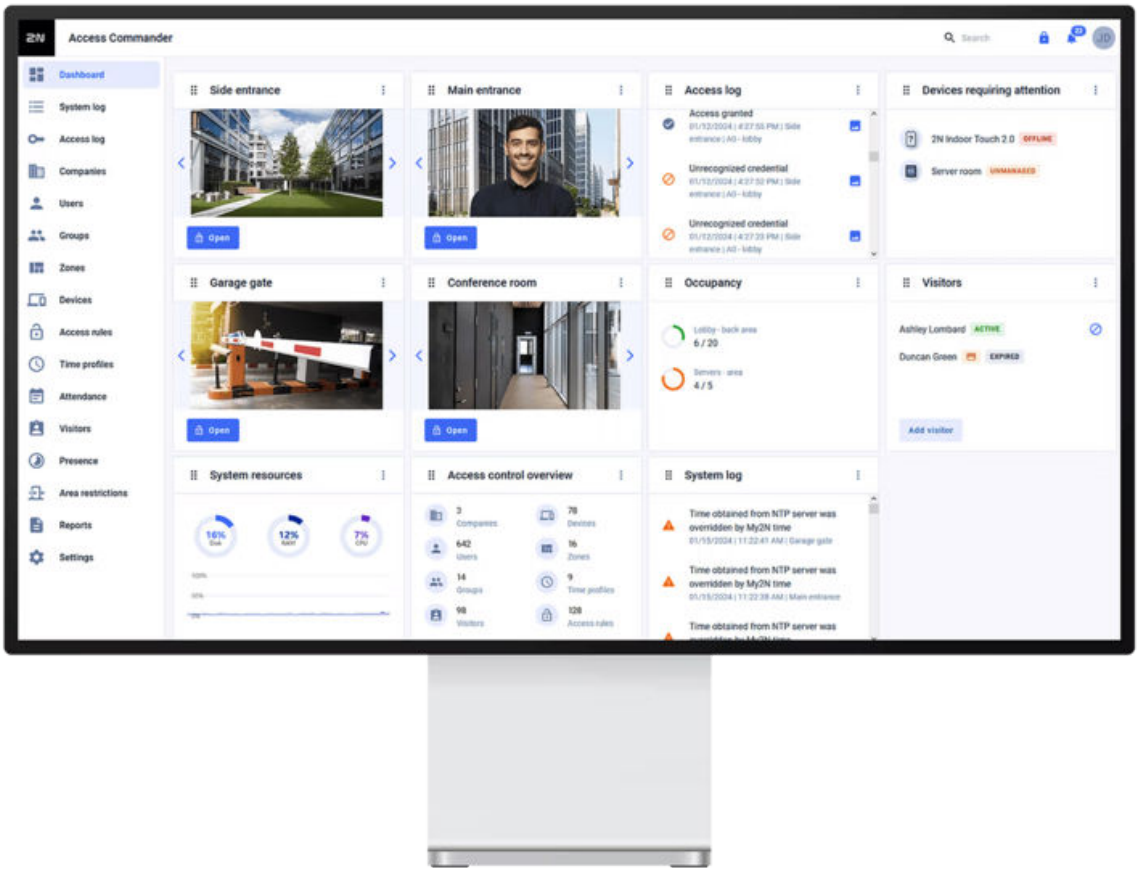
2N Access Commander

Manual de instalación



2N TELEKOMUNIKACE a.s.
Modřanská 621 | Prague 4 | 143 01

2N.com

Tabla de contenidos

Símbolos y términos utilizados.

Los siguientes símbolos y pictogramas se utilizan en el manual:

PELIGRO
Siga siempre las recomendaciones aquí descritas para evitar daños personales.

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

ATENCIÓN
Información importante para el correcto funcionamiento del sistema.

SUGERENCIA
Información útil para la funcionalidad rápida y eficiente.

NOTA
Procedimientos y consejos para el uso efectivo de las funciones del dispositivo.

información general

2N Access Commander es una herramienta de software para la gestión de sistemas de acceso masivo. Interfaz Access Commander es accesible a través de un navegador web.

Los ajustes se pueden realizar dentro de una instalación **Access Commander** dividir en **Compañías**, que se gestionan por separado. Este método permite dividir la administración entre administradores en empresas individuales. Un administrador de una empresa no tiene acceso a la información de otra empresa. Los administradores de una empresa no verán a los usuarios de otra empresa.

Para gestionar el acceso, debe añadir el dispositivo a **Access Commander. Los dispositivos son unidades físicas del edificio que controlan las entradas (2N interfonos,**

Se pueden compartir zonas o instalaciones entre empresas, permitiendo gestionar el acceso de la empresa a zonas comunes (entradas, restaurantes, salas de conferencias...).

Usuarios Son personas individuales cuyo movimiento por el edificio debe gestionarse o a las que se puede llamar desde dispositivos conectados. Los usuarios se agrupan en **Grupos**, en el que se realiza una gestión masiva de su acceso a las zonas. El usuario se autentica en el dispositivo y luego el dispositivo evalúa si el usuario tiene acceso válido al dispositivo. La validez del acceso se rige por **Derechos de acceso**. Los usuarios seleccionados también pueden tener permisos administrativos. **Access Commander** o partes del mismo.

Perfiles de tiempo establecen los horarios en los que el dispositivo permite el acceso o en los que se puede llamar a los usuarios.

Módulo de asistencia permite el seguimiento de la asistencia de los usuarios.

Módulo de presencia le permite rastrear en qué zonas se encuentran actualmente los usuarios.

Visitas son personas cuyos derechos de acceso sólo son válidos por un tiempo limitado.

Permisos de usuario

Informe en **Access Commander** Puede ser realizado por varios usuarios dependiendo de los permisos que se les asignen.

Las cuentas elevadas se configuran a través de una función en la configuración del usuario. Se pueden asignar varios roles a un usuario.

NOTA
Los permisos de usuario se aplican a la gestión dentro de la empresa del usuario. El administrador tiene acceso a la gestión completa de todas las empresas.

Administrador

- Configuración del sistema y de los módulos individuales según la licencia válida.
- Cambio de licencia
- Todos los permisos de otros roles aplicables a todas las empresas.

Administrador de acceso

- Crear y gestionar grupos.
- Gestionar las membresías de sus grupos.
- Crear y gestionar visitas.
- Creación y gestión de perfiles horarios.
- Establecer reglas de acceso.

Administrador de usuarios

- Crear y administrar usuarios.
- Crear y gestionar visitas.
- Gestionar las membresías de sus grupos.
- Visualización del registro de acceso y del sistema.

Gestor de visitas

- Crear y gestionar visitas.
- Administre sus membresías grupales (no disponible en la interfaz simplificada).
- Visualización del registro de acceso de visitas (no disponible en la interfaz simplificada).

Gerente de puerta

- Monitoreo de la transmisión de la cámara desde los dispositivos asignados.
- Apertura remota de dispositivos asignados.
- Bloqueo de emergencia de los dispositivos asignados.
- Ver el registro de acceso de los dispositivos asignados.
- Monitoreo de estados y eventos de seguridad en el log del sistema.

gerente de asistencia

- Seguimiento y gestión de la asistencia de los grupos asignados.
- Visualización del registro de acceso de los usuarios de los grupos asignados.

Administrador de empresa

- Establecer el idioma por defecto de la empresa.
- Supervisión del registro del sistema (limitada a los eventos de la empresa).
- La posibilidad de configurar un widget para el registro del sistema y la función de bloqueo de emergencia en los dispositivos utilizados por la empresa (incluidos los dispositivos compartidos con otras empresas).

Dispositivos y aplicaciones compatibles

Este capítulo enumera los dispositivos compatibles, los navegadores web compatibles y las plataformas de virtualización compatibles a través de las cuales se puede instalar Access Commander.

Dispositivos soportados

A continuación se muestra una descripción general de los dispositivos compatibles con el sistema de acceso Access Commander. Estos dispositivos se pueden gestionar en el sistema.

NOTA
Las versiones de firmware compatibles con estos dispositivos se enumeran en el capítulo firmware (p. 68).

Intercomunicadores 2N

- 2N Style IP: admite lectura de códigos QR
- 2N IP Verso 2.0: admite lectura de códigos QR
- 2N IP Force 2.0: admite lectura de códigos QR
- 2N IP Verso
- 2N LTE Verso
- 2N IP One
- 2N IP Force
- 2N IP Safety
- 2N IP Vario
- 2N IP Base
- 2N IP Solo
- 2N IP Uni
- 2N IP Video Kit
- 2N IP Audio Kit
- 2N IP Audio Kit Lite

Unidades de acceso 2N

- Access Unit QR: admite la lectura de códigos QR
- 2N Access Unit 2.0
- 2N Access Unit
- 2N Access Unit M

Cerraduras electrónicas 2N

- 2N Fortis Handle
- 2N Fortis Cylinder

Unidades de respuesta 2N

- 2N Indoor View (Wi-Fi)
- 2N Indoor Compact
- 2N Indoor Talk
- 2N Indoor Touch 2.0
- 2N Clip
- 2N Clip 2wire-IP

navegadores web

Configuración **Access Commander** se realiza a través de la interfaz web. El sistema ha sido optimizado para el navegador Google Chrome (versión 90 y superior).

Otros navegadores compatibles:

- Mozilla Firefox (versión 78 y superior)
- Microsoft Edge (versión 91 y superior)
- Safari (versión 35 y superior)

Otros navegadores no han sido probados, por lo que no se puede garantizar su funcionalidad completa.

Plataformas de virtualización

- Virtual Box
- VMware Player (versión 6.5 y superior)

- VMware vSphere (versión 6.5 y superior)
- Hyper-V

Puertos utilizados

Lista de servicios y puertos requeridos

Servicio	Puerto
HTTP/HTTPS[a.]	80/443
SMTP	225
DHCP	68
DNS	53
NTP	123
LDAP[b.]	389
SSH	22

[a.] Se utiliza tanto para la comunicación con el cliente como para la comunicación con los gatekeepers.

[b.] El usuario puede en la configuración **Access Commander** elija un puerto diferente para el servicio LDAP.

Resumen de licencias

Después de la instalación inicial **Access Commander** Hay una licencia de prueba disponible. La licencia de prueba le permite probar todas las funciones en la gestión de 1 dispositivo y 5 usuarios. Para una administración completa, necesita activar una de las cuatro licencias: *Básico* (gratis), *Avanzado*, *Para* o *Para ilimitado*.

Licencia:	Trial	Basic	Advanced	Pro	Unlimited
2N Nº de referencia	n/a	n/a	91379031	91379032	91379033
Axis Nº de referencia	n/a	n/a	02309-001	02310-001	02311-001
Número máximo de usuarios	5	50	300	1000	Ilimitado[a.]
Número máximo de dispositivos (tanto activados como desactivados)	1	5	30	100	Ilimitado

Licencia:	Trial	Basic	Advanced	Pro	Unlimited
2N Nº de referencia	n/a	n/a	91379031	91379032	91379033
Axis Nº de referencia	n/a	n/a	02309-001	02310-001	02311-001
Número máximo de administrado-res/gerentes	5	1	5	1000	Ilimitado
Registros de acceso y del sistema	✓	✓	✓	✓	✓
Reglas de acceso	✓	✓	✓	✓	✓
Gestión de API	✓	✓	✓	✓	✓
Activación/desactivación de cuenta	✓	✓	✓	✓	✓
Limitar el número de accesos falli-dos	✓	✓	✓	✓	✓
alarma silenciosa	✓	✓	✓	✓	✓
código de zona	✓	✓	✓	✓	✓
Monitoreo de dispositivos	✓	✓	✓	✓	✓
Gestión de registros	✓	✓	✓	✓	✓
Gestión de cerraduras electrónicas	✓	✓	✓	✓	✓
Importar usuarios desde CSV o des-de dispositivos	✓	×	✓	✓	✓
Gestión masiva de firmware	✓	×	✓	✓	✓
Autenticación múltiple	✓	×	✓	✓	✓
Autorización de usuario	✓	×	✓	✓	✓

Licencia:	Trial	Basic	Advanced	Pro	Unlimited
2N Nº de referencia	n/a	n/a	91379031	91379032	91379033
Axis Nº de referencia	n/a	n/a	02309-001	02310-001	02311-001
Notificación	✓	×	✓	✓	✓
Presencia	✓	×	✓	✓	✓
Claves de acceso API	✓	×	✓	✓	✓
Registros de cámara	✓	×	✓	✓	✓
control de ascensor	✓	×	✓	✓	✓
Panel	✓	×	✓	✓	✓
Bloqueo de emergencia	✓	×	✓	✓	✓
Soporte de credenciales móviles	✓	×	✓	✓	✓
Gestión de visitas	✓	×	✓	✓	✓
Automatización	✓	×	✓	✓	✓
Gestión de ocupación	✓	×	×	✓	✓
Sincronización (LDAP y CSV)	✓	×	×	✓	✓
Anti-passback	✓	×	×	✓	✓
Asistencia	✓	Opcio-nal	Opcional	Opcional	Opcional

[a] Ilimitado dentro de las capacidades máximas de la plataforma de software, a saber Hardware recomendado de la máquina virtual (p. 20)

Instalación

Access Commander Se puede distribuir de dos formas:

- Ordenador de sobremesa pequeño 2N Access Commander Box 2.0 (Nº de pedido 1120120xx; Nº de pieza Axis 03129-00)
- computadora virtual

Solución Access Commander Boxestá limitado a 2000 dispositivos conectados. Otras características del software son idénticas para ambas soluciones.

Distribución a través de Access Commander Box

Access Commander Box 2.0 (1120120xx, 03129-00) es un miniordenador de sobremesa compacto con software preinstalado. Se trata de una solución "plug and play" en la que basta con conectar una fuente de alimentación y un cable Ethernet a este miniordenador. Para un funcionamiento correcto y completo del sistema, se recomienda colocar este miniordenador en un lugar seguro y dejarlo funcionar permanentemente. Access Commander Box 2.0 sirve como servidor para recopilar datos, eventos y registros de todo el sistema de control de accesos.

Recomendamos no exceder la cantidad de 1500 usuarios en el grupo. Si hay restricciones para áreas, como anti-passback o control de ocupación para una gran cantidad de usuarios, la aplicación puede ralentizarse.

Iniciar sesión en Access Commander con una dirección IP dinámica

1. Conectar Access Commander Box a la red mediante un cable Ethernet.
2. Utilice 2N IP Network Scanner y Axis IP Utility para localizar Access Commander Box en la red.
3. En su navegador web, vaya a la dirección IP Access Commander Box e iniciar sesión en **Access Commander**.
   La contraseña predeterminada del usuario administrador es 2n y debe cambiarse después de iniciar sesión.

> **NOTA**
> En caso de distribución a través de Access Commander Box conectarse a la interfaz web desde otra computadora en la red. Sistema operativo Access Commander Box asegura el funcionamiento **Access Commander** y su configuración básica de Linux no permite que se ejecute el navegador web.

Configuración de una dirección estática en la Access Commander Box conectándose directamente al ordenador

1. Conecte la Access Commander Box directamente a su ordenador mediante un cable de red.
2. Después de aproximadamente **15 segundos** establecerá automáticamente la dirección link-local.
3. Abra **accesscommander.local** en su navegador.
   Como alternativa, puede utilizar 2N IP Network Scannder o Axis IP Utility para localizar el dispositivo aunque no haya recibido una dirección IP a través de DHCP.
4. En la interfaz web, configure una dirección estática según sea necesario.

Configuración de una dirección estática de Access Commander en el Access Commander Box

1. Conectar Access Commander Box a la red mediante un cable Ethernet.
2. Conectar a Access Commander Box teclado y monitor. Aparece una pantalla negra.
3. Acceda al sistema como “root” con la contraseña “2n”. Cuando aparezca la pantalla azul, cambie la contraseña por defecto.
4. En el Menú Avanzado, seleccione “Networking” y después “Static IP”.
5. Configure la dirección IP estática, la puerta de enlace y el DNS.
6. Guarde esta configuración y utilice cerrar sesión para salir del menú de la consola.
7. Conéctese a la dirección IP configurada a través de un navegador web.

SUGERENCIA
Conectarse directamente al ordenador y utilizar la dirección **accesscommander.local** es la forma recomendada y más sencilla de configurar una dirección estática en la Access Commander Box.

NOTA
El número de serie que aparece en 2N Network Scanner o Axis IP Utility puede diferir del número de serie que aparece en la etiqueta de Access Commander Box.

Fortis Commander

Fortis Commander es una aplicación independiente que conecta las cerraduras electrónicas **Fortis** al sistema **Access Commander**. La aplicación establece los bloqueos de acuerdo con el archivo de proyecto creado en **Access Commander**u que contiene la configuración de los bloqueos. El archivo está encriptado y sólo puede utilizarse en una instalación específica.

Instalación

Fortis Commander está diseñado para instalarse en un ordenador Windows compatible con Bluetooth Low Energy (BLE).

Encontrará la aplicación en la página web 2N Download Centre.

Procedimiento de instalación

1. Descargue el paquete de instalación desde el enlace proporcionado.
2. Ejecute el instalador y complete la instalación siguiendo las instrucciones en pantalla.

Archivo del proyecto

El archivo del proyecto se crea en **Access Commander** y contiene la configuración completa del proyecto. El archivo está encriptado y protegido por contraseña.

Establecer bloqueos en Access Commander

Antes de cargar llaves en cerraduras individuales, debe emparejar **Access Commander** con **Fortis Commander**.

Generación de la clave maestra de cifrado (MEK) y preparación del proyecto

1. Inicie sesión en Access Commander.
2. Vaya a **Configuración > Cerraduras electrónicas**.
3. En la pestaña **Configuración inicial** haga clic en Generar claves.
4. Cree la clave de cifrado maestra.

ATENCIÓN
La clave de cifrado maestra no se puede ver ni modificar posteriormente .

NOTA
En función de la clave maestra de cifrado (MEK), **2N Access Commander** genera un conjunto de claves de cifrado. Por lo tanto, la clave debe ser única y suficientemente segura. El conjunto de claves se basa en la clave de cifrado maestra, por lo que los proyectos con la misma clave de cifrado maestra generan los mismos conjuntos de claves. Si se pierde un proyecto, se puede crear uno nuevo con la misma clave maestra de encriptación y continuar con la encriptación.

5. Tras generar las claves y establecer la contraseña del archivo de proyecto, puede descargar **el archivo de proyecto**, que es una imagen de la configuración de la cerradura electrónica en el sistema **Access Commander**.
6. En la pestaña **de Fortis Commander** haga clic en Descargar aplicación**,** desde donde se iniciará la descarga de **Fortis Commander** (aplicación para configurar cerraduras electrónicas).

ATENCIÓN
La información sobre el proyecto es confidencial. Protéjalos contra cualquier uso indebido.

Configuración de la cerradura electrónica mediante Fortis Commander

1. Instale **Fortis Commander** y ábralo.
2. Haga clic en Abrir proyecto y abra el archivo del proyecto descargado en el Explorador de archivos.
3. En el cuadro de diálogo que aparece, introduzca la contraseña del archivo de proyecto.
4. Tras abrir el archivo del proyecto, seleccione Conectar al dispositivo y conecte la tarjeta de servicio a la cerradura.
5. Haga clic en **Asignar**, que asigna el bloqueo al proyecto.
6. Desconecte el dispositivo y haga clic en **Archivo > Cerrar proyecto**.
7. Una vez finalizada la configuración, abra el sistema **Access Commander**. Vaya a la pestaña **Configuración > Cerraduras electrónicas** y haga clic de nuevo en Fortis Commander. Cargue el archivo de proyecto.

NOTA
Cuando traslade la cerradura de una instalación a otra o cuando realice una reclamación, deberá realizar un restablecimiento de fábrica . Esta operación restablece la cerradura a los ajustes de fábrica y elimina toda la configuración anterior.

Procedimiento de actualización de la configuración

1. Realice cambios en **Access Commander**.
2. Descargue el archivo del nuevo proyecto.
3. Cargue el archivo en **Fortis Commander** y realice los cambios necesarios en las cerraduras.
4. Si realiza otros cambios en **Access Commander**u, descargue siempre un nuevo archivo de proyecto.

ATENCIÓN
Para cada cambio de configuración en **Access Commander**u debe descargar un nuevo archivo de proyecto - no puede utilizar un archivo más antiguo que ya se haya cargado en **Fortis Commander**.

Bloqueo y desbloqueo permanentes

La aplicación le permite bloquear y desbloquear la cerradura de forma permanente. La función se utiliza para intervenciones de servicio o control de emergencia sin necesidad de utilizar una tarjeta.

Recogida de eventos de cerraduras electrónicas mediante tarjetas / chips RFID

Ajustes de recogida de eventos

1. Abra **Configuración > Cerraduras electrónicas > Eventos de pestañas**.
2. Seleccione el tipo de evento:
   - **Recopilar eventos de acceso y del sistema** - Todos los eventos de acceso y del sistema se registran en la tarjeta/chip y se escriben en el registro del sistema y en el registro de acceso .
   - **Recoger sólo los eventos del sistema** - sólo se registran los eventos del sistema, los eventos de acceso no se almacenan en las tarjetas.
   - **No recoja eventos en las pestañas** - no se escribe ningún evento en la pestaña; sólo se puede acceder a ellos a través de **Fortis Commander**u.

SUGERENCIA
Seleccionando del conjunto de eventos adecuado, puede reducir la carga del sistema y el uso del almacenamiento Sin embargo, el registro detallado es importante para el diagnóstico y las auditorías de seguridad.

Exportar eventos de una tarjeta

La tarjeta almacena un máximo de **16 primeros eventos**. Los eventos pueden leerse de dos maneras:

- En **Access Commander**, haga clic en el icono del cuadro de búsqueda de la cabecera y cargue la pestaña.
- Utilizando un dispositivo con **2N OS**, los eventos se leen de la tarjeta y se envían a **Access Commander**u.

Carga de eventos en la cerradura

1. Abra **Configuración > Cerraduras electrónicas > Fortis Commander** y haga clic en Descargar archivo.
2. Abra el archivo en **Fortis Commander**.
3. En la aplicación **Fortis Commander**, conéctese a la cerradura electrónica.
4. Vuelva a cargar el archivo actualizado en **Access Commander**.

5. Una vez cargados, los eventos se muestran en **Registros de acceso** y **Registros del sistema**.

Operaciones de servicio

Estas operaciones están disponibles para **Cilindro Fortis**:

- **Desmontaje** - desmontaje de cerraduras con fines de servicio.
- **Sustitución de la pila** - Sustitución de la pila de la cerradura.

ATENCIÓN
Las operaciones de servicio no son relevantes para otros tipos de esclusas.

NOTA
Desde el modo de servicio, la cerradura vuelve al modo normal pulsando el botón Lock para bloquearse permanentemente.

Distribución a través de máquina virtual.

Access Commander puede distribuirse como una máquina virtual. A continuación se indican los procedimientos de instalación en las plataformas de virtualización compatibles.

Virtual Box

SUGERENCIA
Se recomienda habilitar la tecnología de virtualización VT-X en BIOS.

1. Descarga la última versión de VirtualBox desde https://www.virtualbox.org/wiki/Downloads.
   Se recomienda descargar la versión que incluye el paquete de extensión de VirtualBox.
2. Descargue el software apropiado desde la sección Soporte > Centro de descargas > Software y firmware en 2N.com. Después de la descarga, descomprima el archivo.
3. Abra VirtualBox y seleccione "Archivo - Importar aplicación...".
4. Edite el título.
5. Verifique la configuración de la CPU (mínimo 2), la configuración de RAM (mínimo 2048 MB) y la selección de la tarjeta de red.
6. Confirme los términos de la licencia.
   Después de la instalación, se abrirá la consola de configuración de Linux, donde podrá realizar la configuración básica del sistema. La configuración completa se realiza en la interfaz web.

VMware Player

ATENCIÓN
La versión compatible de VMWare es 6.5 y superior.

1. Descargue el software apropiado desde la sección Soporte > Centro de descargas > Software y firmware en 2N.com. Después de la descarga, descomprima el archivo.
2. En VMware Player "Archivo - Abrir..." seleccione la ruta al archivo OVA.
3. Cambie el nombre según sea necesario y haga clic en "Importar".
4. Verifique la configuración de la CPU (mínimo 2), la configuración de RAM (mínimo 2048 MB) y la selección de la tarjeta de red.
   Después de la instalación, se abrirá la consola de configuración de Linux, donde podrá realizar la configuración básica del sistema. La configuración completa se realiza en la interfaz web.

VMware vSphere

ATENCIÓN
La versión compatible de VMWare es 6.5 y superior.

1. Descargue el software apropiado desde la sección Soporte > Centro de descargas > Software y firmware en 2N.com. Después de la descarga, descomprima el archivo.
2. En VMware vSphere, seleccione "Archivo – Implementar plantilla OVF..." y siga el asistente.
3. Después de importar, verifique la configuración "Editar configuración..."
   Edite el nombre (en la pestaña Opciones).
4. Verifique la configuración de la CPU (mínimo 2), la configuración de RAM (mínimo 2048 MB) y la selección de la tarjeta de red.
   Después de la instalación, se abrirá la consola de configuración de Linux, donde podrá realizar la configuración básica del sistema. La configuración completa se realiza en la interfaz web.

Hyper-V

1. Descargue el software apropiado desde la sección Soporte > Centro de descargas > Software y firmware en 2N.com. Después de la descarga, descomprima el archivo.
2. Inicie Hyper-V Manager y seleccione la opción para el host deseado Importar máquina virtual.
3. En la guía de instalación, consulte la información mostrada y confirme su lectura con el botón Próximo.
4. Seleccione la ruta de la carpeta del paso 1.
5. Confirme la selección de la máquina virtual.
6. Seleccione el tipo de importación.
7. Seleccione la NIC virtual para la máquina virtual.
8. Verifique el resumen de las configuraciones que fueron seleccionadas en los pasos anteriores y confirme con el botón Finalizar.
   Después de la instalación, se abrirá la consola de configuración de Linux, donde podrá realizar la configuración básica del sistema. La configuración completa se realiza en la interfaz web.

Hardware recomendado de la máquina virtual

El número de dispositivos conectados afecta**Access Commander**. Por lo tanto, establezca el tamaño de los elementos de hardware de acuerdo con la condición real. La siguiente tabla muestra la cantidad mínima recomendada de núcleos de CPU y tamaños de RAM para diferentes cantidades de dispositivos y usuarios administrados Access Commander.

ATENCIÓN
Se recomienda mantener una conexión continua entre **Access Commander** y dispositivos. Si se desconectan, los dispositivos almacenan registros de eventos fuera de línea y, cuando se vuelven a conectar, los datos de registro se sincronizan con Access Commander. Durante el proceso de sincronización, la aplicación continúa ejecutándose, pero con una mayor cantidad de dispositivos, todo el proceso puede tardar más.

hardware de la máquina virtual

Número de dispositivos	Número de usuarios	Número mínimo de núcleos de CPU	Tamaño mínimo de RAM	Asignación mínima de disco duro
1 000	10 000	2	2GB	120 GB
2 000	100 000	2	4 GB	120 GB
2 000	200 000	4	8GB	120 GB
7 000	200 000	4	16 GB	120 GB

Parámetros técnicos

Opciones de programa en Access Commander Box 2.0

Número de dispositivos conectados	Número de usuarios	Número de usuarios en el grupo.
7 000	200 000	1 500

Parámetros técnicos Access Commander Box

1ª generación **2N Nº de pedido 91379030** **Nº de pedido Axis 01672-001**	**2ª generación** **Nº de pedido** **1120120E, 1120120GB, 1120120US** **Nº de pedido Axis 03129-00**
• Dimensiones: 56,1 x 107,6 x 114,4 mm (2,21" x 4,24" x 4,50") • Procesador Intel®Celeron®J3160 (caché de 2 M; máx. 2,24 GHz) • Disco duro SSD SATA III de 2,5" (120 GB) • Memoria DDR3 SODIMM (4 GB) – 1,35 V, 1600 MHz • Soporte de pantalla dual a través de puerto VGA y HDMI • Puerto LAN Gigabit para conexión Ethernet • Marco de montaje VESA (75 x 75 mm + 100 x 100 mm) • Temperatura de almacenamiento: -20 °C a +60 °C • Temperatura ambiente de funcionamiento: 0 °C a +35 °C	• Dimensiones: 127,5 x 132 x 57,6 mm (5,02" x 5,20" x 2,27") • Intel® Processor N100, 6W TDP • SSD 980 NVMe M.2 – 250 GB • DDR4 SO-DIMM memory – 16 GB, 1,2 V, 3200 MHz • Compatible con HDMI 2.1, DisplayPort 1.4 y VGA • Puerto LAN 2,5G RJ45 para conexión Ethernet • Temperatura de almacenamiento: de -40 °C a +85 °C • Temperatura de funcionamiento: de 0 °C a +50 °C

Hardware recomendado de la máquina virtual

El número de dispositivos conectados afecta**Access Commander**. Por lo tanto, establezca el tamaño de los elementos de hardware de acuerdo con la condición real. La siguiente tabla muestra la cantidad mínima recomendada de núcleos de CPU y tamaños de RAM para diferentes cantidades de dispositivos y usuarios administrados Access Commander.

ATENCIÓN
Se recomienda mantener una conexión continua entre **Access Commander** y dispositivos. Si se desconectan, los dispositivos almacenan registros de eventos fuera de línea y, cuando se vuelven a conectar, los datos de registro se sincronizan con Access Commander. Durante el proceso de sincronización, la aplicación continúa ejecutándose, pero con una mayor cantidad de dispositivos, todo el proceso puede tardar más.

hardware de la máquina virtual

Número de dispositivos	Número de usuarios	Número mínimo de núcleos de CPU	Tamaño mínimo de RAM	Asignación mínima de disco duro
1 000	10 000	2	2GB	120 GB

Número de dispositivos	Número de usuarios	Número mínimo de núcleos de CPU	Tamaño mínimo de RAM	Asignación mínima de disco duro
2 000	100 000	2	4 GB	120 GB
2 000	200 000	4	8GB	120 GB
7 000	200 000	4	16 GB	120 GB

Activación de licencia

Se deben obtener licencias para activar archivo de licencia y subirlo a **Access Commander**. La licencia Básica se puede activar directamente en **Access Commander** en la página Configuración > pestaña Licencia.

Obteniendo el archivo de licencia

Para obtener una licencia, debe proporcionar al distribuidor el número de serie de uno de los dispositivos 2N conectados al **Access Commander**. El archivo de licencia se genera en función del número de serie de este dispositivo con licencia. Este debe ser el número de serie de la unidad de interfono principal, la unidad de acceso o la unidad de respuesta (no se puede utilizar 2N Indoor Touch).

Conexión dispositivo con licencia garantiza la validez de la licencia. En caso de desconexión del dispositivo con licencia, se iniciará un período de protección, transcurrido el cual se suspenderá la licencia.

Cargar licencia

ATENCIÓN

- Después de cambiar de la licencia de prueba, ya no es posible reactivar la licencia de prueba.
- Las configuraciones de funciones avanzadas que no son compatibles con la nueva licencia no se guardan.

1. Ir a **Configuración > pestaña Licencia**.
2. Haga clic en Cargar licencia y en la ventana abierta cargue el archivo de licencia obtenido del repositorio.
3. Después de cargar el archivo, haga clic en Activar la licencia.
4. Asegúrese de que el dispositivo con licencia para el que se generó la licencia esté activado.

archivo de licencia
: Un archivo con una licencia, cuya carga activa la licencia. El archivo de licencia lo genera el distribuidor en función del número de serie del dispositivo de licencia.

dispositivo de licencia
: Dispositivo 2N seleccionado conectado a **Access Commander**, que garantiza la validez de la licencia. El dispositivo de licencia sirve como clave de hardware para la licencia.

Renovación de licencias

Para restaurar una licencia suspendida, debe conectar y activar el dispositivo con licencia o hacer que se genere y cargue un nuevo archivo de licencia para otro dispositivo. Si carga una nueva licencia, primero debe activar el dispositivo con licencia para el que se genera la nueva licencia. Una vez activado el dispositivo con licencia, se pueden activar también todos los demás dispositivos.

La suspensión de la licencia se produce si el dispositivo con licencia se desconecta de **Access Commander** durante un período superior al período de protección de la licencia. La duración del período de protección depende del tiempo que el dispositivo con licencia haya estado conectado en **Access Commander**. Las duraciones de los períodos de protección se muestran en la tabla siguiente. Cuando se suspende una licencia, todos los dispositivos conectados se eliminan automáticamente de la administración y se marcan como no administrados.

NOTA

Eliminar dispositivos de la administración significa que no se pueden realizar cambios en su configuración a través de **Access Commander**. Los cambios realizados en **Access Commander** no se propagan al dispositivo. Sin embargo, los dispositivos continúan funcionando según los datos de la última configuración transferida desde **Access Commander**. Esto significa que los accesos y otras configuraciones de los dispositivos siguen siendo los mismos que antes de suspender la licencia.

Puede cambiar la configuración de un dispositivo no gestionado sólo en la interfaz de configuración web del dispositivo individual. Cuando el dispositivo se vuelve a conectar a la administración de **Access Commander**, se sincroniza y los cambios realizados directamente en la interfaz de configuración web del dispositivo se sobrescriben con la configuración en **Access Commander**.

La cantidad de tiempo que el dispositivo con licencia ha estado conectado Access Commander	El plazo de protección por el que será Access Commander en funcionamiento sin un dispositivo de licencia conectado
menos que 24 horas	1 día
1 día - 30 días	10 días
31 días - 180 días	1 mes
más de 180 días	3 meses

Cerraduras electrónicas

El sistema **Access Commander** proporciona gestión de accesos mediante cerraduras electrónicas 2N Fortis, que se desbloquean mediante tarjetas RFID con tecnología MIFARE® DESFire®. Al configurar las cerraduras electrónicas, se asigna a cada cerradura una clave de cifrado. Las llaves de las cerraduras se almacenan en las tarjetas RFID de los usuarios autorizados. Si las claves de la tarjeta y de la cerradura coinciden, se desbloquea el mecanismo de cierre.

Una tarjeta de acceso RFID puede utilizarse para acceder hasta a 90 puertas con cerraduras 2N Fortis, en función del número de perfiles horarios aplicados. Si se supera la capacidad de memoria de la tarjeta, fallará la escritura de datos en la tarjeta. El evento de fallo de escritura se registra en el registro de accesos del sistema. Si se utilizan Grupos de Cerraduras, se pueden escribir más puertas en una sola tarjeta que con la asignación individual. Si se utilizan Grupos de Bloqueo, se pueden inscribir más puertas por tarjeta que en una asignación individual.

Fortis Commander

Fortis Commander es una aplicación independiente que conecta las cerraduras electrónicas **Fortis** al sistema **Access Commander**. La aplicación establece los bloqueos de acuerdo con el archivo de proyecto creado en **Access Commander**u que contiene la configuración de los bloqueos. El archivo está encriptado y sólo puede utilizarse en una instalación específica.

Instalación

Fortis Commander está diseñado para instalarse en un ordenador Windows compatible con Bluetooth Low Energy (BLE).

Encontrará la aplicación en la página web 2N Download Centre.

Procedimiento de instalación

1. Descargue el paquete de instalación desde el enlace proporcionado.
2. Ejecute el instalador y complete la instalación siguiendo las instrucciones en pantalla.

Archivo del proyecto

El archivo del proyecto se crea en **Access Commander** y contiene la configuración completa del proyecto. El archivo está encriptado y protegido por contraseña.

Establecer bloqueos en Access Commander

Antes de cargar llaves en cerraduras individuales, debe emparejar **Access Commander** con **Fortis Commander**.

Generación de la clave maestra de cifrado (MEK) y preparación del proyecto

1. Inicie sesión en Access Commander.
2. Vaya a **Configuración > Cerraduras electrónicas**.
3. En la pestaña **Configuración inicial** haga clic en Generar claves.
4. Cree la clave de cifrado maestra.

ATENCIÓN
La clave de cifrado maestra no se puede ver ni modificar posteriormente .

NOTA
En función de la clave maestra de cifrado (MEK), **2N Access Commander** genera un conjunto de claves de cifrado. Por lo tanto, la clave debe ser única y suficientemente segura. El conjunto de claves se basa en la clave de cifrado maestra, por lo que los proyectos con la misma clave de cifrado maestra generan los mismos conjuntos de claves. Si se pierde un proyecto, se puede crear uno nuevo con la misma clave maestra de encriptación y continuar con la encriptación.

5. Tras generar las claves y establecer la contraseña del archivo de proyecto, puede descargar **el archivo de proyecto**, que es una imagen de la configuración de la cerradura electrónica en el sistema **Access Commander**.

6. En la pestaña **de Fortis Commander** haga clic en Descargar aplicación, desde donde se iniciará la descarga de **Fortis Commander** (aplicación para configurar cerraduras electrónicas).

ATENCIÓN
La información sobre el proyecto es confidencial. Protéjalos contra cualquier uso indebido.

Configuración de la cerradura electrónica mediante Fortis Commander

1. Instale **Fortis Commander** y ábralo.
2. Haga clic en Abrir proyecto y abra el archivo del proyecto descargado en el Explorador de archivos.
3. En el cuadro de diálogo que aparece, introduzca la contraseña del archivo de proyecto.
4. Tras abrir el archivo del proyecto, seleccione Conectar al dispositivo y conecte la tarjeta de servicio a la cerradura.
5. Haga clic en **Asignar**, que asigna el bloqueo al proyecto.
6. Desconecte el dispositivo y haga clic en **Archivo > Cerrar proyecto**.
7. Una vez finalizada la configuración, abra el sistema **Access Commander**. Vaya a la pestaña **Configuración > Cerraduras electrónicas** y haga clic de nuevo en Fortis Commander. Cargue el archivo de proyecto.

NOTA
Cuando traslade la cerradura de una instalación a otra o cuando realice una reclamación, deberá realizar un restablecimiento de fábrica . Esta operación restablece la cerradura a los ajustes de fábrica y elimina toda la configuración anterior.

Procedimiento de actualización de la configuración

1. Realice cambios en **Access Commander**.
2. Descargue el archivo del nuevo proyecto.
3. Cargue el archivo en **Fortis Commander** y realice los cambios necesarios en las cerraduras.
4. Si realiza otros cambios en **Access Commander**u, descargue siempre un nuevo archivo de proyecto.

ATENCIÓN
Para cada cambio de configuración en **Access Commander**u debe descargar un nuevo archivo de proyecto - no puede utilizar un archivo más antiguo que ya se haya cargado en **Fortis Commander**.

Bloqueo y desbloqueo permanentes

La aplicación le permite bloquear y desbloquear la cerradura de forma permanente. La función se utiliza para intervenciones de servicio o control de emergencia sin necesidad de utilizar una tarjeta.

Recogida de eventos de cerraduras electrónicas mediante tarjetas / chips RFID

Ajustes de recogida de eventos

1. Abra **Configuración > Cerraduras electrónicas > Eventos de pestañas**.
2. Seleccione el tipo de evento:
   - **Recopilar eventos de acceso y del sistema** - Todos los eventos de acceso y del sistema se registran en la tarjeta/chip y se escriben en el registro del sistema y en el registro de acceso .
   - **Recoger sólo los eventos del sistema** - sólo se registran los eventos del sistema, los eventos de acceso no se almacenan en las tarjetas.
   - **No recoja eventos en las pestañas** - no se escribe ningún evento en la pestaña; sólo se puede acceder a ellos a través de **Fortis Commander**u.

> **SUGERENCIA**
> Seleccionando del conjunto de eventos adecuado, puede reducir la carga del sistema y el uso del almacenamiento Sin embargo, el registro detallado es importante para el diagnóstico y las auditorías de seguridad.

Exportar eventos de una tarjeta

La tarjeta almacena un máximo de **16 primeros eventos**. Los eventos pueden leerse de dos maneras:

- En **Access Commander**, haga clic en el icono del cuadro de búsqueda de la cabecera y cargue la pestaña.
- Utilizando un dispositivo con **2N OS**, los eventos se leen de la tarjeta y se envían a **Access Commander**u.

Carga de eventos en la cerradura

1. Abra **Configuración > Cerraduras electrónicas > Fortis Commander** y haga clic en Descargar archivo.
2. Abra el archivo en **Fortis Commander**.
3. En la aplicación **Fortis Commander**, conéctese a la cerradura electrónica.
4. Vuelva a cargar el archivo actualizado en **Access Commander**.
5. Una vez cargados, los eventos se muestran en **Registros de acceso** y **Registros del sistema**.

Operaciones de servicio

Estas operaciones están disponibles para **Cilindro Fortis**:

- **Desmontaje** - desmontaje de cerraduras con fines de servicio.
- **Sustitución de la pila** - Sustitución de la pila de la cerradura.

> **ATENCIÓN**
> Las operaciones de servicio no son relevantes para otros tipos de esclusas.

> **NOTA**
> Desde el modo de servicio, la cerradura vuelve al modo normal pulsando el botón Lock para bloquearse permanentemente.

Actualización de tarjeta

Las tarjetas de acceso de los usuarios deben actualizarse periódicamente. El usuario actualiza la tarjeta conectándola al dispositivo 2N IP al que tiene derechos de acceso válidos. El lector del dispositivo debe sujetar la tarjeta hasta que se encienda el interruptor de apertura de la puerta. El interruptor de apertura de la puerta se activa solo después de actualizar el acceso a las cerraduras

Puede cambiar la validez predeterminada de diez días de las tarjetas en **Configuración > Cerraduras electrónicas > pestaña Parámetros de tarjeta**.

ATENCIÓN
Si modifica los derechos de acceso a las cerraduras en **Access Commander**, los cambios sólo se reflejarán en la tarjeta de acceso del usuario una vez que ésta se haya actualizado en el lector de tarjetas del dispositivo 2N. Por razones de seguridad, recomendamos fijar un periodo de validez más corto para las tarjetas, con el fin de garantizar su actualización periódica.

Los lectores de dispositivos IP que permiten actualizar la tarjeta y su configuración se describen en el capítulo Configuración del lector de dispositivos IP (p. 30).

Tarjetas compatibles

NOTA
A efectos de la presente documentación, el término tarjeta **o tarjeta** hace referencia a cualquier identificador compatible que utilice la tecnología MIFARE DESFire.

Para abrir las cerraduras electrónicas 2N Fortis no se pueden utilizar tarjetas con ID aleatorio (random ID).

Las tarjetas con tecnología PICard no se pueden utilizar para abrir cerraduras electrónicas 2N Fortis.

Perfiles temporales en cerraduras electrónicas

Las cerraduras electrónicas admiten perfiles horarios con las siguientes restricciones:

- No se aplican días festivos.
- Se pueden configurar hasta 4 intervalos de tiempo diferentes en un solo día.
- En un perfil temporal se pueden definir 4 horarios diarios de intervalos.

SUGERENCIA
Esto significa que puede tener, por ejemplo, una configuración diferente para el lunes, martes, miércoles y jueves, pero para el viernes, sábado y domingo debe utilizar una de las configuraciones existentes.

ATENCIÓN
Si el perfil temporal incumple las restricciones indicadas, se ignorará la regla de acceso y no se concederá acceso al usuario.

Fortis Commander

Fortis Commander es una aplicación independiente que conecta las cerraduras electrónicas **Fortis** al sistema **Access Commander**. La aplicación establece los bloqueos de acuerdo con el archivo de proyecto creado en **Access Commander**u que contiene la configuración de los bloqueos. El archivo está encriptado y sólo puede utilizarse en una instalación específica.

Instalación

Fortis Commander está diseñado para instalarse en un ordenador Windows compatible con Bluetooth Low Energy (BLE).

Encontrará la aplicación en la página web 2N Download Centre.

Procedimiento de instalación

1. Descargue el paquete de instalación desde el enlace proporcionado.
2. Ejecute el instalador y complete la instalación siguiendo las instrucciones en pantalla.

Archivo del proyecto

El archivo del proyecto se crea en **Access Commander** y contiene la configuración completa del proyecto. El archivo está encriptado y protegido por contraseña.

Establecer bloqueos en Access Commander

Antes de cargar llaves en cerraduras individuales, debe emparejar **Access Commander** con **Fortis Commander**.

Generación de la clave maestra de cifrado (MEK) y preparación del proyecto

1. Inicie sesión en Access Commander.
2. Vaya a **Configuración > Cerraduras electrónicas**.
3. En la pestaña **Configuración inicial** haga clic en Generar claves.
4. Cree la clave de cifrado maestra.

ATENCIÓN
La clave de cifrado maestra no se puede ver ni modificar posteriormente .

NOTA
En función de la clave maestra de cifrado (MEK), **2N Access Commander** genera un conjunto de claves de cifrado. Por lo tanto, la clave debe ser única y suficientemente segura. El conjunto de claves se basa en la clave de cifrado maestra, por lo que los proyectos con la misma clave de cifrado maestra generan los mismos conjuntos de claves. Si se pierde un proyecto, se puede crear uno nuevo con la misma clave maestra de encriptación y continuar con la encriptación.

5. Tras generar las claves y establecer la contraseña del archivo de proyecto, puede descargar **el archivo de proyecto**, que es una imagen de la configuración de la cerradura electrónica en el sistema **Access Commander**.
6. En la pestaña **de Fortis Commander** haga clic en Descargar aplicación**,** desde donde se iniciará la descarga de **Fortis Commander** (aplicación para configurar cerraduras electrónicas).

ATENCIÓN
La información sobre el proyecto es confidencial. Protéjalos contra cualquier uso indebido.

Configuración de la cerradura electrónica mediante Fortis Commander

1. Instale **Fortis Commander** y ábralo.
2. Haga clic en Abrir proyecto y abra el archivo del proyecto descargado en el Explorador de archivos.
3. En el cuadro de diálogo que aparece, introduzca la contraseña del archivo de proyecto.
4. Tras abrir el archivo del proyecto, seleccione Conectar al dispositivo y conecte la tarjeta de servicio a la cerradura.
5. Haga clic en **Asignar**, que asigna el bloqueo al proyecto.
6. Desconecte el dispositivo y haga clic en **Archivo > Cerrar proyecto**.
7. Una vez finalizada la configuración, abra el sistema **Access Commander**. Vaya a la pestaña **Configuración > Cerraduras electrónicas** y haga clic de nuevo en Fortis Commander. Cargue el archivo de proyecto.

NOTA
Cuando traslade la cerradura de una instalación a otra o cuando realice una reclamación, deberá realizar un restablecimiento de fábrica . Esta operación restablece la cerradura a los ajustes de fábrica y elimina toda la configuración anterior.

Procedimiento de actualización de la configuración

1. Realice cambios en **Access Commander**.
2. Descargue el archivo del nuevo proyecto.
3. Cargue el archivo en **Fortis Commander** y realice los cambios necesarios en las cerraduras.
4. Si realiza otros cambios en **Access Commander**u, descargue siempre un nuevo archivo de proyecto.

ATENCIÓN
Para cada cambio de configuración en **Access Commander**u debe descargar un nuevo archivo de proyecto - no puede utilizar un archivo más antiguo que ya se haya cargado en **Fortis Commander**.

Bloqueo y desbloqueo permanentes

La aplicación le permite bloquear y desbloquear la cerradura de forma permanente. La función se utiliza para intervenciones de servicio o control de emergencia sin necesidad de utilizar una tarjeta.

Recogida de eventos de cerraduras electrónicas mediante tarjetas / chips RFID

Ajustes de recogida de eventos

1. Abra **Configuración > Cerraduras electrónicas > Eventos de pestañas**.

2. Seleccione el tipo de evento:
   - **Recopilar eventos de acceso y del sistema** - Todos los eventos de acceso y del sistema se registran en la tarjeta/chip y se escriben en el registro del sistema y en el registro de acceso .
   - **Recoger sólo los eventos del sistema** - sólo se registran los eventos del sistema, los eventos de acceso no se almacenan en las tarjetas.
   - **No recoja eventos en las pestañas** - no se escribe ningún evento en la pestaña; sólo se puede acceder a ellos a través de **Fortis Commander**u.

SUGERENCIA
Seleccionando del conjunto de eventos adecuado, puede reducir la carga del sistema y el uso del almacenamiento Sin embargo, el registro detallado es importante para el diagnóstico y las auditorías de seguridad.

Exportar eventos de una tarjeta

La tarjeta almacena un máximo de **16 primeros eventos**. Los eventos pueden leerse de dos maneras:

- En **Access Commander**, haga clic en el icono del cuadro de búsqueda de la cabecera y cargue la pestaña.
- Utilizando un dispositivo con **2N OS**, los eventos se leen de la tarjeta y se envían a **Access Commander**u.

Carga de eventos en la cerradura

1. Abra **Configuración > Cerraduras electrónicas > Fortis Commander** y haga clic en Descargar archivo.
2. Abra el archivo en **Fortis Commander**.
3. En la aplicación **Fortis Commander**, conéctese a la cerradura electrónica.
4. Vuelva a cargar el archivo actualizado en **Access Commander**.
5. Una vez cargados, los eventos se muestran en **Registros de acceso** y **Registros del sistema**.

Operaciones de servicio

Estas operaciones están disponibles para **Cilindro Fortis**:

- **Desmontaje** - desmontaje de cerraduras con fines de servicio.
- **Sustitución de la pila** - Sustitución de la pila de la cerradura.

ATENCIÓN
Las operaciones de servicio no son relevantes para otros tipos de esclusas.

NOTA
Desde el modo de servicio, la cerradura vuelve al modo normal pulsando el botón Lock para bloquearse permanentemente.

Configuración del lector de dispositivos IP

Configuración en la interfaz web del dispositivo IP

ATENCIÓN
Si acaba de conectar un módulo de ampliación del lector de tarjetas RFID al dispositivo 2N mediante un cable VBUS, deberá emparejar este módulo con el dispositivo. El emparejamiento del módulo de ampliación del lector puede realizarse a través de la interfaz web del dispositivo en **Acceso > Módulos**.

1. Acceda a la interfaz de configuración basada en web para el dispositivo.

   SUGERENCIA
   Puede acceder a la interfaz de configuración basada en web haciendo clic en en la lista de la página Dispositivos.

2. Vaya a Hardware > Módulos de expansión.
3. En la página, vaya a la configuración del módulo lector de tarjetas RFID.
4. Haga clic en (Añadir módulo) y seleccione (Módulo de control de alarma).
5. En el menú **Tipos de tarjeta permitidos** seleccione “Cerraduras electrónicas 2N”

   ATENCIÓN
   Para un funcionamiento óptimo, habilite solo los tipos de tarjetas que realmente utiliza.

6. Guarde los cambios.

Módulos compatibles

La sincronización de las llaves para las cerraduras electrónicas 2N Fortis se puede realizar en todos los lectores RFID 2N comercializados en febrero de 2023 o posteriormente. La mayoría de los lectores fabricados después de esta fecha también son compatibles, con excepción de los modelos que se indican a continuación.

Los siguientes modelos **no son compatibles**:

- **2N IP Base**: todos los lectores RFID
- **2N IP Force**: 9151011, 9151012, 9151016, 9151017, 9151019
- **2N IP Vario**: todos los lectores RFID
- **2N IP Verso**: 915503x, 915504x, 915508x
- **2N Access Unit M**: 91611x
- **2N Access Unit 1.0**: 916008, 916009, 916010, 916011, 916013, 916016, 916019
- **2N Access Unit 2.0**: 916033x

Para los siguientes módulos, la compatibilidad sólo está garantizada para las unidades fabricadas en otoño de 2023 o después:

- **2N IP Force**: 9151031, 9151031S

Establecer bloqueos en Access Commander

Antes de cargar llaves en cerraduras individuales, debe emparejar **Access Commander** con **Fortis Commander**.

Generación de la clave maestra de cifrado (MEK) y preparación del proyecto

1. Inicie sesión en Access Commander.
2. Vaya a **Configuración > Cerraduras electrónicas**.
3. En la pestaña **Configuración inicial** haga clic en Generar claves.
4. Cree la clave de cifrado maestra.

ATENCIÓN
La clave de cifrado maestra no se puede ver ni modificar posteriormente .

NOTA
En función de la clave maestra de cifrado (MEK), **2N Access Commander** genera un conjunto de claves de cifrado. Por lo tanto, la clave debe ser única y suficientemente segura. El conjunto de claves se basa en la clave de cifrado maestra, por lo que los proyectos con la misma clave de cifrado maestra generan los mismos conjuntos de claves. Si se pierde un proyecto, se puede crear uno nuevo con la misma clave maestra de encriptación y continuar con la encriptación.

5. Tras generar las claves y establecer la contraseña del archivo de proyecto, puede descargar **el archivo de proyecto**, que es una imagen de la configuración de la cerradura electrónica en el sistema **Access Commander**.
6. En la pestaña **de Fortis Commander** haga clic en Descargar aplicación**,** desde donde se iniciará la descarga de **Fortis Commander** (aplicación para configurar cerraduras electrónicas).

ATENCIÓN
La información sobre el proyecto es confidencial. Protéjalos contra cualquier uso indebido.

Configuración de la cerradura electrónica mediante Fortis Commander

1. Instale **Fortis Commander** y ábralo.
2. Haga clic en Abrir proyecto y abra el archivo del proyecto descargado en el Explorador de archivos.
3. En el cuadro de diálogo que aparece, introduzca la contraseña del archivo de proyecto.
4. Tras abrir el archivo del proyecto, seleccione Conectar al dispositivo y conecte la tarjeta de servicio a la cerradura.
5. Haga clic en **Asignar**, que asigna el bloqueo al proyecto.
6. Desconecte el dispositivo y haga clic en **Archivo > Cerrar proyecto**.
7. Una vez finalizada la configuración, abra el sistema **Access Commander**. Vaya a la pestaña **Configuración > Cerraduras electrónicas** y haga clic de nuevo en Fortis Commander. Cargue el archivo de proyecto.

NOTA
Cuando traslade la cerradura de una instalación a otra o cuando realice una reclamación, deberá realizar un restablecimiento de fábrica . Esta operación restablece la cerradura a los ajustes de fábrica y elimina toda la configuración anterior.

Procedimiento de actualización de la configuración

1. Realice cambios en **Access Commander**.
2. Descargue el archivo del nuevo proyecto.
3. Cargue el archivo en **Fortis Commander** y realice los cambios necesarios en las cerraduras.
4. Si realiza otros cambios en **Access Commander**u, descargue siempre un nuevo archivo de proyecto.

ATENCIÓN
Para cada cambio de configuración en **Access Commander**u debe descargar un nuevo archivo de proyecto - no puede utilizar un archivo más antiguo que ya se haya cargado en **Fortis Commander**.

Bloqueo y desbloqueo permanentes

La aplicación le permite bloquear y desbloquear la cerradura de forma permanente. La función se utiliza para intervenciones de servicio o control de emergencia sin necesidad de utilizar una tarjeta.

Tarjetas para el mantenimiento

Las tarjetas de mantenimiento permiten el acceso autorizado a la cerradura. Permiten poner la cerradura en servicio, cambiar la pila, desmontar la cerradura.

ATENCIÓN
La tarjeta de mantenimiento no puede utilizarse al mismo tiempo como tarjeta de acceso de usuario.

Configuración de la pestaña Mantenimiento

1. En **Access Commander** vaya a **Configuración > Cerraduras electrónicas**.
2. En la pestaña **Mantenimiento** haga clic en Crear.
3. En el cuadro de diálogo que se abre, seleccione el tipo de tarjeta que desea crear.
   - Configurar cerraduras nuevas: activa las cerraduras nuevas previamente configuradas en fábrica en modo de servicio.
   - Servicio: activa el modo de servicio para la cerradura ya configurada.
   - Desmontaje - libere la cerradura de bombillo 2N Fortis ya ajustada para desmontarla, consulte el Manual de instalación de 2N Fortis.
   - Sustitución de la pila - libere la cerradura de bombillo 2N Fortis ya ajustada para sustituir la pila, consulte el Manual de instalación de 2N Fortis.

   SUGERENCIA
   Una tarjeta física puede cargarse simultáneamente con **Setting New Locks** y cualquier otra tarjeta de servicio. Recomendamos una combinación de **Ajuste de nuevas cerraduras** y **Servicio**.
4. Haga clic en . Continúe en.
5. Conecte la tarjeta al lector RFID USB conectado. Espere hasta que los datos se carguen en la tarjeta.

La validez de los datos de la tarjeta de mantenimiento es de un año. Una vez transcurrido este tiempo, es necesario borrar los datos y volver a configurar la tarjeta.

Compatibilidad con tarjetas DESFire de terceros (creación anónima de aplicaciones)

Access Commander le permite trabajar con tarjetas MIFARE DESFire. Admite tarjetas que ya se utilizan en otros sistemas de control de acceso y permite su reutilización sin necesidad de conocer su clave maestra (PICC Master Key).

Se trata de un modo especial en el que la tarjeta permite crear una nueva aplicación independiente sin necesidad de conocer su clave maestra (PICC Master Key).

Con esta funcionalidad, los administradores pueden:

- Reutilice las tarjetas físicas existentes.
- Escriba la aplicación OSO para **Access Commander** a ellos.
- Evite tener que conocer o gestionar la clave maestra PICC de los sistemas originales.

Para crear una aplicación OSO en una ficha

1. Conecte la tarjeta DESfire existente del usuario a un lector conectado a **Access Commander**.
2. Cree credenciales de usuario.
3. Access Commander detecta automáticamente si la tarjeta admite la creación de aplicaciones anónimas.
4. Si el modo es compatible, **Access Commander** escribe una nueva aplicación anónima en la tarjeta sin afectar a los datos existentes ni a las aplicaciones de terceros.

ATENCIÓN
Si el modo es compatible, Access Commander escribe una nueva aplicación anónima sin la opción de formatear la tarjeta más tarde utilizando una función de la sección Configuración. Sólo se puede borrar el contenido de la aplicación, no el espacio previamente ocupado en la tarjeta.

Acceso básico a la interfaz.

*Este capítulo describe la puesta en servicio y el uso básico **Access Commander**. La instalación se describe en el capítulo* *Instalación (p. 13)**.*

La interfaz **de Access Commander** es accesible a través de un navegador web. La dirección IP de la interfaz web puede consultarse utilizando 2N Network Scanner o Axis IP Utility. También se puede acceder directamente a la interfaz web en **accesscommander.local**. Esta funcionalidad está activada por defecto.

NOTA

- Si se ejecutan varias instancias de Access Commander en la red, el sistema asigna automáticamente nombres únicos: **accesscommander.local**, **accesscommander-2.local**, **accesscommander-3.local**, y otras instancias en función del número de servidores de la red.
- Para la distribución a través de Access Commander Box, conéctese a la interfaz web desde otro ordenador de la red. El sistema operativo Access Commander Box ejecuta **Access Commander** y su configuración básica de Linux, pero no permite ejecutar un navegador web.

NOTA
En caso de distribución a través de Access Commander Box conectarse a la interfaz web desde otra computadora en la red. Sistema operativo Access Commander Box asegura el funcionamiento **Access Commander** y su configuración básica de Linux no permite que se ejecute el navegador web.

Las credenciales predeterminadas son:

Nombre de usuario: **Admin**

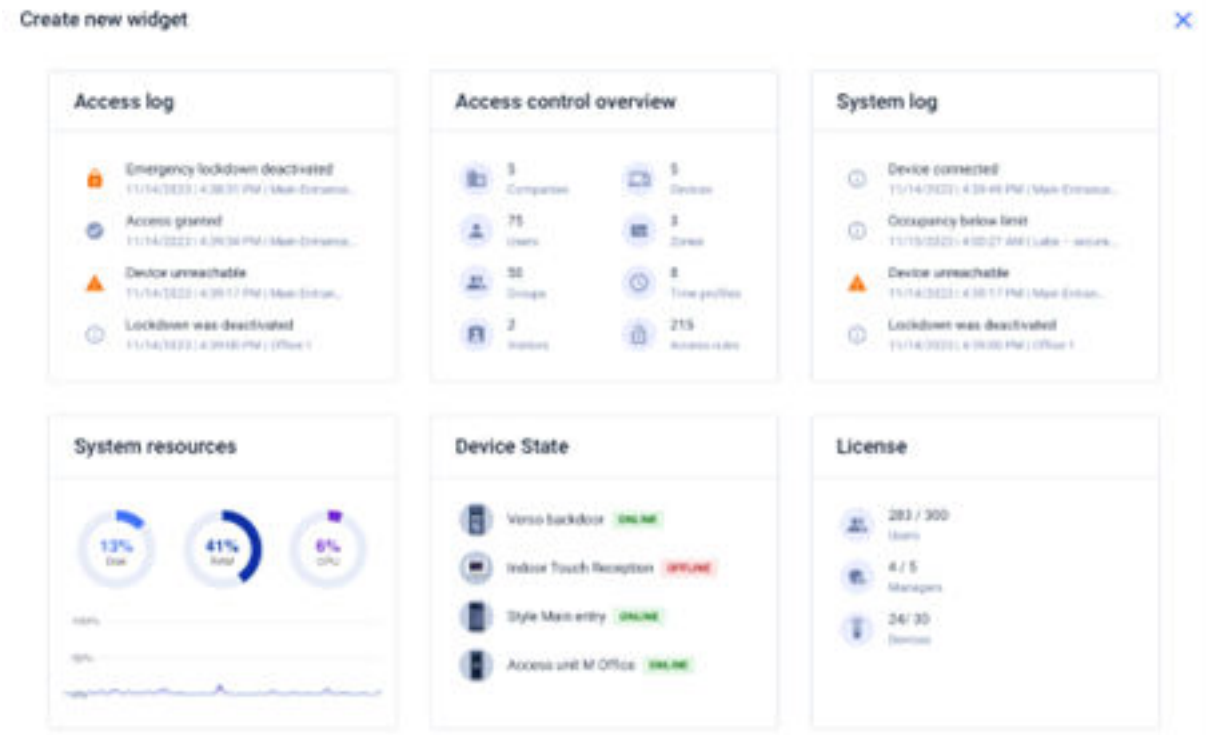
Contraseña: **2n**

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

NOTA
Marque la opción **No cerrar sesión**, si desea evitar volver a introducir sus credenciales de acceso la próxima vez que se conecte. El inicio de sesión es válido durante un máximo de 7 días, transcurridos los cuales deberá iniciar sesión de nuevo.

Es posible que necesite Autenticación de dos factores (p. 103) para iniciar sesión.

Panel



El panel de control es una vista básica de la interfaz web **Access Commander**. Es un tablero configurable que muestra datos en tiempo real. **Access Commander** ofrece varios widgets que se agregan al panel mediante el botón . Los widgets del panel se pueden mover, cambiar de nombre o modificar su configuración básica de varias maneras. La administración y eliminación de Widgets se realiza en el menú extendido en el encabezado de cada Widget.

Cualquier usuario con una cuenta en **Access Commander** puedes configurar tu propio panel de control. La disponibilidad de Widgets está limitada según el rol del usuario y la licencia disponible.

Cambio de idioma

Después del primer inicio de sesión **Access Commander** se muestra en el idioma configurado para la empresa del usuario que inició sesión. Cada usuario puede cambiar el idioma. Después del siguiente inicio de sesión, la interfaz se mostrará en el idioma recién configurado.

1. Haga clic en el icono de usuario en la esquina superior derecha para abrir el menú de usuario.
2. Seleccione Cambiar idioma.
3. Seleccione el idioma apropiado y confirme con Cambiar idioma.

Cambie la contraseña de la cuenta

1. Haga clic en el icono de usuario en la esquina superior derecha para abrir el menú de usuario.
2. Seleccione Mostrar perfil.
3. Haga clic en en el parámetro Contraseña.

4. Confirme la contraseña existente e ingrese una nueva.

> **NOTA**
> Si la contraseña de la cuenta 'admin' es la misma que la contraseña raíz del usuario del sistema (para iniciar sesión en la consola de configuración de Linux), cuando se cambie la contraseña de la cuenta 'admin', la contraseña de la cuenta raíz también se cambiará automáticamente.

Cambia tu foto de perfil

1. Haga clic en el icono de usuario en la esquina superior derecha para abrir el menú de usuario.
2. Seleccione Mostrar perfil.
3. Haga clic en la imagen en el encabezado del detalle del usuario.
4. En el cuadro de diálogo abierto, configure la foto.
   La resolución de la imagen se ajustará automáticamente a 432 × 432 px.

Logotipos

A continuación se ofrece una descripción general de lo que encontrará en el capítulo:

Registros del sistema

NOTA

- Al usuario se le muestran los registros que puede ver según sus permisos de usuario.
- Los datos se escriben en los registros en inglés.

La página Registros del sistema muestra una lista de los eventos y notificaciones que ha generado.

En la lista de registros del sistema se indica lo siguiente para cada evento y notificación:

- gravedad (info, advertencia, error).
- la hora en que se produjo el suceso.
- la categoría a la que pertenece la acción (Estado del dispositivo, Importación, Sincronización de usuarios, Sistema, Acciones de usuario, Restricciones de área).
- sujeto relacionado con la acción (dispositivo, usuario, zona, visita...).
- descripción breve del acontecimiento.
- autor del evento.

Al hacer clic en una línea se expande información detallada sobre el registro dado.

La lista se puede filtrar usando encima de la lista. Alternativamente, se pueden configurar filtros para columnas individuales en el menú extendido que se abre al hacer clic en en el encabezado de cada columna. Menú ampliado de columnas. también permite mover columnas, fijarlas en la primera o última posición u ocultarlas.

Las columnas Gravedad y Tiempo no se pueden ocultar.

Exportación de logotipos

Los registros pueden descargarse en un archivo CSV pulsando el botón Exportar situado encima de la lista. En el archivo CSV exportado, la hora se indica en GMT+0.

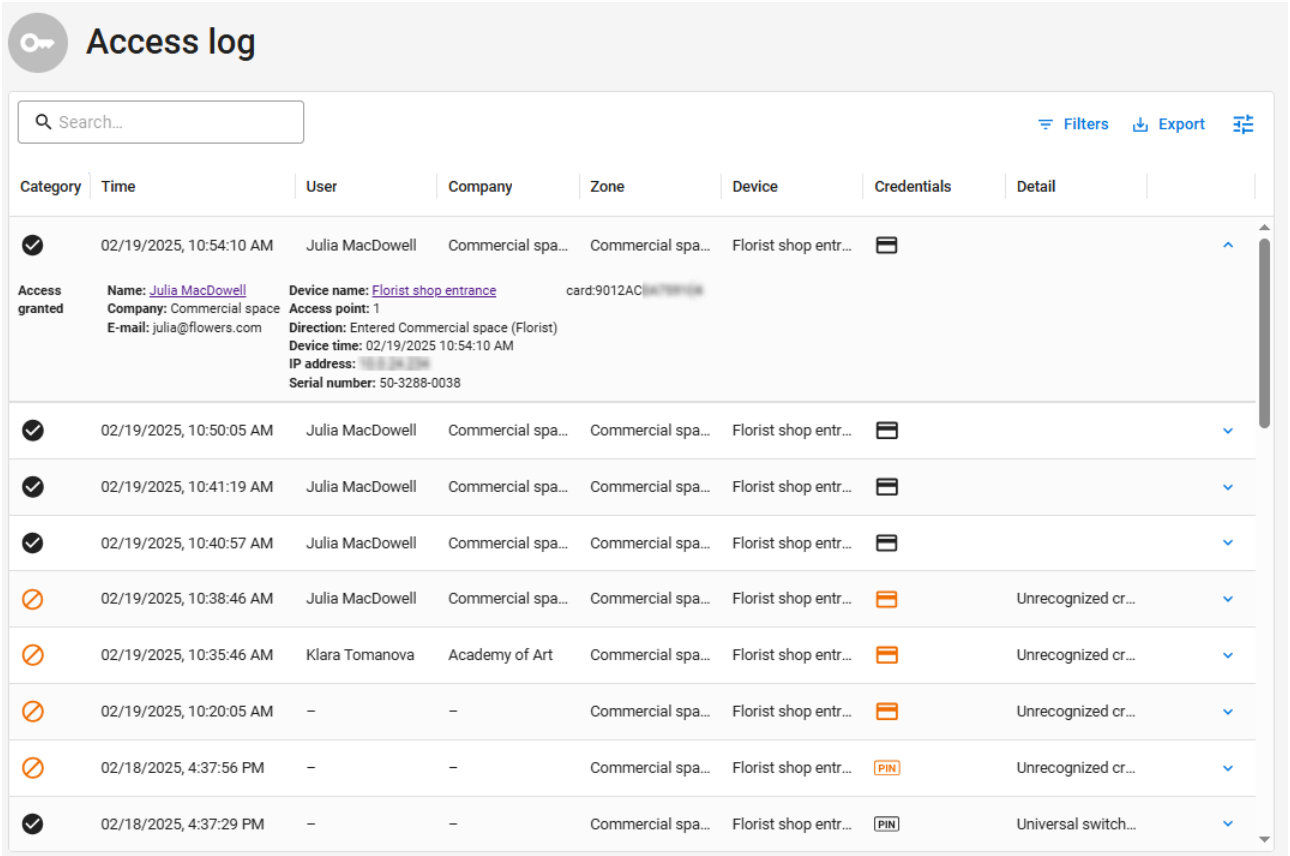
Vida útil de los registros

Una vez que el uso de la capacidad del disco alcance el 80%, se iniciará la eliminación automática del registro. La capacidad del disco se puede controlar en la página Configuración. Los registros del primer tipo se eliminan primero en orden, los demás registros se eliminan gradualmente hasta que el uso del espacio en disco cae al 75 % o hasta que solo quedan registros con el tiempo de almacenamiento mínimo posible incompleto del tipo de registro determinado.

El tiempo de retención para un determinado tipo de registro se establece en la pestaña **Configuración > Retención de Registros**. La retención de los registros de la cámara no puede ser mayor que la retención de los registros del sistema y de acceso.

SUGERENCIA
Si utiliza constantemente el 70% de la capacidad del disco, le recomendamos acortar el tiempo máximo de almacenamiento de registros.

Registros de acceso



NOTA

- Al usuario se le muestran los registros que puede ver según sus permisos de usuario.
- Los datos se escriben en los registros en inglés.

La página Registros de acceso muestra registros de intentos de autenticación exitosos y fallidos y bloqueos de emergencia.

La lista de registros de acceso indica:

- Categoría
  - concedido - acceso permitido
  - denegado - acceso denegado
  - público – permitiendo el libre acceso
  - bloqueo - bloqueo del dispositivo
- La hora en que ocurrió el evento.
- El usuario que realizó la acción.
- La empresa del usuario.
- La zona en la que ocurrió el evento.
- El dispositivo en el que ocurrió la acción.
- Autenticación que se utilizó para el intento (PIN, código QR, etc.)

Al hacer clic en una línea se expande información detallada sobre el registro dado.

La lista se puede filtrar usando encima de la lista. Alternativamente, se pueden configurar filtros para columnas individuales en el menú extendido que se abre al hacer clic en en el encabezado de cada columna. Menú ampliado de columnas. también permite mover columnas, fijarlas en la primera o última posición u ocultarlas.

Exportación de logotipos

Los registros pueden descargarse en un archivo CSV pulsando el botón Exportar situado encima de la lista. En el archivo CSV exportado, la hora se indica en GMT+0.

Vida útil de los registros

Una vez que el uso de la capacidad del disco alcance el 80%, se iniciará la eliminación automática del registro. La capacidad del disco se puede controlar en la página Configuración. Los registros del primer tipo se eliminan primero en orden, los demás registros se eliminan gradualmente hasta que el uso del espacio en disco cae al 75 % o hasta que solo quedan registros con el tiempo de almacenamiento mínimo posible incompleto del tipo de registro determinado.

El tiempo de retención para un determinado tipo de registro se establece en la pestaña **Configuración > Retención de Registros**. La retención de los registros de la cámara no puede ser mayor que la retención de los registros del sistema y de acceso.

SUGERENCIA
Si utiliza constantemente el 70% de la capacidad del disco, le recomendamos acortar el tiempo máximo de almacenamiento de registros.

Registro de llamadas

La página Registro de llamadas registra toda la actividad de llamadas de los interfonos conectados y otros dispositivos SIP (por ejemplo, contestadores automáticos o comunicadores de ascensor).

NOTA
El registro de llamadas sólo está disponible para el permiso de usuario Administrador.

La lista de registro de llamadas para cada evento indica:

- tipo de llamada
- la hora en que se produjo la llamada
- si la puerta está desbloqueada
- tipo de dispositivo
- contraparte
- duración de la llamada
- motivo de la finalización de la llamada

Al hacer clic en una línea se expande información detallada sobre el registro dado.

La lista se puede filtrar usando encima de la lista. Alternativamente, se pueden configurar filtros para columnas individuales en el menú extendido que se abre al hacer clic en en el encabezado de cada columna. Menú ampliado de columnas. también permite mover columnas, fijarlas en la primera o última posición u ocultarlas.

Exportación de logotipos

Los registros pueden descargarse en un archivo CSV pulsando el botón Exportar situado encima de la lista. En el archivo CSV exportado, la hora se indica en GMT+0.

Vida útil de los registros

El tiempo de retención para un tipo de registro determinado se establece en la pestaña *Configuración* > *Guardado de los registros*.

SUGERENCIA
Si utiliza constantemente el 70% de la capacidad del disco, le recomendamos acortar el tiempo máximo de almacenamiento de registros.

ATENCIÓN
Se recomienda utilizar la última versión de firmware en sus dispositivos para que todas las funciones del registro de llamadas funcionen correctamente. Es posible que algunas informaciones y columnas no estén disponibles o no se muestren correctamente en dispositivos con versiones de firmware más antiguas.

- **Duración de la llamada:** La columna Longitud de llamada no es compatible con versiones de firmware más antiguas. Esta información está disponible a partir de la versión 2.49 del firmware.
- **Identificación de la contraparte:** Se requiere la versión 2.50 o superior del firmware para identificar correctamente a la contraparte desde el directorio de dispositivos. En versiones anteriores, es posible que la búsqueda en el directorio de dispositivos no se comporte correctamente.

Notificación

El módulo de Notificaciones le permite configurar el monitoreo de eventos seleccionados y propiedades del sistema de las que tiene conocimiento. **Access commander** informar por correo electrónico o notificación en la barra superior al lado del menú de usuario.

La lista de notificaciones también se muestra en la página **Registros del sistema > Notificaciones**.

Los registros pueden descargarse en un archivo CSV pulsando el botón Exportar situado encima de la lista. En el archivo CSV exportado, la hora se indica en GMT+0.

Configurar un nuevo tipo de notificación

1. Ve a **Ajustes > Notificaciones**.
2. Haga clic en el botón Agregar en la esquina superior derecha de la página.
3. Ingrese un nombre para el nuevo tipo de notificación.
   Luego de la creación, se mostrará el detalle de la notificación, en el cual es posible seleccionar los dispositivos para los cuales se debe monitorear la notificación; agregar usuarios a quienes se debe enviar la notificación; Elija el método de entrega de notificación.

Configuración de las notificaciones

Los tipos de notificación se establecen en los detalles del tipo de notificación. Para abrir los detalles del tipo de notificación, haga clic en la notificación seleccionada en la lista de la página **Configuración > Notificaciones**.

Método de notificación

En esta pestaña, se configuran los métodos de notificación y la lista de destinatarios de notificaciones por correo electrónico.

Las notificaciones aparecen en **Access Commander** bajo el icono de la barra superior, junto al menú de usuario o en **Registro del sistema > Notificaciones**.

Se pueden enviar correos electrónicos de notificación a los usuarios administrados en **Access Commander** y destinatarios fuera del sistema. Los usuarios se pueden seleccionar de la lista. Las direcciones de correo electrónico de los demás destinatarios deben introducirse manualmente.

NOTA
Para el correcto funcionamiento de las notificaciones por correo electrónico, es necesario tener SMTP configurado correctamente, consulte Habilitación y configuración de la función de correo electrónico (SMTP) (p. 103).

Dispositivos monitoreados

El tipo de notificación dado se puede generar tanto para todos los dispositivos como solo para algunos dispositivos. Si Monitorear todos los dispositivos está habilitado, el evento puede ocurrir en cualquier dispositivo y se generará una notificación. Si Monitorear todos los dispositivos está deshabilitado, se generará una notificación solo si el evento ocurre en el dispositivo seleccionado. La selección del dispositivo se realiza en el menú que se abre con .

Vida útil de los registros

Una vez que el uso de la capacidad del disco alcance el 80%, se iniciará la eliminación automática del registro. La capacidad del disco se puede controlar en la página Configuración. Los registros del primer tipo se eliminan primero en orden, los demás registros se eliminan gradualmente hasta que el uso del espacio en disco cae al 75 % o hasta que solo quedan registros con el tiempo de almacenamiento mínimo posible incompleto del tipo de registro determinado.

El tiempo de retención para un determinado tipo de registro se establece en la pestaña **Configuración > Retención de Registros**. La retención de los registros de la cámara no puede ser mayor que la retención de los registros del sistema y de acceso.

SUGERENCIA
Si utiliza constantemente el 70% de la capacidad del disco, le recomendamos acortar el tiempo máximo de almacenamiento de registros.

Compañías

Los ajustes se pueden realizar dentro de una instalación **Access Commander** dividir en **Compañías**, que se gestionan por separado. Este método permite dividir la administración entre administradores en empresas individuales. Un administrador de una empresa no tiene acceso a la información de otra empresa. Los administradores de una empresa no verán a los usuarios de otra empresa.

Se pueden compartir zonas o instalaciones entre empresas, permitiendo gestionar el acceso de la empresa a zonas comunes (entradas, restaurantes, salas de conferencias...).

Creando una nueva empresa

1. ir a la pagina **Compañías**.
2. Haga clic en el botón Agregar empresa en la esquina superior derecha.
3. Complete el nombre de la empresa.
4. Puede iniciar una empresa haciendo clic en Crear.
   La empresa recién creada aparecerá en la lista. En los datos de la empresa es necesario realizar su configuración. La adición de usuarios a la empresa se realiza en la configuración de usuarios individuales.

Configuración de la empresa

La información de la empresa se puede ver y editar en los detalles de la empresa. Los detalles de una empresa se abren haciendo clic en una empresa seleccionada en su lista en la página Empresas.

En la cabecera del registro de empresa, un botón Bloqueo activa Bloqueo de emergencia (p. 64) para todos los dispositivos de las zonas de esta empresa.

Los detalles de la empresa se dividen en las pestañas Descripción general, Correos electrónicos y Sincronización de usuarios.

El lenguaje de la sociedad.

En la pestaña General, puede seleccionar el idioma de la empresa en el que se utilizará la interfaz. **Access Commander** mostrar a los usuarios de esa empresa. Los usuarios pueden cambiar el idioma de la interfaz más tarde. La elección del idioma por parte de la empresa también afecta a las plantillas de correo electrónico enviadas a los Usuarios. La redacción de los correos electrónicos se puede cambiar en la pestaña Correos electrónicos.

Zonas

La asignación de zonas a una empresa define el conjunto de instalaciones a las que tendrán derecho de acceso los usuarios de la empresa (por ejemplo, la zona de zonas comunes y la zona del 4º piso, que incluye la puerta de entrada a la recepción y todos los accesos del cuarto piso).). Se pueden asignar zonas a varias empresas al mismo tiempo y se pueden asignar varias zonas a una empresa.

My2N app

En la empresa es posible configurar parámetros de emparejamiento con Aplicación My2N, que permite la autenticación Bluetooth. Se establecen tanto los dispositivos en los que los usuarios podrán realizar el emparejamiento como el período de validez del acceso móvil necesario para el emparejamiento. El propio acceso móvil se genera en la configuración del usuario.

Visitas

En esta pestaña se configuran grupos a los que el administrador de visitas podrá asignar nuevas visitas. Uno de los grupos se puede especificar como predeterminado. La nueva visita se asignará automáticamente al grupo predeterminado, a menos que se establezca lo contrario.

ATENCIÓN
Sin un grupo predeterminado configurado correctamente, no es posible proporcionar acceso a los visitantes en la interfaz de usuario simplificada.

Es posible seleccionar los métodos de autenticación que se pueden asignar a la visita. Luego, el administrador de visitas asigna el método de autenticación a una visita.

Más información sobre cómo programar visitas en Visitas (p. 81).

Fondo de Trabajo

El grupo de trabajo y los días festivos se utilizan para calcular el grupo de trabajo mensual de los usuarios en el módulo de asistencia. Al seleccionar los días, es posible determinar qué días de la semana se contarán como días laborables. El día se selecciona haciendo clic. Los días verdes identifican qué días se consideran laborables.

El ajuste del tiempo de trabajo define cuánto tiempo tiene un turno diario.

Vacaciones

Al establecer días festivos, usted determina qué días no se incluyen en el cálculo del grupo de trabajo mensual. Las horas trabajadas en días festivos se cuentan de la misma manera que las horas trabajadas los fines de semana: el tiempo trabajado se registra además de las horas de trabajo normales.

oferta extendida ⋮ le permite copiar vacaciones de otra empresa. Los días festivos se copian incluyendo fechas y nombres. La copia se puede utilizar repetidamente, pero si el día festivo recién copiado ya está configurado en la empresa, se sobrescribirá su nombre.

Correos electrónicos enviados a miembros de la empresa.

La configuración del correo electrónico tiene su propia pestaña en los detalles de la empresa. **Access Commander** le permite enviar correos electrónicos automáticos a los miembros de la empresa (incluidos los visitantes) con información sobre la asignación de un método de autenticación. Se envía un correo electrónico al usuario o visitante con la dirección de correo electrónico establecida.

Access Commander le permite enviar correos electrónicos con la siguiente información:

- Código PIN para la visita
- Código QR para visitar
- Código PIN para el usuario
- Código QR para usuarios
- My2N app para configurar la autenticación Bluetooth para el usuario

En los **detalles de la empresa > pestaña Correos electrónicos > pestaña Plantillas** de correo electrónico, es posible configurar la apariencia de estos correos electrónicos y editar su redacción. La edición del texto de un correo electrónico se realiza en una ventana de diálogo que se abre al hacer clic en el tipo de correo electrónico seleccionado. En el cuadro de diálogo, puede editar:

- asunto - el asunto del correo electrónico
- encabezado: se muestra en el campo coloreado del cuerpo del correo electrónico

- Introducción: el texto que aparece antes de los datos generados automáticamente por **Access Commander**
- Siguiente mensaje: el texto que sigue a los datos generados a partir de **Access Commander**
- firma: la firma dada al final del correo electrónico

Sincronización de empresa (LDAP)

La sincronización con LDAP se utiliza para descargar usuarios y sus cambios desde un sistema LDAP externo. Los datos del usuario incluyen nombre de usuario, identificación, identificadores de tarjetas, código PIN/QR, imagen, dirección de correo electrónico, número de teléfono, contraseña e inicio de sesión, marcas de registro del vehículo.

NOTA
Puede encontrar más información sobre LDAP en www.ldap.com.

1. Vaya a **Empresas > detalle de la empresa seleccionada > pestaña Sincronización de usuarios**.
2. Si no se establece ninguna conexión, cree una.
   Llenar:

   - **El nombre del servidor** – si DNS está configurado correctamente, simplemente ingrese el nombre del servidor (“WIN-9ABEB4AUOHD”). Si no se configura DNS, la dirección IP del servidor en el que se ejecuta el servicio LDAP se ingresa en el nombre del servidor.
   - **Puerto** – la configuración predeterminada es el puerto LDAP 389 (sin SSL). Si desea utilizar una conexión cifrada en su empresa, ingrese el número de puerto 636. La compatibilidad con SSL también debe estar habilitada en el lado del servidor LDAP. Si el administrador establece un número de puerto diferente, también se debe cambiar en v **Access Comandaner**.
   - **Nombre de inicio de sesión** – el nombre de inicio de sesión del usuario que tiene los derechos correspondientes para la raíz dada o para todo el árbol. El nombre de inicio de sesión debe ingresarse en el formulario: "administrador@dominio.com"
   - **Contraseña** – la contraseña del usuario dado en el servidor LDAP.
   - **Seguridad de las comunicaciones (SSL)** – cuando SSL está deshabilitado, no es necesario reescribir el número de puerto. Al habilitar SSL, el número de puerto debe cambiarse a 636.
   - **DN base** – el punto raíz desde el que comienza la búsqueda del directorio. Puede ser una extensión o la raíz de un directorio, como por ejemplo: CN=administrador, CN=usuarios, DC=dominio, DC=com.

   La activación de TLS habilita la seguridad de la capa de transporte (TLS) para la conexión FTP. TLS cifrará los datos transmitidos entre **Access Commander** y el servidor.
   Habilitar autenticación de certificados TLS para habilitar la autenticación TLS de los certificados proporcionados por el servidor. Cuando se habilita, **Access Commander** verificará que se está comunicando con un servidor de confianza, lo que aumenta la seguridad de la conexión.
3. Se abre el detalle de la conexión LDAP configurada. Se pueden probar los ajustes de conexión. Usando el botón Sincronizar ahora inicias una sincronización única.
4. La pestaña Opciones de **de** permite gestionar cómo se sincronizan los datos.

   Puede eliminar la conexión establecida en el menú extendido ⋮ tarjetas **Importar**. en tarjeta **Opciones** Se establecen otros parámetros de sincronización.

SUGERENCIA
La sincronización automática está configurada en la tarjeta. **Importar**. Al habilitar la sincronización automática, complete los intervalos en los que debe realizarse la sincronización. Según la frecuencia, elige en qué minuto u hora se sincronizarán los datos.

Ajustes de sincronización de datos LDAP

Atributos importados - La modificación del esquema establece la asignación de atributos del servidor LDAP a los parámetros de **Access Commander**.

NOTA
Los atributos del número de teléfono se amplían con un filtro que convierte los números al formato deseado compatible con la lista de usuarios de la empresa en **Access Commander**. Hay dos filtros disponibles:

- `toPhoneNumber` - elimina los caracteres innecesarios (espacios, guiones, etc.) de los números de teléfono.
- `skipExtension` - elimina la extensión de los números de teléfono.

Ejemplo de uso: Si introduce el atributo `{telephoneNumber|toPhoneNumber|skipExtension}`, el valor original del número de teléfono en Active Directory “+420 123 456 789 x2222” se convierte en “+420123456789”.

Usuarios eliminados de LDAP - define qué debe ocurrir con los usuarios que han sido eliminados de LDAP. Los usuarios eliminados de LDAP pueden conservarse en **Access Commander** o eliminarse también. Si los usuarios deben desactivarse, después de eliminarlos de LDAP, sus datos permanecerán en **Access Commander**, pero no se sincronizarán con los dispositivos. Los usuarios desactivados no tienen derechos de acceso, no se puede acceder a ellos, etc.

Active Directory Banned Users - Establece lo que ocurre con los usuarios que han sido baneados de Active Directory. Este cambio en Active Directory puede ser ignorado por **Access Commander** o puede desactivar al usuario. Los usuarios desactivados no tienen derechos de acceso, no pueden ser localizados, etc. Tras la reactivación en Active Directory, los usuarios desactivados también se reactivan **Access Commander**.

Sincronización de grupos - le permite cargar membresías de grupos desde LDAP a **Access Commander**. Mediante la configuración del esquema de sincronización, puede definir un DN base personalizado y un filtro para sincronizar grupos. En la configuración del esquema, puede habilitar la sincronización de usuarios de grupos anidados.

Sincronización de avatares – establece la descarga de fotos del usuario desde el sistema LDAP.

Seguimiento de enlaces – establece si se sincronizan datos de enlaces LDAP.

Búsqueda anidada - permite la sincronización de usuarios de todo el árbol. Cuando está desactivada, sólo se buscan y sincronizan los datos de la raíz.

Paginación habilitada – la paginación utiliza la extensión LDAP de control de resultados paginados simples. Esto permite dividir los resultados en varias páginas, lo cual es esencial para servicios de directorio grandes. Parámetro **Tamaño de página** determina cuántos registros contendrá una página.

Importar usuarios a la empresa

El menú ampliado ⋮ en la cabecera de los detalles de la empresa le permite importar nuevos usuarios a la empresa una vez, ya sea desde un archivo CSV o desde otro dispositivo 2N.

Importar usuarios desde un archivo CSV

SUGERENCIA
Puede descargar un archivo CSV de muestra para importar usuarios usando este enlace.

Access Commander permite la carga masiva de usuarios en la empresa. La información básica sobre los usuarios se puede preparar en un archivo externo y luego el usuario se puede importar fácilmente. Los usuarios sólo pueden ser cargados a una empresa específica a la vez en un solo archivo.

Esta característica no permite que se eliminen usuarios.

NOTA
Los usuarios con el rol de Administrador pueden realizar una sincronización completa y repetible de la lista de usuarios entre empresas, a saber Sincronización de usuarios con FTP (p. 94).

Importar desde dispositivo 2N

Puede transferir una lista de usuarios desde un dispositivo 2N a **Access Commander**. Sólo puede importar desde un dispositivo que aún no se haya agregado a **Access Commander**. Un dispositivo no puede contener usuarios que ya estén en **Access Commander** (es decir, que tengan el mismo UUID). Todos los usuarios sólo pueden importarse en bloque a una empresa específica.

1. Es aconsejable hacer una copia de seguridad de la configuración antes de importarla. La copia de seguridad del sistema **Access Commander** se realiza en la ficha **Configuración > Copia de seguridad del sistema**. El respaldo de la configuración del dispositivo se realiza en su interfaz de configuración web, en **Sistema > Mantenimiento**.
2. Añada el dispositivo desde el que desea importar la lista de usuarios como un dispositivo **Access Commander**.

   ATENCIÓN
   No añada todavía dispositivos a las zonas. El dispositivo asumiría las reglas de acceso y la lista de usuarios se sobrescribiría en el dispositivo.

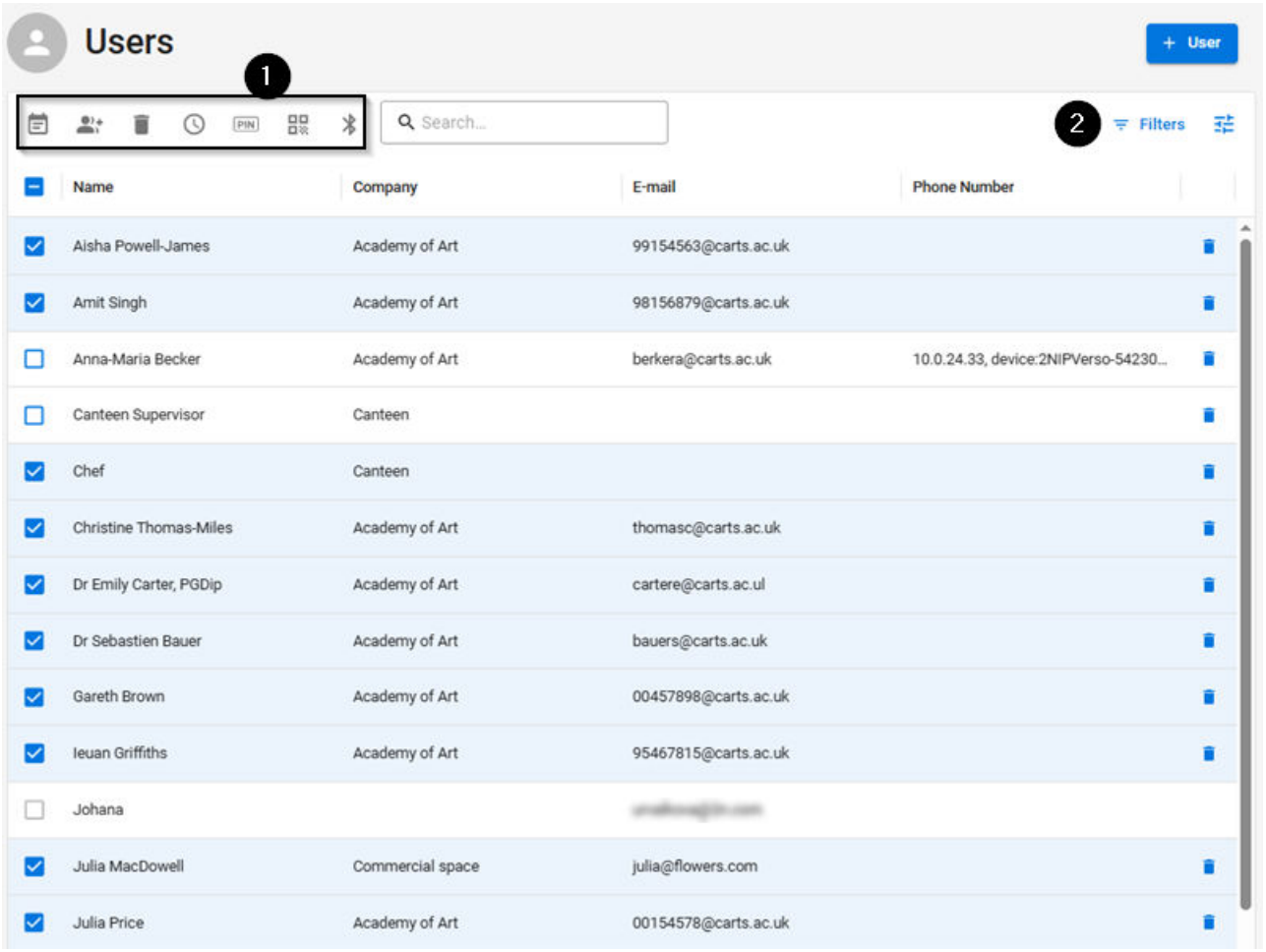
3. Vaya al detalle de la empresa a la que desea importar el usuario. En el menú avanzado ⋮, seleccione Importar desde dispositivo.
4. Se abrirá un cuadro de diálogo. En la lista desplegable de dispositivos disponibles, elija el dispositivo desde el que desea importar la lista de usuarios.
5. Haga clic en Importar para iniciar la importación en segundo plano. La finalización del proceso se registra en el Registro del sistema.
6. Después de una importación exitosa, el dispositivo se puede agregar a zonas e incluir en las reglas de acceso.

ATENCIÓN
El procedimiento de importación solo funciona para usuarios específicos (UUID) en el dispositivo e importa todos los usuarios del dispositivo a la vez a una empresa.

Usuarios

Ayuda **Access Commander** se puede gestionar **Usuarios**, modificar su acceso, gestionar sus datos de contacto, etc.

La lista de usuarios muestra todos los usuarios que se han creado. Encima de la lista puede filtrar los usuarios (número 2 en la imagen) o puede buscar un usuario concreto por nombre, correo electrónico o número de teléfono.



Acciones masivas

Puede seleccionar varios usuarios marcándolos y aplicar las siguientes acciones masivas (número 1 en la figura):

- Activar el seguimiento de asistencia para los usuarios
- Agregar usuario al grupo
- Borrar usuario
- Establecer el intervalo de tiempo de validez de acceso
- Asignar un código PIN de acceso a aquellos usuarios a los que aún no se les ha asignado un PIN o código QR

- Asignar un código QR de acceso a aquellos usuarios a los que aún no se les ha asignado un PIN o código QR
- Asigne acceso móvil a aquellos usuarios de la selección a los que aún no se les ha asignado acceso móvil.

NOTA
Para asignar un código PIN/QR o acceso móvil a un usuario, es necesario que el usuario tenga una dirección de correo electrónico válida.

Crear un nuevo usuario

1. ir a la pagina **Usuarios**.
2. Haga clic en el botón Agregar usuario en la esquina superior derecha.
3. Complete la información requerida: nombre de usuario y empresa a la que pertenece.
   El usuario recién creado aparecerá en la lista y se abrirán los detalles del usuario. Se realizan más configuraciones de usuario en detalle, como asignar un número de teléfono, configurar métodos de autenticación, asignar a grupos, etc.

NOTA
Access Commander permite la carga masiva de usuarios en la empresa. La información básica sobre los usuarios se puede preparar en un archivo externo y luego el usuario se puede importar fácilmente. Los usuarios sólo pueden ser cargados a una empresa específica a la vez en un solo archivo.

La importación a granel se realiza en los detalles de la empresa, a saber Importar usuarios a la empresa (p. 46).

Ajustes de usuario

La información del usuario se puede ver y administrar en los detalles del usuario. Los detalles del usuario se abren haciendo clic en el usuario seleccionado en la lista de la página Usuarios.

Los detalles del usuario se dividen en las pestañas Resumen, Asistencia y Registro de cambios. La pestaña Asistencia sólo se muestra para aquellos usuarios para los que se ha habilitado el seguimiento, consulte Seguimiento de asistencia de usuarios (p. 57). El módulo de asistencia está disponible en función de la licencia.

Cambiar el nombre y la foto del usuario

Las opciones para cambiar el nombre del usuario y configurar la foto se encuentran en el menú extendido en el encabezado de detalles del usuario.

La resolución de la imagen se ajustará automáticamente a 432 × 432 px.

Autenticación

Esta pestaña se utiliza para configurar métodos de autenticación de usuarios en los dispositivos. El usuario debe autenticarse en el dispositivo y, si tiene acceso válido, se le concederá acceso al dispositivo.

tarjeta RFID – agrega una tarjeta RFID existente al usuario. Se abrirá un cuadro de diálogo en el que deberá ingresar el identificador de la tarjeta. El identificador se puede cargar acercando la tarjeta a un lector USB o ingresando la tarjeta de identificación usando el teclado. El identificador debe ser un número hexadecimal de al menos 6 caracteres. A un usuario se le pueden asignar hasta 2 tarjetas de acceso.

Una tarjeta de acceso RFID puede utilizarse para acceder hasta a 90 puertas con cerraduras 2N Fortis, en función del número de perfiles horarios aplicados. Si se supera la capacidad de memoria de la tarjeta, fallará la escritura de datos en la tarjeta. El evento de fallo de escritura se registra en el registro de accesos del sistema. Si se utilizan Grupos de Cerraduras, se pueden escribir más puertas en una sola tarjeta que con la asignación individual. Si se utilizan Grupos de Bloqueo, se pueden inscribir más puertas por tarjeta que en una asignación individual.

SUGERENCIA
El administrador de usuarios y el administrador pueden ver el identificador de la tarjeta en el registro de acceso. De este modo, es posible cargar un vehículo nuevo/no asignado en un dispositivo accesible y luego copiar su identificador del registro. Después de insertar el identificador entre las tarjetas RFID, el usuario puede comenzar a utilizar la tarjeta. La visualización de identificadores en el registro de acceso debe estar habilitada en **Configuración > Autenticación**.

NOTA
Si **Access Commander** informa que la tarjeta nueva que acaba de agregar ya está en uso en el sistema, la razón puede ser que el modo de compatibilidad de tarjetas RFID está habilitado. El administrador habilita este modo en **Configuración > Autenticación > ficha Configuración del modo de compatibilidad**.

My2N app – utilizado para conectarse a la aplicación My2N habilitar la autenticación a través de Bluetooth, consulte el capítulo Autenticación Bluetooth (p. 54).

código PIN – genera automáticamente un PIN de 5 dígitos.

Al usuario se le puede asignar un PIN o un código QR para su acceso, pero no se pueden tener ambos al mismo tiempo.

Código QR – generará automáticamente un código QR. Los dispositivos que permiten la lectura de códigos QR se enumeran en Dispositivos y aplicaciones compatibles (p. 8).

Al usuario se le puede asignar un PIN o un código QR para su acceso, pero no se pueden tener ambos al mismo tiempo.

Huella dactilar – abre un cuadro de diálogo para cargar una huella dactilar que el usuario puede utilizar para autenticarse en dispositivos compatibles con la lectura de huellas dactilares. Cada usuario puede cargar hasta 2 huellas dactilares. El procedimiento se describe en el capítulo Carga de huellas dactilares (p. 54).

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

Tarjeta virtual – le permite configurar la ID de la tarjeta de acceso virtual del usuario. A cada usuario se le puede asignar exactamente una tarjeta virtual. El ID de la tarjeta virtual es una secuencia de 6 a

32 caracteres del conjunto 0-9, A-F. El número de tarjeta virtual se utiliza para identificar al usuario en dispositivos conectados a través de la interfaz Wiegand.

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

ATENCIÓN
Con la autenticación multifactor, es necesario seguir el orden de los métodos de autenticación.

SUGERENCIA
Al completar la dirección de correo electrónico, es posible enviar el código PIN/QR de acceso generado a la dirección indicada.

Cuenta

Estableciendo un nombre de usuario y una contraseña de un solo uso, puede conceder a un usuario acceso a la interfaz de **Access Commander**. Una vez conectado, el usuario puede hacer un seguimiento de su asistencia (si está disponible), cambiar su correo electrónico o cambiar su foto de perfil. La primera vez que el usuario inicie sesión, se le pedirá que cambie su contraseña. Si se requiere la autenticación de dos factores para el usuario, se le pedirá que se conecte a una aplicación de autenticación personalizada, véase Autenticación de dos factores (p. 103). El enlace a la aplicación de autenticación también se puede eliminar en esta pestaña.

En la ficha Cuenta, puede otorgar permisos a los usuarios con credenciales de inicio de sesión para administrar **Access Commander** mediante el uso de roles de usuario. Los permisos para cada rol se describen en Permisos de usuario (p. 7).

Interfaz simplificada

Se puede lanzar una interfaz de usuario simplificada para el gestor de visitas de una única empresa. La interfaz simplificada permite al gestor de visitas añadir, eliminar y gestionar visitas. Los registros y la presencia no pueden visualizarse en la interfaz simplificada. El objetivo de la interfaz simplificada es principalmente facilitar a los usuarios de los apartamentos el acceso a sus visitas. Todas las visitas creadas en la interfaz simplificada se asignan siempre al *grupo por defecto para nuevas visitas*. El gestor de visitas no tiene la posibilidad de cambiar este grupo. El grupo predeterminado para nuevas visitas debe seleccionarse previamente en los ajustes de la empresa, y el grupo debe configurarse con reglas de acceso válidas para acceder al apartamento, incluida la ruta de acceso al apartamento. A continuación, el usuario del apartamento puede gestionar los métodos de autenticación y la duración de las visitas en una interfaz simplificada.

ATENCIÓN
Antes de habilitar la interfaz simplificada, **el administrador del sistema debe establecer el grupo predeterminado para las nuevas visitas** en Configuración de la empresa (p. 43). Al grupo predeterminado se le deben asignar reglas de acceso tales que el visitante tenga acceso a las áreas visitadas. Sin un grupo predeterminado correctamente configurado, no es posible proporcionar acceso a los visitantes en la interfaz simplificada.

Información personal

Se utiliza para agregar información básica sobre el usuario. Le permite agregar la dirección de correo electrónico del usuario a la que se enviará la información relacionada con la cuenta del usuario y agregar un número de teléfono para contactar al usuario.

Es posible escribir en la tarjeta:

- **Correo electrónico** - la dirección a la que se enviará al usuario la información relacionada con su cuenta en **Access Commander**
- **Número de usuario** - un identificador específico necesario para la sincronización masiva con un archivo CSV (véase Sincronización de usuarios con FTP (p. 94))
- **Nota para**

Enfoques

La pestaña de accesos se utiliza para asignar un usuario a un grupo y para establecer el intervalo de tiempo durante el cual serán válidas las credenciales de acceso del usuario. El intervalo de tiempo se establece en el menú avanzado de la pestaña, que se abre haciendo clic en ⋮. El ajuste del tiempo de inicio de validez sólo se aplica a los accesos a dispositivos IP. Los accesos a las cerraduras electrónicas 2N Fortis son válidos desde el momento en que se asigna la tarjeta de acceso al usuario.

SUGERENCIA
Los límites de tiempo de acceso al dispositivo se establecen mediante perfiles de tiempo.

Si el usuario es miembro de un grupo, la pestaña muestra el grupo. Si el usuario no está asignado a un grupo, puede añadirse en la pestaña. El grupo puede modificarse o suprimirse en el menú ampliado ⋮.

Números de teléfono

Esta tarjeta se utiliza para configurar la conexión con el usuario. El número de teléfono es el destino de la llamada del dispositivo que pertenece a este usuario.

Número virtual

El número de teléfono virtual se puede utilizar para llamar a los usuarios mediante el teclado numérico del dispositivo. Los números virtuales no están relacionados con los números de teléfono propios de los usuarios, lo que permite ocultar sus números de teléfono en el dispositivo. Los números virtuales se pueden configurar, por ejemplo, según los números de los apartamentos. De este modo, los números virtuales se pueden utilizar en instalaciones en las que el número de teclas de marcación rápida es insuficiente.

El número virtual puede tener entre 1 y 7 dígitos. El primer y último carácter pueden ser números o letras, pero el resto deben ser números (por ejemplo, A123, 456B, C12E).

Suplente

En la pestaña también es posible configurar un sustituto al que se redirigirá la llamada en caso de que este usuario no esté disponible. El representante puede elegirse entre otros usuarios de la empresa.

Registro de acceso

El registro de acceso muestra el historial de acceso.

Registro de cambios

Todos los cambios en la configuración del usuario se pueden ver en la pestaña Registro de cambios. La clasificación básica es según el momento del cambio. En el registro es posible saber quién realizó el cambio. Luego de hacer clic en la línea, es posible conocer los detalles del cambio realizado.

Carga de huellas dactilares

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

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

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

Carga de huellas dactilares

1. Asegúrate de que el lector de huellas USB está activado en **Configuración > Acceso**.
2. En configuración de usuario v **Pestaña de autenticación** elegir autenticación Huella dactilar.
3. Seleccione el dedo para el cual desea cargar una huella digital.
   Aparecerá una ventana titulada "Carga de huellas digitales".
4. Coloque el dedo seleccionado en el lector. Repita este paso 3 veces, cada vez que se le solicite.
   Después del último escaneo, se le informará sobre el escaneo exitoso de la huella digital.
5. Al presionar el botón**Crear**el proceso está completo.

Autenticación Bluetooth

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

Este proceso está asegurado por el mecanismo de **emparejamiento Bluetooth de confianza** . El proceso de emparejamiento varía en función de la versión del firmware del dispositivo conectado.

GET IT ON Google Play Download on the App Store

La conexión de la app en el teléfono del usuario con los dispositivos 2N se realiza introduciendo el código de emparejamiento en la app My2N.

El código de emparejamiento puede obtenerse de dos maneras:

- conectándose al dispositivo **2N OS**
- a través de un lector USB Bluetooth conectado a su ordenador

ATENCIÓN
Para que el emparejamiento de confianza tenga éxito, el dispositivo debe tener la versión de firmware 2.50 (o 3.0) o superior. Si el dispositivo tiene un firmware más antiguo, el emparejamiento se realizará mediante el mecanismo más antiguo utilizando **PIN** sin **código QR**.

SUGERENCIA
Para un mayor nivel de seguridad, es preferible emparejarse utilizando el código QR de . Si **código QR** no está disponible o no es compatible con su dispositivo, utilice **PIN**.

Crear un código de emparejamiento a través de la computadora

1. Descarga a tu computadora 2N IP USB Driver e instalarlo.
2. Asegúrese de que el lector USB Bluetooth está activado en **Configuración > Autenticación > Lectores USB activados**.
3. Conecte el lector Bluetooth USB al ordenador.
4. En configuración de usuario v **Pestaña de autenticación** elegir autenticación My2N app.
5. En el cuadro de diálogo que se abre, seleccione Emparejar usando un lector. Aparecerá un código de emparejamiento en el cuadro de diálogo.
6. Siga el procedimiento que se indica a continuación (Emparejamiento en la aplicación móvil My2N app (p. 55)) para emparejar en la aplicación.

Crea un código de emparejamiento en el dispositivo.

1. Estar seguro de que
   - El dispositivo de emparejamiento está configurado para la empresa del usuario determinado, consulte???;
   - el dispositivo de emparejamiento está ubicado en una zona a la que el usuario tiene acceso válido, a saber Reglas de acceso (p. 74);
   - se establece un tiempo adecuado para el emparejamiento, a saber???.
2. En configuración de usuario v **Pestaña de autenticación** elegir autenticación My2N app.
3. En el cuadro de diálogo que se abre, seleccione Emparejar usando su dispositivo.
4. El código de emparejamiento generado se muestra en la tarjeta junto con el tiempo de emparejamiento restante. Pase el código de emparejamiento al usuario. Si el usuario tiene una dirección de correo electrónico completa, puede enviar la clave del móvil al correo electrónico haciendo clic en .
5. Siga el procedimiento que se indica a continuación (Emparejamiento en la aplicación móvil My2N app (p. 55)) para emparejar en la aplicación.

Emparejamiento en la aplicación móvil My2N app

1. Descárgalo Aplicación My2N a tu teléfono móvil. La aplicación está disponible en Tienda de aplicaciones y GooglePlay.
2. Abra la aplicación e ingrese el PIN de emparejamiento.

> **NOTA**
> Si la aplicación muestra **código QR**, pero el dispositivo está ejecutando un firmware anterior a 2.50.0, el emparejamiento sólo tendrá éxito introduciendo **PIN**.

3. Habilite todos los permisos importantes para que la aplicación My2N funcione correctamente.
4. Siga las instrucciones del teléfono móvil: acérquese al dispositivo en modo de emparejamiento y haga clic en Empezar a emparejar. A continuación, el teléfono móvil buscará un dispositivo con el que emparejarse.
5. Conceder acceso al teléfono móvil seleccionado. Luego podrá abrir puertas en toda la ubicación.

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

Emparejamiento en la aplicación móvil Clave móvil

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

Permisos de usuario

Informe en **Access Commander** Puede ser realizado por varios usuarios dependiendo de los permisos que se les asignen.

Las cuentas elevadas se configuran a través de una función en la configuración del usuario. Se pueden asignar varios roles a un usuario.

NOTA
Los permisos de usuario se aplican a la gestión dentro de la empresa del usuario. El administrador tiene acceso a la gestión completa de todas las empresas.

Administrador

- Configuración del sistema y de los módulos individuales según la licencia válida.
- Cambio de licencia
- Todos los permisos de otros roles aplicables a todas las empresas.

Administrador de acceso

- Crear y gestionar grupos.
- Gestionar las membresías de sus grupos.
- Crear y gestionar visitas.
- Creación y gestión de perfiles horarios.
- Establecer reglas de acceso.

Administrador de usuarios

- Crear y administrar usuarios.
- Crear y gestionar visitas.
- Gestionar las membresías de sus grupos.
- Visualización del registro de acceso y del sistema.

Gestor de visitas

- Crear y gestionar visitas.
- Administre sus membresías grupales (no disponible en la interfaz simplificada).
- Visualización del registro de acceso de visitas (no disponible en la interfaz simplificada).

Gerente de puerta

- Monitoreo de la transmisión de la cámara desde los dispositivos asignados.
- Apertura remota de dispositivos asignados.
- Bloqueo de emergencia de los dispositivos asignados.
- Ver el registro de acceso de los dispositivos asignados.
- Monitoreo de estados y eventos de seguridad en el log del sistema.

gerente de asistencia

- Seguimiento y gestión de la asistencia de los grupos asignados.
- Visualización del registro de acceso de los usuarios de los grupos asignados.

Administrador de empresa

- Establecer el idioma por defecto de la empresa.
- Supervisión del registro del sistema (limitada a los eventos de la empresa).
- La posibilidad de configurar un widget para el registro del sistema y la función de bloqueo de emergencia en los dispositivos utilizados por la empresa (incluidos los dispositivos compartidos con otras empresas).

Seguimiento de asistencia de usuarios

Access Commander permite el seguimiento de la asistencia de los usuarios. En el modo de asistencia se registran los tiempos de entrada y salida de usuarios individuales.

Se debe activar el registro de asistencia de los usuarios. La activación se realiza en el menú extendido. en el encabezado de detalles del usuario. Se puede activar el registro de asistencia para varios usuarios al mismo tiempo seleccionando usuarios en la lista en la página Usuarios y usando una acción masiva. .

El administrador de asistencia puede editar los datos de asistencia del usuario. La edición se realiza haciendo clic en el intervalo de tiempo que se va a cambiar. Una vez abierto, se pueden editar los tiempos límite y se puede agregar una nota al intervalo.

ATENCIÓN
Para el correcto funcionamiento de la asistencia es necesario contar con **Access Commander**Licencia activa disponible para realizar un seguimiento de la asistencia de los usuarios. El seguimiento de asistencia debe activarse en la configuración de usuario individual.

El seguimiento y ajuste de la asistencia se describen en el capítulo Asistencia (p. 78).

Grupos

El grupo se utiliza para agrupar usuarios y para configurar más fácilmente los derechos de sus miembros para acceder a la zona. No es necesario establecer derechos a nivel de usuarios y visitas individuales, sino que el grupo quedará asociado a la zona.

La lista se puede filtrar usando encima de la lista. Alternativamente, se pueden configurar filtros para columnas individuales en el menú extendido que se abre al hacer clic en en el encabezado de cada columna. Menú ampliado de columnas. también permite mover columnas, fijarlas en la primera o última posición u ocultarlas.

Crear un nuevo grupo

1. ir a la pagina **Grupos**.
2. Haga clic en el botón para agregar un grupo en la esquina superior derecha.
3. En el cuadro de diálogo que se abre, debes ingresar el nombre del grupo y seleccionar a qué empresa pertenece.

   ATENCIÓN
   Una vez creado un grupo, la empresa matriz no se puede cambiar.

   El grupo recién creado aparecerá en la lista y se abrirá su detalle. En los detalles del grupo, debes agregar miembros y establecer sus reglas de acceso.

Configuración de grupo

La información del grupo se puede ver y editar en los detalles del grupo. Los detalles del grupo se abren haciendo clic en el grupo seleccionado en la lista de grupos. En detalle, hay una descripción general de los miembros del grupo y una descripción general de sus reglas de acceso.

Miembros

La pestaña muestra todos los usuarios que pertenecen al grupo. Sólo se pueden agregar al grupo usuarios o tarjetas de visitante que pertenezcan a la misma empresa que el grupo.

Reglas de acceso

Muestra una descripción general de todas las reglas de acceso ya creadas y ofrece modificarlas o crearlas. Al crear una regla de acceso, se permite el acceso a la zona a un grupo específico. Al crear una regla, debe ingresar un grupo y un perfil de tiempo en el que el grupo debería tener acceso a la zona.

Zonas

Las zonas se utilizan para una gestión más sencilla del acceso a dispositivos individuales. Las zonas combinan dispositivos en unidades lógicas. En la página se muestra una lista de todas las zonas.

La lista se puede filtrar usando encima de la lista. Alternativamente, se pueden configurar filtros para columnas individuales en el menú extendido que se abre al hacer clic en en el encabezado de cada columna. Menú ampliado de columnas. también permite mover columnas, fijarlas en la primera o última posición u ocultarlas.

Habilitación de puntos de acceso

Ayuda Se abrirá un cuadro de diálogo en el que se inicia el soporte del punto de acceso, más v Configuración del punto de acceso del dispositivo (p. 79).

Creando una nueva zona

1. ir a la pagina **Zonas**.
2. Haga clic en el botón para agregar una zona en la esquina superior derecha.
3. En el cuadro de diálogo abierto, debes ingresar el nombre de la zona y seleccionar a qué empresas pertenece.
   La zona recién creada aparece en la lista. Los dispositivos se pueden agregar a una zona en el detalle de la zona o en el detalle del dispositivo. Se pueden realizar ajustes adicionales en el detalle de la zona.

Configuración de zona

La información de la zona se puede ver y editar en el detalle de la zona. Los detalles de la zona se abren haciendo clic en la zona seleccionada en la lista.

Autenticación multifactor

Es posible configurar la necesidad de autenticación de varias maneras para todos los dispositivos de la zona. Es posible seleccionar sólo algunos métodos de autenticación, pero se debe observar estrictamente el siguiente orden al utilizarlos:

1. My2N app
2. tarjeta RFID
3. Huella dactilar
4. Código PIN

ATENCIÓN
Con la autenticación multifactor, es necesario seguir el orden de los métodos de autenticación.

La necesidad de autenticación multifactor puede verse limitada por un perfil de tiempo. Cuando la autenticación multifactor está activada, aparecerá una opción **Utilice la autenticación multifactor**, en el que

puedes utilizar seleccione un perfil de tiempo. Al elegir el modo “En cualquier momento”, se requerirá autenticación multifactor todo el tiempo.

La autenticación multifactor solo puede ser necesaria para ingresar a la zona. Esta configuración solo es válida cuando se utilizan puntos de acceso.

Acceder a la configuración

Es posible establecer un volumen en la pestaña. **Código PIN para acceder a la zona** o mostrarlo si ya se ha creado un código PIN.

Además, en la configuración de acceso se pueden habilitar y deshabilitar las siguientes funciones:

alarma silenciosa – cuando se utiliza un código especial, se activa una acción silenciosa que envía un mensaje de alarma; el dispositivo no emite sonidos de alarma durante una alarma silenciosa. La configuración del código especial para la alarma silenciosa y su función exacta se realiza en la configuración del dispositivo.

Bloquear acceso – después de cinco intentos fallidos, el siguiente intento de acceso sólo se permitirá después de 30 segundos.

Verificación de matrícula – los vehículos tendrán acceso a la zona basándose en la verificación de matrículas en todos los dispositivos que admitan esta función.

Dispositivo

La pestaña muestra una descripción general de los dispositivos agregados a la zona determinada. Se pueden agregar dispositivos adicionales en esta pestaña.

Si se utilizan puntos de acceso, se agregan puntos de acceso individuales a la zona. El tipo de punto de acceso del dispositivo dado se describe como Entrada de Zona.

Los métodos de autenticación disponibles se muestran para cada dispositivo/punto de acceso.

Grupos de cerraduras

La pestaña muestra una visión general del grupo de cierre. Puede añadir otro grupo en esta pestaña.

Para cada grupo de bloqueo, puede ver los detalles del grupo.

Compañías

La tarjeta gestiona a qué empresas pertenece la zona determinada. Una zona puede pertenecer a varias empresas.

Reglas de acceso

Muestra una descripción general de todas las reglas de acceso ya creadas y ofrece modificarlas o crearlas. Al crear una regla de acceso, se permite el acceso a la zona a un grupo específico. Al crear una regla, debe ingresar un grupo y un perfil de tiempo en el que el grupo debería tener acceso a la zona.

La edición de una regla de acceso se puede realizar haciendo clic en la regla dada.

Dispositivo

La página Dispositivos muestra todos los dispositivos agregados en ese **Access Commander**.

La lista se puede filtrar usando encima de la lista. Alternativamente, se pueden configurar filtros para columnas individuales en el menú extendido que se abre al hacer clic en en el encabezado de cada columna. Menú ampliado de columnas. también permite mover columnas, fijarlas en la primera o última posición u ocultarlas.

Los registros pueden descargarse en un archivo CSV pulsando el botón Exportar situado encima de la lista. En el archivo CSV exportado, la hora se indica en GMT+0.

Al etiquetar, es posible seleccionar varios dispositivos y aplicarles las siguientes acciones masivas:

- Administrar dispositivos seleccionados
- Eliminar los dispositivos seleccionados de la administración
- Hacer una copia de seguridad de los dispositivos seleccionados

El icono de la barra de dispositivos redirige a la interfaz de configuración web del dispositivo.

Estados del dispositivo

- Online
- No administrado: el usuario ha desactivado la administración de dispositivos.
- Incompatible: el dispositivo no tiene una versión de firmware compatible.
- No configurado: debe cargar la configuración de las cerraduras electrónicas desde un programa de terceros.
- Offline
  - Error al iniciar sesión - Se ingresan credenciales incorrectas en la configuración web del dispositivo.
  - Inaccesible - **Access Commander** no se puede establecer una conexión con el dispositivo.
  - Certificado no válido: se requiere validación del certificado SSL y el dispositivo no tiene un certificado SSL válido.

Añadir un nuevo dispositivo IP

NOTA
La incorporación de cerraduras electrónicas 2N Fortis se describe en Cerraduras electrónicas (p. 22).

1. ir a la pagina **Dispositivo**.
2. Haga clic en el botón Agregar dispositivo en la esquina superior derecha.
3. Para añadir un interfono 2N, una unidad de acceso 2N o un contestador automático 2N, seleccione “2N IP devices”.

4. En el cuadro de diálogo que se abre, localice el dispositivo en su red local o escriba su dirección IP y puerto en el formato: “direcciónIP:puerto”.
   Después de ingresar la dirección IP del dispositivo, es posible presionar ENTER en el teclado para ingresar otro dispositivo.
5. Después de ingresar todos los dispositivos que desea agregar, complete la contraseña para acceder a la configuración web de estos dispositivos. Es posible agregar solo aquellos dispositivos en los que inicia sesión con la misma contraseña al mismo tiempo.
6. Aplicación de plantillas (opcional): Para aplicar una plantilla al dispositivo que está añadiendo, active el conmutador **Después de añadir el dispositivo, utilice la plantilla de configuración**.
   - El principio de selección y aplicación de una configuración a partir de una plantilla es el mismo que el de la aplicación manual de una plantilla a un dispositivo existente, como se detalla en Plantillas de dispositivos (p. 71).
7. Nombra el dispositivo antes de crearlo.
8. Los dispositivos recién agregados aparecen en la lista. Realice más ajustes del dispositivo en los detalles del dispositivo.

Grupos de cerraduras

Los grupos de bloqueos le permiten agrupar bloqueos individuales en unidades lógicas que luego pueden utilizarse para definir reglas de acceso, supervisar o gestionar dispositivos.

Ver grupos

Abra **Dispositivos > Bloquear grupos**.

NOTA
La lista muestra todos los grupos de bloqueo que se han creado. Utilice el cuadro de búsqueda para filtrar los registros por nombre.

Crear un nuevo grupo de bloqueo

1. Abra **Dispositivos > Bloquear grupos**.
2. Haga clic en `+ Grupo de cerraduras`.
3. Introduzca un nombre de grupo y seleccione la pestaña `Crear`.
4. En el módulo **Cerraduras** haga clic en `Añadir cerraduras`. Seleccione las esclusas que formarán parte del grupo.
5. En el módulo **Zonas** pulse en `Añadir zonas`. Seleccione las zonas que formarán parte del grupo.
6. Seleccione ⋮ para añadir, renombrar o eliminar un grupo de bloqueo.

AVISO
Cambiar la asignación del bloqueo a un grupo diferente requiere una reconfiguración. Asegúrese de que todos los cambios del sistema se han completado antes de exportar el archivo de configuración.

Establecer bloqueos en Access Commander

Antes de cargar llaves en cerraduras individuales, debe emparejar **Access Commander** con **Fortis Commander**.

Generación de la clave maestra de cifrado (MEK) y preparación del proyecto

1. Inicie sesión en Access Commander.
2. Vaya a **Configuración > Cerraduras electrónicas**.
3. En la pestaña **Configuración inicial** haga clic en Generar claves.
4. Cree la clave de cifrado maestra.

ATENCIÓN
La clave de cifrado maestra no se puede ver ni modificar posteriormente .

NOTA
En función de la clave maestra de cifrado (MEK), **2N Access Commander** genera un conjunto de claves de cifrado. Por lo tanto, la clave debe ser única y suficientemente segura. El conjunto de claves se basa en la clave de cifrado maestra, por lo que los proyectos con la misma clave de cifrado maestra generan los mismos conjuntos de claves. Si se pierde un proyecto, se puede crear uno nuevo con la misma clave maestra de encriptación y continuar con la encriptación.

5. Tras generar las claves y establecer la contraseña del archivo de proyecto, puede descargar **el archivo de proyecto**, que es una imagen de la configuración de la cerradura electrónica en el sistema **Access Commander**.
6. En la pestaña **de Fortis Commander** haga clic en Descargar aplicación**,** desde donde se iniciará la descarga de **Fortis Commander** (aplicación para configurar cerraduras electrónicas).

ATENCIÓN
La información sobre el proyecto es confidencial. Protéjalos contra cualquier uso indebido.

Configuración de la cerradura electrónica mediante Fortis Commander

1. Instale **Fortis Commander** y ábralo.
2. Haga clic en Abrir proyecto y abra el archivo del proyecto descargado en el Explorador de archivos.
3. En el cuadro de diálogo que aparece, introduzca la contraseña del archivo de proyecto.
4. Tras abrir el archivo del proyecto, seleccione Conectar al dispositivo y conecte la tarjeta de servicio a la cerradura.
5. Haga clic en **Asignar**, que asigna el bloqueo al proyecto.
6. Desconecte el dispositivo y haga clic en **Archivo > Cerrar proyecto**.
7. Una vez finalizada la configuración, abra el sistema **Access Commander**. Vaya a la pestaña **Configuración > Cerraduras electrónicas** y haga clic de nuevo en Fortis Commander. Cargue el archivo de proyecto.

NOTA
Cuando traslade la cerradura de una instalación a otra o cuando realice una reclamación, deberá realizar un restablecimiento de fábrica . Esta operación restablece la cerradura a los ajustes de fábrica y elimina toda la configuración anterior.

Procedimiento de actualización de la configuración

1. Realice cambios en **Access Commander**.
2. Descargue el archivo del nuevo proyecto.
3. Cargue el archivo en **Fortis Commander** y realice los cambios necesarios en las cerraduras.
4. Si realiza otros cambios en **Access Commander**u, descargue siempre un nuevo archivo de proyecto.

ATENCIÓN
Para cada cambio de configuración en **Access Commander**u debe descargar un nuevo archivo de proyecto - no puede utilizar un archivo más antiguo que ya se haya cargado en **Fortis Commander**.

Bloqueo y desbloqueo permanentes

La aplicación le permite bloquear y desbloquear la cerradura de forma permanente. La función se utiliza para intervenciones de servicio o control de emergencia sin necesidad de utilizar una tarjeta.

Bloqueo de emergencia

El bloqueo de emergencia se utiliza para bloquear completamente la puerta controlada por el dispositivo determinado. Durante el bloqueo de emergencia, no es posible abrir la puerta utilizando los accesos de usuario configurados, incluso si el usuario o visitante utiliza un acceso válido con un perfil horario válido.

El bloqueo de emergencia se puede activar/desactivar:

- en detalle del dispositivo: bloquea el dispositivo dado;
- en detalle de zona: bloquea todos los dispositivos en la zona;
- en los detalles de la empresa: bloquea todos los dispositivos de la empresa;
- usando la acción global en la barra superior presionando el botón – bloquea todos los dispositivos **Access Commander**;
- en el widget del panel.

En el widget de bloqueo de emergencia, es posible predefinir un grupo específico de dispositivos que podrán bloquearse en caso de emergencia.

ATENCIÓN
Los dispositivos sin conexión, los dispositivos inactivos, los dispositivos con firmware incompatible y los dispositivos con firmware anterior a 2.32 no se bloquearán después de una solicitud de bloqueo de emergencia. El dispositivo sin conexión se bloqueará tan pronto como vuelva a estar disponible.

Configuración de dispositivo

La información del dispositivo se puede ver y administrar en los detalles del dispositivo. Los detalles del dispositivo se abren haciendo clic en el elemento del dispositivo seleccionado en su lista. Dependiendo del tipo de dispositivo, los detalles se pueden dividir en pestañas Descripción general, Llamada y Levantamiento.

Desde los detalles del dispositivo se puede ir a la configuración web del dispositivo mediante el botón **Configuración de hardware** en la parte superior derecha del detalle del dispositivo. La configuración de

cada dispositivo se describe en el correspondiente manual de configuración. Es posible regresar desde la interfaz web de configuración cerrando la configuración con una cruz en la barra superior azul.

Descripción general

Estado

Esta pestaña muestra el estado del establecimiento de conexiones con los dispositivos. Los dispositivos en línea son aquellos con los que tiene **Access Commander** conexiones establecidas y en las que se carga el firmware aceptado. Gracias a la conexión establecida con el dispositivo, se puede realizar la sincronización de datos. El firmware incompatible se puede habilitar **Página del dispositivo > Firmware**.

La sincronización automática se activa después de cada cambio para reflejarse en la configuración de los dispositivos finales. La sincronización sólo se realiza en los dispositivos afectados. Solo las solicitudes activadas por cambios que pueden afectar a los dispositivos finales se ponen en cola para su sincronización. Dichos cambios tienden a ser cambios en los derechos de acceso, números de teléfono, perfiles de tiempo utilizados, etc. Por ejemplo, cambiar el nombre de un usuario que no está asignado a ningún grupo no activará la sincronización automática. La duración de la sincronización en sí (proyección de todos los cambios en los dispositivos finales) depende de la cantidad de dispositivos que deben sincronizarse, así como de la cantidad de datos que se cargan en el dispositivo.

Control de acceso

Establece la zona a la que pertenece el dispositivo.

Si el dispositivo tiene 2 puntos de acceso configurados y si la detección de puntos de acceso está activada (consulte Configuración del punto de acceso del dispositivo (p. 79)), se muestra la opción de asignar 2 zonas. Un punto de acceso de dispositivo solo puede estar en una zona.

Configuración

La pestaña muestra la versión actual del firmware, la dirección MAC y la dirección IP y permite cambiar la contraseña para acceder a su configuración web.

En la ficha, puede cambiar la dirección IP donde se encuentra el dispositivo, lo que permite que **Access Commander** apunte a un dispositivo que se ha desconectado y vuelto a conectar a la red en una dirección IP diferente.

control de puerta

Esta tarjeta muestra imágenes de las cámaras del dispositivo y permite la apertura remota del interruptor de puerta controlado por el dispositivo. La apertura de la puerta durante un tiempo determinado se puede configurar en el menú ampliado, que se abre haciendo clic en ⋮.

El estado actual del interruptor de la puerta se muestra junto al botón Abrir.

Se utiliza para cerrar puertas incluso para grupos con acceso válido. Bloqueo de emergencia (p. 64).

Respaldo

Esta pestaña le permite hacer una copia de seguridad de la configuración del intercomunicador en un archivo xml. La copia de seguridad se inicia con Inicie una copia de seguridad. Cuando se guarda una copia de seguridad en el almacenamiento local, se almacenará en una memoria delimitada **Access Commander**. Al guardar en un archivo, se abre un cuadro de diálogo en el que puede cifrar el archivo de respaldo con una contraseña. El archivo contiene información confidencial, por lo que se recomienda protegerlo. El cifrado de copias de seguridad está disponible en dispositivos con el firmware 2.45 o superior

Cada última copia de seguridad se mostrará en la pestaña. Es posible sincronizar automáticamente el dispositivo con la última copia de seguridad mediante el menú de Reiniciar. En el menú desplegable de este menú, también puedes elegir restaurar desde una copia de seguridad de otro dispositivo conectado o desde un archivo externo

NOTA
Se puede realizar una copia de seguridad de todos los dispositivos disponibles (dispositivos en línea y dispositivos conectados con firmware incompatible).

Llamar

tarjeta de llamada se muestra si hay una conexión de telecomunicaciones disponible y habilitada en el dispositivo. La pestaña muestra todas las cuentas habilitadas que protegen la conexión y muestra su estado. La conexión de telecomunicaciones se configura directamente en la interfaz de configuración del dispositivo en cuestión, en la sección Llamadas. Se accede a la interfaz de configuración mediante un botón Configuración de hardware en el encabezado de detalles del dispositivo.

Llamar

Esta pestaña se muestra en el detalle del dispositivo desde el que se pueden realizar llamadas.

Visualización de la agenda telefónica

La pestaña Contactos gestiona la visualización de la libreta de direcciones en dispositivos con pantalla. La tarjeta muestra el árbol de contactos tal como aparece en la libreta de direcciones del dispositivo. Al hacer clic en Alterar Se abrirá un cuadro de diálogo para editar el árbol de contactos. En la parte izquierda del cuadro de diálogo abierto, se muestra la clasificación de las carpetas de contactos. En la parte derecha se configuran los contactos dentro de la carpeta seleccionada. La carpeta raíz es la primera página que aparece cuando abre el directorio en su dispositivo. Todos los contactos aparecerán en una página de la libreta de direcciones si están todos almacenados en esta carpeta raíz. Los contactos se pueden agrupar en carpetas y ordenar en la carpeta raíz.

Agregar contactos a la pantalla del dispositivo

1. Ve a **Dispositivo > Detalles del dispositivo > pestaña Llamadas > pestaña Contactos**.
2. Abra la gestión de pantalla haciendo clic en Alterar.
3. En la parte derecha del cuadro de diálogo abierto, seleccione la carpeta a la que desea agregar contactos.
   Puedes agregar a la carpeta:

   1. **Usuarios**
      Es posible seleccionar varios usuarios al mismo tiempo.
   2. **Grupos**
      Los usuarios se pueden agregar a la carpeta en masa por grupo. Cada usuario del grupo aparecerá bajo su nombre en el directorio. Es posible seleccionar varios grupos al mismo tiempo.
   3. **grupos de llamadas**
      Los grupos de llamadas son grupos de contactos que se marcarán al mismo tiempo. Al crear un grupo de llamadas, es necesario ingresar su nombre, bajo el cual se mostrará el grupo de llamadas en la libreta de direcciones. Los contactos de los usuarios se agregan a un grupo de llamadas del mismo modo que los contactos se agregan a las carpetas.
      Puede cambiar el nombre del grupo de llamadas en el menú ampliado al lado de la carpeta, que abre haciendo clic en ⋮.
4. Puede cambiar el nombre de la carpeta en el menú avanzado de la carpeta, que abre haciendo clic en ⋮. En el menú ampliado, es posible agregar una imagen a la carpeta dada, que luego se mostrará en el dispositivo para esta carpeta.
5. Fija las carpetas o grupos de llamadas que quieras que aparezcan en los primeros lugares del menú extendido ⋮ para la carpeta dada usando 📌.

Otros números virtuales

En un dispositivo con teclado numérico, es posible iniciar una llamada saliente ingresando un número virtual. En esta pestaña es posible agregar usuarios que podrán llamar a números virtuales, incluso si estos usuarios no tienen acceso al dispositivo. Se permiten llamadas a números virtuales de usuarios que tienen acceso al dispositivo de forma automática.

Al seleccionar usuarios, solo se muestran aquellos usuarios que tienen un número virtual completado.

Botones

Esta pestaña se muestra en el detalle de los dispositivos que tienen botones que se pueden utilizar para marcar los números de teléfono de los usuarios. En la pestaña Botones, los usuarios individuales se asignan a botones individuales en el dispositivo. Al presionar un botón en el dispositivo se inicia una llamada saliente al destino del usuario asignado. El usuario es asignado al botón haciendo clic en y seleccionando al usuario.

Elevar

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

Configuraciones de control de ascensor

1. Antes de realizar la configuración en **Access Commander**, asegúrese de que el módulo de relé AXIS A9188 esté conectado al dispositivo 2N que proporcionará la autorización de acceso al piso. Asegúrese también de que HTTPS esté configurado en el módulo y que la contraseña raíz esté cambiada.
2. Vaya a los detalles del dispositivo que se supone debe controlar el acceso a pisos individuales. En el menú ampliado en el encabezado, active el control del ascensor. Aparecerá una pestaña en los detalles del dispositivo. **Elevar**.
3. En la cabecera de los detalles del dispositivo, navegue hasta configuración de hardware dispositivo. Navegue hasta **Integración > Control de acceso > pestaña Ascensor**. Habilite todos los módulos de relé que vayan a controlar el acceso desde el ascensor. Si los módulos requieren autenticación, introduzca el nombre de usuario y la contraseña. Guarde la configuración. Salga de la configuración del hardware utilizando la cruz de la barra superior azul.
4. Vaya a la pestaña Elevador en los detalles del dispositivo.
5. En la pestaña Piso del ascensor, seleccione la salida de relé para el piso al que desea configurar el acceso. El etiquetado de las salidas tiene el formato: *salida io_module_relay*. Haga clic en .
6. En el cuadro de diálogo abierto, asigne un nombre al piso y seleccione la zona a la que se ingresa en ese piso. Solo los usuarios autorizados a ingresar a la zona determinada de acuerdo con las reglas de acceso definidas podrán ingresar a este piso. Si la entrada al piso no se rige por las normas de la zona, marque la casilla **acceso público permitido**. Al seleccionar un perfil de horario, limita el acceso público solo al horario definido por el perfil de horario seleccionado. Fuera de este perfil de tiempo, nuevamente se permitirá la entrada solo a usuarios con acceso válido según las reglas de acceso.

> **ATENCIÓN**
> Si el acceso se configura según las reglas de acceso de la zona, el dispositivo del ascensor no asume ninguna otra configuración de esta zona (código PIN, autenticación múltiple, alarma silenciosa, ...).

Piso
Una vez habilitada, esta pestaña muestra una lista de todos los pisos configurables. Cada piso tiene su propia designación en el orden de módulo y salida de relé. A cada piso se le puede asignar su propio nombre.

Módulos
Esta ficha muestra todos los módulos AXIS A9188 conectados y su estado actual. Los módulos individuales se habilitan en la configuración del dispositivo, en **Hardware > Elevator Control**.

Supervisión
Esta página sirve para obtener información sobre los dispositivos IP conectados (intercomunicadores, unidades de acceso, unidades de respuesta). Cada administrador puede configurar la tabla según sus propias necesidades mediante . La configuración es única para cada cuenta. La configuración se realiza seleccionando las columnas que se desean mostrar.

Haga clic en la línea para ir al detalle del dispositivo en cuestión.

firmware
La página Firmware garantiza una actualización masiva del firmware de tipos individuales de dispositivos conectados y, por lo tanto, ayuda a mantenerlos en condiciones óptimas. La gestión masiva de dispositivos se puede suspender. Opcionalmente, algunos dispositivos se pueden excluir de la administración masiva de firmware.

SUGERENCIA
La nueva versión de firmware se puede implementar primero en uno o más dispositivos seleccionados en modo de prueba y solo entonces permitir la actualización de otros dispositivos.

La versión actual del firmware está disponible en línea a través del 2N Update Server; opcionalmente, también es posible cargar el archivo de actualización manualmente. La implementación de una nueva versión siempre está sujeta a la aprobación del administrador, quien así tiene control total sobre el proceso de actualización.

Es posible que se necesiten varios minutos para obtener las versiones de firmware del servidor de actualización 2N.

La versión de gestión masiva muestra una lista de los tipos de intercomunicadores 2N conectados, unidades de respuesta 2N y unidades de acceso 2N.

Exclusión de dispositivos
Puede excluir dispositivos de la gestión masiva de firmware añadiéndolos a la lista en **Dispositivos > Firmware > pestaña Dispositivos excluidos**.

Versión de firmware incompatible
Cuando agrega o actualiza un dispositivo que no tiene firmware compatible, ese dispositivo entrará en un estado incompatible. Un estado incompatible significa que los nuevos usuarios no se almacenan en el dispositivo. Además, los eventos se descargan del dispositivo y es posible utilizar la configuración o copia de seguridad del dispositivo. Se crea una nueva entrada en la tabla y el administrador tiene la opción de permitir el uso de firmware incompatible.

Access Commander desactiva automáticamente los dispositivos con firmware que no es compatible con su versión actual. La pestaña muestra estas versiones de firmware no compatibles en los dispositivos conectados. La lista de versiones de firmware compatibles se proporciona a continuación.

Access Commander puede controlar todos los dispositivos que ejecutan una versión de firmware no compatible si dicha versión está aprobada. La aprobación se realiza en **Dispositivos > Firmware > ficha Versiones de firmware incompatibles** mediante el icono  .

ATENCIÓN
Aprobar una versión no compatible puede provocar problemas como la pérdida de datos o impedir el funcionamiento adecuado.

Versiones de firmware compatibles

- 3.0
- 2.50
- 2.49
- 2.48
- 2.47
- 2.46
- 2.45

Seguridad

El método para asegurar la comunicación entre Access Commander y los dispositivos se establece en **Devices > Security > Device Certificate Verification tab**.

Access Commander proporciona tres niveles de seguridad para comunicarse con los dispositivos.

1. **Comunicación cifrada sin verificación de certificados** – **Access Commander** utiliza un certificado autofirmado para la comunicación HTTPS. Los navegadores web consideran que este certificado no es de confianza.
2. Verificación de impresión del certificado – la comunicación se asegura comprobando el certificado registrado en el dispositivo. Al comunicarse, se verifica la impresión de este certificado
   Cuando la autenticación por huella digital está activada, el administrador del dispositivo debe confirmar la validez de la huella del certificado al agregar un dispositivo nuevo. Se le pedirá al administrador del dispositivo que verifique la huella digital incluso si se cambia el certificado de un dispositivo ya agregado
3. **Verificación completa del certificado** - la comunicación está asegurada por un certificado firmado por una denominada autoridad de certificación. Durante la comunicación, toda la cadena de certificación se verifica de acuerdo con los requisitos de la PKI.

ATENCIÓN
En el dispositivo 2N Indoor Touch no se pueden cargar certificados SSL propios, tras activar la verificación de certificados se perderá la conexión con ellos.

Cómo gestionar los certificados

El método para asegurar la comunicación entre Access Commander y los dispositivos se establece en **Devices > Security > Device Certificate Verification tab**.

Cuando la autenticación con certificado SSL está activada, la sincronización solo se produce en los dispositivos que tienen un certificado SSL con una autoridad de confianza firmada. La sincronización de los dispositivos sin dichos certificados SSL se desactivará. Los dispositivos pasarán al estado desconectado

El certificado de la autoridad firmante debe ser fiable en el servidor en el cual esté funcionando **2N Access Commander**.

SUGERENCIA
El proceso de carga de certificados en el servidor se describe en las FAQ.

Para que la autenticación se realice correctamente, los certificados del dispositivo deben estar firmados por la autoridad de certificación e incluir la dirección IP o el nombre de dominio del dispositivo.

Cargar un certificado de dispositivo

1. Acceda a la interfaz de configuración basada en web para el dispositivo.
2. Vaya a **Sistema > Certificados > pestaña Certificados de usuario**.
3. Cargue el certificado preparado.
4. Vaya a **Sistema > Conexión de red > pestaña Servidor web**.
5. En el parámetro **Certificado de servidor HTTPS**, seleccione el certificado que ha cargado.
6. Guarda los cambios.

Configuración del punto de acceso del dispositivo

Puede dividir lógicamente cada dispositivo en dos puntos de acceso: de llegada y de salida. Cada punto de acceso representa un paso en una dirección y determina si el usuario del dispositivo entra o sale de la zona. Un punto de acceso puede ser controlado por uno o varios módulos de dispositivo. Todos los módulos asignados gestionan entonces los pasillos en la dirección del punto de acceso específico. Los puntos de acceso se utilizan especialmente en situaciones en las que un dispositivo se encuentra en el límite de dos zonas y es necesario registrar con precisión la dirección del movimiento entre ellas (por ejemplo, para funciones anti-retorno).

Los puntos de acceso también se utilizan para realizar un seguimiento de los usuarios en el módulo Presencia (p. 84). Los puntos de acceso también se utilizan para realizar un seguimiento de las entradas y salidas en Restricciones de área (p. 86).

NOTA
En la interfaz de configuración web de cada dispositivo, los puntos de acceso se denominan **Llegada** y **Salida**. Para configurarlas, vaya a **Acceso > Reglas de acceso > Solapa Acceso y salida**.

Habilitación de puntos de acceso en Access Commander

1. Ir a la página de Zonas v **Comandante de acceso**.

2. En la esquina superior derecha, presione y habilitar el uso de puntos de acceso.

Asignación de módulos para la llegada o la salida

1. Acceda a la interfaz de configuración basada en web para el dispositivo.

> **SUGERENCIA**
>
> Puede acceder a la interfaz de configuración basada en web haciendo clic en en la lista de la página Dispositivos.

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

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

Plantillas de dispositivos

La función Plantillas de dispositivos le permite configurar varios dispositivos. Las plantillas simplifican la instalación inicial del sistema y unifican los ajustes en todos los proyectos.

Las plantillas funcionan según el principio del patrón. Las plantillas le permiten guardar la configuración completa de cualquier dispositivo con **2N OS** o sólo partes seleccionadas de la configuración y aplicarlas después a otros dispositivos. La configuración puede basarse en un dispositivo ya configurado, en una copia de seguridad del dispositivo o en una plantilla exportada previamente.

Al crear una plantilla, puede elegir qué partes de la configuración se incluyen. Las partes individuales difieren según el tipo de dispositivo (por ejemplo, configuración de relés, salidas de audio, automatización). Esta selección forma parte del proceso de creación de la plantilla y no puede modificarse una vez guardada.

> **NOTA**
>
> El uso de plantillas puede reducir significativamente el tiempo necesario para la puesta en marcha inicial.

Creación y gestión de plantillas

Para acceder a la función de plantillas, vaya a Dispositivos > Plantillas.

1. Haga clic en + Crear plantilla desde.
2. Se abre el diálogo **Crear plantilla**.
3. En el menú desplegable **Dispositivos***, seleccione un dispositivo existente que servirá como dispositivo base para su plantilla. Sólo se mostrarán los dispositivos compatibles con las plantillas.

4. Haga clic en Siguiente para continuar configurando la plantilla.

ATENCIÓN
Algunas configuraciones pueden mostrar advertencias. Éstas informan de que las configuraciones seleccionadas pueden tener limitaciones o riesgos potenciales. La selección sigue habilitada, pero se recomienda comprobar la notificación.

Importar una plantilla o copia de seguridad desde un archivo

Si ya tiene una plantilla o una copia de seguridad del dispositivo guardada en un archivo, puede importarla fácilmente:

1. Vaya a Dispositivos > Plantillas.
2. Haga clic en Importar desde en la parte superior derecha.
3. Seleccione la plantilla o el archivo de copia de seguridad de su ordenador y haga clic en Importar.

NOTA
Al importar, algunas secciones pueden aparecer desactivadas. Se trata de partes de la configuración que podrían provocar cambios no deseados o interferir en el funcionamiento del aparato. Estas secciones se eliminan automáticamente al importar y el usuario puede verlas brevemente al cargar.

Modificación de la plantilla

La plantilla puede modificarse aún más tras su creación. La interfaz sólo muestra las partes de la configuración que se incluyeron al crear la plantilla.

1. Vaya a Dispositivos > Plantillas.
2. Seleccione una plantilla de la lista.
3. Haga clic en Editar plantilla.

Aparecerá un diálogo con las secciones de configuración.

Ajuste de valores

- El valor se ajusta haciendo doble clic.
- El elemento modificado se marca inmediatamente como modificado.
- El icono de advertencia ⚠ indica valores que pueden no pasar la validación completa en el dispositivo.

ATENCIÓN
La validación realizada al editar una plantilla es sólo indicativa, y se realiza **a nivel de artículo**. La comprobación no captura todos los conflictos entre dispositivos y versiones de firmware y no se corresponde con la validación completa que tiene lugar en **2N OS**.

Un artículo marcado con una advertencia puede seguir siendo utilizable en el aparato, y un artículo sin advertencia puede ser rechazado en la aplicación. La evaluación real tiene lugar en el dispositivo.

Aplicación de una plantilla a un dispositivo

La plantilla puede aplicarse a uno o varios dispositivos. También se puede aplicar mediante acciones masivas en la lista de dispositivos o directamente desde el detalle del dispositivo.

1. Vaya a Dispositivos > Plantillas.
2. Seleccione la plantilla que desea aplicar al dispositivo.
3. Haga clic en Aplicar al dispositivo.
4. Seleccione el dispositivo y confirme.
5. Aparecerá el resumen de la configuración. Estas secciones corresponden a las selecciones realizadas al crear la plantilla, pero pueden modificarse.
6. Haga clic en Aplicar.

ATENCIÓN

Si durante la aplicación de la plantilla se detecta un desajuste entre la versión de firmware o el tipo de dispositivo para el que se creó la plantilla y la versión o el tipo del dispositivo de destino, aparecerá un mensaje de advertencia. La discrepancia debe confirmarse antes de continuar.

NOTA

- El estado sólo confirma el inicio satisfactorio del proceso. No informa sobre el progreso real o la finalización de la solicitud.
- Para obtener instrucciones sobre cómo utilizar la plantilla al añadir un dispositivo, consulte Añadir un nuevo dispositivo (p. 61).

Reglas de acceso

Las reglas de acceso son una herramienta para gestionar claramente el acceso de grupos de usuarios a zonas. El acceso se puede otorgar en función de perfiles de tiempo.

Las reglas de acceso determinan QUIÉN tiene acceso, DÓNDE y CUÁNDO.

- **OMS** viene determinado por el grupo y los usuarios asignados al mismo (un usuario puede estar en varios grupos pertenecientes a una misma empresa al mismo tiempo).
- **DÓNDE** está determinado por la zona o los dispositivos (un dispositivo solo puede estar en una zona a la vez).
- **CUANDO**está determinado por el perfil de tiempo asignado. Este artículo es opcional. Un perfil de tiempo vacío significa acceso ilimitado (24 horas al día, 7 días a la semana).

NOTA
Un grupo puede tener acceso a varias zonas, así como varios grupos pueden tener acceso a una zona.

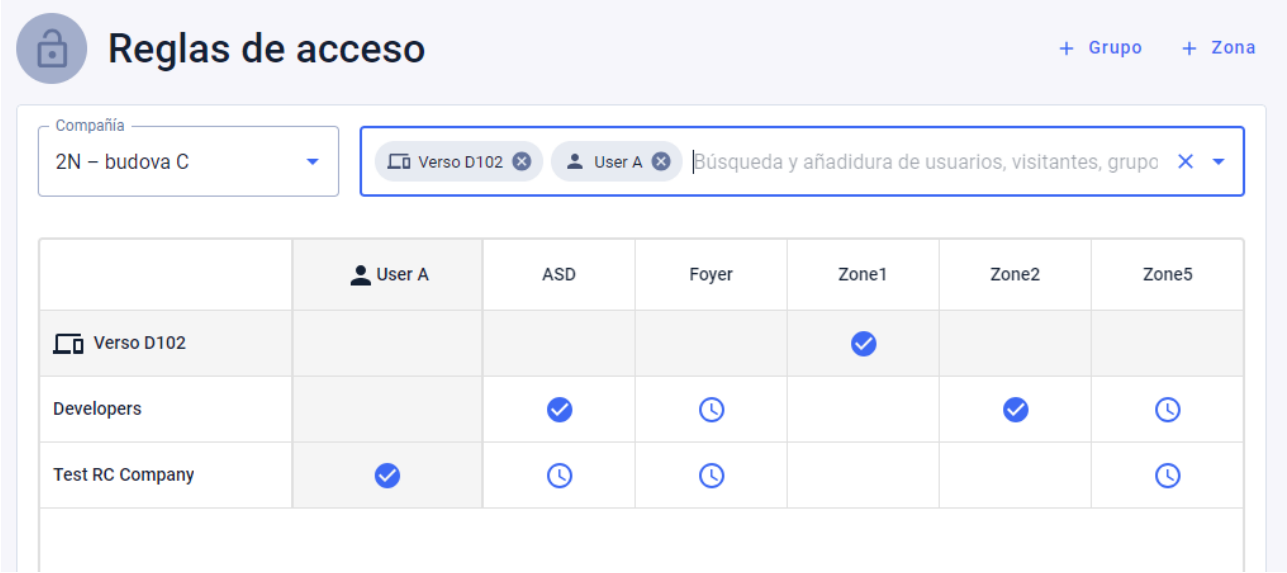
Visualización matricial

La vista matricial de las reglas en la página de reglas de acceso muestra una descripción general de los accesos y permite configurarlos. La matriz está disponible para cada empresa existente y muestra todos los grupos y zonas que tiene asignados. El administrador puede cambiar de empresa en el menú situado encima de la matriz.

Al hacer clic en la celda correspondiente a la zona y grupo seleccionados se establece el acceso del grupo a la zona. Aparecerá un menú en el que podrás elegir entre acceso ilimitado o acceso limitado por un perfil horario. Los perfiles de tiempo deben estar preestablecidos en la página. Perfiles de tiempo (p. 76). Si es necesario, se puede agregar un nuevo grupo o zona a la matriz de la empresa.

En el campo de búsqueda encima de la matriz, es posible agregar usuarios o dispositivos a la matriz. Los usuarios se pueden agregar a un grupo mediante la intersección de usuario y grupo. Al cruzar un dispositivo y una zona, los dispositivos se agregan a la zona.

Un ejemplo de visualización matricial



La imagen ofrece una visión general de la matriz de la empresa 2N Telekomunikace as. Del resumen se desprende claramente que:

- El dispositivo filtrado Verso 2.0 D102 forma parte de Zone1.
- El usuario filtrado Usuario A forma parte del grupo Test RC Company.
- Los usuarios del grupo Desarrolladores tienen acceso ilimitado a las zonas ASD y Zone2, acceso limitado a las zonas Foyer y Zone5 (según el perfil de tiempo establecido) y no tienen acceso a la zona Zone1.
- Los usuarios del grupo Test RC Company tienen acceso limitado a las zonas ASD, Foyer y Zone5 (según el perfil horario establecido) y no tienen acceso a las zonas Zone1 y Zone2.

Lista de reglas

La página Lista de reglas muestra una lista de todas las reglas de acceso válidas actualmente. Haga clic en la regla para editarla. Se puede agregar una nueva regla de acceso haciendo clic en el botón Agregar en la esquina superior derecha. Antes de crear, debe configurar los parámetros de la regla.

Tanto la lista de reglas como la matriz muestran las mismas reglas de acceso. Un cambio en una vista se copia automáticamente en la otra vista. Las reglas de acceso también se ajustan en la configuración de zona y configuración de grupo.

Perfiles de tiempo

Las funciones de intercomunicación seleccionadas pueden tener un límite de tiempo. A las funciones mencionadas se les puede asignar un llamado perfil de tiempo, que determina cuándo está disponible la función determinada.

Los perfiles de tiempo pueden abordar los siguientes requisitos:

- bloquear completamente las llamadas al usuario seleccionado fuera del tiempo reservado
- bloquear llamadas a números de teléfono seleccionados del usuario fuera del tiempo reservado
- bloquear el acceso de los usuarios fuera del tiempo asignado

Cada perfil horario define la disponibilidad de la función a la que está asociado mediante un calendario semanal. Puede configurar fácilmente el tiempo desde hasta y posiblemente días de la semana en los que la función debería estar disponible. La determinación del acceso mediante el perfil de tiempo se establece mediante reglas de acceso. La limitación de la disponibilidad del usuario fuera del perfil horario se establece junto con el número de teléfono del usuario.

Opcionalmente se pueden crear hasta 20 perfiles horarios generales que, además del control de acceso, también se pueden utilizar para casos especiales de configuración local. Estos perfiles de tiempo se cargan en todos los dispositivos sincronizados.

Perfiles temporales en cerraduras electrónicas

Las cerraduras electrónicas admiten perfiles horarios con las siguientes restricciones:

- No se aplican días festivos.
- Se pueden configurar hasta 4 intervalos de tiempo diferentes en un solo día.
- En un perfil temporal se pueden definir 4 horarios diarios de intervalos.

SUGERENCIA
Esto significa que puede tener, por ejemplo, una configuración diferente para el lunes, martes, miércoles y jueves, pero para el viernes, sábado y domingo debe utilizar una de las configuraciones existentes.

ATENCIÓN
Si el perfil temporal incumple las restricciones indicadas, se ignorará la regla de acceso y no se concederá acceso al usuario.

Creando un perfil de tiempo

1. Vaya a **Perfiles de tiempo**.
2. Haga clic en + Perfil de tiempo en la esquina superior derecha.
3. En el cuadro de diálogo abierto, establezca el nombre del perfil de tiempo.

4. Seleccione Añadir franjas horarias para seleccionar una restricción horaria. Los días resaltados en azul identifican los días que entran dentro del perfil horario. Para seleccionar un día, haga clic sobre él. Puede establecer un intervalo de tiempo dentro de los días para determinar la validez del perfil temporal.

   NOTA
   Puede fijar un intervalo de tiempo en días para determinar la validez del perfil temporal.

   ATENCIÓN
   Una vez creado el perfil horario, pueden fijarse diferentes horas para cada día.

5. El perfil de tiempo recién creado se agrega a la lista y se abre su detalle, en el que se pueden realizar más ajustes. En el detalle del perfil horario es posible configurar la posición del perfil en los dispositivos.

NOTA
Los perfiles globales pueden afectar al acceso en todas las empresas. Sólo el administrador puede editarlos.

Un administrador de acceso sólo puede corregir los perfiles horarios de su empresa.

Configurar el perfil de tiempo

El desglose de días y horas se muestra en el detalle del perfil horario. Los intervalos azules muestran cuando el perfil está activo. Se puede establecer cualquier número de intervalos dentro de un día.

El intervalo se agrega haciendo clic en la franja horaria y configurando la hora exacta en la que el perfil debe estar activo. El tiempo de un intervalo individual se puede cambiar haciendo clic en el intervalo. Si el perfil va a estar activo todo el día, se debe crear un intervalo que cubra todo el día, es decir, 00:00-23:59.

En el menú ampliado que se abre al hacer clic en ⋮ Se puede configurar la posición en el dispositivo. La posición en el dispositivo define la posición en la lista de perfiles de tiempo que se carga en todos los dispositivos a los que se asigna el perfil de tiempo.

La limitación de la disponibilidad del usuario fuera del perfil horario se establece junto con el número de teléfono en la configuración del usuario.

Asistencia

Access Commander permite el seguimiento de la asistencia de los usuarios. En el modo de asistencia se registran los tiempos de entrada y salida de usuarios individuales.

La configuración de la asistencia y los modos de asistencia se realiza en **Ajustes > Configuración > pestaña Asistencia**, véase Configuración de asistencia (p. 79).

ATENCIÓN
Para el correcto funcionamiento de la asistencia es necesario contar con **Access Commander**Licencia activa disponible para realizar un seguimiento de la asistencia de los usuarios. El seguimiento de asistencia debe activarse en la configuración de usuario individual.

La página de asistencia ofrece una lista de usuarios con asistencia registrada. Hay un icono en la esquina superior derecha. , con el que es posible descargar un archivo CSV con datos resumidos de la asistencia de todos los usuarios en el archivo CSV. Al descargar los datos, es necesario ingresar el período de tiempo para el cual se desea generar la asistencia.

Asistencia de un usuario específico

Puede seleccionar un usuario específico de la lista de usuarios en la página Asistencia y mostrar información más detallada solo sobre su asistencia. La lista muestra solo aquellos usuarios para quienes el seguimiento de asistencia está habilitado, consulte Usuarios (p. 49).

En la parte superior del estado de cuenta, puede seleccionar el mes del cual desea mostrar la asistencia. Al lado de la selección del mes se muestra el fondo de trabajo establecido para el mes determinado, el saldo y las horas trabajadas.

Hay un menú de expansión al lado del nombre del usuario. permitiendo la descarga de datos sobre la asistencia del usuario mostrado en un archivo CSV o PDF. Ambos archivos contienen registros de días individuales.

SUGERENCIA
También es posible ver la asistencia del usuario en los detalles del usuario, al que se puede acceder seleccionándolo de la lista de usuarios en la página. **Usuarios**.

Cambiar asistencia de usuario

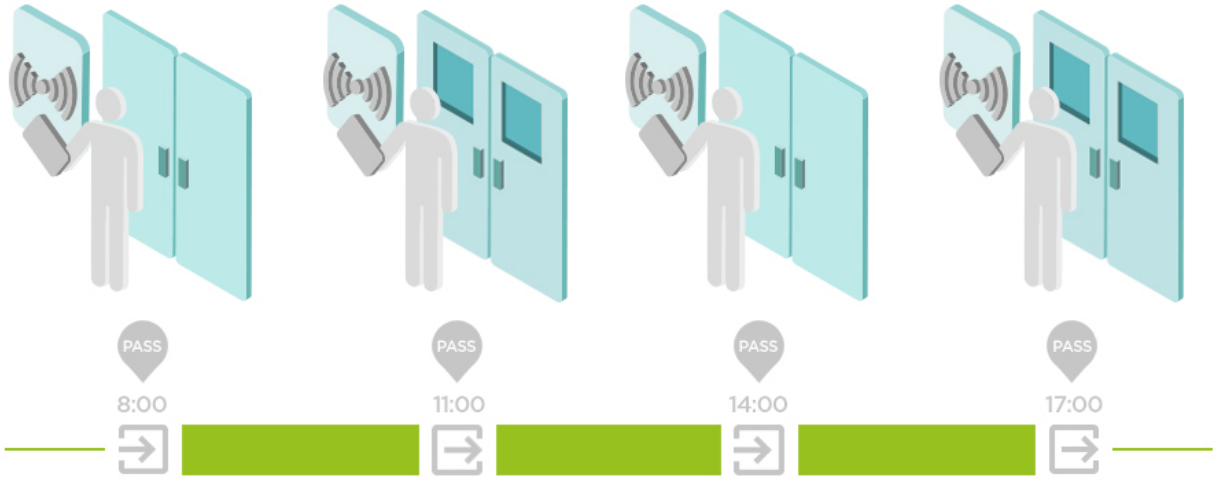
El administrador de asistencia puede editar los datos de asistencia del usuario. La edición se realiza haciendo clic en el intervalo de tiempo que se va a cambiar. Una vez abierto, se pueden editar los tiempos límite y se puede agregar una nota al intervalo.

Configuración de asistencia

Access Commander permite el seguimiento de la asistencia de los usuarios. En el modo de asistencia se registran los tiempos de entrada y salida de usuarios individuales.

Modos de asistencia

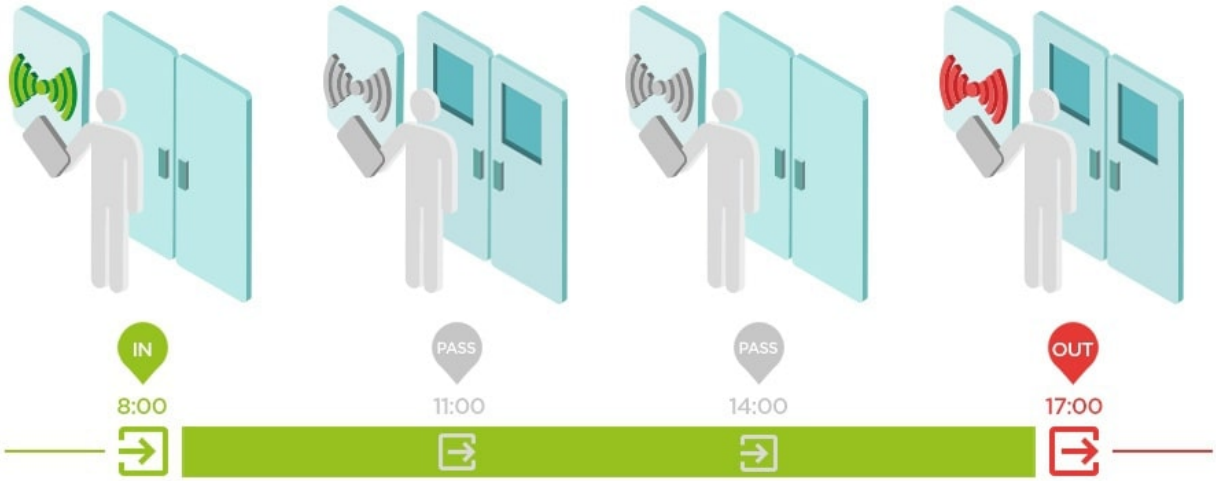
- **GRATIS**



Las llegadas y salidas se cuentan desde la primera y última autenticación de usuario en cualquier dispositivo en un día. El módulo de presencia no funciona en este modo.

- **EN FUERA**

Para que funcione correctamente, el dispositivo debe estar preparado para entrar y salir de la zona.



- **ENTRADA-SALIDA para todos los dispositivos**
  Este modo permite el control de presencia. Las llegadas se registran en los dispositivos entrantes y las salidas se registran en los dispositivos salientes. El movimiento entre zonas no se registra como llegada/salida.
- **IN-OUT para dispositivos seleccionados**
  Este modo permite el control de presencia. Las llegadas y salidas se registran en dispositivos seleccionados que están configurados como llegadas o salidas. Las llegadas y salidas se registran únicamente en estos dispositivos seleccionados. De este modo, el registro de llegada/salida se puede establecer, por ejemplo, sólo en la entrada principal del edificio.

Configuración del punto de acceso del dispositivo

Puede dividir lógicamente cada dispositivo en dos puntos de acceso: de llegada y de salida. Cada punto de acceso representa un paso en una dirección y determina si el usuario del dispositivo entra o sale de la

zona. Un punto de acceso puede ser controlado por uno o varios módulos de dispositivo. Todos los módulos asignados gestionan entonces los pasillos en la dirección del punto de acceso específico. Los puntos de acceso se utilizan especialmente en situaciones en las que un dispositivo se encuentra en el límite de dos zonas y es necesario registrar con precisión la dirección del movimiento entre ellas (por ejemplo, para funciones anti-retorno).

Los puntos de acceso también se utilizan para realizar un seguimiento de los usuarios en el módulo Presencia (p. 84). Los puntos de acceso también se utilizan para realizar un seguimiento de las entradas y salidas en Restricciones de área (p. 86).

NOTA
En la interfaz de configuración web de cada dispositivo, los puntos de acceso se denominan **Llegada** y **Salida**. Para configurarlas, vaya a **Acceso > Reglas de acceso > Solapa Acceso y salida**.

Habilitación de puntos de acceso en Access Commander

1. Ir a la página de Zonas v **Comandante de acceso**.
2. En la esquina superior derecha, presione y habilitar el uso de puntos de acceso.

Asignación de módulos para la llegada o la salida

1. Acceda a la interfaz de configuración basada en web para el dispositivo.

SUGERENCIA
Puede acceder a la interfaz de configuración basada en web haciendo clic en en la lista de la página Dispositivos.

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

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

Visitas

En **Access Commander**es posible crear perfiles de visitantes que tengan privilegios de acceso por un tiempo limitado. Durante la visita es posible añadir una tarjeta de acceso, un código de acceso y rellenar la matrícula del vehículo. No se computará la asistencia a la visita. El número de visitas no está limitado por ninguna licencia.

Configurar la retención de datos de visitantes

El administrador puede establecer el período de retención de los datos de los visitantes. El plazo de conservación de los datos de los visitantes se establece en días haciendo clic en el icono  al lado del botón para crear una nueva visita.

Una vez transcurrido el intervalo de tiempo de la visita y el período de retención de datos establecido, las visitas se eliminan automáticamente cada medianoche. Las visitas a las que todavía se les asignen tarjetas de visitante no se eliminarán.

NOTA
Se pueden utilizar configuraciones para cumplir con las regulaciones locales de protección de datos. El nombre de la visita y la nota se conservarán en el registro de acceso de acuerdo con la configuración de duración en la gestión de registros.

Creando una nueva visita

1. ir a la pagina **Visitas**.
2. Haga clic en el botón Agregar visita en la esquina superior derecha.
3. En la ventana de diálogo que se abre deberás rellenar el nombre de la visita, seleccionar el grupo visitado y establecer el inicio y el final de la visita. Si no establece el inicio y el final de la visita, el intervalo de tiempo para el acceso de la visita comenzará inmediatamente y finalizará al final del día.

   ATENCIÓN
   El intervalo de tiempo para las visitas de acceso no será superior a 90 días.

4. Antes de crear una visita, puede configurar los métodos de autenticación que utilizará la visita para acceder.
   La visita recién creada aparece en la lista. En los detalles de la visita es posible agregar métodos de autenticación a la visita y gestionar su acceso.

Fin de la visita

Transcurrido el intervalo de tiempo, el acceso caducará para la visita.

Si el administrador o administrador finaliza la visita mediante el botón Fin en la pestaña Acceso en la configuración de la visita, el acceso de esta visita se bloqueará inmediatamente. Un botón Detener está disponible para un visitante cuya visita haya finalizado automáticamente porque la zona horaria puede ser diferente en los dispositivos. Puede suceder que, aunque un visitante no tenga acceso válido en un dispositivo, sí lo tenga en otro. Esto sucede si se configuran diferentes zonas horarias para el dispositivo.

Si se ha asignado una tarjeta de visitante a una visita, la tarjeta se desvinculará y podrá utilizarse para otra visita.

Visitar configuración

La información sobre la visita se puede ver y editar en los detalles de la visita. Los detalles de la visita se abren haciendo clic en la visita seleccionada en la lista.

Enfoques

La pestaña de accesos muestra el grupo de acceso y el intervalo de tiempo durante el cual la visita tiene acceso válido. El intervalo de tiempo para el acceso a la visita se puede configurar nuevamente eligiendo Restablecer visita en el menú ampliado ⋮ .

En esta pestaña es posible finalizar la visita, ver Fin de la visita (p. 81).

Visita

La tarjeta muestra la persona visitada y la empresa visitada. Es posible cambiar la persona visitada.

En esta pestaña es posible añadir una nota a la visita.

Información personal

La tarjeta muestra los datos de contacto de la visita y permite modificarlos. El correo electrónico configurado permite el envío de códigos de autenticación.

Autenticación

Durante la visita es posible añadir una tarjeta de acceso, PIN de acceso o código QR y rellenar la matrícula del vehículo. Sólo es posible rellenar una matrícula por visita. Es posible asignar una tarjeta de acceso de visitante a la visita, ver Tarjetas (p. 82).

Al completar la dirección de correo electrónico, es posible enviar el código PIN/QR de acceso generado a la dirección indicada.

La tarjeta de visitante asignada se puede devolver aquí.

Registro de acceso

El registro de acceso muestra el historial de acceso.

Tarjetas

La página Tarjetas se utiliza para gestionar las tarjetas de acceso de los visitantes que están disponibles para añadir una visita. Una nueva tarjeta se añade utilizando el botón de añadir situado en la esquina superior derecha.

Las tarjetas siempre deben estar asignadas a una empresa. La tarjeta sólo se podrá utilizar para visitas que vayan a realizar a esta empresa.

Una tarjeta existente se puede sobrescribir o eliminar seleccionándola en el menú extendido ⋮ .

ATENCIÓN
Una tarjeta asignada a una visita activa no se puede eliminar.

NOTA
Si **Access Commander** informa que la tarjeta nueva que acaba de agregar ya está en uso en el sistema, la razón puede ser que el modo de compatibilidad de tarjetas RFID está habilitado. El administrador habilita este modo en **Configuración > Autenticación > ficha Configuración del modo de compatibilidad**.

Gestión de una tarjeta segura con un lector USB

El lector USB puede utilizarse para diagnosticar y gestionar la tarjeta segura en el campo de búsqueda de la cabecera.

SUGERENCIA
Antes de utilizar el lector USB, debe estar habilitado en **Access Commander**. Para más información, consulte Lectores USB habilitados (p. 109).

1. Conecte el lector USB a su ordenador.
2. Haga clic en el icono en el cuadro de búsqueda de la cabecera.
3. Adjuntar al lector.

Operaciones disponibles

- Recuperar datos de la tarjeta
- Buscar un usuario por tarjeta
- Para ver los eventos almacenados en la ficha
- Actualización de los datos de acceso
- Borrar o formatear una aplicación
- Ampliación de la tarjeta de servicio

Presencia

El módulo **Presencia** le permite supervisar la actividad de los usuarios en tiempo real. Funciona independientemente del módulo **Asistencia**, cuya licencia se adquiere por separado. Se puede supervisar la asistencia incluso sin una licencia de Asistencia activa.

Las dos funciones aparecen juntas en las pestañas **Asistencia y presencia** de la interfaz de Access Commander, pero cada una tiene su propia finalidad y funciona de forma independiente.

Para que el módulo funcione, debe configurar el modo de asistencia IN-OUT en **Ajustes > Configuración > pestaña Asistencia**, consulte Configuración de asistencia (p. 79).

- Si el último evento del usuario en un día determinado es una llegada (**IN** evento), se toma como presente.
- Si un usuario pasa por un lector que está configurado en una dirección no especificada, la zona del usuario cambiará. Lo mismo ocurre si pasa por un lector en modo **IN**.
- Si el último evento del usuario en un día determinado es un cierre de sesión (evento **OUT**), se le tratará como ausente.

ATENCIÓN
El módulo de asistencia no funciona si se utiliza el modo GRATIS dentro del sistema de seguimiento de asistencia. Sólo se pueden utilizar configuraciones IN-OUT.

Caducidad de la presencia del usuario

Haga clic en el icono en la parte superior derecha, se establece la Caducidad de presencia del usuario. La expiración de la presencia del usuario establece la eliminación automática del registro de presencia del usuario si el usuario olvida marcar su salida. Este límite de tiempo se expresa en horas y determina cuánto tiempo después del último paso del usuario actual, su registro de presencia se eliminará automáticamente. Establecer este límite de tiempo le permite definir cuánto tiempo puede permanecer un registro de presencia en el sistema si el usuario no está marcado como ausente. Esto garantiza que la lista de usuarios actuales permanezca actualizada y no contenga registros de usuarios que ya abandonaron el edificio y olvidaron cerrar sesión.

Informes

Es posible descargar datos resumidos sobre usuarios agregados desde la página Informes. Los archivos descargados están en formato CSV (valores separados por comas). El nombre del archivo siempre indica la fecha y hora en que se generó el informe.

NOTA
Algunos programas de hojas de cálculo utilizan diferentes separadores y es posible que el archivo CSV no se muestre correctamente cuando se abre en ellos. En tales casos, se recomienda importar los datos del archivo CSV a un libro abierto.

- **My2N app** – Usuarios emparejados y no emparejados con tiempo de emparejamiento restante
  El informe enumera datos sobre el estado del emparejamiento de usuarios a través de la aplicación. My2N app, o datos sobre el período de validez del código de emparejamiento activo.
- **Usuarios** – Reglas de acceso con grupos, zonas, dispositivos y perfiles horarios.
  El informe enumera datos sobre la asignación de usuarios a grupos, su acceso a zonas y dispositivos en las zonas, y los perfiles de tiempo en los que se permite el acceso a los usuarios. Cada combinación aparece exactamente en una fila de la tabla.
- **Usuarios** – Exportación detallada
  El informe enumera toda la información sobre los usuarios que se completa en sus perfiles, incluidos sus datos personales y de acceso.

  ATENCIÓN
  ¡El archivo contiene datos confidenciales!
- **Usuarios** – Exportación de sincronización global
  El informe enumera datos sobre la asignación de usuarios a grupos, su acceso a zonas y dispositivos en las zonas, y los perfiles de tiempo en los que se permite el acceso a los usuarios. Cada combinación aparece exactamente en una fila de la tabla.
  Este informe puede servir como un archivo CSV para la sincronización de usuarios, consulte Sincronización de usuarios con FTP (p. 94).

  ATENCIÓN
  ¡El archivo contiene datos confidenciales!

Restricciones de área

Utilice las restricciones de área para definir las áreas en las que se pueden usar las funciones de ocupación y antipaso.

NOTA
El módulo de restricciones de área y el módulo de presencia (incluida la asistencia) son independientes entre sí. En los módulos de asistencia y presencia no se pueden usar los módulos de ocupación y antipase. La ocupación y la antitransferencia solo funcionan en el modelo de restricciones de

Establecer restricciones de área

Se agrega un nuevo dispositivo al área usando el botón en el encabezado de detalles del área.

Entrada y salida

Estas tarjetas indican qué dispositivos se enrutan como entrada o salida en un área determinada. Usando el menú extendido en ⋮ Los dispositivos se pueden mover entre pestañas o quitar del área.

Al autenticar al usuario en el dispositivo de entrada, se registra la entrada al área. Al autenticar al usuario en el dispositivo de salida, el usuario abandona el área. Con esto, es posible monitorear si el usuario todavía se encuentra en el área y si desea volver a ingresar a ella.

Si el dispositivo agregado tiene dos puntos de acceso configurados, cada punto se puede usar para una dirección diferente (Entrada/Salida). La configuración del punto de acceso se describe en el capítulo Configuración del punto de acceso del dispositivo (p. 79). Las propiedades del punto de acceso se expanden al hacer clic en la flecha.

Ocupación

Para que funcione correctamente, el dispositivo debe estar preparado para entrar y salir de la zona.

La pestaña de ocupación proporciona una descripción general del número de personas en el área y te permite establecer límites de ocupación. Si se alcanza el límite de ocupación, es posible denegar entradas adicionales o registrar solo estas entradas en el registro del sistema. La función de ocupación no registra qué personas hay en la zona. Un módulo de presencia independiente está diseñado para monitorear la presencia de personas individuales

ATENCIÓN
Al autorizar a un usuario repetidamente, cada autorización cuenta como una entrada. Esto significa que si un usuario se registra tres veces consecutivas en el dispositivo de entrada, se contabilizarán como tres personas en la zona. Por lo tanto, si la instalación física del dispositivo permite retirar repetidamente la tarjeta de un solo usuario, es aconsejable combinar la función de ocupación con la función anti-passback.

Anti-passback

Para que funcione correctamente, el dispositivo debe estar preparado para entrar y salir de la zona.

Es posible activar la función anti-retorno en la zona, que garantiza la ampliación del control de acceso mediante la vigilancia y la prevención de la no utilización de los derechos de reingreso a las zonas reservadas. Las zonas a vigilar están definidas por los dispositivos de delimitación que dan entrada o salida a las zonas. En estos dispositivos, se comprueba si el paso de las personas está autorizado de acuerdo con las normas definidas para la zona. Después de salir del área a través de un dispositivo delimitador, el usuario sólo puede volver al área después de un tiempo de espera, si se ha establecido un tiempo de espera. Si el usuario intenta volver al área antes, el sistema deniega el acceso o simplemente registra el suceso.

AVISO

- La zona anti-retorno pierde su sentido y se vuelve potencialmente peligrosa si hay un dispositivo en la zona que tenga conectado un botón REX activo que permita el acceso no autorizado.

Establecer una excepción

A veces puede ser conveniente que las condiciones anti-passback no se apliquen a determinados usuarios. Normalmente, se trata de usuarios como el administrador del edificio, el director general, usuarios VIP, etc. Los usuarios o grupos enteros que no deben estar sujetos a las condiciones de anti-retorno se configuran en **Configuración > Anti-retorno > Excepciones**.

NOTA
La sección Configuración solo está disponible para usuarios con rol de administrador.

Lista de usuarios bloqueados

Los usuarios bloqueados son aquellos que intentaron acceder al área anti-passback antes de que expirara el tiempo de espera. Utilizando ✕, se puede excluir a los usuarios de la lista y permitirles acceder de nuevo al área.

SUGERENCIA
Cuando se deniega el acceso a un usuario debido a un anti-passback activo, se le puede enviar un correo electrónico informativo automatizado. Para habilitar el envío del correo electrónico, vaya a **Configuración > Antipassback > pestaña de notificación** por correo electrónico de usuario bloqueado.

Restablecer restricciones

La pestaña **Configuración > Anti-retorno > Restablecer restricciones de área** establece los días y horas en los que se borrará el registro de área, es decir, todos los usuarios podrán volver a pasar independientemente de las infracciones de las reglas anteriores.

Estas medidas mejoran el nivel de protección y previenen posibles amenazas a la seguridad. Más específicamente, ayudan a prevenir el acceso no autorizado a ubicaciones seleccionadas, permiten rastrear el movimiento de las personas dentro de un espacio determinado y registran entradas y salidas, lo que puede ser útil para monitorear y analizar eventos de seguridad.

La lista muestra las áreas creadas en el sistema. En esta pestaña, se pueden crear, eliminar áreas y acceder a sus detalles. Al mismo tiempo, permite desactivar el área y mostrar su estado.

Crear un área de restricción

1. ir a la pagina **Restricciones de área**.
2. Haga clic en el botón para agregar una región en la esquina superior derecha.
3. En el cuadro de diálogo abierto, asigne un nombre al área.
4. En el detalle del área abierta, agregue un dispositivo al área. Los dispositivos se agregan usando el botón en el encabezado de detalle del área.
   El área recién creada aparecerá en la lista. En sus detalles, es posible configurar los dispositivos de entrada y salida, configurar la ocupación permitida, activar la función anti-passback y bloquear el acceso al área para usuarios seleccionados.

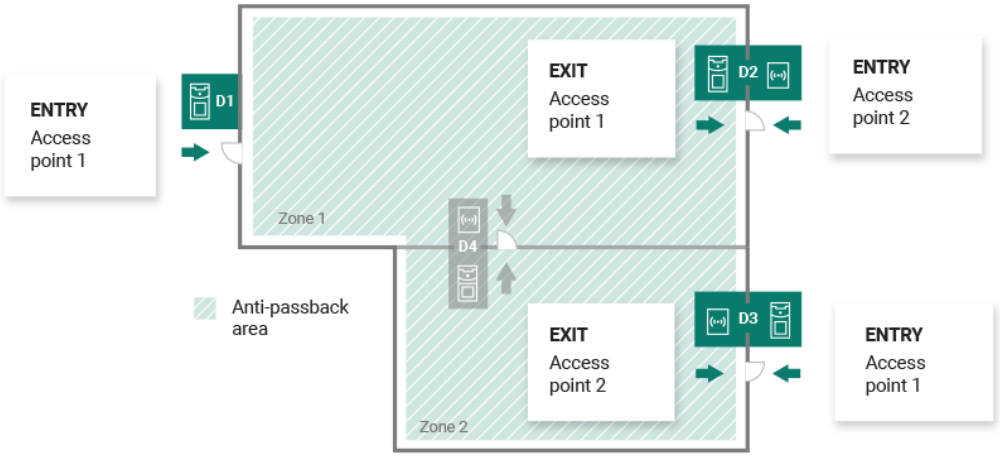
Los errores de configuración más comunes

ATENCIÓN
Si ocurre un error en un área, se desactivará toda el área. Se activará nuevamente después de que se eliminen los errores.

Los siguientes casos pueden impedir que las restricciones regionales funcionen correctamente

- No se agrega ningún dispositivo al área. Se debe asignar al menos un dispositivo.
- Algún dispositivo de entrada/salida no está configurado correctamente o no contiene lector.
- Algún dispositivo de entrada a esta área ya se utiliza como entrada a otra área. Es necesario modificar la asignación para que funcione correctamente.
- Algunos equipos no están equipados con la licencia necesaria.
- Algunos dispositivos han sido desactivados.
- Algún dispositivo ha sido desconectado.
- Algunos dispositivos no tienen una versión de firmware compatible.
  Algunos dispositivos están equipados con un botón REX que permite salir del área APB sin autorización del usuario. Para un funcionamiento correcto, el botón REX debe estar desactivado.

Un ejemplo de establecimiento de restricciones.



La figura muestra un área Anti-passback con tres dispositivos fronterizos D1, D2 y D3. Sólo se utilizan dispositivos de borde para configurar la función Anti-passback. El dispositivo D4 dentro del área Anti-passback no se utiliza para controlar la entrada/salida del área. Los dispositivos D2 y D3 tienen direcciones de entrada y salida configuradas.

Dispositivo D1 solo se usa para ingresar al área Anti-passback. El dispositivo está configurado como entrada.

Dispositivo D2 Sirve tanto para entrada como para salida. El dispositivo tiene un módulo de expansión configurado para ingresar al área y una unidad principal configurada para salir.

Dispositivo D3 Sirve tanto para entrada como para salida. El dispositivo tiene una unidad principal configurada para ingresar al área y un módulo de expansión configurado para salir.

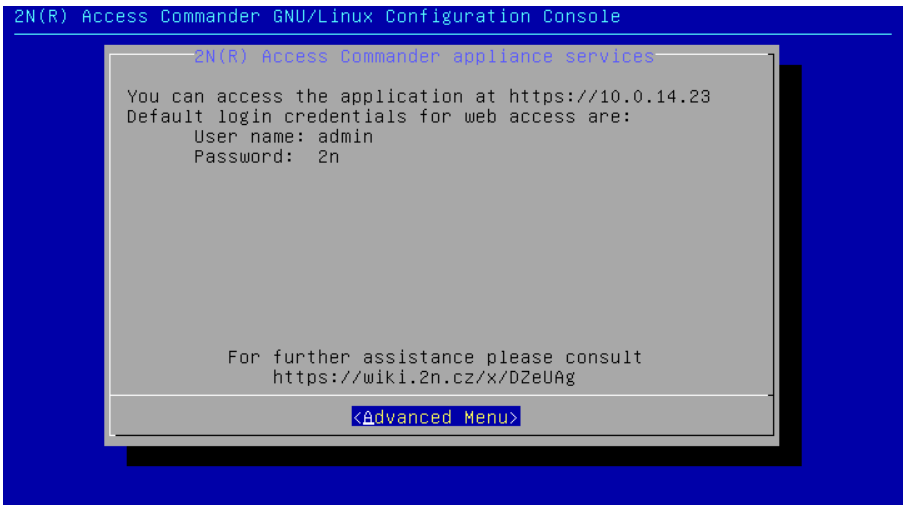
Ajustes del sistema

Configuración de Linux

La configuración básica del sistema se puede realizar en la consola de configuración de Linux.

NOTA
si esto es **Access Commander** distribuido a través de una máquina virtual, es posible conectarse a la versión de Linux de forma remota a través de una conexión SSH.

La consola de configuración se abre iniciando sesión en **Access Commander** usando la cuenta raíz. La página de inicio muestra información básica sobre el acceso del administrador a la interfaz web y redirige al Menú Avanzado.



En el Menú Avanzado es posible configurar:

- **Redes**
  Configuración del servidor proxy, propiedades de red, opciones de sincronización con el servidor DHCP.
- **Timo**
  Configuración manual de hora, servidor NTP y configuración de zona horaria

- **SSH**
  Configura una conexión remota a **Access Commander** vía SSH. Para habilitar SSH, se debe establecer una contraseña distinta a la predeterminada que cumpla con los requisitos para su dificultad.
- **PYME**
  Inicia el asistente para configurar conexiones a carpetas compartidas. Establece la dirección IP o el nombre de dominio y la ruta de la carpeta. P.ej. "192.168.1.1/acción". Para la configuración, es necesario especificar el nombre de usuario del usuario que obtendrá acceso a la carpeta dada y el derecho a escribir. Es necesario completar la contraseña del usuario y seleccionar la versión del protocolo Samba. Después de completar todos los pasos obligatorios, se verificará la conexión al servidor y se mostrará información sobre si la configuración fue exitosa o fallida.
- **Contraseña**
  Permite cambiar la contraseña del usuario root del sistema para iniciar sesión en la consola o acceder vía SSH.

  NOTA
  El cambio de la contraseña de root se realiza en la consola de configuración, no en Access Commander.
- **Copia de seguridad y restaurar**
  Se utiliza para importar datos y configuraciones, configurar copias de seguridad repetidas y restaurar desde copias de seguridad anteriores.

Actualizacion del sistema

Sistema **Access Commander** comprueba periódicamente el servidor de actualizaciones e informa sobre las actualizaciones disponibles y las nuevas versiones de firmware disponibles para los dispositivos conectados. La verificación de actualización automática se puede desactivar en la pestaña **Configuración > pestaña Actualización del sistema**.

Instalar la actualización Access Commander

AVISO
Se recomienda hacer esto antes de instalar la actualización. copia de seguridad del sistema (p. 92). Realizar la copia de seguridad fuera del horario comercial para evitar la indisponibilidad temporal del sistema para los usuarios.

1. Ir a **Configuración > pestaña Actualización del sistema**.
2. Si la comprobación automática de actualizaciones está desactivada, haga clic en Buscar actualizaciones.
3. Haga clic en Descargar en el mensaje de información de actualización disponible y confirme la descarga.
   La pestaña informa que la actualización está lista para instalarse.
4. Haga clic en Instalar en el mensaje informativo y en el cuadro de diálogo abierto, confirme la instalación.
   Después de iniciar la instalación, será redirigido a la página de mantenimiento. La página de mantenimiento informa al administrador que inició la instalación sobre el estado actual de la instalación. Muestra información a otros usuarios de que hay una actualización en curso. Durante la instalación, no es posible**Access Commander**inscribirse.
5. Una vez completada la instalación, haga clic en Ir a iniciar sesión, que le redireccionará a la página de inicio de sesión.

Dominios necesarios para las actualizaciones del sistema

ATENCIÓN
Conectar el 2N Access Commander a los servidores que se indican a continuación es esencial para que la actualización del sistema se realice correctamente. Sin el acceso a estos dominios habilitado, el proceso de actualización fallará y el sistema no se actualizará.

Este acceso es fundamental para descargar las últimas versiones de las aplicaciones, los paquetes del sistema, los parches de seguridad y otros componentes que mantienen su sistema en un estado óptimo y seguro.

- .2n.cz
- .2n.com
- .deb.nodesource.com
- .packages.microsoft.com
- .security.debian.org
- .apt.postgresql.org
- .httpredir.debian.org

Downgrade
No es posible volver a una versión anterior del firmware.

Pruebas beta
Los usuarios pueden optar por participar en pruebas beta de actualizaciones de software. **Access Commander** antes del lanzamiento oficial de las actualizaciones. La autorización se realiza en **Configuración > pestaña Actualización del sistema > parámetro Servidor de actualización**.

AVISO
La versión de prueba no está garantizada y la empresa no la proporciona. 2N TELEKOMUNIKACE a.s. como no es responsable de las limitaciones funcionales y posibles daños que surjan como resultado de las limitaciones funcionales de la versión beta. Las versiones Beta se proporcionan únicamente con fines de prueba. La versión beta no está diseñada para trabajar con datos importantes.

Una vez habilitadas, las versiones beta aparecerán en las actualizaciones disponibles en la pestaña Actualizaciones del sistema.

AVISO
Después de la actualización **Access Commander** la última versión beta no se puede degradar a una versión anterior.

Copia de seguridad del sistema
Desde la ficha **Configuración > Respaldo del sistema**, puede realizar, configurar y controlar el respaldo y la recuperación de datos de **Access Commander**. Los datos se pueden almacenar en el almacenamiento

local o en un bloque de mensajes del servidor (SMB). El SMB es adecuado para el almacenamiento de copias de seguridad a largo plazo.

Se puede realizar una copia de seguridad de los datos una vez o automáticamente a intervalos regulares preestablecidos.

Cada copia de seguridad se puede restaurar, descargar o eliminar en el menú que se expande después de hacer clic en ⋮ para un elemento en la lista de respaldo.

Copia de seguridad de datos única

1. Ve a **Configuración > pestaña Copia de seguridad del sistema**.
2. En la parte inferior de la pestaña, haga clic en Copia ahora.
3. Seleccione si desea cifrar los datos del archivo. Si es así, complete la contraseña que se le solicitará para restaurar la copia de seguridad.

Configuración de copia de seguridad automática de datos

1. Ve a **Configuración > pestaña Copia de seguridad del sistema**.
2. Haga clic en ✎ en el parámetro Copia de seguridad regular.
3. Establezca los parámetros de copia de seguridad necesarios:
   - frecuencia: el intervalo que especifica la frecuencia con la que se realizará la copia de seguridad
   - hora: la copia de seguridad se realizará el día correspondiente a esta hora
   - día – día de la semana o mes en el que se realizará la copia de seguridad
4. Seleccione si desea cifrar los datos del archivo. Si es así, complete la contraseña que se le solicitará para restaurar la copia de seguridad.
5. Al guardar, las copias de seguridad se realizarán automáticamente según la configuración seleccionada.

Configuración de copia de seguridad de datos en SMB

1. Ve a **Configuración > pestaña Copia de seguridad del sistema**.
2. Haga clic en ✎ en el parámetro Almacenamiento.
3. Seleccione el tipo de almacenamiento: SMB.
4. Complete la dirección del servidor, la información de inicio de sesión y la versión del protocolo.
5. Al guardar, todas las copias de seguridad se enviarán al bloque de mensajes del servidor configurado.

Restaurar desde datos de respaldo

1. Ve a **Configuración > pestaña Copia de seguridad del sistema**.
2. Abrir el menú extendido ⋮ en la copia de seguridad seleccionada y seleccione ⟲ Restaurar.

Restaurar desde un archivo de copia de seguridad

1. Ve a **Configuración > pestaña Copia de seguridad del sistema**.
2. En la parte inferior de la pestaña, haga clic en Restaurar desde archivo.
3. Seleccione el archivo de copia de seguridad de su almacenamiento y haga clic en Restaurar.

Transferir datos de otro Access Commander

1. Ve a **Configuración > pestaña Copia de seguridad del sistema**.
2. En la parte inferior de la pestaña, haga clic en Emigrar.
3. Ingrese la dirección IP del Access Commander desde el cual desea transferir los datos.
4. Complete las credenciales de la cuenta de administrador de Access Commander desde la cual desea transferir los datos.

ATENCIÓN
Para importar datos desde otro Access Commander, el servicio SSH debe estar habilitado en el servidor desde el cual se descargarán los datos.

Sincronización de usuarios con FTP

La lista de usuarios y sus configuraciones básicas, incluidas las asignaciones a empresas y grupos, se pueden sincronizar mediante un archivo CSV mantenido externamente.

La sincronización se realiza en **Configuración > pestaña Sincronización de usuario**. Es posible descargar un archivo CSV de muestra desde la tarjeta (en el menú extendido ⋮).

SUGERENCIA
La lista de usuarios actuales, que corresponde a la estructura del archivo CSV de muestra, se puede descargar desde la página Informes (p. 85).

El archivo CSV preparado se puede importar directamente a la tarjeta. Datos del archivo con s **Access Commander** comenzarán a sincronizarse automáticamente.

La información detallada sobre el resultado de cada sincronización se almacena en el registro del sistema. El registro en sí contiene información básica sobre el éxito o el fracaso de la sincronización. La información detallada se almacena en un archivo que se puede descargar usando el icono al final de la línea.

Sincronización automática de usuarios con FTP

La pestaña Sincronización de usuarios en Configuración le permite vincular **Access Commander** con el almacenamiento FTP donde se encuentra el archivo CSV con la lista de usuarios. Luego, la pestaña muestra información sobre este almacenamiento FTP.

1. Vaya a **Configuración > pestaña Sincronización de usuario**.
2. Haga clic en ✎ en el parámetro Almacenamiento.
3. En el cuadro de diálogo abierto, configure la dirección del servidor FTP donde está almacenado el archivo CSV.
4. La activación de TLS habilita la seguridad de la capa de transporte (TLS) para la conexión FTP. TLS cifrará los datos transmitidos entre **Access Commander** y el servidor.
   Habilitar autenticación de certificados TLS para habilitar la autenticación TLS de los certificados proporcionados por el servidor. Cuando se habilita, **Access Commander** verificará que se está comunicando con un servidor de confianza, lo que aumenta la seguridad de la conexión.

   ATENCIÓN
   No se admite proxy para FTP con autenticación TLS.
5. Ingrese las credenciales para acceder al servidor FTP.

Archivo CSV

NOTA
Algunos programas de hojas de cálculo utilizan diferentes separadores y es posible que el archivo CSV no se muestre correctamente cuando se abre en ellos. En tales casos, se recomienda importar los datos del archivo CSV a un libro abierto.

Un archivo CSV tiene una estructura determinada que debe seguirse. Todos los valores están separados por una coma, solo la lista de grupos está separada por un punto y coma. El archivo CSV tiene la siguiente estructura:

- EmployeeID: clave principal que debe completarse. Este es un identificador de usuario único.
- User Name: el nombre del usuario creado en Access Commander.
- Company: el nombre de la empresa bajo la cual se constituirá el usuario. La empresa debe estar creada en Access Commander. Las letras minúsculas y mayúsculas utilizadas en los nombres de empresas o grupos no son intercambiables.
- User Mail: dirección de correo electrónico del usuario.
- Card Numbers: el número de tarjeta del usuario. Se pueden configurar hasta dos tarjetas para un usuario. Los números de las tarjetas individuales deben estar separados por punto y coma (;).
- Switch Code: un código de cambio, siempre se crea un código bajo el primer interruptor.
- Phone Number 1: número de teléfono en la primera posición.
- Group Call: llamada grupal al número de teléfono establecido anteriormente. Toma los valores True/False. Cuando se establece en Verdadero, se activan las llamadas grupales. Cuando se establece en Falso, las llamadas grupales están deshabilitadas.
- Phone Number 2: número de teléfono en la segunda posición.
- Group Call: llamada grupal al número de teléfono establecido anteriormente. Toma los valores True/False. Cuando se establece en Verdadero, se activan las llamadas grupales. Cuando se establece en Falso, las llamadas grupales están deshabilitadas.
- Phone Number 3: número de teléfono en la tercera posición.
- Virtual Number: número virtual del usuario.
- Groups: lista de grupos a los que se debe agregar el usuario. Todos los grupos deben establecerse en **Access Commander**. La lista de grupos está separada por un punto y coma. Las letras minúsculas y mayúsculas utilizadas en los nombres de empresas o grupos no son intercambiables.
- Is Deleted: indica si el usuario debe eliminarse. Cuando se establece en FALSO, se crea el usuario y solo se actualizan sus datos durante la siguiente sincronización. Si se establece en TRUE, el usuario se elimina en la siguiente sincronización. Si se establece en FALSO, el usuario se creará nuevamente.
- License Plates: marcas de registro. Es posible configurar varias matrículas, que deben estar separadas por un punto y coma.

Fecha y hora

Para cambiar el método de recuperación de la hora, vaya a **Ajustes > Configuración > pestaña Fecha y hora**.

La fecha y la hora de **Access Commander** pueden sincronizarse con Internet o configurarse manualmente. Si **Access Commander** no está conectado a Internet, debe configurar la fecha, la hora y la zona horaria manualmente. De lo contrario, es posible cambiar a NTP y obtener la hora del servidor NTP. En este caso, sólo es necesario configurar la zona horaria. El servidor NTP actualiza la fecha y la hora automáticamente.

ATENCIÓN
Después de guardar el cambio de hora se **Access Commander**se reinicia automáticamente.

Sincronización horaria con dispositivos

La hora de los dispositivos conectados puede sincronizarse con la hora de **Access Commander**. El uso compartido de la hora con los dispositivos se activa al alternar el parámetro Sincronización de dispositivos en **Ajustes > Configuración > ficha Fecha y hora**.

Si la sincronización horaria con el dispositivo está activada, es posible elegir entre los siguientes métodos de sincronización:

- **Los dispositivos utilizan el mismo servidor NTP.** – la hora en los dispositivos se rige por el servidor NTP configurado en **Access Commander**.

  SUGERENCIA
  La hora del servidor NTP proporciona la mejor precisión horaria en el dispositivo.

- **Los dispositivos utilizan Access Commander como servidor NTP** – controla el tiempo en los dispositivos según el tiempo establecido en**Access Commander**.

Automatización

La función de automatización está disponible en **2N Access Commander** a partir de la versión 3.2 del firmware con las licencias Advanced, Pro y Unlimited. Construida sobre la plataforma Node-RED, esta incorporación ofrece directamente a **Access Commander** amplias capacidades de programación basadas en flujos. Permite a los usuarios conectar **Access Commander** con varios sistemas de terceros y automatizar flujos de trabajo personalizados basados en eventos dentro de la plataforma.

ATENCIÓN
Para aprovechar al máximo esta versátil herramienta de automatización, es necesario tener en cuenta lo siguiente:

- **Responsabilidad del cliente por la seguridad**: Los usuarios son responsables de garantizar que sus configuraciones y flujos de trabajo de automatización sean seguros y cumplan con las mejores prácticas de ciberseguridad. Esto incluye proteger el entorno de Node-RED, administrar los permisos de manera adecuada y salvaguardar los datos confidenciales dentro de sus automatizaciones.
- **Uso del nodo API REST**: Si no se utiliza correctamente, este nodo puede provocar la pérdida de datos o modificaciones no deseadas. Es responsabilidad del usuario asegurarse de que el nodo esté configurado e implementado correctamente. Tenga cuidado y vuelva a verificar la configuración para evitar posibles riesgos para sus datos.
- **Nodos y complementos de terceros**: 2N Telekomunikace no es responsable del uso o la integración de nodos, complementos o modificaciones personalizadas de terceros en Node-RED dentro de la función de automatización. Los clientes deben evaluar cuidadosamente y garantizar la seguridad y la estabilidad de cualquier componente adicional que elijan instalar. Cualquier problema que surja de las extensiones de terceros deberá ser resuelto por el cliente o el proveedor externo correspondiente.
- **Limitaciones del soporte técnico**: Si bien nuestro equipo de soporte lo ayudará con los problemas relacionados con la funcionalidad básica de la función de automatización dentro de 2N Access Commander, incluidos nuestros nodos de Access Commander personalizados, no podrá brindar asistencia con el diseño, desarrollo o depuración de flujos de Node-RED personalizados. Los usuarios que deseen crear automatizaciones complejas pueden necesitar buscar soporte adicional de expertos calificados de Node-RED o consultar los recursos disponibles.

Para comenzar a utilizar Node-RED, es recomendable explorar las opciones disponibles Recursos en línea, como manuales detallados y numerosos tutoriales de YouTube sobre Node-RED, que brindan orientación sobre la creación y gestión de los flujos.

Para obtener más información sobre los nodos personalizados de **Access Commander** y el uso de la función de automatización dentro de **Access Commander**, consulte este manual.

Esta función mejora las capacidades de **Access Commander**. Se recomienda explorar su potencial al tiempo que se garantiza la seguridad de las configuraciones.

Creación de automatizaciones

Las tareas automatizadas se crean en un editor externo. Se accede al editor desde la pestaña de **Ajustes > Configuración > Automatización**. Los cambios realizados en el editor se reflejarán sólo después de que se desplieguen en el servidor, lo que se hace utilizando el botón Deplay en la esquina superior derecha del editor.

La creación de tareas automatizadas se basa en la creación de flujos. Los flujos se ensamblan a partir de nodos individuales interconectados. El menú de nodos se muestra en el panel izquierdo. En el panel izquierdo, los nodos pueden buscarse por su nombre. También se puede añadir un nuevo nodo tras crear un nuevo enlace a partir de un nodo existente.

Los datos que se transmiten entre nodos se denominan mensajes. Su descripción y el trabajo con ellos se describen en detalle aquí. En esta página también se describen los nodos básicos que manejan el formato de los mensajes individuales o sus secuencias, como Change, Split, Join,... Las automatizaciones no sólo pueden trabajar con los datos obtenidos en esta tarea única (msg.), sino que también pueden trabajar con valores dinámicos en el contexto de todo el historial de flujos (flow.) o incluso de todos los flujos de una instancia (global.).

ATENCIÓN
El botón Deploy envía los flujos configurados al servidor. ¡Sólo mediante el envío al servidor surtirán efecto los nuevos flujos!

Modo seguro (safe mode)

El modo seguro es una herramienta clave para resolver problemas de automatización. Ejecutar el editor en modo seguro le permite realizar cambios en los flujos sin que éstos se ejecuten en segundo plano. Esto significa que puedes entrar en el editor, editar lo que necesites, y luego desplegar los cambios de nuevo usando el botón Deploy. Este modo es particularmente útil si alguno de los flujos está causando que Node-RED funcione mal o falle, por ejemplo debido a un error en el flujo o en un nodo de terceros, o si el flujo necesita ser detenido inmediatamente.

Nodos (nodes) de Access Commander

REST API

El nodo REST API envía una solicitud API HTTP definida. Los datos de entrada contenidos en la propiedad **body** se utilizan como los puntos de petición de esta solicitud. La salida del nodo son los datos de respuesta a la solicitud. La selección y el orden de los datos de salida pueden especificarse en el parámetro **Query**.

Parámetros del nodo

- **Method** – ofrece una selección de métodos de solicitud de API
- **Endpoint** – se utiliza para especificar el endpoint completo al que se dirigirá la petición. La ruta del punto final puede completarse con el parámetro points.
  Trabajar con solicitudes HTTP se describe en API HTTP (p. 119).
- **Query** – se utiliza para especificar qué parámetros de datos deben tratarse en el endpoint y cómo deben devolverse en la salida. Este parámetro puede especificarse mediante un valor de entrada, la propiedad **query**. Una descripción de cómo construir **query** se describe en el documento Data Query Customization (sólo en inglés).
- **Only send non-2xx responses to Catch node** – Esta opción afecta al tipo de respuestas HTTP que se capturarán en el nodo Catch.
- **Name** – permite cambiar el nombre del nodo para orientarse mejor al trabajar con el flujo.

Access log

El nodo carga las entradas en el Registro de acceso y permite un procesamiento posterior de estas entradas.

El administrador puede configurar tareas automatizadas que se ejecutan cuando **Access Commader** ve una entrada de registro definida. La acción se define en la configuración del nodo. La salida son datos específicos sobre el evento registrado. Una función basada en SignalR se ejecuta en segundo plano.

Parámetros del nodo

- **Filter** – se utiliza para especificar qué registros debe procesar el nodo. Los registros que no coincidan con este filtro serán ignorados por el flujo. El formato del filtro es un objeto JSON. Este parámetro puede ser anulado por el valor de entrada.
- **Name** – permite cambiar el nombre del nodo para orientarse mejor al trabajar con el flujo.

System Log

El nodo carga los registros en el registro del sistema y permite que estos registros se procesen más.

El administrador puede configurar tareas automatizadas que se ejecutan cuando **Access Commader** ve una entrada de registro definida. La definición de la acción se realiza en la configuración del nodo. La salida

son datos específicos sobre el evento registrado. Una función basada en SignalR se ejecuta en segundo plano.

Parámetros del nodo

- **Filter** – se utiliza para especificar qué registros debe procesar el nodo. Los registros que no coincidan con este filtro serán ignorados por el flujo. El formato del filtro es un objeto JSON. Este parámetro puede ser anulado por el valor de entrada.
- **Name** – permite cambiar el nombre del nodo para orientarse mejor al trabajar con el flujo.

SignalR

El nodo SignalR lee los datos del tema suscrito. El nodo recupera datos en tiempo real, por lo que es adecuado para escenarios en los que tiene una tarea automatizada para recuperar información de Access Commander sin la necesidad de un sondeo constante.

Parámetros del nodo

- **Topic** – ofrece temas disponibles para la suscripción.
- **Filter** – se utiliza para especificar qué registros debe procesar el nodo. Los registros que no coincidan con este filtro serán ignorados por el flujo. El formato del filtro es un objeto JSON. Este parámetro puede ser anulado por el valor de entrada.
- **Name** – permite cambiar el nombre del nodo para orientarse mejor al trabajar con el flujo.

Se proporciona más información sobre la funcionalidad SignalR en el capítulo SignalR (p. 119).

Dynamic SignalR

Un nodo Dynamic SignalR frente a un nodo SignalR permite cambios dinámicos en el consumo de datos. Esto puede incluir cambiar el tema o el método de suscripción según los valores de entrada. Los valores de salida del nodo son, por un lado, datos obtenidos de los temas (Datos) y, por otro lado, información sobre la ejecución exitosa o fallida de la acción de este nodo.

Parámetros del nodo

- **Topic** – define el tema para el que debe producirse el cambio de recuperación de datos.
- **Filter** – se utiliza para especificar qué registros debe procesar el nodo. Los registros que no coincidan con este filtro serán ignorados por el flujo. El formato del filtro es un objeto JSON. Este parámetro puede ser anulado por el valor de entrada.
- **Records** – define el número de registros que se leerán cuando se utilice el tipo de lectura fetch.
- **Fetch When Ready** – establece si los valores deben recuperarse cuando se activa el comando de recuperación.
- **Name** – permite cambiar el nombre del nodo para orientarse mejor al trabajar con el flujo.

Valores de entrada válidos

El nodo acepta las siguientes propiedades como valores de entrada. Los valores de entrada válidos anularán temporalmente los parámetros establecidos en la configuración del nodo.

- **topic** – una cadena que especifica el tema que debe eliminarse.
- **filter** – encadenado en formato JSON, que especifica los registros que deben recuperarse.
- **fetchWhenReady** – bootlean que especifica el parámetro del nodo Fetch When Ready.
- **action** – una cadena que especifica la acción a realizar. Puede ser suscribirse, darse de baja...
- **update** – puede contener timestamp (cadena) y timeWindow (objeto) indicando cuando se modificó la acción a realizar.

Se proporciona más información sobre la funcionalidad de SignalR en el capítulo.SignalR (p. 119).

Write system log

El nodo de registro del sistema de escritura crea una entrada en el registro del sistema de Access Commander. La entrada del registro contiene la gravedad especificada, la descripción del evento y otros detalles. Si

se produce un error durante el proceso, se registra y el estado del nodo se actualiza en consecuencia. El nodo no tiene valores de salida.

Parámetros del nodo

- **Severity** – determina la gravedad del registro. Este parámetro puede especificarse mediante el valor de entrada de la consulta.
- **Filter** – se utiliza para especificar qué registros debe procesar el nodo. Los registros que no coincidan con este filtro serán ignorados por el flujo. El formato del filtro es un objeto JSON. Este parámetro puede ser anulado por el valor de entrada.
- **Detail** – se utiliza para una descripción más detallada del registro, que se muestra en el registro del sistema. Este parámetro puede anularse mediante un valor de entrada.
- **Name** – permite cambiar el nombre del nodo para orientarse mejor al trabajar con el flujo.

Valores de entrada válidos

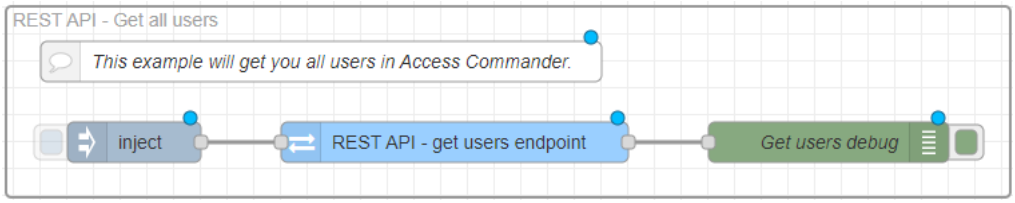
El nodo acepta las siguientes propiedades como valores de entrada. Los valores de entrada válidos anularán temporalmente los parámetros establecidos en la configuración del nodo.

- **severity** – una cadena que especifica la gravedad del registro.
- **event** – una cadena que describe brevemente la acción registrada.
- **detail** – cadena que rellena la descripción detallada del registro que se mostrará en el registro del sistema.

Ejemplos de flujos (flows)

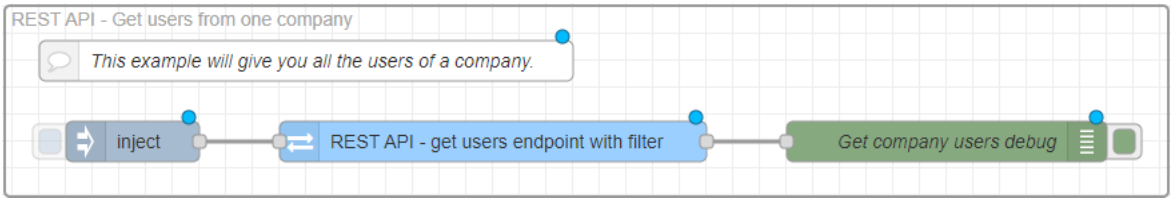
Access Commander ofrece varias tareas automatizadas básicas que representan las posibilidades de uso de la automatización. Los flujos de estas tareas pueden instalarse al iniciar por primera vez la función Automatización en **Access Commander**, pero también pueden importarse posteriormente, véase Exportar/Importar flujos (p. 102). Estos flujos predefinidos pueden modificarse fácilmente para sus propios fines.

Get all users



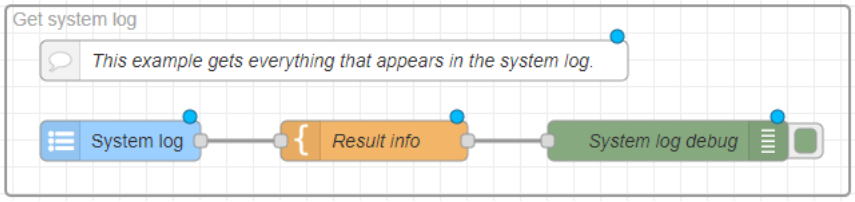
Este flujo genera una lista de todos los usuarios, incluyendo su información. La tarea se inicia activando el nodo Inject. Se puede aplicar un filtro en el nodo **REST API - get users endpoint** para especificar qué usuarios debe devolver el proceso. De este modo, la salida del proceso puede adaptarse a las necesidades del administrador.

Get users from one company



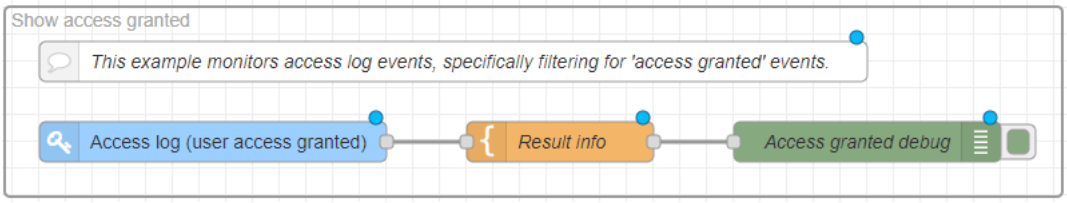
Este flujo genera una lista de todos los usuarios de una misma empresa, incluyendo información sobre ellos. La tarea se inicia activando el nodo Inject. La selección de la empresa se establece en el nodo **REST API - get users endpoint** con fillter especificando su id.

Get system log



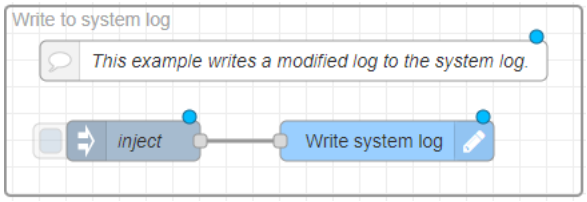
Este flujo lee todas las entradas nuevas en el registro del sistema. Puede refinar la selección de eventos especificando un filtro en el nodo **System log**.

Show access granted



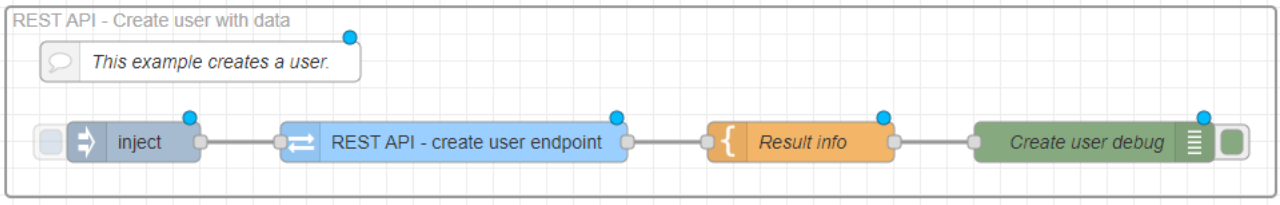
Este flujo lee todas las entradas nuevas en el registro de acceso. El flujo está configurado para leer sólo los accesos concedidos. Puede cambiar esta restricción en el nodo **Access log**.

Write to system log



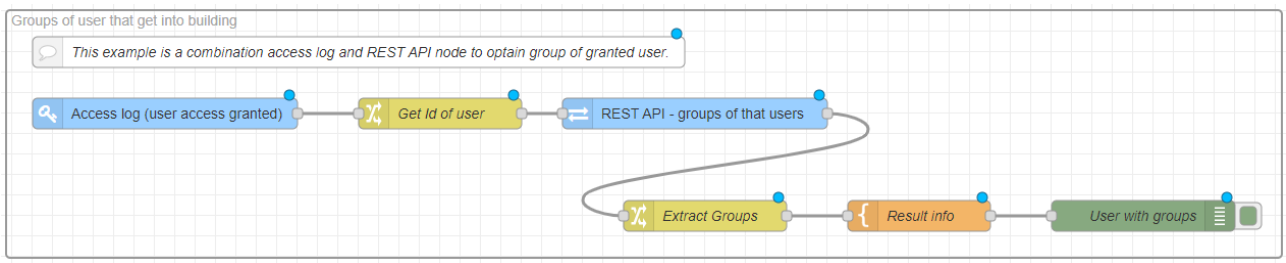
Este flujo crea una entrada en el registro del sistema.El nodo **Write system log** se puede utilizar para establecer la gravedad, el nombre y la descripción detallada de la entrada.

Create user with data



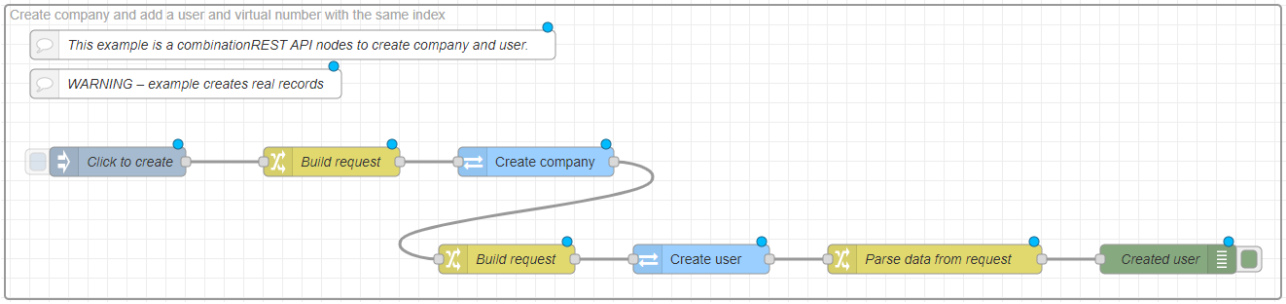
Este flujo se utiliza para crear un nuevo usuario. La tarea se inicia activando el nodo **Inject**. El nodo **Inject** contiene un cuerpo de mensaje que especifica el nombre del usuario Joe Doe y su asignación a la empresa con ID 1. Este cuerpo se aplica en el nodo **Rest API - create user endpoint** y el usuario se crea en base a él. El nodo **Result info** establece el texto del mensaje que aparecerá en los mensajes Debug.

Groups of users that get into building



Este flujo recupera los grupos de usuarios a los que se ha concedido acceso. Los accesos permitidos se recuperan del registro de accesos. A continuación, el flujo recupera el ID del usuario al que se ha concedido acceso y utiliza el nodo **REST API - groups of that users** para recuperar información sobre ese usuario. El nodo **Extrack Groups** recupera los nombres de los grupos de ese usuario y el nodo **Result info** compila el texto del mensaje final.

Create company and add a user and virtual number with the same index



Este flujo crea una nueva empresa, el primer usuario de esa empresa y su número virtual. La tarea se inicia activando el nodo **Inject**. En la inicialización, se genera un número entero aleatorio que se utilizará en el nombre de la empresa, en el nombre del usuario y servirá como número virtual del usuario. El nodo **Create company** crea una empresa con el nombre definido. La respuesta de este nodo arrojará el ID de la empresa, en base al cual el siguiente nodo **Create user** creará un nuevo usuario en esta empresa y le asignará un número virtual al mismo tiempo. El nodo P**arse data from request** recupera el nombre de la empresa, el nombre del usuario y el número virtual del usuario.

Exportar/Importar flujos

Los flujos pueden exportarse a archivos .json y reimportarse posteriormente a la interfaz de automatización. Tanto la exportación como la importación se realizan en el menú ampliado de la esquina superior derecha. Los flujos trasladados de una instalación de **Access Commander** a otra pueden requerir edición.

En las opciones de importación hay flujos de ejemplo precargados para **Access Commander**. Se encuentra en la pestaña Ejemplos, en la carpeta Access-Commander-nodes.

ATENCIÓN
Las configuraciones de funciones avanzadas que no son compatibles con la nueva licencia no se guardan.

Por lo tanto, cuando finalice su licencia de prueba, no olvide exportar los flujos configurados.

Estados de error

Cuando se trabaja con automatizaciones, a veces pueden producirse errores que afectan a su estabilidad y funcionalidad. Si se produce una condición de error, la pestaña Automatización de **Access Commander** le alertará de la condición y le ofrecerá reiniciar la plataforma Node-RED en modo seguro. El modo seguro detiene temporalmente la ejecución de los flujos y permite la reparación segura de los flujos que inducen la condición de error. El reinicio de los flujos se activa con el botón Deploy.

Hay dos condiciones de error básicas:

- **Nodo-RED no responde**
  Esta condición ocurre cuando Node-RED deja de responder. No se están ejecutando automatizaciones establecidas. Este problema puede deberse a varios factores, como sobrecarga del sistema, errores en la configuración del flujo o conflictos entre módulos de terceros importados.

- **El nodo-RED es inestable**
  La inestabilidad de Node-RED se manifiesta al reiniciar repetidamente la plataforma, lo que puede interrumpir el funcionamiento de la automatización y provocar la pérdida de datos. Por lo general, se produce un reinicio repetido si uno de los flujos está mal configurado y desencadena un reinicio. Todas las transmisiones se suspenden mientras dure el reinicio.

Nombre de la instalación

El nombre de la instalación específica de **Access Commander** se muestra en el encabezado de la interfaz web, y el nombre se muestra a todos los usuarios conectados. El nombre predeterminado de **Access Commander** puede cambiarse, por ejemplo, por la dirección del edificio que gestiona una instalación concreta.

Para cambiar el nombre, vaya a **Ajustes > Configuración > pestaña Nombre de la instalación**. Puede utilizar el cambio de nombre para distinguir instalaciones individuales si una persona gestiona varias instalaciones. El nombre de la instalación también se escribe en los correos electrónicos que se envían a las empresas.

Habilitación y configuración de la función de correo electrónico (SMTP)

La función de correo electrónico permite enviar notificaciones o enviar contraseñas de inicio de sesión a los usuarios. Los correos electrónicos se envían a través del protocolo SMTP.

1. Los ajustes se realizan en **Ajustes > Configuración > Correo electrónico**.
2. Después de activar la función de correo electrónico, se abre un cuadro de diálogo en el que puede configurar los siguientes parámetros:
   - **dirección del servidor SMTP**, al que se enviarán los correos electrónicos.
   - **Puerto de servicio**, preestablecido en 25.
   - **Nombre de usuario** y **contraseña** a la cuenta en el servidor SMTP si el servidor SMTP requiere autorización.
   - **Dirección de remitente predeterminada**, desde donde se enviarán los correos electrónicos.
3. Encienda según sea necesario:
   - **SSL** para cifrado de correo electrónico,
   - **Verificación del certificado del servidor SSL**,
   - **Modo de compatibilidad** en caso de conexión a servidores SMTP antiguos que no soportan nuevas funciones (GSSAPI).
4. Después de guardar, puede configurarlo en la pestaña Correo electrónico **Dirección base para enlaces de correo electrónico**, que formará parte de los mensajes de correo electrónico enviados y puede remitir a los destinatarios del correo electrónico a la parte seleccionada de la interfaz **Access Commander**.
5. Puede comprobar la configuración realizada enviando un correo electrónico de prueba.

Autenticación de dos factores

La autenticación de dos factores proporciona un mayor nivel de seguridad de la cuenta de usuario en **Comandante de acceso**. Para iniciar sesión, el usuario ingresa los datos de inicio de sesión y luego debe confirmar su inicio de sesión utilizando la aplicación de autenticación. Una vez que el administrador activa la necesidad de autenticación de dos factores, se le pedirá al usuario que vincule su cuenta con su propia aplicación de autenticación en el próximo inicio de sesión.

Access Commander no requiere que vuelva a verificar su identidad cada vez que inicie sesión o realice acciones protegidas. Una vez que complete la verificación, el sistema le recordará durante un tiempo limitado:

- 7 días para inicios de sesión normales
- 5 minutos para acciones consideradas críticas para la seguridad, como el cambio de claves API, la actualización de su propia contraseña o la modificación de la contraseña raíz.

El sistema puede recordar hasta dos dispositivos autentificados. Si se autentica desde un nuevo dispositivo, se elimina el dispositivo recordado más antiguo. Si intenta realizar una acción crítica para la seguridad fuera de la ventana de tiempo permitida, el sistema simplemente le pedirá que se autentique de nuevo antes de poder continuar.

1. La autenticación de dos factores la configura el administrador en **Configuración > Configuración > Pestaña de autenticación de dos factores**.
2. El administrador puede seleccionar qué usuarios requerirán autenticación de dos factores.
   Opciones para requerir verificación en dos pasos
   - **Opcional**
     La autenticación de dos factores es opcional. Los usuarios pueden activarlo ellos mismos en su perfil.
   - **Obligatorio para los usuarios con rol**
     Cada usuario al que se le haya asignado una función debe confirmar su inicio de sesión mediante una aplicación de autenticación.
   - **Obligatorio**
     Todos los usuarios deben confirmar su inicio de sesión mediante la aplicación de autenticación.

Activar la verificación en dos pasos

Si el administrador configura la verificación en dos pasos opcional, el propio usuario activa la verificación en dos pasos de la siguiente manera:

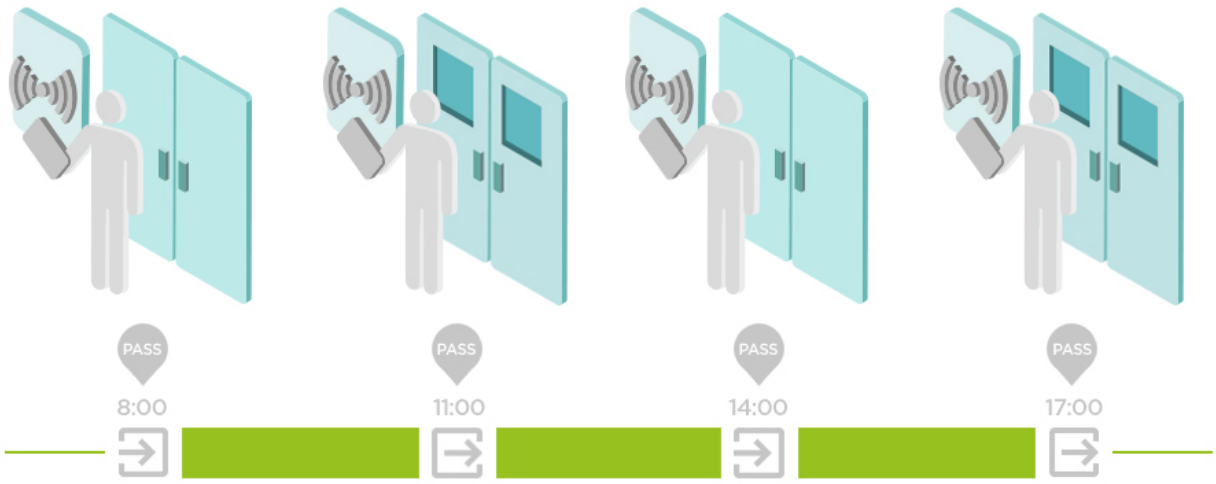
1. Haga clic en el icono de usuario en la esquina superior derecha para abrir el menú de usuario.
2. Utilice la pestaña Aplicaciones de autenticación para vincular su cuenta a la aplicación de autenticación seleccionada. Siga las instrucciones de **Access Commander**.
3. Seleccione Mostrar perfil.

Configuración de asistencia

Access Commander permite el seguimiento de la asistencia de los usuarios. En el modo de asistencia se registran los tiempos de entrada y salida de usuarios individuales.

Modos de asistencia

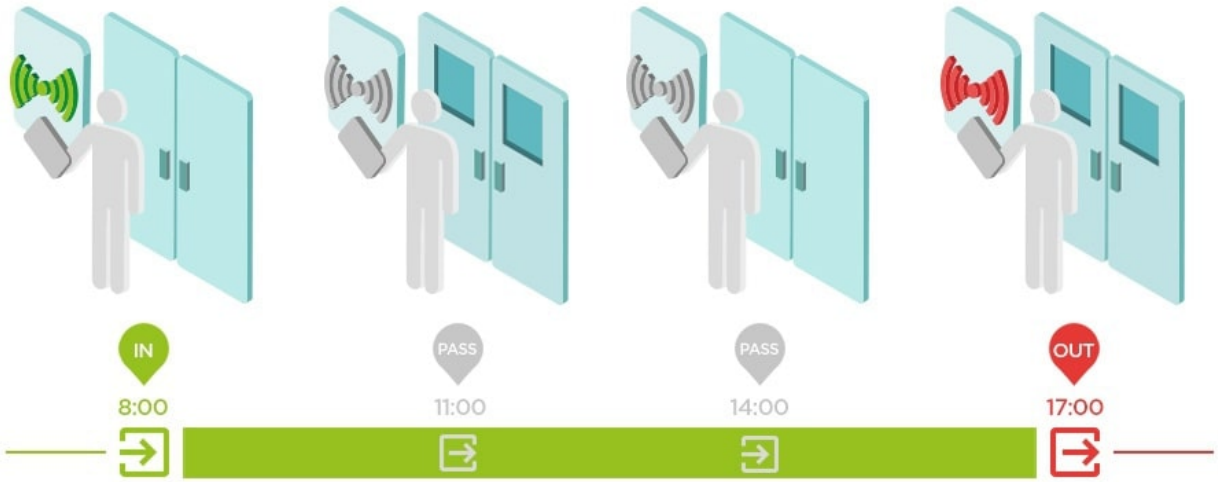
- **GRATIS**



Las llegadas y salidas se cuentan desde la primera y última autenticación de usuario en cualquier dispositivo en un día. El módulo de presencia no funciona en este modo.

- **EN FUERA**

  Para que funcione correctamente, el dispositivo debe estar preparado para entrar y salir de la zona.



- **ENTRADA-SALIDA para todos los dispositivos**
  Este modo permite el control de presencia. Las llegadas se registran en los dispositivos entrantes y las salidas se registran en los dispositivos salientes. El movimiento entre zonas no se registra como llegada/salida.
- **IN-OUT para dispositivos seleccionados**
  Este modo permite el control de presencia. Las llegadas y salidas se registran en dispositivos seleccionados que están configurados como llegadas o salidas. Las llegadas y salidas se registran únicamente en estos dispositivos seleccionados. De este modo, el registro de llegada/salida se puede establecer, por ejemplo, sólo en la entrada principal del edificio.

Configuración del punto de acceso del dispositivo

Puede dividir lógicamente cada dispositivo en dos puntos de acceso: de llegada y de salida. Cada punto de acceso representa un paso en una dirección y determina si el usuario del dispositivo entra o sale de la zona. Un punto de acceso puede ser controlado por uno o varios módulos de dispositivo. Todos los módulos asignados gestionan entonces los pasillos en la dirección del punto de acceso específico. Los puntos de acceso se utilizan especialmente en situaciones en las que un dispositivo se encuentra en el límite de dos zonas y es necesario registrar con precisión la dirección del movimiento entre ellas (por ejemplo, para funciones anti-retorno).

Los puntos de acceso también se utilizan para realizar un seguimiento de los usuarios en el módulo Presencia (p. 84). Los puntos de acceso también se utilizan para realizar un seguimiento de las entradas y salidas en Restricciones de área (p. 86).

NOTA
En la interfaz de configuración web de cada dispositivo, los puntos de acceso se denominan **Llegada** y **Salida**. Para configurarlas, vaya a **Acceso > Reglas de acceso > Solapa Acceso y salida**.

Habilitación de puntos de acceso en Access Commander

1. Ir a la página de Zonas v **Comandante de acceso**.
2. En la esquina superior derecha, presione ⚙ y habilitar el uso de puntos de acceso.

Asignación de módulos para la llegada o la salida

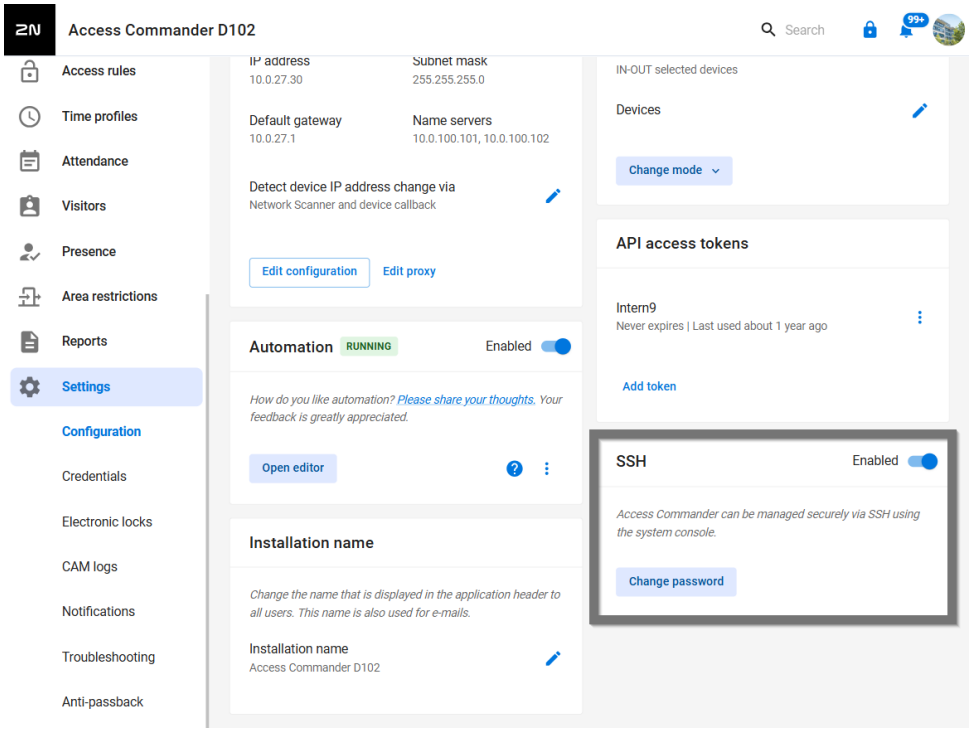
1. Acceda a la interfaz de configuración basada en web para el dispositivo.

> **SUGERENCIA**
>
> Puede acceder a la interfaz de configuración basada en web haciendo clic en ⚙ en la lista de la página Dispositivos.

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

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

Permitir acceso SSH



> **AVISO**
>
> Se recomienda habilitar el acceso SSH solo para usuarios avanzados. El uso inadecuado es un peligro para la seguridad.

Utilice la ficha **Ajustes > Configuración > SSH** para habilitar Secure Shell, que proporciona una comunicación remota segura con la consola del sistema. Habilitar SSH le permite realizar copias de seguridad y restaurar el sistema o reiniciar **Access Commander** por completo.

Para conectar Access Commander box o máquina virtual, el cliente SSH necesita conocer la dirección IP de **Access Commander** y la contraseña raíz del sistema. La contraseña raíz del sistema se puede establecer en **Ajustes > Configuración > ficha SSH**.

NOTA
El cambio de la contraseña de root se realiza en la consola de configuración, no en Access Commander.

El acceso SSH también se puede habilitar y administrar directamente en la consola de configuración de Linux, consulte Configuración de Linux (p. 90).

Claves de cifrado para My2N

Los usuarios pueden utilizar la aplicación My2N para conectarse a los dispositivos 2N. La comunicación entre la aplicación My2N y el dispositivo siempre está cifrada. **Access Commander** gestiona automáticamente las claves de emparejamiento del sistema que se distribuyen a los dispositivos compatibles con WaveKey para garantizar un emparejamiento seguro y de confianza. Sin conocer la clave de cifrado, la aplicación My2N no puede autenticar al usuario. La clave de encriptación principal se genera automáticamente al iniciar el intercomunicador por primera vez o, en el caso de la gestión de **Access Commander**, como parte de su configuración. La clave puede volver a generarse manualmente en cualquier momento. La clave de encriptación primaria se transfiere junto con el Auth ID al dispositivo móvil durante el emparejamiento.

NOTA
En el sistema se utilizan dos tipos de claves: **claves de coincidencia** y **claves de acceso**. Las claves de emparejamiento se utilizan para autenticar la aplicación móvil My2N con el dispositivo. Las claves de acceso determinan los permisos para las funciones dentro de la aplicación móvil.

Creación de nuevas claves

1. Vaya a **Settings > Authentication > Encryption Keys tab for My2N application**.
   Se pueden generar hasta 4 claves de acceso. Al intentar generar una quinta clave **Access Commander** advertirá de que al generarla se eliminará la clave más antigua. La ficha enumera los tiempos de generación de cada clave.
2. Haga clic en Generar una nueva clave.

   SUGERENCIA
   Por razones de seguridad, se recomienda regenerar las claves de emparejamiento una vez cada cierto tiempo (por ejemplo, una vez al año).
3. La clave recién generada se carga automáticamente en la aplicación My2N la primera vez que se utiliza el teléfono móvil con un dispositivo previamente emparejado.

La clave generada puede borrarse pulsando en .

SUGERENCIA
Para un mayor nivel de seguridad, es preferible emparejar utilizando el **código QR** , que contiene la clave pública. Si el código QR no está disponible, puede utilizar el emparejamiento **PIN**.

ATENCIÓN
El emparejamiento por código QR sólo es compatible con dispositivos con firmware HIP 2.50.0 y posterior (incluida la serie 3.0). En un entorno con Access Commander puede mostrarse el **código QR** , pero el emparejamiento en versiones anteriores de HIP sólo se realizará con éxito utilizando el **PIN** .

NOTA

- Si la aplicación My2N no tiene acceso a ninguna clave de cifrado válida, no podrá utilizarse para la autenticación de usuarios. Para restablecer la funcionalidad de la aplicación, deberá volver a emparejarla con el dispositivo conectado a Access Commander, que cargará las claves de cifrado válidas en la aplicación My2N.
- Permitir el acceso al dispositivo depende de los derechos de acceso establecidos por el usuario.

Modo de compatibilidad de tarjetas RFID

Si **Access Commander** informa que la tarjeta nueva que acaba de agregar ya está en uso en el sistema, la razón puede ser que el modo de compatibilidad de tarjetas RFID está habilitado. El administrador habilita este modo en **Configuración > Autenticación > ficha Configuración del modo de compatibilidad**.

ATENCIÓN

- El modo de compatibilidad debe activarse solo cuando haya problemas para cargar las tarjetas registradas anteriormente. El uso del modo de compatibilidad puede afectar a los mecanismos de autenticación
- No se recomienda combinar el modo de compatibilidad con el uso de tarjetas protegidas por la tecnología PiCard.

Teclas PICard

En la pestaña **Configuración > Acceso > Claves PICard**, se almacenan las claves de cifrado de la aplicación 2N PICard Commander. Si las claves de cifrado se cargan en **Access Commander**, la pestaña muestra el nombre del proyecto de PICard Commander y el identificador numérico de exportación de claves. La pestaña permite eliminar las claves cargadas desde **Access Commander.**

ATENCIÓN
Si elimina las claves PICard, todas las tarjetas cifradas con esas claves dejarán de funcionar.

Importar claves de cifrado PICard

1. Vaya a **Configuración > Acceso > pestaña Teclas PICard**.
2. Después de hacer clic en Importar cargue el archivo de clave de cifrado desde su repositorio.
3. Ingrese una contraseña para proteger el archivo si configuró una al exportar desde la aplicación PICard Commander.

2N PICard Commander es una aplicación de software para cifrar credenciales en tarjetas de acceso. La aplicación crea proyectos que generan un conjunto de claves de cifrado y lectura. Las claves del lector de proyectos se pueden importar a dispositivos 2N o a **Access Commander**, que posteriormente garantiza la distribución de claves de lectura a los dispositivos 2N conectados.

Lectores USB habilitados

Para facilitar el registro de algunos métodos de autenticación de usuarios, puede utilizar lectores USB conectados a la computadora en la que se accede a **Access Commander**. Los lectores deben estar habilitados en **Access Commander** en **Configuración > Acceso > ficha Lectores USB permitidos**.

1. Vaya a **Settings > Access > USB Reader Enabled tab.**
2. Haga clic en Habilitar lectores para abrir el cuadro de diálogo.
3. La activación/desactivación del uso de un dispositivo USB externo se realiza en un cuadro de diálogo.
4. A continuación, se modifica su habilitación de lector haciendo clic en Cambiar.

Access Commander permite el uso de los siguientes dispositivos USB:

- Lector de tarjetas RFID de 125 kHz – N.º de pedido 9137420E, Parte del EJE. Bien 01399-001
- Lector de tarjetas RFID de 13,56 MHz y 125 kHz – N.º de pedido 9137421E , Parte del EJE. Bien 01400-001
- Lector de huellas dactilares - N.º de pedido 9137423E, Parte del EJE. Bien 01401-001

Registros de cámara

Los registros CAM se utilizan para grabar automáticamente varios fotogramas que preceden y siguen a un evento seleccionado. En **Configuración > Registros CAM**, puedes gestionar los distintos tipos de eventos para los que se deben generar registros CAM.

Por ejemplo, se pueden generar registros CAM con cada inserción de tarjeta. Si alguien pasa la tarjeta, se registrarán 5 imágenes antes de pasar y 3 imágenes después de pasar en los registros de acceso. Los fotogramas se graban después de 1 segundo. Se crea un almacenamiento de 1, 3 o 5 GB para las imágenes. Si el almacenamiento está lleno, se eliminarán las imágenes más antiguas. Los registros de acceso en sí no se eliminan.

Crear un tipo de registro CAM

1. Ve a **Configuración > Registros CAM**.
2. Haga clic en el botón Agregar en la esquina superior derecha de la página.
3. Introduzca un nombre para el tipo de evento de registro CAM.
   El tipo de evento de registro CAM recién creado se muestra en la lista y se abre el detalle en el registro CAM. En el detalle del registro CAM es necesario establecer para qué eventos y en qué dispositivos se generarán las imágenes de las cámaras.

Configuración de logotipos CAM

La información sobre el tipo de registro CAM se puede administrar en el detalle del registro CAM. El detalle del registro CAM se abre haciendo clic en el registro CAM seleccionado en la lista o después de crear un nuevo registro CAM.

Eventos vistos

La pestaña le permite seleccionar una lista de eventos durante los cuales se capturarán imágenes de las cámaras.

Los eventos rastreados pueden ser los siguientes:

- **Enfoques**
  - Usuario aceptado
  - Se reconoce la matrícula del coche
  - Usuario rechazado
  - Presione el botón REX
- **Seguridad**
  - Interruptor de protección activado
  - Apertura de puerta no autorizada
  - Apertura remota de puertas
  - Acceso denegado: entrada incorrecta repetida
  - Alarma silenciosa activada
- **llamando a**
  - Llamada iniciada

Dispositivos monitoreados

Se recomienda configurar la grabación de registros CAM solo desde dispositivos equipados con una cámara. La selección del dispositivo se realiza en una ventana de diálogo que se abre con . Al mismo tiempo, la tarjeta permite grabar registros CAM desde todos los dispositivos.

Cerraduras electrónicas

El sistema **Access Commander** proporciona gestión de accesos mediante cerraduras electrónicas 2N Fortis, que se desbloquean mediante tarjetas RFID con tecnología MIFARE® DESFire®. Al configurar las cerraduras electrónicas, se asigna a cada cerradura una clave de cifrado. Las llaves de las cerraduras se almacenan en las tarjetas RFID de los usuarios autorizados. Si las claves de la tarjeta y de la cerradura coinciden, se desbloquea el mecanismo de cierre.

Una tarjeta de acceso RFID puede utilizarse para acceder hasta a 90 puertas con cerraduras 2N Fortis, en función del número de perfiles horarios aplicados. Si se supera la capacidad de memoria de la tarjeta, fallará la escritura de datos en la tarjeta. El evento de fallo de escritura se registra en el registro de accesos del sistema. Si se utilizan Grupos de Cerraduras, se pueden escribir más puertas en una sola tarjeta que con la asignación individual. Si se utilizan Grupos de Bloqueo, se pueden inscribir más puertas por tarjeta que en una asignación individual.

Fortis Commander

Fortis Commander es una aplicación independiente que conecta las cerraduras electrónicas **Fortis** al sistema **Access Commander**. La aplicación establece los bloqueos de acuerdo con el archivo de proyecto creado en **Access Commander**u que contiene la configuración de los bloqueos. El archivo está encriptado y sólo puede utilizarse en una instalación específica.

Instalación

Fortis Commander está diseñado para instalarse en un ordenador Windows compatible con Bluetooth Low Energy (BLE).

Encontrará la aplicación en la página web 2N Download Centre.

Procedimiento de instalación

1. Descargue el paquete de instalación desde el enlace proporcionado.
2. Ejecute el instalador y complete la instalación siguiendo las instrucciones en pantalla.

Archivo del proyecto

El archivo del proyecto se crea en **Access Commander** y contiene la configuración completa del proyecto. El archivo está encriptado y protegido por contraseña.

Establecer bloqueos en Access Commander

Antes de cargar llaves en cerraduras individuales, debe emparejar **Access Commander** con **Fortis Commander**.

Generación de la clave maestra de cifrado (MEK) y preparación del proyecto

1. Inicie sesión en Access Commander.
2. Vaya a **Configuración > Cerraduras electrónicas**.
3. En la pestaña **Configuración inicial** haga clic en Generar claves.
4. Cree la clave de cifrado maestra.

ATENCIÓN
La clave de cifrado maestra no se puede ver ni modificar posteriormente .

NOTA
En función de la clave maestra de cifrado (MEK), **2N Access Commander** genera un conjunto de claves de cifrado. Por lo tanto, la clave debe ser única y suficientemente segura. El conjunto de claves se basa en la clave de cifrado maestra, por lo que los proyectos con la misma clave de cifrado maestra generan los mismos conjuntos de claves. Si se pierde un proyecto, se puede crear uno nuevo con la misma clave maestra de encriptación y continuar con la encriptación.

5. Tras generar las claves y establecer la contraseña del archivo de proyecto, puede descargar **el archivo de proyecto**, que es una imagen de la configuración de la cerradura electrónica en el sistema **Access Commander**.
6. En la pestaña **de Fortis Commander** haga clic en Descargar aplicación, desde donde se iniciará la descarga de **Fortis Commander** (aplicación para configurar cerraduras electrónicas).

ATENCIÓN
La información sobre el proyecto es confidencial. Protéjalos contra cualquier uso indebido.

Configuración de la cerradura electrónica mediante Fortis Commander

1. Instale **Fortis Commander** y ábralo.
2. Haga clic en Abrir proyecto y abra el archivo del proyecto descargado en el Explorador de archivos.
3. En el cuadro de diálogo que aparece, introduzca la contraseña del archivo de proyecto.
4. Tras abrir el archivo del proyecto, seleccione Conectar al dispositivo y conecte la tarjeta de servicio a la cerradura.

5. Haga clic en **Asignar**, que asigna el bloqueo al proyecto.
6. Desconecte el dispositivo y haga clic en **Archivo > Cerrar proyecto**.
7. Una vez finalizada la configuración, abra el sistema **Access Commander**. Vaya a la pestaña **Configuración > Cerraduras electrónicas** y haga clic de nuevo en Fortis Commander. Cargue el archivo de proyecto.

NOTA
Cuando traslade la cerradura de una instalación a otra o cuando realice una reclamación, deberá realizar un restablecimiento de fábrica . Esta operación restablece la cerradura a los ajustes de fábrica y elimina toda la configuración anterior.

Procedimiento de actualización de la configuración

1. Realice cambios en **Access Commander**.
2. Descargue el archivo del nuevo proyecto.
3. Cargue el archivo en **Fortis Commander** y realice los cambios necesarios en las cerraduras.
4. Si realiza otros cambios en **Access Commander**u, descargue siempre un nuevo archivo de proyecto.

ATENCIÓN
Para cada cambio de configuración en **Access Commander**u debe descargar un nuevo archivo de proyecto - no puede utilizar un archivo más antiguo que ya se haya cargado en **Fortis Commander**.

Bloqueo y desbloqueo permanentes

La aplicación le permite bloquear y desbloquear la cerradura de forma permanente. La función se utiliza para intervenciones de servicio o control de emergencia sin necesidad de utilizar una tarjeta.

Recogida de eventos de cerraduras electrónicas mediante tarjetas / chips RFID

Ajustes de recogida de eventos

1. Abra **Configuración > Cerraduras electrónicas > Eventos de pestañas**.
2. Seleccione el tipo de evento:
   - **Recopilar eventos de acceso y del sistema** - Todos los eventos de acceso y del sistema se registran en la tarjeta/chip y se escriben en el registro del sistema y en el registro de acceso .
   - **Recoger sólo los eventos del sistema** - sólo se registran los eventos del sistema, los eventos de acceso no se almacenan en las tarjetas.
   - **No recoja eventos en las pestañas** - no se escribe ningún evento en la pestaña; sólo se puede acceder a ellos a través de **Fortis Commander**u.

SUGERENCIA
Seleccionando del conjunto de eventos adecuado, puede reducir la carga del sistema y el uso del almacenamiento Sin embargo, el registro detallado es importante para el diagnóstico y las auditorías de seguridad.

Exportar eventos de una tarjeta

La tarjeta almacena un máximo de **16 primeros eventos**. Los eventos pueden leerse de dos maneras:

- En **Access Commander**, haga clic en el icono del cuadro de búsqueda de la cabecera y cargue la pestaña.
- Utilizando un dispositivo con **2N OS**, los eventos se leen de la tarjeta y se envían a **Access Commander**u.

Carga de eventos en la cerradura

1. Abra **Configuración > Cerraduras electrónicas > Fortis Commander** y haga clic en Descargar archivo.
2. Abra el archivo en **Fortis Commander**.
3. En la aplicación **Fortis Commander**, conéctese a la cerradura electrónica.
4. Vuelva a cargar el archivo actualizado en **Access Commander**.
5. Una vez cargados, los eventos se muestran en **Registros de acceso** y **Registros del sistema**.

Operaciones de servicio

Estas operaciones están disponibles para **Cilindro Fortis**:

- **Desmontaje** - desmontaje de cerraduras con fines de servicio.
- **Sustitución de la pila** - Sustitución de la pila de la cerradura.

ATENCIÓN
Las operaciones de servicio no son relevantes para otros tipos de esclusas.

NOTA
Desde el modo de servicio, la cerradura vuelve al modo normal pulsando el botón Lock para bloquearse permanentemente.

Actualización de tarjeta

Las tarjetas de acceso de los usuarios deben actualizarse periódicamente. El usuario actualiza la tarjeta conectándola al dispositivo 2N IP al que tiene derechos de acceso válidos. El lector del dispositivo debe sujetar la tarjeta hasta que se encienda el interruptor de apertura de la puerta. El interruptor de apertura de la puerta se activa solo después de actualizar el acceso a las cerraduras

Puede cambiar la validez predeterminada de diez días de las tarjetas en **Configuración > Cerraduras electrónicas > pestaña Parámetros de tarjeta**.

ATENCIÓN
Si modifica los derechos de acceso a las cerraduras en **Access Commander**, los cambios sólo se reflejarán en la tarjeta de acceso del usuario una vez que ésta se haya actualizado en el lector de tarjetas del dispositivo 2N. Por razones de seguridad, recomendamos fijar un periodo de validez más corto para las tarjetas, con el fin de garantizar su actualización periódica.

Los lectores de dispositivos IP que permiten actualizar la tarjeta y su configuración se describen en el capítulo Configuración del lector de dispositivos IP (p. 30).

Tarjetas compatibles

NOTA
A efectos de la presente documentación, el término tarjeta **o tarjeta** hace referencia a cualquier identificador compatible que utilice la tecnología MIFARE DESFire.

Para abrir las cerraduras electrónicas 2N Fortis no se pueden utilizar tarjetas con ID aleatorio (random ID).

Las tarjetas con tecnología PICard no se pueden utilizar para abrir cerraduras electrónicas 2N Fortis.

Perfiles temporales en cerraduras electrónicas

Las cerraduras electrónicas admiten perfiles horarios con las siguientes restricciones:

- No se aplican días festivos.
- Se pueden configurar hasta 4 intervalos de tiempo diferentes en un solo día.
- En un perfil temporal se pueden definir 4 horarios diarios de intervalos.

SUGERENCIA
Esto significa que puede tener, por ejemplo, una configuración diferente para el lunes, martes, miércoles y jueves, pero para el viernes, sábado y domingo debe utilizar una de las configuraciones existentes.

ATENCIÓN
Si el perfil temporal incumple las restricciones indicadas, se ignorará la regla de acceso y no se concederá acceso al usuario.

Tarjetas para el mantenimiento

Las tarjetas de mantenimiento permiten el acceso autorizado a la cerradura. Permiten poner la cerradura en servicio, cambiar la pila, desmontar la cerradura.

ATENCIÓN
La tarjeta de mantenimiento no puede utilizarse al mismo tiempo como tarjeta de acceso de usuario.

Configuración de la pestaña Mantenimiento

1. En **Access Commander** vaya a **Configuración > Cerraduras electrónicas**.
2. En la pestaña **Mantenimiento** haga clic en Crear.

3. En el cuadro de diálogo que se abre, seleccione el tipo de tarjeta que desea crear.
   - Configurar cerraduras nuevas: activa las cerraduras nuevas previamente configuradas en fábrica en modo de servicio.
   - Servicio: activa el modo de servicio para la cerradura ya configurada.
   - Desmontaje - libere la cerradura de bombillo 2N Fortis ya ajustada para desmontarla, consulte el Manual de instalación de 2N Fortis.
   - Sustitución de la pila - libere la cerradura de bombillo 2N Fortis ya ajustada para sustituir la pila, consulte el Manual de instalación de 2N Fortis.

   SUGERENCIA
   Una tarjeta física puede cargarse simultáneamente con **Setting New Locks** y cualquier otra tarjeta de servicio. Recomendamos una combinación de **Ajuste de nuevas cerraduras** y **Servicio**.
4. Haga clic en . Continúe en.
5. Conecte la tarjeta al lector RFID USB conectado. Espere hasta que los datos se carguen en la tarjeta.

La validez de los datos de la tarjeta de mantenimiento es de un año. Una vez transcurrido este tiempo, es necesario borrar los datos y volver a configurar la tarjeta.

Solución de problemas

Registros de diagnóstico

El soporte técnico utiliza los registros de diagnóstico para identificar y resolver los problemas informados. Los registros contienen información sobre acciones realizadas, errores, cambios de estado y otros eventos relevantes.

Descargar registros de diagnóstico

1. Vaya a **Configuración > Solución de problemas > pestaña Registros de diagnóstico**.
2. Haga clic en Generar registros.
   Se necesitan unos minutos para generar el paquete de registro.
3. Una vez que el mazo esté listo, aparecerá en la tarjeta y estará disponible. Descargar.

Estadísticas de uso

Si la función está activada, envía **Access Commander** una vez al día datos anónimos sobre las funciones utilizadas a un servidor seguro de 2N. Cada envío se realiza bajo un identificador único, que se vuelve a generar automáticamente con cada nuevo envío. De este modo se impide que el usuario 2N identifique la instalación en cuestión. **Access Commander**. La información obtenida se utiliza para mejorar el desarrollo de productos, desarrollar funciones y mejorar la experiencia del usuario.

Notificación

El módulo de Notificaciones le permite configurar el monitoreo de eventos seleccionados y propiedades del sistema de las que tiene conocimiento. **Access commander** informar por correo electrónico o notificación en la barra superior al lado del menú de usuario.

La lista de notificaciones también se muestra en la página **Registros del sistema > Notificaciones**.

Los registros pueden descargarse en un archivo CSV pulsando el botón Exportar situado encima de la lista. En el archivo CSV exportado, la hora se indica en GMT+0.

Configurar un nuevo tipo de notificación

1. Ve a **Ajustes > Notificaciones**.

2. Haga clic en el botón Agregar en la esquina superior derecha de la página.
3. Ingrese un nombre para el nuevo tipo de notificación.
   Luego de la creación, se mostrará el detalle de la notificación, en el cual es posible seleccionar los dispositivos para los cuales se debe monitorear la notificación; agregar usuarios a quienes se debe enviar la notificación; Elija el método de entrega de notificación.

Configuración de las notificaciones

Los tipos de notificación se establecen en los detalles del tipo de notificación. Para abrir los detalles del tipo de notificación, haga clic en la notificación seleccionada en la lista de la página **Configuración > Notificaciones**.

Método de notificación

En esta pestaña, se configuran los métodos de notificación y la lista de destinatarios de notificaciones por correo electrónico.

Las notificaciones aparecen en **Access Commander** bajo el icono de la barra superior, junto al menú de usuario o en **Registro del sistema > Notificaciones**.

Se pueden enviar correos electrónicos de notificación a los usuarios administrados en **Access Commander** y destinatarios fuera del sistema. Los usuarios se pueden seleccionar de la lista. Las direcciones de correo electrónico de los demás destinatarios deben introducirse manualmente.

NOTA
Para el correcto funcionamiento de las notificaciones por correo electrónico, es necesario tener SMTP configurado correctamente, consulte Habilitación y configuración de la función de correo electrónico (SMTP) (p. 103).

Dispositivos monitoreados

El tipo de notificación dado se puede generar tanto para todos los dispositivos como solo para algunos dispositivos. Si Monitorear todos los dispositivos está habilitado, el evento puede ocurrir en cualquier dispositivo y se generará una notificación. Si Monitorear todos los dispositivos está deshabilitado, se generará una notificación solo si el evento ocurre en el dispositivo seleccionado. La selección del dispositivo se realiza en el menú que se abre con .

Configuración de la red

Para configurar una conexión de red, vaya a **Ajustes > Configuración > ficha Red**. La ficha muestra los parámetros de red actuales de **Access Commander** y permite configurarlos. La configuración de parámetros individuales puede realizarse después de habilitar el método de configuración manual.

El método de configuración le permite configurar los parámetros de configuración de la red automáticamente desde el servidor DHCP o manualmente. Al cambiar la dirección IP configurada automáticamente desde el servidor DHCP a una dirección ingresada manualmente, el navegador web será redirigido a la dirección IP ingresada. Se reiniciará después de la redirección.**Access Commander** y es necesario volver a iniciar sesión en el sistema.

ATENCIÓN

- Si cambia el método de configuración a DHCP, cambiará la dirección IP del servidor y puede provocar que se interrumpa la conexión.
- Si cambia el servidor proxy HTTP,**Access Commander**se reiniciará automáticamente.

Detección del cambio de dirección IP del dispositivo

Access Commander establece una conexión con los dispositivos a través de sus direcciones IP. Para evitar la pérdida de conexión con un dispositivo con una dirección IP dinámica, hay dos métodos disponibles para detectar las direcciones IP

- **Network Scanner**
  Access Commander explora periódicamente el segmento de red local utilizando el 2N Network Scanner integrado para identificar los dispositivos conectados y sus direcciones IP actuales.
- **Device callback**
  Este método detecta las direcciones IP de los dispositivos fuera del segmento de red local. Los dispositivos informarán al inicio, cuando se cambie la dirección IP y a intervalos regulares (una vez por hora). Para un funcionamiento correcto, es necesario especificar el destino al que informarán los dispositivos (normalmente una dirección IP **Access Commander**).

Network Discovery

La detección de redes permite a otros servicios, como **2N IP Utility** o **2N Network Scanner**, encontrar la instalación de **Access Commander** en la red local.

Puede utilizar **Network Scanner** y **Axis Utility** al mismo tiempo. Sin embargo, por motivos de seguridad, ambas detecciones de **Access Commander** pueden desactivarse por completo en la configuración del sistema.

SUGERENCIA
Access Commander puede mostrarse u ocultarse en las aplicaciones **2N Network Scanner** y **2N Axis Utility**. Lo mismo se aplica para acceder a la interfaz web utilizando **accesscommander.local**. Si se ejecutan varias instancias de Access Commander en la red, el sistema asigna automáticamente nombres únicos: **accesscommander.local**, **accesscommander-2.local**, **accesscommander-3.local**, y otras instancias en función del número de servidores de la red.

Configuración del proxy

El proxy se utiliza para servicios como: Solicitudes HTTP, sincronización FTP, actualizaciones, etc.

NOTA
No se admite proxy para FTP con autenticación TLS.

1. Vaya a **Ajustes > Configuración > pestaña Red**.
2. Seleccione Editar proxy.
3. En el cuadro de diálogo que se abre, escriba las direcciones del servidor proxy para los protocolos que desee.
4. En el último campo, puede rellenar las direcciones para las que no debe aplicarse el servidor proxy.
   Las conexiones a localhost y a direcciones IP en el rango 127.0.0.1/8 nunca se enrutarán a través de un servidor proxy.
5. Después de cambiar los ajustes, **2N Access Commander** se reiniciará automáticamente.

Uso de NodeRED

La aplicación NodeRED ignora la configuración del proxy del sistema. Para una funcionalidad adecuada, el servidor proxy debe configurarse explícitamente en cada nodo NodeRED que requiera su uso.

Información adicional

MIFARE and DESFire are registered trademarks of NXP B.V.

API HTTP

La URL de la API de **Access Commander** es: https://acom_ip_address/api/v3/.

Se publica una lista de puntos finales de API en http(s)://acom_ip_address/support/api . Fuera de la interfaz **Access Commander** está disponible para ver lista de puntos finales.

Puede filtrar las respuestas a las solicitudes mediante Query. El documento Data Query Customization describe cómo construir **query**.

Autenticación

Los comandos de la API HTTP se envían con las credenciales de acceso del usuario o utilizando un token de autenticación. El token de autenticación lo crea el administrador en la pestaña **Ajustes > Configuración > Tokens de acceso a la API**. Se trata del token de portador. Al crear un nuevo token de acceso a la API, el administrador puede restringirlo para que sea de sólo lectura, de modo que el token sólo autentique comandos GET. El token puede limitarse a: 1 mes, 6 meses, 1 año.

ATENCIÓN
Después de crear un código de acceso, cópielo en el portapapeles y utilícelo. No podrá ver el código más tarde.

SignalR

SignalR es una herramienta que permite la comunicación en tiempo real entre el servidor y el cliente. Esto significa que el servidor puede enviar contenido a los clientes conectados tan pronto como esté disponible y no tiene que esperar una solicitud del cliente. Los principios básicos de SignalR se describen en el documento SignalR integration manual (sólo en inglés). Lista de temas de SignalR disponibles para usar con **Access Commander** se describen en el documento SignalR topics reference manual (sólo en inglés).

Licencias de terceros

Puede encontrar una lista completa de las licencias de bibliotecas de terceros utilizadas en el menú de usuario ubicado a la derecha de la barra superior, en la sección Acerca de.

2N Access Commander – Manual de instalación

2N.com