VTS digitales

Manual de usuario



V1.0.2

Prefacio

Este manual presenta las configuraciones en el VTS local y la página web. Lea atentamente antes de utilizar el VTS 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	Tiempo de liberación
V1.0.2	Servicios básicos revisados y configuración del dispositivo.	enero 2024
V1.0.1	Parámetros avanzados revisados.	junio 2023
V1.0.0	Primer lanzamiento.	noviembre 2022

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 de usuario en papel, utilice nuestro CD-ROM, escanee el código QR o

visita 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.

requerimientos de instalación

WARNING

- No conecte el adaptador de corriente al dispositivo mientras el adaptador esté encendido.
- No conecte el dispositivo a dos o más tipos de fuentes de alimentación para evitar daños al dispositivo.
- Siga los requisitos eléctricos para alimentar el dispositivo. A continuación se
  - detallan los requisitos para seleccionar un adaptador de corriente.
    - La fuente de alimentación debe cumplir con los requisitos de las normas IEC 60950-1 e IEC 62368-1.
    - El voltaje debe cumplir con los requisitos SELV (voltaje extra bajo de seguridad) y no exceder los estándares ES-1.
    - Cuando la potencia del dispositivo no supera los 100 W, la fuente de alimentación debe cumplir con los requisitos de LPS y no ser superior a PS2.
  - Recomendamos utilizar el adaptador de corriente suministrado con el dispositivo.
  - Al seleccionar el adaptador de corriente, los requisitos de suministro de energía (como el voltaje nominal) están sujetos a la etiqueta del dispositivo.

- 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.
- 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.

Requisitos de operación

DANGER

Precauciones con la batería

Medidas preventivas (incluidas, entre otras):

- No transporte, almacene ni utilice las baterías en altitudes elevadas con baja presión ni en entornos con temperaturas extremadamente altas y bajas.
- No arroje las baterías al fuego ni a un horno caliente, ni las aplaste o corte mecánicamente para evitar una explosión.

- No deje las baterías en ambientes con temperaturas extremadamente altas para evitar explosiones y fugas de líquidos o gases inflamables.
- No exponga las baterías a una presión de aire extremadamente baja para evitar explosiones y fugas de líquidos o gases inflamables.



- 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.

Tabla de contenido

Prefacio..... I Medidas de seguridad y advertencias importantes.....III

1 Estructura del dispositivo..... 1

1.1 Panel frontal..... 1

1.2 Panel trasero.....3

2 Inicializando VTS..... 5

2.1 Inicialización a través del dispositivo local..... 5

2.2 Inicialización a través de la página web..... 5

3 escenas de construcción.....7

3.1 Operaciones en el dispositivo local..... 7

3.1.1 Pantalla Local..... 7

3.1.2 Configuración de los parámetros de visualización.....8

3.1.3 Configuración de los parámetros de sonido..... 8

3.1.4 Configuración de los parámetros del intercomunicador..... 9

3.1.5 Configuración de los parámetros avanzados..... 10

3.1.6 Restablecer contraseña.....11

3.1.7 Configuración del proyecto..... 12

3.1.8 Puesta en servicio..... 18

3.2 Operaciones en la página web..... 23

3.2.1 Iniciar sesión en la página web..... 23

3.2.2 Restablecer contraseña.....24

3.2.3 Introducción a la página de inicio.....25

3.2.4 Configuración de la red..... 26

3.2.5 Gestión del sistema..... 30

3.2.6 Gestión de dispositivos..... 39

3.2.7 Registro..... 41

3.2.8 Seguridad..... 42

4 Escenas Industriales.....53

4.1 Operaciones en el dispositivo local..... 53

4.1.1 Pantalla Local..... 53

4.1.2 Configuración de los parámetros del intercomunicador..... 54

4.1.3 Configuración de los parámetros avanzados..... 54

4.1.4 Configuración del proyecto..... 55

4.1.5 Puesta en servicio..... 56

4.2 Operaciones en la página web..... 61

4.2.1 Configuración de la función del dispositivo..... 62

4.2.2 Configurar el servidor SIP..... 62

4.2.3 Configuración de FTP..... 63

4.2.4 Configuración del dispositivo..... 64

Apéndice 1 Recomendaciones de ciberseguridad..... 69

1 estructura del dispositivo

1.1 Panel frontal

Figura 1-1 Panel frontal

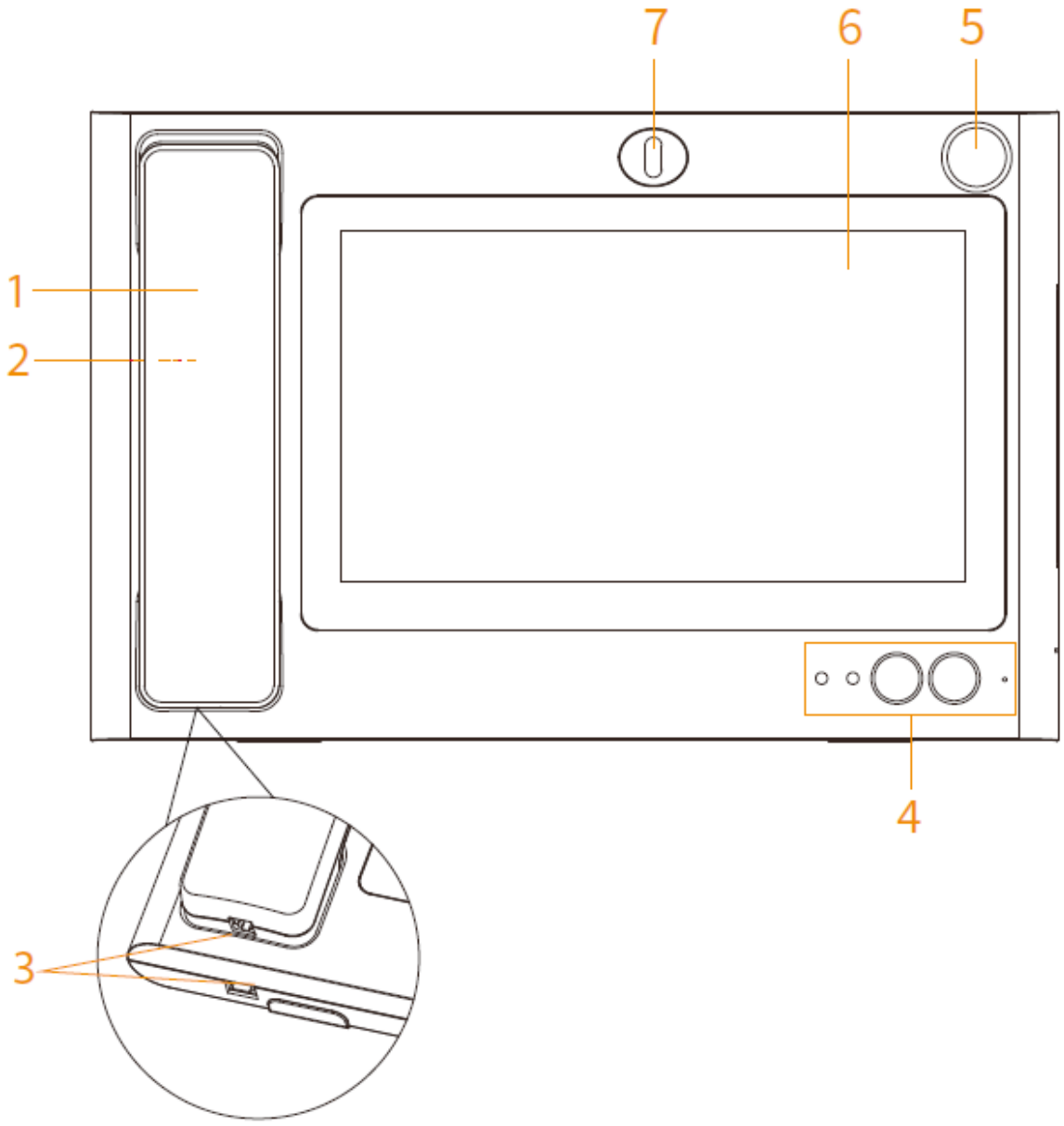


Tabla 1-1 Descripción del panel frontal

No.	Nombre	Descripción
1	micrófono	Si levanta el MIC, el audio y la captación se convierten en MIC.
2	Vocero	Emite sonido.
3	Puerto RJ-11	Conecta VTS y MIC mediante el cable telefónico.

No.	Nombre	Descripción
4	Indicador/Botón	De izquierda a derecha: ● Indicador de encendido ◇ Encendido: el dispositivo está encendido. ◇ Apagado: El dispositivo no está conectado a la fuente de alimentación. ● Indicador de información ◇ Encendido: hay una llamada perdida. ◇ Apagado: La llamada perdida ha sido procesada o no hay ninguna llamada perdida.  En el escenario industrial, si el indicador está encendido, indica que el dispositivo tiene registros de alarma no leídos. ● Botón de desbloqueo Cuando realiza llamadas, mira videos o habla con otras personas a través del VTS, presione el botón de desbloqueo; puede abrir de forma remota la puerta de algunos dispositivos frontales que admiten la función de desbloqueo. ● Botón manos libres Se utiliza para responder llamadas entrantes. Puede seleccionar el modo manos libres o el modo auricular. ● Micrófono incorporado Sonido de las entradas.
5	Cuello de cisne Puerto de micrófono	Se conecta a un micrófono de cuello de cisne.  El puerto está disponible en modelos selectos.
6	Pantalla y toque	Pantalla y zona táctil.
7	Cámara	Sirve para hablar con otro VTS o con la plataforma.  La cámara está disponible en modelos selectos.

1.2 Panel trasero

Figura 1-2 Panel trasero

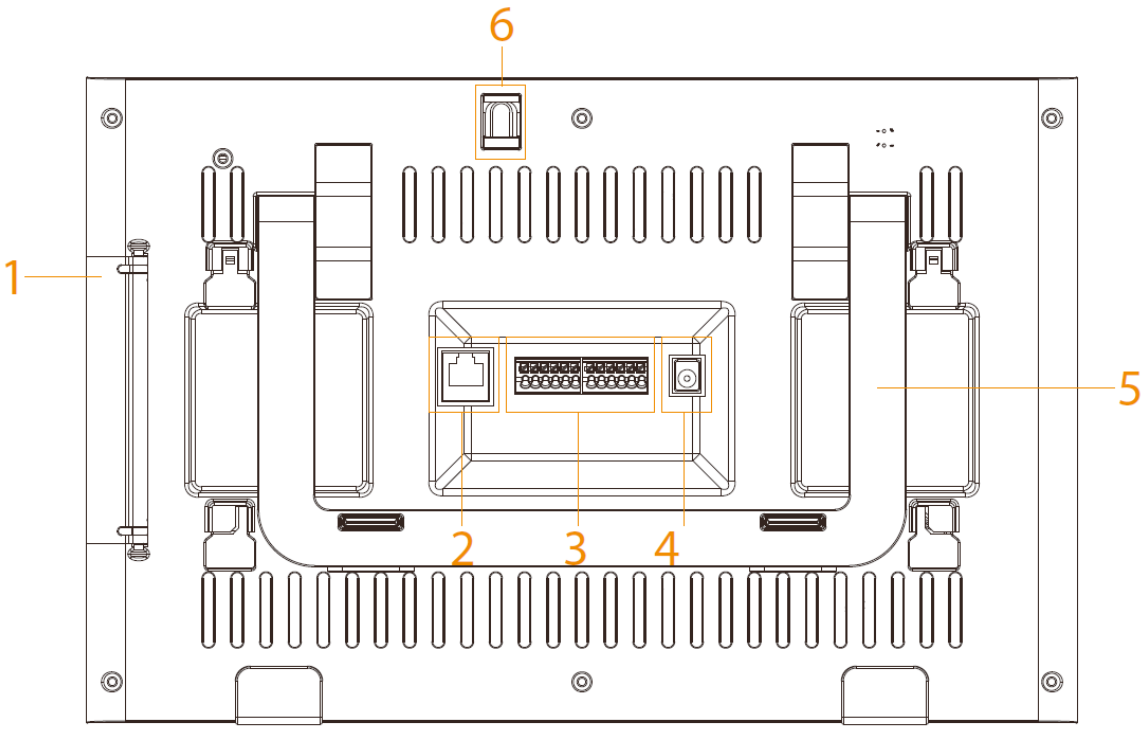


Tabla 1-2 Descripción del panel trasero

No.	Nombre	Descripción
1	Puerto	Abra el panel trasero y los puertos de arriba a abajo son: ● Puerto de transmisión de vídeo HDMI, solo para transmisión de vídeo. ● Puerto USB. ● Puerto USB. ● Ranura para tarjetas SD.
2	Puerto de red	Conecta cable RJ-45. Le recomendamos que utilice FTP (Foil Twisted-Pair).

No.	Nombre	Descripción
3	Puerto de 12 pines	Los puertos de izquierda a derecha son: ● Puerto de salida de energía. ● Tierra. ● Puerto de entrada de alarma 1. ● Puerto de entrada de alarma 2. ● Puerto de entrada de alarma 3. ● Puerto de entrada de alarma 4. ● Puerto de entrada de energía. ● Tierra. ● Puerto RS-485A. ● Puerto RS-485B. ● Puerto de salida de alarma NO. ● Puerto de salida de alarma COM.
4	Puerto de alimentación	Alimentación de 12 VCC.
5	Soporte	Coloque VTS en el escritorio. Puede ajustar el ángulo del soporte a una posición adecuada para el monitoreo.
6	Perilla de la cámara	Puede ajustar la perilla a un ángulo apropiado para monitorear. También puedes ocultar la cámara ajustando la perilla.  La perilla está disponible en modelos selectos.

2 Inicializando VTS

Puede inicializar VTS a través del dispositivo local o a través de la página web.

2.1 Inicialización a través del dispositivo local

Procedimiento

Paso 1 Encienda el VTS.

Paso 2 Seleccione el idioma.

Paso 3 Introduzca la contraseña y la dirección de correo electrónico.

Etapa 4 Seleccionar**He leído y acepto todos los términos Privacidad, Acuerdo de licencia de software**, y luego toque**Próximo**.

Paso 5 Seleccione la escena según sus necesidades.

Figura 2-1 Inicialización a través del dispositivo local



Paso 6 Grifo**Completo**.

2.2 Inicialización a través de la página web

Requisitos previos

Asegúrese de que la computadora esté en el mismo segmento de red que VTS.

Procedimiento

Paso 1 Ingrese la dirección IP de VTS en un navegador y luego haga clic en

Paso 2 **Ingresar**. Seleccione el idioma.

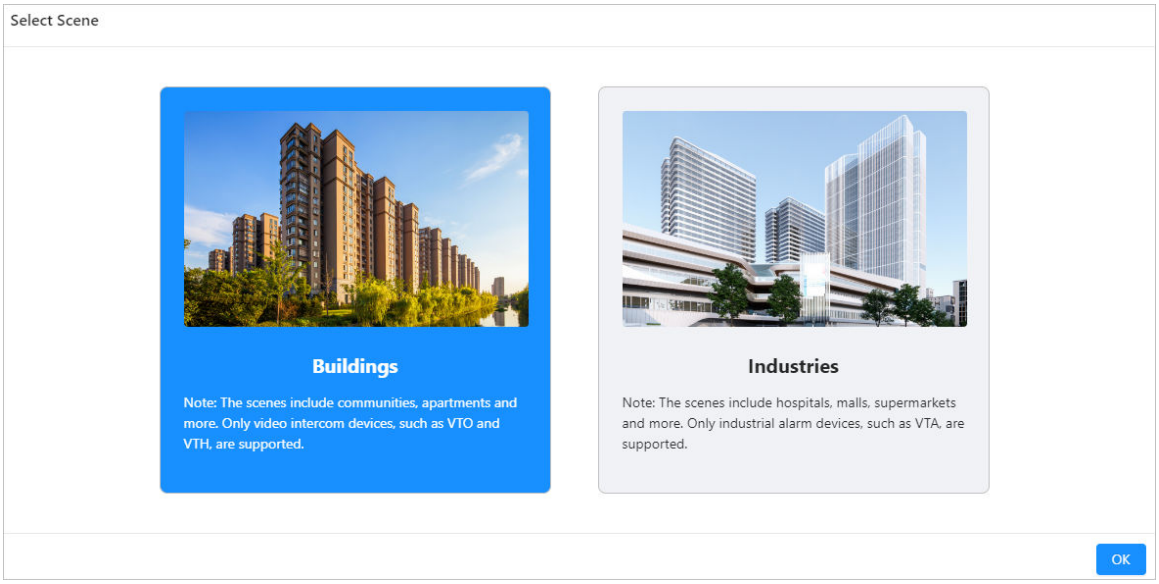
Paso 3 Si hay acuerdos, seleccione**He leído y acepto los términos y condiciones y acepto la política de privacidad y el acuerdo de licencia.**,y luego haga clic**Próximo**.

Etapa 4 Introduzca la contraseña y la dirección de correo electrónico y luego haga clic en**Terminado**.

Paso 5 Ingrese el nombre de usuario y la contraseña y luego haga clic en**Acceso**.

Paso 6 Seleccione la escena y luego haga clic**DE ACUERDO**.

Figura 2-2 Seleccionar escena



3 escenas de construcción

3.1 Operaciones en el dispositivo local

3.1.1 Pantalla local

Figura 3-1 Pantalla local



Tabla 3-1 Introducción a la pantalla de inicio

No.	Descripción
1	El número de VTS.
2	Fecha y hora.
3	Botones de función. ● Teléfono: Llama a VTH y consulta el historial de llamadas. Para obtener más información, consulte "3.1.8.1 Llamada". ● Información: Consulta la reproducción de vídeo y capturas de pantalla. Para obtener más información, consulte "3.1.8.2 Comprobación de la información". ● Monitorear: Monitorear VTH, VTO e IPC. Para obtener más información, consulte "3.1.8.3 Supervisión". ● Configuración: Ingrese a la pantalla de configuración de VTS.
4	Grifo  para bloquear la pantalla. Si seleccionas**Configuración**>**Configuración de pantalla**y enciende**Bloquear pantalla**,necesitas ingresar la contraseña predeterminada**123456**para desbloquear la pantalla cuando la bloquea después de la configuración.

No.	Descripción
5	El estado de conexión de la red, el servidor SIP y la tarjeta SD.

3.1.2 Configuración de los parámetros de visualización

Configura el brillo y el tiempo de apagado de la pantalla. Encender o apagar**Bloquear pantalla**.

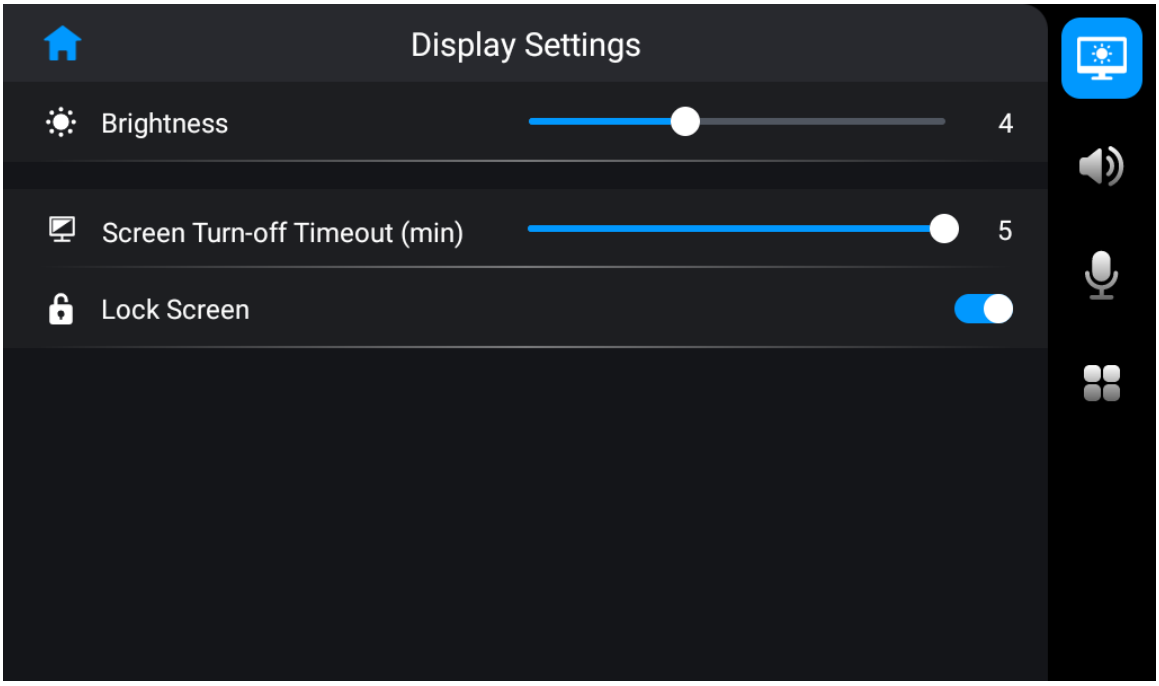
Procedimiento

Paso 1 En la pantalla de inicio, seleccione .

Paso 2 **Configuración**> Configure los parámetros.

Pantalla de bloqueo: después de activar la función, si necesita desbloquear la pantalla nuevamente, ingrese la contraseña predeterminada**123456**.

Figura 3-2 Configuración de pantalla



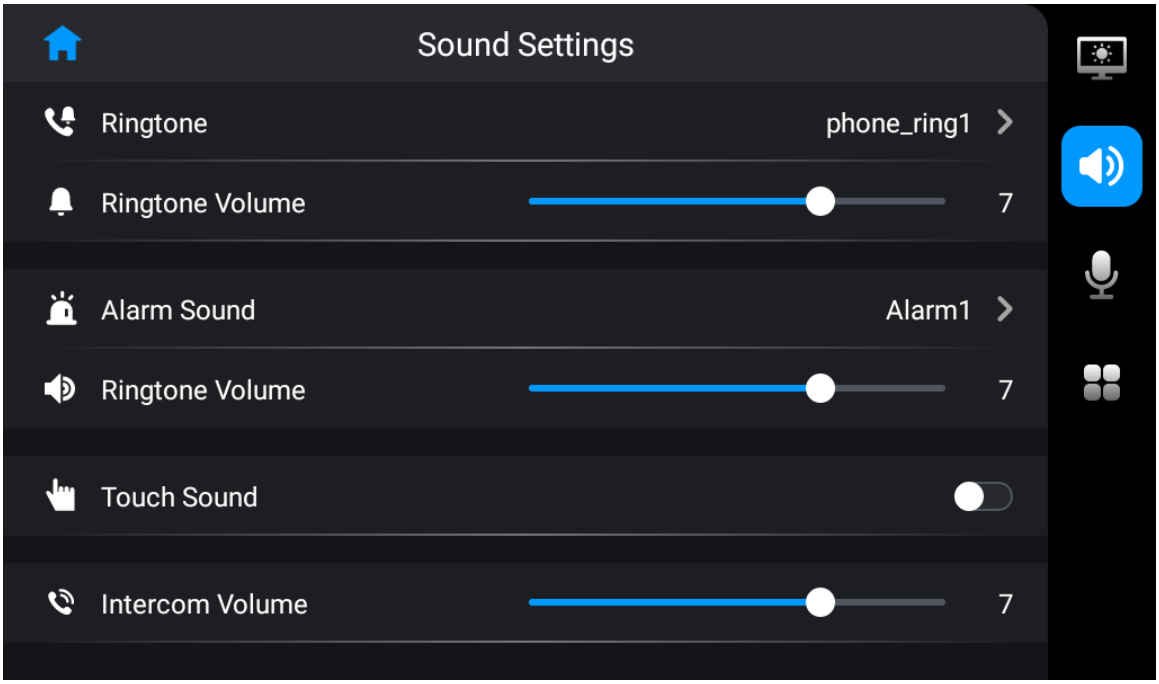
3.1.3 Configuración de los parámetros de sonido

Procedimiento

Paso 1 En la pantalla de inicio, seleccione .

Paso 2 **Configuración**> Configure los parámetros.

Figura 3-3 Configuración de sonido



3.1.4 Configuración de los parámetros del intercomunicador

Configure el tono de llamada y el límite de llamadas de VTO y VTH, y el tiempo de monitoreo.

Procedimiento

Paso 1 En la pantalla de inicio, seleccione .

Paso 2 **Configuración**> Configure los parámetros.

Figura 3-4 Configuración de intercomunicador

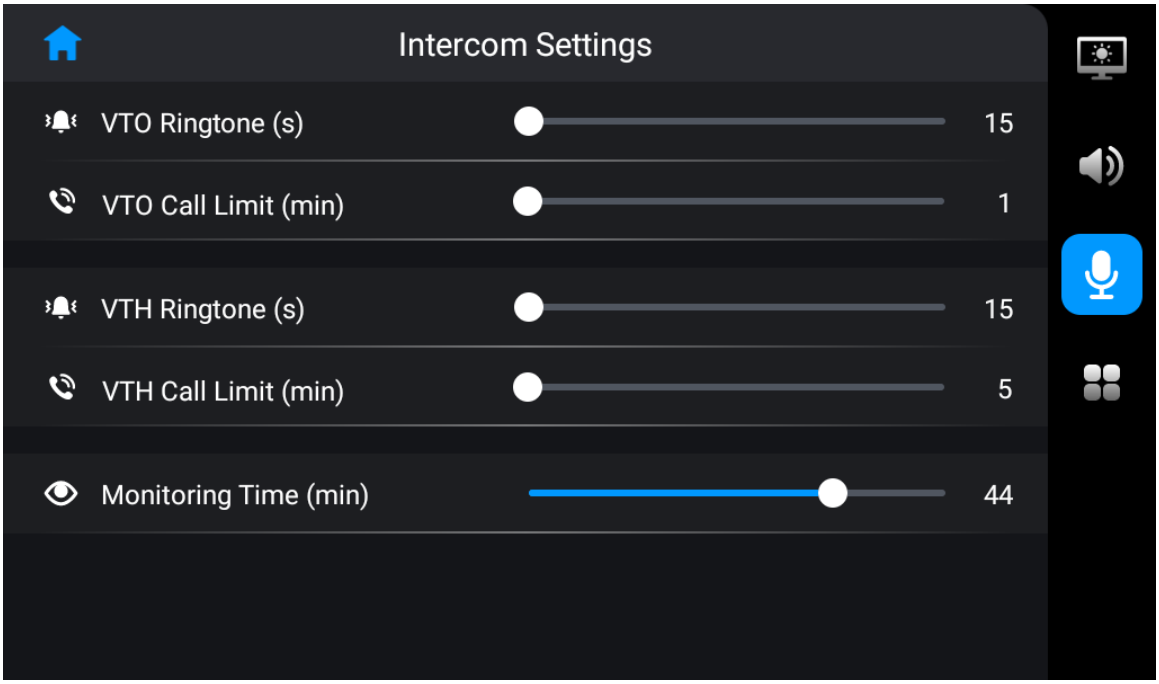


Tabla 3-2 Descripción de los parámetros del intercomunicador

Parámetro	Descripción
Tonos de llamada VTO	La llamada de VTO deja de sonar después de la hora configurada.
Límite de llamadas VTO (min)	VTO cuelga automáticamente la llamada a VTS después de la hora establecida.
Tonos de llamada VTH	La llamada de VTH deja de sonar después de la hora configurada.
Límite de llamadas VTH (min)	VTH cuelga automáticamente la llamada a VTS después de la hora configurada.
Tiempo de monitoreo (min)	El tiempo que VTS monitorea VTO y otros dispositivos.

3.1.5 Configuración de los parámetros avanzados

Procedimiento

Paso 1 En la pantalla de inicio, seleccione .

Paso 2 **Configuración**> Configure los parámetros.

Figura 3-5 Configuración avanzada

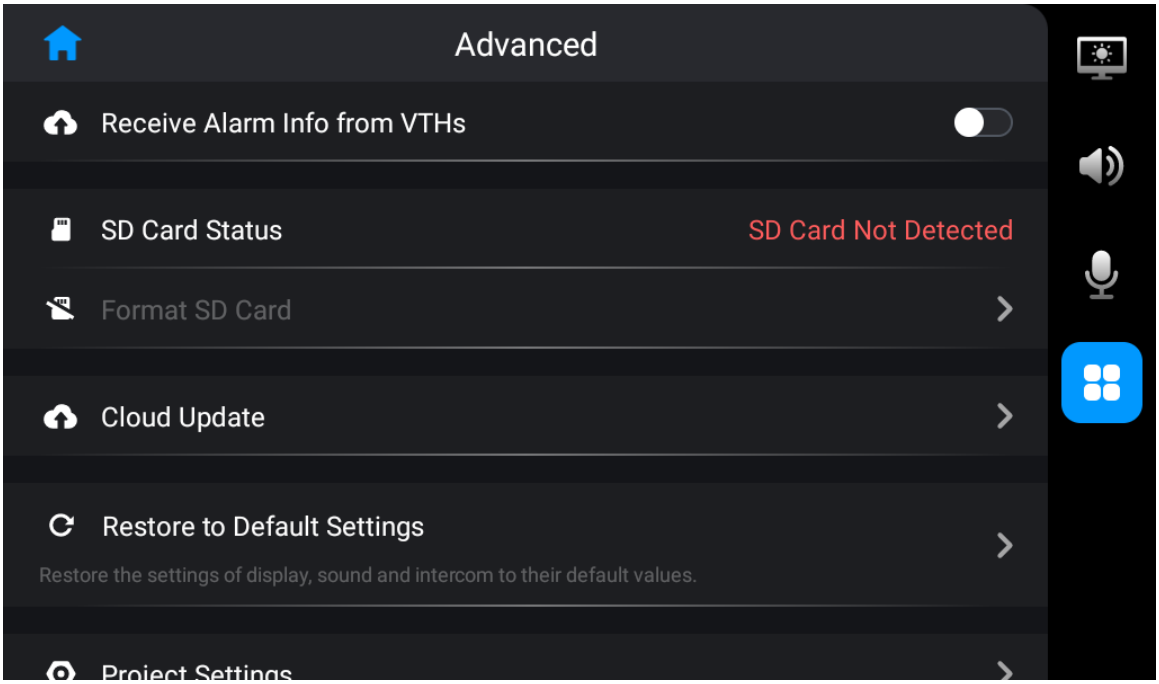


Tabla 3-3 Descripción de la configuración avanzada

Parámetro	Descripción
Estado de la tarjeta SD	Verifique la capacidad utilizada y la capacidad total de la tarjeta SD si hay una tarjeta SD en VTS. El sistema de numeración difiere en el sistema Android y en el sistema Windows al convertir la capacidad. Entonces, la capacidad de la tarjeta SD que se muestra en VTS es mayor que la que se muestra en la computadora.
Formatear tarjeta SD	Admite formatear la tarjeta SD.
Actualización en la nube	Verifique la última versión a través de las interacciones con la nube y luego actualice en línea.
Restaurar a los valores predeterminados Ajustes	Restaure la configuración de pantalla, sonido e intercomunicador a la configuración predeterminada.
Configuración del proyecto	Ingrese la contraseña inicial para ingresar a la pantalla de configuración del proyecto. Para obtener más información, consulte "3.1.7 Configuración del proyecto".
Información del dispositivo	Vea la información legal, la versión y la versión básica de seguridad de VTS.

3.1.6 Restablecer contraseña

Puede restablecer la contraseña a través de la dirección de correo electrónico vinculada.

Requisitos previos

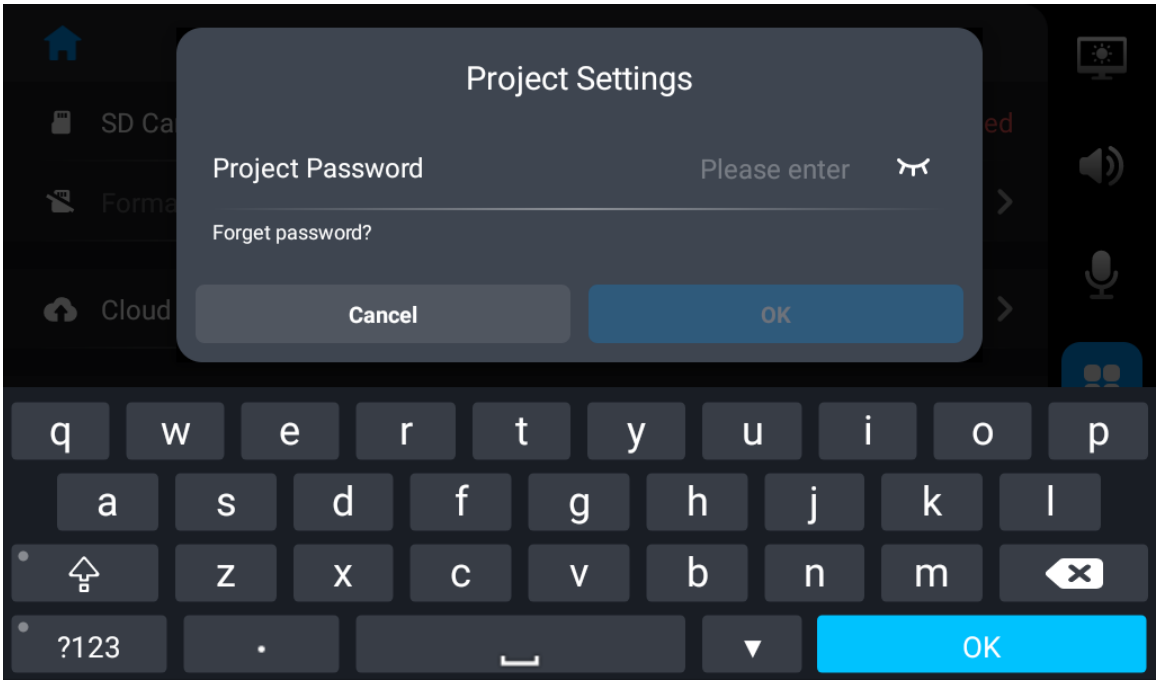
Asegúrate de haber encendido**Restablecer información**en**Configuración del proyecto**. Para obtener más información, consulte "3.1.7.4 Restablecimiento de información".

Procedimiento

Paso 1 En la pantalla de inicio, seleccione**Configuración**> Grifo > **Configuración del proyecto**.

Paso 2 **¿Contraseña olvidada?**,y luego toque**DE ACUERDO**.

Figura 3-6 Restablecer contraseña



Paso 3 Consigue el**Código de seguridad**de acuerdo con las instrucciones y luego ingrese la nueva contraseña y código de seguridad.

Etapa 4 Grifo**DE ACUERDO**.

3.1.7 Configuración del proyecto

3.1.7.1 Configuración del VTS

Configure el número y los parámetros de red de VTS.

Procedimiento

Paso 1 Seleccionar**Ajustes**>  > **Configuración del proyecto**en la pantalla de inicio.

Paso 2 Ingrese la contraseña que configuró durante la inicialización y toque**DE ACUERDO**.

Paso 3 Grifo  y configurar los parámetros.

Figura 3-7 Configurar los parámetros

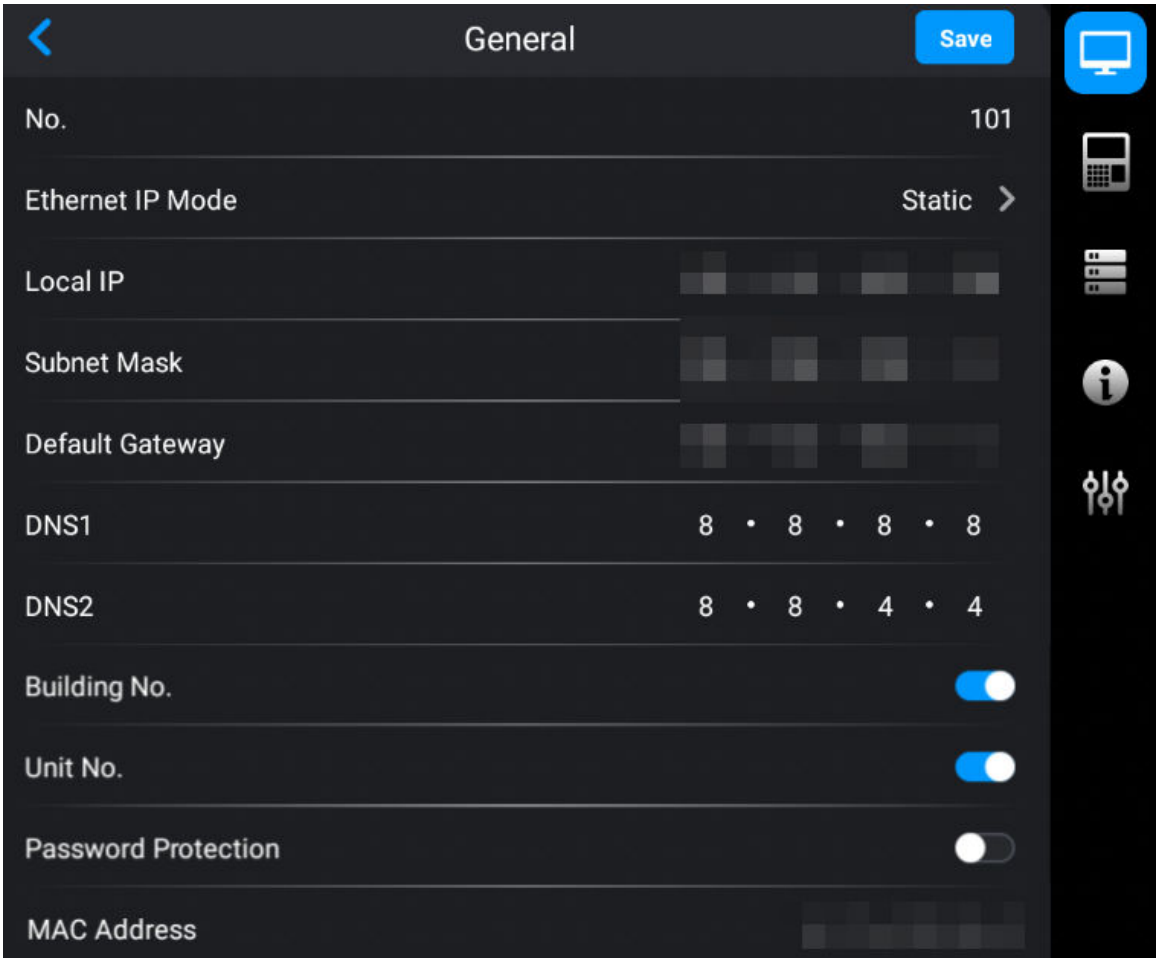


Tabla 3-4 Descripción de los parámetros

Parámetro	Descripción
No.	Usuario definido. Puedes configurar el número del 101 al 999.
Modo IP Ethernet	Configure el modo para obtener la IP. ● Estático: configurado manualmente**IP local**,**Máscara de subred**y**Puerta de enlace predeterminada**. ● DHCP (Protocolo de configuración dinámica de host): seleccione**DHCP**si hay un servidor DHCP. El dispositivo obtiene automáticamente una dirección IP dinámica.
IP local	Si seleccionas**Estático**en**Modo IP Ethernet**, configure la dirección IP, la máscara de subred y la puerta de enlace predeterminada de acuerdo con la planificación de la red.
Máscara de subred	
Puerta de enlace predeterminada	
DNS 1	Dirección IP del servidor DNS.
DNS 2	Dirección IP en espera del servidor DNS.

Parámetro	Descripción
Edificio número.	• Si la plataforma se utiliza como servidor SIP, asegúrese de que el estado de configuración del edificio y el número de unidad sea el mismo en la plataforma, VTS y VTO. • Si se utiliza el VTO como servidor SIP, asegúrese de que el estado de activación/desactivación del edificio y el número de unidad sea el mismo en VTS y VTO. No puede obtener la información del dispositivo de VTO en la pantalla de monitoreo.
Numero de unidad.	
Protección de contraseña	Active la protección con contraseña. La contraseña se transfiere encriptada cuando el dispositivo se registra en la plataforma a través de SIP.

3.1.7.2 Configurar el servidor SIP

Configure los parámetros del servidor SIP. Conéctese a VTO a través del acuerdo SIP para lograr un videoportero.

Procedimiento

Paso 1 Seleccionar**Configuración**> > **Configuración del proyecto**en la pantalla de inicio.

Paso 2 Ingrese la contraseña y toque**DE ACUERDO**.

Paso 3 Grifo y configurar los parámetros.

Figura 3-8 Configurar los parámetros



Tabla 3-5 Descripción de los parámetros

Parámetro	Descripción
Dirección IP	Dirección IP del servidor SIP.

Parámetro	Descripción
Puerto de red	Número de puerto de red del servidor SIP. ● VTO como servidor SIP: 5060. ● La plataforma como servidor SIP: 5080.
Nombre de usuario	Por defecto.
Contraseña	Por defecto.
Nombre de dominio	Mantenga la coherencia con el servidor SIP. El nombre de dominio es VDP de forma predeterminada.

Etapa 4 Grifo**Ahorrar**.

3.1.7.3 Agregar dispositivos

Agregue VTO, estación de cerca o IPC al VTS y luego podrá monitorear el VTO, la estación de cerca o IPC, desbloquear de forma remota y hablar con el VTO o la estación de cerca en el VTS.

Procedimiento

Paso 1 Seleccionar**Ajustes**>  > **Configuración del proyecto**en la pantalla de inicio.

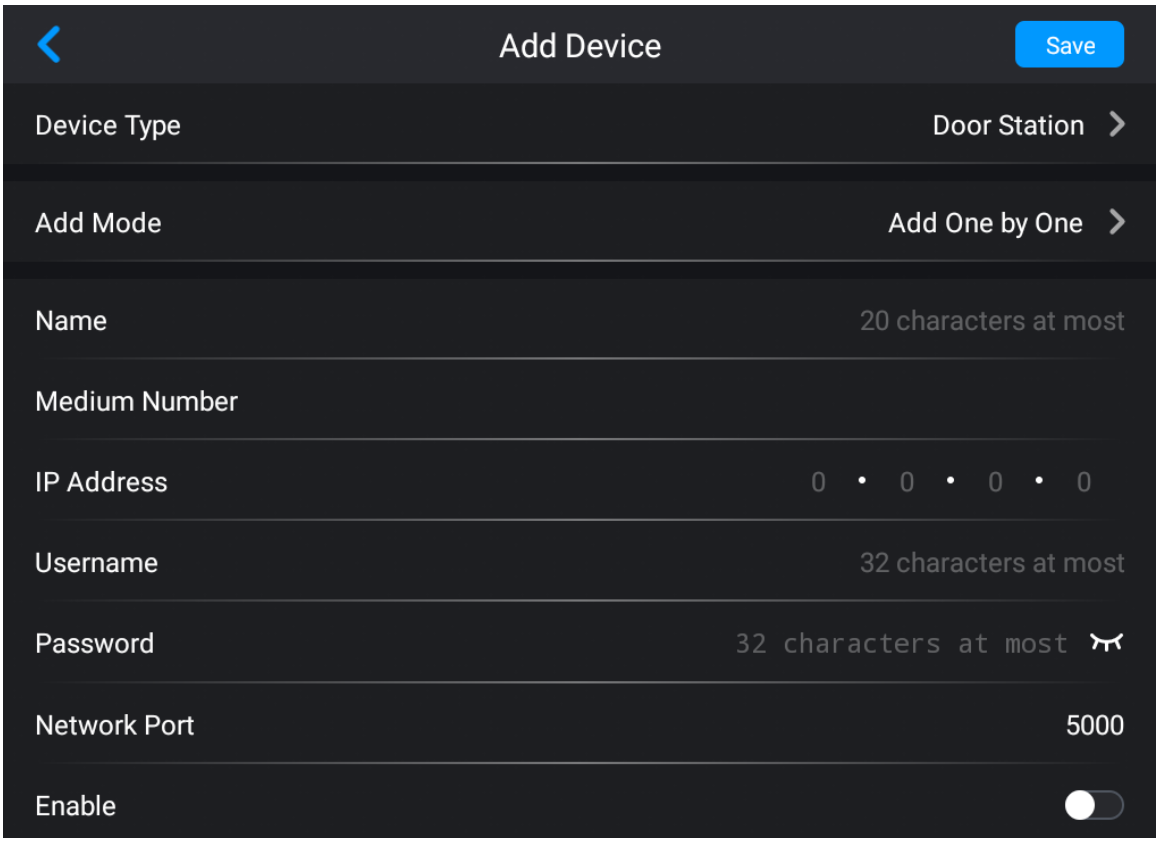
Paso 2 Ingrese la contraseña que configuró durante la inicialización y toque**DE ACUERDO**.

Paso 3 Seleccionar  > **Añadir dispositivo**.

Etapa 4 Agregar dispositivos.

- Agregue el dispositivo uno por uno.

Figura 3-9 Agregar dispositivos uno por uno



- Agregue dispositivos en lotes.

Figura 3-10 Agregar dispositivos en lotes

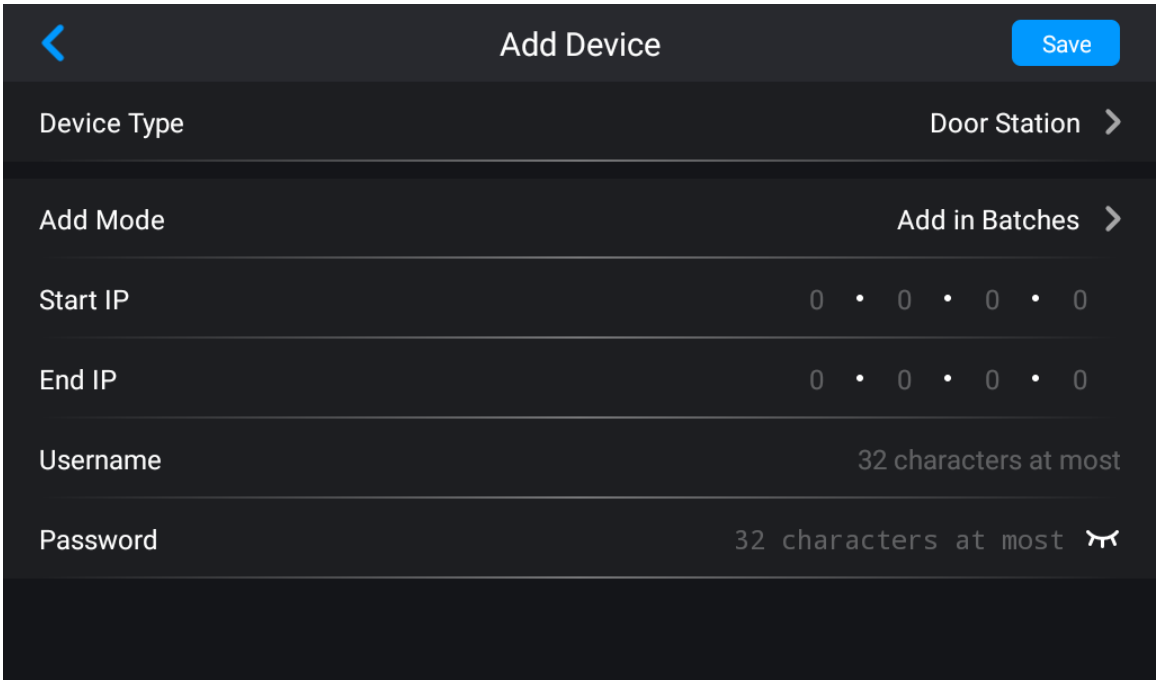


Tabla 3-6 Descripción de los parámetros

Tipo de dispositivo	Parámetro	Descripción
Estación de puerta o Estación de valla	Agregar modo	Admite agregar dispositivos uno por uno o en lotes. Solo VTO admite la adición de dispositivos en lotes.
	Nombre	Usuario definido. Puedes configurar el nombre que distingue el dispositivo.
	Número medio	No se puede editar.
	Dirección IP	La IP, nombre de usuario y contraseña del dispositivo que agregaste.
	Nombre de usuario	
	Contraseña	
	Permitir	Después de encender, seleccione**Monitor**>**VTO**o**Monitor**> **Estación de valla**para monitorear la pantalla.
	Iniciar IP	La dirección IP inicial y final del dispositivo si agrega dispositivos en lotes.
	IP final	
IPC	Nombre	Usuario definido. Puedes configurar el nombre que distingue el dispositivo.
	No.	Usuario definido.
	Dirección IP	La IP, nombre de usuario y contraseña del dispositivo que agregaste.
	Nombre de usuario	
	Contraseña	

Tipo de dispositivo	Parámetro	Descripción
	Tipo de transmisión	Seleccione la transmisión principal o la transmisión secundaria. ● Transmisión principal: la transmisión grande tiene alta definición y ocupa un gran ancho de banda. Utilizado para almacenamiento local. ● Subtransmisión: la imagen fluida ocupa un ancho de banda pequeño. Se utiliza para transmisión de red de bajo ancho de banda.
	Tipo de protocolo	Seleccione el protocolo local o el protocolo ONVIF según el IPC que agregó.
	Cifrado	El vídeo se transfiere encriptado cuando esta función está activada.
	Enlace	VTH admite la visualización de la imagen del IPC conectado cuando VTS llama a VTH si activa esta función.

Paso 5 Grifo**Ahorrar**.

3.1.7.4 Restablecer información

Active la función de restablecimiento aquí; de lo contrario, no podrá restablecer la contraseña si la olvida.

Procedimiento

Paso 1 En la pantalla de inicio, seleccione**Configuración**> > **Configuración del proyecto**.

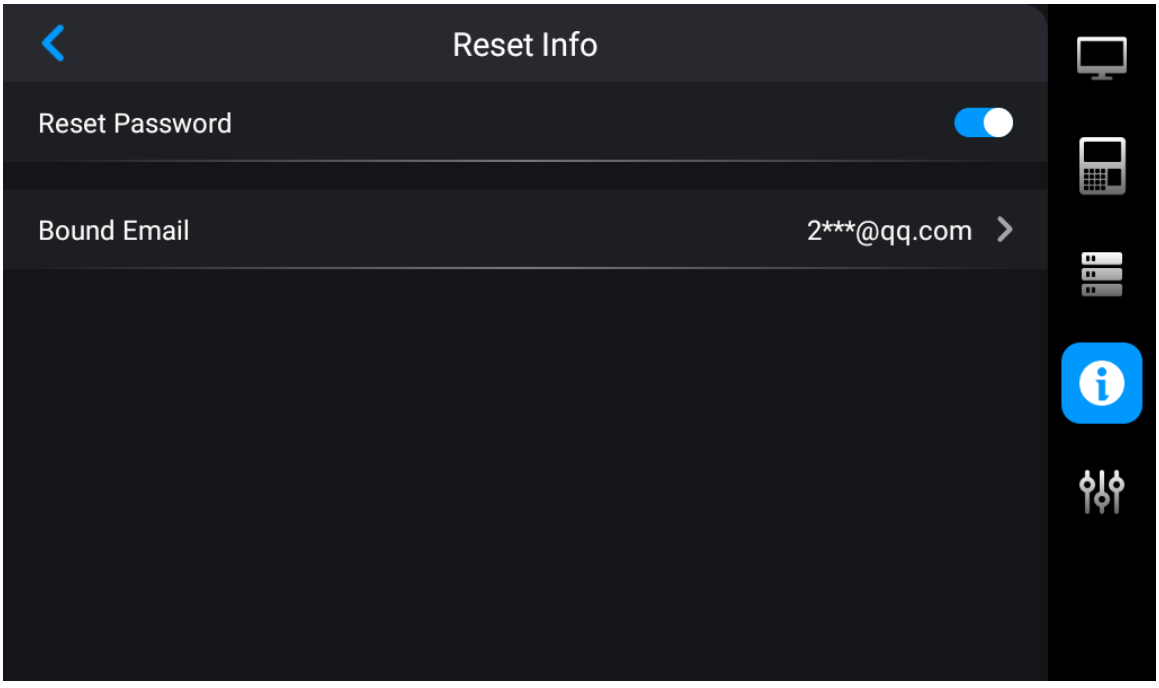
Paso 2 Ingrese la contraseña que configuró durante la inicialización y luego toque**DE ACUERDO**.

Paso 3 Grifo .

Etapa 4 Encender**Restablecer la contraseña**.

Paso 5 Grifo**Correo electrónico vinculado**para ingresar la dirección de correo electrónico.

Figura 3-11 Restablecer información



Paso 6 Hacer clic**DE ACUERDO**.

3.1.7.5 Depuración y valores predeterminados de fábrica

Procedimiento

Paso 1 En la pantalla de inicio, seleccione**Configuración**> > **Configuración del proyecto**.

Paso 2 Ingrese la contraseña y luego toque**DE ACUERDO**.

Paso 3 Grifo y luego configurar las funciones.

Figura 3-12 Valores predeterminados de fábrica y depuración

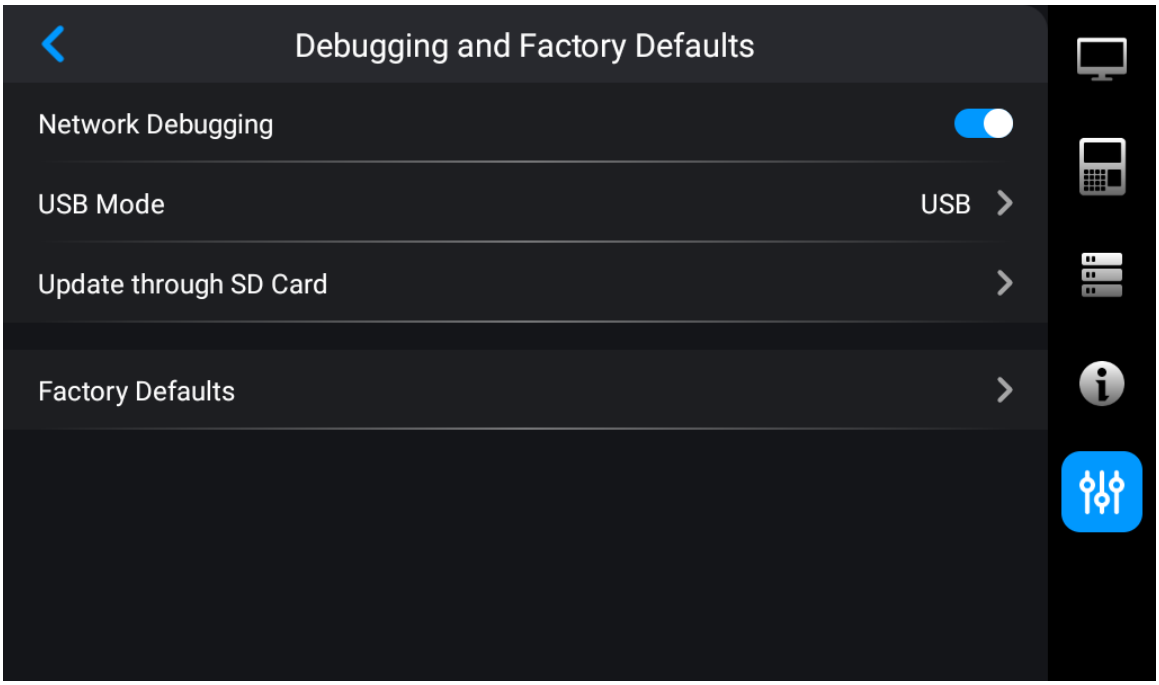


Tabla 3-7 Descripción de los parámetros

Parámetro	Descripción
Depuración de red	Sólo depurado y utilizado por administradores.
Modo USB	• USB: los administradores depuran VTS a través del puerto USB. • OTG: Los administradores transmiten los datos con VTS a través del puerto OTG.
Actualizar a través de SD Tarjeta	Coloque los archivos de actualización en la tarjeta SD. Actualice a través de la tarjeta SD que conectó al VTS. El nombre del archivo de actualización debe ser**actualizar.zip**.
Fallas de fábrica	VTS borra toda la información excepto la dirección IP y luego se reinicia después de los valores predeterminados de fábrica.

3.1.8 Puesta en servicio

3.1.8.1 Llamada

Llamar VTH

En la pantalla de inicio de VTS, toque**Teléfono**, ingrese el número de VTH y luego toque .

Si utilizas el cuello de cisne para hablar, la distancia recomendada es de entre 5 cm y 10 cm.

Figura 3-13 Dial

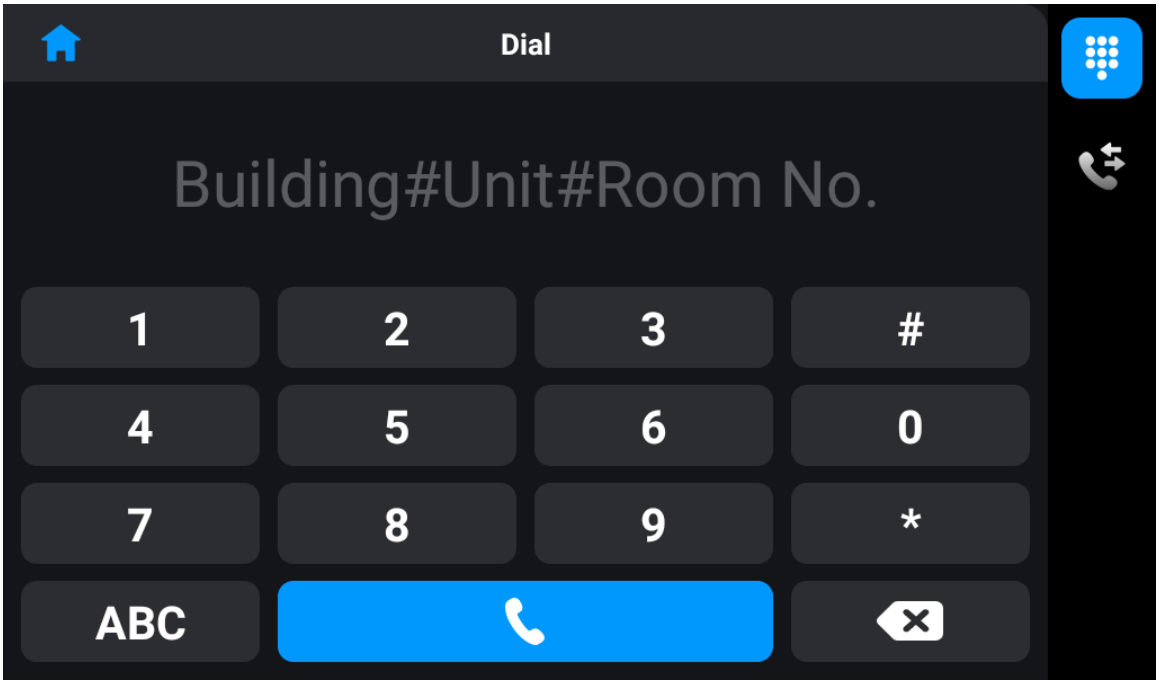


Figura 3-14 Llamar a VTH

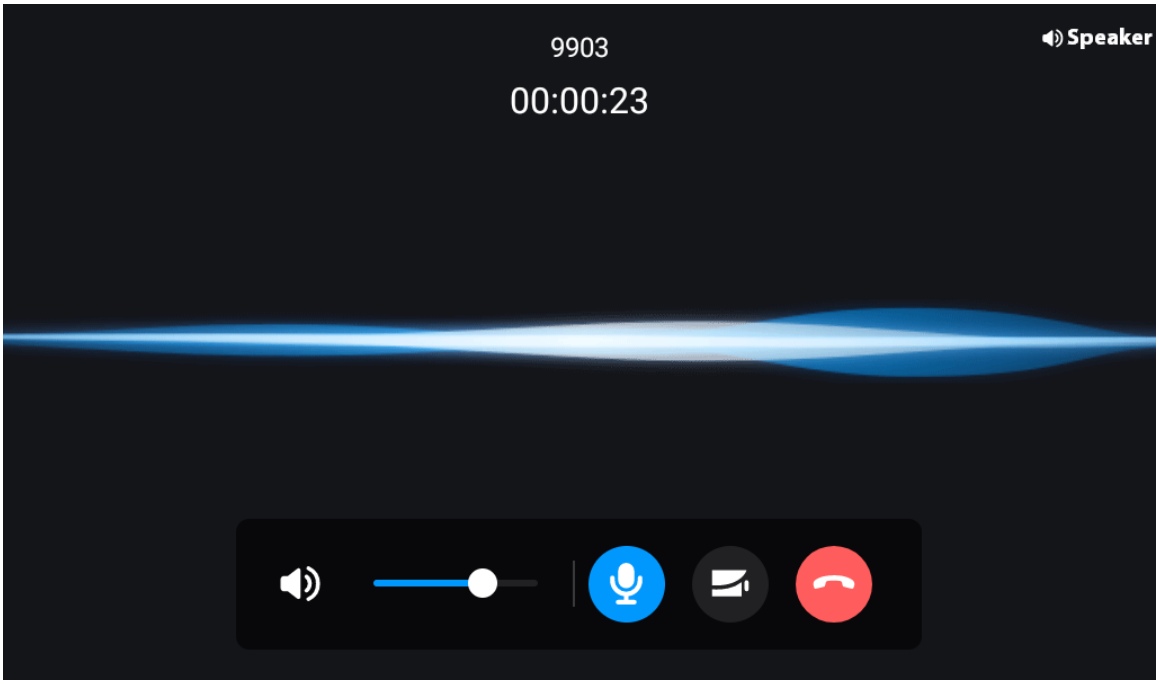


Tabla 3-8 Descripción de los iconos

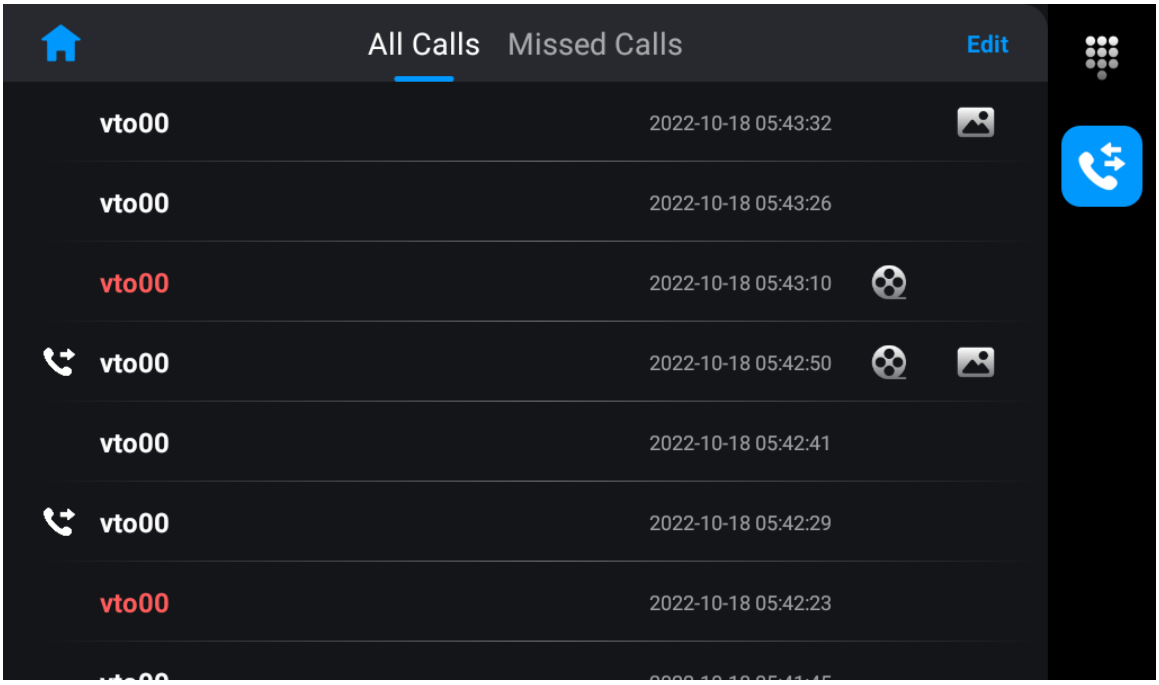
Icono	Descripción
	Ajusta el volumen del altavoz durante la llamada.
	Activa o desactiva la entrada de voz durante la llamada.
	Tóquelo para convertir a una imagen de video IPC durante la llamada.
	Tócalo para colgar la llamada.

Historial de llamadas

En la pantalla de inicio de VTS, toque**Teléfono**y luego toque  para comprobar todas las llamadas y llamadas perdidas.

- Toque la llamada en la lista del historial de llamadas para devolver la llamada.
- : Verifique los archivos de instantáneas de la llamada.
- : Consulta los archivos de vídeo de la llamada.

Figura 3-15 Historial de llamadas

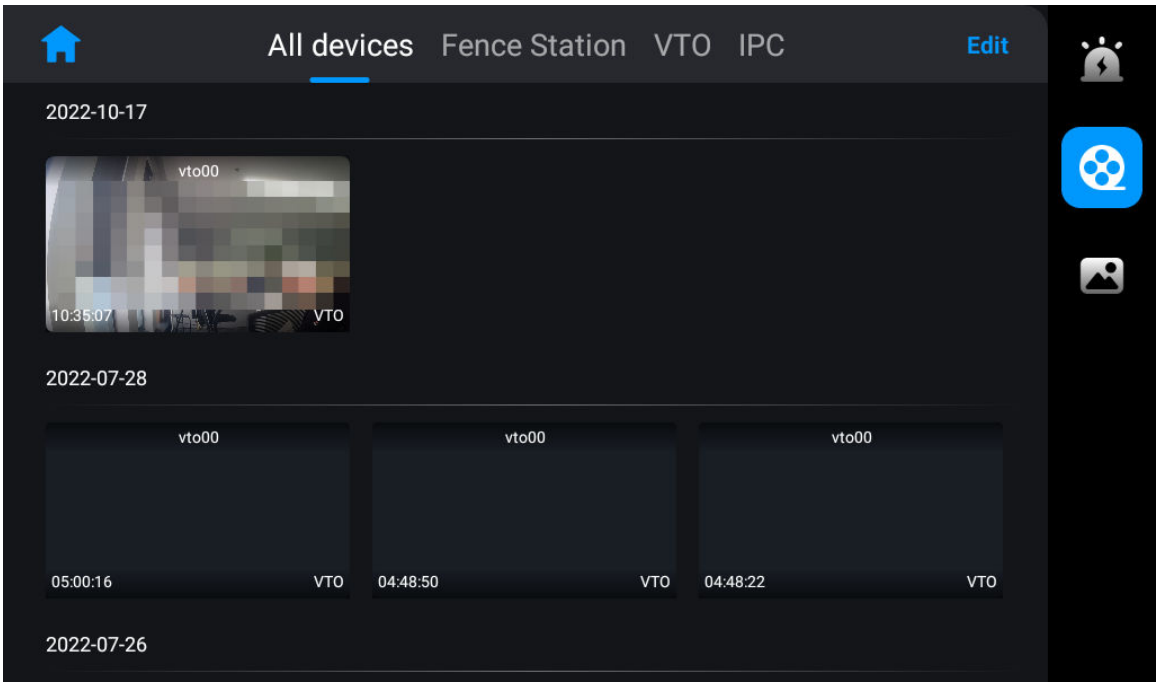


3.1.8.2 Verificación de la información

Archivos de video

Consulta o elimina los archivos de video que VTS grabó en el monitoreo o en la llamada.

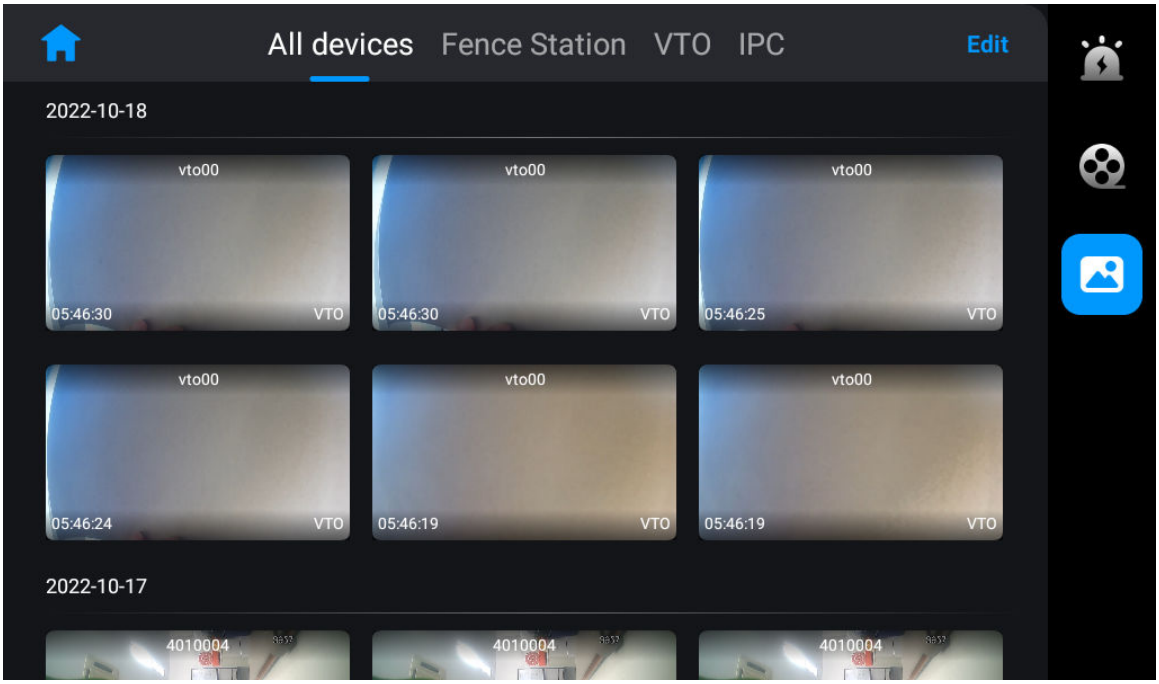
Figura 3-16 Archivos de vídeo



Archivos de instantáneas

Verifique o elimine los archivos de instantáneas que VTS registró en el monitoreo o en la llamada.

Figura 3-17 Archivos de instantáneas



3.1.8.3 Monitoreo

Monitoree VTO, estación de cerca o IPC en VTS. Las operaciones de monitoreo de IPC o estaciones de cerca son las mismas que las operaciones de monitoreo de VTO. Esta sección utiliza el monitoreo de VTO como ejemplo.

Requisitos previos

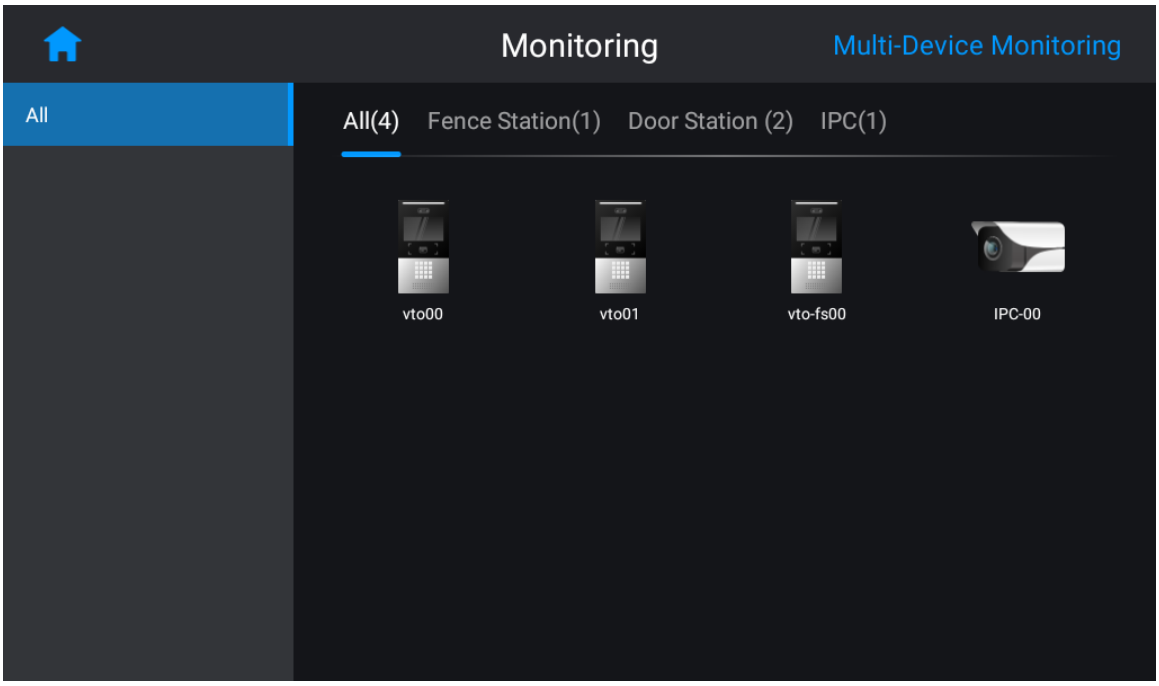
Asegúrese de haber agregado VTO, estación de cerca o IPC antes de monitorearlos. Para obtener más información, consulte "3.1.7.3 Agregar dispositivos".

Procedimiento

Paso 1 En la pantalla de inicio de VTS, toque**Monitor**.

Paso 2 Toque el ícono de VTO para monitorear.

Figura 3-18 Seleccionar VTO



Paso 3 Verifique la imagen de monitoreo.

Figura 3-19 Imagen de monitoreo

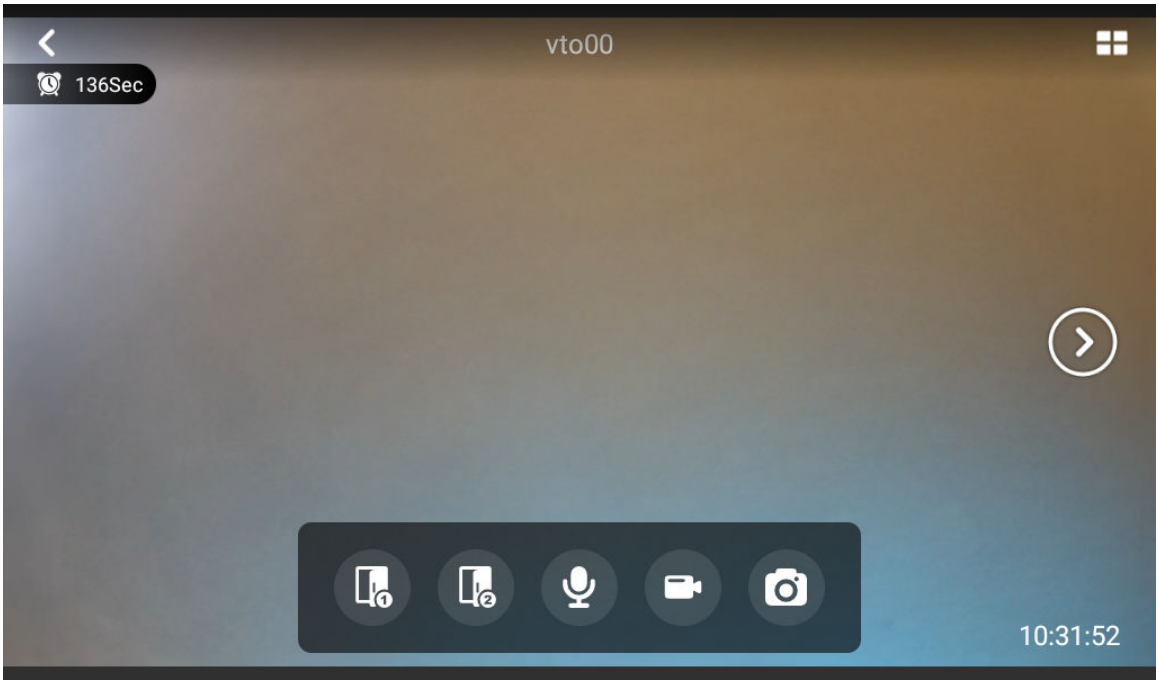


Tabla 3-9 Descripción de la imagen de monitoreo

Icono	Descripción
	Toque para ver la imagen de monitoreo en 4 ventanas.
	Toque para convertir y monitorear otros VTO si VTS conecta más de un VTO.
	Desbloquee VTO de forma remota.
	
	Llame a VTO y VTO reciba directamente la llamada sin tocar ningún icono.
	Toque para iniciar la grabación manual.
	Toque para tomar instantáneas manualmente.

3.2 Operaciones en la página web

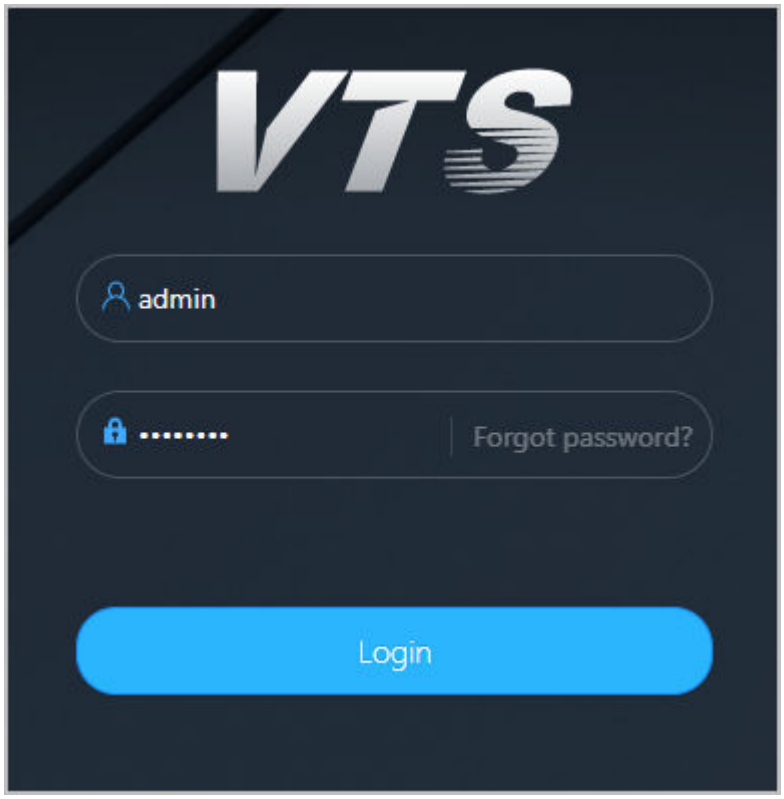
3.2.1 Iniciar sesión en la página web

Procedimiento

Paso 1 Ingrese la dirección IP de VTS en un navegador y luego presione la tecla Enter.

Paso 2 Ingrese el nombre de usuario y la contraseña.

Figura 3-20 Iniciar sesión en la página web



- El nombre de usuario predeterminado del administrador es**administración**. La contraseña predeterminada es la contraseña que configuró durante la inicialización. Le recomendamos cambiar la contraseña periódicamente.
- Si olvida la contraseña, haga clic en**¿Has olvidado tu contraseña?**para restablecer la contraseña. Para obtener más información, consulte "3.2.2 Restablecer contraseña".

Paso 3 Hacer clic**Acceso**.

3.2.2 Restablecer contraseña

Restablezca la contraseña a través de la dirección de correo electrónico que vinculó si la olvida.

Procedimiento

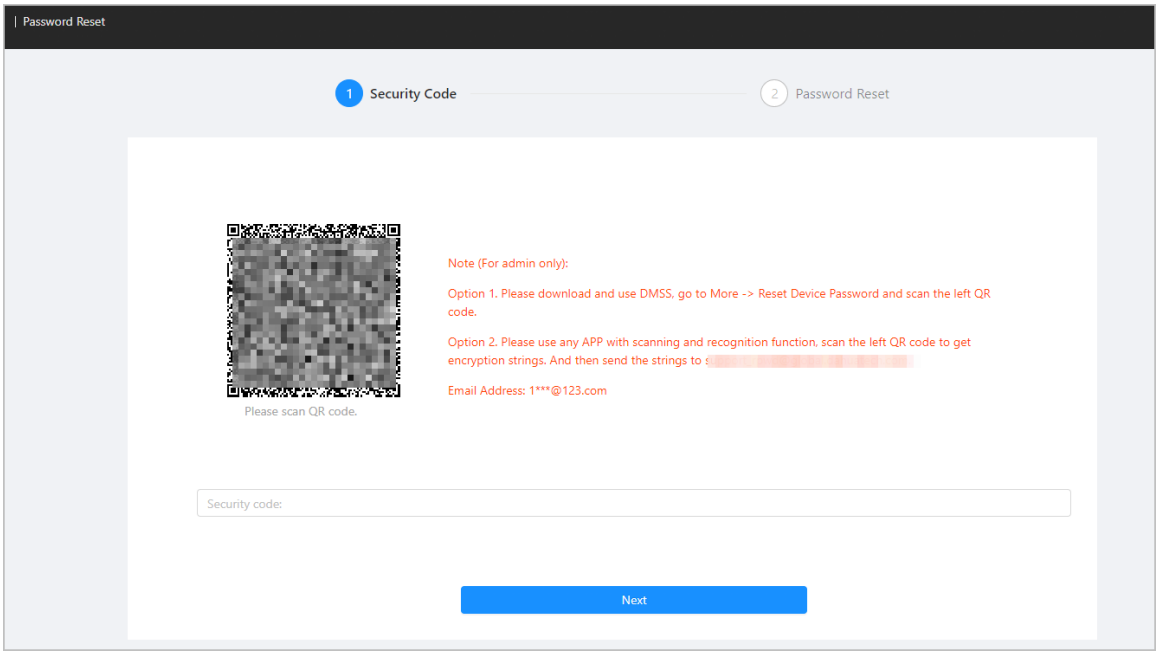
Paso 1 En la página de inicio de sesión, haga clic en**¿Has olvidado tu**

Paso 2 **contraseña?** Hacer clic**DE ACUERDO**en la ventana emergente.

Paso 3 Escanee el código QR en la página y luego obtenga el código de seguridad.

- Escanea el mismo código QR, podrás obtener como máximo 2 códigos de seguridad. Si necesita obtener el código de seguridad nuevamente, actualice la página del código QR.
- Reciba el código de seguridad en su correo electrónico. Utilice el código de seguridad dentro de 24 horas para restablecer la contraseña; de lo contrario, el código de seguridad no será válido.
- La cuenta se bloqueará durante 5 minutos si ingresa el código de seguridad incorrecto 5 veces seguidas.

Figura 3-21 Obtener el código de seguridad



Etapa 4 Ingrese el código de seguridad que recibió en el**Código de seguridad**caja de texto. Hacer clic

Paso 5 **Próximo**.

Paso 6 Restablezca la nueva contraseña y confirme la nueva contraseña.

La contraseña debe constar de 8 a 32 caracteres que no estén en blanco y contener al menos dos tipos de caracteres entre número, letra y carácter común (excluyendo espacios, ', ", ;, :, &).

Paso 7 Hacer clic**DE ACUERDO**para restablecer la contraseña.

3.2.3 Introducción a la página de inicio

El sistema va automáticamente a la página de inicio después de iniciar sesión.

Figura 3-22 Página de inicio

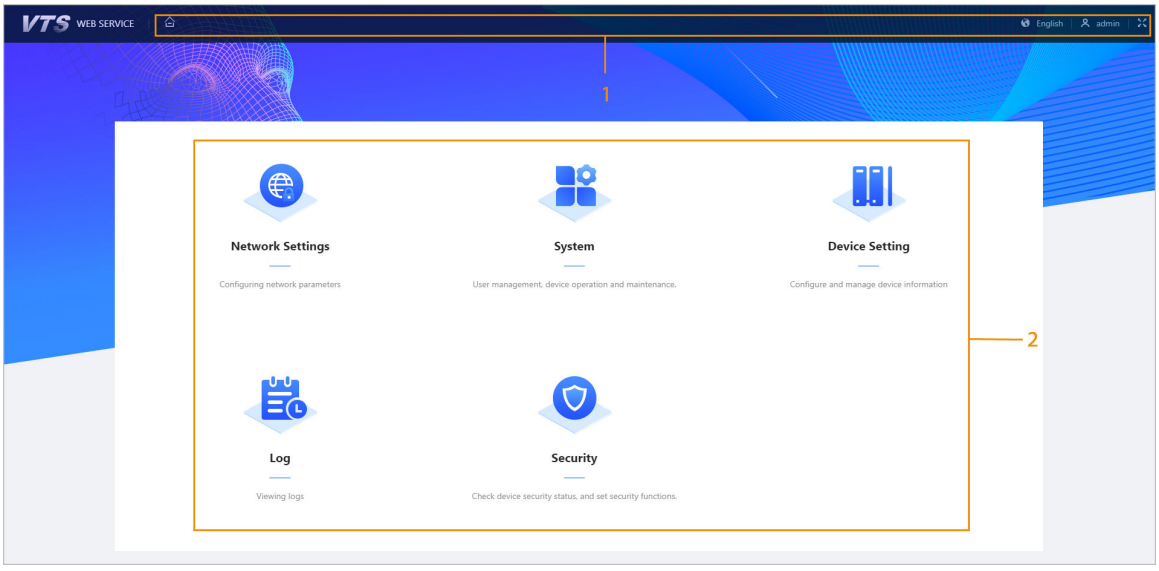


Tabla 3-10 Descripción de la página de inicio

No.	Parámetro		Descripción
1	Navegación Bar		Ir a la pagina principal.
			• Haga clic en el icono. Seleccionar**Reanudar**para reiniciar VTS. • Haga clic en el icono. Seleccionar**Cerrar sesión**para cerrar sesión en la cuenta.
			Abra la ventana en modo de pantalla completa.
2	Menú de funciones		Menú de configuración de funciones del VTS.

3.2.4 Configuración de la red

3.2.4.1 Configuración de TCP/IP

Procedimiento

Paso 1 Inicie sesión en la página web del dispositivo.

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

Paso 3 Configure los parámetros.

Figura 3-23 Configurar los parámetros

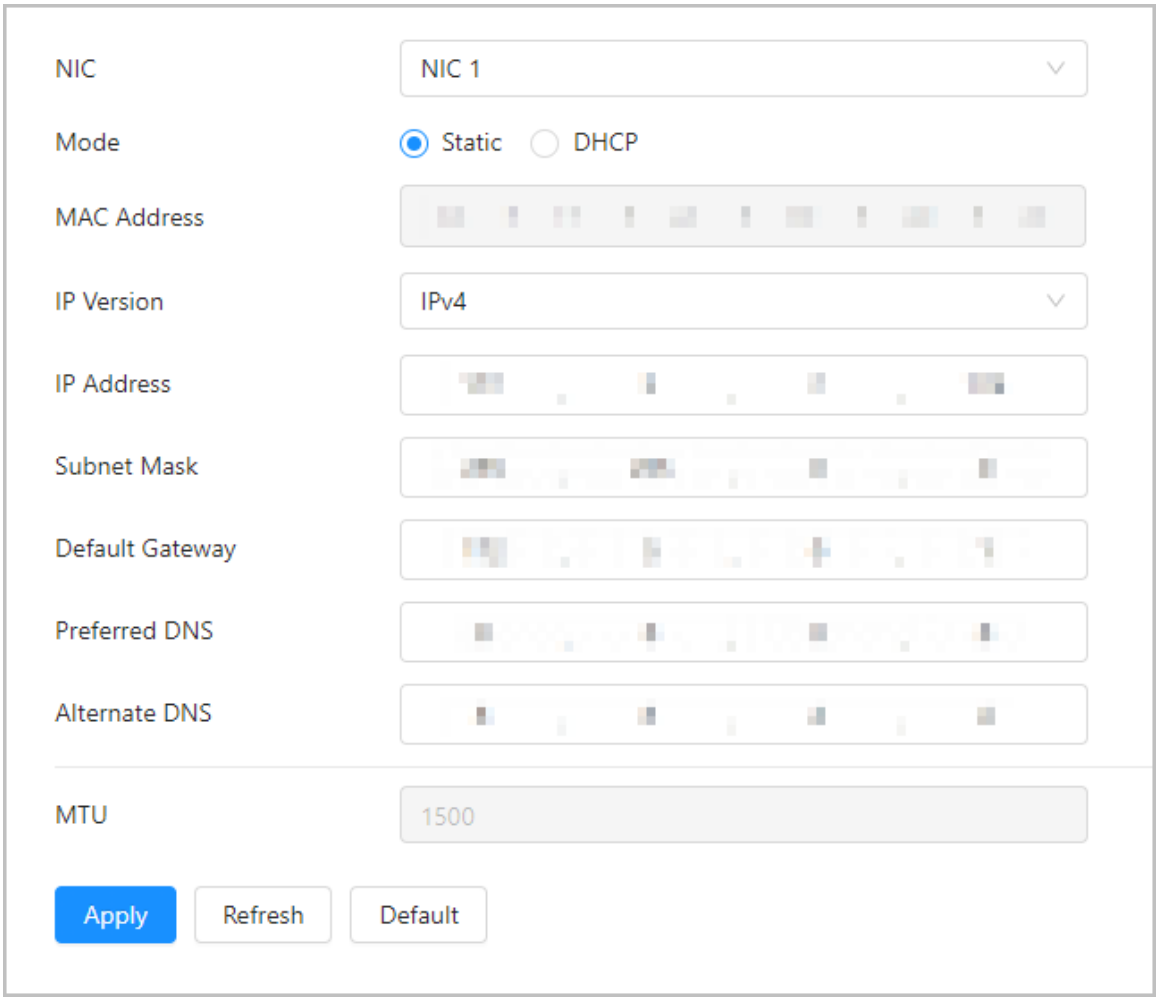


Tabla 3-11 Descripción de los parámetros

Parámetro	Descripción
Modo	• Estático: configurar manualmente**IP**,**Máscara de subred**y**Puerta de enlace predeterminada**. Hacer clic**Aplicar**y la página web va automáticamente a la página de inicio de sesión de la IP que configuró. • DHCP (Protocolo de configuración dinámica de host): seleccione**DHCP**si hay un servidor DHCP. El dispositivo obtiene automáticamente una dirección IP dinámica.
Dirección MAC	Dirección MAC (Control de acceso a medios) del dispositivo.
Versión IP	Seleccionar**IPv4**.
Dirección IP	Si seleccionas**Estático**en**Modo**, ingrese la dirección IP, la máscara de subred y la puerta de enlace predeterminada de acuerdo con la planificación de la red. • No hay máscara de subred en la versión IPv6. • La dirección IP y la puerta de enlace predeterminada deben estar en la misma red segmento.
Máscara de subred	
Puerta de enlace predeterminada	
DNS preferido	Dirección IP del servidor DNS.
DNS alternativo	Dirección IP alternativa del servidor DNS.

Etapa 4 Hacer clic**Aplicar**.

3.2.4.2 Configurar el servidor SIP

Configure los parámetros del servidor SIP. Conéctese a VTO a través del acuerdo SIP para lograr un videoportero.

Procedimiento

Paso 1 Inicie sesión en la página web de VTS.

Paso 2 Seleccionar**Configuración de la red**>**Servidor**

Paso 3 **SIP**. Configure los parámetros.

Figura 3-24 Parámetros del servidor SIP

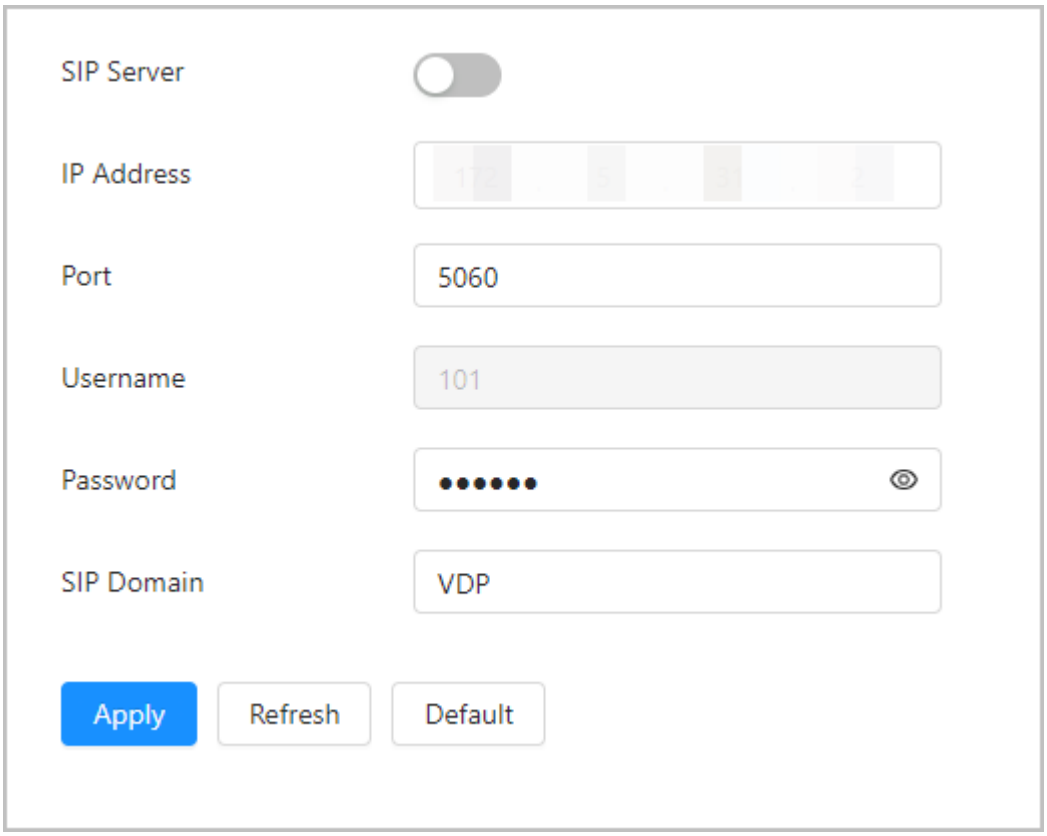


Tabla 3-12 Descripción de parámetros

Parámetro	Descripción
Dirección IP	Dirección IP del servidor SIP.
Puerto	Número de puerto de red del servidor SIP. ● VTO como servidor SIP: 5060. ● La plataforma como servidor SIP: 5080.
Nombre de usuario	Por defecto.
Contraseña	Por defecto.
Dominio SIP	Mantenga la coherencia con el servidor SIP. El nombre de dominio es VDP de forma predeterminada.

Etapa 4 Grifo**Ahorrar**.

3.2.4.3 Configuración de servicios básicos

Active el protocolo según sea necesario cuando conecte el VTS con la plataforma de terceros. Inicie sesión en la página web de VTS y luego seleccione**Configuración de la red**>**Servicios basicos**.

Figura 3-25 Servicios básicos

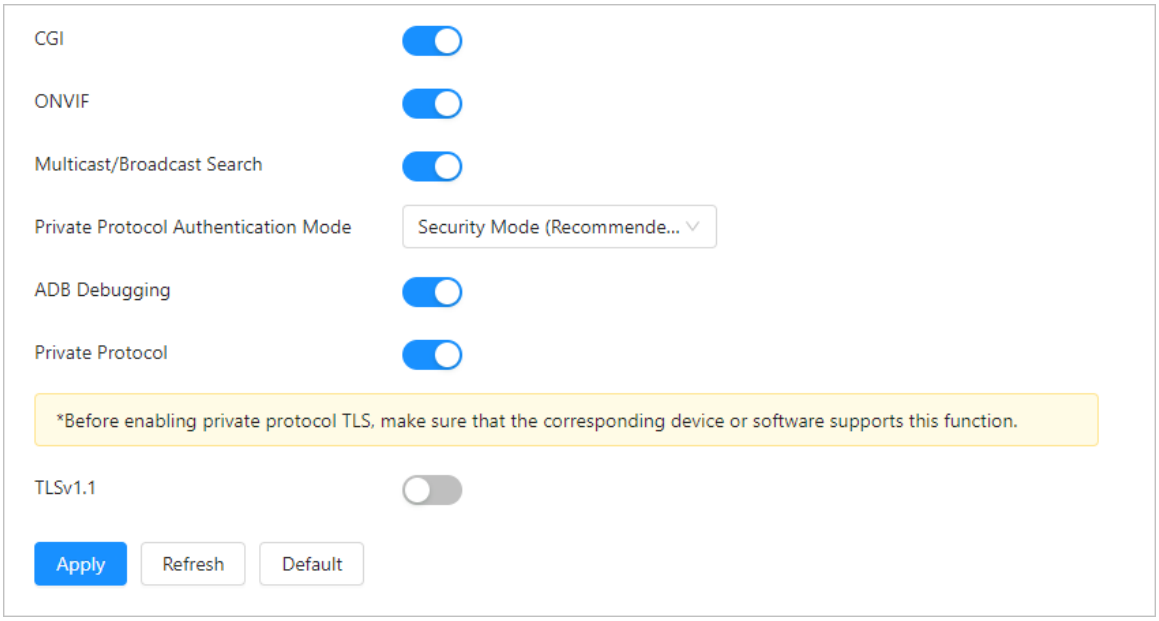


Tabla 3-13 Descripción de servicios básicos

Servicio	Descripción
CGI	Common Gateway Interface (CGI) ofrece un protocolo estándar para que los servidores web ejecuten programas de manera similar a las aplicaciones de consola que se ejecutan en un servidor que genera páginas web dinámicamente. Si está habilitado, se pueden utilizar comandos CGI. El CGI está habilitado de forma predeterminada.
ONVIF	Permita que otros dispositivos extraigan la transmisión de video del dispositivo a través del protocolo ONVIF.
Multidifusión/difusión Buscar	Habilite esta función y luego, cuando varios usuarios obtengan una vista previa de la imagen de video del dispositivo simultáneamente a través de la red, podrán encontrar su dispositivo con protocolo de multidifusión/difusión.
Protocolo privado modo de autenticación	• **Modo de seguridad (recomendado)**:El modo no admite el inicio de sesión con Digest, DES y autenticación de texto sin formato. • **Modo de compatibilidad**:El modo admite el inicio de sesión con autenticación Digest, DES y texto sin formato.
Depuración del BAD	Esta función solo está disponible para el personal de depuración.
Protocolo privado	Si está habilitada, la plataforma puede acceder al dispositivo con protocolo privado.
TLSv1.1	⚠ Existe un riesgo de seguridad si habilita**TLSv1.1**.

3.2.4.4 Configuración del registro automático

VTS se registra automáticamente en el servidor e informa su dirección IP al servidor designado

Procedimiento

Paso 1 Inicie sesión en la página web de VTS.

Paso 2 Seleccionar**Configuración de la red**>**Registro automático**.

Paso 3 Encender**Permitir**. Ingrese la dirección del servidor, el número de puerto y la ID del subdispositivo.

Figura 3-26 Registro automático

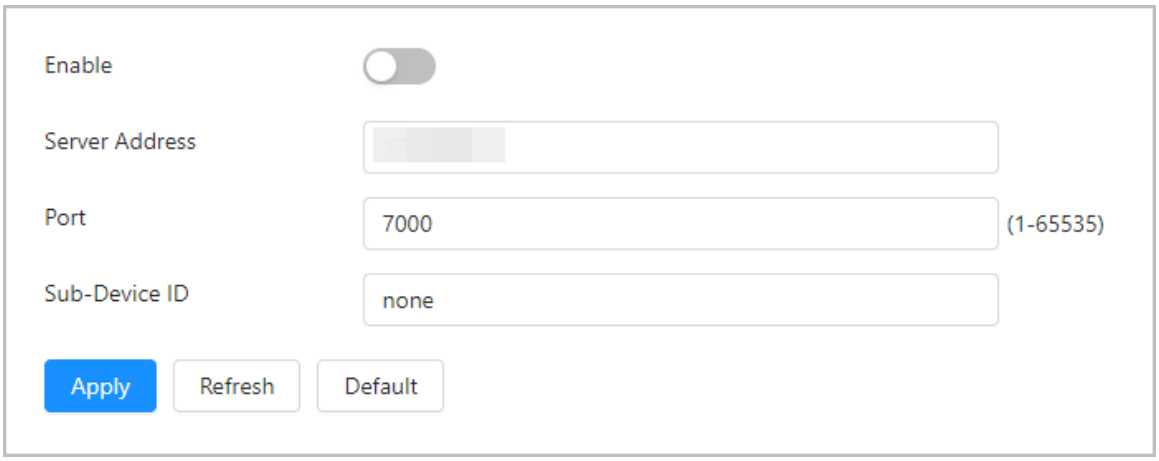


Tabla 3-14 Descripción de parámetros

Parámetro	Descripción
Dirección del servidor	Dirección IP o nombre de dominio del servidor que se necesita en el registro.
Puerto	Número de puerto que el servidor registra automáticamente.
ID de subdispositivo	El servidor distribuye una identificación para el dispositivo. Mantenga la coherencia con la identificación registrada en el servidor.

3.2.5 Gestión del sistema

3.2.5.1 Configuración de parámetros básicos de VTS

Configure el número y otras funciones de VTS.

Procedimiento

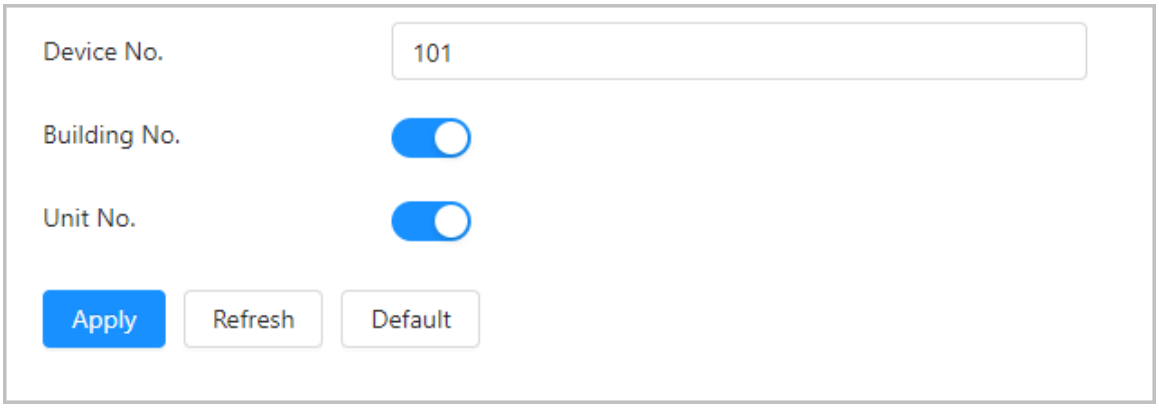
Paso 1 Inicie sesión en la página web de

Paso 2 VTS. Seleccionar**Sistema**>**General**.

Paso 3 Configure los parámetros.

- Puedes configurar el número del 101 al 999.
- Enciende el**Edificio número.**y**Numero de unidad.**según sea necesario.

Figura 3-27 Configurar parámetros básicos



Etapa 4 Hacer clic**Aplicar**.

3.2.5.2 Configuración de parámetros de vídeo

Información de contexto

El video está disponible en modelos selectos.

Procedimiento

Paso 1 Inicie sesión en la página web de

Paso 2 VTS. Seleccionar**Sistema**>**Video**.

Paso 3 Configure los parámetros.

Figura 3-28 Parámetros de vídeo

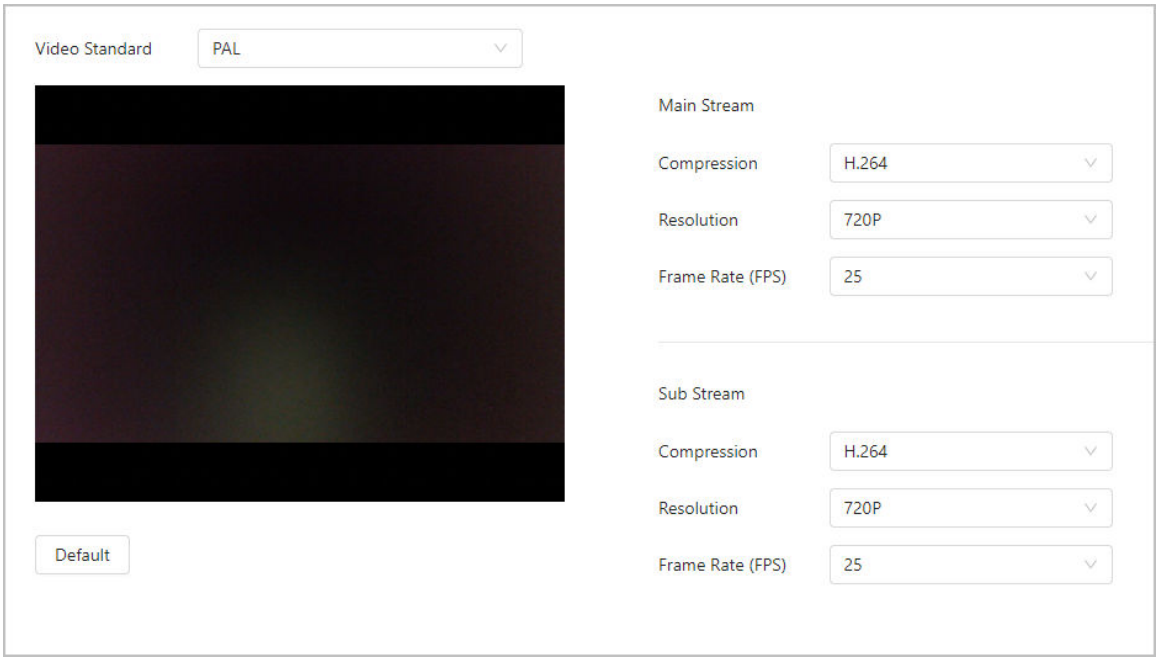


Tabla 3-15 Descripción de parámetros

Parámetro		Descripción
Estándar de vídeo		● PAL: la velocidad de fotogramas de transmisión predeterminada es 25 fps. ● NTSC: la velocidad de cuadros de transmisión predeterminada es 30 fps.
Convencional	Compresión	Seleccione el modo de compresión según el ancho de banda real. ● H.264: Compresión del perfil principal. ● H.265: la compresión del perfil principal ocupa un ancho de banda menor que H.264 con la misma calidad de imagen.
	Resolución	Seleccione la resolución según sea necesario.
	Velocidad de fotogramas (FPS)	El número de fotogramas que aparecen en un segundo. Un FPS más alto se refiere a una imagen más vívida y suave.
Sub corriente	Compresión	Seleccione el modo de compresión según el ancho de banda real. ● H.264: Compresión del perfil principal. ● H.265: la compresión del perfil principal ocupa un ancho de banda menor que H.264 con la misma calidad de imagen.
	Resolución	Seleccione la resolución según sea necesario.
	Velocidad de fotogramas (FPS)	El número de fotogramas que aparecen en un segundo. Un FPS más alto se refiere a una imagen más vívida y suave.

3.2.5.3 Gestión de cuentas

Agregue usuarios y edite la información del usuario según los diferentes protocolos.

3.2.5.3.1 Agregar usuario

Eres usuario administrador por defecto. Puedes agregar usuarios. Los usuarios recién agregados solo pueden iniciar sesión en la página web de VTS.

Procedimiento

Paso 1 Inicie sesión en la página web de VTS.

Paso 2 Seleccionar**Sistema**>**Cuenta**. Hacer clic

Paso 3 **Agregar**.

Etapa 4 Configure los parámetros.

Figura 3-29 Agregar usuarios

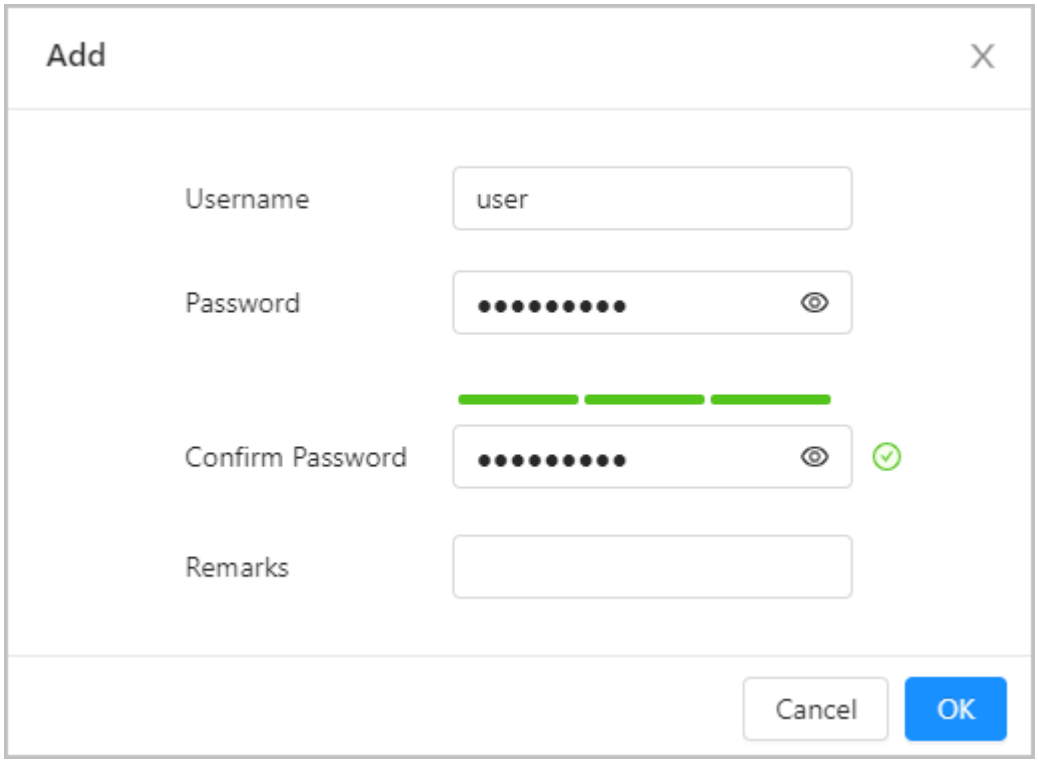


Tabla 3-16 Descripción de los parámetros de usuario

Parámetro	Descripción
Nombre de usuario	Identificación única del usuario. No puede utilizar el nombre de usuario existente. El máximo. La longitud del nombre de usuario es de 31 caracteres que constan de número, letra, subrayado, guión, punto y @.
Contraseña	La contraseña debe tener entre 8 y 32 caracteres que no estén en blanco y contener al menos dos tipos de números, letras y caracteres especiales (excluidos ' " ; : &).
confirmar Contraseña	
Observaciones	Usuario definido.

Paso 5 Hacer clic**DE ACUERDO**.

El usuario recién agregado se muestra en la lista de usuarios.

Operaciones relacionadas

- Modificar la información del usuario. Hacer clic para editar contraseña, grupo del usuario agregado.

  Para la cuenta de administrador, solo puede editar la contraseña.

- Borrar usuario. Hacer clic para eliminar el usuario agregado.

  La cuenta de administrador no se puede eliminar.

3.2.5.3.2 Restablecer contraseña

Restablezca la contraseña a través de la dirección de correo electrónico que vinculó si la olvida.

Procedimiento

Paso 1 Inicie sesión en la página web de

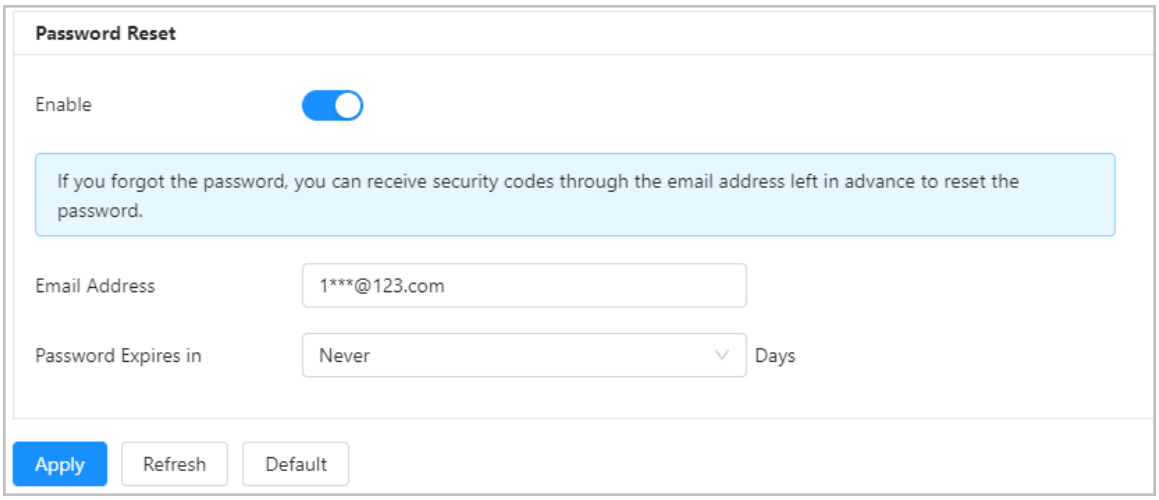
Paso 2 VTS. Seleccionar**Sistema**>**Cuenta**.

Paso 3 Haga clic para habilitar**Restablecimiento de contraseña**.

Etapa 4 Ingrese la dirección de correo electrónico y configure el período de caducidad de la contraseña.

La contraseña caduca en x días: definida por el usuario. Si seleccionas**Nunca**, el sistema no le recuerda cambiar la contraseña.

Figura 3-30 Restablecer contraseña



Paso 5 Hacer clic**Aplicar**.

3.2.5.3.3 Agregar usuario ONVIF

Puede agregar, eliminar usuarios ONVIF y cambiar sus contraseñas. El usuario ONVIF predeterminado es administrador.

Procedimiento

Paso 1 Inicie sesión en la página web de VTS.

Paso 2 Seleccionar**Sistema**>**Cuenta**>**Usuario ONVIF**. Hacer

Paso 3 clic**Agregar**.

Etapa 4 Configure los parámetros.

Figura 3-31 Agregar usuario ONVIF

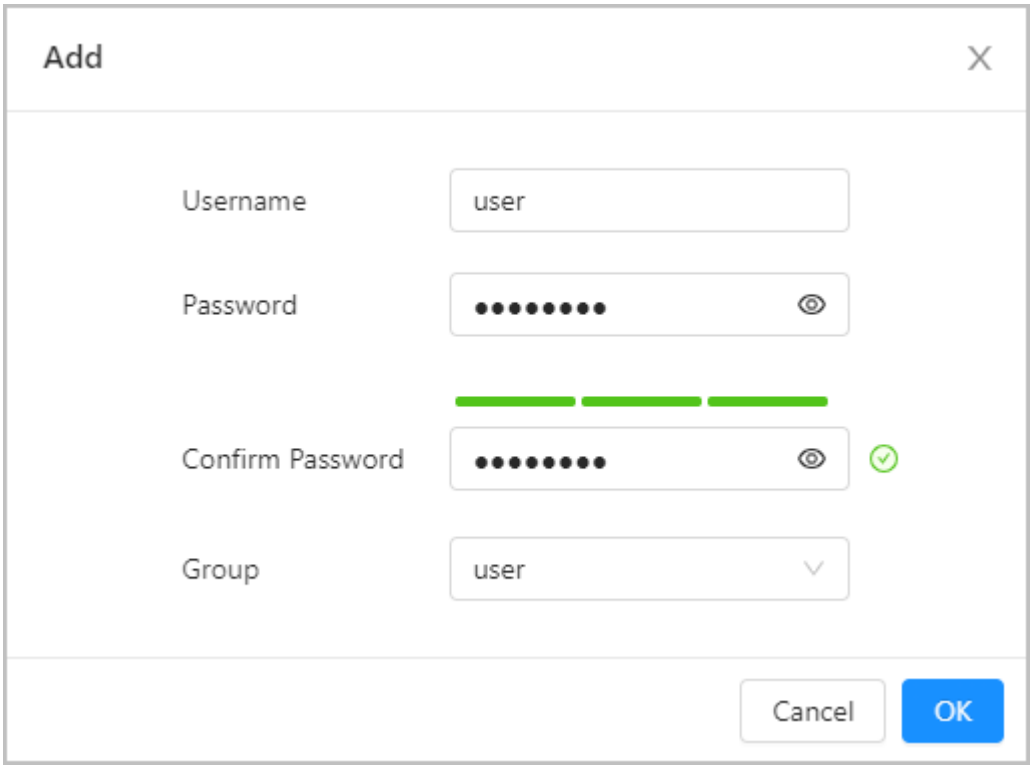


Tabla 3-17 Descripción de los parámetros de usuario de ONVIF

parámetro	Descripción
Nombre de usuario	Identificación única del usuario. No puede utilizar el nombre de usuario existente. La longitud máxima del nombre de usuario o grupo es de 31 caracteres que constan de números, letras, subrayado, guión, punto y @.
Contraseña	La contraseña debe tener entre 8 y 32 caracteres que no estén en blanco y contener al menos dos tipos de números, letras y caracteres especiales (excluidos ' " ; : &).
confirmar Contraseña	
Grupo	El grupo al que pertenecen los usuarios. Cada grupo tiene diferentes autoridades.

Paso 5 Hacer clic**DE ACUERDO**.

El usuario recién agregado se muestra en la lista de nombres de usuario.

Operaciones relacionadas

- Modificar la información del usuario. Hacer clic para editar contraseña, grupo del usuario agregado.

  Para la cuenta de administrador, solo puede editar la contraseña.

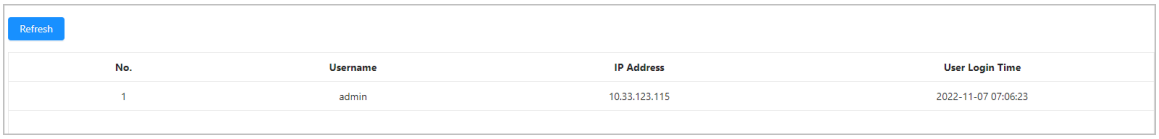
- Borrar usuario. Hacer clic para eliminar el usuario agregado.

  La cuenta de administrador no se puede eliminar.

3.2.5.4 Visualización del usuario en línea

Inicie sesión en la página web de VTS. Seleccionar**Sistema**>**Usuario en línea**para ver los usuarios actuales que inician sesión en la web. Puede ver el nombre de usuario, la dirección IP y la hora de inicio de sesión.

Figura 3-32 Usuario en línea



3.2.5.5 Configurar la hora

Puede configurar la fecha, la zona horaria y el servidor NTP (Protocolo de hora de red).

Procedimiento

Paso 1 Inicie sesión en la página web de

Paso 2 VTS. Seleccionar**Sistema**>**Tiempo**.

Paso 3 Configure los parámetros.

Figura 3-33 Configurar la hora

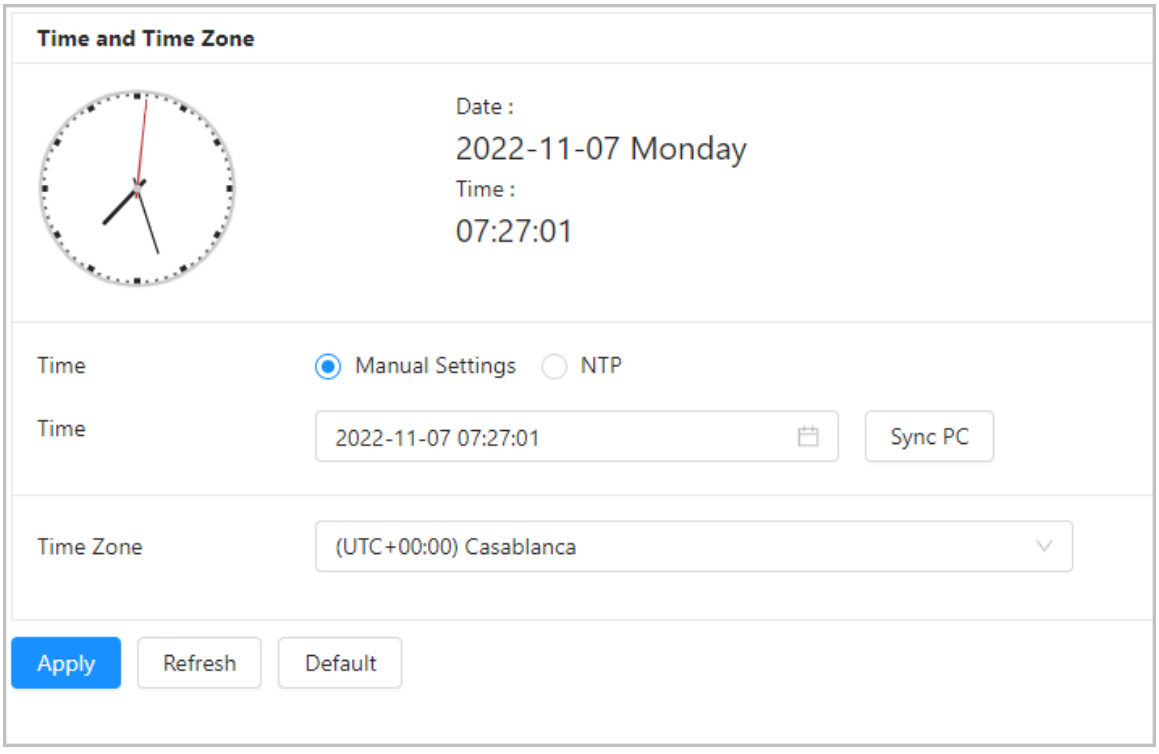


Tabla 3-18 Descripción de los parámetros de fecha y hora

Parámetro		Descripción
Tiempo y tiempo Zona	Tiempo	Seleccionar**Ajustes manuales**o**NTP**.

Parámetro		Descripción
	Tiempo	Si seleccionas**Ajustes manuales**, configure la hora del sistema manualmente. Hacer clic**Sincronizar PC**y la hora del sistema cambia a la hora de la PC.
	Servidor	Si seleccionas**NTP**, el sistema sincroniza la hora con el servidor de Internet en tiempo real. También puede ingresar la dirección IP, el puerto y el intervalo de una PC que ejecuta un servidor NTP para usar NTP.
	Puerto	
	Intervalo	
	Zona horaria	Configure la zona horaria en la que se encuentra VTS.

Etapa 4 Hacer clic**Aplicar**.

3.2.5.6 Configuración del mantenimiento

Configure el tiempo de reinicio automático para que el VTS pueda reiniciarse automáticamente para mejorar la velocidad de carrera.

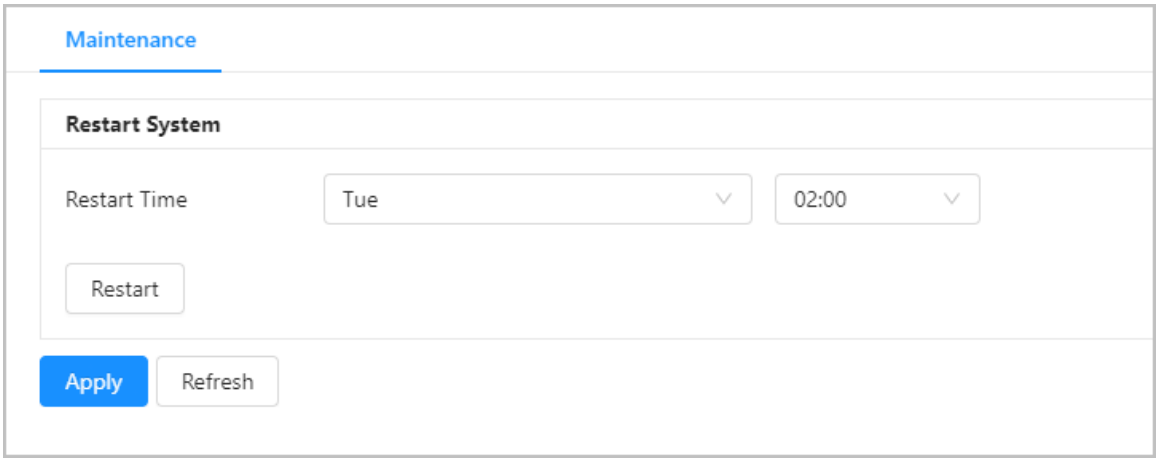
Procedimiento

Paso 1 Inicie sesión en la página web de VTS.

Paso 2 Seleccionar**Sistema**>**Mantenimiento**.

Paso 3 Configurar**Hora de reinicio**.

Figura 3-34 Mantenimiento



La hora de reinicio predeterminada es a las 2 en punto todos los martes.

Etapa 4 Hacer clic**Aplicar**.

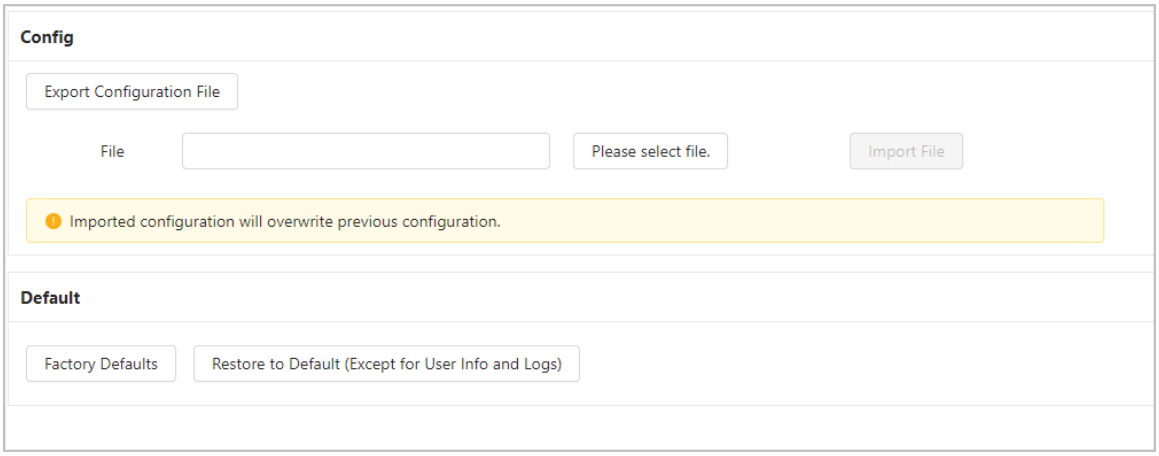
Operaciones relacionadas

Hacer clic**Reanudar**para reiniciar VTS.

3.2.5.7 Gestión de configuración

Inicie sesión en la página web de VTS. Seleccionar**Sistema**>**configuración**.

Figura 3-35 Gestión de configuración



3.2.5.7.1 Importar/exportar archivo de configuración

Importe o exporte el archivo de configuración del sistema. Utilice el archivo de copia de seguridad de configuración cuando muchos dispositivos necesiten la misma configuración de parámetros.

Exportar archivo de configuración

Hacer clic**Exportar archivo de configuración**para exportar el archivo de configuración del sistema al almacenamiento local.

El archivo de exportación excluye la información de IP.

Importar archivo de configuración

1. Haga clic**Por favor seleccione el archivo.**para seleccionar el archivo de configuración local.
2. Haga clic**Importar archivo**.

Admite la importación del archivo de configuración a dispositivos del mismo modo.

3.2.5.7.2 Valor predeterminado de fábrica

Esta función restaurará el dispositivo a la configuración predeterminada o a los ajustes de fábrica. Los datos se perderán. Opérelo con cuidado.

- **Fallas de fábrica**:Todas las configuraciones se restablecen a los valores de fábrica. Se borrará la información del dispositivo y la información del usuario.
- **Restaurar a los valores predeterminados (excepto información de usuario y registros)**:Todas las configuraciones, excepto la información del usuario y los registros, se recuperan a los valores predeterminados.

3.2.5.8 Actualización

Información de contexto



- No apague el dispositivo ni la red, reinicie ni apague el dispositivo.
- Si se utilizó un archivo de actualización incorrecto, reinicie el dispositivo; de lo contrario, es posible que algunas funciones no funcionen correctamente.
- La degradación tiene riesgos potenciales de seguridad. Opérelo con cuidado.

Procedimiento

Paso 1 Inicie sesión en la página web de VTS.

Paso 2 Seleccionar**Sistema**>**Actualizar**.

Paso 3 Seleccione el modo de actualización según sea necesario.

- Actualización de archivos

  1. Haga clic**Navegar**y luego cargue el archivo de actualización. El archivo de actualización debe ser un archivo .bin.
  2. Haga clic**Actualizar**.

- Actualización en línea

  Obtenga la nueva versión mediante verificación automática o verificación manual. Hacer clic**Actualizar ahora**.

  ◇ Comprobación automática: haga clic**Verificación automática**. El sistema verifica automáticamente la nueva versión una vez al día y le recuerda si hay una nueva versión.

  Recopilaremos la dirección IP, el nombre del dispositivo, la versión del hardware, el número de serie del dispositivo y otra información del dispositivo para informarle sobre la actualización a tiempo. La información recopilada se utiliza únicamente para verificar la legitimidad del dispositivo y para notificar la actualización.

  ◇ Comprobación manual: haga clic**Verificación manual**para comprobar manualmente la nueva versión del sistema.

3.2.5.9 Ver versión

Inicie sesión en la página web. Seleccionar**Sistema**>**Versión**para ver el modelo, el número de serie del dispositivo, la versión del sistema y la versión del hardware y otra información de la versión.

3.2.5.10 Ver información legal

Inicie sesión en la página web. Seleccionar**Sistema**>**Información legal**para ver el aviso de software de código abierto y otra información legal.

3.2.6 Gestión de dispositivos

3.2.6.1 Configuración de IPC

Admite la conexión con no más de 32 IPC. VTS supervisa los dispositivos de forma integrada.

Procedimiento

Paso 1 Inicie sesión en la página web de VTS.

Paso 2 Seleccionar**Configuración del dispositivo**>**Información de la CIP**.

Paso 3 Haga clic para configurar los parámetros de IPC.

Figura 3-36 Configurar IPC

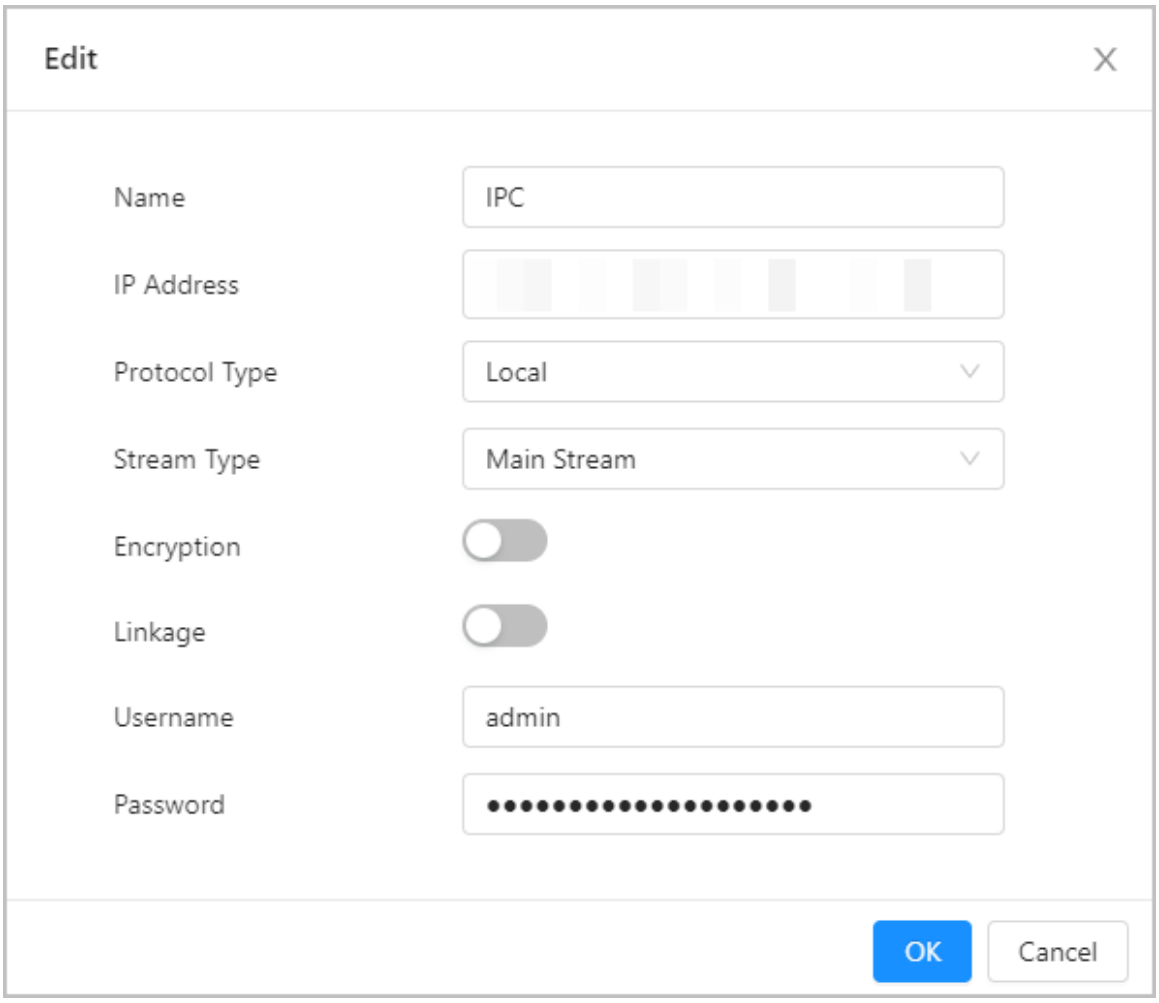


Tabla 3-19 Descripción de los parámetros IPC

Parámetro	Descripción
Nombre	Usuario definido. Puedes configurar el nombre que distingue el dispositivo.
Dirección IP	Dirección IP del IPC agregado.
Tipo de protocolo	Seleccione el protocolo local o el protocolo ONVIF según el IPC que agregó.
Tipo de transmisión	Seleccione la transmisión principal o la transmisión secundaria. ● Transmisión principal: la transmisión grande tiene alta definición y ocupa un gran ancho de banda. Utilizado para almacenamiento local. ● Subtransmisión: la imagen fluida ocupa un ancho de banda pequeño. Se utiliza para transmisión de red de bajo ancho de banda.
Cifrado	Active el cifrado. El vídeo se transfiere encriptado.
Enlace	VTH admite la visualización de la imagen del IPC conectado cuando VTS llama a VTH si activa esta función.

Parámetro	Descripción
Nombre de usuario	El nombre de usuario y contraseña del IPC que agregó.
Contraseña	

3.2.6.2 Agregar VTO o estación de cerca

Procedimiento

Paso 1 Inicie sesión en la página web de VTS.

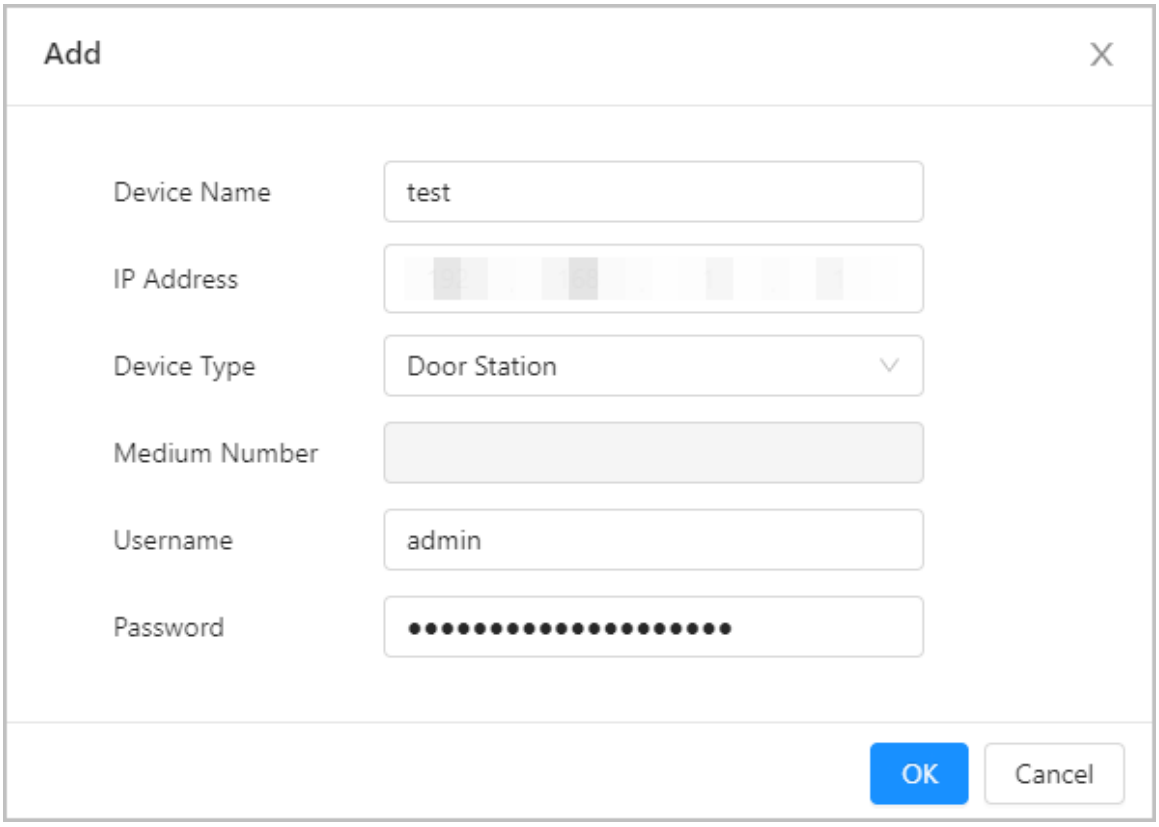
Paso 2 Seleccionar**Configuración del dispositivo**>**Configuración del dispositivo**>**Todo**.

Paso 3 Hacer clic**Agregar**.

Etapa 4 Configure los parámetros.

Puede seleccionar una estación de puerta o una estación de cerca.

Figura 3-37 Agregar estación de puerta de estación de cerca



Paso 5 Hacer clic**DE ACUERDO**.

Operaciones relacionadas

- Exportar: exporta la información del dispositivo.
- Importar: importe el archivo al dispositivo actual para agregar dispositivos en lotes. El archivo debe exportarse desde el dispositivo del mismo modelo.

3.2.7 Registro

3.2.7.1 Ver el registro del sistema

Procedimiento

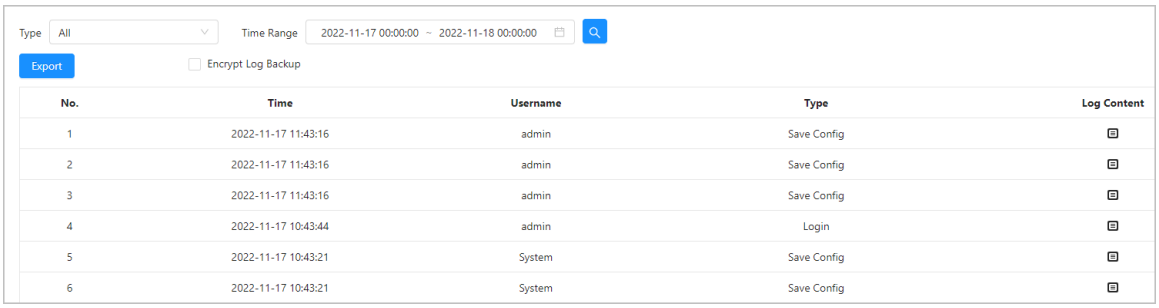
Paso 1 Inicie sesión en la página web de VTS.

Paso 2 Seleccionar**Registro**>**Registro**.

Paso 3 Seleccione el tipo de registro, configure el rango de tiempo y luego haga clic en .

- Hacer clic**Exportar**para exportar el registro a la computadora local. Si seleccionas**Cifrar copia de seguridad de registros**, ingrese la contraseña de cifrado y luego exporte el registro.
- Haga clic para ver la información del registro.

Figura 3-38 Registro del sistema



3.2.7.2 Ver el historial de llamadas

Procedimiento

Paso 1 Inicie sesión en la página web de VTS.

Paso 2 Seleccionar**Registro**>**Historial de llamadas**.

Paso 3 (Opcional) Haga clic**Exportar**para exportar el historial de llamadas a la computadora local.

3.2.7.3 Ver el registro de alarmas

Procedimiento

Paso 1 Inicie sesión en la página web de VTS.

Paso 2 Seleccionar**Registro**>**Registro**.

Paso 3 Seleccione el tipo de registro, configure el rango de tiempo y luego haga clic en .

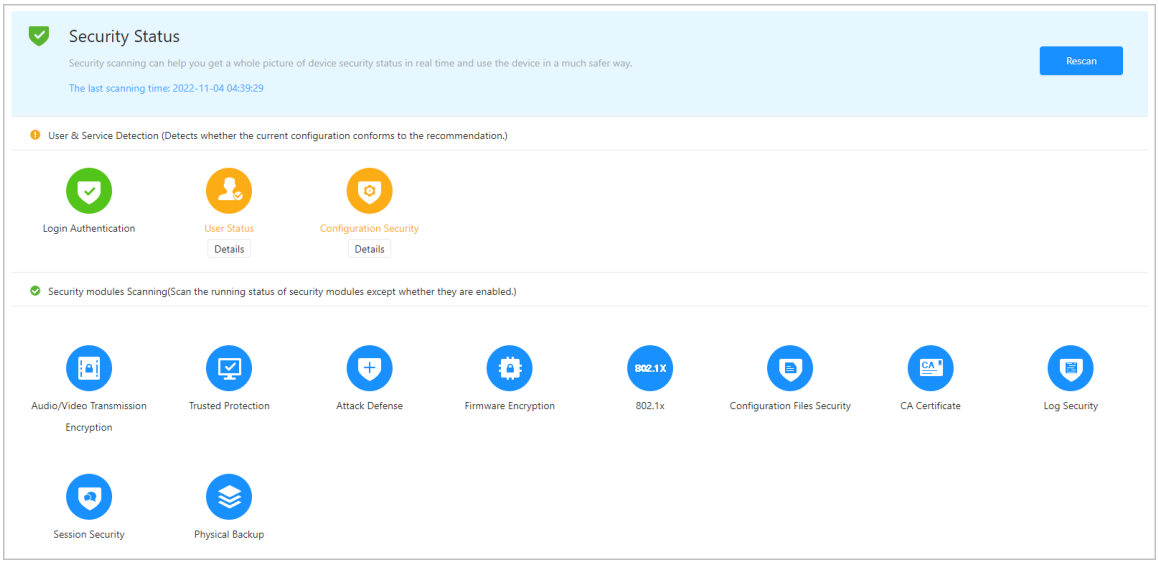
3.2.8 Seguridad

3.2.8.1 Estado de seguridad

Detectar y comprobar el estado de seguridad del dispositivo.

Inicie sesión en la página web de VTS. Seleccionar**Seguridad**>**Estado de seguridad**. Hacer clic**Volver a escanear**para escanear el estado de seguridad del dispositivo.

Figura 3-39 Estado de seguridad



Detección de usuarios y servicios

- Si la configuración del elemento de detección cumple con la recomendación, el icono es verde.
- Si es necesario optimizar el elemento de detección, el icono es amarillo. Hacer clic**Detalles**para ver los detalles del resultado del escaneo. Hacer clic**Ignorar**para ignorar la excepción y no se analizará en el siguiente análisis.
- Si el elemento de detección no se escaneará, el icono será gris. Hacer clic**Iniciar detección**para incluir el elemento de detección en el próximo escaneo.

Pase el cursor sobre el elemento de detección para ver la configuración de la detección actual.

Escaneo de módulos de seguridad

Pase el cursor sobre el icono del módulo de seguridad para ver el estado operativo.

3.2.8.2 Configuración del servicio del sistema

Información de contexto

Cree un certificado o cargue un certificado autenticado y luego podrá iniciar sesión a través de HTTPS con su PC. HTTPS puede proteger la autenticidad de la página en todo tipo de sitios web, proteger cuentas y mantener privadas las comunicaciones, la identidad y la navegación web del usuario.

Le recomendamos habilitar HTTPS. De lo contrario, es posible que se filtren los datos del dispositivo.

Procedimiento

Paso 1 Inicie sesión en la página web de VTS.

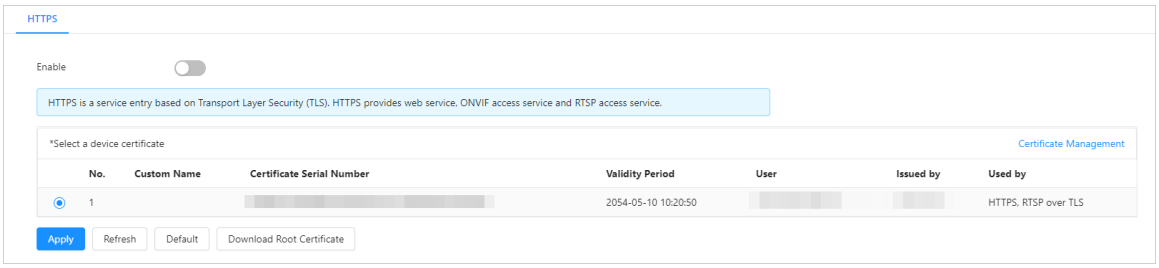
Paso 2 Seleccionar**Seguridad**>**Servicio del sistema**.

Paso 3 Haga clic para habilitar HTTPS.

Etapa 4 Seleccione el certificado.

Si no hay ningún certificado en la lista, haga clic en**Gestión de certificados**en la barra de navegación izquierda. Para obtener más información, consulte "3.2.8.4 Instalación del certificado del dispositivo".

Figura 3-40 HTTPS



Paso 5 Hacer clic**Aplicar**.

Resultados

Ingrese https://*Dirección IP: puerto https*en el navegador.

- Si ya instaló el certificado, se mostrará la página de inicio de sesión normal.
- Si no ha instalado el certificado, el navegador muestra un mensaje de error del certificado.

3.2.8.3 Defensa de ataque

3.2.8.3.1 Configuración del cortafuegos

Configure el firewall para limitar el acceso al dispositivo.

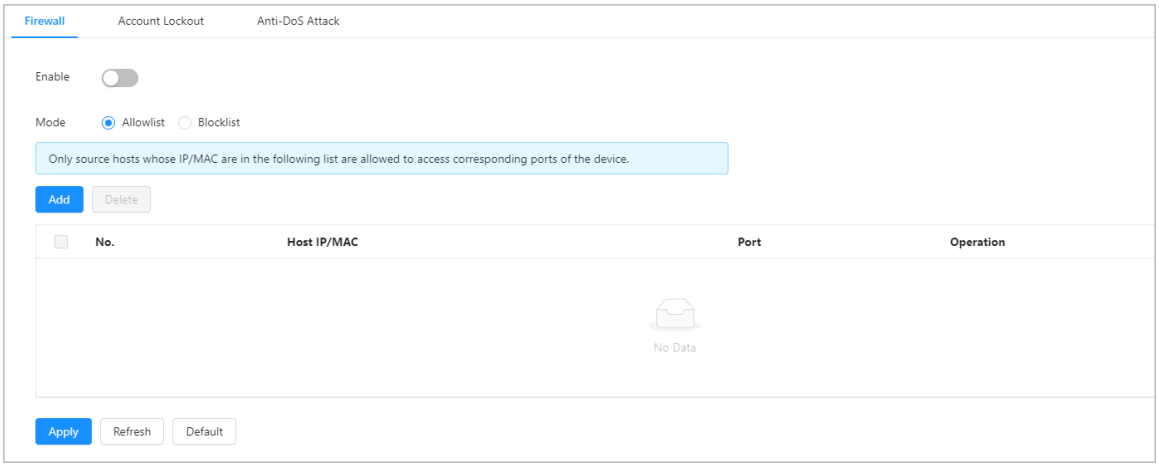
Procedimiento

Paso 1 Inicie sesión en la página web de VTS.

Paso 2 Seleccionar**Seguridad**>**Defensa de ataque**>**Cortafuegos**.

Paso 3 Haga clic para habilitar la función de firewall.

Figura 3-41 Cortafuegos

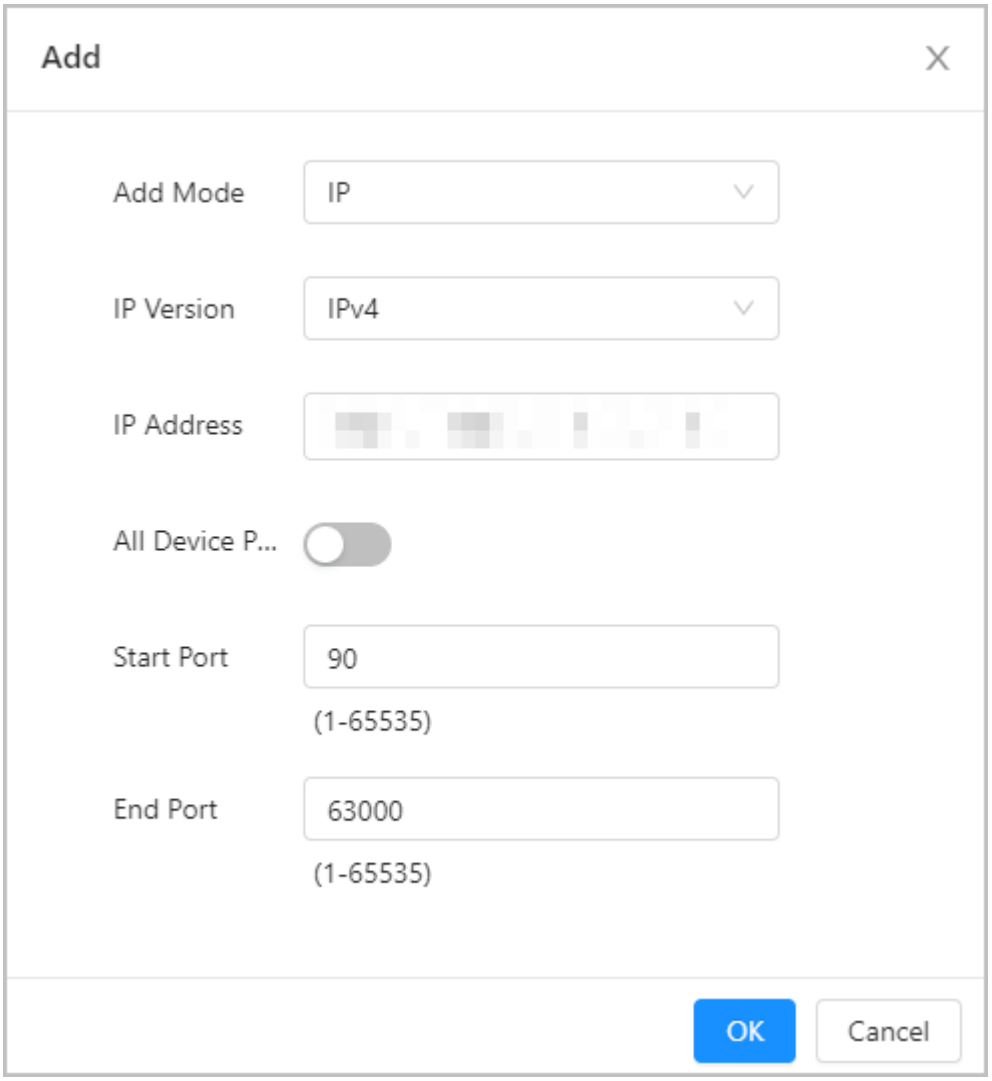


Etapa 4 Seleccionar**Lista de permitidos**o**Lista de bloqueos**como el modo.

- Lista de permitidos: Solo cuando la dirección IP/MAC de su PC esté en la lista de permitidos, podrá acceder a VTS. Los puertos son los mismos.
- Lista de bloqueo: cuando la dirección IP/MAC de su PC está en la lista de bloqueo, no puede acceder a VTS. Los puertos son los mismos.

Paso 5 Hacer clic**Agregar**para agregar la dirección IP/MAC del host a**Lista de permitidos**o**Lista de bloqueos**y luego haga clic en**DE ACUERDO**.

Figura 3-42 Agregar la dirección



Paso 6 Hacer clic**Aplicar**.

Operaciones relacionadas

- Hacer clic para editar la información del host.
- Hacer clic para eliminar la información del host.

3.2.8.3.2 Configurar el bloqueo de cuenta

Si ingresa consecutivamente una contraseña incorrecta mayor que el valor configurado, la cuenta se bloqueará.

Procedimiento

Paso 1 Inicie sesión en la página web de VTS.

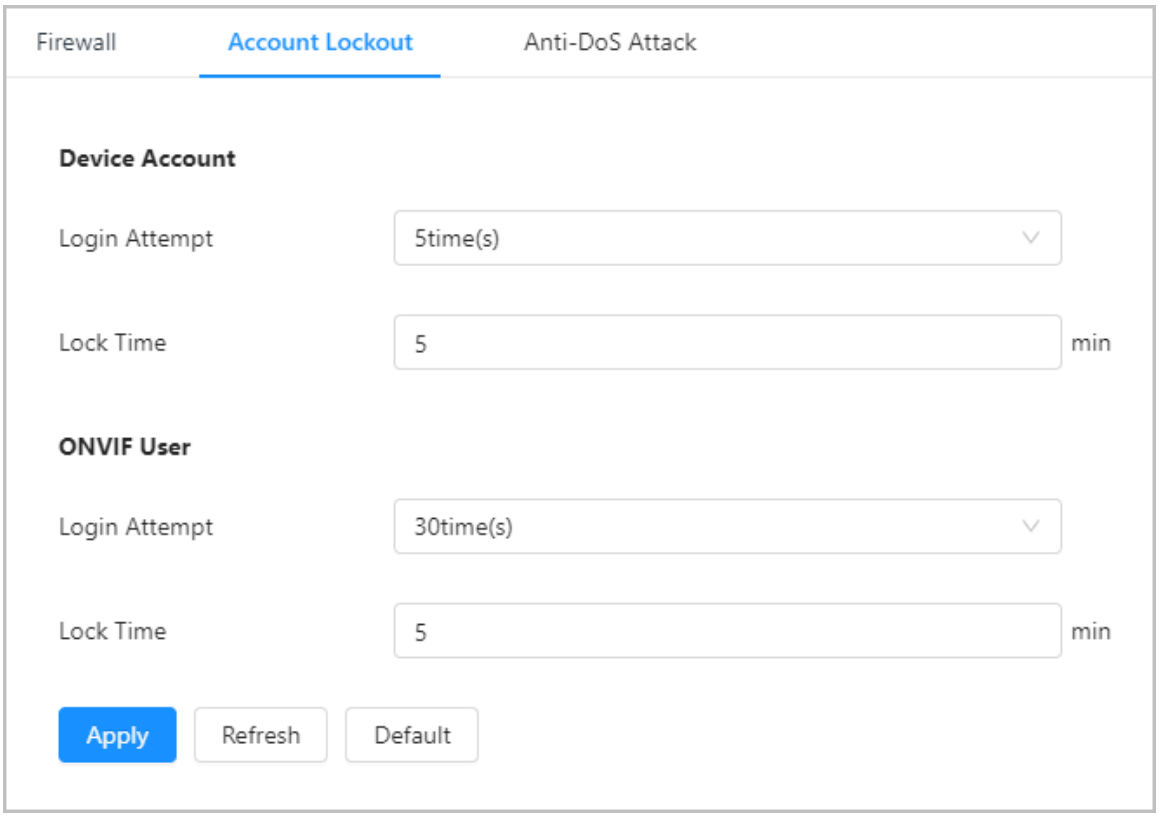
Paso 2 Seleccionar**Seguridad**>**Defensa de ataque**>**Bloqueo de cuenta**.

Paso 3 Configure el intento de inicio de sesión y el tiempo de bloqueo para la cuenta del dispositivo y el usuario de ONVIF.

- Intento de inicio de sesión: límite superior de intentos de inicio de sesión. Si ingresa consecutivamente una contraseña incorrecta mayor que el valor definido, la cuenta se bloqueará.

- Tiempo de bloqueo: el período durante el cual no puede iniciar sesión después de que los intentos de inicio de sesión alcancen el límite superior.

Figura 3-43 Bloqueo de cuenta



Etapa 4 Hacer clic**Aplicar**.

3.2.8.3.3 Configuración del ataque Anti-DoS

Puedes habilitar**Defensa contra ataques de inundación SYN**y**Defensa contra ataques de inundaciones ICMP**para defender el dispositivo contra ataques DoS (Denial of Service).

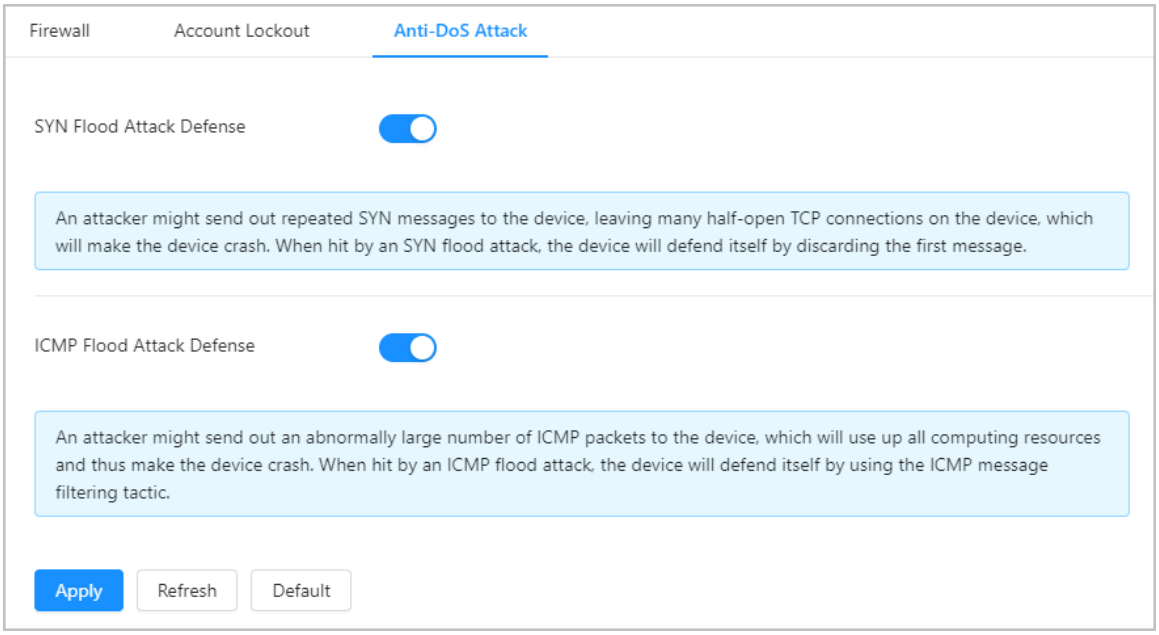
Procedimiento

Paso 1 Inicie sesión en la página web de VTS.

Paso 2 Seleccionar**Seguridad**>**Defensa de ataque**>**Ataque anti-DoS**.

Paso 3 Seleccionar**Defensa contra ataques de inundación SYN**o**Defensa contra ataques de inundaciones ICMP**para defender el dispositivo contra ataques DoS (Denial of Service).

Figura 3-44 Ataque Anti-DoS



Etapa 4 Hacer clic**Aplicar**.

3.2.8.4 Instalación del certificado del dispositivo

Cree un certificado o cargue un certificado autenticado; por ejemplo, cuando inicia sesión a través de HTTPS con su PC, debe verificar el certificado del dispositivo.

3.2.8.4.1 Creación de certificado

Procedimiento

Paso 1 Inicie sesión en la página web de VTS.

Paso 2 Seleccionar**Seguridad**>**Certificado de CA**>**Certificado de dispositivo**. Hacer

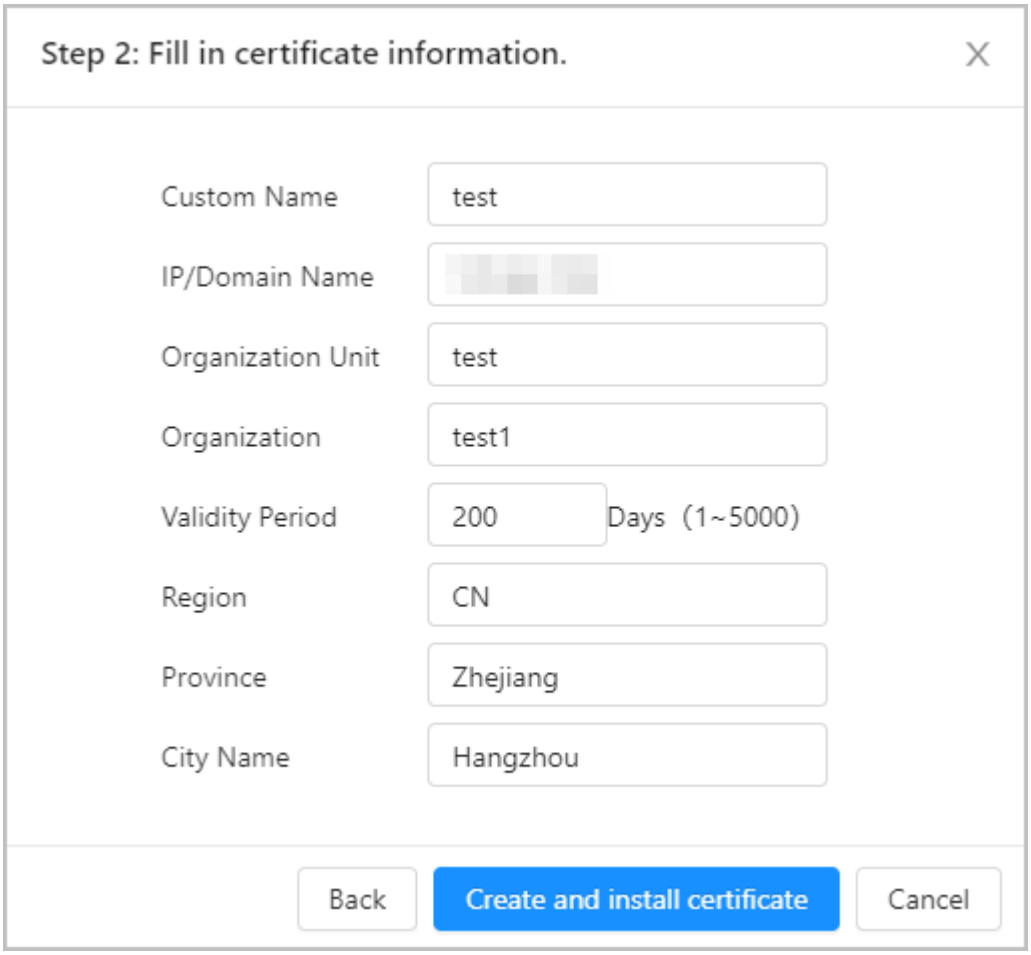
Paso 3 clic**Instalar certificado de dispositivo**.

Etapa 4 Seleccionar**Crear certificado**,y luego haga clic**Próximo**.

Paso 5 Ingrese la información del certificado.

La IP o el nombre de dominio del dispositivo se ingresa automáticamente en**IP/Nombre de dominio**.

Figura 3-45 Información del certificado (1)



Paso 6 Hacer clic**Crear e instalar certificado**.

Una vez que el certificado se haya creado correctamente, podrá ver el certificado creado en la página **Certificado de dispositivo**página.

Operaciones relacionadas

- Hacer clic**Ingrese al modo de edición**para editar el nombre personalizado del certificado.
- Hacer clic para descargar el certificado.
- Hacer clic para eliminar el certificado.

3.2.8.4.2 Solicitud e importación de certificado de CA

Importe el certificado de CA de terceros al dispositivo.

Procedimiento

Paso 1 Inicie sesión en la página web de VTS.

Paso 2 Seleccionar**Seguridad**>**Certificado de CA**>**Certificado de dispositivo**. Hacer

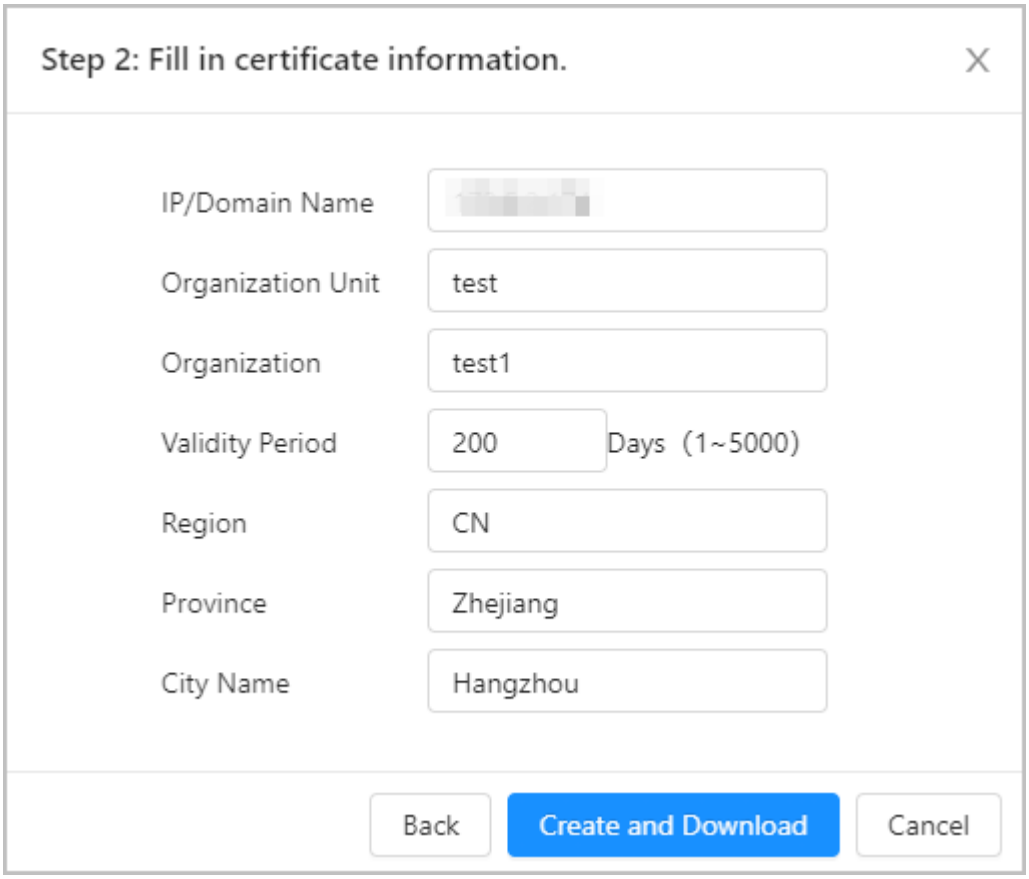
Paso 3 clic**Instalar certificado de dispositivo**.

Etapa 4 Seleccionar**Solicite certificado de CA e importación (recomendado)**,y luego haga clic**Próximo**.

Paso 5 Ingrese la información del certificado.

La IP o el nombre de dominio del dispositivo se ingresa automáticamente en**IP/Nombre de dominio**.

Figura 3-46 Información del certificado (2)



Paso 6 Hacer clic**Crear y descargar**.

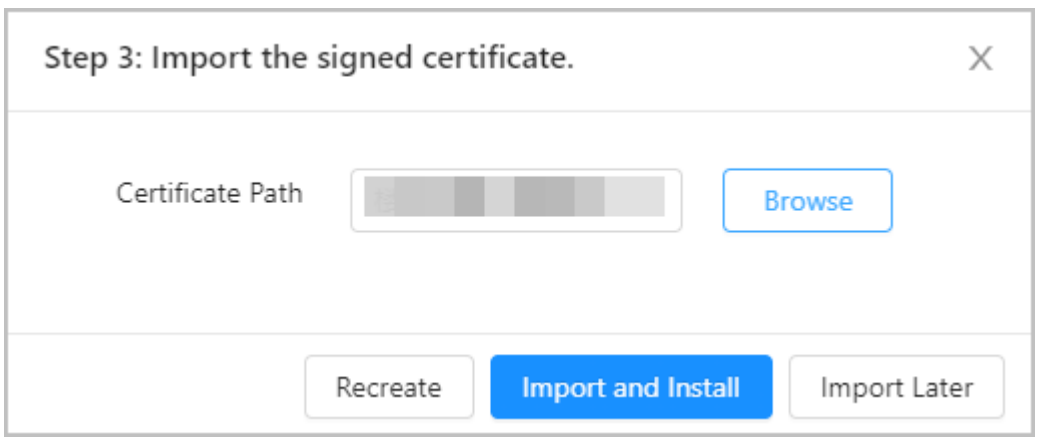
Guarde el archivo de solicitud en su PC.

Paso 7 Solicite el certificado de CA de la autoridad certificadora de terceros.

Paso 8 Importe el certificado de CA firmado.

1. Guarde el certificado de CA en la PC.
2. Seleccione**Instalar certificado de dispositivo**,hacer clic**Solicite certificado de CA e importación (recomendado)**y luego haga clic en**Próximo**.
3. Haga clic**Navegar**para seleccionar el certificado de CA firmado.

Figura 3-47 Importar el certificado de CA firmado



4. Haga clic**Importar e instalar**.

Una vez que el certificado se haya creado correctamente, podrá ver el certificado creado en la página **Certificado de dispositivo**página.

- Hacer clic**Recrear**para crear el archivo de solicitud nuevamente.
- Hacer clic**Importar más tarde**para importar el certificado la próxima vez.

Operaciones relacionadas

- Hacer clic**Ingrese al modo de edición**para editar el nombre personalizado del certificado.
- Hacer clic  para descargar el certificado.
- Hacer clic  para eliminar el certificado.

3.2.8.4.3 Instalación del certificado existente

Importe el certificado de terceros existente al dispositivo. Cuando solicite el certificado de terceros, también deberá solicitar el archivo de clave privada y la contraseña de clave privada.

Procedimiento

Paso 1 Inicie sesión en la página web de VTS.

Paso 2 Seleccionar**Seguridad**>**Certificado de CA**>**Certificado de dispositivo**. Hacer

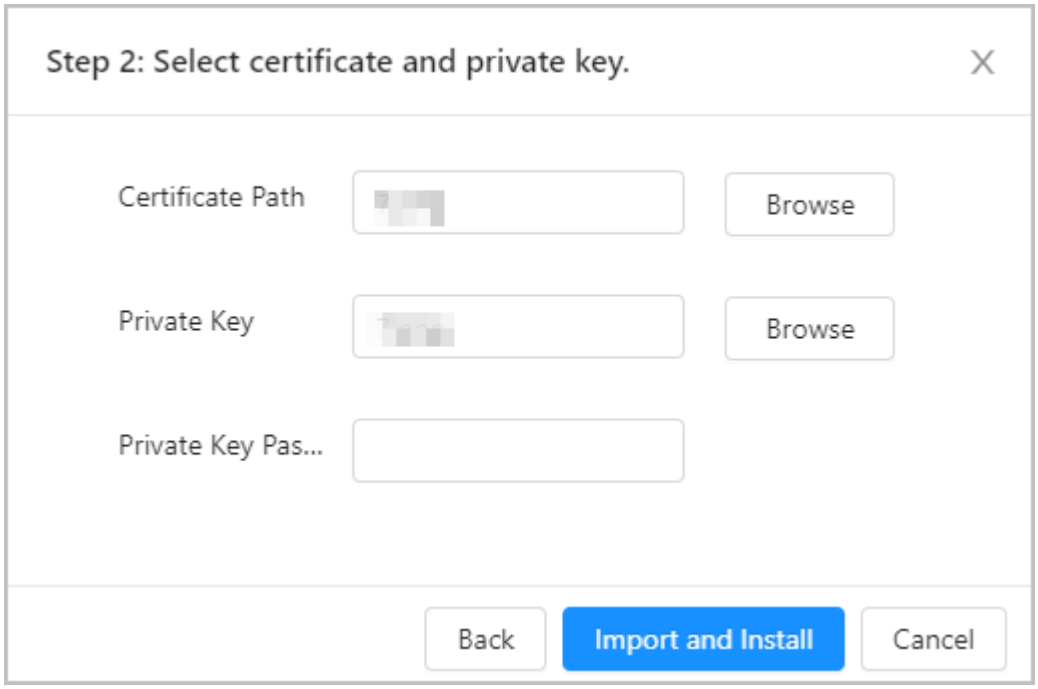
Paso 3 clic**Instalar certificado de dispositivo**.

Etapa 4 Seleccionar**Instalar certificado existente**,y luego haga clic**Próximo**. Hacer clic

Paso 5 **Navegar**para seleccionar el certificado y el archivo de clave privada.

Ingrese la contraseña de la clave privada si el archivo de clave privada está cifrado.

Figura 3-48 Certificado y clave privada



Operaciones relacionadas

- Hacer clic**Ingrese al modo de edición**para editar el nombre personalizado del certificado.
- Hacer clic  para descargar el certificado.

- Hacer clic para eliminar el certificado.

3.2.8.5 Instalación del certificado de CA confiable

El certificado CA es un certificado digital para la identidad legal de la cámara. Por ejemplo, cuando la cámara accede a la LAN a través de 802.1x, se requiere el certificado CA.

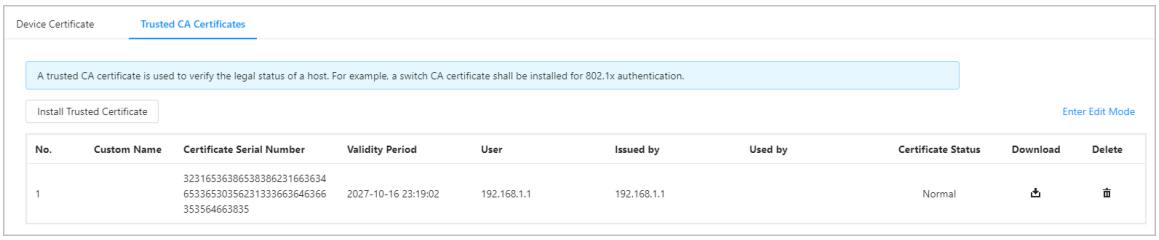
Procedimiento

Paso 1 Inicie sesión en la página web de VTS.

Paso 2 Seleccionar**Seguridad**>**Certificado de CA**>**Certificado de CA de confianza**. Hacer

Paso 3 clic**Instalar certificado de confianza**.

Figura 3-49 Instalar certificado confiable



Etapa 4 Hacer clic**Navegar**en la ventana emergente para seleccionar el certificado. Hacer clic

Paso 5 **DE ACUERDO**para importar el certificado de confianza.

Una vez que el certificado se haya importado correctamente, podrá verlo en la página **Certificado de CA de confianza**página.

Operaciones relacionadas

- Hacer clic**Ingrese al modo de edición**para editar el nombre personalizado del certificado.
- Hacer clic para descargar el certificado.
- Hacer clic para eliminar el certificado.

3.2.8.6 Configurar el cifrado de vídeo

El dispositivo admite cifrado de audio y video durante la transmisión de datos.

Información de contexto

Le recomendamos habilitar la función de cifrado de video. Puede haber riesgos para la seguridad si esta función está desactivada.

Procedimiento

Paso 1 Inicie sesión en la página web de VTS.

Paso 2 Seleccionar**Seguridad**>**Cifrado de vídeo**.

Paso 3 Configure los parámetros.

Figura 3-50 Cifrado de vídeo

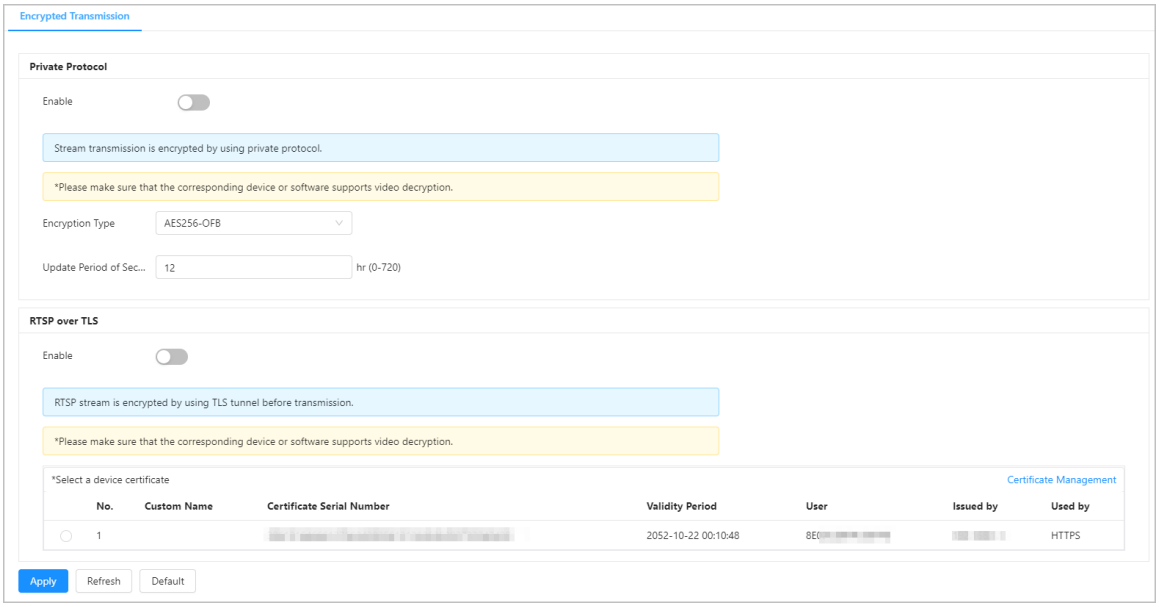


Tabla 3-20 Descripción de los parámetros de cifrado de video

Área	Parámetro	Descripción
Protocolo privado	Permitir	Habilite el cifrado de tramas de flujo mediante un protocolo privado. Hacer clic para habilitar el cifrado de audio y vídeo durante transmisión de datos. Seleccione el tipo de cifrado y luego configure el período de actualización de la clave secreta. ● **Tipo de cifrado**:Utilice la configuración predeterminada. ● **Período de actualización de la clave secreta**:El rango de valores es de 0 a 720 horas. 0 significa nunca actualizar la clave secreta.
	Tipo de cifrado	
	Período de actualización de Llave secreta	
RTSP sobre TLS	Permitir	Habilita el cifrado de flujo RTSP mediante TLS. Hacer clic y luego seleccione un certificado de dispositivo de lista de certificados.
	Certificado Gestión	Para obtener detalles sobre la administración de certificados, consulte "3.2.8.4 Instalación del certificado del dispositivo". El certificado creado del certificado importado se muestra en**Seleccione un certificado de dispositivo**lista.

4 escenas industriales

4.1 Operaciones en el dispositivo local

Este capítulo presenta diferentes configuraciones en la escena industrial. Otras configuraciones son las mismas que en la escena de los edificios.

4.1.1 Pantalla local

Figura 4-1 Pantalla local

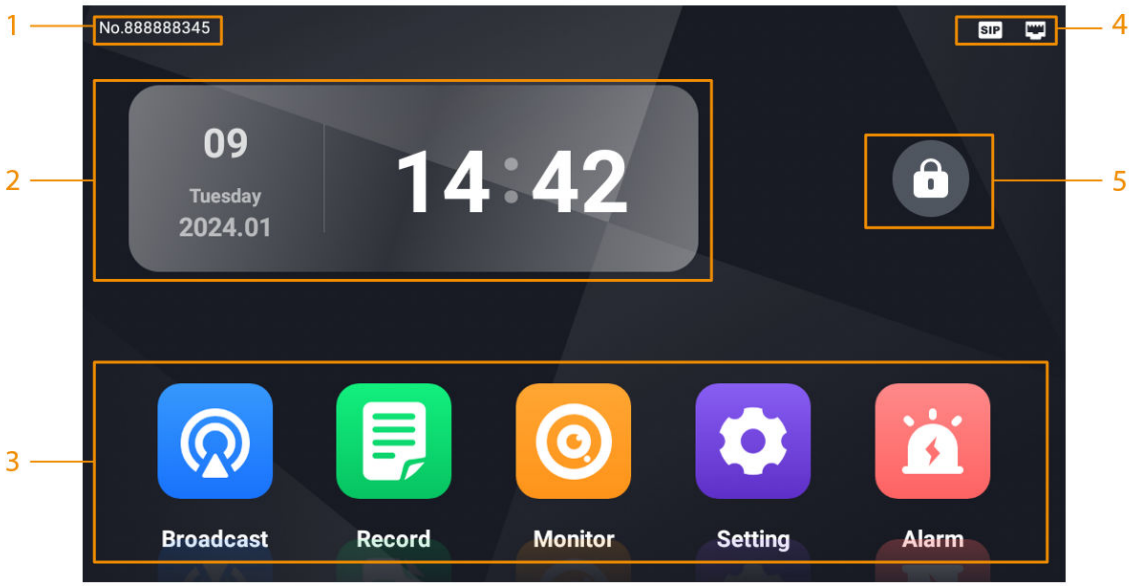


Tabla 4-1 Introducción a la pantalla de inicio

No.	Descripción
1	El número de VTS.
2	Fecha y hora.
3	Botones de función. ● Transmisión: reproduzca la transmisión de voz o manual en parte de los dispositivos terminales o en todos los dispositivos terminales. Para obtener más información, consulte "4.1.5.1 Difusión". ● Grabar: verifique el historial de llamadas, archivos de video y archivos de instantáneas. Para obtener más información, consulte "4.1.5.2 Registro". ● Monitorear: Monitorear VTA e IPC. Para obtener más información, consulte "4.1.5.3 Supervisión". ● Configuración: Ingrese a la pantalla de configuración de VTS. Para obtener más información, consulte "4.1.4 Configuración del proyecto". ● Alarma: Muestra los mensajes de alarma reportados por el VTA.

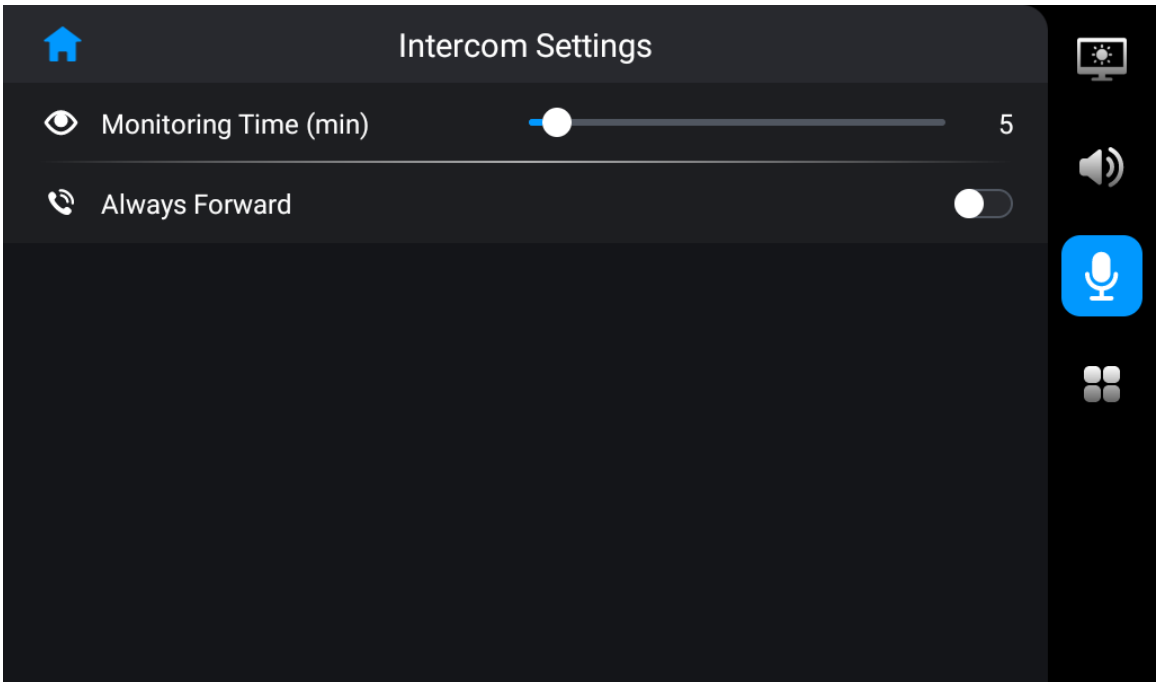
No.	Descripción
4	Grifo  para bloquear la pantalla. Si seleccionas**Configuración**>**Configuración de pantalla**y enciende**Bloquear pantalla**,necesitas ingresar la contraseña predeterminada**123456**para desbloquear la pantalla cuando la bloquea después de la configuración.
5	El estado de conexión de la red, el servidor SIP y la tarjeta SD.

4.1.2 Configuración de los parámetros del intercomunicador

En la pantalla de inicio, seleccione**Configuración**> .

- El servidor SIP no está habilitado: los parámetros son los mismos que los parámetros de la escena del edificio. Para obtener más información, consulte "3.1.4 Configuración de los parámetros del intercomunicador".
- El servidor SIP está habilitado: puede habilitar o deshabilitar**Siempre hacia adelante**. Una vez habilitada, la llamada se reenviará a otros dispositivos que haya configurado en la plataforma.

Figura 4-2 Configuración de intercomunicador



4.1.3 Configuración de los parámetros avanzados

Las configuraciones de los ajustes avanzados son las mismas que en la escena de edificios. Para obtener más información, consulte "3.1.5 Configuración de los parámetros avanzados".

Recibir información de alarma de VTHno está disponible en la escena industrial.

4.1.4 Configuración del proyecto

4.1.4.1 Configuración del VTS

Configure el número y los parámetros de red de VTS.

Procedimiento

Paso 1 Seleccionar**Ajustes**>  > **Configuración del proyecto**en la pantalla de inicio.

Paso 2 Ingrese la contraseña y luego toque**DE ACUERDO**.

Paso 3 Grifo  y luego configure los parámetros.

Figura 4-3 Configurar los parámetros

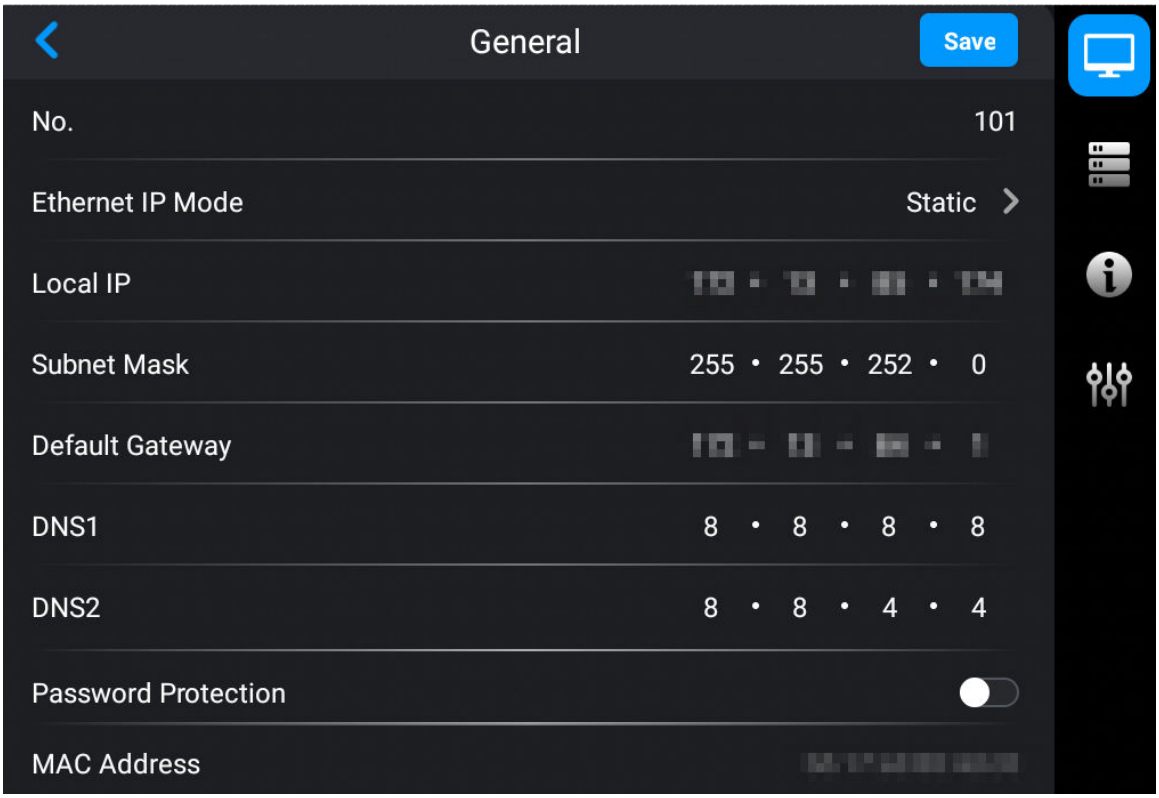


Tabla 4-2 Descripción de los parámetros VTS

Parámetro	Descripción
No.	Usuario definido. Puedes configurar el número del 101 al 999.
Modo IP Ethernet	Configure el modo para obtener la IP. ● Estático: configurado manualmente**IP local**,**Máscara de subred**y**Puerta de enlace predeterminada**. ● DHCP (Protocolo de configuración dinámica de host): seleccione**DHCP**si hay un servidor DHCP. El dispositivo obtiene automáticamente una dirección IP dinámica.
IP local	Si seleccionas**Estático**en**Modo IP Ethernet**, configure la dirección IP, la máscara de subred y la puerta de enlace predeterminada de acuerdo con la planificación de la red.
Máscara de subred	

Parámetro	Descripción
Puerta de enlace predeterminada	
DNS 1	Dirección IP del servidor DNS.
DNS 2	Dirección IP en espera del servidor DNS.
Protección de contraseña	Active la protección con contraseña. La contraseña se transfiere encriptada cuando el dispositivo se registra en la plataforma a través de SIP.

4.1.4.2 Configuración de protocolos

Procedimiento

Paso 1 Seleccionar**Ajustes**>  > **Configuración del proyecto**en la pantalla de inicio.

Paso 2 Ingrese la contraseña y luego toque**DE ACUERDO**.

Paso 3 Grifo  y luego configure los parámetros.

- Si VTS no necesita la plataforma para conectarse, seleccione**Protocolo privado**.
- Si VTS está conectado a la plataforma a través de un acuerdo SIP, seleccione**Servidor SIP**y luego configure los parámetros.

Tabla 4-3 Descripción de los parámetros del servidor SIP

Parámetro	Descripción
Dirección IP	Dirección IP del servidor SIP.
Puerto de red	Número de puerto de red del servidor SIP. La plataforma como servidor SIP: 5080.
Nombre de usuario	Por defecto.
Contraseña	Por defecto.
Nombre de dominio	Mantenga la coherencia con el servidor SIP. VDP por defecto.

Etapa 4 Grifo**Ahorrar**.

4.1.5 Puesta en servicio

4.1.5.1 Radiodifusión

Reproduzca la transmisión de voz o manual en parte de los dispositivos terminales o en todos los dispositivos terminales.

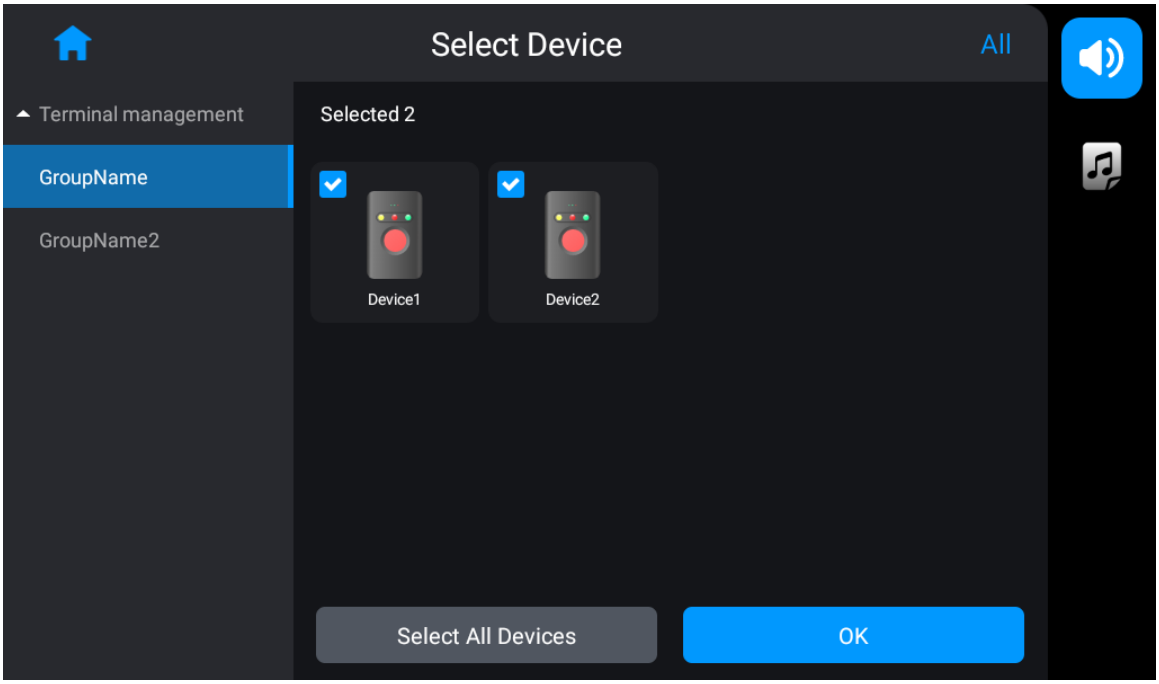
4.1.5.1.1 Difusión en parte de los dispositivos

Procedimiento

Paso 1 Grifo**Transmisión**en la pantalla de inicio de VTS. Seleccione

Paso 2 los dispositivos terminales y luego toque**DE ACUERDO**.

Figura 4-4 Seleccione los dispositivos terminales



Paso 3 Seleccionar**Tipo de transmisión**,y luego toque**Iniciar transmisión**.

- Archivo de audio: seleccione el audio en la lista de archivos de audio y luego toque**Iniciar transmisión**para reproducir el audio.
- Transmisión manual: toque**Iniciar transmisión**y luego toque para transmitir.

Figura 4-5 Transmisión de audio

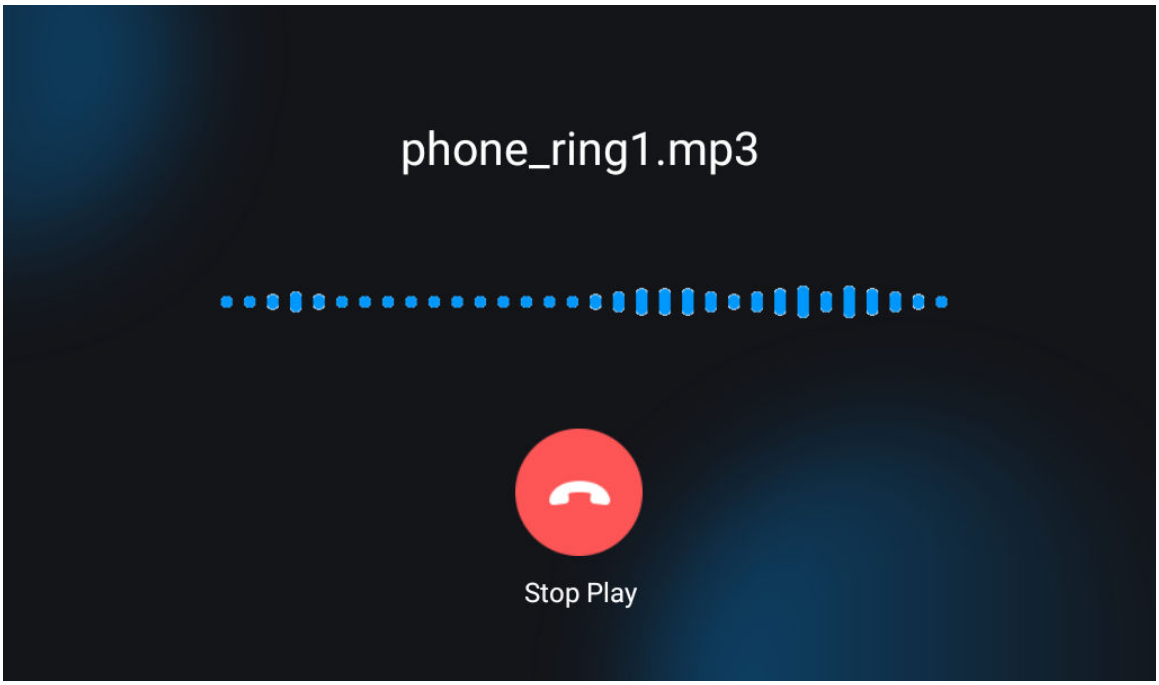
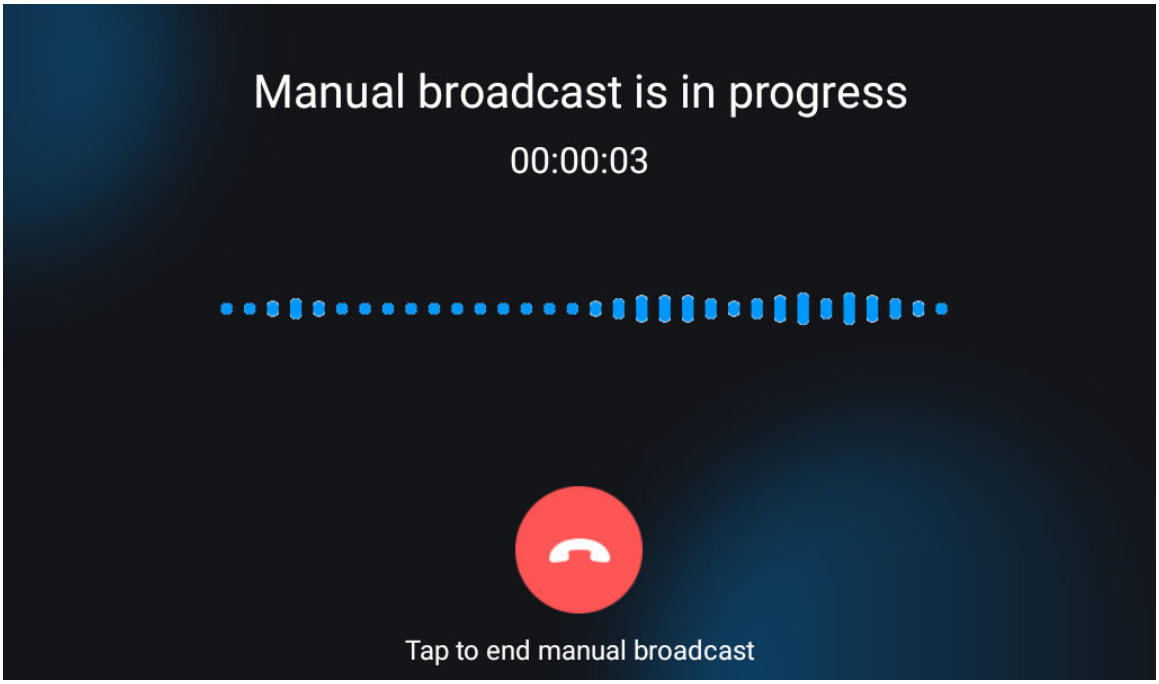


Figura 4-6 Transmisión manual



4.1.5.1.2 Transmitir en todos los dispositivos

Procedimiento

Paso 1 Grifo**Transmisión**en la pantalla de inicio de VTS. Grifo

Paso 2 **Seleccionar todos los dispositivos**.

Paso 3 Seleccionar**Tipo de transmisión**y luego iniciar la transmisión.

- Archivo de audio: seleccione el audio en la lista de archivos de audio y luego toque**Iniciar transmisión**para reproducir el audio.
- Transmisión manual: toque**Iniciar transmisión**y luego toque  para transmitir.

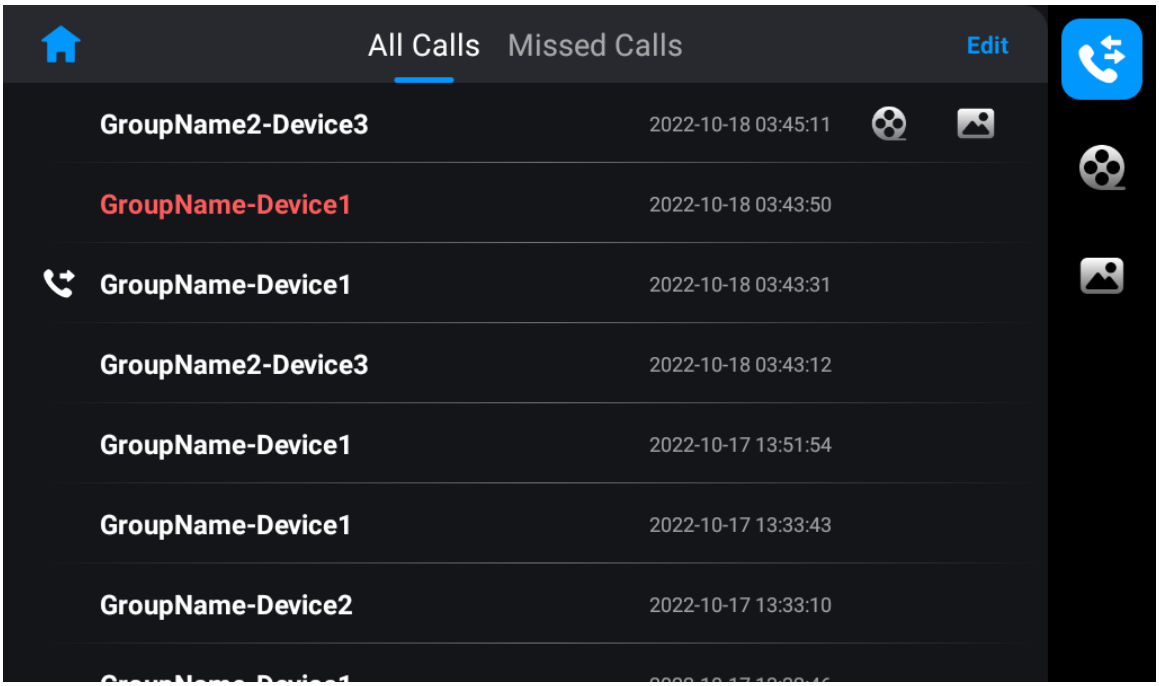
4.1.5.2 Registro

Verifique el historial de llamadas, los registros de llamadas perdidas, los archivos de video y los archivos de instantáneas.

Historial de llamadas

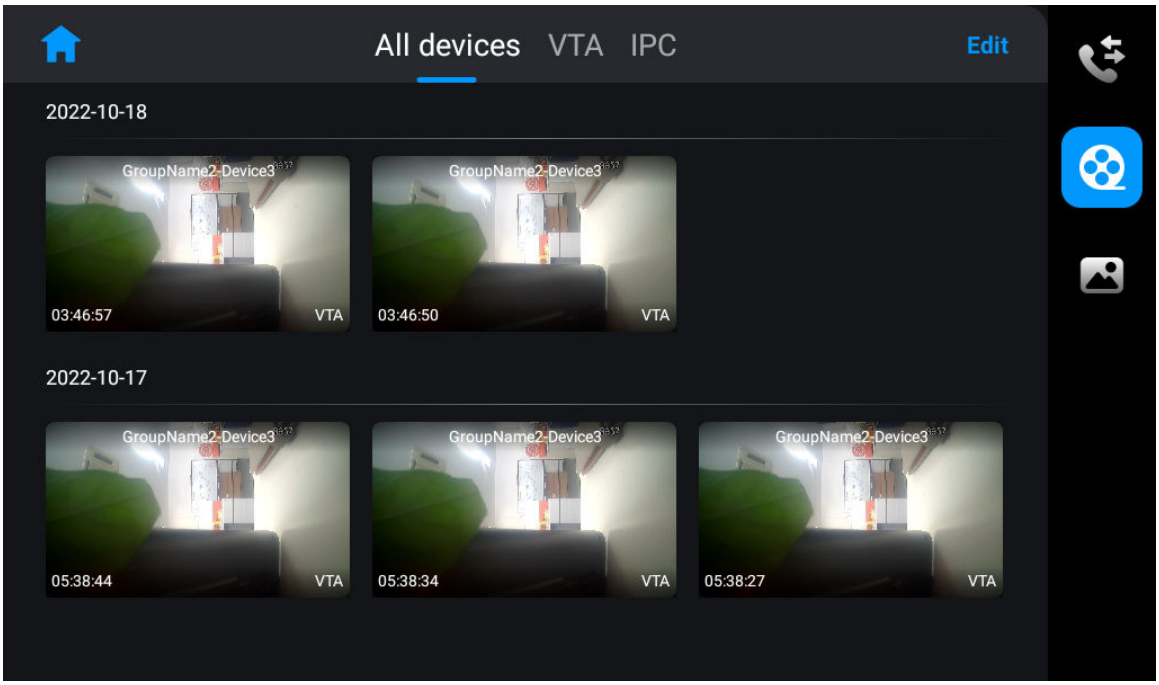
- Toque la llamada en la lista del historial de llamadas para devolver la llamada.
-  : Verifique los archivos de instantáneas de la llamada.
-  : Consulta los archivos de vídeo de la llamada.

Figura 4-7 Historial de llamadas



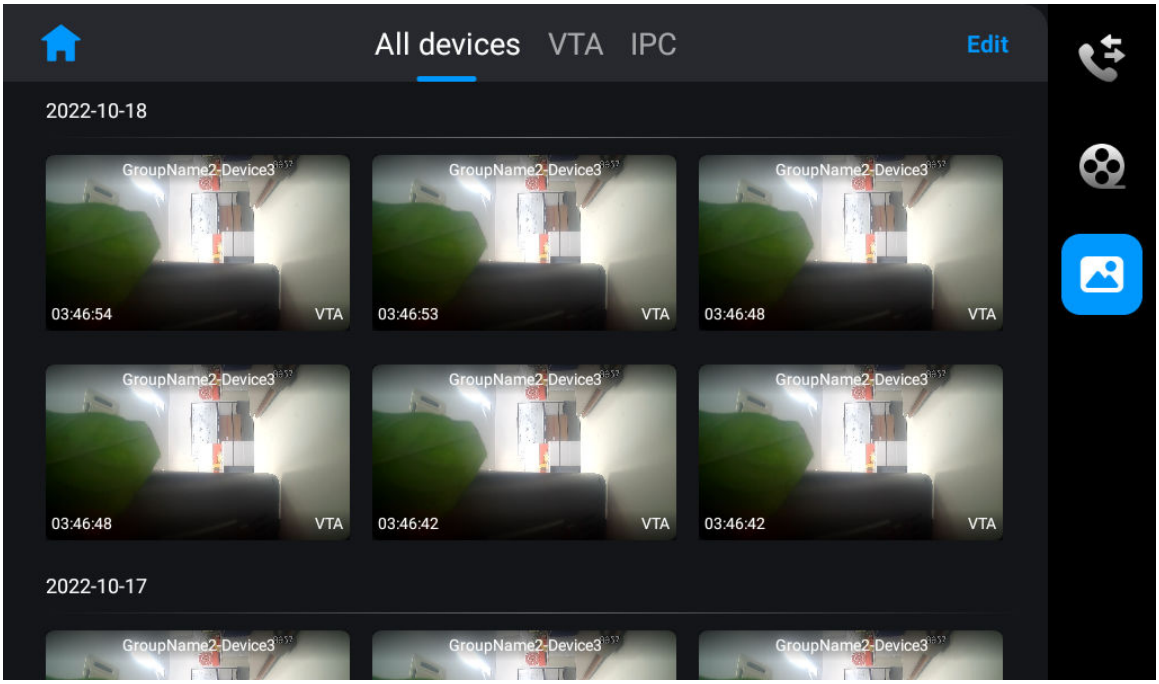
Video

Figura 4-8 Archivos de vídeo



Instantánea

Figura 4-9 Archivos de instantáneas



4.1.5.3 Monitoreo

- VTS como VTS de nivel inferior: puede monitorear y llamar a VTA. IPC y VTA reciben la llamada.
- VTS como VTS de nivel superior: puede monitorear y llamar a VTA.

Utilice la supervisión de VTA como ejemplo.

Grifo**Monitor**en la pantalla de inicio de VTS y luego toque el ícono de VTA.

Figura 4-10 Monitorear VTA

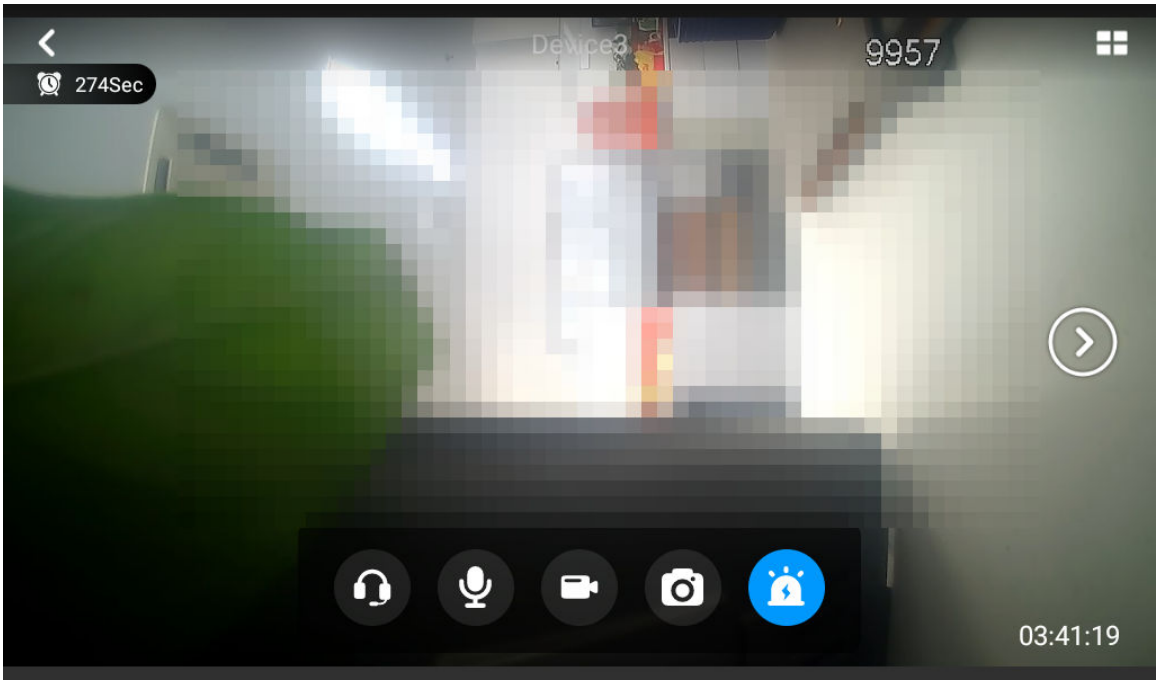


Tabla 4-4 Descripción de la imagen de monitoreo

Icono	Descripción
	Toque para ver la imagen de monitoreo en 4 ventanas.
	Toque para convertir a una imagen de monitoreo de otros dispositivos terminales si VTS conecta más de un dispositivo terminal.
	Toque para recibir el audio de VTA.
	Hable con el dispositivo par.
	Toque para iniciar la grabación manual.
	Toque para tomar una instantánea manualmente.
	Controla el indicador de alarma de VTA. ●  El indicador de alarma está encendido. ●  El indicador de alarma está apagado.

4.2 Operaciones en la página web

Esta sección presenta diferentes configuraciones de VTS en el escenario industrial. Otras configuraciones son las mismas que en la escena de los edificios.

4.2.1 Configuración de la función del dispositivo

Procedimiento

Paso 1 Inicie sesión en la página web del dispositivo.

Paso 2 Seleccionar**Sistema**>**General**. Configure los

Paso 3 parámetros.

Figura 4-11 Configurar los parámetros

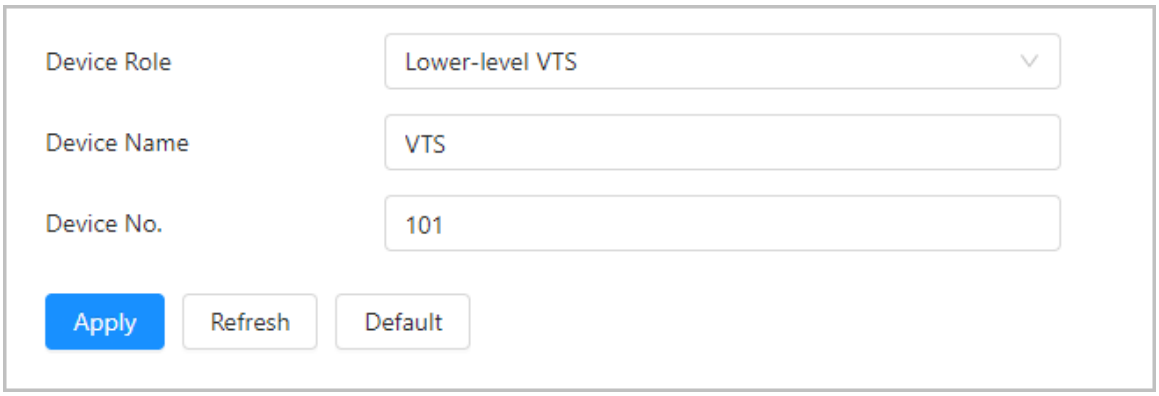


Tabla 4-5 Descripción de los parámetros de función del dispositivo

Parámetro	Descripción
Rol del dispositivo	Seleccione entre VTS de nivel inferior, VTS de nivel superior y cliente de plataforma. La información guardada en el dispositivo se borrará después de cambiar la función del dispositivo. ● VTS de nivel inferior: Se utiliza como VTS de nivel inferior si no hay plataforma. Tiene el permiso de gestión del dispositivo. Puede agregar VTA e IPC. Las operaciones para agregar IPC son las mismas que en la escena de edificios. ● VTS de nivel superior: Se utiliza como VTS de nivel superior si no hay plataforma. Tiene permisos para agregar VTS de nivel inferior. No tiene permiso para gestionar la estructura organizativa. Puede agregar VTS de nivel inferior. ● Cliente de plataforma: Se utiliza como cliente de plataforma si existe la plataforma. No tiene el permiso de gestión del dispositivo.
Nombre del dispositivo	Puedes configurar el nombre que distingue el dispositivo.
Dispositivo No.	Puedes configurar el número del 101 al 999.

Etapa 4 Hacer clic**Aplicar**.

4.2.2 Configurar el servidor SIP

Configure los parámetros del servidor SIP. Conéctese a VTA a través del acuerdo SIP para lograr un videoportero.

Procedimiento

Paso 1 Inicie sesión en la página web de VTS.

Paso 2 Seleccionar**Configuración de la red**>**Servidor**

Paso 3 **SIP**. Configure los parámetros.

Figura 4-12 Parámetros del servidor SIP

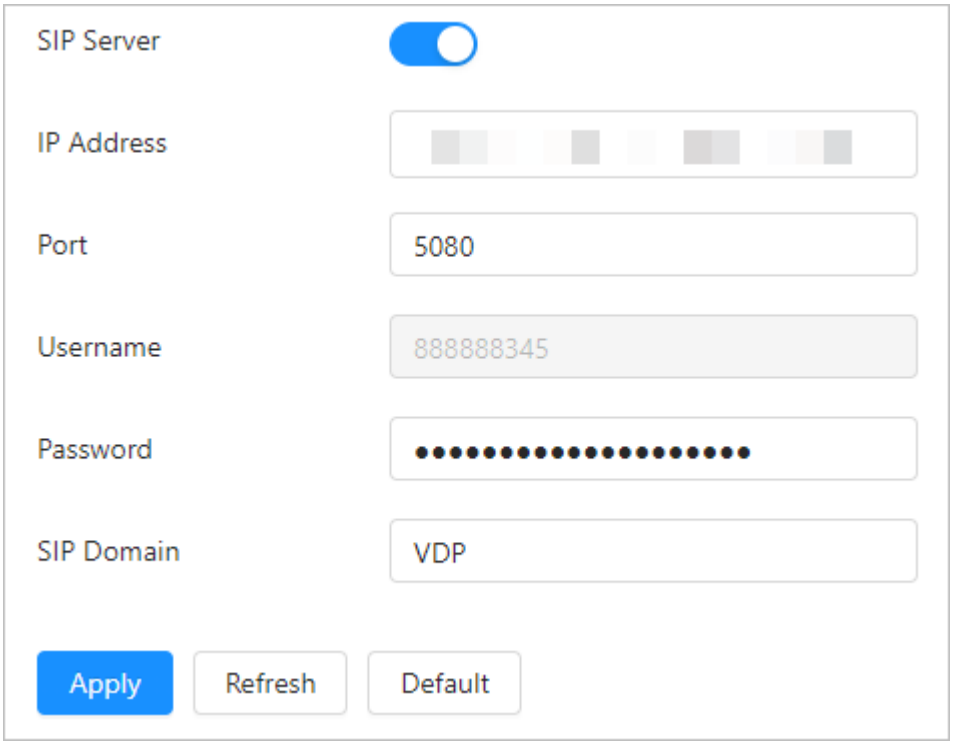


Tabla 4-6 Descripción de los parámetros

Parámetro	Descripción
Dirección IP	Dirección IP del servidor SIP.
Puerto	Número de puerto de red del servidor SIP. La plataforma como servidor SIP: 5080.
Nombre de usuario	Por defecto.
Contraseña	Por defecto.
Dominio SIP	Mantenga la coherencia con el servidor SIP. El nombre de dominio es VDP de forma predeterminada.

Etapa 4 Grifo**Ahorrar**.

4.2.3 Configuración de FTP

Obtenga el archivo de audio de FTP y reprodúzcalo.

Si el servidor SIP está habilitado, esta función no se mostrará.

Procedimiento

Paso 1 Inicie sesión en la página web. Seleccionar

Paso 2 **Configuración de la red**>**ftp**.

Paso 3 Encender**Permitir**y luego configure la dirección IP, el puerto, el nombre de usuario y la contraseña. Hacer clic

Etapa 4 **Aplicar**.

4.2.4 Configuración del dispositivo

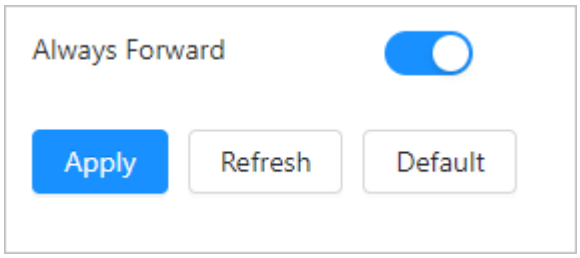
4.2.4.1 Uso con la plataforma

Cuando utilice el dispositivo con la plataforma, habilite el servidor SIP y luego configure los parámetros.

4.2.4.1.1 Desvío de llamadas

Inicie sesión en la página web de VTS y luego seleccione**Configuración del dispositivo**>**Reenvío de llamadas**. Permitir **Siempre hacia adelante**,y luego haga clic**Aplicar**. Configure el dispositivo que recibe la llamada desviada y la llamada será desviada.

Figura 4-13 Desvío de llamadas



4.2.4.1.2 Gestión de dispositivos

Procedimiento

Paso 1 Inicie sesión en la página web.

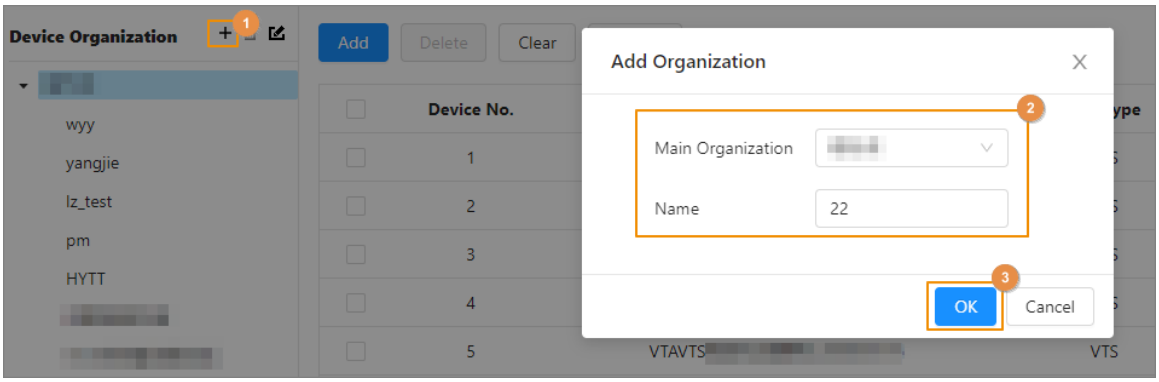
Paso 2 Seleccionar**Configuración del dispositivo**>**Configuración del dispositivo**.

Se muestran los dispositivos que envía la plataforma.

Paso 3 (Opcional) Agregue la organización.

1. Haga clic**+**.
2. Seleccione la organización principal y luego ingrese el nombre.
3. Haga clic**DE ACUERDO**.

Figura 4-14 Agregar la organización



Etapa 4 (Opcional) Agregue el dispositivo.

Puede agregar VTS y VTA.

- VTS: Utilizado como contactos.
- VTA: Puede llamar y monitorear VTA en el VTS.

1. Haga clic**Agregar**.
2. Configure los parámetros y luego haga clic en**DE ACUERDO**.

4.2.4.2 Uso sin la plataforma

Cuando utilice el dispositivo sin la plataforma, configure la función del dispositivo como VTS de nivel inferior o VTS de nivel superior.

4.2.4.2.1 Desvío de llamadas

Gestionar el desvío y recepción de la llamada entre los dispositivos VTS.

Cuando la llamada del dispositivo A se reenvía al dispositivo B, configure**Reenvío**en el dispositivo A y luego configurar**Recepción**en el dispositivo B. Si solo configura un lado, esa llamada no se reenviará.

Reenvío

Configure el desvío y la llamada del VTS actual se confiará o reenviará al VTS que configuró.

1. Inicie sesión en la página web.
2. Seleccione**Configuración del dispositivo**>**Reenvío de llamadas**>**Reenvío**.
3. Haga clic**Agregar**.
4. Configure los parámetros.

Figura 4-15 Agregar el VTS para reenviar la llamada

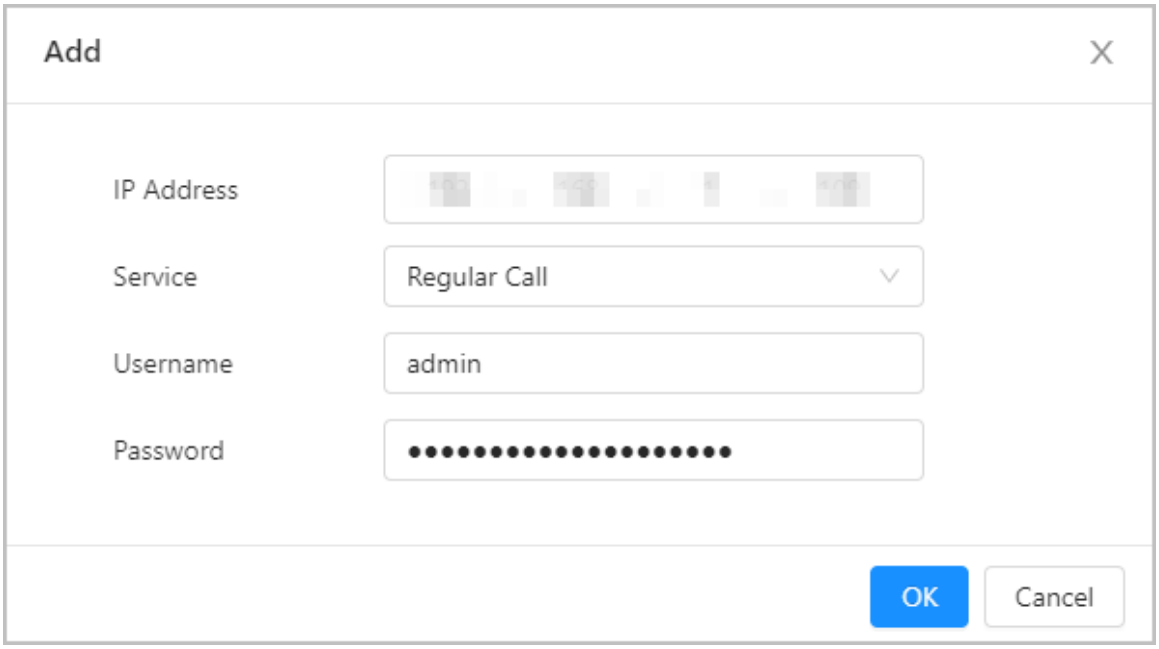


Tabla 4-7 Descripción de los parámetros de reenvío

Parámetro	Descripción
Dirección IP	La dirección IP del VTS que recibe la llamada de reenvío.

Parámetro	Descripción
Servicio	• Llamada regular: Intercomunicador entre VTS y otros VTS. • Encomendar: Todas las llamadas del VTS actual se reenviarán a otros VTS. • Desvío de llamadas: si el VTS actual perdió la llamada, la llamada se desviará a otro VTS.
Nombre de usuario	El nombre de usuario y la contraseña del VTS que recibe la llamada de desvío.
Contraseña	

5. Haga clic**DE ACUERDO**.

Recepción

Configure la recepción y el VTS actual recibirá la llamada que el VTS par confió o reenvió.

1. Inicie sesión en la página web.
2. Seleccione**Configuración del dispositivo**>**Reenvío de llamadas**>**Recepción**.
3. Haga clic**Agregar**.
4. Ingrese la dirección IP, nombre de usuario y contraseña de otro VTS.
5. Haga clic**DE ACUERDO**.

4.2.4.2.2 Agregar VTA

Cuando el dispositivo está configurado como VTS de nivel inferior, puede agregar VTA e IPC. Las operaciones para agregar IPC son las mismas que las operaciones en la escena del edificio. Esta sección presenta las operaciones de agregar VTA.

Procedimiento

Paso 1 Inicie sesión en la página web de VTS.

Paso 2 Seleccionar**Configuración del dispositivo**>**Gestión de**

Paso 3 **terminales**. Hacer clic**Agregar**y luego configure los parámetros.

Figura 4-16 Agregar VTA

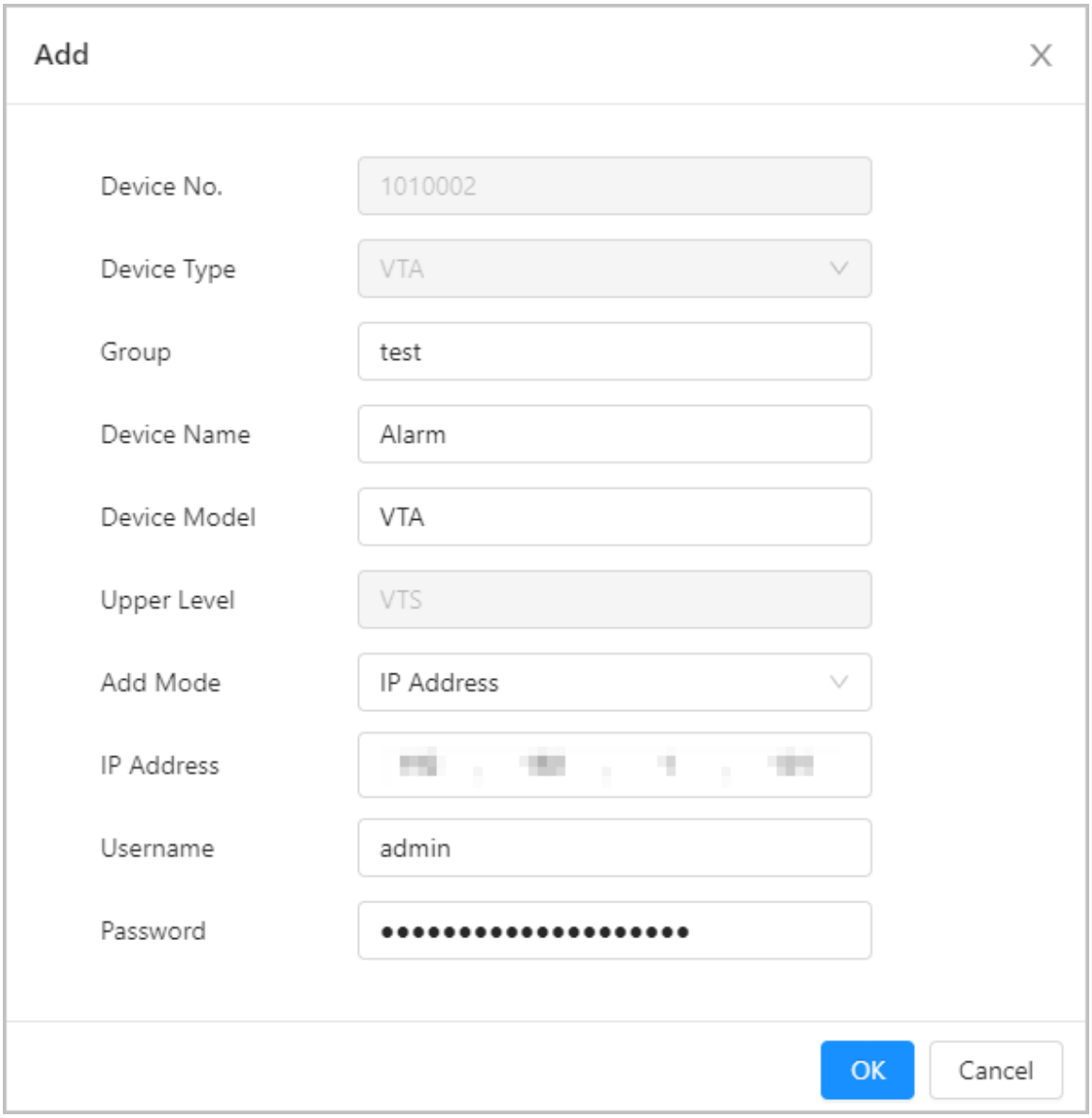


Tabla 4-8 Descripción de parámetros

Parámetro	Descripción
Grupo	Seleccionar**Monitor**>**Gestión de terminales**en el VTS, y luego podrá ver los dispositivos del grupo que configuró.
Nombre del dispositivo	Usuario definido.
Modelo de dispositivo	Introduce el modelo completo del dispositivo que podrás obtener en la etiqueta del dispositivo.
Agregar modo	Puede agregar VTA de las siguientes 2 maneras. ● Dirección IP: Introduzca la dirección IP del VTA. ● Registrarse: Configure los parámetros para registrarse en el VTS.
Nombre de usuario	Ingrese el nombre de usuario y la contraseña del dispositivo que agregó.
Contraseña	

Etapa 4 Hacer clic**DE ACUERDO**.

4.2.4.2.3 Agregar VTS de nivel inferior

Cuando el dispositivo está configurado como VTS de nivel superior, puede agregar el VTS de nivel inferior.

Procedimiento

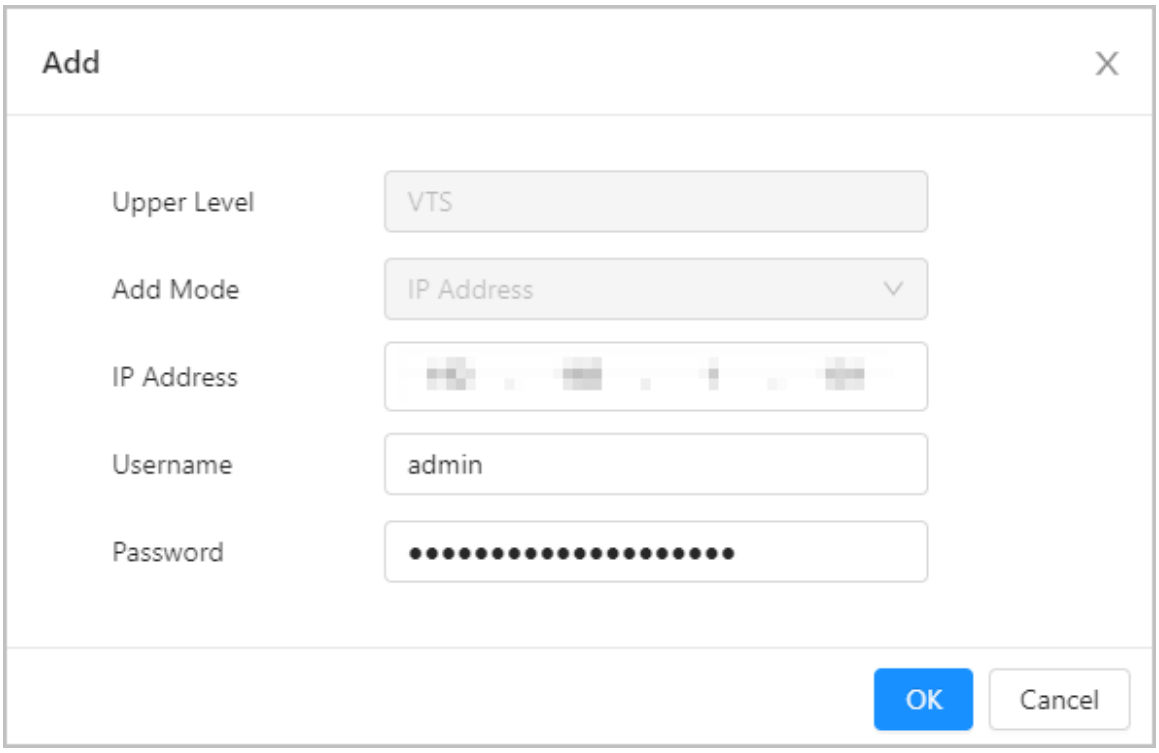
Paso 1 Inicie sesión en la página web del dispositivo.

Paso 2 Seleccionar**Configuración del dispositivo**>**Gestión de terminales**. Hacer clic

Paso 3 **Agregar**.

Etapa 4 Ingrese la dirección IP, nombre de usuario y contraseña del VTS.

Figura 4-17 Agregar VTS de nivel inferior



Paso 5 Hacer clic**DE ACUERDO**.

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 "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.