Akuvox
Open A Smart World

Videoporteros Akuvox R20A y R20B - Guía para el Administrador

Akuvox
Open A Smart World

Gracias por elegir los videoporteros Akuvox serie R20. Este manual está dirigido a los administradores que necesitan configurar de forma correcta el videoportero, es aplicable a la versión 320.30.11.14, y proporciona todas las configuraciones para las funciones y características del videoportero Akuvox. Visite el foro de Akuvox o consulte al servicio de asistencia técnica para obtener información nueva o el firmware más reciente.

Akuvox
Open A Smart World

Índice

Akuvox
Open A Smart World

Información General del Producto

La serie Akuvox R20 puede conectarse con monitores interiores para controlar el acceso y la comunicación a distancia. Permiten realizar llamadas de audio con los visitantes y abrir la puerta.

Especificaciones del Modelo

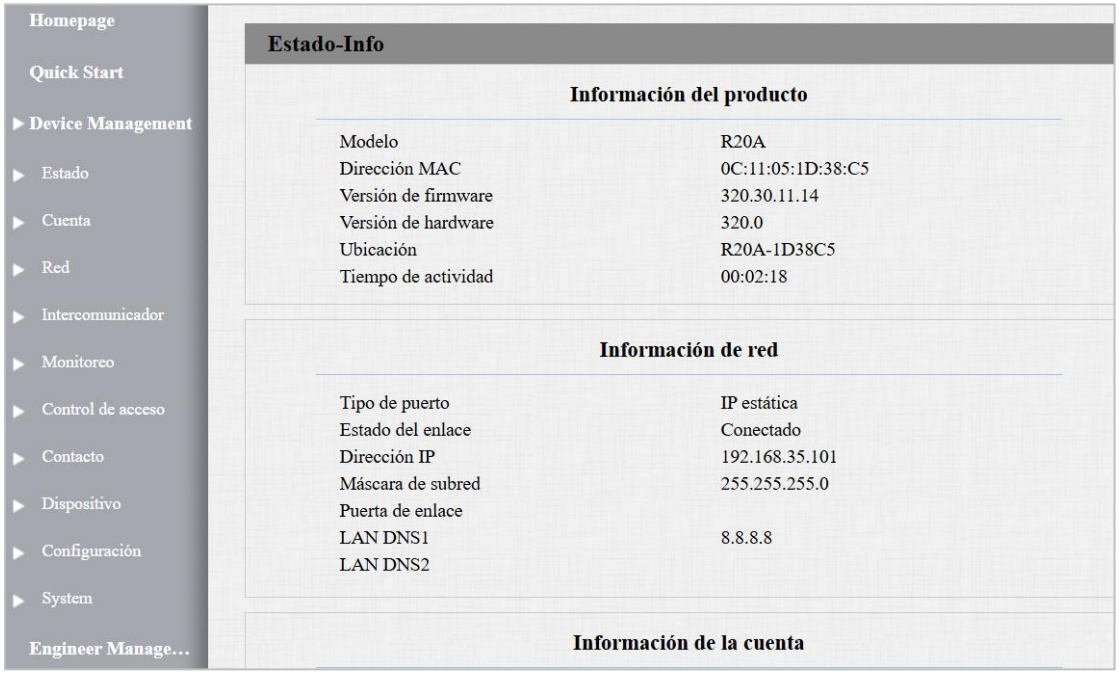
Modelo	R20A/B
Cámara	2 megapíxeles, iluminación automática
Entradas	2
Salida de relés	2
RS485	√
WiFi	X
Lector de tarjetas	13.56MHz, 125kHz y NFC
Micrófono	1
Altavoz	1
Alarma de manipulación	✓

Akuvox
Open A Smart World

Introducción al Menú de Configuración

- Inicio rápido: Esta sección proporciona un acceso rápido a los ajustes básicos del dispositivo, como la configuración de red, usuarios, relés, entre otros.
- Gestión del Dispositivo:
  - Estado: Esta sección contiene información básica sobre el producto, así como ajustes de red, cuentas, etc.
  - Cuenta: Esta sección contiene información acerca de la cuenta SIP, el servidor SIP, el servidor proxy, el tipo de protocolo de transporte, el códec de audio y vídeo, DTMF, etc.
  - Red: Esta sección trata principalmente de la configuración DHCP & IP estática, configuración de puertos RTP, despliegue de dispositivos, etc.
  - Videoportero: Esta sección incluye ajustes de LCD, funciones de llamada, multidifusión, etc.
  - Vigilancia: esta sección abarca la detección de movimiento, la configuración RTSP, la configuración ONVIF, etc.
  - Control de acceso: Esta sección incluye ajustes de relé, ajustes de tarjeta, ajustes de PIN, etc.
  - Directorio: Esta sección es para la gestión de usuarios.
  - Dispositivo: Esta sección cubre los ajustes de LCD, luz, Wiegand, audio y control de ascensor.
  - Ajustes: Esta sección cubre los ajustes de hora e idioma, acción, programación y API HTTP.
  - Sistema: Esta sección incluye información relevante para actualización, mantenimiento, autoaprovisionamiento, etc.
- Gestión de Ingeniería: Esta sección ofrece un acceso rápido a la actualización, mantenimiento y depuración del dispositivo.

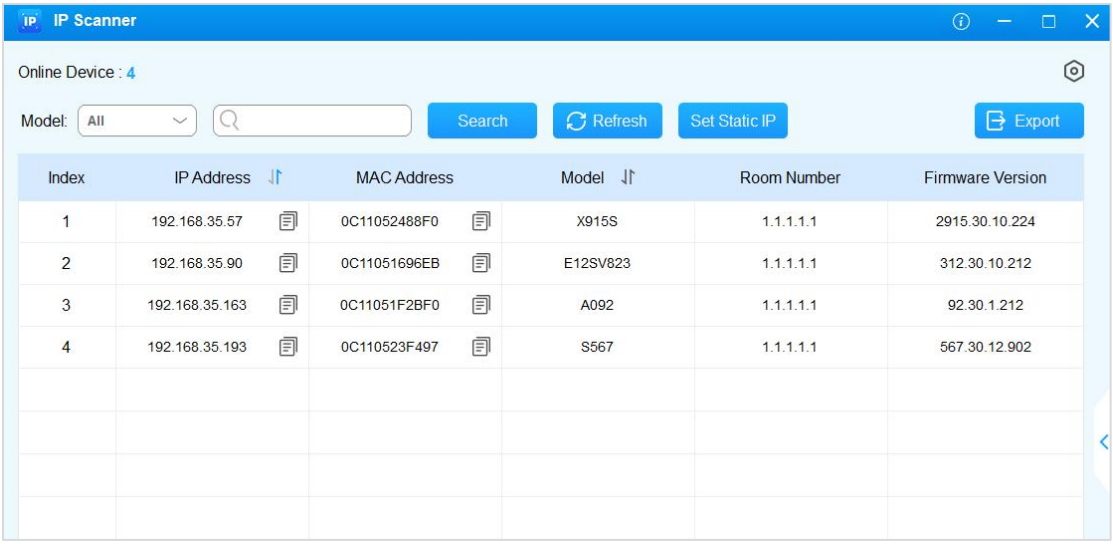
Akuvox
Open A Smart World



Acceder al Dispositivo

Obtener la Dirección IP del Dispositivo

Busque la IP del dispositivo utilizando el escáner IP en la misma red LAN. Haga clic en “Refresh” para actualizar la lista.



Acceder a la Configuración Web del Dispositivo

Puede introducir la dirección IP del dispositivo en un navegador e iniciar sesión en la interfaz web del dispositivo, donde podrá configurar y ajustar los parámetros.

El nombre de usuario y la contraseña iniciales son admin. Recuerde que el sistema distingue entre mayúsculas y minúsculas a la hora de elegir los nombres de usuario y contraseñas.

Nota:

- Descargar escáner IP: https://knowledge.akuvox.com/docs/akuvox-ip-scanner?highlight=IP
- Ver Guía detallada: https://knowledge.akuvox.com/v1/docs/en/how-to-obtain-ip-address-via-ip-scanner?highlight=IP%20Scanner
- Se recomienda especialmente el navegador Google Chrome.

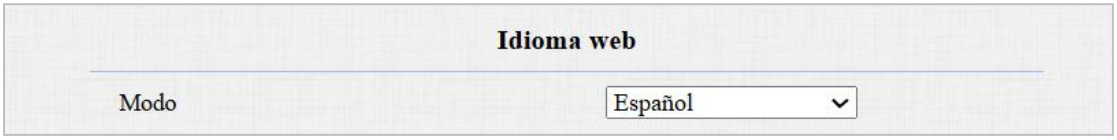
Idioma y Hora

Idioma

Puede cambiar el idioma web en la interfaz Configuración > Hora/Idioma > Idioma web.

Se admiten los siguientes idiomas:

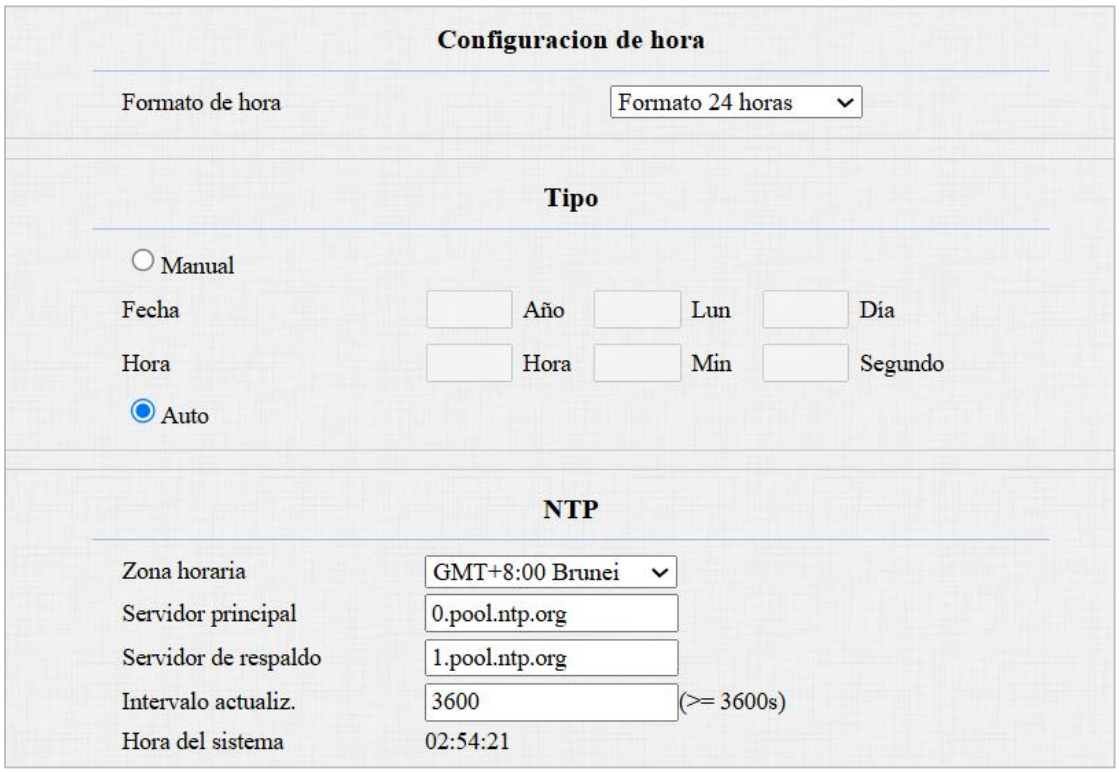
Inglés, chino simplificado, ruso, español, neerlandés, francés, alemán, polaco, japonés y hebreo.



Hora

Los ajustes de hora de la interfaz web permiten configurar la dirección del servidor NTP para la sincronización automática de la hora y la fecha. Una vez seleccionada una zona horaria, el dispositivo notificará al servidor NTP la zona horaria elegida, permitiéndole sincronizar los ajustes de zona horaria de su dispositivo.

Para configurar la hora, vaya a la interfaz web Configuración > Hora/Idioma.



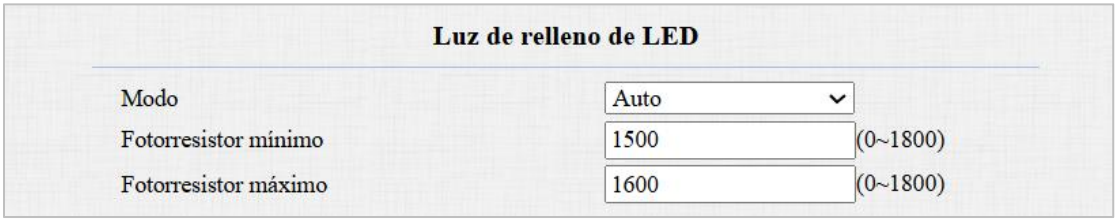
- Formato de hora: Seleccione el formato de 12 horas o el formato de 24 horas.
- Tipo: Puede configurar la hora manualmente seleccionando Manual.
- Servidor Preferido/Alterno: La dirección del servidor NTP. El servidor alternativo tendrá efecto cuando el servidor primario no sea válido.
- Intervalo de actualización ("Update Interval"): El intervalo entre dos peticiones NTP consecutivas.

Ajustes de LED

Luz de relleno LED

La luz de relleno LED está diseñada principalmente para reforzar la luz por la noche o en un entorno oscuro.

Configúrela en la interfaz web Dispositivo > Luz > Luz de relleno LED.

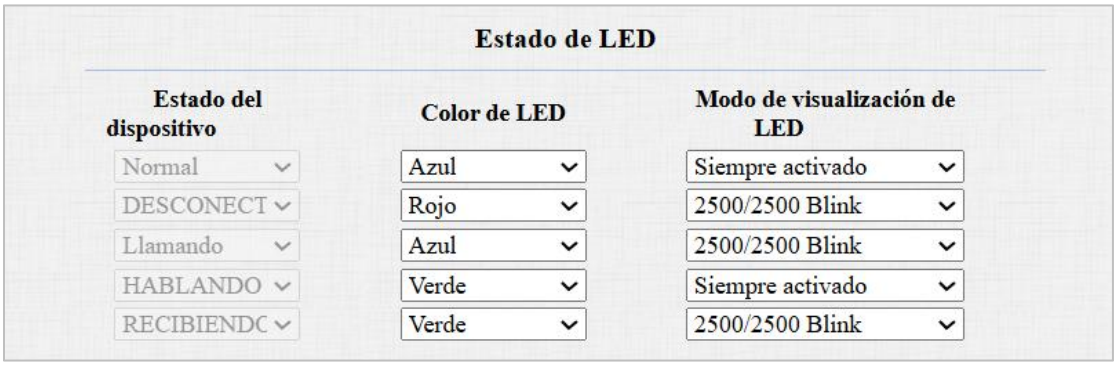


- Modo:
  - Auto: Enciende la luz LED automáticamente en función del valor mínimo y máximo de la fotorresistencia.
  - Siempre encendido: Habilita la luz LED.
  - Siempre apagado: Desactiva la luz LED.
  - Programar: Enciende la luz LED basándose en el horario.
- Fotorresistencia Mín/Máx: Ajuste el valor mínimo y máximo de la fotorresistencia para controlar automáticamente el encendido y apagado de la luz LED. Si el valor de la fotorresistencia es inferior al umbral mínimo, el LED se apagará. Si el valor de la fotorresistencia es superior al umbral máximo, enciende el LED.

Estado de la Pantalla LED

El ajuste de la pantalla LED se utiliza para indicar los cambios de luz del botón de llamada en 5 estados: normal (inactivo), desconectado, llamando, hablando y recibiendo una llamada. El estado del LED permite a los usuarios verificar el modo actual del dispositivo.

Configúrelo en la interfaz web Dispositivo > Luz > Estado de LED.



- Estado del dispositivo: Hay cinco estados: Normal, Desconectado, Llamando, Hablando y Recibiendo.
- Color del LED: Hay tres colores de LED disponibles para cada opción: Azul, Rojo y Verde.
- Modo de visualización del LED: Seleccione la frecuencia de parpadeo del LED deseada.

Modo de Activación de LED

Puede configurar la luz del lector de tarjetas para que se controle por detección de infrarrojos.

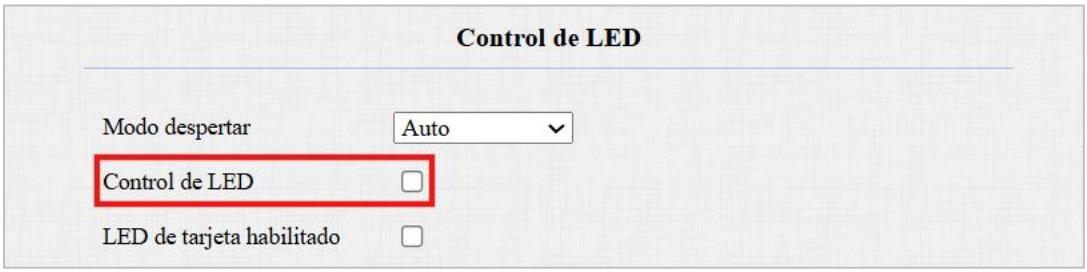
Para configurarlo, vaya a la interfaz Dispositivo > Luz > Control de LED.

- Modo Despertar:
  - Auto: Cuando se activa la detección de infrarrojos, se enciende la luz del lector de tarjetas.
  - Manual: La luz del lector de tarjetas no será controlada por la detección de infrarrojos.

Control de la Pantalla LED mediante URL HTTP

Puede introducir una URL HTTP en un navegador para gestionar el color y la frecuencia de los LED.

Para configurarlo, ve a la interfaz Dispositivo > Luz > Control LED.



El formato de la URL HTTP es:
http://device IP/fcgi/do?action=LedAction&State=1&Color=1&Mode=2500.

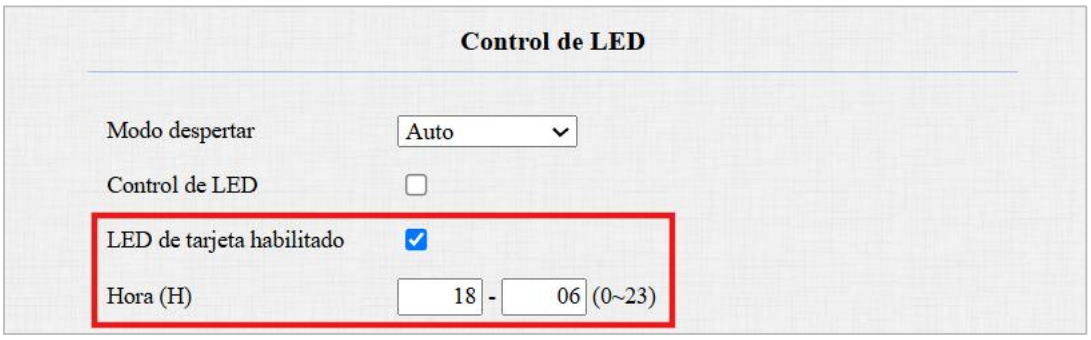
Sustituya el número en el formato para cambiar el LED al estado deseado.

- Estado: 1=Normal ； 2=Fuera de línea ； 3=Llamando；4=Hablando；5= Recibiendo;
- Color: 0=Rojo；1=Verde；2=Bule；
- Modo: 0=Siempre encendido；1=Siempre apagado；500/1000/1500/2000/2500/3000=Frecuencia de parpadeo correspondiente.

Control del LED del Lector de Tarjetas

Puede activar o desactivar la iluminación LED de la zona del lector de tarjetas. También puede establecer una hora específica para encender la luz.

Para configurarlo, vaya a la interfaz Dispositivo > Luz > Control LED.

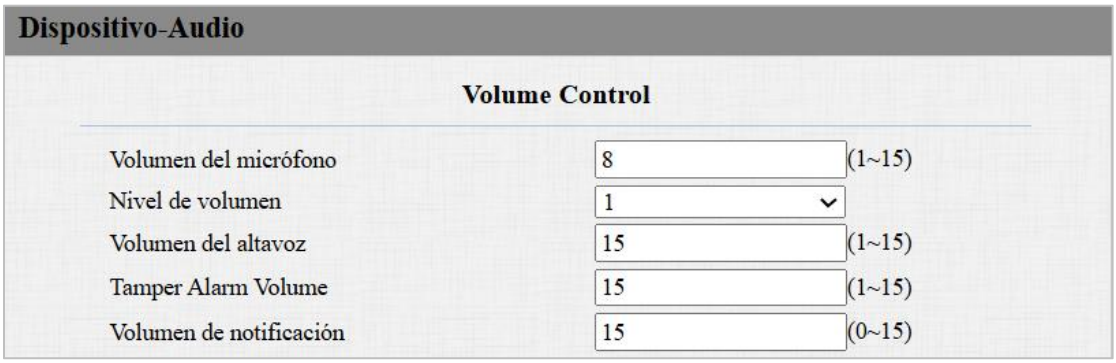


- LED de tarjeta activado: Cuando está habilitado, especifica el periodo en el que la luz está encendida.

Volumen y Tono

Control de Volumen

Puede controlar el volumen del dispositivo en la interfaz Dispositivo > Audio.

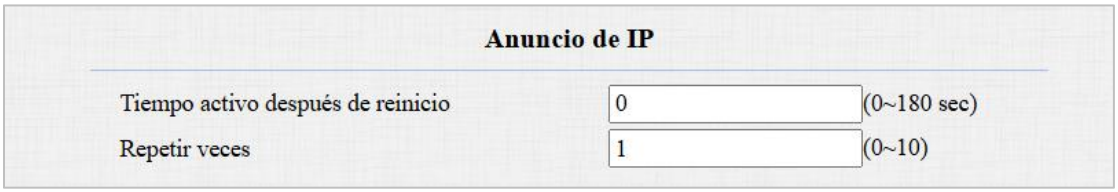


- Nivel de Volumen: Ajusta el volumen general. El rango de volumen del Nivel 1 es aproximadamente 80-95, y el del Nivel 2 es 95-109.
- Volumen de Alarma de Sabotaje: Ajusta el volumen cuando se activa la alarma antimanipulación.
- Volumen de aviso: Varios avisos, incluyendo los avisos de éxito y fracaso en la apertura de la puerta.

Anuncio de IP

Puede configurar cuándo el dispositivo anuncia su IP después de cada reinicio y los tiempos de bucle.

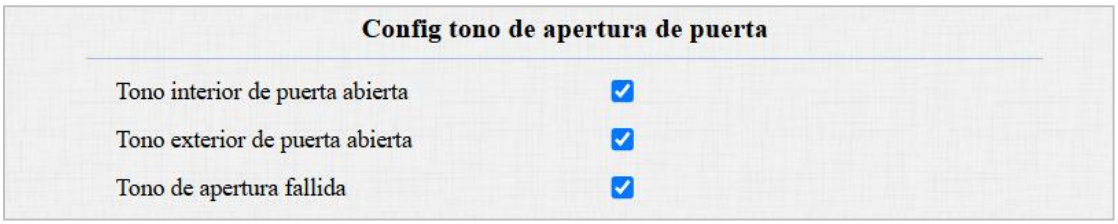
Configúrelo en la interfaz Dispositivo > Audio.



- Tiempo activo tras el reinicio: Para que suene la dirección IP, debe mantener pulsado el botón Llamar durante el tiempo que transcurre después de que se reinicie el dispositivo. Si está ajustado a 0, puede mantener pulsado el botón en cualquier momento para anunciar la IP después del reinicio.

Tonos de Apertura de Puerta

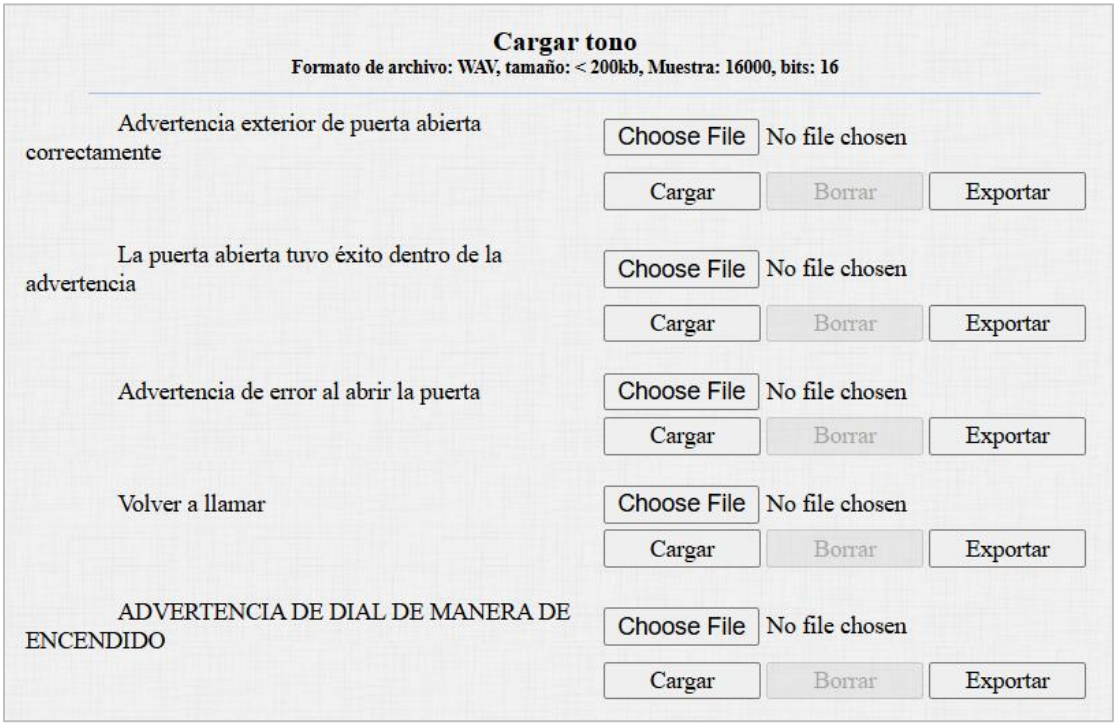
Puede activar o desactivar los tonos de apertura de puerta en la interfaz Dispositivo > Audio.



- Tono interior de puerta abierta: El tono activado por entrada. El tono de apertura de puerta se oye cuando los usuarios abren las puertas pulsando un botón de salida.
- Tono Exterior de Puerta Abierta: El tono activado por relé. El tono de apertura de puerta puede oírse cuando los usuarios abren las puertas mediante los métodos de acceso admitidos por el dispositivo, excepto el botón de salida.

Cargar Archivos de Tonos

Puede cargar varios tonos para enriquecer la experiencia de los usuarios en la interfaz Dispositivo > Audio. Haga clic en Elegir archivo y luego en Cargar para importar el archivo.



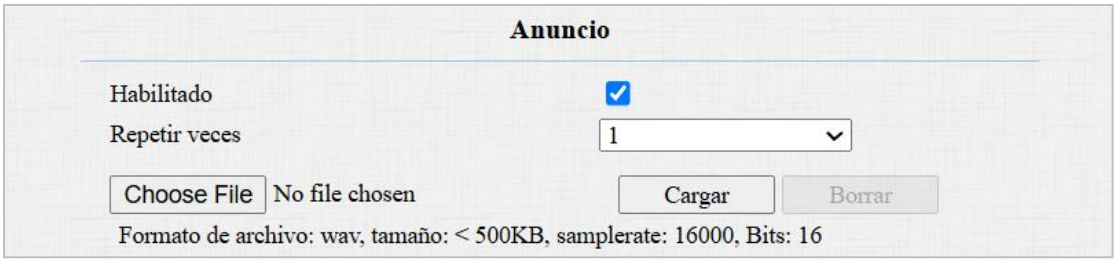
- Advertencia exterior de puerta abierta correctamente: El tono activado por relé. El tono de apertura de puerta puede oírse cuando los usuarios abren las puertas mediante los métodos de acceso admitidos por el dispositivo, excepto el botón de salida.
- Advertencia de puerta abierta exitosa (“La puerta abierta tuvo éxito dentro de la advertencia”): El tono activado por entrada. El tono de apertura de puerta puede oírse cuando los usuarios abren las puertas pulsando un botón de salida.
- Advertencia de Error al Abrir la Puerta: El tono puede oírse cuando falla la apertura de puertas.
- Volver a llamar: Se reproducirá cuando alguien llame al dispositivo.
- Aviso de marcación del administrador de activación: El tono se oye cuando se pulsa el pulsador.

Cargar el Anuncio Reproducido durante las Llamadas de Intercomunicador

El anuncio se reproducirá automáticamente cuando el interlocutor responda a

la llamada desde el portero automático.

Para configurar esta función, vaya a la interfaz Videoportero > Función de llamada > Anuncio.

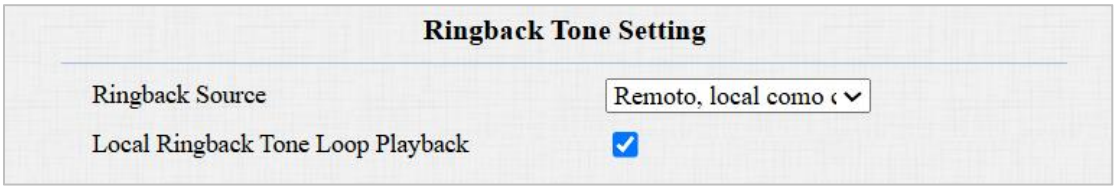


- Tiempos de bucle: Indica cuántas veces se reproducirá el anuncio.

Tono de Retorno de Llamada – “Ringback”

La configuración del tono de llamada de retorno prioriza la reproducción de los tonos de llamada locales y determina qué tipos de previsualizaciones puede recibir el receptor de la llamada.

Para configurarlo, vaya a la interfaz Dispositivo > Audio > Configuración del tono de llamada de retorno.



- “Ringback Source”:
  - Remoto, Local como copia de seguridad: Se reproducirá el tono de llamada local.
    - Cuando el portero automático llama a otro dispositivo, por ejemplo, un monitor interior Akuvox, y el servidor SIP devuelve no-183, el monitor interior no tendrá ninguna vista previa del intercomunicador.
    - Si el servidor SIP devuelve 183, el monitor interior recibirá la previsualización de vídeo sin voz.

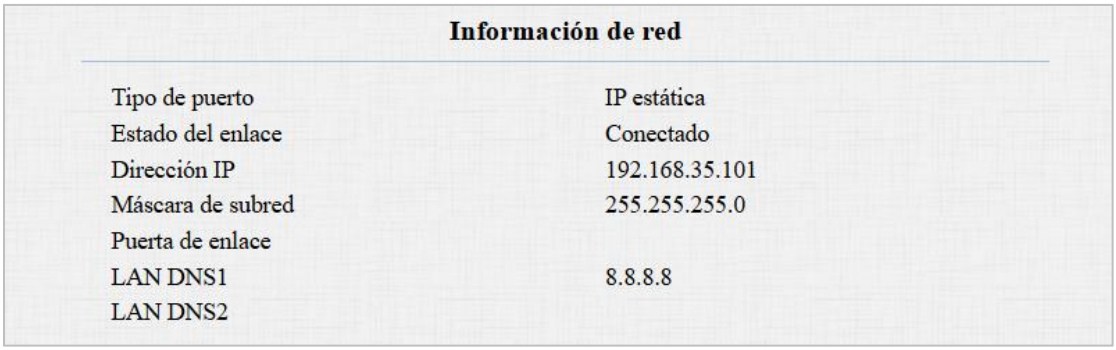
- Local: Se reproducirá el tono de llamada local. Si el servidor SIP devuelve 183 o no, el receptor de la llamada no tendrá ninguna vista previa del intercomunicador.
- Remoto:
  - Si el servidor SIP devuelve un valor distinto de 183, se reproducirá el tono de llamada local y el destinatario de la llamada no tendrá vista previa de intercomunicación.
  - Si el servidor SIP devuelve 183, se reproducirá el tono de llamada del servidor SIP y el destinatario de la llamada recibirá la vista previa de vídeo sin voz.

- Reproducción en bucle del tono de llamada de retorno local: Esta función permite que el tono de llamada de retorno local se reproduzca repetidamente. Está activada por defecto.

Configuración de Red

Estado de Red

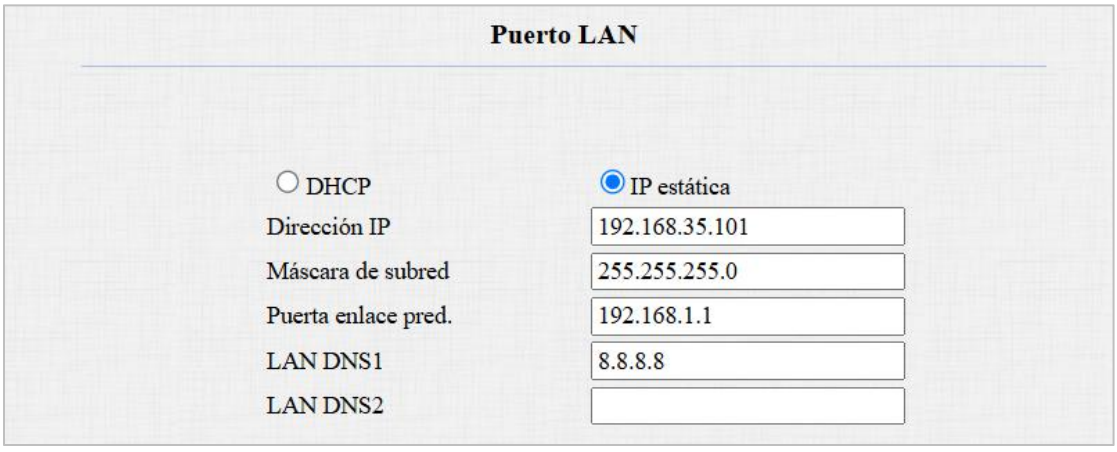
Compruebe el estado de la red en la interfaz web Estado > Información > Información de red.



Configuración de Red del Dispositivo

Para garantizar un funcionamiento normal, asegúrese de que el dispositivo tiene su dirección IP configurada correctamente u obtenida automáticamente del servidor DHCP.

Para configurar la red, vaya a la interfaz web Red > Básico.



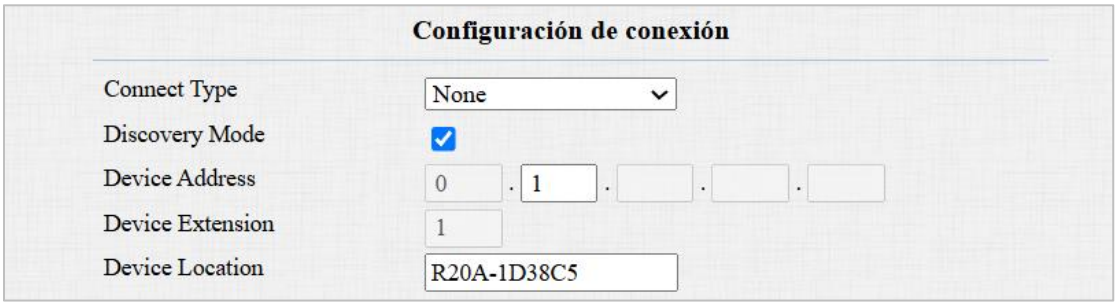
- DHCP: El modo DHCP es la conexión de red por defecto. Si el modo DHCP está activado, el servidor DHCP asignará automáticamente al portero automático una dirección IP, una máscara de subred, una puerta de enlace predeterminada y una dirección de servidor DNS.

- IP estática: Cuando se selecciona el modo IP estática, la dirección IP, la máscara de subred, la puerta de enlace predeterminada y la(s) dirección(es) del servidor DNS deben configurarse manualmente de acuerdo con el entorno de red real.
- Dirección IP: Configure la dirección IP cuando se seleccione el modo IP estático.
- Máscara de Subred: Configure la máscara de subred de acuerdo con el entorno de red real.
- Puerta de Enlace Predeterminada: Establezca la puerta de enlace correcta de acuerdo con la dirección IP.
- Servidor DNS preferido/alternativo: El servidor DNS preferido es la dirección del servidor DNS primario, mientras que el servidor DNS alternativo es el secundario. El portero automático se conectará al servidor alternativo cuando el servidor primario no esté disponible.

Despliegue de Dispositivos en la Red

Para facilitar el control y la gestión de los dispositivos, configure los videoporteros Akuvox con detalles como la ubicación, el modo de funcionamiento, la dirección y los números de extensión.

Para configurarlo, navegue hasta la interfaz web Red > Avanzado.



- Tipo de conexión: Se configura automáticamente según la conexión real del dispositivo con un servidor específico de la red como SDMC, Nube o Ninguno. Ninguno es la configuración predeterminada de fábrica que indica que el dispositivo no está en ningún tipo de servidor. También

puede elegirlo manualmente.

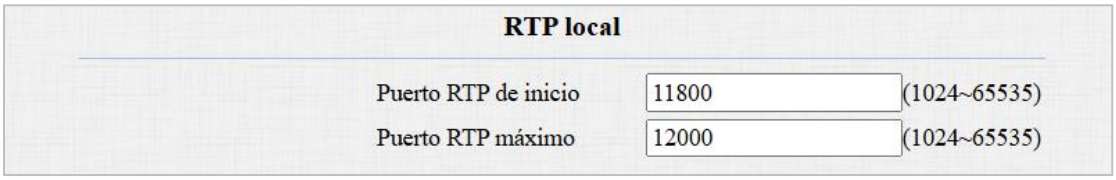
- Modo de Descubrimiento: Cuando está activado, el dispositivo puede ser descubierto por otros dispositivos de la red. Cuando está desactivado, el dispositivo estará oculto y no podrá ser descubierto por otros dispositivos.
- Dirección del dispositivo: Especifique la dirección del dispositivo introduciendo la información de ubicación del dispositivo de izquierda a derecha: Comunidad, Edificio, Unidad, Planta y Habitación en secuencia.
- Extensión del dispositivo: El número de extensión del dispositivo.
- Ubicación del dispositivo: La ubicación en la que está instalado y se utiliza el dispositivo.

Configuración de RTP Local del Dispositivo

El protocolo de transporte en tiempo real (RTP) permite a los dispositivos transmitir datos de audio y vídeo a través de una red en tiempo real.

Para utilizar RTP, los dispositivos necesitan una serie de puertos. Un puerto es como un canal para datos en una red. Si configuras puertos RTP en tu dispositivo y router, puedes evitar interferencias en la red y mejorar la calidad de audio y vídeo.

Para configurar RTP, navega a la interfaz web Red > Avanzado.

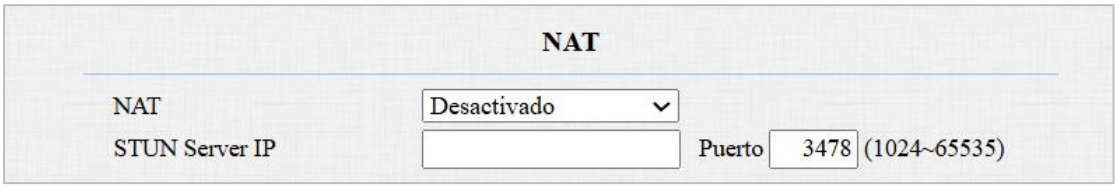


- Puerto RTP inicial: Valor del puerto para establecer el punto inicial del rango de transmisión exclusiva de datos.
- Puerto RTP máximo: El valor de puerto para establecer el punto final para el rango de transmisión exclusiva de datos.

Configuración de NAT

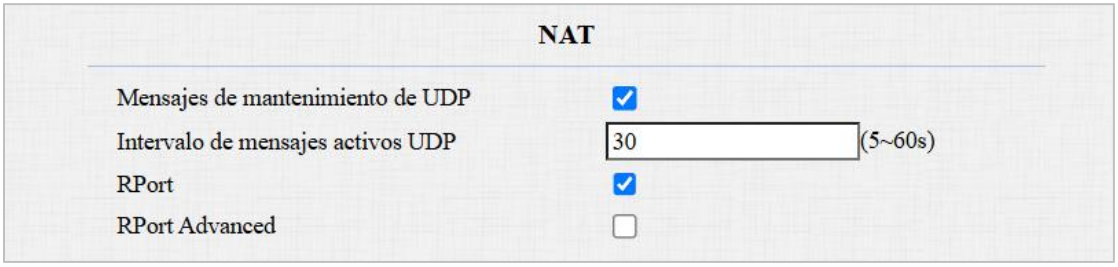
La traducción de direcciones de red (NAT, por su sigla en inglés) permite a los dispositivos de una red privada utilizar una única dirección IP pública para acceder a Internet o a otras redes públicas. NAT guarda las direcciones IP públicas limitadas y oculta las direcciones IP internas y los puertos del mundo exterior.

Para configurar NAT, ve a la interfaz Cuenta > Básico > NAT.



- IP del Servidor SIP: Establezca la dirección del servidor SIP en la Red de Área Amplia(WAN).
- Puerto: Establezca el puerto del servidor SIP.

A continuación, configure NAT en la interfaz Cuenta > Avanzado > NAT.

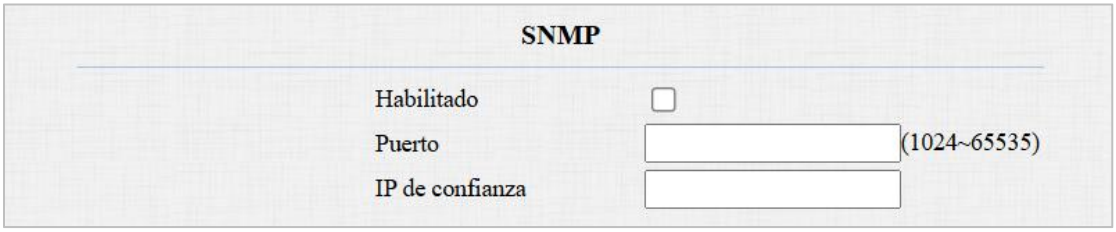


- Mensajes UDP “Keep Alive”: Si está habilitado, el dispositivo enviará el mensaje al servidor SIP para que el servidor SIP reconozca si el dispositivo está en estado en línea.
- Intervalo de Mensajes UDP “Alive”: El intervalo de envío de mensajes oscila entre 5 y 60 segundos. El valor predeterminado es 30 segundos.
- RPort: Habilita el RPort cuando el servidor SIP está en WAN.
- RPort Avanzado: Estabiliza aún más la red basándose en RPort.

Configuración de SNMP

El Protocolo Simple de Gestión de Red (SNMP, por su sigla en inglés) es un protocolo para gestionar dispositivos de red IP. Permite a los administradores de red supervisar los dispositivos y recibir alertas de condiciones dignas de atención. SNMP proporciona variables que describen la configuración del sistema, organizadas en jerarquías y descritas por Bases de Información de Gestión (MIBs, por su sigla en inglés).

Para configurar SNMP, vaya a la interfaz web Red > Avanzado.

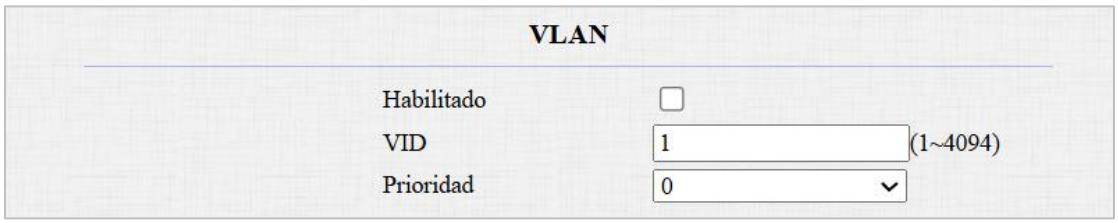


- Puerto: El puerto del servidor SNMP.
- IP Confiable: La dirección permitida del servidor SNMP. Puede ser una dirección IP o cualquier nombre de dominio URL válido.

Configuración de VLAN

Una red de área local virtual (VLAN, por su sigla en inglés) es un grupo lógico de nodos del mismo dominio IP, independientemente de su segmento de red físico. Separa el dominio de difusión de capa 2 mediante switches o routers, enviando paquetes etiquetados sólo a los puertos con IDs VLAN coincidentes. La utilización de VLANs mejora la seguridad al limitar los ataques ARP a hosts específicos y mejora el rendimiento de la red al minimizar las tramas de difusión innecesarias, conservando así el ancho de banda para una mayor eficiencia.

Para configurar una VLAN, vaya a la interfaz web Red > Avanzado.



- VID: El ID de la VLAN para el puerto designado.
- Prioridad: La prioridad de la VLAN para el puerto designado.

Configuración TR069

TR-069 (Informe Técnico 069) proporciona la comunicación entre el Equipo Local del Cliente (CPE) y los Servidores de Autoconfiguración (ACS). Incluye tanto una configuración automática segura como el control de otras funciones de gestión del CPE dentro de un marco integrado. En el caso de los teléfonos de puerta, los administradores pueden gestionar todos los dispositivos en una plataforma TR-069 común. Los teléfonos IP pueden configurarse de forma fácil y segura en la plataforma TR-069 para hacer más eficiente el despliegue masivo.

Para configurarlo, navegue a la interfaz web Red > Avanzado.

- Versión: Seleccione la versión TR069 compatible (versión 1.0 o 1.1).
- URL ACS/CPE: La dirección URL para ACS o CPE. ACS es la abreviatura

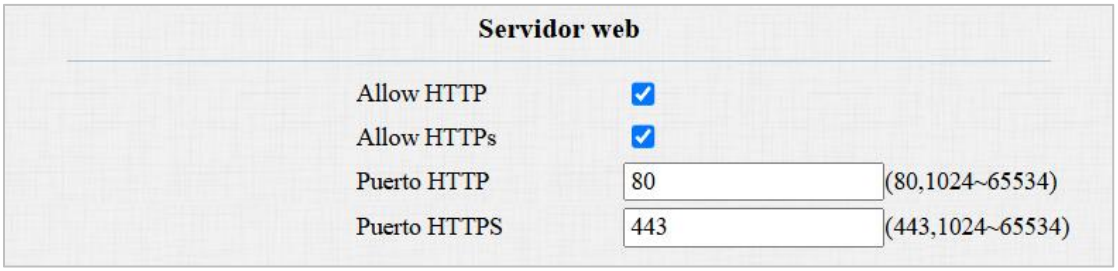
de los servidores de autoconfiguración en el lado del servidor, y CPE es la abreviatura de los equipos locales del cliente como dispositivos del lado del cliente.

- Intervalo periódico: El intervalo para las notificaciones periódicas.

Configuración HTTP de la Web del Dispositivo

Esta función gestiona el acceso al sitio web del dispositivo. El dispositivo admite dos métodos de acceso remoto: HTTP y HTTPS (cifrado).

Para configurarlo, vaya a la interfaz web Red > Avanzado.



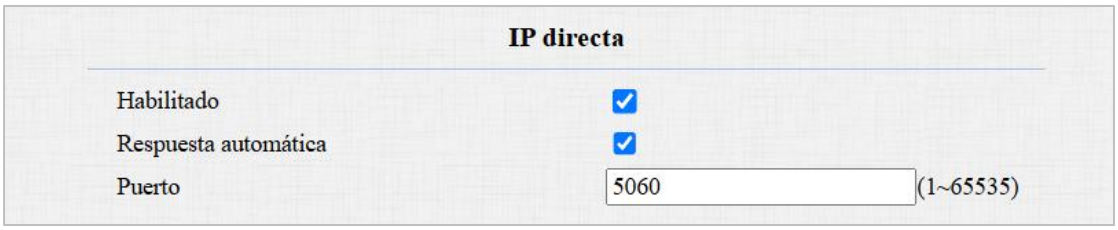
- Permitir HTTP/HTTPS: HTTP y HTTPS están habilitados por defecto.
- Puerto HTTP/HTTPS: Especifique el puerto del servidor web para acceder a la interfaz web del dispositivo a través de HTTP/HTTPS.

Configuración de Llamadas de Videoportero

Configuración de Llamadas IP

Una llamada IP es una llamada directa entre dos videoporteros utilizando sus direcciones IP, sin servidor ni centralita o PBX. Las llamadas IP funcionan cuando los dispositivos están en la misma red.

Active o desactive la función de llamada IP directa en la interfaz web Videoportero > Función de llamada > IP directa.



- Puerto: Establezca el puerto para llamadas IP directas. El valor por defecto es 5060, con un rango de 1-65535. Si introduce un valor dentro de este rango distinto de 5060, asegúrese de la coherencia con el dispositivo correspondiente para la transmisión de datos.

Configuración de Llamadas SIP

El Protocolo de Iniciación de Sesión (SIP, por su sigla en inglés) es un protocolo de transmisión de señalización utilizado para iniciar, mantener y finalizar llamadas.

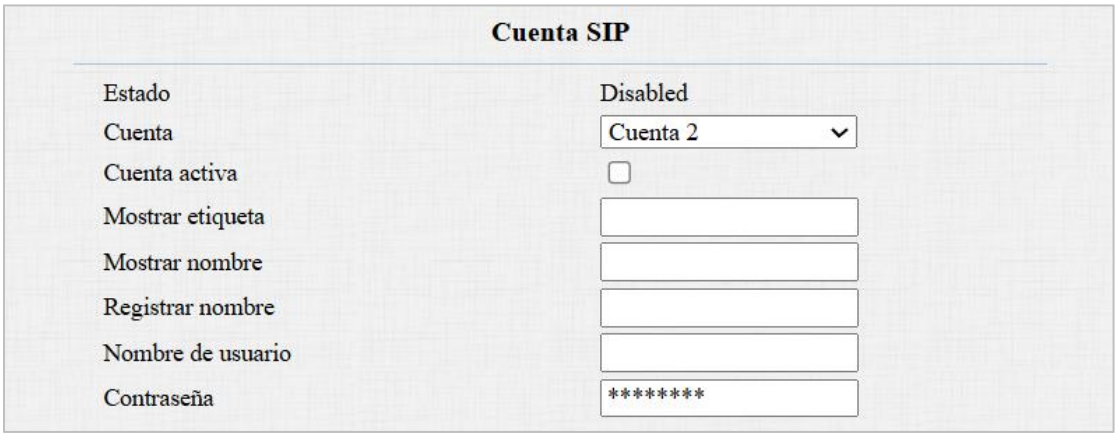
Una llamada SIP utiliza SIP para enviar y recibir datos entre dispositivos SIP, y puede utilizar Internet o una red local para ofrecer una comunicación segura y de alta calidad. Iniciar una llamada SIP requiere una cuenta SIP, una dirección SIP para cada dispositivo y configurar los ajustes SIP en los dispositivos.

Registro de Cuenta SIP

Cada dispositivo necesita una cuenta SIP para hacer y recibir llamadas SIP.

Los dispositivos de intercomunicación Akuvox admiten la configuración de dos cuentas SIP, que pueden registrarse en dos servidores independientes.

Registre la cuenta SIP en la interfaz web Cuenta > Básico.

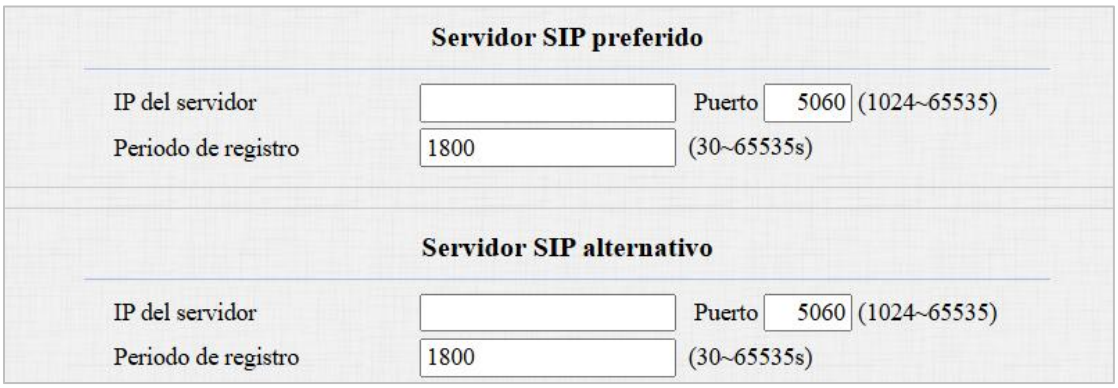


- Estado: Muestra si la cuenta SIP está registrada o no.
- Cuenta 1/Cuenta 2: El videoportero admite 2 cuentas SIP.
  - La cuenta 1 es la cuenta predeterminada para el procesamiento de llamadas. También se utilizará cuando se active el servicio en la nube SmartPlus de Akuvox.
  - El sistema cambia a la Cuenta 2 si la Cuenta 1 no está registrada.
- Cuenta Activa: Marque esta opción para activar la cuenta SIP registrada.
- Mostrar Etiqueta: La etiqueta del dispositivo que se mostrará en la pantalla del dispositivo.
- Mostrar Nombre: El nombre del dispositivo que se mostrará en el dispositivo al que se llama.
- Registrar Nombre: El mismo que el nombre de usuario del servidor de la centralita/PBX.
- Nombre de usuario: Igual que el nombre de usuario del servidor del PBX para la autenticación.
- Contraseña: Igual que la contraseña del servidor del PBX para la autenticación.

Configuración del Servidor SIP

Los servidores SIP permiten a los dispositivos establecer y gestionar sesiones de llamada con otros dispositivos de intercomunicación utilizando el protocolo SIP. Pueden ser servidores de terceros o del PBX integrados en el monitor de interior Akuvox.

Para configurar el servidor SIP, vaya a la interfaz web Cuenta> Básico.

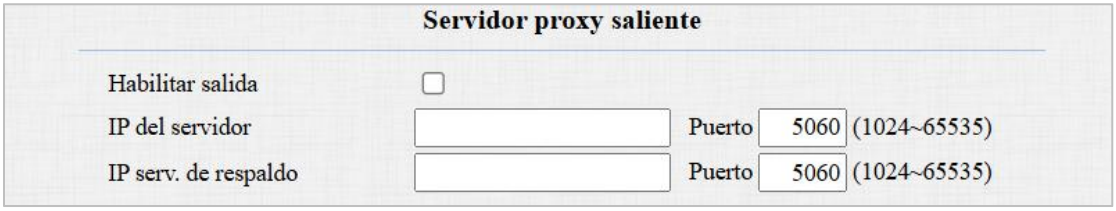


- IP del servidor: Introduzca la dirección IP del servidor o su nombre de dominio.
- Puerto: Especifique el puerto del servidor SIP para la transmisión de datos.
- Periodo de Registro: Defina el límite de tiempo para el registro de la cuenta SIP. Se iniciará un nuevo registro automático si el registro de la cuenta falla dentro de este periodo especificado.

Servidor Proxy de Salida

Un servidor proxy de salida recibe y reenvía todas las peticiones al servidor designado. Es una configuración opcional, pero si se configura, todas las futuras peticiones SIP se enviarán allí en primera instancia.

Para configurarlo, vaya a la interfaz web Cuenta > Básico > Servidor Proxy de Salida.



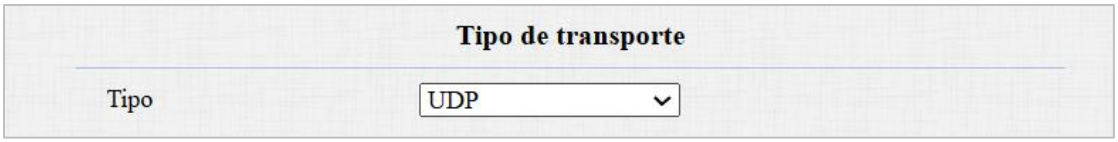
- IP del Servidor Preferido: Introduzca la dirección IP del proxy SIP.
- Puerto: Establezca el puerto para establecer una sesión de llamada a través del servidor proxy saliente.
- IP del Servidor de Respaldo: Introduzca la dirección IP del proxy SIP que se utilizará cuando el proxy principal no funcione correctamente.

- Puerto: Establezca el puerto proxy para establecer una sesión de llamada a través del servidor proxy saliente de reserva.

Tipo de Transmisión de Datos

Los dispositivos de intercomunicación Akuvox admiten cuatro protocolos de transmisión de datos: Protocolo de Datagramas de Usuario (UDP), Protocolo de Control de Transmisión (TCP), Seguridad de la Capa de Transporte (TLS) y DNS-SRV.

Para configurarlo, vaya a la interfaz web Cuenta > Básico.



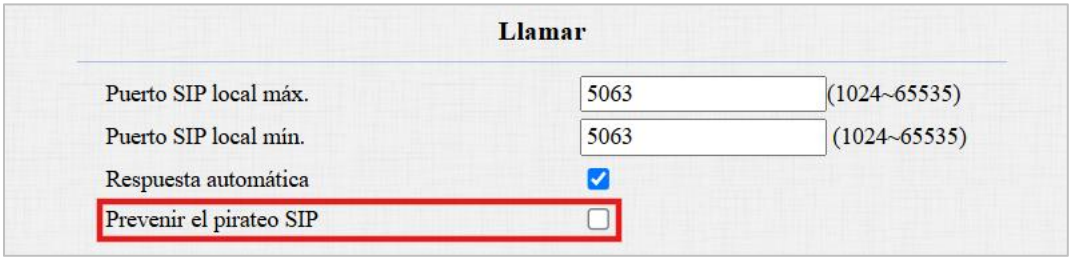
- UDP: Un protocolo de capa de transporte poco fiable pero muy eficiente. Es el protocolo de transporte por defecto.
- TCP: Un protocolo de capa de transporte menos eficiente pero fiable.
- TLS: Un protocolo de capa de transporte cifrado y seguro. Seleccione esta opción si desea cifrar los mensajes SIP para mejorar la seguridad o si el servidor de la otra parte utiliza TLS. Para utilizarlo, es necesario cargar certificados para la autenticación.
- DNS-SRV: Un registro de servicio DNS define la ubicación de los servidores. Este registro incluye el nombre de host y el número de puerto del servidor, así como los valores de prioridad y peso que determinan el orden y la frecuencia de uso del servidor.

Prevención de Pirateo SIP

La escucha telefónica por Internet es un ataque a la red que permite a partes no autorizadas interceptar y acceder al contenido de las sesiones de comunicación entre usuarios de videoporteros. Esto puede exponer

información sensible y confidencial a los atacantes. La protección contra la piratería SIP es una técnica que impide que las llamadas SIP se vean comprometidas en Internet.

Active la prevención contra piratería SIP en la interfaz Cuenta > Avanzado > Llamar.



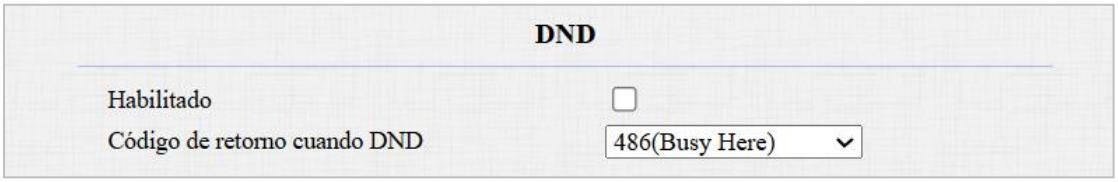
- Prevenir el pirateo SIP: Activa esta función para recibir llamadas sólo de los contactos de la lista blanca. Esto protege la información privada y secreta de los usuarios de posibles piratas informáticos durante las llamadas SIP.

Configuración de Llamadas

Configuración de DND

La función No Molestar (DND, por su sigla en inglés) bloquea las llamadas SIP entrantes no deseadas, garantizando un enfoque ininterrumpido. También permite configurar un código que se enviará al servidor SIP al rechazar una llamada.

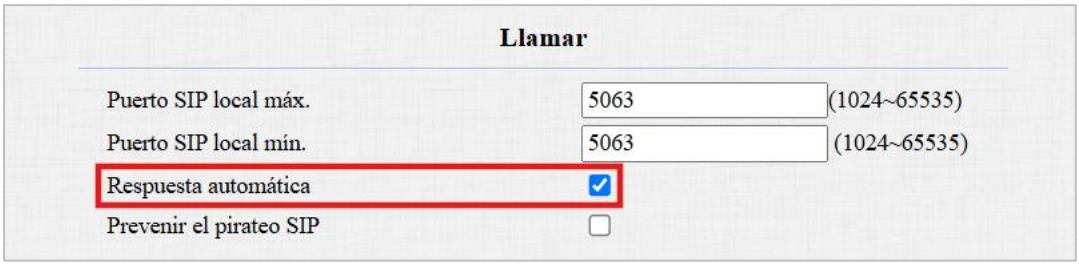
Para configurar la función DND, vaya a la interfaz web Videoportero > Función de llamada.



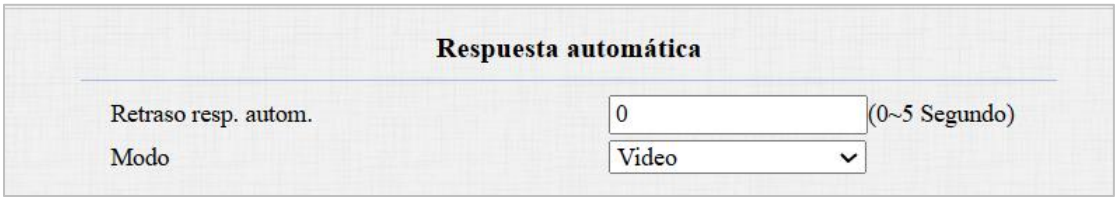
Respuesta Automática

La función de respuesta automática permite al dispositivo responder automáticamente a las llamadas entrantes sin intervención manual. También puede personalizar esta función estableciendo la duración de la respuesta automática y eligiendo el modo de comunicación entre audio y vídeo.

Para configurar la respuesta automática, vaya a la interfaz Cuenta > Avanzado > Llamar.



Para configurarlo, vaya a la interfaz Videoportero > Función de llamada > Respuesta automática.

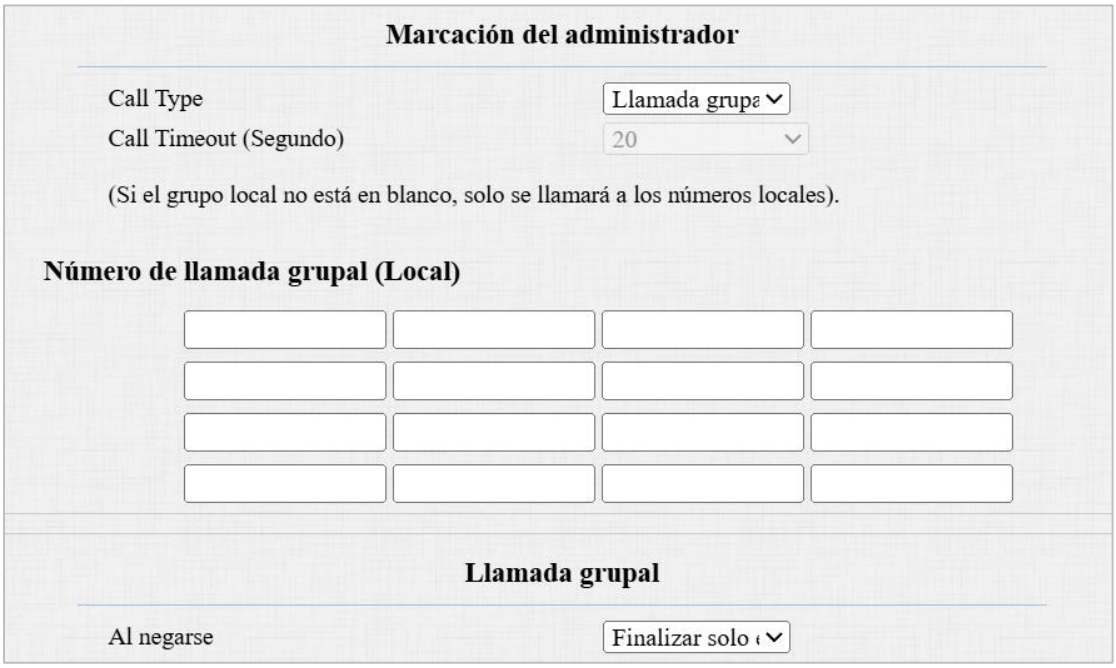


- Retraso Resp. Autom.: Establezca el intervalo de tiempo para que la llamada se descuelgue automáticamente después de sonar. Por ejemplo, si establece el tiempo de retardo en 5 segundos, el portero automático contestará la llamada automáticamente transcurridos 5 segundos.
- Modo: Determine si desea contestar automáticamente la llamada como llamada de vídeo o de audio.

Llamada de Grupo

Esta función permite a los usuarios llamar a un grupo de contactos con una sola pulsación. El dispositivo admite llamadas de grupo locales y con funciones SmartPlus. Para conocer la configuración detallada, pulse aquí.

Para configurar la llamada de grupo, vaya a la interfaz Videoportero > Básico.

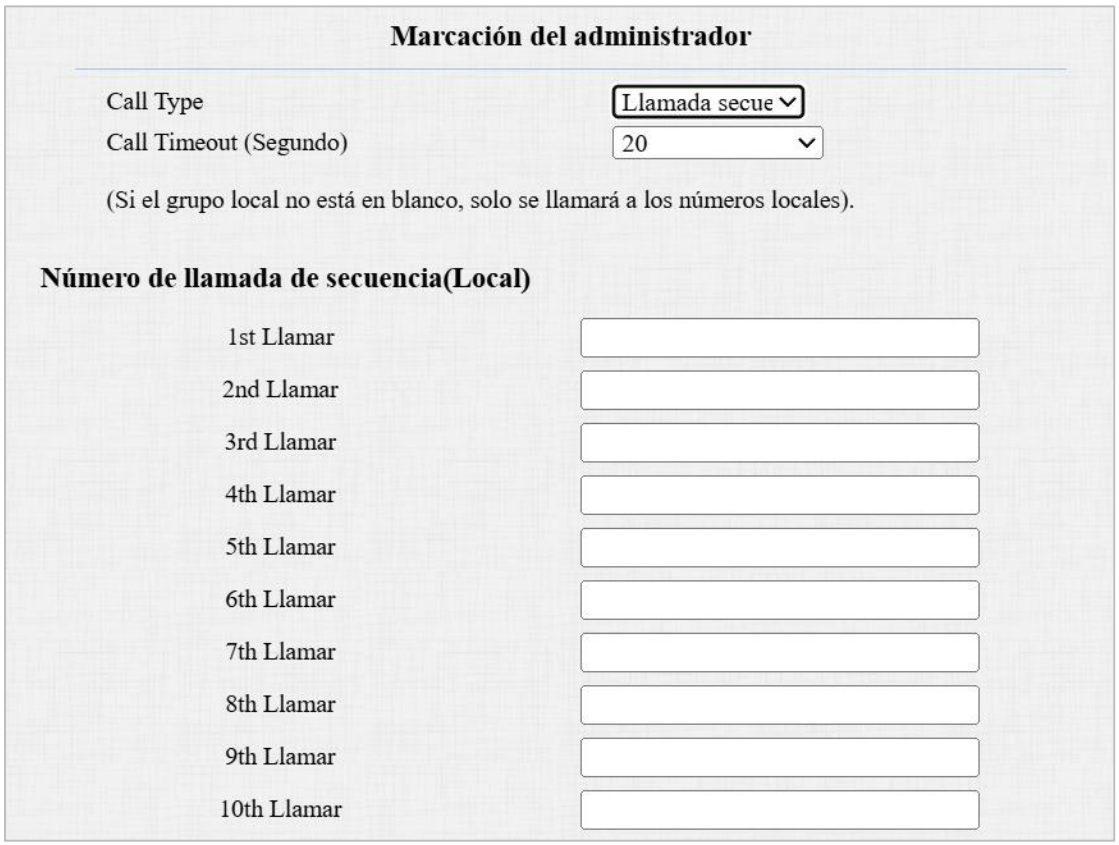


- Tipo de llamada: Seleccione llamada de Grupo.
- Número de llamada de grupo (Local): Introduzca los números de destino.
- Al rechazar:
  - Terminar todas las llamadas: El dispositivo dejará todas las llamadas.
  - Terminar sólo esta llamada: El dispositivo continuará llamando a otros números.

Llamada en Secuencia

La llamada en secuencia es una función que permite marcar un grupo de números en un orden predefinido hasta que uno de ellos conteste. Esta característica es soportada por Akuvox SmartPlus, que proporciona un conjunto de números de llamada de secuencia para la aplicación. Haga clic aquí para ver la configuración detallada.

Para configurar la llamada secuencial, vaya a la interfaz web Videoportero > Básico.

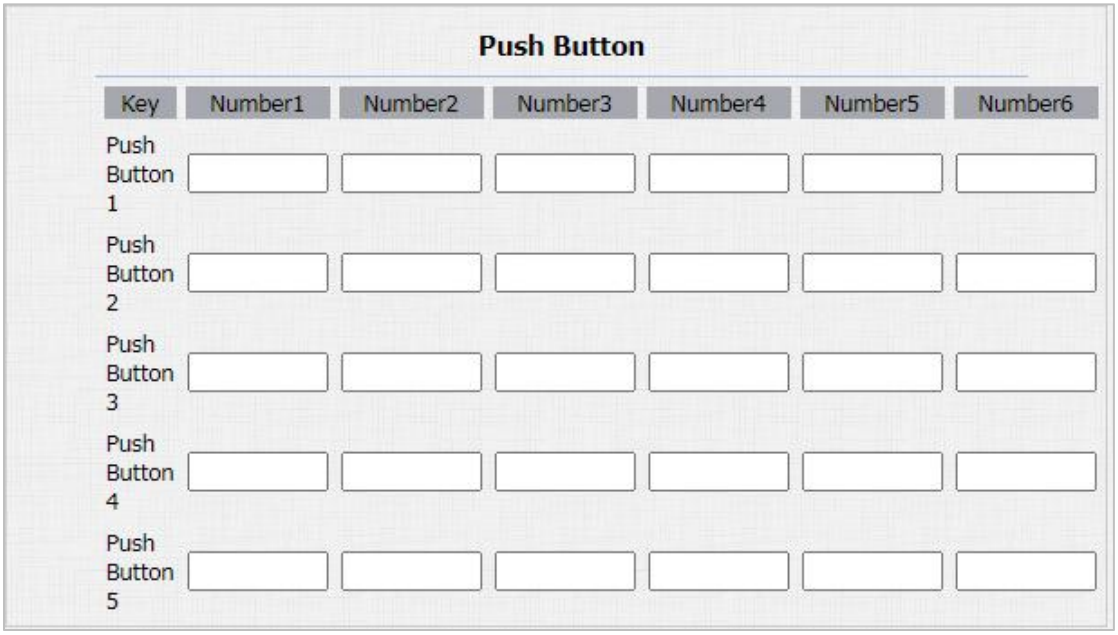


- Tipo de llamada: Seleccionar llamada de secuencia.
- Tiempo de espera de llamada(Seg): Determina la duración antes de llamar al siguiente número cuando no se contesta la llamada anterior.
- Número de Llamada de Secuencia(Local): Introduzca los números de destino.

Marcación Rápida

Para el R20B, puede configurar la función de marcación rápida, que permite a los usuarios realizar llamadas de grupo rápidas pulsando el botón preconfigurado.

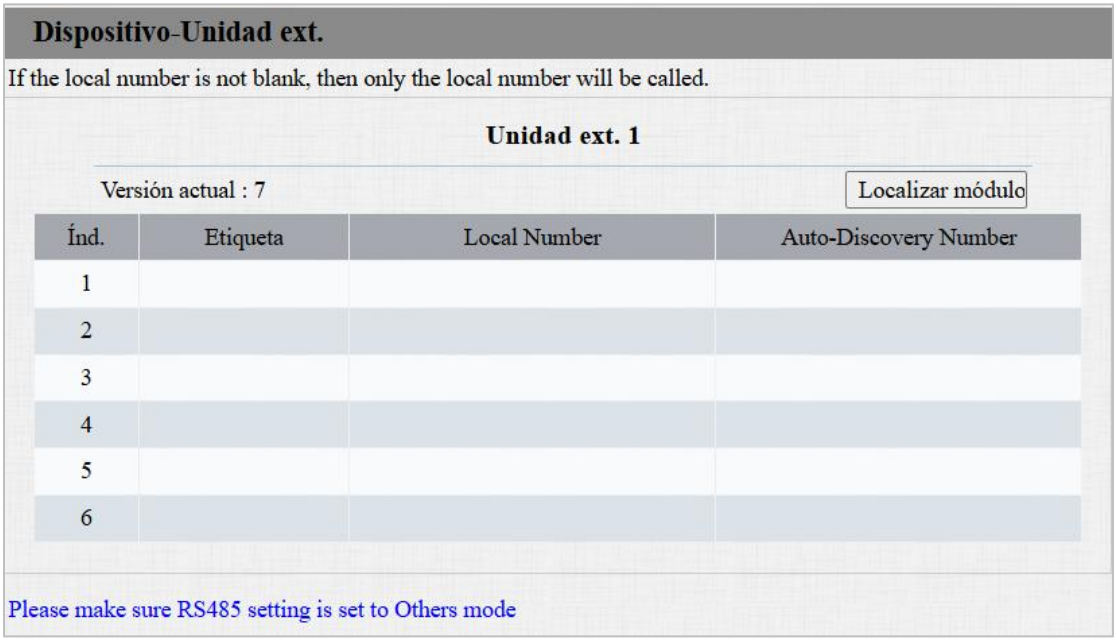
Configúrela en la interfaz Videoportero > Básico. Introduzca los números de destino en la casilla del pulsador deseado.



Marcación Rápida en el Módulo de Expansión

El R20B admite la conexión con una unidad de ampliación, lo que permite configurar más números de marcación rápida. Los usuarios pueden pulsar la tecla de la unidad para llamar.

Configúrelo en la interfaz Dispositivo > Unidad de extensión.



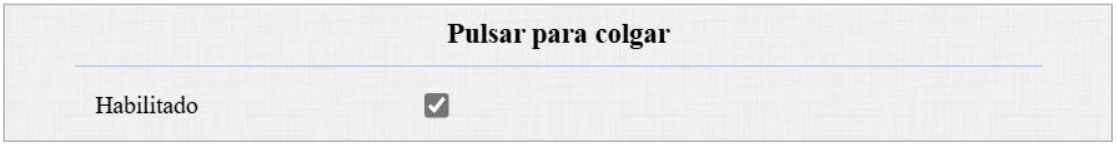
- Localizar módulo: Al pulsarlo, la luz de la llave parpadeará tres veces a intervalos de 500 ms.
- Etiqueta: El nombre de la tecla, normalmente el nombre del llamante.
- Número Local: El número IP/SIP del dispositivo llamado.
- Número de Autodescubrimiento: Cuando el dispositivo se utiliza en la Solución de Red Auto descubierta, se mostrará el número de otros dispositivos de videoporteros de la solución.

Nota:

SÓLO los dispositivos con la versión de firmware 320.30.10.116 o superior admiten esta función.

Colgar Llamada Pulsando el Pulsador

Puede activar o desactivar la pulsación del pulsador para colgar una llamada en la interfaz Videoportero > Básico > Pulsar para colgar.



Multidifusión

La multidifusión es un tipo de comunicación en la que una fuente transmite a varios receptores dentro de un rango determinado. El portero automático puede funcionar como receptor, recibiendo el audio proveniente de la fuente de difusión.

Para configurar la multidifusión, acceda a la interfaz Videoportero > Multidifusión.

- “Paging Barge”: Determina cuántos grupos de multidifusión tienen mayor prioridad que las llamadas SIP. Si se desactiva, las llamadas SIP tendrán mayor prioridad.
- “Paging Priority”: Decide si se realiza la multidifusión por orden de prioridad.
- “Listening Address”: Introduzca la dirección IP. La dirección de escucha debe ser la misma que la dirección de multidifusión. El puerto de escucha

y el puerto multicast no pueden ser el mismo para cada dirección IP. La dirección IP de multidifusión va de 224.0.0.0 a 239.255.255.255.

Nota:

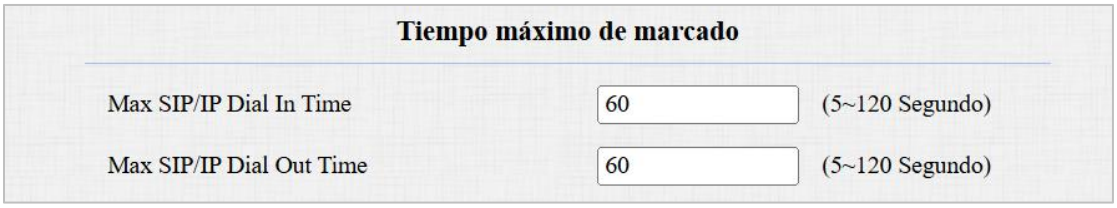
Póngase en contacto con el equipo técnico de Akuvox para obtener una dirección multicast válida.

- Etiqueta: Nombre del grupo de multidifusión.

Duración Máxima de Marcado

La duración máxima de marcado es el límite de tiempo para llamadas entrantes y/o salientes en el portero automático. Si se configura, el portero automático finalizará automáticamente la llamada si nadie responde a la llamada en el tiempo preestablecido, tanto si es entrante como saliente.

Para configurar la duración máxima de marcado, vaya a la interfaz web Videoportero > Funciones de llamada.



- “Max SIP/IP Dial In Time”: Especifique la duración máxima de una llamada entrante. El videoportero finalizará automáticamente la llamada entrante si no se contesta en el tiempo preestablecido.
- “Max SIP/IP Dial Out Time”: Especifique la duración máxima de una llamada saliente. El videoportero finalizará automáticamente la llamada saliente si el destinatario no responde en el tiempo preestablecido.

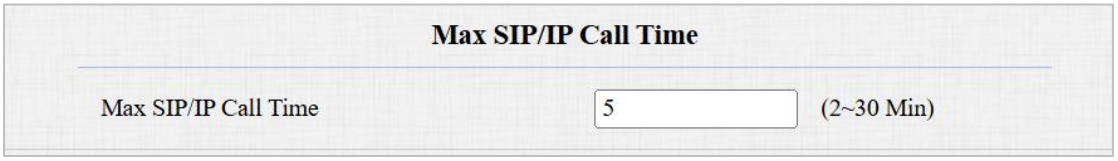
Nota:

El tiempo máximo de marcado se ve afectado por el tiempo máximo de marcado del servidor SIP cuando los usuarios realizan llamadas SIP. El tiempo máximo de llamada no debe exceder la duración de marcación del servidor SIP.

Tiempo Máximo de Llamada

El portero automático le permite establecer la duración máxima de la llamada al recibir la llamada del dispositivo que llama, ya que la persona que llama puede olvidarse de colgar el dispositivo de intercomunicación. Cuando se alcance el tiempo máximo de llamada, el portero terminará la llamada automáticamente.

Para configurar la duración de la llamada, vaya a la interfaz web Videoportero > Funciones de llamada.



- Tiempo máximo de llamada SIP/IP: Especifique la duración máxima de todas las llamadas. El portero terminará la llamada automáticamente cuando se alcance el límite de tiempo.

Nota:
El tiempo máximo de llamada se ve afectado por el tiempo máximo de llamada del servidor SIP cuando los usuarios realizan llamadas SIP. El tiempo máximo de llamada no debe superar la duración de llamada del servidor SIP.

Llamada Web

La función de llamada web permite realizar llamadas a través de la interfaz web del dispositivo, utilizada habitualmente para realizar pruebas de llamadas remotas.

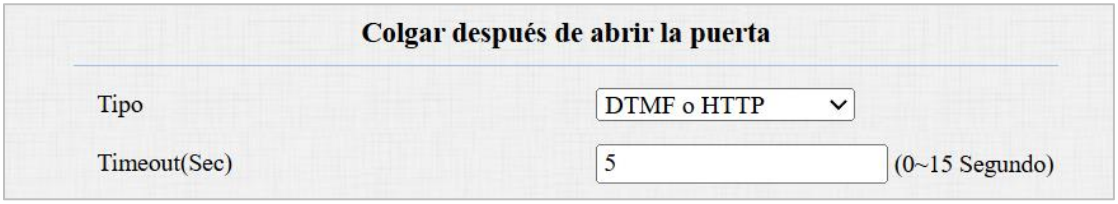
Para configurarla, vaya a la interfaz web Sistema > Mantenimiento > Llamada web.

- Llamada Web (Listo): Introduzca el número IP/SIP de destino y seleccione la cuenta a marcar.

Colgar Después de Abrir la Puerta

Esta función finaliza automáticamente la llamada una vez que se abre la puerta, lo que permite recibir llamadas posteriores sin problemas.

Para configurarla, vaya a la interfaz Videoportero > Función de Llamada > Colgar después de abrir la puerta.



- Tipo: Especifica el método de desbloqueo de la puerta. Si se utiliza este método específico para desbloquear la puerta durante una llamada, el portero automático finalizará la llamada cuando se alcance el tiempo de colgado preestablecido.
- Tiempo de espera(Seg): Especifique el límite de tiempo de colgado. El portero automático finalizará la llamada cuando se alcance el tiempo específico después de abrir la puerta.

Acciones Activadas por Llamada

Puede configurar acciones que se activan cuando el dispositivo está realizando una llamada en la interfaz Videoportero > Básico > Evento de llamada.

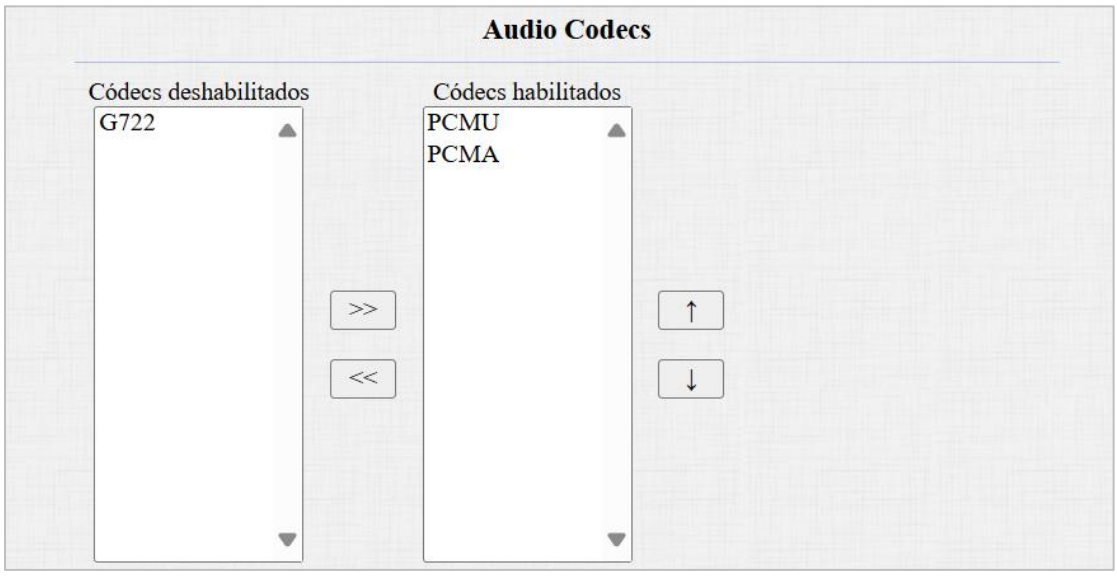
- Acción a ejecutar:
  - FTP: Enviar una captura de pantalla al servidor FTP preconfigurado.
  - Correo electrónico: Envía una captura de pantalla a la Dirección de Correo Electrónico preconfigurada.
  - HTTP: Cuando se activa, el mensaje HTTP puede ser capturado y mostrado en los paquetes correspondientes. Para utilizar esta función, active el servidor HTTP e introduzca el contenido del mensaje en la casilla designada a continuación.
- HTTP URL HTTP: Introduzca el mensaje HTTP si selecciona HTTP como acción a ejecutar. El formato es http://HTTP IP del servidor/Contenido del mensaje.

Configuración del Códec de Audio y Vídeo

Codec de Audio

El portero automático admite tres tipos de códec (PCMU, PCMA y G722) para codificar y descodificar los datos de audio durante la sesión de llamada. Cada códec varía en términos de calidad de sonido. Puede seleccionar el códec específico con diferentes anchos de banda y frecuencias de muestreo de forma flexible según el entorno de red real.

Configúrelo en la interfaz Cuenta > Avanzado > Códecs de audio.



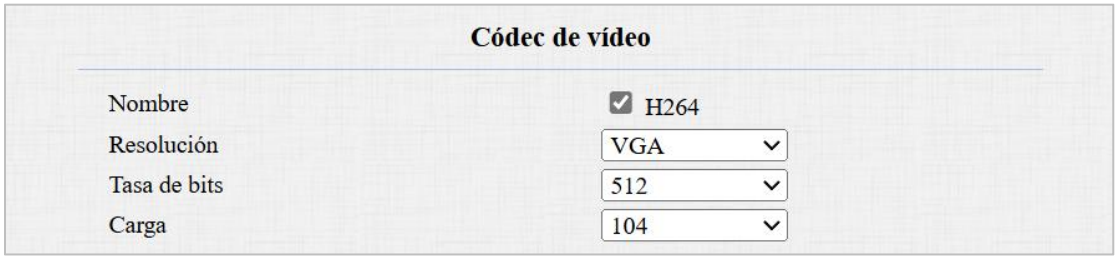
Consulte a continuación el consumo de ancho de banda y la frecuencia de muestreo de los tres tipos de códec:

Tipo de Códec	Consumo de Banda Ancha	Tasa de Muestreo
PCMA	64 kbit/s	8kHZ
PCMU	64 kbit/s	8kHZ
G722	64 kbit/s	16kHZ

Códec de Vídeo

El videoportero soporta el códec H264 que proporciona una mejor calidad de vídeo a una tasa de bits mucho más baja con diferente calidad de vídeo y carga útil.

Para configurar el códec de vídeo, vaya a la interfaz Cuenta > Avanzado > Códec de Vídeo.



- Nombre: Marque esta casilla para activar el formato de códec de vídeo

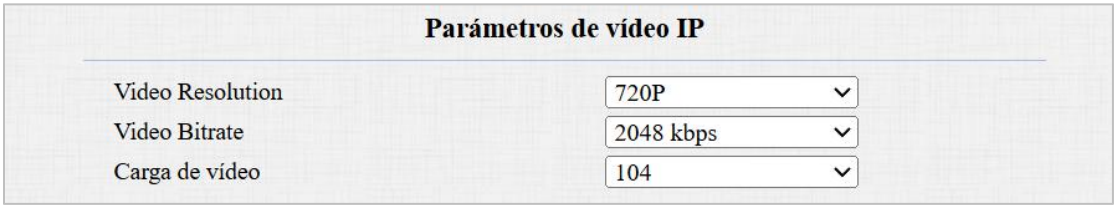
H264 para el flujo de vídeo del portero automático.

- Resolución: Seleccione la resolución entre las opciones proporcionadas. La resolución del código por defecto es VGA.
- Tasa de Bits: La tasa de bits del flujo de vídeo oscila entre 128 y 2048 kbps. Cuanto mayor sea la tasa de bits, más datos se transmitirán por segundo y más nítido será el vídeo. La tasa de bits por defecto del código es 512.
- Carga útil: La carga útil oscila entre 90 y 119 para configurar los archivos de configuración de audio/vídeo. El valor por defecto es 104.

Códec de Vídeo para Llamadas IP Directas

Puede seleccionar la calidad de vídeo de la llamada IP seleccionando la resolución de códec adecuada según las condiciones de la red.

Configúrelo en la interfaz Intercomunicador > Función de llamada > Parámetros de vídeo IP.



- Resolución de vídeo: Selecciona la resolución entre las opciones proporcionadas.
- Tasa de bits de vídeo: La tasa de bits del flujo de vídeo oscila entre 64 y 2048 kbps. La tasa de bits por defecto es 2048.
- Carga útil de vídeo: La carga útil oscila entre 90 y 119 para configurar los archivos de configuración de audio/vídeo. El valor predeterminado es 104.

Configuración de la Lista de Permisos de Acceso

El portero automático puede almacenar hasta 1000 contactos, dando permiso

de acceso a los monitores interiores u otros dispositivos.

Puede buscar, crear, editar y eliminar los contactos de la lista de permitidos.

Configúrela en la interfaz Directorio > Configuración del directorio.

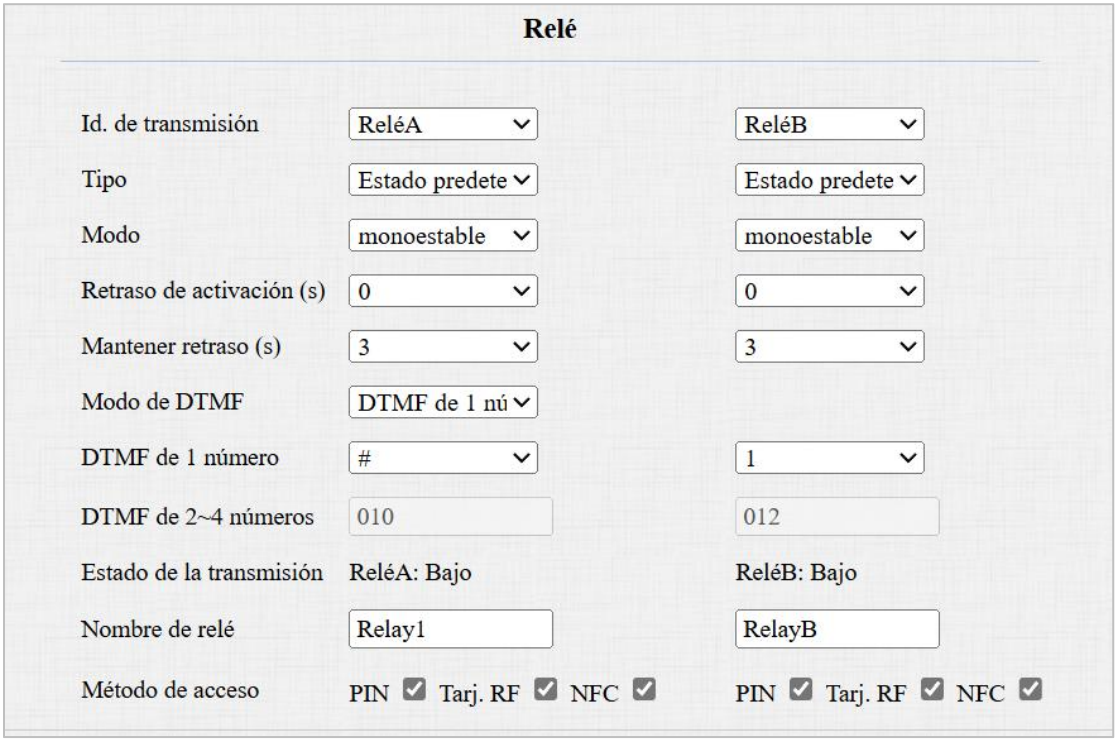
- Nombre: Nombre del contacto.
- Número de teléfono: El número de teléfono del contacto. Admite direcciones IP y números SIP.
- Cuenta: Seleccione la cuenta para recibir la llamada del contacto.
- Piso: Especifique la(s) planta(s) accesible(s) al contacto a través del ascensor.

Ajuste del Relé

Relé Local

Un relé local es una unidad externa que se encuentra físicamente cerca y directamente conectada al videoportero. Permite que el sistema active acciones, como desbloquear una puerta, basándose en la entrada o autorización del usuario.

Puede configurar el(los) interruptor(es) de relé y DTMF para el acceso a la puerta en la interfaz web Control de acceso > Relé.



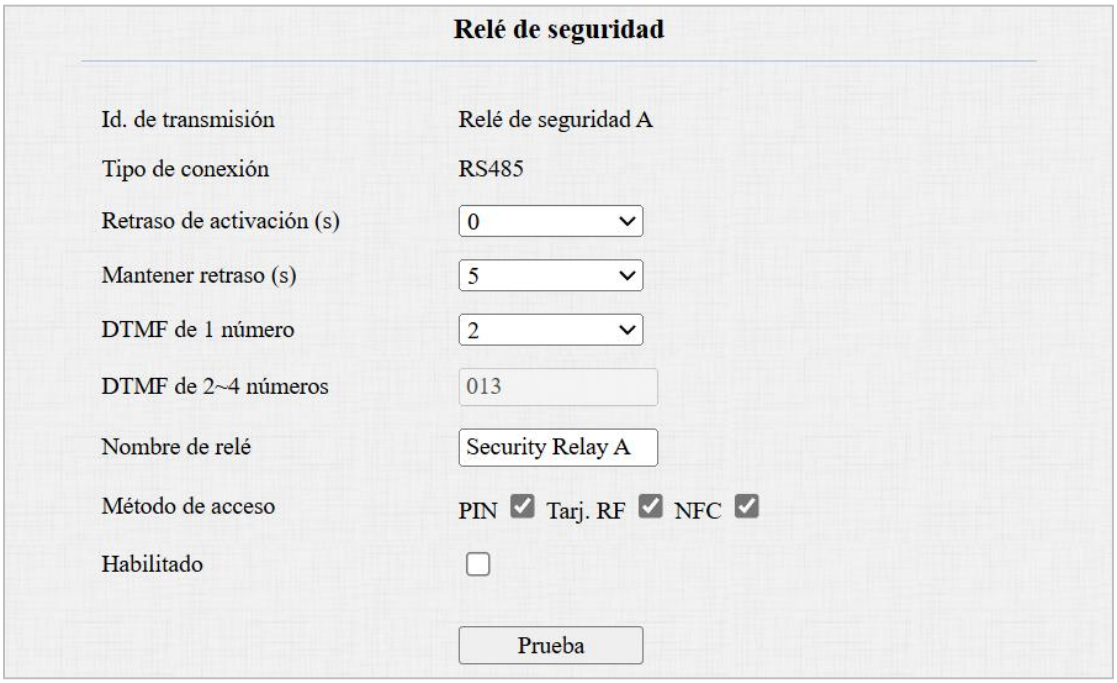
- Tipo de Relé: Determina la interpretación del Estado del Relé respecto al estado de la puerta:
  - Estado predeterminado: Un estado «Bajo» en el campo Estado Relé indica que la puerta está cerrada, mientras que «Alto» indica que está abierta.
  - Estado invertido: Un estado «Bajo» en el campo Estado Relé indica que la puerta está abierta, mientras que «Alto» indica que está cerrada.

- Modo: Especifique las condiciones para restablecer automáticamente el estado del relé.
  - Modo: Especifique las condiciones para restablecer automáticamente el estado del relé.
  - Biestable: El estado del relé se restablece al disparar de nuevo el relé.
- Retraso de Activación (Seg): Ajuste el tiempo de retardo antes de que se active el relé. Por ejemplo, si se ajusta a 5 segundos, el relé se activa 5 segundos después de pulsar el botón de Desbloqueo.
- Mantener retraso (Seg): Determina cuánto tiempo permanece activado el relé. Por ejemplo, si se ajusta a 5 segundos, el relé permanece abierto durante 5 segundos antes de cerrarse.
- Modo DTMF: Defina los dígitos del código DTMF.
- DTMF de 1 Dígito: Defina el código DTMF de 1 dígito dentro del rango (0-9 y *,#) cuando el Modo DTMF esté ajustado a 1 dígito.
- DTMF de 2~4 Dígitos: Defina el código DTMF en función del número de dígitos seleccionados en el Modo DTMF.
- Estado del Relé: Indica los estados del relé, normalmente abierto y cerrado. Por defecto, muestra bajo para normalmente cerrado(NC) y alto para normalmente abierto(NO).
- Nombre del Relé: Asigna un nombre distinto para su identificación.
- Método de Acceso: Marque el método o métodos para activar el relé.

Relé de Seguridad

El Relé de Seguridad, conocido como Akuvox SR01, es un producto diseñado para reforzar la seguridad de los accesos impidiendo intentos de entrada forzada no autorizados. Instalado en el interior de la puerta, gobierna directamente el mecanismo de apertura de la puerta, garantizando que la puerta permanezca segura incluso en caso de daños en el dispositivo.

Para configurar el relé de seguridad, vaya a la interfaz web Control de acceso > Relé de seguridad.



- Tipo de Conexión: El tipo de Conexión por defecto es RS485.
- Retraso de Activación (Seg): Ajuste el tiempo de retardo antes de que se dispare el relé. Por ejemplo, si se ajusta a 5 segundos, el relé se activa 5 segundos después de pulsar el botón de Desbloqueo.
- Retraso de Retención (Seg): Determina el tiempo que el relé permanece activado. Por ejemplo, si se ajusta a 5 segundos, el relé permanece abierto durante 5 segundos antes de cerrarse.
- DTMF de 1 Dígito: Defina el código DTMF de 1 dígito dentro del rango (0-9 y *,#) cuando el Modo DTMF en la sección Relé anterior esté ajustado a 1 Dígito.
- DTMF de 2~4 Dígitos: Defina el código DTMF basado en el número de dígitos seleccionados en el Modo DTMF.
- Nombre del Relé: Asigne un nombre al relé de seguridad. El nombre se

puede mostrar en los registros de apertura de puertas. Al conectarse a SmartPlus Cloud, el servidor Cloud asignará automáticamente el nombre del relé.

- Método de acceso: Marque el método o métodos para activar el relé.
- Prueba: Haga clic en para enviar la señal al SR01. Cuando el portero automático y el SR01 estén emparejados, haga clic en Prueba para finalizar el emparejamiento.

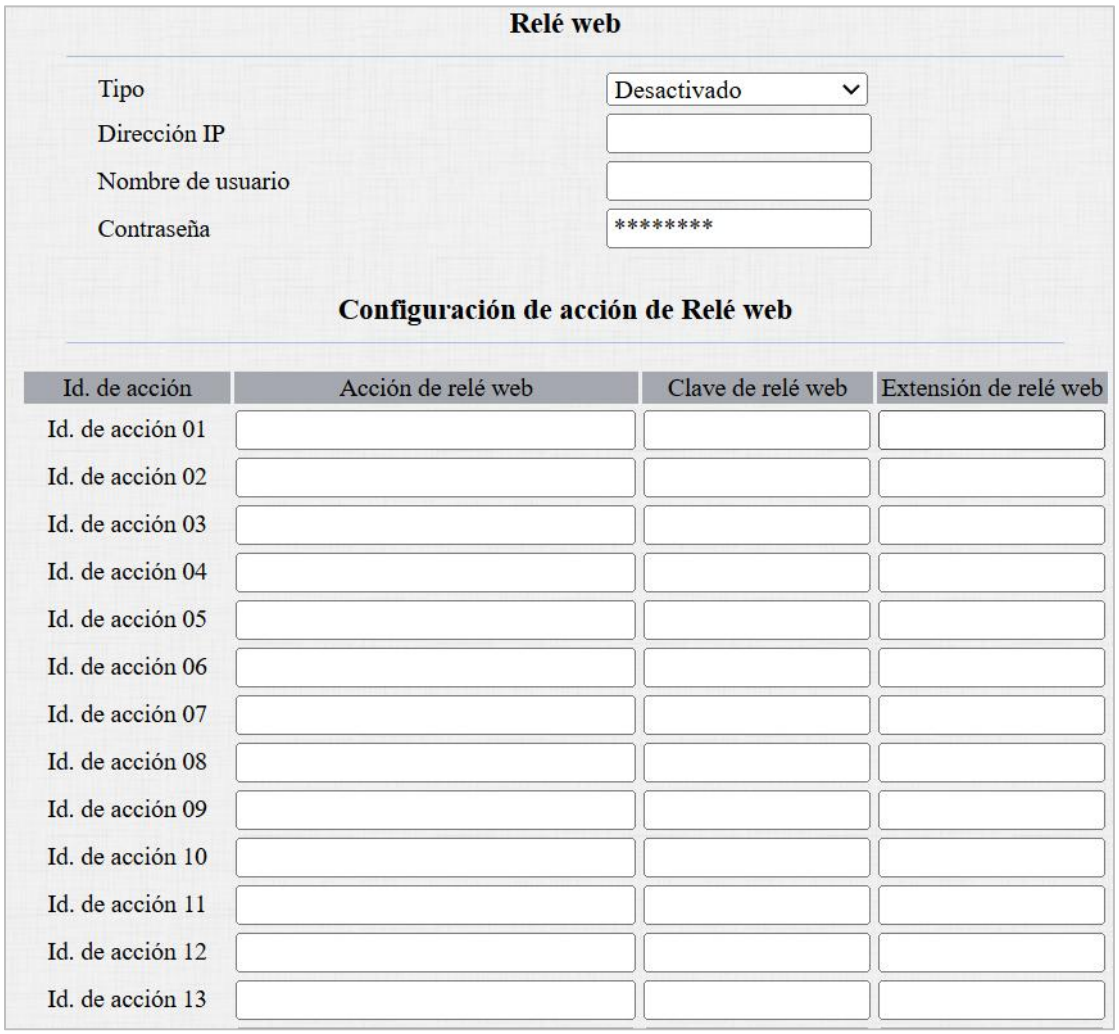
Nota:

Cuando conecte el dispositivo a un SR01 a través de RS485, deberá seleccionar el modo RS485 como Otros en la interfaz Dispositivo > RS485.

Relé Web

Un relé web tiene un servidor web incorporado y puede controlarse a través de Internet o de una red local. El dispositivo puede utilizar un relé web para controlar un relé local o un relé remoto en otro lugar de la red.

Para configurar un relé web, vaya a la Interfaz Control de Acceso > Relé Web.



- Tipo:
  - Deshabilitado: Sólo activar el relé local.
  - Sólo Relé Web: Sólo activar el relé web.
  - Tanto relé local como relé web: Activa tanto el relé local como el relé web. Normalmente, el relé local se activa primero, seguido del relé web para ejecutar sus acciones preconfiguradas.
- Dirección IP: La dirección IP del relé web proporcionada por el fabricante del relé web.
- Nombre de usuario: El nombre de usuario proporcionado por el fabricante de la retransmisión web.
- Contraseña: La clave de autenticación proporcionada por el fabricante para la retransmisión web. La autenticación se realiza a través de HTTP. Dejar el campo Contraseña en blanco indica que no se utiliza la autenticación HTTP. Puede definir la contraseña utilizando HTTP GET en

el campo Acción de retransmisión web.

- Acción de relé web: Las URL proporcionadas por el fabricante para varias acciones, con hasta 50 comandos.

Nota:

➢ Si la URL incluye todo el contenido HTTP (por ejemplo, http://admin:admin@192.168.1.2/state.xml?relayState=2), no se basa en la dirección IP introducida anteriormente. Sin embargo, si la URL es más simple (por ejemplo, «state.xml?relayState=2»), el relé utiliza la dirección IP introducida.

- Clave de Relé Web: Determina los métodos para activar el relé web en función de si se rellena el código DTMF.

  - Rellenando con el código DTMF configurado restringe la activación a pasar la tarjeta y DTMF.

  - Si se deja en blanco, se activan todos los métodos de apertura de puerta.

- Extensión de Relé Web: Especifique el dispositivo de videoportero y los métodos que puede utilizar para activar el relé web durante las llamadas.

  - Cuando se especifica la IP/SIP de un videoportero, sólo ese dispositivo puede activar la retransmisión web (excepto mediante el paso de tarjeta o DTMF) durante las llamadas.

  - Si se deja en blanco, todos los dispositivos pueden activar el relé durante las llamadas.

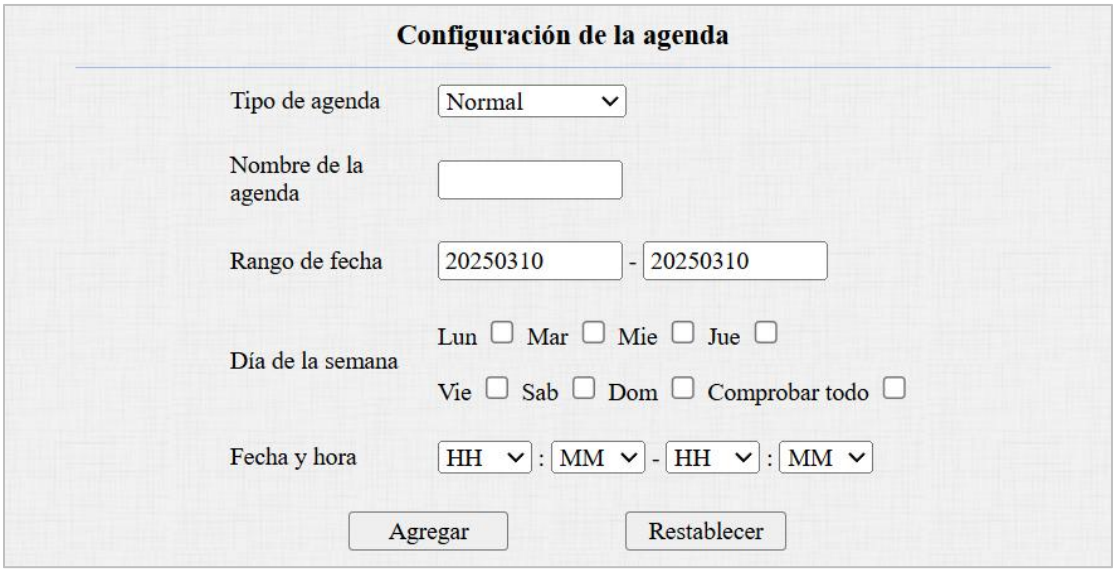
Gestión del Horario de Control de Acceso

Esta función le permite decidir quién puede abrir la puerta y cuándo. Se aplica tanto a individuos como a grupos, garantizando que los usuarios dentro del horario sólo puedan abrir la puerta utilizando el método autorizado durante los periodos de tiempo designados.

Crear un Horario de Acceso

Puede crear horarios de acceso a la puerta para periodos de tiempo diarios, semanales o personalizados.

Configúrelo en la interfaz web Configuración > Age da.



- Tipo de Agenda:
  - Normal: Configura la programación en función del mes, la semana y el día. Se utiliza para un horario de periodo largo.
  - Semanal: Establece el horario basado en la semana.
  - Diario: Establece el horario basado en las 24 horas del día.
- Nombre: Nombre de la agenda.

Importar y Exportar Horarios de Acceso

Además de crear un horario de acceso a la puerta por separado, también puede importar o exportar cómodamente los horarios para maximizar la eficacia de la gestión del horario de acceso a la puerta.

Para configurarlo, vaya a la interfaz web Configuración > Horario.

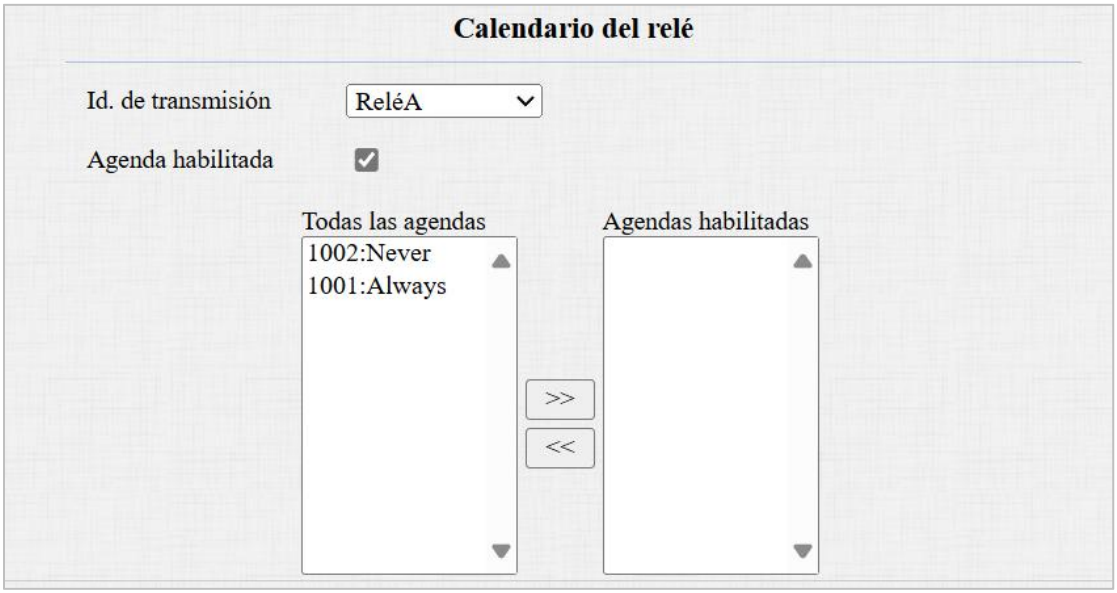
Nota:

El archivo importado/exportado está en formato .xml.

Calendario de Relés

La programación de relés le permite configurar un relé específico para que se abra siempre a una hora determinada. Esto es útil para situaciones como mantener la puerta abierta después de la escuela o mantener la puerta abierta durante las horas de trabajo.

Para configurarlo, vaya a la interfaz Control de Acceso > Relé > Horario de Relé.



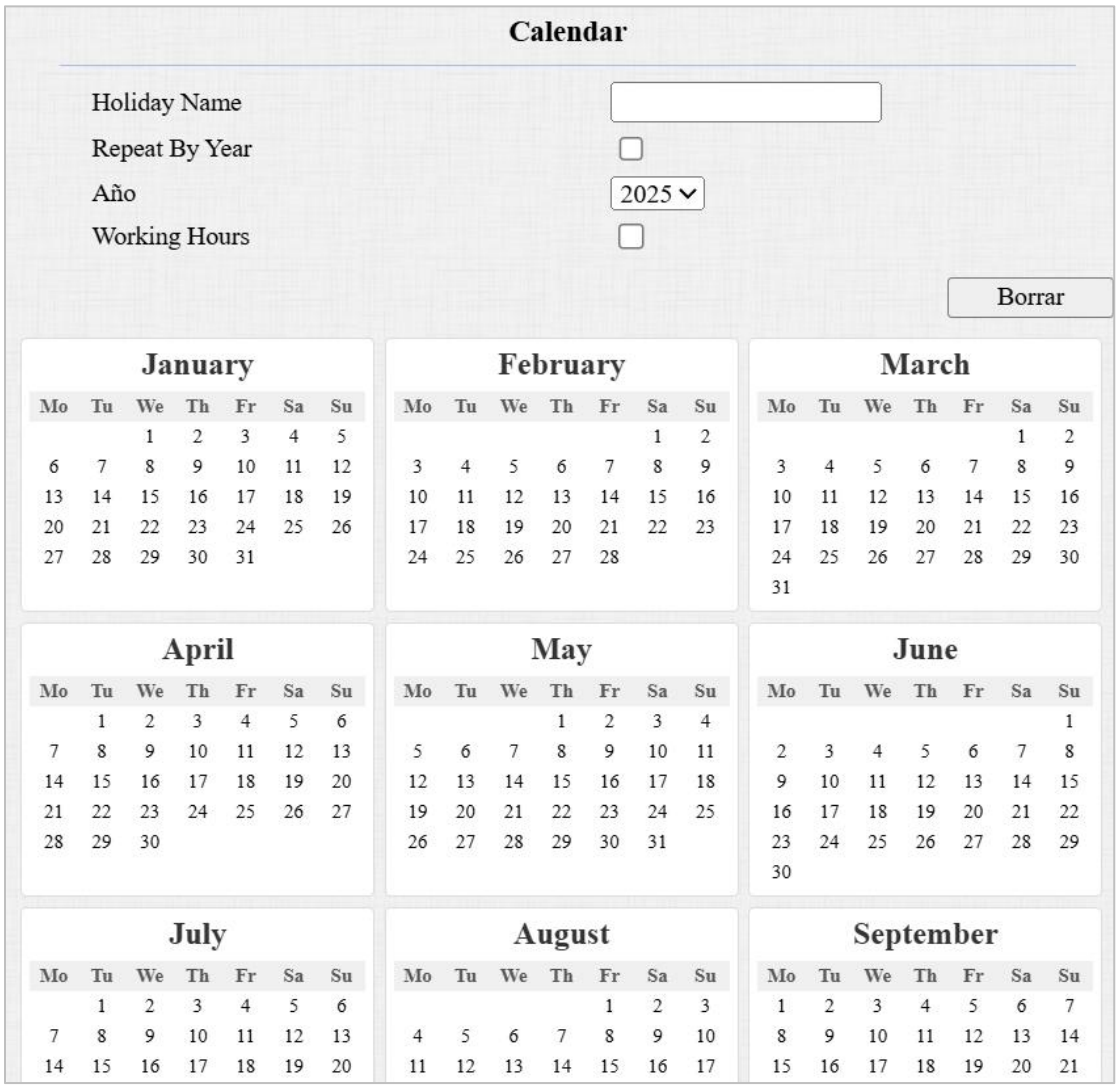
- ID de relé: Aplica el horario al relé específico.
- Horario Activado: Asigna horarios particulares de acceso a la puerta al relé elegido. Simplemente muévalos a la casilla Horarios Habilitados.

Para obtener instrucciones sobre la creación de horarios, consulte la sección Crear Horario de Acceso de Puerta.

Calendario de Días Festivos

Puede definir los días festivos en los que los usuarios no pueden abrir puertas para mejorar la seguridad del control de acceso. También puede establecer el Horario Laboral para permitir que los usuarios autorizados abran las puertas.

Configúrelo en la interfaz **Configuración > Día Festivo**. Haga clic en **+Agregar**.



- Nombre del día festivo: Introduzca el nombre del día festivo.
- Repetir por año: Repite la programación cada año.
- Año: Establezca el año y la fecha de las vacaciones.
- Horario Laboral: Cuando está activado, especifique el horario en el que los usuarios autorizados pueden abrir las puertas.

Importar/Exportar Calendario de Vacaciones

Puede importar o exportar programas de vacaciones para una configuración rápida en la interfaz Configuración > Vacaciones > Importar/Exportar vacaciones.

El formato de archivo de importación/exportación es .xml.

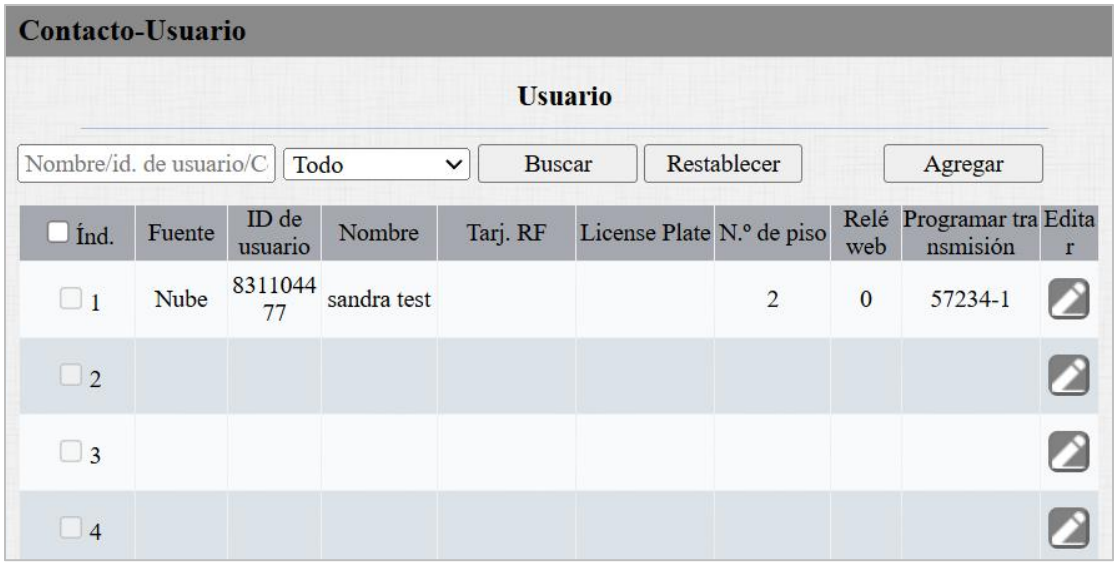
Configuración de Apertura de Puerta

Desbloqueo mediante tarjetas RF

La tarjeta RF debe asignarse a un usuario concreto para la apertura de la puerta.

Al añadir un usuario, también puede personalizar ajustes como definir el horario de acceso a la puerta para determinar cuándo es válido el código y especificar qué relé abrir.

Para añadir un usuario, vaya a Directorio > Usuario y haga clic en Añadir.

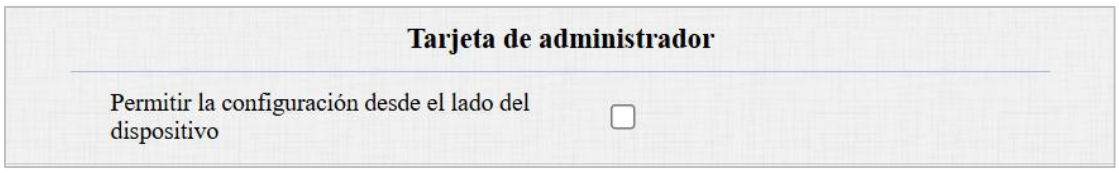


- ID de usuario: El número de identificación único asignado al usuario.
- Nombre: El nombre de este usuario.
- Rol: Define al usuario como Usuario General o Administrador. La tarjeta Admin puede utilizarse para añadir una tarjeta de usuario. Consulte Configuración de tarjetas de administrador y tarjetas de usuario para obtener información detallada sobre la configuración.
- Código: El número de tarjeta que lee el lector de tarjetas.

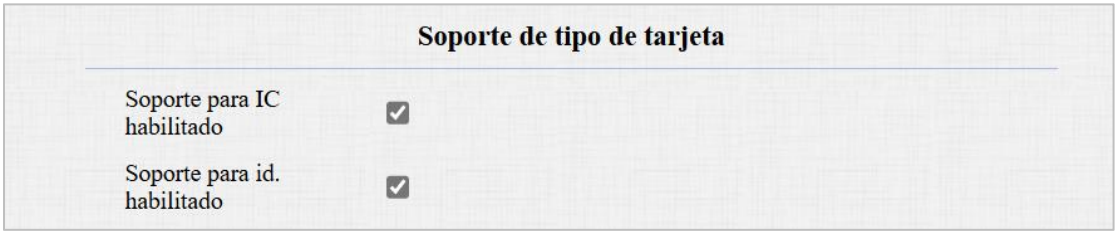
Nota:

- Cada usuario puede tener un máximo de 5 tarjetas añadidas.
- El dispositivo permite añadir 5.000 usuarios.
- Las tarjetas RF que operan en frecuencias de 125 KHz y 13,56 MHz son compatibles con el portero automático para el acceso.

Puede activar o desactivar el uso de la Tarjeta de Administrador en la interfaz Control de acceso > Configuración de tarjeta > Tarjeta de Administrador.



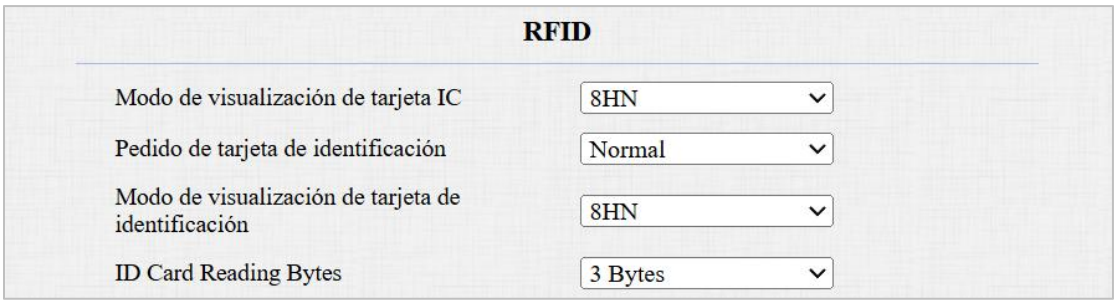
Puede activar o desactivar la función de tarjeta IC/ID en la interfaz Control de acceso > Configuración de tarjeta > Soporte de tipo de tarjeta.



Formato de Código de Tarjeta RF

Para integrar el acceso a la puerta mediante tarjeta RF con el sistema de intercomunicación de terceros, debe hacer coincidir el formato de código de la tarjeta RF con el utilizado por el sistema de terceros.

Para configurarlo, vaya a Control de acceso > Configuración de tarjeta > Interfaz RFID.

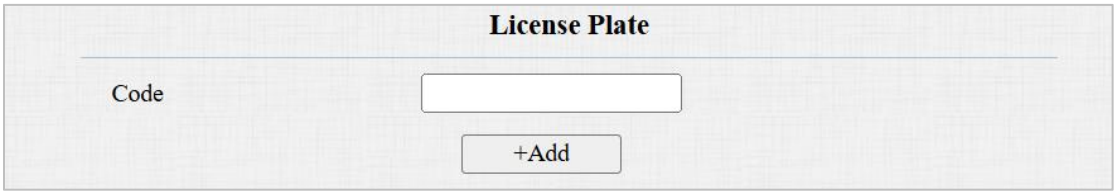


- Modo de visualización de tarjeta IC/ID: Configure el formato del número de tarjeta entre las opciones proporcionadas. El formato por defecto en el dispositivo es 8HN.
- Orden de la tarjeta de identificación: Seleccione el orden de lectura del número de tarjeta de identificación Normal o Invertido.
- Bytes de lectura de tarjeta ID: Seleccione el número de bytes leídos de la tarjeta de identificación.

Desbloqueo por Matrícula

El dispositivo se puede utilizar con el lector de control de acceso Akuvox ACR-CRP12 para abrir la puerta del garaje. Haga clic aquí para ver la configuración detallada de la función.

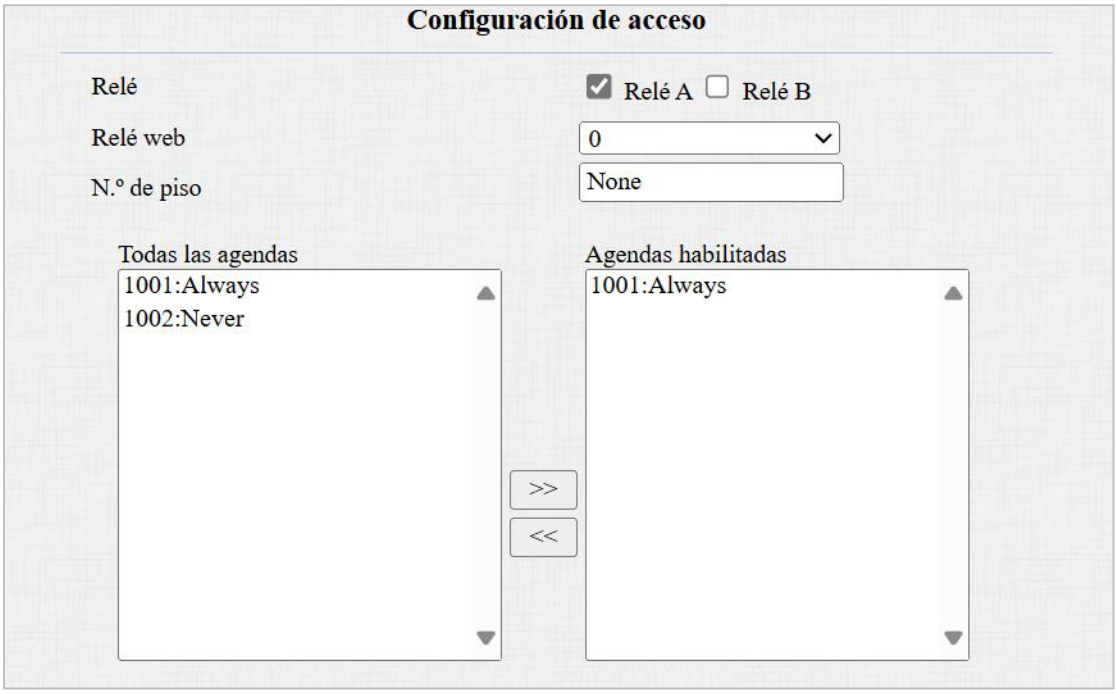
Para asignar la matrícula a un usuario, busque la parte Matrícula en la interfaz Directorio > Usuario > +Añadir.



- **Código**: La información de la matrícula que lee el dispositivo. Un usuario puede tener 5 matrículas como máximo.

Configuración de Acceso

Una vez introducidos los datos de usuario y el código de la tarjeta RF, puede desplazarse hasta la Configuración de acceso y configurar el control de acceso de la tarjeta RF.



- Relé: El relé a desbloquear mediante los métodos de apertura de puerta debe ser asignado al usuario.
- Relé Web: Especifique el ID de los comandos de acción del relé web que ha configurado en la interfaz del relé web. Un valor predeterminado de 0

indica que el relé web no se activará.

- Nº de planta: Especifique la(s) planta(s) a la(s) que puede acceder el usuario a través del ascensor.
- Horario: Conceda al usuario acceso para abrir las puertas designadas durante periodos preestablecidos reubicando el(los) horario(s) deseado(s) de la casilla izquierda a la derecha. Además de los horarios personalizados, existen 2 opciones predeterminadas:
  - Siempre: Permite la apertura de puertas sin limitaciones en el recuento de puertas abiertas durante el periodo válido.
  - Nunca: Prohíbe la apertura de puertas.

Importar/ Exportar Datos de Usuario

Después de añadir usuarios, puede exportar los datos de usuario e importarlos a otro videoportero para una gestión rápida.

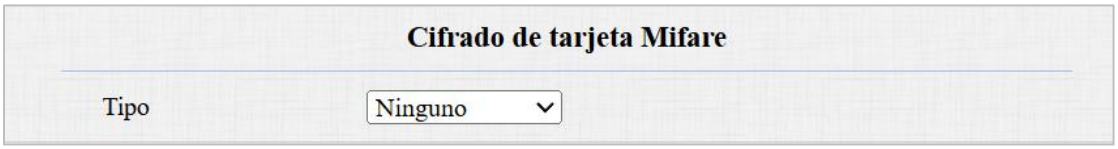
En la interfaz Directorio > Usuario, desplácese hasta la sección Importar/Exportar usuario. Si el archivo está cifrado, introduzca la contraseña en la casilla Clave AES para importación.

Cifrado de Tarjetas Mifare

El dispositivo puede cifrar tarjetas Mifare para mayor seguridad. Cuando esta función está activada, lee los datos de los sectores y bloques designados de las tarjetas, no el UID.

Para configurar la tarjeta Mifare, vaya a la interfaz web Control de acceso >

Configuración de tarjeta Mifare.

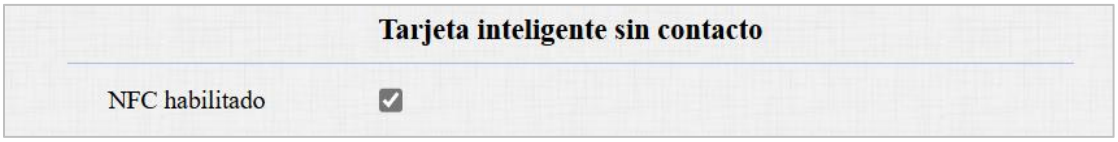


- Tipo: Hay cuatro opciones: Ninguno, Clásico, Plus y DESfire.
  - Clásico:
    - Sector/Bloque: Especifica la ubicación donde se almacenan los datos encriptados de la tarjeta. Una tarjeta Mifare tiene 16 sectores (numerados del 0 al 15), y cada sector tiene 4 bloques (numerados del 0 al 3).
    - Clave de Bloque: Establece una contraseña para acceder a los datos almacenados en el sector/bloque predefinido.
  - Plus: Hay tres opciones de bloque. El dispositivo puede leer los datos encriptados en SL1 y SL3.
    - Bloque: El número de bloque donde se encuentran los datos encriptados.
    - SL3: El número de clave dentro de 32 bits.
  - DesFire:
    - ID de la aplicación: Un número hexadecimal de 6 dígitos
    - ID de Archivo: El ID del archivo encriptado de la app, que puede ser un número del 0 al 16.
    - Cifrado: El método de cifrado, ya sea AES o DES.
    - Clave: La clave del archivo.
    - Índice de la clave: El número de índice de la clave, que puede ser un número del 0 al 11.

Desbloqueo por NFC

NFC (“Near Field Communication”) es una forma popular para el acceso a la puerta. Utiliza ondas de radio para la interacción de transmisión de datos. El dispositivo puede ser desbloqueado por NFC. Puede mantener el teléfono móvil más cerca del dispositivo para el acceso a la puerta.

Para configurar NFC, vaya a la interfaz web Control de acceso > Configuración de tarjeta. Habilite la función NFC para la apertura de puertas.



Nota:

- La función NFC no está disponible en iPhones.
- Haga clic aquí para ver los pasos detallados de configuración de la función NFC.

Acciones Activadas al Pasar Tarjetas

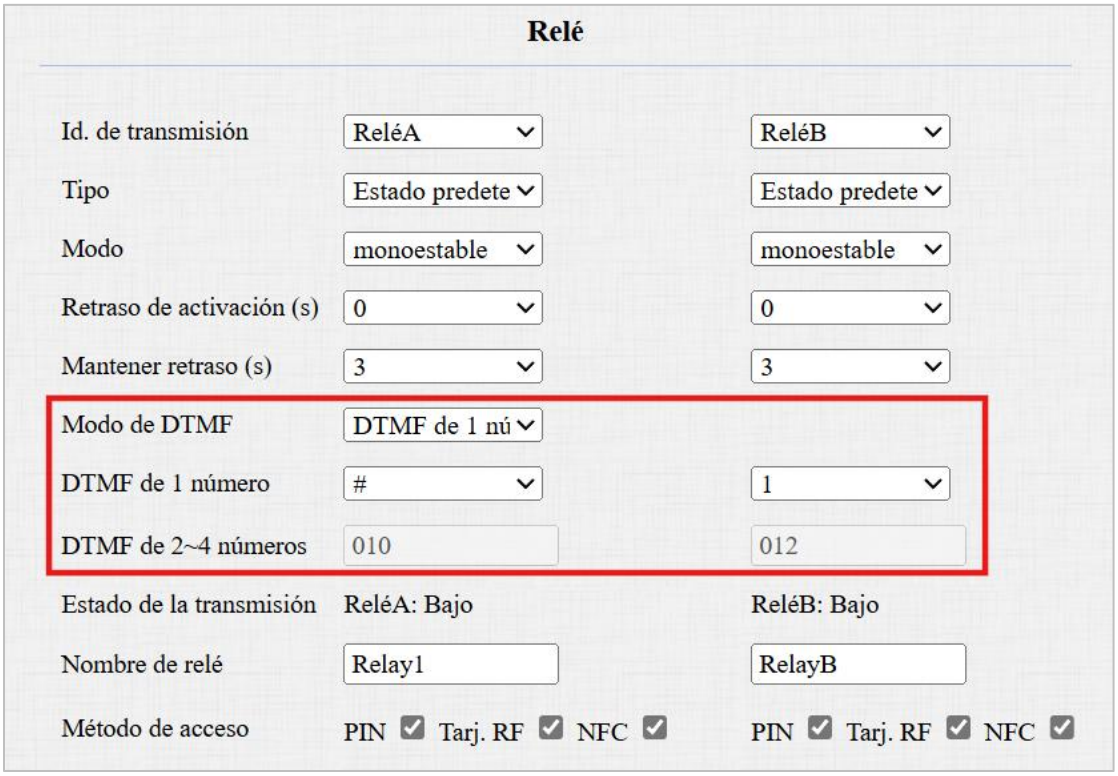
Puede configurar las acciones que se activan al pasar las tarjetas para abrir las puertas en la interfaz Control de acceso > Configuración de tarjeta > Evento de tarjeta.

- Acción a ejecutar:
- FTP: Envía una captura de pantalla al servidor FTP preconfigurado.
- Correo electrónico: Envía una captura de pantalla a la dirección de correo electrónico preconfigurada.
  - HTTP: Cuando se activa, el mensaje HTTP puede ser capturado y mostrado en los paquetes correspondientes. Para utilizar esta función, active el servidor HTTP e introduzca el contenido del mensaje en la casilla designada a continuación.
- URL HTTP: Introduzca el mensaje HTTP si selecciona HTTP como acción a ejecutar. El formato es http://HTTP server's IP/Message content.

Desbloqueo por Código DTMF

La señalización multifrecuencia de doble tono (DTMF) es una forma de enviar señales a través de las líneas telefónicas utilizando diferentes bandas de frecuencia de voz. Los usuarios pueden utilizar la función DTMF para desbloquear la puerta para los visitantes durante una llamada escribiendo el código DTMF en el teclado numérico o pulsando la pestaña de desbloqueo con el código DTMF en la pantalla.

Para configurar los códigos DTMF, vaya a Control de acceso > Relé.



- Modo DTMF: Defina el número de dígitos para el código DTMF.
- DTMF de 1 dígito: Defina el código DTMF de 1 dígito dentro del rango (0-9 y *,#) cuando el Modo DTMF esté configurado en 1 dígito.
- DTMF de 2-4 Dígitos: Defina el código DTMF basado en el número de dígitos seleccionados en el Modo DTMF.

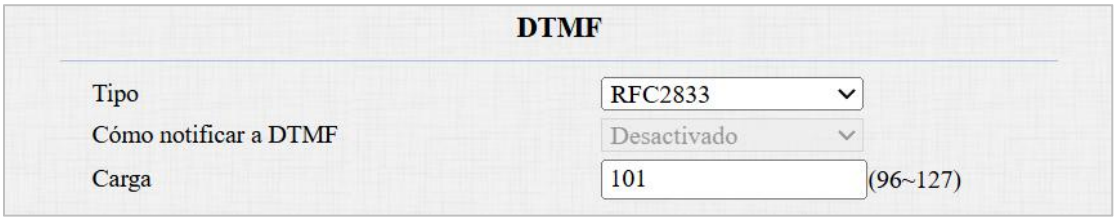
Nota:

Para abrir la puerta con DTMF, los dispositivos de intercomunicación que envían y reciben el comando de desbloqueo deben utilizar el mismo modo y código. De lo contrario, el desbloqueo DTMF puede fallar. Consulte aquí los pasos detallados de configuración DTMF.

Transmisión de Datos DTMF

Para conseguir el acceso a la puerta mediante código DTMF o algunas otras aplicaciones, es necesario configurar correctamente DTMF para establecer una transmisión de datos basada en DTMF entre el portero automático y otros dispositivos de intercomunicación para la integración de terceros.

Para configurar la transmisión de datos DTMF, vaya a la interfaz web Cuenta > Avanzado > DTMF.



- Tipo: Seleccione entre las opciones disponibles en función del tipo de transmisión DTMF específico del dispositivo de terceros para recibir los datos de la señal.
- Cómo notificar DTMF: Seleccione Desactivado, DTMF, DTMF-Relay o Teléfono-Evento según el tipo específico adoptado por el dispositivo de terceros. Sólo es necesario configurarlo cuando el dispositivo de terceros con el que se va a emparejar adopta el modo Info.
- Carga útil: Configure la carga útil según la carga útil de transmisión de datos específica acordada entre el emisor y el receptor durante la transmisión de datos.

Lista de Permitidos - DTMF

Para asegurar el acceso a la puerta mediante códigos DTMF, puede configurar la lista de permitidos para DTMF en la web del dispositivo Control de acceso > Relé > Abrir Relé vía DTMF para que sólo los números de llamada que haya designado en el portero automático puedan utilizar el código DTMF para acceder a la puerta.

- “Assigned The Authority For”: Especifique los contactos autorizados para abrir puertas mediante DTMF:

  - Ninguno: Ningún número puede desbloquear puertas mediante DTMF.

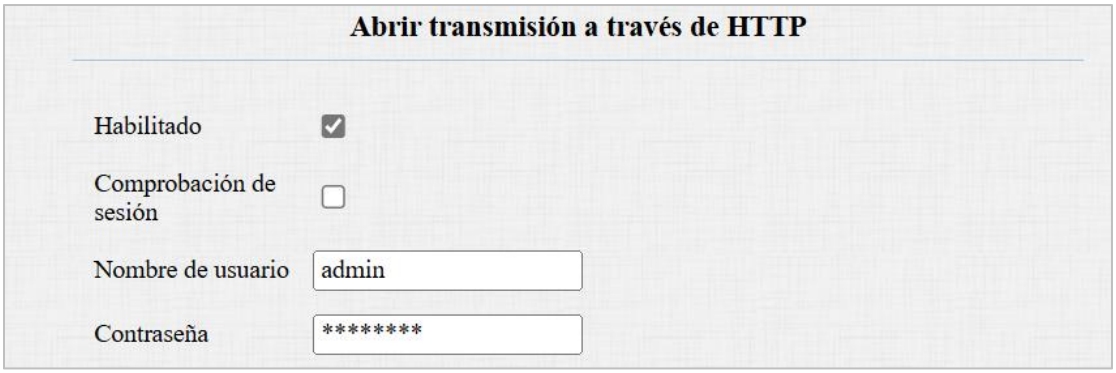
  - Sólo Lista Contactos: Sólo los números añadidos a la lista de contactos pueden abrir mediante DTMF.

  - Todos los números: Cualquier número puede desbloquear mediante DTMF.

Desbloqueo por Comando HTTP

Puede desbloquear la puerta de forma remota sin acercarse físicamente al dispositivo para la entrada de la puerta escribiendo el comando HTTP creado (URL) en el navegador web para activar el relé cuando no esté disponible junto a la puerta para la entrada de la puerta.

Para configurarlo, vaya a la interfaz web Control de acceso > Relé > Abrir transmisión a través de HTTP.



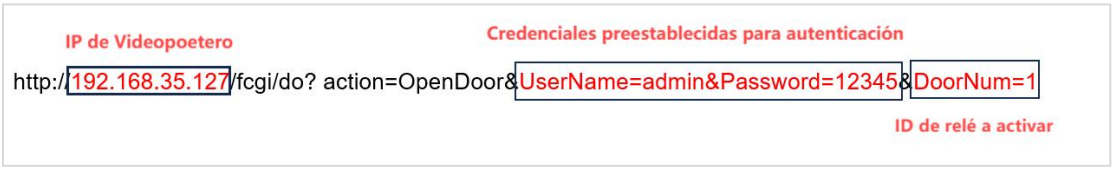
- Comprobación de Sesión: de sesión: Cuando está activado, el desbloqueo HTTP requiere iniciar sesión en la interfaz web del dispositivo. De lo contrario, la apertura puede fallar.
- Nombre de usuario: Establezca un nombre de usuario para la

autenticación en las URL de comandos HTTP.

- Contraseña: Establezca una contraseña para la autenticación en las URL de comandos HTTP.

Consejo:

Este es un ejemplo de URL de comando HTTP:



Nota:

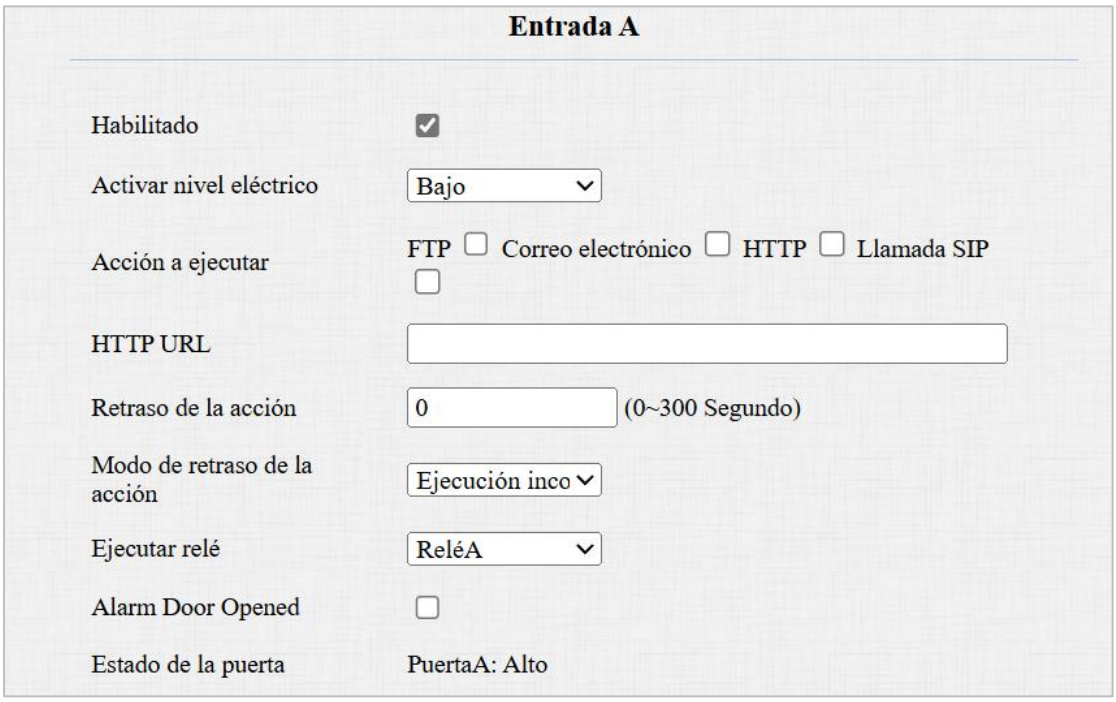
El formato HTTP para la activación del relé varía en función de si está activado el modo de alta seguridad del portero automático. Consulte esta guía práctica para obtener más información: Abrir la puerta mediante comando HTTP.

Desbloqueo con el Botón de Salida

Cuando los usuarios necesiten abrir la puerta desde el interior pulsando el botón Salir, deberá configurar el terminal de entrada que coincida con el botón Salir para activar el relé para el acceso a la puerta.

Pulse aquí para ver el vídeo de instrucciones.

Configúrelo en la interfaz Control de acceso > Entrada.



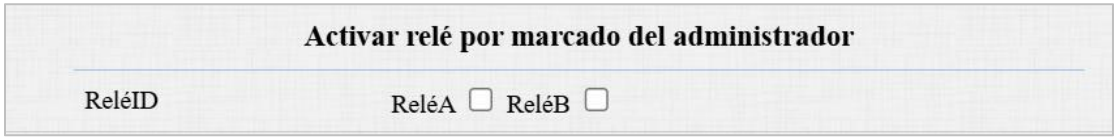
- Habilitado: Para utilizar una interfaz de entrada específica.
- Activar Nivel Eléctrico: Configura la interfaz de entrada para que se dispare a nivel eléctrico bajo o alto.
- Acción a Ejecutar: Establezca las acciones deseadas que se producen cuando se dispara la interfaz de entrada específica.
  - FTP: Envía una captura de pantalla al servidor FTP preconfigurado.
  - Correo electrónico: Envía una captura de pantalla a la dirección de correo electrónico preconfigurada.
  - Llamada SIP: Llama al número preconfigurado al activarse.
  - HTTP: Cuando se activa, el mensaje HTTP puede ser capturado y mostrado en los paquetes correspondientes. Para utilizar esta función, active HTTP e introduzca la URL.
- URL HTTP: Introduzca el mensaje HTTP si selecciona HTTP como acción a ejecutar. El formato es http://HTTP del servidor IP/Contenido del mensaje.
- Retraso de la acción: Especifique si el relé puede activarse en cualquier momento o sólo dentro de un periodo programado.
- Modo de Retraso de Acción:
  - Ejecución Incondicional: la acción se llevará a cabo cuando se dispare la entrada.

- Ejecutar si la entrada sigue activada: La acción se llevará a cabo cuando la entrada permanezca disparada. Por ejemplo, si la puerta permanece abierta después de disparar la entrada, se enviará una acción como un correo electrónico para notificar al receptor.

- Ejecutar Relé: Especifique el relé que se activará con las acciones.
- "Alarm Door Opened": Si está activada, cuando el tiempo de apertura de la puerta supere un límite, se activará una alarma.
  - Tiempo límite de apertura de puerta: El tiempo límite de apertura de puerta.
- "Break-in intrusion": Activa una alarma cuando la puerta se abre por la fuerza o ilegalmente. Sólo marcando esta opción se puede desactivar la alarma una vez activada. Pulse aquí para obtener más información sobre esta función.
- Estado de la Puerta: Muestra el estado de la señal de entrada.

Desbloqueo Pulsando el Botón

Puede seleccionar el relé o relés que se van a activar pulsando el botón en la interfaz Videoportero > Básico > Activar relé por marcación del administrador. En el caso del R20B, puede comprobar el/los relé(s) que se abrirán pulsando el/los botón(es) pulsador(es) deseado(s).

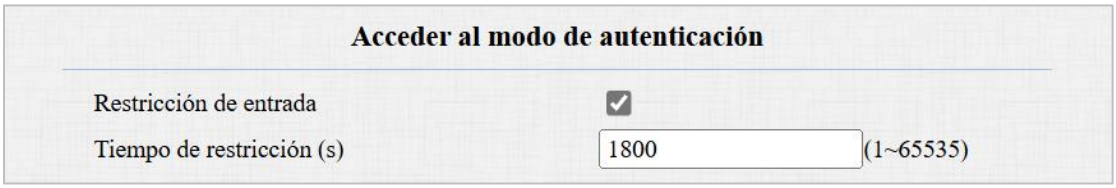


Restricción de Entrada

Puede limitar que los usuarios abran la puerta repetidamente durante un breve periodo de tiempo.

Para configurarlo, vaya a la interfaz Control de acceso > Relé > Modo de

autenticación de acceso.



- Tiempo de restricción(Seg): Especifique el tiempo dentro del cual el mismo usuario no puede abrir la puerta dos veces. Por ejemplo, si se establece en 1800 segundos, el usuario no podrá volver a abrir la puerta hasta 30 minutos después.

Monitorización e Imagen

MJPEG y RTSP son los principales tipos de flujo de monitorización abordados en este capítulo.

MJPEG, o Motion JPEG, es un formato de compresión de video que utiliza imágenes JPEG para cada cuadro de video. Los dispositivos Akuvox muestran flujos en vivo en la interfaz web y capturan pantallas de monitoreo en formato MJPEG. Los ajustes relacionados con MJPEG determinan la calidad de vídeo y el estado de activación/desactivación de la función de transmisión en directo.

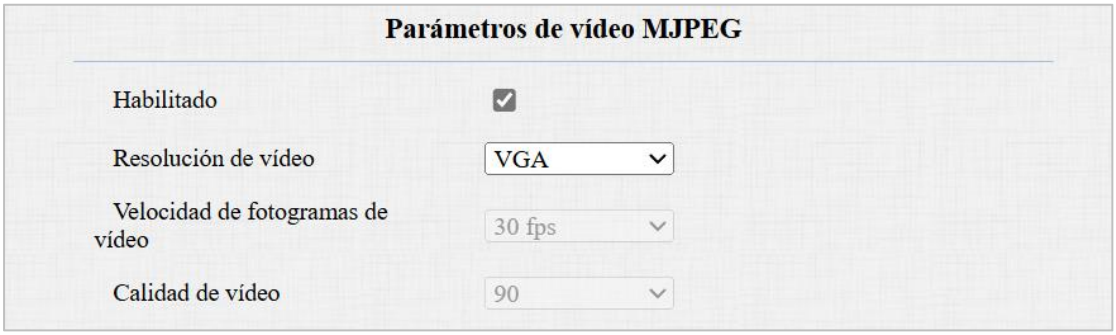
RTSP son las siglas de “Real Time Streaming Protocol”. Se puede utilizar para transmitir vídeo y audio desde cámaras de terceros al dispositivo. Puede añadir el flujo de una cámara añadiendo su URL. El formato URL de los dispositivos Akuvox es rtsp://IP del dispositivo/live/ch00_0

ONVIF es un Foro Abierto de Interfaces de Vídeo en Red. Permite al dispositivo escanear y descubrir cámaras o dispositivos de intercomunicación con funciones ONVIF activadas. Las secuencias en directo obtenidas a través de ONVIF están esencialmente en formato RTSP.

Captura de Imagen MJPEG

Puede tomar una imagen de monitorización o comprobar el vídeo de monitorización en formato MJPEG con el dispositivo. Para ver el flujo de vídeo, debe activar la función de vídeo MJPEG y elegir la calidad de imagen.

Para configurarla, vaya a la interfaz Vigilancia > RTSP.



- Resolución de vídeo: Especifica la resolución de la imagen, variando desde la más baja CIF(352×288 píxeles) hasta la más alta 1080P(1920x1080 píxeles).
- Frecuencia de vídeo: Fotogramas por segundo, se refiere a cuántos fotogramas se muestran en un segundo de vídeo. La tasa de fotogramas por defecto es de 30fps.
- Calidad de vídeo: La tasa de bits de vídeo oscila entre 50 y 90.

Puede configurar la autorización MJPEG en la sección RTSP Básico. Está activada por defecto.

- Autorización MJPEG Activada: Una vez habilitada, para acceder a la

imagen o vídeo en tiempo real del portero automático introduciendo la URL en el navegador es necesario verificar el Modo de autenticación, el Nombre de usuario y la Contraseña.

Consejo:

- Para ver un flujo dinámico, utilice la URL http://device_IP:8080/video.cgi.
- Para capturar una pantalla, utilice las siguientes URL, cuyos formatos de imagen varían en consecuencia:
  - http://device_IP:8080/picture.cgi
  - http://device_IP:8080/picture.jpg
  - http://device_IP:8080/jpeg.cgi
- Por ejemplo, si desea capturar la imagen en formato jpg del portero automático con la dirección IP 192.168.1.104, puede introducir http://192.168.1.104:8080/picture.jpg en el navegador web.

Supervisión de Flujos RTSP

Puede utilizar RTSP para ver un flujo de vídeo en directo desde otros dispositivos de intercomunicación en el dispositivo.

Configuración Básica de RTSP

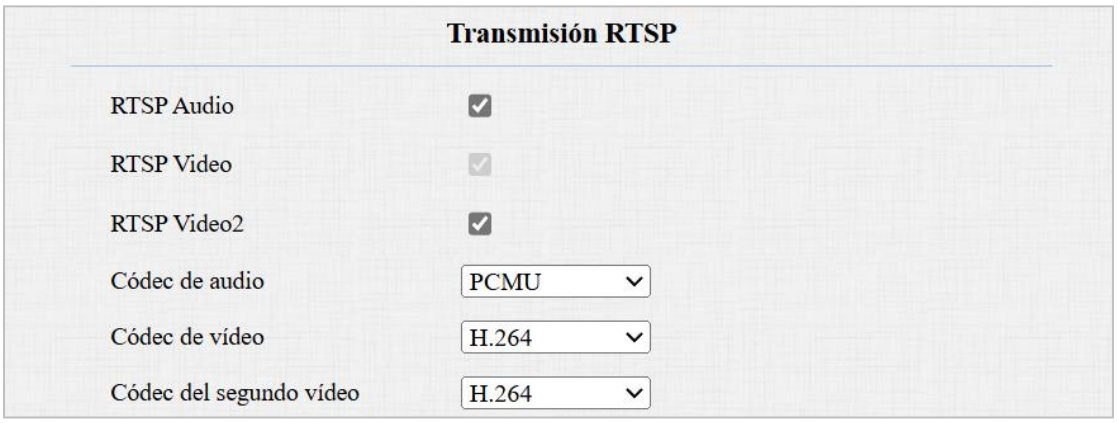
Es necesario configurar la función RTSP en la interfaz Vigilancia > RTSP en términos de Autorización RTSP, autenticación, contraseña, etc, antes de poder utilizar la función.

- Autorización RTSP Habilitada: Una vez habilitado, configure el Modo de autenticación RTSP, el Nombre de usuario RTSP y la Contraseña RTSP. Estas credenciales son necesarias para acceder al flujo RTSP del videoportero desde otros dispositivos de intercomunicación como monitores interiores.
- Modo de Autenticación: Por defecto es Digest, que utiliza hash en lugar de la codificación Base64 fácilmente reversible. Se utiliza un token para la verificación.
- Nombre de usuario: Establezca el nombre de usuario para la autorización.
- Contraseña: Establezca la contraseña para la autorización.

Configuración de la Transmisión RTSP

La transmisión RTSP puede utilizar H.264 o Mjpeg como códec de vídeo. Si elige H.264, también puede ajustar la resolución de vídeo, la tasa de bits y otros parámetros.

Para configurar el flujo RTSP, vaya a la interfaz web Vigilancia > RTSP > Transmisión RTSP.



- RTSP Audio: Decide si el flujo RTSP tiene sonido.
- RTSP Video: Decide si el flujo RTSP tiene vídeo. Después de activar la función RTSP, el vídeo RTSP está activado por defecto y no se puede modificar.
- RTSP Video2: El dispositivo admite dos flujos RTSP.
- Códec de audio: Elija un códec de audio adecuado para el audio RTSP.
- Códec de vídeo: Especifique los formatos de compresión de vídeo.
  - H.264: Ofrecen una compresión muy eficiente, pero a costa de una mayor latencia y carga computacional.
  - H.265: Ofrecen una eficiencia de compresión superior y compatibilidad con resoluciones más altas, pero viene acompañada de mayores requisitos computacionales y posibles problemas de compatibilidad.
  - MJEPG: Ofrecen una calidad mejorada pero una compresión ineficiente.

Consejo:

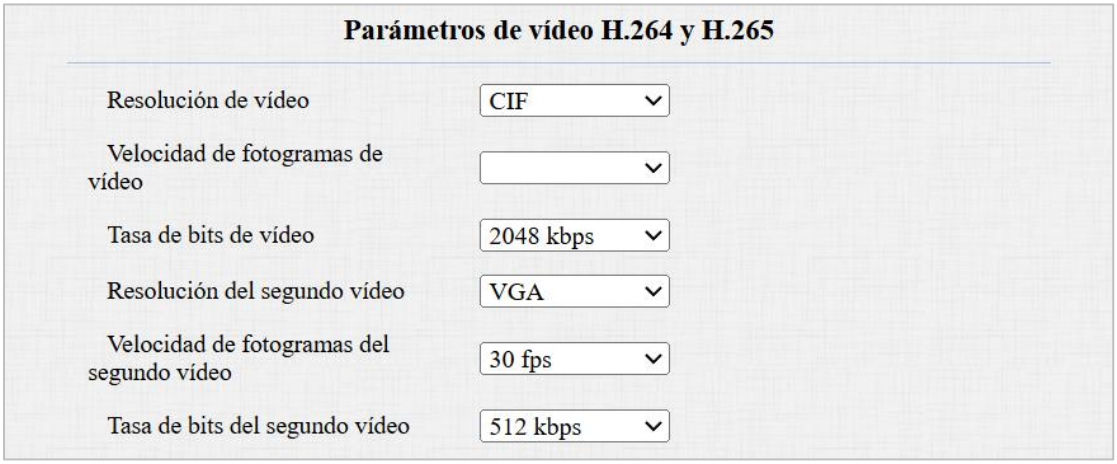
Para ver el flujo de audio y vídeo mediante RTSP:

- Primer canal: rtsp://IP del dispositivo/live/ch00_0
- Segundo canal: rtsp://IP del dispositivo/live/ch00_1

Configuración de los Parámetros de Vídeo H.264 y H.265

Puede configurar los parámetros de vídeo para H.264 y H.265 en la sección

Parámetros de vídeo H.264 y H.265.



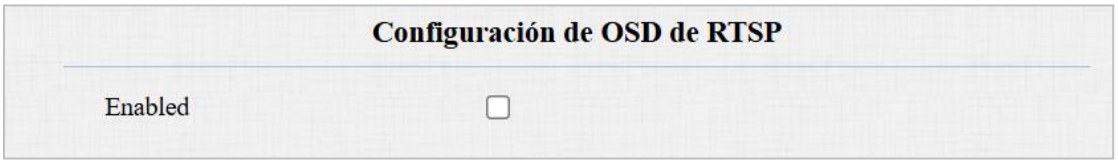
- Resolución de vídeo: Especifica la resolución de la imagen, variando desde la más baja CIF(352×288 píxeles) hasta la más alta 1080P(1920x1080 píxeles).
- Velocidad de Fotogramas de vídeo: Fotogramas por segundo, se refiere a cuántos fotogramas se muestran en un segundo de vídeo. La tasa de fotogramas por defecto es de 30fps.
- Tasa de bits de vídeo: La cantidad de datos de vídeo transferidos en una duración específica de tiempo. Una mayor tasa de bits de vídeo significa una mayor calidad posible, pero también mayores tamaños de archivo y más ancho de banda. El valor predeterminado es 2048 kbps.
- Resolución del 2º vídeo: Especifique la resolución de imagen para el segundo canal de flujo de vídeo.
- Velocidad de Fotogramas del 2º Vídeo: Especifique la velocidad de fotogramas del segundo canal de vídeo.
- Tasa de bits del 2º vídeo: Establezca la tasa de bits para el segundo canal de flujo de vídeo. El valor predeterminado es 512 kbps.

Configuración de OSD de RTSP

Esta función se utiliza para añadir una marca de agua al vídeo o imagen RTSP. Está desactivada por defecto.

Para configurarla, vaya a la interfaz Vigilancia > RTSP > Configuración de

OSD de RTSP.



- Color de OSD: Hay cinco opciones de color, Blanco, Negro, Rojo, Verde y Azul para el texto de la marca de agua RTSP.
- Texto de OSD: Personaliza el texto de la marca de agua.

NACK

Acuse de recibo negativo（NACK, por su sigla en inglés) indica un fallo o error en la transmisión o procesamiento de datos. Se utiliza para solicitar la retransmisión o señalar el fallo al remitente para garantizar la integridad de los datos.

Para activar NACK, vaya a la interfaz Videoportero> Función de llamada > Otros.

- “NACK Enabled”: Se puede utilizar para evitar la pérdida de paquetes de datos en el entorno de red débil cuando se producen imágenes de vídeo discontinuas y en mosaico.

ONVIF

Puede acceder al vídeo en tiempo real de la cámara del dispositivo utilizando el monitor de interior Akuvox u otros dispositivos de terceros como Videograbadores (NVR, por su sigla en inglés). La activación y configuración

de la función ONVIF en el dispositivo permitirá que su vídeo sea visible en otros dispositivos.

Para configurarla, vaya a la interfaz web Vigilancia > ONVIF.

- Descubrible: Cuando está activado, el vídeo de la cámara del portero automático para ser buscado por otros dispositivos.
- Nombre de usuario: Establezca el nombre de usuario necesario para acceder al flujo de vídeo del portero automático en otros dispositivos. Por defecto es admin.
- Contraseña: Establezca la contraseña necesaria para acceder al flujo de vídeo del videoportero en otros dispositivos. Por defecto es admin.

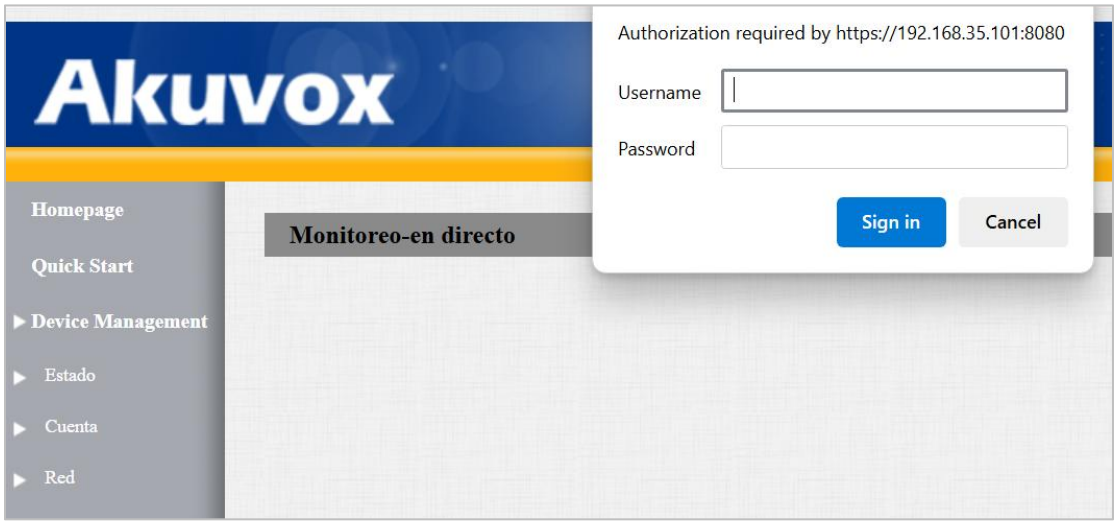
Consejo:
Una vez configurados los ajustes, para acceder al flujo de vídeo en el dispositivo de terceros, basta con introducir la URL ONVIF: http://Device's IP:80/onvif/device_service.

Transmisión en Directo

Hay dos formas de ver el vídeo en tiempo real desde el dispositivo. Una es ir a la interfaz web del dispositivo y ver el vídeo allí. La otra es introducir la URL correcta en el navegador web y acceder al vídeo directamente.

Visualice la secuencia de vídeo en la interfaz Vigilancia > Transmisión en directo. Se le pedirá que introduzca el nombre de usuario y la contraseña establecidos en la sección RTSP Básico antes de ver la transmisión en

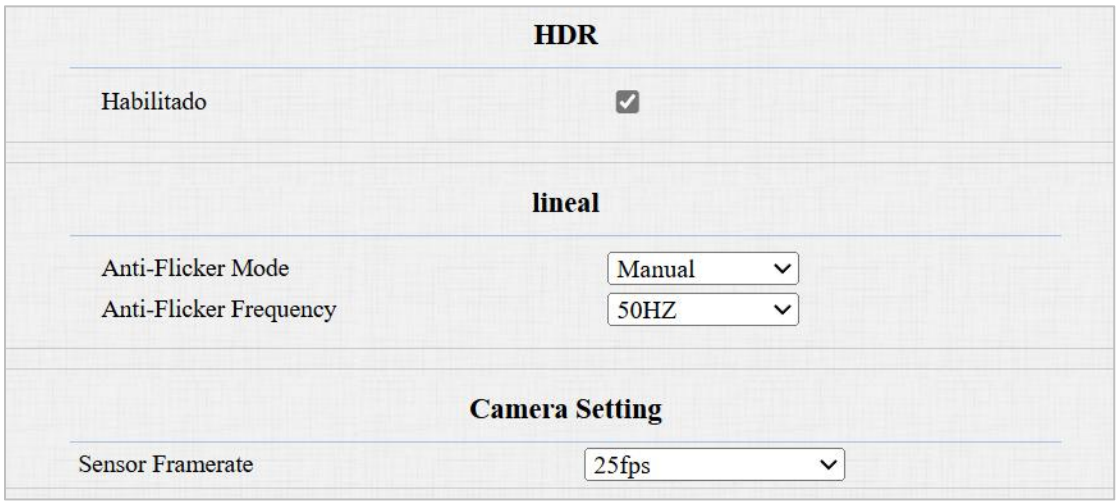
directo.



Modo de Cámara

- El alto rango dinámico (HDR, por su sigla en inglés) es una tecnología utilizada en fotografía, videografía y dispositivos de visualización para mejorar la calidad de la imagen mediante la captura de una gama más amplia de brillo y color.
- Lineal se refiere a una representación directa del brillo en las imágenes. Las imágenes lineales se suelen utilizar en entornos con iluminación controlada, como escenas de interior, donde hay un brillo constante

Puede configurar el modo de la cámara eligiendo entre HDR y Lineal en la interfaz Dispositivo > Cámara. Por defecto es HDR.

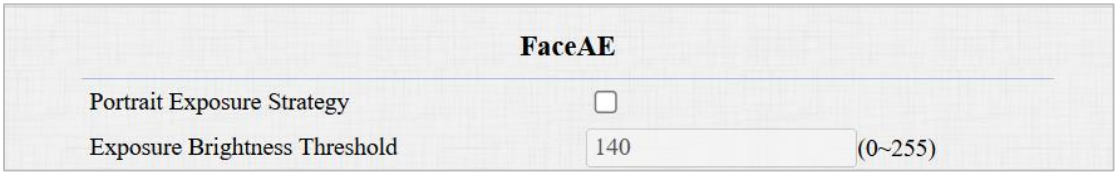


- Modo Antiparpadeo: La función antiparpadeo reduce o elimina el parpadeo en imágenes o vídeos causado por fuentes de luz variables.
  - Auto: El dispositivo cambiará automáticamente entre la frecuencia antiparpadeo de 50HZ y 60HZ.
  - Manual: Selecciona manualmente la frecuencia antiparpadeo.
  - Apagado: Desactiva la función antiparpadeo.
- Frecuencia Antiparpadeo: Seleccione la frecuencia antiparpadeo entre 50HZ y 60HZ.
- Frecuencia de imagen del sensor: Ajusta la velocidad de fotogramas de la cámara.
  - 30fps: Mejor para aplicaciones que necesitan mayor suavidad.
  - 25fps: Adecuado para grabación y reproducción de vídeo estándar, especialmente con una frecuencia de alimentación de 50 Hz para minimizar el parpadeo.

Exposición Automática de la Cara

La función FaceAE se utiliza para ajustar la configuración de exposición en función de las condiciones de iluminación, con el objetivo de capturar imágenes claras y bien expuestas de las personas.

Para activarla, vaya a la interfaz Dispositivo > Cámara.



- Umbral de luminosidad de la exposición: Define qué áreas de una imagen se consideran «sobreexpuestas» en función de los niveles de brillo. Cuando el umbral es cercano a 255, sólo las áreas muy brillantes se consideran sobreexpuestas.

Tipo de Transmisión de Datos para Cámara de Terceros

Puede seleccionar el tipo de transmisión de datos entre el dispositivo y una cámara de terceros cuando está conectada a SmartPlus Cloud.

Para configurarlo, vaya a la interfaz Vigilancia > RTSP > Cámara de terceros.

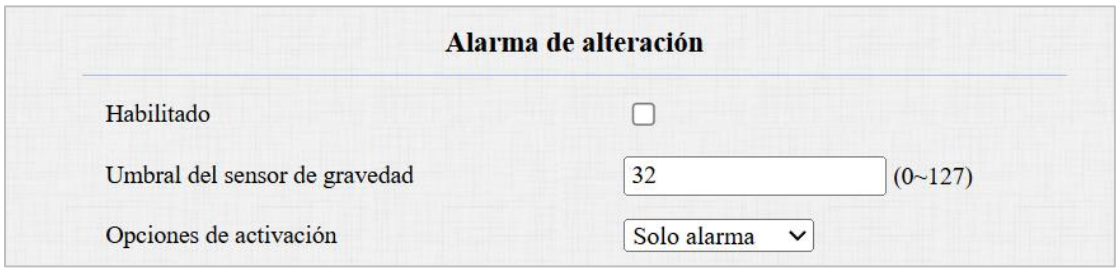
- UDP: Un protocolo de capa de transporte poco fiable pero muy eficiente.
- TCP: Un protocolo de capa de transporte menos eficiente pero fiable. Es el protocolo de transporte por defecto.

Seguridad

Alarma Antisabotaje

La función de alarma antisabotaje impide que se retiren los dispositivos sin permiso. Para ello, activa la alarma antimanipulación y realiza llamadas a una ubicación designada cuando el dispositivo detecta un cambio en su valor de gravedad respecto al original.

Para configurarla, vaya a la interfaz web Sistema > Seguridad > Alarma antimanipulación. Cuando se active la alarma, puede hacer clic en Desarmar para borrarla.



- Umbral del sensor de gravedad: El umbral de sensibilidad del sensor de gravedad. Cuanto más bajo sea el valor, más fácilmente se activará la alarma antimanipulación. Por defecto es 32.
- Opciones de activación: Seleccione lo que puede activarse cuando se activa el sensor de gravedad.

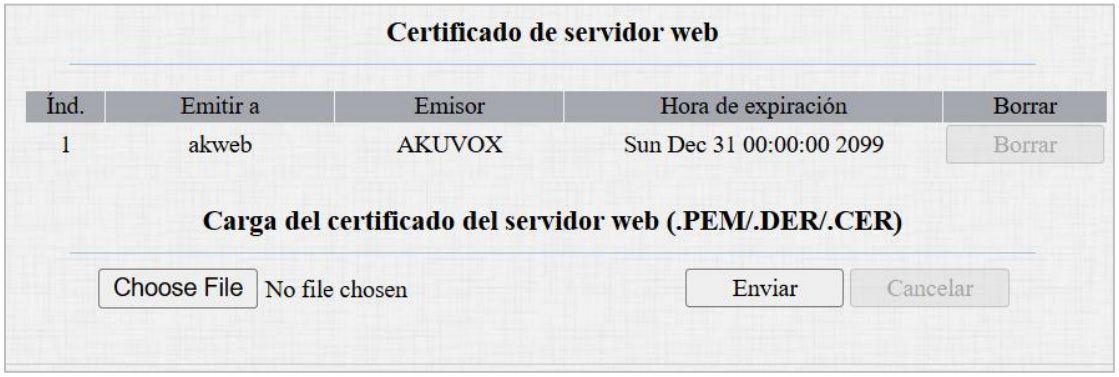
Configuración de Certificados de Cliente

Los certificados garantizan la integridad y privacidad de las comunicaciones. Para utilizar el protocolo SSL, es necesario cargar los certificados adecuados para su verificación.

Certificado del Servidor Web

Es un certificado enviado al cliente para autenticación cuando el cliente solicita una conexión SSL con el portero Akuvox. Cargue los certificados en los formatos aceptados.

Cargue el certificado en la interfaz web Sistema > Certificado.



Certificado de Cliente

Este certificado verifica el servidor al portero automático Akuvox cuando quieren conectarse usando SSL. El portero automático verifica el certificado del servidor con su lista de certificados de cliente.

Cargue el certificado en la interfaz web Sistema > Certificado.

- Índice: Seleccione el valor deseado de la lista desplegable de Índice. Si selecciona Auto, el certificado cargado se mostrará en orden numérico. Si selecciona el valor de 1 a 10, el certificado cargado se mostrará según el número.
- Elegir archivo: Haga clic en Elegir archivo para cargar el certificado.
- Aceptar sólo certificados de confianza: Si está activada, siempre que la autenticación se realice correctamente, el teléfono verificará el certificado del servidor basándose en la lista de certificados del cliente. Si se desactiva, el teléfono no verificará el certificado del servidor, independientemente de si el certificado es válido o no.

Cargar Certificado TLS para Registro de Cuenta SIP

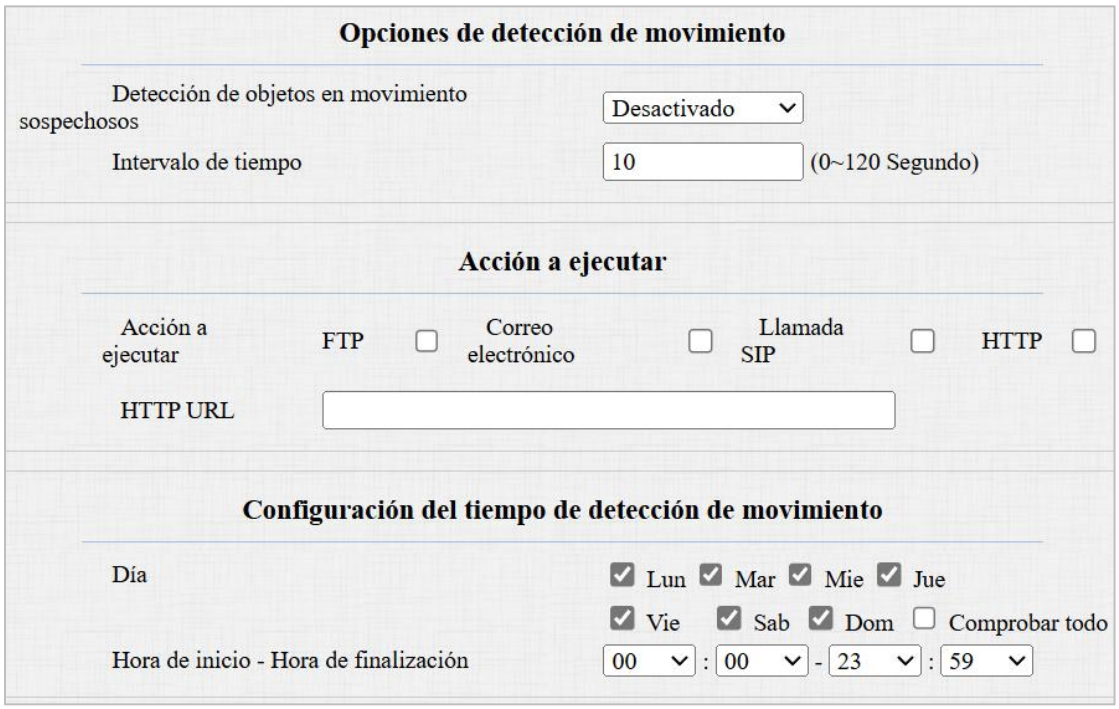
Antes de solicitar una cuenta SIP desde un servidor SIP o DNS que utilice el protocolo TLS, deberá cargar un certificado. Este certificado es esencial para la autenticación del servidor.

Para configurarlo, vaya a Sistema > Certificado.

Detección de Movimiento

La detección de movimiento es una función que permite la videovigilancia desatendida y las alarmas automáticas. Detecta cualquier cambio en la imagen captada por la cámara, como alguien caminando o el objetivo moviéndose, y activa el sistema para realizar la acción apropiada.

Para configurarla, vaya a la interfaz web Vigilancia > Movimiento.



- Detección de objetos en movimiento sospechosos:
  - Desactivado: Desactiva la función de detección de movimiento.
  - Detección IR: Cuando el sensor de infrarrojos detecta objetos en movimiento, se activan las acciones preestablecidas.
  - Detección de Vídeo: Cuando la cámara de vídeo detecta objetos en movimiento, se activan las acciones predefinidas.

Si selecciona Detección de vídeo, deberá configurar las siguientes opciones.

- Área de detección: Puede especificar tres áreas de detección pulsando el botón izquierdo del ratón y dibujando recuadros.
- Precisión de Detección: La sensibilidad de detección. Cuanto mayor sea el valor, más precisa será la detección. El valor por defecto es 3.
- Si se configura el intervalo de tiempo en 10 segundos, este será el periodo durante el cual el sistema evaluará la presencia de movimiento. Por ejemplo, al establecer un intervalo de 10 segundos, el primer movimiento detectado marca el inicio del ciclo de detección. Si el movimiento continúa durante 7 segundos dentro de ese intervalo, la alarma se activará a los 7 segundos (primer punto de activación). A partir de ese momento, la acción asociada a la detección de movimiento (como el envío de una notificación) puede ejecutarse en cualquier momento entre el segundo 7 y el 10. Una vez transcurrido el ciclo completo de 10

segundos, se iniciará un nuevo periodo de detección con la misma duración. Para ser más específicos, el primer punto de activación puede calcularse como el intervalo de tiempo establecido menos tres segundos.

- Acción a ejecutar: Establezca las acciones deseadas que se producen cuando se detecta un movimiento sospechoso.
  - FTP: Envía una captura de pantalla al Servidor FTP preconfigurado.
  - Correo electrónico: Envía una captura de pantalla a la Dirección de correo electrónico preconfigurada.
  - Llamada SIP: Llama al número preconfigurado al activarse.
  - HTTP: Cuando se activa, el mensaje HTTP puede ser capturado y mostrado en los paquetes correspondientes. Para utilizar esta función, active el servidor HTTP e introduzca el contenido del mensaje en la casilla designada a continuación.
- URL HTTP: Introduzca el mensaje HTTP si selecciona HTTP como acción a ejecutar. El formato es http://HTTP server's IP/Message content.
- Hora de Detección de Movimiento: Especifique la hora a la que es efectiva la configuración de detección de movimiento.

Notificación de Seguridad

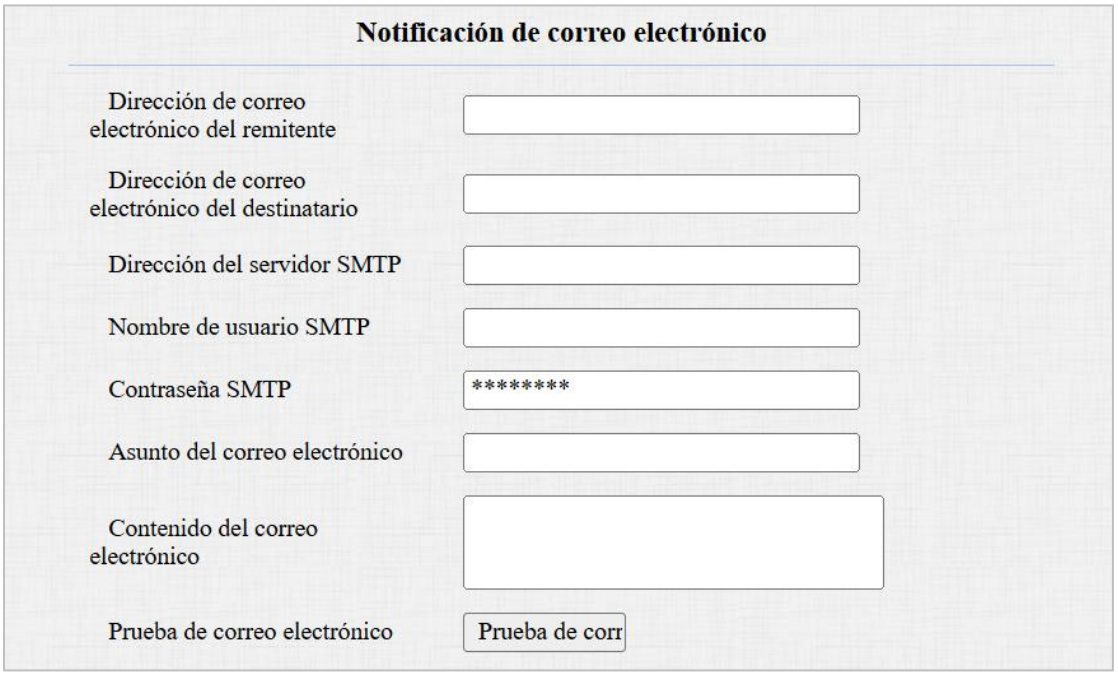
Una notificación de seguridad informa a los usuarios o al personal de seguridad de cualquier infracción o amenaza que detecte el dispositivo. Por ejemplo, si el dispositivo detecta algo inusual, el sistema envía una notificación a los usuarios o al personal de seguridad a través de correo electrónico, llamadas telefónicas u otros métodos.

Para configurar las notificaciones de seguridad, vaya a la interfaz Configuración > Acción.

Notificación por Correo Electrónico

Configure la notificación por correo electrónico para recibir capturas de

pantalla de movimientos inusuales del dispositivo.



- Dirección del servidor SMTP: La dirección del servidor SMTP del remitente.
- Nombre de usuario SMTP: El nombre de usuario SMTP suele ser el mismo que la dirección de correo electrónico del remitente.
- Contraseña SMTP: La contraseña del servicio SMTP es la misma que la dirección de correo electrónico del remitente.
- Prueba de correo electrónico: Sirve para comprobar si el correo electrónico se puede enviar y recibir.

Notificación FTP

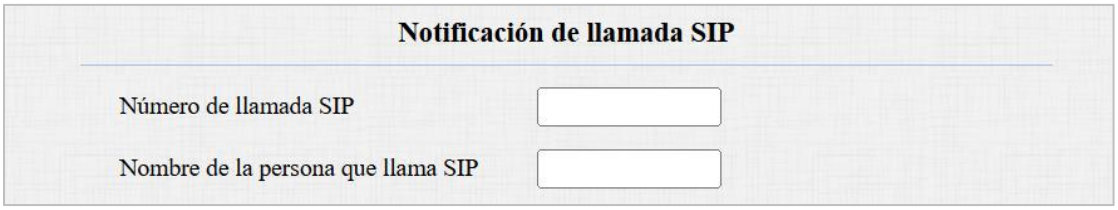
Para recibir notificaciones a través del servidor FTP, debe configurar los ajustes de FTP. El videoportero subirá una captura de pantalla a la carpeta FTP especificada si detecta algún movimiento inusual.

- Servidor FTP: Establezca la dirección (URL) del servidor FTP.
- Nombre de usuario FTP: Introduzca el nombre de usuario para acceder al servidor FTP.
- Contraseña FTP: Introduzca la contraseña para acceder al servidor FTP.
- Prueba FTP: Permite comprobar si el servidor FTP puede enviar y recibir la notificación FTP.

Notificación de Llamada SIP

Además de la notificación por FTP y correo electrónico, el portero automático también puede realizar una llamada SIP cuando se activa alguna acción de la función.

Configúrelo en la sección Notificación de llamada SIP.



URL de Acción

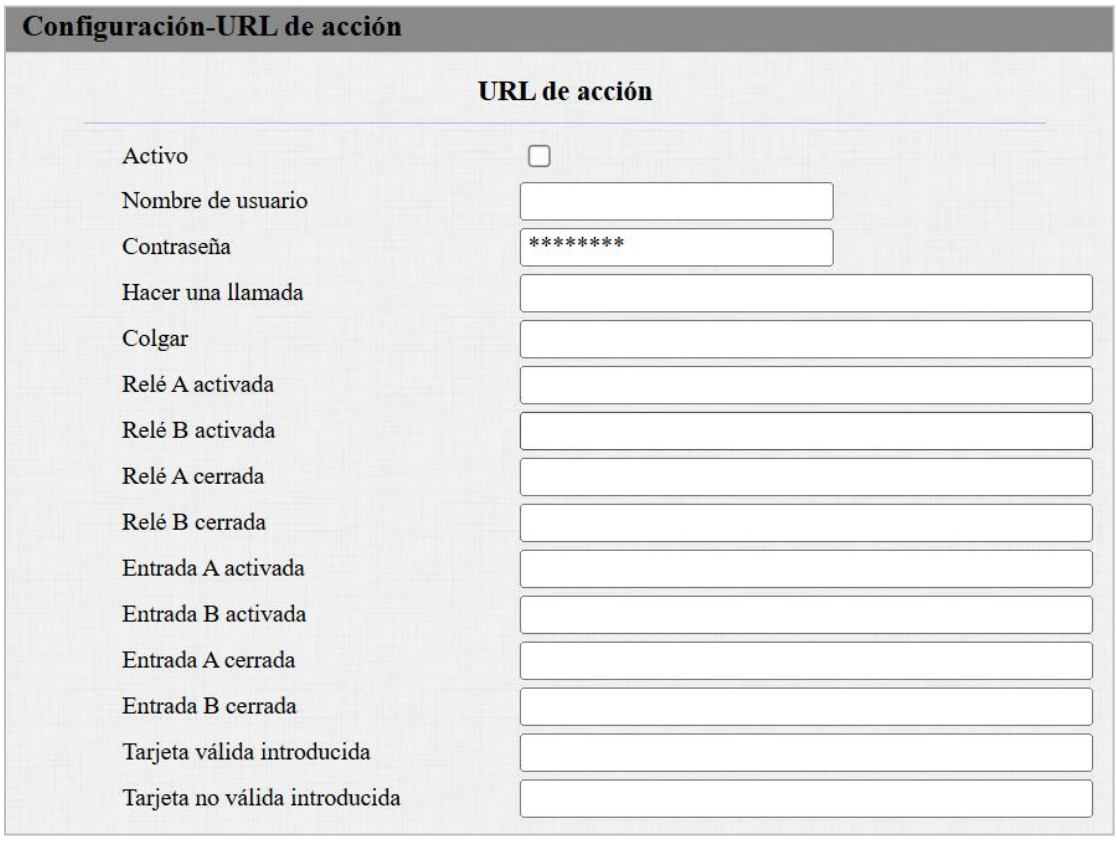
Puede utilizar el dispositivo para enviar comandos URL HTTP específicos al servidor HTTP para determinadas acciones. Estas acciones se activarán cuando cambie el estado del relé, el estado de la entrada, el código PIN o el acceso a la tarjeta RF.

URL de Acción Akuvox:

Nº	Evento	Formato de Parámetro	Ejemplo
1	Realizar llamada	$remote	Http://server ip/Callnumber=$remote
2	Colgar	$remote	Http://server ip/Callnumber=$remote
3	Relé activado	$relay1status	Http://server ip/relaytrigger=$relay1status
4	Relé cerrado	$relay1status	Http://server ip/relayclose=$relay1status
5	Entrada activada	$input1status	Http://server ip/inputtrigger=$input1status
6	Entrada cerrada	$input1status	Http://server ip/inputclose=$input1status
7	Tarjeta válida introducida	$card_sn	Http://server ip/validcard=$card_sn
8	Tarjeta no válida introducida	$card_sn	Http://server ip/invalidcard=$card_sn

Por ejemplo:
http://192.168.16.118/help.xml?
mac=$mac:ip=$ip:model=$model:firmware=$firmware:card_sn=$card_sn

Configure la URL de la acción en la interfaz Configuración > URL de la acción. Puede configurar el nombre de usuario y la contraseña para la autenticación.



Cifrado de Voz

El Protocolo de Transporte Seguro en Tiempo Real (SRTP) es un protocolo derivado del Protocolo de Transporte en Tiempo Real (RTP). Mejora la seguridad de la transmisión de datos proporcionando cifrado, autenticación de mensajes, garantía de integridad y protección contra repeticiones.

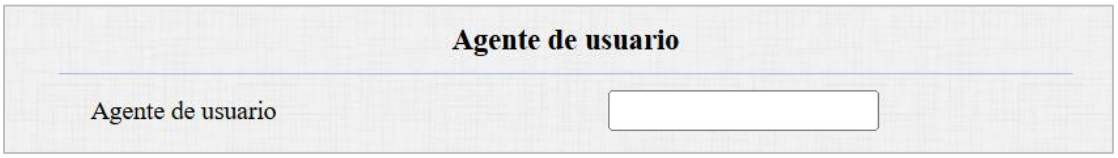
Configúrelo en la interfaz Cuenta > Avanzado > Cifrado.

- Cifrado de voz (SRTP): Elija Desactivado, Opcional u Obligatorio para SRTP. Si se selecciona Opcional u Obligatorio, la voz durante la llamada se encripta y se puede capturar el paquete RTP para verlo.

Agente de Usuario

El agente de usuario se utiliza con fines de identificación cuando se analiza el paquete de datos SIP.

Para configurarlo, vaya a la interfaz Cuenta > Avanzado > Agente de Usuario.



Acción de Emergencia

Esta característica funciona con Akuvox SmartPlus Cloud. Mantiene la puerta abierta cuando se produce una emergencia. Debe especificar la Entrada que aplica la función.

Haga clic aquí para ver la configuración detallada de esta función.

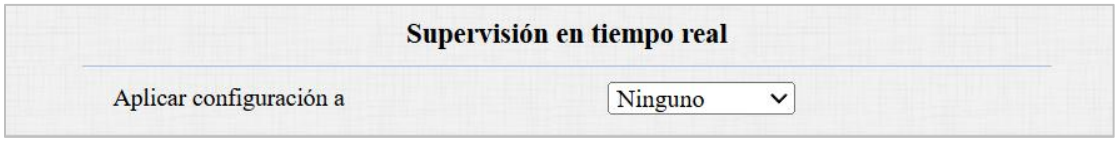
Habilite la función de acción de emergencia en la interfaz Sistema > Seguridad > Acción de emergencia.

Monitorización en Tiempo Real

Esta función muestra el estado de la puerta cuando el dispositivo está conectado a la nube SmartPlus. Los administradores de propiedades y los usuarios finales pueden comprobar el estado de la puerta respectivamente en la plataforma SmartPlus Property Manager y SmartPlus App. Es necesario especificar los relés o entradas que aplican esta función. Haga clic aquí para

ver la configuración detallada.

Para configurarlo, vaya a la interfaz Sistema > Seguridad > Supervisión en tiempo real.

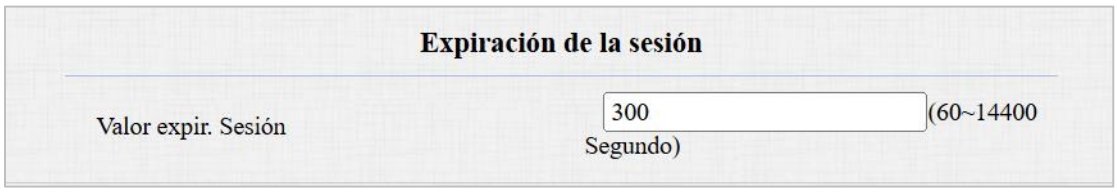


- Aplicar ajuste a:
  - Ninguno: No mostrar el estado de la puerta.
  - Entrada: La puerta se abre por activación de entrada.
  - Relé: La puerta se abre activando el relé.

Desconexión Automática de la Interfaz Web

Puede configurar el tiempo de cierre de sesión automático de la interfaz web, que requiere volver a iniciar sesión introduciendo el nombre de usuario y las contraseñas por motivos de seguridad o para facilitar el funcionamiento.

Para configurarlo, vaya a la interfaz Sistema > Seguridad > Tiempo de espera de la sesión.



Modo de Alta Seguridad

El modo de alta seguridad está diseñado para mejorar la seguridad. Emplea el cifrado en varias facetas, incluido el proceso de comunicación, los comandos de apertura de puertas, los métodos de almacenamiento de contraseñas, etc.

Active o desactive el modo de alta seguridad en la interfaz Sistema > Seguridad> Modo de alta seguridad.

Notas Importantes

1. El modo de alta seguridad está desactivado por defecto cuando se actualiza el dispositivo de una versión sin el modo a otra con él. Pero si restableces el dispositivo a su configuración de fábrica, el modo está activado por defecto.

2. Este modo hace que las herramientas de la versión antigua sean incompatibles. Es necesario actualizarlas a las siguientes versiones o superiores para poder utilizarlas.

- PC Manager: 1.2.0.0
- Escáner IP: 2.2.0.0
- Herramienta de actualización: 4.1.0.0
- SDMC: 6.0.0.34

3. El formato HTTP admitido para la activación del relé varía en función de si el modo de alta seguridad está activado o desactivado.

- Si el modo está activado, el dispositivo sólo acepta los nuevos formatos HTTP que se indican a continuación para la apertura de puertas.
  - http://username:password@deviceIP/fcgi/OpenDoor?action=OpenDoor&DoorNum=1
  - http://deviceIP/fcgi/OpenDoor?action=OpenDoor&DoorNum=1
- Si el modo está desactivado, el dispositivo puede utilizar tanto los nuevos formatos de arriba como el formato antiguo de abajo:
  - http://deviceIP/fcgi/do?action=OpenDoor&UserName=username&Password=password&DoorNum=1

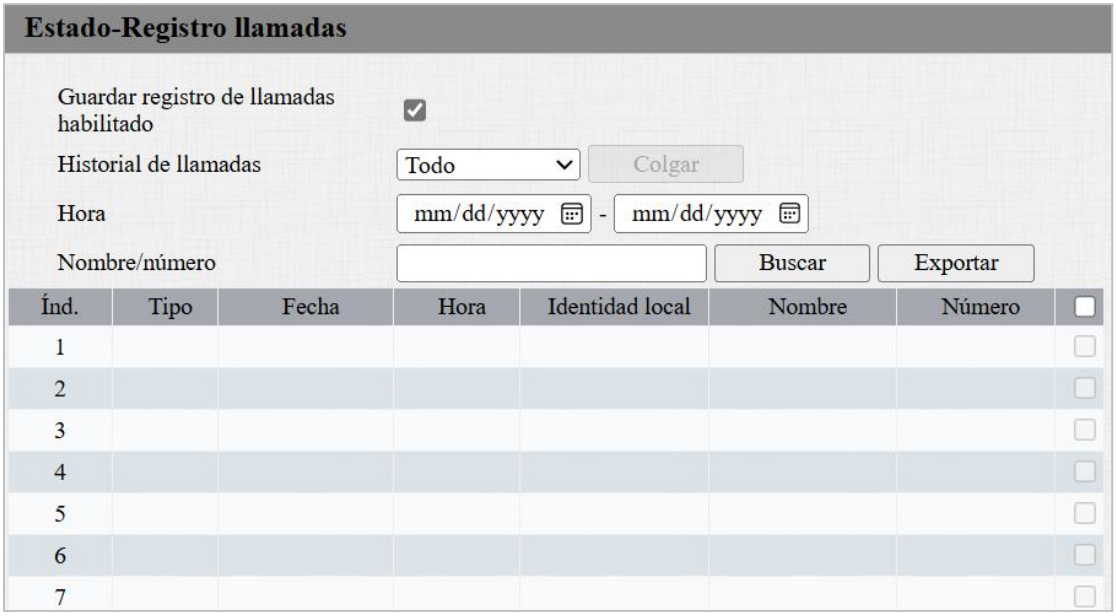
4. No está permitido importar/exportar archivos de configuración en formato tgz. entre un dispositivo con el modo de alta seguridad y otro sin él. Para obtener ayuda con la transferencia de archivos, póngase en contacto con el soporte técnico de Akuvox.

Registros

Registros de Llamadas

Para comprobar las llamadas -incluidas las salientes, las recibidas y las perdidas- dentro de un periodo específico, puede ver el registro de llamadas en la interfaz web del dispositivo. Si es necesario, también puede exportar el registro de llamadas desde el dispositivo.

Comprueba los registros de llamadas en la interfaz web Estado > Registro de llamadas.

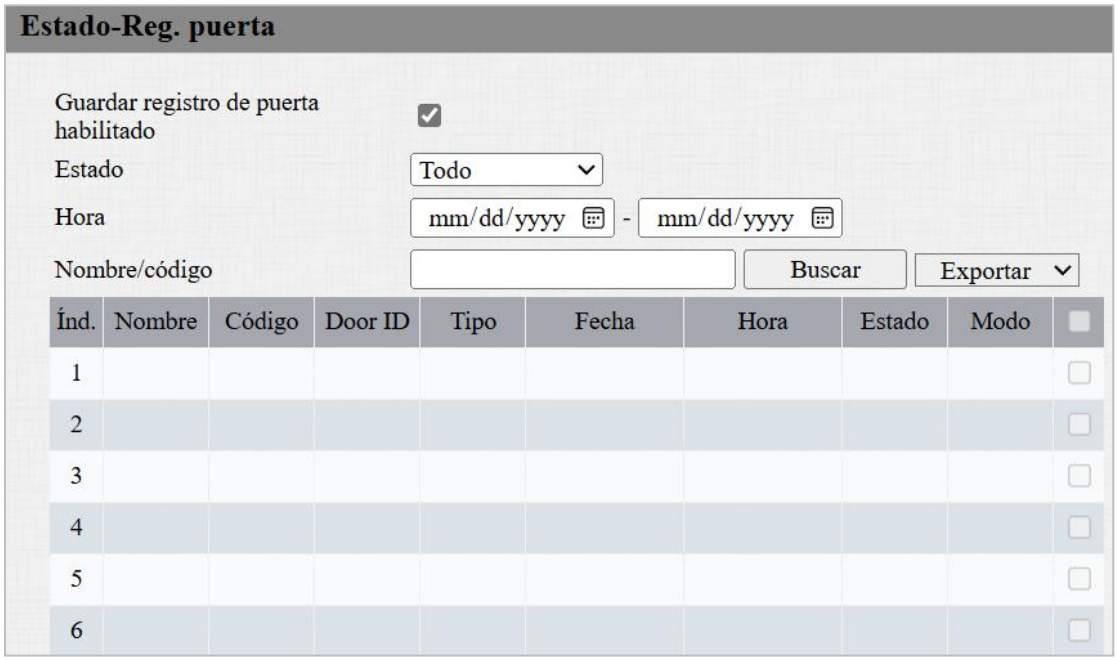


- Historial de llamadas: Existen cuatro tipos específicos de registros de llamadas: Todas, Marcadas, Recibidas y Perdidas.
- Hora: Busque el registro de llamadas deseado introduciendo un periodo determinado.
- Nombre/Número: Busque el registro de llamadas deseado introduciendo el nombre y el número.

Registros de Puerta

Para buscar y revisar varios tipos de historial de acceso a la puerta, sólo tiene que comprobar los registros de puerta en la interfaz web del dispositivo.

Compruebe los registros de puerta en la interfaz web Estado > Registro de acceso.



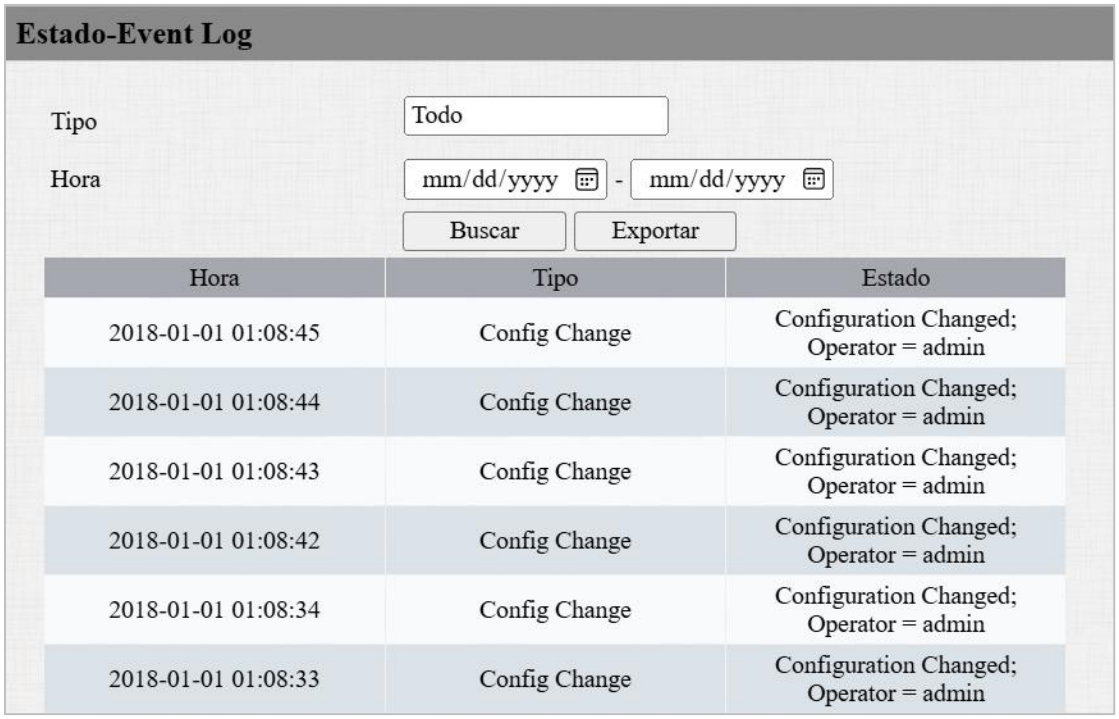
- Estado: Mostrar todos los registros de apertura de puerta, exitosos y fallidos.
- Hora: Buscar el registro de llamadas deseado introduciendo un periodo determinado.
- Nombre: Muestra el nombre del usuario. Si se trata de una llave o tarjeta desconocida, mostrará Desconocido.
- Código: Si la puerta se abre mediante tarjetas RF, se mostrará el código de la tarjeta. Si la puerta se abre mediante un comando HTTP, estará vacío.
- Tipo: Muestra los métodos de acceso.

Registro de Eventos

Los registros de eventos registran los eventos clave, como el cambio de estado de la entrada, el relé, la alarma antisabotaje, etc. Esto ayuda a realizar

un seguimiento del estado y los cambios del dispositivo.

Puede consultar los registros de eventos en la interfaz Estado > Registro de eventos. Puede exportar el registro en formato CSV.



Integración con Dispositivos de Terceros

Integración vía Wiegand

El dispositivo puede integrarse con dispositivos de terceros a través de Wiegand.

Configúrelo en la interfaz Dispositivo > Wiegand.

- Modo de visualización Wiegand: Seleccione el formato de código de tarjeta Wiegand entre las opciones proporcionadas.
- Modo Lector de Tarjeta Wiegand: El formato de transmisión debe ser idéntico entre el terminal de control de acceso y el dispositivo de terceros.
- Modo Transferencia Wiegand:
  - Entrada: El dispositivo sirve como receptor.
  - Salida: El dispositivo sirve como emisor, enviando los datos de la tarjeta a un dispositivo de terceros para el acceso a la puerta.
  - Convertir en número de tarjeta Salida: El dispositivo actúa como emisor. Los datos de acceso, incluido el código de tarjeta DTMF y RF, se convertirán en números de tarjeta para el acceso a la puerta.
- Orden de Datos de Entrada Wiegand: Establezca la secuencia de datos de entrada Wiegand entre Normal e Invertida. Si selecciona Invertido, el número de tarjeta introducido se invertirá.
- Orden de Datos Básicos de Salida Wiegand: Establezca la secuencia de los datos de salida Wiegand.
  - Normal: Los datos se muestran tal como se reciben.
  - Invertido: Se invierte el orden de los bits de datos.
- Orden de Datos de Salida Wiegand: Determina la secuencia del número de tarjeta.
  - Normal: El número de tarjeta se muestra tal como se recibe.

- Invertido: Se invierte el orden del número de tarjeta.

- CRC de salida Wiegand: Está habilitado por defecto para la inspección de datos Wiegand. Deshabilitarlo puede provocar fallos de integración con dispositivos de terceros.

Nota:

Haz click aquí para ver más información sobre la configuración Wiegand incluyendo:

- Dispositivos Akuvox funcionan como entrada/salida Wiegand;
- Conexión del lector de tarjetas Wiegand.

Integración con Milestone

Si desea que el portero automático sea supervisado por Milestone o cualquier dispositivo de terceros que se haya integrado con Milestone, debe habilitar la función.

Habilítela en la interfaz Vigilancia > ONVIF > Configuración avanzada.

Integración mediante API HTTP

La API HTTP está diseñada para lograr una integración basada en red entre el dispositivo de terceros y el dispositivo Akuvox.

Configúrela en la interfaz Configuración web > API HTTP.

- Activado: Habilita o deshabilita la función API HTTP para la integración de terceros. Si la función está deshabilitada, cualquier solicitud para iniciar la integración será denegada y devolverá el estado HTTP 403 prohibido.
- Modo de autorización: Consulte la descripción de cada opción en el siguiente cuadro.
- Nombre de usuario: Introduzca el nombre de usuario para la autenticación. Por defecto es admin.
- Contraseña: Introduzca la contraseña para la autenticación. Por defecto es admin.
- 1ª IP-5ª IP: Introduzca la dirección IP de los dispositivos de terceros cuando se seleccione la autorización por Lista de Permitidos para la integración.

Consulte la siguiente descripción del modo de autenticación:

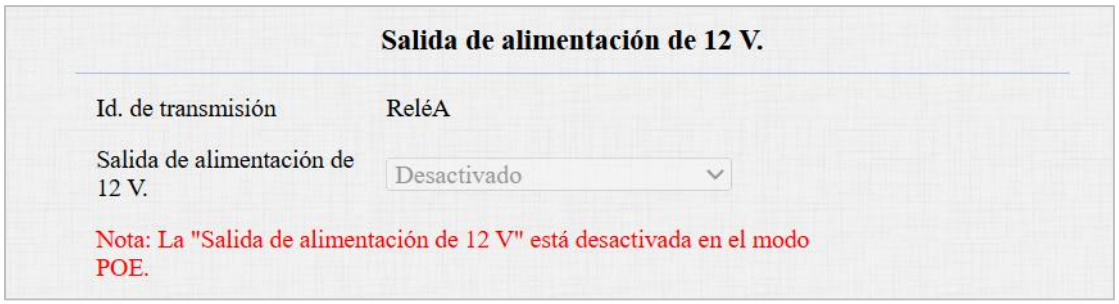
Nº	Modo de autorización	Descripción
1	Ninguno	No se requiere autenticación para la API HTTP, ya que sólo se utiliza para pruebas de demostración.
2	Normal	Este modo sólo lo utilizan los desarrolladores de Akuvox.

3	Lista de permisos	Si se selecciona este modo, sólo se requiere rellenar la dirección IP del dispositivo de terceros para la autenticación. La lista blanca es adecuada para el funcionamiento en la LAN.
4	Básica	Si selecciona este modo, deberá introducir el nombre de usuario y la contraseña para la autenticación. En el campo Autorización de la cabecera de la petición HTTP, utilice el método de codificación Base64 para codificar el nombre de usuario y la contraseña.
5	Digest	El método de codificación de la contraseña sólo admite MD5(Message-Digest Algorithm). En el campo Authorization de la cabecera de la petición Http:WWW-Authenticate: Digest realm=«HTTP API», qop=«auth,auth-int», nonce=«xx», opaque=«xx».
6	Token	Este modo sólo lo utilizan los desarrolladores de Akuvox.

Control de Salida de Alimentación

El dispositivo puede servir como fuente de alimentación para los relés externos.

Para configurarlo, vaya a la interfaz Control de acceso > Relé > Salida de alimentación de 12 V.



- Salida de alimentación de 12 V: Esta función sólo se puede utilizar cuando el dispositivo se alimenta con un adaptador de corriente de 12 V.

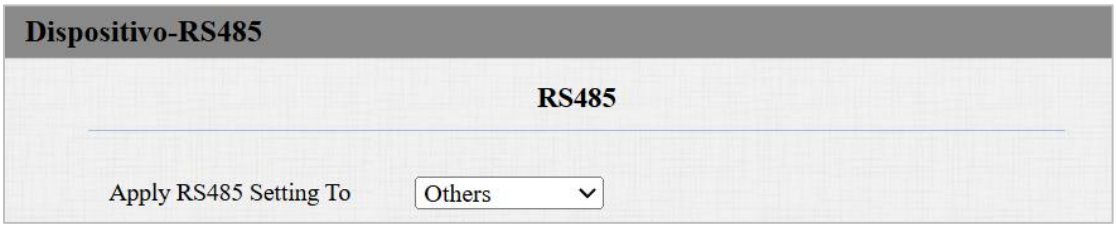
- Desactivado: Desactiva la función.
- Siempre: Proporciona alimentación continua.
- Activado por relé abierto: Proporciona alimentación al dispositivo de terceros cuando el relé A se activa a través de sus puertos NO y GND. Deja de suministrar alimentación cuando se restablece el relé A.
  - Tiempo de espera (Seg): Establezca el tiempo (3, 5 o 10 segundos) para suministrar alimentación cuando se seleccione Activado por relé abierto.

Integración a Través de RS485

Puede conectar el dispositivo a un dispositivo externo, como el SR01 o un lector de tarjetas basado en OSDP, a través de RS485. Para que la conexión sea efectiva, debe seleccionar el modo RS485 adecuado.

Haga clic aquí para ver la configuración detallada de la función OSDP.

Para configurarla, vaya a Dispositivo > Interfaz RS485.



- Desactivado: La función RS485 está desactivada.
- OSDP: El dispositivo está conectado a un dispositivo externo basado en OSDP, como un lector de tarjetas.
  - Cifrado: Marque esta opción cuando el protocolo esté encriptado.
  - Valor SCBK: Valor de la Clave de Comunicación Segura.
    - Cuando se llena, OSDP utilizará este valor para la encriptación, empleando un protocolo personalizado para la comunicación.
    - Cuando se deja vacío, OSDP utilizará el protocolo encriptado por defecto para la comunicación.

- Otros: Seleccione esta opción cuando el dispositivo trabaje con el SR01 u otros dispositivos no basados en OSDP.

Control de Ascensor

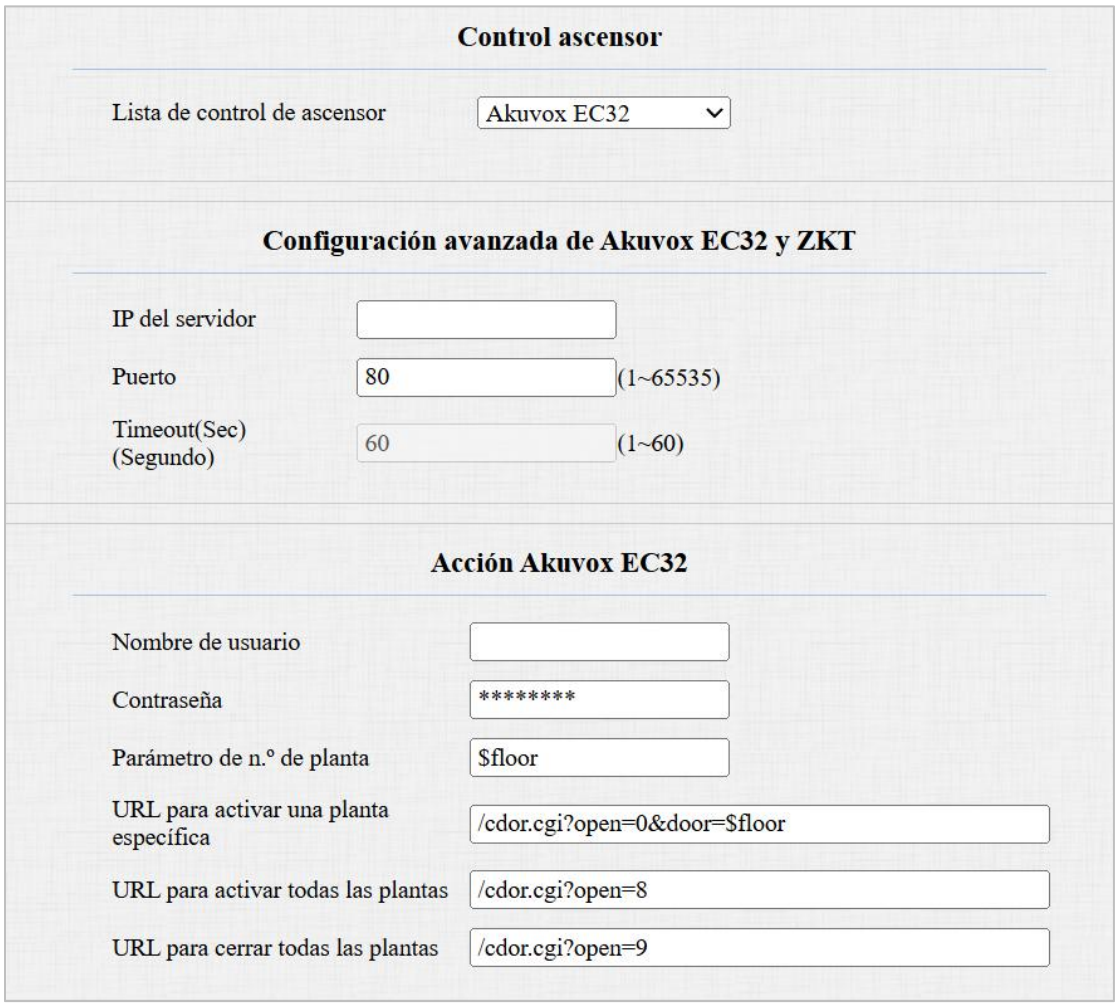
El dispositivo puede conectarse al controlador de ascensor Akuvox para el control del ascensor. Los usuarios pueden llamar al ascensor para que baje a la planta baja cuando se les concede el acceso a través de varios tipos de métodos de acceso en el dispositivo.

Para configurarlo, vaya a la interfaz web Dispositivo > Control de ascensor.

- Lista de controladores de ascensor: Seleccione la marca del controlador del ascensor.
  - Ninguno: La integración se desactivará.
  - Chiyu: Integrar con controlador de ascensor Chiyu.
  - KeyKing: Integrar con controlador de ascensor KeyKing.
  - Akuvox EC32: Conectar el dispositivo con el controlador de ascensor Akuvox EC33.
  - ZKT: Integración con el controlador de ascensor ZKTeco.

Controlador de Ascensor Akuvox

Tras seleccionar Akuvox EC32 en la lista de control de ascensores, deberá configurar los parámetros pertinentes.



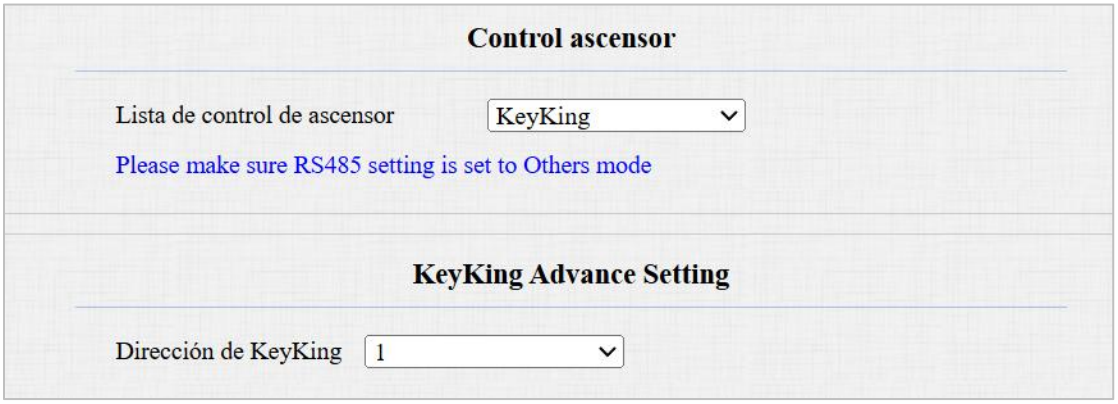
- IP del servidor: Introduzca la dirección IP del controlador de ascensor Akuvox.
- Puerto: Introduzca el puerto del controlador de ascensor Akuvox.
- Tiempo de espera(Seg): Decida el tiempo límite en el que los usuarios deben pulsar el botón del ascensor de las plantas que deseen.
- Nombre de usuario: Introduzca el nombre de usuario establecido en el controlador del ascensor.
- Contraseña: Introduzca la contraseña establecida en el controlador del ascensor.
- Parámetro de NO. de Planta: El parámetro de número de planta lo proporciona Akuvox. Por defecto es $floor. Puede definir su propia cadena de parámetros. URL para activar una planta específica: La URL de control de ascensores Akuvox para activar un piso específico.
- La URL es /cdor.cgi?open=0&door=$floor, pero la cadena $floor al final

debe ser idéntica a la cadena de parámetros que usted definió.

- URL para activar todas las plantas : La URL de Akuvox para activar todas las plantas.
- URL Para Cerrar Todas las Plantas: La URL de Akuvox para cerrar todas las plantas.

Controlador de Ascensor KeyKing

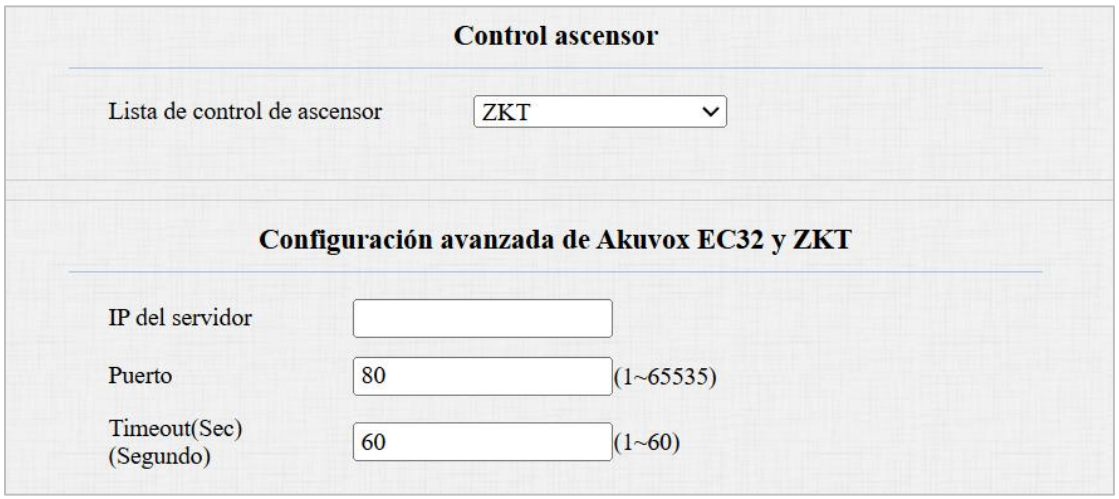
Después de seleccionar KeyKing, debe configurar la dirección KeyKing.



- "KeyKing Advance Setting": Seleccione el número de 0 a 126. El número binario convertido a partir del número de dirección corresponde al interruptor dip de la tarjeta del ascensor. Por ejemplo, si selecciona 5, ajuste el interruptor DIP a 101000.

Controlador de Ascensor ZKT

Tras seleccionar ZKT, debe configurar los parámetros pertinentes.



- IP del servidor: Introduzca la dirección IP del servidor del controlador.
- Puerto: Introduzca el puerto del servidor del controlador.
- Tiempo de espera(Seg): Decida el tiempo límite en el que los usuarios deben pulsar el botón del ascensor de las plantas que deseen.

Actualización del Firmware

Los dispositivos Akuvox pueden actualizarse en la interfaz web del dispositivo.

Actualice el firmware en la interfaz web Sistema > Actualizar.

Nota:

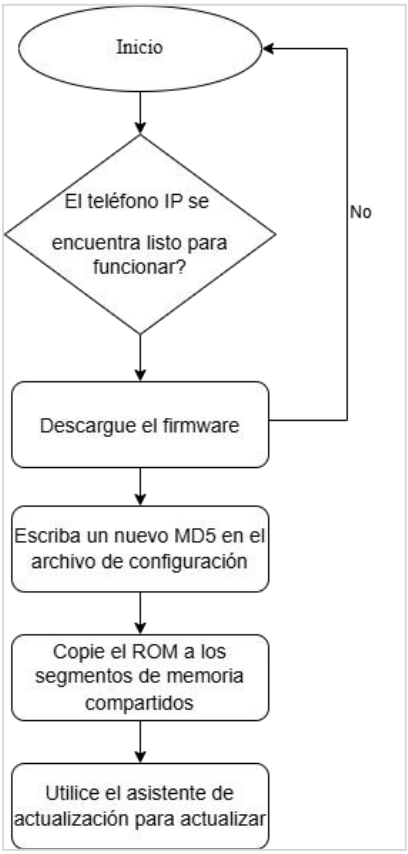
Los archivos de firmware deben estar en formato .rom para su actualización.

Autoaprovisionamiento Mediante Archivo de Configuración

Principio de Autoaprovisionamiento

El autoaprovisionamiento es una función que se utiliza para configurar o actualizar dispositivos por lotes a través de servidores de terceros. DHCP, PNP, TFTP, FTP y HTTPS son los protocolos utilizados por los dispositivos Akuvox para acceder a la URL de la dirección del servidor de terceros que almacena los archivos de configuración y el firmware, que luego se utilizará para actualizar el firmware y los parámetros correspondientes en el dispositivo.

Consulte el diagrama de flujo que figura a continuación:



Akuvox
Open A Smart World

Introducción a los Archivos de Configuración para el Autoaprovisionamiento

Los archivos de configuración para el autoaprovisionamiento vienen en dos formatos: archivos de configuración general y archivos de configuración basados en MAC.

Diferencias:

- Aprovisionamiento de configuración general:

Un archivo de configuración general se almacena en un servidor, lo que permite que todos los dispositivos relacionados descarguen el mismo archivo para actualizar los parámetros.

- Provisión de configuración basada en MAC:

Los archivos de configuración basados en MAC son específicos para dispositivos individuales, identificados por sus direcciones MAC únicas. Los archivos cuyo nombre coincida con la dirección MAC del dispositivo se compararán automáticamente antes de descargarlos para el aprovisionamiento.

Nota:

- Los archivos de configuración deben estar en formato CFG.
- El nombre del archivo de configuración general para la transferencia por lotes varía según el modelo.
- El archivo de configuración basado en MAC recibe el nombre de su dirección MAC.
- Los dispositivos accederán primero a los archivos de configuración general antes que a los basados en MAC si ambos tipos están disponibles.
- Puede hacer clic aquí para ver el formato y los pasos detallados.

Programación de AutoP

Akuvox le proporciona diferentes métodos de AutoP que permiten al dispositivo realizar el aprovisionamiento por sí mismo de acuerdo con la programación.

Para configurarlo, vaya a la interfaz web Sistema > Autoaprovisionamiento > Autoaprovisionamiento automático.

- Modo:
  - Encender: El dispositivo realizará el aprovisionamiento automático cada vez que se inicie.
  - Repetidamente: El dispositivo realizará el aprovisionamiento automático según el horario que se configure.
  - Encendido + Repetidamente: Combina el modo Encendido y el modo Repetidamente que permitirá al dispositivo realizar el aprovisionamiento automático cada vez que arranque o según la programación.
  - Repetición horaria: El dispositivo realizará el aprovisionamiento automático cada hora.

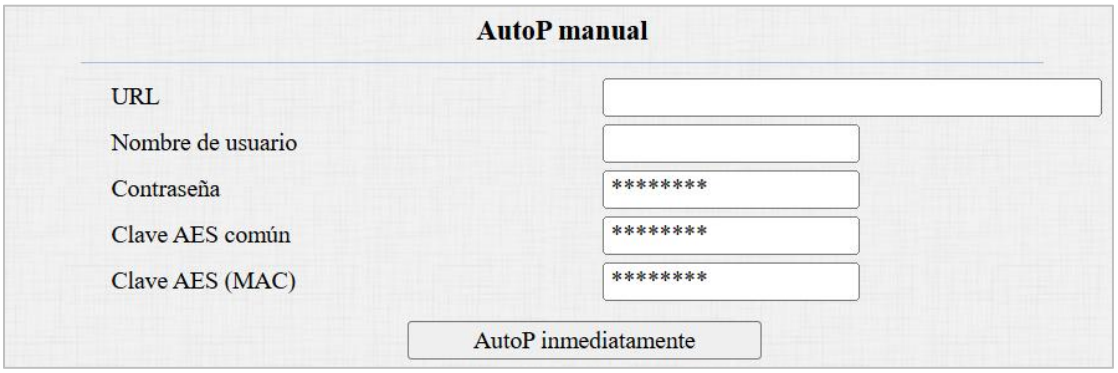
Aprovisionamiento Estático

Puede configurar manualmente una URL de servidor específica para descargar el firmware o el archivo de configuración. Si se configura un programa de autoaprovisionamiento, el dispositivo realizará el autoaprovisionamiento a una hora específica según el programa de autoaprovisionamiento que haya configurado. Además, TFTP, FTP, HTTP y

HTTPS son los protocolos que se pueden utilizar para actualizar el firmware y la configuración del dispositivo.

Para configurarlo, descargue primero la plantilla en Sistema > Autoaprovisionamiento > Interfaz automática AutoP.

Configure el servidor Autop en la sección Autop manual.



- URL: Especifique la dirección del servidor TFTP, HTTP, HTTPS o FTP para el aprovisionamiento.
- Nombre de usuario: Introduzca el nombre de usuario si el servidor necesita un nombre de usuario para acceder.
- Contraseña: Introduzca la contraseña si el servidor necesita una contraseña para acceder.
- Clave AES común: Se utiliza para que el intercomunicador descifre los archivos de configuración general de Autop.
- Clave AES (MAC): Se utiliza para que el Videoportero descifre el archivo de configuración Autop basado en MAC.

Nota:

- AES como un tipo de cifrado debe ser configurado sólo cuando el

archivo de configuración está cifrado con AES.

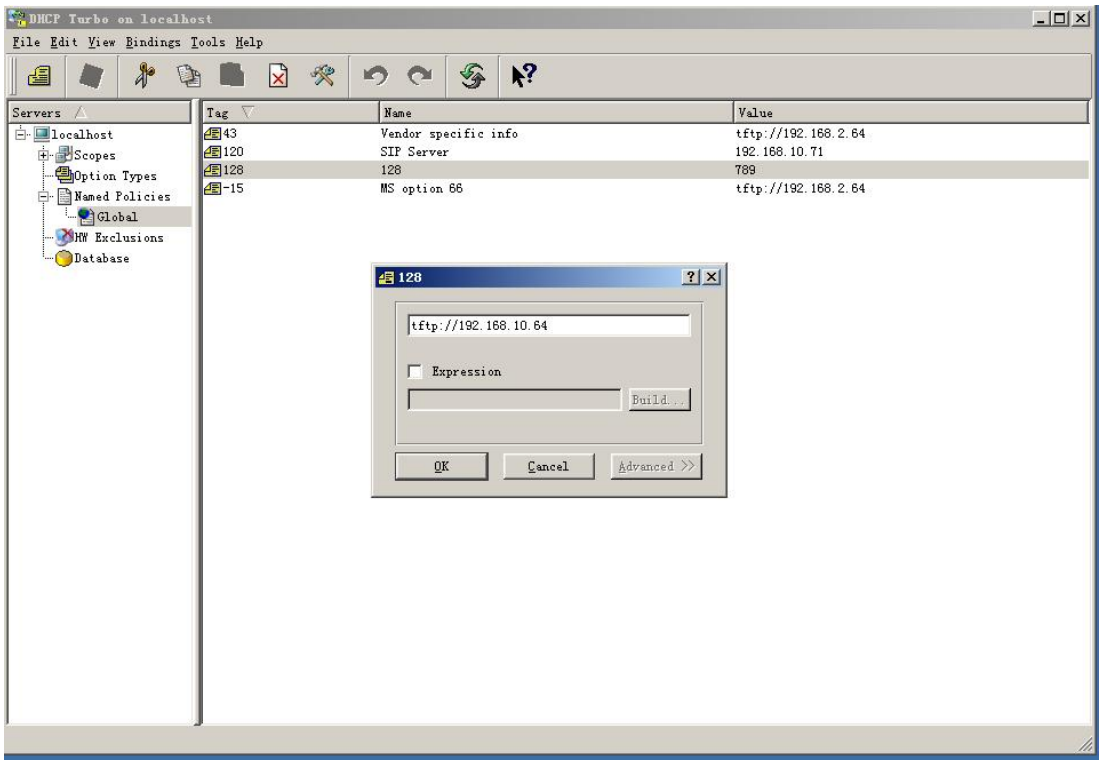
- Formato de la dirección del servidor:
  - TFTP: tftp://192.168.0.19/
  - FTP: ftp://192.168.0.19/(permite inicio de sesión anónimo)
  - ftp://username:password@192.168.0.19/(requiere nombre de usuario y contraseña)
- HTTP: http://192.168.0.19/(utilice el puerto 80 por defecto)
  - http://192.168.0.19:8080/(utilice otros puertos, como el 8080)
- HTTPS: https://192.168.0.19/(utilice el puerto 443 por defecto)

Consejo:

Akuvox no proporciona un servidor especificado por el usuario. Por favor, prepare usted mismo el servidor TFTP/FTP/HTTP/HTTPS.

Configuración del Aprovisionamiento DHCP

La URL de aprovisionamiento automático también se puede obtener utilizando la opción DHCP que permite al dispositivo enviar una solicitud a un servidor DHCP para un código de opción DHCP específico. Si desea utilizar la opción personalizada definida por los usuarios con códigos de opción que van de 128 a 255), deberá configurar la opción personalizada DHCP en la interfaz web.



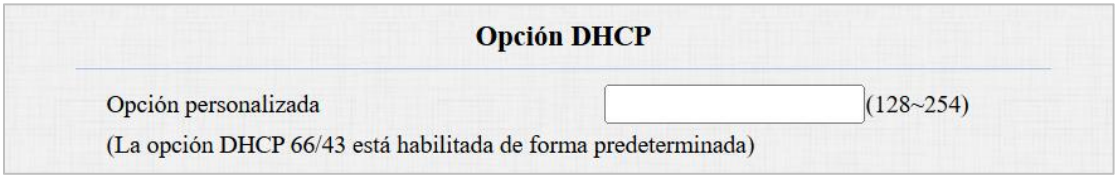
Nota:

El tipo de Opción Personalizada debe ser una cadena. El valor es la URL del servidor TFTP.

Configure DHCP Autop con el modo “Power On” y exporte la plantilla Autop para editar la configuración.

Descargue la plantilla en Sistema > AutoP > AutoP Automático.

A continuación, configure el DHCP.

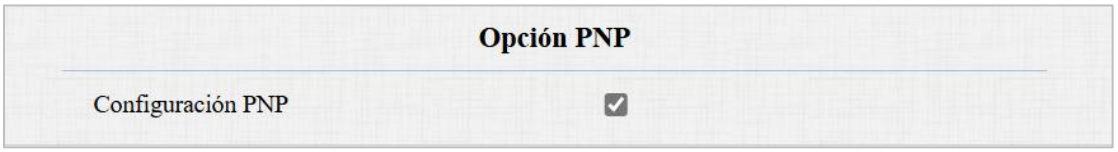


- Opción personalizada: Introduzca el código DHCP que coincida con la URL correspondiente para que el dispositivo encuentre el servidor de archivos de configuración para la configuración o actualización.
- Opción DHCP 66: Si no se configura ninguna de las opciones anteriores, el dispositivo utilizará automáticamente la Opción DHCP 66 para obtener la URL del servidor de actualización. Esto se hace dentro del software y el usuario no necesita especificarlo. Para que funcione, es necesario configurar el servidor DHCP para la opción 66 con la URL del servidor actualizado en él.
- DHCP Opción 43: Si el dispositivo no obtiene una URL de la opción 66 de DHCP, utilizará automáticamente la opción 43 de DHCP. Esto se hace dentro del software y el usuario no necesita especificarlo. Para que funcione, es necesario configurar el servidor DHCP para la opción 43 con la URL del servidor actualizada.

Configuración PNP

Plug and Play (PNP) es una combinación de soporte de hardware y software que permite a un sistema informático reconocer y adaptarse a los cambios de configuración de hardware con poca o ninguna intervención del usuario.

Configúrelo en la interfaz web Sistema > Autoaprovisionamiento > Opción PNP.



Depurar

Registro del Sistema

Los registros del sistema pueden utilizarse con fines de depuración.

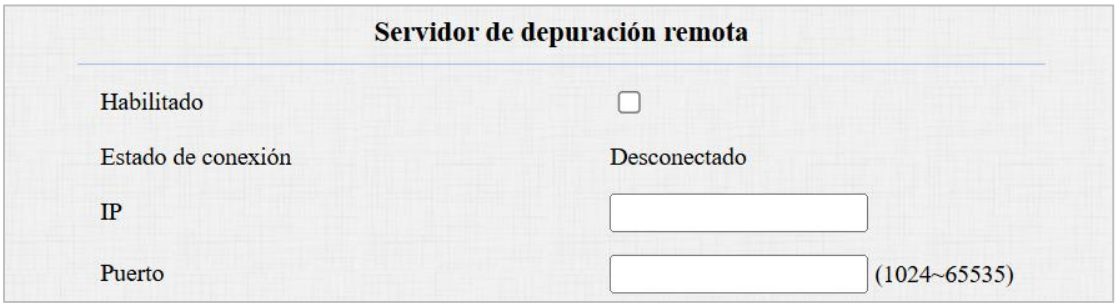
Para configurarlo, vaya a la interfaz web Sistema > Mantenimiento.

- Nivel de registro: Seleccione los niveles de registro de 1 a 7 niveles. Usted será instruido por el personal técnico de Akuvox acerca del nivel de registro específico a ser ingresado para propósitos de depuración. El nivel de registro por defecto es 3. Cuanto más alto sea el nivel, más completo será el registro.
- Exportar registro: Haga clic en la pestaña Exportar para exportar un archivo de registro de depuración temporal a un PC local.
- Servidor del Sistema Remoto: Establezca la dirección del servidor remoto para recibir el registro del dispositivo. La dirección del servidor remoto será proporcionada por el soporte técnico de Akuvox.
- Puerto del sistema remoto: Establezca el puerto del servidor del sistema remoto.

Servidor de Depuración Remoto

Cuando el dispositivo tiene un problema, puede utilizar el servidor de depuración remoto para acceder al registro del dispositivo de forma remota con fines de depuración.

Para configurarlo, vaya a la interfaz web Sistema > Mantenimiento.

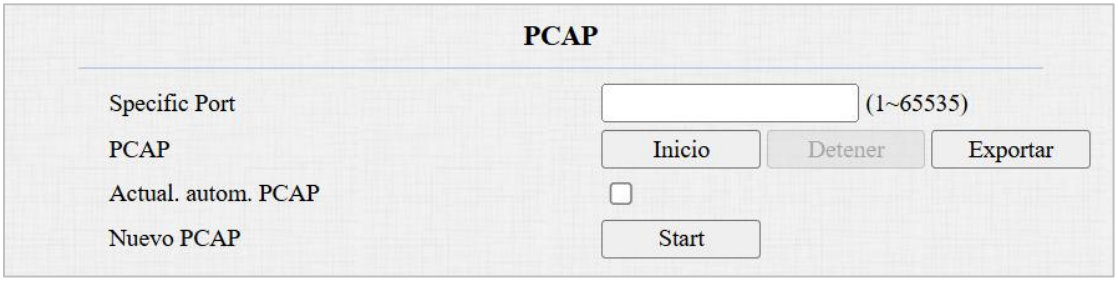


- Estado de la conexión: Muestra el estado de la conexión entre el dispositivo y el servidor.
- IP: Introduzca la dirección IP del servidor.
- Puerto: Introduzca el puerto del servidor.

PCAP para Depuración

PCAP se utiliza para capturar el paquete de datos que entra y sale de los dispositivos con fines de depuración y solución de problemas.

Para configurarlo, vaya a la interfaz web Sistema > Mantenimiento.



- Puerto Específico: Seleccione los puertos específicos del 1-65535 para que sólo el paquete de datos del puerto específico pueda ser capturado. Puede dejar el campo en blanco por defecto.
- PCAP: Haga clic en las pestañas Iniciar y Detener para capturar un cierto rango de paquetes de datos antes de hacer clic en la pestaña Exportar para exportar los paquetes de datos a su PC Local.
- Actualización Automática de PCAP Habilitada: Si está activada, entonces el PCAP continuará capturando paquetes de datos incluso después de que los paquetes de datos alcancen su capacidad máxima de 1M. Si está

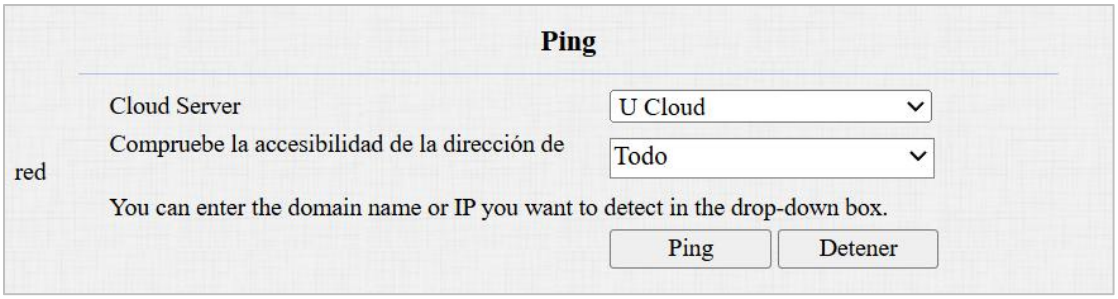
desactivada, el PCAP dejará de capturar paquetes de datos cuando el paquete de datos capturado alcance la capacidad máxima de captura de 1MB.

- Nuevo PCAP: Haga clic en Iniciar para capturar un paquete de datos más grande.

Ping

El dispositivo permite verificar la accesibilidad del servidor de destino.

Para configurarlo, vaya a la interfaz Sistema > Mantenimiento > Ping.



  - Servidor en la nube: El servidor a verificar.
- Verificar la accesibilidad de la dirección de red: El tipo de servicio.

Copia de Seguridad

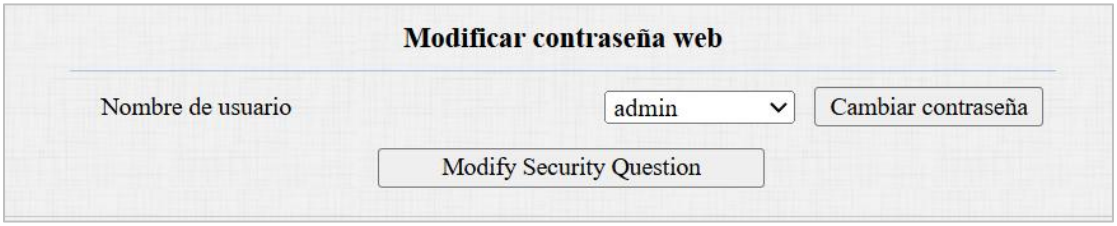
Puede importar o exportar archivos de configuración cifrados a su PC local.

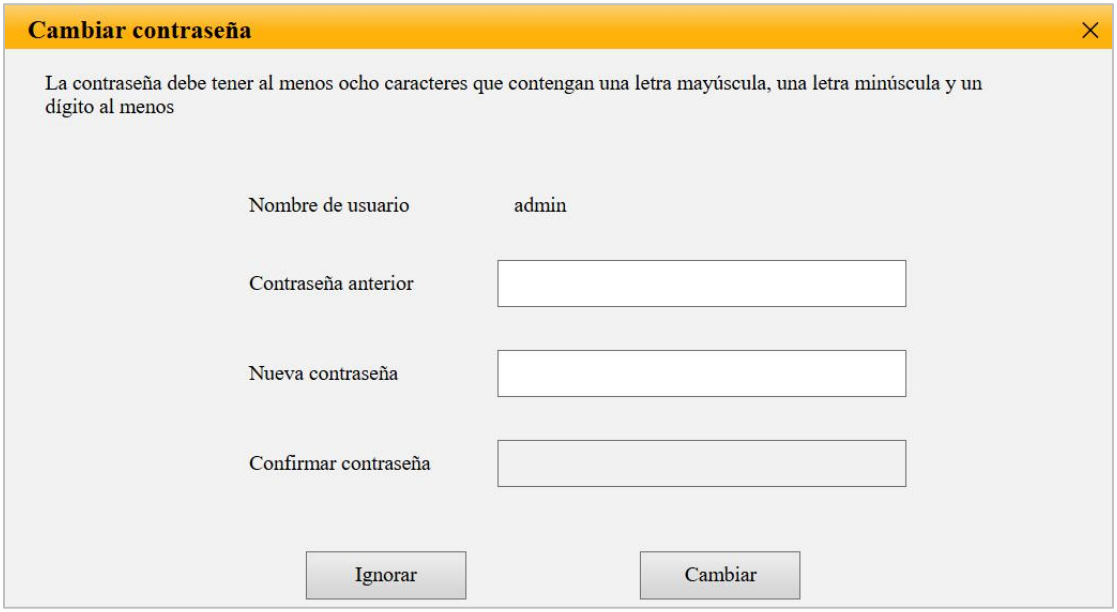
Exporte el archivo en la interfaz Sistema > Mantenimiento > Otros.

Modificación de la Contraseña

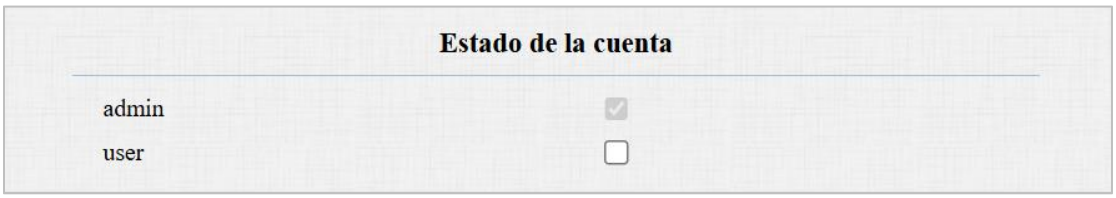
Puede modificar la contraseña web del dispositivo tanto para la cuenta de administrador como para la cuenta de usuario.

Para configurarla, vaya a la interfaz Sistema > Seguridad > Modificación de la contraseña web. Haga clic en Modificar contraseña.





Para activar o desactivar la cuenta de usuario, desplácese hasta la sección Estado de la cuenta.



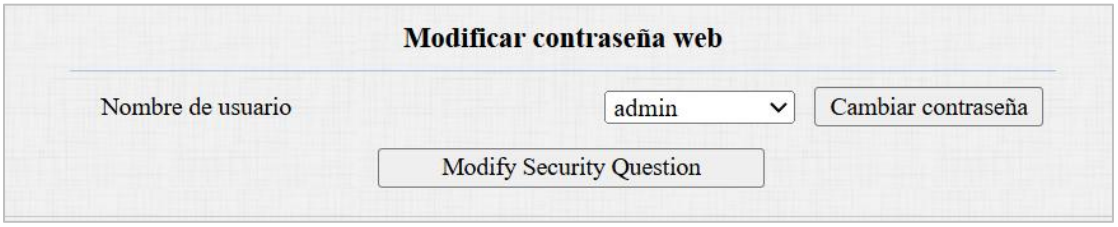
La contraseña por defecto de la cuenta de usuario es **user**.

Modificar las Preguntas de Seguridad

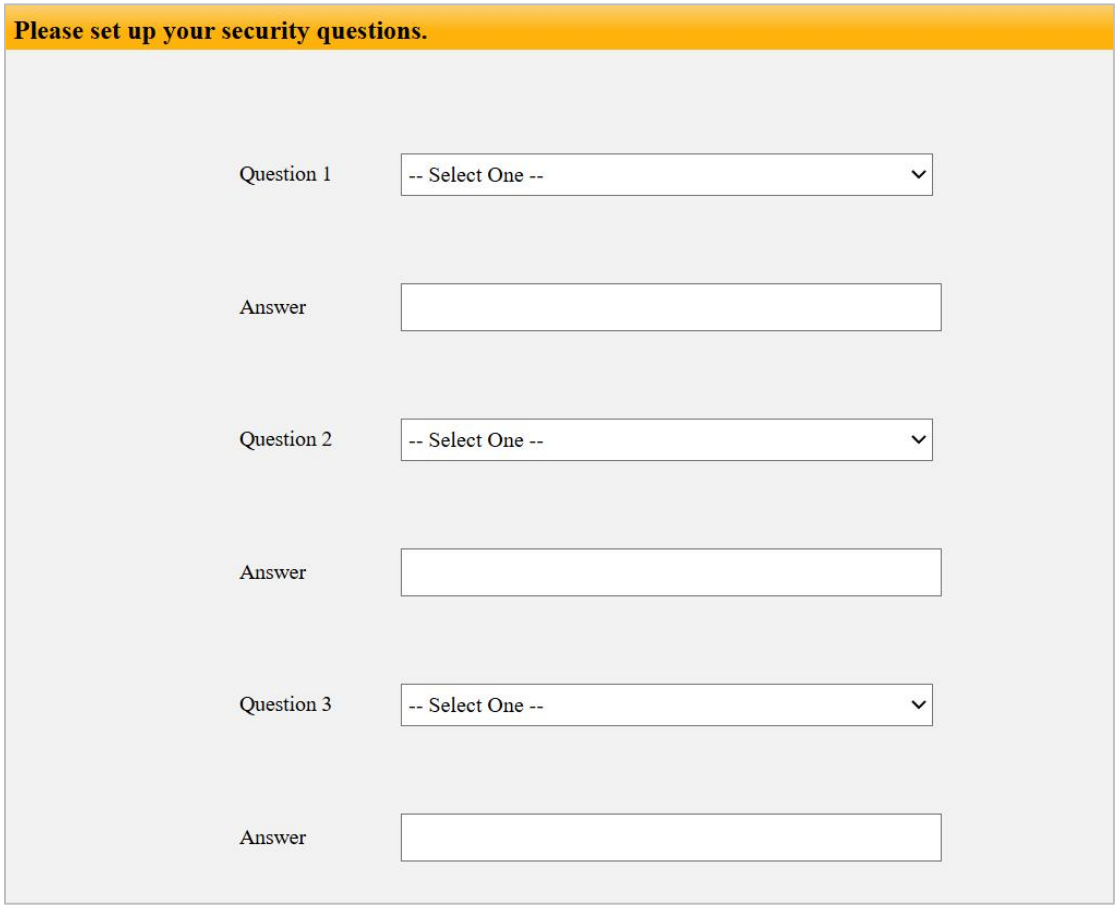
Las preguntas de seguridad le permiten restablecer la contraseña web si la olvida. Después de configurar las preguntas de seguridad, puede hacer clic en «Olvidar contraseña» en la interfaz de inicio de sesión, introducir las respuestas y aparecerá una ventana de restablecimiento de contraseña.

Si no ha configurado las preguntas de seguridad, al hacer clic en «Responder a las preguntas de seguridad» se le pedirá que se ponga en contacto con su proveedor de servicios.

Para configurarla, vaya a la interfaz Sistema > Seguridad > Modificar contraseña web.



Debe introducir la contraseña correcta antes de modificar las preguntas de seguridad.

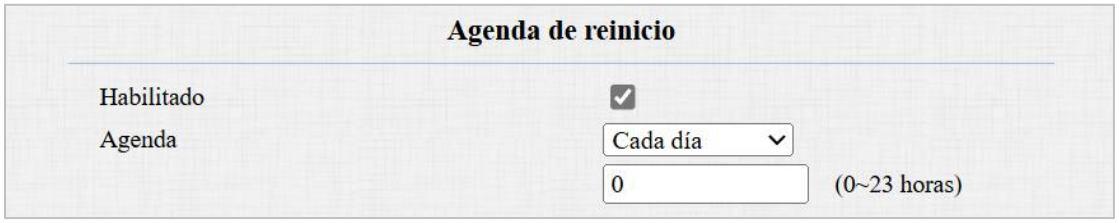


Reinicio y Restablecimiento del Sistema

Reiniciar

Reinicie el dispositivo en la interfaz web Sistema > Actualizar.

Puede configurar el programa de reinicio en la interfaz web Sistema > Autoaprovisionamiento > Programación de reinicio.



Restablecer

Reinicie el dispositivo en la interfaz web Sistema > Actualizar.