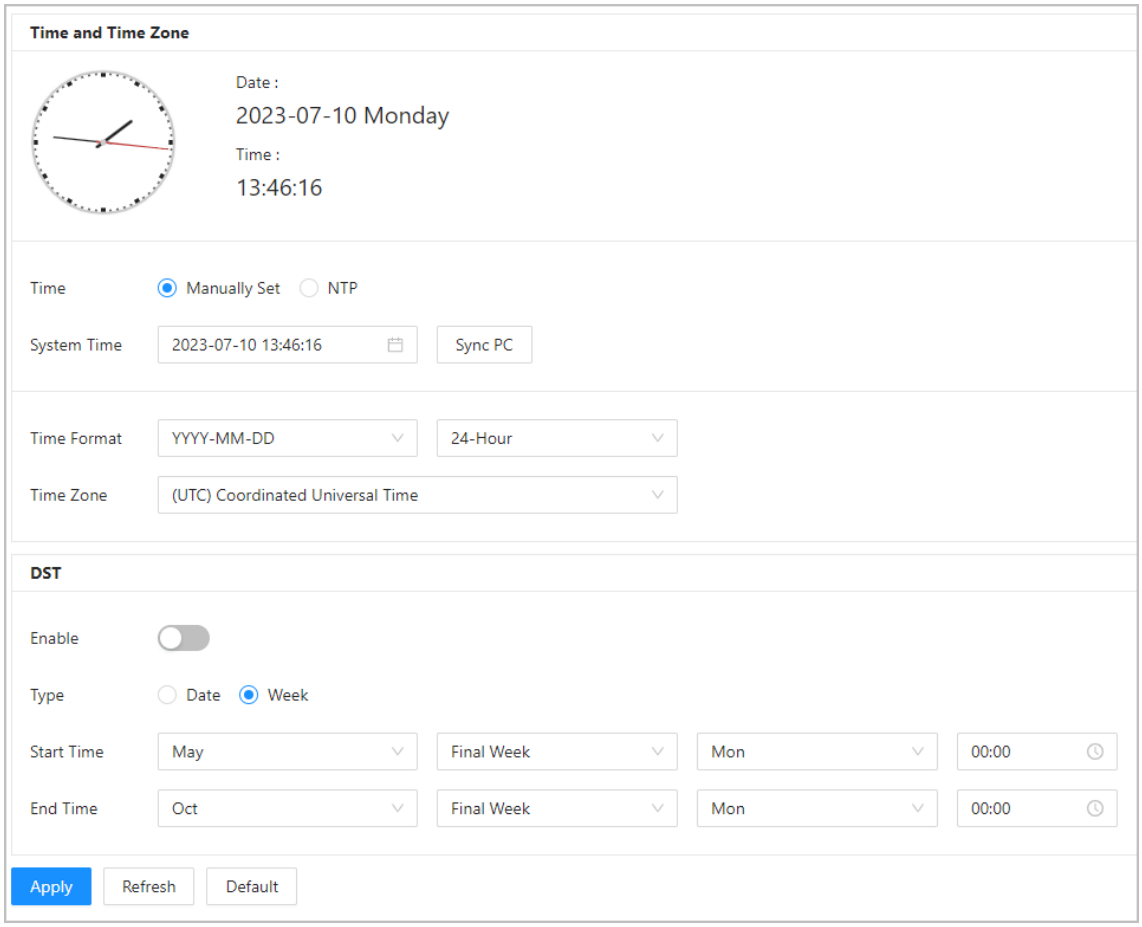


Tabla 7-3 Descripción de parámetros

Módulo	Parámetro	Descripción
Tiempo y tiempo Zona	Tiempo	• Establecer manualmente • NTP
	Hora del sistema	La hora del sistema VTO. ⚠ Cambiar la hora del sistema puede causar problemas en la búsqueda de videos y publicación de información. Desactive la grabación de video y la instantánea automática antes de cambiarlas. 📖 Sólo aplicable bajo el**Establecer manualmente**modo.
	Sincronizar PC	Sincronice la hora del sistema VTO con su PC. 📖 Sólo aplicable bajo el**Establecer manualmente**modo.

Módulo	Parámetro	Descripción
	Servidor	La dirección del servidor NTP. Sólo aplicable bajo el**NTP**modo.
	Actualización manual	Haga clic en el icono y la hora del dispositivo VTO se sincronizará automáticamente con el servidor. Sólo aplicable bajo el**NTP**modo.
	Puerto	Número de puerto del servidor NTP. Sólo aplicable bajo el**NTP**modo.
	Intervalo	Ciclo de actualización de hora VTO. 30 minutos como máximo. Sólo aplicable bajo el**NTP**modo.
	Formato de tiempo	Para el formato de fecha, seleccione uno de los siguientes: ● AAAA-MM-DD ● MM-DD-AAAA ● DD-MM-AAAA Para el formato de hora, seleccione uno de los siguientes: ● 24 horas ● 12 horas
	Zona horaria	Seleccione la zona horaria para el sistema VTO.
horario de verano	Permitir	Haga clic para habilitar el**horario de verano**función.
	Tipo	Seleccionar**Fecha**o**Semana**según sea necesario y luego configure el período específico.
	Hora de inicio	Configure la hora de inicio y finalización del horario de verano.
	Hora de finalización	

Paso 3 Hacer clic**Aplicar**.

7.4 Usuario ONVIF

Agregue cuentas para dispositivos para monitorear el VTO a través del protocolo ONVIF.

Procedimiento

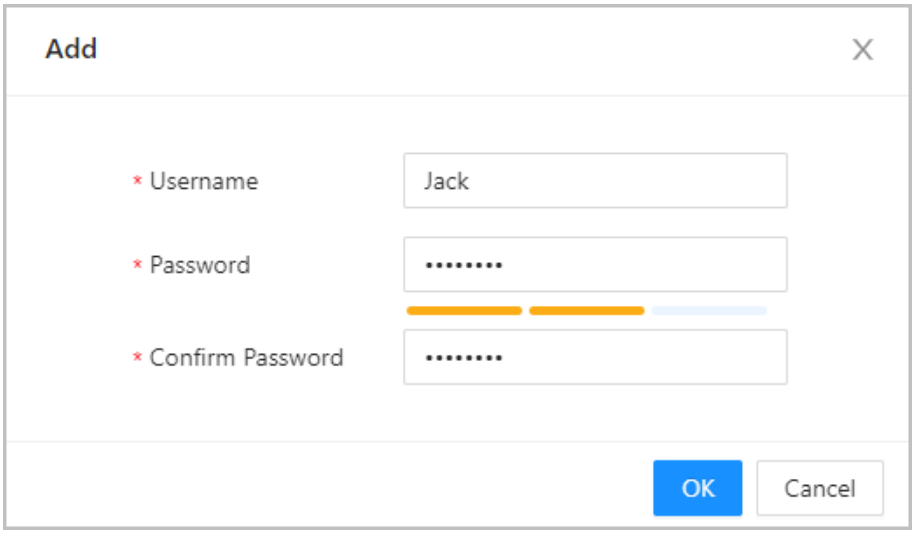
Paso 1 Seleccionar**Sistema**>**Usuario ONVIF**.

Paso 2 Hacer clic**Agregar**.

Paso 3 Ingrese la información y luego haga clic**DE ACUERDO**.

Los dispositivos ONVIF pueden monitorear el VTO usando la cuenta.

Figura 7-4 Usuario ONVIF



7.5 Configuración

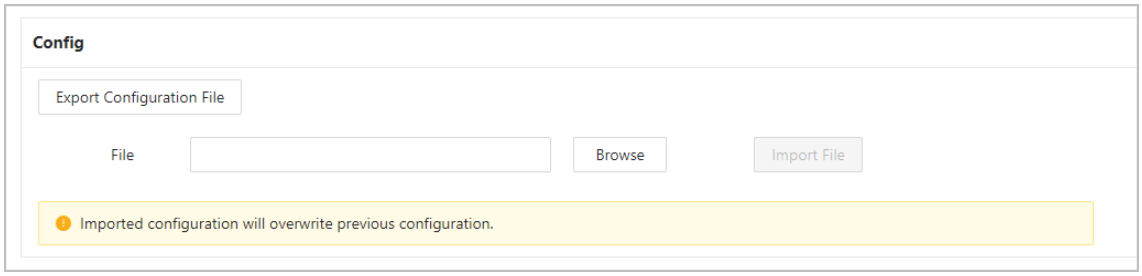
Puede exportar e importar el archivo de configuración.

Procedimiento

Paso 1 Seleccionar**Sistema**>**configuración**.

Paso 2 Hacer clic**Exportar archivo de configuración**, o haga clic**Navegar**para seleccionar el archivo desde la computadora local y luego haga clic en**Importar archivo**.

Figura 7-5 Configuración



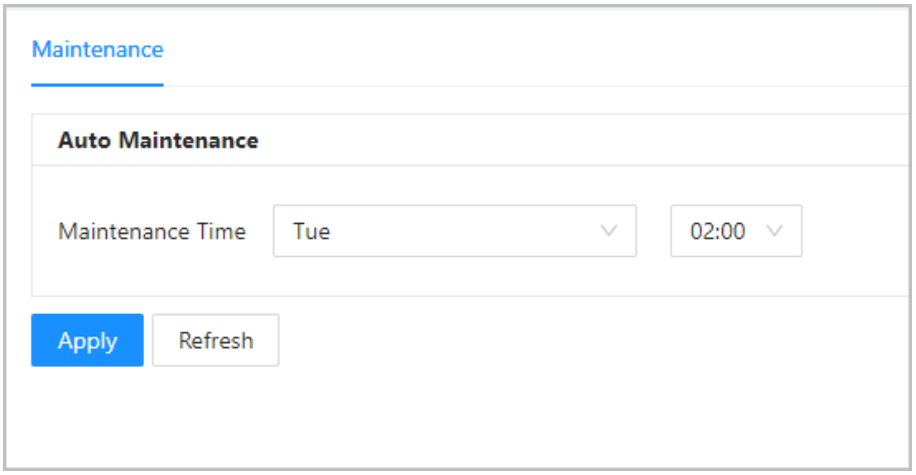
7.6 Mantenimiento

Procedimiento

Paso 1 Seleccionar**Sistema**>**Mantenimiento**. Configure el

Paso 2 tiempo de mantenimiento automático.

Figura 7-6 Mantenimiento automático



Paso 3 Hacer clic**Aplicar**.

7.7 Actualización

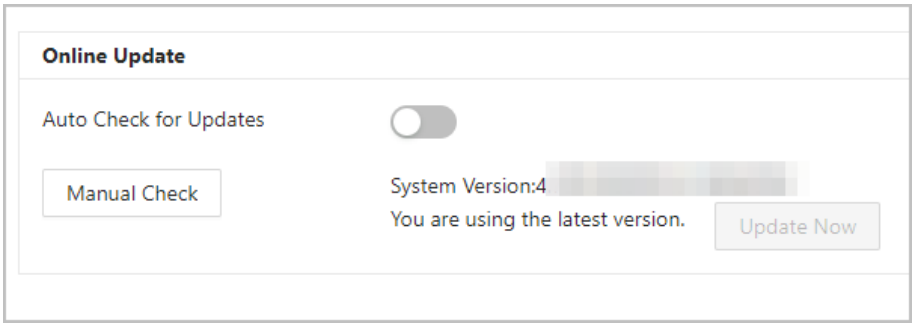
Procedimiento

Paso 1 Seleccionar**Sistema**>**Actualizar**. Seleccione

Paso 2 formas de verificar la actualización.

- **Verificación automática**:Seleccione la función para comprobar automáticamente si hay una nueva versión del sistema.
- **Verificación manual**:Seleccione la función para comprobar si hay una nueva versión del sistema.

Figura 7-7 Actualización



7.8 Información legal

Seleccionar**Sistema**>**Información legal**. Puede consultar avisos de información legal relacionados en esta sección.

7.9 Información del sistema

Procedimiento

Paso 1 Seleccionar**Sistema**>**Información del sistema**.

Paso 2 Vea la versión del software y la versión básica de seguridad.

Figura 7-8 Información del sistema

Software Version	2023-06-21 V4.700.0000000.0.R
Security Baseline Version	

8 Configuración del dispositivo

Este capítulo presenta cómo agregar, modificar y eliminar VTO, VTH, VTS e IPC, y cómo enviar mensajes desde el servidor SIP a VTO y VTH cuando el VTO funciona como servidor SIP. Si está utilizando otros servidores como servidor SIP, consulte el manual correspondiente para obtener más detalles.

8.1 Gestión del nº de VTO

Puede agregar VTO al servidor SIP y todos los VTO conectados al mismo servidor SIP pueden llamarse entre sí.

Procedimiento

Paso 1 Inicie sesión en la página web del VTO que funciona como servidor SIP. Seleccionar

Paso 2 **Configuración del dispositivo**. Hacer clic**Agregar**.

Paso 3

Etapa 4 Configure los parámetros.

Figura 8-1 Agregar VTO

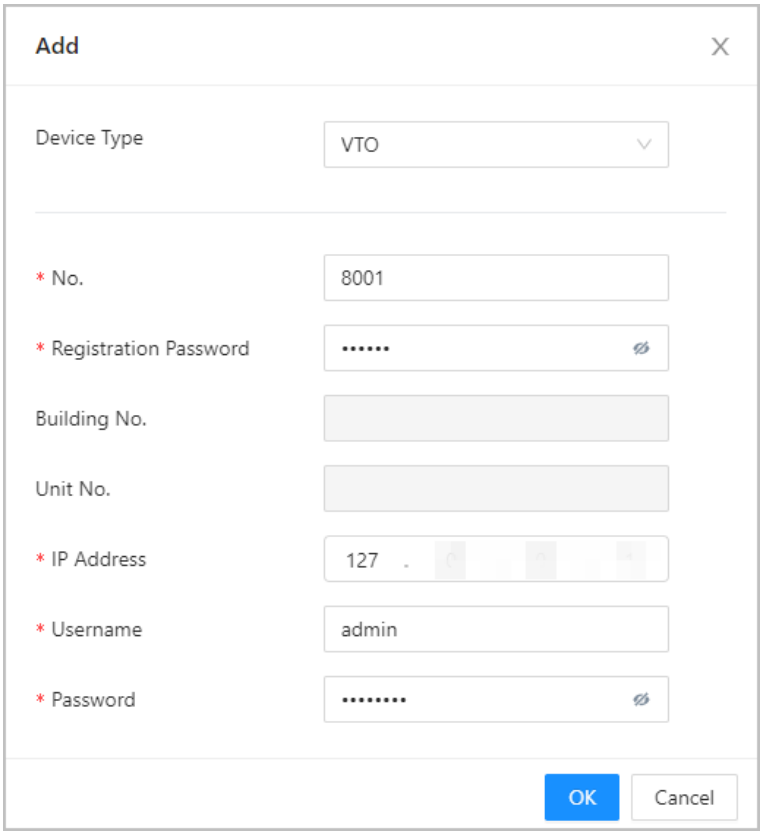


Tabla 8-1 Agregar configuración de VTO

Parámetro	Descripción
Tipo de dispositivo	Seleccionar**VTO**.
No.	El número VTO que configuró.
Contraseña de registro	Déjalo por defecto.

Parámetro	Descripción
Edificio número.	Disponible solo cuando los servidores de la plataforma funcionan como servidor SIP.
Numero de unidad.	
Dirección IP	Dirección IP del VTO.
Nombre de usuario	Nombre de usuario y contraseña utilizados para iniciar sesión en la página web de la VTO.
Contraseña	

Paso 5 Hacer clic**DE ACUERDO**.

Hacer clic para editar el VTO, o para eliminar VTO añadidos, pero el que tienes la sesión iniciada no se puede modificar ni eliminar.

8.2 Gestión de VTH

Puede agregar números de habitación al servidor SIP y luego configurar el número de habitación en los VTH para conectarlos a la red.

Procedimiento

Paso 1 Inicie sesión en la página web del servidor SIP. Seleccionar

Paso 2 **Configuración del dispositivo**. Hacer clic**Agregar**.

Paso 3

Etapa 4 Configure los parámetros.

Figura 8-2 Agregar VTH

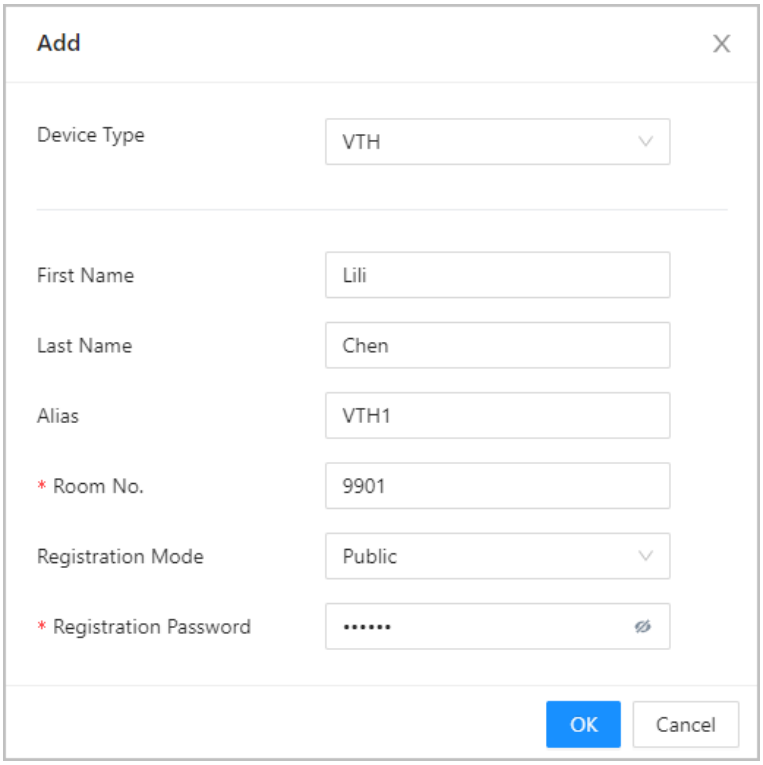


Tabla 8-2 Información de la habitación

Parámetro	Descripción
Nombre de pila	Introduce la información que necesitas para diferenciar cada habitación.
Apellido	
Alias	
Habitación no.	Ingrese un número de habitación y luego configure el número en un VTH para conectarse a la red.
Tipo de registro	Seleccionar**público**.
Contraseña de registro	Déjalo por defecto.

Paso 5 Hacer clic**Ahorrar**.

Hacer clic para editar el VTH, o para eliminar VTH agregados, pero el que tienes la sesión iniciada no se puede modificar ni eliminar.

8.3 Gestión del VTS

Puede agregar un VTS al servidor SIP y luego podrá usarlo como centro de administración. También puede gestionar, llamar o recibir llamadas de todos los VTO y VTH de la red. Consulte el manual del usuario correspondiente para obtener más detalles.

Procedimiento

Paso 1 Inicie sesión en la página web del VTO que funciona como servidor SIP. Seleccionar

Paso 2 **Configuración del dispositivo**. Hacer clic**Agregar**.

Paso 3

Etapa 4 Configure los parámetros.

Figura 8-3 Agregar VTS

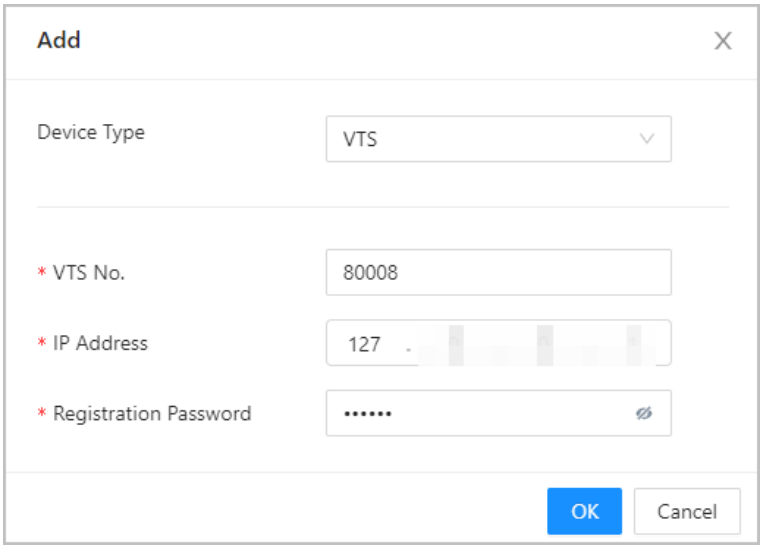


Tabla 8-3 Agregar configuración de VTS

Parámetro	Descripción
Tipo de dispositivo	Seleccionar**VTS**.
VTS No.	El número del VTS.
Contraseña de registro	Déjalo por defecto.
Dirección IP	Dirección IP del VTS.

Paso 5 Hacer clic**DE ACUERDO**.

Gestión de 9 personas

Agregar información del personal.

Información de contexto

Algunas series VTO admiten la función de emisión de tarjetas en la gestión de personas. Emitir una tarjeta de acceso para desbloquear la puerta de una habitación. Para utilizar esta función, el VTO debe tener un lector de tarjetas.

Procedimiento

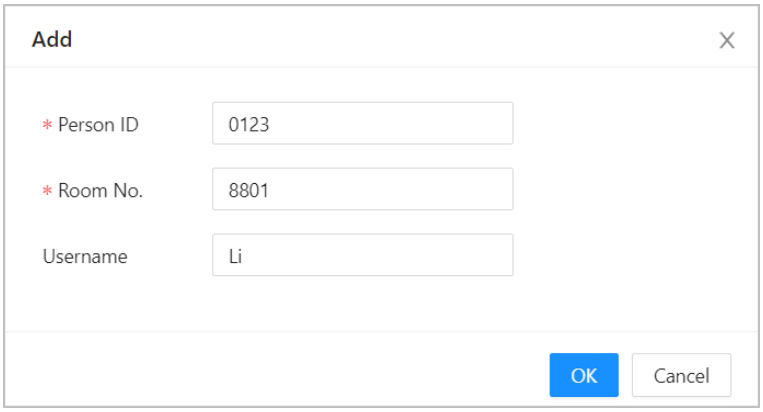
Paso 1 Inicie sesión en la página web de la VTO.

Paso 2 Seleccionar**Gestión de personas**. Hacer clic

Paso 3 **Agregar**.

- VTO que no tienen función de emisión de tarjeta: ingrese la ID de la habitación, el número de la habitación, el nombre de usuario y luego haga clic en**DE ACUERDO**.

Figura 9-1 Agregar persona



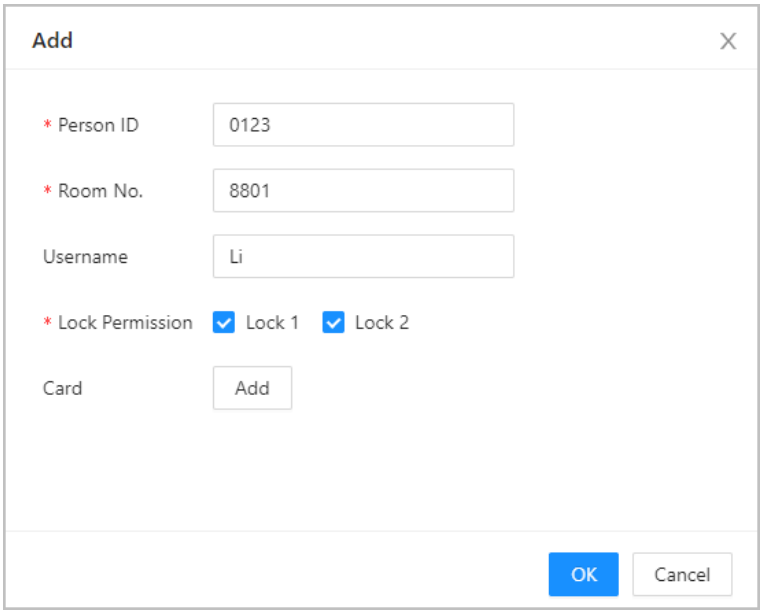
- VTO que tiene función de emisión de tarjetas:

1. Ingrese la ID de la habitación, el número de la habitación, el nombre de usuario y seleccione el permiso de bloqueo.

   - Bloqueo1: bloqueo local.
   - Bloqueo 2: bloqueo 485.

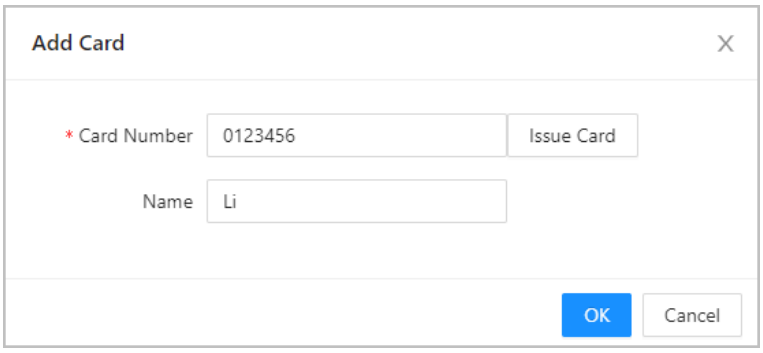
   Sólo los modelos que tienen 485 puertos admiten 2 tipos de cerraduras.

Figura 9-2 Agregar una persona



2. Haga clic**Agregar**junto a**Tarjeta**y luego ingrese el número de tarjeta y el nombre.

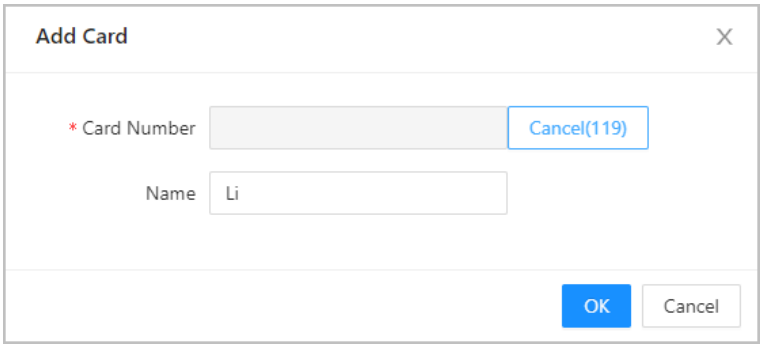
Figura 9-3 Tarjeta de problema



3. Haga clic**Tarjeta de emisión**.

La página web muestra el mensaje de cuenta regresiva (120 segundos). Una vez que comience la cuenta regresiva, deberá deslizar la tarjeta en el lector de tarjetas del VTO dentro de este período de tiempo. Después de pasarla, el VTO reconocerá automáticamente el número de la tarjeta.

Figura 9-4 Cuenta regresiva

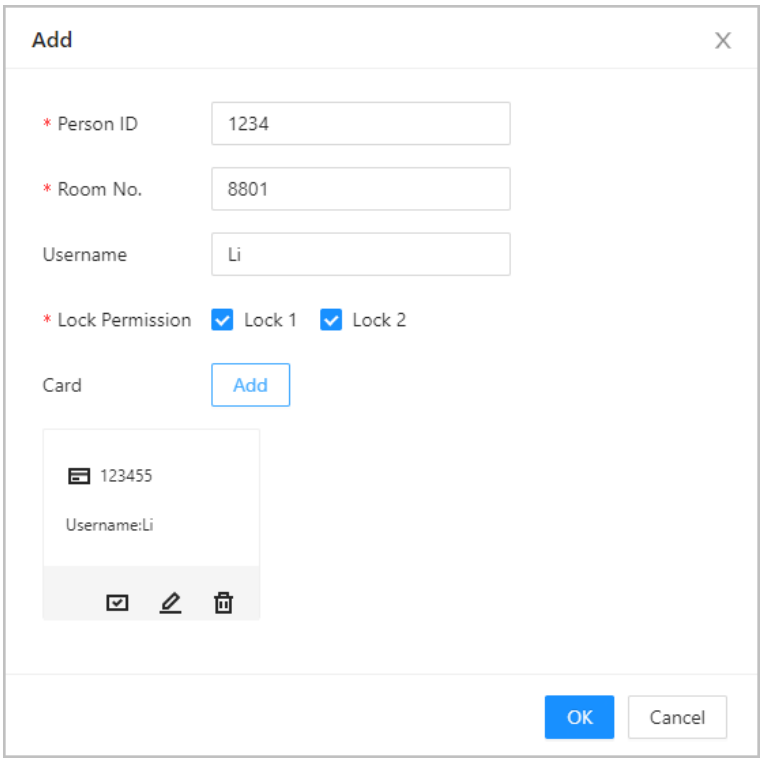


4. Haga clic**DE ACUERDO**después de deslizar para completar el proceso de emisión.

Luego la ventana vuelve a la**Agregar**, añadiendo una tarjeta.

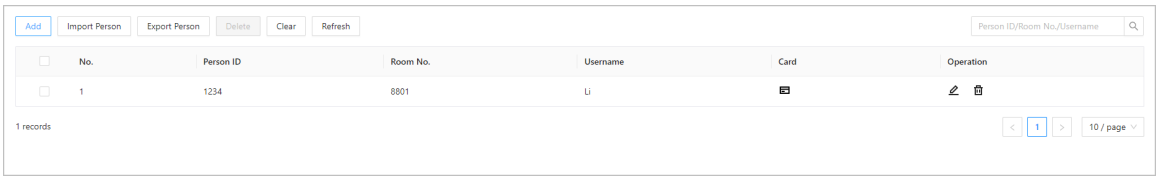
- ◇ : Reportar tarjeta perdida. Después de hacer clic en el icono, se convierte en .
- ◇ : edita la información de la tarjeta.
- ◇ : elimina la tarjeta agregada.

Figura 9-5 Tarjeta emitida



5. Haga clic**DE ACUERDO**.

Figura 9-6 Tarjeta agregada exitosamente



Operaciones relacionadas

- Hacer clic**Persona de exportación**y luego ingrese la contraseña de cifrado del archivo para exportar la información de la persona.
- Hacer clic**Persona de importación**y luego seleccione el archivo para importar la información de la persona.

10 configuraciones de red

Este capítulo presenta cómo configurar los parámetros de red.

10.1 TCP/IP

Debe configurar la información TCP/IP para conectar el VTO a la red.

Procedimiento

Paso 1 Inicie sesión en la página web de la VTO.

Paso 2 Seleccionar**Configuración de la red**>**TCP/IP**

Paso 3 . Configure los parámetros TCP/IP.

Figura 10-1 TCP/IP

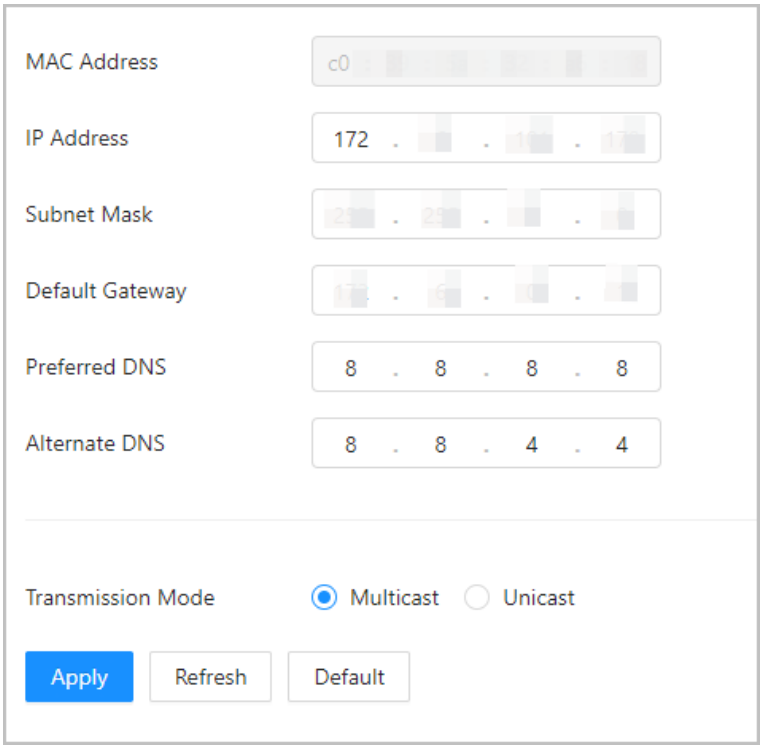


Tabla 10-1 Descripción del parámetro

Parámetro	Descripción
Dirección IP	Su dirección IP planificada para el VTO.
DNS preferido	Es 8.8.8.8 por defecto.
DNS alternativo	Es 8.8.4.4 por defecto.
Modo de transmisión	● Multidifusión. ● Unidifusión. Se prefiere la unidifusión cuando el conmutador no admite la función de multidifusión o cuando la conexión de red no es buena.

10.2 Puerto

Figura 10-2 Puerto

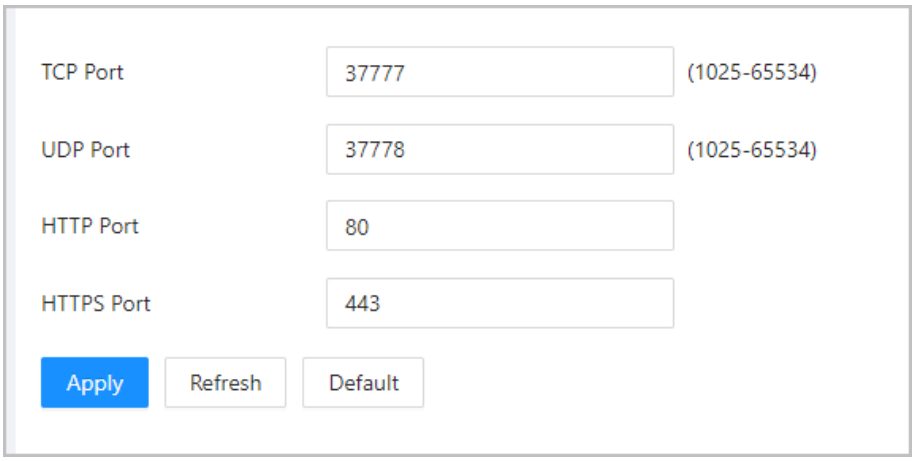


Tabla 10-2 Descripción del parámetro

Parámetro	Descripción
Puerto HTTP	Ahora puede ingresar http://dirección IP de VTO: Puerto HTTPS para iniciar sesión en VTO.
Puerto TCP/UDP	Se utiliza para acceder al VTO con dispositivos en otras redes.
Puerto HTTPS	Ahora puede ingresar https://dirección IP de VTO: puerto HTTPS para iniciar sesión en VTO.

10.3 Servidor SIP

Debe haber un servidor SIP en la red para que todos los VTO y VTH conectados se llamen entre sí. Puede utilizar un VTO u otros servidores como servidor SIP.

Procedimiento

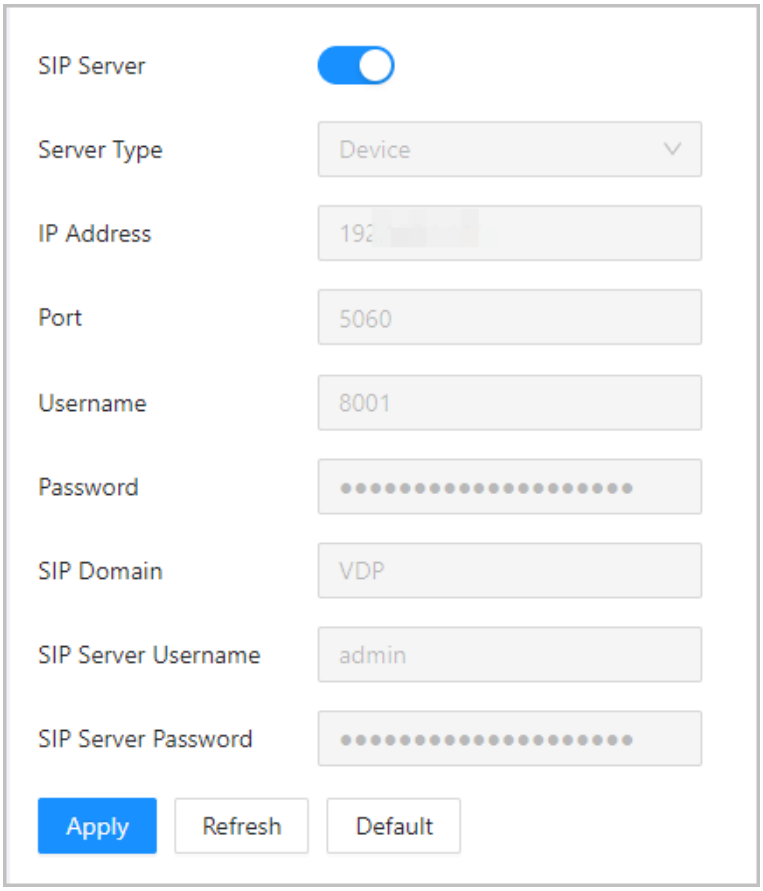
Paso 1 Seleccionar**Configuración de la red**>**Servidor SIP**.

Paso 2 Seleccione un tipo de servidor.

- El VTO en el que ha iniciado sesión como servidor SIP: seleccione el tipo SIP como **Dispositivo**y configure los parámetros para el VTO, y luego haga clic en junto a**Servidor SIP**.

Los parámetros se volverán grises después de habilitar el**Servidor SIP**función.

Figura 10-3 VTO actual como servidor SIP



- Si otro VTO funciona como servidor SIP: seleccione el tipo SIP como**Dispositivo**y configure los parámetros para que el VTO funcione como SIP.

Si el VTO en el que ha iniciado sesión no funciona como servidor SIP, no habilite **Servidor SIP**. De lo contrario, la conexión fallaría.

Figura 10-4 Otro VTO como servidor SIP

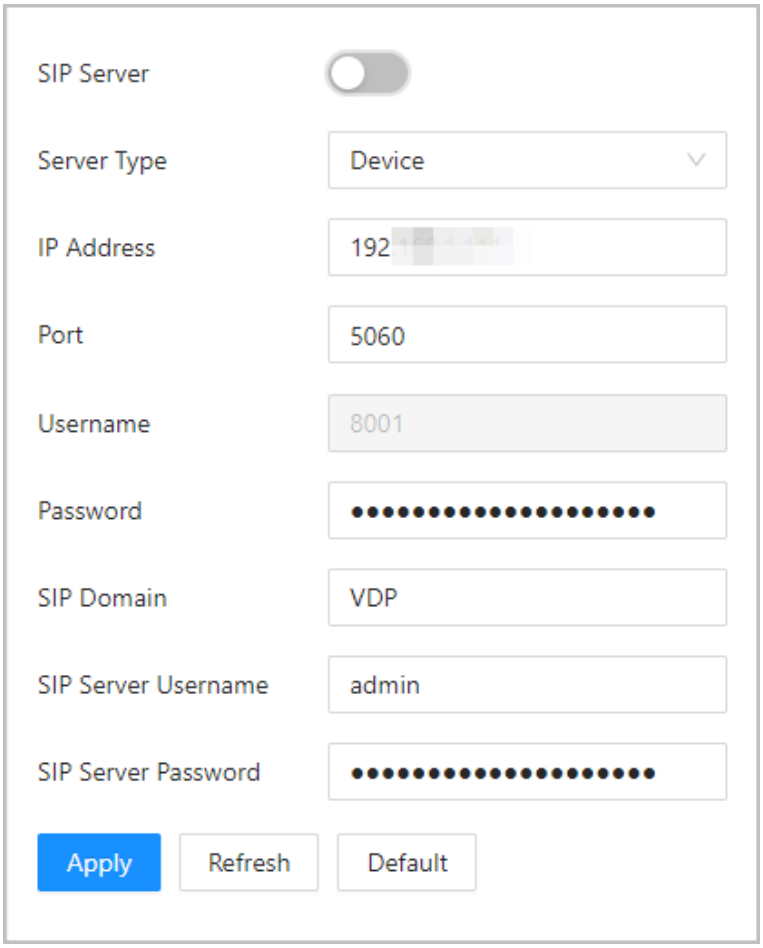


Tabla 10-3 Configuración del servidor SIP (VTO como servidor SIP)

Parámetro	Descripción
Dirección IP	Dirección IP planificada del VTO.
Puerto	5060 por defecto.
Nombre de usuario	Déjalo por defecto.
Contraseña	
Dominio SIP	
Nombre de usuario del servidor SIP	Nombre de usuario y contraseña utilizados para iniciar sesión en la página web del servidor SIP.
Contraseña del servidor SIP	

- La plataforma DSS funciona como servidor SIP: Establecer**Tipo de servidor**como**Servidor SIP privado**y luego configure los parámetros.

Figura 10-5 Servidor SIP privado

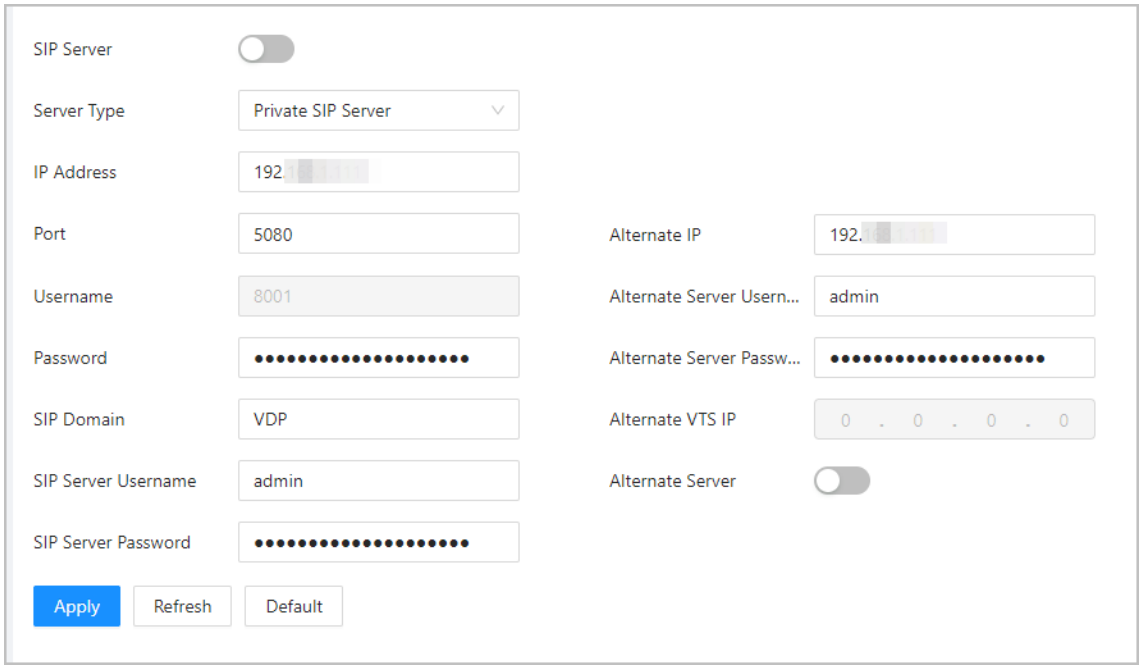


Tabla 10-4 Descripción del servidor SIP (plataforma como servidor SIP)

Parámetro	Descripción
Dirección IP	Dirección IP del servidor SIP.
Puerto	5080 de forma predeterminada cuando la plataforma funciona como servidor SIP.
Usuario Contraseña	Déjalo por defecto.
Dominio SIP	
Nombre de usuario/contraseña del servidor SIP	Se utiliza para iniciar sesión en el servidor SIP.
IP alternativa	El servidor alternativo se utilizará como servidor SIP cuando Express/DSS deje de responder. Le recomendamos configurar la dirección IP alternativa. ◇ Si habilitas**Servidor alternativo**, el VTO actual en el que ha iniciado sesión sirve como servidor alternativo. ◇ Si desea que otro VTO sirva como servidor alternativo, debe ingresar la dirección IP de ese VTO en el campo **IP alternativa**caja de texto. No actives**Servidor alternativo** en este caso.
Nombre de usuario/contraseña del servidor alternativo	Se utiliza para iniciar sesión en el servidor alternativo.
IP VTS alternativa	Dirección IP del VTS alternativo.
Servidor alternativo	Habilítelo para que pueda configurar la IP VTS alternativa.

Paso 3 Hacer clic**Aplicar**.

10.4 Segunda estación de confirmación en cascada

Se aplicó a la situación en la que la segunda estación de confirmación cae en cascada al VTH.

Requisitos previos

La versión de software del VTH debe ser V4.7 y posterior.

Procedimiento

Paso 1 Seleccionar**Configuración de la red**>**Servidor SIP**.

Paso 2 Configure la información de la segunda estación de confirmación en**Configuración del dispositivo local**>**Ajustes básicos**.

El tipo de dispositivo debe configurarse como**Segunda Estación de Confirmación**.

Paso 3 Colocar**Tipo de servidor**como**Dispositivo**y luego configure los parámetros. En esta situación en cascada, el VTH funciona como servidor SIP.

Figura 10-6 Configuración del servidor SIP (VTH como servidor SIP)

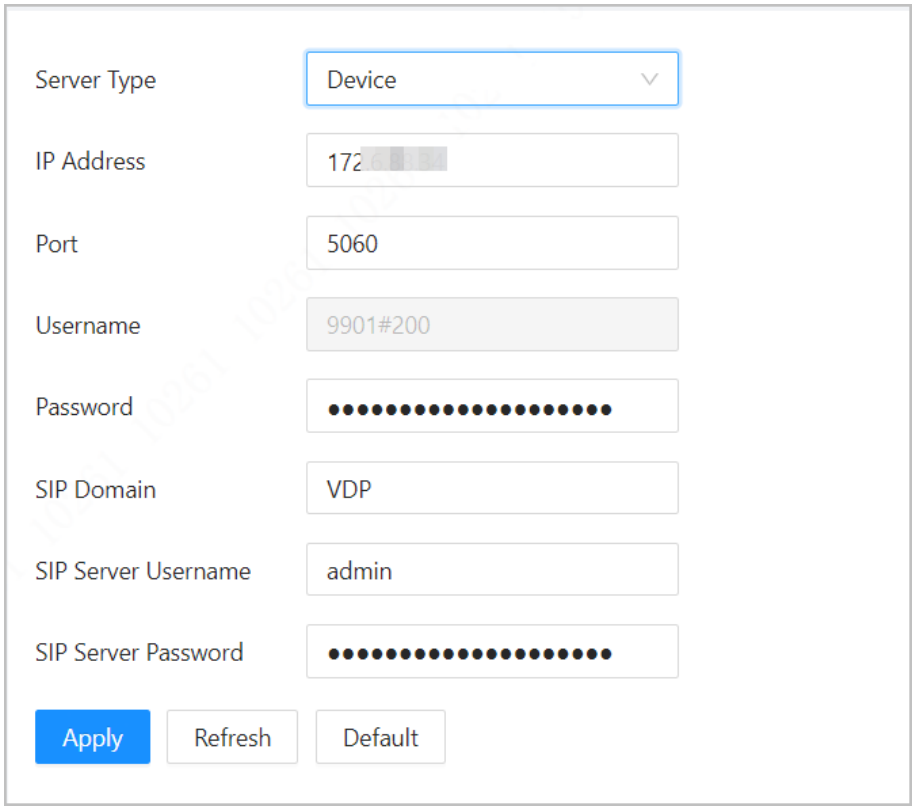


Tabla 10-5 Descripción de la configuración del servidor SIP (VTH como servidor SIP)

Parámetro	Descripción
Dirección IP	Su dirección IP planificada del VTH.
Puerto	5060 por defecto.
Nombre de usuario	Déjalo por defecto.
Contraseña	
Dominio SIP	

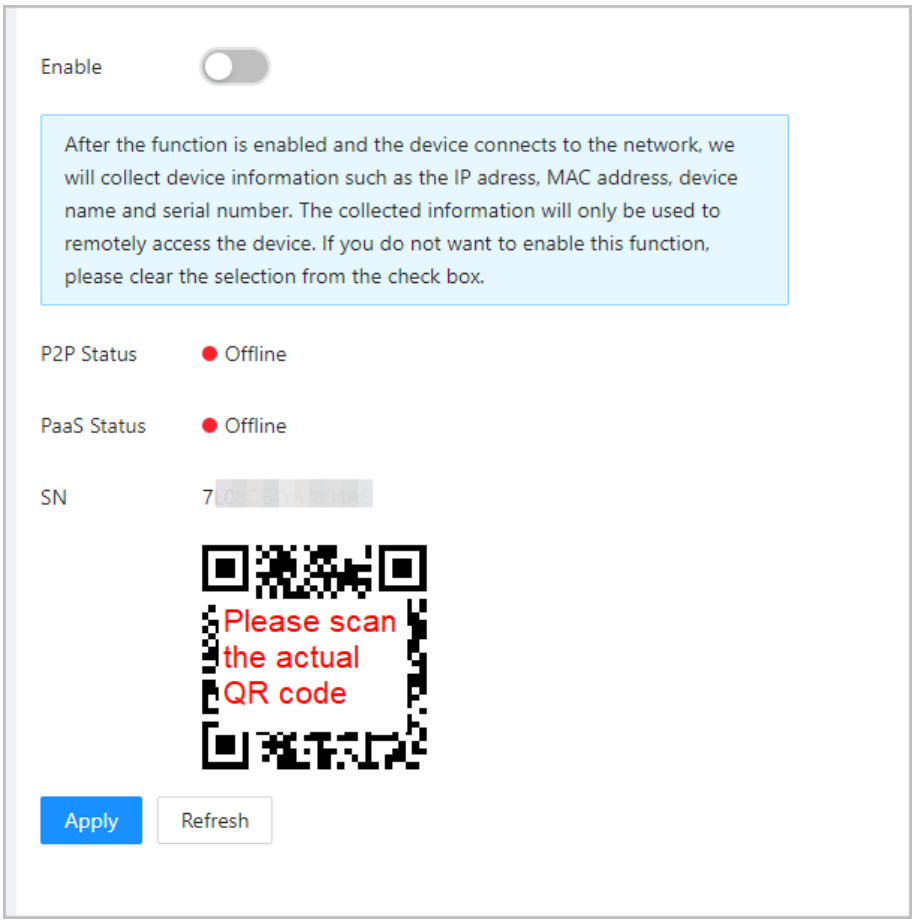
Parámetro	Descripción
Nombre de usuario del servidor SIP	Nombre de usuario y contraseña utilizados para iniciar sesión en el VTH que sirve como servidor SIP.
Contraseña del servidor SIP	

Etapa 4 Hacer clic**Aplicar**.

10.5 Servicio en la nube

Habilitar el**Servicio de almacenamiento en la nube**función, y luego puede escanear el código QR con su teléfono para agregar el VTO a la aplicación en su teléfono.

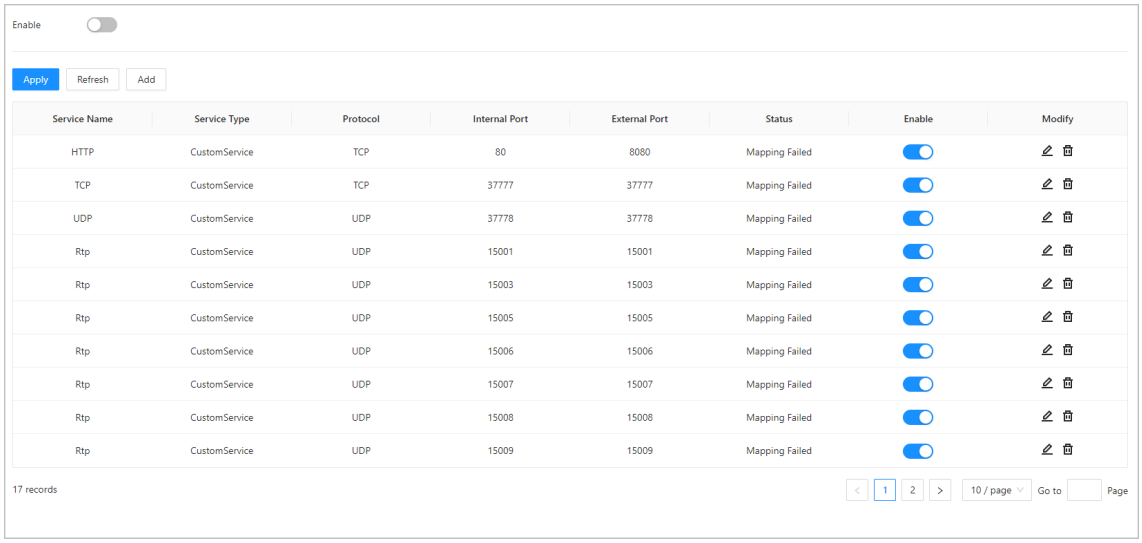
Figura 10-7 Servicio en la nube



10.6 UPnP

Cuando el VTO funciona como servidor SIP, puede configurar la función UPnP para permitir que los dispositivos WAN inicien sesión en el VTO.

Figura 10-8 UPnP



Preparación

- Habilite la función UPnP en el enrutador y luego configure una dirección IP WAN para el enrutador.
- Conecte el VTO al puerto LAN del enrutador.

10.6.1 Habilitación de servicios UPnP

Procedimiento

Paso 1 Seleccionar**Configuración de la red**>**UPnP**.

Paso 2 Habilite los servicios enumerados.

Paso 3 Seleccionar**Permitir**.

Etapa 4 Hacer clic**Ahorrar**.

10.6.2 Agregar servicios UPnP

Procedimiento

Paso 1 Seleccionar**Configuración de la red**>**UPnP**.

Paso 2 Hacer clic**Agregar**.

Paso 3 Configure los parámetros y luego haga clic en**DE ACUERDO**.

Figura 10-9 Agregar un servicio UPnP

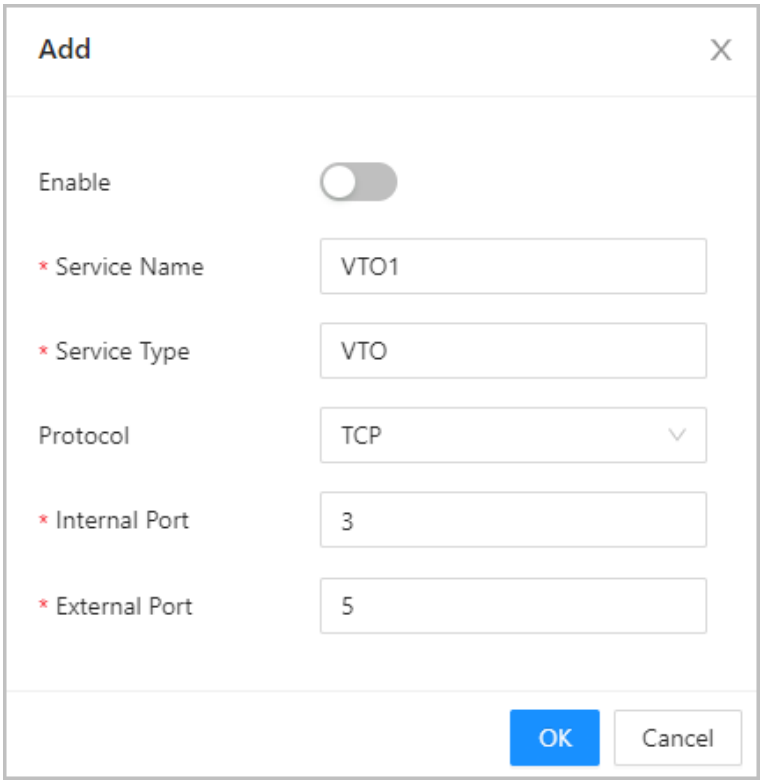


Tabla 10-6 Descripción del parámetro

Parámetro	Descripción
Nombre del Servicio	Ingrese el nombre y tipo del servicio.
Tipo de servicio	
Protocolo	Seleccionar**tcp**o**UDP**.
Puerto interno	Puerto interno del servicio. ● Si necesita configurar esta función para varios dispositivos, asegúrese de que los puertos no sean los mismos. ● El número de puerto que utilice no debe estar ocupado. ● El número de puerto interno y externo debe ser el mismo.
Puerto externo	Puerto externo del servicio. ● Si necesita configurar esta función para varios dispositivos, asegúrese de que los puertos no sean los mismos. ● El número de puerto que utilice no debe estar ocupado. ● El número de puerto interno y externo debe ser el mismo.

10.7 Wi-Fi

Si el VTO admite la función Wi-Fi, configure los parámetros aquí.

Procedimiento

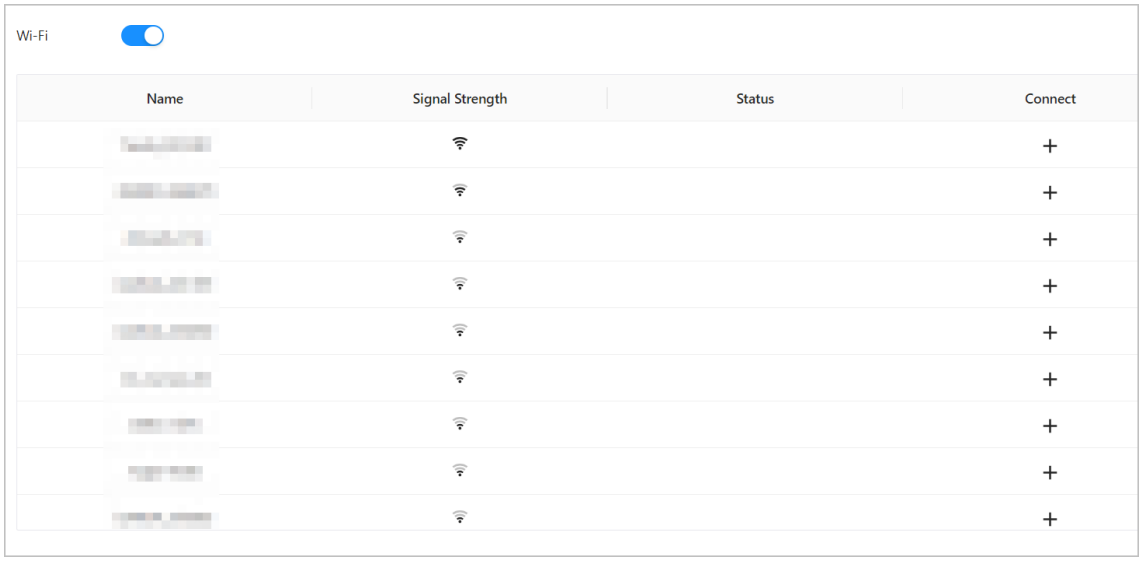
Paso 1 Inicie sesión en la página web de la VTO.

Paso 2 Seleccionar**Configuración de la red**>**Wifi**.

Paso 3 Selecciona el**Wifi**estatus como**En**.

Se muestran todas las redes disponibles.

Figura 10-10 Wi-Fi



Etapa 4 Hacer clic**+**del Wi-Fi que eligió, ingrese la contraseña del mismo y luego conéctese a la red.

10.8 Servicios Básicos

Configurar funciones que involucran la seguridad del dispositivo.

Procedimiento

Paso 1 Seleccionar**Configuración de la red**>**Servicios basicos**. Habilite las

Paso 2 funciones de seguridad según sus necesidades.

Figura 10-11 Servicios básicos

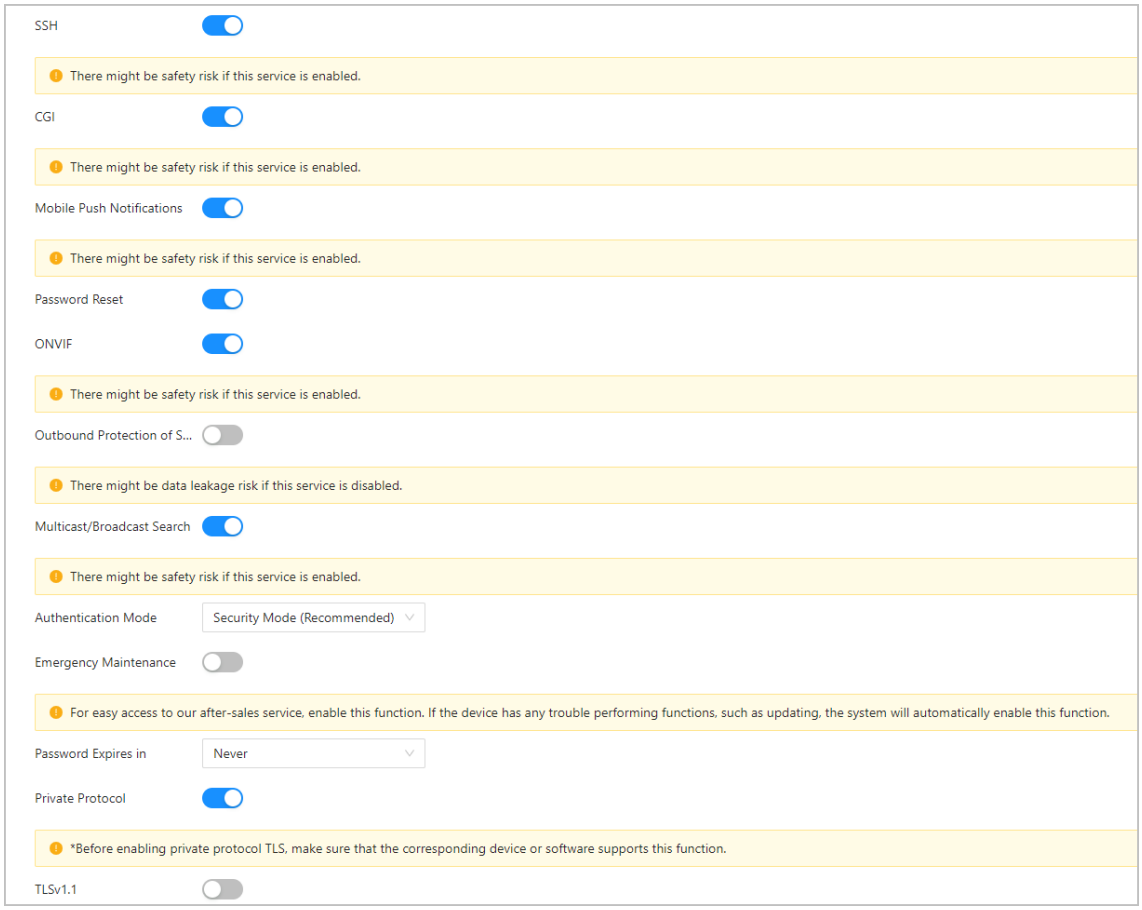


Tabla 10-7 Descripción del parámetro de seguridad

Parámetro	Descripción
SSH	Una alternativa segura a los protocolos remotos no seguros. Le recomendamos que lo desactive porque podría haber riesgos para la seguridad si este servicio está habilitado.
CGI	El uso del comando CGI. Le recomendamos que lo apague. De lo contrario, la VTO podría quedar expuesta a riesgos de seguridad y fuga de datos.
Empuje móvil Notificación	Envía información a la aplicación del teléfono. Le recomendamos que lo apague si no necesita esta función. De lo contrario, la VTO podría quedar expuesta a riesgos de seguridad y fuga de datos.
Restablecimiento de contraseña	Si está desactivado, no podrá restablecer la contraseña.

Parámetro	Descripción
ONVIF	Permita que terceros extraigan la transmisión de video del VTO a través del protocolo ONVIF. Recomendamos apagarlo. De lo contrario, la VTO podría quedar expuesta a riesgos de seguridad y fuga de datos.
Servicio saliente Protección de la información	Proteja sus contraseñas. Le recomendamos que lo encienda. De lo contrario, la VTO podría quedar expuesta a riesgos de seguridad y fuga de datos.
Multidifusión/difusión Buscar	Habilítelo para que otros dispositivos encuentren el VTO. Le recomendamos que lo apague. De lo contrario, la VTO podría quedar expuesta a riesgos de seguridad y fuga de datos.
modo de autenticación	● **modo de seguridad**(recomendado): Admite el inicio de sesión con autenticación implícita. ● **Modo de compatibilidad**:Utilice el antiguo método de inicio de sesión. Le recomendamos utilizar el modo de seguridad. El modo compatible puede exponer al VTO a riesgos de seguridad y fuga de datos.
Emergencia Mantenimiento	Para acceder fácilmente a nuestro servicio postventa, habilite esta función. Si el dispositivo tiene problemas para realizar funciones, como la actualización, el sistema habilitará automáticamente esta función.
La contraseña caduca en	● Seleccione un período de vencimiento de**30**días,**60**días,**90**días,**180**días, **Costumbre**y**Nunca**. ● Si seleccionas**Costumbre**, debe configurar un día de vencimiento entre 0 y 180.
Protocolo privado	Antes de habilitar el protocolo privado TLS, asegúrese de que el dispositivo o software correspondiente admita esta función.
TLSv1.1	Le recomendamos que lo desactive porque podría haber riesgos para la seguridad si este servicio está habilitado.

Paso 3 Hacer clic**Aplicar**.

11 Gestión de registros

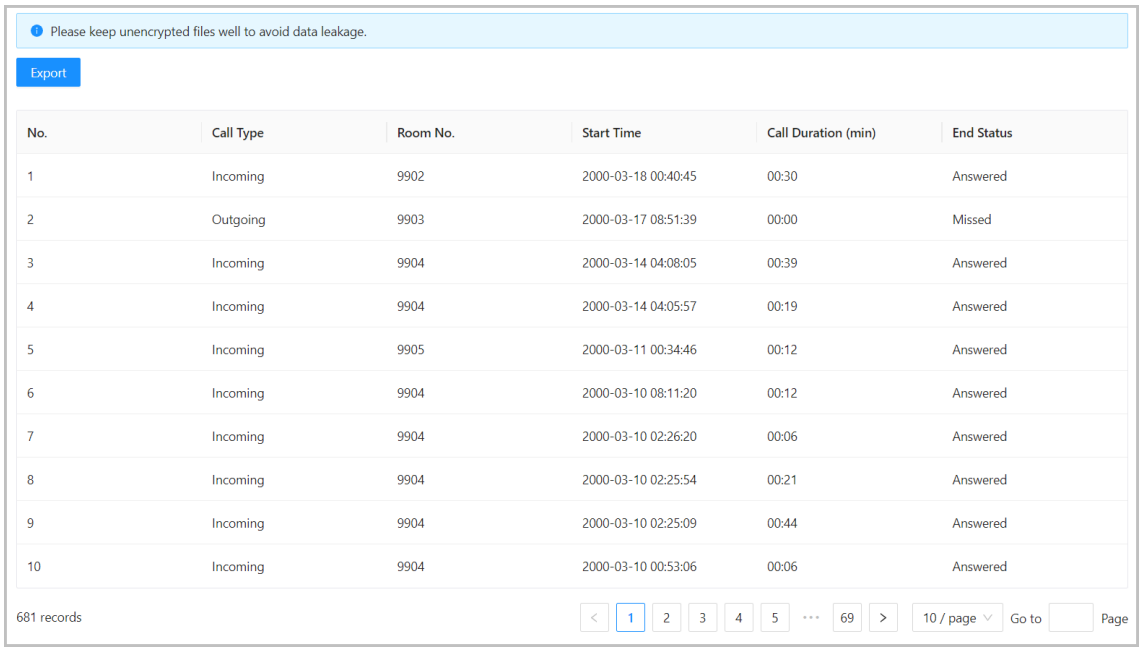
Seleccionar**Registro**. Puede buscar diferentes registros y exportarlos a su computadora local.

Si el almacenamiento está lleno, se sobrescribirán los registros más antiguos. Haga una copia de seguridad de los registros a tiempo.

11.1 Historial de llamadas

Seleccionar**Registro**>**Historial de llamadas**.

Figura 11-1 Historial de llamadas



Please keep unencrypted files well to avoid data leakage.

Export

No.	Call Type	Room No.	Start Time	Call Duration (min)	End Status
1	Incoming	9902	2000-03-18 00:40:45	00:30	Answered
2	Outgoing	9903	2000-03-17 08:51:39	00:00	Missed
3	Incoming	9904	2000-03-14 04:08:05	00:39	Answered
4	Incoming	9904	2000-03-14 04:05:57	00:19	Answered
5	Incoming	9905	2000-03-11 00:34:46	00:12	Answered
6	Incoming	9904	2000-03-10 08:11:20	00:12	Answered
7	Incoming	9904	2000-03-10 02:26:20	00:06	Answered
8	Incoming	9904	2000-03-10 02:25:54	00:21	Answered
9	Incoming	9904	2000-03-10 02:25:09	00:44	Answered
10	Incoming	9904	2000-03-10 00:53:06	00:06	Answered

681 records

< 1 2 3 4 5 ··· 69 > 10 / page Go to Page

11.2 Registros de alarmas

Seleccionar**Registro**>**Registros de alarma**.

Figura 11-2 Alarma

Please keep unencrypted files well to avoid data leakage.

Export

No.	Room No.	Event	Channel	Start Time
1	8001	Tamper	1	2023-07-11 02:00:53
2	8001	Tamper	1	2023-07-07 10:07:18
3	8001	Tamper	1	2023-07-06 22:16:19
4	8001	Tamper	1	2023-07-06 22:09:52
5	8001	Tamper	1	2023-07-04 02:00:49
6	8001	Tamper	1	2023-06-29 16:29:49
7	8001	Tamper	1	2023-06-29 16:26:59
8	8001	Tamper	1	2023-06-29 15:22:09
9	8001	Tamper	1	2023-06-29 15:22:08
10	8001	Tamper	1	2023-06-27 14:07:57

12 records < 1 2 > 10 / page Go to Page

11.3 Desbloquear registros

Seleccionar**Registro**>**Desbloquear registros**.

Figura 11-3 Desbloquear

Please keep unencrypted files well to avoid data leakage.

Export

No.	Unlock Method	VTO ID	Person ID	Room No.	Username	Card	Unlock Results	Unlock Time
1	Remote Unlock	8001		9901			Succeed	2023-07-06 20:59:...
2	Remote Unlock	8001		9901			Succeed	2023-06-29 15:17:...

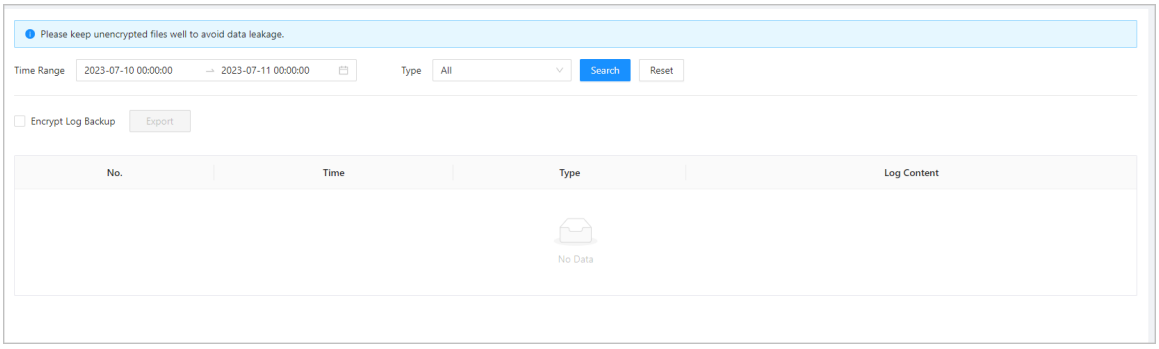
2 records < 1 > 10 / page

11.4 Registro

Seleccionar**Registro**>**Registro**.

Seleccione el rango de tiempo y el tipo, y luego podrá ver toda la información del registro.

Figura 11-4 Registro

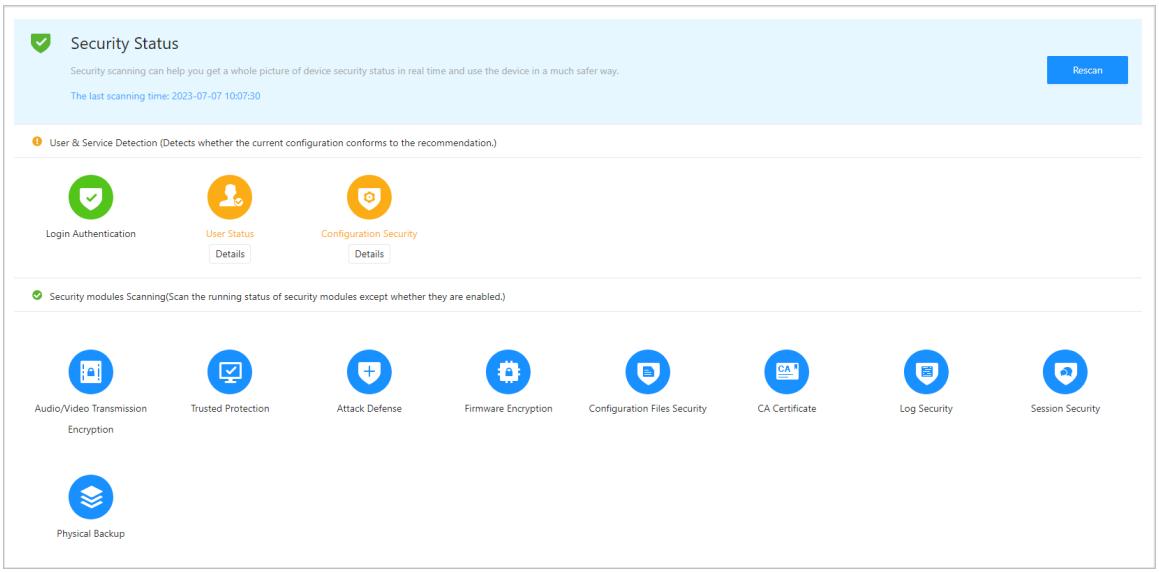


12 Gestión de Seguridad

12.1 Estado de seguridad

En la página de inicio, haga clic en y luego seleccione**Estado de seguridad**.

Figura 12-1 Estado de seguridad



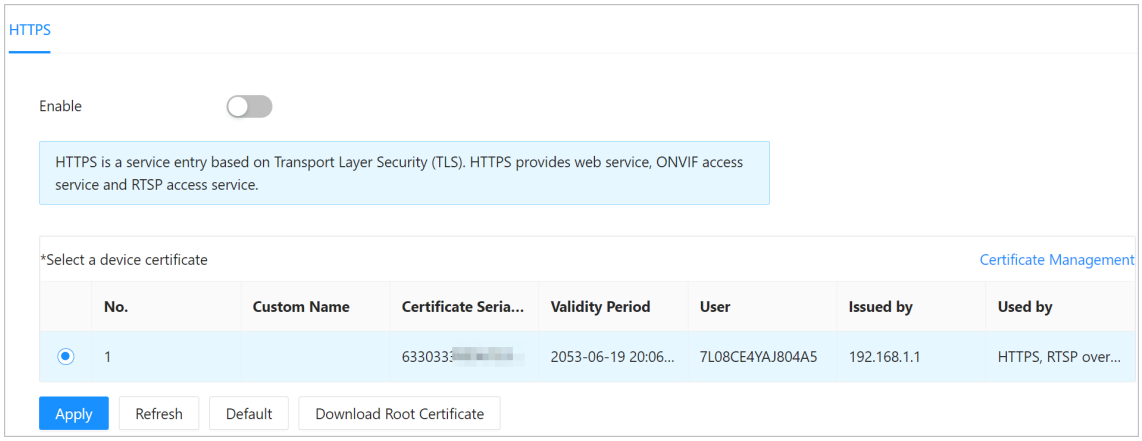
12.2 Servicio del sistema

Procedimiento

Paso 1 En la página de inicio, haga clic en y luego seleccione**Servicio del sistema**.

Paso 2 Seleccione un certificado de dispositivo y luego habilite la función HTTPS.

Figura 12-2 Servicio del sistema



Paso 3 Hacer clic**Aplicar**.

12.3 Defensa de ataque

12.3.1 Cortafuegos

Puede habilitar diferentes tipos de firewall para controlar el acceso de red al VTO.

Procedimiento

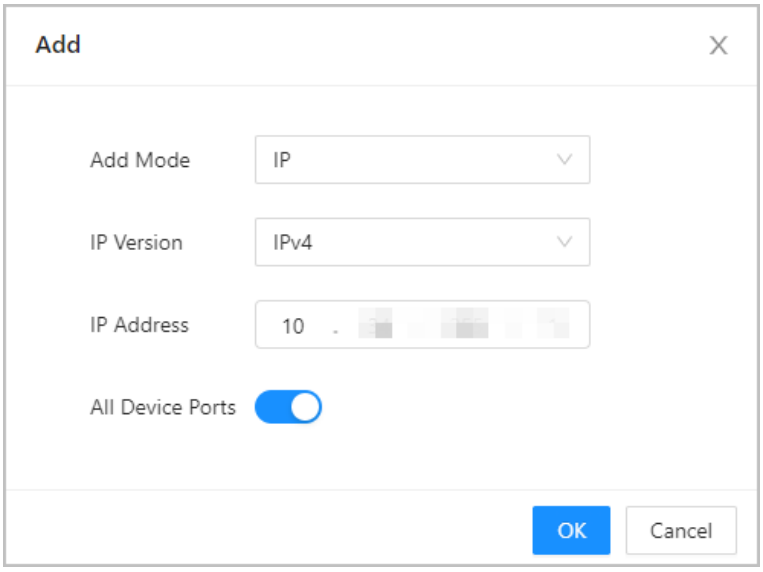
Paso 1 En la página de inicio, haga clic en y luego seleccione**Defensa de ataque**>**Cortafuegos**.

Paso 2 Selecciona el**Modo**Cómo sea**Lista de permitidos**o**Lista de bloqueos**.

- Lista de permitidos: dispositivos a los que se les ha concedido acceso.
- Lista de bloqueo: Dispositivos a los que se les ha prohibido el acceso.

Paso 3 Hacer clic**Agregar**para agregar la dirección IP a la lista de permitidos o de bloqueo.

Figura 12-3 Agregar

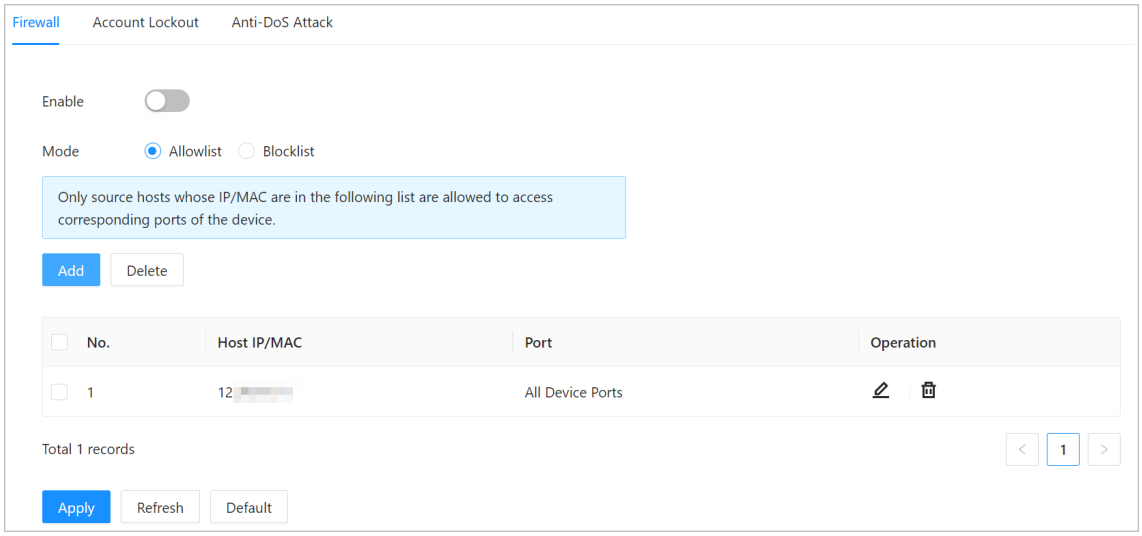


Etapa 4 Hacer clic**DE ACUERDO**.

Paso 5 Hacer clic junto a**Permitir**.

Paso 6 Seleccione una dirección IP agregada para la lista de permitidos o de bloqueo y luego haga clic en**Aplicar**.

Figura 12-4 Aplicar



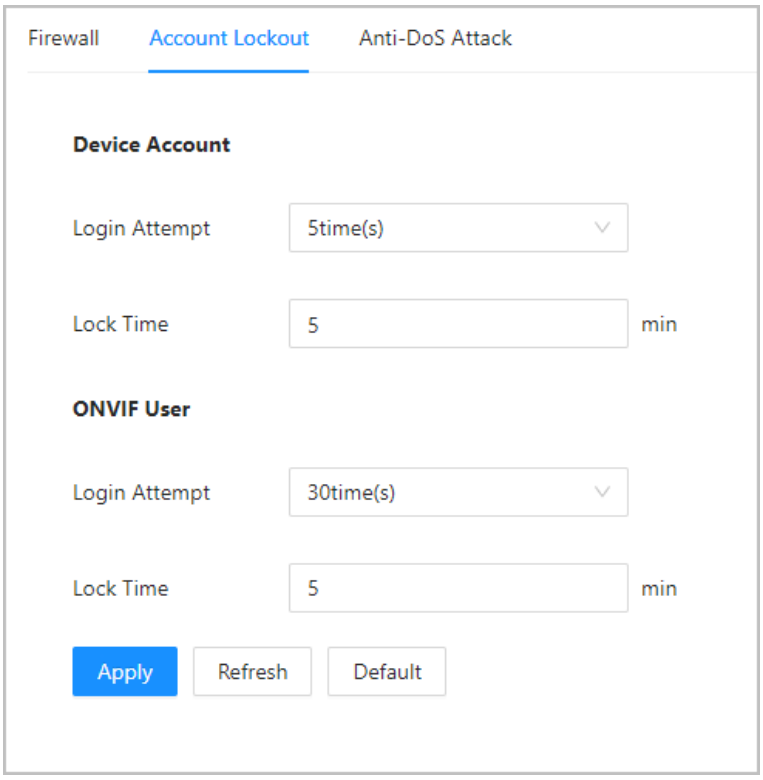
12.3.2 Bloqueo de cuenta

Procedimiento

Paso 1 En la página de inicio, haga clic en y luego seleccione**Defensa de ataque**>**Bloqueo de cuenta**.

Paso 2 Configure los intentos de inicio de sesión y el tiempo de bloqueo.

Figura 12-5 Bloqueo de cuenta



Paso 3 Hacer clic**Aplicar**.

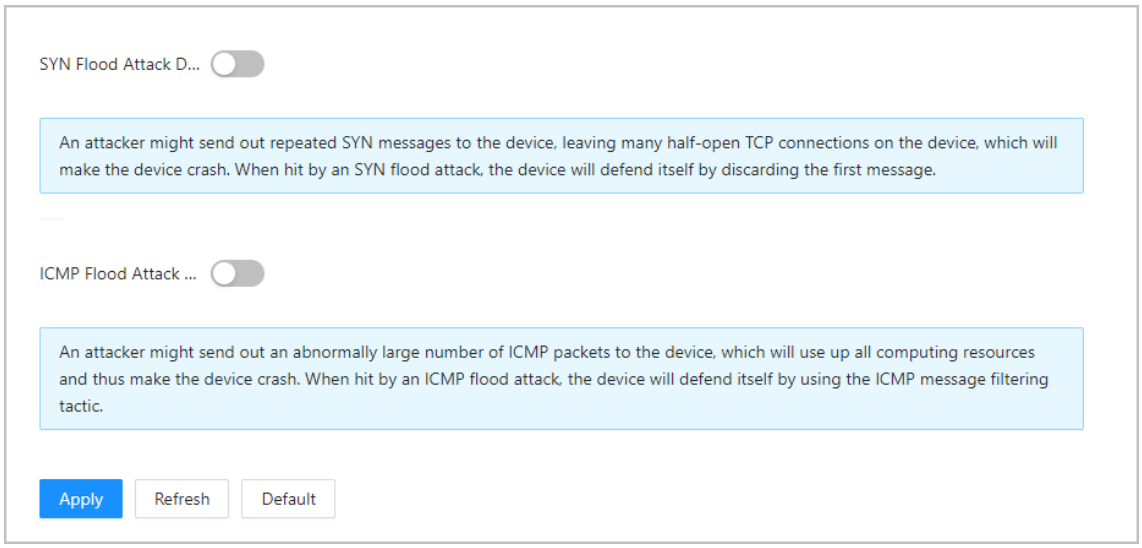
12.3.3 Ataque anti-DoS

Procedimiento

Paso 1 En la página de inicio, haga clic en y luego seleccione**Defensa de ataque**>**Ataque anti-DoS**.

Paso 2 Activar o desactivar la**Defensa contra ataques de inundación SYN**o**Defensa contra ataques de inundaciones ICMP** función.

Figura 12-6 Ataque Anti-DoS



Paso 3 Hacer clic**Aplicar**.

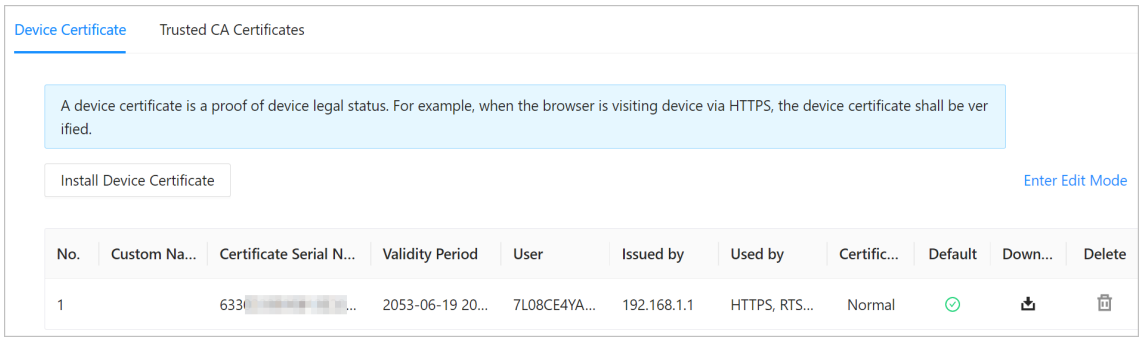
12.4 Certificado de CA

Procedimiento

Paso 1 En la página de inicio, haga clic en y luego seleccione**Certificado de CA**.

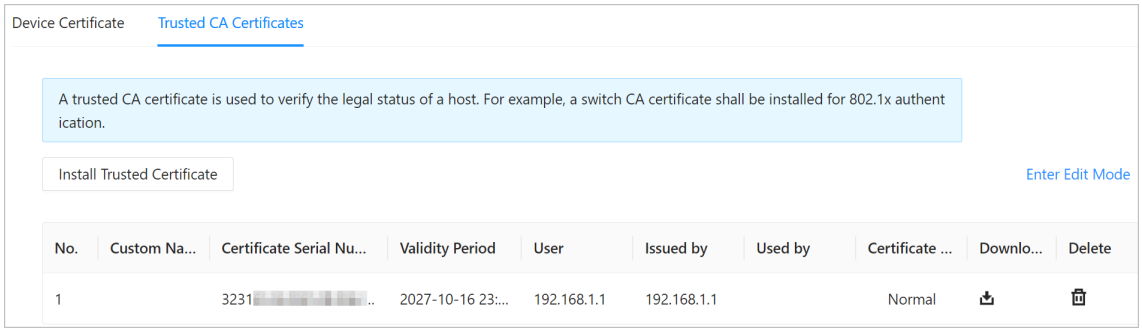
- Certificado de dispositivo

Figura 12-7 Certificado de dispositivo



- Certificados de CA confiables

Figura 12-8 Certificados de CA confiables



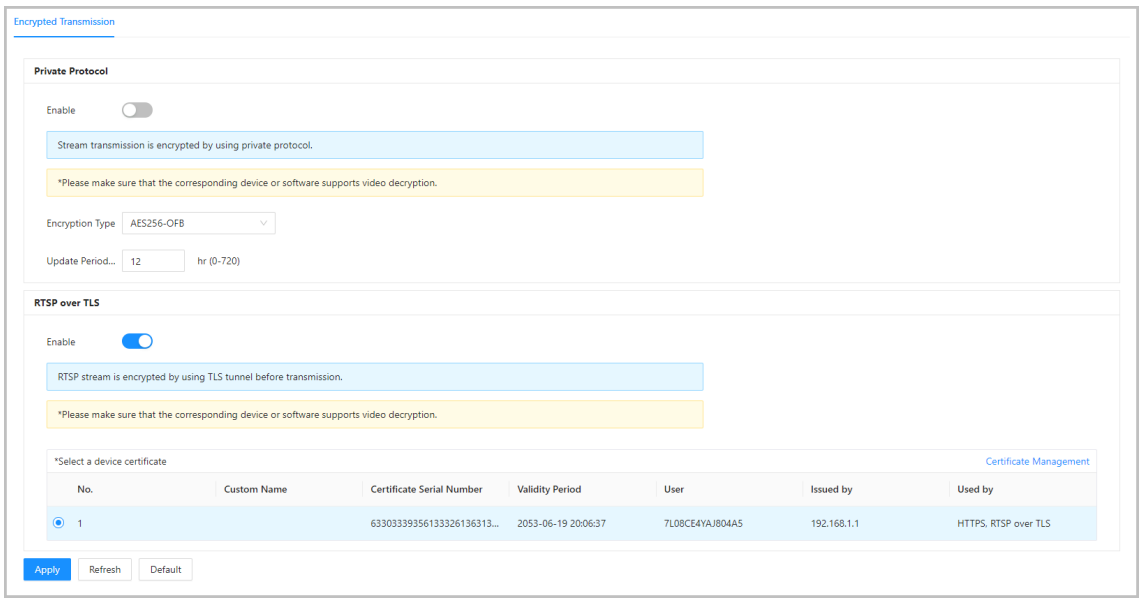
12.5 Cifrado de vídeo

Procedimiento

Paso 1 En la página de inicio, haga clic en y luego seleccione**Cifrado de vídeo**.

Paso 2 Configurar**Protocolo privado**y**RTSP sobre TLS**parámetros.

Figura 12-9 Cifrado de vídeo



Paso 3 Hacer clic**Aplicar**.

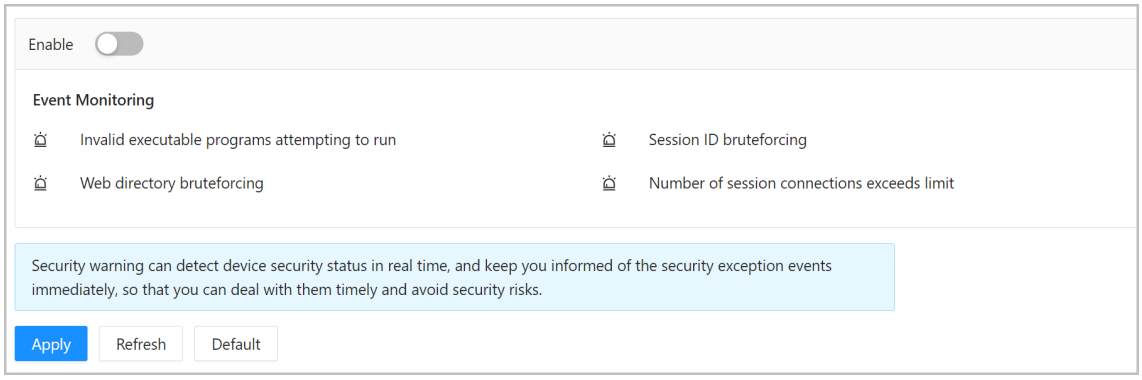
12.6 Advertencia de seguridad

Procedimiento

Paso 1 En la página de inicio, haga clic en y luego seleccione**Advertencia de seguridad**.

Paso 2 Habilite la función de monitoreo de eventos y luego haga clic en**Aplicar**.

Figura 12-10 Advertencia de seguridad



Configuración del modelo de 13 botones

El modelo de botón se puede conectar al VTH para que funcione como botón de entrada de alarma. Presione el botón en el panel frontal del modelo y luego el VTH recibe una señal de alarma.

13.1 Conexión de cables

Conecte el puerto KEY del modelo de botón a cualquiera de los puertos de entrada de alarma del monitor interior (VTH) con un hilo de cable.

Figura 13-1 Modelo de botón

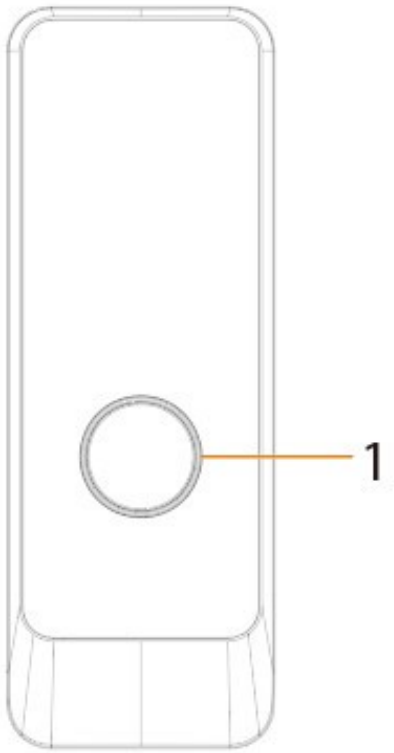
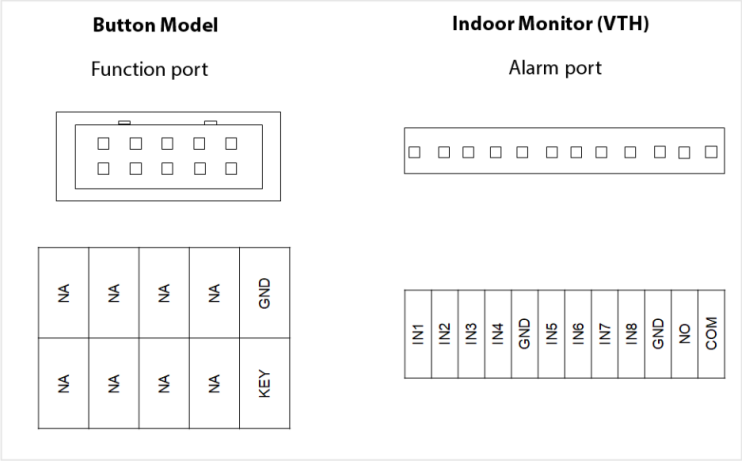


Tabla 13-1 Componente

No.	Nombre	Función
1	presiona el botón	El modelo de botón se puede conectar al VTH. Presione el botón en el modelo y el VTH recibe una señal de alarma.

Figura 13-2 Conexión de cables



13.2 Configuración VTH

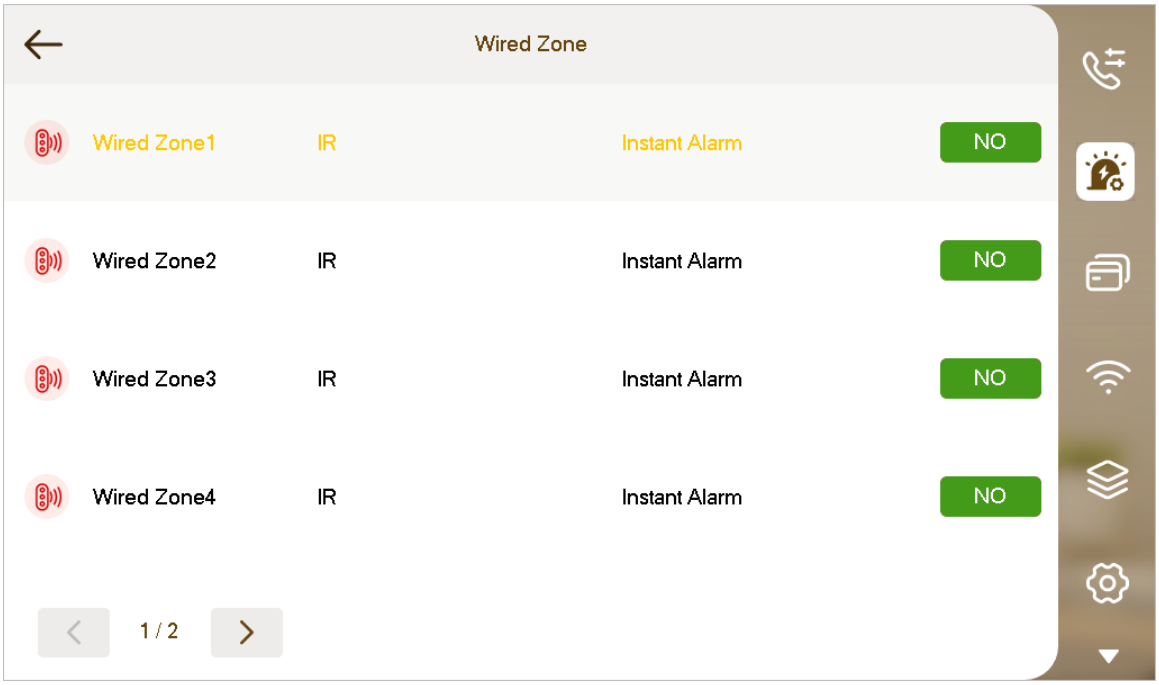
Después de completar la conexión del cable, debe configurar el**tipo de zona cableada**como**Timbre de la puerta**en el VTH para recibir señales de alarma una vez que presione el botón modelo.

Procedimiento

Paso 1 Encienda el VTH.

Paso 2 Seleccionar**Configuración**>**Alarma**>**Zona cableada**en el VTH.

Figura 13-3 Configuración de zona cableada



Paso 3 Selecciona el**Tipo**como**Timbre de la puerta**y configurar el resto de parámetros.

Tabla 13-2 Descripción del parámetro

Parámetro	Descripción
Área	El número no se puede modificar.
NO C	Seleccione NO (normalmente abierto) o NC (normalmente cerrado) según el tipo de detector. Debe ser el mismo que el tipo de detector.
Tipo	Seleccione el tipo correspondiente según el tipo de detector.
Estado	● **Alarma instantánea**:Después de armado, si se activa una alarma, el dispositivo emite una sirena de inmediato y entra en estado de alarma. ● **Alarma de retraso**:Después de armado, si se activa una alarma, el dispositivo ingresa al estado de alarma después de un tiempo específico, durante el cual puede desarmar y cancelar la alarma. ● **Derivación**:La alarma no se activará en el área. Después de desarmar, esta área volverá a su estado de funcionamiento normal. ● **Eliminar**:El área no es válida durante el armado/desarmado. ● **24 horas**:La alarma se activará todo el tiempo en el área independientemente de si se arma o desarma. una zona en**Eliminar**El estado no se puede pasar por alto.
Introducir retraso	Después de ingresar al retraso, cuando el área armada activa una alarma, ingresar al área armada desde el área no armada dentro del período de tiempo de retraso no generará una alarma de vinculación. Se producirá una alarma de enlace si finaliza el tiempo de retardo y no se desarma.
Retardo de salida	Después del brazo,**Alarma de retraso**El área entrará en estado armado al final del**Retardo de salida**. Si varias áreas configuran el retraso de salida, el mensaje en pantalla se ajustará al tiempo de retraso máximo.

El retraso sólo es válido para las áreas de **Alarma de retraso**.

Apéndice 1 Recomendaciones de ciberseguridad

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

1.**Utilice contraseñas seguras**

Consulte las siguientes sugerencias para establecer contraseñas:

- La longitud no debe ser inferior a 8 caracteres.
- Incluya al menos dos tipos de personajes; Los tipos de caracteres incluyen letras mayúsculas y minúsculas, números y símbolos.
- No incluya 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 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 "es bueno tener" para mejorar la seguridad de la red de su dispositivo:

1.Protección física

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

2.**Cambie las contraseñas con regularidad**

Le sugerimos que cambie las contraseñas con regularidad para reducir el riesgo de que las adivinen o las descifren.

3.**Establecer y actualizar contraseñas Restablecer información oportunamente**

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 sobre protección de contraseña. Si la información cambia, modifíquela a tiempo. Al configurar preguntas de protección con contraseña, se sugiere no utilizar aquellas que puedan adivinarse fácilmente.

4.**Habilitar bloqueo de cuenta**

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

5.**Cambiar HTTP predeterminado y otros puertos de servicio**

Le sugerimos que cambie 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 habilitar 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 ARP.

8.**Asignar cuentas y privilegios de forma razonable**

De acuerdo con los requisitos comerciales y de administración, agregue usuarios de manera razonable 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 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 cifrado WPA2-PSK y configure contraseñas seguras.

10. **Transmisión cifrada de audio y vídeo**

Si el contenido de sus datos de audio y video es muy importante o confidencial, le recomendamos que utilice la función de transmisión cifrada 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 la transmisión.

11. **Auditoría segura**

- Verifique los usuarios en línea: le sugerimos que verifique a los usuarios en línea con regularidad para ver si el dispositivo inició sesión sin autorización.
- Verifique 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 habilitar la función de registro de red para garantizar que los registros críticos estén sincronizados 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 asignación de puertos del enrutador para evitar el acceso directo a los dispositivos de la intranet desde la red externa.
- La red debe dividirse y aislarse según las necesidades reales de la red. Si no hay requisitos de comunicación entre dos subredes, se sugiere utilizar VLAN, red GAP y otras tecnologías para dividir la red, a fin de lograr el efecto de aislamiento de la red.
- Establezca el sistema de autenticación de acceso 802.1x para reducir el riesgo de acceso no autorizado a redes privadas.
- Habilite la función de filtrado de direcciones IP/MAC para limitar el rango de hosts permitidos para acceder al dispositivo.