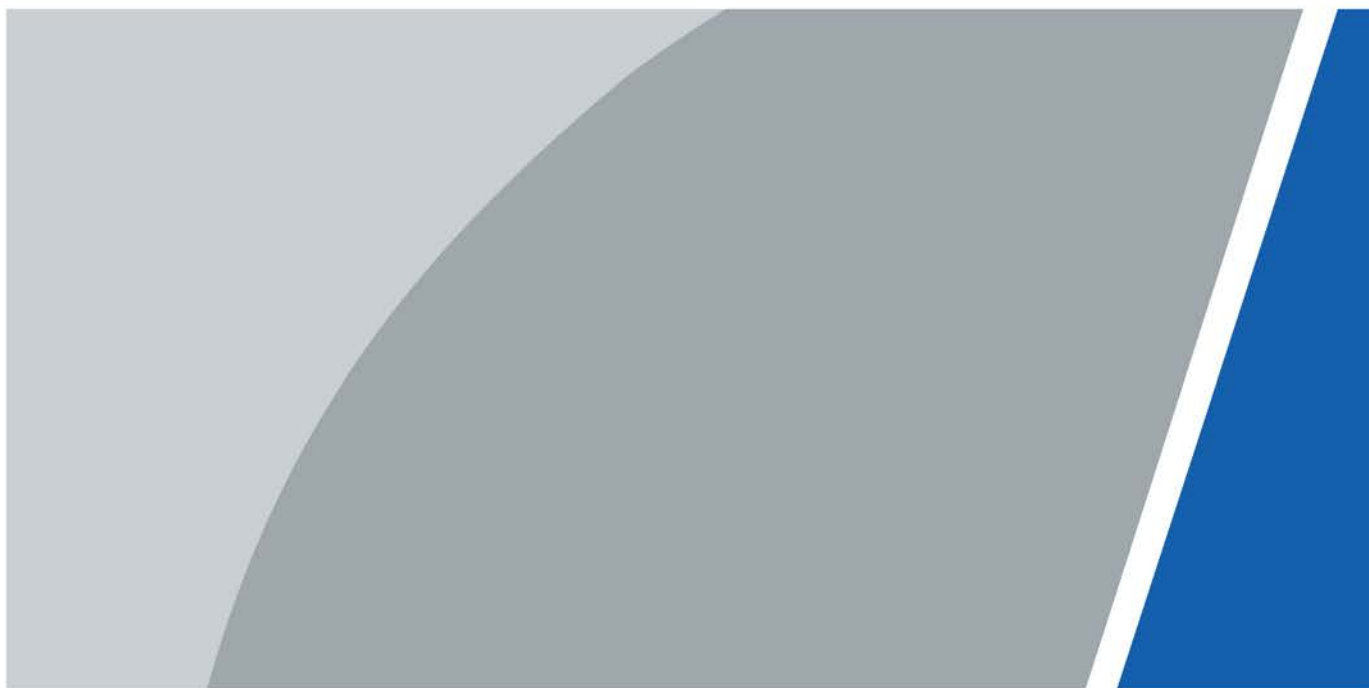


Estación de puerta de villa

Manual de usuario



Prefacio

General

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

Instrucciones de seguridad

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

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

Historial de revisiones

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

Acerca del Manual

- El manual es sólo para referencia. Si hay inconsistencia entre el manual y el producto real, prevalecerá el producto real.
- No somos responsables de ninguna pérdida causada por operaciones que no cumplan con el manual. El manual se actualizará de acuerdo con las últimas leyes y regulaciones de las jurisdicciones relacionadas. Para obtener información detallada, consulte el manual en papel, el CD-ROM, el código QR o nuestro sitio web oficial. Si hay inconsistencia entre el manual en papel y la versión electrónica, prevalecerá la versión electrónica.
- Todos los diseños y 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. Comuníquese con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria.
- Aún así puede haber desviaciones en los datos técnicos, funciones y descripción de operaciones, o errores de impresión. Si hay alguna duda o disputa, nos reservamos el derecho de dar una explicación final.
- Actualice el software del lector o pruebe otro software de lectura convencional si no se puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas comerciales registradas y nombres de empresas que aparecen en el manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, comuníquese con el proveedor o con el servicio de atención al cliente si ocurre algún problema al usar el dispositivo.
- Si existe alguna incertidumbre o controversia, nos reservamos el derecho de dar una explicación final.

Salvaguardias y advertencias importantes

La siguiente descripción es el método de aplicación correcto de la VTO. Lea atentamente el manual antes de usarlo, para evitar peligros y pérdidas de propiedad. Siga estrictamente el manual durante el uso y consérvelo correctamente después de leerlo.

Requisitos operativos

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

Requisitos de energía

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

Tabla de contenido

Prefacio.....	I Medidas de seguridad y advertencias importantes..... II 1
Inicializando el VTO.....	1
2 Iniciar sesión y restablecer la contraseña	2
2.1 Acceso	2
2.2 Restablecer contraseña.....	2
3 Interfaz principal.....	4
4 Configuraciones locales	5
4.1 Básico	5
4.2 Vídeo y audio.....	6
4.3 Configuración de control de acceso	8
4.3.1 Locales.....	8
4.3.2 RS-485	9
4.3.3 Gestión de contraseñas	9
4.4 Sistema.....	10
4.5 Seguridad	11
4.6 Wiegand.....	12
4.7 Usuario Onvif.....	13
4.8 Subir archivo.....	13
5 Entorno del hogar.....	15
5.1 Nro. VTO Gestión	15
5.2 Gestión de VTH	16
5.2.1 Agregar número de habitación.....	16
5.2.2 Emisión de Tarjeta de Acceso	17
5.2.3 Emisión de huellas dactilares	18
5.3 Gestión VTS.....	19
5.4 Configuración de IPC	20
5.5 Estado	21
5.6 Publicar información.....	22
5.6.1 Enviar información	22
5.6.2 Información del historial.....	22
6 Red.....	24
6.1 Básico	24
6.1.1 TCP/IP.....	24
6.1.2 Puerto.....	24
6.1.3 P2P.....	25
6.2 UPnP.....	25
6.2.1 Habilitación de servicios UPnP.....	25
6.2.2 Agregar servicios UPnP.....	25
6.3 Servidor SIP.....	26
6.4 Cortafuegos	27
7 Gestión de registros	29
Appendix 1 Recomendaciones de ciberseguridad	30

1 Inicializando el VTO

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

Step 1 Encienda el VTO.

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



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

Figure 1-1 Inicialización del dispositivo

Device Init

1 One 2 Two 3 Three

Username admin

Password

Low Middle High

Confirm Password

Next

Step 3 Ingrese y confirme la contraseña y luego haga clic en **Próximo**. Ingrese una

Step 4 dirección de correo electrónico para restablecer la contraseña.

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

2 Iniciar sesión y restablecer la contraseña

2.1 Acceso

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

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



Para iniciar sesión por primera vez, ingrese la IP predeterminada (192.168.1.108). Si tiene varios VTO, nosotros recomendamos cambiar la dirección IP predeterminada (**Red > Básico**) para evitar conflictos.

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

Figure 2-1 Acceso

2.2 Restablecer contraseña

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

Figure 2-2 Restablecer la contraseña

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

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

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



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

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

3 interfaz principal

Figure 3-1 Interfaz principal

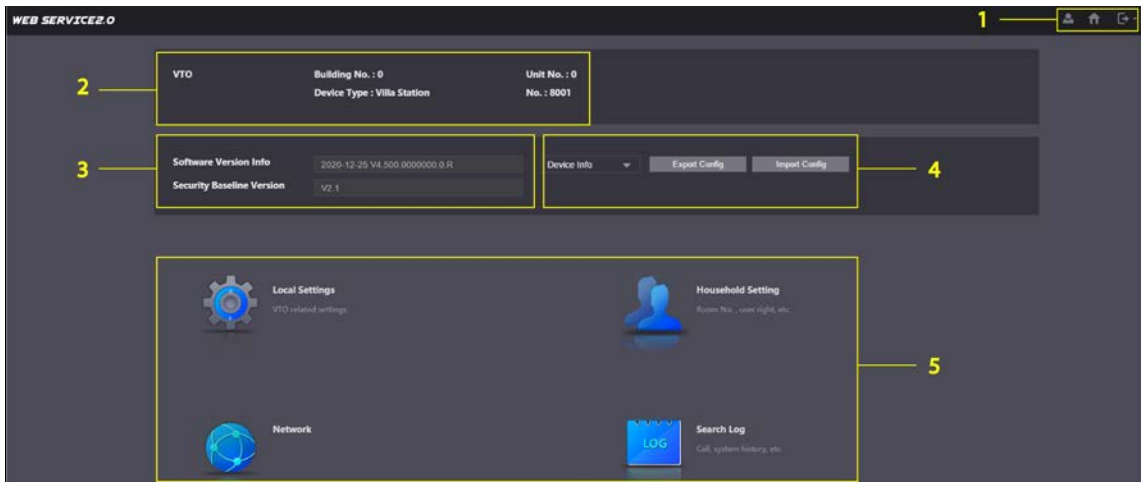


Tabla 3-1 Introducción a la interfaz principal

No.	Función	Descripción
1	Función general	 : Cambie la contraseña y su dirección de correo electrónico.  : Vaya a la interfaz principal.  : cierre sesión, reinicie el VTO o restaure el VTO a la configuración de fábrica.  Si restaura el VTO a la configuración de fábrica, se eliminarán todos los datos excepto el almacenamiento externo. Puede formatear la tarjeta SD para eliminar los datos que contiene.
2	información OVT	Ver la información del VTO y del sistema.
3	Información del sistema	
4	Configuración gerente	Exporte o importe la configuración de VTO o la información del usuario.
5	Función	Configurar parámetros para diferentes funciones.  La interfaz y la función pueden variar según los modelos. El producto real prevalecerá.

4 configuraciones locales

Este capítulo presenta la configuración detallada del VTO.

4.1 Básico

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

Figure 4-1 Básico

Step 2 Configure los parámetros.

Tabla 4-1 Descripción de parámetros básicos

Parámetro	Descripción
Tipo de dispositivo	Seleccionar Estación VillaoApartamento pequeño según sea necesario.
Número de llamada del centro.	El número de teléfono predeterminado para el centro de gestión es 888888 y puede configurarlo en cualquier número de hasta 9 dígitos.
Nombre del dispositivo	Cuando otros dispositivos estén monitoreando este VTO, el nombre del dispositivo aparecerá en la imagen de monitoreo.
Período del centro de llamadas	Periodo de tiempo en el que se puede llamar al centro gestor.
No.	Se utiliza para diferenciar cada VTO, y recomendamos configurarlo según la unidad o el número de edificio, y luego puede agregar VTO al servidor SIP usando sus números.  Puede cambiar el número del VTO cuando no esté funcionando como servidor SIP.
Periodos en los que se pueden realizar llamadas	Configura la hora si solo quieres recibir llamadas durante un periodo específico.
Llamada grupal	Habíltelo en el VTO que funciona como servidor SIP, y cuando un VTH principal reciba una llamada, todos los VTH de extensión también recibirán la llamada.

Parámetro	Descripción
Tarjeta SD total Capacidad	Muestra la capacidad total y utilizada de la tarjeta SD. Puedes hacer clic Formato para eliminar todos los datos de la tarjeta SD.
Capacidad utilizada SD	
Formato	
Captura automática (Descubrir)	Cuando la puerta esté desbloqueada, el VTO tomará dos instantáneas y las guardará en la tarjeta SD.
Captura automática (llamada)	Tome una instantánea y guárdela en la tarjeta SD del VTO cuando el VTO esté llamando.
Subir vídeo Mensajes	Cuando está habilitado: ● Si se inserta una tarjeta SD tanto en el VTH como en el VTO, el mensaje de video se guardará tanto en las tarjetas SD del VTH como en el VTO. ● Si solo se inserta una tarjeta SD en el VTH o el VTO, el mensaje de video se guardará solo en la tarjeta SD del VTH o el VTO. ● Si no se inserta ninguna tarjeta SD en el VTH o VTO, no se guardará ningún mensaje de video.
Grabación automática (llamada)	Realice una grabación cuando el VTO esté en una llamada y guárdela en la tarjeta SD del VTO.

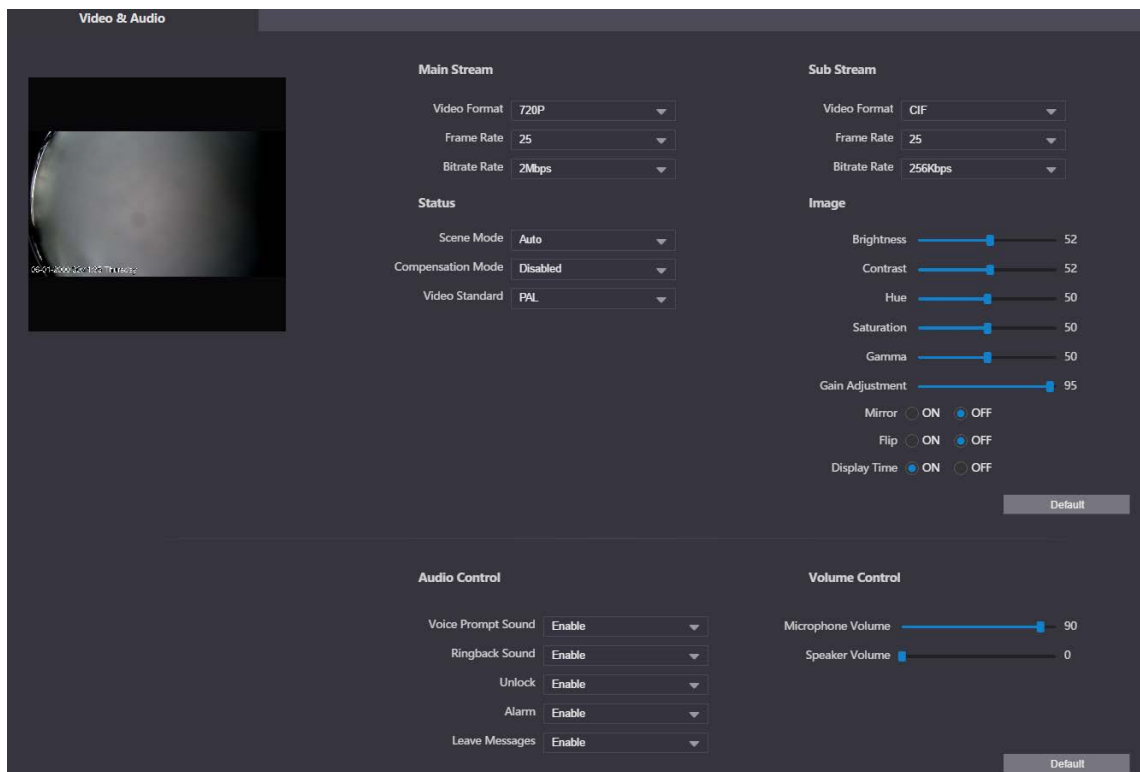
Step 3 Hacer clic **Ahorrar**.

4.2 Vídeo y audio

Configurar el formato y calidad de vídeo y audio del VTO.

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

Figure 4-2 Vídeo y audio



Step 2 Configure los parámetros, que entrarán en vigor tras el cambio.

Tabla 4-2 Descripción de los parámetros de vídeo

Parámetro		Descripción
Principal/Sub Arroyo	Video Formato	Seleccione una resolución diferente según sea necesario: ● 1080P: 1920 × 1080. ● 720P: 1280 × 720. ● WVGA: 800 × 480. ● QVGA: 320 × 240. D1: ● 720 × 480. ● CIF: 352 × 288.
	Velocidad de fotogramas	Cuanto mayor sea el valor, más fluido será el vídeo, pero requiere más ancho de banda.
	Tasa de bits	Cuanto mayor sea el valor, mejor será la calidad del vídeo, pero requiere más ancho de banda.
Estado	Modo de escena	Seleccione según sea necesario según las condiciones de iluminación. Auto está seleccionado de forma predeterminada.
	compensati en modo	● BLC: Compensación de contraluz. Mejora la claridad del objetivo en la imagen. ● WDR: Amplio rango dinámico. Mejore el brillo de las áreas oscuras y reduzca el brillo de las áreas brillantes para mejorar la imagen. CHL: ● Compensación de luz alta. Reduzca el brillo de los puntos fuertes para mejorar la imagen general.
	Video Estándar	Seleccionar CAMARADA o NTSC según tu zona.  CAMARADA se utiliza principalmente en China y Europa, y NTSC principalmente en Estados Unidos y Japón.
Imagen	Brillo	Cuanto mayor sea el valor, más brillante será la imagen.
	Contraste	Valor mayor para mayor contraste entre áreas brillantes y oscuras.
	Matiz	Haz que el color sea más brillante o más oscuro. El valor predeterminado lo establece el sensor de luz y recomendamos mantenerlo predeterminado.
	Saturación	Cuanto mayor sea el valor, más denso será el color.
	Gama	Cambia el brillo de la imagen y mejora el rango dinámico de la imagen de forma no lineal. Cuanto mayor sea el valor, más brillante será la imagen.
	Ganar Ajuste	Amplifique la señal de vídeo para aumentar el brillo de la imagen. Si el valor es demasiado grande, habrá más ruido en la imagen.
	Espejo	Muestre la imagen con los lados izquierdo y derecho invertidos.
	Voltear	Muestre la imagen al revés.
	Hora de visualización	Muestra la hora y fecha actuales en la imagen de vídeo.
Audio Control	—	Activa o desactiva cada tipo de sonido.
Volumen Control	Micrófono Volumen	Ajuste el volumen según sea necesario.
	Vocero Volumen	

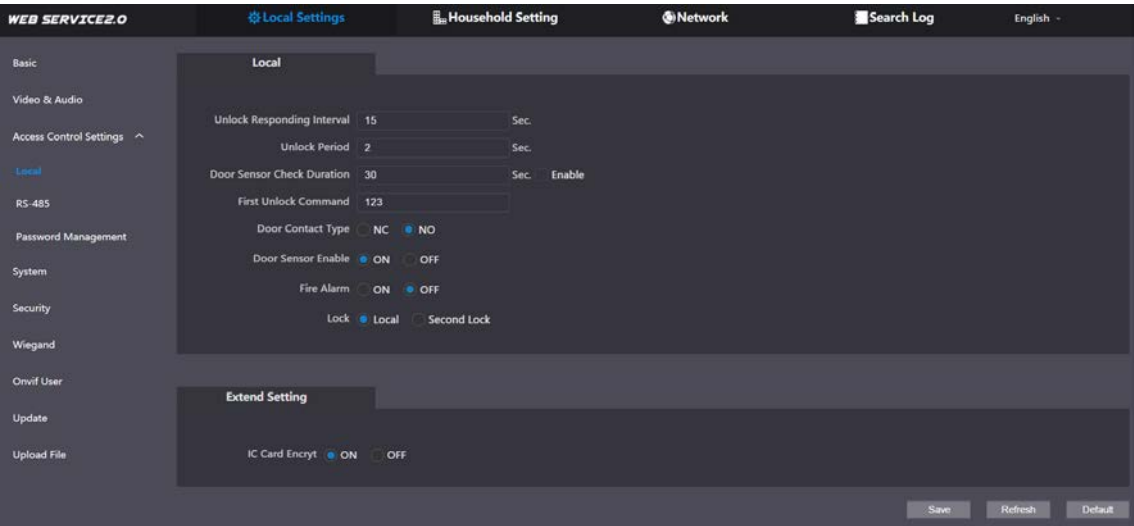
4.3 Configuración de control de acceso

Esta sección presenta cómo configurar las dos cerraduras conectadas al puerto de cerradura o al puerto RS-485 del VTO.

4.3.1 Locales

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

Figure 4-3 Local



Step 2 Configure los parámetros.

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

Parámetro	Descripción
Descubrir Respondiendo Intervalo	La puerta sólo se podrá volver a desbloquear después de ese intervalo.
Período de desbloqueo	El tiempo durante el cual la cerradura permanece desbloqueada.
Sensor de puerta Verificar duración	● Habilítelo y la puerta no se bloqueará hasta que los sensores de la puerta entren en contacto entre sí. Si la puerta permanece desbloqueada por más tiempo que el Duración de la verificación del sensor de puerta, se activará la alarma del sensor de la puerta y la alarma se enviará al centro de gestión. ● Desactívelo y luego la puerta se bloqueará después de Período de desbloqueo.  Necesita instalar un contacto de puerta para configurar este parámetro.
Primero/Segundo Comando de desbloqueo	Puede conectar un teléfono de terceros, como un teléfono SIP, al VTO y usar el comando para abrir la puerta de forma remota.
Contacto de puerta Tipo	● CAROLINA DEL NORTE: Normalmente cerrado. ● NO: Normalmente abierto.
Sensor de puerta Permitir	Sincronice el estado del sensor de puerta con los monitores interiores (VTH).
Alarma de incendios	Si está activado, puede conectar un dispositivo de alarma al puerto que originalmente es para el contacto de la puerta, pero no puede usar la función de contacto de la puerta.
Cerrar	Los métodos no remotos, como la contraseña o la tarjeta, desbloquearán el bloqueo que

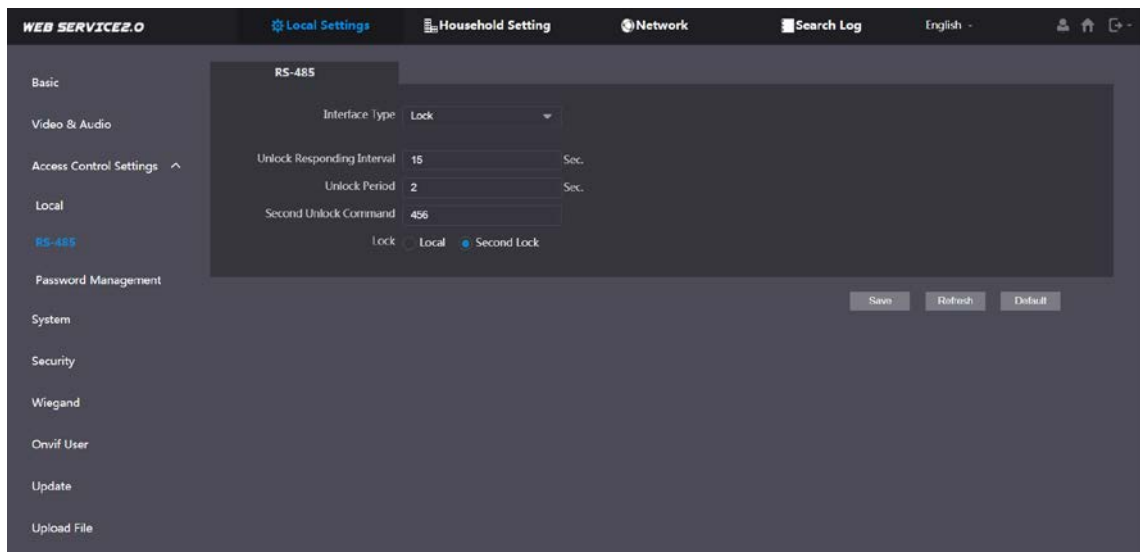
Parámetro	Descripción
	seleccionar.
Cifrado de tarjeta IC	Las tarjetas de acceso emitidas por VTO estarán cifradas y no se podrán clonar.

Step 3 Hacer clic **Ahorrar**.

4.3.2 RS-485

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

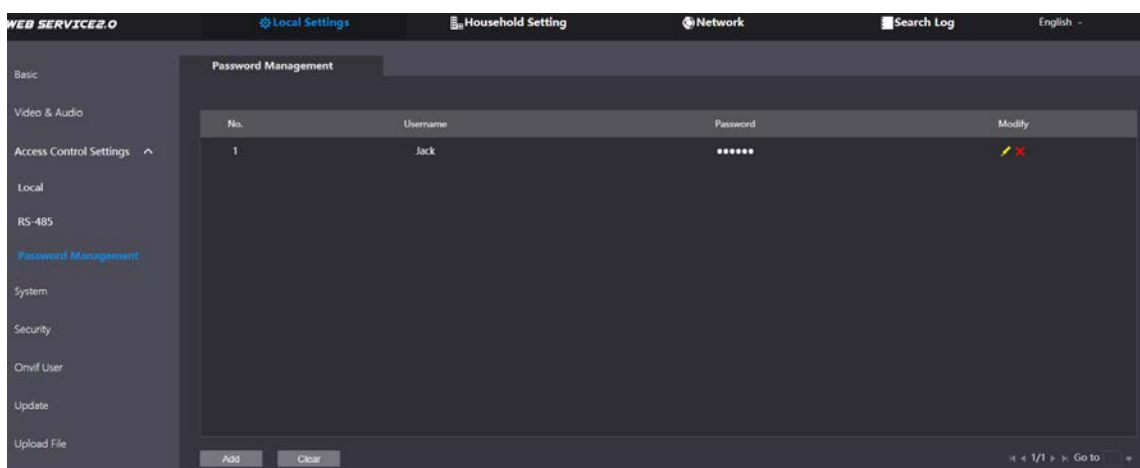
Figure 4-4 Cerradura conectada a través del puerto RS-485



4.3.3 Gestión de contraseñas

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

Figure 4-5 Gestión de contraseñas

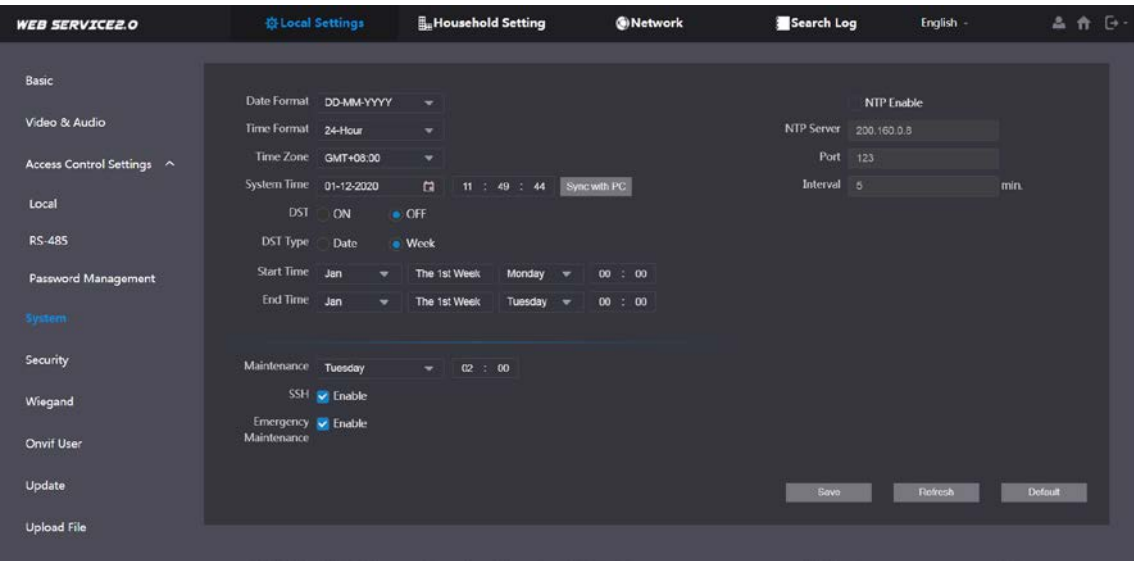


4.4 Sistema

Configure parámetros de tiempo, servidor NTP y más.

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

Figure 4-6 Sistema



Step 2 Configure los parámetros.

Tabla 4-4 Descripción de los parámetros del sistema

Parámetro	Descripción
Formato de fecha	Seleccione un formato según sea necesario.
Formato de hora	
Hora del sistema	 Cambiar la hora del sistema puede causar problemas en la búsqueda de videos y publicación de información. Desactive la grabación de video y la instantánea automática antes de cambiarlas.
Huso horario	Configure la zona horaria según sea necesario.
Sincronizar con la computadora	Sincronice la hora del sistema VTO con su PC.
horario de verano	Horario de verano. Si es aplicable a su área, debe habilitarlo y luego configurar el tipo de horario de verano, la hora de inicio y la hora de finalización.
Tipo de horario de verano	Seleccionar Fecha o Semana según sea necesario y luego configure el período específico.
Hora de inicio	Configure la hora de inicio y finalización del horario de verano.
Hora de finalización	
Habilitar NTP	Habilite NTP e ingrese la dirección IP del servidor NTP, y luego el VTO sincronizará la hora con el servidor NTP automáticamente.
Servidor NTP	
Puerto	Número de puerto del servidor NTP.
Intervalo	Ciclo de actualización de hora VTO. 30 minutos como máximo.
Mantenimiento	Defina la hora en la que el VTO se reiniciará automáticamente.
SSH	Puede conectar dispositivos de depuración al VTO a través del protocolo SSH.  Recomendamos desactivarlo y activar el modo de seguridad y la protección de la información del servicio saliente. Consulte "4.5 Seguridad". De lo contrario, el VTO podría quedar expuesto.

Parámetro	Descripción
	a riesgos de seguridad y fuga de datos.
Emergencia Mantenimiento	Habilítelo para el análisis y reparación de fallas.  Esta función ocupará los puertos 8088 y 8087.

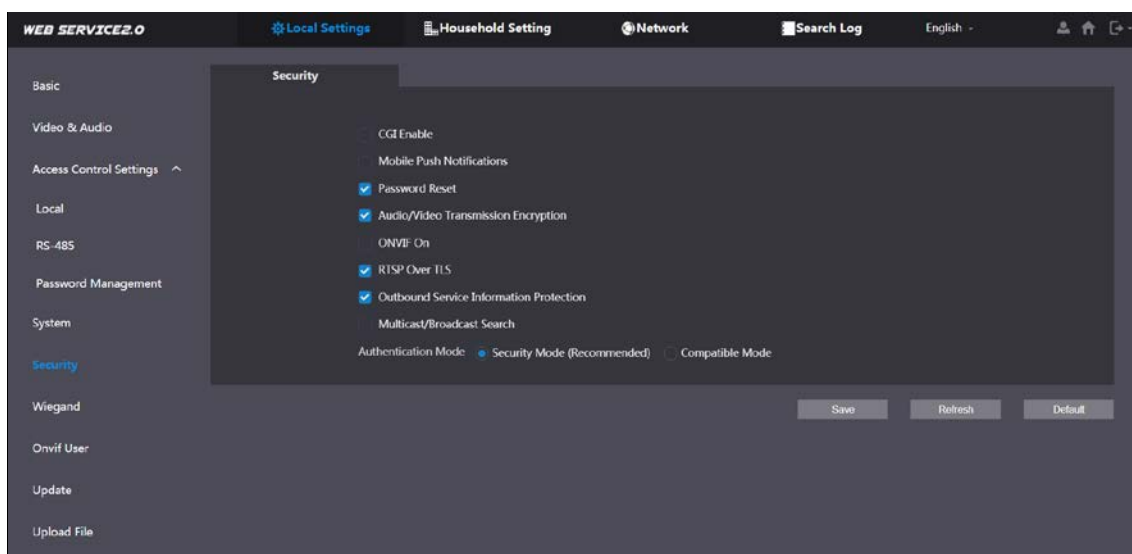
Step 3 Hacer clic **Ahorrar**.

4.5 Seguridad

Configurar funciones que involucran la seguridad del dispositivo.

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

Figure 4-7 Seguridad



Step 2 Configure los parámetros.

Tabla 4-5 Descripción del parámetro de seguridad

Parámetro	Descripción
Habilitar CGI	Habilite el uso del comando CGI.  Recomendamos apagarlo. De lo contrario, la VTO podría quedar expuesta a riesgos de seguridad y fuga de datos.
Empuje móvil Notificación	Envía información a la aplicación en el teléfono inteligente.  Recomendamos apagarlo si no necesita esta función. De lo contrario, la VTO podría quedar expuesta a riesgos de seguridad y fuga de datos.
Restablecer contraseña	Si está desactivado, no podrá restablecer la contraseña.
Audio/vídeo Transmisión Cifrado	Cifre todos los datos durante una llamada de voz o video.  Recomendamos encenderlo. De lo contrario, el VTO podría quedar expuesto a

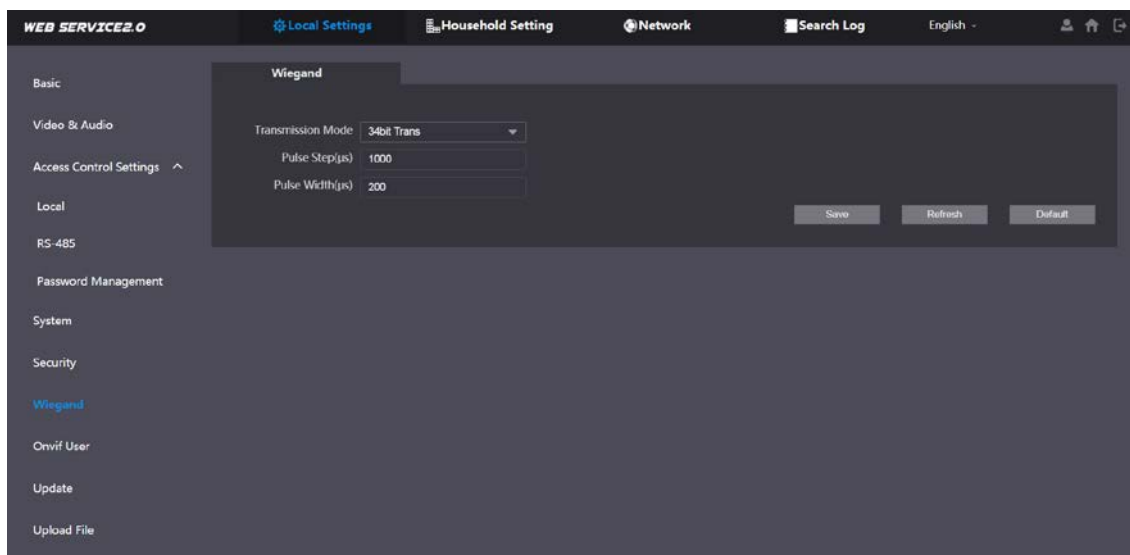
Parámetro	Descripción
	riesgos de seguridad y fuga de datos.
ONVIF activado	Permita que terceros extraigan la transmisión de video del VTO a través del protocolo ONVIF.  Recomendamos apagarlo. De lo contrario, la VTO podría quedar expuesta a riesgos de seguridad y fuga de datos.
RTSP sobre TSL	Salida de flujo de bits cifrado a través de RTSP.  Recomendamos encenderlo. De lo contrario, la VTO podría quedar expuesta a riesgos de seguridad y fuga de datos.
Servicio saliente Información Protección	Proteja sus contraseñas.  Recomendamos encenderlo. De lo contrario, la VTO podría quedar expuesta a riesgos de seguridad y fuga de datos.
Multidifusión/difusión Buscar	Habilítelo y otros dispositivos encontrarán el VTO.  Recomendamos apagarlo. De lo contrario, la VTO podría quedar expuesta a riesgos de seguridad y fuga de datos.
Autenticación Modo	● Modo de seguridad(recomendado): Admite el inicio de sesión con autenticación implícita. ● Modo compatible: Utilice el método de inicio de sesión anterior.  Recomendamos el modo de seguridad. El modo compatible puede exponer al VTO a riesgos de seguridad y fuga de datos.

Step 3 Hacer clic **Ahorrar**.

4.6 Wiegand

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

Figure 4-8 Wiegand



4.7 Usuario Onvif

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



Si elimina una cuenta, no se puede deshacer.

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

Step 2 Hacer clic **Agregar**.

Figure 4-9 Agregar un usuario ONVIF

Step 3 Ingrese la información y luego haga clic **Ahorrrar**.

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

4.8 Cargar archivo

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

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

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

Figure 4-10 Cambiar el mensaje de sonido

The screenshot shows the 'WEB SERVICE2.0' interface with the 'Local Settings' tab selected. The left sidebar contains a menu with 'Upload File' highlighted. The main content area is titled 'Upload File' and includes an 'Audio Types' dropdown menu set to 'Unlocked'. Below this is a 'Local Upload' section with a text input field, a 'Browse' button, and an 'Upload' button. A red error message states: 'Please upload mp3 files, and the file size cannot exceed 20 Kb'. At the bottom, there is a table with two columns: 'No.' and 'Audio Types'. The table is currently empty, displaying 'No data...'.

No.	Audio Types
No data...	

Step 3 Hacer clic **Subir**.

5 entorno doméstico

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



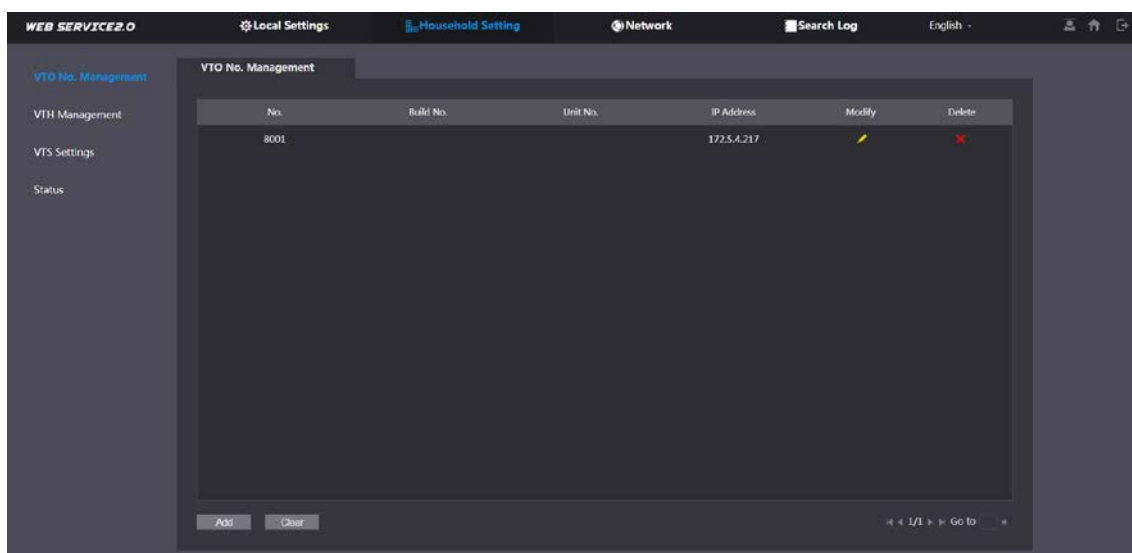
Para configurar los parámetros del servidor SIP, consulte "6.3 Servidor SIP" para obtener más detalles.

5.1 VTO No. Gestión

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

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

Figure 5-1 Gestión de OVT



Step 2 Hacer clic **Agregar**.

Figure 5-2 Agregar VTO

Add

No.

Registration Password

Build No.

Unit No.

IP Address

127.0.0.1

Username

Password

Save

Cancel

Step 3 Configure los parámetros.



Se debe agregar el servidor SIP.

Tabla 5-1 Agregar configuración de VTO

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

Step 4 Hacer clic **Ahorrar**.



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

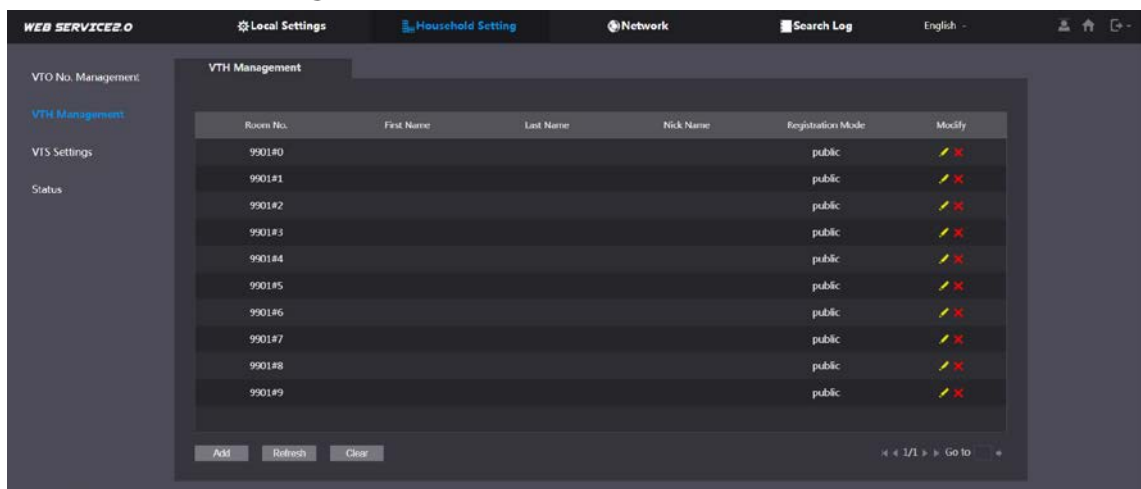
5.2 Gestión VTH

5.2.1 Agregar número de habitación

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

Step 1 Inicie sesión en la interfaz web del servidor SIP y luego seleccione **Entorno doméstico > Gestión de VTH**.

Figure 5-3 Gestión de números de habitaciones



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

Step 2 Hacer clic **Agregar**.

Figure 5-4 Añadir un número de habitación

Step 3 Configure los parámetros.

Tabla 5-2 Información de la habitación

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

Step 4 Hacer clic **Ahorrar**.



Hacer clic O para modificar o eliminar un número de habitación.

5.2.2 Emisión de tarjeta de acceso

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



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

Step 1 Seleccionar **Entorno doméstico > Gestión de VTH**, haga clic **Agregar** luego haga clic en **Tarjeta de emisión**.

Figure 5-5 aviso de cuenta regresiva

Step 2 Pase la tarjeta en el VTO.

Figure 5-6 Tarjeta de emisión

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

Figure 5-7 Tarjeta de acceso emitida

Username	Card No.	Modify
mm	mm	

Otras operaciones

- Haga clic para establecerla como tarjeta principal y luego el icono cambia a . La tarjeta principal puede ser utilizada para emitir tarjetas de acceso para esta sala en el VTO.
- Haga clic para configurarlo como pérdida y luego el icono cambia a . La tarjeta perdida no se puede utilizar para abrir la puerta.
- Haga clic o para modificar el nombre de usuario o eliminar la tarjeta.

5.2.3 Emisión de huellas dactilares

Emitir huellas dactilares para desbloquear la puerta de una habitación.



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

Step 1 Seleccionar **Entorno doméstico > Gestión de VTH**, haga clic **Agregar** luego haga clic en **Emitir huella digital**.

Figure 5-8 Emitir huella digital

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

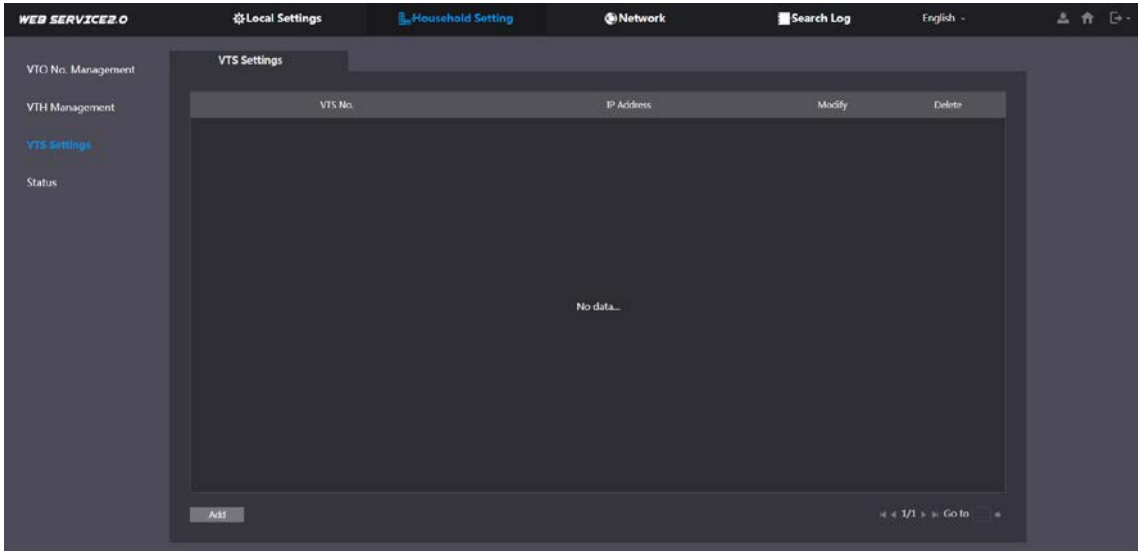
Step 3 Presione su huella digital en el escáner.

5.3 Gestión VTS

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

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

Figure 5-9 Gestión VTS



Step 2 Hacer clic **Agregar**.

Figure 5-10 Agregar VTS

Add

VTS No.

Registration Password

IP Address

127.0.0.1

Save

Cancel

Step 3 Configure los parámetros.

Tabla 5-3 Agregar configuración de VTS

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

Step 4 Hacer clic **Ahorrar**.

5.4 Configuración de IPC

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



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

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

Figure 5-11 configuración de IPC

IPC Name	IP Addr.	Username	Port No	Protocol	Stream	Channel	Device Type	Modify	Delete
1000	0.0.0.0	admin	554	Local	Main	1	IPC		
	0.0.0.0	admin	554	Local	Extra1	1	IPC		
	0.0.0.0	admin	554	Local	Extra1	1	IPC		
	0.0.0.0	admin	554	Local	Extra1	1	IPC		
	0.0.0.0	admin	554	Local	Extra1	1	IPC		
	0.0.0.0	admin	554	Local	Extra1	1	IPC		
	0.0.0.0	admin	554	Local	Extra1	1	IPC		
	0.0.0.0	admin	554	Local	Extra1	1	IPC		
	0.0.0.0	admin	554	Local	Extra1	1	IPC		
	0.0.0.0	admin	554	Local	Extra1	1	IPC		
	0.0.0.0	admin	554	Local	Extra1	1	IPC		
	0.0.0.0	admin	554	Local	Extra1	1	IPC		

Step 2 Hacer clic

Figure 5-12 Agregar IPC

Modify

IPC Name

IP Address

Username

Password

Port

Protocol

Stream Type

Channel

Device Type

MediaEncrypt ☐ ON ☒ OFF

Step 3 Configure los parámetros.

Tabla 5-4 Agregar configuración de IPC

Parámetro	Descripción
Nombre del consultor	Ingrese el nombre que identifica al IPC.
Dirección IP	Dirección IP del IPC.
Nombre de usuario	Nombre de usuario y contraseña de inicio de sesión de la interfaz web del dispositivo.
Contraseña	
Puerto	Manténgalo predeterminado.
Protocolo	Seleccionar Local o onvif .
Tipo de flujo	● Principal: Mejor calidad de vídeo pero requiere más ancho de banda. ● Extra1: Vídeo más fluido con peor calidad, pero requiere menos ancho de banda.
Canal	El número de canales que admite un dispositivo.
Tipo de dispositivo	Seleccione el que sea necesario.
cifrado de medios	Seleccionar EN si el IPC que se va a agregar está cifrado.

Step 4 Hacer clic **Ahorrar**.

Otras operaciones

- **Exportar configuración**: Exporta la información del dispositivo a tu PC. **Importar**
- **configuración**: Importa información del dispositivo.

5.5 Estado

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

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

Figure 5-13 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 dispositivos VTH y ver el historial de mensajes.

5.6.1 Enviar información

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

Figure 5-14 Enviar información

Validity Period: 2000-01-16 23:59:59

Send to: All devices

Title:

Contents:

Confirm Refresh

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

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

Step 4 Hacer clic **Confirmar**.

5.6.2 Información del historial

Puede ver la información de los mensajes enviados.

Inicie sesión en la interfaz web del servidor SIP, seleccione **Configuración del hogar > Publicar información > Información histórica**.

Figure 5-15 Información histórica

WEB SERVICE2.0

Local Setting Household Setting Network Setting Log Management

VTO No. Management

Room No. Management

VTS Management

IPC Setting

Status

Publish Information ^

Send Info

History Info

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

< 1/1 > Go to

6 Red

Este capítulo presenta cómo configurar los parámetros de red.

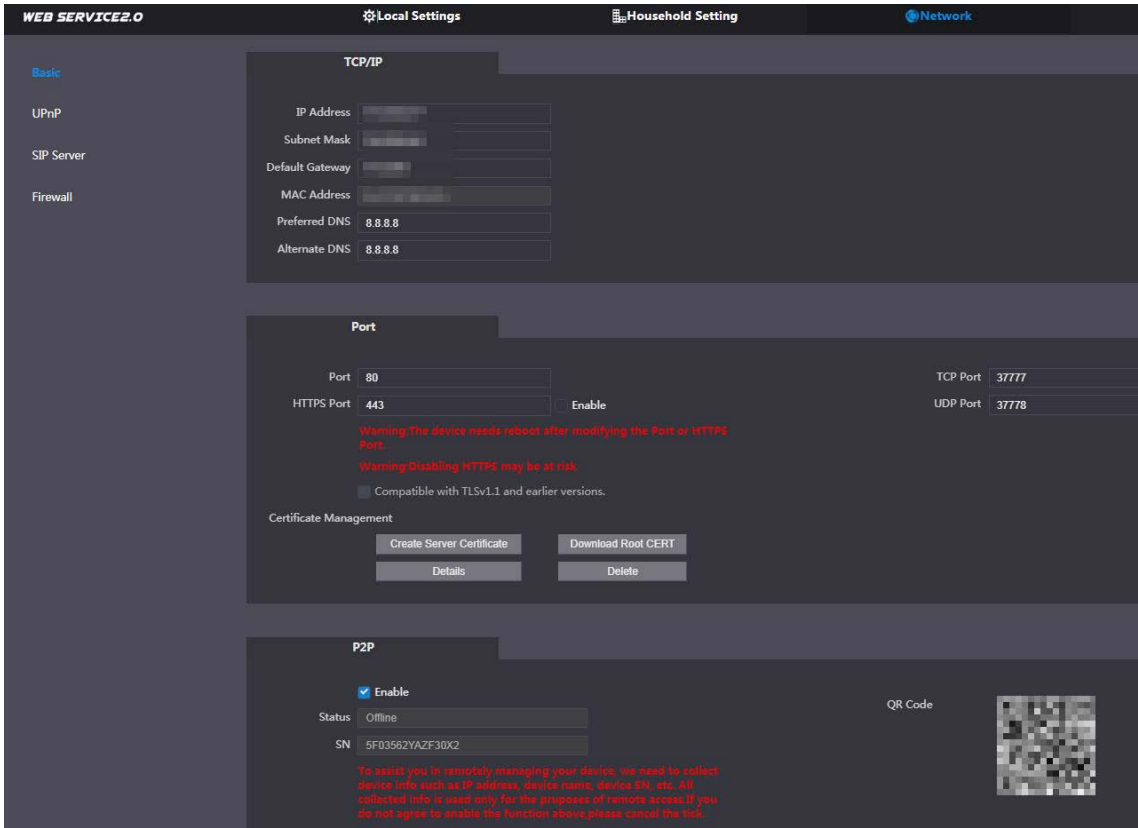
6.1 Básico

6.1.1 TCP/IP

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

Step 1 Seleccionar **Red > Básico**.

Figure 6-1 TCP/IP y puerto



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

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

6.1.2 Puerto

Tabla 6-1 Descripción del parámetro

Parámetro	Descripción
Puerto	80 por defecto. Si ya lo utiliza, elija cualquier número entre 1025 y 65535 según sea necesario. puedes entrar <code>http://Dirección IP de VTO:Puerto</code> para iniciar sesión en VTO.
Puerto HTTPS	Habilítelo y haga clic Ahorrar . Ya puedes entrar <code>https://Dirección IP VTO:Puerto HTTPS</code>

Parámetro	Descripción
	inicie sesión en el VTO.
Puerto TCP/UDP	Se utiliza para acceder al VTO con dispositivos en otras redes. Consulte "6.2 UPnP" para obtener más detalles.
Crear Servidor Certificado	La identificación digital única de VTO para el protocolo SSL. Para usarlo por primera vez o después de cambiar la dirección IP del VTO, debe realizar este proceso.  Si elimina el certificado que se ha creado, no se puede deshacer.
Descargar raíz CERTIFICADO	Si está utilizando una PC que nunca ha iniciado sesión en VTO, debe descargar el certificado raíz, hacer doble clic para instalarlo y luego podrá usar la función HTTPS mencionada anteriormente.  Si elimina el certificado que se ha instalado, no se puede deshacer.

6.1.3 P2P

Habilitar el **P2P** función, y luego puede escanear el código QR con su teléfono para agregar el VTO a la aplicación en su teléfono inteligente. Consulte la guía de inicio rápido para obtener más detalles.

6.2 UPnP

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

Preparación

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

6.2.1 Habilitación de servicios UPnP

- Step 1** Seleccionar **Red > UPnP**.
- Step 2** Habilite los servicios enumerados según sea necesario.
- Step 3** Seleccionar **Permitir**.
- Step 4** Hacer clic **Ahorrar**.

6.2.2 Agregar servicios UPnP

- Step 1** Seleccionar **Red > UPnP**. Hacer
- Step 2** clic **Agregar**.

Step 3 Configure los parámetros según sea necesario.

Figure 6-2 Agregar un servicio UPnP

Add

ON

OFF

Service Name

Service Type

Protocol

TCP

Internal Port

External Port

Save

Cancel

Tabla 6-2 Descripción del parámetro

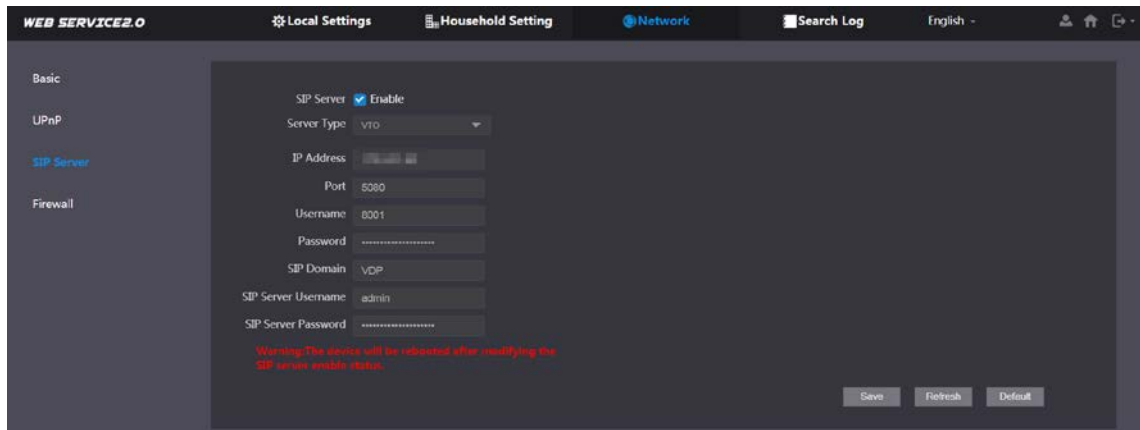
Parámetro	Descripción
Nombre del servicio	Ingrese la información según sea necesario.
Tipo de servicio	
Protocolo	Seleccionar tcp o UDP según sea necesario.
Puerto interno	Utilice el número de puerto del 1024 al 5000.
Puerto externo	- No utilice el número de puerto 1-1023 para evitar conflictos. - Si necesita configurar esta función para varios dispositivos, asegúrese de que los puertos no sean los mismos. - El número de puerto que utilice no debe estar ocupado. - El número de puerto interno y externo debe ser el mismo.

6.3 Servidor SIP

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

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

Figure 6-3 Servidor SIP



Step 2 Seleccione un tipo de servidor según sea necesario.

- El VTO en el que ha iniciado sesión como servidor SIP:

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



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

- Si otro VTO funciona como servidor SIP:

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

Tabla 6-3 Configuración del servidor SIP

Parámetro	Descripción
Dirección IP	Dirección IP de VTO.
Puerto	● 5060 de forma predeterminada cuando VTO funciona como servidor SIP. 5080 por ● defecto cuando la plataforma funciona como servidor SIP.
Nombre de usuario	Manténgalo predeterminado.
Contraseña	
Dominio SIP	VDP.
Nombre de usuario del servidor SIP	Nombre de usuario y contraseña de inicio de sesión de la interfaz web del VTO.
Contraseña del servidor SIP	

- Si otros servidores funcionan como servidor SIP:

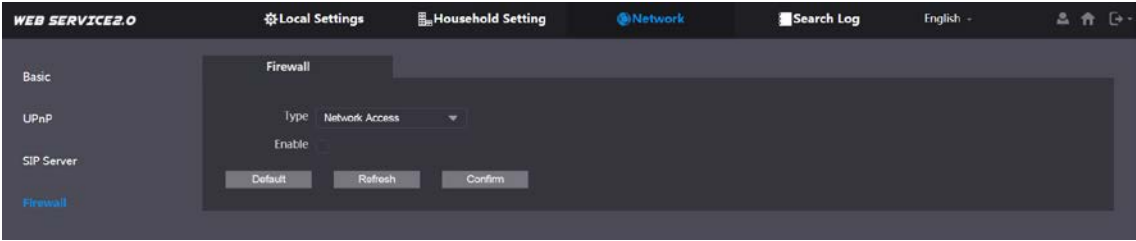
Seleccione el**Tipo de servidor**según sea necesario y luego consulte el manual correspondiente para obtener más detalles.

6.4 Cortafuegos

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

Step 1 Seleccionar**Red > Cortafuegos**.

Figure 6-4 Cortafuegos



- Step 2** Seleccione uno o más tipos de firewall y luego habilítelos.
- Step 3** Configure los parámetros.

Tabla 6-4 Descripción del tipo de firewall

Tipo	Descripción
Acceso a la red	Seleccione cualquiera Lista de permitidos o Lista de bloqueos y luego agregue una dirección IP o segmento al que se le permite o deniega el acceso al VTO.
ping prohibido	El VTO no responderá al ping para evitar ataques de ping.
Anti-semiunión	Protege el rendimiento de VTO bloqueando el exceso de paquetes SYN.

7 Gestión de registros

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



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

Appendix 1 Recomendaciones de ciberseguridad

La ciberseguridad es más que una simple palabra de moda: es algo que pertenece a todos los dispositivos 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 conectados los hará menos susceptibles a los ataques. A continuación se presentan algunos consejos y recomendaciones sobre cómo crear un sistema de seguridad más seguro.

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

1. Utilice contraseñas seguras

Consulte las siguientes sugerencias para establecer contraseñas:

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

2. Actualice el firmware y el software cliente a tiempo

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

Recomendaciones "es bueno tener" para mejorar la seguridad de la red de su dispositivo: 1. Protección física

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

2. Cambie las contraseñas con regularidad

Le sugerimos que cambie las contraseñas con regularidad para reducir el riesgo de que las adivinen o las descifren.

3. Establecer y actualizar contraseñas Restablecer información oportuna

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

4. Habilite el bloqueo de cuenta

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

5. Cambie HTTP predeterminado y otros puertos de servicio

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

6. Habilite HTTPS

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

7. Vinculación de direcciones MAC

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

8. Asigne cuentas y privilegios de manera razonable

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

9. Deshabilite los servicios innecesarios y elija modos seguros

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

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

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

10. Transmisión cifrada de audio y vídeo

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

Recordatorio: la transmisión cifrada provocará cierta pérdida en la eficiencia de la transmisión.

11. Auditoría segura

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

12. Registro de red

Debido a la capacidad de almacenamiento limitada del dispositivo, el registro almacenado es limitado. Si necesita guardar el registro durante un período prolongado, se recomienda habilitar la función de registro de red para garantizar que los registros críticos estén sincronizados con el servidor de registro de red para su seguimiento.

13. Construya un entorno de red seguro

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

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