

Unidad VTO
(Versión 4.3)

Manual de usuario

V1.0.1

Recomendaciones de ciberseguridad

Acciones obligatorias a emprender hacia la ciberseguridad

1. Cambie las contraseñas y utilice contraseñas seguras:

La razón número uno por la que los sistemas son "pirateados" es porque tienen contraseñas débiles o predeterminadas. Se recomienda cambiar las contraseñas predeterminadas de inmediato y elegir una contraseña segura siempre que sea posible. Una contraseña segura debe estar formada por al menos 8 caracteres y una combinación de caracteres especiales, números y letras mayúsculas y minúsculas.

2. Actualiza el firmware

Como es el procedimiento estándar en la industria de la tecnología, recomendamos mantener actualizado el firmware de la cámara IP, DVR y NVR para garantizar que el sistema esté actualizado con los últimos parches y correcciones de seguridad.

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

1. Cambie las contraseñas con regularidad

Cambie periódicamente las credenciales de sus dispositivos para asegurarse de que solo los usuarios autorizados puedan acceder al sistema.

2. Cambie los puertos HTTP y TCP predeterminados:

- Cambiar los puertos HTTP y TCP predeterminados para los sistemas. Estos son los dos puertos que se utilizan para comunicarse y ver transmisiones de video de forma remota.
- Estos puertos se pueden cambiar a cualquier conjunto de números entre 1025-65535. Evitar los puertos predeterminados reduce el riesgo de que personas externas puedan adivinar qué puertos está utilizando.

3. Habilite HTTPS / SSL:

Configure un certificado SSL para habilitar HTTPS. Esto cifrará toda la comunicación entre sus dispositivos y la grabadora.

4. Habilite el filtro de IP:

Habilitar su filtro de IP evitará que todos, excepto aquellos con direcciones IP específicas, accedan al sistema.

5. Cambiar la contraseña de ONVIF:

En firmware de cámara IP anterior, la contraseña de ONVIF no cambia cuando cambia las credenciales del sistema. Deberá actualizar el firmware de la cámara a la última revisión o cambiar manualmente la contraseña de ONVIF.

6. Reenvíe solo los puertos que necesita:

- Solo reenvíe los puertos HTTP y TCP que necesita usar. No reenvíe una gran variedad de números al dispositivo. No DMZ la dirección IP del dispositivo.
- No necesita reenviar ningún puerto para cámaras individuales si todas están conectadas a una grabadora en el sitio; solo se necesita el NVR.

7. Desactive el inicio de sesión automático en SmartPSS:

Aquellos que usan SmartPSS para ver su sistema y en una computadora que es utilizada por varias personas deben deshabilitar el inicio de sesión automático. Esto agrega una capa de seguridad para evitar que los usuarios sin las credenciales adecuadas accedan al sistema.

8. Utilice un nombre de usuario y una contraseña diferentes para SmartPSS:

En caso de que su cuenta de redes sociales, banco, correo electrónico, etc. se vea comprometida, no querrá que alguien recopile esas contraseñas y las pruebe en su sistema de videovigilancia. El uso de un nombre de usuario y una contraseña diferentes para su sistema de seguridad hará que sea más difícil para alguien adivinar su camino hacia su sistema.

9. Limitar las funciones de las cuentas de invitado:

Si su sistema está configurado para varios usuarios, asegúrese de que cada usuario solo tenga derechos sobre las características y funciones que necesita utilizar para realizar su trabajo.

10. UPnP:

- UPnP intentará automáticamente reenviar puertos en su enrutador o módem. Normalmente esto sería bueno. Sin embargo, si su sistema reenvía automáticamente los puertos y deja las credenciales predeterminadas, puede terminar con visitantes no deseados.
- Si reenvió manualmente los puertos HTTP y TCP en su enrutador / módem, esta función debe desactivarse independientemente. Se recomienda deshabilitar UPnP cuando la función no se usa en aplicaciones reales.

11. SNMP:

Desactive SNMP si no lo está utilizando. Si está utilizando SNMP, debe hacerlo solo temporalmente, solo con fines de seguimiento y prueba.

12. Multidifusión:

La multidifusión se utiliza para compartir secuencias de video entre dos grabadoras. Actualmente no hay problemas conocidos relacionados con la multidifusión, pero si no está utilizando esta función, la desactivación puede mejorar la seguridad de su red.

13. Verifique el registro:

Si sospecha que alguien ha obtenido acceso no autorizado a su sistema, puede consultar el registro del sistema. El registro del sistema le mostrará qué direcciones IP se utilizaron para iniciar sesión en su sistema y a qué se accedió.

14. Bloquear físicamente el dispositivo:

Idealmente, desea evitar cualquier acceso físico no autorizado a su sistema. La mejor manera de lograrlo es instalar la grabadora en una caja de seguridad, en un bastidor de servidor con cerradura o en una habitación que esté detrás de una cerradura y una llave.

15. Conecte las cámaras IP a los puertos PoE en la parte posterior de un NVR:

Las cámaras conectadas a los puertos PoE en la parte posterior de un NVR están aisladas del mundo exterior y no se puede acceder a ellas directamente.

16. Aislar la red de cámaras IP y NVR

La red en la que residen su NVR y su cámara IP no debe ser la misma red que su red informática pública. Esto evitará que los visitantes o invitados no deseados accedan a la misma red que el sistema de seguridad necesita para funcionar correctamente.

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

No.	Versión	Contenido de la revisión	Fecha de lanzamiento
1	V1.0.0	Primer lanzamiento	Septiembre 2018

Aviso de protección de privacidad

Como usuario del dispositivo o controlador de datos, puede recopilar datos personales de otras personas, como rostro, huellas dactilares, número de placa del automóvil, dirección de correo electrónico, número de teléfono, GPS, etc. 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 al sujeto de los datos la existencia de un área de vigilancia y proporcionar información relacionada. contacto.

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. El producto

Las actualizaciones 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 lugar húmedo, polvoriento o fuliginoso.
- 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 lleno de líquido, para evitar que fluyan líquidos al 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, utilice 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

Recomendaciones de ciberseguridad	I Prólogo
.....	IV Salvaguardias y advertencias
importantes	VI 1 Inicialización
.....	1
2 Interfaz de inicio de sesión	3
2.1 Iniciar sesión	3
2.2 Restablecimiento de la contraseña	3
3 Interfaz principal	5
4 Configuración local	6
4.1 Básico	6
4.2 Video y audio	7
4.3 Control de acceso	9
4.3.1 Local	10
4.3.2 RS485	11
4.4 Sistema	12
4.5 Seguridad	13
4.6 Wiegand	13
4.7 Reconocimiento facial	14
5 Entorno del hogar	15
5.1 Gestión de No. de VTO	15
5.1.1 Agregar VTO	15
5.1.2 Modificación de VTO	dieciséis
5.1.3 Eliminación de VTO	17
5.2 Gestión de número de habitación	17
5.2.1 Agregar número de habitación	17
5.2.2 Modificación del número de habitación	19
5.2.3 Emisión de tarjeta de acceso	19
5.3 Gestión de VTS	20
5.4 Configuración de IPC	22
5.5 Estado	23
5.6 Publicar información	24
5.6.1 Enviar información	24
5.6.2 Información del historial	24
5.7 Gestión de rostros	25
5.7.1 Exportación de datos faciales	25
5.7.2 Importación de datos faciales	26
5.7.3 Eliminación de datos faciales	26
6 Configuración de red	27
6.1 Básico	27
6.1.1 TCP / IP	27
6.1.2 HTTPS	27

6.2 FTP	27
6.3 UPnP	28
6.4 Servidor SIP	30
6.5 Permisos de IP	31
7 Gestión de registros	33
7.1 Llamar	33
7.2 Alarma	33
7.3 Desbloquear	34
7.4 Registro	34

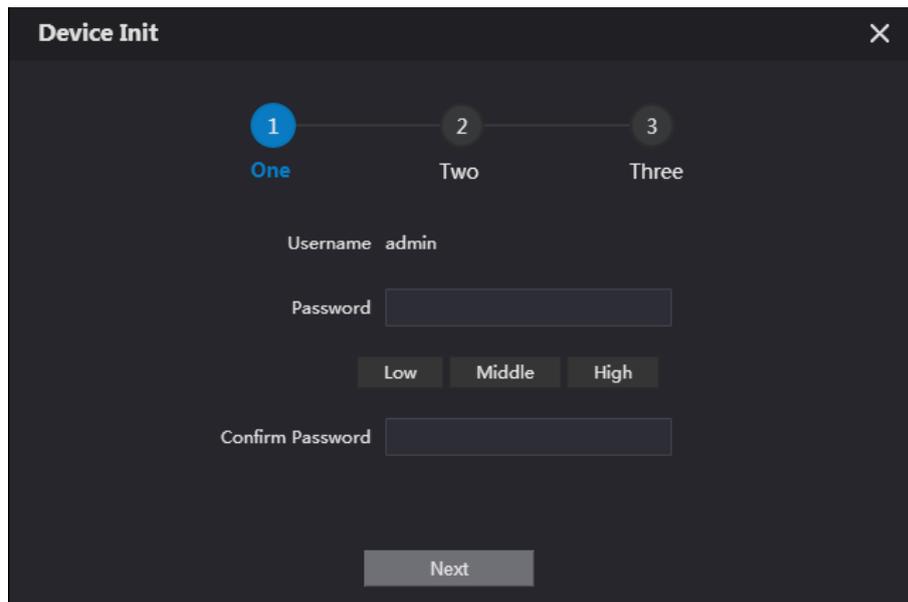
1 Inicialización

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. Los **Inicialización del dispositivo** se muestra la interfaz. Vea la Figura 1-1.

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. Seleccione el **Email** casilla de verificación y luego ingrese su dirección de correo

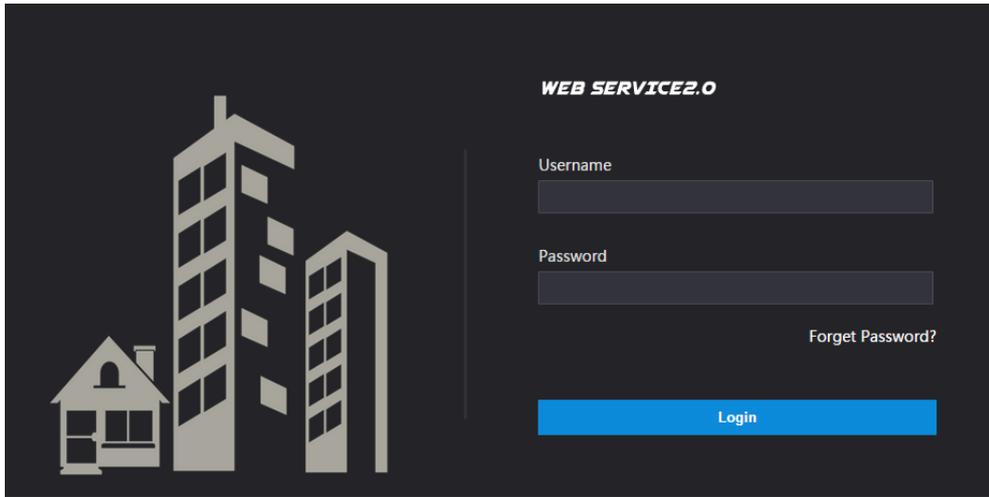
Paso 4 electrónico. Esta dirección de correo electrónico se puede utilizar para restablecer la contraseña y se recomienda finalizar esta configuración. Hacer clic **Próximo**. La inicialización tuvo éxito. Hacer clic **OKAY**.

Paso 5

Paso 6

Se muestra la interfaz de inicio de sesión. Vea la Figura 1-2.

Figura 1-2 Interfaz de inicio de sesión



2 Interfaz de inicio de sesión

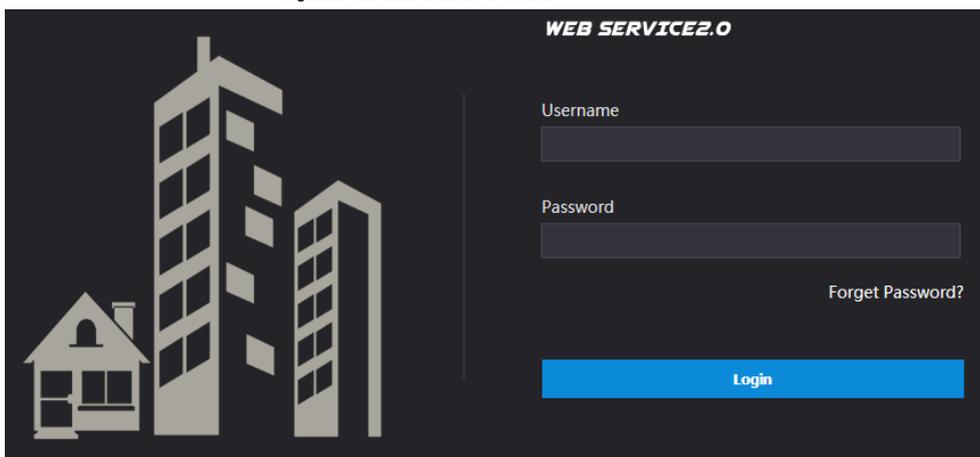
2.1 Iniciar sesión

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 Enter.

Se muestra la interfaz de inicio de sesión. Vea la Figura 2-1.

Figura 2-1 Interfaz de inicio de sesión



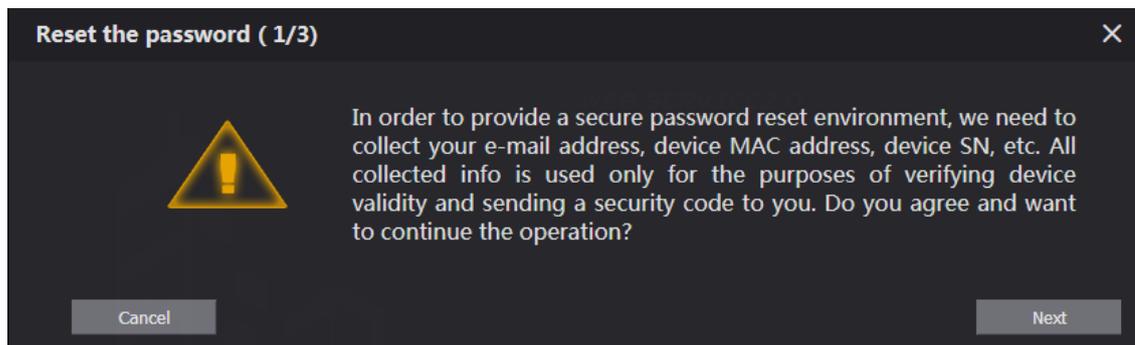
Paso 2 Ingrese "admin" como nombre de usuario, luego la contraseña que estableció durante la inicialización, y luego hacer clic **Iniciar sesión**.

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?**.

los **Restablecer la contraseña (1/3)** Se muestra el cuadro de diálogo. Vea la Figura 2-2.

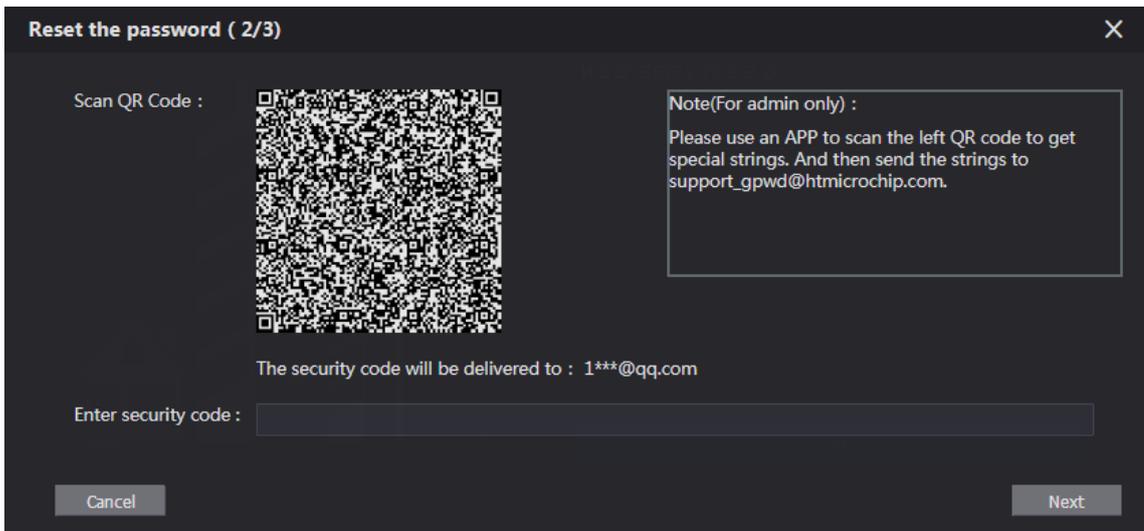
Figura 2-2 Restablecer la contraseña (1/3)



Paso 2 Haga clic en **Próximo**.

los **Restablecer la contraseña (2/3)** Se muestra el cuadro de diálogo. Vea la Figura 2-3.

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



Paso 3 Escanee el código QR 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.

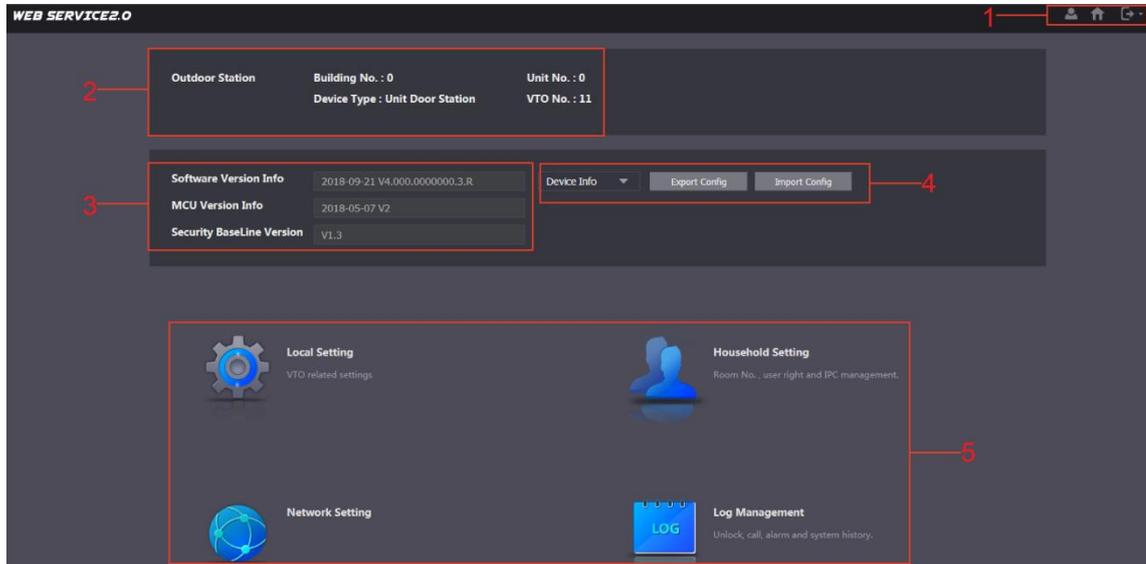
Paso 4 Haga clic en **Próximo**, y luego el **Restablecer la contraseña (3/3)** Se muestra el cuadro de diálogo.

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. Vea la Figura 3-1.

Figura 3-1 Interfaz principal



Para la introducción de la interfaz principal, consulte la Tabla 3-1.

Tabla 3-1 Introducción a la interfaz principal

No.	Función	Descripción
1	General función	Estos botones se muestran todo el tiempo <ul style="list-style-type: none"> Hacer clic  para cambiar la contraseña y su Dirección de correo electrónico. 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	VTO información	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	Config gerente	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.

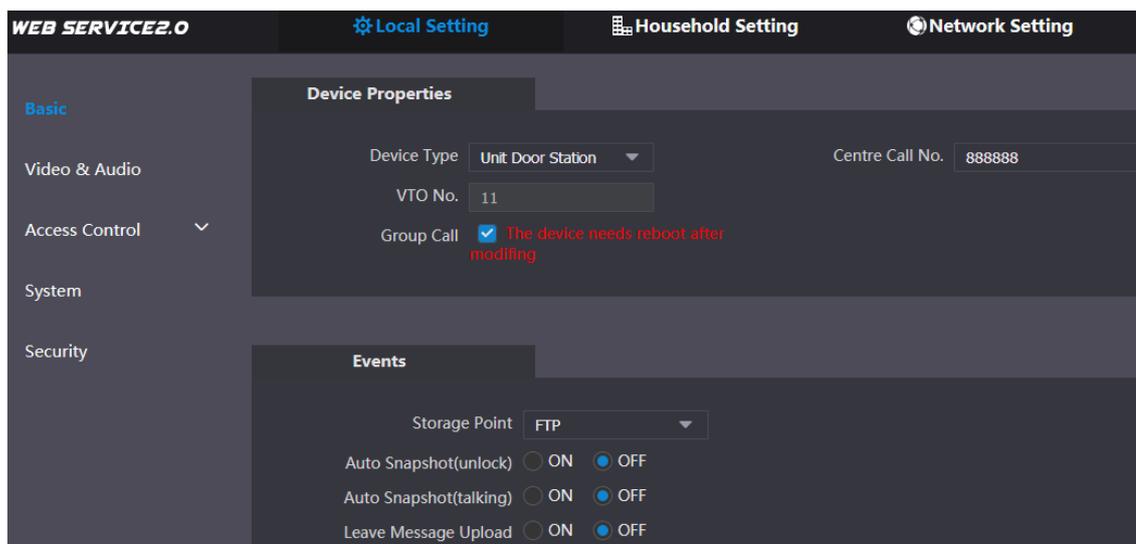
4.1 Básico

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**.

los **Básico** se muestra la interfaz. Vea la Figura 4-1.

Figura 4-1 Básico



Paso 2 Configure los parámetros y, para obtener una descripción detallada, consulte la Tabla 4-1.

Tabla 4-1 Descripción de los parámetros básicos

Parámetro	Descripción
Tipo de dispositivo	<p>Puede seleccionar la estación de puerta de la unidad o la estación de cerca.</p> <ul style="list-style-type: none">• Estación de puerta de la unidad: Normalmente se instala dentro de la comunidad con un número de edificio o número de unidad específico.• Estación de valla: Normalmente se instala en la puerta de la comunidad, y debe ingresar el número del edificio, el número de la unidad y el número de la habitación para llamar a una habitación específica. No puede dejar un mensaje o ver el contacto en la estación de la cerca. <p></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 "6.4 Servidor SIP".

Parámetro	Descripción
	<ul style="list-style-type: none"> La estación de valla se utiliza normalmente cuando otros servidores funcionan como servidor SIP.
Centro de llamadas No.	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.
VTO No.	<p>El número de VTO se puede utilizar para diferenciar cada VTO, y normalmente se configura según la unidad o el número de edificio. Puede agregar dispositivos VTO al servidor SIP con sus números.</p>  <p>Si un VTO no sirve como servidor SIP, entonces se puede modificar su número de VTO (inicie sesión en la página web del VTO y luego podrá modificarlo).</p>
Llamada grupal	<p>Seleccione la casilla de verificación para habilitar esta función, y cuando llame a un VTH maestro, los dispositivos de extensión VTH también recibirán la llamada. Solo puedes seleccionar FTP, y todas las instantáneas se guardarían en el servidor FTP automáticamente.</p>
Punto de almacenamiento	<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 al servidor FTP automáticamente.</p>  <ul style="list-style-type: none"> Primero debe habilitar la función FTP. Consulte "6.2 FTP". Si hay una tarjeta SD en el VTH principal, los mensajes de la izquierda se guardarán en la tarjeta SD de forma predeterminada. 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** ahorrar.

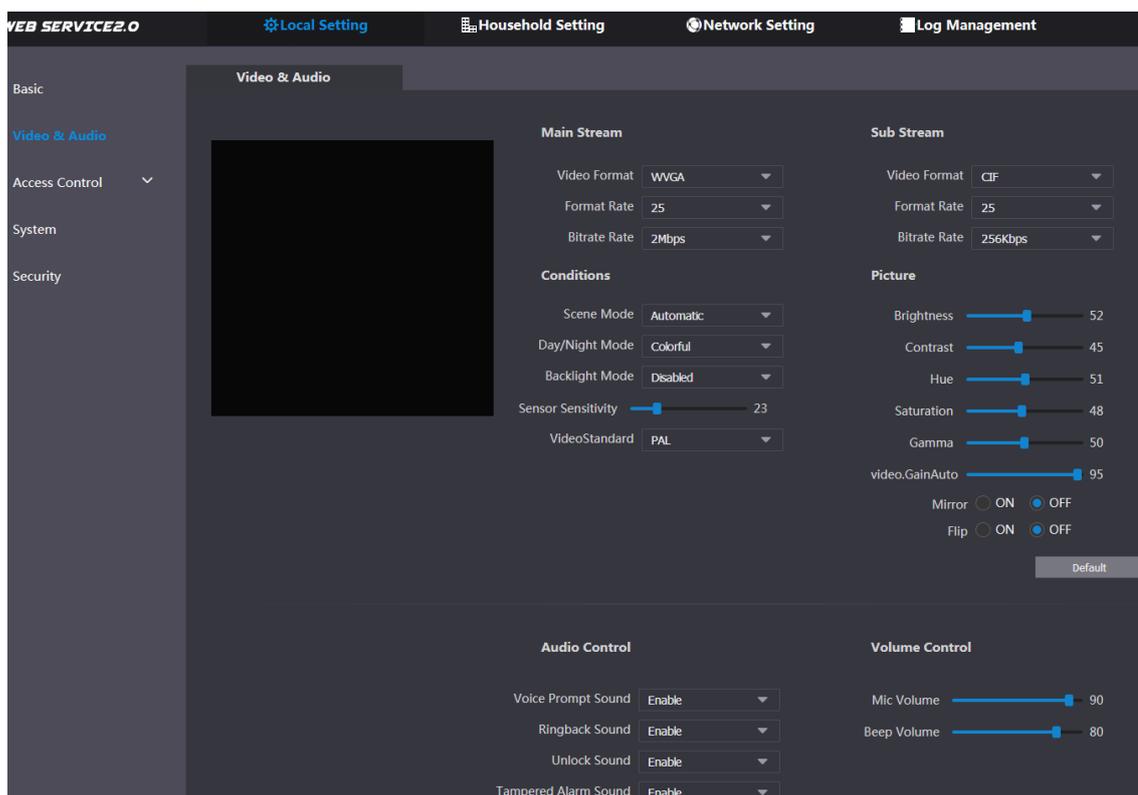
4.2 Video y audio

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**.

los **Audio video** se muestra la interfaz. Vea la Figura 4-2.

Figura 4-2 Video y audio



Paso 2 Configure los parámetros y estas configuraciones entrarán en vigor inmediatamente. Consulte la Tabla 4-2.

Tabla 4-2 Descripción de los parámetros de video

Parámetro	Descripción	
Principal Corriente	Formato de video	Seleccione la resolución de video 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 . Cuanto mayor sea el valor, más suave será el video.
	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 video.
Sub Corriente	Formato de video	Seleccione la resolución de video 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 . Cuanto mayor sea el valor, más suave será el video.
	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 video.
Condiciones	Modo escena	Ajusta el video para adaptarlo a diferentes escenarios. Puede seleccionar entre Automático, soleado, nocturno y Discapacitado . 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"> Discapacitado: sin luz de fondo. Iluminar desde el fondo: la cámara obtiene una imagen más clara de la oscuridad

Parámetro		Descripción
		<p>áreas del objetivo al disparar contra la luz.</p> <ul style="list-style-type: none"> • 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 video	Seleccionar 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.
	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
	Video.GainAuto	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.
	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

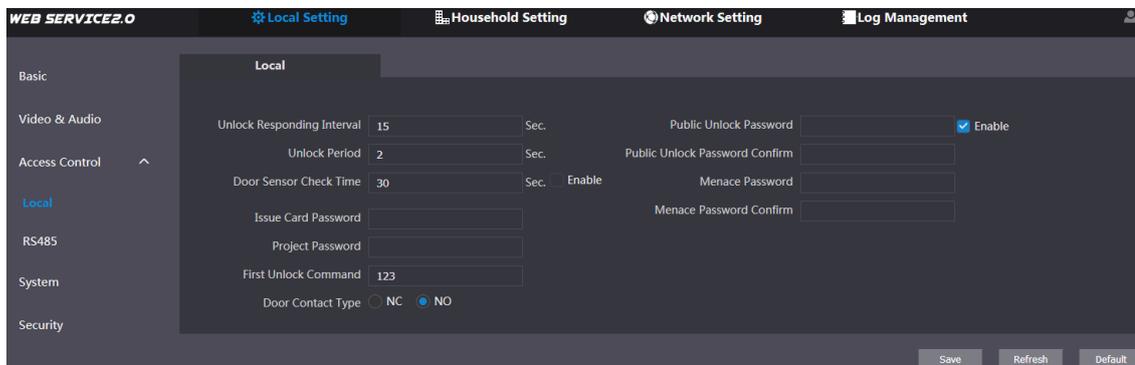
Esta sección presenta cómo configurar la cerradura, incluido el intervalo de respuesta de desbloqueo, el comando de puerta abierta, la contraseña de la tarjeta de emisión, la contraseña de coacción y el protocolo de control del ascensor.

4.3.1 Local

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

los **Local** se muestra la interfaz. Vea la Figura 4-3.

Figura 4-3 Local



Paso 2 Configure los parámetros y, para obtener una descripción detallada, consulte la Tabla 4-3.

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.
Comprobación del sensor de puerta Hora	<p>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.</p> <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.
Emitir contraseña de tarjeta	<p>Esta contraseña se puede utilizar para emitir una nueva tarjeta.</p> <p></p> <ul style="list-style-type: none"> • Esta contraseña es solo para administradores o ingenieros. Es 888888 • por defecto.
Contraseña del proyecto	<p>Se puede usar para ir a la interfaz de ingeniería y es 888888 por defecto.</p> <p></p> <p>La contraseña del proyecto es solo para administradores o ingenieros.</p>
Primer desbloqueo Mando	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
Tipo de contacto de puerta	utilice.
Desbloqueo público Contraseña	<p>Selecciona el Habilitar, luego configure la contraseña de desbloqueo público, y luego todos los residentes en esta unidad pueden abrir la puerta con esta contraseña.</p>
Desbloqueo público Contraseña confirmada	

Parámetro	Descripción
Contraseña de amenaza	En cualquiera de estas dos situaciones, puede utilizar una contraseña de amenaza.
Contraseña de amenaza	<ul style="list-style-type: none"> De forma predeterminada, la contraseña de amenaza es ingresar la contraseña de desbloqueo público invertida. Puede configurar cualquier número según sea necesario. Una vez que se usa la contraseña de coacción
Confirmar	<ul style="list-style-type: none"> Al usar VTO como servidor SIP, habrá un registro de alarma en Gestión de registros> Alarma. Al usar la plataforma como servidor SIP, puede conectar un dispositivo de salida de alarma para recibir un aviso de alarma.

Paso 3 Haga clic en **Salvar**.

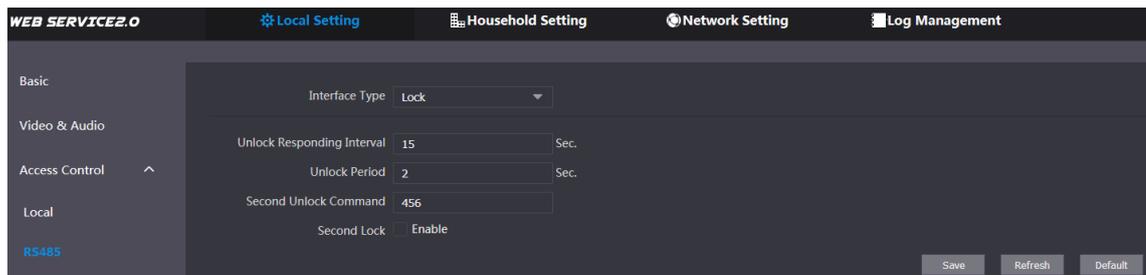
4.3.2 RS485

Esta sección presenta la configuración de control de acceso de los dispositivos RS-485, incluido el control de bloqueo y elevación.

Paso 1 En la interfaz principal (Figura 3-1), seleccione **Configuración local> Control de acceso> RS485**.

los **RS485** se muestra la interfaz. Vea la Figura 4-4.

Figura 4-4 RS485



Paso 2 Configure los parámetros y podrá seleccionar **Bloquear** o **Control de elevación** en el **Tipo de interfaz**

lista. Para obtener una descripción detallada, consulte la Tabla 4-4.

Tabla 4-4 Descripción de los parámetros de control de acceso RS-485

Parámetro	Descripción	
Bloquear	desbloquear Respondiendo 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.
	Segundo desbloqueo Mando	Puede conectar un teléfono de terceros, como un teléfono SIP, a su VTO y usar el comando para abrir la puerta de forma remota. Puede conectar una puerta más al dispositivo RS-485.
	Segundo bloqueo	<ul style="list-style-type: none"> Si selecciona el Habilitar casilla de verificación, el segundo candado se abrirá de forma predeterminada al presionar el botón de desbloqueo, deslizar la tarjeta de acceso o usar la contraseña de desbloqueo. Si no selecciona el Habilitar casilla de verificación, el primer candado se abrirá de forma predeterminada al presionar el botón de desbloqueo, deslizar la tarjeta de acceso o usar la contraseña de desbloqueo. Seleccione el protocolo según sea necesario para habilitar la función de control de ascensor, y luego puede configurar los pisos
Ascensor	Control de elevación	que levantan a los usuarios
<u>Controlar</u>	Protocolo	

Parámetro	Descripción
	puede ir a.
Tasa de baudios	Ingrese la velocidad en baudios del dispositivo RS-485 de terceros que necesita.
Bit de datos	Estos elementos se pueden utilizar para la depuración del puerto serie.
Comprobar Bit	
Bit de parada	

Paso 3 Haga clic en **Salvar**.

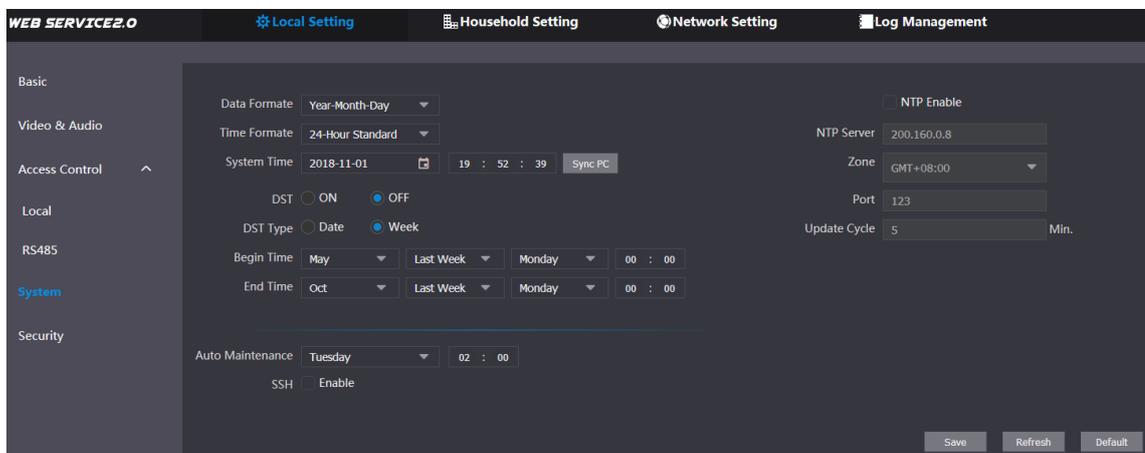
4.4 Sistema

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**.

los **Sistema** se muestra la interfaz. Vea la Figura 4-5.

Figura 4-5 Sistema



Paso 2 Configure los parámetros y, para obtener una descripción detallada, consulte la Tabla 4-5.

Tabla 4-5 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	Configure la fecha, hora y zona horaria del sistema VTO.  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. Haga clic para sincronizar la hora del sistema VTO y la hora del sistema de la PC.
Sincronizar PC	Seleccione EN para habilitar DST. Seleccione Fecha para definir una fecha específica para el horario de verano o
DST	seleccionar Semana para ello.
Tipo de DST	
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 NTP.

Parámetro	Descripción
Servidor NTP	Ingrese el nombre de dominio del servidor NTP. La zona
Zona	horaria del área actual. El número de puerto del servidor
Puerto	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**.

los **Seguridad** se muestra la interfaz. Vea la Figura 4-6.

Figura 4-6 Seguridad



Paso 2 Configure los parámetros y, para obtener una descripción detallada, consulte la Tabla 4-6.

Tabla 4-6 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.

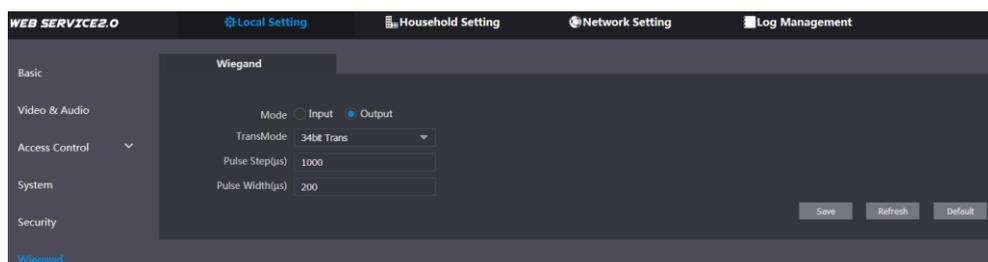
4.6 Wiegand

Esta sección presenta cómo configurar los parámetros para dispositivos Wiegand.

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

los **Wiegand** se muestra la interfaz. Vea la Figura 4-7.

Figura 4-7 Wiegand



Paso 2 Configure los parámetros. Consulte la Tabla 4-7.

Tabla 4-7 Parámetro Wiegand

Parámetro	Descripción
Modo	Seleccione Entrada o Salida según el tipo de dispositivo Wiegand. Seleccione la velocidad de
TransMode	transmisión de 34 bits , 66 bits , y 26 bits . Cuanto mayor sea el valor, más rápida será la transmisión.
Paso de pulso (µs)	La frecuencia de la señal Wiegand es 1000 por defecto. El valor máximo
Ancho de pulso (µs)	de la señal Wiegand es 200 por defecto.

Paso 3 Haga clic en **Salvar**.

4.7 Reconocimiento facial



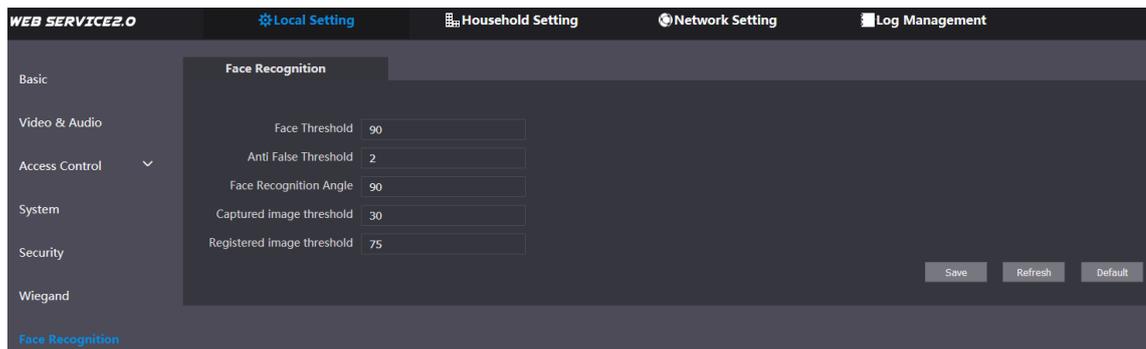
El reconocimiento facial está disponible en modelos seleccionados.

Esta sección presenta cómo configurar el umbral de reconocimiento facial, el umbral anti-falso y el ángulo de reconocimiento facial.

Paso 1 Seleccione **Configuración local > Reconocimiento facial**.

los **Reconocimiento facial** se muestra la interfaz. Vea la Figura 4-8.

Figura 4-8 Reconocimiento facial



Paso 2 Configure los parámetros de reconocimiento facial. Consulte la Tabla 4-8.

Tabla 4-8 Descripción del parámetro de reconocimiento facial

Parámetro	Descripción
Umbral facial	Cuanto mayor sea el valor, más similar será el objetivo y los datos faciales guardados se requieren para abrir la puerta.
Anti falso Límite	Cuanto mayor sea el valor, menor será la posibilidad de que el sistema defina un objetivo como rostro humano, por lo tanto, más preciso será.
Reconocimiento facial Ángulo	Cuanto mayor sea el valor, mayor será el ángulo en el que el objetivo puede girar su rostro durante el reconocimiento.
Imagen capturada límite	La calidad de las imágenes capturadas, cuanto mayor sea el valor, mejor será la calidad.
Imagen registrada límite	La calidad de imagen requerida para registrarse correctamente, cuanto mayor sea el valor, mejor se requiere que sea la calidad.

Paso 3 Haga clic en **Salvar**.

5 Entorno del hogar

Este capítulo se aplica a la condición en la que el VTO funciona como servidor SIP (consulte 6.4 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

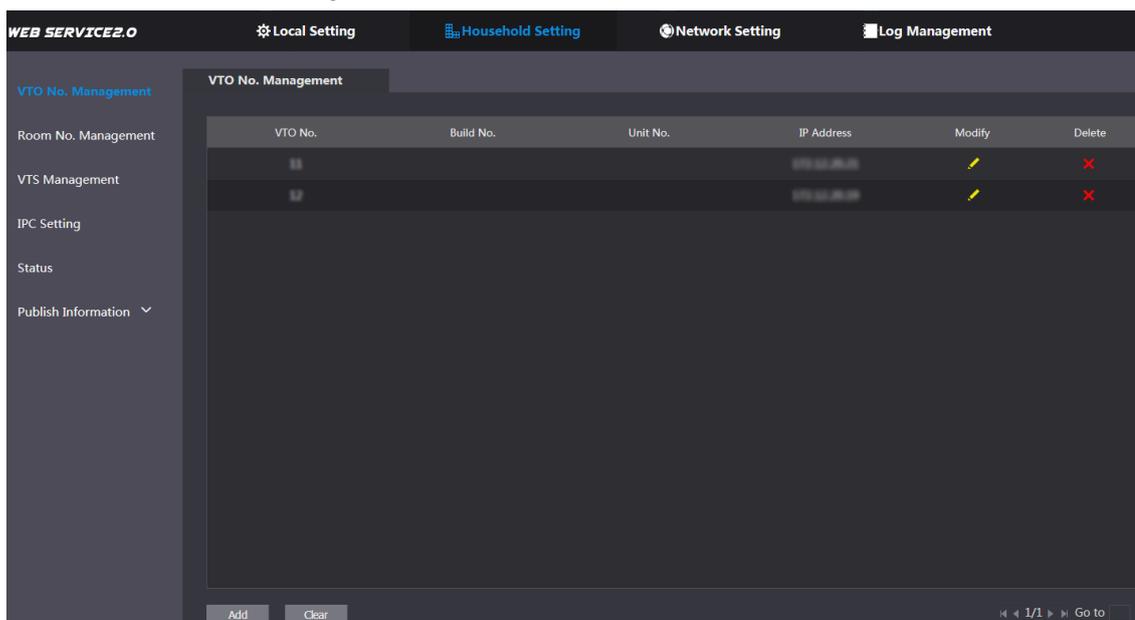
Puede agregar dispositivos VTO al servidor SIP y todos los dispositivos VTO conectados al mismo servidor SIP pueden realizar videollamadas entre sí.

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

No. Gestión.

los **VTO No. Gestión** se muestra la interfaz. Vea la Figura 5-1.

Figura 5-1 Gestión del número de VTO



Paso 2 Haga clic en **Añadir**.

los **Añadir** se muestra la interfaz. Vea la Figura 5-2.

Figura 5-2 Agregar VTO

Paso 3 Configure los parámetros y asegúrese de agregar también el servidor SIP. Consulte la Tabla 5-1.

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 VTO



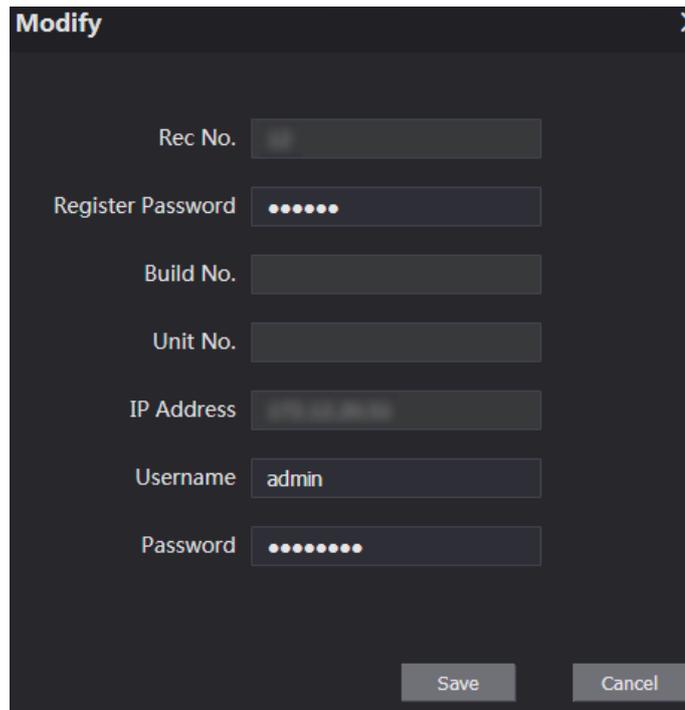
El VTO que está actualmente en uso no se puede modificar ni eliminar.

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



los **Modificar** se muestra la interfaz. Vea la Figura 5-3.

Figura 5-3 Modificar VTO



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

Paso 2 Puede modificar el **Rec No.**, **nombre de usuario**, y **Contraseña**. Consulte la Tabla 5-1 para obtener más detalles.

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

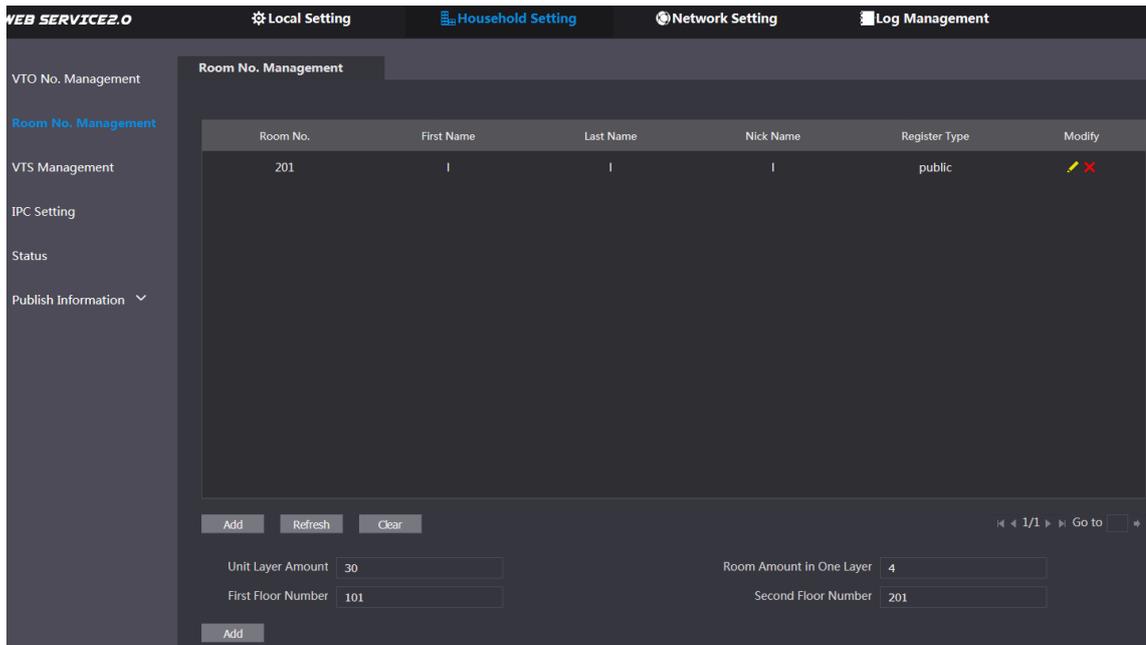
Puede agregar el número de habitación planificado al servidor SIP y luego configurar el número de habitación en los dispositivos VTH para conectarlos a la red.

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

No. Gestión.

los **Gestión de número de habitación** se muestra la interfaz. Vea la Figura 5-4.

Figura 5-4 Gestión del número de habitación



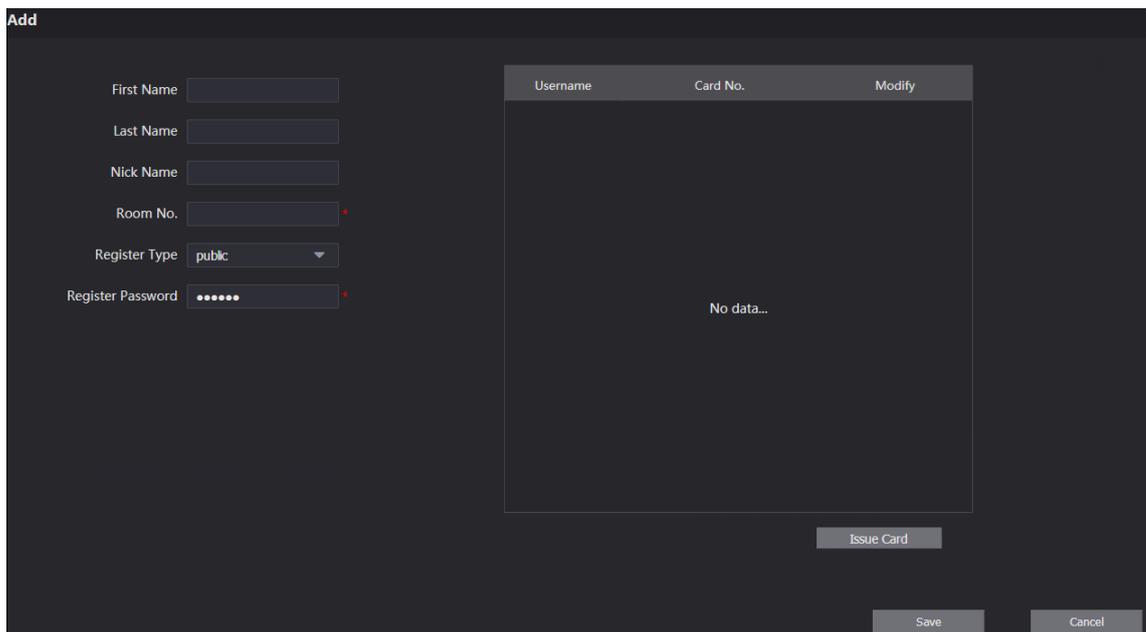
Paso 2 Puede agregar un número de habitación individual o hacerlo por lotes.

- Agregar número de habitación individual

1) Haga clic en el **Añadir** en la posición media inferior.

los **Añadir** se muestra la interfaz. Vea la Figura 5-5.

Figura 5-5 Agregar número de habitación individual



2) Configure la información de la habitación y la descripción detallada. Consulte la Tabla 5-2.

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. Seleccione público , y local está
Tipo de registro	reservado para uso futuro.

Parámetro	Descripción
Registrar contraseña Conservar	el valor 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 Configure el **Cantidad de capa de unidad, cantidad de habitación en una capa, número de primer piso, y Número del segundo piso** según la condición real. Haga clic en el **Añadir** en la posición inferior.

2)

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



los **Modificar** se muestra la interfaz. Vea la Figura 5-6.

Figura 5-6 Modificar el número de habitación

Paso 2 Puede modificar los nombres de la habitación. Consulte la Tabla 5-2 para obtener más detalles.

Paso 3 Haga clic en **Salvar**.

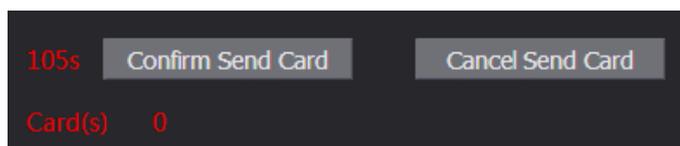
5.2.3 Emisión de tarjeta de acceso

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 la interfaz Modificar número de habitación (Figura 5-6), haga clic en **Tarjeta de emisión**.

Se muestra el aviso de cuenta regresiva. Vea la Figura 5-7.

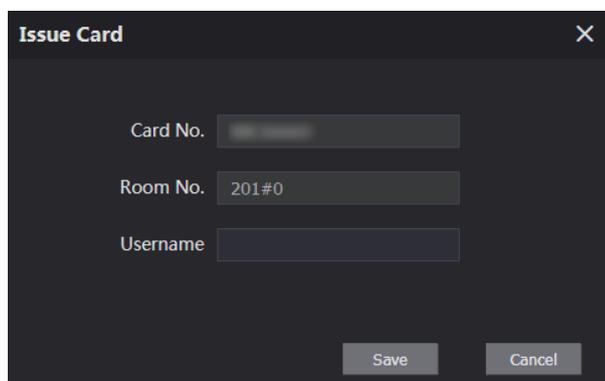
Figura 5-7 Aviso de cuenta regresiva



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

Se muestra el cuadro de diálogo. Vea la Figura 5-8.

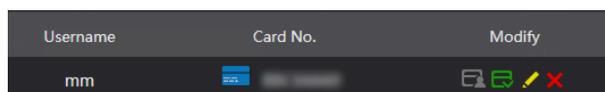
Figura 5-8 Tarjeta de emisión



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).

Se muestra la tarjeta de acceso emitida. Vea la Figura 5-9.

Figura 5-9 Tarjeta de acceso emitida



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

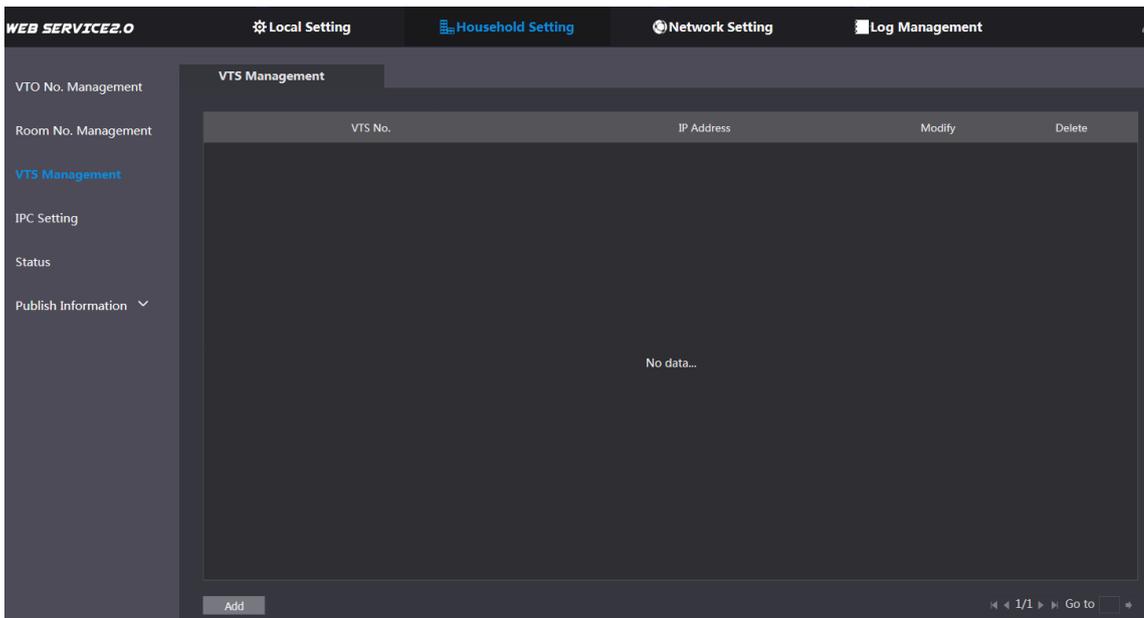
Puede agregar un dispositivo VTS al servidor SIP y el VTS se puede utilizar como centro de administración. Puede administrar todos los dispositivos VTO y VTH en la red, realizar o recibir videollamadas de ellos y realizar configuraciones básicas. Para la introducción detallada, consulte el manual de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

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

administración

los **Gestión de VTS** se muestra la interfaz. Vea la Figura 5-10.

Figura 5-10 Gestión de VTS



Paso 2 Haga clic en **Añadir**.

los **Añadir** se muestra la interfaz. Vea la Figura 5-11.

Figura 5-11 Agregar VTS

Paso 3 En VTS, seleccione **Configuración > Configuración avanzada**, luego ingrese la contraseña (123456 por predeterminado), y luego seleccione **Servidor SIP**, el **VTS No.** se muestra como **Nombre de usuario** (normalmente es 888888XXX).

Paso 4 Configure los parámetros y, para obtener una descripción detallada, consulte la Tabla 5-3.

Tabla 5-3 Agregar configuración de VTS

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

Paso 5 Haga clic en **Salvar**, y luego se muestra el VTS agregado. Hacer clic



para modificar la dirección IP, y



hacer clic **borrar**.

Paso 6 Seleccione **Configuración local > Básico**, luego ingrese el No. de VTS del VTS agregado en **Centro de llamadas**

No., y luego puede llamar al VTS presionando el botón del centro de llamadas en el VTO. Vea la Figura 5-12.

Figura 5-12 Número de llamada al centro



Paso 7 Haga clic en **Confirmar**.

5.4 Configuración de IPC

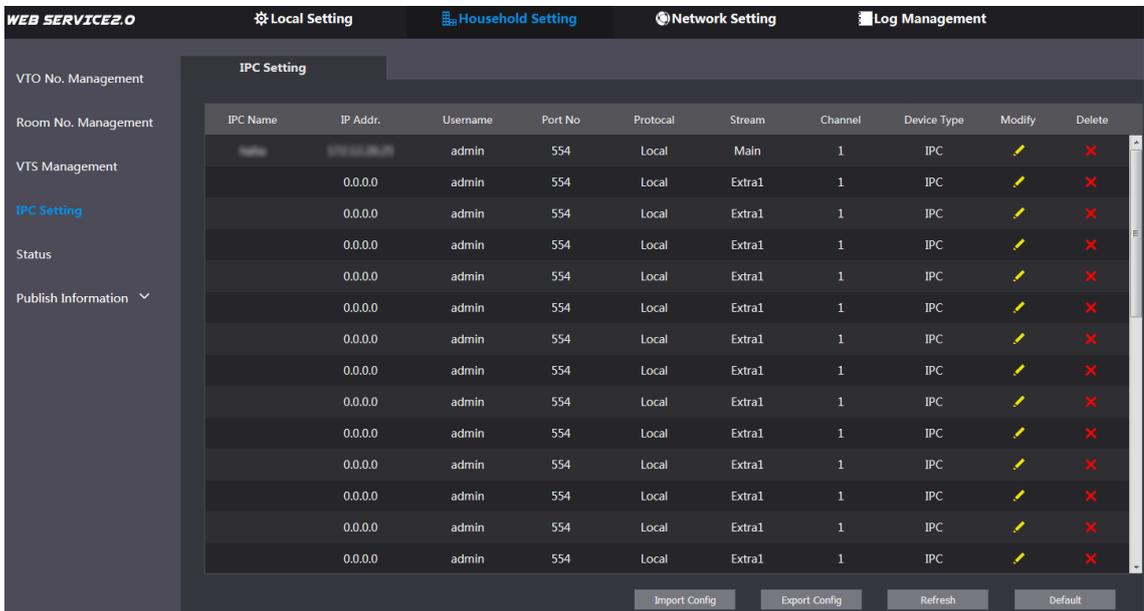
Puede agregar IPC, NVR, HCVR y XVR al servidor SIP, y luego todo el VTH conectado puede monitorear con las cámaras agregadas.

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

Ajuste

los **Configuración de IPC** se muestra la interfaz. Vea la Figura 5-13.

Figura 5-13 Configuración de IPC



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



para agregar el

dispositivo que necesita.

los **Modificar** se muestra la interfaz. Vea la Figura 5-14.

Figura 5-14 Agregar IPC

Paso 3 Configure los parámetros y, para obtener una descripción detallada, consulte la Tabla 5-4.

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 .
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**.

los **Estado** se muestra la interfaz. Vea la Figura 5-15.

Figura 5-15 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**.

los **Enviar información** se muestra la interfaz. Vea la Figura 5-16.

Figura 5-16 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.



- Si desea enviar información a más de un VTH, los números VTH deben estar separados por punto y coma. Por ejemplo, si ingresa 101; 102; 103 y más, y VTH de estos números VTH recibirán información enviada por el VTO. 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**.

los **Información de historia** se muestra la interfaz. Vea la Figura 5-17.

Figura 5-17 Información del historial

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

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

5.7 Gestión facial

Puede agregar, eliminar, importar y exportar datos faciales.



- El reconocimiento facial está disponible en modelos seleccionados. El VTO
- puede salvar 10,000 caras como máximo.

Seleccione **Configuración del hogar** > **Gestión facial**.

los **Gestión facial** se muestra la interfaz. Vea la Figura 5-18.

Figura 5-18 Gestión de rostros

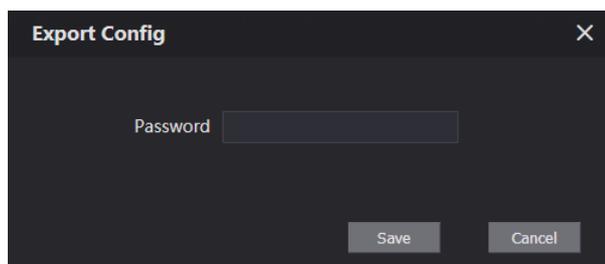
No.	Room No.	Username	Personnel No.	Modify	Delete
1	101		L101_1540223183	✏	✖
2	101		L101_1540223188	✏	✖
3	101		L101_1540223193	✏	✖
4	101		L101_1540223198	✏	✖
5	101		L101_1540223211	✏	✖
6	101		L101_1540223216	✏	✖
7	13	10020013.jpg	100000013	✏	✖
8	14	10020014.jpg	100000014	✏	✖
9	15	10020015.jpg	100000015	✏	✖
10	16	10020016.jpg	100000016	✏	✖
11	17	10020017.jpg	100000017	✏	✖
12	18	10020018.jpg	100000018	✏	✖
13	19	10020019.jpg	100000019	✏	✖
14	20	10020020.jpg	100000020	✏	✖

5.7.1 Exportación de datos faciales

Paso 1 clic **Exportación de información facial**.

los **Exportar configuración** se muestra la interfaz. Vea la Figura 5-19.

Figura 5-19 Exportar configuración



Paso 2 Ingrese la contraseña para la interfaz web y luego haga clic en **Salvar** para exportar datos faciales.

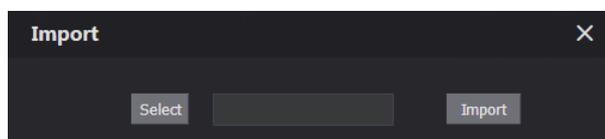
5.7.2 Importación de datos faciales

Paso 1 clic **Importación de información facial**.

Paso 2 Ingrese la contraseña para la interfaz web y luego haga clic en **Salvar**.

Se muestra la interfaz de importación. Vea la Figura 5-20.

Figura 5-20 Importar



Paso 3 Haga clic en **Seleccione**, y luego seleccione el archivo que necesita.

Paso 4 Haga clic en **Importar**.

5.7.3 Eliminar datos faciales

Hacer clic  para eliminar los datos de una sola cara.

Hacer clic **Eliminar todo** para eliminar todos los datos faciales.

6 Configuración de red

Este capítulo presenta cómo configurar la dirección IP, FTP, 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**.

Se muestran la información de TCP / IP y la información del puerto. Vea la Figura 6-1.

Figura 6-1 TCP / IP y puerto

The screenshot shows the 'Network Setting' page of the WEB SERVICE2.0 interface. The 'TCP/IP' section includes fields for IP Addr., Subnet Mask, Gateway, MAC Addr., Preferred DNS (8.8.8.8), and Alternate DNS (8.8.8.8). The 'Port' section includes fields for Port (80) and HTTPS Port (443) with an 'Enable' checkbox. Below the HTTPS Port field is a red warning message: 'Warning: The device needs reboot after modifying the Port or HTTPS Port.' At the bottom of the Port section are two buttons: 'Create Server CERT' and 'Download Root CERT'. At the very bottom of the page are 'Save', 'Refresh', and 'Default' buttons.

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.

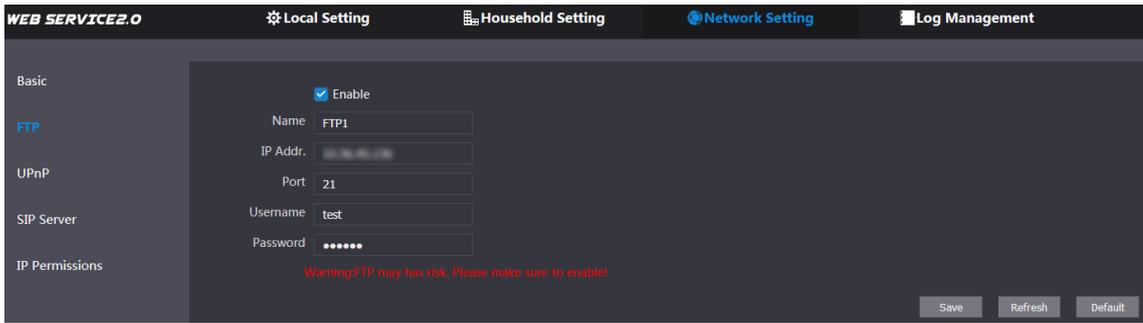
6.2 FTP

Configure el servidor FTP y luego podrá guardar los videos grabados y las instantáneas en el servidor FTP.

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

los **FTP** se muestra la interfaz. Vea la Figura 6-2.

Figura 6-2 FTP



Paso 2 Configure los parámetros. Consulte la Tabla 6-1.

Tabla 6-1 Descripción de los parámetros de FTP

Parámetro	Descripción
Habilitar	Seleccione la casilla de verificación para habilitar la función FTP.
Nombre	Ingrese el nombre del servidor FTP según sea necesario. La dirección
IPAddr.	IP del servidor FTP.
Puerto	Es 21 por defecto.
Nombre de usuario	El nombre de usuario y la contraseña del servidor FTP.
Contraseña	

Paso 3 Haga clic en **Salvar**.

6.3 UPnP

Universal Plug and Play, un protocolo que establece la relación de mapeo de puertos en LAN y WAN. Esta función le permite visitar el dispositivo de área local a través de una red de área amplia.

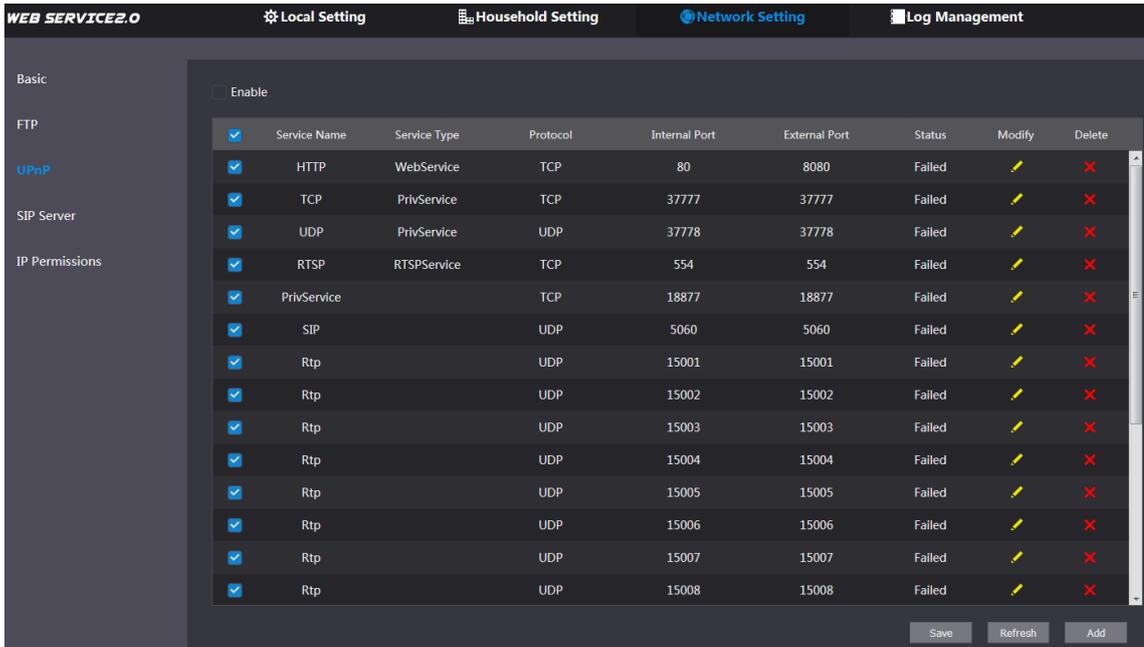


- Esta función es válida solo cuando VTO funciona como servidor SIP.
- Esta función es necesaria solo cuando el VTO está conectado a un enrutador con función UPnP.

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

los **UPnP** se muestra la interfaz. Vea la Figura 6-3.

Figura 6-3 UPnP



Paso 2 Seleccione el **Habilitar** casilla de verificación para habilitar la función UPnP.

Paso 3 Se han realizado algunas relaciones de mapeo en la fábrica, y puede hacer clic

modificarlos. O puede hacer clic **Añadir** para agregar uno nuevo.

los **Modificar / Agregar** se muestra la interfaz. Vea la Figura 6-4.



Figura 6-4 Modificar / Agregar UPnP

Paso 4 Configure los parámetros. Consulte la Tabla 6-2.

Tabla 6-2 Descripción de los parámetros UPnP

Parámetro	Descripción
ENCENDIDO APAGADO	Seleccione EN para habilitar esta relación de mapeo.
Nombre del servicio	El nombre del servicio. Tipo de
servicio	Defina el tipo de servicio según sea necesario. Puede seleccionar entre TCP y UDP . Para la
Protocolo	estabilidad de la transmisión, TCP es recomendado.

Parámetro	Descripción
Puerto interno	El puerto en el área local VTO que debe visitar.
Puerto externo	El puerto del enrutador al que se está asignando el puerto VTO.



- Intente utilizar un número de puerto entre 1024 y 5000 y no entre 1 y 255 y entre 256 y 1023 cuando asigne puertos al enrutador para evitar conflictos. Cuando asigne varios dispositivos a los puertos externos, haga la planificación con anticipación para evitar asignar diferentes dispositivos al mismo puerto externo.
- Asegúrese de que los puertos que está utilizando no se utilicen ni estén restringidos. Los puertos externos de TCP y UDP deben ser los mismos.

Paso 5 Haga clic en **Salvar**.

Abra el navegador web en la PC e ingrese "http:// dirección IP WAN: número de puerto externo", y luego puede visitar el dispositivo de área local con el puerto correspondiente.

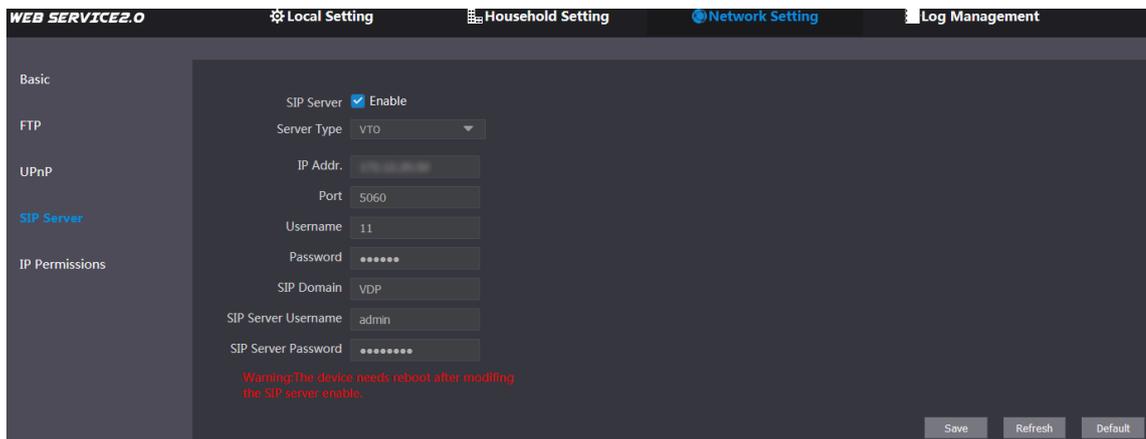
6.4 Servidor SIP

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**.

los **Servidor SIP** se muestra la interfaz. Vea la Figura 6-5.

Figura 6-5 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**, 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. Consulte la Tabla 6-3.

Tabla 6-3 Configuración del servidor SIP

Parámetro	Descripción
IPAddr.	La dirección IP del VTO que funciona como servidor SIP.
Puerto	5060
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.

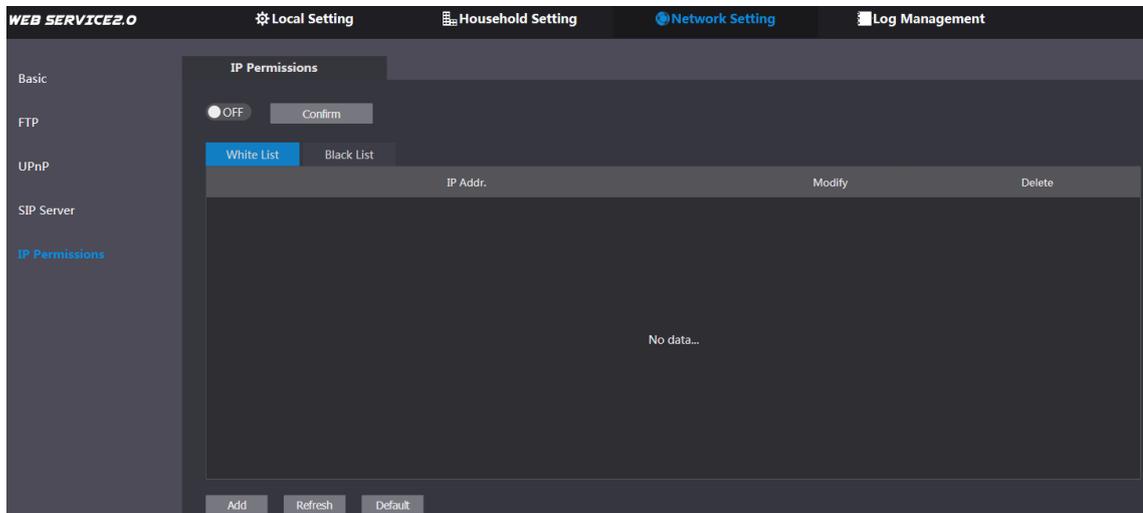
6.5 Permisos de IP

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**.

los **Permisos de IP** se muestra la interfaz. Vea la Figura 6-6.

Figura 6-6 Permisos de IP

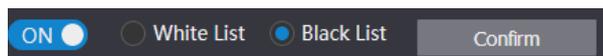


Paso 2 Haga clic en



los **Lista blanca** opción y **Lista negra** se muestran las opciones. Vea la Figura 6-7.

Figura 6-7 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.

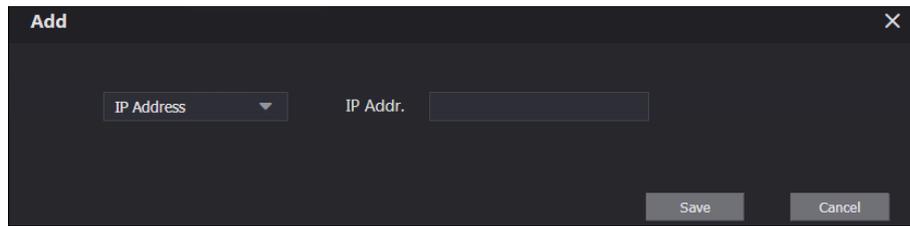
- Si necesita utilizar la lista negra, seleccione **Lista negra**, y luego haga clic en **Confirmar**.

- 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. Vea la Figura 6-8.

Figura 6-8 Agregar dirección IP



The image shows a dark-themed dialog box titled "Add" with a close button (X) in the top right corner. Inside the dialog, there is a dropdown menu labeled "IP Address" with a downward arrow. To its right is the label "IP Addr." followed by a text input field. At the bottom right of the dialog, there are two buttons: "Save" and "Cancel".

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

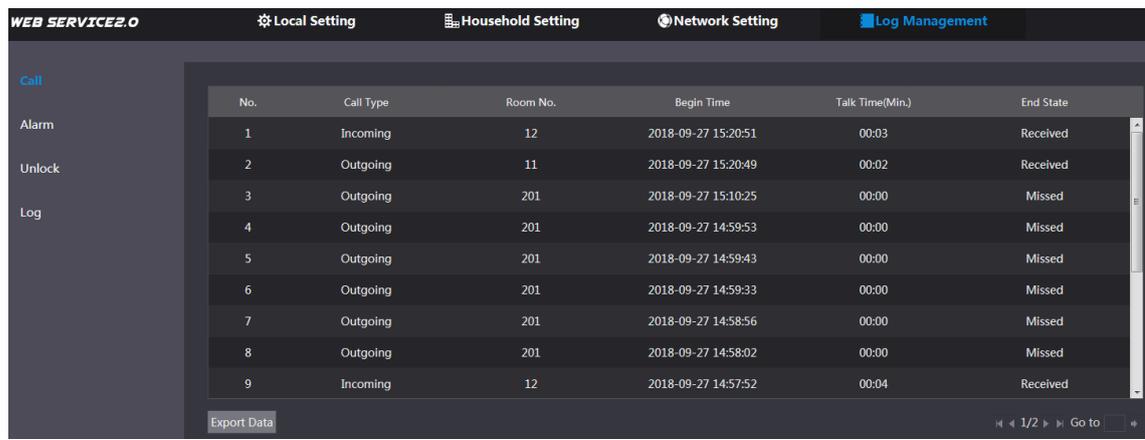
Puede ver el historial de llamadas, el registro de alarma, el registro de desbloqueo y varios registros del sistema.

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**.

los **Llamada** se muestra la interfaz. Vea la Figura 7-1.

Figura 7-1 Llamada



No.	Call Type	Room No.	Begin Time	Talk Time(Min.)	End State
1	Incoming	12	2018-09-27 15:20:51	00:03	Received
2	Outgoing	11	2018-09-27 15:20:49	00:02	Received
3	Outgoing	201	2018-09-27 15:10:25	00:00	Missed
4	Outgoing	201	2018-09-27 14:59:53	00:00	Missed
5	Outgoing	201	2018-09-27 14:59:43	00:00	Missed
6	Outgoing	201	2018-09-27 14:59:33	00:00	Missed
7	Outgoing	201	2018-09-27 14:58:56	00:00	Missed
8	Outgoing	201	2018-09-27 14:58:02	00:00	Missed
9	Incoming	12	2018-09-27 14:57:52	00:04	Received

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

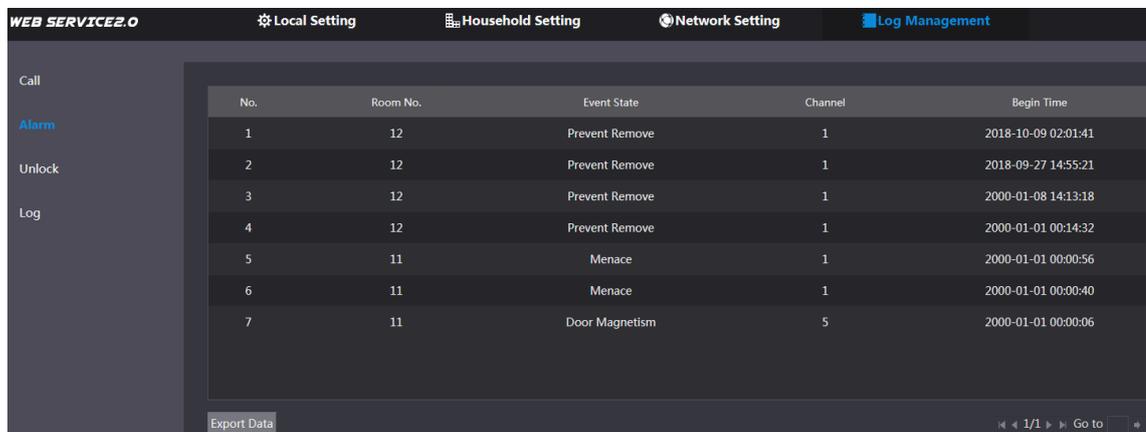
7.2 Alarma

Esta función se muestra solo cuando el VTO que está visitando funciona como servidor SIP, y puede ver el registro de alarma de VTO y VTH y el registro de alarma de contraseña de coacción.

Seleccione **Gestión de registros> Alarma**.

los **Alarma** se muestra la interfaz. Vea la Figura 7-2.

Figura 7-2 Alarma



No.	Room No.	Event State	Channel	Begin Time
1	12	Prevent Remove	1	2018-10-09 02:01:41
2	12	Prevent Remove	1	2018-09-27 14:55:21
3	12	Prevent Remove	1	2000-01-08 14:13:18
4	12	Prevent Remove	1	2000-01-01 00:14:32
5	11	Menace	1	2000-01-01 00:00:56
6	11	Menace	1	2000-01-01 00:00:40
7	11	Door Magnetism	5	2000-01-01 00:00:06

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

7.3 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**.

los **desbloquear** se muestra la interfaz. Vea la Figura 7-3.

Figura 7-3 Desbloqueo

No.	Unlock Type	Room No.	Username	Card No.	Unlock Result	Unlock Time
1	Card Unlock	201	mm	bbc66660	Succeeded	2018-10-10 10:49:34
2	Card Unlock	201	mm	bbc66660	Succeeded	2018-10-09 01:41:35
3	Card Unlock			bbc66660	Failure	2018-10-09 01:41:28
4	Card Unlock	201	mm	bbc66660	Succeeded	2018-10-09 01:31:02
5	Password Unlock				Succeeded	2018-09-29 13:50:46
6	Password Unlock	88888			Failure	2018-09-27 14:55:59
7	Password Unlock	8001			Failure	2018-09-27 10:27:51
8	Self Password Unlock	Center			Failure	2018-09-27 10:18:56
9	Password Unlock	11			Failure	2000-01-01 00:00:59

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

7.4 Registro

Puede ver varios registros del sistema, incluido el sistema, el registro, la configuración, la cuenta y la seguridad.

Paso 1 Seleccione **Gestión de registros > Registro**.

los **Iniciar sesión** se muestra la interfaz. Vea la Figura 7-4.

Figura 7-4 Registro

No.	Record Time	Event
1	2018-10-10 11:20:05	Save Config
2	2018-10-10 11:19:54	Save Config
3	2018-10-10 11:19:11	Save Config
4	2018-10-10 11:19:11	Save Config
5	2018-10-10 11:18:27	Save Config
6	2018-10-10 11:18:10	Save Config
7	2018-10-10 11:02:16	Save Config
8	2018-10-10 11:01:43	Start
9	2018-10-10 11:00:49	Reboot
10	2018-10-10 11:00:49	Clear Record

Paso 2 Configure el intervalo de tiempo, seleccione el tipo de registro que necesita y haga clic en **Buscar**.

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