

# **Estación de puerta modular**

## **Manual de usuario**



# Prefacio

## General

Este manual presenta cómo configurar la estación de puerta modular (en adelante, "VTO") en la interfaz web.

### Instrucciones de seguridad

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

Palabras de advertencia	Significado
 PRECAUCIÓN	Indica un riesgo potencial que, si no se evita, podría provocar daños a la propiedad, pérdida de datos, menor rendimiento o resultados impredecibles.
 NOTA	Proporciona información adicional como énfasis y complemento del texto.

## Revisión histórica

Versión	Contenido de revisión	Fecha de lanzamiento
V1.0.0	Primer lanzamiento.	enero 2021

## Sobre el Manual

- El manual es solo para referencia. Si hay inconsistencia entre el manual y el producto real, prevalecerá el producto real.
- No somos responsables de ninguna pérdida causada por las operaciones que no cumplen con el manual.
- El manual se actualizaría de acuerdo con las últimas leyes y reglamentos de las jurisdicciones relacionadas. Para obtener información detallada, consulte el manual en papel, el CD-ROM, el código QR o nuestro sitio web oficial. Si hay inconsistencia entre el manual en papel y la versión electrónica, prevalecerá la versión electrónica.
- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto pueden causar algunas diferencias entre el producto real y el manual. Póngase en contacto con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria.
- Todavía puede haber desviación en los datos técnicos, descripción de funciones y operaciones, o errores en la impresión. Si hay alguna duda o disputa, nos reservamos el derecho de dar una explicación final.
- Actualice el software del lector o pruebe con otro software del lector convencional si no se puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas comerciales registradas y nombres de compañías en el manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, comuníquese con el proveedor o el servicio al cliente si ocurre algún problema al usar el dispositivo.
- Si hay alguna duda o controversia, nos reservamos el derecho de la explicación final.

## **Medidas de seguridad y advertencias importantes**

La siguiente descripción es el método de aplicación correcto del VTO. Lea el manual detenidamente antes de usar, para evitar peligros y pérdidas materiales. Siga estrictamente el manual durante el uso y guárdelo correctamente después de leerlo.

### **Requisitos operativos**

- No exponga el dispositivo a la luz solar directa ni a una fuente de calor. No instale el dispositivo en un ambiente húmedo o polvoriento. Instale horizontalmente el dispositivo en lugares estables para evitar que se caiga.
- No gotee ni salpique líquidos sobre el dispositivo, ni coloque sobre el dispositivo ningún objeto lleno de líquido. Instale el dispositivo en lugares bien ventilados y no bloquee su abertura de ventilación.
- Use el dispositivo solo dentro del rango nominal de entrada y salida. No desmonte el dispositivo usted mismo.
- Transporte, use y almacene el dispositivo dentro del rango permitido de humedad y temperatura.

### **requerimientos de energía**

- Utilice cables eléctricos recomendados en su área y dentro de su especificación nominal.
- Utilice una fuente de alimentación que cumpla con los requisitos SELV (voltaje extra bajo de seguridad) y suministre energía con un voltaje nominal que cumpla con la fuente de alimentación limitada en IEC60950-1. Para conocer los requisitos específicos de la fuente de alimentación, consulte la etiqueta del dispositivo.
- El acoplador de electrodomésticos es un dispositivo de desconexión. Durante el uso normal, mantenga un ángulo que facilite la operación.

# Tabla de contenido

<b>Prefacio.....</b>	<b>I Medidas</b>
<b>de seguridad y advertencias importantes .....</b>	<b>II 1</b>
<b>Inicialización del VTO .....</b>	<b>1</b>
<b>2 Inicio de sesión y restablecimiento de contraseña .....</b>	<b>2</b>
2.1 Acceso .....	2
2.2 Restablecimiento de contraseña .....	2
<b>3 Interfaz principal.....</b>	<b>4</b>
<b>4 Ajustes locales .....</b>	<b>5</b>
4.1 Básico .....	5
4.2 Audio video.....	6
4.3 Ajustes de control de acceso .....	8
4.3.1 Locales .....	8
4.3.2 RS-485 .....	9
4.3.3 Gestión de contraseñas .....	9
4.4 Sistema.....	9
4.5 Seguridad .....	11
4.6 Wiegand.....	12
4.7 Usuario de Onvif.....	13
4.8 Subir archivo.....	13
<b>5 Entorno doméstico .....</b>	<b>15</b>
5.1 Gestión de nº de VTO .....	15
5.2 Gestión de VTH .....	dieciséis
5.2.1 Adición de número de habitación.....	dieciséis
5.2.2 Emisión de Tarjeta de Acceso .....	19
5.2.3 Emisión de huellas dactilares .....	20
5.3 Gestión de VTS .....	21
5.4 Configuración de IPC .....	22
5.5 Estado .....	23
5.6 Publicar información.....	24
5.6.1 Enviar información .....	24
5.6.2 Información del historial .....	24
<b>6 Red.....</b>	<b>26</b>
6.1 Básico .....	26
6.1.1 TCP/IP .....	26
6.1.2 Puerto .....	26
6.1.3 P2P.....	27
6.2 UPnP.....	27
6.2.1 Habilitación de los servicios UPnP.....	27
6.2.2 Adición de servicios UPnP.....	27
6.3 Servidor SIP .....	28
6.4 cortafuegos .....	29
<b>7 Gestión de registros .....</b>	<b>30</b>
<b>Appendix 1 Recomendaciones de ciberseguridad .....</b>	<b>31</b>

# 1 Inicializar el VTO

Para iniciar sesión por primera vez o después de restablecer el VTO, debe inicializarlo en la interfaz web.

Step 1 Encienda el VTO.

Step 2 Ingrese la dirección IP predeterminada (192.168.1.108) del VTO en la barra de direcciones del navegador.



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

Figure 1-1 Inicialización del dispositivo

Device Init

1 One 2 Two 3 Three

Username admin

Password

Low Middle High

Confirm Password

Next

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

Step 4 una dirección de correo electrónico para restablecer la contraseña.

Step 5 Hacer clic **Próximo** y luego haga clic en **DE ACUERDO**.

## 2 Inicio de sesión y restablecimiento de contraseña

### 2.1 Acceso

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

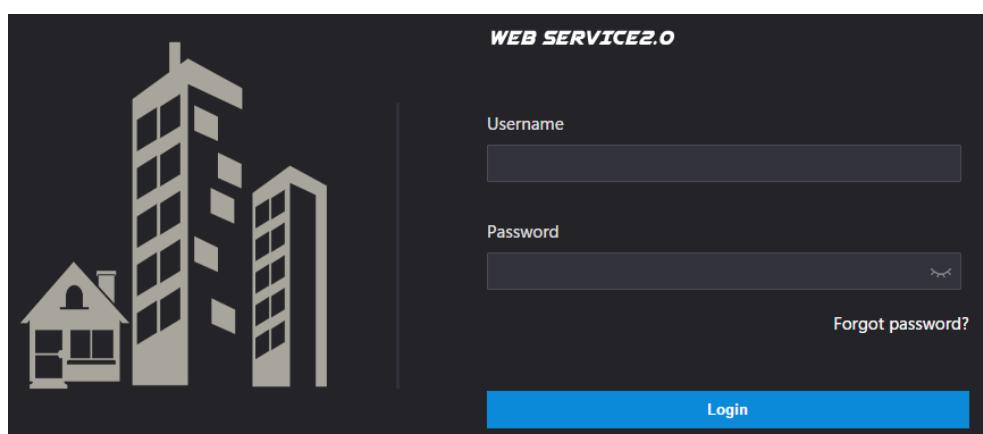
Step 1 Vaya a la dirección IP del VTO en el navegador.



Para iniciar sesión por primera vez, ingrese la IP predeterminada. Si tiene varios VTO, le recomendamos cambiar la dirección IP predeterminada (**Red > Básico**) para evitar conflictos.

Step 2 Ingrese "admin" como nombre de usuario y la contraseña que estableció durante la inicialización y luego haga clic en **Acceso**.

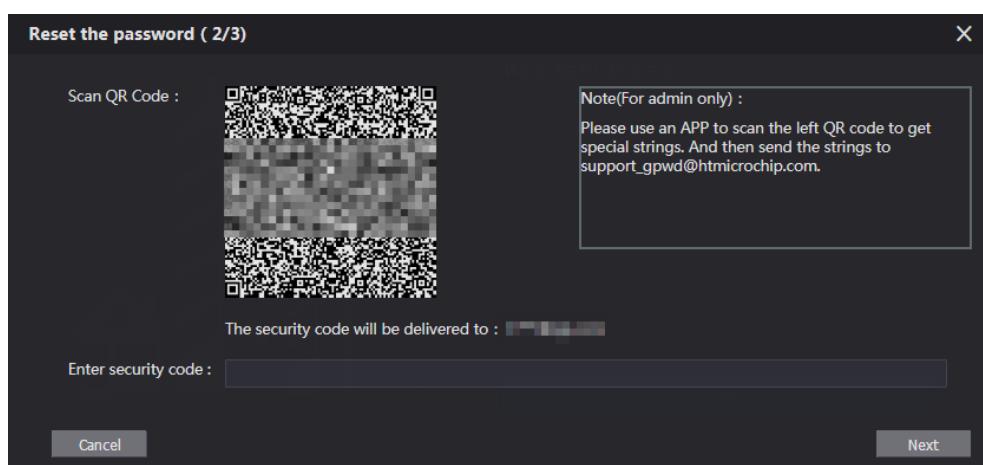
Figure 2-1 Interfaz de inicio de sesión



### 2.2 Restablecimiento de contraseña

Step 1 En la interfaz de inicio de sesión, haga clic en **¿Has olvidado tu contraseña?** luego haga clic en **Próximo**.

Figure 2-2 Restablecer la contraseña (2/3)



Step 2 Escanee el código QR y luego obtendrá una cadena de números y letras.

Step 3 Envíe la cadena al correo electrónico: support\_gpwd@htmicrochip.com , y luego el código de seguridad se enviará a la dirección de correo electrónico configurada durante la inicialización.

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



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

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

### 3 Interfaz principal

Figure 3-1 Interfaz principal

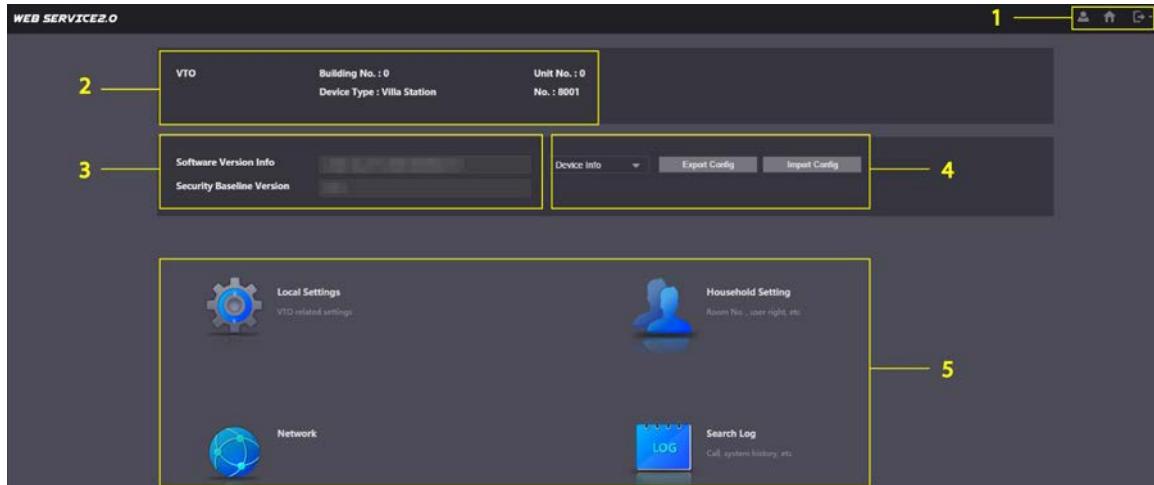


Tabla 3-1 Introducción a la interfaz principal

No.	Función	Descripción
1	Función general	<ul style="list-style-type: none"> <li>●  Cambie la contraseña y su dirección de correo electrónico.</li> <li>●  Vaya a la interfaz principal.</li> <li>●  Cierre la sesión, reinicie el VTO o restaure el VTO a la configuración de fábrica.</li> </ul> <p></p> <p>Si restaura el VTO a la configuración de fábrica, se eliminarán todos los datos excepto el almacenamiento externo. Puede formatear la tarjeta SD para eliminar los datos que contiene.</p>
2	información VTO	Ver la información del VTO y del sistema.
3	Información del sistema	
4	Configuración gerente	Exporte o importe la configuración de VTO o la información del usuario.
5	Función	<p>Configurar parámetros para diferentes funciones.</p> <p></p> <p>La interfaz y la función pueden variar según el tipo de dispositivo que configuró para el VTO. La interfaz y la función reales prevalecerán.</p>

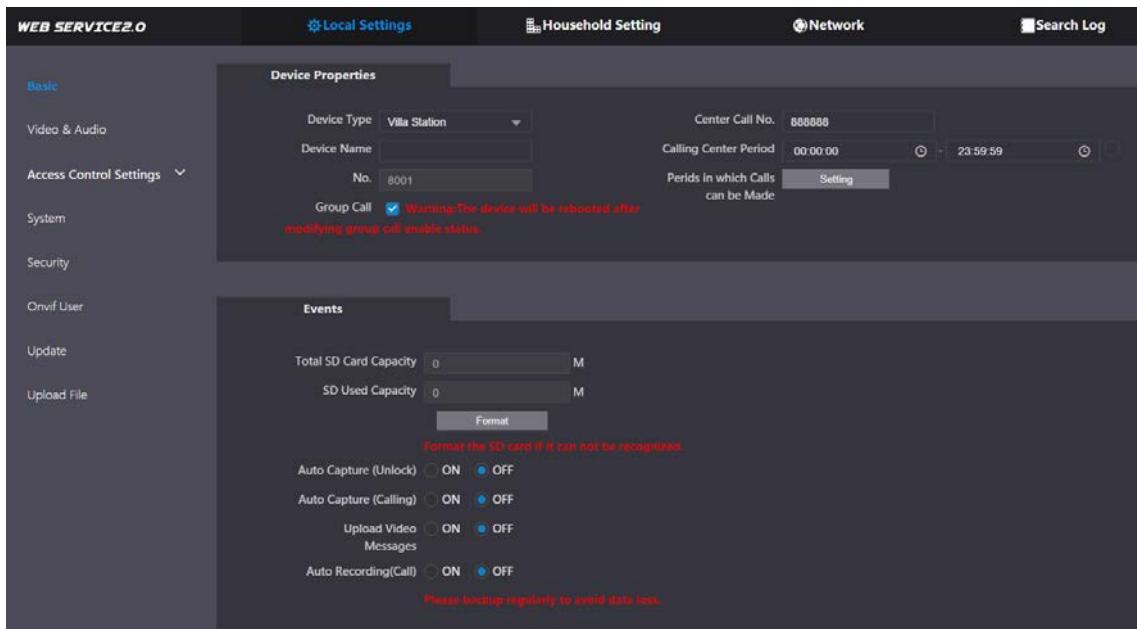
## 4 Configuraciones locales

Este capítulo presenta la configuración detallada del VTO.

### 4.1 Básico

Step 1 Seleccionar **Configuración local > Básico**.

Figure 4-1 Básico



Step 2 Configure los parámetros.

Tabla 4-1 Descripción de parámetros básicos

Parámetro	Descripción
Tipo de dispositivo	Seleccionar <b>Estación Villa o Apartamento pequeño</b> según sea necesario.
Número de llamada del centro	El número de teléfono predeterminado para el centro de administración es 888888 y puede configurarlo en cualquier número con hasta 9 dígitos.
Nombre del dispositivo	Cuando otros dispositivos están monitoreando este VTO, el nombre del dispositivo aparecerá en la imagen de monitoreo.
Período del centro de llamadas	Periodo de tiempo en el que se puede llamar al centro de gestión.
No.	Se usa para diferenciar cada VTO, y recomendamos configurarlo según la unidad o el número de edificio, y luego puede agregar VTO al servidor SIP usando sus números.  Puede cambiar el número de VTO cuando no funciona como servidor SIP.
Periodos en los que se pueden realizar llamadas	Configure la hora si solo desea recibir llamadas durante un período específico.
Llamada de grupo	Habilítelo en el VTO que funciona como servidor SIP, y cuando un VTH principal reciba una llamada, todos los VTH de extensión también recibirán la llamada.

Parámetro	Descripción
Tarjeta SD total	
Capacidad	Muestra la capacidad total y utilizada de la tarjeta SD. Puedes hacer clic <b>Formato</b> para eliminar todos los datos de la tarjeta SD.
Capacidad utilizada SD	
Formato	
Captura automática (Desbloquear)	Cuando la puerta esté desbloqueada, el VTO tomará dos instantáneas y las guardará en la tarjeta SD.
Captura automática (llamadas)	Tome una instantánea y guárdela en la tarjeta SD del VTO cuando el VTO esté llamando.
Subir vídeo Mensajes	Cuando está habilitado: <ul style="list-style-type: none"> <li>Si se inserta una tarjeta SD tanto en VTH como en VTO, el mensaje de video se guardará en las tarjetas SD de VTH y VTO.</li> <li>Si solo se inserta una tarjeta SD en el VTH o el VTO, el mensaje de video se guardará solo en la tarjeta SD del VTH o el VTO.</li> <li>Si no se inserta una tarjeta SD en el VTH o VTO, no se guardará ningún mensaje de video.</li> </ul>
Grabación automática (llamada)	Grabe video cuando el VTO esté en una llamada y guarde la grabación en la tarjeta SD del VTO.

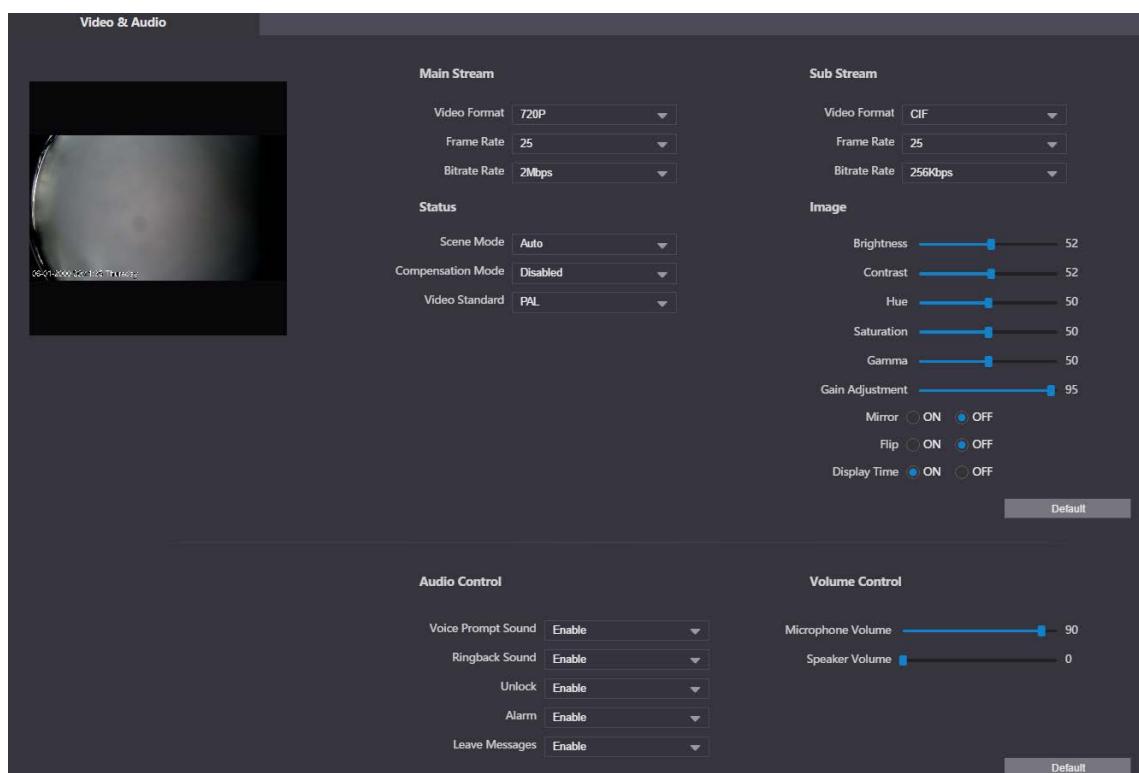
Step 3 Hacer clic **Ahorrar**.

## 4.2 Audio video

Configure el formato y la calidad de video y audio del VTO.

Step 1 Seleccionar **Configuración local > Vídeo y audio**.

Figure 4-2 vídeo y audio



Step 2 Configure los parámetros, que tendrán efecto al cambiar.

Tabla 4-2 Descripción de los parámetros de video

<b>Parámetro</b>		<b>Descripción</b>
Principal/Secundario Arroyo	Formato de video	<p>Seleccione una resolución diferente según sea necesario:</p> <ul style="list-style-type: none"> <li>● <b>1080P:</b> 1920 × 1080.</li> <li>● <b>720P:</b> 1280 × 720.</li> <li>● <b>WVGA:</b> 800 × 480.</li> <li>● <b>QVGA:</b> 320 × 240. <b>D1:</b> 720 × 480.</li> <li>● <b>C.I.F.:</b> 352 × 288.</li> </ul>
	Cuadros por segundo	Cuanto mayor sea el valor, más suave será el video, pero requiere más ancho de banda.
	Tasa de bits	Cuanto mayor sea el valor, mejor será la calidad del video, pero requiere más ancho de banda.
Estado	Modo escena	Seleccione según sea necesario según las condiciones de iluminación. <b>Autose</b> selecciona de forma predeterminada.
	Compensación Modo	<ul style="list-style-type: none"> <li>● <b>CLB:</b> Compensación de contraluz. Mejorar la claridad del objetivo en la imagen.</li> <li>● <b>WDR:</b> Amplio rango dinámico. Mejore el brillo de las áreas oscuras y reduzca el brillo de las áreas brillantes para mejorar la imagen.</li> <li>● <b>LLC:</b> Compensación de luz alta. Reduzca el brillo de los puntos fuertes para mejorar la imagen general.</li> </ul>
	Estándar de vídeo	<p>Seleccionar <b>CAMARADA</b> o <b>NTSC</b> según tu zona.</p>  <p><b>CAMARADA</b> se utiliza principalmente en China y Europa, y <b>NTSC</b> principalmente en los Estados Unidos y Japón.</p>
Imagen	Brillo	Cuanto mayor sea el valor, más brillante será la imagen.
	Contraste	Valor mayor para mayor contraste entre áreas claras y oscuras.
	Matiz	Haz que el color sea más brillante o más oscuro. El valor predeterminado lo establece el sensor de luz y recomendamos mantenerlo predeterminado.
	Saturación	Cuanto más brillante sea el valor, más grueso será el color.
	Gama	Cambia el brillo de la imagen y mejora el rango dinámico de la imagen de forma no lineal. Cuanto mayor sea el valor, más brillante será la imagen.
	Ajuste de ganancia	Amplifica la señal de video para aumentar el brillo de la imagen. Si el valor es demasiado grande, habrá más ruido en la imagen.
	Espejo	Muestra la imagen con los lados izquierdo y derecho invertidos.
	Voltear	Muestra la imagen al revés.
	Tiempo de visualización	Muestra la hora y la fecha actuales en la imagen de video.
Audio Control	—	Activa o desactiva cada tipo de sonido.
Volumen Control	Micrófono	Ajuste el volumen según sea necesario.
	Volumen	
	Volumen del altavoz	

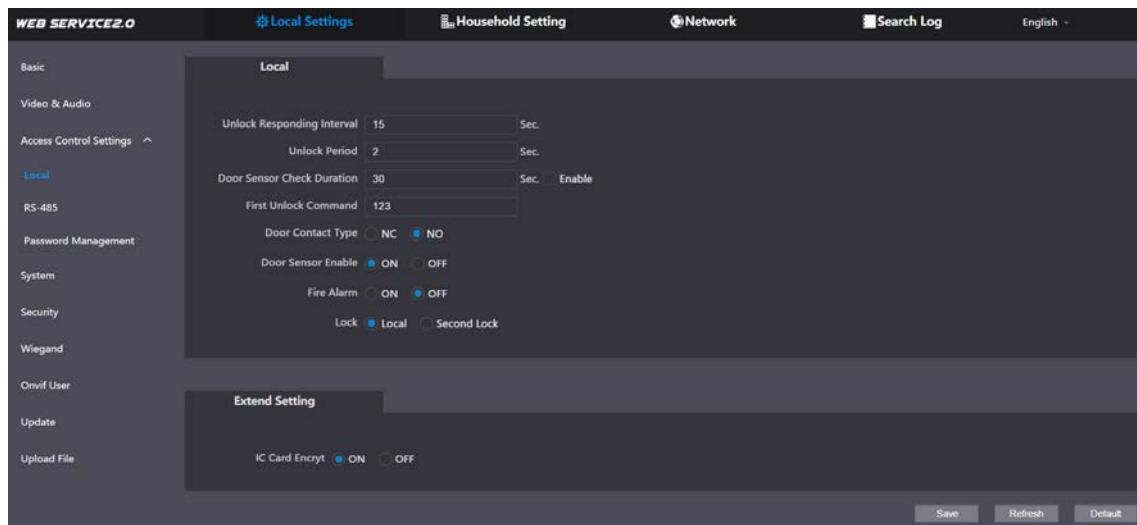
## 4.3 Configuración de control de acceso

Esta sección presenta cómo configurar los dos bloqueos conectados al puerto de bloqueo o al puerto RS-485 del VTO.

### 4.3.1 locales

**Step 1** Seleccionar **Configuración local > Configuración de control de acceso**.

Figure 4-3 Local



**Step 2** Configure los parámetros.

Tabla 4-3 Descripción del parámetro de control de acceso local

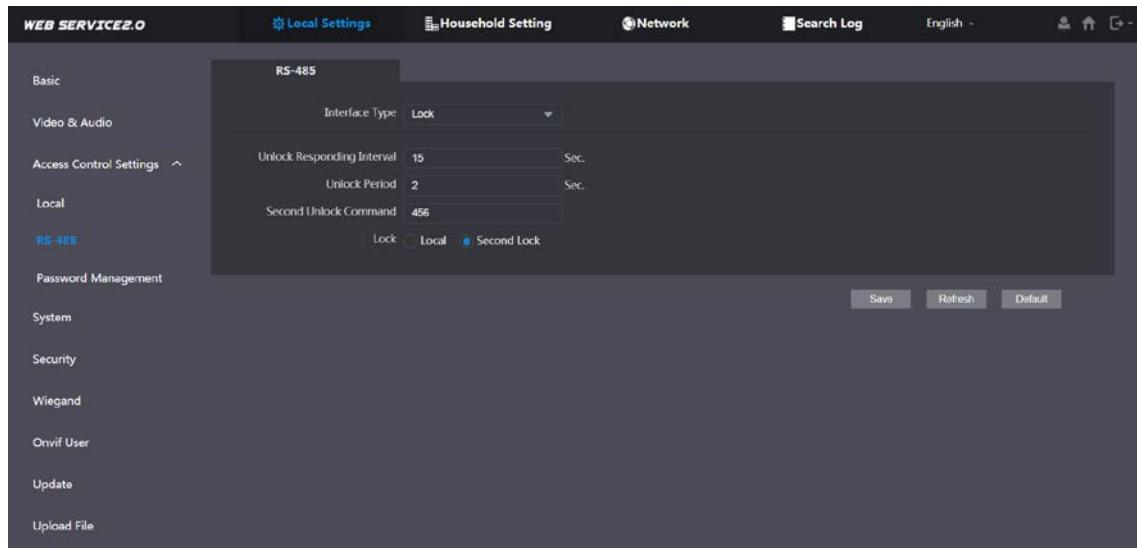
Parámetro	Descripción
Desbloquear respondiendo Intervalo	La puerta solo se puede desbloquear de nuevo después del intervalo.
Período de desbloqueo	El tiempo durante el cual la cerradura permanece desbloqueada.
Comprobación del sensor de puerta Duración	<ul style="list-style-type: none"><li>Actívelo y la puerta no se bloqueará hasta que los sensores de la puerta entren en contacto. Si la puerta está desbloqueada por más tiempo que el <b>Duración de la comprobación del sensor de puerta</b>, se activará la alarma del sensor de la puerta y se enviará la alarma al centro de gestión.</li><li>Desactívelo, y luego la puerta se bloqueará después de la <b>Período de desbloqueo</b>.</li></ul> <p> Debe instalar un contacto de puerta para configurar este parámetro.</p>
Primero/Segundo Desbloqueo Dominio	Puede conectar un teléfono de terceros, como un teléfono SIP, al VTO y usar el comando para abrir la puerta de forma remota.
Tipo de contacto de puerta	<ul style="list-style-type: none"><li><b>CAROLINA DEL NORTE:</b> Normalmente</li><li><b>cerrado, NO:</b> Normalmente abierto.</li></ul>
Habilitar sensor de puerta	Sincronice el estado del sensor de la puerta con los monitores interiores (VTH).
Alarma de incendios	Si está activado, puede conectar un dispositivo de alarma al puerto que es originalmente para el contacto de puerta, pero no puede usar la función de contacto de puerta.
Cerrar	Los métodos no remotos, como la contraseña o la tarjeta, desbloquearán el bloqueo que seleccione.
Cifrado de tarjeta IC	Las tarjetas de acceso emitidas por el VTO serán encriptadas y no clonables.

**Step 3** Hacer clic Ahorrar.

## 4.3.2 RS-485

Seleccionar **Configuración local > Configuración de control de acceso**, y luego configure los parámetros de la cerradura conectada a través del puerto RS-485. Consulte la Tabla 4-3 para obtener una descripción de los parámetros.

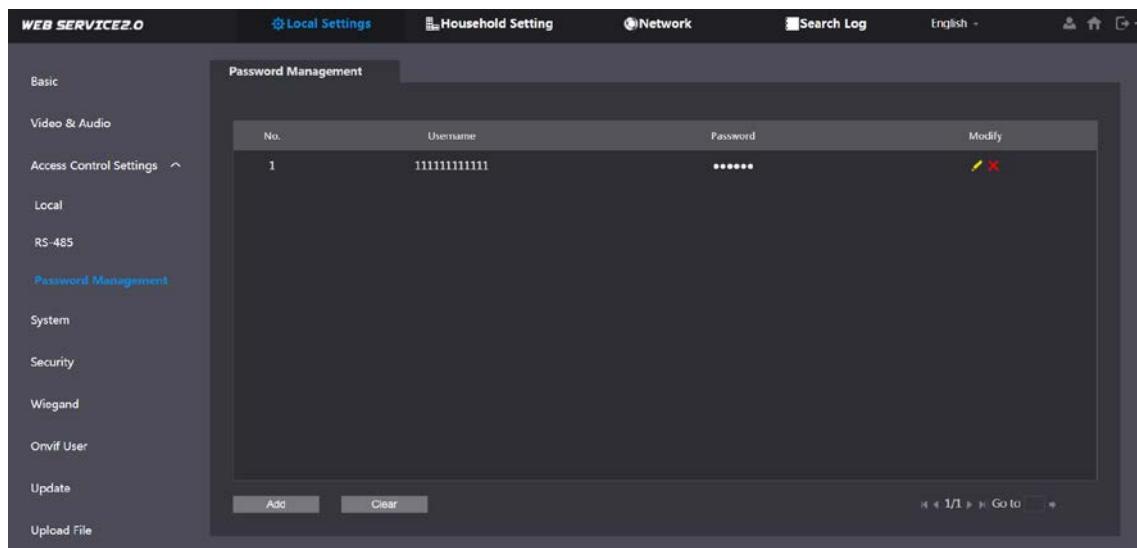
Figure 4-4 Cerradura conectada a través del puerto RS-485



## 4.3.3 Gestión de contraseñas

Agregue un nombre de usuario y una contraseña para desbloquear la puerta.

Figure 4-5 Gestión de contraseñas

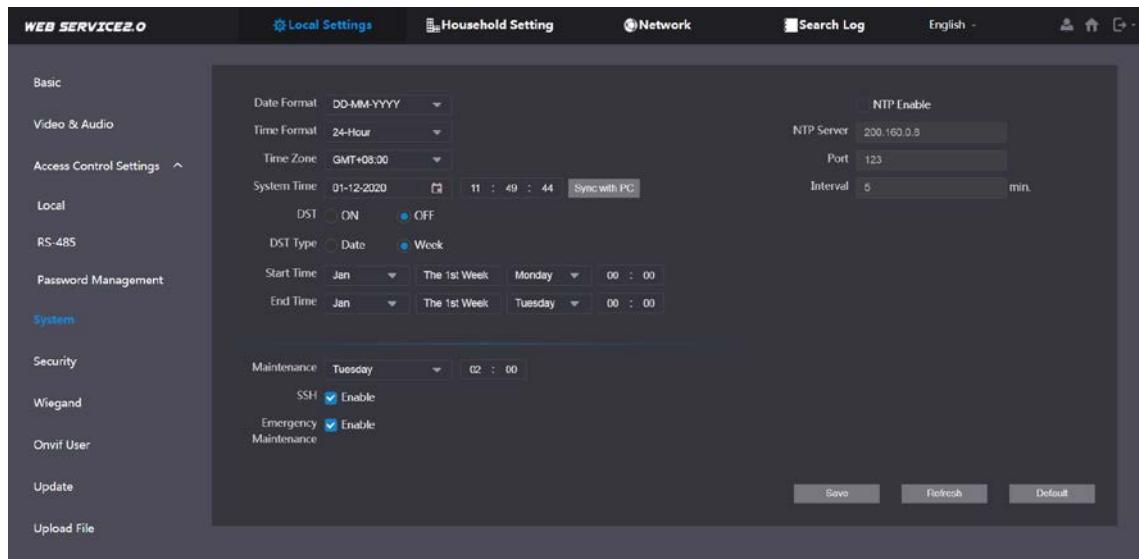


## 4.4 Sistema

Configure parámetros de tiempo, servidor NTP y más.

**Step 1** Seleccionar **Configuración local > Sistema**.

Figure 4-6 Sistema



**Step 2** Configure los parámetros.

Tabla 4-4 Descripción de los parámetros del sistema

Parámetro	Descripción
Formato de fecha	Seleccione un formato según sea necesario.
Formato de tiempo	
Hora del sistema	<p><b>⚠</b></p> <p>Cambiar la hora del sistema puede causar problemas en la búsqueda de videos y la publicación de información. Desactive la grabación de video y la instantánea automática antes de cambiarla.</p>
Zona horaria	Configure la zona horaria según sea necesario.
Sincronizar con PC	Sincronice la hora del sistema VTO con su PC.
horario de verano	Horario de verano. Si es aplicable a su área, debe habilitarlo y luego configurar el tipo de horario de verano, la hora de inicio y la hora de finalización.
Tipo de horario de verano	Seleccionar <b>Fecha o Semana</b> según sea necesario, y luego configure el período específico.
Hora de inicio	Configure la hora de inicio y la hora de finalización del horario de verano.
Hora de finalización	
Habilitar NTP	Habilite NTP e ingrese la dirección IP del servidor NTP, y luego el VTO sincronizará la hora con el servidor NTP automáticamente.
Servidor NTP	
Puerto	Número de puerto del servidor NTP.
Intervalo	Ciclo de actualización de tiempo VTO. 30 minutos como máximo.
Mantenimiento	Defina la hora en que el VTO se reiniciará automáticamente.
SSH	<p>Puede conectar dispositivos de depuración al VTO a través del protocolo SSH.</p> <p><b>⚠</b></p> <p>Recomendamos apagarlo y activar el modo de seguridad y la protección de la información del servicio saliente. Consulte "4.5 Seguridad". De lo contrario, el VTO podría estar expuesto a riesgos de seguridad y fuga de datos.</p>
Emergencia Mantenimiento	<p>Habilítelo para el análisis y la reparación de fallas.</p> <p><b>⚠</b></p> <p>Esta función ocupará los puertos 8088 y 8087.</p>

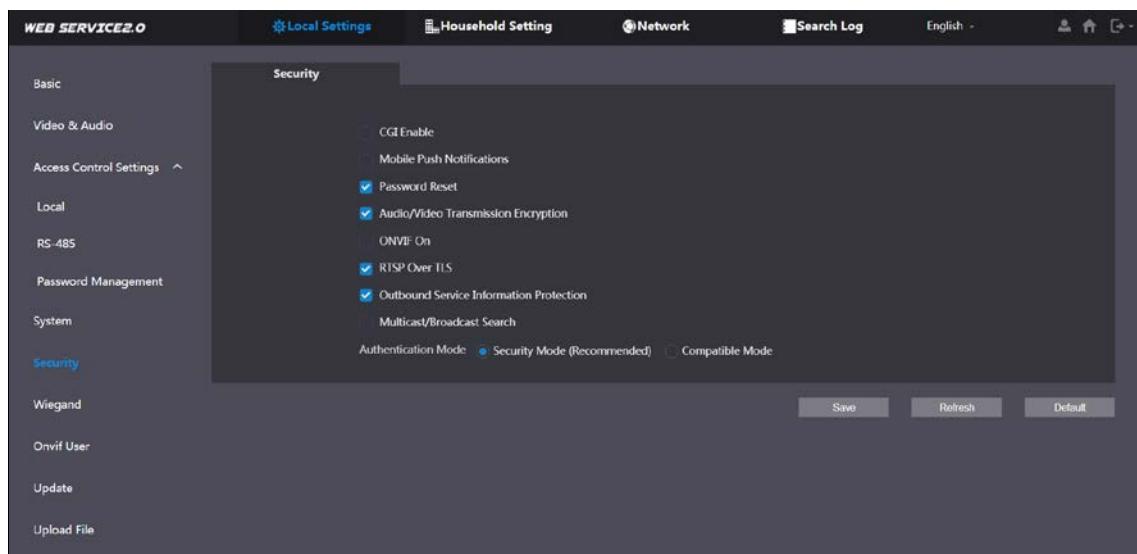
**Step 3** Hacer clic**Ahorrar**.

## 4.5 Seguridad

Configure funciones que involucren la seguridad del dispositivo.

**Step 1** Seleccionar**Configuración local > Seguridad**.

Figure 4-7 Seguridad



**Step 2** Configure los parámetros.

Tabla 4-5 Descripción del parámetro de seguridad

Parámetro	Descripción
Habilitar CGI	<p>Habilite el uso del comando CGI.</p> <p><b>!</b></p> <p>Recomendamos apagarlo. De lo contrario, el VTO podría estar expuesto a riesgos de seguridad y fuga de datos.</p>
Empuje móvil Notificación	<p>Envíe información a la aplicación en el teléfono inteligente.</p> <p><b>!</b></p> <p>Recomendamos apagarlo si no necesita esta función. De lo contrario, el VTO podría estar expuesto a riesgos de seguridad y fuga de datos.</p>
Restablecimiento de contraseña	<p>Si está desactivado, no podrá restablecer la contraseña.</p>
Audio Video Transmisión Cifrado	<p>Cifre todos los datos durante la llamada de voz o video.</p> <p><b>!</b></p> <p>Recomendamos encenderlo. De lo contrario, el VTO podría estar expuesto a riesgos de seguridad y fuga de datos.</p>
ONVIF encendido	<p>Permita que los dispositivos de terceros extraigan la transmisión de video del VTO a través del protocolo ONVIF.</p> <p><b>!</b></p>

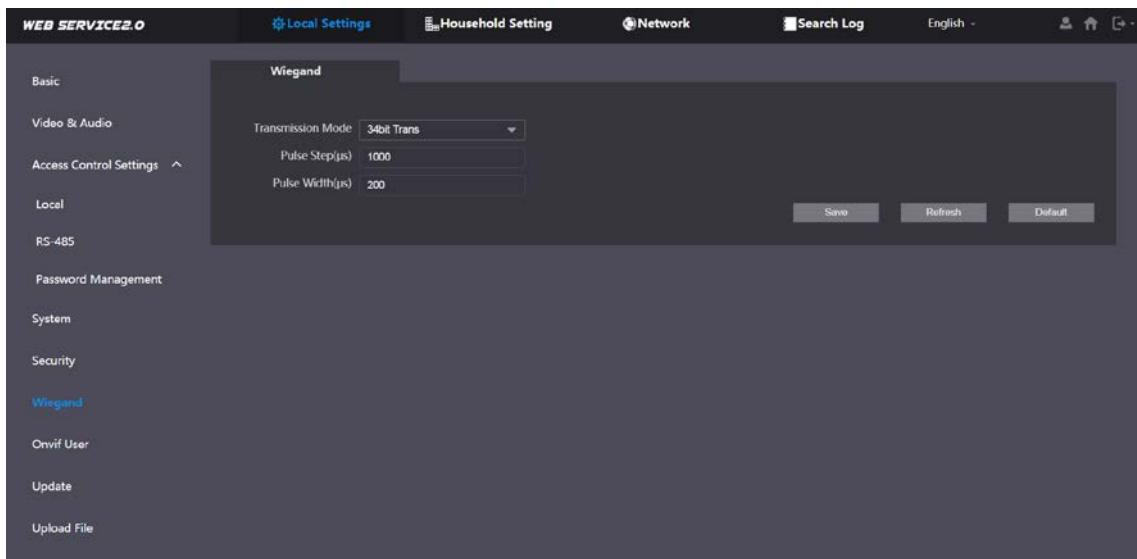
Parámetro	Descripción
	Recomendamos apagarlo. De lo contrario, el VTO podría estar expuesto a riesgos de seguridad y fuga de datos.
RTSP sobre TSL	<p>Flujo de bits encriptado de salida a través de RTSP.</p>  <p>Recomendamos encenderlo. De lo contrario, el VTO podría estar expuesto a riesgos de seguridad y fuga de datos.</p>
Servicio saliente Información Protección	<p>Proteja sus contraseñas.</p>  <p>Recomendamos encenderlo. De lo contrario, el VTO podría estar expuesto a riesgos de seguridad y fuga de datos.</p>
Multidifusión/Difusión Buscar	<p>Habilítelo y otros dispositivos encontrarán el VTO.</p>  <p>Recomendamos apagarlo. De lo contrario, el VTO podría estar expuesto a riesgos de seguridad y fuga de datos.</p>
Autenticación Modo	<ul style="list-style-type: none"> <li>● <b>modo de seguridad</b>(recomendado): admite el inicio de sesión con autenticación Digest.</li> <li>● <b>Modo compatible</b>: utilice el método de inicio de sesión anterior.</li> </ul>  <p>Recomendamos el modo de seguridad. El modo compatible puede exponer el VTO a riesgos de seguridad y fuga de datos.</p>

Step 3 Hacer clic Ahorrar.

## 4.6 Wiegand

Configure los parámetros según sea necesario cuando esté conectado a otros dispositivos, como un lector de tarjetas con un puerto Wiegand.

Figure 4-8 Wiegand



## 4.7 Usuario Onvif

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



Si elimina una cuenta, no se puede deshacer.

**Step 1** Seleccionar **Configuración local > Usuario de Onvif**. Hacer

**Step 2** clic **Agregar**.

Figure 4-9 Añadir un usuario ONVIF

Username	<input type="text"/>
Password	<input type="password"/>
Weak    Medium    Strong	
Confirm	<input type="password"/>
Save	Cancel

**Step 3** Ingrese la información y luego haga clic en **Ahorrar**.

Los dispositivos ONVIF ahora pueden monitorear el VTO usando la cuenta. Consulte el manual del usuario del dispositivo ONVIF para obtener más detalles.

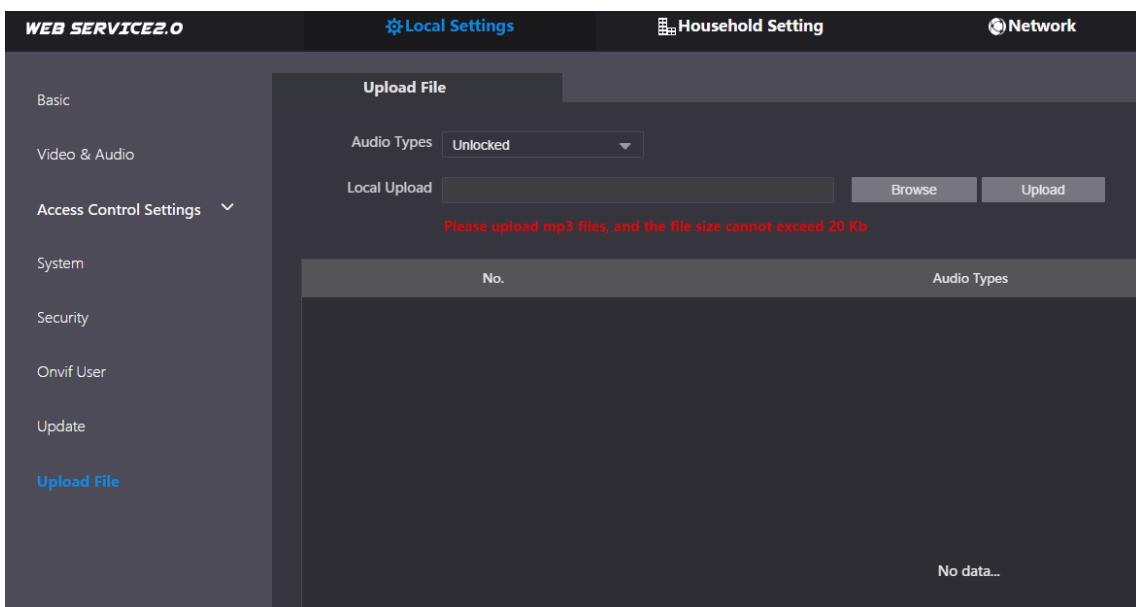
## 4.8 Subir archivo

Cargue un archivo de audio para cambiar el sonido al llamar, desbloquear la puerta y más.

**Step 1** Seleccionar **Configuración local > Cargar archivo**.

Step 2 Seleccione un tipo de audio y luego haga clic en **Navegar** para seleccionar el archivo de audio según sea necesario.

Figure 4-10 Cambiar el mensaje de sonido



Step 3 Hacer clic **Subir**.

# 5 entorno doméstico

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



Para configurar los parámetros del servidor SIP, consulte "Servidor SIP" para obtener más detalles.

## 5.1 Gestión de número de VTO

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

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

Figure 5-1 gestión de VTO

**Step 2** Hacer clic **Agregar**.

Figure 5-2 Agregar VTO

**Step 3** Configure los parámetros.



Se debe agregar el servidor SIP.

Tabla 5-1 Agregar configuración de VTO

Parámetro	Descripción
No.	El número de VTO que configuró. Consulte la Tabla 4-1 para obtener más información.
Registro Contraseña	Manténgalo predeterminado.
construir no. Número de unidad.	Disponible solo cuando otros servidores funcionan como servidor SIP.
Dirección IP	Dirección IP del VTO.
Nombre de usuario Contraseña	Nombre de usuario y contraseña de inicio de sesión de la interfaz web del VTO.

**Step 4** Hacer clic Ahorrar.



Hacer clic o para modificar o eliminar un VTO, o para eliminar todos los VTO agregados, pero el en el que ha iniciado sesión no se puede modificar ni eliminar.

## 5.2 Gestión VTH

### 5.2.1 Agregar número de habitación

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



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

#### Usando el VTO en una Villa

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

Figure 5-3 Propiedades del dispositivo (1)

WEB SERVICE 2.0

Local Settings Household Setting Network Search Log English -

Basic

Device Properties

Device Type: Villa Station

Device Name: 8801

Center Call No.: 888888

Calling Center Period: 00:00:00 - 23:59:59

No.: 8801

Group Call:  Warning: The device will be rebooted after modifying group call ansala status.

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

**Step 3** Seleccionar **Configuración del hogar > Gestión de VTH**.

Figure 5-4 Gestión del número de habitación

The screenshot shows a web-based management interface for VTH (Virtual Home). The top navigation bar includes 'WEB SERVICE 2.0', 'Local Settings', 'Household Setting' (which is highlighted in blue), 'Network', 'Search Log', and language selection ('English'). On the left, a sidebar lists 'VTO No. Management', 'VTH Management' (which is highlighted in blue), 'VTS Settings', and 'Status'. The main content area is titled 'VTH Management' and displays a table with columns: Room No., First Name, Last Name, Nick Name, Registration Mode, and Modify. Two rows are listed: '9901#0' and '9901#1', both with 'public' in the registration mode column and a red 'X' icon in the modify column. At the bottom of the table are buttons for 'Add', 'Refresh', 'Clear', and navigation links like '< 1/1 > Go to'.

**Step 4** Hacer clicAregar.

Figure 5-5 Agregar un número de habitación

This screenshot shows a modal dialog box titled 'Add' for adding a new room number. It contains fields for 'First Name', 'Last Name', 'Nick Name', 'Room No.' (with a red asterisk indicating it's required), 'Registration Mode' (set to 'public'), and 'Registration Password' (containing '12345'). To the right of these fields is a table with columns 'Username', 'Card No.', and 'Modify'. The table displays a single row with the message 'No data...'. At the bottom of the dialog are buttons for 'Issue Card', 'Save', and 'Cancel'.

**Step 5** Configure los parámetros de la izquierda.

Tabla 5-2 Información de la habitación

Parámetro	Descripción
Nombre de pila	
Apellido	Introduce la información que necesitas para diferenciar cada habitación.
Apodo	
Habitación no.	Ingrese un número de habitación y luego configure el número en un VTH para conectarse para conectarlo a la red.
Tipo de registro	Seleccionar <b>público</b> .
Registro	
Contraseña	Manténgalo predeterminado.

**Step 6** Hacer clicAhorar.

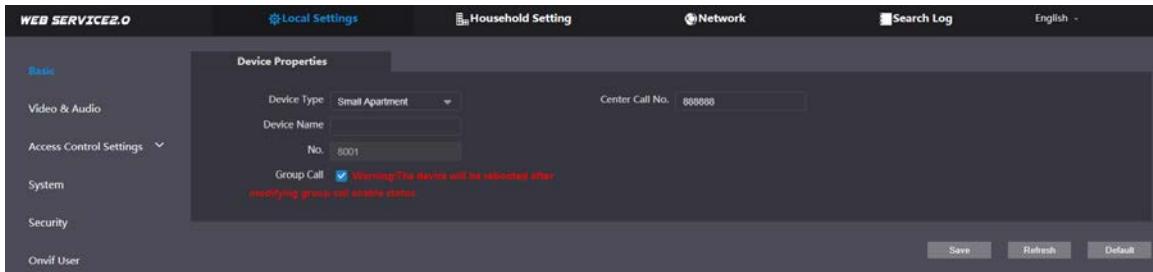


- Hacer clic o para modificar o eliminar un número de habitación.
- Hacer clic para borrar todos los números de habitación.

## Usando el VTO en un apartamento pequeño

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

Figure 5-6 Propiedades del dispositivo (2)

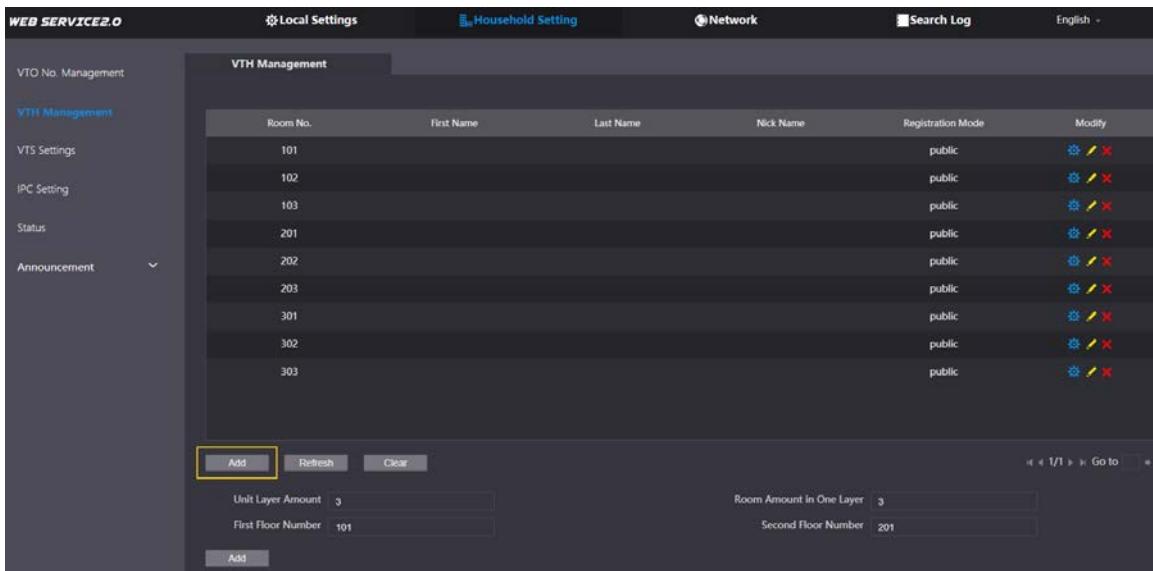


**Step 2** Colocar **Tipo de dispositivo** a **Apartamento pequeño** y luego haga clic en **Ahorrar**.

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

- Agregue un número de habitación individual.

Figure 5-7 Añadir números de habitación



- 1) Haga clic **Agregar**.

Figure 5-8 Añadir un número de habitación individual

2) Configure la información de la izquierda. Consulte la Tabla 5-2 para obtener más información.

3) Haga clic **Añadir**.

- Adición de varios números de habitación.

Figure 5-9 Agregar números de habitación en lotes

1) Configurar la información.

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

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



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

## 5.2.2 Emisión de Tarjeta de Acceso

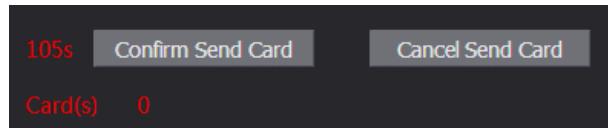
Emita una tarjeta de acceso para desbloquear la puerta de una habitación.



Para usar esta función, el VTO debe tener un lector de tarjetas.

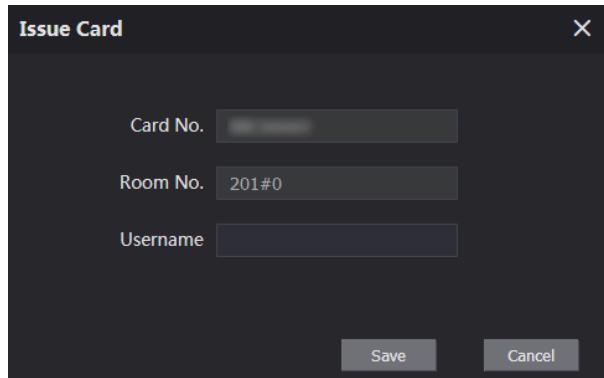
**Step 1** Seleccionar **Configuración del hogar > Gestión de VTH**, haga clic **Agregar** luego haga clic en **Tarjeta de emisión**.

Figure 5-10 Aviso de cuenta regresiva



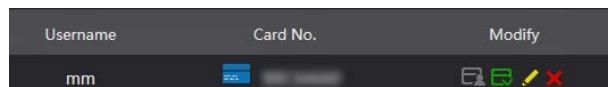
Step 2 Pase la tarjeta en el VTO.

Figure 5-11 Emitir tarjeta



Step 3 Introduzca el nombre de usuario, haga clic en **Ahorrary** luego haga clic en **Confirmar enviar tarjeta**.

Figure 5-12 Tarjeta de acceso emitida



## Otras operaciones

- Hacer clic para configurarlo en la tarjeta principal, y luego el ícono cambia a la carta principal se puede usar para emitir tarjetas de acceso para esta sala en el VTO.
- Hacer clic para establecerlo en pérdida, y luego el ícono cambia a La tarjeta extraviada no puede ser solía abrir la puerta.
- Hacer clic o para modificar el nombre de usuario o eliminar la tarjeta.

### 5.2.3 Emisión de huellas dactilares

Emite huellas dactilares para desbloquear la puerta de una habitación.



Para usar esta función, el VTO debe tener un escáner de huellas dactilares.

Step 1 Seleccionar **Configuración del hogar > Gestión de VTH**, haga clic **Agregary** luego haga clic en **Emitir huella digital**.

Figure 5-13 Emitir huella digital

The screenshot shows a modal dialog box titled "Add". It contains fields for "Username" and "Room No." (set to 101). Below these are two checkboxes labeled "Unlock Permission" with "Lock 1" and "Lock 2" checked. At the bottom are "Save" and "Cancel" buttons.

Step 2 Ingrese un nombre de usuario, asigne el permiso de desbloqueo según sea necesario y luego haga clic en

Step 3 **Ahorrar.** Presione su huella digital en el escáner.

## 5.3 Gestión VTS

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

Step 1 Inicie sesión en la interfaz web del VTO que funciona como servidor SIP y luego seleccione**Configuración del hogar > Configuración de VTS.**

Figure 5-14 gestión VTS

The screenshot shows the "VTS Settings" page under "VTS Settings" in the sidebar. The main area displays a table with columns: VTS No., IP Address, Modify, and Delete. A message "No data..." is shown below the table. At the bottom are "Add" and navigation buttons.

Step 2 Hacer clic**Agregar.**

Figure 5-15 Añadir VTS

The screenshot shows a dark-themed 'Add' dialog box. At the top left is the word 'Add'. On the right is a close button ('X'). Below the title are three input fields: 'VTS No.' (empty), 'Registration Password' (empty with a password mask icon), and 'IP Address' (127.0.0.1). At the bottom right are two buttons: 'Save' and 'Cancel'.

Step 3 Configure los parámetros.

Tabla 5-3 Agregar configuración de VTS

Parámetro	Descripción
VTS No.	El número del VTS.
Contraseña de registro	Manténgalo predeterminado.
Dirección IP	Dirección IP de VTS.

Step 4 Hacer clic Ahorrar.

## 5.4 Configuración de CIP

Puede agregar IPC y NVR al VTO que funciona como servidor SIP, y luego todos los VTH conectados pueden monitorearlos.



Las interfaces pueden variar con diferentes productos. Prevalecerá la interfaz real.

Step 1 Inicie sesión en la interfaz web del VTO que funciona como servidor SIP y luego seleccione **Configuración del hogar > Configuración de IPC**.

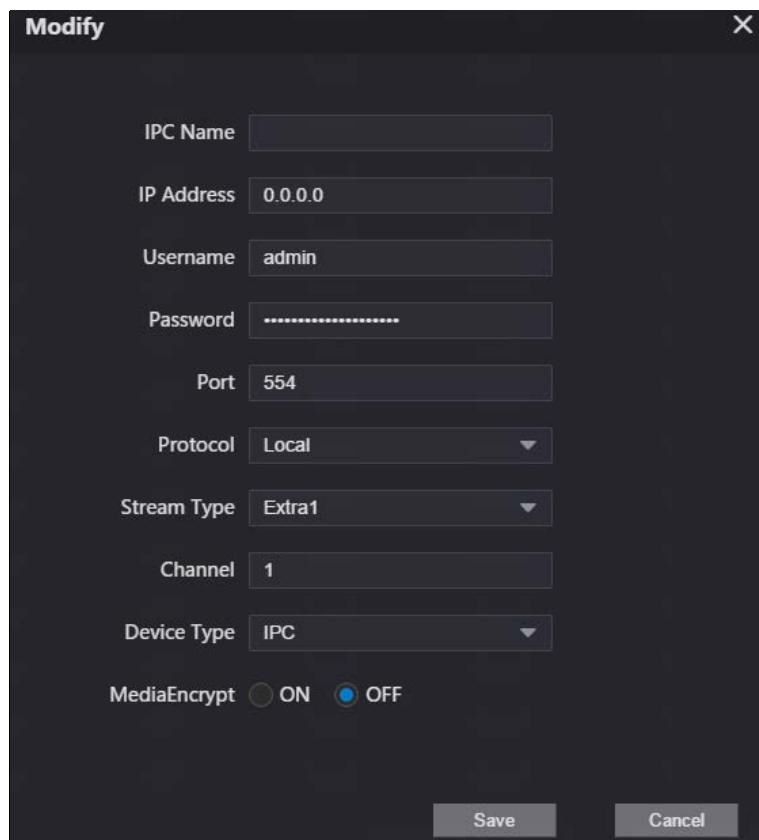
**Configuración de IPC.**

Figure 5-16 Configuración de CIP

The screenshot shows the 'IPC Setting' section of the configuration interface. The left sidebar includes 'WEB SERVICE 2.0', 'Local Setting', 'Household Setting' (which is selected), 'Network Setting', and 'Log Management'. The main area has a table titled 'IPC Setting' with the following columns: IPC Name, IP Addr., Username, Port No, Protocol, Stream, Channel, Device Type, Modify, and Delete. There are 12 rows of data in the table. At the bottom of the table are buttons for 'Import Config', 'Export Config', 'Refresh', and 'Default'.

Step 2 Hacer clic .

Figure 5-17 Agregar CIP



Step 3 Configure los parámetros.

Tabla 5-4 Agregar configuración de IPC

Parámetro	Descripción
Nombre de la CIP	Introduzca el nombre que identifica al IPC.
Dirección IP	Dirección IP del IPC.
Nombre de usuario	Nombre de usuario y contraseña de inicio de sesión de la interfaz web del dispositivo.
Contraseña	
Puerto	Manténgalo predeterminado.
Protocolo	Seleccionar <b>LocaloOnvif</b> .
Tipo de transmisión	<ul style="list-style-type: none"> <li>● <b>Principal:</b> Mejor calidad de video pero requiere más ancho de banda.</li> <li>● <b>Adicional1:</b> Video más suave con peor calidad, pero requiere menos ancho de banda.</li> </ul>
Canal	El número de canales que admite un dispositivo.
Tipo de dispositivo	Seleccione el que sea necesario.
MediaEncrypt	Seleccionar <b>ENsi</b> si el IPC que se agregará está encriptado.

Step 4 Hacer clic Ahorrar.

## Otras operaciones

- **Exportar configuración:** exporte la información del dispositivo a su PC. **Importar configuración:** Importar información del dispositivo.

## 5.5 Estado

Puede ver el estado en línea y las direcciones IP de todos los dispositivos conectados.

Inicie sesión en la interfaz web del servidor SIP y luego seleccione**Configuración del hogar > Estado**.

Figure 5-18 Estado

Status				
Room No.	Status	IP:Port	Reg Time	Off Time
201#0	Online	192.168.1.100:5000	2018-10-09 02:01:58	0
201#1	Online	192.168.1.100:5001	2018-10-09 02:02:11	0
12	Online	192.168.1.100:5002	2018-10-09 02:02:15	0
11	Online	192.168.1.100:5003	2018-10-09 02:06:20	0

## 5.6 Publicar información

Puede enviar mensajes desde el servidor SIP a dispositivos VTH y ver el historial de mensajes.

### 5.6.1 Enviar información

**Step 1** Inicie sesión en la interfaz web del servidor SIP y luego seleccione**Configuración del hogar > Publicar información > Enviar información**.

Figure 5-19 Enviar información

The screenshot shows the 'Announcement' section of the configuration menu. On the left, there's a sidebar with options like VTO Management, VTH Management, VTS Settings, IPC Setting, Status, Announcement, Send Info, and History Info. The main panel is titled 'Send Info' and contains the following fields:

- Validity Period: A date range from 2000-01-16 to 23:59:59.
- Send to: A dropdown menu showing 'All devices'.
- Title: An input field.
- Contents: A large text area for message content.
- Buttons at the bottom: 'Confirm' and 'Refresh'.

**Step 2** Especifica el**Período de validez**que el mensaje será válido.

**Step 3** Ingrese el número VTO o el número VTH, o seleccione**Todos los dispositivos**para enviar el mensaje a todos los dispositivos de la red y luego ingrese el título y el contenido de su mensaje.

**Step 4** Hacer clic**Confirmar**.

### 5.6.2 Información histórica

Puede ver la información de los mensajes enviados.

Inicie sesión en la interfaz web del servidor SIP, seleccione**Configuración del hogar > Información de publicación > Información de histórico**.

Figure 5-20 Información histórica

	IssueTime	Period of validity	Title	Delete
	2018-10-09 16:52:31	2018-10-09 16:54:00	[redacted]	X
	2018-10-09 16:52:31	2018-10-09 16:53:00	[redacted]	X
	2018-10-09 03:15:38	2018-10-09 16:52:00	[redacted]	X

Navigation controls at the bottom right include arrows for navigation, a 'Go to' input field, and a search icon.

# 6 Red

Este capítulo presenta cómo configurar los parámetros de red.

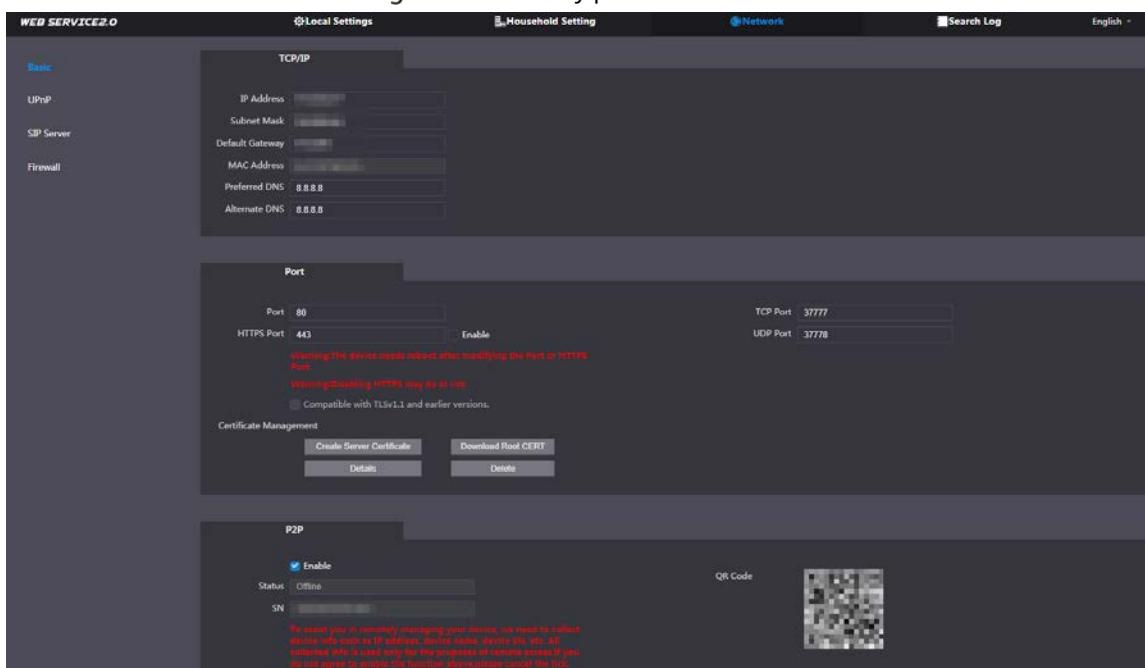
## 6.1 Básico

### 6.1.1 TCP/IP

Puede modificar la dirección IP, la máscara de subred, la puerta de enlace predeterminada y el DNS del VTO.

**Step 1** Seleccionar **Red > Básico**.

Figure 6-1 TCP/IP y puerto



**Step 2** Configure los parámetros y luego haga clic en **Ahorrar**.

El VTO se reiniciará y deberá modificar la dirección IP de su PC al mismo segmento de red que el VTO para iniciar sesión nuevamente.

### 6.1.2 Puerto

Tabla 6-1 Descripción de parámetros

Parámetro	Descripción
Puerto	80 por defecto. Si ya se usó, elija cualquier número del 1025 al 65535 según sea necesario. Puedes entrar <a href="http://VTO Dirección IP:Puerto">http://VTO Dirección IP:Puerto</a> para iniciar sesión en el VTO.
Puerto HTTPS	Habilítalo y haz clic <b>Ahorrar</b> . Ya puedes entrar <a href="https://VTO Dirección IP:Puerto HTTPS">https://VTO Dirección IP:Puerto HTTPS</a> para iniciar sesión en el VTO.
Puerto TCP/UDP	Se utiliza para acceder al VTO con dispositivos en otras redes. Consulte "6.2 UPnP" para obtener más información.
Crear Servidor	La identificación digital única de VTO para el protocolo SSL. Para uso por primera vez

Parámetro	Descripción
Certificado	<p>o después de cambiar la dirección IP del VTO, debe realizar este proceso.</p> <p></p> <p>Si elimina el certificado que se ha creado, no se puede deshacer.</p>
Descargar raíz certificado	<p>Si está utilizando una PC que nunca ha iniciado sesión en VTO, debe descargar el certificado raíz, hacer doble clic para instalarlo y luego puede usar la función HTTPS mencionada anteriormente.</p> <p></p> <p>Si elimina el certificado que se ha instalado, no se puede deshacer.</p>

## 6.1.3 P2P

Habilitar el P2P función, y luego puede escanear el código QR con su teléfono para agregar el VTO a la aplicación en su teléfono inteligente.



si configuras **Tipo de dispositivo** a **Apartamento pequeño** (consulte "4.1 Básico"), el código QR se reubicará en

**Configuración del hogar > Gestión de VTH.** Hacer clic  de cualquier número de habitación, y luego puedes ver tanto el número de serie como el código QR del VTO.

## 6.2 UPnP

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

### Preparación

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

### 6.2.1 Habilitación de servicios UPnP

**Step 1** Seleccionar **Red > UPnP**.

**Step 2** Habilite los servicios enumerados según sea necesario.

**Step 3** Seleccionar **Permitir**.

**Step 4** Hacer clic **Ahorrar**.

### 6.2.2 Adición de servicios UPnP

**Step 1** Seleccionar **Red > UPnP**.

Step 2 Hacer clic **Agregar**.

Step 3 Configure los parámetros según sea necesario.

Figure 6-2 Agregar un servicio UPnP

The screenshot shows a dark-themed 'Add' dialog box. At the top left is the word 'Add'. On the right is a close button ('X'). Below the title are two radio buttons: 'ON' (gray) and 'OFF' (blue, selected). The main area contains five input fields: 'Service Name', 'Service Type', 'Protocol' (with 'TCP' selected), 'Internal Port', and 'External Port'. At the bottom are two buttons: 'Save' and 'Cancel'.

Tabla 6-2 Descripción de parámetros

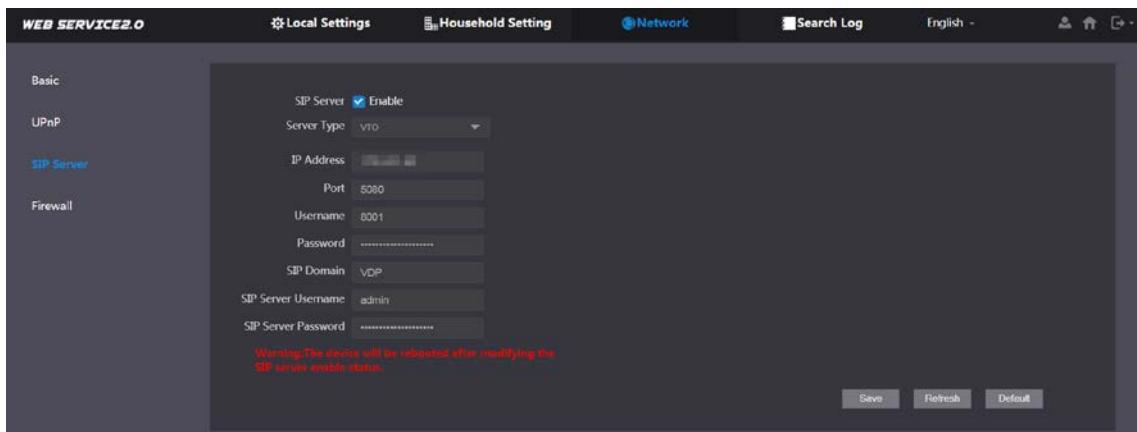
Parámetro	Descripción
Nombre del Servicio	Ingrese la información según sea necesario.
Tipo de servicio	
Protocolo	Seleccionar <b>TCP</b> o <b>UDP</b> según sea necesario.
Puerto interno	Utilice el número de puerto del 1024 al 5000.
Puerto externo	 <ul style="list-style-type: none"><li>- No utilice el número de puerto 1-1023 para evitar conflictos.</li><li>- Si necesita configurar esta función para varios dispositivos, asegúrese de que los puertos no sean los mismos.</li><li>- El número de puerto que utilice no debe estar ocupado.</li><li>- El número de puerto interno y externo debe ser el mismo.</li></ul>

## 6.3 Servidor SIP

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

Step 1 Seleccionar **Red > Servidor SIP**.

Figure 6-3 Servidor SIP



**Step 2** Seleccione un tipo de servidor según sea necesario.

- El VTO que ha iniciado sesión como servidor SIP:

Permitir **Servidor SIP** y haga clic en **Ahorrar**, y luego el VTO se reiniciará. Puede agregar VTO y VTH a este VTO. Consulte los detalles en "5 Configuración del hogar".



Si el VTO en el que ha iniciado sesión no es un servidor SIP, no habilite **Servidor SIP**; de lo contrario la conexión fallará.

- Si otro VTO funciona como servidor SIP:

No active **servidor SIP**. Colocar **Tipo de servidor** a **VTO**, configure los parámetros y luego haga clic en **Ahorrar**.

Tabla 6-3 Configuración del servidor SIP

Parámetro	Descripción
Dirección IP	Dirección IP de VTO.
Puerto	<ul style="list-style-type: none"> <li>● 5060 por defecto cuando VTO funciona como servidor SIP. 5080 por defecto cuando la plataforma funciona como servidor SIP.</li> </ul>
Nombre de usuario	Manténgalo predeterminado.
Contraseña	
Dominio SIP	VDP.
Nombre de usuario del servidor SIP	
Contraseña del servidor SIP	Nombre de usuario y contraseña de inicio de sesión de la interfaz web del VTO.

- Si otros servidores funcionan como servidor SIP:

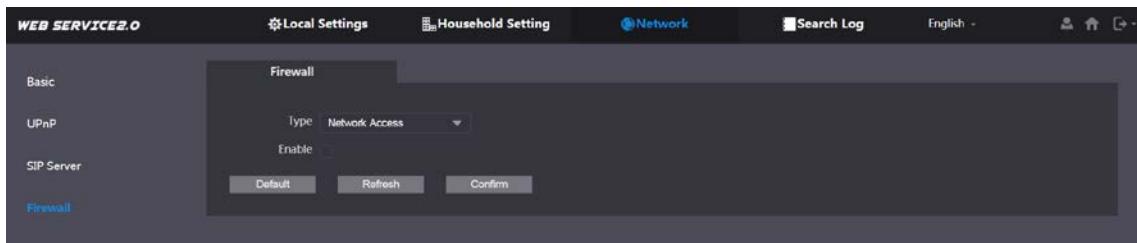
Seleccione el **Tipo de servidor** según sea necesario y, a continuación, consulte el manual correspondiente para obtener más información.

## 6.4 cortafuegos

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

**Step 1** Seleccionar **Red > Cortafuegos**.

Figure 6-4 cortafuegos



Step 2 Seleccione uno o más tipos de firewall y luego habilítelos.

Step 3 Configure los parámetros.

Tabla 6-4 Descripción del tipo de cortafuegos

Tipo	Descripción
Acceso a la red	Seleccione cualquiera <b>Lista de permitidos</b> o <b>Lista de bloqueos</b> , a continuación, agregue una dirección IP o un segmento al que se permita o deniegue el acceso al VTO.
PING Prohibido	El VTO no responderá al ping para evitar ataques de ping.
Anti-semiunión	Protege el rendimiento de VTO al bloquear el exceso de paquetes SYN.

## 7 Gestión de registros

Seleccionar **Registro de búsqueda**, y luego puede ver el historial de llamadas, registros de alarmas, registros de desbloqueo y varios registros del sistema, y exportarlos a su PC según sea necesario.



Si el almacenamiento está lleno, se sobrescribirán los registros más antiguos. Haga una copia de seguridad de los registros según sea necesario.

# Appendix 1 Recomendaciones de ciberseguridad

La ciberseguridad es más que una palabra de moda: es algo que pertenece a todos los dispositivos que están conectados a Internet. La videovigilancia IP no es inmune a los riesgos cibernéticos, pero tomar medidas básicas para proteger y fortalecer las redes y los dispositivos en red los hará menos susceptibles a los ataques. A continuación se presentan algunos consejos y recomendaciones sobre cómo crear un sistema de seguridad más seguro.

## **Acciones obligatorias que se deben tomar para la seguridad básica de la red del dispositivo:**

### **1. Use contraseñas seguras**

Consulte las siguientes sugerencias para establecer contraseñas:

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

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

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

## **Recomendaciones "agradables de tener" para mejorar la seguridad de la red de su dispositivo:**

### **1. Protección física**

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

### **2. Cambie las contraseñas regularmente**

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

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

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

### **4. Habilitar bloqueo de cuenta**

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

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

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

## **6. Habilitar HTTPS**

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

## **7. Enlace de dirección MAC**

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

## **8. Asigne cuentas y privilegios de manera razonable**

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

## **9. Deshabilite los servicios innecesarios y elija modos seguros**

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

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

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

## **10. Transmisión encriptada de audio y video**

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

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

## **11. Auditoría segura**

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

## **12. Registro de red**

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

## **13. Construya un entorno de red seguro**

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

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