



2N Access Commander

User Manual



Firmware 3.1

Abstract

Table of Contents

Symbols and Terms Used	6
General Information	7
User Rights	7
Supported Devices and Applications	8
Supported Devices	8
Web Browsers	9
Virtualization Platforms	9
Used Ports	10
License Overview	10
Installation	13
Access Commander Box Distribution	13
Technical Parameters of Access Commander Box	14
Virtual Machine Distribution	14
Recommended Hardware	15
License Activation	16
Getting License File	16
License Upload	16
License Suspension	17
Basic Access to Interface	18
Dashboard	18
Language Change	18
Account Password Change	18
Profile Image Change	19
Logs	20
System Logs	20
Log Export	20
Log Lifetime	20
Access Logs	21
Log Export	21
Log Lifetime	21
Notifications	22
Notification Settings	22
Log Lifetime	23
Companies	24
Company Creation	24
Company Settings	24
Company Language	24
Zones	24
Mobile Key	24
Visitors	24
Working Time	25
Holidays	25
E-Mails Sent to Company Users	25
Company Synchronization (LDAP)	25
Users	28
User Creation	28
User Settings	28
User Name and Photo Change	29
Credentials	29
Account	29
Personal Information	30
Access	30

Phone Numbers	31
Access Log	31
Change Log	31
Fingerprint Enrollment	31
Bluetooth Authentication	31
User Attendance	32
Groups	34
Group Creation	34
Group Settings	34
Members	34
Access Rules	34
Zones	35
Zone Creation	35
Zone Settings	35
Multi-Factor Authentication	35
Access Settings	36
Devices	36
Companies	36
Access Rules	36
Devices	37
Device Adding	37
Emergency Lockdown	37
Device Configuration	38
Overview	38
Calling	39
Lift	40
Monitoring	41
Firmware	41
Device Exclusion	41
Incompatible Firmware Versions	41
Security	42
Setting Device Access Points	42
Access Rules	44
Matrix Display	44
Example of Matrix Display	45
Rule List	45
Time Profiles	46
Time Profile Creation	46
Time Profile Settings	46
Attendance	47
Specific User Attendance	47
User Attendance Change	47
Attendance Settings	47
Setting Device Access Points	48
Visitors	50
Visitor Data Retention Settings	50
Visitor Creation	50
End of Visit	50
Visitor Settings	51
Access	51
Visitor	51
Personal Information	51
Credentials	51
Access Log	51

Cards	51
Presence	52
User Presence Expiration	52
Reports	53
Area Restrictions	54
Area Restriction Creation	54
Area Restriction Settings	54
Entry and Exit	54
Occupancy	54
Anti-Passback	54
Exception Settings	55
List of Blocked Users	55
Restriction Reset	55
The most common setup errors	55
Example of Restriction Setting	56
System Setup	57
Date and Time	57
Time Synchronization with Devices	57
Network Configuration	57
E-Mail (SMTP) Enable and Setting	58
System Update	58
Beta Testing	59
System Backup	59
User Synchronization	60
Enabled USB readers	62
PICard Keys	62
Encryption Keys for Mobile Key	62
CAM Logs	63
CAM Log Settings	63
Two-Factor Authentication	64
SSH Access Enable	64
Linux Settings	65
Troubleshooting	67
Diagnostic Logs	67
Usage Statistics	67
Supplementary Information	68
HTTP API	68
Third Party Licenses	68

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 management. Devices are access controlling (2N intercoms or 2N access units) or communication providing (2N answering units) physical units in a building. Devices are gathered in **Zones**. Each device can be in one zone only.

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 time profiles.
- Setting access rules.

User Manager

- Creating and managing users.
- Creating and managing visitors.
- Managing user and visitor assignment 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.

Supported Devices and Applications

This subsection includes lists of supported devices, supported web browsers and compatible virtualization platforms via which **Access Commander** 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 \(p. 41\)](#).

2N Intercoms

- 2N IP Style – QR code reading support
- 2N IP Verso 2.0 – QR code reading support
- 2N IP Verso
- 2N LTE Verso
- 2N IP Force
- 2N IP Safety

- 2N IP Vario
- 2N IP Base
- 2N IP Solo
- 2N IP Uni
- 2N IP Video Kit
- 2N IP Audio Kit
- 2N IP Audio Kit Lite

2N Access Units

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

2N Answering Units

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

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

Table 1. 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

^aIt is used both for client communication and intercom communication.

^bThe 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*.

General Information

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
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	✓	✓	✓	✓	✓
User Import from CSV or Device	✓	×	✓	✓	✓
Bulk Firmware Administration	✓	×	✓	✓	✓
Multi-Factor Authentication	✓	×	✓	✓	✓

General Information

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
User Rights	✓	×	✓	✓	✓
Notification	✓	×	✓	✓	✓
Presence	✓	×	✓	✓	✓
API access keys	✓	×	✓	✓	✓
CAM Logs	✓	×	✓	✓	✓
Lift Control	✓	×	✓	✓	✓
Dashboard	✓	×	✓	✓	✓
Emergency Lockdown	✓	×	✓	✓	✓
Mobile Credential Support	✓	×	✓	✓	✓
Visitor Management	✓	×	✓	✓	✓
Occupancy Management	✓	×	×	✓	✓
Synchronization (LDAP & CSV)	✓	×	×	✓	✓
Anti-Passback	✓	×	×	✓	✓
Attendance	✓	Optional	Optional	Optional	Optional

^aUnlimited within the maximum capabilities of the software platform, refer to [Recommended Hardware \(p. 15\)](#).

Installation

Access Commander can be distributed as:

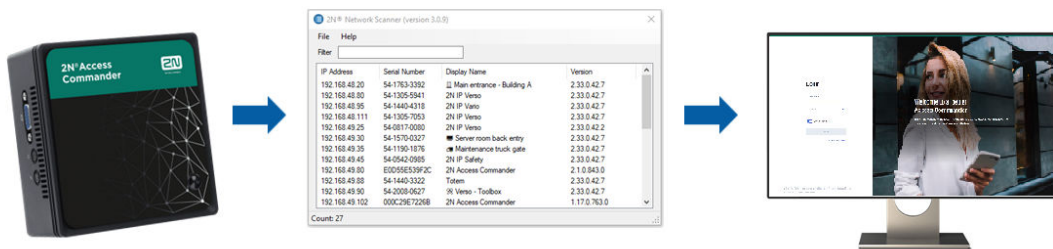
- 2N Access Commander Box, a small desktop computer (Part No. 91379030, Axis Part No. 01672-001)
- Virtual machine

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

Access Commander Box Distribution

Access Commander Box (Part No. 91379030, Axis Part No. 01672-001) is a small compact desktop computer 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. The Access Commander Box is used as a data/event/log collection server for the entire access system.

Login to Access Commander with Dynamic IP Address



1. Connect the Access Commander Box to the network using an Ethernet cable.
2. Localize the Access Commander Box in the network using 2N IP Network Scanner.
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.

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.

Technical Parameters of Access Commander Box

- Ultra compact PC design – 0.69L (56.1 x 107.6 x 114.4mm)
- 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

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 [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 [Software & Firmware](#) at 2N.com. Unpack the downloaded file.
2. In VMware 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 [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).
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 [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 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.

Table 2. 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

Table 3. Access Commander Box

Connected device count 2.0	User count 2.0	User count per group
2000	100000	1500

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.

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**. The License file is generated on the basis of the serial number of this license device.

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.

License Upload



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 Suspension

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 protective period values.

When a license is suspended, all the connected devices are automatically removed from the management and marked as unmanaged. To reactivate them, connect and activate the license 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.

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

Basic Access to Interface

This subsection describes putting in operation and basic operation of **Access Commander**. Installation is described in Subs. [Installation \(p. 13\)](#).

The **Access Commander** interface is available via a web browser. Find the web interface IP address using 2N Network Scanner.





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.

Dashboard

Dashboard is the basic display of the **Access Commander** web interface. It is a configurable notice board showing real time data. **Access Commander** provides several Widgets, which are added to the Dashboard

using the . The Dashboard Widgets can be moved or renamed or their basic settings can be made. Use the extended menu  in the header of each Widget to administer and delete the Widgets.


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.

Language Change

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 the 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 Logs \(p. 20\)](#)
- [Access Logs \(p. 21\)](#)
- [Notifications \(p. 22\)](#)
- [Log Lifetime \(p. 20\)](#)

System Logs



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 by **Access Commander**.

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


- Severity (info, warning, error);
- Event time;
- Action category (Device state, Import, User synchronization, System, User actions, Area restrictions);
- Related subject (device, user, zone, visitor...);
- Brief event description;
- 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 export the list as a CSV file or print it out. 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 Logs



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 export the list as a CSV file or print it out. 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.

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 export the list as a CSV file or print it out. 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 \(p. 58\)](#).

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.

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.

Mobile Key

In Company, you can also set the pairing parameters for the 2N Mobile Key application, which allows for Bluetooth authentication. Set both the devices that can be used for pairing and the validity of the mobile keys necessary for pairing. The mobile key 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 \(p. 50\)](#) 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
- Mobile key 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.

The set LDAP connection detail opens up. Now you can test the connection settings. Press **Synchronize Now** to start one-time synchronization.
3. 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.
4. You can assign user data to the LDAP server attributes on the **Options** card.

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

LDAP Synchronization Options

Imported Attributes – edit the scheme to assign the **Access Commander** data to the LDAP server attributes.

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 disabled, their data will remain in **Access Commander** but will not synchronized with the devices.

Users Disabled in Active Directory – define what to do with the users disabled in the Active Directory. **Access Commander** can ignore the disable or delete (disable) the users disabled in the Active Directory. Once recovered in the Active Directory, the earlier deleted users are reloaded to **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. The scheme enables synchronization for 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 searching of the whole tree or, if the parameter is disabled, just the root.

Companies

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.








Users

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

The user list includes all the users created. You can filter the users above the list or just find a user by the name, e-mail or phone number.

Bulk Actions

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

-  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.

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 their 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 [User Attendance \(p. 32\)](#). 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 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.

Mobile Key – used for interconnection with 2N Mobile Key app, which provides authentication via Bluetooth, refer to Subs. [Bluetooth Authentication \(p. 31\)](#).

PIN Code – automatic generation of a 6-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 \(p. 31\)](#) for details.

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

Virtual Card – 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 \(p. 64\)](#). 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 \(p. 24\)](#). 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's account in **Access Commander** will be sent;
- **User number (User ID)** – specific identifier necessary for bulk synchronization with the CSV file (refer to [User Synchronization \(p. 60\)](#));
- **Note**.


Access

The Access 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.



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.

A virtual phone number can be used for user calling via the numeric keypad on the device. A virtual number can include two to four digits. Virtual numbers are not related to the users' personal phone numbers and thus help hide the users' personal phone numbers on the device. 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 that 2N USB Driver has been installed. Download the driver [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 Mobile Key application is installed in your mobile phone to make successful authentication via Bluetooth.




Enter the Mobile Key pairing code to connect the application in your phone with the devices in **Access Commander**.



Get the pairing code as follows:

- through a USB Bluetooth reader connected to your PC
- through interconnection with the device.

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 Mobile key 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 \(p. 32\)](#) for pairing in the application.

Pairing Code Creation Using Device



1. Make sure that
 - the pairing device is set for the given user's company, refer to [Company Settings \(p. 24\)](#);
 - the pairing device is located in the zone which the user is allowed to access, refer to [Access Rules \(p. 44\)](#);
 - an adequate pairing time value is set, refer to [Company Settings \(p. 24\)](#).
2. Select Mobile key 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 \(p. 32\)](#) for pairing in the application.

Mobile Key Pairing

1. Download the Mobile Key application to your mobile phone. The application is now 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 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.

Users

Monitoring and editing attendance are described in the chapter [Attendance \(p. 47\)](#).

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 \(p. 48\)](#).

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. Mobile Key
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.

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 export the list as a CSV file or print it out. 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 States

- Online
- Unmanaged
- Incompatible
- 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.

Device Adding


1. Go to the **Devices** page.
2. Click the device adding button in the right-hand upper corner.
3. 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.
4. 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.
5. Name the device before creation.

The new devices appear on the list. Make other settings in the device detail.

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 card 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 \(p. 48\)](#)), 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.

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 \(p. 37\)](#) 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**. The last backup is displayed on the card from which the backup file can be downloaded. You can synchronize the device automatically with the last backup using the menu in **Restore**. In this menu, you can synchronize the device with a backup stored on another device.



NOTE

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

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.

- 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

To control the floor lift access, connect the AXIS A9188 relay module to a 2N IP intercom (2N IP Verso, 2N IP Force, 2N IP Safety, 2N IP Vario) or to an Access Unit. Up to 8 relay modules can be connected to one 2N IP intercom or Access Unit, each of which can control up to 8 floors, which makes a total of 64 floors. Make sure that the licenses for 2N IP intercoms (Part No. 9137916) and Access Unit (Part No. 9160401) are active for this function.

Lift Control Settings

- 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.
- Go to  hardware configuration of the device in the device detail header. Enable the lift access control modules in Hardware > Lift control. If the modules require authentication, enter the user name and password. Save the settings. Click the cross in the upper blue bar to quit configuration.
- Go to the Lift tab in the device detail.
- 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 .
- 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 helps you find information on the devices connected. 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.

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.

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


Device Exclusion

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

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

Security

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.

To be verified successfully, the device certificates have to be signed by a certification authority and include an IP address/domain name of the device. The certification authority (CA) certificate has to be trustworthy on the server on which **Access Commander** is running. The device certificates have to be uploaded via the device web interface (System > Certificates > User Certificates) and set as HTTPS Server Certificate in Services > Web Server > Advanced Settings.



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.

Setting Device Access Points

The devices (2N intercom or 2N Access Unit) can have up to two access points. Each access point allows for passage in one direction. Access points differentiate passage direction through the device. Each access point can be assigned one or more readers that are connected to the device and work in the direction of the point. Access points are used for recording a zone entry/exit. They have to be used if the device is located on a zone border.

In addition, access points help monitor the users in the [Presence \(p. 52\)](#) module. Also, access points are used for monitoring entries/exits in [Area Restrictions \(p. 54\)](#).



NOTE

The access point settings in **Access Commander** are propagated into Services > Access control in the device web interface:


- Access point 1 = Entry Rules
- Access point 2 = Exit Rules


Setting Access Rules

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. Find the module that provides the access to be used as access point 1 (Entry) or access point 2 (Exit).
4. Set the required direction in the Door parameter and save the setting.
5. Go to Zones in **Access Commander**.
6. Press  in the right-hand upper corner and enable the use of access points.

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 \(p. 46\)](#). 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

	User A	ASD	Foyer	Zone1	Zone2	Zone5
Verso D102				✓		
Developers		✓	🕒		✓	🕒
Test RC Company	✓	🕒	🕒			🕒

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 adding 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 Profile Creation


1. Go to the **Time Profiles** page.
2. Click the time profile adding 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 limitation. Green days identify the days falling into the time profile. Click a day to select it. You can set a time interval within days to define the time profile validity. Different times for each day cannot be set until the time profile has been created.

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.

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 \(p. 47\)](#).



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 \(p. 28\)](#).

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

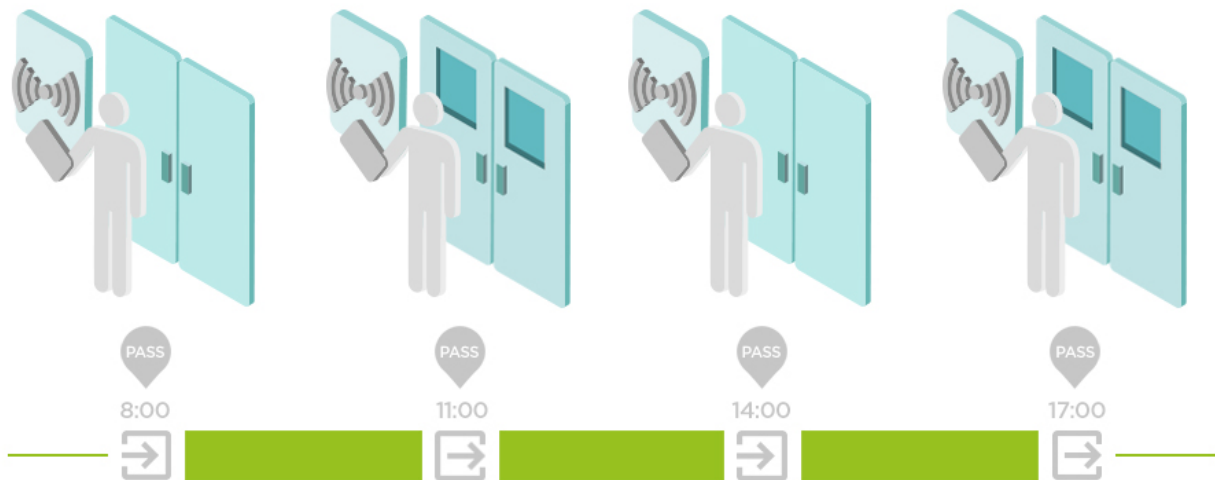
The attendance manager can edit the user attendance data. To do this, click the time interval to be changed. You can also edit the border times and add a note to an interval.

Attendance Settings

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

Attendance Modes

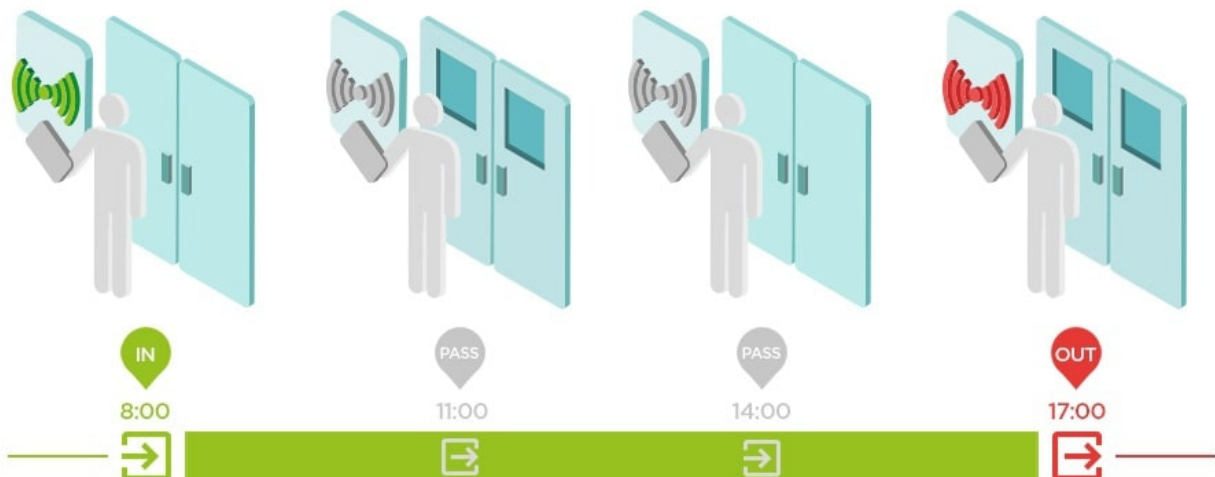
- **FREE**



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**

It is necessary to set the arrival and departure devices 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

The devices (2N intercom or 2N Access Unit) can have up to two access points. Each access point allows for passage in one direction. Access points differentiate passage direction through the device. Each access point can be assigned one or more readers that are connected to the device and work in the direction of the point. Access points are used for recording a zone entry/exit. They have to be used if the device is located on a zone border.

In addition, access points help monitor the users in the [Presence \(p. 52\)](#) module. Also, access points are used for monitoring entries/exits in [Area Restrictions \(p. 54\)](#).



NOTE

The access point settings in **Access Commander** are propagated into Services > Access control in the device web interface:


- Access point 1 = Entry Rules
- Access point 2 = Exit Rules


Setting Access Rules

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. Find the module that provides the access to be used as access point 1 (Entry) or access point 2 (Exit).
4. Set the required direction in the Door parameter and save the setting.
5. Go to Zones in **Access Commander**.
6. Press  in the right-hand upper corner and enable the use of access points.

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 one month.

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 \(p. 50\)](#).

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 \(p. 51\)](#).

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.

Presence


The Presence module is an extension to the Attendance module and displays the list of currently present employees. Remember to set the attendance IN-OUT mode in v **Settings > Configuration > Attendance card**, refer to [Attendance Settings \(p. 47\)](#), 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 user zone will be changed. The same happens if the user passes the reader in the **IN** mode.
- If Departure (**OUT** event) is the 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.

- **Mobile Key** – Paired and unpaired users with pairing time remaining
The report includes status data on user pairing via Mobile Key, 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 \(p. 60\)](#).

**CAUTION**

The file contains sensitive data!

Area Restrictions

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

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.

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 extended 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 the added device has two access points set, each point can be used for a different direction (Entry/Exit). Access point settings are described in the chapter [Setting Device Access Points \(p. 48\)](#). Access point properties are expanded by clicking the arrow.

Occupancy

It is necessary to set the arrival and departure devices for a proper function.

The Occupancy card helps monitor and control the count of persons in an area. Occupancy limitations help control 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. The entry and exit devices are required for this function.

Anti-Passback

It is possible to activate Anti-passback for areas, which extends 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 users 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 > Reset area restrictions card 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.

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.

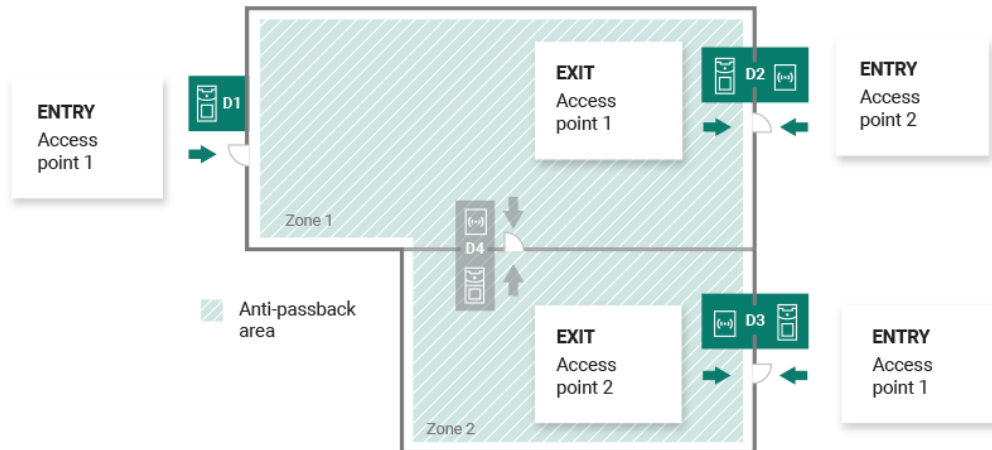
The following cases may prevent the correct operation of area restrictions

- 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

- [Date and Time \(p. 57\)](#)
- [Network Configuration \(p. 57\)](#)
- [E-Mail \(SMTP\) Enable and Setting \(p. 58\)](#)
- [System Update \(p. 58\)](#)
- [User Synchronization \(p. 60\)](#)
- [Enabled USB readers \(p. 62\)](#)
- [PICard Keys \(p. 62\)](#)
- [Encryption Keys for Mobile Key \(p. 62\)](#)
- [CAM Logs \(p. 63\)](#)
- [Linux Settings \(p. 65\)](#)

Date and Time

Date and time can be synchronized with the Internet or set manually in **Access Commander**. Change the date/time retrieval method in Settings > Configuration > card Server date and time. 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**.
- **Devices Use Access Commander as NTP Server** – the device time synchronizes with the **Access Commander** time.

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.

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.

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

1. 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.
2. 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).
3. 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.
4. Send a test e-mail to check the settings.

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 \(p. 59\)](#) 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.

- When the installation is completed, click **Go to login** to get to the login page.

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


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

Automatic Data Backup Settings

- Go to **Settings > System Backup card**.
- Click  at the Periodic Backup parameter.
- Set the required backup parameters:
 - Frequency – periodic backup interval
 - Time – backup time
 - Day – day in a week/month for backup
- Select whether or not to use data encryption. If so, complete the password to be entered for backup restoration.



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.

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 card**. Download a CSV template from the card.



TIP


Download the current user list matching the CSV template structure at [Reports \(p. 53\)](#).

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. Click  in the Storage parameter.
2. Set the FTP server address on which the CSV file is stored in the open dialog box.
3. Enter the FTP server login data.

CSV file



DOWNLOADS

Download the CSV template for user synchronization via [this link](#).



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.

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**.

Click **Allow readers** to open a dialog box to enable/disable the use of an external USB device. Subsequently, click **Change** to edit the 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
- External USB Bluetooth reader (dongle) – Part No. 9137422E, AXIS Part No. 01402-001

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. Click **Import** to upload the file with encryption keys from your storage.
2. 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.

Encryption Keys for Mobile Key

Users can use the Mobile Key application for connection with the 2N devices. The Mobile Key – device communication is always encrypted. Mobile Key cannot authenticate a user without knowing the encryption key. The primary encryption key is automatically generated upon the intercom first launch and can be re-generated manually any time later. Together with AuthID, the primary encryption key is transmitted to the mobile device for pairing.

The Mobile Key – device communication is always encrypted. Mobile Key cannot authenticate a user without knowing the encryption key. The primary encryption key is automatically generated upon the intercom first launch and can be re-generated manually any time later. Together with AuthID, the primary encryption key is transmitted to the mobile device for pairing.

You can generate up to 4 encryption keys in **Settings > Credentials > Encryption Keys for Mobile Key**. The generated key is automatically uploaded into Mobile Key upon the first use of the mobile phone with the

device paired earlier. 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.

If Mobile Key has no access to any of the valid encryption keys, the application cannot be used for user authentication. To restore the function, re-pair the application with the device connected to **Access Commander**, which results in uploading the valid encryption keys to Mobile Key.



NOTE

The access to the device depends on the access rights of the given user.

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

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.

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.

The administrator sets two-factor authentication in Settings > Configuration > Two-factor authentication. 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, see [Two-Factor Authentication Enable \(p. 64\)](#).

- **Mandatory for user with 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. Select View profile.
3. Interconnect the account with the authentication application on the Two-factor authentication card. Follow the wizard instructions.

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 \(p. 65\)](#).

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.

```
2N(R) Access Commander GNU/Linux Configuration Console

2N(R) Access Commander appliance services

You can access the application at https://10.0.14.23
Default login credentials for web access are:
  User name: admin
  Password: 2n

For further assistance please consult
https://wiki.2n.cz/x/DZeUAg

<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.

System Setup

- **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.

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.

Supplementary Information

HTTP API

The **Access Commander** API URL address is `https://acom_ip_address/api/v3/`.

Refer to `http(s)://acom_ip_address/support/api` for the API endpoint list. The [endpoint list](#) issued with firmware version 2.7 is available outside the **Access Commander** interface.

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 key. The API access key has the Bearer Token function. While creating a new API access key, the administrator can limit the key validity for reading only to make the authenticate the GET commands only. The key can be limited to: 1 month, 6 months, 1 year.



CAUTION

Copy the created access key to the box for use. Later, the key cannot be displayed.

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



wiki.2n.com

2N Access Commander – User Manual

© 2N Telekomunikace a. s., 2024

[2N.com](https://2n.com)