Cámara de red web 5.0

Manual de funcionamiento

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.0.0

Prólogo

General

Este manual incluye las funciones, la configuración, el funcionamiento general y el mantenimiento del sistema de la cámara de red.

Instrucciones de seguridad

En el manual pueden aparecer las siguientes palabras de señalización clasificadas con significado definido.

Palabras de señalización	Significado
 ADVERTENCIA	Indica un riesgo de potencial medio o bajo que, de no evitarse, podría ocasionar lesiones leves o moderadas.
 PRECAUCIÓN	Indica un riesgo potencial que, de no evitarse, podría ocasionar daños en la propiedad, pérdida de datos, bajo rendimiento u otro resultado impredecible.
 CONSEJOS	Proporciona métodos para ayudarle a solucionar un problema o ahorrar tiempo.
 NOTA	Proporciona información adicional como énfasis o complemento al texto.

Historial de revisión

Versión	Contenido de la revisión	Fecha de lanzamiento
V1.0.0	Primer lanzamiento.	Octubre de 2020

Acerca del manual

- El manual es solo una referencia. Si detecta alguna discrepancia entre el manual y el producto real, el producto real prevalecerá.
- No aceptaremos ninguna responsabilidad por las pérdidas producidas por el uso del dispositivo sin seguir las indicaciones del manual.
- El manual se actualizará en conformidad con las últimas leyes y normativas de las jurisdicciones relacionadas. Para ver más información, consulte el manual impreso, el CD-ROM, el código QR o nuestra página web oficial. En caso de existir una discrepancia entre el manual impreso y la versión electrónica, prevalecerá la versión electrónica.
- Todos los diseños y el software aquí incluidos están sujetos a cambios sin aviso previo por escrito. Las actualizaciones del producto podrían ocasionar discrepancias entre el producto real y el manual. Contacte con el servicio de atención al cliente solicitando el programa actualizado y la documentación suplementaria.
- Aun así podría haber alguna desviación en los datos técnicos, funciones y descripción de las operaciones, o errores de impresión. Si existiera alguna duda o controversia, nos reservamos el derecho de explicación final.
- Actualice el software del lector o intente con otro software lector convencional en el caso de que no pueda abrir el manual (en formato PDF).

- Todas las marcas comerciales, marcas comerciales registradas y nombres de empresas en el manual pertenecen a sus respectivos propietarios.
- Visite nuestra página web, contacte con su vendedor o con el servicio de atención al cliente si tiene problemas al usar el dispositivo.
- Si hubiera incertidumbres o controversias, nos reservamos el derecho de explicación final.

Advertencias y precauciones de seguridad importantes

Seguridad eléctrica

- Todas las instrucciones de utilización e instalación deben realizarse conforme a las normas de seguridad eléctrica de su país.
- La fuente de alimentación debe cumplir con el estándar de seguridad de bajo voltaje (SELV) y suministrar potencia con un voltaje nominal que cumpla con el requisito de fuente de energía limitada de acuerdo con IEC60950-1. Los requisitos de la fuente de alimentación están indicados en la etiqueta del dispositivo.
- Asegúrese de que la fuente de alimentación sea la adecuada antes de utilizar el dispositivo.
- Es necesario incorporar un dispositivo de desconexión de fácil acceso en el cableado de la instalación del edificio.
- Evite que el cable de alimentación quede aplastado o presionado, especialmente en el conector, la toma de corriente y en el punto de unión que sale del dispositivo.

Entorno de funcionamiento

- No apunte el dispositivo directamente a una luz fuerte a la hora de realizar el enfoque, como la luz de una lámpara y la luz solar; de lo contrario, podría causar un exceso de brillo o marcas de luz, que no serán provocados a causa de un mal funcionamiento del dispositivo y podría afectar a la vida útil del semiconductor complementario de óxido de metal (CMOS).
- No coloque el dispositivo en un ambiente húmedo, polvoriento, extremadamente caliente o frío, o en lugares con radiación electromagnética fuerte o iluminación inestable.
- Mantenga el dispositivo alejado de cualquier líquido para evitar que se produzcan daños en los componentes internos.
- Mantenga el dispositivo interior alejado de la lluvia o la humedad para evitar incendios o rayos.
- Mantenga una buena ventilación para evitar la acumulación de calor.
- Transporte, utilice y guarde el dispositivo conforme a los límites permitidos de humedad y temperatura.
- No someta a la unidad a grandes presiones, fuertes vibraciones o salpicaduras de agua durante el transporte, el almacenamiento y la instalación.
- Cuando vaya a transportar el dispositivo, guárdelo en el paquete de fábrica o utilice materiales equivalentes.
- Instale el dispositivo en un lugar al que solo pueda acceder el personal profesional con los conocimientos correspondiente sobre las protecciones de seguridad y las advertencias. De lo contrario, se podrían producir daños a personas no profesionales que ingresen al área de instalación cuando el dispositivo está funcionando con normalidad.

Utilización y mantenimiento diario

- No toque el componente de disipación de calor del dispositivo para evitar quemaduras.

- Siga cuidadosamente las instrucciones del manual cuando realice cualquier operación de desmontaje del dispositivo; de lo contrario, podría ocasionar fugas de agua o una mala calidad de imagen debido a un desmontaje no profesional. Póngase en contacto con el servicio posventa para reemplazar el desecante si existe niebla condensada en la lente después cuando saque el producto de la caja o si el desecante se vuelve verde. (No todos los modelos incluyen desecante).
- Es recomendable usar el dispositivo junto con un pararrayos, para mejorar el efecto de protección de rayos.
- Se recomienda conectar a tierra el dispositivo para mejorar la fiabilidad.
- No toque el sensor de imagen (CMOS) directamente. El polvo y la suciedad pueden eliminarse con un soplador de aire, o puede limpiar la lente suavemente con un paño suave humedecido con alcohol.
- Puede limpiar la carcasa del dispositivo con un paño suave y seco y, para las manchas más complicadas, utilice el paño con un detergente suave. Para evitar posibles daños en el revestimiento de la carcasa del dispositivo que podrían ocasionar una disminución del rendimiento, no utilice disolventes volátiles como alcohol, benceno, aguarrás, etc., para limpiar la carcasa del dispositivo, ni tampoco puede utilizar un detergente fuerte y abrasivo.
- La cubierta abovedada es un componente óptico. No toque ni limpie la cubierta con las manos directamente durante la instalación o el funcionamiento. Para retirar el polvo, la grasa o las huellas dactilares, limpie suavemente con un algodón sin aceite humedecido con dietil o un paño suave humedecido. También puede eliminar el polvo con un soplador de aire.

ADVERTENCIA

- Refuerce la protección de la red, los datos del dispositivo y la información personal mediante la adopción de medidas que incluyen, entre otras, el uso de contraseñas seguras, el cambio de contraseñas con regularidad, la actualización del firmware a la última versión y el aislamiento de la red informática. Para algunos dispositivos con versiones de firmware antiguas, la contraseña de ONVIF no se modificará automáticamente junto con la modificación de la contraseña del sistema, y deberá actualizar el firmware o actualizar manualmente la contraseña de ONVIF.
- Utilice componentes o accesorios suministrados por el fabricante y asegúrese de que ingenieros profesionales realicen la instalación y mantenimiento del dispositivo.
- La superficie del sensor de imagen no se debe exponer a la radiación del rayo láser en un entorno en el que se utilice un dispositivo de rayo láser.
- No proporcione dos o más fuentes de alimentación para el dispositivo a menos que se especifique lo contrario. El incumplimiento de estas instrucciones podría dañar el dispositivo.

Índice de contenidos

1 Visión general

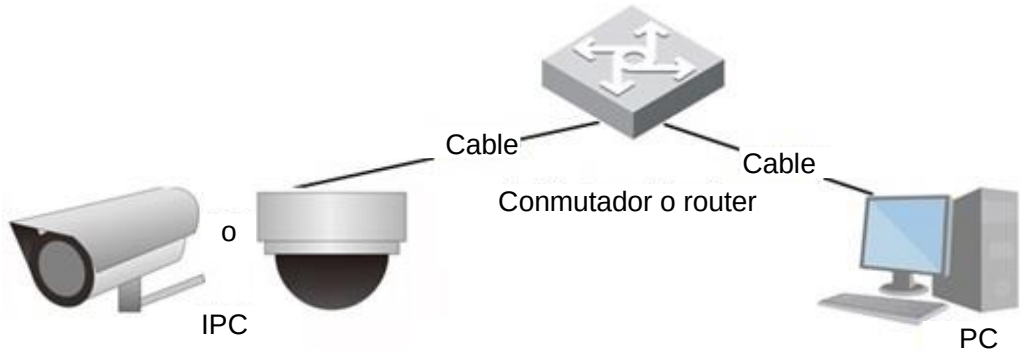
1.1 Introducción

Una cámara IP (cámara de protocolo de Internet), es un tipo de cámara de vídeo digital que recibe datos de control y envía datos de imágenes a través de Internet. Se utilizan comúnmente para la vigilancia y no requieren un dispositivo de grabación local, sino únicamente una red de área local.
La cámara IP se divide en cámara monocanal y cámara multicanal según la cantidad de canales. Para la cámara multicanal, puede configurar los parámetros para cada canal.

1.2 Conexión a la red

En la topología de red general de la cámara IP (IPC), la IPC se conecta al PC a través de un conmutador de red o router.

Figura 1:1 red de la IPC general



Obtenga la dirección IP buscando en ConfigTool y seguidamente podrá comenzar a acceder a la IPC a través de la red.

1.3 Flujo de configuración

Para obtener más información, consulte Figura 1:2. Para ver los detalles, consulte Tabla 1:1. Configure el dispositivo de acuerdo con la situación real.

Figura 1:2 flujo de configuración

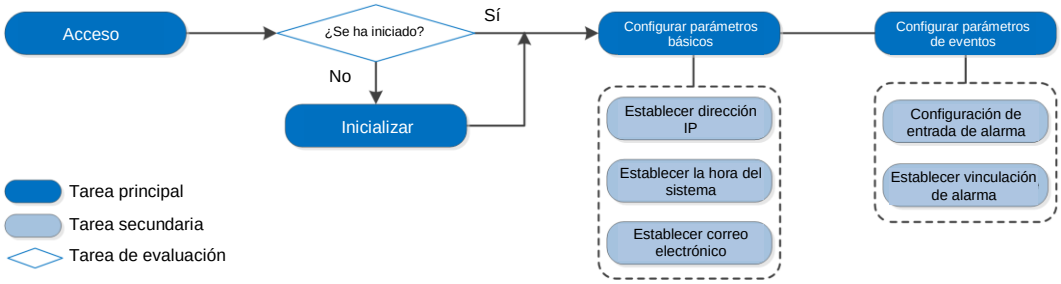


Tabla 1:1 descripción de flujo

Configuración		Descripción	Referencia
Acceso		Abra el navegador IE e ingrese la dirección IP para iniciar sesión en la interfaz web. La dirección IP de la cámara es 192.168.1.108 por defecto.	"3 Acceso".
Inicialización		Inicie la cámara cuando la use por primera vez.	"2 Inicialización del dispositivo"
Parámetros básicos	Dirección IP	Cambie la dirección IP de acuerdo con la planificación de la red para utilizar el producto por primera vez o durante el ajuste de la red.	"5.1.1 TCP/IP"
	Fecha y hora	Configure la fecha y la hora para asegurarse de que la hora de grabación sea la correcta.	"5.3.1.2 Fecha y hora"

2 Inicialización del dispositivo

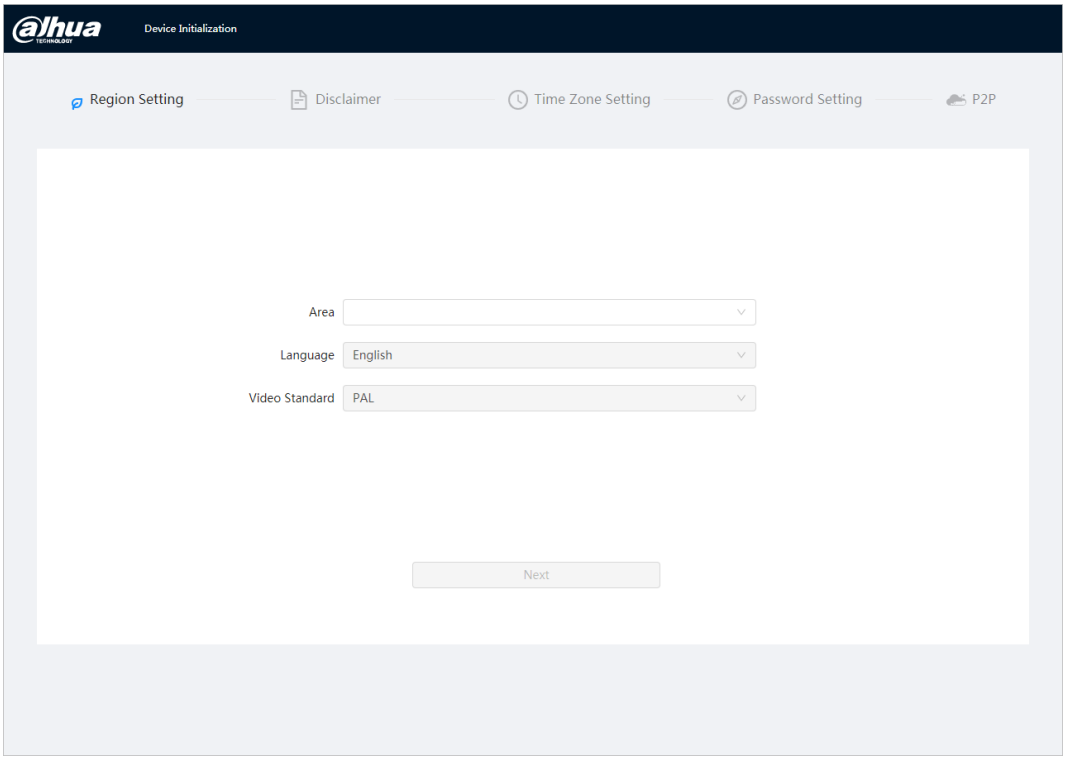
Es necesario iniciar el dispositivo para el primer uso. Este manual se basa en el funcionamiento de la interfaz web. También puede iniciar el dispositivo a través de ConfigTool o NVR.

- Para garantizar la seguridad del dispositivo, mantenga la contraseña correctamente después del inicio y cámbiela con regularidad.
- Al iniciar el dispositivo, mantenga la IP del PC y la IP del dispositivo en la misma red.

Paso 1: Abra el navegador Chrome, ingrese la dirección IP del dispositivo en la barra de direcciones y, a continuación, pulse la tecla Enter.

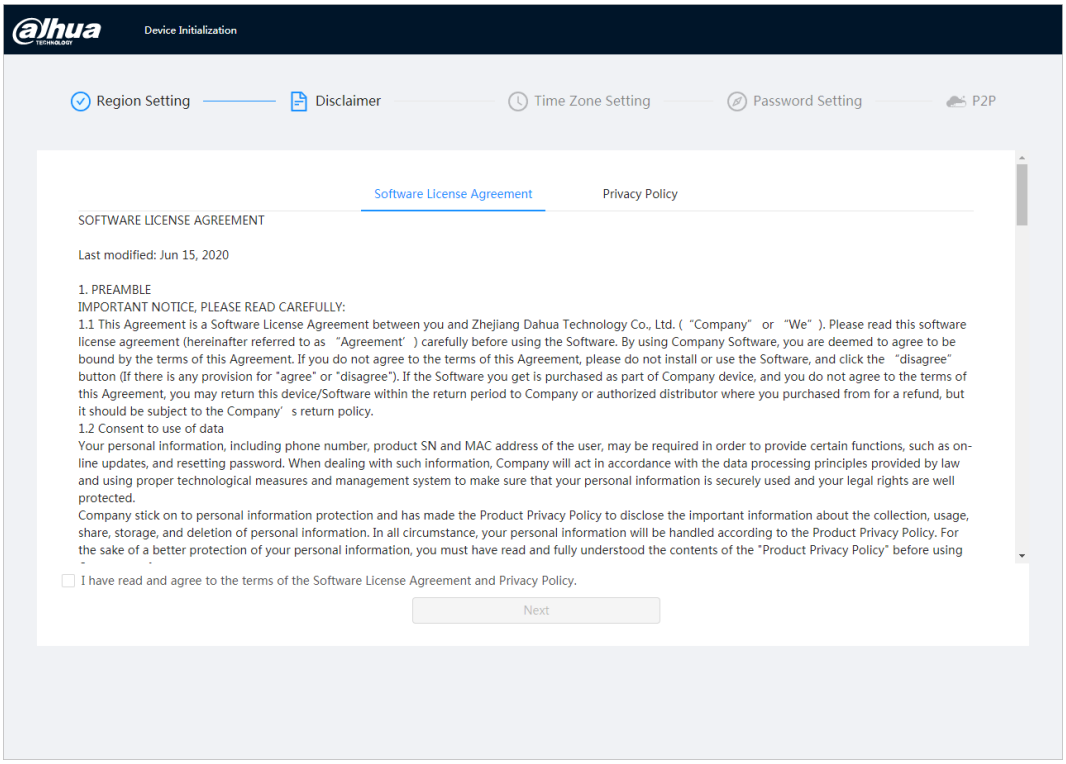
La IP es 192.168.1.108 por defecto.

Figura 2:1 configuración de región



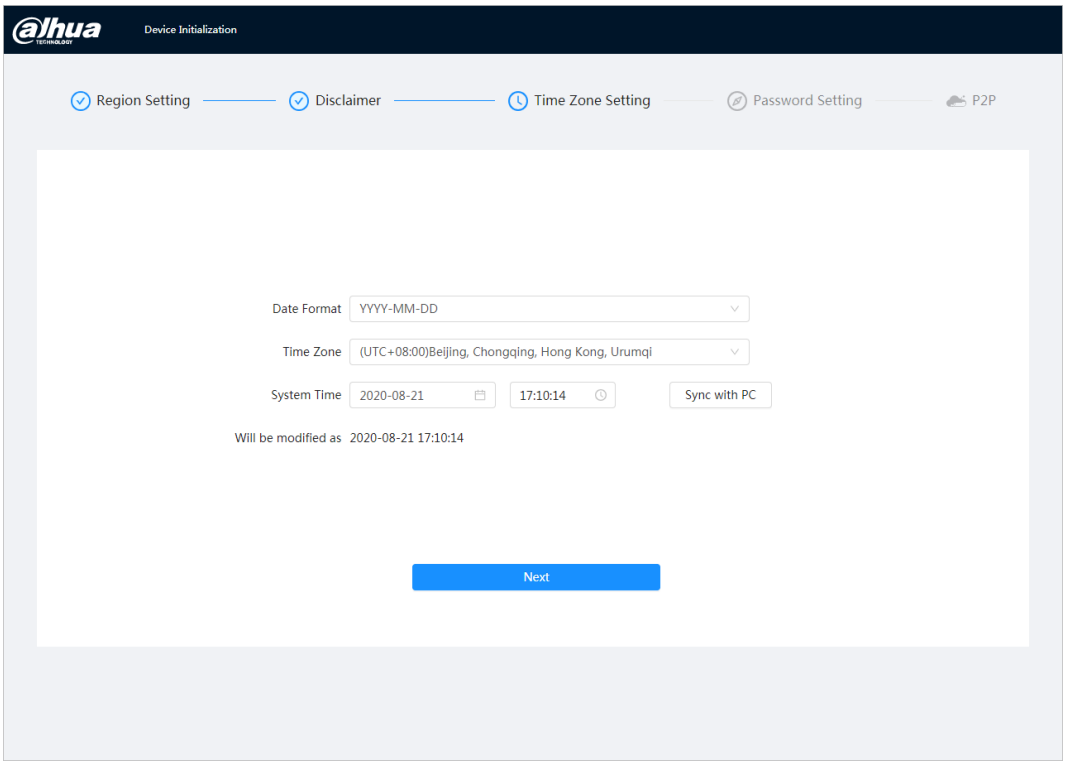
Paso 2: Seleccione el área, el idioma y el estándar de vídeo según la situación real y, a continuación, haga clic en **Siguiente** (Next).

Figura 2:2 descargo de responsabilidad



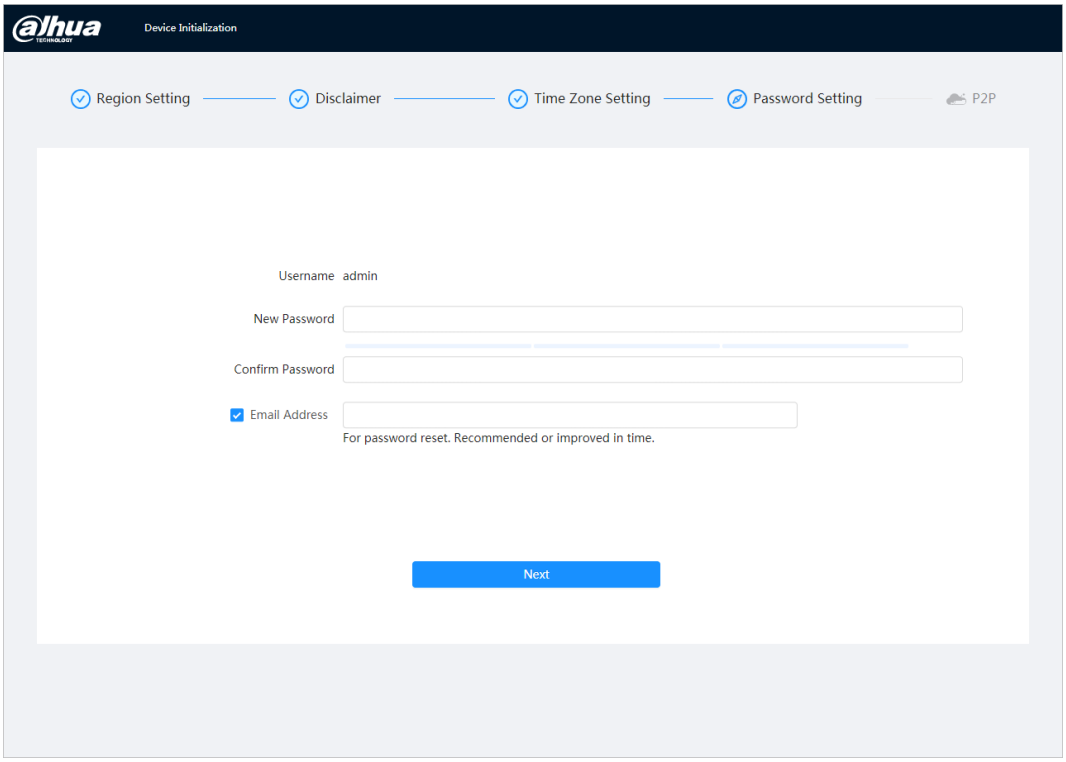
Paso 3: Seleccione la casilla de verificación **He leído y acepto los términos del Acuerdo de licencia de software y la Política de privacidad** (I have read and agree to the terms of the Software License Agreement and Privacy Policy) y, a continuación, haga clic en **Siguiente** (Next).

Figura 2:3 configuración de zona horaria



Paso 4: Configure los parámetros de la hora y, a continuación, haga clic en **Siguiente** (Next).

Figura 2:4 configuración de contraseña



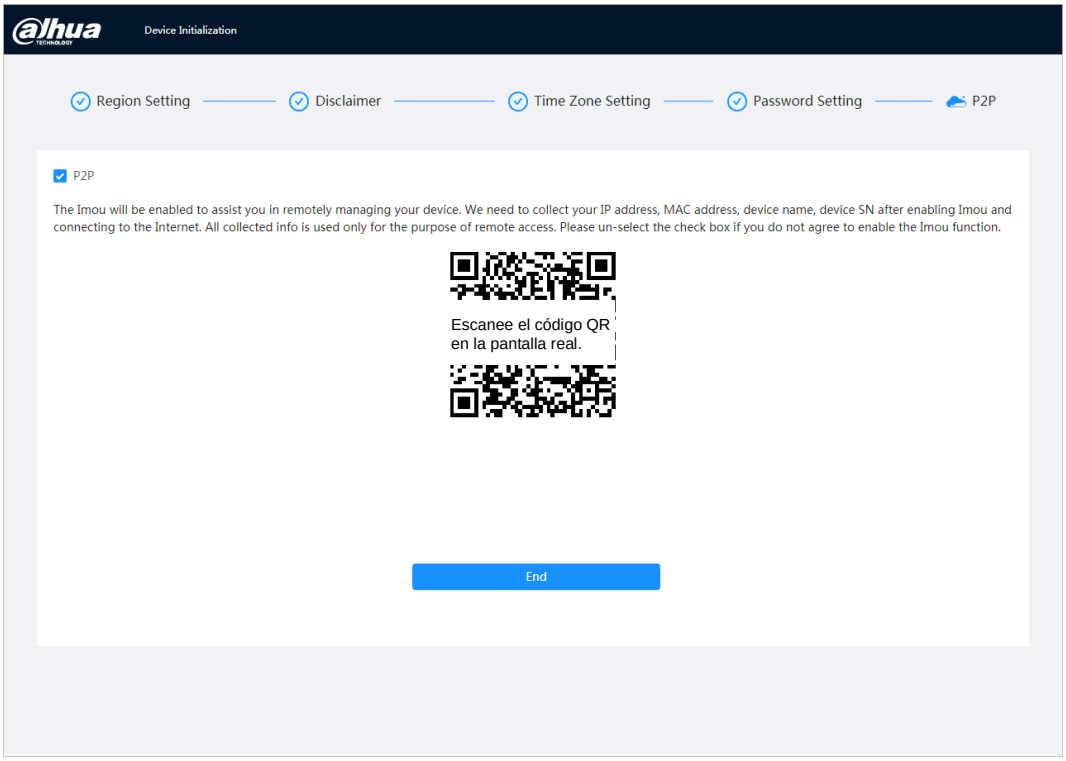
Paso 5: Establezca la contraseña para la cuenta de administrador.

Tabla 2:1 descripción de la configuración de la contraseña

Parámetro	Descripción
NombreUsuario	El nombre de usuario predeterminado es admin.
Contraseña	La contraseña debe constar de 8 a 32 caracteres no vacíos y contener al menos dos tipos de caracteres entre mayúsculas, minúsculas, números y caracteres especiales (excluyendo ‘ " ; : &). Establezca una contraseña con un alto nivel de seguridad de acuerdo con el aviso de seguridad de la contraseña.
Confirmar contraseña	
Correo electrónico guardado	Ingrese una dirección de correo electrónico para restablecer la contraseña y se seleccionará de manera predeterminada. Cuando necesite restablecer la contraseña de la cuenta de administrador, se enviará un código de seguridad para restablecer la contraseña a la dirección de correo electrónico guardada.

Paso 6: Haga clic en **Siguiente** (Next) y, a continuación, aparecerá la interfaz **P2P**.

Figura 2–5 P2P



3 Acceso

3.1 Iniciar sesión en el dispositivo

Esta sección explica cómo iniciar y cerrar sesión en la interfaz web. Esta sección toma como ejemplo al navegador Chrome.

- Debe iniciar la cámara antes de iniciar sesión en la interfaz web. Para conocer los detalles, consulte "2 Inicialización del dispositivo".
- Al iniciar la cámara, mantenga la IP del PC y la IP del dispositivo en la misma red.
- Siga las instrucciones para descargar e instalar el complemento para el primer inicio de sesión.

Paso 1: Abra el navegador Chrome, ingrese la dirección IP de la cámara (192.168.1.108 por defecto) en la barra de direcciones y pulse Enter.
Paso 2: Introduzca el nombre de usuario y la contraseña.
El nombre de usuario es admin de forma predeterminada.

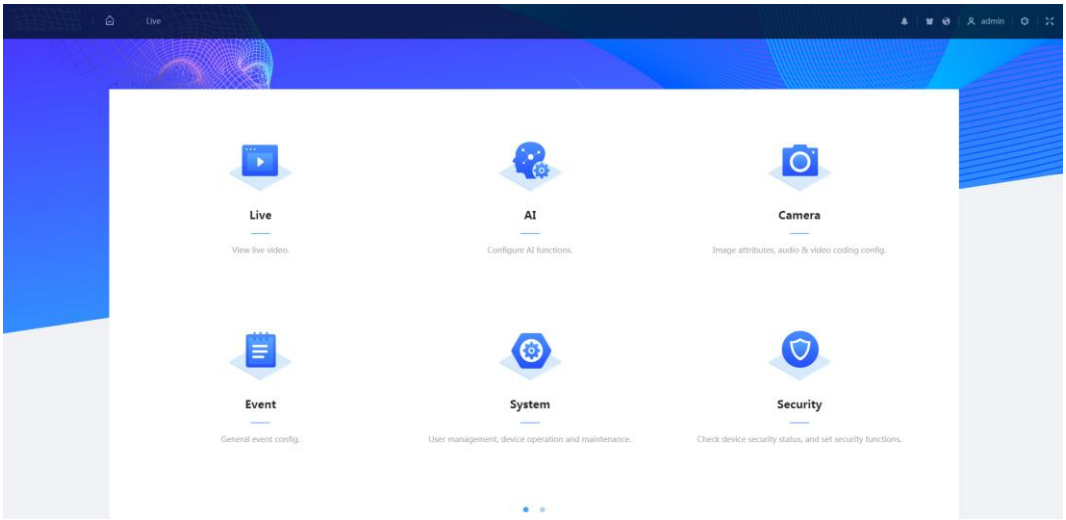
Haga clic en **¿Olvidó la contraseña?** (Forgot password?) para restablecer la contraseña a través de la dirección de correo electrónico que se estableció en el inicio. Para conocer los detalles, consulte "3.2 Restablecer la contraseña."

Figura 3–1 Inicio de sesión

Paso 3: Haga clic en **Iniciar sesión** (Login).
Aparecerá la interfaz **En directo** (Live). Haga clic en en la esquina superior izquierda de la interfaz para que aparezca la interfaz principal.

Para iniciar sesión por primera vez, instale el complemento siguiendo las instrucciones de la pantalla.

Figura 3–2 Pantalla principal



- Directo: vea la imagen de monitoreo en tiempo real.
- IA: configure las funciones de IA de la cámara.
- Cámara: configure los parámetros de la cámara, incluidos los parámetros de imagen, los parámetros del codificador y los parámetros de audio.
- Evento: configure eventos generales, incluida la excepción de la vinculación de alarma, la detección de vídeo y la detección de audio.
- Sistema: configure los parámetros del sistema, incluidos general, fecha y hora, cuenta, seguridad, configuración PTZ, predeterminado, importación/exportación, remoto, mantenimiento automático y actualización.
- Seguridad: verifique el estado de seguridad del dispositivo y configure las funciones de seguridad.
- Grabación: reproduzca o descargue vídeos grabados.
- Imagen: reproduzca o descargue archivos de imagen.
- Informe: busque el informe de eventos de IA y el informe del sistema.

3.2 Restablecer la contraseña

Cuando necesite restablecer la contraseña de la cuenta de administrador, se enviará un código de seguridad a la dirección de correo electrónico ingresada, la cual se podrá utilizar para restablecer la contraseña.

Requisitos previos

Ha habilitado el servicio de restablecimiento de contraseña > **Sistema** (System)> **Cuenta** (Account) > **Usuario** (User).

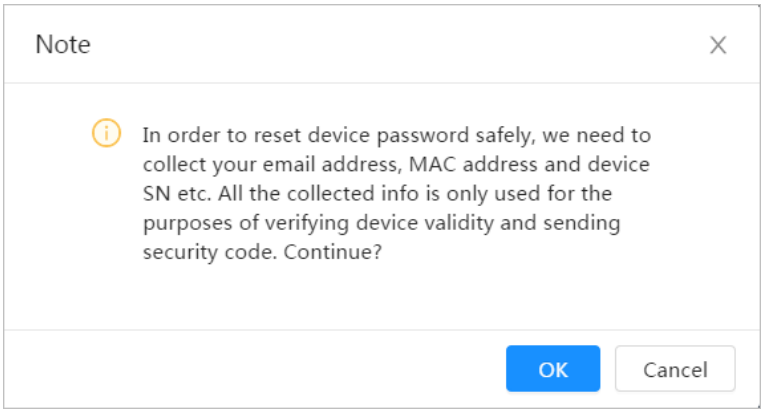
Procedimiento

Paso 1: Abra el navegador Chrome, ingrese la dirección IP del dispositivo en la barra de direcciones y, a continuación, pulse la tecla Enter.

Figura 3–3 Inicio de sesión

Paso 2: Haga clic en **¿Olvidó la contraseña?** (Forgot password?) para restablecer la contraseña a través de la dirección de correo electrónico que se estableció en el inicio.

Figura 3–4 Inicio de sesión



4 Directo

Esta sección presenta el diseño de la interfaz y la configuración de funciones.

4.1 Interfaz En directo

Inicie sesión o haga clic en la pestaña **En directo** (Live).

La interfaz puede variar según los diferentes modelos y prevalecerá la interfaz real.

Figura 4:1 en directo (monocanal)

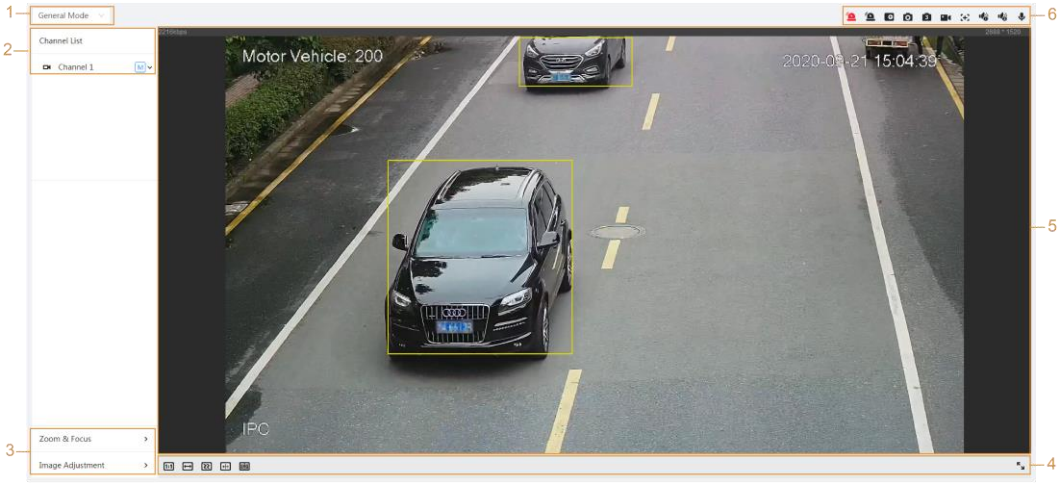


Figura 4:2 en directo (multicanal)

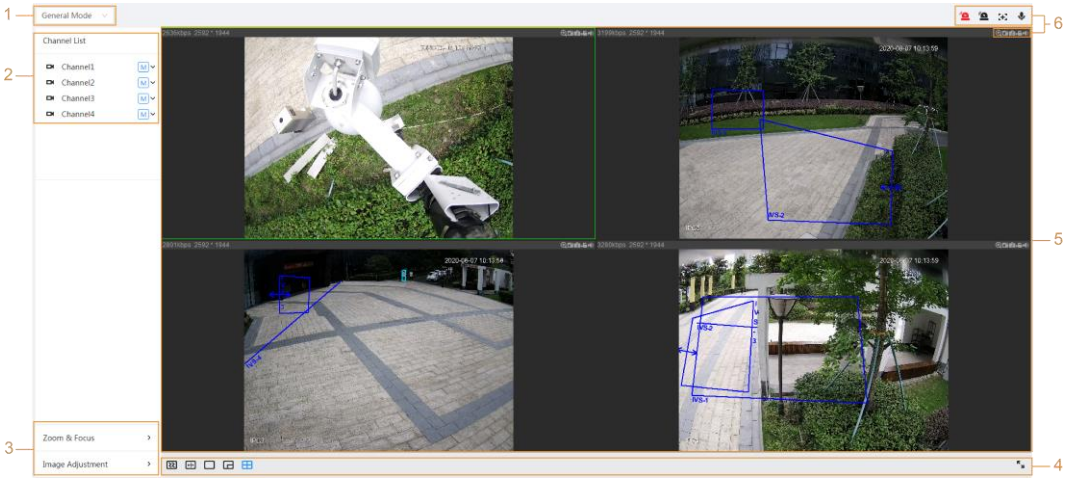


Tabla 4:1 descripción de la barra de funciones

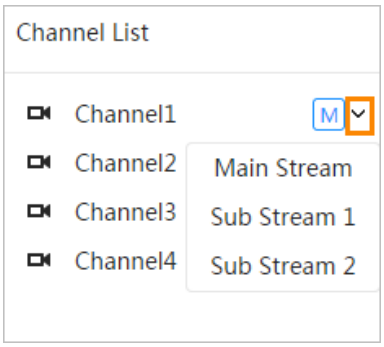
Núm.	Función	Descripción
1	Modo de visualización	Puede seleccionar el modo de visualización entre **Modo general** (General Mode) y **Modo facial** (Face Mode).
2	Lista de canales	Muestra todos los canales. Puede seleccionar el canal según sea necesario y establecer el tipo de transmisión.

Núm.	Función	Descripción
3	Ajuste de imagen	Operaciones de ajuste en visionado en directo.
4		
5	Visionado en directo	Muestra la imagen de monitoreo en tiempo real.
6	Barra de funciones de visionado en directo	Funciones y operaciones en visionado en directo.

4.2 Configuración de codificación

Haga clic en ⌄ y, a continuación, seleccione la transmisión según sea necesario.

Figura 4:3 barra de codificación



- **Transmisión principal:** Tiene un gran valor de transmisión de bits e imagen con alta resolución, pero también requiere un gran ancho de banda. Esta opción se puede usar para almacenamiento y monitorización.
- **Transmisión secundaria:** Tiene un valor de transmisión de bits pequeño y una imagen fluida, y requiere menos ancho de banda. Esta opción se usa normalmente para sustituir la transmisión principal cuando el ancho de banda no es suficiente.
- M significa que la transmisión actual es la transmisión principal; S1 significa que la transmisión actual es la transmisión secundaria 1; S2 significa que la transmisión actual es la transmisión secundaria 2.

5 Config.

Esta sección presenta la configuración básica de la cámara, incluida la configuración de Red, Evento y Sistema.

5.1 Red

Esta sección presenta la configuración de la red.

5.1.1TCP/IP

Puede configurar la dirección IP y el servidor DNS (Sistema de nombres de dominio) y así sucesivamente de acuerdo con la planificación de la red.

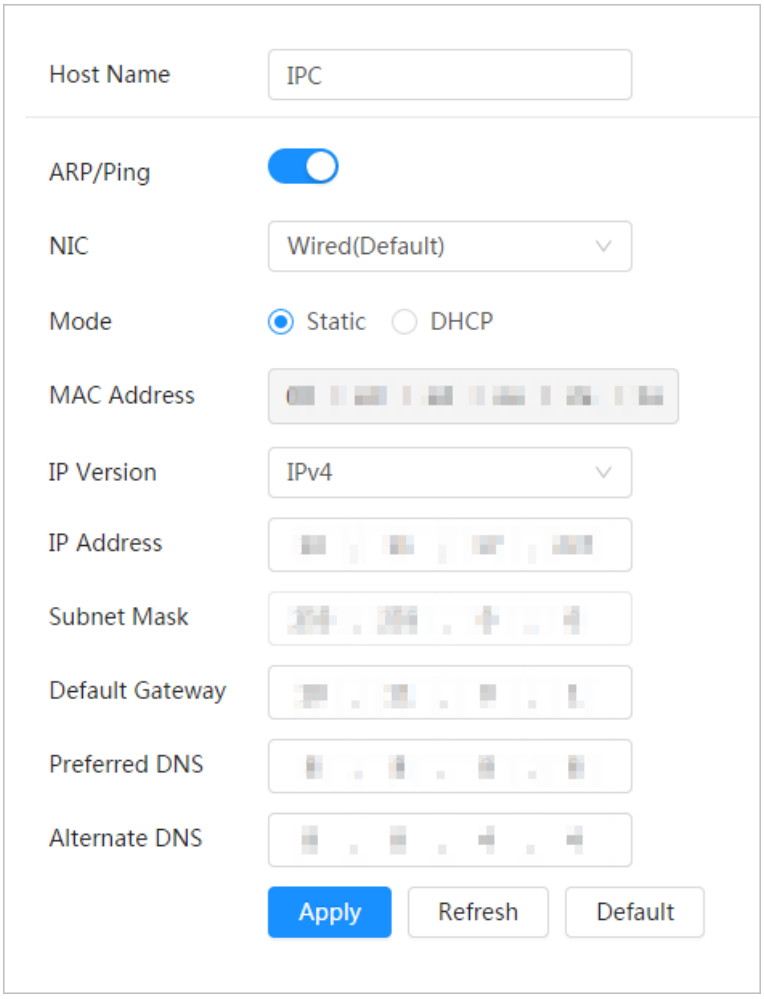
Requisitos previos

La cámara se ha conectado a la red.

Procedimiento

Paso 1: Seleccione  > **Red** (Network) > **TCP/IP** (TCP/IP).

Figura 5–1 TCP/IP



Paso 2: Configure los parámetros de TCP/IP.

Tabla 5:1 descripción de los parámetros de TCP/IP

Parámetro	Descripción
Nombre de host	Ingrese el nombre del host; la longitud máxima es de 15 caracteres.

<table>
<tr><th>Parámetro</th><th>Descripción</th></tr>
<tr><td>ARP/Ping</td><td>Haga clic en  para habilitar ARP/Ping y configurar el servicio de dirección IP. Obtenga la dirección MAC de la cámara para de este modo poder cambiar y configurar la dirección IP del dispositivo con el comando ARP/ping.
Esta característica viene habilitada por defecto. Durante el reinicio, no tendrá más de 2 minutos para configurar la dirección IP del dispositivo mediante un paquete ping con cierta longitud; el servidor se apagará en 2 minutos o se apagará inmediatamente después de que la dirección IP se configure correctamente. Si no se habilita, la dirección IP no se podrá configurar con el paquete ping.
Demostración de cómo configurar la dirección IP con ARP/Ping.
1. Mantenga la cámara que debe configurarse y el PC dentro de la misma red local, y seguidamente obtenga una dirección IP utilizable.
2. Obtenga la dirección MAC de la cámara que aparece en la etiqueta del dispositivo.
3. Abra el editor de comandos en el PC e introduzca el siguiente comando.
Windows syntax
arp –s <IP Address> <MAC>
ping –l 480 –t <IP Address>
Windows example
arp -s 192.168.0.125 11-40-8c-18-10-11
ping -l 480 -t 192.168.0.125
UNIX/Linux/Mac syntax
arp –s <IP Address> <MAC>
ping –s 480 <IP Address>
UNIX/Linux/Mac example
arp -s 192.168.0.125 11-40-8c-18-10-11
ping -s 480 192.168.0.125
4. Reinicie la cámara.
5. Verifique la línea de comando del PC; si aparece el mensaje informativo Responder desde 192.168.0.125…(Reply from 192.168.0.125…), la configuración se habrá realizado correctamente y podrá apagar la cámara.
6. Introduzca http://(Dirección IP) en la barra de direcciones del navegador para iniciar sesión.</td></tr>
<tr><td>NIC</td><td>Seleccione la tarjeta Ethernet que se debe configurar y la predeterminada es Con cable (Wired).</td></tr>
</table>

Parámetro	Descripción
Modo	El modo en que la cámara obtiene la IP: ● **Estática** Configure la **dirección IP** (IP Address), la **máscara de subred** (Subnet Mask) y la **puerta de enlace predeterminada** (Default Gateway) manualmente y, a continuación, haga clic en **Guardar** (Save); aparecerá la interfaz de inicio de sesión con la dirección IP configurada. ● **DHCP** Cuando haya un servidor DHCP en la red, seleccione **DHCP** y la cámara obtendrá la dirección IP automáticamente.
Dirección MAC	Muestra la dirección MAC del host.
Versión IP	Seleccione **IPv4** o **IPv6**.
Dirección IP	Cuando seleccione **Estática** (Static) en **Modo** (Mode), ingrese la dirección IP y la máscara de subred que necesita. ● IPv6 no tiene máscara de subred. ● La puerta de enlace predeterminada debe estar en el mismo segmento de red que la dirección IP.
Máscara de subred	
Portal de acceso predeterminado	
DNS preferido	Dirección IP del DNS preferido
DNS alternativo	Dirección IP del DNS alternativo

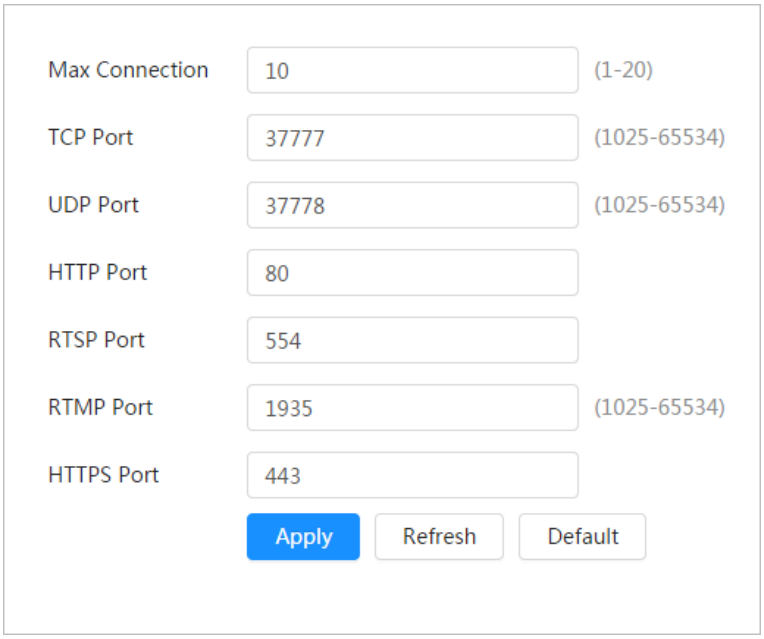
Paso 3: Haga clic sobre **Aplicar** (Apply).

5.1.2Puerto

Configure los números de puerto y el número máximo de usuarios (incluye web, cliente de plataforma y cliente de teléfono móvil) que pueden conectarse al dispositivo simultáneamente.

Paso 1: Seleccione > **Red** (Network) > **TCP/IP** (TCP/IP).

Figura 5:2 puerto



Paso 2: Configure los parámetros del puerto.

- 0–1024, 1900, 3800, 5000, 5050, 9999, 37776, 37780–37880, 39999, 42323 están ocupados para usos específicos.
- No utilice el mismo valor de ningún otro puerto durante la configuración del puerto.

Tabla 5:2 descripción de los parámetros del puerto

Parámetro	Descripción
Conexiones máximas	El número máximo de usuarios (cliente web, cliente de plataforma o cliente de teléfono móvil) que pueden conectarse al dispositivo simultáneamente. El valor predeterminado es 10.
Puerto TCP	Puerto de protocolo de control de transmisión. El valor predeterminado es 37777.
Puerto UDP	Puerto de protocolo de datagramas de usuario. El valor predeterminado es 37778.
Puerto HTTP	Puerto de protocolo de transferencia de hipertexto. El valor predeterminado es 80.

Parámetro	Descripción
Puerto RTSP	● Puerto de protocolo de transmisión en tiempo real, y el valor predeterminado es 554. Si reproduce el visionado en directo con QuickTime, VLC o un teléfono inteligente Blackberry, el siguiente formato de URL está disponible. ● Cuando el formato de URL requiere RTSP, debe especificar el número de canal y el tipo de transmisión de bits en la URL, y también el nombre de usuario y la contraseña si es necesario. Ejemplo de formato de URL: rtsp://username:password@ip:port/cam/realmonitor?channel=1&subtype=0 Entre eso: ● Nombreusuario: El nombre de usuario, que sería admin. ● Contraseña: La contraseña, que sería admin. ● IP: La IP del dispositivo, que sería 192.168.1.112. ● Puerto: Déjelo si el valor es el valor 554 predeterminado. ● Canal: El número de canal, que comienza en 1. Por ejemplo, si está utilizando el canal 2, entonces el canal = 2. ● Subtipo: El tipo de transmisión de bits; 0 significa transmisión principal (subtipo = 0) y 1 significa transmisión secundaria (subtipo = 1). Ejemplo: Si necesita la transmisión secundaria del canal 2 desde un dispositivo determinado, la URL debe ser: rtsp://admin:admin@10.12.4.84:554/cam/realmonitor?channel=21&=1 Si el nombre de usuario y la contraseña no son necesarios, la URL puede ser: rtsp://ip:port/cam/realmonitor?channel=11&=0
Puerto RTMP	Protocolo de mensajería en tiempo real. El puerto que RTMP proporciona servicio. Es 1935 por defecto.
Puerto HTTPS	Puerto de comunicación HTTPS. Es 443 por defecto.

Paso 3: Haga clic sobre **Aplicar** (Apply).

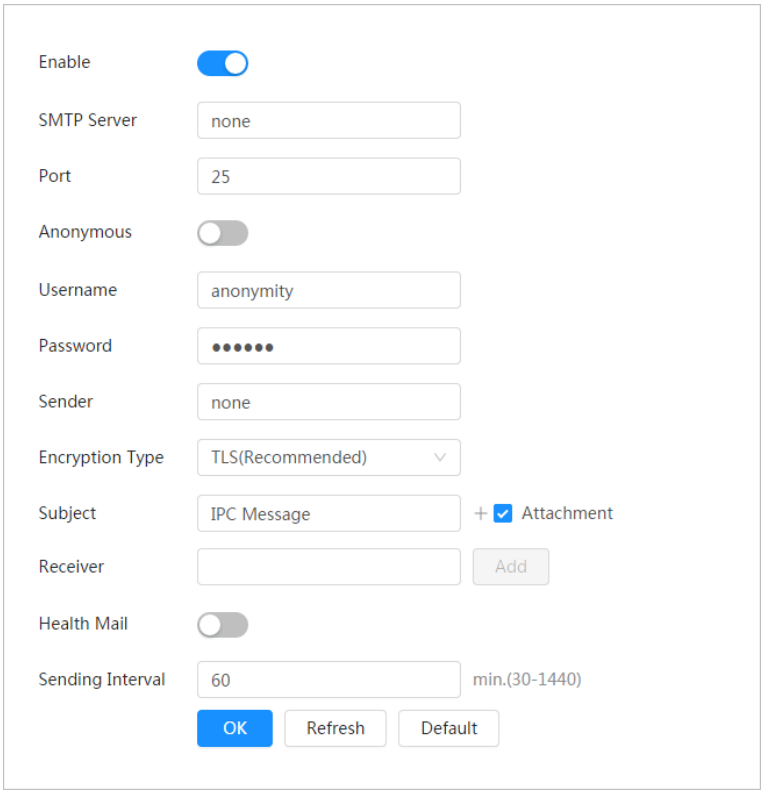
La configuración de **Conexiones Máx.** (Max Connection) entra en vigor de inmediato, y las otras entrarán en vigor después del reinicio.

5.1.3Correo electrónico

Configure el parámetro de correo electrónico y habilite la vinculación de correo electrónico. El sistema envía un correo electrónico a la dirección definida cuando se activa la alarma correspondiente.

Paso 1: Seleccione > **Red** (Netwok) > **Correo electrónico** (Email).

Figura 5:3 correo electrónico



Paso 2: Haga clic en para habilitar la función.

Paso 3: Configure los parámetros del correo electrónico

Tabla 5:3 descripción de los parámetros del correo electrónico

Parámetro	Descripción	
Servidor SMTP	Dirección del servidor SMTP	Para ver los detalles, consulte Tabla 5:4.
Puerto	El número de puerto del servidor SMTP.	
NombreUsuario	La cuenta del servidor SMTP.	
Contraseña	La contraseña del servidor SMTP.	
Anónimo	Haga clic en y la información del remitente no se mostrará en el correo electrónico.	
Remitente	Dirección de correo electrónico del remitente.	
Tipo de cifrado	Seleccione entre **Ninguno** (None) **SSL** y **TLS**. Para ver los detalles, consulte Tabla 5:4.	
Título	Ingrese un máximo de 63 caracteres en chino, inglés y números arábigos. Haga clic en para seleccionar el tipo de título, incluido **el nombre del dispositivo** (Device Name), la **identificación del dispositivo** (Device ID) y el **tipo de evento** (Event Type); puede establecer un máximo de 2 títulos.	
Datos adjuntos	Marque la casilla de verificación para poder adjuntar archivos en el correo electrónico.	

Parámetro	Descripción
Destinatario	• Dirección de correo electrónico del receptor. Admite 3 direcciones como máximo. • Después de ingresar la dirección de correo electrónico del destinatario, aparecerá el botón **Probar** (Test). Haga clic en **Probar** (Test) para probar si los correos electrónicos se pueden enviar y recibir correctamente.
Correo de comprobación	El sistema envía un correo de prueba para comprobar que la conexión se haya configurado correctamente. Haga clic en y configure el **Intervalo de envío** (Sending Interval), y seguidamente el sistema enviará el correo de prueba en el intervalo establecido.

Para la configuración de los principales buzones de correo, consulte. Tabla 5:4.

Tabla 5:4 descripción de la configuración del Buzón

Buzón	Servidor SMTP	Autenticación	Puerto	Descripción
gmail	smtp.gmail.com	SSL	465	• Es necesario que tenga activado el servicio SMTP en su buzón de correos. • Es necesario el código de autenticación. La contraseña del correo electrónico no es de aplicación. Código de autenticación: El código que recibe al habilitar el servicio SMTP.
		TLS	587	

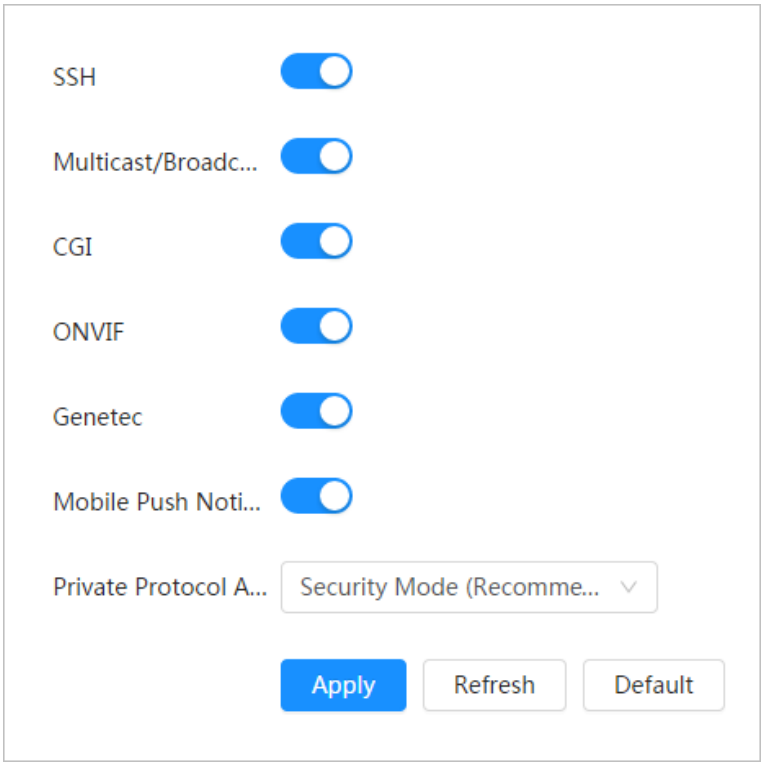
Paso 4: Haga clic sobre **Aplicar** (Apply).

5.1.4Servicio básico

Configure los servicios básicos para mejorar la seguridad de la red y los datos.

Paso 1: Seleccione > **Red** (Network) > **Servicio básico** (Basic Service).

Figura 5:4 servicio básico



Paso 2: Habilite el servicio básico según las necesidades reales.

Tabla 5:5 descripción de los parámetros básicos del servicio

Función	Descripción
SSH	Puede habilitar la autenticación SSH para administrar la seguridad.
Búsqueda multidifusión/transmisión	Habilite esta función y, a continuación, cuando varios usuarios estén viendo la imagen de vídeo del dispositivo simultáneamente a través de la red, pueden encontrar su dispositivo con el protocolo de multidifusión/transmisión.
CGI	Habilite la función y, a continuación, otros dispositivos podrán acceder a través de este servicio. La función está activada por defecto.
Onvif	
Genetec	
*******Notificaciones automáticas del móvil*******	Habilite esta función y, a continuación, el sistema enviará la instantánea que se tomó cuando se activó la alarma a su teléfono, esto está habilitado de manera predeterminada.
Modo de autenticación del protocolo privada	Seleccione el modo de autenticación entre **Modo de seguridad** (Security Mode)y **Modo compatible** (Compatible Mode). Se recomienda el modo de seguridad.

Paso 3: Haga clic sobre **Aplicar** (Apply).

5.2 Evento

Esta sección toma la entrada de alarmas, por ejemplo, para presentar la configuración de la vinculación de alarmas.

Figura 5:5 configuración de eventos de alarma

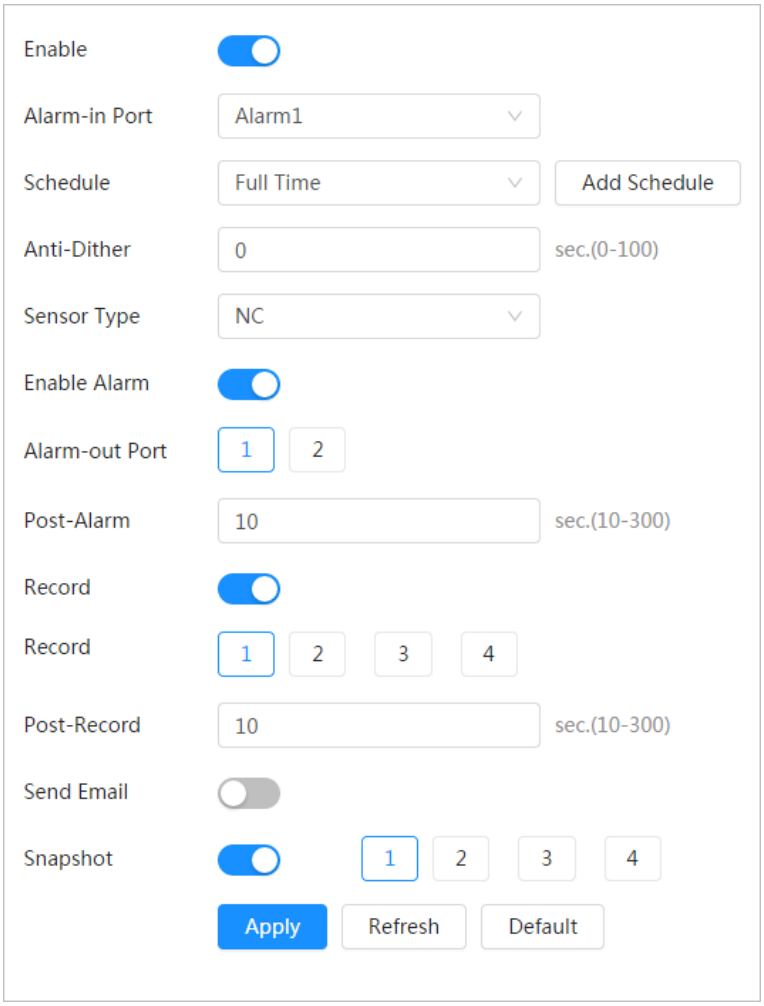
5.2.1Configuración de entrada de alarma

Cuando el dispositivo conectado al puerto de entrada de alarma activa una alarma, el sistema realiza la vinculación de la alarma establecida.

Paso 1: Seleccione > **Evento** (Event) > **Alarma** (Alarm).

Paso 2: Haga clic en junto a **Habilitar** (Enable) para habilitar la vinculación de alarmas.

Figura 5–6 Vinculación de alarma



Paso 3: Seleccione un puerto de entrada de alarma y un tipo de sensor.

- Tipo de sensor: NO o NC.
- Antifluctuación: Únicamente registre un evento de alarma durante el período de anti-interpolado.

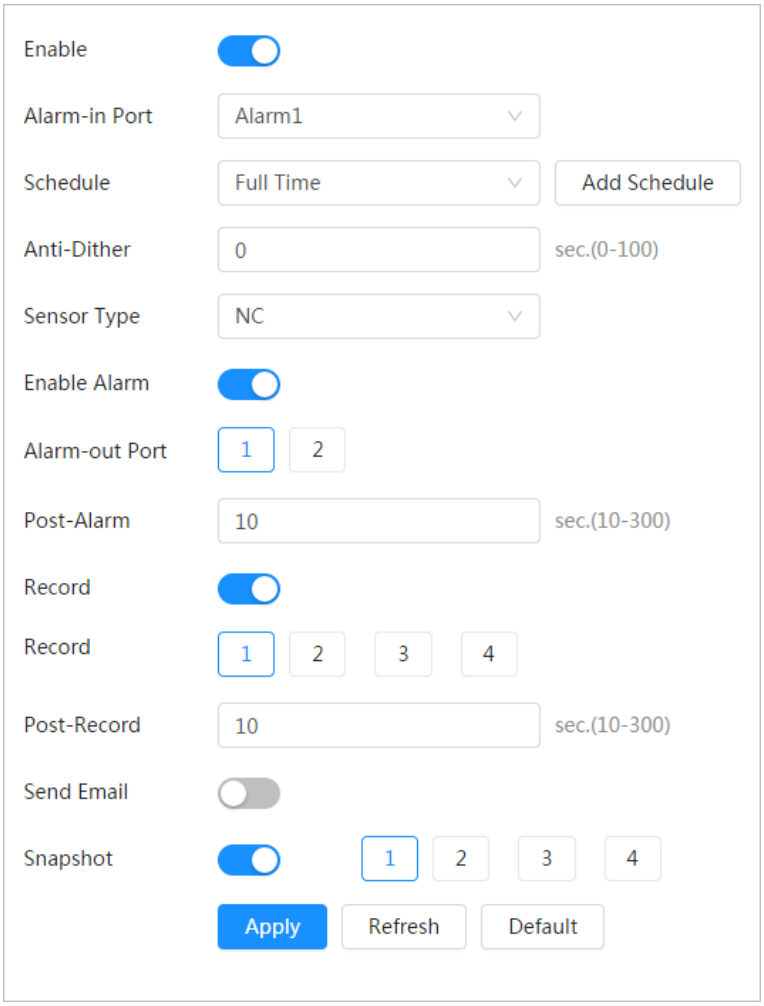
Paso 4: Seleccione la programación y los períodos de armado y la acción de vinculación de alarma. Para conocer los detalles, consulte "5.2.2 Establecer vinculación de alarma."
Si las programaciones existentes no pueden cumplir con el requisito de la escena, puede hacer clic en **Añadir programación** (Add Schedule) para agregar una nueva programación. Para conocer los detalles, consulte "5.2.2.1 Añadir programación."
Paso 5: Haga clic sobre **Aplicar** (Apply).

5.2.2Establecer vinculación de alarma

Al configurar eventos de alarma, seleccione vínculos de alarma (como registro, instantánea). Cuando se activa la alarma correspondiente en el período de armado configurado, el sistema emitirá una alarma.

Seleccione > **Evento** (Event)> **Alarma** (Alarm), junto a **Habilitar** (Enable) para habilitar la vinculación de alarmas.

Figura 5–7 Vinculación de alarma

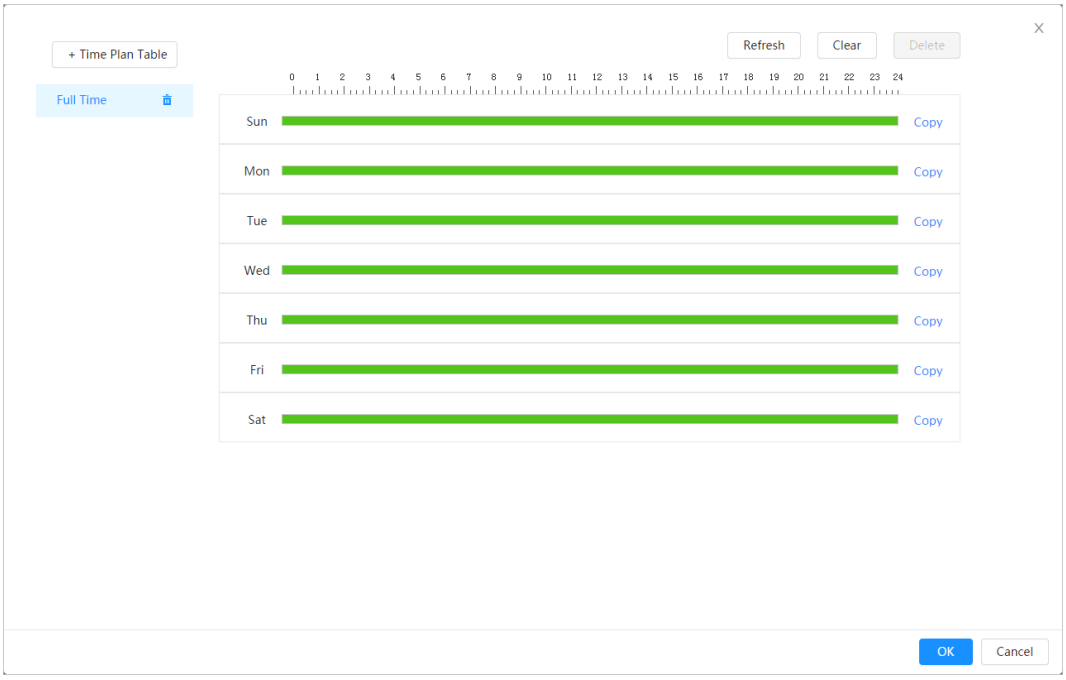


5.2.2.1Añadir programación

Establecer períodos de armado. El sistema solo realiza la acción de vinculación correspondiente en el período configurado.

Paso 1: Haga clic en **Agregar programación** (Add Schedule) junto a **Programación** (Schedule).

Figura 5:8 programación



Paso 2: Presione y arrastre el botón izquierdo del ratón sobre la línea de tiempo para establecer períodos de armado. Las alarmas se activarán en el período de tiempo en verde en la línea de tiempo.

- Haga clic en **Copiar** (Copy) junto a un día y seleccione los días en los que desea copiar en la interfaz de solicitud; puede copiar la configuración a los días seleccionados. Seleccione la casilla de verificación **Seleccionar todo** (Select All) para seleccionar todos los días para copiar la configuración.
- Puede establecer 6 períodos de tiempo por día.

Paso 3: Haga clic sobre **Aplicar** (Apply).

Paso 4: (Opcional) Haga clic en **Tabla de plan de tiempo** (Time Plan Table) para añadir una nueva tabla de plan de tiempo.

Puede:

- Haga doble clic en el nombre de la tabla para editarlo.
- Haga clic en para eliminar el historial según sea necesario.

5.2.2.2Vinculación de grabación

El sistema puede vincular el canal de grabación cuando ocurre un evento de alarma. Después de la alarma, el sistema deja de grabar después de un período de tiempo prolongado de acuerdo con el ajuste **Posgrabación** (Post-Record).

Requisitos previos

- Una vez habilitado el tipo de alarma correspondiente (**Normal**, **Movimiento** (Motion) o **Alarma** (Alarm)), el canal de grabación vincula la grabación.
- Habilite el modo de grabación automática, se aplicará la vinculación de grabación.

Establecer vinculación de grabación

En la interfaz de **Alarma** (Alarm), haga clic para habilitar la vinculación de grabación, seleccione el canal según sea necesario y configure **Posgrabación** (Post-Record) para

configurar la vinculación de alarma y el retraso de grabación.
Una vez configurada la **Posgrabación** (Post-Record), la grabación de alarma continúa durante un período prolongado después de que finalice la alarma.

Figura 5:9 vínculo de grabación

5.2.2.3Vinculación de instantáneas

Una vez configurada la vinculación de instantáneas, el sistema puede activar la alarma y hacer fotografías automáticamente cuando se active una alarma.

Requisitos previos

Una vez habilitado el tipo de alarma correspondiente (**Normal**, **Movimiento** (Motion) o **Alarma** (Alarm)) , el canal de la instantánea vincula la captura de la imagen.

Establecer vinculación de grabación

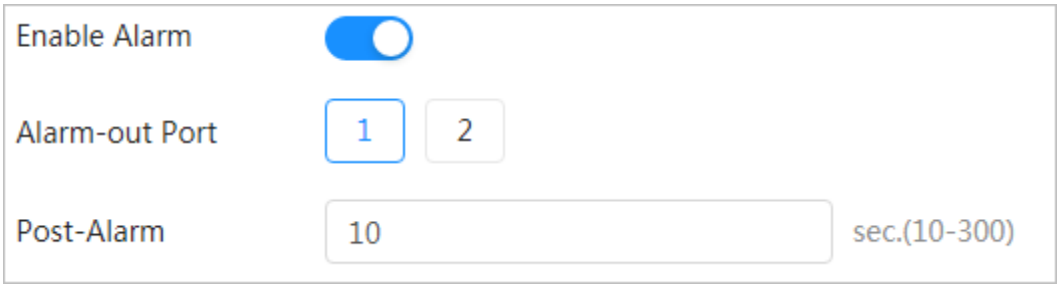
En la interfaz de **Alarma** (Alarm), haga clic en para habilitar la vinculación de instantáneas y seleccione el canal según sea necesario.

Figura 5:10 vínculo de instantáneas

5.2.2.4Vinculación de salida de alarma

Cuando se activa una alarma, el sistema puede vincularse automáticamente con el dispositivo de salida de alarma.
En la interfaz de **Alarma** (Alarm), haga clic en para habilitar la vinculación de salida de alarma, seleccione el canal según sea necesario y, a continuación, configure **Post alarma** (Post alarm).
Cuando se configura el retraso de la alarma, la alarma continúa durante un período prolongado después de que finalice la alarma.

Figura 5:11 vínculo de salida de alarma



5.2.2.5Vinculación de correo electrónico

Cuando se activa una alarma, el sistema enviará automáticamente un correo electrónico a los usuarios.

La vinculación de correo electrónico tiene efecto únicamente cuando se configura SMTP. Para conocer los detalles, consulte "5.1.3 Correo electrónico."

Figura 5:12 vínculo de correo electrónico

5.3 Sistema

Esta sección presenta las configuraciones del sistema, incluidos general, fecha y hora, cuenta, seguridad, configuración PTZ, predeterminado, importación/exportación, remoto, mantenimiento automático y actualización.

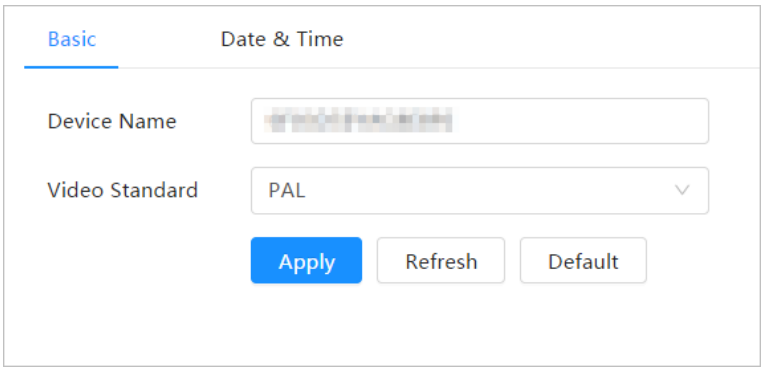
5.3.1General

5.3.1.1Básico

Puede configurar el nombre del dispositivo, el idioma y el estándar de vídeo.

Paso 1: Seleccione > **Sistema** (System) > **General** (General) > **Básico** (Basic).

Figura 5:13 básico



Paso 2: Configure los parámetros generales

Tabla 5:6 descripción de los parámetros generales

Parámetro	Descripción
Nombre	Introduzca el nombre de dispositivo
Estándar de vídeo	Seleccione el estándar de vídeo entre **PAL** y **NTSC**.

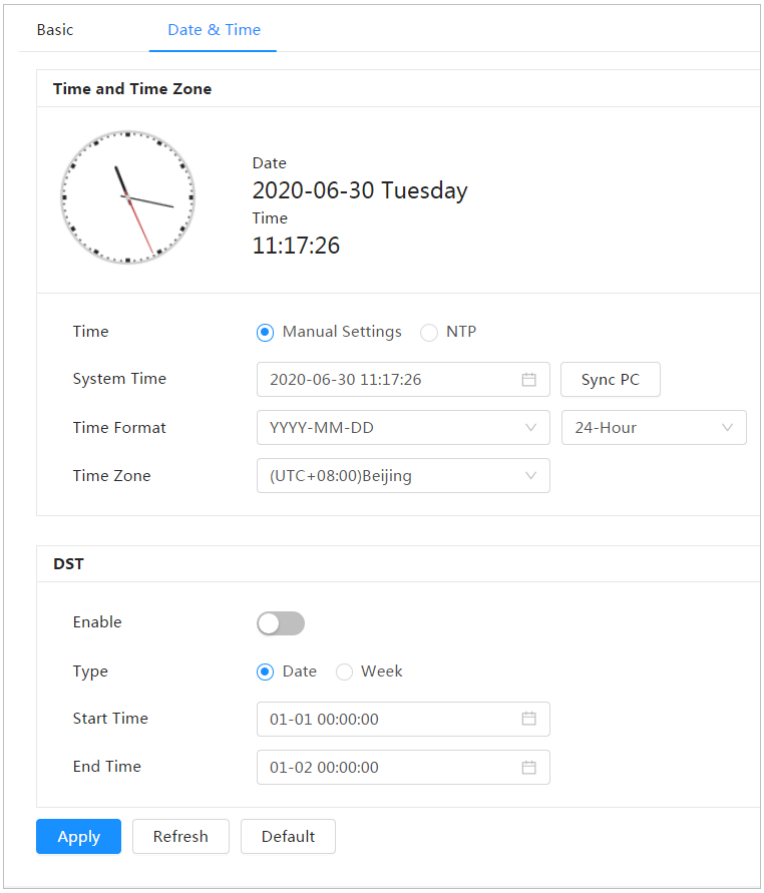
Paso 3: Haga clic sobre **Aplicar** (Apply).

5.3.1.2Fecha y hora

Puede configurar el formato de fecha y hora, zona horaria, hora actual, DST (horario de verano) o servidor NTP.

Paso 1: Seleccione > **Sistema** (System) > **General** (General) > **Básico** > **Fecha y Hora** (Date & Time).

Figura 5:14 fecha y hora



Paso 2: Configure los parámetros de fecha y hora.

Tabla 5:7 descripción de los parámetros de fecha y hora

Parámetro	Descripción
Formato de la fecha	Configure el formato de la fecha.

Parámetro	Descripción
Hora	● **Configuración manual:** configure los parámetros de forma manual. ● **NTP:** Al seleccionar NTP, el sistema sincroniza la hora con el servidor de Internet en tiempo real. También puede ingresar la dirección IP, la zona horaria, el puerto y el intervalo de un PC con servidor NTP para usar NTP.
Formato de la hora	Configure el formato de la hora. Puede seleccionar entre **12 horas** (12-Hour) o **24 horas** (24-Hour).
Zona horaria	Configure la zona horaria en la que se encuentra la cámara.
Hora actual	Configure la hora del sistema. Haga clic en **Sincronizar PC** (Sync PC) y el sistema adoptará la hora del PC.
DST	Habilite DST según sea necesario. Haga clic en , y configure la hora de inicio y finalización del horario de verano con **Fecha** o **Semana** (Date o Week).

Paso 3: Haga clic sobre **Aplicar** (Apply).

5.3.2Cuenta

Puede administrar usuarios, como añadirlos, eliminarlos o editarlos. Los usuarios incluyen administradores, usuarios añadidos y usuarios de ONVIF.

La gestión de usuarios y grupos solo está disponible para usuarios administradores.

- La longitud máxima del nombre de usuario o grupo es de 31 caracteres, que consta de número, letra, subrayado, guión, punto y @.
- La contraseña debe constar de 8 a 32 caracteres no vacíos y contener al menos dos tipos de caracteres entre mayúsculas, minúsculas, números y caracteres especiales (excluyendo ‘ " ; : &).
- Puede tener 18 usuarios y 8 grupos como máximo.
- Puede administrar usuarios a través de un solo usuario o grupo y no se permiten nombres de usuario o nombres de grupo duplicados. Un usuario solo puede estar en un grupo, y los usuarios del grupo pueden tener permisos dentro del rango de autoridad del grupo.
- Los usuarios en línea no pueden editar su propio permiso.
- Hay un administrador por defecto que tiene la autorización máxima.
- Seleccione **Inicio de sesión anónimo** (Anonymous Login) y, a continuación inicie sesión solo con la dirección IP en lugar del nombre de usuario y la contraseña. Los usuarios anónimos solo tienen autorización de vista previa. Durante el inicio de sesión anónimo, haga clic en **Cerrar sesión** (Logout) y luego podrá iniciar sesión con otro nombre de usuario.

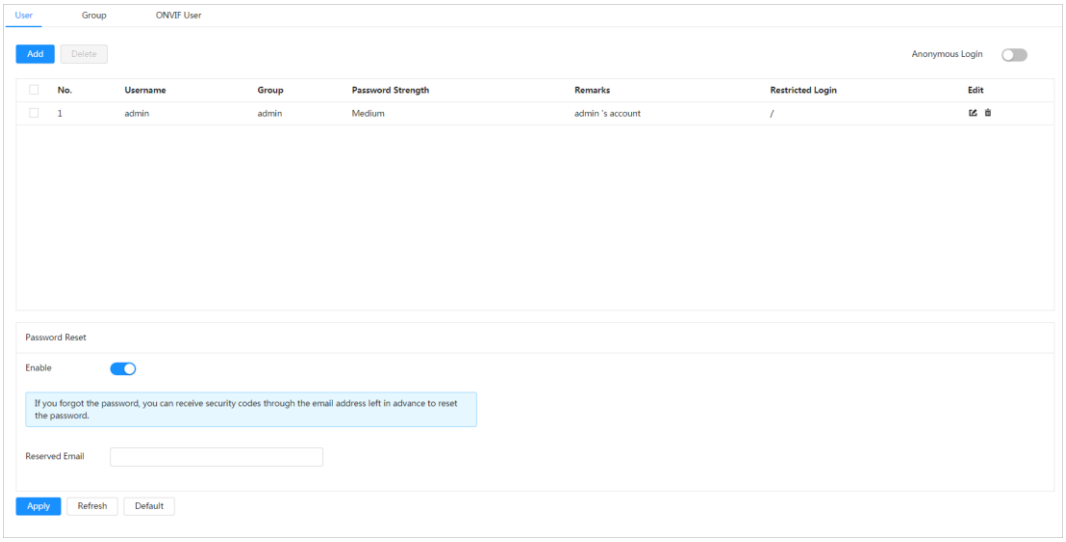
5.3.2.1Usuario

5.3.2.1.1 Añadir usuarios

Eres un usuario administrador por defecto. Puede añadir usuarios y configurar diferentes permisos.

Paso 1: Seleccione > **Sistema** (System) > **Cuenta** > (Account) **Usuario** (User).

Figura 5:15 usuario



Paso 2: Haga clic sobre **Agregar** (Add).

Figura 5:16 añadir usuario (sistema)

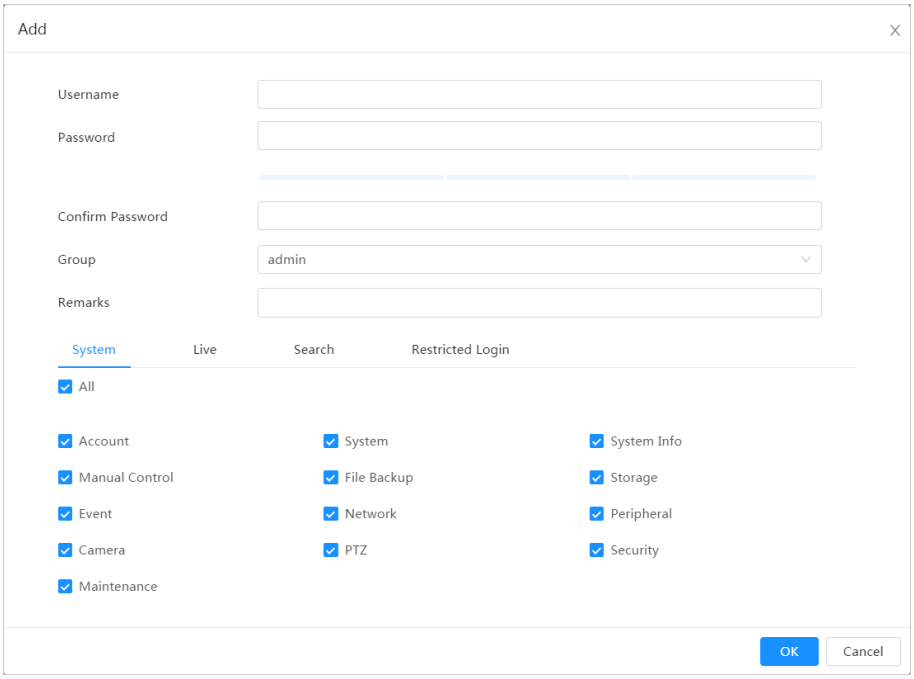
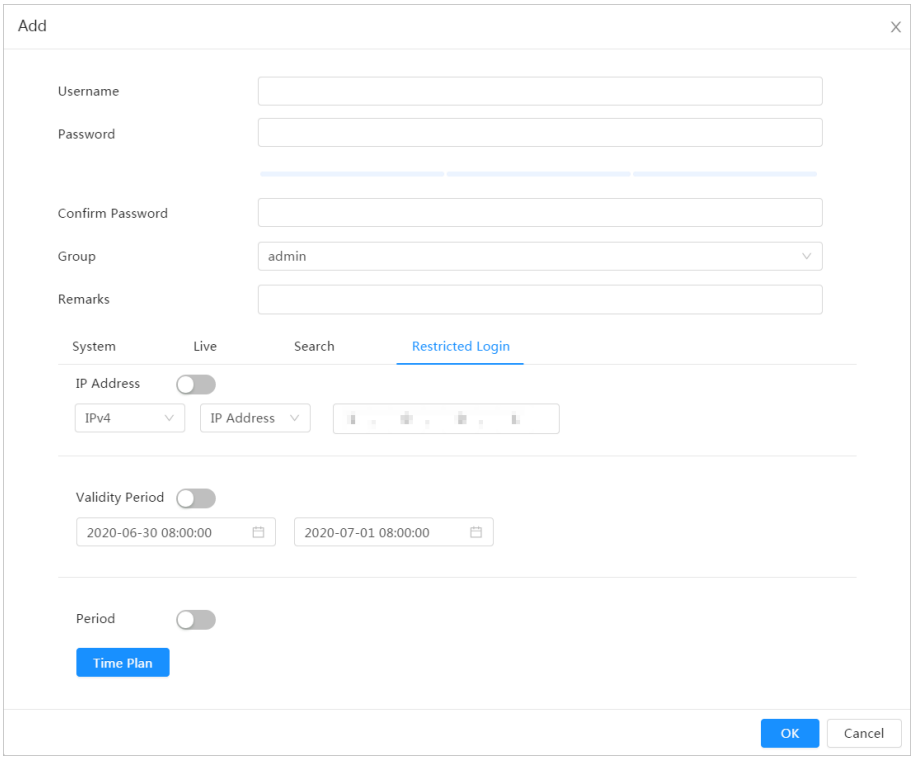


Figura 5:17 añadir usuario (inicio de sesión restringido)



Paso 3: Configure los parámetros del usuario

Tabla 5:8 descripción de los parámetros del usuario (1)

Parámetro	Descripción
NombreUsuario	Identificación única del usuario. No puede utilizar el nombre de usuario existente.
Contraseña	Ingrese la contraseña y confírmela nuevamente.

Parámetro	Descripción
Confirmar contraseña	La contraseña debe constar de 8 a 32 caracteres no vacíos y contener al menos dos tipos de caracteres entre mayúsculas, minúsculas, números y caracteres especiales (excluyendo ‘ " ; : &).
Grupo	El grupo al que pertenecen los usuarios. Cada grupo tiene diferentes permisos.
Observación	Describa al usuario.
Sistema	Seleccione permisos según sea necesario. Se recomienda otorgar menos permisos a los usuarios normales que a los usuarios premium.
Directo	Seleccione el permiso de visualizado en directo al usuario que se va a añadir.
Buscar	Seleccione el permiso de búsqueda al usuario que se va a añadir.
Inicio de sesión restringido	Configure la dirección del PC que permite al establecido iniciar sesión en la cámara y el período de validez y el rango de tiempo. Puede iniciar sesión en la interfaz web con la IP establecida en el rango de tiempo establecido como período de validez. ● Dirección IP: puede iniciar sesión en la web a través del PC con la IP establecida. ● Período de validez: puede iniciar sesión en la web en el período de validez establecido. ● Rango de tiempo: puede iniciar sesión en la web en el intervalo de tiempo establecido. Establecer de la siguiente manera 1. Dirección IP: ingrese la dirección IP del host que se va a añadir. 2. Segmento IP: ingrese la dirección de inicio y la dirección final del host que se va a añadir.

Paso 4: Haga clic sobre **Aplicar** (Apply).

El usuario recién añadido aparece en la lista de nombres de usuario.

Operaciones relacionadas

- Haga clic en para editar la contraseña, el grupo, la nota o los permisos.

  Para la cuenta de administrador, solo puede editar la contraseña.

- Haga clic en para eliminar los usuarios añadidos. El usuario administrador no se puede eliminar.

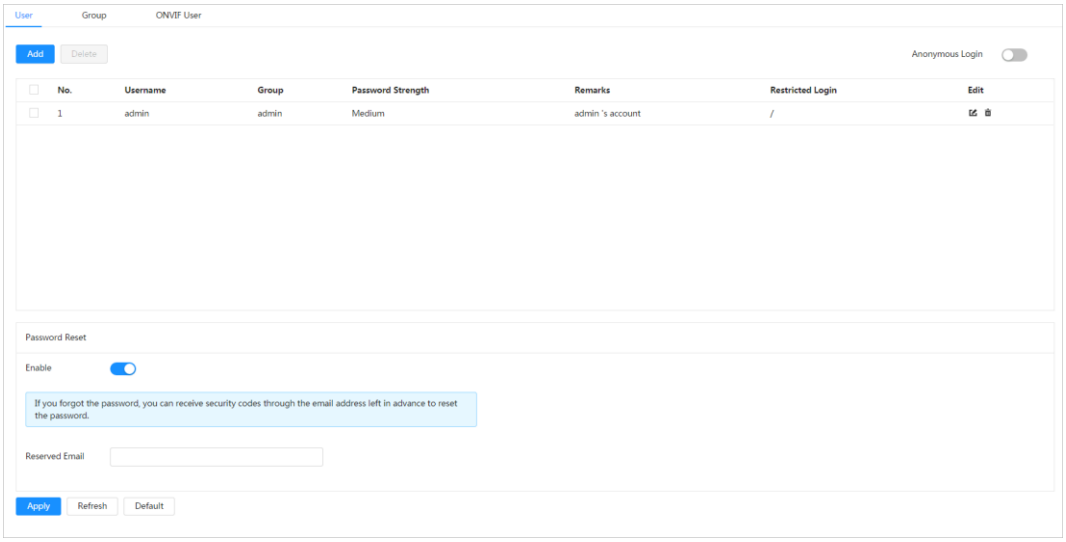
  La cuenta de administrador no se puede eliminar.

5.3.2.1.2 Restablecer la contraseña

Habilite la función y podrá restablecer la contraseña haciendo clic en **¿Olvidó la contraseña?** (Forget password?) en la interfaz de inicio de sesión. Para conocer los detalles, consulte "3.2 Restablecer la contraseña."

Paso 1: Seleccione > **Sistema** (System) > **Cuenta** > (Account) **Usuario** (User).

Figura 5:18 usuario



Paso 2: Haga clic en junto a **Habilitar** (Enable) en **Restablecer contraseña** (Password Reset).

Si la función no está habilitada, solo podrá restablecer la contraseña restableciendo la cámara.

Paso 3: Introduzca la dirección de correo electrónico reservada.

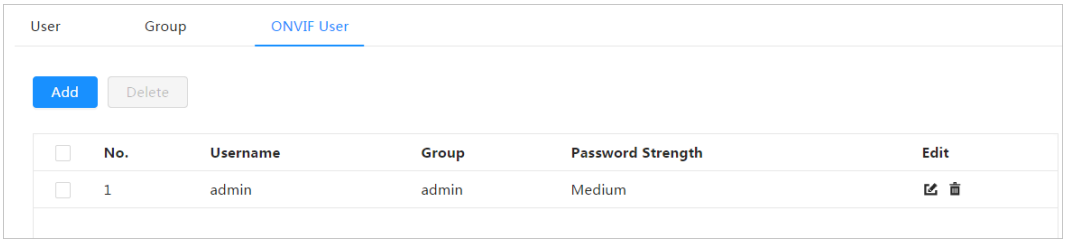
Paso 4: Haga clic sobre **Aplicar** (Apply).

5.3.2.2Usuario ONVIF

Puede añadir, eliminar usuarios de ONVIF y cambiar sus contraseñas.

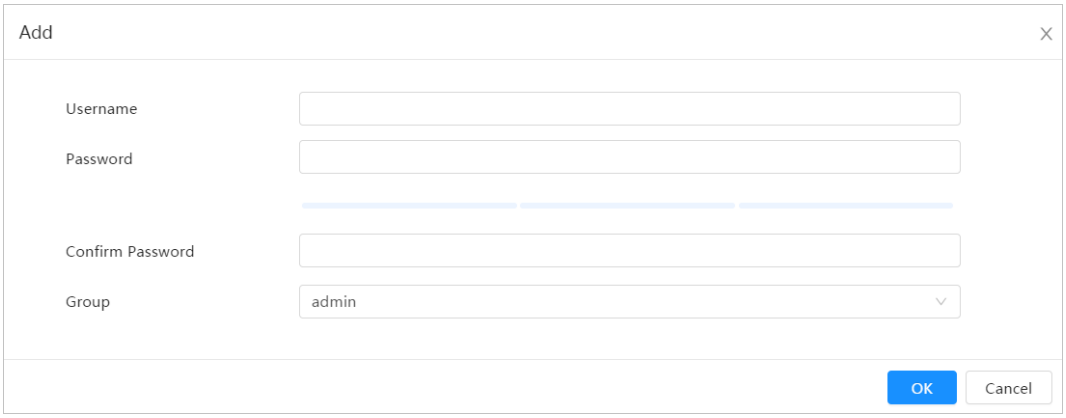
Paso 1: Seleccione > **Sistema** (System) > **Cuenta** (Account) > **Usuario de ONVIF** (ONVIF User).

Figura 5–19 Usuario ONVIF



Paso 2: Haga clic sobre **Agregar** (Add).

Figura 5:20 añadir usuario de ONVIF



Paso 3: Configure los parámetros del usuario

Tabla 5:9 descripción de los parámetros del usuario de ONVIF

Parámetro	Descripción
NombreUsuario	Identificación única del usuario. No puede utilizar el nombre de usuario existente.
Contraseña	Ingrese la contraseña y confírmela nuevamente. La contraseña debe constar de 8 a 32 caracteres no vacíos y contener al menos dos tipos de caracteres entre mayúsculas, minúsculas, números y caracteres especiales (excluyendo ' " ; : &).
Confirmar contraseña	
Nombre del grupo	El grupo al que pertenecen los usuarios. Cada grupo tiene diferentes permisos.

Paso 4: Haga clic sobre **Aceptar** (OK).

El usuario recién añadido aparece en la lista de nombres de usuario.

Operaciones relacionadas

- Haga clic en para editar la contraseña, el grupo, la nota o los permisos.

  Para la cuenta de administrador, solo puede cambiar la contraseña.
- Haga clic en para eliminar los usuarios añadidos. El usuario administrador no se puede eliminar.

  La cuenta de administrador no se puede eliminar.

5.3.3Gerentes

5.3.3.1Requisitos

Para asegurarse de que el sistema funcione correctamente, realice las siguientes acciones:

- Verifique las imágenes de vigilancia con regularidad.
- Borre con regularidad la información de usuarios y grupos de usuarios que no se utilizan con frecuencia.
- Cambie la contraseña cada tres meses. Para conocer los detalles, consulte "5.3.2 Cuenta."

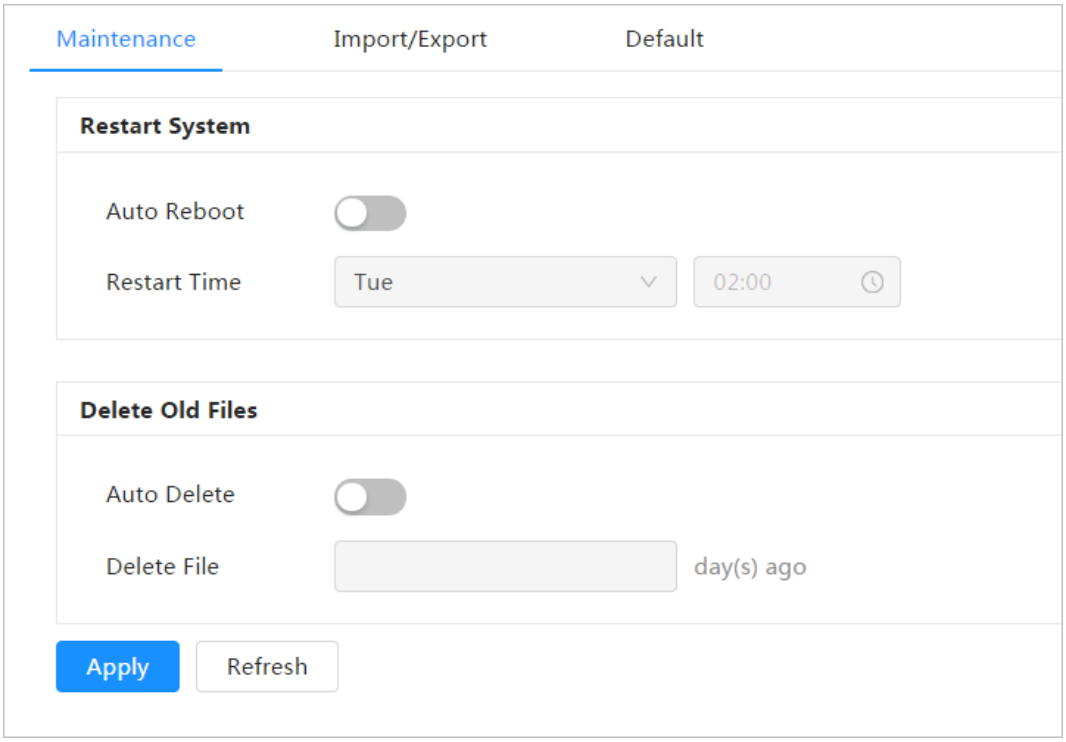
- Vea los registros del sistema y analícelos, y soluciones los errores de forma oportuna.
- Realice una copia de seguridad de la configuración del sistema con regularidad.
- Reinicie el dispositivo y elimine los archivos antiguos con regularidad.
- Actualice el firmware correspondientemente.

5.3.3.2Mantenimiento

Puede reiniciar el sistema manualmente y establecer la hora del reinicio automático,a demás de la eliminación automática de archivos antiguos. Esta función está desactivada por defecto.

Paso 1: Seleccione > **Sistema** (System) > **Cuenta** (Account) > **Mantenimiento**(Maintenance).

Figura 5:21 mantenimiento



Paso 2: Configure los parámetros para el mantenimiento automático.

- Haga clic en junto a **Reinicio automático** (Auto Reboot) en **Reiniciar sistema** (Restart System) y configure la hora de reinicio; el sistema se reinicia automáticamente como la hora establecida cada semana.
- Haga clic en junto a **Eliminar automáticamente** (Auto Delete) en **Eliminar archivos antiguos** (Delete Old Files) y configure la hora; el sistema elimina automáticamente los archivos antiguos según la hora establecida. El intervalo de tiempo es de 1 a 31 días.

Cuando habilita y confirma la función de **Eliminar automáticamente** (Auto Delete), los archivos eliminados no se pueden restaurar. Realice el procedimiento con cuidado.

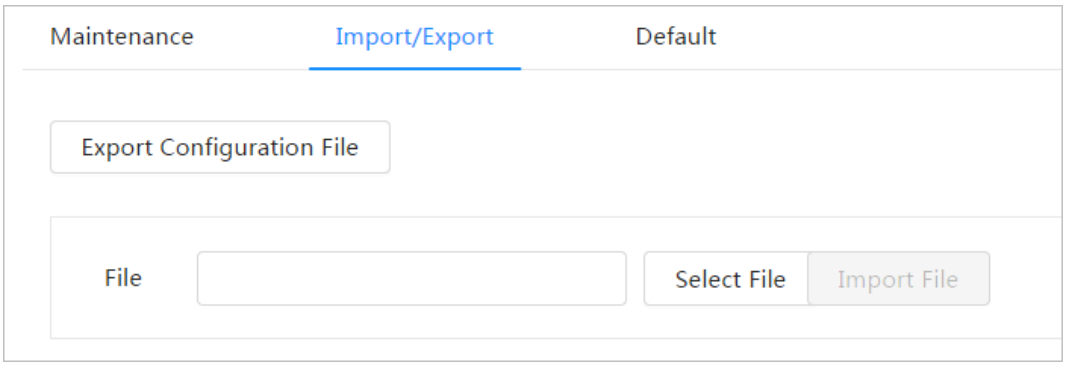
Paso 3: Haga clic sobre **Aplicar** (Apply).

5.3.3.3Importar/Exportar

- Exporte el archivo de configuración del sistema para realizar una copia de seguridad de la configuración del sistema.
- Importe el archivo de configuración del sistema para realizar una configuración rápida o recuperar la configuración del sistema.

Paso 1: Seleccione > **Sistema** (System)> **Cuenta** (Account) > **Importar/Exporta**(Import/Export).

Figura 5–22 Importar/Exportar



Paso 2: Importar y exportar.

- Importar: seleccione el archivo de configuración local y haga clic en **Importar archivo** (Import File) para importar el archivo de configuración del sistema local al sistema.
- Exportación: haga clic en **Exportar archivo de configuración** (Export Configuration File) para exportar el archivo de configuración del sistema al almacenamiento local.

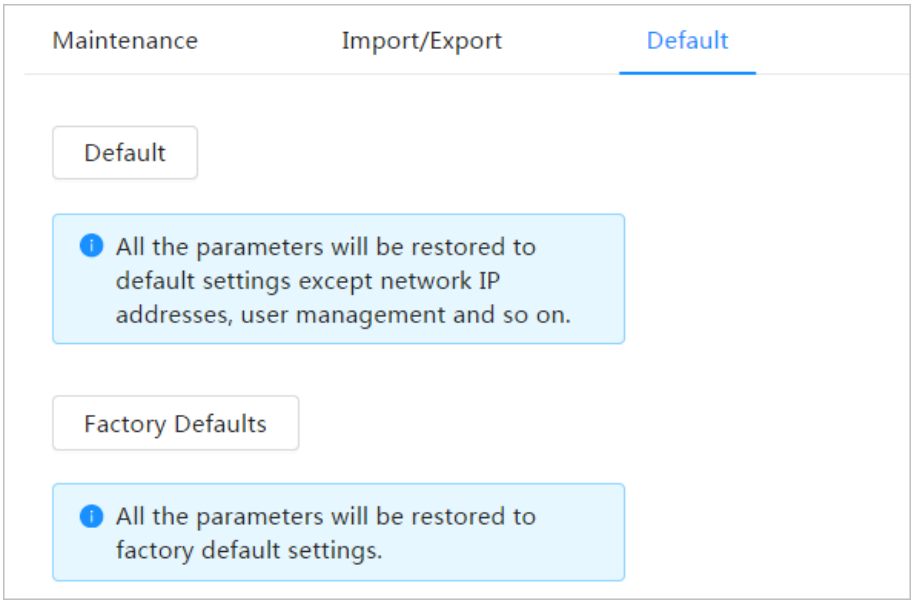
5.3.3.4Predeterminado

Restaure el dispositivo a la configuración predeterminada o la configuración de fábrica.
Esta función restaurará el dispositivo a la configuración predeterminada o la configuración de fábrica.

Seleccione > **Sistema** (System) > **Cuenta** > (Account) **Predeterminado** (Defautl).

- Haga clic en **Predeterminado** (Default) y, a continuación, todas las configuraciones, excepto la dirección IP y la cuenta, se restablecerán a los valores predeterminados.
- Haga clic en **Valores predeterminados de fábrica** (Factory Default) y todas las configuraciones se restablecerán a los valores de fábrica.

Figura 5:23 predeterminado



5.3.4Actualización

La actualización a la última versión puede mejorar las funciones de la cámara y la estabilidad. Si se ha utilizado un archivo de actualización incorrecto, reinicie el dispositivo; de lo contrario, es posible que algunas funciones no funcionen correctamente.

Paso 1: Seleccione > **Sistema** (System) > **Actualizar** (Upgrade).

Figura :24 actualización

Paso 2: Haga clic en **Examinar** (Browse) y, a continuación, suba el archivo de actualización. El archivo de actualización debe ser un archivo .bin.

Paso 3: Haga clic en **Actualizar** (Upgrade).

La actualización comenzará a ejecutarse.

Apéndice 1 Recomendaciones de ciberseguridad

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

Medidas obligatorias que debe tomar para la seguridad de la red del equipo básico:

1. **Usar contraseñas seguras**

   Consulte las siguientes sugerencias para establecer contraseñas:

   - La longitud no puede ser inferior a 8 caracteres;
   - Incluya al menos dos tipos de caracteres: letras mayúsculas y minúsculas, números y símbolos;
   - No utilice el nombre de la cuenta o el nombre de la cuenta al revés.
   - No utilice caracteres continuos, como 123, abc, etc.;
   - No utilice caracteres repetidos continuos, como 111, aaa, etc.;

2. **Actualizar el firmware y el software cliente puntualmente**

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

Medidas recomendadas para mejorar la seguridad de la red de su equipo:

1. **Protección física**

   Le sugerimos que proteja físicamente su equipo, especialmente los dispositivos de almacenamiento. Por ejemplo, coloque el equipo en una sala y armario especiales para ordenadores e implemente un correcto permiso de control de acceso y una administración de claves para evitar que el personal no autorizado pueda acceder físicamente al equipo y dañar el hardware, conectarse sin autorización a equipos extraíbles (como un disco flash USB, un puerto serie), etc.

2. **Cambiar contraseñas periódicamente**

   Le sugerimos que cambie las contraseñas periódicamente para reducir el riesgo de que puedan adivinarse o descifrarse.

3. **Establecer y actualizar puntualmente la información de restablecimiento de contraseñas**

   El equipo admite la función de restablecimiento de contraseña. Configure la información relacionada para restablecer la contraseña puntualmente, incluyendo las preguntas de protección de contraseña y la dirección electrónica del usuario final. Si la información cambia, modifíquela inmediatamente. Al establecer las preguntas de protección de la contraseña, le sugerimos que no utilice las que se puedan adivinar fácilmente.

4. **Habilitar bloqueo de cuenta**

   La función de bloqueo de cuenta está habilitada de manera predeterminada, y le

recomendamos que la mantenga activada para garantizar la seguridad de la cuenta. Si un atacante intenta iniciar sesión con la contraseña incorrecta varias veces, la cuenta correspondiente y la dirección IP de origen se bloquearán.

5. **Cambiar HTTP y otros puertos de servicio predeterminados**
   Le sugerimos que cambie el HTTP y otros puertos de servicio predeterminados a cualquier serie de números entre 1024 y 65535, reduciendo el riesgo de que personas externas puedan adivinar qué puertos está utilizando.
6. **Habilitar HTTPS**
   Le sugerimos que habilite HTTPS para que visite el servicio web a través de un canal de comunicación seguro.
7. **Enlace de dirección MAC**
   Le recomendamos que enlace la dirección IP y MAC de la puerta de enlace al equipo, reduciendo el riesgo de redireccionamiento de ARP.
8. **Asignar cuentas y privilegios razonablemente**
   De acuerdo con los requisitos comerciales y de gestión, agregue razonablemente usuarios y asígneles un conjunto mínimo de permisos.
9. **Inhabilitar servicios innecesarios y elegir modos seguros**
   Si no son necesarios, se recomienda desactivar algunos servicios como SNMP, SMTP, UPnP, etc., para reducir los riesgos.

   Si son necesarios, se recomienda encarecidamente que utilice modos seguros, incluyendo, entre otros, los siguientes servicios:
   - SNMP: Seleccione SNMP v3 y configure contraseñas de cifrado fuertes y contraseñas de autenticación.
   - SMTP: Seleccione TLS para acceder al servidor de buzones.
   - FTP: Seleccione SFTP y configure contraseñas seguras.
   - Punto de acceso AP: Seleccione el modo de cifrado WPA2-PSK y configure contraseñas seguras.
10. **Transmisión cifrada de audio y vídeo**
    Si su contenido de datos de audio y vídeo es muy importante o sensible, le recomendamos que utilice la función de transmisión cifrada para reducir el riesgo de robo de datos de audio y vídeo durante la transmisión.

    Recuerde: la transmisión cifrada causará alguna pérdida en la eficiencia de la transmisión.
11. **Auditoría segura**
    - Comprobar usuarios en línea: le sugerimos que compruebe los usuarios en línea periódicamente para ver si alguien se ha conectado al dispositivo sin autorización.
    - Verificar registro del equipo: Al consultar los registros, puede conocer las direcciones IP que se han utilizado para iniciar sesión en sus dispositivos y sus operaciones clave.
12. **Registro de red**
    Debido a la capacidad de almacenamiento limitada del equipo, el registro almacenado es limitado. Si necesita guardar el registro durante mucho tiempo, le recomendamos que habilite la función de registro de red para asegurarse de que los registros importantes estén sincronizados con el servidor de registro de red para su seguimiento.
13. **Crear un entorno de red seguro**
    Para garantizar mejor la seguridad de los equipos y reducir los posibles riesgos cibernéticos, le recomendamos:

- Inhabilitar la función de asignación de puertos del enrutador para evitar el acceso directo a los dispositivos de la Intranet desde una red externa.
- Particionar y aislar la red según las necesidades reales de la red. Si no hay requisitos de comunicación entre dos subredes, le sugerimos que utilice VLAN, GAP de red y otras tecnologías para particionar 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 las redes privadas.
- Habilitar la función de filtrado de direcciones IP/MAC para limitar el rango de hosts permitidos para acceder al dispositivo.

AYUDANDO A CREAR UNA SOCIEDAD MÁS SEGURA Y UN MODO DE VIDA MÁS INTELIGENTE

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Dirección: No.1199 Bin'an Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Código postal: 310053
Correo electrónico: overseas@dahuatech.com | Fax: +86-571-87688815 | Tel.: +86-571-87688883