Estación de puerta modular

Manual del usuario

Versión 1.0.0

Prefacio

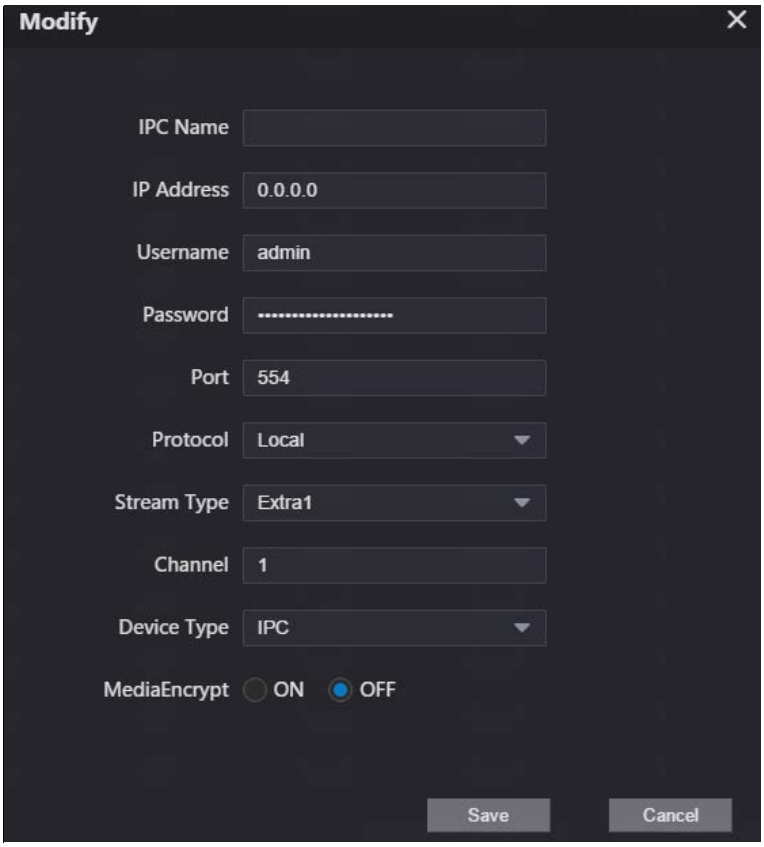
General

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

Instrucciones de seguridad

Las

Añadir IPC



Configurar los parámetros.

Tabla 5-4 Agregar configuración de IPC

Parámetro	Descripción
Nombre del IPC	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	Mantenlo por defecto
Protocolo	Seleccionar**Local**o**Onvif**.
Tipo de flujo	**Principal**:Mejor calidad de video pero requiere más ancho de banda. **Extra1**:Video más fluido y de peor calidad, pero que requiere menos ancho de banda.
Canal	La cantidad de canales que admite un dispositivo.
Tipo de dispositivo	Seleccione el que necesite.
Cifrado de medios	Seleccionar**EN**Si el IPC que se va a agregar está encriptado.

Hacer clic**Ahorrar**.

Otras operaciones

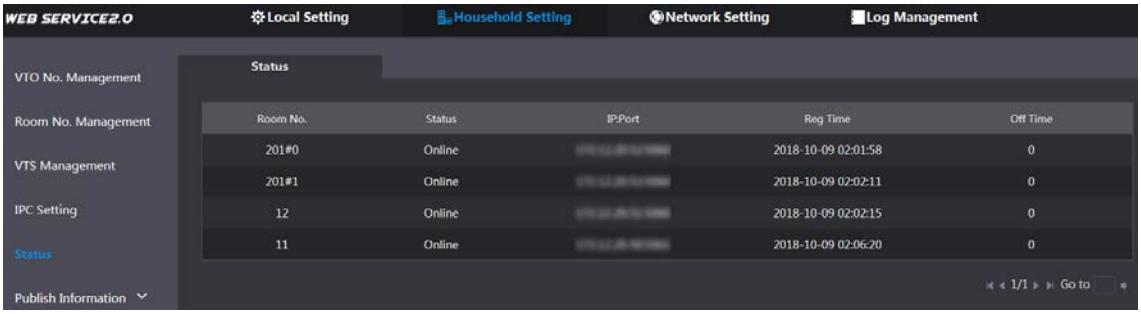
- **Exportar configuración**:Exporta la información del dispositivo a tu PC. **Importar**
- **configuración**:Importar información del dispositivo.

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**.

Estado



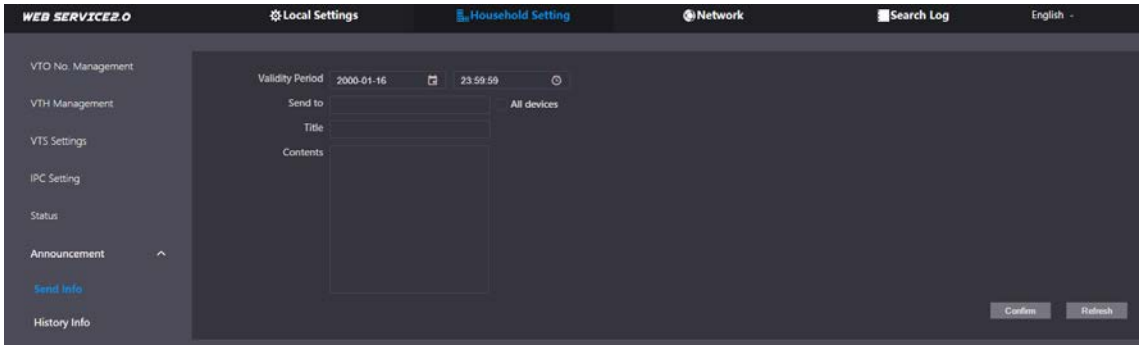
Publicar información

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

5.6.1 Enviar información

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

Enviar información



Especificar el**Periodo de validez**que el mensaje será válido.

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.

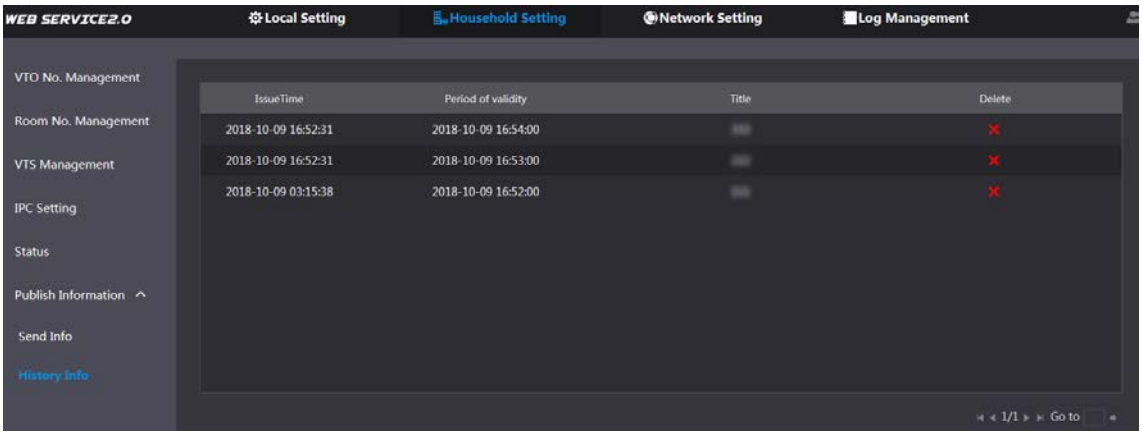
Hacer clic**Confirmar**.

5.6.2 Información histórica

Puede ver la información de los mensajes enviados.

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

Información histórica



6 Red

Este capítulo presenta cómo configurar los parámetros de red.

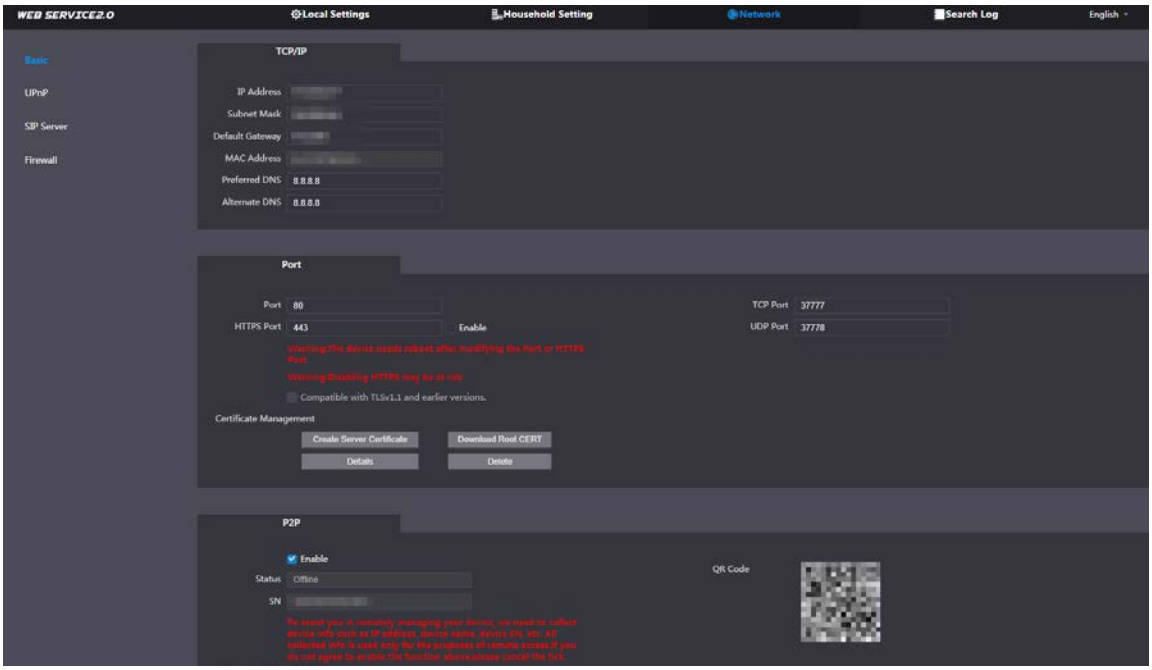
Básico

6.1.1 TCP/IP

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

Seleccionar**Red > Básica**.

TCP/IP y puerto



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 de parámetros

Parámetro	Descripción
Puerto	80 por defecto. Si ya está en uso, elija cualquier número entre 1025 y 65535 según sea necesario. Puede ingresar*http://VTO Dirección IP:Puerto*para iniciar sesión en el VTO.
Puerto HTTPS	Habilítelo y haga clic**Ahorrar**Ya puedes entrar*https://VTO Dirección IP: Puerto HTTPS*para iniciar sesión en el VTO.
Puerto TCP/UDP	Se utiliza para acceder al VTO con dispositivos en otras redes. Consulte "6.2 UPnP" para obtener más detalles.
Crear Servidor	Identificación digital única de VTO para el protocolo SSL. Para uso por primera vez

Parámetro	Descripción
Certificado	o después de cambiar la dirección IP del VTO, debe realizar este proceso. Si elimina el certificado que se ha creado, no se podrá deshacer.
Descargar Root CERT	Si está utilizando una PC que nunca ha iniciado sesión en VTO, debe descargar el certificado raíz, hacer doble clic para instalarlo y luego puede usar la función HTTPS mencionada anteriormente. Si elimina el certificado que se ha instalado, no podrá deshacer la acción.

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.

Si lo configuras**Tipo de dispositivo**a**Apartamento pequeño**(ver "4.1 Básico"), el código QR se reubicará en **Entorno del hogar > Gestión de VTH.**Hacer clic de cualquier número de habitación, y luego podrás ver tanto el número de serie como el código QR del VTO.

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

Seleccionar**Red > UPnP**.

Habilite los servicios enumerados según sea necesario.

Seleccione**Permitir**.

Hacer clic**Ahorrar**.

6.2.2 Agregar servicios UPnP

Seleccionar**Red > UPnP**.

Hacer clic**Agregar**.

Configure los parámetros según sea necesario.

Agregar un servicio UPnP

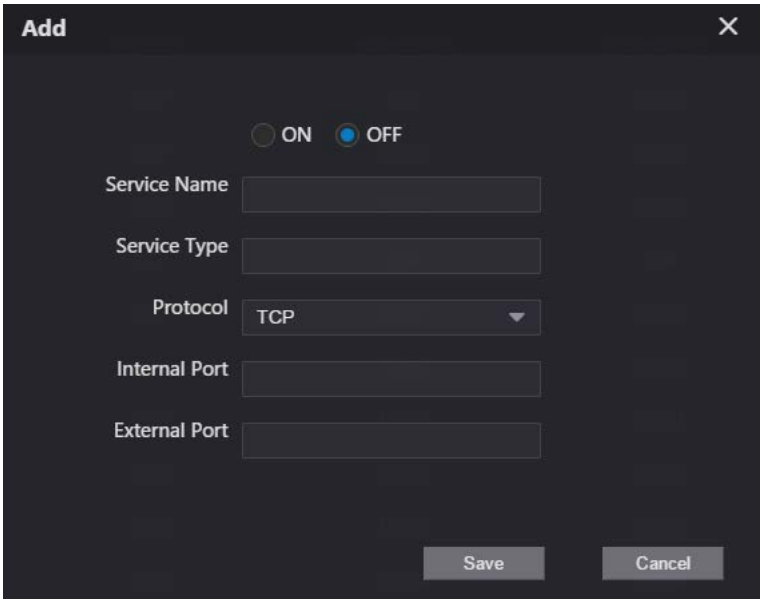


Tabla 6-2 Descripción de parámetros

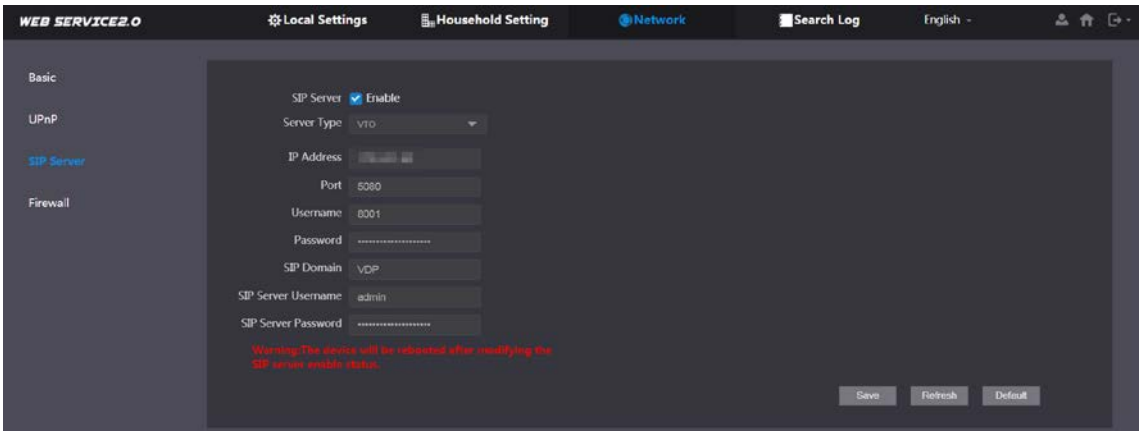
Parámetro	Descripción
Nombre del servicio	Ingrese la información según sea necesario.
Tipo de servicio	
Protocolo	Seleccionar**Protocolo de control de tráfico**o**Unión Popular de Palestina**según sea necesario.
Puerto interno	Utilice el número de puerto del 1024 al 5000. - No utilice el número de puerto 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 deben ser el mismo.
Puerto externo	

Servidor SIP

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

Seleccionar**Red > Servidor SIP**.

Servidor SIP



Seleccione un tipo de servidor según sea necesario.

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

  Permitir**Servidor SIP**y haga clic**Ahorrar**y luego se reiniciará el VTO. 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 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 servidor**a**VTO**, configure los parámetros y luego haga clic en**Ahorrar**.

Tabla 6-3 Configuración del servidor SIP

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

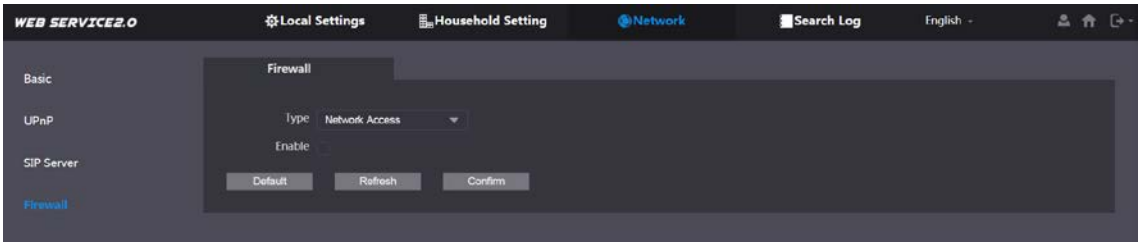
- Si otros servidores funcionan como servidor SIP:

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

Cortafuegos

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

Seleccionar**Red > Cortafuegos**.



Seleccione uno o más tipos de firewall y habilítelos.

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 bloqueo**y luego agregue una dirección IP o un segmento al que se le permita o deniegue el acceso al VTO.
PING Prohibido	El VTO no responderá al ping para evitar ataques de ping.
Anti-semijunta	Protege el rendimiento de VTO al bloquear los paquetes SYN excesivos.

7 Gestión de registros

Seleccionar**Registro de búsqueda**, y luego podrá ver el historial de llamadas, registros de alarmas, registros de desbloqueo y varios registros del sistema, y exportarlos a su PC según sea necesario.

Si el almacenamiento está lleno, se sobrescribirán los registros más antiguos. Realice copias de seguridad de los registros según sea necesario.

Recomendaciones de ciberseguridad

La ciberseguridad es más que una palabra de moda: es algo que concierne 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 ofrecen 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 caracteres; los tipos de caracteres incluyen letras mayúsculas y minúsculas, números y símbolos;
- No contenga el nombre de la cuenta ni el nombre de la cuenta en orden
- inverso; No utilice caracteres continuos, como 123, abc, etc.;
- No utilice caracteres superpuestos, como 111, aaa, etc.;

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

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

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

Le sugerimos que proteja físicamente el dispositivo, especialmente los dispositivos de almacenamiento. Por ejemplo, coloque el dispositivo en una sala de computadoras y un gabinete especiales e implemente un control de acceso y una gestión de claves bien hechos para evitar que personal no autorizado realice contactos físicos, como dañar el hardware, conectar sin autorización dispositivos extraíbles (como un disco flash USB, un puerto serial), etc.

2. Cambie las contraseñas periódicamente

Le sugerimos que cambie sus contraseñas periódicamente para reducir el riesgo de que sean adivinadas o descifradas.

3. Establezca y actualice la información de restablecimiento de contraseñas de manera oportuna

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

4. Habilitar bloqueo de cuenta

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

5. Cambiar el puerto HTTP predeterminado y otros puertos de servicio

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

6. Habilitar HTTPS

Le sugerimos que habilite HTTPS, para que pueda visitar 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. Asignar cuentas y privilegios de manera razonable

Según los requisitos comerciales y de gestión, agregue usuarios de manera razonable y asígneles un conjunto mínimo de permisos.

9. Desactivar servicios innecesarios y elegir 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 autenticación seguras.
- SMTP: Elija TLS para acceder al servidor de buzón. FTP:
- Elija SFTP y configure contraseñas seguras.
- Punto de acceso AP: elija el modo de cifrado WPA2-PSK y configure contraseñas seguras.

10. Transmisión de audio y vídeo encriptados

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

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

11. Auditoría segura

- Comprobar usuarios en línea: le sugerimos que compruebe periódicamente los usuarios en línea para ver si el dispositivo ha iniciado sesión sin autorización.
- Comprobar 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 que habilite la función de registro de red para garantizar que los registros críticos se sincronicen con el servidor de registro de red para realizar el seguimiento.

13. Construya un entorno de red seguro

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

- Deshabilite la función de mapeo de puertos del enrutador para evitar el acceso directo a los dispositivos de intranet desde la red externa.
- La red debe estar dividida y aislada de acuerdo con las necesidades reales de la red. Si no hay requisitos de comunicación entre dos subredes, se recomienda utilizar VLAN, GAP de red y otras tecnologías para dividir la red, a fin de lograr el efecto de aislamiento de la red.
- Establecer 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 a los que se les permite acceder al dispositivo.