Villa VTO

Manual de usuario

V1.0.0

Prefacio

General

Este manual presenta el funcionamiento de la interfaz web de la estación de villa (VTO).

Las instrucciones de seguridad

La siguiente categoriz Las palabras de señalización con significado definido pueden aparecer en el Manual.

Palabras de advertencia	Sentido
 PRECAUCIÓN	Indica un riesgo potencial que, si no se evita, podría ocasionar 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	Revisión de contenido	Fecha de lanzamiento
V1.0.0	Primer lanzamiento	Abril 2020

Sobre el manual

- El manual es solo de referencia. Si hay inconsistencia entre el Manual y el producto real, prevalecerá el producto real.
- No somos responsables de ninguna pérdida causada por las operaciones que no cumplan con el Manual.
- El Manual se actualizará 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 al cliente para obtener el último programa y la documentación complementaria.
- Todavía puede haber desviación en los datos técnicos, descripción de funciones y operaciones, o errores en la impresión. Si hay alguna duda o disputa, 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 compañías en el Manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, póngase en contacto con el proveedor o con el servicio al cliente si se produce algún problema al utilizar el dispositivo.
- Si existe alguna incertidumbre o controversia, consulte nuestra explicación final.

Importantes salvaguardas y advertencias

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

Requisito de funcionamiento

- No coloque ni instale el dispositivo en un área expuesta a la luz solar directa o cerca del dispositivo generador de calor.
- No instale el dispositivo en un área húmeda, polvorienta o fuliginosa.
- Mantenga su instalación horizontal o instálela en lugares estables y evite que se caiga.
- No gotee ni salpique líquidos sobre el dispositivo; no coloque sobre el dispositivo nada que esté lleno de líquidos, para evitar que fluyan líquidos al dispositivo.
- Instale el dispositivo en lugares bien ventilados; No bloquee la abertura de ventilación.
- Use el dispositivo solo dentro del rango de entrada y salida nominal.
- No desmonte el dispositivo arbitrariamente.
- 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) requeridos por la región donde se utilizará el dispositivo.
- Use una fuente de alimentación que cumpla con los requisitos de SELV (voltaje extra bajo de seguridad) y suministre energía con voltaje nominal que se ajuste a 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

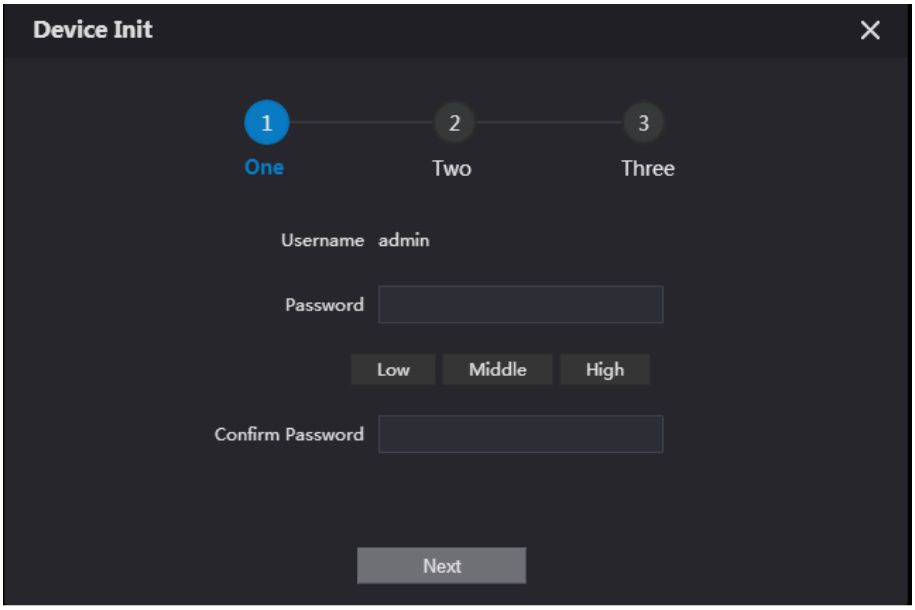
1 inicialización

Para iniciar sesión por primera vez o después de restablecer el VTO, debe inicializar la interfaz web. La dirección IP predeterminada de la VTO es 192.168.1.108, y asegúrese de que la PC esté en el mismo segmento de red que la 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



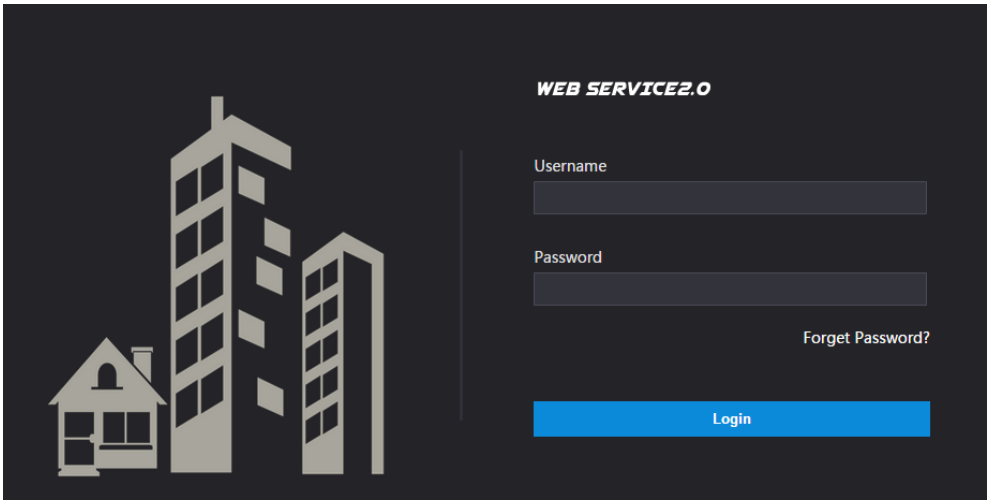
Paso 3 Ingrese y confirme la contraseña, y luego haga clic **Próximo.**

Paso 4 Se muestra la interfaz de configuración de correo electrónico. Selecciona el **Email** casilla de verificación y luego ingrese su dirección de correo electrónico. Esta dirección de correo electrónico se puede usar para restablecer la contraseña. Hacer clic **Próximo.**

Paso 5 La inicialización tuvo éxito.

Paso 6 Hacer clic **OKAY.**

Figura 1-2 Interfaz de inicio de sesión



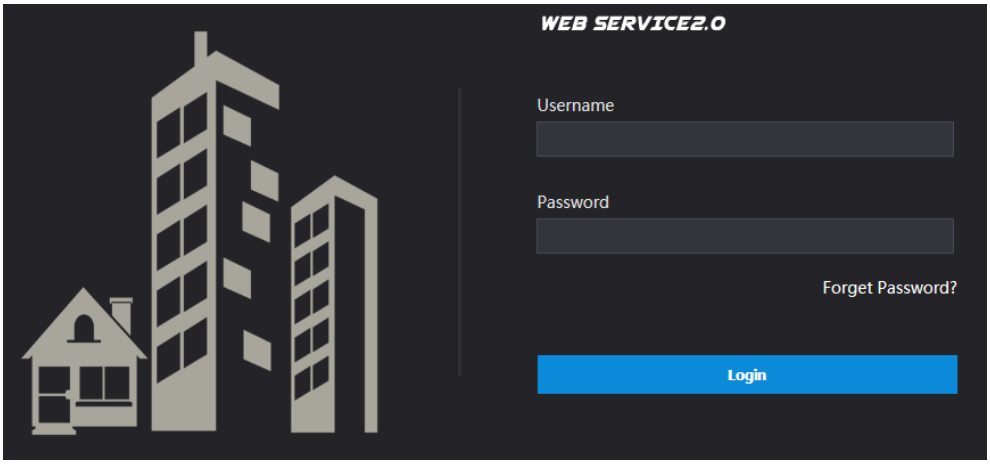
2 Interfaz de inicio de sesión

2.1 Iniciar sesión

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

Paso 1 Ingrese la dirección IP de VTO en la barra de direcciones del navegador y luego presione **Entrar.**

Figura 2-1nterfaz de inicio de sesión

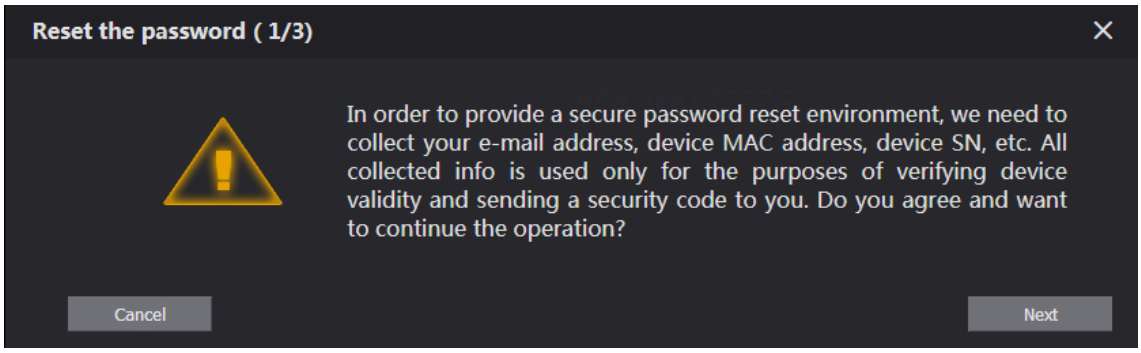


Paso 2 Ingrese "admin" como nombre de usuario, luego la contraseña que estableció durante la inicialización, y luego hacer clic **Iniciar sesión.**

2.2 2.2Restableciendo Contraseña

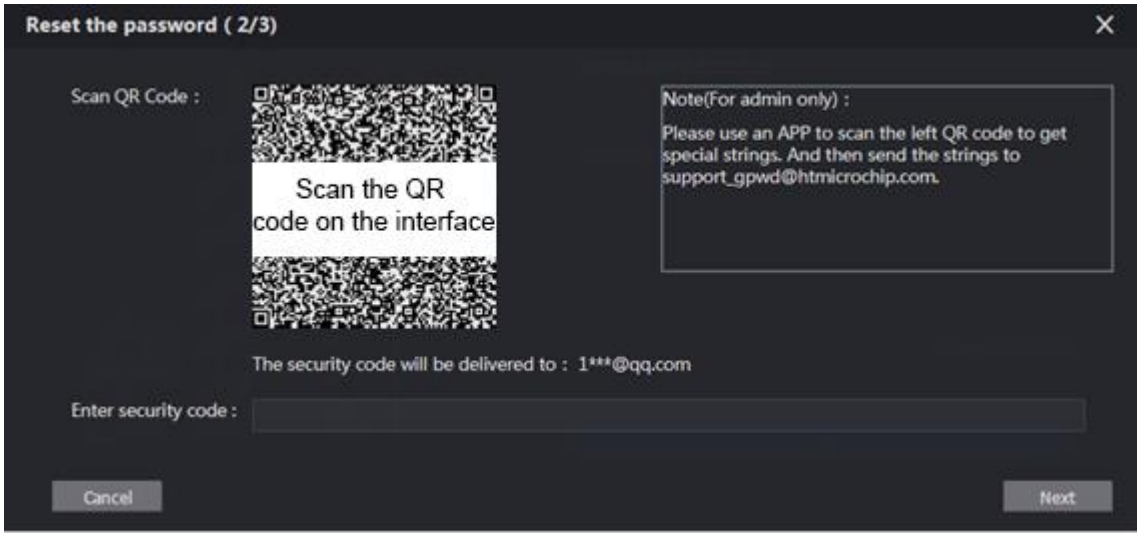
Paso 1 En la interfaz de inicio de sesión (Figura 2-1), haga clic en **¿Se te olvidó tu contraseña?.**

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



Paso 2 Hacer clic **Próximo.**

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



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, póngase en contacto con el proveedor o con el servicio al cliente para obtener ayuda.
- Para obtener nuevamente el código de seguridad, actualice la interfaz del código QR.
- Use el código de seguridad dentro de las 24 horas posteriores a su recepción. De lo contrario, se invalidará.
- Si se ingresa un código de seguridad incorrecto 5 veces seguidas, esta cuenta se bloqueará durante 5 minutos. Hacer clic **Próximo,** y luego el **Restablecer la contraseña (3/3)** se muestra el cuadro de diálogo.

Paso 4

Paso 5 Establezca y confirme la nueva contraseña como se 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

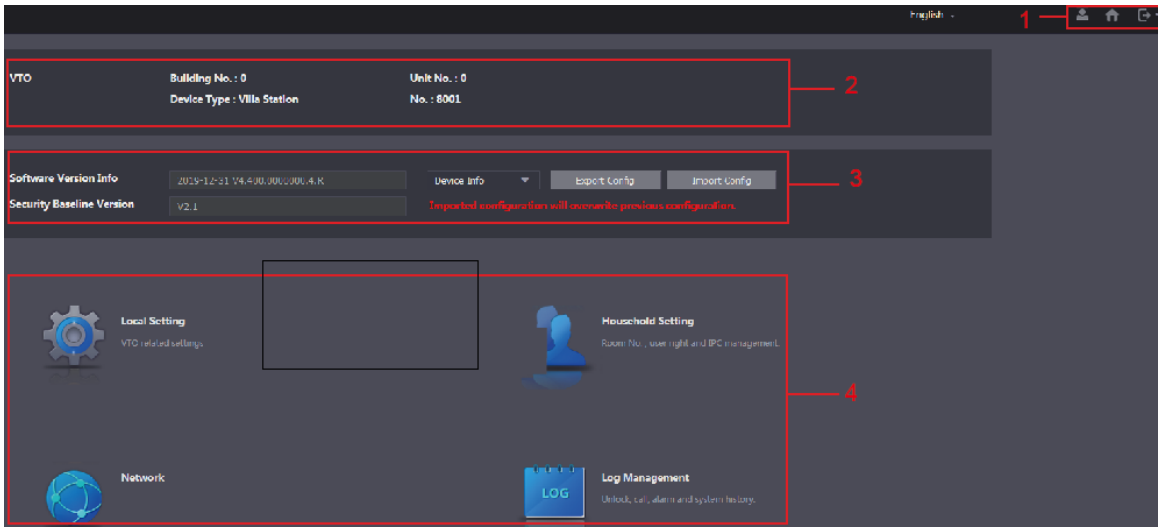


Tabla 3-1 Introducción a la interfaz principal

No.	Función	Descripción
1	Función general	• Hacer clic para cambiar la contraseña y tu correo electrónico habla a. • Hacer clic para ir a la interfaz principal. • Hacer clic para cerrar sesión, reinicie el VTO o restaure el VTO a la configuración de fábrica.
2	Información VTO	Puede ver la información general de la VTO, incluido el número de edificio, la unidad, el tipo de dispositivo y el número de VTO.
3	Información del sistema	Puede ver la versión de software, la versión de MCU y la versión de referencia de seguridad.
4 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 5	Área de funciones	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 el audio, la contraseña de acceso, la hora del sistema y la función de seguridad.

Operaciones generales:

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

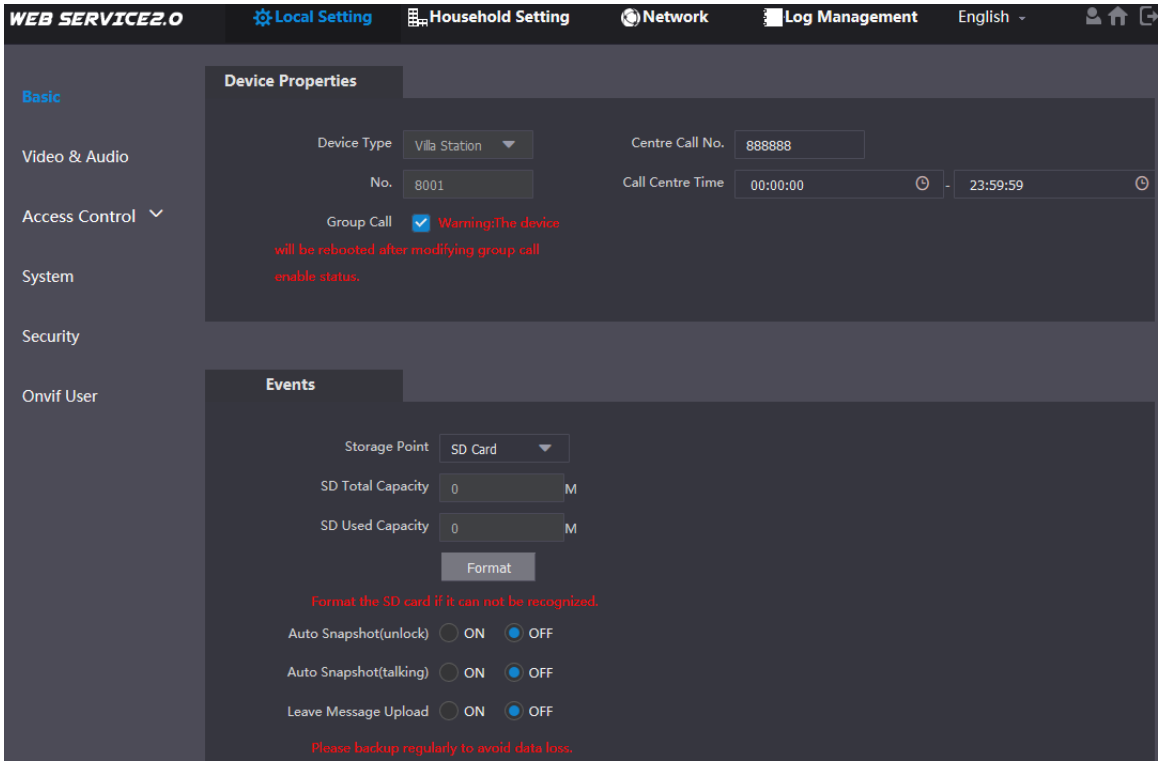
4.1 Básico

4.1.1 Propiedades y eventos del dispositivo

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

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

básica Figura



Paso 2 Configurar parámetros.

Tabla 4-1 Descripción del parámetro básico

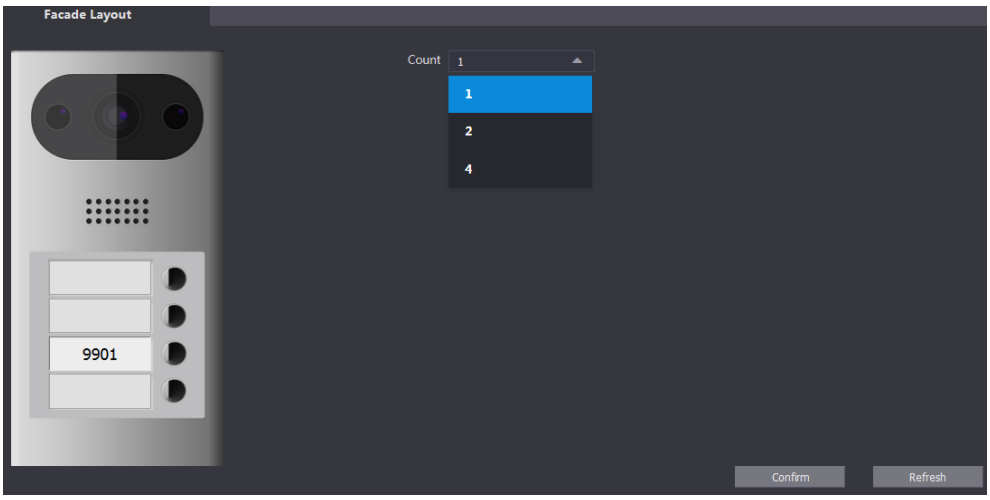
Parámetro	Descripción
Tipo de dispositivo	Mantener el valor predeterminado. • El número de edificio y el número de unidad solo están disponibles cuando otros servidores funcionan como servidor SIP. Consulte "6.2 Servidor SIP".

Parámetro	Descripción
	• La estación de valla se usa normalmente cuando otros servidores funcionan como servidor SIP.
Centro de llamadas No.	Configure el número del centro de administración, y puede llamar al centro de administración en cada VTO o VTH en la red. El número predeterminado es 888888.
Hora del centro de llamadas	Período de tiempo en el que puede llamar al centro de gestión.
VTO No.	El número de VTO se puede usar para diferenciar cada VTO, y normalmente se configura de acuerdo con la unidad o el número de edificio. Puede agregar dispositivos VTO al servidor SIP con sus números.
Punto de almacenamiento	Todas las instantáneas se guardarían en la tarjeta SD en la estación de villa automáticamente. • Instantánea automática (desbloqueo) Seleccione **EN** para habilitar esta función, y luego el sistema toma una instantánea cada vez que se desbloquea la puerta. • Instantánea automática (hablando) Seleccione **EN** para habilitar esta función, y luego el sistema toma una instantánea cada vez que el usuario VTH responde una llamada del VTO. • Mensajes Seleccione **EN** para habilitar esta función, y luego el sistema carga los mensajes de los visitantes a la tarjeta SD automáticamente. • Si hay una tarjeta SD en el VTH principal, los mensajes de la izquierda se guardarán en la tarjeta SD del VTH principal de forma predeterminada. • Para recibir el mensaje, el **Tiempo de mensaje VTO** debe configurarse para que sea mayor que 0. Consulte el manual del usuario de VTH.

Paso 3 Hacer clic **Confirmar.**

4.1.2 Diseño de fachada (solo para VTO3211D)

Si selecciona 1 del **Contar** lista desplegable, solo el tercer botón será válido; si selecciona 2, solo los botones segundo y cuarto serán válidos; y si selecciona 4, los cuatro botones serán válidos.

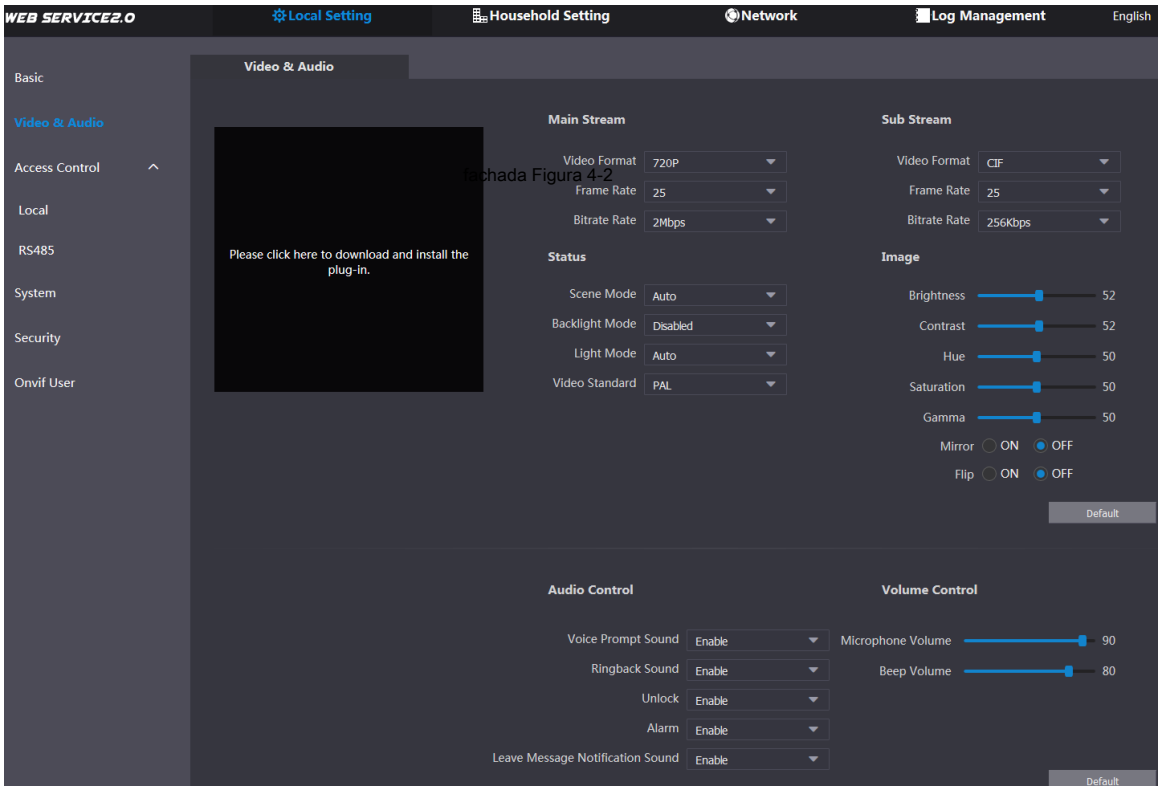


4.2 4.2Audio video

Esta sección presenta cómo configurar el formato y la calidad del video capturado por VTO, y la configuración de control de audio.

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

Figura 4-3 Video y audio



fachada Figura 4-2

Paso 2 Configure los parámetros, y estas configuraciones entrarán en vigencia de inmediato.

Tabla 4-2 Descripción del parámetro de video

Parámetro		Descripción
Convencional	Formato de video	Seleccione la resolución de video de **720P, WVGA,** y **D1**
	Tasa de formato	Configure el número de cuadros en 1 segundo. Puedes seleccionar de **1** a **25** debajo **CAMARADA,** y **1** a **30** debajo **NTSC** vídeo

Parámetro		Descripción
		estándar. Cuanto mayor sea el valor, más suave será el video.
	Bitrate	Configure la cantidad de datos que transmitió 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, D1,** y **1080P.**
	Tasa de formato	Configure el número de cuadros en 1 segundo. Puedes seleccionar de **1** a **25** debajo **CAMARADA,** y **1** a **30** debajo **NTSC** estándar de video Cuanto mayor sea el valor, más suave será el video.
	Bitrate	Configure la cantidad de datos que transmitió en 1 segundo. Cuanto mayor sea el valor, mejor será la calidad del video.
Estado	Modo escena	Ajuste el video para adaptarse a diferentes escenarios. Puedes seleccionar de **Automático, soleado, noche** y **Discapacitado.** Es **Automático** por defecto.
	Modo día / noche	Puedes seleccionar de **Deshabilitado, Automático, Soleado** o **Noche.**
	Modo de luz de fondo	Puede seleccionar entre los siguientes modos: • **Discapacitado:** Sin luz de fondo. • **BLC:** La cámara obtiene una imagen más clara de las áreas oscuras. en el blanco al disparar contra la luz. • **WDR:** El sistema atenúa las áreas brillantes y compensa áreas oscuras para garantizar la claridad de toda el área. • **HLC:** El sistema restringe las áreas brillantes y reduce tamaño de halo para atenuar el brillo general.
	Modo de luz	Hay cuatro modos de luz: NO, NC, Automático y Programado. Seleccione según sea necesario.
	Estándar de video	Seleccionar de **CAMARADA** o **NTSC** De acuerdo con su dispositivo de visualización.
Imagen	Brillo	Cambia el valor para ajustar el brillo de la imagen. Cuanto mayor sea el valor, más brillante será la imagen y más pequeña será la más oscura. La imagen puede ser borrosa si el valor es 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 menor será el valor. Si el valor es demasiado grande, el área oscura sería demasiado oscura y el área brillante sería más fácil de sobreexponer. La imagen puede ser 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.
	Saturación	Hace que el color sea más profundo o más claro. Cuanto mayor sea el valor, más profundo será el color y más bajo será el 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,

Parámetro		Descripción
		cuanto más brillante sea la imagen, y más pequeña será la más oscura.
	Espejo	Seleccione **En,** y luego la imagen se muestra con el lado izquierdo y derecho invertidos.
	Dar la vuelta	Seleccione **En,** y luego la imagen se muestra al revés.
Control de audio	Seleccione **Habilitar** o **Discapacitado** para encender o apagar cada sonido.	
Control del volumen	Volumen del micrófono	Ajuste el valor, y cuanto mayor sea el valor, más alto será el volumen del micrófono VTO.
	Volumen del pitido	Ajuste el valor, y cuanto mayor sea el valor, más alto será el volumen del sistema.

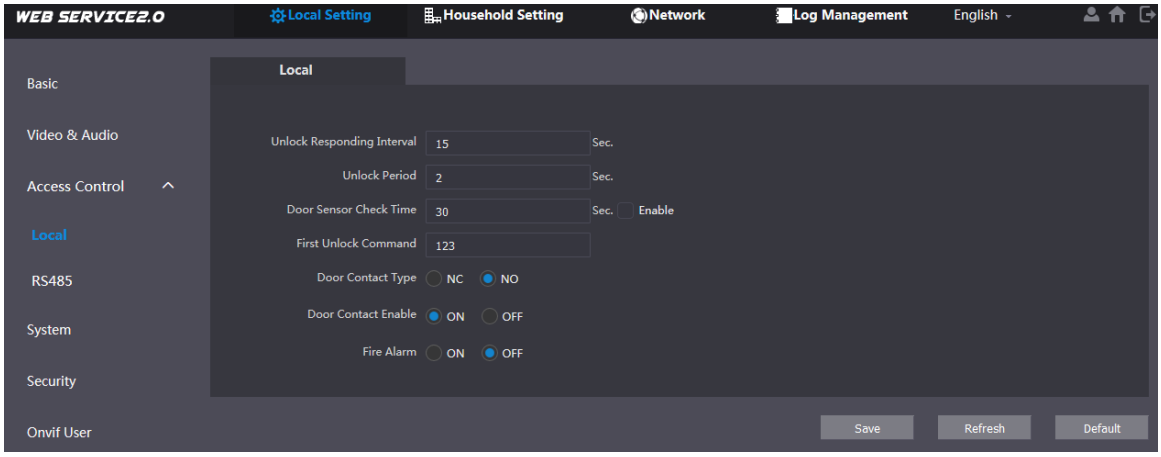
4.3 Control de acceso

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.

4.3.1 Local

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

local 4-Figura



Paso 2 Configurar parámetros.

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

Parámetro	Descripción
Desbloquear intervalo de respuesta	El intervalo de tiempo para desbloquear nuevamente después del desbloqueo anterior, y la unidad es la segunda.
Periodo de desbloqueo	La cantidad de tiempo durante la cual el bloqueo permanece abierto después del desbloqueo, y la unidad es la segunda.
Tiempo de comprobación del sensor de puerta	Si ha instalado el sensor de puerta, debe 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. • Selecciona el **Habilitar** casilla de verificación, y la puerta no se bloqueará

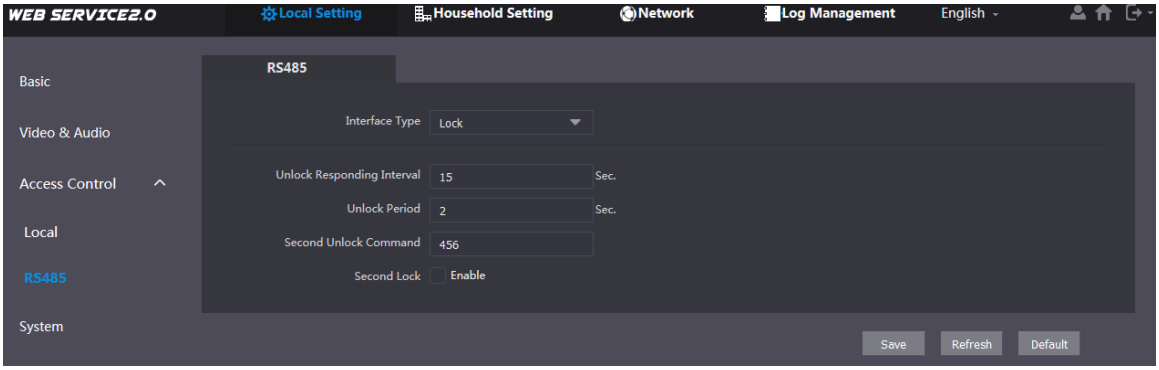
Parámetro	Descripción
	hasta que el sensor de la puerta entre en contacto. Si no selecciona el **Habilitar** casilla de • verificación, la puerta será bloqueado después de la **Periodo de desbloqueo** acabados.
Primer comando de desbloqueo	Puede conectar un teléfono de terceros, como un teléfono SIP, a su VTO y usar el comando para abrir la puerta de forma remota.
Tipo de contacto de puerta	**Seleccione CAROLINA DEL NORTE o NO De acuerdo con la cerradura que utiliza.**
Contacto de puerta habilitado	Después de habilitar el contacto de la puerta, si las puertas no están bloqueadas en cierto período, se activarán las alarmas y los mensajes de alarma se enviarán al monitor interior (VTH).
Alarma de incendios	Seleccione según sea necesario.

Paso 3 Hacer clic **Salvar.**

4.3.2 RS-485

Puede configurar el intervalo de respuesta de desbloqueo, el período de desbloqueo y el segundo comando de desbloqueo.

Figura 4-5 RS-485

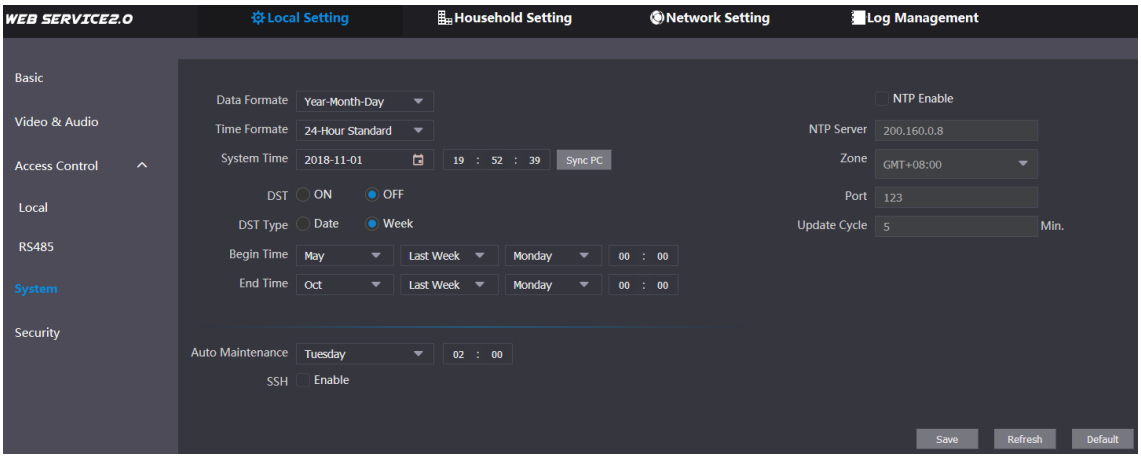


4.4 Sistema

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 4-6 Sistema



Paso 2 Configurar parámetros.

Tabla 4-4 Descripción de los parámetros del sistema

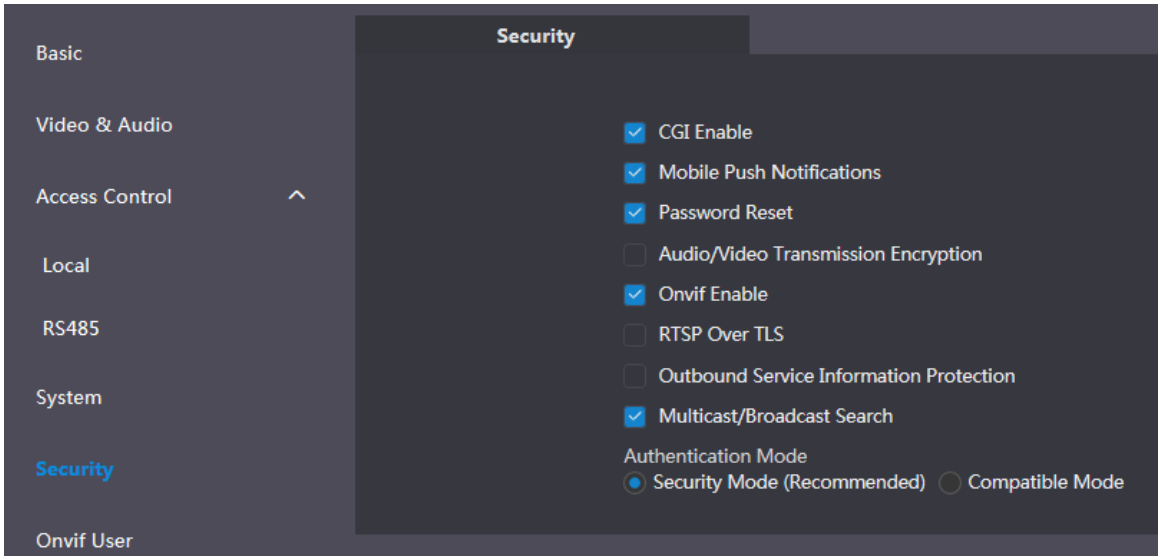
Parámetro	Descripción
Formato de fecha	Puede seleccionar entre Año-Mes-Día, Mes-Día-Año y Día-Mes-Año.
Formato de tiempo	Configure el formato de hora, y puede seleccionar entre **12 horas** o **24 horas.**
Zona horaria	Seleccione una zona horaria según sea necesario.
Hora del sistema	Configure la fecha, hora y zona horaria del sistema VTO. No cambie la hora del sistema arbitrariamente; puede causar problemas en la búsqueda de videos y publicación de instantáneas o avisos. Antes de cambiar la hora del sistema, apague la grabación de video o la instantánea automática.
Sincronizar PC	Haga clic para sincronizar la hora del sistema VTO y la hora del sistema de la PC.
DST	Seleccione **EN** para habilitar el horario de verano.
Tipo de horario de verano	Seleccione **Fecha** para definir una fecha específica para el horario de verano o seleccione **Semana** para ello.
Hora de inicio	Configure la hora de inicio y la hora de finalización para el horario de verano.
Hora de finalización	
NTP habilitado	Seleccione la casilla de verificación para habilitar la sincronización NTP.
Servidor NTP	Ingrese el nombre de dominio del servidor NTP.
Puerto	El número de puerto del servidor NTP.
Ciclo de actualización	El intervalo de tiempo durante el cual el VTO sincroniza el tiempo con el servidor NTP, y es de 30 minutos como máximo.
Mantenimiento	Seleccione el día y la hora para el mantenimiento automático, y el VTO se reiniciará entonces.
SSH	Selecciona el **Habilitar** casilla de verificación, y luego puede conectar dispositivos de depuración al VTO a través del protocolo SSH.

Paso 3 Hacer clic **Salvar.**

4.5 4.5Seguridad

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

Figura 4-7 seguridad



Paso 2 Configurar parámetros.

Tabla 4-5 Descripción del parámetro de seguridad

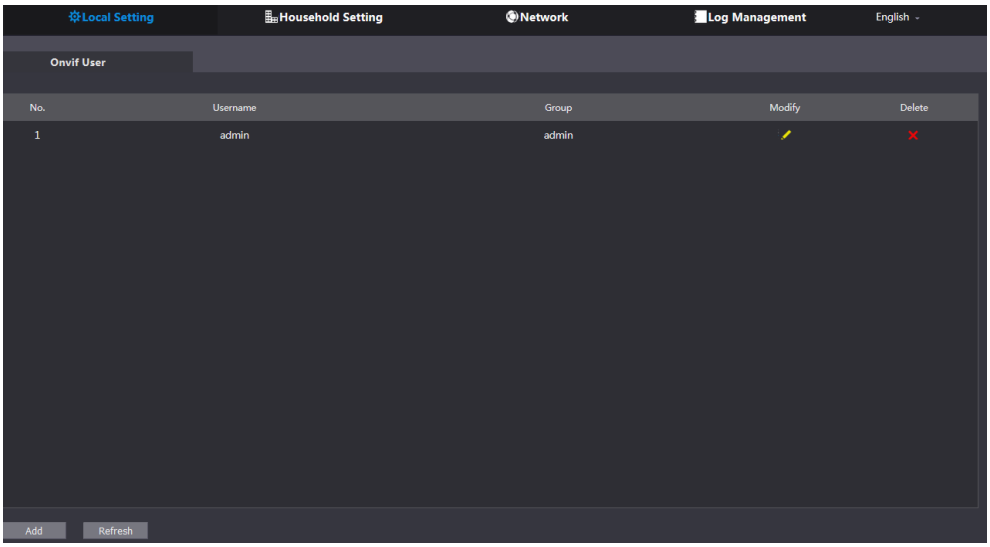
Parámetro	Descripción
Habilitar CGI	Seleccione la casilla de verificación para habilitar, y luego puede usar el comando CGI.
Notificación de inserción móvil	Después de habilitar esto, las nitificaciones se enviarán a la aplicación instalada en su teléfono.
Restablecimiento de contraseña	Seleccione la casilla de verificación para habilitar, y luego el restablecimiento de contraseña está disponible.
Cifrado de transmisión de audio / video	Si ha habilitado esto, la transmisión de audio y video se cifrará.
Onvif Enable	Después de habilitar Onvif, los videos de dispositivos fabricados por otras compañías se pueden mostrar en la interfaz web de la estación de puerta.
RTSP sobre TLS	RTSP es la abreviatura de protocolo de transmisión en tiempo real, es un protocolo de control de red diseñado para su uso en sistemas de entretenimiento y comunicaciones para controlar servidores de transmisión de medios. El protocolo se utiliza para establecer y controlar sesiones de medios entre puntos finales.
Información de servicio saliente	Una vez habilitado, la información de la contraseña del servicio no se puede enviar a otros.
Multicast / Broadcast Search	Si ha deshabilitado esto, las herramientas de configuración de VDP no pueden encontrar este dispositivo.
Modo de autenticación	Hay dos modos: Modo de seguridad (recomendado) y modo compatible.

Paso 3 Hacer clic **Salvar** ahorrar.

4.6 Usuario de Onvif

El usuario de Onvif es solo para ingenieros. Puede agregar, eliminar y modificar la información del usuario de ONVIF. El nombre de usuario de Onvif es admin por defecto.

Figura 4-8 Usuario de Onvif



5 Configuración del hogar

Este capítulo trata sobre las configuraciones de las estaciones de puerta (VTO) que funcionan como servidores SIP (consulte 6.2 Servidor SIP). Sabrá cómo agregar, modificar y eliminar dispositivos VTO, VTH, VTS e IPC, y cómo enviar mensajes desde el servidor SIP a otros dispositivos VTO y VTH. Si está utilizando otros servidores como servidor SIP, consulte el manual correspondiente para la configuración detallada.

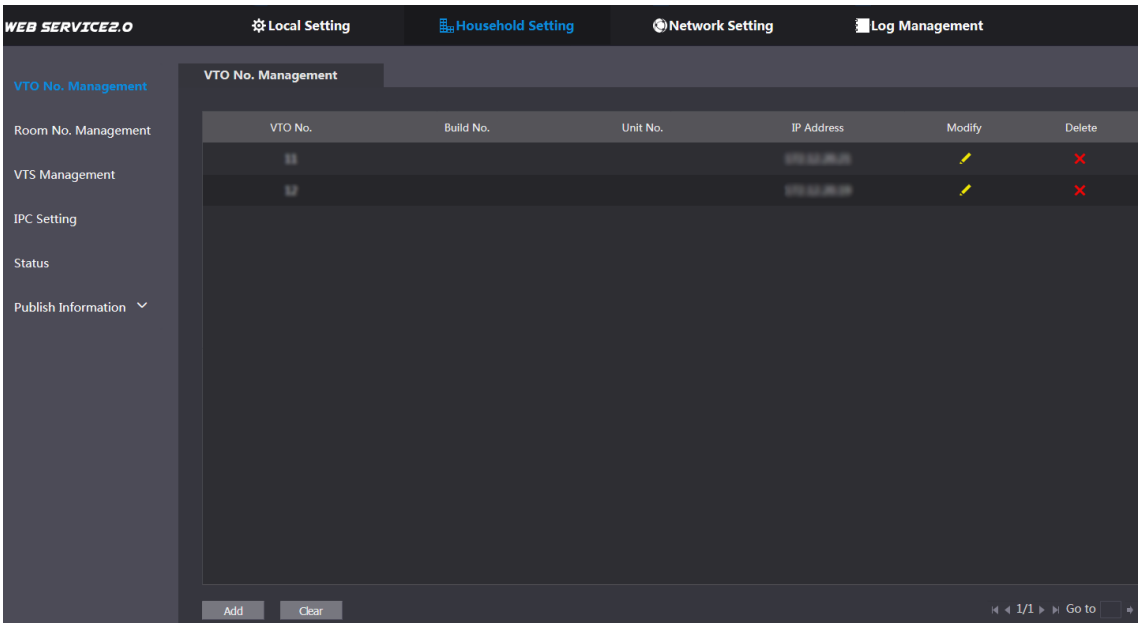
5.1 VTO No. Gestión

5.1.1 Agregar VTO

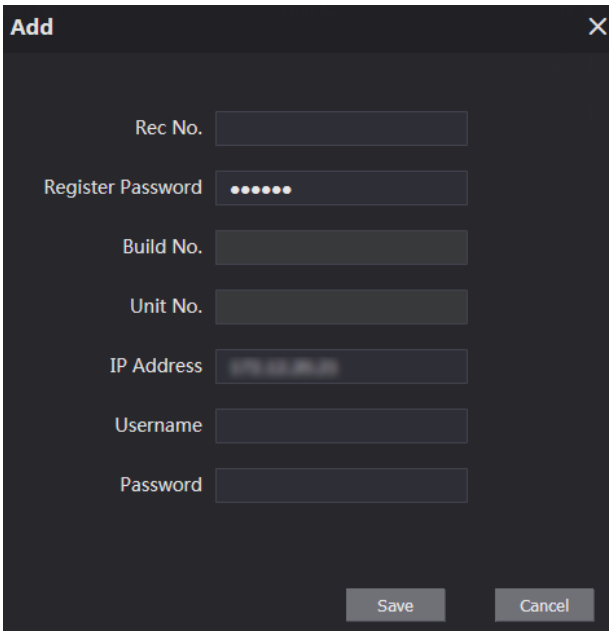
Puede agregar VTO al servidor SIP, y luego puede hacer videollamadas entre los videoporteros que están conectados al mismo servidor SIP.

Paso 1 Inicie sesión en la interfaz web del servidor SIP y luego seleccione **Configuración del hogar> VTO No. Gestión.**

VTO No. gestión Figura 5-1



Paso 2 Hacer clic **Añadir.**



Paso 3 Configura los parámetros.

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".
Registrarse contraseña	Mantener el valor por defecto.
Build No.	Disponible solo cuando otros servidores funcionan como servidor SIP.
Numero de unidad.	Figura 5-2
Dirección IP	La dirección IP de la VTO de destino.
Nombre de usuario	El nombre de usuario y la contraseña para la interfaz WEB de la VTO de destino.
Contraseña	

Paso 4 Hacer clic **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 Sobre el **VTO No. Gestión** interfaz (Figura 5-1), haga clic en  .

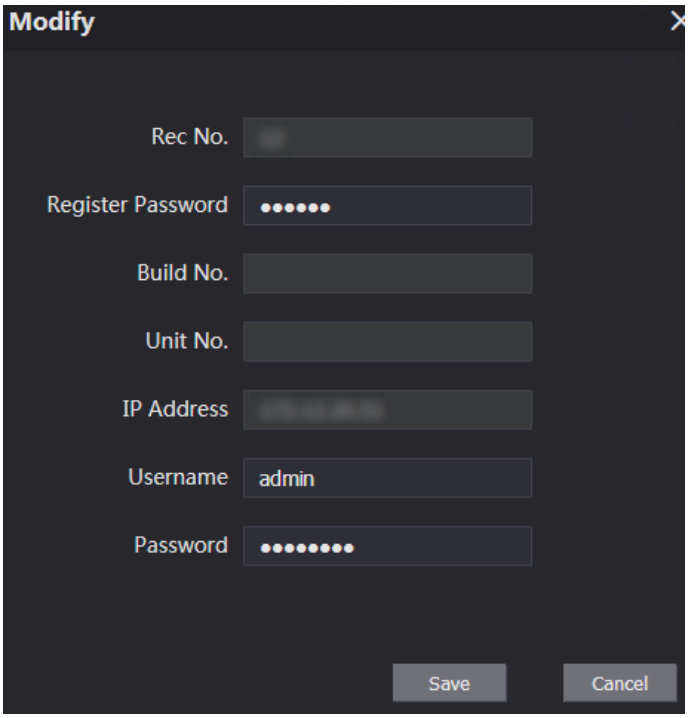


Figura 5-3

Paso 2 Puedes modificar el **Número de registro, nombre de usuario, y Contraseña.**

Paso 3 Hacer clic **Salvar.**

5.1.3 Eliminar VTO

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

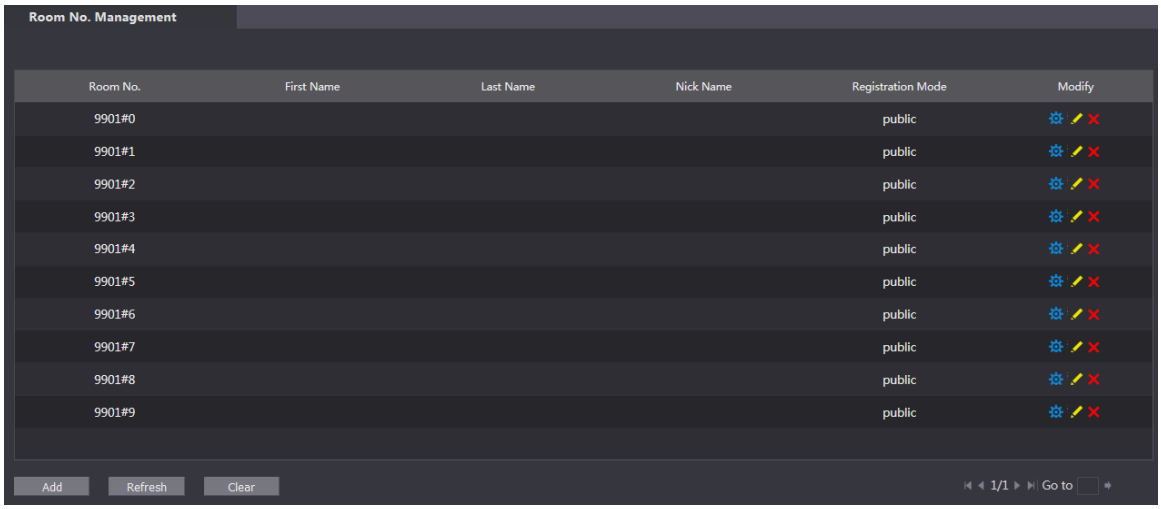
Sobre el **VTO No. Gestión** interfaz (Figura 5-1), haga clic en eliminar VTO uno por uno; y hacer clic **Claro** para eliminar todo el VTO.

5.2 Sala No. Gestión

5.2.1 Agregar número de habitación

Puede agregar los números de habitación planificados al servidor SIP y luego configurar los números de habitación en los dispositivos VTH para que pueda conectarlos a la red.

Paso 1 Inicie sesión en la interfaz web del servidor SIP y luego seleccione **Configuración del hogar> Sala No. Gestión.**



Paso 2 Agregar números de habitación.

1) Haga clic **Añadir.**

Figura 5-3 Agregar números de habitación

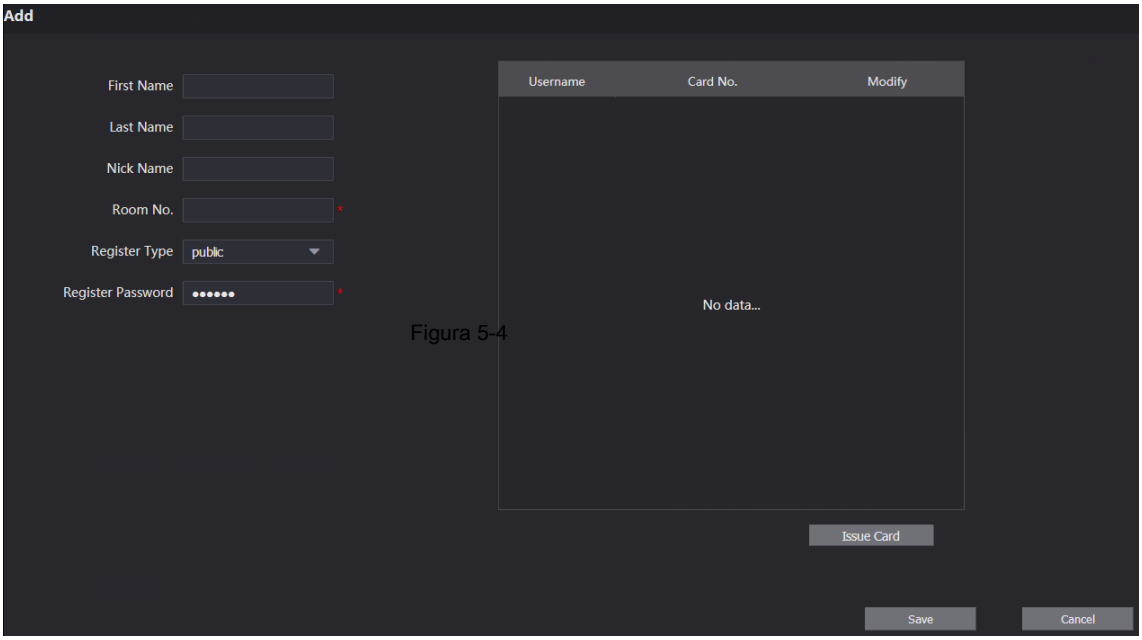


Figura 5-4

2) Configurar la información de la sala.

Tabla 5-2 Información de la sala

Parámetro	Descripción
Nombre de pila	Ingrese la información que ayuda a diferenciar cada habitación.
Apellido Apodo	
Habitación no.	El número de habitación que planeaste.
Tipo de registro	**Seleccione público, y local está reservado para uso futuro.**
Registrarse contraseña	Mantener el valor predeterminado.

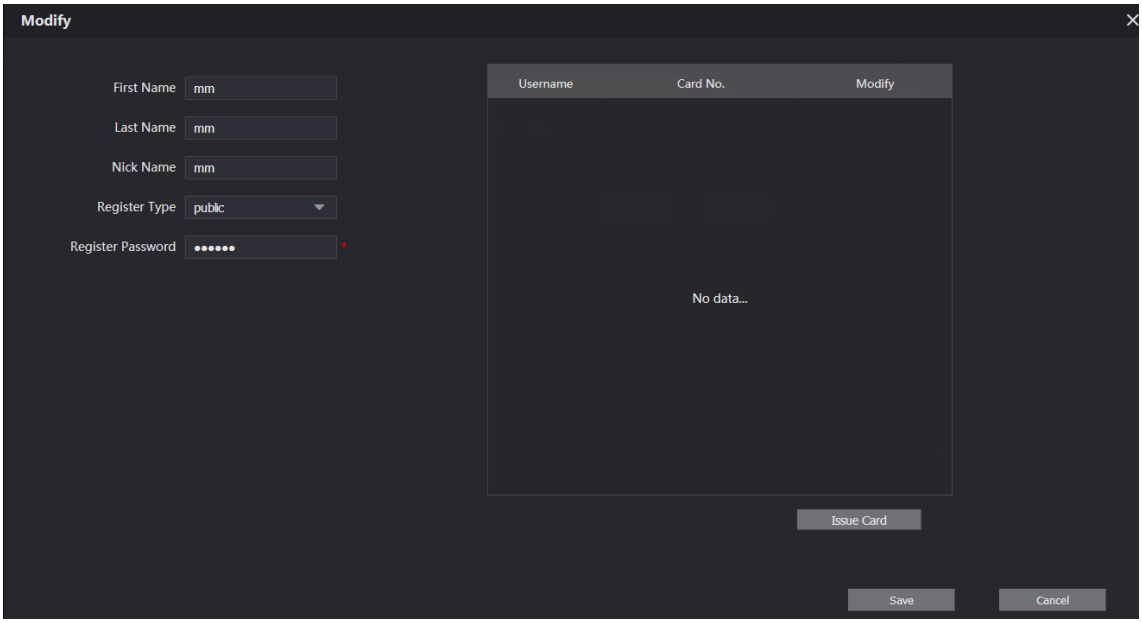
3) Haga clic **Salvar.**

Se muestran los números de habitación agregados. Hacer clic para modificar la información de la sala, haga clic en para ver el número de serie del dispositivo y haga clic en **para eliminar una habitación Hacer clic Actualizar a ver el último estado y hacer clic Claro para borrar todos los números de habitación.**

5.2.2 Modificación del número de habitación

Paso 1 Sobre el **Sala No. Gestión** interfaz (Figura 5-4), haga clic en  .

Figura 5-6 Modificar el número de habitación



Paso 2 Puede modificar los nombres de la sala.

Paso 3 Hacer clic **Salvar.**

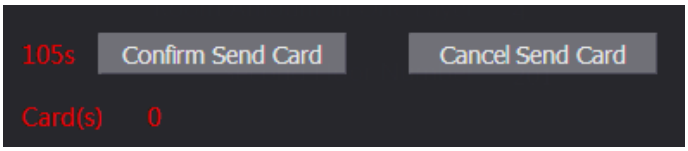
5.2.3 Emisión de tarjeta de acceso

Puede emitir la tarjeta a una habitación, y también puede configurar la tarjeta como la tarjeta principal, o configurar la tarjeta en el estado perdido. Las tarjetas principales se utilizan para emitir tarjetas para otras habitaciones.

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

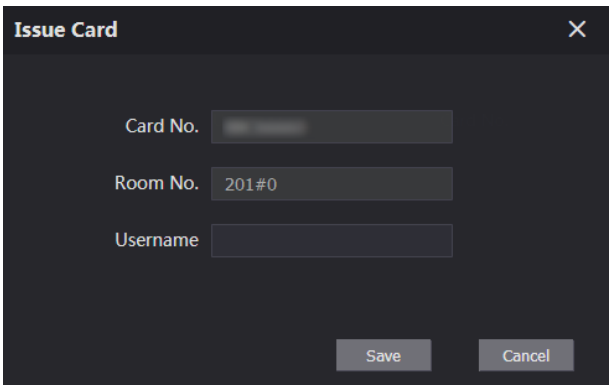
Se muestra el aviso de cuenta regresiva.

Figura 5-7 Aviso de cuenta regresiva



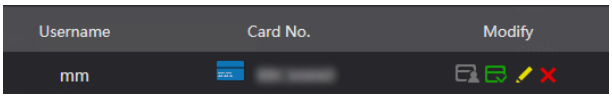
Paso 2 Pase la tarjeta que necesita ser autorizada en el VTO, y luego el **Tarjeta de emisión** se muestra el cuadro de diálogo.

Figura 5-8 Ficha de problemas



Paso 3 **Ingrese un nombre de usuario, haga clic Salvar, y luego haga clic Confirmar Enviar tarjeta en la cuenta regresiva** aviso (Figura 5-7).

Figura 5-9 Tarjeta de acceso emitida



Paso 4 Puede modificar la información de la tarjeta.

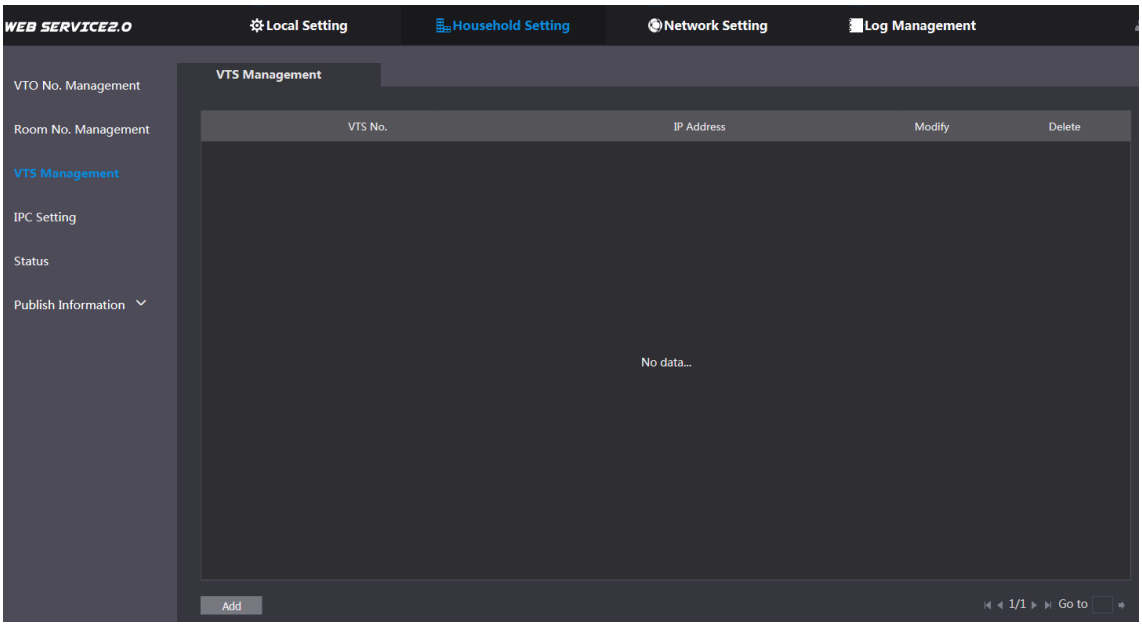
- Hacer clic para configurarlo en la tarjeta principal, y luego el icono se convierte en . La carta principal se puede usar para emitir tarjetas de acceso para esta sala en el VTO. Haga clic nuevamente para reanudar.
- Hacer clic para configurar la tarjeta en el estado perdido, y luego el ícono cambia a . La tarjeta bajo estado perdido no se puede usar 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 usar como centro de administración. Puede gestionar todos los videoporteros de la red, realizar o recibir videollamadas y realizar configuraciones básicas. Para más detalles, consulte el manual del usuario de VTS.

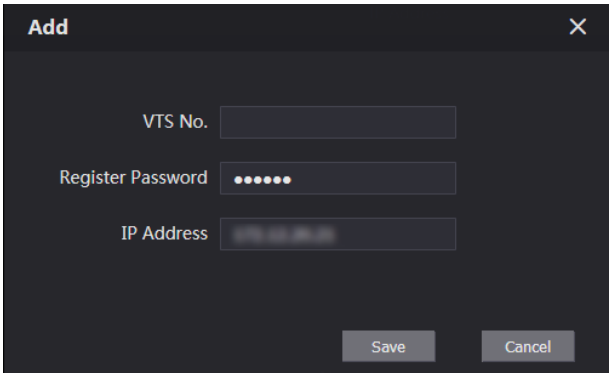
Paso 1 Inicie sesión en la interfaz web del servidor SIP y luego seleccione **Configuración del hogar> Gestión de VTS.**

Figura 5-10 Gestión VTS



Paso 2 Hacer clic **Añadir.**

Figura 5-11 Añadir VTS



Paso 3 Configure los parámetros y para 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.
Registrarse contraseña	Mantener el valor por defecto.
Dirección IP	La dirección IP del VTS de destino.

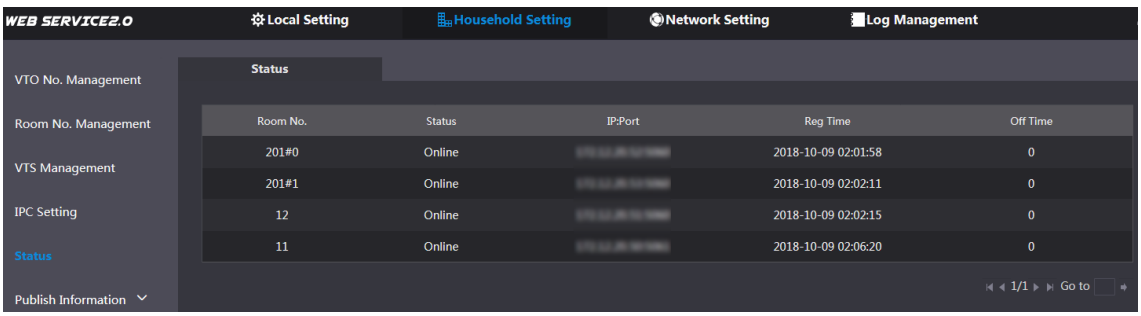
Paso 4 **Hacer clic Salvar, y luego se muestra el VTS agregado. Hacer clic** para modificar la dirección IP, y hacer clic borrar.

5.4 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 5-12. Estado



6 Configuración de red

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

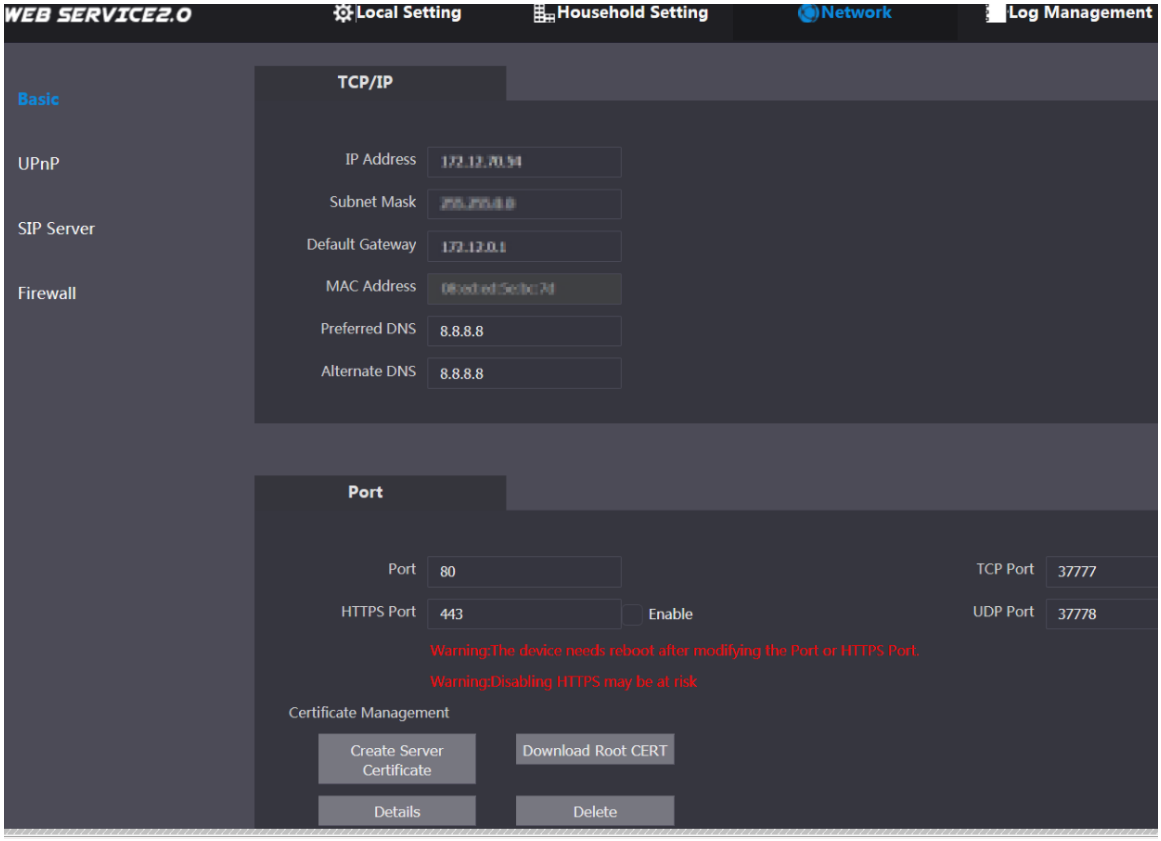
6.1 Básico

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 6-3 TCP / IP y puerto



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

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

6.1.2 Puerto

6.1.2.1 Crear certificado de servidor

Hacer clic **Crear certificado de servidor,** ingrese la información necesaria, haga clic **Salvar,** y luego la terminal se reiniciará.

6.1.2.2 Descarga del certificado raíz

Paso 1 Hacer clic **Descargue el certificado raíz.**

Paso 2 Seleccione una ruta para guardar el certificado en el cuadro de diálogo Guardar archivo.

Paso 3 Haga doble clic **Certificado de raíz** que ha descargado para instalar el certificado. Instalar en pc el certificado siguiendo las instrucciones en pantalla.

6.1.3 HTTPS

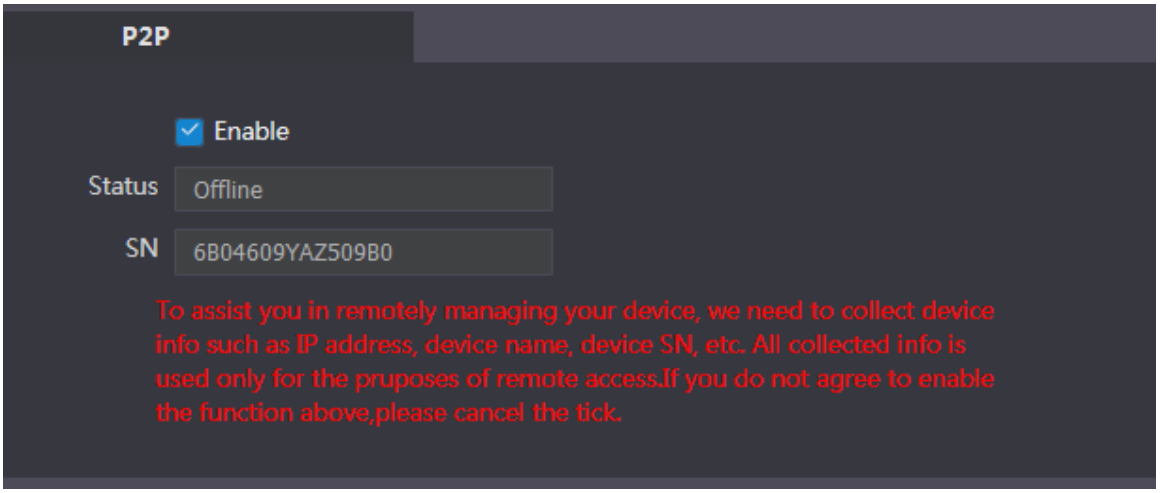
Selecciona el Habilitar casilla de verificación en Puerto HTTPS, y luego el VTO se reiniciará. Después de reiniciar, puede iniciar sesión en el VTO ingresando "https: // Dirección IP del VTO" en la barra de direcciones del explorador.

- Puede usar el valor predeterminado y también puede modificar el número de puerto según sea necesario.
- Cuando el puerto HTTPS está habilitado, puede ingresar https: // Dirección IP de VTO: número de puerto HTTPS / # / Iniciar sesión para iniciar sesión en la interfaz web; o puede ingresar http: // Dirección IP de VTO: número de puerto, y la dirección se cambiará automáticamente a https: // Dirección IP de VTO: número de puerto HTTPS / # / Iniciar sesión.

6.1.4 P2P

La red P2P es aquella en la que dos o más PC comparten archivos y acceden a dispositivos como impresoras sin requerir una computadora servidor o software de servidor por separado.

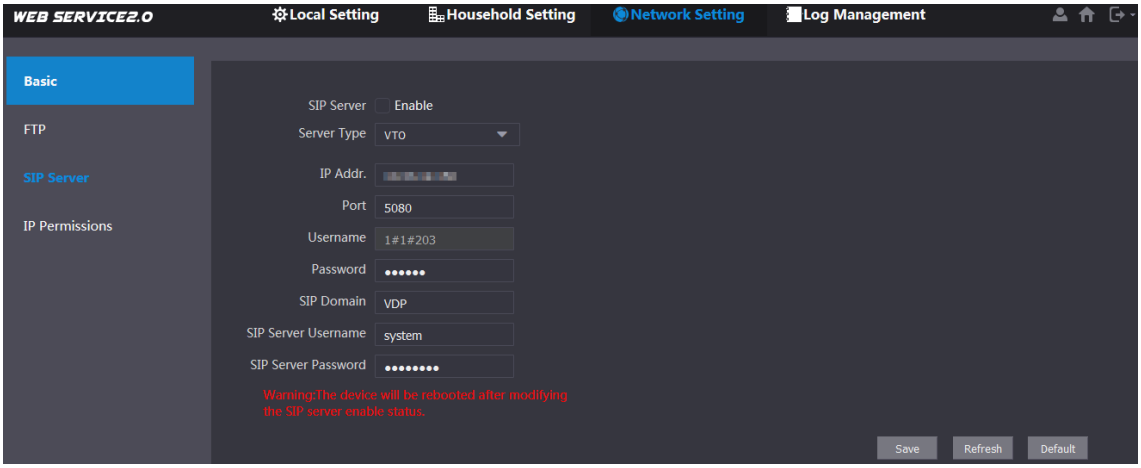
Figura 6-22 P2P



6.2 Servidor SIP

El servidor SIP se requiere en la red para transmitir el protocolo de intercomunicación, y luego todos los dispositivos VTO y VTH conectados al mismo servidor SIP pueden hacer videollamadas entre sí.

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

  El VTO se reiniciará y, después de reiniciar, puede agregar dispositivos VTO y VTH a este VTO. Vea 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 configurar** los parámetros.

Tabla 6-1 Configuración del servidor SIP

Parámetro	Descripción
Dirección IP	La dirección IP del VTO que funciona como servidor SIP.
Puerto	5060
Nombre de usuario	Mantener el valor predeterminado.
Dominio SIP de	
contraseña	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	

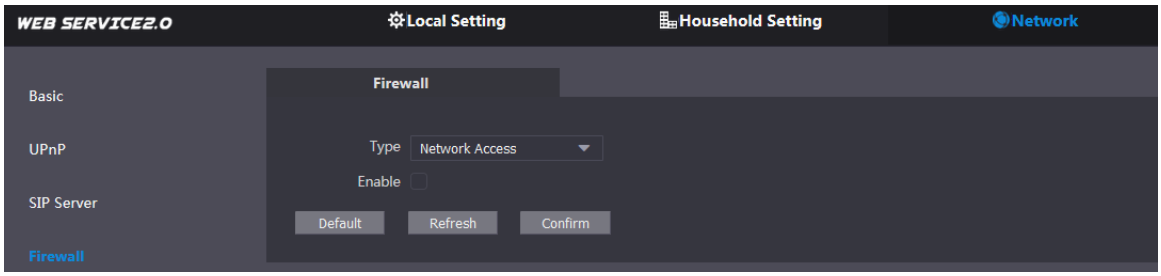
- **Si otros servidores funcionan como servidor SIP Seleccione el tipo de servidor que necesita en Tipo de servidor, y luego** vea el manual correspondiente para la configuración detallada.

Figura 6-3

6.3 Cortafuegos

El firewall es solo para ingenieros. Seleccione según sea necesario.

Figura 64 Cortafuegos



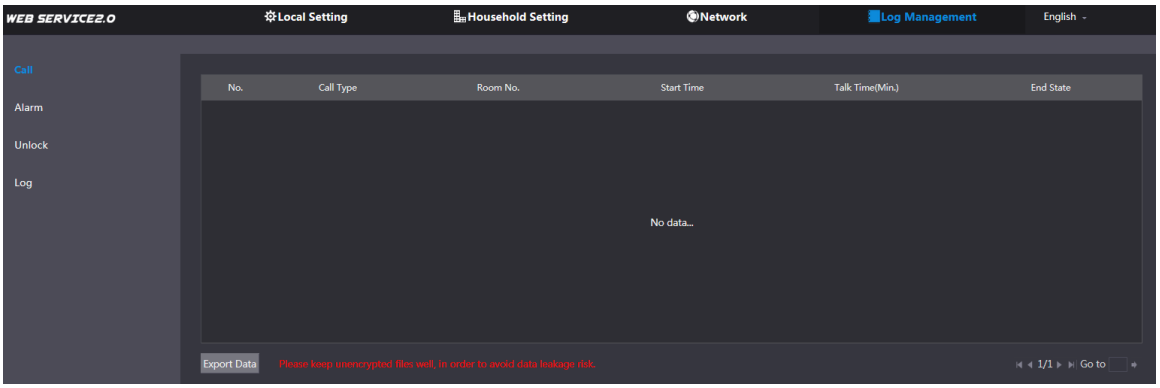
7 Gestión de registros

Puede ver el historial de llamadas, registros de alarmas, registros de desbloqueo y registros del sistema.

7.1 Llamada

Puede ver los registros de llamadas, incluidos los tipos de llamadas, los números de habitación, la hora de inicio, la hora de conversación y el estado final.

la figura 7-1ame a

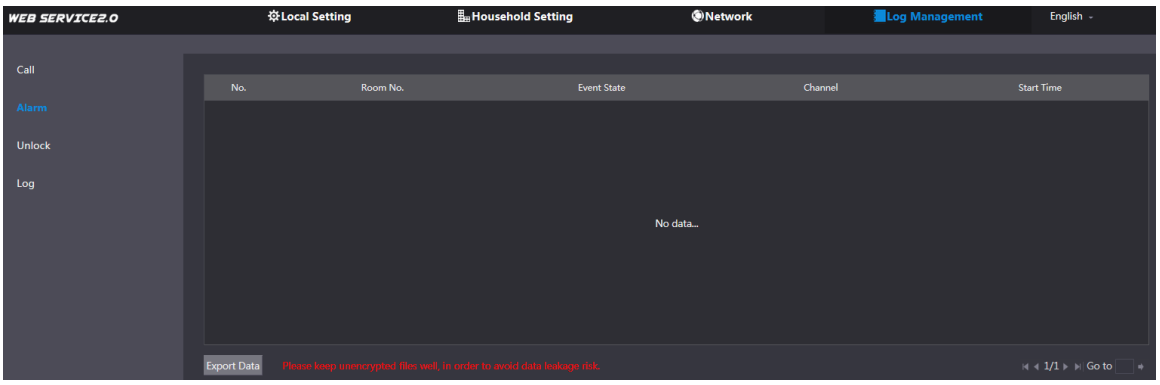


Hacer clic **Exportar datos** para exportar los registros a su PC.

7.2 Alarma

Puede ver y exportar registros de alarmas.

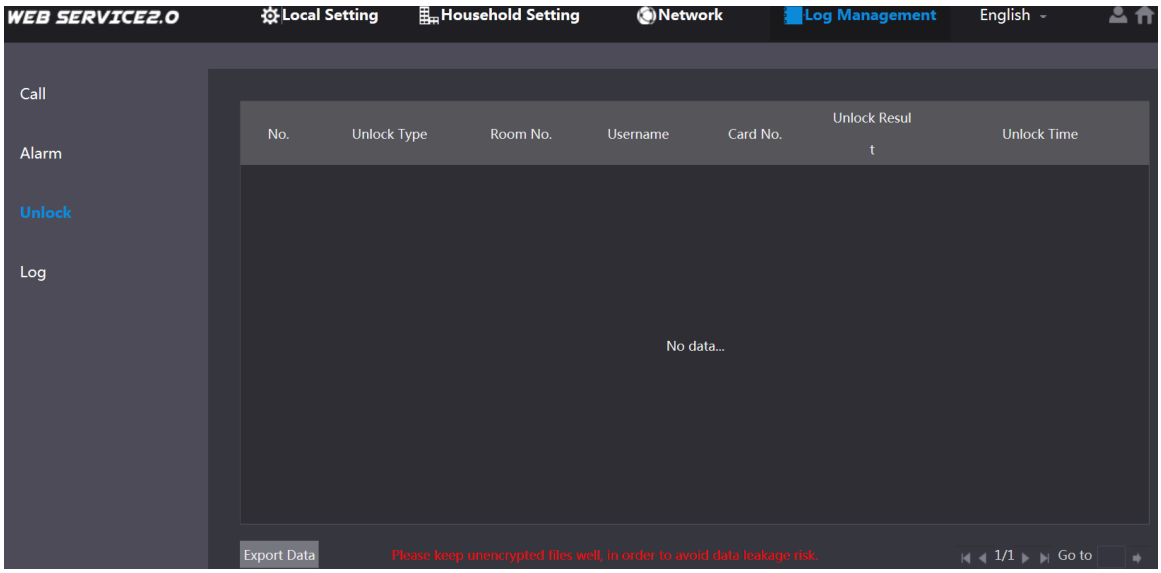
Figura 7-2arma



7.3 desbloquear

Puede ver y exportar registros de desbloqueo, incluidos desbloqueo de tarjeta de acceso, desbloqueo de contraseña, desbloqueo remoto y desbloqueo de botones.

la Figura 7-3 Desbloquee

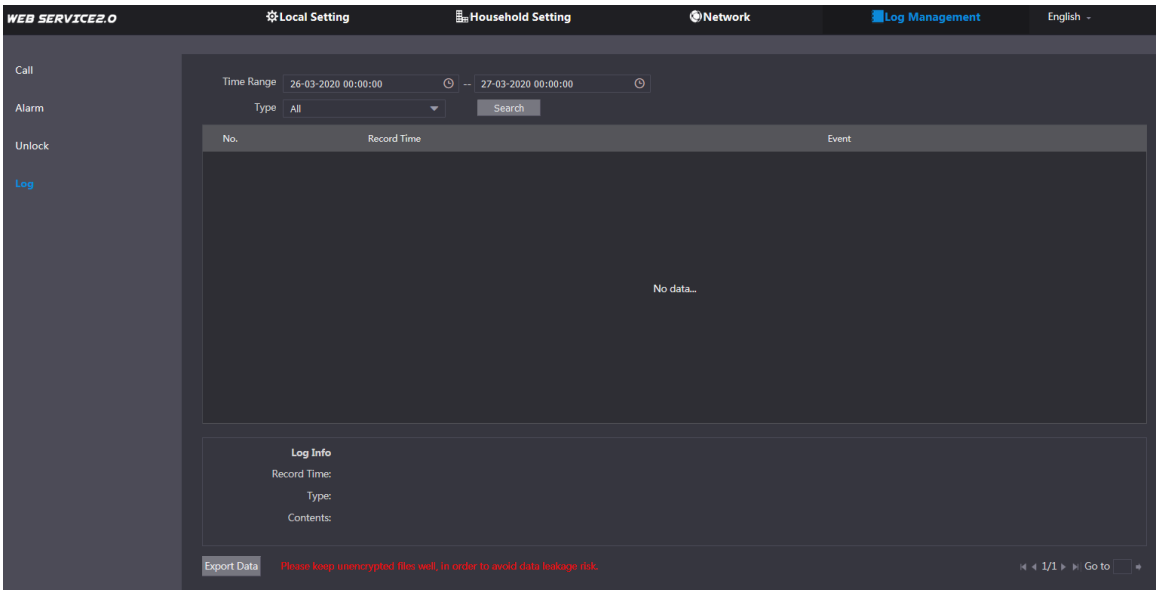


Hacer clic **Exportar datos** para exportar los registros a su PC.

7.4 Iniciar sesión

Puede buscar, ver y ver registros de eventos en períodos específicos.

Figura 7-4 Registro



Apéndice 1 Recomendaciones de ciberseguridad

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

Acciones obligatorias a tomar para la seguridad de la red del equipo básico:

1. Use contraseñas seguras

Consulte las siguientes sugerencias para establecer contraseñas:

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

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

- De acuerdo con el procedimiento estándar en la industria de la tecnología, 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 "comprobación automática de actualizaciones" para obtener información oportuna de las actualizaciones de firmware lanzadas por el fabricante.

- Sugerimos que descargue y use la última versión del software del cliente.

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

1. Protección física

Sugerimos que realice protección física a los equipos, especialmente a los dispositivos de almacenamiento. Por ejemplo, coloque el equipo en una sala y gabinete de computadoras especiales e implemente un permiso de control de acceso bien hecho y una administración de claves para evitar que personal no autorizado realice 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 regularmente

Sugerimos que cambie las contraseñas regularmente para reducir el riesgo de ser adivinado o descifrado.

3. Establecer y actualizar las contraseñas Restablecer la información a tiempo

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

4. Habilitar bloqueo de cuenta

La función de bloqueo de cuenta está habilitada de manera 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 los puertos HTTP y otros servicios predeterminados

Le sugerimos que cambie los puertos HTTP y otros puertos de servicio predeterminados en cualquier conjunto de números entre 1024 ~ 65535, lo que reduce el riesgo de que personas externas puedan adivinar qué puertos está utilizando.

6. Habilite HTTPS

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

7. Habilite la lista blanca

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

8. Enlace de dirección MAC

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

9. Asignar cuentas y privilegios razonablemente

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

10. Desactiva los servicios innecesarios y elige modos seguros

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

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

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

11. Transmisión cifrada de audio y video

Si el contenido de sus 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 causará alguna pérdida en la eficiencia de la transmisión.

12. Auditoría segura

- Verificar usuarios en línea: le sugerimos que revise los usuarios en línea regularmente 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 capacidad de almacenamiento limitada 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 el seguimiento.

14. Construir un entorno de red seguro

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

- Deshabilite la función de asignación de puertos del enrutador para evitar el acceso directo a los dispositivos de la intranet desde 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, es

sugirió usar VLAN, GAP de red y otras tecnologías para particionar la red, a fin de lograr el efecto de aislamiento de la red.

- Establezca el sistema de autenticación de acceso 802.1x para reducir el riesgo de acceso no autorizado a redes privadas.