Manual de configuración para intercomunicadores 2N IP

v.2.43

www.2n.com

Contenido:

1. Visión general del producto

Los **intercomunicadores** de puerta **2N IP** son capaces de sustituir el panel de timbres clásico con teléfono sonoro y todo el sistema de distribuciones, timbres e interfonos de casa en los edificios donde están instaladas las distribuciones del cableado estructurado. El intercomunicador proporciona servicios mucho más sofisticados y amplios que los interfonos de casa habituales. La instalación del intercomunicador en su red es muy sencilla, basta con conectarlo mediante el cable UTP a otros elementos de la red local y configurar los parámetros necesarios.

Gracias al protocolo integrado SIP el intercomunicador puede utilizar todos los servicios de las redes VoIP – desvío durante la ausencia (a otro centro de trabajo, al contestador o teléfono móvil) o redirigir la llamada (por ej. desde la secretaría hacia la persona concreta requerida).

Los intercomunicadores están equipados con un número opcional de botones de marcado rápido que permiten definir la llamada al número de usuario guardado previamente en la lista de usuarios en el intercomunicador. A cada botón de marcado rápido es posible asignar hasta tres números de teléfono a los que se puede llamar a la vez o uno por uno. Gracias al calendario integrado es posible configurar cada botón de manera que el participante llamado esté siempre disponible, o al contrario, impedir las llamadas a los números de teléfono determinados fuera del tiempo establecido.

Algunos modelos del **intercomunicador 2N IP** están equipados con el teclado numérico que se puede utilizar como cerradura de códigos o como el teléfono clásico con teclado.

Los **intercomunicadores 2N IP** permiten a los usuarios en la red seguir los acontecimientos delante dela cámara mediante el servicio de stream del vídeo. Gracias al soporte total del estándar ONVIF pueden convertirse en una parte del Sistema Video Surveillance en su edificio.

Los **intercomunicadores 2N IP** pueden estar equipados con el lector de tarjetas RFID que permite no solo habilitar el acceso al edificio a las personas autorizadas, sino a la vez convertirse en una parte del sistema de seguridad del edificio o del sistema de asistencia en su empresa.

Los **intercomunicadores 2N IP** están equipados con el interruptor de relé (de forma opcional con otros relés y salidas) mediante el cual se puede controlar la cerradura eléctrica u otros dispositivos conectados al intercomunicador. Para el intercomunicador es posible configurar de forma muy flexible cuando y como se deben activar estos interruptores – mediante el código, automáticamente por una llamada, pulsando el botón de marcado rápido, etc. Para aumentar la seguridad se recomienda siempre el uso de 2N® Relé de seguridad (Nº de referencia 9159010).

Los siguientes símbolos y pictogramas se utilizan en el manual:

Seguridad

- Siga **siempre** las recomendaciones aquí descritas para evitar daños personales.

Advertencia

- Siga **siempre** las recomendaciones aquí descritas para evitar daños en los dispositivos.

Precaución

- **Información importante** para el correcto funcionamiento del sistema.

Consejo

- **Información útil** para la funcionalidad rápida y eficiente.

Nota

- Información adicional.

2. Guía exprés de la configuración básica

Configuración de la conexión a la red local

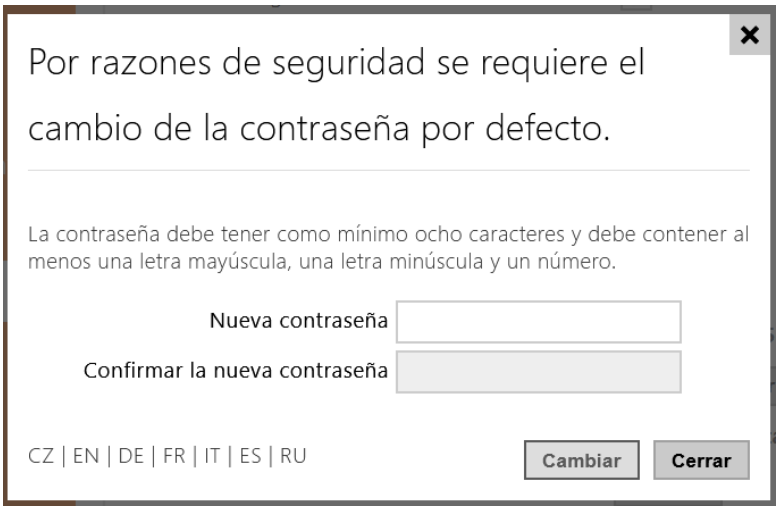
Para que Usted pueda iniciar la sesión en la interfaz de configuración del intercomunicador, debe conocer su dirección IP. Los **intercomunicadores 2N IP** tienen de la fábrica configurada la obtención automática de la dirección IP desde el servidor DHCP. Es decir, si Usted conecta el intercomunicador a la red en la cual se encuentra el servidor DHCP configurado de manera que asigne las direcciones IP a todos los dispositivos nuevos, obtendrá su propia dirección IP también su intercomunicador. La dirección IP del intercomunicador la puede averiguar directamente desde el estado del servidor DHCP (según la dirección MAC del intercomunicador expuesta en la placa de fabricación), eventualmente se la puede proporcionar directamente el intercomunicador a través de la función de voz – ver el Manual de instalación del modelo del intercomunicador correspondiente.

En el caso de que en su red no se encuentre el servidor DHCP, debe configurar el intercomunicador a la dirección IP estática mediante los botones del intercomunicador, ver el Manual de instalación del modelo correspondiente. Su intercomunicador luego obtendrá la dirección fija **192.168.1.100** la cual utilizará solo para el primer inicio de sesión y luego la podrá cambiar.

En el caso de que ya conozca la dirección IP de su intercomunicador, introdúzcala en su explorador preferido. Recomendamos utilizar la versión actual del explorador Chrome, Firefox o Internet Explorer 9+. Los **intercomunicadores 2N IP** no están plenamente compatibles con las versiones más antiguas de los exploradores.

Para el primero inicio de sesión en la interfaz de configuración utilice el nombre admin y la contraseña 2n (contraseña válida tras la puesta del dispositivo en estado inicial).

El intercomunicador requiere a la hora del primer inicio de sesión el cambio de contraseña. Solamente contraseñas fuertes son aceptables – que contienen al menos ocho caracteres que incluyen al menos una letra mayúscula, una letra minúscula y un número.



Memorice bien la contraseña elegida, eventualmente apúntesela. En el caso de que se le olvide la contraseña, tendrá que poner el intercomunicador en estado inicial (ver el manual de instalación del modelo correspondiente) y con ello perderá a la vez todos los cambios realizados de la configuración.

Consejo

- FAQ: Dirección IP – Como averiguar la dirección IP del intercomunicador 2N IP

Actualización del firmware

Tras el primer inicio de sesión en el intercomunicador recomendamos al mismo tiempo actualizar el firmware del intercomunicador. El firmware más reciente para su intercomunicador lo encontrará en las páginas www.2n.cz. Para la actualización del firmware sirve el botón **Actualizar Firmware** en el menú **Sistema / Mantenimiento**. Tras el upload del firmware en el dispositivo el dispositivo se reiniciará una vez y la actualización está hecha. La actualización tarda aproximadamente medio minuto.

Configuración de la conexión al servidor SIP

Para que el intercomunicador pueda telefonear y para que esté disponible dentro del marco de su infraestructura VoIP, debe configurar varios parámetros importantes. Estos parámetros se configuran en el menú **Servicios / Teléfono / SIP**.

- **Nombre mostrado** – establezca el nombre que se mostrará en el teléfono del destinatario como la identificación de la persona que llama. Este nombre se muestra también en la ventana de inicio de sesión y en la página de inicio de la interfaz web.
- **Número de teléfono (ID)** – establezca el número de teléfono propio del intercomunicador (eventualmente otro ID inconfundible que consiste en caracteres y números). Este número, junto con el dominio, identifica de forma inconfundible al intercomunicador durante las llamadas y registros.
- **Dominio** – establezca el nombre de dominio del servicio en el que está registrado el intercomunicador. Normalmente coincide con la dirección SIP proxy o con el registrador. En el caso de que en su instalación del intercomunicador no utilice SIP proxy, introduzca la dirección IP del intercomunicador.

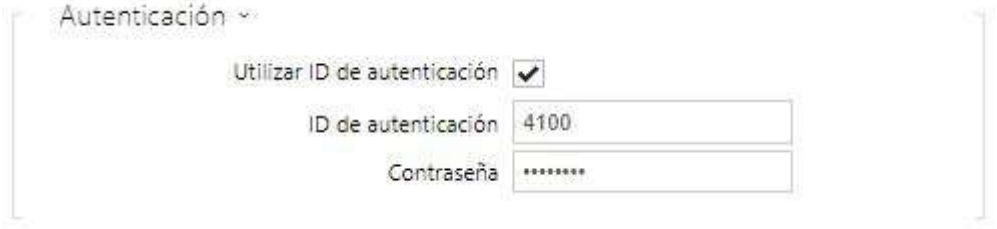
En el caso de que en su red utilice el servidor SIP (proxy, registrador), será necesario configurar la dirección de los siguientes elementos en la red:

- **Dirección proxy** – configure la dirección IP o el nombre de domino de SIP proxy.
- **Puerto proxy** – configure el puerto SIP proxy (habitualmente 5060).
- **Dirección de proxy de respaldo** – dirección IP o nombre de dominio de proxy SIP de respaldo. La dirección se utilizará en el caso de que el proxy principal no responda a las peticiones.
- **Puerto de proxy de respaldo** – configure el puerto de SIP proxy de respaldo (habitualmente 5060).

- **Permiso de registro** – permite el registro del intercomunicador con el registrador SIP configurado.
- **Dirección del registrador** – dirección IP o el nombre de dominio del Registrador SIP.
- **Puerto del registrador** – configura el puerto del registrador SIP (normalmente 5060).
- **Dirección del registrador de respaldo** – dirección IP o nombre de dominio del registrador SIP de respaldo. La dirección se utilizará en el caso de que el registrador principal no responda a las peticiones.
- **Puerto del registrador de respaldo** – configura el puerto del registrador SIP de respaldo (habitualmente 5060).
- **Tiempo de expiración del registro** – permite configurar el tiempo de vencimiento del registro, lo cual afecta a la carga de la red y del Registrador SIP por las peticiones de

registro enviados periódicamente. El Registrador SIP puede modificar el tiempo de la expiración sin su conocimiento.
- **Estado del registro** – muestra el estado actual del registro (No registrado, Regístrese..., Registrado, El registro finaliza...).
- **Causa del fallo** – muestra la causa del fallo del último intento del registro – muestra la última respuesta de error del registrador, por ej. 404 Not Found.

En el caso de que su servidor SIP requiera la autenticación de los dispositivos terminales, introduzca los siguientes parámetros:

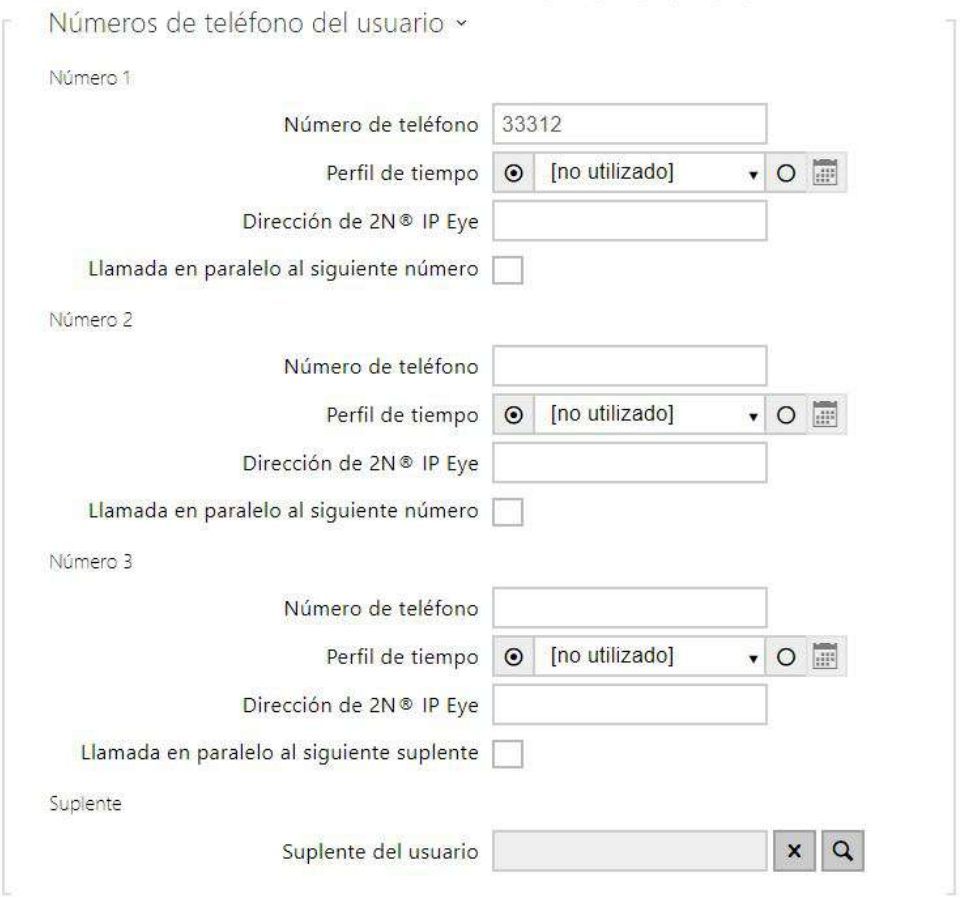


- **Contraseña** – introduzca la contraseña utilizada para la autenticación del intercomunicador.

Configuración de los botones del marcado rápido

Todos los modelos de los **intercomunicadores 2N IP** están equipados con botones de marcado rápido. En el caso de que el usuario pulse uno de los botones del marcado rápido se define la llamada al número de teléfono pre-configurado en la posición correspondiente en la lista de usuarios.

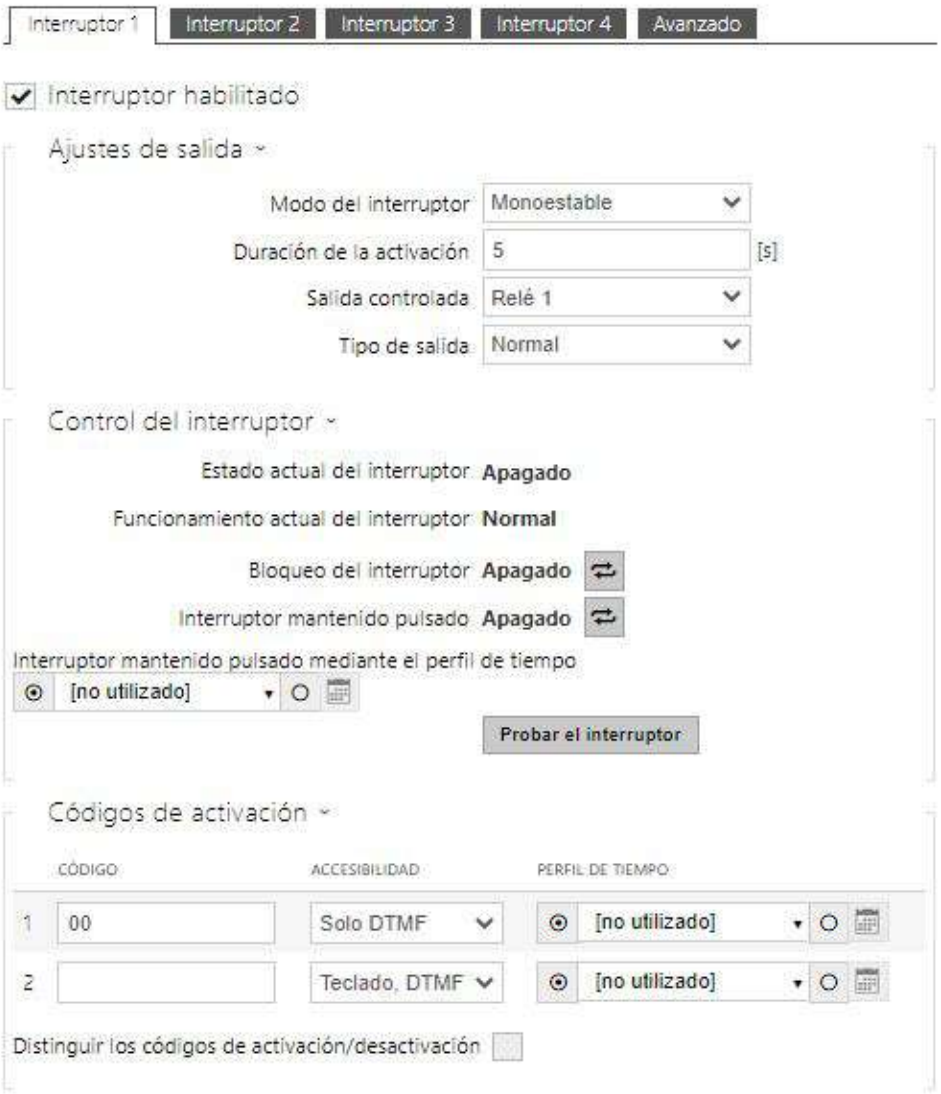
En el menú Hardware / Botones se muestra la lista de todos los botones potencialmente disponibles en el intercomunicador. La lista contiene botones, incluidos aquellos que no están presentes físicamente en el intercomunicador. En algunos modelos (**2N® IP Vario**, **2N® IP Verso**) está la lista de botones dividida en grupos de 8, event. 5 botones correspondientes a los módulos de botones de ampliación. En el campo de edición se pueden añadir usuarios mediante el icono  al marcarlo y confirmarlo con el botón añadir. El usuario deseado se puede buscar también en la lista utilizando el campo de fulltext según el nombre. Un botón del marcado rápido pueden compartir varios usuarios a la vez.



Puede utilizar los **intercomunicadores 2N IP** también con uno o varios teléfonos IP sin el servidor SIP. Para llamar desde el intercomunicador se utilizará el llamado Direct SIP Call. En tal caso en lugar de introducir el número de teléfono, introduzca la dirección SIP del teléfono llamado en formato sip:número de_teléfono@dirección_ip_del teléfono.

Configuración de la activación de la cerradura eléctrica

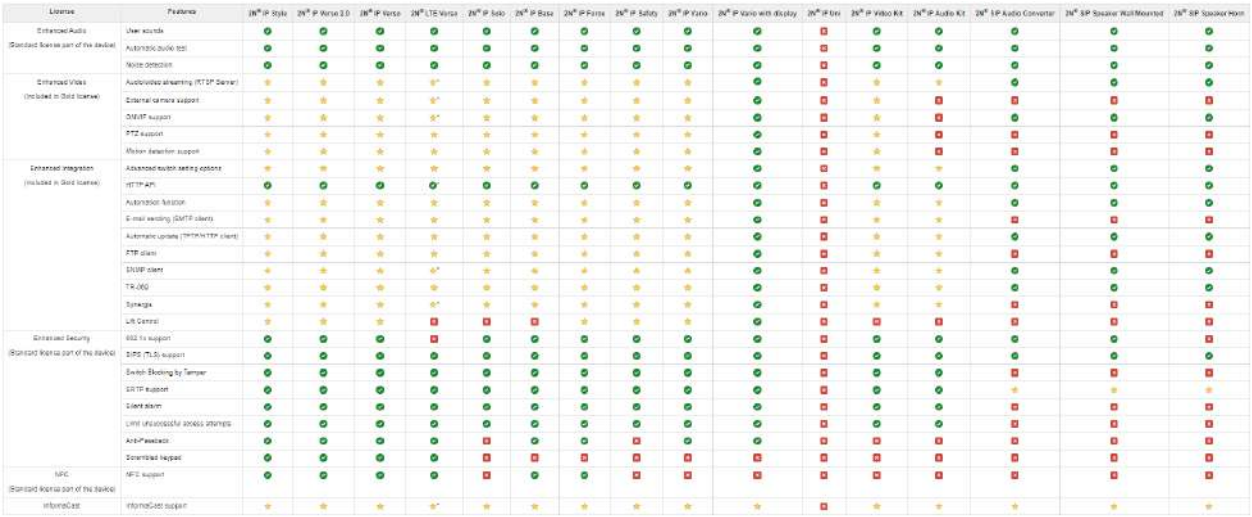
A los **intercomunicadores 2N IP** se puede conectar la cerradura eléctrica de puerta que se puede controlar utilizando el código introducido mediante el teclado numérico del intercomunicador, event. utilizando el código introducido mediante el teclado del teléfono IP durante la llamada. Conecte la cerradura eléctrica de puerta según la descripción en el Manual de instalación del modelo correspondiente.



En la solapa **Hardware / Interruptores / Interruptor 1** habilite el interruptor mediante el campo Interruptor habilitado, configure el parámetro salida controlada al cual está conectada la cerradura eléctrica de puerta. Luego configure uno o varios códigos para la activación del interruptor – cerradura eléctrica de puerta.

3. Diferencias entre modelos y licencias de funciones

Aquí se expone el resumen de lo que encontrará en este capítulo:



✅ – Contiene desde la fábrica
⭐ – Función con licencia, se puede comprar adicionalmente
❌ – No se puede utilizar

*) La disponibilidad del servicio depende de la configuración de la red del operador móvil.

> **⚠ Nota**
>
> - Todo lo que hace referencias a licencias no se aplica a los Estados Unidos, Canadá, México, el Caribe y América Central y del Sur.

3.1 Diferencias entre modelos

Este manual es común para toda la familia de los **intercomunicadores 2N IP** y por eso algunas de las funciones descritas aquí están disponibles solo en modelos concretos, event. están disponibles solo después de introducir la clave de licencia vigente. En este capítulo se expone el resumen de las diferencias entre cada uno de los modelos. La lista de las diferencias no es completa, se limita solo a aquellas que afectan las posibilidades de configuración. En el caso de que la función determinada no esté disponible en todos los modelos, en el capítulo correspondiente hay una nota y la referencia de este capítulo.

En la table siguiente está el resumen de las características y funciones de cada uno de los modelos de los **intercomunicadores 2N IP**.

Característica/ Modelo	2N® IP Style	2N® IP Verso 2.0	2N® IP Verso	2N® IP Base	2N® IP Solo	2N® IP Vario	2N® IP Force	2N® IP Safety	2N® IP Uni	2N® IP Audio Kit	2N® IP Video Kit
Números de referencia	9157...	91552...	9155…	9156...	91553...C	9137….	9151…	9152…	9153…	9154…	9154…C
Procesador Artpec-7	sí		no								
Cámara integrada	sí		opcional	sí		opcional		no			
Resolución de la cámara	2560 x 1920	1920 x 1440	1280 x 960			640 x 480	640 x 480 ó 1280 x 960				
Soporte de la cámara analógica externa	no										sí
Soporte de la cámara IP externa	sí								no		sí
Lector interno de tarjetas RFID	sí	opcional			no	opcional		no			
Pantalla	sí	opcional		no		opcional	no				

Característica/ Modelo	2N® IP Style	2N® IP Verso 2.0	2N® IP Verso	2N® IP Base	2N® IP Solo	2N® IP Vario	2N® IP Force	2N® IP Safety	2N® IP Uni	2N® IP Audio Kit	2N® IP Video Kit
Interruptor adicional	sí	opcional		no	opcional				no		
Número de botones de la unidad básica	0	1		1 ó 2	1	1, 3 o 6	1, 2 o 4	1	1 ó 2	hasta 16 botones programables externos	
Ampliación del número de botones (extendedores)	0	hasta 145		no		hasta 48	no				
Teclado numérico	sí	opcional		no		opcional		no			
Entrada digital	sí					opcional			no	2	
Códecs de audio de banda ancha (L16, G.722)	sí								no		sí
Potencia del amplificador	4 W	2 W				150 mW	10 W			10 W	
Configuración de la subida de volumen del micrófono	no									sí	
Ampliación de la potencia del amplificador a 10 W	no						sí		no	no	

Característica/ Modelo	2N® IP Style	2N® IP Verso 2.0	2N® IP Verso	2N® IP Base	2N® IP Solo	2N® IP Vario	2N® IP Force	2N® IP Safety	2N® IP Uni	2N® IP Audio Kit	2N® IP Video Kit
Tamper / Interruptor antisabotaje	sí	opcional		sí		no	opcional		sí	no	
Número de posiciones en la lista de usuarios	10 000								2	16	
Suplente en el caso de no disponibilidad	sí								no	sí	
Número de interruptores controlados	4			2	4				1	4	
Número de códigos universales de los interruptores	10			2	10				2	10	
Número de perfiles de usuario	20										
JPEG HTTP vídeo	sí							no			sí
Soporte de **2N® IP Eye**	sí							no			sí
Modo telefónico	sí			no		sí		no		sí	

Algunas funciones de los **intercomunicadores 2N IP** están disponibles solo tras introducir la clave de licencia válida (ver el capítulo Licencias).

3.2 Licencia de funciones

Licencia de funciones

Para el uso habitual del intercomunicador 2N IP basta con las licencias básicas que ya forman parte del dispositivo desde la fábrica. Los intercomunicadores 2N IP se pueden ampliar por otras funciones, las cuales están condicionadas por la licencia de pago.

Tipos de licencias

Algunas funciones de los **intercomunicadores 2N IP** están disponibles solo tras introducir la clave de licencia válida. Están disponibles los siguientes tipos de licencia:

- NFC (parte del dispositivo)
- Audio mejorado (parte del dispositivo)
- Seguridad mejorada (parte del dispositivo)
- Gold (Nº de referencia 9137909)
- InformaCast (Nº de referencia 9137910, Axis Nº de referencia 01381-001)

> **Nota**
>
> - La licencia InformaCast permite el uso del protocolo SingleWire InformaCast.

2N® IP Style, Verso, **Base**, **Solo**, **Vario**, **Force**, **Safety** a **Audio Kit** con **Video Kit** soportan este esquema de licencia. Para el modelo **2N® IP Uni** no está disponible ninguna licencia.

> **Consejo**
>
> - El resumen de las diferencias entre los modelos y las licencias de funciones los encontrará en el capítulo 3. Diferencias entre modelos y licencias de funciones.

El la siguiente table se enumeran las funciones que se activan mediante la introducción de las claves de licencia correspondientes a las licencias mencionadas. Las licencias se pueden combinar de cualquier manera.

Función	Enhanced Audio	Enhanced Vídeo	Enhanced Integration	Enhanced Security	NFC	InformaCast	IP intercoms Lift module license	Licencia
Sonidos de usuario	•							parte del dispositivo
Test automático de audio	•							parte del dispositivo
Detección de ruidos	•							parte del dispositivo
Streaming de audio/vídeo (servidor RTSP)		•						GOLD
Soporte de la cámara IP externa		•						GOLD
Soporte de ONVIF		•						GOLD
Soporte de la función PTZ		•						GOLD
Soporte de la detección de movimiento		•						GOLD
Opciones ampliados de la configuración de los interruptores			•					GOLD

Función	Enhanced Audio	Enhanced Vídeo	Enhanced Integration	Enhanced Security	NFC	InformaCast	IP intercoms Lift module license	Licencia
HTTP API (ver la nota más abajo)			•					parte del dispositivo
Función para la automatización			•					GOLD
Envío de E-mails (SMTP Client)			•					GOLD
Update automático (cliente TFTP/ HTTP)			•					GOLD
Cliente FTP			•					GOLD
Cliente SNMP			•					GOLD
TR-069			•					GOLD
Soporte de 802.1x				•				parte del dispositivo
Soporte de SIPS (TLS)				•				parte del dispositivo
Soporte de SRTP				•				parte del dispositivo
Alarma silenciosa				•				parte del dispositivo

Función	Enhanced Audio	Enhanced Vídeo	Enhanced Integration	Enhanced Security	NFC	InformaCast	IP intercoms Lift module license	Licencia
Limitación del número de intentos fallidos de acceso				•				parte del dispositivo
Bloqueo de interruptores				•				parte del dispositivo
Teclado mezclado				•				parte del dispositivo
Soporte de NFC					•			parte del dispositivo
Soporte de Informacast						•		InformaCast
Anti-Passback				•				parte del dispositivo
Genetec Synergis			•					GOLD
Control del ascensor							•	GOLD
Relé IP			•					GOLD

¿Qué más productos tienen los mismos esquemas de licencia?

2N® SIP Audio Converter, **2N® SIP Speaker** y **2N® SIP Speaker Horn**, que se venden con la licencia Gold instalada previamente, así que se puede realizar el upgrade solo a InformaCast.

¿Cómo puedo obtener la licencia?

La licencia es generada por la compañía 2N según el número de serie. En cuanto se decida sobre que licencia quiere, le comunicará a su distribuidor el número de serie de su unidad y él le proporcionará la clave de licencia.

La propia licencia la recibirá por ej. por e-mail en forma de clave (cadena alfa-numérica) que copiará e introducirá al intercomunicador.

Las licencias no están limitadas por el tiempo. Una vez obtenga la licencia, la tendrá para siempre.

En el caso de que quiera activar la licencia, conéctese a la interfaz de web del intercomunicador determinado e inserte la clave de licencia copiada en el campo en el menú Sistema / Licencia. Haga clic en Guardar y las funciones con licencia se activarán inmediatamente.

La licencia se puede descargar automáticamente en el menú Sistema / Licencia.

Consejo

- FAQ: Licencia para los intercomunicadores 2N IP – Cómo obtenerla

¿Puedo obtener una licencia demo?

Sí, tiene a su disposición 800 horas de la licencia Gold durante las cuales puede probar las características con licencia. Este demo está normalmente apagado, sin embargo, puede activarlo en la interfaz de web del intercomunicador determinado en el menú Sistema / Licencia. En el temporizador de la cuenta atrás verá el tiempo restante y una vez transcurrido el período de prueba se volverán a desactivar todas las funciones con licencia.

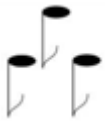
Para la licencia InformaCast no existe la opción de probarla.

4. Señalización de los estados de operación

Los **intercomunicadores 2N IP** señalizan mediante las notificaciones acústicas los cambios y pasos entre diferentes estados de operación. Para cada tipo de cambio existe otro tipo de notificación. La lista de cada una de las notificaciones está expuesta en la tabla siguiente:

Nota

- *La señalización de algunos de los estados mencionados se puede modificar, ver el capítulo Sonidos de usuario.*

Tonos	Significado
	**Señalización de la confirmación de la prolongación de la llamada** **El intercomunicador 2N IP** tiene por el motivo de protección contra el bloqueo configurada la duración máxima de llamada, ver el cap. Varios.
	**Aplicación interna iniciada** Tras encender la alimentación tras el reinicio del **intercomunicador 2N IP** comienza el inicio de la aplicación interna del **intercomunicador 2N IP**. El inicio satisfactorio de la aplicación interna está señalizado mediante esta combinación de tonos.
	**Conectado a la red local, obtenida dirección IP** Tras el inicio de la aplicación interna el **intercomunicador 2N IP** inicia la sesión en la red local. El inicio de sesión satisfactorio en la red local está señalizado mediante esta combinación de tonos.
	**Desconectado de la red local, dirección IP perdida** En el caso de que se desconecte el cable UTP del **intercomunicador 2N IP**, este estado está señalizado mediante esta combinación de tonos.
	**Número de teléfono no válido o código no válido par ala activación del interruptor** **Los intercomunicadores 2N IP** permiten mediante el teclado seleccionar directamente el número de teléfono de la sucursal o introducir el código para la apertura de la puerta. En el caso de que el código no sea válido, este estado está señalizado mediante esta combinación de tonos.

	**Puesta de los parámetros de red al estado inicial** Tras encender la alimentación está configurado el límite de tiempo de 30 segundos para la introducción del código de la puesta de los parámetros de red en estado inicial. La puesta de los parámetros de red en estado inicial está descrita en el cap. Configuración del dispositivo en el Manual de instalación determinado del **intercomunicador 2N IP**.
	**Señalización del final de llamada aproximándose** **Los intercomunicadores 2N IP** permiten configurar el límite de tiempo después del cual finaliza la llamada. La llamada se puede prolongar pulsando la tecla del teléfono VoIP. El límite de tiempo está configurado con el motivo de protección contra el bloqueo de la llamada.
	**Llamada conectada durante la llamada desde el teléfono VoIP al intercomunicador 2N IP** Al llamar desde el teléfono VoIP a los **intercomunicadores 2N IP** se reproduce un tono corto para señalizar la conexión de la llamada.

5. Configuración del intercomunicador

Inicio e sesión en la interfaz de web de configuración

El dispositivo se configura mediante la interfaz de web de configuración. Para poder acceder hay que conocer la dirección IP del dispositivo o el nombre de dominio del dispositivo. El dispositivo debe estar conectado a la red IP local y debe estar alimentado.

Nombre del dominio

La conexión con el dispositivo se puede realizar introduciendo la dirección del dominio en el formato *hostname.local* (por ej.: 2NIPStyle-00000001.local). Hostname del nuevo dispositivo está compuesto del nombre del dispositivo y del número de serie del dispositivo. Los formatos de los nombres de dispositivos se especifican más abajo. El número de serie se introduce en el nombre de dominio sin guiones altos. Hostname se puede cambiar más tarde en la sección Sistema > Red

Dispositivo 2N	Nombre del dispositivo en Hostname
2N IP Verso	2NIPVerso
2N IP Verso 2.0	2NIPVerso20

Dispositivo 2N	Nombre del dispositivo en Hostname
2N LTE Verso	2NLTEVerso
2N IP Style	2NIPStyle
2N IP One	2NIPOne
2N IP Vario	2NIPVario
2N IP Base	2NIPBase
2N IP Force	2NIPForce
2N IP Safety	2NIPSafety
2N IP Solo	2NIPSolo
2N IP Uni	2NIPUni

El inicio de sesión mediante el nombre de dominio tiene la ventaja en el caso de utilizar una dirección IP dinámica del dispositivo. Mientras que la dirección IP dinámica cambia, el nombre de dominio permanece igual. Para el nombre de dominio se pueden generar certificados firmados por la autoridad de certificación fiable.

Pantalla de inicio de resumen

La página de inicio aparecerá tras iniciar la sesión en la interfaz de web del intercomunicador. Puede volver a ella mediante el botón  situado en la esquina superior izquierda de las otras páginas de la interfaz de web. En el encabezado de la página aparece el nombre del intercomunicador (ver el parámetro Nombre mostrado en la configuración **Servicios / Teléfono / SIP**). Para elegir el idioma se puede utilizar el menú el la equina superior derecha de la interfaz de web. Puede cerrar la sesión en el dispositivo utilizando el botón Cerrar sesión en la esquina superior derecha de la página, visualizar el asistente mediante el icono del signo de interrogante o utilizando la burbuja proporcionar el feedback.

La página de inicio sirve como el primer nivel del menú y como navegación rápida (al hacer clic sobre cualquier baldosa) hacia las partes determinadas de la configuración del intercomunicador. En algunas baldosas aparece a la vez el estado de los servicios determinados.

Menú de configuración

La configuración de los **intercomunicadores 2N IP** está dividida en 5 menús principales – **Estado**, **Directorio**, **Hardware**, **Servicios** y **Sistema**; cada menú está dividido en más partes, ver el resumen siguiente.

Estado

- **Dispositivo** – información básica acerca del intercomunicador
- **Servicios** – información acerca de los servicios iniciados y su estado
- **Licencia** – estado actual de la licencia y de las funciones disponibles del intercomunicador
- **Registro de acceso** – muestra los últimos 10 registros de accesos
- **Registros de llamadas** – muestra las últimas 20 llamadas realizadas
- **Eventos** – muestra los últimos 500 eventos registrados por el dispositivo

Directorio

- **Usuarios** – configuración de números de teléfono de los usuarios, botones de llamada rápida, tarjetas de acceso y códigos de usuario para el control de los interruptores
- **Perfiles de tiempo** – configuración de los perfiles de tiempo
- **Vacaciones** – configuración de los festivos periódicos y variables en el año de calendario

Llamada

- **Configuración general** – configuración que afecta a las llamadas entrantes y salientes
- **Marcación** – configuración de la asignación de los botones de marcado rápido a cada uno de los usuarios
- **SIP 1 / SIP 2** – configuración completa de dos cuentas SIP del intercomunicador
- **Llamadas locales** – configuración de las llamadas locales, conexión, parámetros del vídeo
- **Crestron**– configuración de la conexión con dispositivos Crestron

Hardware

- **Interruptores** – configuración de la activación de la cerradura eléctrica, iluminación, etc.
- **Audio** – volumen del audio, tono de señalización, etc., parámetros del micrófono
- **Cámara** – configuración de la cámara interna y de la cámara IP externa
- **Teclado** – configuración del comportamiento de los botones y del teclado
- **Retroiluminación** – configuración del nivel de la retroiluminación
- **Pantalla** – configuración básica de la pantalla
- **Lector de tarjetas** – configuración del lector de tarjetas, Wiegand interface
- **Entradas digitales** – configuración de las entradas digitales
- **Extensiones** – configuración de los módulos de ampliación **2N® IP Verso**
- **Control del ascensor** – configuración para el acceso a cada una de las plantas mediante el ascensor

Servicios

- **Control de acceso** – la configuración de las reglas para la llegada y la salida
- **Transmisión** – configuración del stream de audio y vídeo (ONVIF, RTSP, Multicast. etc.)
- **E-Mail** – configuración de los e-mails enviados y conexión al servidor SMTP
- **Automatización** – configuración flexible del intercomunicador según los requisitos específicos del usuario
- **HTTP API** – configuración de la autorización HTTP API
- **Sonidos del usuario** – configuración y upload de los sonidos de usuario
- **Servidor Web** – configuración del servidor web y de la contraseña de acceso
- **Prueba de audio** – configuración del test automático del audio
- **SNMP** – configuración del servicio SNMP

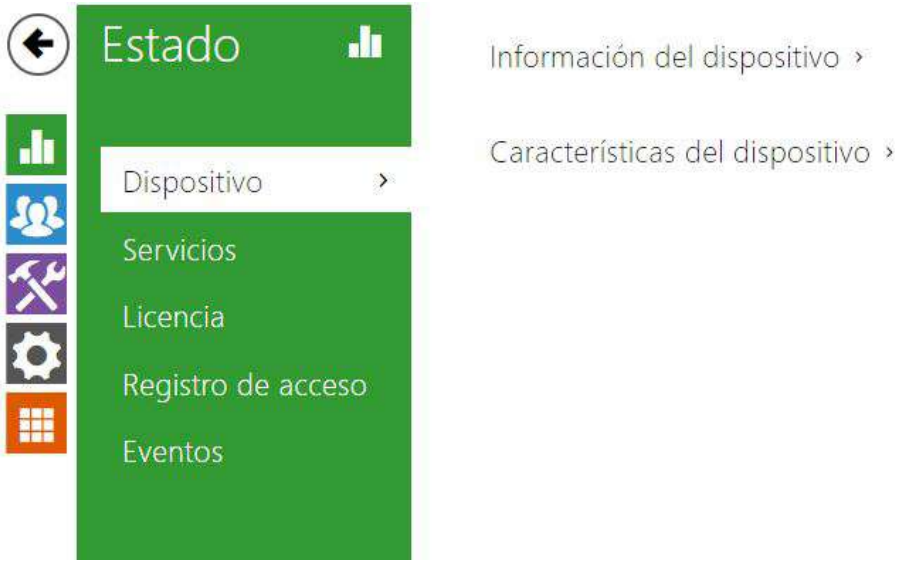
Sistema

- **Red** – configuración de la conexión a la red local, 802.1x, captación de los paquetes
- **Fecha y hora** – configuración de la hora real y del huso horario
- **Función** – configuración de las funciones de test
- **Licencia** – configuración de licencias, activación de la licencia trial
- **Certificados** – configuración de certificados y claves privadas
- **Aprovisionamiento** – configuración de las actualizaciones automáticas del firmware y de la configuración
- **Syslog** – configuración del envío de mensajes de sistema al servidor syslog
- **Mantenimiento** – respaldo y restauración de la configuración, actualización del firmware

Aviso

Precaución
Con el fin de asegurar el pleno funcionamiento y las salidas garantizadas recomendamos encarecidamente una verificación de la puntualidad de la versión del producto o instalación ya durante el proceso de instalación. El cliente tiene en cuenta que el producto o instalación puede alcanzar los rendimientos garantizados y ser plenamente operativo de acuerdo con las instrucciones del productor sólo mediante el uso de la versión más reciente del producto o instalación, que ha sido probado para la plena interoperabilidad y no ha sido determinado por el productor como incompatible con ciertas versiones de otros productos, sólo de conformidad con las instrucciones del productor, directrices, manual o recomendación y sólo en conjunción con los productos adecuados y las instalaciones de los otros productores. Las versiones más recientes están disponibles en el sitio web https://www.2n.com/cs_CZ/, o instalaciones específicas, según su capacidad técnica, permiten la actualización en la interfaz de configuración. En caso de que el cliente utilice cualquier otra versión del producto o instalación que no sea la más reciente, o la versión que haya sido determinada por el productor como incompatible con ciertas versiones de los productos o instalaciones de otros productores, o el producto o la instalación de una manera incompatible con las instrucciones, directrices, manual o recomendación del productor o en conjunción con productos o instalaciones inadecuadas de los otros productores, es consciente de todas las posibles limitaciones de funcionalidad de dicho producto o instalación y todas las consecuencias relacionadas. En caso de que el cliente utilice una versión distinta a la más reciente del producto o instalación, o la versión que ha sido determinada por el productor como incompatible con ciertas versiones de los productos o instalaciones de otros productores, o el producto o instalación de una manera incompatible con las instrucciones, directrices, manual o recomendación del productor o en conjunto con productos o instalaciones inadecuadas de los otros productores, él o ella está de acuerdo en que la empresa 2N TELEKOMUNIKACE a. s. no es responsable de ninguna limitación de la funcionalidad de dicho producto, ni de ningún daño, pérdida o perjuicio relacionado con dicha limitación potencial.

5.1 Estado



En el menú **Estado** se muestra de forma clara la información actual y las características del dispositivo. El menú está dividido en cinco solapas: **Dispositivos**, **Servicios**, **Registro de accesos**, **Registros de llamadas** y **Sucesos**.

Solapa Dispositivo

Muestra la información sobre el modelo y sus características, versión del firmware y bootloader, etc.

- **Certificado instalado de fábrica** – especifica el certificado de usuario y la clave privada mediante los cuales se verifica la autorización del intercomunicador para comunicarse con el servidor de terceros.
- **Localizar dispositivo** – señalización óptica y acústica del dispositivo. La señalización óptica es posible solo en el caso de que el aparato esté equipado con la retroiluminación (**2N® IP Style, 2N® IP Verso**, **2N® IP Solo**, **2N® IP Base**, **2N® IP Vario**, **2N® IP Force**, **2N® IP Safety** y **2N® IP Uni**). En el caso de que en el aparato no esté integrado el reproductor, asegúrese de que a la conexión de la señalización acústica esté conectado el reproductor externo (**2N® IP Audio Kit** y **2N® IP Video Kit**).

Solapa Servicios

Muestra el estado de la interfaz de red y de los servicios determinados.

Solapa Registro de acceso

En la solapa **Registro de accesos** se muestran los 10 últimos registros sobre las tarjetas acercadas. Cada registro contiene la hora del acercamiento de la tarjeta, su ID, tipo y descripción que contiene la información sobre si la tarjeta es válida, eventualmente a que usuario ha sido asignada.

Záznamy

	ČAS	ID KARTY	TYP KARTY	POPIS
1	04/09/2013 09:33:01	AA7C56	HID-26, H10301	Access denied
2	04/09/2013 09:32:49	150868	HID-26, H10301	Access denied
3	04/09/2013 09:32:14	CCD0000C	HID-35, Corp.1000	Access denied
4	04/09/2013 09:31:52	0F0304CF48	EM41XX	Access denied
5	04/09/2013 09:31:47	3F00F31572	EM41XX	Access denied
6	04/09/2013 09:31:41	AA7C56	HID-26, H10301	Access denied
7				
8				
9				
10				

Solapa Registros de llamadas

Los registros de llamadas muestran el resumen de todas las llamadas realizadas. Cada llamada lleva información sobre el tipo del contacto, ID de la persona llamada, sobre la fecha y hora de la realización, tiempo de duración y estado (entrante, saliente, perdida, aceptada en otro lugar, botón del timbre). Campo para la búsqueda permite la búsqueda de fulltext en el nombre de las llamadas. El campo de marcado sirve para marcar todos los registros para el borrado masivo. El registro de llamada seleccionado se puede borrar también de forma individual utilizando el botón  . El resumen muestra los últimos 20 registros que están ordenados desde el más reciente hasta el más antiguo.

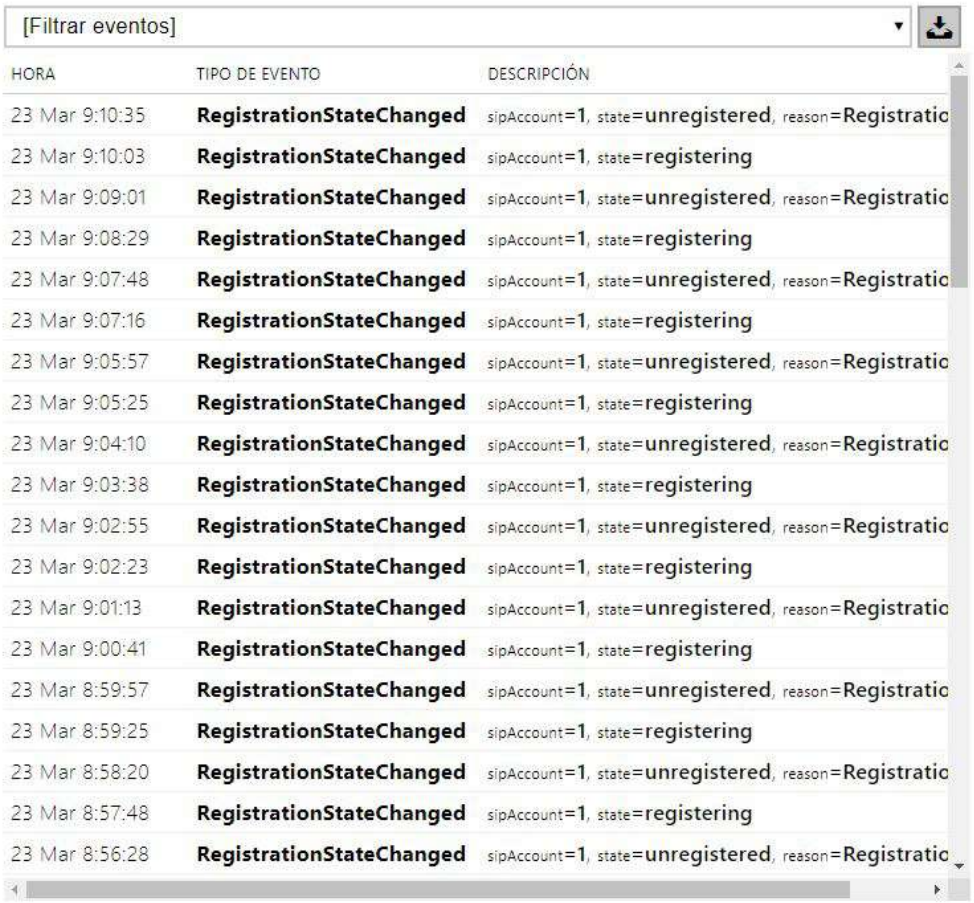
Registros de llamadas

Buscar

	Nombre	Fecha y hora	Tiempo de llamada	
☐	sip:5742014380@proxy-19.my2n.com:5...	2022-04-04 08:45:10	0s	🗑
☐	sip:5742014380@proxy-19.my2n.com:5...	2022-04-04 08:45:09	0s	🗑
☐	sip:5742014380@proxy-19.my2n.com:5...	2022-04-04 08:45:08	0s	🗑
☐	IndoorViewDagmar	2022-03-02 12:52:45	29s	🗑
☐	10.0.24.21	2022-03-02 11:05:04	0s	🗑

Solapa Eventos

En esta solapa se pueden ver los últimos 500 sucesos registrados por el dispositivo. Cada suceso contiene la hora y la fecha de la captura, tipo del suceso y descripción que especifica con más detalle el suceso. Los sucesos se pueden filtrar en el menú desplegable encima del propio registro de sucesos según el tipo del suceso.



-  – sirve para exportar todos los sucesos registrados en el archivo CSV.

Suceso	Significado
AccessLimited	Suceso que se produce tras introducir 5 intentos fallidos de autenticación del usuario (tarjeta, código, huella dactilar). El módulo de acceso se bloqueará durante 30 segundos incluso en el caso de que la siguiente autenticación haya sido correcta.

Suceso	Significado
ApiAccessRequested	Suceso cuando se ha enviado la solicitud a /api/accesspoint/grantaccess con resultado "success" : true.
AccessTaken	Al acercar la tarjeta en la zona de Anti-passback.
AudioLoopTest	Resultado del test de audio realizado.
CallSessionStateChanged	Suceso que describe el sentido, estado de la llamada, dirección, número creado por sesión y qué número de llamada se había generado.
CallStateChanged	Al cambiar el estado de la llamada (ringing, connected, terminated) indica también el sentido (entrante, saliente) y la identificación de la parte opuesta o de la cuenta SIP.
CardHeld	Tras el acercamiento de la tarjeta que dura 4 segundos o más.
CardEntered	Al acercar la tarjeta.
CodeEntered	Tras introducir el código que termina con el símbolo * en el teclado numérico.
DeviceState	Indicación del estado del dispositivo, como por ejemplo iniciación.
DoorOpenTooLong	Detección de la puerta abierta mucho tiempo, configurable en Hardware / Puerta / Puerta.
DoorStateChanged	Detecta al apertura/cierre de la puerta. La configuración se puede realizar en Hardware / Puerta / Puerta.
DtmfEntered	Recepción del código DTMF en la llamada o de forma local fuera de la llamada.
DtmfPressed	Introducción del código DTMF en la llamada o de forma local fuera de la llamada.
DtmfSent	Envío del código FTMF en la llamada o de forma local fuera de la llamada.
FingerEntered	Autorización mediante la huella dactilar.

Suceso	Significado
InputChanged	Señaliza el cambio de la entrada lógica.
KeyPressed	Al pulsar el botón (los números son 0, 1, 2 ..., 9 y los botones del marcado rápido son %1, %2 etc.).
KeyReleased	Al soltar el botón (los números son 0, 1, 2 ..., 9 y los botones del marcado rápido son %1, %2 etc.).
LiftFloorsEnabled	Acceso a la planta mediante el ascensor.
LiftStatusChanged	Detección de la conexión/desconexión del módulo Lift Control.
LoginBlocked	Al introducir 3 logins incorrectos en la Web, dispositivo. Contiene los datos sobre la dirección OP de estos accesos.
MobKeyEntered	Autorización mediante bluetooth.
MotionDetected	Tras activar la detección del movimiento, la configuración se puede realizar en Hardware / Cámara / Cámara interna.
NoiseDetected	Tras activar la detección del ruido, la configuración se puede realizar en Hardware / Audio.
OutputChanged	Señaliza el cambio del estado de la salida lógica.
RegistrationStateChanged	Cambio del estado del registro al SIP proxy.
RexActivated	Suceso al activar la entrada que está configurada para el botón REX.
SilentAlarm	Suceso de la alarma silenciosa tras introducir el código que es superior al código correcto por uno. Es decir, el código para la apertura es 123 y el código de la alarma silenciosa es 124. O tras acercar el dedo al módulo del lector de huellas dactilares que está señalizado para ser utilizado para la activación de la alarma silenciosa.
SwitchesBlocked	Interruptores bloqueados por introducir el acceso no válido.

Suceso	Significado
SwitchOperationChanged	Cambio del funcionamiento del interruptor (señaliza el estado del bloqueo o el pulsado mantenido del interruptor, arranque y reinicio del temporizador o su finalización – paso al pulsado mantenido permanentemente).
SwitchStateChanged	Cambio del estado del interruptor, configuración en Hardware / Interruptores.
TamperSwitchActivated	Señaliza la activación del interruptor antisabotaje – apertura de la cubierta del dispositivo. La función del interruptor antisabotaje debe configurarse en el menú Entradas digitales / Interruptor antisabotaje.
UnauthorizedDoorOpen	Detección de la apertura no autorizada de la puerta, configurable en Hardware / Puerta / Puerta.
UserAuthenticated	Señaliza la autenticación del usuario y la siguiente apertura de la puerta.
UserRejected	Verificación no válida del usuario.
VirtualInput	Cambio de la entrada virtual.
VirtualOutput	Cambio de la salida virtual.
CallSessionStateChanged	Informa sobre la fase en la cual se encuentra la llamada (creación, establecimiento de conexión, sonido del tono, conexión, finalización).

5.2 Directorio

Aquí se expone el resumen de lo que encontrará en este capítulo:

5.2.1 Usuarios

La lista de usuarios es una de las partes más importantes de la configuración del intercomunicador. Contiene la información importante sobre los usuarios que hacen accesibles las funciones del intercomunicador, como es la apertura de la puerta mediante las tarjetas RFID o activación de la cerradura de código, información para el usuario sobre las llamadas perdidas mediante e-mails, etc.

Puede contener hasta 10 000 usuarios (en cada uno de los módulos de los **intercomunicadores 2N IP** puede variar el número de elementos). Contiene usuarios que deben estar accesibles mediante los botones de marcado rápido (se les puede llamar), pero a la vez también usuarios que deben tener solo acceso al edificio mediante las tarjetas RFID, código, etc.

En el caso de que usted utilice el lector externo de tarjetas conectado al intercomunicador a través de la interfaz wiegand, durante la transmisión de la tarjeta ID mediante esta interfaz se reduce ID a 6 u 8 caracteres (según la configuración del modo de transmisión). En el caso de que acerque la misma tarjeta al lector interno, obtendrá un ID completo que es normalmente más largo – 8 caracteres o más. Sin embargo, los últimos 6, eventualmente 8 caracteres ID, son idénticos. Esto se utiliza a la hora de comparar las tarjetas ID con la base de datos en el intercomunicador – en el caso de que los ID comparados tienen longitud diferente, se comparan desde el final y la coincidencia debe hallarse en al menos 6 caracteres. En el caso de que los ID son igual de largos, se comparan todos los caracteres. Con este mecanismo se logra la compatibilidad mutua del lector interno y externo.

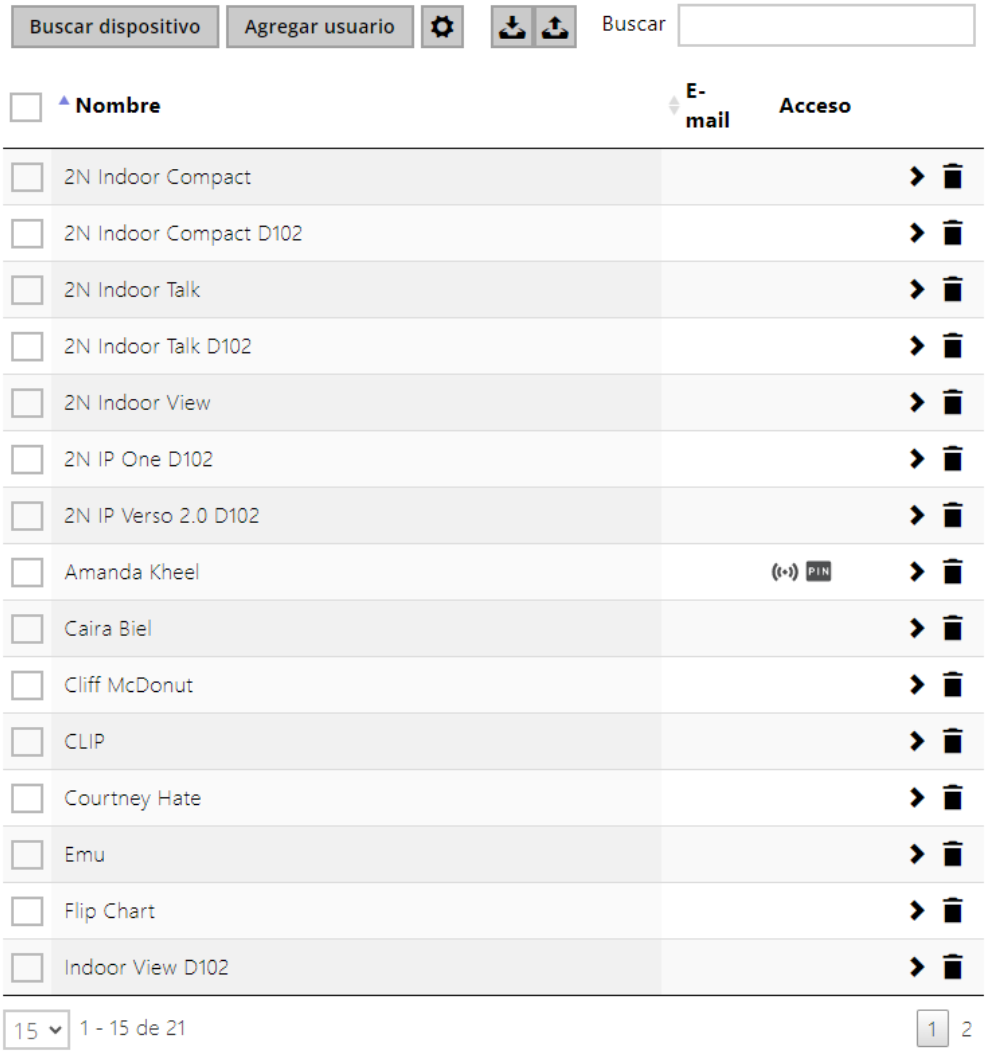
Todas las tarjetas acercadas al lector internos o aceptadas mediante la interfaz wiegand están siendo registradas y las últimas 10 tarjetas las puede visualizar en el menú **Estado / Historial de accesos**. En la lista puede encontrar, a parte de las tarjetas ID, también los tipos de ellas, hora del acercamiento y eventualmente otra información. En el caso de un sistema pequeño puede utilizar para la introducción de las tarjetas ID un truco sencillo – acerque la tarjeta al lector del intercomunicador y búsquela en la solapa **Historial de accesos**. Marque las tarjetas ID con el ratón, por ej. haciendo el doble clic sobre el ID de la tarjeta, y pulse las teclas CTRL+C. Ahora tiene las tarjetas ID en el buzón y utilizando las teclas CTRL+V las puede introducir en cualquier campo en la configuración del intercomunicador.

Tras acercar la tarjeta al lector RFID se compara el ID de la tarjeta con la base de datos de las tarjetas en el intercomunicador. En el caso de que el ID de la tarjeta acercada coincide con una de las tarjetas en la base de datos, se realiza la acción correspondiente – activación del interruptor (desbloqueo de la cerradura eléctrica de la puerta, etc.). El número del interruptor activado lo puede cambiar en la configuración **Hardware / Lector de tarjetas** mediante el parámetro Interruptor asociado (modelos **2N® IP Base**, **Vario**, **Force**), eventualmente en la configuración **Hardware / Módulos** mediante el parámetro **Interruptor asociado** en el módulo del lector de tarjetas (modelo **2N® IP Style**, **2N® IP Verso**).

La vinculación de los usuarios con los botones de marcado rápido se realiza en el menú **Hardware / Botones**. Los vínculos entre cada uno de los usuarios y los botones se pueden cambiar según la necesidad. La mayoría de los **intercomunicadores 2N IP** está equipada con uno o varios botones de marcado rápido. Su cantidad, posibilidad de ampliación, la encontrará en el manual de instalación del modelo del intercomunicador correspondiente.

Advertencia

- Desaconsejamos modificar el directorio del dispositivo que está siendo gestionado mediante **2N® Access Commander** a través de la interfaz de web del dispositivo. Tras la sincronización con **2N® Access Commander** se perderán las modificaciones en el directorio realizados a través de la interfaz de web del dispositivo.



Función Búsqueda en el directorio funciona como búsqueda fulltext del nombre, números de teléfono y e-mail. Busca todas las coincidencias en toda la lista.
Un nuevo usuario se añade mediante el botón encima de la tabla. También es posible buscar el dispositivo en la red local y luego añadir este dispositivo en el Directorio como un contacto nuevo.

Para mostrar el detalle de la configuración del usuario sirve el icono . Para configurar las columnas de la tabla sirve el icono , la visualización por defecto de la tabla muestra el nombre, e-mail del usuario y sus accesos configurados. Para eliminar al usuario de la lista, cuando se borran todos sus datos introducidos, sirve el icono . En la columna para los accesos se muestran iconos que describen las autenticaciones activas del usuario. La posición del usuario en la lista está ordenada según el orden alfabético.

Desde/al dispositivo es posible, utilizando el icono / , exportar/importar el archivo CSV con la lista de usuarios. En el caso de que el directorio esté vacío, se exportará solo el archivo con el encabezado (en inglés), el cual puede servir como plantilla para la importación de los usuarios. En el caso de que se importase un archivo vacío solo con el encabezado y se selecciona la variante **Sustituir el directorio**, se borrará todo el directorio. En el caso de que en el directorio haya usuarios, se exportarán todos a excepción de los tipos especiales de usuarios. La importación permite cargar hasta 10 000 usuarios, dependiendo del tipo de dispositivo.

Aviso

- En el caso de modificar el archivo CSV mediante Microsoft Excel hay que guardar el archivo en el formato CSV UTF-8 (con separadores).

Cada registro en la lista de usuarios contiene los siguientes datos:

- **Nombre** – datos opcional que sirve para una mejor orientación en la lista, por ej. a la hora de buscar usuarios.
- **Fotografía** – permite cargar la fotografía del usuario. Tras hacer clic en el marco para introducir la fotografía aparecerá el Editor de fotografías que permite cargar la fotografía elegida desde el archivo, eventualmente crear una fotografía del usuario mediante la cámara integrada. La fotografía se puede cargar en el formato de tipo .jpg, .png y .bmp. Esta función está disponible solo para los modelos con pantalla, **2N® IP Style**, **2N® IP Verso** y **2N® IP Vario**.

Aviso

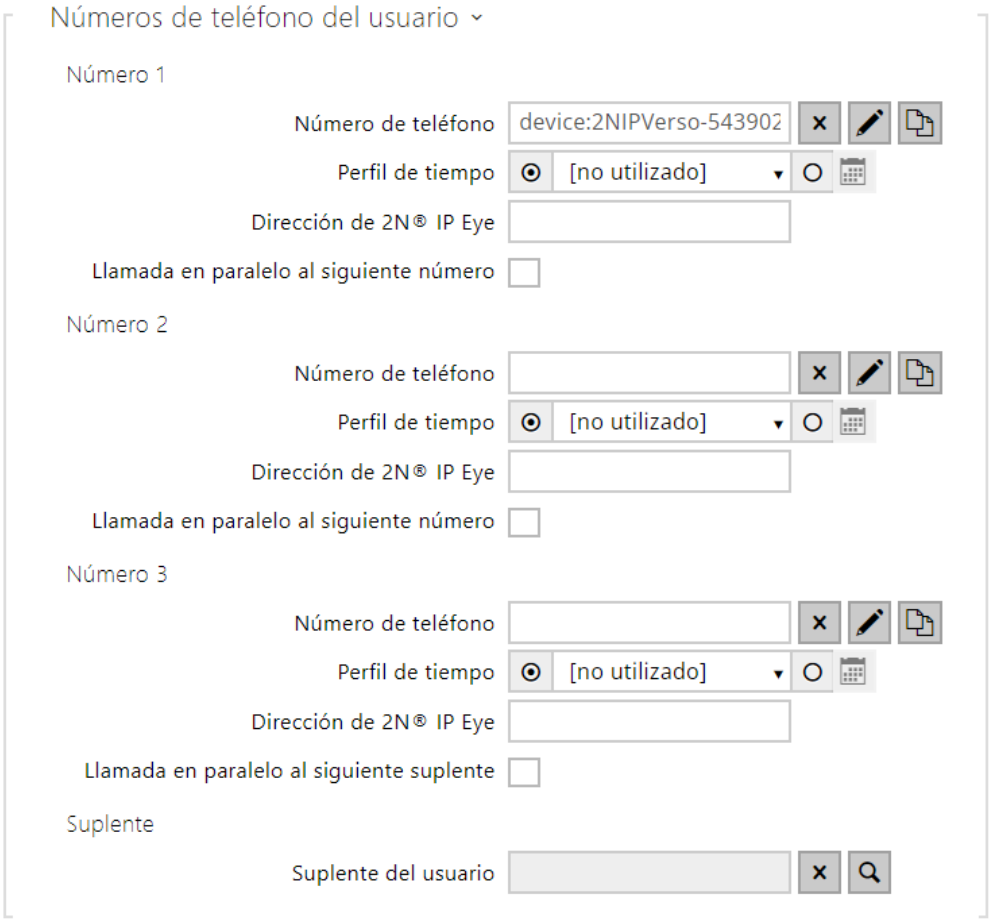
- Los usuarios especiales, por ejemplo aquellos creados por el servicio **My2N** o por el sistema **2N Access Commander**, no forman parte de la exportación del directorio.
- En el caso de que la sección de la imagen no ocupa todo el espacio de la ventana de recorte, la imagen resultante en **2N® IP Style** se centrará.

- **E-mail** – una o varias direcciones de e-mail del usuario a las que se puede enviar la información sobre las llamadas perdidas o sobre todas las llamadas realizadas. Las direcciones de e-mail se separan por una coma o punto y coma (por ej.: faith.pearl@gmail.com, kelly.black@gmail.com).
- **Número virtual** – número que se puede utilizar para llamar al usuario mediante el teclado numérico. El número puede contener de dos a cuatro dígitos. Los números virtuales no están relacionados con los propios números de teléfono del usuario. Pueden formar un plan numérico totalmente distinto que es independiente de los números de teléfono y de esta manera permite ocultar los propios números de teléfono de los usuarios. Esta función se puede utilizar con ventaja en las instalaciones donde el número de los botones de marcado rápido no es suficiente. La persona que viene introduce mediante el teclado numérico el número virtual y pulsa el botón *. En el caso de que utilice esta manera de llamada al usuario es conveniente colocar cerca del intercomunicador una lista resumida de los nombres de usuarios y de sus números virtuales, incluido un sencillo manual de uso. Las funciones de los números virtuales se pueden activar en el menú **Servicios / Teléfono / Llamadas / Llamadas salientes** con la ayuda del parámetro **Llamada a los números virtuales**. El número puede contener 1–7 dígitos.

- **Posición dentro del directorio** – en el estado inicial está creada solo la raíz del directorio a la cual se pueden añadir directamente los usuarios desde el directorio. La raíz del directorio no se puede borrar, ni renombrar. Un usuario puede formar parte de un máximo de 5 sub-grupos de la raíz del directorio.
- **Grupo de llamada** – sirve para poner el nombre a los grupos de usuarios que se mostrarán en el directorio de la pantalla. A la hora de llamar al grupo determinado se realiza la llamada a todos los usuarios a la vez. Tras aceptar una de las llamadas se cancelarán automáticamente las demás llamadas.

Aviso

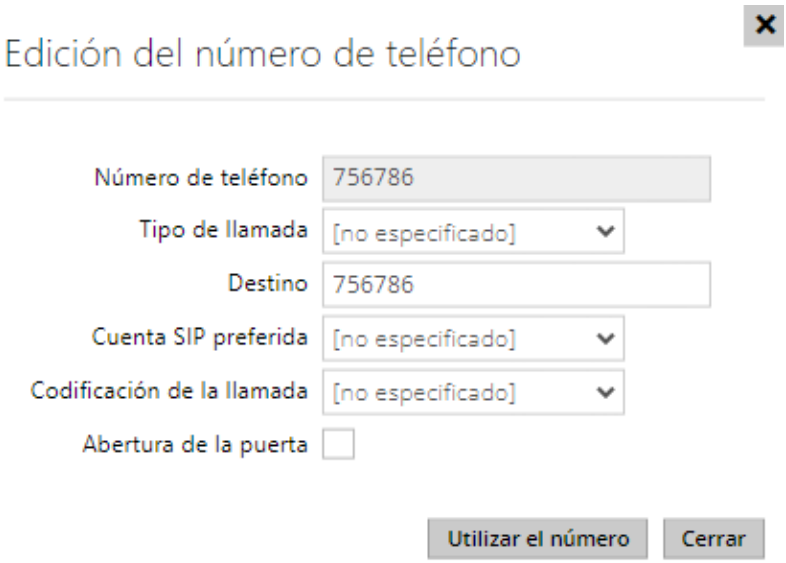
- Para los parámetros Nombre, Posición dentro del directorio y Grupo de llamada no están permitidos los símbolos <, > y /.



A cada usuario de la lista de pueden añadir hasta tres números de teléfono. En el caso de que el usuario no esté disponible en uno de los números, se utilizará tras el tiempo configurado del sonido de tono el siguiente número de teléfono. También se puede llamar a varios número a la vez, habilitando la función Llamar dentro del grupo con el número siguiente. La vigencia de cada uno de los números de teléfono se puede a la vez limitar mediante el perfil de tiempo.

- **Número de teléfono** – número de teléfono de la estación a la que se debe dirigir la llamada. Para realizar una llamada SIP directa introduzca la dirección en formato sip:[user_id@]dominio[:puerto], por ej.: sip:200@192.168.22.15 o sip:nombre@suempresa. Para la llamada local a los intercomunicadores 2N IP y a las unidades de respuesta introduzca device:ID del dispositivo. El nombre del dispositivo lo configurará en los dispositivos correspondientes. Para llamar al dispositivo Crestron

introduzca la dirección en formato RAVA:device_name. Si detrás del número de teléfono introduce caracteres **/1** resp. **/2**, se utilizará para las llamadas salientes de forma explícita la cuenta SIP 1, resp. 2. Al añadir /**S** es posible forzar una llamada cifrada, /**N** llamada no cifrada. Al añadir /**B** se activa la función de la apertura de la puerta mediante la devolución de llamada. La selección de la cuenta, el cifrado y la apertura mediante la devolución de llamada se puede realizar a la vez como por ej. /1S, /1B etc. El parámetro puede contener hasta 255 caracteres.
La configuración detallada del número de teléfono se puede realizar en la edición que se abrirá al pulsar  .



- **Tipo de llamada** – configura el esquema en URI del destino de la llamada. Con la elección Sin esquema, URI es completado con los datos de la configuración de la cuenta SIP. Utilice otra configuración para la llamada SIP directa (sip:), 2N llamada local (device:), llamada al dispositivo Crestron (rava:) o llamada con el sistema de administración del vídeo, por ejemplo AXIS Camera Station (vms:).
- **Destino** – configura otras partes de URI del destino de la llamada. Normalmente contiene el número, dirección IP, dominio, puerto o identificador del dispositivo. Para llamar a VMS se introduce el asterisco (*).
- **Cuenta SIP preferida** – para llamar se utiliza preferentemente la cuenta SIP número 1 o número 2.
- **Codificación de la llamada** – es posible configurar la codificación obligatoria de la llamada o, de lo contrario, llamada sin codificación.
- **Abertura de la puerta** – mediante la devolución de llamada"

- **Perfil de tiempo** – permite asignar un perfil de tiempo al número de teléfono y de esta manera controlar su vigencia. Si el perfil no está inactivo, no se utilizará el número de teléfono y para llamar se utilice el número de teléfono siguiente, en el caso de que esté definido.

- **Dirección 2N® IP Eye** – configura la dirección del ordenador al que se enviará la información mediante un mensaje UDP especial sobre la llamada en curso al número de teléfono del usuario. Este mensaje lo utiliza la aplicación **2N® IP Eye** para abrir y visualizar la ventana con la imagen de la cámara, lo cual pueden utilizar con ventaja los usuarios que no tienen a su disposición un vídeo-teléfono equipado con pantalla. La dirección del ordenador se introduce en el formato: dominio[:**puerto1**][:**puerto2**], por ej.: ordenador.suempresa.cz o 192.168.22.111. Los parámetros **puerto1** y **puerto2** son opcionales y se utilizan cuando en el camino entre el ordenador y el intercomunicador haya la traducción de direcciones (NAT) y haya que configurar los puertos en conformidad con el router u otro dispositivo que realiza NAT. El parámetro puerto1 (con el valor inicial 8003) define el puerto de meta para los mensajes UDP enviados a la aplicación **2N® IP Eye**. El parámetro puerto2 (con el valor inicial 80) define el puerto de meta para la comunicación HTTP de la aplicación **2N® IP Eye** con el intercomunicador.

Nota

- *La función "Dirección de IP Eye" está disponible solo en los modelos determinados de los **intercomunicadores 2N IP** (ver el capítulo Resumen de modelos y licencias).*
- *En el caso de que en el dispositivo se encuentren funciones sin licencia Enhanced Integration, es posible controlar las cerraduras solo durante la llamada en curso. En el caso de que esté en curso una llamada con el usuario en el que esté introducida la dirección **2N® IP Eye**, no se necesitará ninguna licencia para abrir la cerradura.*

Consejo

- FAQ: 2N® IP Eye – Como configurarlo con los intercomunicadores 2N IP

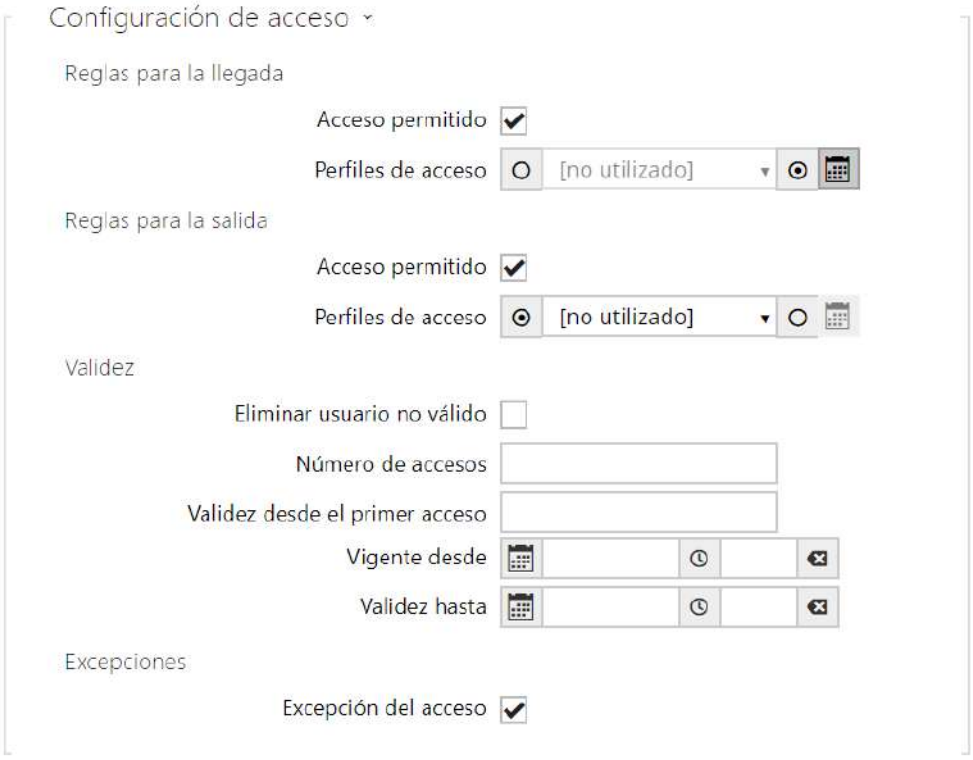
Consejo

- Tutorial en vídeo: SW application for IP intercoms – 2N® IP Eye

- **Llamar dentro del grupo con el siguiente número** – permite configurar la función de llamada colectiva, es decir, llamar a varios números de teléfono a la vez. Se puede llamar a los dos primeros números, los últimos dos números, eventualmente a los tres números del usuario a la vez. Tras aceptar una de las llamadas se cancelarán automáticamente las demás llamadas.
- **Llamar dentro del grupo con el suplente** – permite configurar la función de llamada colectiva – es decir, llamar a varios números de teléfono a la vez. Se puede llamar a los dos primeros números, los últimos dos números, eventualmente a los tres números del usuario a la vez. Tras aceptar una de las llamadas se cancelarán automáticamente las demás llamadas. La cantidad total máxima de los números llamados al mismo tiempo es 16, lo cual puede suceder al utilizar a la vez la llamada de grupo y al configurar varios números llamados en un botón de marcado rápido.
- **Suplente en el caso de indisponibilidad** – permite seleccionar un usuario al que se dirigirá la conexión en el caso de que el usuario determinado no esté disponible. Introduzca el nombre o elija al usuario con la ayuda del botón Buscar. La cantidad total máxima de los números llamados al mismo tiempo es 16, lo cual puede suceder al utilizar a la vez la llamada de grupo y al configurar varios números llamados en un botón de marcado rápido.

Nota

- *La función "Suplente en el caso de indisponibilidad" está disponible solo en los modelos determinados de los **intercomunicadores 2N IP** (ver el capítulo Resumen de modelos y licencias).*



- **Reglas para la llegada**
  - **Acceso permitido** – permite la autenticación en este punto de acceso.
  - **Perfiles de acceso** – ofrecen la elección entre los perfiles pre-definidos del Directorio / Perfiles de tiempo o configuración manual del perfil de tiempo directamente para este elemento.
- **Reglas para la salida**
  - **Acceso permitido** – permite la autenticación en este punto de acceso.
  - **Perfiles de acceso** – ofrecen la elección entre los perfiles pre-definidos del Directorio / Perfiles de tiempo o configuración manual del perfil de tiempo directamente para este elemento.
- **Validez**
  - **Eliminar usuario no válido** – seleccione si el usuario se elimina del dispositivo una vez que es inválido (es decir, ha pasado su período de validez o el número de sus accesos autorizados es 0).
  - **Número de accesos** – establezca el número de accesos autorizados para este usuario. Deje vacío para establecer un número indefinido de accesos.
  - **Validez desde el primer acceso** – establezca el tiempo durante el cual el usuario estará válido desde su primera autorización exitosa. Deje vacío para ningún período de validez relativa. La validez relativa puede acortar el período de validez pero nunca extenderlo. El tiempo se establece en el formato HH:MM, por ejemplo, 06:09.
  - **Vigente desde** – permite configurar el comienzo de vigencia del acceso configurado. Deje vacío para que el inicio no esté restringido. El Valido desde debe preceder al Valido hasta.

  - **Vigente hasta** – permite configurar el final de vigencia del acceso configurado. Deje vacío para que el fin no esté restringido. El Valido hasta debe ser posterior al Valido desde.
- **Excepción del acceso** – habilitar a este usuario para eludir las reglas de bloqueo de acceso y anti-retorno.

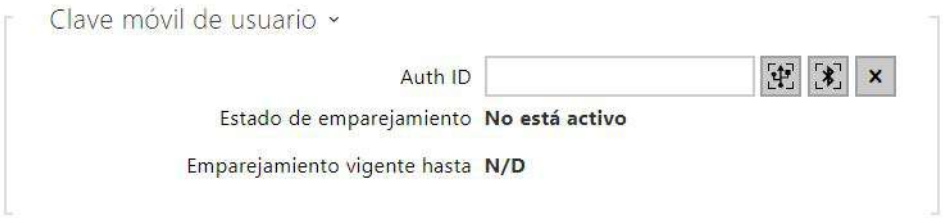
Cada usuario puede tener asignado su propio código QR / numérico privado para la activación del interruptor. Los códigos de usuario de los usuarios se pueden combinar libremente con los códigos universales de los interruptores introducidos en el menú **Hardware / Interruptores**. En el caso de que los códigos se solapen con otros códigos introducidos previamente en la configuración del intercomunicador, junto a estos códigos que colisionan aparece la marca .

- **Código PIN** – permite configurar el código numérico personal de acceso del usuario. El código debe contener al menos dos caracteres.
  - – generará la imagen del código QR. Por motivos de seguridad no es posible introducir códigos que contienen menos de 10 dígitos mediante la lectura del código QR. Los códigos deben contener solo dígitos. En el caso de que se necesite la autenticación mediante el código QR hexadecimal, habrá que convertir este código al formato hexadecimal antes de introducirlo.
- **Interruptor 1–4** – permite configurar el código privado del usuario para activar el interruptor. El código puede tener longitud de hasta 16 caracteres y puede contener solo dígitos 0–9. El código debe contener al menos dos caracteres para desbloquear la puerta desde el teclado del intercomunicador, y como mínimo un carácter para desbloquear la puerta con la ayuda de DTMF desde el teléfono.
  - – generará la imagen del código QR. Por motivos de seguridad no es posible introducir códigos que contienen menos de 10 dígitos mediante la lectura del código QR. Los códigos deben contener solo dígitos. En el caso de que se necesite la

autenticación mediante el código QR hexadecimal, habrá que convertir este código al formato hexadecimal antes de introducirlo.

Cada usuario del intercomunicador puede tener asignadas dos tarjetas RFID de acceso.

- **ID de tarjeta RFID** – permite configurar el ID de la tarjeta de acceso del usuario. Cada usuario puede tener asignadas como máximo dos tarjetas de acceso. El ID de la tarjeta de acceso es una secuencia de 6–32 caracteres del grupo de 0–9, A–F. Tras acercar una tarjeta válida al lector se activa el interruptor asociado al lector de tarjetas correspondiente. En el caso de que esté seleccionado el modo de la autenticación doble, se activa el interruptor determinado por el código numérico tras acercar la tarjeta.
- **Tarjetas ID virtuales** – permite configurar el ID de la tarjeta virtual de acceso del usuario. Cada usuario puede tener asignada solo una tarjeta virtual. El ID de la tarjeta virtual es una secuencia de 6–32 caracteres del grupo de 0–9, A–F. El número de la tarjeta virtual se utilizará para identificar al usuario en los dispositivos conectados a través de la interfaz Wiegand. Tras la identificación del usuario se envía el ID de la tarjeta virtual en Bluetooth o en el lector biométrico a la interfaz Wiegand en el caso de que en la configuración (Puerta / Reglas para la llegada / Configuración avanzada) esté configurado el envío de los identificadores a Wiegand.



- **Auth ID** – identificador inconfundible del dispositivo móvil (resp. de su usuario). El valor del parámetro se genera automáticamente durante el emparejamiento. Auth ID se puede desplazar a otro usuario, eventualmente es posible copiarlo en otro dispositivo dentro de la misma localización.
- **Estado de emparejamiento** – estado actual del emparejamiento (Inactivo, Esperando el emparejamiento, Validez del PIN caducada o Emparejado).

- **Emparejamiento vigente hasta** – fecha y hora del final de vigencia del PIN de autorización generado PIN.
  - emparejar mediante lector USB
  - emparejar mediante este dispositivo
  - borrar Auth ID

Emparejamiento mediante módulo Bluetooth en el intercomunicador

El procedimiento para el emparejamiento del teléfono móvil con el usuarios es el siguiente:

1. En la cuenta de usuario elegida iniciamos el emparejamiento pulsando el botón junto al elemento Auth ID.
2. Aparecerá la ventana de diálogo con el código PIN.
3. En la aplicación **2N® Mobile Key** encontraremos el lector correspondiente y pulsamos el botón Start pairing.
4. En el campo para la entrada introducimos el código del punto 2.
5. El emparejamiento ha finalizado.

El manual detallado, sobre la manera de proceder, Información detallada sobre la configuración del servicio **2N® Mobile Key** la encontrará en el capítulo 5.4.5 Mobile Key.

- **Huella dactilar** – muestra el número de las huellas dactilares configuradas, se pueden configurar hasta 2 huellas dactilares diferentes. Esta sección aparece solo en el caso de presencia del módulo del lector biométrico.
  - lectura del dedo mediante el lector USB
  - realizar la lectura mediante el módulo del lector de huellas dactilares

Aviso

- La capacidad de las huellas dactilares de usuario cargadas está limitada a un máximo de 2000 para un dispositivo.

El manual detallado, sobre como cargar las huellas dactilares del usuario, está descrito en el sub-capítulo 5.2.1.1 Instrucciones para la configuración de las huellas dactilares de usuario.

El intercomunicador 2N IP permite utilizar las matrículas reconocidas de vehículos enviadas en el requerimiento HTTP mediante las cámaras de la empresa AXIS equipadas con la aplicación adicional VaxALPR a api/lpr/licenseplate (para más información ver Manual HTTP API para los intercomunicadores IP).
En el caso de que la función esté encendida, tras recibir el requerimiento HTTP válido se producirá el registro del suceso en el historial bajo el suceso LicensePlateRecognized.

En el caso de que dentro del marco del requerimiento HTTP se envíe también una imagen (por ej. recorte de una fotografía o fotografía entera de la escena a la hora de detectar la matrícula), ésta se guardará. En la memoria del dispositivo están guardadas las últimas cinco fotografías que se pueden leer en el dispositivo mediante el requerimiento HTTP enviado a api/lpr/image y las cuales están disponibles en el sistema **2N® Access Commander**.

Para la función correcta es recomendable que cada matrícula esté asignada a un registro en el directorio. En el caso de matrículas introducidas de forma múltiple sucede la situación que no se puede asignar de forma inequívoca un registro en el directorio que tenga configurada la matrícula (se selecciona el primer registro que tiene configurada la matrícula correspondiente y se aplicarán sus reglas de acceso).

- **Matrículas** – configura las matrículas de los vehículos del registro determinado en el directorio. Al registro se puedes asignar varias matrículas separadas por una coma (máximo 20). Las matrículas introducidas se utilizan en la función de reconocimiento de matrículas en la imagen de la cámara externa (para más información vea el manual de Interoperability). Una matrícula puede contener 10 caracteres como máximo. La longitud de la cadena determinada está limitada a 255 caracteres.

- **Plantas** – elección de plantas accesibles para el usuario.
- **Perfil de tiempo** – ofrece la elección de uno o varios perfiles de tiempo a la vez que se aplicarán. La propia configuración de los perfiles de tiempo se puede realizar en la sección Directorio / Perfiles de tiempo.
  - ⊙ con la marca se configura la elección de los perfiles pre-definidos o la configuración manual del perfil de tiempo para el elemento determinado.

-  con la marca se configura el perfil de tiempo directamente para el elemento determinado.

5.2.1.1 Ajustes de conexión de llamada

Para poder realizar llamadas con otros dispositivos terminales en las redes IP hay que asignar el dispositivo al contacto en el Directorio.

Conexión con dispositivos 2N en la red local

1. Asegúrese de que en ambos dispositivos 2N está habilitada la función Llamadas locales.
2. Haga clic en el botón **Buscar dispositivo** encima de la tabla. En la lista marque los dispositivo con los cuales quiere establecer la conexión. Una vez añadido el dispositivo se abrirá el editor del usuario añadido recientemente.
3. En el editor puede modificar la información básica sobre el usuario o gestionar las opciones de su acceso. En el caso de que marque las llamadas mediante el teclado numérico configure un número virtual para el usuario.
4. Tras el guardado el contacto aparecerá en la lista telefónica en la pantalla del dispositivo. En el caso de que marque las llamadas mediante el botón en el dispositivo deberá asignar al usuario al botón de selección rápida en Hardware > Botones, ver 5.3.5 Tlačítka.
5. Para poder realizar la llamada con éxito en el dispositivo 2N al que está llamando debe estar habilitado el servicio Llamadas locales.

Conexión con otros dispositivos

1. Cree un nuevo contacto haciendo clic en el botón **Agregar usuario** encima de la tabla o abra el detalle del contacto existente.
2. Al hacer clic en el icono de lápiz  junto al parámetro Número de teléfono abrirá el editor del número de teléfono.
3. En el editor elija el tipo de llamada:
   - *SIP* para llamada realizada a través de SIP,
   - *rava* para llamadas con el dispositivo Creston,
   - *vms* para llamadas con Axis Camera Station,
   - *device* pata llamadas con dispositivo 2N local.

- En el campo de destino introduzca la dirección del destino de llamada a la cual debe dirigirse la llamada.
  Rellene SIP URI en el formato *nombre_de usuario@anfitrión* o la dirección IP de destino (por ej.: *johana@255.0.255.0* o *johana@calls.2N.com*). En el caso de llamadas ocales rellene ID del dispositivo 2N llamado, ver Llamadas locales en 5.4.1 Teléfono.
- En el editor puede modificar la información básica sobre el usuario o gestionar las opciones de su acceso. En el caso de que marque las llamadas mediante el teclado numérico configure un número virtual para el usuario.

- Tras el guardado el contacto aparecerá en la lista telefónica en la pantalla del dispositivo. En el caso de que marque las llamadas mediante el botón en el dispositivo deberá asignar al usuario al botón de selección rápida en Hardware > Botones, ver 5.3.5 Botones.
- Para poder realizar la llamada con éxito en el dispositivo al que está llamando debe estar habilitado el servicio que proporciona la transmisión de llamada.

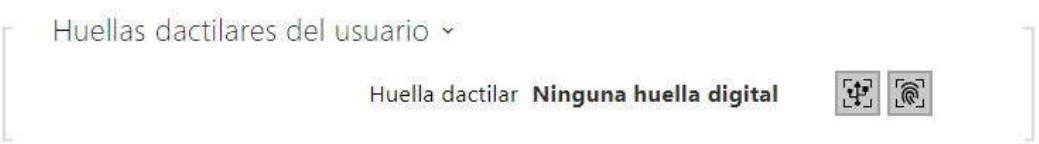
Consejo

- A cada usuario se pueden asignar hasta 3 números de teléfono. En el caso de que el usuario no responda en el primer número de teléfono, la llamada se desviará al siguiente número. De forma alternativa se puede configurar la llamada a varios números de teléfono a la vez. La llamada a varios números de teléfono del mismo usuario a la vez se configura marcando la casilla *Lamar en el grupo* entre los números de teléfono determinados.
- En el caso de que ninguno de los números de teléfono del usuario esté disponible es posible configurar el desvío de la llamada al Suplente.
- Los usuarios se pueden agrupar en grupos de llamada. El nombre del grupo de llamada aparecerá en la lista telefónica en la pantalla del dispositivo. El grupo de llamada se puede asignar al botón de la selección rápida. En el caso de que la llamada saliente de grupo deba cancelarse con el primer rechazo de alguno de los usuarios llamados, habrá que configurar está función en Servicios > Teléfono > Llamadas, ver 5.4.1 Teléfono.

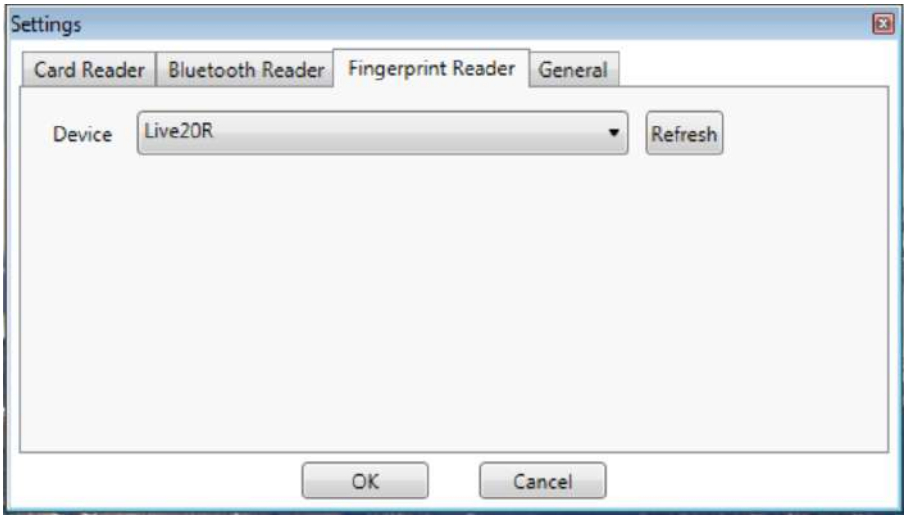
5.2.1.2 Instrucciones para la configuración de las huellas dactilares de usuario

Las huellas dactilares se pueden cargar mediante el lector de huellas dactilares **2N® IP Verso** (No de referencia 9155045) o lector de huellas dactilares USB (No de referencia 9137423E). El procedimiento es el siguiente:

1a) La lectura mediante el módulo del lector de huellas dactilares **2N® IP Verso** se puede realizar mediante la interfaz de web del dispositivo en el usuario concreto en la sección Directorio / Usuarios / Huellas dactilares de usuario al seleccionar Realizar la lectura mediante el módulo del lector de huellas dactilares  .



1b) La lectura mediante el lector de huellas dactilares USB externo se puede realizar mediante el **2N® IP USB Driver**, en su configuración seleccione Fingerprint Reader (lector de huellas dactilares) y confirme con el botón OK. En la interfaz de web del dispositivo en el usuarios concreto en la sección Directorio / Usuarios / Huellas dactilares de usuario, seleccione Realizar la lectura mediante el módulo del lector de huellas dactilares .



2) Haciendo clic elija el dedo para cargar la huella.

Para un usuario se pueden configurar hasta dos huellas dactilares.

3) Para cargar la huella dactilar pulse el botón ESCANEAR EL DEDO.

4) Acerque el dedo elegido en el lector USB externo. Para una mayor precisión este proceso se repite, tres veces en total.

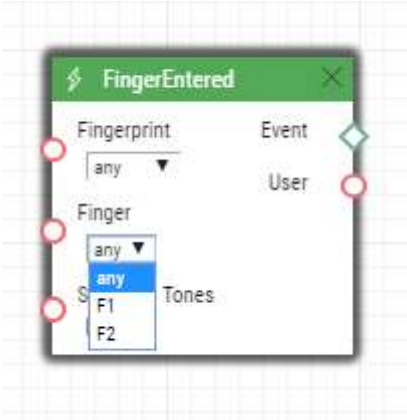
En el caso de que la lecturas de las huellas dactilares no coincida, repita el proceso.

5) En el caso de que el escaneo de los dedos haya transcurrido satisfactoriamente, confirme la configuración haciendo clic en el botón HECHO.

Para configurar la función del dedo, haga clic en el icono del menú , aparecerá el menú de las funciones disponibles:

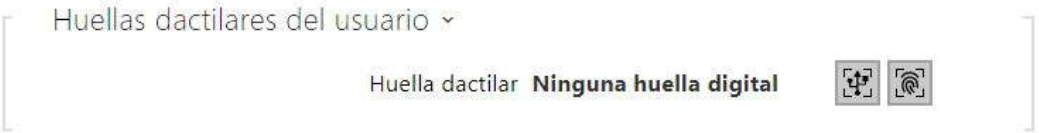
- Abrir la puerta
- Alarma silenciosa. Se puede configurar solo en el caso de que la función Apertura de la puerta esté activa.
- Automatización F1 – genera el suceso FingerEntered en Automation. F1 sirve para distinguir el dedo acercado en Automation.

- Automatización F2 – genera el suceso FingerEntered en Automation. F2 sirve para distinguir el dedo acercado en Automation.



Tras configurar las huellas dactilares y sus funciones confirme el proceso haciendo clic en el botón GUERDAR Y CERRAR.

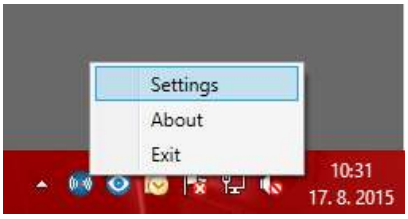
6) En la solapa Usuarios es posible comprobar el estado actual de la configuración.



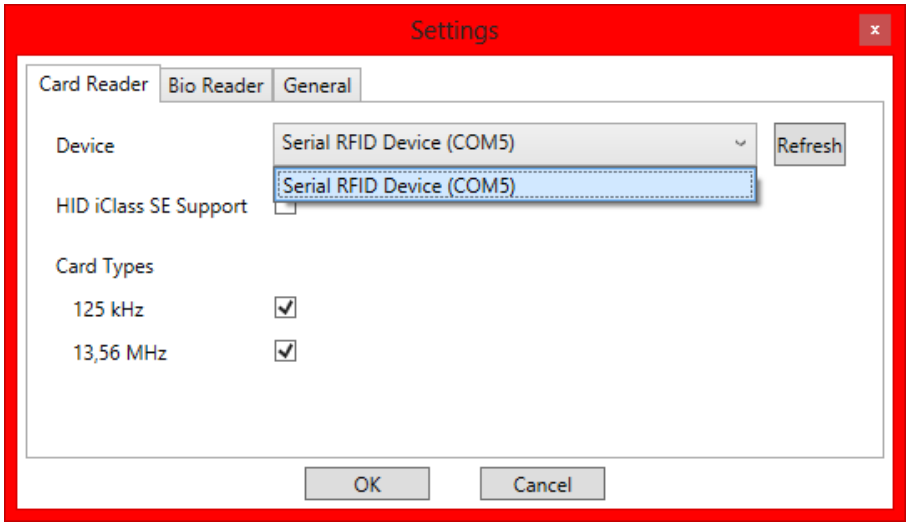
5.2.1.3 Lector de tarjetas USB RFID

La lectura de las tarjetas ID se puede realizar mediante el lector USB RFID. El procedimiento es el siguiente:

1. Vaya a la configuración **2N IP USB Driver**

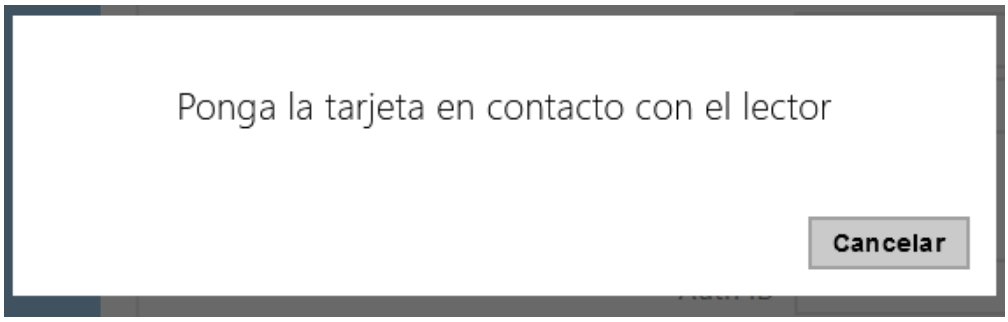


2. Configure el puerto COM del lector conectado



3. En la web del intercomunicador **2N IP** pulse junto al usuario el botón de la lectura de tarjeta

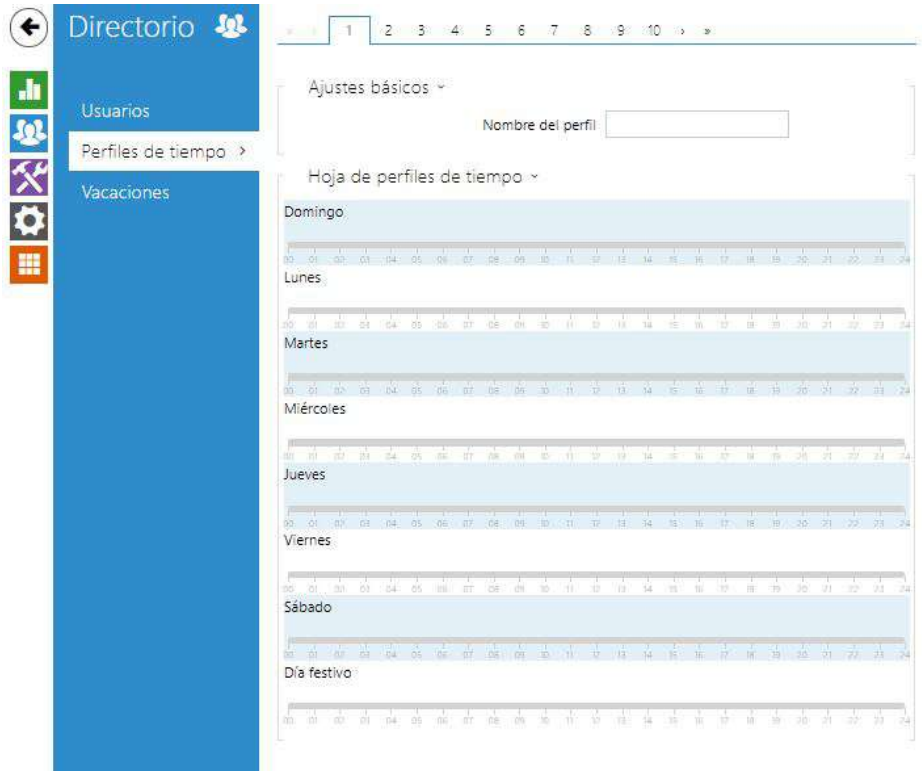
4. Acerque la tarjeta al lector



5. La tarjeta ha sido leída

6. No olvide guardar la configuración.

5.2.2 Perfiles de tiempo



En determinadas funciones del intercomunicador, como por ej. llamada saliente, acceso mediante la tarjeta RFID o código numérico, se puede limitar el tiempo. A las funciones mencionadas de puede asignar el llamado **perfil de tiempo**, que determina cuando la función

está disponible y cuando no. Mediante los perfiles de tiempo se pueden resolver los siguientes requisitos:

- bloquear totalmente las llamadas al usuario determinado fuera del tiempo restringido
- bloquear totalmente las llamadas a los números de teléfono determinados fuera del tiempo restringido
- bloquear el acceso mediante la tarjeta RFID del usuario fuera del tiempo restringido
- bloquear el acceso mediante el código numérico determinado fuera del tiempo restringido
- bloquear la activación del interruptor fuera del tiempo restringido

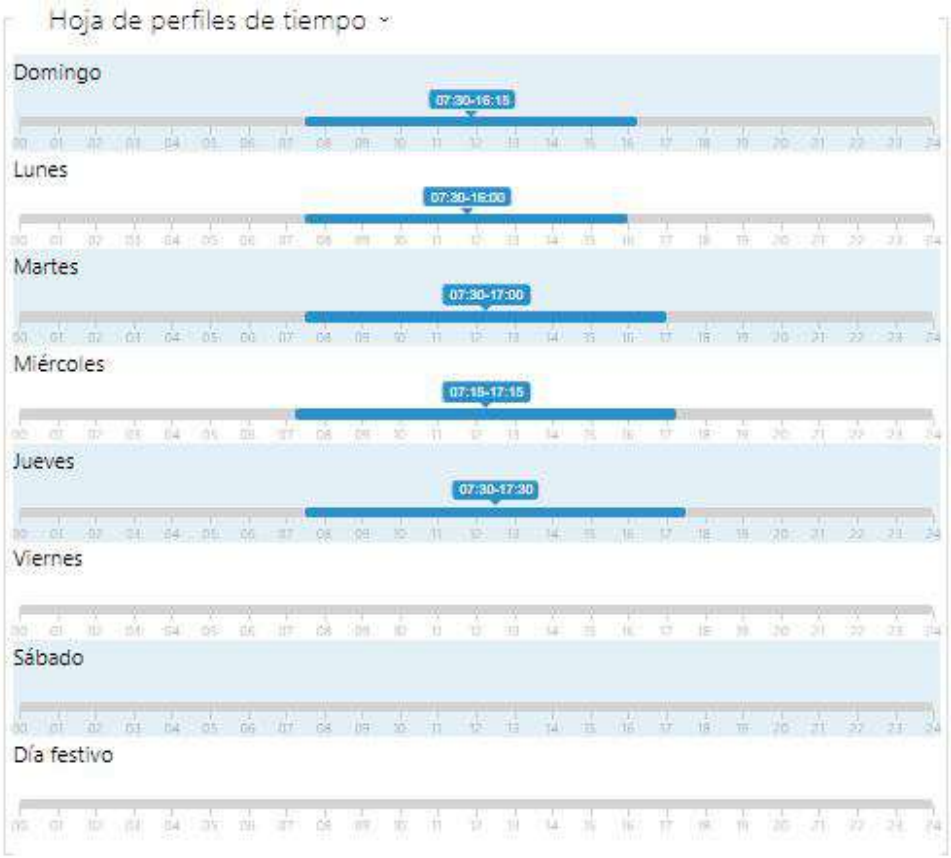
Cada perfil de tiempo define la disponibilidad de la función son la cual está vinculado mediante el calendario semanal. Se puede configurar fácilmente el tiempo desde-hasta y eventualmente los días de la semana cuando la función debe estar disponible. Los **intercomunicadores 2N IP** permiten crear hasta 20 perfiles de tiempo diferentes (en cada uno de los modelos IP puede variar el número de perfiles. A la función determinada podrá asignar cualquier perfil de tiempo creado, ver la configuración Usuarios, Tarjetas de acceso, Interruptores.

La vigencia del perfil de tiempo puede controlar no solo mediante la configuración del calendario semanal, sino también mediante los códigos especiales de activación y desactivación asignados al perfil determinado. Los códigos de activación y desactivación se pueden introducir en cualquier momento mediante el teclado numérico del intercomunicador o mediante su teléfono (durante la llamada con el intercomunicador). De esta manera se puede activar, eventualmente desactivar manualmente algunas de las funciones, por ej. a la hora de llegar o salir del edificio.

La configuración de los perfiles de tiempo se encuentra en el menú **Directorio** → **Perfiles de tiempo**.

Lista de parámetros

- **Nombre del perfil** – el nombre del perfil elegido por usted. Este parámetro es opcional y sirve solo para la orientación más sencilla en la lista de perfiles y para elegir más fácilmente el perfil en las configuraciones de los interruptores, tarjetas y números de teléfono.



Sirve para configurar el tiempo del perfil activo dentro del período semanal. El perfil está activo en el caso de que la hora actual esté dentro de los intervalos configurados.

En el caso de que el día determinado esté señalado como festivo (ver la configuración **Directorio** → **Festivos**), sin tener en cuenta en que día de la semana estamos, se aplicará la última línea de la tabla marcada como Festivo.

Para el uso correcto de esta función es imprescindible que en el dispositivo esté configurado correctamente la hora actual (ver el capítulo Fecha y hora).

Nota

- *Dentro del marco de un día se puede configurar cualquier número de intervalos, por ej. 8:00–12:00, 13:00–17:00, 18:00–20:00.*
- *En el caso de que quiera que el perfil esté activo doto el día, introduzca un intervalo que cubra todo el día, es decir, 00:00–24:00.*

5.2.3 Festivos

En esta página se configuran los días en los que cae el festivo (eventualmente el día de descanso laboral). Para los días en los que cae un festivo se pueden configurar en el perfil de tiempo intervalos de tiempo diferentes a los perfiles establecidos para los demás días.
Los festivos se pueden configurar hasta para 10 años de antelación (el año se puede elegir haciendo clic sobre el número del año en la parte superior de la página. En la página se muestra el calendario para todo el año. Al hacer clic sobre el día en el calendario se marcará o se desmarcará el festivo. Los festivos periódicos (que se repiten cada año en el mismo día de calendario) están marcados con el color verde. Los festivos irregulares (caen en un día concreto de calendario solo en el año determinado) están marcados con el color azul. El primer clic marcará el día como el día de festividad laboral, el siguiente clic marcará el día como el festivo irregular y otro clic eliminará el día de la lista de los festivos.

5.3 Llamada

La llamada es la función básica del intercomunicador – permite establecer conexión con otros dispositivos terminales en las redes IP. Los **intercomunicadores 2N IP** soportan el protocolo ampliado SIP y son compatibles con los fabricantes de renombre de las centralitas SIP y dispositivos terminales certificados por ellos – CISCO, Avaya, Broadsoft etc.

El intercomunicador soporta hasta cinco llamadas en curso a la vez – 1 saliente y hasta 4 entrantes. Solo una de las llamadas en curso puede ser **activa** – el stream de audio está conectado con el micrófono y el reproductor y con el stream de vídeo con la cámara. Las demás llamadas están siempre **inactivas** – el micrófono y el reproductor tienen el volumen bajado y el intercomunicador recibe solo los signos DTMF mediante los cuales puede la otra parte controlar el intercomunicador – activar/desactivar perfiles, usuarios etc.

Los intercomunicadores se utilizan normalmente sobre todo para las llamadas salientes y las llamadas entrantes están siempre inactivas – el micrófono y el reproductor tienen el volumen bajado. Sin embargo, puede configurarlos de manera que las llamadas entrantes estén activas y se señalicen con el timbre, ver el capítulo 5.3.1 Obecné nastavení. Aceptar y finalizar la llamada se puede mediante las teclas * y # en la pantalla numérica.

Los **intercomunicadores 2N IP** utilizan para la codificación (event. compresión) del stream de audio los protocolos **G.711**, **L16**, **G.722** y **G.729**. Los códec de banda ancha L16 y G.722 están disponibles solo en los **intercomunicadores 2N IP** determinados. Para la compresión del stream de vídeo se utilizan los códec **H.263** o **H.264**. Mediante la configuración en la solapa Audio, event. Vídeo, podrá elegir sus preferencias de códec.

Explicación de los términos de la telefonía IP

- **SIP (Session Initiation Protocol)** – protocolo para la transmisión de la señalización de las llamadas telefónicas utilizado en la telefonía IP. Este protocolo sirve en principio para establecer, finalizar y desviar la conexión entre dos dispositivos SIP (en este caso entre el intercomunicador y otro teléfono IP). Los dispositivos SIP pueden establecer la conexión directamente entre sí (Direct SIP Call – llamada directa), sin embargo normalmente suelen utilizar para este fin uno o varios servidores – SIP Proxy y SIP Registrar.
- **SIP Proxy** – servidor en la red IP responsable de direccionar las llamadas (traspaso de llamadas a otra entidad que está más cerca al destino). En la ruta entre los participantes puede haber una o varias SIP Proxy.
- **SIP Registrar** – servidor en la red IP responsable de registrar los participantes en una parte determinada de la red. El registro del dispositivo SIP en general una condición indispensable para que el participante esté disponible para los demás en un número de teléfono determinado. SIP Registrar y SIP Proxy suelen estar muy a menudo instalados en el mismo servidor.
- **RTP (Real-Time Transport Protocol)** – protocolo que define el formato estándar de los paquetes para la transmisión de audio y vídeo en las redes IP. Los intercomunicadores **2N IP** utilizan este protocolo para transmitir el stream de audio y vídeo durante la llamada.

Los parámetros (números de los puertos, protocolos y códec) de los stream están definidos y convenidos mediante el protocolo SDP (Session Description Protocol).

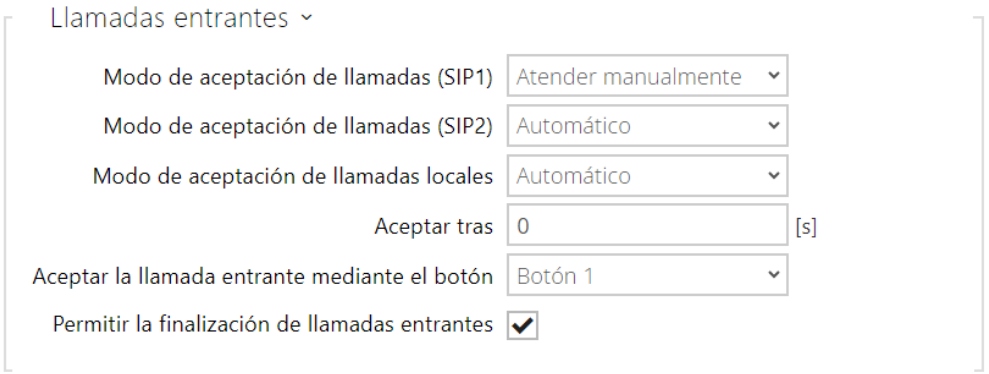
Los intercomunicadores **2N IP** soportan tres formas de señalización SIP:

- mediante el protocolo **UDP**, la cual es la forma más común no asegurada de la señalización
- mediante el protocolo **TCP** , la cual es la forma menos extendida, sin embargo recomendada de la señalización no asegurada
- mediante el protocolo **TLS** , cuando los mensajes SIP están asegurados contra las escuchas y modificaciones por terceros (no vale para los modelos **2N® IP Base**, **Uni**)

Aquí se expone el resumen de lo que encontrará en este capítulo:

5.3.1 Configuración general

- **Tiempo límite de llamada** – configura la duración máxima de llamada tras la cual la llamada finalizará automáticamente. El intercomunicador señaliza que se aproxima el final de la llamada mediante un pitido durante la llamada 10 segundos antes de que esta finalice. La llamada se puede prolongar enviando cualquier carácter DTMF a la llamada (por ej. pulsando la tecla # en el teléfono IP). En el caso de que el tiempo máximo de llamada esté configurado a 0 y no se utilice SRTP, el tiempo de llamada no está limitado.



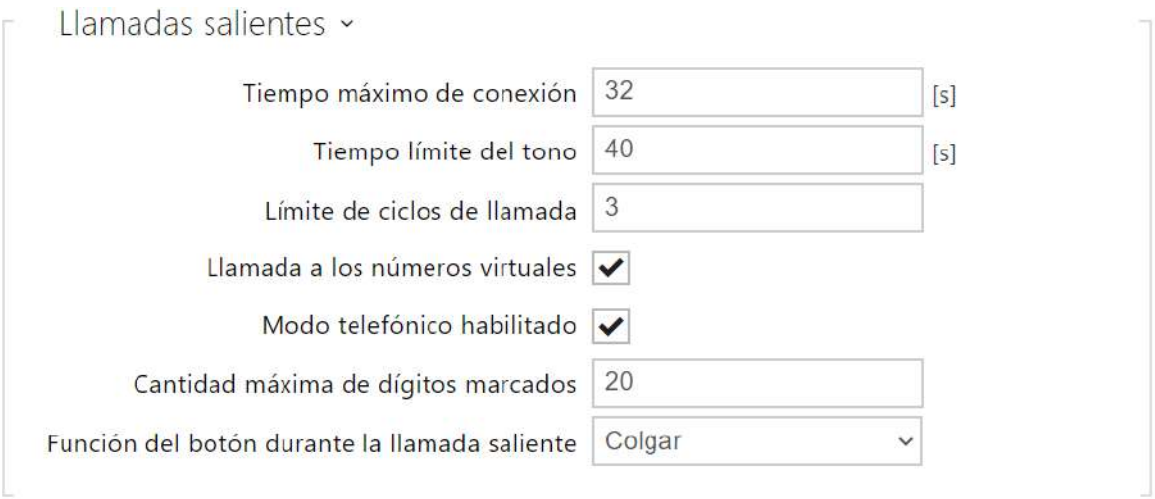
- **Modo de aceptación de llamadas (SIP1, SIP2)** – configura el modo del que el intercomunicador aceptará las llamadas entrantes. Se puede elegir entre tres opciones:

    - **Siempre ocupado** – el intercomunicador rechaza las llamadas entrantes
    - **Aceptación manual** – el intercomunicador señaliza las llamadas entrantes mediante el timbre y el usuario las puede aceptar mediante el botón en el teclado numérico
    - **Automática** – el intercomunicador acepta automáticamente la llamada entrante. El modo de aceptación de llamadas se puede configurar para cada cuenta SIP de forma independiente.
    - **Automática (solo DTMF)** – el intercomunicador acepta automáticamente la llamada entrante solo en el caso de recibir DTMF sin la conexión de micrófono y reproductor.
    - **Automático (oculto)** – el intercomunicador aceptará la llamada entrante de forma automática, sin que se muestre la identidad de la persona que llama o sin ningún signo acompañante sobre la aceptación de la llamada.
- **Modo de aceptación de llamadas locales** – configura el modo del que el intercomunicador aceptará las llamadas entrantes locales. Se puede elegir entre tres opciones:
    - **Siempre ocupado** – el intercomunicador rechaza las llamadas entrantes
    - **Aceptación manual** – el intercomunicador señaliza las llamadas entrantes mediante el timbre y el usuario las puede aceptar mediante el botón en el teclado numérico
    - **Automática** – el intercomunicador acepta automáticamente la llamada entrante. El modo de aceptación de llamadas se puede configurar para cada cuenta SIP de forma independiente.
    - **Automático (oculto)** – el intercomunicador aceptará la llamada entrante de forma automática, sin que se muestre la identidad de la persona que llama o sin ningún signo acompañante sobre la aceptación de la llamada.
- **Aceptar tras** – tiempo después del cual se acepta automáticamente la llamada en el modo de la aceptación automática de llamadas. En el caso de que en los dispositivos compatibles con el buzón de voz esté habilitado uno de los **modos del buzón de voz**, la llamada será aceptada después de este tiempo y se reproducirá el anuncio elegido en al modo automático o manual de aceptación de llamadas. En el caso de que este valor sea 0, el anuncio se reproducirá inmediatamente. Común para todas las cuentas SIP.
- **Aceptar la llamada entrante con el botón** – permite aceptar la llamada entrante mediante el botón elegido de marcado rápido. Al configurar 'Ninguno' la función queda apagada.

Aviso

- La función Aceptar la llamada entrante mediante el botón no se muestra para los modelos **2N® IP Force** y **2N® IP Vario** con teclado. En estos modelos es posible aceptar la llamada entrante mediante el botón marcado con un auricular verde en el teclado sin necesidad de configuración previa.

- **Permitir la finalización de llamadas entrantes** – permite a los usuarios rechazar o finalizar la llamada mediante el intercomunicador. Cuando la función está apagada el botón del auricular para rechazar o finalizar la llamada no funciona y en la pantalla no aparece el icono para rechazar o finalizar la llamada. La llamada se puede entonces interrumpir iniciando una nueva llamada saliente desde el intercomunicador.



- **Tiempo máximo de conexión** – define el tiempo máximo de conexión en las llamadas salientes, tras el cual estas se cancelarán automáticamente. Si las llamadas se envían a la red GSM mediante los portales GSM, es conveniente configurar el valor al tiempo superior a 20 segundos.
- **Tiempo máximo del sonido del timbre** – configura el tiempo máximo de establecimiento y sonido de tono tras el cual finalizarán automáticamente las llamadas salientes. En el caso de que las llamadas se dirijan a la red GSM mediante portales GSM, es recomendable configurar el valor al tiempo superior a 20 s. Valor mínimo 1 s, valor máximo 600 s. Para apagar el parámetro de tiempo configure el valor 0.
- **Número máximo de ciclos del marcado** – configura el número máximo de ciclos del marcado del suplente en el caso de indisponibilidad del usuario en la lista telefónica. Esta función evita el interbloqueo en caso de que el parámetro Suplente en el caso de indisponibilidad en la lista telefónica esté configurado al mismo usuario. Las opciones de la configuración de los límites de los ciclos de llamada están expuestas en el sub-capítulo 5.4.1.1 Limit volacích cyklů.
- **Finalizar las llamadas en grupo en el caso del primer rechazo** – permite al dispositivo finalizar todas las llamadas en la llamada saliente en grupo en el caso de que alguna de las destinaciones llamadas rechace la llamada."
- **Llamada a los números virtuales** – permite llamadas a los números virtuales configurados de usuarios.
- **Modo de llamada a la planta y piso** – habilita el modo espacial de llamada a la planta y piso. En este modo se introduce en el teclado numérico el número virtual del usuario asignado. Esta función está disponible solo en el modelo **2N® IP Vario**. El código de la

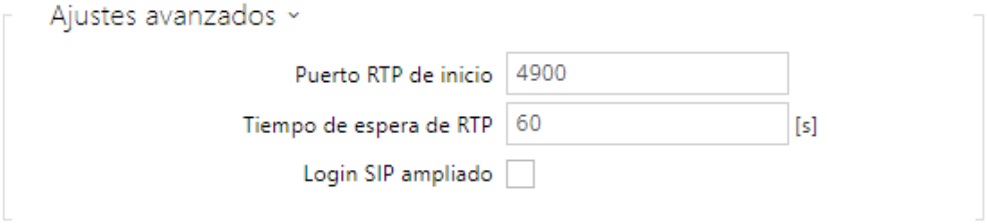
planta y piso se introduce en el campo Número virtual del usuario. Puede contener números y letras dentro del rango de A–F.

- **Habilitación del modo teléfono** – habilita la opción de establecer llamadas directamente a los números de teléfono introducidos desde el teclado numérico del intercomunicador. Introduzca el número de teléfono para establecer la llamada.

Inclinar

- Es posible establecer la llamada al número de teléfono en **2N® IP Force** y **2N® IP Vario** mediante la sucesión de teclas **número_de teléfono** , en **2N® IP Verso** **número_de teléfono** y en **2N® IP Verso** con pantalla **número_de teléfono** y pulsando el icono **Llamar**. En el caso de que no se utilice el símbolo de finalización (tecla en el caso del teclado en **2N® IP Verso**), la elección se confirma automáticamente tras agotarse el límite de tiempo para la introducción del código, como si se pulsase la tecla (tecla en el caso del teclado en **2N® IP Verso**).

- **Longitud máxima del número** – configura el número máximo de dígitos del número de teléfono en el modo teléfono. Al alcanzarse dicho máximo, el número de teléfono se marca automáticamente sin pulsar la tecla de asterisco (*).
- **Función del botón durante la llamada saliente** – configura la función del botón de marcado rápido durante la llamada saliente. La configuración afecta solo al botón con el que se inició la llamada.



- **Puerto RTP de inicio** – configura el puerto local RTP inicial en el rango de longitud de 64 puertos utilizados para las transferencias de audio y vídeo. El valor predeterminado es 4900 (es decir, el rango empleado es de 4900-4963). El parámetro es común para ambas cuentas SIP y se configura solo en la cuenta 1.
- **RTP Timeout** – configura el límite de tiempo para la recepción de paquetes RTP del stream de audio durante una llamada. Si se supera este límite (los paquetes RTP no se entregan), la llamada será finalizada por el intercomunicador. Este control se puede apagar configurando el parámetro al valor 0. El parámetro es común para ambas cuentas SIP y se configura solo en la cuenta 1.
- **Login SIP ampliado** – habilita el registro de la información más detallada relacionada con SIP de telefonía en el syslog (sirve solo para la solución de problemas).

5.3.1.1 Límite de ciclos de llamada

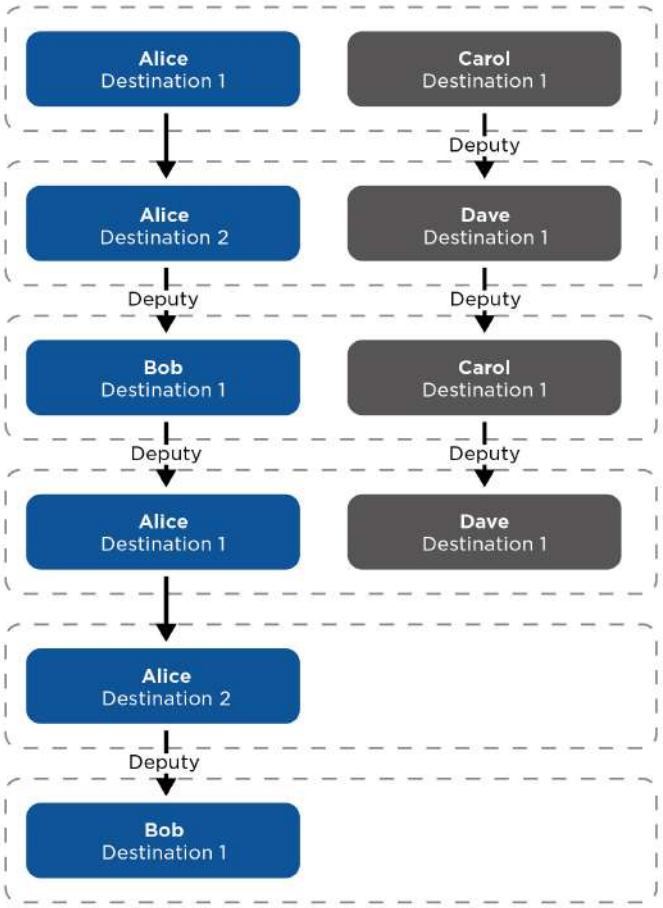
Con este parámetro se establece el número máximo de llamadas generadas consecutivamente a la estación de llamada (destinación) en el caso de que esté establecido el ciclo de llamada de los suplentes en el caso de indisponibilidad (el ejemplo más simple del ciclo de llamada es cuando el usuario configura a sí mismo como suplente, otro ejemplo son dos usuarios configurados como suplentes mutuos).

Ejemplo 1

El algoritmo primero soluciona las ramas del esquema de forma independiente entre sí. En el ejemplo expuesto a continuación están los usuarios Alice y Carol configurados bajo un botón (al pulsar el botón se generan dos llamadas paralelas a la vez). El límite del ciclo de llamada está establecido a 2. Alice tiene dos números de teléfono (estaciones de llamada), los demás usuarios tienen solo una estación de llamada. Los suplentes están configurados de la siguiente manera:

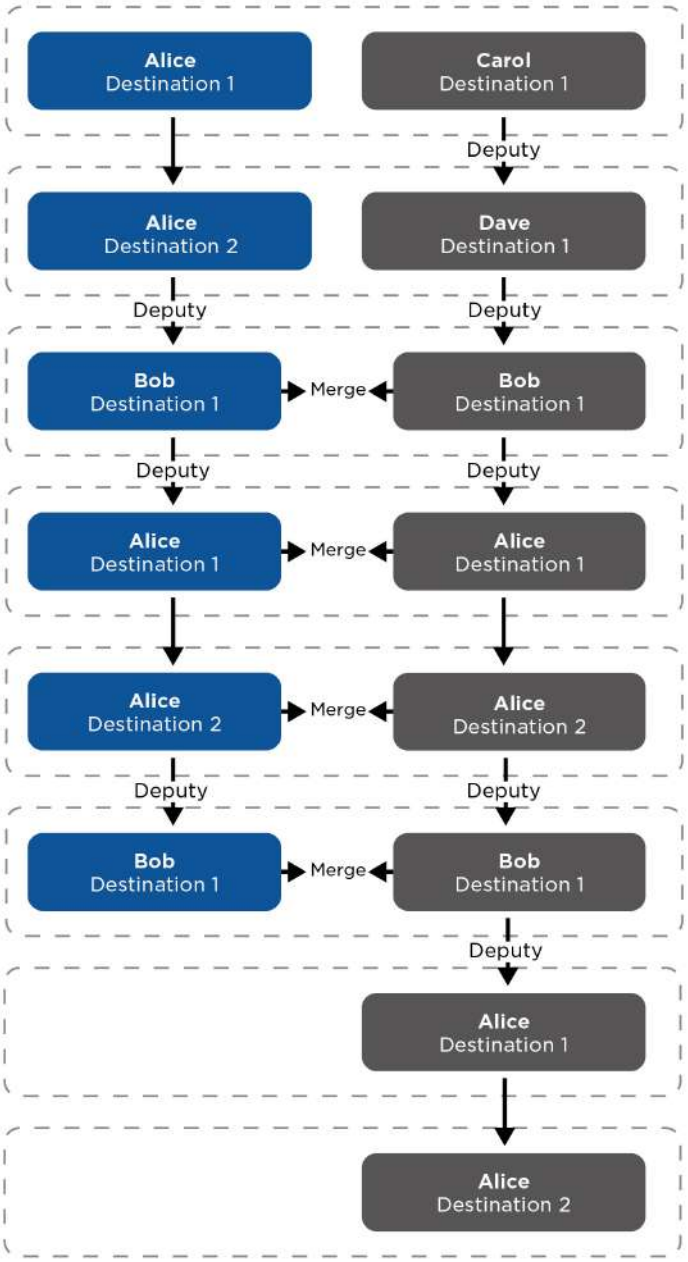
- Alice es suplente de Bob
- Bob es suplente de Alice
- Carol es suplente de Dave
- Dave es suplente de Carol

El esquema de llamada es el siguiente (en el caso de que nadie acepte o rechace la llamada):



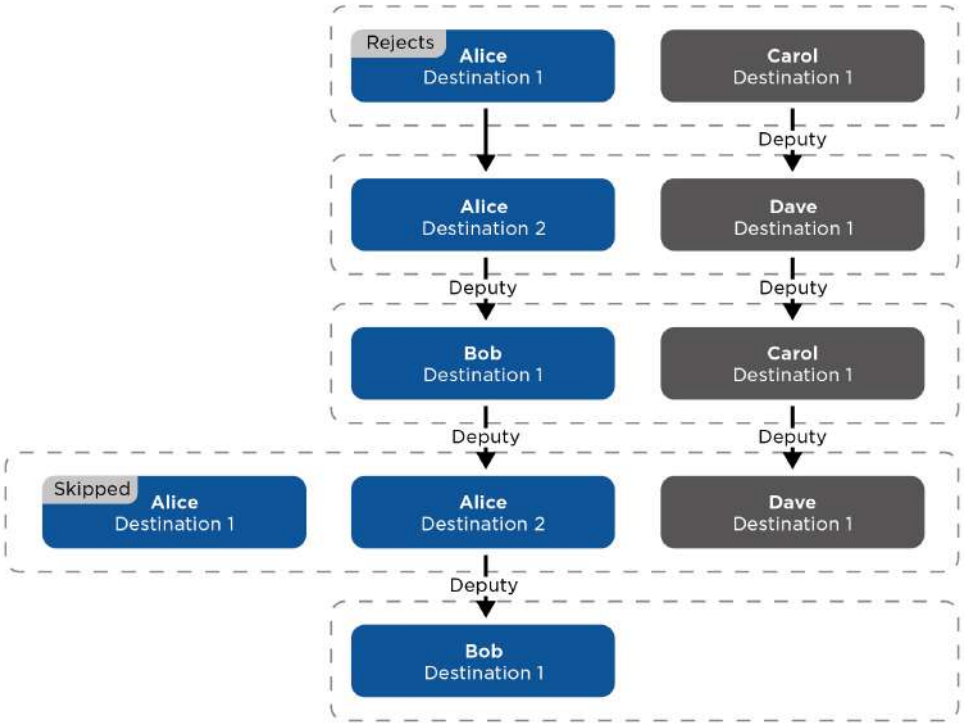
Ejemplo 2

Tomemos el ejemplo anterior y cambiemos al suplente de Dave al suplente de Bob. Con ello se unirán ambas ramas (luego, desde el paso 3 se realiza solo una llamada). En el gráfico se ve también que a Alice al final se le llama tres veces. Eso sucede a causa de que el límite del ciclo de llamada se aplica para cada rama por separado y Alice está siendo llamada en realidad solo dos veces en la rama azul y solo dos veces en la rama lila.



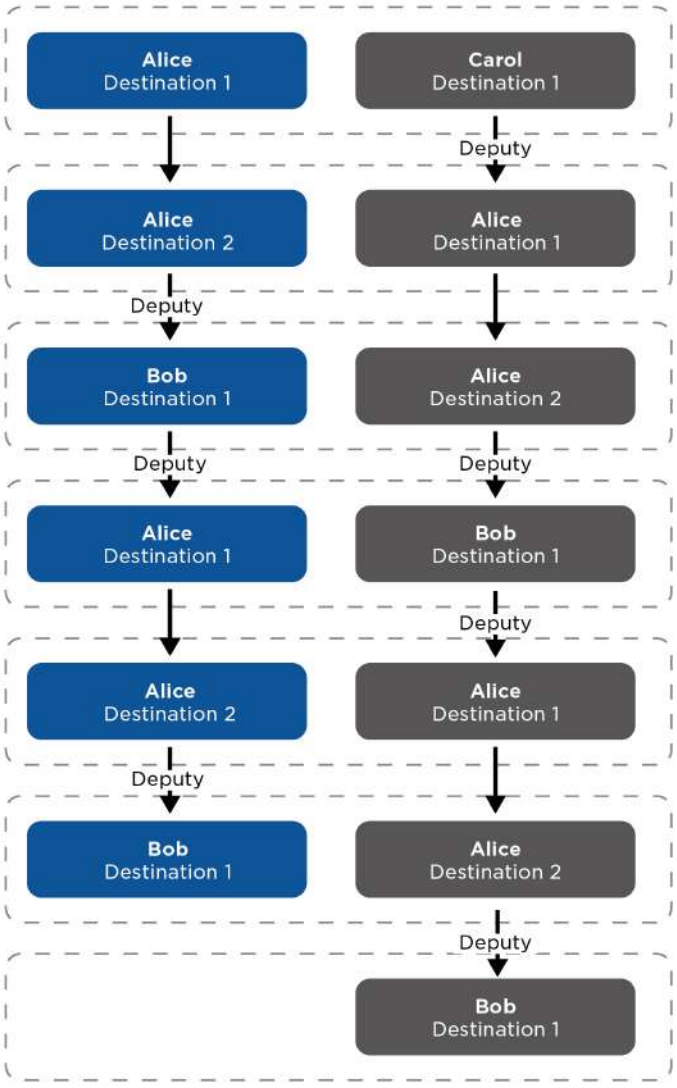
Ejemplo 3

Tomemos la configuración del ejemplo 1 y sopesemos la situación en la que Alice rechace la llamada de su primera estación. Luego, el algoritmo saltará esta destinación (ya que el usuario rechazó activamente la llamada y no tiene sentido volver a llamarlo otra vez). Entonces, con los rechazos de llamadas desde diferentes estaciones de llamada, cambian dinámicamente los grupos de llamada en cada uno de los pasos. El salto de la estación de llamada, que había rechazado la llamada, vale para todas las ramas sin tener en cuenta en cuál de ellas se había rechazado la llamada.



Ejemplo 4

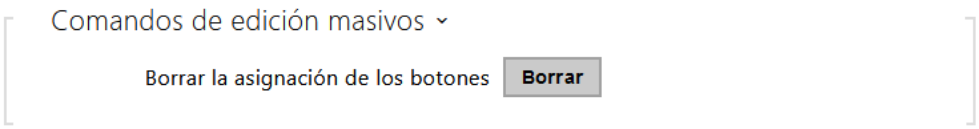
Puede suceder que dos estaciones de llamada de un solo usuario están siendo llamadas a la vez. Esto se puede lograr configurando el esquema de manera parecida a la figura abajo, pero esto puede suceder también al saltar las destinaciones que habían rechazado la llamada previamente.



5.3.2 Marcación

Botones de marcación rápida

En esta página se puede asignar a los botones de marcado rápido un usuario introducido en la lista de usuarios en la página **Directorio** > **Usuarios**. En el estado inicial están todos los botones disponibles del intercomunicador vinculados con el usuario en la lista. En el caso de que el botón no esté asignado a ningún usuario, aún se puede utilizar por ej. en la automatización o activación del interruptor. En el modelo **2N® IP Base** hay que elegir primero el número de botones en el menú Hardware >Módulos de ampliación.



- **Borrar la asignación de los botones** – borrará todas las asignaciones de los botones a los usuarios.

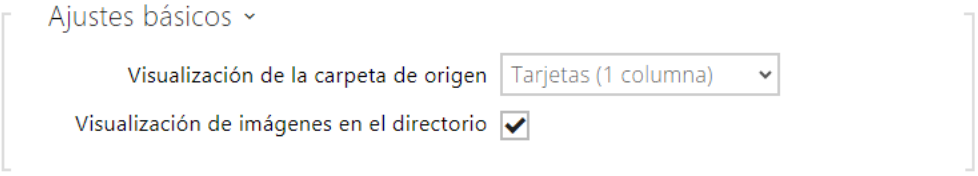
Muestra la lista de todos los botones potencialmente disponibles en el intercomunicador. La lista contiene botones, incluidos aquellos que no están presentes físicamente en el intercomunicador. En algunos modelos (**2N® IP Vario**, **2N® IP Verso**) está la lista de botones dividida en grupos de 8, event. 5 botones correspondientes a los módulos de botones de ampliación. En el campo de edición se pueden añadir usuarios mediante el icono  al marcarlo y confirmarlo con el botón añadir. El usuario deseado se puede buscar también en la lista utilizando el campo de fulltext según el nombre. Un botón del marcado rápido pueden compartir varios usuarios a la vez. El botón configurado del marcado rápido se puede probar mediante el icono  . Tras pulsar el botón aparecerá la ventana de diálogo con la información detallada sobre la llamada en curso (participante, dirección de la llamada, estado, causa y hora del último suceso).

Nota

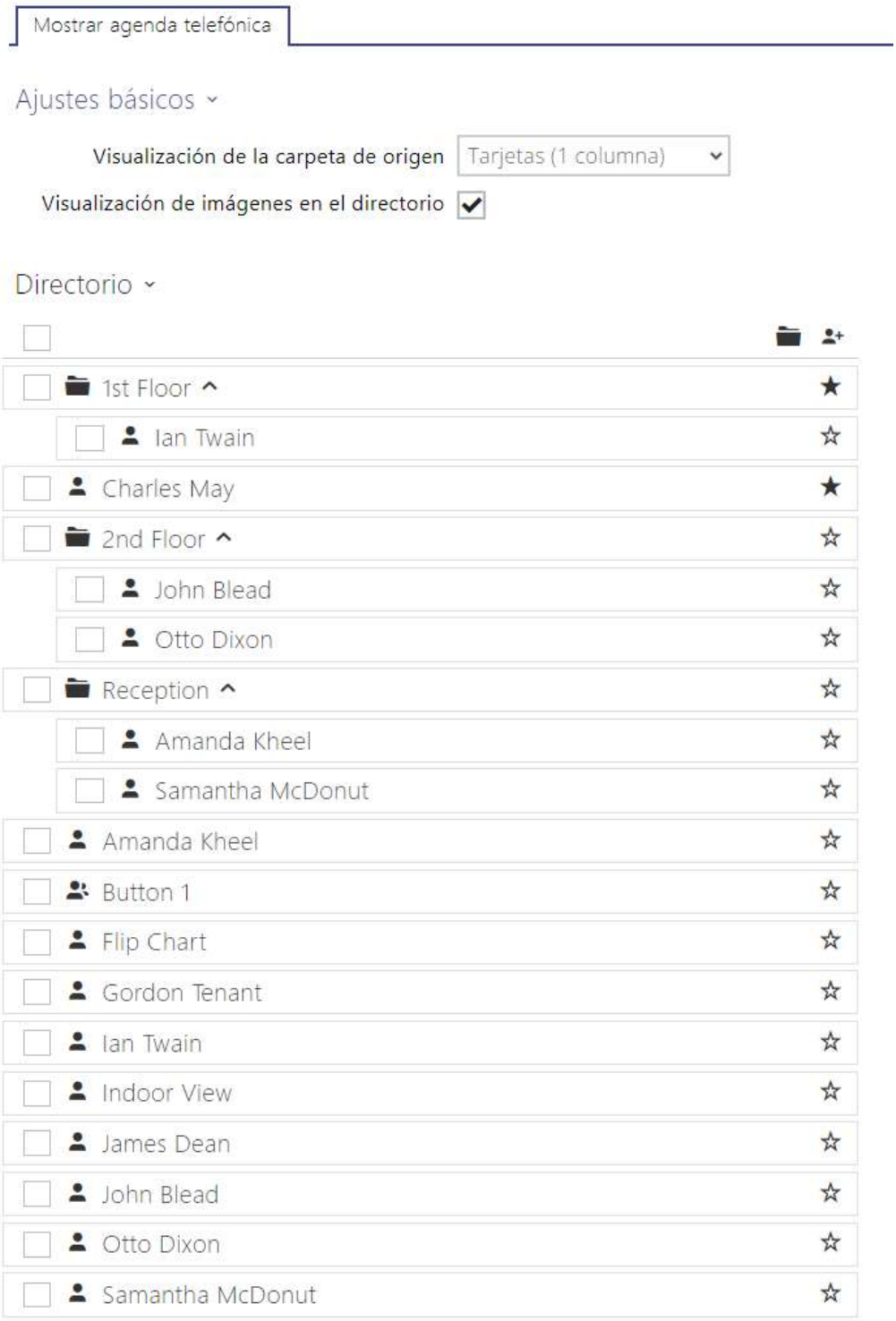
- Al botón del marcado rápido se pueden vincular hasta 16 usuarios.
- La cantidad total máxima de los números llamados al mismo tiempo es 16, lo cual puede suceder al utilizar a la vez la llamada de grupo y al configurar varios números llamados en un botón de marcado rápido.

Mostrar agenda telefónica

En esta solapa se configura la lista estructurada de usuarios visualizada en la pantalla. La lista se puede dividir prácticamente en cualquier cantidad de grupos y en cada uno de los grupos de puede introducir cualquier número de usuarios desde el directorio. En un grupo no se puede introducir un usuario varias veces, sin embargo, cada usuario del directorio puede estar en varios grupos a la vez.



- **Visualización de la carpeta de origen** – Permite seleccionar la visualización de la carpeta de origen del directorio en la pantalla de inicio del dispositivo. Es posible elegir la visualización en tarjetas (con una imagen más grande) o visualización de lista de elementos estándar (entonces, la visualización en la lista de elementos se rige por la configuración Mostrar imágenes). La configuración no tendrá efecto antes de que el usuario pase a otra parte de la interfaz gráfica (por ejemplo a la Búsqueda).
- **Visualización de imágenes en el directorio** – Permite elegir si las imágenes se mostrarán o no en la visualización del directorio en la pantalla en el caso de la visualización en la lista de elementos.



En la parte izquierda de la pantalla aparecen las carpetas creadas y los usuarios por separado. Una nueva carpeta se puede añadir mediante el botón . El directorio se puede eliminar

mediante el botón con los usuarios y grupos incluidos. Un grupo creado previamente se puede renombrar pulsando el botón . El traslado del un usuario del árbol principal del directorio a la carpeta se realiza mediante el icono .

En la parte derecha de la pantalla aparecen los usuarios incluidos en el grupo actualmente seleccionado. Mediante el botón se puede añadir al grupo un usuario, el cual se queda a la vez en el árbol principal del directorio. Para resaltar el primer elemento en el grupo en la pantalla sirve el botón . El usuario se puede eliminar pulsando el botón .

Los grupos y los usuarios están ordenados en la pantalla según el orden alfabético. El orden de los grupos y de los usuarios se puede precisar asignando la prioridad pulsando el icono .

Los elementos del directorio tienen 8 posibles prioridades. La prioridad 1 colocará el elemento al principio de la lista, si no hay prioridad ninguna lo colocará al final de la lista. En el caso de que existan varios elementos con la misma prioridad, estos se agrupan y se ordenan según el orden alfabético.

Precaución

- Siempre hay que guardar los cambios de configuración en el directorio.
- Los cambios en la configuración (visualización de las fotografías, carpeta de origen, contenido, etc.) no tendrán efecto antes de pasar al menú de búsqueda o marcado.

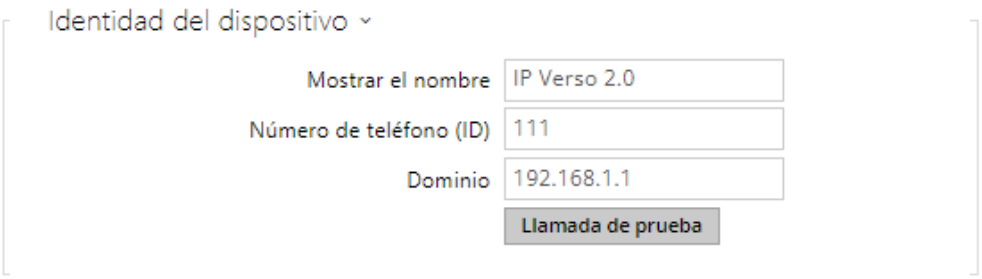
5.3.3 SIP 1 / SIP 2

Los intercomunicadores **2N IP** permiten configurar dos cuentas SIP independientes. El intercomunicador puede ser de esta manera registrado en paralelo bajo dos números de teléfono, en dos centralitas SIP diferentes, etc. Desde el punto de vista de las llamadas entrantes son ambas cuentas SIP equivalentes. Las llamadas salientes están en principio realizadas mediante la cuenta SIP 1. En el caso de que la cuenta SIP 1 no esté registrada (por ej. debido al fallo de la centralita SIP), se utilizará automáticamente la cuenta SIP 2 para las llamadas salientes. Junto a los números de teléfono en la lista telefónica se puede de forma explícita especificar el número de cuenta que se debe utilizar para las llamadas de salida (por ej. **2568/1** – llamada al número 2568 mediante la cuenta SIP 1, **sip:1234@192.168.1.1/2** llamada a sip uri mediante la cuenta SIP 2).

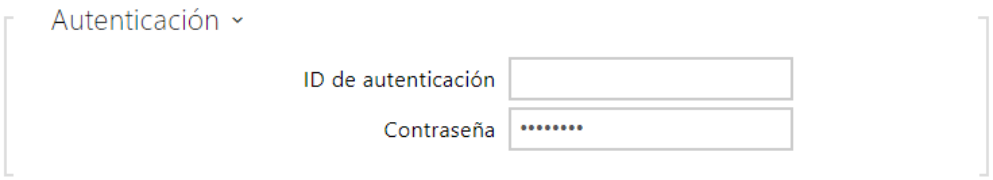
Solapa Configuración

- 

Permiso de la cuenta SIP – permite el uso de la cuenta SIP para hacer llamadas. En el caso de que la cuenta no esté permitida no se puede utilizar para realizar llamadas salientes ni recibir llamadas entrantes.



- **Nombre mostrado** – configura el nombre que se mostrará en el teléfono del destinatario como la identificación de la persona que llama.
- **Número de teléfono (ID)** – configura el número de teléfono propio del intercomunicador (eventualmente otro ID inconfundible que consiste en caracteres y números). Este número, junto con el dominio, identifica de forma inconfundible al intercomunicador durante las llamadas y registros.
- **Dominio** – configura el nombre de dominio del servicio en el que se registra el intercomunicador. Normalmente coincide con la dirección SIP proxy o con el Registrador.
- **Llamada de prueba** – llama a la ventana de diálogo con la opción de realizar la llamada de prueba al número de teléfono elegido, ver a continuación.



- **ID de autenticación** – ID alternativo del usuario utilizado para la autenticación del dispositivo. El número de teléfono (ID) se utilizará en el caso de que este parámetro esté vacío.
- **Contraseña** – contraseña utilizada para la autenticación del intercomunicador. En el caso de que su centralita IP no requiera la autenticación, el parámetro no se aplicará.

- **Dirección proxy** – dirección IP o el nombre de dominio del SIP Proxy.
- **Puerto proxy*** – configura el puerto SIP Proxy. El dispositivo utilizará el puerto inicial según la capa de transporte (5060 ó 5061) u otro puerto obtenido del DNS en el caso de que el parámetro esté vacío o esté configurado a 0.
- **Dirección del proxy de respaldo** – dirección IP o el nombre de dominio del SIP Proxy. La dirección se utilizará en el caso de que el proxy principal no responda a las peticiones.
- **Puerto de proxy de respaldo*** – configura el puerto de SIP proxy de respaldo. El dispositivo utilizará el puerto inicial según la capa de transporte (5060 ó 5061) u otro puerto obtenido del DNS en el caso de que el parámetro esté vacío o esté configurado a 0.

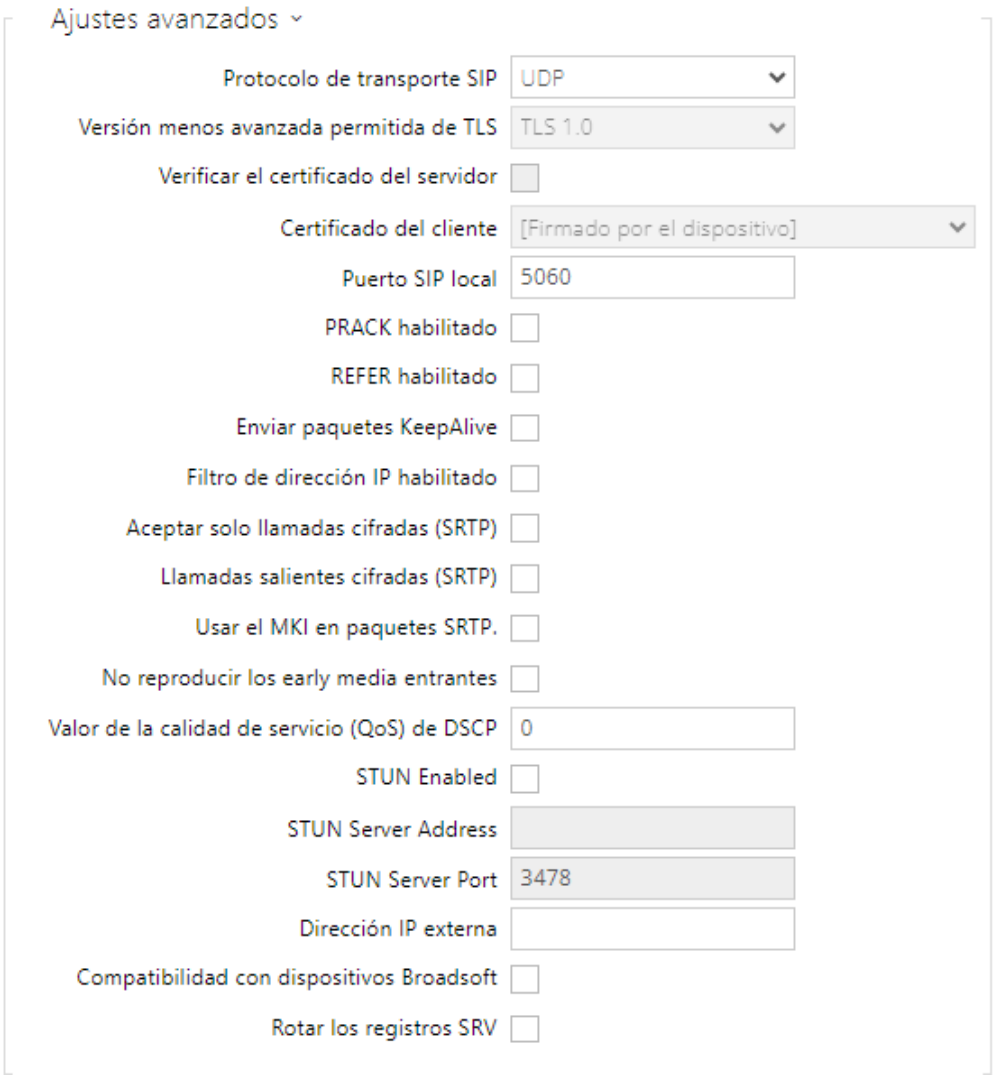
- **Permiso de registro** – permite el registro del intercomunicador con el registrador SIP configurado.
- **Dirección del registrador** – dirección IP o el nombre de dominio del Registrador SIP.
- **Puerto del registrador*** – configura el puerto del registrador SIP. El dispositivo utilizará el puerto inicial según la capa de transporte (5060 ó 5061) u otro puerto obtenido del DNS en el caso de que el parámetro esté vacío o esté configurado a 0.
- **Dirección del registrador de respaldo** – dirección IP o nombre de dominio del registrador SIP de respaldo. La dirección se utilizará en el caso de que el registrador principal no responda a las peticiones.
- **Puerto del registrador de respaldo*** – configura el puerto del registrador SIP de respaldo. El dispositivo utilizará el puerto inicial según la capa de transporte (5060 ó 5061) u otro puerto obtenido del DNS en el caso de que el parámetro esté vacío o esté configurado a 0.
- **Tiempo de expiración del registro** – permite configurar el tiempo de vencimiento del registro, lo cual afecta a la carga de la red y del Registrador SIP por las peticiones de registro enviados periódicamente. El Registrador SIP puede modificar el tiempo de la expiración sin su conocimiento.
- **Estado del registro** – muestra el estado actual del registro (No registrado, Regístrese..., Registrado, El registro finaliza...).
- **Causa del fallo** – muestra la causa del fallo del último intento del registro – muestra la última respuesta de error del registrador, por ej. 404 Not Found.

Consejo

- Outbound proxy es posible configurar de manera que la dirección Outbound proxy se introduce en los parámetros Dirección proxy y Dirección del registrador. Dominio = dirección del registrador.

Precaución

- En el caso de que el **parámetro*** se deje vacío, o el valor del parámetro sea 0, se utilizará el puerto inicial según el protocolo de transporte elegido (5060 para TCP o UDP, 5061 para TLS).



- **Protocolo de transporte para SIP** – configura el protocolo utilizado para la comunicación SIP. Se puede elegir entre UDP (predeterminado), TCP o TLS.

- **Versión menos avanzada permitida de TLS** – determina la versión menos avanzada de TLS que se permitirá para la conexión a los dispositivos.
- **Verificar el certificado del servidor** – verificará el certificado público SIP del servidor con respeto a los certificados CA cargados en el dispositivo.
- **Certificado del cliente** – especifica el certificado de cliente y la clave privada, con la ayuda de los cuales se verifica la autorización del intercomunicador para comunicarse con el servidor SIP.
- **Puerto local para SIP** – configura el puerto local al cual utiliza el intercomunicador para la señalización SIP. El cambio de este parámetro no se notará hasta después del reinicio del intercomunicador. El valor predeterminado del parámetro es 5060.
- **PRACK habilitado** – habilita el método PRACK (confirmación fiable de los mensajes SIP con códigos del 101–199).
- **REFER habilitado** – habilita el desvío de llamadas mediante el método REFER.
- **Enviar paquetes Keep Alive** – configura si el intercomunicador realiza en intervalos periódicos preguntas acerca del estado de la estación llamada mediante las peticiones SIP OPTIONS durante la llamada (sirve para detectar el fallo de la estación durante la llamada).
- **Habilitación del filtro de las direcciones IP** – permite activar la función del bloqueo de la recepción de los paquetes SIP desde otras direcciones que no sean la dirección de SIP Proxy y SIP Registrar. La función sirve sobre todo para aumentar la seguridad de la comunicación y evitar las llamadas telefónicas no autorizadas.
- **Aceptar solo llamadas cifradas (SRTP)** – configura la restricción de llamadas aceptadas en esta cuenta a llamadas cifradas con el protocolo SRTP. Las llamadas no cifradas serán rechazadas. A la vez es recomendable utilizar, para aumentar la seguridad, el TLS como protocolo de transporte para SIP.
- **Llamadas salientes cifradas (SRTP)** – configura las llamadas salientes en esta cuenta a llamadas cifradas con el protocolo SRTP. A la vez es recomendable utilizar, para aumentar la seguridad, el TLS como protocolo de transporte para SIP.
- **Utilizar MKI en los paquetes SRTP** – permite utilizar MKI (Master Key Indentifier), el cual es requerido por la parte opuesta, para la identificación de la clave principal al haber rotación de varias claves en los paquetes SRTP.
- **No reproducir los early media entrantes** – prohíbe la reproducción del stream de audio entrante antes de aceptar la llamada (early media) que envían algunas centralitas u otros dispositivos. En lugar de ello se reproducirá el tono de timbre local estándar.
- **Valor QoS DSCP** – configura la prioridad de los paquetes SIP en la red. El valor configurado se envía en el campo TOS (Type of Service) del encabezado del paquete IP. El valor se introduce como un número decimal.

Tip

Valores QoS DSCP recomendados			
	QoS decimales	**QoS hexadecimales**	**Qos DSCP decimales (ToS)**
Señalización	24 / 26	18 / 1A	96 / 104
Audio	46	2E	184
Video	40	28	160

- **STUN habilitado** – habilita la funcionalidad STUN para la cuenta SIP. La dirección y los puertos adquiridos del servidor STUN configurado se utilizarán en los encabezados SIP y en la negociación de medios SDP.
- **Dirección del servidor STUN** – establezca la dirección IP del servidor STUN que se utilizará para esta cuenta SIP.
- **Puerto del servidor STUN** – establezca el puerto del servidor STUN que se utilizará para esta cuenta SIP.
- **Dirección IP externa** – configura la dirección IP pública o el nombre del router al que está conectado el intercomunicador. Si la dirección IP del dispositivo es pública, deje el campo en blanco.
- **Compatibilidad con dispositivos Broadsoft** – configura el modo de compatibilidad con las centralitas Broadsoft. Cuando en este modo el intercomunicador acepta al re-invite de la centralita, responde en vez del menú completo mediante la repetición del último SDP enviado con los códecs utilizados actualmente.
- **Rotar los registros SRV** – permite la rotación de los registros SRV para SIP proxy y registrar. Este método es un método alternativo para pasar a los servidores de respaldo en el caso de un fallo o falta de disponibilidad de los servidores principales.

Precaución

- Para utilizar el requerimiento NAPTR / SRV DNS hay que cancelar la configuración del puerto para Proxy/Registrar.

Solapa Vídeo

- Permite habilitar/prohibir el uso de cada uno de los códec de vídeo ofrecidos a la hora de establecer la conexión y configurar su prioridad.

- **Resolución de la imagen** – configura la resolución de la imagen durante las llamadas telefónicas.
- **Frecuencia de imágenes** – configura la frecuencia de imágenes de vídeo durante las llamadas telefónicas.
- **Velocidad de transferencia** – configura la velocidad de transferencia del stream de vídeo durante las llamadas telefónicas.

- **Modo PTZ** – habilita la función de PTZ (Pan-Tilt-Zoom) que permite elegir la sección visualizada de la imagen de la cámara durante la llamada mediante DTMF (se necesita la licencia **GOLD**).
  En el caso de que la función esté habilitada, se puede controlar la cámara mediante el teclado numérico del teléfono IP. El modo PTZ se enciende y se apaga con la tecla *****. El significado de las teclas del teléfono IP en el modo PTZ es el siguiente:

Tecla del teléfono IP	Funciones en el modo PTZ
*****	Encendido y apagado de la función PTZ
1	Aumento
3	Disminución
2	Desplazamiento de la sección de la imagen hacia arriba
4	Desplazamiento de la sección de la imagen hacia la izquierda
6	Desplazamiento de la sección de la imagen hacia la derecha
8	Desplazamiento de la sección de la imagen hacia abajo
5	Vuelta al estado inicial

- **PTZ y Face Zooming** – Habilita las funciones PTZ (Pan-Tilt-Zoom) o Face Zooming que permiten modificar la sección mostrada de la imagen de la cámara durante la llamada. Con la opción *Face Zooming* la imagen de la cámara acercará la cara del usuario que está parado frente al dispositivo. Con la opción *Face Zooming – solo inclinación* se desplazará el recorte de la imagen solo de manera que enfoque la cara.

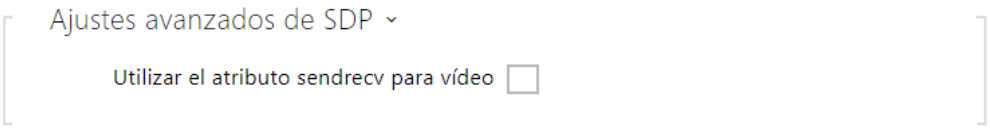
> **Aviso**
>
> - La función Face Zooming está disponible solo en los modelos con procesador ARTPEC-7 de la compañía Axis.

- **Valor QoS DSCP** – configura la prioridad de los paquetes de vídeo RTP en la red. El valor configurado se envía en el campo TOS (Type of Service) del encabezado del paquete IP. El valor se introduce como un número decimal. Los valores QoS recomendados válidos para la señalización, audio y vídeo se muestran en la tabla más arriba.
- **Tamaño máximo del paquete** – permite configurar el tamaño máximo de los paquetes de vídeo RTP enviados.

La lista de las configuraciones ampliadas de los códecs puede variar según el tipo del dispositivo.

- **H.264 Baseline Profile, Packetization Mode 1**
- **H.264 Baseline Profile, Packetization Mode 0**
- **H.264 Main Profile, Packetization Mode 1**
- **H.264 Main Profile, Packetization Mode 0**
- **H.264 High Profile, Packetization Mode 1**
- **H.264 High Profile, Packetization Mode 0**
- **H.264 Constrained Baseline Profile, Packetization Mode 1**
- **H.264 Constrained Baseline Profile, Packetization Mode 0**

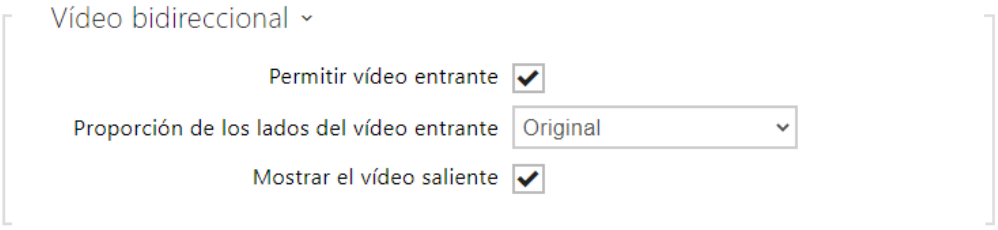
  - **Permitido** – habilita el modo de paquetización y configura el tipo de payload para cada uno de los códecs. El tipo de payload se seleccionará automáticamente en el caso de que no pueda ser configurado manualmente.
  - **SDP Payload Type** – configura el llamado payload type del códec de vídeo H.264 (packetisation mode 1). Puede configurar el valor dentro del rango de 96 hasta 127, event. 0 para que no se ofrezca más esta variante del códec.
- **H.263+**
  - **SDP Payload Type** – configura el llamado payload type del códec de vídeo H.263+. Puede configurar un valor dentro del rango desde 96 hasta 127.



- **Utilizar el atributo sendrecv para vídeo** – esta configuración se llamaba antes Compatibilidad con teléfonos Polycom. Esta configuración sirve para asegurar la compatibilidad con algunos dispositivos de terceros (Polycom/Cisco y otros). Si este modo está activado, el intercomunicador envía el indicio sendrecv en vez de sendonly en el mensaje SDP del menú del códec de vídeo.

Consejo

- Para la función Video Preview en el teléfono **Grandstream GXV 3275** (el vídeo se transmite mediante Early Media) no hace falta ninguna configuración. En el caso de conexión a través de PBX contacte con el fabricante para verificar si la centralita determinada soporta esta función.
- Para la función Video Preview en el teléfono **Gigaset Maxwell 10** (el vídeo se transmite mediante imágenes .jpg) es necesario en la solapa **HTTP API** junto al elemento **Cámara API** configurar el **Tipo de conexión** = **No asegurada (TCP)** y **Autenticación** = **Ninguna**



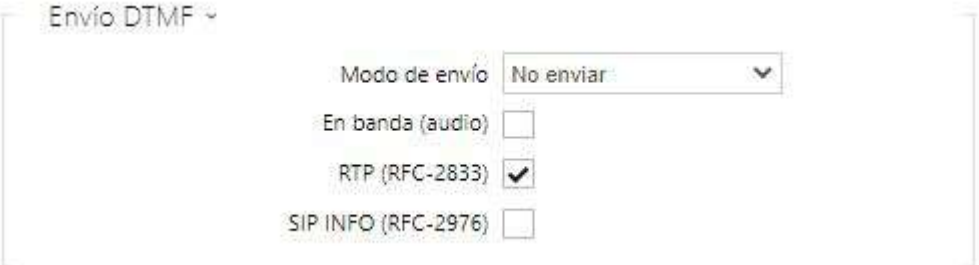
- **Permitir vídeo entrante** – en el caso de que este modo esté encendido, el intercomunicador mostrará durante la llamada el vídeo de la parte opuesta en el caso de que ésta se lo permita.

- **Proporción de los lados del vídeo entrante** – configura la proporción preferida de los lados del vídeo entrante mostrado en la pantalla. Cuando está establecida proporción que no sea la original, el vídeo se recorta de manera que en la proporción nueva de los lados llene el ancho de la pantalla.
- **Mostrar el vídeo saliente** – selecciona si el intercomunicador mostrará durante la llamada la vista previa del vídeo enviado.

Solapa Audio

- Permite habilitar/prohibir el uso de cada uno de los códec de audio ofrecidos a la hora de establecer la conexión y configurar su prioridad. Los códec de banda ancha L16 y G.722 están disponibles solo en los modelos de intercomunicadores determinados. El códec G.729 está disponible en todos los intercomunicadores 2N IP.

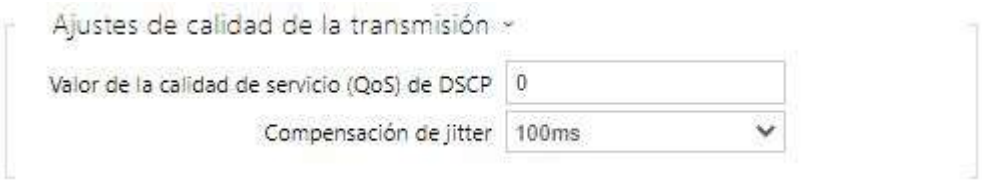
El envío DTMF sirve para configurar el modo de envío de los signos DTMF desde el intercomunicador. Para la función correcta verifique las posibilidades y configuración de la recepción de DTMF por la parte opuesta.



- **Modo de envío** – configura si será posible enviar los signos DTMF durante la llamada al pulsar las teclas 0 hasta 9, * y # en el teclado numérico del intercomunicador. El envío lo puede configurar solo en las llamadas entrantes o salientes, event. en todas las llamadas.
- **In-Band (Audio)** – habilita el modo habitual de envío de DTMF en la banda de audio mediante los tonos dobles estandarizados.
- **RTP (RFC-2833)** – habilita el envío de los signos de DTMF mediante el protocolo RTP según RFC-2833.
- **SIP INFO (RFC-2976)** – habilita el envío de los signos de DTMF mediante mensajes SIP INFO según RFC-2976.

Recepción de DTMF sirve para configurar la recepción de los signos DTMF desde el intercomunicador. Para la función correcta verifique las posibilidades y configuración del envío de DTMF por la parte opuesta.

- **In-Band (Audio)** – habilita la recepción de tonos dobles de DTMF clásicos en la banda de audio.
- **RTP (RFC-2833)** – habilita la recepción de los signos de DTMF mediante el protocolo RTP según RFC-2833.
- **SIP INFO (RFC-2976)** – habilita la recepción de los signos de DTMF mediante mensajes SIP INFO según RFC-2976.



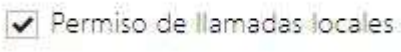
- **Valor QoS DSCP** – configura la prioridad de los paquetes de audio RTP en la red. El valor configurado se envía en el campo TOS (Type of Service) del encabezado del paquete IP. El valor se introduce como un número decimal. Los valores QoS recomendados válidos para la señalización, audio y vídeo se muestran en la tabla más arriba.
- **Jitter Compensation** – configura la longitud de la memoria de compensación para compensar las irregularidades de los intervalos entre las llegadas de los paquetes de

audio. La configuración de la memoria de compensación más duradera aumentará la resistencia de recepción a cambio de un mayor retardo de sonido.

5.3.4 Llamadas locales

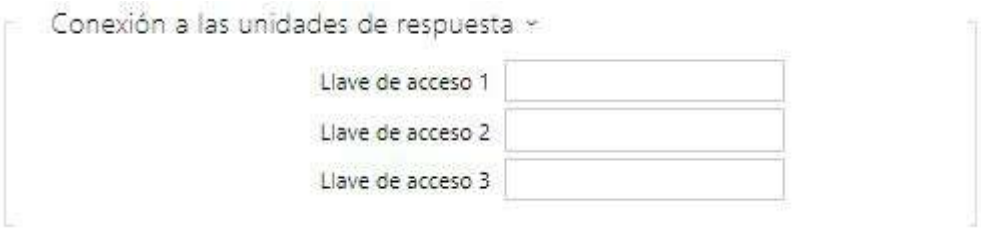
En esta solapa se configura la conexión de las unidades de respuesta 2N con el intercomunicador. El parámetro básico es la clave de acceso que permite asegurar la comunicación entre el intercomunicador y la unidad de respuesta 2N, event. crear dentro de la red local varios grupos independientes de intercomunicadores y unidades de respuesta 2N. También se puede configurar la resolución y la calidad del vídeo mostrado en las unidades de respuesta 2N.

Configuración



- **Habilitación de llamadas locales** – habilita llamadas entre los dispositivos 2N en la red local. Al apagar esta función, otros dispositivos en la red no encontrarán este dispositivo, es decir, no podrán llamar a este dispositivo en formato device:ID_dispositivo.

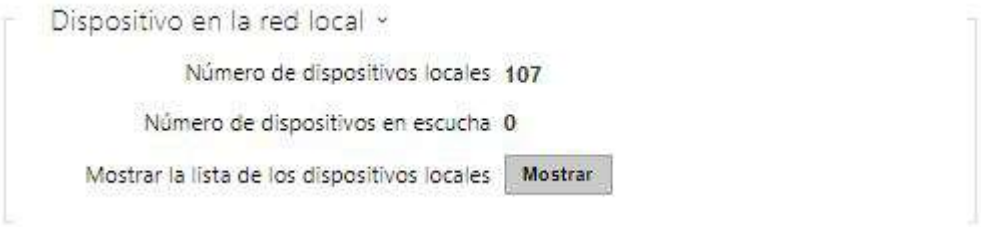
- **ID del dispositivo** – configura la identificación del dispositivo que se mostrará en la lista de los dispositivos locales en todos los dispositivos 2N en la misma red local. Mediante la configuración del número de teléfono del usuario en estos dispositivos en device:ID_del dispositivo, es posible dirigir la llamada a este dispositivo.
- **Llamada de prueba** – llama a la ventana de diálogo con la opción de realizar la llamada de prueba al número de teléfono elegido, ver a continuación.



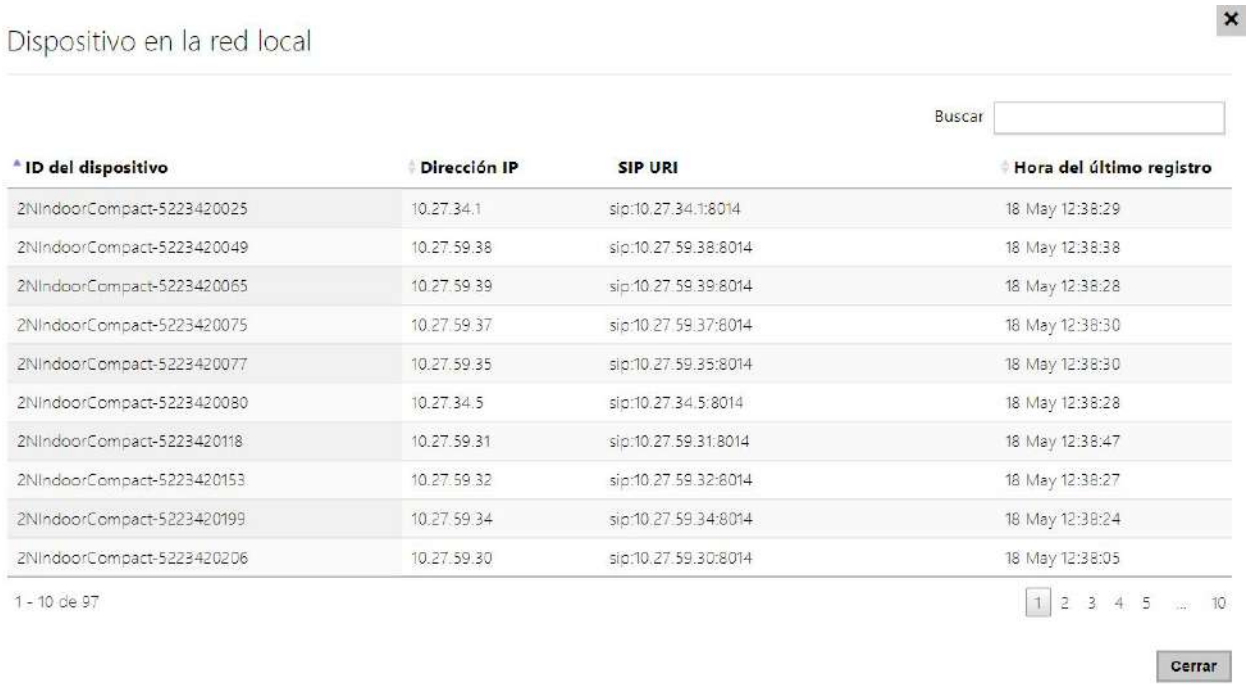
- **Clave de acceso 1–3** – configura la clave de acceso compartido entre el intercomunicador y las unidades de respuesta 2N. En el caso de que la clave introducida en el intercomunicador no coincida con la clave de la unidad de respuesta 2N, no podrán comunicar entre sí, es decir, el intercomunicador no podrá llamar a la unidad de respuesta 2N y a la vez la unidad de respuesta 2N no podrá ver el vídeo del intercomunicador. A cada intercomunicador se pueden asignar hasta tres claves de acceso con lo cual se convertirá en una parte de los grupos independientes de intercomunicadores y de unidades de respuesta 2N. La clave de acceso puede tener longitud de hasta 63 caracteres.

Nota

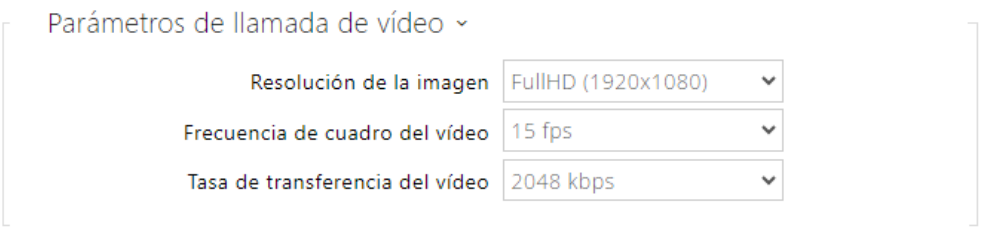
- En el caso de que en la red utilice **2N® Indoor Touch** equipado con firmware de versión 2 ó 3, la clave de acceso no se podrá utilizar y debe configurarse como vacío. La clave de acceso puede utilizarse solo con **2N® Indoor Touch** de la versión 4 y superior.



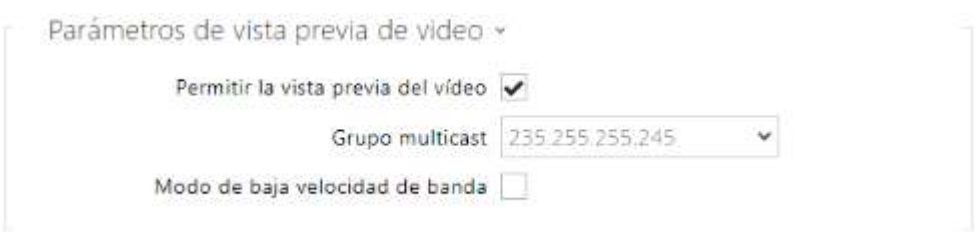
- **Número de dispositivos locales** – muestra el número actual de las unidades de respuesta 2N locales.
- **Número de dispositivos seguidores** – muestra el número actual de las unidades de respuesta 2N que siguen el vídeo del intercomunicador.
- **Mostrar la lista de los dispositivos locales** – abre la ventana con la lista de las unidades de respuesta 2N locales.



Vídeo



- **Resolución de la imagen** – define la resolución de vídeo para las llamadas telefónicas (para el códec de vídeo).
- **Frecuencia de cuadro del vídeo** – define la frecuencia de cuadro de vídeo para las llamadas telefónicas (para el códec de vídeo).
- **Tasa de transferencia del vídeo** – define la tasa de transferencia de transmisión de vídeo para las llamadas telefónicas (para el códec de vídeo).



- **Habilitar la vista previo del vídeo** – habilita la transmisión de la vista previa del vídeo en multicast.
- **Grupo multicast** – configura la dirección de multicast a la que se enviará el stream de vídeo desde el intercomunicador. Se puede elegir 1 de las 8 direcciones pre-configuradas, event. configurar el modo en el que el intercomunicador elige la dirección automáticamente.
- **Modo de baja velocidad de banda** – reduce la calidad del flujo de vista previa de video para conservar el ancho de banda.

- **Modo PTZ** – habilita la función de PTZ (Pan-Tilt-Zoom) que permite elegir la sección visualizada de la imagen de la cámara durante la llamada mediante DTMF (se necesita la licencia **GOLD**).
  En el caso de que la función esté habilitada, se puede controlar la cámara mediante el teclado numérico del teléfono IP. El modo PTZ se enciende y se apaga con la tecla *****. El significado de las teclas del teléfono IP en el modo PTZ es el siguiente:

Tecla del teléfono IP	Funciones en el modo PTZ
*****	Encendido y apagado de la función PTZ
1	Aumento
3	Disminución
2	Desplazamiento de la sección de la imagen hacia arriba
4	Desplazamiento de la sección de la imagen hacia la izquierda
6	Desplazamiento de la sección de la imagen hacia la derecha
8	Desplazamiento de la sección de la imagen hacia abajo
5	Vuelta al estado inicial

- **PTZ y Face Zooming** – Habilita las funciones PTZ (Pan-Tilt-Zoom) o Face Zooming que permiten modificar la sección mostrada de la imagen de la cámara durante la llamada. Con la opción *Face Zooming* la imagen de la cámara acercará la cara del usuario que está parado frente al dispositivo. Con la opción *Face Zooming – solo inclinación* se desplazará el recorte de la imagen solo de manera que enfoque la cara.

  Aviso

  - La función Face Zooming está disponible solo en los modelos con procesador ARTPEC-7 de la compañía Axis.

- **Permitir vídeo entrante** – en el caso de que este modo esté encendido, el intercomunicador mostrará durante la llamada el vídeo de la parte opuesta en el caso de que ésta se lo permita.
- **Proporción de los lados del vídeo entrante** – configura la proporción preferida de los lados del vídeo entrante mostrado en la pantalla. Cuando está establecida proporción que no sea la original, el vídeo se recorta de manera que en la proporción nueva de los lados llene el ancho de la pantalla.
- **Mostrar el vídeo saliente** – configura la proporción preferida de los lados del vídeo entrante mostrado en la pantalla. Cuando está establecida proporción que no sea la original, el vídeo se recorta de manera que en la proporción nueva de los lados llene el ancho de la pantalla.

Audio

- **Compensación de jitter** – configura la longitud de la memoria de compensación para compensar las irregularidades de los intervalos entre las llegadas de los paquetes de audio. La configuración de la memoria de compensación más duradera aumentará la resistencia de recepción a cambio de un mayor retardo de sonido.

5.3.5 Crestron

- **Habilitar Crestron Network Discovery** – habilita la identificación de los intercomunicadores 2N IP dentro de la red Crestron.

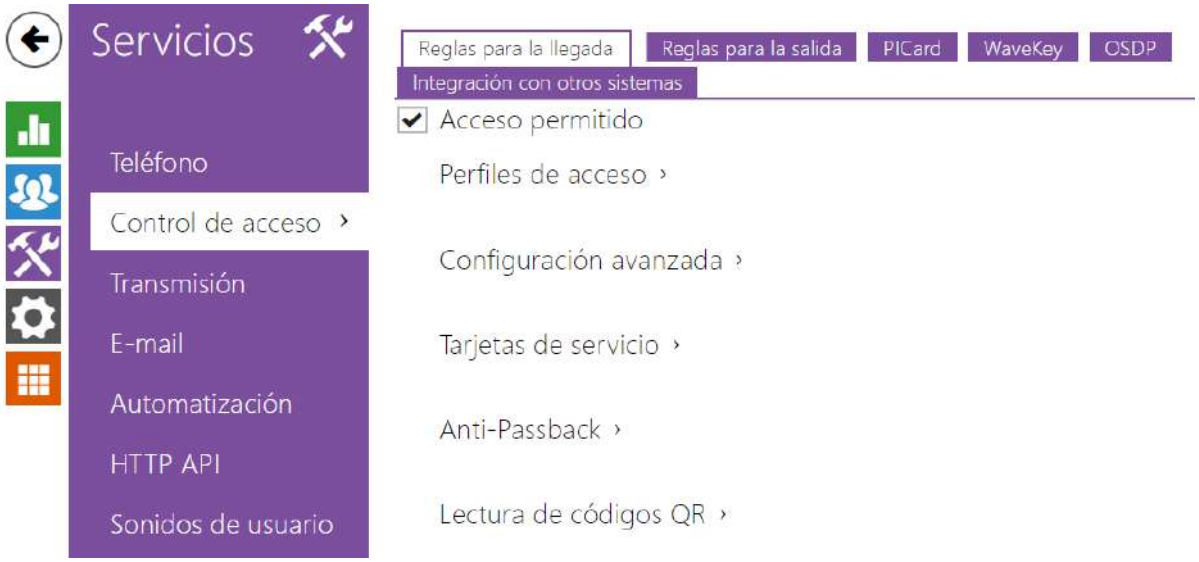
- **Nombre del dispositivo Crestron** – nombre del dispositivo.
- **Lista de los grupos Crestron** – nombre del grupo.
- **Habilitar multicast del vídeo para los paneles Crestron** – habilita multicast del vídeo para los paneles Crestron. Eso permite recibir el mismo vídeo a varios dispositivos Crestron y de esa manera ahorra la capacidad de transferencia de la red local.
- **Dirección de multicast para Crestron** – dirección de multicast que se utilizará para el vídeo de multicast con los dispositivos Crestron.
- **Puerto de muticast para Crestron** – puerto de multicast que se utilizará para el vídeo de multicast con los dispositivos Crestron.
- **Valor TTL para multicast Crestron** – Valor TTL (Time To Live) que se utilizará para la emisión del vídeo como early media para los dispositivos Crestron.

5.4 Servicios

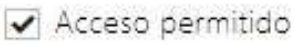
Aquí se expone el resumen de lo que encontrará en este capítulo:

5.4.1 Control de acceso

El servicio Control de acceso sirve para administrar los accesos y la forma de verificación la autenticación del usuario.



Solapa Reglas para la llegada



- **Acceso permitido** – permite cualquier acceso desde un lado determinado de la puerta (llegada, salida). En el caso de que el acceso no esté permitido, no es posible abrir la puerta desde este lado.

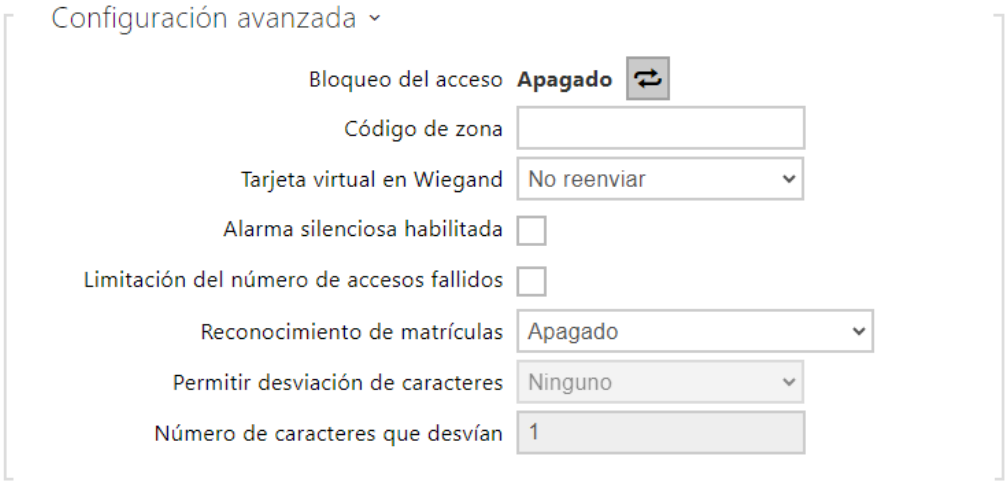
- **Perfil de tiempo** – ofrece la elección de uno o varios perfiles de tiempo a la vez que se aplicarán. La propia configuración de los perfiles de tiempo se puede realizar en la sección Directorio / Perfiles de tiempo.

-  con la marca se configura la elección de los perfiles de tiempo pre-definidos o la configuración manual del perfil de tiempo para el elemento determinado.

- **Forma de la autenticación** – configura la forma de la autenticación (Bluetooth, huella dactilar, tarjeta de acceso, código numérico) durante el período de validez del perfil de tiempo en esta línea, incluida la posibilidad de autenticación múltiple para aumentar la seguridad. Con la opción 'Acceso denegado' se puede prohibir totalmente el acceso.
- **Código de zona** – permite el código de zona para la combinación del perfil de tiempo y la forma de autenticación en esta línea. El código de zona se puede utilizar luego en lugar del código PIN del usuario.

Aviso

- En el caso de que el perfil de tiempo no esté configurado, la forma de la autenticación es ignorado en la línea determinada.



- **Bloqueo del acceso** – muestra la configuración actual de acceso. Encendido/ Apagado.
- **Código de zona** – permite introducir el código numérico del interruptor. El código debe contener al menos dos caracteres, sin embargo, recomendamos utilizar al menos cuatro caracteres.
- **Tarjetas visuales en Wiegand** – permite elegir la salida Wiegand a la que se enviará el número de la tarjeta virtual del usuario tras su autenticación satisfactoria. Se puede utilizar con cualquier manera de autenticación, incluidos los códigos, huellas dactilares, etc.
- **Habilitar alarma silenciosa** – a cada código de acceso está asignado un código virtual que es mayor por un uno que el de acceso y está destinado para activar el alarma silenciosa. Por ejemplo, si el código de acceso es 0000, el código para activar el alarma silenciosa es 0001. La longitud del código debe conservarse, lo que significa que por ejemplo para el código de acceso 9999 el alarma silenciosa es 0000, etc. La acción ejecutada para el alarma silenciosa se puede configurar en la sección para la automatización.

Aviso

- En el caso de que el usuario utilice la autenticación para activar el alarma silenciosa y el alarma silenciosa no está permitida, su acceso se denegará y el alarma no se activará.

- **Limitación del número de accesos fallidos** – permite limitar el número de intentos fallidos de autenticación. Tras cinco intentos fallidos de acceso (código numérico incorrecto, tarjeta no válida, etc.) se bloqueará el módulo de acceso durante treinta segundos, incluso en el caso de que la autenticación haya sido válida.

- **Reconocimiento de matrículas** – elige el escenario para el reconocimiento de la matrícula del vehículo.

> **Aviso**
>
> - Para la función correcta es recomendable que cada matrícula esté asignada a un registro en el directorio. En el caso de matrículas introducidas de forma múltiple sucede la situación que no se puede asignar de forma inequívoca un registro en el directorio que tenga configurada la matrícula (se selecciona el primer registro que tiene configurada la matrícula correspondiente y se aplicarán sus reglas de acceso).

  - **Apagado**
  - **Apertura utilizando la matrícula** – La apertura de la puerta se producirá en el caso de que el registro en el directorio con la matrícula leída tenga actualmente el derecho de llegada o salida. La apertura de la puerta (respectivamente barrera, etc.) tras detectar la matrícula válida **funciona independientemente** de otros Modos de autenticación que están configurados en los Perfiles de acceso.
  - **Multi-factor con marca** – esta opción está disponible solo en el caso de activar la función beta Verificación de varios factores de matrículas. Enciende el bloqueo permanente del acceso y apaga de forma permanente el modo de autenticación mediante Bluetooth (WaveKey). Una vez leída la matrícula se le concederá al usuario con la matrícula leída una excepción temporal de 60 seg de duración y a la vez se activará durante este tiempo la función WaveKey. El acceso se concederá solo al usuario con la matrícula leída, el cual se autenticará dentro de los 60 segundos mediante otro modo de autenticación (WaveKey/código QR). A los usuarios con la excepción permanente se les permite el acceso durante todo el tiempo del bloqueo permanente de acceso, aunque solo durante 60 segundos desde el registro de la matrícula pueden autenticarse también mediante WaveKey.
    Cada siguiente matrícula admitida cancela la excepción temporal anterior y, en el caso de que exista el usuario con una nueva matrícula admitida, se le concederá la excepción temporal a este usuario.

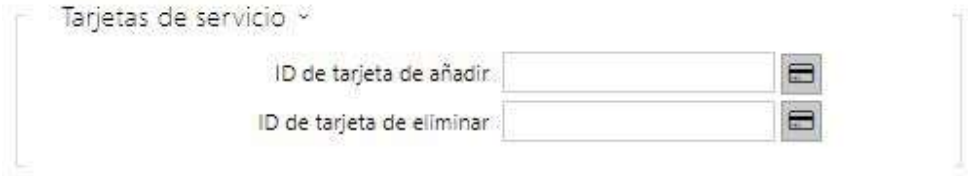
- **Tolerar desviación de caracteres** – determina si se tolera la desviación en la matrícula del vehículo reconocida. Es posible elegir entre la tolerancia cero, tolerancia desde el inicio, tolerancia desde el final o tolerancia tanto desde el inicio, como desde el final. A la hora de elegir la tolerancia de caracteres de ambos extremos se tolera primero, a la hora de la lectura de la matrícula, la desviación de caracteres desde el inicio, y si la matrícula no se reconoce, a la hora de la siguiente lectura se tolera la desviación desde el final.
- **Número de desviaciones de caracteres** – determina si se tolerara la desviación de uno o dos caracteres. La desviación de caracteres incumbe el principio y/o el final, según la configuración del parámetro **Tolerar la desviación de caracteres**. A la hora de la primera lectura de la matrícula el dispositivo no tolera ninguna desviación. Solo en el caso de que no reconozca la matrícula guardada en el directorio tolerará, a la hora de la siguiente lectura, la desviación de un carácter en las direcciones configuradas más arriba. En el caso de que aún así el dispositivo no identifique la matrícula en el directorio, el dispositivo tolerará, a la hora de la siguiente lectura, la desviación de dos caracteres.

El dispositivo permite utilizar las matrículas reconocidas de vehículos enviadas en el requerimiento HTTP mediante las cámaras de la empresa AXIS equipadas con la aplicación adicional VaxALPR a api/lpr/licenseplate (ver Manual HTTP API para los intercomunicadores IP).

En el caso de que la función esté encendida, tras recibir el requerimiento HTTP válido se producirá el registro del suceso en el historial bajo el suceso LicensePlateRecognized. En el caso de que dentro del marco del requerimiento HTTP se envíe también una imagen (por ej. recorte de una fotografía o fotografía entera de la escena a la hora de detectar la matrícula), ésta se guardará. En la memoria del dispositivo están guardadas las últimas cinco fotografías que se pueden leer en el dispositivo mediante el requerimiento HTTP enviado a api/lpr/image y las cuales están disponibles en el sistema **2N Access Commander**.

Advertencia

- Con la restauración de software de la configuración de fábrica, o con la carga de una configuración diferente, no se realizarán cambios en la configuración del bloqueo de acceso. Solo la restauración de hardware de la configuración de fábrica mediante el botón Reset en el dispositivo establecerá la configuración inicial del parámetro.
- El relé de seguridad aumenta la protección de la instalación contra el uso no autorizado mediante el reset de hardware.



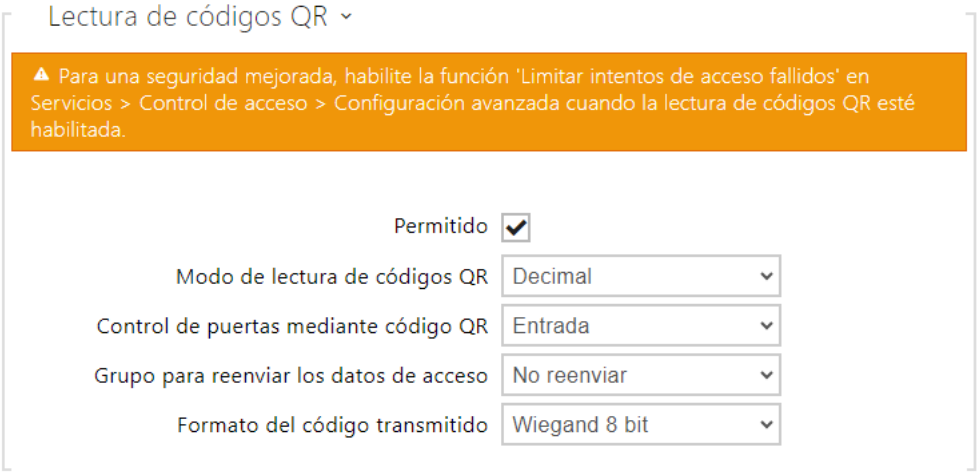
Para la administración de las tarjetas de usuarios sirven las llamadas tarjetas de añadidura y de eliminación. Al acercar la tarjeta de añadidura al lector se añadirán luego a la lista en el Directorio todas las siguientes tarjetas acercadas como usuario nuevo con la tarjeta de acceso asignada. En el dispositivo se crea automáticamente el usuario !Visitor #ID_de la tarjeta. Al acercar la tarjeta de eliminación al lector se borrarán luego de la lista en el Directorio todas las siguientes tarjetas acercadas y su usuario.

- **ID de la tarjeta de añadidura** – el ID de la tarjeta de servicio destinada para añadir tarjetas instaladas a la lista. El ID de la tarjeta es una secuencia de 6–32 caracteres del grupo de 0–9, A–F.
- **ID de la tarjeta de eliminación** – el ID de la tarjeta de servicio destinada para eliminar tarjetas instaladas de la lista. El ID de la tarjeta es una secuencia de 6–32 caracteres del grupo de 0–9, A–F.

Anti-Passback es una función de seguridad que impide el uso de la tarjeta de acceso o de otra autenticación para la entrada a la zona por segunda vez, sin que el usuario la haya abandonado anteriormente (es decir, la tarjeta no puede pasar atrás a otra persona que quiere entrar).

- **Modo** – selecciona el modo de la función Anti-Passback:

  - **Apagado** – la función está apagada por defecto, el usuario puede utilizar la tarjeta de acceso u otra autenticación para acceder a la entrada a la zona por segunda vez, sin que la haya abandonado anteriormente.
  - **Moderado** – la función está apagada por defecto, el usuario puede utilizar la tarjeta de acceso u otra autenticación para acceder a la entrada a la zona por segunda vez, sin que la haya abandonado anteriormente. En la sección Estado / Sucesos se creará un nuevo registro de tipo **UserAuthenticated** con parámetro *apbBroken*=***true***.
  - **Estricto** – el usuario no tiene permiso para utilizar la tarjeta de acceso u otra autenticación para el acceso a la entrada en la zona por segunda vez, sin que la haya abandonado anteriormente. En la sección Estado / Sucesos se creará un nuevo registro de tipo **UserRejected** con parámetro *apbBroken*=***true***.
- **Restricción del tiempo** – selecciona el tiempo de restricción del acceso para la función Anti-passback. Durante un tiempo elegido desde el último acceso con la autenticación determinada (con tarjeta, código, etc.) no es posible volver a utilizarla en la misma dirección.

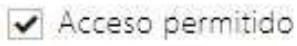


- **Permitido** – Enciende/apaga la lectura de códigos QR mediante la cámara del dispositivo. En el caso de que la lectura de códigos QR esté encendida es posible introducir los códigos PIN y los códigos individuales de los interruptores que contienen más de diez números mostrando el código QR a la cámara del dispositivo.
- **QR Code Reading Mode** – El dispositivo siempre almacena códigos decimales. En modo decimal, los códigos escaneados deben coincidir con los códigos de 4 a 15 dígitos almacenados en el dispositivo. En modo hexadecimal, los códigos se convierten a decimal después de la escaneo y se comparan con los códigos decimales almacenados, sin tener en cuenta los ceros iniciales. Rango hexadecimal aceptado: de 1000 a FFFFFFFF.
- **Control de la puerta mediante el código QR** – Habilita o prohíbe la abertura de la puerta a través de la lectura del código QR.
- **Grupo para reenviar datos de acceso** – le permite establecer un grupo al que se reenviarán todos los códigos de acceso de usuario recibidos.
- **Formato de los códigos transmitidos** – elección del formato de 4bit y 8bit (mayor fiabilidad) de los códigos transmitidos.

Precaución

- Para la correcta realización de la lectura de los códigos QR no utilice a la vez la función de protección de privacidad.
- Para aumentar la seguridad limite el número de accesos fallidos en el bloque Configuración avanzada más arriba.
- La función de la lectura de los códigos QR está disponible solo en los modelos con procesador ARTPEC-7 de la compañía Axis.

Solapa Reglas para la salida



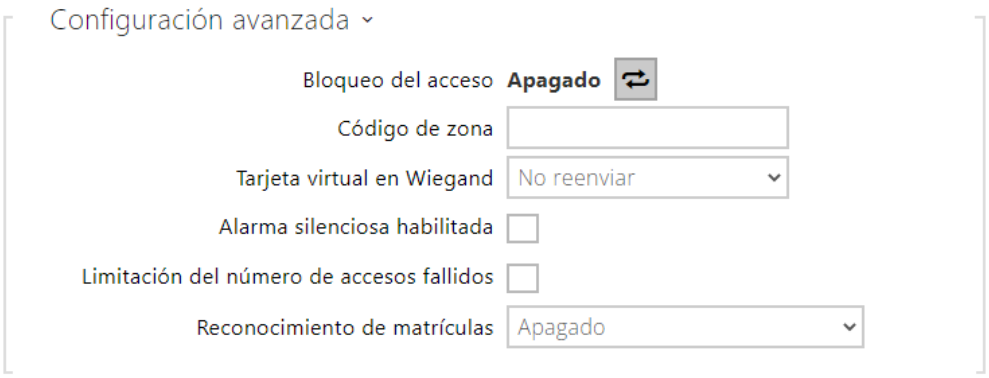
- **Acceso permitido** – permite cualquier acceso desde un lado determinado de la puerta (llegada, salida). En el caso de que el acceso no esté permitido, no es posible abrir la puerta desde este lado.

- **Perfil de tiempo** – ofrece la elección de uno o varios perfiles de tiempo a la vez que se aplicarán. La propia configuración de los perfiles de tiempo se puede realizar en la sección Directorio / Perfiles de tiempo.
  -  con la marca se configura la elección de los perfiles de tiempo pre-definidos o la configuración manual del perfil de tiempo para el elemento determinado.
- **Forma de la autenticación** – configura la forma de la autenticación (Bluetooth, huella dactilar, tarjeta de acceso, código numérico) durante el período de validez del perfil de tiempo en esta línea, incluida la posibilidad de autenticación múltiple para aumentar la seguridad. Con la opción 'Acceso denegado' se puede prohibir totalmente el acceso.
- **Código de zona** – permite el código de zona para la combinación del perfil de tiempo y la forma de autenticación en esta línea. El código de zona se puede utilizar luego en lugar del código PIN del usuario.

- **Botón REX** – habilita la función del botón de salida para el perfil de tiempo determinado. La entrada asignada al botón de salida se configura en la sección Hardware / Puerta, solapa Puerta.

Aviso

- En el caso de que el perfil de tiempo no esté configurado, la forma de la autenticación es ignorado en la línea determinada.



- **Bloqueo del acceso** – muestra la configuración actual de acceso. Encendido/ Apagado.
- **Código de zona** – permite introducir el código numérico del interruptor. El código debe contener al menos dos caracteres, sin embargo, recomendamos utilizar al menos cuatro caracteres.
- **Tarjetas visuales en Wiegand** – permite elegir la salida Wiegand a la que se enviará el número de la tarjeta virtual del usuario tras su autenticación satisfactoria. Se puede utilizar con cualquier manera de autenticación, incluidos los códigos, huellas dactilares, etc.
- **Habilitar alarma silenciosa** – a cada código de acceso está asignado un código virtual que es mayor por un uno que el de acceso y está destinado para activar el alarma silenciosa. Por ejemplo, si el código de acceso es 0000, el código para activar el alarma silenciosa es 0001. La longitud del código debe conservarse, lo que significa que por ejemplo para el código de acceso 9999 el alarma silenciosa es 0000, etc. La acción ejecutada para el alarma silenciosa se puede configurar en la sección para la automatización.

Aviso

- En el caso de que el usuario utilice la autenticación para activar el alarma silenciosa y el alarma silenciosa no está permitida, su acceso se denegará y el alarma no se activará.

- **Limitación del número de accesos fallidos** – permite limitar el número de intentos fallidos de autenticación. Tras cinco intentos fallidos de acceso (código numérico

incorrecto, tarjeta no válida, etc.) se bloqueará el módulo de acceso durante treinta segundos, incluso en el caso de que la autenticación haya sido válida.

- **Reconocimiento de matrículas** – elige el escenario para el reconocimiento de la matrícula del vehículo.

  Aviso

  - Para la función correcta es recomendable que cada matrícula esté asignada a un registro en el directorio. En el caso de matrículas introducidas de forma múltiple sucede la situación que no se puede asignar de forma inequívoca un registro en el directorio que tenga configurada la matrícula (se selecciona el primer registro que tiene configurada la matrícula correspondiente y se aplicarán sus reglas de acceso).

  - **Apagado**
  - **Apertura utilizando la matrícula** – La apertura de la puerta se producirá en el caso de que el registro en el directorio con la matrícula leída tenga actualmente el derecho de llegada o salida. La apertura de la puerta (respectivamente barrera, etc.) tras detectar la matrícula válida **funciona independientemente** de otros Modos de autenticación que están configurados en los Perfiles de acceso.
  - **Multi-factor con marca** – esta opción está disponible solo en el caso de activar la función beta Verificación de varios factores de matrículas. Enciende el bloqueo permanente del acceso y apaga de forma permanente el modo de autenticación mediante Bluetooth (WaveKey). Una vez leída la matrícula se le concederá al usuario con la matrícula leída una excepción temporal de 60 seg de duración y a la vez se activará durante este tiempo la función WaveKey. El acceso se concederá solo al usuario con la matrícula leída, el cual se autenticará dentro de los 60 segundos mediante otro modo de autenticación (WaveKey/código QR). A los usuarios con la excepción permanente se les permite el acceso durante todo el tiempo del bloqueo permanente de acceso, aunque solo durante 60 segundos desde el registro de la matrícula pueden autenticarse también mediante WaveKey.
    Cada siguiente matrícula admitida cancela la excepción temporal anterior y, en el caso de que exista el usuario con una nueva matrícula admitida, se le concederá la excepción temporal a este usuario.
- **Tolerar desviación de caracteres** – determina si se tolera la desviación en la matrícula del vehículo reconocida. Es posible elegir entre la tolerancia cero, tolerancia desde el inicio, tolerancia desde el final o tolerancia tanto desde el inicio, como desde el final. A la hora de elegir la tolerancia de caracteres de ambos extremos se tolera primero, a la hora de la lectura de la matrícula, la desviación de caracteres desde el inicio, y si la matrícula no se reconoce, a la hora de la siguiente lectura se tolera la desviación desde el final.
- **Número de desviaciones de caracteres** – determina si se tolerara la desviación de uno o dos caracteres. La desviación de caracteres incumbe el principio y/o el final, según la configuración del parámetro **Tolerar la desviación de caracteres**. A la hora de la primera lectura de la matrícula el dispositivo no tolera ninguna desviación. Solo en el caso de que no reconozca la matrícula guardada en el directorio tolerará, a la hora de la siguiente

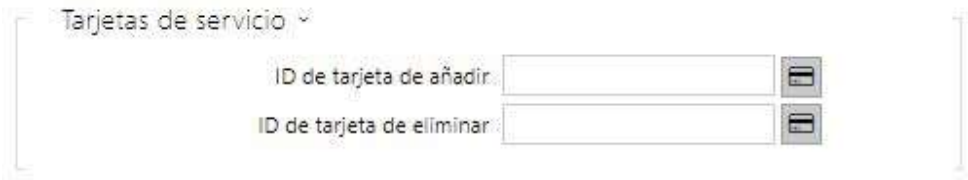
lectura, la desviación de un carácter en las direcciones configuradas más arriba. En el caso de que aún así el dispositivo no identifique la matrícula en el directorio, el dispositivo tolerará, a la hora de la siguiente lectura, la desviación de dos caracteres.

El dispositivo permite utilizar las matrículas reconocidas de vehículos enviadas en el requerimiento HTTP mediante las cámaras de la empresa AXIS equipadas con la aplicación adicional VaxALPR a api/lpr/licenseplate (ver Manual HTTP API para los intercomunicadores IP).

En el caso de que la función esté encendida, tras recibir el requerimiento HTTP válido se producirá el registro del suceso en el historial bajo el suceso LicensePlateRecognized. En el caso de que dentro del marco del requerimiento HTTP se envíe también una imagen (por ej. recorte de una fotografía o fotografía entera de la escena a la hora de detectar la matrícula), ésta se guardará. En la memoria del dispositivo están guardadas las últimas cinco fotografías que se pueden leer en el dispositivo mediante el requerimiento HTTP enviado a api/lpr/image y las cuales están disponibles en el sistema **2N Access Commander**.

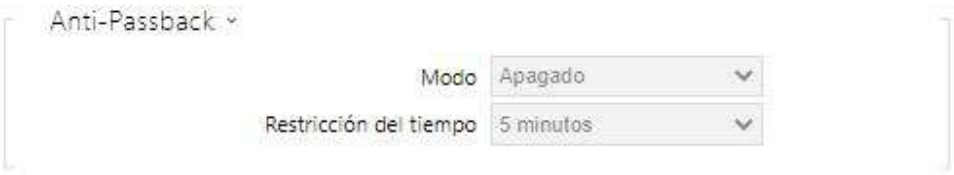
Advertencia

- Con la restauración de software de la configuración de fábrica, o con la carga de una configuración diferente, no se realizarán cambios en la configuración del bloqueo de acceso. Solo la restauración de hardware de la configuración de fábrica mediante el botón Reset en el dispositivo establecerá la configuración inicial del parámetro.
  - El relé de seguridad aumenta la protección de la instalación contra el uso no autorizado mediante el reset de hardware.



Para la administración de las tarjetas de usuarios sirven las llamadas tarjetas de añadidura y de eliminación. Al acercar la tarjeta de añadidura al lector se añadirán luego a la lista en el Directorio todas las siguientes tarjetas acercadas como usuario nuevo con la tarjeta de acceso asignada. En el dispositivo se crea automáticamente el usuario !Visitor #ID_de la tarjeta. Al acercar la tarjeta de eliminación al lector se borrarán luego de la lista en el Directorio todas las siguientes tarjetas acercadas y su usuario.

- **ID de la tarjeta de añadidura** – el ID de la tarjeta de servicio destinada para añadir tarjetas instaladas a la lista. El ID de la tarjeta es una secuencia de 6–32 caracteres del grupo de 0–9, A–F.
- **ID de la tarjeta de eliminación** – el ID de la tarjeta de servicio destinada para eliminar tarjetas instaladas de la lista. El ID de la tarjeta es una secuencia de 6–32 caracteres del grupo de 0–9, A–F.



Anti-Passback es una función de seguridad que impide el uso de la tarjeta de acceso o de otra autenticación para la entrada a la zona por segunda vez, sin que el usuario la haya abandonado anteriormente (es decir, la tarjeta no puede pasar atrás a otra persona que quiere entrar).

- **Modo** – selecciona el modo de la función Anti-Passback:
  - **Apagado** – la función está apagada por defecto, el usuario puede utilizar la tarjeta de acceso u otra autenticación para acceder a la entrada a la zona por segunda vez, sin que la haya abandonado anteriormente.
  - **Moderado** – la función está apagada por defecto, el usuario puede utilizar la tarjeta de acceso u otra autenticación para acceder a la entrada a la zona por segunda vez, sin que la haya abandonado anteriormente. En la sección Estado / Sucesos se creará un nuevo registro de tipo **UserAuthenticated** con parámetro *apbBroken*=***true***.
  - **Estricto** – el usuario no tiene permiso para utilizar la tarjeta de acceso u otra autenticación para el acceso a la entrada en la zona por segunda vez, sin que la haya abandonado anteriormente. En la sección Estado / Sucesos se creará un nuevo registro de tipo **UserRejected** con parámetro *apbBroken*=***true***.
- **Restricción del tiempo** – selecciona el tiempo de restricción del acceso para la función Anti-passback. Durante un tiempo elegido desde el último acceso con la autenticación determinada (con tarjeta, código, etc.) no es posible volver a utilizarla en la misma dirección.

Solapa PICard

La tecnología 2N PICard sirve para codificar los datos de inicio de sesión en las tarjetas de acceso. Para poder leer los datos de inicio de sesión los dispositivos 2N necesitan el acceso a las claves correspondientes, las cuales genera la aplicación 2N PICard Commander. A estas se pueden importar luego a 2N Access Commander, el cual asegurará su distribución a todos los dispositivos 2N compatibles.

> **Aviso**
>
> - Los dispositivos, en los cuales se pueden leer las tarjetas con la tecnología PICard, están especificados en el Manual de configuración 2N PICard Commander.

- **Descripción** – nombre para la clave de codificación creada.
- **Hash** – indentificador numérico del proyecto.
- **Cargar llaves PICard** – al seleccionar el archivo con las llaves y al introducir la contraseña válida se cargará la llave PICard.
- **Borrar llaves PICard** – borrará las llaves PICard cargadas.

Solapa WaveKey

Los **intercomunicadores 2N IP** equipados con módulo Bluetooth permiten autenticar al usuario mediante la aplicación móvil **2N Mobile Key** disponible para los dispositivos con los sistemas operativos iOS 12 y superiores (teléfonos iPhone 4s y superiores) event. Android 6.0 Marshmallow y superiores (teléfonos con soporte de Bluetooth 4.0 Smart).

Identificación del usuario (Auth ID)

La aplicación **2N Mobile Key** se autentica en la parte del intercomunicador mediante el identificador inconfundible – llamado **Auth ID**. Auth ID (número 128bit) es generado para cada usuario de forma aleatoria y mediante el proceso del llamado **emparejamiento** conectado con el usuario registrado en el intercomunicador y con su dispositivo móvil.

> **Nota**
>
> - Auth ID generado no puede ser guardado en varios dispositivos móviles a la vez. Es decir, Auth ID identifica de forma inconfundible al dispositivo móvil concreto (resp. a su usuario).

El valor de Auth ID se puede configurar en cada usuario y se puede modificar en la sección Mobile Key de la lista telefónica del intercomunicador. Auth ID se puede trasladar a otro usuario, event. copiar en otro intercomunicador. Tras borrar el valor del campo se bloqueará el acceso del usuario.

Claves de codificación y localización

La comunicación entre la aplicación **2N Mobile Key** y el intercomunicador está siempre cifrada. Sin el conocimiento de la clave de codificación la aplicación **2N Mobile Key** no puede autenticar al usuario. La clave de codificación primaria se genera automáticamente durante el primer

arranque del intercomunicador y se puede volver a generar manualmente en cualquier momento más adelante. La clave de codificación primaria se transfiere junto con Auth ID al dispositivo móvil durante el emparejamiento.

Las claves de codificación y el identificador de la localización se puede exportar del intercomunicador y luego importar a otros intercomunicadores. Los intercomunicadores con el mismo nombre de localización y con la misma llave de codificación forman las llamadas **localizaciones.** Dentro de una localización el dispositivo móvil se empareja solo una vez y se identifica con solo un único Auth ID (es decir, dentro de la localización se puede copiar Auth ID del usuario desde un intercomunicador a otro).

Emparejamiento

Con el proceso del llamado emparejamiento se entiende la transferencia de los datos de acceso del usuario a su dispositivo móvil personal. Los datos de acceso pueden estar guardados solo en un dispositivo móvil – es decir, el usuario no puede tener por ej. dos dispositivos móviles mediante los cuales se autentica. Sin embargo, en un dispositivo móvil pueden estar guardados los datos de acceso del usuario para varias localizaciones a la vez (es decir, el dispositivo móvil sirve como la clave para varias localizaciones a la vez).

El emparejamiento del usuario con el dispositivo móvil se puede activar en la lista telefónica del intercomunicador en la página del usuario correspondiente. El emparejamiento se puede realizar físicamente de forma local mediante el módulo USB bluetooth conectado al PC, event. de forma remota mediante el módulo bluetooth integrado en el intercomunicador. Ambas formas de emparejamiento dan el mismo resultado.

Durante el emparejamiento se transfieren al dispositivo móvil los siguientes datos:

- Identificador de la localización
- Claves de codificación de la localización
- Auth ID del usuario

Clave de codificación para el emparejamiento

En el modo de emparejamiento se utiliza, por razones de seguridad para proteger la comunicación, una clave distinta a la utilizada durante la comunicación tras el emparejamiento. Esta clave se genera automáticamente durante el primer arranque del intercomunicador y se puede volver a generar en cualquier momento.

Administración de las claves de codificación

El intercomunicador puede mantener vigentes hasta 4 claves de codificación – es decir, 1 clave primaria y hasta 3 claves secundarias. El dispositivo móvil puede utilizar para el cifrado de la comunicación cualquiera de estas 4 claves. Las claves de codificación están bajo pleno control del administrador del sistema. Por razones de seguridad es recomendable actualizar

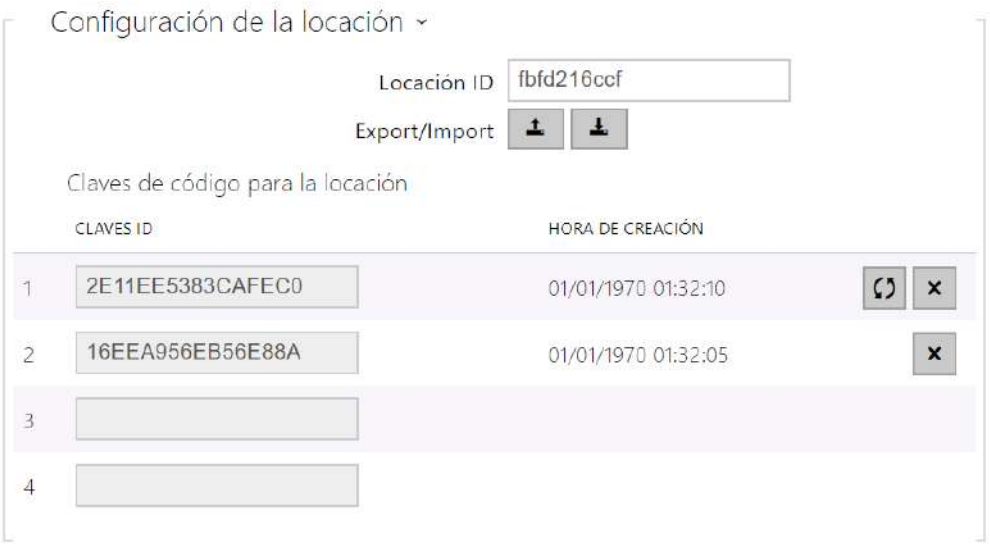
periódicamente las claves de codificación, event. en el caso de pérdida del dispositivo móvil o fuga de la configuración del intercomunicador.

> **Nota**
>
> - Durante el primer arranque del intercomunicador se generan automáticamente las claves de codificación y se guardan en el archivo de configuración del intercomunicador. Para una mayor seguridad recomendamos volver a generar manualmente estas claves de codificación antes del primer uso.

Es posible volver a generar en cualquier momento la clave primaria. La clave primaria original se luego convierte en la primera clave secundaria, la primera clave secundaria se convierte en la segunda secundaria, etc. Las claves secundarias se pueden eliminar en cualquier momento.

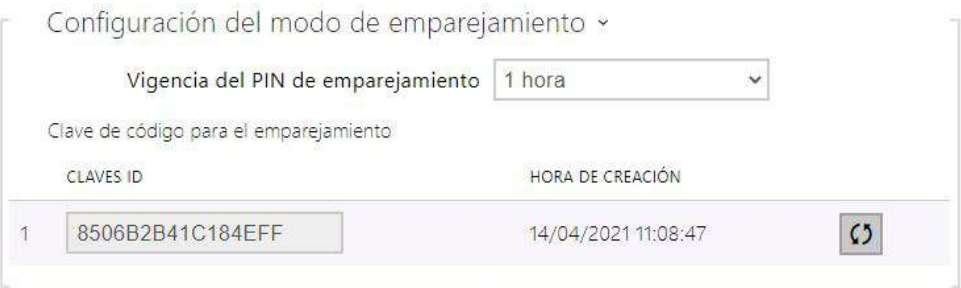
Tras eliminar la clave los usuarios de la aplicación **2N Mobile Key** que siguen utilizando esta clave no podrán realizar la autenticación en el caso de que antes de eliminar la clave no actualicen las claves de codificación en su dispositivo móvil. Las claves en el dispositivo móvil se actualizan cada vez que se utiliza la aplicación **2N Mobile Key**.

Lista de parámetros



- **ID de la localización** – identificador inconfundible de la localización dentro de la cuál está vigente el conjunto de las claves de codificación configuradas.
- **Botón Exportar** – exporta al identificador de la localización y las claves de codificación actuales al archivo. El archivo exportado se puede luego importar en otro dispositivo.
- **Botón Importar** – importa las localizaciones ID y las claves de codificación actuales del archivo exportado desde otro intercomunicador.
- **Botón Actualizar la llave primaria** – al generarse una nueva clave de codificación primaria se borrará la clave secundaria más antigua. Los usuarios de la aplicación **2N Mobile Key**que siguen utilizando esta clave no se podrán autenticar si antes de esta operación no actualicen las claves de codificación en su dispositivo móvil. Las claves en el dispositivo móvil se actualizan cada vez que se utiliza la aplicación **2N Mobile Key**.

- **Botón Borrar la clave primaria** – al eliminar la clave primaria los usuarios que utilizan esta clave no se podrán autenticar.
- **Botón Borrar la clave secundaria** – los usuarios de la aplicación **2N Mobile Key** que siguen utilizando esta clave no se podrán autenticar después del borrado de esta clave si antes de esta operación no actualicen las claves de codificación en su dispositivo móvil. Las claves en el dispositivo móvil se actualizan cada vez que se utiliza la aplicación **2N Mobile Key**.



- **Vigencia del PIN de emparejamiento** – periodo de vigencia del PIN de autorización para el emparejamiento del dispositivo móvil del usuario con el intercomunicador.

Consejo

- En el caso de notificar la pérdida del teléfono con los datos de acceso guardados recomendamos proceder de la siguiente manera:

1. Borre el valor Mobile Key Auth ID del usuario correspondiente – con ello se bloqueará el teléfono perdido y se impedirá su uso indebido.
2. Vuelva a generar la clave de codificación primaria (paso opcional) – con ello impedirá el posible uso indebido de la clave de codificación guardado en el dispositivo móvil.

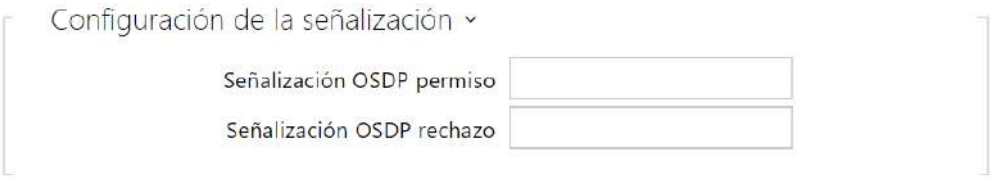
Advertencia

- Con el upgrade a la versión 2.30 se realiza el upgrade también en los módulos bluetooth. El downgrade a la versión 2.29 y anterior puede causar su falta de funcionalidad.

Solapa OSDP

El protocolo OSDP se encarga de la comunicación segura para el envío los datos de acceso, como es ID de la tarjeta de acceso o el código PIN entre el dispositivo OSDP conectado (panel de control, controlador de puerta) y el **intercomunicador 2N IP**. El objetivo es facilitar la activación

de la señalización en el **intercomunicador 2N IP**nen base de la respuesta de la parte opuesta a la definición enviada de la señalización de la tarjeta.



- **Señalización OSDP permiso** – cadena de definición para la señalización del permiso de acceso.
- **Señalización OSDP rechazo** – cadena de definición para la señalización del rechazo de acceso.

⚠
- En el caso de que en ambos parámetros esté introducida la misma definición se realizará la evaluación con las manifestaciones audiovisuales que se correspondan con el caso cuando para un acceso seguido por el otro se utilizase el acceso autorizado y no autorizado.

Ventana Mensajes recibidos sirve para obtener la cadena de definición. Al acercar la tarjeta de acceso al lector del intercomunicador 2N IP aparecerá la definición de la señalización OSDP del dispositivo de la parte opuesta para el acceso autorizado o no autorizado.

El mensaje recibido se muestra con el dato horario en el formato:

13:46:39] led(0,0,0,0,0,0,0,0,1,1,1,2,2)
13:46:39] buz(0,2,1,1,1)
13:46:42] led(0,0,0,0,0,0,0,0,1,1,1,1,1)
13:46:42] buz(0,1,0,0,0)

Como la cadena de definición se utilizará la parte (sin el dato horario), teniendo en cuenta de que su longitud no debe superar los 255 caracteres, por ej.: led(0,0,0,0,0,0,0,0,1,1,1,1,1) o buz(0,2,1,1,1). Al evaluar la coincidencia en la parte opuesta el dispositivo reacciona mediante la

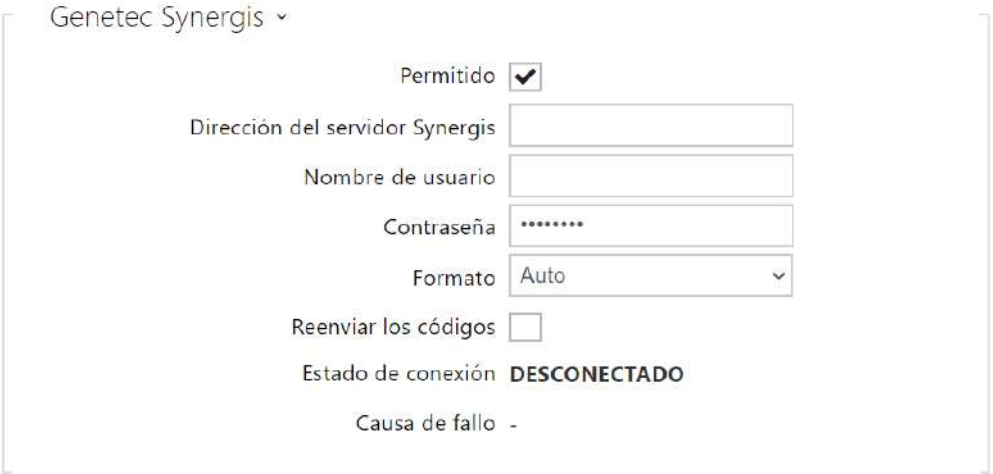
señalización correspondiente. Cualquier parte de la definición se puede sustituir por "*", esta parte se considerará como cualquier contenido del mensaje (por ej. de esta manera es posible lograr que la señalización se active al encenderse cualquier LED 0 en el dispositivo sin tener el cuenta los demás parámetros del mensaje).

- **Borrar el log** – borrará el registro del mensaje recibido.

Precaución

- Para el funcionamiento correcto es necesario tener el la sección Hardware / Módulos de ampliación para el lector de tarjetas y el teclado configurado el parámetro Puerta/No utilizado. El intercomunicador 2N IP confirmará la lectura de la tarjeta mediante el pitido de señalización, tras la evaluación el dispositivo reaccionará mediante la señalización correspondiente.

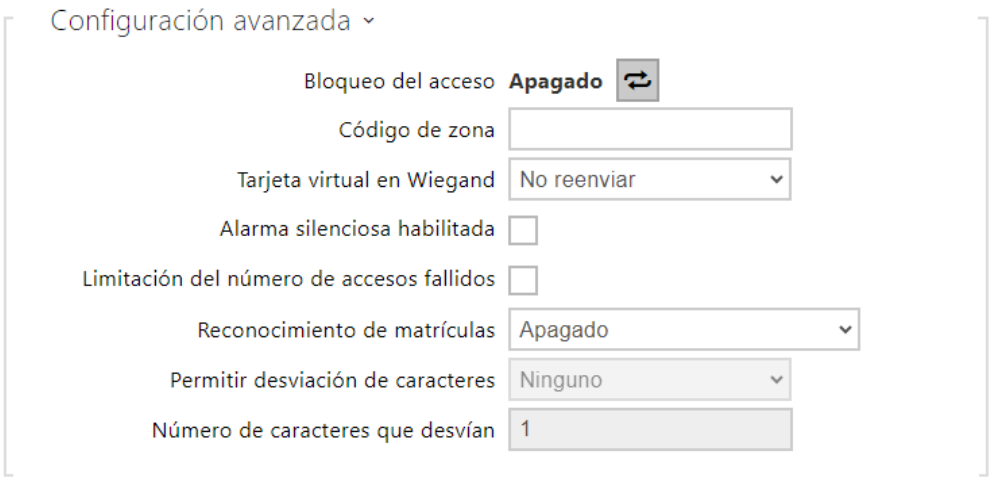
Solapa Integración con otros sistemas



- **Permitido** – permite la conexión con el sistema de seguridad Genetec Synergis externo.
- **Dirección del servidor Synergis** – dirección IP o nombre de dominio del servidor Synergis.
- **Nombre de usuario** – nombre de usuario utilizado durante la autenticación.
- **Contraseña** – contraseña utilizada durante la autenticación.
- **Formato** – configura el formato de la lectura de tarjetas para el envío del ID de la tarjeta al sistema Genetec Synergis.
- **Reenviar los códigos** – configura si se deben reenviar los códigos introducidos. Los códigos pueden contener como máximo 6 cifras y al final hay que pulsar la tecla de confirmación.
- **Estado de conexión** – muestra el estado actual de la conexión al servidor Synergis, event. descripción del estado de error.

- **Causa del fallo** – muestra la causa del fallo del último intento de conexión al servidor Synergis – muestra la última respuesta de error, por ej. La conexión al servidor ha fallado.

Solapa Avanzados



- **Modo de compatibilidad** – soporte de modos más antiguos de lectura de tarjetas. Desaconsejamos utilizarlo en combinación con las tarjetas PICard. En el caso de que este modo esté apagado, los números de tarjetas deberán coincidir totalmente para una autenticación satisfactoria.

5.4.2 Transmisión

Los **intercomunicadores 2N IP** ofrecen varias opciones del stream de audio y vídeo, ver la siguiente tabla:

Método de transmisión	Descripción
JPEG/HTTP	Descarga de las imágenes JPEG estáticas. Ver la solapa JPEG más abajo.
MJPEG/HTTP	Serie de imágenes JPEG consecutivas, método Server Push – multipart/x-mixed-replace. Ver la solapa JPEG más abajo.
RTSP + RTP/UDP	RTSP con streams RTP/UDP independientes de audio y vídeo. Compatible con audio (G.711) y vídeo (H.264, H.263, MPEG-2 y MJPEG). Ver la solapa RTSP más abajo.
RTP/RTSP	Túnel (encapsulamiento) RTP mediante el protocolo RTSP. Compatible con audio (G.711) y vídeo (H.264, H.263, MPEG-2 y MJPEG). Ver la solapa RTSP más abajo.
RTP/RTSP/HTTP	Túnel (encapsulamiento) del protocolo RTSP mediante HTTP. Compatible con audio (G.711) y vídeo (H.264, H.263, MPEG-2 y MJPEG). Ver la solapa RTSP más abajo.

Método de transmisión	Descripción
RTP/UDP-Multicast	Multicast no controlado de los paquetes RTP. Compatible solo con audio (G.711). Ver la solapa Multicast más abajo.

Explicación de los términos

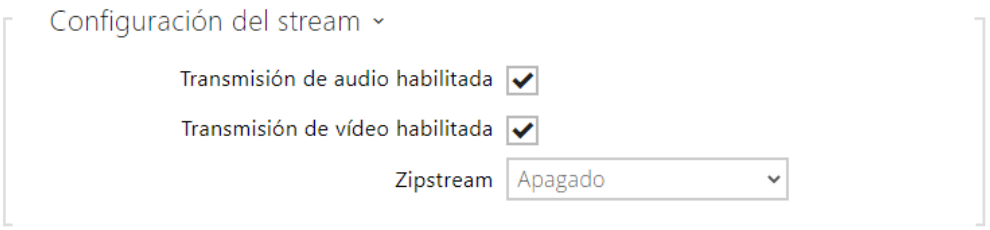
- **RTP (Real-Time Transport Protocol)** – protocolo que define el formato estándar de los paquetes para la transmisión de audio y vídeo en las redes IP. Los **intercomunicadores 2N IP** utilizan este protocolo para transmitir el stream de audio y vídeo. El protocolo de transporte para RTP suele ser directamente el protocolo UDP, sin embargo, puede ser también el protocolo RTSP, event. HTTP.
- **RTSP (Real-Time Streaming Protocol)** – protocolo de red para controlar los servidores de stream (controla el establecimiento, inicio y finalización del stream de audio y vídeo).
- **HTTP (Hypertext Transfer Protocol)** – protocolo que permite transmitir prácticamente cualquier contenido, utilizado sobre todo por los exploradores de internet para la comunicación con los servidores web. Los intercomunicadores **2N IP** permiten mediante el protocolo HTTP transmitir imágenes JPEG estáticas, event. stream MJPEG de manera llamada HTTP Server Push.
- **IP Multicast** – modo de envío de paquetes en las redes IP desde una fuente a varias estaciones a la vez. Los **intercomunicadores 2N IP** utilizan IP multicast para emitir y recibir el stream de audio.
- **ONVIF (Open Network Video Interface Forum)** – conjunto de especificaciones para la búsqueda, configuración y administración de las cámaras de vídeo en la red IP. Los **intercomunicadores 2N IP** son dispositivos compatibles con ONVIF e implementan plenamente el llamado ONVIF Profile T y Profile S .
- **JPEG** – método estándar del algoritmo de compresión con pérdida de la imagen.
- **MJPEG** – formato de codificación del stream de vídeo donde cada imagen se comprime por separado mediante el método JPEG. La codificación MJPEG produce vídeo de alta calidad a cambio de una mayor velocidad de transferencia en comparación con los métodos descritos a continuación.
- **H.263** – estándar para la compresión del stream de vídeo utilizado en las telecomunicaciones. A comparación con el método MJPEG utiliza la información diferencial entre las imágenes consecutivas y proporciona un grado mucho más alto de compresión a cambio del empeoramiento de la calidad del stream de vídeo.
- **H.263+** – igual que H.263, solo se trata de otro tipo de paquetización de bitstream.
- **MPEG-4 part 2** – estándar para la compresión del stream de vídeo utilizado más bien fuera de la rama de telecomunicaciones, aunque es muy a menudo compatible con las cámaras IP o sistemas de vídeo surveillance. En el caso de los intercomunicadores **2N IP** el grado de compresión y la calidad de imagen son comparables con el estándar H.263.
- **H.264** – estándar para la compresión del stream de vídeo. A diferencia con los métodos H.263 el formato MPEG-4 produce el stream de vídeo de la calidad de más o menos igual

con la mitad de la velocidad de transmisión. A esta forma de compresión la llamamos a veces también MPEG-4 part 10.
- **G.711** – uno de los estándares más comunes para la transmisión de audio en las redes de telecomunicación. Utiliza la frecuencia de muestreo 8 kHz y los datos se comprimen mediante la compresión logarítmica.

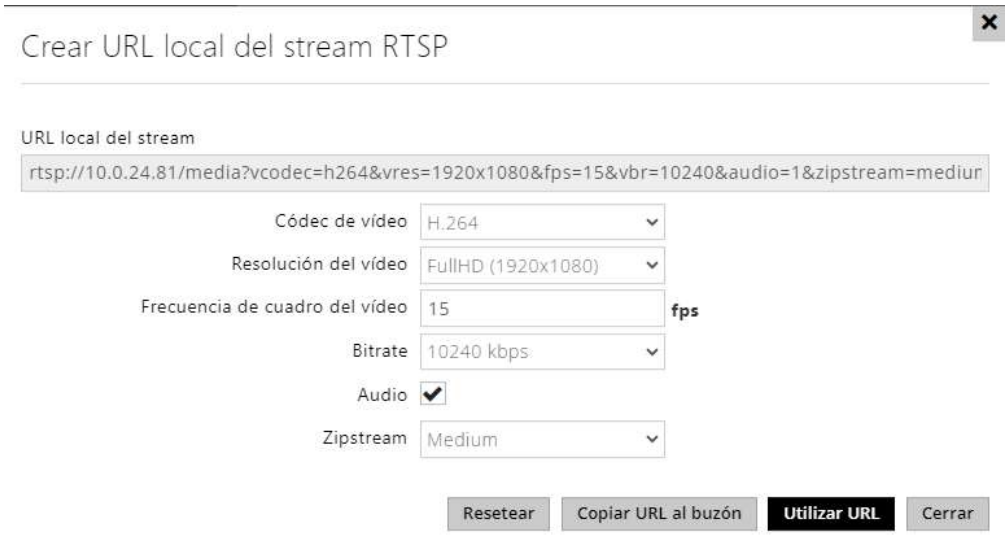
Solapa ONVIF/RTSP

Los intercomunicadores **2N IP** integran el servidor RTSP que se configura en esta solapa. El servidor RTSP permite realizar el stream tanto de audio, como de vídeo. Se puede elegir el modo de transferencia de datos, método y parámetros de compresión de vídeo y otros parámetros relacionados con el aseguramiento y calidad de transmisión.

- **Servidor RTSP habilitado** – habilita la función del servidor RTSP en el intercomunicador.



- **Transmisión de audio habilitada** – habilita la oferta del stream de audio a la hora de establecer la conexión con el servidor RTSP. En el caso de que el streaming de audio no esté habilitado, el audio no se transmitirá a través de los perfiles fijos de streaming, ni a través del URL local de stream.
- **Transmisión de vídeo habilitada** – habilita la oferta del stream de vídeo a la hora de establecer la conexión con el servidor RTSP. En el caso de que el streaming de vídeo no esté habilitado, el vídeo no se transmitirá a través de los perfiles fijos de streaming, ni a través del URL local de stream.
- **Zipstream** – elije el nivel inicial de compresión Zipstream (para H.264). AXIS Zipstream conserva todos los detalles forenses importantes que necesita y a la vez reduce las exigencias de la transferencia de datos y del almacenamiento en un promedio del 50 %. La compresión de Zipstream está disponible solo para el dispositivo con procesador Artpec-7 y para el códec H.264.



- **Códec de vídeo** – elección de los códec de vídeo disponibles.
- **Resolución del vídeo** – elección de las posibles resoluciones de la imagen.
- **Frecuencia de cuadro del vídeo** – configuración de la frecuencia de imágenes (de 1 hasta 30 fps, el valor máximo posible para el códec de vídeo MJPEG es de 15 fps).
- **Bitrate** – elección de la velocidad de transmisión disponible.
- **Audio** – permiso de la transmisión del sonido.
- **Zipstream** (disponible solo para H.264) – configuración del zipstream del URL local de stream, la cual tiene preferencia ante el valor introducido en la **Configuración del stream**.

El número de los streams RTSP está limitado a 4 strems simultáneos. Esta cantidad incluye también los streams de audio sin vídeo y el canal de audio de dirección opuesta hacia el intercomunicador.

Para la función correcta de ONVIF hay que crear al menos una cuenta de usuario y configurar el nivel correcto de acceso (según la especificación de ONVIF y de VMS utilizada). Sin la configuración de las cuentas de usuario estarán disponibles solo las funciones básicas.

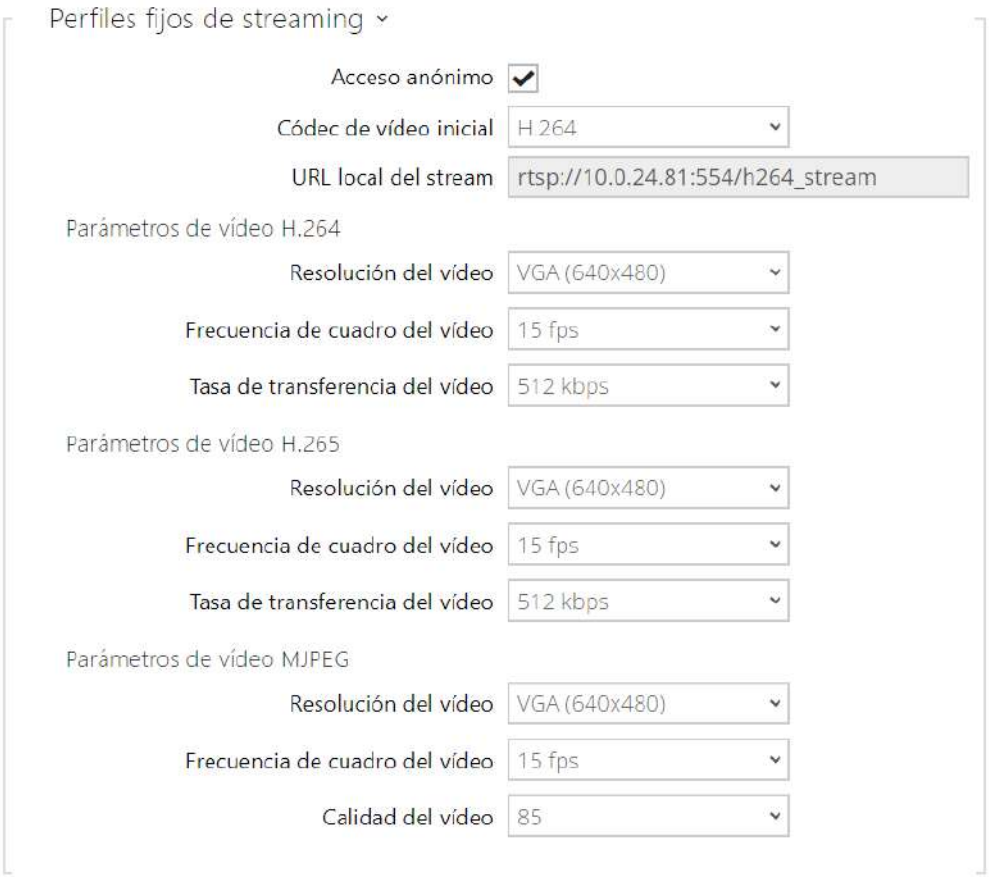
- **Nombre** – configura el nombre de usuario para acceder al servicio ONVIF.
- **Contraseña** – configura la contraseña para acceder al servicio ONVIF.
- **Nivel de acceso Onvif** – configura el nivel de acceso del usuario al servicio ONVIF (Anonymous, User, Operator, Administrator)

- **Dirección IP 1–4** – permite configurar hasta 4 direcciones IP autorizadas desde las cuales se puede iniciar la sesión en el servidor RTSP. Si ninguno de los cuatro campos está completado, se podrá utilizar cualquier dirección IP para conectarse.

- **Valor QoS DSCP** – configura la prioridad de los paquetes de audio y vídeo RTP en la red. El valor configurado se envía en el campo TOS (Type of Service) del encabezado del paquete IP.
- **Habilitación del modo UDP unicast** – habilita el modo de envío de datos del stream de audio y vídeo mediante el protocolo RTP/UDP. En el caso de que este modo esté apagado, los datos de stream de audio y vídeo se transmiten siempre solo mediante el protocolo RTP/RTSP.
- **Longitud máxima del paquete** – permite configurar el tamaño máximo de los paquetes de vídeo enviados mediante el protocolo RTP/UDP.
- **Puerto inicial para RTP** – configura el puerto local RTP inicial en el rango de longitud de 60 puertos utilizados para las transferencias de audio y vídeo. El valor inicial es 4800 (es decir, el rango utilizado es de 4800–4859).
- **Compensación Jitter** – configura la longitud de la memoria de compensación para compensar las irregularidades de los intervalos entre las llegadas de los paquetes de audio. La configuración de la memoria de compensación más duradera aumentará la resistencia de recepción a cambio de un mayor retardo de sonido.

Consejo

- FAQ: VLC player – Como ver el vídeo del intercomunicador 2N IP
- FAQ: VLC player – Como cargar el vídeo del intercomunicador 2N IP



Nota

- El servicio media 1 no soporta el perfil H.265.

- **Acceso anónimo** – habilita el acceso a los stream originales del servidor RTSP sin la autorización del usuario. En el caso de que esta casilla no esté marcada, el cliente RTSP debe autenticarse como uno de los usuarios del servicio ONVIF a la hora de acceder al servidor.
- **Códec de vídeo initial** – configuración inicial del códec de vídeo ofrecido durante el stream mediante RTSP.
- **Local Stream URL** – muestra la URL local del stream dependiendo de la elección del códe

- **Resolución del vídeo** – configuración de la resolución de imagen durante el stream mediante RTSP.
- **Frecuencia de cuadro del vídeo** – configuración la frecuencia de imágenes del vídeo durante el stream mediante RTSP.

- **Tasa de transferencia del vídeo** – configuración de la velocidad de transferencia durante el stream mediante RTSP.
- **Calidad del vídeo** – configuración del nivel de compresión de la imagen (solo MJPEG) dentro del rango de 10 (calidad baja, la velocidad de transferencia más baja) – 99 (la mayor calidad, la mayor velocidad de transferencia).

Solapa JPEG

En esta solapa se configura la manera más sencilla del stream de vídeo utilizando los métodos JPEG/HTTP y MJPEG/HTTP. Las imágenes se pueden descargar desde el intercomunicador mediante la pregunta GET por la dirección en el formato:

- http://dirección_ip_del intercomunicador/api/cámara/snapshot?width= **W**&height=**H**

o (para MJPEG, HTTP Server Push):

- http://dirección_ip_del intercomunicador/api/cámara/snapshot?width= **W**&height=**H**&fps=**N**

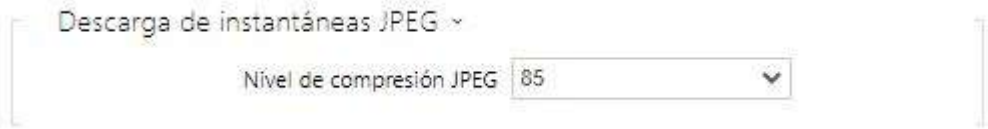
Los valores W y H especifican la resolución de la imagen (están soportadas las resoluciones 160 x 120, 320 x 240, 640 x 480, 176 x 144, 322 x 272, 352 x 288, 1280 x 960 – solo modelos equipados con cámara de 1 MPix). El valor N especifica el número de imágenes por segundo (se puede elegir entre valores desde 1 hasta 10).

En la siguiente tabla están expuestas las cantidades máximas simultáneas de los streams MJPEG/HTTP en los cuales aún no se produce la reducción de la frecuencia de las imágenes enviadas al utilizar el nivel inicial de compresión JPEG.

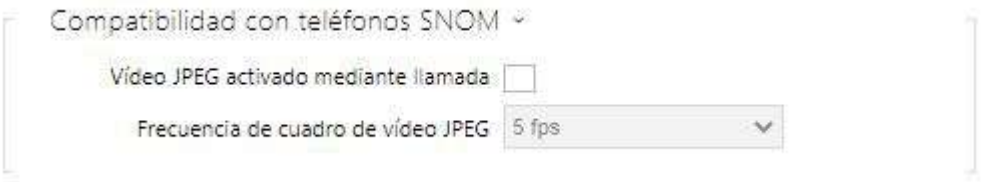
Tipo del intercomunicador	Resolución	Número de streams
Force/Vario	640 x 480	15
Force HD	640 x 480	15
Force HD	1280 x 960	3
Verso	640 x 480	8
Verso	1280 x 960	2

Nota

- *El método HTTP Server Push que contiene multipart/x-mixed-replace no está soportado por todos los exploradores de internet. Esta función la puede probar por en. en el explorador Firefox.*



- **Nivel de compresión JPEG** – configura el nivel de compresión JPEG dentro del rango (1–99). El valor recomendado es 85. Este parámetro afecta el tamaño y la calidad de la imagen.



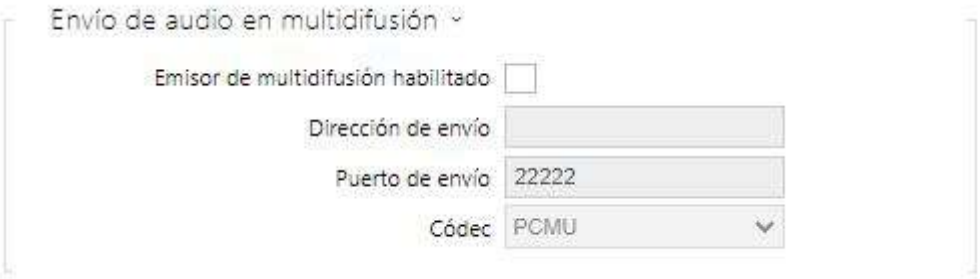
Algunos teléfonos IP (SNOM 820/870) no soportan las llamadas de vídeo, pero son capaces durante la llamada descargar y mostrar periódicamente las imágenes JPEG descargadas desde la dirección IP definida. Los intercomunicadores **2N IP** soportan esta función y usted la puede configurar en esta solapa.

- **Activar el vídeo JPEG mediante la llamada** – habilita la descarga de las imágenes de la cámara mediante los teléfonos Snom 820/870,D765,870 durante la llamada.
- **Frecuencia de imágenes del vídeo JPEG** – configura la frecuencia de imágenes, resp. el período de descarga de las imágenes de la cámara mediante los teléfonos Snom 820/870.

Solapa Multicast

Los intercomunicadores **2N IP** permiten realizar el stream de audio (señal desde el micrófono u otra entrada de audio del intercomunicador) mediante los paquetes RTP enviados a la dirección de multicast y a la vez recibir el stream de audio en el mismo formato y reproducirlo mediante el reproductor incorporado (event. otra salida de audio configurada). El stream de audio está codificado mediante el códec G.711 u-law.

- **Recepción de multicast habilitada** – habilita la recepción de paquetes RTP en la dirección de multicast y puerto elegidos. El stream de audio recibido se reproduce también durante una llamada activa, cuando se mezclan los audios de ambas fuentes.
- **Dirección IP de la fuente** – configura la dirección IP de multicast en la que se están esperando los paquetes RTP de multicast.
- **puerto de la fuente** – configura el puerto local para la recepción de los paquetes RTP de multicast.
- **Volumen** – permite configurar el volumen de reproducción del stream de audio recibido.
- **Códec** – permite configurar el códec de audio para decodificar los paquetes RTP entrantes. Se puede elegir entre PCMU, PCMA, G.722, L.16. Los códec de banda ancha G.722 y L16 están disponibles solo en los modelos de intercomunicadores determinados.



- **Transmisión de multicast habilitada** – habilita la transmisión de los paquetes RTP hacia la dirección y el puerto de multicast seleccionados.
- **Dirección IP de destino** – configura la dirección IP de multicast de destino hacia la que se transmite el stream de vídeo.
- **Puerto de destino** – configura el puerto de destino hacia el que se enviará el stream de audio.
- **Códec** – permite configurar el códec de audio para codificar los paquetes RTP salientes. Se puede elegir entre PCMU, PCMA, G.722, L.16. Los códec de banda ancha G.722 y L16 están disponibles solo en los modelos de intercomunicadores determinados.

Solapa Informacast

Los intercomunicadores **2N IP** soportan el protocolo InformaCast para el stream de audio. El protocolo InformaCast permite establecer un stream de audio (unicast/multicast RTP/UDP codificado por el códec G.711 U-law) entre el intercomunicador y el servidor de InformaCast, event.. otro cliente de InformaCast.

Tras habilitar este servicio se buscan automáticamente mediante el protocolo SLP los servidores InformaCast en la red local y el intercomunicador se registra en ellos de forma automática. El servidor InformaCast en el que está registrado el intercomunicador puede enviarle comandos para establecer el stream de audio:

- **Broadcast** – el intercomunicador recibe el stream de audio desde el servidor InformaCast y lo reproduce mediante el reproductor incorporado.
- **Capture** – el intercomunicador registra el audio mediante el micrófono interno y envía el stream de audio al servidor InformaCast.
- **Listen** – el intercomunicador recibe el stream de audio enviado por otro cliente de InformaCast.

El intercomunicador soporta el registro en hasta 4 servidores InformaCast a la vez y permite establecer hasta 6 streams de audio paralelos.

- **Servicio InformaCast habilitado** – habilita el servicio InformaCast por el lado del intercomunicador.

- **Comando Broadcast habilitado** – habilita el comando Broadcast que permite establecer el stream de audio enviado desde el servidor InformaCast al intercomunicador.
- **Comando Capture habilitado** – habilita el comando Capture que permite establecer el stream de audio enviado desde el intercomunicador al servidor InformaCast.
- **Comando Listen habilitado** – habilita el comando Listen que permite establecer el stream de audio enviado por otro cliente de InformaCast al intercomunicador.

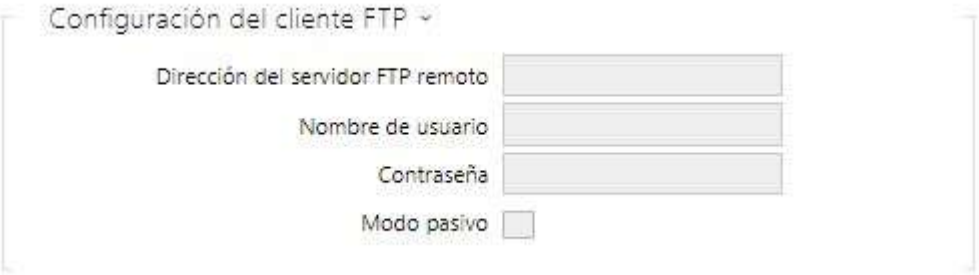
- **Comando Reboot habilitado** – habilita el comando Reboot que permite al servidor InformaCast reiniciar el intercomunicador.

Solapa FTP

En esta solapa se pueden configurar los datos de acceso al servidor FTP(S) en el que se pueden guardar imágenes de la cámara interna o externa conectada al intercomunicador. Las imágenes están siendo guardadas en el servidor FTP en formato JPEG en resolución seleccionada, el nombre de la imagen contiene la fecha y la hora de la creación de la imagen.

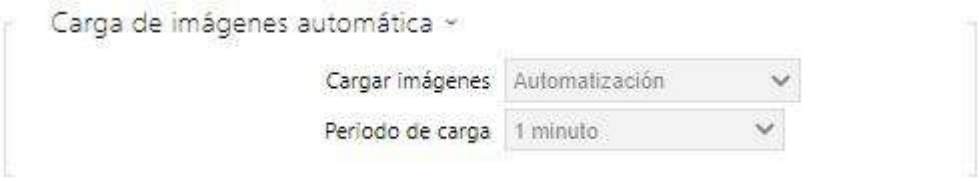
Las imágenes están siendo guardadas en el servidor FTP de forma automática (periódicamente o al empezar la llamada), event. mediante la automatización mediante la acción **Action.UploadSnapshotToFTP**.

- **Habilitación del cliente FTP** – habilita el servicio para el guardado de la imagen de la cámara en el servidor FTP.



- **Dirección del servidor FTP remoto** – configura la dirección del servidor FTP. La dirección tiene que estar en formato ftp://dirección_ip o ftps://dirección_ip.
- **Nombre de usuario** – configura el nombre del usuario del servidor FTP. Este parámetro es obligatorio en el caso de que el servidor FTP requiera la autenticación del usuario.
- **Contraseña** – configura la contraseña del usuario antes mencionado del servidor FTP.
- **Modo pasivo** – configura el modo pasivo de la transferencia (como un navegador web).

- **Directorio remoto** – configura el directorio en el servidor FTP en el que se guardarán las imágenes de la cámara.
- **Resolución de imágenes** – configura la resolución de las imágenes guardadas.



- **Envío de imágenes** – permite configurar el envío automático de las imágenes al servidor FTP al principio de la llamada, eventualmente, de forma periódica una vez transcurrido el tiempo establecido. El envío automático de la imagen se puede desactivar (opción Automatización), luego se pueden seguir enviando las imágenes mediante la acción de automatización Action.UploadSnapshotToFtp.
- **Período de envío** – configura el período del envío automático de las imágenes al FTP con la configuración del parámetro **Envío de imágenes** ajustado al valor **Periódicamente**. El período se puede configurar en varios pasos desde 10 segundos hasta 30 minutos.

Tras pulsar el botón **Guardar y realizar el test** se guarda la configuración actual del servidor FTP, se descarga la imagen de la cámara y se guarda en el servidor FTP. Durante el guardado de la imagen aparece en la ventana de arriba el transcurso detallado de la comunicación con el servidor FTP.

5.4.3 E-Mail

En el caso de que quiera informar al usuario sobre las llamadas perdidas, event. sobre todas las llamadas realizadas desde el intercomunicador, puede configurar los **intercomunicadores 2N IP** de manera que envíen tras cada llamada así un e-mail al usuario llamado. Puede configurar su propio asunto y el texto del mensaje de e-mail. En el caso de que su intercomunicador esté equipado con cámara, puede adjuntar al e-mail una o varias imágenes de la cámara captadas durante la llamada o sonido del tono.

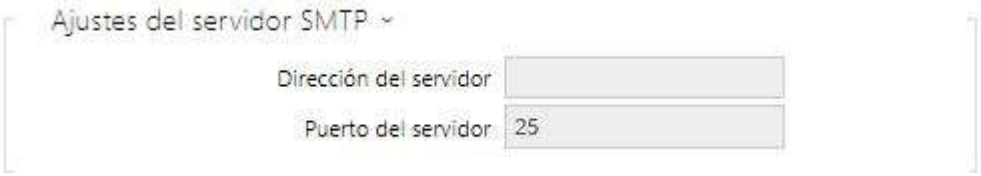
El intercomunicador envía e-mails a todos los usuarios que tienen en la lista de usuarios configurada su dirección de e-mail. En el caso de que deje en blanco el parámetro **e-mail** en la lista de usuarios, los e-mail se enviarán a la dirección de e-mail configurada inicialmente.

Los e-mails se pueden enviar también mediante la automatización utilizando la acción **Action.SendEmail**.

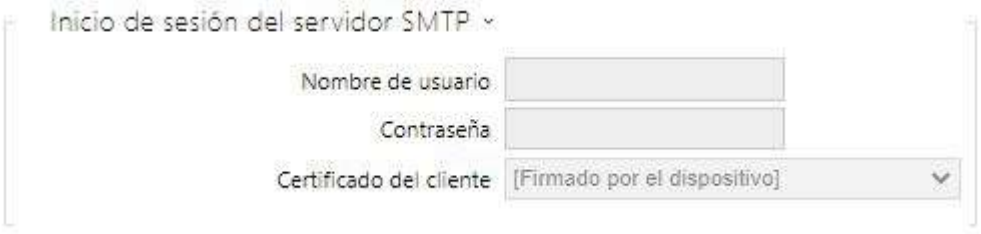
> **Nota**
>
> - *La función e-mail está disponible solo con la licencia Gold.*

Solapa SMTP

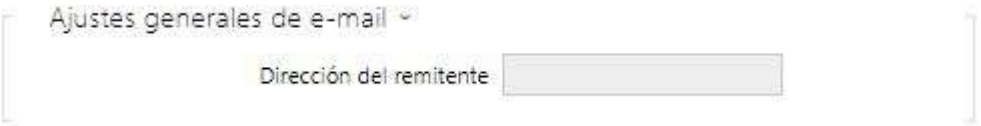
- **Habilitación del servicio SMTP** – permite habilitar o bloquear el servicio de envío de los e-mails desde el intercomunicador.



- **Dirección del servidor** – dirección del servidor SMTP a la que se enviarán los e-mails.
- **Puerto del servidor** – puerto del servidor SMTP. Modifique el valor solo en el cado de la configuración no estándar del servidor SMTP. El puerto SMTP está normalmente configurado al valor 25.

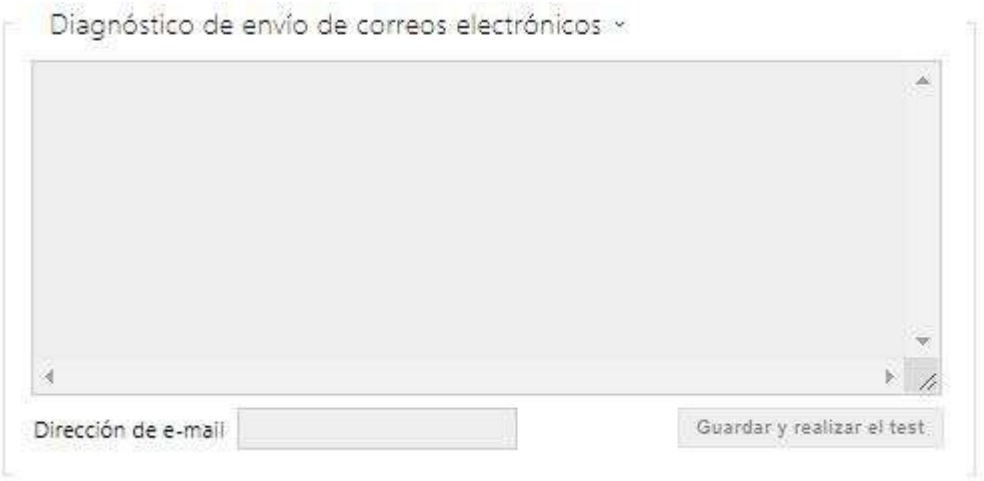


- **Nombre de usuario** – en el caso de que el servidor SMTP requiere la autorización, debe introducirse en este campo el nombre válido para el inicio de sesión en este servidor. En caso contrario puede dejar el campo en blanco.
- **Contraseña** – contraseña para el inicio de sesión en el servidor SMTP.
- **Certificado del cliente** – especifica el certificado de cliente y la clave privada, con la ayuda de los cuales se realiza el cifrado de la comunicación entre el intercomunicador y el servidor SMTP. Se puede elegir uno de los tres conjuntos de certificados y claves privadas, ver el capítulo Certificados, o conservar la configuración **SelfSigned** donde se utilizará el certificado generado automáticamente creado durante el primer arranque del intercomunicador.



- **Dirección del remitente** – configura la dirección del remitente para todos los e-mails enviados desde el dispositivo.

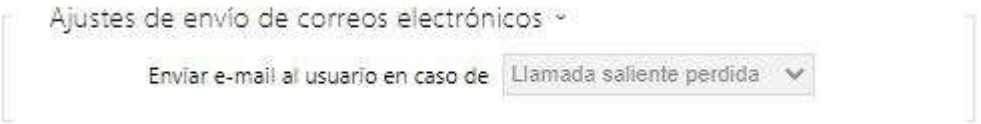
- **Entregan en** – configura el tiempo máximo durante el cual el intercomunicador intenta entregar el e-mail al servidor SMTP que no está disponible.



Mediante el botón **Guardar y realizar el test** se puede enviar el e-mail de prueba a la dirección introducida y de esta manera probar la funcionalidad de la configuración actual del envío de los e-mails. En el campo Dirección del e-mail de prueba introduzca la dirección de e-mail de destino y pulse el botón. Durante el envío del e-mail aparece en la ventana el estado actual del envío en base del cual se puede detectar un posible problema con la configuración del e-mail en el intercomunicador, event. mediante otro elemento de la red. Al e-mail se le adjunta una imagen de la cámara. Esto vale también pata los modelos sin cámaras donde se envía una imagen con N/A.

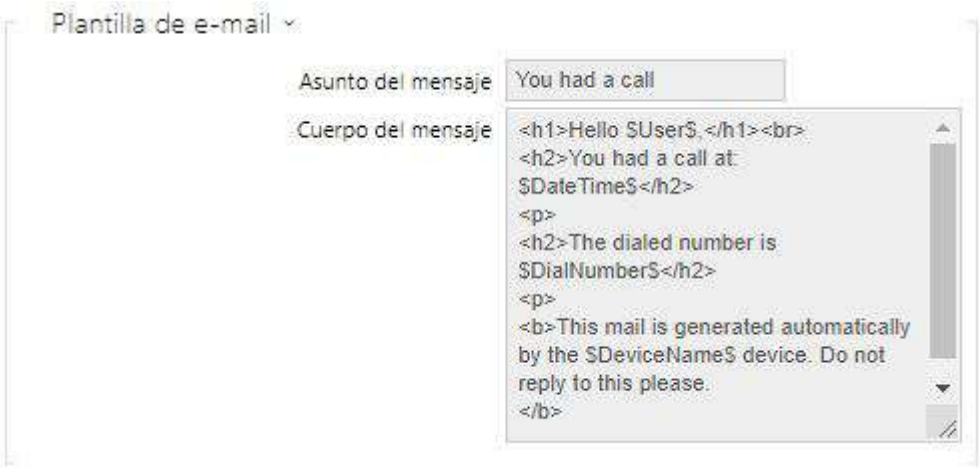
Solapa E-mail – llamada

En esta solapa se puede configurar el envío de los e-mails durante las llamadas salientes.



- **Enviar e-mail al usuario en caso de** – permite configurar el envío del e-mail al usuario en el caso de una llamada telefónica saliente o llamada saliente perdida. El e-mail se enviará tras finalizar la conexión. Se puede elegir entre las siguientes opciones:
  - **No enviar el e-mail** – los e-mails no se enviarán en el caso de llamadas salientes.
  - **Todas las llamadas salientes** – el e-mail se enviará después de cada llamada saliente.
  - **Llamada saliente perdida** – el e-mail se enviará tras cada llamada saliente no aceptada.

> **Nota**
>
> - Siempre es posible enviar los e-mails mediante la Automatización.



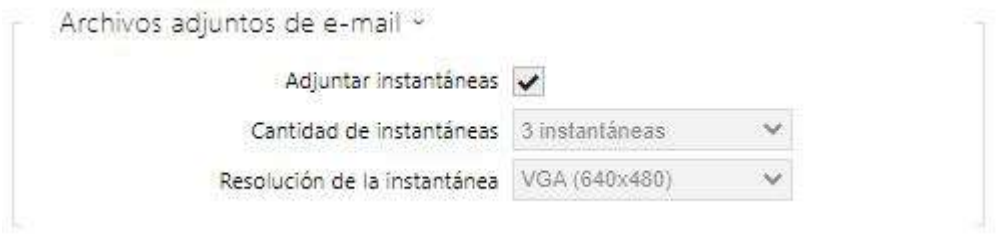
- **Asunto** – configura el asunto del mensaje de e-mail enviado.
- **Cuerpo del mensaje** – permite modificar el contenido del mensaje enviado. En el texto se pueden utilizar los símbolos de formateo del lenguaje HTML. Se pueden utilizar símbolos especiales para sustituir la fecha y hora, identificación del intercomunicador, número llamado. Se pueden utilizar símbolos especiales para la fecha y hora y para la identificación del intercomunicador. Estos símbolos serán sustituidos por los valores reales antes de enviar el mensaje. La lista de los símbolos sustitutivos que aparecen en la plantilla se muestra en la tabla de resumen al final de este capítulo.

Cuerpo del mensaje

```
<p>Hello <b>$User$</b>
</p>
<p>You had a call on: <b>$DateTime$</b>
  <br>The number dialed was: <b>$DialNumber$</b>
</p>
<p>This e-mail message is generated automatically by device: <b>$DeviceName$</b>. Do
not reply to this message.
</p>
```

Precaución

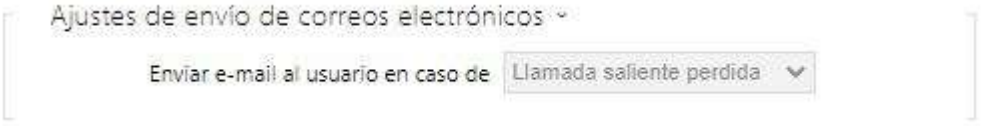
- Si la llamada se realiza a varios usuarios, el marcador de posición para el nombre del usuario llamado $Usuario$ está vacío.



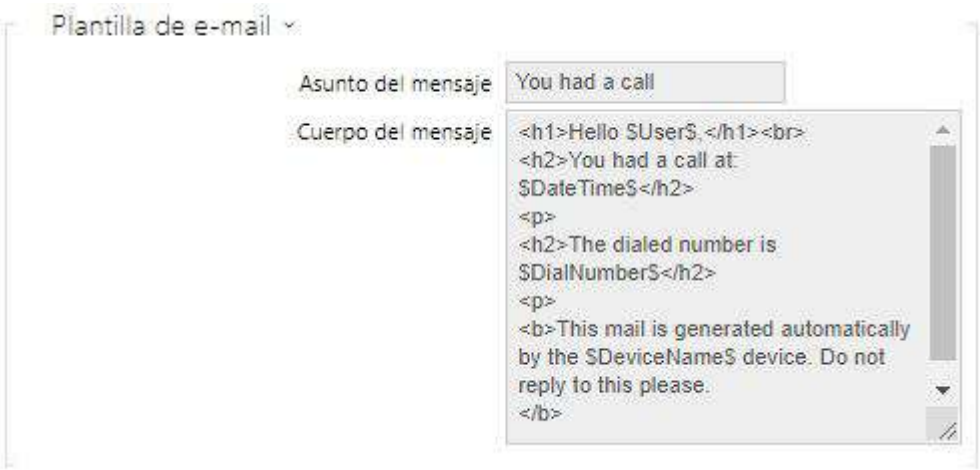
- **Adjuntar imágenes** – habilita el envío del archivo adjunto con una o varias imágenes de la cámara tomadas durante el sonido del tono o durante la llamada.
- **Número de imágenes adjuntas** – configura la cantidad de imágenes que se adjuntarán al e-mail.
- **Resolución de imágenes** – configura la resolución de las imágenes enviadas.

Solapa E-mail – acceso

En esta solapa se puede configurar el envío de los e-mails en el momento de acercar la tarjeta RFID al lector de tarjetas, identificación mediante el módulo Bluetooth o lector de huellas dactilares.



- **Enviar a la dirección de e-mail** – configuración de la dirección de e-mail del administrador.
- **Enviar un e-mail en caso de** – permite configurar el envío del e-mail. Se puede elegir entre las siguientes opciones:
  - **No enviar el e-mail** – el e-mail no se enviará.
  - **Todos los accesos** – el e-mail se enviará tras cada acceso registrado.
  - **Accesos denegados** – el e-mail se enviará solo en el caso de acceso denegado.



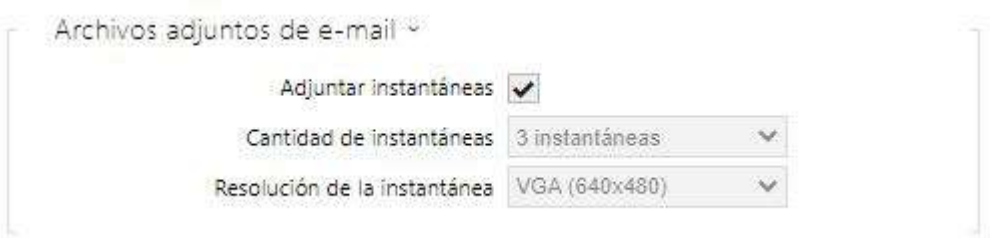
- **Asunto** – configura el asunto del mensaje de e-mail enviado.
- **Cuerpo del mensaje** – permite modificar el contenido del mensaje enviado. En el texto se pueden utilizar los símbolos de formateo del lenguaje HTML. Se pueden utilizar símbolos especiales para sustituir la fecha y hora, identificación del intercomunicador, número llamado. Se pueden utilizar símbolos especiales para la fecha y hora y para la identificación del intercomunicador. Estos símbolos serán sustituidos por los valores reales antes de enviar el mensaje. La lista de los símbolos sustitutivos que aparecen en la plantilla se muestra en la tabla de resumen al final de este capítulo.

Cuerpo del mensaje

```
<p>Hello,
</p>
<p>User <b>$User$</b> generated a new access event on device <b>$DeviceName$</b> (IP:
<b>$Ip4Address$</b>)
</p>
<ul>
  <li>Authentication Type: <b>$AuthIdType$</b>
  </li>
  <li>Authentication ID: <b>$AuthId$</b>
  </li>
  <li>Validity: <b>$AuthIdValid$</b>
  </li>
  <li>Reason: <b>$AuthIdReason$</b>
  </li>
  <li>Direction: <b>$AuthIdDirection$</b>
  </li>
  <li>Date/Time: <b>$DateTime$</b>
  </li>
</ul>
<p>This e-mail message is generated automatically by device: <b>$DeviceName$</b>. Do
not reply to this message.
</p>
```

Precaución

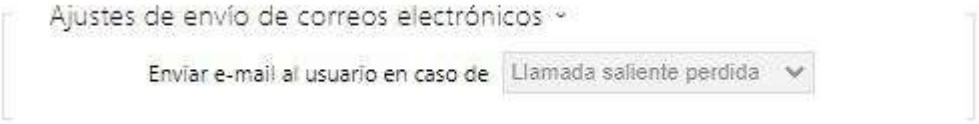
- Para los símbolos de sustitución $AuthIdType$ y $AuthIdValid$ es posible utilizar la síntaxis ampliada que sirve para reemplazar los valores incorporados, por ejemplo para el texto en checo: $AuthIdValid|Valid=válido|Invalid=no válido$
- En el valor no válido $AuthId$ se enmascara la primera mitad de ID, por ej.: ******11188, **********792d9044158891fa etc.
- En el valor válido $AuthId$ se enmascara todo ID ****.
- En el caso de que el valor del símbolo de sustitución no se encuentre en la cadena de sustituciones, se utilizará directamente.



- **Adjuntar imágenes** – habilita el envío del archivo adjunto con una o varias imágenes de la cámara tomadas durante el sonido del tono o durante la llamada.
- **Resolución de imágenes** – configura la resolución de las imágenes enviadas.

Solapa E-mail – suceso

En esta solapa se puede configurar el envío de los e-mail informativos en el momento cuando se produzca la pérdida de SIP, reinicio del dispositivo o activación del interruptor antisabotaje en el dispositivo.



Enviar a la dirección de e-mail – permite configurar el envío del e-mail. Se puede elegir entre las siguientes opciones:

- **Pérdida del registro SIP**
- **Reinicio del dispositivo**
- **Activación del interruptor antisabotaje**

Mensaje en el caso de pérdida de registro SIP – configuración del mensaje que se enviará a la dirección de e-mail determinado en el caso de la pérdida de registro SIP.

- **Asunto** – configura el asunto del mensaje de e-mail enviado.
- **Cuerpo del mensaje** – permite modificar el contenido del mensaje enviado. En el texto se pueden utilizar los símbolos de formateo del lenguaje HTML. Se pueden utilizar símbolos especiales para sustituir la fecha y hora, identificación del intercomunicador, número llamado. Se pueden utilizar símbolos especiales para la fecha y hora y para la identificación del intercomunicador. Estos símbolos serán sustituidos por los valores

reales antes de enviar el mensaje. La lista de los símbolos sustitutivos que aparecen en la plantilla se muestra en la tabla de resumen al final de este capítulo.

Cuerpo del mensaje

```
<p>Hello,
</p>
<p>SIP account <b>$SipAccountNumber$</b> of device <b>$DeviceName$</b> (IP:
<b>$Ip4Address$</b>) got unregistered on <b>$DateTime$</b>
</p>
<p>This e-mail message is generated automatically by device: <b>$DeviceName$</b>. Do
not reply to this message.
</p>
```

Precaución

- En el caso de que el valor del símbolo de sustitución no se encuentre en la cadena de sustituciones, se utilizará directamente.

Mensaje al reiniciarse el dispositivo – configuración del mensaje que se enviará a la dirección de e-mail determinada al reiniciarse el dispositivo.

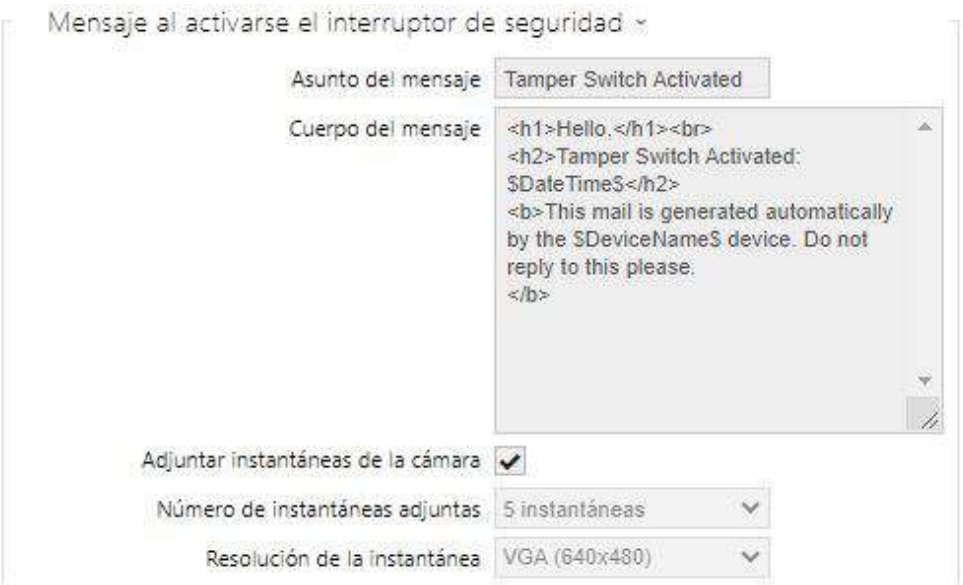
- **Asunto** – configura el asunto del mensaje de e-mail enviado.
- **Cuerpo del mensaje** – permite modificar el contenido del mensaje enviado. En el texto se pueden utilizar los símbolos de formateo del lenguaje HTML. Se pueden utilizar símbolos especiales para sustituir la fecha y hora, identificación del intercomunicador, número llamado. Se pueden utilizar símbolos especiales para la fecha y hora y para la identificación del intercomunicador. Estos símbolos serán sustituidos por los valores reales antes de enviar el mensaje. La lista de los símbolos sustitutivos que aparecen en la plantilla se muestra en la tabla de resumen al final de este capítulo.

Cuerpo del mensaje

```
<p>Hello,
</p>
<p>Device <b>$DeviceName$</b> (IP: <b>$Ip4Address$</b>) rebooted on <b>$DateTime$</b>
</p>
<ul>
  <li>Reason: <b>$RebootReason$</b>
  </li>
  <li>Uptime: <b>$UpTime$</b>
  </li>
  <li>Firmware version: <b>$SoftwareVersion$</b>
  </li>
  <li>Build date: <b>$BuildTime$</b>
  </li>
</ul>
<p>This e-mail message is generated automatically by device: <b>$DeviceName$</b>. Do
not reply to this message.
</p>
```

Precaución

- En el caso de que el valor del símbolo de sustitución no se encuentre en la cadena de sustituciones, se utilizará directamente.



Mensaje al activarse el interruptor antisabotaje – configuración del mensaje que se enviará a la dirección de e-mail determinada al activarse el interruptor antisabotaje.

- **Asunto** – configura el asunto del mensaje de e-mail enviado.
- **Cuerpo del mensaje** – permite modificar el contenido del mensaje enviado. En el texto se pueden utilizar los símbolos de formateo del lenguaje HTML. Se pueden utilizar símbolos especiales para sustituir la fecha y hora, identificación del intercomunicador, número llamado. Se pueden utilizar símbolos especiales para la fecha y hora y para la identificación del intercomunicador. Estos símbolos serán sustituidos por los valores reales antes de enviar el mensaje. La lista de marcadores de posición que se encuentran en la plantilla se muestra en la tabla de resumen al final de este capítulo.

- **Adjuntar imágenes** – habilita el envío del archivo adjunto con una o varias imágenes de la cámara tomadas durante el sonido del tono o durante la llamada.
- **Número de imágenes adjuntas** – configura la cantidad de imágenes que se adjuntarán al e-mail.
- **Resolución de imágenes** – configura la resolución de las imágenes enviadas.

Cuerpo del mensaje

```
<p>Hello,
</p>
<p>Tamper switch of device <b>$DeviceName$</b> (IP: <b>$Ip4Address$</b>) was
activated on <b>$DateTime$</b>
</p>
<p>This e-mail message is generated automatically by device: <b>$DeviceName$</b>. Do
not reply to this message.
</p>
```

Precaución

- En el caso de que el valor del símbolo de sustitución no se encuentre en la cadena de sustituciones, se utilizará directamente.

Precaución

- El nombre para el símbolo sustitutivo $DeviceName$ está directamente vinculado con el valor del parámetro *Nombre del dispositivo* en la sección Servicios / Servidor Web / Ajustes básicos Recomendamos utilizar un nombre que define claramente el dispositivo del que se trata.

Lista de símbolos de sustitución

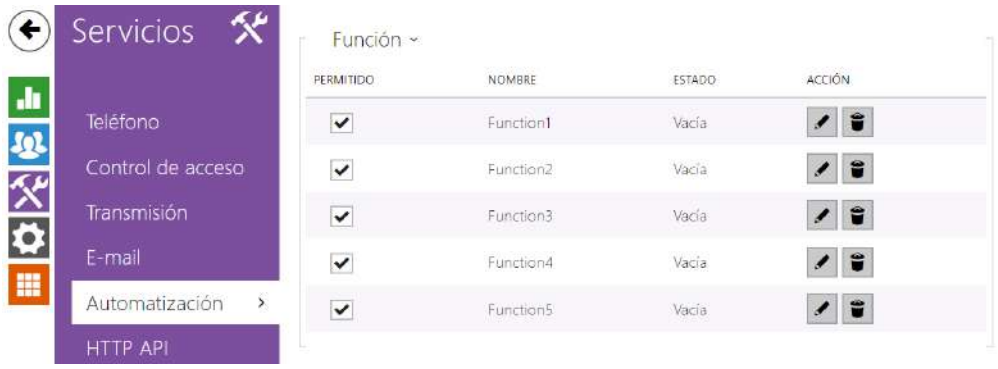
Aparición	Símbolo de sustitución	Descripción
Siempre	$DateTime$	fecha y hora actual
	$DeviceName$	nombre del dispositivo
	$Ip4Address$	dirección IP del dispositivo
	$SoftwareVersion$	versión del FW
	$BuildTime$	fecha y hora de ensamblaje
	$UpTime$	tiempo de operación del dispositivo
Dependiendo de cada caso en concreto	$User$	nombre de usuario
	$RebootReason$	motivo del reinicio
	$DialNumber$	número llamado, entrante o saliente
	$SipAccountNumber$	número de la cuenta SIP
	$AuthId$	ID de autenticación
	$AuthIdDirection$	dirección (salida/entrada)
	$AuthIdType$	tipo de certificación
	$AuthIdValid$	válido, no válido
	$AuthIdReason$	motivo del rechazo

Resumen de los símbolos de sustitución en los sucesos

Símbolo de sustitución / Función	E-mail del acceso	E-mail de la llamada	E-mail – perder el registro SIP	E-mail – reiniciar el dispositivo	E-mail – activación del interruptor antisabotaje	E-mail – envío de diagnósticos	Automatización
$DateTime$	*	*	*	*	*	*	*
$DeviceName$	*	*	*	*	*	*	*
$Ip4Address$	*	*	*	*	*	*	*
$SoftwareVersion$	*	*	*	*	*	*	*
$BuildTime$	*	*	*	*	*	*	*
$UpTime$	*	*	*	*	*	*	*
$User$	*	*				*	*
$RebootReason$				*			
$DialNumber$		*				• (enviará "E-Mail test")	CallStateChanged
$SipAccountNumber$			*				
$AuthId$	*						CardEntered, CardHeld
$AuthIdDirection$	*						CardEntered, CardHeld

Símbolo de sustitución / Función	E-mail del acceso	E-mail de la llamada	E-mail – perder el registro SIP	E-mail – reiniciar el dispositivo	E-mail – activación del interruptor antisabotaje	E-mail – envío de diagnósticos	Automatización
$AuthIdType$	*						CardEntered, CardHeld
$AuthIdValid$	*						CardEntered, CardHeld
$AuthIdReason$	*						

5.4.4 Automatización



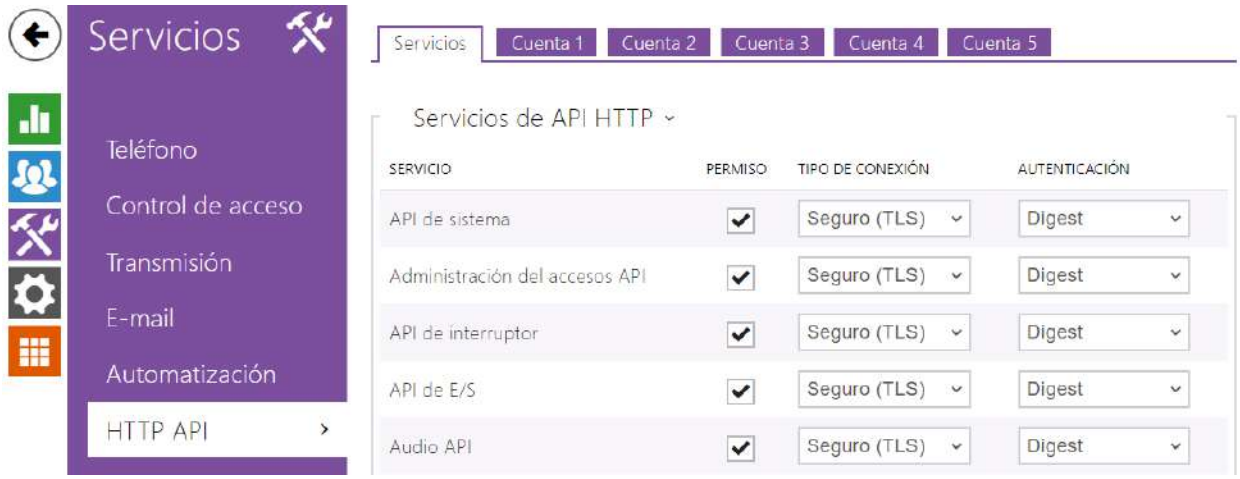
Los **intercomunicadores 2N IP** proporcionan las posibilidades muy flexibles de configuración según los diversos requisitos del usuarios. Existen situaciones cuando la envergadura habitual de la configuración (por ej. configuración del comportamiento de los interruptores o llamadas) no es suficiente y para estos casos los **intercomunicadores 2N IP** proporcionan una interfaz programable especial **Automation**. El uso típico de **Automation** está en las aplicaciones que requieren una conexión más compleja con los sistemas de terceros.

La descripción detallada de la función y configuración de **Automation** está disponible en el manual de Configuración Automation.

> **Nota**
>
> - *La función de la automatización está disponible solo con la licencia Gold.*

5.4.5 HTTP API

HTTP API es una interfaz de aplicación para controlar las funciones determinadas del intercomunicador mediante el protocolo **HTTP**. Esta interfaz permite integrar de forma sencilla los **intercomunicadores 2N IP** con productos de terceros, por ej. sistemas de automatización doméstica, sistemas de seguridad y de monitorización de edificios etc.



Services

HTTP API está dividido según su función entre los siguientes servicios:

- **API de sistema** – permite cambios de configuración, obtención del estado y upgrade del intercomunicador.
- **Administración del accesos API** – permite controlar los accesos y la forma de verificar la autenticación del usuario.
- **API de interruptor** – permite controlar y vigilar el estado de los interruptores, por ej. apertura de las cerraduras de puertas, etc.
- **API de E/S** – permite controlar y vigilar las entradas y salidas lógicas del intercomunicador.
- **Audio API** – permite controlar la reproducción de los sonidos y monitorear el micrófono del dispositivo.
- **API de cámara** – permite controlar y vigilar la imagen de la cámara.
- **API de pantalla** – permite controlar la pantalla y visualizar la información de usuario en la pantalla.
- **API de e-mail** – permite enviar desde el dispositivo los e-mails de usuario.
- **API de teléfono/llamada** – permite controlar y vigilar las llamadas entrantes y salientes.
- **API de registro** – permite leer los sucesos registrados en el dispositivo.
- **API de automatización** – permite configurar la comunicación Secure/Unsecure y los requisitos de autorización.

para cada servicio se puede configurar un protocolo de transporte (**HTTP** o **HTTPS**) y la forma de autenticación (**ninguna**, **Basic** o **Digest**). En la configuración **HTTP API** se puede crear hasta

cinco cuentas de usuario (con nombre y contraseña propios) con la posibilidad de controlar detalladamente el acceso a cada uno de los servicios y funciones.

En cada servicio se puede configurar la forma requerida de autenticación de las solicitudes enviadas al intercomunicador. En el caso de que no se realice la autenticación, la solicitud es rechazada. Las solicitudes están siendo autenticadas mediante el protocolo de autenticación estándar descrito en **RFC-2617**. Se pueden elegir estos tres métodos de autenticación:

- **Ninguna** – el servicio no requiere ninguna autenticación. En este caso el servicio está totalmente desprotegido en la red local.
- **Basic** – el servicio requiere autenticación Basic según **RFC-2617**. En este caso el servicio requiere la contraseña, sin embargo, ésta está siendo enviada en formato abierto. Recomendamos combinar esta opción con el protocolo **HTTPS**, si es posible.
- **Digest** – el servicio requiere autenticación Digest según **RFC-2617**. Esta variante es inicial y es la más segura de los métodos mencionados anteriormente.

La descripción detallada de la función y de la configuración de HTTP API está disponible en el manual HTTP API.

Consejo

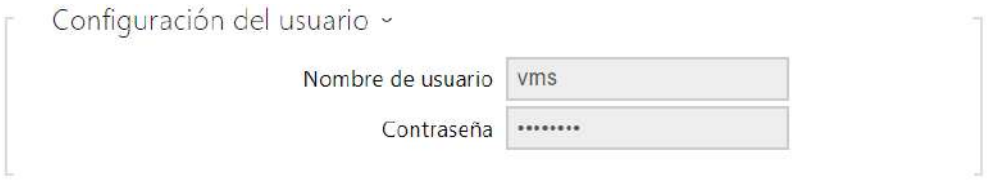
- Para la función Video Preview en el teléfono Gigaset Maxwell 10 es necesario en la solapa **HTTP API** junto al elemento **Camera API** configurar el **Tipo de conexión = No asegurada (TCP)** y **Autenticación = Ninguna**.

Cuenta 1–2

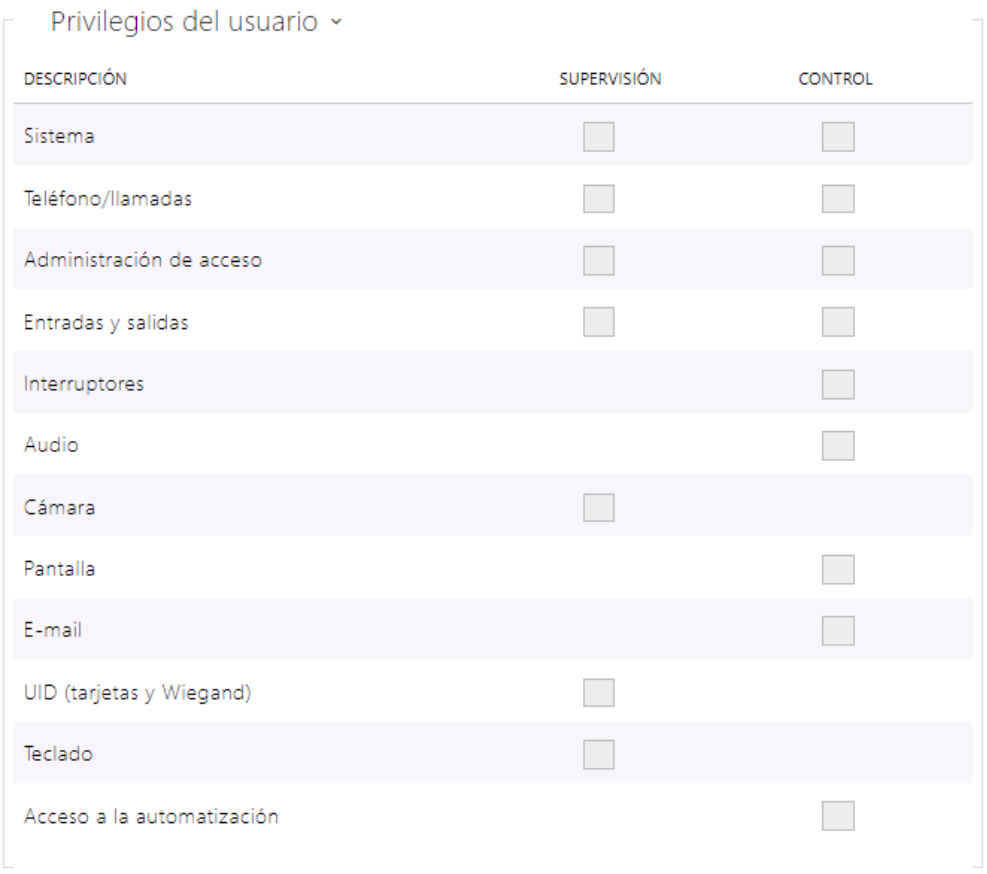
El intercomunicador 2N IP permite administrar hasta cinco cuentas de usuario destinados al acceso a los servicios **HTTP API**. Una parte de la cuenta de usuario forma el nombre y la contraseña del usuario y la tabla de los derechos de acceso del usuario a cada uno de los servicio **HTTP API**.

Cuenta habilitado

- **Cuenta habilitado** – permite esta cuenta de usuario.



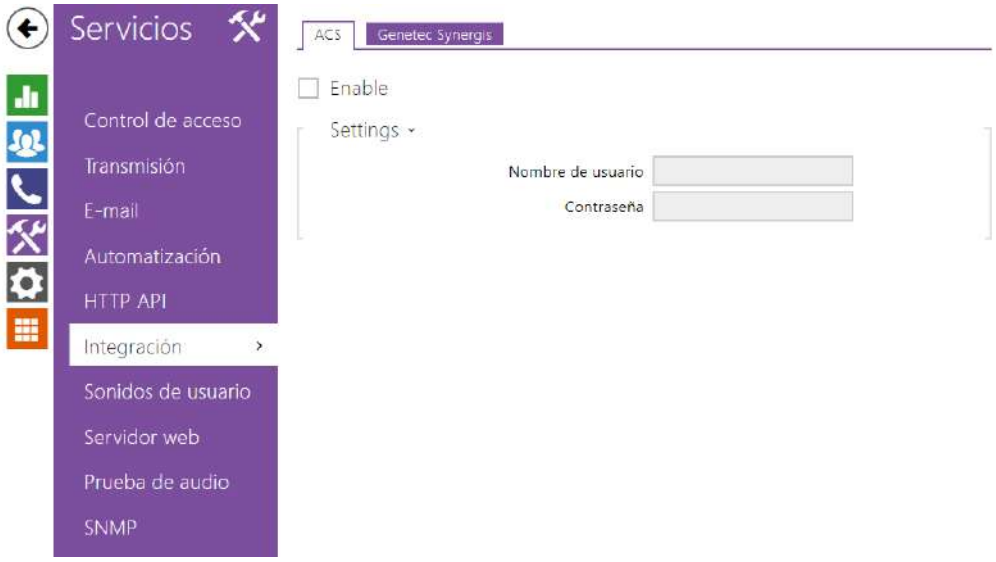
- **Nombre de usuario** – introduzca el nombre de usuario para autenticar con el HTTP API.
- **Contraseña** – introduzca la contraseña de autenticación de la HTTP API.



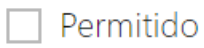
Con la ayuda de la tabla de derechos de acceso se pueden gestionar los privilegios de la cuenta de usuario a cada uno de los servicios.

5.4.6 Integrace

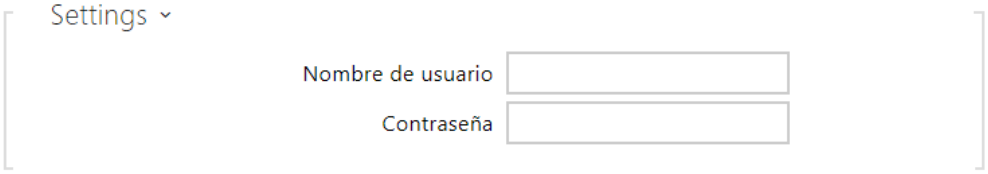
El servicio Integración permite al dispositivo conectarse con los sistemas de terceros.



Solapa ACS

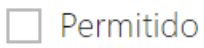


- **Habilitado** – habilita la función de llamada a Axis Camera Station (ACS). Para llamar a ACS se utiliza un URI especial en formato vms:*.

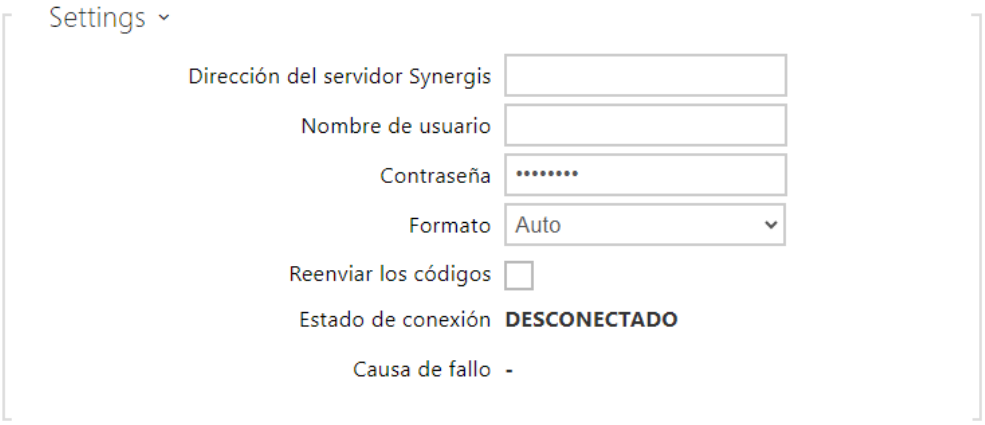


- **Nombre de usuario** – nombre de usuario para la autenticación de la llamada a ACS.
- **Contraseña** – contraseña para la autenticación de la llamada a ACS.

Solapa Genetec Synergis



- **Habilitado**– habilita la conexión con el sistema de seguridad Genetec Synergis externo.



- **Dirección del servidor Synergis**– dirección IP o nombre de dominio del servidor Synergis.
- **Nombre de usuario**– nombre de usuario utilizado durante la autenticación.
- **Contraseña**– contraseña utilizada durante la autenticación.
- **Formato** – formato de los códigos emitidos.
- **Reenviar códigos** – configura si se deben reenviar los códigos introducidos. Los códigos pueden contener como máximo 6 cifras y al final hay que pulsar la tecla de confirmación.

5.4.7 Sonidos de usuario

Los intercomunicadores **2N IP** señalizan de forma estándar diferentes estados de operación mediante una secuencia de tonos, ver el capítulo Señalización de los estados de operación. En el caso de que a sus requisitos no le satisfacen los tonos de señalización estándar, puede modificarlos.

El intercomunicador permite modificar la señalización acústica para los siguientes estados:

a. **Tono previo a la aceptación de la llamada entrante**
b. **Tono de timbre**
c. **Tono de línea ocupada**

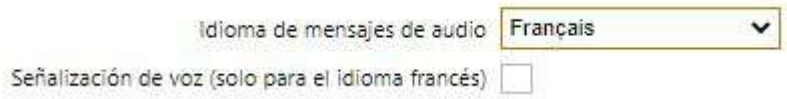
d. **Finalización de la llamada**
e. **Introducción de un código no válido**
f. **Elección de la posición de usuario no válida**
g. **Activación del interruptor**

Puede reducir totalmente la señalización de los estados mencionados anteriormente, sustituirla por uno de los diez sonidos predefinidos o por un archivo de audio propio que grabará fácilmente en el intercomunicador. Los archivos de audio deben estar en formato WAV y deben utilizar la codificación PCM con la frecuencia de muestreo de 8 ó 16 kHz y con la resolución de la muestra de 8 ó 16 bits. El tamaño del archivo no debe superar en los **intercomunicadores 2N IP** los 256 kB, en **2N® SIP Horn** 2048 kB.

Frecuencia	Bits por muestra	Longitud del sonido	Calidad del sonido
16 kHz	16 bit	up to 8 s	1 best
16 kHz	8 bit	up to 16 s	2
8 kHz	16 bit	up to 16 s	3 (not recommended combination)
8 kHz	8 bit	up to 32 s	4 low

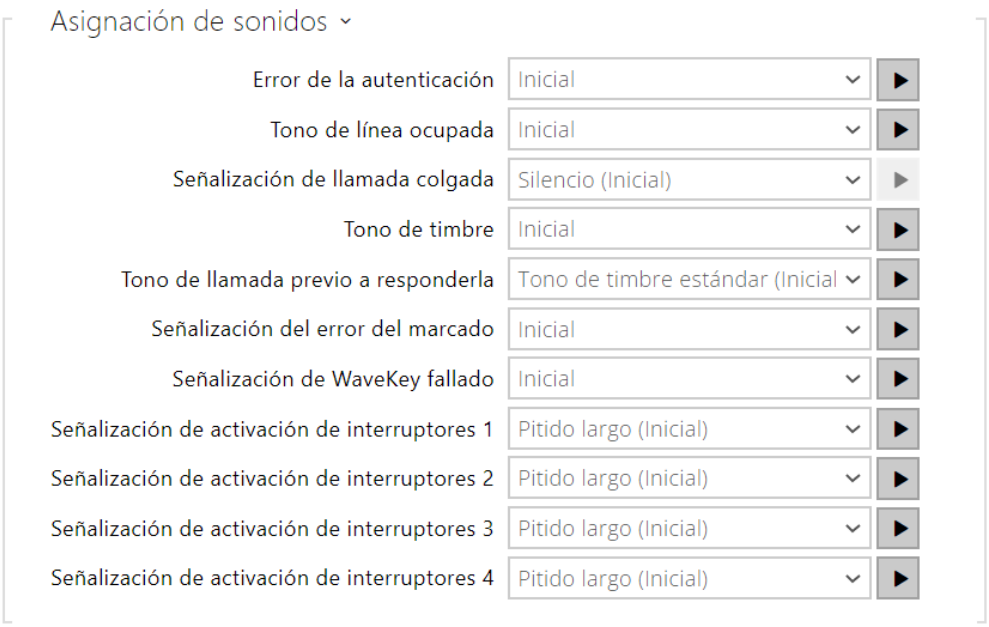
A los archivos de audio grabados puede reproducir también mediante la automatización utilizando la acción **Action.PlayUserSound**. Los sonidos se pueden reproducir opcionalmente mediante el reproductor del intercomunicador y/o directamente en la llamada telefónica.

Lista de parámetros



- **Idioma de mensajes de audio** – selecciona el idioma para las notificaciones de audio del intercomunicador. En el caso de que para un suceso determinado esté mapeado el archivo para el cual esté disponible la traducción, el mensaje se reproducirá en el idioma seleccionado. Si la traducción no está disponible, se reproducirá en inglés o como un sonido de idioma neutral.
- **Activar la señalización por voz (solo el idioma francés)** – para cumplir los reglamentos legislativos en los regiones de habla francesa es posible activar la señalización de voz para las personas con hendikep en idioma francés para estas acciones: configuración de llamadas, conexión de llamada y desbloqueo de la puerta.

Asignación de sonidos



- **Error de la autenticación** – configura el sonido reproducido en el caso de acceso denegado.
- **Tono de línea ocupada** – configura el sonido reproducido en el caso de que el participante llamado esté ocupado.
- **Señalización del fin de llamada** – configura el sonido reproducido tras finalizar la llamada.
- **Tono de timbre** – configura el sonido que se reproduce al sonar el timbre de la persona llamada. El tono del timbre de la centralita tiene preferencia ante el tono del timbre configurado en el intercomunicador.
- **Sonido del timbre antes de aceptar la llamada** – configura el sonido del sonido del timbre reproducido antes de aceptar la llamada entrante (tono del timbre del intercomunicador).
- **Señalización del error del marcado** – configura el sonido reproducido al pulsar el botón del marcado rápido en el caso de que la posición correspondiente en la lista telefónica no esté programada.
- **Señalización de WaveKey fallado** – configura el sonido que se reproducirá en el caso de que ningún teléfono haya abierto la puerta durante el tiempo de búsqueda.
- **Señalización del interruptor activado 1–4** – configura el sonido generado al activarse el interruptor. En la configuración de cada uno de los interruptores hay que precisar la señalización de la activación, ver el capítulo Interruptores.

Aviso

- En el caso de que no se pueda reproducir el audio del sonido asignado, es porque el sonido está configurado como "Silencio".

Grabación de sonidos

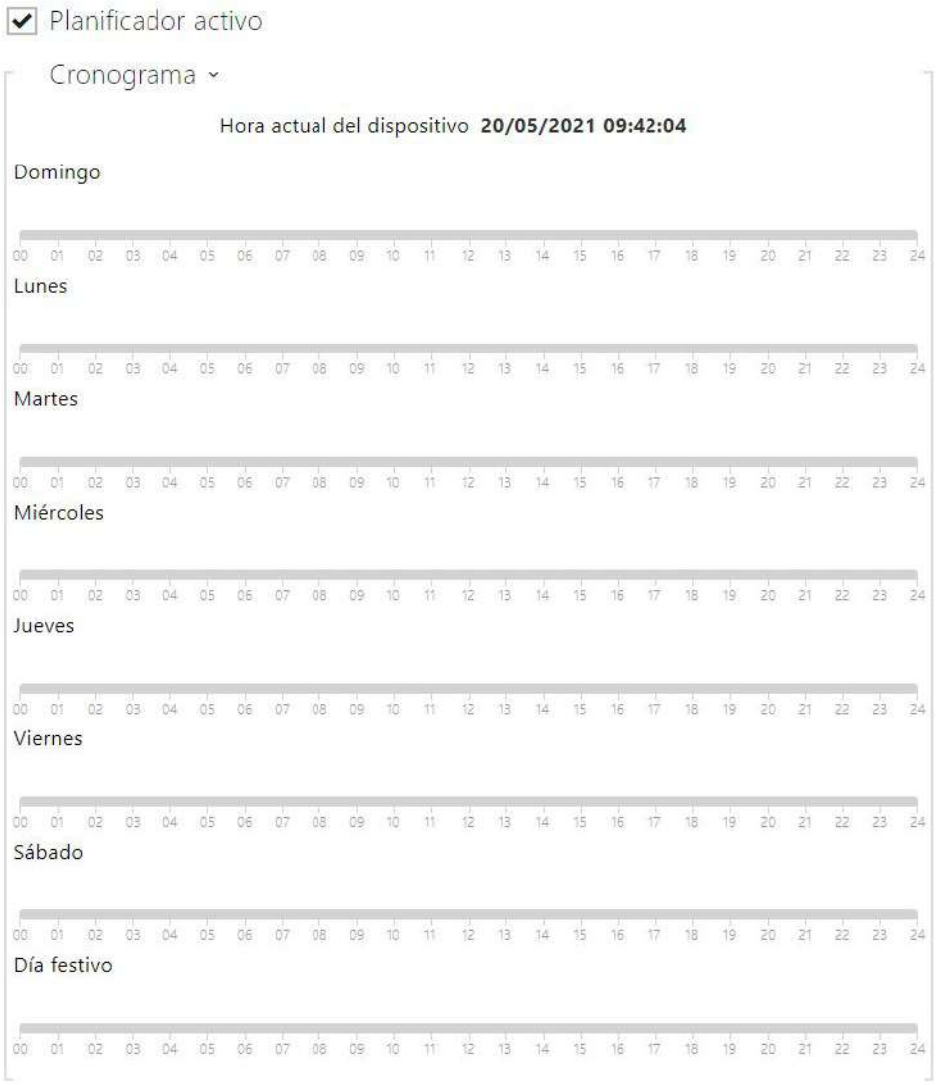
En el intercomunicador puede cargar hasta 10 archivos propios de audio. Para mayor claridad puede asignar a cada sonido grabado su propio nombre.

El archivo de audio puede grabar en el intercomunicador pulsando el botón . Seleccione en la ventana de diálogo el archivo guardado en su PC y pulse en botón **Cargar**. Puede eliminar el archivo mediante el botón . El archivo de audio cargado puede reproducir (de forma local en su PC) mediante el botón . Mediante el botón podrá cargar el archivo de audio directamente utilizando el micrófono en su PC.

El archivo de audio podrá grabar utilizando el micrófono en su PC. Mediante el botón se reproduce la grabación. Finaliza al pulsar el botón . El sonido grabado se puede reproducir mediante el botón . Tras pulsar el botón **Cargar** el sonido se guardará en el intercomunicador.

Planificador de anuncios

Permite la reproducción periódica de los sonidos de usuario a la hora configurada. En el plan de tiempo se pueden configurar las horas exactas para cada uno de los días de la semana cuando se reproducirá el sonido determinado. La añadidura de la reproducción del sonido se realiza haciendo clic sobre el lugar requerido en el eje temporal del día seleccionado. Durante la añadidura se puede configurar la hora exacta, elegir el sonido de usuario y configurar su volumen. La solapa **Planificador de anuncios** está disponible solo para los **productos** 2N SIP Audio.



- **Planificador activo** – activa la reproducción de los sonidos de usuario configurados previamente según el planificador de tiempo.

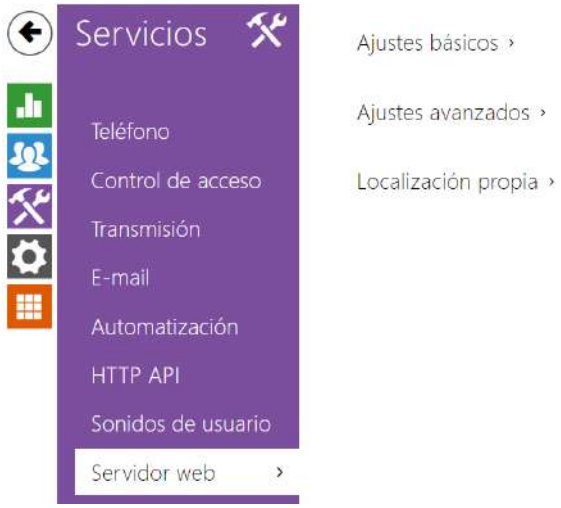
Consejo

- Para obtener ayuda de como crear los sonidos de usuario proceda según la información en este enlace https://wiki.2n.cz/hip/inte/latest/en/10-media-applications/audacity.

Nota

- La función para la grabación de sonido no está disponible en los exploradores que no soportan el estándar WebRTC (por ej. Internet Explorer).

5.4.8 Servidor Web



Los **intercomunicadores 2N IP** se pueden configurar mediante un explorador habitual que accede al servidor web integrado en el intercomunicador. Para la comunicación entre el explorador y el intercomunicador se utiliza el protocolo HTTPS asegurado. Para iniciar la sesión en el intercomunicador hay que introducir el nombre y la contraseña de inicio de sesión. El nombre y la contraseña inicial para iniciar la sesión es **admin** y **2n**. Recomendamos cambiar lo antes posible la contraseña inicial.

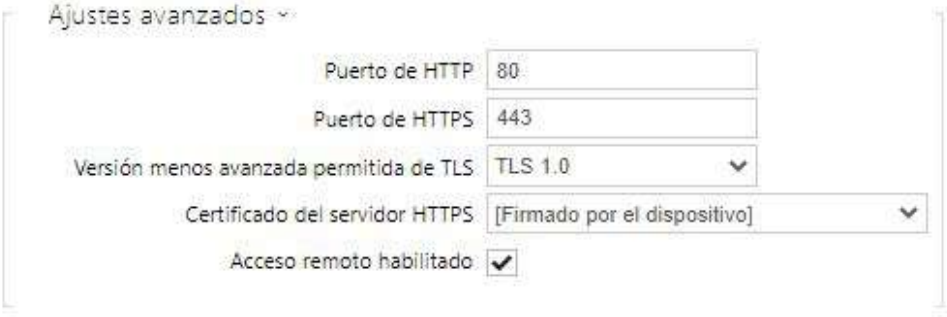
El servicio de servidor web está siendo utilizada también por otras funciones del intercomunicador:

a. Descarga de instantáneas JPEG, event. vídeo MJPEG, ver el capítulo Streaming.
b. Protocolo ONVIF para realizar stream de vídeo, ver el capítulo Streaming
c. Comandos HTTP para controlar los interruptores, ver el capítulo Interruptores
d. Suceso Event.HttpTrigger en **Automatización**, ver el manual correspondiente.

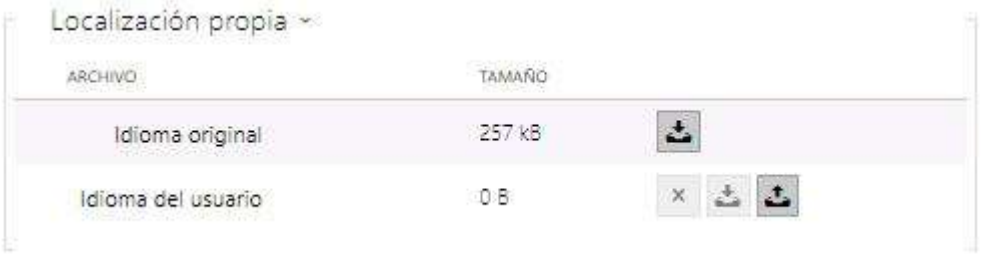
Para estos casos especiales se puede utilizar para la comunicación el protocolo HTTP no asegurado.

Lista de parámetros

- **Nombre del dispositivo** – configura el nombre del dispositivo que se muestra en la esquina superior derecha de la interfaz de web, en la ventana de inicio de sesión y eventualmente también en otras aplicaciones (Network Scanner etc.)
- **Idioma de la interfaz de web** – configura el idioma inicial tras el inicio de sesión en el servidor web de administración. El idioma de la interfaz de web lo puede cambiar en cualquier momento de forma temporal mediante los botones en la barra superior de la página.
- **Contraseña** – configura la contraseña de inicio de sesión en el intercomunicador. Para cambiar la contraseña utilice el botón  . La contraseña debe contener como mínimo 8 caracteres, de los cuales debe haber una letra minúscula, una mayúscula y al menos un dígito.



- **Puerto HTTP** – configura el puerto de comunicación del servidor web para la comunicación mediante el protocolo HTTP no asegurado. El cambio de este puerto no se notará hasta después del reinicio del intercomunicador.
- **Puerto HTTPS** – configura el puerto de comunicación del servidor web para la comunicación mediante el protocolo HTTPS asegurado. El cambio de este puerto no se notará hasta después del reinicio del intercomunicador.
- **Versión menos avanzada permitida de TLS** – determina la versión menos avanzada de TLS que se permitirá para la conexión a los dispositivos.
- **Certificado HTTPS privado** – configura el certificado de usuario y la clave privada mediante los cuales se realiza el cifrado de la comunicación entre el servidor HTTP del intercomunicador y el explotador web del usuario. Se puede elegir uno de los tres conjuntos de certificados y claves privadas, ver el capítulo Certificados, o conservar la configuración **Self Signed** donde se utilizará el certificado generado automáticamente creado durante el primer arranque del dispositivo.
- **Habilitar acceso remoto** – permite habilitar el acceso remoto al servidor web del intercomunicador desde las direcciones IP fuera de la red local.

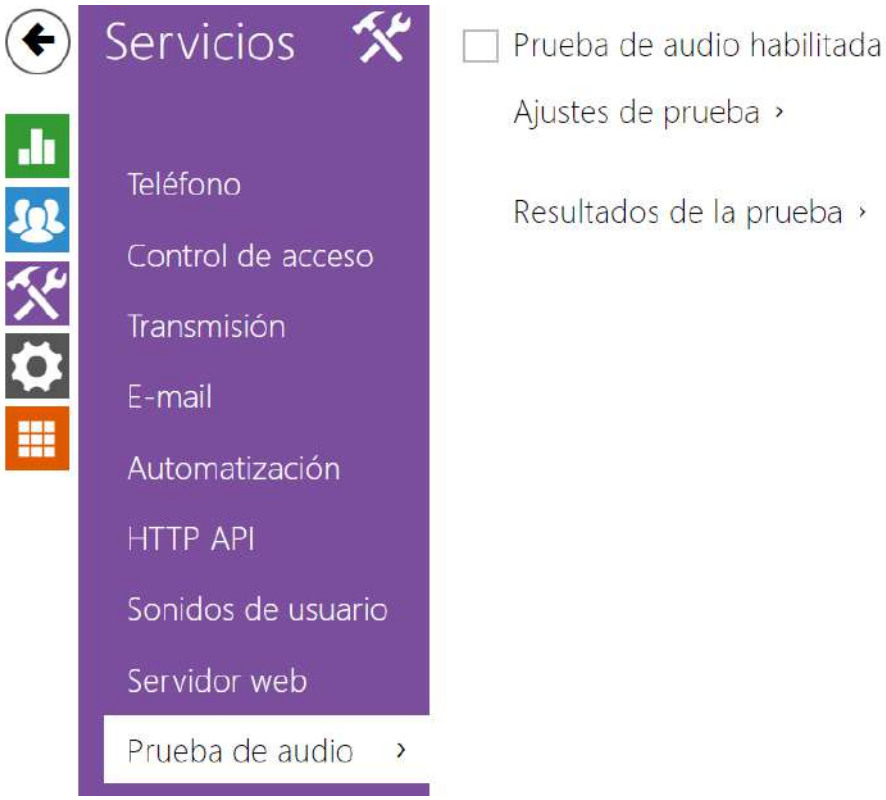


- **Idioma original** – permite descargar desde el dispositivo el archivo original que contienen todos los textos de la interfaz de web en el idioma inglés. El archivo está en formato XML, ver más abajo.
- **Idioma del usuario** – permite cargar, descargar y eventualmente eliminar el archivo del usuario con sus propias traducciones de los textos de las interfaz de web.

```
<?xml version="1.0" encoding="UTF-8"?> <strings language="English" languageshort="EN">
 <!-- Global enums--> <s id="enum/error/1">Invalid value!</s> <s id="enum/bool_yesno/
0">NO</s> <s id="enum/bool_yesno/1">YES</s> <s id="enum/bool_user_state/0">ACTIVE</s>
<s id="enum/bool_user_state/1">INACTIVE</s> <s id="enum/bool_profile_state/
0">ACTIVE</s> <s id="enum/bool_profile_state/1">INACTIVE</s> .. .. .. </strings>
```

Durante la traducción modifique solo los valores de los elementos **<s>** y no modifique los valores de los atributos **id**. El nombre del idioma dado por el atributo **language** del elemento **<strings>** se especificará en las opciones del parámetro Idioma de la interfaz de web. La abreviatura del nombre del idioma dada por el atributo **languageshort** del elemento **<strings>** se especificará en la lista de idiomas en la esquina superior derecha de la ventana y servirá para cambiar rápidamente entre los idiomas.

5.4.9 Test de audio

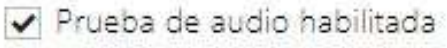


Los **intercomunicadores 2N IP** permiten realizar el control periódico del reproductor y del micrófono incorporado. Durante el test el reproductor del dispositivo emite uno o varios tonos breves. Mediante el micrófono incorporado se detecta el tono emitido y en el caso de que se detecte correctamente el test es declarado satisfactorio. El tiempo de duración del test son aproximadamente 4 s. En el caso de que el test sea insatisfactorio (lo cual puede ser causado por ej. por un ruido ambiental extremo), el test se realiza una vez más dentro de diez minutos. El resultado del último test se puede visualizar en la interfaz de confirmación del intercomunicador o procesarlo mediante **Automation**.

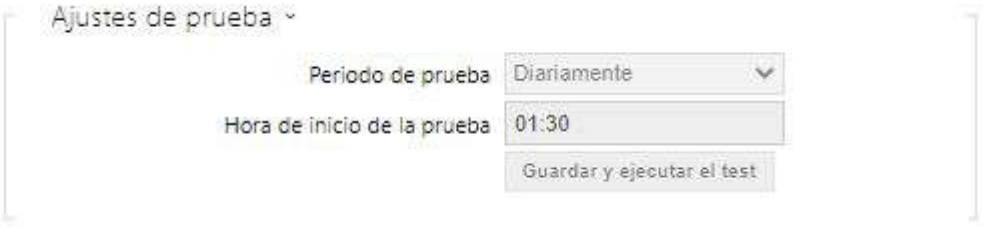
Nota

- *En el caso de que durante la ejecución del test de audio se esté realizando una llamada, el test de audio se pospone hasta que la llamada finalice. El test de audio se realizará inmediatamente tras finalizar la llamada.*

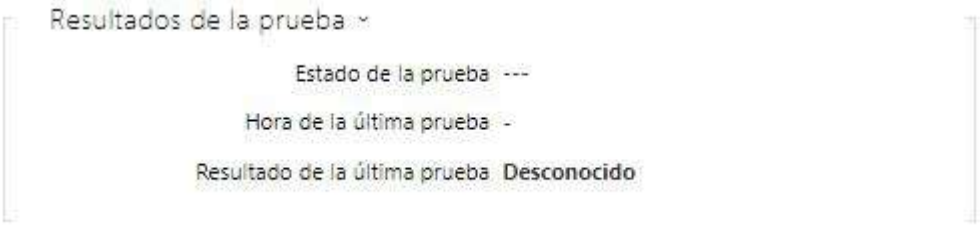
Lista de parámetros



- **Habilitación del test de audio** – habilita la ejecución automática del test de audio.

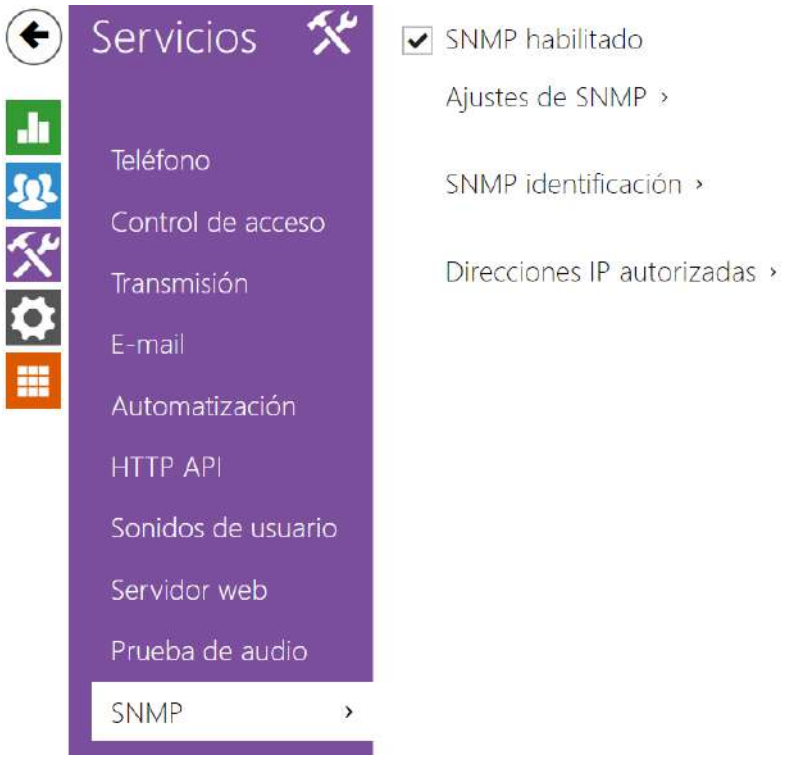


- **Período del test** – permite configurar el período de la realización del test. El test se puede ejecutar de forma automática una vez al día o una vez a la semana.
- **Hora de inicio del test** – permite configurar la hora a la cual se debe realizar el test periódico. La hora se puede configurar en el formato HH:MM. Recomendamos configurar el tiempo cuando se prevé el uso mínimo del intercomunicador.
- **Guardar y ejecutar el test** – mediante el botón puede ejecutar y guardar el test inmediatamente, sin tener en cuenta la configuración actual.



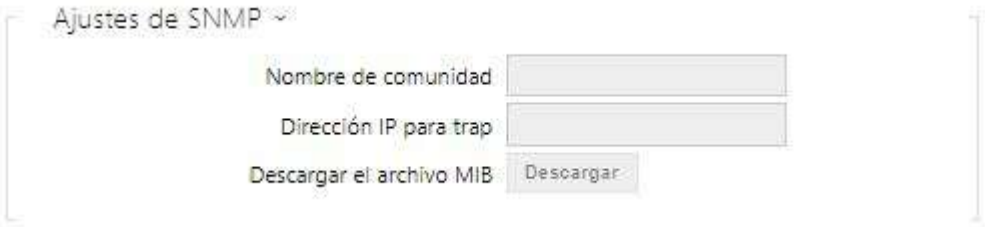
- **Estado del test** – muestra continuamente el estado del transcurso del test.
- **Hora del último test** – muestra la hora del último test realizado.
- **Resultado del último test** – muestra el resultado del último test realizado.

5.4.10 SNMP



Los **intercomunicadores 2N IP** integran la funcionalidad que permite la vigilancia remota de los intercomunicadores en la red mediante el protocolo SNMP. El agente SNMP integrado en el dispositivo está disponible tras introducir la clave de licencia con la licencia **Enhanced Integration**. Los intercomunicadores soportan el protocolo SNMP versión 2c.

Lista de parámetros



- **Identificador de la comunidad** – cadena de texto que representa la clave de acceso para acceder a los edificios en la table MIB
- **Dirección IP para traps** – dirección IP a la que se enviarán los traps SNMP

Nota

- En la versión actual los traps no son soportados. El **intercomunicador 2N IP** trabaja solo en el modo requerimiento - respuesta.

- **Descargar el archivo MIB** – permite descargar la definición actual de la tabla MIB desde el dispositivo

- **Contacto** – permite introducir el contacto de administrador del dispositivo (por ej. nombre, e-mail, etc.)
- **Nombre** – permite introducir el nombre del dispositivo
- **Localización** – permite introducir la descripción de la localización del dispositivo (por ej. 1er piso).

- **Dirección IP** – permite introducir hasta 4 direcciones IP válidas para el acceso al agente SNMP. El acceso desde otras direcciones estará bloqueado. En el caso de que este campo se quede en blanco, se puede acceder al dispositivo desde cualquier dirección IP.

5.5 Hardware

Aquí se expone el resumen de lo que encontrará en este capítulo:

5.5.1 Interruptores

Los interruptores permiten el control muy flexible de diferentes periferias conectadas al intercomunicador (como son las cerraduras de puerta eléctricas, iluminación, señalización adicional del sonido del timbre, etc.).

Los **intercomunicadores 2N IP** permiten configurar hasta 4 (en diferentes modelos esto puede variar) interruptores independientes que se pueden utilizar para cualquier fin.

El interruptor se puede activar:

- introduciendo el código válido en el teclado numérico del intercomunicador o aceptando la secuencia de los símbolos DTMF durante la llamada,
- acercando la tarjeta RFID al lector,
- con retardo definido desde la activación de otro interruptor,
- mediante la llamada entrante o saliente,
- pulsando uno de los botones del marcado rápido *),
- mediante el perfil de tiempo *),
- aceptando el comando HTTP desde otro dispositivo en la red,
- con la automatización mediante la acción Action.ActivateSwitch *).

En el caso de necesidad se puede bloquear el interruptor mediante el perfil de tiempo seleccionado.

Aviso

- Las opciones marcados con *) requieren las licencias activas correspondientes.

Bloqueo y pulsado prolongado del interruptor
Las condiciones de la activación del interruptor se pueden modificar mediante dos funciones. Una de ellas es el bloqueo, la otra se el pulsado prolongado del interruptor. En el caso de que el interruptor esté bloqueado, está permanentemente en estado "apagado" y no es posible manipularlo hasta que no se desbloquee (el bloqueo tiene la prioridad superior a la del pulsado prolongado – en el caso de que el interruptor esté a la vez bloqueado y pulsado durante un tiempo prolongado, se aplicará el bloqueo). En el caso de que el interruptor esté pulsado durante un tiempo prolongado, está permanentemente en estado "activado" y no es posible manipularlo hasta que no se suelte.
El bloqueo y el pulsado prolongado se puede controlar, entre otras cosas, mediante los perfiles de tiempo. En la función de bloqueo no se recomienda utilizar el perfil de tiempo (el control de bloqueo mediante el perfil de tiempo está presente en el dispositivo por razones de compatibilidad retroactiva), ya que en ese caso al final del perfil de tiempo se desbloqueará el interruptor a pesar de que el interruptor haya sido bloqueado manualmente.
La combinación de estas dos funciones muestra el parámetro **Funcionamiento actual del interruptor** (Normal – el bloqueo y el pulsado prolongado están apagados; Pulsado durante un tiempo prolongado – el bloqueo está apagado y el pulsado prolongado está encendido; Bloqueado – el bloqueo está encendido, no se tiene en cuenta la configuración del pulsado prolongado).
Tras el reinicio del dispositivo revise si el bloqueo o el pulsado prolongado está influenciado por el perfil de tiempo. En el caso de que sea así, la función correspondiente se activa o desactiva teniendo en cuenta la configuración del perfil de tiempo. En el caso de que no sea así, se establece el último estado de bloqueo antes del apagado del dispositivo, respectivamente el pulsado prolongado está configurado al estado inactivo (el interruptor no está pulsado de forma prolongada).

En el caso de que el interruptor esté activo, se puede configurar:

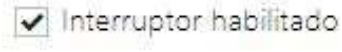
- activación de cualquier salida lógica del intercomunicador (relé, salida de potencia)
- activación de la salida a la cual está conectada el módulo **Intercomunicador 2N® IP – Relé de seguridad**
- envío del comando HTTP a otro dispositivo

El interruptor puede trabajar en el modo monoestable o biestable. En el modo monoestable, el interruptor se apaga automáticamente tras el tiempo configurado. En el modo biestable, el interruptor se enciende con la primera activación y se apaga con la siguiente.

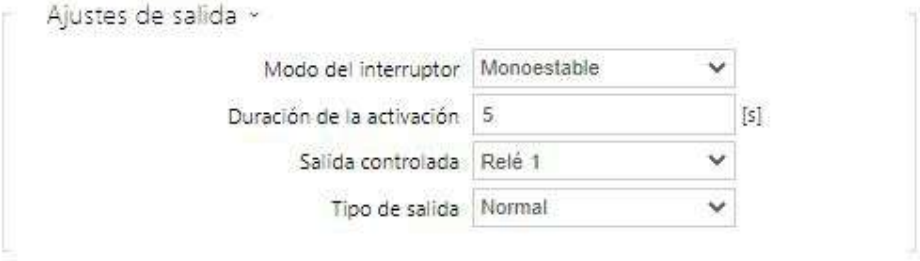
El interruptor puede señalizar su estado mediante:

- pitido configurable, eventualmente mediante el sonido elegido de usuario
- diodo LED de señalización en el caso de que el intercomunicador esté equipado con él
- en la pantalla (en el caso de que el modelo correspondiente del intercomunicador esté equipado con ella) mediante el icono de la puerta abierta

Solapa Interruptor 1–4



- **Interruptor habilitado** – habilita o prohíbe deshabilita globalmente el control del interruptor. Si el interruptor no está habilitado, no es posible activarlo con ninguno de los códigos introducidos (incluidos los códigos de usuario para los interruptores), no se puede activar con una llamada ni con el botón de marcado rápido.



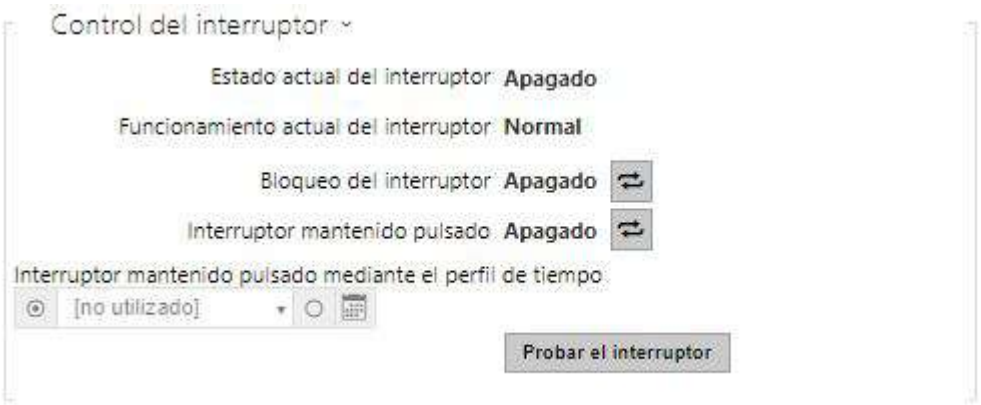
- **Modo del interruptor** – configura el modo monoestable o biestable para el interruptor. En el modo monoestable, el interruptor se apaga automáticamente tras el tiempo configurado de activación. En el modo biestable, el interruptor se enciende con la primera activación y se apaga con la siguiente.
- **Tiempo de activación** – configura el tiempo de activación del interruptor en el modo monoestable. En el modo biestable del interruptor el tiempo configurado de activación no se aplicará.
- **Salida controlada** – permite asignar una salida eléctrica al interruptor. Se puede elegir entre todas las salidas disponibles del modelo del intercomunicador correspondiente: relé, salidas de potencia o salidas en los módulos de ampliación, etc. En el caso de que elija la opción **ninguno**, el interruptor no controlará ninguna salida eléctrica, pero usted podrá seguir utilizándolo para controlar el dispositivo externo mediante los comandos HTTP.
- **Tipo de salida** – en el caso de que utilice **2N® IP Intercomunicador Relé de seguridad**, configure el tipo de salida al valor **security**. En el modo **security** la salida funciona de modo inverso, es decir, permanece activada y controla el módulo **2N® IP Intercomunicador Relé de seguridad** a través de una secuencia de pulsos específica. En el caso de que utilice la cerradura reversible de la puerta (es decir, la puerta se bloquea al llegar la tensión a la cerradura), configure el tipo de salida al valor de **inversión.** En el caso de que varios interruptores estén configurados para la misma salida, pero tienen diferentes tipos de salida, se controlarán según la siguiente prioridad: 1. security, 2. de inversión, 3. normal.

Nota

- ***2N® IP Vario*** *– en el conector de configuración es necesario configurar la alimentación interna y el relé de activación.* ***2N® IP Force*** *– el relé de seguridad se conecta a los bornes DOOR + y -.*
- *Para el tipo de salida:* ***security*** *se puede configurar el tiempo de activación del interruptor solo un valor superior a 1 s. Para el tipo de salida:* ***normal, inverso*** *se puede configurar el tiempo de activación al valor 0.1 s o superior.*

Seguridad

- La salida 12V sirve para conectar la cerradura. Sin embargo, cuando la unidad (2N IP Interkom, 2N Access Unit) se encuentra en un lugar (revestimiento del edificio) donde existe el riesgo de irrupción no autorizada en el dispositivo, se recomienda con mucha énfasis utilizar el 2N® Relé de seguridad (No de referencia 9159010) para la máxima seguridad de la instalación.



- **Estado actual del interruptor** – muestra el estado actual del interruptor (Encendido o Apagado).
- **Funcionamiento actual del interruptor** – muestra el funcionamiento actual del interruptor.
  - **Normal**: el interruptor no está bloqueado ni mantenido pulsado.
  - **Mantenido pulsado**: el interruptor se mantiene pulsado y no está bloqueado.
  - **Bloqueado**: el interruptor está bloqueado (en este caso no importa si el interruptor se mantiene pulsado, el bloqueo tiene la prioridad).
- **Bloqueo del interruptor** – encendido: el interruptor permanece en la posición 0 y no es posible controlarlo hasta que no se desbloquee. Apagado: el interruptor no está bloqueado.

- **Interruptor mantenido pulsado** – encendido: el interruptor permanece en la posición 1 y no es posible controlarlo hasta que no se libere (en el caso de que a la vez esté mantenido pulsado y bloqueado, el interruptor está bloqueado. Apagado: el interruptor no se mantiene pulsado en la posición 1.
- **Interruptor mantenido pulsado mediante el perfil de tiempo** – permite asignar al interruptor el perfil de tiempo pre-definido o configurar manualmente el perfil de tiempo que habilita la activación del interruptor. En el caso de que el perfil de tiempo asignado de esté activo, el interruptor se puede activar acercando la tarjeta RFID válida, mediante una llamada, introduciendo el código o utilizando el botón de marcado rápido.
- **Botón „Probar interruptor“** – permite activar manualmente el interruptor para comprobar su función, por ejemplo de la cerradura eléctrica o de otro dispositivo conectado.

Aviso

- En el caso de que el interruptor esté bloqueado y se produzca el apagado y un nuevo encendido del dispositivo, el interruptor permanecerá bloqueado tras el encendido del dispositivo. El interruptor se comporta de la misma manera en el caso de que esté prohibido y luego habilitado.
- En el caso de que el interruptor se mantenga pulsado y se produzca el apagado y un nuevo encendido del dispositivo, el interruptor no se mantendrá pulsado tras el encendido del dispositivo. El interruptor se mantiene pulsado tras el encendido del dispositivo solo en el caso de que esté configurado el perfil de tiempo para que el interruptor se mantenga pulsado y este perfil esté activo en el momento del encendido del dispositivo. El interruptor se comporta de la misma manera en el caso de que esté prohibido y luego habilitado.

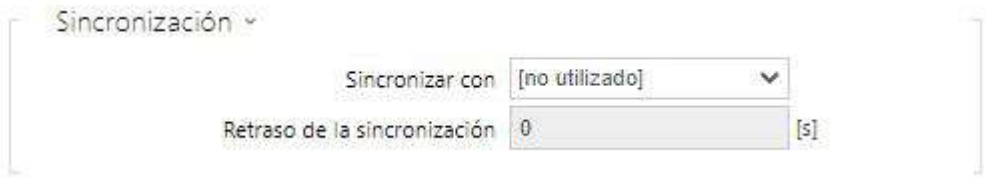
Lista de los códigos universales mediante los cuales se puede desde el aparato telefónico o desde el teclado del intercomunicador activar los interruptores. Para cada interruptor se pueden introducir hasta 10 códigos universales (el número de los códigos pueden variar en cada uno de los modelos de los intercomunicadores).

- **Código** – permite introducir el código numérico del interruptor. El código debe contener al menos dos caracteres para desbloquear la puerta desde el teclado del intercomunicador, y como mínimo un carácter para desbloquear la puerta con la ayuda de DTMF desde el teléfono. Recomendamos utilizar al menos cuatro caracteres. Los códigos 00 y 11 no se pueden introducir desde el teclado numérico y están reservados para la apertura mediante DTMF y no se aceptarán desde el teclado. El código de confirma utilizando el símbolo *. El código puede tener longitud de hasta 16 caracteres.
- **Disponibilidad** – permite bloquear la introducción del código para la activación del interruptor desde el teclado numérico del intercomunicador o el aparato telefónico del usuario.
- **Perfil de tiempo** – permite asignar al código del interruptor un perfil de tiempo y de esta manera controlar su vigencia.
- **Distinguir los códigos para la activación y apagado** – permite configurar el modo de códigos de los interruptores cuando los códigos impares (1, 3, etc.) estén destinados a activar el interruptor y los pares (2, 4, etc.) para el apagado del interruptor. Solo se puede usar este modo si el interruptor está configurado al modo biestable.

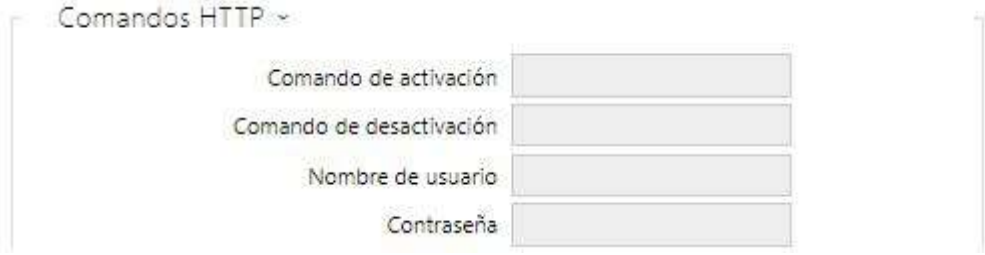
- **Activación mediante llamada** – permite configurar la activación del interruptor mediante una llamada entrante, eventualmente saliente. En el caso de llamada saliente el interruptor se activa tras recibir el mensaje 180 Ringing, mediante la cual la parte opuesta confirma que el timbre está sonando. En el caso del modo biestable del interruptor éste se mantiene activo durante todo el tiempo de la llamada. En el caso del modo monoestable se activa el interruptor al iniciarse la llamada y se apaga una vez transcurrido el tiempo de activación configurado.
- **Activación mediante el botón de marcado rápido** – permite asignar al interruptor un botón de marcado rápido. El interruptor se activa al pulsar este botón.

Nota

- *La activación mediante el botón del marcado rápido está disponible solo con la licencia Gold.*



- **Sincronizar** – habilita la función de la sincronización del interruptor que permite la activación automática del interruptor tras el tiempo configurado desde el momento de la activación de otro interruptor. La longitud del intervalo entre la activación de los interruptores determina el parámetro **Retardo de sincronización**.
- **Retardo de sincronización** – configura la longitud del intervalo entre la activación sincronizada de dos interruptores. El parámetro no se aplicará en el caso de que no esté habilitada la función **Sincronizar**.



- **Comando enviado en el momento de activación** – permite configurar el comando enviado al dispositivo externo (por ej. relé WEB) en el momento de activación del interruptor. El comando se envía mediante el protocolo HTTP (GET request). El comando debe tener formato http://ip_dirección/ruta. Por ej. http://192.168.1.50/relay1=on.
- **Comando enviado en el momento de desactivación** – permite configurar el comando enviado al dispositivo externo (por ej. relé WEB) en el momento de desactivación del interruptor. El comando se envía mediante el protocolo HTTP (GET request). El comando debe tener formato http://ip_dirección/ruta. Por ej. http://192.168.1.50/relay1=off
- **Nombre de usuario** – nombre de usuario para la autenticación de la conexión al dispositivo externo (relé WEB, etc.). El parámetro es obligatorio solo en el caso de que el dispositivo externo requiera la autenticación.
- **Contraseña** – contraseña para la autenticación de la conexión al dispositivo externo (WEB relé etc.). El parámetro es obligatorio solo en el caso de que el dispositivo externo requiera la autenticación.

Consejo

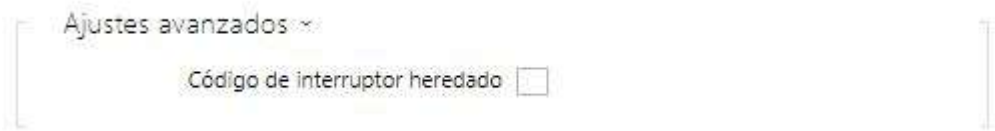
Los comandos HTTP no añaden la codificación URL. En el caso de que se introduce el comando, por ej. http://10.27.24.6/message.cgi?action=9%3A%2F, se enviará: http://10.27.24.6/message.cgi?action=9%3A%2F
En el caso de que el comando deba enviarse con la codificación URL, es necesario introducirlo en este formato, por ej. http://10.27.24.6/message.cgi?action=9%253A%252F, se enviará: http://10.27.24.6/message.cgi?action=9%253A%252F.

Consejo

En el caso del uso del relé externo **Nº de referencia: 9137410E** se utilizan los siguientes comandos HTTP:
Para la activación permanente – http://ip_adresa/state.xml?relayState=1 (por ej.: http://192.168.1.10/state.xml?relayState=1)
Para la activación a la hora pre-definida (por defecto 1,5 s) – http://ip_adresa/state.xml?relayState=2 (por ej.: http://192.168.1.10/state.xml?relayState=2)
Para la desactivación – http://ip_adresa/state.xml?relayState=0 (por ej.: http://192.168.1.10/state.xml?relayState=0)

En el caso del uso del relé externo **Nº de referencia: 9137411E** se utilizan los siguientes comandos HTTP (el signo X en los comandos hay que sustituirlo con el número del relé):
Para la activación permanente – http://ip_adresa/state.xml?relayState=1 (por ej.: http://192.168.1.10/state.xml?relay1State=1)
Para la activación a la hora pre-definida (por defecto 1,5 s) – http://ip_adresa/state.xml?relayXState=2 (por ej.: http://192.168.1.10/state.xml?relay1State=2)
Para la desactivación – http://ip_adresa/state.xml?relayXState=0 (por ej.: http://192.168.1.10/state.xml?relay1State=0)

Solapa Ampliados



- **Código del interruptor sin confirmación** – habilita la opción de la activación **del primer código del interruptor** especificado en la lista de códigos de parte del teléfono sin la confirmación mediante el símbolo *. En al caso de que esté marcado, el primer código no se confirma. Esta configuración no afecta otros códigos del interruptor especificados en la lista ni la introducción del código desde el teclado, estos hay que confirmar siempre mediante *. Sirve para configurar la compatibilidad retroactiva con otros modelos de intercomunicadores de la empresa 2N más antiguos.

- **Consumo máximo de energía de la salida 1** – configura el valor máximo de la potencia de entrada de la salida 1.

5.5.2 Audio

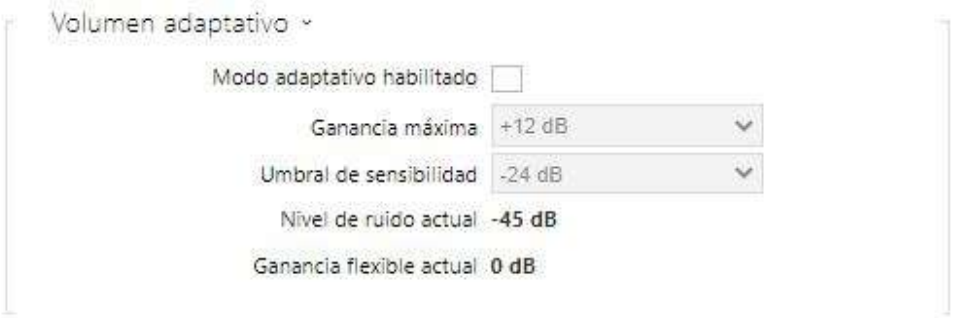
Todos los modelos de los intercomunicadores 2N IP están equipados con un reproductor, event. salida del amplificador de potencia, al que se puede conectar un reproductor externo. En esta parte de configuración se configura el volumen de las llamadas telefónicas y el volumen de la señalización de diferentes estados del dispositivo. El parámetro **Volumen general** controla el volumen general del dispositivo y afecta no solo el volumen de la llamada, sino también el volumen de los tonos de señalización, etc. Configure este parámetro según el nivel de ruido del ambiente en el cual se utiliza el intercomunicador. En el caso de que el nivel de ruido del ambiente no es constante, se puede utilizar el modo adaptativo que permite aumentar temporalmente el volumen general del dispositivo según el nivel de ruido actual del ambiente.

Modelo	Volumen general
IP Style	−12 dB .. +8 dB (2 x 4 W)
IP Vario	−10 db .. +0 dB (150 mW)

Modelo	Volumen general
Force/Safety 1W	−12 dB .. +6 dB (1 W)
Force/Safety 10W	−12 dB .. +20 dB (10 W)
IP Uni	−12 dB .. +6 dB (1 W)
IP Verso	−8 dB .. +8 dB (2 W)
IP Solo	−8 dB .. +4 dB (2 W)
IP Base	−8 dB .. +8 dB (2 W)
Audio/Video Kit	−10 dB .. +10 dB
SIP Speaker	−10 dB .. +10 dB
SIP Speaker Horn	−16 dB .. +16 dB

Lista de parámetros

- **Volumen general** – configura el volumen general del dispositivo. Esta configuración afecta al volumen de las llamadas telefónicas y a todos los tonos de señalización.



- **Permiso del modo adaptativo** – enciende el modo adaptativo de control del volumen en el que se configura automáticamente el volumen del reproductor según el nivel de ruido del ambiente en el que está instalado el intercomunicador.
- **Volumen máximo** – volumen máximo que se puede aplicar en el modo adaptativo sobre el volumen general.
- **Umbral de sensibilidad** – umbral del ruido ambiental con el cual se aplica el aumento de volumen de adaptación.
- **Nivel de ruido actual** – muestra el nivel del ruido ambiental medido actualmente.
- **Aumento de volumen adaptativo actual** – muestra el aumento de volumen aplicado actualmente del volumen general. El valor está dado por la diferencia entre el Nivel actual del ruido y el umbral establecido de sensibilidad y nunca supera el aumento máximo del volumen configurado.

- **Volumen del tono de la llamada** – configura el volumen de la señalización de la llamada entrante.
- **Volumen de los tonos de llamada** – configura el volumen del tono de notificación, del tono de llamada y del tono de ocupado. En el caso de que los tonos de llamada los genere automáticamente la centralita, no se aplicará esta configuración.

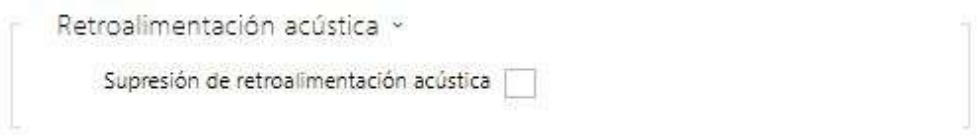
- **Volumen del pitido al pulsar la tecla** – configura el volumen del pitido generado al pulsar la tecla. El volumen configurado es relativo al volumen general configurado.
- **Volumen de los tonos de advertencia** – configura el volumen de los tonos de advertencia y señalización descritos en el capítulo Señalización de los estados de operación. El volumen configurado es relativo al volumen general configurado.

- **Volumen de la señalización de la activación del interruptor** – configura el volumen del tono generado al activar el interruptor. El volumen configurado es relativo al volumen general configurado.
- **Volumen de los sonidos de usuario** – configura el volumen de los sonidos de usuario reproducidos. El volumen configurado es relativo al volumen general configurado.

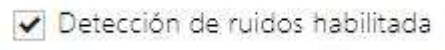
- **Entrada de audio inicial** – permite configurar la entrada de audio inicial (micrófono, entrada de línea o entrada del módulo de audio) que se utilizará para las llamadas telefónicas y para el stream de audio.
- **Aumento de volumen de la entrada de micrófono** – permite configurar el aumento de la entrada de micrófono.
- **Aumento de la entrada de línea** – permite configurar el aumento de la entrada de línea independientemente del aumento de volumen del micrófono.

Consejo

El aumento de volumen del micrófono se puede configurar solo en los modelos **2N® SIP Speaker Horn**, **2N® IP Audio Kit** y **2N® IP Video Kit**.
La configuración del aumento de la entrada de micrófono (event. de línea) está relacionada con el nivel de la señal de entrada y con el modo de instalación del micrófono externo. El rango amplio de la configuración de la subida de volumen (0 hasta 39 dB en el caso e la entrada de micrófono y −6 dB hasta 24 dB en el caso de la entrada de línea) debería ser suficiente para la mayoría de las instalaciones. El aumento de volumen debería estar configurado de manera que esté garantizada la audibilidad suficiente y a la vez que con los volúmenes más altos del reproductor no se produzca el retorno acústico y la consecuente saturación de la señal en la entrada de micrófono (event. de línea) que podría causar el empeoramiento de la función de supresión del eco (AEC).



- **Supresión del retorno acústico** – configura el modo de la supresión automática del retorno acústico (normalmente pitido) entre el reproductor del intercomunicador y el auricular del aparato telefónico, en el caso de que se encuentre en la cercanía inmediata del intercomunicador. Este modo está apagado por defecto.



- **Detección de ruido encendida** – activa la detección automática del ruido, resp. de la superación del umbral establecido del nivel de la señal del micrófono. El alarma provocada por la superación del valor umbral se puede procesar mediante el suceso de automatización **Event.NoiseDetected** y relacionarlo con otras acciones de usuario.

- **Umbral de nivel de ruido** – configura el umbral del nivel de la señal del micrófono tras cuya superación saltará el alarma.
- **Retardo de la activación del alarma** – configura el tiempo durante el cual debe estar la señal por encima del límite umbral para que salte el alarma.
- **Retardo de la desactivación del alarma** – configura el tiempo durante el cual debe estar la señal por debajo del límite umbral para que se pare el alarma.
- **Gráfico de nivel de ruido** – muestra el historial del nivel de la señal medida. Con el color rojo están marcados los momentos cuando se activa el alarma.

5.5.3 Cámara

Este menú está disponible solo en los **intercomunicadores 2N IP** que están equipados con la cámara interna o permiten conectar una cámara externa. La señal de la cámara se puede transmitir directamente a la llamada al videoteléfono, enviar mediante e-mails, transmitir mediante el protocolo ONVIF/RTSP a otro dispositivo (por ej. vídeo surveilance) o descargar fácilmente desde el intercomunicador como imágenes JPEG mediante el protocolo HTTP.

Como fuente de la señal de vídeo se puede utilizar:

- cámara interna integrada o cámara analógica externa (solo **2N® IP Video Kit**)
- cámara IP externa común que soporta stream RTSP con códecs MJPEG (resolución máx. 640 x 480) o H.264 (resolución máx. 640 x 480 Base Line Profile). La frecuencia de imágenes máxima recomendada es en ambos casos 15 imágenes por segundo. Con secuencias de imágenes superiores pueden producirse efectos indeseados (reducción de la fluidez de la reproducción).

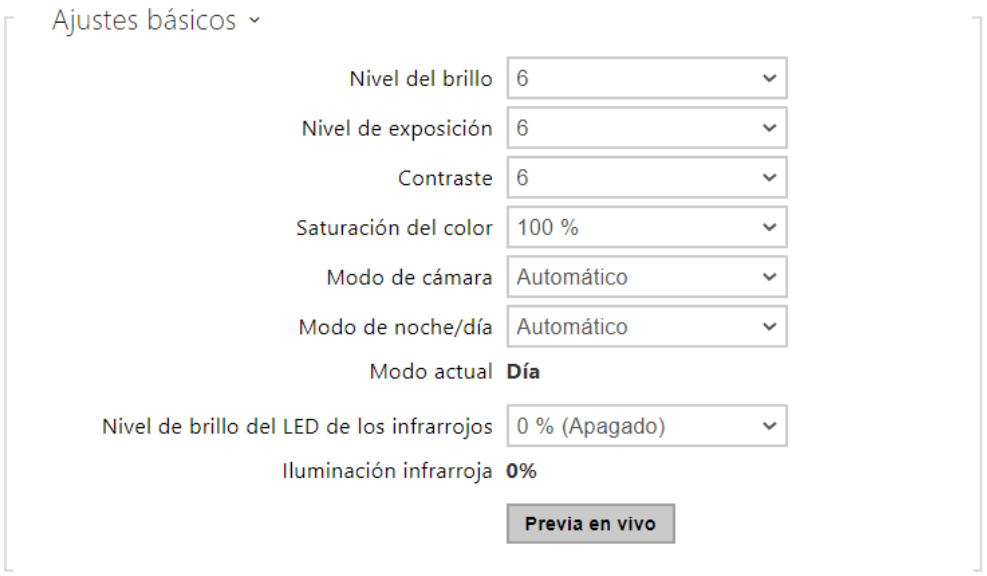
En el menú Cámara se configuran los parámetros de la cámara, como es el brillo, saturación de colores, event. datos de inicio de sesión para la cámara IP externa. Los parámetros relacionados con las llamadas de vídeo y con el stream de vídeo se encuentran en el menú **Servicios / Teléfono, Servicios / Stream** y **Servicios / E-Mail**.

Solapa Configuración básica

- **Fuente de vídeo inicial** – configura la fuente de la señal de vídeo inicial. Se puede elegir entre la cámara interna (resp. cámara analógica conectada al intercomunicador) o la

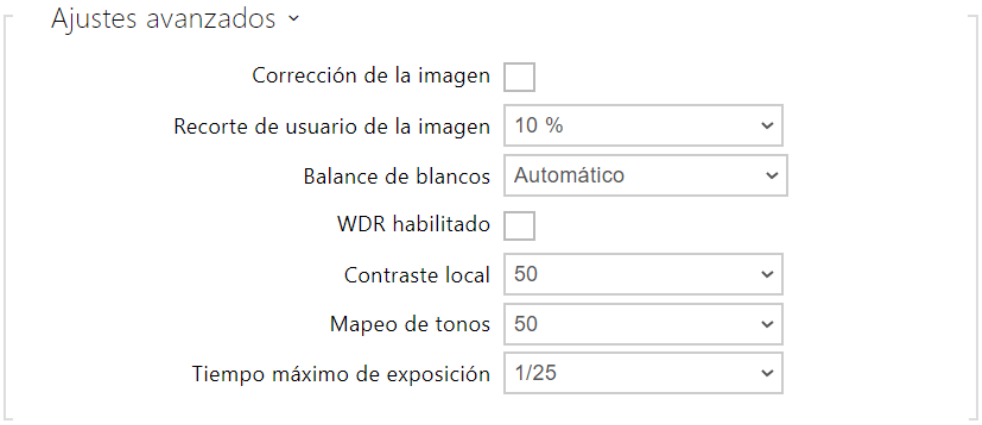
cámara IP externa. El cambio de la fuente de la señal de vídeo inicial se aplica en el stream RTSP y en el caso de utilizar HTTP API. En la aplicación **2N® IP Eye** es necesario elegir la cámara externa manualmente, incluso en el caso de que el dispositivo no tenga la cámara interna y solo esté conectada la externa. En el caso de que al intercomunicador no esté conectada la cámara interna, se puede elegir como la fuente inicial del vídeo solo la cámara IP externa. En el caso de que la cámara externa no esté conectada o configurada correctamente, aparecen símbolos N/A sobre un fondo azul.
- **Vista previa en vivo** – mostrará la ventana con la vista previa en vivo desde la cámara del intercomunicador 2N IP.

Solapa Cámara interna



- **Nivel del brillo** – configura el nivel de brillo de la imagen de la cámara.
- **Nivel de exposición** – Define el nivel de exposición dela imagen (los valores más elevados significan que el dispositivo prefiere un tiempo de exposición más prolongado).
- **Contraste** – define el contraste de la imagen de la cámara. El parámetro está disponible solo en el modelo **2N® IP Style**.
- **Saturación del colores** – configura la saturación de los colores de la imagen de la cámara.
- **Modo de cámara** – permite configurar diferentes modos de captura de imagen según la instalación actual del intercomunicador (uso interno y externo). En el caso de la instalación interna se puede elegir entre diferentes modos de reducción del parpadeo de la imagen causado por las fuentes de luz artificial. En el caso de la instalación externa se puede configurar el modo de reducción de la luz solar directa.
- **Reducción automática de la frecuencia de captura** – habilita la reducción automática de la frecuencia de captura condiciones empeoradas de iluminación con lo cual mejorará la calidad de la imagen a cambio de la frecuencia reducida de captura.

- **Recorte de la imagen** – el ángulo de visión de la cámara del intercomunicador **2N® IP Force** está configurado de manera que la cámara abarque el mayor espacio posible. Este parámetro le permite configurar el recorte automático de la imagen de la cámara de manera que no se vea el marco del dispositivo, lo cual en algunos casos puede ser molesto. En el caso de que desee tener el máximo ángulo de visión, apague esta función. Este parámetro está disponible solo en el modelo **2N® IP Force**.
- **Modo de noche/día** – configura el modo de control del modo de día y de noche de la cámara. Es posible configurar el modo automático (controlado por el nivel de la luz ambiental), eventualmente el modo de noche o día permanentes.
- **Modo actual** – muestra el modo actualmente seleccionado de la cámara (día/noche). En el modo de día la cámara utiliza un filtro supresor de la radiación infrarroja y la iluminación adicional infra está apagada. En modo de noche. En el modo de noche se elimina el filtro supresor de la radiación infrarroja y se activa la iluminación adicional infra.
- **Nivel de la iluminación adicional infrarroja** – permite configurar el nivel de la iluminación adicional infrarroja en el rango de 0 hasta 100 % en varios pasos. La iluminación adicional infrarroja se enciende automáticamente en el modo de noche. La configuración del nivel de iluminación adicional está disponible solo en el modelo **2N® IP Style, 2N® IP Verso** y **2N® IP Force** con cámara HD.
- **Nivel actual de la iluminación adicional** – muestra el nivel actual de la iluminación adicional infrarroja en % del nivel máximo. El nivel puede reducirse automáticamente debajo del valor configurado de manera que no se produzca el exceso del consumo máximo posible desde la fuente de alimentación (normalmente por ej. en el caso de conexión de un número más elevado de los módulos de ampliación y alimentaciones mediante PoE).
- **Vista previa en vivo** – mostrará la ventana con la vista previa en vivo desde la cámara del intercomunicador 2N IP.

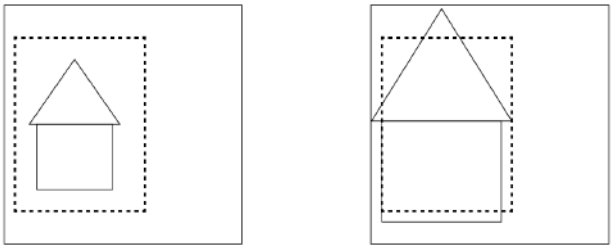


El grupo de funciones Ajustes avanzados es válida para los modelos del intercomunicador **2N® IP Style**.

- **Corrección de la imagen** – configura las correcciones digitales (rectificación) de la imagen de la cámara interna del dispositivo.
- **Recorte de usuario de la imagen** – configura el recorte centrado inicial de la imagen (los bordes están recortados de forma uniforme).
- **Balance de blancos** – la configuración del balance de blancos según la fuente predominante de luz es recomendable en el caso de que no baste con el balance de blancos automático (la elección inadecuada del balance de blancos deriva en coloración indeseada de la imagen).
- **WDR habilitado** – es recomendable encender WDR (Wide Dynamic Range) en el caso de que en la escena haya zonas muy oscuras y a la vez zonas muy iluminadas. WDR asegurará la visibilidad de toda la escena.
- **Contraste local** – al configurar un nivel más alto se resaltará el contraste de los contornos de las partes claras y oscuras de la escena.
- **Mapeo de tonos** – al configurar un nivel más alto resaltará la imagen y mejorará la visibilidad (en tal caso los colores de la imagen pueden resultar distorsionados).
- **Tiempo máximo de exposición** – configura el tiempo máximo durante el cual se expone y se crea cada imagen. En el caso de que haya disponible más luz, no es necesario que el diafragma esté abierto todo el tiempo y la cámara ajusta automáticamente el tiempo más corto de la exposición actual.

Precaución

- Tras cambiar la configuración del parámetro Recorte de usuario de la escena en el dispositivo con procesador ARTPEC-7 hay que revisar el límite de la zona para la zona de detección del movimiento y la zona de la protección de privacidad, cuyo espacio cambiará, ver la ilustración.



Nota

- *Esta configuración está disponible solo en los modelos equipados con las entradas para la cámara analógica externa.*

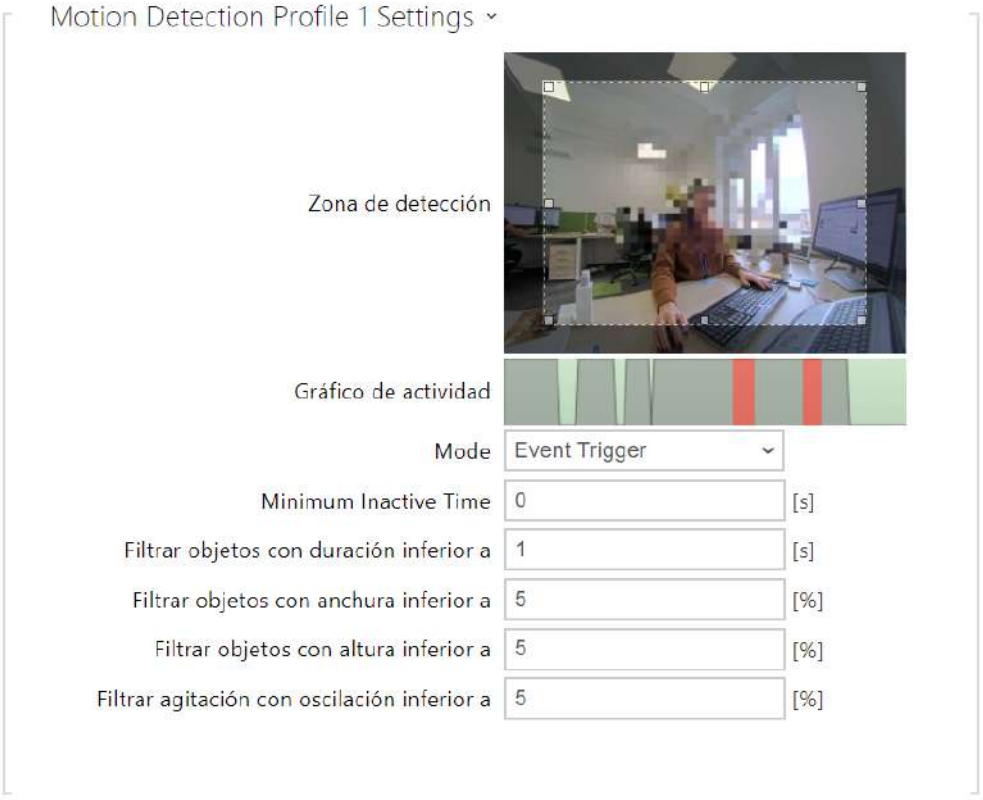
- **Entrada de vídeo** – permite elegir una de las dos entradas para la conexión de la cámara analógica. También es posible modificar la entrada durante la operación mediante la automatización con la acción Action.SetCameraInput.
- **Estándar de vídeo** – permite configurar el estándar de vídeo de la cámara conectada. Modifique el valor del parámetro solo en el caso de que no funcione correctamente la detección automática del estándar de vídeo (valor Auto).

- **Detección de movimiento encendida** – permite encender la detección automática de movimiento desde la imagen de la cámara interna. El movimiento se detecta mediante la observación del cambio del elemento del brillo en la parte determinada de la imagen durante un período de tiempo. Con el movimiento de los objetos en la toma de la cámara se produce cambio de una parte determinada de la imagen – actividad que se puede expresar en porcentaje. En el caso de que la actividad supere el umbral superior configurado de sensibilidad, se indica el movimiento. El movimiento se indica hasta que la actividad no baje por debajo del umbral inferior configurado de sensibilidad. Los umbrales de sensibilidad se pueden configurar según los requisitos, instalación concreta y de la misma manera se puede configurar la zona de detección (sección en la que se está vigilando la actividad).

- **Umbral de sensibilidad** – permite configurar el umbral inferior y superior y la histéresis del algoritmo de la detección de movimiento.
- **Zona de detección** – permite configurar una sección rectangular en el cual se realiza la detección de movimiento.
- **Gráfico de actividad** – muestra el historial de la actividad detectada (cambios del elemento del brillo de la imagen) junto con el umbral inferior y superior de sensibilidad.

Detección del movimiento y protección de privacidad para el dispositivo con el procesador ARTPEC-7

- **Detección de movimiento – perfil 1/2 encendida** – permite encender la detección automática de movimiento desde la imagen de la cámara interna.. El movimiento se detecta mediante la observación del cambio del elemento del brillo en la parte determinada de la imagen durante un período de tiempo. Al haber movimiento de los objetos en la toma de la cámara se produce el cambio de una parte determinada de la imagen. En el caso de que la actividad supere el umbral superior de sensibilidad, se indica el movimiento. El movimiento se indica hasta que la actividad no baje por debajo del umbral inferior de sensibilidad.



- **Zona de detección** – permite configurar una sección rectangular en el cual se realiza la detección de movimiento.
- **Gráfico de actividad** – muestra el historial de la actividad detectada en el eje temporal. Verde significa que no hay movimiento, gris significa el movimiento detectado, pero no cumple las condiciones, rojo significa el movimiento detectado que cumple las condiciones.
- **Modo** – el modo de ejecución de sucesos está diseñado de manera que genere los sucesos breves de la detección del movimiento para las acciones como por ej. carga de imágenes. El modo de carga está diseñado de manera que genere los sucesos más largos, por ej. para la carga mediante ONVIF.

- **Tiempo mínimo de inactividad** – configura el tiempo mínimo entre dos sucesos de detección del movimiento. Eso impide la creación de muchos sucesos rápidamente seguidos uno tras otro.
- **Filtrar objetos con duración inferior a** – configura en segundos el tiempo mínimo necesario durante el cual debe registrarse continuamente el movimiento para que se notifique el suceso de detección del movimiento. El rango de configuración está entre 1 y 5 seg. El movimiento debe cumplir también otras condiciones establecidas en esta sección.
- **Filtrar objetos con anchura inferior a** – configura la anchura mínima de los objetos, en relación con toda la anchura de la imagen de la cámara, que debe tener el objeto para que se notifique el suceso. El rango de configuración está entre 3 y 100 %. El movimiento debe cumplir también otras condiciones establecidas en esta sección.
- **Filtrar objetos con altura inferior a** – configura la altura mínima de los objetos, en relación con toda la altura de la imagen de la cámara, que debe tener el objeto para que se notifique el suceso. El rango de configuración está entre 3 y 100 %. El movimiento debe cumplir también otras condiciones establecidas en esta sección.
- **Filtrar agitación con oscilación inferior a** – configura la amplitud de oscilación mínima de los objetos agitados en relación con toda la anchura, respectivamente la altura del la imagen de la cámara, que deben superar los objetos para que se detecte el objeto (la configuración no influye de ninguna manera sobre los objetos no agitados). El rango de configuración está entre 3 y 20 %. El movimiento debe cumplir también otras condiciones establecidas en esta sección.

Precaución

- En los dispositivos con el procesador ARTPEC-7 se evalúan los objetos móviles también fuera de la zona activa, incluidos los filtros configurados (en el caso de utilizar el ***Recorte de usuario*** de la imagen se evaluarán también las imágenes en aquellas partes de la imagen que están recortadas y el usuario no las ve en la vista previa). Los objetos que entran en la zona activa luego generan el suceso del movimiento detectado. Por ejemplo en el caso del ajuste del filtro de tiempo a 5 s, el objeto que se mueve fuera de la zona activa durante 10 s generará el suceso del movimiento detectado inmediatamente después de la entrada en la zona activa debido a que ya había cumplido la condición fuera de la zona activa. El objeto se seguirá detectando incluso al abandonar la zona activa y al entrar de nuevo en la zona activa generará inmediatamente el suceso (en el caso de que no abandone por completo la zona de la imagen de la cámara y no quede 'olvidado').

- **Protección de privacidad habilitada** – habilita la función de la protección de privacidad la cual enmascara una parte de la imagen con el color elegido o con el mosaico.

- **Modo de ocultación** – legt die Farbe oder das Mosaik des abgedeckten Bereichs fest.
- **Grosor del mosaico** – configura el grosor del mosaico en la zona de protección de privacidad.
- **Zona de la protección de privacidad** – configura la posición y tamaño de la zona de protección de privacidad.

Precaución

- La protección de la privacidad puede limitar la actividad de otras funciones, por ej. lectura de códigos QR o detección de movimiento. Desaconsejamos utilizar la protección de la privacidad a la vez con las funciones mencionadas.

Solapa Cámara externa

- **Cámara externa habilitada** – habilita la descarga de transmisión RTSP desde la cámara IP externa. Para un funcionamiento correcto es necesario introducir la dirección válida del stream RTSP, eventualmente el nombre de usuario y contraseña.
- **Dirección del stream RTSP** – dirección del stream RTSP de la cámara IP en el formato rtsp://ip_dirección_cámara/parámetros. Los parámetros son específicos para el modelo determinado de la cámara IP conectada. En el caso de que utilice como cámara externa otro intercomunicador **2N IP**, utilice la dirección en el formato http://dirección_ip/mjpeg_stream o http://dirección_ip/h264_stream.

Parámetro	Descripción	Ejemplo / valores
vcodec	Códec de vídeo	vcodec=h264 para el código H.264 vcodec=mjpeg para el código MJPEG
vres	Resolución del vídeo	vres=1920x1080 para FullHD
fps	Frecuencia de cuadro del vídeo	fps=15 (de 1 hasta 30 fps, el valor máximo posible para el códec de vídeo MJPEG es de 15 fps)
vbr	Bitrate	vbr=768 para 768 kbps
audio	Audio	• audio=1 (habilitado) • audio=0 (deshabilitado)
zipstream	Zipstream	• zipstream=off (deshabilitado) • zipstream=low • zipstream=medium • zipstream=high • zipstream=higher

- **Nombre de usuario** – nombre del usuario para la autenticación de la conexión a la cámara IP externa. El parámetro es obligatorio solo en el caso de que la cámara IP externa requiera la autenticación.
- **Contraseña** – contraseña para la autenticación de la conexión a la cámara IP externa. El parámetro es obligatorio solo en el caso de que la cámara IP externa requiera la autenticación.
- **Puerto local para RTP** – configura el puerto local UDP para la recepción del stream RTP.

Consejo

- FAQ: Cámara externa – ¿Cómo configurarla en el intercomunicador 2N IP?

En la ventana Vista previa de la cámara se muestra la imagen actual recibido de la cámara externa. En el caso de que la cámara externa no esté conectada o configurada correctamente, aparecen símbolos N/A sobre un fondo azul.

En la ventana Comunicación de la cámara IP externa se muestra el transcurso de la comunicación RTSP con la cámara IP externa configurada, incluidos los posibles errores y estados de fallo.

5.5.4 Teclado

Esta parte de la configuración sirve para configurar las funciones del teclado numérico y de los botones del marcado rápido. Los **intercomunicadores 2N IP** permiten:

- utilizar el teclado numérico para llamar introduciendo el número virtual del usuario,
- utilizar el teclado numérico para introducir el código de acceso, por ej. para abrir la cerradura de la puerta,
- configurar la función de la tecla #,
- configurar el límite de tiempo al introducir los códigos y números de teléfono,
- elegir la función de los botones y teclas conectadas a **2N® IP Audio/Video Kit**.

Disposición del teclado

Los modelos de los intercomunicadores **2N® IP Audio Kit** y **2N® IP Video Kit** están equipados con ocho bornes para la conexión de botones o teclado externos y permiten conectar hasta 16 botones. La función de cada uno de los botones se puede configurar de forma independiente.

Los botones están organizados en una matriz de 4 columnas x 4 líneas, ver la imagen siguiente, y con ello corresponde también su configuración.

La configuración inicial de los botones está especificado en la imagen siguiente.

A cada posición de la matriz puede asignar una de las funciones – tecla del teclado numérico 0 hasta 9, *, # o uno de los botones de marcado rápido 1–16.

5.5.5 Retroiluminación

En esta solapa se puede configurar de forma independiente la retroiluminación de las etiquetas con nombre, botones, event. nivel del brillo de las LED de señalización.

En el caso de que el intercomunicador esté equipado con un sensor del nivel de la luz de entorno, seleccionará automáticamente el nivel adecuado de la retroiluminación dentro del rango de los valores configurados. Los intercomunicadores determinados permiten controlar de forma independiente el nivel de retroiluminación de las etiquetas con nombre (botones) y de los LED de señalización (por ej. pictogramas retroiluminados). Ver las tablas siguientes:

Característica/ Modelo	2N® IP Style	2N® IP Verso/ LTE Verso	2N® IP Solo	2N® IP Base	2N® IP Vario	2N® IP Force	2N® IP Safety	2N® IP Uni	2N® IP Audio Kit	2N® IP Video Kit
Control del nivel de la retroiluminación	**Sí**			**Sí**	**Sí**				No	
Sensor del nivel de la luz del entorno	**Sí**			No	No				No	

Característica/ Modelo	2N® IP Style	2N® IP Verso/ LTE Verso	2N® IP Solo	2N® IP Base	2N® IP Vario	2N® IP Force	2N® IP Safety	2N® IP Uni	2N® IP Audio Kit	2N® IP Video Kit
Control independiente del nivel de la retroiluminación de las etiquetas y de los LED de señalización	**Sí**			**Sí**	No				No	

La configuración de los parámetros en el grupo Retroiluminación es válida para la retroiluminación de la unidad principal, botones y módulos adicionales.

Las configuraciones de los parámetros en el grupo de LED de señalización son válidos para los LED de señalización de los módulos de extensión de **2N® IP Verso**.

- **Intensidad durante el día** – configura los valores de la intensidad de la retroiluminación durante el día. El valor se define en porcentajes del máximo brillo posible de los LED.
- **Intensidad por la noche** – configura el valor del brillo de los LED por la noche. El valor se define en porcentajes del máximo brillo posible de los LED. En el caso de que los parámetros de la Intensidad durante el día y la Intensidad por la noche estén configurados al mismo valor, el nivel de la luz de entrono no se tendrá en cuenta.
- **Valor actual** – muestra el valor actual elegido automáticamente de la intensidad del LED según el nivel actual detectado de la luz de entorno.

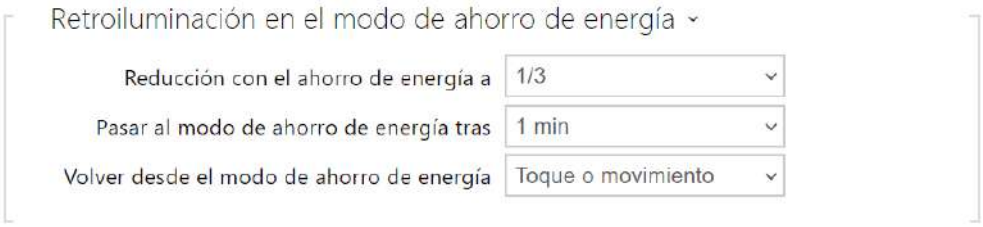
Nota

- La configuración de la intensidad del brillo afecta la funcionalidad, consumo y el aspecto general del dispositivo. Un brillo alto de la retroiluminación de las etiquetas con nombre y botones, en al caso de nivel bajo de la luz alrededor, puede causar el deslumbramiento de la persona situada frente al intercomunicador, y a la vez aumenta el consumo general del dispositivo. Un brillo bajo de la led de señalización, al utilizar el intercomunicador en la luz solar directa, puede provocar la reducción del contraste entre la LED apagada y la encendida y dificultar el reconocimiento del estado de la LED.

Configuración de la retroiluminación de la pantalla del intercomunicador 2N® IP Style

Las configuraciones de los parámetros en los grupos de Retroiluminación y Retroiluminación en el modo de ahorro de energía son válidos para la retroiluminación de la pantalla y para los LED de ambiente.

- **Intensidad en modo activo durante el día** – configura el valor máximo del brillo de la retroiluminación durante el día (el valor está controlado por el sensor de la luz de entorno). El valor se define en porcentajes del máximo brillo posible.
- **Intensidad en modo activo durante la noche** – configura el valor máximo del brillo de la retroiluminación durante la noche (el valor está controlado por el sensor de la luz de entorno). El valor se define en porcentajes del máximo brillo posible.
- **Valor actual** – muestra el valor actual elegido automáticamente de la intensidad del LED según el nivel actual detectado de la luz de entorno.



- **Reducción con el ahorro de energía a** – nivel de la reducción de la intensidad de retroiluminación en el caso de que el dispositivo pase al modo de inactividad.
- **Pasar al modo de ahorro de energía tras** – configura el tiempo de inactividad del dispositivo (es decir, el tiempo durante el cual no se realiza la interactuación con el dispositivo) tras el cual se realiza el cambio automático al modo de ahorro de energía. El valor se define en segundos dentro del rango entre 1 y 600.
- **Volver desde el modo de ahorro de energía** – configura las formas de interacción mediante las cuales es posible interrumpir el modo de ahorro de energía. Es posible elegir entre el tacto en la pantalla y el tacto o detección del movimiento. Además, el dispositivo siempre pasa del modo de ahorro de energía en el caso de autenticación del usuario, llamada entrante y otros estados de funcionamiento.

Las configuraciones de los parámetros en el grupo de LED de señalización son válidos para los LED de señalización (retroiluminación del lector de **2N® IP Style**).

- **Intensidad por el día** – ajusta el valor del brillo de las LED de señalización durante el día. El valor se define en porcentajes del máximo brillo posible de los LED.
- **Intensidad por la noche** – ajusta el valor del brillo de las LED de señalización durante la noche. El valor se define en porcentajes del máximo brillo posible de los LED. En el caso de que los parámetros de la Intensidad durante el día y la Intensidad por la noche estén configurados al mismo valor, el nivel de la luz de entrono no se tendrá en cuenta.
- **Valor actual** – muestra el valor actual elegido automáticamente de la intensidad del LED según el nivel actual detectado de la luz de entorno.

5.5.6 Pantalla

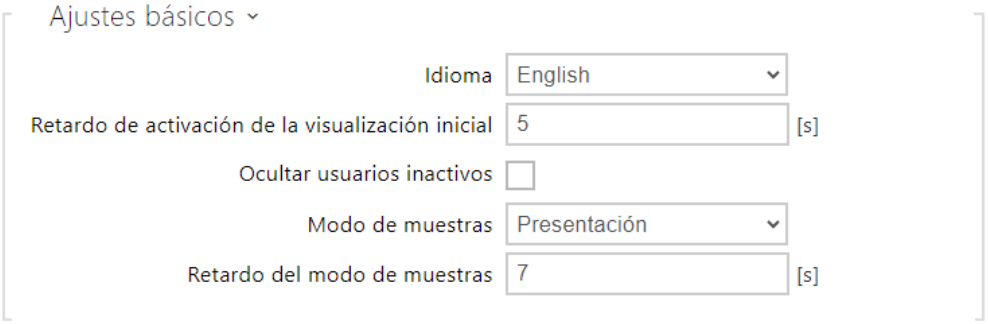
Algunos modelos del intercomunicador **2N® IP Vario** event. **2N® IP Verso** pueden estar equipados con una pantalla LED de color. En la pantalla se muestra el estado del dispositivo (por ej. el progreso de la llamada, apertura de la puerta) y la pantalla puede trabajar a la vez en varios modos:

Pantalla – en el caso de que **2N® IP Vario** permita la función de la pantalla y la configuración del idioma. En **2N® IP Verso** permite la configuración básica y la configuración de idioma.

Presentación – tras un tiempo configurado de inactividad puede aparecer en la pantalla la presentación en forma de una serie de imágenes grabadas. El cambio de las imágenes es automático y el tiempo de visualización se puede configurar.

Solapa Pantalla (solo modelos 2N® IP Vario)

- **Botón del teclado para introducir el código** – enciende la visualización del teclado en la pantalla para introducir los códigos numéricos.
- **Modo del teclado para introducir el código** – configura el modo del teclado en la pantalla para introducir los códigos numéricos. Los modos son teclado normal o teclado con teclas mezcladas para aumentar la seguridad. La configuración tiene su aplicación también en el caso de la autenticación múltiple.



- **Idioma** – configura el idioma de los textos visualizados en la pantalla. Se puede elegir uno de los idiomas pre-definidos – inglés, checo, alemán, italiano, francés, español, ruso, finlandés, danés, polaco, neerlandés, portugués, turco, noruego, sueco o idioma definido por el usuario (custom).
- **Retardo de la activación de la visualización inicial** – configura el tiempo máximo de inactividad de la pantalla (es decir, cuando la pantalla no es controlada a través de los botones del teclado numérico), después de este tiempo surge el regreso de la lista telefónica al modo de visualización de las etiquetas con nombres, en el caso de que estén configuradas. En el caso contrario aparecerá la pantalla por defecto con el logotipo 2N.
- **Ocultar usuarios inactivos** – tras marcarlo oculta automáticamente en la pantalla al usuario que tiene activo el perfil de tiempo, el cual impide que sea contactado.
- **Modo de muestras** – configura si el dispositivo pasa al modo de muestras durante la inactividad. Es posible seleccionar diferentes comportamientos en el modo de muestras (Apagado, Presentación).
- **Retardo de la activación del modo de muestras** – configura el intervalo de tiempo en caso de inactividad en el rango entre 1 hasta 600 segundos, el tiempo después de cual el dispositivo pasará al modo de muestras. Siempre está configurado el timeout fijo de 15 segundos, el tiempo entes del cual el dispositivo volverá a la pantalla de inicio.

- **Idioma original** – permite descargar una plantilla del archivo de localización para realizar su propia traducción. Se trata de archivo XML con todos los textos mostrados en la pantalla.
- **Idioma de usuario** – permite cargar, eliminar y descargar un archivo de localización propio.
- **Fuente de usuario** – permite cargar, eliminar y descargar una fuente propia para los textos mostrados en la pantalla. El archivo debe estar en formato TTF y no debe superar los 4 MB.

> **Nota**
>
> En el caso de que no le convenga ninguno de los idiomas pre-definidos de la pantalla, proceda de la siguiente manera:
> - descargue el archivo de idioma original (está en inglés),
> - modifique el texto mediante el editor de texto (sustituya los textos en inglés por sus propios textos),
> - vuelva a cargar el archivo de localización modificado al intercomunicador,
> - configure el parámetro **Configuración del idioma | Idioma** al valor **propio**,
> - revise los textos directamente en la pantalla del intercomunicador y modifíquelos en caso de necesidad.

En el caso de que no le convenga el aspecto gráfico inicial de las etiquetas con nombre, podrá cargar al intercomunicador su propio fondo de etiquetas con nombre. La imagen tiene que tener la resolución de 320 x 240 píxeles. En el caso de que cargue al intercomunicador su propia imagen de etiquetas con nombre, el aspecto original de las etiquetas con nombre será sustituido, aunque la asignación de los usuarios a cada uno de los botones se conservará.

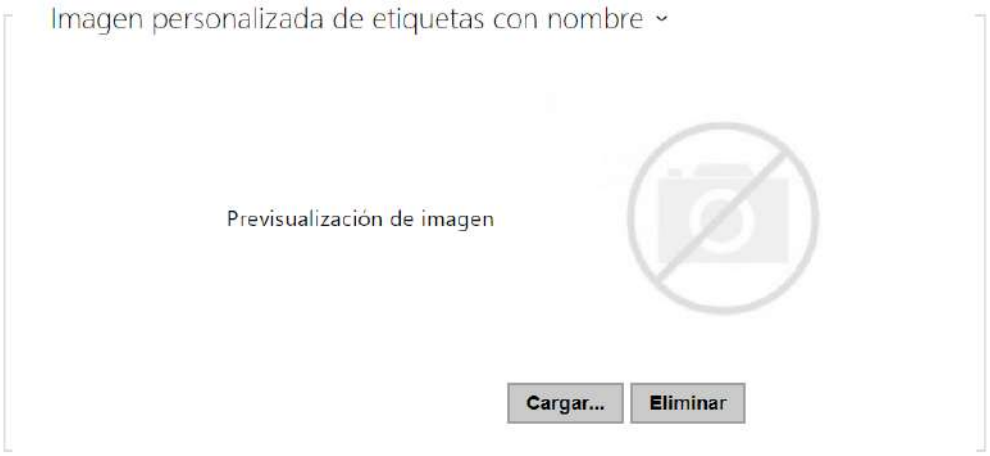
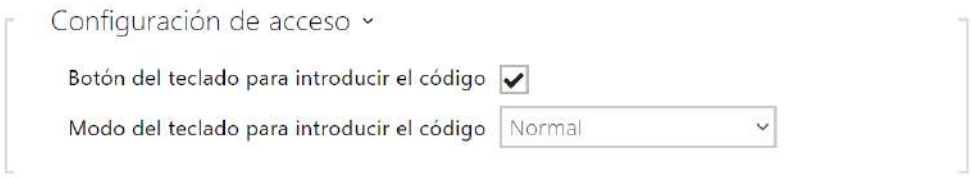
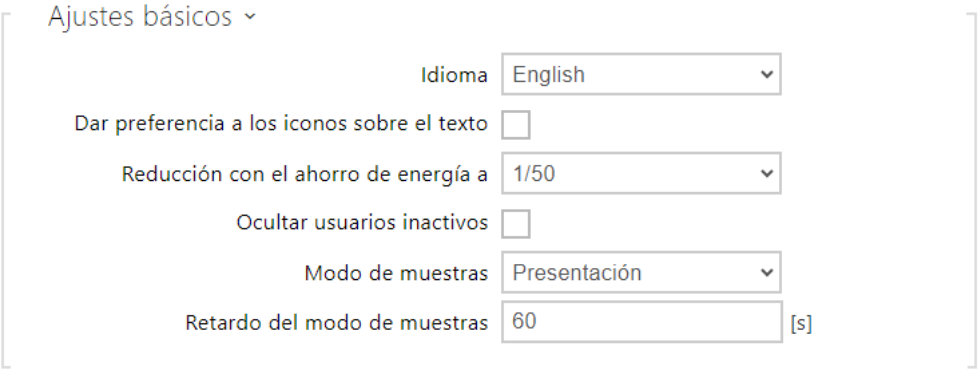


Imagen personalizada de etiquetas con nombre
Previsualización de imagen
Cargar...
Eliminar

Solapa Pantalla (solo modelos 2N® IP Verso)

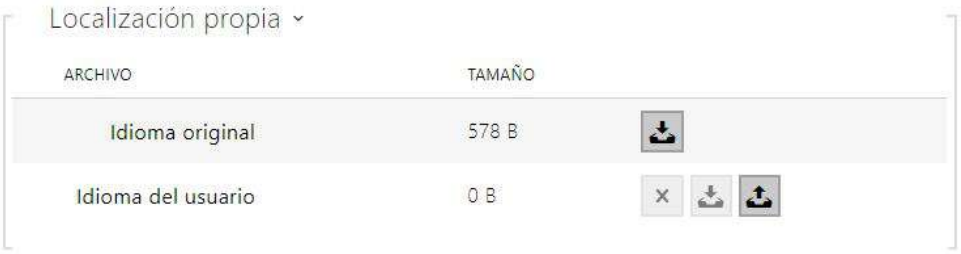


- **Botón del teclado para introducir el código** – enciende la visualización del teclado en la pantalla para introducir los códigos numéricos.
- **Modo del teclado para introducir el código** – configura el modo del teclado en la pantalla para introducir los códigos numéricos. Los modos son teclado normal o teclado con teclas mezcladas para aumentar la seguridad. La configuración tiene su aplicación también en el caso de la autenticación múltiple.



- **Idioma** – configura el idioma de los textos visualizados en la pantalla. Se puede elegir uno de los idiomas pre-definidos – inglés, checo, alemán, italiano, francés, español, ruso, finlandés, danés, polaco, neerlandés, portugués, turco, noruego, sueco o idioma definido por el usuario (custom).
- **Dar preferencia a los iconos sobre el texto** – los iconos en la pantalla tendrán preferencia sobre el texto.
- **Modo de ahorro de energía** – permite activar el modo de ahorro con el cual se reduce el brillo de la pantalla. En el caso de que no se produzca ningún suceso durante dos Retardos de activación de la presentación, la activación de modo de ahorro ha transcurrido satisfactoriamente. El modo de ahorro está apagado en el caso de que en el campo para el Retardo de activación de la presentación esté el número 0. Con el movimiento delante de la cámara del intercomunicador o en el caso de cualquier suceso en la pantalla (por ej. activación de la cerradura de la puerta, o contacto con la pantalla), la pantalla pasa al brillo total.
- **Ocultar usuarios inactivos** – tras marcarlo oculta automáticamente en la pantalla al usuario que tiene activo el perfil de tiempo, el cual impide que sea contactado.
- **Modo de muestras** – configura si el dispositivo pasa al modo de muestras durante la inactividad. Es posible seleccionar diferentes comportamientos en el modo de muestras (Apagado, Presentación).

- **Retardo de la activación del modo de muestras** – configura el intervalo de tiempo en caso de inactividad en el rango entre 1 hasta 600 segundos, el tiempo después de cual el dispositivo pasará al modo de muestras. Siempre está configurado el timeout fijo de 15 segundos, el tiempo entes del cual el dispositivo volverá a la pantalla de inicio.



- **Idioma original** – permite descargar una plantilla del archivo de localización para realizar su propia traducción. Se trata de archivo XML con todos los textos mostrados en la pantalla.
- **Idioma de usuario** – permite cargar, eliminar y descargar un archivo de localización propio.

ⓘ En el caso de que no le convenga ninguno de los idiomas pre-definidos de la pantalla, proceda de la siguiente manera:
- descargue el archivo de idioma original (está en inglés),
- modifique el texto mediante el editor de texto (sustituya los textos en inglés por sus propios textos),
- vuelva a cargar el archivo de localización modificado al intercomunicador,
- configure el parámetro **Configuración del idioma / Idioma** al valor **propio**,
- revise los textos directamente en la pantalla del intercomunicador y modifíquelos en caso de necesidad.

Solapa Presentación modelos 2N® IP Verso

En esta solapa se configura la lista de imágenes y vídeos mostrados en el modo de presentación. Se puede cargar hasta 8 imágenes/vídeos que cambian progresivamente con el retardo configurado.

- **Intervalo de transición** – configura el tiempo de visualizado de una imagen de la presentación antes de pasar a otra imagen.
- **Perfil de tiempo** – ofrece la elección de uno o varios perfiles de tiempo a la vez que se aplicarán. La propia configuración de los perfiles de tiempo se puede realizar en la sección Directorio / Perfiles de tiempo.
  -  con la marca se configura la elección de los perfiles de tiempo pre-definidos o la configuración manual del perfil de tiempo para el elemento determinado.

La resolución de las imágenes/vídeos cargados debería ser de 214 x 214 o 214 x 320 píxeles hasta el tamaño máximo de 2 MB.
En el caso contrario se adaptarán de forma automática a la resolución de la pantalla.

Para la vista previa de la imagen cargada sirve el icono de la lupa  , la imagen se puede eliminar mediante el icono  , el icono  permite ocultar la vista previa de la imagen o del vídeo determinado en la pantalla del dispositivo. La visualización se puede condicionar por el perfil de tiempo  haciendo clic en el icono variable  de la imagen de vídeo. En el caso de que el perfil de tiempo no esté activo la presentación no incluirá el contenido condicionado por el perfil de tiempo. La presentación incluirá en el mismo caso siempre el contenido que no está condicionado por el perfil de tiempo. En el caso de que no haya ninguna imagen cargada, el modo de presentación no se activará jamás.

Consejo

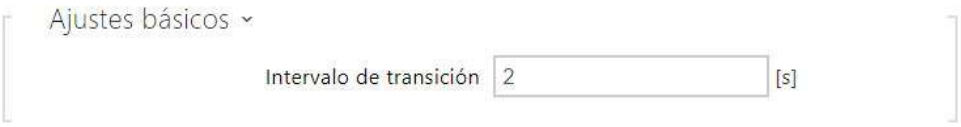
- Para ocultar la parte visualizada "Toque para comenzar" en la pantalla del modelo **2N® IP Verso** es necesario cargar una imagen de 214 x 320 píxeles de resolución.

Precaución

- En las versiones de FW inferiores a 2.35 no se pueden cargar vídeos con 214 x 320 de resolución.

Solapa Presentación modelos 2N® IP Vario

En esta solapa se configura la lista de imágenes mostradas en el modo de presentación. Se puede cargar hasta 8 imágenes que cambian progresivamente con el retardo configurado.



- **Paso entre las imágenes de la presentación** – configura el tiempo de visualizado de una imagen de la presentación antes de pasar a otra imagen.

La resolución de las imágenes cargadas debería ser de 320 x 240 píxeles. En el caso contrario se adaptarán de forma automática a la resolución de la pantalla.

Para la vista previa de la imagen cargada sirve el icono de la lupa, la imagen se puede eliminar mediante el icono, el icono permite ocultar la vista previa de la imagen o del vídeo determinado en la pantalla del dispositivo.

En el caso de que no haya ninguna imagen cargada, el modo de presentación no se activará jamás.

Precaución

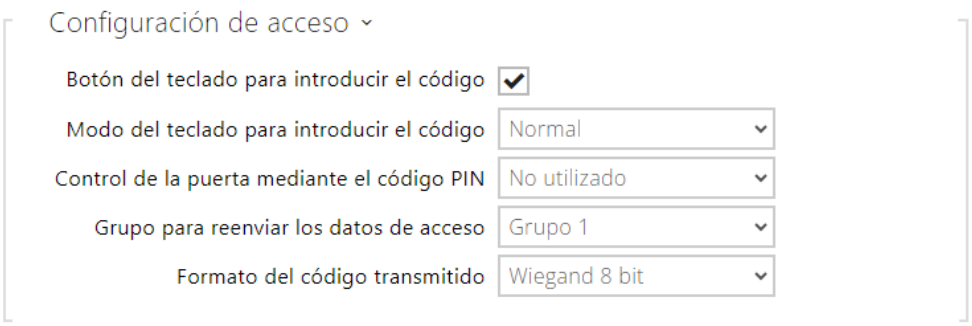
- **2N® IP Vario** soporta solo la visualización de imágenes.

5.5.6.1 Pantalla 2N® IP Style

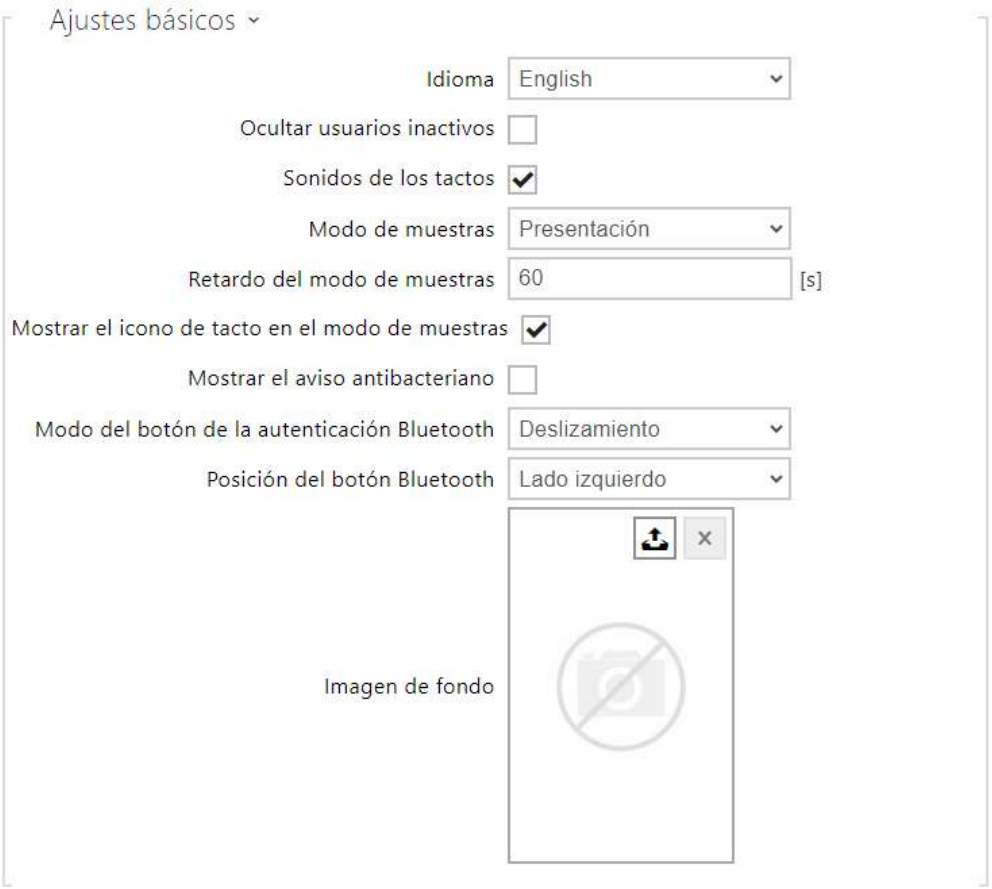
El intercomunicador 2N IP **2N® IP Style** está equipado con pantalla LCD de color de 10″ con 800 x 1280 de resolución. En la pantalla se muestra el estado del dispositivo (por ej. el progreso de la llamada, apertura de la puerta) y la pantalla puede trabajar a la vez en varios modos:

- **Pantalla** – muestra el directorio con usuarios a los que se puede llamar, y el teclado numérico para el acceso mediante el código.
- **Presentación** – tras un tiempo configurado de inactividad puede aparecer en la pantalla la presentación en forma de una serie de imágenes grabadas. El cambio de las imágenes es automático y el tiempo de visualización se puede configurar.
- **Logo** – tras el tiempo establecido de inactividad se puede en la pantalla visualizar el logotipo cargado en la configuración del dispositivo.
- **Dirección** – tras el tiempo establecido de inactividad puede aparecer en la pantalla la dirección y el número de casa, eventualmente otro identificador del lugar.
- **Fecha y hora** – permite configurar los parámetros de la fecha, hora y el tiempo.
- **Mensaje de bienvenida** – permite configurar el mensaje que aparecerá en la pantalla tras una autenticación satisfactoria.

Solapa Pantalla



- **Botón del teclado para introducir el código** – enciende la visualización del teclado en la pantalla para introducir los códigos numéricos.
- **Modo del teclado para introducir el código** – configura el modo del teclado en la pantalla para introducir los códigos numéricos. Los modos son teclado normal o teclado con teclas mezcladas para aumentar la seguridad. La configuración tiene su aplicación también en el caso de la autenticación múltiple.
- **Control de la puerta mediante el código PIN** – Permite o prohíbe el control de la puerta mediante la introducción del código PIN desde la pantalla.
- **Grupo para reenviar datos de acceso** – le permite establecer un grupo al que se reenviarán todos los códigos de acceso de usuario recibidos.
- **Formato de los códigos transmitidos** – elección del formato de 4bit y 8bit (mayor fiabilidad) de los códigos transmitidos.



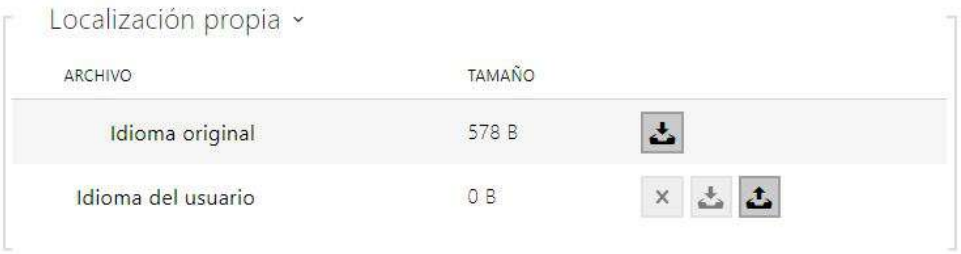
- **Idioma** – configura el idioma de los textos visualizados en la pantalla. Se puede elegir uno de los idiomas pre-definidos – inglés, checo, alemán, italiano, francés, español, ruso, finlandés, danés, polaco, neerlandés, portugués, turco, noruego, sueco o idioma definido por el usuario (custom).
- **Ocultar usuarios inactivos** – tras marcarlo oculta automáticamente en la pantalla al usuario que tiene activo el perfil de tiempo, el cual impide que sea contactado.
- **Sonidos de los tactos** – activa la señalización sonora de los tactos en la pantalla.
- **Modo de muestras** – configura si el dispositivo pasa al modo de muestras durante la inactividad. Es posible seleccionar diferentes comportamientos en el modo de muestras (Apagado, Presentación, Logotipo, Dirección, Fecha y hora).
- **Retardo del modo de muestras** – configura el tiempo de inactividad tras el cual el dispositivo pasa al modo de muestras en el rango entre 1 hasta 600 segundos.

Aviso

- El dispositivo tiene establecido de forma fija el retorno a la página inicial de la pantalla tras 60 segundos de inactividad. PUna vez transcurrido este tiempo empieza la cuenta atrás del tiempo establecido en este parámetro y luego el dispositivo pasará al modo de muestras.

- Tras 2 minutos de inactividad se activa en el dispositivo **2N® IP Style** el salvapantallas con el cual se reduce y aumenta el brillo de la pantalla de forma intermitente en intervalos de 20 segundos. El salvapantallas se cancela al tocar la pantalla, intentando el acceso, con una llamada entrante, al mostrarse una notificación en la pantalla o al detectar el movimiento incluso en el caso de que la función de la detección de movimiento no esté habilitada. En el caso de que el salvapantallas se esté ejecutando en el fondo del modo de muestras, al cancelar el salvapantallas con un toque el dispositivo cambiará a la vez a la pantalla de inicio.

- **Permitir el icono de tacto en el modo de muestras** – permite la visualización del icono de tacto (mano pulsante) en el modo de muestras.
- **Mostrar el aviso antibacteriano** – permite mostrar la información sobre la capa antibacteriana aplicada en la pantalla (accesorio opcional para 2N® IP Style) a lo largo del tiempo durante el cual está el dispositivo en el modo de muestras.
- **Modo del botón de la autenticación Bluetooth** – configura si el botón de la activación de la autenticación Bluetooth se activa con el deslizamiento o con el contacto. La configuración tendrá efecto en el momento cuando en el entorno de **2N® IP Style** no se encuentre ningún teléfono con la aplicación Mobile Key.
  - **Deslizamiento** – para activar la cerradura arrastre el botón desde la izquierda a la derecha en la pantalla.
  - **Contacto** – para activar la cerradura pulse el botón .
- **Posición del botón Bluetooth** – configura la posición del botón de la autenticación Bluetooth. La configuración tendrá efecto en el momento cuando en el entorno de IP Style no se encuentre ningún teléfono con la aplicación Mobile Key.
- **Imagen de fondo** – permite cargar la imagen de fondo (utilizada en diferentes páginas en la pantalla). El archivo debe ser una imagen con la resolución mínima de 800 x 1280 píxeles. Las imágenes con una resolución mayor se reducirán.



- **Idioma original** – permite descargar una plantilla del archivo de localización para realizar su propia traducción. Se trata de archivo XML con todos los textos mostrados en la pantalla.

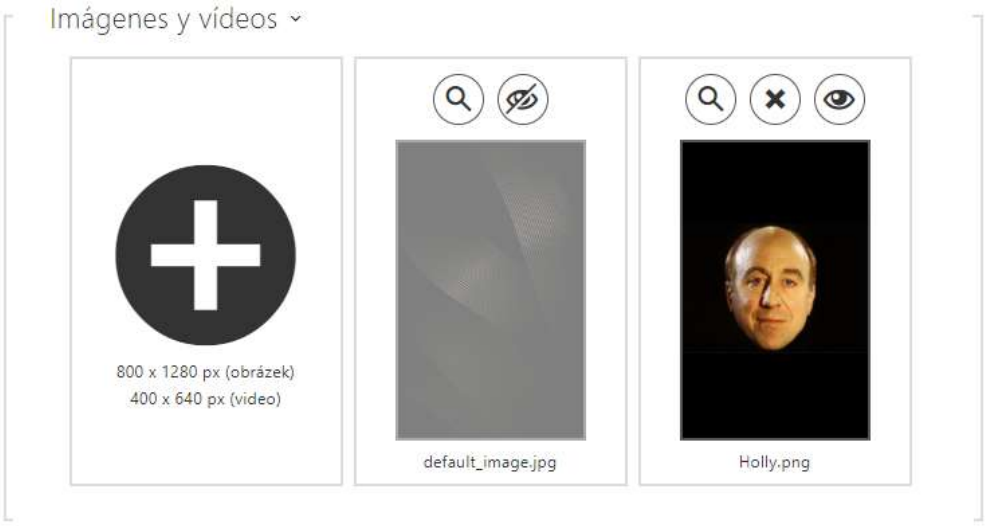
- **Idioma de usuario** – permite cargar, eliminar y descargar un archivo de localización propio.

> ⓘ En el caso de que no le convenga ninguno de los idiomas pre-definidos de la pantalla, proceda de la siguiente manera:
> - descargue el archivo de idioma original (está en inglés),
> - modifique el texto mediante el editor de texto (sustituya los textos en inglés por sus propios textos),
> - vuelva a cargar el archivo de localización modificado al intercomunicador,
> - configure el parámetro **Configuración del idioma / Idioma** al valor **propio**,
> - revise los textos directamente en la pantalla del intercomunicador y modifíquelos en caso de necesidad.

Solapa Presentación

En esta solapa se configura la lista de imágenes y vídeos mostrados en el modo de presentación. Se puede cargar hasta 14 imágenes/vídeos que cambian progresivamente con el retardo configurado.

- **Intervalo de transición** – configura el tiempo de visualizado de una imagen de la presentación antes de pasar a otra imagen.
- **Perfil de tiempo** – ofrece la elección de uno o varios perfiles de tiempo a la vez que se aplicarán. La propia configuración de los perfiles de tiempo se puede realizar en la sección Directorio / Perfiles de tiempo.
  -  con la marca se configura la elección de los perfiles de tiempo pre-definidos o la configuración manual del perfil de tiempo para el elemento determinado.



El tamaño de las imágenes cargadas debería ser 800 x 1280 píxeles para los modelos **2N® IP Style**. En el caso contrario se adaptarán de forma automática a la resolución de la pantalla.

Los archivos de vídeo deben tener la resolución de 400 x 640 px, tamaño máximo de 7 MB y framerate máximo de 24 fps.

Para la vista previa de la imagen cargada sirve el icono de la lupa, la imagen se puede eliminar mediante el icono, el icono permite ocultar la vista previa de la imagen o del vídeo determinado en la pantalla del dispositivo. La visualización se puede condicionar por el perfil de tiempo haciendo clic en el icono variable de la imagen de vídeo. En el caso de que el perfil de tiempo no esté activo la presentación no incluirá el contenido condicionado por el perfil de tiempo. La presentación incluirá en el mismo caso siempre el contenido que no está condicionado por el perfil de tiempo. En el caso de que no haya ninguna imagen cargada, el modo de presentación no se activará jamás.

Aviso

- Las muestras "Presentación" tendrán efecto en la pantalla solo al habilitar el modo determinado en el menú Hardware / Pantalla / Pantalla.

Solapa Logotipo

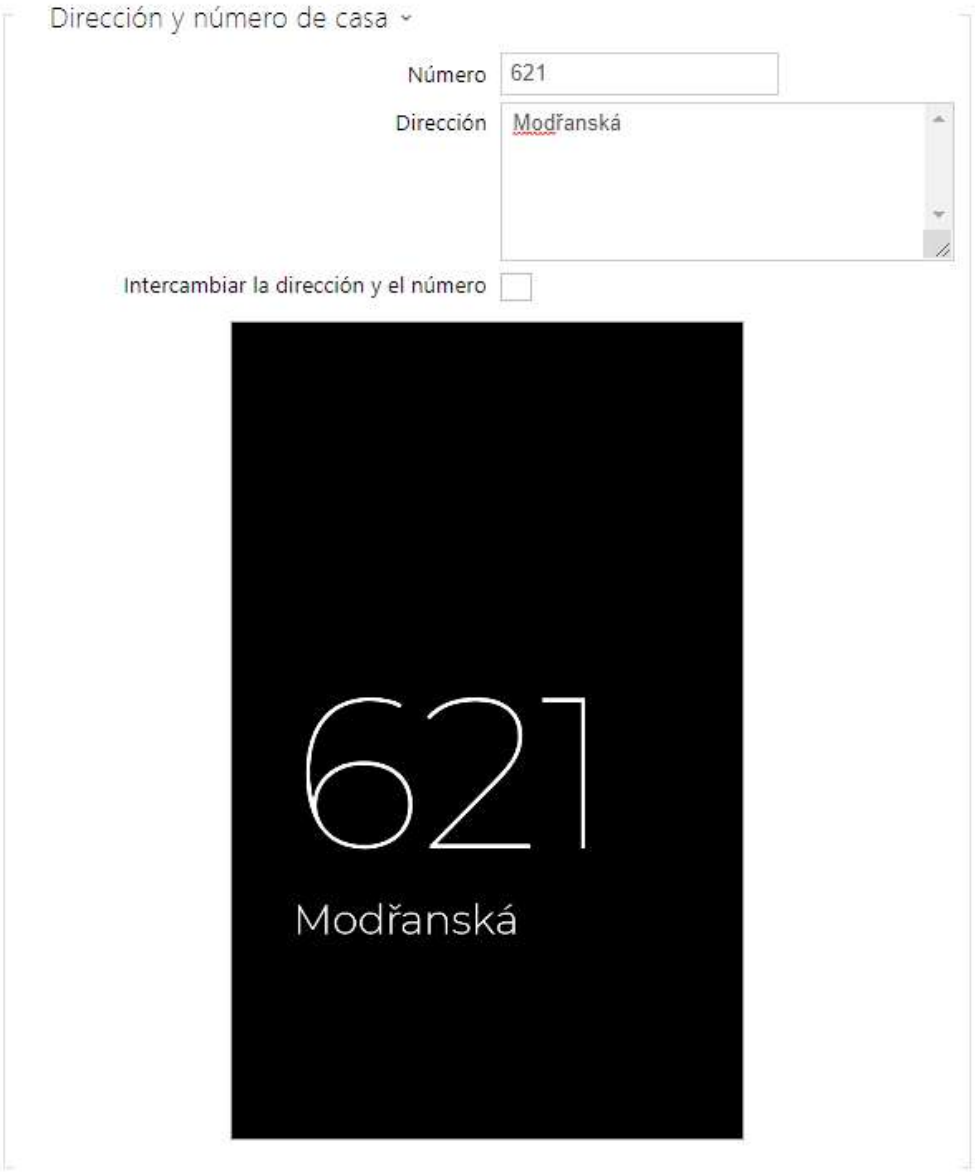
Permite cargar el logotipo para el modo de muestras. La imagen con resolución mayor a 800 x 1280 píxeles se reducirá. El archivo más pequeño permanecerá pequeño y no ocupará toda la pantalla. Se soportan también imágenes en formato PNG con fondo transparente.

Aviso

- La muestra "Logotipo" tendrá efecto en la pantalla solo al habilitar el modo determinado en el menú Hardware / Pantalla / Pantalla.

Solapa Dirección

Permite configurar la dirección de la casa u otro identificador para el modo de muestras que se mostrará en la pantalla durante el tiempo de inactividad del dispositivo.



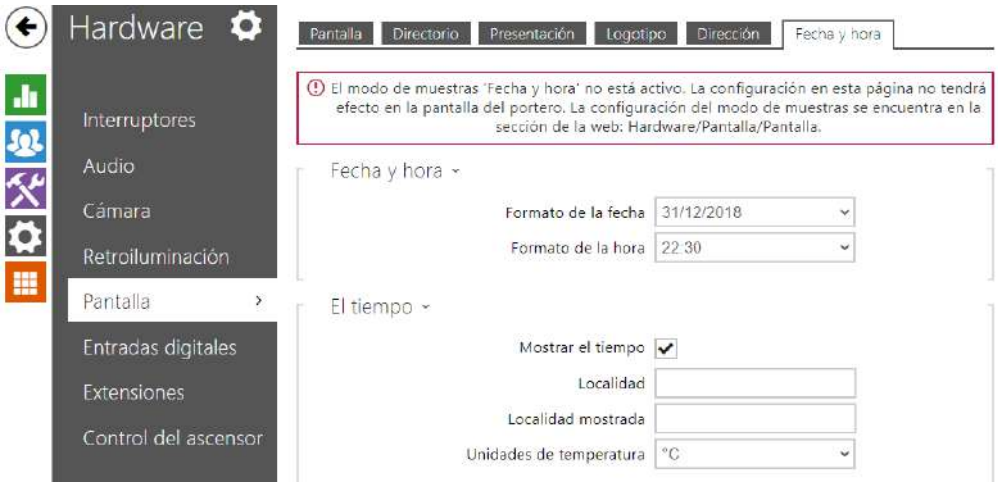
- **Número** – permite introducir el número de casa, o eventualmente otra identificación según las costumbres locales. Aparece en el modo de muestras en el caso de la opción Dirección.
- **Dirección** – permite introducir la dirección, nombre del edificio, etc. que aparece en el modo de muestras en el caso de la opción Dirección.
- **Intercambiar la dirección y el número** – intercambia el orden de visualización del número y de la dirección.

Aviso

- La muestra "Direccioón" tendrá efecto en la pantalla solo al habilitar el modo determinado en el menú Hardware / Pantalla / Pantalla.

Fecha y hora

Permite configurar los parámetros de la fecha, hora y el tiempo.



- **Formato de la fecha** – configuración del formato de la fecha visualizada en la pantalla del dispositivo.
- **Formato de la hora** – configuración del formato de la hora visualizada en la pantalla del dispositivo.

El tiempo

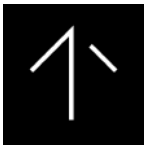
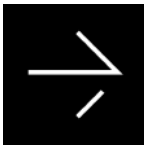
- **Mostrar el tiempo** – en la pantalla del dispositivo irá apareciendo la información sobre el tiempo actual.
- **Localidad** – localidad, en la cual se encuentra este dispositivo, para la previsión del tiempo. En el caso de que no esté introducida, se utilizará automáticamente la localidad determinada.
- **Localidad mostrada** – localidad mostrada en la pantalla. En el caso de que no esté introducida, aparece la localidad de la previsión del tiempo.
- **Unidades de temperatura** – elección de unidades de temperatura mostrados en la pantalla. Las opciones son °C y °F.

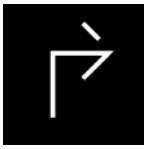
Mensaje de bienvenida

	
Imagen peronalizada	Mensaje de texto

Permite configurar el mensaje que aparecerá en la pantalla tras una autenticación satisfactoria.

- **Modo de la pantalla de bienvenida** – elija el tipo del contenido del mensaje de bienvenida.
- **Hora de la visualización** – configura el tiempo durante el cual el dispositivo mostrará el mensaje de bienvenida.
- **Icono** – elija un icono para el mensaje de texto de bienvenida. Se puede elegir entre los siguientes iconos:

		
Info	Aviso	Entrada prohibida
		

Flecha hacia la izquierda	Flecha hacia arriba	Flecha hacia la derecha
		
Flecha girar a la izquierda	Flecha hacia abajo	Flecha girar a la derecha

- **Título del mensaje** – configura el título del mensaje de texto de bienvenida.
- **Cuerpo del mensaje** – configura el cuerpo del mensaje de texto de bienvenida.
- **Confirmación** – configura si el mensaje de texto de bienvenida tenga el botón 'OK'.
- **Cargar una imagen personalizada** – cargue la imagen que se mostrará como un mensaje de bienvenida. La imagen debe tener la resolución de 800 x 1280 px y el formato JPEG o PNG.

5.5.7 Lector de tarjetas

Este menú está disponible solo en los modelos de intercomunicadores **2N® IP Base**, **2N® IP Vario** y **2N® IP Force**. En el modelo **2N® IP Verso** se configura aquí solo la opción de limitar los accesos fallidos de acceso. Las demás funciones se configuran en la sección **Módulos de ampliación**.

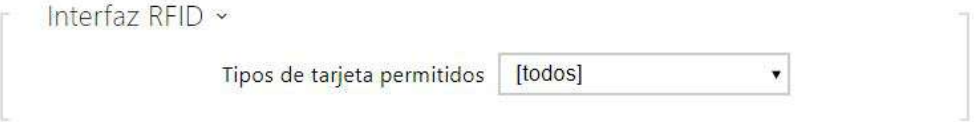
El lector de tarjetas permite el control efectivo de acceso en el edificio mediante las tarjetas sin contacto RFID. El tipo de las tarjetas soportadas depende del modelo concreto del lector utilizado.

Los lectores de tarjetas para los modelos **2N® IP Vario** y **2N® IP Force** están equipados con la interfaz Wiegand. Esta interfaz puede funcionar como de entrada o de salida. El sentido de la interfaz es configurable. En el modo de entrada se puede utilizar la interfaz para conectar los lectores externos de tarjetas, huellas dactilares, biometría, etc. En el modo de salida se puede gracias a esta interfaz conectar el intercomunicador, por ej. a la centralita de seguridad, y enviar los ID de las tarjetas acercadas desde el lector de tarjetas interno a esta centralita.

Configuración básica

- **Puerta** – configura la dirección del paso en el caso del uso del lector (Entrada, Salida). El parámetro dirección es utilizado por el sistema de presencia.
- **Interruptor asociado** – configura el número del interruptor activado tras acercar la tarjeta RFID válida. El valor configurado no se aplicará en el caso de acercar una tarjeta válida del usuario cuando está a la vez configurada la función de autenticación doble de este usuario. En tal caso se espera, tras acercar la tarjeta válida, la introducción del código numérico para la activación del interruptor y este código numérico identifica al interruptor activado a continuación.

Interfaz RFID



- **Tipos de tarjeta permitidos** – permite elegir uno o varios tipos aceptados de tarjetas. En el caso de que no se seleccione ningún tipo, se aceptarán todos los tipos de tarjetas soportadas.

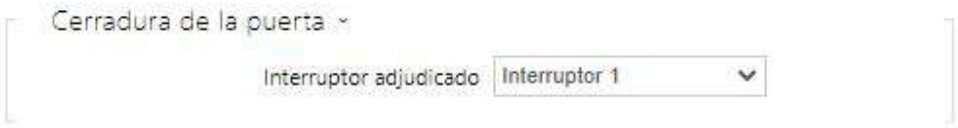
Interfaz Wiegand

- **Modo de interfaz** – permite activar la función de la interfaz wiegand y configurar la interfaz como de entrada o de salida. Siempre cuando la interfaz wiegand esté configurado como de salida, se le reenviarán los ID de las tarjetas acercadas al lector interno.
- **Puerta** – configura la dirección del paso en el caso del uso del lector (Entrada, Salida). El parámetro dirección es utilizado por el sistema de presencia.
- **Formato de los códigos recibidos** – configura el formato de los códigos recibidos (Wiegand 26, 32, 37 y RAW).
- **Formato de los códigos transmitidos** – configura el formato de los códigos transmitidos (Wiegand 26, 32, 37 y RAW).
- **Cambiar el código Facility** – permite configurar la primera parte del código a través de la interfaz Wiegand. Afecta al modo de salida de la interfaz para el formato del código transmitido 26 bit. Contacte con el proveedor de sus sistema de seguridad para verificar si se requiere Facility Code.
- **Código Facility** – determina la localización del intercomunicador **2N IP** en el sistema de seguridad. Introduzca el valor decimal de la localización (0–255).

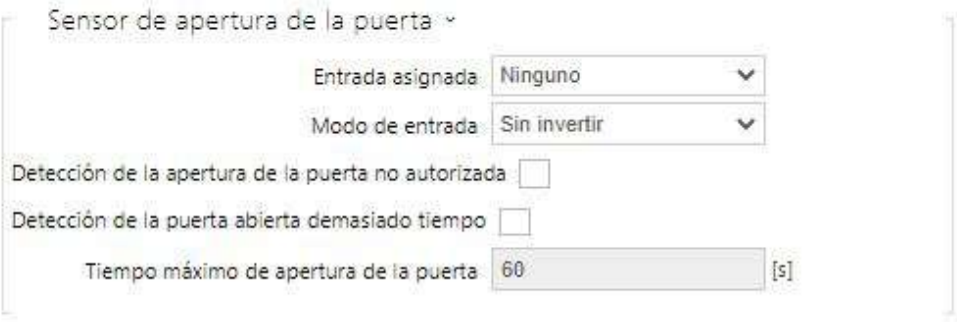
5.5.9 Entradas digitales

En esta parte de la configuración del intercomunicador puede configurar los parámetros relacionados con las entradas digitales y su conexión con otras funciones del intercomunicador. La estradas digitales están disponibles solo en modelos determinados de los intercomunicadores, event. tras la instalación del accesorio adecuado (por ej. lector de tarjetas).

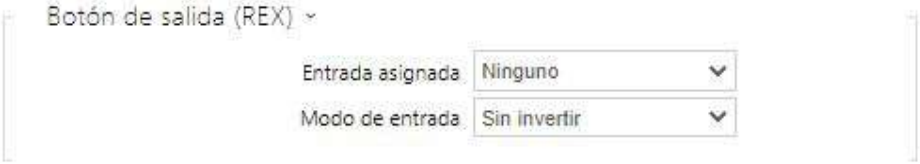
Solapa Puerta



- **Interruptor asignado** – permite elegir el interruptor destinado para el control de la cerradura electromagnética de la puerta. Por el estado de este interruptor se controla la señalización del desbloqueo de la puerta (símbolo verde de la puerta, LED verde).

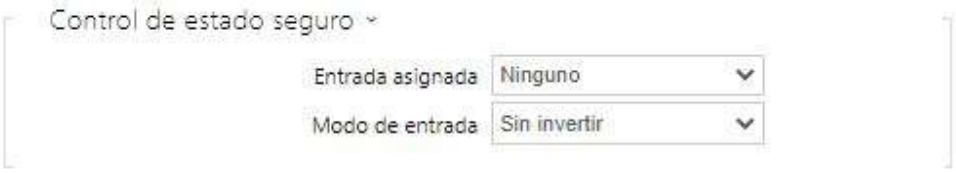


- **Entrada asignada** – permite determinar una de las entradas lógicas (event. ninguna entrada) para la detección de la puerta abierta.
- **Modo de entrada** – permite configurar el nivel activo (polaridad) de la entrada. No invertido / Invertido.
- **Detección de la apertura no autorizada de la puerta** – permite detectar la apertura de la puerta con la cerradura bloqueada.
- **Detección de la puerta abierta mucho tiempo** – permite detectar la puerta abierta durante mucho tiempo.
- **Tiempo máximo de la puerta abierta** – tiempo máximo permitido de la puerta abierta en segundos.



- **Entrada asignada** – permite especificar una de las entradas lógicas (event. ninguna entrada) para la función del botón de salida. La activación de la entrada del botón de salida implica la activación del interruptor seleccionado. El tiempo y el método de activación se basan en la configuración actual del interruptor seleccionado.
- **Modo de entrada** – permite configurar el nivel activo (polaridad) de la entrada. No invertido / Invertido.

Solapa Seguridad



- **Entrada asignada** – permite determinar uno una (event. ninguna) entrada lógica para la señalización del estado "Asegurado". El estado "Asegurado" se señaliza luego mediante la LED roja en el intercomunicador (cuya posición varía según el tipo del intercomunicador).
- **Modo de entrada** – permite configurar el nivel activo (polaridad) de la entrada.

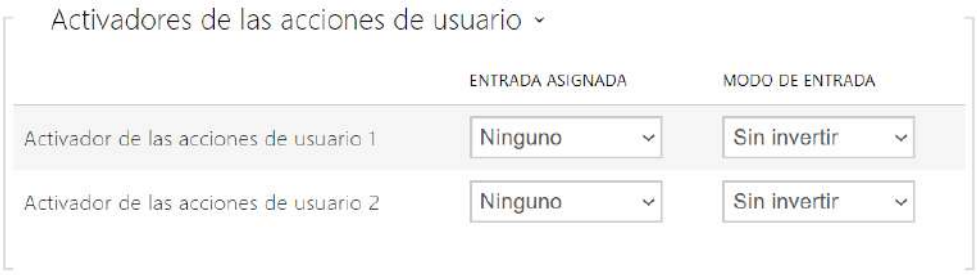
> **Nota**
>
> - *La señalización del estado asegurado se utiliza normalmente en relación con la centralita de seguridad conectada a una de las entradas digitales del intercomunicador. El conductor tendido desde la centralita está conectado directamente, o mediante el módulo de ampliación, al intercomunicador. La posición de las LED de señalización del estado asegurado varía según cada modelo de intercomunicador:*
>
> *Los intercomunicadores **2N® IP Vario** (91371…U) están equipados con una LED de señalización roja situada en el centro de las etiquetas con nombre retroiluminadas.*
> *Los intercomunicadores **2N® IP Force** están equipados con una LED de señalización roja situada en la ventana del lector de tarjetas instalado*
> *Los intercomunicadores **2N® IP Verso** están equipados con un pictograma de candado rojo en la esquina superior izquierda del módulo básico*

Los modelos equipados con un interruptor antisabotaje permiten detectar la apertura de la cubierta del dispositivo y señalizar esta situación como suceso **TamperSwitchActivated**. Los sucesos se registran en el log que se puede leer mediante HTTP API (ver el manual HTTP API).

En el caso de que la función esté habilitada, tras la activación del tamper se bloquearán todos los interruptores durante 30 minutos. El bloqueo seguirá activo incluso tras el reinicio del dispositivo. Cada puerto se puede controlar mediante **Automation**. El desbloqueo de los interruptores se puede realizar mediante el botón **Desbloquear**, prohibiendo esta función o restaurando la configuración de fábrica.

- **Entrada asignada** – permite elegir la entrada lógica a la que está conectado el interruptor antisabotaje. Tras la activación del interruptor antisabotaje se señaliza el suceso **TamperSwitchActivated**.
- **Permitir el bloqueo automático de los interruptores** – bloqueará los interruptores mediante la activación del tamper durante 30 minutos.
- **Estado del bloqueo de los interruptores** – muestra y permite configurar el bloqueo de los interruptores.

Solapa Activadores



- **Activador de las acciones de usuario 1, 2**
  - **Entrada asignada** – permite elegir la entrada lógica que cumplirá la función de la acción de usuario. En el caso de que la función esté activada, en la lista de sucesos en el dispositivo se registra el suceso UserActionActivated con el parámetro state=in (desactivación de la función está indicada mediante state=out). En base de este suceso pueden, por ejemplo, los sistemas superiores activar la alarma, bloquear todo el edificio o realizar cualquier otra acción.
  - **Modo de entrada** – determinan, si la acción de usuario se evaluará en base del valor invertido de la entrada asignada, o en base del valor normal.

5.5.9 Módulos de ampliación

Los intercomunicadores **2N® IP Verso** y **2N® IP Style** se pueden ampliar mediante los llamados módulos de ampliación conectados a la unidad básica del intercomunicador a través del colector VBUS. Disponibles están los siguientes módulos:

- módulo con cinco botones
- nódulo del teclado
- módulo del infopanel
- módulo del lector de tarjetas
- módulo del lector bluetooth
- módulo de entradas y salidas I/O
- módulo de la interfaz Wiegand
- módulo de la interfaz OSDP
- módulo del bucle inductivo
- módulo de la pantalla
- módulo del lector de huellas dactilares
- módulo del teclado táctil
- módulo del teclado táctil y lector RFID 125 kHz, 13.56 MHz, NFC
- módulo del Bluetooth y lector RFID 125 kHz, 13.56 MHz, NFC
- módulo del teclado táctil y Bluetooth y lector RFID 125 kHz, 13.56 MHz, NFC

Los módulos están conectados entre sí y forman una cadena. Cada módulo tiene su número dado por la posición del orden en la cadena (el primer módulo tiene el número 1). La unidad básica es un caso especial de módulo y tiene el número 0.

La mayoría de los módulos se puede configurar de forma independiente. Los parámetros son específicos para el tipo determinado de módulo.

Precaución

- La detección del módulo conectado no se realiza de forma automática. Reinicie el dispositivo para visualizar el módulo conectado en la lista de los módulos de ampliación.
- En el caso de que la versión de firmware del módulo conectado y de la unidad principal no sean compatibles, el módulo no se detectará. Por eso es necesario, una vez conectados los módulos, actualizar el firmware del dispositivo. El firmware se puede actualizar mediante la interfaz de web del dispositivo en la parte Sistema > Mantenimiento.

Aviso

- Tras cambiar los módulos hay que volver a configurar los módulos nuevos. La configuración está vinculada al número de serie del módulo.

Nota

- Los módulos de ampliación conectados aparecen en el orden correspondiente a su conexión. Los módulos conectados en una posición más alejada de la unidad básica aparecen en la parte más baja de la lista. En el caso de que al intercomunicador estén conectados varios módulos del mismo tipo, puede haber dificultades a la hora de asignar la configuración al módulo concreto. En tal caso es posible identificar los módulos conectados mediante el botón **Localizar el módulo**. Tras pulsar el botón el módulo parpadeará brevemente varias veces.

Aviso

- Tras la conexión del módulo con el lector de tarjetas al dispositivo en el cual están cargadas las claves de lectura de **2N® PICard** habrá que emparejar el módulo con el dispositivo. Sin el emparejamiento el módulo del lector no tendrá el acceso a las claves de lectura y no podrá cargar las tarjetas codificadas. El emparejamiento del módulo se realiza mediante el botón **Emparejar el módulo**.

Aviso

- El nombre del módulo debe ser único.
- En el caso de los módulos que no cuenten con la posibilidad de configuración del nombre, es posible localizarlos mediante la ext <posición_del módulo>.

Consejo

- Al colocar el cursor del ratón en la imagen del módulo aparecerá su información básica de fabricación y del software.

Configuración del módulo de la unidad básica

- **Localizar el dispositivo** – señalización luminosa y sonora del dispositivo concreto. Nota: La señalización óptica se realizará solo en los dispositivos con los elementos de control retroiluminados (Verso, Base, Vario, Force, Safety y Uni). En el caso de que el dispositivo no tenga un reproductor integrado, para reproducir la señal sonora debe estar conectado un reproductor externo (Audio Kit y Video Kit).

Configuración del módulo de teclas

- **Funciones de los botones** – permite asignar a los botones posiciones en la lista de usuarios.

Configuración del módulo del teclado

- **Nombre del módulo** – configura el nombre del módulo. El nombre del módulo se utiliza a la hora de realizar log de sucesos desde el teclado.
- **Puerta** – configura la dirección del paso en el caso del uso del lector (Entrada, Salida). El parámetro de la dirección es utilizado por el sistema de presencia.
- **Reenviar a la salida Wiegand** – configura el grupo de salidas wiegand a la cual se reenviarán todos los botones pulsados.

- **Formato de los códigos transmitidos** – elección del formato de 4bit y 8bit (mayor fiabilidad) de los códigos transmitidos.

Configuración del módulo del infopanel

- Actualmente no está publicado ningún parámetro de esté módulo.

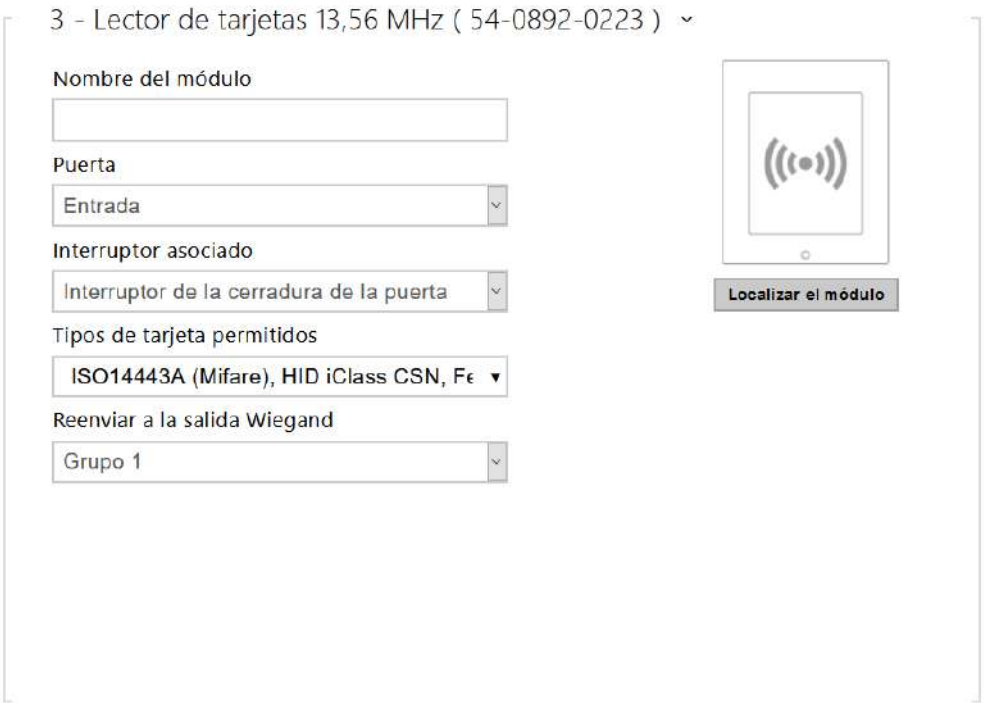
Configuración del módulo del lector de tarjetas 125 kHz

- **Nombre del módulo** – configura el nombre del módulo. El nombre del módulo se utiliza a la hora de realizar log de sucesos desde el teclado.
- **Puerta** – configura la dirección del paso en el caso del uso del lector (Entrada, Salida). El parámetro dirección es utilizado por el sistema de presencia.
- **Interruptor asociado** – configura el número del interruptor activado tras la autenticación del usuario mediante este módulo. En el caso de la configuración de la opción Interruptor de la cerradura de la puerta se aplican las reglas para la autenticación en el menú Hardware / Puerta.
- **Tipos de tarjeta permitidos** – permite configurar el tipo de tarjeta que será aceptado por el lector. El lector soporta en un momento solo un tipo de tarjeta.
- **Reenviar a la salida Wiegand** – configura el grupo de salidas wiegand a la cual se reenviarán todos los ID de las tarjetas RFID.

Consejo

- Para una lectura más rápida de las tarjetas de acceso recomendamos elegir en la configuración del módulo en cuestión solo aquellos tipos de tarjetas que son utilizados por el usuario.

Configuración del módulo del lector de tarjetas 13,56 MHz

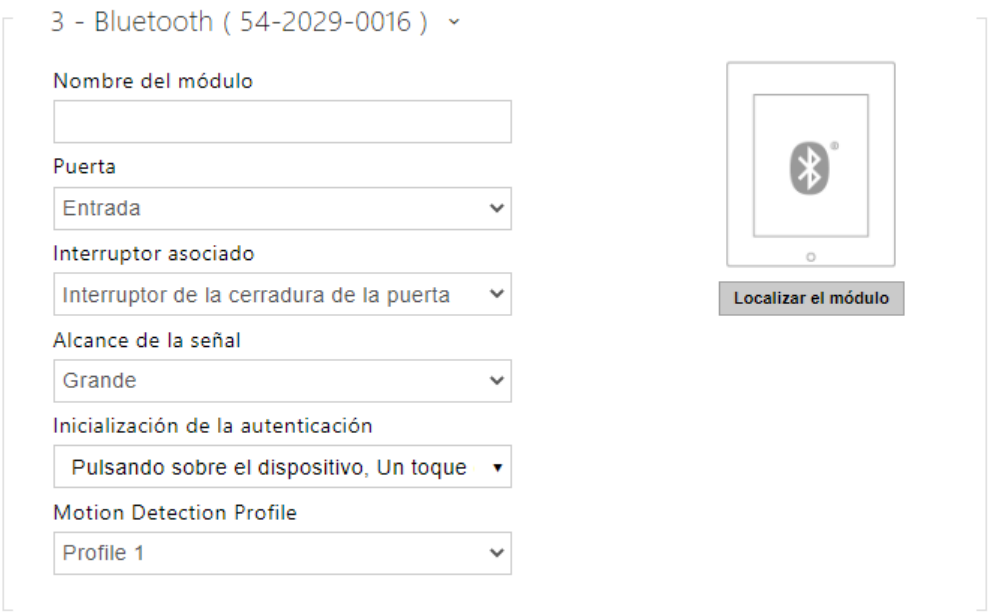


- **Nombre del módulo** – configura el nombre del módulo. El nombre del módulo se utiliza a la hora de realizar log de sucesos desde el teclado.
- **Puerta** – configura la dirección del paso en el caso del uso del lector (Sin especificar, Entrada, Salida). El parámetro dirección es utilizado por el sistema de presencia.
- **Interruptor asociado** – configura el número del interruptor activado tras la autenticación del usuario mediante este módulo. En el caso de la configuración de la opción Interruptor de la cerradura de la puerta se aplican las reglas para la autenticación en el menú Hardware / Puerta.
- **Tipos de tarjeta permitidos** – permite elegir uno o varios tipos aceptados de tarjetas. En el caso de que no se seleccione ningún tipo, se aceptarán todos los tipos de tarjetas soportadas.
- **Compatibilidad NFC con los teléfonos Samsung** – habilita la compatibilidad son los teléfonos Samsung.
- **Reenviar a la salida wiegand** – configura el grupo de salidas wiegand a la cual se reenviarán todos los ID recibidos de las tarjetas RFID.

Consejo

- Para una lectura más rápida de las tarjetas de acceso recomendamos elegir en la configuración del módulo en cuestión solo aquellos tipos de tarjetas que son utilizados por el usuario.

Configuración del módulo bluetooth del lector



- **Nombre del módulo** – configura el nombre del módulo. El nombre del módulo se utiliza a la hora de realizar log de sucesos desde el módulo bluetooth.
- **Puerta** – configura la dirección del paso en el caso del uso del lector (Entrada, Salida). El parámetro dirección es utilizado por el sistema de presencia.
- **Interruptor asociado** – configura el número del interruptor activado tras la autenticación del usuario mediante este módulo. En el caso de la configuración de la opción Interruptor de la cerradura de la puerta se aplican las reglas para la autenticación en el menú Hardware / Puerta.
- **Alcance de la señal** – configura el alcance de la señal (el valor 5 representa el mayor alcance, el valor 1 el menor), es decir, la distancia a la cuál el módulo Bluetooth aún comunicará con el teléfono móvil. A la hora de la configuración se recomienda comprobar el alcance real de la señal, al cual afecta una serie de factores (sobre todo por la disposición espacial de la instalación, teléfono móvil utilizado y su posición).

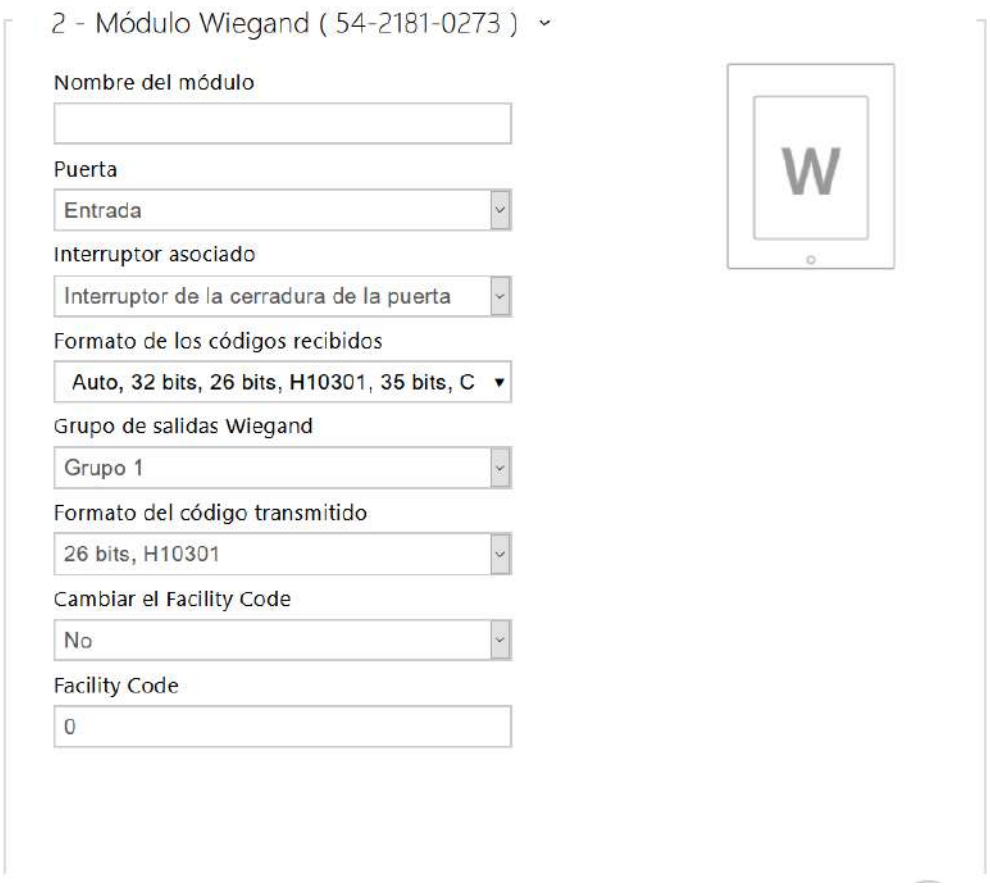
- **Inicialización de la autenticación** – configura la forma de autenticación mediante el teléfono móvil:
  - **Un toque en la aplicación** – hay que confirmar la autenticación picando sobre el icono en la aplicación abierta en el teléfono móvil
  - **Pulsando sobre el dispositivo** – hay que confirmar la autenticación mediante el contacto con el lector en presencia del teléfono con la aplicación emparejada **2N® Mobile Key** .
  - **Detección de movimiento** – la autenticación se activará mediante la detección del movimiento al existir el teléfono con la aplicación **2N® Mobile Key** emparejada.
- **Perfil de la detección de movimiento** – configura el perfil de la detección de movimiento por el cual se regirá el módulo para la autenticación mediante el teléfono móvil.

Configuración del módulo de entradas y salidas I/O

- **Nombre del módulo** – configura el nombre del módulo. El nombre del módulo se utiliza en el caso de especificar la entrada o la salida en los objetos SetOutput, GetInput y InputChanged en la configuración **Automation**.

Configuración del módulo Wiegand

El módulo Wiegand está equipado con la interfaz wiegand de entrada y salida que son independientes la una de la otra, tienen la configuración independiente y pueden recibir y transmitir los códigos a la vez. La interfaz wiegand de entrada se puede utilizar para la conexión de dispositivos externos, como son los lectores de tarjetas RFID, lectores biométricos, etc. Mediante la interfaz wiegand de salida se puede conectar el intercomunicador por ej. al sistema de seguridad en el edificio (se pueden enviar los ID de las tarjetas RFID acercadas al lector RFID conectado, event. los códigos recibidos en cualquier interfaz wiegand de entrada. El módulo Wiegand está además equipado con una entrada lógica y una salida lógica, las cuales se pueden controlar mediante Automation.



- **Nombre del módulo** – configura el nombre del módulo. El nombre del módulo se utiliza en el caso de especificar la entrada o la salida en los objetos SetOutput, GetInput y InputChanged en la configuración **Automation**.
- **Puerta** – configura la dirección del paso en el caso del uso del lector (Entrada, Salida). El parámetro dirección es utilizado por el sistema de presencia.
- **Interruptor asociado** – configura el número del interruptor activado tras la autenticación del usuario mediante este módulo. En el caso de la configuración de la opción Interruptor de la cerradura de la puerta se aplican las reglas para la autenticación en el menú Hardware / Puerta.
- **Formato de los códigos recibidos** – configura el formato de los códigos recibidos (Wiegand 26, 32, 37 y RAW).
- **Grupo de salidas Wiegand** – asigna las salidas wiegand al grupo al que se pueden reenviar los códigos de los lectores de tarjetas conectados, event. entradas wiegand.
- **Formato de los códigos transmitidos** – configura el formato de los códigos transmitidos (26 bit, 32 bit, 37 bit, formato RAW, 35 bit, Corp. 1000, 48 bit, Corp. 1000 y Auto).
- **Cambiar el Facility Code** – permite configurar la primera parte del código a través de la interfaz Wiegand. Afecta al modo de salida de la interfaz para el formato del código transmitido 26 bit. Contacte con el proveedor de sus sistema de seguridad para verificar si se requiere Facility Code.

- **Facility Code** – determina la localización del dispositivo 2N IP en el sistema de seguridad. Introduzca el valor decimal de la localización (0–255).

Configuración del módulo OSDP

El módulo OSDP está equipado con interfaz (de entrada-salida) OSDP (RS-485). Mediante la interfaz OSDP de salida se puede conectar el intercomunicador 2N IP por ej. al sistema de seguridad en el edificio, panel de control (se pueden enviar los ID de las tarjetas RFID acercadas al lector RFID conectado, event. códigos PIN).

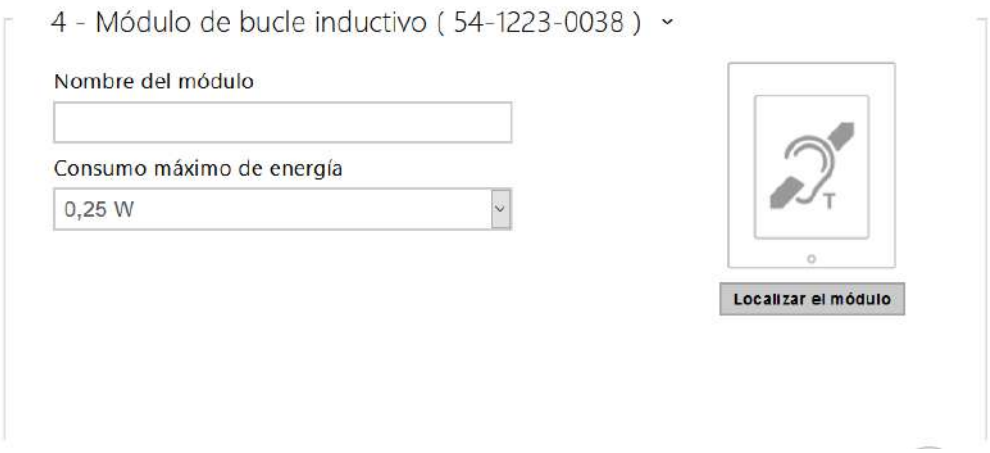
- **Nombre del módulo** – configura el nombre del módulo. El nombre del módulo se utiliza en el caso de especificar la entrada o la salida en la configuración **Automation**.
- **Grupo para reenviar los datos de acceso** – asigna las salidas OSDP al grupo al que se pueden reenviar los códigos de los lectores de tarjetas conectados, event. entradas OSDP.
- **Formato del código transmitido** – configura el formato de los códigos transmitidos.
- **Dirección OSDP** – dirección del módulo OSDP dentro del rango 0–126 en la linea OSDP.
- **Tasa de baudios** – configuración de la tasa de baudios en conformidad con el dispositivo conectado.
- **Clave de codificación** – calve propia para la comunicación codificada.
- **Modo** – para la configuración remota de la clave de codificación en la periferia es posible utilizar el modo de instalación en el caso de que eso esté permitido. Tras ser aceptada la clave de codificación se producirá el cambio automático al modo habitual. El modo de

instalación está señalizado mediante el parpadeo rápido de la LED de señalización en el módulo OSDP.
- **Forzar el cifrado** – configuración de la codificación forzada solo para la comunicación codificada.

Precaución

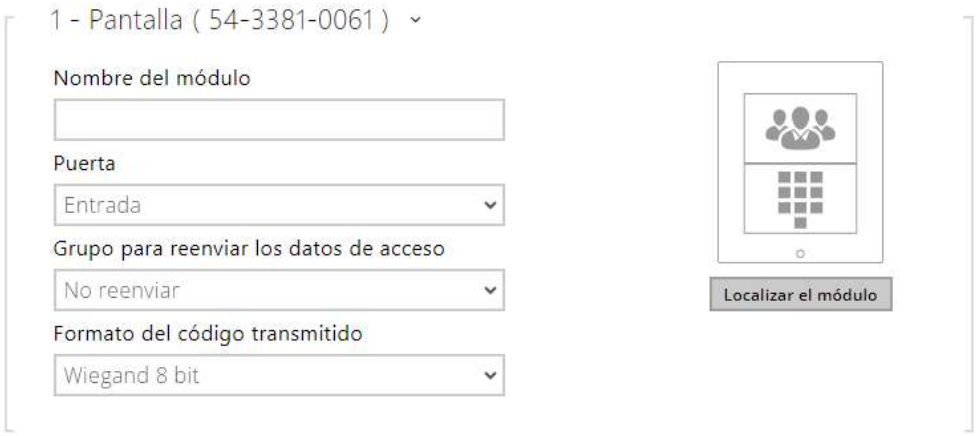
- En el caso de que tras configurar la codificación forzada se produzca la comunicación por parte del dispositivo OSDP en forma no codificada, esta comunicación será rechazada.

Configuración del módulo del bucle inductivo



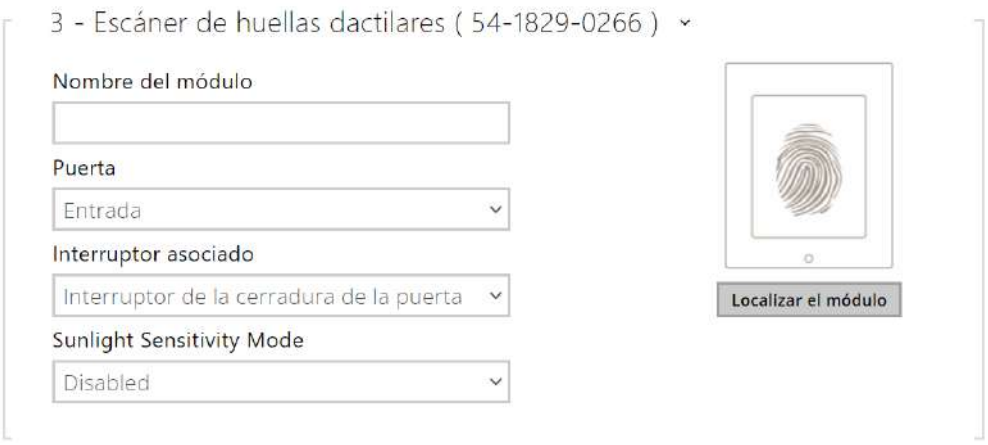
- **Nombre del módulo** – configura el nombre del módulo. El nombre del módulo se utiliza a la hora de realizar log de sucesos del bucle de inducción.
- **Consumo máximo** – configura la máxima potencia de transmisión de la antena del bucle inductivo. Una mayor potencia de transmisión significa un mayor alcance, sin embargo, una menor potencia para las demás funciones del intercomunicador. En circunstancias normales debería ser satisfactorio el valor de 0,25 W.

Configuración del módulo de la pantalla



- **Nombre del módulo** – configura el nombre del módulo. El nombre del módulo se utiliza a la hora de realizar log de sucesos de la pantalla.
- **Puerta** – configura la dirección del paso en el caso del uso del lector (Entrada, Salida). El parámetro dirección es utilizado por el sistema de presencia.
- **Grupo para reenviar datos de acceso** – le permite establecer un grupo al que se reenviarán todos los códigos de acceso de usuario recibidos.
- **Formato de los códigos transmitidos** – elección del formato de 4bit y 8bit (mayor fiabilidad) de los códigos transmitidos.

Configuración del módulo del lector de huellas dactilares



- **Nombre del módulo** – configura el nombre del módulo. El nombre del módulo se utiliza a la hora de realizar log de sucesos del lector de huellas dactilares.
- **Puerta** – configura la dirección del paso en el caso del uso del lector (Entrada, Salida). El parámetro dirección es utilizado por el sistema de presencia.
- **Interruptor asociado** – configura el número del interruptor activado tras la autenticación del usuario mediante este módulo. En el caso de la configuración de la opción Interruptor de la cerradura de la puerta se aplican las reglas para la autenticación en el menú Hardware / Puerta.
- **Sunlight Sensitivity Mode** – Durch die Freigabe wird verhindert, dass das Lesegerät bei direkter Sonneneinstrahlung fehlerhaft arbeitet. Um die Einstellungen zu ändern, muss das Gerät neugestartet werden. Dieser Modus kann zu einer verminderten Leseempfindlichkeit führen.

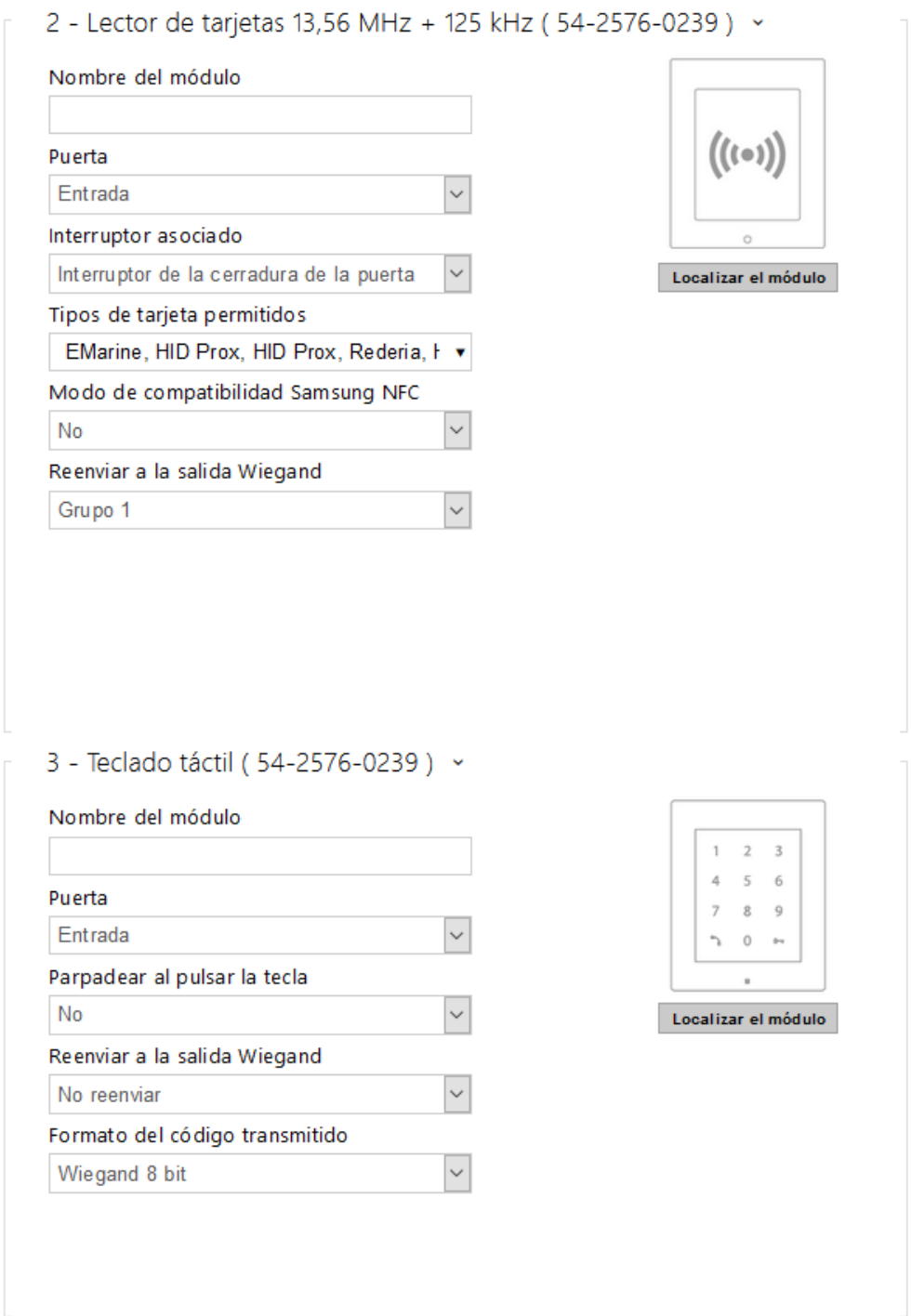
Nota

- Al desconectar el módulo del lector de huellas dactilares, tras el reinicio del dispositivo, en el perfil de usuario en el Directorio, se ocultará la parte Huellas dactilares del usuario que muestra el número de huellas que tiene el usuario grabado en la memoria del intercomunicador. Tras volver a conectar cualquier módulo del lector de huellas dactilares se volverá a mostrar la parte de la configuración del usuario.

Configuración del módulo del teclado táctil

- **Nombre del módulo** – configura el nombre del módulo. El nombre del módulo se utiliza a la hora de realizar log de sucesos desde el teclado táctil.
- **Puerta** – configura la dirección del paso en el caso del uso del lector (Entrada, Salida). El parámetro de la dirección es utilizado por el sistema de presencia.
- **Parpadear al pulsar la tecla** – configura la señalización luminosa mediante el parpadeo que confirma el pulsado de la tecla. Se utiliza en ambientes ruidosos cuando la señalización acústica no se percibe claramente.
- **Reenviar a la salida Wiegand** – configura el grupo de salidas wiegand a la cual se reenviarán todos los códigos de acceso recibidos de usuarios.
- **Formato de los códigos transmitidos** – elección del formato de 4bit y 8bit (mayor fiabilidad) de los códigos transmitidos.

Configuración del módulo del teclado táctil y lector RFID 125 kHz, 13.56 MHz, NFC



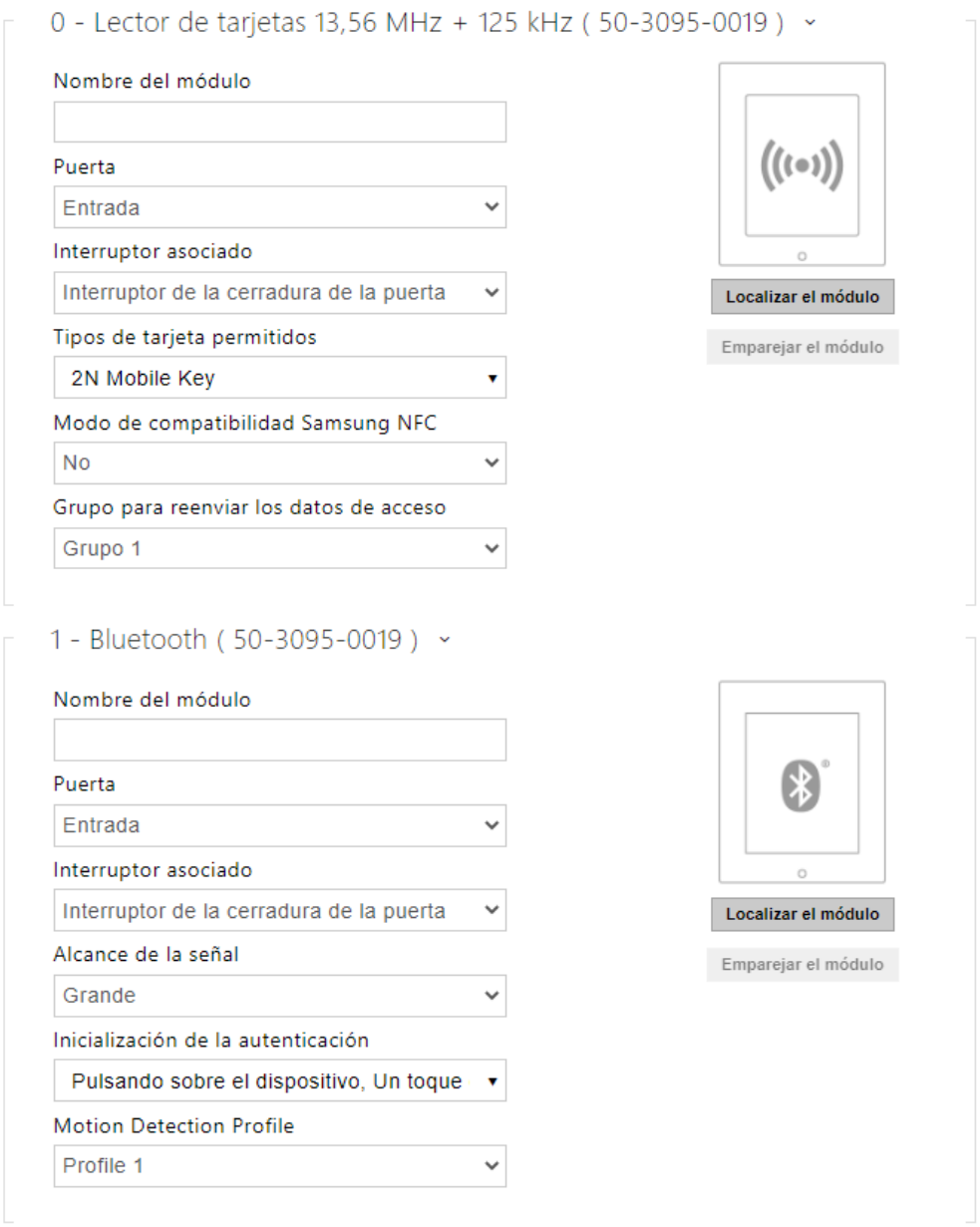
Lector de tarjetas 13,56 MHz (125 kHz) (número de serie)

- **Nombre del módulo** – configura el nombre del módulo. El nombre del módulo se utiliza a la hora de realizar log de sucesos desde el módulo del lector de tarjetas.
- **Puerta** – configura la dirección del paso en el caso del uso del lector (Entrada, Salida). El parámetro dirección es utilizado por el sistema de presencia.
- **Interruptor asociado** – configura el número del interruptor activado tras la autenticación del usuario mediante este módulo. En el caso de la configuración de la opción Interruptor de la cerradura de la puerta se aplican las reglas para la autenticación en el menú Hardware / Puerta.
- **Tipos de tarjeta permitidos** – permite configurar el tipo de tarjeta que será aceptado por el lector. El lector soporta en un momento solo un tipo de tarjeta.
- **Compatibilidad NFC con los teléfonos Samsung** – habilita la compatibilidad son los teléfonos Samsung.
- **Reenviar a la salida wiegand** – configura el grupo de salidas wiegand a la cual se reenviarán todos los ID recibidos de las tarjetas RFID.

Teclado táctil (número de serie)

- **Nombre del módulo**– configura el nombre del módulo. El nombre del módulo se utiliza a la hora de realizar log de sucesos desde el módulo del teclado táctil.
- **Puerta** – configura la dirección del paso en el caso del uso del lector (Entrada, Salida). El parámetro de la dirección es utilizado por el sistema de presencia.
- **Parpadear al pulsar la tecla** – configura la señalización luminosa mediante el parpadeo que confirma el pulsado de la tecla. Se utiliza en ambientes ruidosos cuando la señalización acústica no se percibe claramente.
- **Reenviar a la salida Wiegand** – configura el grupo de salidas wiegand a la cual se reenviarán todos los códigos de acceso recibidos de usuarios.
- **Formato de los códigos transmitidos** – elección del formato de 4bit y 8bit (mayor fiabilidad) de los códigos transmitidos.

Configuración del módulo de Bluetooth y lector RFID 125 kHz, 13.56 MHz, NFC



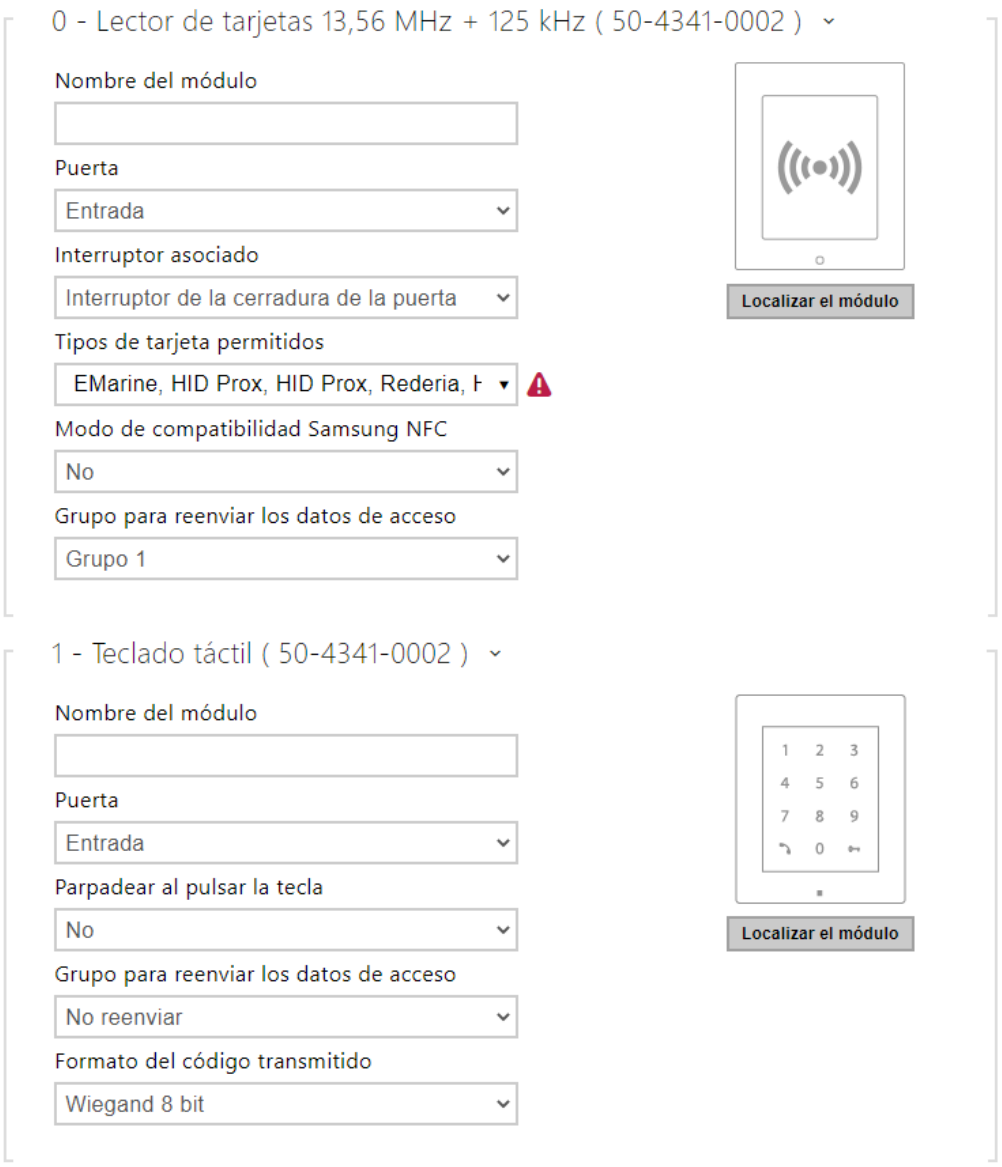
Lector de tarjetas 13,56 MHz (125 kHz)

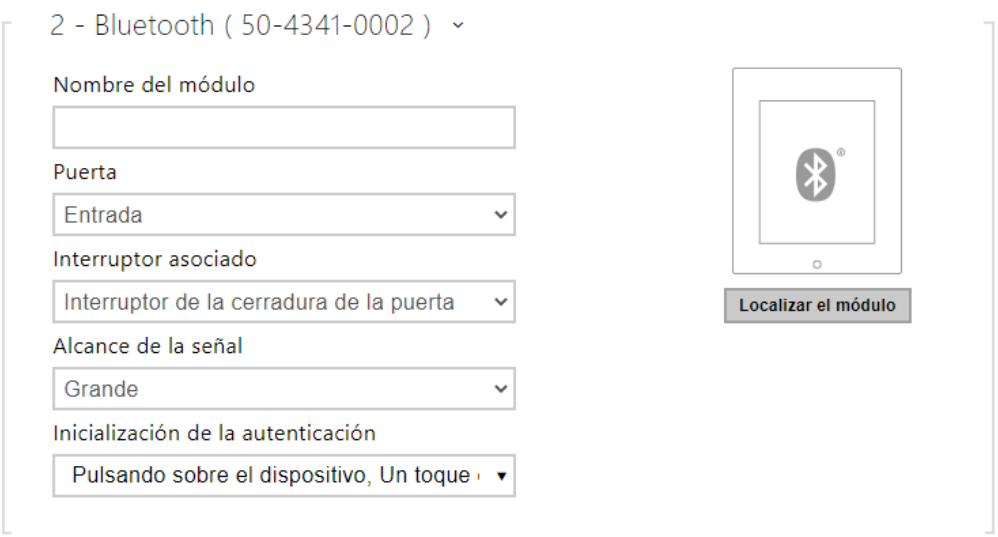
- **Nombre del módulo** – configura el nombre del módulo. El nombre del módulo se utiliza a la hora de realizar log de sucesos desde el módulo del lector de tarjetas.
- **Puerta** – configura la dirección del paso en el caso del uso del lector (Entrada, Salida). El parámetro dirección es utilizado por el sistema de presencia.
- **Interruptor asociado** – configura el número del interruptor activado tras la autenticación del usuario mediante este módulo. En el caso de la configuración de la opción Interruptor de la cerradura de la puerta se aplican las reglas para la autenticación en el menú Hardware / Puerta.
- **Tipos de tarjeta permitidos** – permite configurar el tipo de tarjeta que será aceptado por el lector. El lector soporta en un momento solo un tipo de tarjeta.
- **Retroiluminación del símbolo RFID** (solo para IP Style) – enciende o apaga la retroiluminación del símbolo RFID en el dispositivo.
- **Compatibilidad NFC con los teléfonos Samsung** – habilita la compatibilidad son los teléfonos Samsung.
- **Reenviar a la salida wiegand** – configura el grupo de salidas wiegand a la cual se reenviarán todos los ID de las tarjetas RFID.

Bluetooth

- **Nombre del módulo** – configura el nombre del módulo. El nombre del módulo se utiliza a la hora de realizar log de sucesos desde el módulo bluetooth.
- **Puerta** – configura la dirección del paso en el caso del uso del lector (Entrada, Salida). El parámetro dirección es utilizado por el sistema de presencia.
- **Interruptor asociado** – configura el número del interruptor activado tras la autenticación del usuario mediante este módulo. En el caso de la configuración de la opción Interruptor de la cerradura de la puerta se aplican las reglas para la autenticación en el menú Hardware / Puerta.
- **Alcance de la señal** – configura el alcance de la señal (el valor 5 representa el mayor alcance, el valor 1 el menor), es decir, la distancia a la cuál el módulo Bluetooth aún comunicará con el teléfono móvil. A la hora de la configuración se recomienda comprobar el alcance real de la señal, al cual afecta una serie de factores (sobre todo por la disposición espacial de la instalación, teléfono móvil utilizado y su posición).
- **Inicialización de la autenticación** – configura la forma de autenticación mediante el teléfono móvil:
  - **Un toque en la aplicación** – hay que confirmar la autenticación picando sobre el icono en la aplicación abierta en el teléfono móvil
  - **Pulsando sobre el dispositivo** – hay que confirmar la autenticación mediante el contacto con el lector en presencia del teléfono con la aplicación emparejada **2N® Mobile Key** .
  - **Detección de movimiento** – la autenticación se activará mediante la detección del movimiento al existir el teléfono con la aplicación **2N® Mobile Key** emparejada.
- **Perfil de la detección de movimiento** – configura el perfil de la detección de movimiento por el cual se regirá el módulo para la autenticación mediante el teléfono móvil.

Configuración del módulo del teclado táctil y Bluetooth y lector RFID 125 kHz, 13.56 MHz, NFC





Lector de tarjetas 13,56 MHz (125 kHz) (número de serie)

- **Nombre del módulo** – configura el nombre del módulo. El nombre del módulo se utiliza a la hora de realizar log de sucesos desde el módulo del lector de tarjetas.
- **Puerta** – configura la dirección del paso en el caso del uso del lector (Entrada, Salida). El parámetro dirección es utilizado por el sistema de presencia.
- **Interruptor asociado** – configura el número del interruptor activado tras la autenticación del usuario mediante este módulo. En el caso de la configuración de la opción Interruptor de la cerradura de la puerta se aplican las reglas para la autenticación en el menú Hardware / Puerta.
- **Tipos de tarjeta permitidos** – permite configurar el tipo de tarjeta que será aceptado por el lector. El lector soporta en un momento solo un tipo de tarjeta.
- **Compatibilidad NFC con los teléfonos Samsung** – habilita la compatibilidad son los teléfonos Samsung.
- **Grupo para reenviar datos de acceso** – le permite establecer un grupo al que se reenviarán todos los códigos de acceso de usuario recibidos.

Teclado táctil (número de serie)

- **Nombre del módulo** – configura el nombre del módulo. El nombre del módulo se utiliza a la hora de realizar log de sucesos desde el módulo del lector de tarjetas.
- **Puerta** – configura la dirección del paso en el caso del uso del lector (Entrada, Salida). El parámetro dirección es utilizado por el sistema de presencia.
- **Parpadear al pulsar la tecla** – configura la señalización luminosa mediante el parpadeo que confirma el pulsado de la tecla. Se utiliza en ambientes ruidosos cuando la señalización acústica no se percibe claramente.
- **Grupo para reenviar datos de acceso** – le permite establecer un grupo al que se reenviarán todos los códigos de acceso de usuario recibidos.
- **Formato de los códigos transmitidos** – elección del formato de 4bit y 8bit (mayor fiabilidad) de los códigos transmitidos.

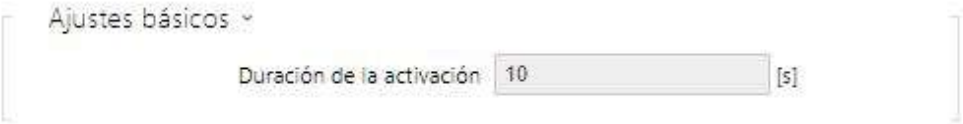
Bluetooth

- **Nombre del módulo** – configura el nombre del módulo. El nombre del módulo se utiliza a la hora de realizar log de sucesos desde el módulo bluetooth.
- **Puerta** – configura la dirección del paso en el caso del uso del lector (Entrada, Salida). El parámetro de la dirección es utilizado por el sistema de presencia.
- **Interruptor asociado** – configura el número del interruptor activado tras la autenticación del usuario mediante este módulo. En el caso de la configuración de la opción Interruptor de la cerradura de la puerta se aplican las reglas para la autenticación en el menú Hardware / Puerta.
- **Alcance de la señal** – configura el alcance de la señal (el valor 5 representa el mayor alcance, el valor 1 el menor), es decir, la distancia a la cuál el módulo Bluetooth aún comunicará con el teléfono móvil. A la hora de la configuración se recomienda comprobar el alcance real de la señal, al cual afecta una serie de factores (sobre todo por la disposición espacial de la instalación, teléfono móvil utilizado y su posición).
- **Inicialización de la autenticación** – configura la forma de autenticación mediante el teléfono móvil. Uno, una combinación de dos o los tres.
    - **Un toque en la aplicación** – hay que confirmar la autenticación picando sobre el icono en la aplicación abierta en el teléfono móvil
    - **Pulsando sobre el dispositivo** – hay que confirmar la autenticación mediante el contacto con el lector en presencia del teléfono con la aplicación emparejada **2N® Mobile Key** .
    - **Detección de movimiento** – la autenticación se activará mediante la detección del movimiento al existir el teléfono con la aplicación **2N® Mobile Key** emparejada.

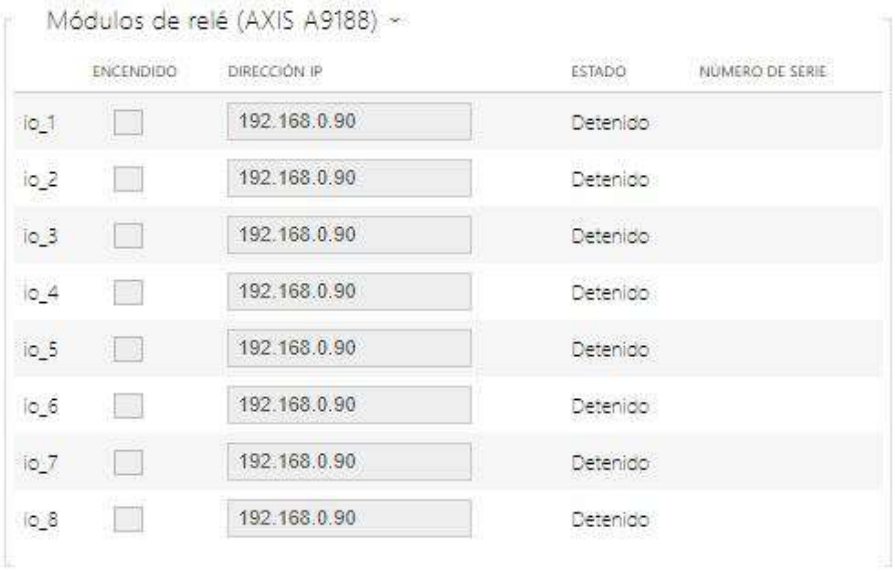
5.5.10 Control del ascensor

Mediante la conexión del módulo del relé AXIS A9188 al intercomunicador 2N IP (**2N® IP Style**, **2N® IP Verso**, **2N® IP Force**, **2N® IP Safety**, **2N® IP Vario**) se puede controlar el acceso a cada una de las plantas en el edificio en el caso de utilizar el ascensor. A un intercomunicador 2N IP se pueden conectar como máximo 8 de estos módulos de relé, cada módulo puede controlar 8 plantas, es decir, en total un máximo de 64 plantas.

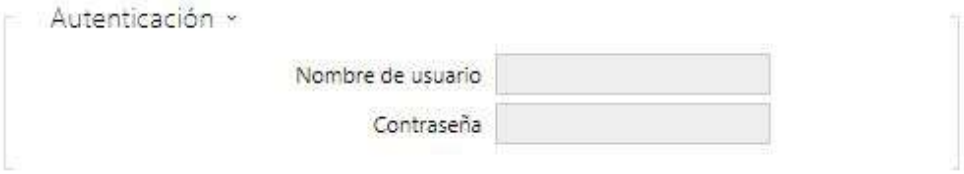
Solapa Módulos de relé



- **Tiempo de activación** – configura el tiempo de activación del módulo de relé (rango 1–600 s).



- **Encendido** – sirve para activar y desactivar el módulo AXIS A9188 que sirve para controlar el ascensor en hasta 8 plantas.
- **Dirección IP** – dirección IP de AXIS A9188.
- **Estado** – muestra el estado del módulo AXIS A9188 conectado (Error/Acceso denegado/ Preparado/Detenido).
- **Número de serie** – número de serie del módulo AXIS A9188.



- **Nombre de usuario** – nombre de usuario para la autenticación de la conexión al dispositivo externo. El parámetro es obligatorio solo en el caso de que el dispositivo externo requiera la autenticación.
- **Contraseña** – contraseña para la autenticación de la conexión al dispositivo externo (WEB relé etc.). El parámetro es obligatorio solo en el caso de que el dispositivo externo requiera la autenticación.

Aviso

- La autenticación se realiza para todos los módulos con un nombre de usuario y una contraseña.

Solapa Plantas

- **Nombre de la planta** – configura el nombre de la planta.
- **Acceso libre** – activa el acceso permanente a la planta sin necesidad de ninguna autenticación.
- **Perfil** – ofrece la elección de uno o varios perfiles de tiempo a la vez que se aplicarán. La propia configuración de los perfiles de tiempo se puede realizar en la sección Directorio / Perfiles de tiempo.
  -  con la marca se configura la elección de los perfiles pre-definidos o la configuración manual del perfil de tiempo para el elemento determinado.
  -  con la marca se configura el perfil de tiempo directamente para el elemento determinado.

Consejo

Generación del certificado para el módulo de relé AXIS A9188

1. Busque el módulo de relé AXIS A9188 en la red local mediante AXIS IP Utility.
2. Introduzca los datos de inicio de sesión root/root.
3. En el menú seleccione Preferences / Additional device configuration.
4. Aparecerá una nueva ventana con la configuración del dispositivo.
5. En el menú seleccione System Options / Security / Certificates.
6. Genere el certificado haciendo clic en Create self-signed certificate.
7. Rellene todos los campos requeridos y confirme con el botón OK.
8. Pase al menú System Options / Security / HTTPS.
9. Elija un certificado en el menú desplegable y guárdelo pulsando el botón Save.
10. Pase a la interfaz de web del intercomunicador 2N IP, configuración Hardware / Control del ascensor. Introduzca los datos de inicio de sesión y rellene la dirección IP del módulo de relé.
11. En el caso de conexión satisfactoria aparecerá junto al módulo de relé READY.

5.6 Sistema

Aquí se expone el resumen de lo que encontrará en este capítulo:

5.6.1 Red

El **intercomunicador 2N IP** se conecta a la red local y para un funcionamiento correcto debe tener configurada la dirección IP válida, event. puede obtener la dirección IP desde el servidor DHCP en esta red. La dirección IP y la configuración de DCHP se configura en la solapa Red.

Consejo

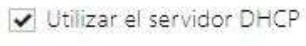
- *En el caso de que quiera averiguar la dirección IP de su intercomunicador, puede utilizar la aplicación **2N® IP Scanner** cuya descarga libre está disponible en las páginas www.2n.com o puede utilizar el mecanismo descrito en el manual de instalación del intercomunicador correspondiente – el intercomunicador le comunicará su dirección IP por sí solo mediante la función de voz.*

En el caso de que en su red utilice el servidor RADIUS y el mecanismo de verificación de los dispositivos conectados basado en los protocolos 802.1x, puede configurar el intercomunicador de manera que utilice la autenticación EAP-MD5 o EAP-TLS. Para configurar esta función sirve la solapa 802.1x.

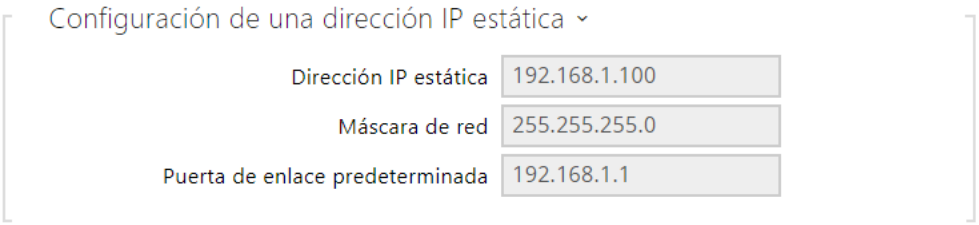
En la solapa Trace puede ejecutar la captación de los paquetes entrantes y salientes en la interfaz de red del intercomunicador. El archivo con los paquetes captados se puede descargar y luego procesar por ej. mediante la aplicación Wireshark (www.wireshark.org).

Lista de parámetros

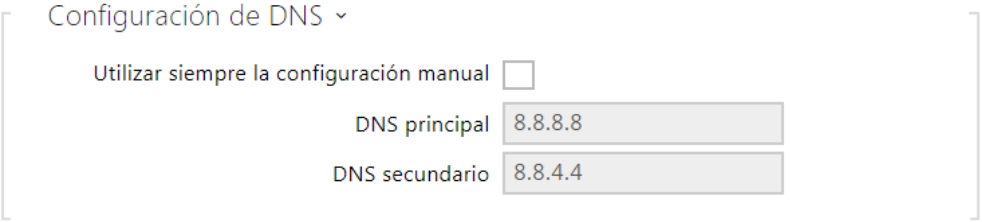
Solapa Básico



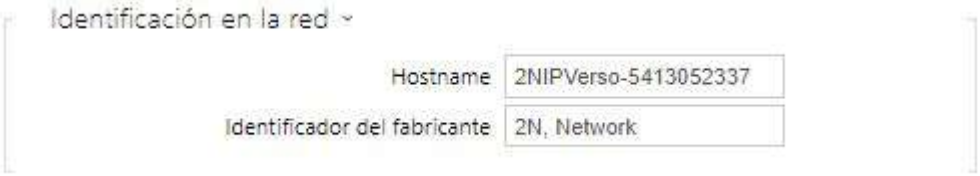
- **Utilizar el servidor DHCP** – habilita la obtención automática de la dirección IP desde el servidor DHCP en la red local. En el caso de que el servidor DHCP no se encuentre en su red, o no se pueda utilizar por otro motivo, utilice la configuración manual de la red.



- **Dirección IP estática** – dirección IP estática del intercomunicador. La dirección se utiliza en conjunto con los siguientes parámetros en el caso de que el parámetro Utilizar el servidor DHCP no esté configurado.
- **Máscara de red** – configura la máscara de red.
- **Puerta de enlace predeterminada** – dirección del portal inicial que permite la comunicación con los dispositivos fuera de la red local.



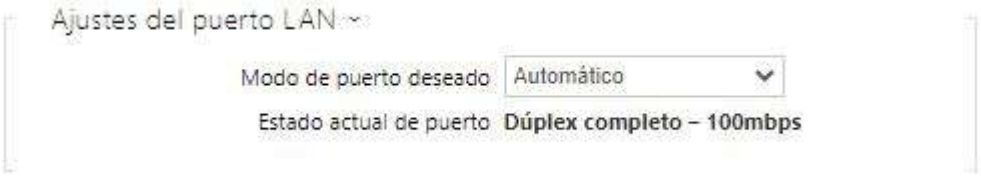
- **DNS primario** – dirección del servidor DNS primario para traducir los nombres de dominio en direcciones IP. En el caso de restaurar la configuración de fábrica del dispositivo se configurará el servidor DNS primario a la dirección 8.8.8.8.
- **DNS secundario** – dirección del servidor DNS secundario utilizado en el caso de que el servidor DNS primario no esté disponible. En el caso de restaurar la configuración de fábrica del dispositivo se configurará el servidor DNS secundario a la dirección 8.8.4.4.



- **Hostname** – configuración de la identificación del intercomunicador 2N IP en la red.
- **Identificador del fabricante** – configura el identificador del fabricante como una cadena de símbolos para DHCP Option 60.

- **WS-Discovery habilitado** – habilita la función WS-Discovery, que le permite a los demás clientes ONVIF buscar un dispositivo compatible en la red LAN. Habilita la función para utilizar el dispositivo como dispositivo compatible con ONVIF.

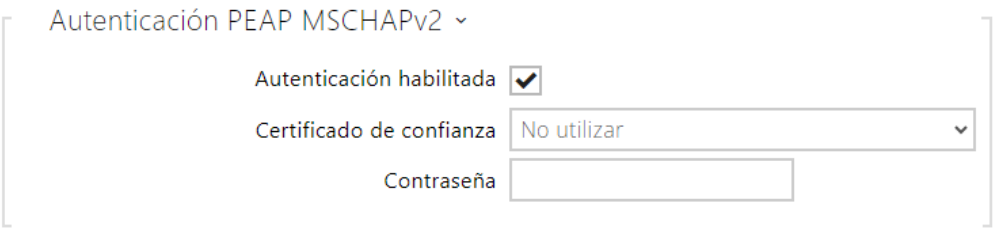
- **VLAN habilitada** – enciende el soporte de la red virtual (VLAN según la recomendación 802.1q). Para la función correcta es necesario configurar también el ID de la red virtual.
- **VLAN ID** – ID elegido de la red virtual dentro del rango 1-4094 El dispositivo solo recibirá los paquetes marcados con este ID. En el caso de una configuración inconveniente se puede producir la pérdida de conexión y a consecuencia habrá que poner el dispositivo en el estado inicial mediante la configuración de fábrica.



- **Modo requerido del puerto** – modo preferido del puerto de la interfaz de red (Automáticamente o Half Duplex – 10 mbps). Permite reducir la velocidad de transferencia

a los 10 mbps en el caso de que la infraestructura de red utilizada (cableado) no sea fiable para el funcionamiento de 100 mbps.
- **Estado actual del puerto** – estado actual del puerto de la interfaz de red (Half o Full Duplex – 10 mbps o 100 mbps).

- **MTU reducida** – activa el soporte de MTU reducida (Maximum Transmission Unit) para la correcta función del dispositivo en las redes que soportan solo MTU reducida.



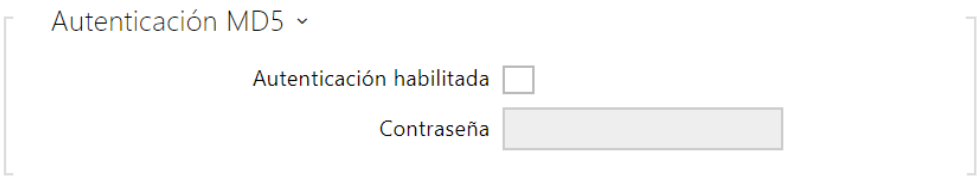
- **Autenticación habilitada** – habilita el uso de la autenticación de los dispositivos de red mediante el protocolo 802.1x PEAP MSCHAPv2. No habilite esta función si su red LAN no es compatible con 802.1x. Si lo hace, no podrá acceder al dispositivo.
- **Certificado de confianza** – especifica el certificado de la autoridad de certificación para verificar la validez del certificado público del servidor RADIUS. En el caso de no estar especificado, el certificado público del servidor RADIUS no se verifica.
- **Contraseña** – contraseña de acceso utilizado para la autenticación mediante el método PEAP MSCHAPv2.

Solapa 802.1x

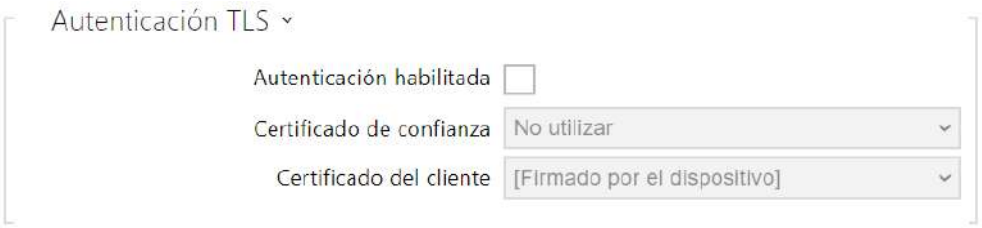
Precaución

- Los cambios de la configuración de la autenticación tendrán efecto después de reiniciar el dispositivo.

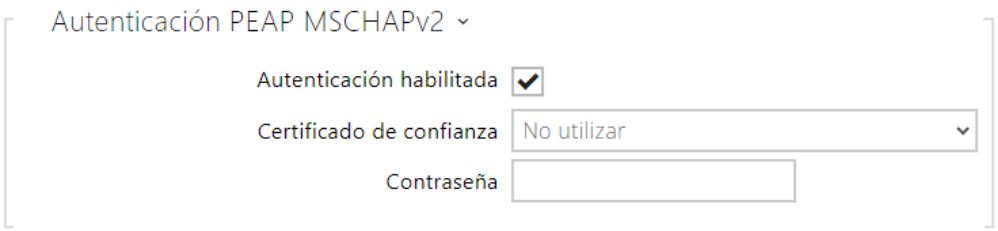
- **Identidad del dispositivo** – nombre del usuario (identidad) para autenticar mediante los métodos EAP-MD5 y EAP-TLS.



- **Autenticación MD5 habilitada** – habilita el uso de la autenticación de los dispositivos en la red mediante el protocolo 802.1x EAP-MD5. No habilite esta función si su red LAN no es compatible con 802.1x. De lo contario el intercomunicador se volverá inaccesible.
- **Contraseña** – contraseña de acceso utilizado para la autenticación mediante el método EAP-MD5.



- **Autenticación TLS habilitada** – habilita el uso de la autenticación de los dispositivos en la red mediante el protocolo 802.1x EAP-TLS. No habilite esta función si su red LAN no es compatible con 802.1x. De lo contario el intercomunicador se volverá inaccesible.
- **Certificado de la autoridad de certificación** – especifica el conjunto de certificados de las autoridades de certificación para verificar la validez del certificado público del servidor RADIUS. Se puede elegir uno de los tres conjuntos de certificados, ver el capítulo Certificados. En el caso de que el certificado de la autoridad de certificación no aparece, el certificado público del servidor RADIUS no se verifica.
- **Certificado personal** – especifica el certificado de usuario y la clave mediante los cuales de verifica la autorización del intercomunicador para la comunicación en la red local en el puerto del elemento de red asegurado mediante 802.1x. Se puede elegir uno de los tres conjuntos de los certificados de usuario y de las claves privadas, ver el capítulo Certificados.



- **Autenticación habilitada** – habilita el uso de la autenticación de los dispositivos de red mediante el protocolo 802.1x EAP-TLS. No habilite esta función si su red LAN no es compatible con 802.1x. Si lo hace, no podrá acceder al dispositivo.
- **Certificado de confianza** – especifica el certificado de la autoridad de certificación para verificar la validez del certificado público del servidor RADIUS. En el caso de no estar especificado, el certificado público del servidor RADIUS no se verifica.
- **Contraseña** – para la autenticación a través de EAP-MD5.

Solapa OpenVPN

Mediante OpenVPN se puede conectar el dispositivo a otra red.

- **Habilitada** – activa la red virtual privada (VPN).

- **Configuración inicial** – cuando está habilitada se dirige todo el tráfico de salida de la red fuera de la máscara de la red local a la interfaz VPN.
- **Dirección del servidor** – dirección del servidor OpenVPN.

- **Puerto del servidor** – puerto del servidor OpenVPN.
- **Certificado de la autoridad de certificación** – especifica el conjunto de certificados de las autoridades de certificación para verificar la validez del certificado público del servidor OpenVPN. Se puede elegir uno de los tres conjuntos de certificados, ver la sección Certificados. En el caso de que el certificado de la autoridad de certificación no aparezca, el certificado público del servidor OpenVPN no se verificará.
- **Certificado del cliente** – especifica el conjunto de los certificados del cliente para verificar la identidad del cliente mediante el servidor OpenVPN. Se puede elegir uno de los tres conjuntos de certificados, ver la sección Certificados. En el caso de no estar especificado el certificado del cliente, OpenVPN no verifica la identidad del cliente.
- **Estado** – muestra el estado de la conexión de OpenVPN. Conectado/Desconectado.
- **Error** – muestra el tipo del error de la conexión de OpenVPN en el caso de que surja.
- **Inicio** – conecta el dispositivo a OpenVPN.
- **Stop** – desconecta el dispositivo de OpenVPN.

- **Red VPN** – muestra la información básica sobre VPN.

Consejo

- La información detallada sobre la configuración del servidor OpenVPN y del cliente está disponible en la sección FAQ.

5.6.2 Fecha y hora

En el caso de que esté utilizado la configuración de los perfiles de tiempo para controlar la validez de los números de teléfono, códigos para la activación de la cerradura, etc., es imprescindible que el intercomunicador tenga configurada correctamente la fecha y la hora interna.

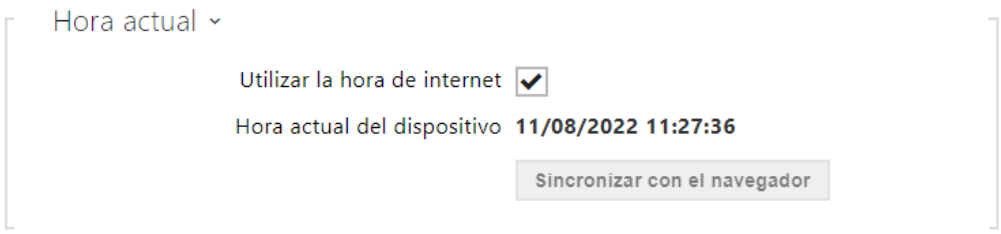
La mayoría de los modelos de los **intercomunicadores 2N IP** está equipada con reloj respaldado de hora real, el cual permite superar el corte de alimentación incluso durante varios días. En el caso de que el intercomunicador no esté equipado con esta función, tras el corte de alimentación (event. el reinicio) perderá la hora actual. Debido a ello, tras conectar la alimentación al intercomunicador tras un tiempo prolongado (por ej. tras la instalación de un intercomunicador nuevo) la hora configurada en el intercomunicador tiene el valor inicial y hay que configurarla. La hora en el intercomunicador la puede sincronizar en cualquier momento con la hora de internet marcando la función **Utilizar la hora actual de internet** o con la hora actual en su PC utilizando el botón **Sincronizar el en navegador**.

Nota

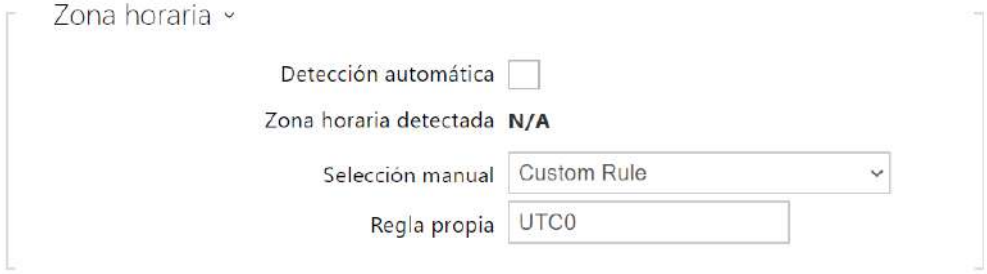
- *La configuración correcta de la fecha y hora no es imprescindible para la función básica del intercomunicador. La fecha y la hora actual son necesarios para la función correcta de los perfiles de tiempo y para la visualización correcta de la hora de sucesos en diferentes listas (Syslog, registros sobre las tarjetas acercadas, log del dispositivo descargado mediante **HTTP API** etc.)*

Para la máxima precisión y fiabilidad recomendamos utilizar siempre la función **Utilizar la hora actual de internet**. En condiciones habituales de operación en los dispositivos puede haber error de la hora hasta ±2 minutos/mes.

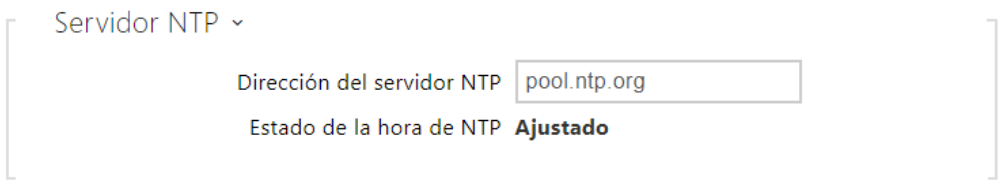
Lista de parámetros



- **Utilizar la hora de internet** – Habilita el uso del servidor NTP para sincronizar la hora del dispositivo.
- **Sincronizar con el navegador** – mediante este botón puede sincronizar la hora en el intercomunicador con la hora actual en su PC.

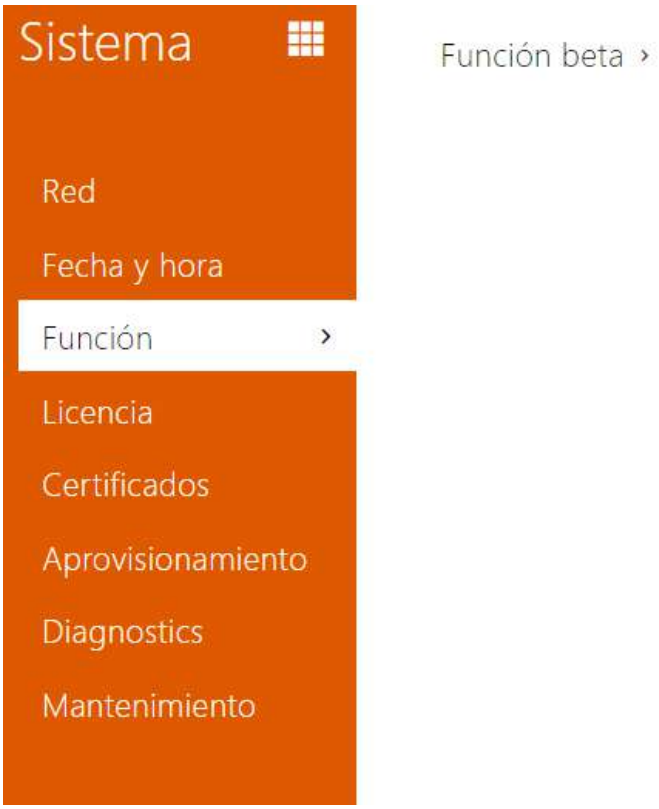


- **Detección automática** – determina si la zona horaria se detecta automáticamente desde el servicio My2N. En el caso de que la detección automática esté apagada, se utiliza la configuración en el parámetro Selección manual (zona horaria seleccionada manualmente o Regla propia).
- **Zona horaria detectada** – muestra la franja horaria detectada automáticamente. En el caso de que el servicio no esté disponible o esté apagado, aparece N/A.
- **Selección manual** – ajusta la franja horaria del lugar de instalación del dispositivo. El ajuste determina la diferencia horaria y los cambios entre el horario de verano y de invierno.
- **Regla propia** – si el dispositivo se instala en un sitio que no está incluido en el parámetro Zona horaria, defina la regla de forma manual. La regla solo se aplicará si el parámetro Zona horaria es manual.



- **Dirección del servidor NTP** – configura la dirección IP o el nombre del dominio del servidor NTP según el cual el intercomunicador sincroniza la hora interna.
- Ni la dirección IP del servidor, ni tampoco el nombre de dominio, se puede configurar al apagar la función **Utilizar la hora actual de internet**.
- **Estado de la hora de NTP** – muestra el estado del último intento de configuración de la hora local mediante el servidor NTP (No configurada, Configurada, Error).

5.6.3 Función



Muestra la lista de las funciones beta publicadas, las cuales están destinadas a ser probadas por los usuarios.
La lista contiene:

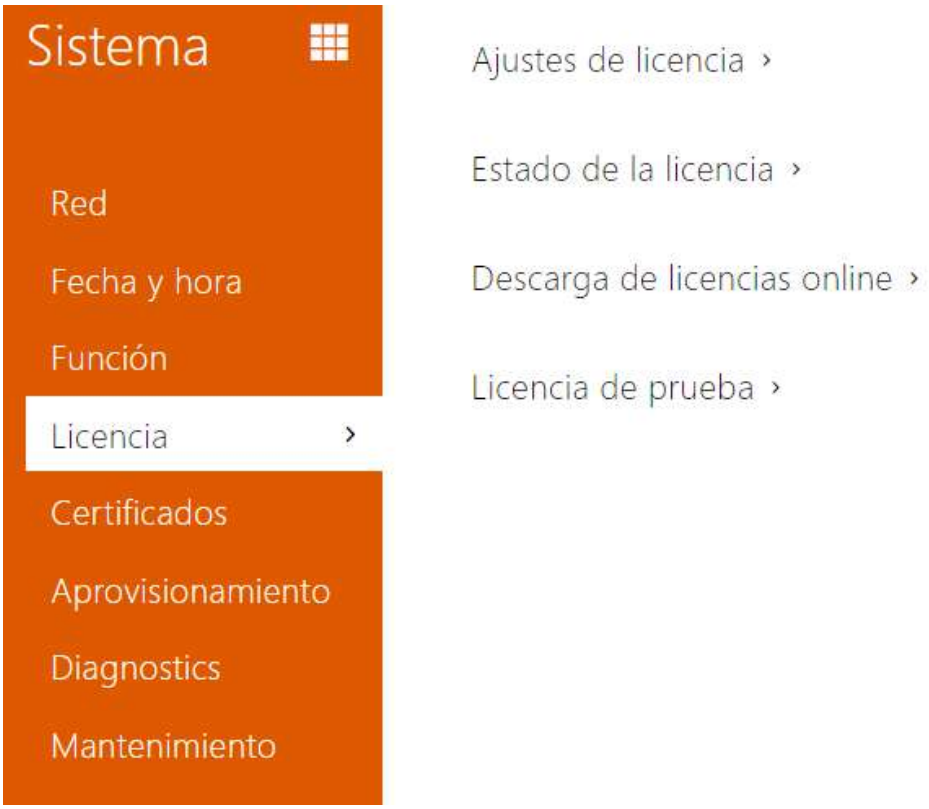
- nombre de la función,
- estado de la función que indica si la función está ejecutándose o está parada,
- acción que permite ejecutar o parar la función.

La ejecución o la parada de la función no se produce antes de reiniciar el dispositivo. En el caso de que el dispositivo no se reinicie se puede cancelar la solicitud del cambio del estado mediante la acción **Interrumpir**.

> **Nota**
>
> - Las funciones de prueba no están cubiertas por la garantía y la compañía 2N TELEKOMUNIKACE a.s. no se responsabiliza de las limitaciones funcionales y los posibles daños a causa de las limitaciones funcionales de las funciones beta. Las funciones beta son proporcionadas exclusivamente para los fines de realización de pruebas.

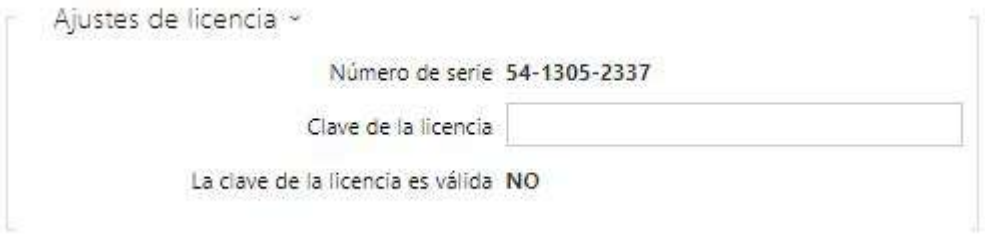
Nombre de la función beta	Descripción
Archivo de configuración protegido con contraseña	Esta función permite codificar el archivo de configuración mediante la contraseña durante la realización de la copia de seguridad (ver 5.5.8 Mantenimiento). A la hora de cargar el archivo de configuración en el dispositivo se requerirá la contraseña, la cual protege al archivo de configuración. En el caso de que la contraseña no coincida, el archivo de configuración no se cargará al dispositivo.
Verificación de varios factores de matrículas	Una vez activada esta función aparecerá la opción Multifactor en la sección Servicios > Control de acceso > Reglas para la llegada > Configuración avanzada > Reconocimiento de matrículas. El acceso se permitirá solo después de la conexión de al menos dos métodos de autenticación en función de las reglas de acceso establecidas. En el caso de reconocimiento de la matrícula es imprescindible introducir dentro de 60 segundos otro método de autenticación.
Noise Cancelling	Esta función suprime el ruido ambiental del micrófono a la hora de detectar la voz.

5.6.4 Licencias



Algunas funciones de los **intercomunicadores 2N IP** están disponibles solo tras introducir la clave de licencia válida. La lista de las opciones de licencias para los intercomunicadores encontrará en el capítulo **Diferencias entre modelos y licencias de funciones**.

Lista de parámetros

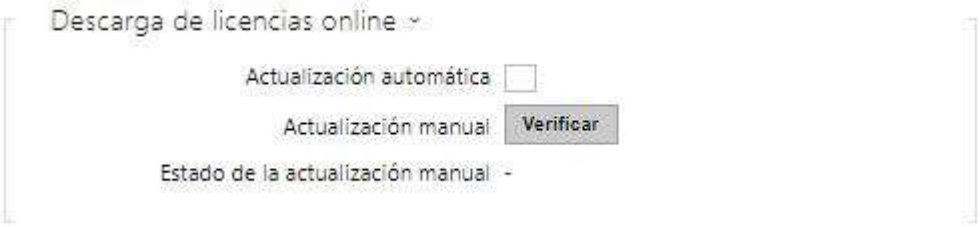


- **Número de serie** – muestra el número de serie del dispositivo para los cuales es válida la licencia.
- **Clave de la licencia** – permite introducir la clave de licencia válida.
- **Clave de la licencia válida** – muestra si la clave de licencia introducida es válida.

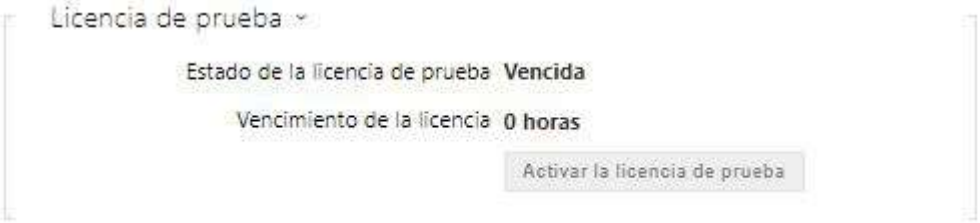
- **Licencias estándar** – muestra la lista de las licencias que forman parte del dispositivo desde la fábrica.
  - **Enhanced Audio** – muestra si están disponibles funciones activadas por la licencia Enhanced Audio.
  - **Enhanced Security** – muestra si están disponibles funciones activadas por la licencia Enhanced Security.
  - **Soporte NFC** – muestra si está disponible el soporte de la identificación del usuario mediante los teléfonos equipados con la tecnología NFC.
- **Licencias de pago** – muestra la lista de las licencias que están disponibles tras introducir la clave de licencia válida.
  - **Enhanced Video** – muestra si están disponibles funciones activadas por la licencia Enhanced Video.
  - **Enhanced Intergration** – muestra si están disponibles funciones activadas por la licencia Enhanced Integration.
  - **Soporte Informacast** – muestra si está disponible el soporte del protocolo Informacast.
  - **Soporte del control de ascensores** – muestra si está disponible la función de la licencia Lift Module activada.

Consejo

- Resumen de las licencias y de sus funciones



- **Actualización automática** – el dispositivo actualiza la clave de licencia del servidor de licencias 2N.
- **Actualización manual** – requerimiento manual de verificación de la disponibilidad de la licencia.
- **Estado de la actualización manual** – en curso, actualizado, no especificado.

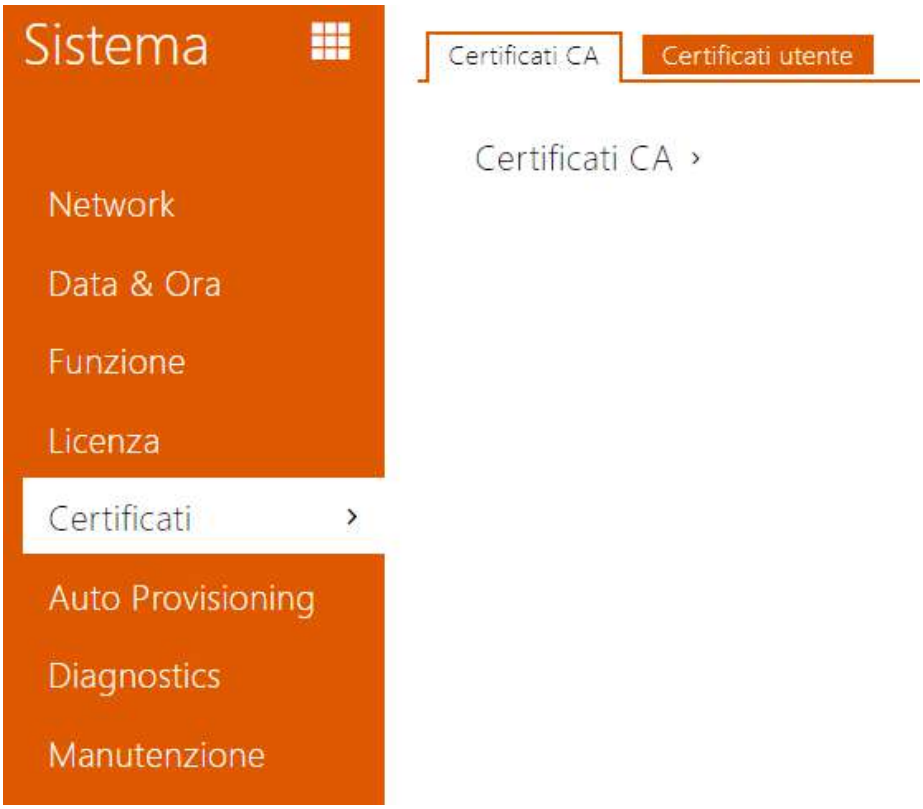


- **Estado de la licencia trial** – muestra el estado de la licencia trial (no activada, activada, validez caducada).
- **Tiempo restante de la validez de la licencia trial** – muestra el tiempo restante de la validez de la licencia trial. Con cada reinicio y tras la restauración de la configuración original se resta automáticamente 1 hora del tiempo restante de la validez de licencia, en otro caso este tiempo no está afectado de ninguna manera.

Aviso

- El reset del SW del dispositivo no provoca el borrado de la calve de licencia y no se produce el reinicio del propio dispositivo. En el caso de que la actualización automática de las licencias esté apagada antes del reset del SW, tras el reset se activará automáticamente y luego se enviará el requerimiento al servidor de licencias. En el caso de que la actualización automática de las licencias esté activada, se enviará el requerimiento al servidor de licencias en el tiempo planificado.
- El reset del HW del dispositivo provocará el borrado de la clave de licencia, el siguiente reinicio del dispositivo tras un tiempo aleatorio enviará el requerimiento al servidor de licencias.
    - Intervalo de requerimientos – de forma aleatoria 1–100 minutos tras el inicio y luego tras 8 horas en los dispositivos con licencia trial, o tras 8 horas 7 días desde el reinicio en los dispositivos con la licencia limitada por el tiempo.

5.6.5 Certificados



Algunos servicios de red del **intercomunicador 2N IP** utilizan para la comunicación con otros dispositivos en la red el protocolo TLS asegurado. Este protocolo impide a terceros realizar escuchas, event. modificar el contenido de la comunicación. Durante el establecimiento de la conexión mediante el protocolo TLS se realiza la autenticación de una parte, event. de ambas partes, que requiere certificados y claves privadas.
Servicios del intercomunicador que utilizan el protocolo TLS:

a. Servidor Web (protocolo HTTPS)
b. E-mail (protocolo SMTP)
c. 802.1x (protocolo EAP-TLS)
d. SIPs

Los **intercomunicadores 2N IP** permiten cargar conjuntos de certificados de las autoridades de certificación que sirven para verificar la identidad del dispositivo con el que está comunicando el intercomunicador, y a la vez cargar certificados personales y claves privadas mediante los cuales se cifra la comunicación.

A cada servicio que requiere certificados puede asignar uno de los conjuntos de certificados, ver los capítulos **Servidor Web**, **E-mail** y **Streaming**. Los certificados pueden ser compartidos por varios servicios a la vez.

- El **intercomunicador 2N IP** acepta certificados en formatos DER (ASN1) y PEM.
- El **intercomunicador 2N IP** soporta el cifrado AES, DES y 3DES.

- El **intercomunicador 2N IP** soporta los siguientes algoritmos:
  - RSA de tamaño de llave de hasta 2048bits para los certificados cargados por el usuario; de forma interna llaves de hasta 4096bits (durante la conexión – certificados temporales y del mismo valor)
  - Elliptic Curves

Aviso

- Los certificados CA deben utilizar el formato X.509 v3.

Durante la primera conexión de la alimentación al intercomunicador se generará automáticamente el llamado **certificado Self Signed** y **la llave privada** que se puede utilizar para el servicio **Servidor Web** y **E-mail** sin la necesidad de cargar certificado o clave privada propios.

Nota

- *En el caso de que utilice el certificado Self Signed para cifrar la comunicación entre el servidor web del intercomunicador y el explorador, la comunicación está asegurada, sin embargo, el explorador le avisará que no puede verificar la fiabilidad del certificado del intercomunicador.*

El resumen actual de los certificados cargados de las autoridades de certificación y de los certificados privados se muestra en dos solapas:

Al pulsar el botón puede cargar en el dispositivo el certificado guardado en su PC. En la ventana de diálogo se puede introducir el ID del certificado para la identificación a l ahora de seleccionarlo, modificarlo o borrarlo. ID puede tener como máximo 40 caracteres, puede contener caracteres minúsculos o mayúsculos del abecedario, números y caracteres '_' y '-'. ID no es obligatorio. En la ventana de diálogo elija el archivo con el certificado (event. con clave privada) y pulse el botón **Cargar**. Al pulsar el botón eliminará el certificado del dispositivo. Pulsando el botón visualizará la información sobre el certificado.

Aviso

- Tras la actualización del firmware o tras el reinicio el dispositivo cambiará el certificado Self signed por uno nuevo. Hay que revisar y comparar el certificado que aparece en el dispositivo con el certificado en la web, para asegurarse de que son idénticos.

Aviso

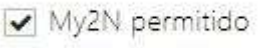
- Es posible que el certificado con una llave privada RSA cuya longitud supera los 2048 bits sea rechazada. En este caso aparecerá la notificación: **¡El dispositivo no aceptó el archivo con clave privada o la contraseña!**
- En el caso de utilizar los certificados basados en curvas elípticas es posible utilizar solo las curvas secp256r1 (aka prime256v1 aka NIST P-256) y secp384r1 (aka NIST P-384).

5.6.6 Actualizaciones

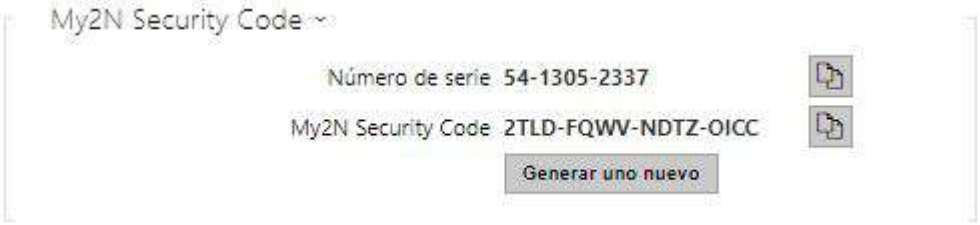
Los **intercomunicadores 2N IP** permiten, a parte de la actualización manual del firmware y de la configuración, también descargar y actualizar el firmware y la configuración, según las reglas establecidas, desde el almacenamiento al servidor TFTP o HTTP definido por usted.

La dirección del servidor TFTP y HTTP puede configurarse manualmente. Los **intercomunicadores 2N IP** soportan la averiguación automática de la dirección mediante el servidor DHCP local (el llamado Option 66).

Solapa My2N



- **My2N / TR069 habilitado** – habilita la conexión al servicio My2N, event. al otro servidor ACS.



- **Número de serie** – muestra el número de serie de los dispositivos para los cuales es válido el código My2N.

- **My2N Security Code** – muestra el texto completo del código que sirve para activar la aplicación.
- **GENERAR UNO NUEVO** – El My2N Security Code actual será inhabilitado y se generará uno nuevo.

Se muestra la información sobre el estado de conexión del dispositivo a My2N.

- **My2N ID** – identificador exclusivo de la compañía, creado con la ayuda del portal My2N.

Solapa Firmware

En esta solapa se configura la descarga automática del firmware desde el servidor definido por usted. El intercomunicador compara en intervalos establecidos el archivo en el servidor con el firmware actual y en el caso e que el firmware en el servidor es más reciente, realizará la actualización automática con el reinicio del intercomunicador incluido (aprox. 30 s). Por eso recomendamos configurar el tiempo de configuración de manera que se realice durante el uso mínimo del intercomunicador (por ej. por la noche). El

intercomunicador 2N IP espera encontrar en los servidores archivos llamados:

a. **MODEL**-firmware.bin – firmware del intercomunicador
b. **MODEL**-common.xml – configuración conjunta de todos los intercomunicadores del modelo determinado
c. **MODEL**-**MACADDR**.xml – configuración específica para un intercomunicador

MODEL en el nombre del archivo especifica el nombre técnico del intercomunicador 2N IP o del dispositivo de audio 2N IP:

a. **hipv – 2N® IP Vario**
b. **hipf – 2N® IP Force**
c. **hipsf – 2N® IP Safety**

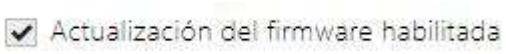
d. **hipak – 2N® IP Audio Kit**
e. **hipvk – 2N® IP Video Kit**
f. **hipve – 2N® IP Verso**
g. **verso2 – 2N® IP Verso 2.0**
h. **au – 2N Access Unit**
i. **aug2 – 2N Access Unit 2.0**
j. **aum – 2N Access Unit M**
k. **hipso – 2N® IP Solo**
l. **hipba – 2N® IP Base**
m. **sac – 2N® SIP Audio Converter**
n. **sassh – 2N® SIP Speaker Horn**
o. **ss – 2N® SIP Speaker**
p. **style – 2N® IP Style**

MACADDR es la dirección MAC del intercomunicador en formato 00-00-00-00-00-00. La dirección MAC del intercomunicador encontrará en la etiqueta de fabricación o directamente en la interfaz de web en la solapa **Estado del intercomunicador**.

Ejemplo:

2N® IP Vario con dirección MAC 00-87-12-AA-00-11 descargará del servidor TFTP archivos con los siguientes nombres:

- hipv-firmware.bin
- hipv-common.xml
- hipv-00-87-12-aa-00-11.xml

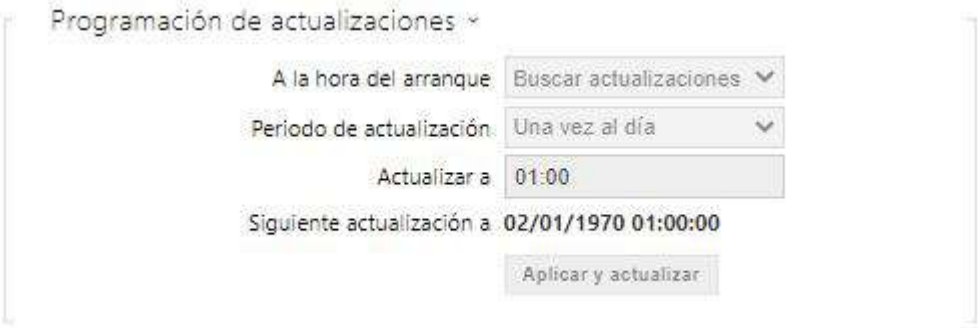


- **Actualizar firmware automáticamente** – habilita la descarga automática del firmware desde el servidor TFTP/HTTP.

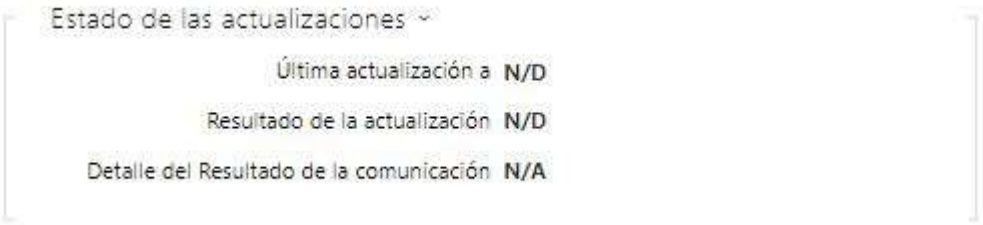
- **Modo de obtención de la dirección** – permite elegir si la dirección del servidor TFTP/ HTTP se debe introducir de forma manual o si se utiliza la dirección obtenida automáticamente desde el servidor DHCP mediante el parámetro Option 66.
- **Dirección del servidor** – permite introducir manualmente la dirección del servidor TFTP (tftp://dirección_ip), HTTP (http://dirección_ip) o HTTPS (https://dirección_ip).
- **Dirección DHCP (Option 66/150)** – muestra la dirección del servidor obtenida mediante DHCP Option 66 ó 150.
- **Ruta hacia el archivo** – Establezca la ruta a la carpeta de archivos de firmware. Ingrese / para buscar model-firmware.bin (modelo específico) en la carpeta raíz del servidor. Consulte la barra lateral (?) para obtener detalles sobre modelos, etc.
- **Utilizar la autenticación** – permite configurar la autenticación para el acceso al servidor HTTP.
- **Nombre de usuario** – nombre de usuario utilizado para la autenticación en el servidor.
- **Contraseña** – contraseña utilizada para la autenticación en el servidor.
- **Verificar el certificado del servidor** – especifica el conjunto de certificados de las autoridades de certificación para verificar la validez del certificado público del servidor ACS.
- **Certificado del cliente** – especifica el certificado de cliente y la clave privada, con la ayuda de los cuales se verifica la autorización del intercomunicador para comunicarse con el servidor ACS.

Info

- El intercomunicador contiene el certificado Factory Cert, un certificado firmado, que es posible utilizar por ej. par ala integración con British Telecom.



- **Durante el arranque del intercomunicador** – permite realizar el control o la actualización tras cada arranque del intercomunicador.
- **Período de la actualización** – configura el período en el que se realizará la actualización. Se puede configurar la actualización automática una vez por hora, día, semana, mes, o configurar el período de forma manual.
- **Hora de la actualización** – permite configurar la hora en formato HH:MM a la que se debe realizar la actualización periódica. De esta manera se puede configurar la realización de la actualización durante el tiempo cuando el intercomunicador se utilice con la menor frecuencia. Este parámetro no se aplicará en el caso de que el período de la actualización esté configurado a un tiempo inferior a un día.
- **Hora de la próxima actualización** – muestra la hora de la realización planificada de la siguiente actualización.



- **Hora de la última actualización** – muestra la hora de la última actualización realizada.
- **Resultado de la actualización** – muestra el resultado de la última actualización realizada. Los siguientes valores son posibles: DHCP option 66 failed, Firmware is up to date, Server connection failed, Running..., File not found.

- **Detalle del Resultado de la comunicación** – código erróneo de la comunicación con el servidor o código de estado del protocolo TFTP/HTTP.

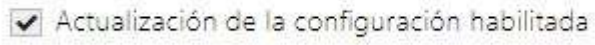
Resultado	Descripción
La dirección del servidor no es válida	La dirección del servidor no es válida.
El protocolo no es compatible	El protocolo no es compatible. Solo son compatibles los protocolos HTTP(s) y TFTP.
La localización del archivo no es válida	La localización del archivo determinado no es válida.
La función DHCP Option 66 ha fallado	La carga de la dirección del servidor a través del protocolo DHCP Option 66 ó 150 ha fallado.
El nombre del dominio no es válido	El nombre de dominio del servidor no es válido debido a la configuración incorrecta o a la indisponibilidad del servidor DNS.
No se encontró el servidor	El servidor HTTP/TFTP requerido no responde.
La autenticación ha fallado	Los datos HTTP de autenticación no son correctos.
No se encontró el archivo	El archivo no ha sido encontrado en el servidor.
La petición está esperando en la cola...	La petición de actualización está esperando en la cola.
En curso...	Actualización en curso.
Archivo no válido	El archivo a descargar está dañado o es de tipo incorrecto.
El firmware está actualizado	El intento de actualización del firmware ha demostrado que se había cargado la versión más reciente del firmware.
La actualización ha transcurrido con éxito	La actualización de la configuración/del firmware ha transcurrido con éxito. En el caso de la actualización del firmware el dispositivo se reiniciará dentro de unos segundos.

Resultado	Descripción
Error interno	Durante la descarga del archivo ha surgido un error no identificado.

Solapa Configuración

En esta solapa se configura la descarga automática de la configuración desde el servidor definido por usted. El intercomunicador descarga en intervalos configurados el archivo desde el servidor y se reconfigura. Durante esta actualización no se realiza el reinicio del intercomunicador.

> **Nota**
>
> - *En el caso del intercomunicador **2N® IP Vario** con pantalla, se produce en cada actualización una interrupción de la función de la pantalla de varios segundos de duración en el momento cuando se realiza su configuración. Por eso recomendamos configurar el tiempo de configuración de manera que se realice durante el uso mínimo del intercomunicador (por ej. por la noche).*

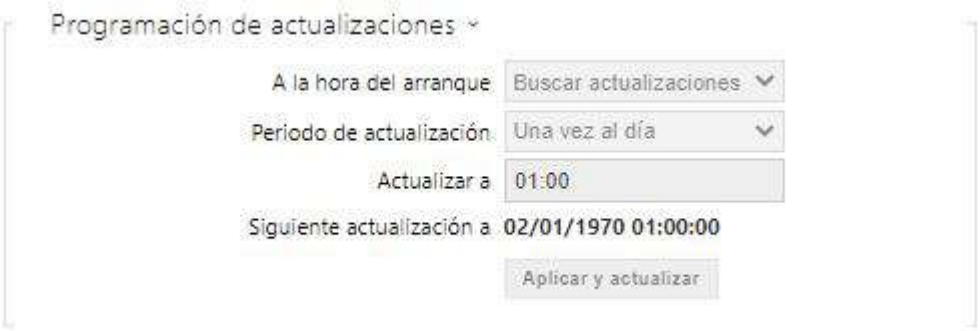


- **Actualizar la configuración automáticamente** – habilita la descarga automática de la configuración desde el servidor TFTP/HTTP.

- **Modo de obtención de la dirección** – permite elegir si la dirección del servidor TFTP/ HTTP se debe introducir de forma manual o si se utiliza la dirección obtenida automáticamente desde el servidor DHCP mediante el parámetro Option 66.
- **Dirección del servidor** – permite introducir manualmente la dirección del servidor TFTP (tftp://dirección_ip), HTTP (http://dirección_ip) o HTTPS (https://dirección_ip).
- **Dirección DHCP (Option 66)** – muestra la dirección del servidor obtenida mediante DHCP Option 66 ó 150.
- **Ruta hacia el archivo** – configura el directorio, event. el prefijo del nombre de archivo con el firmware o con la configuración en el servidor. El intercomunicador espera archivos con nombres XhipY_firmware.bin, XhipY-common.xml y XhipY-MACADDR.xml, donde X es el prefijo dado por este parámetro e Y especifica el modelo del intercomunicador.
- **Utilizar la autenticación** – permite configurar la autenticación para el acceso al servidor HTTP.
- **Nombre de usuario** – nombre de usuario utilizado para la autenticación en el servidor.
- **Contraseña** – contraseña utilizada para la autenticación en el servidor.
- **Verificar el certificado del servidor** – especifica el conjunto de certificados de las autoridades de certificación para verificar la validez del certificado público del servidor ACS.
- **Certificado del cliente** – especifica el certificado de cliente y la clave privada, con la ayuda de los cuales se verifica la autorización del intercomunicador para comunicarse con el servidor ACS.

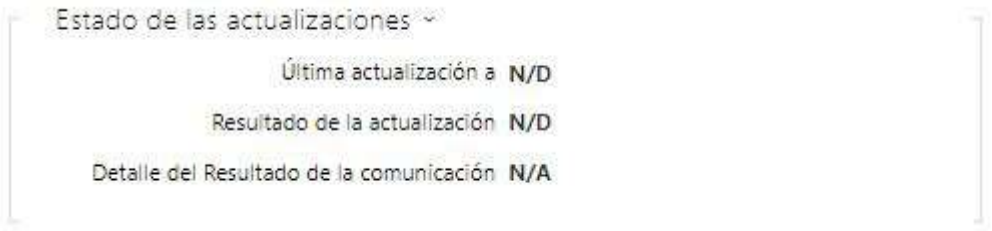
Info

- El intercomunicador contiene el certificado Factory Cert, un certificado firmado, que es posible utilizar por ej. par ala integración con British Telecom.



- **Durante el arranque del intercomunicador** – permite realizar el control o la actualización tras cada arranque del intercomunicador.
- **Período de la actualización** – configura el período en el que se realizará la actualización. Se puede configurar la actualización automática una vez por hora, día, semana, mes, o configurar el período de forma manual.

- **Hora de la actualización** – permite configurar la hora en formato HH:MM a la que se debe realizar la actualización periódica. De esta manera se puede configurar la realización de la actualización durante el tiempo cuando el intercomunicador se utilice con la menor frecuencia. Este parámetro no se aplicará en el caso de que el período de la actualización esté configurado a un tiempo inferior a un día.
- **Hora de la próxima actualización** – muestra la hora de la realización planificada de la siguiente actualización.



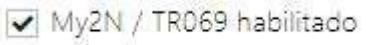
- **Hora de la última actualización** – muestra la hora de la última actualización realizada.
- **Resultado de la actualización (Configuración conjunta)** – muestra el resultado de la última actualización conjunta realizada. Los siguientes valores son posibles: DHCP option 66 failed, Firmware is up to date, Server connection failed, Running..., File not found.
- **Detalle del Resultado de la comunicación (Configuración conjunta)** – código erróneo de la comunicación con el servidor o código de estado del protocolo TFTP/HTTP.
- **Resultado de la actualización (Configuración privada)** – la configuración privada se produce después de la actualización de la configuración conjunta. El dispositivo con la configuración privada se identifica según la dirección MAC. Muestra el resultado de la última actualización privada realizada. Los siguientes valores son posibles: DHCP option 66 ha fallado, Firmware is up to date, Server connection failed, Running..., File not found.
- **Detalle del Resultado de la comunicación (Configuración privada)** – código erróneo de la comunicación con el servidor o código de estado del protocolo TFTP/HTTP.

Solapa TR069

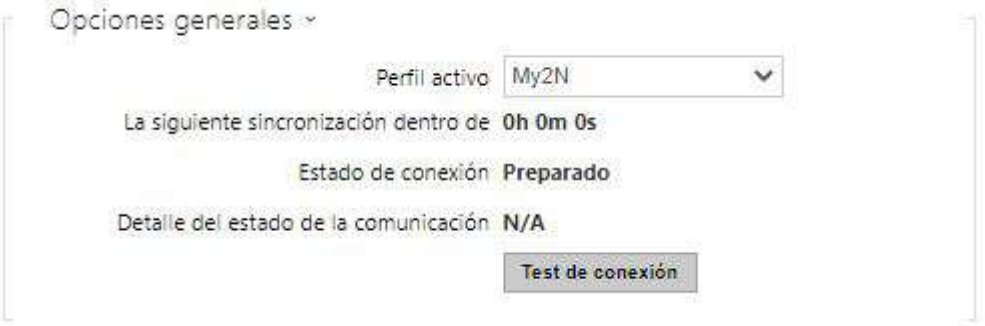
En esta solapa se habilita y se configura la administración remota del intercomunicador mediante el protocolo TR-069. El protocolo TR-069 permite configurar de forma fiable los parámetros del intercomunicador, restablecer y respaldar la configuración, event. realizar el upgrade del firmware del dispositivo.

El protocolo TR-069 lo utiliza al servicio de cloud My2N. Para la función correcta del intercomunicador con My2N es necesario habilitar el servicio TR-069 y configurar el parámetro perfil activo al valor My2N. Después, el intercomunicador iniciará periódicamente la sesión en el servicio My2N el cual lo puede configurar.

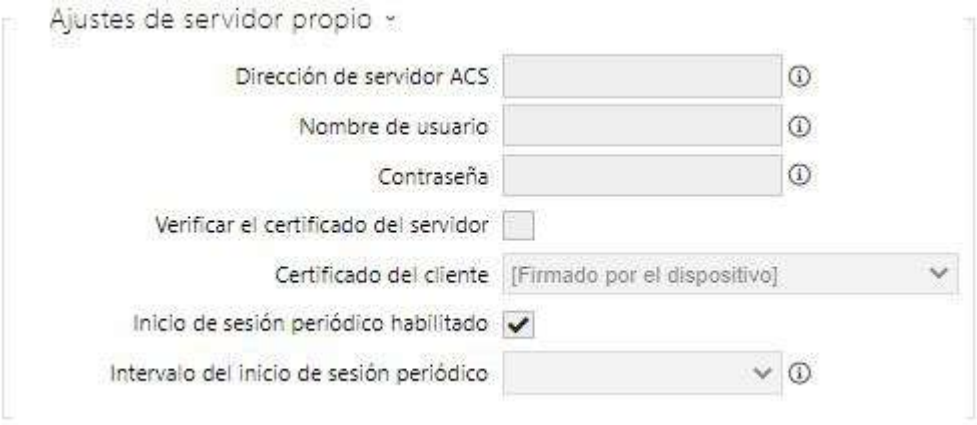
Esta función permite conectar el intercomunicador a su propio ACS (Auto Configuration Server). En tal caso se apagará la conexión al servicio My2N en el intercomunicador.



- **My2N / TR069** – habilita el servicio My2N / TR069.



- **Perfil activo** – permite elegir uno de los perfiles pre-configurados (del servidor ACS), event. elegir configuración propia y configurar manualmente la conexión con el servidor ACS.
- **Próxima sincronización dentro de** – muestra el tiempo que queda para que el intercomunicador contacte con el servidor remoto ACS.
- **Estado de conexión** – muestra el estado actual de la conexión al servidor ACS, event. descripción del estado de error.
- **Detalle del estado de la comunicación** – código erróneo de la comunicación con el servidor o código de estado del protocolo TFTP/HTTP.
- **Test de conexión** – realiza el test de conexión al servicio TR069 según el perfil configurado, ver Perfil activo. El resultado del test aparecerá en el campo Estado de conexión.



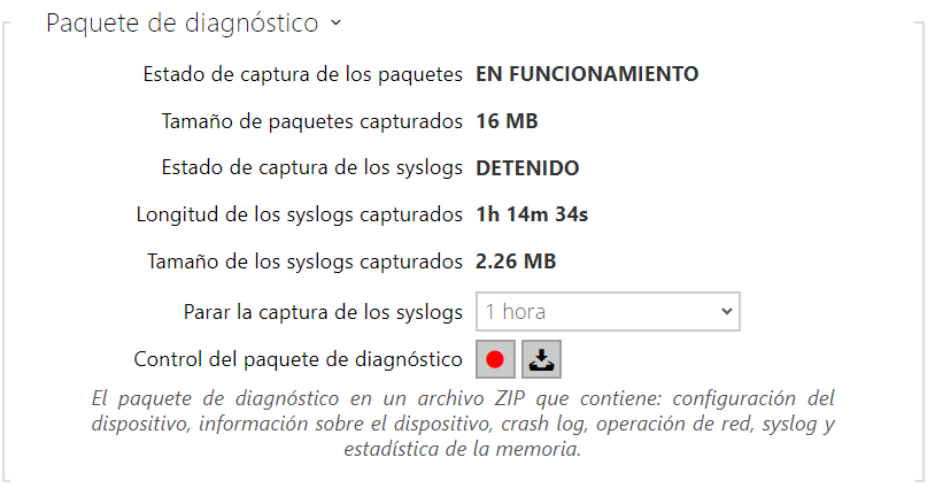
- **Dirección del servidor ACS** – configura la dirección del servidor ACS en el formato direcciónip[: puerto], por ej. 192.168.1.1:7547
- **Nombre de usuario** – configura el nombre de usuario para la autenticación del intercomunicador en el servidor ACS
- **Contraseña** – configura la contraseña del usuario para la autenticación del intercomunicador en el servidor ACS
- **Verificar el certificado del servidor** – especifica el conjunto de certificados de las autoridades de certificación para verificar la validez del certificado público del servidor ACS. Se puede elegir uno de los tres conjuntos de certificados, ver el capítulo Certificados. En el caso de que el certificado de la autoridad de certificación no aparece, el certificado público del servidor ACS no se verifica.
- **Certificado del cliente** – especifica el certificado de cliente y la clave privada, con la ayuda de los cuales se verifica la autorización del intercomunicador para comunicarse con el servidor ACS. Se puede elegir uno de los tres conjuntos de los certificados de usuario y de las claves privadas, ver el capítulo Certificados.
- **Habilitación del inicio de sesión periódico** – habilita el inicio de sesión periódico del intercomunicador en el servidor ACS.
- **Intervalo del inicio de sesión periódico** – configura el intervalo del inicio de sesión periódico en el servidor ACS en el caso de que esté permitido mediante el parámetro **Habilitación del inicio de sesión periódico**.

5.6.7 Diagnóstico

El **intercomunicador 2N IP** permite enviar los mensajes de sistema, que contienen la información importante sobre el estado y procesos del dispositivo, al servidor syslog donde se pueden registrar estos mensajes u utilizar para el siguiente análisis y audit del dispositivo monitorizado. En la operación habitual del intercomunicador no es necesario configurar este servicio.

Solapa Diagnóstico

La interfaz permite iniciar la captura de los logs de diagnóstico, los cuales se pueden posteriormente descargar y enviar al Soporte técnico. Los logs de diagnóstico captador ayudan a identificar y resolver los problemas reportados. Los logs contienen la información sobre el dispositivo, sobre su configuración, sobre operación de red, crash log y la estadística de la memoria.



- **Estado de captura de los paquetes** – muestra si está activada la captura de los paquetes en la solapa Captura de los paquetes.
- **Tamaño de paquetes capturados** – muestra la cantidad de paquetes capturados.
- **Estado de captura de los syslogs** –muestra si está activada la captura de los mensajes syslog en la solapa Syslog.
- **Longitud de los syslogs capturados** – muestra el tiempo durante el cual se están capturando los mensajes syslog en la solapa Syslog.
- **Tamaño de los syslogs capturados** – muestra la cantidad de mensajes syslog capturados.
- **Parar la captura de los syslogs** – configura el tiempo durante el cual se capturarán los datos.

La captura se activa mediante el botón para la grabación  . Al pulsar de nuevo el botón para la grabación, la captura se reinicia y empieza a correr de nuevo. El archivo con los paquetes capturados se puede descargar mediante el botón  .

Precaución

- La activación de la captura de los datos de diagnóstico reinicia la captura de los paquetes en el caso de que ya esté en marcha.

- **Verificar la disponibilidad de la dirección en la red** – sirve para verificar la disponibilidad de la dirección determinada en la red como comando „Ping“ en los sistemas de operación habituales. Tras pulsar la tecla „Ping“ aparecerá el diálogo en el que se puede introducir la dirección IP o el nombre de dominio y pulsando el botón „Ping“ enviar los datos de prueba a esta dirección. En el caso de que esté introducida la dirección IP o el nombre de dominio no válidos, aparecerá un aviso y el botón „Ping“ estará inactivo hasta que la dirección introducida no sea válida.
  En el diálogo aparece además el estado de la realización de la función y el resultado. El estado „Fallido“ („Failed“) puede significar la indisponibilidad de la dirección introducida dentro de 10 segundos, o la imposibilidad de traducir el nombre de dominio en dirección. En el caso de que se reciba una respuesta válida, aparece la dirección IP desde la cual ha llegado dicha respuesta y la longitud de la espera a la respuesta en milésimas de segundo. Al pulsar de nuevo el botón „Ping“ se enviará otra pregunta por la misma dirección.

Solapa Captura de los paquetes

En la solapa se puede iniciar la captura de paquetes entrantes y salientes en la interfaz de red del interfono. Los paquetes capturados pueden almacenarse localmente en el búfer del dispositivo, cuyo tamaño depende del dispositivo, o remotamente en el ordenador del usuario, limitado únicamente por el tiempo de almacenamiento especificado y el espacio disponible en disco. El archivo de paquetes capturados puede descargarse y procesarse posteriormente, por ejemplo, utilizando Wireshark (www.wireshark.org).

Cuando el búfer está lleno durante la captura local, los paquetes almacenados más antiguos se sobrescriben automáticamente. Al captar paquetes de forma local, recomendamos reducir la velocidad de transmisión del video por debajo de 512 kbps. La captura la puede iniciar mediante

el botón , pararla mediante el botón y descargar el archivo con los paquetes captados mediante el botón .

Puede iniciar la captación remota puede utilizar el botón . Es necesario especificar el tiempo (s) durante el cual los paquetes entrantes y salientes serán captados. Una vez transcurrido el tiempo ajustado, el archivo con los paquetes captados se descargará automáticamente al PC del usuario. Detener la captación se puede con el botón .

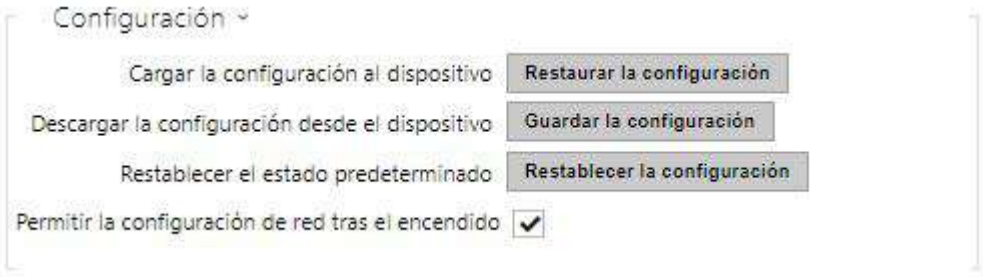
Solapa Syslog

- **Enviar mensajes de Syslog** – habilita el envío de mensajes de sistema al servidor Syslog. Para la función correcta debe estar configurada la dirección válida del servidor.
- **Dirección del servidor** – establezca la dirección IP[:puerto] o la dirección MAC del servidor en el que se ejecuta la aplicación para capturar mensajes de syslog.
- **Nivel de los mensajes enviados** – configura el nivel del detalles de los mensajes enviados (Error, Warning, Notice, Info, Debug 1–3). Se recomienda configurar el nivel Debug 1–3 solo en el caso de facilitar la localización de un problema en el dispositivo, que requiere el soporte técnico.

Resumen general sobre los mensajes syslog locales.

5.6.8 Mantenimiento

Este menú sirve para el mantenimiento de la configuración y del firmware del intercomunicador. Permite respaldar y restaurar la configuración de todos los parámetros, actualizar el firmware del intercomunicador, event. configurar todos los parámetros del intercomunicador a estado inicial.



- **Restaurar la configuración** – sirve para restaurar la configuración del respaldo anterior. Tras pulsar el botón aparecerá la ventana de diálogo en el que puede seleccionar el archivo con la configuración y cargarlo en el dispositivo. Antes de cargar el archivo en el dispositivo puede elegir si del archivo de configuración se debe aplicar la configuración general, importar el directorio, importar la configuración de la red y certificados o configuración de la conexión a la centralita SIP.
- **Respaldar la configuración** – sirve para respaldar la configuración actual completa del intercomunicador. Tras pulsar el botón se descargará la configuración completa la cual

puede guardar en su PC.

Aviso

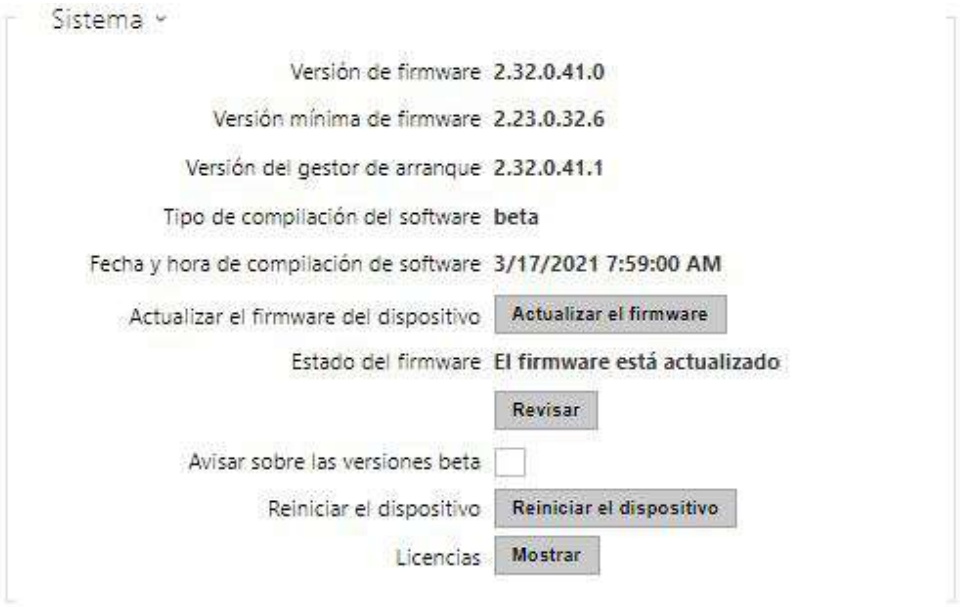
- *La configuración del intercomunicador puede contener información sensible, como son los números de teléfono de los usuarios y las contraseñas de acceso, por eso trate este archivo con prudencia.*

- **Configuración inicial** – sirve para configurar todos los parámetros del intercomunicador al estado inicial a excepción de los parámetros de la configuración de red. En el caso de que quiera poner el intercomunicador en el estado inicial completo, utilice la unión correspondiente o el botón reset, ver el manual de instalación del intercomunicador correspondiente.

Aviso

- *La restauración de la configuración inicial borrará la posible clave de licencia grabada. Por eso es recomendable guardarla haciendo una copia en otro almacenamiento para la necesidad posterior.*
- *La clave de licencia no se borra en el caso del reinicio de HW (es decir, reinicio mediante el botón en el dispositivo) en el caso de que esté habilitada la función de la actualización automática (Sistema / Licencia), la cual actualiza la clave de licencia desde el servido de licencia 2N. Con el reinicio del software se produce la restauración de todos los parámetros al estado original, a excepción de los certificados y de la configuración de red.*

- **Permitir la configuración de red tras el encendido** – habilita la opción de restablecer los parámetros de red a la configuración inicial mediante el pulsado de la sucesión de botones del marcado rápido tras el reinicio del intercomunicador de manera descrita en el capítulo Configuración del dispositivo en el Manual de instalación del modelo correspondiente.



Nota

La función, la fiabilidad y la seguridad del dispositivo dependen del firmware instalado.. La actualización periódica del firmware a la versión actual forma parte de las condiciones de uso del producto. Los posibles errores causados por el uso de la versión de firmware obsoleto no pueden ser el objeto de reclamación. El firmware actual implementa las experiencias de los clientes y los requisitos del sector de la protección de datos personales.

- **Actualizar el firmware** – sirve para cargar un nuevo firmware en el intercomunicador. Tras pulsar el botón aparecerá la ventana de diálogo en el que puede seleccionar el archivo con el firmware destinado a su intercomunicador. Tras un upload satisfactorio del firmware el intercomunicador se reiniciará automáticamente. Tras el reinicio está plenamente disponible con un nuevo firmware. Todo el proceso de la actualización tarda menos de un minuto. L aversión actual del firmware para su intercomunicador puede obtener en la dirección www.2n.com. La actualización del firmware no afecta a la configuración. El intercomunicador verifica el archivo de firmware y no permite cargar un archivo incorrecto o dañado.

Advertencia

- En el caso de downgrad del firmware se produce en el dispositivo con procesador Artpec el restablecimiento de la configuración de fábrica con el cual se perderá toda la configuración, incluidas las claves de licencia. Antes de realizar downgrade recomendamos hacer la copia de seguridad de la configuración y guardar la clave de licencia válida.

- **Revisar** – sirve para verificar online si está disponible un firmware más reciente. En el caso de que esté disponible un firmware nuevo, se le ofrecerá la posibilidad de su descarga con el upgrade automático posterior del dispositivo.
- **Reiniciar el dispositivo** – realiza el reinicio del intercomunicador. Todo el proceso del reinicio tarda aproximadamente 30 s. Tras finalizar el reinicio, cuando el intercomunicador obtiene su propia dirección IP, aparecerá automáticamente la ventana de inicio de sesión.

Aviso

- El registro del cambio de configuración se realiza en el intercomunicador dentro del límite de tiempo de 3–15 s, dependiendo de la envergadura de la configuración correspondiente del intercomunicador. No reinicie el intercomunicador durante este tiempo.

- **Mostrar** – tras hacer clic en el botón Mostrar se abrirá la ventana de diálogo con una lista de las licencias utilizadas y del software de terceros. También incluye el enlace para el documento EULA.

- **Envío de datos anónimos de estadística** – permite enviar al fabricante los datos anónimos de estadística sobre el uso del dispositivo. Estos datos no contienen ninguna información sensible, como por ej. contraseñas, códigos de acceso o números de teléfono. 2N TELEKOMUNIKACE a.s. utiliza esta información para mejorar la calidad, fiabilidad y rendimiento del software. La participación es voluntaria y usted puede cancelar el envío de los datos de estadística en cualquier momento.

5.7 Puertos utilizados

Servicio	Puerto	Protocolo	Dirección	Encendido de forma estándar	Configurable	Configuración
802.1x	–	–	In/Out	No	No	–
DHCP	68	UDP	In/Out	Sí	No	–
DNS	53	TCP/ UDP	In/Out	Sí	No	–
Echo (device discovery)*	8002	UDP	In/Out	Sí	No	–
FTP	21	TCP	Out	No	No	–
2N IP Eye	8003	UDP	Out	No	No	–

Servicio	Puerto	Protocolo	Dirección	Encendido de forma estándar	Configurable	Configuración
HTTP	80	TCP	In/Out	Sí	Sí	5.4.8 Web server
HTTPS	443	TCP	In/Out	Sí	Sí	5.4.8 Web server
Multicast audio	22222	UDP	Out	No	Sí	5.4.2 Streamování
Multicast audio for ICU protocol	8006	UDP	Out	Sí	No	–
Multicast video for ICU protocol	8008	UDP	Out	Sí	No	–
Multicast video (wide) for ICU protocol	8016	UDP	In/Out	Sí	No	–
NTP client	123	UDP	In/Out	Sí	No	–
ONVIF	80, 443, 3702	TCP/UDP	In/Out	No	No	–
RTP+RTCP ports (SIP)	4900+ (range of 64 ports)	UDP	In/Out	No	Sí	5.4.1 Teléfono
RTP+RTCP ports (External camera)	4800+ (range of 64 ports)	UDP	In/Out	No	Sí	5.4.2 Streamování
RTSP client	554	UDP	In/Out	No	Sí	5.4.1 Teléfono
RTSP server	554	UDP	In/Out	No	No	–

Servicio	Puerto	Protocolo	Dirección	Encendido de forma estándar	Configurable	Configuración
SingleWire Commands	80	TCP	In/Out	Sí	No	–
SingleWire Communication	8081	TCP	Out	Sí	No	–
SLP	427	UDP	In/Out	Sí	No	–
SingleWire Media	20000+	UDP	In	Sí	No	–
SIP	5060, 5062	TCP/ UDP	In/Out	No	Sí	5.4.1 Teléfono
SIPS	5061	TCP	In/Out	No	Sí	5.4.1 Teléfono
SMTP	25	TCP	Out	No	Sí	5.4.3 E-Mail
Syslog	514	UDP	Out	No	No	–
TFTP	69	UDP	Out	Sí	No	–
My2N Knocker	443	TCP	Out	Sí	No	–
My2N Tribble Tunnel	443	TCP	Out	Sí	No	–
SNMP Agent	161	UDP	In/Out	Sí	No	–
SNMP Trap	162	UDP	Out	Sí	No	–
SSDP	1900	UDP	In/Out	Sí	No	–
SDDP	1902	UDP	In/Out	Sí	No	–
Multicast receiver (Automation)	4433	UDP	In	No	No	–

Servicio	Puerto	Protocolo	Dirección	Encendido de forma estándar	Configurable	Configuración
WS-Discovery	3702	UDP	In/Out	Sí	No	–
CIP Client (Crestron)	41794	UDP	In/Out	No	No	–
Sitechannel (ICU protocol)	8004	UDP	In/Out	Sí	No	–

Echo – protocolo de propietario para la búsqueda de los intercomunicadores en la red. Parte de los productos **2N® IP Network Scanner**, **2N® IP Eye**, **2N® Access Commander**.

6. Información complementaria

Aquí se expone el resumen de lo que encontrará en este capítulo:

6.1 Solución de problemas

Para consultar consejos sobre la resolución de otros problemas, visite la página faq.2n.cz.

6.2 Directivas, leyes y reglamentos

2N® Intercomunicador IP cumple con las siguientes directivas y reglamentos:

- 2014/35/UE para el material eléctrico destinado a utilizarse con determinados límites de tensión
- 2014/30/UE para la compatibilidad electromagnética
- 2011/65/UE sobre restricciones a la utilización de determinadas sustancias peligrosas en aparatos eléctricos y electrónicos
- 2012/19/UE sobre residuos de aparatos eléctricos y electrónicos

Industria de Canadá

Este aparato digital de clase B cumple con la norma canadiense ICES-003/NMB-003.

FCC

Este equipo ha sido probado y se ha comprobado que cumple con los límites para un dispositivo digital de Clase B, de acuerdo con la parte 15 de las normas de la FCC.

NOTA: Estos límites están diseñados para proporcionar una protección razonable contra las interferencias perjudiciales en una instalación residencial. Este equipo genera, utiliza y puede irradiar energía de radiofrecuencia y, si no se instala y utiliza de acuerdo con las instrucciones, puede causar interferencias perjudiciales en las comunicaciones de radio.

Sin embargo, no se puede garantizar que no se produzcan interferencias en una instalación concreta. Si este equipo causa interferencias perjudiciales en la recepción de radio o televisión, lo cual puede determinarse apagando y encendiendo el equipo, se recomienda al usuario que intente corregir las interferencias mediante una o varias de las siguientes medidas:

- Reorientar o reubicar la antena receptora
- Aumentar la separación entre el equipo y el receptor
- Conectar el equipo a una toma de corriente en un circuito diferente al que está conectado el receptor
- Consulte al distribuidor o a un técnico de radio/televisión experimentado para obtener ayuda

Los cambios o modificaciones a esta unidad que no estén expresamente aprobados por la parte responsable del cumplimiento podrían anular la autoridad del usuario para operar este equipo.

6.3 Instrucciones y avisos generales

Lea detenidamente el presente manual antes de utilizar el producto. Siga todas las instrucciones y recomendaciones aquí recogidas.

La utilización del producto de manera contraria a dichas instrucciones puede provocar un mal funcionamiento del mismo, dañarlo o destruirlo.

El fabricante no se responsabiliza de los daños derivados de la utilización del producto de manera distinta a la aquí descrita, de la aplicación indebida o del incumplimiento de las recomendaciones y advertencias aquí contenidas.

En caso de que se utilice o se conecte el producto de manera distinta a la indicada en el presente documento, el fabricante no se responsabilizará de las consecuencias derivadas de tales prácticas inapropiadas.

Asimismo, el fabricante tampoco se hace responsable del daño ni de la destrucción del producto como consecuencia de una colocación errónea del mismo, una instalación incorrecta, un manejo indebido o un uso en contradicción con lo aquí descrito.

El fabricante no asume ningún tipo de responsabilidad por el mal funcionamiento, el daño o la destrucción del producto por causa de la sustitución indebida de piezas o del uso de piezas o componentes no originales.

El fabricante no se responsabiliza de las pérdidas o daños derivados de desastres naturales o situaciones semejantes ocasionadas por la naturaleza.

Asimismo, tampoco se responsabiliza de los posibles daños ocasionados al producto durante su transporte.

El fabricante no ofrece ninguna garantía en cuanto a la pérdida o daño de datos.

El fabricante no se responsabiliza de los fallos o daños, directos o indirectos derivados de la utilización del producto de manera contraria a la indicada en el presente manual.

Es obligatorio respetar todos los reglamentos legales vigentes en relación con la instalación y el uso del producto, así como las disposiciones referentes a los estándares técnicos de las instalaciones eléctricas. El fabricante no se responsabiliza del daño o la destrucción del producto ni de los daños del consumidor, si el producto se utiliza y se manipula de forma distinta a la indicada en dichas normativas y disposiciones.

El consumidor debe, a su cargo, obtener software de protección para el producto. El fabricante no se responsabiliza del daño derivado del uso de software de seguridad deficiente o poco adecuado.

El consumidor debe cambiar de inmediato la contraseña de acceso tras la instalación del producto. El fabricante no se responsabiliza de los daños que el consumidor pueda sufrir en relación con el uso de la contraseña original.

El fabricante tampoco asume responsabilidad alguna por los costes adicionales en los que incurra el consumidor al realizar llamadas a través de una línea con una tarifa elevada.

Gestión de baterías usadas y residuos eléctricos

No deposite dispositivos eléctricos y baterías usadas en los contenedores de residuos municipales. Recuerde que la eliminación indebida de residuos daña el medioambiente.

Entregue los dispositivos eléctricos y sus baterías al final de su vida útil en lugares o contenedores acondicionados para tal fin, o devuélvalos al proveedor o fabricante para que su eliminación se haga respetando el medioambiente. El proveedor o fabricante deberá recoger el producto de manera totalmente gratuita y sin exigir otra compra. Asegúrese de que los dispositivos que desecha están completos.

No tire baterías al fuego. No divida las baterías en pedazos ni produzca su cortocircuito.