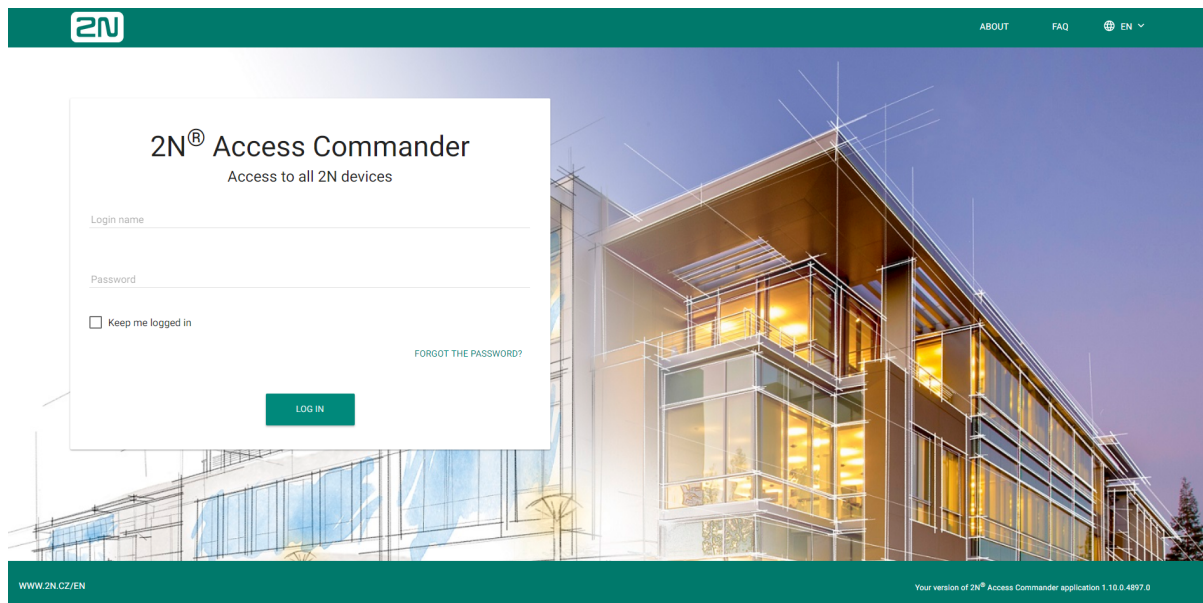


2N[®] Access Commander





- [1. Product Overview](#)
- [2. Linux Settings](#)
- [3. System Setup](#)
- [4. System Administration](#)
- [5. Extensions](#)
- [6. HTTP API](#)

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](#)

1.1 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.

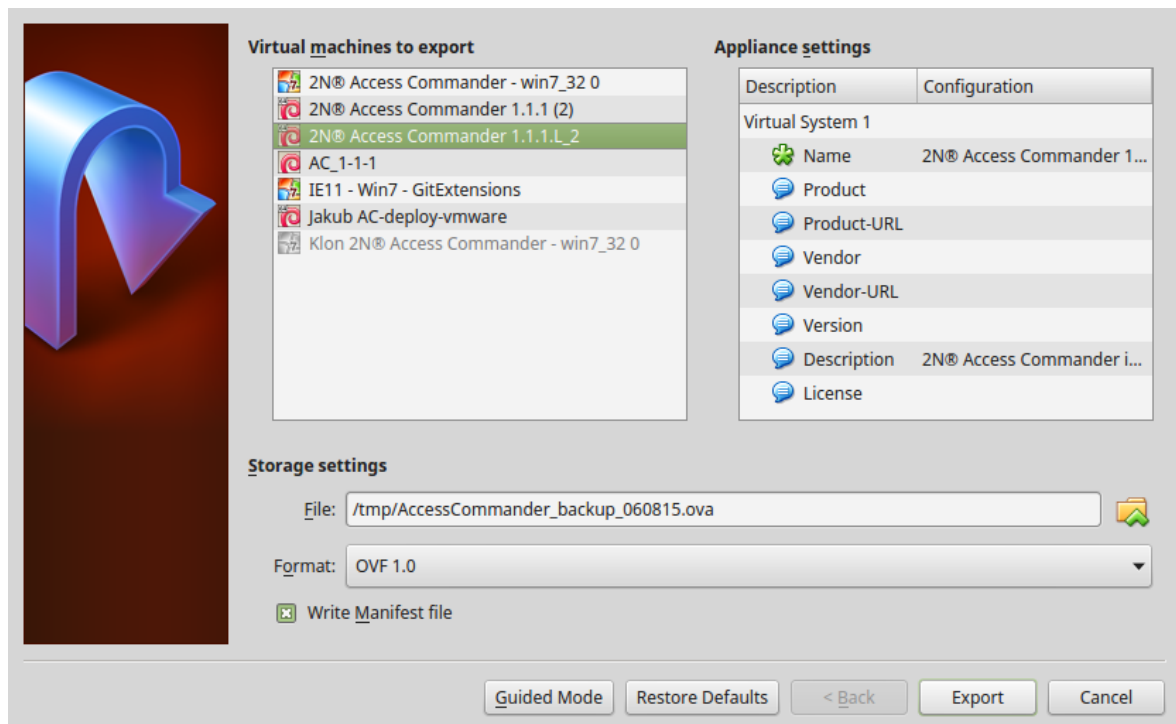
VirtualBox:

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...

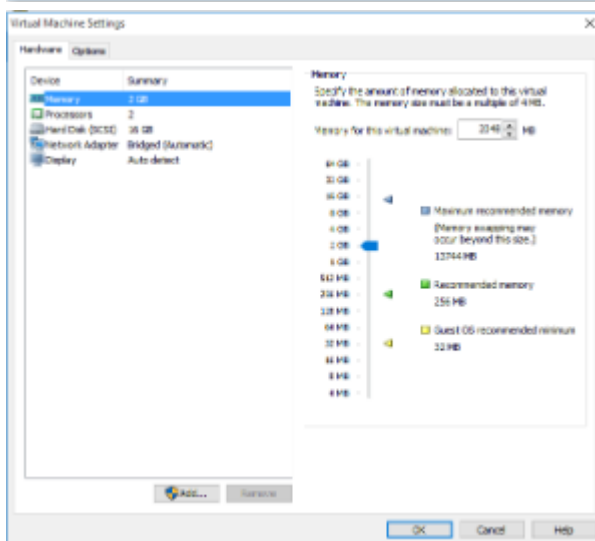
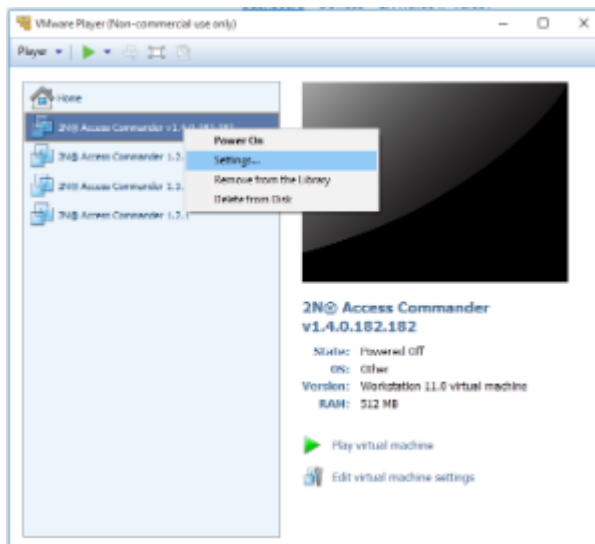


- a. edit the name,
 - b. check the CPU settings (2 at least),
 - c. check the RAM settings (2048 MB at least),
 - d. check the network card selection.
4. Confirm the License terms.

1.1.2 VMware

VMware Player

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



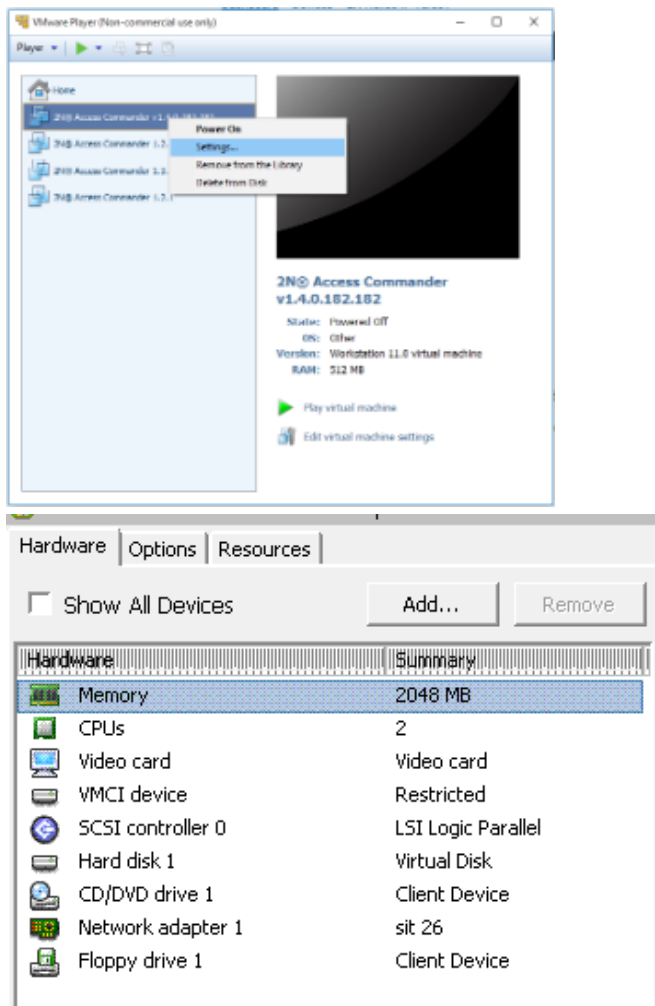
5. Check the settings:
 - a. check the RAM settings (2048 MB at least),
 - b. check the CPU settings (2 at least),
 - c. check the network card selection.

VMware vSphere

Warning

- Created in VMware vSphere - VMware ESXi 5.1.0. Not tested for other versions.

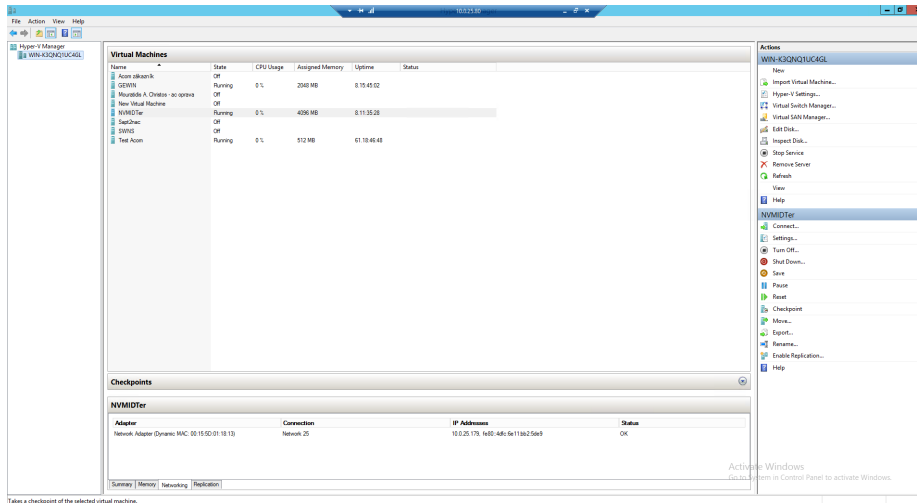
- Download the image from the [official 2N web site](#).
- In VMware vSphere select File – Deploy OVF Template... and follow the wizard instructions.
- After the import, check the Edit Settings...:



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

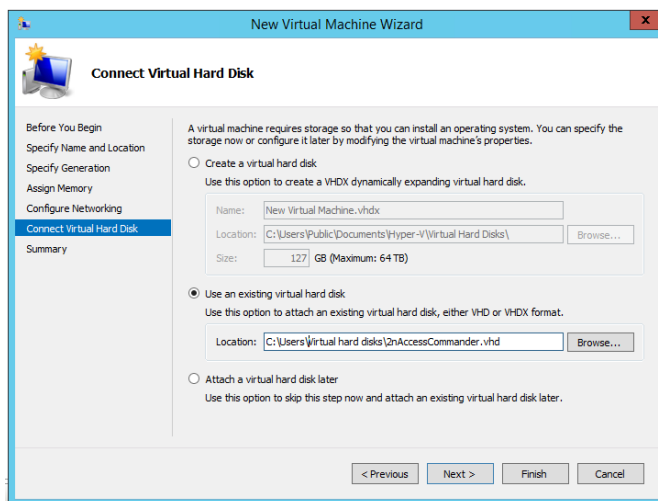
1.1.3 Hyper-V

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](#)



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

The count of connected devices affects **2N® Access Commander** in variable ways. Therefore, set the size of hardware elements for the server accordingly. The table below includes the recommended CPU kernel counts and RAM sizes for different counts of devices connected to **2N® Access Commander**.

Count of connected devices	Count of CPU kernels	Assigned RAM size
50	2	2 GB
100	4	4 GB
200	8	8 GB
500	16	16 GB

1.2 BOX Distribution



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 Box

Package Contents

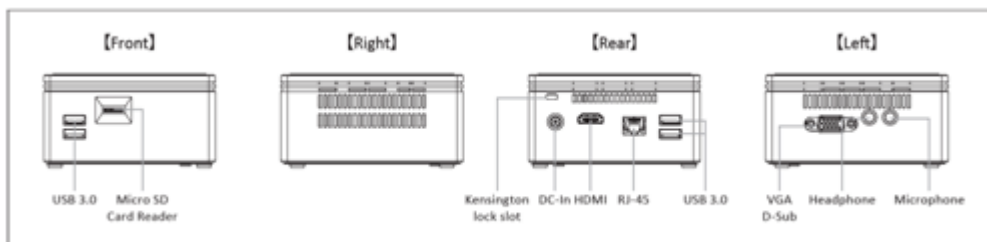
- 1 Gigabyte BRIX BACE with:

- **2N® Access Commander**
- 2.5” 32 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 (32 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.

 **Note**




- You are entitled to a free 5-device licence when you purchase **2N® Access Commander Box**.
- All the setting procedures are applicable for the virtual machine and box version.

1.3 Supported Browsers

Optimised for the following browser:

-  Google Chrome (version 40 and higher)

Other supported browsers:

-  Mozilla Firefox (version 35 and higher)
-  Internet Explorer (version 11 and higher)
-  Microsoft Edge (version 38.14393 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

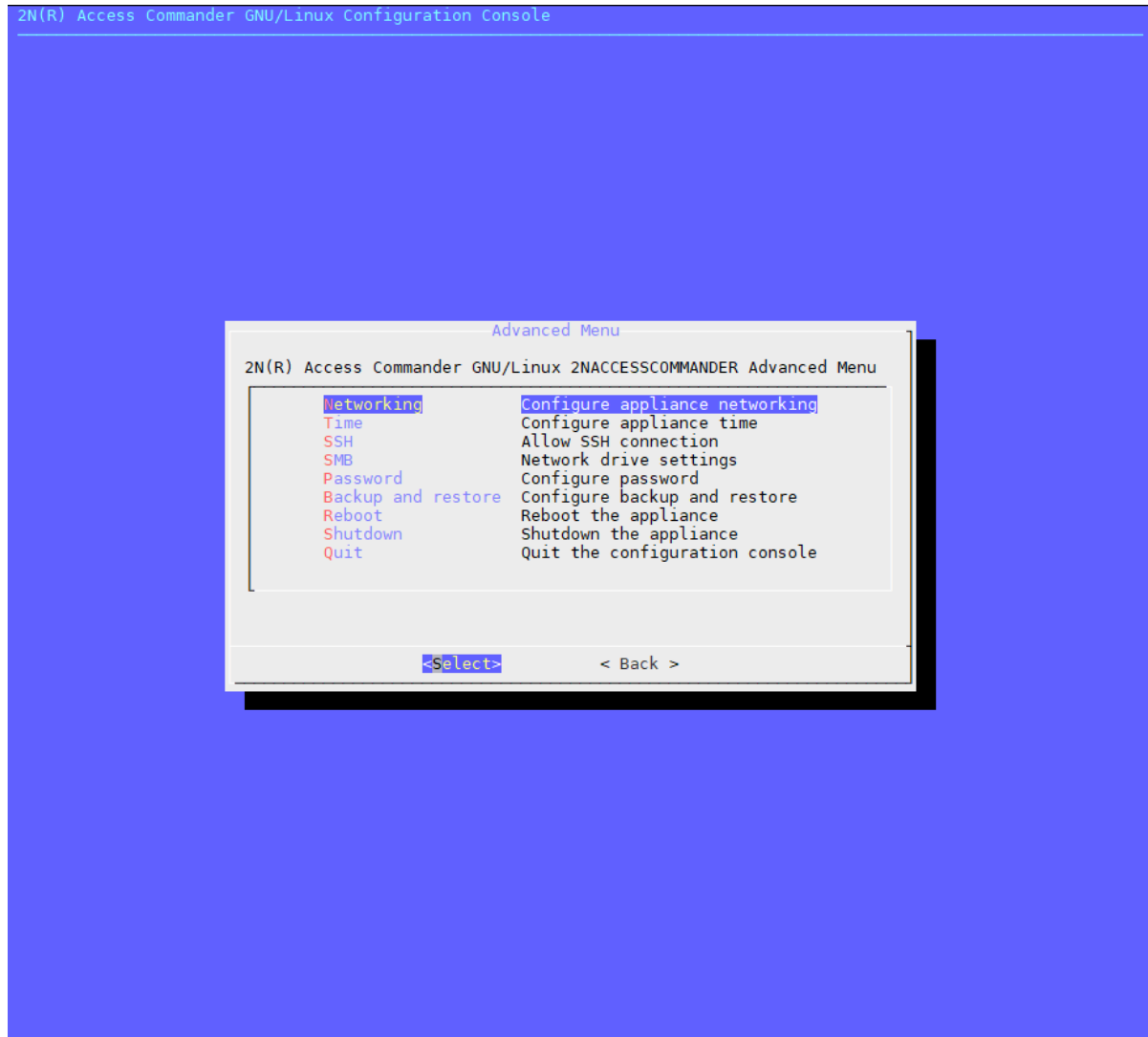
Service	Port
HTTP/HTTPS*	80/443
SMTP	225
DHCP	68
DNS	53
NTP	123
LDAP**	389
SSH	22

* 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.

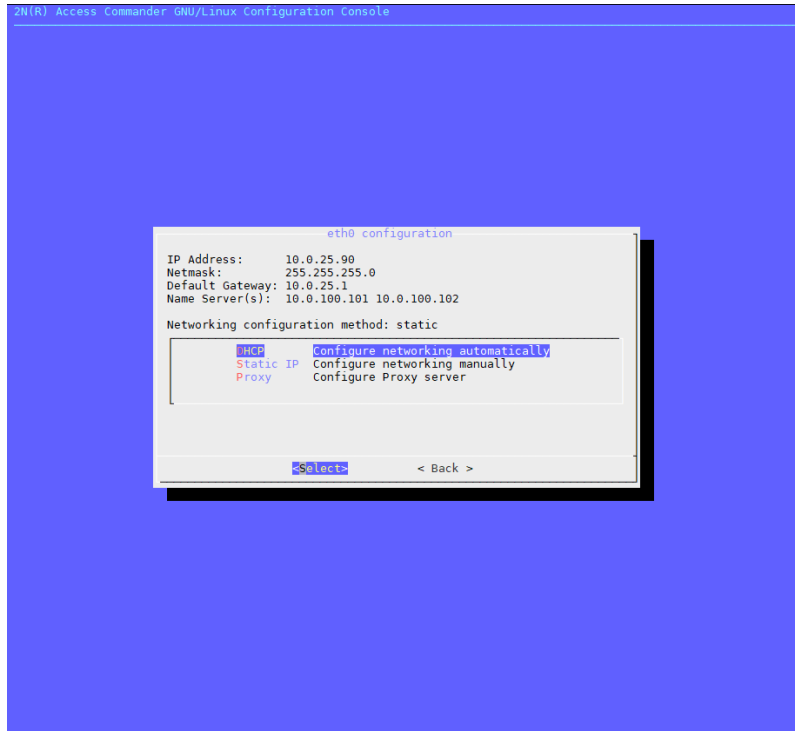
2. Linux Settings

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

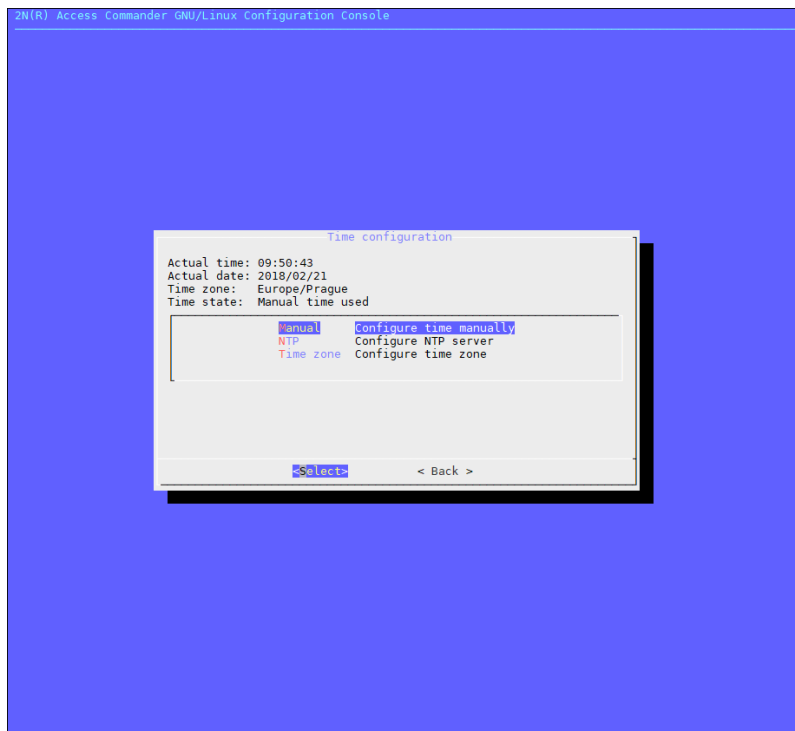


Set the basic Linux parameters:

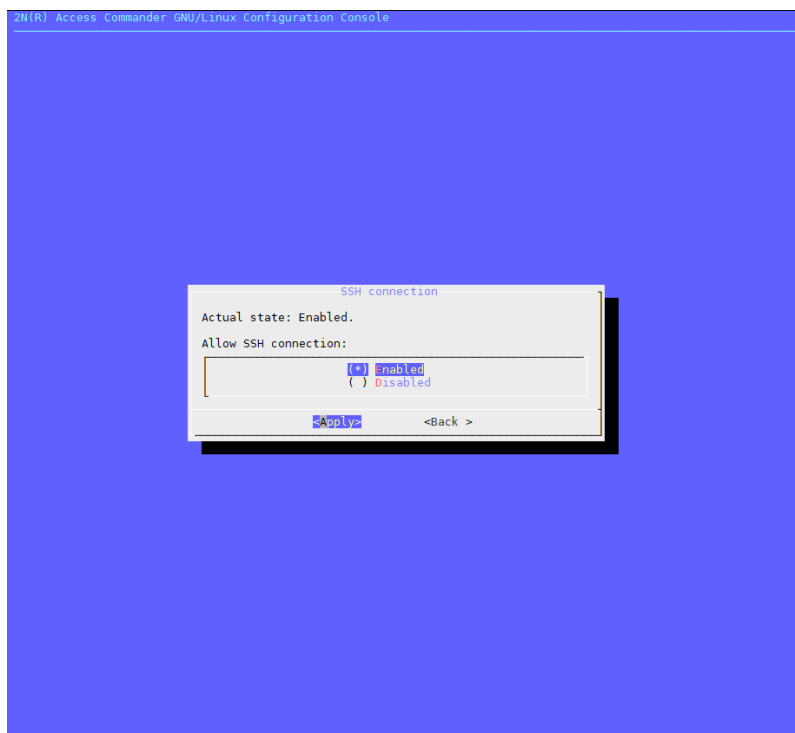
Networking – set the Proxy server and network parameters. Set the network parameters manually or via the **2N® Access Commander** DHCP server.



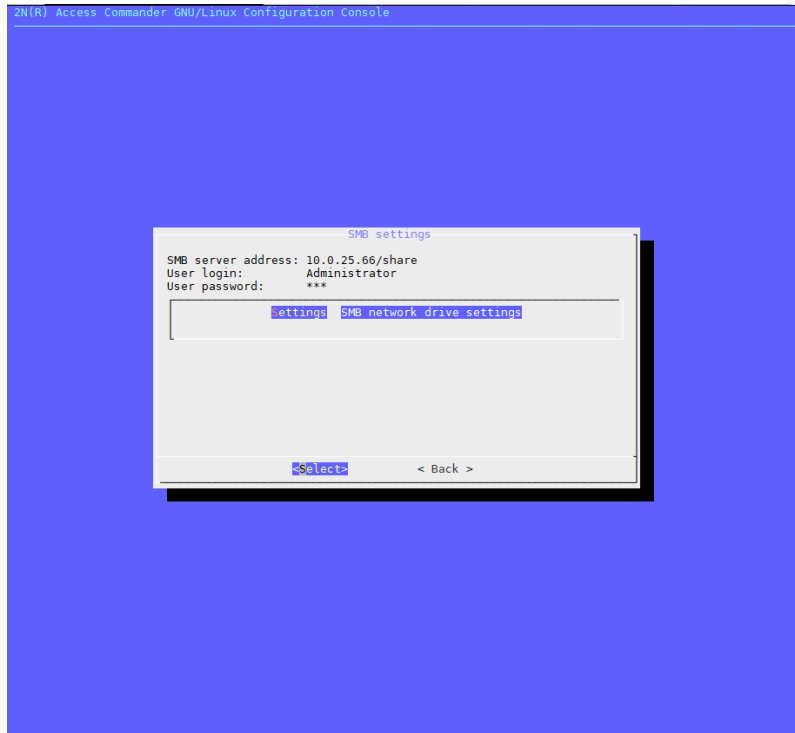
- **Time** – set the time, NTP server and time zone for **2N® Access Commander**. Ideally, the time zone should match the value set for the **2N® IP intercoms**.



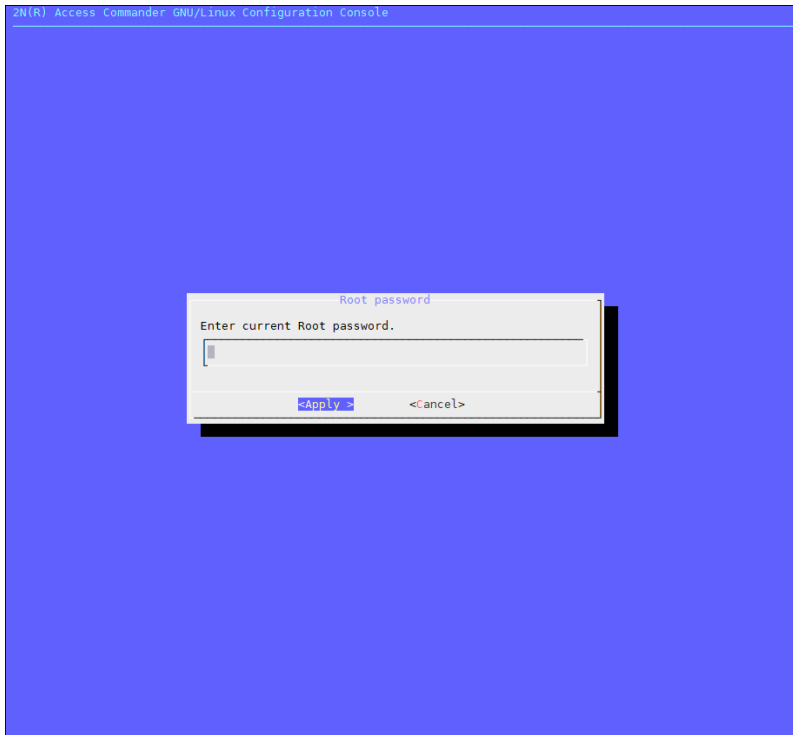
- **SSH** – set the SSH connection to the 2N® Access Commander server. Make sure that a password is set for SSH that is different from the default one and meets the SSH requirements.



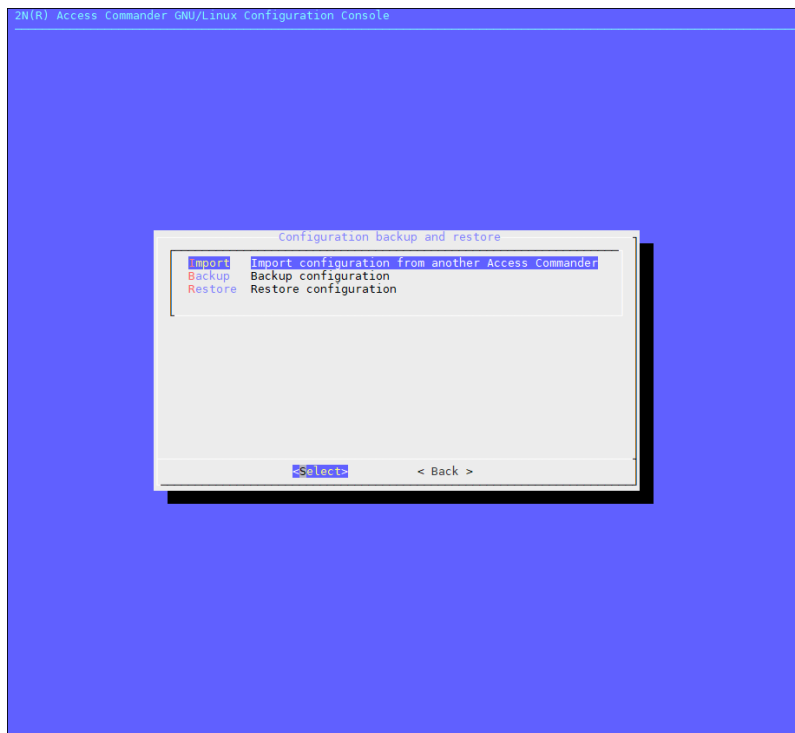
- **SMB** – enable the shared folder connection wizard. Set the IP address/domain name and folder path. E.g.: 192.168.1.1/share. Set the user name for folder access and right to write. Type the user password. Once all the mandatory parameters are set, the server connection is verified and the successful/wrong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



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



- **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
 - **Restore** – restore configuration from backup



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

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

3. System Setup

Settings

LICENCES SMTP ATTENDANCE MODULE MODE USB DEVICE BLUETOOTH SYNCHRONISATION DATA ARCHIVES

Active licences
 Licence device S/N: 54-1105-0190
 Count of available Attendance Monitoring licences: 95 (of the total count 100)
 Count of available device licences: 43 (of the total count 50)
 LDAP synchronisation: Yes
 CSV synchronisation: Yes
 Licence adding date: 03/29/2018 14:46:23

[ADD LICENCE](#) [INFO](#)

SYSTEM UPDATE SYSTEM BACKUP DIAGNOSTICS DEVICE COMPATIBILITY

CURRENT SYSTEM VERSION

1.11.0.4894.0

URL for upgrade
<http://10.0.26.31/upgrade/HIPSU-3231/LTE-Verso-support-in-AC-analysis/feat/>

STATUS

✓ This is the current system version. No later versions are available.

[CHECK FOR UPDATE](#)

- [3.1 Licenses](#)
- [3.2 SMTP](#)
- [3.3 Attendance Module Mode](#)
- [3.4 USB Devices](#)
- [3.5 Bluetooth](#)
- [3.6 CSV Synchronisation](#)
- [3.7 Data Archives](#)
- [3.8 System Update](#)
- [3.9 System Backup](#)
- [3.10 Diagnostics](#)
- [3.11 Device Compatibility](#)

3.1 Licenses

Refer to the **License** tile on the administrator's **Dashboard** for the current count of licensed devices and Attendance users. Upon the initial installation of the **2N® Access Commander**, a Trial license (see below for details) will be available for you to configure one device and monitor Attendance of one user free of charge. Order extending licenses to manage a higher count of devices or monitor more users than one. The following license types can be ordered:

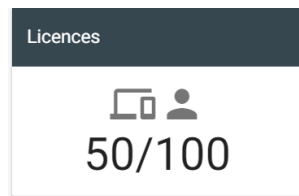
91379040	2N® Access Commander – license for +5 devices (5-device license package)*
-----------------	--

91379041	2N® Access Commander – license for +25 users (25-user license package)** – for employees' Attendance monitoring only
91379042	2N® Access Commander – Integration License (LDAP + CSV synchronisation package)

Info

* If you need a license for 17 devices, e.g., then order 4 licenses No. 91379040 (to connect up to 20 devices in total to the system).

** If you need a license for 69 users, e.g., then order 3 licenses No. 91379041 (to monitor arrivals/departures of up to 75 users in total).



Click on the icon to pass to the **Setting – License** menu, where you can find the following sections:

Active licenses

The section displays the count of required and owned device and user Attendance management licenses (in the required / owned format). Including the last license adding date. Every license addition rewrites the original one. Licenses are not added up.

Settings

[LICENCES](#)
 [SMTP](#)
 [ATTENDANCE MODULE MODE](#)
 [USB DEVICE](#)
 [BLUETOOTH](#)
 [SYNCHRONISATION](#)
 [DATA ARCHIVES](#)

Active licences
 Licence device S/N: 54-1105-0190
 Count of available Attendance Monitoring licences: 95 (of the total count 100)
 Count of available device licences: 43 (of the total count 50)
 LDAP synchronisation: Yes
 CSV synchronisation: Yes
 Licence adding date: 03/29/2018 14:46:23

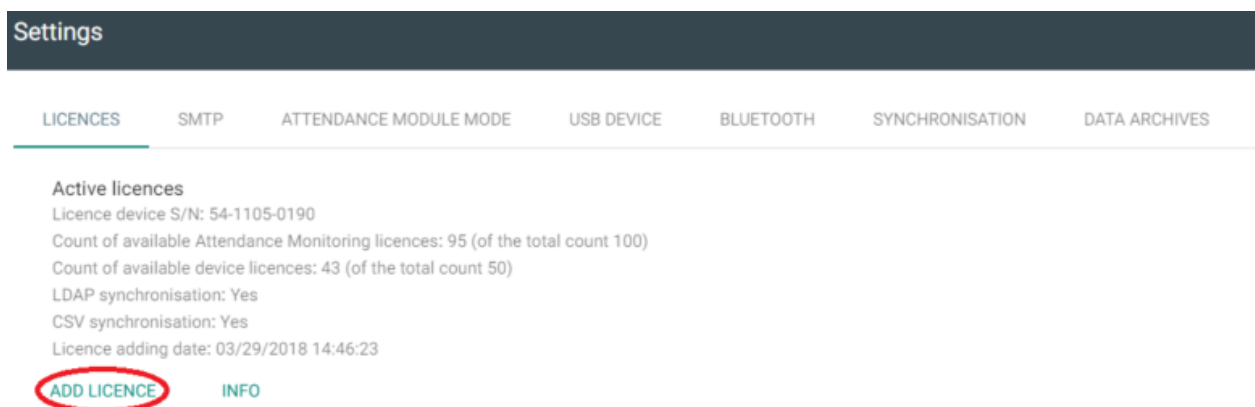
[ADD LICENCE](#)
 [INFO](#)

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. When the protective period expires, all the devices will become inactive and a new license will have to be generated.

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
- 1 Attendance user
- unlimited count of system users

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.

Active licences

Licence device S/N: 54-1105-0190

Count of available Attendance Monitoring licences: 95 (of the total count 100)

Count of available device licences: 43 (of the total count 50)

LDAP synchronisation: Yes

CSV synchronisation: Yes

Licence adding date: 03/29/2018 14:46:23

[ADD LICENCE](#)

[INFO](#)

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 SMTP

The SMTP helps **2N® Access Commander** send e-mail messages. The module also provides [notifications](#) and sends the login password to the user. The SMTP server is set by default via which e-mail messages can be sent. You are recommended to reset the default server to your own one.

Settings

- LICENCES
- SMTP**
- ATTENDANCE MODULE MODE
- USB DEVICE
- BLUETOOTH
- SYNCHRONISATION
- DATA ARCHIVES

Make sure that SMTP is enabled and configured to use system e-mail notifications (user creation confirmation, e.g.).

SMTP SETTINGS

SMTP on

Server Address
smtp.2nac.cz

Port
25

User name
noreply@2nac.cz

Default sender address
noreply@2nac.cz

SSL off

[SEND TEST E-MAIL](#)

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

SMTP settings
×

SMTP on

Server Address *
smtp.2nac.cz

Port *
25

User name *
noreply@2nac.cz

Password *
.....

Default sender address *
noreply@2nac.cz

SSL off

SET DEFAULT VALUE
CANCEL
CHANGE

- **SMTP enable/disable** – enable/disable the e-mail sending service.
- **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.
- **Username** – 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** – set the sender address for all outgoing e-mails from **2N® Access Commander**.
- **SSL enable/disable** – enable/disable e-mail encryption.
- **Reset default value** – reset the default value.

3.3 Attendance Module Mode

2N® Access Commander treats Attendance in two modes:

1. **Režim FREE** – arrivals and departures in the FREE mode are recorded according to the first and the last card swipes through any 2N reader within the company. The Presence module is disabled in this mode.



2. **Režim IN-OUT** – arrivals and departures are recorded in the IN-OUT mode whenever an arrival or departure reader is used (set directly on the device). This mode is essential for correct functioning of the Presence module.



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.

Settings


LICENCES SMTP ATTENDANCE MODULE MODE **USB DEVICE** BLUETOOTH SYNCHRONISATION DATA ARCHIVES

Select USB device for user login data loading


125kHz RFID card reader




13.56MHz and 125kHz RFID card reader



External fingerprint reader



External Bluetooth reader



- **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

Bluetooth settings help you specify the pairing devices, set the pairing timeout and enable/disable an external card reader.

Settings

LICENCES SMTP ATTENDANCE MODULE MODE USB DEVICE **BLUETOOTH** SYNCHRONISATION DATA ARCHIVES


2N DEVICE FOR INITIAL PAIRING WITH SMARTPHONE

My Company

PAIRING TIME

Pairing time
1 hour

PRIMARY PAIRING DEVICE – USB READER

 External Bluetooth reader (USB interface)

[SETTING INSTRUCTIONS](#)

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. Click Set Bluetooth to display an administrator window to set the pairing device and pairing timeout.

Bluetooth settings ✕

2N device for initial pairing with smartphone

Caution: You cannot pair your phone via a device to which you are assigned no access rules.

My Company ▾

Pairing time

10 minutes

30 minutes

1 hour

2 hours

6 hours

12 hours

CANCEL PASSED

Make sure that the device is set for every company. If a device is assigned to a zone that is assigned to multiple companies, you can set one device for multiple companies. The pairing timeout is valid until you click Generate on the user and the PIN is displayed. You can enable USB dongle for pairing in this window. Click OK to set all the parameters. You will be redirected to the user list to choose a user. Refer to [4.2.1 Bluetooth](#).

3.6 CSV Synchronisation

Synchronisation via a CSV file.

Settings

LICENCES
SMTP
ATTENDANCE MODULE MODE
USB DEVICE
BLUETOOTH
SYNCHRONISATION
DATA ARCHIVES

SYNCHRONISATION	INFO
FTP storage Empty	Last synchronisation
Automatic synchronisation	Next synchronisation at (server time)
<div style="display: flex; gap: 10px;"> <div style="border: 1px solid #ccc; background-color: #eee; padding: 2px 5px; font-size: x-small;">SYNCHRONISE FROM STORAGE</div> <div style="color: #007060; font-size: x-small;">SYNCHRONISE FROM FILE</div> </div>	Current synchronisation status <div style="display: flex; align-items: center; gap: 5px;"> i Synchronisation results are stored in the system log. </div> <div style="text-align: right; color: #007060; font-size: x-small;"> SHOW SYSTEM LOGS </div>

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

FTP storage settings
×

FTP server address
ftp://10.0.25.65/import.csv

User Name
111

Password
...


CANCEL CHANGE

- i. **FTP server address** – set an IP address/domain name as the FTP server address. The address must include the ftp:// prefix and filename for synchronisation.
 - ii. **Username** – specify the FTP server user with access to the required file.
 - iii. **Password** – set the user password.
- 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 Number,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**.
- **User Mail** – set the user mail.
- **Card Number** – enter the user card ID.
- **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.
- **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.

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 12:15:13	Info: License authentication succeeded. Device used for licensing: 2N Access Unit (S/N: 54-1105-0190, IP: 10.0.25.136)
11.04.2018 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).

Note

- CSV synchronisation a licensed function. The tab is hidden unless the **91379042 2N® Access Commander – Integration License** is added.

3.7 Data Archives

Data archives are used for setting the size of the storage to be used for camera logs. When the storage is filled to capacity, 20% of the oldest logs are deleted. Set the storage capacity to 1, 3 or 5 GB.

Camera log storage setting



Storage capacity:

- 1 GB
 3 GB
 5 GB

When the storage capacities decreases, the oldest camera logs can be deleted.

CANCEL

CHANGE

When you set a lower capacity, mind that the oldest logs may be deleted if the capacity is exceeded.

3.8 System Update

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

SYSTEM UPDATE
SYSTEM BACKUP
DIAGNOSTICS
DEVICE COMPATIBILITY

CURRENT SYSTEM VERSION

1.11.0.4894.0

URL for upgrade
[http://10.0.26.31/upgrade/HIPSU-3231/LTE-Verso-support-in-AC-analysis\(feat\)/](http://10.0.26.31/upgrade/HIPSU-3231/LTE-Verso-support-in-AC-analysis(feat)/)

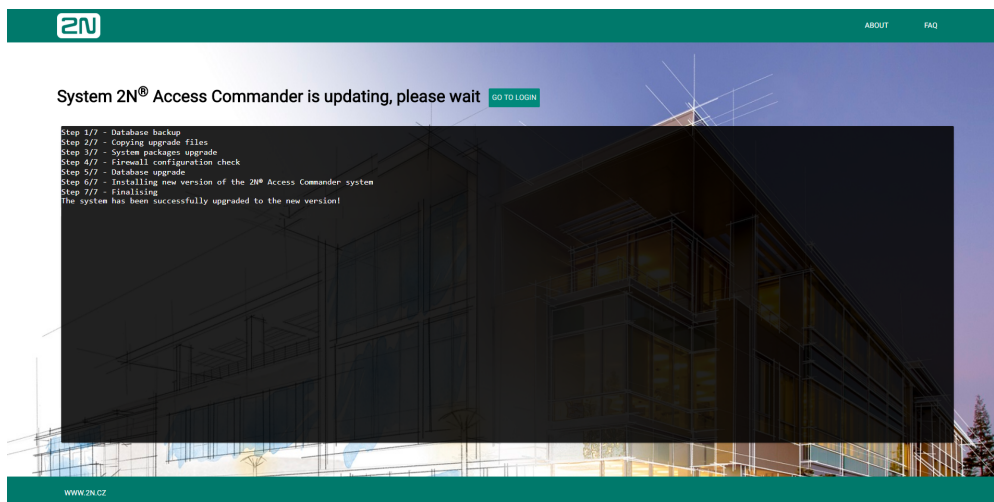
STATUS

✓ This is the current system version. No later versions are available.

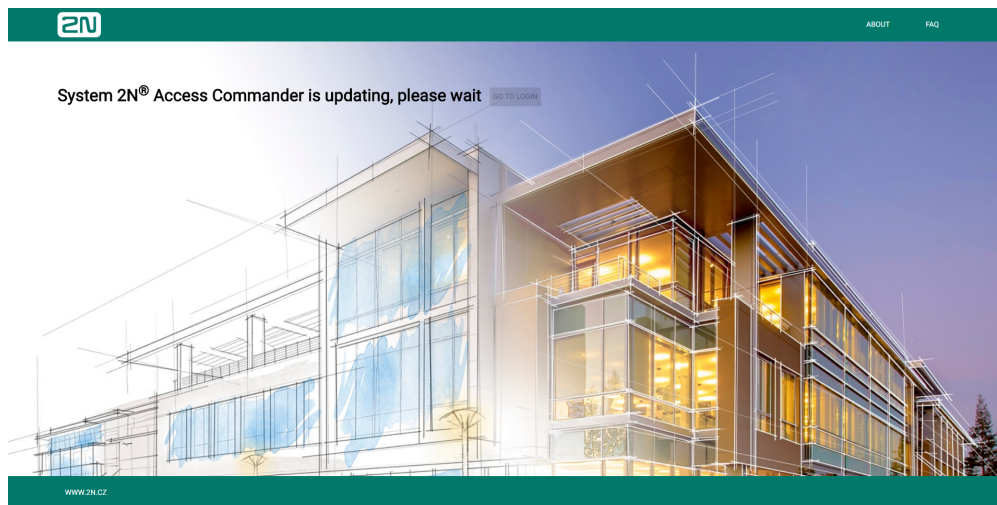
[CHECK FOR UPDATE](#)

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

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.

3.9 System Backup

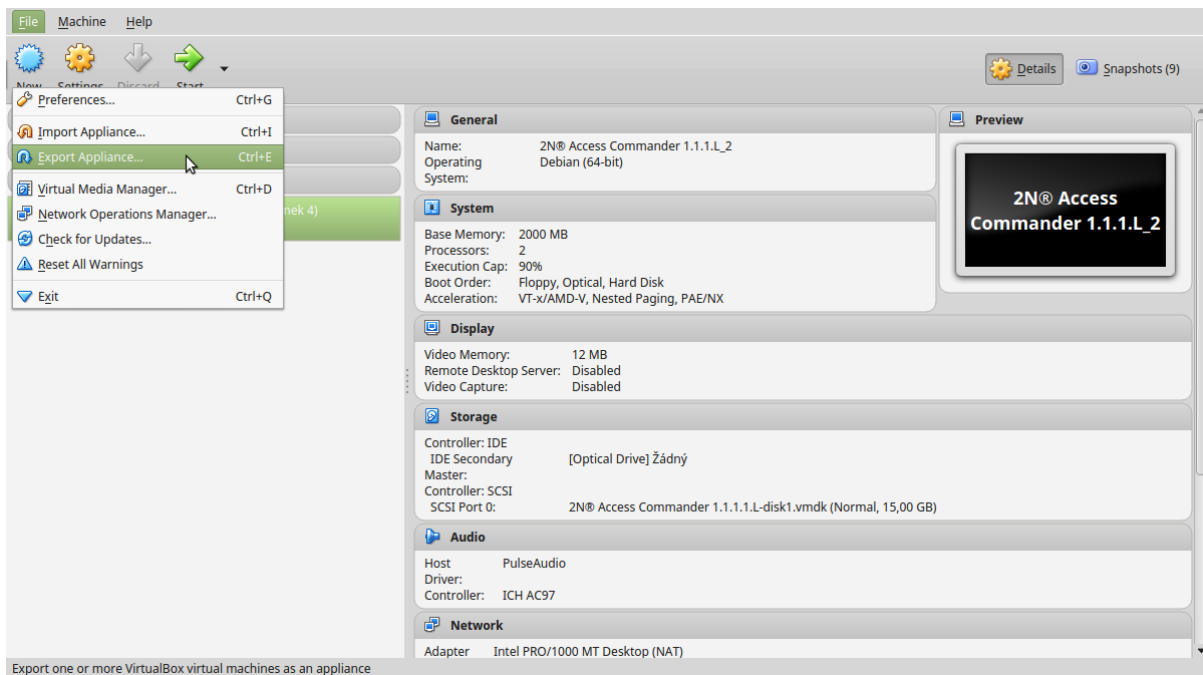
2N® Access Commander offers the following ways of system backup.

1. Virtual machine backup
2. Import from another **2N® Access Commander**
3. Backup and restore

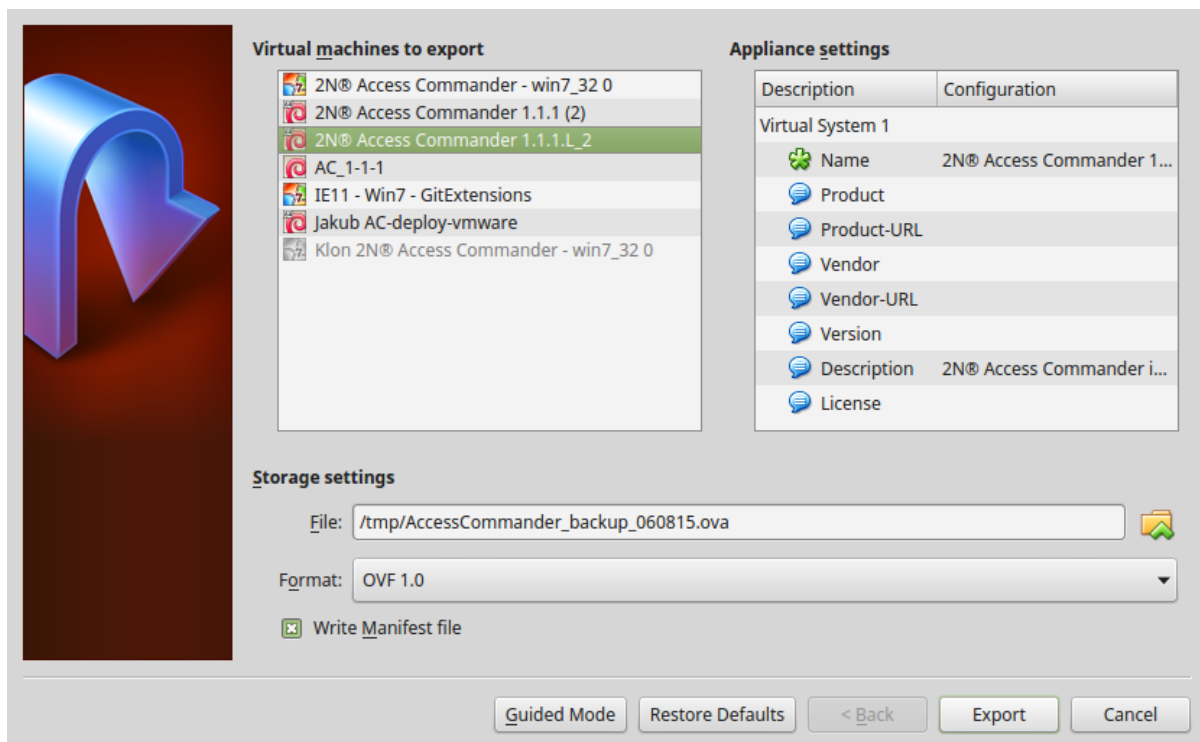
Virtual Machine Backup

VirtualBox

- Make sure that the virtual machine is off.
- Select Export appliance... in the File menu.



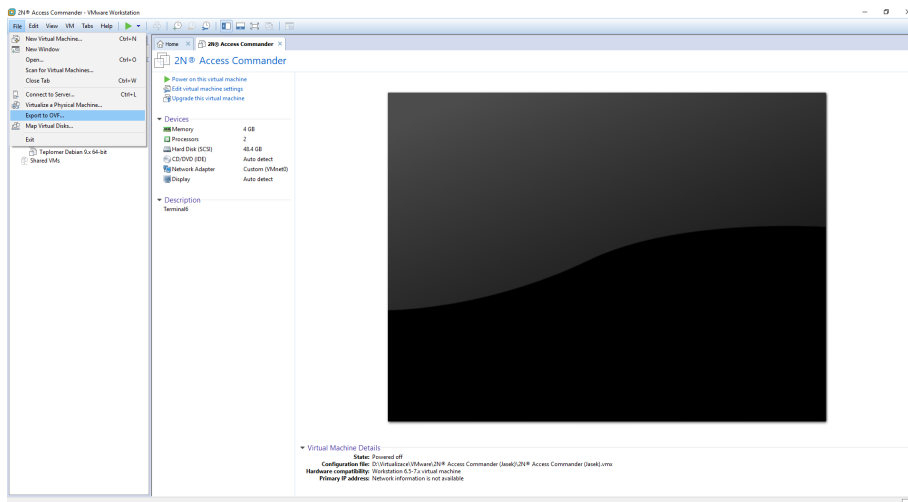
- Select the virtual machine and set the export path. Click Export.



You can transfer and import the exported file arbitrarily (refer to [Virtual Box installation](#)) using any machine (see Minimum requirements in [1.1.4 Recommended HW](#)) to the VirtualBox application. Or, you can import the exported file to other virtualisation tools after reconverting the file for the selected application.

VMware Workstation

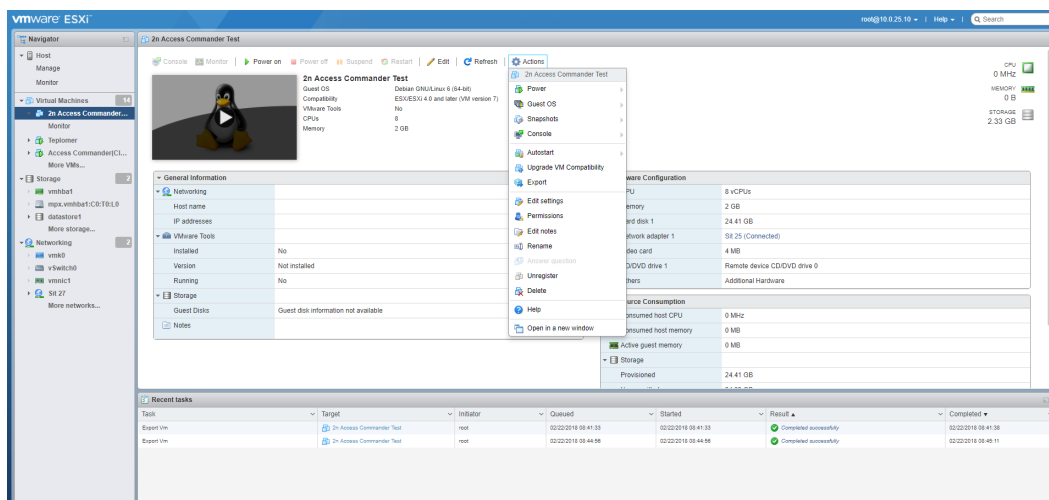
- Make sure that the virtual machine is off.
- Select Export to OVF in the File menu.



- A window is displayed for you to choose where to save the exported machine. Also, you can save the virtual machine to two files (OVF + VMDK) or one OVA file. All you have to do to save the machine into an OVA file is overwrite the filename extension. By overwriting ovf to ova you save the virtual machine into one file.

VMware ESXi 6.5

- Make sure that the virtual machine is off.
- Click Actions and select Export in the detail of the machine to be exported.

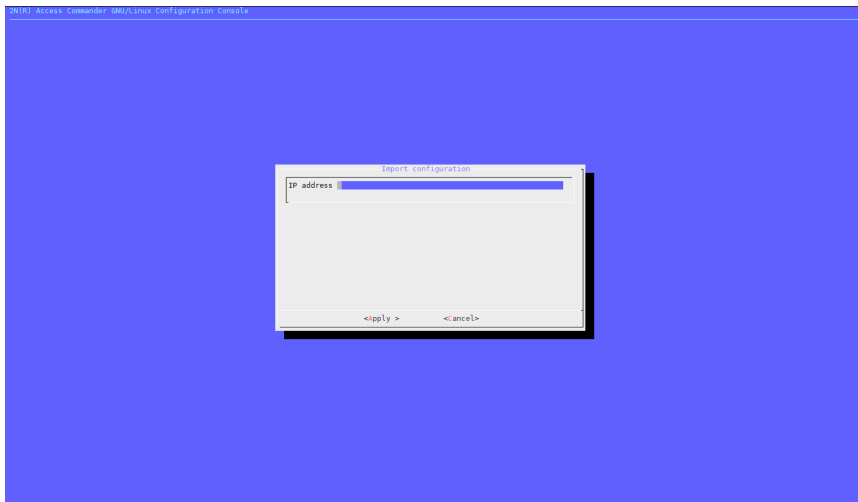


- Having clicked Export, you are informed that two files (OVF and VMDK) are being downloaded.

Import from Another 2N® Access Commander Installation

Used for data transfer between two 2N® Access Commander servers. Open the Linux configuration console to transfer data from another server.

1. Select Backup and restore.
2. Select Import in the new menu.



3. Now you are invited to enter the 2N® AccessCommander IP address from which configuration is to be downloaded.
4. Enter the IP address and the SSH access password. I.e. the source machine root password.

```

root@10.0.25.141's password:
Copying HIPDB data
98.2KiB 0:00:02 [40.7KiB/s] [ <=>
Copying IMGDB data
1.58KiB 0:00:00 [ 2KiB/s] [ <=>

```

5. If the import has been successful, Apache2 will be disabled on the source machine and the source machine will be turned off.



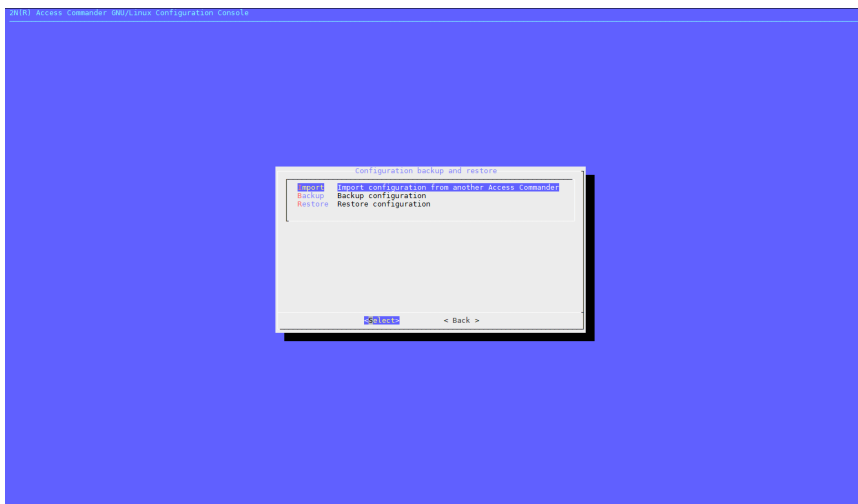
- To import data from another **2N® Access Commander installation**, make sure that SSH is enabled on the data transferring server.



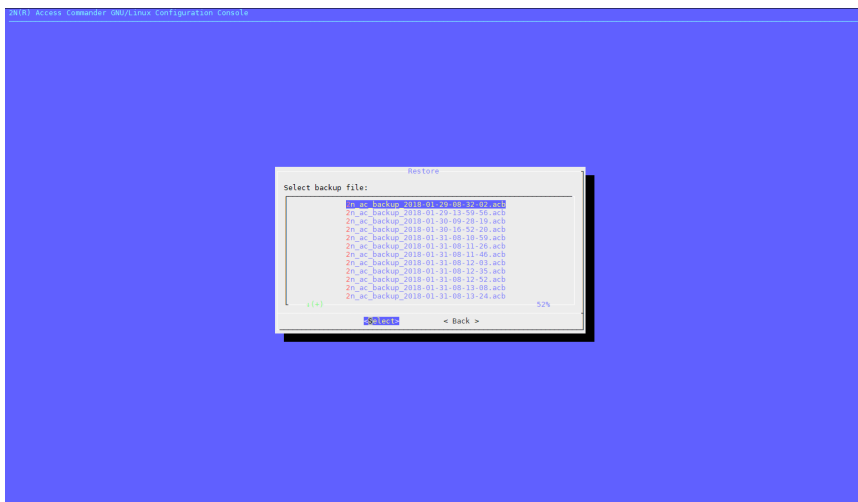
- Data can only be imported from an older or identical **2N® Access Commander** version. Data cannot be imported from a new version to an earlier one.

Backup and Restore

Used for backing up and restoring data in **2N® Access Commander**. Data is stored on a samba server. For setting details refer to [2. Linux Settings](#).



Click Backup to enter the password for encryption. The backup process may take a few seconds or a few minutes depending on the installation to be backed up.



Click Restore and select the backup to be used. System restore name includes the backup date and time. To select a backup enter the password used for its encryption. After restoring you will be redirected back to the Configuration backup and restore menu.



- Data encryption helps prevent data misuse by unauthorised persons.

3.10 Diagnostics

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

SYSTEM UPDATE SYSTEM BACKUP **DIAGNOSTICS** DEVICE COMPATIBILITY

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

- **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.

3.11 Device Compatibility

These settings inform the administrator that a device with unsupported firmware is connected. Once detected, any incompatible device is deactivated and the administrator is informed by means of an e-mail message and notification. Enable this firmware version in the system configuration to activate the device.

SYSTEM UPDATE SYSTEM BACKUP DIAGNOSTICS **DEVICE COMPATIBILITY**

All the devices work with the correct firmware version. ✓

[INFO](#)

When an incompatible device is added or upgraded, the device becomes inactive. A new record is created in the table and the administrator can enable the use of incompatible firmware in the **2N® Access Commander** environment. Once enabled, the device can be activated and used as a standard device. Or, the administrator can disable the firmware and all the devices become inactive.



- Incompatible firmware means that correct functioning of all the features cannot be guaranteed and thus the product cannot be recommended by the manufacturer.

The user is notified of incompatible firmware in the device list too.

Device						SEARCH	STATE
	Name ↑	State	IP address	Serial Number	Firmware Version		
<input type="checkbox"/>	2N Access Unit	Online	10.0.25.136	54-1105-0190	2.23.0.32.3		
<input type="checkbox"/>	2N Access Unit + TouchKeyboard	Online	10.0.25.159	54-1168-0217	2.23.0.32.6		
<input type="checkbox"/>	2N Helios IP Base	Online	10.0.25.151	54-1685-0483	2.23.0.32.5		
<input type="checkbox"/>	2N Helios IP Force	Online	10.0.25.146	54-0473-0646	2.23.0.32.5		
<input type="checkbox"/>	2N Helios IP Vario	Online	10.0.25.183	54-0889-0018	2.23.0.32.4		
<input type="checkbox"/>	2N Helios IP Verso Ondra	Online	10.0.25.133	54-0917-0075	2.23.0.32.5		
<input type="checkbox"/>	2N LTE Verso	Online	89.24.76.81	54-1763-0989	2.23.0.32.5		

Page: 1 Rows per page: 15 1 - 7 of 7

- The devices marked with this symbol are approved as incompatible for system use.
- The devices marked with this symbol are disapproved for system use.

4. System Administration

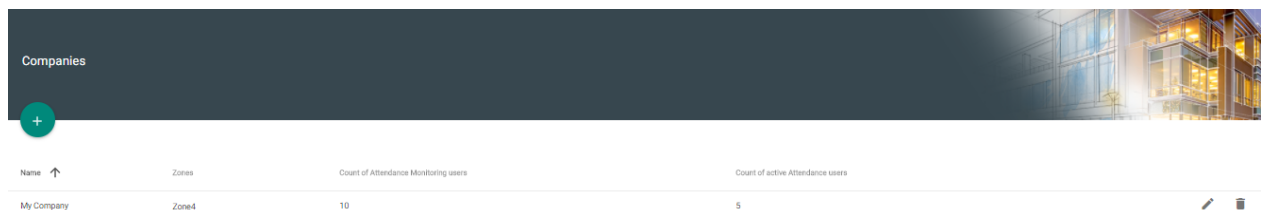
- [4.1 Companies](#)
- [4.2 Users](#)
- [4.3 Groups](#)
- [4.4 Devices](#)
- [4.5 Zones](#)
- [4.6 Time Profiles](#)
- [4.7 Access Rules](#)

4.1 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.).

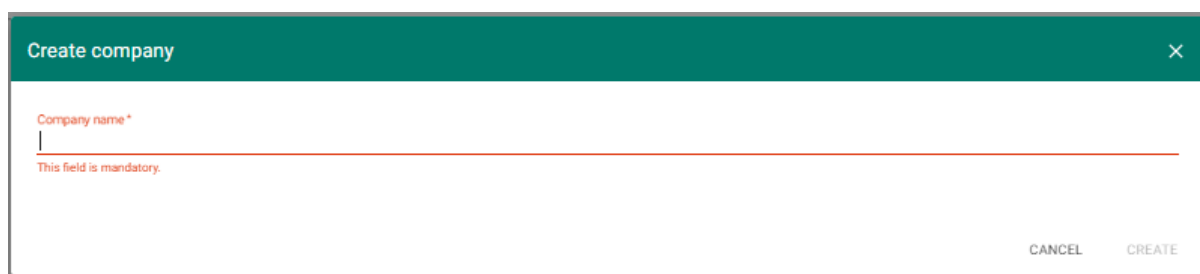
Company list



Name ↑	Zones	Count of Attendance Monitoring users	Count of active Attendance users
My Company	Zone4	10	5

Company creation

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



Create company

Company name*

This field is mandatory.

CANCEL CREATE

Company details

My Company

GENERAL SETTINGS HOLIDAYS ATTENDANCE MODE

Company name
My Company

Count of available Attendance Monitoring licences
10

Default language
English

Count of users with Attendance Monitoring active
5

ZONES DATA IMPORT LDAP

ADD

Zones

Zone4

General settings

- **Company name** – edit the company name.
- **User Attendance license count** – display and modify the count of licenses assigned to a company. Thus, you can assign all the Attendance licenses to the companies. The assignment is necessary for user Attendance monitoring in the selected company.
- **Count of active Attendance Monitoring users** – display how many users are assigned active Attendance Monitoring
- **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.

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

- **Import of HPROJ file settings** – import the basic user/device configuration from the earlier 2N® IP Manager application.
- **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.

LDAP

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

Create LDAP configuration ✕

Server Settings:

Server name * Port* 389

Login name *

Password

Use SSL

LDAP Schema:

Base DN *

Advanced Settings:

Nested search

[VALIDATE LDAP CONFIGURATION](#) [CANCEL](#) [CREATE](#)

See below for more LDAP setting details:

- [4.1.1 LDAP](#)

4.1.1 LDAP

LDAP synchronisation is used for downloading users from the external Active Directory.

ZONES
DATA IMPORT
LDAP

SYNCHRONISATION

Scheduled synchronisation time
00:00:00

Last synchronisation state
Synchronisation failed [01.01.0001 01:00:00]

SYNCHRONISE WITH

<p>SERVER SETTINGS:</p> <p>Server name Test</p> <p>Port 389</p> <p>Login name Test</p> <p>Password ***</p> <p><input type="checkbox"/> Use SSL</p>	<p>LDAP SCHEMA:</p> <p>Base DN AAA</p> <p>ADVANCED SETTINGS:</p> <p><input type="checkbox"/> Nested search</p>
--	--

DELETE CONFIGURATION
VALIDATE LDAP CONFIGURATION

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

 **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.

Warning

Users are only imported via LDAP. User deletion on the LDAP side does not affect deletion in v 2N® Access Commander.

Tip

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

4.2 Users

- [4.2.1 Bluetooth](#)
- [4.2.2 User Types and Rights](#)

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.

<input type="checkbox"/>	Users ↑	Companies	E-mail	Phone Number	
	System admin		tabor@2n.cz		
<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	

Page: 1 Rows per page: 15 1-6 of 6 < >

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**.

Create user
✕

Name*
|
This field is mandatory.

Select company
My Company

Create login credentials?

CANCEL CREATE

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

+

James White

ACCOUNT SETTINGS
AUTHORISATION
ACCESSES
PHONE NUMBERS

INFO

Name
James White

User number
Empty

E-mail
Empty

LOGIN INFO

Login
Empty

GENERATE NEW PASSWORD

ASSIGNMENT

In company
My Company

In group
No item has been added yet.

ADD

ADVANCED

Attendance Monitoring: No

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

User01
Working time: 178:30 Balance: -171:23 Time worked: 7:07

ACCOUNT SETTINGS AUTHORISATION ACCESSES PHONE NUMBERS

INFO

Name
User01

User number
ABC01

E-mail
tabor@2n.cz

LOGIN INFO

Login
Empty

GENERATE NEW PASSWORD

ASSIGNMENT

In company
My Company

In group
Group1

ADD

ADVANCED

Attendance Monitoring: Yes


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.
- **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**.
- **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** – activate Attendance Monitoring if the user access card is set up.

2. Authorisation

- Set the authorisation level assigned to the user. Four options are available; refer to [User Types and Rights](#). User rights can be combined.

3. Accesses



User01
Working time: 178:30 Balance: -171:23 Time worked: 7:07

ACCOUNT SETTINGS AUTHORISATION **ACCESSES** PHONE NUMBERS

ALLOWED ZONES

Zone4

ACCESS RESTRICTIONS

Access time restrictions
No restriction

CARD (3F00F2FBC2) ▼

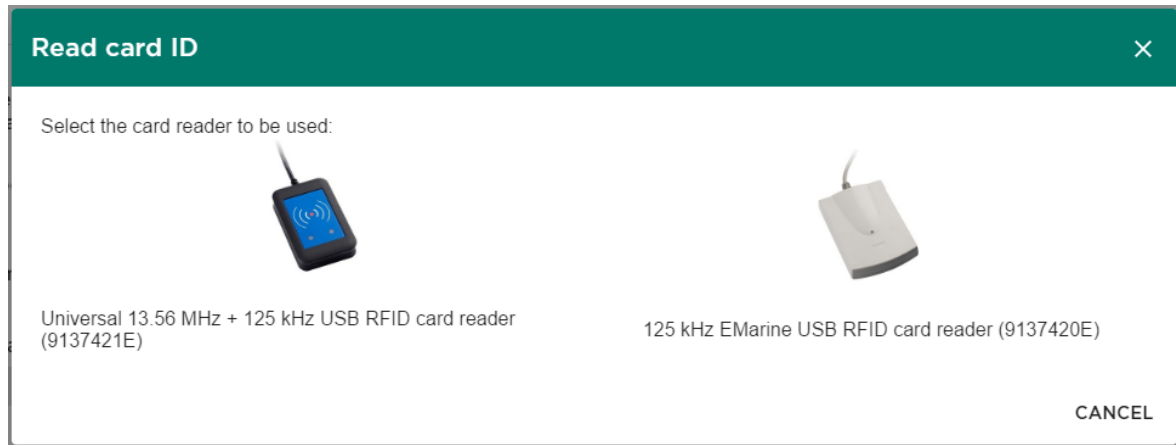
PHONE (UNPAIRED) ▼

BIOMETRY (INACTIVE) ▼

SWITCH CODES (ACTIVE) ▼

- **Allowed zones** – display the zones to which the user has access via the access rule.
- **Access restriction** – set the access rule validity. You can set from, to or both.

- **Identification number** – fill in a number for manual user card entering.
- **Read from reader** – start reading from a reader.



- 13.56 MHz + 125 kHz USB RFID card reader (9137421E) – install the card reader driver. Download from **2N® Access Commander** or www.2n.cz.
 - **Phone** – refer to [4.2.1 Bluetooth](#) for Bluetooth settings.
 - **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.cz.

Fingerprint loading procedure:

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

4. Phone Numbers

User01

Working time: 178:30 Balance: -171:23 Time worked: 7:07

ACCOUNT SETTINGS AUTHORISATION ACCESSES **PHONE NUMBERS**

PHONE NUMBERS

[CREATE](#)

Order	Phone Number	Time Profile	HP Eye	Group call	
#1	1100	N/A	Empty	No	

VIRTUAL NUMBER

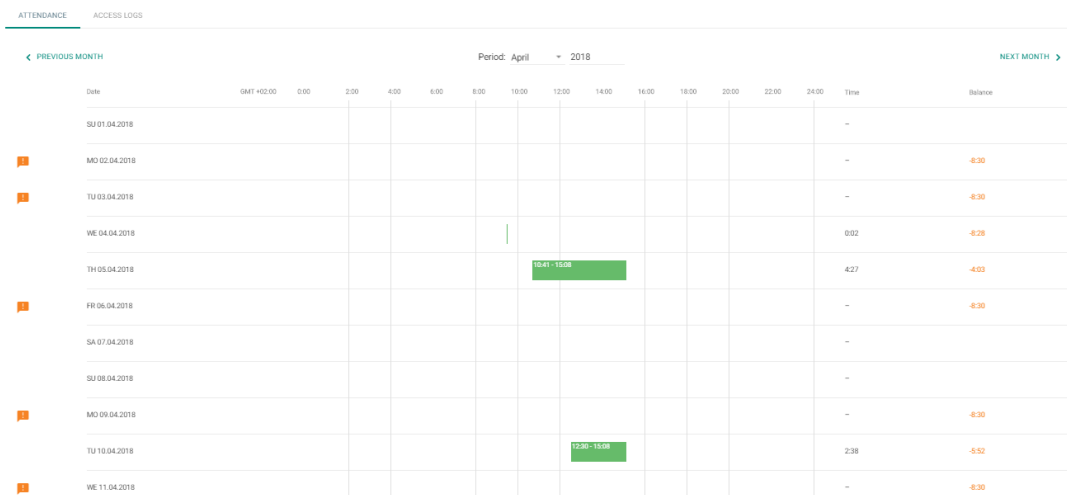
Virtual Number
Empty

Create phone number – set the following parameters:

- The phone number sequence specifies which number is to be dialled first. If the first number is unavailable, the second, third... number is dialled and so on.
- Enter the station phone number to which the call shall be routed.
- 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 means a simultaneous call to the next phone number; when the call is answered via one phone, the other phone will stop ringing.

5. Attendance

Attendance data are displayed in the user detail.



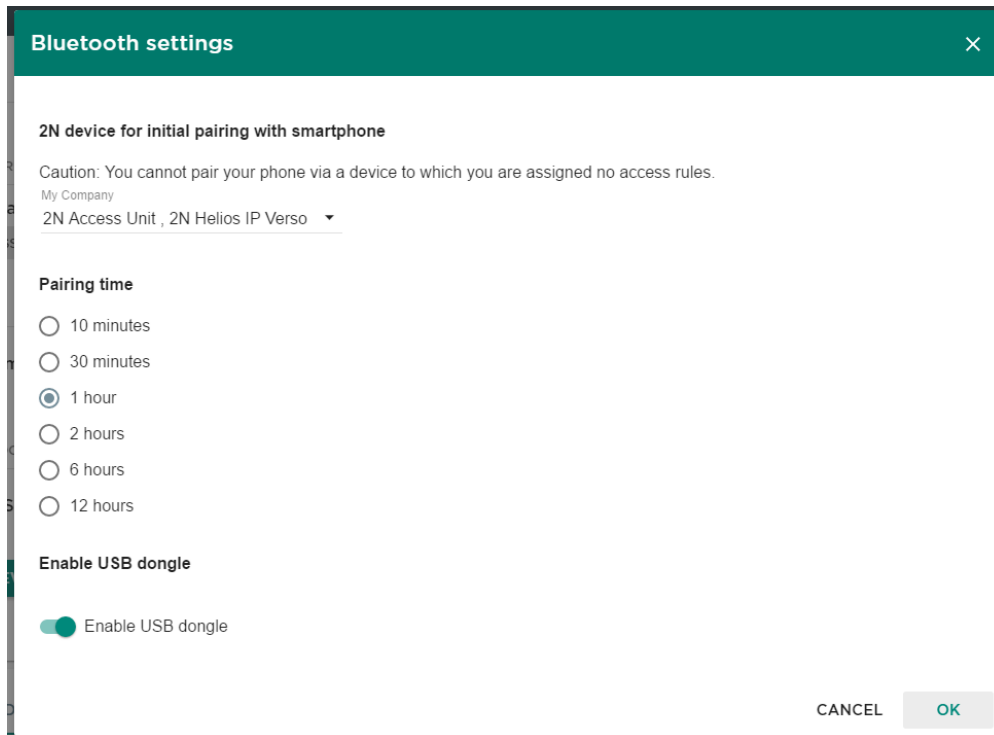
6. Access Logs

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

Time	Zone	Device	Event Type	Event code	User	Description
10.04.2018 15:08:20	Zone4	2N Access Unit + TouchKeyboard	Keypad entered	01	User01	PIN code accepted
10.04.2018 15:08:15	Zone4	2N Access Unit + TouchKeyboard	Card swiped	3F00F2FBC2	User01	Door Entry
10.04.2018 15:08:09	Zone4	2N Access Unit	Card swiped	3F00F2FBC2	User01	Door Entry
10.04.2018 15:07:28	Zone4	2N Helios IP Base	Card swiped	3F00F2FBC2	User01	Door Entry
10.04.2018 15:07:20	Zone4	2N Helios IP Vario	Card swiped	3F00F2FBC2	User01	Door Entry
10.04.2018 15:07:18	Zone4	2N Helios IP Force	Card swiped	3F00F2FBC2	User01	Door Entry
10.04.2018 15:07:14	Zone4	2N Helios IP Verso Ondra	Card swiped	3F00F2FBC2	User01	Door Entry
10.04.2018 15:07:07	Zone4	2N Helios IP Vario	Keypad entered	01	User01	PIN code accepted
10.04.2018 15:04:06	Zone4	2N Helios IP Vario	Keypad entered	01	User01	PIN code accepted
10.04.2018 15:04:02	Zone4	2N Helios IP Vario	Keypad entered	01	User01	PIN code accepted
10.04.2018 15:04:00	Zone4	2N Helios IP Vario	Keypad entered	01	User01	PIN code accepted
10.04.2018 12:31:04	Zone4	2N Helios IP Verso Ondra	Card swiped	3F00F2FBC2	User01	Door Entry

4.2.1 Bluetooth



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.

Vyberte, jakou možnost chcete využít pro spárování

- Spárovat se přes dongle
 Spárovat se přes zařízení

V blízkosti zařízení pro prvotní spárování uživatel zadá kód pro spárování do mobilní aplikace 2N® Mobile Key.

Kód pro spárování

805081 [ODESLAT NA E-MAIL](#)

Čas na spárování

1 hodina (14:30)

Zařízení pro prvotní spárování

2N Helios IP Verso Ondra 2N Access Unit + TouchKeyboard 2N Access Unit

[ZRUŠIT PÁROVÁNÍ](#)

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

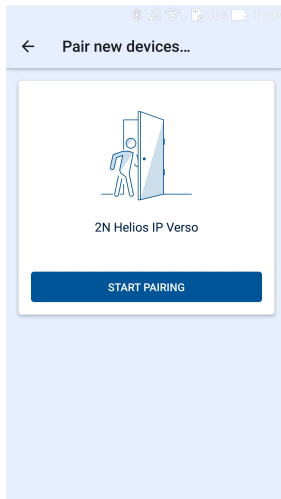
PAIR AGAIN **DELETE**

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

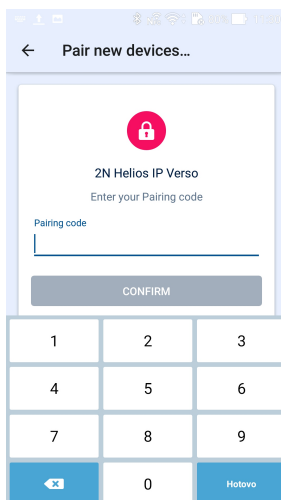
Mobile Application Pairing

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

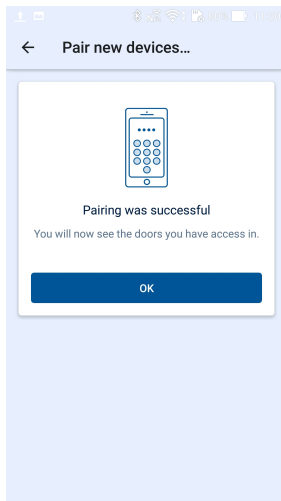
1. The pairing device is displayed in the application.



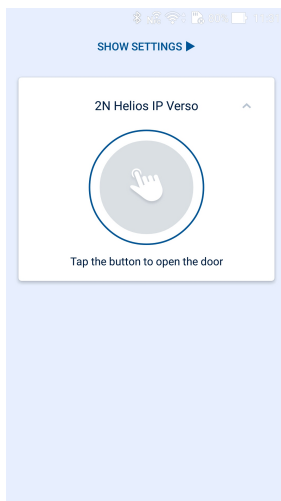
2. Click START PAIRING and, when asked so, enter the PIN generated in **2N® Access Commander**.



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



4. The device can be used for opening doors.

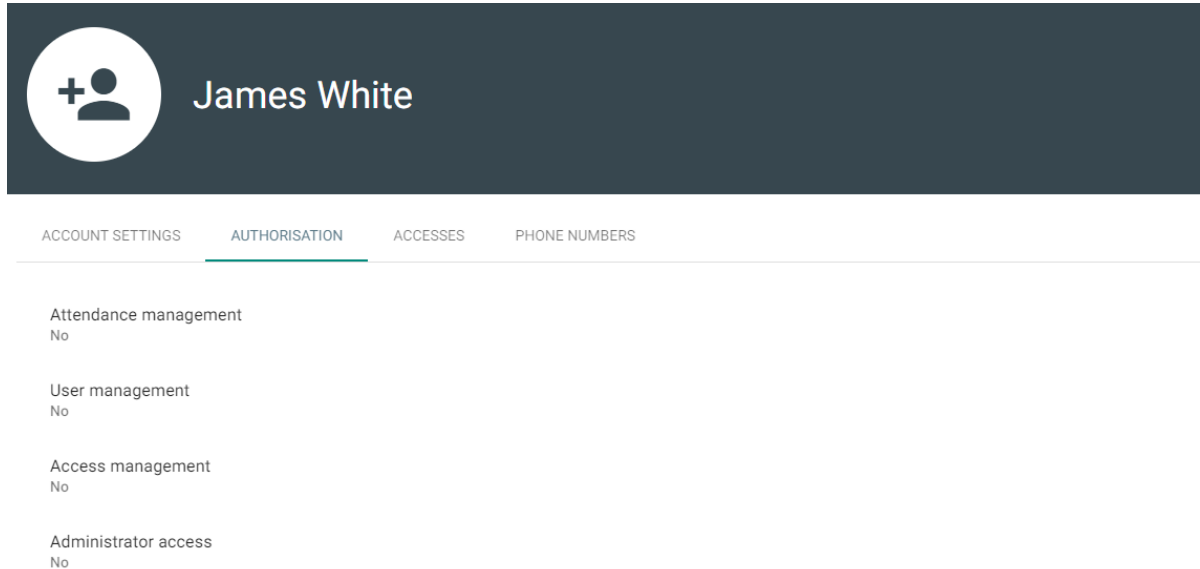


Links to stores:



4.2.2 User Types and Rights

The following five user right types are available:



The screenshot displays the user interface for James White. The header includes a profile icon and the name 'James White'. The navigation menu has four tabs: ACCOUNT SETTINGS, AUTHORISATION (which is selected), ACCESSES, and PHONE NUMBERS. The main content area lists the following user rights and their status:

User Right	Status
Attendance management	No
User management	No
Access management	No
Administrator access	No

Full admin access

- Can create and edit all user/device parameters.
- Sets the access rules.
- Can change licenses.
- Has access to all the modules (as licensed).
- Can change the system and module settings (Attendance, ...).
- Can monitor and edit Attendance of all the users.
- Can create visitor cards.
- Can assign visitor cards to users.

User with user management rights

- Can create/delete and fully edit users.
- Can assign users to groups, add user access cards, edit user phone numbers and edit switch codes.
- Can monitor and export its Attendance.
- Cannot assign rights to users.
- Cannot display or edit other users' Attendance.

User with Attendance management rights

- Can edit Attendance for its group users.
- Can monitor and export user Attendance in the same groups.
- Can neither view nor edit the other users.
- Has no right to assign users to groups.

User with access management rights

- Can create, delete and edit groups.
- Can add/remove users to/from groups.
- Can create and edit time profiles.
- Can create, delete and edit access rules.
- Can assign visitor cards to users.
- Cannot create and edit users.

User

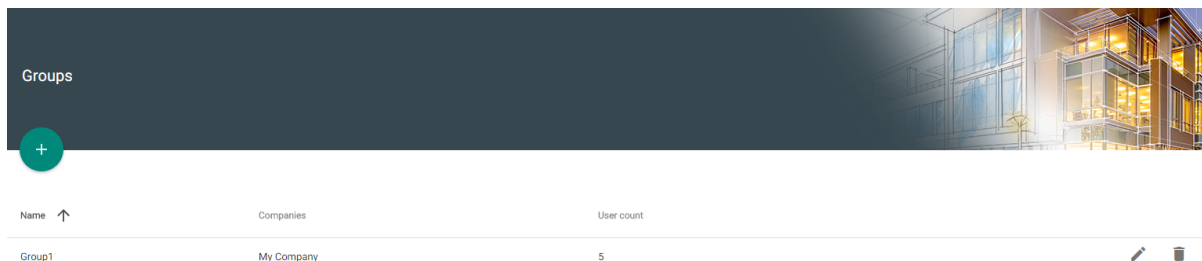
- Can change its password.
- Can neither view nor edit the other users.
- Can view the other modules as licensed and authorised (Presence, Attendance, ...).
- Can monitor and export its Attendance (as licensed and configured).

✓ Tip

- User management, Attendance and access rights can be combined arbitrarily.


4.3 Groups

Groups make it easier to set zone access rights for users. It is because the rights are not set on the user level but a group is associated with a zone.



Group list:

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

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

Group1
5

Group name
Group1

In company
My Company

USERS VISITOR CARDS

ADD

Users		
User01	↗	🗑
User02	↗	🗑
User03	↗	🗑
User04	↗	🗑
User05	↗	🗑

Assign the users and visitor cards via the group detail. You can only assign the users and visitor cards that are assigned to the same company as the group.

4.4 Devices

Device List

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

Device

+

Q STATE

	Name ↑	State	IP address	Serial Number	Firmware Version	
<input type="checkbox"/>	2N Access Unit	Online	10.0.25.136	54-1105-0190	2.23.0.32.3	✎ ⚙ 🗑
<input type="checkbox"/>	2N Access Unit + TouchKeyboard	Online	10.0.25.159	54-1168-0217	2.23.0.32.6	✎ ⚙ 🗑
<input type="checkbox"/>	2N Helios IP Base	Online	10.0.25.151	54-1685-0483	2.23.0.32.5	✎ ⚙ 🗑
<input type="checkbox"/>	2N Helios IP Force	Online	10.0.25.146	54-0473-0646	2.23.0.32.5	✎ ⚙ 🗑
<input type="checkbox"/>	2N Helios IP Vario	Online	10.0.25.183	54-0889-0018	2.23.0.32.4	✎ ⚙ 🗑
<input type="checkbox"/>	2N Helios IP Verso Ondra	Online	10.0.25.133	54-0917-0075	2.23.0.32.5	✎ ⚙ 🗑
<input type="checkbox"/>	2N LTE Verso	Online	89.24.76.81	54-1763-0989	2.23.0.32.5	✎ ⚙ 🗑

Page: 1 Rows per page: 15 1-7 of 7 < >

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 **+** to display the device adding window.

Create device
×

IP Address
 SEARCH NETWORK

Login*

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.

Device Management

2N LTE Verso

Device Status: Online

GENERAL
NETWORK SETTINGS
FEATURES
BACKUP AND RESTORE





<p><small>Device Name</small> 2N LTE Verso</p> <p><small>Serial Number</small> 54-1763-0989</p> <p><small>Firmware Version</small> 2.23.0.32.5</p> <p><small>MAC address</small> 7C-1E-B3-02-BF-CA</p> <p><small>Zone</small> Zone4</p>	<p><small>Synchronisation state</small> Successfully synchronised [11.04.2018 21:11:14]</p> <p><small>Backup state</small> No backup yet</p> <p><small>Active device</small> <input checked="" type="checkbox"/></p>
---	--

COPY SETTINGS
SYNCHRONISE DEVICE
CHANGE PASSWORD
CONFIGURE DEVICE

• General

- **Device name** – set the device name.
- **Serial number** – display the device S/N.
- **Firmware version** – display the device firmware version.
- **MAC address** – display the device MAC address.

- **Zone** – display and edit the zone where the device is located.
- **Device synchronisation** – display the last synchronisation date and time.
- **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.
- **Copy configuration** – select the device to which configuration is to be copied and select the configuration sections to be copied.
- **Synchronise device** – start manual synchronisation.
- **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.

Management			
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.
- **Display configuration**
 - Set the 2N® IP Vario or 2N® IP Verso display. For details refer to Display Configuration [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.
- [4.4.2 Display Configuration](#)
- [4.4.3 Device Configuration via 2N® Access Commander](#)
- [4.4.4 Automatic Synchronisation](#)
- [4.4.5 Device Backup and Restore](#)

4.4.2 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: 54-1763-0989
Firmware Version: 2.23.0.32.5
MAC address: 7C-1E-B3-02-BF-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

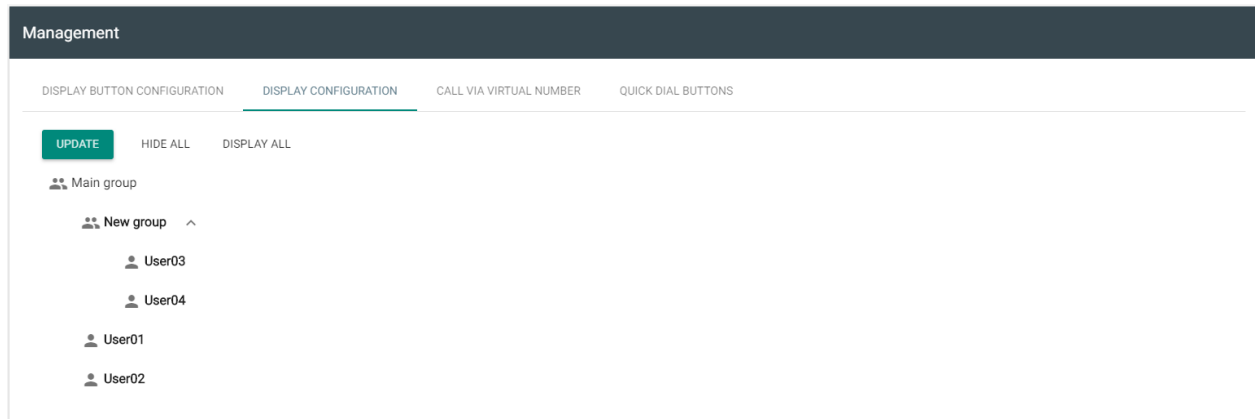
Management

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

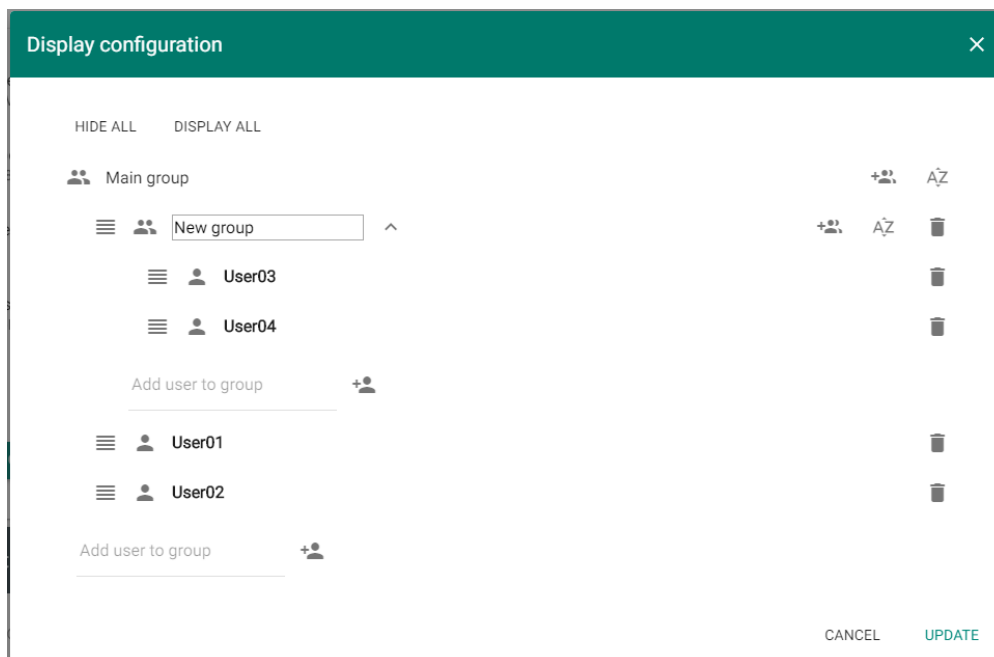
Button number	User
#1	Empty
#2	Empty
#3	Empty
#4	Empty

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 Edit to configure the display.

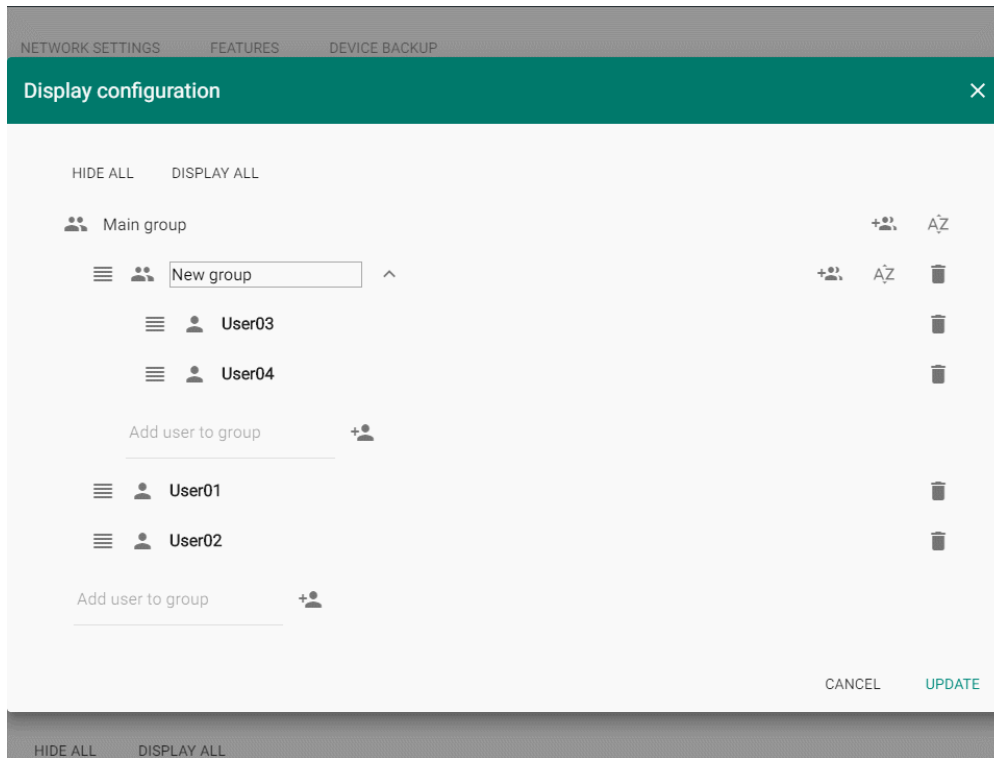


Create the display structure using groups and assigned users.

- Click the  icon to create a group. A group is created under a superior group.
- Use the input at the group end to add a user to the group. You can select more users at once. Click  for confirmation. If you fail to confirm, the selected users are not added to the group.
- All elements marked with  are Drag&Drop. They can be moved to any phonebook level.
























- Click  to arrange the users alphabetically.
- Click  to remove the users and groups.

Adding users to the phonebook:




4.4.3 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	10.0.25.136	54-1105-0190	2.23.0.32.3	  
<input type="checkbox"/> 2N Access Unit + TouchKeyboard	Online	10.0.25.159	54-1168-0217	2.23.0.32.6	  
<input type="checkbox"/> 2N Helios IP Base	Online	10.0.25.151	54-1685-0483	2.23.0.32.6	  
<input type="checkbox"/> 2N Helios IP Force	Inactive	10.0.25.146	54-0473-0646		  
<input type="checkbox"/> 2N Helios IP Vario	Inactive	10.0.25.183	54-0889-0018		  
<input type="checkbox"/> 2N Helios IP Verso Ondra	Online	10.0.25.133	54-0917-0075	2.23.0.32.6	  
<input type="checkbox"/> 2N LTE Verso	Online	89.24.76.81	54-1763-0989	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 LTE Verso

Device Status: Online

GENERAL NETWORK SETTINGS FEATURES BACKUP AND RESTORE

Device Name
2N LTE Verso

Serial Number
54-1763-0989

Firmware Version
2.23.0.32.5

MAC address
7C-1E-B3-02-BF-CA

Zone
Zone4

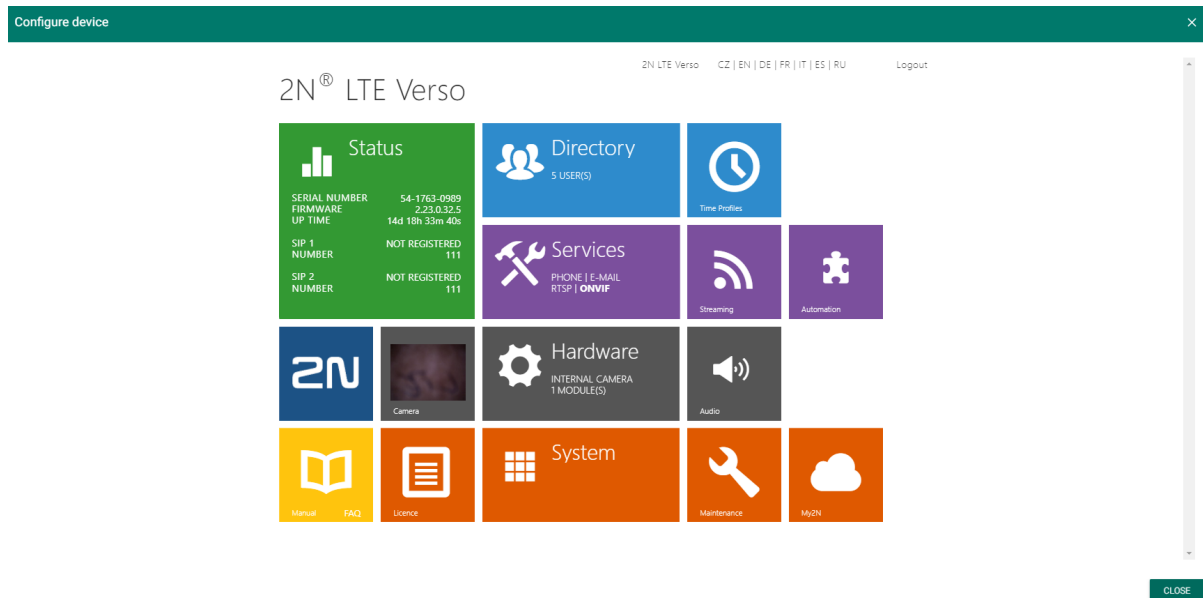
Synchronisation state
Successfully synchronised [11.04.2018 21:11:14]

Backup state
No backup yet

Active device

COPY SETTINGS
SYNCHRONISE DEVICE
CHANGE PASSWORD
CONFIGURE DEVICE

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.



4.4.4 Automatic Synchronisation

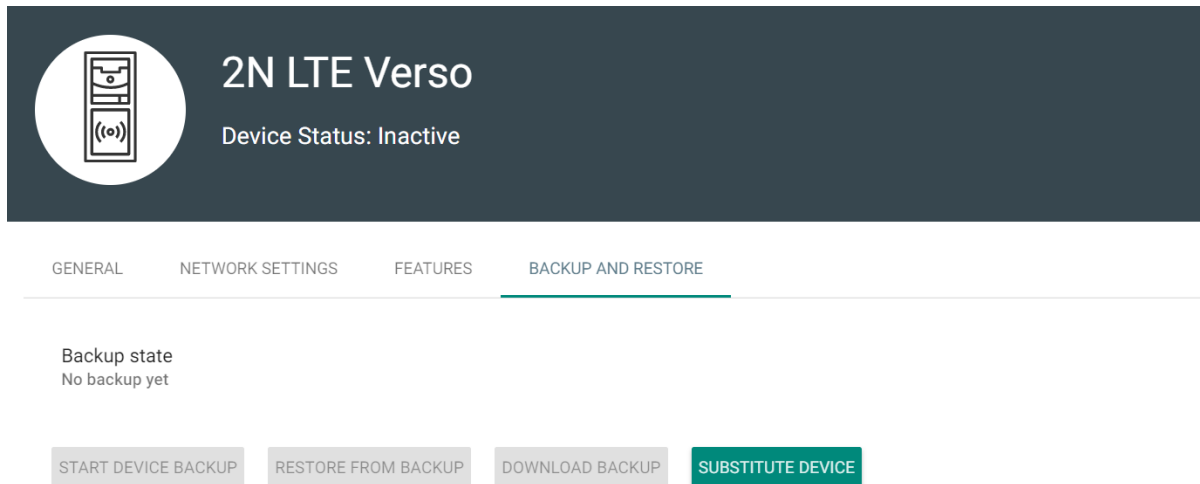
Automatic synchronisation helps maintain the current settings of terminal equipment within the access control system. It starts whenever a change is made that applies to terminal equipment, i.e. that is associated with user access rights, phone numbers, time rules and/or button assignments. The synchronisation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

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.

4.4.5 Device Backup and Restore



2N LTE Verso
Device Status: Inactive

GENERAL NETWORK SETTINGS FEATURES **BACKUP AND RESTORE**

Backup state
No backup yet

START DEVICE BACKUP RESTORE FROM BACKUP DOWNLOAD BACKUP **SUBSTITUTE DEVICE**

- **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 *

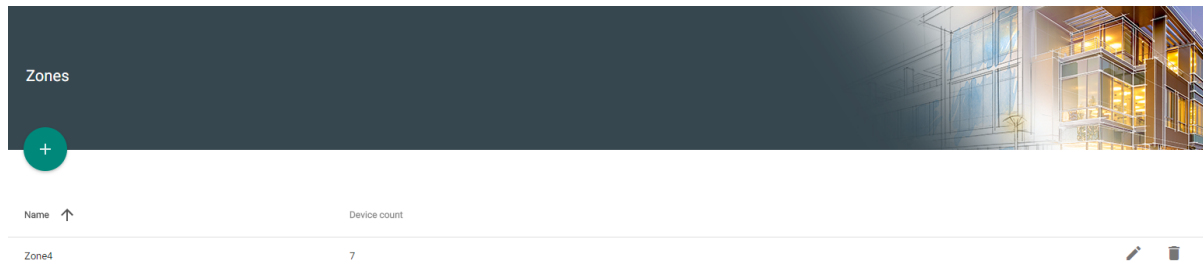
Password *

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

CANCEL SUBSTITUTE

4.5 Zones

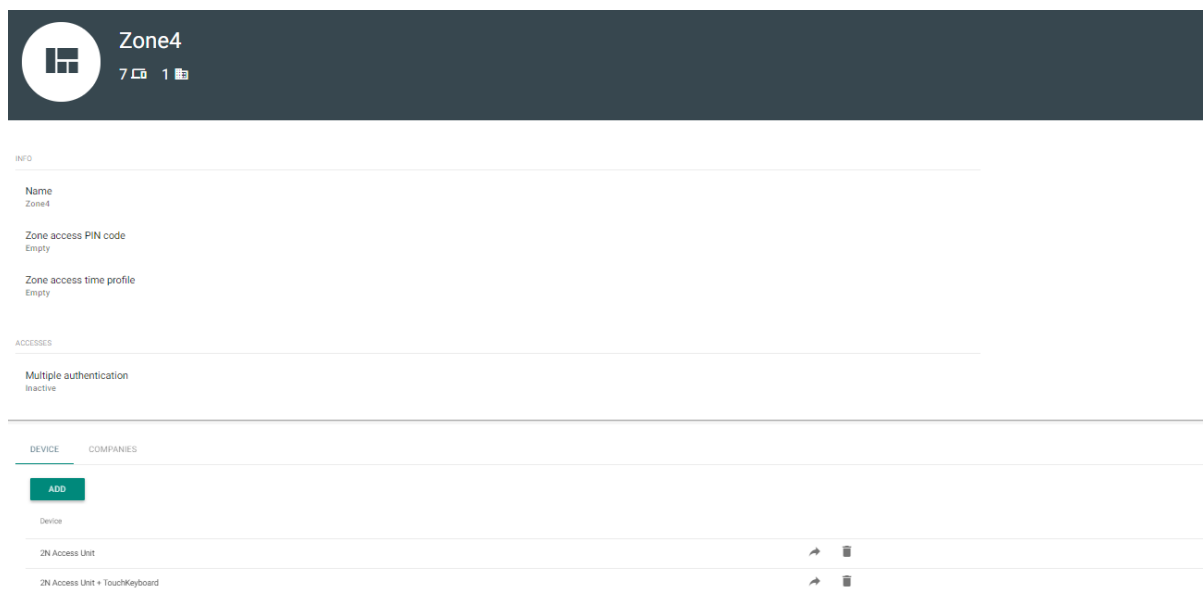
Zones make it easier to administer accesses to devices. Zones unite devices into logical complexes.



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** – zone name.
 - **Zone access PIN code** – set the zone access code as the only authentication method.
 - **Zone access time profile** – limit the zone access code to the set time interval. This is an optional item.

Zones
×

Name*

Zone4

Zone access PIN code

Zone access time profile

CANCEL CHANGE

- **Accesses**

- **Multiple authentication** – set the access rules and their combinations for all the zone devices. Multiple authentication includes, e.g., a card + PIN combination.

Multiple authentication setting
×

Card

Biometry

PIN

Bluetooth

CANCEL CHANGE

- **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

4.6 Time Profiles

Time Profiles

+

Order ↑	Name	Active days	✎	🗑
#1	01	Mo Tu We Th	✎	🗑
#3	02	Sa No	✎	🗑
#4	03	Ho	✎	🗑

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

Create time profile
×

Profile Name*

This field is mandatory.

Order* ▼

CANCEL CREATE

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

Day	0:00	2:00	4:00	6:00	8:00	10:00	12:00	14:00	16:00	18:00	20:00	22:00	24:00
Monday						08:00-18:00							
Tuesday						08:00-18:00							
Wednesday						08:00-18:00							
Thursday						08:00-18:00							
Friday						08:00-18:00							
Saturday						08:00-18:00							
Sunday						08:00-18:00							
Monday						08:00-18:00							

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

Add/set data

- Add **Device**
- Create **Zones** and add devices to them
- Add **User**
- Create **Groups** and add users to them
- Create **Time profiles**
- Set **Access rules**

Group	Zone	Time Profile
Group1	Zone4	N/A

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:



i 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.

5. Extensions

- [5.1 Presence](#)
- [5.2 Attendance](#)
- [5.3 Device Monitoring](#)
- [5.4 Visitor Cards](#)
- [5.5 Notification](#)
- [5.6 CAM Logs](#)
- [5.7 Anti-Passback](#)

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](#)



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 midnight, the presence records are reset in case any of the users forgot to mark 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**.

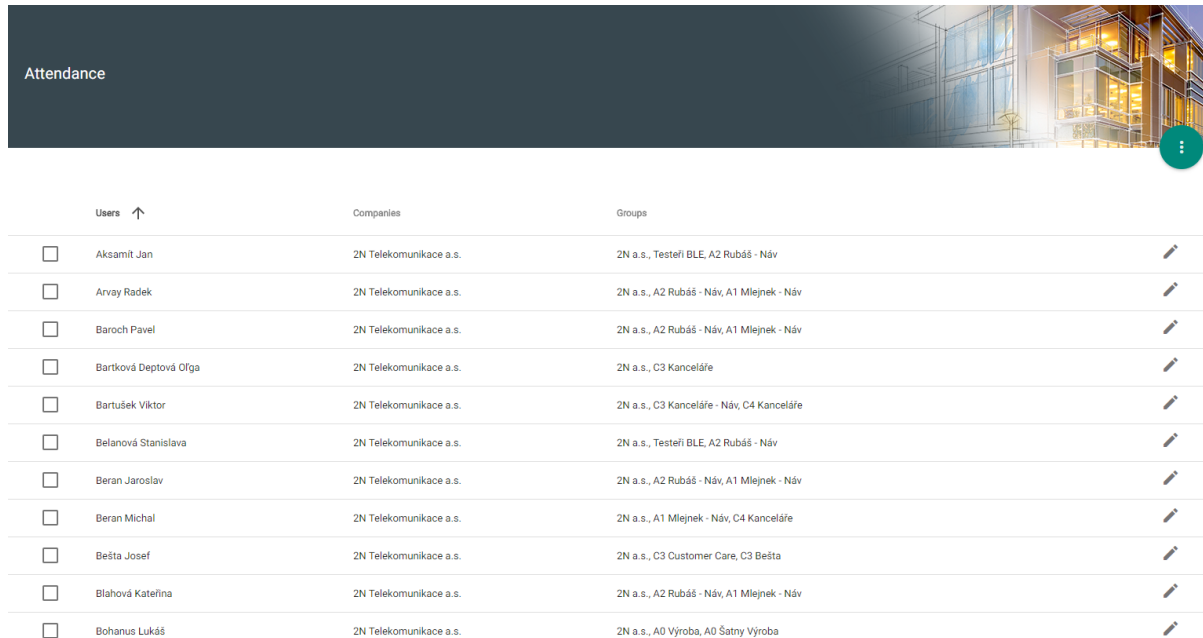
5.2 Attendance

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. Use the Burger menu to export all the monitored user records to a CSV file. The CSV file provides the user attendance balance and the working fund for a given period.

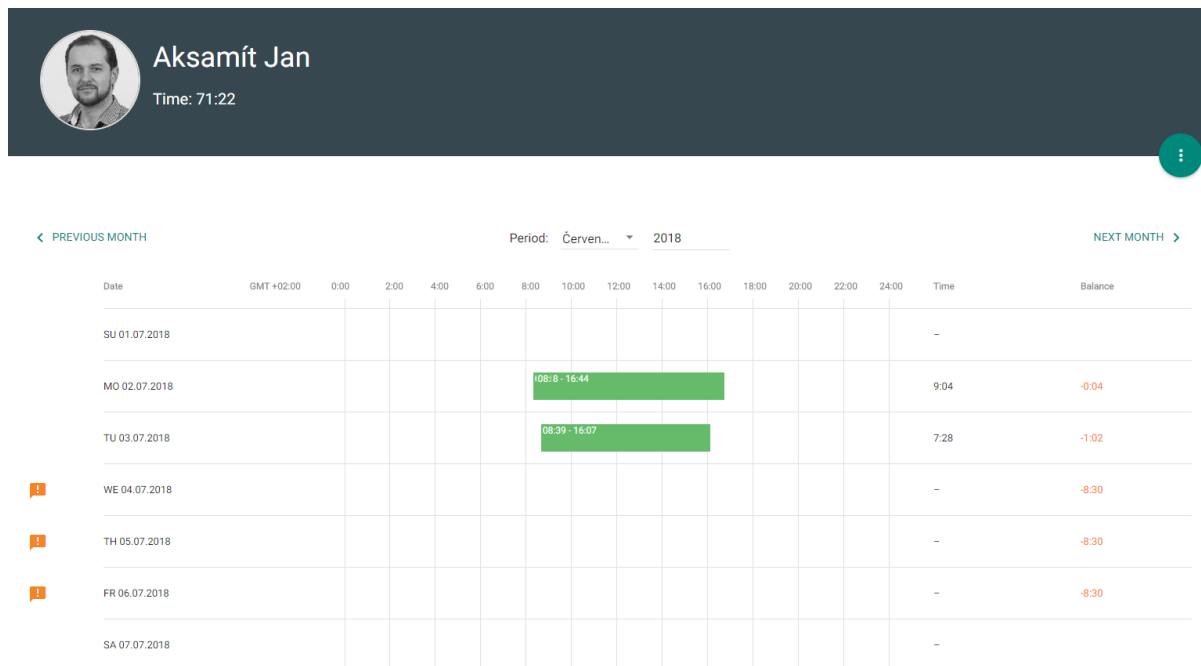
Attendance



Users ↑	Companies	Groups	
<input type="checkbox"/> Aksamit Jan	2N Telekomunikace a.s.	2N a.s., Testeři BLE, A2 Rubáš - Náv	
<input type="checkbox"/> Arvaj Radek	2N Telekomunikace a.s.	2N a.s., A2 Rubáš - Náv, A1 Mlejnek - Náv	
<input type="checkbox"/> Baroch Pavel	2N Telekomunikace a.s.	2N a.s., A2 Rubáš - Náv, A1 Mlejnek - Náv	
<input type="checkbox"/> Bartková Deptová Olga	2N Telekomunikace a.s.	2N a.s., C3 Kanceláře	
<input type="checkbox"/> Bartušek Viktor	2N Telekomunikace a.s.	2N a.s., C3 Kanceláře - Náv, C4 Kanceláře	
<input type="checkbox"/> Belanová Stanislava	2N Telekomunikace a.s.	2N a.s., Testeři BLE, A2 Rubáš - Náv	
<input type="checkbox"/> Berán Jaroslav	2N Telekomunikace a.s.	2N a.s., A2 Rubáš - Náv, A1 Mlejnek - Náv	
<input type="checkbox"/> Berán Michal	2N Telekomunikace a.s.	2N a.s., A1 Mlejnek - Náv, C4 Kanceláře	
<input type="checkbox"/> Bešta Josef	2N Telekomunikace a.s.	2N a.s., C3 Customer Care, C3 Bešta	
<input type="checkbox"/> Blahová Kateřina	2N Telekomunikace a.s.	2N a.s., A2 Rubáš - Náv, A1 Mlejnek - Náv	
<input type="checkbox"/> Bohanus Lukáš	2N Telekomunikace a.s.	2N a.s., A0 Výroba, A0 Šatny Výroba	

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

No special intercom settings are needed for the Attendance free mode. Attendance is generated from the first and last passages on the given day.






















IN/OUT Mode

Set the reader directions for all the devices in **Hardware / Extending modules / Doors** for the IN/OUT mode. Attendance is generated from the first IN and OUT events. This mode is necessary for a correct Presence module function.

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.

Device Monitoring			
Icon	Device Name ↑	Device Status	
	2N Access Unit	Online	 
	2N Access Unit + TouchKeyboard	Online	 
	2N Helios IP Base	Online	 
	2N Helios IP Force	Inactive	 
	2N Helios IP Vario	Inactive	 
	2N Helios IP Verso Ondra	Online	 
	2N LTE Verso	Online	 

[CHANGE TABLE DISPLAY](#)

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.
- Relay state – four state options:
 - a. Closed
 - b. Open
 - c. Door open too long
 - d. Smashed door
- 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 Visitor Cards

You can create so-called visitor cards in **2N® Access Commander**. The administrator adds a few visitor cards to the system, sets the required rights and the user with access rights can assign the cards to visitors.

The visitor card allows to:

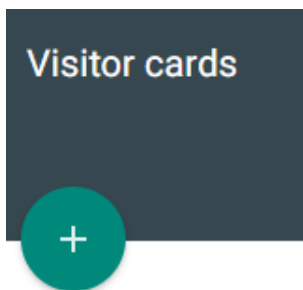
- grant visitors access to selected zones with a limited time validity
- assign access to visitors easily
- monitor visitors' access logs

This card disallows to:

- monitor Attendance
- use BT or PIN for access
- support phone numbers

Administrator settings (add, edit and delete visitor cards):

1. Select Add new card and click Create on the Visitor cards tab.



2. Complete the visitor card data, e.g. 2N – visitor, and the assigned company.

Create Visitor card ×

Card name*
2N guest

Select company*
My Company ▾

CANCEL CREATE

3. Fill in the card ID (manually or load from a reader) and assign the card to a group.

2N guest

ACCOUNT SETTINGS VISITOR

INFO

Visitor card name
2N guest

Card ID
Empty

ASSIGNMENT

Company
My Company

In group
No item has been added yet.

ADD

ENTER MANUALLY READ FROM CARD READER

- Now you have created a visitor card; click on a field to edit the card. As administrator, you can assign a user to the card on the Visitor tab. This can be done by users with Access management rights too, see below. Use the trash bin icon on the visitor card list to delete a visitor card.

Settings as viewed by user with Access management rights (assign, edit and delete visitors)

- Go to the Visitor cards tab to assign a visitor card to a user.
- Select a card from the visitor card list and click the editing pencil to move to the card details.

Visitor cards

Name ↑	Company	Visitor name	Purpose of visit	Validity
2N guest	My Company			
Guest 3rd floor	My Company			
Plumber	2N			

- A table is displayed for you to click one field and complete the user data. Specifically, enter Name, Reason for visit and Access time restriction.

Visitor settings
×


Name*
Walter White

Purpose of visit
Sales manager

From:

Now

Manually


 4/12/2018

Time*

To:

4 hours

Manually

 4/12/2018

Time*

CANCEL CHANGE

4. Save the settings to grant the user a visitor card access. This user is thus allowed to enter the zones assigned to it by the administrator for a time period specified above.
5. Click the user field to edit the user data and access time restriction. Click Delete visitor to delete the user data. After deletion, you can use the card for another user.

Visitor History

Search the access logs for the history of a visitor card. The log includes the card and user names as completed in the card detail.

Time ↓	Zone	Device	Event Type	Event code	User	Description
--------	------	--------	------------	------------	------	-------------

5.5 Notification

The Notification module helps you monitor selected device properties via e-mail. There are five notifications by default. These default notifications relate to the main system functions and cannot thus be deleted. They are as follows:

- Default SMTP host
- Device for licensing is not connected
- License is invalid
- License is obsolete
- Unsupported firmware

Name ↑	Caution	Device	Internal users	External recipients	
Default SMTP host	DefaultSmtpHost				🔔 (⊕) ✎ 🗑️
Device for licensing is not ...	LicenseDeviceInvalid		System admin		🔔 (⊕) ✎ 🗑️
License is invalid	LicenseInvalid		System admin		🔔 (⊕) ✎ 🗑️
License is obsolete	LicensesObsolete		System admin		🔔 (⊕) ✎ 🗑️
Unsupported firmware	UnsupportedFirmware		System admin		🔔 (⊕) ✎ 🗑️

Create a new notification:

1. Complete the notification name
2. Select the notification type
3. Click Create

Create notification
×

Notification name *

This field is mandatory.

Notification type

Device Status
Notification that communication between the device and 2N® Access Commander server has been lost/recovered

Input – status change
Notification that a change on the device input terminals has occurred (departure button pressed, door contact open, etc.)

Output – status change
Notification that a change on the device output terminals has occurred (unlocking, e.g.)

Audio Loop Test
Notification that the device microphone/speaker is not working

SIP Proxy registration
Notification that the device has been unregistered from the SIP Proxy server

Tamper switch activation
Notification that someone is trying to tamper with the unit

Forced entry
Notification that the door has been smashed/kicked out or has not been opened via the access device

Door open too long
Notification that someone failed to close the door

Invalid password entered repeatedly
Notification that the user used invalid login data for three times successively

CSV Synchronization failure
Notification, that the CSV synchronization has failed.

CSV Synchronization success
Notification, that the CSV synchronization has succeeded.

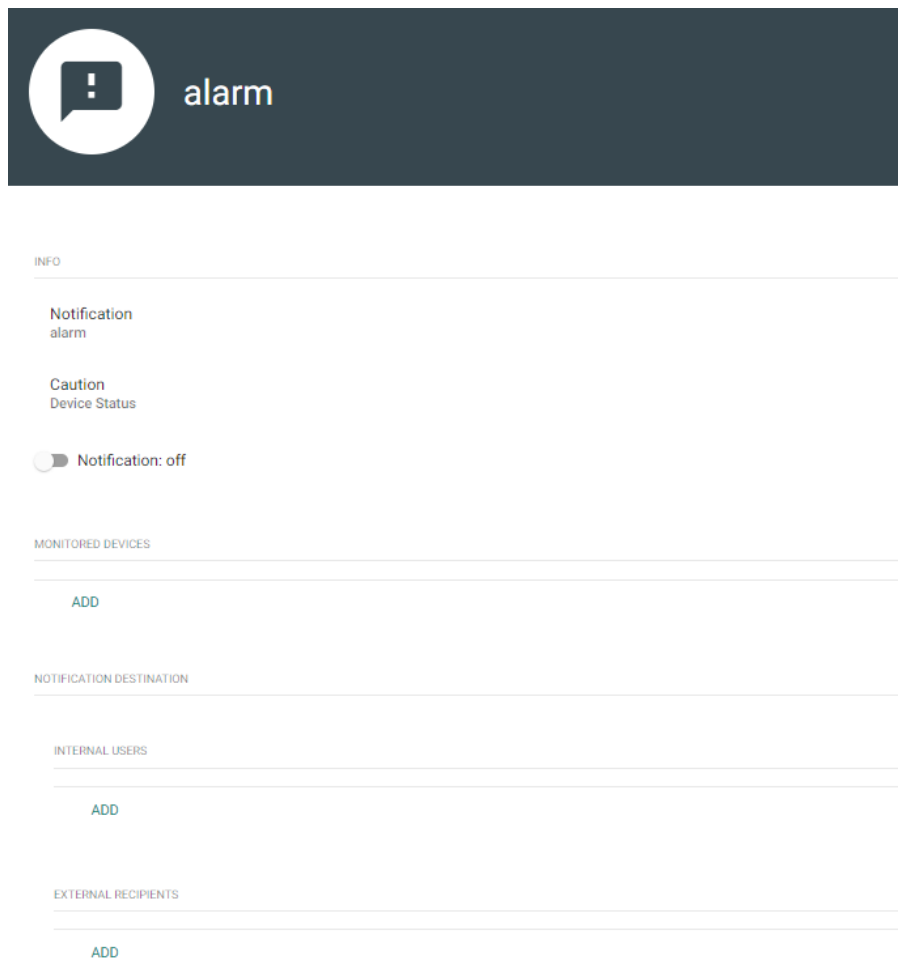
CSV Synchronization partial success
Notification, that the CSV synchronization has been finished with warnings.

Notification type – bulk

Security
Includes "Device state", "Forced entry", "Tamper switch activation", "Door open too long", "Repeatedly entered invalid password"

CANCEL
CREATE

4. After creation, a new page is displayed for you to:
 - a. activate the notification,
 - b. add the devices to be monitored,
 - c. add the users to be sent e-mail,
 - d. add the e-mail address that is not assigned to the user in the system.



- Make sure that [SMTP](#) is set correctly to make 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
×

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
-
-
-

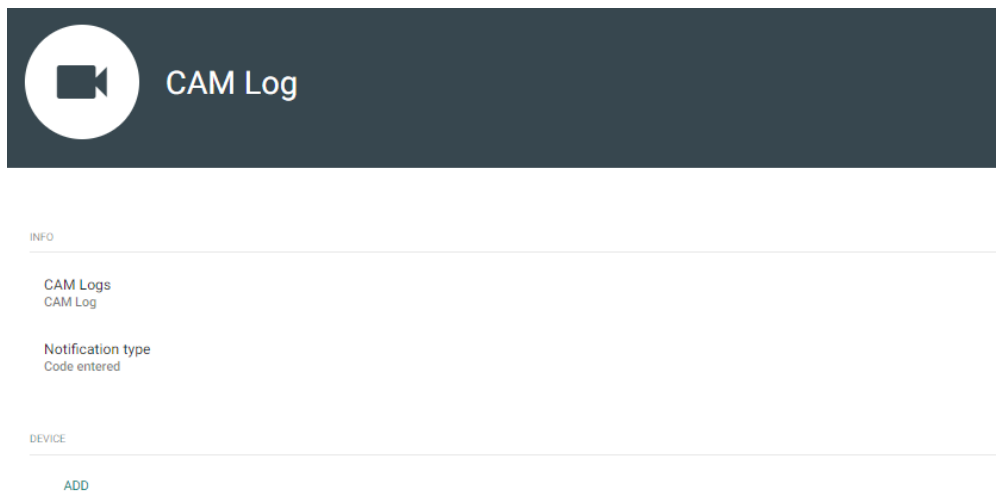
CANCEL
CREATE

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

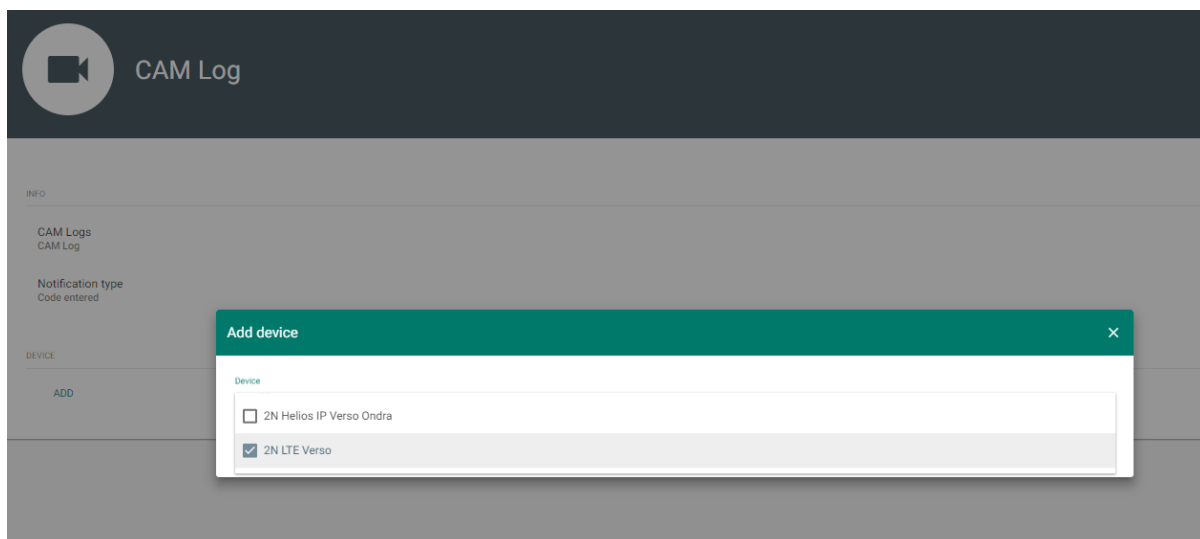
- Code entered
 - Take snapshots whenever the code is entered via the keypad.
- Card applied
 - Take snapshots whenever a card is applied. The snapshot is taken even if the user is not authorised.
- Tamper switch activated
 - Take snapshots whenever the tamper switch is activated. Make sure that the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

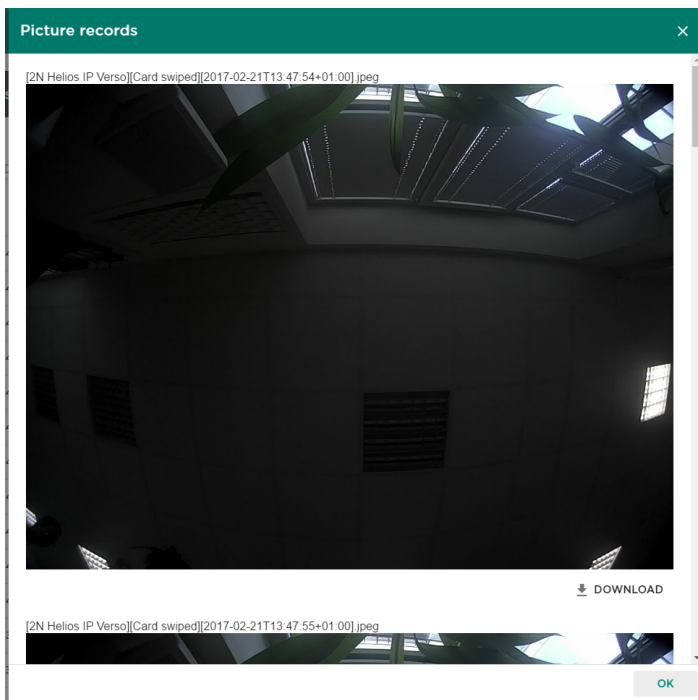


The access logs then display not only passage information but also an image displaying icon. No CAM logs are displayed for the intercoms that are not equipped with a camera.

CAM Log Viewing

Access logs										
FROM:	DD/MM/YY	HH:MM	TO:	12/04/2018	HH:MM	EVENT TYPE	COMPANY	DEVICE	CARD ID:	Q
Time	Zone	Device	Event Type	Event code	User	Description				
11.04.2018 10:44:08	Zone4	2N Helios IP Verso Ondra	Fingerprint			Direction unspecified				
11.04.2018 10:44:08	Zone4	2N Helios IP Verso Ondra	User authorised	User01		-				
11.04.2018 09:52:57	Zone4	2N Helios IP Verso Ondra	User authorised	User01		-				
11.04.2018 09:52:57	Zone4	2N Helios IP Verso Ondra	Bluetooth			Direction unspecified				
11.04.2018 09:50:38	Zone4	2N Helios IP Verso Ondra	User authorised	User01		-				
11.04.2018 09:50:38	Zone4	2N Helios IP Verso Ondra	Bluetooth			Direction unspecified				
11.04.2018 09:50:27	Zone4	2N Helios IP Verso Ondra	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 Anti-Passback


The Anti-passback function enhances the access control system with monitoring of unauthorised re-entering of a reserved space. The areas to be monitored are delimited by edge devices which monitor all entries and exits. These devices check the authorisations of the passing persons as specified for the areas monitored.

Active	Name ↑	Status		
<input checked="" type="checkbox"/>	Common areas	✔		
<input checked="" type="checkbox"/>	Development	✔		
<input checked="" type="checkbox"/>	Warehouse	✘		

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.

Info

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

Settings

Settings applies to all the Anti-passback areas.

- **Type** – set the Anti-passback type:
 - **Soft Anti-passback** – no Anti-passback area access is limited if the rules are broken; the event is only logged with an optional administrator notification.
 - **Hard Anti-passback** – the Anti-passback area access is limited temporarily or permanently and unblocked as a result of the time limit, system administrator's instructions or exit passage.
- **Notification settings** – switch to the [Notifications](#) section.
- **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.
- **User timeout** – set the timeout in which the user will be allowed to re-enter after its previous Anti-passback breach.

Anti-Passback Area Detail


Warehouse

▲ Count of problems to be solved: 1
SHOW ▾

Activate Anti-passback i INFO

Anti-passback area name
Warehouse

Authorization check
On entry

When Anti-passback is set up incorrectly and thus limited in function, the error list is written out automatically. Use the detail to activate/deactivate the function and edit the Anti-passback area name.

- **Error list** – display the list when an Anti-passback error occurs.
- **Activate Anti-passback** – use this parameter to activate/deactivate an Anti-passback area.
- **Anti-passback area name** – edit the Anti-passback area name.
- **Authorisation check** – check the Anti-passback area entry/exit direction.
 - **On entry** – check authorisation on entry. On entry disables an Anti-passback area entry without prior exit.

DEVICES		BLOCKING	
Name ↑	IP	Entry	Exit
2N IP Force	10.0.25.151	Access point 1	↔
▲ 2N IP Verso	10.0.25.139	Access point 1	↔ Access point 2

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

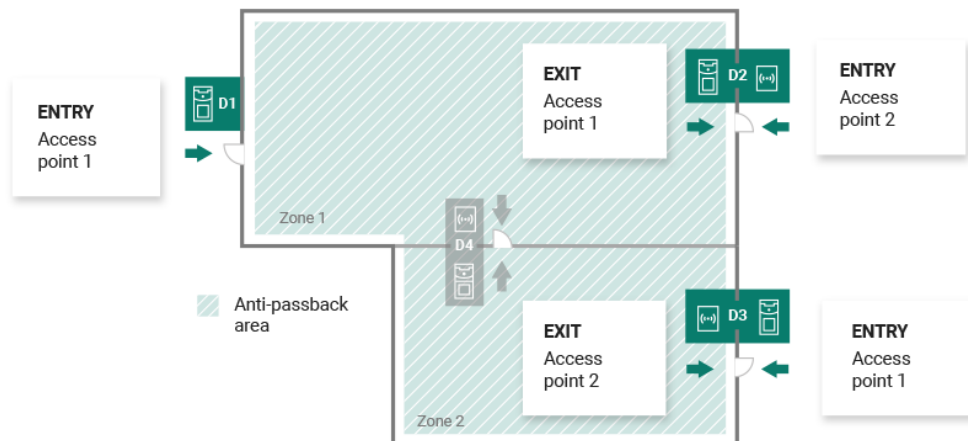
- No device is added to the APB area. Assign one device at least.
- The entry/exit is not defined. Assign one device at least to define the entry/exit direction.
- An entry/exit device has not been configured correctly or does not include a reader.
- An APB area entry device has been used for entry to 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 authorisation. 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.

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.

Area Settings

Set the area in **2N® Access Commander** where multiple devices are used in large areas.

Click Add device to open a bulk adding window. The Access points are completed automatically:

AP 1 = entry, AP 2 = exit. Click the arrows  to switch the Access points if necessary.

Blocking

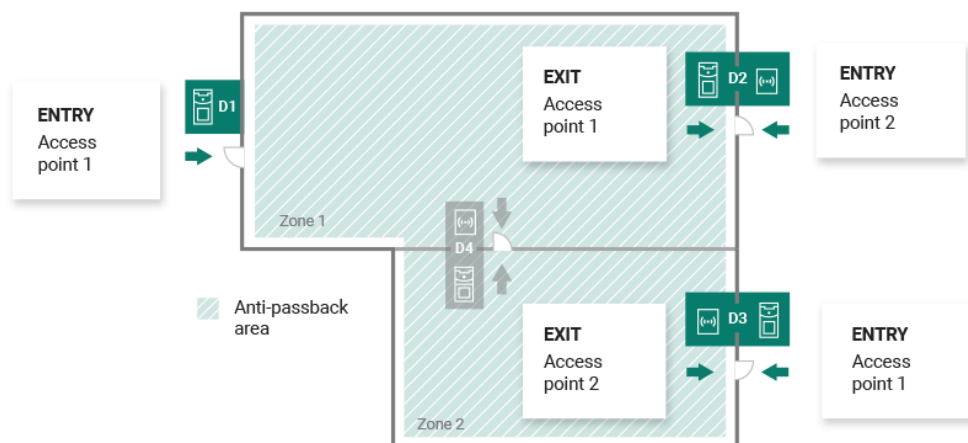
The tab displays the list of blocked users who tried to breach the Anti-passback rules. The system administrator can unblock a user by clicking the icon next to the username or unblock all the users at once by clicking Unblock all.

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 unauthorised 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.

Upozornění

- 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](#)
- [6.2 HTTP API Changes](#)

6.1 API Documentation

6.2 HTTP API Changes

Caution

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

New API changes (full list of changes: [diff file](#)):

- Endpoint added: `/devices/{deviceId}/display/phonebook/view`
- Endpoint added: `/devices/withbackup`
- Endpoint added: `/devices/{deviceId}/replace`
- Endpoint added: `/users/{userId}/mobilekey/pairing/sendmail`
- Endpoint added: `/system/info`
- Endpoint added: `/devices/{deviceId}/switches/`
- Endpoints added: `/users/{userId}/fingerprints/`
- Endpoints added: `/system/diagnostic/package/`
- `POST /visitorcards/{visitorcardID}/visitor` is no longer supported; please use the `PUT` method to create a new card
- New objects: `DisplayObject` a `DisplayNode`
- New objects: `SwitchAction` a `SwitchStatus`
- New objects: `SystemInfo`, `Fingerprint`, `DiagnosticStatus` and `Emails`
- New `Device` parameters: `HasBackup` and `LastBackup`
- New authentication parameters for `Zone`
- New parameter for `User` : `Fingerprints`
- `BackupBase` transformed into a new `Backup` object

