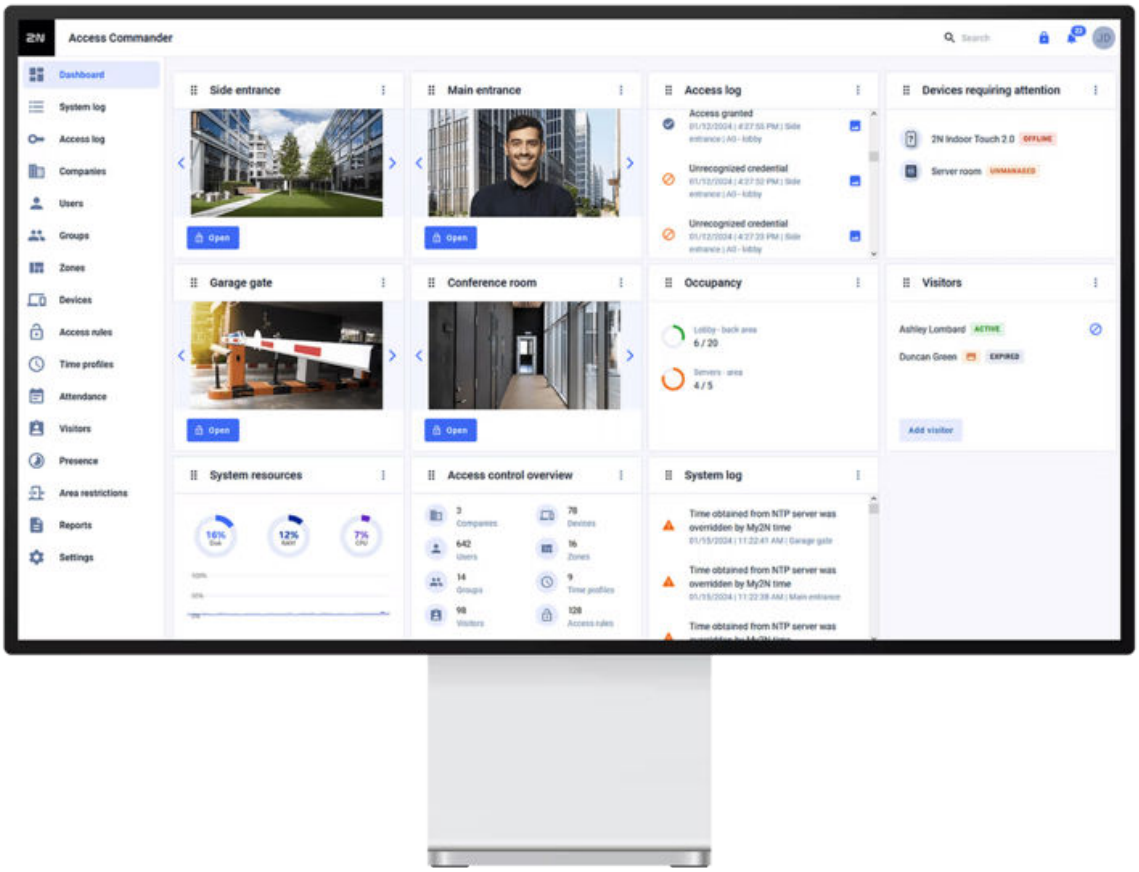
2N Access Commander

Installation Manual



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

2N.com

Table of Contents

Symbols and Terms Used

The following symbols and pictograms are used in the manual:

DANGER
Always abide by this information to prevent persons from injury.

WARNING
Always abide by this information to prevent damage to the device.

CAUTION
Important information for system functionality.

TIP
Useful information for quick and efficient functionality.

NOTE
Routines or advice for efficient use of the device.

General Information

2N Access Commander is a software tool for access system bulk management. The **Access Commander** interface is available via a web browser.

Within one installation, the **Access Commander** settings can be divided into **Companies** and managed separately. This enables you to distribute management among the administrators in the companies. Thus, the administrator from one company has no access to information from another company. The administrators from one company cannot see the users of another company.

Add **Device** to **Access Commander** for access control. The devices are physical units in a building that control entrances (2N intercoms, 2N access control units, 2N electronic locks) or enable communication (2N answering units). The devices are grouped into **Zones**. Each device can only be in one zone.

Zones or devices can be shared by all the companies, which helps manage the company access to common areas (entrances, restaurants, conference halls, etc.).

Users are individuals whose movement around the building is to be managed or who are to be called from the connected devices. Users are gathered in **Groups** for bulk management of their zone accesses. The user authenticates themselves on the device and the device then evaluates the user access for validity. Access validity obeys the **Access rules**. Selected users can also be entitled to manage **Access Commander** or parts thereof.

Time profiles set the times at which the device grants access or the users can be called.

The **Attendance module** monitors user attendance.

The **Presence module** monitors the current user presence in the zones.

Visitors are persons whose access rights are limited to a limited period of time.

User Rights

Multiple users can manage accesses in **Access Commander** depending on their assigned rights or privileges.

Accounts with extended rights are set through the role in the user settings. One user can be assigned multiple roles.

NOTE
User rights relate to the management within the user's company. The administrator has access to the complete management across the companies.

Administrator

- System and module settings according to the valid license.
- License Change.
- All rights of other roles related to all the companies.

Access Manager

- Creating and managing groups.
- Adding users to groups.
- Creating and managing visitors.
- Creating and managing time profiles.
- Setting access rules.

User Manager

- Creating and managing users.
- Creating and managing visitors.
- Adding users to groups.
- Viewing access and system logs.

Visitor Manager

- Creating and managing visitors.
- Managing visitor assignment to groups (not available in the simplified interface).
- Viewing visitor access log (not available in the simplified interface).

Door Manager

- Viewing camera transmissions from assigned devices.
- Remote opening of assigned devices.
- Emergency lockdown of assigned devices.
- Viewing access log of assigned devices.
- Monitoring states and security events in the system log.

Attendance Manager

- Monitoring and managing attendance of assigned groups.
- Viewing access log of users in assigned groups.

Company Administrator

- Setting the company's default language.
- System log monitoring (limited to the company events).
- Setting a widget for the system log and emergency lockout on the devices used by the company (including the devices shared with other companies).

Supported Devices and Applications

This subsection includes lists of supported devices, supported web browsers and compatible virtualization platforms via which **Access Commande**r can be installed.

Supported Devices

See below for a list of devices supported by the **Access Commander** access system. These devices can be managed in the system.

NOTE
The supported firmware versions for the devices are included in Subs. Firmware (p. 64).

2N Intercoms

- 2N IP Style – QR code reading support
- 2N IP Verso 2.0 – QR code reading support
- 2N IP Force 2.0 – QR code reading support
- 2N IP Verso
- 2N LTE Verso
- 2N IP One
- 2N IP Force
- 2N IP Safety
- 2N IP Vario
- 2N IP Base
- 2N IP Solo
- 2N IP Uni
- 2N IP Video Kit
- 2N IP Audio Kit
- 2N IP Audio Kit Lite

2N Access Units

- Access Unit QR – QR code reading support
- 2N Access Unit 2.0
- 2N Access Unit
- 2N Access Unit M

2N Electronic Locks

- 2N Fortis Handle
- 2N Fortis Cylinder

2N Answering Units

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

Web Browsers

Access Commander is configured via the web interface. The system has been optimized for the Google Chrome browser (version 90 and higher).

Other supported browsers:

- Mozilla Firefox (version 78 and higher)
- Microsoft Edge (version 91 and higher)
- Safari (version 14 and higher)

The other browsers have not been tested and thus their full functionality cannot be guaranteed.

Virtualization Platforms

- Virtual Box
- VMware Player (version 6.5 and higher)

- VMware vSphere (version 6.5 and higher)
- Hyper-V

Used Ports

List of Services and Necessary Ports

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

[a.] It is used both for client communication and intercom communication.

[b.] The user can choose another port for LDAP in the **Access Commander** settings.

License Overview

A Trial license is available after the first installation of **Access Commander**. The Trial license enables you to test all the management functions with 1 device and 5 users. One of the following four licenses has to be activated for a full management functionality: *Basic* (free), *Advanced*, *Pro* or *Unlimited*.

Licenses:	Trial	Basic	Advanced	Pro	Unlimited
2N Part No.	n/a	n/a	91379031	91379032	91379033
Axis Part No.	n/a	n/a	02309-001	02310-001	02311-001
Maximum User Count	5	50	300	1000	Unlimited[a.]
Maximum Device Count (both activated and deactivated)	1	5	30	100	Unlimited

Licenses:	Trial	Basic	Advanced	Pro	Unlimited
2N Part No.	n/a	n/a	91379031	91379032	91379033
Axis Part No.	n/a	n/a	02309-001	02310-001	02311-001
Maximum Administrator/Manager Count	5	1	5	1000	Unlimited
Access and System Logs	✓	✓	✓	✓	✓
Access Rules	✓	✓	✓	✓	✓
API Management	✓	✓	✓	✓	✓
Account Activation/Deactivation	✓	✓	✓	✓	✓
Failed Access Attempts Limit	✓	✓	✓	✓	✓
Silent Alarm	✓	✓	✓	✓	✓
Zone Code	✓	✓	✓	✓	✓
Device Monitoring	✓	✓	✓	✓	✓
Log Management	✓	✓	✓	✓	✓
Electronic Lock Management	✓	✓	✓	✓	✓
User Import from CSV or Device	✓	×	✓	✓	✓
Bulk Firmware Administration	✓	×	✓	✓	✓
Multi-Factor Authentication	✓	×	✓	✓	✓
User Rights	✓	×	✓	✓	✓

Licenses:	Trial	Basic	Advanced	Pro	Unlimited
2N Part No.	n/a	n/a	91379031	91379032	91379033
Axis Part No.	n/a	n/a	02309-001	02310-001	02311-001
Notification	✓	×	✓	✓	✓
Presence	✓	×	✓	✓	✓
API access keys	✓	×	✓	✓	✓
CAM Logs	✓	×	✓	✓	✓
Lift Control	✓	×	✓	✓	✓
Dashboard	✓	×	✓	✓	✓
Emergency Lockdown	✓	×	✓	✓	✓
Mobile Credential Support	✓	×	✓	✓	✓
Visitor Management	✓	×	✓	✓	✓
Automation	✓	×	✓	✓	✓
Occupancy Management	✓	×	×	✓	✓
Synchronization (LDAP & CSV)	✓	×	×	✓	✓
Anti-Passback	✓	×	×	✓	✓
Attendance	✓	Optional	Optional	Optional	Optional

[a.] Unlimited within the maximum capabilities of the software platform, refer to Recommended Virtual Machine Hardware (p. 20).

Installation

Access Commander can be distributed as:

- 2N Access Commander Box 2.0, a small desktop computer (Part No. 1120120xx, Axis Part No. 03129-00)
- Virtual machine

The Access Commander Box solution is limited to 2000 connected devices. The other software feature are identical for both the solutions.

Access Commander Box Distribution

Access Commander Box 2.0 (1120120xx, 03129-00) is a compact desktop minicomputer with pre-installed software. It is a plug & play solution, which requires only a power supply and an Ethernet cable connected to the computer. It is recommended that this computer is placed safely and kept running for a correct and full system functionality. Access Commander Box 2.0 serves as a server to collect data, events and logs from the entire access control system.

We recommend that 1500 users per group is not exceeded. If there are some restrictions in the area, such as Anti-passback or occupancy check due to a high user count, the application may slow down.

Login to Access Commander with Dynamic IP Address

1. Connect the Access Commander Box to the network using an Ethernet cable.
2. Use the 2N IP Network Scanner and Axis IP Utility to locate Access Commander Box on the network.
3. Go to the Access Commander Box IP address in the web browser and log in to **Access Commander**. The default password of the Admin user is 2n and after login change is required.

NOTE
With the Access Commander Box distribution, connect to the web interface from another LAN computer. The Access Commander Box operating system ensures the **Access Commander** operation and basic Linux settings, but does not allow the web browser to be started.

Static Address Setting on Access Commander Box by Direct PC Interconnection

1. Connect Access Commander Box directly to your computer using a network cable.
2. The link-local address will automatically be set in approximately **15 seconds**.
3. Open **accesscommander.local** in your browser.
   Alternatively, you can use the 2N IP Network Scannder or Axis IP Utility to locate the device even if it has not received an IP address via DHCP.
4. Set a static address as required in the web interface.

Access Commander Static Address Setting via Access Commander Box

1. Connect the Access Commander Box to the network using an Ethernet cable.
2. Connect a keypad and monitor to the Access Commander Box. A black screen appears.
3. Log in as “root” with the password “2n”. Once a blue screen is displayed, change the default password.
4. Select “Networking” in the Advanced Menu and then “Static IP”.
5. Set the static IP address, gateway and DNS.
6. Save the settings and click Log out to quit the console menu.

7. Connect to the set IP address via your web browser.

TIP
Direct interconnection with the computer and using the **accesscommander.local** address is the recommended and easiest way to set up a static address on Access Commander Box.

NOTE
The serial number displayed in the 2N Network Scanner or Axis IP Utility may differ from the serial number shown on the Access Commander Box label.

Fortis Commander

Fortis Commander is a standalone application that interconnects the **Fortis** electronic locks with the **Access Commander** system. The application sets the locks according to the project file created in **Access Commander**, which contains the lock configuration. The file is encrypted and can only be used for one specific installation.

Installation

Fortis Commander is designed to be installed on a Windows computer with Bluetooth Low Energy (BLE) support.

The app can be found at 2N Download Centre.

Installation Procedure

1. Download the installation package from the link provided.
2. Run the installer and complete the installation by following the on-screen instructions.

Project File

The project file is created in **Access Commander** and contains the complete project configuration. The file is encrypted and password protected.

Lock Settings in Access Commander

Before uploading keys to individual locks, you must pair **Access Commander** with **Fortis Commander**.

Master Encryption Key (MEK) Generation and Project Preparation

1. Log in to Access Commander.
2. Go to **Settings > Electronic locks**.
3. Click Generate Keys in **Initial Settings**.

4. Create the master encryption key.

CAUTION
The master encryption key cannot be **displayed or changed** later.

NOTE
According to the master encryption key (MEK), **2N Access Commander** generates a set of encryption keys. Thus, the key should be unique and sufficiently secure. As the key set is based on the master encryption key, projects with one and the same master encryption keys generate the same sets of keys. If a project is lost, you can create a new project with the same master encryption key and continue encryption.

5. Having generated the keys and set the password for the project file, you can download the **project file**, which represents an image of the electronic lock configuration in the **Access Commander** system.
6. On the **Fortis Commander** tab, click Download Application, to download the **Fortis Commander** electronic lock configuring application.

CAUTION
Project information is sensitive data. Protect it from abuse.

Propagation of Electronic Lock Configuration via Fortis Commander

1. Install and open the **Fortis Commander** application.
2. Click Open Project to open the downloaded project file in the File Explorer.
3. In the open dialog box, enter the project file password.
4. After opening the project file, select Connect to Device and tap the service card on the lock.
5. Click **Assign** to assign the lock to the project.
6. Disconnect the device and click **File > Close project**.
7. When the configuration is complete, open **Access Commander**. Go to the **Settings > Electronic Locks** and click the Fortis Commander button again. Upload the project file.

NOTE
When moving the lock between installations or when making a claim, you must perform **Factory Reset**. This operation resets the lock to factory settings and removes all previous configuration.

Configuration Update Instructions

1. Make changes in **Access Commander**.
2. Download a new project file.
3. Upload the file to **Fortis Commander** and make the required changes to the locks.
4. If you make other changes in **Access Commander**, always download a new project file.

CAUTION
Make sure to download a new project file for every configuration change in **Access Commander** – never use an older file already uploaded to **Fortis Commander**.

Permanent Locking/Unlocking

The app allows you to permanently lock and unlock the lock. The function is used for service interventions or emergency control without the use of a card.

Collection of events from electronic locks using RFID cards / chips

Event collection settings

1. Open **Settings > Electronic locks > Tab events**.
2. Select the event type:
   - **Collect access and system events** - All access and system events are recorded on the card/chip and written to the **System Log** and **Access Log**.
   - **Collect only system events** - only system events are logged, access events are not stored on cards.
   - **Do not collect events on** tabs - no events are written to the tab; they can only be accessed through **Fortis Commander**u.

TIP
Selecting the appropriate event set can reduce system load and storage utilization. However, detailed logging is important for diagnostics and safety audits.

Exporting events from a card

The card stores a maximum of **16 first events**. Events can be read in two ways:

- In **Access Commander**, click on the icon in the search box in the header and load the tab.
- Using a device with **2N OS**, events are read from the card and sent to **Access Commander**u.

Uploading events to the lock

1. Open **Settings > Electronic Locks > Fortis Commander** and click on Download File.
2. Open the file in **Fortis Commander**.
3. In the **Fortis Commander** app, connect to the electronic lock.
4. Upload the updated file back to **Access Commander**.
5. Once uploaded, the events are displayed in **Access Logs** and **System Logs**.

Service Operations

The following operations are available for **Fortis Cylinder**:

- **Disassembly** – disassembly of locks for service purposes.
- **Battery Replacement** – replacing the battery in the lock.

CAUTION
The service operations are not relevant for other types of locks.

NOTE
Press the Lock button for permanent locking to switch the lock from the service mode to the normal mode.

Virtual Machine Distribution

Access Commander can be distributed as a virtual machine. See below for installation procedures on the supported virtualization platforms.

Virtual Box

TIP
It is recommended to enable the VT-X virtualization technology in the BIOS.

1. Download the latest VirtualBox version from https://www.virtualbox.org/wiki/Downloads.
   Preferably including the VirtualBox Extension Pack.
2. Download the appropriate software from Support > Download Center > Software & Firmware at 2N.com.
   Unpack the downloaded file.
3. Open VirtualBox and select “File – Import appliance...”.
4. Edit the name.
5. Check the CPU setting (2 at least), RAM setting (2048 MB at least) and network card selection.
6. Confirm the license terms.
   After installation, the Linux configuration console opens for you to make basic system settings. Make the complete configuration via the web interface.

VMware Player

CAUTION
The supported VMWare version is 6.5 and higher.

1. Download the appropriate software from Support > Download Center > Software & Firmware at 2N.com.
   Unpack the downloaded file.
2. In WMware Player File – Open... select the path to the OVA file.
3. Rename it if necessary and click Import.
4. Check the CPU setting (2 at least), RAM setting (2048 MB at least) and network card selection.
   After installation, the Linux configuration console opens for you to make basic system settings. Make the complete configuration via the web interface.

VMware vSphere

CAUTION
The supported VMWare version is 6.5 and higher.

1. Download the appropriate software from Support > Download Center > Software & Firmware at 2N.com. Unpack the downloaded file.
2. In VMware vSphere select File – Deploy OVF Template... and follow the wizard instructions.
3. After import, check Edit Settings...
   Edit the name (on the Options card).
4. Check the CPU setting (2 at least), RAM setting (2048 MB at least) and network card selection.
   After installation, the Linux configuration console opens for you to make basic system settings. Make the complete configuration via the web interface.

Hyper-V

1. Download the appropriate software from Support > Download Center > Software & Firmware at 2N.com. Unpack the downloaded file.
2. Launch the Hyper-V Manager and select Import Virtual Machine for the required host.
3. Check the displayed information in the installation wizard and press Next to confirm reading.
4. Select the path to the folder from step 1.
5. Confirm the virtual machine selection.
6. Select the import type.
7. Select the virtual network card for the virtual machine.
8. Check the summary of the settings selected in the previous steps and press Finish for confirmation.
   After installation, the Linux configuration console opens for you to make basic system settings. Make the complete configuration via the web interface.

Recommended Virtual Machine Hardware

Access Commander is affected by the count of connected devices. Therefore, set the hardware size according to the real situation. The table below shows the recommended minimum CPU core counts and RAM sizes for different device and user counts managed by **Access Commander**.

CAUTION
It is recommended that you keep continuous connection between **Access Commander** and the devices. When disconnected, the devices save the event logs offline and, once reconnected, synchronize the log data with **Access Commander**. The application keeps running during synchronization, but the process may take a rather long time with a high number of devices.

Virtual Machine Hardware

Device count	User count	Minimum CPU core count	Minimum RAM size	Minimum HDD allocation
1 000	10 000	2	2 GB	120 GB
2 000	100 000	2	4 GB	120 GB
2 000	200 000	4	8 GB	120 GB
7 000	200 000	4	16 GB	120 GB

Technical Parameters

Access Commander Box 2.0 Options

Connected device count	User count	User count per group
7 000	200 000	1 500

Technical Parameters of Access Commander Box

1st generation Part. No. 91379030 Axis Part No. 01672-001	2nd generation Part. No. 1120120E, 1120120GB, 1120120US Axis Part No. 03129-00
• Dimensions: 56,1 x 107,6 x 114,4 mm (2,21" x 4,24" x 4,50") • Intel® Celeron® Processor J3160 (2M cache; up to 2.24 GHz) • 2.5” SSD SATA III hard disk (120 GB) • DDR3 SO-DIMM memory (4 GB) – 1.35 V, 1600 MHz • Supports dual displays via a VGA and HDMI port • Gigabit LAN port for Ethernet connection • VESA mounting bracket (75 × 75mm + 100 × 100mm) • System storage temperature: -20°C to +60°C • System environment operating temperature: 0°C to +35°C	• Dimensions: 127.5 x 132 x 57.6 mm (5.02 " x 5.20" x 2.27") • Intel® Processor N100, 6W TDP • SSD 980 NVMe M.2 – 250 GB • DDR4 SO-DIMM memory – 16 GB, 1,2 V, 3200 MHz • HDMI support 2.1, DisplayPort 1.4 a VGA • 2.5G RJ45 LAN port for Ethernet connection • System storage temperature: −40 °C to +85 °C • System environment operating temperature: 0°C to +50 °C

Recommended Virtual Machine Hardware

Access Commander is affected by the count of connected devices. Therefore, set the hardware size according to the real situation. The table below shows the recommended minimum CPU core counts and RAM sizes for different device and user counts managed by **Access Commander**.

CAUTION
It is recommended that you keep continuous connection between **Access Commander** and the devices. When disconnected, the devices save the event logs offline and, once reconnected, synchronize the log data with **Access Commander**. The application keeps running during synchronization, but the process may take a rather long time with a high number of devices.

Virtual Machine Hardware

Device count	User count	Minimum CPU core count	Minimum RAM size	Minimum HDD allocation
1 000	10 000	2	2 GB	120 GB
2 000	100 000	2	4 GB	120 GB
2 000	200 000	4	8 GB	120 GB
7 000	200 000	4	16 GB	120 GB

License Activation

Get the license file and upload it to **Access Commander**. You can activate Basic license directly in **Access Commander** in Settings > card License.

Getting License File

To get the license file, communicate the serial number of one of the 2N devices connected to **Access Commander** to the distributor. The License file is generated on the basis of the serial number of this license device. It must be the serial number of the intercom main unit, access unit or answering unit (**2N Indoor Touch** cannot be used).

The license device connection ensures the license validity. When the license device is disconnected, a protective period will start running and the license is suspended when the period expires.

Upload License

CAUTION

- Once switched off, the Trial license cannot be reactivated.
- The advanced settings that are not supported by the new license are not saved.

1. Go to **Settings > card License**.
2. Click Upload license and upload the license file from the storage in the open box.
3. Click Activate license after uploading.
4. Make sure that the license device for which the license has been generated is activated.

License Device	Selected 2N device connected to **Access Commander** to ensure the license validity. The license device is used as a hardware key for the license.
License File	License file used for license activation. The license file is generated by the distributor based on the license device serial number.

License Renewal

To restore a suspended license, connect and activate the licensed device or have a new license file generated and uploaded for another device. Once a new license is uploaded, first activate the license device for which the license has been generated. The other devices cannot be activated until this license device is activated.

A license is suspended whenever the license device keeps disconnected from **Access Commander** for a period longer than the protective period. The protective period lengths depend on how long the license device was connected to **Access Commander**. Refer to the table below for the protective period values. When a license is suspended, all the connected devices are automatically removed from the management and marked as unmanaged.

NOTE

Removal from management means that no changes can be made in the device configuration using **Access Commander**. Any changes made in **Access Commander** will not be transferred to the device. However, the device keeps working based on the configuration data sent in the last **Access Commander** transmission. This means that all the access and other settings remain the same as they were before the license was suspended.

You can change the configuration of an unmanaged device in the device web configuration interface only. Once the device is reconnected to the **Access Commander** management, synchronization will be made and all the changes made in the device web configuration interface will be overwritten by the **Access Commander** settings.

Period of time during which the license device was connected to Access Commander	Protective period during which Access Commander will keep running without the license device connected
less than 24 hours	1 day
1 day – 30 days	10 days
31 days – 180 days	1 month
over 180 days	3 months

Electronic Locks

The **Access Commander** system provides access control via the 2N Fortis electronic locks, which are unlocked by the MIFARE ® DESFire® RFID cards. Each electronic lock is assigned an encryption key during configuration. The lock keys are then stored on the RFID cards of the authorized users. If the keys match on the card and in the lock, the locking mechanism is unlocked.

One RFID access card can be used for access to up to 90 doors with the 2N Fortis locks, depending on the number of the time profiles applied. If the card memory capacity is exceeded, data writing to the card will fail. The write failure event is recorded in the system Access Log. If Lock Groups are used, more doors can be written to a single card than the case is with individual assignment.

Fortis Commander

Fortis Commander is a standalone application that interconnects the **Fortis** electronic locks with the **Access Commander** system. The application sets the locks according to the project file created in **Access Commander**, which contains the lock configuration. The file is encrypted and can only be used for one specific installation.

Installation

Fortis Commander is designed to be installed on a Windows computer with Bluetooth Low Energy (BLE) support.

The app can be found at 2N Download Centre.

Installation Procedure

1. Download the installation package from the link provided.
2. Run the installer and complete the installation by following the on-screen instructions.

Project File

The project file is created in **Access Commander** and contains the complete project configuration. The file is encrypted and password protected.

Lock Settings in Access Commander

Before uploading keys to individual locks, you must pair **Access Commander** with **Fortis Commander**.

Master Encryption Key (MEK) Generation and Project Preparation

1. Log in to Access Commander.

2. Go to **Settings > Electronic locks**.
3. Click Generate Keys in **Initial Settings**.
4. Create the master encryption key.

CAUTION
The master encryption key cannot be **displayed or changed** later.

NOTE
According to the master encryption key (MEK), **2N Access Commander** generates a set of encryption keys. Thus, the key should be unique and sufficiently secure. As the key set is based on the master encryption key, projects with one and the same master encryption keys generate the same sets of keys. If a project is lost, you can create a new project with the same master encryption key and continue encryption.

5. Having generated the keys and set the password for the project file, you can download the **project file**, which represents an image of the electronic lock configuration in the **Access Commander** system.
6. On the **Fortis Commander** tab, click Download Application, to download the **Fortis Commander** electronic lock configuring application.

CAUTION
Project information is sensitive data. Protect it from abuse.

Propagation of Electronic Lock Configuration via Fortis Commander

1. Install and open the **Fortis Commander** application.
2. Click Open Project to open the downloaded project file in the File Explorer.
3. In the open dialog box, enter the project file password.
4. After opening the project file, select Connect to Device and tap the service card on the lock.
5. Click **Assign** to assign the lock to the project.
6. Disconnect the device and click **File > Close project**.
7. When the configuration is complete, open **Access Commander**. Go to the **Settings > Electronic Locks** and click the Fortis Commander button again. Upload the project file.

NOTE
When moving the lock between installations or when making a claim, you must perform **Factory Reset**. This operation resets the lock to factory settings and removes all previous configuration.

Configuration Update Instructions

1. Make changes in **Access Commander**.
2. Download a new project file.
3. Upload the file to **Fortis Commander** and make the required changes to the locks.

4. If you make other changes in **Access Commander**, always download a new project file.

CAUTION
Make sure to download a new project file for every configuration change in **Access Commander** – never use an older file already uploaded to **Fortis Commander**.

Permanent Locking/Unlocking

The app allows you to permanently lock and unlock the lock. The function is used for service interventions or emergency control without the use of a card.

Collection of events from electronic locks using RFID cards / chips

Event collection settings

1. Open **Settings > Electronic locks > Tab events**.
2. Select the event type:
   - **Collect access and system events** - All access and system events are recorded on the card/chip and written to the **System Log** and **Access Log**.
   - **Collect only system events** - only system events are logged, access events are not stored on cards.
   - **Do not collect events on** tabs - no events are written to the tab; they can only be accessed through **Fortis Commander**u.

TIP
Selecting the appropriate event set can reduce system load and storage utilization. However, detailed logging is important for diagnostics and safety audits.

Exporting events from a card

The card stores a maximum of **16 first events**. Events can be read in two ways:

- In **Access Commander**, click on the icon in the search box in the header and load the tab.
- Using a device with **2N OS**, events are read from the card and sent to **Access Commander**u.

Uploading events to the lock

1. Open **Settings > Electronic Locks > Fortis Commander** and click on Download File.
2. Open the file in **Fortis Commander**.
3. In the **Fortis Commander** app, connect to the electronic lock.
4. Upload the updated file back to **Access Commander**.
5. Once uploaded, the events are displayed in **Access Logs** and **System Logs**.

Service Operations

The following operations are available for **Fortis Cylinder**:

- **Disassembly** – disassembly of locks for service purposes.
- **Battery Replacement** – replacing the battery in the lock.

CAUTION
The service operations are not relevant for other types of locks.

NOTE
Press the Lock button for permanent locking to switch the lock from the service mode to the normal mode.

Card Update

User access cards need to be updated on a regular basis. The user updates the card by tapping it on the 2N IP device to which the user has valid access rights. The card must be held against the reader until the door opening switch is activated. The door opening switch is not activated until the lock accesses have been updated.

You can change the default ten-day validity of the cards in **Settings > Electronic locks > Card parameters**.

CAUTION
If you change the lock access rights in **Access Commander**, the changes will not be reflected on the user access card until the card has been updated on a 2N device card reader! For security reasons, we recommend that a shorter validity period is set for the cards to ensure they are updated regularly.

The IP readers in the devices that allow for card updates and their settings are described in the Subs. IP Device Reader Settings (p. 29).

Compatible Cards

NOTE
For the purposes of this documentation, the term **card** refers to any compatible identifier using the MIFARE DESFire technology.

Cards with random ID cannot be used for opening the 2N Fortis electronic locks.

Cards with PICard technology cannot be used for opening the 2N Fortis electronic locks.

Time Profiles on Electronic Locks

Electronic locks support time profiles with the following limitations:

- Holidays do not apply.
- You can set up to 4 different time intervals per day.

- 4 daily interval schedules can be defined within one time profile.

TIP
This means that you can have different settings for Monday, Tuesday, Wednesday and Thursday, for example, but you must use one of the existing settings for Friday, Saturday, and Sunday.

CAUTION
If the time profile violates the specified restrictions, the access rule will be ignored and the user will not be granted access.

Fortis Commander

Fortis Commander is a standalone application that interconnects the **Fortis** electronic locks with the **Access Commander** system. The application sets the locks according to the project file created in **Access Commander**, which contains the lock configuration. The file is encrypted and can only be used for one specific installation.

Installation

Fortis Commander is designed to be installed on a Windows computer with Bluetooth Low Energy (BLE) support.

The app can be found at 2N Download Centre.

Installation Procedure

1. Download the installation package from the link provided.
2. Run the installer and complete the installation by following the on-screen instructions.

Project File

The project file is created in **Access Commander** and contains the complete project configuration. The file is encrypted and password protected.

Lock Settings in Access Commander

Before uploading keys to individual locks, you must pair **Access Commander** with **Fortis Commander**.

Master Encryption Key (MEK) Generation and Project Preparation

1. Log in to Access Commander.
2. Go to **Settings > Electronic locks**.
3. Click Generate Keys in **Initial Settings**.

4. Create the master encryption key.

CAUTION
The master encryption key cannot be **displayed or changed** later.

NOTE
According to the master encryption key (MEK), **2N Access Commander** generates a set of encryption keys. Thus, the key should be unique and sufficiently secure. As the key set is based on the master encryption key, projects with one and the same master encryption keys generate the same sets of keys. If a project is lost, you can create a new project with the same master encryption key and continue encryption.

5. Having generated the keys and set the password for the project file, you can download the **project file**, which represents an image of the electronic lock configuration in the **Access Commander** system.
6. On the **Fortis Commander** tab, click Download Application, to download the **Fortis Commander** electronic lock configuring application.

CAUTION
Project information is sensitive data. Protect it from abuse.

Propagation of Electronic Lock Configuration via Fortis Commander

1. Install and open the **Fortis Commander** application.
2. Click Open Project to open the downloaded project file in the File Explorer.
3. In the open dialog box, enter the project file password.
4. After opening the project file, select Connect to Device and tap the service card on the lock.
5. Click **Assign** to assign the lock to the project.
6. Disconnect the device and click **File > Close project**.
7. When the configuration is complete, open **Access Commander**. Go to the **Settings > Electronic Locks** and click the Fortis Commander button again. Upload the project file.

NOTE
When moving the lock between installations or when making a claim, you must perform **Factory Reset**. This operation resets the lock to factory settings and removes all previous configuration.

Configuration Update Instructions

1. Make changes in **Access Commander**.
2. Download a new project file.
3. Upload the file to **Fortis Commander** and make the required changes to the locks.
4. If you make other changes in **Access Commander**, always download a new project file.

CAUTION
Make sure to download a new project file for every configuration change in **Access Commander** – never use an older file already uploaded to **Fortis Commander**.

Permanent Locking/Unlocking

The app allows you to permanently lock and unlock the lock. The function is used for service interventions or emergency control without the use of a card.

Collection of events from electronic locks using RFID cards / chips

Event collection settings

1. Open **Settings > Electronic locks > Tab events**.
2. Select the event type:
   - **Collect access and system events** - All access and system events are recorded on the card/chip and written to the **System Log** and **Access Log**.
   - **Collect only system events** - only system events are logged, access events are not stored on cards.
   - **Do not collect events on** tabs - no events are written to the tab; they can only be accessed through **Fortis Commander**u.

TIP
Selecting the appropriate event set can reduce system load and storage utilization. However, detailed logging is important for diagnostics and safety audits.

Exporting events from a card

The card stores a maximum of **16 first events**. Events can be read in two ways:

- In **Access Commander**, click on the icon in the search box in the header and load the tab.
- Using a device with **2N OS**, events are read from the card and sent to **Access Commander**u.

Uploading events to the lock

1. Open **Settings > Electronic Locks > Fortis Commander** and click on Download File.
2. Open the file in **Fortis Commander**.
3. In the **Fortis Commander** app, connect to the electronic lock.
4. Upload the updated file back to **Access Commander**.
5. Once uploaded, the events are displayed in **Access Logs** and **System Logs**.

Service Operations

The following operations are available for **Fortis Cylinder**:

- **Disassembly** – disassembly of locks for service purposes.
- **Battery Replacement** – replacing the battery in the lock.

CAUTION
The service operations are not relevant for other types of locks.

NOTE
Press the Lock button for permanent locking to switch the lock from the service mode to the normal mode.

IP Device Reader Settings

IP Device Web Interface Settings

CAUTION
If you connect a new RFID card reader extending module to a 2N device via a VBUS cable, you need to pair this module with the device. Pair the card reader via the device web interface in the **Access > Modules**.

1. Enter the web configuration of the selected device.

   TIP
   Click in the list on the Devices page to enter the web configuration interface.
2. Go to Hardware > Extending modules.
3. Go to the RFID card reader module settings on the page.
4. Click Pair module.
5. Select “2N electronic locks” in the **Allowed card types** menu.

   CAUTION
   Enable only the card types you actually use for optimal functionality.
6. Save the changes.

Compatible Modules

Synchronization of the keys to the 2N Fortis electronic locks can be performed on all of the 2N RFID readers released on the market in February 2023 or later. Most readers manufactured after this date are also compatible, with the exception of the models listed below.

The following models **are not compatible**:

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

For the following modules, compatibility is only guaranteed for the units manufactured in autumn 2023 or later:

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

Lock Settings in Access Commander

Before uploading keys to individual locks, you must pair **Access Commander** with **Fortis Commander**.

Master Encryption Key (MEK) Generation and Project Preparation

1. Log in to Access Commander.
2. Go to **Settings > Electronic locks**.
3. Click Generate Keys in **Initial Settings**.
4. Create the master encryption key.

> **CAUTION**
> The master encryption key cannot be **displayed or changed** later.

> **NOTE**
> According to the master encryption key (MEK), **2N Access Commander** generates a set of encryption keys. Thus, the key should be unique and sufficiently secure. As the key set is based on the master encryption key, projects with one and the same master encryption keys generate the same sets of keys. If a project is lost, you can create a new project with the same master encryption key and continue encryption.

5. Having generated the keys and set the password for the project file, you can download the **project file**, which represents an image of the electronic lock configuration in the **Access Commander** system.
6. On the **Fortis Commander** tab, click Download Application, to download the **Fortis Commander** electronic lock configuring application.

> **CAUTION**
> Project information is sensitive data. Protect it from abuse.

Propagation of Electronic Lock Configuration via Fortis Commander

1. Install and open the **Fortis Commander** application.
2. Click Open Project to open the downloaded project file in the File Explorer.
3. In the open dialog box, enter the project file password.
4. After opening the project file, select Connect to Device and tap the service card on the lock.
5. Click **Assign** to assign the lock to the project.
6. Disconnect the device and click **File > Close project**.
7. When the configuration is complete, open **Access Commander**. Go to the **Settings > Electronic Locks** and click the Fortis Commander button again. Upload the project file.

> **NOTE**
> When moving the lock between installations or when making a claim, you must perform **Factory Reset**. This operation resets the lock to factory settings and removes all previous configuration.

Configuration Update Instructions

1. Make changes in **Access Commander**.
2. Download a new project file.
3. Upload the file to **Fortis Commander** and make the required changes to the locks.
4. If you make other changes in **Access Commander**, always download a new project file.

CAUTION
Make sure to download a new project file for every configuration change in **Access Commander** – never use an older file already uploaded to **Fortis Commander**.

Permanent Locking/Unlocking

The app allows you to permanently lock and unlock the lock. The function is used for service interventions or emergency control without the use of a card.

Maintenance Cards

Maintenance cards provide authorized access to the lock. They allow for putting the lock in service, battery replacement, lock disassembly.

CAUTION
The maintenance card cannot be used as a user access card at the same time.

Maintenance Card Settings

1. In **Access Commander** go to **Settings > Electronic locks**.
2. Click Create in **Maintenance cards**.
3. Select the card type to be created in the open dialog box.
   - New locks setup – activate the previously configured new locks in factory settings into the service mode.
   - Service – activate the service mode for the already set lock.
   - Disassembly – release the already set 2N Fortis Cylinder lock for disassembly, see the 2N Fortis Installation Manual.
   - Battery Replacement – release the already set 2N Fortis Cylinder lock for battery replacement, see the 2N Fortis Installation Manual.

   TIP
   New locks setup and any other service card can be uploaded on one physical card simultaneously. We recommend a combination of **New locks setup** and **Service**.
4. Click Continue.
5. Tap the card on the connected USB RFID reader. Wait until the data has been loaded on the card.

The validity of the maintenance card data is one year. After this time, the data must be deleted and the card set up again.

Support for Third-Party DESFire Cards (Anonymous App Creation)

Access Commander allows you to work with the MIFARE DESFire cards. It supports the cards that are already in use in other access control systems and allows for their reuse without the need to know their master key (PICC Master Key).

This is a special mode in which the card enables the creation of a new independent application without the need to know its master key (PICC Master Key).

With this functionality, administrators can:

- Reuse the existing physical cards.
- Write the OSO application for **Access Commander** to them.
- Avoid the necessity to know or manage the PICC Master Key of the original systems.

Creating OSO Application on Tab

1. Attach the user's existing DESfire card to a reader connected to **Access Commander**.
2. Create user credentials.
3. Access Commander automatically detects whether the card supports anonymous application creation.
4. If the mode is supported, **Access Commander** writes a new anonymous application to the card without affecting the existing data or third-party applications.

CAUTION
If the mode is supported, Access Commander writes a new anonymous application without the option of formatting the card later using a feature in the Settings section. Only the contents of the application can be deleted, not the previously occupied space on the card.

Basic Access to Interface

*This subsection describes putting in operation and basic operation of **Access Commander**. The installation is described in Subs.* *Installation (p. 13)**.*

The **Access Commander** interface is accessible through a web browser. The IP address of the web interface can be looked up using 2N Network Scanner or Axis IP Utility. The web interface can also be accessed directly at **accesscommander.local**. This functionality is enabled by default.

NOTE

- If multiple Access Commander instances are running in the network, the system automatically assigns unique names: **accesscommander.local**, **accesscommander-2.local**, **accesscommander-3.local** and other instances according to the count of servers in the network.
- With the Access Commander Box distribution, connect to the web interface from another LAN computer. The Access Commander Box operating system ensures the **Access Commander** operation and basic Linux settings, but does not allow the web browser to be started.

NOTE
With the Access Commander Box distribution, connect to the web interface from another LAN computer. The Access Commander Box operating system ensures the **Access Commander** operation and basic Linux settings, but does not allow the web browser to be started.

The default login data are:

Username: **Admin**

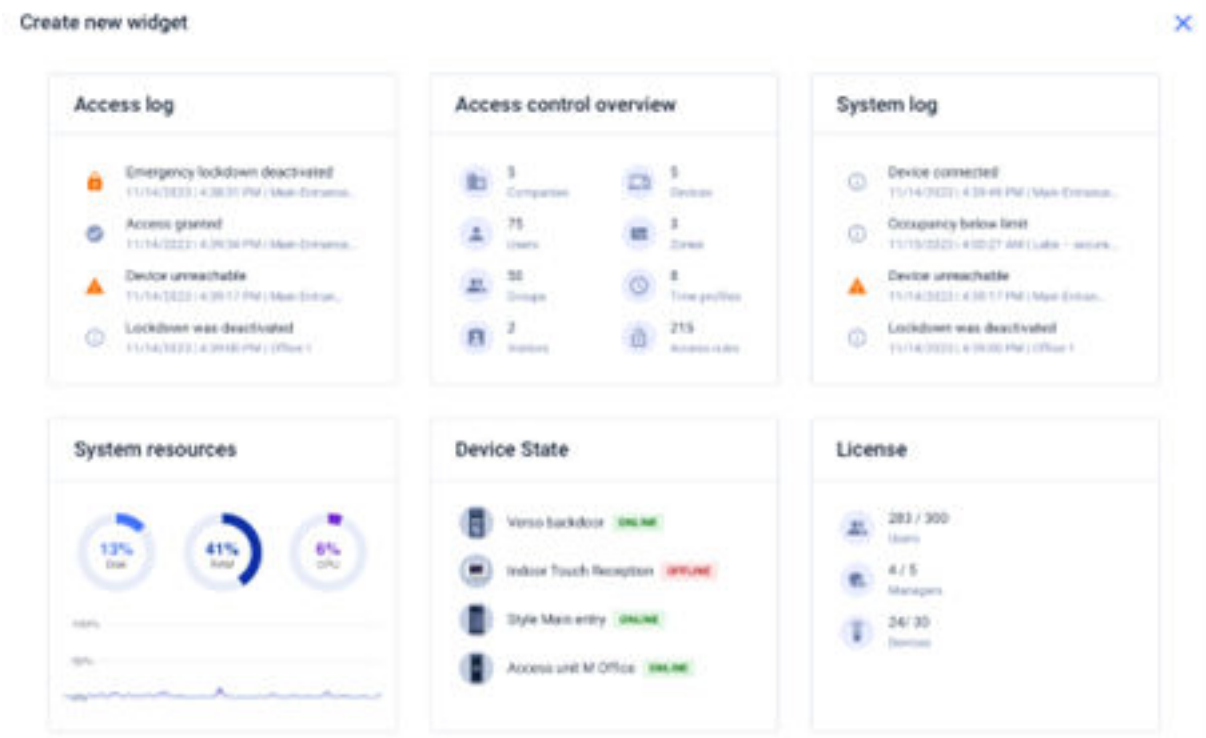
Password: **2n**

It is necessary to change the password immediately upon the first login.

NOTE
Select **Do Not Log Out** if you want to avoid login data re-entering during the next login. The login is valid for up to 7 days, after which you have to log in again.

Two-Factor Authentication (p. 98) may be required for login.

Dashboard



Dashboard is the basic display of the **Access Commander** web interface. It is a configurable notice board showing real time data. **Access Commander** offers several Widgets that are added to the Dashboard using the + button. The Dashboard Widgets can be moved, renamed or set basically. The Widgets are managed and deleted in the ⋮ extended menu in the header of each Widget.

Every user with an account on **Access Commander** can set a Dashboard of their own. The Widget availability is limited depending on the user role and available license.

Change Language

Upon the first login, **Access Commander** is displayed in the language set for the logged-in user's company. Every user can change the language. For the next logins, the interface will be available in the newly set language.

1. Click the user image in the right-hand upper corner to open the user menu.
2. Select Change language
3. Select the required language and press Change language to confirm the selection.

Account Password Change

1. Click the user image in the right-hand upper corner to open the user menu.
2. Select View profile.
3. Click ✎ at the Password parameter.
4. Confirm the current password and enter a new one.

> **NOTE**
> If the 'admin' account password is the same as the system root user password (for login to the Linux setting console), the root account password will automatically change once the 'admin' account password is changed.

Profile Image Change

1. Click the user image in the right-hand upper corner to open the user menu.
2. Select View profile.
3. Click the image in the user detail header.
4. Set photo in the open dialog box.
   The image resolution will be adjusted to 432 x 432 px automatically.

Logs

Here is what you can find in this subsection:

System log

NOTE

- Those logs are displayed that the user may observe based on their user rights.
- Data is written in English into the logs.

The System Logs page shows a list of events and notifications that have been generated.

The system log list provides the following data on each event and notification:

- severity (info, warning, error).
- time of the event.
- category to which the action falls (Device state, Import, User synchronization, System, User actions, Area limits).
- entity concerned (device, user, zone, visitor...).
- brief description of the event.
- Author.

Click the row to open detailed information on the selected record.

Filter the list items using above the list. Or, click in each column header to open an extended menu and set filters for each column. The extended column menu also enables you to move, pin to the first/last position or hide the columns.

The Importance and Time columns cannot be hidden.

Log Export

Press Export above the list to download the list in a CSV file. The time is GMT+0 in the CSV file exported.

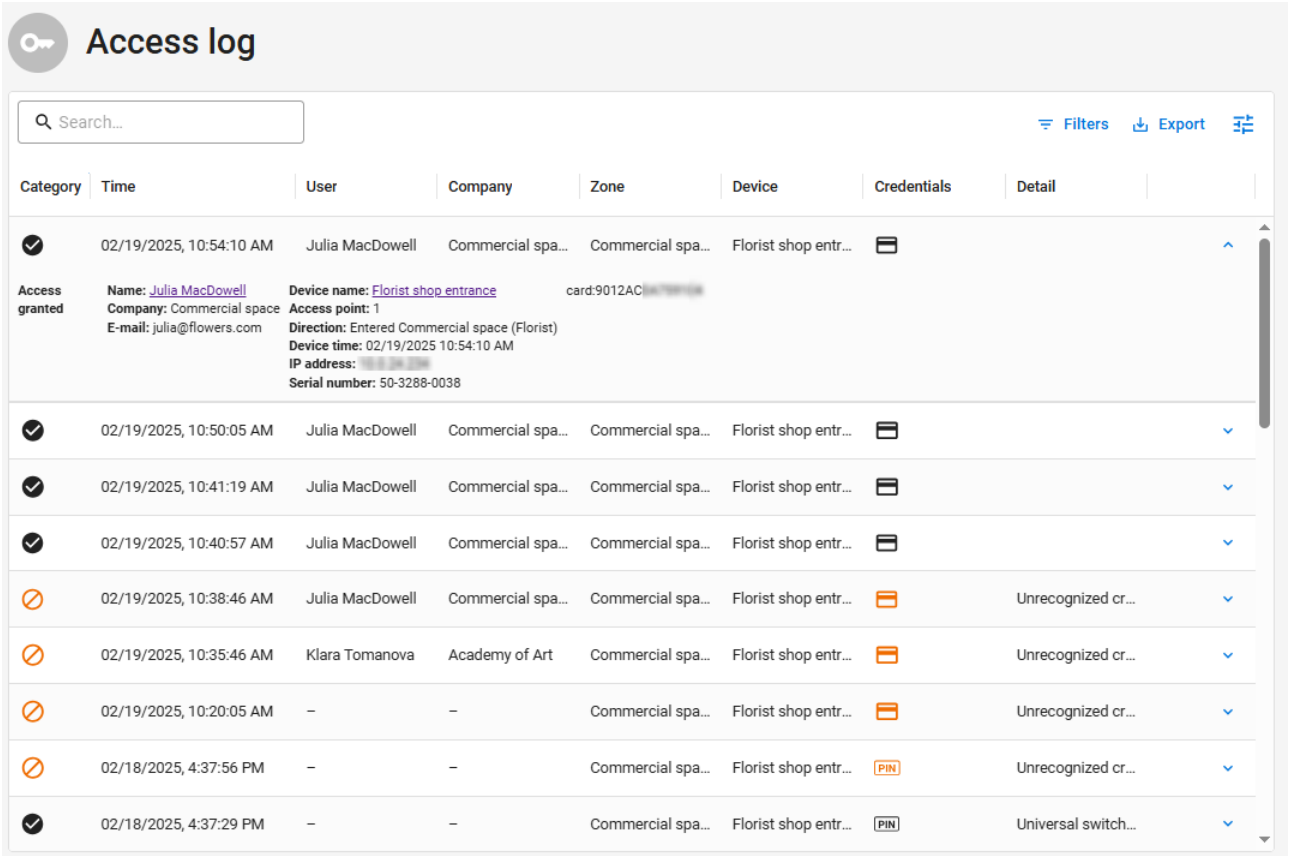
Log Lifetime

Auto-deletion will be triggered the moment the disk space usage reaches 80%. Follow the disk capacity on the Settings page. Logs of the first type in the sequence are deleted first, the other logs are deleted one by one until the disk space usage drops to 75 % or until only the logs with the unfinished maximum lifetime for the given log type remain stored.

Set the storage period for the given log type in **Settings > Log retention card**. The camera log retention time may not be longer than the system and access log retention time.

TIP
In case you use 70 % of the disk capacity continually, we recommend that the maximum log storage period is shortened.

Access log



NOTE

- Those logs are displayed that the user may observe based on their user rights.
- Data is written in English into the logs.

The Access Logs page shows records on successful/unsuccessful authentication attempts and emergency lockdown records.

The Access log list includes:

- **Category**
  - Access enabled
  - Access denied
  - Public Access
  - Locking – device lockdown
- **Time** of the event
- **User** who executed the action
- Given user's **company**
- **Zone** where the action happened
- **Device** on which the action happened
- **Authentication** used for the attempt (PIN, QR code, etc.)

Click the row to open detailed information on the selected record.

Filter the list items using above the list. Or, click in each column header to open an extended menu and set filters for each column. The extended column menu also enables you to move, pin to the first/last position or hide the columns.

Log Export

Press Export above the list to download the list in a CSV file. The time is GMT+0 in the CSV file exported.

Log Lifetime

Auto-deletion will be triggered the moment the disk space usage reaches 80%. Follow the disk capacity on the Settings page. Logs of the first type in the sequence are deleted first, the other logs are deleted one by one until the disk space usage drops to 75 % or until only the logs with the unfinished maximum lifetime for the given log type remain stored.

Set the storage period for the given log type in **Settings > Log retention card**. The camera log retention time may not be longer than the system and access log retention time.

TIP
In case you use 70 % of the disk capacity continually, we recommend that the maximum log storage period is shortened.

Call Log

The Call Log page records all call activity from the intercoms and other SIP devices connected (answering units or lift communicators, e.g.).

NOTE
The call log is available to the Admin user only.

The call log list includes the following for each event:

- Call type
- Time when the call was made
- Whether the door is unlocked
- Device type
- Counterparty
- Call duration
- Reason for call termination

Click the row to open detailed information on the selected record.

Filter the list items using above the list. Or, click in each column header to open an extended menu and set filters for each column. The extended column menu also enables you to move, pin to the first/last position or hide the columns.

Log Export

Press Export above the list to download the list in a CSV file. The time is GMT+0 in the CSV file exported.

Log Lifetime

Set the storage period for the given log type in *Settings* > *Log Retention*.

TIP
In case you use 70 % of the disk capacity continually, we recommend that the maximum log storage period is shortened.

CAUTION
It is recommended that the latest firmware version is used on the devices to make all the Call Log functionalities work properly. Some information and columns may not be available or may not display correctly on devices with earlier firmware versions.

- **Call duration:** Call duration is not supported in earlier firmware versions. This information is available in firmware version 2.49 and higher.
- **Counterparty identification:** Firmware version 2.50 and higher is required to identify the counterparty from the device directory correctly. Searching the device directory may not behave correctly in earlier versions.

Notifications

The Notifications module helps you monitor selected system events and features, which are to be reported by **Access Commander** by e-mail or notification in the upper bar next to the user menu.

The notification list is also displayed in **System logs > Notifications**.

Press Export above the list to download the list in a CSV file. The time is GMT+0 in the CSV file exported.

Notification Type Setting

1. Go to **Settings > Notifications**.
2. Click the adding button in the right-hand upper corner of the page.
3. Enter the new notification type name.
   After creation, the notification detail will be displayed for you to choose the devices whose notifications are to be monitored, add the user to be sent notifications to and select the way of notification delivery.

Notification Settings

Set the notification type in the detail of the selected notification type. Click the selected notification in the **Settings > Notifications** to open the notification type detail.

Delivery Methods

Set the notification delivery method and the list of e-mail notification recipients on the card.

In **Access Commander**, notifications appear under the icon in the upper bar next to the user menu or in **System log > Notifications**.

Notification e-mails can be sent to the users listed in **Access Commander** as well as recipients outside the system. The users can be selected from a list. E-mail addresses of other recipients have to be added manually.

NOTE
Make sure that SMTP is set correctly to make e-mail notifications work properly, refer to E-Mail (SMTP) Enable and Setting (p. 97).

Monitored Devices

The given notification type can be generated both for all the devices and selected devices. If Monitoring of all devices is enabled, the event can happen on any device and a notification is generated. If Monitoring of all devices is disabled, a notification is generated only if the event happens on a selected device. Select the device in a menu opened using .

Log Lifetime

Auto-deletion will be triggered the moment the disk space usage reaches 80%. Follow the disk capacity on the Settings page. Logs of the first type in the sequence are deleted first, the other logs are deleted one by one until the disk space usage drops to 75 % or until only the logs with the unfinished maximum lifetime for the given log type remain stored.

Set the storage period for the given log type in **Settings > Log retention card**. The camera log retention time may not be longer than the system and access log retention time.

TIP
In case you use 70 % of the disk capacity continually, we recommend that the maximum log storage period is shortened.

Companies

Within one installation, the **Access Commander** settings can be divided into **Companies** and managed separately. This enables you to distribute management among the administrators in the companies. Thus, the administrator from one company has no access to information from another company. The administrators from one company cannot see the users of another company.

Zones or devices can be shared by all the companies, which helps manage the company access to common areas (entrances, restaurants, conference halls, etc.).

Company Creation

1. Go to the **Companies** page.
2. Click the company adding button in the right-hand upper corner.
3. Complete the company name.
4. Click Create to create a company.
   The new company appears on the list. Set the company in the company detail. Add users to the company in the user settings.

Company Settings

View and edit the company information in the company detail. Click the selected company list item on the Companies page to open the company detail.

There is a Lock button in the company detail header, which activates Emergency Lockdown (p. 61) for all the devices in the zones of this company.

The company detail is divided into the Overview, E-Mails and User Synchronization cards.

Company Language

Select the language on the General card for the **Access Commander** interface to communicate with the users of the given company. The users can change the interface language any time later. The company language selection also affects the templates of the e-mails to be sent to the users. The e-mail texts can be changed in the E-mail folder.

Zones

Assigning zones to a company means to define a set of facilities that may be accessed by the company users (e.g. the common space and 4th floor zones, which include the reception entrance door and all the 4th floor entrances). A zone can be assigned to multiple companies and one company can be assigned more zones.

My2N app

In Company, you can also set the pairing parameters for the My2N app, which allows for Bluetooth authentication. Set both the devices that can be used for pairing and the validity of the mobile access necessary for pairing. The mobile accesss itself is generated in the user settings.

Visitors

Here set the groups to which the visitor administrator can assign new visitors. One of the groups can be determined as default. A new visitor will automatically be assigned to the default group unless defined otherwise.

CAUTION
Without a correctly set default group, it is not possible to provide access to visitors in the simplified user interface.

It is possible to select the authentication methods that can be assigned to the visit. Authentication method is then assigned to a visit by the visit manager.

Refer to Visitors (p. 77) for more details.

Working Time

Working time and Holidays are used for calculating the monthly user working time in the Attendance module. You can select the days in a week that will be calculated as working days. Click a day to select it. Green days identify the days that are considered working days.

Working hours modification defines the time of one day shift.

Holidays

Set the holidays to define which days are not included in the monthly working time calculation. The hours worked on holidays are counted as hours worked on weekends – the worked time is filed beyond the common working hours.

The extended menu ⋮ helps you copy holidays from another company. Holidays are copied including their dates and names. Copying can be used repeatedly, but if the holiday to be copied already exists in the company, it will be renamed.

E-Mails Sent to Company Users

Find the e-mail settings in a dedicated folder in the company detail. **Access Commander** allows for sending automatic e-mails informing of the authentication method assignment to the company users (including visitors). The e-mail is sent to the user's or visitor's e-mail address.

Access Commander allows for sending e-mails with the following information:

- PIN code for visitor
- QR code for visitor
- PIN code for user
- QR code for user
- My2N app for Bluetooth user authentication settings

Set the appearance and edit the text for these e-mails in the **Company detail > E-mails > E-mail templates**. Click the selected e-mail type to open a dialog box to edit the e-mail text. You can edit the following in the dialog box:

- Subject – e-mail subject
- Header – in the e-mail body color field
- Introduction – text preceding the automatically generated data from **Access Commander**
- Additional message – text following the data generated from **Access Commander**
- Signature – signature at the e-mail end

Company Synchronization (LDAP)

LDAP synchronization is used for downloading users and user changes from an external LDAP system. The user data include user name, user ID, card identifiers, PIN/QR code, photo, e-mail address, phone number, password and login, vehicle license plates.

NOTE
Refer to www.ldap.com for more LDAP details.

1. Go to **Companies > Company detail > User synchronization**.
2. If no connection is set, create one.
   Complete:

   - **Server name** – if DNS is set correctly, just enter the server name (“WIN-9ABEB4AUOHD”). If DNS is not set, enter the IP address of the server on which LDAP is running.
   - **Port** – the default LDAP port is 389 (w/o SSL). If you want to use encrypted connection in your company, enter port number 636. Make sure that the SSL support is enabled on the LDAP server side too. If the administrator sets another port number, make sure it is changed in **Access Commander** too.
   - **Login name** – login name for the user with the root/tree rights. Enter the login name as “administrator@domain.com”.
   - **Password** – LDAP server user password.
   - **Communication Security (SSL)** – it is unnecessary to rewrite the port number if SSL is disabled. It is necessary to change the port to 636 if SSL is enabled.
   - **Base DN** – the root point from which the directory search starts. It can be an extension or a directory root, for example: CN=administrator, CN=users, DC=domain, DC=com.

   By enabling TLS you activate Transport Layer Security (TLS) for your FTP connection. TLS will encrypt the data transferred between **Access Commander** and the server.
   By enabling TLS Certificate Authentication you activate authentication of the TLS certificates provided by the server. When this option is enabled, **Access Commander** verifies that it is communicating with a trusted server, thus increasing the connection security.
3. The set LDAP connection detail opens up. Now you can test the connection settings. Press Synchronize Now to start one-time synchronization.
4. The **Options** tab helps you manage how data is synchronized.

   You can delete the set connection in the extended menu ⋮ on the **Import** card. Set more synchronization parameters on the **Options** card.

TIP
Set Automatic synchronization on the **Import** card. Enabling Automatic synchronization, complete the synchronization intervals. Select the minute/time for the data to be synchronized according to the required frequency.

LDAP Data Synchronization Settings

Imported Attributes – modify the scheme to set the assignment of attributes from the LDAP server to the **Access Commander** parameters.

NOTE
The phone number attributes are extended with a filter that converts the numbers into the desired format compatible with the company's user list in **Access Commander**. Two filters are available:

- `toPhoneNumber` – remove unnecessary characters (spaces, hyphens, etc.) from the phone numbers.
- `skipExtension` – remove the extension from the phone numbers.

Example of use: If you enter the attribute `{telephoneNumber|toPhoneNumber|skipExtension}`, the original value of the phone number in Active Directory “+420 123 456 789 x2222” is converted into “+420123456789”.

Users Removed from LDAP – define what to do with the users deleted from LDAP. You can keep or delete the users deleted from LDAP in **Access Commander**. Should the users removed from LDAP be deactivated, their data will remain in **Access Commander** but will not be synchronized with the devices. Deactivated users do not have access rights, cannot be reached, etc.

Active Directory Banned Users – set what happens to the users who have been banned from Active Directory. **Access Commander** can ignore this Active Directory change or disable the user. Deactivated users do not have access rights, cannot be reached, etc. Having been reactivated in Active Directory, the disabled users will also be reactivated in **Access Commander**.

Group Synchronization – upload group assignments from LDAP to **Access Commander**. By setting a synchronization scheme you can set a Base DN and filter of your own to be used for group synchronization. In the scheme settings, you can enable synchronization of users from nested groups.

Avatar Synchronization – set user photo uploading from the LDAP system.

Reference Monitoring – set whether or not data from the LDAP references should be synchronized.

Nested Search – enable user synchronization from the entire tree. When disabled, only data from the root is searched and synchronized.

Paging Enable – LDAP uses paging for extending the Simple Paged Results Control. This allows the results to be split into multiple pages, which is necessary for extensive directory services. The **Page Size** parameter defines the count of records per page.

User Import to Company

The extended menu ⋮ in the company detail header allows new users to be imported into the company on a one-time basis, either from a CSV file or from another 2N device.

User Import from CSV File

TIP
You can download a CSV template for importing users using this link.

Access Commander allows users to be uploaded to the company in bulk. Therefore, it is possible to pre-prepare basic user information simply in an external file and then simply import the user. Users in one file can only be uploaded to one specific company at a time.

This feature does not allow the users to be deleted.

NOTE
Users with the Administrator role can perform complex, repeatable user list synchronization across companies, see User Synchronization (p. 89).

Import from 2N Device

You can transfer the user list from a 2N device to **Access Commander**. Import can only be done from a device that has not yet been added to **Access Commander**. The device cannot contain the users who are already in **Access Commander** (i.e. have the same UUID). It is possible to import all users in bulk to one specific company only.

1. It is advisable to back up the configuration before import. The **Access Commander** system is backed up in **Settings > System Backup**. The device configuration backup is made in the device web configuration interface, in **System > Maintenance**.
2. Add the device from which you want to import the user list to the list of **Access Commander** devices.

   CAUTION
   Do not add devices to zones just yet! The device would override the access rules and the list of users would be rewritten on the device.

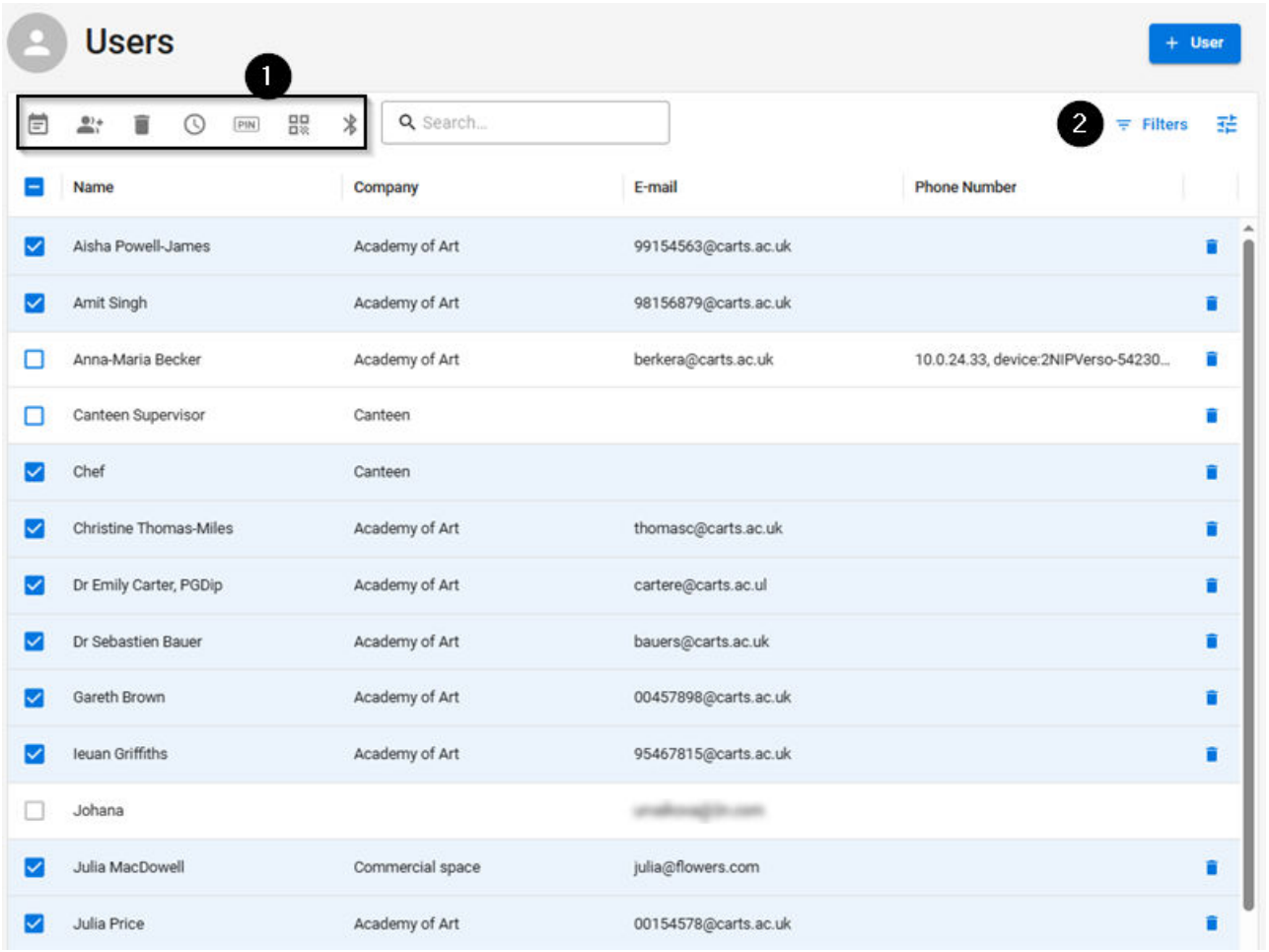
3. Go to the detail of the company to which you want to import the user. Select Import from Device from the ⋮ advanced menu.
4. A dialog box opens. Select the device from which you want to import the user list from the drop-down list of available devices.
5. Click Import to start importing on the background. The termination of the process is written in the System Log.
6. After successful import, it is possible to add the device to the zones and include it in the access rules.

CAUTION
The import procedure only works for specific device users (UUIDs) and imports all the users from the device into one company at once.

Users

Access Commander helps you manage **Users**, modify their accesses, administer their contact data, etc.

The user list shows all the users that have been created. Above the list, you can filter the users (number 2 in the figure) or search for a specific user by name, email or phone number.



Bulk Actions

Select multiple users to be applied the following bulk actions to (number 1 in the figure):

- Enable user attendance monitoring
- Add user to group
- Remove user
- Set access validity time interval
- Assign access PIN code to those users who have not been assigned PIN/QR code
- Assign access QR code to those users who have not been assigned PIN/QR code
- Assign mobile key to those selected users who have not been assigned any mobile key

NOTE
Make sure that a valid e-mail address has been completed for the user to be assigned the PIN/QR code or mobile key.

User Creation

1. Go to the **Users** page.
2. Click the user adding button in the right-hand upper corner.
3. Complete the mandatory data: user name and the company to which the user is assigned to.
   The newly created user appears on the list and the user detail opens up. You can set such other user parameters in the detail as user phone number assignment, authentication method selection, group assignment, etc.

NOTE
Access Commander allows users to be uploaded to the company in bulk. Therefore, it is possible to pre-prepare basic user information simply in an external file and then simply import the user. Users in one file can only be uploaded to one specific company at a time.

Bulk import is carried out in the company detail; see User Import to Company (p. 44).

User Settings

You can view and administer user information in the user detail. Click the selected user list item on the Users page to open ther user detail.

The user detail is split into the Overview, Attendance and Change log tabs. Attendance is only displayed to the users whose attendance monitoring has been enabled, refer to Attendance (p. 53). The Attendance module is available depending on the license.

User Name and Photo Change

Find the user renaming and photo setting options in an advanced menu ⋮ in the user detail header.

The image resolution will be adjusted to 432 x 432 px automatically.

Credentials

This card helps you set the user authentication methods on devices. The user has to authenticate themselves on a device and, if granted access, will be allowed to access the device.

RFID Card – add an existing RFID card to the user. A dialog box opens for you to enter the card identifier. To do this, tap a card on the USB reader or enter the card ID via a keypad. The identifier must be a hexadecimal number including 6 characters at least. One user may be assigned up to 2 access cards.

One RFID access card can be used for access to up to 90 doors with the 2N Fortis locks, depending on the number of the time profiles applied. If the card memory capacity is exceeded, data writing to the card will fail. The write failure event is recorded in the system Access Log. If Lock Groups are used, more doors can be written to a single card than the case is with individual assignment.

TIP
The User Manager and Administrator can view the card identifier in the Access Log. The new/unassigned card can thus be loaded on an accessible device and then its identifier can be copied from the log. After adding the identifier to the RFID cards, the user can start using the card. The display of identifiers in the Access Log must be enabled in **Settings > Authentication**.

NOTE
If **Access Commander** reports that the brand new card just added is already in use in the system, the reason may be that the RFID card compatibility mode is enabled. This mode is activated by the Administrator in **Settings > Authentication > Compatibility Mode Settings**.

My2N app – used for interconnection with My2N app app, which provides authentication via Bluetooth, refer to Subs. Bluetooth Authentication (p. 50).

PIN Code – automatic generation of a 5-digit PIN code.

A user can be assigned a PIN code or a QR code, never both of them at the same time.

QR Code – automatic generation of QR code. The devices that allow QR codes to be read are included in Supported Devices and Applications (p. 8).

A user can be assigned a PIN code or a QR code, never both of them at the same time.

Fingerprint – a dialog box helps you enroll fingerprints for authentication on the devices that support fingerprint reading. Each user can enroll up to 2 fingerprints. Refer to Subs. Fingerprint Enrollment (p. 50) for details.

License Plate – set the vehicle license plate to be scanned by the device and used for user authentication.

Virtual Credential – set the user virtual access card ID. Each user can be assigned just one virtual card. The virtual card ID is a sequence of 6–32 characters: 0–9, A–F. The virtual card ID is used for user identification in the devices connected via the Wiegand interface.

Switch Code – set up to 4 switch activation codes (e.g. for the door lock). The switch code is used for door unlocking via the device keypad even as a DTMF code.

CAUTION
Remember to keep the sequence of authentication methods while using multi-factor authentication.

TIP
It is possible to send the generated access PIN/QR code to an e-mail address if available.

Account

A user can be assigned access to the **Access Commander** interface by setting a login name and one-time password. Upon login, the user can follow their attendance (if available), and change their e-mail or profile image. The user will be prompted to change the password upon the first login. If two-factor authentication is requested for a user, the user will be prompted to interconnect with their own authentication application, see Two-Factor Authentication (p. 98). The interconnection with the authentication application can be removed on this card too.

On the Account card, the users with login data can be assigned rights to administer **Access Commander** through user roles. Refer to Subs. User Rights (p. 7) for a description of role rights.

Simplified Interface

It is possible to run a simplified user interface for the visitor manager of one company. The simplified interface allows the visitor manager to add, remove and manage visitors. Logs and Presence cannot be viewed in the simplified interface. The primary purpose of the simplified interface is to facilitate visitor access to users' apartments. All the visitors created in the simplified interface are always assigned to the *default group for new visitors*. The visitor manager cannot change this group. It is necessary to select the default group for new visitors in the company settings and set valid apartment access rules for the group, including the path to the apartment. Thus, the apartment user can manage the authentication methods and visit duration in the simplified interface.

CAUTION
Before activating the simplified interface, **the system administrator must set the default group for new visitors** in Company Settings (p. 41). The default group must be assigned such access rules that allow visitors to access the required spaces. No visitor access can be guaranteed in the simplified interface without a properly set default group.

Personal Information

Used for adding basic information on the user. The user e-mail address to which account info shall be sent and a user contact phone number can be added.

The following can be written on the card:

- **E-Mail** – address to which information related to the user account in **Access Commander** will be sent
- **User ID** – specific identifier necessary for bulk synchronization with the CSV file (refer to User Synchronization (p. 89))
- **Note**

Access

The Accesses card helps assign a user to a group and set the time interval in which the user access data shall be valid. Click ⋮ to open an advanced menu to set the time interval. The beginning of the validity term is only applied to access to IP devices. Access to the 2N Fortis electronic locks is valid from the moment the access card is assigned to the user.

TIP
Time limitations for accesses from the devices are set using time profiles.

The card shows the group the user is assigned to. If not assigned to a group, a user can be added on this card. A group can be changed or deleted in an advanced menu .

Phone Numbers

This card helps you set connection with a user. The phone number is the calling destination of the device assigned to the user.

Virtual number

A virtual phone number can be used for user calling via the numeric keypad on the device. Virtual numbers are not related to the users' personal phone numbers and thus help hide the users' personal phone numbers on the device. Virtual numbers can be set up according to apartment numbers, for example. Virtual numbers can therefore be used in installations where the number of speed dial buttons is insufficient.

A virtual number can have 1 to 7 digits. The first and last characters can be either digits or letters, while the rest must consist solely of digits (A123, 456B, C12E, e.g.).

Deputy

A deputy can also be defined on the card to which a call is forwarded in the case of user unavailability. The deputy can be chosen among the other users in the company.

Access Log

The Access Log shows access history.

Change Log

All the user setting changes can be displayed in the Change Log folder. The basic arrangement is based on the change time. It is possible to find out who made the change in the log. Click the row to find details on the change accomplished.

Fingerprint Enrollment

Each user can enroll up to 2 fingerprints.Use an external fingerprint reader for enrollment. Make sure you have installed the 2N USB Driver. The driver can be downloaded here.

The enrolled user fingerprint can be used for the following actions:

- Open the door;
- Trigger silent alarm – can only be set if the Open door function is active;
- F1 and F2 automation – generates the FingerEntered event in Automation. F1 and F2 help distinguish the scanned finger in Automation.

Fingerprint Enrollment

1. Make sure that the USB fingerprint reader is enabled in **Settings > Credentials**.
2. Select Fingerprint authentication in the user settings on the **Credentials card**.
3. Select the finger to be scanned and enrolled.
   The Fingerprint enrollment box is displayed.
4. Put the selected finger on the reader. Repeat this step 3 times, always upon invitation.
   You will be informed that your fingerprint has been scanned successfully after the last scanning.
5. Click **Create** to complete the process.

Bluetooth Authentication

Make sure that the My2N app is installed in your mobile phone to make successful authentication via Bluetooth.

This process is secured by the **Bluetooth trusted pairing** mechanism. The pairing process varies depending on the firmware version of the device connected.

Enter the pairing code into the My2N application to connect the application on the user's phone to the 2N devices.

Get the pairing code as follows:

- by connection with a **2N OS** device
- through a USB Bluetooth reader connected to your PC

CAUTION
Make sure that the device firmware version is 2.50 (or 3.0) and higher to achieve successful trusted pairing. If the device has an older firmware version, pairing will be made via an older mechanism using a **PIN** without a **QR code**.

TIP
Pairing via a **QR code** is recommended for higher security. If the **QR code** is unavailable or unsupported, use the **PIN**.

Pairing Code Creation via PC

1. Download and install 2N IP USB Driver into your PC.
2. Make sure that the USB Bluetooth reader is enabled in **Settings > Credentials > Enabled USB readers card**.
3. Connect the USB Bluetooth reader to the PC.
4. Select My2N app authentication in the user settings on the **Credentials card**.
5. Select Pair using reader in the open dialog box.
   The pairing code appears in the dialog box.
6. Follow the steps below for pairing in the application (My2N Mobile Application Pairing (p. 52)).

Pairing Code Creation Using Device

1. Make sure that
   - the pairing device is set for the given user's company, refer to Company Settings (p. 41);
   - the pairing device is located in the zone which the user is allowed to access, refer to Access Rules (p. 70);
   - an adequate pairing time value is set, refer to Company Settings (p. 41).
2. Select My2N app authentication in the user settings on the **Credentials card**.
3. Select Pair using devices in the open dialog box.
4. The generated pairing code is displayed on the card together with the remaining pairing time. Transfer the pairing code to the user. If the user's e-mail address is completed, you can send the mobile key by clicking .
5. Follow the steps below for pairing in the application (My2N Mobile Application Pairing (p. 52)).

My2N **Mobile Application Pairing**

1. Download the My2N application to your mobile phone. The app is available at App Store and Google Play.
2. Open the My2N app and enter the pairing PIN.

> **NOTE**
> If the application displays a **QR code** yet the device uses firmware older than 2.50.0, pairing will be successful only if the **PIN** is entered.

3. Allow all the important authorizations to make My2N work properly.
4. Follow the instructions on your mobile phone – bring the phone close to the device in the pairing mode and click Start pairing. Subsequently, the mobile phone starts searching a device for pairing.
5. Grant access to the selected mobile phone. Now you can open doors in the whole location.

> **WARNING**
> Use the Mobile Key application for pairing of mobile phones with older OSs (Android 9 / iOS 17 and lower).
>
> ### Mobile Key **Pairing**
>
> 1. Download the Mobile Key application to your mobile phone. The app is available at App Store and Google Play.
> 2. Open the application and enable Bluetooth access for Mobile Key.
> 3. According to the mobile key type, draw your mobile phone near the USB reader or the pairing device.
> 4. Click the device offered for pairing in Mobile Key.
> 5. The application prompts you to enter the PIN code. Enter the pairing code and confirm.

User Rights

Multiple users can manage accesses in **Access Commander** depending on their assigned rights or privileges.

Accounts with extended rights are set through the role in the user settings. One user can be assigned multiple roles.

> **NOTE**
> User rights relate to the management within the user's company. The administrator has access to the complete management across the companies.

Administrator

- System and module settings according to the valid license.
- License Change.
- All rights of other roles related to all the companies.

Access Manager

- Creating and managing groups.
- Adding users to groups.
- Creating and managing visitors.
- Creating and managing time profiles.
- Setting access rules.

User Manager

- Creating and managing users.
- Creating and managing visitors.
- Adding users to groups.
- Viewing access and system logs.

Visitor Manager

- Creating and managing visitors.
- Managing visitor assignment to groups (not available in the simplified interface).
- Viewing visitor access log (not available in the simplified interface).

Door Manager

- Viewing camera transmissions from assigned devices.
- Remote opening of assigned devices.
- Emergency lockdown of assigned devices.
- Viewing access log of assigned devices.
- Monitoring states and security events in the system log.

Attendance Manager

- Monitoring and managing attendance of assigned groups.
- Viewing access log of users in assigned groups.

Company Administrator

- Setting the company's default language.
- System log monitoring (limited to the company events).
- Setting a widget for the system log and emergency lockout on the devices used by the company (including the devices shared with other companies).

Attendance

Access Commander helps you monitor user attendance. The user entry/exit times are recorded in the Attendance mode.

User attendance monitoring has to be activated. To do this, use the extended menu in the user detail header. To activate attendance monitoring for multiple users at the same time, select the users listed on the Users page and use bulk action .

The attendance manager can edit the user attendance data. To do this, click the time interval to be changed. You can also edit the border times and add a note to an interval.

CAUTION
Make sure that the user attendance monitoring license is active in **Access Commander** to monitor attendance properly. Remember to activate attendance monitoring for each user in the user settings.

Monitoring and editing attendance are described in the chapter Attendance (p. 74).

Groups

A group is used for gathering users and easier setting of the group member zone access rights. The rights do not have to be set on the user/visitor level but the group can be associated with a zone.

Filter the list items using above the list. Or, click in each column header to open an extended menu and set filters for each column. The extended column menu also enables you to move, pin to the first/last position or hide the columns.

Group Creation

1. Go to the **Groups** page.
2. Click the group adding button in the right-hand upper corner.
3. Enter the group name and assign the group to a company in the open dialog box.

   CAUTION
   Once a group is created, the superior company cannot be changed.

   The new group appears on the list and its detail opens up. Add the group members and set their access rules in the group detail.

Group Settings

View and edit the group information in the group detail. Click the selected group list item to open the group detail. The detail shows a list of the group members and their access rules.

Members

The card shows all the users assigned to a group. You can only add those users/visitors to the group that are assigned to the same company as the group.

Access Rules

This is an overview of all the access rules that you can edit or create. By creating an access rule, you grant zone access to a particular group. To create a rule, enter the group and a time profile to limit the group's zone access.

Zones

Zones make it easier to manage accesses to devices. Zones combine devices into logical sets. The page shows a list of all zones.

Filter the list items using above the list. Or, click in each column header to open an extended menu and set filters for each column. The extended column menu also enables you to move, pin to the first/last position or hide the columns.

Enabling access points

With , a dialog box will open in which access point support can be activated, see Setting Device Access Points (p. 75).

Zone Creation

1. Go to the **Zones** page.
2. Click the zone adding button in the right-hand upper corner.
3. Enter the zone name and assign the zone to a company (companies) in the open dialog box.
   The new zone appears on the list. Add a device to the zone in the zone detail or device detail. More settings can be made in the zone detail.

Zone Settings

View and edit the zone information in the zone detail. Click the selected zone list item to open the zone detail.

Multi-Factor Authentication

You can set multi-factor authentication for all the devices in a zone. You can select just some of the authentication methods but always keep the following order:

1. My2N app
2. RFID card
3. Fingerprint
4. PIN code

CAUTION
Remember to keep the sequence of authentication methods while using multi-factor authentication.

The necessity of multi-factor authentication can be limited by a time profile. With multi-factor authentication on, the **Use Multi-Factor Authentication** option is displayed for you to choose a time profile using . If “Anytime” is selected, multi-factor authentication will always be required.

Multi-factor authentication can only be required for zone access. This setting only applies if access points are used.

Access Settings

You can set a bulk **PIN Code for Zone Access** on the card or display the PIN code if already created.

Moreover, you can enable/disable the following functions in Access Settings:

Silent alarm – once a special code is used, Silent alarm is activated, which sends an alarm report; the device does not signal any alarm sounds in this mode. Set the special Silent alarm code and function in the device configuration.

Access lockout – after five unsuccessful attempts, the next attempt will not be allowed until 30 seconds pass.

License plate authentication – vehicles are granted zone access based on their license plate verifications by all the devices that support this function.

Devices

The card shows a list of all the devices added to the given zone. More devices can be added on the card.

If used, access points are assigned to a zone. The access point type for the given device is described as Entry to Zone.

Available authentication methods are displayed for each device / access point.

Lock Groups

The tab shows an overview of the lock groups. More groups can be added on this tab.

You can view the group details for each lock group.

Companies

This card shows a list of the companies that are granted access to the zone. Multiple companies can have access to one zone.

Access Rules

This is an overview of all the access rules that you can edit or create. By creating an access rule, you grant zone access to a particular group. To create a rule, enter the group and a time profile to limit the group's zone access.

Click the selected access rule to edit it.

Devices

The Devices page shows all the devices added to **Access Commander**.

Filter the list items using above the list. Or, click in each column header to open an extended menu and set filters for each column. The extended column menu also enables you to move, pin to the first/last position or hide the columns.

Press Export above the list to download the list in a CSV file. The time is GMT+0 in the CSV file exported.

Select multiple devices to be applied the following bulk actions to:

- Manage selected devices
- Remove selected devices from management
- Back up selected devices

The icon on the device row redirects to the web configuration interface of the device.

Devices Status

- Online
- Unmanaged — Device management has been turned off by the user.
- Incompatible — the device does not have a supported firmware version.
- Not configured — you need to upload the configuration of electronic locks from a third-party program.
- Offline
  - Login Failed – wrong login data has been entered into the device web configuration in **Access Commander**.
  - Inaccessible – **Access Commander** cannot establish connection with the device.
  - Invalid Certificate – SSL certificate verification is required and the device has no valid SSL certificate.

Adding IP Device

NOTE
Adding 2N Fortis electronic locks is described in Electronic Locks (p. 22).

1. Go to the **Devices** page.
2. Click the device adding button in the right-hand upper corner.
3. To add a 2N intercom/2N access unit/2N answering unit, select “2N IP Devices”.
4. In the open dialog box, find the device in the LAN or enter its IP address and port in the following format: “IPaddress:port”.
   Having entered the IP address, you can press ENTER on the keypad and add another device.
5. Having added all the selected devices, complete the web configuration access password for these devices. You can only add those devices at the same time to which you log in with one and the same password.

6. Template Application (optional): To apply a template to the device to be added, activate the switch **After adding the device, use the configuration template**.
   - The principle of selecting and applying a configuration from a template is the same as manually applying a template to an existing device, refer to Device Templates (p. 67).
7. Name the device before creation.
8. The new devices appear on the list. Make other settings in the device detail.

Lock Groups

Lock groups help you group locks into logical complexes for subsequent definition of access rules, monitoring or device management.

Displaying Groups

Open **Devices > Lock Groups**.

NOTE
The list includes all the lock groups created. Use the search field to filter the records by their names.

Lock Group Creation

1. Open **Devices > Lock Groups**.
2. Click + Lock Group.
3. Enter the group name and choose the Create tab.
4. In the **Locks** module, click Add Locks. Select the locks to be assigned to the group.
5. In the **Zones** module, click Add Zones. Select the zones to be assigned to the group.
6. Select ⋮ for adding, renaming or deleting a lock group.

WARNING
Changing the lock assignment to another group requires repeated configuration. Make sure that all the system changes have been completed before exporting the configuration file.

Lock Settings in Access Commander

Before uploading keys to individual locks, you must pair **Access Commander** with **Fortis Commander**.

Master Encryption Key (MEK) Generation and Project Preparation

1. Log in to Access Commander.
2. Go to **Settings > Electronic locks**.
3. Click Generate Keys in **Initial Settings**.

4. Create the master encryption key.

CAUTION
The master encryption key cannot be **displayed or changed** later.

NOTE
According to the master encryption key (MEK), **2N Access Commander** generates a set of encryption keys. Thus, the key should be unique and sufficiently secure. As the key set is based on the master encryption key, projects with one and the same master encryption keys generate the same sets of keys. If a project is lost, you can create a new project with the same master encryption key and continue encryption.

5. Having generated the keys and set the password for the project file, you can download the **project file**, which represents an image of the electronic lock configuration in the **Access Commander** system.
6. On the **Fortis Commander** tab, click Download Application, to download the **Fortis Commander** electronic lock configuring application.

CAUTION
Project information is sensitive data. Protect it from abuse.

Propagation of Electronic Lock Configuration via Fortis Commander

1. Install and open the **Fortis Commander** application.
2. Click Open Project to open the downloaded project file in the File Explorer.
3. In the open dialog box, enter the project file password.
4. After opening the project file, select Connect to Device and tap the service card on the lock.
5. Click **Assign** to assign the lock to the project.
6. Disconnect the device and click **File > Close project**.
7. When the configuration is complete, open **Access Commander**. Go to the **Settings > Electronic Locks** and click the Fortis Commander button again. Upload the project file.

NOTE
When moving the lock between installations or when making a claim, you must perform **Factory Reset**. This operation resets the lock to factory settings and removes all previous configuration.

Configuration Update Instructions

1. Make changes in **Access Commander**.
2. Download a new project file.
3. Upload the file to **Fortis Commander** and make the required changes to the locks.
4. If you make other changes in **Access Commander**, always download a new project file.

CAUTION
Make sure to download a new project file for every configuration change in **Access Commander** – never use an older file already uploaded to **Fortis Commander**.

Permanent Locking/Unlocking

The app allows you to permanently lock and unlock the lock. The function is used for service interventions or emergency control without the use of a card.

Emergency Lockdown

Emergency lockdown is used for complete locking of the doors controlled by the given device. During the emergency lockdown, it is impossible to open doors using pre-defined user accesses even in case the user/visitor uses a valid access with a valid time profile.

You can activate/deactivate the emergency lockdown:

- in the device detail – lock the given device;
- in the zone detail – lock all devices in a zone;
- in the company detail – lock all devices in a company;
- using a global action by pressing on the upper bar to lock all devices in **Access Commander**;
- in the Widget on the Dashboard.

It is possible to pre-define a group of devices that are subject to emergency lockdown in the Emergency lockdown Widget.

CAUTION
Offline devices, inactive devices, device with incompatible firmware and devices with FW version lower than 2.32 will not be locked down after the Emergency lockdown request. Offline devices will be locked down when they become available again.

Device Configuration

You can view and administer device information in the device detail. Click the selected device list item to open the device detail. According to the device type, the detail can be divided into Overview, Calls and Lift.

Click the **Configure hardware** button in the right-hand upper corner of the device detail to move from the device detail to the web configuration. Refer to the Configuration Manual of the selected device for its configuration. Click the cross in the blue upper bar to quit the configuration web interface and return.

Overview

State

This tab shows the state of connection with a device. Online devices are such devices that are connected with **Access Commander** and equipped with the acceptable firmware. Data synchronization can take place thanks to the established connection with the device. If incompatible, firmware can be allowed in **Devices > Firmware**.

Automatic synchronization is started upon every change that is to be reflected in the end device configuration. Synchronization only takes place over the devices that it relates to. Only the synchronization requests caused by the changes that can affect the end devices are queued. Such changes include changes of

access rights, phone numbers, time profiles, etc. For example, a name change for the user that is not assigned to any group never starts automatic synchronization. The synchronization time (necessary for all the changes to be applied to end devices) depends on the count of devices to be synchronized and the amount of data to be uploaded into the device.

Access Control

Set the zone to which the device is to be assigned.

If the device has 2 access points set up and if access point detection is enabled (see Setting Device Access Points (p. 75)), the option to assign 2 zones is displayed. One device access point can only be in one zone.

Configuration

The card shows the current firmware version, MAC address and IP address and enables you to change the web configuration access password.

In the tab, it is possible to change the IP address on which the device is located, which allows **Access Commander** to be pointed to the device that has been disconnected and reconnected at a different IP address.

Door Control

This card shows images from the device cameras and provides remote opening of the door switch controlled by this device. Click ⋮ to open an advanced menu to set door opening for a certain period of time.

The current door switch state is displayed next to the Open button.

Use Emergency Lockdown (p. 61) to lock the door even for groups with valid access.

Backup

Backup helps you back up the device configuration in an xml file. Start the backup using Start backup. If stored in the local storage, the backup will be stored in the **Access Commander** dedicated memory. If stored in a file, a dialog box will open for you to secure the backup file with a password. As the file contains sensitive data, file protection is recommended. Backup encryption is available in devices with firmware 2.45 and higher.

Each last backup is displayed on the tab. The device can be automatically synchronized with the last backup using the Restore option. In this drop-down menu option, you can also choose to Restore from backup of another connected device or from an external file.

NOTE
All the available devices (online devices and connected devices with incompatible firmware) can be backed up.

Calling

The call tab is displayed if a telecommunication connection is available and enabled on the device. The tab displays all enabled accounts providing the connection including their statuses. The telecommunication connection is set directly in the configuration interface of the given device, in the Calling section. The configuration interface is entered using the Hardware configuration button in the device detail header.

Calling

This folder is displayed in the detail of the device from which calls can be made.

Touchscreen phonebook

Use the Contacts card to administer phonebook displays on devices equipped with a display. The card displays a tree of contacts as shown in the device directory. Click Change to open a dialog box for contact tree editing. The sequence of the contact items is displayed in the left part of the dialog box. The contacts are set within the selected folder in the right-hand part. The root folder is the first page displayed whenever the device directory is opened. All the contacts stored in this root folder are displayed on one directory page. The contacts can also be grouped into folders and the folders can be assigned to the root folder.

Adding Contacts to Device Display

1. Go to **Devices > Device detail > Calls > Touchscreen phonebook.**
2. Click Change to open display administration.
3. Select the folder to add contacts in the right-hand part of the open dialog box.
   You can add the following to the folder:

   1. **Users**
      You can choose multiple users simultaneously.
   2. **Groups**
      You can use bulk adding for groups of users. The directory shows every user in the group under the user name. You can choose multiple groups simultaneously.
   3. **Calling Groups**
      Calling groups are groups of contacts that are to be dialed simultaneously. While creating a calling group, enter the group name to be displayed in the directory. User contacts are added to calling groups in the same way as contacts are added to folders.

      You can rename a calling group in an extended menu at the folder opened by clicking .

4. You can rename a folder in an extended menu at the folder opened by clicking . You also add an image to a selected folder in the extended menu, which then appears at this folder on the device.
5. Pin the folders/calling groups to be displayed in the first places in the extended menu at the given folder using .

Additional virtual numbers

It is possible to start an outgoing call by dialing a virtual number on a device with a numeric keypad. On this card, you can add the users that can be called using virtual numbers even if these users do not have access to the device. Calls to the virtual numbers of the users that have access to the device are allowed automatically.

In the selection of users, those users are only displayed whose virtual numbers have been completed.

Buttons

This card is displayed in the details of the devices equipped with buttons used for dialing user phone numbers. The Buttons card helps you assign users to the buttons on the device. A press of the device button starts an outgoing call to the destination of the assigned user. The user is assigned to the button by clicking and selecting the user.

Lift

By connecting the AXIS A9188 relay module to a 2N intercom or to a 2N access unit, access to the elevator floors in the building can be controlled. Up to 8 of these relay modules can be connected to one 2N intercom or 2N access unit, each of which being able to control 8 floors, which makes a total of 64 floors. To use this function, you must have an active license: for IP intercoms (Part No. 9137916) or for access units (Part No. 9160401).

Lift Control Settings

1. Make sure before configuring via **Access Commander** that the AXIS A9188 relay module is interconnected with the 2N device responsible for floor access authorization. Also make sure that HTTPS has been set and the root password has been changed on the module.
2. Go to the detail of the device to be used for floor access control. Activate lift control in the advanced menu . **Lift** is displayed in the device detail.
3. In the header of the device details, navigate to the hardware configuration. Go to **Integration > Access Control > Elevator**. Enable all the relay modules that are to control access from the elevator. If the modules require authentication, enter the username and password. Save the settings. Click the cross in the top blue bar to exit the hardware configuration.
4. Go to the Lift tab in the device detail.
5. Select the relay output for the floor for which access is to be set on the Lift floors card. Specify the output(s) as follows: *io_module_relay output*. Click .
6. Name the floors and select a floor zone to be accessed in the open dialog box. Thus, only the users with valid zone access based on the defined access rules may access this particular floor. If the access rules are not to be applied, select **public access allowed**. Select a time profile to limit the public access to a period of time defined by the selected time profile. Beyond this time profile, access will only be granted to the users with valid access based on the access rules.

> **CAUTION**
> If access is set according to the zone access rules, the lift device does not assume any of the other zone settings (PIN code, multi-factor authentication, silent alarm, etc.).

Lift Floors

If enabled, a list of all configurable floors is displayed on this card. Each floor has its designation in the sequence of the module and relay output. Each floor can be assigned a name of its own.

Lift Control Modules

This card shows all the connected AXIS A9188 modules including their current states. Enable the modules in the device configuration in **Hardware > Lift control**.

Monitoring

The page is used for finding information on the connected IP devices (intercoms, access units, answering units). Every administrator can configure the table as needed using . Each account has a unique setup. Select the columns displayed to make the setting.

Click a row to get to the detail of the selected device.

Firmware

The Firmware page provides a bulk firmware upgrade for all the types of connected devices to maintain them in the optimum condition. You can suspend bulk administration of the devices. Optionally, some devices can be excluded from bulk administration.

> **TIP**
> A new firmware version may be installed for one or more selected devices in the test mode and only then upgrade can be allowed for the other devices.

The current firmware version is available online via the 2N Update Server and, optionally, the upgrade file can be uploaded manually. The deployment of a new version is always subject to the administrator's approval so that the whole upgrading process is under the administrator's full control.

It may take a few minutes to get the firmware versions from the 2N update server.

The version displays a list of connected 2N intercom types, 2N answering units and 2N access units in bulk administration.

Excluded Devices

To exclude a device from bulk firmware administration, add it to the list in **Devices > Firmware > Excluded Devices**.

Incompatible Firmware Versions

When added or upgraded, a device with incompatible firmware goes into the incompatible state. Incompatible state means that no new users are stored in the device. Events can still be downloaded from the device and its configuration or backup can still be used. A new record is created in the table and the administrator can enable the use of incompatible firmware.

Access Commander automatically excludes a device with firmware that is not supported by the latest firmware version. The card shows these unsupported firmware versions on the devices connected. See the list of supported firmware versions below.

Access Commander can control all the devices that use an unsupported firmware version when this version is approved. Approve the version in **Devices > Firmware > Incompatible Firmware Version** using the  .

CAUTION
The approval of an unsupported version may lead to such problems as data loss or some kind of malfunction.

Supported Firmware Versions

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

Security

Set the communication security method for Access Commander and the devices in **Devices > Security > Device Certificate Verification**.

Access Commander provides three levels of device communication security:

1. **Encrypted communication without certificate authentication** - **Access Commander** uses a self-signed certificate for HTTPS communication. This certificate is considered untrustworthy by web browsers.

2. **Certificate Fingerprint Verification** – communication is ensured by checking the certificate uploaded to the device. The certificate fingerprint is verified during the communication.
   When fingerprint verification is turned on, the device administrator must confirm the validity of the certificate fingerprint whenever a new device is added. The device administrator will be prompted to verify the fingerprint even if the certificate of an already added device is changed.
3. **Complete Certificate Verification** – communication is secured by a certificate signed by a so-called certification authority. During communication, the entire certification chain is verified according to the PKI requirements.

CAUTION
It is impossible to upload own SSL certificates to the 2N Indoor Touch devices as the connection with them will be lost after certificate verification is enabled.

How to Manage Certificates

Set the communication security method for Access Commander and the devices in **Devices > Security > Device Certificate Verification**.

After SSL certificate verification is enabled, synchronization will only take place on the devices that have a SSL certificate signed by a trusted certification authority. Synchronization of devices without such SSL certificates is disabled. The devices will go offline.

The certification authority (CA) certificate has to be trustworthy on the server on which **Access Commander** is running.

TIP
The process of uploading certificates to the server is described in the FAQ.

To be verified successfully, the device certificates have to be signed by a certification authority and include the device IP address/domain name.

Device Certificate Upload

1. Enter the web configuration of the selected device.
2. Go to **System > Certificates > User Certificates**.
3. Upload the pre-prepared certificate.
4. Go to **System > Network Connection > Web Server**.
5. Select the certificate you uploaded in the **HTTPS Server Certificate** parameter.
6. Save your changes.

Setting Device Access Points

You can logically divide each device into two access points - arrival and departure. Each access point represents a passage in one direction and determines whether the device user enters or leaves the zone. One access point can be controlled by one or more device modules. All the assigned modules then manage the passageways in the direction of the specific access point. The access points are used especially where a device is on the boundary of two zones and the direction of movement between them needs to be accurately recorded (for anti-passback, for example).

In addition, access points help monitor the users in the Presence (p. 80) module. Also, access points are used for monitoring entries/exits in Area restrictions (p. 82).

NOTE
The access points are referred to as **Arrival** and **Departure** in the web configuration interface of each device. Go to **Access > Access Rules > Entry and Exit tabs** to set them up.

Enabling Access Points in Access Commander

1. Go to Zones in **Access Commander**.
2. Press in the right-hand upper corner and enable the use of access points.

Module Assignment for Arrival or Departure

1. Enter the web configuration of the selected device.

   TIP
   Click in the list on the Devices page to enter the web configuration interface.

2. Go to **Access > Access Rules**.
3. Go to Zones in **Access Commander**.
4. A dialog box opens with a list of available access managing modules.
5. Drag and drop the modules into groups according to the direction they are supposed to provide.

   TIP
   Click to locate a specific module. The module triggers a visual or acoustic signal depending on its capabilities.

Device Templates

The Device Templates function helps you configure multiple devices. The templates simplify initial system installation and unify settings across projects.

The templates work on the principle of pattern. The templates help you save the entire configuration of any **2N OS** device or just selected configuration parts and apply the configuration to other devices. The configuration can be based on a device already configured, a device backup or a template previously exported.

While creating a template, you can choose which parts of the configuration are to be included. The components vary according to the device type (e.g. relay settings, audio outputs, automation). This selection is part of the template creating process and cannot be changed after saving.

NOTE
Using templates significantly reduces the initial commissioning time of the device.

Template Creation and Management

Go to Device > Templates to access the template function.

1. Click + Create Template from Device.
2. The **Create Template** dialog opens.
3. Select an existing device from the **Device*** pop-up menu to be the basic device for your template. Only template compatible devices will be displayed.
4. Click Next to continue configuring the template.

> **CAUTION**
> Warnings may appear for some configurations. They inform that selected configurations may have limitations or potential risks. The selection is still possible, but it is recommended that you check the notification.

Import Template or Backup from File

If you already have a template or device backup saved in a file, you can easily import it:

1. Go to Devices > Templates.
2. Click Import from File at the top right.
3. Select the template/backup file from your PC and click Import.

> **NOTE**
> Some sections may show as deactivated during import. They include the configuration parts that could cause unintentional changes or impair the device function. These sections are automatically removed upon import and can be seen briefly by the user while loading.

Template Modification

The template can be modified after creation. The interface only displays the configuration parts that were included in the template creation.

1. Go to Devices > Templates.
2. Select a template from the list.
3. Click Edit Template.

A dialog with the configuration sections is displayed.

Edit Values

- Double-click a value to edit it.
- The modified item is marked as changed immediately.
- The ⚠ warning icon indicates the values that may not be fully validated on the device.

CAUTION
The validation performed at the template modification is for guidance only and is performed **at the item level**. The check does not capture all conflicts across devices and firmware versions and does not match the full validation process performed on **2N OS**.

An item marked with a warning may still be usable on the device and, on the contrary, an item without a warning may be rejected during application. The real evaluation takes place on the device.

Apply Template to Device

A template can be applied to one or more devices. It can also be applied using bulk actions in the device list or directly from the device detail.

1. Go to Devices > Templates.
2. Select the template to be applied to the device.
3. Click Apply to Device.
4. Select a device and confirm.
5. The configuration list is displayed. These sections correspond to the selections made during template creation, but can be modified.
6. Click Apply.

CAUTION
A warning is displayed if a discrepancy between the firmware version or device type for which the template was created and the target device version/type is detected during the template application. Non-compliance must be confirmed before proceeding.

NOTE

- The state only confirms that the process has started successfully. It does not provide information on the actual progress or completion of the application.
- Refer to Adding Device (p. 58) for the instructions for use of a template while adding a device.

Access Rules

Access Rules represent a clear management tool for user group accesses to zones. Accesses can be granted based on time profiles.

The access rules define TO WHOM, WHERE and WHEN access is granted.

- **WHO** is defined by the group and the users assigned to it (one user may be in more groups assigned to one company at the same time).
- **WHERE** is defined by the zone or devices (one device may be assigned to one zone only).
- **WHEN** is defined by the time profile assigned. This item is not mandatory. An empty time profile means an unlimited access (24/7).

NOTE
One group can have access to multiple zones and multiple groups can have access to one zone.

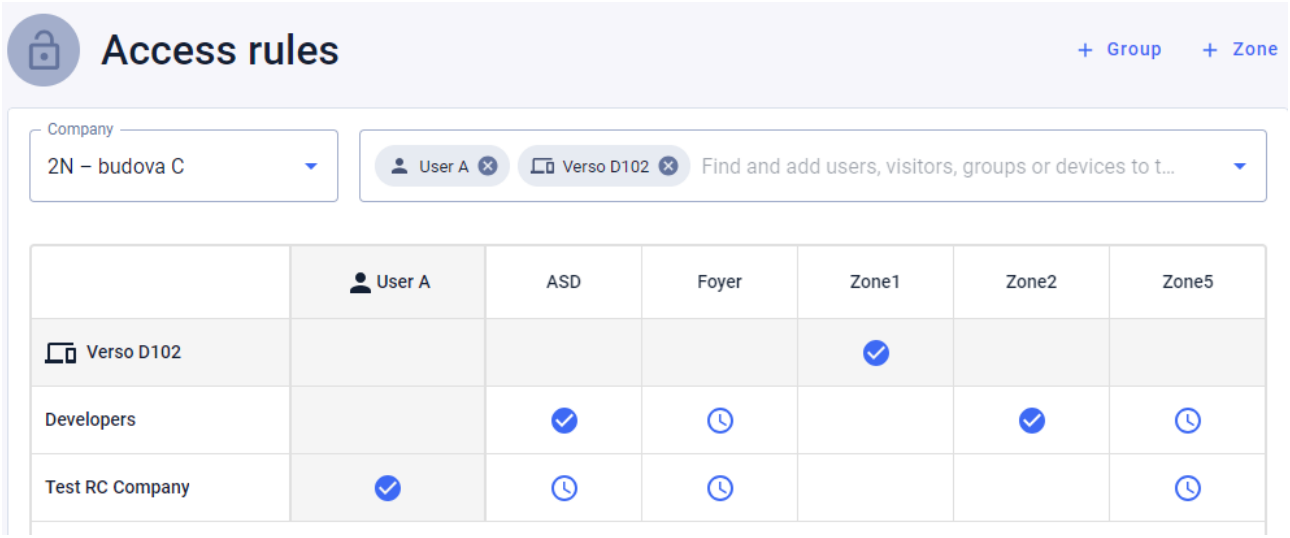
Matrix Display

The matrix display of rules on the Access Rules page provides an overview of accesses and their setting options. The matrix is available to every existing company and shows all the groups and zones assigned to it. The administrator can switch companies in the menu above the matrix.

Click the cell corresponding to the selected zone and group to set the group access to the zone. A menu is displayed for you to choose either an unlimited access or access limited by a time profile. The time profiles have to be preset on the page Time Profiles (p. 72). A new group/zone can be added to the company matrix if necessary.

A user/device can be added to the matrix in the search field above the matrix. Users can be added to groups by uniting the user and the group. Devices can be added to a zone by uniting the device and the zone.

Example of Matrix Display



The figure shows a matrix survey for 2N Telekomunikace. It is obvious from the survey that:

- The filtered device Verso 2.0 D102 is part of Zone1.
- The filtered User A is part of the Test RC Company group.
- The users from the Developers group have unlimited access to ASD and Zone2, limited access to Foyer and Zone5 (according to the set time profile) and no access to Zone1.
- The users from the Test RC Company group have limited access to ASD, Foyer and Zone5 (according to the set time profile) and no access to Zone1 and Zone2.

Rule List

The Rule List page shows a list of all the currently valid access rules. Click a rule to edit it. Click the Access rule button in the right-hand upper corner to add a new access rule. Remember to set the rule parameters before creating a rule.

The Rule list and the Matrix show the same access rules. A change in one display will automatically propagate to the other one. The access rules are also edited in the zone and group settings.

Time Profiles

Selected device functions can be time limited. A time profile can be assigned to a selected function to define when the function is available.

Time profiles can meet the following requirements:

- block all calls to a selected user beyond the set time interval;
- block calls to selected user phone numbers beyond the set time interval;
- block user access beyond the set time interval.

Each time profile defines the function availability based on a week calendar. Simply set From-To and specify the weekdays for availability. The time profile based access is defined by the access rules. Limitation of user availability beyond the time profile is set together with the user phone number.

Optionally, up to 20 general time profiles can be created, which, in addition to access control, can be used for special local configuration cases. These time profiles are uploaded to all synchronized devices.

Time Profiles on Electronic Locks

Electronic locks support time profiles with the following limitations:

- Holidays do not apply.
- You can set up to 4 different time intervals per day.
- 4 daily interval schedules can be defined within one time profile.

TIP
This means that you can have different settings for Monday, Tuesday, Wednesday and Thursday, for example, but you must use one of the existing settings for Friday, Saturday, and Sunday.

CAUTION
If the time profile violates the specified restrictions, the access rule will be ignored and the user will not be granted access.

Time Profile Creation

1. Go to **Time Profiles**.
2. Click the + Time Profile button in the right-hand upper corner.
3. Set the time profile name in the open dialog box.

4. Select Add Time Periods for time restrictions. The days highlighted in blue identify the days assigned to the time profile. Click to select a day. Set the time interval within the days to define the time profile validity.

> **NOTE**
> You can set a time interval within days to define the time profile validity.

> **CAUTION**
> Different times for each day cannot be set until the time profile has been created.

5. The new time profile is added to the list and its detail opens up for you to set other parameters. You can set the profile position on the devices in the time profile detail.

> **NOTE**
> Global profiles may affect access across all the companies. They can only be edited by the Administrator.
>
> The Access Administrator may only correct the time profiles of his company.

Time Profile Settings

The time profile detail displays a day and time schedule. Blue intervals show when the given time profile is active. You can set any count of time intervals per day.

Click the hour slot and set the time profile active time to add an interval. Click the interval to change the interval time value. To make a profile active whole day, add an interval covering one whole day, i.e. 00:00–23:59.

Click ⋮ to open an extended menu to set the position on a device. The position on a device defines the position in the time profile list, which is uploaded to all the devices that are assigned time profiles.

Limitation of user availability beyond the time profile is set together with the phone number in the user settings.

Attendance

Access Commander helps you monitor user attendance. The user entry/exit times are recorded in the Attendance mode.

Set Attendance and its modes in **Settings > Configuration > Attendance**, refer to Attendance Settings (p. 74).

CAUTION
Make sure that the user attendance monitoring license is active in **Access Commander** to monitor attendance properly. Remember to activate attendance monitoring for each user in the user settings.

The Attendance page provides a list of users whose attendance is to be monitored. There is an icon in the right-hand upper corner, which helps you download a CSV file including summary attendance data for all users. Specify the time interval for attendance data generation before download.

Specific User Attendance

Select a user from the user list on the Attendance page to display attendance details for this particular user. The list only shows the users for which attendance monitoring is allowed, refer to Users (p. 46).

Choose a month in the upper part of the list for which attendance should be displayed. In addition, the set working time for the given month, balance and worked hours are displayed.

There is an advanced menu next to the user name, which allows the given user's attendance data to be exported into a CSV/PDF file. Both the files include daily records.

TIP
User attendance can also be viewed in the user detail, which is selected in the user list on the **Users** page.

User Attendance Change

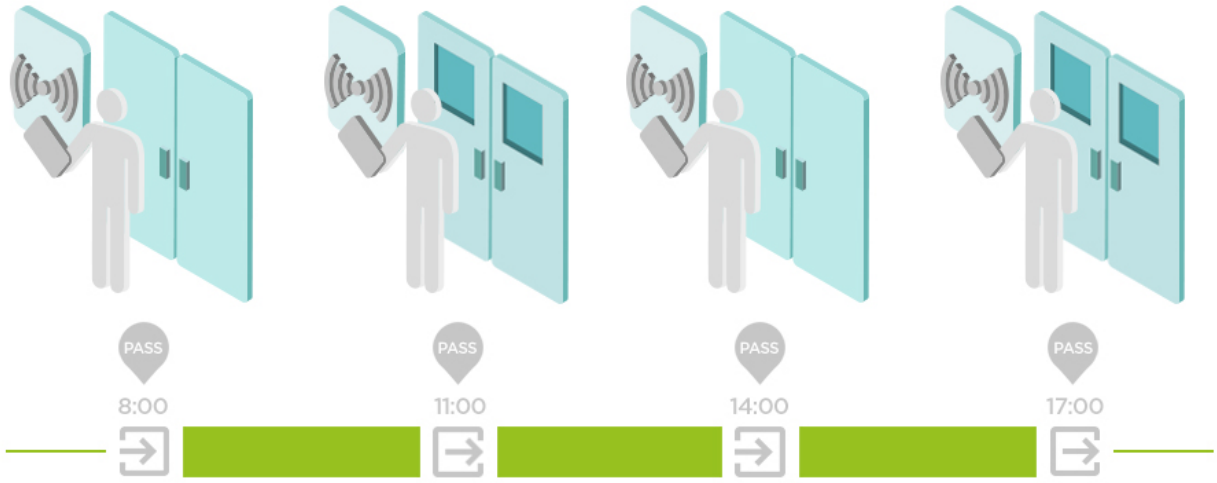
The attendance manager can edit the user attendance data. To do this, click the time interval to be changed. You can also edit the border times and add a note to an interval.

Attendance Settings

Access Commander helps you monitor user attendance. The user entry/exit times are recorded in the Attendance mode.

Attendance Modes

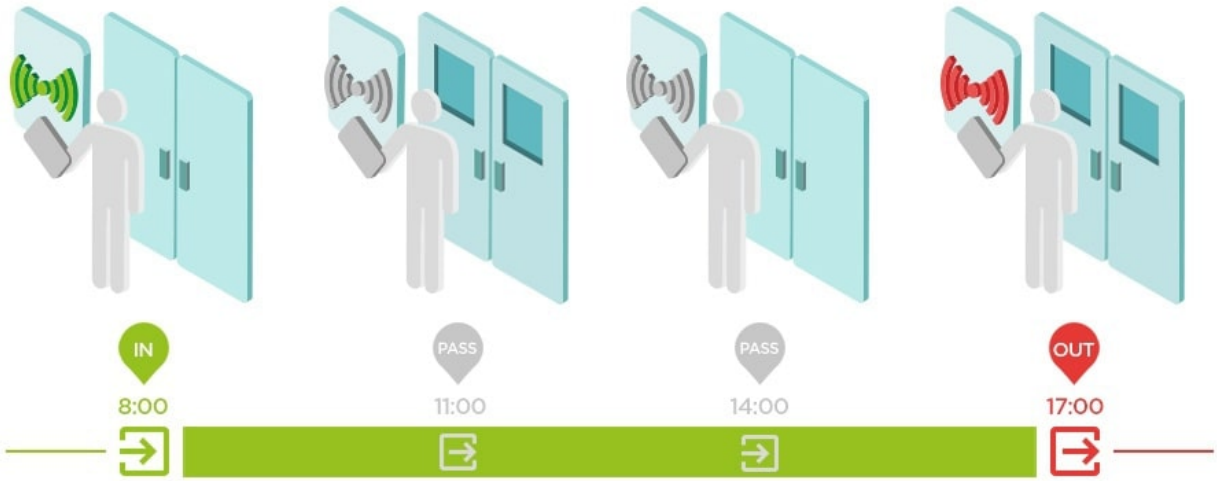
- **FREE**



Arrivals/departures are recorded by the first and last authentications of the user on any device in one day The Presence module is disabled in this mode.

- **IN-OUT**

Make sure that the device is set to enter and exit the area for a proper function.



- **IN-OUT for All Devices**
  This mode allows Presence to be monitored. Arrivals are recorded on the entry devices, departures are recorded on the exit devices. Movement across zones is not registered as arrival/departure.
- **IN-OUT for Selected Devices**
  This mode allows Presence to be monitored. Arrivals and departures are recorded on selected devices that are set as entry or exit. Arrivals and departures are only registered on these selected devices. Thus, arrival/departure recording can only be set for the main entrance of the building, for example.

Setting Device Access Points

You can logically divide each device into two access points - arrival and departure. Each access point represents a passage in one direction and determines whether the device user enters or leaves the zone. One access point can be controlled by one or more device modules. All the assigned modules then manage the passageways in the direction of the specific access point. The access points are used especially where a device is on the boundary of two zones and the direction of movement between them needs to be accurately recorded (for anti-passback, for example).

In addition, access points help monitor the users in the Presence (p. 80) module. Also, access points are used for monitoring entries/exits in Area restrictions (p. 82).

NOTE
The access points are referred to as **Arrival** and **Departure** in the web configuration interface of each device. Go to **Access > Access Rules > Entry and Exit tabs** to set them up.

Enabling Access Points in Access Commander

1. Go to Zones in **Access Commander**.
2. Press in the right-hand upper corner and enable the use of access points.

Module Assignment for Arrival or Departure

1. Enter the web configuration of the selected device.

TIP
Click in the list on the Devices page to enter the web configuration interface.

2. Go to **Access > Access Rules**.
3. Go to Zones in **Access Commander**.
4. A dialog box opens with a list of available access managing modules.
5. Drag and drop the modules into groups according to the direction they are supposed to provide.

TIP
Click to locate a specific module. The module triggers a visual or acoustic signal depending on its capabilities.

Visitors

In **Access Commander**, it is possible to create profiles for the visitors who are authorized to enter the facility for a limited period of time. A visitor can be assigned an access card and an access code and the visitor's vehicle license plate can be registered. Attendance is not calculated for a visitor. The visitor count is not limited by any license.

Visitor Data Retention Settings

The administrator can set the retention period for visitor data. The visitor data retention period is set in days by clicking the icon next to the visitor creating button.

When the visitor access time interval and the preset data retention period have expired, the visitors are automatically deleted at midnight every day. The visitors that are still assigned visitor cards are not deleted.

NOTE
The setting can be used for meeting the local data protection regulations. The visitor's name and note will be retained in the Access Log according to the lifetime setting in the log administration.

Visitor Creation

1. Go to the **Visitors** page.
2. Click the visitor adding button in the right-hand upper corner.
3. Complete the visitor's name, select the group to be visited and set the visit start/end in the open dialog box. If you do not complete the visit start and end times, the visitor access time interval starts immediately and ends at the end of the day.

   CAUTION
   The visitor access time interval may not be longer than 90 days.

4. Before creating a visitor, you can set the authentication methods for visitor access.
   The new visitor appears on the list. You can add authentication methods and manage visitor accesses in the visitor detail.

End of Visit

The visitor's access validity expires when the time interval elapses.

If the administrator terminates a visit by pressing the End now button in the visitor settings on the Accesses card, the visitor's access will be blocked immediately. The End button is available when a visitor's access has been terminated automatically due to possible different time zones on the devices. It is because the visitor may have an invalid access on one device but a valid access on another one. This happens when different time zones are set for different devices.

If a visitor was assigned a visitor card, the card will be released for another visitor.

Visitor Settings

View and edit the visitor information in the visitor detail. Click the selected visitor list item to open the visitor detail.

Access

The Access card shows the access group and time interval during which the visitor has a valid access. The visitor access time interval can be reset by selecting Renew visit in the extended menu ⋮.

A visit can be ended on this card, refer to End of Visit (p. 77).

Visitor

The card shows the person and the company to be visited. The person to be visited can be changed.

A note can be added to a visitor on this card.

Personal Information

The card shows the visitor's contact data and allows the data to be edited. The set e-mail allows authentication codes to be sent.

Credentials

A visitor can be assigned an access card and a PIN/QR access code and the visitor's vehicle license plate can be registered. Just one license plate can be added to one visitor. A visitor can be assigned a visitor access card, refer to Cards (p. 78).

It is possible to send the generated access PIN/QR code to an e-mail address if available.

The assigned visitor card can be returned here.

Access Log

The Access Log shows access history.

Cards

The Cards subpage helps you manage the visitor access cards that are available for assignment. Click the adding button in the right-hand upper corner to assign a card.

Remember to assign the cards to a company. A card can be only be used for the visitors accessing this company.

An existing card can be overwritten or deleted in the advanced menu ⋮.

CAUTION
A card assigned to an active visitor cannot be deleted.

NOTE
If **Access Commander** reports that the brand new card just added is already in use in the system, the reason may be that the RFID card compatibility mode is enabled. This mode is activated by the Administrator in **Settings > Authentication > Compatibility Mode Settings**.

Secure Card Management with USB Reader

The USB reader can be used for diagnosing and managing a secure card in the search box in the header.

TIP
Make sure to enable the USB reader in **Access Commander** before use. Refer to Enabled USB readers (p. 103) for more details.

1. Connect the USB reader to your PC.
2. Click the icon in the search box in the header.
3. Tap on the reader.

Available Operations

- Retrieving data from card
- User search by card
- Viewing events stored on card
- Access data update
- Application deletion or formatting
- Service card validity extension

Presence

The **Presence** module allows you to monitor user activity in real time. It works independently of the **Attendance** module, which is separately licensed. Presence can be monitored even without an active Attendance license.

The two features are displayed together on the **Attendance and Presence** tab in the Access Commander interface, but each has its own purpose and works independently.

Remember to set the Attendance IN-OUT mode in **Settings > Configuration > Attendance**, refer to Attendance Settings (p. 74), to make the module work.

- If Arrival (**IN** event) is the last event of the day, the user is considered present.
- If a user passes a reader with an unspecified direction, the current user zone will be changed. The same thing happens if a user passes through a reader in the **IN** mode.
- If Departure (**OUT** event) is the user's last event of the day, the user is considered absent.

CAUTION
The Presence module does not work correctly if the FREE attendance mode is selected. The only mode to be selected is IN-OUT.

User Presence Expiration

Click the icon in the right-hand upper part to set the User presence expiration. The User presence expiration sets automatic deletion of the user's presence record if the user fails to record the departure. This timeout is expressed in hours and defines the timeout after which the presence record is deleted automatically after the last passage of a present user. This timeout helps define how long a presence record can be kept in the system if the user is not considered absent. This ensures that the list of present users remains up-to-date and free of records on those who have left the building without checking out.

Reports

Summary data on added users can be downloaded from the Reports page. The downloads are in the CSV format (Comma-Separated Values). The file always includes the report generating date and time.

NOTE
Some spreadsheet programs use different separators and the CSV file may not be displayed correctly in them. In such cases, it is recommended that the CSV file data be imported into an open workbook.

- **My2N app** – Paired and unpaired users with pairing time remaining
  The report includes status data on user pairing via My2N app, or the pairing code validity data if necessary.
- **Users** – Access rules with groups, zones, devices and time profiles
  The report includes data on user assignments to groups, user accesses to zones and zone devices and time profiles for user accesses. Each and every combination is written on just one row of the table.
- **Users** – Detailed export
  The report includes all the user information that is completed in the user profiles, including the user personal and access data.

  CAUTION
  The file contains sensitive data!
- **Users** – Global synchronization export
  The report includes data on user assignments to groups, user accesses to zones and zone devices and time profiles for user accesses. Each and every combination is written on just one row of the table.
  This report can be used as a CSV file for user synchronization, refer to User Synchronization (p. 89).

  CAUTION
  The file contains sensitive data!

Area restrictions

Area Restrictions helps define the areas where the Occupancy and Anti-passback functions can be used.

NOTE
The Area Restrictions module and the Presence module (including Attendance) are independent of each other. The Occupancy and Anti-passback functions cannot be used for the Attendance and Presence modules. Occupancy and Anti-passback only work in the Area Restrictions model.

Area Restriction Settings

A new device is added to the area using the button in the area detail header.

Entry and Exit

These cards define which devices are entry and exit devices in the selected area. Use the advanced menu under ⋮ to move devices between the cards or remove them from the area.

By authenticating the user at the entry device, entry into the area is recorded. By authenticating the user at the exit device, the user leaves the area. With this, it is possible to monitor whether the user is still in the area and whether he wants to re-enter it.

If two access points have been set up for device added, each of them can be used for a different direction (In/Out). The access point settings are described in Subs. Setting Device Access Points (p. 75). Click the arrow to expand the access point properties.

Occupancy

Make sure that the device is set to enter and exit the area for a proper function.

The Occupancy card helps monitor and limit the count of persons in an area. When the Occupancy limit is reached, further access can be denied or any limit exceeding can only be recorded in the system log. A separate Presence module is used for monitoring the presence of individual persons.

CAUTION
Every authorization in repeated authorizations of one user is counted as one access. This means that if one user is read three times consecutively by the entry device, three persons will be recorded in the area. Hence, if the physical installation of a device allows for repeated reading of a single user card, it is recommended that the Occupancy module is combined with the anti-passback function.

Anti-Passback

Make sure that the device is set to enter and exit the area for a proper function.

It is possible to activate anti-passback for the areas to extend the access control to include monitoring and misuse of the right to re-enter the restricted areas. The areas to be monitored are defined by border devices,

which enable entry to or exit from the areas. Passing persons are checked for authorized access on these devices according to the area access rules defined. Having left an area through a border device, the user may not return to the area until the timeout, if defined, expires. If the user tries to return to the area earlier, the system will deny access or only record the event into the log.

WARNING

- The anti-passback area ceases to make sense and can be potentially dangerous if there is a device in the area equipped with an active REX button, which allows for an unauthorized access.

Exception Settings

Sometimes it is desirable that the Anti-passback conditions should not apply to selected users. Typically, these users include the building managers, CEOs, VIP users, etc. Set the users/groups exempted from the Anti-passback conditions in **Settings > Anti-Passback > Exceptions**.

NOTE
The Settings section is only available to the user with the administrator role.

List of Blocked Users

Blocked users are those who tried to access an anti-passback area before the end of the timeout. Use ✕ to exclude a user from the blocked user list to re-grant the user access to the area.

TIP
When denied access due to active Anti-passback, the user can be sent an automatic information e-mail. Enable this e-mail sending in **Setting > Anti-Passback > E-Mail Notification to Blocked User**.

Restriction Reset

Set the days and times in **Settings > Anti-Passback > Area Restriction Reset** on which the area records shall be deleted, i.e. all users will be able to pass regardless of their previous breach of the rules.

These measures increase the level of protection and prevent potential security threats. Specifically, they help prevent unauthorised access to selected locations, allow tracking of people's movements within a given area, and record entries and exits, which can be useful for monitoring and analysing security events.

The list shows the areas created in the system. You can create and delete areas and open their details on this folder. Also, you can deactivate an area and display its state.

Area Restriction Creation

1. Go to the **Area Restrictions** page.

2. Click the area adding button in the right-hand upper corner.
3. Name the area in the open dialog box.
4. Add a device to the area in the open area detail. Use the button in the area detail header to add a device.
   The new area appears on the list. You can define the entry/exit devices, set the allowed occupancy, enable Anti-passback and block area access for selected users in the area detail.

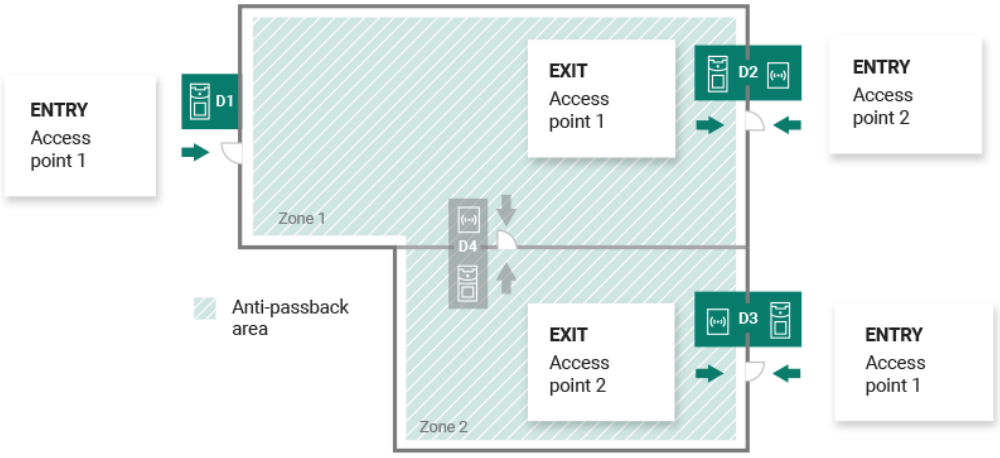
The most common setup errors

CAUTION
Should an error occur in an Anti-passback area, the whole area will be deactivated and reactivated once the error is removed.

The following cases may prevent the correct operation of area restrictions

- No device is added to the APB area. Assign one device at least.
- An entry/exit device has not been configured correctly or does not include a reader.
- An APB area entry device has been used for entry to another area. Modify the assignments to make the function work correctly.
- A device has not the proper license.
- A device has been deactivated.
- A device has been disconnected.
- A device has an incompatible firmware version.
  A device is equipped with the REX button that allows the user to leave the APB area without authorization. Deactivate the REX button to make the function work correctly.

Example of Restriction Setting



The figure shows one Anti-passback area with three border devices D1, D2 and D3. The only devices that can set the Anti-passback function are border devices. Device D4 inside the Anti-passback area is not used for area entry/exit control. Both the entry and exit directions are set for devices D2 and D3.

Device D1 is only used for entry to the Anti-passback area. The device is set as an entry device.

Device D2 is used both for entry and exit. The device has an extending module for entry and the set main unit for exit.

Device D3 is used both for entry and exit. The device has the set main unit for entry and an extending module for exit.

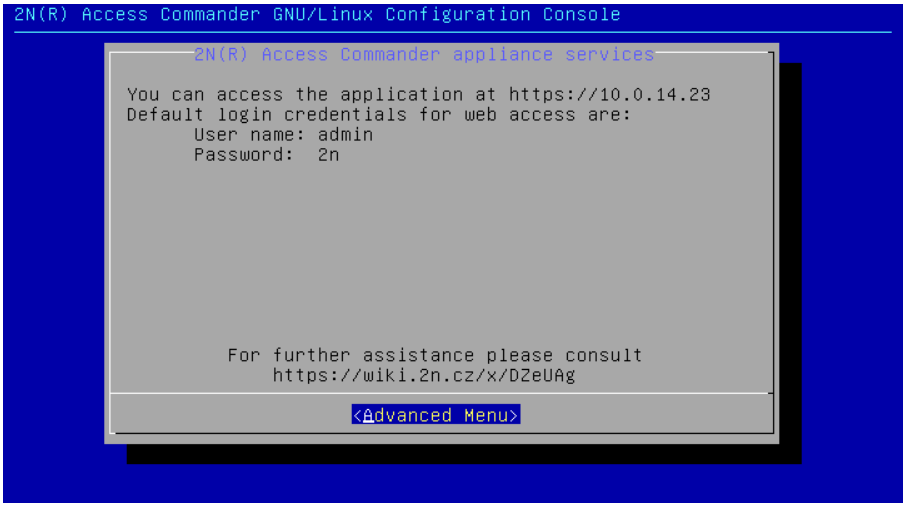
System Setup

Linux Settings

The basic system settings can be made via a Linux configuration console.

NOTE
If **Access Commander** is distributed via a virtual machine, it is possible to connect to the Linux version remotely through SSH connection.

The configuration console is opened by login to **Access Commander** using the root account. The introductory page shows basic information on the administrator access to the web interface and redirects to the Advanced Menu.



The following can be set in the Advanced Menu:

- **Networking**
  Set the Proxy server, network properties and DHCP server synchronization options.
- **Time**
  Set time manually, set the NTP server and time zone.

- **SSH**
  Set remote access to **Access Commander** via SSH. Make sure that the SSH enable password is different from the default one and meets the SSH requirements.
- **SMB**
  Enable the shared folder connection wizard. Set the IP address/domain name and path to the folder. E.g.: 192.168.1.1/share. Set the user name for folder access and right to write. Complete the user password and choose the Samba protocol version. Once all the mandatory parameters are set, the server connection is verified and the successful/wrong information is displayed.
- **Password**
  Change the system root user password for console login or access via SSH.

  NOTE
  The root user password is changed in the configuration console, not Access Commander.
- **Backup and Restore**
  You can import data and configuration, set repeated backup and restore from earlier backup.

System Update

Access Commander checks the update server and informs of available updates and new firmware versions for the connected devices on a regular basis. You can disable automatic update check in **Settings > System Update card**.

Access Commander Update Installation

WARNING
it is recommended that a system backup (p. 88) is made before updating. Perform the backup outside the working hours to avoid temporary system unavailability to the users.

1. Go to **Settings > System Update card**.
2. If Automatic update check is disabled, click Check for Updates.
3. Click Download in the update availability message and confirm the download.
   The card informs that update is ready for installation.
4. Click Install in the information message and confirm the installation in the open dialog box.
   Once the installation starts, you will be redirected to the Maintenance page. The Maintenance page informs the administrator who launched installation of the ongoing installation states. The other users get information that update is in progress. it is impossible to log in to **Access Commander** during installation.
5. When the installation is completed, click Go to login to get to the login page.

Required Domains for System Update

CAUTION
Connecting 2N Access Commander to the servers listed below is essential for a successful system upgrade. Without permission to access these domains, the update process fails and the system fails to update.

This approach is critical for downloading the latest application versions, system packages, security patches and other components that keep the system in optimal and secure condition.

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

Downgrade

No return to the previous firmware version is possible.

Beta Testing

The user can choose to join beta testing of the **Access Commander** software updates before the updates are issued officially. Enable this in **Settings > System Update card > Update Server parameter**.

WARNING
The test functions are not warranted and 2N TELEKOMUNIKACE a.s. shall not be held liable for any functionality limitations and potential damage incurred as a result of functionality limitations of the beta version. The beta versions are provided for testing purposes exclusively. The beta version is not meant for work with important data.

Once enabled, the beta versions will be displayed in available updates on the System Update card.

WARNING
After **Access Commander** is updated to the latest beta version, downgrade to the earlier version cannot be made.

System Backup

You can perform, set and check the **Access Commander** data backup and recovery in **Settings > System Backup card**. Data can be stored at the local storage or Server message Block (SMB). SMB is suitable for long-time backup retention.

Data backups can be performed one time or automatically in preset periodical intervals.

Every backup can be restored, downloaded or removed in a menu opened by clicking ⋮ at the backup list item.

One-Time Data Backup

1. Go to **Settings > System Backup card**.
2. Click Back Up Now in the bottom part of the card.
3. Select whether or not to use data encryption. If so, complete the password to be entered for backup restoration.

Automatic Data Backup Settings

1. Go to **Settings > System Backup card**.
2. Click at the Periodic Backup parameter.
3. Set the required backup parameters:
   - Frequency – periodic backup interval
   - Time – backup time
   - Day – day in a week/month for backup
4. Select whether or not to use data encryption. If so, complete the password to be entered for backup restoration.
5. Save the settings to make backups be performed automatically as set.

SMB Data Backup Settings

1. Go to **Settings > System Backup card**.
2. Click at the Storage parameter.
3. Choose the storage type: SMB.
4. Complete the server address, login data and protocol version.
5. Save the settings to make the backups be sent to the preset Server Message Block.

Backup Data Restore

1. Go to **Settings > System Backup card**.
2. Open the extended menu at the selected backup and select Restore.

Restore from Backup File

1. Go to **Settings > System Backup card**.
2. Click Restore from file in the bottom part of the card.
3. Select the backup file from your storage and click Restore.

Data Transfer from Other Access Commander

1. Go to **Settings > System Backup card**.
2. Click Migrate in the bottom part of the card.
3. Enter the **Access Commander** IP address from which the data will be transferred.
4. Complete the administrator account login data of the **Access Commander** from which the data will be transferred.

CAUTION
Make sure that the SSH service is enabled on the **Access Commander** from which the data will be transferred in order to import the data successfully.

User Synchronization

The user list including the basic user settings and company/group assignments can be synchronized using an externally kept CSV file.

Synchronize in **Settings > User Synchronization**. Download a CSV template from the card (in advanced menu).

TIP
Download the current user list matching the CSV template structure at Reports (p. 81).

The prepared CSV file can be imported directly on the card. The file data will start synchronizing automatically with **Access Commander**.

Refer to the system log for detailed information on each synchronization result. The log informs whether or not the synchronization was successful. Click the icon at the end of the row to download a detailed information file.

Automatic User Synchronization with FTP

User Synchronization in Settings helps you interconnect **Access Commander** with the FTP storage where the user list CSV file is stored. The card then shows information on this FTP storage.

1. Go to **Settings > User sync**.
2. Click in the Storage parameter.
3. Set the FTP server address on which the CSV file is stored in the open dialog box.
4. By enabling TLS you activate Transport Layer Security (TLS) for your FTP connection. TLS will encrypt the data transferred between **Access Commander** and the server.
   By enabling TLS Certificate Authentication you activate authentication of the TLS certificates provided by the server. When this option is enabled, **Access Commander** verifies that it is communicating with a trusted server, thus increasing the connection security.

   CAUTION
   Proxy for FTP with TLS authentication is not supported.
5. Enter the FTP server login data.

CSV file

NOTE
Some spreadsheet programs use different separators and the CSV file may not be displayed correctly in them. In such cases, it is recommended that the CSV file data be imported into an open workbook.

Always keep the CSV file structure. All the values are separated with a comma, the group list is separated with a semicolon. The CSV file structure is as follows:

- EmployeeID – primary key to be fulfilled every time. It is a unique user identifier.
- User Name – name of the user created in **Access Commander**.
- Company – name of the company to which the user is assigned. Make sure that the company has been created in **Access Commander.** The small and capital letters used in the company/group names are not interchangeable.
- User Mail – user e-mail address.
- Card Numbers – user card ID. Up to two cards can be set per user. The card IDs must be separated with a semicolon (;).

- Switch Code – switch code; the code is always set for switch 1.
- Phone Number 1 – phone number for position 1.
- Group Call – group call to the above completed phone. The values are True/False. If True is selected, the group call is enabled. If False is selected, the group call is disabled.
- Phone Number 2 – phone number for position 2.
- Group Call – group call to the above completed phone. The values are True/False. If True is selected, the group call is enabled. If False is selected, the group call is disabled.
- Phone Number 3 – phone number for position 3.
- Virtual Number – user virtual number.
- Groups – list of the groups to which the user is to be assigned. Make sure all the groups have been created in **Access Commander**. The group list is separated with a semicolon. The small and capital letters used in the company/group names are not interchangeable.
- Is Deleted – user should/should not be deleted. If FALSE is selected, the user is created and its data will only be updated at the next synchronization. If TRUE is selected, the user is deleted at the next synchronization. If FALSE is selected, the user is recreated.
- License Plates – license plates. Multiple license plates can be set, separated with a semicolon.

Date and Time

Change the date/time retrieval method in **Settings > Configuration > Server date and Time**.

Date and time can be synchronized with the Internet or set manually in **Access Commander**. In case **Access Commander** is disconnected from the Internet, set the date, time and time zone manually. If connected, switch to NTP and get time from the NTP server. In that case, set the time zone only. The NTP server updates date and time automatically.

CAUTION
Once the time change is saved, **Access Commander** restarts automatically.

Time Synchronization with Devices

It is possible to synchronize the device time values with the **Access Commander** time. Enable the Device time synchronisation parameter in **Settings > Configuration > Server date and time card** to share time with the devices.

When time synchronization with devices is on, choose one of the following synchronization methods:

- **Devices Use Same NTP Server** – the device time obeys the NTP server set in **Access Commander**.

  TIP
  The NTP server time provides then highest time accuracy to the device.

- **Devices Use Access Commander as NTP Server** – the device time synchronizes with the **Access Commander** time.

Automation

The Automation feature is available in **2N Access Commander** from firmware version 3.2 under the Advanced, Pro, and Unlimited licenses. Built on the Node-RED platform, this addition directly offers extensive flow-based programming capabilities to **Access Commander**. It allows users to connect **Access Commander** with various third-party systems and automate custom workflows based on events within the platform.

CAUTION
To fully utilize this versatile automation tool, it is necessary to bear in mind the following:

- **Customer Responsibility for Security**: Users are responsible for ensuring that their Automation configurations and workflows are secure and in line with cybersecurity best practices. This includes securing the Node-RED environment, managing permissions appropriately, and safeguarding sensitive data within their automations.
- **Use of the REST API node**: If not used properly, this node may lead to data loss or unintended modifications. It is the user's responsibility to ensure that the node is configured and implemented correctly. Please exercise caution and double-check your settings to avoid potential risks to your data.
- **Third-Party Nodes and Add-ons**: 2N Telekomunikace is not responsible for the use or integration of any third-party nodes, add-ons, or custom modifications to Node-RED within the Automation feature. Customers should carefully evaluate and ensure the security and stability of any additional components they choose to install. Any issues arising from third-party extensions will need to be resolved by the customer or the respective third-party provider.
- **Technical Support Limitations**: While our support team will assist with issues related to the basic functionality of the Automation feature within 2N Access Commander, including our custom Access Commander nodes, they will not be able to provide assistance with the design, development, or debugging of custom Node-RED flows. The users who wish to create complex automations may need to seek additional support from qualified Node-RED experts or consult available resources.

To get started with Node-RED, it is advisable to explore available online resources, such as detailed manuals and numerous YouTube tutorials on Node-RED, which provide guidance on creating and managing the flows.

For more information about custom **Access Commander** nodes and using the Automation feature within **Access Commander**, please refer to this manual.

This feature enhances the capabilities of **Access Commander**. Exploring its potential while ensuring the security of configurations is recommended.

Creating Automations

Automated tasks are created in an external editor. Access the editor from **Settings > Configuration > Automation**. Changes made in the editor will not take effect until deployed to the server, which is done by clicking the Deploy button in the right-hand upper corner of the editor.

The creation of automated tasks is based on the compilation of flows. The flows are formed from nodes tied to each other. The node menu is displayed in the left panel. You can search for nodes by name in the left panel. You can also add a new node after creating a new connection from an existing node.

The data transferred between the nodes is referred to as messages. Refer to here for the message details. This page also describes the basic nodes that handle the message formats or sequences such as the Change, Split, Join... nodes. Automations can work not only with the data obtained in this unique task (msg.), but also with dynamic values in the context of the entire flow history (flow.) or even all the flows in the installation (global.).

CAUTION
The Deploy button sends the set flows to the server. The new flows will not become effective until sent to the server!

Safe mode

The Safe Mode is a key automation troubleshooting tool. Running the editor in the safe mode allows you to make flow changes without the flows running on the background. This means that you can go to the editor, edit what you need and then deploy the changes using the Deploy button. This mode is especially useful if any of the flows causes Node-RED to malfunction or fail, due to an error in the flow or a third-party node, for example, or if the flow needs to be stopped immediately.

Access Commander Nodes

REST API

The REST API node sends a defined HTTP API request. The input data contained in **Body** is used as the request body for this request. The node output includes data from the response to the request. You can specify the selection and arrangement of output data in the **Query** parameter.

Node Parameters

- **Method** – offers a choice of API request methods.
- **Endpoint** – specifies the entire endpoint to which the request will be directed. The endpoint path can be completed with the Body parameter.
  Working with HTTP requests is described in HTTP API (p. 113).
- **Query** – specifies which data parameters should be addressed in the endpoint and how they should be returned in the output. This parameter can be specified by the input value, in **Query**. Refer to Data Query Customization (in English only) for the **Query** building details.
- **Only send non-2xx responses to Catch node** – affects the kind of the HTTP responses to be captured in the Catch node.
- **Name** – allows you to rename a node for better orientation when working with the flow.

Access Log

The node loads records in the Access Log and allows you to process those records further.

The Administrator can set up automated tasks that start when **Access Commader** records a defined log entry. The action is defined in the node settings. The output includes specific data on the recorded event. The SignalR-based functionality runs on the background of this function.

Node Parameters

- **Filter** – specifies the records to be processed by the node. Records not matching this filter will be ignored by the flow. The filter format is a JSON object. This parameter can be overwritten by an input value.
- **Name** – allows you to rename a node for better orientation when working with the flow.

System Log

The node loads records in the System Log and allows you to process those records further.

The Administrator can set up automated tasks that start when **Access Commader** records a defined log entry. The action is defined in the node settings. The output includes specific data on the recorded event. The SignalR-based functionality runs on the background of this function.

Node Parameters

- **Filter** – specifies the records to be processed by the node. Records not matching this filter will be ignored by the flow. The filter format is a JSON object. This parameter can be overwritten by an input value.
- **Name** – allows you to rename a node for better orientation when working with the flow.

SignalR

The SignalR node reads data in the sampled topic. Obtaining data in real time, the node is suitable for scenarios where the automated task is to extract information from Access Commander without constant querying.

Node Parameters

- **Topic** – offers available topics for subscription.
- **Filter** – specifies the records to be processed by the node. Records not matching this filter will be ignored by the flow. The filter format is a JSON object. This parameter can be overwritten by an input value.
- **Name** – allows you to rename a node for better orientation when working with the flow.

Refer to Subs. SignalR (p. 113) for more SignalR functionality details.

Dynamic SignalR

Compared to SignalR, the Dynamic SignalR node allows for dynamic changes in data sampling. This may include changing the topic or sampling method based on the input values. The node output values include data obtained from the topics (Data) and information about the successful/unsuccessful execution of the node action.

Node Parameters

- **Topic** – defines the topic for which the data acquisition is to be changed.
- **Filter** – specifies the records to be processed by the node. Records not matching this filter will be ignored by the flow. The filter format is a JSON object. This parameter can be overwritten by an input value.
- **Records** – define the number of records to be loaded when you use the fetch read type.
- **Fetch When Ready** – set whether the values should be retrieved backwards when the fetch command is activated.
- **Name** – allows you to rename a node for better orientation when working with the flow.

Valid Input Values

The node accepts the following properties as input values. The valid input values temporarily override the parameters set in the node configuration.

- **topic** – a string that specifies the topic to be subscribed.
- **filter**– chain in the JSON format, which specifies the retrieved records.
- **fetchWhenReady** – bootlean specifying the Fetch When Ready node parameter.
- **action** – a string that specifies the action to be performed. It can be subscribe to subscribe, unsubscribe...
- **update** – may contain a timestamp (string) and a timeWindow (object) indicating when the action to be changed took place.

Refer to Subs. SignalR (p. 113) for more SignalR functionality details.

Write system log

The Write system log node creates a record in the Access Commander system log. The log entry contains the specified severity, event description and other details. If an error occurs during the process, it is recorded and the node status is updated accordingly. The node has no output values.

Node Parameters

- **Severity** – determines the severity of the record. This parameter can be specified by the query input value.
- **Filter** – specifies the records to be processed by the node. Records not matching this filter will be ignored by the flow. The filter format is a JSON object. This parameter can be overwritten by an input value.
- **Detail** – provides a more detailed description of the record that appears in the System log. This parameter can be overwritten by an input value.
- **Name** – allows you to rename a node for better orientation when working with the flow.

Valid Input Values

The node accepts the following properties as input values. The valid input values temporarily override the parameters set in the node configuration.

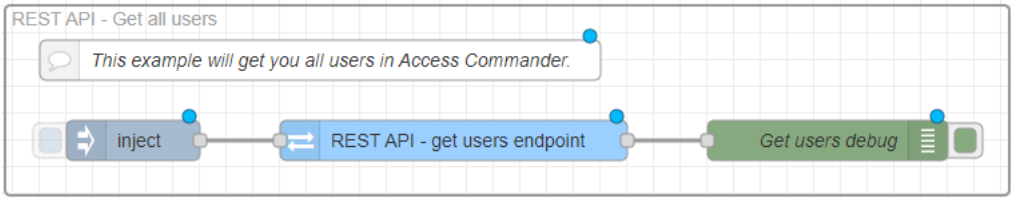
- **severity** – the string that determines the severity of the record.

- **event** – a string that briefly describes the recorded action.
- **detail** – a chain that fills the detailed description of the record that appears in the System log.

Examples of Flows

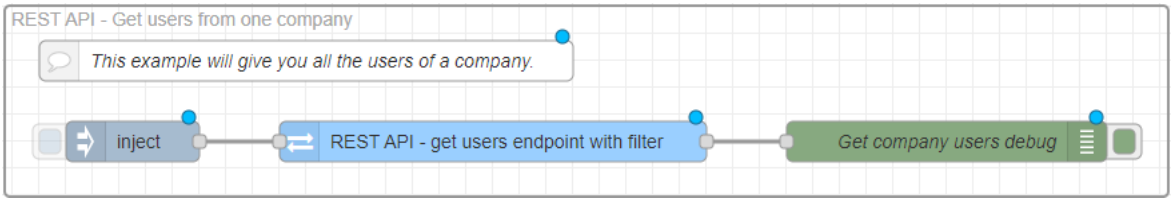
Access Commander offers several basic automated tasks that represent the possibilities of using automations. The flows of these tasks can be installed when you first run Automation in **Access Commander**, but you can import them later, see Flow Export/Import (p. 97). These pre-installed flows can simply be modified for your own purposes.

Get all users



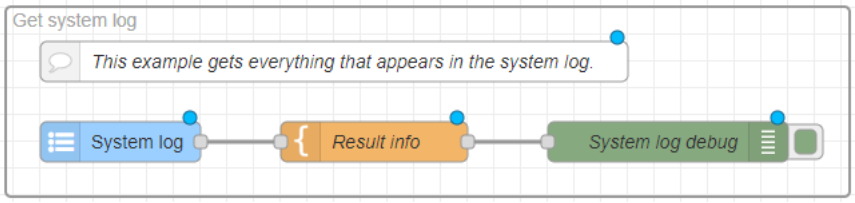
This flow generates a list of all users, including user information. The task is initiated by the Inject node activation. You can apply a filter in the **REST API – get users endpoint** node to specify the users to be returned by the process. In this way, you can make the process output meet the administrator's needs.

Get users from one company



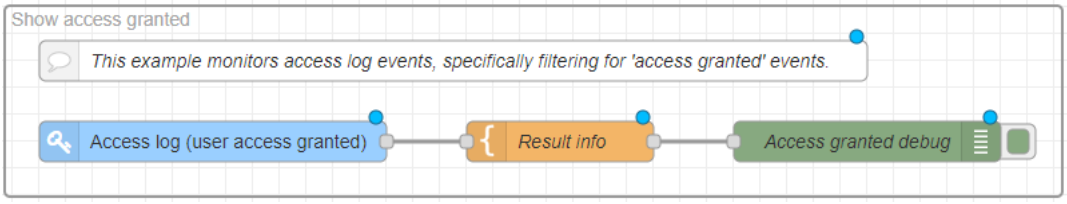
This flow generates a list of all users within one company, including user information. The task is initiated by the Inject node activation. Set the company selection in the **REST API – get users endpoint with filter** by entering the company ID.

Get system log



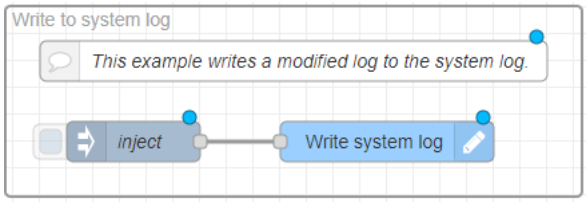
This flow loads all the new entries in the System log. You can specify a filter in the **System log** to make the event selection more precise.

Show access granted



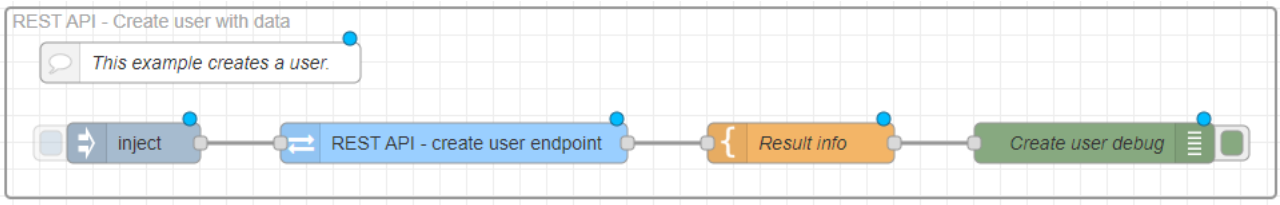
This flow loads all the new records in the Access log. The flow is set to load granted access only. You can change this restriction in the **Access log** node.

Write to system log



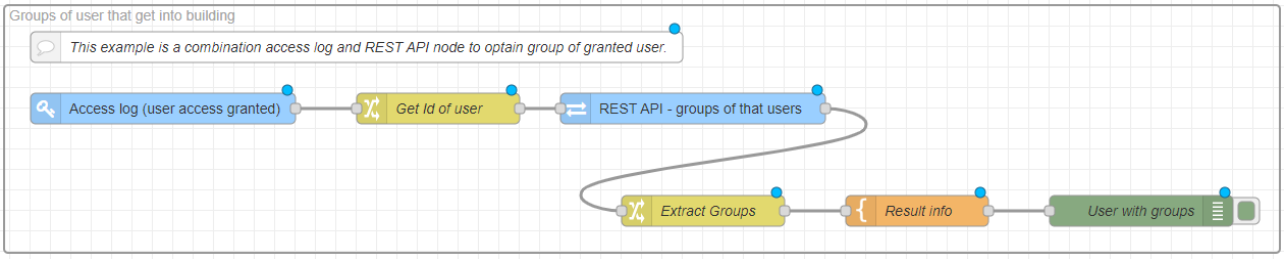
This flow creates a record in the System log. You can set the record Severity, Name and detailed Description in the **Write System log** node.

Create user with data



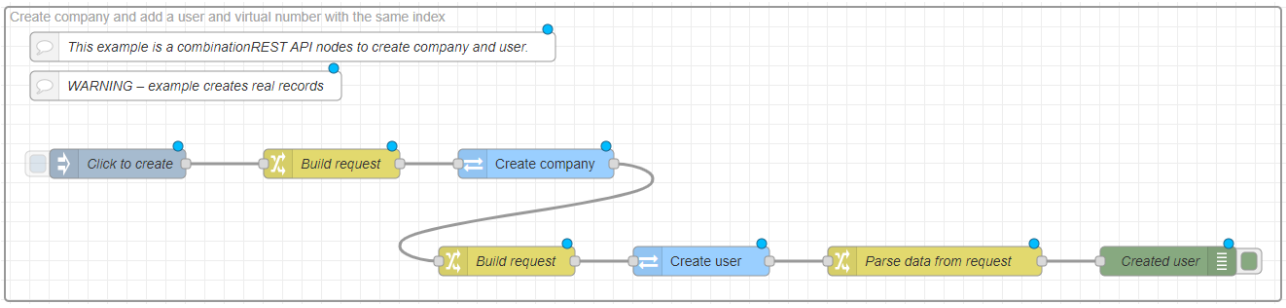
Use this flow to create a new user. The task is initiated by the **Inject** node activation. The **Inject** node contains a message body that specifies the username Joe Doe and its inclusion in the company with ID 1. This body is applied in the **REST API - create user endpoint** node and the user is created on this basis. The **Result info** node sets the message text to appear in the Debug messages.

Groups of users that get into building



This flow loads the user groups that have been granted access. Permitted accesses are loaded from the Access log. Subsequently, the flow obtains the ID of the user with the granted access and uses the **REST API node - groups of those users** node to retrieve data about this user. The **Extract Groups** node retrieves the group names for this user and the **Result info** node compiles the text of the final message.

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



This flow creates a new company, the first user in the company and its virtual number. The task is initiated by the **Inject** node activation. When initiating, a random integer is generated to be used in the company name and the user name and serve as the user virtual number. The **Create company** node creates a company with the defined name. From the response of this node, a company ID is obtained, on the basis of which the following **Create user** node creates a new user in this company and simultaneously assigns the user a

virtual number. The **Parse data from request** node then retrieves the company name, the user name and the user virtual number.

Flow Export/Import

Flows can be exported to .json files and later re-imported into the Automation interface. Export and import is performed in the extended menu in the right-hand upper corner. Flows moved from one **Access Commander** installation to another may require editing.

There are preloaded example flows for **Access Commander** in the import options. They are located on the Examples tab, in the Access-Commander-nodes folder.

CAUTION
The advanced settings that are not supported by the new license are not saved.

Therefore, remember to export the set flows after the your Trial license is terminated.

Error States

When working with automations, errors may occasionally occur that affect their stability and functionality. When an error occurs, the Automation tab in **Access Commander** notifies you of this condition and offers you to restart the Node-RED platform in the safe mode. The safe mode temporarily halts the flows and allows for a safe repair of the flows that induce the error state. Click the Deploy button to restart the flows.

There are two basic error states:

- **Node-RED is not responding**
  This situation occurs when Node-RED stops responding. No automations are in progress. This problem can be caused by various factors, such as system overload, errors in flow settings or conflicts between the imported third-party modules.
- **Node-RED is unstable**
  The Node-RED instability manifests itself by a repeated restarting of the platform, which can disrupt automation operations and cause data loss. As a rule, repeated restarts usually occur if one of the flows is misconfigured and triggers restart. During the restart, the course of all the flows is suspended.

Installation Name

The name of the particular **Access Commander** installation is displayed in the web interface header to all the logged in users. You can change the default **Access Commander** name, e.g. to the address of the building that the particular installation manages.

Change the name in **Settings > Configuration > Installation Name**. By changing the name, you can distinguish multiple installations if managed by one person. The installation name is also written into the e-mails sent to the companies.

E-Mail (SMTP) Enable and Setting

The E-mail function helps you send notifications or access passwords to users. E-mails are sent using the SMTP.

1. Set the function in **Settings > Configuration > E-Mail card**.

2. When the E-mail function is switched on, a dialog box will open for you to set the following parameters:
   - **SMTP Server Address**, to which e-mails shall be sent.
   - **Server Port**, preset to 25.
   - **Username** and **Password** to the SMTP server account in case the SMTP server requires authorization.
   - **Default Sender Address**, from which e-mails shall be sent.
3. Switch on if necessary:
   - **SSL** for e-mail encryption;
   - **SSL Server Certificate verification**;
   - **Legacy Mode** in the case of connection to older SMTP servers that do not support new functions (GSSAPI).
4. After saving, you can set **Base address for e-mail links**, which will be part of the sent e-mails and refer to a selected part of the **Access Commander** interface, on the E-Mail card.
5. Send a test e-mail to check the settings.

Two-Factor Authentication

Two-factor authentication provides a higher level of security for the **Access Commander** user account. To log in, the user enters the login data and has to confirm the login using an authentication application. Once the administrator turns on two-factor authentication, the user will be prompted to interconnect the user account with an authentication application of their own in the next login.

Access Commander does not require that you re-verify your identity whenever you log in or perform protected actions. Once you complete the authentication, the system remembers you for a limited time:

- 7 days for normal logins
- 5 minutes for actions considered security critical, such as changing API keys, updating your own password or modifying the root password.

The system can remember up to two authenticated devices. If you authenticate from a new device, the oldest remembered device is removed. If you try to perform a security-critical action outside the allowed time window, the system will simply ask you to authenticate again before you can proceed.

1. The administrator sets two-factor authentication in **Settings > Configuration > Two-factor authentication**.
2. The administrator can choose which users will be requested to use two-factor authentication.
   Two-factor authentication request options
   - **Optional**
     Two-factor authentication is voluntary. Users can enable two-factor authentication in their profiles.
   - **Mandatory for user with a role**
     Every user that has been assigned a role has to verify the login using an authentication application.
   - **Mandatory**
     All users must verify their logins using an authentication application.

Two-Factor Authentication Enable

If the administrator sets optional two-factor authentication, you enable two-factor authentication yourself as follows:

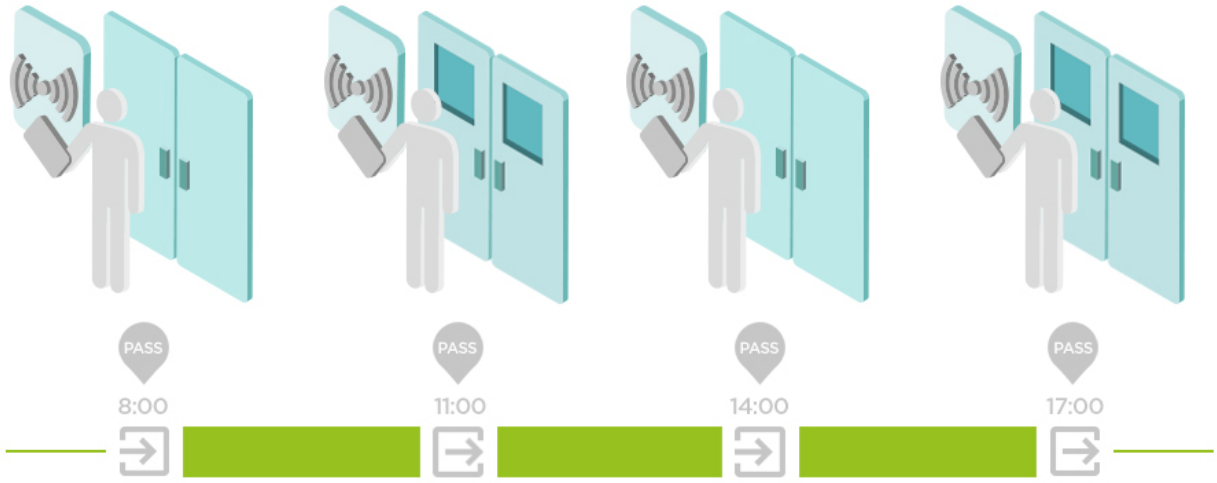
1. Click the user image in the right-hand upper corner to open the user menu.
2. Use the Authentication Applications tab to link your account to the selected authentication application. Follow the instructions in **Access Commander**.
3. Select View profile.

Attendance Settings

Access Commander helps you monitor user attendance. The user entry/exit times are recorded in the Attendance mode.

Attendance Modes

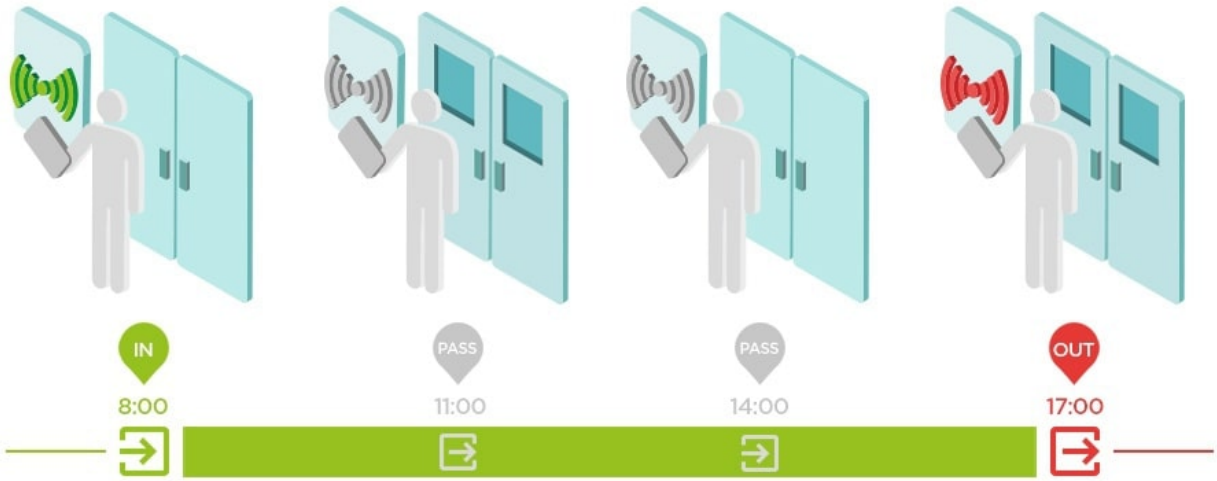
- **FREE**



Arrivals/departures are recorded by the first and last authentications of the user on any device in one day The Presence module is disabled in this mode.

- **IN-OUT**

Make sure that the device is set to enter and exit the area for a proper function.



- **IN-OUT for All Devices**
  This mode allows Presence to be monitored. Arrivals are recorded on the entry devices, departures are recorded on the exit devices. Movement across zones is not registered as arrival/departure.
- **IN-OUT for Selected Devices**
  This mode allows Presence to be monitored. Arrivals and departures are recorded on selected devices that are set as entry or exit. Arrivals and departures are only registered on these selected devices. Thus, arrival/departure recording can only be set for the main entrance of the building, for example.

Setting Device Access Points

You can logically divide each device into two access points - arrival and departure. Each access point represents a passage in one direction and determines whether the device user enters or leaves the zone. One access point can be controlled by one or more device modules. All the assigned modules then manage the passageways in the direction of the specific access point. The access points are used especially where a device is on the boundary of two zones and the direction of movement between them needs to be accurately recorded (for anti-passback, for example).

In addition, access points help monitor the users in the Presence (p. 80) module. Also, access points are used for monitoring entries/exits in Area restrictions (p. 82).

NOTE
The access points are referred to as **Arrival** and **Departure** in the web configuration interface of each device. Go to **Access > Access Rules > Entry and Exit tabs** to set them up.

Enabling Access Points in Access Commander

1. Go to Zones in **Access Commander**.
2. Press in the right-hand upper corner and enable the use of access points.

Module Assignment for Arrival or Departure

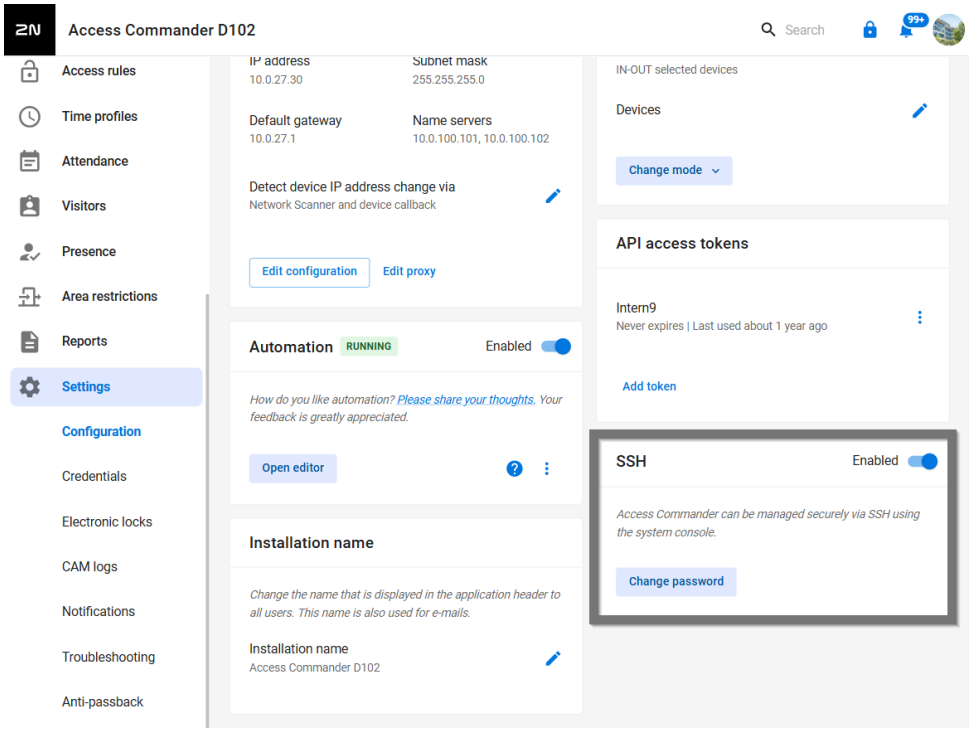
1. Enter the web configuration of the selected device.

   TIP
   Click in the list on the Devices page to enter the web configuration interface.

2. Go to **Access > Access Rules**.
3. Go to Zones in **Access Commander**.
4. A dialog box opens with a list of available access managing modules.
5. Drag and drop the modules into groups according to the direction they are supposed to provide.

   TIP
   Click to locate a specific module. The module triggers a visual or acoustic signal depending on its capabilities.

SSH Access Enable



WARNING
SSH access enable is recommended to experienced users only. Any improper use represents a security risk.

Settings > Configuration > SSH card is used for Secure Shell enable, which provides secure remote communication with the system console. The enabled SSH service provides backup and restore of the system or full restart of **Access Commander**.

The SSH client needs to know the **Access Commander** IP address and root user password to connect to the Access Commander Box or virtual machine. The system root user password can be set in **Settings > Configuration > SSH card**.

NOTE
The root user password is changed in the configuration console, not Access Commander.

The SSH access can also be enabled and managed directly in the Linux configuration console, refer to Linux Settings (p. 86).

Encryption keys for My2N app

Users can use the My2N application to connect to 2N devices. Communication between the My2N application and the device is always encrypted. **Access Commander** automatically manages the system pairing keys that are distributed on a WaveKey supporting device and ensure secure trusted pairing. The My2N application cannot authenticate a user without knowing the encryption key. The primary encryption key

is automatically generated either upon the intercom first launch or as part of the intercom configuration in case of **Access Commander** administration. The key can be re-generated manually any time. Together with Auth ID, the primary encryption key is transmitted to the mobile device for pairing.

NOTE
Two key types are used in the system: **pairing keys** and **access keys**. The pairing keys help authenticate the My2N application with the device. The access keys define permissions to functions within a mobile application.

Creating New Keys

1. Go to **Settings > Authentication > Encryption keys for My2N**.
   Up to 4 access keys can be generated. When you attempt to generate the fifth key, **Access Commander** will warn you that the oldest key will be removed. The card shows the generation time for each key.
2. Click Generate New Key.

   TIP
   It is recommended that the pairing keys are re-generated once in a longer period of time (once a year, e.g.) for security reasons.
3. The generated key is automatically uploaded into My2N upon the first use of the mobile phone with the device paired earlier.

The generated key can be deleted by clicking .

TIP
Pairing using a **QR code** containing a public key is recommended for higher security. If no QR code is available, you can use **PIN** pairing.

CAUTION
QR code pairing is only supported for devices with HIP firmware 2.50.0 and higher (including the 3.0 series). **The QR code** may be displayed in an environment with Access Commander, but pairing on older HIP versions will only be successful if the **PIN** is used.

NOTE

- If the My2N application has no access to any of the valid encryption keys, it cannot be used for user authentication. To restore the application functionality, it will be necessary to re-pair the application with the device connected to Access Commander and thus upload the valid encryption keys to the My2N application.
- The access to the device depends on the access rights of the given user.

RFID Card Compatibility Mode

If **Access Commander** reports that the brand new card just added is already in use in the system, the reason may be that the RFID card compatibility mode is enabled. This mode is activated by the Administrator in **Settings > Authentication > Compatibility Mode Settings**.

CAUTION

- The compatibility mode should only be activated if there are problems with loading previously registered cards. The use of the compatibility mode can affect the authentication mechanisms.
- The compatibility mode should not be combined with the use of the PICard secured cards.

PICard Keys

The encryption keys for 2N PICard Commander are saved in **Settings > Credentials > PICard Keys card**. If the encryption keys have been uploaded to **Access Commander**, the PICard Commander project name and key export numeric ID are displayed on the card. The card allows the encryption keys uploaded to **Access Commander** to be deleted.

CAUTION
With PICard keys removed, all the cards encrypted using these keys will cease to work.

PICard Encryption Key Import

1. Go to **Settings > Accesses > PICard keys**.
2. Click Import to upload the file with encryption keys from your storage.
3. Enter the file protection password if set during export from PICard Commander.

PICard Commander is a software application used for the encryption of login data on access cards. The application creates projects that generate a set of encryption and reading keys. The reading keys can be imported to 2N devices or **Access Commander** for distribution to the connected 2N devices.

Enabled USB readers

USB readers connected to the PC used for access to **Access Commander** can facilitate uploading of some user authentication methods. Remember to enable the readers in **Settings > Credentials > Enabled USB readers** in **Access Commander**.

1. Go to **Settings > Accesses > Enabled USB readers.**
2. Click Enable Readers to open a dialog box.
3. Enable/disable the use of an external USB device in the open dialog box.
4. Subsequently, click Change to modify the reader enable.

Access Commander enables you to use the following USB devices:

- 125 kHz RFID card reader – Part No. 9137420E, AXIS Part No. 01399-001
- 13.56 MHz and 125 kHz RFID card reader – Part No. 9137421E, AXIS Part No. 01400-001
- Fingerprint Reader– Part No. 9137423E, AXIS Part No. 01401-001

CAM Logs

CAM logs are used for automatic recording of several images preceding and following a selected event. You can manage various types of events in **Settings > CAM Logs** for which CAM logs are to be generated.

CAM logs can, for example, be generated whenever a card is swiped. Thus, 5 snapshots before the card swipe and 3 snapshots after the card swipe will be recorded in the access logs. The images are taken in 1-second intervals. A storage of the size of 1, 3 or 5 GB has been created for the snapshots. When the storage is full, the oldest snapshots are deleted. The access logs are not deleted.

CAM Log Type Creation

1. Go to **Settings > CAM logs**.
2. Click the adding button in the right-hand upper corner of the page.
3. Enter the CAM log event type name.
   The new CAM log event type appears on the list and its detail opens in the CAM log. Set the events and devices for which the camera images shall be generated in the CAM log detail.

CAM Log Settings

You can administer information on the CAM log type in the CAM log detail. Click the selected CAM log list item to open the CAM log detail or the detail opens whenever a new CAM log is created.

Monitored Events

The card helps you select a list of events during which camera images shall be captured.

The monitored events can be as follows:

- **Accesses**
  - User accepted
  - Vehicle license plate recognized
  - User denied
  - REX button pressed
- **Security**
  - Tamper switch activated
  - Unauthorized door opening
  - Remote door opening
  - Access denied – repeated wrong entry
  - Silent Alarm activated
- **Calling**
  - Call Initiated

Monitored Devices

It is recommended that CAM logs are only recorded from a device equipped with a camera. Select a device in a dialog box opened using . At the same time, the card allows the CAM log recording from all devices to be enabled.

Electronic Locks

The **Access Commander** system provides access control via the 2N Fortis electronic locks, which are unlocked by the MIFARE ® DESFire® RFID cards. Each electronic lock is assigned an encryption key during configuration. The lock keys are then stored on the RFID cards of the authorized users. If the keys match on the card and in the lock, the locking mechanism is unlocked.

One RFID access card can be used for access to up to 90 doors with the 2N Fortis locks, depending on the number of the time profiles applied. If the card memory capacity is exceeded, data writing to the card will fail. The write failure event is recorded in the system Access Log. If Lock Groups are used, more doors can be written to a single card than the case is with individual assignment.

Fortis Commander

Fortis Commander is a standalone application that interconnects the **Fortis** electronic locks with the **Access Commander** system. The application sets the locks according to the project file created in **Access Commander**, which contains the lock configuration. The file is encrypted and can only be used for one specific installation.

Installation

Fortis Commander is designed to be installed on a Windows computer with Bluetooth Low Energy (BLE) support.

The app can be found at 2N Download Centre.

Installation Procedure

1. Download the installation package from the link provided.
2. Run the installer and complete the installation by following the on-screen instructions.

Project File

The project file is created in **Access Commander** and contains the complete project configuration. The file is encrypted and password protected.

Lock Settings in Access Commander

Before uploading keys to individual locks, you must pair **Access Commander** with **Fortis Commander**.

Master Encryption Key (MEK) Generation and Project Preparation

1. Log in to Access Commander.
2. Go to **Settings > Electronic locks**.
3. Click Generate Keys in **Initial Settings**.
4. Create the master encryption key.

CAUTION
The master encryption key cannot be **displayed or changed** later.

NOTE
According to the master encryption key (MEK), **2N Access Commander** generates a set of encryption keys. Thus, the key should be unique and sufficiently secure. As the key set is based on the master encryption key, projects with one and the same master encryption keys generate the same sets of keys. If a project is lost, you can create a new project with the same master encryption key and continue encryption.

5. Having generated the keys and set the password for the project file, you can download the **project file**, which represents an image of the electronic lock configuration in the **Access Commander** system.

6. On the **Fortis Commander** tab, click Download Application, to download the **Fortis Commander** electronic lock configuring application.

CAUTION
Project information is sensitive data. Protect it from abuse.

Propagation of Electronic Lock Configuration via Fortis Commander

1. Install and open the **Fortis Commander** application.
2. Click Open Project to open the downloaded project file in the File Explorer.
3. In the open dialog box, enter the project file password.
4. After opening the project file, select Connect to Device and tap the service card on the lock.
5. Click **Assign** to assign the lock to the project.
6. Disconnect the device and click **File > Close project**.
7. When the configuration is complete, open **Access Commander**. Go to the **Settings > Electronic Locks** and click the Fortis Commander button again. Upload the project file.

NOTE
When moving the lock between installations or when making a claim, you must perform **Factory Reset**. This operation resets the lock to factory settings and removes all previous configuration.

Configuration Update Instructions

1. Make changes in **Access Commander**.
2. Download a new project file.
3. Upload the file to **Fortis Commander** and make the required changes to the locks.
4. If you make other changes in **Access Commander**, always download a new project file.

CAUTION
Make sure to download a new project file for every configuration change in **Access Commander** – never use an older file already uploaded to **Fortis Commander**.

Permanent Locking/Unlocking

The app allows you to permanently lock and unlock the lock. The function is used for service interventions or emergency control without the use of a card.

Collection of events from electronic locks using RFID cards / chips

Event collection settings

1. Open **Settings > Electronic locks > Tab events**.

2. Select the event type:
   - **Collect access and system events** - All access and system events are recorded on the card/chip and written to the **System Log** and **Access Log**.
   - **Collect only system events** - only system events are logged, access events are not stored on cards.
   - **Do not collect events on** tabs - no events are written to the tab; they can only be accessed through **Fortis Commander**u.

> **TIP**
> Selecting the appropriate event set can reduce system load and storage utilization. However, detailed logging is important for diagnostics and safety audits.

Exporting events from a card

The card stores a maximum of **16 first events**. Events can be read in two ways:

- In **Access Commander**, click on the icon in the search box in the header and load the tab.
- Using a device with **2N OS**, events are read from the card and sent to **Access Commander**u.

Uploading events to the lock

1. Open **Settings > Electronic Locks > Fortis Commander** and click on Download File.
2. Open the file in **Fortis Commander**.
3. In the **Fortis Commander** app, connect to the electronic lock.
4. Upload the updated file back to **Access Commander**.
5. Once uploaded, the events are displayed in **Access Logs** and **System Logs**.

Service Operations

The following operations are available for **Fortis Cylinder**:

- **Disassembly** – disassembly of locks for service purposes.
- **Battery Replacement** – replacing the battery in the lock.

> **CAUTION**
> The service operations are not relevant for other types of locks.

> **NOTE**
> Press the Lock button for permanent locking to switch the lock from the service mode to the normal mode.

Card Update

User access cards need to be updated on a regular basis. The user updates the card by tapping it on the 2N IP device to which the user has valid access rights. The card must be held against the reader until the door opening switch is activated. The door opening switch is not activated until the lock accesses have been updated.

You can change the default ten-day validity of the cards in **Settings > Electronic locks > Card parameters**.

CAUTION
If you change the lock access rights in **Access Commander**, the changes will not be reflected on the user access card until the card has been updated on a 2N device card reader! For security reasons, we recommend that a shorter validity period is set for the cards to ensure they are updated regularly.

The IP readers in the devices that allow for card updates and their settings are described in the Subs. IP Device Reader Settings (p. 29).

Compatible Cards

NOTE
For the purposes of this documentation, the term **card** refers to any compatible identifier using the MIFARE DESFire technology.

Cards with random ID cannot be used for opening the 2N Fortis electronic locks.

Cards with PICard technology cannot be used for opening the 2N Fortis electronic locks.

Time Profiles on Electronic Locks

Electronic locks support time profiles with the following limitations:

- Holidays do not apply.
- You can set up to 4 different time intervals per day.
- 4 daily interval schedules can be defined within one time profile.

TIP
This means that you can have different settings for Monday, Tuesday, Wednesday and Thursday, for example, but you must use one of the existing settings for Friday, Saturday, and Sunday.

CAUTION
If the time profile violates the specified restrictions, the access rule will be ignored and the user will not be granted access.

Maintenance Cards

Maintenance cards provide authorized access to the lock. They allow for putting the lock in service, battery replacement, lock disassembly.

CAUTION
The maintenance card cannot be used as a user access card at the same time.

Maintenance Card Settings

1. In **Access Commander** go to **Settings > Electronic locks**.
2. Click Create in **Maintenance cards**.
3. Select the card type to be created in the open dialog box.
   - New locks setup – activate the previously configured new locks in factory settings into the service mode.
   - Service – activate the service mode for the already set lock.
   - Disassembly – release the already set 2N Fortis Cylinder lock for disassembly, see the 2N Fortis Installation Manual.
   - Battery Replacement – release the already set 2N Fortis Cylinder lock for battery replacement, see the 2N Fortis Installation Manual.

   TIP
   New locks setup and any other service card can be uploaded on one physical card simultaneously. We recommend a combination of **New locks setup** and **Service**.
4. Click Continue.
5. Tap the card on the connected USB RFID reader. Wait until the data has been loaded on the card.

The validity of the maintenance card data is one year. After this time, the data must be deleted and the card set up again.

Troubleshooting

Diagnostic Logs

Diagnostic logs helps the Technical Support staff identify and solve reported troubles. The logs include information on performed actions, errors, status changes and other relevant events.

Diagnostic Log Download

1. Go to **Settings > Troubleshooting > Diagnostic Logs**.
2. Click Generate logs.
   The log packet generating process takes a few minutes.
3. Once prepared, the packet is displayed on the card and is ready for Download.

Usage Statistics

If the function is enabled, **Access Commander** sends anonymous data on used functions to a secure 2N server once a day. Every sending is performed with a unique identifier, which is regenerated automatically for every new sending. This prevents the 2N side to identify the given **Access Commander** installation. The so-obtained information helps improve product development, innovate functions and enhance user experience.

Notifications

The Notifications module helps you monitor selected system events and features, which are to be reported by **Access Commander** by e-mail or notification in the upper bar next to the user menu.

The notification list is also displayed in **System logs > Notifications**.

Press Export above the list to download the list in a CSV file. The time is GMT+0 in the CSV file exported.

Notification Type Setting

1. Go to **Settings > Notifications**.
2. Click the adding button in the right-hand upper corner of the page.
3. Enter the new notification type name.
   After creation, the notification detail will be displayed for you to choose the devices whose notifications are to be monitored, add the user to be sent notifications to and select the way of notification delivery.

Notification Settings

Set the notification type in the detail of the selected notification type. Click the selected notification in the **Settings > Notifications** to open the notification type detail.

Delivery Methods

Set the notification delivery method and the list of e-mail notification recipients on the card.

In **Access Commander**, notifications appear under the icon in the upper bar next to the user menu or in **System log > Notifications**.

Notification e-mails can be sent to the users listed in **Access Commander** as well as recipients outside the system. The users can be selected from a list. E-mail addresses of other recipients have to be added manually.

NOTE
Make sure that SMTP is set correctly to make e-mail notifications work properly, refer to E-Mail (SMTP) Enable and Setting (p. 97).

Monitored Devices

The given notification type can be generated both for all the devices and selected devices. If Monitoring of all devices is enabled, the event can happen on any device and a notification is generated. If Monitoring of all devices is disabled, a notification is generated only if the event happens on a selected device. Select the device in a menu opened using .

Network Configuration

Set the network connection in **Settings > Configuration > Network card**. The Network card shows and helps set the current parameters of **Access Commander**. Remember to enable manual configuration before setting the parameters.

The configuration methods include setting of the network parameters automatically from the DHCP server or manually. When the automatically set IP address from DHCP is changed into a manually set IP address, redirection to the manually entered IP address is made in the web browser. After redirection, **Access Commander** is restarted and system re-login is required.

CAUTION

- By changing the configuration method to DHCP, you change the server IP address and may cause connection interruption.
- If you change the HTTP Proxy server, **Access Commander** will automatically restart.

Device IP Address Change Detection

Access Commander establishes connections to devices via their IP addresses. To avoid losing connection to a device with a dynamic IP address, two methods of detecting device IP addresses are available.

- **Network Scanner**
  Access Commander periodically scans the local network segment using the integrated 2N Network Scanner to identify the connected devices and their current IP addresses.
- **Device Callback**
  This method detects the IP addresses of the devices outside the local network segment. The devices will report themselves on startup, whenever the IP address changes and at periodical intervals (once an hour). For a proper operation, you must specify the target destination to which the devices shall report (typically the **Access Commander** IP address).

Network Discovery

Network discovery helps other services, such as **2N IP Utility** or **2N Network Scanner**, locate the **Access Commander** installation in your LAN.

Network Scanner and **Axis Utility** can be used at the same time. However, you can disable both **Access Commander** detections in the system settings for security reasons.

TIP

You can show/hide **Access Commander** in **2N Network Scanner** and **2N Axis Utility**. The same holds true for access to the web interface via **accesscommander.local**. If multiple instances of Access Commander are running in the network, the system automatically assigns unique names: **accesscommander.local**, **accesscommander-2.local**, **accesscommander-3.local** and other instances according to the count of servers in the network.

Proxy Settings

The proxy is used for such services as: HTTP requests, FTP synchronization, upgrades, etc.

NOTE
Proxy for FTP with TLS authentication is not supported.

1. Go to **Settings > Configuration > Network**.
2. Select Edit Proxy.
3. Type the proxy server addresses for the required protocols in the open dialog box.
4. In the last field, you can fill in addresses for which the proxy server should not be applied.
   Connections to localhost and to IP addresses in the range of 127.0.0.1/8 will never be routed through a proxy server.
5. After the settings are changed, **2N Access Commander** will automatically restart.

Using NodeRED

The NodeRED application ignores proxy server settings. For proper functionality, the proxy server has to be explicitly configured in each NodeRED node that requires its use.

Supplementary Information

MIFARE and DESFire are registered trademarks of NXP B.V.

HTTP API

The **Access Commander** API URL address is as follows: https://acom_ip_address/api/v3/.

Refer to http(s)://acom_ip_address/support/api for the API endpoint list. The endpoint list is available outside the **Access Commander** interface.

The responds to requests can be filtered using Query. Refer to Data Query Customization (in English only) for the **Query** building details.

Authentication

The HTTP API commands are sent under the user login data or using token authentication. The authentication token is created by the administrator in **Settings > Configuration > API access tokens**. It is the Bearer Token. While creating a new API access token, the administrator can limit the token validity for reading only to make the token authenticate the GET commands only. The token can be limited to: 1 month, 6 months, 1 year.

CAUTION
Copy the created access token to the box. Later, the token cannot be displayed.

SignalR

SignalR is a protocol that enables real-time server to client communication. This means that the server can send messages to connected clients as soon as they become available, and does not have to wait for a request from the client. The basic principles of SignalR are described in SignalR integration manual (in English only). A list of available SignalR topics for use with **Access Commander** are described in SignalR topics reference manual (in English only).

Third Party Licenses

A long list of the used third party library licenses is included in the user menu located to the right on the upper bar in the About Application section.

2N Access Commander – Installation Manual

2N.com