

Villa VTO

Manual de usuario






Prefacio

General

Este manual presenta el funcionamiento de la interfaz web.

Las instrucciones de seguridad

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

Palabras de advertencia	Sentido
 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 la revisión	Fecha de lanzamiento
V1.0.0	Primer lanzamiento	Enero 2020

Acerca del manual

- El manual es solo para referencia. Si hay inconsistencia entre el Manual y el producto real, prevalecerá el producto real.
- No nos hacemos responsables de ninguna pérdida ocasionada por las operaciones que no cumplan con el Manual. El Manual se actualizaría de acuerdo con las últimas leyes y reglamentos de las regiones 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 actualizado y la documentación complementaria. Todavía puede haber desviaciones en los datos técnicos, la descripción de funciones y operaciones, o errores en la impresión. Si tiene alguna duda o disputa, consulte nuestra explicación final. Actualice el software del lector o pruebe con otro software de lectura convencional si no puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas comerciales registradas y los nombres de empresas que aparecen en el manual son propiedad de sus respectivos propietarios.
- Visite nuestro sitio web, comuníquese con el proveedor o con el servicio de atención al cliente si se produce algún problema al utilizar el dispositivo.
- Si hay alguna duda o controversia, consulte nuestra explicación final.

Advertencias y medidas de seguridad importantes

La siguiente descripción es el método de aplicación correcto del dispositivo. Lea atentamente el manual antes de usarlo para evitar peligros y pérdidas materiales. Cumpla estrictamente con el manual durante la aplicación y consérvelo correctamente después de leerlo.

Requisito de funcionamiento

- No coloque ni instale el dispositivo en un área expuesta a la luz solar directa o cerca de un dispositivo generador de calor.
- No instale el dispositivo en un área húmeda, polvorienta o fuliginosa.
- Mantenga su instalación horizontal, o instálelo en lugares estables, y evite que se caiga.
- No gotee ni salpique líquidos sobre el dispositivo; No coloque sobre el dispositivo nada que contenga líquidos, para evitar que los líquidos fluyan hacia el dispositivo.
- Instale el dispositivo en lugares bien ventilados; no bloquee su abertura de ventilación. Utilice el dispositivo solo dentro del rango nominal de entrada y salida.
- No desmonte el dispositivo de forma arbitraria.
- Transporte, use y almacene el dispositivo dentro del rango permitido de humedad y temperatura.

Requisitos de energía

- El producto utilizará cables eléctricos (cables de alimentación) recomendados por esta área, que se utilizarán dentro de su especificación nominal.
- Utilice una fuente de alimentación que cumpla con los requisitos de SELV (voltaje extra bajo de seguridad) y suministre energía con un voltaje nominal que cumpla con la Fuente de energía limitada en IEC60950-1. Para conocer los requisitos específicos de la fuente de alimentación, consulte las etiquetas 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

Prólogo	YO Advertencias y salvaguardias importantes	Il 1 Inicialización
.....	1
2 Interfaz de inicio de sesión		2
2.1 Iniciar sesión		2
2.2 Restablecimiento de la contraseña		2
3 Interfaz principal		4
4 Configuración local		5
4.1 Básico		5
4.2 Video y audio		6
4.3 Control de acceso		8
4.4 Sistema		9
4.5 Seguridad		10
5 Entorno del hogar		11
5.1 Gestión de No. de VTO		11
5.1.1 Agregar VTO		11
5.1.2 Modificación de la información de VTO		12
5.1.3 Eliminación de VTO		13
5.2 Gestión de número de habitación		13
5.2.1 Agregar número de habitación		13
5.2.2 Modificación del número de habitación		15
5.2.3 Emisión de tarjeta de acceso		15
5.3 Gestión de VTS		dieciséis
5.4 Configuración de IPC		17
5.5 Estado		19
5.6 Publicar información		19
5.6.1 Enviar información		19
5.6.2 Información del historial		20
6 Configuración de red		21
6.1 Básico		21
6.1.1 TCP / IP		21
6.1.2 HTTPS		21
6.2 Servidor SIP		21
6.3 Permisos de IP		22
7 Gestión de registros		24
7.1 Llamar		24
7.2 Desbloquear		24
Apéndice 1 Recomendaciones de ciberseguridad		25

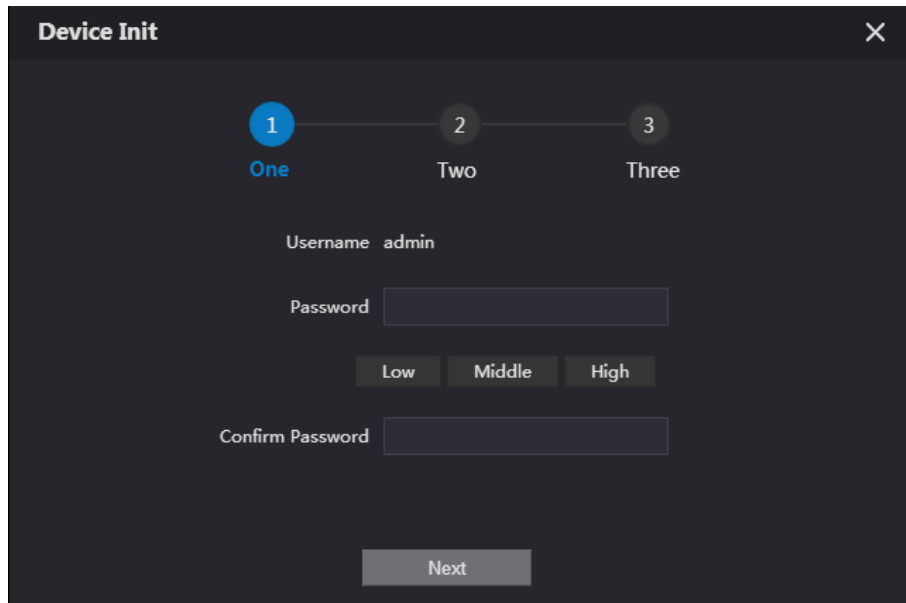
1 Inicialización

Para iniciar sesión por primera vez o después de restablecer el VTO, debe inicializar la interfaz web. La dirección IP predeterminada del VTO es 192.168.1.110 y asegúrese de que la PC esté en el mismo segmento de red que el VTO.

Paso 1 Conecte el VTO a la fuente de alimentación y luego inícielo.

Paso 2 Abra el navegador de Internet en la PC, luego ingrese la dirección IP predeterminada del VTO en la barra de direcciones y luego presione **Entrar**.

Figura 1-1 Inicialización del dispositivo



Paso 3 Ingrese y confirme la contraseña, y luego haga clic en **Próximo**.

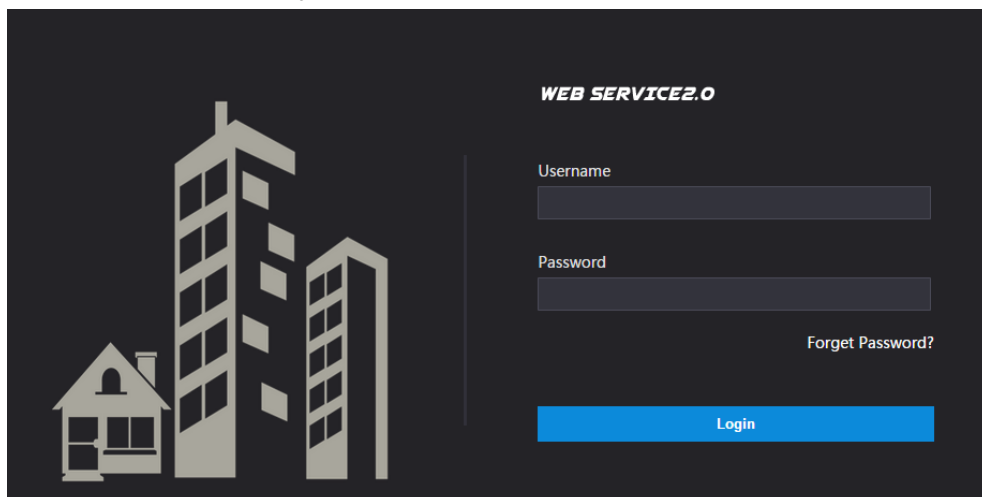
Se muestra la interfaz de configuración de correo electrónico.

Paso 4 Seleccione el **Email** casilla de verificación y luego ingrese su dirección de correo electrónico. Esta dirección de correo electrónico se puede utilizar para restablecer la contraseña.

Paso 5 Haga clic en **Próximo**. La inicialización tuvo éxito.

Paso 6 Haga clic en **OKAY**.

Figura 1-2 Interfaz de inicio de sesión



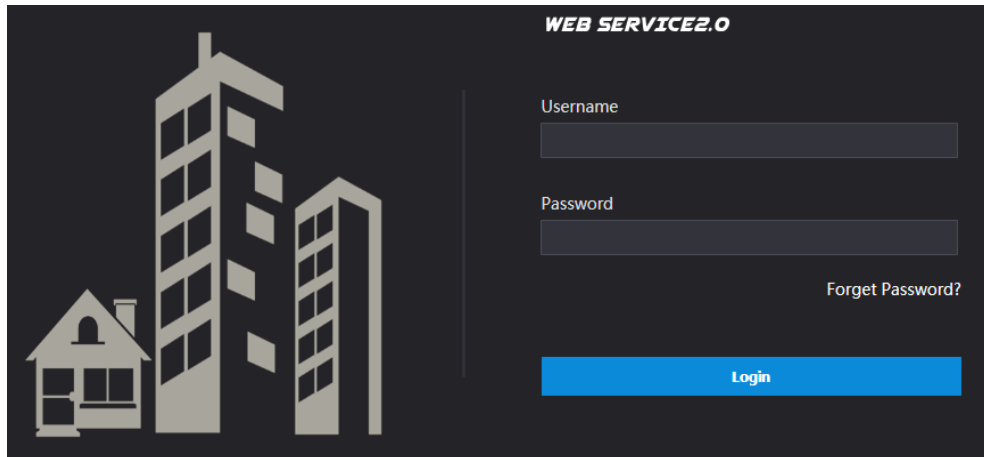
2 Interfaz de inicio de sesión

2.1 Iniciar sesión

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

Paso 1 Abra el navegador de Internet en la PC, luego ingrese la dirección IP de VTO en la barra de direcciones, y luego presione **Entrar**.

Figura 2-1 Interfaz de inicio de sesión

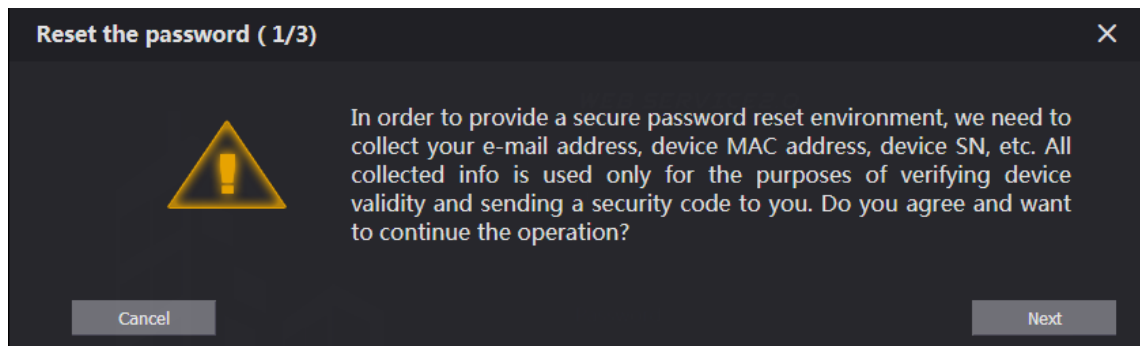


Paso 2 Ingrese "admin" como nombre de usuario, luego la contraseña que estableció durante la inicialización, y luego hacer clic **Iniciar sesión**.

2.2 Restablecimiento de la contraseña

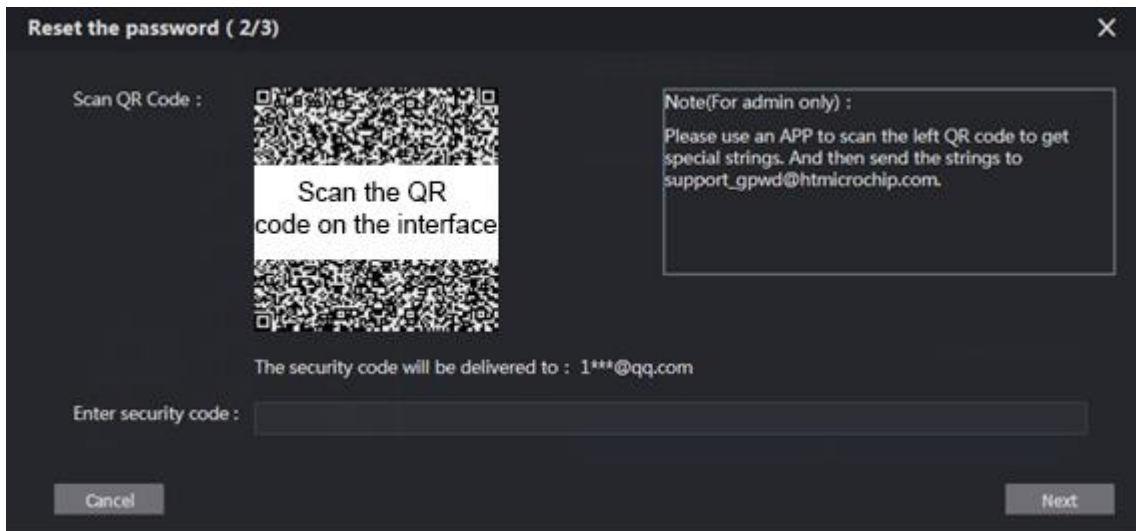
Paso 1 En la interfaz de inicio de sesión (Figura 2-1), haga clic en **¿Se te olvidó tu contraseña?**.

Figura 2-2 Restablecer la contraseña (1/3)



Paso 2 Haga clic en **Próximo**.

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



Paso 3 Escanee el código QR en la interfaz web para obtener el código de seguridad en su buzón y

luego ingrese el código de seguridad en el cuadro de entrada.



- Si no configuró el correo electrónico durante la inicialización, comuníquese con el proveedor o con el servicio de atención al cliente para obtener ayuda.
- Para obtener el código de seguridad nuevamente, actualice la interfaz del código QR.
- Utilice el código de seguridad dentro de las 24 horas posteriores a su recepción. De lo contrario, dejará de ser válido.
- Si se ingresa un código de seguridad incorrecto 5 veces seguidas, esta cuenta se bloqueará durante 5 minutos.

Paso 4 Haga clic en **Próximo**, y luego el **Restablecer la contraseña (3/3)** Se muestra el cuadro de diálogo.

Paso 5 Configure y confirme la nueva contraseña como se le indica y luego haga clic en **OKAY**.

3 Interfaz principal

Inicie sesión en la interfaz web del VTO y luego se muestra la interfaz principal.

Figura 3-1 Interfaz principal

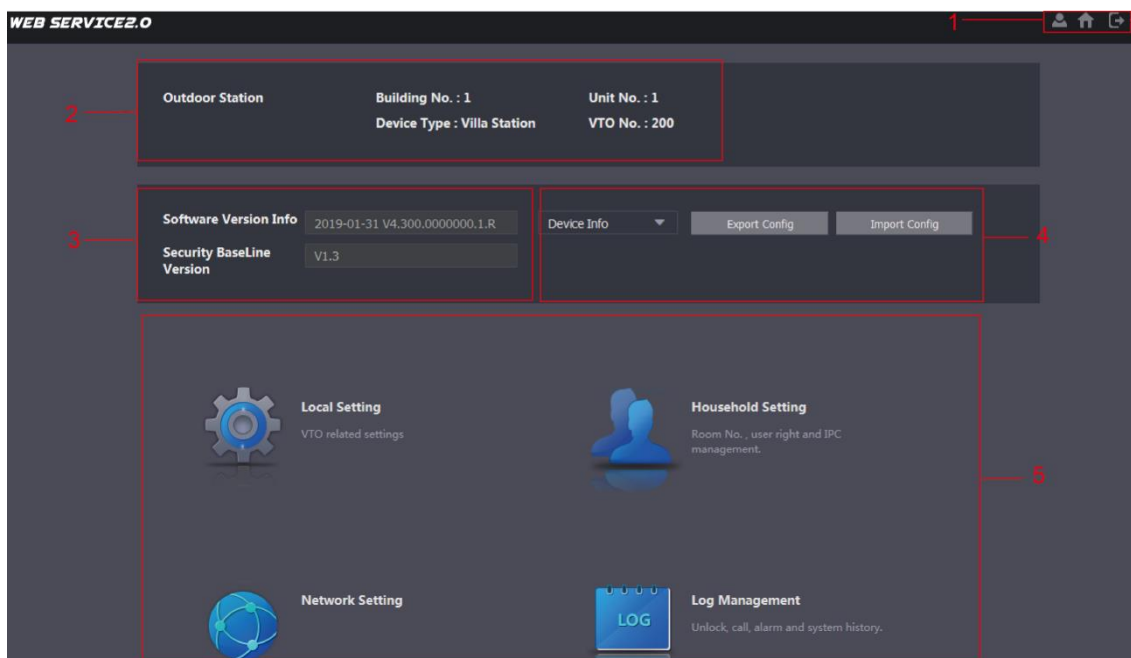





Tabla 3-1 Introducción a la interfaz principal

No.	Función	Descripción
1	Función general	<ul style="list-style-type: none"> Hacer clic  para cambiar la contraseña y su correo electrónico habla a. Hacer clic  para ir a la interfaz principal. Hacer clic  para cerrar sesión, reiniciar el VTO o restaurar el VTO a la configuración de fábrica.
2	Información VTO	Puede ver la información general del VTO, incluido el número de edificio, el número de unidad, el tipo de dispositivo y el número de VTO.
3	Sistema información	Puede ver la versión de software, la versión de MCU y la versión de referencia de seguridad.
4	Administrador de configuración	Seleccione Información del dispositivo o Información de usuario , y luego puede exportar la configuración de VTO o la información del usuario a la PC o importarlos desde ella.
5	Área funcional	Haga clic en los botones para ir al menú correspondiente.

4 Configuración local

Este capítulo presenta cómo configurar el tipo de VTO, el número de VTO, el video y audio, la contraseña de acceso, la hora del sistema y la función de seguridad.

Operaciones generales:

- Después de cada configuración, haga clic en **Confirmar** para guardar y haga clic en **Actualizar** para ver el último cambio.
- Si hace clic en **Defecto**, todas las configuraciones en la página actual se restaurarán a los valores predeterminados, y debe hacer clic en **Confirmar** ahorrar.

4.1 Básico


Esta sección presenta la configuración del tipo de dispositivo VTO, el número VTO y el almacenamiento automático.


Paso 1 En la interfaz principal (Figura 3-1), seleccione **Configuración local**> **Básico**.

Figura 4-1 Básico

Paso 2 Configure los parámetros.

Tabla 4-1 Descripción de los parámetros básicos

Parámetro	Descripción
Tipo de dispositivo	<p>Puede seleccionar Villa Station o Second Confirmation.</p>  <ul style="list-style-type: none"> • El número de edificio y el número de unidad están disponibles solo cuando otros servidores funcionan como servidor SIP. Consulte "6.2 Servidor SIP". • La estación de valla se utiliza normalmente cuando otros servidores funcionan como servidor SIP.
Número de llamada del centro	Configure el número del centro de gestión y podrá llamar al centro de gestión en cada VTO o VTH de la red. El número predeterminado es 888888.
Centro de llamadas Hora	Período de tiempo en el que puede llamar al centro de gestión.
VTO No.	El número VTO se puede utilizar para diferenciar cada VTO, y normalmente es

Parámetro	Descripción
	Configurado según unidad o número de edificio. Puede agregar dispositivos VTO al servidor SIP con sus números.
Punto de almacenamiento	<p>Todas las instantáneas se guardarían en la tarjeta SD automáticamente.</p> <ul style="list-style-type: none"> Instantánea automática (desbloqueo) <p>Seleccione EN para habilitar esta función, y luego el sistema toma una instantánea cada vez que se abre la puerta.</p> <ul style="list-style-type: none"> Instantánea automática (hablando) <p>Seleccione EN para habilitar esta función, y luego el sistema toma una instantánea cada vez que el usuario de VTH responde a una llamada del VTO.</p> <ul style="list-style-type: none"> Dejar carga de mensaje <p>Seleccione EN para habilitar esta función, y luego el sistema carga los mensajes de los visitantes a la tarjeta SD automáticamente.</p>  <ul style="list-style-type: none"> Si hay una tarjeta SD en el VTH principal, los mensajes de la izquierda se guardarán en la tarjeta SD del VTH principal por defecto. Para recibir el mensaje, el Tiempo de mensaje VTO debe configurarse para ser mayor que 0. Consulte el manual del usuario de VTH.

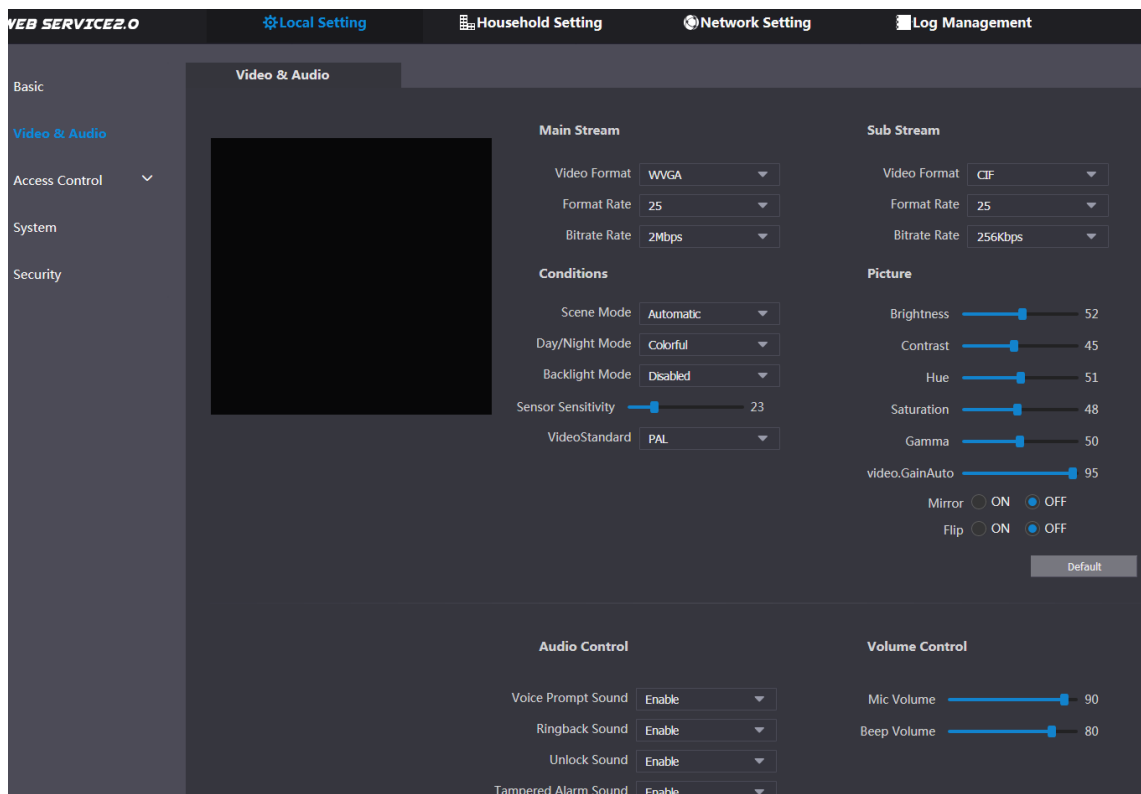
Paso 3 Haga clic en **Confirmar**.

4.2 Video y audio

Esta sección presenta cómo configurar el formato y la calidad del video que graba el VTO y los ajustes de control de audio.

Paso 1 En la interfaz principal (Figura 3-1), seleccione **Configuración local** > **Video y audio**.

Figura 4-2 Video y audio



Paso 2 Configure los parámetros y estas configuraciones entrarán en vigor inmediatamente.

Tabla 4-2 Descripción de los parámetros de vídeo

Parámetro		Descripción
Principal Corriente	Formato de vídeo	Seleccione la resolución de vídeo de 720P, WVGA, y D1 .
	Tasa de formato	Configure el número de fotogramas en 1 segundo. Puede seleccionar entre 1 a 25 debajo CAMARADA , y 1 a 30 debajo NTSC estándar de vídeo. Cuanto mayor sea el valor, más suave será el vídeo.
	Tasa de bitrate	Configure la cantidad de datos que se transmitieron en 1 segundo. Puede seleccionar según sea necesario. Cuanto mayor sea el valor, mejor será la calidad del vídeo.
Sub Corriente	Formato de vídeo	Seleccione la resolución de vídeo de CIF, WVGA, QVGA, y D1 .
	Tasa de formato	Configure el número de fotogramas en 1 segundo. Puede seleccionar entre 1 a 25 debajo CAMARADA , y 1 a 30 debajo NTSC estándar de vídeo. Cuanto mayor sea el valor, más suave será el vídeo.
	Tasa de bitrate	Configure la cantidad de datos que se transmitieron en 1 segundo. Puede seleccionar según sea necesario. Cuanto mayor sea el valor, mejor será la calidad del vídeo.
Condiciones	Modo escena	Ajusta el vídeo para adaptarlo a diferentes escenarios. Puede seleccionar entre Automático, soleado, nocturno y Discapitado . Es Automático por defecto.
	Día / noche Modo	Puede seleccionar entre Automático, Colorido o Blanco negro modo.
	Iluminar desde el fondo Modo	Puede seleccionar entre los siguientes modos: <ul style="list-style-type: none"> • Discapitado: sin luz de fondo. • Iluminar desde el fondo: la cámara obtiene una imagen más clara de las áreas oscuras del objetivo cuando dispara a contraluz. • Amplia dinámica: el sistema atenúa las áreas brillantes y compensa las áreas oscuras para asegurar la claridad de toda el área. • Inhibición: el sistema restringe las áreas brillantes y reduce el tamaño del halo para atenuar el brillo general. Ajuste el valor y cuanto mayor sea el valor,
	Sensor Sensibilidad	más fácil será la activación del sensor.
	Estándar de vídeo	Seleccione de CAMARADA o NTSC según su dispositivo de visualización. Cambia el
Imagen	Brillo	valor para ajustar el brillo de la imagen. Cuanto mayor sea el valor, más brillante será la imagen y cuanto más pequeña, más oscura. La imagen puede aparecer borrosa si el valor está configurado demasiado grande.
	Contraste	Cambia el contraste de la imagen. Cuanto mayor sea el valor, mayor será el contraste entre las áreas brillantes y oscuras, y cuanto menor sea el menor. Si el valor es demasiado grande, el área oscura será demasiado oscura y el área brillante más fácil de sobreexponer. La imagen puede aparecer borrosa si el valor es demasiado pequeño.

Parámetro		Descripción
	Matiz	Hace que el color sea más profundo o más claro. El valor predeterminado lo establece el sensor de luz y se recomienda.
	Saturación	Hace que el color sea más profundo o más claro. Cuanto mayor sea el valor, más profundo será el color y cuanto más bajo, más claro. El valor de saturación no cambia el brillo de la imagen.
	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 y cuanto más pequeña, más oscura. Amplifique la señal de video para aumentar el brillo de la imagen. Si el valor es demasiado grande, habrá más ruido en la imagen. Seleccione En , y luego la imagen se muestra con los lados izquierdo y derecho invertidos.
	Video.GainAuto	
	Espejo	
	Dar la vuelta	Seleccione En , y luego la imagen se muestra al revés.
Audio Controlar	Seleccione Habilitar o Discapacitado para activar o desactivar cada sonido.	
Volumen Controlar	Volumen del micrófono	Ajuste el valor, y cuanto mayor sea el valor, más alto será el micrófono en el VTO.
	Volumen del pitido	Ajuste el valor y cuanto mayor sea el valor, más fuerte será el sonido del sistema.

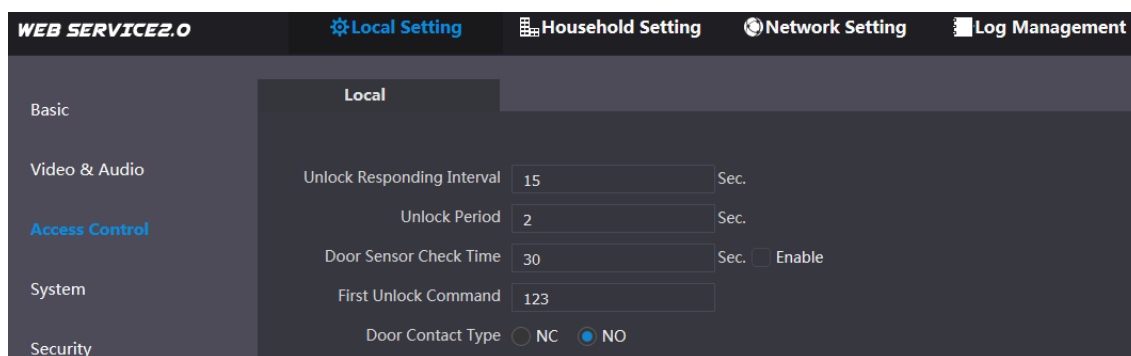
4.3 Control de acceso

Esta sección presenta cómo configurar la cerradura, incluido el intervalo de respuesta de desbloqueo, comando de puerta abierta, tiempo de verificación del sensor de puerta, primer comando de desbloqueo y tipo de contacto de puerta.

Paso 1 En la interfaz principal (Figura 3-1), seleccione **Configuración local** > **Control de acceso** > **Local**.

los **Local** se muestra la interfaz.

Figura 4-3 Local



Paso 2 Configure los parámetros y la descripción detallada.

Tabla 4-3 Descripción de los parámetros de control de acceso local

Parámetro	Descripción
Desbloquear Responder Intervalo	El intervalo de tiempo para desbloquear nuevamente después del desbloqueo anterior, y la unidad es la segunda.
Período de desbloqueo	La cantidad de tiempo durante el cual la cerradura permanece abierta después del desbloqueo y la unidad es la segunda.

Parámetro	Descripción
Comprobación del sensor de puerta	Si ha instalado un sensor de puerta, puede configurar el período de tiempo, y si el tiempo de desbloqueo excede el Tiempo de verificación del sensor de puerta , la alarma del sensor de la puerta se activa y la alarma se enviará al centro de gestión.
Hora	<ul style="list-style-type: none"> • Selecciona el Habilitar casilla de verificación, y la puerta no se bloqueará hasta que el sensor de la puerta entre en contacto. • Si no selecciona el Habilitar casilla de verificación, la puerta se bloqueará después de la Período de desbloqueo acabados.
Primer desbloqueo	Puede conectar un teléfono de terceros, como un teléfono SIP, a su VTO y usar el comando para abrir la puerta de forma remota. Seleccione CAROLINA DEL NORTE o NO según la cerradura que
Mando	
Tipo de contacto de puerta	utilice.

Paso 3 Haga clic en **Salvar**.

4.4 Sistema


Esta sección presenta cómo configurar el formato de fecha, el formato de hora y el servidor NTP.

Paso 1 En la interfaz principal (Figura 3-1), seleccione **Configuración local > Sistema**.

Figura 4-4 Sistema

Paso 2 Configure los parámetros.

Tabla 4-4 Descripción de los parámetros del sistema

Parámetro	Descripción
Formato de fecha	Puede seleccionar entre Año-Mes-Día, Mes-Día-Año y Día-Mes-Año.
Formato de tiempo	Configure el formato de hora, y puede seleccionar entre 12 horas o 24 horas .
Hora del sistema	<p>Configure la fecha, hora y zona horaria del sistema VTO.</p>  <p>No cambie la hora del sistema arbitrariamente; podría causar problemas en la búsqueda de videos y la publicación de instantáneas o avisos. Antes de cambiar la hora del sistema, apague la grabación de video o la instantánea automática.</p>
Sincronizar PC	Haga clic para sincronizar la hora del sistema VTO y la hora del sistema de la PC. Seleccione EN para habilitar
DST	DST. Seleccione Fecha para definir una fecha específica para el horario de verano o seleccionar Semana para ello.
Tipo de DST	

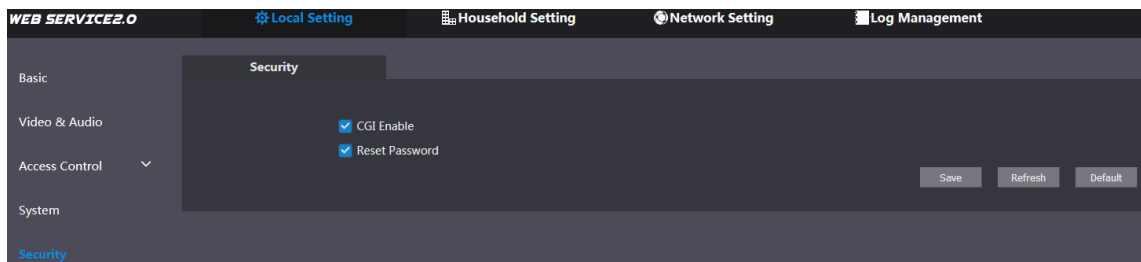
Parámetro	Descripción
Hora de inicio	Configure la hora de inicio y la hora de finalización del horario de verano.
Hora de finalización	
Habilitar NTP	Seleccione la casilla de verificación para habilitar la sincronización
Servidor NTP	NTP. Ingrese el nombre de dominio del servidor NTP. La zona
Zona	horaria del área actual.
Puerto	El número de puerto del servidor NTP.
Ciclo de actualización	El intervalo de tiempo que el VTO sincroniza con el servidor NTP y es de 30 minutos como máximo.
Auto Mantenimiento	Seleccione el día y la hora para el mantenimiento automático y el VTO se reiniciará.
SSH	Selecciona el Habilitar casilla de verificación, y luego puede conectar dispositivos de depuración al VTO a través del protocolo SSH.

Paso 3 Haga clic en **Salvar**.

4.5 Seguridad

Paso 1 En la interfaz principal (Figura 3-1), seleccione **Configuración local > Seguridad**.

Figura 4-5 Seguridad



Paso 2 Configure los parámetros.

Tabla 4-5 Descripción de los parámetros de seguridad

Parámetro	Descripción
Habilitar CGI	Seleccione la casilla de verificación para habilitar y luego puede usar el comando CGI. Seleccione la casilla de
Restablecer la contraseña	verificación para habilitar y luego el restablecimiento de la contraseña estará disponible.

Paso 3 Haga clic en **Salvar** ahorrar.

5 Entorno del hogar

Este capítulo se aplica a la condición en la que el VTO funciona como servidor SIP (consulte 6.2 Servidor SIP) y presenta cómo agregar, modificar y eliminar dispositivos VTO, VTH, VTS e IPC, y cómo enviar mensajes desde el SIP. servidor a otros dispositivos VTO y VTH. Si está utilizando otros servidores como servidor SIP, consulte el manual correspondiente para obtener la configuración detallada.

5.1 Gestión de número de VTO

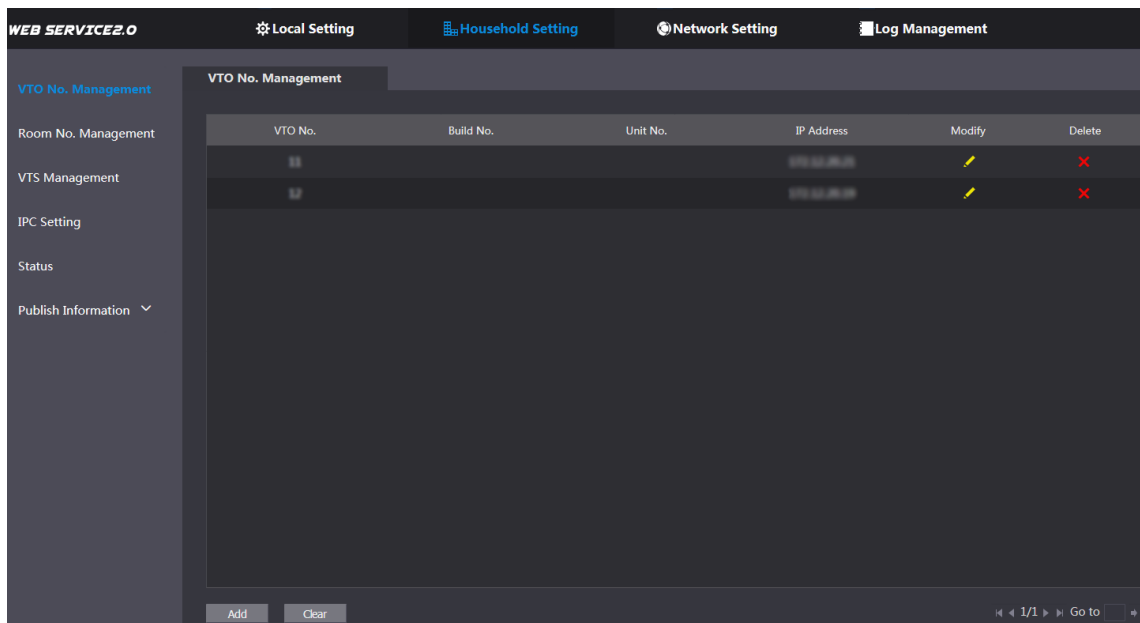
5.1.1 Agregar VTO

Puede agregar dispositivos VTO al servidor SIP y todos los dispositivos VTO conectados al mismo servidor SIP pueden realizar videollamadas entre sí.

Paso 1 Inicie sesión en la interfaz web del servidor SIP y luego seleccione **Entorno del hogar > VTO**

No. Gestión.

Figura 5-1 Gestión del número de VTO



Paso 2 Haga clic en **Añadir**.

Figura 5-2 Agregar VTO

Paso 3 Configure los parámetros y asegúrese de agregar también el servidor SIP.

Tabla 5-1 Agregar configuración de VTO

Parámetro	Descripción
Rec No.	El número de VTO que configuró para el VTO de destino. Consulte los detalles en la "Tabla 4-1".
Registrar contraseña	Mantener el valor predeterminado.
Construir No.	Disponible solo cuando otros servidores funcionan como servidor SIP.
Numero de unidad.	
Dirección IP	La dirección IP del VTO de destino.
Nombre de usuario	El nombre de usuario y la contraseña para la interfaz WEB del VTO de destino.
Contraseña	

Paso 4 Haga clic en **Salvar**.

5.1.2 Modificación de la información de VTO



El VTO que está actualmente en uso no se puede modificar ni eliminar.

Paso 1 En el **VTO No. Gestión** interfaz (Figura 5-1), haga clic en



Figura 5-3 Modificar VTO

The image shows a 'Modify' dialog box with a dark background and white text. It contains several input fields: 'Rec No.', 'Register Password', 'Build No.', 'Unit No.', 'IP Address', 'Username' (with 'admin' entered), and 'Password'. At the bottom right, there are 'Save' and 'Cancel' buttons. A close button (X) is in the top right corner.


Paso 2 Puede modificar el **Rec No.**, **nombre de usuario**, y **Contraseña**.

Paso 3 Haga clic en **Salvar**.

5.1.3 Eliminar VTO



El VTO que está actualmente en uso no se puede modificar ni eliminar.

Sobre el **VTO No. Gestión** interfaz (Figura 5-1), haga clic en  para eliminar VTO uno por uno; y

hacer clic **Claro** para borrar todos los VTO.

5.2 Gestión del número de habitación

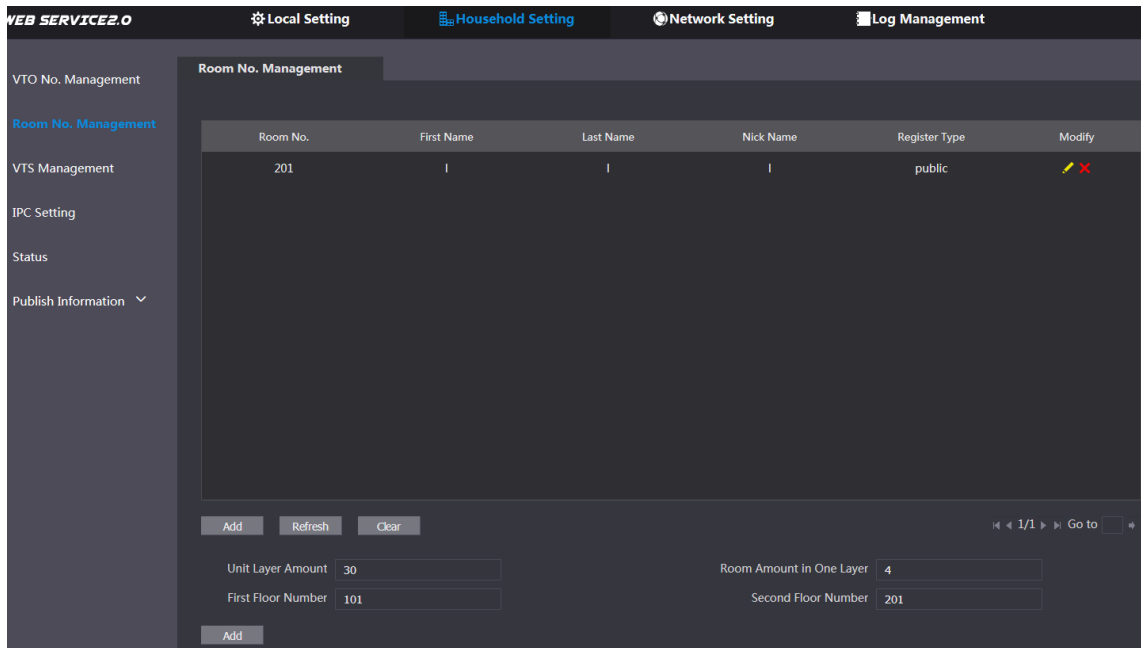
5.2.1 Agregar número de habitación

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.

Paso 1 Inicie sesión en la interfaz web del servidor SIP y luego seleccione **Ambiente doméstico > Habitación**

No. Gestión.

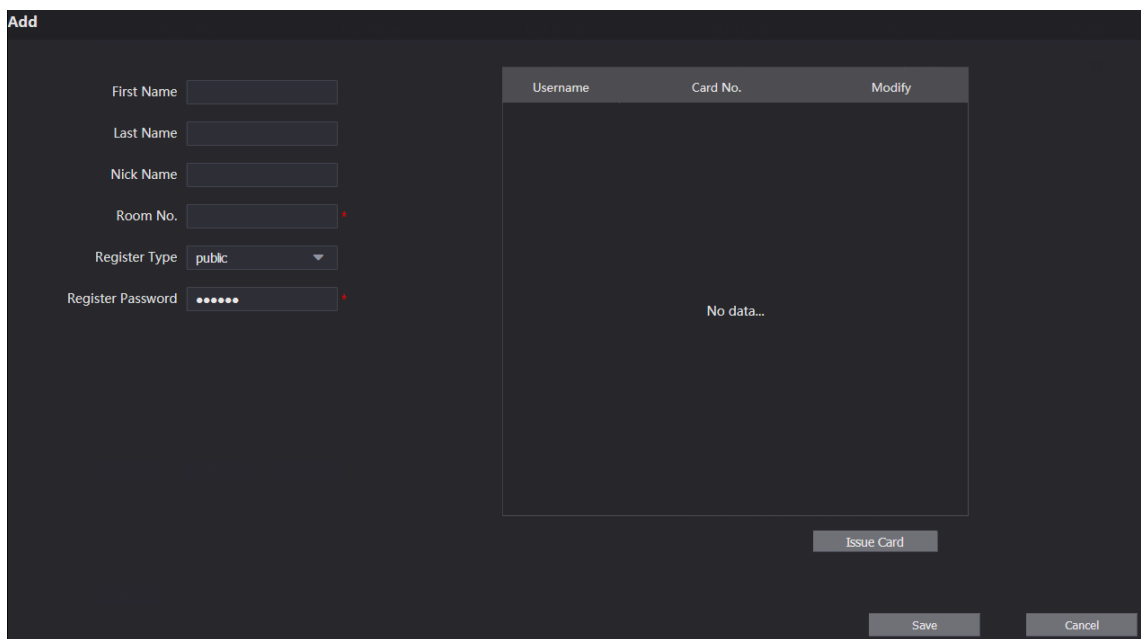
Figura 5-4 Gestión del número de habitación



Paso 2 Puede agregar un número de habitación individual o hacerlo por lotes.

- Agregar número de habitación individual
- 1) Haga clic en el **Añadir** en la posición media inferior.

Figura 5-5 Agregar número de habitación individual



- 2) Configure la información de la habitación.

Tabla 5-2 Información de la habitación

Parámetro	Descripción
Nombre de pila	Ingrese la información que necesita para diferenciar cada habitación.
Apellido	
Nombre de Nick	
Habitación no.	El número de habitación que planeaste.
Tipo de registro	Seleccione público , y local está reservado para uso futuro. Mantenga el valor
Registrar contraseña	predeterminado.

3) Haga clic en **Salvar**.

Se muestra el número de habitación agregado. Hacer clic



para modificar la información de la habitación y haga clic en



para eliminar una habitación.

• Agregar número de habitación en lote

1) Configure la Cantidad de capa de unidad, Cantidad de habitación en una capa, Número de primer piso y Número de segundo piso de acuerdo con la condición real.

2) Haga clic en el **Añadir** en la posición inferior.

Se muestran todos los números de habitación añadidos. Hacer clic **Actualizar** para ver el estado más reciente y haga clic en **Claro** para borrar todos los números de habitación.

5.2.2 Modificación del número de habitación

Paso 1 En el **Gestión de número de habitación** interfaz (Figura 5-4), haga clic en



Figura 5-6 Modificar el número de habitación

Username	Card No.	Modify
No data...		

Paso 2 Puede modificar los nombres de la habitación.

Paso 3 Haga clic en **Salvar**.

5.2.3 Emisión de tarjeta de acceso

Puede emitir una tarjeta a una habitación y también puede configurarla para que sea la tarjeta principal o para el estado perdido.

Paso 1 En el **Modificar el número de habitación** interfaz (Figura 5-6), haga clic en **Tarjeta de emisión**.

Se muestra el aviso de cuenta regresiva.

Figura 5-7 Aviso de cuenta regresiva

105s

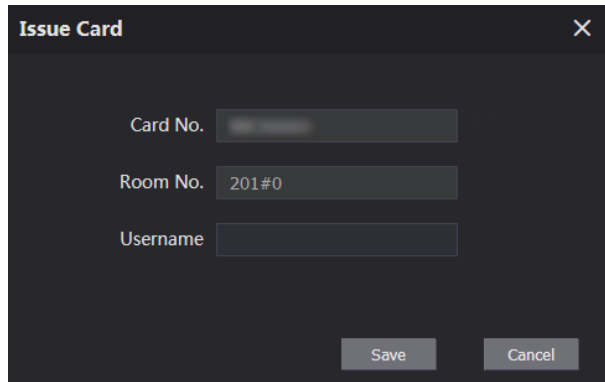
Card(s) 0

Confirm Send Card Cancel Send Card

Paso 2 Pase la tarjeta que necesita ser autorizada en el VTO y luego la **Tarjeta de emisión**

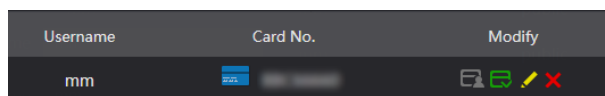




Se muestra el cuadro de diálogo.

Figura 5-8 Tarjeta de emisión









Paso 3 Ingrese el nombre que necesita, luego haga clic en **Salvar**, y luego haga clic en **Confirmar enviar tarjeta** en el aviso de cuenta regresiva (Figura 5-7).

Figura 5-9 Tarjeta de acceso emitida

Username	Card No.	Modify
mm	 [blurred]	   

Paso 4 Puede configurar la tarjeta de acceso.

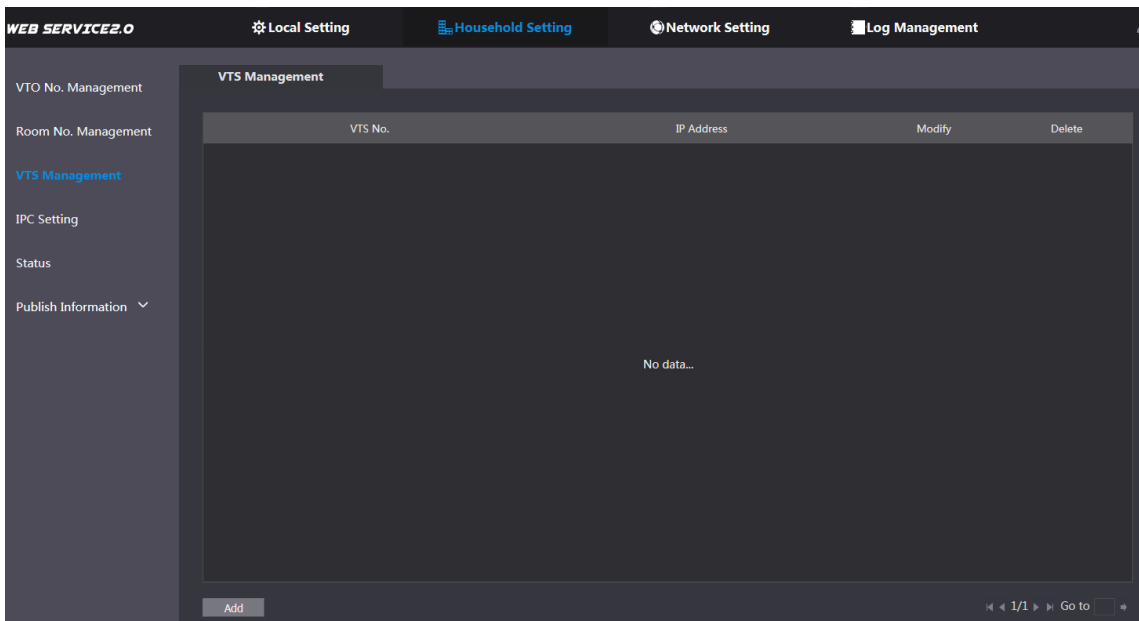
- Hacer clic  para configurarlo en la tarjeta principal, y luego el icono se convierte en . El principal
La tarjeta se puede utilizar para emitir una tarjeta de acceso para esta sala en el VTO. Haga clic nuevamente para reanudar.
- Hacer clic  para configurarlo en el estado perdido, y luego el icono se convierte en . La tarjeta
bajo estado perdido no se puede utilizar para abrir la puerta. Haga clic nuevamente para reanudar.
- Hacer clic  para modificar el nombre de usuario.
- Hacer clic  para borrar la tarjeta.

5.3 Gestión de VTS

Puede agregar un dispositivo VTS al servidor SIP y el VTS se puede utilizar como centro de administración. Puede administrar todos los dispositivos VTO y VTH en la red, realizar o recibir videollamadas de ellos y realizar configuraciones básicas. Para la introducción detallada, consulte el manual de usuario correspondiente.

Paso 1 Inicie sesión en la interfaz web del servidor SIP y luego seleccione **Configuración del hogar> VTS administración**

Figura 5-10 Gestión de VTS



Paso 2 Haga clic en **Añadir**.

Figura 5-11 Agregar VTS

Paso 3 Configure los parámetros y la descripción detallada.

Tabla 5-3 Agregar configuración de VTS

Parámetro	Descripción
VTS No.	El número de VTS que configuró para el VTS de destino. Mantener el valor
Registrar contraseña	predeterminado.
Dirección IP	La dirección IP del VTS de destino.

Paso 4 Haga clic en **Salvar**, y luego se muestra el VTS agregado. Hacer clic



para modificar la dirección IP, y

hacer clic  borrar.

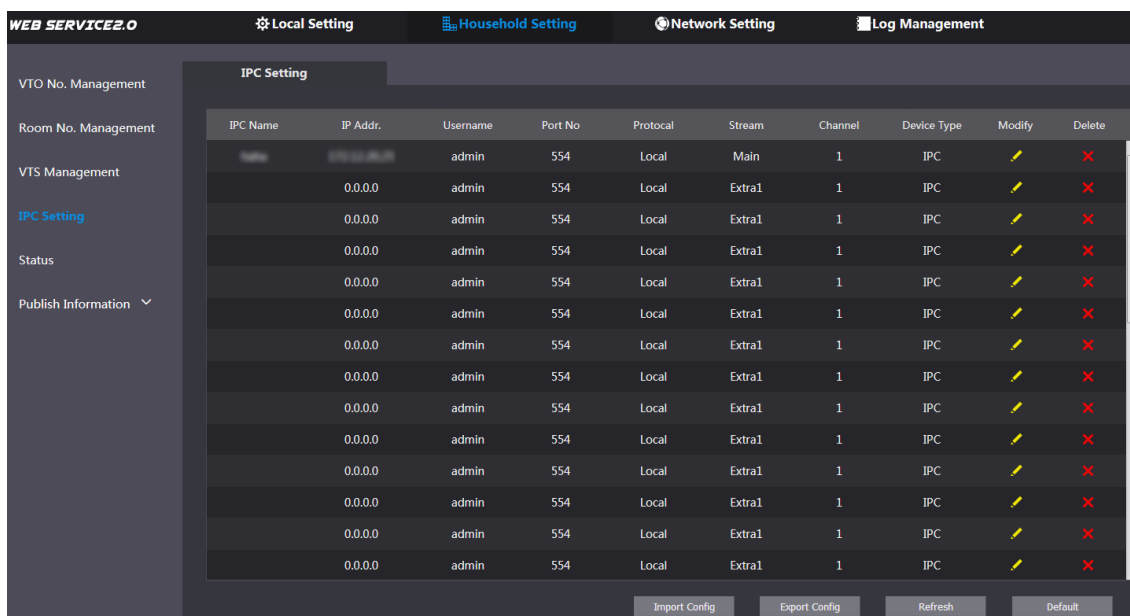
5.4 Configuración de IPC

Puede agregar IPC, NVR, HCVR y XVR al servidor SIP, y luego todo el VTH conectado puede monitorear con las cámaras agregadas.

Paso 1 Inicie sesión en la interfaz web del servidor SIP y luego seleccione **Entorno del hogar > IPC**

Ajuste

Figura 5-12 Configuración de IPC



Paso 2 La cantidad total del dispositivo que puede agregar es fija. Puede hacer clic



para agregar el

dispositivo que necesita.

Figura 5-13 Agregar IPC

Paso 3 Configure los parámetros y la descripción detallada.

Tabla 5-4 Agregar configuración de IPC

Parámetro	Descripción
Nombre del IPC	Ingrese el nombre del dispositivo que necesita. La
IPAddr.	dirección IP del dispositivo.
Nombre de usuario	El nombre de usuario y la contraseña de la interfaz web del dispositivo.
Contraseña	
Puerto No.	Mantener el valor predeterminado.
Protocolo	Seleccionar de Local o Onvif .

Parámetro	Descripción
Corriente	Seleccionar de Principal o Extra1 , y la transmisión principal tiene una mejor calidad de imagen, pero también cuesta más ancho de banda.
Canal	Defina un canal para el dispositivo. Seleccionar de IPC , NVR , HCVR , y XVR según
Tipo de dispositivo	sea necesario.

Paso 4 Haga clic en **Salvar**, y luego se muestra el dispositivo agregado. Hacer clic



para modificar y haga clic en



borrar.

También puede hacer clic en **Exportar configuración** para exportar los dispositivos actuales a la PC local, o haga clic en

Importar configuración para importar la configuración existente.

5.5 Estado

Puede ver el estado de funcionamiento y la dirección IP de todos los dispositivos conectados.

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

Figura 5-14 Estado

Room No.	Status	IP-Port	Reg Time	Off Time
201#0	Online	192.168.1.100	2018-10-09 02:01:58	0
201#1	Online	192.168.1.101	2018-10-09 02:02:11	0
12	Online	192.168.1.102	2018-10-09 02:02:15	0
11	Online	192.168.1.103	2018-10-09 02:06:20	0

5.6 Publicar información

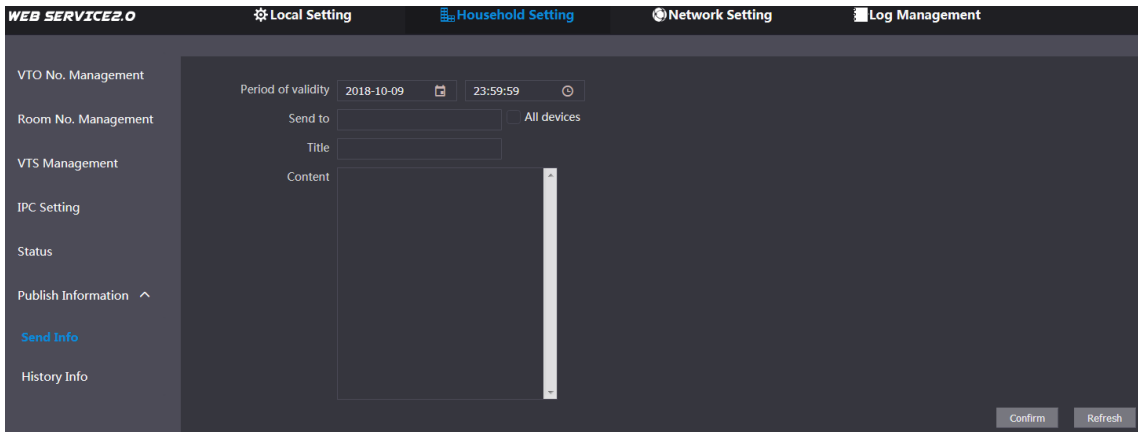
Puede enviar mensajes desde el servidor SIP a otros dispositivos VTH y ver el historial de envío de mensajes.

5.6.1 Enviar información

Paso 1 Inicie sesión en la interfaz web del servidor SIP y luego seleccione **Entorno del hogar>**

Publicar información> Enviar información.

Figura 5-15 Enviar información



Paso 2 Introduzca el número de VTO de destino o seleccione **Todo dispositivo** para enviar el mensaje a todos los dispositivos en la red, y luego el título y el contenido de su mensaje.



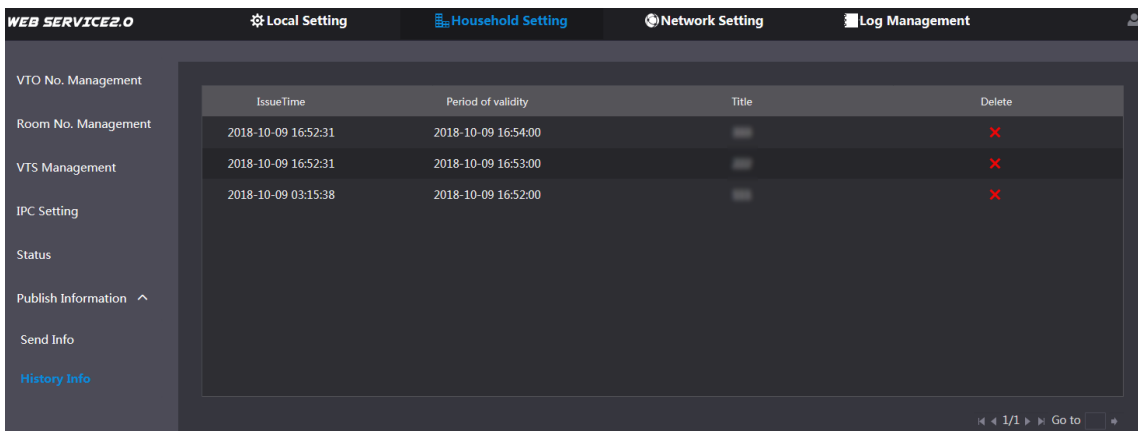
El período de validez está reservado para uso futuro.

Paso 3 Haga clic en **Confirmar**.

5.6.2 Información del historial

Inicie sesión en la interfaz web del servidor SIP y luego seleccione **Configuración del hogar > Publicar información > Información del historial**.

Figura 5-16 Información del historial



Puede ver la hora y el título de los mensajes enviados.

6 Configuración de red

Este capítulo presenta cómo configurar la dirección IP, el servidor SIP, DDNS y UPnP.

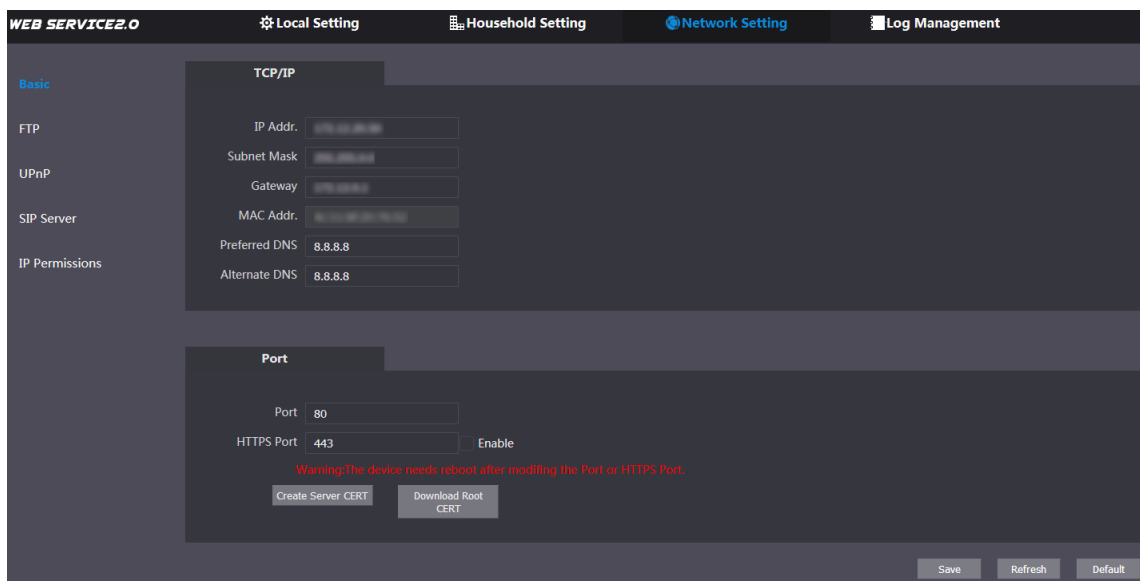
6.1 Básico

6.1.1 TCP / IP

Puede modificar la dirección IP y el número de puerto del VTO.

Paso 1 Seleccione **Configuración de red**> **Básico**.

Figura 6-1 TCP / IP y puerto



Paso 2 Ingrese los parámetros de red y el número de puerto que planeó, y luego haga clic en **Salvar**.

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 HTTPS

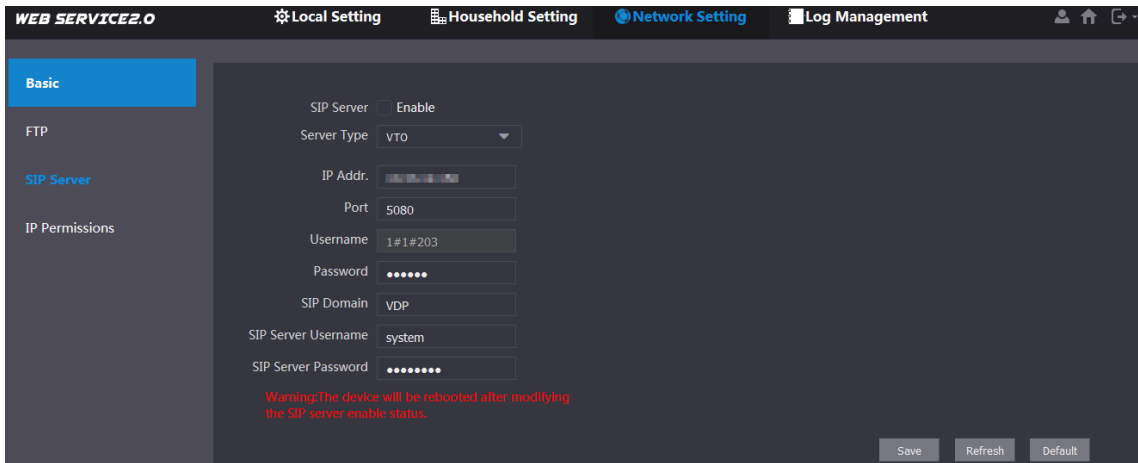
Selecciona el **Habilitar** casilla de verificación en **Puerto HTTPS**, y luego el VTO se reiniciará. Después de reiniciar, puede iniciar sesión en el VTO ingresando "https: // dirección IP de VTO" en la barra de direcciones del explorador.

6.2 Servidor SIP

Se requiere el servidor SIP en la red para transmitir el protocolo de intercomunicación, y luego todos los dispositivos VTO y VTH conectados al mismo servidor SIP pueden realizar videollamadas entre sí. Puede utilizar el dispositivo VTO u otros servidores como servidor SIP.

Paso 1 Seleccione **Configuración de red**> **Servidor SIP**.

Figura 6-2 Servidor SIP



Paso 2 Seleccione el tipo de servidor que necesita.

- Si el VTO que está visitando funciona como servidor SIP Seleccione el **Habilitar** casilla de verificación en **Servidor SIP**, y luego haga clic en **Salvar**.

El VTO se reiniciará y, después de reiniciar, podrá agregar dispositivos VTO y VTH a este VTO. Consulte los detalles en "5 Configuración del hogar".



Si el VTO que está visitando no funciona como servidor SIP, no seleccione el **Habilitar** casilla de verificación en **Servidor SIP**, de lo contrario, la conexión fallará.

- Si otro VTO funciona como servidor SIP Seleccione **VTO** en el **Tipo de servidor** lista y luego configure los parámetros.

Tabla 6-1 Configuración del servidor SIP

Parámetro	Descripción
IPAddr.	La dirección IP del VTO que funciona como servidor SIP. 5060
Puerto	
Nombre de usuario	Mantenga el valor predeterminado.
Contraseña	
Dominio SIP	VDP
Nombre de usuario del servidor SIP	El nombre de usuario y la contraseña para la interfaz web del servidor SIP.
Contraseña del servidor SIP	

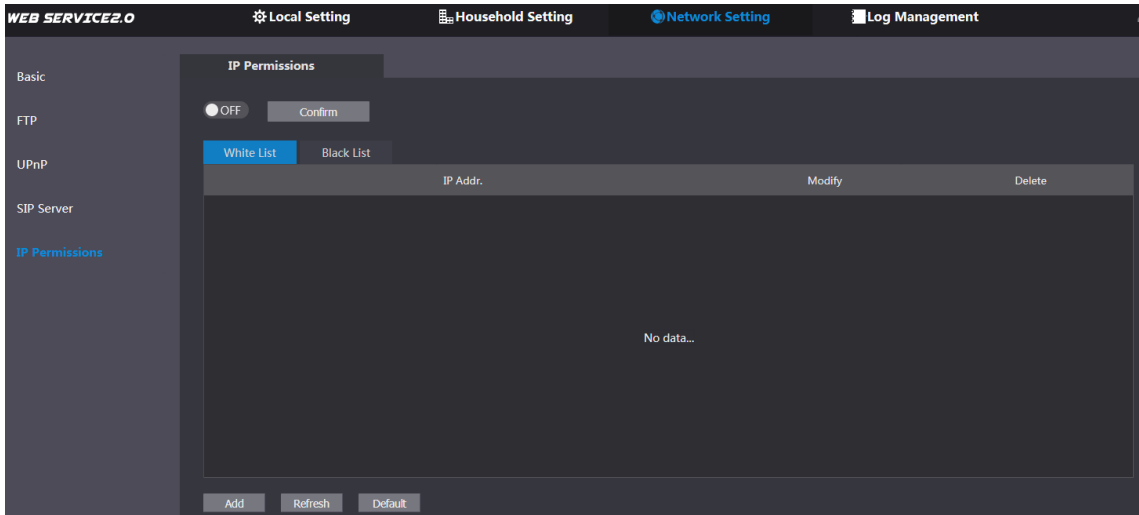
- Si otros servidores funcionan como servidor SIP Seleccione el tipo de servidor que necesita en **Tipo de servidor**, y luego consulte el manual correspondiente para la configuración detallada.

6.3 Permisos de IP

Para mejorar la seguridad de la red y los datos, debe configurar la autoridad de acceso para diferentes direcciones IP.

Paso 1 Seleccione **Configuración de red**> **Permisos de IP**.

Figura 6-3 Permisos de IP

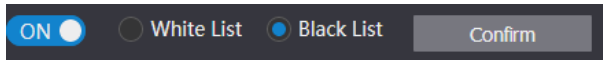


Paso 2 Haga clic en



los **Lista blanca** opción y **Lista negra** se muestran las opciones.

Figura 6-4 Lista blanca y lista negra



Solo puede usar uno de ellos al mismo tiempo.

- **Lista blanca:** solo las direcciones IP de la lista pueden iniciar sesión en el VTO.
- **Lista negra:** Todas las direcciones IP de la lista tienen prohibido iniciar sesión en el VTO.

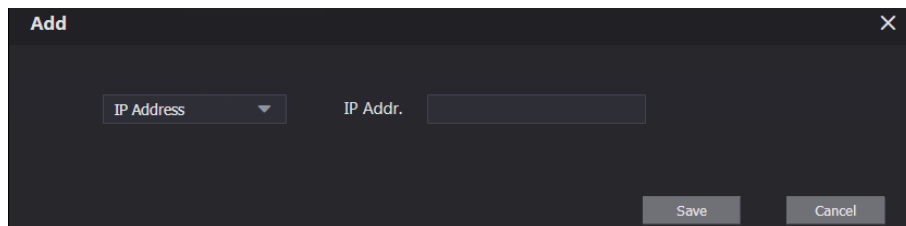
Paso 3 Seleccione **Lista blanca** o **Lista negra**.

- Si necesita utilizar la lista negra, seleccione **Lista negra**, y luego haga clic en **Confirmar**.
- Si necesita utilizar la lista blanca, seleccione **Lista Blanca**, y luego agregue una dirección IP o sección IP en la lista blanca antes de hacer clic **Confirmar**.

Paso 4 Haga clic en **Añadir**.

los **Añadir** se muestra la interfaz.

Figura 6-5 Agregar dirección IP



Paso 5 Puede seleccionar e ingresar una dirección IP única o una sección de IP y luego hacer clic en **Salvar**.

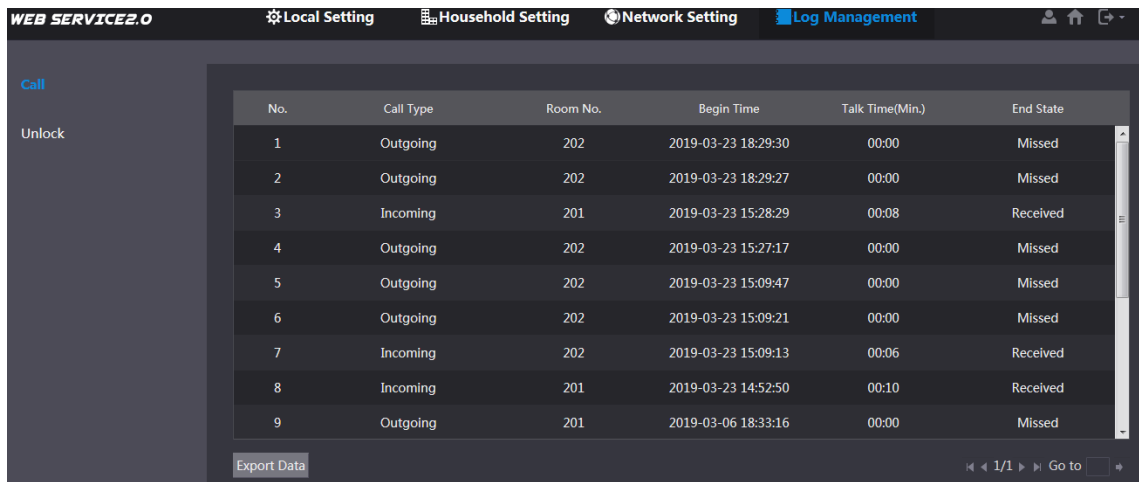
7 Gestión de registros

Puede ver el historial de llamadas, el registro de alarma, el registro de desbloqueo y varios registros del sistema.

7.1 Llamar

Puede ver el tipo de llamada, el número de habitación, la hora de inicio, el tiempo de conversación y el estado final. Seleccione **Gestión de registros> Llamar**.

Figura 7-1 Llamada



No.	Call Type	Room No.	Begin Time	Talk Time(Min.)	End State
1	Outgoing	202	2019-03-23 18:29:30	00:00	Missed
2	Outgoing	202	2019-03-23 18:29:27	00:00	Missed
3	Incoming	201	2019-03-23 15:28:29	00:08	Received
4	Outgoing	202	2019-03-23 15:27:17	00:00	Missed
5	Outgoing	202	2019-03-23 15:09:47	00:00	Missed
6	Outgoing	202	2019-03-23 15:09:21	00:00	Missed
7	Incoming	202	2019-03-23 15:09:13	00:06	Received
8	Incoming	201	2019-03-23 14:52:50	00:10	Received
9	Outgoing	201	2019-03-06 18:33:16	00:00	Missed

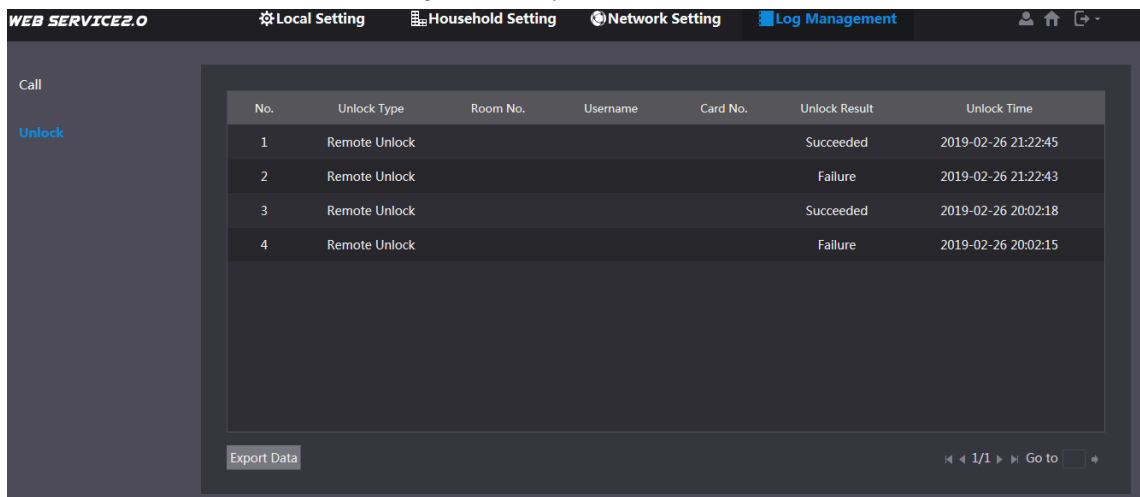
Hacer clic **Exportar datos** para exportar los registros a su PC.

7.2 Desbloquear

Puede ver varios registros de desbloqueo, incluido el desbloqueo de la tarjeta de acceso, el desbloqueo de contraseña, el desbloqueo remoto y el desbloqueo de botón de presión.

Seleccione **Gestión de registros> Desbloquear**.

Figura 7-2 Desbloqueo



No.	Unlock Type	Room No.	Username	Card No.	Unlock Result	Unlock Time
1	Remote Unlock				Succeeded	2019-02-26 21:22:45
2	Remote Unlock				Failure	2019-02-26 21:22:43
3	Remote Unlock				Succeeded	2019-02-26 20:02:18
4	Remote Unlock				Failure	2019-02-26 20:02:15

Hacer clic **Exportar datos** para exportar los registros a su PC.

Apéndice 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 muestran algunos consejos y recomendaciones sobre cómo crear un sistema de seguridad más seguro.

Acciones obligatorias que deben tomarse para la seguridad de la red de equipos básicos:

1. Utilice contraseñas seguras

Consulte las siguientes sugerencias para establecer contraseñas:

- La longitud no debe ser inferior a 8 caracteres;
- Incluya al menos dos tipos de personajes; los tipos de caracteres incluyen letras mayúsculas y minúsculas, números y símbolos;
- No 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 cliente a tiempo

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

Recomendaciones "Es bueno tener" para mejorar la seguridad de la red de su equipo:

1. Protección física

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

2. Cambie las contraseñas con regularidad

Le sugerimos que cambie las contraseñas con regularidad para reducir el riesgo de ser adivinado o descifrado.

3. Establecer y actualizar contraseñas Restablecer información a tiempo

El equipo admite la función de restablecimiento de contraseña. Configure la información relacionada para restablecer la contraseña a tiempo, incluido el buzón del usuario final y las preguntas sobre protección de contraseña. Si la información cambia, modifíquela a tiempo. Al configurar las preguntas de protección por contraseña, se sugiere no utilizar aquellas que se puedan 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 con la contraseña incorrecta varias veces, 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 en cualquier conjunto de números

entre 1024 ~ 65535, lo que reduce el riesgo de que personas externas 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. Habilitar lista blanca

Le sugerimos que habilite la función de lista blanca para evitar que todos, excepto aquellos con direcciones IP específicas, accedan al sistema. Por lo tanto, asegúrese de agregar la dirección IP de su computadora y la dirección IP del equipo adjunto a la lista blanca.

8. Enlace de dirección MAC

Le recomendamos que vincule la dirección IP y MAC de la puerta de enlace al equipo, reduciendo así el riesgo de suplantación de ARP.

9. Asignar cuentas y privilegios de forma razonable

De acuerdo con los requisitos comerciales y de administración, agregue usuarios de manera razonable y asígneles un conjunto mínimo de permisos.

10. Deshabilite los servicios innecesarios y elija modos seguros

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

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

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

11. Transmisión encriptada de audio y video

Si su contenido de datos de audio y video es muy importante o sensible, 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 provocará cierta pérdida en la eficiencia de transmisión.

12. Auditoría segura

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

13. Registro de red

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

14. Construya un entorno de red seguro

Para garantizar mejor la seguridad de los equipos y reducir los posibles riesgos cibernéticos, recomendamos:

- Desactive la función de asignación de puertos del enrutador para evitar el acceso directo a los dispositivos de la 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, red GAP y otras tecnologías para particionar la red.

para 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.