Terminal de llamada de emergencia

Manual del usuario



Versión 1.0.0

Prefacio

Este manual presenta las configuraciones de la página web del terminal de llamadas de emergencia. Lea atentamente antes de utilizar el dispositivo y guarde el manual para futuras consultas.

Instrucciones de seguridad

Las siguientes palabras de advertencia pueden aparecer en el manual.

Palabras de señal	Significado
DANGER	Indica un alto riesgo potencial que, si no se evita, provocará la muerte o lesiones graves.
WARNING	Indica un peligro potencial medio o bajo que, si no se evita, podría provocar lesiones leves o moderadas.
CAUTION	Indica un riesgo potencial que, si no se evita, podría provocar daños a la propiedad, pérdida de datos, reducciones en el rendimiento o resultados impredecibles.
	Proporciona métodos para ayudarle a resolver un problema o ahorrar tiempo.
NOTE	Proporciona información adicional como complemento al texto.

Historial de revisiones

Versión	Contenido de la revisión	Hora de lanzamiento
Versión 1.0.0	Primer lanzamiento.	Octubre de 2023

Aviso de protección de la privacidad

Como usuario del dispositivo o responsable del tratamiento de datos, es posible que recopile datos personales de otras personas, como su rostro, audio, huellas dactilares y número de matrícula. Debe cumplir con las leyes y regulaciones locales de protección de la privacidad para proteger los derechos e intereses legítimos de otras personas mediante la implementación de medidas que incluyen, entre otras: Proporcionar una identificación clara y visible para informar a las personas de la existencia del área de vigilancia y proporcionar la información de contacto requerida.

Acerca del manual

- El manual es solo de referencia. Pueden existir ligeras diferencias entre el manual y el producto.
- No seremos responsables de pérdidas ocasionadas por el uso del producto de formas 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 del usuario en papel, utilice nuestro CD-ROM, escanee el código QR o visite nuestro sitio web oficial. El manual es solo para referencia. Pueden encontrarse ligeras diferencias entre la versión electrónica y la versión en papel.

- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto pueden provocar que aparezcan algunas diferencias entre el producto real y el manual. Póngase en contacto con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria.
- Puede haber errores de impresión o desviaciones en la descripción de las funciones, operaciones y datos técnicos. En caso de duda o controversia, nos reservamos el derecho de 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 registradas y nombres de empresas en el manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, comuníquese con el proveedor o el servicio de atención al cliente si ocurre algún problema durante el uso del dispositivo.
- Si existe alguna incertidumbre o controversia, nos reservamos el derecho de explicación final.

Medidas de seguridad y advertencias importantes

Esta sección presenta contenido que cubre el manejo adecuado del dispositivo, la prevención de riesgos y la prevención de daños a la propiedad. Lea atentamente antes de usar el dispositivo y cumpla con las pautas al usarlo.

Requisitos de funcionamiento



- Compruebe si la fuente de alimentación es correcta antes de usarlo.
- No desconecte el cable de alimentación del costado del dispositivo mientras el adaptador esté encendido.
- Utilice el dispositivo dentro del rango nominal de entrada y salida de energía.
- Transporte, utilice y almacene el dispositivo en condiciones de humedad y temperatura permitidas.
- Si el dispositivo permanece apagado durante más de un mes, debe colocarse en su paquete original y sellarse. Asegúrese de mantenerlo alejado de la humedad y almacenarlo en condiciones de humedad y temperatura permitidas.
- No deje caer ni salpique líquidos sobre el dispositivo y asegúrese de que no haya ningún objeto lleno de líquido sobre el dispositivo que evite que el líquido fluya hacia él.
- No desmonte el dispositivo sin instrucción profesional.

Requisitos de instalación



- No conecte el adaptador de corriente al dispositivo mientras el adaptador esté encendido.
- Cumpla estrictamente con los códigos y normas de seguridad eléctrica locales. Asegúrese de que el voltaje ambiental sea estable y cumpla con los requisitos de suministro de energía del dispositivo.
- No conecte el dispositivo a dos o más tipos de fuentes de alimentación, para evitar dañar el dispositivo.
- El uso inadecuado de la batería podría provocar un incendio o una explosión.



- El personal que trabaja en altura debe tomar todas las medidas necesarias para garantizar su seguridad personal, incluido el uso de casco y cinturones de seguridad.
- No coloque el dispositivo en un lugar expuesto a la luz solar o cerca de fuentes de calor.
- Mantenga el dispositivo alejado de la humedad, el polvo y el hollín.
- Instale el dispositivo sobre una superficie estable para evitar que se caiga.
- Instale el dispositivo en un lugar bien ventilado y no bloquee su ventilación.
- Utilice un adaptador o una fuente de alimentación de armario proporcionada por el fabricante.
- Utilice los cables de alimentación recomendados para la región y que cumplan con las especificaciones de potencia nominal.
- La fuente de alimentación debe cumplir con los requisitos de ES1 en la norma IEC 62368-1 y no ser superior a PS2. Tenga en cuenta que los requisitos de la fuente de alimentación están sujetos a la etiqueta del dispositivo.
- El dispositivo es un aparato eléctrico de clase I. Asegúrese de que la fuente de alimentación del dispositivo esté conectada a una toma de corriente con toma de tierra.

Tabla de contenido

Prólogo..... I

Medidas de seguridad y advertencias importantes..... III 1

Introducción..... 1

2 Estructura.....2

2.1 Panel frontal..... 2

2.2 Panel trasero.....5

2.3 Cableado de funciones..... 7

3 Instalación..... 8

3.1 Montaje en superficie..... 8

3.2 Montaje empotrado.....9

4 Operaciones en la página web..... 11

4.1 Inicialización..... 11

4.2 Inicio de sesión en la página web.....11

4.3 Restablecimiento de contraseña..... 12

4.4 Introducción a la página de inicio..... 13

4.5 Configuración local..... 14

4.5.1 Configuración de ajustes básicos..... 14

4.5.2 Configuración de parámetros del intercomunicador..... 15

4.5.3 Configuración de parámetros de audio..... 15

4.5.4 Configuración de la vinculación de alarmas..... 17

4.5.5 Gestión de la fuente de alimentación..... 18

4.6 Configuración de la red.....18

4.6.1 Configuración de TCP/IP..... 18

4.6.2 Configuración del puerto.....20

4.6.3 Configuración de FTP.....21

4.6.4 Adición de VTA..... 21

4.6.5 Configuración de UPnP.....24

4.6.6 Configuración de servicios básicos..... 25

4.7 Gestión del sistema.....27

4.7.1 Configuración de parámetros de vídeo.....27

4.7.2 Configuración de la hora.....32

4.7.3 Agregar usuario ONVIF.....33

4.7.4 Configuración del almacenamiento.....34

4.8 Centro de mantenimiento..... 35

4.8.1 Diagnóstico con un solo clic..... 35

4.8.2 Información del sistema.....35

4.8.3 Registro..... 36

4.8.4 Gestión.....37
4.8.5 Actualización.....39
4.8.6 Mantenimiento avanzado..... 40
4.9 Búsqueda de registros..... 40
4.10 Búsqueda de imágenes.....41
4.11 Seguridad.....42
4.11.1 Estado de seguridad.....42
4.11.2 Configuración del servicio del sistema..... 44
4.11.3 Defensa de ataque..... 44
4.11.4 Configuración del certificado CA.....48
4.11.5 Configuración del cifrado de vídeo..... 52
4.11.6 Configuración de advertencias de seguridad.....53
4.11.7 Configuración de la autenticación de seguridad..... 53
Apéndice 1 Recomendaciones de ciberseguridad..... 55

1 Introducción

El terminal de llamada de emergencia se utiliza para llamar en caso de emergencia, transmitir y monitorear mediante la conexión con la plataforma o el centro de recepción de alarmas. Es aplicable en escuelas, aeropuertos, fábricas y áreas escénicas donde se necesitan métodos convenientes para buscar ayuda.

2 Estructura

La apariencia y los puertos pueden variar según los modelos reales. Las siguientes imágenes son solo de referencia.

2.1 Panel frontal

Serie VTA-2501G

Figura 2-1 Panel frontal

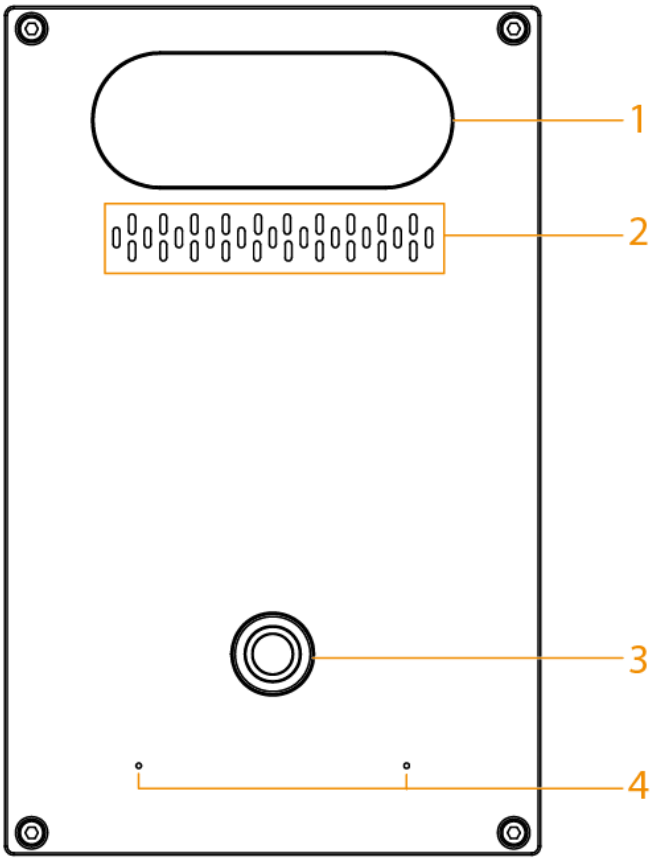


Tabla 2-1 Descripción del panel frontal

No.	Nombre del componente	Descripción
1	Cámara	Recopila imágenes de vídeo.
2	Vocero	Salida de audio.
3	Botón de emergencia	Pulse el botón para llamar al centro de gestión.

No.	Nombre del componente	Descripción
4	Micrófono	Recopila audio y admite intercomunicador de voz bidireccional.

Serie VTA-2502G (montaje en superficie)

Figura 2-2 Panel frontal

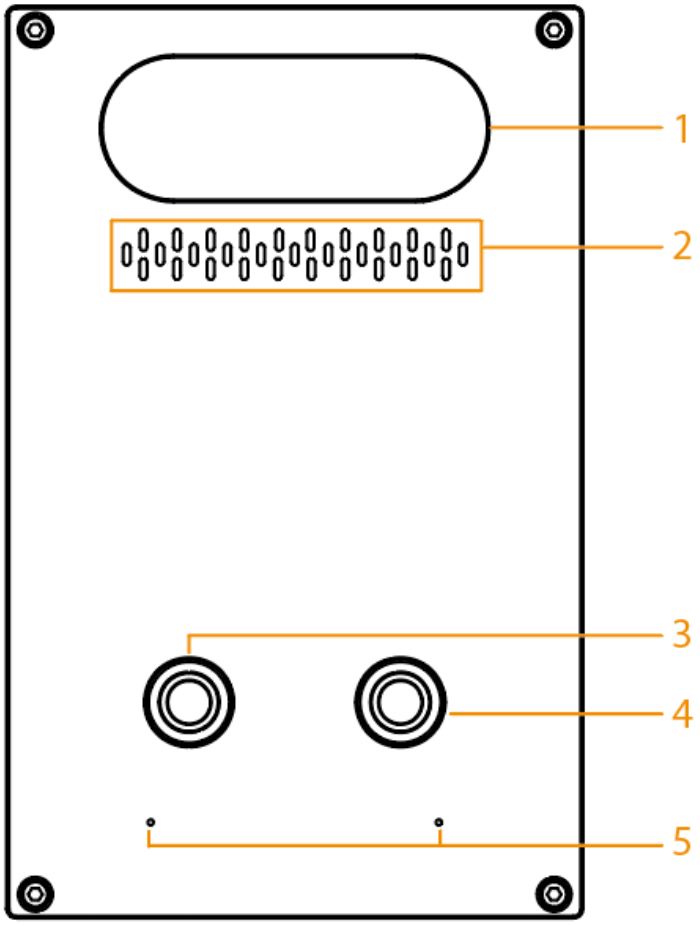


Tabla 2-2 Descripción del panel frontal

No.	Nombre del componente	Descripción
1	Cámara	Recopila imágenes de vídeo.
2	Vocero	Salida de audio.
3	Botón de emergencia	Pulse el botón para llamar al centro de gestión.
4	Botón de llamada	Pulse el botón para llamar al centro de gestión.
5	Micrófono	Recopila audio y admite intercomunicador de voz bidireccional.

Serie VTA-2502G (montaje empotrado)

Figura 2-3 Panel frontal

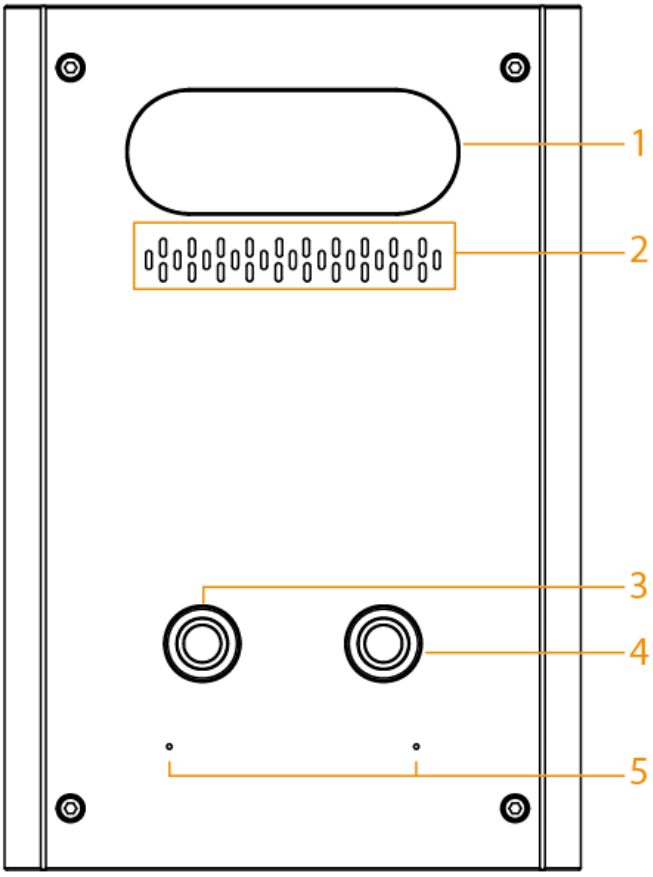


Tabla 2-3 Descripción del panel frontal

No.	Nombre del componente	Descripción
1	Cámara	Recopila imágenes de vídeo.
2	Vocero	Salida de audio.
3	Botón de emergencia	Pulse el botón para llamar al centro de gestión.
4	Botón de llamada	Pulse el botón para llamar al centro de gestión.
5	Micrófono	Recopila audio y admite intercomunicador de voz bidireccional.

Serie VTA-2511G

Figura 2-4 Panel frontal

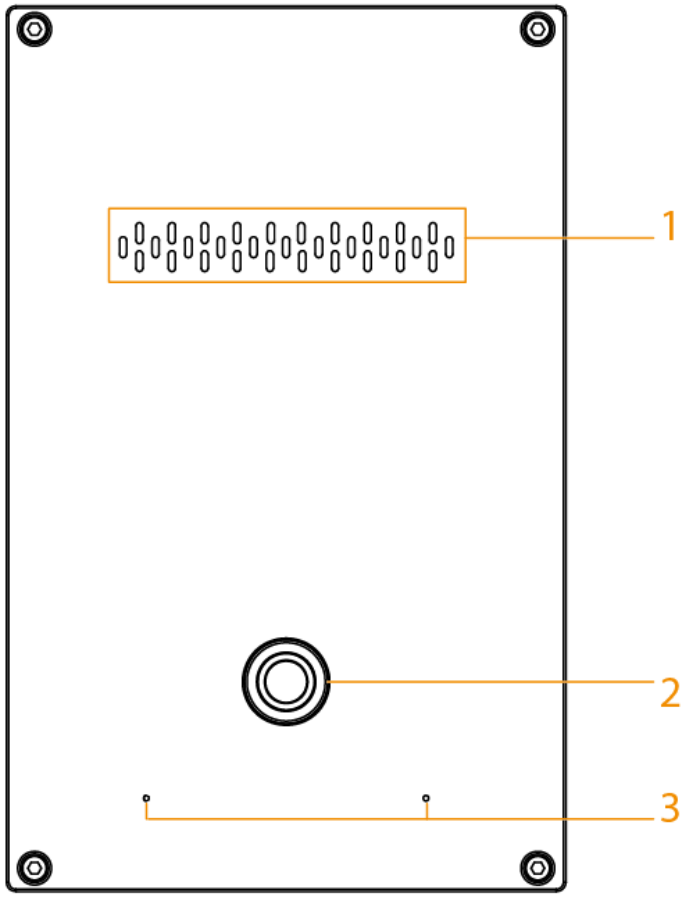


Tabla 2-4 Descripción del panel frontal

No.	Nombre del componente	Descripción
1	Vocero	Salida de audio.
2	Botón de emergencia	Pulse el botón para llamar al centro de gestión.
3	Micrófono	Recopila audio y admite intercomunicador de voz bidireccional.

2.2 Panel trasero

Los paneles traseros de los diferentes modelos son iguales.

Figura 2-5 Panel trasero

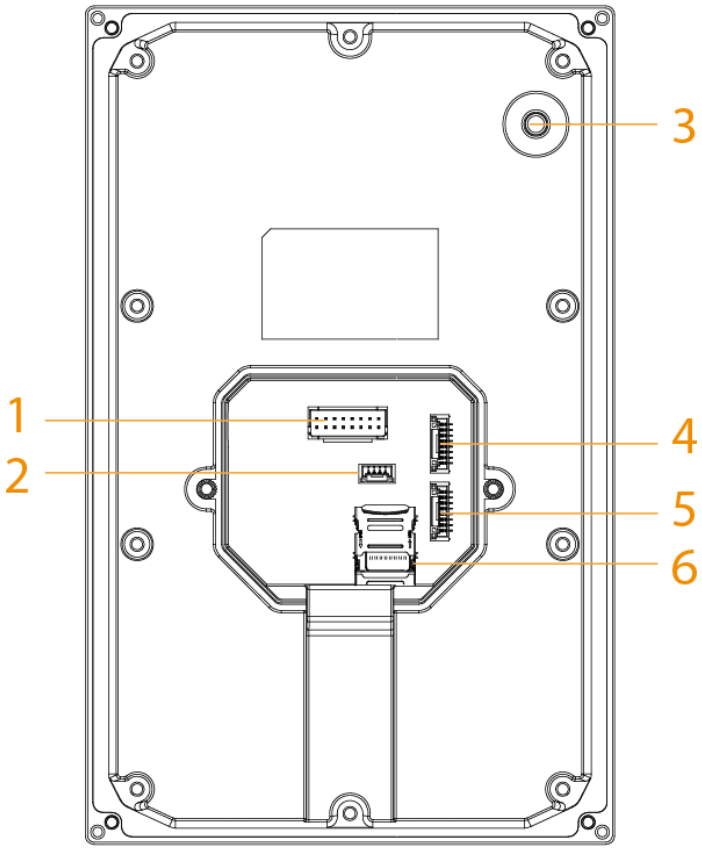


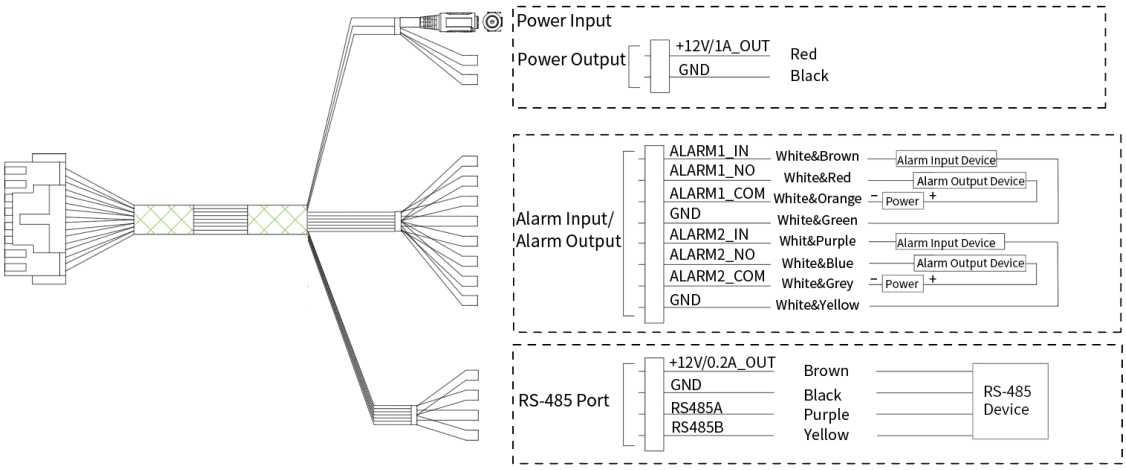
Tabla 2-5 Descripción del panel trasero

No.	Componentes y Puertos	Descripción
1	Puerto de cable de función	El puerto incluye entrada de alarma, salida de alarma, entrada de alimentación (12 VCC), salida de alimentación y puerto RS-485. Conecte el cable de función estándar. Para obtener más detalles, consulte "2.3 Cableado del cable de función".
2	Extensión de audio Puerto	Puertos de entrada y salida de audio. Conecte el cable de audio estándar.
3	Botón de manipulación	Cuando se retira el dispositivo de la pared, se activa una alarma anti-retirada.
4	Puerto de red	Conecte el cable de red estándar.
5	Puerto de red (PoE)	Fuente de alimentación PoE estándar. Conecte el cable de red estándar.

No.	Componentes y **Puertos**	Descripción
6	Puerto para tarjeta SD	Inserte la tarjeta SD para almacenar archivos de video e imágenes. La capacidad máxima es de 512 GB. No se admite el intercambio en caliente. Sólo VTA250*incógnita*La serie G admite esta función.

2.3 Cableado del cable de función

Figura 2-6 Cableado



3 Instalación

⚠

- Evite instalar el terminal de llamada de emergencia en entornos adversos, como condensación, altas temperaturas, aceite, polvo, corrosión química y luz solar directa, entre otros.
- Si se produce alguna anomalía después de encender el dispositivo, corte el suministro eléctrico y desconecte el cable de red. Vuelva a encender el dispositivo después de solucionar el problema.
- La instalación y la depuración del dispositivo deben ser realizadas por personal profesional. En caso de que el dispositivo presente algún error, no lo desarme ni lo repare usted mismo. Póngase en contacto con el departamento de posventa.

3.1 Montaje en superficie

Procedimiento

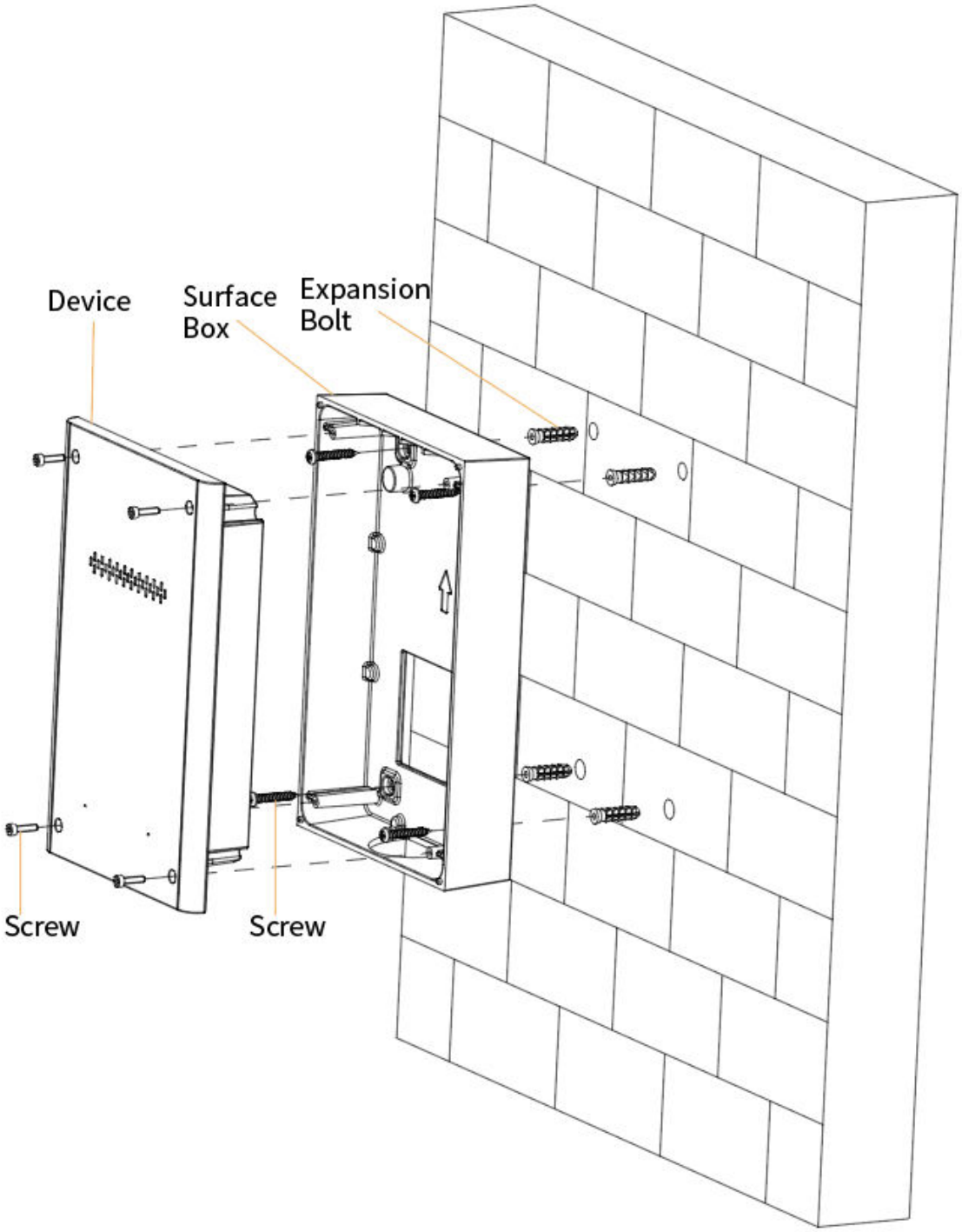
Paso 1 Perfore 4 agujeros en la pared de acuerdo con la posición de los agujeros en la caja de superficie y luego martille los pernos de expansión.

Paso 2 Fije la caja de superficie a la pared con 4 tornillos.

Paso 3 Conecte los cables. Para obtener más información, consulte "2.3 Cableado de

Paso 4 funciones". Fije el dispositivo a la caja de superficie con 4 tornillos.

Figura 3-1 Montaje en superficie



3.2 Montaje empotrado

Procedimiento

Paso 1 Ranura en la pared según dimensiones de la caja de empotrar.

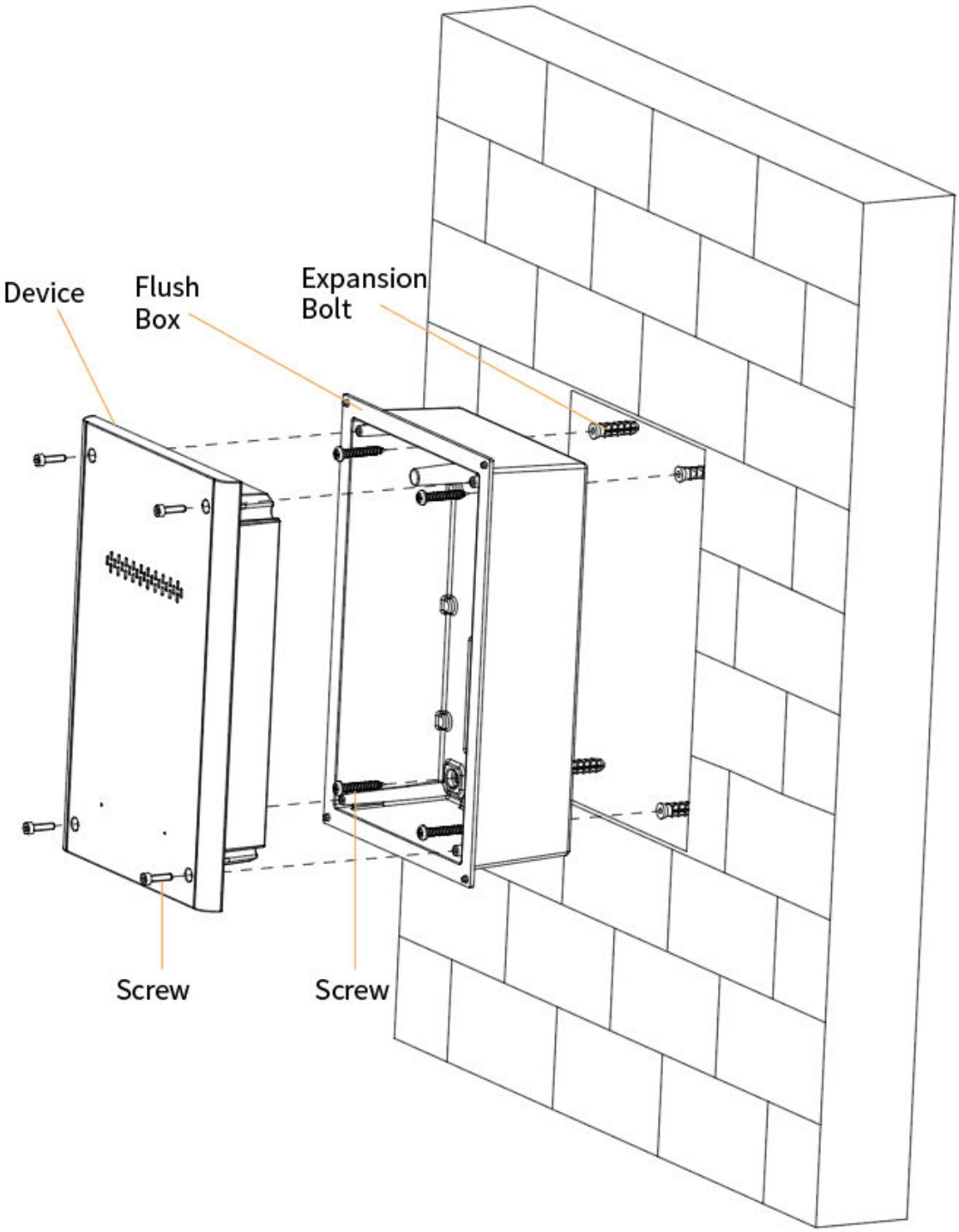
Paso 2 Perfore 4 agujeros en la ranura de acuerdo con la posición de los agujeros en la caja de empotrar y luego martille los pernos de expansión.

Paso 3 Fije la caja de empotrar en la pared con 4 tornillos.

Paso 4 Conecte los cables. Para obtener más información, consulte "2.3 Cableado de funciones".

Paso 5 Fije el dispositivo en la caja empotrada con 4 tornillos.

Figura 3-2 Montaje empotrado



4 Operaciones en la página web

4.1 Inicialización

Inicialice el dispositivo para iniciar sesión por primera vez o cuando inicie sesión en el dispositivo después de restaurarlo a la configuración de fábrica.

Prerrequisitos

Asegúrese de que la computadora esté en el mismo segmento de red que la terminal de llamada de emergencia.

Procedimiento

Paso 1 Ingrese la dirección IP del terminal de llamada de emergencia en un navegador y luego presione la tecla Enter.



- La dirección IP predeterminada para el adaptador de red 1 es 192.168.1.108. La dirección IP predeterminada para el adaptador de red 2 es 192.168.2.108.
- Le recomendamos que utilice Google Chrome con la versión 100 o posterior, o Firefox con la versión 100 o posterior.

Paso 2 Seleccione el idioma.

Paso 3 Ingrese la contraseña y la dirección de correo electrónico y luego haga clic en**Hecho**.



- La contraseña debe constar de 8 a 32 caracteres que no sean espacios en blanco y contener al menos dos tipos de los siguientes caracteres: mayúsculas, minúsculas, números y caracteres especiales (excepto ' " ; : &). Establezca una contraseña de alta seguridad siguiendo las indicaciones de seguridad de la contraseña.
- Mantenga la contraseña segura después de la inicialización y cámbiela periódicamente para mejorar la seguridad.
- Ingrese la dirección de correo electrónico y si olvida la contraseña, podrá recibir el código de seguridad a través del correo electrónico.

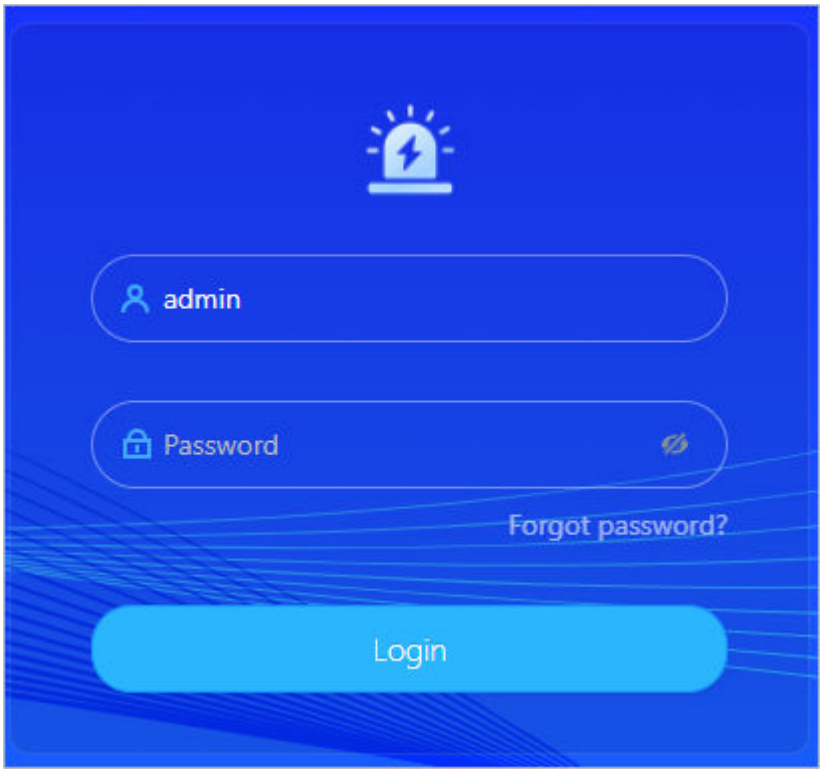
4.2 Iniciar sesión en la página web

Procedimiento

Paso 1 Introduzca la dirección IP del dispositivo en un navegador y, a continuación, pulse la tecla Enter. Introduzca

Paso 2 el nombre de usuario y la contraseña.

Figura 4-1 Iniciar sesión



- El nombre de usuario predeterminado del administrador es**administración**La contraseña predeterminada es la que configuró durante la inicialización. Le recomendamos que cambie la contraseña periódicamente.
- Si olvida la contraseña, haga clic en**¿Has olvidado tu contraseña?**Para restablecer la contraseña. Para obtener más información, consulte "4.3 Restablecimiento de contraseña".

Paso 3 Hacer clic**Acceso**.

4.3 Restablecimiento de contraseña

Restablezca la contraseña a través de la dirección de correo electrónico que vinculó si olvida la contraseña.

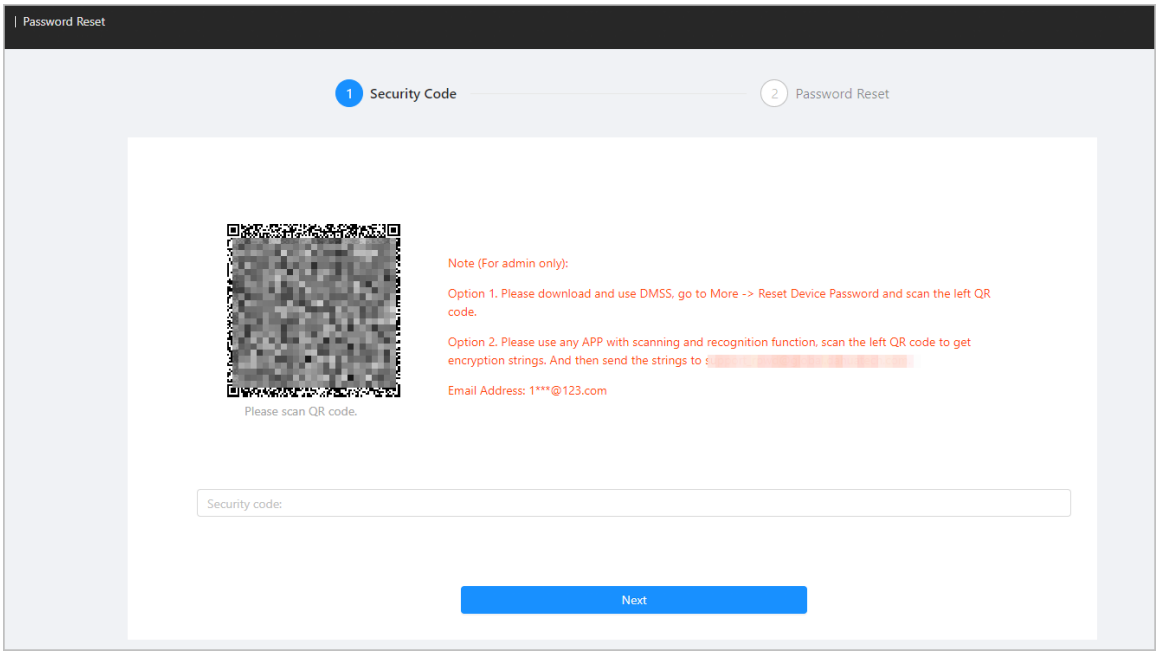
Procedimiento

Paso 1 En la página de inicio de sesión, haga clic en**¿Has olvidado tu**

Paso 2 **contraseña?** Hacer clic**DE ACUERDO**en la ventana emergente.

Paso 3 Escanee el código QR en la página y luego obtenga el código de seguridad.

Figura 4-2 Obtener el código de seguridad



- Se generarán un máximo de dos códigos de seguridad al escanear el mismo código QR. Si necesita obtener el código de seguridad nuevamente, actualice la página del código QR.
- Utilice el código de seguridad dentro de las 24 horas posteriores a su recepción. De lo contrario, el código de seguridad perderá su validez.
- La cuenta se bloqueará durante 5 minutos si ingresa el código de seguridad incorrecto 5 veces seguidas.

Paso 4 Ingresa el código de seguridad que recibiste. Haz clic

Paso 5 **Próximo**.

Paso 6 Restablecer nueva contraseña y confirmar la nueva contraseña.

La contraseña debe constar de 8 a 32 caracteres que no sean espacios en blanco y contener al menos dos tipos de caracteres entre números, letras y caracteres comunes (excluyendo espacios, ', ", ;, :, &).

Paso 7 Hacer clic**DE ACUERDO**.

4.4 Introducción a la página de inicio

El sistema va automáticamente a la página de inicio después de iniciar sesión.

Figura 4-3 Página de inicio

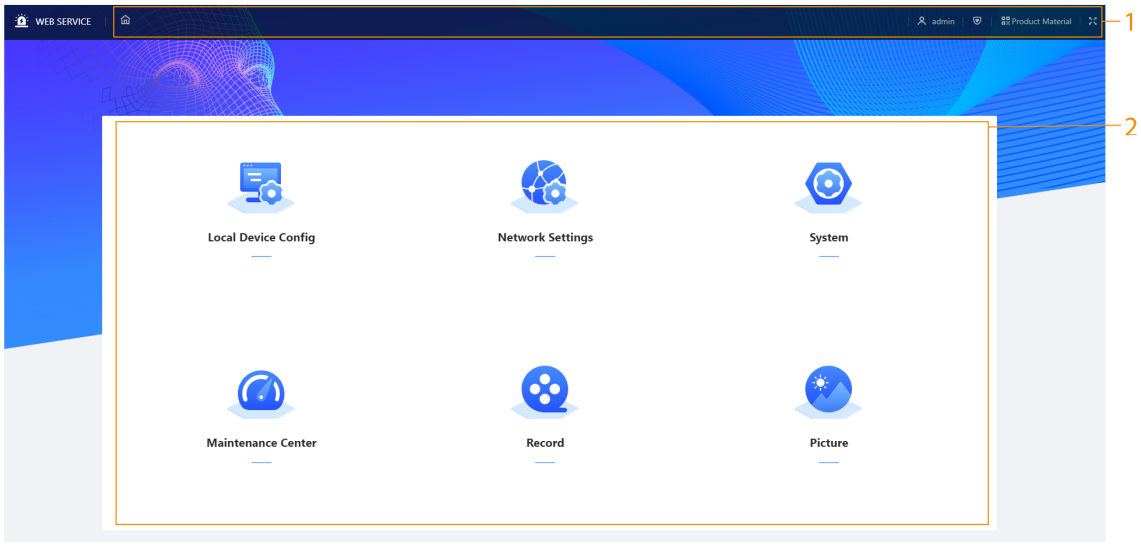


Tabla 4-1 Descripción de la página de inicio

No.	Parámetros e iconos		Descripción
1	Navegación Bar		Ir a la página de inicio.
		admin	• Haga clic en el icono. Seleccione**Cambiar la contraseña**,Ingrese la contraseña antigua y la nueva y luego haga clic en**DE ACUERDO**. • Haga clic en el icono. Seleccione**Reanudar**para reiniciar el dispositivo. • Haga clic en el icono. Seleccione**Cerrar sesión**para cerrar sesión en la cuenta.
			Vaya a la página de seguridad para ver el estado de seguridad.
		Producto Material	Haga clic para ver el código QR y luego escanee el código para obtener el documento del producto.
			Abra la ventana en modo de pantalla completa.
2	Menú de funciones		Menú de configuración de funciones del dispositivo. Las funciones pueden variar según los diferentes modelos.

4.5 Configuración local

4.5.1 Configuración de ajustes básicos

Procedimiento

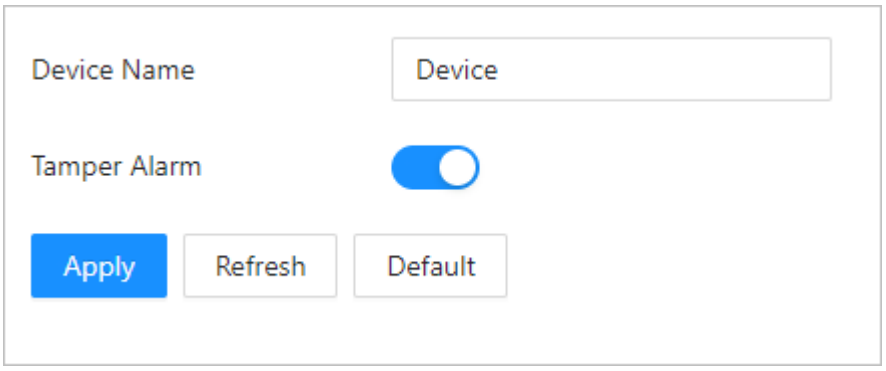
Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Configuración del dispositivo local**>**Configuración básica**.

Paso 3 Configure los parámetros y luego haga clic en**Aplicar**.

Alarma de manipulación:Cuando está habilitado, si el dispositivo se separa de la pared, se activa una alarma.

Figura 4-4 Configuración básica



4.5.2 Configuración de parámetros del intercomunicador

Procedimiento

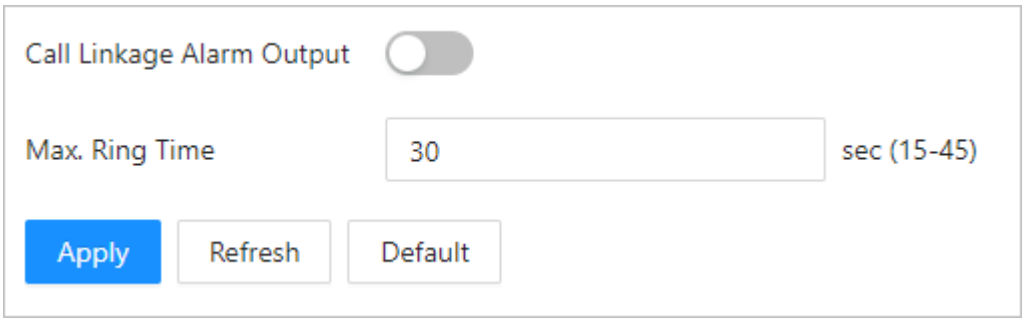
Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Configuración del dispositivo local**>**Intercomunicador**.

Paso 3 Configure los parámetros y luego haga clic en**Aplicar**.

- **Salida de alarma de enlace de llamada**:Cuando está habilitado, si presiona el botón de emergencia en el dispositivo, el dispositivo de salida de alarma conectado a**ALARMA1_NO**y**ALARMA1_COM** Los puertos estarán vinculados.
- **Tiempo máximo de llamada**:Configurar el tiempo de llamada para llamar al número de teléfono. Si no hay respuesta una vez transcurrido el tiempo, el dispositivo llamará al siguiente número.

Figura 4-5 Intercomunicador



4.5.3 Configuración de parámetros de audio

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Configuración del dispositivo local**>**Audio**.

Paso 3 Configure los parámetros y luego haga clic en**Aplicar**.

Figura 4-6 Audio

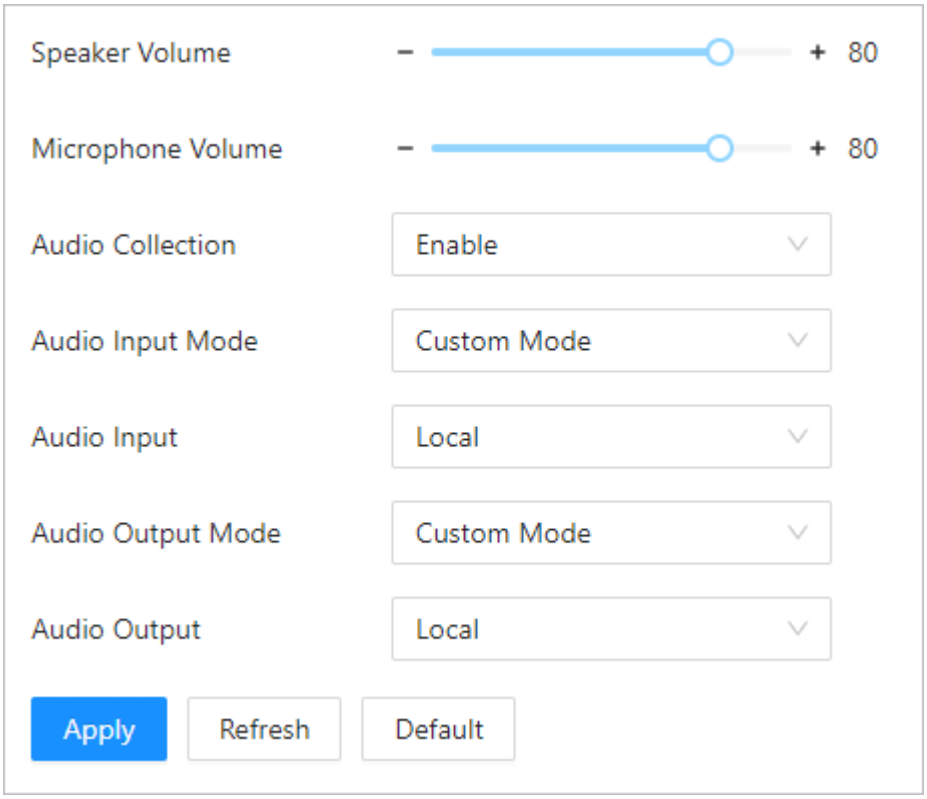


Tabla 4-2 Descripción de los parámetros de audio

Parámetros	Descripción
Volumen del altavoz	Arrastrar o haga clic+y–para ajustar el volumen del altavoz.
Volumen del micrófono	Arrastrar o haga clic+y–para ajustar el volumen de la voz recogida.
Colección de audio	Es**Permitir**De forma predeterminada, cuando está habilitado, se puede recopilar la voz.
Modo de entrada de audio	Modo personalizado.
Entrada de audio	• **Local**:Recoge la voz a través del micrófono del dispositivo. • **Periférico extendido**:Recoge la voz a través del dispositivo de audio extendido conectado al puerto de audio de 3,5 mm.
Modo de salida de audio	Modo personalizado.
Salida de audio	• **Local**:Reproducir la voz a través del altavoz del dispositivo. • **Periférico extendido**:Reproduzca la voz a través del dispositivo de audio extendido conectado al puerto de audio de 3,5 mm. • **Periféricos locales y extendidos**:Reproduzca la voz a través del altavoz del dispositivo y del dispositivo de audio extendido conectado al puerto de audio de 3,5 mm al mismo tiempo.

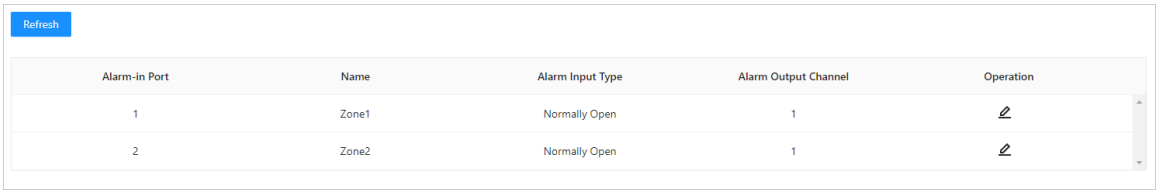
4.5.4 Configuración de la vinculación de alarmas

Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Configuración del dispositivo local**>**Configuración de vinculación de alarma**.

Figura 4-7 Vinculación de alarmas



Paso 3 Hacer clic para modificar los parámetros.

Figura 4-8 Modificar los parámetros

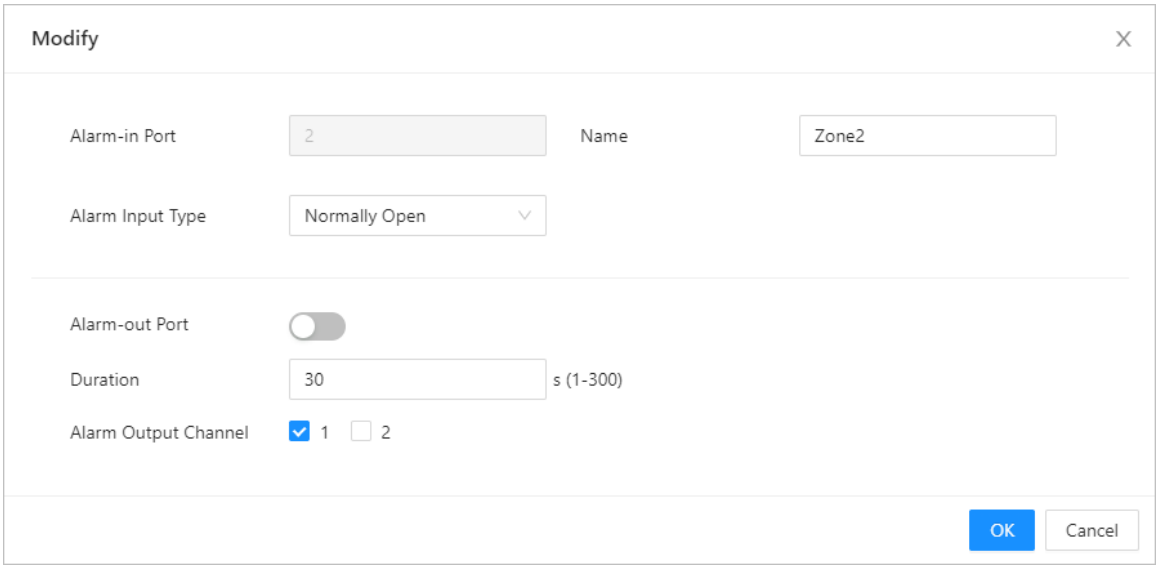


Tabla 4-3 Descripción de los parámetros de vinculación de alarmas

Parámetro	Descripción
Puerto de entrada de alarma	El número de puerto de entrada de alarma no se puede modificar.
Nombre	Personalizado.
Tipo de entrada de alarma	Seleccione el tipo según el dispositivo que haya adquirido. ● **Normalmente abierto**:El circuito del dispositivo de alarma normalmente está abierto y se cierra cuando se activa una alarma. ● **Normalmente cerrado**:El circuito del dispositivo de alarma normalmente está cerrado y se abre cuando se activa una alarma.
Puerto de salida de alarma	Si la salida de alarma está habilitada, el relé puede generar mensajes de alarma. Configure la duración de la alarma y luego seleccione el canal según los canales reales.
Duración	
Canal de salida de alarma	

Paso 4 Hacer clic**DE ACUERDO**.

4.5.5 Gestión de la fuente de alimentación

Si está habilitado, la salida de alimentación de 12 V/1 A está disponible.

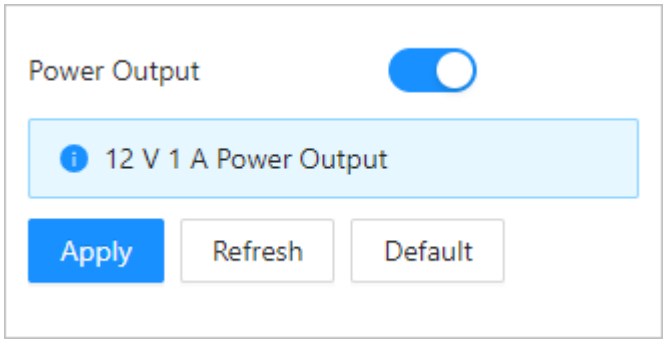
Procedimiento

Paso 1 Inicie sesión en la página web.

Paso 2 Seleccionar**Configuración del dispositivo local**>**Gestión de la fuente de**

Paso 3 **alimentación**. Permitir**Potencia de salida**,y luego haga clic**Aplicar**.

Figura 4-9 Potencia de salida



4.6 Configuración de la red

4.6.1 Configuración de TCP/IP

Procedimiento

Paso 1 Inicie sesión en la página web del dispositivo.

Paso 2 Seleccione**Configuración de red**>**Protocolo**

Paso 3 **TCP/IP**. Configure los parámetros.

Figura 4-10 Configurar los parámetros

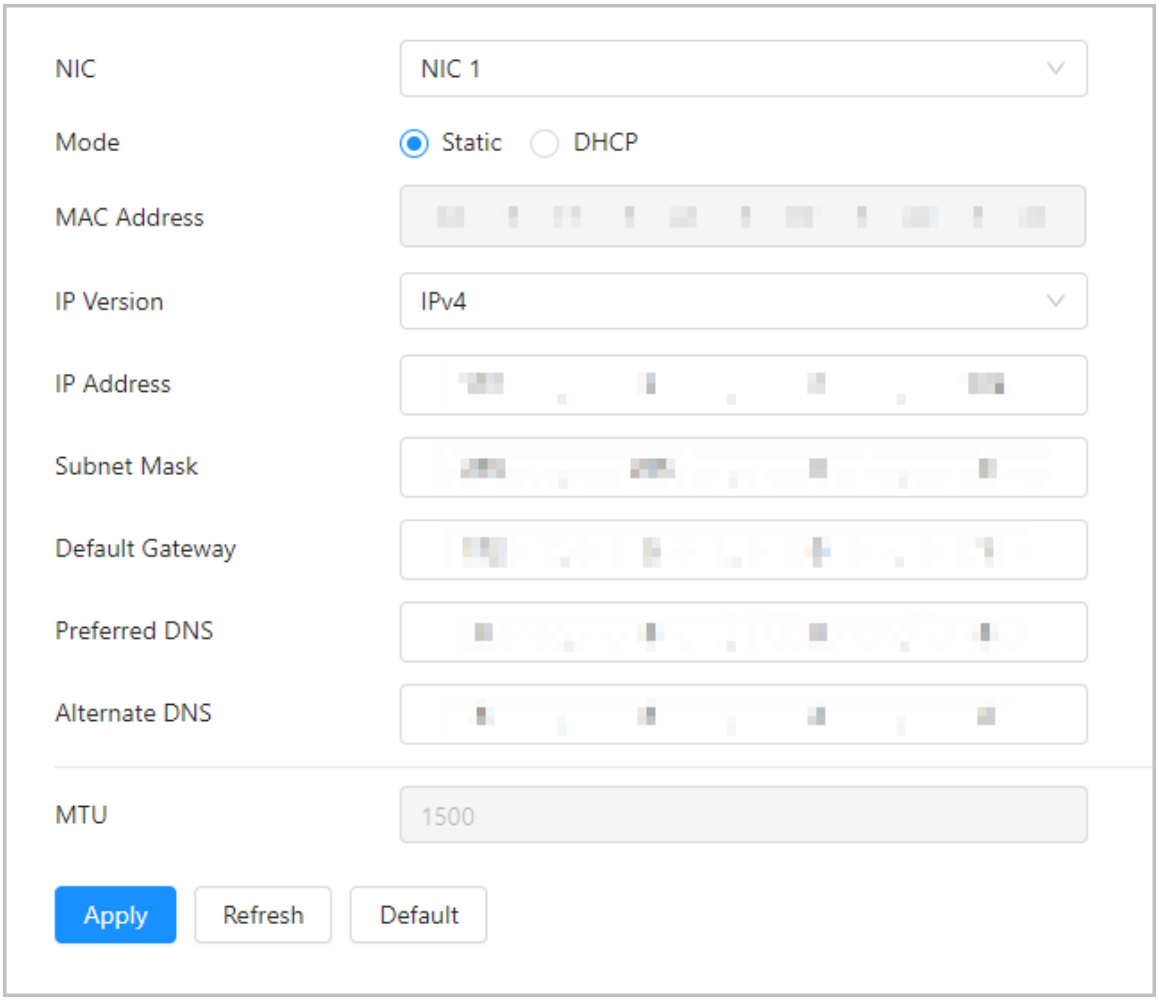


Tabla 4-4 Descripción de parámetros

Parámetro	Descripción
Modo	• Estático: configurar manualmente**Propiedad intelectual**,**Máscara de subred**y**Puerta de enlace predeterminada**Haga clic en**Aplicar**y la página web va automáticamente a la página de inicio de sesión de la IP que configuraste. • DHCP (Protocolo de configuración dinámica de host): seleccione**DHCP**Si hay un servidor DHCP, el dispositivo obtiene automáticamente una dirección IP dinámica.
Dirección MAC	Dirección MAC (Media Access Control) del dispositivo.
Versión IP	Seleccione de**IPv4**y**IPv6**.
Dirección IP Máscara de subred Puerta de enlace predeterminada	Si seleccionas**Estático**en**Modo**, ingrese la dirección IP, la máscara de subred y la puerta de enlace predeterminada de acuerdo con la planificación de la red. • No hay máscara de subred en la versión IPv6. • La dirección IP y la puerta de enlace predeterminada deben estar en la misma red segmento.
DNS preferido	Dirección IP del servidor DNS.
DNS alternativo	Dirección IP alternativa del servidor DNS.

Parámetro	Descripción
Unidad de medida máxima	Es 1.500 por defecto.

Paso 4 Hacer clic**Aplicar**.

4.6.2 Configuración del puerto

Puede limitar el acceso al terminal de llamadas de emergencia al mismo tiempo a través de la página web y el cliente de escritorio, y configurar los números de puerto del dispositivo.

Procedimiento

Paso 1 Inicie sesión en la página web del dispositivo.

Paso 2 Seleccione**Configuración de red**>**Puerto**.

Paso 3 Configurar los puertos.

Excepto**Conexión máxima**y**Puerto RTSP**, es necesario reiniciar el terminal de llamada de emergencia para que las configuraciones sean efectivas después de cambiar otros parámetros.

Figura 4-11 Configurar puertos

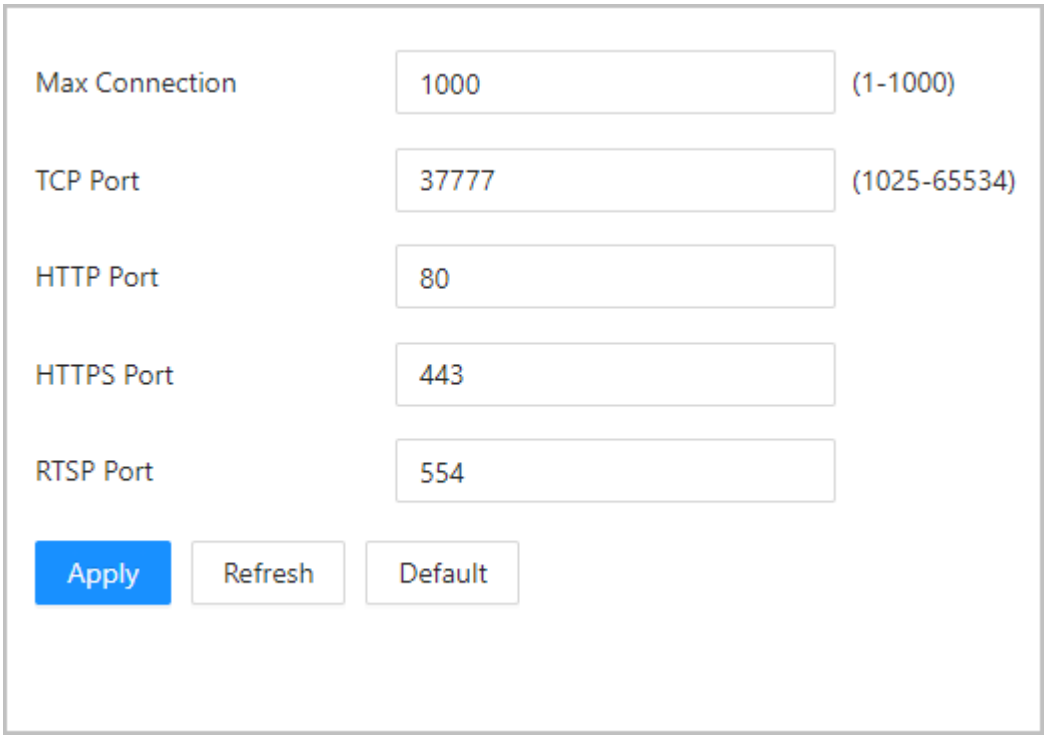


Tabla 4-5 Descripción de los puertos

Parámetro	Descripción
Conexión máxima	Establezca el número máximo de clientes (como página web y cliente de escritorio) que pueden acceder a la terminal de llamada de emergencia al mismo tiempo. Los clientes de plataforma como SmartPSS AC no se cuentan.

Parámetro	Descripción
Puerto TCP	El valor predeterminado es 37777.
Puerto HTTP	El valor predeterminado es 80. Si ha cambiado el número de puerto, agregue el número de puerto después de la dirección IP cuando acceda a la página web.
Puerto HTTPS	El valor predeterminado es 443.
Puerto RTSP	El valor predeterminado es 554.

Paso 4 Hacer clic**Aplicar**.

4.6.3 Configuración de FTP

Información de contexto

Cuando conecte el terminal de llamadas de emergencia con el VTS, configure los parámetros FTP en el VTS y luego cargue los archivos de transmisión al servidor FTP para su transmisión en el terminal de llamadas de emergencia. Después de la conexión, las configuraciones FTP en el terminal de llamadas de emergencia se sincronizarán con las configuraciones en el VTS.

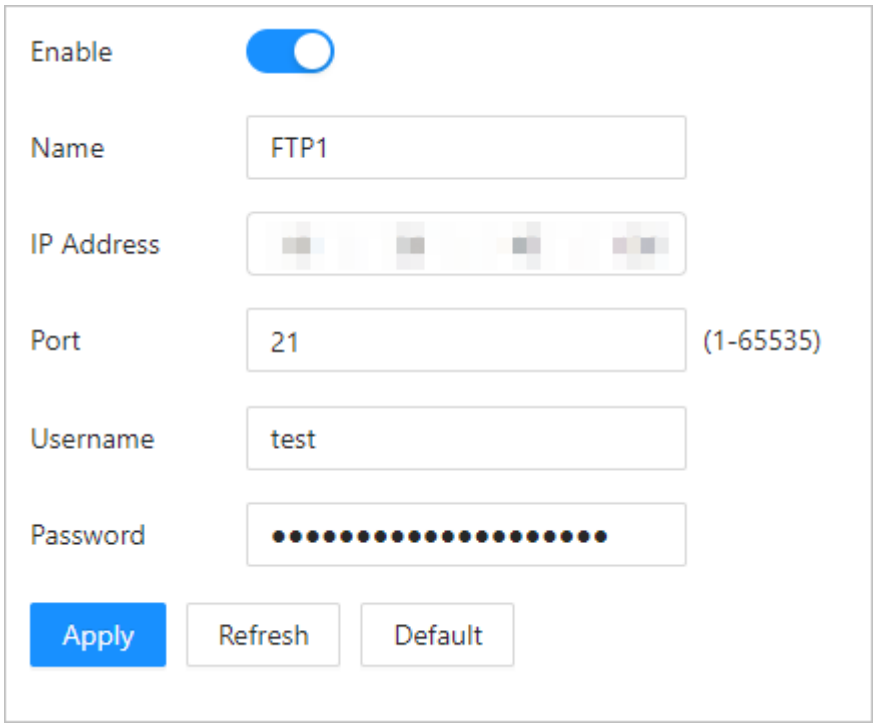
Procedimiento

Paso 1 Inicie sesión en la página web del dispositivo.

Paso 2 Seleccione**Configuración de red**>**FTP**.

Paso 3 Habilite la función, configure los parámetros y luego haga clic en**Aplicar**.

Figura 4-12 Configurar parámetros FTP



4.6.4 Agregar VTA

4.6.4.1 Agregar VTA mediante registro automático

Después de habilitar esta función, cuando el dispositivo se conecte a Internet, informará la ubicación actual al servidor especificado, como VTS, que actúa como tránsito para facilitar que el software del cliente acceda a la cámara.

Procedimiento

Paso 1 Inicie sesión en la página web del dispositivo. Seleccione

Paso 2 **Configuración de red**>**Registro automático**.

Paso 3 Haga clic en y luego configure los parámetros.

Figura 4-13 Registro automático

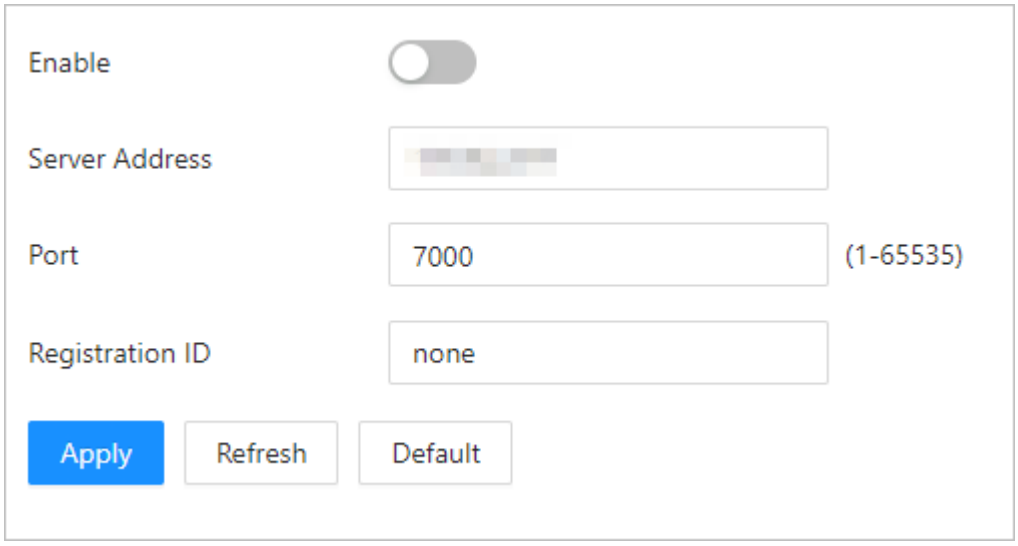


Tabla 4-6 Descripción de los parámetros de registro

Parámetro	Descripción
Dirección del servidor	La dirección IP o el nombre de dominio del servidor que se va a registrar. Por ejemplo, la dirección IP del VTS.
Puerto	El número de puerto del servidor que se registrará. El número de puerto del VTS es 9050.
ID de registro	Mantenga la coherencia con el ID de registro en el servidor. Cuando el VTS funciona como servidor, el ID de registro es el**Número de dispositivo** en la página web de VTS. Para más detalles, consulte "4.6.4.2 Agregar VTA a través de VTS".

Paso 4 Hacer clic**Aplicar**.

4.6.4.2 Agregar VTA a través de VTS

Procedimiento

Paso 1 Inicie sesión en la página web de VTS.

Paso 2 Seleccionar**Configuración del dispositivo**>**Gestión de**

Paso 3 **terminales**Haga clic en**Agregar**y luego configure los parámetros.

Figura 4-14 Agregar VTA

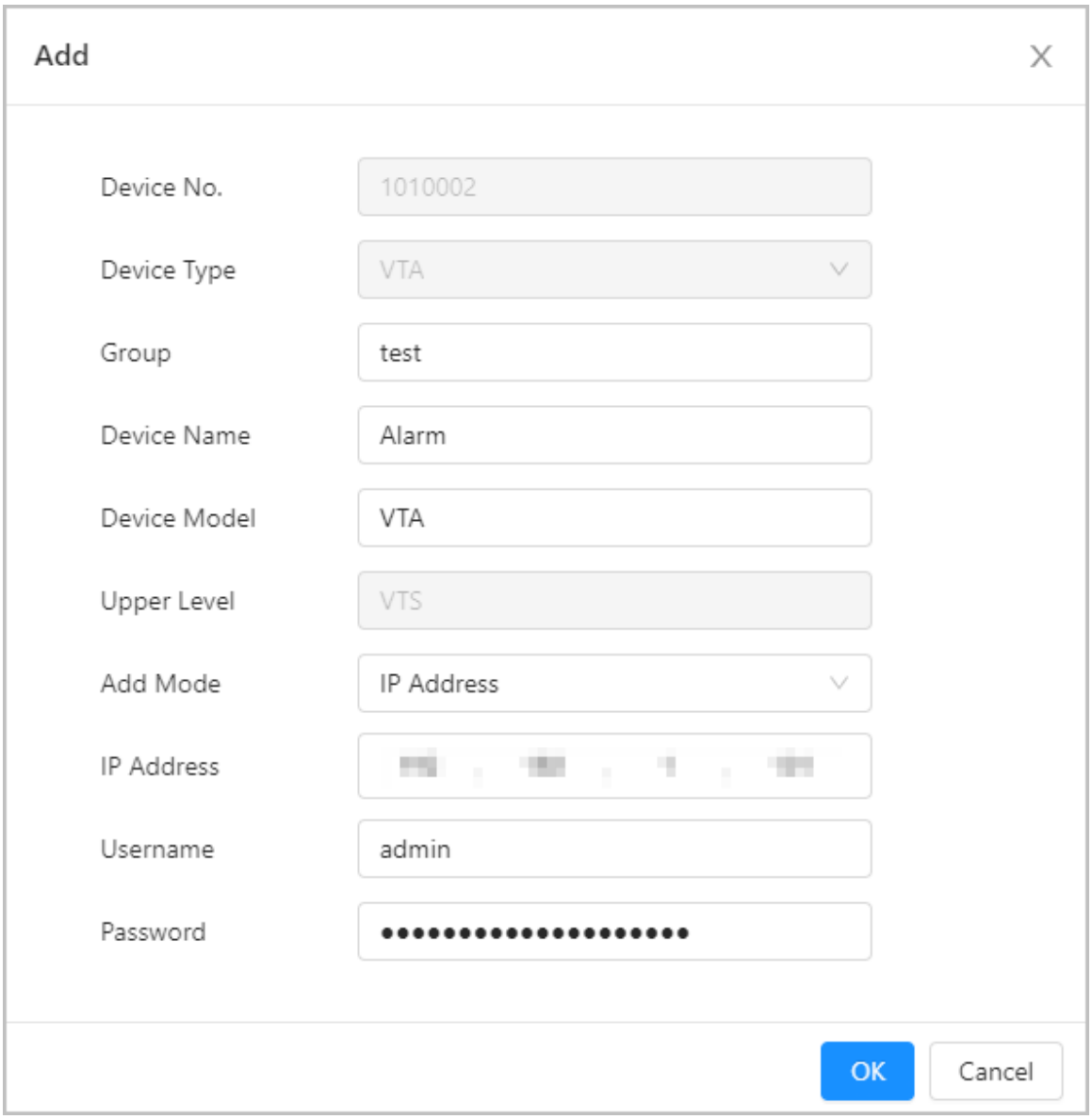


Tabla 4-7 Descripción de parámetros

Parámetro	Descripción
Número de dispositivo	Cuando se agrega el VTA a través del registro automático, el ID de registro en el VTA debe ser el mismo que el número de dispositivo aquí.
Grupo	Seleccionar**Monitor**>**Gestión de terminales**en el VTS local y luego podrá ver los dispositivos del grupo que configuró.

Parámetro	Descripción
Nombre del dispositivo	Definido por el usuario.
Modelo del dispositivo	Ingrese el modelo completo del dispositivo que puede obtener de la etiqueta del dispositivo.
Añadir modo	Puede agregar VTA de las siguientes 2 maneras. ● Dirección IP: Ingrese la dirección IP del VTA. ● Registrarse: Configure los parámetros para registrarse en el VTA.
Nombre de usuario	Introduzca el nombre de usuario y contraseña del VTA.
Contraseña	

Paso 4 Hacer clic**DE ACUERDO**.

4.6.5 Configuración de UPnP

UPnP (Universal Plug and Play) es un protocolo que establece una relación de mapeo entre la intranet y la extranet. Esta función le permite acceder a un dispositivo de la intranet a través de la dirección IP de la extranet.

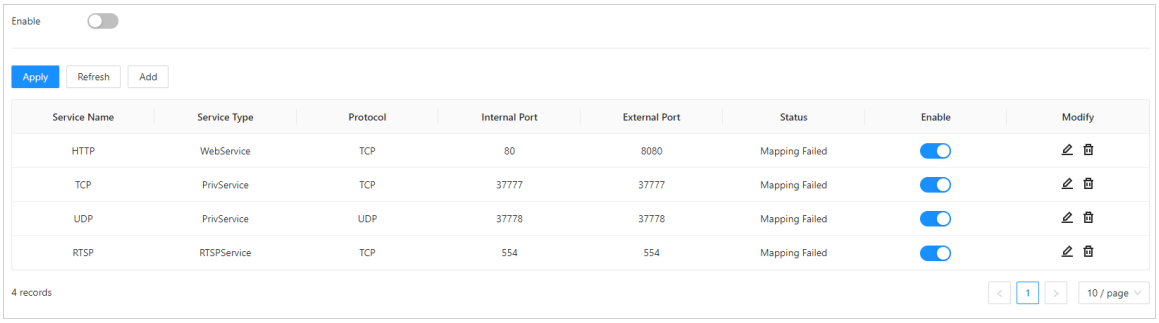
Procedimiento

Paso 1 Inicie sesión en la página web del dispositivo.

Paso 2 Seleccione**Configuración de red**>**UPnP**.

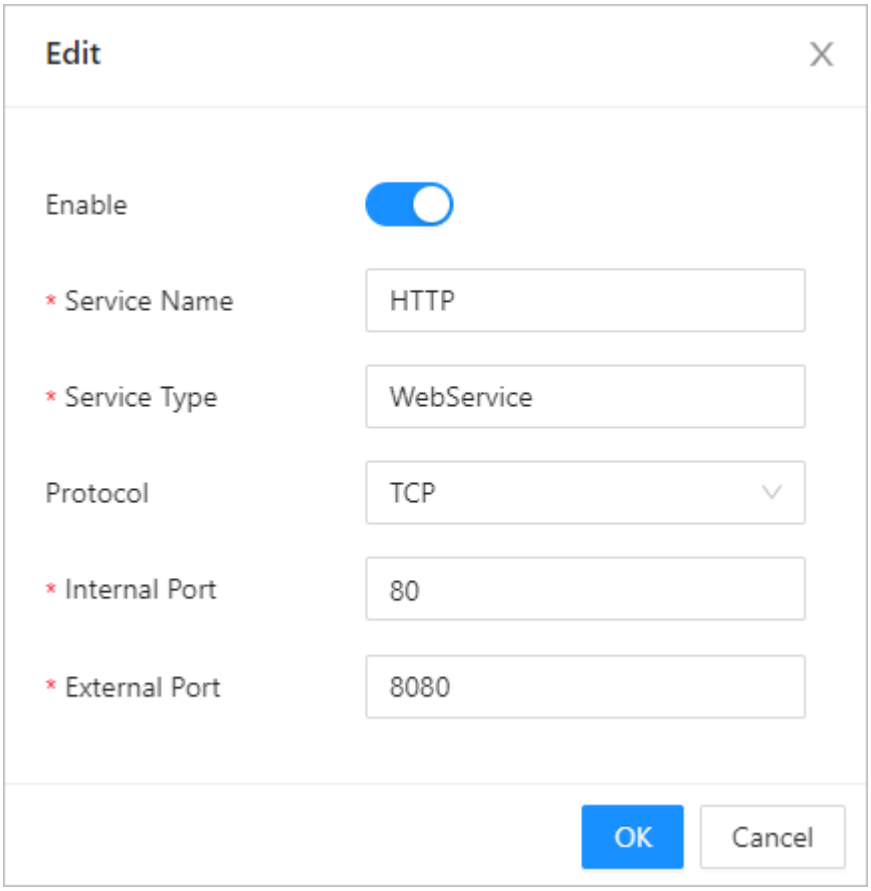
Paso 3 Haga clic en junto a**Permitir**.

Figura 4-15 UPnP



Paso 4 Hacer clic para modificar los puertos y luego haga clic en**DE ACUERDO**.

Figura 4-16 Modificar los puertos



Paso 5 Hacer clic**Aplicar**.

Abra un navegador en la computadora, ingrese*http:// dirección IP de la extranet: número de puerto externo*y luego puede visitar el dispositivo de intranet con el puerto correspondiente.

4.6.6 Configuración de servicios básicos

Configurar los servicios básicos para lograr la gestión de la seguridad del sistema.

Procedimiento

Paso 1 Inicie sesión en la página web del dispositivo. Seleccione

Paso 2 **Configuración de red**>**Servicios básicos**. Configure los

Paso 3 parámetros y luego haga clic en**Aplicar**.

Figura 4-17 Servicios básicos

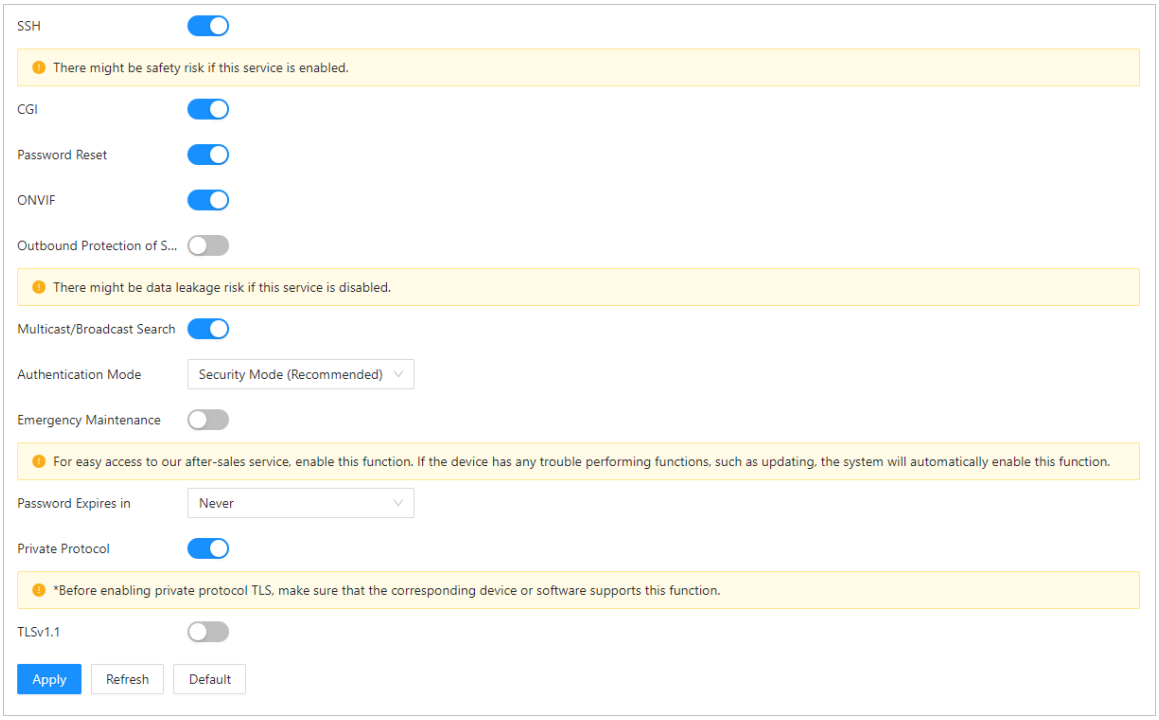


Tabla 4-8 Descripción de los servicios básicos

Servicio	Descripción
SSH	Secure Shell (SSH) es un protocolo de red criptográfico para operar servicios de red de forma segura a través de una red no segura. Si está habilitado, SSH proporciona un servicio criptográfico para la transmisión de datos. No está habilitado de manera predeterminada.
CGI	La interfaz de puerta de enlace común (CGI) ofrece un protocolo estándar para que los servidores web ejecuten programas de manera similar a las aplicaciones de consola que se ejecutan en un servidor que genera páginas web dinámicamente. Si está habilitado, se pueden usar comandos CGI. El CGI está habilitado de manera predeterminada.
Restablecer contraseña	Si está habilitada, después de configurar la dirección de correo electrónico, puede restablecer la contraseña. Esta función está habilitada de manera predeterminada.
ONVIF	Permitir que otros dispositivos extraigan la transmisión de video del dispositivo a través del protocolo ONVIF.
Protección de salida Contraseña de servicio	Si está habilitado, no se puede obtener la contraseña de inicio de sesión del dispositivo a través del protocolo.
Multidifusión/Difusión Buscar	Habilite esta función y, luego, cuando varios usuarios estén obteniendo una vista previa de la imagen de video del dispositivo simultáneamente a través de la red, podrán encontrar su dispositivo con el protocolo de multidifusión/difusión.
Modo de autenticación	• **Modo de seguridad (recomendado)**:El modo no admite el inicio de sesión con Digest, DES y autenticación de texto sin formato. • **Modo de compatibilidad**:El modo admite el inicio de sesión con autenticación Digest, DES y texto simple.

Servicio	Descripción
Emergencia Mantenimiento	Le recomendamos que habilite esta función para el análisis de fallas y el mantenimiento.
La contraseña caduca en	Configura la hora. El sistema te recordará que debes cambiar la contraseña antes de que caduque. Si seleccionas**Nunca**, el sistema nunca te recuerda cambiar la contraseña.
Protocolo privado	Si está habilitado, la plataforma puede acceder al dispositivo con protocolo privado.
Versión 1.1 de TLS	 Existe un riesgo de seguridad si lo habilita**Versión 1.1 de TLS**.

4.7 Gestión del sistema

4.7.1 Configuración de parámetros de vídeo

Inicie sesión en la página web del dispositivo y luego seleccione**Sistema**>**Video**.



Sólo VTA250*incógnita*La Serie G admite esta función.

Tabla 4-9 Descripción de parámetros

Parámetro		Descripción
Estándar de vídeo		● PAL: La velocidad de cuadros de transmisión predeterminada es 25 fps. ● NTSC: La velocidad de cuadros de transmisión predeterminada es 30 fps.
Corriente principal	Compresión	Seleccione el modo de compresión dependiendo del ancho de banda real. ● H.264: Compresión del perfil principal. ● H.265: La compresión del perfil principal ocupa un ancho de banda menor que H.264 en la misma calidad de imagen.
	Resolución	Seleccione la resolución.
	Velocidad de cuadros (FPS)	La cantidad de cuadros que aparecen en un segundo. Un FPS más alto se refiere a una imagen más vívida y fluida.
Subtransmisión	Compresión	Seleccione el modo de compresión dependiendo del ancho de banda real. ● H.264: Compresión del perfil principal. ● H.265: La compresión del perfil principal ocupa un ancho de banda menor que H.264 en la misma calidad de imagen.
	Resolución	Seleccione la resolución según sea necesario.
	Velocidad de cuadros (FPS)	La cantidad de cuadros que aparecen en un segundo. Un FPS más alto se refiere a una imagen más vívida y fluida.

Tasa de bits

Figura 4-18 Velocidad de bits

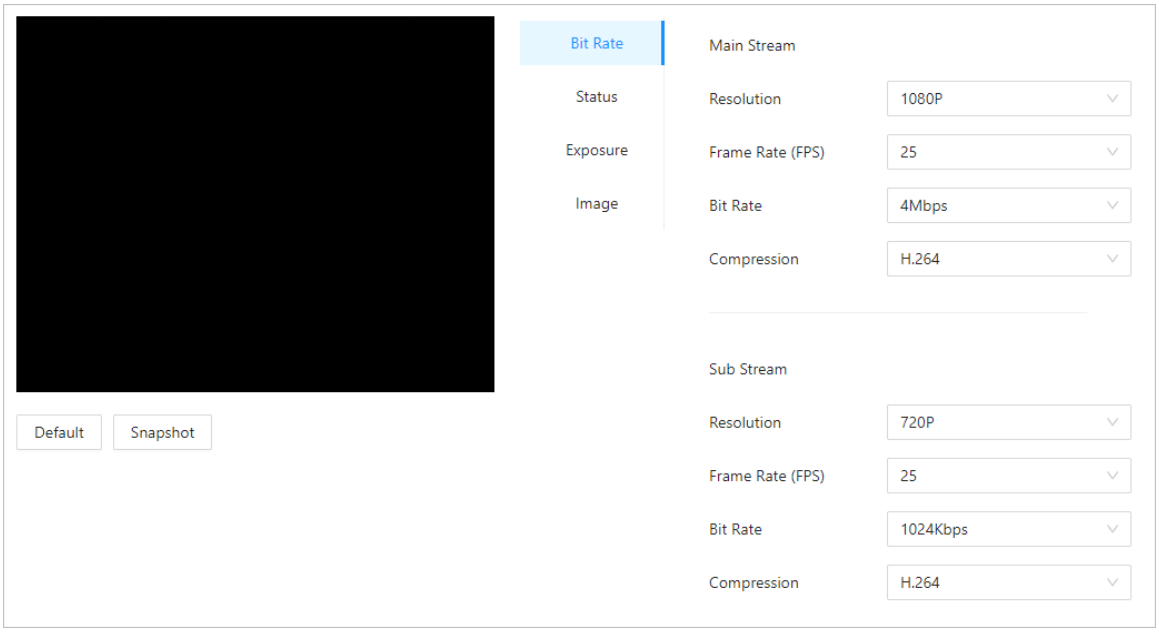


Tabla 4-10 Descripción de los parámetros de velocidad de bits

Parámetro		Descripción
Corriente principal	Resolución	Seleccione la resolución. Cuando el terminal de llamada de emergencia está conectado al VTH como un VTO, la resolución está limitada a 720P. Si selecciona**1080P**, la función de intercomunicación y monitoreo se verán afectadas.
	Velocidad de cuadros (FPS)	El número de fotogramas en un segundo de vídeo.
	Tasa de bits	Seleccione la velocidad de bits según la situación real.
	Compresión	Seleccione de**H.264**y**H.265**. En comparación con H.264, H.265 requiere un ancho de banda menor.
Subtransmisión	Resolución	Seleccione la resolución.
	Velocidad de cuadros (FPS)	Número de fotogramas por segundo de vídeo. Seleccione entre 1 y 25.
	Tasa de bits	Seleccione la velocidad de bits según la situación real.
	Compresión	Seleccione de**H.264**y**H.265**. En comparación con H.264, H.265 requiere un ancho de banda menor.

Estado

Figura 4-19 Estado

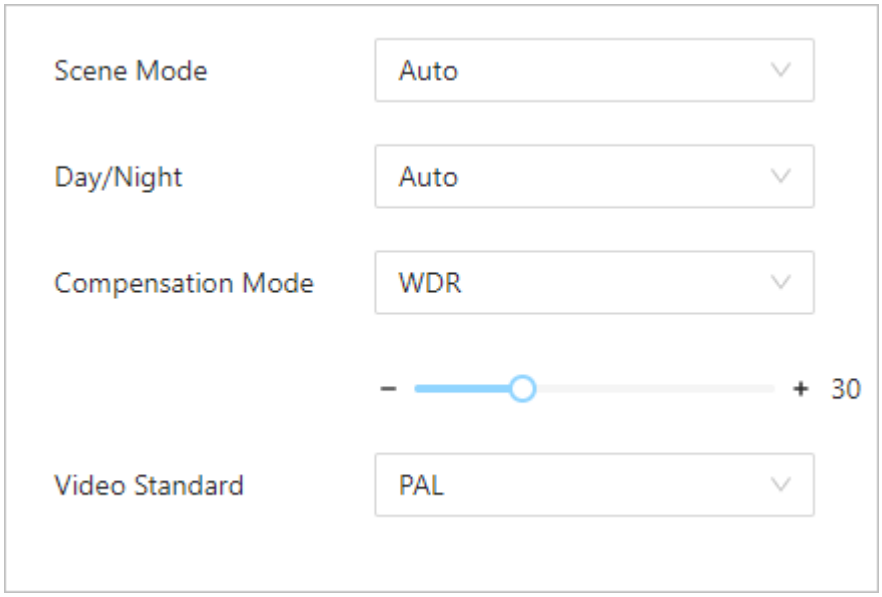


Tabla 4-11 Descripción de los parámetros de estado

Parámetro	Descripción
Modo de escena	Diferentes modos determinan el tono del color.**Auto**por defecto. ● **Desactivar**:El modo no está configurado. ● **Auto**:Ajuste el modo de escena para mostrar la imagen según la situación real. ● **Soleado**:El color de la imagen es más oscuro. ● **Noche**:El color de la imagen es más claro.
Día/Noche	● **Auto**:El sistema cambia entre color y blanco y negro según la situación real. ● **Color**:El sistema muestra la imagen en color. ● **Blanco y negro**:El sistema muestra imágenes en blanco y negro.
Modo de compensación	● **Desactivar**:No habrá luz de fondo. ● **BLC**:El sistema obtiene una imagen más clara de las áreas oscuras del objetivo cuando se dispara contra la luz. ● **Amplio rango dinámico (WDR)**:El sistema atenúa las áreas brillantes y compensa las áreas oscuras para garantizar la claridad de todas las áreas. ● **HLCC (Centro de Información de Conducta Humana)**:El sistema atenúa las luces fuertes y reduce el tamaño de la zona de Halo para disminuir el brillo de toda la imagen. Le recomendamos que seleccione**Amplio rango dinámico (WDR)**Para retroiluminación.
Estándar de vídeo	Seleccione de**CAMARADA**y**Sistema de clasificación de números arábigos (NTSC)**.

Exposición

Figura 4-20 Exposición

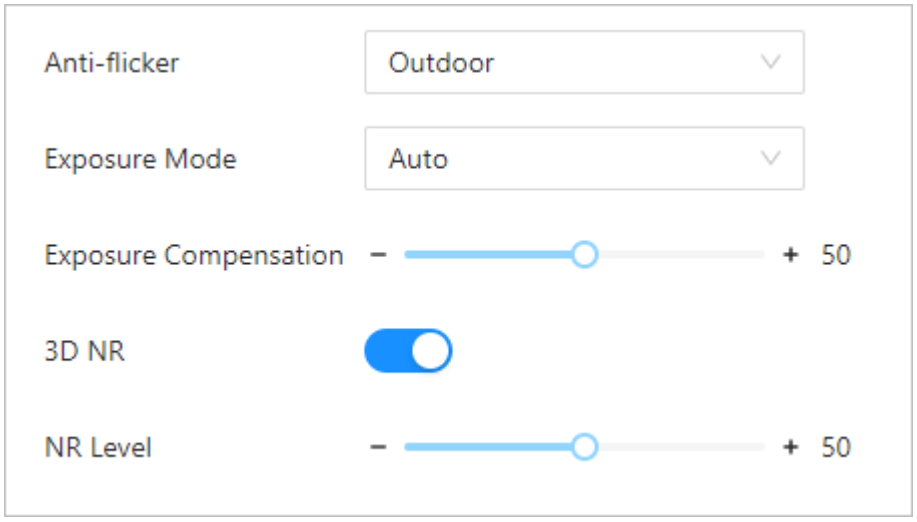


Tabla 4-12 Descripción de los parámetros de exposición

Parámetro	Descripción
Anti-parpadeo	• **50 Hz**:El sistema ajusta automáticamente la exposición según la luz ambiental para garantizar que no aparezcan rayas. • **60 Hz**:El sistema ajusta automáticamente la exposición según la luz ambiental para garantizar que no aparezcan rayas. • **Exterior**:Si seleccionas**Exterior**, se puede ajustar el modo de exposición para mostrar la imagen.
Modo de exposición	• **Auto**:La exposición se ajusta automáticamente según el brillo de la escena si el brillo general de las imágenes está dentro del rango de exposición normal. • **Prioridad de obturador**:Configurar el**Obturador**Valor. El dispositivo se ajustará según el valor configurado. • **Manual**:Puedes ajustar el**Ganar**y**Obturador**valor manualmente. • Si el**Anti-parpadeo**se establece como**Exterior**, puedes seleccionar**Prioridad de obturador**. • Diferentes dispositivos admiten distintos modos de exposición.
Exposición Compensación	Puede configurar el valor de compensación de exposición. Cuanto mayor sea el valor, más brillante será la imagen.
Reducción de ruido 3D	Reduzca el ruido de imágenes de varios fotogramas (al menos dos fotogramas) utilizando información entre fotogramas adyacentes en un vídeo. Cuanto más alto sea el nivel, menor será el ruido y mayor será la mancha de arrastre.
Nivel NR	

Imagen

Figura 4-21 Imagen

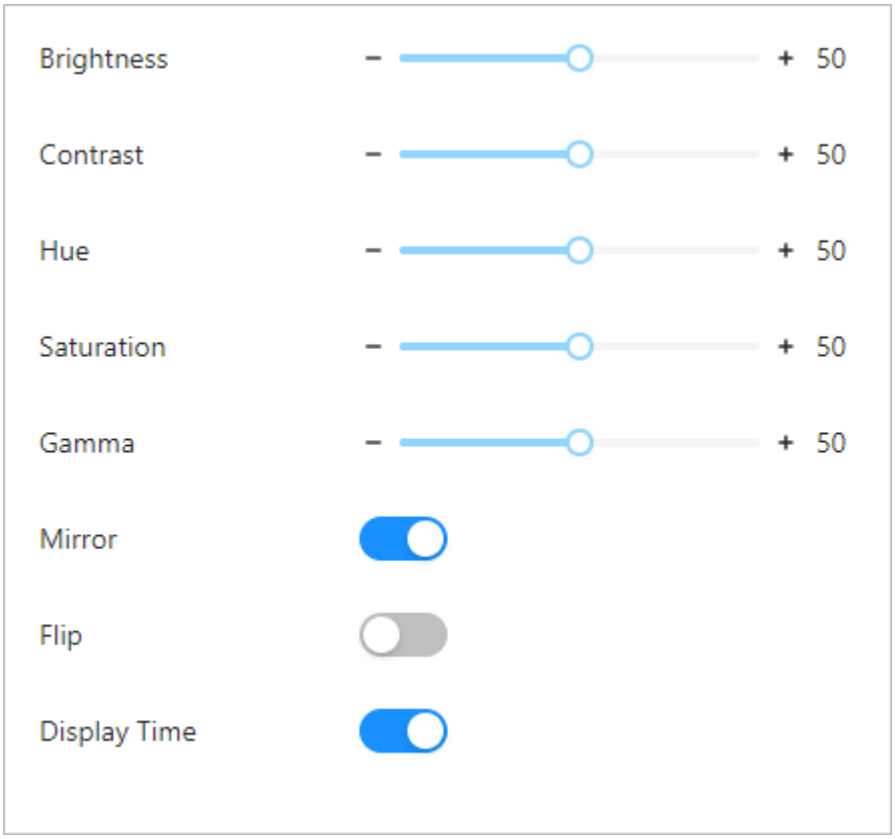


Tabla 4-13 Descripción de los parámetros de la imagen

Parámetro	Descripción
Brillo	Cambia el brillo general de la imagen. Cuanto mayor sea el valor, más brillante será la imagen.
Contraste	Cambie el contraste de la imagen. Cuanto mayor sea el valor, mayor será el contraste entre las áreas claras y oscuras. Si el valor es demasiado grande, el área oscura será demasiado oscura y el área clara será más vulnerable a la sobreexposición.
Matiz	Hace que el color sea más oscuro o más claro. El valor predeterminado lo establece el sensor de luz y es el recomendado.
Saturación	Establece la intensidad de los colores. Cuanto mayor sea el valor, más profundo será el color. El valor de saturación no modifica el brillo de la imagen.
Gama	Cambia el brillo y el contraste de la imagen de forma no lineal. Cuanto mayor sea el valor, más brillante será la imagen.
Espejo	Si está habilitado, la imagen se gira hacia la izquierda y hacia la derecha.
Voltear	Si está habilitado, la imagen se gira hacia arriba y hacia abajo.
Hora de visualización	Si está habilitado, la hora actual se muestra en la imagen de vídeo.

4.7.2 Configuración de la hora

Puede configurar la fecha, la zona horaria y el servidor NTP (Protocolo de tiempo de red).

Procedimiento

Paso 1 Inicie sesión en la página web del dispositivo.

Paso 2 Seleccione**Sistema**>**Tiempo**. Configure los

Paso 3 parámetros.

Figura 4-22 Configurar tiempo

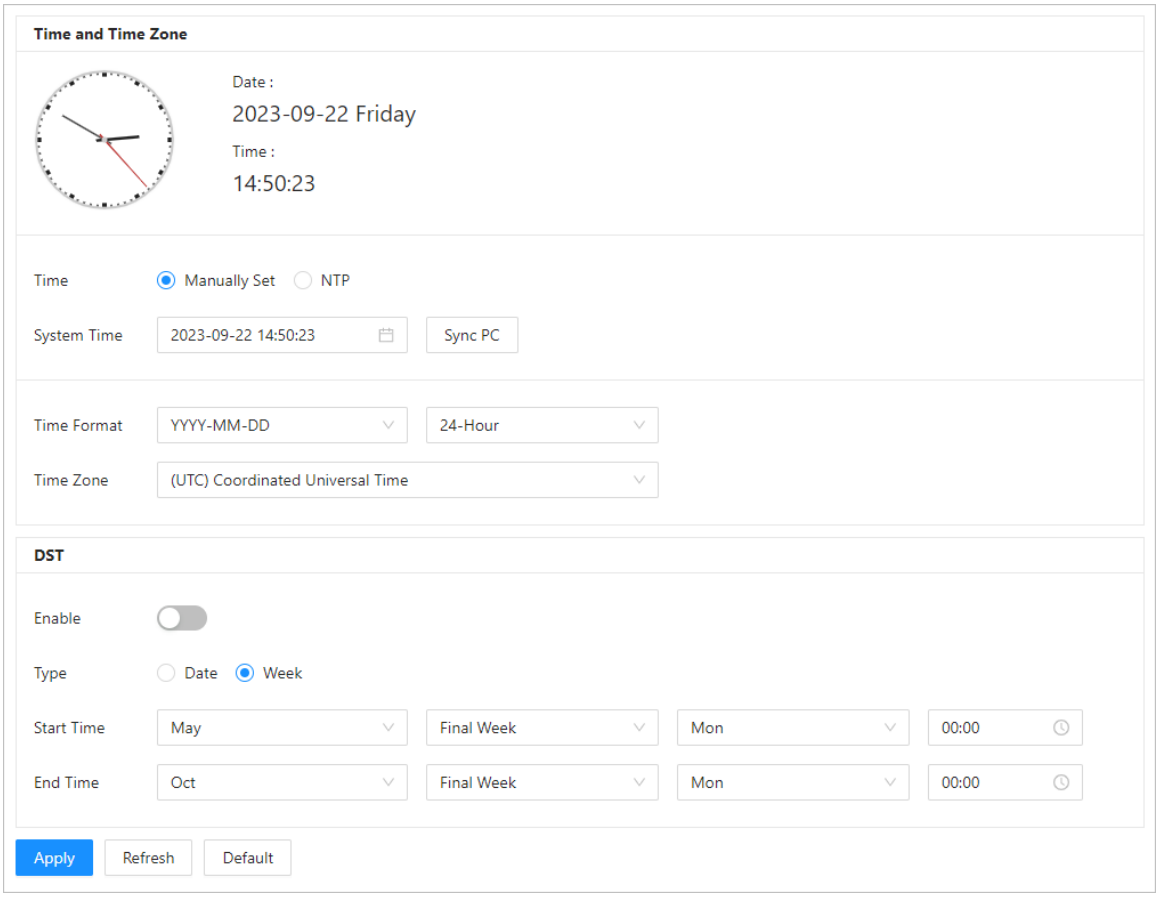


Tabla 4-14 Descripción de los parámetros de fecha y hora

Parámetro		Descripción
Tiempo y tiempo Zona	Tiempo	Seleccionar**Conjunto manual**o**Programa Nacional de Pruebas**.
	Hora del sistema	Si seleccionas**Ajustes manuales**, configure la hora del sistema manualmente. Hacer clic**Sincronizar PC**, y la hora del sistema cambia a la hora de la PC.
	Servidor	Si seleccionas**Programa Nacional de Pruebas**Luego, el sistema sincroniza la hora con el servidor de Internet en tiempo real. También puede ingresar la dirección IP, el puerto y el intervalo de una PC que ejecute un servidor NTP para utilizar NTP.
	Puerto	
	Intervalo	

Parámetro		Descripción
	Formato de hora	Seleccione el formato de hora.
	Huso horario	Configure la zona horaria en la que se encuentra el dispositivo.
Horario de verano	Permitir	Si el área donde se encuentra el dispositivo usa horario de verano, habilítelo.
	Tipo	Seleccione el tipo de**Fecha**y**Semana**y luego configure la hora de inicio y la hora de finalización del horario de verano.
	Hora de inicio	
	Fin del tiempo	

Paso 4 Hacer clic**Aplicar**.

4.7.3 Agregar usuario ONVIF

Los usuarios de ONVIF se utilizan para el protocolo ONFVIF.

Procedimiento

Paso 1 Inicie sesión en la página web del dispositivo.

Paso 2 Seleccione**Sistema**>**Usuario ONVIF**.

Paso 3 Hacer clic**Agregar**y luego configure los parámetros.

Figura 4-23 Agregar usuario ONVIF

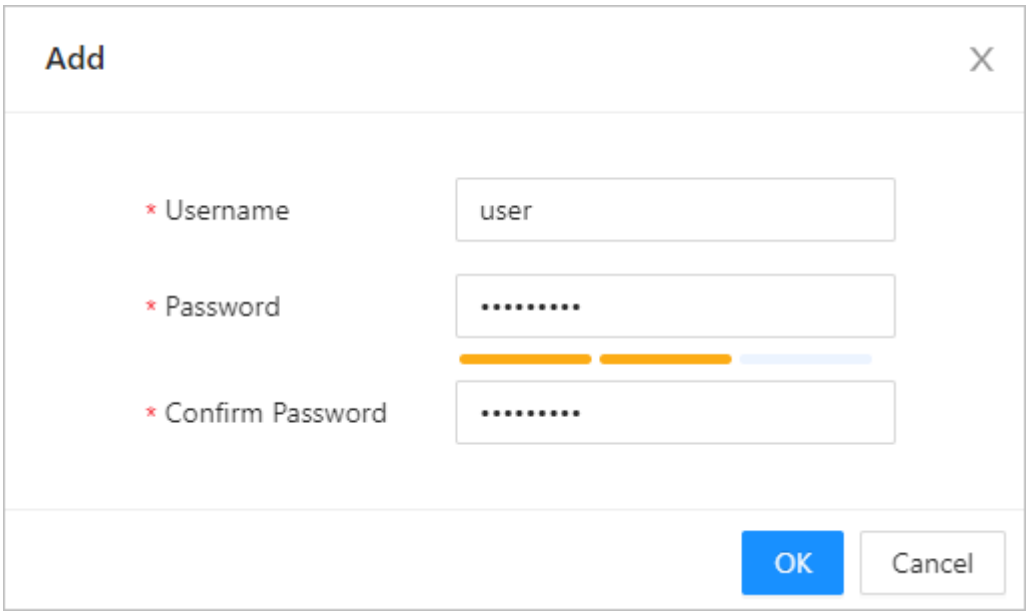


Tabla 4-15 Descripción de los parámetros de usuario de ONVIF

Parámetro	Descripción
Nombre de usuario	El nombre de usuario es único. El nombre de usuario consta de hasta 31 caracteres, incluidos números, letras, guiones bajos, puntos y @.
Contraseña	La contraseña debe constar de 8 a 32 caracteres que no sean espacios en blanco y contener al menos dos tipos de los siguientes caracteres: mayúsculas, minúsculas, números y caracteres especiales (excluyendo ' " ; : &).
confirmar Contraseña	

Paso 4 Hacer clic**DE ACUERDO**.

El usuario ONVIF agregado se muestra en la lista.

Operaciones relacionadas

- Hacer clic para modificar el nombre de usuario, contraseña y el grupo.
- Hacer clic para eliminar el usuario ONVIF.

4.7.4 Configuración del almacenamiento

Información de contexto

Sólo VTA250*incógnita*La Serie G admite esta función.

Procedimiento

Paso 1 Inicie sesión en la página web del dispositivo.

Paso 2 Seleccione**Sistema**>**Almacenamiento**.

Ver el estado y la capacidad de la tarjeta SD insertada.

Paso 3 (Opcional) Si no se puede reconocer la tarjeta SD insertada, haga clic en**Formatear tarjeta de**

Paso 4 **almacenamiento**. Configure los parámetros y luego haga clic en**Aplicar**.

Figura 4-24 Almacenamiento

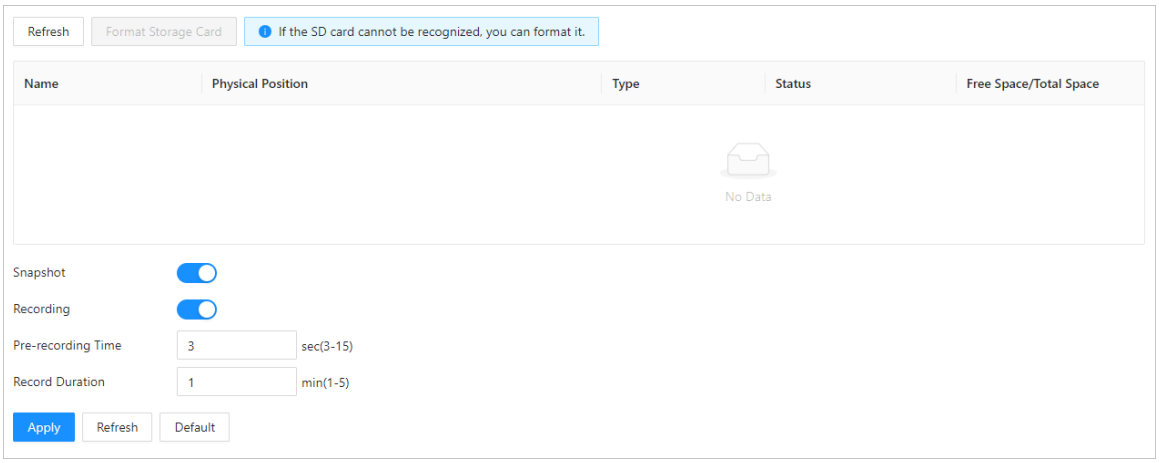


Tabla 4-16 Descripción de los parámetros de almacenamiento

Parámetro	Descripción
Instantánea	Si está habilitado, cuando se activa la alarma, el dispositivo toma la instantánea. Cuando ocurre el evento, el dispositivo toma una instantánea.
Grabación	Si está habilitado, cuando se activa la alarma, el dispositivo comienza a grabar. Cuando ocurre el evento el dispositivo comienza a grabar.
Tiempo de pregrabación	El valor predeterminado es 3 s. El dispositivo comienza a grabar 3 s antes de que se detecte el evento.

Parámetro	Descripción
Duración del registro	El valor predeterminado es 1 minuto. Cada tiempo de grabación será de 1 minuto.

4.8 Centro de mantenimiento

4.8.1 Diagnóstico con un solo clic

Detectar las configuraciones y el estado del dispositivo para mejorar el rendimiento.

Procedimiento

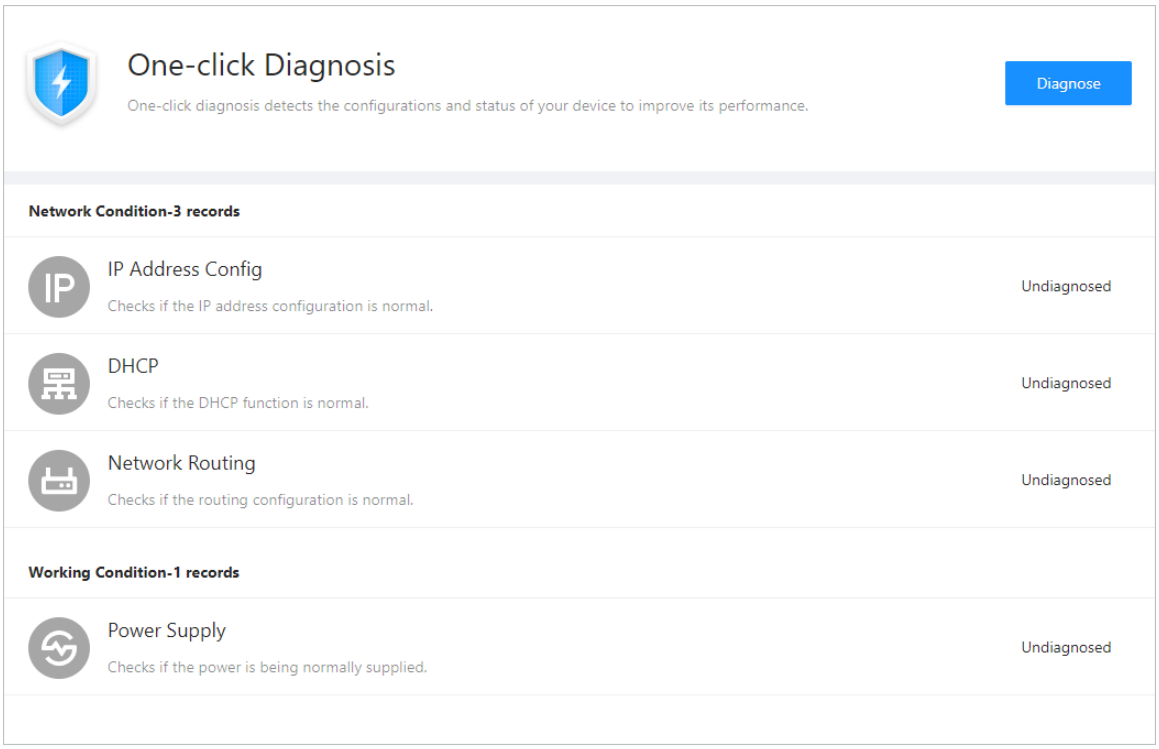
Paso 1 Inicie sesión en la página web del dispositivo.

Paso 2 Seleccionar**Centro de mantenimiento**>**Diagnóstico con un solo clic**Haga

Paso 3 clic en**Diagnosticar**.

Hacer clic**Diagnosticar de nuevo**Si no es la primera vez que se diagnostica.

Figura 4-25 Diagnóstico



4.8.2 Información del sistema

Inicie sesión en la página web del dispositivo. Seleccione**Centro de mantenimiento**>**Información del sistema**Haga clic en **Información legal** Para ver el acuerdo de licencia del software, la política de privacidad y el aviso sobre software de código abierto, haga clic en **Información del sistema**para ver la información básica del dispositivo, incluido el modelo y la versión del dispositivo.

4.8.3 Registro

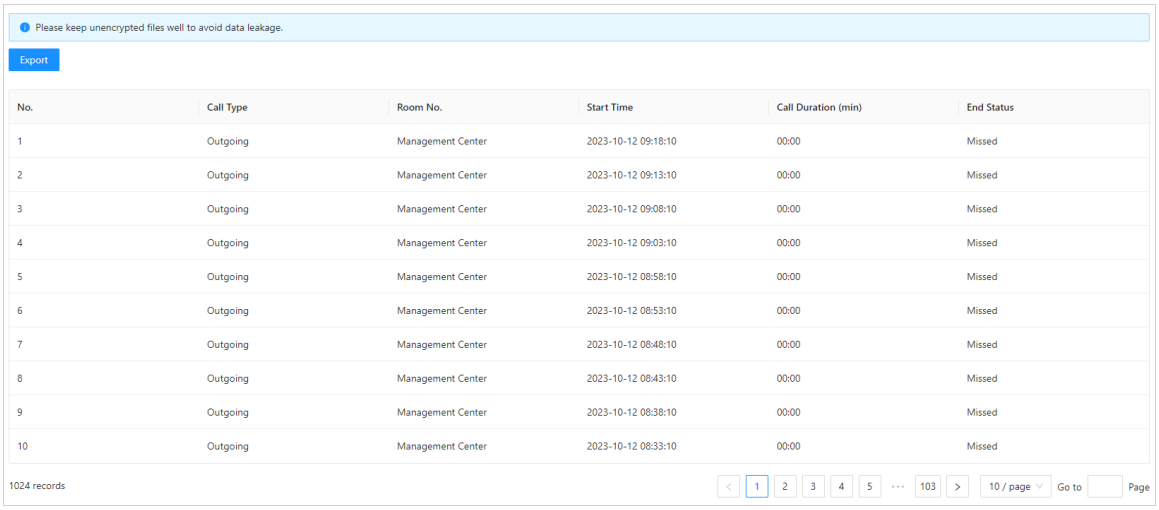
4.8.3.1 Visualización del historial de llamadas

Procedimiento

Paso 1 Inicie sesión en la página web del dispositivo.

Paso 2 Seleccionar**Centro de mantenimiento**>**Registro**>**Historial de llamadas**para ver los registros de llamadas.

Figura 4-26 Historial de llamadas



Paso 3 (Opcional) Haga clic en**Exportar**para exportar los registros de llamadas.

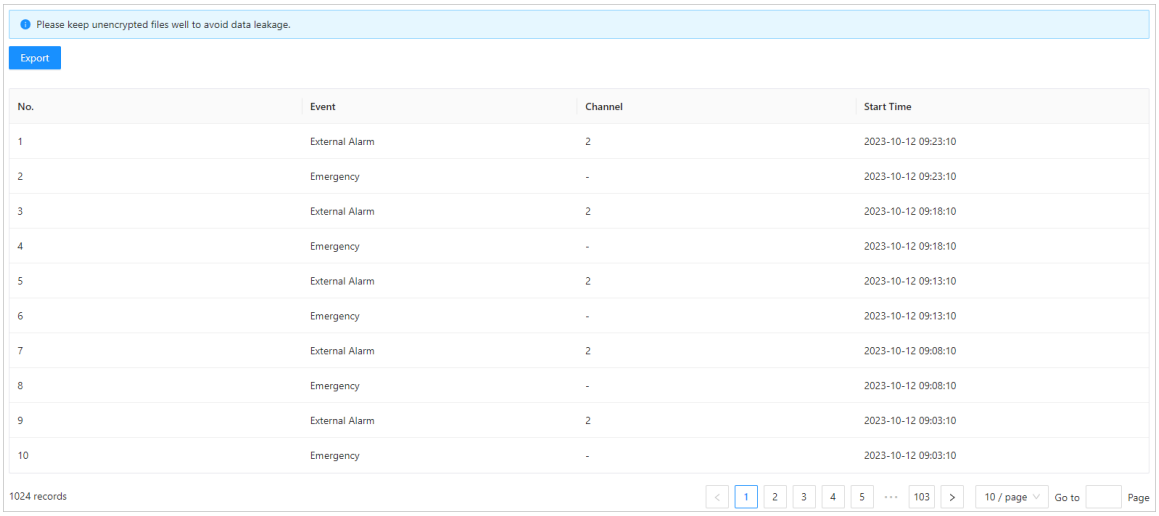
4.8.3.2 Visualización de los registros de alarmas

Procedimiento

Paso 1 Inicie sesión en la página web del dispositivo.

Paso 2 Seleccionar**Centro de mantenimiento**>**Registro**>**Registros de alarmas**.

Figura 4-27 Registro de alarmas



Paso 3 (Opcional) Haga clic en**Exportar**para exportar los registros de alarma.

4.8.3.3 Visualización de los registros del sistema

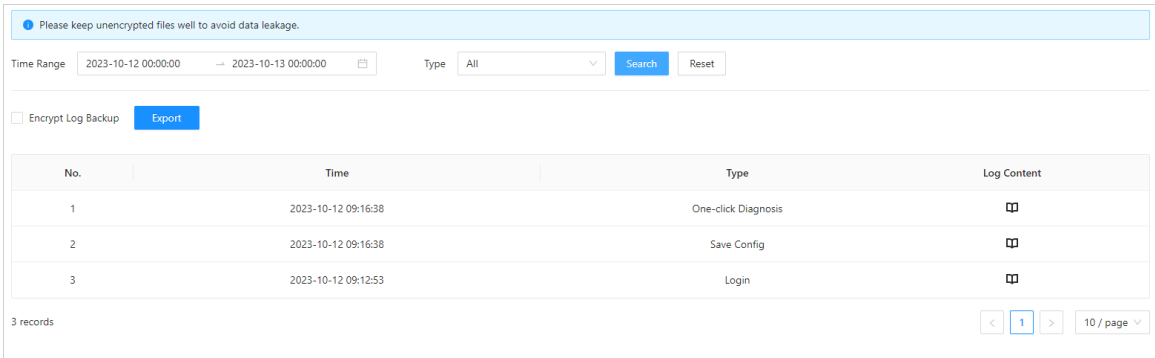
Procedimiento

Paso 1 Inicie sesión en la página web del dispositivo. Seleccione

Paso 2 **Centro de mantenimiento**>**Registro**>**Registro**.

Paso 3 Seleccione el rango de tiempo y el tipo de registro y luego haga clic en**Buscar**.

Figura 4-28 Registro del sistema



Operaciones relacionadas

- Hacer clic**Exportar**para descargar los resultados a su computadora.

  Si lo habilita**Copia de seguridad de registros cifrada**e ingrese la contraseña antes de exportar el registro, debe ingresar la contraseña para abrir el archivo exportado.

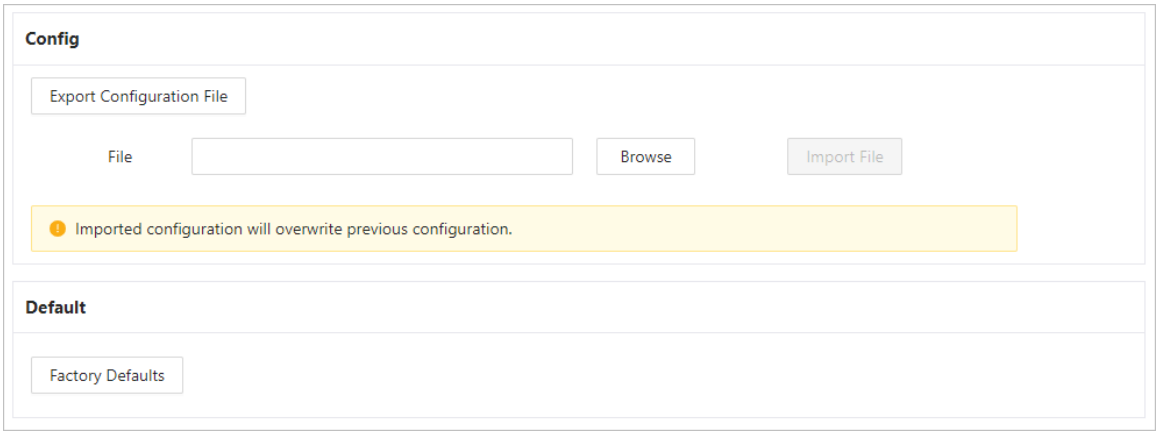
- Hacer clic para ver los detalles del registro.

4.8.4 Gestión

4.8.4.1 Configuración

Inicie sesión en la página web del dispositivo. Seleccione**Centro de mantenimiento**>**Gerente**>**Configuración**.

Figura 4-29 Configuración



4.8.4.1.1 Exportación/importación del archivo de configuración

Exporte o importe el archivo de configuración. Cuando necesite las mismas configuraciones en varios dispositivos, puede utilizar el archivo de configuración exportado.

Exportar archivo de configuración

Hacer clic**Exportar archivo de configuración**, descargue el archivo a su computadora.

La dirección IP no se exportará.

Importar archivo de configuración

1. Haga clic**Navegar**, seleccione el archivo de configuración.
2. Haga clic**Importar archivo**.

El archivo de configuración debe importarse a los dispositivos con el mismo modelo. Después de la importación, el dispositivo se reinicia.

4.8.4.1.2 Restauración a los valores predeterminados de fábrica

Si se restaura el dispositivo a la configuración predeterminada, se perderán los datos. Tenga en cuenta lo siguiente.

Hacer clic**Valores predeterminados de fábrica**,Ingrese la contraseña de inicio de sesión y luego haga clic en**DE ACUERDO**. Restaurar todas las configuraciones a los valores predeterminados excepto la dirección IP.

4.8.4.2 Mantenimiento

Configure el tiempo de reinicio automático para mantener el rendimiento del dispositivo.

Procedimiento

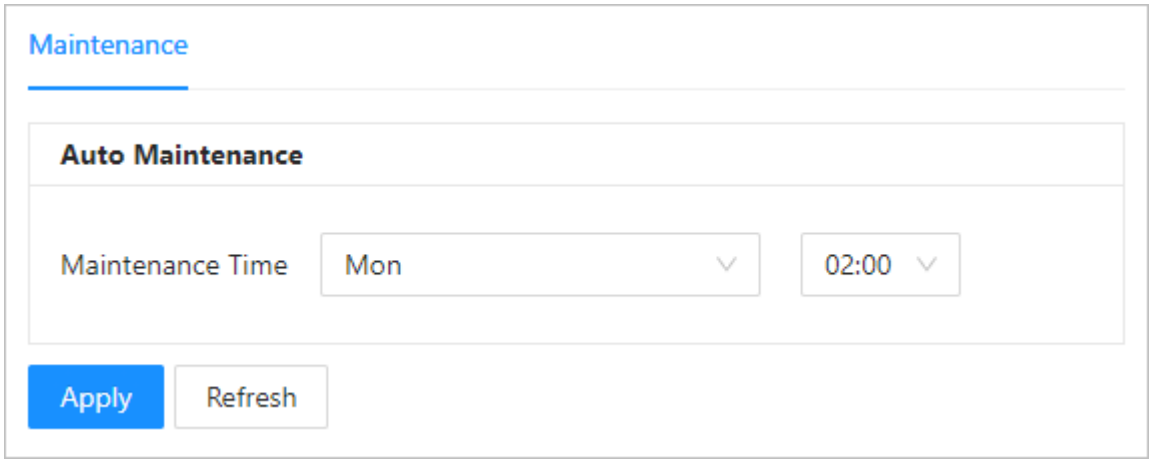
Paso 1 Inicie sesión en la página web del dispositivo.

Paso 2 Seleccionar**Centro de mantenimiento**>**Gerente**>**Mantenimiento**

Paso 3 Seleccione el tiempo de mantenimiento y luego haga clic en**Aplicar**.

La hora de mantenimiento predeterminada es a las 2:00 todos los martes.

Figura 4-30 Mantenimiento



4.8.5 Actualización

- No desconecte la fuente de alimentación ni la red, ni reinicie o apague el dispositivo durante la actualización.
- Utilice el archivo de actualización correcto. Asegúrese de obtener el archivo de actualización correcto del soporte técnico.
- Volver a versiones anteriores puede causar un riesgo de seguridad. Tenga cuidado.

Procedimiento

Paso 1 Inicie sesión en la página web del dispositivo. Seleccione

Paso 2 **Centro de mantenimiento**>**Actualizar**Seleccione el tipo

Paso 3 de actualización.

- Actualización de archivo

  1. Haga clic**Navegar**y luego seleccione el archivo de actualización.

     El archivo de actualización debe ser un archivo .bin.

  2. Haga clic**Actualizar**.

- Actualización en línea

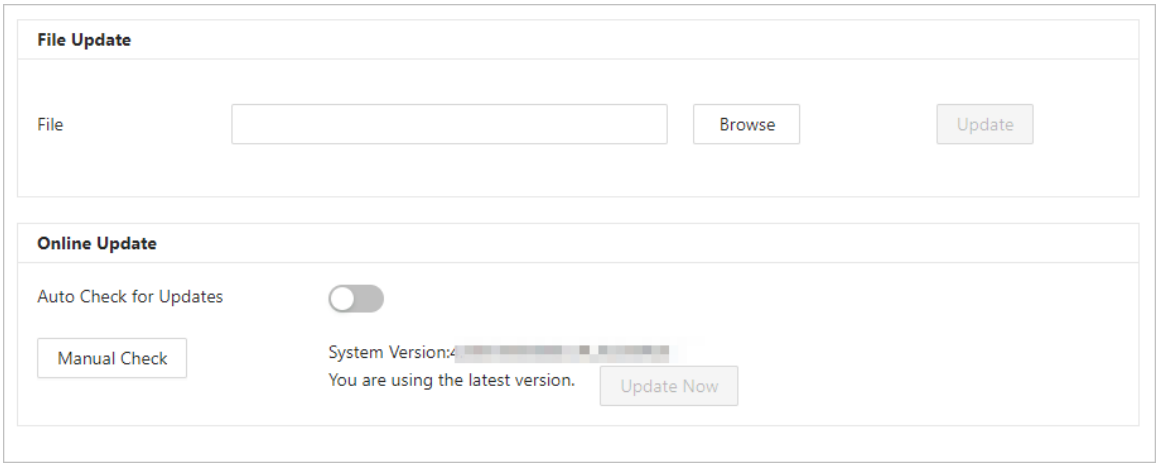
  Compruebe la nueva versión de forma automática o manual y luego haga clic en**Actualizar**.

  - **Búsqueda automática de actualizaciones**:Si está habilitado, el sistema verifica la versión todos los días. Se le avisará si el sistema detecta una nueva versión.

    Para informarle sobre la actualización automática, recopilaremos la dirección IP, el nombre del dispositivo, el número de serie, la versión del firmware y otra información. La información solo se utiliza para la verificación y la notificación de actualizaciones.

  - **Comprobación manual**:Hacer clic**Comprobación manual**para detectar la nueva versión.

Figura 4-31 Actualización



4.8.6 Mantenimiento avanzado

Obtenga la información del dispositivo y los datos del paquete para solucionar problemas.

Exportar

Inicie sesión en la página web del dispositivo, seleccione**Centro de mantenimiento**>**Mantenimiento avanzado**> **Exportar**y luego haga clic en**Exportar**para exportar el número de serie, la versión de firmware, los registros de funcionamiento del dispositivo y la información de configuración.

Captura de paquetes

1. Inicie sesión en la página web del dispositivo.
2. Seleccionar**Centro de mantenimiento**>**Mantenimiento avanzado**>**Captura de paquetes**.
3. Ingrese la dirección IP y luego haga clic en .

   El icono se convierte en .
4. Después de obtener los datos, haga clic en .
5. Los datos se guardarán automáticamente en su computadora.

Figura 4-32 Captura de paquetes



4.9 Búsqueda de registros

Sólo VTA250*incógnita*La Serie G admite esta función.

Procedimiento

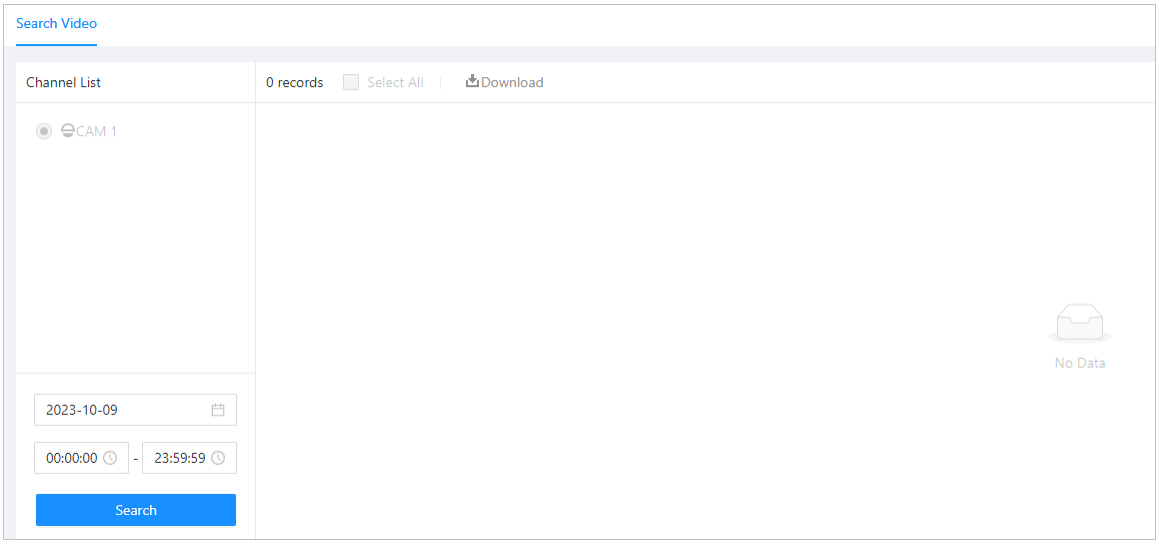
Paso 1 Inicie sesión en la página web del dispositivo. Haga

Paso 2 clic en**Registro**.

Paso 3 Seleccione la hora y luego configure**Buscar**.

Sólo puedes ver los registros diarios.

Figura 4-33 Registro



Operaciones relacionadas

- Seleccione los archivos y luego haga clic**Descargar**para guardar los archivos en su computadora.
- Hacer clic**Seleccionar todo**,y luego haga clic**Descargar**para descargar todos los archivos.

4.10 Búsqueda de imágenes

Sólo VTA250*incógnita*La Serie G admite esta función.

Procedimiento

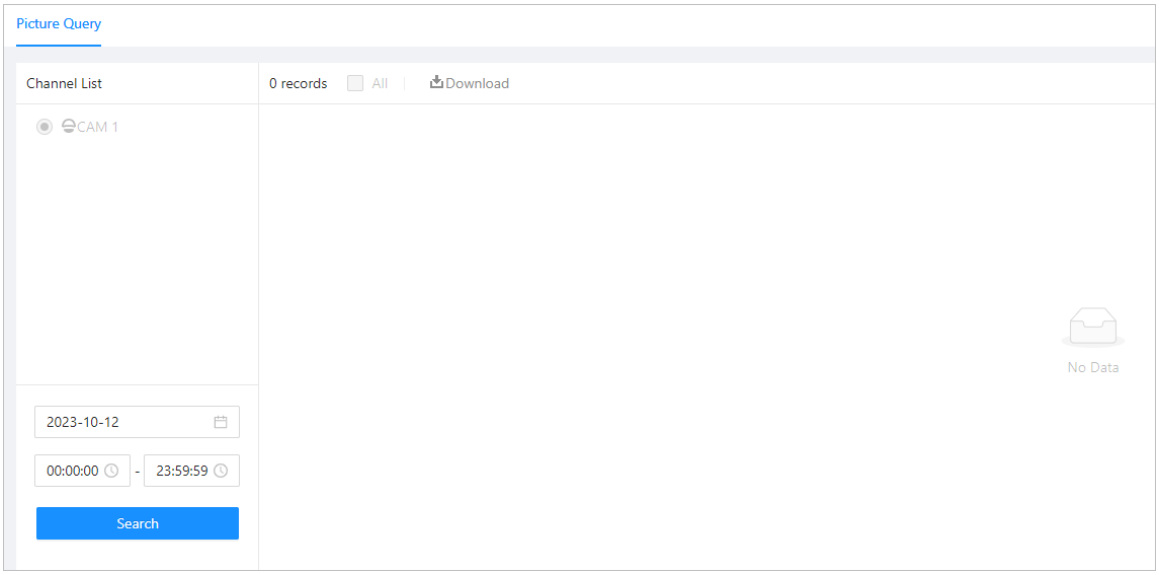
Paso 1 Inicie sesión en la página web del dispositivo. Haga

Paso 2 clic en**Imagen**.

Paso 3 Seleccione la hora y luego configure**Buscar**.

Sólo puedes ver las imágenes diarias.

Figura 4-34 Imagen



Operaciones relacionadas

- Seleccione los archivos y luego haga clic**Descargar**para guardar los archivos en su computadora.
- Hacer clic**Seleccionar todo**,y luego haga clic**Descargar**para descargar todos los archivos.

4.11 Seguridad

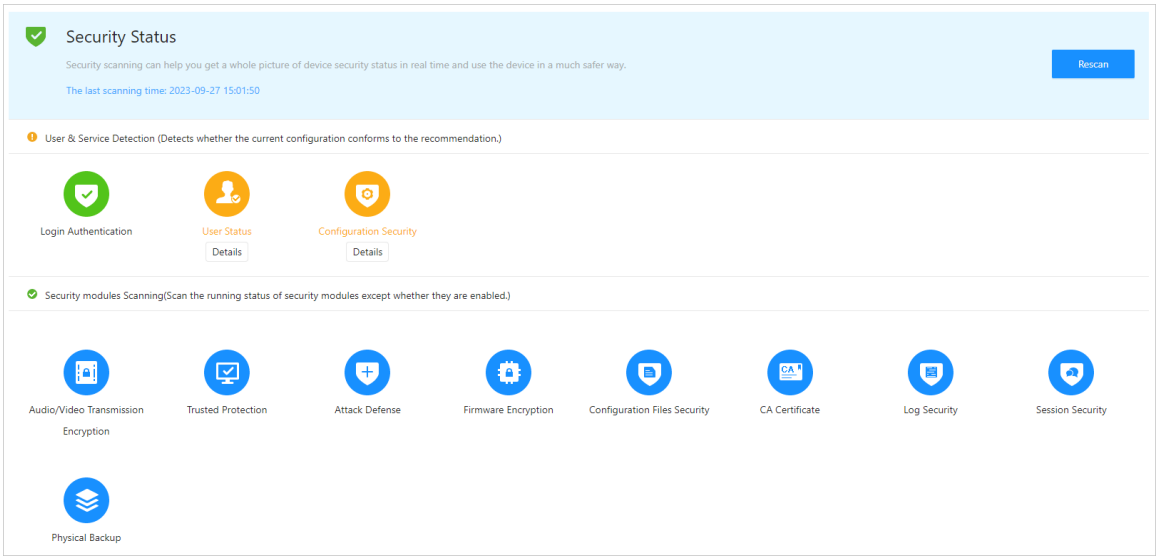
4.11.1 Estado de seguridad

Detectar y verificar el estado de seguridad del dispositivo.

Inicie sesión en la página web del dispositivo. Seleccione > **Estado de seguridad**Haga clic en**Escanear**Para escanear la seguridad el estado del dispositivo.

Hacer clic**Volver a escanear**Si no es la primera vez que escanea.

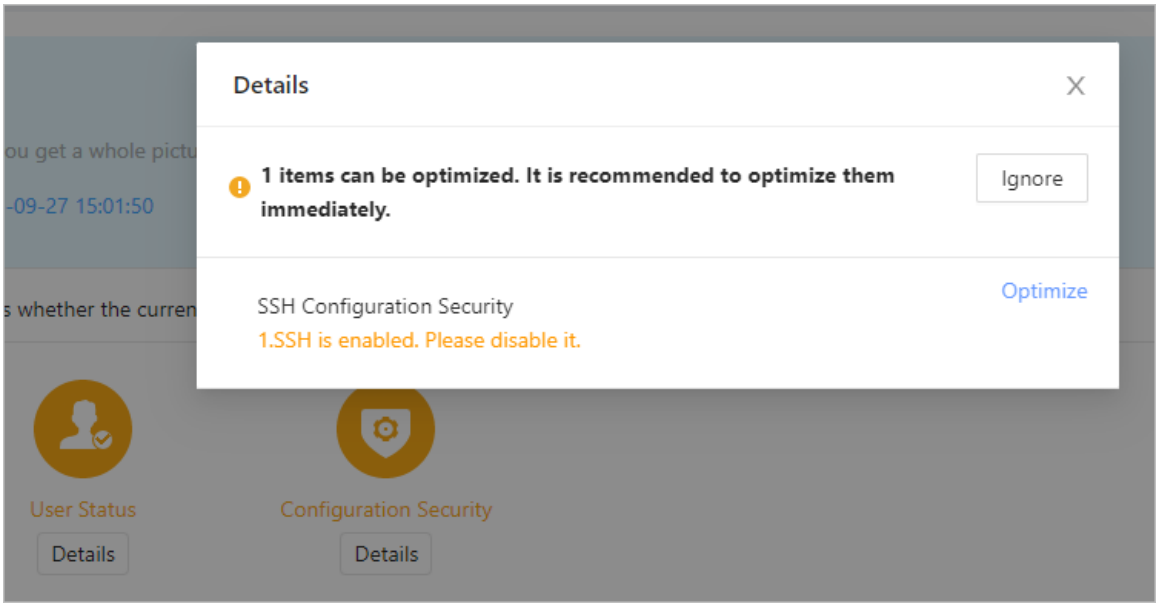
Figura 4-35 Estado de seguridad



Detección de usuarios y servicios

- Si la configuración del elemento de detección se ajusta a la recomendación, el icono es verde.
- Si es necesario optimizar el elemento de detección, el icono es amarillo. Haga clic**Detalles**Para ver los detalles del resultado del escaneo, haga clic en**Ignorar**para ignorar la excepción y no se escaneará en el próximo escaneo.

Figura 4-36 Detalles



- Si no se escaneará el elemento de detección, el ícono estará gris. Haga clic**Detección de inicio**para incluir el elemento de detección en el próximo escaneo.

Pase el cursor sobre el elemento de detección para ver la configuración de la detección actual.

Escaneo de módulos de seguridad

Pase el cursor sobre el ícono del módulo de seguridad para ver el estado operativo.

4.11.2 Configuración del servicio del sistema

Información de contexto

Cree un certificado o cargue un certificado autenticado y luego podrá iniciar sesión a través de HTTPS con su PC. El protocolo HTTPS puede proteger la autenticidad de las páginas en todo tipo de sitios web, proteger las cuentas y mantener privadas las comunicaciones, la identidad y la navegación web de los usuarios.

Le recomendamos que habilite el protocolo HTTPS. De lo contrario, los datos del dispositivo podrían filtrarse.

Procedimiento

Paso 1 Inicie sesión en la página web del dispositivo.

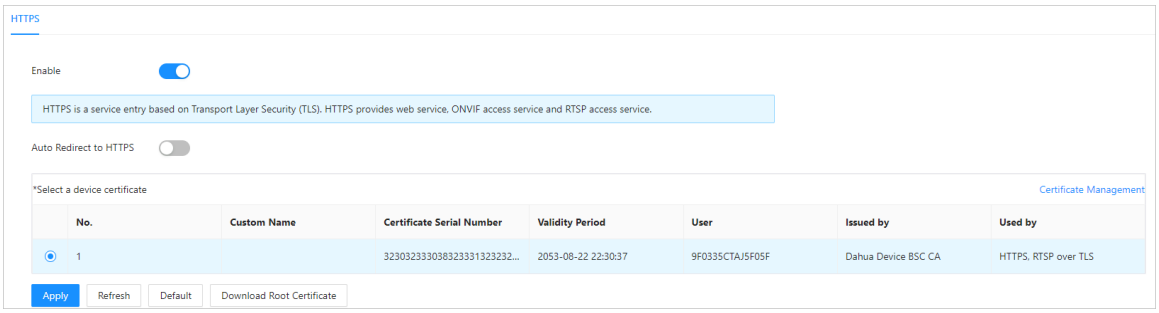
Paso 2 Seleccionar > **Servicio del sistema**.

Paso 3 Hacer clic para habilitar HTTPS.

Paso 4 Seleccione el certificado.

Si no hay ningún certificado en la lista, haga clic en**Gestión de certificados**Para obtener más detalles, consulte "4.11.4 Configuración del certificado CA".

Figura 4-37 HTTPS



Paso 5 Hacer clic**Aplicar**.

Resultados

Ingresa https://*Dirección IP: puerto https*en el navegador.

- Si ya ha instalado el certificado, se mostrará la página de inicio de sesión normal.
- Si no ha instalado el certificado, el navegador muestra un mensaje de error de certificado.

4.11.3 Defensa de ataque

4.11.3.1 Configuración del firewall

Configurar el firewall para limitar el acceso al dispositivo.

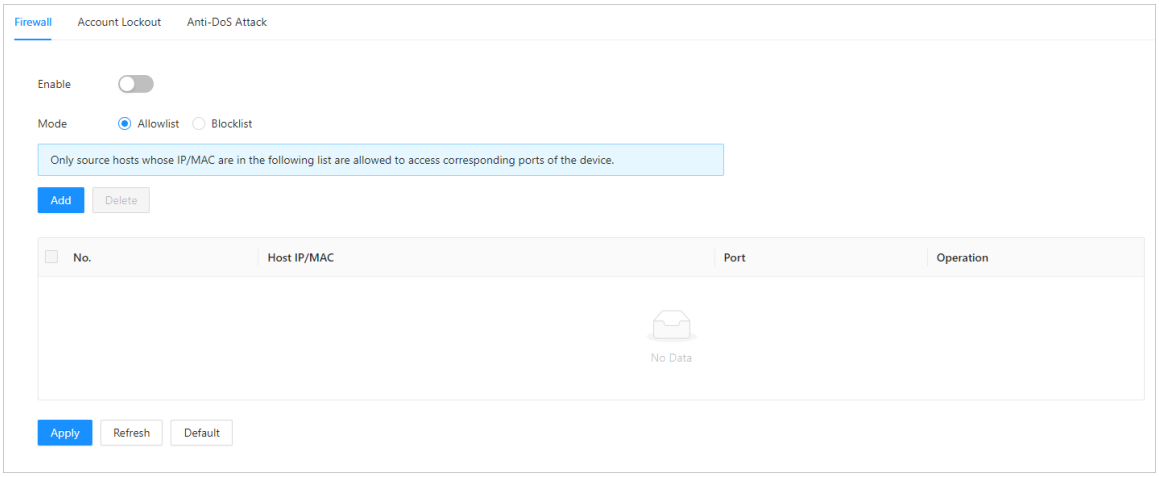
Procedimiento

Paso 1 Inicie sesión en la página web del dispositivo.

Paso 2 Seleccionar > **Ataque Defensa**>**Cortafuegos**.

Paso 3 Hacer clic para habilitar la función de firewall.

Figura 4-38 Cortafuegos

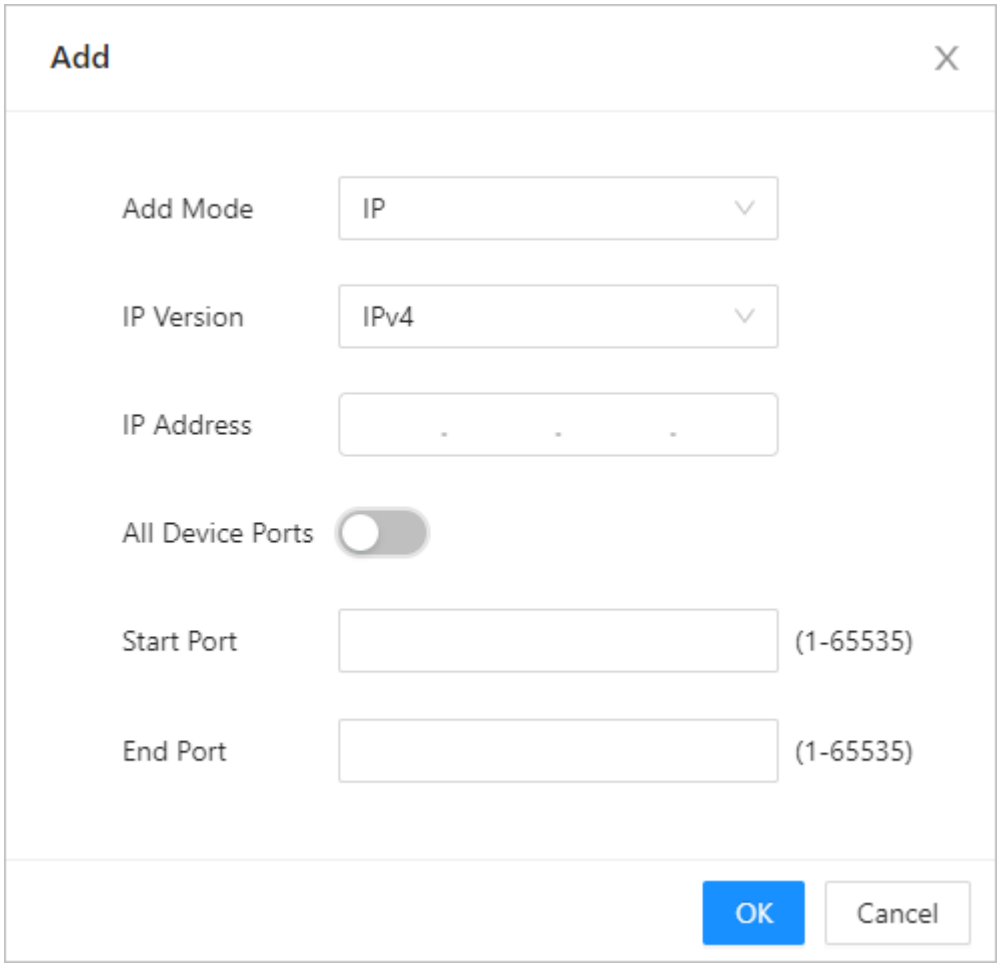


Paso 4 Seleccionar**Lista de permitidos**o**Lista de bloqueo**como el modo.

- Lista de permitidos: solo cuando la dirección IP/MAC de su PC se encuentra en la lista de permitidos, podrá acceder al dispositivo. Los puertos son los mismos.
- Lista de bloqueo: cuando la dirección IP/MAC de su PC está en la lista de bloqueo, no puede acceder al dispositivo. Los puertos son los mismos.

Paso 5 Hacer clic**Agregar**para agregar la dirección IP/MAC del host a**Lista de permitidos**o**Lista de bloqueo**y luego haga clic en**DE ACUERDO**.

Figura 4-39 Agregar la dirección



Paso 6 Hacer clic**Aplicar**.

Operaciones relacionadas

- Hacer clic para editar la información del host. para
- Hacer clic eliminar la información del host.

4.11.3.2 Configuración del bloqueo de cuenta

Si ingresa consecutivamente una contraseña incorrecta mayor que el valor configurado, la cuenta se bloqueará.

Procedimiento

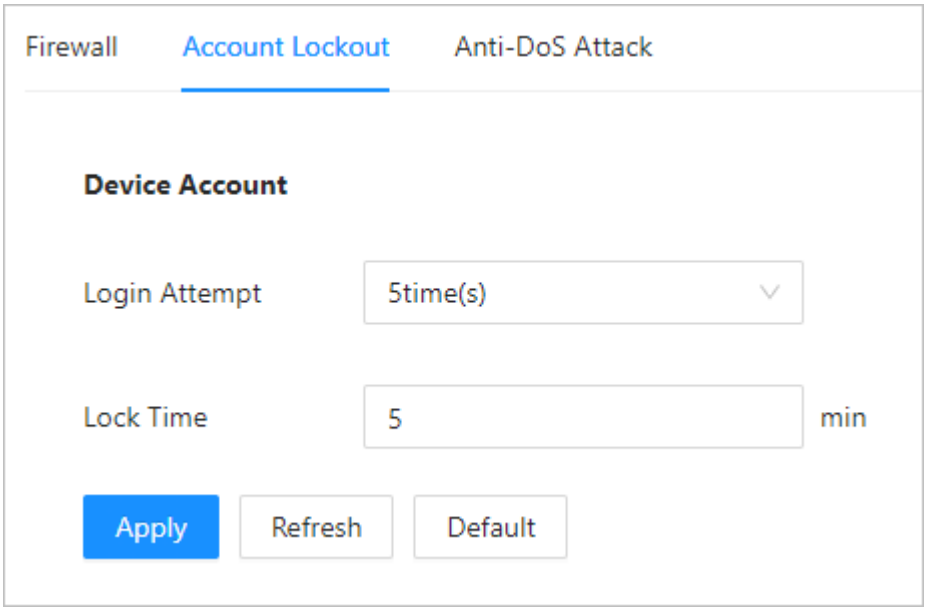
Paso 1 Inicie sesión en la página web del dispositivo.

Paso 2 Seleccionar > **Ataque Defensa**>**Bloqueo de cuenta**.

Paso 3 Configure el intento de inicio de sesión y el tiempo de bloqueo para la cuenta del dispositivo y el usuario ONVIF.

- Intento de inicio de sesión: límite superior de intentos de inicio de sesión. Si ingresa una contraseña incorrecta varias veces, más del valor definido, la cuenta se bloqueará.
- Tiempo de bloqueo: el período durante el cual no puede iniciar sesión después de que los intentos de inicio de sesión alcanzan el límite superior.

Figura 4-40 Bloqueo de cuenta



Paso 4 Hacer clic**Aplicar**.

4.11.3.3 Configuración de ataques anti-DoS

Puedes habilitar**Defensa contra ataques de inundación SYN**o**Defensa contra ataques de inundación ICMP**para defender el dispositivo contra ataques DoS (denegación de servicio).

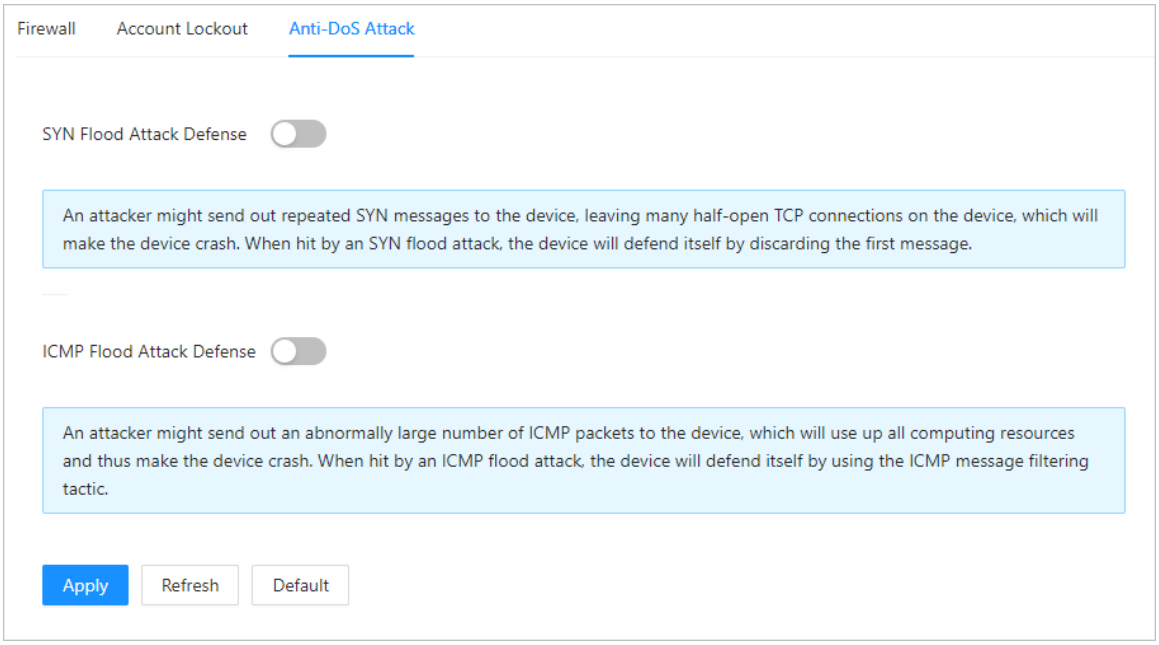
Procedimiento

Paso 1 Inicie sesión en la página web del dispositivo.

Paso 2 Seleccionar > **Ataque Defensa**>**Ataque anti-DoS**.

Paso 3 Permitir**Defensa contra ataques de inundación SYN**o**Defensa contra ataques de inundación ICMP**para defender el dispositivo contra ataques DoS (denegación de servicio).

Figura 4-41 Ataque anti-DoS



Paso 4 Hacer clic**Aplicar**.

4.11.4 Configuración del certificado CA

4.11.4.1 Instalación del certificado del dispositivo

Cree un certificado o cargue un certificado autenticado, por ejemplo, cuando inicia sesión a través de HTTPS con su PC, debe verificar el certificado del dispositivo.

4.11.4.1.1 Creación de certificado

Procedimiento

Paso 1 Inicie sesión en la página web del dispositivo.

Paso 2 Seleccionar > **Certificado CA**>**Certificado del dispositivo**Haga

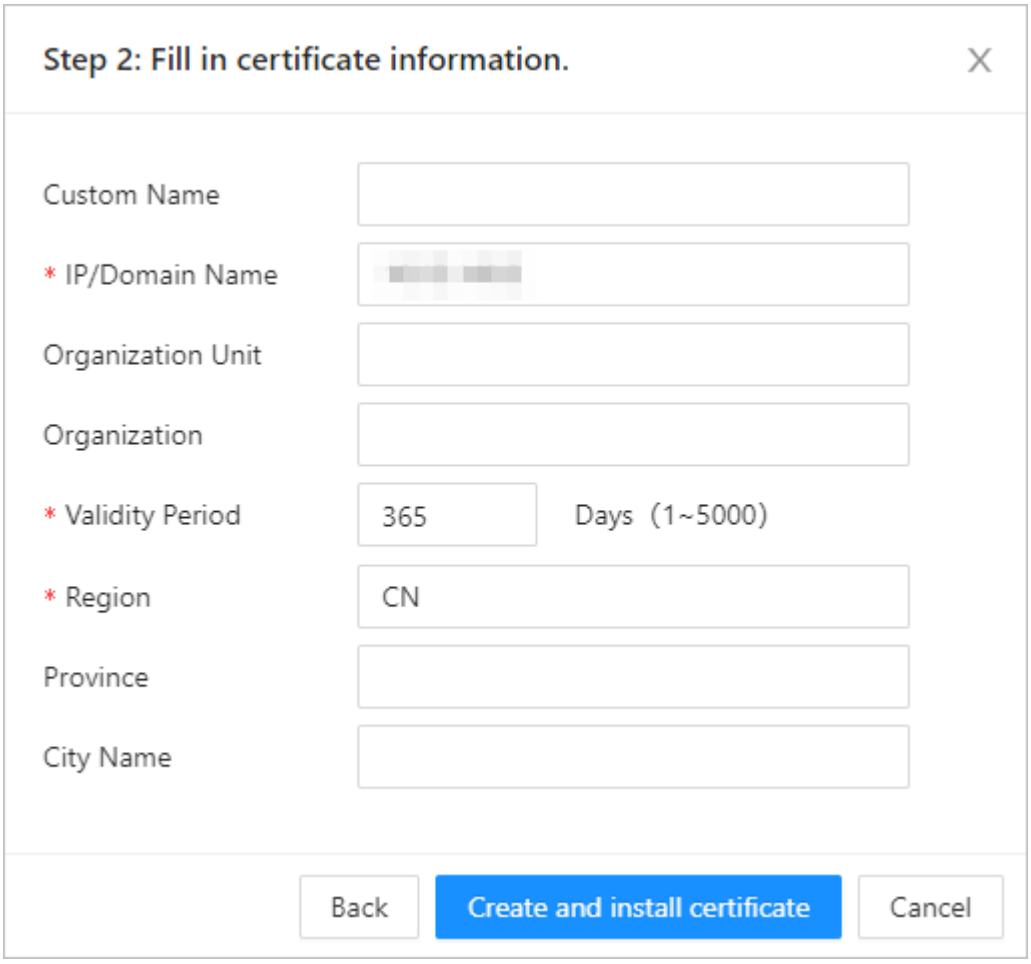
Paso 3 clic en**Instalar certificado de dispositivo**.

Paso 4 Seleccionar**Crear certificado**,y luego haga clic**Próximo**.

Paso 5 Ingrese la información del certificado.

La IP o el nombre de dominio del dispositivo se ingresa automáticamente en**Nombre de dominio/IP**.

Figura 4-42 Información del certificado



Paso 6 Hacer clic**Crear e instalar certificado**.

Una vez creado el certificado correctamente, puede verlo en el **Certificado del dispositivo**página.

Operaciones relacionadas

- Hacer clic**Entrar al modo de edición**para editar el nombre personalizado del certificado.
- Hacer clic para descargar el certificado.
- Hacer clic para eliminar el certificado.

4.11.4.1.2 Solicitud e importación de un certificado de CA

Importe el certificado CA de terceros al dispositivo.

Procedimiento

Paso 1 Inicie sesión en la página web del dispositivo.

Paso 2 Seleccionar > **Certificado CA**>**Certificado del dispositivo**Haga

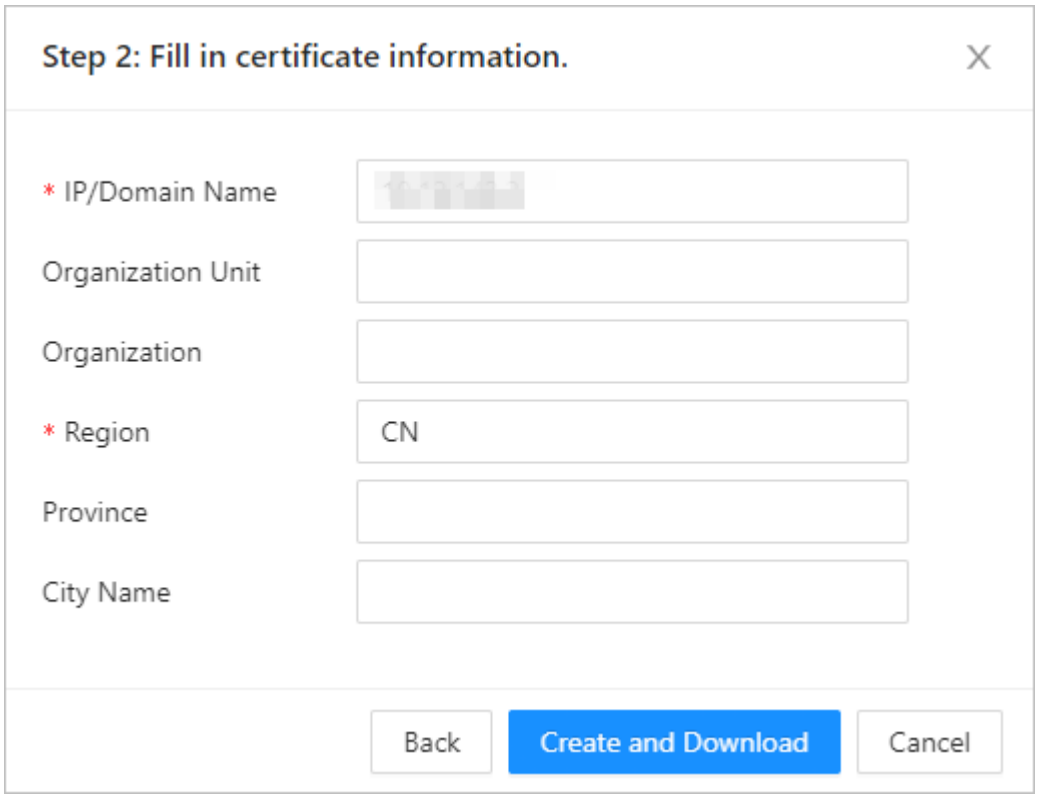
Paso 3 clic en**Instalar certificado de dispositivo**.

Paso 4 Seleccionar**Solicitar certificado CA e importación (recomendado)**,y luego haga clic**Próximo**. Ingrese

Paso 5 la información del certificado.

La IP o el nombre de dominio del dispositivo se ingresa automáticamente en**Nombre de dominio/IP**.

Figura 4-43 Información del certificado



Paso 6 Hacer clic**Crear y descargar**.

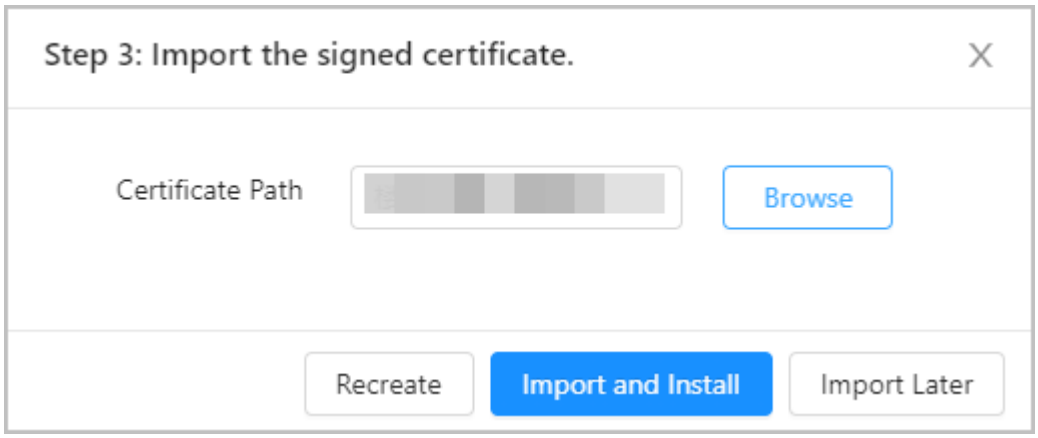
Guarde el archivo de solicitud en su PC.

Paso 7 Solicite el certificado de CA a la autoridad de certificación externa. Importe

Paso 8 el certificado de CA firmado.

1. Guarde el certificado de CA en la PC.
2. Seleccionar**Instalar certificado de dispositivo**,hacer clic**Solicitar certificado CA e importación (recomendado)**y luego haga clic en**Próximo**.
3. Haga clic**Navegar**para seleccionar el certificado CA firmado.

Figura 4-44 Importar el certificado CA firmado



4. Haga clic**Importar e instalar**.

   Una vez creado el certificado correctamente, puede verlo en el **Certificado del dispositivo**página.

   - Hacer clic**Recrear**para crear nuevamente el archivo de solicitud.
   - Hacer clic**Importar más tarde**para importar el certificado la próxima vez.

Operaciones relacionadas

- Hacer clic**Entrar al modo de edición**para editar el nombre personalizado del certificado.
- Hacer clic para descargar el certificado.
- Hacer clic para eliminar el certificado.

4.11.4.1.3 Instalación de un certificado existente

Importe el certificado de terceros existente al dispositivo. Cuando solicite el certificado de terceros, también deberá solicitar el archivo de clave privada y la contraseña de la clave privada.

Procedimiento

Paso 1 Inicie sesión en la página web del dispositivo.

Paso 2 Seleccionar > **Certificado CA**>**Certificado del dispositivo**Haga

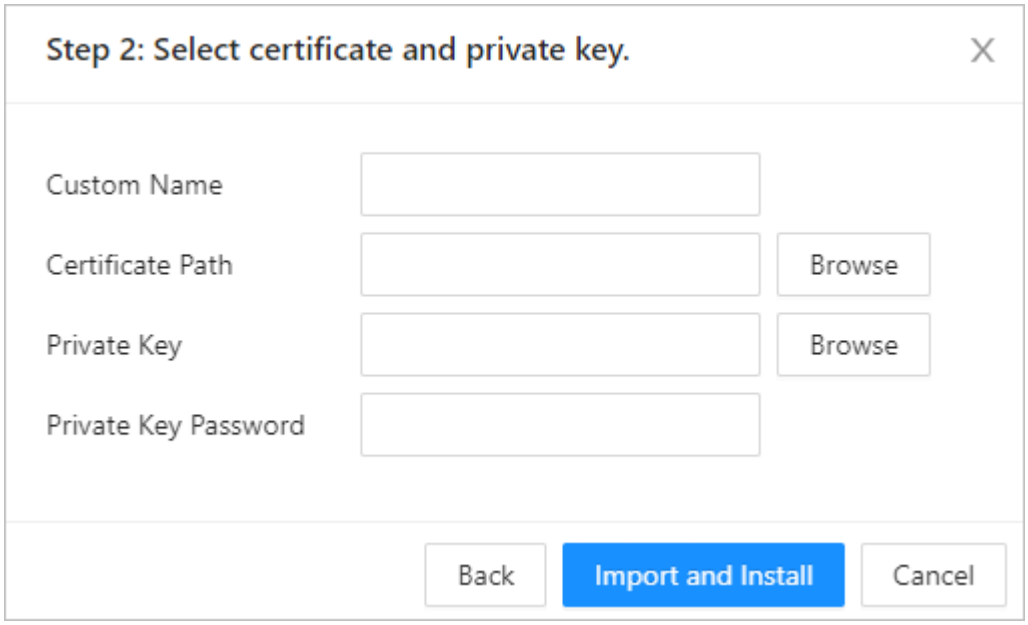
Paso 3 clic en**Instalar certificado de dispositivo**.

Paso 4 Seleccionar**Instalar certificado existente**,y luego haga clic**Próximo**Haga clic en

Paso 5 **Navegar**para seleccionar el certificado y el archivo de clave privada.

Introduzca la contraseña de la clave privada si el archivo de clave privada está cifrado.

Figura 4-45 Certificado y clave privada



Operaciones relacionadas

- Hacer clic**Entrar al modo de edición**para editar el nombre personalizado del certificado.
- Hacer clic para descargar el certificado.
- Hacer clic para eliminar el certificado.

4.11.4.2 Instalación de un certificado CA de confianza

El certificado CA es un certificado digital que acredita la identidad legal de la cámara. Por ejemplo, cuando la cámara accede a la LAN a través de 802.1x, se requiere el certificado CA.

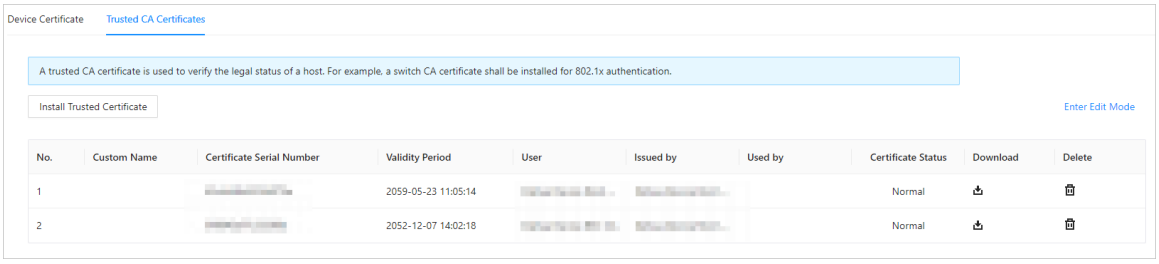
Procedimiento

Paso 1 Inicie sesión en la página web del dispositivo.

Paso 2 Seleccionar > **Certificado CA**>**Certificado CA de confianza**Haga clic

Paso 3 en**Instalar certificado de confianza**.

Figura 4-46 Instalar certificado confiable



Paso 4 Hacer clic**Navegar**En la ventana emergente, seleccione el certificado. Haga clic en**DE**

Paso 5 **ACUERDO**para importar el certificado de confianza.

Una vez que el certificado se haya importado correctamente, puede verlo en el **Certificado CA de confianza**página.

Operaciones relacionadas

- Hacer clic**Entrar al modo de edición**para editar el nombre personalizado del certificado.

- Hacer clic para descargar el certificado.
- Hacer clic para eliminar el certificado.

4.11.5 Configuración del cifrado de vídeo

El dispositivo admite el cifrado de audio y vídeo durante la transmisión de datos.

Información de contexto

Le recomendamos que habilite la función de cifrado de video. Si no habilita esta función, puede haber riesgos de seguridad.

Sólo VTA250*incógnita*La Serie G admite esta función.

Procedimiento

Paso 1 Inicie sesión en la página web del dispositivo.

Paso 2 Seleccionar > **Encriptación de video**.

Paso 3 Configure los parámetros y luego haga clic en**Aplicar**.

Figura 4-47 Cifrado de video

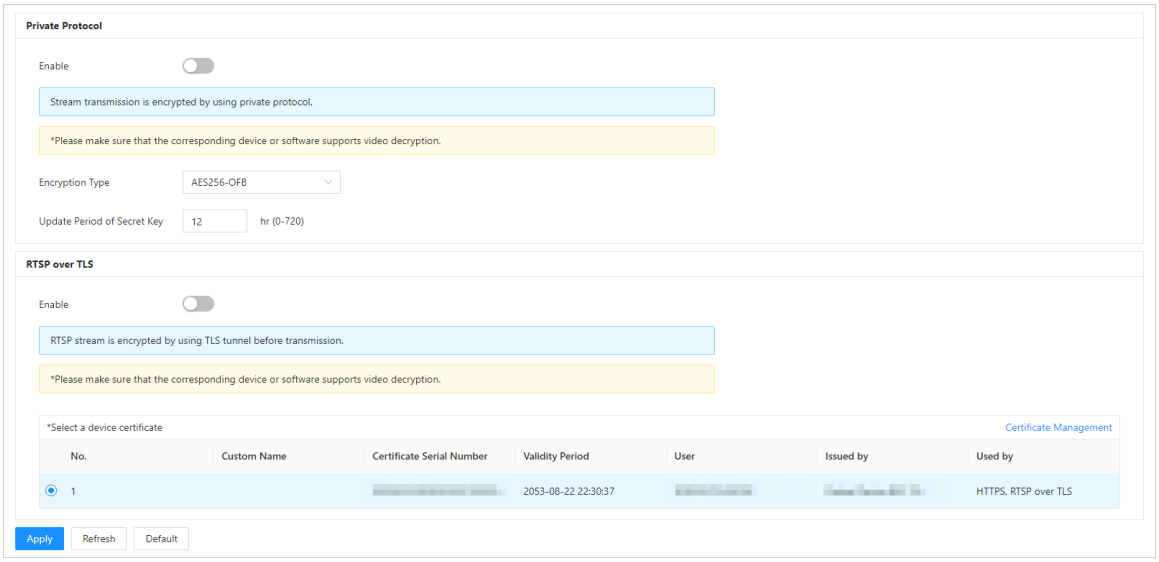


Tabla 4-17 Descripción de los parámetros de cifrado de vídeo

Área	Parámetro	Descripción
Protocolo privado	Permitir	Habilite el cifrado de cuadros de flujo mediante el uso de un protocolo privado. Hacer clic para habilitar el cifrado de audio y video durante Transmisión de datos. Seleccione el tipo de cifrado y, a continuación, configure el período de actualización de la clave secreta. ● **Tipo de cifrado**:Utilice la configuración predeterminada. ● **Periodo de actualización de la clave secreta**:El rango de valores es de 0 a 720 horas. 0 significa nunca actualizar la clave secreta.
	Tipo de cifrado	
	Periodo de actualización de Clave secreta	

Área	Parámetro	Descripción
RTSP sobre TLS	Permitir	Habilita el cifrado de transmisión RTSP mediante TLS. Hacer clic y luego seleccione un certificado de dispositivo de lista de certificados.
	Certificado Gestión	Para obtener más información sobre la administración de certificados, consulte "4.11.4 Configuración de certificados de CA". Los certificados creados o importados se muestran en**Seleccione un certificado de dispositivo**lista.

4.11.6 Configuración de advertencias de seguridad

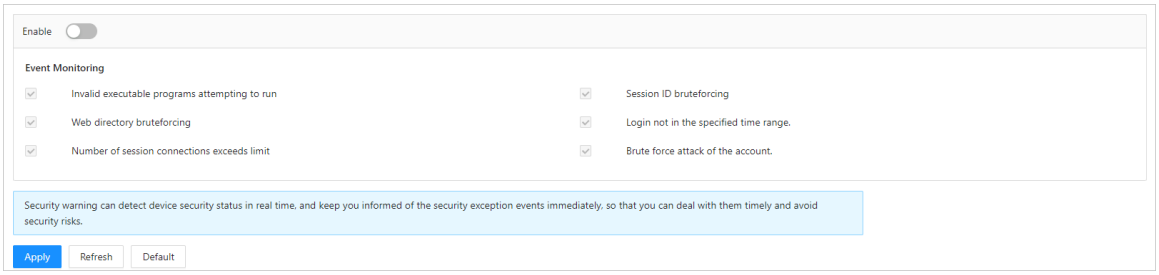
Procedimiento

Paso 1 Inicie sesión en la página web del dispositivo.

Paso 2 Seleccionar > **Advertencia de seguridad**.

Paso 3 Habilite la función de advertencia, seleccione los eventos y luego haga clic en**Aplicar**.

Figura 4-48 Advertencia de seguridad



4.11.7 Configuración de la autenticación de seguridad

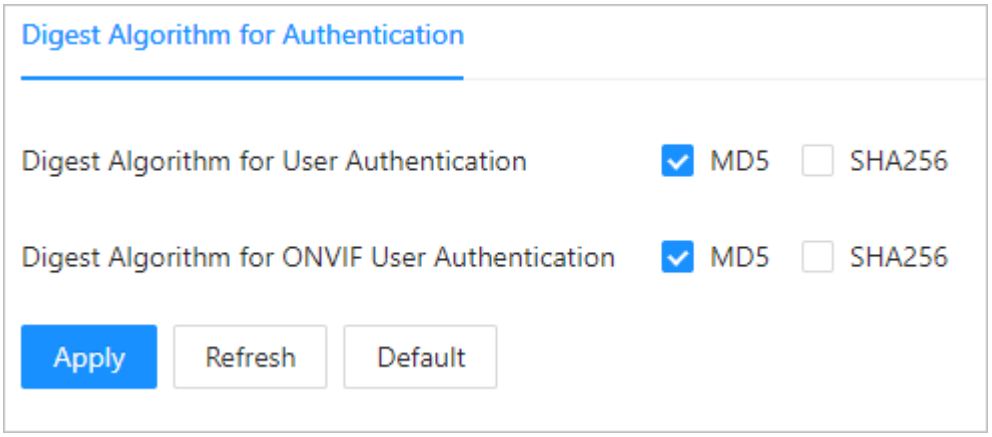
Procedimiento

Paso 1 Inicie sesión en la página web del dispositivo.

Paso 2 Seleccionar > **Autenticación de seguridad**Seleccione los

Paso 3 algoritmos de resumen y luego haga clic en**Aplicar**.

Figura 4-49 Autenticación de seguridad



Apéndice 1 Recomendaciones de ciberseguridad

Acciones obligatorias a 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, se recomienda 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.**Establecer y actualizar contraseñas Restablecer información oportunamente**

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 dirección 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, se recomienda desactivar algunos servicios como SNMP, SMTP, UPnP, etc., para reducir riesgos.

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

- SNMP: elija SNMP v3 y configure contraseñas de 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. **Construir 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.