

Estación de puerta de villa

Manual de usuario



Prefacio

General

Este manual presenta las operaciones básicas de la estación de puerta digital (en lo sucesivo, "VTO").

Las instrucciones de seguridad

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

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

Revisión histórica

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

Aviso de protección de privacidad

Como usuario del dispositivo o controlador de datos, puede recopilar datos personales de otros, como su rostro, huellas dactilares y número de matrícula. Debe cumplir con las leyes y regulaciones locales de protección de la privacidad para proteger los derechos e intereses legítimos de otras personas mediante la implementación de medidas que incluyen, entre otras: Proporcionar una identificación clara y visible para informar a las personas sobre la existencia del área de vigilancia y proporcione la información de contacto requerida.

Sobre el Manual

- El manual es solo para referencia. Se pueden encontrar ligeras diferencias entre el manual y el producto.
- No somos responsables de las pérdidas sufridas debido a la operación del producto de manera que no cumpla con el manual.
- El manual se actualizará de acuerdo con las últimas leyes y reglamentos de las jurisdicciones relacionadas. Para obtener información detallada, consulte el manual del usuario en papel, use nuestro CD-ROM, escanee el código QR o visite nuestro sitio web oficial. El manual es solo para referencia. Se pueden encontrar ligeras diferencias

entre la versión electrónica y la versión en papel.

- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto pueden dar lugar a que aparezcan algunas diferencias entre el producto real y el manual. Póngase en contacto con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria.
- Puede haber errores en la impresión o desviaciones en la descripción de las funciones, operaciones y datos técnicos. Si hay alguna duda o disputa, nos reservamos el derecho de dar una explicación final. Actualice el software del lector o pruebe con otro software del lector convencional si no se puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas registradas y nombres de compañías en el manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, comuníquese con el proveedor o el servicio al cliente si ocurre algún problema mientras utilizando el dispositivo.
- Si hay alguna duda o controversia, nos reservamos el derecho de la explicación final.

Medidas de seguridad y advertencias importantes

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

Requisitos de operación



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

requerimientos de instalación



ADVERTENCIA

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



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

Tabla de contenido

Prefacio.....	I Medidas
de seguridad y advertencias importantes	III 1
Inicialización del VTO	1
1.2 Web.....	1
1.3 APLICACIÓN DMSS	3
2 Inicio de sesión y restablecimiento de contraseña	7
2.1 Acceso	7
2.2 Restablecimiento de contraseña	7
3 Página de inicio.....	9
4 Ajustes locales	10
4.1 Ajustes básicos.....	10
4.2 Audio video.....	13
4.3 Ajustes de control de acceso	15
4.3.1 Locales	15
4.3.2 RS-485	dieciséis
4.4 Sistema.....	17
4.5 Seguridad	18
4.6 Usuario de Onvif.....	20
4.7 Actualizar.....	21
4.8 Subir archivo.....	21
4.9 Información legal	22
5 Entorno doméstico	23
5.1 Gestión de nº de VTO	23
5.2 Gestión de VTH	24
5.3 Gestión de personal	25
5.4 Gestión de VTS	28
5.5 Estado	29
6 Red.....	30
6.1 Básico	30
6.1.1 TCP/IP	30
6.1.2 Puerto	31
6.1.3 Servicio en la nube	32
6.2 UPnP.....	32
6.2.2 Habilidadación de los servicios UPnP.....	32
6.2.3 Adición de servicios UPnP.....	33
6.3 Servidor SIP	33
6.4 Wifi.....	35
6.5 cortafuegos	36
7 Gestión de registros	37
7.1 Llamada	37
7.2 Alarma	37
7.3 Desbloquear	38
7.4 Tronco.....	38
Configuración del modelo de 8 botones	39

8.1 Conexión de cable	39
8.2 Configuración VTH	39
Appendix 1 Recomendaciones de ciberseguridad	41

1 Inicializar el VTO

Puede inicializar el VTO en la web o a través de la aplicación DMSS, según la conexión de red que admita su modelo.

Tabla 1-1 Tipo de inicialización

Conexión de red	Inicialización a través de la web	Inicialización a través de la aplicación DMSS
Conexión wifi	No	Sí
Conexión por cable	Sí	Sí

1.2 Web

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

Step 1 Encienda el VTO.

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



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

Figure 1-2 Inicialización del dispositivo

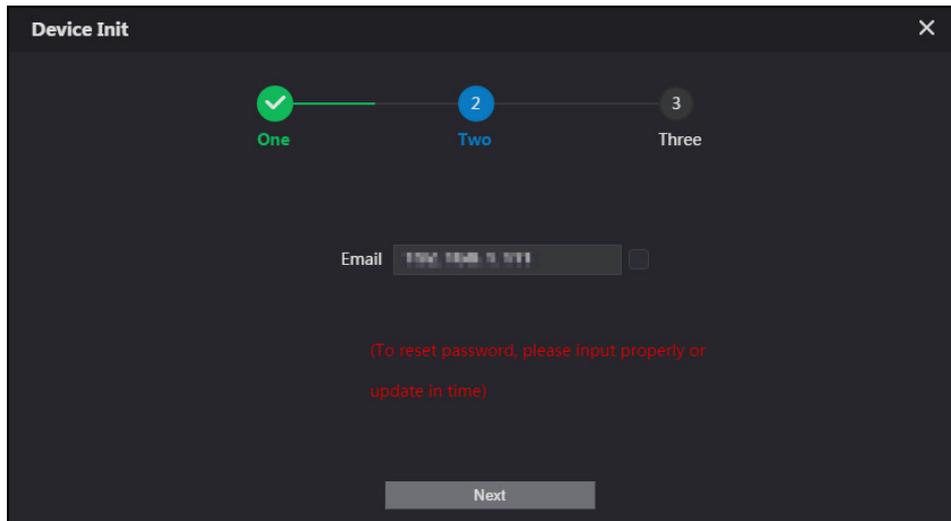
The screenshot shows a dark-themed 'Device Init' window. At the top, there are three numbered steps: '1 One', '2 Two', and '3 Three'. Step 1 is highlighted in blue. Below the steps, the 'Username' field is pre-filled with 'admin'. The 'Password' field is empty, with three buttons below it labeled 'Low', 'Middle', and 'High'. The 'Confirm Password' field is also empty. A 'Next' button is located at the bottom center of the window.

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



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

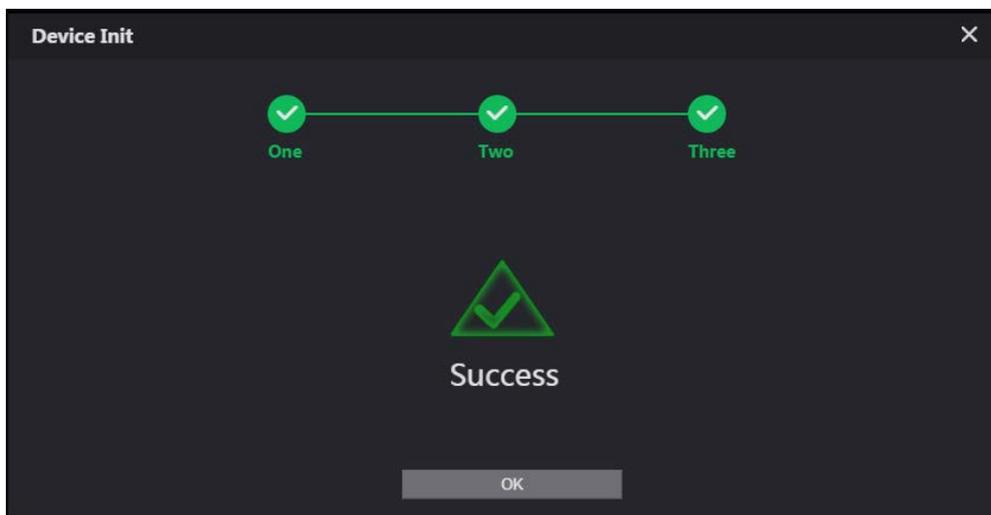
Figure 1-3 Establecer una dirección de correo electrónico



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

Step 5 **Próximo.**

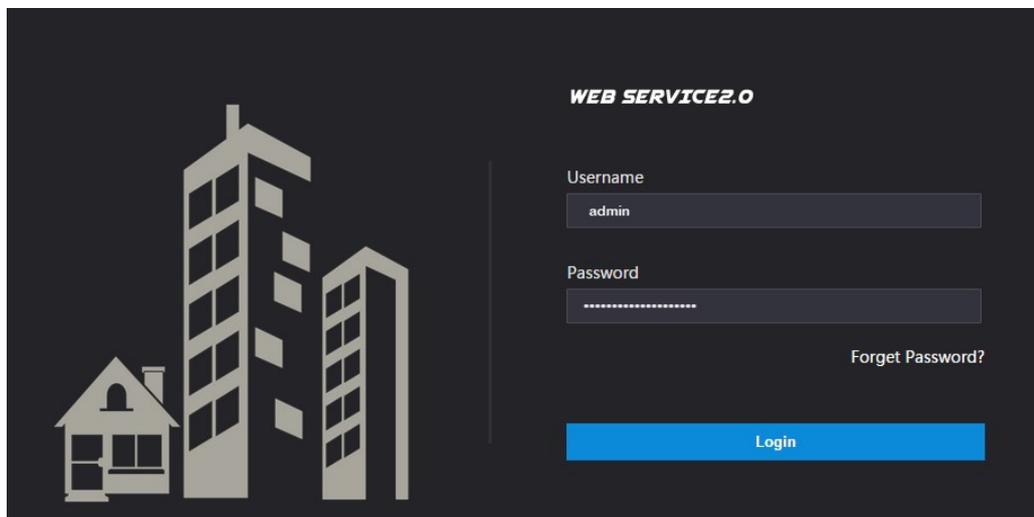
Figure 1-4 Inicialización exitosa



Step 6 Hacer clic **OK** para ir a la página de inicio de sesión.

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

Figure 1-5 Página de inicio de sesión



1.3 APLICACIÓN DMSS

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

requisitos previos

Ha descargado el DMSS en la tienda de aplicaciones (iOS) o Google Play (Android), ha creado una cuenta y ha iniciado sesión en la aplicación.

Operaciones

Step 1 Encienda el VTO.

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



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

Step 3 Agregue el VTO a la aplicación DMSS. 1) En el **Casa** pantalla, toque  y luego seleccione **NS/escaneo**.
2) Agregue un VTO.

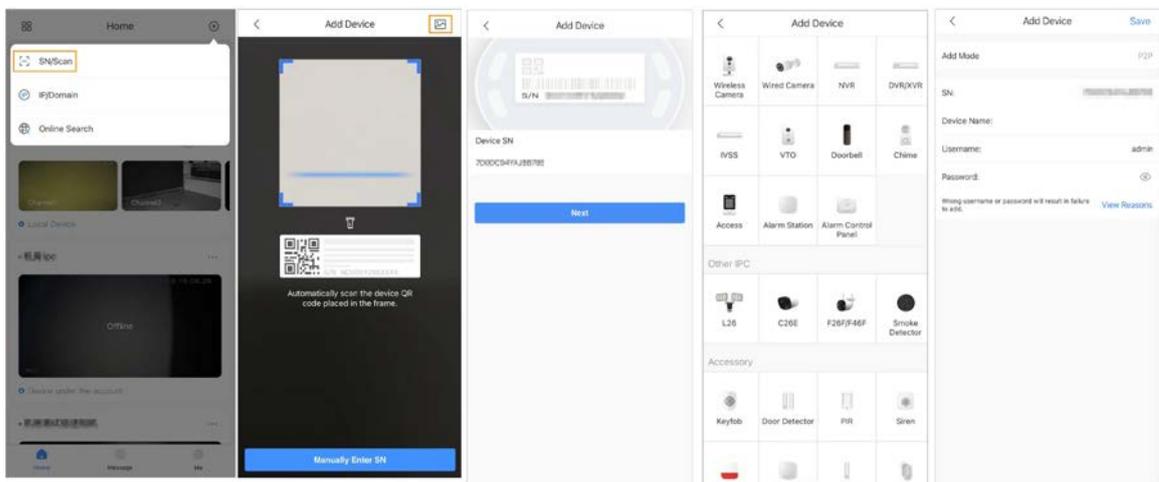
Puede agregar escaneando el código QR en el panel posterior del VTO.

3) El número SN del VTO aparece automáticamente y luego toque **Próximo**.

4) Seleccione el tipo de dispositivo como **VTO**, a continuación, aparece la información del dispositivo.

5) Toca **Ver Razones**.

Figure 1-6 Agregar VTO a DMSS



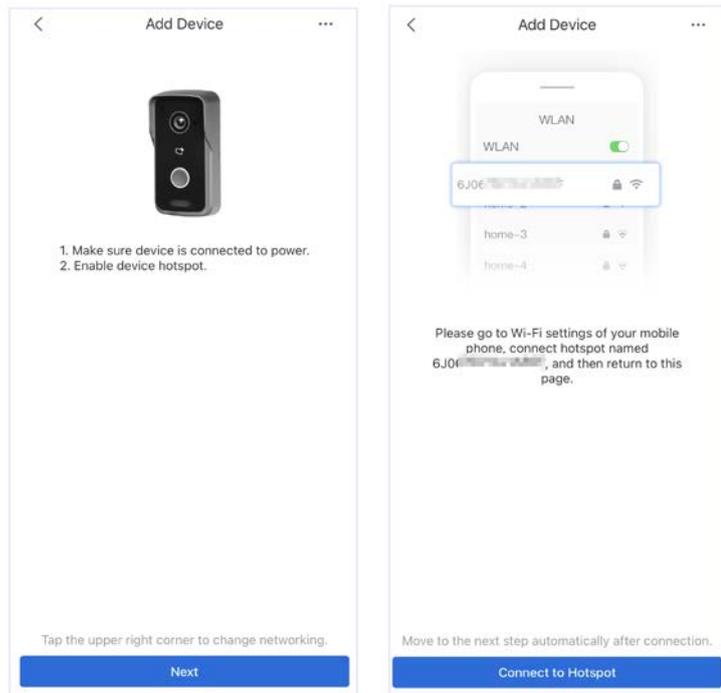
6) Configure la red cambiando la red a **Configuración AP** y luego toque **Próximo**.

7) Conecte su teléfono al punto de acceso que acaba de habilitar en el VTO.



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

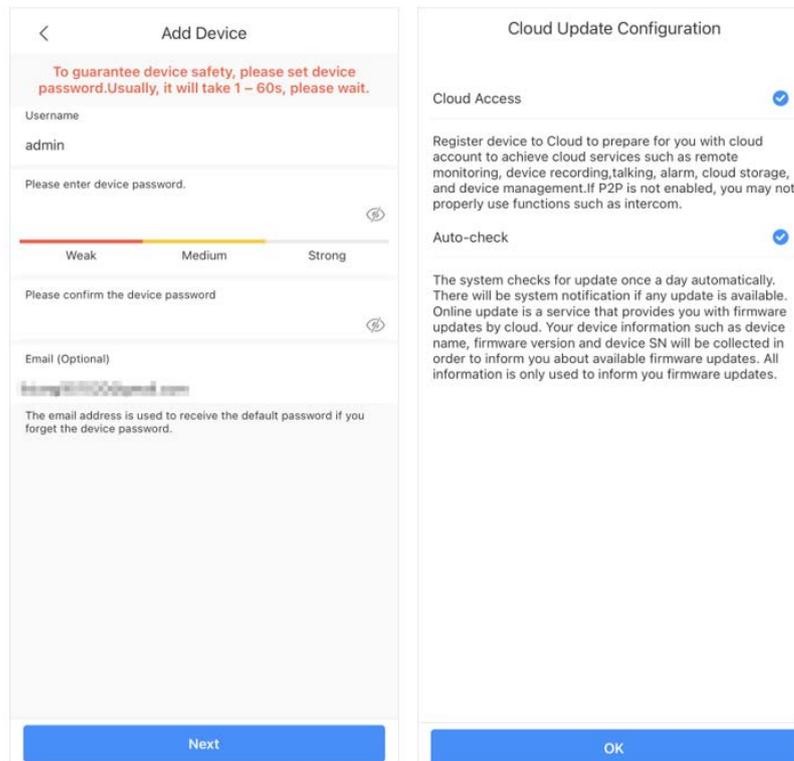
Figure 1-7 Configuración de puntos de acceso



Step 4 Inicialización completa según las instrucciones de la aplicación.

- 1) Ingrese la contraseña que planeó para el VTO, confírmela y luego toque **Próximo**.
- 2) Seleccione **Acceso a la nube** **Verificación automática** y luego toque **OK**. El proceso de inicialización se ha completado.

Figure 1-8 Inicialización

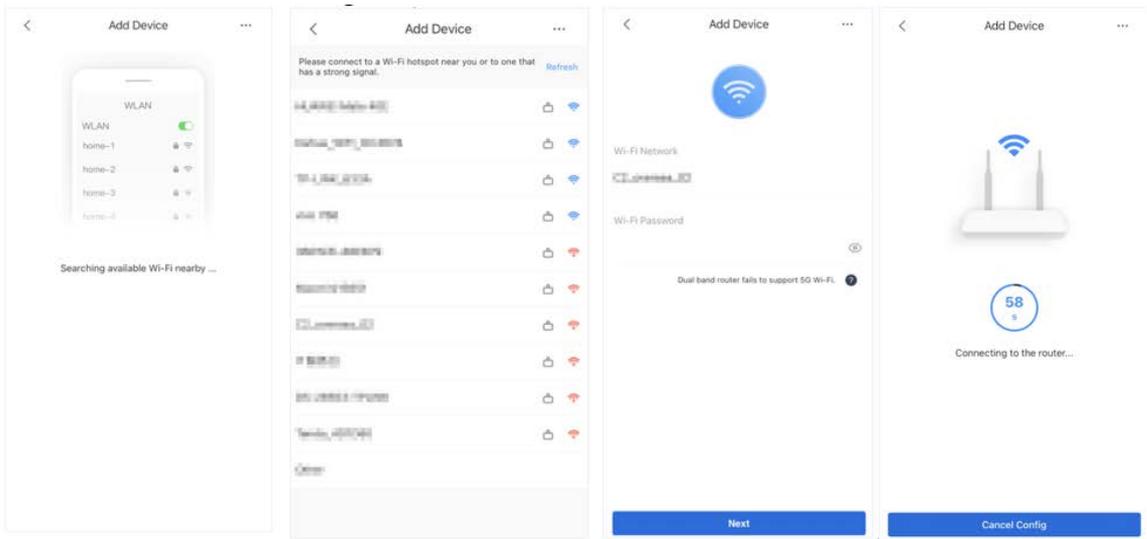


Step 5 Conecte el VTO a la red a través de Wi-Fi. 1)

Seleccione un Wi-Fi disponible.

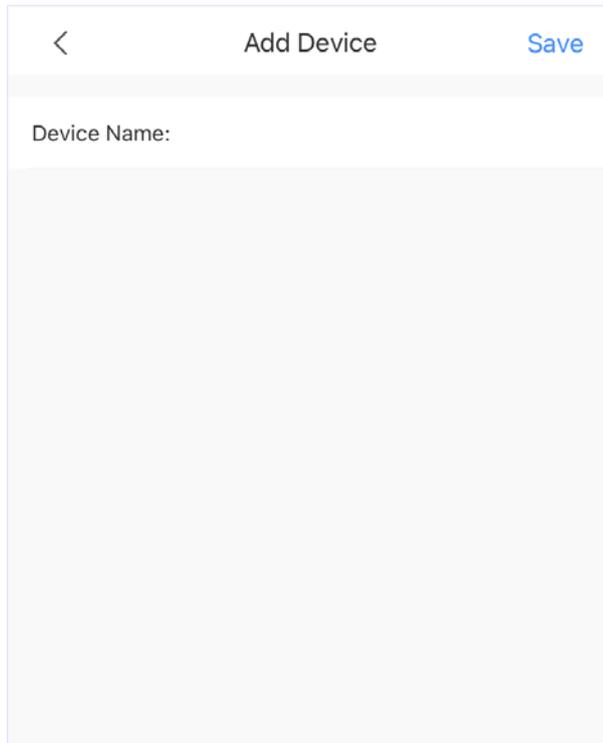
- 2) Introduzca la contraseña y toque **Próximo**. Espere a que el VTO se conecte al enrutador.

Figure 1-9 Conexión wifi



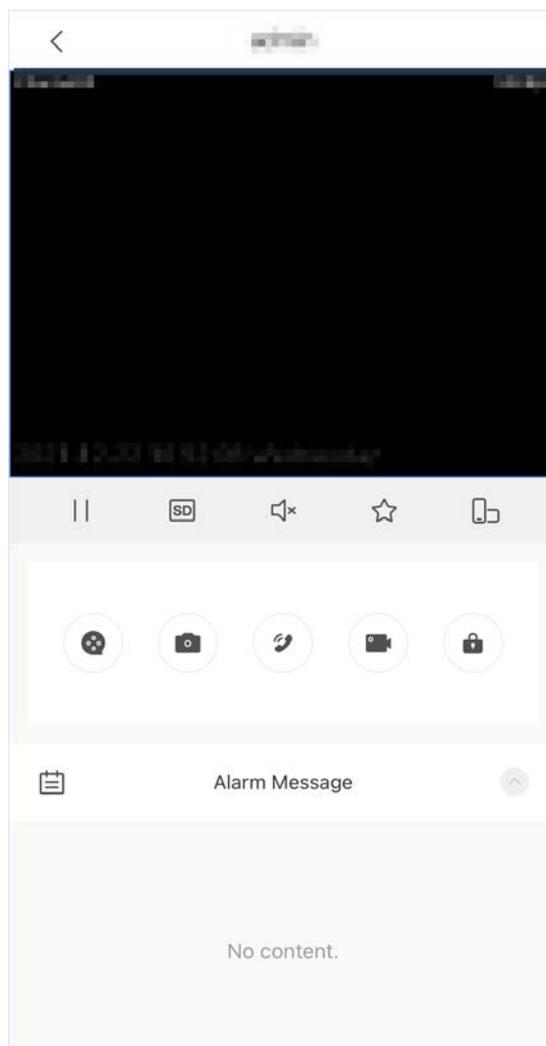
Step 6 Configure el nombre del dispositivo y toque **Salvar**.

Figure 1-10 Configurar el nombre del dispositivo



Step 7 Vea el video de monitoreo de la cámara en el VTO.

Figure 1-11 Supervisión



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.

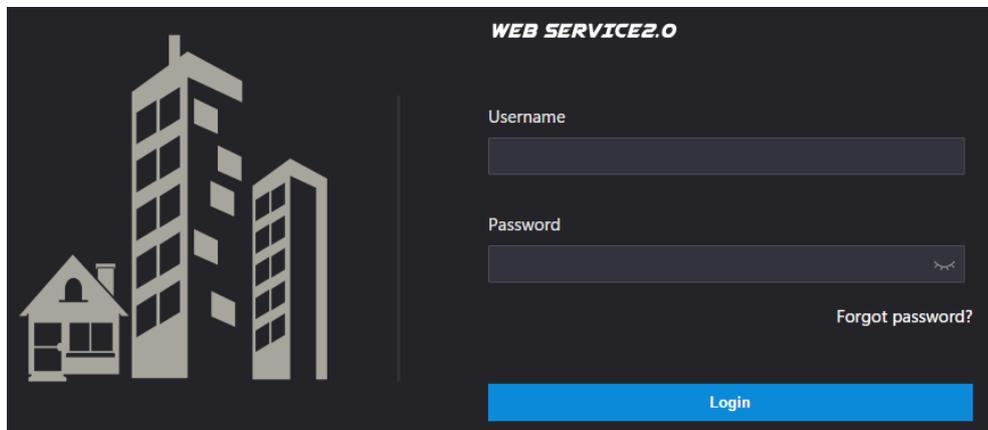
Step 1 Vaya a la dirección IP del VTO en el navegador.



Para iniciar sesión por primera vez, ingrese la IP predeterminada (192.168.1.108). Si tiene varios VTO, nosotros 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**.

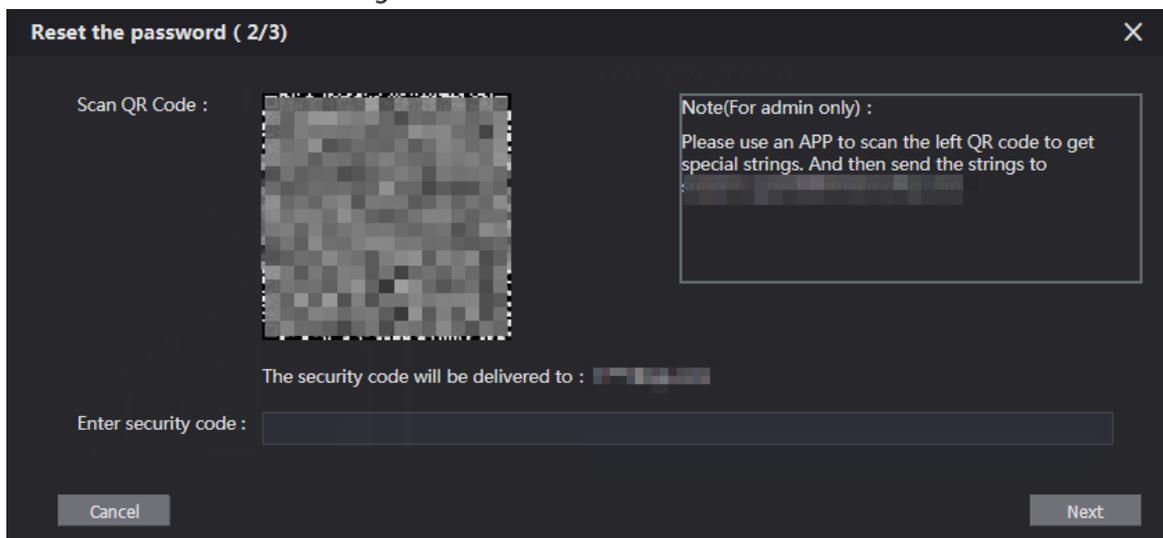
Figure 2-1 Acceso



2.2 Restablecimiento de contraseña

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

Figure 2-2 restablecer la contraseña



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

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

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 bloqueado durante 5 minutos.

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

3 Página de inicio

Figure 3-1 Página de inicio

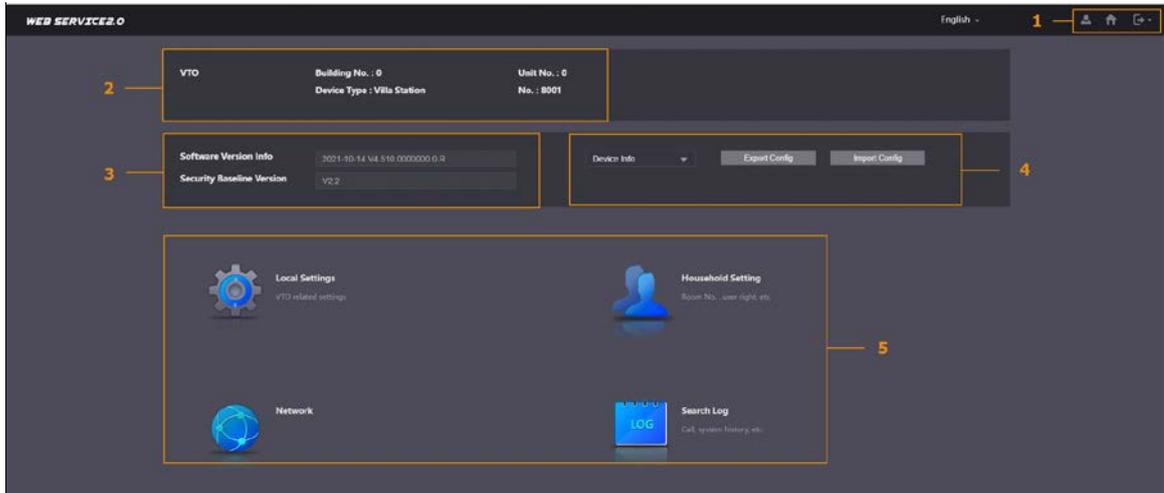


Tabla 3-1 Introducción a la página de inicio

No.	Función	Descripción
1	Función general	<ul style="list-style-type: none"> : Cambie la contraseña y su dirección de correo electrónico. : Ir a la pagina principal. : Cierre la sesión, reinicie el VTO o restaure el VTO a la configuración de fábrica. <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 página web y las funciones pueden ser diferentes según el modelo.</p>

4 Configuraciones locales

Este capítulo presenta la configuración detallada del VTO.



Se pueden encontrar ligeras diferencias en diferentes modelos.

4.1 Ajustes básicos

Propiedades y eventos del dispositivo

Step 1 Seleccione **Configuraciones locales**>

Step 2 **Básico**. Configure los parámetros.

Figure 4-1 Básico

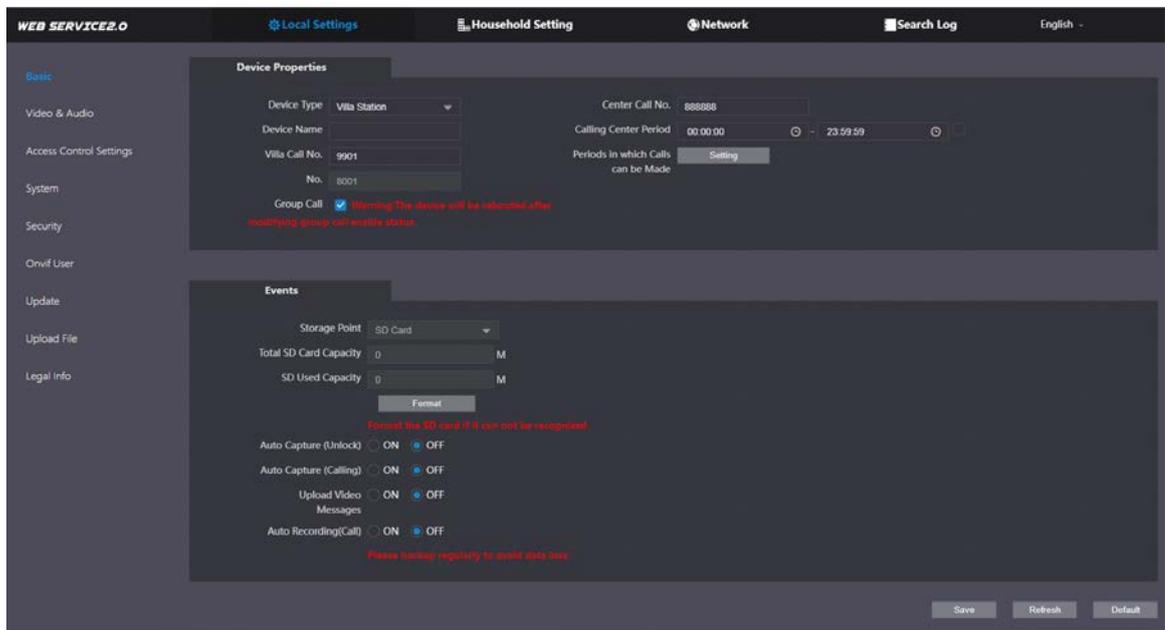


Tabla 4-1 Descripción de parámetros básicos

Parámetro	Descripción
Tipo de dispositivo	Seleccione Estación Villa o Apartamento pequeño .
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. Configura la hora y activa la función para que recibas llamadas solo en ese periodo.
Número de llamada de Villa	Se utiliza para llamar a VTH.

Parámetro	Descripción
No.	Se usa para diferenciar cada VTO, y le recomendamos que lo configure según la unidad o el número de edificio, y luego puede agregar VTO al servidor SIP usando sus números.  El número no se puede cambiar cuando el VTO sirve como servidor SIP.
Periodos en los que se pueden realizar llamadas	Configure la hora si solo desea recibir llamadas de VTH 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.
Punto de almacenamiento	Tarjeta SD por defecto.
Tarjeta SD total	Muestra la capacidad total y utilizada de la tarjeta SD. Puedes hacer clic Formato para eliminar todos los datos de la tarjeta SD.
Capacidad	
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"> ● 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. ● Si solo se inserta una tarjeta SD en el VTH o el VTO, el mensaje de video se guardará solo en la tarjeta SD del VTH o el VTO. ● Si no se inserta una tarjeta SD en el VTH o VTO, no se guardará ningún mensaje de video.
Grabación automática (llamada)	Tome la grabación cuando el VTO esté en una llamada y guarde la grabación en la tarjeta SD del VTO.

Step 3 Hacer clic **Salvar**.

Diseño de fachada

Esta función solo está disponible para el modelo VTO con varios botones.

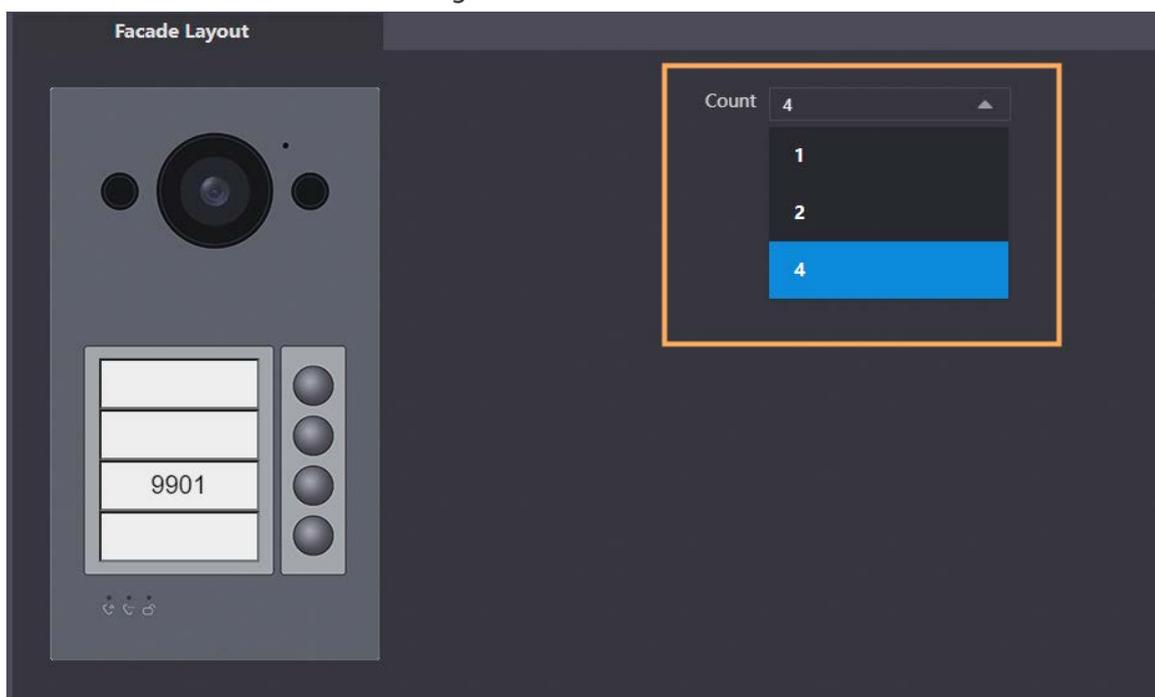
Step 1 Inicie sesión en la página web de VTO.

Step 2 Seleccione **Configuraciones locales > Básico**.

Step 3 En el **Diseño de fachada** sección, seleccione **Contar** escribe.

- Recuento 1: solo se puede vincular un número de habitación.
- Cuenta 2: Puede vincular dos números de habitación. Cuenta 4: puede vincular cuatro números de habitación.

Figure 4-2 Contar



Step 4 Haga clic en el módulo blanco y seleccione el número de habitación de la **Lista de habitaciones** que quiere atar.

Figure 4-3 Módulo blanco

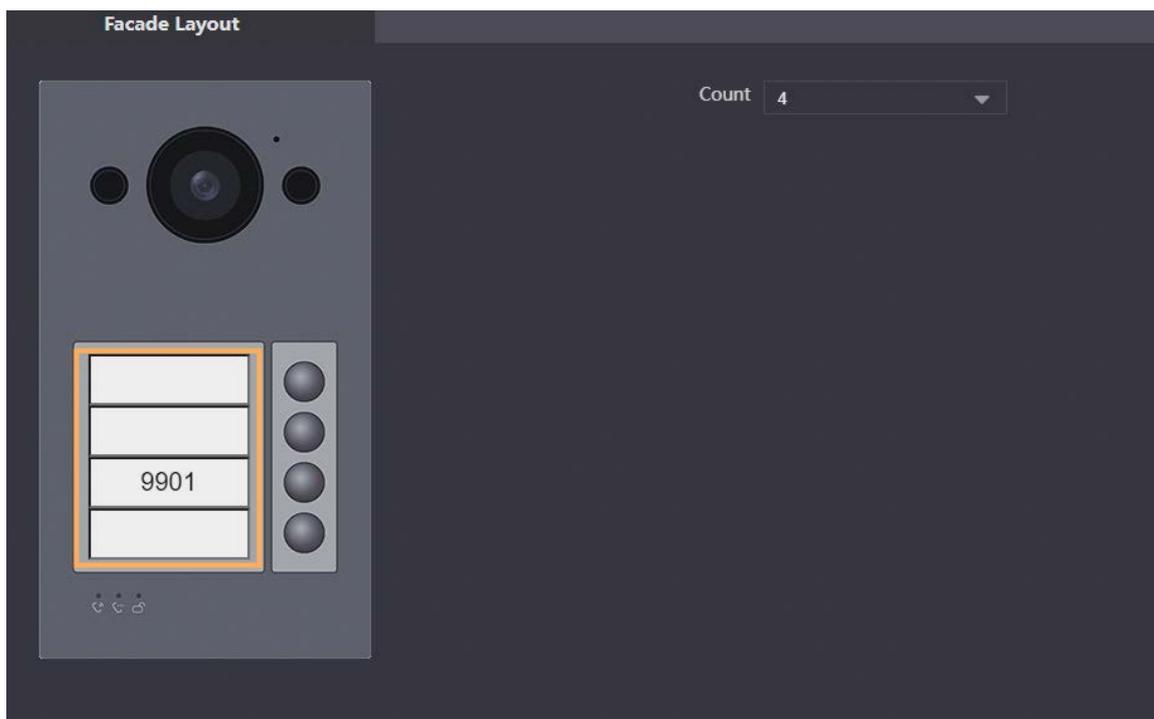
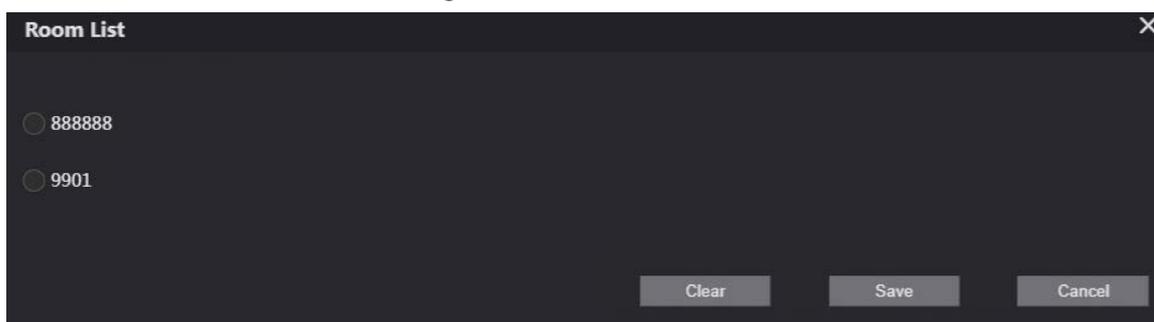


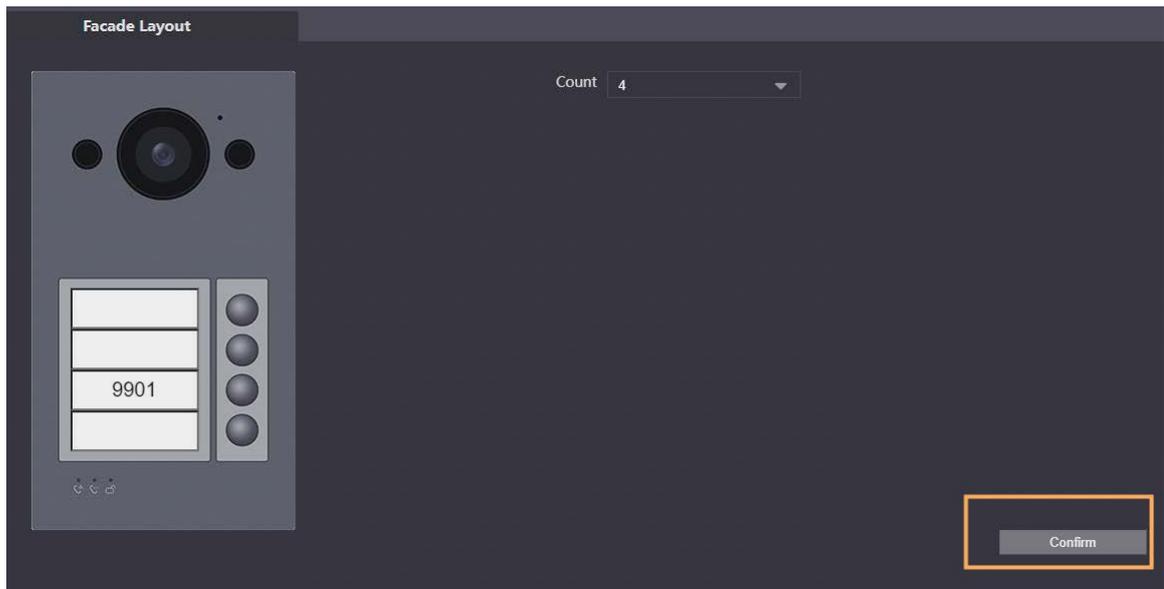
Figure 4-4 Lista de habitaciones



Step 5 Hacer clic **Salvar** para guardar el número de habitación seleccionado.

Step 6 Hacer clic **Confirmar** para guardar todos los ajustes.

Figure 4-5 Confirmar



4.2 Audio video

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

Step 1 Seleccione **Configuraciones locales** > **Audio video**.

Figure 4-6 Video

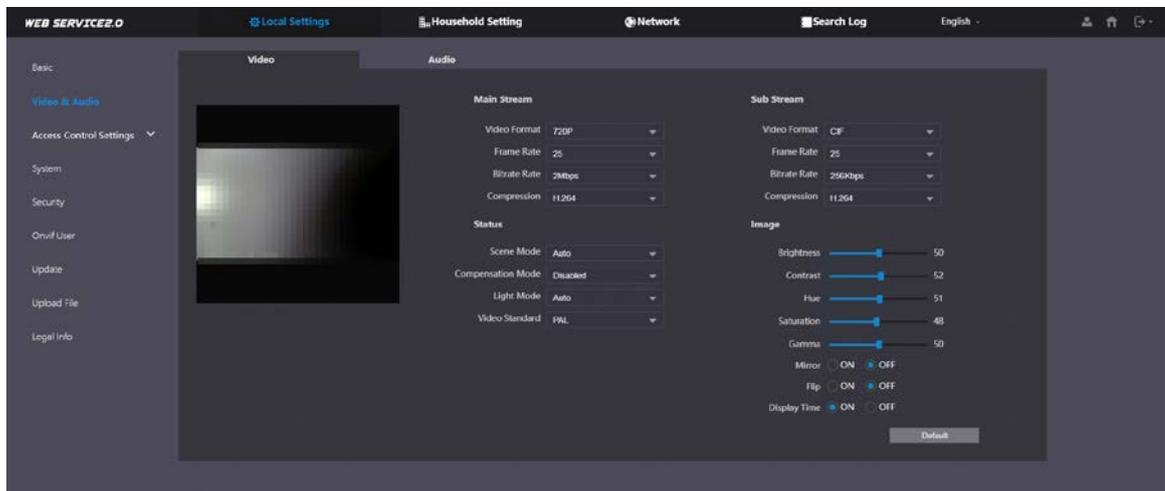
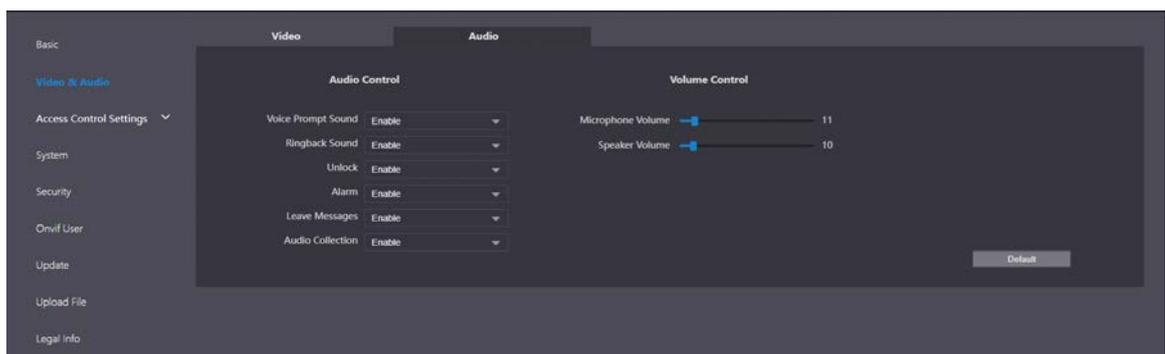


Figure 4-7 Audio



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

Tabla 4-2 Descripción de los parámetros de video

Parámetro		Descripción
Principal Arroyo	Formato de video	<ul style="list-style-type: none"> ● 720P: 1280 × 720. ● WVGA: 800 × 480. ● D1: 720 × 480. ● C.I.F.: 352 × 288.
	Cuadros por segundo	El rango es de 1 a 25. Cuanto mayor sea el valor, más suave será el video, pero requiere más ancho de banda.
	Tasa de bits	Incluye 768 Kbps, 896 Kbps, 1024 Kbps, 1,25 Mbps, 1,5 Mbps, 1,75 Mbps, 2 Mbps y 4 Mbps. Cuanto mayor sea el valor, mejor será la calidad del video, pero requiere más ancho de banda.
	Compresión	<ul style="list-style-type: none"> - H.264. - H.265.  <p>En comparación con H.264, H.265 requiere un ancho de banda más pequeño.</p>
Sub Arroyo	Formato de video	<ul style="list-style-type: none"> - 1080P: 1920 × 1080. - WVGA: 800 × 480. - QVGA: 320 × 240. D1: 720 × 480. - C.I.F.: 352 × 288.
	Cuadros por segundo	El rango es de 1 a 25. Cuanto mayor sea el valor, más suave será el video, pero requiere más ancho de banda.
	Tasa de bits	Incluye 224 Kbps, 256 Kbps, 320 Kbps, 384 Kbps, 448 Kbps, 512 Kbps, 640 Kbps, 768 Kbps. Cuanto mayor sea el valor, mejor será la calidad del video, pero requiere más ancho de banda.
	Compresión	<ul style="list-style-type: none"> - H.264. - H.265.  <p>En comparación con H.264, H.265 requiere un ancho de banda más pequeño.</p>
Estado	Modo escena	Seleccionar de Auto , Discapacitado , Soleado y Noche . Auto se selecciona de forma predeterminada.
	Compensación Modo	<ul style="list-style-type: none"> ● CLB: Compensación de contraluz. Mejorar la claridad del objetivo en la imagen. ● WDR: Amplio rango dinámico. Mejore el brillo de las áreas oscuras y reduzca el brillo de las áreas brillantes para mejorar la imagen. ● LLC: Compensación de luz alta. Reduzca el brillo de los puntos fuertes para mejorar la imagen general.
	Modo de luz	Seleccionar de NO , CAROLINA DEL NORTE , Auto y Programado .
	Estándar de vídeo	Seleccione CAMARADA o NTSC según tu zona.  <p>CAMARADA se utiliza principalmente en China y Europa, y NTSC principalmente en el Estados Unidos y Japón.</p>

Parámetro		Descripción
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 mayor 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.
	Ganar Ajustamiento	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	Muestre la imagen con los lados izquierdo y derecho invertidos.
	Dar la vuelta	Muestre la imagen al revés.
	Tiempo de visualización	Muestra la hora y la fecha actuales en la imagen de vídeo.
Audio Control	Mensaje de voz Sonar	Activar o desactivar cada tipo de sonido.
	Volver a llamar Sonar	Ajuste el volumen según sea necesario.
	Alarma	
	Deja mensajes	
	desbloquear	
	Audio Colección	
Volumen Control	Micrófono	
	Volumen	
	Volumen del altavoz	

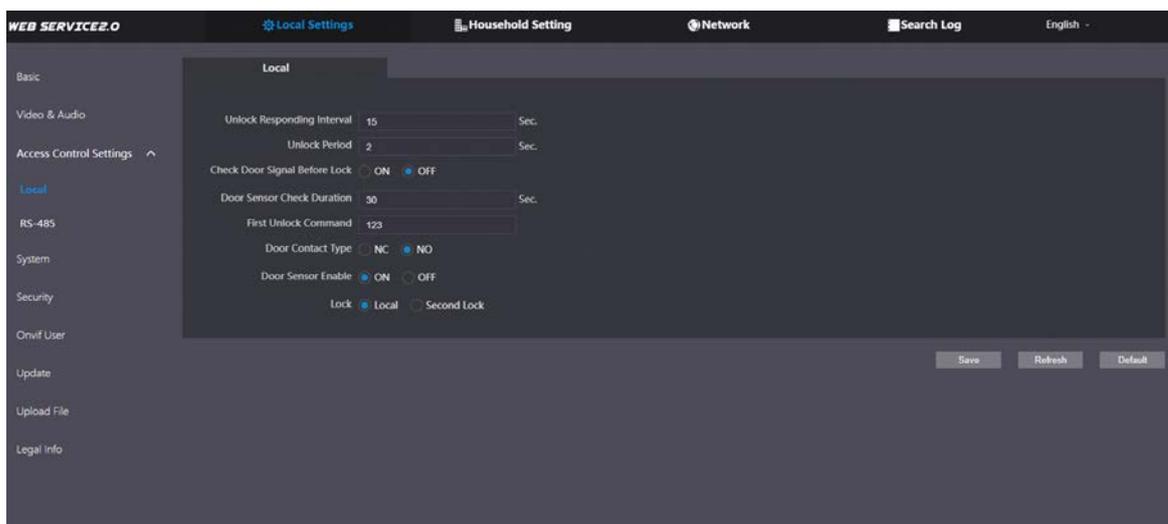
4.3 Configuración de control de acceso

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 Seleccione **Configuraciones locales > Configuración de control de acceso**.

Figure 4-8 Local



Step 2 Configure los parámetros.

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

Parámetro	Descripción
Desbloquear intervalo de respuesta	La puerta solo se puede desbloquear de nuevo después del intervalo.
Período de desbloqueo	El tiempo durante el cual la cerradura permanece desbloqueada.
Verifique la señal de la puerta antes de bloquear	Seleccione EnoApagado según sea necesario.
Duración de la comprobación del sensor de puerta	Si la puerta está desbloqueada por más tiempo que el Duración de la comprobación del sensor de puerta , se activará la alarma del sensor de la puerta y se enviará la alarma al centro de gestión.  Debe instalar un contacto de puerta para configurar este parámetro.
Primer comando de desbloqueo	Puede conectar un teléfono de terceros, como un teléfono SIP, al VTO y usar el comando para abrir la puerta de forma remota.
Tipo de contacto de puerta	<ul style="list-style-type: none"> ● CAROLINA DEL NORTE: Normalmente cerrado. ● NO: Normalmente abierto.
Habilitar sensor de puerta	Sincronice el estado del sensor de la puerta con los monitores interiores (VTH).
Cerrar con llave	<ul style="list-style-type: none"> - Local: bloqueo local. Segundo - candado: 485 bloqueo. Seleccione el Cerrar con llave escriba para desbloquear el bloqueo que seleccione.

Step 3 Hacer clic **Salvar**.

4.3.2 RS-485

Seleccione **Configuración local > Configuración de control de acceso**, y luego configure los parámetros de la cerradura conectada a través del puerto RS-485.

Figure 4-9 Cerradura conectada a través del puerto RS-485

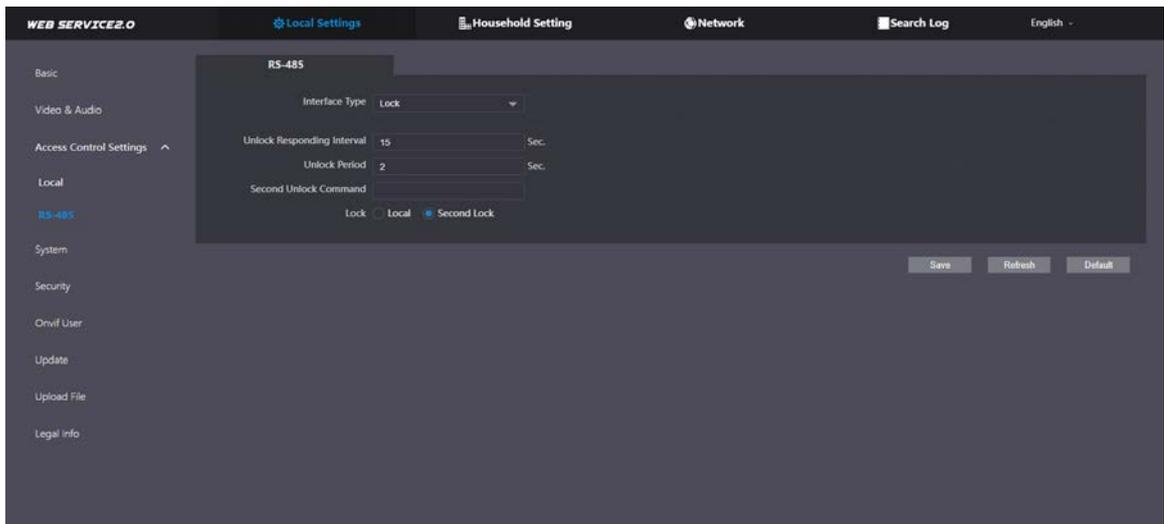


Tabla 4-4 Descripción de RS-485

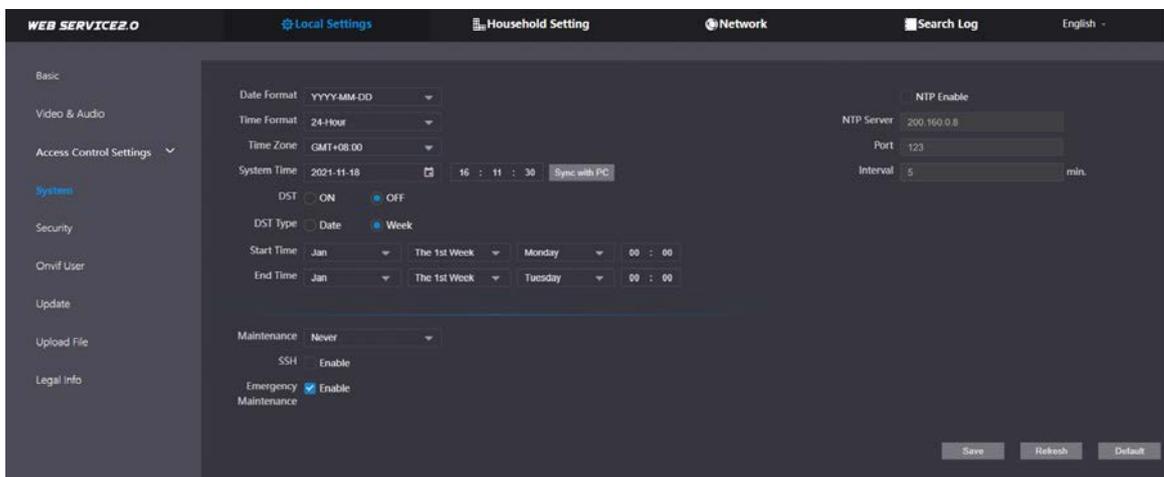
Parámetro	Descripción
Tipo de interfaz	Bloqueo por defecto.
Desbloquear intervalo de respuesta	La puerta solo se puede desbloquear de nuevo después del intervalo.
Período de desbloqueo	El tiempo durante el cual la cerradura permanece desbloqueada.
Segundo comando de desbloqueo	Puede conectar un teléfono de terceros, como un teléfono SIP, al VTO y usar el comando para abrir la puerta de forma remota. El comando predeterminado es 456.
Cerrar con llave	Selecciona el Cerrar con llave para desbloquear el bloqueo que seleccione. <ul style="list-style-type: none"> - Local: bloqueo local. Segundo - candado: 485 bloqueo.

4.4 Sistema

Configure parámetros de tiempo, servidor NTP y más.

Step 1 Seleccione **Configuraciones locales > Sistema**.

Figure 4-10 Sistema



Step 2 Configure los parámetros.

Tabla 4-5 Descripción de los parámetros del sistema

Parámetro	Descripción
Formato de fecha	<p>Seleccione uno de los siguientes:</p> <ul style="list-style-type: none"> - AAAA-MM-DD - MM-DD-AAAA - DD-MM-AAAA
Formato de tiempo	<p>Seleccione uno de los siguientes:</p> <ul style="list-style-type: none"> - 24 horas - 12 horas
Hora del sistema	 <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	Seleccione Fecha o Semana 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	<p>Defina la hora en que el VTO se reiniciará automáticamente.</p> <p>Elija entre Nunca, Lunes, Martes, Miércoles, Jueves, Viernes, Sábado y Domingo.</p>
SSH	<p>Puede conectar dispositivos de depuración al VTO a través del protocolo SSH.</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>Esta función ocupará los puertos 8088 y 8087.</p>
Habilitar NTP	Habilite NTP para que la hora del dispositivo se sincronice automáticamente con el servidor.

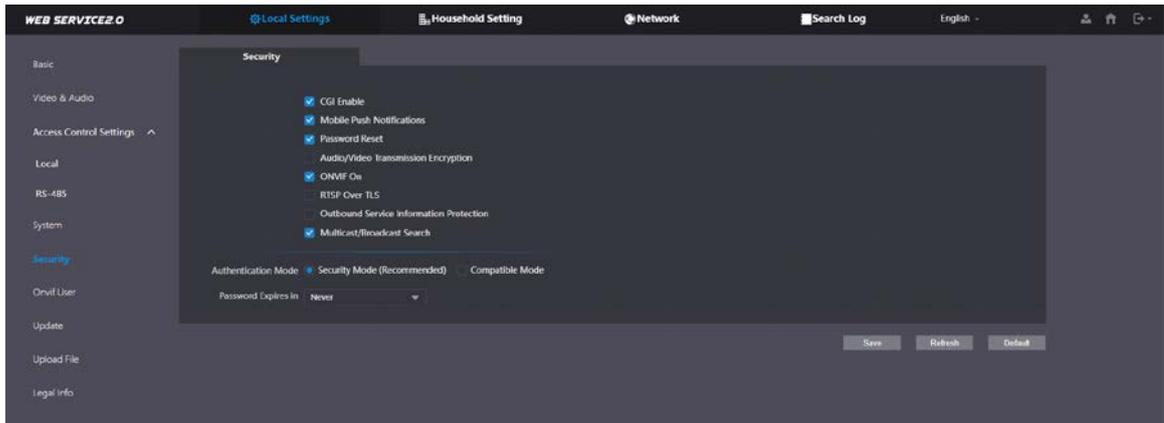
Step 3 Hacer clic **Salvar**.

4.5 Seguridad

Configure funciones que involucren la seguridad del dispositivo.

Step 1 Seleccione **Configuraciones locales > Seguridad**.

Figure 4-11 Seguridad



Step 2 Configure los parámetros.

Tabla 4-6 Descripción de los parámetros de seguridad

Parámetro	Descripción
Habilitar CGI	Habilite el uso del comando CGI.  Le recomendamos que lo apague. De lo contrario, el VTO podría estar expuesto a riesgos de seguridad y fuga de datos.
Notificación de inserción móvil	Envíe información a la aplicación en el teléfono inteligente.  Le recomendamos que lo apague si no necesita esta función. De lo contrario, el VTO podría estar expuesto a riesgos de seguridad y fuga de datos.
Restablecimiento de contraseña	Si está desactivado, no podrá restablecer la contraseña.
Audio Video Cifrado de transmisión	Cifre todos los datos durante la llamada de voz o video.  Le recomendamos que lo encienda. De lo contrario, el VTO podría estar expuesto a riesgos de seguridad y fuga de datos.
ONVIF encendido	Permita que un tercero extraiga la transmisión de video del VTO a través del protocolo ONVIF.  Recomendamos apagarlo. De lo contrario, el VTO podría estar expuesto a riesgos de seguridad y fuga de datos.
RTSP sobre TSL	Flujo de bits encriptado de salida a través de RTSP.  Le recomendamos que lo encienda. De lo contrario, el VTO podría estar expuesto a riesgos de seguridad y fuga de datos.
Servicio saliente Protección de la información	Proteja sus contraseñas.

Parámetro	Descripción
	 <p>Le recomendamos que lo encienda. De lo contrario, el VTO podría estar expuesto a riesgos de seguridad y fuga de datos.</p>
Multidifusión/Difusión Búsqueda	<p>Habilítelo y otros dispositivos encontrarán el VTO.</p>  <p>Le recomendamos que lo apague. De lo contrario, el VTO podría estar expuesto a riesgos de seguridad y fuga de datos.</p>
modo de autenticación	<ul style="list-style-type: none"> ● modo de seguridad(recomendado): Admite el inicio de sesión con autenticación Digest. ● Modo compatible: utilice el método de inicio de sesión antiguo.  <p>Le recomendamos que utilice el modo de seguridad. El modo compatible puede exponer el VTO a riesgos de seguridad y fuga de datos.</p>
La contraseña caduca en	<p>Seleccione un período de caducidad según sea necesario.</p>  <p>Le recomendamos que no utilice nunca. El VTO podría estar expuesto a riesgos de seguridad y fuga de datos si elige ese.</p>

Step 3 Hacer clic **Salvar**.

4.6 Usuario Onvif

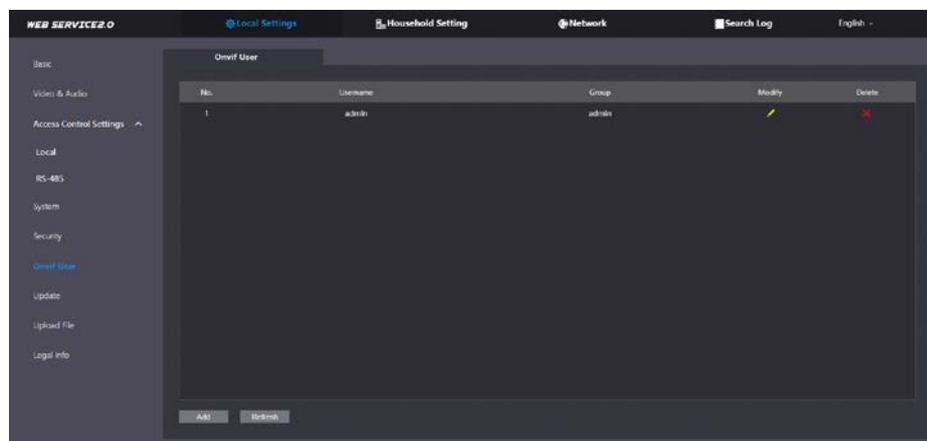
Agregue cuentas para dispositivos para monitorear el VTO a través del protocolo ONVIF.



La operación de eliminación de una cuenta no se puede deshacer.

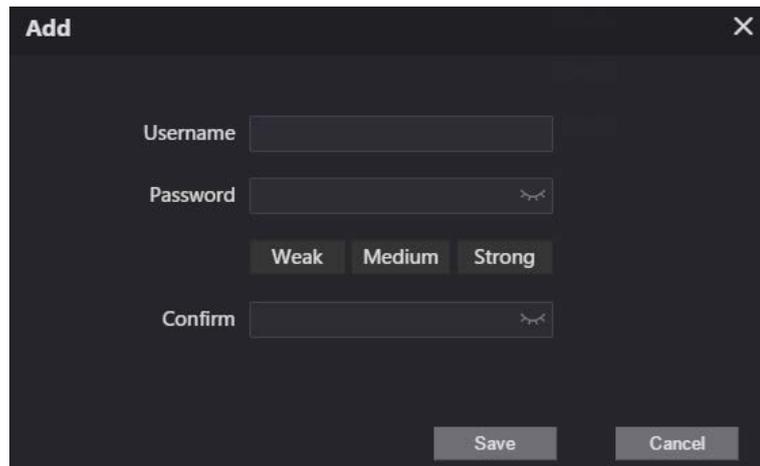
Step 1 Seleccione **Configuraciones locales > Usuario de Onvif**.

Figure 4-12 Usuario de Onvif



Step 2 Hacer clic **Agregar**.

Figure 4-13 Añadir un usuario ONVIF



The image shows a dark-themed dialog box titled "Add" with a close button (X) in the top right corner. It contains three input fields: "Username", "Password", and "Confirm". The "Password" and "Confirm" fields have a small eye icon to the right, indicating they are password fields. Below the "Password" field, there are three buttons labeled "Weak", "Medium", and "Strong", representing password strength indicators. At the bottom right of the dialog, there are two buttons: "Save" and "Cancel".

- Step 3** Ingrese la información y luego haga clic en **Salvar**.
Los dispositivos ONVIF ahora pueden monitorear el VTO usando la cuenta.

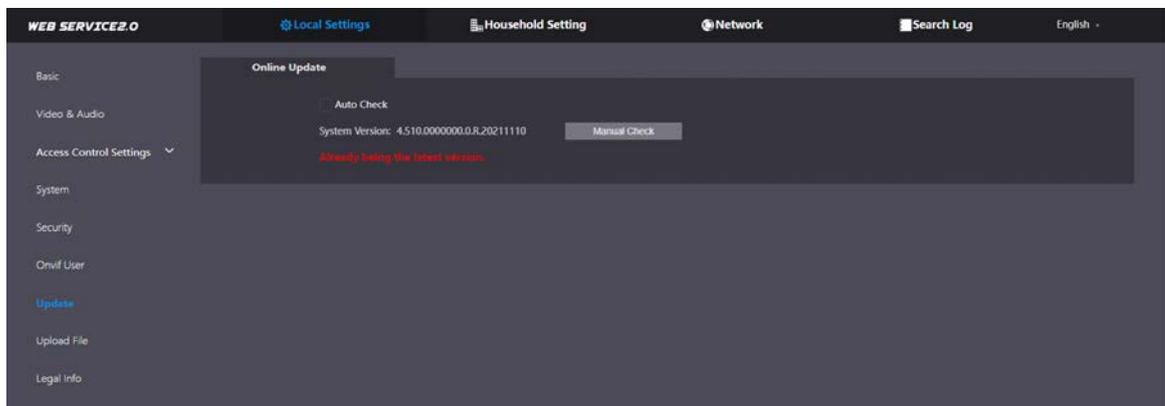
4.7 Actualizar

Step 1 Seleccione **Configuraciones locales** > **Actualizar**.

Step 2 Seleccione formas de comprobar la actualización.

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

Figure 4-14 Actualizar



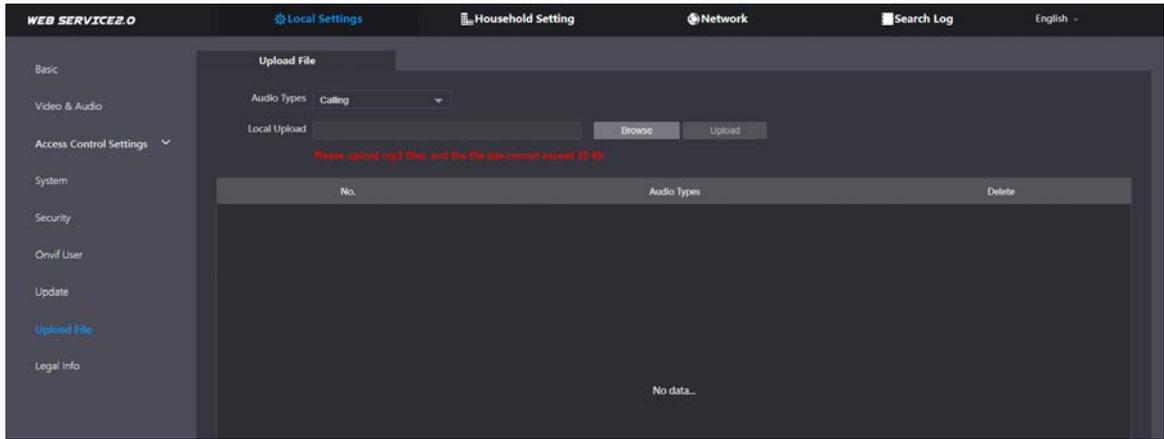
4.8 Subir archivo

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

Step 1 Seleccione **Configuraciones locales** > **Subir archivo**.

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

Figure 4-15 Cambiar el mensaje de sonido

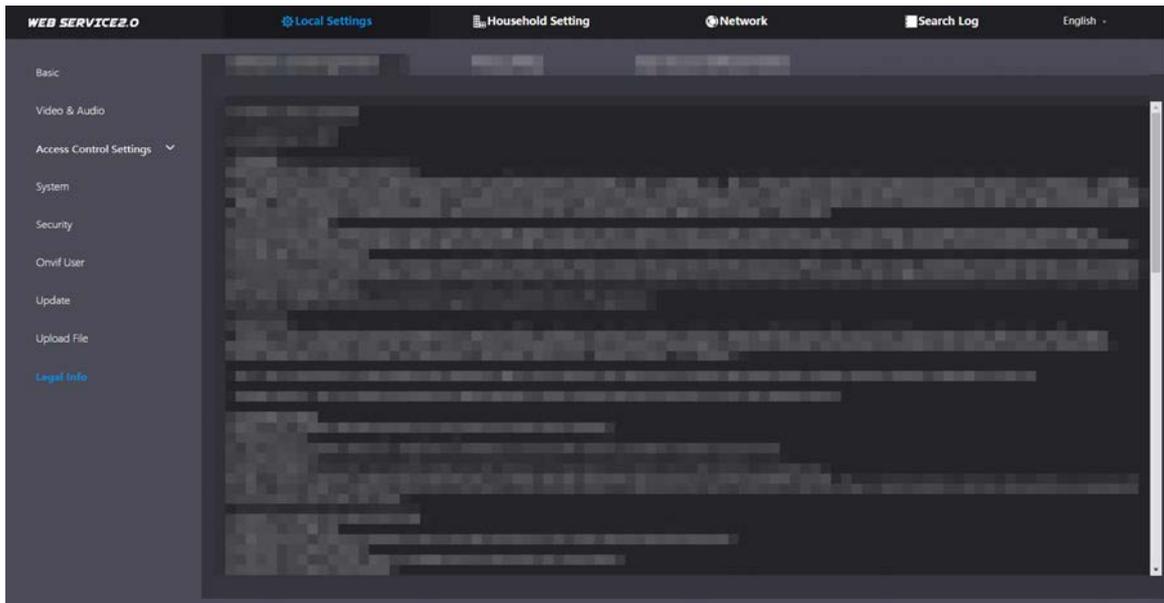


Step 3 Hacer clic **Subir**.

4.9 Información legal

Puede consultar los avisos de información legal relacionados en esta sección.

Figure 4-16 Información legal



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.

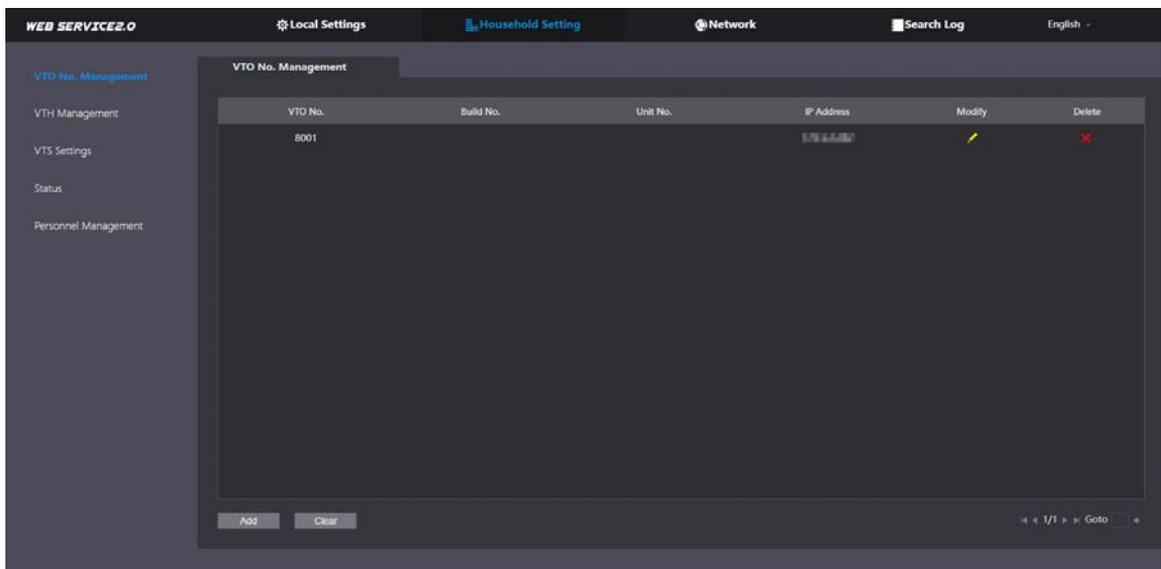
5.1 Gestión de número de VTO

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 página web del VTO que funciona como servidor SIP.

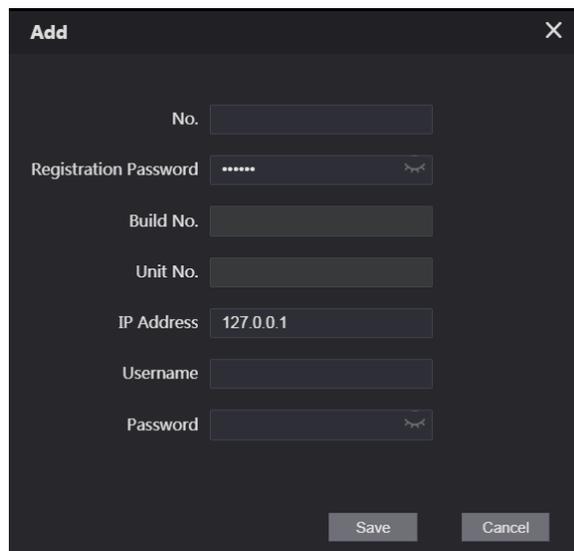
Step 2 Seleccione **Entorno doméstico** > **Gestión de número de VTO**.

Figure 5-1 gestión de VTO



Step 3 Hacer clic **Agregar**.

Figure 5-2 Agregar VTO



Step 4 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.
Registro Clave	Déjalo como predeterminado.
construir no.	Disponible solo cuando los servidores de la plataforma funcionan como servidor SIP.
Numero de unidad.	
Dirección IP	Dirección IP del VTO.
Nombre de usuario	Nombre de usuario y contraseña utilizados para iniciar sesión en la página web de la VTO.
Clave	

Step 5 Hacer clic **Salvar**.



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

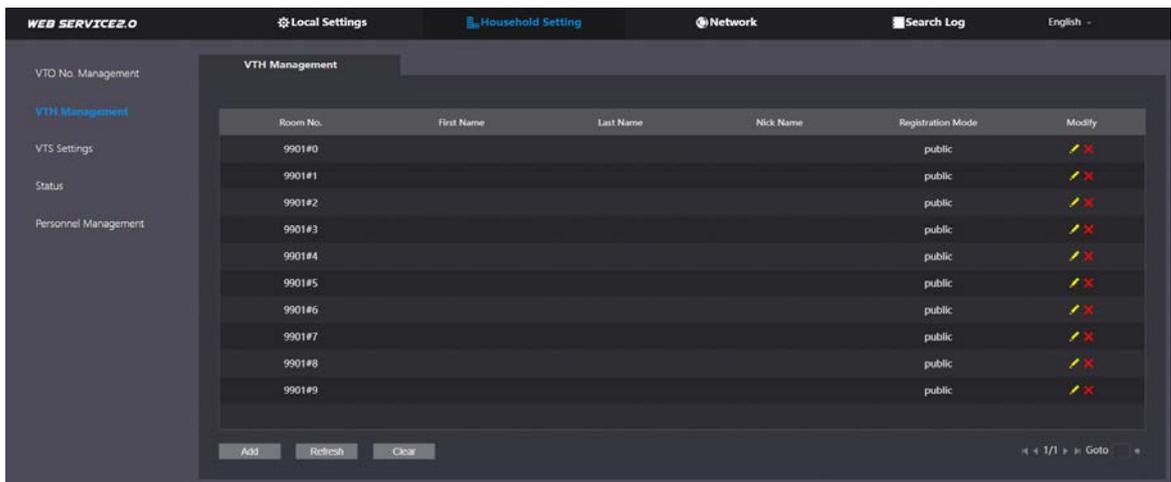
5.2 Gestión VTH

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

Step 1 Inicie sesión en la página web del servidor SIP.

Step 2 Seleccione **Entorno doméstico** > **Gestión VTH**.

Figure 5-3 Gestión del número de habitación



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

Step 3 Hacer clic **Agregar**.

Figure 5-4 Agregar un número de habitación

Step 4 Configure los parámetros.

Tabla 5-2 Información de la habitación

Parámetro	Descripción
Primer nombre	Introduce la información que necesitas para diferenciar cada habitación.
Apellido	
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	Seleccione público .
Registro Clave	Déjalo como predeterminado.

Step 5 Hacer clic **Salvar**.



Hacer clic para modificar o eliminar un número de habitación.

5.3 Gestión de personal

Adición de información de personal.

emisión de tarjetas

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

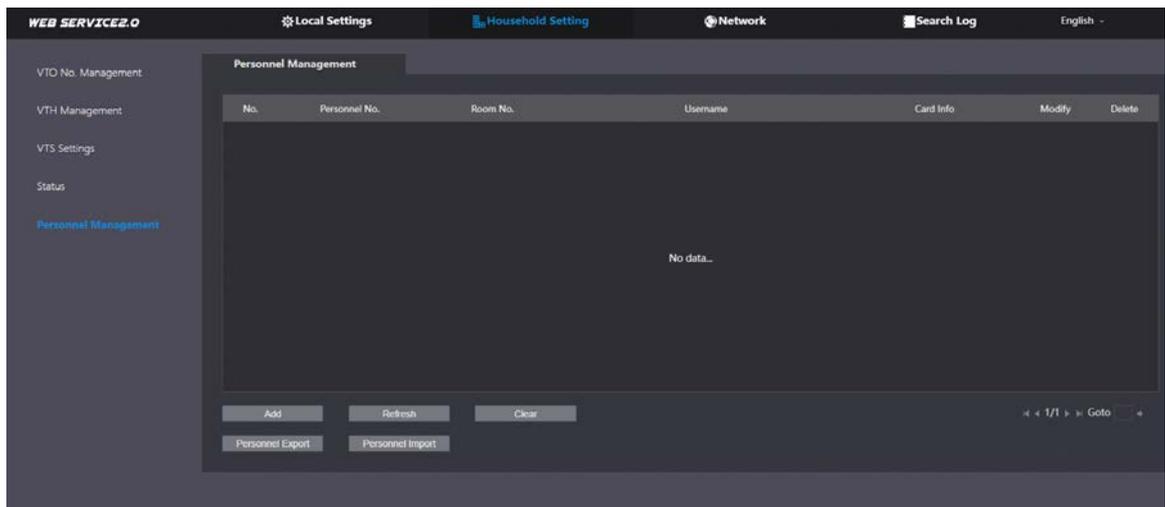


Para usar esta función, el VTO debe tener un lector de tarjetas.

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

Step 2 Seleccione **Entorno doméstico** > **Gestión de personal**.

Figure 5-5 Gestión de personal



Step 3 Hacer clic **Agregar**.

Figure 5-6 Agregar información del personal

Add

Personnel No.

Room No.

Username

Unlock Permission Lock 1 Lock 2

Save Cancel

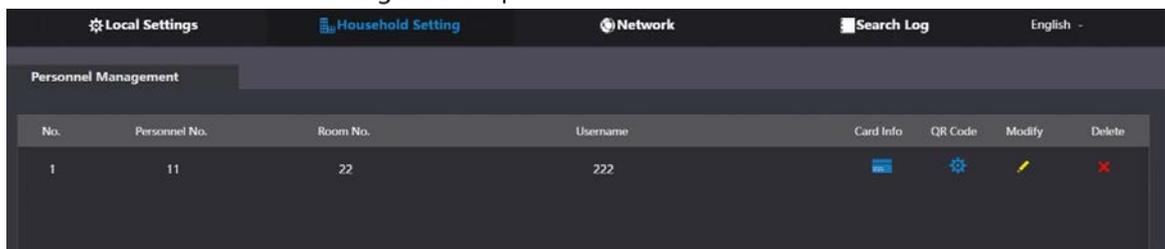
Step 4 Ingrese los parámetros y luego haga clic en **Salvar**.

- Lock1: bloqueo local.
- Bloqueo 2: bloqueo 485.



Solo los modelos que tienen 485 puertos admiten 2 tipos de bloqueos.

Figure 5-7 Operación exitosa



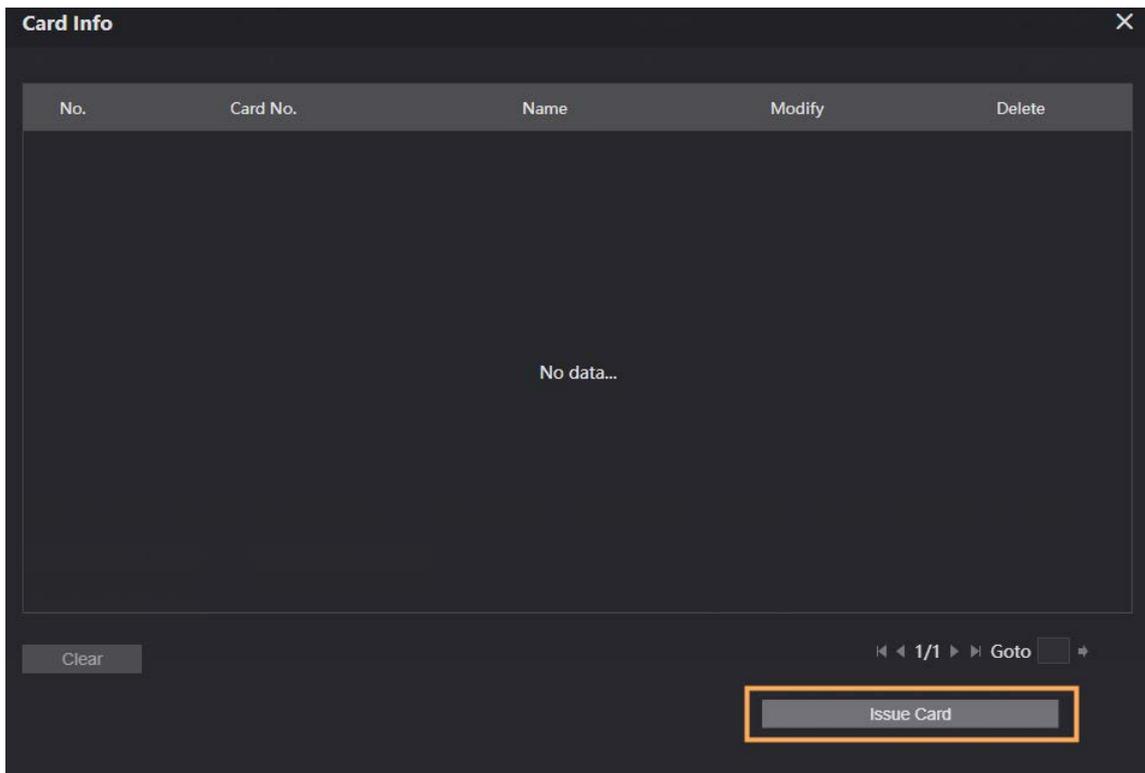
Step 5 Seleccione  para ir a la ventana de emisión de tarjetas.



Para algunos modelos VTO, el código QR está incrustado en el **Gestión de personal** página. Aún

para algunos modelos, debe ir a **La red > Básico > Servicio de almacenamiento en la nube** para comprobar el código QR.

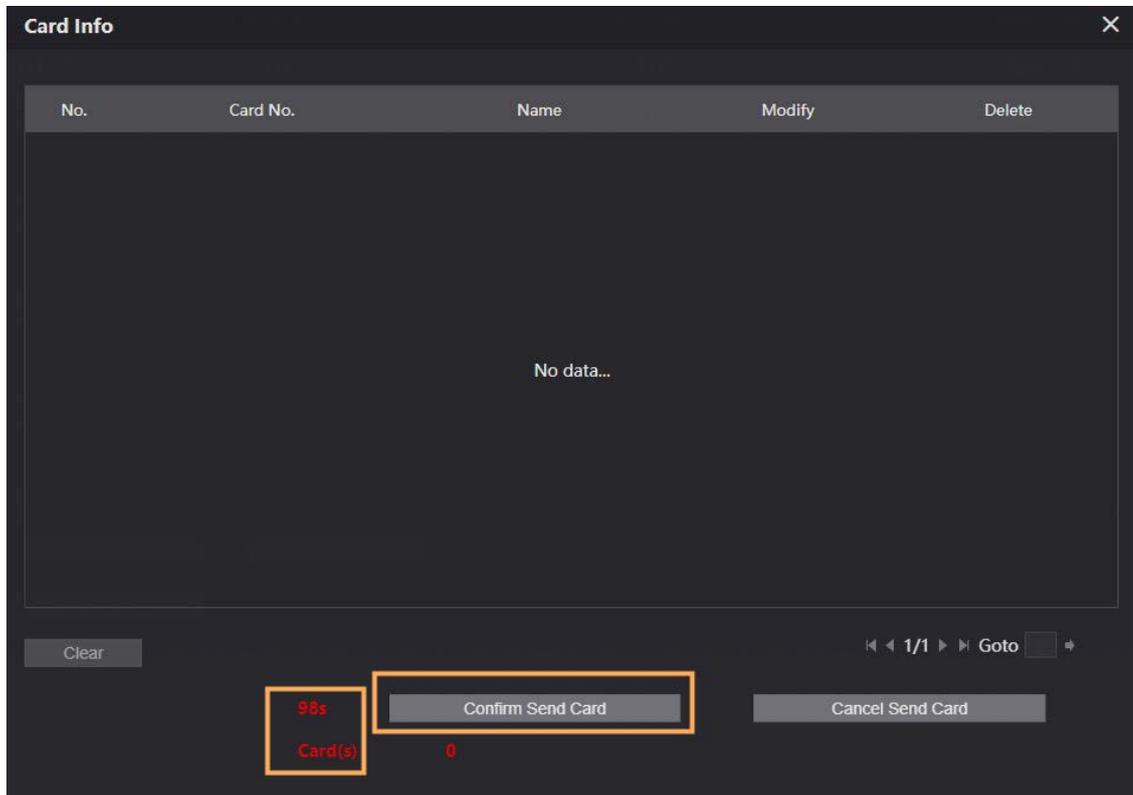
Figure 5-8 Ventana de emisión de tarjetas



Step 6 Hacer clic **Tarjeta de emisión** para emitir tarjetas.

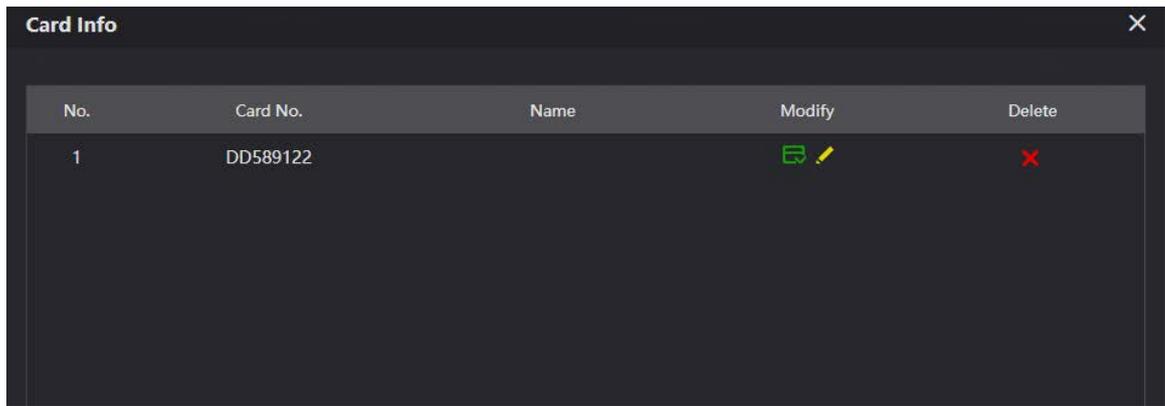
Step 7 La página web muestra el indicador de cuenta regresiva (120 s). Una vez que comienza la cuenta regresiva, debe deslizar la tarjeta en el lector de tarjetas del VTO dentro de este período de tiempo. Después de deslizar, el VTO reconocerá automáticamente el número de tarjeta.

Figure 5-9 Cuenta regresiva en proceso



Step 8 Hacer clic **Confirmar enviar tarjeta** después de deslizar para completar el proceso de emisión.

Figure 5-10 Tarjetas recién emitidas



No.	Card No.	Name	Modify	Delete
1	DD589122			

Otras operaciones

- Hacer clic  para establecerlo en pérdida, y luego el ícono cambia a . La tarjeta perdida no se puede utilizar para abrir la puerta.
- Haga clic o  para modificar el nombre de usuario o eliminar la tarjeta.

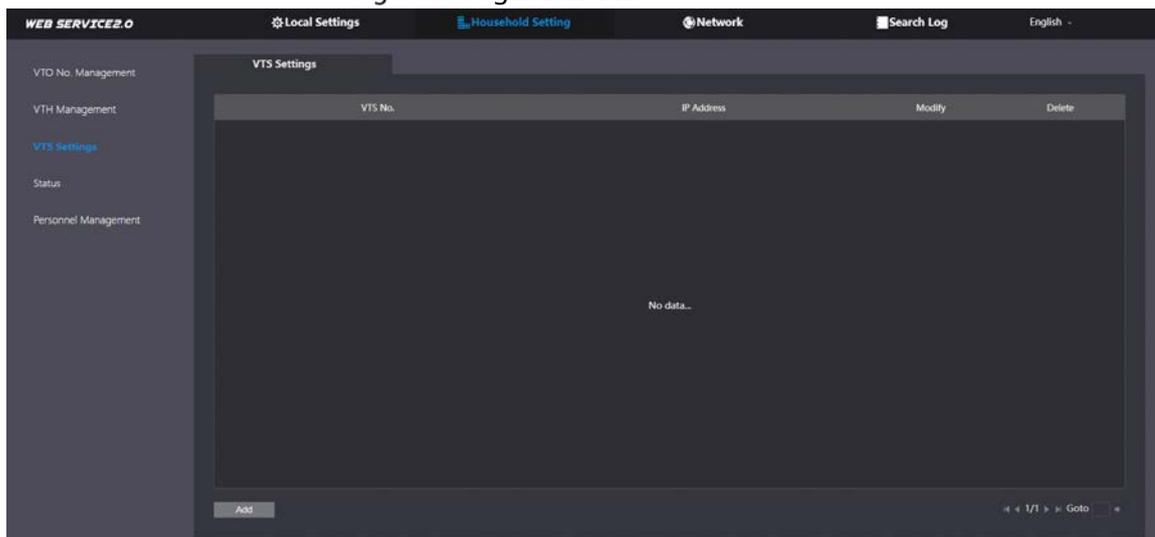
5.4 Gestión VTS

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 página web del VTO que funciona como servidor SIP.

Step 2 Seleccione **Entorno doméstico** > **Configuración VTS**.

Figure 5-11 gestión VTS



The screenshot shows the 'VTS Settings' page with a table that is currently empty. The table has columns for 'VTS No.', 'IP Address', 'Modify', and 'Delete'. The text 'No data...' is displayed in the center of the table area. There is an 'Add' button at the bottom left and a pagination control at the bottom right showing '1/1' and a 'Goto' field.

Step 3 Hacer clic **Agregar**.

Figure 5-12 Añadir VTS

Step 4 Configure los parámetros.

Tabla 5-3 Agregar configuración de VTS

Parámetro	Descripción
VTS No.	El número del VTS.
Registro Clave	Déjalo como predeterminado.
Dirección IP	Dirección IP de VTS.

Step 5 Hacer clic **Salvar**.

5.5 Estado

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

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

Figure 5-13 Estado

Room No.	Status	IP:Port	Reg Time	Off Time
0001	Online	192.168.1.100	2021-10-25 09:24:15	0

6 Red

Este capítulo presenta cómo configurar los parámetros de red.

6.1 Básico

6.1.1 TCP/IP

Debe configurar la información de TCP/IP para conectar el VTO a la red. Las descripciones a continuación son para modelos con una tarjeta LAN inalámbrica. Un dispositivo LAN inalámbrico es opcional.

LAN inalámbrico

- Step 1** Inicie sesión en la página web de la VTO.
- Step 2** Seleccione **La red > Básico**.
- Step 3** Configure los parámetros TCP/IP en el **WiFi** sección.

LAN

- Step 1** Inicie sesión en la página web de la VTO.
- Step 2** Seleccione **La red > Básico**.
- Step 3** Configure los parámetros TCP/IP en el **LAN** sección.

Figure 6-1 Configuración de la red

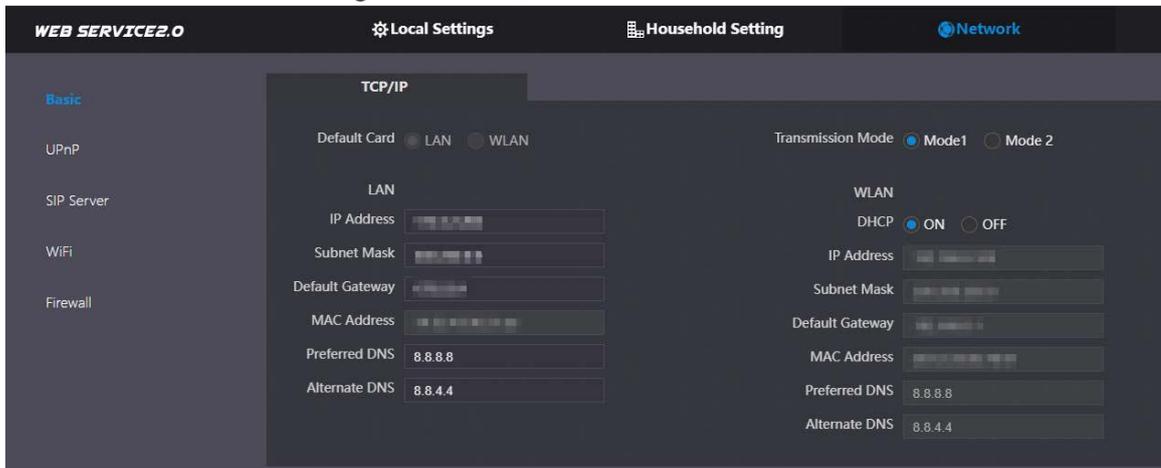


Tabla 6-1 Descripción de parámetros

Parámetro	Descripción
Dirección IP	Su dirección IP planificada para el VTO.
DNS preferido	Es 8.8.8.8 por defecto.
DNS alternativo	Es 8.8.4.4 por defecto.

Parámetro	Descripción
Transmisión Modo	<p>Elija el modo de transmisión en función de sus necesidades reales.</p> <ul style="list-style-type: none"> - Modo 1: Streaming de multidifusión (UDP). - Modo 2: Transmisión RTSP (TCP).  <p>Se prefiere el modo 2 cuando el conmutador no admite la función de multidifusión o cuando la conexión de red no es buena.</p>
DHCP	Habilite la función para obtener la dirección IP asignada para el VTO.

6.1.2 Puerto

Figure 6-2 Puerto

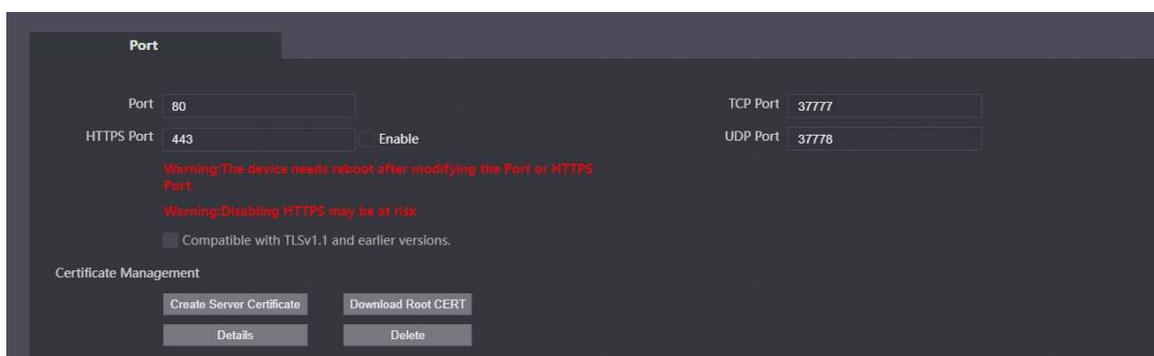


Tabla 6-2 Descripción de parámetros

Parámetro	Descripción
Puerto	80 por defecto. Si ya se usó, elija cualquier número del 1025 al 65535 según sea necesario. Puedes entrar <i>http://VTO Dirección IP: Puerto</i> para iniciar sesión en el VTO.
Puerto HTTPS	Habilítalo y haz clic Salvar . Ya puedes entrar <i>https://VTO Dirección IP: Puerto HTTPS</i> 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 Certificado	<p>La identificación digital única de VTO para el protocolo SSL. Para el uso por primera vez o después de cambiar la dirección IP del VTO, debe realizar este proceso.</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>Si elimina el certificado que se ha instalado, no se puede deshacer.</p>

Step 2 Habilite los servicios enumerados.

Step 3 Seleccione **Habilitar**.

Step 4 Hacer clic **Salvar**.

6.2.3 Adición de servicios UPnP

Step 1 Seleccione **La red > UPnP**. Hacer

Step 2 clic **Agregar**.

Step 3 Configure los parámetros según sea necesario.

Figure 6-5 Agregar un servicio UPnP

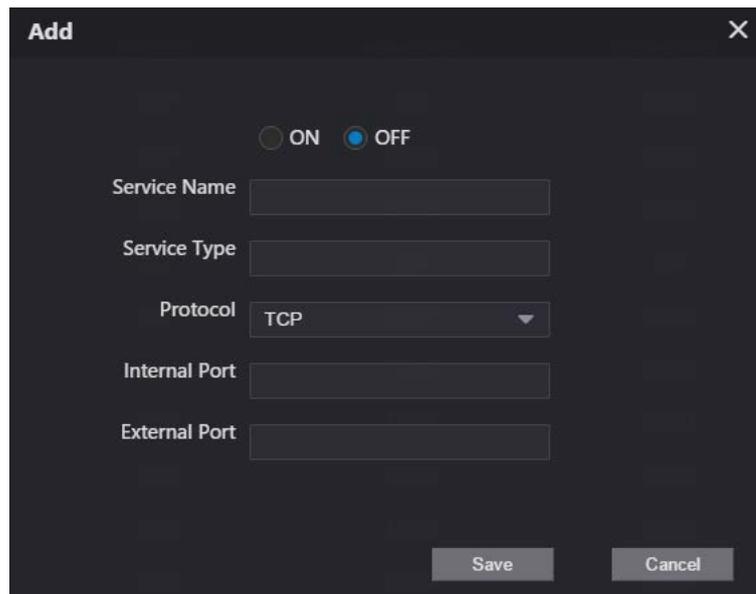


Tabla 6-3 Descripción de parámetros

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

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 Seleccione **La red > Servidor SIP**.

Step 2 Seleccione un tipo de servidor.

- El VTO que ha iniciado sesión como servidor SIP:
Habilitar **Servidor SIP** y haga clic en **Salvar**. 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 funciona como servidor SIP, no habilite **Servidor SIP**; de lo contrario, la conexión fallará.

- Si otro VTO funciona como servidor SIP:
No active **Servidor SIP**. Coloque **Tipo de servidor** para **VTO**, configure los parámetros y luego haga clic en **Salvar**.

Figure 6-6 VTO como servidor SIP

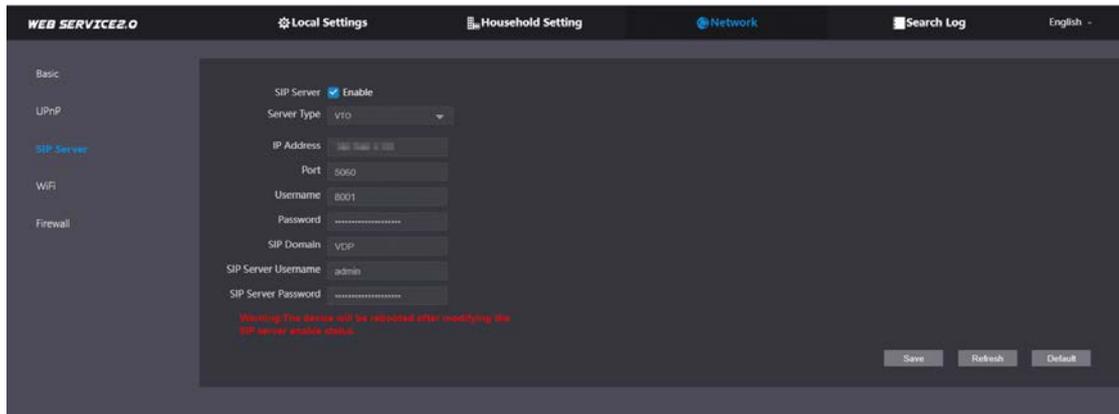


Tabla 6-4 Configuración del servidor SIP (VTO como servidor SIP)

Parámetro	Descripción
Dirección IP	Su dirección IP planificada del VTO.
Puerto	5060 por defecto cuando un VTO funciona como servidor SIP.
Nombre de usuario	Déjalo como predeterminado.
Clave	
Dominio SIP	Déjalo como predeterminado.
Nombre de usuario del servidor SIP	Nombre de usuario y contraseña utilizados para iniciar sesión en la página web del servidor SIP.
Contraseña del servidor SIP	

- Si la plataforma funciona como servidor SIP:
Coloque **Tipo de servidor** como **DSS Express/DSS Proy** configure los parámetros, y luego habilite el **Servidor SIP**.

Figure 6-7 Plataforma como servidor SIP

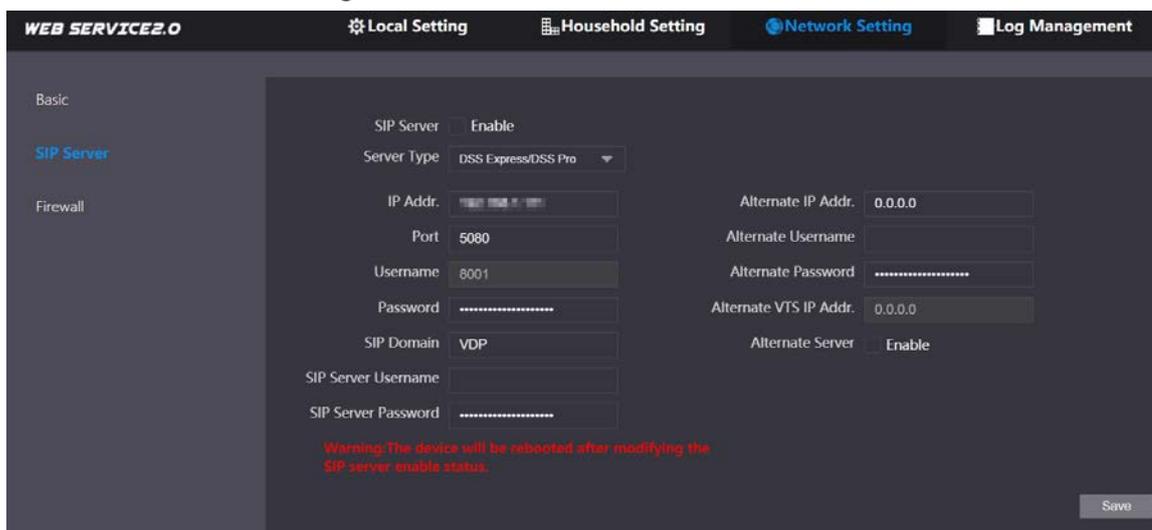


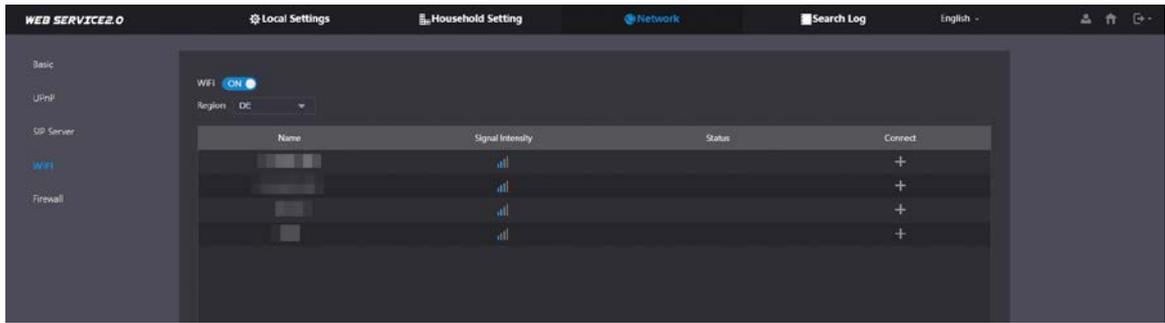
Tabla 6-5 Descripción del servidor SIP (plataforma como servidor SIP)

Parámetro	Descripción
Dirección IP	Dirección IP del servidor SIP.
Puerto	5080 por defecto cuando la plataforma funciona como servidor SIP.
Usuario Contraseña	Déjalo como predeterminado.
Dominio SIP	Déjalo como predeterminado.
Nombre de usuario del servidor SIP/ Clave	Se utiliza para iniciar sesión en el servidor SIP.
Dirección IP alternativa	<p>El servidor alternativo se utilizará como servidor SIP cuando Express/DSS deje de responder. Le recomendamos que configure la dirección IP alternativa.</p> <p></p> <ul style="list-style-type: none"> - si habilita servidor alternativo, el VTO actual en el que ha iniciado sesión sirve como servidor alternativo. - Si desea que otro VTO sirva como servidor alternativo, debe ingresar la dirección IP de ese VTO en el Dirección IP alternativa caja de texto. No active Servidor alternativo en este caso.
Nombre de usuario alternativo/ Clave	Se utiliza para iniciar sesión en el servidor alternativo.
Dirección IP VTS alternativa	Dirección IP del VTS alternativo.
Servidor alternativo	Habilítelo según sea necesario.

6.4 Wifi

Si el VTO es compatible con la función Wi-Fi, configure los parámetros aquí.

Figure 6-8 Wifi



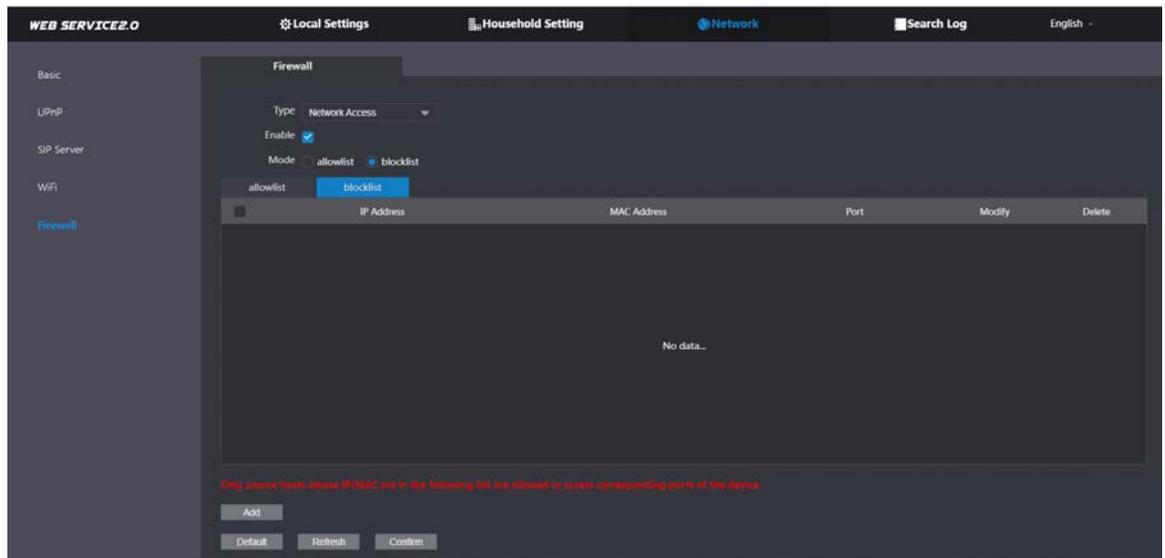
- Step 1** Seleccione **La red > Wifi**.
- Step 2** Seleccione el **Wifi** estado como **en**.
- Step 3** Seleccione una región y se mostrarán todas las redes disponibles en esta
- Step 4** región. Haga clic para conectarse a la red que eligió.

6.5 cortafuegos

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

- Step 1** Seleccione **La red > cortafuegos**.

Figure 6-9 cortafuegos



- Step 2** Seleccione **Escribey**, a continuación,
- Step 3** actívelo. Configure los parámetros. Hacer
- Step 4** clic **Confirmar**.

Tabla 6-6 Descripción del tipo de cortafuegos

Escribe	Descripción
Acceso a la red	Seleccione cualquiera Lista de permitidos o Lista de bloqueos , y, 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.
Modo	Lista de permitidos: Dispositivos a los que se les ha otorgado un acceso. Blocklist: Dispositivos a los que se les ha prohibido el acceso.

7 Gestión de registros

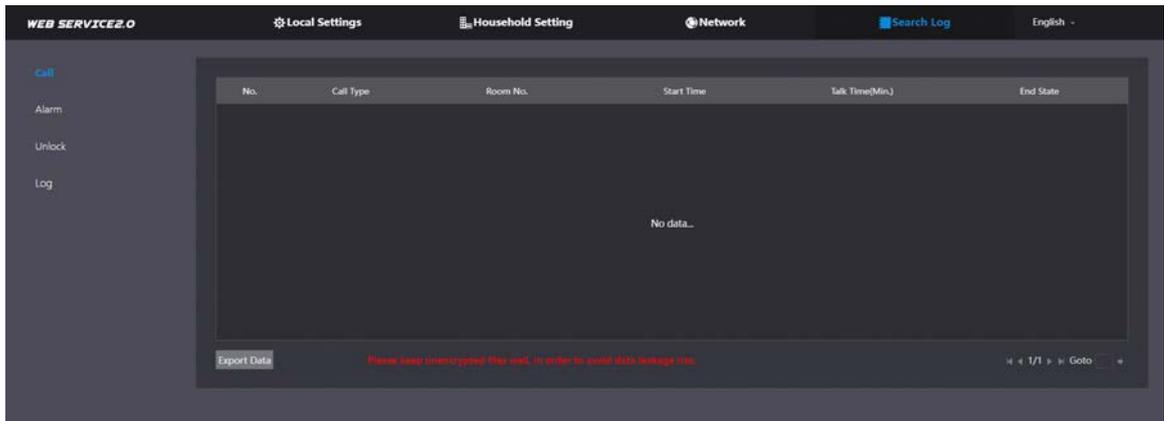
Seleccione **Registro de búsqueda**. Puede buscar diferentes registros y exportarlos a su PC según sea necesario.



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

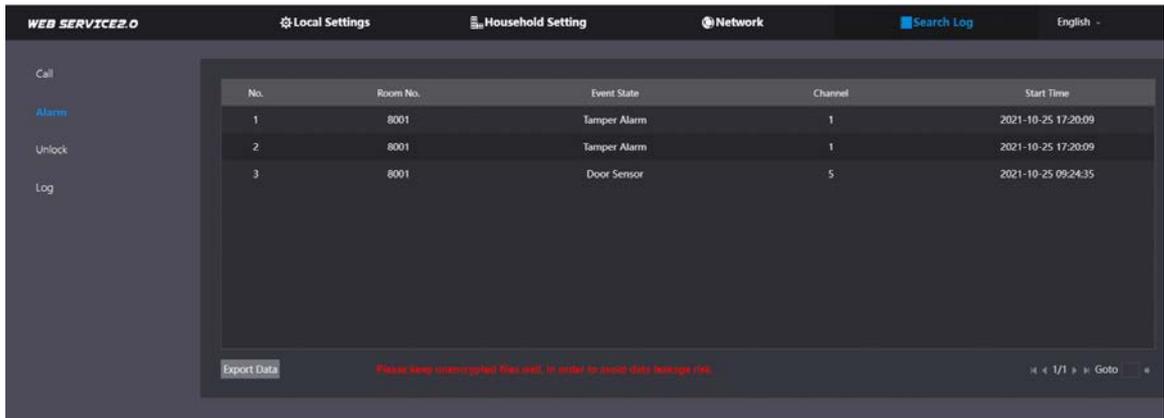
7.1 Llamada

Figure 7-1 Llamada



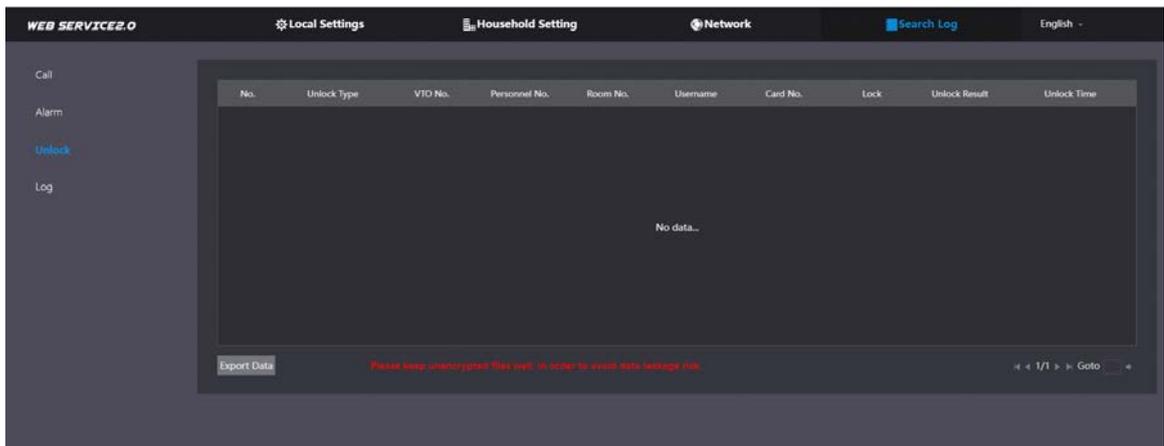
7.2 Alarma

Figure 7-2 Alarma



7.3 desbloquear

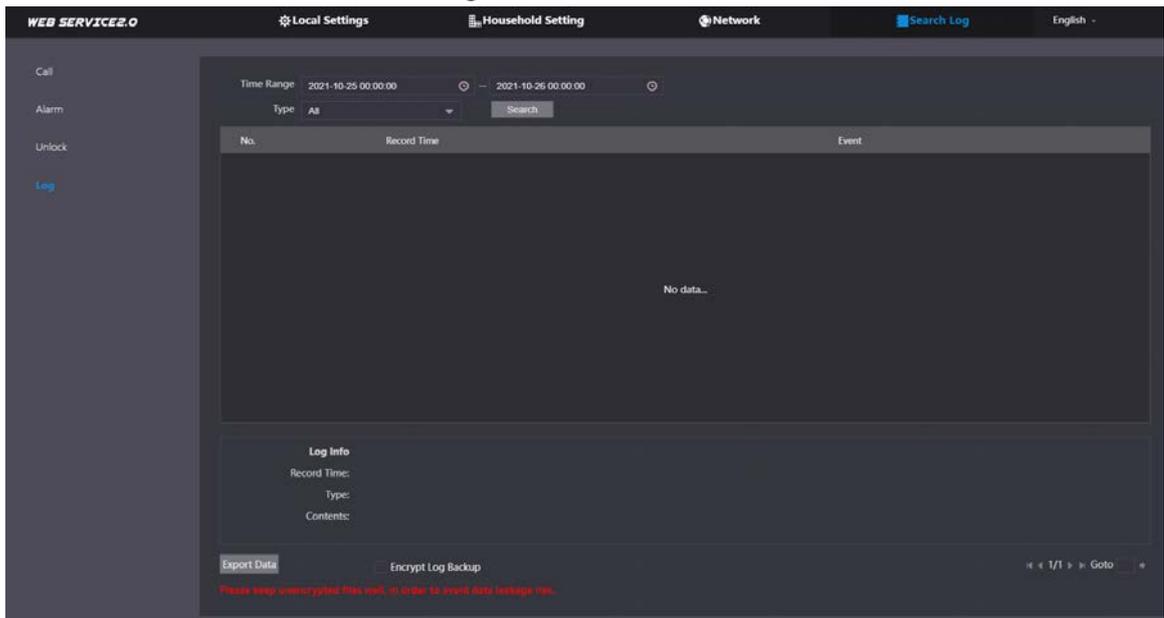
Figure 7-3 desbloquear



7.4 Tronco

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

Figure 7-4 Tronco



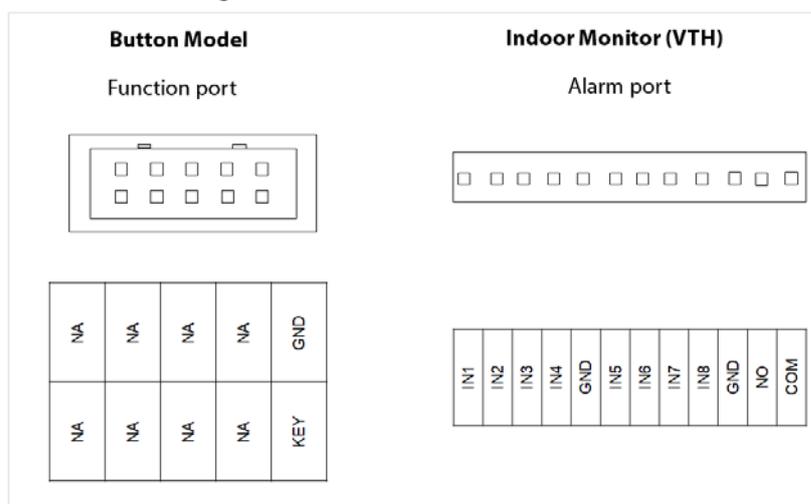
Configuración del modelo de 8 botones

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

8.1 Conexión de cable

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

Figure 8-1 Conexión de cable



8.2 Configuración VTH

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

Step 1 Encienda el VTH.

Step 2 Grifo **Ajuste** > **Alarma** > **Zona Cableada** en el VTH.

Figure 8-2 Configuración de zona cableada



Step 3 Selecciona el **Escrib** como **Timbre de la puerta**, y configurar el resto de parámetros. **Grifo**

Step 4 Aceptar para completar la configuración.

Tabla 8-1 Descripción de parámetros

Parámetro	Descripción
Área	El número no se puede modificar.
NO C	Seleccione NO (normalmente abierto) o NC (normalmente cerrado) según el tipo de detector. Debe ser el mismo que el tipo de detector.
Escribe	Seleccione el tipo correspondiente según el tipo de detector, incluidos IR, gas, humo, botón de urgencia, puerta, alarma antirrobo, perímetro y timbre.
Estado	<ul style="list-style-type: none"> ● Alarma instantánea: Después de armado, si se activa una alarma, el dispositivo emite una sirena de inmediato y entra en estado de alarma. ● Alarma de retraso: Después de armado, si se activa una alarma, el dispositivo entra en estado de alarma después de un tiempo específico, durante el cual puede desarmar y cancelar la alarma. ● Derivación: La alarma no se disparará en el área. Después de desarmar, esta área se restaurará al estado de funcionamiento normal. ● Eliminar: El área no es válida durante el armado/desarmado. ● 24 horas: La alarma se activará todo el tiempo en el área independientemente de si se arma o desarma. <p> una zona en Eliminar El estado no se puede omitir.</p>
Introducir retraso	<p>Después de ingresar el retraso, cuando el área armada activa una alarma, ingresar al área armada desde un área no armada dentro del período de tiempo de retraso no generará una alarma de vinculación. La alarma de vinculación se producirá si el tiempo de retardo llega a su fin y no se desarma.</p> <p> El retraso solo es válido para</p>
Retardo de salida	<p>Después del brazo, Alarma de retraso área entrará en estado de armado al final de Retardo de salida.</p> <p> Si varias áreas establecen el retraso de salida, el aviso en pantalla se ajustará al tiempo de retraso máximo.</p> <p>Alarma.</p>

Appendix 1 Recomendaciones de ciberseguridad

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

dispositivo: 1. Use contraseñas seguras

Consulte las siguientes sugerencias para establecer contraseñas:

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

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

- De acuerdo con el procedimiento estándar en la industria tecnológica, recomendamos mantener actualizado el firmware de su dispositivo (como NVR, DVR, cámara IP, etc.) para garantizar que el sistema esté equipado con los últimos parches y correcciones de seguridad. Cuando el dispositivo está conectado a la red pública, 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 una sala y gabinete de computadoras especiales, e implemente un permiso de control de acceso y una administración de claves bien hechos para evitar que el personal no autorizado realice contactos físicos, como dañar el hardware, la conexión no autorizada de un dispositivo extraíble (como un disco flash USB), puerto serie), etc.

2. Cambie las contraseñas regularmente

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

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

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

4. Habilitar bloqueo de cuenta

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

5. Cambiar HTTP predeterminado y otros puertos de servicio

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

6. Habilitar HTTPS

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

7. Enlace de dirección MAC

Le recomendamos vincular la dirección IP y MAC de la puerta de enlace al dispositivo, reduciendo así

el riesgo de suplantación de 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 cibernéticos, recomendamos:

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