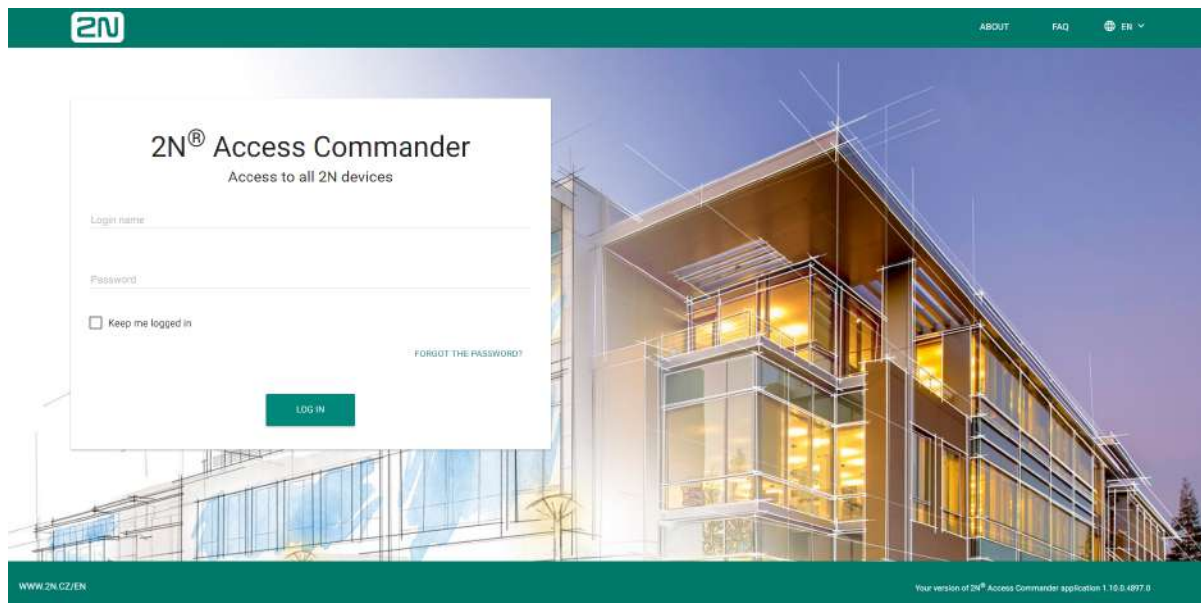


2N[®] Access Commander





- 1. Product Overview
 - 1.1 Virtual Machine Distribution
 - 1.1.1 Virtual Box
 - 1.1.2 VMware
 - 1.1.3 Hyper-V
 - 1.1.4 Recommended HW
 - 1.2 BOX Distribution
 - 1.3 Supported Browsers
 - 1.4 Used Ports
 - 1.5 Supported devices
 - 1.5.1 QR Code Supporting Devices
- 2. Linux Settings
- 3. System Setup
 - 3.1 Licenses
 - 3.2 E-mail
 - 3.3 Attendance Module Mode
 - 3.4 USB Devices
 - 3.5 Bluetooth
 - 3.6 2N Picard
 - 3.7 Synchronisation
 - 3.8 Log Management
 - 3.9 System Update
 - 3.10 System Backup
 - 3.11 Diagnostics
 - 3.12 Date and Time
 - 3.13 Network Settings
 - 3.14 SSH
- 4. System Administration

- 4.1 Companies
 - 4.1.1 LDAP
- 4.2 Users
 - 4.2.1 Bluetooth
- 4.3 Groups
- 4.4 Devices
 - 4.4.1 Display Configuration
 - 4.4.2 Device Configuration via 2N® Access Commander
 - 4.4.3 Automatic Synchronisation
 - 4.4.4 Device Backup and Restore
 - 4.4.5 Lift Control
- 4.5 Zones
- 4.6 Time Profiles
- 4.7 Access Rules
- 4.8 Lockdown
- 5. Extensions
 - 5.1 Presence
 - 5.2 Attendance
 - 5.3 Device Monitoring
 - 5.4 Visitors
 - 5.5 Notification
 - 5.6 CAM Logs
 - 5.7 Area Restrictions
 - 5.7.1 Example of Settings
- 6. HTTP API
 - 6.1 API Documentation version 2
 - 6.2 API Documentation version 3
 - 6.3 HTTP API Changes version 2
 - 6.4 HTTP API changes version 3
- 7. Supplementary Information
 - 7.1 Third Party License

1. Product Overview

Prevent unauthorised persons from entering your facility by using the 2N IP access system. The easily and intuitively controllable **2N® Access Commander** software is the brain of the entire system. It provides you not only facility access control but also real-time access unit status monitoring.

- [1.1 Virtual Machine Distribution](#)
- [1.2 BOX Distribution](#)
- [1.3 Supported Browsers](#)
- [1.4 Used Ports](#)
- [1.5 Supported devices](#)

1.1 Virtual Machine Distribution

2N® Access Commander is distributed as a virtual machine to be imported into your virtualisation software. The following options are available:

- [1.1.1 Virtual Box](#)
- [1.1.2 VMware](#)
- [1.1.3 Hyper-V](#)
- [1.1.4 Recommended HW](#)

1.1.1 Virtual Box

Note

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

VirtualBox:

Note

- *Open Source Software under the terms of the GNU General Public License (GPL) version 2.*

(<https://www.virtualbox.org/>)

1. Download the latest **VirtualBox** version from <https://www.virtualbox.org/wiki/Downloads>:
 - a. preferably including the **VirtualBox Extension Pack**.
2. Download the image from the [official 2N site](#).
3. In VirtualBox select File – Import appliance...

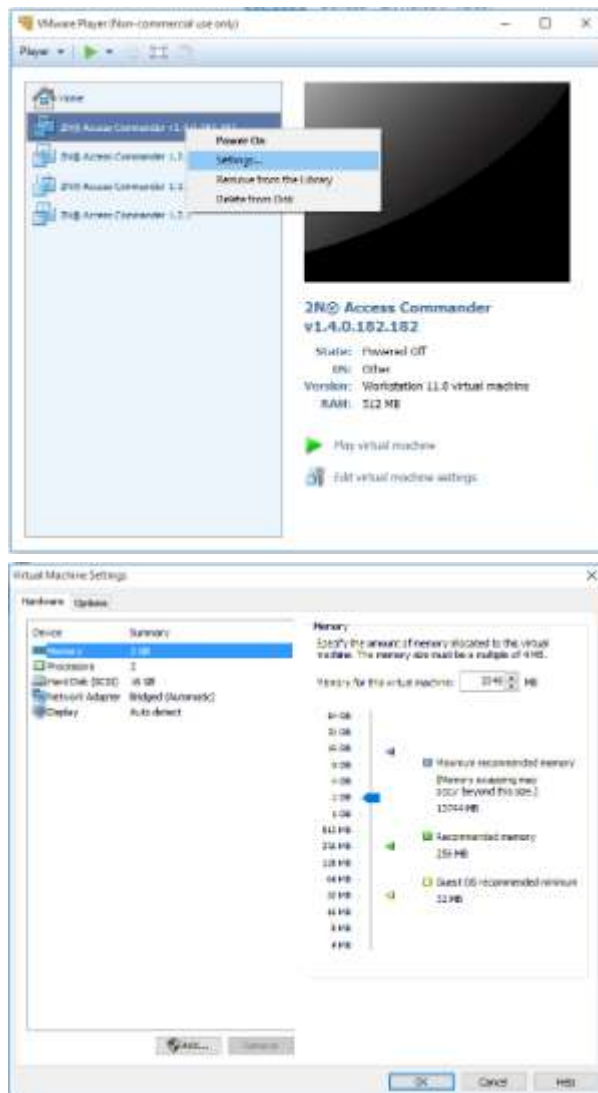


- a. edit the name,
 - b. check the CPU settings (2 at least),
 - c. check the RAM settings (2048 MB at least),
 - d. check the network card selection.
4. Confirm the License terms.

1.1.2 VMware

VMware Player

1. Download the image from the [official 2N web site](#).
2. In VMware Player File – Open... select the path to the OVA file.
3. Rename if necessary and click Import.
4. After the import, check the Settings.



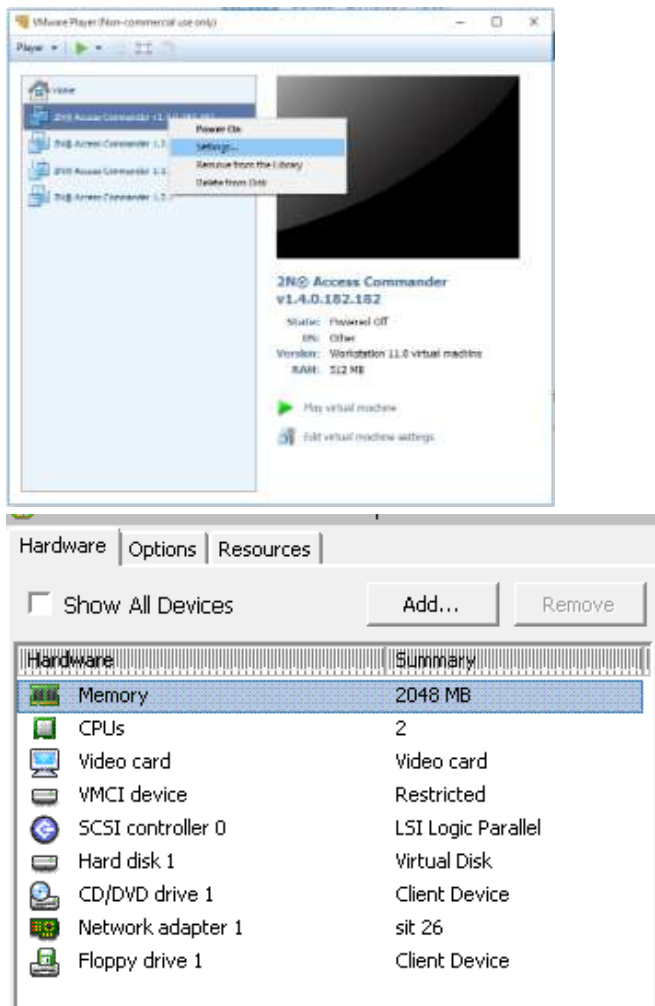
5. Check the settings:
 - a. check the RAM settings (2048 MB at least),
 - b. check the CPU settings (2 at least),
 - c. check the network card selection.

VMware vShere

Warning

- Created in VMware vShere - VMware ESXi 6.5.0. Not tested for other versions.

1. Download the image from the [official 2N web site](#).
2. In VMware vShere select File – Deploy OVF Template... and follow the wizard instructions.
3. After the import, check the Edit Settings...:



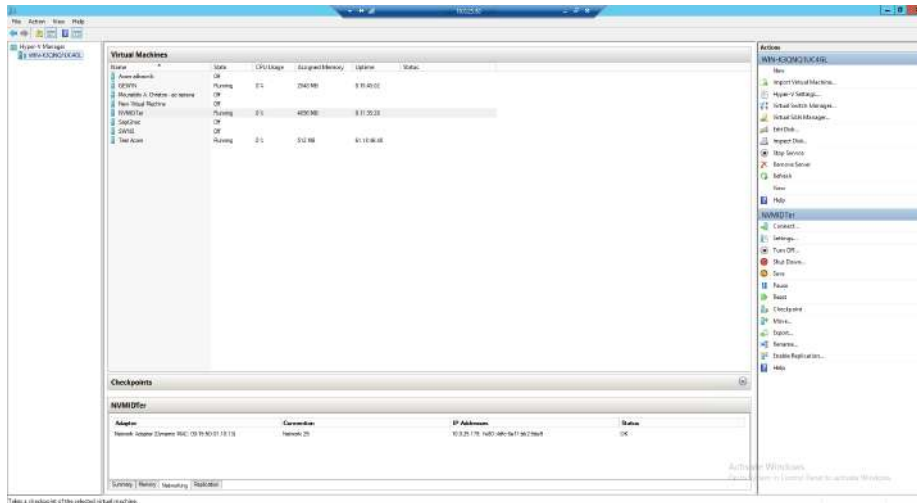
- a. edit the name (Options)
- b. check the CPU settings (2 at least),
- c. check the RAM settings (2048 MB at least),
- d. check the network card selection.

Caution

- A supported version of VMWare is 6.5 a higher.

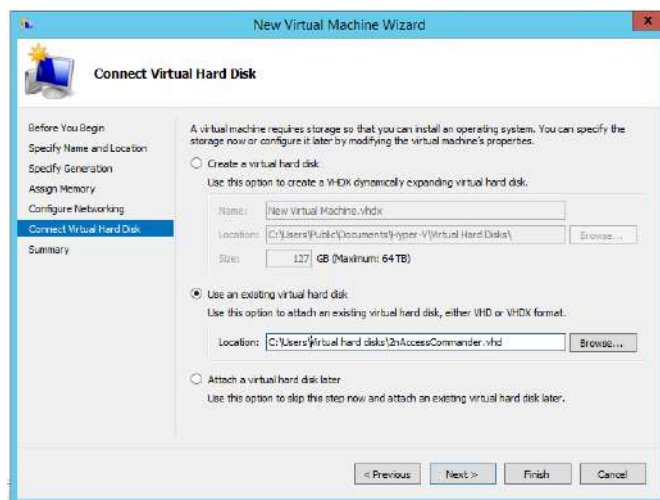
1.1.3 Hyper-V

Virtual machine creation in Hyper-V.



Take the steps below to create a new machine in the Hyper-V environment:

- Right-click the server for the virtual machine.
- Select New → Virtual Machine...
- Follow the wizard instructions.
- Select Use an existing virtual hard disk in Connect Virtual Hard Disk.
- Set the path to the file downloaded from here https://www.2n.cz/en_GB/products/access-control/2n-access-commander



- After the creation, check the virtual machine hardware tools as specified in [1.1.4 Recommended HW](#)

Warning

- Make sure that the 2nAccessCommander.vhd.7z file is downloaded to make **2N® Access Commander** work in Hyper-V; the 2nAccessCommander.ova file cannot be used.

1.1.4 Recommended HW

Virtual Machine Distribution

The count of the connected devices affects **2N® Access Commander** in variable ways. Therefore, set the size of hardware elements for the server accordingly.

The table below indicates the recommended minimum count of CPU cores and RAM sizes for different counts of devices and users managed by **2N® Access Commander**.

Count of connected devices	Count of users*	Count of CPU cores	Assigned RAM size
1 000	10 000	2	2 GB
2 000	100 000	2	4 GB
2 000	200 000	4	8 GB
7 000	200 000	4	16 GB

*We recommend group sizes no bigger than 1 500 users. Where area restrictions like anti pass-back or occupancy management are used with many users, the application might slow down.

Caution

- We recommend **2N® Access Commander** be connected to the devices 24/7. If **2N® Access Commander** becomes disconnected from your devices, they will store an event log autonomously and, upon reconnection, synchronize the offline log data back to **2N® Access Commander**. While this is happening, the application continues to run, but if there are many devices, this can take a long time.

2N® Access Commander Box

Count of connected devices 2.0	Number of users 2.0	Number of users per group*
2 000	100 000	1 500

*We recommend group sizes no bigger than 1,500 users. Where area restrictions like anti pass-back or occupancy management are used with many users, the application might slow down.

Caution

- We recommend **2N® Access Commander** be connected to the devices 24/7. If **2N® Access Commander** becomes disconnected from your devices, they will store an event log autonomously and, upon reconnection, synchronize the offline log data back to **2N® Access Commander**. While this is happening, the application continues to run, but if there are many devices, this can take a long time.

1.2 BOX Distribution



1x Gigabyte BRIX BACE with:
 - **2N® Access Commander**
 - 2.5" 120GB HD
 - 4GB DDR3 memory



1x 40W wall mount adapter
 with plugs for EU, US, Asia
 and Australia



1x VESA mount bracket
 6x Screws



1x Quick Start Guide
 (Data Sheet) in 7 languages

2N® Access Commander Box is access control software pre-installed on a powerful, ultra compact and small PC. It is a plug and play solution, which requires only a power supply and an Ethernet cable to be connected to the computer.

It is recommended to place this PC to a secure area and keep it up and running all the time for the proper and full functionality (it works as the system data, event and log acquiring server).

Part No. 91379030 – 2N® Access Commander BoxPackage Contents

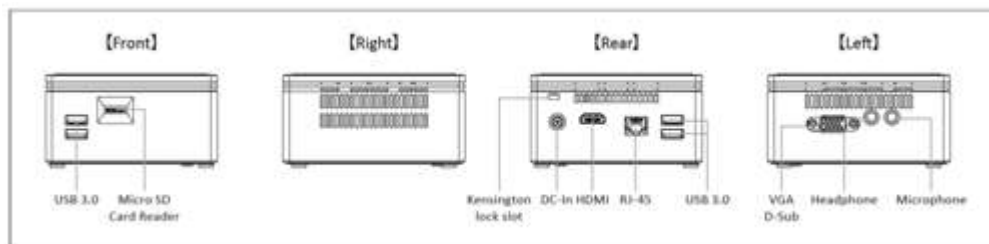
- 1 Gigabyte BRIX BACE with:
 - **2N® Access Commander**
 - 2.5" 120 GB HDD
 - 4 GB DDR3 memory

- 1 VESA mount bracket
- 6 screws
- 1 Quick Start Guide (datasheet) in 7 languages
- 1 40W wall mount adapter with plugs for EU, US, Asia and Australia

Technical Parameters of PC

- 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 x 75mm + 100 x 100mm)
- System environment operating temperature: 0°C to +35°C
- System storage temperature: -20°C to +60°C

The computer includes the following elements and connectors accessible to the user:



IP address

- The default setting is **DHCP ON**.
- Use the **2N® IP Network Scanner** to locate the computer with **2N® Access Commander** in the network.
- To set the **static IP address** (DHCP OFF), connect a keyboard and a monitor to the computer. Once the black screen appears, follow the steps below:

- 1) Log in to the system as root – the default login is **root : 2n**
- 2) Once the blue screen appears, change the default “root” password to a more secure one.
- 3) Go to the Advanced Menu.
- 4) Select Networking and then Static IP.
- 5) Set up the static IP address, gateway and DNS.
- 6) Apply the settings and quit the console menu (logout).

7) Connect to the set IP address via the web browser and log in to **2N® Access Commander** – the default login is:

- User name: **admin**
- password: **2n**

VESA Mounting Bracket

- 1) Attach the screws provided to the BRIX underside.
- 2) Attach the VESA mounting plate to the rear of a compatible display using the screws provided.
- 3) Now slide the BRIX BACE into the mounting bracket.

User and device limits (assuming use of 2N® Access Commander 2.0)

Where using **2N® Access Commander box's** own application interface:

Count of connected devices 2.0	Number of users 2.0	Number of users per group*
2 000	100 000	1 500


* Where Anti-passback is being used, the number of users who may enter the anti-passback area should be no higher than the maximum users per group.

Caution



- Please be advised that we recommend **2N® Access Commander** being connected to the devices 24/7. If **2N® Access Commander** becomes disconnected from your devices, a feature of our products are that the devices will store an event log autonomously and, upon reconnection, will synchronise the offline log data back to **2N® Access Commander**. Whilst it this happens, the application will continue to run but the event and access logs will be updated in the background whilst the data is being processed. If there are many devices, this can take a long time.

1.3 Supported Browsers

Optimised for the following browser:

-  Google Chrome (version 40 and higher)

Other supported browsers:

-  Mozilla Firefox (version 35 and higher)
-  Microsoft Edge (version 84.0.522 and higher)

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

1.4 Used Ports

List of services and necessary ports

Service	Port
HTTP/HTTPS*	80/443
SMTP	225
DHCP	68
DNS	53
NTP	123
LDAP**	389
SSH	22

* Used for communication with both the clients and door communicators.

** Port 389 is used for LDAP by default. Select another port in the **2N® Access Commander** configuration if necessary.

1.5 Supported devices

This subsection includes an overview of devices supported by the **2N® Access Commander** access system.

Supported devices
2N® IP Style
2N® LTE Verso
2N® IP Verso
2N® IP Vario
2N® IP Force
2N® IP Safety
2N® IP Uni
2N® IP Audio Kit
2N® IP Audio Kit Lite
2N® IP Video Kit
2N® IP Base
2N® IP Solo
2N Access Unit
2N Access Unit 2.0
2N Access Unit M
2N® Indoor Talk
2N® Indoor Compact
2N® Indoor View
2N® Indoor Touch
2N® Indoor Touch 2.0

1.5.1 QR Code Supporting Devices

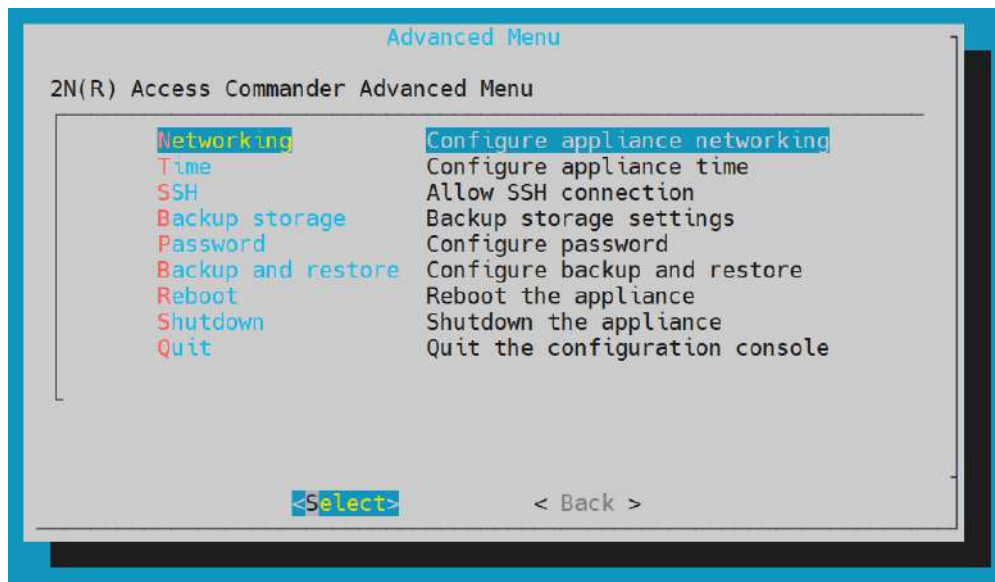
This subsection gives a list of QR code supporting devices supported by **2N® Access Commander**.

QR code supporting devices
2N® IP Style

2. Linux Settings

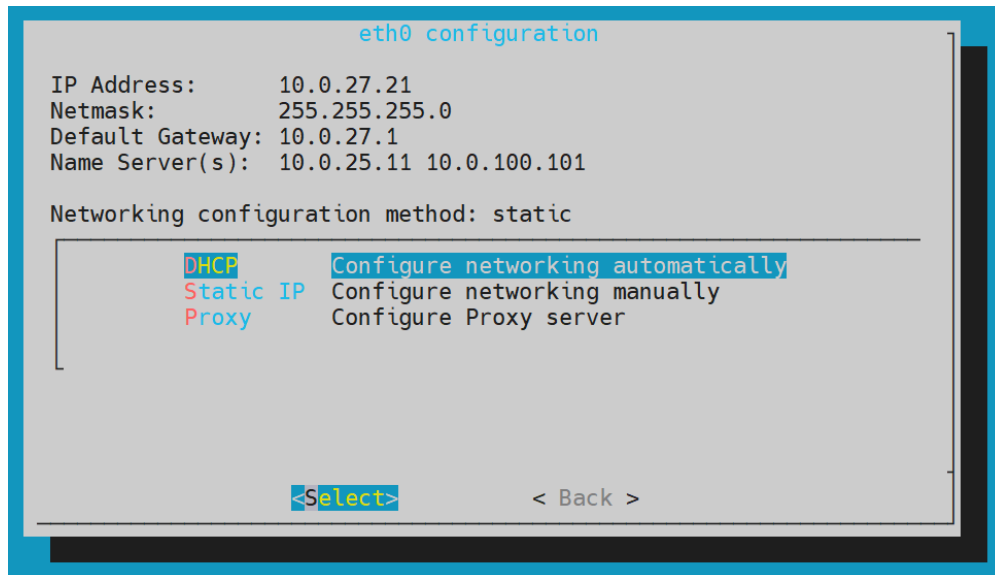
A setting console is available for easier configuration of **2N® Access Commander**.

- **Reboot** – restart the machine.
- **Shutdown** – shut the machine down.
- **Quit** – quit the configuration console and display the Linux terminal input.

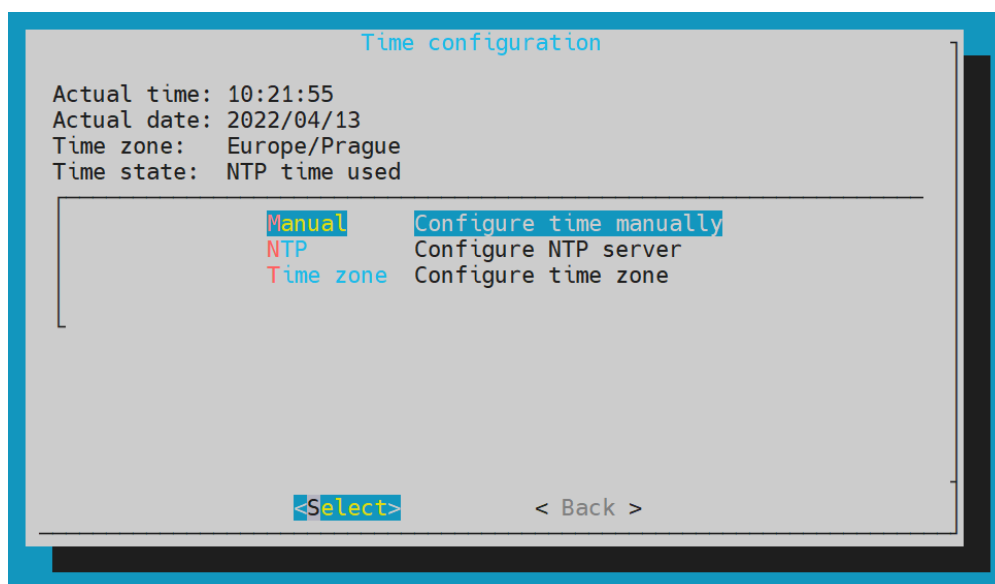


Set the basic Linux parameters:

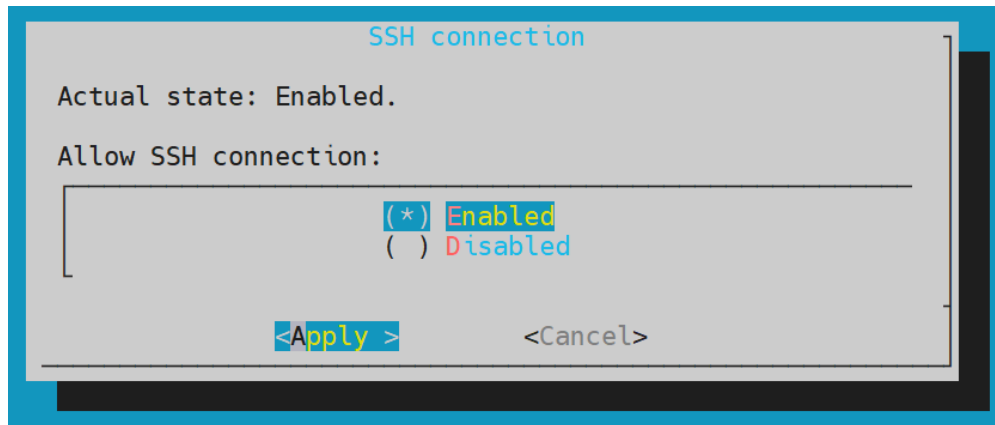
Networking – set the Proxy server and network parameters. Set the network parameters manually or via the **2N® Access Commander** DHCP server.



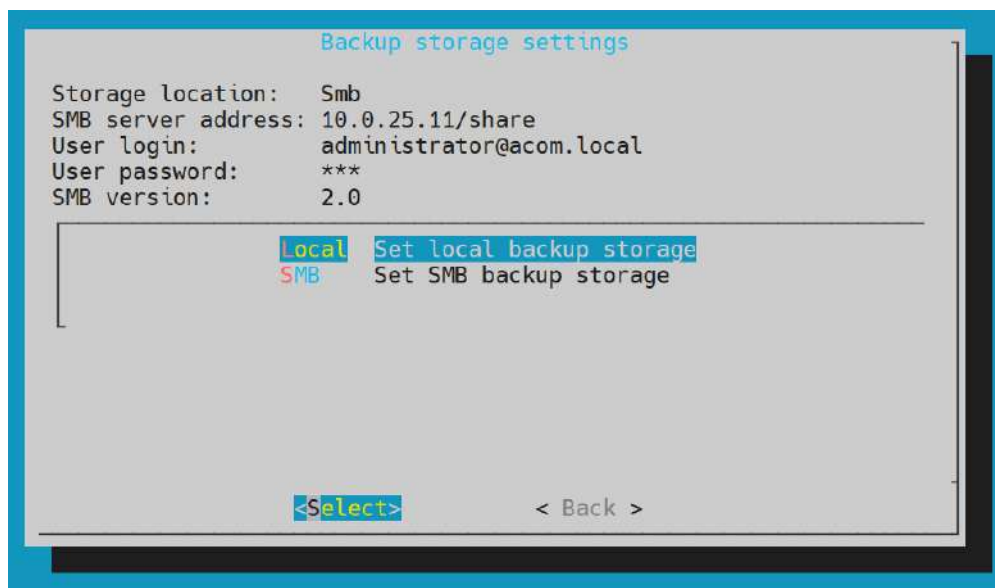
- **Time** – set the time, NTP server and time zone for **2N® Access Commander**. Ideally, the time zone should match the value set for the **2N® IP intercoms**.



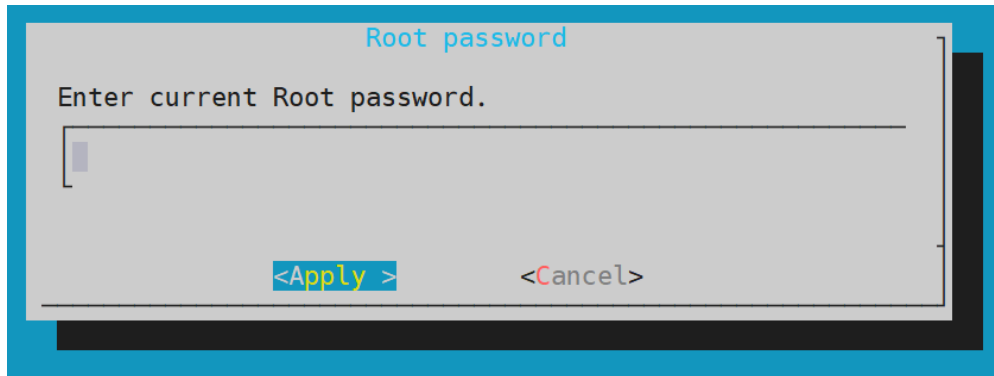
- **SSH** – set the SSH connection to the **2N® Access Commander** server. Make sure that a password is set for SSH that is different from the default one and meets the SSH requirements.



- **SMB** – enable the shared folder connection wizard. Set the IP address/domain name and folder path. E.g.: 192.168.1.1/share. Set the user name for folder access and right to write. Type the user password and select the Samba protocol version. Once all the mandatory parameters are set, the server connection is verified and the successful/wrong information is displayed.



- **Password** – set the root user account password. Use the password for Linus login or SSH access.

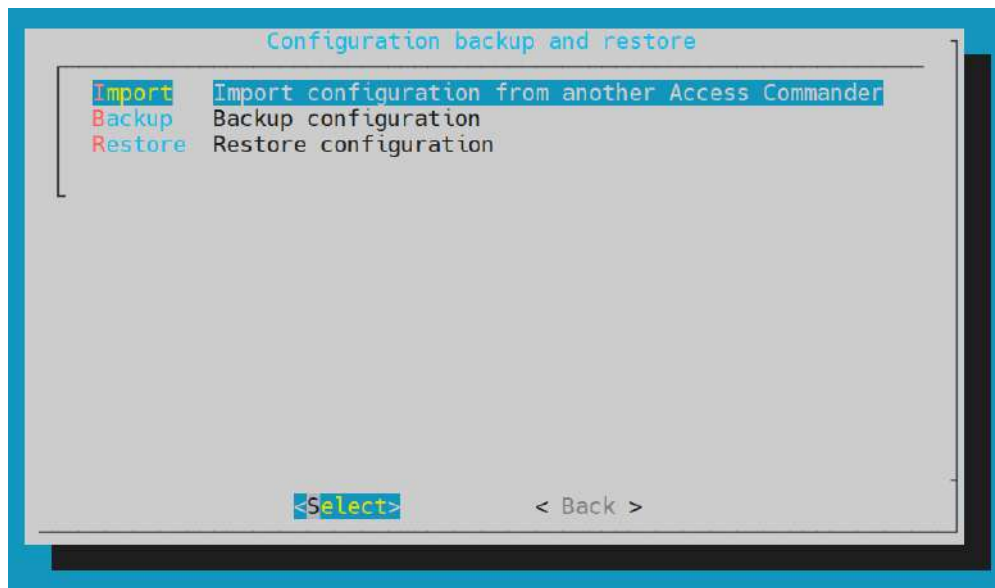


Root password

Enter current Root password.

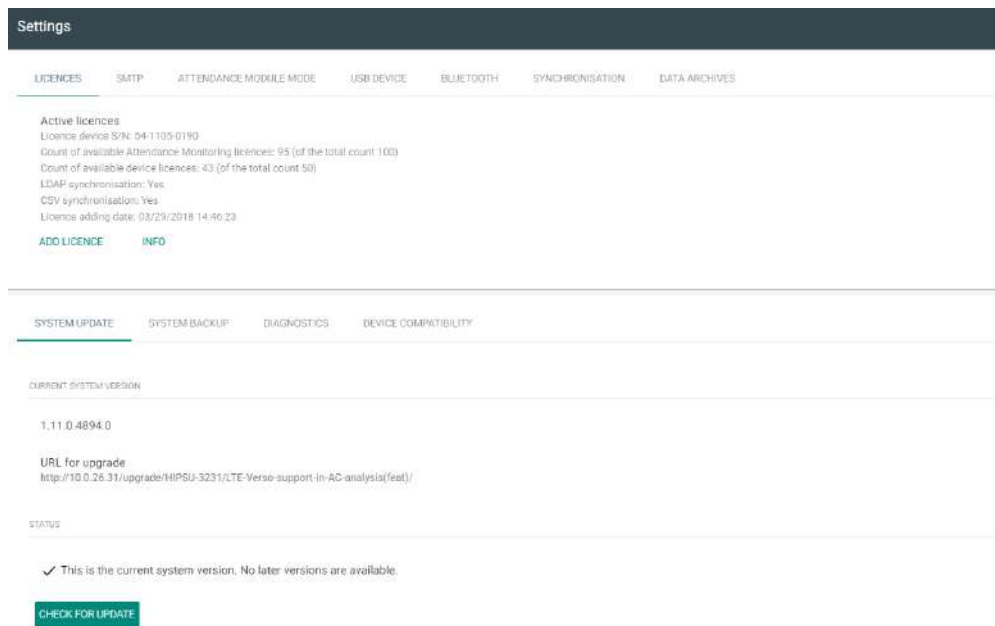
<Apply > <Cancel>

- **Backup and restore** – back up and restore the 2N® Access Commander data:
 - **Import** – import settings from another 2N® Access Commander
 - **Backup** – back up the current configuration and user list to a samba server
 - **Backup** – unrepeated backup
 - **Periodical backup** – backup period
 - Every day
 - Every week
 - Every month
 - Disabled
 - **Restore** – restore configuration from backup



Refer to [3.9 System Backup](#) for backup details.

3. System Setup



- [3.1 Licenses](#)
- [3.2 E-mail](#)
- [3.3 Attendance Module Mode](#)
- [3.4 USB Devices](#)
- [3.5 Bluetooth](#)
- [3.6 2N Picard](#)
- [3.7 Synchronisation](#)
- [3.8 Log Management](#)
- [3.9 System Update](#)
- [3.10 System Backup](#)
- [3.11 Diagnostics](#)
- [3.12 Date and Time](#)
- [3.13 Network Settings](#)
- [3.14 SSH](#)

3.1 Licenses

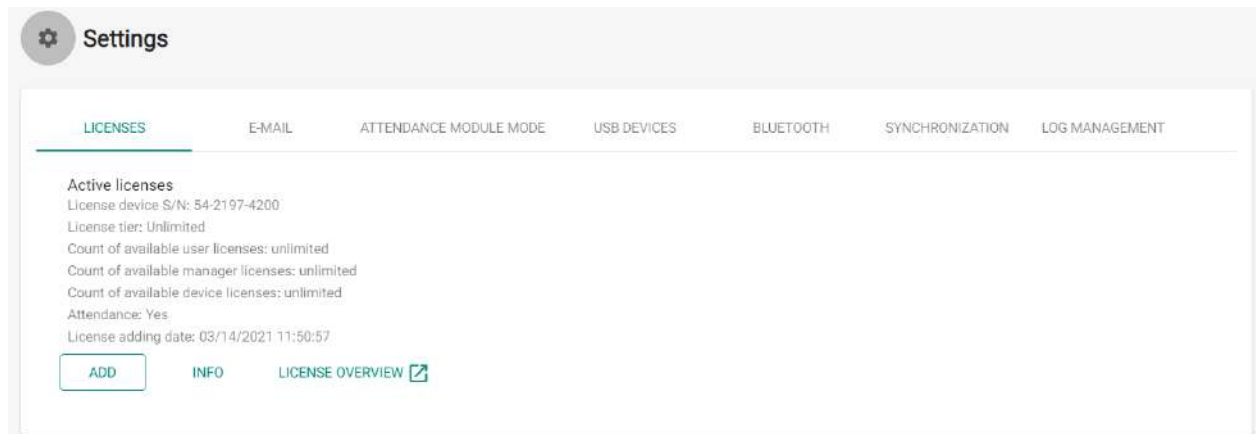
Use the License settings to see the current count of licensed devices, users and users with extended rights. Upon the initial installation of **2N® Access Commander**, a Trial license (see below for details) will be available. To manage more devices, users and users with extended rights order extended licenses. The following license types can be ordered:

	Basic (free)	Advanced	Pro	Pro Unlimited
Max directory users	50	300	1000	Unlimited*
Max (included) devices	5	30	100	Unlimited*
Max admins	1	5	Unlimited*	Unlimited*
Access, Event and System logs	✓	✓	✓	✓
Access Rules	✓	✓	✓	✓
API Access	✓	✓	✓	✓
Account enable/disable	✓	✓	✓	✓
Limit failed attempts	✓	✓	✓	✓
Silent alarm	✓	✓	✓	✓
Zone code	✓	✓	✓	✓
Device monitoring	✓	✓	✓	✓
Log management	✓	✓	✓	✓
Import from CSV or device	✗	✓	✓	✓
Bulk FW management	✗	✓	✓	✓
Multiple authentication support	✗	✓	✓	✓
User roles	✗	✓	✓	✓
Notifications	✗	✓	✓	✓
Presence	✗	✓	✓	✓
CAM Logs	✗	✓	✓	✓
Lift access control	✗	✓	✓	✓
Personalised dashboard	✗	✓	✓	✓

	Basic (free)	Advanced	Pro	Pro Unlimited
Lockdown	✗	✓	✓	✓
Mobile Credential Support	✗	✓	✓	✓
Visitor management	✗	✓	✓	✓
Occupancy management	✗	✗	✓	✓
Synchronization (LDAP & CSV)	✗	✗	✓	✓
Anti-passback	✗	✗	✓	✓
Attendance Monitoring	Optional	Optional	Optional	Optional
*For Unlimited within maximum capabilities of software platform see < 1.1.4 Recommended HW >				

Active Licenses

The section shows the count of required and owned licenses for the management of devices, users and users with extended rights. Including the last license adding date. Every license addition rewrites the original one. Licenses are not added up.

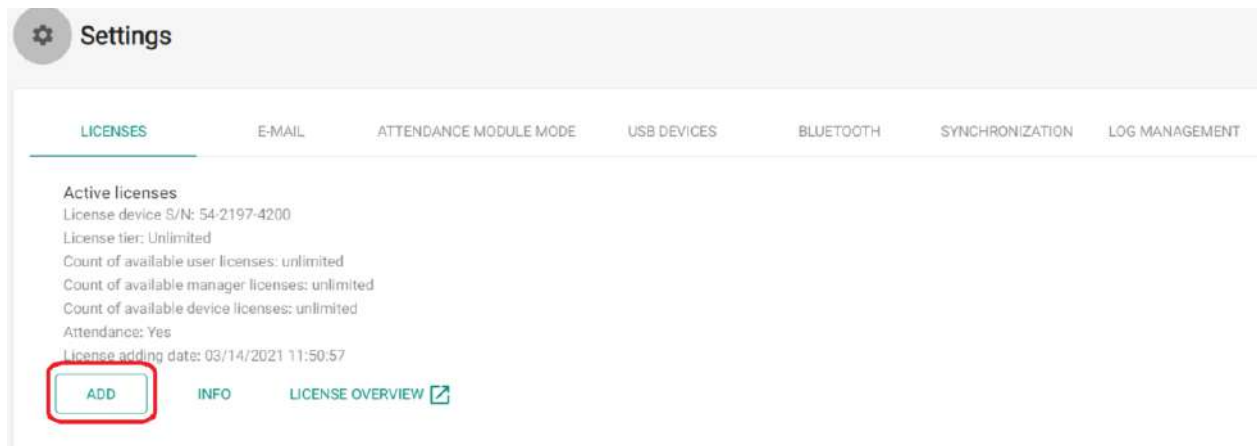


License Device S/N for License Generation

One of the connected devices (2N IP intercom, Access Unit, etc.) is used for license generation. Send the serial number to your distributor. A license will be generated and remain valid as long as the license device is connected (the device is used as a hardware key). When the license device is disconnected, a protective period will start running to keep the **2N® Access Commander** active. After the protective period, all the devices switch into the negative state and a new license has to be generated or the license device has to be reconnected to **2N® Access Commander**.

License Adding

The section helps you add a new license by reading the license file from your PC disk.



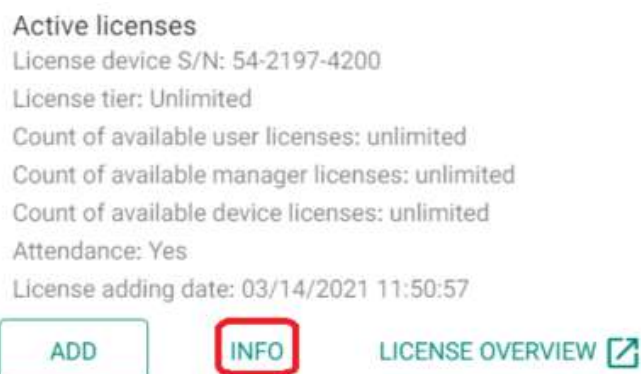
System without License

For testing purposes, a license will become active on the server upon installation with the following parameters:

- 1 device
- 5 users
- unlimited functions

License Expiration


A license expires when the license device is disconnected from **2N® Access Commander** for a long time. The time during which **2N® Access Commander** is functional depends on the time during which the license device was connected. The longer the connection time the longer the reconnection timeout. See the license detail for the license expiration date and time.



When the license expires, all the devices are switched into the inactive mode. Once a new license is added, first activate the device for which the license has been generated. The other devices cannot be activated until this license device is activated.

3.2 E-mail

The SMTP helps **2N® Access Commander** send e-mail messages. The module also provides [notifications](#) and sends the login password to the user.

LICENSES	E-MAIL	ATTENDANCE MODULE MODE	USB DEVICES	BLUETOOTH	SYNCHRONIZATION	LOG MANAGEMENT
<div>  SMTP on </div> <p>Make sure that SMTP is enabled and configured to use system e-mail notifications (user creation confirmation, e.g.).</p>						
SMTP SETTINGS						
Server Address mail.2n.cz		SSL Off				
Port 25		Validate SSL server certificate On				
User name Empty		Legacy mode (default Off) On				
Default sender address noreply@2nac.cz		<div>SEND TEST E-MAIL</div>				
HTTP SETTINGS						
Base address Off						

- **SMTP enable/disable** – enable/disable the e-mail sending service.

Click any parameter to change an SMTP setting. You can also send a test e-mail to verify the SMTP server configuration.

SMTP settings ×

Server Address*

mail.2n.cz

Port*

25

User name

Password

Default sender address*

noreply@2nac.cz

☐ SSL

☒ Validate SSL server certificate

☒ Legacy mode (default Off)

CANCEL CHANGE

- **Server address** – set the SMTP server address to which e-mails shall be sent.
- **Port** – specify the SMTP server port. Modify the value only if the SMTP server setting is substandard. The typical SMTP port value is 25.
- **User name** – enter a valid user name for login if the SMTP server requires authentication, or leave the field empty if not.
- **Password** – enter the password for the **2N® Access Commander** login to the SMTP server.
- **Default sender address** – set the sender address for all outgoing e-mails from **2N® Access Commander**.
- **SSL** – enable/disable e-mail encryption.
- **Validate SSL server certificate** – verify the SSL server certificate.
- **Legacy mode (default Off)** – connect to older SMTP servers that do not support the new functions.

Caution

- In case the set SMTP server does not have a valid certificate, no connection is established. The user is notified thereof when the test e-mail is sent.

HTTP SETTINGS

Base address
Off

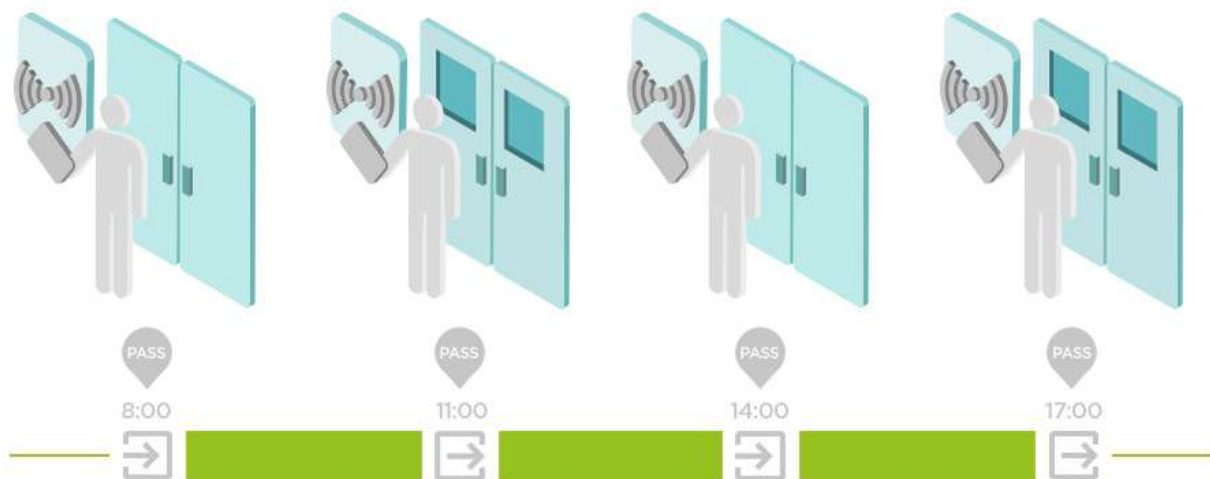
- **Base address** – if enabled, the e-mails contain a direct password resetting link.
Links in e-mails: Off

3.3 Attendance Module Mode

2N® Access Commander treats Attendance in two modes:

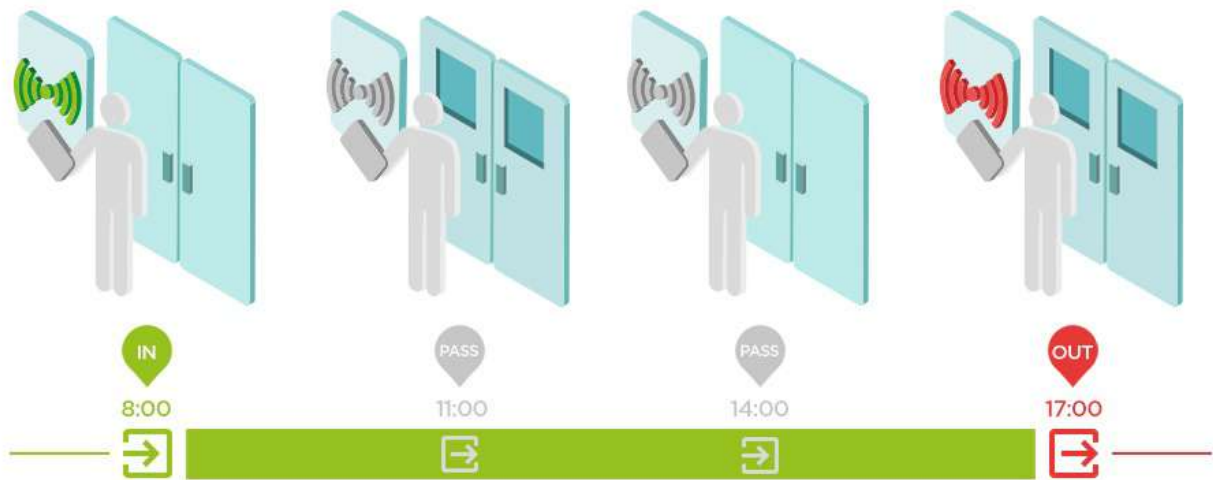
FREE mode

Arrivals/departures in the FREE mode are recorded by the first/last use of a 2N reader during the day. The Presence module does not work in this mode.



IN-OUT mode

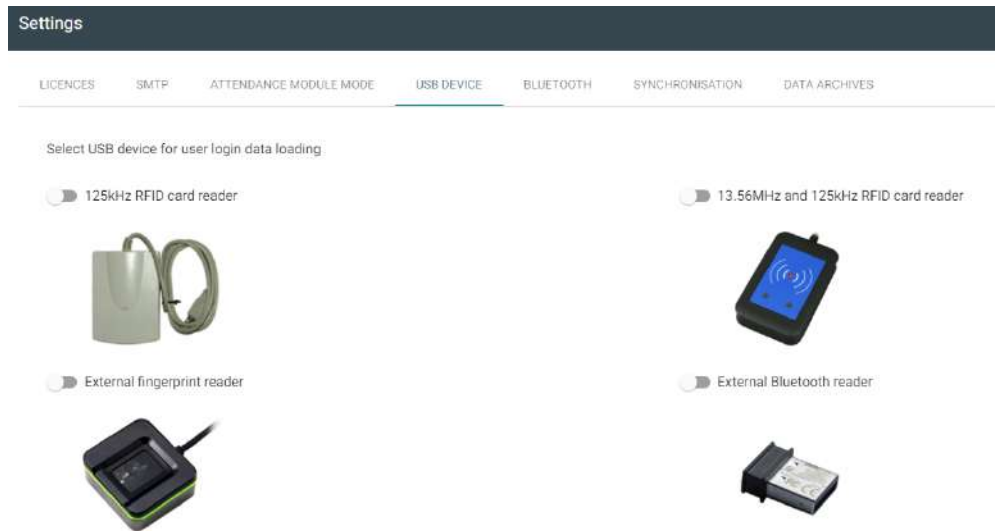
Arrivals/departures in the IN-OUT mode are always recorded by the arrival/departure reader (as set on the device). Use this mode to make the Presence module work properly.

**Note**

- IN/OUT for all devices – attendance is monitored for all the readers that the user may use for access. Movement between zones will not be recorded as attendance arrival/departure.
- IN-OUT for selected devices – attendance is monitored for selected readers only, e.g. at the main building entrance.

3.4 USB Devices

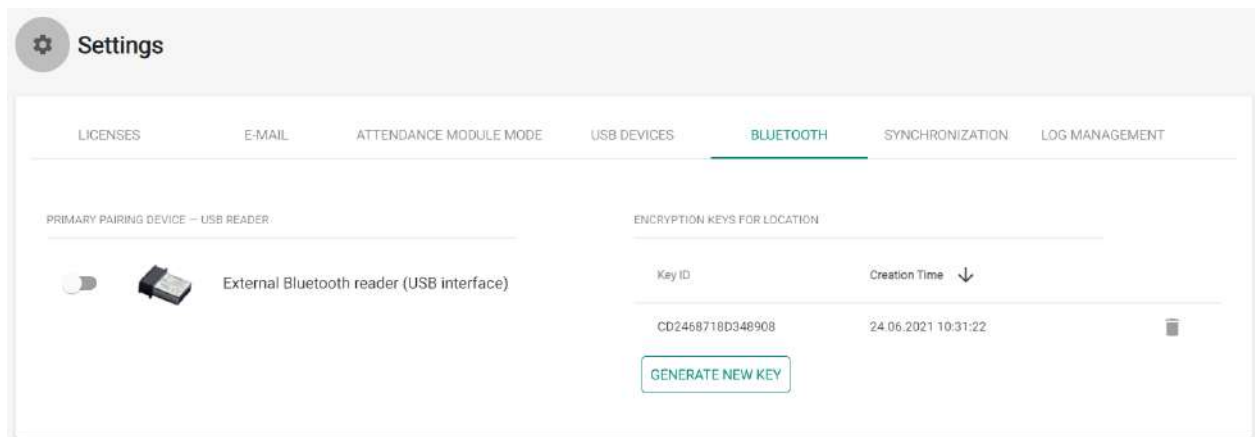
External USB devices are enabled/disabled in this mode. Once disabled, a device cannot be used for loading user access data.



- **125 kHz RFID card reader**
 - Part No. 9137420E
- **13.56 MHz and 125 kHz RFID card reader**
 - Part No. 9137421E
- **External fingerprint reader**
 - Part No. 9137423E
- **External Bluetooth reader**
 - Part No. 9137422E

3.5 Bluetooth

Use the Bluetooth settings to enable/disable the use of an external reader and manage the encryption keys for locations.



- **Encryption keys for location** – the **2N® Mobile Key** - intercom communication is always encrypted. **2N® Mobile Key** cannot authenticate a user without knowing the encryption key. The primary encryption key is automatically generated upon the first start of the intercom and can be re-generated manually any time later. Together with Auth ID, the primary encryption key is transferred to the mobile device while pairing.

3.6 2N Picard

The 2N® PICard technology is used for encrypting login data on access cards. To read the login data, the 2N devices need access to the keys generated by the 2N® PICard Commander application. The keys are then imported to 2N® Access Commander for distribution to all of the supported 2N devices.

The screenshot shows the '2N PICARD' tab in the software interface. It displays the 'PICARD READ KEYS' section with the following details:

- Project name:** Testing Project
- Hash:** 51012195
- Buttons:** IMPORT and REMOVE

- **Project name** – name of the encryption key created.
- **Hash** – numerical project code.

3.7 Synchronisation

Synchronisation via a CSV file.

The screenshot shows the 'Settings' window with the 'SYNCHRONIZATION' tab selected. It is divided into two main sections: 'SYNCHRONIZATION' on the left and 'INFO' on the right.

SYNCHRONIZATION Section:

- FTP storage:** Empty
- Automatic synchronization:** Neaktivní – FTP úložiště není nastaveno
- Buttons:** SYNCHRONIZE FROM STORAGE and SYNCHRONIZE FROM FILE

INFO Section:

- Last synchronization:** Nesynchronizováno
- Next synchronization at (server time):** Automatická synchronizace nenastavena.
- Current synchronization status:** Nesynchronizováno
- Information:** Synchronization results are stored in the system log.
- Links:** SHOW SYSTEM LOGS and SAMPLE CSV FILE DOWNLOAD

There are two ways of CSV synchronisation.

1. Synchronise from file:

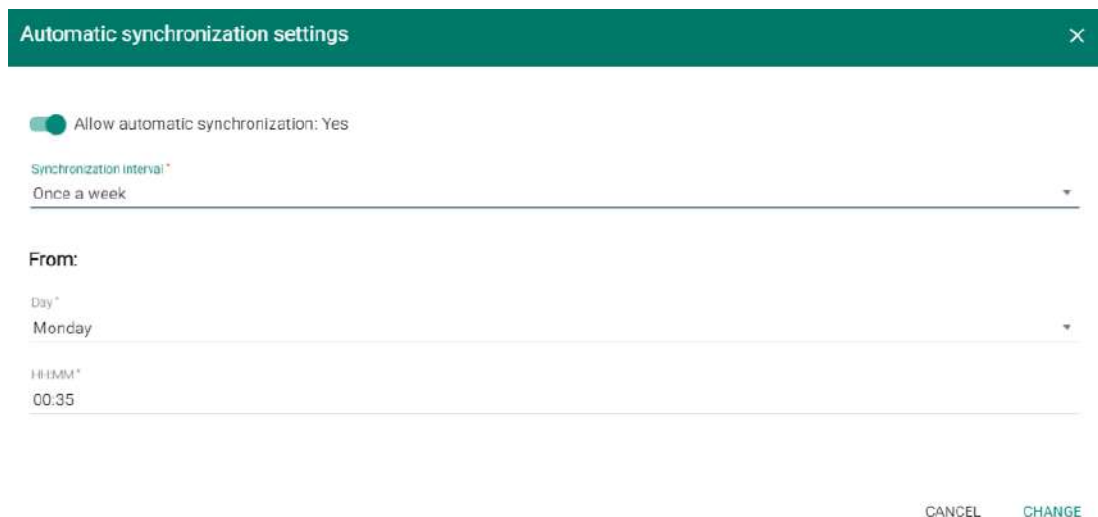


Synchronisation from local file

Select file **SELECT**

CANCEL **SYNCHRONISE WITH**

- a. Create a CSV file as follows:
 - b. Select a synchronisation file and click Synchronise.
2. Synchronisation via a storage:
- a. Set connection to the FTP storage



Automatic synchronization settings

☒ Allow automatic synchronization: Yes

Synchronization interval: *

Once a week

From:

Day *

Monday

HH:MM*

00:35

CANCEL **CHANGE**

- i. **Automatic synchronisation enable**
 - ii. **Synchronisation interval** – set the interval for **2N® Access Commander** synchronisation with the FTP storage. The following options are available: Once an hour, Once a day and Once a week.
 - iii. **From** – set the synchronisation date and time.
- b. Automatic synchronisation setting

Automatic synchronisation settings

☐ Allow automatic synchronisation

From:

4/11/2018

Time *

13:48

Synchronisation interval *

Once per day

CANCEL CHANGE

- i. **Automatic synchronisation enable**
- ii. **From** – set the synchronisation date and time.
- iii. **Synchronisation interval** – set the interval for 2N® Access Commander synchronisation with the FTP storage. The following options are available: Once an hour, Once a day and Once a week.

3. Information:

- a. **Last synchronisation** – display the last synchronisation date and time.
- b. **Next synchronisation at (server time)** – display the next synchronisation date and time.
- c. **Current synchronisation state** – display the last synchronisation result.

CSV template:

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,User Name,Company,User Mail,Card Numbers,Switch Code,Phone Number 1,Group Call,Phone Number 2,Group Call,Phone Number 3,Virtual Number,Groups,Is Deleted

- **EmployeeID** – enter the primary key to be fulfilled every time. It is a unique user identifier.
- **User Name** – enter the user created in 2N® Access Commander.
- **Company** – enter the company to which the user is assigned. Make sure that the company is created in 2N® Access Commander. Lower and upper case letters in company/group names are not interchangeable.
- **User Mail** – set the user mail.
- **Card Numbers** – enter the user card ID. Up to two cards can be set per user separated with a semicolon (;).

- **Switch Code** – set the switch code; the code is always set for switch 1.
- **Phone Number 1** – enter the phone number for position 1.
- **Group Call** – set the phone number for group calls. 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** – enter the phone number for position 2.
- **Group Call** – set the phone number for group calls. 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** – enter the phone number for position 3.
- **Virtual Number** – enter the user virtual number.
- **Groups** – fill in the list of groups to which the user is to be assigned. Make sure all the companies are created in **2N® Access Commander**. The group list is separated with a semicolon. Lower and upper case letters in company/group names are not interchangeable.
- **Is Deleted** – the user has been deleted. If FALSE is selected, the user is created and its data only updated at the next synchronisation. If TRUE is selected, the user is deleted at the next synchronisation. If FALSE is selected, the user is recreated.
- **Licence Plates** – set a licence plate. Multiple license plates, if any, have to be separated with a semicolon.

Synchronisation logs:

Refer to the system log for detailed information on each synchronisation result. The log just informs whether or not the synchronisation was successful. Click the icon at the end of the row to display detailed information.

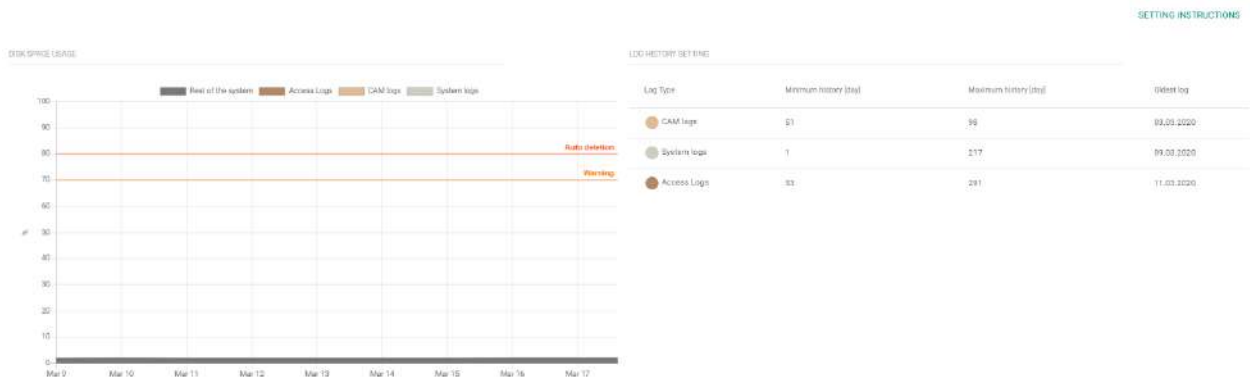
System logs		UPGRADE NOW
FROM:	DD/MM/YY HH:MM	TO: 11/04/2018 HH:MM
	EVENT TYPE	DEVICE
	WARNING LEVEL	
Time	Description	
 11.04.2018 13:47:35	Synchronization failed: FTP Status: ProtocolError, Message: Server returned an error: 530 Login or password incorrect!	
 11.04.2018 13:47:12	Synchronization failed: FTP Status: ProtocolError, Message: Server returned an error: 530 Login or password incorrect!	
 11.04.2018 13:46:27	Synchronization failed. Exception Message: Invalid URI: The format of the URI could not be determined.	
 11.04.2018 13:45:47	Synchronization failed. Exception Message: Invalid URI: The format of the URI could not be determined.	
 11.04.2018 13:45:44	Synchronization failed. Exception Message: Invalid URI: The format of the URI could not be determined.	
 11.04.2018 13:15:13	Info: License authentication succeeded. Device used for licensing: 2N Access Unit (S/N: 54-1105-0190, IP: 10.0.25.136)	
 11.04.2018 12:19:13	Info: License authentication succeeded. Device used for licensing: 2N Access Unit (S/N: 54-1105-0190, IP: 10.0.25.136)	
 11.04.2018 11:14:13	Info: License authentication succeeded. Device used for licensing: 2N Access Unit (S/N: 54-1105-0190, IP: 10.0.25.136)	
 11.04.2018 10:44:18	Info: Switch 1 state changed on device 2N Helios IP Verso Ondra (S/N: 54-0917-0075, IP address: 10.0.25.133-443) - state: "False" at 04/11/2018 08:44:18(UTC).	
 11.04.2018 10:44:08	Info: Switch 1 state changed on device 2N Helios IP Verso Ondra (S/N: 54-0917-0075, IP address: 10.0.25.133-443) - state: "True" at 04/11/2018 08:44:08(UTC).	
 11.04.2018 10:35:48	Info: Registration state changed on SIP account 1 on device 2N Helios IP Base (S/N: 54-1685-0483, IP address: 10.0.25.151-443) - state: "registered" at 04/11/2018 08:35:48(UTC).	

Caution

- Lower and upper case letters in company/group names are not interchangeable.
 - Example: "My Company" and "my company" are interpreted as different company names.

3.8 Log Management

Here you may set the maximum duration for which logs will be stored. Logs older than the maximum history value will be discarded. You may use this setting to comply with your GDPR obligations. Consider lowering this value if your disk space usage reaches 70 %. The table also provides the date of the oldest log currently recorded for each log type.



Disk Space Usage:

- **Rest of the system** – linux part and applications.
- **Access logs** – records including access logs.
- **CAM logs** – records including CAM logs.
- **System logs** – records including system logs.

Log History Settings

Auto-deletion will be triggered if the disk space usage reaches 80%. You can set the minimum history for which logs must be stored and the order by which each log type may be deleted. Starting with the first log type in your chosen order, logs will be deleted incrementally until the disk space usage falls to 75 % or until the minimum history of the log type is reached.

Note

- The maximum CAM log history may not be longer than the maximum history of system or access logs.

3.9 System Update

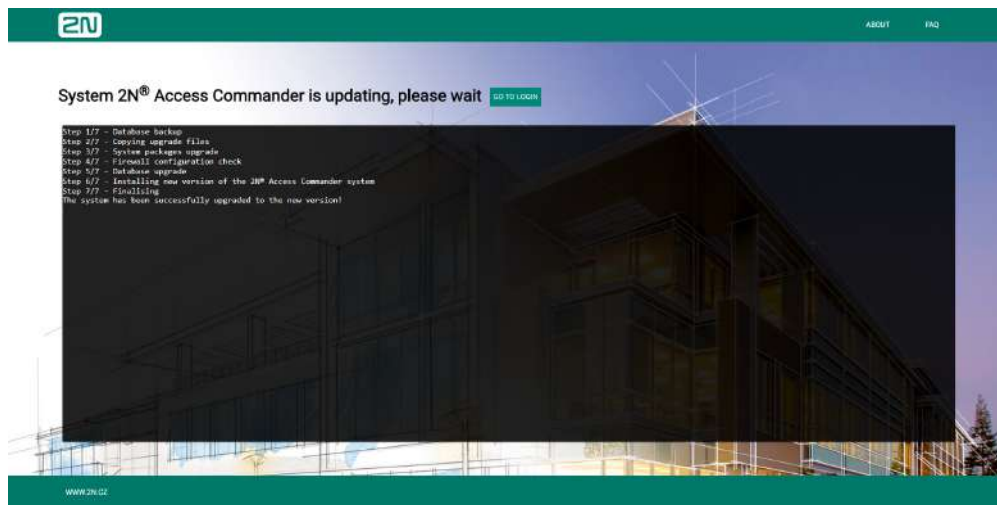
You are notified that a system update is available in the Settings.

The screenshot shows the 'SYSTEM UPDATE' tab selected in a settings menu. Below the tab bar, there are three sections: 'CURRENT SYSTEM VERSION' showing '1.13.0.19583.0', 'URL for upgrade' with the link 'https://update.2n.cz/accesscommander/', and 'STATUS' which displays a green checkmark and the text 'This is the current system version. No later versions are available.' At the bottom of the status section is a green button labeled 'CHECK FOR UPDATE'.

Click Download file to download the update file to **2N® Access Commander** for installation. Click Install to start installation.

This is an identical duplicate of the screenshot above, showing the 'SYSTEM UPDATE' settings page with the current version 1.13.0.22879.0 and a 'CHECK FOR UPDATE' button.

When the installation starts, you will be redirected to the maintenance page. Here the update initiating administrator will be informed of the update progress. The other users will be notified of the update and will be unable to log in to **2N® Access Commander**.



Page displayed to administrator during update



Page displayed to user during update

When the update is completed, the Go to login button becomes active again and the users can click to go to the login screen.

3.10 System Backup

System Backup helps you back up and restore the **2N® Access Commander** data.

SYSTEM UPDATE	SYSTEM BACKUP	DIAGNOSTICS	DATE AND TIME	NETWORK SETTINGS	SSH
---------------	---------------	-------------	---------------	------------------	-----

BACKUP			
Storage 10.0.25.11/share	Periodic backup Daily		
BACKUP NOW			
Backup date	Size	Location	AC version
Apr 13, 2022 12:00:07 PM	17.17 MB	Smb	2.4.0.199
Apr 13, 2022 9:15:58 AM	14.24 MB	Smb	2.3.0.990
Apr 12, 2022 9:16:07 AM	14.19 MB	Smb	2.3.0.990
Apr 11, 2022 9:15:18 AM	14.14 MB	Smb	2.3.0.990
Apr 10, 2022 9:15:32 AM	14.08 MB	Smb	2.3.0.990

Page 1 1 - 5 of 76 < >

Data can be stored in a local storage or samba server. The samba server is suitable for long-time backups. Complete the samba server address, login name and password as well as the protocol version to use the samba server as a backup storage.

Set up storage

Storage

SMB

Server address *

10.0.25.11/share

Login name *

Administrator

Password

Protocol version

2.0

CANCEL

SAVE

The system backups can be stored periodically or outside the periodic backup time.

Set the time frequency (daily, weekly, monthly) and backup day and time. If you want to encrypt the system backup file, create a password for the encrypted backup.

Periodic backup time

Frequency

Daily

Backup time *

12:00

☒ Encrypt backup file

Backup password *

Repeat password *




CANCEL

SAVE

Press the BACKUP NOW button to store an immediate system backup outside the set periodic backup time. The backup will be added to the backup list.

Backup date	Size	Location	AC version
Apr 13, 2022 12:00:07 PM	17.17 MB	Snb	2.4.0.159
Apr 13, 2022 9:15:58 AM	14.24 MB	Snb	2.3.0.590
Apr 12, 2022 9:16:57 AM	14.19 MB	Snb	2.3.0.590
Apr 11, 2022 9:15:16 AM	14.14 MB	Snb	2.3.0.590
Apr 10, 2022 9:15:32 AM	14.08 MB	Snb	2.3.0.590

Page: 1 1 - 5 of 76

-  – restore a selected system backup file.
-  – download a selected system backup file.
-  – remove a selected system backup file.

You can restore the system data not only from the stored system backups but also from an external file or another installation.

To restore data, select the file target destination or simply drag the file to the Restore from file field. The maximum allowed size of the file to be uploaded is 2 GB.

RESTORE FROM FILE

RESTORE

To import data from another installation, complete the other **2N® Access Commander** IP address and enter the user name and password for SSH connection. I.e. the root password on the source machine.

Import from another installation



IP address *

Username *

root

Password *

Note

- To import data from another **2N® Access Commander** installation, make sure that SSH is enabled on the data transferring server.

Caution

- Data can only be imported from an older or identical **2N® Access Commander** version. Data cannot be imported from a new version to an earlier one.
- The import will replace all your data and system settings. After the import, the source installation can no longer be used.
- The system will not be available during the import. Depending on how much data you have, this may take a while.

3.11 Diagnostics

Diagnostics is used for **2N® Access Commander** troubleshooting.

SYSTEM UPDATE

SYSTEM BACKUP

DIAGNOSTICS

DIAGNOSTIC LOGS

Diagnostic logs are intended for troubleshooting with the manufacturer's technical support.

Current state

Log package does not exist, create one.

CREATE LOGS

DOWNLOAD LOGS

USAGE STATISTICS

☐ Send anonymous data

INFO

- **Diagnostic logs** – click Create logs to collect system logs, which may take a few minutes. Having completed acquisition, the system offers download of diagnostic logs. The logs are intended for communication with the manufacturer's technical support staff.
- **Use statistics** – enable sending of anonymous statistic data on the device use to the manufacturer. The data does not contain any sensitive information such as passwords, access codes or phone numbers. 2N TELEKOMUNIKACE a.s. uses this information to improve its software quality, reliability and performance. Your participation is voluntary and you can disable sending of statistic data any time.

3.12 Date and Time

Date and Time helps you set the date and time parameters. If **2N® Access Commander** is not connected to the Internet, set the time zone, date and time manually. If connected, set the time zone only. The NTP server updates date and time automatically.

SYSTEM UPDATE SYSTEM BACKUP DIAGNOSTICS **DATE AND TIME** NETWORK SETTINGS SSH

⌚ If 2N® Access Commander is not connected to the internet, you need to set your time zone, date, and time manually.
If it is connected, just set your time zone. The NTP server will automatically update the date and time.

Time zone
Europe/Prague

Configuration method
NTP

Current time
08:51:20

Current date
2022/11/15

SYNCHRONIZATION WITH DEVICES

Mode
Do not synchronize

Caution

- Whenever a time setting is changed, **2N® Access Commander** is automatically restarted.

The Mode section helps you synchronize the set data with the connected devices.

- **Do not synchronize** – the device time shall be governed by the respective setting of each device.
- **Distribute Access Commander NTP server to devices** – the device time shall be governed by the NTP server set in **2N® Access Commander**.
- **Synchronize with Access Commander time** – the device time shall be governed by the time value set in **2N® Access Commander**.

3.13 Network Settings

Network Settings helps you set the **2N® Access Commander** network parameters.

SYSTEM UPDATE

SYSTEM BACKUP

DIAGNOSTICS

DATE AND TIME

NETWORK SETTINGS

SSH

Configuration method

Manual

IP Address

10.0.27.22

Subnet mask

255.255.255.0

Default gateway

10.0.27.1

Name servers

10.0.25.11, 10.0.100.102

EDIT PROXY SERVERS

The Configuration method helps set the network parameters automatically from the DHCP server or manually. When the IP address automatically obtained from the DHCP sever is changed into a manually set address, the web browser redirects you to the set IP address. After redirection, **2N® Access Commander** is restarted and you are required to relog in the system.

Proxy configuration

X

☐ Configure using DHCP (automatic)

☒ Manual IP address configuration

IP Address*

10.0.27.22

Subnet mask*

255.255.255.0

Default gateway

10.0.27.1

Name server

10.0.25.11

Name server 2

10.0.100.102

CANCEL

CHANGE

Caution

- By changing the configuration method to DHCP you also change the server IP address, which may result in a connection loss.

The Network Settings folder also allows you to edit the Proxy server parameters (HTTP Proxy, HTTPS Proxy, FTP Proxy, Socks Proxy).

A dialog box titled "Proxy configuration" with a close button (X) in the top right corner. It contains four input fields labeled "HTTP Proxy", "HTTPS Proxy", "FTP Proxy", and "Socks Proxy". At the bottom right, there are two buttons: "CANCEL" and "CHANGE".

Proxy configuration

HTTP Proxy

HTTPS Proxy

FTP Proxy

Socks Proxy


CANCEL CHANGE

Caution

- When you change the HTTP proxy server, **2N® Access Commander** will automatically restart.

3.14 SSH

The SSH folder allows you to enable the SSH protocol to ensure a secure remote connection to the system console. With SSH enabled, you can back up and restore the system or restart **2N® Access Commander**.

A screenshot of the SSH configuration interface. At the top, there is a navigation bar with tabs: "SYSTEM UPDATE", "SYSTEM BACKUP", "DIAGNOSTICS", "DATE AND TIME", "NETWORK SETTINGS", and "SSH". The "SSH" tab is selected. Below the tabs, it says "SSH service" and "Enabled". To the right, there are two buttons: "CHANGE PASSWORD" and "DISABLE".

SYSTEM UPDATE SYSTEM BACKUP DIAGNOSTICS DATE AND TIME NETWORK SETTINGS SSH

SSH service
Enabled

CHANGE PASSWORD DISABLE

Upon the first activation of SSH, a password setting dialog is automatically displayed. The next password change must be set manually. A root user password change is not performed in **2N® Access Commander**, but in Linux.

Note

- We strongly recommend that the SSH access should only be enabled for experienced users to avoid security risk.

4. System Administration

- [4.1 Companies](#)
- [4.2 Users](#)
- [4.3 Groups](#)
- [4.4 Devices](#)
- [4.5 Zones](#)
- [4.6 Time Profiles](#)
- [4.7 Access Rules](#)
- [4.8 Lockdown](#)

4.1 Companies

What Is a Company Used For?

Within one installation, divide the **2N® Access Commander** settings into companies to prevent the managers of one company from seeing the users of the other company. This method also enables common building facilities to be shared by multiple companies (entrances, lifts, restaurants, meeting/conference rooms, etc.).

Company list



Name ↑	Zones		
Company0	test, test5, Zone10...		
Company1	test, test5, Zone0...		

Company creation

1. Select the **Company** card.
2. Select **Companies – Create** (Add button).
3. Enter **Company name** and click Create.

Company details

General settings

- **Company name** – edit the company name.
- **Default application language** – set the default application language for all of the company users. A new user can change the default language in its profile (if login is created).

Holidays

- **Holidays** – set the company holidays for monthly balance computation. The hours worked on holidays are counted as hours worked on weekends (i.e. above the common working hours).
- **Copy holidays** – copy holidays from another company. Go to the company to which holidays are to be copied and select the company from which holidays are to be copied. Just click Save. Holidays are copied including dates and names. You can copy holidays repeatedly, but if the holiday to be copied is already listed, only the holiday name is rewritten. If unlisted, the holiday is added.

Attendance Mode

- **Working days** – workday selection.
- **Common working hours** – set the common working hours (from – to) for company user Attendance balance computation. If you set from 8 a.m. to 4,30 p.m., the working hours include 8 hours plus a 30-minute lunch break. If a user works less than 8 hours and 30 minutes per day, its account will show a negative balance for that day.

Visitors

- **Default groups for new visitor** – set the groups that will be automatically assigned to a new visitor when this company has been selected.

E-mail

- **Company colors**
 - **Background color** – select the header background color for the e-mail to be sent.
 - **Foreground text color** – select the header foreground color for the e-mail to be sent.

Tip

- The e-mail header preview shows the final appearance of the e-mail to be sent.

- **Restore default** – restore the default header appearance.

E-MAIL TEMPLATES	
Template name	
Visitor PIN code	
Visitor QR code	
User PIN code	
User QR code	

- **E-mail templates** – display the list of available e-mail templates. Use a template to set the e-mail subject, header, salutation, complementary text and signature. The e-mail preview shows the final appearance of the e-mail to be sent. You can send a test e-mail to the set e-mail address to check the e-mail appearance.
 - Visitor PIN code
 - Visitor QR code
 - User PIN code

- User PIN code

Bluetooth

- **Pairing time** – set the pairing time.
- **2N device for initial pairing with smartphone** – make sure that at least one device equipped with a Bluetooth module is added to **2N® Access Commander**. And that the device is added to the zone assigned to the user company.

The pairing time starts running when you press Generate on the user and the PIN is displayed. In this window, you can enable the use of the USB dongle for pairing. Having set all the parameters, click OK. You will be redirected to the user list for user selection. Refer to [4.2.1 Bluetooth](#).

Zones

- **Company zones** – assign zones to a company to define the set of facilities to be used by the company users (e.g. the Common space and 4th floor zones, which include the reception entrance door and all 4th floor entrances). One zone can be assigned to multiple companies and one company can be assigned more zones.

Data Import

- **User import from device** – import users from a selected device.
- **User import from CSV file** – import users and groups from a CSV file.
- **Download CSV template file** – download a CSV template file for user import.

User import from device

- Importing users who have been assigned Bluetooth credentials requires replacing any existing keys in Access Commander. This means the Bluetooth credentials of existing users in Access Commander will stop functioning and those users must go through Bluetooth pairing again.

LDAP

LDAP is used for downloading users from the external Active Directory. For more information on how to set LDAP in **2N® Access Commander**.

ZONES

DATA IMPORT

LDAP

IMPORT

Periodical import time
Inactive

Last import status
Successfully completed [20.11.2020 15:51:32]

IMPORT

SERVER SETTINGS

Server name
10.0.25.11

Port
389

Login name
administrator@acom.local

Password

Use SSL

LDAP SCHEMA

Base DN
OU=test,DC=acom,DC=local

ADVANCED SETTINGS

Nested search

Follow referral

Import user's photo

Disable users when disabled in Active Directory

Treating removed users
Deleted

Pagination
Page Size: 1000

CUSTOM USER SCHEMA SETTINGS

DELETE CONFIGURATION

VALIDATE LDAP CONFIGURATION

See below for more LDAP setting details:

- [4.1.1.1 LDAP](#)

55 / 149

4.1.1 LDAP

LDAP synchronization is used for downloading users and their changes (user name, user ID, card, PIN code, image, e-mail, phone number, password and login, license plate) from an external LDAP system. The behavior of the users deleted from external LDAP systems obeys the setting of the "Treated removed users" parameter. The behavior of the deactivated users in the Active Directory obeys the setting of the "Disable users when disabled in Active Directory" parameter.

- Synchronization
 - a. Scheduled synchronization time
 - Define when **2N® Access Commander** shall send a query to the LDAP server regarding user changes.
 - b. Last synchronization state
 - Display information on the last synchronization state. Whether it ended with an error or went successfully in accordance with the time of the action.
 - c. Synchronize button
 - Click the button to start synchronization immediately. The administrator thus need not wait for scheduled synchronization.

- Server settings
 - a. Server name
 - If DNS is set properly, enter the server name (**WIN-9ABEB4AUOHD**).
 - If DNS is unset, fill in the IP address of the server on which LDAP is running.
 - b. Port
 - The LDAP port is 389 (without SSL) by default. If you want to use encrypted connection in your company, enter port number 636. The SSL support must be on the LDAP server side too.
 - If set differently by the administrator, the port number must be changed in **2N® Access Commander** too.
 - c. Login name
 - Login name of the user with appropriate rights to the root or the whole tree. Enter the login name as follows: administrator@domain.com
 - d. Password
 - LDAP server user password.
 - e. Use SSL
 - If SSL is disabled, it is unnecessary to rewrite the port number.
 - If SSL is enabled, it is necessary to rewrite the port number to 636.
 - f. Delete configuration button
 - Click the button to delete all the settings. The earlier loaded users are not deleted.
 - g. Test LDAP setting
 - Verify the LDAP setting.
- LDAP schema
 - a. Base DN
 - This is the root point from where the directory search starts. It can be an extension or a root, for example:
CN=administrator,CN=users,DC=domain,DC=com
- Advanced Settings
 - a. Nested search
 - With nested search, not only the root, but the whole tree is searched.
 - b. Follow referral – enable the LDAP Referral function.
 - c. Import user's photo – import the user photo from the LDAP system.
 - d. Disable users when disabled in Active Directory – deactivate the **2N® Access Commander** users while synchronization, who were disabled in the Active Directory.
 - e. Synchronize group membership – load group membership from LDAP to **2N® Access Commander**.
 - f. Treating removed users – define how to treat the users removed from an external system.
 - g. Pagination – pagination uses the Simple Paged Results Control LDAP extension, allowing results to be split into pages for synchronization with larger directories.
 - h. Custom user schema settings – use the schema to define selected attributes set in the LDAP system.

- i. Group schema settings – refer to another LDAP tree place using own Base DN settings and import nested groups.

Note

- Make sure that the **91379042 2N® Access Commander – Integration License** has been purchased and added so that the LDAP company tab can be accessible.

Tip

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

4.2 Users

- [4.2.1 Bluetooth](#)

User List

The user list shows all users added to **2N® Access Commander**. You can filter users by companies or just find a user by its name, e-mail or phone number.

Users	Companies	E-Mail	Phone Number
<input type="checkbox"/> John Blake	My Company		1485
<input type="checkbox"/> System admin		tabor@2n.cz	
<input type="checkbox"/> Test	My Company		
<input type="checkbox"/> User01	My Company	tabor@2n.cz	1100
<input type="checkbox"/> User02	My Company	tabor@2n.cz	1101
<input type="checkbox"/> User03	My Company	tabor@2n.cz	1102
<input type="checkbox"/> User04	My Company	tabor@2n.cz	1103
<input type="checkbox"/> User05	My Company	tabor@2n.cz	1104

Stránka: 1 Počet řádků na stránku: 15 1-8 z 8

The following bulk actions can be used:

- Add user to group
- Bulk delete user
- Set access time restrictions

Add user to 2N® Access Commander

1. Select the **Users** card.

2. Select **Users – Create** (Add button).
3. Complete mandatory data: the new user's **Name** and **Company** and press **Create**.
4. Create login data (optional). Create **Login / Password**.

5. Once added, the administrator is redirected to the user card and can be added to **Groups** and configured (**Cards, Phone numbers, Switch codes...**).

Use the user detail to set all user, user access and phone number parameters.

1. Account Settings

- **Name** – enter the user name for **2N® Access Commander** and the **2N IP intercom**.
- **User number** – use the number for external system administration.
- **E-mail** – enter the address to which **2N® Access Commander** user account information shall be sent.
- **Note** – add optional notes.
- **Login** – set the user login name.

- **Generate new password** – send an e-mail to the user (provided the user e-mail address and login are completed) with a newly generated password. The user shall change this password upon its first login to **2N® Access Commander**.
- **Set one time password** – set a one-time password just for the first login. Change the password after the first login.
- **In company** – display the company assignment.
- **In group** – display the group assignment. The user may be assigned to more groups than one within a company,
- **Attendance Monitoring** – make sure that the access card, Bluetooth authorization or fingerprint are set for the user to enable Attendance Monitoring.
- **Account enabled** – if the account is disabled, the user has no **2N® Access Commander** login rights, no notifications are sent to the user, the user access to devices is deactivated and the user phone number cannot be called. Once the account reactivated, all the user actions are available to the full extent.

2. Authorization

- A user can be assigned user, attendance and access management authorizations:
 - **Attendance management** – an attendance manager can monitor and edit attendance and view the access log of assigned users.

Caution

- Attendance management is not possible without assigned groups.

- **Visitor management** – a visitor manager can: create visitors in assigned companies and manage their membership in assigned groups, view the visitors' access log.
- **Door control** – the authorized user can: view the camera feed, open and lockdown assigned devices; view the devices' access log, their states, and security events in the system log.

Caution

- Door control is not possible without assigned devices.

- **User management** – a user manager can: create and edit users and visitors; manage group membership in the manager's company; view the users' access and system log.
- **Access management** – an access manager can: manage groups, time profiles, access rules and visitors in the manager's company; view related changes in the system log and the company's access log.
- **Administrator access** – an administrator has full control over all companies.

3. Accesses

ACCOUNT SETTINGS AUTHORIZATION **ACCESSES** PHONE NUMBERS



ALLOWED ZONES

Zone1 Zone2 Zone3 Zone4 Zone5

ACCESS RESTRICTIONS

Access time restrictions
No restriction

CARD (3F00F2FBC2) ^

Card	Identification number	
1	3F00F2FBC2	 

[ADD](#)

Virtual Card ID

- **Card** – enable manual setting or automatic reading of the user card number.
 - **Identification number** – set the user access card ID. The access card ID is a sequence of 6–32 characters of 0–9, A–F.
- **Add** – add a user card by tapping the card on a reader or entering the ID via the keypad. The ID must be a hexadecimal number consisting of 6 characters at least. Each user can be assigned up to two access cards.
- **Virtual Card ID** – 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 of 0–9, A–F. The virtual card ID is used for user identification in devices connected via Wiegand.

Tip

- 13.56 MHz + 125 kHz USB RFID card reader (9137421E) – install the card reader driver. Download from **2N® Access Commander** or www.2n.com.

PHONE (UNPAIRED) ^

Select the pairing option to be used

- ☒ Pair via dongle
- ☐ Pair via device

START PAIRING

- **Phone** – refer to [4.2.1 Bluetooth](#) for Bluetooth settings.

BIOMETRY (INACTIVE) ^



Click to select a finger for fingerprint loading

Not selected

Not selected

- **Biometry** – display the finger selecting window for fingerprint enrollment. Each user can enroll up to 2 fingerprints. Use an external fingerprint reader for enrollment. Make sure that the **2N® USB Driver** is installed. Download it from **2N® Access Commander** or www.2n.com. An uploaded user fingerprint can be used for the following actions:
 - Open door
 - Silent Alarm. Only if Open door is active.
 - Automation F1 – the FingerEntered event is generated in Automation. F1 helps identify the fingerprint in Automation.
 - Automation F2 – the FingerEntered event is generated in Automation. F2 helps identify the fingerprint in Automation.

Note

Fingerprint loading procedure:




1. Select a finger and click it.
2. The Fingerprint loading window is displayed.
3. Put the selected finger on the reader (repeat 3 times upon request).
4. You will be informed that your fingerprint has been scanned successfully after the third scanning.
5. Click Create to complete the process.

PIN/QR CODE (INACTIVE) ^



- **PIN / QR code** – assign either a PIN code, or a QR code for user access. A user cannot have both the codes simultaneously.
- **+ PIN** – automatic generation of a 6-digit PIN.
- **+ QR** – automatic generation of a QR code.

Note

-  – show / hide the PIN code characters. Show the QR code including the printing / e-mail sending option.
-  – edit the automatically generated PIN code. The PIN may contain 2–15 digits.
-  – send the PIN / QR code by e-mail. Make sure that the user e-mail is completed before e-mailing the QR code.

SWITCH CODES (ACTIVE) ^



- **User codes** – set the switch codes and user PINs.
 - **Switch codes** – set your own switch activation codes (door lock, e.g.). The switch code opens the door lock via a keypad like the DTMF code.

- **PIN code** – set the user's personal numerical access code. The code must include two characters at least.

Note

- In case the Silent alarm is on, the codes must be every other digit in a sequence. For example: if the access code is 0000, then the silent alarm code is 0001. Make sure that the code length is the same, i.e. the silent alarm code is 0000 for the access code 9999 and so on.

CAR LICENSE PLATES (INACTIVE) ^

ADD

No item has been added yet.

- **Car license plates** – set the user car license plate number.

4. Phone Numbers

John Blake

ACCOUNT SETTINGS AUTHORIZATION ACCESSSES **PHONE NUMBERS**

PHONE NUMBERS

CREATE

Order	Phone Number	Time profile	HP Eye	Group call
#1	1485	asd	Empty	Yes

USER DEPUTY

User Deputy
User01

VIRTUAL NUMBER

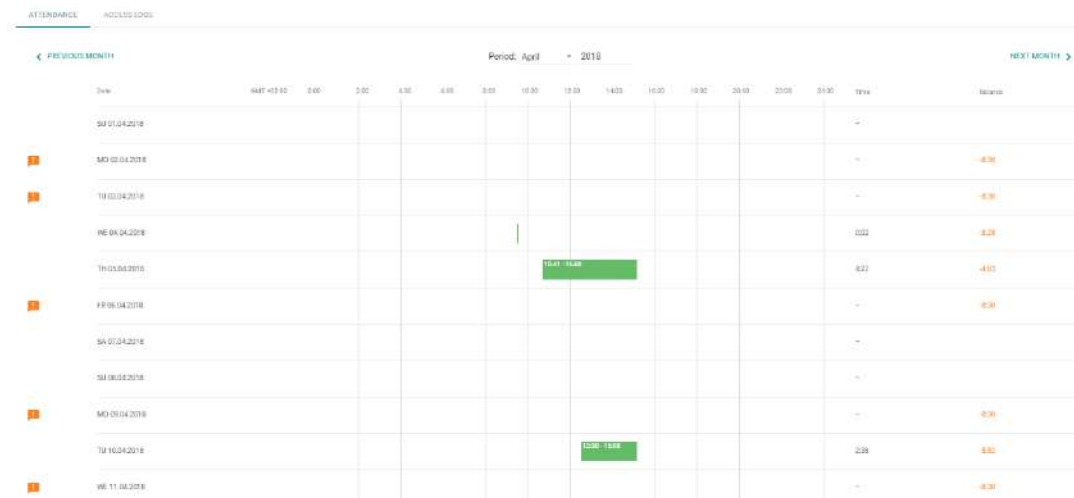
Virtual Number
123

- **CREATE** – set the following parameters:
 - the phone number sequence to be dialled first. If the first number is unavailable, the second, third... number is dialled and so on.
 - the station phone number to which the call shall be routed.
 - the time profile for phone number restrictions.
 - IP Eye address – used by **2N® IP Eye** for displaying a camera image window; useful for video phone users without displays.
 - Group call, which means a simultaneous call to the next phone number; when the call is answered via one phone, the other phone will stop ringing.

- **User Deputy** – select the user from the list to be directed calls at in case the original user is unavailable.
- **Virtual Number** – set a number to be used for user calling via the numeric keypad. The number can have two to four digits. Virtual numbers are not associated with the user's own phone numbers. They can be part of another numbering plan, which is independent of phone numbers and can thus hide user phone numbers.

5. Attendance

Attendance data is displayed on the user detail.



6. Access Logs

Filtered access logs. This tab shows you all the passages and keypad clicks on all the devices that are added to **2N® Access Commander**.

ATTENDANCE		ACCESS LOGS	SYSTEM LOGS			
	Time	User	Zone	Device	Access data	Details
✓	25.03.2020 10:00:36	User01	Zone1	2N IP Verso	☰	📷
✓	25.03.2020 09:50:19	User01	Zone1	2N IP Verso	☰	📷
✓	25.03.2020 09:26:52	User01	Zone1	2N IP Verso	☰	📷
✓	25.03.2020 09:26:29	User01	Zone1	2N IP Verso	☰	📷
✓	25.03.2020 09:19:21	User01	Zone1	2N IP Verso	☰	📷
✓	25.03.2020 09:15:08	User01	Zone1	2N IP Verso	☰	📷
✓	25.03.2020 09:15:06	User01	Zone1	2N IP Verso	☰	📷
✓	25.03.2020 08:59:09	User01	Zone1	2N IP Verso	☰	📷
✓	25.03.2020 08:21:08	User01	Zone1	2N IP Verso	☰	📷
✓	25.03.2020 08:07:42	User01	Zone1	2N IP Verso	☰	📷
✓	25.03.2020 08:06:10	User01	Zone1	2N IP Verso	☰	📷
✓	24.03.2020 15:50:55	User01	Zone1	2N IP Verso	✂	
✓	24.03.2020 15:59:44	User01	Zone1	2N IP Verso	✂	
✓	24.03.2020 15:58:32	User01	Zone1	2N IP Verso	✂	
✓	24.03.2020 15:59:26	User01	Zone1	2N IP Verso	✂	
✓	24.03.2020 15:59:19	User01	Zone1	2N IP Verso	✂	
✓	24.03.2020 15:59:13	User01	Zone1	2N IP Verso	✂	
✓	24.03.2020 15:59:07	User01	Zone1	2N IP Verso	✂	
✓	24.03.2020 15:58:50	User01	Zone1	2N IP Verso	✂	
✓	24.03.2020 12:02:02	User01	Zone1	2N IP Verso	☰	📷

7. System Logs

The system logs include changes on the displayed user only.

ATTENDANCE	ACCESS LOGS	SYSTEM LOGS				
	Time	Category	Subject	Event	Author	Detail
	25.03.2020 10:04:58	User action	User01	Attendance interval entered manually	System admin	Start={3/1 ...
	25.03.2020 10:04:41	User action	User01	Attendance interval entered manually	System admin	Start={3/2 ...
	25.03.2020 10:04:02	User action	User01	Attendance interval entered manually	System admin	Start={3/1 ...
	18.03.2020 09:43:35	User action	User01	PhoneNumber [1] updated	System admin	Properties ...
	18.03.2020 09:43:30	User action	User01	PhoneNumber [0] deleted	System admin	
	18.03.2020 09:42:23	User action	User01	PhoneNumber [0] created	System admin	Properties ...
	18.03.2020 09:35:16	User action	User01	User updated	System admin	Changes ...
	17.03.2020 16:56:47	User action	User01	PhoneNumber [1] updated	System admin	Properties ...
	11.03.2020 13:51:25	User action	User01	Card [7d57593d-2e3b-4a0b-b45b-b4ed8a03afed] updated	System admin	Properties ...
	09.03.2020 14:25:15	User action	User01	User updated	System admin	Changes ...
	09.03.2020 14:22:00	User action	User01	User updated	System admin	Changes ...
	09.03.2020 14:21:31	User action	User01	Password reset e-mail sent	System admin	
	09.03.2020 14:21:29	User action	User01	User updated	System admin	Changes ...
<div>SHOW ALL</div>						

4.2.1 Bluetooth

Select the pairing option to be used

- ☐ Pair via dongle
- ☒ Pair via device

When close to the initial pairing device, the user enters its pairing code into the 2N® Mobile Key application.

GENERATE

Pairing time

1 hour

Devices for initial pairing

IT Department

Select in the user detail whether to pair via dongle or a device. If you select dongle, make sure that dongle is connected and the **2N® IP USB Driver 1.2.4** application is installed (download). With dongle, click Start pairing and enter the generated PIN on a mobile phone equipped with **2N® Mobile Key**.

Note

- To generate a device pairing PIN, the user must be in the group that is added to the access rule with the zone where the device is installed.

When close to the initial pairing device, the user enters its pairing code into the 2N® Mobile Key application.

Pairing code

794364 SEND TO E-MAIL

Pairing time

1 hour (12:39)

Devices for initial pairing

2N Access Unit + KeyBoard

2N Access Unit

2N IP Verso

CANCEL PAIRING

If you select device pairing, click Generate to display the primary pairing PIN and click Send to e-mail to e-mail the PIN. The user has to approach the device and enter the PIN within a timeout. If

the user fails to enter the PIN within the timeout, the code expires and the administrator must generate a new PIN. If pairing is successful, the phone ID is displayed in the user detail.

PHONE

Identification number

e7ea641d005248b0a0d1b5ecf0567086

PAIR AGAIN

DELETE

After pairing, you can start new pairing on the user or delete the ID to remove the phone access.

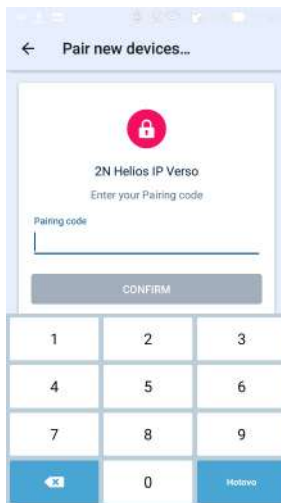
Mobile Application Pairing

Enter the generated PIN in a mobile application to start pairing via **2N® Access Commander**.

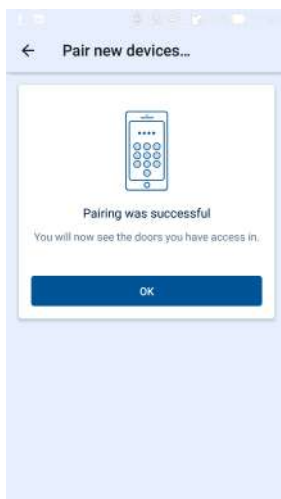
1. The pairing device is displayed in the application.



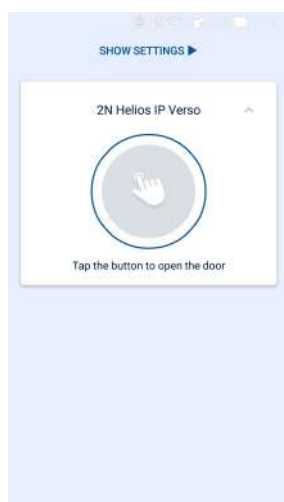
2. Click START PAIRING and, when asked so, enter the PIN generated in **2N® Access Commander**.



3. Once the PIN is entered successfully, the pairing result is displayed.



4. The device can be used for opening doors.



Links to stores:



4.3 Groups

Groups helps you set the zone access rights for the group members more easily. Thus, you do not have to set the rights on the user / visitor level but assign a group to a zone.

Name	Companies	Member count	
Customer Care	2N Telekomunikace s.s.	0	
Meeting room	J.J s.s.	1	
R&D	2N Telekomunikace s.s.	1	

Group list:

- **Create group** – enter the group name and superior company.
- **Delete group** – click the icon and confirm deletion.

Caution

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

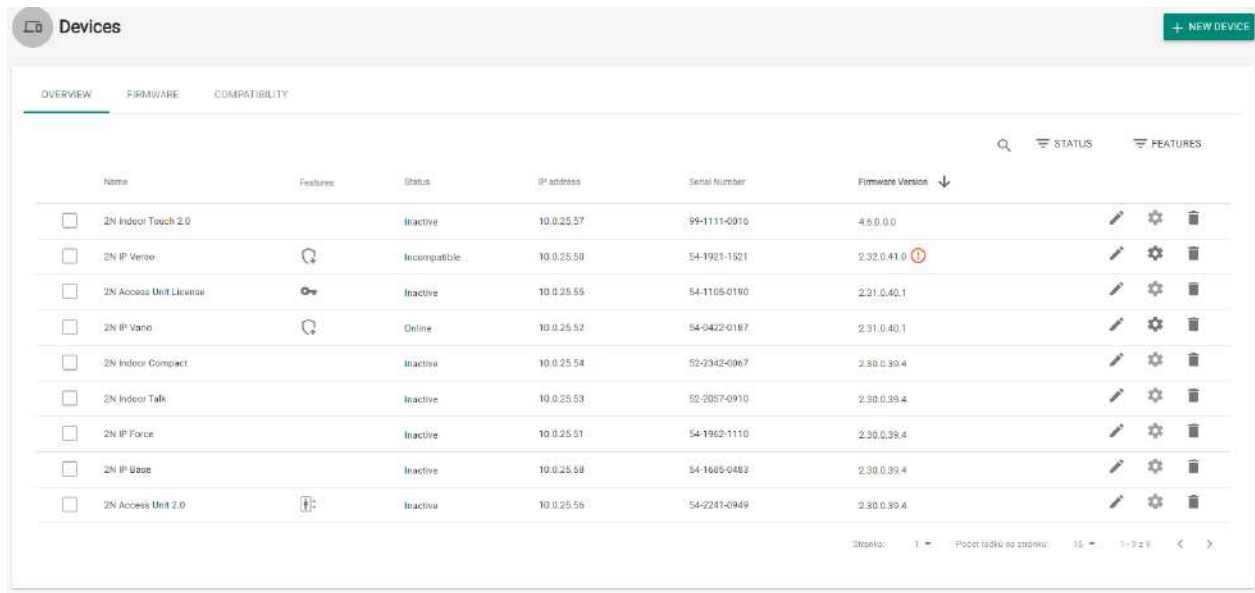
Type	Name

- **Members** – assign the users and visitor cards on the group detail. You can only add the user and visitor cards that are assigned to one and the same company as the group.
- **Access rules** – display the list of all available access rules for editing or creation.

4.4 Devices

Overview

Overview provides a list of all devices added to **2N® Access Commander**. The devices can be filtered by their states or a specific device can be searched.



Devices						+ NEW DEVICE
OVERVIEW FIRMWARE COMPATIBILITY						
Name	Features	Status	IP address	Serial Number	Firmware Version ↓	
<input type="checkbox"/> 2N Indoor Touch 2.0		Inactive	10.0.25.57	99-1111-0016	4.6.0.0.0	
<input type="checkbox"/> 2N IP Verio		Incompatible	10.0.25.58	54-1921-1521	2.32.0.41.0	
<input type="checkbox"/> 2N Access Unit License		Inactive	10.0.25.55	54-1105-0190	2.31.0.40.1	
<input type="checkbox"/> 2N IP Vano		Online	10.0.25.52	54-0422-0187	2.31.0.40.1	
<input type="checkbox"/> 2N Indoor Compact		Inactive	10.0.25.54	52-2342-0967	2.30.0.39.4	
<input type="checkbox"/> 2N Indoor Talk		Inactive	10.0.25.53	52-2057-0910	2.30.0.39.4	
<input type="checkbox"/> 2N IP Force		Inactive	10.0.25.51	54-1962-1110	2.30.0.39.4	
<input type="checkbox"/> 2N IP Base		Inactive	10.0.25.59	54-1685-0483	2.30.0.39.4	
<input type="checkbox"/> 2N Access Unit 2.0		Inactive	10.0.25.56	54-2247-0949	2.30.0.39.4	

Stranek: 1 Počet řádků na stránku: 15 1-9 z 9

The following bulk actions can be used:

- Activate selected devices
- Deactivate selected devices
- Add selected devices to zones
- Back up selected devices

Add device to 2N® Access Commander

Click Add device to create a device.

Create device

×

IP Address

Fill in IP address:

SEARCH NETWORK

Login*

Admin

Password*

Device Name

CANCEL

CREATE

Enter the IP address/domain name, click Enter and add more devices if necessary. Having completed the devices to be added, enter the login data and click Create.

Firmware

Firmware provides a bulk firmware upgrade for all the types of connected devices to maintain them in the optimum condition.

Upload the current firmware version online via 2N Update Server or manually. Every new version is subject to the administrator's approval for full control of the upgrading process. You can install a new version in one or more selected devices for test purposes and only then allow the other devices to be upgraded.

Optionally, a device can be excluded from the bulk firmware administration and thus the function can be deactivated for the selected device

Devices

+ NEW DEVICE

OVERVIEW

FIRMWARE

COMPATIBILITY



Automated firmware management

INFO

FIRMWARE VERSIONS

Device Type (count)	Target version	
2N Indoor Talk (1)	None	
2N IndoorTouch A33 (1)	None	
2N Access Unit 2.0 (1)	None	
2N IP Vario (1)	None	

- **Automated firmware management** – enable/disable bulk firmware management.
- **Firmware versions** – display the list of types of the connected 2N IP intercoms, answering units and 2N Access Units.




- **Device Type (count)** – display the type and count of connected devices.
- **Distributed version** – display the required version for all the devices of one type. Every new device will be upgraded to this version too.
- **New Version button** – notifies that a new version is available.
 - **Version Info** – show the release notes for the new FW version.
 - **Distribute** – start distributing the new FW version to all the devices of the given type.
 - **Test on device** – upload the new version to a selected device. When the test is successful, upload the version to the other devices too.
-  – click this paper clip icon to manually select and upload the firmware file and start distributing the new version to all devices of the same type.
-  – click the trash bin icon to stop distributing the FW to the connected devices.

Info

- If the distribution to the connected devices is stopped, the version will not be removed from the device.

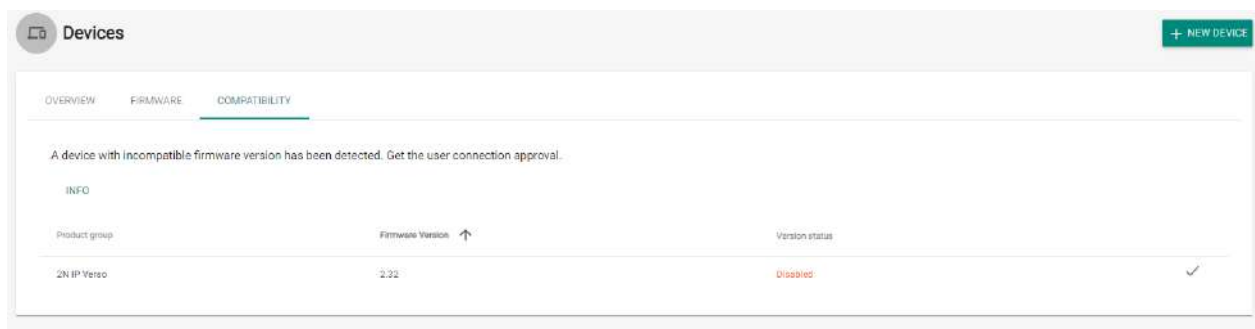
Caution

- If the firmware is not supported by the current **2N® Access Commander** version, enable this version on the Compatibility tab. Make sure that you have chosen a device whose temporary idleness shall not affect the building's operation and security.

- **Excluded devices** – optionally, a device can be excluded from the bulk firmware administration and thus the function can be deactivated for the selected device.
 -  – click this paper clip icon to manually select and upload the firmware file and start distributing the new version to all devices of the same type.
 -  – remove a device from the list of excluded devices. After exclusion, the FW distributed for the given type of device is uploaded automatically to the device.
 -  – go to the device detail.

Compatibility

These settings inform the administrator via an e-mail and notification that a device with unsupported firmware is connected. Enable this firmware version to activate the device.

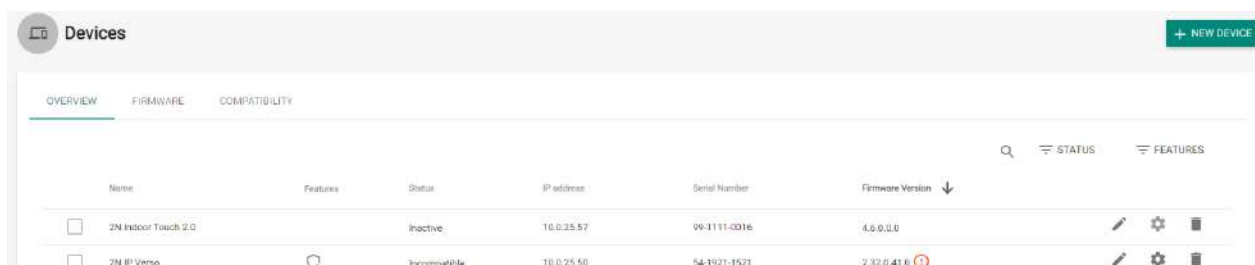




Once a device with incompatible firmware is added or upgraded, the device turns incompatible. A new record is created in the table and the administrator can allow the use of incompatible firmware for **2N® Access Commander**. If the FW is approved, the device goes online and can be used as a standard device. If it is disapproved, all the devices using this FW become incompatible.

Caution

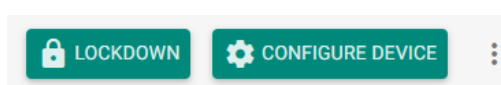
- Incompatible means that no new users are created on the device but events are downloaded from the device and the device configuration or backup can be used.
- Incompatible firmware cannot guarantee the correct performance of all features and is thus not recommended by the manufacturer.


The user is warned about the use of incompatible firmware in the device overview.

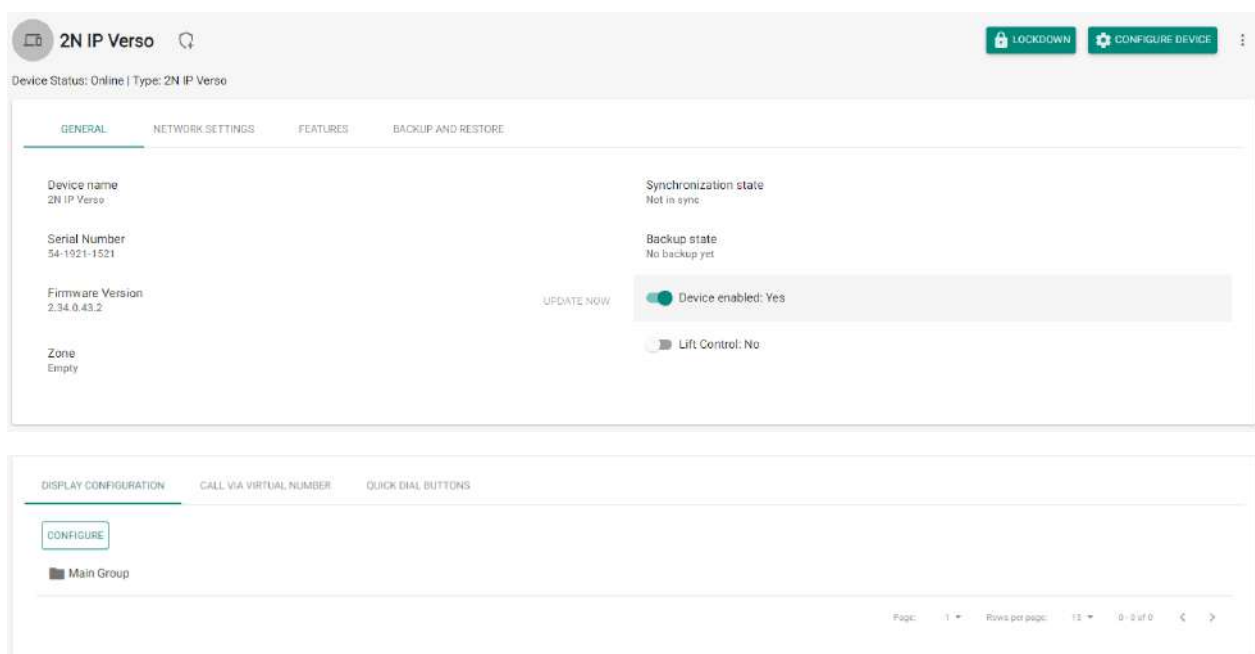


-  The so-marked devices use disapproved incompatible firmware.
-  Incompatible firmware cannot guarantee the correct performance of all features and is thus not recommended by the manufacturer. The so-marked devices use approved incompatible firmware.

Device Management







- **Lockdown** – activate emergency lockdown for a selected device. During lockdown, it is impossible for the user to unlock a door even if the user uses a valid access with a valid time profile.
- **Configure device** – display the user interface for user configuration.
-  – further options:
 - **New device** – add a device to the **2N® Access Commander** device list.
 - **Open door** – unlock a device-controlled door lock remotely.
 - **Hold unlocked** – hold a device-controlled door lock open (unlocked) for 1 minute to 12 hours without authentication as preset.
 - **Delete device** – remove a device from the **2N® Access Commander** device list.



- **General**
 - **Device name** – set the device name.
 - **Serial number** – display the device S/N.
 - **Firmware version** – display the device firmware version.
 - **Upgrade now** – start upgrade for a selected device only.
 - **Zone** – display and edit the zone where the device is located.
 - **Backup state** – display the backup state. The last backup date and time are displayed if existing.
 - **Active device** – activate/deactivate a device. An inactive device disables synchronisation event downloading.
 - **Lift Control** – enable/disable the lift control function.
 - **Change password** – change the device password. The change is made both in **2N® Access Commander** and the connected device.

- **Configure device** – open the device configuration web in the **2N® Access Commander** environment. Refer to [4.4.3 Device Configuration via 2N® Access Commander](#) for more details.
- **Network Settings**
 - Set all parameters necessary for intercom connection.
- **Features**
 - Display the supported features.
- **Backup and Restore**
 - Use the device configuration backup xml file. Refer to [4.4.5 Device Backup and Restore](#) for more details.

DISPLAY BUTTON CONFIGURATI...	DISPLAY CONFIGURATION	CALL VIA VIRTUAL NUMBER	QUICK DIAL BUTTONS
Button number		User	
#1		Empty	
#2		Empty	
#3		Empty	
#4		Empty	

- **Display button configuration**
 - Configure the buttons to be displayed as name tags (**2N® IP Vario**).
 - **Display configuration**
 - Set the **2N® IP Vario** or **2N® IP Verso** display. For details refer to [4.4.2 Display Configuration](#).
 - **Call via virtual number**
 - Add the user(s) with a virtual number. Unnecessary if the user is synchronised otherwise, via an access rule, for example.
 - **Quick dial buttons**
 - Assign a **2N® Access Commander** user to the buttons of the connected device.
- [4.4.1 Display Configuration](#)
 - [4.4.2 Device Configuration via 2N® Access Commander](#)
 - [4.4.3 Automatic Synchronisation](#)
 - [4.4.4 Device Backup and Restore](#)
 - [4.4.5 Lift Control](#)

4.4.1 Display Configuration

Go to the details of the device on which the display is to be configured. Select Display button configuration or Display configuration in the General menu.

2N LTE Verso
Device Status: Online

GENERAL NETWORK SETTINGS FEATURES BACKUP AND RESTORE

Device Name
2N LTE Verso

Serial Number
64-1763-0989

Firmware Version
2.23.0.32.5

MAC address
7C-1E-B3-02-8F-CA

Zone
Zone4

Synchronisation state
Successfully synchronised [11.04.2018 21:11:14]

Backup state
No backup yet

Active device

COPY SETTINGS SYNCHRONISE DEVICE CHANGE PASSWORD CONFIGURE DEVICE

Management

Nametag configuration

2N LTE Verso
Device Status: Online

DISPLAY BUTTON CONFIGURATION DISPLAY CONFIGURATION CALL VIA VIRTUAL NUMBER QUICK DIAL BUTTONS

Button number	User
#1	Empty
#2	Empty
#3	Empty
#4	Empty

Nametags help dial user phones quickly by a single button press. Click Empty next to the button number and enter the user name to be added. Now click OK and let the device synchronise.









Phonebook configuration



The window includes the phonebook structure to be loaded to the display. Click Configure to configure the display.



Create the display structure using groups and assigned users.

- Click the  icon to create a group. A group is created under a superior group.
- The  icon helps to create a calling group.
- Click the user/group adding icon  to add a user to a group or calling group. You can select more users at once. Choose a group directly from **2N® Access Commander**, all the users will be uploaded to the device display.
- Click  to remove the users and groups
- Click  to add priority to a user.
- When  is clicked, the list will be arranged so that the users with priority are preferred to those without priority.
 -  user with priority
 -  user without priority

Adding users to the phonebook:

2N IP Verso – Configuration de l'écran

MODIFIER

ANNULER

Groupe principal

<input type="checkbox"/>	<div><div></div><div>Group 1 (vide)</div></div>	<div><div></div><div></div><div></div></div>
<input type="checkbox"/>	<div><div></div><div>User01</div></div>	<div><div></div><div></div><div></div></div>
<input type="checkbox"/>	<div><div></div><div>User04</div></div>	<div><div></div><div></div><div></div></div>
<input type="checkbox"/>	<div><div></div><div>User05</div></div>	<div><div></div><div></div><div></div></div>
<input type="checkbox"/>	<div><div></div><div>User02</div></div>	<div><div></div><div></div><div></div></div>
<input type="checkbox"/>	<div><div></div><div>User03</div></div>	<div><div></div><div></div><div></div></div>

Page

1

Rows per page

15

1 - 5 of 5

<


>


4.4.2 Device Configuration via 2N® Access Commander

1. Select the **Device** card.
2. Select an **active** device from the device list and choose **Edit** (click anywhere in the selected device row).

	Name ↑	State	IP address	Serial Number	Firmware Version	
<input type="checkbox"/>	2N Access Unit	Online	10.0.25.135	54-1105-0190	2.23.0.32.3	  
<input type="checkbox"/>	2N Access Unit + TouchKeyboard	Online	10.0.25.159	54-1108-0217	2.23.0.32.6	  
<input type="checkbox"/>	2N Helios IP Base	Online	10.0.25.151	54-1005-0402	2.23.0.32.6	  
<input type="checkbox"/>	2N Helios IP Force	Inactive	10.0.25.146	54-0475-0646		  
<input type="checkbox"/>	2N Helios IP Value	Inactive	10.0.25.103	54-0809-0078		  
<input type="checkbox"/>	2N Helios IP Verso OnSite	Online	10.0.25.133	54-0917-0073	2.23.0.32.6	  
<input type="checkbox"/>	2N LTE Verso	Online	89.24.76.81	54-1703-0209	2.23.0.32.5	  

3. Select **Configure device** in the **General** menu. If the device is not **active**, you cannot use the **Configure device** option. The parameter icon is inactive in this case.



2N IP Base


Device Status: Online

GENERAL NETWORK SETTINGS FEATURES BACKUP AND RESTORE

Device name
2N IP Base

Serial Number
54-2208-0428

Firmware Version
2.23.0.37.1

Zone
sdagfad

UPGRADE NOW

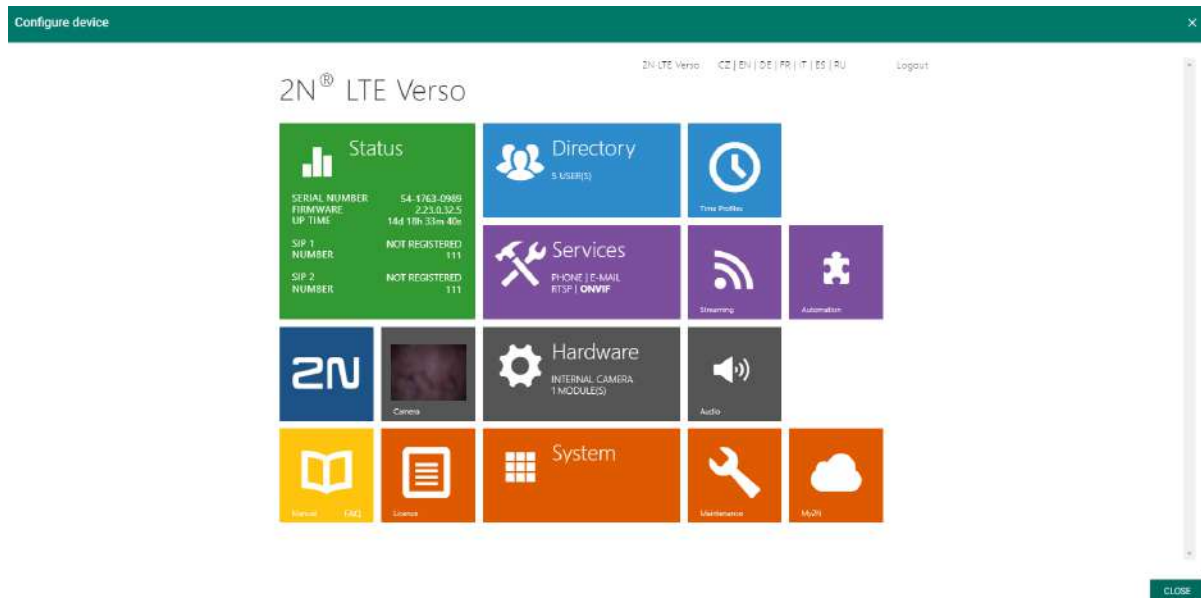
Synchronization state
Successfully synchronized [07.11.2019 07:50:55]

Backup state
No backup yet

Active device:

CONFIGURE DEVICE

4. A new window opens up for you to configure the selected device (for parameter details refer to the Configuration Manual at [HERE](#). You can close the window in the right-hand upper corner any time and return to the **2N® Access Commander** environment.



4.4.3 Automatic Synchronisation

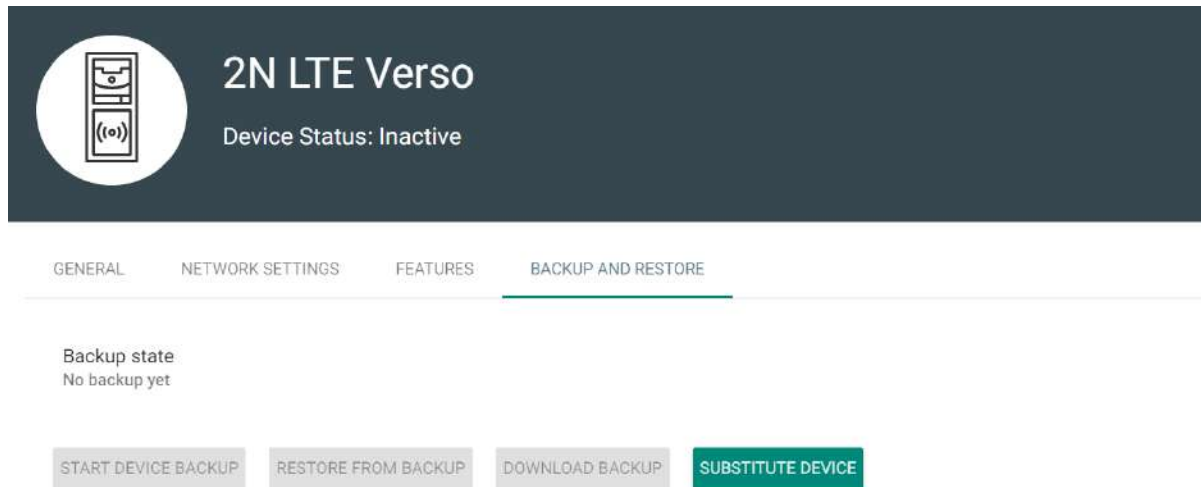
Automatic synchronisation helps maintain the current settings of terminal equipment within the access control system. It starts whenever a change is made that applies to terminal equipment, i.e. that is associated with user access rights, phone numbers, time rules and/or button assignments.

Only the devices are synchronised that are configured so in the access rules. Only the synchronisation requests are queued that may affect terminal equipment. For example, a name change for a user that is not assigned to any group never starts automatic synchronisation.

Note

- The synchronisation time (necessary for all changes to be applied in terminal equipment) depends on the count of devices to be synchronised and the amount of data to be loaded.

4.4.4 Device Backup and Restore



- **Backup state** – display the backup state. If a backup is available, the last backup date and time are displayed.
- **Restore state** – display the last restore from backup.
- **Run device backup** – start the device configuration backup.
- **Download backup** – download the xml configuration file to the disk. This XML file can be loaded to the intercom directly.
- **Device replacement**
 - Device replacement helps you quickly substitute a defective device for another keeping the original configuration.
 - i. Go to the **Devices** card.
 - ii. Select the device to be replaced. Make sure that the device is **inactive**.
 - iii. Select **Device replacement** in the **Backup and restore** menu.
 - iv. Select a device to replace the existing one (select only such device that is not added to Access Commander and that is installed in the same LAN as Access Commander).
 - v. Fill in **Login** and **Password**.
 - vi. If no configuration backup was made for the original device, configure the new device manually. If a configuration backup was made for the original device, this backup will be used for the new device after replacement.
 - vii. Click **Substitute** to replace the device and upload the device backup if available to the new device.

Substitute device

Substitute for device *

Login *

Password *

Backup configuration is unavailable for the original device. Set the new device manually.

CANCEL

SUBSTITUTE










4.4.5 Lift Control

Management

FLOORS

I/O MODULES

Display all: No ⓘ

Floor ID 	Name	Access According to Zone Rules	Public Access	Public Access Time Profile
io_1_1	Basement-2	Zone2	No	
io_1_2	Basement-1		No	
io_1_3	Ground floor		No	
io_1_4	1st Floor		No	
io_1_5	2nd Floor		No	
io_1_6	3rd Floor		No	
io_1_7	4th Floor		No	
io_1_8	5th Floor		No	

To control the floor lift access, connect the AXIS A9188 relay module to the 2N IP intercom (**2N® IP Verso**, **2N® IP Force**, **2N® IP Safety**, **2N® IP Vario**) or Access Unit. Up to 5 relay modules can be connected to one 2N IP intercom/Access Unit, each of which can control up to 8 floors, which makes a total of 40. Make sure that the respective 2N IP intercom (Part No. 9137916) and Access Unit (Part No. 9160401) licenses are active to make this function work

Floors

Display all: Yes ⓘ

- **Show all** – display all the floors to be configured.

Floor ID ↑	Name	Access According to Zone Rules	Public Access	Public Access Time Profile
------------	------	--------------------------------	---------------	----------------------------

- **Floor ID** – module and relay output sequence.
- **Name** – floor name.
- **Access according to zone rules** – assign a zone to the particular floor to give access only to the users authorized by the zone access rules.
- **Public access** – activate permanent floor access without any authentication.
- **Public access time profile** – define the public access validity. Select a time profile in [Time Profiles](#).

Caution

- If access is set according to the zone rules, the lift control does not assume any zone setting (PIN code, multiple authentication, silent alarm...).

I/O Modules

Management

FLOORS I/O MODULES













Module ID	Enable	Status	IP Address	Serial Number
io_1	Enabled	Online	10.0.25.220	ACCC8E9D37A7
io_2	Disabled	Offline	192.168.0.90	
io_3	Disabled	Offline	192.168.0.90	
io_4	Disabled	Offline	192.168.0.90	
io_5	Disabled	Offline	192.168.0.90	

Add, remove or modify the module in the device configuration.

- **Module ID** – display the module sequence.
- **Enabled** – display the activation/deactivation of the AXIS A9188 module used for lift control for up to 8 floors. Set the module in the device.
- **State** – display the state of the connected AXIS A9188 module (Error/Access denied/Ready/Offline).
- **IP Address** – AXIS A9188 IP address.
- **Serial Number** – AXIS A9188 serial number.

4.5 Zones

Zones makes it easier to administer accesses to devices. Zones unite devices into logical complexes.

Zones			+ NEW ZONE
Name ↑	Companies	Device count	
NewCompany	My Company	0	 
Zone1	My Company	1	 
Zone2	My Company	1	 
Zone3	My Company	1	 
Zone4	My Company	1	 
Zone5	My Company	1	 

The zone list includes the following actions:

- Create zone

- Delete zone
- Go to detail

Use the zone details to set the following parameters.

INFO

Name
Zone1

Zone access PIN code
Empty

ADDSSES

Multiple authentication
Active: Bluetooth, Card, Biometry, PIN
Time profile: 01

☒ Silent Alarm: Yes

☒ Limit Failed Access Attempts: Yes

☒ License Plate Authentication: Yes

- Info
 - **Name** – zone name.
 - **Zone access PIN code** – set the zone access code as the only authentication method. .

Zones

Name *
Zone4

Zone access PIN code

Zone access time profile

CANCEL CHANGE

- Accesses
 - **Multi-factor authentication** – set the access rules and their combinations for all the zone devices. Multi-factor authentication includes, e.g., a card + PIN combination.
 - **Time profile** – enable multi-factor authentication for the selected time profile only.
 - **Apply multi-factor only for zone entry** – enable multi-factor authentication for the selected zone entry only.

Caution

- The multi-factor authentication time profile can only be applied in devices with FW 2.33 and higher.

Multiple authentication setting ×

☒ Bluetooth

☒ Card

☒ Biometry

☒ PIN

Time profile

01 ×

Apply multi-factor only for selected Time profile

☒ Apply multi-factor only for zone entry

CANCEL
CHANGE

- **Silent Alarm** – enable Silent Alarm for all the devices assigned to a zone.
- **Limit Failed Access Attempts** – enable this function for all the devices in a zone. Enable the maximum count of unsuccessful authentication attempts. After five unsuccessful attempts (wrong numeric code, invalid card, etc.), the access module will be blocked for 30 seconds even if authentication is valid.
- **License Plate Authentication** – enable license plate authentication for all devices supporting this function in the zone.

- ☒ Silent Alarm: Yes
- ☒ Limit Failed Access Attempts: Yes
- ☒ License Plate Authentication: Yes

- **Device** – add a device to a zone. Logically associates the premises that are to be accessed by the same users. Such as offices with two entrances. Add the devices at both the doors to the zone.

Device

Device

CANCEL

ADD

- **Companies** – assign one zone to multiple companies. Used in [Access rules](#) for zone-group interconnection.

Add zone to company

Companies

CANCEL

ADD

- **Access rules** – display the list of all available access rules for editing or creation.

DEVICES			COMPANIES			ACCESS RULES		
ADD								
Groups			Time Profiles					
Group1			No profile / Unlimited					
Dagmar group			02					

Setting of zone access points

- The device (2N IP intercom or Access Unit) can have up to two access points allowing a bidirectional passage. They are called "Arrival rules" and "Departure rules" in the device configuration interface.
- Each access point can be assigned one or more readers connected to the device. The access points record zone entry / exit. They need to be used in case the device is located on a boundary between two zones to monitor the user zone movement precisely.

Name	Companies	Device count
Meeting rooms	J.J. a.s.	1
Relax Room	Stápmirov	0

- When the function is enabled, the access point settings are available on the device and zone details.

Note

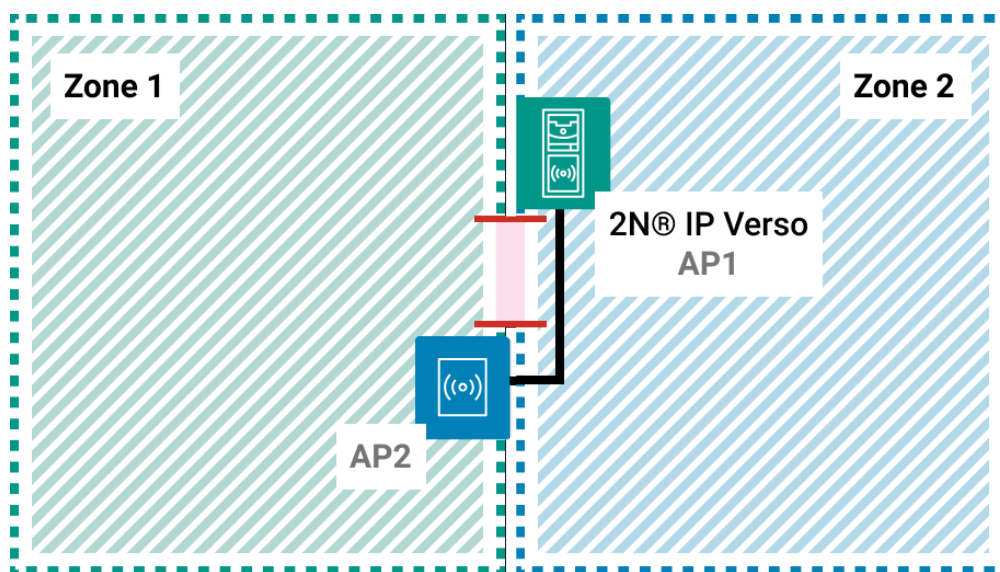
- If the access points are active on a zone, multiple authentication will be checked on a selected access point only.
- Multiple authentication can be activated for zone entry or for both the access points at the same time.

Examples of Access Point Settings

Active access points

Suppose there is a connecting door between two zones (Zone 1 and Zone 2) controlled by a single intercom (2N® IP Verso). Another separate reading unit is located on the other side of the door (AP2) and connected to this control device.

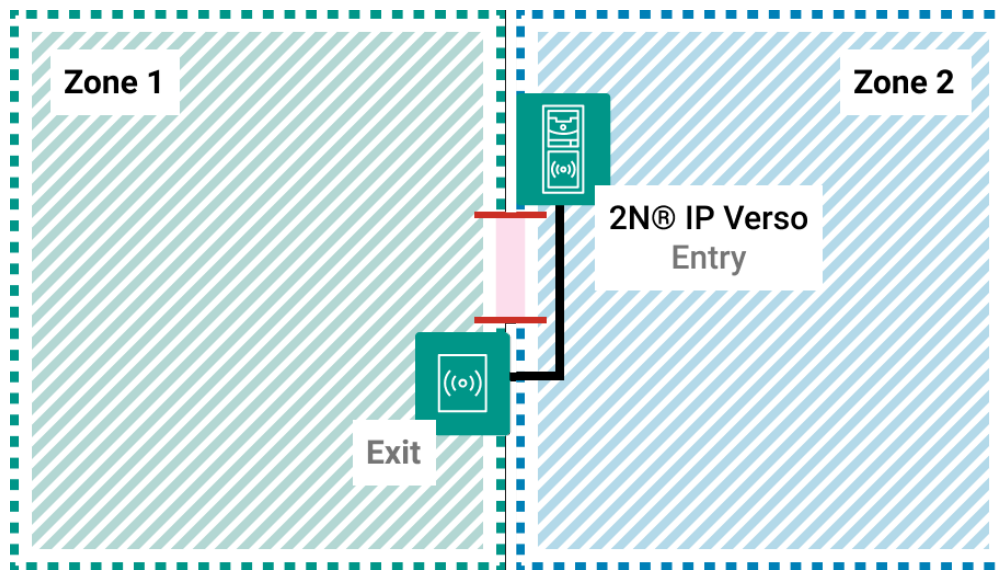
The active access points make it possible to assign AP2 as the entry point to Zone 2, while the main unit with AP1 remains as the entry point to Zone 1. This provides occupancy and presence monitoring in both the zones simultaneously.



Without access points

In this mode, 2N® Access Commander cannot distinguish transition between the zones, because the controlled door is only part of Zone 1.

The door can thus be opened from either side. The zone occupancy and presence check, however, can work for Zone 1 only, because exiting Zone 1 does not automatically mean entering Zone 2.



4.6 Time Profiles

Time Profiles			+ NEW PROFILE	
Order	Name ↑	Active days		
	Holidays	Ho		
	Weekend	Sa Su Ho		
	Working hours	Mo Tu We Th Fr		

Some intercom functions, such as outgoing calls, RFID card or numeric code access, can be time-defined. Assign a **Time profile** to such functions to define when the functions are to be 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 via a week calendar. Just set From-To and specify the weekdays for availability. **2N® Access Commander** allows you to create up to 20 time profiles.

Time Profile Creation

The access control time profiles are automatically uploaded to the devices that provide user accesses to zones. No order need to be defined for these profiles.

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.

- **Profile Name** – enter a profile name. This parameter is mandatory and helps you search the time profile list and select profiles easily.



You can edit a time profile name and upload it to all the devices. Make sure that the time profile sequence (1–20) is defined to upload the time profile to the device correctly.

Set the active time profile within a week. A profile is active when the current time falls into the set intervals.

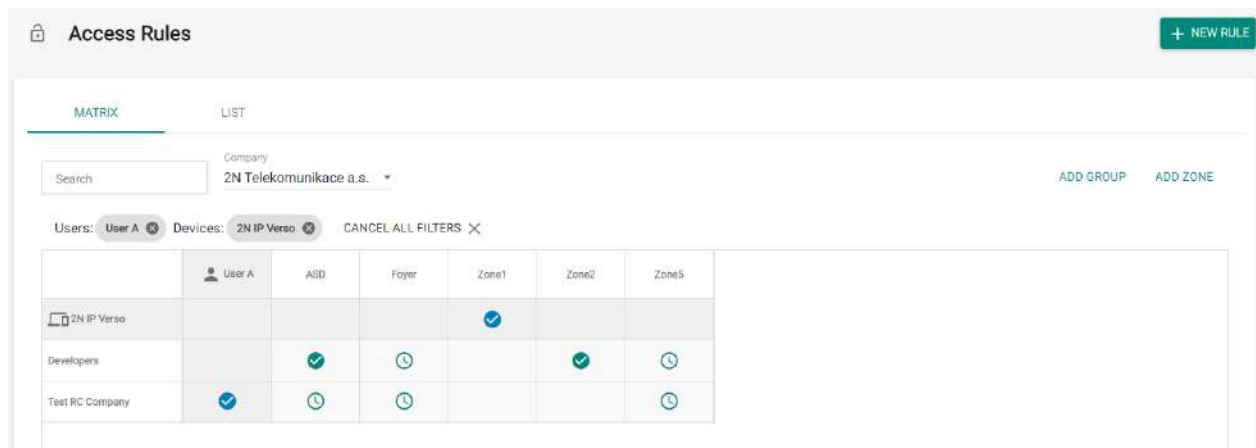
Make sure that time and time zone are set correctly for the intercoms to make this function work properly.

Note

- You can set any count of time intervals per day: 8:00–12:00, 13:00–17:00, 18:00–20:00, for example.
- To make a time profile valid during the whole day, enter one daily interval: 00:00–23:59.

4.7 Access Rules

Access Rules helps manage company group user accesses clearly in zones based on time profiles.



The screenshot displays the 'Access Rules' interface in 'MATRIX' view. At the top, there's a '+ NEW RULE' button. Below it, a search bar and a company filter '2N Telekomunikace a.s.' are visible. The interface shows filters for 'Users: User A' and 'Devices: 2N IP Verso'. The main table lists access rules for three entities: '2N IP Verso', 'Developers', and 'Test RC Company'. The columns represent different zones: 'Zone1', 'Zone2', and 'Zone5'. The '2N IP Verso' row shows a blue checkmark in the 'Zone1' column. The 'Developers' row shows green checkmarks in the 'Zone2' and 'Zone5' columns. The 'Test RC Company' row shows a blue checkmark in the 'Zone1' column and green checkmarks in the 'Zone2' and 'Zone5' columns.

	User A	ASD	Foyer	Zone1	Zone2	Zone5
2N IP Verso				✓		
Developers		✓	⌚		✓	⌚
Test RC Company	✓	⌚	⌚			⌚

The Matrix folder provides clear and easy access settings. Matrix is available to every existing company and shows all the groups and zones assigned to it. Use the +NEW RULE button to create an access rule. Assign a group, zone and time profile to each new rule.

The Search field helps you add users and devices, thus providing a more detailed overview.

Tip

MATRIX LIST

Search Company: 2N Telekomunikace a.s.

Users: **User A** Devices: **2N IP Verso** CANCEL ALL FILTERS

	User A	ASD	Foyer	Zone1	Zone2	Zone5
2N IP Verso				✓		
Developers		✓	⌚		✓	⌚
Test RC Company	✓	⌚	⌚			⌚

The 2N Telekomunikace matrix example shows that:

- The filtered **2N® IP Verso** device is included in Zone1.
- The filtered user is assigned to the Test RC Company group.
- The Developers group and its users have an unlimited access to ASD and Zone2, a limited access to Foyer and Zone5 (based on the time profile setting) and no access to Zone1.
- The Test RC Company group and its users have a limited access to ASD, Foyer and Zone5 (based on the time profile setting) and no access to Zone1 and Zone2.

Matrix helps you change group/zone time profiles quickly and easily, place the device in a different zone and add/remove a user to/from a group. You can simply add a new group or zone to a company matrix if necessary. Refer to [4.3 Groups](#) and [4.5 Zones](#) for more group/zone details.

Create group

Group name *

This field is mandatory

Select company *

2N Telekomunikace a.s.

CANCEL CREATE

Create zone

Zone name *

This field is mandatory




















2N Telekomunikace a.s.

CANCEL CREATE

The List folder shows a list of all the groups including the zones and time profiles assigned to them for all the companies, thus helping you make zone and time profile changes in the groups.

MATRIX

LIST

			 GROUP	 ZONE	 TIME PROFILE
Group	Zone	Time profile			
APB Group	Foyer	No profile / Unlimited			 
APB Group	Zone2	Pracovní dny			 
APB Group	Zone3	asd			 
APB Group	Zone4	01			 
Developers	ASD	No profile / Unlimited			 
Developers	Foyer	Pracovní dny			 
Developers	Zone2	No profile / Unlimited			 
Developers	Zone5	02			 

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

- **WHO** is defined by the group and 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 and devices assigned to it (one device may be assigned to one zone only).
- **WHEN** is defined by the time profile assigned. This item is not mandatory. An incomplete time profile means an unlimited access (24/7).

The figure below shows the rule creating logics:




Note

- One group can be assigned to multiple zones as well as one zone can be assigned to multiple groups.
- A selected zone-group pair can be added repeatedly with different time profiles.

4.8 Lockdown

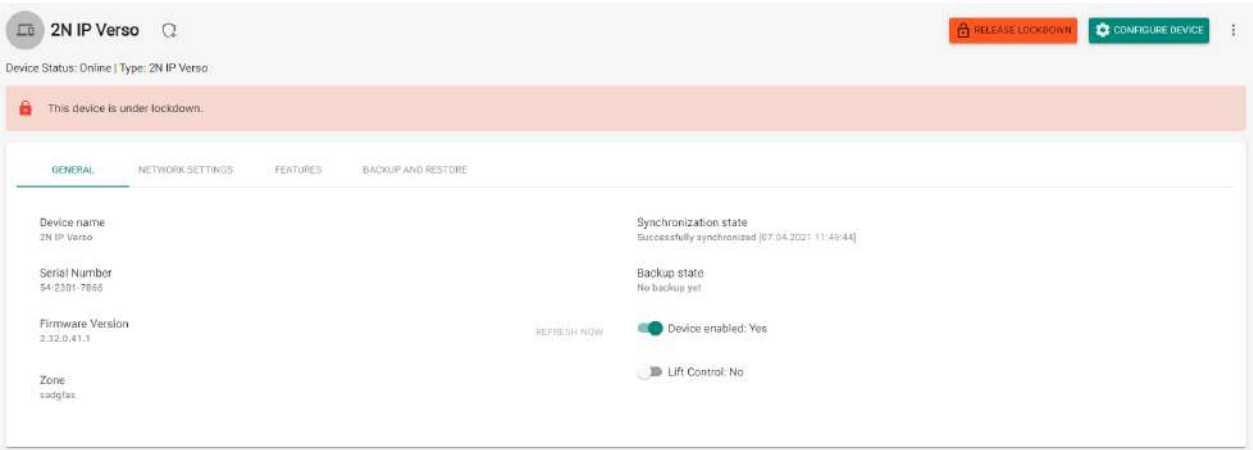
It is impossible to open doors using preset user access rules during emergency lockdowns even if a valid access with a valid time profile is used. Emergency lockdown can be activated/deactivated from the device detail, zone detail, company detail or using a global action on the

upper bar by pressing . Emergency lockdown can also be activated/deactivated from the dashboard or emergency lockdown widget, where a particular device group can be defined.

Offline devices, inactive devices, device with incompatible firmware and devices with FW older than 2.32 will not be locked down by the emergency lockdown request.

Device state	Lockdown activation/deactivation option	Included in total devices for lockdown	Note
Offline	Yes	Yes	Emergency lockdown will not be activated/deactivated until the device is available.
Active (Online)	Yes	Yes	Emergency lockdown will be activated/deactivated for the device.
Inactive	✗ No	✗ No	Emergency lockdown cannot be activated/deactivated for the device. These devices are not included in the total count of devices available for emergency lockdown.
Incompatible	✗ No	✗ No	Emergency lockdown cannot be activated/deactivated for the device. These devices are not included in the total count of devices available for emergency lockdown.

In case one or more devices are unavailable at the emergency lockdown request time, the Device / Zone / Company transits into a partial lockdown. The emergency lockdown request will be met when the device is available again.



Device Detail in Active Emergency Lockdown

5. Extensions

- [5.1 Presence](#)
- [5.2 Attendance](#)
- [5.3 Device Monitoring](#)
- [5.4 Visitors](#)
- [5.5 Notification](#)
- [5.6 CAM Logs](#)
- [5.7 Area Restrictions](#)

5.1 Presence

The **Presence** module is an extension to the Attendance module and displays the list of currently present employees. Set the IN-OUT Attendance mode for the module to work properly. For more details refer to [Attendance Module Mode](#)


Presence (5 )								
Type	Users 	Companies	Groups	Zone	Passage time	Phone Number		
	User01	My New Company	Group1	Zone1	10.09.2018 11:21:06	1100		
	User02	My New Company	Group1	Zone1	10.09.2018 11:21:08	1101		
	User03	My New Company	Group1	Zone1	10.09.2018 11:21:10	1102		
	User04	My New Company	Group1	Zone1	10.09.2018 11:21:13	1103		
	User05	My New Company	Group1	Zone1	10.09.2018 11:21:18	1104		

All the users are then displayed in the Presence module. Presence is detected from the count of card swipes through end terminals (2N IP intercoms, Access Units).

1. If **arrival** (IN event) is the **last** event of the day, the user is considered as **present**.
2. If a user passes a reader in an unspecified direction, the user zone will be changed. The same happens if the user passes in the **IN** mode.
3. If **departure** (OUT event) is the **last** event of the day, the user is considered as **absent**.
4. After the timeout the user presence record is removed in case the user failed to validate its departure.

Note

- The Presence module does not work if the **FREE** Attendance mode is selected. The only mode to be selected is **IN-OUT**.

Click the Configure icon  to set the user presence timeout for the list of present users. When this timeout expires, the user will be removed from the list automatically if arrival was the last event of day.

Presence module settings

User presence timeout [h]

8

CANCEL










CHANGE

5.2 Attendance

The Attendance section displays the list of users to be monitored and their Attendance details.

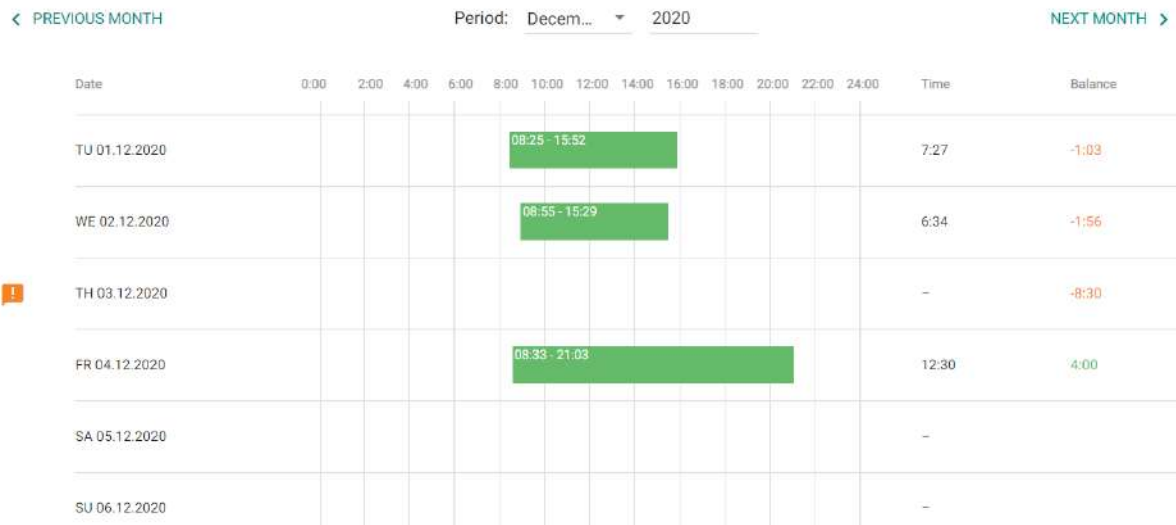
Attendance User List

The list includes all the users whose attendance is to be monitored. Select a user to display its attendance detail. A Burger menu helps you export records of all the monitored users to a CSV or PDF file. The file contains a total balance of all the users and a working fund for the given period.

Attendance 			
Users 	Companies	Groups	
<input type="checkbox"/> Aksamit Jan	2N Telekomunikace a.s.	Displej Development, A1 Mechanika – Náv, A1 Elektronika – Náv ...	
<input type="checkbox"/> Arvay Radek	2N Telekomunikace a.s.	Displej Development, A1 Mechanika – Náv, A1 Elektronika – Náv ...	
<input type="checkbox"/> Aubrecht Přemysl	2N Telekomunikace a.s.	Displej Development, A1 Mechanika – Náv, A1 Elektronika – Náv ...	
<input type="checkbox"/> Aubrecht Přemysl malíčky	2N Telekomunikace a.s.	A1 Mechanika – Náv, A1 Elektronika – Náv, A2 Access systems ...	
<input type="checkbox"/> Baptista Guilherme Santos ...	2N Telekomunikace a.s.	A1 Mechanika – Náv, A1 Elektronika – Náv, A2 TPV – Náv ...	
<input type="checkbox"/> Baroch Pavel	2N Telekomunikace a.s.	A1 Mechanika – Náv, A1 Elektronika – Náv, Display Building A ...	
<input type="checkbox"/> Bartková Deptová Oľga	2N Telekomunikace a.s.	C4 Plocha Sales Front - Náv, Display 4rd floor, 2N a.s. ...	

Attendance Detail

The Attendance detail helps you edit the user intervals. Click an interval to open the editing window. Use the Burger menu to export the selected user records to a CSV or PDF file. The files include daily records.



Attendance Settings

Make sure that Attendance Monitoring is active in **2N® Access Commander** to make the Attendance function work correctly. The licence is generated per 25 users. Having uploaded the licence, set the maximum count of available Attendance licences in User administration / Companies. With this limit on, you cannot activate Attendance Monitoring for more users than as licensed. Remember to activate Attendance Monitoring at the users.

Tip

- Refer to [3.1 Licence](#) for **2N® Access Commander** licence details.

FREE mode

Arrivals/departures in the FREE mode are recorded by the first/last use of a 2N reader during the day. The Presence module does not work in this mode.

IN-OUT mode

Arrivals/departures in the IN-OUT mode are always recorded by the arrival/departure reader (as set on the device). Use this mode to make the Presence module work properly.

Note

- IN/OUT for all devices – attendance is monitored for all the readers that the user may use for access. Movement between zones will not be recorded as attendance arrival/departure.
- IN-OUT for selected devices – attendance is monitored for selected readers only, e.g. at the main building entrance.

5.3 Device Monitoring

The Device monitoring module helps you find information on the devices connected. Every administrator can configure the module according to its needs. Each user has a unique setup.

Click Edit table display to change the table settings. A new window will open for you to add columns and change the column arrangement.

Icon	Device name	Device Status	Sip Proxy 1	Sip Proxy 2	Audio Test	Tamper Switch	Door state	Relay state	Up Time	
✓	AD-Digipress_MTZ-VNC	Online	Registered	Registered	N/A	N/A	N/A	Inactive	16d 23h 30m 40s	
✓	AD-Hansa_vndod-VNC	Online	Registered	Registered	N/A	N/A	N/A	Inactive	1d 11h 45m 0s	
✓	AD-Nokup_Lodden-VNC	Online	Registered	Registered	N/A	N/A	N/A	Inactive	17d 0h 13m 1s	
✓	AD-Opsvika-VNC	Online	Registered	Registered	N/A	N/A	N/A	Inactive	1d 11h 46m 30s	
✓	AD-Prisavik-VNC	Online	Registered	Registered	OK	N/A	N/A	Inactive	1d 21h 45m 21s	
✓	AD-Privat_MTZ_Prisavik-VNC	Online	Registered	Registered	N/A	N/A	N/A	Inactive	16d 23h 14m 5s	
✓	AD-Sansa_vika-AU	Online			N/A	N/A	N/A	Inactive	1d 11h 47m 22s	
✓	AD-Sansa_vika-480	Online			N/A	N/A	N/A	Inactive	1d 11h 45m 28s	
✓	AD-SDR_vika-VNC	Online	Registered	Registration in progress	N/A	N/A	N/A	Inactive	1d 11h 46m 37s	
✓	AD-Skorpens-VNC	Inactive			N/A	N/A	N/A	Inactive		

Table items:

- Icon – display the device state (OK or not).
- Device name
- Device state
- SIP Proxy – display the SIP Proxy state on a device. If there is an error, mouse click the description to get a detail.
- Audio test – display the last audio test result.
- Tamper switch – if there is an error, mouse click the description to know when the tamper switch was opened.
- Door state – four state options:
 - a. Closed
 - b. Open
 - c. Door open too long
 - d. Smashed door
- Relay state – two state options
 - a. Active

b. Inactive

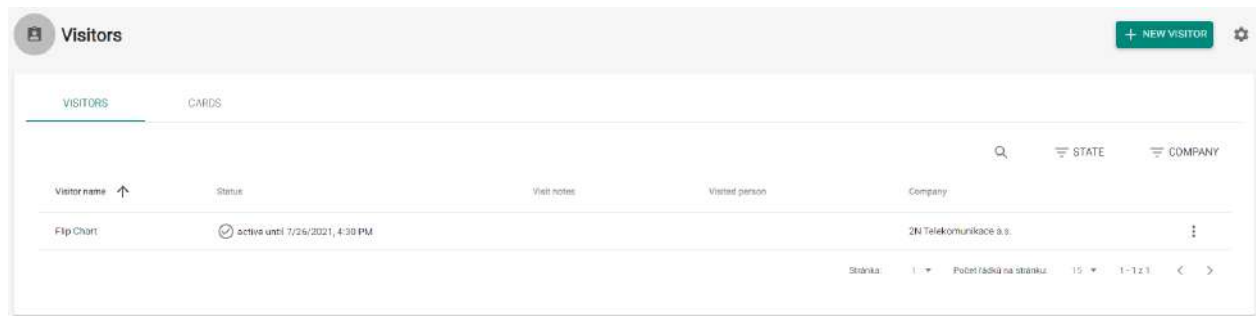
- Up time

Select whether the device shall be monitored or not. Click the crossed-out eye icon to disable device monitoring. The device will turn grey and move to the list end. Click the eye icon to re-enable device monitoring.

Click the row or pencil icon to display the device detail.

5.4 Visitors

It is possible to create visitor profiles in **2N® Access Commander** to assign access authorizations for a limited period of time. A visitor can be added an access card, access PIN code and car license plate number. Attendance is not monitored for a visitor.



Visitors

Visitor setting

The visitor including its details will be removed after a set period of time.

This setting can be used for meeting the local data protection regulations. The visitor name and note will be preserved in the access log as set in the log management.

Caution

- Visitors are automatically deleted every day at midnight after the time interval and set time period expire.
- The visitors that are still assigned their visitor cards are not deleted.

Visitor creation:

1. To create a new visitor, enter the visitor name and name of the company to be visited and assign an access group and time interval for a valid access.
2. Optionally, a visitor note and the person to be visited can be completed and an access card can be assigned.

Caution

- The visitor access time interval may not be longer than one month.

Note

- The count of visitors is not limited by any license.
- The visitor card can be entered manually, read from a reader or added as a predefined card.

Access logs

The access logs show the history of visitor accesses.


Access logs

	Time	User	Zone	Devices	Access data	Detail
✓	14.07.2021 15:34:10	11 (119)	API_Zone	2N IP Verso		
SHOW ALL						

Access methods

A visitor can be assigned an access card, access PIN or QR code and the visitor's car license plate (one license plate per visitor).

Credentials

	Card Not set	ASSIGN
	PIN / QR code 	+ PIN + QR
	License plate Not set	ADD

If the visitor's e-mail address is completed, the generated access PIN / QR code can be sent to this address.

Access

Access

From:

21.07.2021 13:43

To:

26.07.2021 16:30

In group

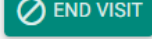
R&D

ADD

In the Access folder you can assign an access group and time interval for a valid visitor access.

End of visitation

The access validity expires when the set time interval expires. An End visit button is available for the visitor whose visit has been terminated automatically, because there may be different time zones on different devices. Hence, a visitor can have an invalid access on one device but a valid access on another one. This is because different time zones have been set for the devices.

If the administrator / manager ends a visit using the  button, the visitor access to the device access points is blocked instantly and the visitor cannot get through any device.

Cards

In the Cards folder you can create access cards to be assigned to visitors.

Visitors

+ NEW VISITOR

VISITORS CARDS

ADD

Search

COMPANY

Name	Company	Visitor
2.33	2N Telekomunikace a.s.	

Page: 1 Rows per page: 15 1 of 1

Caution

- The card that is assigned to a visitor cannot be deleted.

5.5 Notification

The Notification module helps you monitor selected system events and properties through e-mails or application bar notifications.

Notification + NEW NOTIFICATION				
Name ↑	Monitored events	Monitored devices	Channels	E-mail recipients
Device notifications	Device (connection) state, Directory limit exceeded, 3rd party (access) records ...	All		
Global	Device (connection) state, Mic/speaker status (Audio loop test), Lift module state ...	All		System admin
Security notifications	Forced entry, Device tampering, Door open too long ...	All		
System notifications	License problem, Low disk space			
Update available notification	New 2N® Access Commander version available, Unsupported device firmware			

Create a new notification:

1. Complete the notification name
2. Click Create

Create notification

Notification name *

Notification

CANCEL

CREATE

3. After creation, a new page is displayed for you to:
 - a. select the system events / properties to be monitored,
 - b. add the devices to be monitored,
 - c. add the users to be notified both in and off the system,
 - d. select the way of notification (e-mail, notification bar or both).

Device notifications

Name

Device notifications

MONITORED EVENTS

Device (connection) state

Directory limit exceeded

3rd party (access) records

Silent Alarm

Forced entry

Anti-passback violation

Anti-passback - area deactivation

Device tampering

CHANGE

CLEAR ALL

MONITORED DEVICES

☒ Monitor all devices: Yes

To add individual devices, disable monitoring of all devices.

ADD

CLEAR ALL

CHANNELS AND RECIPIENTS

☒ Notify via application bar: on

☐ Notify via e-mail: off

ADD

CLEAR ALL

Note

- Make sure that the [SMTP](#) is set correctly to make the e-mail notifications work properly.

5.6 CAM Logs

Set this function to record a few snapshots of the preceding and following event. Suppose you set recording of an applied card, for example. From now on, 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. See [here](#) for more details. When the storage is full, the oldest snapshots are deleted. The access logs are not deleted.

Make sure that firmware v. 2.18.0 or higher is downloaded to the intercoms to make the CAM logs work properly.

CAM Log Creation

Create CAM Log [X]

CAM Log name *

This field is mandatory.

Notification type

- ☒ Code entered
- ☐ Card applied
- ☐ Tamper switch activated
- ☐ Unauthorised door opening
- ☐ User accepted
- ☐ Remote door opening
- ☐ Bluetooth accepted
- ☐ Finger applied
- ☐
- ☐
- ☐

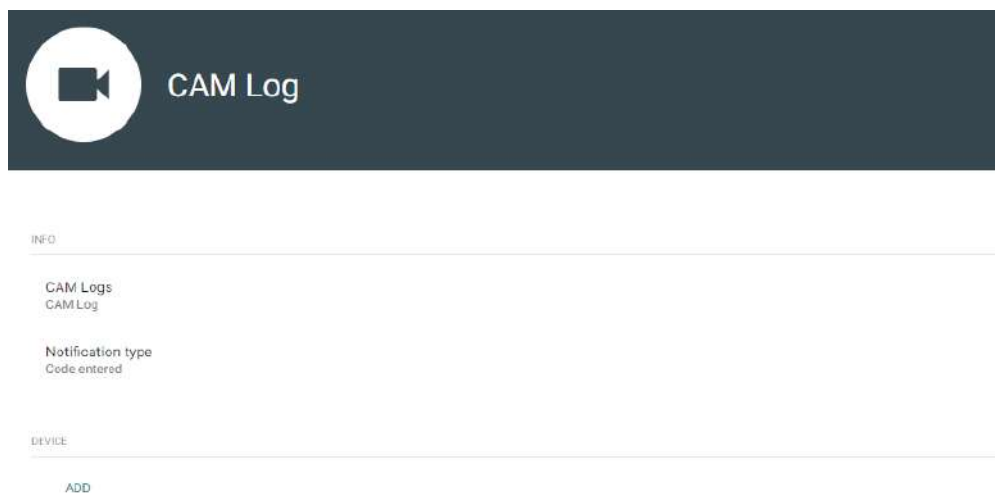
CANCEL CREATE

To create a CAM log, enter the log name and select one of the following notifications for the rule to be applied.

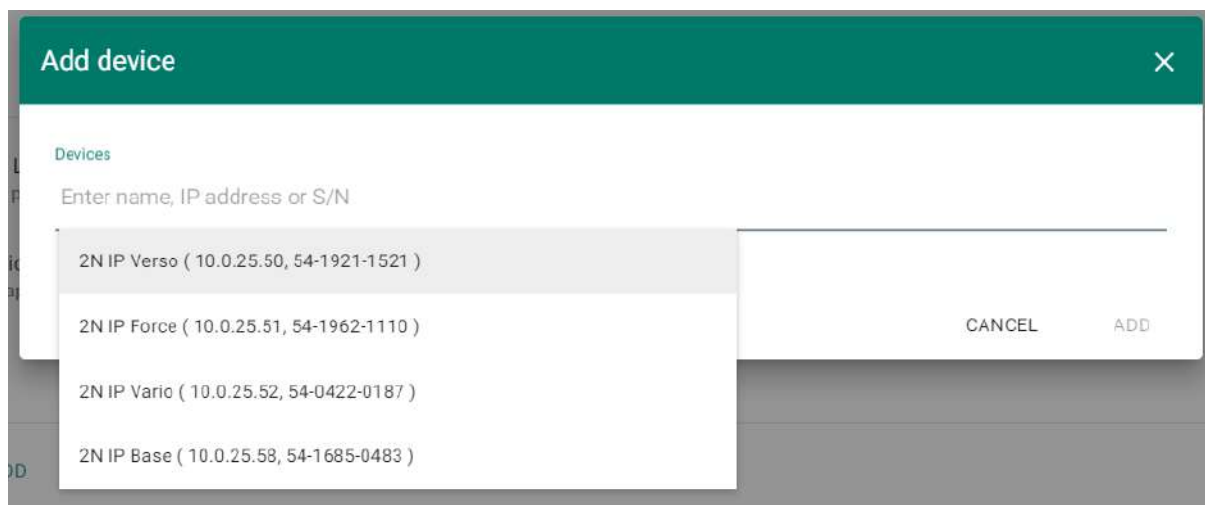
- Code entered
 - Take snapshots whenever the code is entered via the keypad.
- Card applied
 - Take snapshots whenever a card is applied. The snapshot is taken even if the user is not authorised.
- Tamper switch activated

- Take snapshots whenever the tamper switch is activated. Make sure that the function is set up in the **2N IP intercom**. For setup instructions refer to [Intercom Configuration](#).
- Unauthorised door opening
 - Take snapshots whenever the unauthorised door opening event is received. Make sure that the function is set up in the **2N IP intercom**. For setup instructions refer to [Intercom Configuration](#).
- User accepted
 - Take snapshots when the user authenticates itself.
- Remote door opening
 - Respond to door opening via DTMF or HTTP API.
- Bluetooth accepted
 - Take snapshots whenever the user sends Bluetooth authentication.
- Finger applied
 - Take snapshots whenever the user uses fingerprint authentication.
- User rejected
 - Take a snapshot when the user authentication is invalid.
- Access denied – repeated wrong entering
 - Take a snapshot when 5 invalid codes have been entered by the user.
- Silent alarm activated
 - Take a snapshot when the user activates the Silent alarm by entering a code that is higher by 1 than the right one. That means, the unlocking code is 123 and the Silent alarm code is 124. Or, when the user taps a finger to the fingerprint reader that is designated for Silent alarm activation.

Having entered the log name and selected an action, click Create. Once the CAM log is created, you are redirected to the CAM log detail.



Here choose the device(s) from which the CAM logs are to be downloaded.

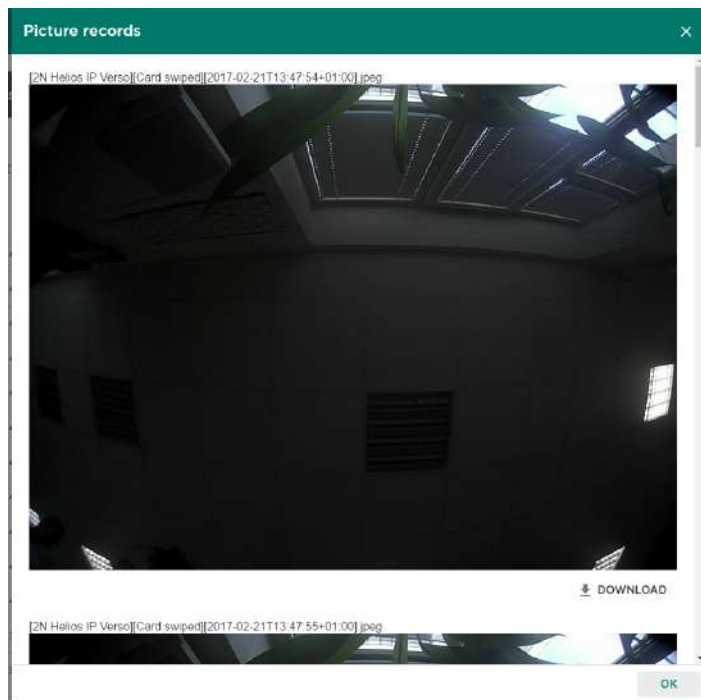


The access logs then display not only passage information but also an image displaying icon. No CAM logs are displayed for the intercoms that are not equipped with a camera.

CAM Log Viewing

Access logs							
FROM:	DD/MM/YY	FROM:	DD/MM/YY	EVENT TYPE	COMPANY	DEVICE	CARD ID
Time	Zone	Device	Event type	Event code	User	Description	
11.04.2018 10:44:08	Zone4	2N Helios IP Verso Onbia	Fingerprint			Direction unspecified	
11.04.2018 10:44:08	Zone4	2N Helios IP Verso Onbia	User authorized	User01		—	
11.04.2018 08:52:57	Zone4	2N Helios IP Verso Onbia	User authorized	User01		—	
11.04.2018 08:52:57	Zone4	2N Helios IP Verso Onbia	Bluetooth			Direction unspecified	
11.04.2018 08:50:38	Zone4	2N Helios IP Verso Onbia	User authorized	User01		—	
11.04.2018 08:50:38	Zone4	2N Helios IP Verso Onbia	Bluetooth			Direction unspecified	
11.04.2018 08:50:27	Zone4	2N Helios IP Verso Onbia	Bluetooth			Direction unspecified	

Click the icon to display the intercom image window.



Each snapshot header includes [device]event[time] information. The images are arranged from the oldest to the latest ones. Each snapshot can be downloaded separately.

Note

- The intercom snapshot size is up to 150 kB.

Note

- The tamper switch activated and Unauthorised door opening events are displayed in the system log.

Warning

- Make sure that correct time is set both for the intercom and the **2N® Access Commander** server to make the CAM logs work properly.

5.7 Area Restrictions

The Area restrictions menu helps you define the areas where the Anti-passback and Occupancy functions can be used.

Name	Status	Anti-passback	Occupancy	Current occupancy
Front Entry		Unused	Deny access	0/2
Relax Room		Unused	Deny access	0/6

List of Areas

The tab provides a list of all Anti-passback areas created in the system. Use the tab to create, delete and show details of the areas as well as deactivate and show states of the areas.

- functional
- non-functional

Exceptions

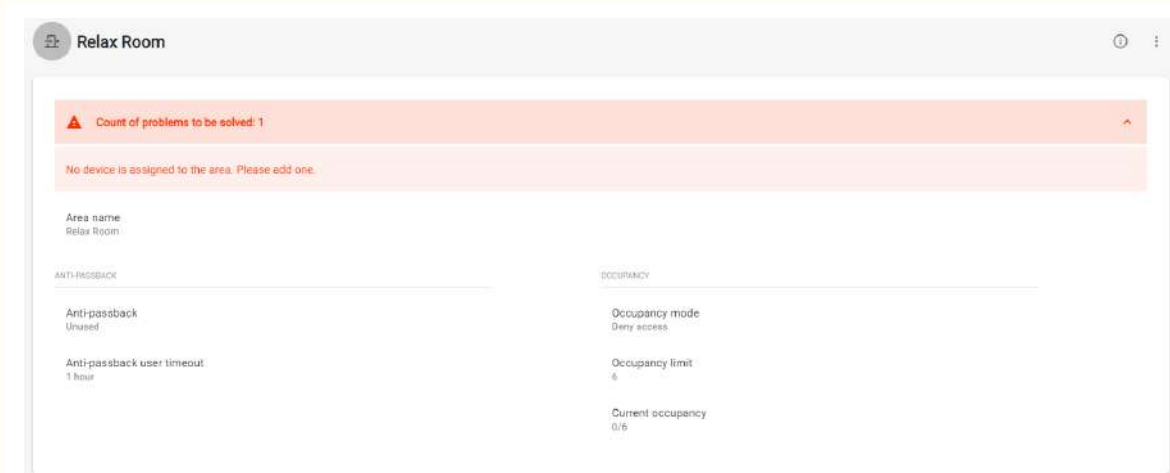
Use the tab to add and remove the users to which no Anti-passback rules are applied.

Note

- Typically, the exceptions are used for:
 - CEOs
 - building managers
 - VIP users

Settings

- Notify blocked user via email** – the Anti-passback rule-breaking user is sent an information e-mail.
- Reset** – set the day/time on which the Anti-passback log is deleted, i.e. when all the users are allowed to pass regardless of the previous Anti-passback breach.

Caution

If an area is set incorrectly and the function cannot work properly, a list of errors is displayed automatically on the area detail.

Caution**Most frequent Anti-passback problems:**

- No device is added to the APB area. Assign one device at least.
- The entry/exit is not defined. Assign one device at least to define the entry/exit direction.
- 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 licence.
- 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.

Warning

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

Anti-Passback Area Detail

You can activate the Anti-passback function for an area, which extends access control by including monitoring and preventing misuse of re-access to restricted areas. The monitored areas are defined by the border devices that help control entering / leaving the areas. Using these devices, the rights of the passing users are checked against the rules defined for the given area.

Front Entry	
Area name Front Entry	
ANTI-PASSBACK	
Anti-passback	Unused
Anti-passback user timeout	1 hour
OCCUPANCY	
Occupancy mode	Deny access
Occupancy limit	2
Current occupancy	0/2

Anti-passback type – set one of the Anti-passback modes:

- **Unused** – Anti-passback is inactive.
- **Log violations only** – a breach of conditions does not result in a restriction of the Anti-passback area access; the event is only recorded in the log with an optional administrator notification.
- **Deny access** – a breach of conditions results in a temporary or permanent restriction of the Anti-passback area access – can be unblocked by a timeout or upon the system administrator's instruction or by passage through the departure device.
- **User timeout** – set the time when the user will be allowed to re-access after a breach.

Occupancy

Occupancy management helps monitor and control the count of persons in an area. The count of persons in an area can be controlled by occupancy limits. Once the limit is reached, further access can be denied or limit exceeding can only be recorded. An entry / exit device is required for this functionality.

- **Occupancy mode** – set the occupancy mode.
 - **Unused** – occupancy is inactive.
 - **Log violations only** – occupancy limit exceeding is only recorded.
 - **Deny access** – once the occupancy limit is reached, further access is denied until the count of persons in the area drops below the limit.
- **Current occupancy** – set the occupancy limit for an area.

Devices

The tab displays all the devices that border the Anti-passback area.



Make sure that an active **Enhanced security** or **Gold licence** is available on all the edge devices.

- Refer to the [Configuration Manual for 2N IP Intercoms](#) for 2N IP intercom licences.
- No special licence is required for the **2N® Access Unit** models.

Caution

- The Access points in **2N® Access Commander** are marked 1 and 2 as follows:
 - **Access point 1 = Entry rules**
 - **Access point 2 = Exit rules**
- Make sure that a reader is added to the device for each Access point.

Device Settings before Adding to Area

Set the entry/exit rules in the [Door](#) section for selected devices to make Anti-passback work properly. Also, specify the entry/exit readers in the device settings. This setting is used for an independent device.

Blocking

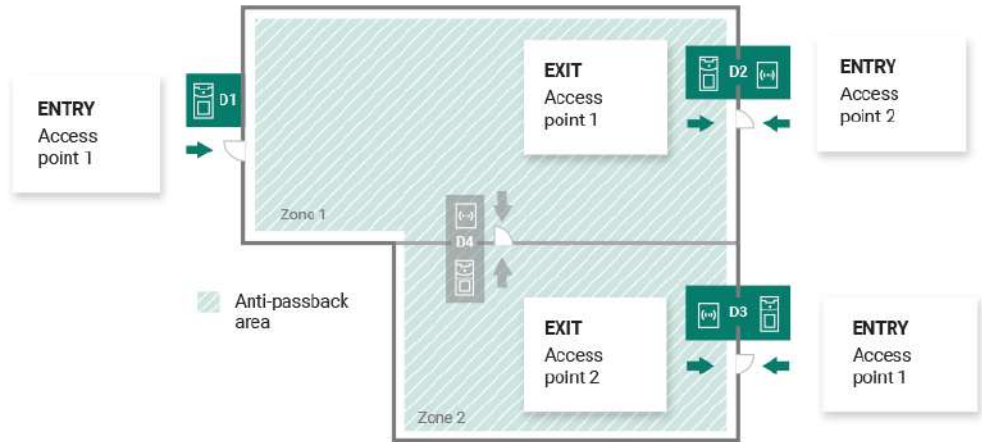
The tab displays the list of blocked users who tried to breach the Anti-passback rules. The system administrator can unblock a user by clicking the icon next to the username or unblock all the users at once by clicking Unblock all.

Warning

- The Anti-passback area becomes useless and can be potentially dangerous if there is a device in the area with an active REX button, which provides unauthorized access.

- [5.7.1 Example of Settings](#)

5.7.1 Example of Settings



The figure above shows an example of an Anti-passback area. All you have to do to set the Anti-passback function is configure the edge devices. The inside devices are not used for entry/exit control.

- **D1** – device D1 is only used for entry to the Anti-passback area.
 - Access point 1 is set for entry.
- **D2** – device D2 is used for both entry and exit.
 - Access point 2 is set for entry, Access point 1 is set for exit.
- **D3** – device D3 is used for both entry and exit.
 - Access point 1 is set for entry, Access point 2 is set for exit.

Caution

- The Access points in **2N® Access Commander** are marked 1 and 2 as follows:
 - **Access point 1 = Entry rules**
 - **Access point 2 = Exit rules**
- Make sure that a reader is added to the device for each Access point.

Name ↓	IP	Entry	Exit	
D1	10.0.25.140	Access point 1		🗑️
D2	10.27.20.10	Access point 2	Access point 1	🗑️
D3	10.0.25.151	Access point 1	Access point 2	🗑️

The table above sums up the device settings in the figure above. Any Access point can be used for entry/exit.

6. HTTP API

- [6.1 API Documentation version 2](#)
- [6.2 API Documentation version 3](#)
- [6.3 HTTP API Changes version 2](#)
- [6.4 HTTP API changes version 3](#)

6.1 API Documentation version 2

6.2 API Documentation version 3

6.3 HTTP API Changes version 2

Caution

- The section includes the **2N® Access Commander API** upgrade changes. The changes below may make your API communication, whatever it is, non-functional.

Version 2.4 to 2.5

What's New

- GET /api/v2/Devices/ntpmode null
- PUT /api/v2/Devices/ntpmode null

What's Deprecated

- GET /api/v2/Users/{userId}/widgets null
- PUT /api/v2/Users/{userId}/widgets null

What's Changed

GET /api/v2/Antipassback/areas null

Return Type

```
Modify data.Devices.AP0Properties  
Modify data.Devices.AP1Properties
```

POST /api/v2/Antipassback/areas null

Parameters

Modify body.Devices.AP0Properties

Modify body.Devices.AP1Properties

Return Type

Modify data.Devices.AP0Properties

Modify data.Devices.AP1Properties

DELETE /api/v2/Antipassback/areas/{areaid} null

Parameters

Modify body.Devices.AP0Properties

Modify body.Devices.AP1Properties

GET /api/v2/Antipassback/areas/{areaid} null

Return Type

Modify data.Devices.AP0Properties

Modify data.Devices.AP1Properties

PUT /api/v2/Antipassback/areas/{areaid} null

Parameters

Modify body.Devices.AP0Properties

Modify body.Devices.AP1Properties

Return Type

Modify data.Devices.AP0Properties

Modify data.Devices.AP1Properties

PUT /api/v2/Antipassback/areas/{areaid}/devices/{deviceid} null

Parameters

Modify body.AP0Properties

Modify body.AP1Properties

DELETE /api/v2/Antipassback/areas/{areaid}/devices null

Parameters

Insert body.LiftFloors.Type

Insert body.LastBackup.Type

Return Type

Modify data.Devices.AP0Properties

Modify data.Devices.AP1Properties

PUT /api/v2/Antipassback/areas/{areaid}/devices null

Parameters

Insert body.LiftFloors.Type

Insert body.LastBackup.Type

Return Type

Modify data.Devices.AP0Properties

Modify data.Devices.AP1Properties

DELETE /api/v2/Antipassback/areas/{areaid}/blocked null

Parameters

Insert body.Type

PATCH /api/v2/Antipassback/resets null

Parameters

Delete body.Id

PUT /api/v2/users/{userId}/attendance/export.csv null

Parameters

Insert body.Users.Type

PUT /api/v2/users/{userId}/attendance/export.pdf null

Parameters

Insert body.Users.Type

PUT /api/v2/users/attendance/export.pdf null

Parameters

Insert body.Users.Type

PUT /api/v2/users/attendance/export.csv null

Parameters

Insert body.Users.Type

PUT /api/v2/Companies/{companyId}/holidays/copy null

Parameters

Insert body.Type

GET /api/v2/Devices null

Return Type

Insert data.LiftFloors.Type

Insert data.LastBackup.Type

POST /api/v2/Devices null

Parameters

Insert body.LiftFloors.Type

Insert body.LastBackup.Type

Return Type

Insert data.LiftFloors.Type

Insert data.LastBackup.Type

PATCH /api/v2/Devices null

Parameters

Insert body.LiftFloors.Type

Insert body.LastBackup.Type

DELETE /api/v2/Devices/{deviceId} null

Parameters

Insert body.LiftFloors.Type

Insert body.LastBackup.Type

Return Type

Insert data.LiftFloors.Type

Insert data.LastBackup.Type

GET /api/v2/Devices/{deviceId} null

Return Type

Insert data.LiftFloors.Type

Insert data.LastBackup.Type

PUT /api/v2/Devices/{deviceId} null

Parameters

Insert body.LiftFloors.Type

Insert body.LastBackup.Type

Return Type

Insert data.LiftFloors.Type

Insert data.LastBackup.Type

GET /api/v2/Devices/scannetwork null

Return Type

Insert data.LiftFloors.Type

Insert data.LastBackup.Type

DELETE /api/v2/Devices/{deviceId}/cleardirectory null

Parameters

Insert body.LiftFloors.Type

Insert body.LastBackup.Type

DELETE /api/v2/Devices/{deviceId}/factoryreset null

Parameters

Insert body.LiftFloors.Type

Insert body.LastBackup.Type

PUT /api/v2/Devices/backup null

Parameters

Insert body.LiftFloors.Type

Insert body.LastBackup.Type

GET /api/v2/Devices/{deviceId}/password null

Return Type

Insert data.LiftFloors.Type

Insert data.LastBackup.Type

PUT /api/v2/Devices/{deviceId}/password null

Parameters

```

    Insert body.LiftFloors.Type
    Insert body.LastBackup.Type
Return Type

```

```

    Insert data.LiftFloors.Type
    Insert data.LastBackup.Type

```

PUT /api/v2/Devices/{deviceId}/password/generate null

Parameters

```

    Insert body.LiftFloors.Type
    Insert body.LastBackup.Type
Return Type

```

```

    Insert data.LiftFloors.Type
    Insert data.LastBackup.Type

```

PUT /api/v2/Devices/{deviceId}/replace null

Parameters

```

    Insert body.LiftFloors.Type
    Insert body.LastBackup.Type
Return Type

```

```

    Insert data.LiftFloors.Type
    Insert data.LastBackup.Type

```

PUT /api/v2/DeviceUpdate/firmware/{firmwareId}/candidate/devicetest null

Parameters

```

    Insert body.SerialNumber
    Insert body.IPAddress
    Insert body.MACAddress
    Insert body.ProductName
    Insert body.SoftwareVersion
    Insert body.ButtonCount
    Insert body.Buttons
    Insert body.Keypad
    Insert body.Ap0Zone
    Insert body.Ap1Zone
    Insert body.LiftModules
    Insert body.LiftFloors
    Insert body.HasAccessControl
    Insert body.HasDoorControl
    Insert body.Display
    Insert body.KeyBoard
    Insert body.Camera
    Insert body.HasRexButton
    Insert body.DoorSwitch
    Insert body.HasLiftControl
    Insert body.LiftEnabled
    Insert body.HasHiSecFeatures
    Insert body.IsSupportedFirmware
    Insert body.IsAllowedFirmware
    Insert body.IsLicensedDevice

```

```

Insert body.HasBackup
Insert body.LastBackup
Insert body.BackupState
Insert body.RestoreState
Insert body.UploadState
Insert body.IsInSystem
Insert body.Status
Insert body.Lockdown
Insert body.Ap0Modules
Insert body.Ap1Modules
Insert body.HasDisplayFolderImages
Insert body.HasVirtualNumbers
Insert body.AttendanceEnabled
Insert body.CamLogSupported
Insert body.IsFirmwareLocked
Insert body.IsAnsweringUnit
Insert body.IsIndoorTouch
Insert body.IsIndoorTouch2
Insert body.IsLockdownable
Insert body.HasSwitchControl
Insert body.Problems
Insert body.ModifiedGuid
Insert body.Type
Insert body.IsLockdownActiveAndConfirmed
Insert body.IsLockdownUnConfirmed
Delete body.Hardware
Delete body.State
Delete body.IpAddress
Delete body.RecordingAttendance
Delete body.AccessControl
Delete body.Calling
Delete body.Firmware
Delete body.Revision

```

Return Type

```

Insert data.LiftFloors.Type
Insert data.LastBackup.Type

```

GET /api/v2/Groups/{groupId}/members null

Return Type

```

Insert data.Type

```

GET /api/v2/Notifications null

Return Type

```

Modify data.Events

```

POST /api/v2/Notifications null

Parameters

```

Modify body.Events

```

Return Type

Modify data.Events

GET /api/v2/Notifications/types null

Return Type

Modify data

DELETE /api/v2/Notifications/{notificationId} null

Parameters

Modify body.Events

GET /api/v2/Notifications/{notificationId} null

Return Type

Modify data.Events

PUT /api/v2/Notifications/{notificationId} null

Parameters

Modify body.Events

Return Type

Modify data.Events

GET /api/v2/Snapshots/setting null

Return Type

Insert data.Devices.LiftFloors.Type

Insert data.Devices.LastBackup.Type

POST /api/v2/Snapshots/setting null

Parameters

Insert body.Devices.LiftFloors.Type

Insert body.Devices.LastBackup.Type

Return Type

Insert data.Devices.LiftFloors.Type

Insert data.Devices.LastBackup.Type

DELETE /api/v2/Snapshots/setting/{camLogId} null

Parameters

Insert body.Devices.LiftFloors.Type

Insert body.Devices.LastBackup.Type

GET /api/v2/Snapshots/setting/{camLogId} null

Return Type

Insert data.Devices.LiftFloors.Type

Insert data.Devices.LastBackup.Type

PUT /api/v2/Snapshots/setting/{camLogId} null

Parameters

Insert body.Devices.LiftFloors.Type

Insert body.Devices.LastBackup.Type

Return Type

Insert data.Devices.LiftFloors.Type

Insert data.Devices.LastBackup.Type

DELETE /api/v2/Snapshots/setting/{camLogId}/devices null

Parameters

Insert body.LiftFloors.Type

Insert body.LastBackup.Type

Return Type

Insert data.LiftFloors.Type

Insert data.LastBackup.Type

GET /api/v2/Snapshots/setting/{camLogId}/devices null

Return Type

Insert data.LiftFloors.Type

Insert data.LastBackup.Type

PUT /api/v2/Snapshots/setting/{camLogId}/devices null

Parameters

Insert body.LiftFloors.Type

Insert body.LastBackup.Type

Return Type

Insert data.LiftFloors.Type

Insert data.LastBackup.Type

GET /api/v2/System/logs/system null

Return Type

Modify data.NotificationEvent

GET /api/v2/System/mobilekey null

Return Type

Insert UseDongle

Insert Keys

Insert ModifiedGuid

PUT /api/v2/System/mobilekey null

Parameters

Insert body.Keys.Modified

Return Type

Insert data

DELETE /api/v2/System/mobilekey/keys/{ordinal} null

Return Type

Insert data

POST /api/v2/System/mobilekey/keys null

Return Type

Insert data

GET /api/v2/System/securecardssetting null

Return Type

Insert data.Revision

Delete data.ModifiedGuid

PUT /api/v2/System/securecardssetting null

Return Type

Insert data.Revision

Delete data.ModifiedGuid

GET /api/v2/TimeProfiles null

Return Type

Delete data.Intervals.DayOfWeek

Delete data.Intervals.Enabled

Delete data.Intervals.From

Delete data.Intervals.To

Delete data.Intervals.Id

Delete data.Intervals.Revision

POST /api/v2/TimeProfiles null

Parameters

Delete body.Intervals.DayOfWeek

Delete body.Intervals.Enabled

Delete body.Intervals.From

Delete body.Intervals.To

Delete body.Intervals.Id

Delete body.Intervals.Revision

Return Type

Delete data.Intervals.DayOfWeek

Delete data.Intervals.Enabled

Delete data.Intervals.From

Delete data.Intervals.To

Delete data.Intervals.Id

Delete data.Intervals.Revision

DELETE /api/v2/TimeProfiles/{timeProfileId} null

Parameters

Delete body.Intervals.DayOfWeek

Delete body.Intervals.Enabled

Delete body.Intervals.From

Delete body.Intervals.To

Delete body.Intervals.Id

Delete body.Intervals.Revision

GET /api/v2/TimeProfiles/{timeProfileId} null

Return Type

Delete data.Intervals.DayOfWeek
Delete data.Intervals.Enabled
Delete data.Intervals.From
Delete data.Intervals.To
Delete data.Intervals.Id
Delete data.Intervals.Revision

PUT /api/v2/TimeProfiles/{timeProfileId} null

Parameters

Delete body.Intervals.DayOfWeek
Delete body.Intervals.Enabled
Delete body.Intervals.From
Delete body.Intervals.To
Delete body.Intervals.Id
Delete body.Intervals.Revision

Return Type

Delete data.Intervals.DayOfWeek
Delete data.Intervals.Enabled
Delete data.Intervals.From
Delete data.Intervals.To
Delete data.Intervals.Id
Delete data.Intervals.Revision

GET /api/v2/TimeProfiles/{timeProfileId}/days null

Return Type

Delete data.Intervals.DayOfWeek
Delete data.Intervals.Enabled
Delete data.Intervals.From
Delete data.Intervals.To
Delete data.Intervals.Id
Delete data.Intervals.Revision

DELETE /api/v2/Users/{userId} null

Parameters

Insert body.PhoneNumbers.TimeProfile.Monday
Insert body.PhoneNumbers.TimeProfile.Tuesday
Insert body.PhoneNumbers.TimeProfile.Wednesday
Insert body.PhoneNumbers.TimeProfile.Thursday
Insert body.PhoneNumbers.TimeProfile.Friday
Insert body.PhoneNumbers.TimeProfile.Saturday
Insert body.PhoneNumbers.TimeProfile.Sunday
Insert body.PhoneNumbers.TimeProfile.Holiday
Insert body.PhoneNumbers.TimeProfile.Type
Delete body.PhoneNumbers.TimeProfile.Intervals

GET /api/v2/Users/{userId} null

Return Type

```

Insert data.PhoneNumbers.TimeProfile.Monday
Insert data.PhoneNumbers.TimeProfile.Tuesday
Insert data.PhoneNumbers.TimeProfile.Wednesday
Insert data.PhoneNumbers.TimeProfile.Thursday
Insert data.PhoneNumbers.TimeProfile.Friday
Insert data.PhoneNumbers.TimeProfile.Saturday
Insert data.PhoneNumbers.TimeProfile.Sunday
Insert data.PhoneNumbers.TimeProfile.Holiday
Insert data.PhoneNumbers.TimeProfile.Type
Delete data.PhoneNumbers.TimeProfile.Intervals

```

PUT /api/v2/Users/{userId} null

Parameters

```

Insert body.PhoneNumbers.TimeProfile.Monday
Insert body.PhoneNumbers.TimeProfile.Tuesday
Insert body.PhoneNumbers.TimeProfile.Wednesday
Insert body.PhoneNumbers.TimeProfile.Thursday
Insert body.PhoneNumbers.TimeProfile.Friday
Insert body.PhoneNumbers.TimeProfile.Saturday
Insert body.PhoneNumbers.TimeProfile.Sunday
Insert body.PhoneNumbers.TimeProfile.Holiday
Insert body.PhoneNumbers.TimeProfile.Type
Delete body.PhoneNumbers.TimeProfile.Intervals

```

Return Type

```

Insert data.PhoneNumbers.TimeProfile.Monday
Insert data.PhoneNumbers.TimeProfile.Tuesday
Insert data.PhoneNumbers.TimeProfile.Wednesday
Insert data.PhoneNumbers.TimeProfile.Thursday
Insert data.PhoneNumbers.TimeProfile.Friday
Insert data.PhoneNumbers.TimeProfile.Saturday
Insert data.PhoneNumbers.TimeProfile.Sunday
Insert data.PhoneNumbers.TimeProfile.Holiday
Insert data.PhoneNumbers.TimeProfile.Type
Delete data.PhoneNumbers.TimeProfile.Intervals

```

DELETE /api/v2/Users null

Parameters

```

Insert body.PhoneNumbers.TimeProfile.Monday
Insert body.PhoneNumbers.TimeProfile.Tuesday
Insert body.PhoneNumbers.TimeProfile.Wednesday
Insert body.PhoneNumbers.TimeProfile.Thursday
Insert body.PhoneNumbers.TimeProfile.Friday
Insert body.PhoneNumbers.TimeProfile.Saturday
Insert body.PhoneNumbers.TimeProfile.Sunday
Insert body.PhoneNumbers.TimeProfile.Holiday
Insert body.PhoneNumbers.TimeProfile.Type
Delete body.PhoneNumbers.TimeProfile.Intervals

```

GET /api/v2/Users null

Return Type

```

Insert data.PhoneNumbers.TimeProfile.Monday
Insert data.PhoneNumbers.TimeProfile.Tuesday
Insert data.PhoneNumbers.TimeProfile.Wednesday
Insert data.PhoneNumbers.TimeProfile.Thursday
Insert data.PhoneNumbers.TimeProfile.Friday
Insert data.PhoneNumbers.TimeProfile.Saturday
Insert data.PhoneNumbers.TimeProfile.Sunday
Insert data.PhoneNumbers.TimeProfile.Holiday
Insert data.PhoneNumbers.TimeProfile.Type
Delete data.PhoneNumbers.TimeProfile.Intervals

```

POST /api/v2/Users null

Parameters

```

Insert body.PhoneNumbers.TimeProfile.Monday
Insert body.PhoneNumbers.TimeProfile.Tuesday
Insert body.PhoneNumbers.TimeProfile.Wednesday
Insert body.PhoneNumbers.TimeProfile.Thursday
Insert body.PhoneNumbers.TimeProfile.Friday
Insert body.PhoneNumbers.TimeProfile.Saturday
Insert body.PhoneNumbers.TimeProfile.Sunday
Insert body.PhoneNumbers.TimeProfile.Holiday
Insert body.PhoneNumbers.TimeProfile.Type
Delete body.PhoneNumbers.TimeProfile.Intervals

```

Return Type

```

Insert data.PhoneNumbers.TimeProfile.Monday
Insert data.PhoneNumbers.TimeProfile.Tuesday
Insert data.PhoneNumbers.TimeProfile.Wednesday
Insert data.PhoneNumbers.TimeProfile.Thursday
Insert data.PhoneNumbers.TimeProfile.Friday
Insert data.PhoneNumbers.TimeProfile.Saturday
Insert data.PhoneNumbers.TimeProfile.Sunday
Insert data.PhoneNumbers.TimeProfile.Holiday
Insert data.PhoneNumbers.TimeProfile.Type
Delete data.PhoneNumbers.TimeProfile.Intervals

```

PUT /api/v2/Users/attendanceMonitoring null

Parameters

```

Insert body.PhoneNumbers.TimeProfile.Monday
Insert body.PhoneNumbers.TimeProfile.Tuesday
Insert body.PhoneNumbers.TimeProfile.Wednesday
Insert body.PhoneNumbers.TimeProfile.Thursday
Insert body.PhoneNumbers.TimeProfile.Friday
Insert body.PhoneNumbers.TimeProfile.Saturday
Insert body.PhoneNumbers.TimeProfile.Sunday
Insert body.PhoneNumbers.TimeProfile.Holiday
Insert body.PhoneNumbers.TimeProfile.Type
Delete body.PhoneNumbers.TimeProfile.Intervals

```

GET /api/v2/Users/{userId}/mobilekey null

Return Type

```

Delete data.Settings.ModifiedGuid

```

DELETE /api/v2/Users/{userId}/mobilekey/{authId} null

Return Type

Delete data.Settings.ModifiedGuid

PUT /api/v2/Users/{userId}/mobilekey/pairing/start null

Return Type

Delete data.Settings.ModifiedGuid

PUT /api/v2/Users/{userId}/mobilekey/pairing/stop null

Return Type

Delete data.Settings.ModifiedGuid

PUT /api/v2/Users/{userId}/mobilekey/pairing/dongle null

Return Type

Delete data.Settings.ModifiedGuid

POST /api/v2/Users/{id}/pin null

Return Type

Insert data.PhoneNumbers.TimeProfile.Monday
 Insert data.PhoneNumbers.TimeProfile.Tuesday
 Insert data.PhoneNumbers.TimeProfile.Wednesday
 Insert data.PhoneNumbers.TimeProfile.Thursday
 Insert data.PhoneNumbers.TimeProfile.Friday
 Insert data.PhoneNumbers.TimeProfile.Saturday
 Insert data.PhoneNumbers.TimeProfile.Sunday
 Insert data.PhoneNumbers.TimeProfile.Holiday
 Insert data.PhoneNumbers.TimeProfile.Type
 Delete data.PhoneNumbers.TimeProfile.Intervals

POST /api/v2/Users/{id}/qrcode null

Return Type

Insert data.PhoneNumbers.TimeProfile.Monday
 Insert data.PhoneNumbers.TimeProfile.Tuesday
 Insert data.PhoneNumbers.TimeProfile.Wednesday
 Insert data.PhoneNumbers.TimeProfile.Thursday
 Insert data.PhoneNumbers.TimeProfile.Friday
 Insert data.PhoneNumbers.TimeProfile.Saturday
 Insert data.PhoneNumbers.TimeProfile.Sunday
 Insert data.PhoneNumbers.TimeProfile.Holiday
 Insert data.PhoneNumbers.TimeProfile.Type
 Delete data.PhoneNumbers.TimeProfile.Intervals

POST /api/v2/Users/{userId}/phonenumbers null

Parameters

Insert body.TimeProfile.Monday
 Insert body.TimeProfile.Tuesday
 Insert body.TimeProfile.Wednesday
 Insert body.TimeProfile.Thursday
 Insert body.TimeProfile.Friday
 Insert body.TimeProfile.Saturday

```

Insert body.TimeProfile.Sunday
Insert body.TimeProfile.Holiday
Insert body.TimeProfile.Type
Delete body.TimeProfile.Intervals

```

Return Type

```

Insert data.TimeProfile.Monday
Insert data.TimeProfile.Tuesday
Insert data.TimeProfile.Wednesday
Insert data.TimeProfile.Thursday
Insert data.TimeProfile.Friday
Insert data.TimeProfile.Saturday
Insert data.TimeProfile.Sunday
Insert data.TimeProfile.Holiday
Insert data.TimeProfile.Type
Delete data.TimeProfile.Intervals

```

DELETE /api/v2/Users/{userId}/phonenumbers/{phoneNumberId} null

Parameters

```

Insert body.TimeProfile.Monday
Insert body.TimeProfile.Tuesday
Insert body.TimeProfile.Wednesday
Insert body.TimeProfile.Thursday
Insert body.TimeProfile.Friday
Insert body.TimeProfile.Saturday
Insert body.TimeProfile.Sunday
Insert body.TimeProfile.Holiday
Insert body.TimeProfile.Type
Delete body.TimeProfile.Intervals

```

PUT /api/v2/Users/{userId}/phonenumbers/{phoneNumberId} null

Parameters

```

Insert body.TimeProfile.Monday
Insert body.TimeProfile.Tuesday
Insert body.TimeProfile.Wednesday
Insert body.TimeProfile.Thursday
Insert body.TimeProfile.Friday
Insert body.TimeProfile.Saturday
Insert body.TimeProfile.Sunday
Insert body.TimeProfile.Holiday
Insert body.TimeProfile.Type
Delete body.TimeProfile.Intervals

```

Return Type

```

Insert data.TimeProfile.Monday
Insert data.TimeProfile.Tuesday
Insert data.TimeProfile.Wednesday
Insert data.TimeProfile.Thursday
Insert data.TimeProfile.Friday
Insert data.TimeProfile.Saturday
Insert data.TimeProfile.Sunday

```

```

Insert data.TimeProfile.Holiday
Insert data.TimeProfile.Type
Delete data.TimeProfile.Intervals

```

PUT /api/v2/Users/{userId}/password null

Return Type

```

Insert data.PhoneNumbers.TimeProfile.Monday
Insert data.PhoneNumbers.TimeProfile.Tuesday
Insert data.PhoneNumbers.TimeProfile.Wednesday
Insert data.PhoneNumbers.TimeProfile.Thursday
Insert data.PhoneNumbers.TimeProfile.Friday
Insert data.PhoneNumbers.TimeProfile.Saturday
Insert data.PhoneNumbers.TimeProfile.Sunday
Insert data.PhoneNumbers.TimeProfile.Holiday
Insert data.PhoneNumbers.TimeProfile.Type
Delete data.PhoneNumbers.TimeProfile.Intervals

```

GET /api/v2/visitors null

Return Type

```

Insert data.VisitorCard.Type
Insert data.PinCollisions.Type

```

POST /api/v2/visitors null

Parameters

```

Insert body.VisitorCard.Type
Insert body.PinCollisions.Type

```

Return Type

```

Insert data.VisitorCard.Type
Insert data.PinCollisions.Type

```

DELETE /api/v2/visitors/{id} null

Parameters

```

Insert body.VisitorCard.Type
Insert body.PinCollisions.Type

```

GET /api/v2/visitors/{id} null

Return Type

```

Insert data.VisitorCard.Type
Insert data.PinCollisions.Type

```

PUT /api/v2/visitors/{id} null

Parameters

```

Insert body.VisitorCard.Type
Insert body.PinCollisions.Type

```

Return Type

```

Insert data.VisitorCard.Type
Insert data.PinCollisions.Type

```

POST /api/v2/visitors/{id}/pin null

Return Type

Insert data.VisitorCard.Type
Insert data.PinCollisions.Type

POST /api/v2/visitors/{id}/qrcode null

Return Type

Insert data.VisitorCard.Type
Insert data.PinCollisions.Type

POST /api/v2/visitors/cards null

Parameters

Insert body.Type

GET /api/v2/Zones/{zoneId}/companies null

Return Type

Insert data.Type

6.4 HTTP API changes version 3

Caution

- The section includes the **2N® Access Commander API** upgrade changes. The changes below may make your API communication, whatever it is, non-functional.

Version 2.4 to 2.5 (API v3)

What's New

- GET /api/v3/AccessRules null
- POST /api/v3/AccessRules null
- PATCH /api/v3/AccessRules null
- POST /api/v3/AccessRules/bulk null
- GET /api/v3/AccessRules/{ruleId} null
- PUT /api/v3/AccessRules/{ruleId} null
- DELETE /api/v3/AccessRules/{ruleId} null
- PATCH /api/v3/AccessRules/{accessRuleId} null
- GET /api/v3/Areas null
- POST /api/v3/Areas null
- PATCH /api/v3/Areas null
- GET /api/v3/Areas/{areaId} null
- PUT /api/v3/Areas/{areaId} null
- DELETE /api/v3/Areas/{areaId} null

- PATCH /api/v3/Areas/{areaid} null
- GET /api/v3/Areas/antipassback/setting null
- PUT /api/v3/Areas/antipassback/setting null
- PATCH /api/v3/Areas/antipassback/setting null
- DELETE /api/v3/Areas/{areaid}/antipassback/blocked null
- GET /api/v3/users/{userId}/attendance null
- GET /api/v3/users/{userId}/attendance/{year}/{month} null
- POST /api/v3/users/{userId}/attendance/intervals null
- PUT /api/v3/users/{userId}/attendance/intervals/{intervalId} null
- DELETE /api/v3/users/{userId}/attendance/intervals/{intervalId} null
- PUT /api/v3/users/{userId}/attendance/{year}/{month}/export.csv null
- PUT /api/v3/users/{userId}/attendance/{year}/{month}/export.pdf null
- PUT /api/v3/users/attendance/{year}/{month}/export.pdf null
- PUT /api/v3/users/attendance/export.csv null
- PUT /api/v3/system/backup/run null
- GET /api/v3/system/backup/storage null
- PUT /api/v3/system/backup/storage null
- GET /api/v3/system/backup/periodic null
- PUT /api/v3/system/backup/periodic null
- DELETE /api/v3/system/backup/periodic null
- PUT /api/v3/system/restore/file null
- DELETE /api/v3/system/restore/file null
- PUT /api/v3/system/restore null
- GET /api/v3/system/restore/files null
- DELETE /api/v3/system/restore/files null
- GET /api/v3/system/restore/files/download/{location}/{fileName} null
- PUT /api/v3/system/import null
- GET /api/v3/search null
- GET /api/v3/search/suggestions null
- GET /api/v3/search/suggestions/accesslog null
- GET /api/v3/search/suggestions/systemlog null
- GET /api/v3/search/suggestions/lockdown null
- GET /api/v3/presence null
- GET /api/v3/CamLogs null
- POST /api/v3/CamLogs null
- PATCH /api/v3/CamLogs null
- GET /api/v3/CamLogs/{camLogId} null
- PUT /api/v3/CamLogs/{camLogId} null
- DELETE /api/v3/CamLogs/{camLogId} null
- PATCH /api/v3/CamLogs/{camLogId} null
- GET /api/v3/CamLogs/eventtypes null
- GET /api/v3/CamLogs/{camLogId}/devices null
- GET /api/v3/Dashboard/info null
- GET /api/v3/Devices/ntpmode null

- PUT /api/v3/Devices/ntpmode null
- GET /api/v3/DeviceUpdate null
- PUT /api/v3/DeviceUpdate null
- PUT /api/v3/DeviceUpdate/firmware/{firmwareId}/current null
- DELETE /api/v3/DeviceUpdate/firmware/{firmwareId}/current null
- PUT /api/v3/DeviceUpdate/firmware/{firmwareId}/candidate/deploy null
- PUT /api/v3/DeviceUpdate/firmware/{firmwareId}/candidate/devicetest null
- GET /api/v3/DeviceUpdate/firmware/{firmwareId}/candidate/releasenotes null
- GET /api/v3/Groups null
- POST /api/v3/Groups null
- PATCH /api/v3/Groups null
- GET /api/v3/Groups/{groupId} null
- PUT /api/v3/Groups/{groupId} null
- DELETE /api/v3/Groups/{groupId} null
- PATCH /api/v3/Groups/{groupId} null
- GET /api/v3/Groups/{groupId}/members null
- PUT /api/v3/Groups/{groupId}/members null
- DELETE /api/v3/Groups/{groupId}/members null
- PUT /api/v3/Lockdown/activate null
- PUT /api/v3/Lockdown/deactivate null
- GET /api/v3/Notifications null
- POST /api/v3/Notifications null
- PATCH /api/v3/Notifications null
- GET /api/v3/Notifications/types null
- PUT /api/v3/Notifications/clear null
- GET /api/v3/Notifications/{notificationId} null
- PUT /api/v3/Notifications/{notificationId} null
- DELETE /api/v3/Notifications/{notificationId} null
- PATCH /api/v3/Notifications/{notificationId} null
- GET /api/v3/SignalR/topics null
- GET /api/v3/System/attendance null
- PUT /api/v3/System/attendance null
- GET /api/v3/System/license null
- PUT /api/v3/System/license/import.xml null
- PUT /api/v3/System/license/activatebasic null
- PUT /api/v3/System/license/renew null
- GET /api/v3/System/logs/attendance null
- GET /api/v3/System/logs/attendance/export.csv null
- GET /api/v3/System/logs/system null
- GET /api/v3/System/logs/system/export.csv null
- GET /api/v3/System/smtp null
- PUT /api/v3/System/smtp null
- PUT /api/v3/System/smtp/sendtestemail null
- GET /api/v3/System/smtp/status null

- GET /api/v3/System/http null
- PUT /api/v3/System/http null
- GET /api/v3/System/zones null
- PUT /api/v3/System/zones null
- GET /api/v3/System/visitors null
- PUT /api/v3/System/visitors null
- GET /api/v3/System/updatesetting null
- PUT /api/v3/System/updatesetting null
- GET /api/v3/System/update/status null
- GET /api/v3/System/update/check null
- GET /api/v3/System/update/download null
- DELETE /api/v3/System/update/download null
- PUT /api/v3/System/update/run null
- GET /api/v3/System/licenseagreement null
- PUT /api/v3/System/licenseagreement null
- GET /api/v3/System/mobilekey/keys null
- POST /api/v3/System/mobilekey/keys null
- DELETE /api/v3/System/mobilekey/keys/{ordinal} null
- PUT /api/v3/System/data/synchronization/import.csv null
- PUT /api/v3/System/data/synchronization/run null
- GET /api/v3/System/data/synchronization null
- PUT /api/v3/System/data/synchronization null
- GET /api/v3/System/data/synchronization/status null
- PUT /api/v3/System/verification null
- PUT /api/v3/System/verification/loadimage null
- GET /api/v3/System/info null
- GET /api/v3/System/diagnostic/package null
- PUT /api/v3/System/diagnostic/package/create null
- GET /api/v3/System/diagnostic/package/download null
- GET /api/v3/System/diagnostic/statistics null
- PUT /api/v3/System/diagnostic/statistics null
- GET /api/v3/System/compatible null
- PUT /api/v3/System/compatible null
- GET /api/v3/System/compatible/versions null
- GET /api/v3/System/readers null
- PUT /api/v3/System/readers null
- GET /api/v3/System/presence null
- PUT /api/v3/System/presence null
- GET /api/v3/System/spaceusage null
- GET /api/v3/System/loglifetime null
- PUT /api/v3/System/loglifetime null
- GET /api/v3/System/ssh null
- PUT /api/v3/System/ssh null
- PUT /api/v3/System/rootPassword null

- GET /api/v3/System/datetime null
- PUT /api/v3/System/datetime null
- PUT /api/v3/System/datetime/timezone null
- GET /api/v3/System/network null
- PUT /api/v3/System/network null
- GET /api/v3/System/network/proxy null
- PUT /api/v3/System/network/proxy null
- GET /api/v3/System/securecardssetting null
- PUT /api/v3/System/securecardssetting null
- DELETE /api/v3/System/securecardssetting null
- GET /api/v3/TimeProfiles null
- POST /api/v3/TimeProfiles null
- PATCH /api/v3/TimeProfiles null
- GET /api/v3/TimeProfiles/{timeProfileId} null
- PUT /api/v3/TimeProfiles/{timeProfileId} null
- DELETE /api/v3/TimeProfiles/{timeProfileId} null
- PATCH /api/v3/TimeProfiles/{timeProfileId} null
- PUT /api/v3/Users/{userId}/sendcredentials null
- POST /api/v3/Users/{id}/pin null
- POST /api/v3/Users/{id}/qrcode null
- GET /api/v3/Users/{id}/qr.png null
- GET /api/v3/Users/{id}/qr.svg null
- GET /api/v3/visitors null
- POST /api/v3/visitors null
- PATCH /api/v3/visitors null
- GET /api/v3/visitors/{id} null
- PUT /api/v3/visitors/{id} null
- DELETE /api/v3/visitors/{id} null
- PATCH /api/v3/visitors/{id} null
- POST /api/v3/visitors/{id}/pin null
- POST /api/v3/visitors/{id}/qrcode null
- GET /api/v3/visitors/{id}/qr.png null
- GET /api/v3/visitors/{id}/qr.svg null
- PUT /api/v3/visitors/{id}/email null
- GET /api/v3/visitors/cards null
- POST /api/v3/visitors/cards null
- PATCH /api/v3/visitors/cards null
- GET /api/v3/visitors/cards/{id} null
- PUT /api/v3/visitors/cards/{id} null
- DELETE /api/v3/visitors/cards/{id} null
- PATCH /api/v3/visitors/cards/{id} null
- POST /api/v3/visitors/cards/find null
- PATCH /api/v3/Companies null
- PATCH /api/v3/Devices null

- PATCH /api/v3/Users null
- PATCH /api/v3/Zones null

What's Deprecated

- GET /api/v3/Users/{userId}/widgets null
- PUT /api/v3/Users/{userId}/widgets null
- PUT /api/v3/Users/{userId}/email null

What's Changed

GET /api/v3/Companies null

Return Type

Insert items.Type

POST /api/v3/Companies null

Parameters

Insert body.Type

Return Type

Insert Type

GET /api/v3/Companies/{companyId} null

Return Type

Insert Type

PUT /api/v3/Companies/{companyId} null

Parameters

Insert body.Type

Return Type

Insert Type

PATCH /api/v3/Companies/{companyId} null

Return Type

Insert Type

GET /api/v3/Companies/{companyId}/zones null

Return Type

Insert items.Type

GET /api/v3/Companies/{companyId}/devices null

Return Type

```

Insert Type
Insert State.BackupStatus
Insert State.RestoreStatus
Insert State.UploadStatus
Insert AccessControl.LiftFloors.Type
Delete State.BackupState
Delete State.RestoreState
Delete State.UploadState

```

GET /api/v3/Companies/{companyId}/visitorManagerGroups null

Return Type

```

Insert items.Users
Insert items.Type

```

GET /api/v3/Devices null

Return Type

```

Insert items.Type
Insert items.State.BackupStatus
Insert items.State.RestoreStatus
Insert items.State.UploadStatus
Insert items.AccessControl.LiftFloors.Type
Delete items.State.BackupState
Delete items.State.RestoreState
Delete items.State.UploadState

```

POST /api/v3/Devices null

Parameters

```

Insert body.Type
Insert body.AccessControl.LiftFloors.Type

```

Return Type

```

Insert Type
Insert State.BackupStatus
Insert State.RestoreStatus
Insert State.UploadStatus
Insert AccessControl.LiftFloors.Type
Delete State.BackupState
Delete State.RestoreState
Delete State.UploadState

```

GET /api/v3/Devices/{deviceId} null

Return Type

```

Insert Type
Insert State.BackupStatus
Insert State.RestoreStatus
Insert State.UploadStatus
Insert AccessControl.LiftFloors.Type
Delete State.BackupState
Delete State.RestoreState
Delete State.UploadState

```

PUT /api/v3/Devices/{deviceId} null

Parameters

Insert body.Type

Insert body.AccessControl.LiftFloors.Type

Return Type

Insert Type

Insert State.BackupStatus

Insert State.RestoreStatus

Insert State.UploadStatus

Insert AccessControl.LiftFloors.Type

Delete State.BackupState

Delete State.RestoreState

Delete State.UploadState

DELETE /api/v3/Devices/{deviceId} null

Parameters

Insert body.Type

Insert body.AccessControl.LiftFloors.Type

PATCH /api/v3/Devices/{deviceId} null

Return Type

Insert Type

Insert State.BackupStatus

Insert State.RestoreStatus

Insert State.UploadStatus

Insert AccessControl.LiftFloors.Type

Delete State.BackupState

Delete State.RestoreState

Delete State.UploadState

GET /api/v3/Devices/scannetwork null

Return Type

Insert items.Type

Insert items.State.BackupStatus

Insert items.State.RestoreStatus

Insert items.State.UploadStatus

Insert items.AccessControl.LiftFloors.Type

Delete items.State.BackupState

Delete items.State.RestoreState

Delete items.State.UploadState

DELETE /api/v3/Devices/{deviceId}/cleardirectory null

Parameters

Insert body.Type

Insert body.AccessControl.LiftFloors.Type

DELETE /api/v3/Devices/{deviceId}/factoryreset null

Parameters

Insert body.Type
 Insert body.AccessControl.LiftFloors.Type

GET /api/v3/Devices/{deviceId}/backup null

Return Type

Insert Type

PUT /api/v3/Devices/{deviceId}/replace null

Parameters

Insert body.LiftFloors.Type
 Insert body.LastBackup.Type
 Insert body.BackupState.path
 Insert body.BackupState.op
 Insert body.BackupState.from
 Insert body.RestoreState.path
 Insert body.RestoreState.op
 Insert body.RestoreState.from
 Insert body.UploadState.path
 Insert body.UploadState.op
 Insert body.UploadState.from
 Delete body.BackupState.When
 Delete body.BackupState.State
 Delete body.RestoreState.When
 Delete body.RestoreState.State
 Delete body.UploadState.When
 Delete body.UploadState.State

Return Type

Insert Type
 Insert State.BackupStatus
 Insert State.RestoreStatus
 Insert State.UploadStatus
 Insert AccessControl.LiftFloors.Type
 Delete State.BackupState
 Delete State.RestoreState
 Delete State.UploadState

GET /api/v3/Devices/{deviceId}/floors null

Return Type

Insert Type

PUT /api/v3/Devices/{deviceId}/floors/{floorId} null

Parameters

Insert body.Type

Return Type

Insert Type

PUT /api/v3/login null

Return Type

Insert Type

PUT /api/v3/passwordresetverification null

Return Type

Insert Token

Delete data

PUT /api/v3/setnewpassword null

Return Type

Insert Id

Insert Name

Insert Login

Insert Email

Insert AvatarUrl

Insert ModifiedGuid

Insert Localization

Insert ShowWizard

Insert ShowGiveFeedback

Insert AttendanceMonitored

Insert IsSysAdmin

Insert Right

Insert Company

Delete data

GET /api/v3/Users null

Return Type

Insert items.Type

POST /api/v3/Users null

Parameters

Insert body.Type

Return Type

Insert Type

DELETE /api/v3/Users null

Parameters

Insert body.Type

GET /api/v3/Users/{id} null

Return Type

Insert Type

PUT /api/v3/Users/{userId} null

Parameters

Insert body.Type

Return Type

Insert Type

PATCH /api/v3/Users/{userId} null

Return Type

Insert Type

PUT /api/v3/Users/{userId}/password null

Return Type

Insert Type

GET /api/v3/Users/{userId}/mobilekey null

Return Type

Delete Settings.ModifiedGuid

DELETE /api/v3/Users/{userId}/mobilekey/{authId} null

Return Type

Delete Settings.ModifiedGuid

PUT /api/v3/Users/{userId}/mobilekey/pairing/start null

Return Type

Delete Settings.ModifiedGuid

PUT /api/v3/Users/{userId}/mobilekey/pairing/stop null

Return Type

Delete Settings.ModifiedGuid

PUT /api/v3/Users/{userId}/mobilekey/pairing/dongle null

Return Type

Delete Settings.ModifiedGuid

GET /api/v3/Zones null

Return Type

Insert items.Type

POST /api/v3/Zones null

Parameters

Insert body.Type

Return Type

Insert Type

GET /api/v3/Zones/{zoneId} null

Return Type

Insert Type

PUT /api/v3/Zones/{zoneId} null

Parameters

Insert body.Type

Return Type

Insert Type

PATCH /api/v3/Zones/{zoneId} null

Return Type

Insert Type

7. Supplementary Information

Here is what you can find in this section:

- [7.1 Third Party License](#)

7.1 Third Party License



Refer to About application in the pop-up menu on the right-hand side of the upper toolbar in the 2N® Access Commander web interface for a complete list of the third party library licenses used.

