

2N LiftIP 2.0

Manual de usuario



Tabla de contenidos

Presentación de producto	5
Variantes de producto	5
Propiedades básicas	6
Ventajas de uso	6
Variantes de producto	6
Accesorios	8
Descripción e instalación	9
Funcionamiento del equipo	9
Diseño universal	9
Ejecución de la COP	10
Ejecución de la COT	11
Antes de comenzar la instalación	12
Condiciones de instalación 2N LiftIP 2.0	12
Diseño universal	13
Instalación mecánica	13
Condiciones de instalación	13
Ubicación 2N LiftIP 2.0	13
Instalación del panel electrónico 2N LiftIP 2.0	14
Plano de instalación de la versión con altavoz de 50 mm	14
Instalación de la variante del COT 2N LiftIP 2.0	15
Montaje del micrófono fuera del panel	15
Instalación del altavoz fuera del panel	15
Consejos para conseguir unas propiedades acústicas ideales	16
Instalación de elementos indicadores	17
Conexión	17
Conexión del 2N LiftIP 2.0 a la red	17
Conexión del botón ALARM1/2 - control por contacto	18
Conexión del botón ALARM1/2 - control de tensión	19
Cableado de los elementos indicadores	20
Conexión de entrada CANCELAR (contacto de puerta, opcional)	22
Conexión del bucle de inducción	23
Descripción de terminales, puentes, conectores y LEDs	24
Funciones de botones	30
Control de volumen	30
Ajustes por defecto de las entradas ALARM1/2	30
Reinicia el dispositivo	30
dirección IP, cambiándola y restableciendo el aparato a los valores de fábrica	30
Obtención de la dirección IP actual	30
Configuración de la dirección IP estática del dispositivo	31
Configuración de la dirección IP dinámica del dispositivo	32
Restauración de la configuración original	33
2N Lift Voice Alarm Station	34
Instalación 2N Voice Alarm Station	35
Configuración	40
Manejo	40
Dimensiones 2N Voice Alarm Station	40
2N LiftIP 2.0 Relay extender	40
Conexión 2N Extensor de relé LiftIP 2.0	41
Parámetros técnicos 2N Extensor de relé LiftIP 2.0	42
Encontrar la dirección IP usando 2N IP Utility	43
Interfaz de configuración web	45
Orientación básica	45
Menú	45

Leyenda	46
Acceso a la interfaz de configuración web	46
Inicie sesión en la interfaz de configuración web	46
Navegadores recomendados	47
Estado	47
Elevar	47
Dispositivo	48
Servicios	48
Registros de llamadas	48
Eventos	48
Directorio	49
Usuarios	50
Llamar	51
Configuración general	51
llamadas locales	51
SIP	52
llamada de alarma	57
llamada de control	58
llamada operativa	58
Servicios	59
Elevar	59
Correo electrónico	60
Automatización	60
API HTTP	61
Integración	62
Sonidos de usuario	63
Servidor web	64
prueba de audio	65
SNMP	65
Hardware	66
Audio	66
Entradas digitales	66
cámara externa	67
Sistema	67
Cosér	67
Fecha y hora	68
Función	69
Certificados	70
Actualizar	71
Diagnóstico	72
Mantenimiento	74
Puertos utilizados	76
Funciones y uso	77
Descripción de la función	77
Llamada saliente	77
llamada de control	77
llamada operativa	78
Llamada entrante	78
Protección contra el arranque innecesario	78
Finalizar llamada (llamada saliente y entrante)	78
Instrucciones de envío	78
Control de marcación por tonos durante una llamada (DTMF)	78
Resumen de los informes de 2N LiftIP 2.0	79
Identificación 2N LiftIP 2.0	79
Tipo de confirmación de llamada	79
Confirme pulsando 1	79

Evaluar situaciones durante la elección con confirmación	80
Confirmación por recogida	80
CPC (Antena y KONE)	80
P100	81
Autodetección del protocolo DTMF (CPC/P100)	81
CPC (Antena), P100 2N ext (sólo para llamadas de alarma)	81
Prueba auditiva de ortografía	81
Evento tras error de audio	81
Proceso de liberación y fin de la liberación	81
Activación del proceso de liberación	81
Finalización del proceso de liberación	81
Evento tras finalizar el proceso de liberación	82
Protocolos CPC y P100	82
CPC	82
P100	85
Pruebas funcionales conforme a la norma EN 81-28	86
6.2.2 Información de señalización de emergencia ALARMA (4.1.2)	87
6.2.3 Fin de la señalización de emergencia ALARMA (4.1.3)	87
6.2.4 Suministro eléctrico de emergencia (4.1.4)	87
6.2.5 Señales visuales y acústicas en la jaula del ascensor (4.1.5)	87
6.2.6 Comunicación (4.1.8), verificación de la señalización de emergencia ALARMA (4.1.6), identificación (4.1.7)	88
Accesibilidad y fiabilidad (4.2.1)	89
Parámetros técnicos	90

Presentacion de producto

Este capítulo presenta el producto. **2N LiftIP 2.0**, las posibilidades de su uso y los beneficios que se derivan de su uso.

Variantes de producto

Unidades básicas en diseño universal

Estas unidades están destinadas a ser colocadas detrás del panel del ascensor, el cual ya está preparado anteriormente para su instalación.



Número de referencia: 921640E

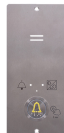
2N LiftIP 2.0 COP unit, EN



Número de referencia: 921640XE

2N LiftIP 2.0 COP unit, EN, Cable version

Incluye 2 LED (verde, amarillo), micrófono y altavoz conectados por cable.



Número de referencia: 921618BE

2N LiftIP 2.0 COP unit – Flush mounting, EN, With button

Las unidades con carcasa de acero inoxidable están diseñadas para su instalación en el panel del ascensor.



Número de referencia: 921618E

2N LiftIP 2.0 COP unit – Flush mounting, EN, Without button

Las unidades con carcasa de acero inoxidable están diseñadas para su instalación en el panel del ascensor.

Unidades básicas en el diseño del COT

■ **Número de referencia: 921630E**

2N LiftIP 2.0 TOC unit, EN

Las unidades con carcasa metálica están diseñadas para instalarse en la cabina del ascensor.

Unidades básicas en el diseño del COT

■ **Número de referencia: 921630E**

2N LiftIP 2.0 TOC unit long, EN

Juego básico con interruptor para conectar la estación de alarma por voz 2N en carcasa metálica

Incluye 2 LED (verde, amarillo), micrófono y altavoz conectados por cable.

Las unidades con carcasa metálica están diseñadas para instalarse en la cabina del ascensor.

Propiedades básicas

EI 2N LiftIP 2.0 es un comunicador de emergencia para ascensores que permite la transmisión de audio full-duplex mediante tecnología VoIP directamente desde la cabina del ascensor. Para la comunicación bidireccional se utilizan un micrófono y un altavoz incorporados detrás del panel (tablero) del ascensor.

EI 2N LiftIP 2.0 está diseñado para lugares en los que se disponga de una red LAN a la que se conecta a través de un conector RJ-45. **EI 2N LiftIP 2.0** puede alimentarse a través de una fuente de alimentación externa de 10-30 V CC / 0,5 A o directamente desde una red LAN equipada con elementos de red compatibles con la tecnología 802.3af PoE. Desde **2N LiftIP 2.0**, sólo se pueden realizar llamadas a números preprogramados. Gracias a la conectividad IP, **2N LiftIP 2.0** puede supervisarse constantemente, configurarse a distancia y hacer un seguimiento de su estado. La ventaja es la posibilidad de conectar un número casi ilimitado de unidades de comunicación.

Ventajas de uso

- reproduce un conjunto básico de mensajes
- Le permite grabar mensajes personalizados de hasta 8 minutos de duración (10 mensajes de usuario)
- propiedades acústicas óptimas
- Volumen del altavoz ajustable mediante los botones del altavoz (durante una llamada)
- configuración a través de la interfaz web del dispositivo
- Función "Comprobar llamada" una vez cada 3 días (puede modificarse)
- indicación de funcionamiento - dos luces indicadoras de acuerdo con la normativa vigente para ascensores
- rellamada automática de hasta cuatro números marcados
- protección contra el arranque no deseado o innecesario (CANCELAR)
- control de llamadas desde la sala de control
- no requiere una fuente de alimentación adicional cuando se utiliza PoE
- fácil instalación en cualquier tablero
- posibilidad de conectar potentes elementos indicadores - pictogramas iluminados (también con bombillas)
- DTMF utilizando RFC-2833, inband o SIP INFO

Variantes de producto

Unidades básicas en diseño universal

Estas unidades están destinadas a ser colocadas detrás del panel del ascensor, el cual ya está preparado anteriormente para su instalación.



Número de referencia: 921640E

2N LiftIP 2.0 COP unit, EN



Número de referencia: 921640XE

2N LiftIP 2.0 COP unit, EN, Cable version

Incluye 2 LED (verde, amarillo), micrófono y altavoz conectados por cable.



Número de referencia: 921618BE

2N LiftIP 2.0 COP unit – Flush mounting, EN, With button

Las unidades con carcasa de acero inoxidable están diseñadas para su instalación en el panel del ascensor.



Número de referencia: 921618E

2N LiftIP 2.0 COP unit – Flush mounting, EN, Without button

Las unidades con carcasa de acero inoxidable están diseñadas para su instalación en el panel del ascensor.

Unidades básicas en el diseño del COT

■ **Número de referencia: 921630E**

2N LiftIP 2.0 TOC unit, EN

Las unidades con carcasa metálica están diseñadas para instalarse en la cabina del ascensor.

Unidades básicas en el diseño del COT

■ **Número de referencia: 921630E**

2N LiftIP 2.0 TOC unit long, EN

Juego básico con interruptor para conectar la estación de alarma por voz 2N en carcasa metálica

Incluye 2 LED (verde, amarillo), micrófono y altavoz conectados por cable.

Las unidades con carcasa metálica están diseñadas para instalarse en la cabina del ascensor.

Accesorios

■ **Número de referencia: 921661E**

2N Voice Alarm Station – Switch

Interruptor para conectar sonidos con 2N LiftIP 2.0

🔊 **Número de referencia: 921001SET**

■ 2N Voice Alarm Station Set

El kit incluye 2 estaciones de alarma por voz 2N y 1 estación de alarma por voz 2N con interruptor

🔊 **Número de referencia: 921623E**

2N LiftIP 2.0 Relay extender

Extensor para 1 extensión de salida

Descripción e instalación

En este capítulo describimos el producto **2N LiftIP 2.0** y su instalación.

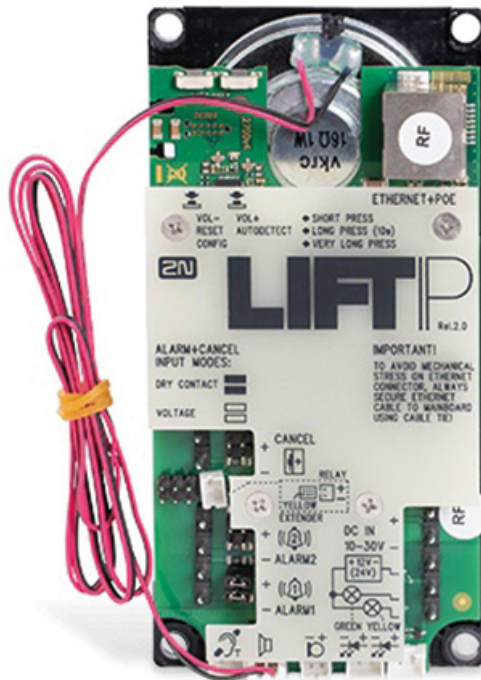
El 2N LiftIP 2.0 es un comunicador de emergencia para ascensores que permite la transmisión de audio full-duplex mediante tecnología VoIP directamente desde la cabina del ascensor. Para la comunicación bidireccional se utilizan un micrófono y un altavoz incorporados detrás del panel (tablero) del ascensor. Incluye terminales para la conexión de alimentación externa, botón de ALARMA, pictogramas luminosos (estados del aparato según la norma) y entrada de CANCELACIÓN (señal opcional de apertura de la puerta de la cabina).

Funcionamiento del equipo

Pulse el botón ALARMA. El pictograma **Espere** se encenderá inmediatamente, una vez establecida la comunicación se encenderá el pictograma **Conexión establecida**.

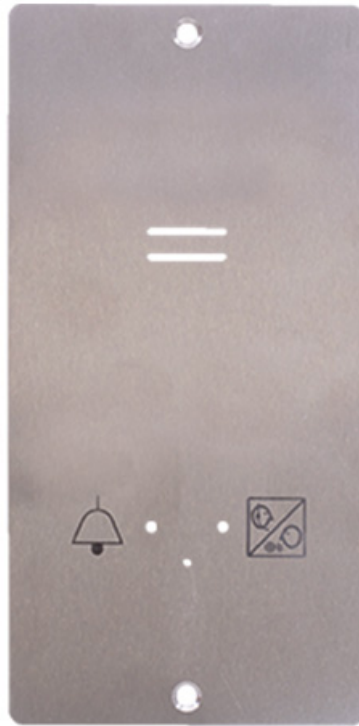
Diseño universal

La placa electrónica se coloca entre el panel de montaje y la cubierta impresa con las instrucciones (véase la figura). Las dimensiones totales son (An) 65 x (Al) 130 x (Pr) 24 mm. El altavoz, el micrófono y 2 LED (verde, amarillo) están conectados en la placa base (según el número de pedido). En el lado izquierdo, se conectan los puentes de cortocircuito (jumpers), que puede encontrar en el paquete del producto. Los pequeños conectores de la parte inferior se utilizan para conectar la bobina de inducción (para las personas con discapacidad auditiva) y los LED indicadores. Este producto suele llevar pictogramas luminosos (también son posibles los pictogramas incandescentes). Los pictogramas, así como el botón de ALARMA, no están incluidos (son elementos de diseño del ascensor).



Ejecución de la COP

La placa electrónica se encuentra bajo el panel de acero inoxidable con pictogramas (ver imagen). Las dimensiones totales son (An) 100 x (Al) 220 x (F) 26 mm. Altavoz, micrófono y LED incluidos. En el lado izquierdo, se conectan los puentes de cortocircuito (jumpers), que puede encontrar en el paquete del producto. Para la conexión de la bobina de inducción (para hipoacúsicos) hay un conector en la parte inferior.



Ejecución de la COT

La placa electrónica está alojada en una carcasa metálica (véase la figura). Las dimensiones totales son (An) 82 x (Al) 186 x (Pr) 33 mm para la versión básica y (An) 82 x (Al) 257 x (Pr) 33 mm para la versión larga con 2N Estación de alarma por voz. El altavoz y el micrófono están montados en el panel. El altavoz, el micrófono y 2 LED (verde, amarillo) están conectados en la placa base (según el número de pedido). En el lado izquierdo, se conectan las abrazaderas (slip-on), que puede encontrar en el paquete del producto. Los pequeños conectores de la parte inferior se utilizan para conectar la bobina de inducción (para las personas con discapacidad auditiva) y los LED indicadores. Este producto suele llevar pictogramas luminosos (también son posibles los pictogramas incandescentes). Los pictogramas, así como el botón de ALARMA, no están incluidos (son elementos de diseño del ascensor).



Antes de comenzar la instalación

Asegúrese, antes de iniciar la instalación, de que el paquete del producto esté completo.

Contenido del paquete

- **2N LiftIP 2.0**
- 4x abrazadera de conexión múltiple
- 6x puente de cortocircuito
- 1x altavoz y micrófono
- 2x cable con LED
- 3x pegatina
- 5x cinturón de cordón
- 1x Certificado de propiedad
- 1x guía rápida



NOTA

La cantidad y el tipo de accesorios pueden variar según el número de pedido.

Condiciones de instalación 2N LiftIP 2.0

- **2N LiftIP 2.0** no está diseñado para su uso en exteriores.

- El producto se conecta a la LAN.
- En caso necesario, la empresa instaladora deberá proporcionar protección contra daños mecánicos, agua, polvo y otras influencias adversas.
- La superficie para montar el comunicador debe ser plana, consulte el capítulo [Instalación mecánica \(p. 13\)](#) para más detalles.



ATENCIÓN

La instalación y el ajuste de este dispositivo, incluido cualquier manejo de este dispositivo, solo deben ser realizados por personas calificadas.



NOTA

2N LiftIP 2.0 recibe una dirección IP del servidor DHCP tras conectarse a la red.

Diseño universal

Compruebe que el panel de la grúa está listo para su instalación **2N LiftIP 2.0**.

Instalación mecánica



ATENCIÓN

La ubicación, el aspecto y el marcado de los mandos del comunicador (por ejemplo, el botón **ALARMA**) deberán cumplir las normas aplicables a los ascensores.

Condiciones de instalación

- El panel debe estar listo para su instalación, con al menos una perforación para el altavoz.
- El panel debe estar equipado con los elementos prescritos:
 - Botón de ALARMA;
 - Pictograma luminoso **Solicitud aceptada**;
 - pictograma luminoso **Conexión establecida**.
- La ubicación de todos estos elementos debe cumplir la normativa.
- Debe haber un espacio libre detrás del panel de min. (An) 65 x (Al) 130 x (Pr) 25 mm.

Ubicación 2N LiftIP 2.0

El **2N LiftIP 2.0** puede montarse en cualquier posición según sus necesidades. La posición óptima **2N LiftIP 2.0** es aproximadamente a la altura de la boca de un adulto. El **2N LiftIP 2.0** está diseñado para instalarse en lugares en los que esté excluido el contacto con el operario (consulte el aviso de seguridad).



ATENCIÓN

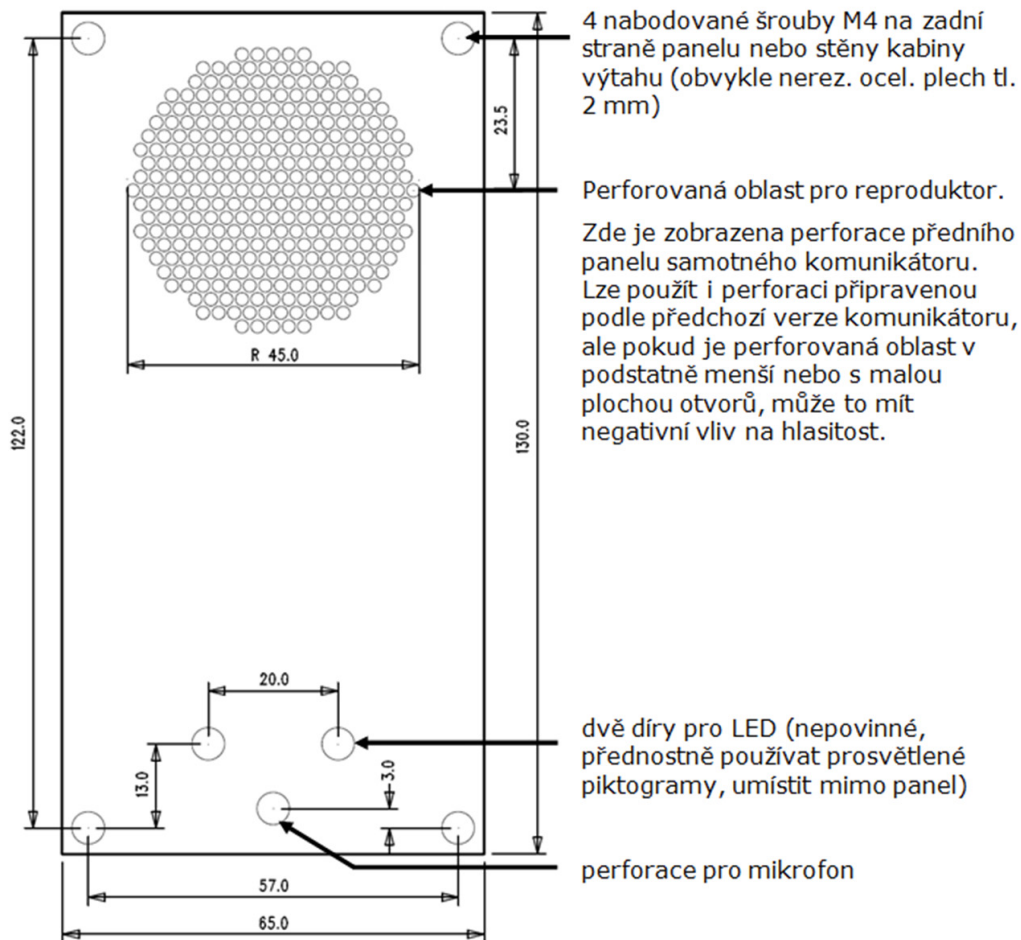
No se recomienda la instalación de componentes electrónicos sin un panel de montaje, en cuyo caso el fabricante no puede garantizar la seguridad. El panel sirve de aislamiento eléctrico.

Instalación del panel electrónico 2N LiftIP 2.0

Para montar el panel en el tablero del elevador se necesita lo siguiente:

- 4 tornillos M4 en el interior con un paso de (An) 57 x (Al) 122 mm
- Superficie perforada suficiente para el altavoz - puede ser mayor que en la imagen, pero **no debe superar las dimensiones del panel**, lo que crearía un cortocircuito acústico.
- orificio del micrófono
- posiblemente agujeros para 2 LED

Plano de instalación de la versión con altavoz de 50 mm



Cuando realice un montaje distinto al de los tornillos prescritos, asegúrese de que existe una distancia de aislamiento de al menos 2 mm entre los componentes electrónicos y los elementos de fijación no estándar. El panel de montaje debe montarse de forma que no resuene cuando el producto esté en funcionamiento. No debe haber ningún hueco entre la placa y el panel **2N LiftIP 2.0** o debe estar sellado para evitar el cortocircuito acústico del altavoz y el acoplamiento acústico entre el altavoz y el micrófono (véase más abajo).



ATENCIÓN

Asegúrese siempre de que la abertura del micrófono está sellada contra el entorno, es decir, que capta los sonidos de la cabina y no del hueco o de la cavidad que hay detrás del tablero.

Instalación de la variante del COT 2N LiftIP 2.0

La variante TOC es adecuada para su instalación en la cabina del ascensor. La carcasa metálica con el dispositivo se sujeta con tornillos idealmente más pequeños que el propio orificio, que tiene 0,8 mm de diámetro. Utilice tornillos de cabeza plana solos o tornillos de cabeza cónica en combinación con una arandela adecuada. Fije el aparato en el lugar de instalación seleccionado, marcando los orificios como puntos de colocación de los tornillos.



ATENCIÓN

- El uso de un tamaño de tornillo superior al recomendado puede dar lugar a una situación en la que el dispositivo no pueda retirarse fácilmente de los tornillos y sea necesario desenroscarlos.
- De lo contrario, si se utiliza un tamaño de tornillo demasiado pequeño, es posible que el dispositivo suspendido no se sujete firmemente.

Montaje del micrófono fuera del panel

Normalmente, el micrófono se coloca directamente en la placa de circuito impreso **2N LiftIP 2.0** (véase el dibujo anterior). En la versión con cable, el micrófono externo se monta en un soporte de 25 mm de diámetro con lámina autoadhesiva, y el micrófono se conecta mediante un cable estándar al conector correspondiente de la placa base. El adhesivo permite montar el micrófono detrás de cualquier orificio de la placa (el diámetro mínimo del orificio es de 3 mm o un grupo de orificios más pequeños con la misma superficie total). Las dimensiones detalladas del micrófono externo están disponibles en [este archivo](#). **La distancia mínima entre los centros del altavoz y del micrófono es de 90 mm.** A distancias menores, podría producirse un acoplamiento acústico. Más distancia no es algo malo.

Durante la operación del dispositivo el cambio del estado de la conexión del micrófono externo se mantiene sin cambio. El estado actual del micrófono externo se detecta solo a la hora de inicio/reinicio del dispositivo.

Instalación del altavoz fuera del panel

El altavoz se conecta mediante un cable estándar al conector correspondiente de la placa base. Las dimensiones detalladas del altavoz externo están disponibles en [este archivo](#). La longitud del cable permite su colocación opcional a una distancia de hasta 1 m de la placa base **2N LiftIP 2.0**. **En este caso, ¡preste atención a la seguridad eléctrica, véase más abajo!**



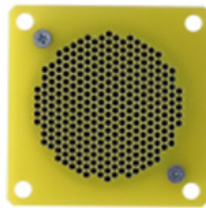
ATENCIÓN

Si la junta del altavoz se coloca por separado, asegúrese de que no se produce un cortocircuito acústico entre la parte delantera y la trasera del altavoz - ¡la rejilla nunca debe superar las dimensiones del altavoz, ya que provocaría un cortocircuito acústico!



PELIGRO

El altavoz de 50 mm sólo puede montarse sobre una superficie aislante (no metálica). En caso contrario, deberá solicitar un panel externo, véase la imagen inferior (no incluido).



ATENCIÓN

No recomendamos colocar el micrófono y el altavoz en lugares completamente distintos de la cabina, por ejemplo, el altavoz en el techo y el micrófono en la pared, ya que los usuarios deben localizar fácilmente la ubicación del altavoz (rejilla, perforación) y después buscar el micrófono por el que hablan en sus proximidades.



ATENCIÓN

Si se produce retroalimentación entre el micrófono y el altavoz (eco) al máximo volumen, le recomendamos que baje el volumen del altavoz.

Consejos para conseguir unas propiedades acústicas ideales

Para alcanzar la presión sonora mínima necesaria para cumplir los requisitos de la norma EN 81-28:2015, las aberturas del panel que cubre el altavoz del comunicador deben ocupar al menos el 20 % de la superficie del altavoz y estar situadas delante de éste.

El altavoz y el micrófono deben encajar perfectamente en el panel de la cubierta. Si esto no es posible debido a la irregularidad de la superficie del panel, le recomendamos que utilice una junta de altavoz

para evitar que el sonido del altavoz se filtre en el espacio situado detrás del panel. Un buen sellado del micrófono es importante para una transmisión del sonido de calidad y una buena inteligibilidad.

Al realizar el montaje, intente minimizar el acoplamiento acústico entre el micrófono y el altavoz.



ATENCIÓN

Si está probando el panel de control de la cabina fuera del ascensor (por ejemplo, sobre una mesa), el sonido puede parecer demasiado bajo. Esto se debe a la falta de una barra de sonido y a las propiedades acústicas del panel del ascensor. El volumen final corresponde sólo después de haber instalado correctamente el aparato.

Instalación de elementos indicadores

Existen tres opciones para la indicación del estado **2N LiftIP 2.0**:

1. Pictogramas luminosos que forman parte del panel de control de la cabina.
2. LEDs directamente en la electrónica **2N LiftIP 2.0**.
3. Dos LED (amarillo, verde) están conectados a la electrónica de la versión de cable **2N LiftIP 2.0**.



NOTA

El método de indicación debe elegirse para cumplir la legislación vigente. Para la función real **2N LiftIP 2.0** (comunicación), sin embargo, no es necesario conectar los elementos indicadores.

Conexión

Conexión del 2N LiftIP 2.0 a la red

El **2N LiftIP 2.0** se conecta a la red (LAN) mediante un cable UTP Cat-5e o superior terminado en un conector RJ-45 (conector LAN). El **2N LiftIP 2.0** puede alimentarse a través de PoE o de una fuente de alimentación externa (DC 10-30 V, 0,5 A). Cuando se conecta a la LAN, el **2N LiftIP 2.0** recibe una dirección IP del servidor DHCP.

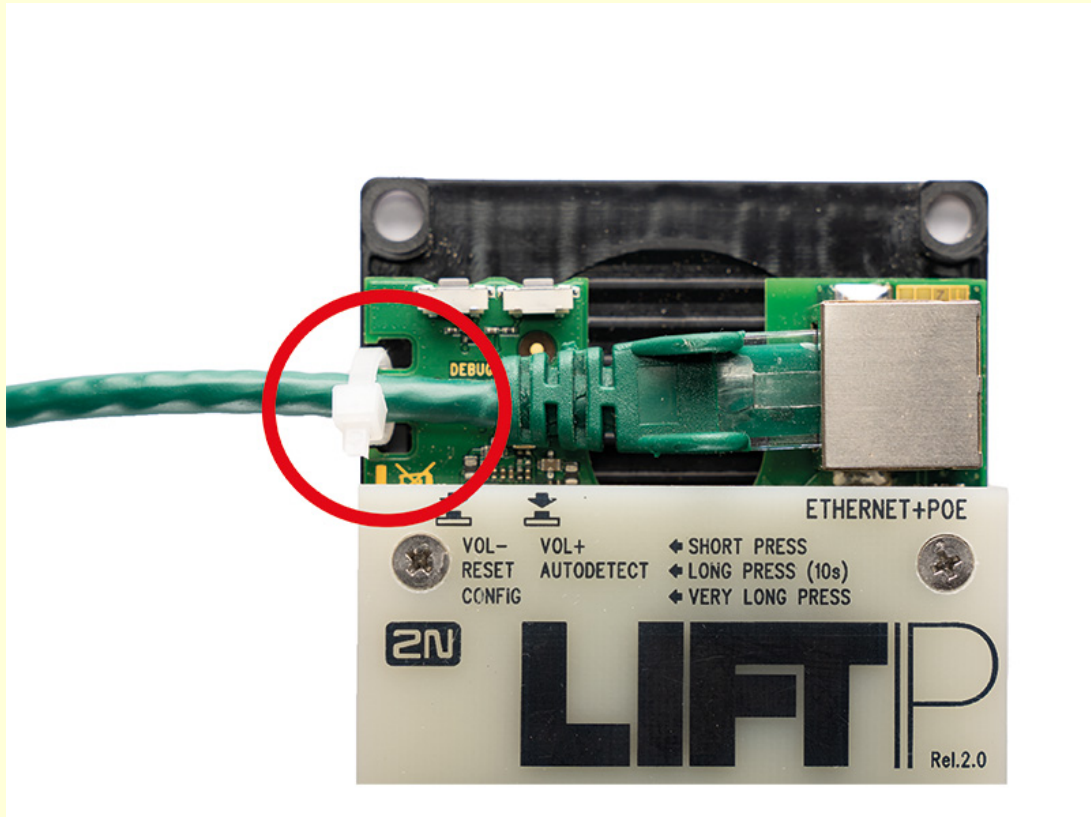
También puede averiguar la dirección IP utilizando la aplicación 2N Network Scanner, que incluye un escáner de red. Para obtener información más detallada, consulte [Encontrar la dirección IP usando 2N Network Scanner](#).

2N LiftIP 2.0 recibe DTMF por defecto utilizando RFC-2833 o el detector puede configurarse como en banda o SIP INFO.



ATENCIÓN

Para evitar tensiones mecánicas en el conector, fije el cable Ethernet a la placa base con una brida para cables.



Conexión del botón ALARM1/2 - control por contacto



PELIGRO

El pulsador debe ser seguro: los contactos del pulsador no deben estar conectados a ningún otro circuito. Si no se pueden cumplir estas condiciones, utilice el control de tensión.

1. Conecte los contactos de los botones al terminal ALARMA. La alarma viene ajustada de fábrica como alarma de conmutación (ambos puentes están ajustados).
2. El pulsador puede tener un contacto de conmutación y otro de apertura. En el caso de un contacto ampliable, la función del botón debe invertirse en la configuración web del aparato, consulte [Entradas digitales \(p. 66\)](#).

ALARM+CANCEL INPUT MODES:

DRY CONTACT

VOLTAGE

Conexión del botón ALARM1/2 - control de tensión



SUGERENCIA

Puede utilizarse una tensión continua del orden de 5-48 V. Sin embargo, esta fuente de alimentación debe estar respaldada contra fallos de alimentación.

1. La activación puede producirse conectando o desconectando esta tensión. La alarma viene ajustada de fábrica para la conmutación de contactos.
2. Para controlar la alarma mediante la conexión de la tensión retire todos los jumpers de la unión de configuración.

ALARM+CANCEL
INPUT MODES:

DRY CONTACT 

VOLTAGE 



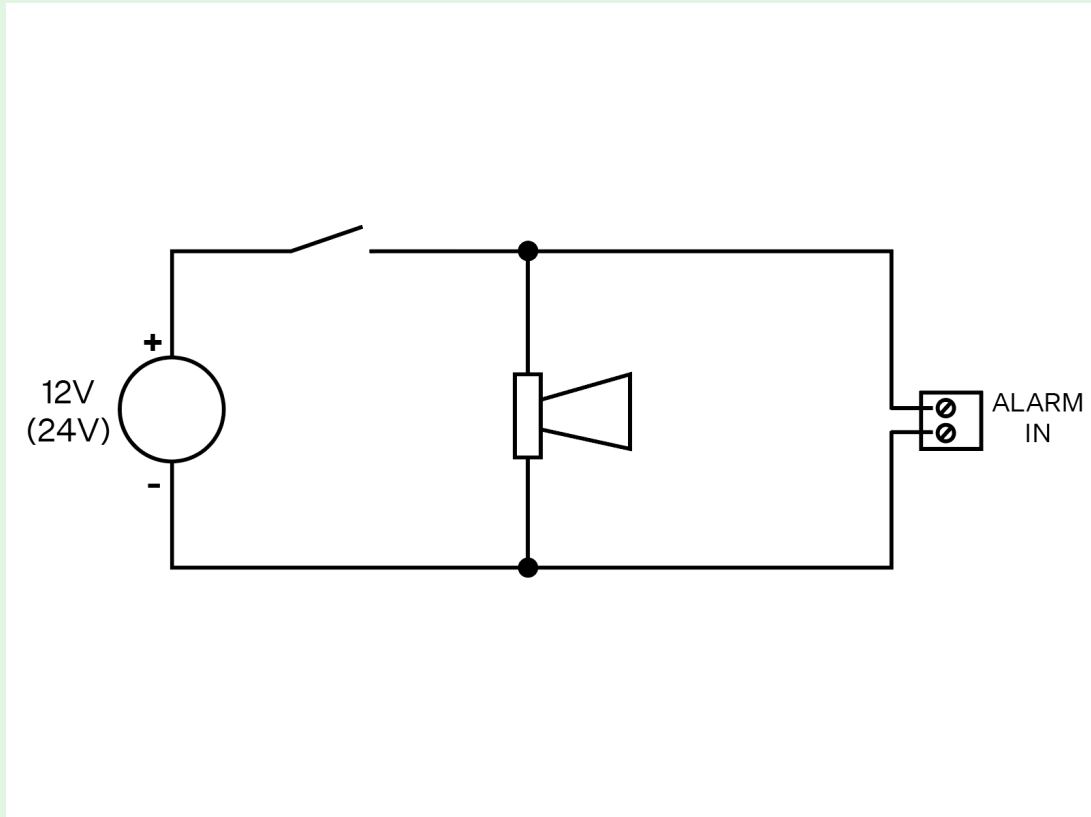
AVISO

Observe la polaridad (véase la impresión en la cubierta).



SUGERENCIA

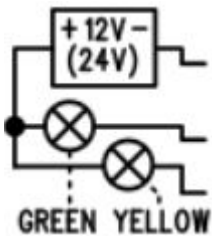
Aquí se muestra un ejemplo de conexión del botón de alarma con sirena:



Cableado de los elementos indicadores

Cableado básico

En este circuito puede utilizarse cualquier elemento de indicación (por ejemplo, pictogramas luminosos). Utilizando una fuente externa, se puede garantizar una luminosidad suficiente de los elementos indicadores. **2N LiftIP 2.0** sólo contiene interruptores, cualquier limitación de corriente, por ejemplo al utilizar LEDs, debe ser proporcionada por el circuito conectado.



Requisitos

- Fuente de alimentación de 12-24 V (de reserva para que la indicación funcione incluso en caso de corte del suministro eléctrico).



AVISO

Atención, ¡es necesario respetar la polaridad correcta de la fuente de alimentación!

- Corriente continua máx. 200 mA (se pueden conectar bombillas).
- ¡Ambos elementos indicadores deben estar conectados!

Utilización de LED montados directamente en la electrónica 2N LiftIP 2.0

En este caso, los LED se montan directamente en la electrónica y no es necesario ningún cableado adicional.

LEDs conectados por cable



NOTA

Si los LED de señalización están conectados por cable, la correcta colocación del elemento de señalización y la forma de los pictogramas utilizados son responsabilidad de la empresa que instala el dispositivo

Puede utilizarse cuando no se disponga de pictogramas luminosos. Estos LED forman parte de los accesorios de la versión con cable del aparato. Se trata de un LED de 5 mm de diámetro con una intensidad luminosa muy elevada.



Requisitos

- Observe la polaridad de los LED (véase la impresión en la cubierta).
- Observe los colores: confirmación de solicitud - amarillo, confirmación de conexión - verde.



NOTA

Cuando se utiliza este circuito, el LED de la placa de circuito impreso no se enciende.

Conexión de entrada CANCELAR (contacto de puerta, opcional)



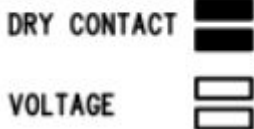
ATENCIÓN

El interruptor de la puerta o la señal de puerta abierta sólo indicará una puerta abierta si tanto la puerta interior como la exterior del ascensor están abiertas y se puede salir realmente de la cabina.

Control del interruptor

1. Conecte el interruptor al terminal CANCELAR.
2. De fábrica, **2N LiftIP 2.0** está configurado para la conmutación por contacto. Ambos puentes están montados en el puente de configuración.
3. CANCELAR también puede ajustarse en el contacto de apertura. En el caso de un contacto de expansión, la función de entrada CANCELAR debe invertirse en la configuración web del aparato, consulte [Entradas digitales \(p. 66\)](#).

**ALARM+CANCEL
INPUT MODES:**

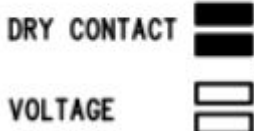


Control de tensión

Se puede utilizar una tensión continua en el rango de 5-48 V CC.

1. Para controlar la conexión de tensión, retire ambos puentes del puente de configuración.
2. Para controlar desenergizando, necesita invertir la función de entrada CANCELAR en la configuración web del aparato, véase [Entradas digitales \(p. 66\)](#).

**ALARM+CANCEL
INPUT MODES:**



ATENCIÓN

Si la presencia de tensión indica **una puerta** cerrada, esta fuente de alimentación debe estar respaldada contra un fallo eléctrico.



AVISO

Observe la polaridad (véase la impresión en la cubierta).

Conexión del bucle de inducción

A la hora de instalar un comunicador, es necesario atenerse a la normativa vigente, que puede estipular la instalación de un bucle auditivo como parte obligatoria del comunicador en la cabina del ascensor. El bucle se conecta al conector de la parte posterior de **2N LiftIP 2.0**. La polaridad es arbitraria. Previo acuerdo, se puede incluir un cable de 4 m.

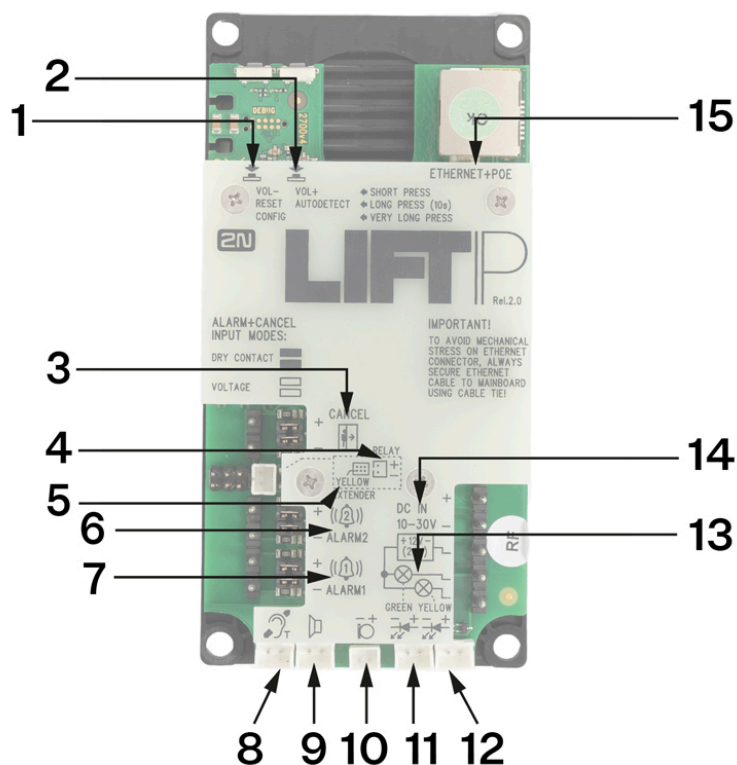


Requisitos

- Se recomienda colocar el bucle de inducción detrás de un elemento de cubierta no metálico ni magnético para evitar el deterioro de la radiación del campo del bucle de inducción.
- El bucle de inducción debe estar marcado con el pictograma apropiado (oreja) y su ubicación debe cumplir las normas aplicables.


Descripción de terminales, puentes, conectores y LEDs

Descripción de terminales y conectores



- | | | |
|-------|----------------------------------|---|
| 1 | Botón VOL-, RESET, CONFIG | <p>Pulsación corta (VOL-) - reduce el volumen del altavoz</p> <p>Pulsación larga (RESET) - después de aprox. 10 s el aparato se reiniciará</p> <p>Pulsación muy larga (CONFIG) - se utiliza para detectar la dirección IP del dispositivo, cambiar la dirección IP a modo estático o dinámico y restaurar el dispositivo a su configuración original de fábrica.</p> |
| <hr/> | | |
| 2 | Botón VOL+, AUTODETECT | <p>Pulsación corta (VOL+) - aumenta el volumen del altavoz</p> <p>Pulsación larga (AUTODETECT) - tras aprox. 10 s se ajusta la polaridad por defecto de las entradas ALARM1/2</p> |

Descripción de terminales y conectores

3	Svorka CAN-CEL	Controlado por contacto	Contacto de conmutación (por defecto)	El ajuste se realiza mediante las uniones de configuración (jumpers).	<p>ALARM+CANCEL INPUT MODES:</p> <p>DRY CONTACT </p> <p>VOLTAGE </p>
			Contacto del interruptor: ambos puentes están activados.		
			Contacto de apertura	Contacto dividido: ambos puentes están desplegados y la polaridad de entrada está invertida en la sección de configuración del software de Entradas digitales (p. 66) .	
		Controlado por tensión	Mediante la conexión de la tensión continua de 5-48 V	Controle conectando la tensión: no se despliega ningún puente de polaridad y la entrada se invierte en la sección de configuración del software, véase Entradas digitales (p. 66) .	
		Mediante la desconexión de la tensión continua de 5-48 V	Controle interrumpiendo la tensión: no se despliega ningún puente.		

Descripción de terminales y conectores

4	Conector RELÉ	Conector para conectar el relé extensor 2N LiftIP 2.0 .
5	EXTENDEDOR AMARILLO (conector de 6 patillas)	Se utiliza para conectar la estación de alarma por voz 2N.

Descripción de terminales y conectores

6/7 Abrazadera
ALARM1/2

Controlado por
contacto

Contacto de
conmutación
(por defecto)

El ajuste se realiza mediante las uniones de configuración (jumpers).

**ALARM+CANCEL
INPUT MODES:**

DRY CONTACT 

VOLTAGE 

Contacto del interruptor: ambos puentes están activados.

Contacto de
apertura

Contacto dividido: se colocan ambos puentes y se invierte la polaridad de entrada en la sección de configuración del software, consulte [Entradas digitales \(p. 66\)](#) Inversión de entrada.

Controlado por
tensión

Mediante la
conexión de la
tensión continua de 5-48 V

Controle **conectando la tensión:** no se despliega ningún puente y se invierte la polaridad de entrada en la sección de configuración del software, véase [Entradas digitales \(p. 66\)](#).

Mediante la
desconexión
de la tensión
continua de
5-48 V

Controle **interrumpiendo la tensión:** no se despliega ningún puente.

Descripción de terminales y conectores

8	Conector bucle de inducción	El bucle de inducción no se incluye de serie. Debe instalarse detrás de una cubierta no conductora y no magnética. La polaridad no importa.	
<i>Notas:</i>			
<ul style="list-style-type: none"> • <i>Si el altavoz se monta detrás de una carcasa no conductora ni magnética, puede desempeñar la función de una bobina de inducción hasta cierto punto.</i> • <i>La salida es a prueba de cortocircuitos. La potencia de salida está limitada por la resistencia.</i> 			
9	conector de altavoz	El altavoz se suministra enchufado a este conector.	
10	Conector de micrófono externo	Durante la operación del dispositivo el cambio del estado de la conexión del micrófono externo se mantiene sin cambio. El estado actual del micrófono externo se detecta solo a la hora de inicio/reinicio del dispositivo.	
11	Conector GREEN " Enlace de seguimiento "	LED verde	Los LED no se incluyen de serie (sólo en la versión con cable).
12	Conector YELLOW " Conexión establecida "	LED amarillo	La conexión de un LED externo no desactivará el LED de la placa.
13	Pinzas para conectar elementos indicadores + 12 V (24 V)	Elementos indicadores (pictogramas luminosos) CC 12-24 V / 2x 200 mA alimentados desde una fuente externa, es necesario observar el esquema eléctrico.	
14	Pinza DC IN 10-30 V	Fuente de alimentación externa (si no se alimenta a través de PoE)	DC 10–30 V
15	ETHERNET + POE	Conector RJ-45 (PoE según 800.3af) para la conexión en LAN	



AVISO

Observe la polaridad de los botones de ALARMA y CANCELACIÓN controlados por tensión (consulte la impresión de la cubierta).

LED (parte frontal - durante la llamada)

Color	Estado	Función	Descripción
Ámbar	se ilumina	Llamada de seguimiento	Indica la conexión de una llamada de alarma y también el modo de liberación en curso, si el modo está activado.
Verde	se ilumina	Conexión establecida	Señala el establecimiento de una llamada de alarma con la posibilidad de hablar con la otra parte. Se reconoce la llamada de alarma, se descuelga la llamada entrante.
Amarillo + Verde	Intermitencia alterna	Fallo en la llamada de control	Indica un fallo en la llamada de control. Si se inicia otra llamada, se señala, véanse los casos anteriores. Cuando finaliza la llamada, el estado de señalización vuelve a parpadear. La condición de error finaliza con el acuse de recibo de la llamada de alarma (sólo ALARM1) o con una posterior llamada de comprobación satisfactoria.
Sin señalización luminosa		Estado de reposo	Indica el estado de reposo del dispositivo.

Funciones de botones

Los botones situados en la parte superior izquierda de la placa de la unidad base se utilizan para configurar los parámetros básicos y controlar el aparato sin acceder a la interfaz web del mismo.

Control de volumen

Pulse brevemente el botón VOL-/VOL+ para bajar/aumentar un nivel el volumen de los altavoces. El ajuste más bajo/más alto del volumen general del aparato se confirma mediante una señal acústica.

Ajustes por defecto de las entradas ALARM1/2

Una pulsación prolongada del botón marcado con AUTODETECT durante 10 segundos detecta el tipo de control de entrada ALARM1/2. Los valores detectados se escribirán en la configuración del software. En el momento de la autodetección, el tipo de control de entrada se trata como un estado de reposo. El restablecimiento de los ajustes de entrada por defecto se indica mediante una señal acústica.

Reinicia el dispositivo

Una pulsación larga del botón marcado con RESET durante unos 10 segundos reiniciará el aparato sin ningún cambio en la configuración.



NOTA

El intervalo de tiempo desde una pulsación larga del botón RESET hasta la reconexión del dispositivo a la red después de un reinicio es de varias decenas de segundos.

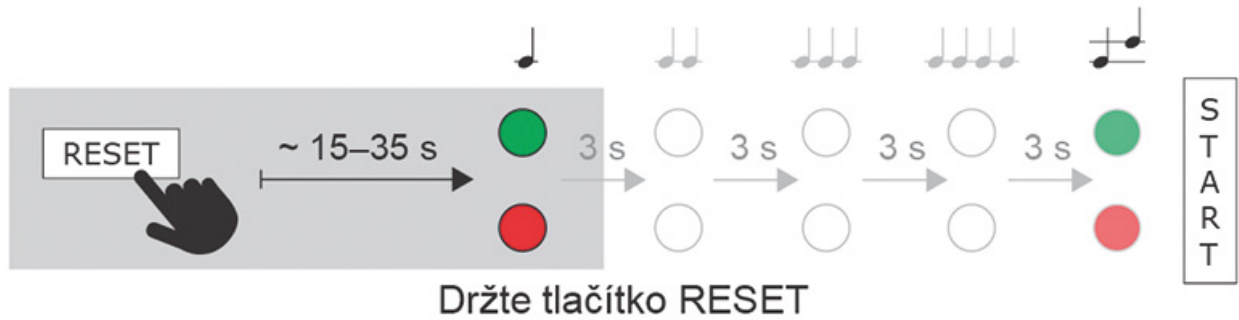
dirección IP, cambiándola y restableciendo el aparato a los valores de fábrica

El botón izquierdo denominado VOL-/RESET/CONFIG, situado en la parte superior izquierda de la unidad base, se utiliza para determinar la dirección IP del aparato, cambiarlo a modo estático o dinámico y restaurar los ajustes originales de fábrica del aparato,

Obtención de la dirección IP actual

Para **conocer la dirección IP actual**, proceda de la siguiente manera:

1. Mantenga presionado el botón RESET.
2. Espere hasta que los LED rojo y verde del dispositivo se enciendan simultáneamente y suene una señal acústica 📢 (aprox. 30 s).
3. Suelte el botón RESET.
4. El dispositivo anunciará automáticamente la dirección IP actual por voz.



NOTA

El intervalo de tiempo desde que pulsa el botón **RESET** hasta la primera señal luminosa y sonora es de aprox. 30 s.

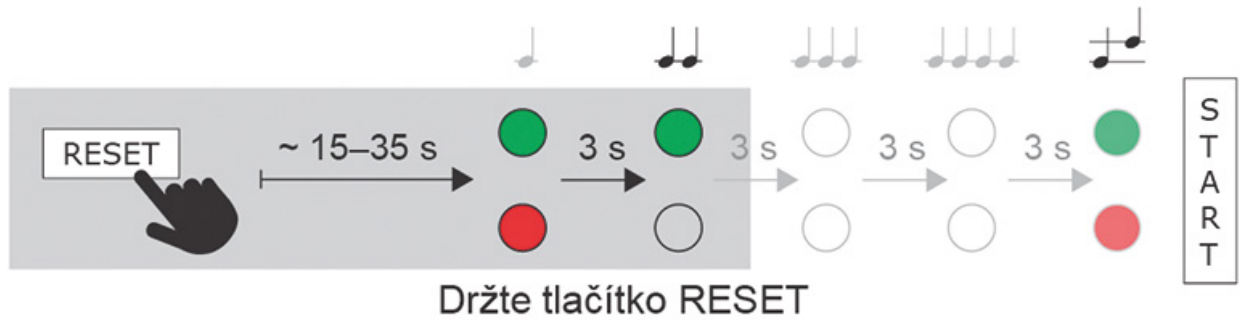
Configuración de la dirección IP estática del dispositivo

Para configurar la configuración de red del dispositivo al modo **con dirección IP estática** (DHCP OFF), proceda de la siguiente manera:

1. Mantenga presionado el botón RESET.
2. Espere hasta que los LED rojo y verde del dispositivo se enciendan simultáneamente y suene una señal acústica (aprox. 30 a 35 s).
3. Espere hasta que el LED rojo se apague y suene la señal sonora (aprox. otros 3 s).
4. Suelte el botón RESET.

Después de reiniciar, el dispositivo tendrá configurados los siguientes parámetros de red:

- Dirección IP: 192.168.1.100
- Máscara de red: 255.255.255.0
- Portal inicial: 192.168.1.1



Para configurar la configuración de red de un dispositivo con una **dirección IP dinámica** (DCHP ON), siga los puntos a continuación:

Configuración de la dirección IP dinámica del dispositivo

1. Pulse y mantenga pulsado el botón RESET.
2. Espere hasta que los LED rojo y verde del dispositivo se enciendan simultáneamente y suene una señal acústica (aprox. 30 a 35 s).
3. Espere hasta que el LED rojo se apague y suene la señal sonora. (aprox. otros 3 s).
4. Espere hasta que el LED verde se apague, el LED rojo se vuelva a encender y suene la señal sonora. (aprox. otros 3 s).
5. Suelte el botón RESET.



Restauración de la configuración original

Para restaurar la **configuración original de fábrica** del dispositivo siga el siguiente procedimiento:

1. Pulse y mantenga pulsado el botón RESET.
2. Espere hasta que los LEDs rojo y verde se enciendan simultáneamente y se oiga la señal acústica 🎵 (aprox. 30-35 s).
3. Espere hasta que el LED rojo se apague y suene la señal sonora 🎵 (aprox. otros 3 s).
4. Espere hasta que el LED verde se apague y el LED rojo se encienda de nuevo y se oiga la señal acústica 🎵 (aprox. otros 3 s).
5. Espere hasta que el LED rojo se apague y suene la señal sonora. (aprox. otros 3 s).
6. Suelte el botón RESET.



2N Lift Voice Alarm Station

2N Voice Alarm Station sirve para ampliar **2N LiftIP 2.0** por la unidad de sonido en el tejado de la cabina y debajo de la cabina. Está equipada con su propio micrófono, altavoz y botón de emergencia. Para la conexión sirve switch, el cual conecta **2N LiftIP 2.0** con una o dos unidades de sonido.



Instalace 2N Voice Alarm Station

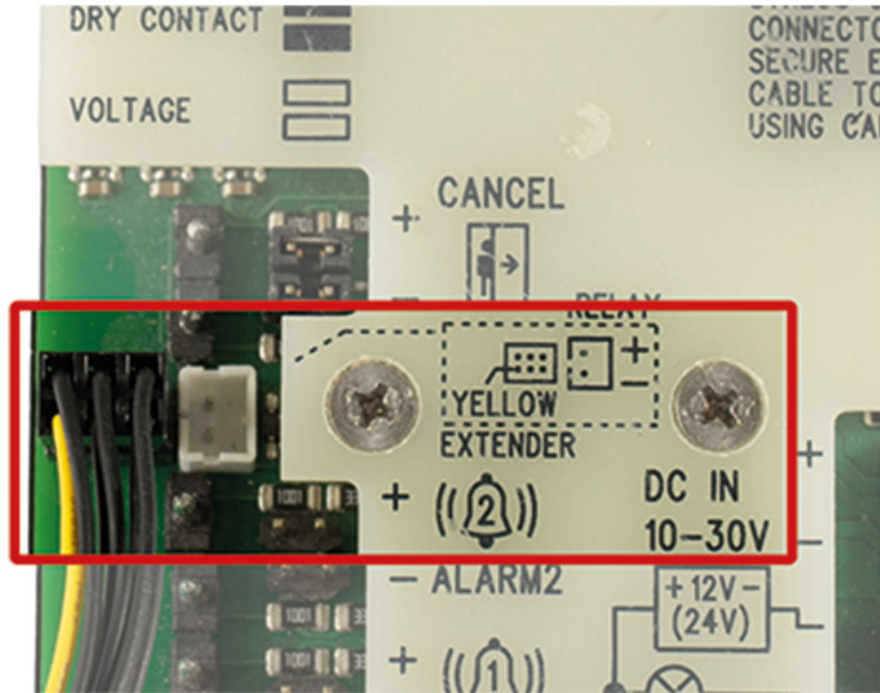
1. A la hora de conectar 2N Voice Alarm Station desconecte **2N LiftIP 2.0** de la alimentación.

2. Coloque el enchufe de 6 pines del cable de conexión del switch sobre el conector de 6 pines marcado como EXTENDER en 2N LiftIP 2.0. Respete la orientación correcta de la conexión del conductor amarillo.



AVISO

En el caso de una colocación incorrecta se pueden producir daños en el módulo.



3. Desconecte el reproductor y el micrófono de los conectores (micrófono externo, en el caso de que esté instalado) en 2N LiftIP 2.0.

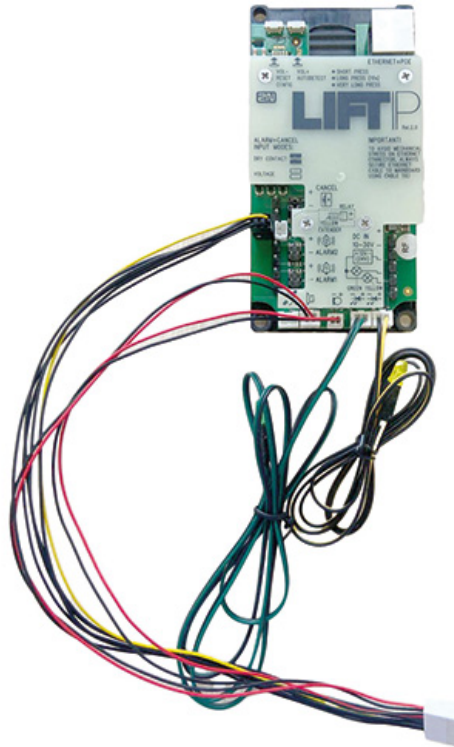


ATENCIÓN

Durante la operación del dispositivo el cambio del estado de la conexión/desconexión del micrófono externo se mantiene sin cambio. El estado actual del micrófono externo se detecta solo a la hora de inicio/reinicio del dispositivo.

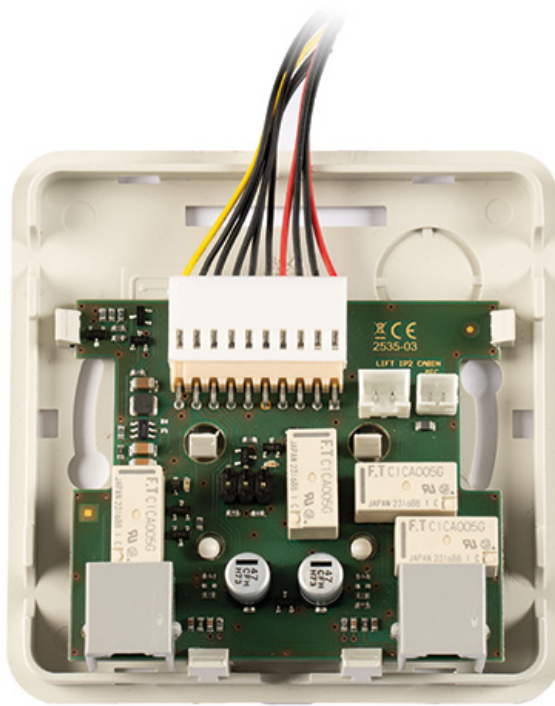
Descripción e instalación

4. En el conector del micrófono y del reproductor en **2N LifIP 2.0** conecte los conectores del cable de conexión del switch (los conectores para la conexión del micrófono y del reproductor tienen cada uno tamaño diferente y en la cubierta de **2N LifIP 2.0** hay pictogramas, así que no se pueden confundir).



Descripción e instalación

5. Retire la cubierta del switch. Al colocar el enchufe del cable de conexión en el conector de 10 pines del switch se produce la conexión del switch y de **2N LiftIP 2.0**.

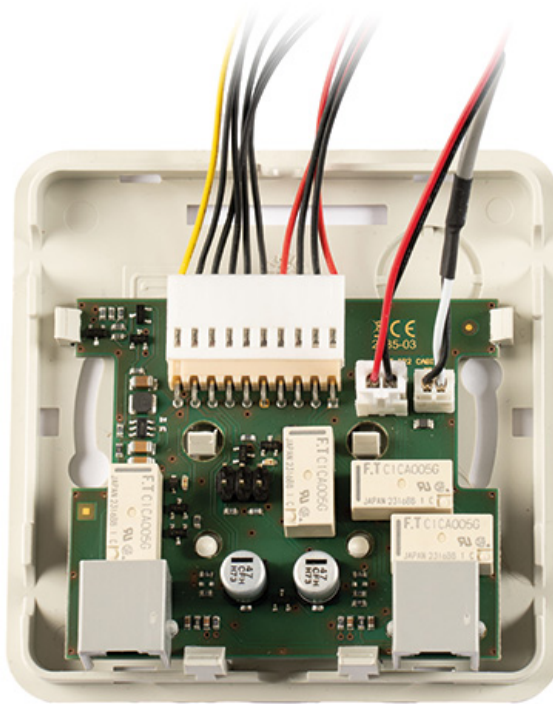


6. Conecte el micrófono con el reproductor, los cuales han sido inicialmente desconectados de **2N LiftIP 2.0**, en los conectores en el switch. Los conectores para la conexión están marcados, SPK para el reproductor y MIC para el micrófono.



AVISO

En el caso de que utilice la versión por cable de **2N LiftIP 2.0**, conecte el micrófono en el cable en el conector MIC en el switch, de lo contrario se queda este conector sin ser instalado.



7. En el canto superior de la cubierta del switch rompa el plástico para crear el agujero para pasar los cables. Según la forma de colocación de la instalación se pueden pasar los cables de forma alternativa por el agujero, el cual se puede crear rompiendo el plástico en la esquina superior derecha en la parte posterior de la cubierta del switch. Tras pasar los cables de forma elegida cierre el switch utilizando la cubierta superior. En la parte inferior del switch está en cada lado colocado un conector de tipo RJ-12 para conectar las unidades de sonido. Mediante el cable adjunto a la unidad de sonido conecte la unidad de sonido con el switch. El conector para la conexión se encuentra en el lado derecho de la unidad de sonido debajo de la cubierta abatible. Después de conectar el cable asegure el cierre de la cubierta abatible utilizando el tornillo adjunto.
8. Tras finalizar la instalación vuelva a conectar **2N LiftIP 2.0** de nuevo a la alimentación.



NOTA

El conector de 6 pines en el panel del switch sirve para las tareas avanzadas de diagnóstico del hardware para los fines de servicio, al usuario convencional no le proporciona ninguna función.

Configuración

El enrutamiento de llamadas desde la estación de alarma por voz 2N se establece en la interfaz de configuración web del dispositivo **2N LiftIP 2.0**, al que está conectada la estación de alarma por voz 2N. Los ajustes se realizan en el menú **Llamada > Llamada de alarma > Llamada de alarma 2**.

El resumen de sucesos de la llamada de alarma 2 se registra en el menú de configuración **Estado > Eventos**.



AVISO

En el caso de que no se rellene el destino para la Llamada de alarma 2, la llamada no se podrá crear. Es posible tener establecido el mismo usuario como en el botón ALARMA1.

Manejo

Para activarla, pulse brevemente **Pulse para llamar a** en la estación de alarma por voz 2N. La llamada está establecida al destino para la llamada de alarma ALARM2 desde **2N LiftIP 2.0**.



NOTA

La unidad de sonido 2N Voice Alarm Station no contiene LED para indicar el establecimiento de la conexión. A la hora de establecer la llamada, y tras la confirmación, la LED en la unidad de sonido de **2N LiftIP 2.0** está encendida.

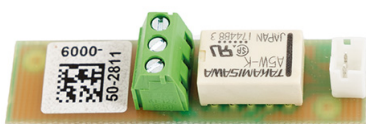
Dimensiones 2N Voice Alarm Station

Unidad de sonido – 2N Voice Alarm Station: 225 x 87 x 67 mm

Switch: 81 x 81 x 30 mm

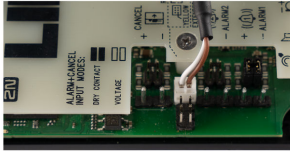
2N LiftIP 2.0 Relay extender

El extensor de relés 2N LiftIP 2.0 ampliará **2N LiftIP 2.0** en 1 salida. El tipo de la salida del relé permite activar ambas polaridades de tensión. La salida de bloqueo se desactiva/activa según el modo de conexión, en el caso de que no sea posible establecer la llamada de emergencia desde **2N LiftIP 2.0** (no está introducido el número en la configuración para el botón Alarma o no hay registro en el servidor SIP, a excepción del caso cuando esté configurado direct call (llamada P2P) para el botón Alarma).



Conexión 2N Extensor de relé LiftIP 2.0

El extensor de relés 2N LiftIP 2.0 se enchufa en el conector RELAY (consulte en [la descripción de los terminales, puentes, conectores y LEDs \(p. 24\)](#)).



1. Cuando conecte el 2N LiftIP 2.0 Relay extender, desconecte el **2N LiftIP 2.0** de la fuente de alimentación (DC 10-30 V o PoE).
2. Para proteger los circuitos de cortocircuitos con otros objetos conductores 2N LiftIP 2.0 Extensor de relé **introdúzcalo siempre en el tubo aislante incluido y fíjelo con las lengüetas antes de la instalación.**



3. Conecte el cable **2N LiftIP 2.0** y el extensor de relé 2N LiftIP 2.0.
- 4.



ATENCIÓN

Respete la conexión correcta en el conector (conductor amarillo). En el caso de una colocación incorrecta se pueden producir daños en el módulo.



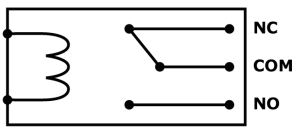
NOTA

El estado de la salida de relé en caso de error se señala del mismo modo que en caso de desconexión del aparato de la red eléctrica. La salida del relé está desenergizada.

Parámetros técnicos 2N Extensor de relé LiftIP 2.0

Salida	
Potencia máxima de conmutación	15 W
Tensión de conmutación máxima	30 V
Corriente de conmutación máxima	2 A
Tipo de salida	aislado galvánicamente, permite conmutar tensiones de ambas polaridades

Diagrama



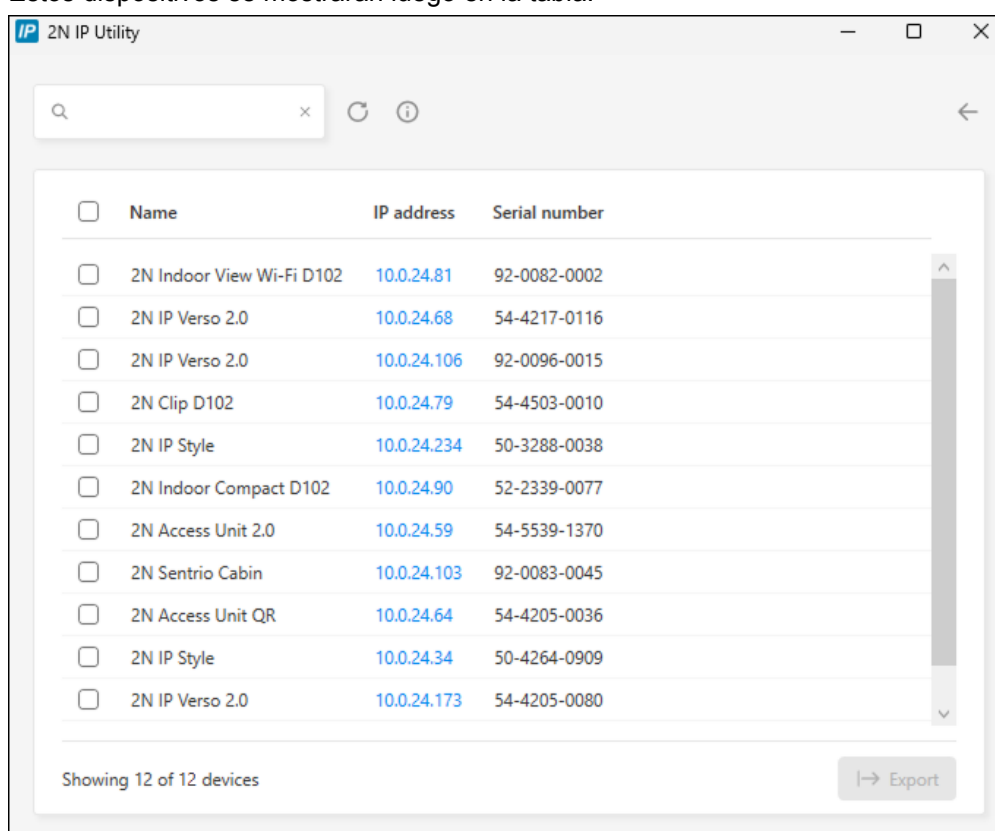
Ejemplo: Mediante los contactos COM y NA, el relé conecta el circuito tras aplicar tensión a la bobina.

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. 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.
3. 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.



The screenshot shows the 2N IP Utility application window. At the top, there is a search bar and navigation icons. Below is a table with columns for Name, IP address, and Serial number. The table lists 12 devices. At the bottom, it says 'Showing 12 of 12 devices' and has an 'Export' button.

<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

4. 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.).


Interfaz de configuración web

Orientación básica



La página de inicio mostrada es ilustrativa. La visualización de los mosaicos depende de la disponibilidad de funciones en el dispositivo específico.

La página de inicio se muestra después de iniciar sesión en la interfaz de configuración web **2N LiftIP 2.0**.

Es posible volver a él en cualquier momento utilizando el botón  ubicado en la esquina superior izquierda de otras páginas de la interfaz de configuración web. El nombre del dispositivo se muestra en el encabezado de la página (consulte el parámetro Nombre del dispositivo en **sección Servicios > Servidor web**).

Menú

Para seleccionar un idioma, puede utilizar el menú en la esquina superior derecha de la interfaz web. Puede cerrar sesión en el dispositivo usando el botón Cerrar sesión en la esquina superior derecha de la página, vea la ayuda usando el ícono del signo de interrogación o use la burbuja para brindar comentarios.

Leyenda

La página de inicio sirve como primer nivel de orientación y navegación rápida (haciendo clic en cualquier mosaico) hacia partes seleccionadas de la configuración. **2N LiftIP 2.0**.



Acceso a la interfaz de configuración web

2N LiftIP 2.0 se configura mediante la interfaz de configuración web. Para acceder es necesario conocer la dirección IP.

Inicie sesión en la interfaz de configuración web

1. Aparecerá la pantalla de inicio de sesión.
Si no aparece la pantalla de inicio de sesión, asegúrese de haber introducido la dirección IP correcta, el puerto correcto o el nombre de dominio correcto. La pantalla de inicio de sesión tampoco aparece si el servidor web de la interfaz está apagado. Si no tienes una dirección IP o nombre de dominio certificado generado, es posible que veas una alerta de certificado de seguridad no válido. En este caso, debe confirmar que desea ir a la interfaz de configuración web.
2. Ingrese su información de inicio de sesión.
Las credenciales predeterminadas son:
Nombre de usuario: **Admin**
Contraseña: **2n**
Después de iniciar sesión por primera vez, debes cambiar tu contraseña inmediatamente.
Después de iniciar sesión con la contraseña predeterminada, el acceso a las funciones de la interfaz de configuración web es limitado.



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.

Estado

La información actual y las propiedades del dispositivo se muestran claramente en la sección Estado.

Elevar

El menú Elevador muestra información sobre el modelo y sus propiedades y estados de error.

Estado del ascensor

Identificación del ascensor – establece el número de identificación del ascensor o del comunicador de ascensor, que se envía o lee en llamadas individuales. El número de identificación deberá constar de un máximo de 16 dígitos.

Última llamada de control exitosa – muestra la hora de la última llamada de control exitosa.

Próxima llamada de control – indica la hora de la próxima llamada de control regular.

Modo de recuperación – indica si el modo de recuperación está actualmente activo.

Relé de bloqueo activo – muestra el estado de la salida del relé, donde en caso de error de registro o configuración SIP el parámetro estará activo. Si ocurre alguno de los errores el ascensor quedará bloqueado.

Micrófono externo – muestra la conexión de un micrófono externo al dispositivo.



ATENCIÓN

Durante la operación del dispositivo el cambio del estado de la conexión del micrófono externo se mantiene sin cambio. El estado actual del micrófono externo se detecta solo a la hora de inicio/reinicio del dispositivo.

Estados de error

Error de registro SIP – indica si actualmente hay un problema con el registro de la cuenta SIP.

Error de configuración – indica si el dispositivo tiene una configuración válida para llamadas de alarma (ALARMA1).

Fallo de audio – indica si la última prueba de audio finalizó exitosamente y por lo tanto no se registró ningún error de audio.

Fallo del botón ALARMA1 – indica si el botón ALARMA1 está actualmente defectuoso.

comprobar error de llamada – indica si la última llamada de verificación falló.

Dispositivo

El menú Dispositivo muestra información sobre el modelo y sus características, versión de firmware y gestor de arranque, etc.

Información del dispositivo

Certificado de fábrica instalado – especifica el certificado de usuario y la clave privada utilizados para verificar la autorización del intercomunicador para comunicarse con el servidor ACS.

Localiza el dispositivo – óptico o señalización acústica del dispositivo.


Servicios

El menú Servicios muestra el estado de la interfaz de red y los servicios seleccionados.

Registros de llamadas

El menú Registros de llamadas muestra una descripción general de todas las llamadas realizadas. Cada llamada lleva la siguiente información:

- Tipo de Contacto,
- identificador de llamadas/llamadas,
- fecha y hora de implementación,
- duración de la llamada y su estado (entrante, saliente, perdida, contestada en otro lugar, botón de timbre).

El campo de búsqueda permite búsquedas de texto completo en el nombre de la llamada. La casilla de verificación se utiliza para marcar todos los registros para su eliminación masiva. La grabación de llamada seleccionada también se puede eliminar individualmente usando el botón . La descripción general muestra los últimos 20 registros, ordenados desde la llamada más reciente hasta la más antigua.

Eventos

El menú Eventos muestra los últimos 500 eventos registrados por el dispositivo. Cada evento incluye la fecha y hora de captura, el tipo de evento y una descripción más descriptiva del evento. Los eventos se pueden filtrar en el menú desplegable encima de su propio registro de eventos por tipo.

Eventos	Importancia
CallSessionStateChanged	Un evento que describe la dirección, el estado de la llamada, la dirección, el número de sesión creada y cuántas llamadas se generaron.
CallStateChanged	Cuando el estado de la llamada cambia (sonando, conectada, terminada), también indica la dirección (entrante, saliente) e identificación de la contraparte o cuenta SIP.
CapabilitiesChanged	Suceso que informa sobre el cambio de la lista de las funciones disponibles del dispositivo.

Eventos	Importancia
ConfigurationChanged	Cambio de la configuración del dispositivo.
DeviceState	Indicación del estado del dispositivo, como el inicio.
DirectoryChanged	Cambio de directorio.
DirectorySaved	Guarde el cambio en el directorio.
DtmfEntered	Recepción de código DTMF en una llamada o localmente fuera de una llamada.
ErrorStateChanged	Informa sobre el estado de error del dispositivo.
KeyPressed	Al presionar una tecla (los dígitos son 0, 1, 2..., 9 y las teclas de marcación rápida son %1, %2, etc.).
KeyReleased	Cuando se suelta la tecla (los dígitos son 0, 1, 2..., 9 y las teclas de marcación rápida son %1, %2, etc.).
LogAutomationEvent	
LoginBlocked	Al ingresar 3 inicios de sesión incorrectos a la Web, el dispositivo. Contiene información sobre la dirección IP de estos accesos.
OutputChanged	Señala un cambio en el estado de la salida lógica.
RegistrationStateChanged	Cambiar el estado de registro del proxy SIP.
RescueStateChanged	Indica un cambio en el estado del modo de rescate.

Directorio

La sección Directorio es una de las partes más importantes de la configuración del dispositivo. Sirve para crear y gestionar contactos .

Usuarios



ATENCIÓN

Para poder realizar comunicaciones de emergencia en el ascensor, es necesario tener al menos un usuario en la agenda con un número de teléfono y el modo de confirmación seleccionado .

Función de búsqueda en el menú El dispositivo funciona como una búsqueda de texto completo en nombres y números de teléfono. Busca todas las coincidencias en la lista completa. **Buscar dispositivo** se utiliza para buscar dispositivos registrados, o para agregarlos posteriormente a la lista.

Agregar usuario se utiliza para crear un nuevo usuario, el icono se utiliza para mostrar los detalles de la configuración del usuario . El icono se utiliza para eliminar a un usuario de la lista, cuando se eliminarán todos los datos ingresados. . La lista se puede ordenar por nombre, número de teléfono o modo de confirmación. Se pueden mostrar 15, 25 o 50 dispositivos en 1 página de la lista.

Información básica del usuario

Cada entrada en la lista de usuarios contiene la siguiente información:

Nombre – el nombre del usuario en la posición dada en la guía telefónica. Este parámetro se utiliza para facilitar la orientación entre usuarios.

Tipo de dispositivo — el tipo de dispositivo se puede ajustar manual o automáticamente mediante la función de búsqueda de dispositivos registrados en la lista de dispositivos del directorio.

Correo electrónico – el dispositivo envía información a estos correos electrónicos, por ejemplo sobre llamadas perdidas, etc. Es posible ingresar varias direcciones de correo electrónico, separadas por comas o punto y coma.

Números de teléfono de usuario

Se pueden asignar hasta 6 números de teléfono a cada usuario de la lista. La llamada saliente se dirige a todos los números simultáneamente. Una vez que la llamada se conecta a un número de teléfono (es decir, se confirma), las llamadas a los demás números de teléfono se terminan. Esta regla se aplica independientemente del modo de confirmación configurado.

Número de teléfono — número de teléfono de la estación a la que se dirigirá la llamada. Para la llamada SIP directa, introduzca la dirección "sip: [user_id@] dominio [:puerto]", p. ej.: "sip: 200 @192 .168.22.15" o "sip: nombre@company". Para llamadas locales y llamadas a la aplicación móvil My2N Entrar "dispositivo: ID del dispositivo_". Si escribes /1 o /2 después del número de teléfono, la cuenta SIP 1 o 2 se usa explícitamente para las llamadas salientes. Al añadir /S, es posible forzar una llamada cifrada y /N sin cifrar. La selección y el cifrado de la cuenta al mismo tiempo se pueden especificar, por ejemplo

Se pueden realizar ajustes detallados del número de teléfono pulsando el botón

Configurar el número de teléfono

- **tipo de llamada** – establece el esquema en el URI del destino llamado. Cuando se selecciona Ningún esquema ([sin especificar]), el URI se complementa con datos de la configuración de la cuenta SIP. Otras opciones incluyen llamadas SIP directas (sip:), llamadas locales 2N (dispositivo:), llamadas a dispositivos Crestron (rava:), conexiones a MS Teams (msteams:) o llamadas a VMS, por ejemplo, AXIS Camera Station (vms:).

- **Destino** – establece otras partes del URI del destino llamado. Suele contener un número, dirección IP, dominio, puerto o identificador de dispositivo. Se ingresa un asterisco para las llamadas VMS“**”.
- **Cuenta SIP preferida** – Para las llamadas se utiliza preferentemente la cuenta SIP número 1 o número 2.
- **Cifrado de llamadas** – es posible configurar el cifrado obligatorio de la llamada o, por el contrario, una llamada sin cifrado.

Modo de confirmación – determina cómo se recibirá una llamada de alarma para un número determinado.

Llamar

El servicio de Llamada es una función básica del dispositivo **2N LifIP 2.0** – permite el establecimiento de conexiones con otros dispositivos terminales en redes IP. El dispositivo admite el protocolo SIP extendido.

Configuración general

Configuración general

Tiempo máximo de conversación – establece el tiempo máximo de llamada después del cual finaliza automáticamente. El dispositivo señala que se acerca el final de la llamada emitiendo un pitido 10 segundos antes de que finalice. Si el tiempo máximo de llamada se establece en 0 y no se utiliza SRTP, la llamada no se cronometra.

Límite de tiempo de la confirmación – establece el tiempo durante el cual es posible confirmar la llamada tras la conexión de la llamada. En el caso de que el tiempo se agote, el dispositivo llamará al siguiente número. En el caso de que esté configurada la confirmación mediante la aceptación de llamada, este parámetro es irrelevante.

Llamadas salientes

Tiempo máximo de conexión – establece el tiempo máximo de conexión para las llamadas salientes, después del cual finalizan automáticamente. Si las llamadas se enrutarán a la red GSM a través de pasarelas GSM, se recomienda configurar el valor en un tiempo superior a 20 s.

Tiempo máximo de timbre – establece el tiempo máximo de configuración y timbre después del cual las llamadas salientes finalizan automáticamente. Si las llamadas se dirigirán a la red GSM a través de puertas de enlace GSM, se recomienda configurar el valor en un tiempo superior a 20 s. El valor mínimo es 1 s, el valor máximo es 600 s. Para desactivar el parámetro de tiempo, configure 0.

Ajustes avanzados

Puerto de inicio para RTP – establece el puerto RTP local inicial en un rango de 64 puertos utilizados para la transmisión de audio y video. El valor predeterminado es 4900 (es decir, el rango utilizado es 4900-4963). El parámetro es común a ambas cuentas SIP.

Tiempo de espera de RTP – establece el límite de tiempo para recibir paquetes de flujo de audio RTP dentro de una llamada. Si se excede este límite (los paquetes RTP no se entregan), el dispositivo finalizará la llamada. Esta verificación se puede desactivar configurando el parámetro en el valor 0. El parámetro es común para ambas cuentas SIP y está configurado solo para la cuenta 1.

Registro SIP avanzado – permite escribir información más detallada relacionada con la telefonía SIP en syslog (destinado únicamente a la resolución de problemas).

Llamadas locales

Pestaña de configuración

Permitir llamadas locales – permite llamadas entre dispositivos 2N en la red local. Si esta función está desactivada, otros dispositivos en la red no encontrarán este dispositivo, es decir, no pueden llamar a este dispositivo en el formato dispositivo:ID_dispositivo.

Identificación de red

ID del dispositivo – establece la identificación del dispositivo que se mostrará en la lista de dispositivos locales en todos los dispositivos 2N en la misma red local. Al configurar el número de teléfono del usuario en estos dispositivos para “dispositivo: ID_dispositivo” es posible enrutar la llamada a este dispositivo.

Llamada de prueba – abre una ventana de diálogo con la opción de realizar una llamada de prueba al número de teléfono seleccionado, ver más abajo.

Conexión a las unidades en los vestíbulos

Clave de acceso 1 y 2: configura la clave de acceso entre la unidad de cabina (comunicador 2N) y la unidad del vestíbulo (**2N Sentrio Cabin**). Si la clave de acceso está vacía o no coincide con la clave del dispositivo emparejado, los dispositivos no podrán comunicarse entre sí.

Dispositivos en la red local.

Número de dispositivos locales – muestra el número de dispositivos locales en la red.

Ver una lista de dispositivos locales – muestra una lista detallada de los dispositivos locales en la red.

Pestaña de vídeo

Parámetros de vista previa del 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 **2N LiftIP 2.0**. 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 ancho de banda reducido: reduce la calidad de la vista previa del vídeo para ahorrar ancho de banda.

Pestaña de audio

Enviando DTMF

RTP (RFC-2833) – permite enviar caracteres DTMF utilizando el protocolo RTP según RFC-2833.

INFORMACIÓN SIP (RFC-2976) – permite enviar caracteres DTMF utilizando mensajes SIP INFO según RFC-2976.

recepción DTMF

RTP (RFC-2833) – permite la recepción de caracteres DTMF utilizando el protocolo RTP según RFC-2833.

INFORMACIÓN SIP (RFC-2976) – permite la recepción de caracteres DTMF mediante mensajes SIP INFO según RFC-2976.

Configuración de calidad de transmisión

Compensación de inquietud – establece la longitud del buffer para compensar la desigualdad de los intervalos entre las llegadas de paquetes de audio. Configurar un buffer más largo aumentará la resistencia de recepción a costa de un mayor retraso de audio.

SIP

Dispositivo **2N LiftIP 2.0** le permite configurar dos cuentas SIP independientes. De esta manera, el dispositivo se puede registrar en paralelo con dos números de teléfono, con dos centrales SIP diferentes, etc. Desde el punto de vista de las llamadas entrantes, ambas cuentas SIP son equivalentes. Las llamadas salientes se realizan principalmente a través de la cuenta SIP 1. En caso de que la cuenta SIP 1 no esté registrada (por ejemplo, debido a un mal funcionamiento de la centralita SIP), para las llamadas salientes se utiliza automáticamente la cuenta SIP 2. Para los números de teléfono de la agenda, se puede indicar explícitamente el número de cuenta, que debe usarse para llamadas salientes (por ejemplo, 2568/1: llame al 2568 usando la cuenta 1, sip:1234@192.168.1.1/2 llame a sip uri usando la cuenta 2).

Pestaña de configuración

Habilitar cuenta SIP – permite el uso de una cuenta SIP para llamadas. Si la cuenta no está habilitada, no se puede utilizar para realizar llamadas salientes ni recibir llamadas entrantes.

Identidad del dispositivo

Nombre mostrado – establece el nombre que se mostrará en el teléfono de la persona llamada como identificador de llamadas.

Número de teléfono (identificación) – establece el número de teléfono propio del dispositivo (u otra identificación única que consta de caracteres y números). Este número, junto con el dominio, identifica de forma única el dispositivo durante las llamadas y el registro.

Dominio – establece el nombre de dominio del servicio en el que está registrado el dispositivo. Por lo general, coincide con la dirección SIP Proxy o Registrar.

llamada de prueba – abre una ventana de diálogo con la opción de realizar una llamada de prueba al número de teléfono seleccionado, ver más abajo.

Autenticación

ID para autenticación – ID de usuario alternativo utilizado en la autenticación del dispositivo.

Contraseña – la contraseña utilizada para autenticar el dispositivo. Si su panel de control IP no requiere autenticación, el parámetro no aplica.

Proxy SIP

Dirección proxy – Dirección IP o nombre de dominio del proxy SIP.

Puerto proxy – establece el puerto SIP Proxy (normalmente 5060).

Dirección del primer proxy de respaldo – dirección IP o nombre de dominio del proxy SIP de respaldo. La dirección se utilizará en el caso de que el proxy principal no responda a las peticiones. En el caso de que aquí esté configurado el nombre de dominio y no esté introducido el número del puerto SIP proxy de respaldo, la dirección IP resultante de SIP proxy de respaldo se configurará según los datos de los registros NAPTR y SRV obtenidos de DNS para el nombre correspondiente. En el caso de que DNS no proporcione estos registros, o esté introducido también el número del puerto SIP proxy de respaldo, se utilizará la dirección del registro A para el nombre correspondiente.

Puerto del primer proxy de respaldo – configura el puerto del proxy SIP de respaldo. En el caso de que el parámetro esté vacío, o esté configurado a 0, el dispositivo intentará configurar el número del puerto según los datos de los registros NAPTR y SRV obtenidos de DNS. En el caso de que DNS no proporcione estos registros, se utilizará el valor inicial del número del puerto según la capa de transporte (5060 para UDP y TCP, 5061 para TLS).

Dirección del segundo proxy de respaldo – dirección IP o nombre de dominio del proxy SIP de respaldo. La dirección se utilizará en el caso de que el proxy principal no responda a las peticiones. En el caso de que aquí esté configurado el nombre de dominio y no esté introducido el número del puerto SIP proxy de respaldo, la dirección IP resultante de SIP proxy de respaldo se configurará según los datos de los registros NAPTR y SRV obtenidos de DNS para el nombre correspondiente. En el caso de que DNS no proporcione estos registros, o esté introducido también el número del puerto SIP proxy de respaldo, se utilizará la dirección del registro A para el nombre correspondiente.

Puerto del segundo proxy de respaldo – configura el puerto del proxy SIP de respaldo. En el caso de que el parámetro esté vacío, o esté configurado a 0, el dispositivo intentará configurar el número del puerto según los datos de los registros NAPTR y SRV obtenidos de DNS. En el caso de que DNS no proporcione estos registros, se utilizará el valor inicial del número del puerto según la capa de transporte (5060 para UDP y TCP, 5061 para TLS).

Registrador SIP

Permiso para registrarse – permite el registro del dispositivo con el registrador SIP configurado.

dirección del registrador – Dirección IP o nombre de dominio del Registrador SIP.

El puerto del registrador. – establece 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 cuando el registrador principal no responda a las solicitudes.

Puerto de registro de respaldo – establece el puerto de respaldo del registrador SIP (generalmente 5060).

Vencimiento del registro – le permite configurar el tiempo de vencimiento del registro, lo que afecta la carga en la red y el registrador SIP mediante solicitudes de registro enviadas periódicamente. SIP Registrar puede ajustar el tiempo de vencimiento sin su conocimiento.

Estado de registro – muestra el estado de registro actual (No registrado, Registrando..., Registrado, Registro finalizando...).

Razón del fracaso – muestra el motivo del error del último intento de registro – muestra la última respuesta de error del registrador, por ejemplo, 404 No encontrado.

Ajustes avanzados

Protocolo de transporte para SIP – establece el protocolo utilizado para la comunicación SIP. Puede elegir entre UDP (predeterminado), TCP y TLS.

Versión TLS más baja permitida – especifica la versión más baja de TLS, que se utilizará para registrarse en el servidor y establecer una conexión.

Aplicar esquema URI SIPS - El esquema URI SPS se aplica si el parámetro está activado (los **sips** se utilizan en los mensajes salientes y los mensajes entrantes deben contener **sips**).

Verificar el certificado del servidor – verifica el certificado público del servidor SIP con los certificados de CA cargados en el dispositivo.

Certificado de cliente – especifica el certificado de cliente y la clave privada utilizados para verificar la autorización del intercomunicador para comunicarse con el servidor SIP.

Puerto local para SIP – establece el puerto local que el dispositivo usa para la señalización SIP. El cambio en este parámetro tendrá efecto solo después de reiniciar el dispositivo. Si el parámetro se deja en blanco, se utiliza el valor predeterminado

Valores predeterminados del puerto local para SIP

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

PRACK habilitado – habilita el método PRACK (acuse de recibo confiable de mensajes SIP con códigos 101-199).

REFERIR habilitado – permite el desvío de llamadas mediante el método REFER.

Enviar 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).

Habilitar filtro de dirección IP – le permite activar la función de bloquear la recepción de paquetes SIP desde direcciones distintas a la dirección del SIP Proxy y SIP Registrar. La función se utiliza principalmente para aumentar la seguridad de las comunicaciones y evitar llamadas telefónicas no autorizadas.

Recibir solo llamadas cifradas (SRTP) – establece la restricción de llamadas entrantes en esta cuenta para cifrarlas con el protocolo SRTP. Las llamadas no cifradas serán rechazadas. Al mismo tiempo, para mayor seguridad, se recomienda utilizar TLS como protocolo de transporte para SIP.

Llamadas salientes cifradas (SRTP) – establece las llamadas salientes en esta cuenta encriptadas con SRTP. Al mismo tiempo, para mayor seguridad, se recomienda utilizar TLS como protocolo de transporte para SIP.

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 medios entrantes tempranos – prohíbe la reproducción de la transmisión de vídeo entrante antes de que se conteste la llamada (medios tempranos) enviada por algunas centrales u otros dispositivos. En su lugar, se reproducirá el tono de llamada local estándar.

Valor DSCP de QoS – establece la prioridad de los paquetes SIP en la red. El valor establecido se envía en el campo TOS (Tipo de servicio) en el encabezado del paquete IP. El valor se ingresa como un número decimal. El cambio de este parámetro entra en vigor después de reiniciar el dispositivo.

Permiso para aturdir – habilita la funcionalidad STUN para la cuenta SIP. La dirección y los puertos obtenidos del servidor STUN configurado se utilizarán en los encabezados SIP y la negociación de medios SDP.

dirección del servidor STUN – establece la dirección IP del servidor STUN que se utilizará para esta cuenta SIP.

Puerto del servidor STUN – establece el puerto del servidor STUN que se utilizará para esta cuenta SIP.

Dirección IP externa – establece la dirección IP pública o el nombre del enrutador al que está conectado el dispositivo. Si la dirección IP del dispositivo es pública, deje este campo en blanco.

Compatibilidad con dispositivos Broadsoft – establece el modo de compatibilidad con los paneles de control de Broadsoft. En este modo, cuando el intercomunicador recibe una nueva invitación del panel de control, responde repitiendo el último SDP enviado con los códecs utilizados actualmente en lugar de la oferta completa.

Rotar registros SRV – permite la rotación de registros SRV para el proxy y registrador SIP. Este es un método alternativo para cambiar a servidores de respaldo en caso de falla o indisponibilidad de los servidores principales.

Pestaña de vídeo

Códecs de vídeo

Le permite habilitar/deshabilitar el uso de códecs de video individuales ofrecidos al establecer una conexión y establecer su prioridad.

Configuración de calidad de transmisión

Valor DSCP de QoS – establece la prioridad de los paquetes de vídeo RTP en la red. El valor establecido se envía en el campo TOS (Tipo de servicio) del encabezado del paquete IP.

Longitud máxima del paquete– le permite configurar el tamaño máximo de los paquetes de video RTP enviados.

Configuración avanzada de códec

Activado – habilita el modo de paquetización y establece el tipo de carga útil para códecs individuales. El tipo de carga útil se seleccionará automáticamente si no se puede configurar manualmente.

Tipo de carga útil SDP – establece el "tipo de carga útil" del códec de video H.264 (modo de paquetización 1). Es posible establecer un valor de 96 a 127 o 0 por no ofrecer esta variante de códec.

Pestaña de audio

Códecs de audio

En este bloque, es posible habilitar/deshabilitar el uso de códecs de audio individuales ofrecidos al establecer una conexión y establecer su prioridad.

Enviando DTMF

Este bloque se utiliza para configurar el método de envío de caracteres DTMF desde el dispositivo. Verifique que las opciones y configuraciones de recepción DTMF de la otra parte funcionen correctamente.

Modo de envío — establece si será posible enviar caracteres DTMF al pulsar del 0 al 9, * y # en el teclado numérico del dispositivo durante la llamada. El envío solo se puede configurar para las llamadas entrantes o salientes, o para todas las llamadas

Dentro de banda (audio) – habilita la forma clásica de enviar DTMF en la banda de audio utilizando dos tonos estandarizados.

RTP (RFC-2833) – permite enviar caracteres DTMF utilizando el protocolo RTP según RFC-2833.

INFORMACIÓN SIP (RFC-2976) – permite enviar caracteres DTMF utilizando mensajes SIP INFO según RFC-2976.

recepción DTMF

Este bloque se utiliza para configurar la recepción de caracteres DTMF desde el intercomunicador. Verifique que las opciones y configuraciones de envío DTMF de la otra parte funcionen correctamente.

Dentro de banda (audio) – permite la recepción de tonos clásicos de dos tonos DTMF en la banda de audio.

RTP (RFC-2833) – permite la recepción de caracteres DTMF utilizando el protocolo RTP según RFC-2833.

INFORMACIÓN SIP (RFC-2976) – permite la recepción de caracteres DTMF mediante mensajes SIP INFO según RFC-2976.

Configuración de calidad de transmisión

Valor DSCP de QoS – establece la prioridad de los paquetes de audio RTP en la red. El valor establecido se envía en el campo TOS (Tipo de servicio) del encabezado del paquete IP.

Compensación de inquietud – establece la longitud del buffer para compensar la desigualdad de los intervalos entre las llegadas de paquetes de audio. Configurar un buffer más largo aumentará la resistencia de recepción a costa de un mayor retraso de audio.

llamada de alarma

Pestaña de llamada de alarma

Configuraciones básicas

Tiempo de pulsación para activar la función – establece el tiempo mínimo en milisegundos durante el cual debe pulsarse el botón ALARM1 para iniciar la llamada de alarma. De acuerdo con las normas vigentes de la UE, el valor máximo no debe superar los 3000 ms. El rango recomendado es de 2000 a 3000 ms.

llamada retrasada – al marcar se establece si la llamada de alarma se retrasará (durante el retraso se reproduce en la cabina el mismo mensaje de audio que cuando se estableció la llamada).

Retraso de llamada – establece el retraso de la llamada de alarma en segundos (durante el retraso se reproduce un mensaje de audio en la cabina como cuando se realiza una llamada). No establezca este parámetro en un valor inferior al del parámetro **Duración de la pulsación para activar** en el bloque **Alarma de prueba**. Según las normas vigentes de la UE, la función debe ajustarse a más de 0 s.

alarma de prueba



NOTA

Según las normas vigentes de la UE, esta función debe estar habilitada.

Permitir – establece si es posible iniciar una llamada de alarma de prueba presionando prolongadamente el botón ALARMA1.

Duración de la pulsación para activar – establece el tiempo de presión del botón ALARMA1 en segundos, lo que inicia la llamada de alarma de prueba. El valor no debe ser mayor que el valor del parámetro **llamada retrasada**. De acuerdo con las normas vigentes de la UE, el valor debe establecerse en 30 s.

Destino

El bloque Destino permite seleccionar el usuario al que se dirigirá la conexión durante una llamada de alarma.

Número de repeticiones – establece el número de ciclos de llamada en caso de que la llamada no sea reconocida/atendida. El número predeterminado de repeticiones es 3; se puede configurar un máximo de 9 repeticiones. Si se produce el número establecido de ciclos de llamada y la llamada no se atiende, se finaliza automáticamente.

Prueba de llamada de ALARMA – permite el lanzamiento de una llamada de alarma de prueba.

Pestaña de llamada de alarma 2

Destino

El bloque Destino permite seleccionar el usuario al que se dirigirá la conexión durante una llamada de alarma.

Número de repeticiones – establece el número de ciclos de llamada en caso de que la llamada no sea reconocida/atendida. El número predeterminado de repeticiones es 3; se puede configurar un máximo de 9 repeticiones. Si se produce el número establecido de ciclos de llamada y la llamada no se atiende, se finaliza automáticamente.

Prueba de llamada ALARMA2 – permite lanzar la llamada de alarma de prueba 2.

llamada de control

La llamada de control sirve para establecer automáticamente una llamada de control, cuya función es comprobar el correcto funcionamiento de **2N LiftIP 2.0**. La función simula una llamada entrante.



NOTA

Según las normas vigentes de la UE, esta función debe estar habilitada.

Llamada de control habilitada – permite realizar llamadas de control.

Configuraciones básicas



NOTA

Según las normas vigentes de la UE, la función de llamada de control debe realizarse al menos una vez cada tres días.

Período – la llamada de control se repite una vez cada determinado número de días. La primera llamada de control se realiza en un momento seleccionado aleatoriamente dentro de las primeras 24 horas después de iniciar el dispositivo.

Próxima llamada – indica la hora de la próxima llamada de control regular.

Destino

El bloque Destino permite seleccionar el usuario al que se dirigirá la conexión durante la llamada de control.

Número de repeticiones – establece el número de ciclos de llamada en caso de que la llamada no sea reconocida/atendida. El número predeterminado de repeticiones es 3; se puede configurar un máximo de 9 repeticiones. Si se produce el número establecido de ciclos de llamada y la llamada no se atiende, se finaliza automáticamente.

Prueba de llamada de control – permite el lanzamiento de una llamada de control de prueba.

llamada operativa

Destino

El bloque Destino permite seleccionar el usuario al que se dirigirá la conexión durante una llamada operativa.

La llamada operativa se utiliza para crear automáticamente una llamada operativa si ocurre uno de los eventos preestablecidos. Esta sección establece el destino al que se dirigirá la llamada de servicio. La configuración de la llamada en sí se realiza mediante automatización, consulte [Automatización \(p. 60\)](#). Una llamada operativa se activa mediante la acción StartLiftCall con el parámetro CallType = operacional. La acción se activa cuando se produce el evento al que está vinculada la acción:

- **RescueTerminated** para realizar una llamada operativa al salir del modo de rescate.
- **ErrorStateChanged** para establecer una llamada operativa en caso de falla/reparación del botón o falla/reparación del audio. El tipo de cambio de estado de error está determinado por los parámetros de este evento.

1-2 – permite seleccionar el usuario al cuál se dirigirá la conexión.

Número de repeticiones – establece el número de ciclos de llamada en caso de que la llamada no sea reconocida/atendida. El número predeterminado de repeticiones es 3; se puede configurar un máximo de 9 repeticiones. Si se produce el número establecido de ciclos de llamada y la llamada no se atiende, se finaliza automáticamente.

Servicios

Elevar

Configuraciones generales

Identificación del ascensor – establece el número de identificación del ascensor o del comunicador de ascensor, que se envía o lee en llamadas individuales. El número de identificación deberá constar de un máximo de 16 dígitos.

Modo de recuperación

El modo de rescate ocurre cuando se conecta una llamada de alarma (emergencia). Al habilitar el modo, también es necesario configurar el método para su terminación posterior.



NOTA

Para la versión UE: En **sección Servicios > Ascensor > Modo de recuperación** habilitar el modo de recuperación. **Este paso es necesario para cumplir con la legislación de la UE.** Una vez activado, el dispositivo le permite tener un Modo de Rescate activo, durante el cual es posible tener múltiples llamadas de alarma. Esto facilita Elevator Center vea múltiples llamadas de alarma dentro de un modo de recuperación y regrese a las conversaciones de chat.

Para la versión estadounidense: En **sección Servicios > Ascensor > Modo de recuperación** El modo de recuperación no debe estar habilitado. **Este paso es necesario para cumplir con la legislación estadounidense.** Cada llamada de alarma será en Elevator Center mantenido como un nuevo récord.

Habilitar el modo de recuperación– habilita el modo de recuperación (el modo de recuperación habilitado requiere al menos una forma de salir del modo de recuperación).

Terminación con el botón ALARM2– establece si es posible finalizar el modo de recuperación presionando el botón ALARM2.

Salir introduciendo la contraseña - establece si la salida del modo de desbloqueo se confirma mediante una contraseña (la contraseña se envía al dispositivo como DTMF en la llamada). La introducción de una contraseña para salir del modo de desbloqueo no es efectiva si hay una llamada de alarma en curso.

Contraseña - Configura la contraseña para la cancelación del modo de rescate. La contraseña se envía al dispositivo como DTMF durante la llamada y puede estar formada solo con números (máx. 16). La contraseña se introduce en el DTMF en el formato “*contraseña*”. Por ejemplo, si la contraseña es 12345, deberá introducir “*12345*” en la llamada.

Monitoreo de cabina

Modo de monitoreo – establece el modo de monitoreo del dispositivo. Esto cambia el comportamiento del micrófono (silencio) y la indicación del modo de monitoreo del dispositivo (el dispositivo indica que el audio y video de la cabina no están disponibles por razones de privacidad). El seguimiento puede ser:

Habilitar después de una llamada de alarma a – establece cuánto tiempo permanecerá silenciado el micrófono y el dispositivo indicará que el monitoreo no está habilitado (el audio y el video desde la cabina no

están disponibles por razones de privacidad) después de una llamada de alarma. Esto sólo se aplica si es **Modo de monitoreo** empezar a "Habilitado después de una llamada de alarma".

Correo electrónico

Pestaña SMTP

Servicio SMTP habilitado – permite o bloquea el servicio de envío de correos electrónicos desde el dispositivo.

Configuración del servidor SMTP

Dirección del servidor – Dirección del servidor SMTP al que se enviarán los correos electrónicos.

Puerto del servidor – establece el puerto del servidor SMTP. El valor predeterminado es 25, la modificación es adecuada sólo en el caso de una configuración del servidor SMTP no estándar.

Tipo de seguridad – selecciona el tipo de seguridad para la comunicación con el servidor SMTP.

Inicie sesión en el servidor SMTP

Nombre de usuario – especifica un nombre de inicio de sesión de servidor válido si el servidor SMTP requiere autorización. De lo contrario, el campo puede estar vacío.

Contraseña – especifica una contraseña válida para iniciar sesión en el servidor si el servidor SMTP requiere autorización. De lo contrario, el campo puede estar vacío.

Certificado de cliente – especifica el certificado del cliente y la clave privada, que se utilizan para cifrar la comunicación entre el dispositivo y el servidor SMTP.

Configuraciones generales de correo electrónico

dirección del remitente – especifica la dirección predeterminada para todos los correos electrónicos salientes.

Configuraciones avanzadas

Entregar a – establece el tiempo máximo que el dispositivo intenta enviar correo electrónico a un servidor SMTP no disponible.

Automatización

Los dispositivos 2N ofrecen opciones de configuración muy flexibles según los distintos requisitos del usuario. Hay situaciones en las que la gama habitual de ajustes (por ejemplo, configurar el comportamiento de los interruptores o las llamadas) no es suficiente y, para estos casos, los dispositivos 2N proporcionan una interfaz de automatización programable especial. Un uso típico de la automatización es en aplicaciones que requieren una integración más compleja con sistemas de terceros.

Se ingresa a la interfaz de Automatización haciendo clic en  para la función que desea crear o cambiar.



SUGERENCIA

Una descripción detallada de la función y configuración de Automatización está disponible en [Automatización manual](#).



NOTA

La función de automatización solo está disponible con la licencia Gold.

API HTTP

La API HTTP es una interfaz de aplicación para controlar funciones de dispositivos seleccionados mediante el protocolo HTTP. Esta interfaz facilita la integración de dispositivos 2N con productos de terceros, p.e. sistemas domóticos, sistemas de vigilancia y seguridad de edificios, etc.

Pestaña de servicios

Servicios API HTTP

La API HTTP se divide en los siguientes servicios por función:

- **API del sistema**– permite cambios de configuración, adquisición de estado y actualización del dispositivo.
- **I/O AP**– permite el control y seguimiento de las entradas y salidas lógicas del dispositivo.
- **Audio API** – permite controlar la reproducción de los sonidos y monitorear el micrófono del dispositivo.
- **E-mail API** – permite enviar desde el dispositivo los e-mails de usuario.
- **Phone/Call API** – permite controlar y vigilar las llamadas entrantes y salientes.
- **Logging API** – permite leer los sucesos registrados en el dispositivo.
- **API de automatización**– le permite establecer requisitos de autorización y comunicación segura/no segura.
- **Ascensor API** - proporciona conexión **Sentrio Lobby** al comunicador del ascensor de emergencia.

Para cada servicio, se puede configurar el protocolo de transporte (HTTP=TCP o HTTPS=TLS) y el método de autenticación (ninguno, Básico o Digest). En la configuración de la API HTTP, se pueden crear hasta cinco cuentas de usuario (con su propio nombre y contraseña) con la posibilidad de un control detallado del acceso a servicios y funciones individuales.

Para cada servicio, se puede configurar el método de autenticación requerido para las solicitudes enviadas al dispositivo. Si no se realiza la autenticación, la solicitud se rechaza. Las solicitudes se autentican mediante el protocolo de autenticación estándar descrito en RFC-2617. Es posible elegir los siguientes tres métodos de autenticación:

- **Ninguno**– el servicio no requiere ninguna autenticación. En este caso, el servicio queda completamente desprotegido en la red local.
- **Basic**– el servicio requiere autenticación básica según RFC-2617. El servicio en este caso requiere una contraseña, pero ésta se envía en formato abierto. Recomendamos combinar esta opción con el protocolo HTTPS si es posible.
- **Digest**– el servicio requiere autenticación Digest según RFC-2617. Esta opción es la predeterminada y la más segura de los métodos anteriores.

Pestaña Cuenta 1-5

El dispositivo 2N le permite administrar hasta cinco cuentas de usuario para acceder a los servicios API HTTP. La cuenta de usuario incluye el nombre y la contraseña del usuario y una tabla de derechos de acceso de usuario a servicios API HTTP individuales.

Cuenta habilitada – habilita la cuenta de usuario.

Asignar sonidos

Nombre de usuario – le permite ingresar un nombre de usuario para la autenticación en la API HTTP.

Contraseña – ingrese la contraseña para autenticarse en la API HTTP.

Derechos de usuario

La tabla de derechos de acceso se puede utilizar para administrar los privilegios de la cuenta de usuario para servicios individuales.

Integración

Pestaña de equipos de MS

La integración con Microsoft Teams garantiza las llamadas entre el dispositivo 2N y la cuenta de Microsoft Teams. Para conectar el dispositivo con Microsoft Teams, primero es necesario configurar la puerta SIP de la instalación de Microsoft Teams. El procedimiento se describe en [FAQ](#) (en inglés) o en la documentación de MS Teams. Después de introducir la dirección del servidor de configuración en la configuración del dispositivo 2N, se realizará la conexión (onboarding). Tras el onboarding, es posible iniciar sesión en la cuenta de Microsoft Teams en la interfaz de configuración web.

Equipos de Microsoft habilitados – habilita el servicio de integración con MS Teams

Servicio

Estado – muestra el estado actual del proceso de incorporación e inicio de sesión.

- “Apagado” – la función está desactivada.
- “Onboarding” – el dispositivo adquiere/ha adquirido una configuración común para la incorporación o una configuración individual para la incorporación (antes de iniciar sesión).
- “Fallo en el onboarding” – el dispositivo no pudo obtener una configuración de incorporación compartida o individual o no pudo registrarse con el servidor de incorporación SIP.
- “Desconectado” – no hay respuesta del servidor.
- “En línea” – el dispositivo se registró correctamente en el servidor final SIP.
- “Error en la inscripción” – el dispositivo no pudo registrarse con el servidor final SIP.
- “Licencia requerida” – el dispositivo no tiene la licencia adecuada para esta función.

Número telefónico – muestra el número de teléfono (ID) que el dispositivo recibió del servidor de MS Teams.

llamada de prueba – abre una ventana de diálogo con la opción de realizar una llamada de prueba al número de teléfono seleccionado.

Configuración del servidor de configuración

Cómo obtener una dirección – le permite elegir si la dirección del servidor de incorporación de MS Teams se ingresará manualmente o se utilizará la dirección obtenida automáticamente del servidor DHCP usando el parámetro Opción 66 o 150.

Dirección del servidor – le permite ingresar manualmente la dirección del servidor de incorporación de MS Teams.

Dirección DHCP (opción 66/150) – muestra la dirección del servidor obtenida utilizando la opción DHCP 66 o 150.

Programar actualizaciones de configuración

Cuando el dispositivo se inicia – permite la inspección y posiblemente realizando una actualización cada vez que se inicia el dispositivo.

Período de actualización – establece el período de ejecución de la actualización. Se puede configurar para que se ejecute una vez cada hora, día, semana y mes.

Hora de actualización – le permite configurar la hora en formato HH:MM en la que la actualización debe realizarse periódicamente. El parámetro no se utiliza si el intervalo de actualización se establece en menos de 1 día. La hora está configurada en UTC. Verifique el valor de Hora de próxima actualización para ver la hora real en la que está programada la actualización.

Solapa Discovery Service

Configuración

Dirección del servidor de integración – configura la URL del servicio de búsqueda del dispositivo. El dispositivo envía requerimientos HTTP con datos básicos al inicio, cuando se cambia la dirección IP y periódicamente (si está configurado). Si el campo está vacío, los requerimientos no se envían.



NOTA

La solicitud JSON enviada contiene la siguiente información sobre el dispositivo: MacAddress, Dhcp, IpAddress, NetMask, Gateway, SwVersion, SerialNumber, Variant, VariantId, Description, ProductName, CameraResolution (max.), HttpPort, HttpsPort.

Verificar el certificado del servidor – habilita la verificación del certificado del servidor de integración, lo cual garantiza que los requerimientos de Discover se envíen a un servidor de confianza.

Certificado de cliente – elige cuál de los certificados cargados se utilizará para la comunicación cifrada con el servidor de integración.

Enviar requerimientos de búsqueda periódicamente – permite enviar requerimientos HTTP de Discovery.

Período de búsqueda – configura el período de envío de un requerimiento HTTP a la URL configurada en segundos.

Estado de integración – muestra el estado de integración según la respuesta del servidor.

Detalles – muestra los detalles contenidos en la respuesta del servidor.

Sonidos de usuario

2N LiftIP 2.0 Señaliza distintos estados de funcionamiento mediante secuencias de tonos. Si los tonos de señalización estándar no se adaptan a sus necesidades, puede modificarlos.

Pestaña Asignaciones de sonido

Idioma 1-3 – selecciona el idioma para las notificaciones de audio del dispositivo. 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.





Asignar sonidos

- “Estableciendo una conexión” – establece el mensaje sonoro que se reproducirá en la cabina cuando se establezca una llamada de alarma.
- “Llamada de alarma” – establece el mensaje de audio que se reproducirá en la llamada cuando se conecte la llamada de alarma.
- “Llamada de control” – establece el mensaje de audio que se reproducirá en la llamada cuando se conecte la llamada de control.
- “extensión de llamada” – establece un mensaje de audio que se reproducirá en la llamada cuando la llamada esté a punto de finalizar.
- “Desconexión” – establece un mensaje de audio que se reproducirá en la llamada y en la cabina (si es relevante para el tipo de llamada) en caso de que sea necesario interrumpir una llamada en curso.
- “fin de llamada” – establece un mensaje de audio que se reproducirá en la cabina si la llamada ha finalizado.
- “El fin de la redención” – establece el mensaje de sonido que se reproducirá en la llamada y en la cabina si se finaliza el modo de rescate (relevante solo si el modo de rescate está habilitado).

Pestaña de grabación de sonidos

Se pueden agregar hasta 10 archivos de audio con una duración máxima de 60 s al dispositivo para una mayor claridad, es posible asignar un nombre personalizado a cada audio grabado.

Cómo agregar sonidos

1. Sube el archivo de sonido al dispositivo presionando el botón .
2. En el cuadro de diálogo, seleccione el archivo guardado en su computadora y presione **Registro**.
3. Usando el botón  Puede grabar el archivo de sonido directamente usando el micrófono de su PC.
4. Puede eliminar el archivo usando el botón . Puede reproducir el archivo de audio grabado (localmente en su computadora) usando el botón .


Servidor web

2N LiftIP 2.0 Se puede configurar mediante un navegador normal que accede al servidor web integrado en el dispositivo. El protocolo HTTPS seguro se utiliza para la comunicación entre el navegador y el dispositivo.

Ajustes básicos

Nombre de la instalación – establece el nombre del dispositivo que se muestra en la esquina superior derecha de la interfaz web, en la ventana de inicio de sesión y posiblemente en otras aplicaciones (2N Network Scanner etc.).

Idioma de la interfaz web – establece el idioma predeterminado después de iniciar sesión en el servidor web de administración. Puede cambiar temporalmente el idioma de la interfaz web en cualquier momento usando los botones en la barra superior de la página.

Contraseña – establece la contraseña para iniciar sesión en el dispositivo. Puedes cambiar tu contraseña haciendo clic en el ícono del lápiz . La contraseña debe contener al menos 8 caracteres, de los cuales una letra minúscula del alfabeto, una letra mayúscula del alfabeto y al menos un número.

Ajustes avanzados

puerto HTTP – establece el puerto de comunicación del servidor web para la comunicación utilizando el protocolo HTTP inseguro. El cambio de puerto entrará en vigor solo después de que se reinicie el dispositivo.

Puerto HTTPS – establece el puerto de comunicación del servidor web para la comunicación utilizando el protocolo HTTPS seguro. El cambio de puerto entrará en vigor solo después de que se reinicie el dispositivo.




Versión TLS más baja permitida – especifica la versión más baja de TLS que podrá conectarse al dispositivo.

Certificado de servidor HTTPS – establece el certificado del servidor y la clave privada, que se utilizan para cifrar la comunicación entre el servidor HTTP del dispositivo y el navegador web del usuario.

Permitir acceso remoto – permite el acceso remoto al servidor web del dispositivo desde direcciones IP fuera de la red local.

Localización de usuarios

Idioma original – permite descargar un archivo original en formato XML desde el dispositivo, que contiene todos los textos de la interfaz de usuario web en inglés.

Idioma del usuario – te permite subir , descargar  y posiblemente eliminar  Archivo de usuario con traducciones personalizadas de textos de la interfaz de usuario web.

prueba de audio

Prueba de audio habilitada – permite la ejecución automática de la prueba de audio.

Configuración de prueba

Período de prueba – le permite configurar el período de ejecución de la prueba. La prueba se puede ejecutar automáticamente una vez al día o una vez a la semana.

Tiempo de ejecución de la prueba – le permite configurar la hora a la que se debe realizar la prueba periódicamente. La hora se puede configurar en formato HH:MM. Recomendamos establecer una hora en la que se espera un uso mínimo del dispositivo.

Resultado de la prueba

Estado de la prueba – muestra el estado actual de la prueba en curso.

Hora de la última prueba – muestra la hora de inicio de la última prueba.

El resultado de la última prueba. – muestra el resultado de la última prueba.

SNMP

Las unidades de control de acceso 2N integran la funcionalidad que permite la supervisión remota de los dispositivos en la red mediante el protocolo SNMP.

Servicio habilitado – permite activar esta función.

Ajustes de SNMP

Versión mínima permitida – selecciona la versión SNMP más baja aceptada por el dispositivo. SNMPv3 aplica el cifrado.

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

[Descargar el archivo MIB](#) – permite descargar la definición actual de la tabla MIB desde el dispositivo

SNMP identificación

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).

Direcciones IP autorizadas

Dirección IP 1 – introduzca direcciones IP válidas para acceder 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.

Configuración de SNMPv3

Nombre de usuario – establecer el algoritmo que se utiliza para la autenticación de trampas SNMPv3.

Autenticación – establece el algoritmo que se utilizará para descifrar las trampas SNMPv3.

Contraseña de autenticación – establecer la contraseña de autenticación SNMPv3.

Privacidad/Encriptación – establece el algoritmo que se utilizará para descifrar las trampas SNMPv3.

Contraseña de descifrado – establece la contraseña para descifrar las trampas SNMPv3.

Hardware

Audio

En esta parte de la configuración, se ajustan el volumen de las llamadas y el volumen de la señalización de los diferentes estados del dispositivo.

El volumen general del dispositivo afecta al volumen de las llamadas y al volumen de los tonos de señalización. Ajuste este parámetro según el nivel de ruido del entorno en el que se utilice el dispositivo.



SUGERENCIA

El volumen general del dispositivo también se puede controlar mediante los botones VOL+ y VOL-.

Volumen de llamadas telefónicas

Volumen del timbre – establece el volumen de los tonos de marcación, timbre y ocupado. Esta configuración no se aplica si los tonos de marcado se generan externamente. El valor es relativo al volumen total.

Volumen de señal

Volumen del tono de advertencia – ajusta el volumen de los tonos de aviso y señalización descritos en el capítulo Señalización de estados de funcionamiento. El valor es relativo al volumen total.

No reproduzca tonos de advertencia – cuando está marcado, no reproducirá la señalización de los siguientes estados operativos: aplicación interna en ejecución, dirección IP recibida y dirección IP perdida.

Volumen de sonidos de usuario. – establece el volumen de los sonidos del usuario reproducidos por la automatización. El valor es relativo al volumen total.

Señalización del inicio y del estado de la red - Selecciona el modo de señalización acústica del inicio de la aplicación y de la ganancia o pérdida de la dirección IP.

- **Activado** - el dispositivo reproduce señales de audio cada vez que se inicia la aplicación y cada vez que cambia la dirección IP.
- **Desactivado** - no se reproduce ninguna señal de audio.
- **Sólo una vez** - el aparato reproducirá las señales que le notifican que inicie la aplicación y obtendrá una dirección IP sólo una vez después de iniciarla. Esta función es útil cuando la dirección IP cambia con frecuencia o cuando hay conexiones intermitentes en las que las señales repetidas podrían molestar a los usuarios.

Configuración de entrada de audio

Ganancia de entrada de micrófono – le permite configurar la ganancia de la entrada del micrófono.

Entradas digitales

Las opciones de entradas digitales del dispositivo se describen en el menú Entradas digitales.

Inversión de entrada

Botón ALARMA1 invertido – la entrada invertida está activa cuando el contacto está abierto o se aplica tensión.

Botón ALARM2 invertido – la entrada invertida está activa cuando el contacto está abierto o se aplica tensión.

Entrada CANCELAR invertida – la entrada invertida está activa cuando el contacto está abierto o se aplica tensión.

Botones

Tiempo de evaluación de falla del botón – establece el tiempo durante el cual el botón ALARMA1 debe estar cerrado antes de que se detecte una falla en el botón.

cámara externa

Cámara IP externa

Cámara habilitada – al marcar, se permite la descarga de transmisión RTSP desde una cámara IP externa. Para que funcione correctamente, es necesario completar una dirección de transmisión RTSP válida, o nombre de usuario y contraseña.

Dirección de transmisión RTPS – establece la dirección IP de la transmisión RTSP en el formato “rtsp:// dirección_ip_cámara/parámetros”. Los parámetros son específicos del modelo de cámara IP seleccionado.

Nombre de usuario – nombre de usuario para autenticar la conexión a la cámara IP externa. El parámetro es obligatorio sólo si la cámara IP externa requiere autenticación.

Contraseña – contraseña para autenticar la conexión a la cámara IP externa. El parámetro es obligatorio sólo si la cámara IP externa requiere autenticación.

Puerto RTP local – el puerto local para RTP se puede cambiar si así lo requiere la configuración de la red.

Comunicación de cámara IP externa

La ventana Comunicación de la cámara IP externa muestra el progreso de la comunicación RTSP con la cámara IP externa configurada, incluidos los errores y el mal funcionamiento.

Sistema

Coser

Dispositivo **2N LiftIP 2.0** se conecta a la red local y debe tener una dirección IP válida configurada para un funcionamiento adecuado, o puede obtener una dirección IP de un servidor DHCP en esta red. La dirección IP y la configuración de DHCP se configuran en la sección Red.



SUGERENCIA

La dirección IP actual del dispositivo se puede encontrar en la aplicación. 2N Network Scanner, que se puede descargar gratuitamente en el sitio web 2N.com. El procedimiento se describe en el capítulo. [Encontrar la dirección IP usando 2N Network Scanner](#).

Solapa Básico

Utilizar el servidor DHCP – habilita la obtención automática de la dirección IP desde el servidor DHCP en la red local. Si no hay servidor DHCP en la red o si no se puede utilizar, deberá configurar la red manualmente.

Configuración de una dirección IP estática

Dirección IP estática – la dirección IP estática del dispositivo. La dirección se utiliza en conjunto con los siguientes parámetros en el caso de que el parámetro Utilizar el servidor DHCP esté deshabilitado.

Máscara de red – configura la máscara de red.

Portal inicial – dirección del portal inicial que permite la comunicación con los dispositivos fuera de la red local.

Configuración de DNS

Utilizar siempre la configuración manual: permite configurar manualmente las direcciones de los servidores DNS.

DNS primario – dirección del servidor DNS primario para traducir los nombres de dominio en direcciones IP.

DNS secundario – dirección del servidor DNS secundario utilizado en el caso de que el servidor DNS primario no esté disponible.

Configuración de la interfaz de red

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).

Identificación de red

Nombre de host – configuración de la identificación de los dispositivos de la red.

Identificador del fabricante – configura el identificador del fabricante como una cadena de símbolos para DHCP Option 60.

Ajustes de VLAN

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.

ID VLAN – el ID de red virtual seleccionado en el 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](#).

Pestaña Firewall

Habilite el firewall: protege el dispositivo frente a solicitudes maliciosas. Se recomienda encarecidamente mantener el cortafuegos activado en todo momento.

Firewall

Habilitado – habilitado el firewall que protege el dispositivo de solicitudes maliciosas.

Estado – indica el estado del firewall. El estado del cortafuegos puede ser Desactivado, En funcionamiento o Posible ataque detectado (cuando se detecta un problema y se ignoran algunas solicitudes).

Fecha y hora

La hora del dispositivo se puede sincronizar con la hora de Internet en cualquier momento marcando la función [Aprovecha el tiempo de internet](#) o con la hora actual en su PC usando el botón [Sincronizar con el navegador](#).



ATENCIÓN

Para obtener máxima precisión y confiabilidad, se recomienda tener la función activada [Aprovecha el tiempo de internet](#). En condiciones normales de funcionamiento, el error horario en el dispositivo puede ser de hasta ± 2 minutos/mes.



NOTA

La configuración correcta de fecha y hora no es necesaria para el funcionamiento básico del dispositivo..

Tiempo actual

Aprovecha el tiempo de internet – permite el uso de un servidor NTP para sincronizar la hora interna del dispositivo.

Sincronizar con el navegador – puede utilizar el botón para sincronizar la hora del dispositivo con la hora actual de su PC en cualquier momento.

Zona horaria

Detección automática – establece si la zona horaria será detectada automáticamente por el servicio My2N. Si la detección automática está desactivada, se utiliza la configuración del parámetro Selección manual (zona horaria seleccionada manualmente o regla personalizada).

Zona horaria detectada – muestra la zona horaria detectada automáticamente. Si el servicio no está disponible o está deshabilitado, muestra N/A.

Selección manual – establece la zona horaria para la ubicación de instalación del dispositivo. El ajuste determina el cambio de hora y las transiciones entre el horario de verano y el de invierno.

Regla propia – si el dispositivo está instalado en una ubicación que no figura en el parámetro Zona horaria, la regla de zona horaria se puede configurar manualmente.

Servidor NTP

Dirección del servidor NTP – establece la dirección IP o el nombre de dominio del servidor NTP con el que el dispositivo sincroniza la hora interna. Ni la dirección IP del servidor ni el nombre de dominio se pueden configurar cuando la función está deshabilitada [Aprovecha el tiempo de internet](#).

Estado de tiempo de NTP – muestra el estado del último intento de ajustar la hora local utilizando el servidor NTP (No ajustado, Ajustado, Error).

Función

El menú muestra una lista de funciones beta lanzadas que están destinadas a pruebas de usuarios.

La lista dice:

- nombre de la función,
- estado de la función que indica si la función está ejecutándose o detenida,
- acción para iniciar o detener la función.

Para iniciar o detener la función, espere hasta que se reinicie el dispositivo. Mientras no se reinicie el dispositivo, es posible cancelar la solicitud de cambio de estado con una acción **Interrumpir**.



NOTA

Las funciones de prueba no están garantizadas y 2N TELEKOMUNIKACE a.s. no es responsable de las limitaciones funcionales y posibles daños que surjan como resultado de las limitaciones funcionales de las funciones beta. Las funciones Beta se proporcionan únicamente con fines de prueba.

Certificados

Algunos servicios de red de dispositivos **2N LifiIP 2.0** utilizan el protocolo seguro TLS para comunicarse con otros dispositivos en la red. Este protocolo evita que terceros escuchen a escondidas, o modificar el contenido de la comunicación. Al establecer una conexión utilizando el protocolo TLS, una unilateral, posiblemente autenticación bidireccional que requiere certificados y claves privadas.

Servicios de dispositivos que utilizan el protocolo TLS:

1. Servidor web (protocolo HTTPS)
2. 802.1x (protocolo EAP-TLS)
3. SIP

El dispositivo le permite cargar hasta 3 conjuntos de autoridades de certificación, que se utilizan para verificar la identidad del dispositivo con el que se comunica y, al mismo tiempo, cargar 3 certificados personales y claves privadas, que se utilizan para cifrar la comunicación.

Puede asignar uno de los conjuntos de certificados a cada servicio de dispositivo que requiera certificados, a saber [Servidor web \(p. 64\)](#). Los certificados pueden ser compartidos por varios servicios al mismo tiempo.

El dispositivo acepta certificados en formatos DER (ASN1) y PEM.

Cuando se conecta la alimentación al dispositivo por primera vez, se genera automáticamente un certificado autofirmado y una clave privada, que se pueden utilizar para el servicio del servidor web. sin tener que cargar su propio certificado y clave privada.





NOTA

Si se utiliza un certificado autofirmado para cifrar la comunicación entre el servidor web del dispositivo y el navegador, la comunicación es segura; sin embargo, el navegador advierte que no puede verificar la confiabilidad del certificado del dispositivo.

La descripción general actual de los certificados cargados de autoridades de certificación y certificados personales se muestra en dos pestañas: Certificados de autoridades de certificación (certificados CA) y Certificados personales.

Carga de certificado

1. Al presionar un botón  puede cargar el certificado desde la tienda al dispositivo.
2. Seleccione el archivo con el certificado (o clave privada) en la ventana de diálogo.
3. presiona el botón **Registro**.
4. Al presionar un botón  retire el certificado del dispositivo.


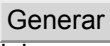



NOTA

- Se puede rechazar un certificado con una clave privada RSA de más de 2048 bits. En este caso, se muestra un mensaje:
“¡El dispositivo no aceptó el archivo de clave privada o la contraseña!”
- Cuando se utilizan certificados basados en curvas elípticas, solo se pueden utilizar curvas secp256r1 (también conocido como prime256v1, también conocido como NIST P-256) y secp384r1 (también conocido como NIST P-384).

Solapa CSR

Puede crear una solicitud de firma de certificado (CSR) personalizada en la interfaz de configuración web, que luego enviará a una autoridad de certificación (CA) para que la firme. Este proceso garantiza que el certificado se empareja correctamente con la clave privada que se generó al crear la CSR y permanece almacenada de forma segura únicamente en su dispositivo.

1. Para crear una nueva solicitud de certificado, haga clic en .
2. Aparecerá un cuadro de diálogo en el que deberá rellenar la siguiente información:
 - **Nombre común (CN)** - esta entrada debe contener la dirección IP o el nombre de dominio bajo el cual se puede acceder a la interfaz web del dispositivo 2N IP Intercom.
 - **SAN: mDNS:** activa la inclusión de **mDNS (DNS multidifusión)** como nombre de asunto alternativo (SAN) en el certificado. Se utiliza para acceder a través de un nombre de dominio en la red local.
 - **SAN: IP:** permite incluir la dirección IP como nombre alternativo del asunto (SAN) en el certificado. Se utiliza para el acceso a través de la dirección IP.
 - **Algoritmo de clave pública** - Especifica el tipo de algoritmo utilizado para generar la clave pública en el certificado.
 - **CSR ID** - identificador único de la solicitud de firma de certificado (CSR).
 - **Country (C)** - código de dos letras del país donde está registrada la organización (según ISO 3166-1 alfa-2).
 - **State/Country/Region (S)** - el estado o región donde está registrada la organización (no abreviado).
 - **City/Locality (L)** - el nombre de la ciudad o localidad donde está registrada la organización (no abreviado).
 - **Organization (O)** - el nombre legal de la organización, incluyendo cualquier sufijo como Inc., Corp., Ltd.
 - **Organizational Unit (OU)** - el nombre de un departamento o unidad dentro de una organización.
 - **Correo electrónico** - dirección de correo electrónico de la persona de contacto o gestor del certificado.
3. Haga clic en  para crear una solicitud de firma de certificado. Descargue el archivo CSR creado y guárdelo en un lugar seguro.
4. Envíe el archivo CSR creado a una autoridad de certificación (CA), que emitirá un certificado digital basado en él.
5. Vuelva a cargar el certificado digital emitido en el archivo CSR de la interfaz web. Para cargar, haga clic en  en la fila de la solicitud de certificación.

Pulse  para borrar el CSR. Pulse  para ver los parámetros del CSR.

Actualizar

Marcador My2N

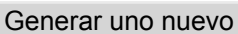
La plataforma en la nube My2N se utiliza para la gestión y configuración remota de dispositivos IP 2N y permite la conexión remota a la interfaz web del dispositivo.

My2N habilitado – permite la conexión al servicio My2N.

Código de seguridad My2N

Número de serie – muestra el número de serie del dispositivo para el cual el código My2N es válido.

Código de seguridad My2N – el código utilizado para agregar el dispositivo a My2N.

 – el Código de Seguridad My2N actual quedará invalidado y se generará uno nuevo.

Estado de conexión

Muestra información sobre el estado de conexión del dispositivo a My2N.

Identificación de My2N – identificador único de empresa creado mediante el portal My2N.

Marcador TR069

En esta pestaña se habilita y configura la gestión remota de dispositivos mediante el protocolo TR-069. El protocolo TR-069 le permite configurar de manera confiable los parámetros del dispositivo, restaurar y hacer una copia de seguridad de la configuración, o actualizar el firmware del dispositivo.

El servicio en la nube My2N utiliza el protocolo TR-069. Para que el dispositivo funcione correctamente con My2N, el servicio TR-069 debe estar habilitado y el parámetro Perfil Activo debe estar configurado en el valor My2N. Después de eso, el dispositivo iniciará sesión periódicamente en el servicio My2N, que podrá configurarlo.

Esta característica le permite conectar el dispositivo a su propio ACS (Servidor de configuración automática). En este caso, se desactivará la conexión al servicio My2N en el dispositivo.

My2N / TR069 habilitado – permite la conexión al servicio My2N, o otro servidor ACS.

Configuración general

Perfil activo – le permite seleccionar uno de los perfiles preestablecidos (del servidor ACS), o elija sus propios ajustes y configure la conexión al servidor ACS manualmente.

Otra sincronización para – muestra cuánto tiempo le tomará al dispositivo comunicarse con el servidor ACS remoto.

Estado de conexión – muestra el estado actual de la conexión al servidor ACS, o descripción de la condición de error.

Detalle del estado de la comunicación – código de error de comunicación del servidor o código de estado del protocolo HTTP.

Prueba de conexión – prueba la conexión al servicio TR069 según el perfil configurado, consulte Perfil activo. El resultado de la prueba se muestra en el campo Estado de la conexión.

Diagnóstico

Pestaña de diagnóstico

La interfaz le permite iniciar la captura de registros de diagnóstico, que luego se pueden descargar y enviar al soporte técnico. Los registros de diagnóstico capturados ayudan en la identificación y resolución de problemas informados. Los registros contienen información sobre el dispositivo, su configuración, tráfico de red, registro de fallos y estadísticas de memoria.

Paquete de diagnóstico

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 syslog– muestra si la captura de mensajes syslog está habilitada en la pestaña Syslog.

Estado de captura de los syslogs – muestra si está activada la captura de 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 comienza con el botón de grabación . Cuando vuelves a pulsar el botón de grabación  la captura se reinicia y comienza a ejecutarse de nuevo. El archivo con los paquetes capturados se puede

descargar con el botón . Un archivo de paquetes capturado contiene un archivo de configuración del dispositivo guardado

Para aumentar la seguridad, cifre el archivo con una contraseña. Esta contraseña será necesaria al restaurar la configuración para descifrar el archivo y acceder a su contenido. Asegúrese de no perder la contraseña y guárdela en un lugar seguro

La exportación del hash para la salida segura añade a los valores en el archivo de configuración su forma hash, tal como se inscriben en el syslog. La forma hash se añade a los valores como atributo **DiscreteHash**.



ATENCIÓN

- Al iniciar la captura de datos de diagnóstico se reinicia la captura de paquetes si ya se está ejecutando.
- Para aumentar la seguridad cifre el archivo con una contraseña. Esta contraseña será necesaria a la hora de restaurar la configuración para descifrar el archivo y acceder a su contenido. Asegúrese de no perder la contraseña y guárdela en un lugar seguro.

Herramientas




Verificar la disponibilidad de la dirección en la red – se utiliza para verificar la disponibilidad de una dirección determinada en la red como un comando **Ping** en sistemas operativos comunes. Después de presionar **Ping** Aparecerá un cuadro de diálogo en el que puede ingresar la dirección IP o el nombre de dominio y presionar **Ping** enviar datos de prueba a esta dirección. Si la dirección IP o el nombre de dominio ingresados no son válidos, se muestra una advertencia y **Ping** está inactivo hasta que la dirección ingresada sea válida. El cuadro de diálogo también muestra el estado de ejecución de la función y el resultado. El estado "Error" puede significar la falta de disponibilidad de la dirección ingresada dentro de los 10 segundos o la imposibilidad de traducir el nombre de dominio a la dirección. Si se recibe una respuesta válida, se muestra la dirección IP de la que provino la respuesta y el tiempo de espera para recibir una respuesta en milisegundos. Al presionar nuevamente **Ping** se envía otra consulta a la misma dirección.

Pestaña Captura de paquetes


En la pestaña Trace, es posible iniciar la captura de paquetes entrantes y salientes en la interfaz de red. Los paquetes capturados se pueden almacenar localmente en un búfer de 4 MB o de forma remota en la PC del usuario. El archivo con los paquetes capturados se puede descargar y procesar posteriormente, por ejemplo, utilizando la aplicación Wireshark (www.wireshark.org).


Captura de paquetes locales

Al capturar paquetes localmente, recomendamos reducir la velocidad de transmisión del flujo de video por debajo de 512 kbps. Una vez que se llena el búfer durante la captura local, los paquetes almacenados más antiguos se sobrescriben automáticamente.

1. Haga clic en para iniciar la captura de paquetes .
2. Para detener la captura, haga clic en .
3. Puede guardar el archivo del paquete capturado en el disco haciendo clic en .

Captura remota de paquetes

1. Haga clic en .
2. En la ventana que se abre, establezca el tiempo (en segundos) durante el cual se deben capturar los paquetes entrantes y salientes.

3. Haga clic en Aceptar para comenzar a capturar.
4. Seleccione una ubicación de disco para guardar el archivo del paquete capturado.
5. Puedes detener la captura haciendo clic en .

Pestaña de registro del sistema

Dispositivo **2N LiffIP 2.0** le permite enviar mensajes del sistema que contienen información importante sobre el estado y los procesos del dispositivo al servidor Syslog, donde estos mensajes pueden grabarse y usarse para análisis y auditoría adicionales del dispositivo monitoreado. En funcionamiento normal del dispositivo no es necesario configurar este servicio.

Datos sensibles, como códigos de acceso, identificadores de tarjetas, datos de inicio de sesión, etc., se almacenan en el syslog en forma cifrada (hash). La asignación de valores hash a valores reales se puede realizar según el archivo de configuración.



Configuración del servidor Syslog

Enviar mensajes Syslog – permite enviar mensajes del sistema al servidor Syslog. Se debe configurar una dirección de servidor válida para un funcionamiento adecuado.

Dirección del servidor – establece la dirección IP en el formato “IP[:puerto]” o la dirección MAC del servidor en el que se ejecuta la aplicación para registrar mensajes syslog.

El nivel de mensajes enviados. – establece el nivel de detalle de los mensajes enviados (Error, Advertencia, Aviso, Información, Depuración 1-3). Se recomienda el nivel de mensaje de depuración 1-3 solo para facilitar la localización del problema en el dispositivo requerido por el soporte técnico.

Mensajes de Syslog locales

Este bloque ofrece una descripción general de los mensajes Syslog locales. Se pueden cargar mensajes de syslog locales  y descargar .

Mantenimiento

Este menú se utiliza para mantener la configuración y el firmware del dispositivo. Le permite realizar una copia de seguridad y restaurar la configuración de todos los parámetros, actualizar el firmware del dispositivo o configurar todos los parámetros del dispositivo al estado predeterminado.

Configuración

Restaurar configuración – se utiliza para restaurar la configuración de una copia de seguridad anterior. Después de presionar el botón, aparecerá un cuadro de diálogo en el que se puede seleccionar el archivo de configuración y cargarlo en el dispositivo. Antes de cargar el archivo al dispositivo, es posible elegir si se deben aplicar la configuración de los parámetros de red y la configuración de conexión a la centralita SIP desde el archivo de configuración.

Al restaurar la configuración desde un archivo cifrado, debe introducir una contraseña para descifrarlo.



ATENCIÓN

El archivo de configuración tiene una contraseña de inicio de sesión almacenada. Si la contraseña del archivo no está cifrada o la contraseña predeterminada es 2n, solo se cargará la parte válida de la configuración. Esto significa que la configuración se cargará, pero la contraseña seguirá siendo original y no cambiará al valor especificado en el archivo.

Configuración de copia de seguridad – sirve para realizar una copia de seguridad de la configuración completa actual del dispositivo. Después de presionar el botón, se descargará la configuración completa, que se puede guardar en el almacenamiento.



ATENCIÓN

- La configuración del dispositivo puede contener información confidencial como números de teléfono de usuario y contraseñas de acceso, por lo que el archivo debe manejarse con cuidado.
- Para aumentar la seguridad, cifre el archivo con una contraseña. Esta contraseña será necesaria al restaurar la configuración para descifrar el archivo y acceder a su contenido. Asegúrese de no perder la contraseña y guárdela en un lugar seguro

Configuración predeterminada - se utiliza para restaurar todos los parámetros del dispositivo al estado por defecto. La restauración de los parámetros de red y de los ajustes del certificado requiere una confirmación adicional en el cuadro de diálogo de confirmación.

Sistema

Actualizar el firmware – se utiliza para cargar nuevo firmware al dispositivo. Después de presionar el botón, aparecerá un cuadro de diálogo en el que podrá seleccionar el archivo con el firmware destinado a su dispositivo. Una vez cargado correctamente el firmware, el dispositivo se reinicia automáticamente. Después de reiniciar, estará completamente disponible con el nuevo firmware. Todo el proceso de actualización lleva menos de un minuto. Puede obtener la versión actual del firmware para su dispositivo en 2N.com. La actualización del firmware no afecta la configuración. El dispositivo verifica el archivo de firmware y no permitirá cargar un archivo incorrecto o dañado.

Estado del firmware – muestra si hay una nueva versión de firmware disponible. Si no está disponible, se muestra **Controlar**, que se utiliza para comprobar en línea si hay disponible un firmware más reciente. Si está disponible, **Actualizar** el firmware se descarga después de presionar y luego actualiza automáticamente el dispositivo.

Notificar sobre versiones beta – marque la casilla para habilitar el seguimiento y también descargar la última versión beta del firmware.



NOTA

No hay una actualización automática del firmware en este dispositivo para garantizar un funcionamiento estable y evitar posibles problemas de compatibilidad con sistemas de terceros integrados en su entorno. Para garantizar la integridad del sistema y eliminar las fallas involuntarias, el usuario debe confirmar o iniciar manualmente todas las actualizaciones. Revise las notas de la nueva versión para verificar la compatibilidad con su infraestructura actual antes de realizar cualquier actualización.

Reanudar – reiniciará el dispositivo. Todo el proceso de reinicio tarda unos 30 segundos. Una vez completado el reinicio, cuando el dispositivo obtenga su propia dirección IP, aparecerá automáticamente una ventana de inicio de sesión.



ATENCIÓN

El registro del cambio de configuración del dispositivo se lleva a cabo en un intervalo de tiempo de 3 a 15 s, según el tamaño de la configuración en cuestión. No reinicie el dispositivo durante este tiempo

Licencias de bibliotecas de terceros – después de hacer clic en **Mostrar** Se abrirá un cuadro de diálogo con una lista de licencias utilizadas y bibliotecas de terceros. También incluye un enlace al documento EULA.

Estadísticas de uso

Envío de datos estadísticos anónimos – permite enviar datos estadísticos anónimos sobre el uso del dispositivo al fabricante. Estos datos no contienen ninguna información sensible como contraseñas, códigos de acceso o números de teléfono. 2N TELEKOMUNIKACE as utiliza esta información para mejorar la calidad, confiabilidad y rendimiento del software. La participación es voluntaria y el envío de datos estadísticos puede cancelarse en cualquier momento.

Puertos utilizados

Servicio	Puerto	Protocolo	Dirección	Ajustable	Ajustes
RTP	9 000			✓	Llamada > Ajustes generales
DHCP	68	UDP	In/Out	×	–
DNS	53	TCP/UDP	In/Out	×	–

Funciones y uso

En este capítulo están descritas las funciones básicas y de ampliación del producto **2N LiftIP 2.0**.

Descripción de la función

Esta sección está destinada a la resolución de problemas. Si el sistema no funciona correctamente y un técnico cualificado es capaz de seguir punto por punto el funcionamiento del sistema según esta descripción, se llegará a un punto en el que la descripción y la realidad divergen. A continuación, describe la discrepancia, lo que acelera enormemente la búsqueda de la causa. A menudo, este procedimiento también revela que el sistema funciona correctamente, pero el usuario tenía una idea diferente sobre su función.

Llamada saliente

El proceso se inicia con el botón ALARMA del anunciador (la entrada CANCELAR puede retrasar o bloquear la llamada). Tras pulsar el botón de ALARMA **2N LiftIP 2.0** establece una conexión con el centro de envío (para más detalles, consulte la opción automática). **2N LiftIP 2.0** reproduce el mensaje "Por favor, espere, estoy realizando una conexión" a la persona que se encuentra en el ascensor y la instrucción a la sala de control "Pulse 1 para confirmar" (si se utiliza la confirmación DTMF 1). La llamada debe confirmarse manual o automáticamente. La llamada es de duración limitada (mensaje de advertencia "Atención, se acerca el final de la llamada. Para prolongar la llamada, pulse 4."), pero puede prolongar la llamada. El control durante una llamada (marcación DTMF) se describe en el capítulo "Instrucciones de envío".



SUGERENCIA

Establezca destinos para las llamadas de alarma y otros para las llamadas de control y servicio.

Llamada de control

Una llamada de comprobación es una llamada saliente realizada automáticamente (normalmente cada 3 días) para comprobar el correcto funcionamiento del 2N LiftIP 2.0. El funcionamiento real es el mismo que para una llamada saliente. La diferencia es que se reproduce un mensaje diferente, por ejemplo "Esta es una llamada de comprobación", y se utiliza un conjunto diferente de números de teléfono (véase Llamadas de comprobación). La llamada de control permite el procesamiento automático. En caso de descolgado manual (confirmación 1 o descolgado de configuración), se reproducirá el mensaje de comprobación de llamada; en caso de procesamiento automático, no se reproducirá el mensaje.



SUGERENCIA

También es posible realizar la llamada de control manualmente. El tiempo de una llamada de control normal no se verá afectado.



AVISO

Si la memoria configurada para la llamada de comprobación está completamente vacía, no se realizará la llamada de comprobación, ni siquiera a la memoria configurada para la llamada de alarma.

llamada operativa

Una llamada operativa es una llamada realizada automáticamente tras uno de los eventos (botón atascado, fin de la liberación, error de audio, ...). Para los ajustes y una descripción más detallada, consulte [llamada operativa](#) (p. 58).

Llamada entrante

El despachador también puede llamar al número al que está conectado **2N LiftIP 2.0**, que recibirá automáticamente cualquier llamada entrante. La llamada entrante está limitada en el tiempo del mismo modo que la saliente y se controla de la misma manera (identificación de la extensión y del aparato).

A través de una llamada entrante podrá, por ejemplo, informar a una persona varada de cuándo llegará el servicio de rescate, etc. También puede comprobar a distancia que **2N LiftIP 2.0** está conectado y funciona.

Protección contra el arranque innecesario

Dado que el único propósito de **2N LiftIP 2.0** es pedir ayuda si alguien queda atrapado en la cabina del ascensor, la llamada puede considerarse innecesaria si la puerta de la cabina está abierta. Así, si el ascensor está equipado con un contacto de puerta, es posible conectar este contacto a la entrada **2N LiftIP 2.0** marcada como CANCELAR y programar el tiempo durante el cual **2N LiftIP 2.0** esperará tras pulsar el botón de ALARMA antes de establecer una conexión. Así, si alguien pulsa el botón de ALARMA por error, el ascensor llegará a una planta durante ese tiempo, la puerta se abrirá y la llamada se cancelará. También es posible fijar un tiempo mínimo para pulsar el botón, eliminando así la mayoría de los casos en los que alguien pulsa el botón por error.

Finalizar llamada (llamada saliente y entrante)

La terminación de la llamada (colgar) se produce por las siguientes razones:

- el otro lado (despacho) colgó;
- expira la duración máxima de llamada establecida - 10 segundos antes de que expire **2N LiftIP 2.0** reproduce el mensaje "Atención, se acerca el final de la llamada. Para prolongar la llamada, pulse 4.", la llamada puede prolongarse.

Instrucciones de envío

Control de marcación por tonos durante una llamada (DTMF)

Durante una llamada, puede utilizar la marcación por tonos para controlar el **2N LiftIP 2.0** durante una llamada (si se utiliza la marcación automática de confirmación) de acuerdo con la siguiente tabla. Los comandos 1 a 4 se enumeran en el orden en que se utilizan normalmente para facilitar su recuerdo.

Carácter DTMF	Descripción de la función
1	Confirmación por la que 2N LiftIP 2.0 sabe que la llamada se ha realizado correctamente. 2N LiftIP 2.0 silencia el mensaje que se está reproduciendo y envía su señal de confirmación, la llamada continúa hasta que expira el límite y se puede utilizar cualquiera de los siguientes comandos.
3	Para ver información sobre el comunicador.
4	Prolongación de la llamada - la llamada se prolonga 120 segundos, puede utilizarse repetidamente.

Resumen de los informes de 2N LiftIP 2.0

Informar	Importancia
"Espere, por favor, estoy haciendo una conexión".	El anuncio se reproduce para el usuario en la cabina del ascensor cuando se está estableciendo la llamada (antes de la confirmación).
"Esta es una llamada de socorro".	Suena hacia la sala de control antes de que se confirme la llamada.
"Esta es una llamada de control".	El mensaje sólo se transmite hacia la central (sólo para el acuse de recibo DTMF 1).
"Atención, nos acercamos al final de la llamada. Para prolongar la llamada, pulse 4".	Este mensaje, tanto en las llamadas salientes como en las entrantes, indica que la duración máxima de llamada establecida expirará en 10 segundos.
"Lo siento, su llamada debe ser desconectada".	El anuncio se reproduce para el usuario en la cabina del ascensor mientras la llamada está en curso.
"Fin de la llamada."	El mensaje se envía antes de que se cuelgue la llamada.
"El proceso de extricación se ha completado".	Acuse de recibo del fin de la señalización de emergencia.

Identificación 2N LiftIP 2.0


Tras confirmar la llamada de emergencia, el expedidor puede pulsar DTMF 3 y se reproduce el número de identificación del comunicador. También puede obtener información sobre el comunicador durante una llamada entrante.

Tipo de confirmación de llamada

Este ajuste se aplica a las llamadas de alarma, las llamadas de comprobación y los mensajes de avería.

Confirme pulsando 1

Se pueden almacenar hasta 4 números de teléfono y el número de repeticiones para las llamadas a la sala de control.

2N LiftIP 2.0 intenta entonces llamar uno a uno a todos los números almacenados. El criterio más fiable para confirmar el éxito de una conexión, **2N LiftIP 2.0** utiliza la marcación por tonos (DTMF). Cuando reciba una llamada manualmente, el expedidor deberá pulsar el botón  de su teléfono (en marcación por tonos). Si el número llamado está ocupado o si nadie responde al teléfono en el tiempo establecido o no acusa recibo de la llamada, **2N LiftIP 2.0** intenta llamar al siguiente número de la secuencia hasta agotar el número de intentos establecido para todos los números introducidos. La llamada de control o la notificación de averías es la misma, pero es posible utilizar un conjunto separado de 2 números.

Evaluar situaciones durante la elección con confirmación

Situación	2N LiftIP 2.0
Recibir una rescisión de la contraparte (Ocupado, Número no encontrado, etc.)	Marca inmediatamente el siguiente número.
Llamada	Espera durante un periodo de tiempo determinado.
Tono de llamada	Espera durante un periodo de tiempo determinado.
Carácter DTMF ¹	Confirma la recepción ("Conexión confirmada"), silencia el mensaje que se está reproduciendo y la llamada continúa durante el tiempo máximo establecido (tiempo máximo de llamada).
¹ ³ ⁴	Estos dígitos se interpretan como caracteres de control.

Confirmación por recogida

VOIP



ATENCIÓN

Una vez reproducido el mensaje, se confirma la llamada.

La persona llamada no tiene que pulsar ningún botón. Ambos modos tienen en común el conjunto de números, el número de ciclos y reaccionan de la misma manera ante las situaciones durante la marcación.



AVISO

Cuando utilice este modo, asegúrese de que ningún buzón de voz, fax u otro dispositivo descuelgue la llamada antes del número de timbres establecido. Esto pondría fin a la elección automática.

CPC (Antena y KONE)

Se utiliza cuando la contraparte dispone del SW necesario. Se envía una cadena DTMF cuando se descuelga la línea. El ascensor se identificará. Según el tipo de llamada, pasa a comunicación de voz (llamada de emergencia) o se confirma y finaliza automáticamente (llamada de verificación).

P100

Se utiliza cuando la contraparte dispone del SW necesario. Se envía un carácter DTMF cuando se descuelga la línea. El ascensor se identificará. Según el tipo de llamada, pasa a comunicación de voz (llamada de emergencia) o se confirma y finaliza automáticamente (llamada de verificación).

Autodetección del protocolo DTMF (CPC/P100)

El ascensor determina de qué protocolo se trata tras enviar la cadena DTMF y responde en consecuencia.



AVISO

- Si la llamada se ha dirigido, por ejemplo, a través de GSM, puede haber un problema con la detección de caracteres DTMF y **2N LiftIP 2.0** no es capaz de distinguir de qué protocolo se trata.
- Si se produce esta situación, le recomendamos que cambie el ajuste a CPC o P100 (3 ó 5).

CPC (Antena), P100 2N ext (sólo para llamadas de alarma)

Los protocolos funcionan igual que en 3 y 4 para CPC y 5 para P100. La única diferencia es que también se transmite el tipo de sílaba. Sólo se utiliza en llamadas de emergencia al comunicador.

Prueba auditiva de ortografía

La prueba de cabecera de audio permite la ejecución automática de la comprobación de audio. Establece un periodo de una vez al día o una vez a la semana a una hora seleccionada en el que la prueba debe realizarse periódicamente. Si la sílaba es correcta, se realizará la siguiente llamada de control. Si se detecta un error durante la prueba de audio, no se realizará la siguiente llamada de comprobación.

Evento tras error de audio

Es posible informar de una prueba de audio fallida mediante un evento. Los ajustes se realizan a través de la configuración del dispositivo basada en la web, consulte [llamada operativa \(p. 58\)](#). Se ejecuta un evento cuando se evalúa una prueba de audio defectuosa ([se configura mediante la llamada al servicio](#)).

- Llamada operativa: la llamada se establece a un número de destino almacenado para una llamada operativa.

Proceso de liberación y fin de la liberación

Activación del proceso de liberación

Si se establece una llamada de emergencia, el LED amarillo del altavoz permanecerá encendido una vez finalizada la llamada. Esto señala un proceso de liberación activo.

Finalización del proceso de liberación

El proceso de liberación puede finalizar llamando a **2N LiftIP 2.0** e introduciendo la contraseña (***password***) para confirmar el final del modo de liberación durante la llamada. O pulsando el botón ALARM2 de la cabina del ascensor.

Cuando el proceso de extricación haya finalizado, se anunciará "El proceso de extricación ha finalizado" desde el anunciador.

La configuración se realiza a través de la interfaz web, consulte [Modo de liberación](#).

Evento tras finalizar el proceso de liberación

Una vez completado el proceso de liberación, el evento puede ejecutarse. **2N LiftIP 2.0** sólo admite llamadas operativas.

- Llamada operativa - la llamada se establece a un número de destino almacenado para una llamada operativa

La configuración se realiza a través de la interfaz web del dispositivo, consulte [Llamadas de funcionamiento \(p. 58\)](#).

Protocolos CPC y P100

CPC

El protocolo CPC admite 3 variantes: **KONE**, **Antena** y **Antena 2N Ext.**

El mensaje de datos consta de:

Comando - Tipo de llamada - DATOS - ID

CPC

Tipo de llamada	Dominio	Tipo de llamada	Datos	ID
Alarm	04	10	000000000000	número de identificación del ascensor
Alarm 2	04	10	000000000000	número de identificación del ascensor
llamada de control	04	21	000000000000	número de identificación del ascensor
Proceso de autorización completado	04	84	000000000000	número de identificación del ascensor
Fallo del botón	04	90	000000000000	número de identificación del ascensor
Corrección del botón	04	90	000000000001	número de identificación del ascensor

Tipo de llamada	Dominio	Tipo de llamada	Datos	ID
Fallo del audio	04	91	000000000000	número de identificación del ascensor
Corrección del audio	04	91	000000000001	número de identificación del ascensor



AVISO

Esto es sólo una parte del mensaje de datos. No contiene un principio, una suma de comprobación y un final.

0490000000000000187654321 - Botón corregido, número de identificación 87654321.

El mensaje de datos consta de:

Comando - Tipo de llamada - ID

CPC Antenna

Tipo de llamada	Dominio	Tipo de llamada	Datos	ID
Alarm	04	27	-	número de identificación del ascensor
Alarm 2	04	27	-	número de identificación del ascensor
llamada de control	04	26	-	número de identificación del ascensor
Proceso de autorización completado	04	84	-	número de identificación del ascensor

Tipo de llamada	Dominio	Tipo de llamada	Datos	ID
Fallo del botón	04	90	-	número de identificación del ascensor
Corrección del botón	04	90	-	número de identificación del ascensor
Fallo del audio	04	91	-	número de identificación del ascensor
Corrección del audio	04	91	-	número de identificación del ascensor



AVISO

Esto es sólo una parte del mensaje de datos. No contiene un principio, una suma de comprobación y un final.

0492687654321 - Llamada de control, número de identificación 87654321.

El mensaje de datos consta de:

Comando - Tipo de llamada - DATOS - ID

CPC Antenna 2N Ext

Tipo de llamada	Dominio	Tipo de llamada	Datos	ID
Alarm	04	27	00000	número de identificación del ascensor
Alarm 2	04	27	00000	número de identificación del ascensor

Tipo de llamada	Dominio	Tipo de llamada	Datos	ID
llamada de control	04	26	00000	número de identificación del ascensor
Proceso de autorización completado	04	84	00000	número de identificación del ascensor
Fallo del botón	04	90	00000	número de identificación del ascensor
Corrección del botón	04	90	00001	número de identificación del ascensor
Fallo del audio	04	91	00000	número de identificación del ascensor
Corrección del audio	04	91	00001	número de identificación del ascensor



AVISO

Esto es sólo una parte del mensaje de datos. No contiene un principio, una suma de comprobación y un final.

04910000087654321 - Error de audio, ID 87654321.



ATENCIÓN

- La información Botón corregido y Audio corregido sólo puede transmitirse utilizando el protocolo 2N Ext.
- Si el modo 2N Ext no está configurado, no se establecerá la llamada de servicio.
- El protocolo CPC utiliza hasta 16 dígitos para el número de identificación del ascensor, el protocolo P100 sólo utiliza 8 dígitos.

P100

El mensaje de datos consta de:

Tipo de llamada - ID - DATA

P100

Tipo de llamada	Tipo de llamada	ID	DATOS
Alarm	1	número de identificación del ascensor	
Alarm 2	1	número de identificación del ascensor	
llamada de control	3	número de identificación del ascensor	
Proceso de autorización completado	2	número de identificación del ascensor	500
Fallo del botón	2	número de identificación del ascensor	800
Corrección del botón	2	número de identificación del ascensor	801
Fallo del audio	2	número de identificación del ascensor	200
Corrección del audio	2	número de identificación del ascensor	201



AVISO

Esto es sólo una parte del mensaje de datos. No contiene un principio, una suma de comprobación y un final.

287654321500 - Proceso de alta completado, número de identificación 87654321.

Pruebas funcionales conforme a la norma EN 81-28

Este capítulo describe los procedimientos para verificar el funcionamiento del sistema de señalización de emergencia ALARM en un ascensor con cabina **2N LiftIP 2.0** de acuerdo con los requisitos de la norma EN 81-28. Deben realizarse pruebas antes de poner en funcionamiento la grúa y periódicamente como parte del mantenimiento.

Preparación

1. Abra la interfaz de configuración del dispositivo basada en la web **2N LiftIP 2.0**.
2. Vaya a **Llamada > Llamada de Alarma** y verifique los siguientes ajustes:
 - La función de llamada retardada está activada.
 - La función **Alarma de prueba** está activada y la duración de la pulsación del botón para activar la alarma de prueba está fijada en 30 segundos.
3. Vaya a **Servicios > Ascensor** y verifique los siguientes ajustes:
 - **El modo de descarga** está activado.
 - Si **Salir introduciendo la contraseña** está activada, anote la contraseña.

6.2.2 Información de señalización de emergencia ALARMA (4.1.2)

1. Mantenga pulsado el botón ALARMA con el símbolo de la campana durante el tiempo necesario para activar la alarma de prueba (mín. 30 segundos).
2. Compruebe que el LED amarillo se ilumina y suena el pitido.
3. Cuando la llamada esté conectada al servicio de rescate, asegúrese de que el LED verde empieza a parpadear.
4. Verifique la comunicación bidireccional con el servicio de salvamento.

6.2.3 Fin de la señalización de emergencia ALARMA (4.1.3)

1. Siga los pasos de la prueba [6.2.2 Información de señalización de emergencia ALARMA \(4.1.2\) \(p. 87\)](#).
2. Llame al servicio de rescate para finalizar la llamada.
3. Compruebe que el LED verde deja de encenderse cuando finaliza la llamada. El LED amarillo permanece encendido.
4. Salga del modo de desbloqueo.

Salir con el botón 2

- a. Pulse el botón 2 durante 3 segundos.
El botón 2 es un botón externo enchufado en el conector de la bocina etiquetado como ALARMA 2; la ubicación la determina el instalador.

Salir introduciendo una contraseña







- a. Llame a **2N LiftIP 2.0** - marque **2N LiftIP 2.0**.
 - b. Introduzca la contraseña de desbloqueo y confírmela con un asterisco.
5. Compruebe que el LED amarillo ha dejado de iluminarse.

6.2.4 Suministro eléctrico de emergencia (4.1.4)

Los informes de **2N LiftIP 2.0** no disponen de su propia fuente de alimentación de emergencia. Su funcionamiento durante el suministro de energía de emergencia debe verificarse en la pasarela/elemento que suministra energía de emergencia al sistema de comunicación de emergencia.

6.2.5 Señales visuales y acústicas en la jaula del ascensor (4.1.5)

Para algunos anuncios, los LED externos se dirigen hacia el interior de la cabina del ascensor. El instalador es responsable de su colocación. Compruebe que los LED externos están guiados hacia la cabina del ascensor.

Informe	Conectar una llamada	Llamada en progreso	Modo de desbloqueo activo	Salir del modo de recuperación
921618B, 2N LiftIP 2.0 COP unit – Flush mounting, EN, With button	LED amarillo  + alarma acústica	LED amarillo  + LED verde intermitente	LED amarillo 	no se enciende ningún LED
921618 2N LiftIP 2.0 COP unit – Flush mounting, Without button	LED amarillo  + alarma acústica	LED amarillo  + LED verde intermitente	LED amarillo 	no se enciende ningún LED

6.2.6 Comunicación (4.1.8), verificación de la señalización de emergencia ALARMA (4.1.6), identificación (4.1.7)

Respuesta de comunicación

1. Asegúrese de que las puertas del ascensor no están completamente abiertas.
2. Pulse el botón ALARMA con el símbolo de la campana durante el tiempo que esté pulsado el botón ALARMA (parámetro 962).
3. Compruebe que el LED amarillo se ilumina y suena el pitido.
4. Cuando la llamada esté conectada al servicio de rescate, asegúrese de que el LED verde empieza a parpadear.
5. Verifique la comunicación bidireccional con el servicio de salvamento.

Comprobación y reinicio de la ALARMA

1. Asegúrese de que las puertas del ascensor no están completamente abiertas.
2. Pulse el botón ALARMA con el símbolo de la campana durante el tiempo que esté pulsado el botón ALARMA (parámetro 962).
3. Compruebe que el LED amarillo se ilumina y suena el pitido.
4. Cuando la llamada esté conectada al servicio de rescate, asegúrese de que el LED verde empieza a parpadear.
5. Verifique la comunicación bidireccional con el servicio de salvamento.
6. Llame al servicio de rescate para finalizar la llamada.
7. Compruebe que el LED verde deja de encenderse cuando finaliza la llamada. El LED amarillo permanece encendido.
8. Pulse brevemente el botón ALARMA.
9. Asegúrese de que suena una señal acústica para indicar que se está conectando la llamada. El sistema debe establecer una conexión inmediatamente después de una pulsación corta.
10. Cuando la llamada esté conectada al servicio de rescate, asegúrese de que el LED verde empieza a parpadear.

Es necesario verificar que el dispositivo está correctamente identificado en el lado del dispositivo receptor. Los equipos receptores no están en la cartera de **2N LiftIP 2.0**.

Accesibilidad y fiabilidad (4.2.1)

Comunicación cuando el equipo receptor principal no está disponible y es necesario verificar los registros de las autocomprobaciones (llamadas de servicio) en el equipo receptor. Los equipos receptores no están en la cartera de **2N LiftIP 2.0**.

Parámetros técnicos

Parámetros eléctricos

Tensión de alimentación 10-30 V CC (debe mantener la polaridad) o 48 V PoE 802.3af

Consumo: máx. 2 W con reproductor integrado, máx. 3,5 W con reproductor con impedancia de 4 Ω conectado

Rango de tensión para las entradas de ALARMA y CANCELACIÓN

Entradas: 5-48 V CC (debe mantenerse la polaridad)

Parámetros de audio

Reproductor: integrado 16 Ω / 1 W (potencia de salida 0,45 W)
Opción de aumentar la potencia de salida a 0,75 W conectando un altavoz de 4 Ω

Micrófono: integrado, posibilidad de conectar un micrófono electret externo

Conmutación de voz: Procesador de audio full dúplex

Salida para bucle de inducción: 3,35 V RMS, impedancia de salida de 100 Ω

Códec: PCMU, PCMA, G.711 (aprox. 90 kbit/s), L16, G.722 y G.729

Conexión de elementos indicadores externos

Tensión: 10-30 V CC, fuente de alimentación externa

Corriente máxima: 200 mA (al utilizar bombilla máx. 100 mA)

Parámetros técnicos

Resto de parámetros

Dimensiones: (An) 65 x (Al) 130 x (Pr) 23 mm

Rango de temperatura de trabajo: -20 a 50°C

Humedad relativa de funcionamiento: 10 a 90% sin condensación

Altitud recomendada: 0 – 2000 m



2N LiftIP 2.0 – Manual de usuario

© 2N Telekomunikace a. s., 2026

2N.com