Akuvox
Open A Smart World

Videoportero Akuvox S532

Guía para el Administrador

Akuvox
Open A Smart World

Gracias por elegir los videoporteros Akuvox serie S532. Este manual está dirigido a los administradores que necesitan configurar de forma correcta el videoportero. Este manual es aplicable a la versión 532.30.10.238, y proporciona todas las configuraciones para las funciones y características del videoportero Akuvox. Visite el sitio web 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

- LCD de 2.8”
- Superficie de Aluminio
- Sistema operativo Linux
- Teclado numérico
- Múltiples métodos de control de acceso (RFID, NFC, Bluetooth)
- Salida IP a Audio/video analógico (opcional)
- Protección IK08 e IP66

Akuvox
Open A Smart World

Especificaciones del Modelo

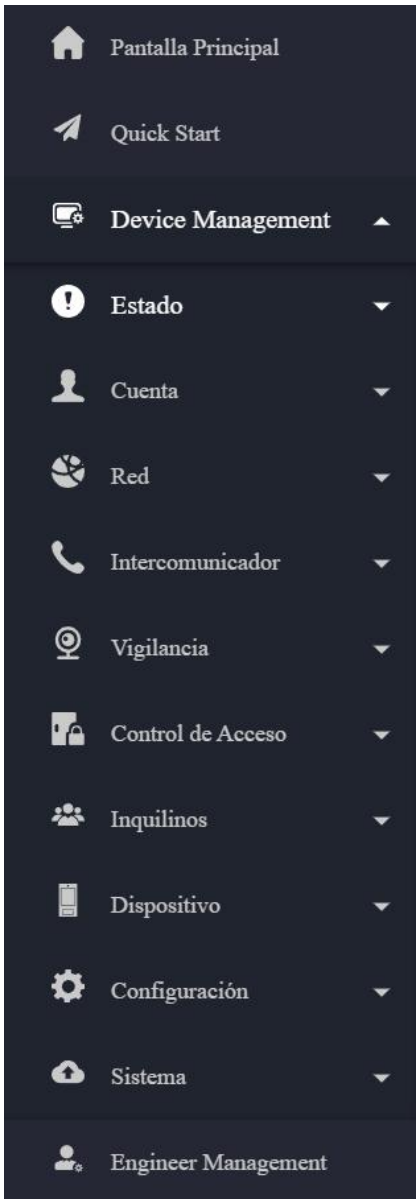
S532	
Cámara	x 1
LEDs IR	✓
Lector de tarjetas	✓
Pantalla táctil	X
Ethernet	x 1, PoE+(802.3at)
Wiegand	x 1
RS485	x 1
Relé	x 2
Entradas	x 4
Audio analógico	Opcional
Vídeo analógico	Opcional
Ranura para tarjeta TF	x 1
Salida de línea	x 1
Entrada de alimentación	x 1, 12V/2A
Micrófono	x 1
Altavoz	x 1
BLE	✓

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

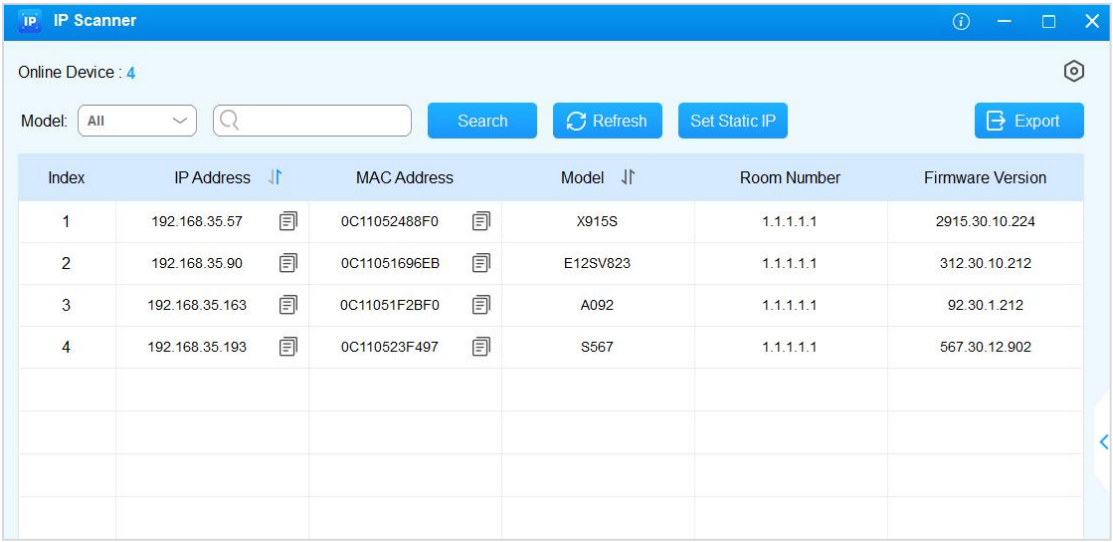


Acceder al Dispositivo

Se puede acceder a la configuración del sistema del videoportero desde el dispositivo o desde su interfaz.

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 del Dispositivo

Pulse «*2396#» para acceder a la configuración de administración del dispositivo, incuyendo:

- información del sistema;
- tarjeta admin, código admin y gestión del código de servicio;
- ajustes de red del sistema;
- reinicio del sistema.

Puede comprobar la IP, MAC y versión de firmware del dispositivo en la pantalla Información del sistema.

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 seleccionar el idioma de la pantalla LCD del dispositivo en la interfaz Configuración > Hora/Idioma. Actualmente, admite inglés, español, francés, polaco y turco.

Puede cambiar el idioma de la web en la esquina superior derecha. Actualmente admite inglés, español, francés, polaco y turco.

Para personalizar los nombres de configuración y el texto de los avisos, debe exportar y editar el archivo .json antes de cargarlo en el dispositivo.

Configúrelo en la interfaz Configuración > Hora/Idioma > Lenguaje personalizado.

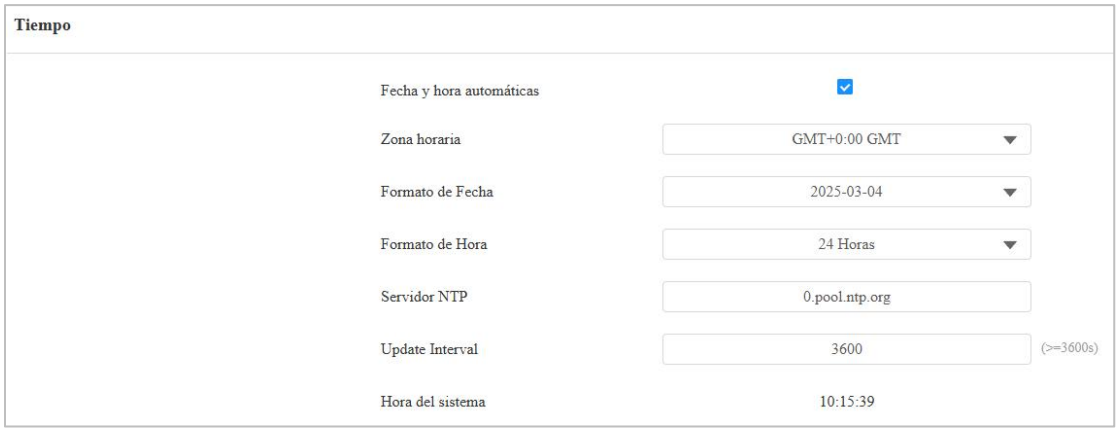
Nota:

- El archivo cargado para personalizar el lenguaje web debe estar en formato .json.
- El archivo cargado para personalizar el lenguaje LCD debe estar en formato .xml.

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.



- Fecha y hora automáticas: Cuando está activada, la fecha y la hora del dispositivo se configuran y sincronizan automáticamente con la zona horaria predeterminada y el servidor NTP (“Network Time Protocol”).
- Servidor NTP: La dirección del servidor NTP.
- Intervalo de actualización ("Update Interval"): El intervalo entre dos peticiones NTP consecutivas.

LED y LCD

Ajuste del LED Infrarrojo

El LED infrarrojo está diseñado principalmente para reforzar la luz para el reconocimiento facial por la noche o en un entorno oscuro.

Para configurar el LED, vaya a la interfaz web Dispositivo > Luz > Configuración de LED.

- Modo:
  - Auto: Enciende el LED infrarrojo automáticamente en función del valor mínimo y máximo de la fotorresistencia.
  - Siempre encendido: Activa el LED infrarrojo.
  - Siempre apagado: Desactiva el LED infrarrojo.
  - Programar: Enciende el LED infrarrojo basándose en el horario. Especifique la hora de inicio y la hora de finalización cuando seleccione esta opción.
- Configuración del fotorresistor: Establezca el valor mínimo y máximo de la fotorresistencia para controlar automáticamente el ENCENDIDO-APAGADO de la luz LED infrarroja. Si el valor de la fotorresistencia es inferior al umbral mínimo, apáguela. Si el valor de la fotorresistencia es mayor que el umbral máximo, enciéndala.
- Fotorresistor actual: Haga clic en Leer para obtener los datos de la fotorresistencia actual.
- Brillo del LED IR: Ajuste el brillo del LED IR del nivel 0 al 10. Cuanto más alto sea el nivel, más brillante será.

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 web Dispositivo > Luz > LED del área de lectura de tarjetas.

- Hora de inicio- Hora de finalización (H): Introduzca el tiempo de validez de la iluminación LED, por ejemplo, si el tiempo se establece de 8-0 (Hora de inicio- Hora de finalización), significa que la luz LED permanecerá encendida durante el tiempo comprendido entre las 8:00 am y las 12:00 pm durante un día (24 horas).

Control de los LED del Teclado

Puede activar o desactivar la iluminación LED del teclado. También puede establecer una hora específica para encender la luz.

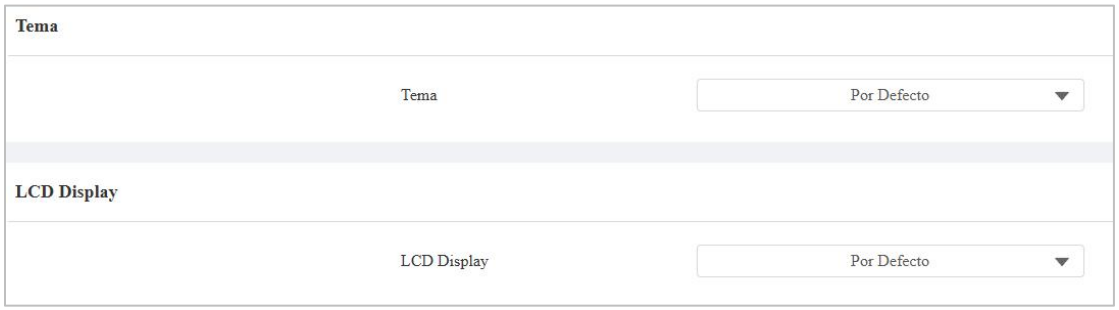
Para configurarlo, vaya a la interfaz web Dispositivo > Luz > LED del Área del Teclado.

- Hora de inicio- Hora de finalización (H): Introduzca el tiempo de validez de la iluminación LED, por ejemplo, si el tiempo se establece de 8-0 (Hora de inicio- Hora de finalización), significa que la luz LED permanecerá encendida durante el tiempo comprendido entre las 8:00 am y las 12:00 pm durante un día (24 horas).

Pantalla de Inicio

Existen tres tipos de temas de visualización de la pantalla de inicio para diferentes aplicaciones.

Para configurarlo, vaya a la interfaz Configuración > Teclado/Pantalla.



- Tema:
  - Por defecto: Muestra las instrucciones para realizar llamadas por números de habitación, abrir puertas introduciendo PIN y entrar en la pantalla de la lista de directorios.
  - Texto personalizado: Mostrar texto personalizado en la pantalla de inicio. Cuando se seleccione, introduzca el contenido en el cuadro Texto.
  - Directorio: Muestra la lista del directorio.
- Pantalla LCD: Disponible para el tema Por Defecto.
  - Ocultar directorio: Oculta las instrucciones para entrar en la pantalla de la lista del directorio.
  - Ocultar directorio y número de habitación: Mostrar sólo las instrucciones para abrir puertas introduciendo PINs.

Configuración del Salvapantallas

Puede establecer la duración del salvapantallas, así como el tiempo de apagado de la pantalla, tanto para la protección de la pantalla como para la reducción de energía.

Para configurarlo, vaya a la interfaz web **Dispositivo > LCD**.

- Tiempo de reposo automático: Dentro del tiempo de reposo automático, si el dispositivo no detecta ninguna operación o nadie se acerca, empezará a mostrar el salvapantallas. Oscila entre 5 segundos y 30 minutos. Por defecto es de 15 segundos.
- Modo de Protector de Pantalla:
  - Imagen: Muestra la imagen por defecto o la imagen cargada.
  - Desactivado: El dispositivo no entrará en Modo Salvapantallas.
- Tiempo de Salvapantallas: Tiempo de duración del salvapantallas. La pantalla se oscurecerá una vez transcurrido el tiempo.
- Modo de Despertar:
  - Auto: La pantalla puede despertarse cuando alguien se acerca sin necesidad de tocarla.
  - Manual: Tocar y despertar la pantalla.

Cargar Protector de Pantalla

Puede cargar imágenes de salvapantallas en el dispositivo con fines publicitarios o para disfrutar de una mayor experiencia visual.

Vaya a la interfaz web Dispositivo > LCD.

- Tiempo de transición: intervalo de tiempo de conmutación entre dos imágenes.

Nota:

El archivo debe estar en formato .jpg con un tamaño máximo de 1M.

Brillo de Retroiluminación de la Pantalla

Puede ajustar el brillo de la retroiluminación de la pantalla y del salvapantallas.

Navega a la interfaz web Dispositivo > LCD.

- Modo: Cuando se selecciona Auto, el brillo de la retroiluminación de la pantalla se ajustará automáticamente.

Nota:

- El brillo de la retroiluminación tiene tres modos, Día, Noche y Alto.

Están determinados por la fotorresistencia.

- Si la fotorresistencia actual es inferior a la fotorresistencia mínima preestablecida, el dispositivo está en modo Alto.
- Si el valor de la corriente está entre la fotorresistencia mínima y la máxima, el dispositivo está en modo Día.
- Si el valor de la corriente es superior a la fotorresistencia máxima, el aparato está en modo Noche.

- Brillo de la retroiluminación (Día): El valor de brillo oscila entre 1 y 255. El valor por defecto es 200. Cuanto mayor sea el valor, más brillante será la pantalla.
- Brillo de Retroiluminación del Salvapantallas (Día): La luz de fondo para el salvapantallas durante el día con el valor que oscila entre 1-255.
- Brillo de Retroiluminación (Noche): La luz de fondo por la noche con un valor que oscila entre 1-255.
- Brillo de la retroiluminación del salvapantallas (Noche): La retroiluminación del salvapantallas por la noche con el valor comprendido entre 1-255.
- Brillo de la retroiluminación (Alto): La luz de fondo con un valor que oscila entre 1-255.
- Brillo de la retroiluminación del salvapantallas (Alto): La luz de fondo del salvapantallas con un valor que oscila entre 1-255.

Control de Temperatura de la Pantalla LCD

Para garantizar el funcionamiento normal del videoportero en entornos con bajas temperaturas, puede calentar la pantalla LCD del dispositivo de acuerdo con la configuración del control de calor.

Vaya a Videoportero > Básico.

- Habilitado: Esta función no puede utilizarse en modo de bajo consumo. Es necesario utilizar POE+ para garantizar un suministro de energía suficiente.
- Umbral de Calor: Cuando la temperatura del dispositivo alcance el umbral, el dispositivo empezará a calentarse.
- Temperatura actual: Haga clic en Leer para adquirir la temperatura actual del dispositivo.

Volumen y Tono

Las configuraciones de volumen y tono incluyen el volumen del micrófono, el volumen del teclado, el volumen del altavoz, el volumen de la alarma antisabotaje y la configuración del tono de puerta abierta. Además, puede cargar el tono para enriquecer la experiencia del usuario.

Configuración del Volumen

Puede configurar el volumen del micrófono según sus necesidades para la notificación de puerta abierta. Además, también puede configurar el volumen de la alarma antimanipulación cuando se produce una extracción no deseada del terminal de control de acceso.

Configure los volúmenes en la interfaz web Dispositivo > Audio.

- Volumen del micrófono(Proxy): El volumen del micrófono del conmutador analógico.
- Volumen analógico: El volumen del conmutador analógico durante una llamada.

Cargar Archivos de Tonos

Puede cargar el tono para la apertura de puerta o para el fallo de apertura de puerta en la interfaz web del dispositivo.

Cargue los tonos en la interfaz web **Dispositivo > Audio**.

Nota:

Formato de archivo: wav; Tamaño: < 200KB; Frecuencia de muestreo: 16000, Bits: 16.

Configuración de Red

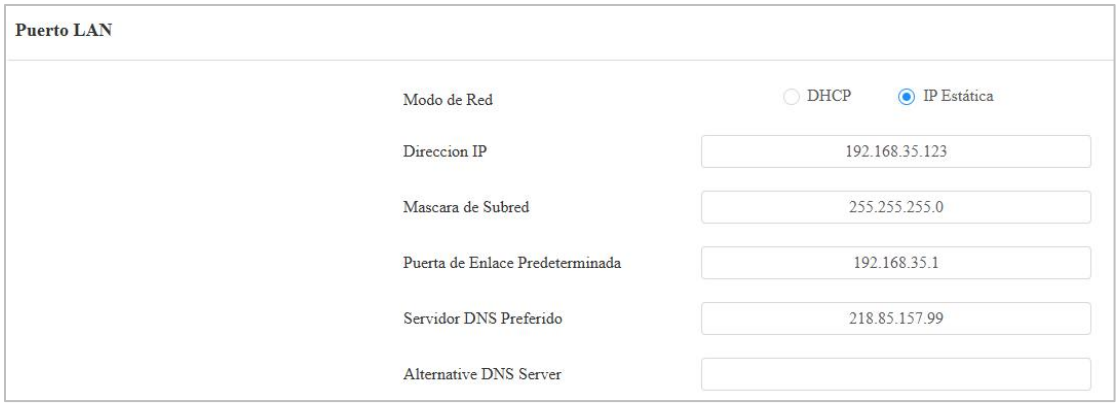
Estado de Red

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.

También puede configurar la red en el dispositivo. Pulse ***2396#** en el teclado del dispositivo y pulse 3 y 1 para acceder a la pantalla de configuración de red.

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.
- 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 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).

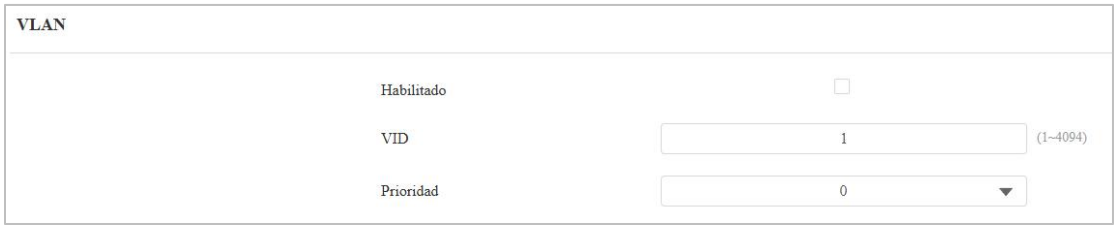
Para configurar SNMP, vaya a la interfaz web Red > Avanzado.

- 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 de QoS

La calidad de servicio (QoS, por su sigla en inglés) es la capacidad de una red para ofrecer un mejor servicio a determinadas comunicaciones de red utilizando diversas tecnologías. Sirve como mecanismo de seguridad en las redes, abordando problemas como la latencia y la congestión de la red. Garantizar la calidad del servicio es crucial para redes con capacidad limitada, sobre todo para aplicaciones multimedia como VoIP e IPTV. Estas aplicaciones suelen requerir una velocidad de transmisión constante y son sensibles a los retrasos.

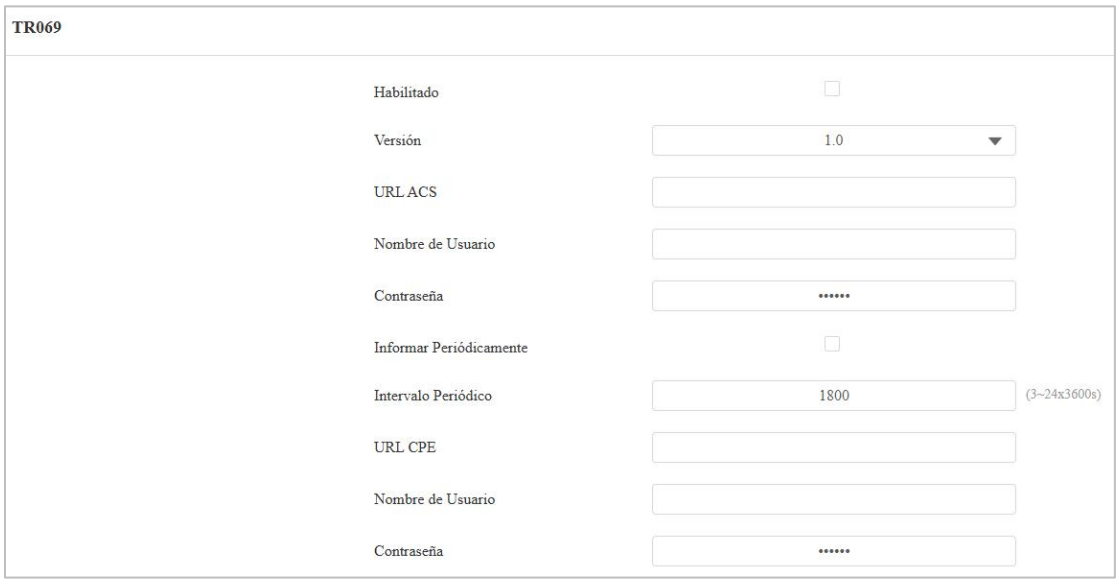
Para configurar la QoS, vaya a la interfaz web Red > Avanzado.

- SIP QoS: SIP QoS puede analizarse registrando una cuenta y capturando paquetes SIP.
- QoS de voz: La QoS de voz puede ser analizada durante una llamada capturando y examinando paquetes RTP.
- Calidad del servicio de señalización RTSP: Puede ser analizada usando VLC y capturando paquetes RTP.
- Calidad del servicio de Medios RTSP: Puede ser analizada visualizando el stream en VLC y capturando paquetes RTP.

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.

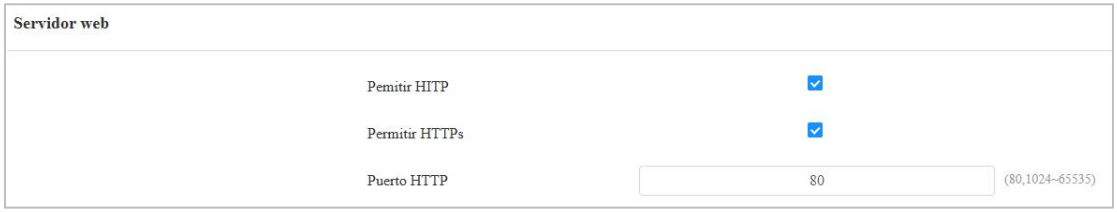


- Versión: Seleccione la versión TR069 compatible (versión 1.0 o 1.1).
- URL ACS/CPE: La dirección URL para ACS o CPE. ACS es la abreviatura de los servidores de autoconfiguración en el lado del servidor, y CPE es la abreviatura de los equipos locales del cliente como dispositivos del lado del cliente.
- 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.



- Puerto HTTP: El puerto para el método de acceso HTTP. 80 es el puerto por defecto.

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.

To Para configurar NAT, vaya a la interfaz Cuenta > Básico > NAT.

- IP del Servidor STUN: 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.

Configuración de Llamadas de Videoportero

Llamadas IP y 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.
- Para designar la cuenta que se utilizará para las llamadas salientes, seleccione el número de cuenta para los contactos o los prefijos del plan de marcación en sus ajustes.

- Cuenta Habilitada: Marque esta opción para activar la cuenta SIP

registrada.

- Etiqueta en pantalla: La etiqueta del dispositivo que se mostrará en la pantalla del dispositivo.
- Nombre para mostrar: El nombre del dispositivo que se mostrará en el dispositivo al que se llama.
- Nombre de Registro: 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 Alternativo: 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.

Configuración Analógica

Los usuarios pueden utilizar un conmutador analógico para responder a las llamadas realizadas al portero automático después de conectarlo a éste.

Configúrelo en la interfaz web Videoportero > Básico > Configuración Analógica.

- Adaptador: La marca del conmutador analógico al que se conecta el portero automático. Puede elegir entre Akuvox, Vizit, Cyfral, Eltis, Metakom y Lascomex.

Configuración de Contactos

Gestionar Grupos de Contactos

Puede crear y editar un grupo de contactos. El grupo de contactos se utilizará cuando añada un usuario.

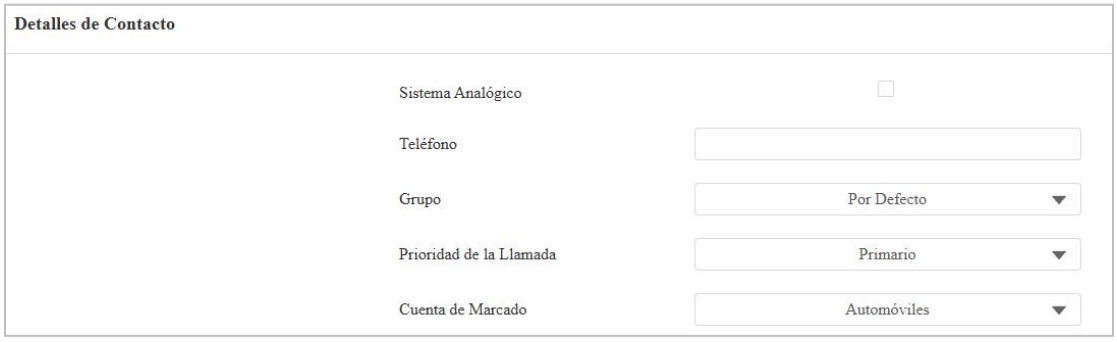
Configúrelo en la interfaz web Directorio > Usuario > Grupo. Haga clic en +Agregar para añadir un grupo. El dispositivo permite añadir hasta 1000 grupos.

Configurar los Datos de Contacto

Añada la información de contacto de los usuarios en la interfaz web Directorio > Usuario. El dispositivo permite añadir hasta 10.000 usuarios. Haga clic en +Agregar para agregar un usuario.

Establezca el ID y el nombre del usuario.

Busque la sección **Detalles de Contacto**.



- Sistema analógico: Cuando está activado, configura el número analógico y los usuarios pueden llamar al conmutador analógico.
- Número analógico: El número del conmutador analógico.
- Sustituir analógico: Configuración opcional. El número corto sustituye al número analógico. Los usuarios pueden llamar al microteléfono analógico introduciendo el número corto en el teclado del portero automático.
- Modo Analógico: Directo significa que el conmutador analógico está conectado al portero automático a través de cables. Proxy significa que el interruptor analógico no está conectado al portero automático a través de cables y cuando se selecciona esta opción, es necesario rellenar la dirección proxy analógica.
- Dirección proxy analógica: La dirección IP del portero automático en modo Proxy.
- Grupo: Ponga el contacto en un grupo de contactos deseado.
- Prioridad de llamada: Establezca la prioridad de la llamada entre tres opciones: Primaria, Secundaria y Terciaria. Por ejemplo, si establece la prioridad de llamada para uno de los contactos de un grupo de contactos específico como Primaria, entonces el contacto será el primero en ser llamado entre todos los contactos cuando alguien pulse sobre el grupo de contactos para realizar una llamada de grupo.
- Cuenta de marcación: La cuenta para realizar la llamada.

Consejo:

Para ver los pasos detallados de la configuración de la función analógica, consulte:
Integración entre el S532 y las Unidades Contestadoras Akuvox.

Visualización de la Lista de Contactos

Puede personalizar la visualización de la lista de contactos para adaptarla a las preferencias operativas y visuales de los usuarios.

Configúrelo en la interfaz Directorio > Configuración del directorio.

- Mostrar Contactos de la Nube: Se pueden mostrar los contactos sincronizados desde la nube de SmartPlus.
- Modo de Visualización de Contactos:
  - Todos los contactos: Mostrar todos los contactos.
  - Sólo Grupos: Mostrar los grupos de contactos. Pulse el grupo deseado en la pantalla del dispositivo para realizar una llamada de grupo.
  - Visualización de contactos por grupo: Muestra los contactos por grupos. Pulse el grupo y los usuarios podrán ver los contactos que contiene.
  - No mostrar contactos: No se mostrarán ni los contactos ni los grupos.
- Ordenar Por:
  - Código ASCII: lista los inquilinos por sus nombres en la secuencia del código ASCII.
  - Número de habitación: lista los inquilinos según su número de habitación.
  - Importar lista: los inquilinos según su orden en el archivo importado.

- Control de Permisos de Llamada a la Nube: Esta opción se mostrará cuando el dispositivo esté conectado a SmartPlus Cloud. Decide si se vinculan los permisos del usuario de SmartPlus para abrir puertas y realizar llamadas.
  - Por ejemplo, cuando los usuarios no están autorizados a abrir puertas durante un tiempo específico y la función de Control de Permisos de Llamada a la Nube está activada, su SmartPlus App y/o monitores interiores no recibirán llamadas del portero automático.
  - Si esta función está desactivada, aunque los usuarios no puedan abrir las puertas, podrán recibir las llamadas.

Lista de Contactos en la Nube

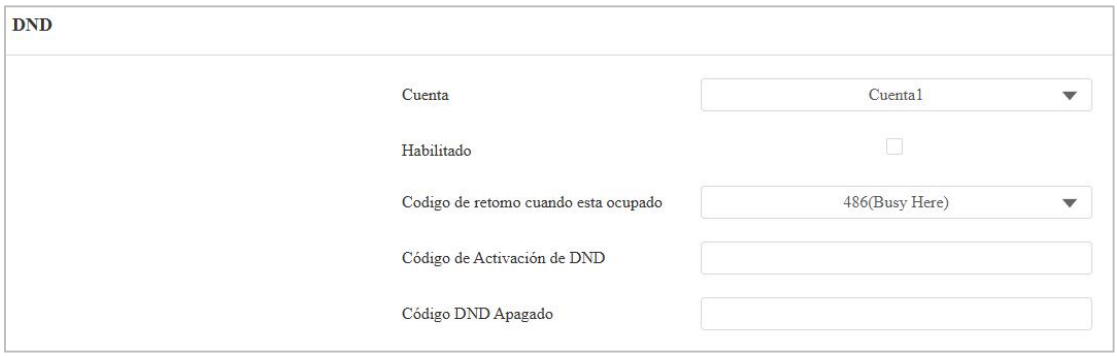
Cuando el dispositivo está conectado a SmartPlus Cloud, los contactos de la nube se mostrarán en Directorio > Ajustes de directorio > Lista de contactos de la nube.

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.



- Cuenta: La cuenta para aplicar la función DND.
- Código de retorno cuando está ocupado: Especifique el código que se envía a la persona que llama a través del servidor SIP cuando se rechaza una llamada entrante en modo DND.
- Código de Activación de DND: El código utilizado para activar DND en el servidor SIP.
- Código DND Apagado: El código utilizado para desactivar DND en el 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.

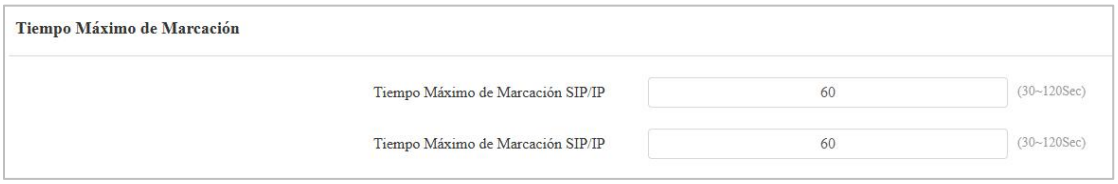
Para configurar la duración de la llamada, vaya a la interfaz web Interfono > Funciones de llamada.

- 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.

Tiempo Máximo de Marcación

El tiempo máximo de marcación es el límite de tiempo para las llamadas entrantes y/o salientes en el portero automático. Si se configura, el portero automático finalizará la llamada si nadie responde a la llamada dentro del tiempo preestablecido, tanto si es entrante como saliente.

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



- Tiempo máximo de marcación SIP/IP: Especifique la duración máxima de una llamada entrante. El videoportero finalizará automáticamente la llamada entrante si no se contesta en el tiempo preestablecido.
- Tiempo máximo de marcación SIP/IP: Especifique la duración máxima de una llamada saliente. El videoportero finalizará automáticamente la llamada saliente si el destinatario no responde en el tiempo preestablecido.

Configuración de 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 web

Videoportero > Funciones de llamada.

- Activado:
  - IP Directa: Esta función se aplica a las llamadas IP.
  - Cuenta1/2: Esta función se aplica a las llamadas SIP realizadas a la cuenta1/2.
- Retraso de Auto Respuesta: 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.

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 web Videoportero > Función de llamada.

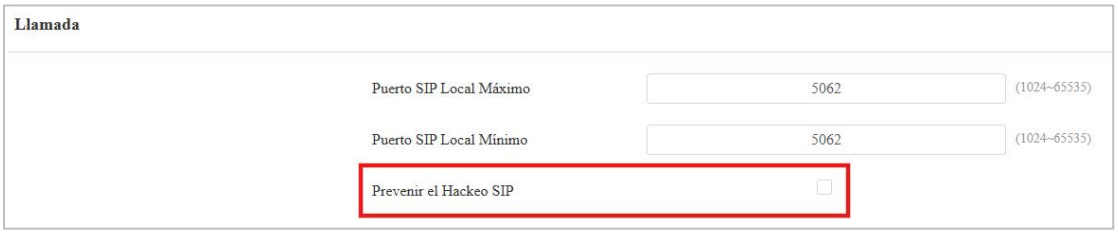
- Tipo: Especifica el método de desbloqueo de la puerta. Si se utiliza este método específico para desbloquear la puerta durante una llamada, el portero automático finalizará la llamada cuando se alcance el tiempo de colgado preestablecido.
- Tiempo de espera(Seg): Especifique el límite de tiempo de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

portero automático finalizará la llamada cuando se alcance el tiempo específico después de abrir la puerta.

Prevenir las Escuchas SIP

Las escuchas telefónicas por Internet son 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 el pirateo SIP es una técnica que impide que las llamadas SIP se vean comprometidas en Internet.

Para configurar esta función, vaya a la interfaz web Cuenta > Avanzado.



- Evitar el Hackeo SIP: Active esta función para recibir llamadas únicamente 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.

Marcación Rápida

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.
Puede crear hasta 16 números de llamada de grupo.

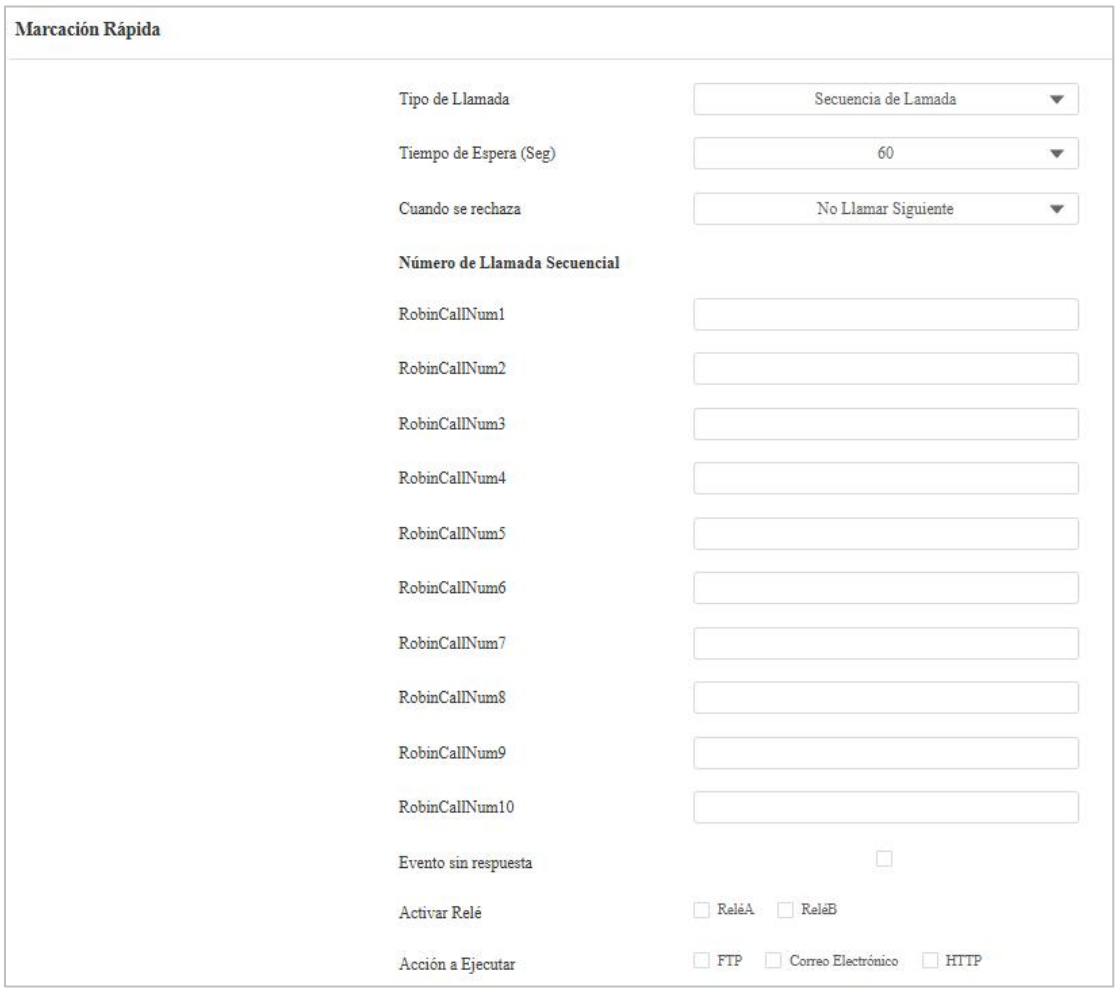
Para configurar la llamada de grupo, vaya a la interfaz web Videoportero > Básico.

- Tipo de llamada: Llamada de Grupo o Llamada de Secuencia.
- Cuando se rechaza:
  - Terminar sólo esta llamada: El dispositivo continuará llamando a otros números.
  - Terminar todas las llamadas: El dispositivo dejará de llamar.
- Número de llamada de grupo: Si introduce el número de llamada de grupo local, se llamará al número de grupo local en lugar de al número de llamada de grupo de SmartPlus.
- Evento Sin Respuesta: Cuando no se responda a la llamada, se activarán acciones.
- Activar Relé: Relé que se activará cuando no se conteste la llamada.
- Acción a Ejecutar: Acción(es) a ejecutar cuando la llamada no es atendida.

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.

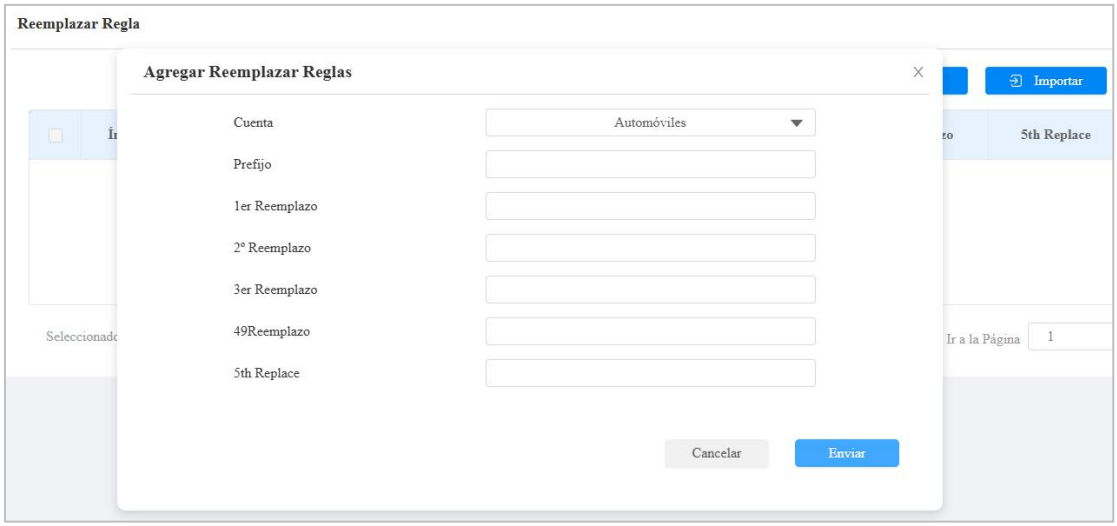


- Tipo de llamada: Llamada de Grupo o Llamada de Secuencia.
- Tiempo de espera (Seg): Establece el tiempo de espera de la llamada antes de llamar al siguiente interlocutor llamado cuando el primer interlocutor llamado no recibe la llamada dentro del tiempo de espera.
- Cuando se rechaza:
  - No llamar siguiente: El dispositivo dejará de llamar.
  - Llamar siguiente: El dispositivo continuará llamando a otros números.
- Evento Sin Respuesta: cuando no se contesta la llamada, se activan acciones.
- Activar Relé: relé(s) que se activarán cuando no se conteste la llamada.
- Acción a Ejecutar: Acción(es) a ejecutar cuando la llamada no es atendida.

Plan de Marcación

La función de sustitución de números de marcación simplifica los números de marcación largos y complejos del dispositivo, proporcionando alternativas más cortas y fáciles de usar para realizar llamadas. Permite sustituir varios números de marcación, como direcciones IP o números SIP, por un único número simplificado.

Para configurar el plan de marcación, vaya a la interfaz web Videoportero > Plan de marcación. Haga clic en Añadir.



- Cuenta: Seleccione la cuenta de marcación.

- Auto: Marcar utilizando la cuenta registrada. Cuando hay 2 cuentas registradas, la Cuenta 1 es la predeterminada.

- Cuenta 1/2: Llamada saliente utilizando la cuenta elegida.

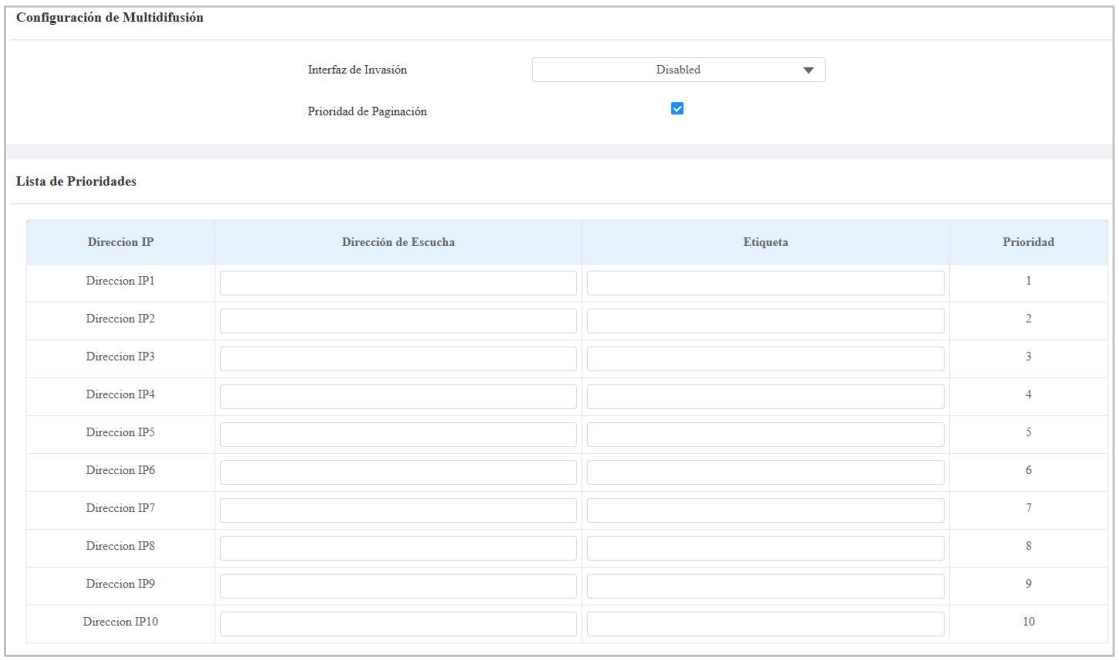
- Prefijo: Especifique un número corto para sustituir los números marcados especificados.

- Reemplazar 1/2/3/4/5: Especifique hasta 5 números, que pueden ser números SIP o direcciones IP, para ser reemplazados por el prefijo. Todos estos números serán llamados simultáneamente cuando la persona que llama marque el prefijo.

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 opción Videoportero > Multidifusión.



- Interfaz de Invasión: Multidifusión o cuántas llamadas multicast tienen mayor prioridad que una llamada SIP. Si desactiva la prioridad de paginación, la llamada SIP tendrá mayor prioridad.
- Prioridad de Paginación: Las llamadas multicast se realizan en orden de prioridad o no.
- Dirección de Escucha: La dirección IP multicast a la que se debe

escuchar. La dirección IP multicast debe ser la misma que la parte escuchada, y el puerto multicast no puede ser el mismo para cada dirección IP. La dirección IP multicast está en el rango de 224.0.0.0 a 239.255.255.255.

Llamada por Internet

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

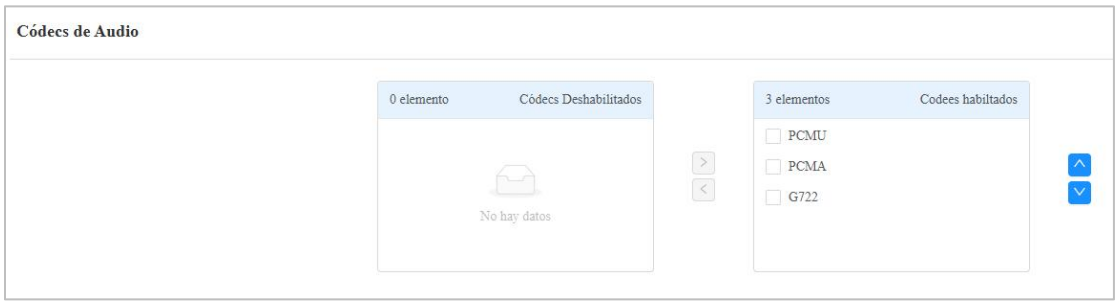
Para configurarla, vaya a la interfaz web Sistema > Mantenimiento > Llamada web. Seleccione la cuenta SIP registrada, introduzca el número IP/SIP y haga clic en Marcar para realizar la llamada.

Configuración de Codecs de Audio y Video

Configuración del Códec 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.

Para configurar el códec de audio, vaya a Cuenta web > Avanzado.



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

Tipo de códec	Consumo de ancho de banda	Frecuencia de muestreo
PCMA	64 kbit/s	8kHZ
PCMU	64 kbit/s	8kHZ
G722	64 kbit/s	16kHZ

Configuración del 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 web > Avanzado.

- Nombre: Marque esta opción para habilitar el formato de códec de vídeo H264 para el flujo de vídeo del portero automático.
- Resolución: Seleccione la resolución del código para la calidad de vídeo

entre las opciones disponibles. La resolución de código por defecto es CIF.

- Tasa de bits: La tasa de bits del flujo de vídeo oscila entre 128 y 2048 kbps. Cuanto mayor sea la tasa de bits, mayor será la cantidad de datos transmitidos por segundo y, por tanto, 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.
- Control de tasa: Configura la tasa de bits de llamada de la cuenta. El valor predeterminado es VBR.
- VBR: Tasa de bits variable, ajusta la tasa de bits dinámicamente en función de la complejidad del contenido.
- CBR: Tasa de bits constante, mantiene una tasa de bits fija durante toda la transmisión.
- Perfil: Los atributos del vídeo codificado localmente, como la resolución, la tasa de bits y la frecuencia de imagen.
- BP: Perfil básico, diseñado para aplicaciones de baja complejidad y en tiempo real, como videoconferencias y dispositivos móviles.
- MP: Perfil principal, ofrece mayor eficiencia de compresión y calidad de vídeo que Baseline.
- HP: perfil alto, ofrece la máxima calidad de vídeo y eficiencia de compresión, y admite funciones de codificación avanzadas.

Configuración del 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 > IP directa.

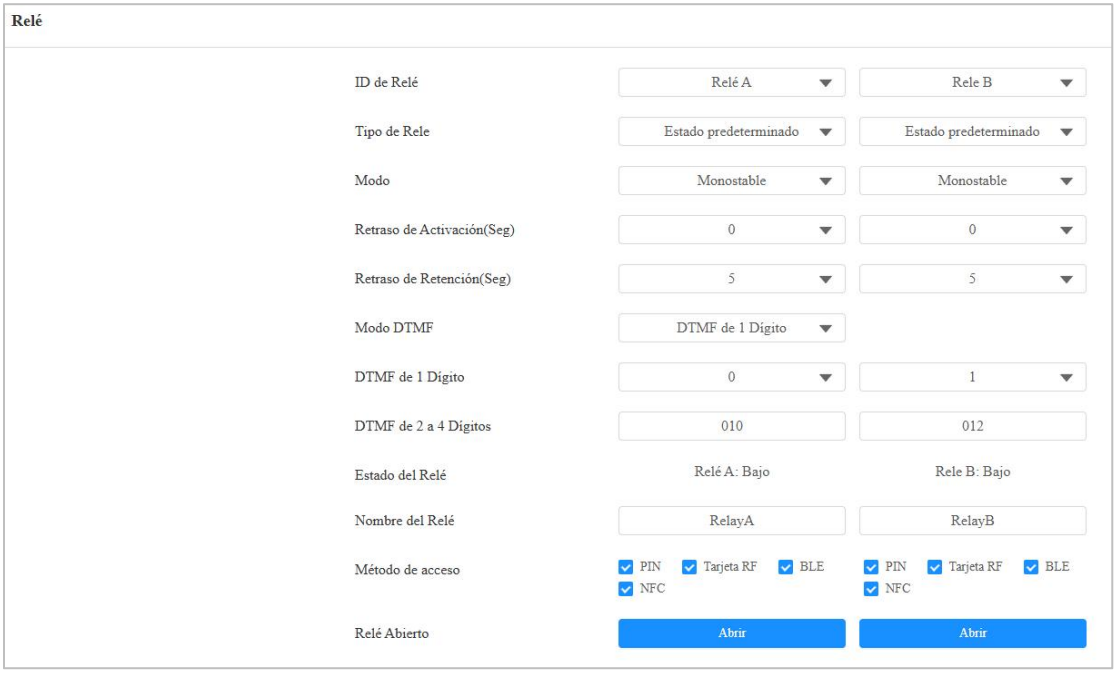
- Resolución de vídeo: Seleccione el código de resolución para la calidad de vídeo entre las opciones disponibles. Por defecto es 720P.
- Tasa de bits de vídeo: La tasa de bits del flujo de vídeo oscila entre 128 y 2048 kbps. La tasa de bits de código por defecto es 2048.
- Carga de vídeo: La carga útil oscila entre 90 y 119 para configurar archivos de configuración de audio/vídeo. El valor predeterminado es 104.

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 del videoportero 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.



- ID de relé: El relé específico para el acceso a la puerta.
- 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.

- Monoestable: El estado del relé se restablece automáticamente dentro del tiempo de retardo del relé después de la activación.
- Biestable: El estado del relé se restablece al disparar de nuevo el relé.
- Retardo Disparo (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.
- Retardo (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 Abierto: Puede hacer clic en Abrir para activar el relé manualmente.

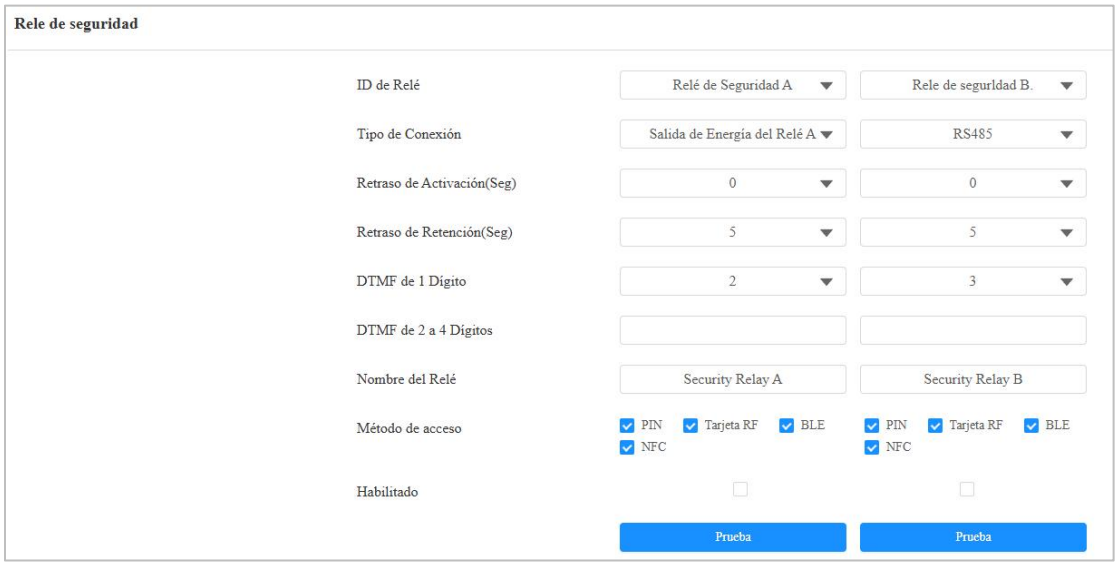
Nota:

Los dispositivos externos conectados al relé requieren un adaptador de alimentación independiente.

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: Seleccione el tipo de conexión entre el relé de seguridad y el portero automático. Puede seleccionar la conexión a través de la salida de alimentación del relé A del portero automático o 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.

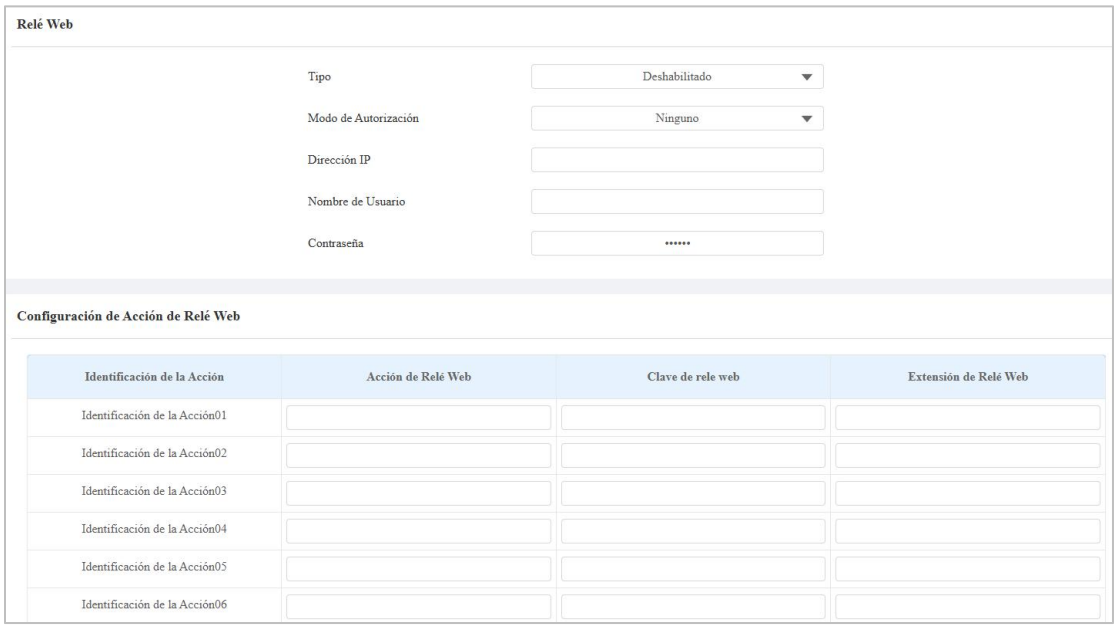
Nota:

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.
- Modo de autorización: Seleccione el modo de autorización entre Ninguno y Digerir. Cuando se selecciona Digest, el nombre de usuario y la contraseña se utilizan para la autenticación.
- 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 retransmisión 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 dispositivo de interfonía, 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 Acceso de Puertas

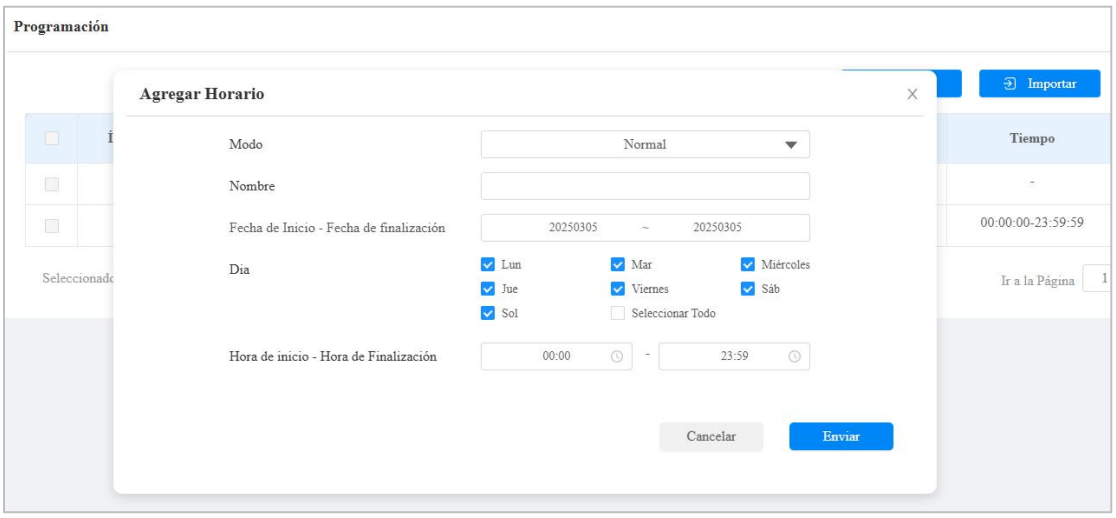
Esta función le permite decidir quién puede abrir la puerta y cuándo. Se aplica tanto a individuos como a grupos, garantizando que los usuarios dentro del horario sólo puedan abrir la puerta utilizando el método autorizado durante los periodos de tiempo designados.

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 > Horario. Haga clic en +Agregar

para crear un horario.



- Modo:
  - 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 del horario.

Importar y Exportar Horarios de Acceso

Puede crear horarios de acceso de puerta uno a uno o en bloque. Puede exportar el archivo de horario actual, editarlo o añadir más horarios siguiendo el formato, e importar el nuevo archivo a los dispositivos deseados. Esto le ayudará a gestionar fácilmente sus horarios de acceso.

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

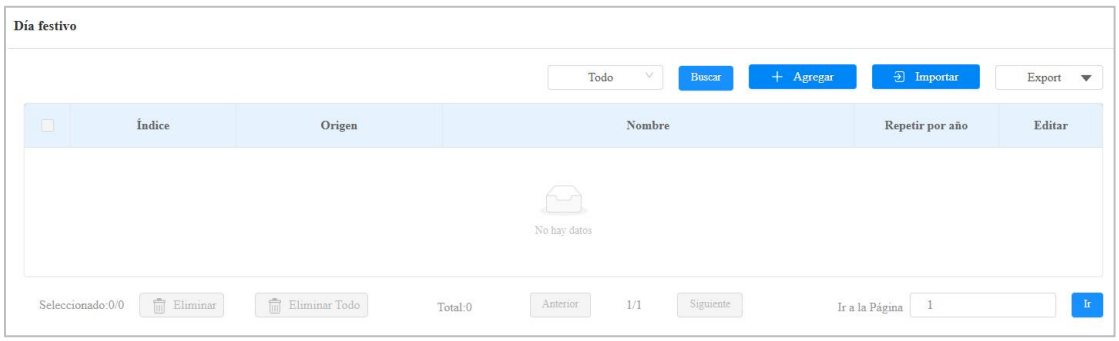
Nota:

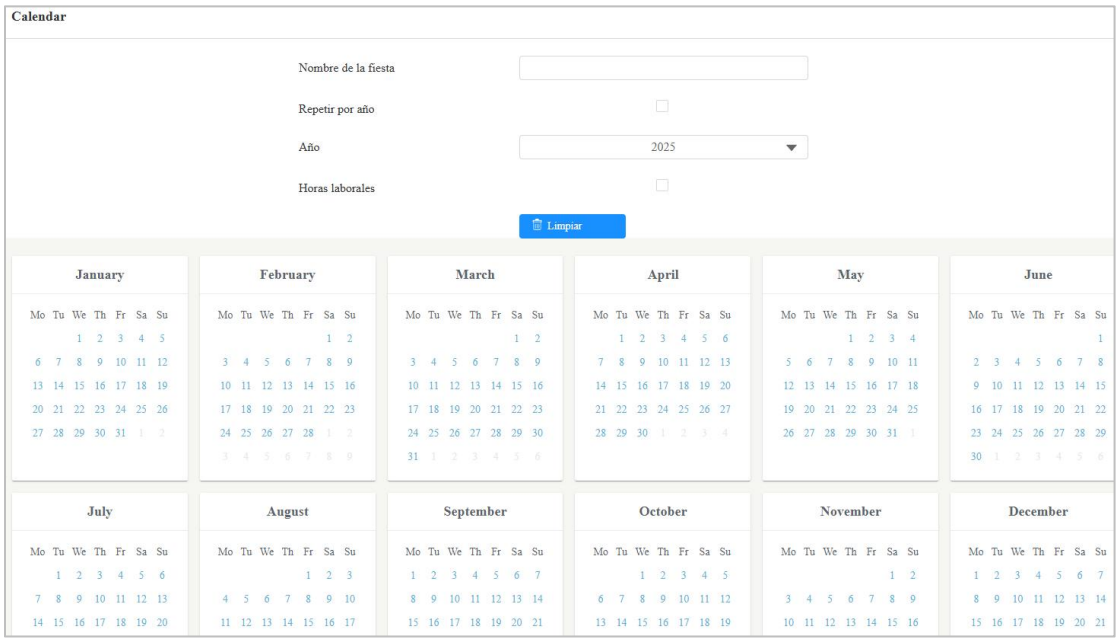
El archivo importado/exportado está en formato .xml.

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.

Programación de Relés

a programación de relés le permite configurar un relé específico para que se abra siempre a una hora determinada. Esta función es útil en casos como cuando se desea mantener la puerta abierta después de la escuela o 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.

Configuración de Apertura de Puerta

Desbloqueo mediante PIN público

Existen dos tipos de códigos PIN para el acceso a las puertas: público y privado. El PIN privado es único para cada usuario, mientras que el público es compartido por los residentes de un mismo edificio o complejo. Puede crear y modificar tanto el PIN público como el privado.

Para configurar el PIN público, vaya a la interfaz web Control de acceso > Configuración de PIN.

- Código PIN: Configure un código PIN de 5-8 dígitos accesible para uso universal.
- Relé: El relé que se activará.

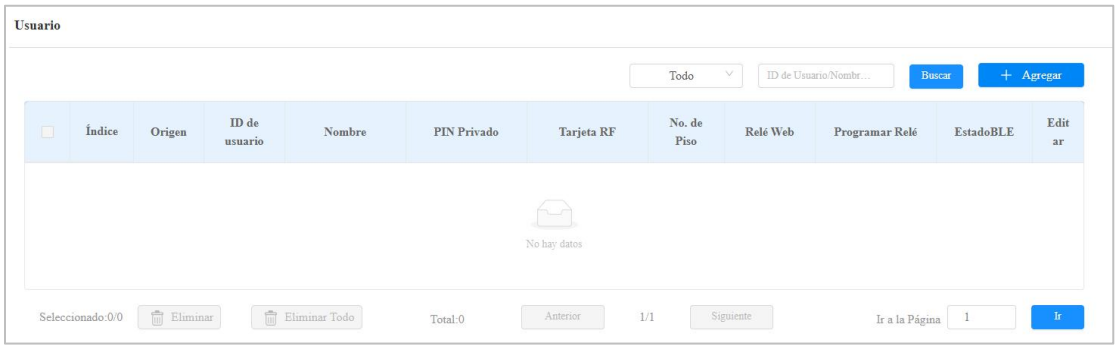
Consejo:
También puede modificar el PIN Público en el dispositivo pulsando «*3888#» en el teclado para entrar en la pantalla de Configuración del Método de Acceso.

Métodos de Acceso Específicos para Usuarios

El código PIN privado y la tarjeta RF deben 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 > Interfaz de usuario y haga clic en +Agregar.



- ID de usuario: El número de identificación único asignado al usuario.
- Nombre: El nombre de este usuario.

Desbloqueo mediante PIN Privado

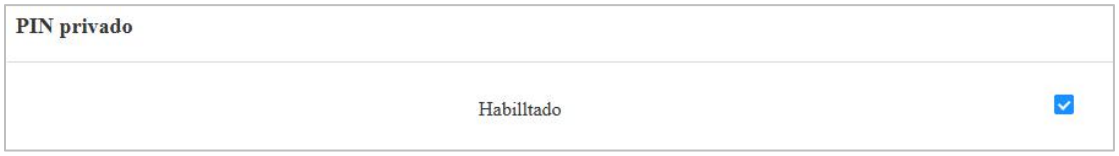
En la interfaz Directorio > Usuario > Añadir, busque la parte PIN Privado.

- Código: Establezca un código PIN de 2 a 8 dígitos para uso exclusivo de este usuario.

Consejo:

- También puede modificar el PIN Privado en el dispositivo pulsando «*3888#» en el teclado para entrar en la pantalla de Configuración del Método de Acceso.
- A continuación, introduzca el Código Admin «2396» para acceder a la pantalla de Adición y Eliminación de PIN Privado.

Active/desactive la función de PIN Privado en la interfaz Control de Acceso > Configuración de PIN > PIN Privado.



Acciones Activadas al Introducir PIN Privados

Puede configurar acciones activadas al introducir PIN privados en la interfaz Control de acceso > Configuración de PIN > Evento de clave privada.

- 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 debajo.
- URL HTTP: Introduzca el mensaje HTTP si selecciona HTTP como acción

a ejecutar. El formato es http://HTTP del servidor IP/Contenido del mensaje.

Desbloqueo mediante Tarjeta RF/Mando Bluetooth (Bkey)

En la interfaz Directorio > Usuario > Añadir, busque la sección Tarjeta RF.

- Código: El código de tarjeta o Bkey que lee el dispositivo.

Nota：

- Haga clic aquí para ver los pasos detallados de la configuración de Bkey.
- Las tarjetas RF que operan en frecuencias de 13,56 MHz y 125 KHz son compatibles con el dispositivo para el acceso.
- Cada usuario puede tener un máximo de 5 tarjetas añadidas.
- El dispositivo permite añadir 10.000 usuarios.
- También puede añadir tarjetas de administrador en el dispositivo. Pulse *2396#, en el teclado. A continuación, pulse 2 y 1 para acceder a la pantalla de configuración de tarjetas, donde podrá añadir o eliminar una tarjeta RF.

Puede activar y desactivar el uso de tarjetas RF en la interfaz Control de acceso > Configuración de tarjeta.

Consejo:

1. También puede modificar la tarjeta de usuario en el dispositivo pulsando «*3888#» en el teclado para entrar en la pantalla de configuración del método de acceso.

2. A continuación, introduzca el código de administración «2396» para acceder a la pantalla de adición y eliminación de tarjetas de usuario.

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: Seleccione el formato del número de tarjeta entre las opciones proporcionadas.
- Orden de Tarjeta ID: Establezca el modo de lectura de la tarjeta de identificación entre Normal e Invertido.

Acciones Activadas al Pasar Tarjetas

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

- Acciones 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.

- URL HTTP: Introduzca el mensaje HTTP si selecciona HTTP como acción a ejecutar. El formato es http://HTTP IP del servidor/Contenido del mensaje.

Desbloqueo por Bluetooth

El dispositivo permite abrir la puerta a través de las aplicaciones My MobileKey o SmartPlus habilitadas para Bluetooth. Los usuarios pueden abrir la puerta con las aplicaciones en sus bolsillos o agitar sus teléfonos hacia el dispositivo a medida que se acercan a la puerta.

Nota:
Antes de utilizar Bluetooth para abrir puertas, debe activar la función Bluetooth en la interfaz Control de acceso > BLE.

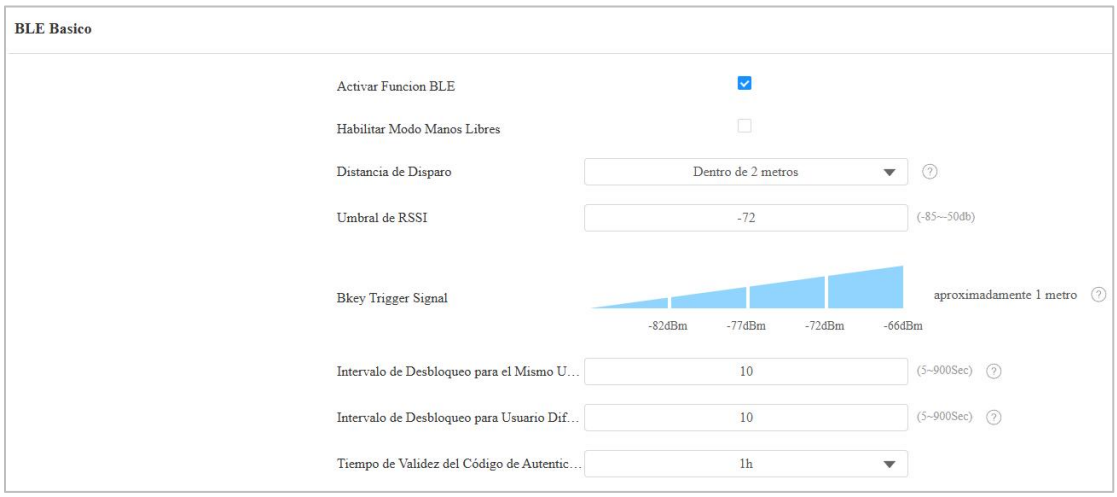
Desbloqueo mediante My MobileKey

En la interfaz Directorio > Usuario > +Agregar, desplácese hasta la sección Configuración BLE.

- Código de autenticación: Haga clic en Generar para generar un código de verificación de 6 dígitos.

Configuración del Desbloqueo Bluetooth

Configure la función de desbloqueo Bluetooth en la interfaz Control de acceso > BLE.



- Activar Modo Manos Libres. Activar Modo Manos Libres: Si está activado, los usuarios pueden acceder a las puertas con las manos libres. Si está desactivado, los usuarios tienen que acercar sus manos al dispositivo para abrir las puertas.
- Distancia de Disparo: Establezca la distancia de activación del Bluetooth para el acceso a la puerta. Puede seleccionar Dentro de 1 metro, Dentro de 2 metros y Dentro de 3 metros. La distancia de activación es de 3 metros como máximo.
- Umbral de RSSI: Establece la intensidad de la señal recibida. Los valores más altos indican una mayor intensidad de la señal, lo que facilita la recepción de la señal Bluetooth.
- Bkey Trigger Señal: Hay cuatro rangos que determinan la distancia de activación de Bkey.
- Intervalo de desbloqueo para el mismo usuario (Seg): Establece el intervalo de tiempo entre intentos consecutivos de acceso a la puerta Bluetooth para el mismo usuario.
- Intervalo de Desbloqueo para Usuarios Diferentes(Seg): Ajuste el intervalo de tiempo entre intentos consecutivos de acceso a la puerta Bluetooth para diferentes usuarios.
- Tiempo de validez del código de autenticación: El tiempo de validez del emparejamiento dentro del cual los usuarios deben finalizar el emparejamiento con la aplicación My MobileKey.

Nota:

Para conocer los pasos detallados de configuración de los diferentes métodos de acceso basados en Bluetooth, puede hacer clic en los siguientes artículos.

- Abrir la puerta mediante Bkey.
- Desbloquear por Bluetooth mediante la aplicación My MobileKey.
- Desbloquear por Bluetooth a través de SmartPlus App.

Configuración de la Información del Dispositivo

Puede personalizar el nombre y el ID del dispositivo para un emparejamiento Bluetooth más cómodo.

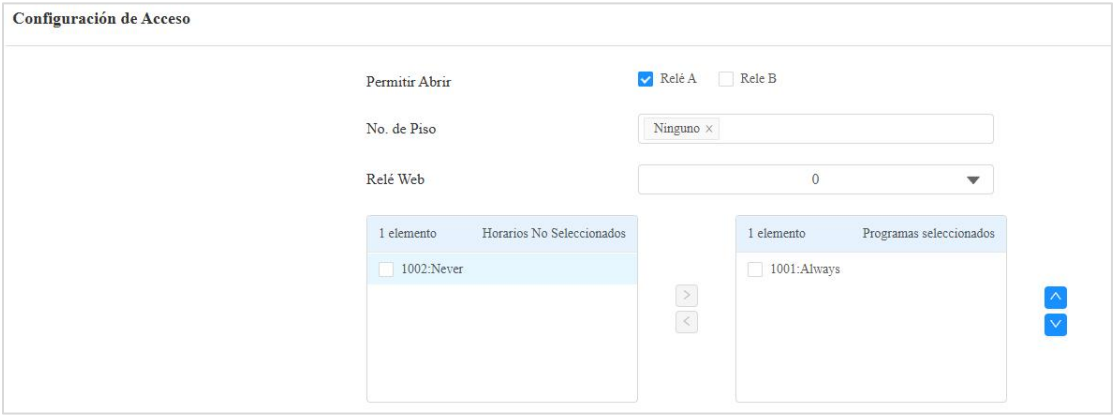
Para configurarlo, vaya a la interfaz **Control de acceso > BLE > Configuración de la información del dispositivo**.

- Nombre del dispositivo: Limitado a 1-63 números o caracteres.
- ID de dispositivo: Limitado a 1-12 números o caracteres.

Configuración de Acceso

Puede personalizar los ajustes de acceso, como definir el horario de acceso a la puerta para determinar cuándo es válido el código y especificar qué relé abrir.

En la interfaz Directorio > Usuario > Añadir, desplácese hasta la sección Configuración de acceso.



- Permitir Abrir: Especifique el relé o relés que se desbloquearán utilizando los métodos de apertura de puerta asignados al usuario.
- NO. de piso: Especifique el piso o pisos accesibles para el usuario a través del ascensor: Especifique la(s) planta(s) accesible(s) al usuario a través del ascensor.
- Relé Web: Especifique el ID de los comandos de acción de retransmisión web que ha configurado en la interfaz de retransmisión web. Un valor predeterminado de 0 indica que no se activará la retransmisión web.
- Horario: Conceda al usuario acceso para abrir puertas designadas durante periodos preestablecidos reubicando los horarios deseados de la casilla derecha a la izquierda. Además de los horarios personalizados, existen 2 opciones por defecto:

- 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

El videoportero permite compartir los datos de usuario del control de acceso entre los videoporteros Akuvox a través de la importación y la exportación, mientras que usted también puede exportar los datos faciales del videoportero e importarlos a un dispositivo de terceros.

Para configurarlo, vaya a la interfaz Directorio > Usuario > Importar/Exportar

Usuario.

El archivo de importación debe estar en formato TGZ. El archivo de exportación está en formato XML o CSV.

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:
Haga click aquí para ver los pasos detallados de la configuración de la función NFC.

Desbloqueo por Comando HTTP

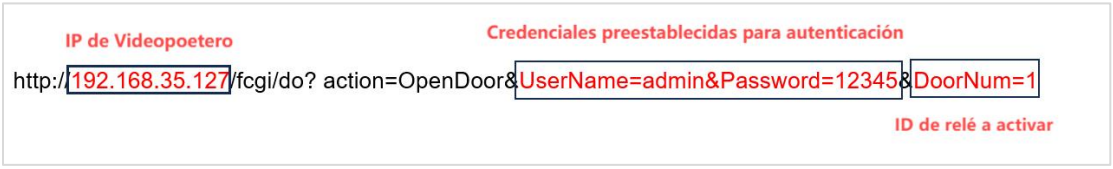
Puede desbloquear la puerta de forma remota sin acercarse físicamente al dispositivo para la entrada de la puerta escribiendo el comando HTTP creado (URL) en el navegador web para activar el relé cuando no esté disponible junto a la puerta para la entrada de la puerta.

Para configurarlo, vaya a la interfaz web Control de acceso > Retransmisión > Retransmisión abierta a través de HTTP.

- Chequeo 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:

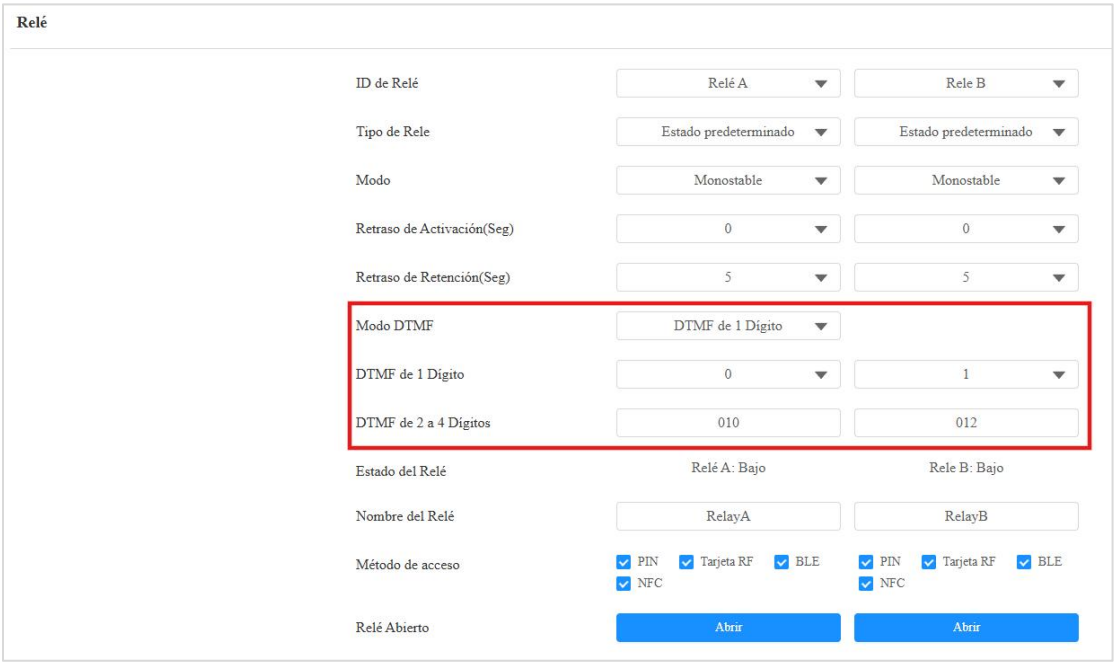
El formato HTTP para la activación del relé varía en función de si está activado el modo de alta seguridad del portero automático. Consulte esta guía práctica para obtener más información: Abrir la puerta mediante comando HTTP.

Desbloqueo 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 > Interfaz de retransmisión.



- 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.

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 > Retransmisión > Retransmisión abierta mediante interfaz 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.

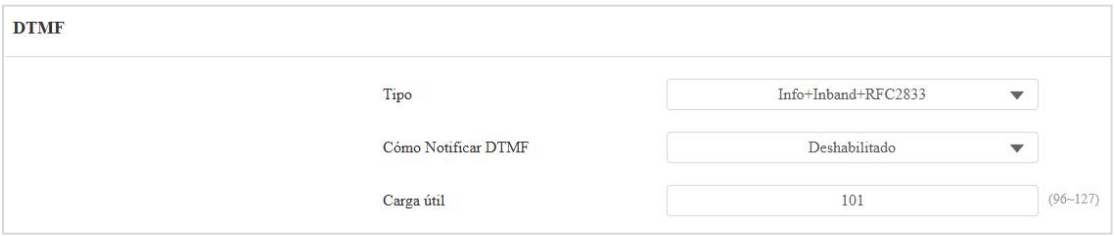
- "Assigned The Authority For": Especifique los contactos autorizados para abrir puertas mediante DTMF:

- Ninguno: Ningún número puede desbloquear puertas mediante DTMF.
- Sólo Lista Contactos: Sólo los números añadidos a la lista de contactos del portero automático pueden desbloquear mediante DTMF.
- Todos los números: Cualquier número puede desbloquear mediante 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 Cuenta web > Avanzado > Interfaz 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.

Transmisión de Datos DTMF para Llamadas IP

Seleccione el tipo de transmisión de datos DTMF para llamadas IP en la interfaz Videoportero> Función de llamada > IP directa.

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 web > Entrada.

- Activado: Para utilizar una interfaz de entrada específica.
- Nivel Eléctrico de Disparo: 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 Retardo 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.
- Alarma de Puerta Abierta: Si está activada, cuando el tiempo de apertura de la puerta supere un límite, se activará una alarma.
- Tiempo de Apertura de Puerta: El tiempo límite de apertura de la 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.

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 stream 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.

Flujo de Vídeo MJPEG

Puede tomar una imagen de vigilancia y ver secuencias de vídeo en formato MJPEG con el dispositivo.

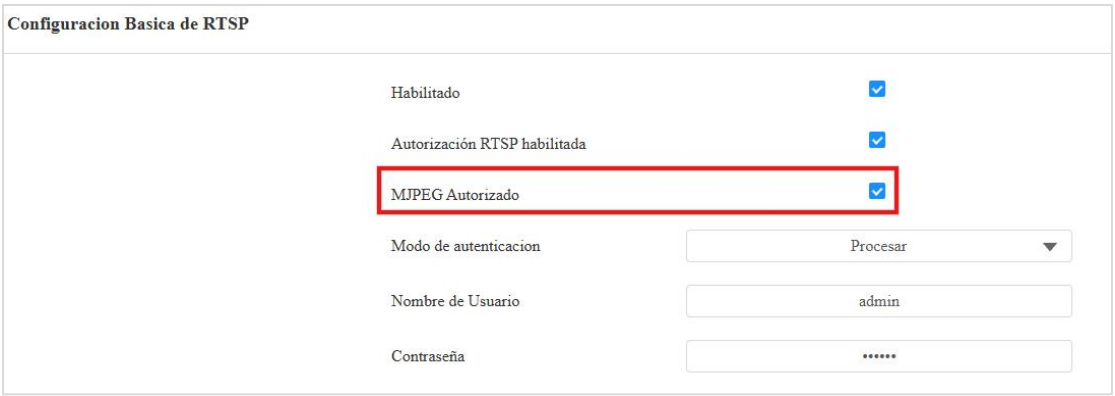
Para configurarlo, vaya a la interfaz Vigilancia > RTSP > Parámetros de vídeo MJPEG.

- Resolución de vídeo: Especifica la resolución de vídeo desde la más baja QVGA(240×320 píxeles) hasta la más alta 1080P(1920×1080 píxeles).
- Frecuencia de vídeo: Por defecto es de 30 fps.
- Calidad de Video: Por defecto es 90.

Autorización MJPEG

Puede activar la autorización MJPEG para limitar el acceso a las imágenes y vídeos MJPEG.

Para configurarla, vaya a la interfaz Vigilancia > RTSP > RTSP Básico.



- 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 RTSP y la Contraseña RTSP.

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 Secuencias RTSP

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

Para configurarlo, vaya a la interfaz Vigilancia > RTSP > RTSP Básico.

- Autorización RTSP Habilitada: Una vez habilitada, 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 portero automático desde otros dispositivos de interfonía como monitores interiores.

- Modo de autenticación: Seleccione entre Básica y Digest. Por defecto es Digest, que utiliza hashing 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 del Flujo RTSP

El flujo 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 > Flujo RTSP.

- Audio RTSP: Permite que el portero automático envíe información de audio al monitor mediante RTSP.
- Vídeo RTSP: El videoportero puede enviar la información de vídeo al monitor. Después de activar la función RTSP, el vídeo RTSP está activado por defecto y no se puede modificar.
- Vídeo RTSP 2: Los porteros automáticos Akuvox soportan 2 flujos RTSP, puede habilitar el segundo.
- Puerto de Vídeo RTSP: Especifique el puerto de vídeo.
- Codec de Vídeo : Elija un códec de vídeo adecuado para el vídeo RTSP.

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 Parámetros de Vídeo H.264

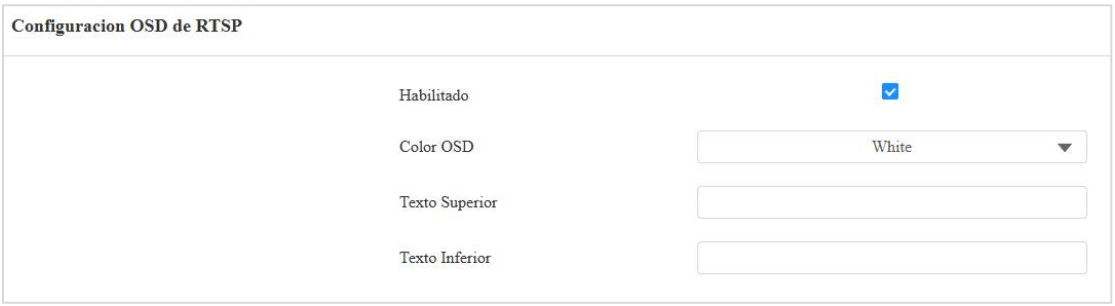
Configure los parámetros de vídeo H.264 para el flujo de vídeo RTSP en la interfaz Vigilancia > RTSP > Parámetros de vídeo H.264.

- Resolución de vídeo: Especifica la resolución de la imagen, variando desde la más baja QVGA(240×320 píxeles) hasta la más alta 1080P(1920x1080 píxeles).
- Frecuencia de imagen de vídeo: Fotogramas por segundo, se refiere a cuántos fotogramas se muestran en un segundo de vídeo.
- Tasa de bits de vídeo: La cantidad de datos de vídeo transferidos en un periodo de tiempo específico. Una mayor tasa de bits de vídeo significa una mayor calidad posible, pero también un mayor tamaño de los archivos y más ancho de banda.
- 2ª Resolución de Vídeo: Especifica la resolución de imagen para el segundo canal de flujo de vídeo.
- 2ª Frecuencia de Video: Establece la frecuencia de imagen para el segundo canal de flujo de vídeo.
- 2ª Tasa de bits de vídeo: Establezca la tasa de bits para el segundo canal de flujo de vídeo. El valor predeterminado es 512 kbps.

Configuración OSD 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 OSD RTSP.



- Color OSD: Seleccione el color entre Blanco, Negro, Rojo, Verde y Azul.
- Texto superior/inferior: Personalice el contenido del OSD.

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 Videoportero> Función de llamada > Interfaz de otros.

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.

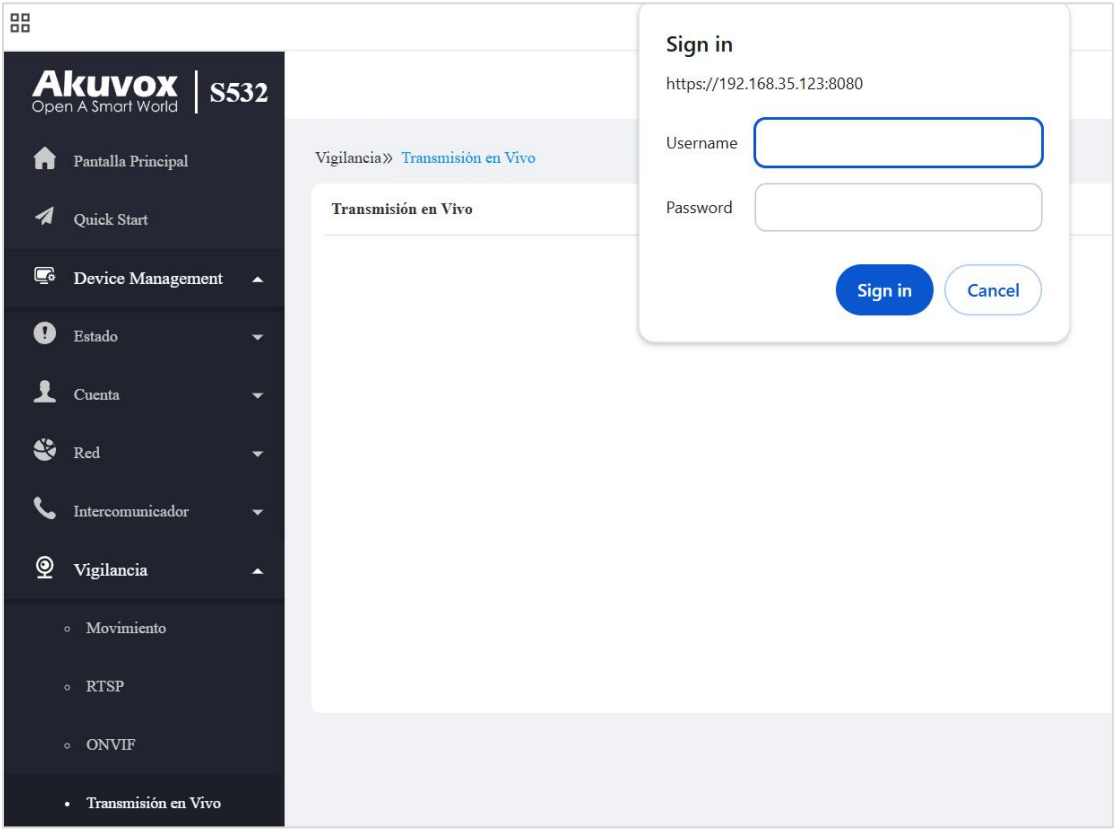
- Descubrible: Cuando está activado, el vídeo de la cámara del portero automático para ser buscado por otros dispositivos.
- Nombre de usuario: Establezca el nombre de usuario necesario para acceder al flujo de vídeo del portero automático en otros dispositivos. Por defecto es admin.
- Contraseña: Establezca 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 el flujo de vídeo en la interfaz Vigilancia > Flujo en directo. Si ha habilitado la autorización RTSP, deberá introducir el nombre de usuario y la contraseña establecidos en la sección RTSP Básico para ver el flujo.

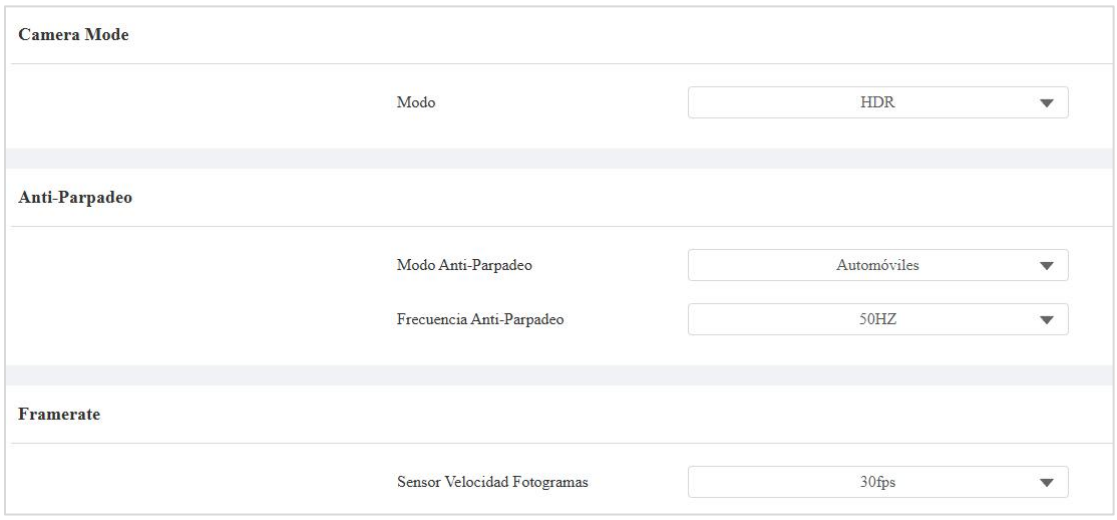


Modo de Cámara

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 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.

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.

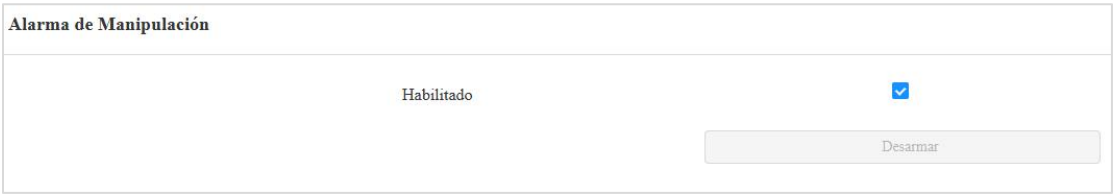
Seguridad

Alarma Antisabotaje

La función de alarma antisabotaje impide que nadie retire el dispositivo sin permiso. Los dispositivos Akuvox admiten dos tipos de antisabotaje: detección de gravedad y detección del estado de los botones.

Haga clic aquí para ver qué tipo admite el dispositivo y conocer los detalles de la función.

Para configurarlo, vaya a la interfaz web Sistema > Seguridad > Alarma de manipulación. Cuando se active la alarma, puede hacer clic en Desarmar para borrar la alarma.



Configuración de Desarmado

Puede configurar el código de desarmado en la interfaz web Sistema > Seguridad > Configuración de desarmado. El valor predeterminado es 0000.

PIN Virtual

El PIN virtual le permite proteger su código PIN para evitar que alguien lo filtre.

Para configurarlo, vaya a la interfaz web Control de acceso > Configuración de PIN > PIN virtual.

- Habilitado: Si está habilitado, se le permite poner números falsos en ambos lados del código PIN para la protección del código PIN. Por ejemplo, si su contraseña es 1234567 puede poner 99 y 88 en ambos lados (99123456788). La contraseña virtual se corresponde con los usuarios por el número de dígitos coincidentes. Por ejemplo, si el usuario A tiene un mayor número de dígitos que coinciden con la contraseña virtual introducida que el usuario B, entonces se considerará como la contraseña del usuario A. Sin embargo, cuando se aplica la doble autenticación, la contraseña virtual se asociará con los usuarios que superen el primer nivel de autenticación, por ejemplo, Cara + PIN.

Nota:
Esta función no se utiliza para PIN público y Apartamento+PIN.

Configuración del Certificado de Cliente

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

Certificado de Servidor Web

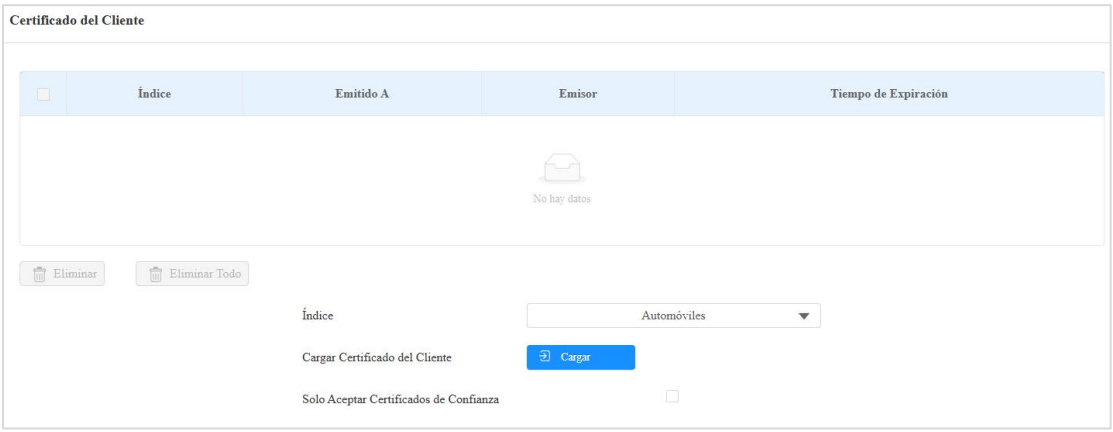
Es un certificado que se envía al cliente para su autenticación cuando éste solicita una conexión SSL con el portero automático Akuvox. Cargue los certificados en los formatos aceptados.

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.

- Cargar certificado de cliente: Localice y cargue el certificado deseado (sólo *.pem).
- Sólo aceptar certificados de confianza: Si está activada, mientras 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.

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 de Vídeo: Cuando la cámara de vídeo detecte objetos en movimiento, se activarán las acciones preestablecidas. Se centra en el análisis de la información visual captada a través de las cámaras.
  - Detección por Radar Cuando el radar detecte objetos en movimiento,

se activarán las acciones preestablecidas. Ofrece mayor alcance y mejor detección en condiciones de poca visibilidad.

- Vídeo + Radar: Detecta movimiento con la combinación de cámara de vídeo y radar.

- Alcance de detección: Después de activar la detección de radar, puede seleccionar el rango de detección entre 1, 2 y 3 metros.
- Time Interval (Intervalo de tiempo): El intervalo de disparo absoluto es de 3 segundos. Si selecciona un número superior a 3 segundos, necesitará un segundo intervalo de activación para activar la alarma. Por ejemplo, si selecciona 3 segundos, entonces la alarma se disparará cuando se detecte un objeto en movimiento una vez de 0 a 3 segundos (se disparará en cualquier momento de 0 a 3 segundos). Sin embargo, por ejemplo, si selecciona 5 segundos (mayor que 3), entonces la alarma no se activará hasta que se detecte un objeto en movimiento por segunda vez de 3 a 5 segundos (activada en cualquier momento de 3 a 5 segundos). El intervalo por defecto es de 10 segundos.
- Precisión de detección: La sensibilidad de detección. Especifique esta opción al seleccionar Detección de vídeo. Cuanto mayor sea el valor, más precisa será la detección. El valor por defecto es 3.
- Área de detección: Haga clic y mantenga pulsado el botón del ratón para seleccionar hasta tres áreas de detección.
- Acción a ejecutar: El tipo de notificación incluye FTP, Correo electrónico, Llamada SIP y HTTP.
  - FTP: La notificación se enviará al servidor FTP designado.
  - Correo electrónico: El correo electrónico se enviará a la dirección de correo electrónico preconfigurada.
  - Llamada SIP: Se realizará una llamada al número preconfigurador.
  - HTTP: La notificación se enviará al servidor designado.
    - URL HTTP: Introduzca el mensaje HTTP si selecciona HTTP como acción a ejecutar. El formato es http://HTTP IP del servidor/Contenido del mensaje.
- Ejecutar Relé: El relé a activar.

Horario de Detección de Movimiento

Cuando la detección de movimiento está activada, puede establecer una hora específica para que la función sea efectiva.

Configúrelo en la interfaz Vigilancia > Movimiento > Configurar hora de detección de movimiento.

Notificación de Seguridad

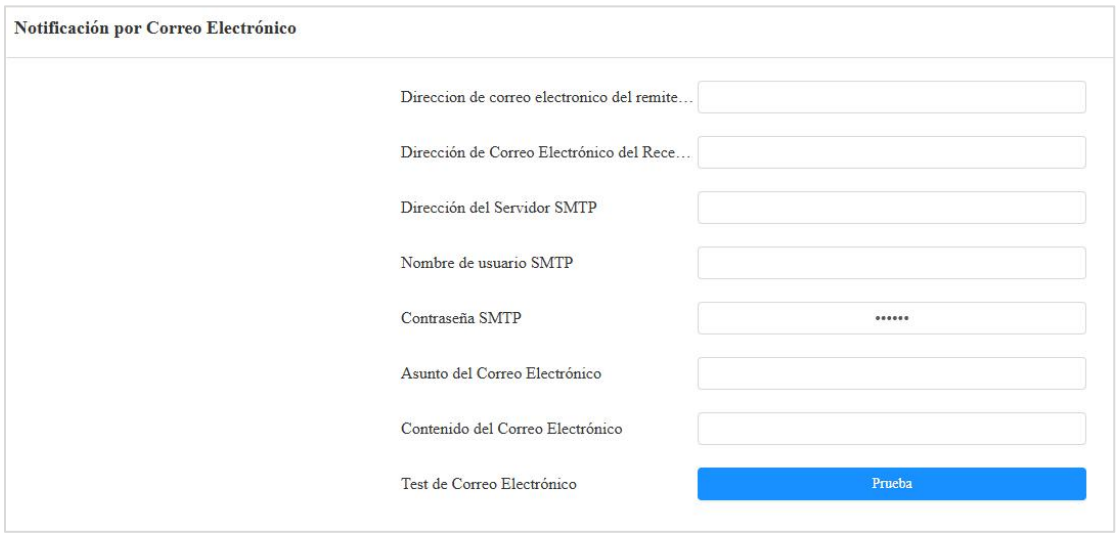
Una notificación de seguridad informa a los usuarios o al personal de seguridad de cualquier infracción o amenaza que detecte el dispositivo. Por ejemplo, si el dispositivo detecta algo inusual, el sistema envía una notificación a los usuarios o al personal de seguridad a través de correo electrónico,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

Configúrela en la sección Notificación por correo electrónico.



- 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.

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.

Configúrelo en la sección Notificación FTP.

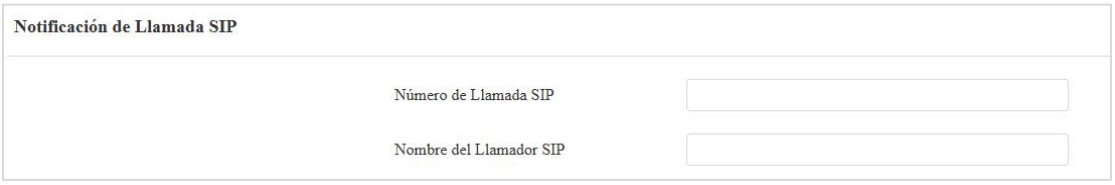
- Servidor FTP: Establezca la dirección (URL) del servidor FTP.
- Nombre de usuario FTP: Introduzca el nombre de usuario para acceder al servidor FTP.

- Contraseña FTP: Introduzca la contraseña para acceder al servidor FTP.

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 las funciones.

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	Parámetro de formato	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

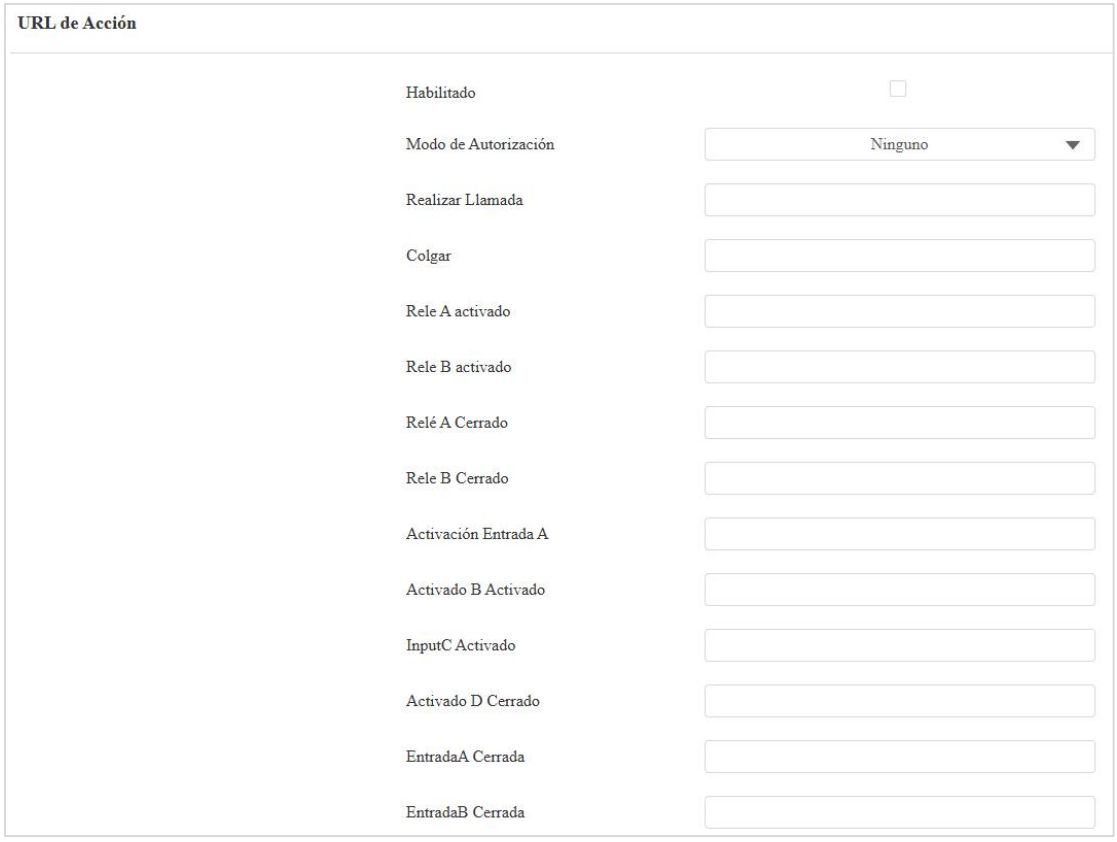
			ip/inputtrigger=$input1status
6	Entrada cerrada	$input1status	Http://server ip/inputclose=$input1status
7	Código válido introducido	$code	Http://server ip/validcode=$code
8	Código no válido introducido	$code	Http://server ip/invalidcode=$code
9	Tarjeta válida introducida	$card_sn	Http://server ip/validcard=$card_sn
10	Tarjeta no válida introducida	$card_sn	Http://server ip/invalidcard=$card_sn

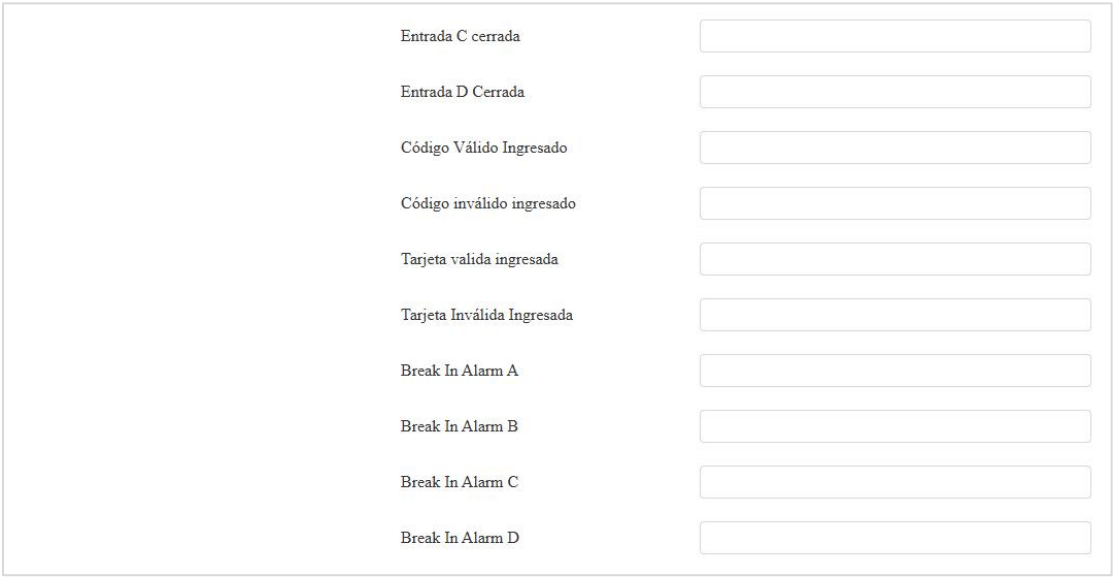
Por ejemplo:

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.





- Modo de autorización: Seleccione el modo de autorización. Si se selecciona Digest, puede configurar el nombre de usuario y la contraseña para la autenticación.

Cifrado de Voz

La función de cifrado ofrece tres métodos de cifrado para proteger las señales de voz de escuchas durante una llamada.

Configúrela en la interfaz Cuenta > Básico > Cifrado.

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.

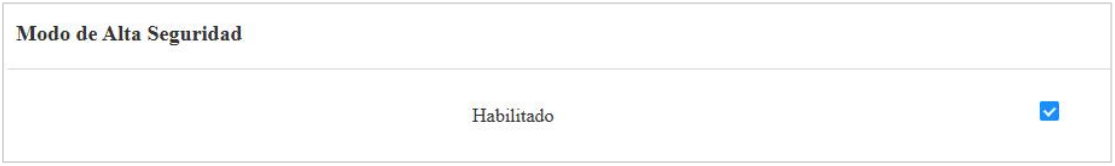
Para configurarlo, vaya a la interfaz Sistema > Seguridad > Tiempo de espera

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://usuario:contraseña@IPdedispositivo/fcgi/OpenDoor?action=OpenDoor&DoorNum=1
- http://dispositivoIP/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://IPdedispositivo/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.

Modo de Bajo Consumo

Muestra el modo de alimentación del dispositivo. Cuando el dispositivo se alimenta por POE, muestra Modo POE+. Cuando está alimentado por la fuente de alimentación de 12 voltios, muestra Modo de bajo consumo.

Consulte el modo de alimentación en la interfaz Sistema > Seguridad > Aviso de modo de baja potencia.

Acción de Emergencia

Esta función opera 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.

Configúrela en la interfaz Sistema > Seguridad > Acción de emergencia.

Supervisión 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.

Configúrelo en la interfaz Sistema > Seguridad > Supervisión en tiempo real.

- Aplicar configuración 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.

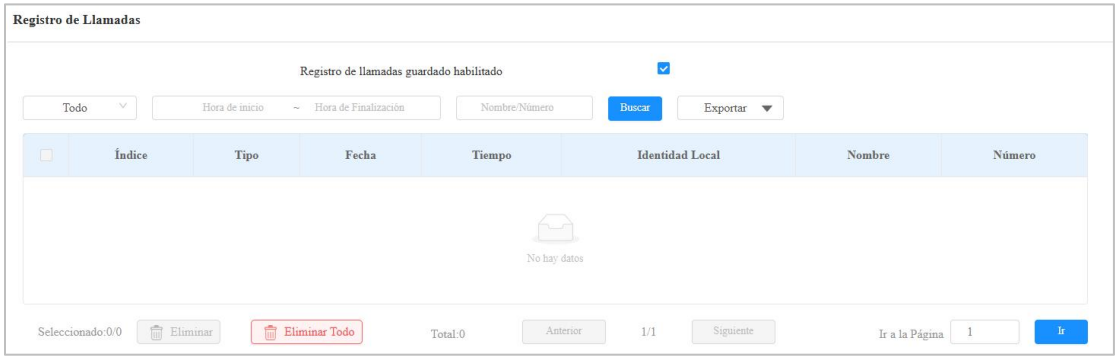
Registros

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.

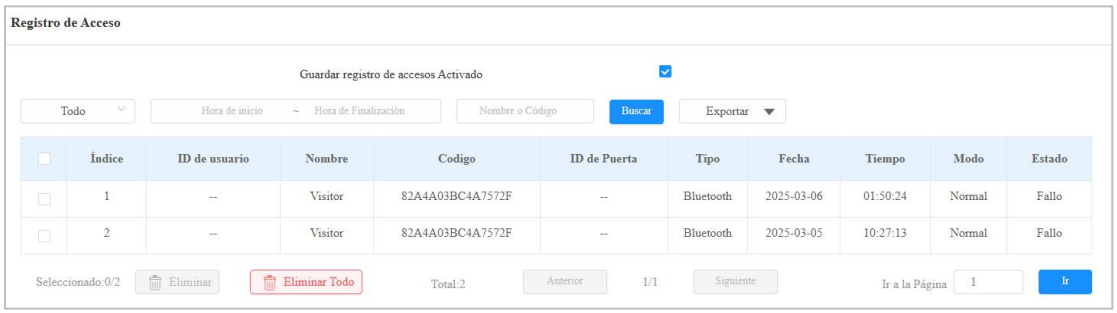


- Todas: Están disponibles cuatro tipos de historial de llamadas: Todas, Marcadas, Recibidas y Perdidas.
- Hora inicial-Hora final: La hora específica de los registros de llamadas que desea buscar, comprobar o exportar.
- Nombre/Número: Busque el registro de llamadas por el nombre o por el número SIP o IP.
- Exportar: Los registros de llamadas se pueden exportar en formato .csv.

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.

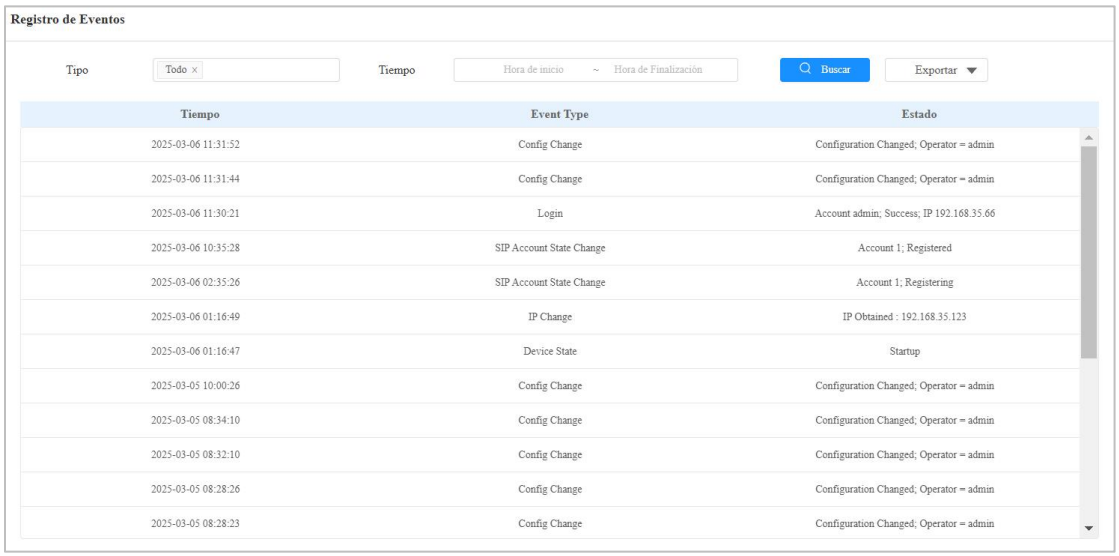


- Todos: Hay disponibles tres tipos de registros de acceso: Todos, Éxito y Fallo.
- Hora de inicio-Hora final: La hora específica de los registros de llamadas que desea buscar, comprobar o exportar.
- Nombre/Código: Busque el registro de la puerta por el nombre o por el código PIN.
- Exportar: Los registros de puerta se pueden exportar en formato .csv o .xml.
- Imagen: Haga clic para ver la imagen capturada.

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.



Actualización del Firmware

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

Actualice el firmware en la interfaz web Sistema > Actualizar.

Nota:

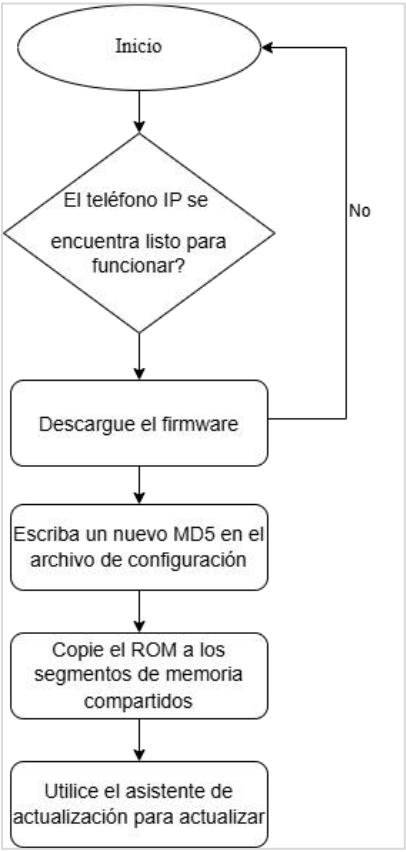
Los archivos de firmware deben estar en formato .rom para su actualización.

Autoaprovisionamiento

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:



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:

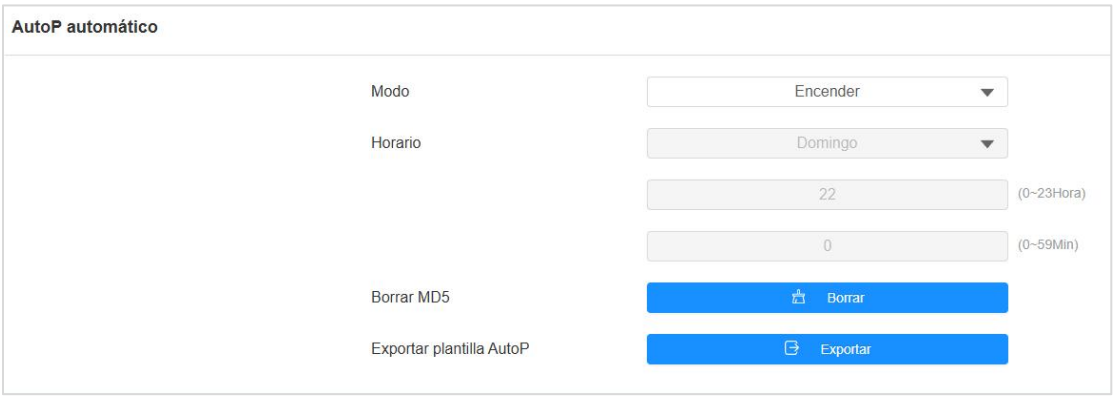
- Los archivos de configuración deben estar en formato CFG.
- El nombre del archivo de configuración general para la transferencia por lotes varía según el modelo.
- El archivo de configuración basado en MAC recibe el nombre de su dirección MAC.
- Los dispositivos accederán primero a los archivos de 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.



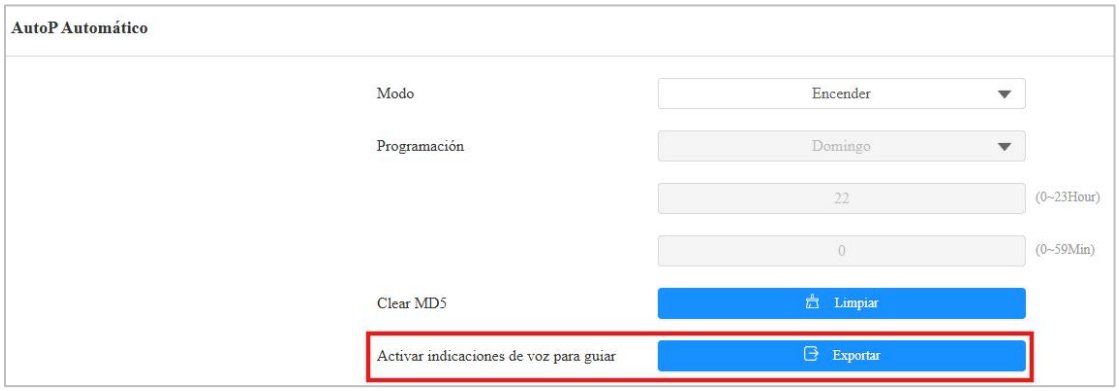
- Modo:
  - Encender: El dispositivo realizará el aprovisionamiento automático cada vez que se inicie.
  - Repetidamente: El dispositivo realizará el aprovisionamiento automático según el horario que se configure.
  - Encendido + Repetidamente: Combina el modo Encendido y el modo Repetidamente que permitirá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

Configuración de Aprovisionamiento Estático

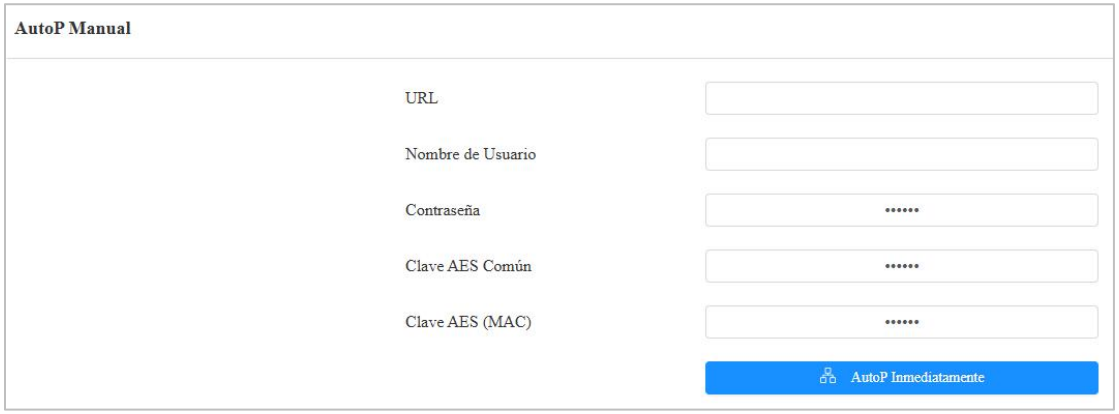
Puede configurar manualmente una URL de servidor específica para descargar el firmware o el archivo de configuración. Si se configura un programa de autoaprovisionamiento, el dispositivo realizará el autoaprovisionamiento a una hora específica según el programa de autoaprovisionamiento que haya configurado. 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 interfono descifre el archivo de configuración Autop basado en MAC.

Nota:

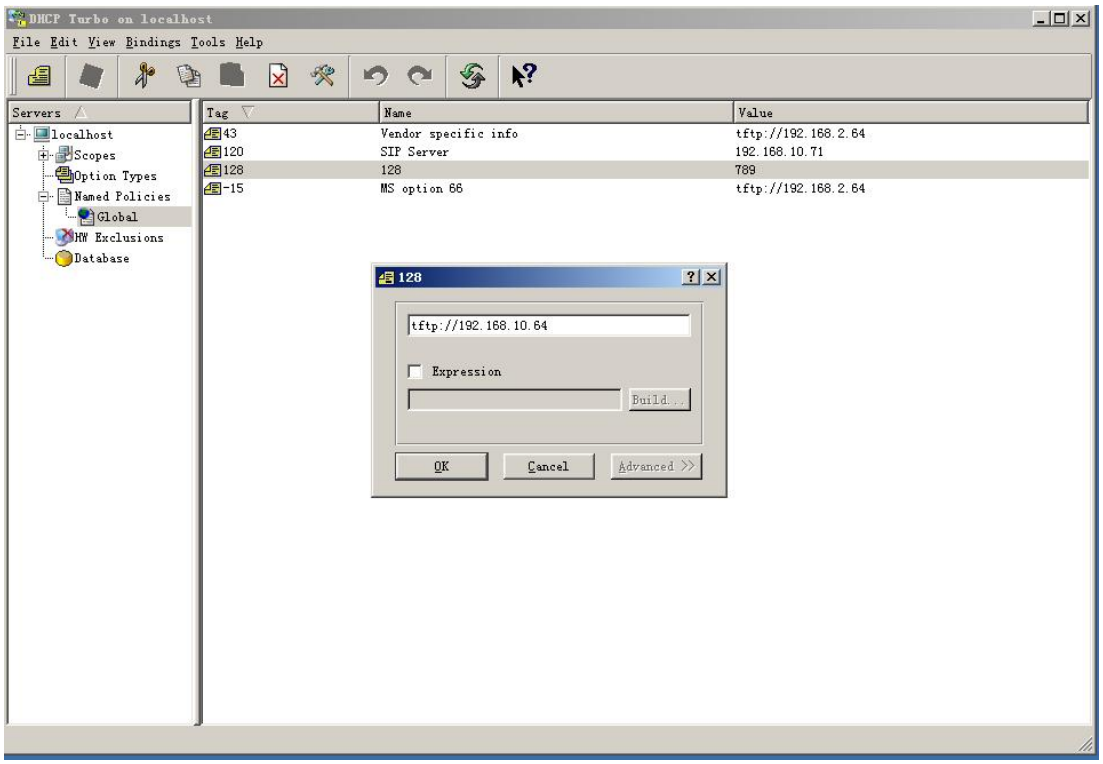
- AES como un tipo de cifrado debe ser configurado sólo cuando el archivo de configuración está cifrado con AES.
- Formato de la dirección del servidor:
  - TFTP: tftp://192.168.0.19/

  - 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.

Copia de Seguridad

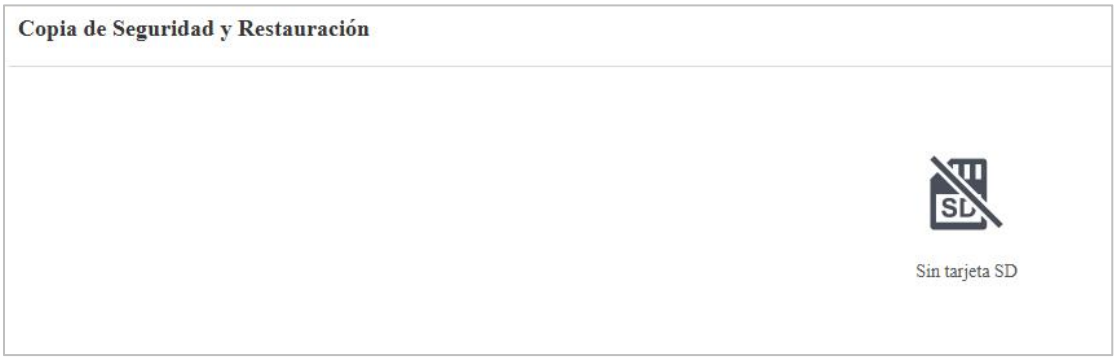
Puede importar o exportar archivos de configuración cifrados a su PC local.

Exporte el archivo en la interfaz Sistema > Mantenimiento. El archivo de importación debe estar en formato .tgz/.conf/.cfg.

Copia de Seguridad mediante Tarjeta SD

El dispositivo admite la inserción de una tarjeta SD para importar y exportar archivos de configuración.

Para configurarla, ve a la interfaz Dispositivo > Tarjeta SD.

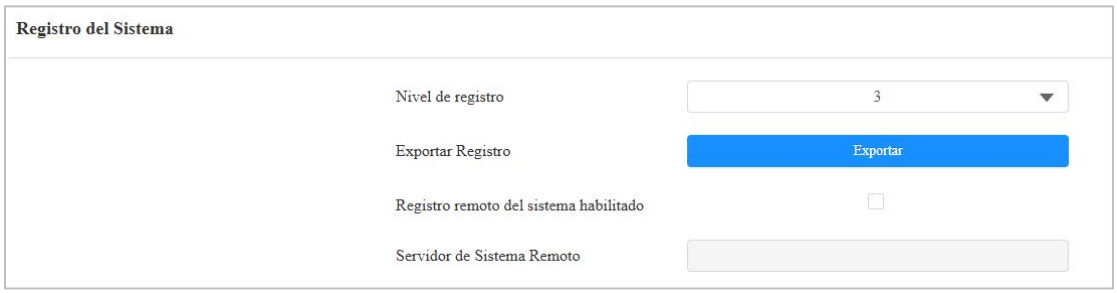


Depurar

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.

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.

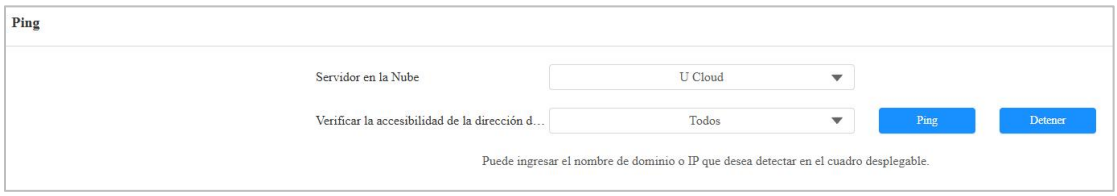
Para configurarlo, vaya a la interfaz web Sistema > Mantenimiento.

- 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.

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.

Integración con Dispositivos de Terceros

Integración mediante Wiegand

La función Wiegand permite al dispositivo Akuvox actuar como controlador o lector de tarjetas.

Configúrela en la interfaz web Dispositivo > Wiegand.

- Modo de visualización Wiegand: Seleccione el formato de código de tarjeta Wiegand entre las opciones proporcionadas.
- Modo Lector de Tarjetas Wiegand: El formato de transmisión debe ser idéntico entre el terminal de control de acceso y el dispositivo de terceros. Se configura automáticamente.
- Modo de Transferencia Wiegand:
  - Entrada: El dispositivo sirve de receptor.
  - Salida: El dispositivo sirve como emisor. Si los usuarios sólo pueden abrir la puerta pasando una tarjeta RF, seleccione el modo de

transferencia Wiegand como Salida.

- Convertir a nº de tarjeta Salida: El dispositivo sirve como emisor. Si los usuarios tienen asignados varios métodos de apertura de puerta, seleccione el modo de transferencia Wiegand como Convertir en salida de número de tarjeta.

- 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 de entrada 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 recibió.
  - Invertido: Se invierte el orden del número de tarjeta.
- Salida Wiegand CRC Activada: Está habilitado por defecto para la inspección de datos Wiegand. Deshabilitarlo puede provocar fallos de integración con dispositivos de terceros.
- Verificación de tarjeta RF: Cuando está habilitada, el dispositivo verificará si la tarjeta está asignada a un usuario. Si no lo está, aparecerá el mensaje «Fallo al abrir la puerta» en la pantalla del portero automático, pero la puerta podrá abrirse. Si está desactivado, el portero automático no realizará la verificación local.
- Relé de Apertura Wiegand: Compruebe el relé que se activará a través de Wiegand.

Nota:

Haga clic aquí para ver más información sobre la configuración Wiegand, incluyendo:

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

Cuando el dispositivo está en modo Salida Wiegand, puede configurar el formato de salida del código PIN Wiegand que determina cómo se transmiten los datos. El formato debe ser coherente con el del dispositivo de terceros.

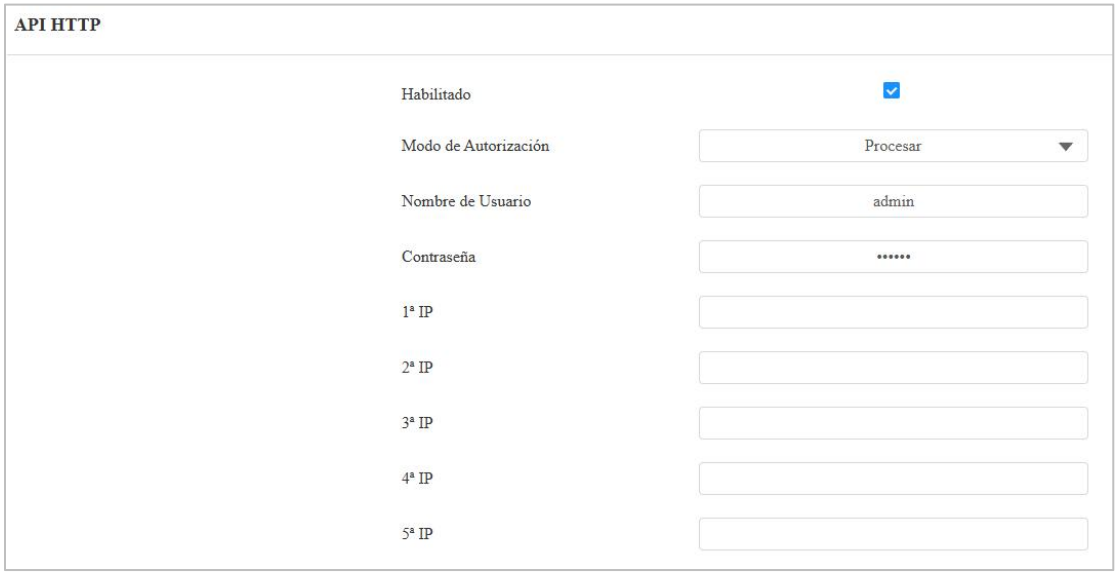
Configúrelo en la interfaz Dispositivo > Wiegand > Convertir a salida Wiegand.

- 8 bits por dígito: Cuando los usuarios pulsen «1» en el teclado, los datos binarios se transmitirán en 8 bits «11100001».
- 4 bits por dígito: Cuando el usuario pulsa «1» en el teclado, los datos binarios se transmiten en 4 bits «0001».

Integración a través de HTTP API

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

Para configurarlo, vaya a la web Configuración > Interfaz API HTTP.



- Activado: Habilita o deshabilita la función API HPTT 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: Seleccione entre las siguientes opciones: Ninguno, Normal, Lista de Permitidos, Básico, Digest y Token para el tipo de autorización, que se explicará detalladamente en el siguiente cuadro.
- Nombre de usuario: Introduzca el nombre de usuario cuando se seleccione el modo de autorización Básico o Digest. El nombre de usuario por defecto es admin.
- Contraseña: Introduzca la contraseña cuando se seleccione el modo de autorización Básico o Digerir. La contraseña por defecto es admin.
- 1ª IP-5ª IP: Introduzca la dirección IP de los dispositivos de terceros cuando se seleccione la autorización de 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 es necesario rellenar la dirección IP del dispositivo de terceros para la autenticación. Este modo es adecuado para el funcionamiento en la LAN.
4	Básico	ISi 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. MD5(Message-Digest Algorithm) En el campo Autorización de la cabecera de la petición HTTP: WWW-Autenticar: Digest realm=«HTTPAPI»,qop=«auth,auth-int»,nonce=«xx», opaque=«xx».
6	Token	Este modo sólo lo utilizan los desarrolladores de Akuvox.

Control de Salida de Potencia

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

Para configurarlo, vaya a la web Control de acceso > Relé > Interfaz de salida de relé de 12 V.

- 12V Potencia de salida:
  - Siempre: Proporciona alimentación continua al dispositivo de terceros.
  - Activado por relé abierto: Proporciona alimentación al dispositivo de terceros a través de la salida 12 y la interfaz GND durante el tiempo de espera cuando el estado de los relés pasa de bajo a alto.
  - Relé de seguridad A: El dispositivo puede funcionar con el relé de seguridad, SR01.

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.

Habilite la función en la interfaz web Vigilancia > ONVIF > Configuración avanzada.

Integración mediante 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.

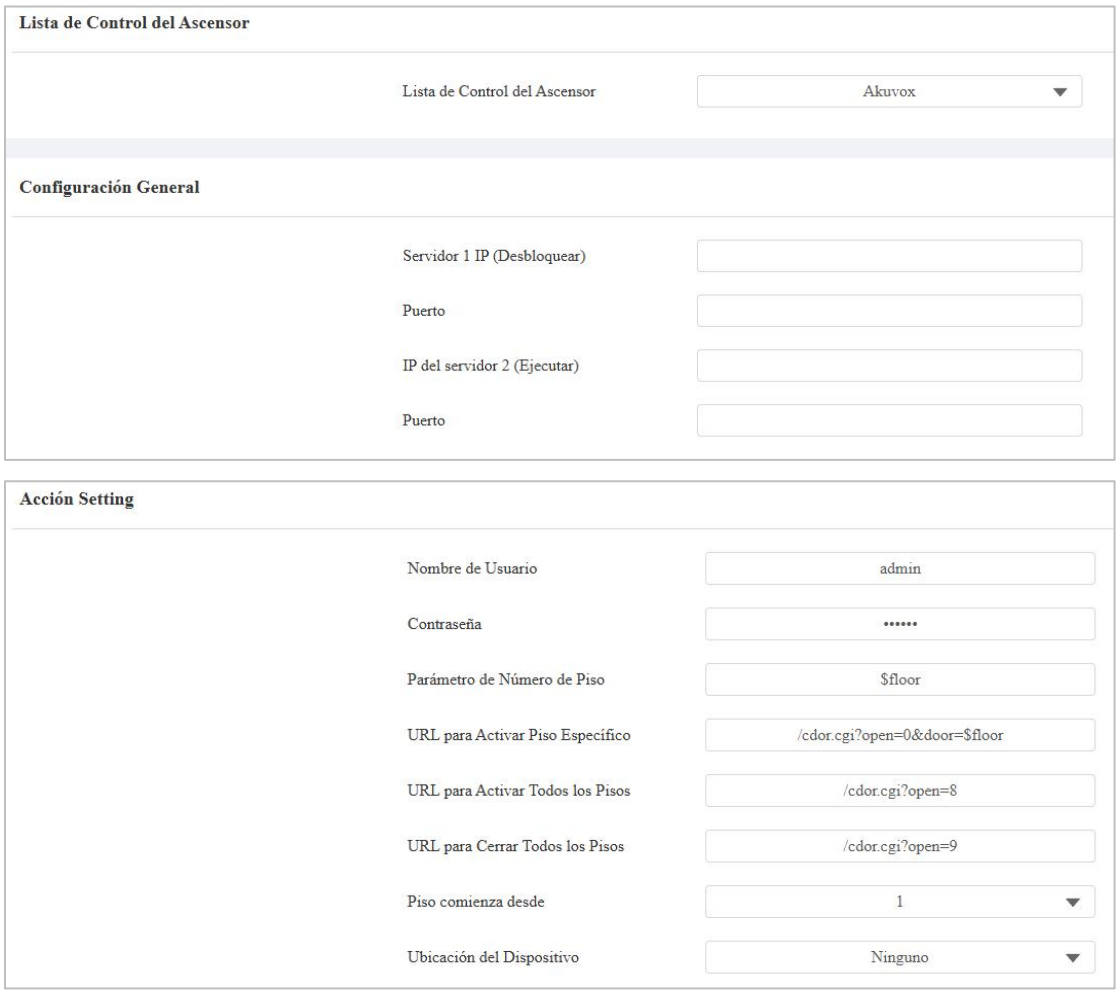
Para que la conexión sea efectiva, debe configurar el RS485 en Dispositivo > Interfaz RS485.

- 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 rellena, 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.

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 control de ascensor: Seleccione Ninguno para desactivar la función y seleccione Akuvox para integrar el portero automático con el controlador Akuvox.
- Servidor 1 IP(Desbloquear): La dirección IP del servidor de control de ascensores Akuvox. Admite hasta 10 direcciones de servidor separadas por «;».
- IP Servidor 2 (Ejecutar): La dirección IP del servidor que ejecuta el control de ascensor.
- Puerto: El puerto del servidor que activa el control de ascensores.
- Nombre de usuario: El nombre de usuario del controlador de ascensor para la autenticación.
- Contraseña: La contraseña del controlador del ascensor para la autenticación.

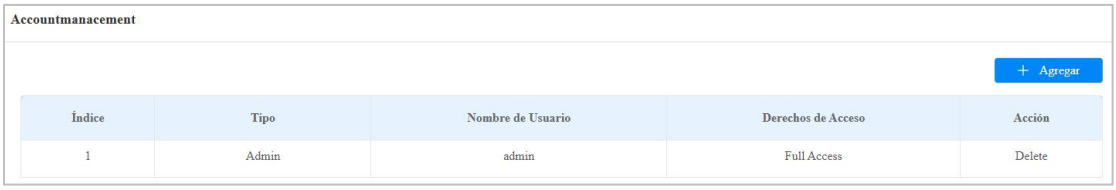
- Parámetro de número de piso: Introduzca el parámetro de número de planta proporcionado por Akuvox. La cadena de parámetros por defecto es «$planta». Puede definir su propia cadena de parámetros si es necesario.
- URL Para Activar Piso Específico: Introduzca la URL del control de ascensores Akuvox para activar un piso específico. La URL es /cdor.cgi?open=0&door=$floor, pero la cadena «$floor» al final debe ser idéntica a la cadena de parámetros que usted definió.
- URL para activar todos los pisos: Introduzca la URL de Akuvox para activar todos los pisos.
- URL para cerrar todos los pisos: Introduzca la URL de Akuvox utilizada para cerrar todos los pisos, lo que significa que todos los botones activados para los pisos correspondientes dejarán de ser válidos.
- Desde donde empieza el piso: Por ejemplo, si selecciona -3, la 3ª planta del sótano se considerará la primera planta coincidente con el relé nº 1 (primera planta).
- Ubicación del dispositivo: Seleccione la planta donde está instalado el dispositivo.

Modificación de Contraseñas

Gestión de Cuentas

Puede añadir cuentas de administrador y de usuario y configurar sus contraseñas para iniciar sesión en la interfaz web del dispositivo.

Vaya a la interfaz web Sistema > Seguridad > Gestión de cuentas. Haga clic en +Agregar para crear una cuenta.

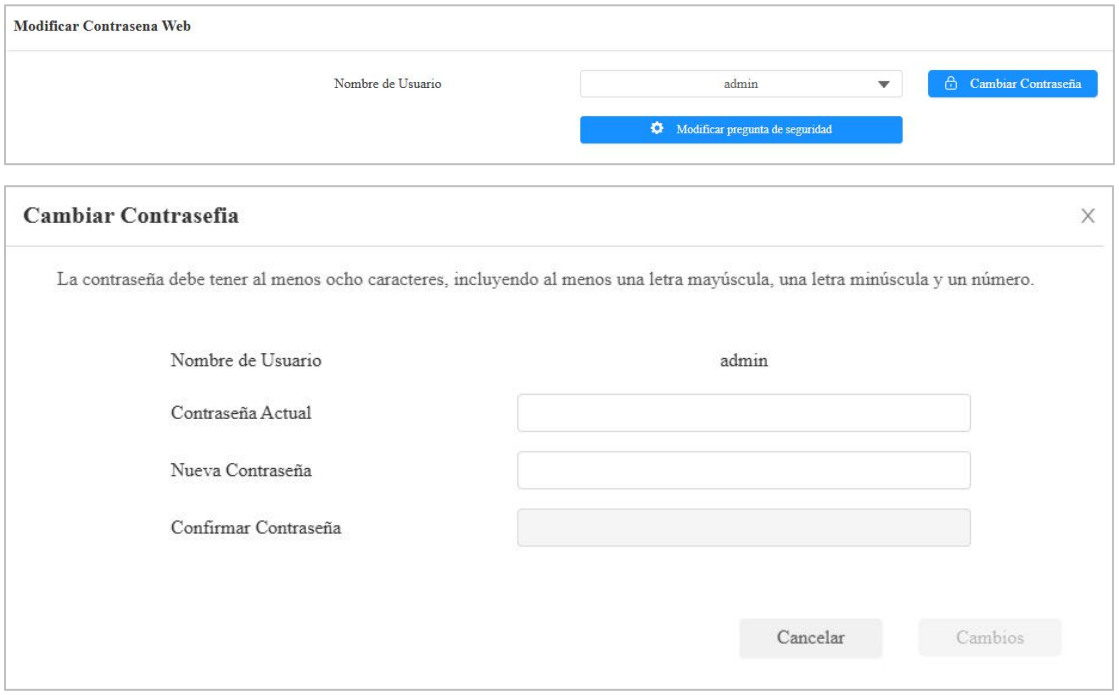


Modificación de la Contraseña de la Interfaz Web

You can modify the device web interface login password for both administrator and user accounts.

Go to the System > Security > Web Password Modify interface. Select admin for the administrator account and select user for the user account.

Click Change Password to modify the password.

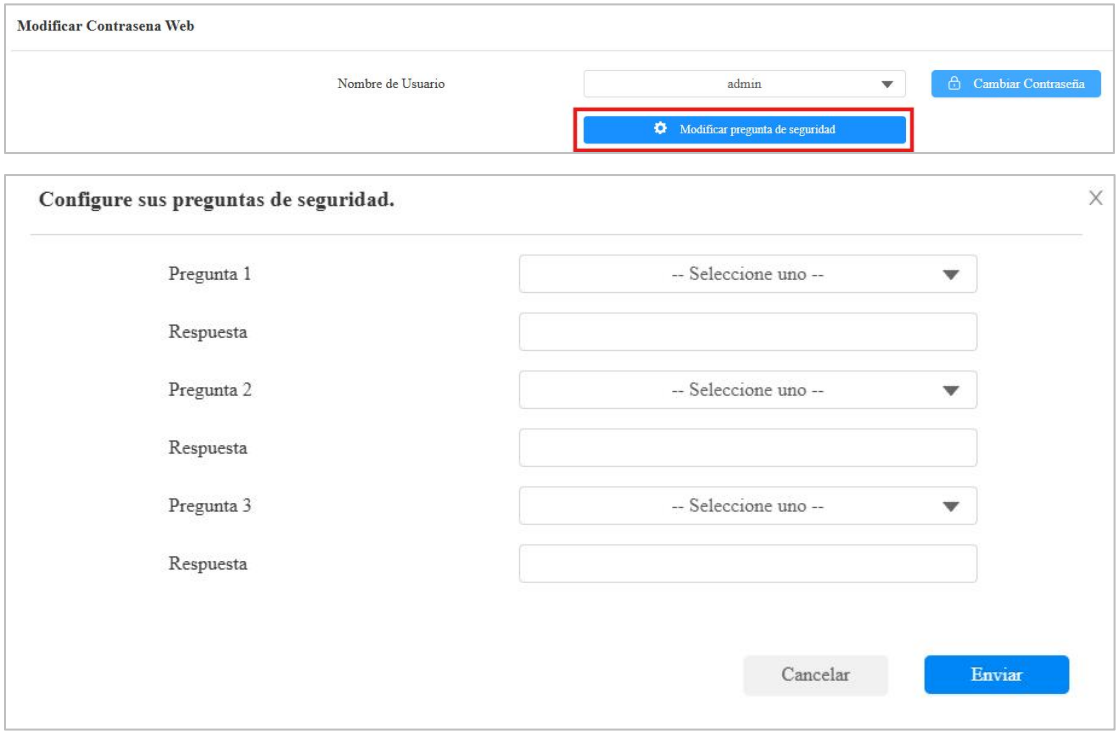


Modificar Preguntas de Seguridad

Las preguntas de seguridad te permiten restablecer la contraseña web si la olvidas. Después de configurar las preguntas de seguridad, puedes 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.



Modificar el Código Admin

El código de administración se utiliza para acceder a la configuración de administración del dispositivo.

El valor predeterminado es 2396. Puede cambiar la contraseña en la interfaz Sistema > Seguridad > Configuración del código admin.

Modificar Código de Servicio

El código de servicio se utiliza para acceder a los ajustes que incluyen el PIN público, el PIN privado y la modificación del código de la tarjeta de usuario. Puede modificar el código en el dispositivo.

Pulse *2396# en el teclado del dispositivo y pulse 2 y luego 3 para acceder a la pantalla de configuración del código de servicio.

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 > Programa de reinicio.

Restablecer

Reinicie el dispositivo en la interfaz web Sistema > Actualizar.