2N Access Commander

Manual de usuario

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

2N.com

Resumen

Firmware 3.1

Tabla de contenidos

Símbolos y términos utilizados.

En el manual se utilizan los siguientes símbolos y pictogramas:

PELIGRO
Cumplir siempre estas instrucciones para evitar el riesgo de lesiones.

AVISO
Cumplir siempre estas instrucciones para evitar daños al dispositivo.

ATENCIÓN
Advertencia importante. No seguir las instrucciones puede provocar un mal funcionamiento del dispositivo.

SUGERENCIA
Información útil para un uso o configuración más fácil y rápido.

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 los accesos es necesario añadir a **Access Commander Dispositivo**. Los dispositivos son unidades físicas en el edificio que controlan las entradas (intercomunicadores 2N o unidades de acceso 2N) o permiten la comunicación (unidades de contestación 2N). Los dispositivos se agrupan en **Zona**. Cada dispositivo solo puede estar en una zona.

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.
- Agregar usuarios a grupos.
- 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.

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. 42).

Intercomunicadores 2N

- 2N Style IP: admite lectura de códigos QR
- 2N IP Verso 2.0: admite lectura de códigos QR
- 2N IP Verso
- 2N LTE Verso

- 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 IP Access Unit M

Unidades de respuesta 2N

- 2N Indoor View
- 2N Indoor Compact
- 2N Indoor Talk
- 2N Indoor Touch 2.0
- 2N Clip

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

Tabla 1. 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
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	✓	✓	✓	✓	✓
Importar usuarios desde CSV o des-de dispositivos	✓	×	✓	✓	✓
Gestión masiva de firmware	✓	×	✓	✓	✓
Autenticación múltiple	✓	×	✓	✓	✓

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
Autorización de usuario	✓	×	✓	✓	✓
Notificación	✓	×	✓	✓	✓
Presencia	✓	×	✓	✓	✓
Claves de acceso API	✓	×	✓	✓	✓
Registros de cámara	✓	×	✓	✓	✓
control de ascensor	✓	×	✓	✓	✓
Panel	✓	×	✓	✓	✓
Bloqueo de emergencia	✓	×	✓	✓	✓
Soporte de credenciales móviles	✓	×	✓	✓	✓
Gestión de visitas	✓	×	✓	✓	✓
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 (p. 15)

Instalación

Access Commander Se puede distribuir de dos formas:

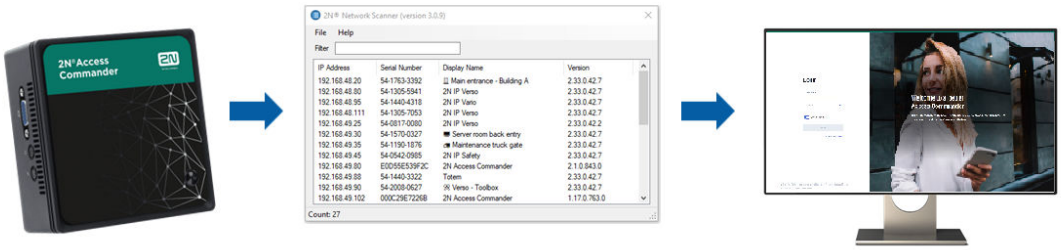
- Una pequeña computadora de escritorio 2N Access Commander Box(2N Nº de referencia 91379030 , Axis Nº de referencia 01672-001)
- computadora virtual

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(2N Nº de referencia 91379030, Axis Nº de referencia 01672-001) es una mini-computadora de escritorio compacta con software preinstalado. Es una solución "plug and play", donde sólo necesitas conectar una fuente de alimentación y un cable Ethernet a esta minicomputadora. Para una correcta y completa funcionalidad del sistema, se recomienda colocar esta minicomputadora en un lugar seguro y dejarla funcionando permanentemente. Access Commander Box Sirve como servidor para recopilar datos, eventos y registros de todo el sistema de acceso.

Iniciar sesión en Access Commander con una dirección IP dinámica



1. Conectar Access Commander Box a la red mediante un cable Ethernet.
2. Usando la aplicación 2N Network Scanner 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.

Establecer una dirección estática Access Commander ayuda 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. Inicie sesión en el sistema como “raíz” con contraseña “2n”. Una vez que aparezca la pantalla azul, cambie la contraseña predeterminada.
4. En el menú avanzado, seleccione “Redes” y posteriormente “IP estática”.
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.

Parámetros técnicos Access Commander Box

- Diseño ultracompacto: 0,69 L (56,1 x 107,6 x 114,4 mm)
- 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

Distribución a través de máquina virtual.

Access Commander Se puede distribuir como una máquina virtual. A continuación se detallan los procedimientos de instalación en plataformas de virtualización compatibles.

Virtual Box

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

1. DE https://www.virtualbox.org/wiki/DownloadsDescargue la última versión de VirtualBox.
   Se recomienda descargar la versión que incluye el paquete de extensión de VirtualBox.
2. Descargue el software apropiado de la sección 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.

Reproductor VMware

ATENCIÓN
La versión compatible de VMWare es 6.5 y superior.

1. Descargue el software apropiado de la sección 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 de la sección 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).
   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 de la sección 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

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.

Tabla 2. 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

Tabla 3. Access Commander Box

Número de dispositivos conectados 2.0	Número de usuarios 2.0	Número de usuarios en el grupo.
2000	100000	1500

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.

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 indicar al distribuidor el número de serie de uno de los dispositivos 2N conectados a **Comandante de acceso**. El archivo de licencia se genera en función del número de serie de este dispositivo de licencia.

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 **Ajustes** > **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.

Suspensión de licencia

La suspensión de la licencia ocurre si el dispositivo con licencia se desconecta de**Access Commander**por un período superior al período de protección de la licencia. La duración del período de protección depende de cuánto tiempo el dispositivo con licencia ha estado conectado en **Access Commander**. La duración de los períodos de protección se enumeran en la mesa debajo.

Cuando se suspende una licencia, todos los dispositivos conectados automáticamente dejan de administrarse y se marcan como no administrados. Para reactivarlos, debe conectar y activar el dispositivo con licencia o generar y cargar un nuevo archivo de licencia para otro dispositivo.

En el caso de cargar una nueva licencia, primero deberá activar el dispositivo de licencia para el cual se genera la nueva licencia. Después de activar el dispositivo con licencia, también será posible activar todos los demás dispositivos.

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

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).*

Interfaz **Access Commander** es accesible a través de un navegador web. La dirección IP de la interfaz web se puede buscar usando el programa 2N Network Scanner.

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.

Panel

El panel es la vista básica de la interfaz web. **Access Commander**. Es un tablón de anuncios configurable que muestra datos en tiempo real. **Access Commander** ofrece varios widgets que se agregan al panel mediante un botón . Los widgets en el Panel se pueden mover, cambiar de nombre o realizar su configuración básica de varias maneras. La gestión y eliminación de widgets se realiza en el menú ampliado. 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 Ver 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 Ver 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 eventos y notificaciones que **Access Commander** generado.

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

- gravedad (información, advertencia, error);
- la hora en que ocurrió el hecho;
- la categoría a la que pertenece la acción (Estado del dispositivo, Importación, Sincronización de usuarios, Sistema, Acciones de usuario, Restricciones de área);
- sujeto al que se refiere la acción (dispositivo, usuario, zona, visita...);
- una breve descripción del evento;
- 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

La lista se puede descargar en un archivo CSV o imprimir haciendo clic en el botón Exportar 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 almacenamiento para un tipo determinado de registro se establece en la pestaña Configuración > Retención de registros. La retención de las grabaciones de la cámara no puede durar más que la retención de los registros de acceso y del sistema.

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

La lista se puede descargar en un archivo CSV o imprimir haciendo clic en el botón 

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 almacenamiento para un tipo determinado de registro se establece en la pestaña Configuración > Retención de registros. La retención de las grabaciones de la cámara no puede durar más que la retención de los registros de acceso y del sistema.

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

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.

También se muestra una lista de notificaciones en la página Registros del sistema > Notificaciones.

La lista se puede descargar en un archivo CSV o imprimir haciendo clic en el botón 

encima de la lista. En el archivo CSV exportado, la hora se indica en GMT+0.

Configurar un nuevo tipo de notificación

1. ir a la pagina **Ajustes** > **Notificación**.
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 determinado. El detalle del tipo de notificación se abre haciendo clic en la notificación seleccionada en la lista en 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.

La notificación en **Access Commander** aparece debajo del icono  en la barra superior, al lado del 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. 59).

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 almacenamiento para un tipo determinado de registro se establece en la pestaña Configuración > Retención de registros. La retención de las grabaciones de la cámara no puede durar más que la retención de los registros de acceso y del sistema.

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.

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.

llave móvil

En la empresa es posible configurar los parámetros de emparejamiento con la aplicación 2N Mobile Key, que permite la autenticación Bluetooth. Se establecen tanto los dispositivos en los que los usuarios podrán realizar la vinculación como el tiempo de validez de la Mobile Key necesaria para la vinculación. La propia Mobile Key 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. 51).

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
- Mobile Key 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.

   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.
3. 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.
4. en tarjeta **Opciones** puede asignar datos de usuario a atributos en el servidor LDAP.

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

Opciones de sincronización LDAP

Atributos importados – editando el esquema, la asignación de datos de **Access Comandaner** a los atributos en el servidor LDAP.

Usuarios eliminados de LDAP – define lo que debería suceder con los usuarios que han sido eliminados en LDAP. Los usuarios eliminados de LDAP pueden ser **Access Comandaner** guárdelos o elimínelos también. Si los usuarios se van a deshabilitar, después de eliminarlos de LDAP, sus datos permanecerán en **Access Comandaner**, pero no se sincronizará con los dispositivos.

Usuarios deshabilitados en Active Directory – establece lo que sucede con los usuarios que han sido prohibidos en Active Directory. Deshabilitar en Active Directory puede **Access Comandaner** ignorar o puede eliminar (prohibir) al usuario. Después de la reactivación en Active Directory, los usuarios eliminados se cargan nuevamente en **Access Comandaner.**

Sincronización de grupos – permite cargar membresías de grupos desde LDAP a **Access Comandaner**. Usando la configuración del esquema de sincronización, es posible definir su propio DN base y el filtro según el cual se sincronizarán los grupos. El esquema permite la sincronización 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 buscar en todo el árbol, en caso contrario sólo se busca en 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.

Usuarios

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

Todos los usuarios creados se muestran en la lista de usuarios. Los usuarios se pueden filtrar encima de la lista o puede buscar directamente un usuario específico por su nombre, correo electrónico o número de teléfono.

Acciones masivas

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

- 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
- Asignar una Mobile Key a aquellos usuarios de la selección a los que aún no se les ha asignado una Mobile Key

NOTA
Para poder asignar un código PIN/QR o una Mobile Key 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.

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 Descripción general, Asistencia y Registro de cambios. La pestaña de asistencia se muestra solo para aquellos usuarios que han habilitado el seguimiento, consulte Seguimiento de asistencia de usuarios (p. 34). El módulo de asistencia está disponible según 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 leer acercando la tarjeta al lector o introduciendo la tarjeta de identificación mediante 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.

Mobile Key – utilizado para conectarse a la aplicación 2N Mobile Key habilitar la autenticación a través de Bluetooth, consulte el capítulo autenticación Bluetooth (p. 33).

Código PIN – genera automáticamente un PIN de 6 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 digital, que el usuario puede usar para autenticarse en dispositivos que admitan su lectura. Cada usuario puede cargar hasta 2 huellas dactilares. El procedimiento se describe en el capítulo. Carga de huellas dactilares (p. 32).

Placa – establece la matrícula del vehículo del usuario, que el dispositivo puede escanear 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

Al establecer un nombre de inicio de sesión y una contraseña de un solo uso, es posible otorgar al usuario acceso a la interfaz **Access Commander**. Una vez que haya iniciado sesión, el usuario puede realizar un seguimiento de su asistencia (si está disponible), cambiar su correo electrónico o cambiar su foto de perfil. En el primer inicio de sesión, se le pedirá al usuario que cambie la contraseña. Si se requiere autenticación de dos factores para un usuario, se le pedirá que se vincule a una aplicación de autenticación personalizada, consulte Autenticación de dos factores (p. 65). En esta pestaña también es posible eliminar la conexión con la aplicación de autenticación.

En la pestaña Cuenta, es posible otorgar permisos administrativos a los usuarios con datos de inicio de sesión. **Access Commander** utilizando roles de usuario. Las autorizaciones de roles individuales se describen en el capítulo Permisos de usuario (p. 7).

Interfaz simplificada

Se puede iniciar una interfaz de usuario simplificada para un único administrador de visitas a la empresa. Una interfaz simplificada permite al administrador de visitantes agregar, eliminar y administrar visitantes. Los registros y la presencia no se pueden ver en la interfaz simplificada. El objetivo de la interfaz simplificada es principalmente facilitar a los usuarios de los apartamentos la concesión de acceso a sus visitantes. Todas las visitas creadas en la interfaz simplificada siempre se asignan a *grupo predeterminado para nuevas visitas*. El administrador de visitas no tiene la opción de cambiar este grupo. El grupo predeterminado para nuevos visitantes debe seleccionarse de antemano en la configuración de la empresa y se deben establecer reglas de acceso válidas para el acceso al apartamento, incluida la ruta hasta el mismo, para el grupo. 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 configurar el grupo predeterminado para nuevas visitas** en Configuración de la empresa (p. 25). Dichas reglas de acceso deben asignarse al grupo predeterminado para que el visitante tenga acceso a las áreas visitadas. Sin un grupo predeterminado configurado correctamente, 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 información relacionada con su cuenta v**Access Commander**;
- **Número de usuario** – identificador específico, necesario para la sincronización masiva con un archivo CSV (ver Sincronización de usuarios con FTP (p. 62));
- **Una nota**.

Enfoques

La pestaña de accesos se utiliza para asignar el usuario a un grupo y establecer el intervalo de tiempo en el que los datos de acceso del usuario serán válidos. El intervalo de tiempo se establece en el menú ampliado de la tarjeta, que se abre haciendo clic en .

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 ese grupo. Si el usuario no está asignado a un grupo, se puede agregar en la pestaña. El grupo se puede cambiar o eliminar en el menú avanzado. .

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.

El número de teléfono virtual se puede utilizar para llamar al usuario mediante el teclado numérico del dispositivo. Un número virtual puede tener de dos a cuatro dígitos. Los números virtuales no están relacionados con los números de teléfono propios del usuario, lo que les permite ocultar sus propios números de teléfono en el dispositivo. En la pestaña también es posible configurar un representante a quien se desviará la llamada en caso de indisponibilidad de este usuario. El representante puede ser elegido 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 dactilares externo para cargarlas. Comprueba si tienes el controlador instalado 2N USB Driver. El controlador está disponible para descargar. 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 esté en **Ajustes** > **Enfoques** Lector de huellas USB habilitado.
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 Mobile Key, que el usuario deberá tener descargado en su teléfono móvil.

Conexión de la aplicación en el teléfono del usuario con dispositivos v **Access Commander** se realiza ingresando el código de emparejamiento en la aplicación Mobile Key.

El código de emparejamiento se puede obtener de dos formas:

- a través de un lector USB Bluetooth conectado a una computadora
- conectando al dispositivo.

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 esté habilitado en el **Ajustes** > **Enfoques** > **la pestaña Lectores USB habilitados**.
3. Conecte el lector Bluetooth USB al ordenador.
4. En configuración de usuario v **Pestaña de autenticación** elegir autenticación Mobile Key.
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 a continuación para emparejar en la aplicación abajo (p. 33).

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. 45);
   - se establece un tiempo adecuado para el emparejamiento, a saber???.
2. En configuración de usuario v **Pestaña de autenticación** elegir autenticación Mobile Key.
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 a continuación para emparejar en la aplicación abajo (p. 33).

Emparejamiento en la aplicación móvil Mobile Key

1. Descarga la aplicación Mobile Key a tu teléfono móvil. La aplicación está disponible en App Store y Google Play.
2. Abra la aplicación y habilítela Mobile Key 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 Mobile Key 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.

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. 48).

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. 49).

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. Mobile Key
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.

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.

La lista se puede descargar en un archivo CSV o imprimir haciendo clic en el botón 

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

Icono  en la línea del dispositivo redirige a la interfaz de configuración web del dispositivo determinado.

Estados del dispositivo

- Online
- No administrado
- Incompatible
- 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.

Agregar un nuevo dispositivo

1. ir a la pagina **Dispositivo**.
2. Haga clic en el botón Agregar dispositivo en la esquina superior derecha.
3. En la ventana de diálogo abierta, busque el dispositivo en la red local o escriba su dirección IP y el puerto correspondiente en el formato:“Dirección: puerto”
   Después de ingresar la dirección IP del dispositivo, es posible presionar ENTER en el teclado para ingresar otro dispositivo.
4. 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.
5. Nombra el dispositivo antes de crearlo.

Los dispositivos recién agregados aparecen en la lista. Realice más ajustes del dispositivo en los detalles del dispositivo.

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 dispositivos. Los dispositivos en línea son los que tiene con **Access Commander** conexión establecida y en la 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 en la página **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 habilitada (consulte Configuración del punto de acceso del dispositivo (p. 49)), se muestra la opción de asignar 2 zonas. Un punto de acceso de dispositivo solo puede estar en una zona.

Configuración

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

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 al lado del botón Abierto.

Se utiliza para cerrar puertas incluso para grupos con acceso válido. Bloqueo de emergencia (p. 39).

Respaldo

Permite realizar una copia de seguridad de la configuración del intercomunicador en un archivo xml. La copia de seguridad se inicia usando Comenzar respaldo. La última copia de seguridad se muestra en la pestaña desde donde puede descargar el archivo de copia de seguridad. El dispositivo se puede sincronizar automáticamente con la última copia de seguridad usando el menú v Restaurar. En este menú es posible sincronizar el dispositivo según una copia de seguridad almacenada en otro dispositivo.

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

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. Ir a **Dispositivo** > detalle del dispositivo > **Pestaña de llamadas** > **Pestaña de 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

Usando la conexión del módulo de relé EJE A9188 a Intercomunicador IP 2N (2N IP Verso, 2N IP Force, 2N IP Safety, 2N IP Vario) o para Access Unit El acceso a plantas individuales del edificio se puede controlar mediante un ascensor. A uno Intercomunicador IP 2N cuyo Access Unit Es posible conectar un máximo de estos 5 módulos de relé, mientras que cada uno de los módulos puede controlar 8 plantas, es decir, un máximo de 40 plantas en total. Para utilizar esta función, debe tener una licencia activa para Intercomunicadores IP 2N (n.º de pedido 9137916) y licencia Access Unit (2N Nº de referencia 9160401).

Configuraciones de control de ascensor

1. 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**.

2. En el encabezado de detalles del dispositivo, vaya a Configuración de hardware dispositivo. En la sección Hardware > Control del ascensor, active los módulos que se supone deben controlar el acceso desde el ascensor. Si los módulos requieren autenticación, ingrese un nombre de usuario y contraseña. Guarde la configuración. Salga de la configuración de hardware usando la cruz en la barra azul superior.
3. Vaya a la pestaña Elevador en los detalles del dispositivo.
4. 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 .
5. 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 pestaña muestra todos los módulos AXIS A9188 conectados y sus estados actuales.

Supervisión
La página se utiliza para encontrar información sobre los dispositivos conectados. Cada administrador puede configurar la mesa según sus propias necesidades utilizando . La configuración es única para cada cuenta. La configuración se realiza seleccionando las columnas mostradas.

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.

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.

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

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.

Exclusión de dispositivos

Los dispositivos se pueden excluir de la administración masiva de firmware agregándolos a la lista en la pestaña Dispositivos > Firmware > 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 utilizando una versión de firmware no compatible si esa versión está aprobada. La aprobación se realiza en la pestaña Dispositivo > Firmware > Versión de firmware incompatible usando el ícono .

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

Versiones de firmware compatibles

- 2.43
- 2.42
- 2.41
- 2.40
- 2.39
- 2.38

Seguridad

Después de habilitar la verificación del certificado SSL, la sincronización solo se producirá en dispositivos que tengan un certificado SSL firmado por una autoridad confiable. Se deshabilitará la sincronización de dispositivos sin dichos certificados SSL.

Para una autenticación exitosa, los certificados del dispositivo deben estar firmados por una CA y contener la dirección IP o el nombre de dominio del dispositivo. El servidor en el que se ejecuta debe confiar en el certificado de la autoridad firmante.**Access Commander**. Los certificados del dispositivo deben cargarse a través de la interfaz web del dispositivo (Sistema > Certificados > Certificados personales) y configurarse como un certificado de servidor HTTPS en Servicios > Servidor web > Configuración avanzada.

ATENCIÓN
en el dispositivo 2N Indoor Touch No puede cargar sus propios certificados SSL; después de habilitar la verificación del certificado, se perderá la conexión con ellos.

Configuración del punto de acceso del dispositivo

Dispositivo (intercomunicador 2N o Unidad de Acceso 2N) puede tener hasta dos puntos de acceso. Cada punto de acceso permite el paso en una dirección. Los puntos de acceso distinguen la dirección de paso a través del dispositivo. A cada punto de acceso se le pueden asignar uno o más lectores que están conectados al dispositivo y operan en la dirección del punto. Los puntos de acceso se utilizan para registrar la entrada o salida de una zona. Su uso es necesario si el dispositivo está ubicado en la interfaz entre dos zonas.

Los puntos de acceso también se utilizan para rastrear a los usuarios en el módulo. Presencia (p. 53). Los puntos de acceso también se utilizan para monitorear la entrada y salida. Restricciones de área (p. 55).

NOTA
Configuración de puntos de acceso individuales en **Comandante de acceso** se prescribe en la interfaz web del dispositivo en la sección Servicios > Control de acceso:

- Punto de acceso 1 = Reglas de llegada
- Punto de acceso 2 = Reglas de salida

Configurar puntos de acceso

1. Ingrese a la interfaz de configuración web del dispositivo.

   SUGERENCIA
   Es posible ingresar a la configuración web del dispositivo directamente en la interfaz desde la configuración del dispositivo.

2. Vaya a la sección Hardware > menú Módulos de expansión.
3. Ubique el módulo de acceso que se utilizará como Punto de acceso 1 (llegada) o Punto de acceso 2 (salida).
4. En el parámetro Puerta, establezca la dirección deseada y guarde la configuración.
5. Ir a la página de Zonas v **Comandante de acceso**.
6. En la esquina superior derecha, presione y habilitar el uso de puntos de acceso.

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.

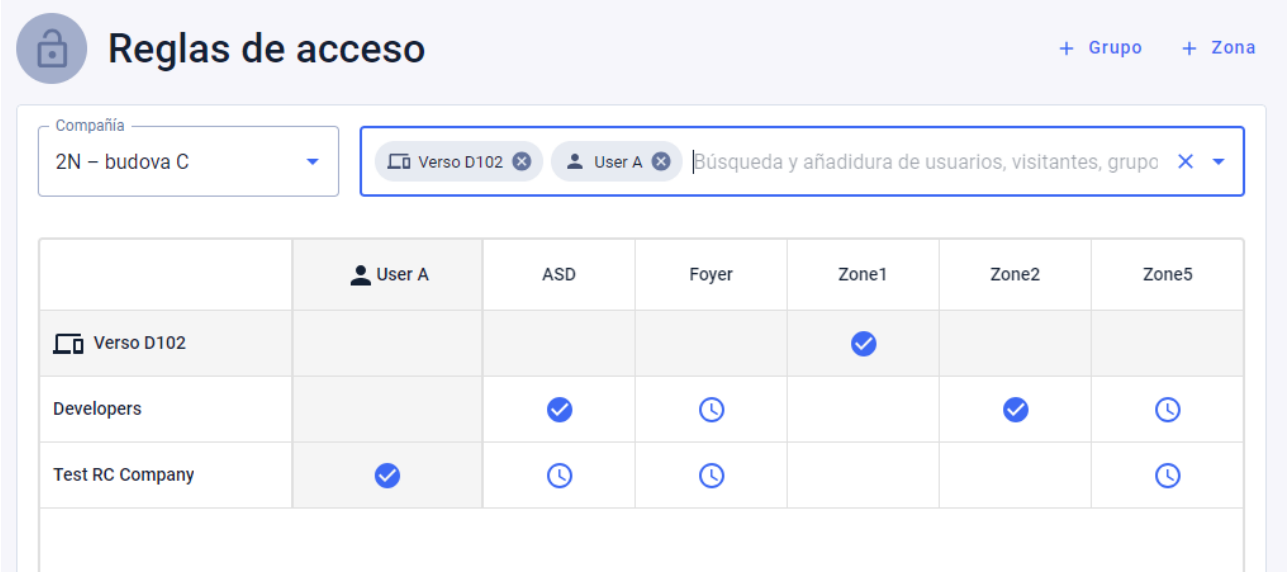
Visualización matricial

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. 47). 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.

Creando un perfil de tiempo

1. ir a la pagina **Perfiles de tiempo**.
2. Haga clic en el botón para agregar un perfil de tiempo en la esquina superior derecha.
3. En el cuadro de diálogo abierto, establezca el nombre del perfil de tiempo.
4. Seleccione una opción para elegir un límite de tiempo Agregar franjas horarias. Los días verdes identifican los días que caen dentro del perfil horario. El día se selecciona haciendo clic. En unos días, es posible establecer un intervalo de tiempo que determine la validez del perfil horario.
   Solo se pueden configurar diferentes horas para cada día cuando se crea el perfil de hora.

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.

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 su modalidad se realiza en **Ajustes** > **Configuración** > **la pestaña Asistencia**, ver Configuración de asistencia (p. 49).

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. 29).

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

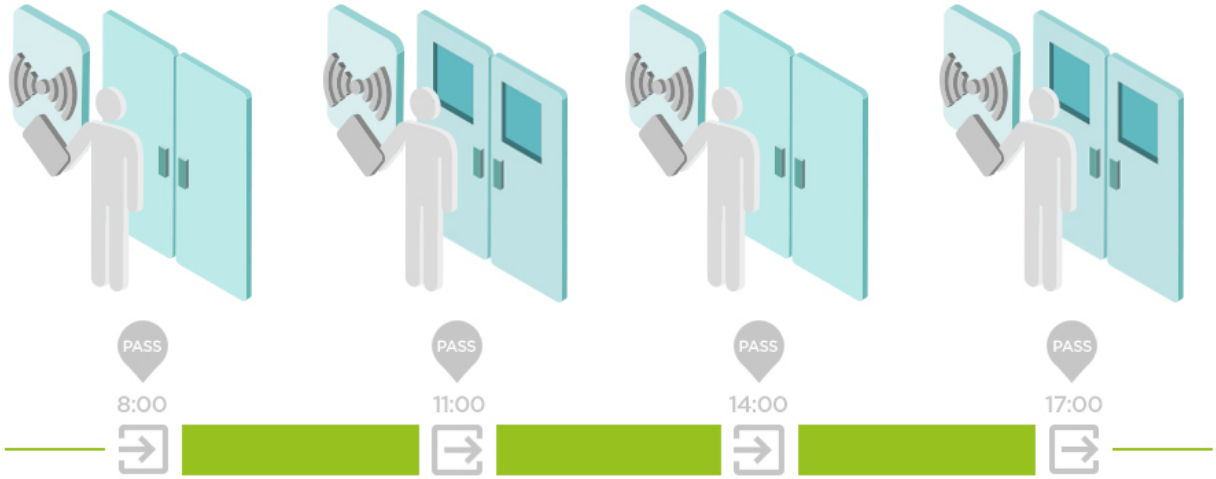
El administrador de asistencia puede editar los datos de asistencia del usuario. La edición se realiza haciendo clic en el intervalo de tiempo que se va a cambiar. Una vez abierto, se pueden editar los tiempos límite y se puede agregar una nota al intervalo.

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

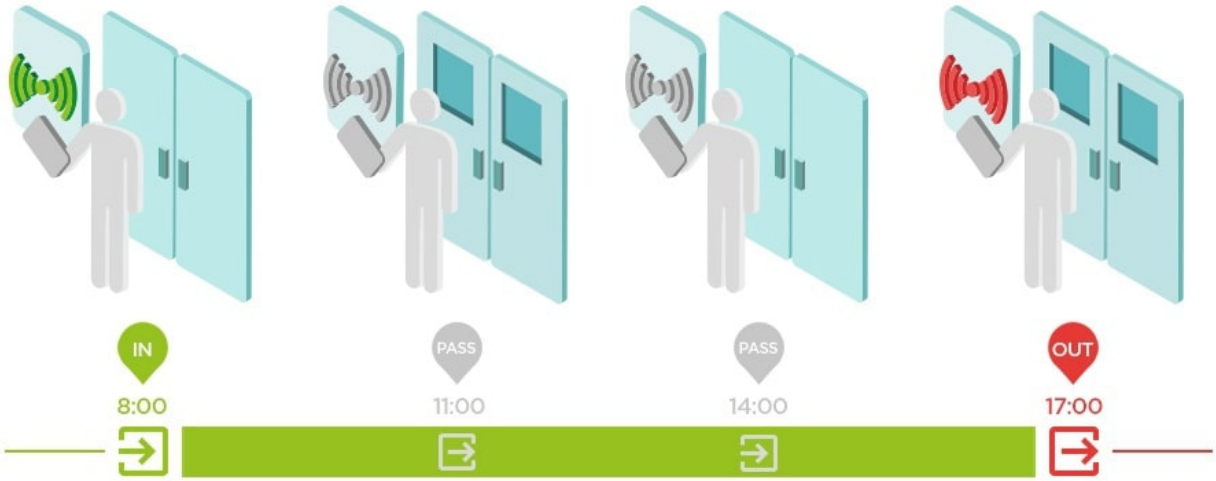
- **GRATIS**



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**

Los dispositivos de entrada y salida deben configurarse para que funcionen correctamente.



- **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

Dispositivo (intercomunicador 2N o Unidad de Acceso 2N) puede tener hasta dos puntos de acceso. Cada punto de acceso permite el paso en una dirección. Los puntos de acceso distinguen la dirección de paso

a través del dispositivo. A cada punto de acceso se le pueden asignar uno o más lectores que están conectados al dispositivo y operan en la dirección del punto. Los puntos de acceso se utilizan para registrar la entrada o salida de una zona. Su uso es necesario si el dispositivo está ubicado en la interfaz entre dos zonas.

Los puntos de acceso también se utilizan para rastrear a los usuarios en el módulo. Presencia (p. 53). Los puntos de acceso también se utilizan para monitorear la entrada y salida. Restricciones de área (p. 55).

NOTA
Configuración de puntos de acceso individuales en **Comandante de acceso** se prescribe en la interfaz web del dispositivo en la sección Servicios > Control de acceso:

- Punto de acceso 1 = Reglas de llegada
- Punto de acceso 2 = Reglas de salida

Configurar puntos de acceso

1. Ingrese a la interfaz de configuración web del dispositivo.

   SUGERENCIA
   Es posible ingresar a la configuración web del dispositivo directamente en la interfaz desde la configuración del dispositivo.

2. Vaya a la sección Hardware > menú Módulos de expansión.
3. Ubique el módulo de acceso que se utilizará como Punto de acceso 1 (llegada) o Punto de acceso 2 (salida).
4. En el parámetro Puerta, establezca la dirección deseada y guarde la configuración.
5. Ir a la página de Zonas v **Comandante de acceso**.
6. En la esquina superior derecha, presione y habilitar el uso de puntos de acceso.

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 el acceso de las visitas no deberá exceder de un mes.

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. 51).

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. 52).

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 subpágina Tarjetas se utiliza para administrar las tarjetas de acceso de visitantes que están disponibles para agregar a una visita. Se agrega una nueva tarjeta usando el botón Agregar 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.

Presencia

El módulo de presencia es una extensión del módulo de asistencia y se utiliza para mostrar una lista de usuarios que se encuentran actualmente en el edificio. Para el funcionamiento del módulo, es necesario configurar el modo de asistencia IN-OUT v **Ajustes** > **Configuración** > **la pestaña Asistencia**, ver Configuración de asistencia (p. 49).

- Si el último evento del usuario en un día determinado es una llegada (**EN** evento), se toma como presente.
- Si el usuario pasa por un lector que tiene configurada una dirección no especificada, la zona en la que se encuentra el usuario cambiará. Lo mismo sucede si pasa por el lector en el modo**EN**.
- Si el último Evento en el día dado es una salida (**AFUERA** evento), se toma 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.

- **Mobile Key** – 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. Mobile Key, 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. 62).

  ATENCIÓN
  ¡El archivo contiene datos confidenciales!

Restricciones de área

Las restricciones de área se utilizan para definir las áreas en las que se pueden utilizar las funciones Anti-passback y Ocupación.

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.

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. 49). Las propiedades del punto de acceso se expanden al hacer clic en la flecha.

Ocupación

Los dispositivos de entrada y salida deben configurarse para que funcionen correctamente.

La pestaña Ocupación le permite monitorear y controlar la cantidad de personas en un área. Las restricciones de ocupación ayudan a administrar la cantidad de personas en un área. Si se alcanza el límite de ocupación, es posible denegar más accesos o registrar únicamente la superación del límite. Se requiere un dispositivo de entrada y salida para esta función.

Anti-passback

Es posible activar la función Anti-passback en el área, que asegura la extensión del control de acceso mediante monitoreo y uso indebido de los derechos de reingreso a áreas reservadas. Las áreas monitoreadas

están definidas por dispositivos fronterizos que conducen al interior de las instalaciones o permiten salir de ellas. En estos dispositivos, cuando las personas pasan, se comprueba la autorización según las reglas definidas para la zona determinada. Después de abandonar el área a través del dispositivo fronterizo, el usuario solo puede regresar al área después de que haya expirado el tiempo de espera, si el tiempo de espera está configurado. Si el usuario intenta regresar al área antes, el sistema le negará el acceso o solo registrará este evento en el registro.

AVISO
Un área anti-passback pierde su significado y puede ser potencialmente peligrosa si hay un dispositivo en el área con un botón REX activo adjunto que permite el acceso no autorizado.

Establecer una excepción

A veces puede ser deseable que los términos anti-passback no se apliquen a usuarios seleccionados. Normalmente, se trata de usuarios como el administrador del edificio, el director ejecutivo, usuarios VIP, etc. Los usuarios o grupos completos que no deben estar sujetos a las condiciones anti-passback se configuran en Configuración > Anti-passback > Excepciones.

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

Lista de usuarios bloqueados

Los usuarios bloqueados son aquellos usuarios que intentaron acceder al área Anti-passback antes de que expirara el tiempo de espera. Ayuda  Los usuarios pueden ser excluidos de la lista, permitiéndoles acceder nuevamente al área.

SUGERENCIA
Cuando a un usuario se le niega el acceso debido a un anti-passback activo, se le puede enviar un correo electrónico de información automática. Puede habilitar el envío de correo electrónico en Configuración > Anti-passback > Notificar al usuario bloqueado mediante la pestaña de correo electrónico.

Restablecer restricciones

En Configuración > Anti-passback > pestaña Restablecer restricciones de área, se configuran los días y horas en que se eliminará el registro de área, es decir, todos los usuarios podrán volver a pasar independientemente de infracciones anteriores.

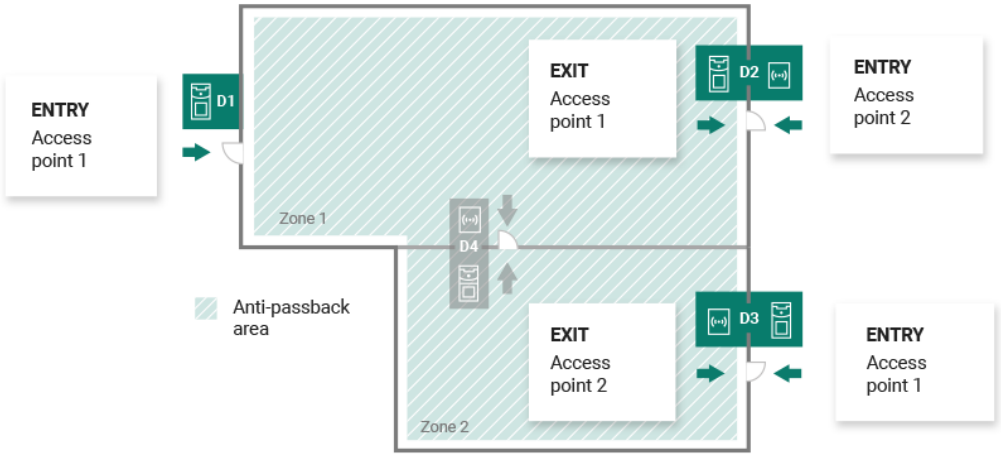
Los errores de configuración más comunes

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. Para que funcione correctamente, es necesario ajustar la asignación.
- 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

Fecha y hora

Fecha y hora en **Access Commander** Se puede sincronizar con Internet o configurar manualmente. El cambio del método de adquisición de hora se realiza en la pestaña Configuración > Configuración > Fecha y hora. En caso de que no lo sea **Access Commander** conectado a Internet, deberá configurar la fecha, la hora y la zona horaria manualmente. De lo contrario, es posible cambiar a NTP y obtener la hora de un servidor NTP. En este caso, sólo necesitas 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 se puede unificar con la hora. **Access Commander**. El tiempo compartido con dispositivos se activa alternando el parámetro Sincronizar con el dispositivo en Configuración > Configuración > pestaña 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**.
- **Los dispositivos utilizan Access Commander como servidor NTP** – controla el tiempo en los dispositivos según el tiempo establecido en**Access Commander**.

Configuración de la red

Los ajustes de conexión de red se realizan en la pestaña Configuración > Configuración > Red. La pestaña muestra los parámetros de red actuales. **Access Commander** y permite configurarlos. Es posible configurar parámetros individuales 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.

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.

Los ajustes se realizan en Ajustes > Configuración > Correo electrónico.

1. 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.
2. 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).
3. 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**.
4. Puede comprobar la configuración realizada enviando un correo electrónico de prueba.

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> Actualizaciones del sistema.

Instalar la actualización Access Commander

AVISO

Se recomienda hacer esto antes de instalar la actualización. copia de seguridad del sistema (p. 60). Realizar la copia de seguridad fuera del horario comercial para evitar la indisponibilidad temporal del sistema para los usuarios.

1. Ir a **Ajustes** > **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.

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 habilitación se realiza en Configuración > pestaña Actualización del sistema > Actualizar parámetro del servidor.

AVISO
La versión de prueba no está garantizada y la empresa no la proporciona. 2N TELEKOMUNIKACE 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

En la página Configuración > pestaña Copia de seguridad del sistema, es posible realizar, configurar y controlar la copia de seguridad y restauración de datos.**Access Commander**. Los datos se pueden almacenar en un almacenamiento local o en un bloque de mensajes del servidor (SMB). 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. Ir a **Ajustes** > **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. Ir a **Ajustes** > **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.

Al guardar, las copias de seguridad se realizarán automáticamente según la configuración seleccionada.

Configuración de copia de seguridad de datos en SMB

1. Ir a **Ajustes** > **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.

Al guardar, todas las copias de seguridad se enviarán al bloque de mensajes del servidor configurado.

Restaurar desde datos de respaldo

1. Ir a **Ajustes** > **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. Ir a **Ajustes** > **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. Ir a **Ajustes** > **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 **Ajustes** > **Pestaña Sincronización de usuarios**. Puede descargar un archivo CSV de muestra desde la tarjeta.

SUGERENCIA
La lista de usuarios actuales, que corresponde a la estructura del archivo CSV de muestra, se puede descargar desde la página Informes (p. 54).

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. Haga clic en en el parámetro Almacenamiento.
2. En el cuadro de diálogo abierto, configure la dirección del servidor FTP donde está almacenado el archivo CSV.
3. Ingrese las credenciales para acceder al servidor FTP.

archivo CSV

DESCARGAR
Puede descargar un archivo CSV de muestra para la sincronización de usuarios usando este enlace.

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.

Lectores USB habilitados

Para facilitar el registro de algunos métodos de autenticación de usuarios, es posible utilizar lectores USB conectados al ordenador en el que se encuentra **Access Commander**. Se requieren lectores en **Access Commander** habilítelo en Configuración > Acceso > pestaña Lectores USB permitidos.

Habilitar/deshabilitar el uso de un dispositivo USB externo se realiza en un cuadro de diálogo que se abre al hacer clic en Habilitar lectores. Posteriormente se modifica su permiso haciendo clic en Alterar.

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
- Lector Bluetooth USB externo (dongle) – N.º de pedido 9137422E, Parte del EJE. Bien 01402-001

Teclas PICard

Las claves de cifrado de aplicaciones se almacenan en Configuración > Acceso > pestaña Claves PICard 2N PICard Commander. Si las claves de cifrado están en **Access Commander** cargado, el nombre del proyecto se muestra en la pestaña PICard Commander y un identificador de exportación de clave numérica. La tarjeta permite cargar claves desde **Access Commander** borrar.

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

Importar claves de cifrado PICard

1. Después de hacer clic en Importar cargue el archivo de clave de cifrado desde su repositorio.
2. 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.

Claves de cifrado para Mobile Key

Los usuarios pueden utilizar la aplicación para conectarse con dispositivos 2N Mobile Key. Comunicación entre aplicaciones Mobile Keyy siempre está cifrado por el dispositivo. Sin conocimiento de la clave de cifrado, la aplicación no puedeMobile Keyautenticar al usuario. La clave de cifrado principal se genera automáticamente cuando se inicia el intercomunicador por primera vez y se puede regenerar manualmente en cualquier momento posterior. La clave de cifrado principal se transfiere junto con el ID de autenticación al dispositivo móvil durante el emparejamiento.

Comunicación entre aplicaciones Mobile Keyy siempre está cifrado por el dispositivo. Sin conocimiento de la clave de cifrado, la aplicación no puedeMobile Keyautenticar al usuario. La clave de cifrado principal se genera automáticamente cuando se inicia el intercomunicador por primera vez y se puede regenerar manualmente en cualquier momento posterior. La clave de cifrado principal se transfiere junto con el ID de autenticación al dispositivo móvil durante el emparejamiento.

EN **Configuración > Acceso > pestaña Claves de cifrado para Mobile Key** es posible generar hasta 4 claves de cifrado. La clave recién generada se carga automáticamente en la aplicación. Mobile Key la primera vez que utiliza un teléfono móvil con un dispositivo previamente emparejado. Al intentar generar la quinta clave **Access Commander** advierte que generarla eliminará la clave más antigua. La tarjeta muestra los tiempos de generación de claves individuales.

Si no tiene aplicación Mobile Key acceso a cualquiera de las claves de cifrado válidas, no será posible utilizarla para autenticar al usuario. Para restaurar la funcionalidad de la aplicación, es necesario volver a emparejar la aplicación con el dispositivo conectado a **Access Commander**, que cargará claves de cifrado válidas en la aplicación Mobile Key.

NOTA
Permitir el acceso al dispositivo depende de los derechos de acceso establecidos por el usuario.

Registros de cámara

Los registros CAM se utilizan para grabar automáticamente varias imágenes antes y después del evento seleccionado. En Configuración > Registros CAM, puede administrar diferentes tipos de eventos para los cuales 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. ir a la pagina **Ajustes** > **Registros de cámara**.
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

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.

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.

El administrador establece la autenticación de dos factores en la pestaña Configuración > Configuración > Autenticación de dos factores. El administrador puede elegir qué usuarios deberán tener 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, ver Activar la verificación en dos pasos (p. 66).

- **Requerido para usuarios con un rol**
  Cada usuario al que se le ha asignado un rol debe confirmar su inicio de sesión mediante aplicaciones de autenticación.
- **Obligatorio**
  Todos los usuarios deben confirmar su inicio de sesión mediante una 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. Seleccione Ver perfil.
3. En la pestaña Verificación en dos pasos, vincula la cuenta a la aplicación de verificación. Sigue las instrucciones.

Permitir acceso SSH

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

En Configuración > Configuración > la pestaña SSH se usa para habilitar Secure Shell, que proporciona comunicación remota segura con la consola del sistema. Con el servicio SSH habilitado, puede realizar una copia de seguridad y restaurar su sistema o realizar un reinicio completo**Access Commander**.

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

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

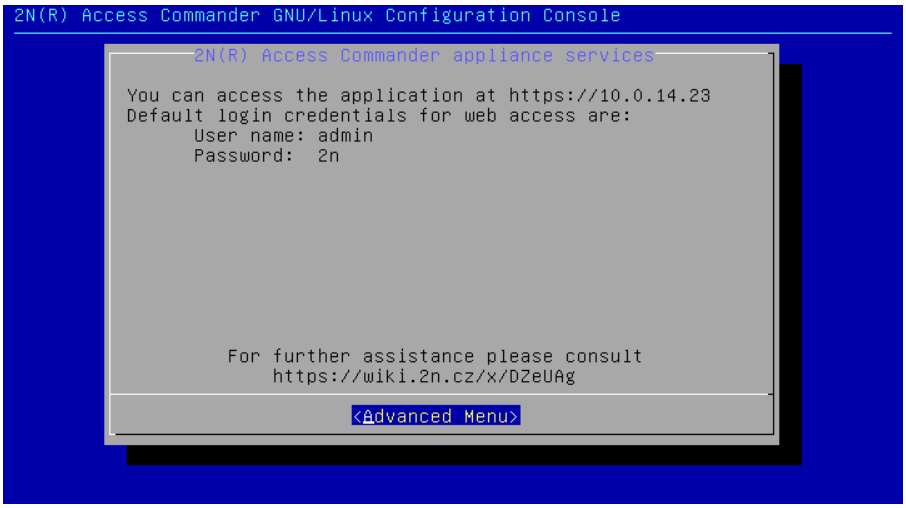
El acceso SSH también se puede habilitar y administrar directamente en la consola de configuración de Linux, consulte Configuración de Linux (p. 66).

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.

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. Ir a **Ajustes** > **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.

Información adicional

API HTTP

La URL de la API **Comandante de acceso** 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 lanzado con la versión de firmware 2.7.

Autenticación

Los comandos HTTP API se envían con credenciales de usuario o mediante autenticación de token. El token de autenticación lo crea el administrador en Configuración > Configuración > pestaña Clave de acceso API. La clave de acceso API tiene la función de Bearer Token. Al crear una nueva clave de acceso API, el administrador puede restringir la validez de la clave a solo lectura, por lo que la clave solo será autenticada mediante comandos GET. Las claves se pueden limitar a: 1 mes, 6 meses, 1 año.

ATENCIÓN
Después de crear la clave de acceso, cópiela en el portapapeles y úsela. Más tarde, la clave ya no será visible.

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.

wiki.2n.com

2N Access Commander – Manual de usuario

2N.com