



# Intercomunicadores IP

Manual de configuración



# Tabla de contenidos

<b>Primer acceso</b> .....	<b>4</b>
Encontrar dispositivos en la red .....	4
Nombre de dominio .....	4
Dirección IP del dispositivo .....	4
Conmutación DHCP .....	6
Acceso a la configuración del dispositivo a través de la web .....	7
Cambio de contraseña .....	8
Navegadores recomendados .....	8
<b>Ajustes básicos del dispositivo</b> .....	<b>9</b>
Actualización del firmware .....	9
Directorio .....	10
Gestión masiva de usuarios en Access Commander o My2N .....	10
Llamar .....	10
Creación de contactos de llamada .....	10
Añadir un dispositivo local 2N .....	11
Marcación de llamadas en el dispositivo .....	11
Llamadas a través de SIP .....	13
Llamadas locales entre dispositivos 2N .....	14
Accesos .....	15
Verificación del usuario .....	15
En la interfaz de configuración web .....	15
Estableciendo un perfil temporal .....	15
Desde llamada (DTMF) .....	15
Uso de la API HTTP .....	16
Estableciendo la automatización .....	16
Configuración de acceso de usuarios .....	16
Configuración del acceso Bluetooth .....	22
Configuración de la autenticación de matrículas .....	24
Control del ascensor .....	24
Ajuste del interruptor de la puerta .....	24
Módulos .....	25
Ajustes de pantalla .....	25
Para cargar su propio idioma de visualización .....	25
Presentación .....	26
Modo Demo ( <b>2N IP Style</b> ) .....	26
Informes informativos ( <b>2N IP Style</b> ) .....	27
<b>Ajustes avanzados</b> .....	<b>29</b>
Ajustes de cámara y vídeo .....	29
Ajustes internos de la cámara .....	29
Cámara externa .....	31
Creación de un flujo de vídeo .....	32
Ajustes de sonido .....	33
Ajuste del volumen del dispositivo .....	33
Transmisión de audio en las llamadas .....	33
Sonidos de usuario .....	34
Otras características de audio del dispositivo .....	34
Perfiles de tiempo .....	35
Vacaciones .....	35
Configuración avanzada de la cuenta SIP .....	36
Funciones SIP .....	36
Medios de comunicación .....	36
Configuración avanzada .....	36
<b>Sistema</b> .....	<b>38</b>

Ajustes de fecha y hora .....	38
Sincronización con NTP .....	38
Actualización de la hora en caso de interrupción .....	38
Configuración de la red .....	38
Licencia .....	39
Actualización de la clave de licencia .....	39
Licencia de prueba .....	39
Puertos utilizados .....	40
<b>Automatización .....</b>	<b>44</b>

# Primer acceso

## Encontrar dispositivos en la red

Para poder acceder a la interfaz 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 de dominio

Para acceder a la interfaz de configuración web, puede introducir un nombre de dominio en el navegador con el formato "hostname.local" en lugar de la dirección IP. El nombre de host de un nuevo dispositivo está formado por el nombre del producto y el número de serie del dispositivo. Cuando introduzca un nombre de host, utilice sólo letras y números; no utilice espacios, puntos, guiones ni otros caracteres especiales.

**El nombre de dominio predeterminado del dispositivo** : 2NIPIntercom20-{número de serie sin guiones}.local (p.ej.: "2NIPIntercom20-0000000001.local")

El formato del nombre del dispositivo específico se especifica en el Manual de instalación del producto en el capítulo Nombre de dominio.



#### SUGERENCIA

Puede cambiar el nombre de host más tarde en la interfaz de configuración web en **Sistema > Conexión de red > pestaña Configuración avanzada > Nombre de host**.

Iniciar sesión con un nombre de dominio tiene la ventaja de utilizar la dirección IP dinámica del dispositivo. Mientras la dirección IP dinámica cambia, el nombre de dominio sigue siendo el mismo. Es posible generar certificados firmados por una autoridad certificadora confiable para un nombre de dominio.

## Dirección IP del dispositivo

Por defecto, el dispositivo utiliza una dirección IP dinámica asignada por el servidor DHCP.

Para averiguar la dirección IP de un dispositivo 2N de su red local, utilice la utilidad 2N IP Utility. La aplicación 2N IP Utility se puede descargar de las páginas web [2N.com](http://2N.com). Para la instalación es necesario tener instalado Microsoft .NET Framework 4.7.2.

Dependiendo de las capacidades del aparato, también puede averiguar la dirección IP de una de las siguientes maneras:

- Botón de marcación rápida
- en la pantalla del aparato (consulte la Guía de instalación del producto para conocer el procedimiento)

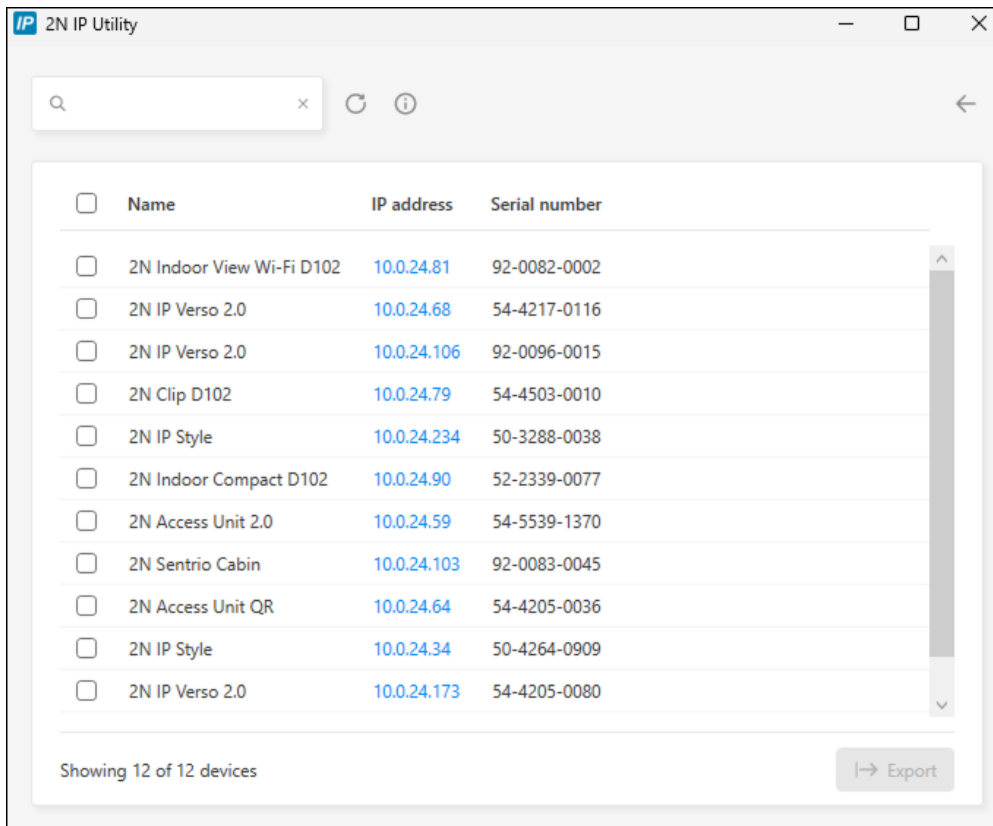
## Encontrar la dirección IP usando 2N IP Utility

Para averiguar la dirección IP de un dispositivo 2N de su red local, utilice la utilidad 2N IP Utility. La aplicación 2N IP Utility se puede descargar de las páginas web [2N.com](http://2N.com). Para la instalación es necesario tener instalado Microsoft .NET Framework 4.7.2.

1. Ejecute el instalador 2N IP Utility.
2. El asistente de instalación lo guía a través del proceso de instalación.

- Después de instalar la aplicación 2N IP Utility ejecute la aplicación desde el menú Inicio del sistema operativo Microsoft Windows.

Después de iniciarse, la aplicación comenzará a buscar automáticamente en la red local todos los dispositivos 2N y AXIS que tengan una dirección IP asignada por DHCP o configurada estáticamente. Estos dispositivos se mostrarán luego en la tabla.



<input type="checkbox"/>	Name	IP address	Serial number
<input type="checkbox"/>	2N Indoor View Wi-Fi D102	10.0.24.81	92-0082-0002
<input type="checkbox"/>	2N IP Verso 2.0	10.0.24.68	54-4217-0116
<input type="checkbox"/>	2N IP Verso 2.0	10.0.24.106	92-0096-0015
<input type="checkbox"/>	2N Clip D102	10.0.24.79	54-4503-0010
<input type="checkbox"/>	2N IP Style	10.0.24.234	50-3288-0038
<input type="checkbox"/>	2N Indoor Compact D102	10.0.24.90	52-2339-0077
<input type="checkbox"/>	2N Access Unit 2.0	10.0.24.59	54-5539-1370
<input type="checkbox"/>	2N Sentries Cabin	10.0.24.103	92-0083-0045
<input type="checkbox"/>	2N Access Unit QR	10.0.24.64	54-4205-0036
<input type="checkbox"/>	2N IP Style	10.0.24.34	50-4264-0909
<input type="checkbox"/>	2N IP Verso 2.0	10.0.24.173	54-4205-0080

Showing 12 of 12 devices Export

- Seleccione de la lista el dispositivo que desea configurar y haga clic con el botón izquierdo del ratón. Se abrirá la parte derecha de la ventana de configuración web.



#### SUGERENCIA

- También se puede acceder a la interfaz de configuración web a través del botón **Abrir en navegador externo**, que permite abrir la interfaz en una ventana independiente del navegador.
- Pulse sobre un dispositivo de la lista para ver información detallada. Pulse el botón **IP settings** para cambiar la dirección IP introduciendo la dirección IP estática deseada o activando DHCP.
- La aplicación también le permite exportar los dispositivos seleccionados a un archivo CSV. En primer lugar, seleccione el dispositivo marcando las casillas de cada dispositivo de la lista y, a continuación, utilice el botón **Exportar** que aparece en la parte inferior de la ventana. El archivo exportado contendrá el nombre, la dirección IP y el número de serie de los dispositivos seleccionados.

Las credenciales predeterminadas son:

Nombre de usuario: **Admin**

Contraseña: **2n**

Después de iniciar sesión por primera vez, debes cambiar tu contraseña inmediatamente.



### SUGERENCIA

Se recomienda utilizar una contraseña que sea difícil de descifrar. No se recomienda utilizar nombres, nombres de lugares o cosas en la contraseña, especialmente aquellos que tienen una conexión directa con el usuario.

Para una mayor seguridad de la contraseña, recomendamos:

- utilizar un generador de contraseñas aleatorias,
- longitud de la contraseña de al menos 12 caracteres,
- una combinación de diferentes caracteres de diferentes conjuntos de caracteres (por ejemplo, letras minúsculas/mayúsculas, números, caracteres especiales, etc.).

## Encontrar la dirección IP usando el botón de marcación rápida

Para encontrar la dirección IP de , proceda de la siguiente manera:

1. Conecte el dispositivo a la red eléctrica (si ya está conectado, desconéctelo y vuelva a conectarlo).
2. Pulse 5 veces el primer Botón de marcación rápida de la unidad principal.
3. El dispositivo lee su dirección IP.



### NOTA

- Si la dirección es 0.0.0.0, significa que el dispositivo no ha obtenido la dirección IP del servidor DHCP.
- Por motivos de seguridad se puede introducir la secuencia de los botones dentro de un máximo de treinta segundos a partir de la señal acústica. Entre cada pulsado puede haber una pausa no superior a 2 s.

## Conmutación DHCP

Por defecto, el dispositivo utiliza una dirección IP dinámica asignada por el servidor DHCP.

### Dirección IP dinámica

DHCP (Dynamic Host Configuration Protocol) es un protocolo de red que mantiene una lista de direcciones IP disponibles y las asigna automáticamente a los dispositivos de la red local. La dirección IP asignada es dinámica, por lo que al dispositivo se le puede asignar una nueva dirección IP tras un periodo de tiempo (tiempo de arrendamiento).

### Dirección IP estática

Si desea que la dirección IP del dispositivo permanezca inalterada, debe desactivar la asignación de direcciones IP por parte del servidor DHCP en el dispositivo. Puede desactivar el servidor DHCP en la interfaz de configuración web o mediante el hardware del dispositivo.



### NOTA

Los valores específicos para la dirección IP estática sólo pueden establecerse en la interfaz de configuración web del aparato.

## Configuración de los parámetros de red en la interfaz de configuración web

1. Vaya a la interfaz de configuración web.
2. Vaya a **Sistema > Conexión de red > pestaña Configuración básica > Configuración de la dirección IP**.
3. Ajuste los parámetros de red deseados.
4. Guarde los cambios.

## Cambio de DHCP en el hardware del dispositivo

Dependiendo de las capacidades del aparato, la dirección IP puede conmutarse de la siguiente manera:

- Botón de marcación rápida
- en la pantalla del aparato (consulte la Guía de instalación del producto para conocer el procedimiento)



### SUGERENCIA

Consulte el manual de instalación del producto para conocer la ubicación del botón RESET.

## Encontrar la dirección IP usando el botón de marcación rápida

Para encontrar la dirección IP de , proceda de la siguiente manera:

1. Conecte el dispositivo a la red eléctrica (si ya está conectado, desconéctelo y vuelva a conectarlo).
2. Pulse 5 veces el primer Botón de marcación rápida de la unidad principal.
3. El dispositivo lee su dirección IP.



### NOTA

- Si la dirección es 0.0.0.0, significa que el dispositivo no ha obtenido la dirección IP del servidor DHCP.
- Por motivos de seguridad se puede introducir la secuencia de los botones dentro de un máximo de treinta segundos a partir de la señal acústica. Entre cada pulsado puede haber una pausa no superior a 2 s.

## Acceso a la configuración del dispositivo a través de la web

La configuración del dispositivo se realiza a través de una interfaz de configuración basada en web a la que se puede acceder desde un navegador web.

Para poder acceder a la interfaz 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.



También se puede acceder a la interfaz de configuración basada en web desde el portal My2N conectado o desde la herramienta de configuración 2N Access Commander.

## Inicio e sesión en la interfaz de web de configuración

1. Inicie su navegador de Internet.
2. Introduzca la dirección IP del dispositivo o el nombre de dominio del dispositivo (consulte el capítulo [Encontrar dispositivos en la red \(p. 4\)](#)).

3. En el caso de que no disponga del certificado para la dirección IP, es posible que aparezca una advertencia sobre que el certificado de seguridad no es válido. En tal caso hay que confirmar que quiere pasar a la interfaz de web de configuración.
4. Aparecerá la pantalla de inicio de sesión.
5. Ingrese su información de inicio de sesión.  
Las credenciales predeterminadas son:
  - Nombre de usuario: **Admin**
  - Contraseña: **2n**
6. Tras el primer inicio de sesión cambie la contraseña.

### Acceso desde 2N Access Commander

1. Inicie sesión en la interfaz Access Commander.
2. Vaya a  Dispositivos.
3. Para el dispositivo seleccionado, pulse .

### Cambio de contraseña

Debe cambiar la contraseña predeterminada para acceder completamente a las funciones de la interfaz de configuración web. No puede configurar el dispositivo sin cambiar la contraseña predeterminada.



#### SUGERENCIA

Se recomienda utilizar una contraseña que sea difícil de descifrar. No se recomienda utilizar nombres, nombres de lugares o cosas en la contraseña, especialmente aquellos que tienen una conexión directa con el usuario.

Para una mayor seguridad de la contraseña, recomendamos:

- utilizar un generador de contraseñas aleatorias,
- longitud de la contraseña de al menos 12 caracteres,
- una combinación de diferentes caracteres de diferentes conjuntos de caracteres (por ejemplo, letras minúsculas/mayúsculas, números, caracteres especiales, etc.).

### Navegadores recomendados

La interfaz de configuración web está optimizada para navegadores basados en Chrome (como Google Chrome, Microsoft Edge u Opera). Al utilizar otros navegadores, puede haber ligeras diferencias de funcionalidad en el aspecto de la interfaz.

# Ajustes básicos del dispositivo

## Actualización del firmware

Las nuevas versiones del firmware están disponibles en el servidor de actualización. Si la interfaz de configuración web no tiene acceso a la Internet pública, es posible cargar el archivo de firmware manualmente en el dispositivo.



### NOTA

Las actualizaciones del firmware no son automáticas. Para garantizar la integridad del sistema y eliminar fallos involuntarios, todas las actualizaciones deben ser confirmadas manualmente o iniciadas por el usuario. Antes de realizar cualquier actualización, consulte las notas de la nueva versión y verifique la compatibilidad con su infraestructura actual.

## Obtener el firmware del servidor de actualización



### ATENCIÓN

En la versión 3.0.0, las actualizaciones del firmware desde el servidor de actualización sólo están disponibles desde la versión anterior de la interfaz web.

- a. En la cabecera de la interfaz de configuración web, haga clic en **Ir a la interfaz antigua**.

1. Vaya a **Sistema > Mantenimiento > pestaña Firmware**.
2. Haga clic en **Buscar actualizaciones**.
3. Cuando una actualización está disponible, se cargan sus notas de publicación. Para iniciar la actualización, haga clic en **Actualización** en la cabecera de la ventana.
4. Una vez que el firmware se ha cargado correctamente, el aparato se reinicia automáticamente. Tras el reinicio el dispositivo está plenamente disponible con un nuevo firmware. La actualización del firmware no afecta a la configuración.

## Carga de nuevo firmware desde el almacenamiento

1. Vaya a **Sistema > Mantenimiento > pestaña Firmware**.
2. Haga clic en **Cargar Firmware**.
3. En el cuadro de diálogo que se abre, seleccione un archivo de su propio repositorio.
4. Confirme la carga del archivo pulsando en **Cargar**.  
El dispositivo verifica el archivo de firmware y no permite cargar un archivo incorrecto o dañado.
5. Una vez que el firmware se ha cargado correctamente, el aparato se reinicia automáticamente. Tras el reinicio el dispositivo está plenamente disponible con un nuevo firmware. La actualización del firmware no afecta a la configuración.

## Directorio

La sección Directorio es una parte clave de la configuración del dispositivo. Usted crea usuarios en el directorio y gestiona sus derechos de acceso o los parámetros de la conexión telefónica. Cada usuario puede actuar como titular de derechos de acceso, como contacto de llamada o como ambos a la vez.

### Añadir manualmente un usuario a un directorio

1. En la página Directorio, haga clic en **Añadir usuario**.
2. Se abrirá el detalle del usuario. En la pestaña Información personal, asigne un nombre al usuario.
3. Establezca el número de teléfono del dispositivo del contacto según [Creación de contactos de llamada \(p. 10\)](#).
4. Configure las opciones de acceso según [Accesos \(p. 15\)](#).

### Gestión masiva de usuarios en Access Commander o My2N

Si el dispositivo se gestiona a través de las herramientas de configuración masiva Access Commander o My2N, cualquier cambio realizado en la interfaz de configuración basada en web se sobrescribirá con los ajustes de la herramienta de configuración masiva. Un usuario creado directamente en la interfaz web será eliminado.

La columna titular de la tabla de directorios enumera la herramienta de configuración masiva que creó el usuario. La columna del soporte está oculta por defecto.

## Llamar

El dispositivo 2N permite varias formas de conectar las llamadas. Antes de poder crear contactos y configurar el método de marcación, deberá activar y configurar los servicios que mediarán en la llamada:

- [Llamadas a través de SIP \(p. 13\)](#)
- [Llamadas locales entre dispositivos 2N \(p. 14\)](#)
- otras integraciones especiales


### Creación de contactos de llamada

La creación de un contacto de llamada consiste en añadir un número de teléfono al usuario correspondiente en el directorio del dispositivo.



#### SUGERENCIA

Puede utilizar la función de llamadas locales para conectarse a otro aparato 2N de su red local, consulte [Añadir un dispositivo local 2N \(p. 11\)](#).

1. Vaya a **Directorio**.
2. Abra el detalle del usuario haciendo clic en la fila o seleccione **Añadir usuario** para crear un nuevo usuario.
3. En la pestaña **Números de teléfono de** abra la edición del número de teléfono haciendo clic en el icono .
4. Seleccione **Tipo de llamada**, en la que el contacto debe estar disponible (SIP, red local, MS Teams, VMS, ...).
  - [Llamadas a través de SIP \(p. 13\)](#) - para servicios y cuentas VoIP
  - [Llamadas locales entre dispositivos 2N \(p. 14\)](#) - para llamadas a dispositivos 2N
  - MS Teams, VMS,... - para integraciones especiales
5. Introduzca el número o la dirección de destino a la que desea que llame el aparato. Introduzca el número de extensión, el URI SIP (por ejemplo, "sip:101@192.168.1.50"), el nombre de dominio (por ejemplo, "2NIPVerso20-22222222" u otro número según corresponda al tipo de llamada).

6. En el campo **Opciones**, configure las características adicionales de la llamada que afectan a su comportamiento.  
Estas opciones permiten al administrador configurar la seguridad, la funcionalidad y la lógica de marcación para adaptarlas a las necesidades exactas de la instalación, por ejemplo, para utilizar la transmisión encriptada, acelerar la conexión o habilitar la inversión de la puerta.
7. En la sección **Disponibilidad de**, especifique el límite de tiempo en el que se puede llamar al número. Por ejemplo, puede establecer la disponibilidad sólo para las horas de trabajo del usuario.
8. Guarde el cambio haciendo clic en **Confirme**.
9. Si desea utilizar el botón de marcación rápida para llamar al contacto, asígnele un botón en la pestaña **Botones**.

## Configuración de 2N IP Eye

La aplicación 2N IP Eye le permite ver el vídeo del interfono IP en la pantalla de su ordenador. Tras introducir la dirección **del 2N IP Eye**, cuando un contacto realiza una llamada entrante, el vídeo se muestra en el ordenador.

## Añadir un dispositivo local 2N



### ATENCIÓN

Las llamadas locales deben estar activadas tanto en este dispositivo como en el que se está buscando con la misma **Clave de acceso** configurada, consulte [Llamadas locales entre dispositivos 2N \(p. 14\)](#).

1. En la página **Directorio** haga clic en **Añadir dispositivo local**.
2. En el cuadro de diálogo que se abre, marque el dispositivo al que desea conectarse.
3. Seleccione **Añadir al directorio**.
4. Aparece un nuevo usuario en la guía con un número de teléfono configurado.
5. Haga clic en la fila del usuario para seguir editándola.



### SUGERENCIA

Para configurar los derechos de acceso del titular de este dispositivo, siga las instrucciones de [Accesos \(p. 15\)](#).

## Marcación de llamadas en el dispositivo

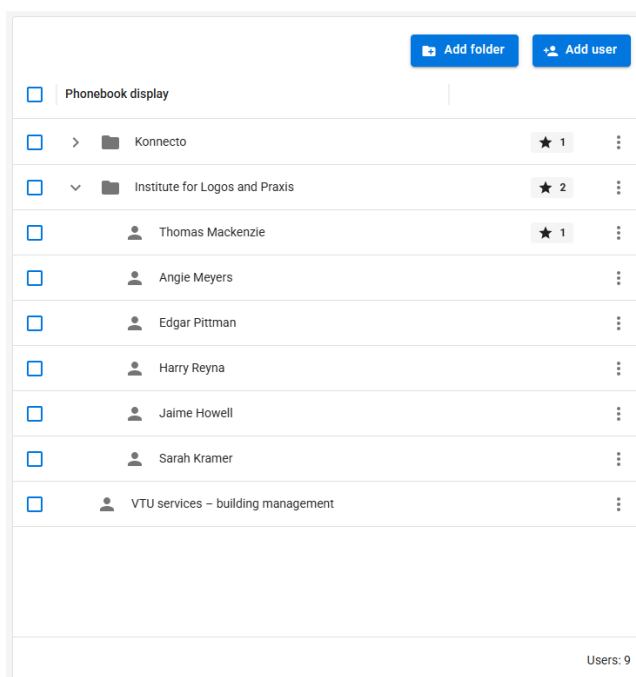
### Asignación de los botones del marcado rápido

Para asignar contactos a los botones de marcación rápida, vaya a **Llamadas > Marcación > pestaña Botones de marcación rápida**.

Aquí también se ajustan los botones para la selección rápida de los módulos conectados a la unidad principal a través del VBUS.

### Para visualizar los contactos de la agenda en la pantalla

Para configurar la visualización y el orden de los contactos en la pantalla del dispositivo, vaya a **Llamadas > Marcación > pestaña Visualización de la agenda**.




Todos los contactos con un número de teléfono asignado se almacenan por defecto en la carpeta troncal. Los contactos pueden clasificarse además en carpetas, por ejemplo por departamento o planta del edificio.


### Mover contactos a una carpeta


1. En la cabecera de la tabla de la guía telefónica, cree una nueva carpeta y asígnele un nombre.



#### SUGERENCIA

En el menú de extensión  para una carpeta, puede añadir una imagen a la carpeta bajo la cual aparecerá en la pantalla en la vista de Agenda.


2. Para mover sus contactos a otra carpeta, primero selecciónelos y después haga clic en .
3. Seleccione una nueva ubicación dentro de la guía telefónica.
4. Guarde los cambios haciendo clic en **Mover**.

En cada carpeta, los contactos suelen estar ordenados alfabéticamente. Este orden puede modificarse ajustando la prioridad (en el menú ampliado  para el contacto).

Un usuario recién creado con un número de teléfono aparecerá automáticamente en la carpeta troncal.

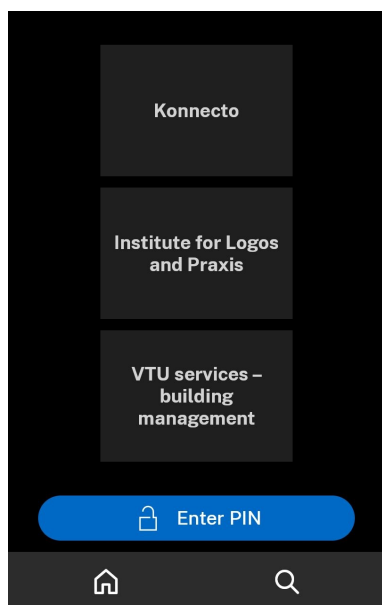
### Grupos de llamada

Los grupos de llamadas permiten llamar a varios contactos a la vez (por ejemplo, llamar a la recepción y al almacén al mismo tiempo).

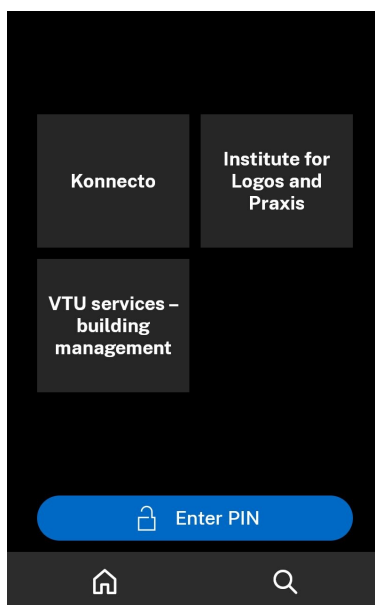
1. En la tabla de la vista de la agenda, **seleccione todos los contactos que desee que formen parte del grupo**.
2. Encima de la tabla, haga clic en .
3. Introduzca el nombre del grupo de llamada y su ubicación dentro de la guía telefónica.
4. Seleccione si desea mantener los contactos visibles como contactos individuales o sólo mostrarlos en la agenda bajo el grupo de llamada.
5. Guarde los cambios haciendo clic en **Mover**.

## Ajustes de pantalla 2N IP Style

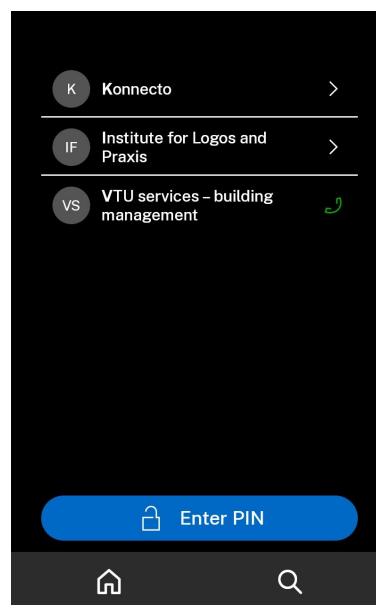
En la pestaña izquierda **Configuración de la pantalla** puede seleccionar entre las siguientes formas de mostrar el directorio en la pantalla del dispositivo **2N Estilo IP**.



Tarjetas (1 columna)



Tarjetas (2 columnas)



Phonebook

## Llamadas a través de SIP

### Registro del dispositivo en el servidor SIP

El registro en el servidor SIP es crucial para la plena funcionalidad del dispositivo en un entorno SIP.

1. Vaya a **Llamadas > SIP** de la cuenta que desee configurar.
2. Habilite la cuenta SIP en la parte superior.
3. En la pestaña , **Identidad del dispositivo**, rellene:
  - **Nombre para mostrar** - este texto se mostrará a la otra parte como identificador de llamada.
  - **Número de teléfono (ID)** - este número, junto con el dominio, identifica de forma exclusiva el dispositivo durante las llamadas y el registro.
  - **Dominio** – configura el nombre de dominio del servicio en el que se registra el dispositivo. Normalmente coincide con la dirección SIP proxy o con el SIP registrador.Estos tres valores juntos identifican al dispositivo en el entorno SIP.
4. En **Authentication**, rellene las credenciales de inicio de sesión asignadas por el administrador del servidor SIP para autenticar el dispositivo en el servidor proxy SIP. Esta autenticación impide el acceso no autorizado, las llamadas fraudulentas o la suplantación de identidad.  
Si no se rellena el ID de autenticación , el dispositivo se autenticará con **Número de teléfono**.
5. En **Opciones de protocolo de transporte**, seleccione el protocolo utilizado por el servidor SIP.
6. Active la función **SIP Registrar** tab feature.

7. Introduzca los datos del registrador SIP en el que desea registrar el dispositivo 2N.  
Si deja en blanco el parámetro **Puerto** o el valor del parámetro es 0, se aplicará el puerto por defecto según el protocolo de transporte seleccionado.

### Valores de puerto por defecto según el protocolo de transporte

Cuenta	UDP / TCP	TLS
SIP 1	5060	5061
SIP 2	5062	5063
SIP 3	5064	5065
SIP 4	5066	5067

8. La cabecera de la pestaña muestra el estado del registro y muestra los mensajes de error de registro.



#### NOTA

En el capítulo [Configuración avanzada de la cuenta SIP \(p. 36\)](#) se describen otros ajustes de la cuenta SIP.

## Configuración de la dirección IP pública del dispositivo

Este ajuste se utiliza cuando el dispositivo se encuentra detrás de un router (NAT) y se comunica con el panel de control fuera de la red local (por ejemplo, en la nube o a través de Internet). En la comunicación SIP, el dispositivo debe especificar la dirección IP pública con la que es accesible desde Internet. Si enviara su dirección IP interna, la centralita no podría enrutar la llamada o el flujo de datos RTP correctamente.

Si el aparato y la centralita están en la misma red local, no es necesario configurar una dirección IP pública.

- Vaya a **Llamadas > SIP** de la cuenta que desee configurar.
- En la pestaña, **seleccione la dirección IP pública** entre las siguientes opciones :
  - STUN (Automático)**  
Introduzca los datos de su servidor STUN.
  - Introducir manualmente**  
Introduzca su propia dirección IP externa para el dispositivo.

## Llamadas locales entre dispositivos 2N

Es posible establecer las llamadas locales entre dispositivos 2N IP, que permiten la comunicación directa entre dispositivos 2N dentro de una red local sin necesidad de conectarse a un servidor SIP o a una infraestructura externa.

### Para activar las llamadas locales

- Vaya a **Llamadas > Llamadas locales**.
- Habilite la función en la cabecera de la página.

3. Establezca claves de acceso para garantizar una comunicación segura con otros dispositivos de la red. Las claves de acceso garantizan que sólo los dispositivos con claves idénticas puedan comunicarse entre sí. Esto contribuye a la seguridad y a la capacidad de definir grupos independientes de dispositivos.

## Accesos

Una de las funciones básicas del dispositivo es gestionar el acceso y el desbloqueo de la cerradura eléctrica de la puerta. El dispositivo gestiona el acceso basándose en la evaluación de las solicitudes de acceso según unas reglas de acceso predefinidas. Si el dispositivo considera que la solicitud es legítima, activa el interruptor de la puerta que controla el cierre eléctrico de la puerta. Esto desbloqueará la puerta.

Además de la autenticación de usuario convencional (tarjeta RFID, biometría, Bluetooth, etc.), el interruptor también puede activarse mediante señales e interfaces externas, lo que ofrece opciones flexibles de integración y automatización. A continuación se describen las diferentes formas de activar el interruptor de la puerta:

## Verificación del usuario

El usuario utiliza su método de autenticación y si sus permisos de usuario se ajustan a las normas de acceso, se le concede el acceso. El acceso permitido activará el interruptor de la puerta.

La configuración se describe en el capítulo [Configuración de acceso de usuarios \(p. 16\)](#).

## En la interfaz de configuración web

1. Vaya a **Integración > Interruptores**.
2. Encuentre la tarjeta interruptor que controla la puerta.



### NOTA

La función del interruptor de puerta en el aparato la realiza **Interruptor 1**.

3. En **Control manual del interruptor** pulse **Mantenga**.
4. El interruptor permanecerá encendido hasta que vuelva a cancelar la retención en control manual.

## Estableciendo un perfil temporal

En la interfaz de configuración web, puede configurar el interruptor para que mantenga la puerta desbloqueada durante un periodo de tiempo predeterminado, por ejemplo durante la hora de comer.

1. Vaya a **Integración > Interruptores**.
2. Encuentre la tarjeta interruptor que controla la puerta.



### NOTA

La función del interruptor de puerta en el aparato la realiza **Interruptor 1**.

3. Pulse en la flecha del interruptor seleccionado para ir a su detalle.
4. En la pestaña **Estado** active la opción **Interruptor de retención controlada por tiempo**.
5. Seleccione los perfiles temporales en los que debe mantenerse el interruptor o introduzca un periodo de tiempo personalizado.

## Desde llamada (DTMF)

### Ajustes del código DTMF


1. Vaya a **Integración > Interruptores**.

- Encuentre la tarjeta interruptor que controla la puerta.



**NOTA**

La función del interruptor de puerta en el aparato la realiza **Interruptor 1**.

- Pulse en la flecha  del interruptor seleccionado para ir a su detalle.
- En la pestaña **Códigos de activación de**, puede configurar los códigos que podrá introducir mediante DTMF durante una llamada con el aparato.  
La validez de cada código puede estar limitada en el tiempo.



**NOTA**

Para el primer código de activación, puede establecer que se procese como una forma más antigua del código. De esta forma, no tendrá que confirmar el código con un asterisco al introducirlo en el teclado del teléfono.

## Utilización del código DTMF

- Cuando esté conectado al aparato, introduzca el código de activación en el teclado de su teléfono y confírmelo con un asterisco.



**NOTA**

La recepción de señales DTMF está activada por defecto en el aparato. Puede comprobar los permisos en la página Servicio de llamadas (SIP/Llamadas locales) en la pestaña **Audio**, en la pestaña **Recibir DTMF**.

## Uso de la API HTTP

El uso completo, incluida una descripción de la autorización necesaria de la API HTTP, se describe en el manual de la API HTTP [para dispositivos 2N](#). El interruptor de la puerta está controlado por el punto final `api switch ctrl`. Para el conmutador 1, el comando tiene el siguiente aspecto: `https://ip_adre-sa/api/switch/ctrl?switch=1&action=on`.

## Estableciendo la automatización

La configuración de la automatización se describe en el manual de automatización <https://wiki.2n.com/hip/auto>. El interruptor se activa mediante la acción **ActivateSwitch**.

## Configuración de acceso de usuarios

Para autenticarse correctamente en la unidad de control de acceso y desbloquear la puerta, el usuario debe cumplir dos condiciones: tener derechos de acceso asignados al dispositivo y tener establecido al menos un método de autenticación. Los métodos de autenticación disponibles dependen del dispositivo específico y pueden incluir tarjetas RFID, PIN numérico, código QR para escanear con la cámara, etc.

### Configuración de la autenticación:

- Vaya a **Directorio**.
- Abra el detalle del usuario haciendo clic en la fila o seleccione **Añadir usuario** para crear un nuevo usuario.
- En la pestaña **Autenticación** configure todos los métodos por los que se autenticará el usuario, consulte [Métodos de autenticación \(p. 17\)](#).

4. En la pestaña **Configuración de acceso de**, rellene cuándo se debe conceder al usuario acceso para entrar y salir.
- En cualquier momento
  - Perfil de tiempo - ofrece perfiles de tiempo establecidos
  - Personalizado - utilice el botón **Editar** para establecer intervalos de tiempo exclusivos para este usuario

Establezca una fecha de caducidad para limitar el acceso del usuario a un periodo concreto del calendario.

La concesión de **Exceptions** proporcionará al usuario un acceso permanente que no restringirá ni siquiera el bloqueo temporal del dispositivo indicado por las reglas de acceso (véase [Reglas de acceso](#) (p. 19)).

## Métodos de autenticación



### ATENCIÓN

Los métodos de autenticación disponibles dependen del dispositivo específico y de los módulos conectados.

## Tarjeta RFID

A un usuario se le pueden asignar hasta 2 tarjetas RFID.

El identificador puede introducirse manualmente mediante el teclado o leerse introduciendo la tarjeta en un lector USB conectado al ordenador.

### Requisitos de la tarjeta RFID

- El identificador debe ser un número hexadecimal.
- La longitud mínima del identificador es de 6 caracteres.
- Sólo se pueden utilizar tarjetas compatibles con el dispositivo - el tipo de tarjeta debe estar habilitado en la configuración del módulo (véase **Acceso > Módulos**).



### SUGERENCIA

Puede leer el identificador de una tarjeta existente en el registro en **Sistema > Registro de eventos**. Cargue la tarjeta nueva/no asignada en el dispositivo y, a continuación, copie su identificador (UUID) del registro. Después de introducir el identificador entre las tarjetas RFID, el usuario puede comenzar a utilizar la tarjeta para autenticarse.

## My2N

**My2N** – utilizado para conectarse a la aplicación My2N app habilitar la autenticación a través de Bluetooth.

## Código PIN / Código QR

El PIN sirve como código de acceso numérico personal, que el usuario introduce en el teclado del dispositivo o puede ser escaneado por la cámara del dispositivo en forma de código QR.



### ATENCIÓN

Los códigos QR sólo pueden leerse en la cámara interna del dispositivo.

### Requisitos del PIN

- La longitud mínima es de 2 dígitos.
- El código sólo puede contener dígitos (0-9).
- Los códigos QR sólo pueden utilizarse para PIN de entre 4 y 15 dígitos.
- Si utiliza la función de alarma silenciosa, le recomendamos que cree números PIN pares.



### NOTA

Si utiliza un código QR hexadecimal, deberá convertir el valor a formato decimal antes de introducirlo.

Rango hexadecimal aceptado: desde 1000 hasta FFFFFFFF.

### Huella dactilar

Cada usuario puede cargar hasta 2 huellas dactilares. Utilice un lector de huellas externo para cargarlas. Asegúrese de haber instalado el controlador USB 2N. Puede descargar el controlador [aquí](#).

La huella digital cargada por un usuario se puede utilizar para las siguientes acciones:

- Abre la puerta;
- Iniciar una alarma silenciosa: se puede configurar solo si la función Apertura de puerta está activa;
- Automatización F1 y F2: genera el evento FingerEntered en Automatización. F1 y F2 se utilizan para distinguir el dedo adjunto en Automatización.

### Matrícula

Algunos dispositivos admiten el reconocimiento de matrículas de vehículos mediante cámaras AXIS externas equipadas con la aplicación complementaria **VaxALPR**. Las matrículas reconocidas se envían en una petición HTTP al punto final `api/lpr/licenseplate` (más manual de la API HTTP para interfonos IP).



### SUGERENCIA

El procedimiento para añadir una cámara externa se describe en [???](#).

**Matrícula** – establece el número de matrícula del vehículo del usuario, que el dispositivo puede leer y utilizar para autenticar al usuario.

### Requisitos de la matrícula:

- La longitud máxima de una matrícula es de 10 caracteres.
- Se pueden asignar hasta 20 matrículas a un usuario.
- Cada matrícula debe asignarse a un solo usuario; si se realizan varias asignaciones, se utilizará el primer registro encontrado.

- Las matrículas se utilizan en la función de reconocimiento a partir de la imagen de la cámara externa (véase el manual de interoperabilidad).

### Tarjeta virtual

La tarjeta virtual se utiliza para identificar al usuario en los dispositivos conectados a través de la interfaz Wiegand. Tras la autenticación satisfactoria del usuario a través de la aplicación My2N o en el lector biométrico, el identificador de la tarjeta virtual se envía a la interfaz Wiegand (si el envío de identificadores está habilitado en la configuración, consulte **Acceso > Reglas de acceso > pestaña Acceso/Salida > Avanzado**).

#### Requisitos de la tarjeta virtual:

- El ID debe ser un número hexadecimal (caracteres 0-9, A-F).
- La longitud del ID es de 6 a 32 caracteres.
- A un usuario puede tener asignada solo una tarjeta virtual.

### Código de interruptor

**Cambiar código** – permite configurar hasta 4 códigos para activar interruptores (por ejemplo, cerradura de puerta). El código de interruptor se utiliza para abrir la cerradura usando el teclado del dispositivo, así como un código DTMF.

### Reglas de acceso

La página **Acceso > Reglas de acceso** establece los parámetros y la lógica para el desbloqueo de la puerta, que gestiona el interruptor de puerta del dispositivo. Esta configuración determina cómo se evalúan las solicitudes de acceso (autenticación), las condiciones necesarias para autorizar con éxito a un usuario y las reglas para gestionar los accesos individuales.

Mientras que usted define los permisos individuales en la configuración del usuario, las reglas de acceso determinan cuándo, bajo qué condiciones y cómo pueden utilizarse estos permisos. Por ejemplo, puede establecer si se permite el paso de la puerta en una sola dirección, si la autenticación puede activar una alarma silenciosa o si el usuario sólo puede autenticarse una vez por intervalo de tiempo definido.

### Estado de la puerta y la cerradura

La **pestaña Estado** muestra si el interruptor de la puerta está activo y si la puerta está abierta.

#### Puerta

- “Abierto” - se ha concedido el acceso, el interruptor de la puerta está cerrado y la puerta puede abrirse.
- “Cerrado” - la puerta está cerrada y no puede abrirse.

#### Cerradura

- “Desbloqueado” - el interruptor está activo, se puede accionar.
- “Bloqueado” - el conmutador está desactivado y no puede controlarse mediante reglas de acceso.



#### SUGERENCIA

El botón con el símbolo del candado de esta pestaña se utiliza para bloquear o desbloquear el conmutador desde la interfaz web.

### Detección de puertas

En la pestaña **Puertas se puede habilitar** para que la apertura no autorizada de una puerta o su apertura durante mucho tiempo active un evento. Este acontecimiento puede ser seguido por automatizaciones. Los eventos también se escriben en el logotipo del dispositivo.

## Llegada y salida


Un dispositivo puede utilizarse para gestionar pasillos en dos direcciones. Puede acoplar algunos módulos al dispositivo en el lado opuesto de la puerta y después colocar estos dos lados por separado. Así, puede restringir qué hora del día se permitirá el paso en la dirección **Llegada** y qué hora del día se permitirá el paso en la dirección **Salida**, o qué métodos de autenticación se aceptarán en una dirección determinada, etc.

## Asignación de módulos para la llegada o la salida

1. Vaya a **Acceso > Reglas de acceso**.
2. En la pestaña **Llegada** o **Salida**, haga clic en **Gestionar**.
3. Se abrirá un cuadro de diálogo con una lista de los módulos de gestión de acceso disponibles.
4. Arrastre y suelte los módulos en grupos según la dirección que deban proporcionar.



### SUGERENCIA

Haga clic en  para localizar un módulo concreto. El módulo activa una señal visual o acústica en función de sus capacidades.

## Reglas de acceso

Las reglas de acceso determinan qué métodos de autenticación se aceptarán para conceder el acceso. Es posible establecer varias reglas de acceso para diferentes perfiles horarios. Las reglas de acceso también pueden utilizarse para determinar cuándo debe denegarse cualquier acceso.

Puede utilizar reglas de acceso para restringir los métodos de autenticación aceptados, por ejemplo, puede obligar a los usuarios a utilizar una tarjeta RFID de 8:00 a 9:00.



### SUGERENCIA

La restricción de autenticación es útil para utilizarla en un dispositivo que gestione claves para **2N IP Fortis**. Así, los usuarios se verán obligados a actualizar regularmente las claves de **2N IP Fortis** en su tarjeta RFID.

Al configurar las reglas, puede elegir si desea utilizar un código de zona para abrir la puerta. **El código de zona** se aplica cuando el dispositivo se zonifica en una gestión masiva de dispositivos (como Access Commander). **El código de zona** también puede ajustarse manualmente en la sección **Avanzado**. Funciona de forma similar a **Código de activación del interruptor**; al introducirlo en el teclado del módulo se activará el interruptor de la puerta.

## Alarma silenciosa

La alarma silenciosa es un modo especial de apertura de la cerradura que le permite desencadenar una acción de seguridad de forma discreta. La alarma silenciosa se utiliza sobre todo en locales y edificios buscados por los ladrones: casinos, centros financieros, bancos, etc. Tras introducir el código PIN, la puerta se abre, pero al mismo tiempo se activa la alarma sin que el atacante se dé cuenta.

Al activar la alarma silenciosa se activará el evento **SilentAlarm**. Este acontecimiento puede ir seguido de una automatización, por ejemplo:

- Envío de una solicitud HTTP al sistema de seguridad.
- Tomar imágenes desde la cámara del dispositivo.
- Establecimiento de una llamada a un destino preestablecido.

## Activación de la alarma silenciosa

1. El usuario introduce un código superior a su PIN normal.  
Ejemplo: El usuario ha establecido un código PIN "1926". Introduzca el código "1927" para abrir la puerta. La puerta se abre y al mismo tiempo se activa el evento SilentAlarm.



### ATENCIÓN

Para poder abrir la puerta con un código PIN (aunque se active al mismo tiempo la alarma silenciosa), es necesario activar la pestaña **In/Out debajo de**.

## Bloqueo del acceso tras intentos fallidos

Tras cinco intentos de acceso fallidos consecutivos, el acceso se bloqueará durante 30 segundos. No se permitirá el acceso durante este periodo aunque la autenticación del usuario sea válida.

Esta función sólo bloquea el acceso mediante autorización del usuario. El interruptor de la puerta también puede conmutarse por otros métodos como DTMF, comando HTTP, etc.

## Lectura de códigos QR

El código PIN de acceso asignado al usuario o el código de activación del interruptor pueden ser leídos por la cámara en forma de código QR.

Para que la carga sea correcta, debe configurar el modo de lectura de códigos QR. Los códigos se almacenan siempre en el aparato en formato decimal. Cuando se leen en modo decimal, los códigos QR leídos deben coincidir exactamente con los códigos PIN (de 4 a 15 dígitos de longitud) almacenados en el dispositivo. En el modo hexadecimal, los códigos QR se convierten al formato de números decimales tras la lectura y luego se comparan con los códigos decimales almacenados. Los ceros preasignados se ignoran durante la lectura hexadecimal.



### NOTA

Rango hexadecimal aceptado: desde 1000 hasta FFFFFFFF.

Para la lectura de códigos QR, también puede configurarlo para que sólo active el evento **CodeEntered** en lugar de controlar el interruptor de la puerta. A continuación, este evento puede seguirse con otras acciones a través de Automatizaciones.

El código QR escaneado puede reenviarse a un sistema de control de acceso externo que se comunique a través de una interfaz Wiegand (véase ???).

## Anti-Passback

El anti-passback es una extensión del sistema de control de acceso que impide el reingreso durante un intervalo de tiempo determinado. El dispositivo en este modo sólo permitirá al usuario entrar una vez en un tiempo determinado. Después de que un usuario entre con éxito, el sistema registra este evento y el usuario sólo podrá acceder de nuevo al sistema una vez transcurrido el tiempo especificado. Este tiempo se establece cuando está activado el Anti-passback.

## Modos de la función Anti-passback

- “Difícil” - El usuario no puede atravesar el dispositivo en ninguna dirección durante el periodo de tiempo establecido. Se deniega el acceso al usuario hasta que expire el intervalo o el administrador del dispositivo restablezca el acceso.
- “Soft” - Las infracciones de las normas sólo se registran y pueden alertar al administrador, pero se permite el acceso al usuario.

## Transferencia de datos para Wiegand



### ATENCIÓN

Para reenviar datos Wiegand, es necesario conectar correctamente un módulo de expansión Wiegand al aparato. El módulo de expansión Wiegand no suele estar incluido en el paquete del producto.

La función de reenvío Wiegand permite al dispositivo reenviar los datos de identificación del usuario autenticado a un sistema de control de acceso externo que se comunice a través de la interfaz Wiegand. Esto garantiza la integración de los dispositivos 2N con los sistemas tradicionales de control de accesos. El ajuste le permite seleccionar el grupo adecuado para el enrutamiento de datos.

El reenvío de datos para Wiegand se configura en **Access > Access Rules > I/O > Advanced**. El envío de autorizaciones a los usuarios que han leído su código QR se configura en la pestaña **Acceso/Salida** para habilitar la lectura de códigos QR.

## Configuración del acceso Bluetooth

La autenticación del usuario vía Bluetooth se realiza a través de la aplicación My2N app, que el usuario deberá tener descargado en su teléfono móvil.



### ATENCIÓN

Actualmente, el ajuste del código de emparejamiento debe realizarse en la antigua interfaz de configuración.

## Crea un código de emparejamiento en el dispositivo.

1. Vaya a **Directorio** y abra el detalle del usuario para el que desea crear el código de correspondencia.
2. En la cabecera de la interfaz de configuración web, haga clic en [Ir a la interfaz antigua](#).  
Abre el detalle del usuario en la antigua interfaz de configuración.
3. En el bloque **WaveKey**, haga clic en .  
En el cuadro de diálogo que se abre se generará un código de emparejamiento que deberá introducir en la aplicación My2N de su dispositivo.

4. Abra la aplicación e ingrese el PIN de emparejamiento.



#### NOTA

Si ya tiene una aplicación conectada a otro dispositivo, puede introducir el PIN de emparejamiento a través del icono de añadir situado en la parte superior de la pantalla.

5. Siga las instrucciones de su teléfono móvil – acérquese al dispositivo en modo de emparejamiento y haga clic en **Iniciar emparejamiento**.



#### AVISO

Para teléfonos móviles con sistemas operativos más antiguos (Android 9/iOS 17 y anteriores), necesitarás utilizar una aplicación para emparejar. Clave móvil.

#### Emparejamiento en la aplicación móvil Clave móvil

1. Descarga la aplicación Clave móvil a tu teléfono móvil. La aplicación está disponible en [Tienda de aplicaciones](#) y [GooglePlay](#).
2. Abra la aplicación y habilítela Clave móvil acceso a Bluetooth.
3. Según el tipo de llave móvil, acercar el lector USB o dispositivo de emparejamiento con el teléfono móvil.
4. en la aplicación Clave móvil haga clic en el dispositivo ofrecido para emparejar.
5. La aplicación le solicita que ingrese un código PIN. Ingrese el código de emparejamiento y confirme su entrada.

## Métodos de autenticación Bluetooth

Se pueden establecer diferentes métodos de autenticación Bluetooth en la interfaz de configuración web.

- **Directamente en la aplicación móvil** - el usuario selecciona la puerta que desea abrir directamente en la aplicación móvil My2N. Si su dispositivo móvil se encuentra dentro del radio de alcance del dispositivo 2N, éste conectará con el dispositivo y si se cumplen las normas de acceso, la puerta se desbloqueará.
- **Acercando el teléfono móvil al dispositivo y tocando el dispositivo** - un usuario con un dispositivo móvil y Bluetooth activado se acerca al dispositivo 2N y toca el lugar de autenticación Bluetooth del dispositivo 2N, que suele estar marcado con el icono Bluetooth . Una vez establecida la conexión y verificados los derechos de acceso, se desbloquea la puerta.
- **Detección de movimiento** - Los dispositivos 2N con cámara detectan movimiento en los alrededores, activando automáticamente el Bluetooth. Si un dispositivo 2N detecta dentro de su alcance un dispositivo móvil de un usuario con acceso válido, la puerta se desbloqueará.

## Configuración de los métodos de autenticación Bluetooth aceptados

1. Vaya a **Acceso > Módulos**.
2. En la pestaña **del módulo Bluetooth** seleccione los métodos posibles en el campo **Iniciar autenticación**.
3. Si ha seleccionado “detección de movimiento”, seleccione el perfil con el que se va a detectar el movimiento.



#### NOTA

Los perfiles de detección de movimiento se configuran en **Personalización > Cámara > Cámara interna**.

## Configuración de la autenticación de matrículas

Algunos dispositivos admiten el reconocimiento de matrículas de vehículos mediante cámaras AXIS externas equipadas con la aplicación complementaria **VaxALPR**. Las matrículas reconocidas se envían en una petición HTTP al punto final `api/lpr/licenseplate` (más manual de la API HTTP para interfonos IP).



### SUGERENCIA

El procedimiento para añadir una cámara externa se describe en ???.


## Habilitación de los servicios API HTTP

La autenticación de la matrícula se evalúa en función de la solicitud HTTP. Por lo tanto, debe habilitar los servicios apropiados de la API HTTP en el dispositivo. Este ajuste aún se realiza en una versión más antigua de la interfaz de configuración web. Para conocer el procedimiento detallado, consulte [FAQ](#).


## Control del ascensor

Conectando el módulo de relé AXIS A9188 a un interfono 2N o a una unidad de control de acceso 2N, se puede controlar el acceso a plantas individuales del ascensor en el edificio. Se puede conectar un máximo de 8 de estos módulos de relé a un interfono 2N o a una unidad de acceso 2N, cada uno de los cuales puede controlar 8 plantas, para un total de 64 plantas. Para utilizar esta función, debe disponer de una licencia activa: para los interfonos IP (nº de pedido 9137916) o para las unidades de acceso (nº de pedido 9160401).

## Conexión con el ascensor

1. Conecte las entradas de los controladores del ascensor al relé AXIS A9188 y conecte el relé a la red IP. Anote la dirección IP del relé.  
Siga la documentación del módulo de relé de E/S AXIS A9188, disponible en <http://www.axis.com>.
2. Abra la interfaz de configuración web del dispositivo 2N que vaya a gestionar los accesos del ascensor.
3. Vaya a **Integration > Access Control > Elevator tab**.
4. En la pestaña **Módulos de relé (AXIS A9188)** habilite uno de los módulos.
5. Pulse el icono del lápiz  e introduzca la dirección IP del módulo de relés en el cuadro que se abre.
6. Si el acceso al relé está sujeto a autenticación, introduzca el nombre de usuario y la contraseña en la pestaña **General**.
7. Cuando el módulo de relés esté habilitado, los pisos que gestione este módulo aparecerán en la pestaña **Pisos de ascensor**. Puede nombrar cada piso.

## Establecimiento del acceso público al suelo

1. En la pestaña **Pisos del ascensor**, seleccione los pisos que serán accesibles al público (el acceso no está sujeto a autorización).
2. Haga clic en el icono del lápiz  situado junto a la planta seleccionada.
3. En los ajustes abiertos, active **Acceso público**.
4. Opcionalmente, limite el tiempo de acceso público seleccionando un perfil horario o estableciendo un tiempo de acceso personalizado.

## Ajuste del interruptor de la puerta

El interruptor de la puerta es una función lógica del dispositivo que controla la cerradura eléctrica de la puerta. El interruptor puede activarse de varias formas (por ejemplo, mediante un comando HTTP, una tarjeta RFID o una señal DTMF).

La función del interruptor de puerta en el aparato la realiza **Interruptor 1**.

La página **Acceso > Módulos** puede utilizarse entonces para asignar un módulo de acceso específico para controlar otro conmutador.

### Ajuste del interruptor de la puerta

1. Conecte los contactos eléctricos de la cerradura de la puerta (por ejemplo, el contacto magnético) a la entrada designada en el intercomunicador.
2. En la interfaz de configuración web, vaya a **Integración > Conmutadores**.
3. Abra los ajustes del Conmutador 1 pulsando en la flecha de la cabecera de la pestaña.
4. En la pestaña **Configuración del interruptor**, configure los parámetros de la salida de hardware que el interruptor de puerta va a controlar.
  - **Salida controlada** - especifica la salida que conmuta la cerradura eléctrica de la puerta.
  - **Modo** - Monoestable / Biestable.
  - **Tiempo de conexión**— configura el tiempo de activación del interruptor en el modo monoestable. El valor aquí definido no se aplica al modo biestable.
  - **Tipo de salida** - en el modo "Seguridad", la salida funciona en modo invertido, lo que significa que está permanentemente conectada y controla el relé de seguridad mediante una secuencia de impulsos específica. Si utiliza una cerradura de puerta inversa (es decir, la cerradura se bloquea cuando se aplica corriente), ajuste el tipo de salida a "Inversa".



#### SUGERENCIA

Si utiliza un relé de seguridad, ajuste el tipo de salida a "Seguridad".

Si se conectan a una salida varios interruptores con un tipo de salida ajustado de forma diferente, se controlarán de acuerdo con la siguiente prioridad:

1. Security
  2. Invertido
  3. Normal
5. En las pestañas **Activación** y **Códigos de activación**, puede establecer formas adicionales de activar el interruptor. Si no establece ningún otro método, el interruptor sólo se activará permitiendo el acceso del usuario.
  6. Guarde los cambios.

### Módulos

La página **Access > Modules** proporciona una gestión centralizada de todas las tecnologías de hardware de acceso del dispositivo. Cada módulo tiene su propia pestaña en la página que permite su gestión. Aquí se gestionan tanto los módulos integrados directamente en la unidad principal del aparato como los conectados a través de VBUS.

A cada módulo se le puede asignar un nombre y un interruptor específico para controlarlo. Otros parámetros dependen del tipo de módulo.

En los ajustes de fábrica, todos los módulos controlan el interruptor de la puerta.

## Ajustes de pantalla

### Para cargar su propio idioma de visualización

La interfaz de configuración basada en web le permite personalizar los textos en otros idiomas que aparecen en la pantalla del aparato. De este modo, podrá adaptar el dispositivo a un entorno lingüístico diferente o mostrar mensajes personalizados.

1. En la interfaz de configuración web, vaya a **Customization > Display**.
2. En la pestaña **Idioma** descargue la plantilla del archivo de traducción. La plantilla contiene textos en inglés por defecto.

3. Abra el archivo descargado en un editor de texto.
4. Sustituya las expresiones inglesas del archivo por sus propios textos.



#### ATENCIÓN

No cambie la estructura ni el formato de las frases clave. Si se modifica la sintaxis o faltan algunos elementos, es posible que el archivo de traducción no se cargue correctamente.

5. Guarde el archivo modificado en el formato `.ini`.
6. Vuelva a la pestaña **Idioma** de la interfaz web y seleccione "Personalizado" en el menú desplegable de idiomas.
7. Aparecerá la opción de carga de archivos - seleccione y cargue su archivo `.ini` modificado.
8. Guarde los cambios después de cargarlos correctamente.

## Presentación



#### NOTA

En la pantalla **2N IP Style** se pueden configurar otros modos de demostración además de la presentación (consulte [Modo Demo \(2N IP Style\)](#) (p. 26)).

Presentación es un modo de demostración que muestra una secuencia de imágenes y vídeos en la pantalla. Puede ajustar el tiempo de visualización de cada elemento (imagen o vídeo).

1. Vaya a **Personalización > Mostrar**.
2. Active la función en la cabecera de la pestaña **Presentación**.
3. Establezca cuánto tiempo desea que la pantalla de inicio pase al modo de vista previa.
4. Para cada elemento, puede especificar si desea mostrarlo sólo en una ventana de tiempo específica o fuera de ella. Para ver por ventana de tiempo, pulse en **Editar presentación**. Amplíe el menú avanzado haciendo clic en para un elemento específico para establecer cuándo debe mostrarse el elemento en la presentación.
5. Guarde los cambios.

## Modo Demo (2N IP Style)

El modo de demostración en **2N IP Style** es el estado de visualización al que pasa el aparato tras un cierto periodo de inactividad en la pantalla de inicio. La pantalla del dispositivo puede mostrar, por ejemplo, una serie de imágenes o vídeos, la dirección de un edificio o la fecha y la hora.



#### NOTA


Tras 2 minutos de inactividad se activa en el dispositivo 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.

## Ajustes del modo de vista previa

1. Vaya a **Personalización > Mostrar**.
2. En la cabecera de la pestaña , **active la función de modo de vista previa de**.
3. Establezca cuánto tiempo desea que la pantalla de inicio pase al modo de vista previa.
4. Seleccione el tipo de modo de muestreo seleccionado.
5. Puede activar la visualización de pictogramas informativos sobre la superficie antibacteriana o el icono táctil en la sección **Visualización de iconos de**.
6. Guarde los cambios.

## Presentación

Presentación es un modo de demostración que muestra una secuencia de imágenes y vídeos en la pantalla. Puede ajustar el tiempo de visualización de cada elemento (imagen o vídeo).

Para cada elemento, puede especificar si desea mostrarlo sólo en una ventana de tiempo específica o fuera de ella. Para ver por ventana de tiempo, pulse en **Editar presentación** . Amplíe el menú avanzado haciendo clic en  para un elemento específico para establecer cuándo debe mostrarse el elemento en la presentación.

## Logotipo

**Modo logotipo** se utiliza para mostrar un logotipo estático de la empresa en la pantalla.

Puede cargar una imagen de fondo para la pantalla (detrás del logotipo) en la pestaña **Imagen de fondo**.

## Texto

El modo de texto muestra un texto estático en la pantalla, que puede ser, por ejemplo, la dirección de la instalación, un mensaje de bienvenida u otra información para las personas que se desplacen por la instalación.

## Fecha y hora

Modo **Fecha y hora** muestra la fecha, la hora actual del aparato y la ubicación del mismo.

## Informes informativos (2N IP Style)

El dispositivo **2N IP Style** puede en su pantalla mostrar mensajes informativos que se pueden preconfigurar. A los usuarios o visitantes se les puede mostrar un mensaje tras concedérseles el acceso que les guíe por el edificio, les informe de los acontecimientos que tengan lugar en él, etc.

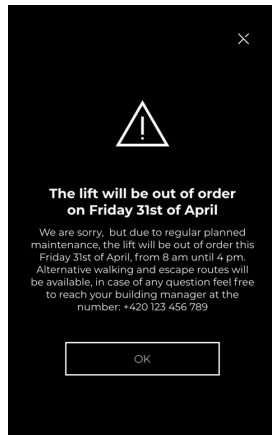
En cada pestaña, puede establecer mensajes de información específicos para cada uno de los siguientes eventos:

- **Usuario autorizado** - Este mensaje aparece en la pantalla después de que un usuario almacenado en el directorio del dispositivo se autentique en el mismo.
- **Visitante** – este mensaje aparecerá cuando se le posibilite al visitante el acceso durante la llamada. El visitante es una persona que en el dispositivo inició una llamada a un usuario del directorio. El mensaje aparece cuando este usuario concede acceso al visitante durante la llamada.
- **Acceso denegado** – este mensaje aparece cuando el dispositivo rechaza el acceso.

## Ajustes del mensaje de información

1. Vaya a **Acceso > Boletines**.
2. En las pestañas de la página, seleccione el tipo de mensaje informativo que desea configurar.
3. Habilite el mensaje de información en la cabecera de la pestaña.
4. En la pestaña **Programación y ajustes de la hora**, establezca la hora a la que debe mostrarse el mensaje de la hora y también el tiempo que debe permanecer el mensaje informativo en la pantalla. También puede especificar el periodo del calendario durante el cual debe mostrarse el mensaje.

5. En la pestaña **Contenido del mensaje de**, cree un mensaje. Puede crear un mensaje de texto o insertar una imagen.
6. Guarde los cambios.



Ejemplo de mensaje informativo con imagen y texto

# Ajustes avanzados


## Ajustes de cámara y vídeo

La cámara de los intercomunicadores 2N transmite la imagen a la otra parte durante una videollamada, detecta el movimiento en los alrededores y lee los códigos QR,

Es posible conectar cámaras externas al aparato, desde las que se podrá visualizar la imagen. Durante una llamada, podrá ver la vista desde otra cámara además del vídeo del dispositivo llamado.

Es posible conectar cámaras externas al dispositivo, desde las que se podrá leer la imagen.

## Ajustes internos de la cámara

1. Vaya a **Personalización > Cámara**.
2. En la pestaña **Cámara interna** haga clic en .
3. La pestaña **Ajustes** le permite editar los parámetros básicos de la imagen de la cámara.
4. Tras guardar, los cambios se reflejarán en la vista previa de la cámara.

## Modo

El modo cámara le permite ajustar la combinación óptima de modo de exposición y frecuencia de alimentación para conseguir imágenes estables y de alta calidad. Este modo se utiliza para reducir los parpadeos no deseados que pueden producirse cuando se utiliza iluminación artificial o cuando varía la frecuencia de la red eléctrica. Cuando se instalan cámaras en interiores, se puede seleccionar un método adecuado para suprimir el parpadeo causado por las fuentes de luz, mientras que cuando se colocan en exteriores, se puede activar un modo de supresión de la luz solar directa para garantizar una adaptación óptima de la imagen a las condiciones de iluminación del momento.

## IR LED

La función de retroiluminación IR LED se utiliza para garantizar una imagen de alta calidad incluso en condiciones de poca luz ambiental. Este modo se activa cuando las condiciones de luz caen por debajo del nivel establecido. El nivel límite de las condiciones de luz se establece sólo después de activar la iluminación LED IR.



### NOTA

Si el consumo de energía permitido pudiera excederse -por ejemplo, cuando varios módulos de expansión alimentados por PoE funcionan simultáneamente- el nivel de potencia IR se optimiza automáticamente para mantener la estabilidad del dispositivo.

## Configuración avanzada

**Modo día/noche** - le permite alternar entre imágenes en color y en blanco y negro en función de las condiciones de iluminación. Configure **Siempre de día**, si desea que la cámara utilice un filtro de supresión de infrarrojos y que la retroiluminación IR esté apagada. El ajuste "Siempre de noche", por el contrario, apaga el filtro y enciende la iluminación IR, lo que cambia la imagen al modo blanco y negro, adecuado para la visión nocturna. El modo automático cambia la cámara entre estos dos estados en función del nivel de luz ambiental.

**Contraste local** - realiza los detalles y las texturas aumentando las diferencias de brillo entre las zonas adyacentes de la imagen (bordes).

**Mapeado de tonos** - aumenta el brillo y la visibilidad de la imagen, pero puede causar una ligera distorsión del color.



**Tiempo máximo de exposición** - Especifica el tiempo máximo de exposición de la 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.

### Detección de movimiento

La detección de movimiento en los dispositivos 2N es una función que detecta automáticamente el movimiento en el campo de visión de la cámara interna y le permite desencadenar diversas acciones, como activar el Bluetooth o enviar una notificación.

Para un rendimiento óptimo, la detección puede calibrarse en función del entorno y las condiciones, por ejemplo modificando los parámetros de sensibilidad y la zona que debe vigilar la cámara.

### Configuración de la detección de movimiento

1. Vaya a **Personalización > Cámara**.
2. En la pestaña **Cámara interna** haga clic en .
3. En la pestaña **Vista previa de la cámara** haga clic en el icono del lápiz  situado junto al parámetro **Detección de movimiento**.
4. Se abre una ventana con los ajustes del perfil de detección de movimiento.
5. Despliegue la pestaña del perfil que desee configurar.
6. Ajustando el cuadrado en la vista previa de la cámara de un área específica en la que la cámara debe grabar el movimiento.



#### ATENCIÓN

El área de imagen es relativa al recorte de imagen actual. Si cambia el recorte de la imagen de la cámara, las zonas existentes seguirán siendo las mismas, pero cubrirán efectivamente una parte diferente del espacio. Por ello, se recomienda siempre comprobar y ajustar estas zonas después de editar un recorte.

7. Seleccione el modo de captura de movimiento para el perfil, véase [Modos de perfil \(p. 30\)](#)
8. Ajuste otros parámetros, si es necesario, según el modo.
9. ¡Recuerde siempre habilitar el perfil!
10. Para guardar sus cambios, pulse el botón **Guardar** o **Guardar y cerrar** en la parte superior de la página.

### Modos de perfil

#### Ejecución de sucesos

En este modo, la cámara capta movimientos instantáneos y únicos. El ejemplo del uso es la captura de una imagen cuando alguien entra en la habitación o cuando un vehículo pasa cerca del dispositivo.

La activación del evento disparado puede retrasarse utilizando el retardo establecido.

Utilice el filtro para definir los tipos de movimientos que desea que la cámara ignore, por ejemplo, objetos pequeños (pájaros pequeños) o movimientos repetitivos (árboles al viento).

#### Grabación

Este perfil activará un evento de 30 segundos cuando se detecte movimiento. Si se produce otro movimiento durante este tiempo, el perfil lo combinará todo en un solo evento. Este modo es adecuado para la vigilancia continua y evita la creación de un gran número de registros cortos.

Utilice el filtro para definir los tipos de movimientos que desea que la cámara ignore, por ejemplo, objetos pequeños (pájaros pequeños) o movimientos repetitivos (árboles al viento).

### Detección facial

El perfil detecta el movimiento cuando aparece un rostro en la zona vigilada. También puede producirse un suceso cuando una imagen estática de un rostro (por ejemplo, una fotografía) aparece en el encuadre.

### Detección de personas entrantes

El perfil sólo reconoce a las personas en movimiento e ignora las imágenes estáticas de rostros.

### Política de privacidad



La función de privacidad enmascara parte de la imagen para que no se vea ni se grabe en el vídeo. Esta opción es ideal para situaciones en las que desee proteger zonas sensibles de la imagen, por ejemplo. Por ejemplo, si el dispositivo se coloca en el mostrador de recepción y la cámara también capta el pasillo por el que se mueven los desconocidos, puede ocultar la zona del pasillo.



#### ATENCIÓN

La protección de la privacidad puede restringir la actividad de lectura de códigos QR o la detección de movimiento. Desaconsejamos utilizar la protección de la privacidad a la vez con las funciones mencionadas.

### Configuración de la detección de movimiento

1. Vaya a **Personalización > Cámara**.
2. En la pestaña **Cámara interna** haga clic en .
3. En la pestaña **Vista previa de la cámara** haga clic en el icono del lápiz  situado junto al parámetro **Privacidad**.
4. En la vista previa de la cámara, ajuste el cuadrado para cubrir el área que desea enmascarar.



#### ATENCIÓN

El área de imagen es relativa al recorte de imagen actual. Si cambia el recorte de la imagen de la cámara, las zonas existentes seguirán siendo las mismas, pero cubrirán efectivamente una parte diferente del espacio. Por ello, se recomienda siempre comprobar y ajustar estas zonas después de editar un recorte.

5. Seleccione el modo de ocultación:
  - **Color** - el área seleccionada se superpondrá con el color de su elección
  - **Mosaico** - el área seleccionada se pixelará. Fije el tamaño del mosaico en función del nivel de anonimización de datos que necesite.
6. No olvide activar la protección de la privacidad en la cabecera de configuración de los parámetros.
7. Para guardar sus cambios, pulse el botón **Guardar** o **Guardar y cerrar** en la parte superior de la página.

### Cámara externa

La cámara externa se añade al dispositivo 2N como flujo de vídeo (RTSP). La conexión de una cámara externa le permite cambiar de vista durante una llamada. La función de la cámara externa es, por tanto, puramente de imagen.

**ATENCIÓN**

Los códigos QR sólo pueden leerse en la cámara interna del dispositivo.

**Añadir una cámara externa:**

1. Vaya a **Personalización > Cámara**.
2. En la pestaña **Cámara externa** seleccione **Añadir cámara**.
3. En el cuadro de diálogo que se abre, active la cámara.
4. Introduzca la dirección de origen del flujo de la cámara IP externa en el formato `rtsp://dirección_ip_cámara/parámetros`.
5. Si el flujo de la cámara externa está sujeto a autenticación, rellene **con los datos de acceso al flujo**.
6. Guarde los cambios haciendo clic en **Añadir cámara**.
7. Si la cámara externa va a ser la cámara principal del dispositivo, después de guardarla en la pestaña **Cámara externa** haga clic en **Establecer como fuente predeterminada**.  
Cuando hable con el aparato, se mostrará primero la imagen de la cámara establecida como fuente por defecto.

**Crear un flujo de vídeo desde la cámara del dispositivo**

La función de transmisión de vídeo se utiliza para transmitir vídeo en directo desde la cámara del dispositivo a través de la red a un dispositivo receptor, como una aplicación móvil, un software de seguimiento o en un ordenador en un reproductor de vídeo. Este proceso garantiza que los usuarios puedan ver vídeo en tiempo real desde diversos dispositivos.

**Creación de un flujo de vídeo**

1. Vaya a **Integración > ONVIF / RTSP**.
2. Habilite el servicio del servidor RTSP.
3. Configure los parámetros del flujo, consulte [Parámetros del flujo de vídeo \(p. 32\)](#).
4. En la pestaña **Restricciones de conexión** puede rellenar las direcciones IP desde las que estará disponible el flujo. Si no se rellena ninguna dirección IP, es posible conectarse desde cualquier dirección IP.
5. En la pestaña **Flujos preconfigurados**, especifique si el flujo debe ser accesible:
  - anónimamente
  - con autenticación - establezca los detalles de autenticación en la pestaña **Autenticación**.
6. En la pestaña **Streams preconfigurados** encontrará las direcciones IP de los streams configurados según el códec de vídeo seleccionado.

**Parámetros del flujo de vídeo****Ajustes generales del flujo**

**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. Una memoria más larga significa una mayor resistencia a los cortes, pero más retardo de audio.

**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. Si este modo no está activado, los datos de transmisión de audio o vídeo se envían a través de RTP/RTSP únicamente.

**Puerto RTP inicial** – 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).

**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 %.

### Configuración de flujos de formato personalizado

1. En la pestaña **Streams del formato personalizado** haga clic en **Generar URL del stream**. Se abrirá un cuadro de diálogo.
2. En el cuadro de diálogo, establezca:
  - **Códec** - selecciona entre los códecs disponibles
  - **Activar audio** - especifica si se transmite sólo vídeo o vídeo con audio
  - **Resolución** - fija la resolución de la imagen
  - **Framerate** - fija la frecuencia de imagen del vídeo grabado
  - **Bitrate** - fija el bitrate
  - **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 %.
3. La dirección del flujo con los parámetros se carga automáticamente en la parte inferior del cuadro de diálogo.
4. Copie la dirección del flujo y guarde los cambios.

## Ajustes de sonido

### Ajuste del volumen del dispositivo

Para ajustar el volumen de su dispositivo, vaya a **Personalización > Audio**.

El volumen general determina el nivel de volumen básico de todos los demás sonidos del aparato. Ajuste este parámetro para reflejar el nivel de ruido del entorno en el que está instalado el aparato. Así, el ajuste de los otros sonidos es siempre relativo a este **volumen global**.

### Volumen adaptativo

En la pestaña **Volumen adaptativo** puede activar el ajuste automático del volumen en función del ruido ambiente. Esta característica es especialmente adecuada para instalaciones en entornos en los que el ruido ambiente es variable.

En la pestaña, ajuste **Umbral de sensibilidad**, a partir del cual el volumen del aparato empezará a aumentar. El aparato puede amplificarse hasta un valor ajustable **Amplificación máxima del sonido**.

### Transmisión de audio en las llamadas

Los parámetros de audio de la llamada se configuran directamente en la pestaña del servicio que proporciona la llamada ([Llamadas a través de SIP \(p. 13\)](#) o [Llamadas locales entre dispositivos 2N \(p. 14\)](#)), en la pestaña **Video**.

1. Abra la sección **Llamando a**.
2. Vaya a la página del servicio que proporciona la llamada (cuenta SIP específica, llamadas locales).
3. Abra la pestaña **Audio**.
4. En esta pestaña, ajuste los parámetros de sonido necesarios.

### Activación de la transmisión de señales DTMF

Mediante comandos DTMF enviados a este dispositivo, es posible activar su bloqueo y abrir así la puerta.

1. Abra la sección **Llamando a**.

2. Vaya a la página del servicio que proporciona la llamada (cuenta SIP específica, llamadas locales).
3. Abra la pestaña **Audio**.
4. En la pestaña **Envío DTMF**, seleccione **Modo de envío** para determinar durante qué llamadas se pueden enviar señales DTMF.
5. Seleccione los métodos de envío DTMF deseados.



### SUGERENCIA

Compruebe que ha habilitado los métodos aceptados por el dispositivo al que va a llamar.

6. En la pestaña **Recibir DTMF**, configure los métodos DTMF que recibirá el dispositivo.
7. Guarde los cambios.

## Sonidos de usuario

El aparato realiza varias acciones que van acompañadas de sonido (timbre, conmutación, etc.). Puede cambiar los sonidos reproducidos en **Personalización > Sonidos de usuario**.

También se pueden cargar en el dispositivo hasta 10 sonidos de usuario personalizados.

## Otras características de audio del dispositivo

### Multidifusión

El dispositivo es capaz de transmitir audio desde el micrófono mediante paquetes RTP enviados a una dirección multidifusión y, al mismo tiempo, recibir un flujo de audio en el mismo formato, que el dispositivo reproduce a continuación a través del altavoz integrado (u otra salida de audio configurada).

### Detección del ruido

El dispositivo puede supervisar el sonido recibido por el micrófono y, cuando el nivel de la señal del micrófono supera un umbral establecido, el dispositivo puede lanzar un evento `Event.NoiseDetected`. Este acontecimiento puede ir seguido de otros acontecimientos en la automatización (véase [Automatización \(p. 44\)](#)).

### Activación de la detección de ruido

1. Vaya a **Integración > Audio**.
2. En la cabecera de la pestaña **Detección de ruido**, active la función.
3. En el parámetro **Nivel de umbral de ruido**, especifique el valor [dB] que activa el evento **Event.NoiseDetected** cuando se supera.
4. En el parámetro **Retraso del inicio de la alarma** puede fijar la cantidad de tiempo que el ruido debe estar por encima de un nivel umbral para que se active el evento.
5. Por otro lado, en el parámetro **Retraso de fin de alarma**, puede especificar la cantidad de tiempo que la señal debe estar por debajo del umbral para que finalice el evento.

### prueba de audio

El resultado de la última prueba puede encontrarse en **Integración > Audio > pestaña General > pestaña Prueba de audio**.

Los dispositivos 2N pueden realizar una comprobación periódica del altavoz y el micrófono integrados. 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 de la última prueba puede visualizarse en la interfaz de configuración basada en web del aparato o procesarse mediante Automatización.

**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.

**Informacast**

Si su dispositivo es compatible con el protocolo InformaCast para la transmisión de audio, puede encontrar su configuración en **Integración > Audio > pestaña Informacast**. El protocolo InformaCast permite establecer un stream de audio (unicast/multicast RTP/UDP codificado por el códec G.711 U-law) entre el dispositivo 2N y el servidor de InformaCast (u otro cliente InformaCast).

Tras habilitar el servicio en **Integración > Audio > pestaña InformaCast**, los servidores InformaCast se encuentran automáticamente en la red local mediante el protocolo SLP y el dispositivo 2N se registra automáticamente con ellos.

**Perfiles de tiempo**

Algunas de las funciones que realiza el aparato dependen del tiempo. La sección **Perfiles de tiempo** de le permite preestablecer intervalos de tiempo entre los que podrá seleccionar estas funciones. Esto significa que no tendrá que introducir manualmente la hora cada vez que la ajuste. Puede asignar un nombre al perfil temporal para mayor claridad.

**Crear perfil de tiempo:**

1. Vaya a **Customization > Time Profiles**.
2. Pulse en vacío para crear un nuevo perfil.
3. Introduzca un nombre de perfil.
4. Haga clic en **Guardar**. Se abrirá el detalle del perfil.
5. Establezca los intervalos en los que debe estar activo el perfil temporal.
  1. Haga clic en el intervalo deseado.
  2. Puede especificar el inicio y el final en el menú abierto.

**NOTA**

La línea **Vacaciones** se utiliza para establecer diferentes intervalos de tiempo durante los días seleccionados, véase [Vacaciones \(p. 35\)](#).

6. Guarde los cambios.

**Vacaciones**

En la configuración del dispositivo, puede definir varios días que se marcarán como festivos. A continuación, se fijan intervalos especiales en los perfiles horarios para estos días. Normalmente se trata de días como los festivos, las vacaciones de empresa y otros días especiales.

Para cada festividad, especifique si sólo se aplica a un año concreto o si se repite el mismo día cada año. Las vacaciones pueden planificarse con varios años de antelación.

**Entornos de vacaciones:**

1. Vaya a **Customization > Time Profiles > Holidays tab**.
2. Seleccione el año para el que desea fijar las vacaciones.

3. Haga clic en el día en el calendario:
  - El primer clic marcará la festividad que se repetirá cada año en ese día y mes.
  - Un segundo clic cambiará las vacaciones a vacaciones únicas para el año seleccionado.
4. Guarde los cambios.

## Configuración avanzada de la cuenta SIP

Esta sección describe las funciones opcionales y los parámetros de la cuenta SIP que se configuran en la sección **Llamadas > SIP**.

La configuración avanzada de las cuentas SIP le permite aumentar la seguridad, optimizar la calidad de las llamadas y garantizar la compatibilidad con diferentes centralitas. Recomendamos que sólo los administradores experimentados cambien la configuración.

1. Vaya a **Llamadas > SIP** de la cuenta que desee configurar.

### Funciones SIP

El método REFER permite el reenvío dinámico de llamadas activas entre diferentes identidades SIP, lo que proporciona un control más flexible de los flujos de comunicación.

El método PRACK proporciona un acuse de recibo fiable de los estados de llamada continua entre dispositivos, lo que mejora la calidad y la estabilidad de la comunicación en los sistemas SIP.

### Medios de comunicación

**Recibir sólo llamadas encriptadas (SRTP)** - le permite recibir sólo llamadas encriptadas SRTP. Las llamadas no codificadas serán rechazadas automáticamente. 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.

**Control de calidad de vídeo adaptable** - Permite el uso de un perfil RTP ampliado para la retroalimentación RTCP (RTP/AVPF). Esta opción permite el uso del control interactivo de la calidad del vídeo según RFC-4585, y de esta manera la adaptación del flujo de datos del vídeo a la calidad actualmente disponible de la conexión de red.

**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.

Utilice MKI en paquetes SRTP – permite el uso de MKI (Identificador de clave maestra), que la contraparte requiere para identificar la clave maestra al rotar varias claves en paquetes SRTP.

No reproducir los early media entrantes – **prohíbe la reproducción del stream de audio entrante antes de aceptar la llamada que envían algunas centralitas u otros dispositivos. En lugar de ello se reproducirá el tono de timbre estándar.**

### Configuración avanzada

**Envío de paquetes KeepAlive** – establece si el dispositivo consultará el estado de la estación llamada a intervalos regulares durante la llamada usando solicitudes de OPCIONES SIP (utilizadas para detectar una interrupción de la estación durante una llamada).

**Rotación de registros SRV** – permite la rotación de los registros SRV para SIP proxy y registrar. 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.

**Filtro de 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 finalidad principal de la función es mejorar la seguridad de la comunicación y anular las llamadas telefónicas que no estén autorizadas.

**Evaluación del estado de las copias de seguridad más antiguas -**

**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.

# Sistema

## Ajustes de fecha y hora



### ATENCIÓN

Si el dispositivo está gestionado por una herramienta de gestión masiva (2N Access Commander / 2N My2N), la hora del dispositivo puede ser gestionada por esta herramienta. Los cambios manuales en la interfaz web del aparato no afectan al ajuste de la hora.

### Sincronización con NTP

Si el aparato está conectado a Internet, la hora y la fecha pueden sincronizarse mediante NTP.

1. Vaya a **Sistema > Fecha y Hora**.
2. En la pestaña de **Ajustes de sincronización horaria** active la opción **Hora automática desde NTP o Internet**.
3. Introduzca la dirección del servidor NTP de su elección.

### Actualización de la hora en caso de interrupción

1. Vaya a **Sistema > Fecha y Hora**.
2. En la pestaña de **Ajustes de sincronización horaria** pulse **Sincronización con el navegador**. Esto sincroniza la hora del dispositivo con la hora de su ordenador.



### NOTA

Los aparatos 2N están equipados con un reloj de reserva en tiempo real que le permite superar un corte de electricidad de hasta varios días.

## Configuración de la red

Por defecto, el dispositivo utiliza una dirección IP dinámica asignada por el servidor DHCP.

Una configuración adecuada de las direcciones IP es clave para garantizar que sus dispositivos estén conectados a su red de forma estable y fiable.

1. Para configurar los parámetros de red del aparato, vaya a **Sistema > Conexión de red**.

2. En Configuración básica > Configuración de la dirección IP, puede activar o desactivar el servidor DHCP.

### Configuración de una dirección IP estática:

- a. Desactive la opción del servidor DHCP .
- b. Introduzca la dirección IP deseada, la máscara de subred, la puerta de enlace predeterminada y los servidores DNS.
- c. Guarde los cambios. El dispositivo se está reiniciando.

### Configuración DHCP

- a. Habilite la opción **Servidor DHCP**.
- b. Introduzca la dirección IP deseada, la máscara de red, la puerta de enlace predeterminada y los servidores DNS.
- c. Guarde los cambios. El dispositivo se está reiniciando.



#### NOTA

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 dispositivo de manera que utilice la autenticación EAP-MD5 o EAP-TLS. Para configurar esta función sirve la solapa 802.1x.

## Licencia

Algunas funciones sólo están disponibles con la licencia correspondiente. Para obtener una visión general de las licencias y saber si están activas, consulte **Sistema > Licencias > pestaña Información general**. En la pestaña **Funciones con licencia** encontrará un resumen de las funciones disponibles sujetas a licencia.



#### NOTA

Tras seleccionar la licencia adecuada, póngase en contacto con su distribuidor 2N. Si es usted socio de 2N, puede ponerse en contacto con nuestro servicio de atención al cliente en [customercare@2n.com](mailto:customercare@2n.com). Por favor, incluya el número de serie del aparato en su solicitud.

## Actualización de la clave de licencia

La clave de licencia actual está disponible en el servidor de actualización. Si la interfaz de configuración web no tiene acceso a la Internet pública, puede cargar manualmente el archivo de claves en el dispositivo.

Cada vez que se reinicia el dispositivo, se recarga la última clave de licencia disponible.

## Licencia de prueba

La licencia de prueba le permite utilizar temporalmente todas las funciones de la licencia Gold y de la licencia Microsoft Teams durante un máximo de 800 horas tras la activación. Una licencia de prueba activada no puede suspenderse.

Para activar una licencia de prueba, vaya a **Sistema > Licencias > ficha Licencia de prueba**.

**ATENCIÓN**

Cada vez que se reinicia el aparato se elimina una hora de la licencia de prueba.

**Puertos utilizados**

Servicio	Puerto	Protocolo	Dirección	Habilitado por defecto	Ajustable	Ajustes
802.1x	–	–	In/Out	×	×	–
DHCP	68	UDP	In/Out	✓	×	–
DNS	53	TCP/UDP	In/Out	✓	×	–
Eco (descubrimiento de dispositivos)*	8002	UDP	In/Out	✓	×	–
FTP	21	TCP	Out	×	×	–
2N IP Eye	8003	UDP	Out	×	×	–
HTTP	80	TCP	In/Out	✓	✓	<b>Sistema &gt; Conexión a la red &gt; pestaña SERVIDOR WEB</b>
HTTPS	443	TCP	In/Out	✓	✓	<b>Sistema &gt; Conexión a la red &gt; pestaña SERVIDOR WEB</b>
Multicast audio	22222	UDP	Out	×	✓	<b>Integración &gt; Audio</b>

Sistema

Servicio	Puerto	Protocolo	Dirección	Habilitado por defecto	Ajustable	Ajustes
Audio multidifusión para protocolo ICU	8006	UDP	Out	x	x	–
Vídeo multidifusión para protocolo ICU	8008	UDP	Out	x	x	–
Vídeo multidifusión (ancho) para protocolo ICU	8016	UDP	In/Out	x	x	–
cliente NTP	123	UDP	In/Out	✓	x	–
ONVIF	80, 443, 3702	TCP/UDP	In/Out	x	x	–
Puertos RTP+RTCP (SIP)	4900+ (rango de 64 puertos)	UDP	In/Out	x	✓	<b>Llamada &gt; Ajustes generales</b>
Puertos RTP+RTCP (cámara externa)	4800+ (rango de 64 puertos)	UDP	In/Out	x	✓	<b>Integración &gt; ONVIF / RTSP</b>
cliente RTSP	554	UDP	In/Out	x	✓	
RTSP server	554	UDP	In/Out	x	x	–
SingleWire Commands	80	TCP	In/Out	x	x	–
SingleWire Communication	8081	TCP	Out	x	x	–
SingleWire Media	20000+	UDP	In	x	x	–

Sistema

Servicio	Puerto	Protocolo	Dirección	Habilitado por defecto	Ajustable	Ajustes
SLP	427	UDP	In/Out	✓	×	–
SIP	5060, 5062	TCP/UDP	In/Out	×	✓	Llamada > SIP
SIPS	5061	TCP	In/Out	×	✓	Llamada > SIP
SMTP	25	TCP	Out	×	✓	Integración > Notificaciones por correo electrónico
Syslog	514	UDP	Out	×	×	–
TFTP	69	UDP	Out	×	×	–
My2N Knocker	443	TCP	Out	✓	×	–
My2N Tribble Tunnel	443	TCP	Out	✓	×	–
SNMP Agent	161	UDP	In/Out	✓	×	–
SNMP Trap	162	UDP	Out	✓	×	–
SSDP	1900	UDP	In/Out	✓	×	–
SDDP	1902	UDP	In/Out	✓	×	–
Multicast receiver (Automation)	4433	UDP	In	×	×	–
WS-Discovery	3702	UDP	In/Out	✓	×	–

Sistema

Servicio	Puerto	Proto- colo	Direc- ción	Habi- litado por defec- to	Ajusta- ble	Ajustes
CIP Client (Crestron)	41794	UDP	In/Out	×	×	–
Canal del sitio (proto- colo UCI)	8004	UDP	In/Out	×	×	–
Multicast DNS	5353	UDP	In/Out	✓	×	–


# Automatización

**NOTA**

La función está disponible solo con la licencia Gold.

La configuración estándar del dispositivo 2N cubre la mayoría de los escenarios habituales. Para casos avanzados, como la necesidad de adaptar el dispositivo a requisitos específicos o integrarlo con sistemas de terceros, puede utilizarse la función de automatización. La automatización le permite definir una lógica personalizada para el comportamiento del dispositivo que responda a diferentes eventos, señales o combinaciones de condiciones. Por ejemplo, se pueden desencadenar acciones específicas pulsando un botón de marcación rápida concreto, activando una alarma silenciosa, detectando una puerta abierta, activando una entrada o detectando movimiento cerca del dispositivo.

## Ajustes de automatización:

1. En la interfaz web del aparato, vaya a **Integración > Automatización**.
2. En el resumen de funciones, habilite el número de funciones que desee.
3. Haga clic en  para abrir la interfaz de configuración de la automatización.
4. En la cabecera de la interfaz Automatizaciones, escriba el nombre de la función bajo la que se guardará la función.
5. Cree un flujo de automatización.  
Una descripción detallada de la función y configuración de Automatización está disponible en [Automatización manual](#).
6. Una vez finalizada la función, pulse **GUARDAR** y salga de la interfaz de automatización.



Intercomunicadores IP – Manual de configuración

© 2N Telekomunikace a. s., 2026

**2N.com**