

# 2N<sup>®</sup> Access Commander



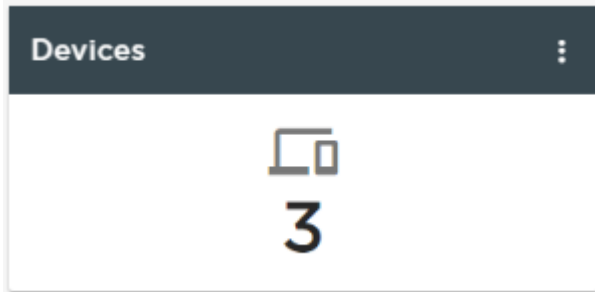
## Content:

- How to Add Device?
- Companies
- User Card Adding
- User Card
- User Types and Rights
- How to Start Monitoring Staff Attendance?
- How to Create and Record Access Rules to Device?
- How Do Access Rules Work?
- Device Configuration via AC
- Copying of Settings between Devices
- Supported Browsers
- 2N® Helios IP and Access Unit Firmware Version
- 2N® Access Commander Server HW and SW Requirements
- 2N® Access Commander Licensing
- Virtual System Setup
- Adding Users to Device
- How to Set Static IP Address
- Back-Up - VirtualBox (AC)
- Presence Module
- Automatic Synchronisation
- Display Configuration
- Device Monitoring
- Notification
- Bluetooth Configuration
- LDAP
- CAM Log
- Visitor Cards
- CSV Synchronisation
- HTTP API

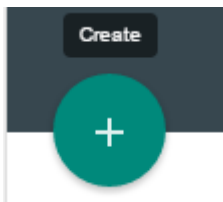


## How to Add Device?

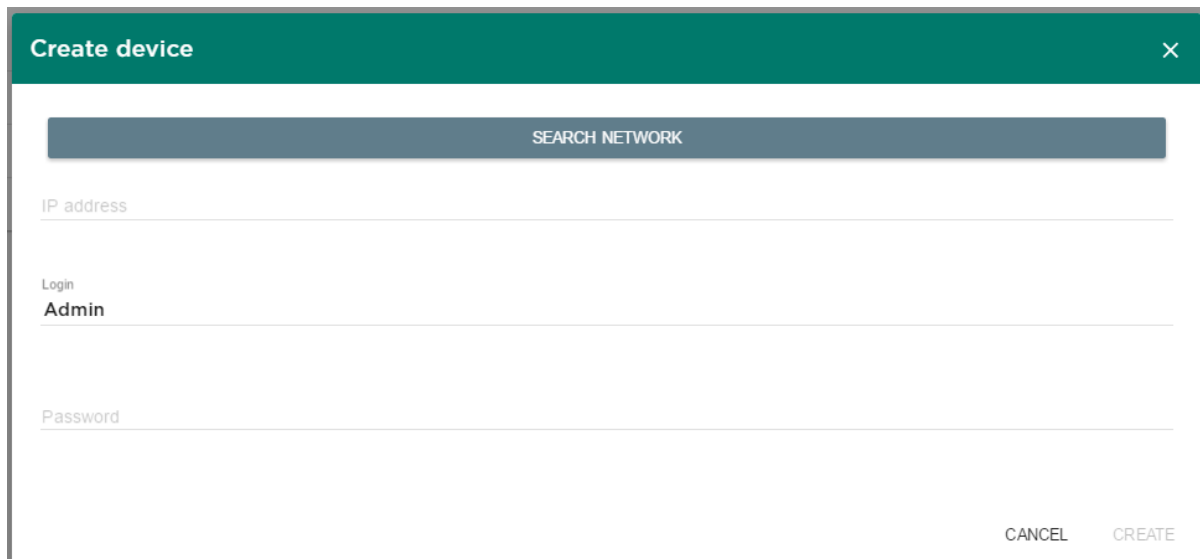
1. Select the **Device** card.



2. Select **Device - Create**.



3. Complete the IP address + port (if other than 443 because the device is behind NAT, e.g.) and access data. You can add multiple devices in one step if they are assigned the same login data. Click Enter to confirm the IP address and port.



Or try to find the device in the network



And select

### Create device ×

**PREVIOUS** **REFRESH**

Type	IP address	Serial number	Name	
2N Helios IP Vario	10.0.25.187	54-0068-0074	Not added to system	<b>ADD</b>
2N Helios IP Verso	10.0.25.193	54-0776-0060	Not added to system	<b>ADD</b>
2N Helios IP Verso	10.0.25.192	54-0917-0375	Not added to system	<b>ADD</b>
2N Access Unit	10.0.25.239	54-1105-0190	2N Access Unit	<b>ADD</b>
2N Helios IP Vario	10.0.25.219	54-0889-0018	2N Helios IP Vario	<b>ADD</b>
2N Helios IP Verso	10.0.25.198	54-0917-0075	2N Helios IP Verso	<b>ADD</b>

**CANCEL** **CREATE**

**Note**

- If the device is in a network other than the AC server, create NAT translation (on the router) and complete the port in the IP address field. Example: “10.0.10.1:44301”.

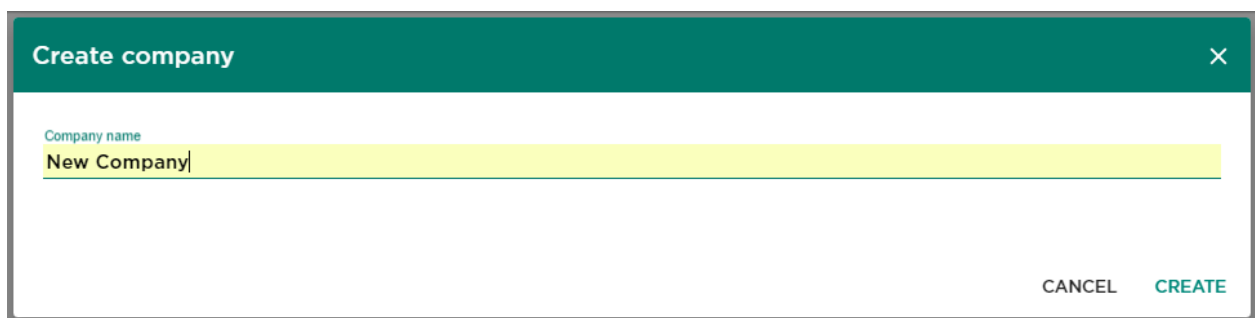
## Companies

### 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 Creation

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



**Create company** ×

Company name

New Company

CANCEL CREATE

## Company Card

## General Settings

- **Company name** – edit the company name.
- **Attendance user count (licensed)**– display and modify the count of licences assigned to a company. Thus, you assign all the Attendance licences to the companies. The assignment is necessary for you to monitor the user attendance in the selected company.
- **Count of available Attendance Monitoring licences** – display how many users have active Attendance Monitoring licences.
- **Default 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. Copy holidays from another company 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 only the name is rewritten if the holiday to be copied is already listed. If unlisted, the holiday is not added.

## Attendance Mode

- **Working days** – display a list of working days.
- **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 earlier 2N® Helios IP Manager versions.
- **User import from device** – import users from a selected device.
- **User import from CSV file** – import users and groups from a CSV file.
- **Download sample CSV file** – download a sample CSV file for user import.

## LDAP

The screenshot shows the LDAP configuration page with the following details:

- SYNCHRONIZATION:**
  - Scheduled synchronization time: 00:00:00
  - Last synchronization state: SUCCESSFUL
  - Buttons: Synchronize
- SERVER SETTINGS:**
  - Server name: Empty
  - Port: 389
  - Login name: Empty
  - Password: [input field]
- LDAP SCHEMA:**
  - Base DN: Empty
  - Nested search
- ADVANCED SETTINGS:**
  - Use SSL
- DELETE CONFIGURATION:** [button]

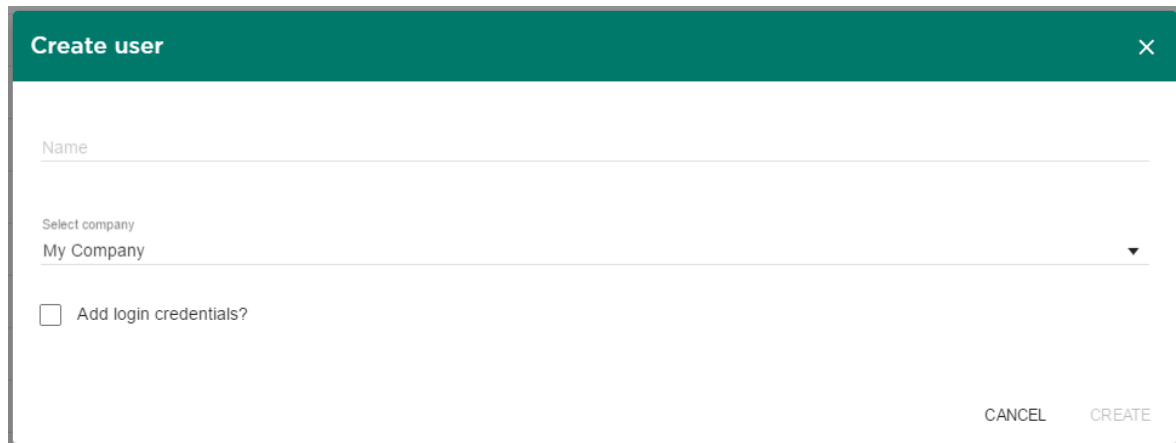
LDAP is used for downloading users from an external Active Directory system. Refer to [LDAP](#) for more information on how to set up LDAP in 2N® Access Commander.



## User Card Adding

Refer to Subs. [Who is assigned what rights? User Types.](#)

1. Select the **Users** card.
2. Select **Users – Create (Add button)**.
3. Complete the mandatory data: **Name / Company / Role** and press the **Create** button.
4. Create login data (optional). Create **Login / Password**



The screenshot shows a 'Create user' dialog box. It features a dark green header bar with the text 'Create user' and a close button (X) in the top right corner. Below the header, there is a text input field labeled 'Name'. Underneath that is a dropdown menu labeled 'Select company' with 'My Company' selected. At the bottom left, there is a checkbox labeled 'Add login credentials?'. At the bottom right, there are two buttons: 'CANCEL' and 'CREATE'.

5. If added successfully, the new user is displayed in the **Users** table and can thus be assigned to **Groups** and its parameters can be configured (**Cards, Phone numbers, Switch codes, ...**).

## User Card

Use the User card to set the user details, accesses and phone numbers.

**User01**  
Working period: 170:00 Balance: -83:51 Worked hours: 86:09

ACCOUNT SETTINGS | AUTHORISATION | ACCESSES | PHONE NUMBERS

**INFO**

**Name**  
User01

**User number**  
Empty

**E-mail**  
noreply@2n.cz

**LOGIN INFO**

**Login**  
user1

[GENERATE A NEW PASSWORD](#)

**INCLUSION**

**In company**  
My Company

**In group**  
Group1 X

[ADD](#)

**EXTENDED**

Attendance Monitoring: Yes

### 1. Account setting

- Name – set the user name for the **2N® Access Commander** operation and Helios IP upload.
- User number – used for administration with external systems.
- E-mail – set the address on which the **2N® Access Commander** account information shall be sent.
- Login set the user login.
- Generate new password – click this button to send an e-mail to the user including a new password. The user must change this password upon the first login to the **2N® Access Commander**.
- In company – display the company assignment.
- In group – display the user group assignment. A user can be assigned to multiple groups within a company.
- Attendance monitoring – make sure that an access card is set for the user to be monitored.

### 2. Authorisation

- set the user right assigned to the user. Refer to User Types and Rights for details. User rights can be combined.

### 3. Accesses

**User01**  
Working period: 170:00 Balance: -83:51 Worked hours: 86:09

ACCOUNT SETTINGS AUTHORIZATION **ACCESSES** PHONE NUMBERS

ALLOWED ZONES  
Zone1 Zone2 Zone3

CARD  
Identification number: 3F00F2F512  
LOAD FROM READER

DOUBLE AUTHENTICATION  
 Double authentication: No

ACCESS LIMITATION  
Access time limitations: Unselected

PHONE  
The user enters the pairing code to the 2N Mobile Key application near the primary pairing device.  
Pairing code:   
Pairing time: 1 hour  
Primary pairing device: 2N Helios IP Verso

SWITCH CODES  
  
Switch: Switch code

#1 1

- Allowed zones – display the zones to which the user has access via the access rule.
- Identification number – display a window to set the user card number manually.
- Read from reader – click to display the reader selecting window.

**Read card ID** [X]

Select the card reader to be used:

Universal 13.56 MHz + 125 kHz USB RFID card reader (9137421E)

125 kHz EMarine USB RFID card reader (9137420E)

CANCEL

1. 13.56 MHz + 125 kHz (9137421E) USB RFID reader – install a card reader driver. Download from **2N® Access Commander** or [www.2n.cz](http://www.2n.cz).
  2. 125 kHz EMarine (9137420E) USB RFID reader – no driver is required, but make sure that the English keypad version is enabled.
- Telephone – a separate screen, Bluetooth configuration, is available for [Bluetooth setting](#).
  - Switch codes – user switch activation codes. The switch code helps you open a door lock, e.g., via the keypad or DTMF code.
  - Double authentication – used for higher user security. The user must enter its code after applying its card. Make sure that the card Id and switch code are defined to make this function work properly.
  - Access limitation – limit the access data validation time: from, to or both.

## 4. Phone numbers

**User01**  
Working period: 170:00 Balance: -83:51 Worked hours: 86:09

ACCOUNT SETTINGS    AUTHORISATION    ACCESSES    **PHONE NUMBERS**

PHONE NUMBERS

**CREATE**

Order	Phone number	Time profile	HIP Eye	Group call	
#1	1100	N/A	Empty	No	

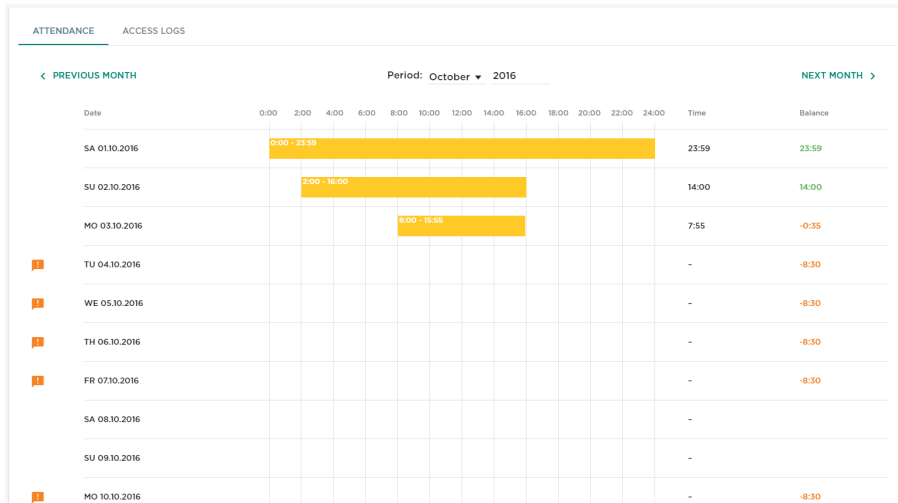
VIRTUAL NUMBER

Virtual number  
Empty

Create phone number via the following parameters.

- Phone number sequence – define which number shall be called first. If the first number is unavailable, the second and then the third number shall be dialled.
- Phone number of the station to be called.
- Time profile for phone number time limitations.
- HIP Eye address to be used by **2N® Helios IP Eye** for displaying a camera image window to users that are not equipped with a display-equipped video telephone.
- Group calls are used for simultaneous calling to the following phone number. When the call is answered on one phone, the other phone will stop ringing.

## 5. Attendance



Attendance data in user detail.

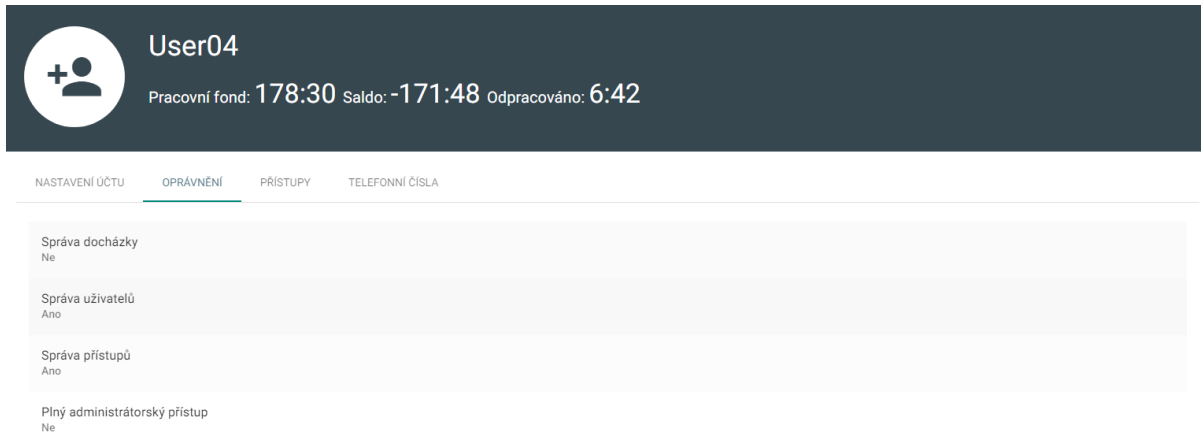
## 6. Access logs

Time	Zone	Devices	Event type	Event code	User	Description
31. 10. 2016 11:37:06	Zone1	2N Helios IP Verso	Card swiped	3F00F2FBC2	User01	Check in
31. 10. 2016 10:38:16	Zone1	2N Helios IP Verso	Card swiped	3F00F2FBC2	User01	Check in
31. 10. 2016 10:38:14	Zone1	2N Helios IP Verso	Card swiped	3F00F2FBC2	User01	Check in
31. 10. 2016 10:11:47	Zone1	2N Helios IP Verso	Card swiped	3F00F2FBC2	User01	Check in
26. 10. 2016 17:23:21	Zone1	2N Helios IP Verso	Keypad entered	1	User01	PIN accepted
26. 10. 2016 17:22:59	Zone1	2N Helios IP Verso	Keypad entered	1	User01	PIN accepted
26. 10. 2016 17:22:12	Zone1	2N Helios IP Verso	Keypad entered	1	User01	PIN accepted
26. 10. 2016 17:21:37	Zone1	2N Helios IP Verso	Keypad entered	1	User01	PIN accepted

Filtered-out access logs. You can see all passages and keypad presses for all the devices added to the **2N® Access Commander**.

## User Types and Rights

The following five types of user rights are available with the following meanings:



**User04**  
Pracovní fond: 178:30 Saldo: -171:48 Odpracováno: 6:42

NASTAVENÍ ÚČTU   OPRÁVNĚNÍ   PŘÍSTUPY   TELEFONNÍ ČÍSLA

- Správa docházky  
Ne
- Správa uživatelů  
Ano
- Správa přístupů  
Ano
- Plný administrátorský přístup  
Ne

### Full administrator access:

- Can create and edit all the user and device parameters.
- Can set the access rules.
- Can change licences.
- Can access 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 administration right is authorised to:

- Can create/delete and fully edit users.
- Can add 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 attendance of the other users.

### User with attendance administration right

- Can edit attendance of users from its groups.
- Can monitor and export user attendance in the same groups.
- Cannot see or edit the other users.
- Has no right to assign users to groups.

### User with access administration right

- 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.
- Cannot create new users or edit existing ones.

### User

- Can change its password.
- Cannot see or edit the other users.
- Can see other modules (Presence, Attendance, ...) as licensed and authorised.
- Can monitor and export its attendance as licensed and configured.

 **Tip**

- User rights for user/attendance/access administration can be combined arbitrarily.

## How to Start Monitoring Staff Attendance?

Set the following to monitor the staff **Attendance**:

### 1. Event Reading

- Configure the passage direction for all the selected card readers (**Hardware / Extending modules / Direction**).
- Set the automatic download period in the Access Commander (**Settings / Download data from device**).
- Set the attendance mode (**Settings / Attendance module mode**).
  - Free
  - In-Out (necessary for Presence function)

### 2. Attendance Control at User

- Complete the user access card ID (**Users → Access card → Card ID (Identification number)**).
- Enable user attendance monitoring – use a checkbox (**Users → Attendance monitoring**).

### 3. Licence

- User attendance monitoring is licensed for a defined count of users. See the current state in **Setting → Licence → User count for attendance**.
- Set the user count to be monitored in **Companies → Count of available user attendance monitoring licences**.



## How to Create and Record Access Rules to Device?

### Add/Set Data

- Add **Device**.
- Create **Zones** and add a device to them.
- Add **User**.
- Create **Groups** and add a user to them.
- Create **Time profiles**.
- Set **Access rules**.

### Record to Device

Once the access rule is created, the device to which the users are to be added joins the synchronisation queue. Automatic synchronisation takes place within a minute after the access rule creation.

### Synchronisation can be started manually too:

1. Go to the **Device** card to record to device.
2. Open the selected device.
3. Press the dedicated button in **Device synchronisation** in the Management block.

## How Do Access Rules Work?

Group ↑	Zone	Time profile ↓
Group1	Zone1	N/A

The access rules define to WHOM, WHERE and WHEN is access 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 Info**


- 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.

## Device Configuration via AC

1. Select the **Device** card.
2. Select the **active** device to be configured from the list of added devices and choose the **Modify** device option (click anywhere in the selected device row).

Name ↑	Status	IP address	Serial number	Firmware version	
2N Access Unit	Online	10.0.25.239	54-1105-0190	2.15.0.24.3	  
2N Helios IP Vario	Online	10.0.25.219	54-0889-0018	2.15.0.24.3	  
2N Helios IP Verso	Online	10.0.25.198	54-0917-0075	2.15.0.24.3	  

3. In the **General** menu select **Configure device**. If the device is not in the **active state**, the **Configure device** option cannot be used. The parameter icon is inactive in this case.



### 2N Access Unit

Device state: Online

GENERAL
NETWORK SETTINGS
FEATURES
DEVICE BACKUP

**Device name**  
2N Access Unit

**Serial number**  
54-1105-0190

**Firmware version**  
2.15.0.24.3

**MAC address**  
7C-1E-B3-01-39-DD

**Zone**  
Zone2

**Synchronisation state**  
Synchronisation completed successfully [30.03.2016 13:35:14]

**Backup state**  
No backup yet

COPY SETTINGS
SYNCHRONISE ALL DEVICES
CONFIGURE DEVICE

4. A new window opens up for you to configure the selected device (for parameter details refer to the Configuration Manual at <https://manuals.2n.cz/is/en>). Click the right-hand upper corner to close the window any time and return to the environment of the **2N® Access Commander**.

Configure device

2N Helios IP Verso CZ | EN | DE | FR | IT | ES | RU Logout

### 2N® Helios IP Verso

<b>Status</b> SERIAL NUMBER: 54-0917-0075 FIRMWARE: 2.15.0.24.3 UP TIME: 0d 16h 22m 9s SIP 1 NUMBER: NOT REGISTERED 201 SIP 2 NUMBER: NOT REGISTERED 111 <b>Warning: Default Password in Use</b>	<b>Directory</b> 5 USERS(S) 5 CARDS(S) Time Profile	
<b>2N</b>	<b>Services</b> PHONE   E-MAIL RTSP   ONVIF Streaming Automation	
Camera	<b>Hardware</b> INTERNAL CAMERA 6 MODULE(S) Audio	
Manual   FAQ	License	<b>System</b> DHCP   TLS   MDS Maintenance

CLOSE

## Copying of Settings between Devices

1. Go to **Device**.
2. Select the **active** device whose configuration is to be copied and select **Modify device**.
3. In the **General** menu select **Copy setting**. If the device is not in the **active state**, this option cannot be used. The parameter icon is inactive in this case.
4. Select the target device. Hold **Ctrl** and mouse click more list items to select multiple target devices at once.
5. Moreover, you can specify the setting parts to be copied in this window. Again, use **Ctrl** to choose more sections.
6. Having completed selection, click **Copy setting** to save the device selection.

**Copy settings to another device** ×

Select the target devices for loading device settings:

- 2N Access Unit
- 2N Helios IP Vario

Select the section(s) to be copied:

- Network
- Authentication
- WebServer
- HttpApi




CANCEL COPY SETTINGS

## 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.

## 2N® Helios IP and Access Unit Firmware Version

## Connected Device Firmware Overview

FW version	Synchronisation	Downloading events	Monitoring devices	Bluetooth	Access data validity	CAM Log
2.20.0.2 9.5	✓	✓	✓	✓	✓	✓
2.19.2.2 8.9	✓	✓	✓	✓	✓	✓
2.19.1.2 8.8	✓	✓	✓	✓	✓	✓
2.18.0.2 7.5	✓	✓	✓	✓	✓	✓
2.17.0.2 6.5	✓	✓	✓	✓	✓	✗
2.16.1.2 5.7	✓	✓	✓	✗	✗	✗
2.16.0.2 5.4	✓	✓	✓	✗	✗	✗
2.15.2.2 4.7	✓	✓	✓	✗	✗	✗
2.15.1.2 4.5	✓	✓	✓	✗	✗	✗
2.15.0.2 4.3	✓	✓	✓	✗	✗	✗



**Note**

The Bluetooth module is available only for **2N® Helios IP Verso** and **2N® Access Unit**.

## 2N® Access Commander Server HW and SW Requirements

**2N® Access Commander** is distributed as a virtual image for Oracle VirtualBox and VMWare.

### Host system requirements

**Note**

- **2N® Access Commander** requires 64bit OS.

Minimum hardware configuration that allows for connection of up to 50 Helios IP devices:

- **OS:** any 64bit OS (Windows, OS X, Linux, Solaris)
- **CPU:** 64bit, 2 GHz, 2 cores (VT-X support recommended)
- **RAM:** 4 GB
- **LAN:** 1Gbit

### Minimum guest system requirements

- **CPU:** 2 cores
- **RAM:** 2 GB
- **LAN:** bridged

### 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.

## 2N® Access Commander Licensing

### **Note**

There is a change in licensing from version 1.5.0: one connected device has to be selected as a licensed one.

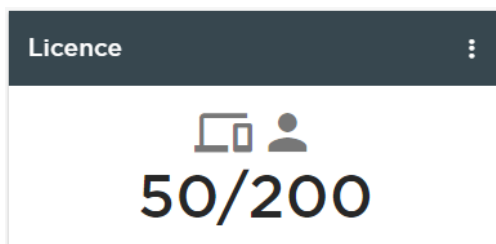
Refer to the **Licence** tile on the administrator's **Dashboard** for the current count of licensed devices and Attendance users. Upon the initial installation of the **2N® Access Commander**, a Trial licence (see below for details) will be available for you to configure one device and monitor Attendance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

<b>91379040</b>	<b>2N® Access Commander – licence for +5 devices (5-device licence package)*</b>
<b>91379041</b>	<b>2N® Access Commander – licence for +25 users (25-user licence package)** – for employees' Attendance Monitoring only</b>
<b>91379042</b>	<b>2N® Access Commander – Integration Licence (LDAP + CSV synchronisation licence package)</b>

### **Note**

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

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



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

### **Current Licences**

The section displays the count of required and owned device and user attendance management licences (in the required / owned format). Including the last licence adding date. Every licence addition rewrites the original one. Licences are not added up.

### Active license

Licensed devices S/N: 54-1105-0190

Count of available Attendance Monitoring licenses: 23 (of the total count 25)

Count of available device licenses: 0 (of the total count 5)

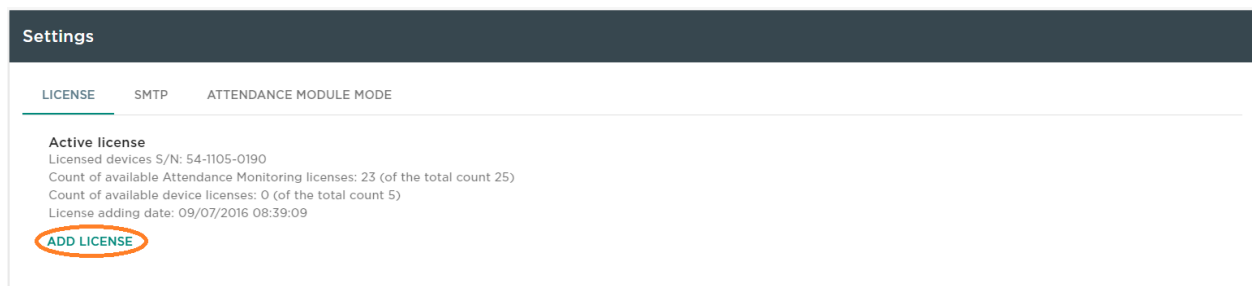
License adding date: 09/07/2016 08:39:09

### Licence Device S/N for Licence Generation

One of the connected devices (Helios IP, Access Unit, etc.) is used for licence generation. Send the serial number to your distributor. A licence will be generated and remain valid as long as the licence device is connected (the device is used as a hardware key). When the licence device is disconnected, a protective period will start running to keep the Access Commander active. When the protective period expires, all the devices will become inactive and a new licence will have to be generated.

### Licence Adding

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



### Trial Licence

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

- 1 device
- 1 attendance user
- unlimited count of system users

### Licence Expiration

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

**Active licence**

S/N of licensed device: 54-1105-0190

Count of available Attendance Monitoring licences: 24 (of the total count 25)

Count of available device licences: 0 (of the total count 5)

Licence adding date: 10/31/2016 13:33:47

Expiration date: 11/11/2016 09:20:19

**ADD LICENCE**

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

## Virtual System Setup

### Note

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

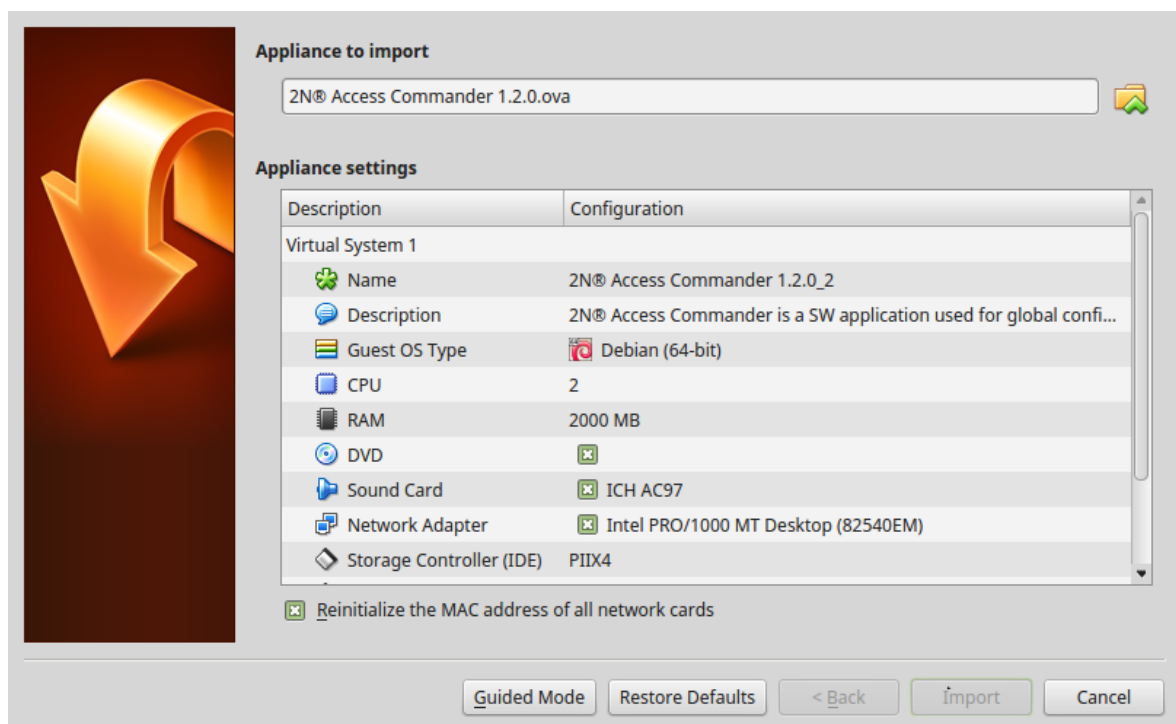
### VirtualBox

### 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**
  - a. version from <https://www.virtualbox.org/wiki/Downloads>, preferably including the **VirtualBox Extension Pack**
2. Download the image from the [official 2N website](#).
3. In VirtualBox go to File → Import appliance...

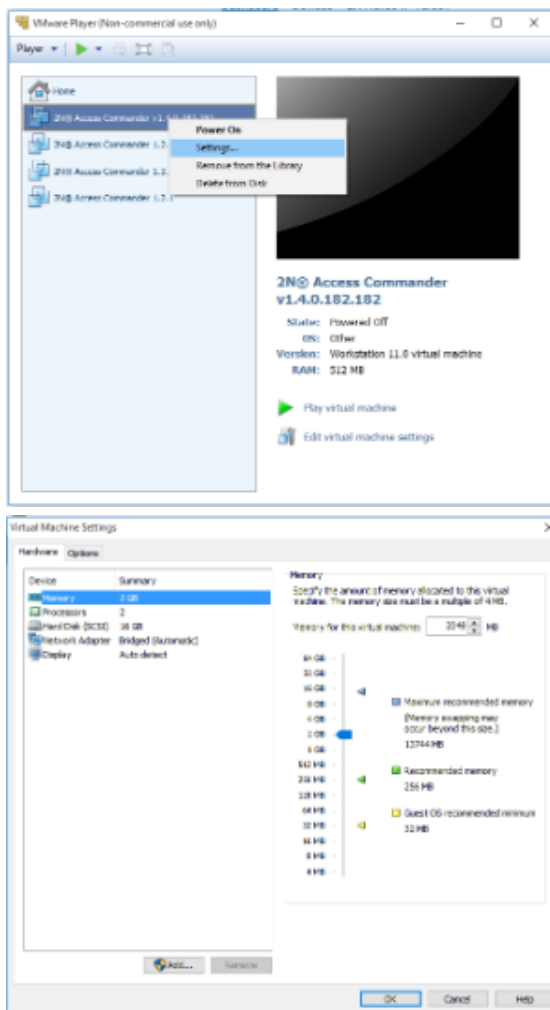


- a. Edit the name.
- b. Check the CPU setting (2 at least).
- c. Check the RAM setting (2048 MB at least).
- d. Check whether the correct network adapter is selected.

4. Confirm the Licence Terms and Conditions in the next step.

## VMware Player

1. Download the image from the [official 2N website](#).
2. In VMware Player File → Open... select the path to the OVA file.
3. As needed, rename and click Import.
4. After importing check the Settings.



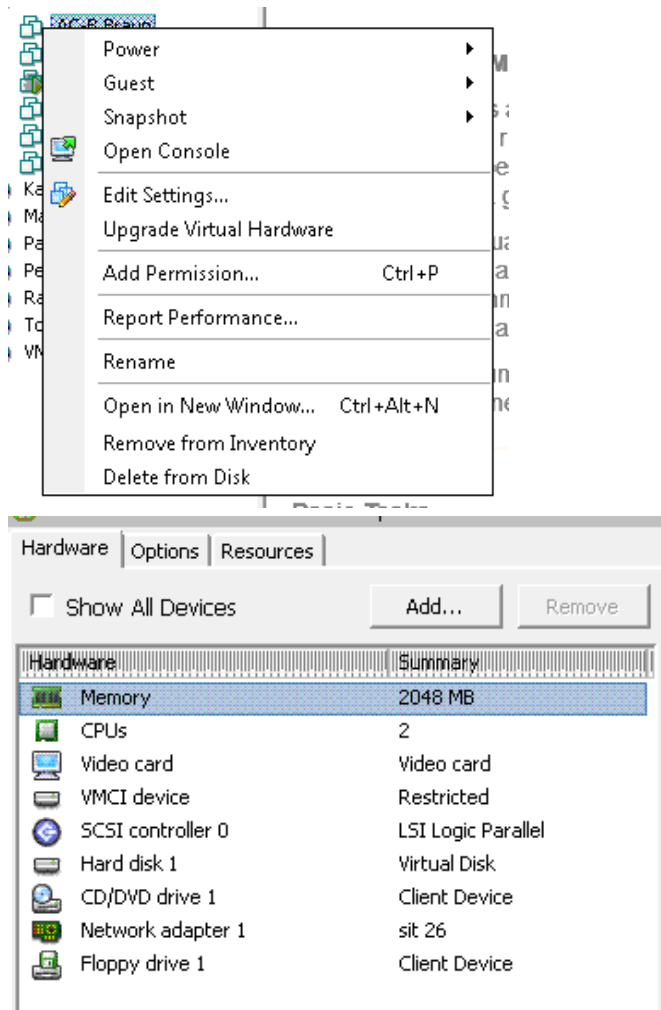
5. Check the settings
  - a. Check the CPU setting (2 at least).
  - b. Check the RAM setting (2048 MB at least).
  - c. Check whether the correct network adapter is selected.

## VMware vSphere

### Warning

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

1. Download the image from the [official 2N website](#).
2. Follow the wizard instructions in VMware vSphere File → Deploy OVF Template...
3. Check the Edit Settings...



- a. Edit the name (Options)
- b. Check the CPU setting (2 at least).
- c. Check the RAM setting (2048 MB at least).
- d. Check whether the correct network adapter is selected.



## Adding Users to Device

The users are added to the device during synchronisation depending on their relations to the device:

1. The user should have access to the device, i.e. is assigned to the group that is tied by the access rule with the zone that the device is assigned to.
2. The user is assigned to a device button.
3. The user is assigned to the quick dial list for the given device.
4. The user is a deputy in the case of inaccessibility of a user mentioned in item 2 or 3 above.
5. The user is displayed.

The above mentioned rules yield variable sets of users, which can be combined into a final user list to be added to the device during synchronisation.

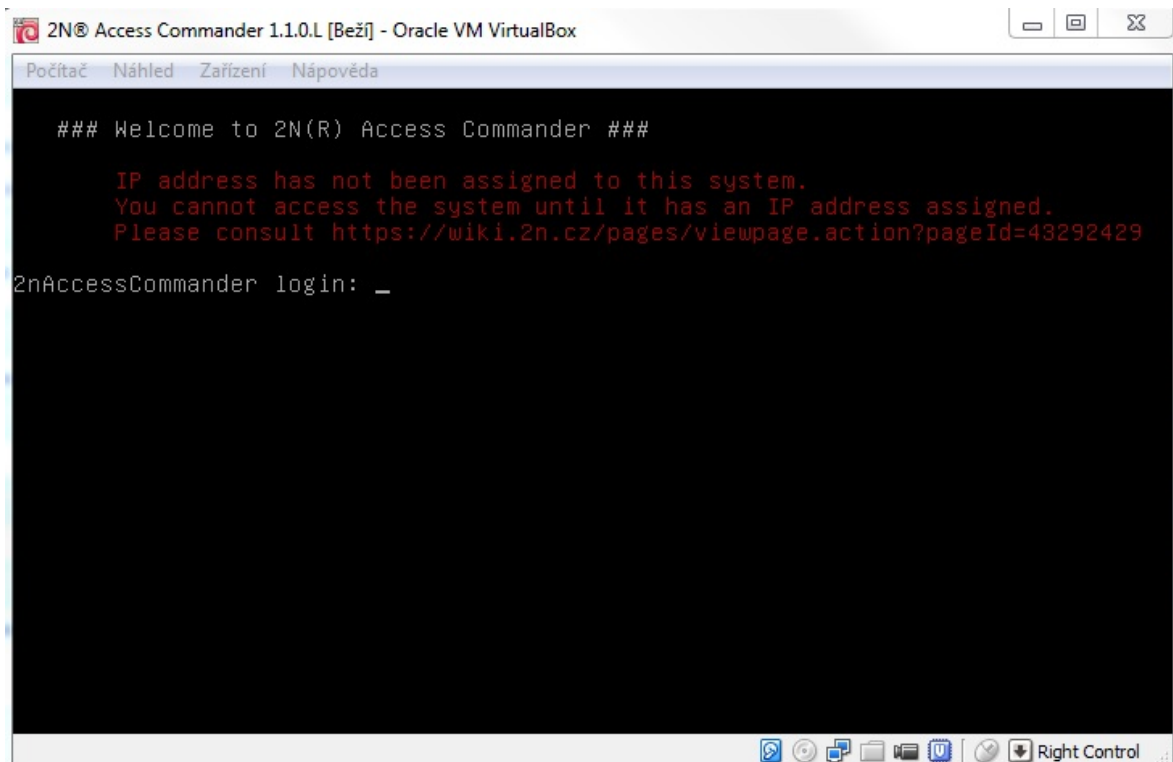
As a rule, the users are added to the device including their card IDs and switch codes. In addition to the card ID and switch code, the time profile assigned to the access rule is added too. If a user is assigned to multiple groups with different access rules and different time conditions, its card ID (switch code) is added to the device with more time profiles (mask used).

Phone numbers are loaded instead of card IDs and switch codes for users from rules 2, 3, 4 and 5.

## How to Set Static IP Address

**2N® Access Commander** (Linux based) is configured to obtain the IP address from the DHCP server by default. In case you have no DHCP server in your network or wish to assign the static IP address to the virtual server, please follow the steps described below.

1. Run the virtual server with **2N® Access Commander** and open the console. You should see the following message:



```
2N® Access Commander 1.1.0.L [Beží] - Oracle VM VirtualBox
Počítač  Náhled  Zařízení  Nápověda

### Welcome to 2N(R) Access Commander ###

IP address has not been assigned to this system.
You cannot access the system until it has an IP address assigned.
Please consult https://wiki.2n.cz/pages/viewpage.action?pageId=43292429

2nAccessCommander login: _
```

**Note**

- In case the IP address has been assigned to **2N® Access Commander** and you want to access it remotely, you can use **SSH connection**. Any SSH client will work, we recommend you to use **putty**.

2. Sign in with the following credentials:
  - login name: **root**
  - password: **2n**
3. Edit **/etc/network/interfaces** using a text editor, for example "**nano**" or "**mcedit**"
  - To run the text editor enter one of the commands below:
  - **mcedit /etc/network/interfaces**
  - or
  - **nano /etc/network/interfaces**

The screenshot shows a terminal window titled "2N® Access Commander 1.1.0.L [Beží] - Oracle VM VirtualBox". The terminal output is as follows:

```
Počítač  Náhled  Zařízení  Nápověda

2nAccessCommander login: root
Password:
Last login: Thu Jul  2 08:52:45 CEST 2015 on tty1
Linux 2nAccessCommander 3.2.0-4-amd64 #1 SMP Debian 3.2.68-1+deb7u1 x86_64
#-----#
| Access Commander v1.1.0 |
| https://wiki.2n.cz/x/xB6qAg |
#-----#

root@2nAccessCommander:~# nano /etc/network/interfaces _
```

4. Search for a line containing "**iface eth0 inet dhcp**" and change it to (see the figure below):
  - **iface eth0 inet static**
    - **address 192.168.0.10** – IP address
    - **netmask 255.255.255.0** – subnet mask
    - **gateway 192.168.0.1** – default gateway

```

GNU nano 2.2.6      Soubor: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug eth0
iface eth0 inet dhcp
type: address 192.168.0.10
netmask 255.255.255.0
gateway 192.168.0.1

^G Získat náp^O Uložit      ^R Otevřít so^V Předchozí ^K Vyjmout te^C Poloha ukazo
^X Ukončit   ^J Zarovnat  ^W Kde je   ^V Další stra^U Zrušit vyj^T Pravopis

```

5. Save the changes:
  - **mcedit** – press **F10**
  - **nano** – press "**ctrl+x**" and then "**y**" to confirm
6. Add DNS servers to **/etc/resolv.conf** using a text editor:
  - Enter one of the commands below:
    - **mcedit /etc/resolv.conf** or
    - **nano /etc/resolv.conf**
7. Add the following lines to the file:
  - **nameserver 8.8.8.8** – primary DNS server
  - **nameserver 8.8.4.4** – secondary DNS server
8. Save the changes:
  - **mcedit** – press **F10**
  - **nano** – press "**ctrl+x**" and then "**y**" to confirm
9. Apply the changes either by restarting the virtual server or the networking service.
  - Use one of the commands below:
    - **reboot** – restart the virtual server or
    - **service networking restart** – restart just the networking service

**Note**

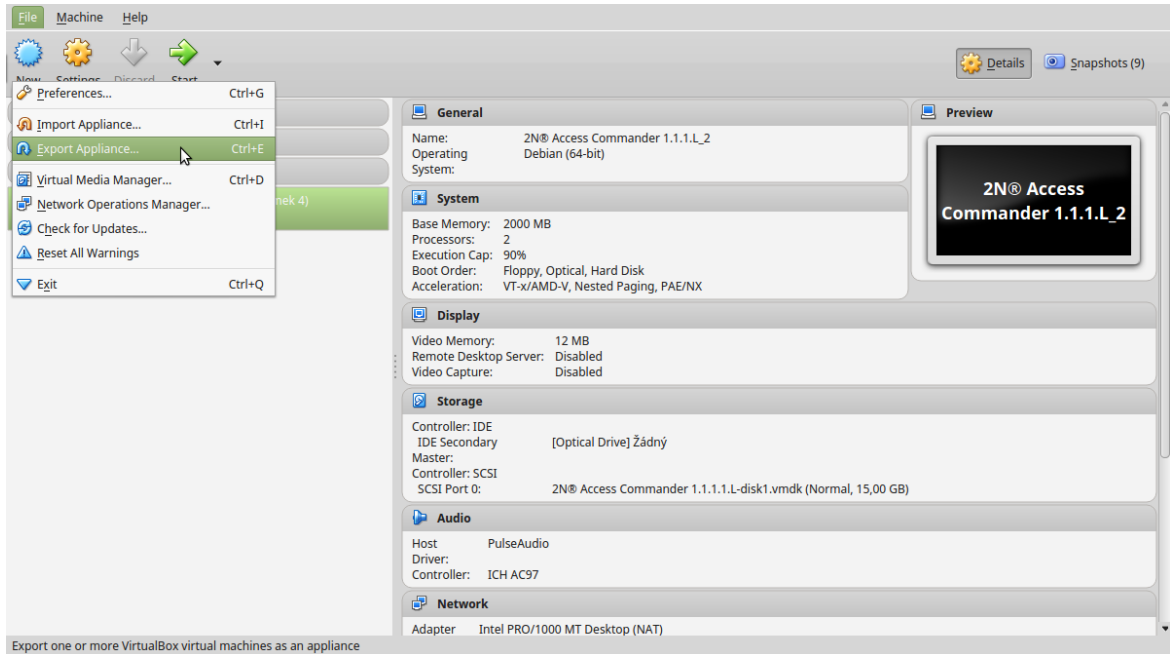
- If you are connected via SSH, you will be disconnected at this point.

Now that all the steps above have been taken, your **2N® Access Commander** is configured successfully to use the static IP address.

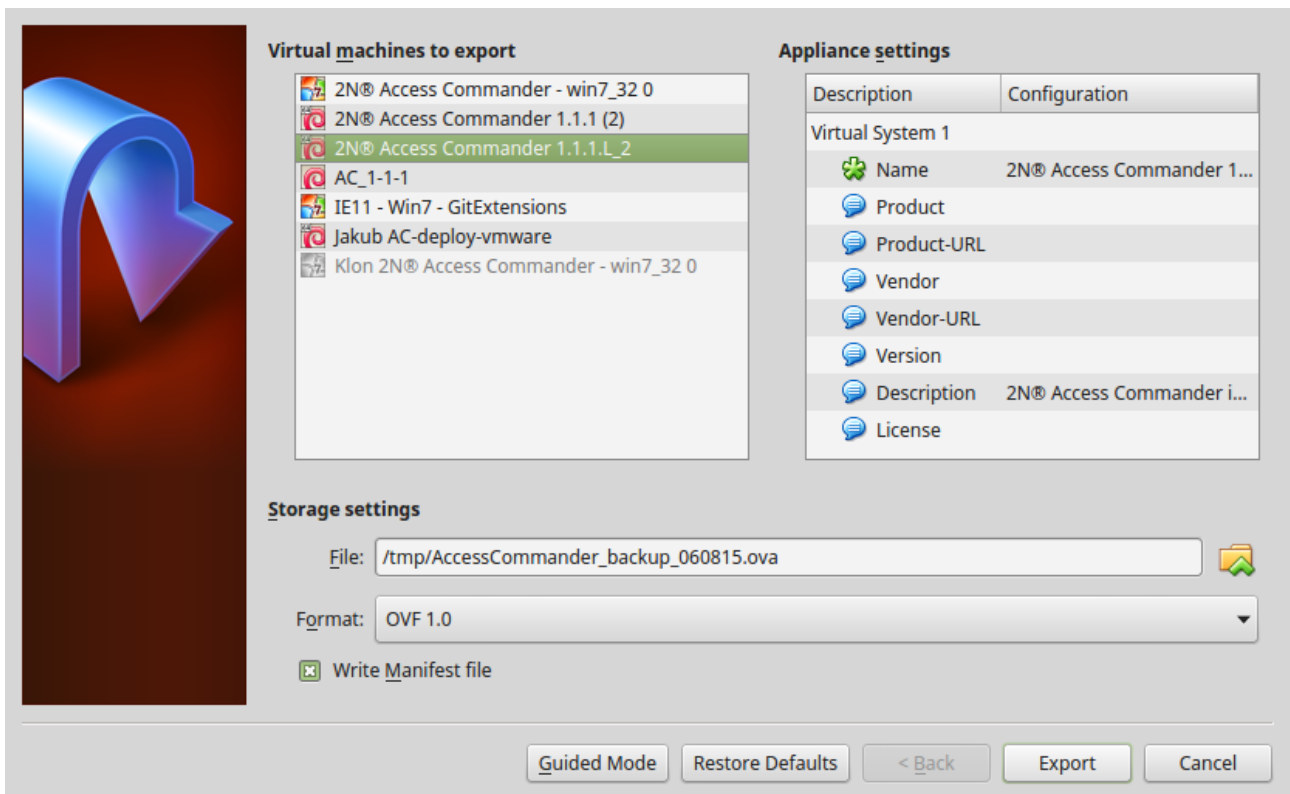
## Back-Up - VirtualBox (AC)

### Virtual Machine Back-Up to File (Export to OVA)

- Keep the virtual machine off.
- Go to File → Export appliance...



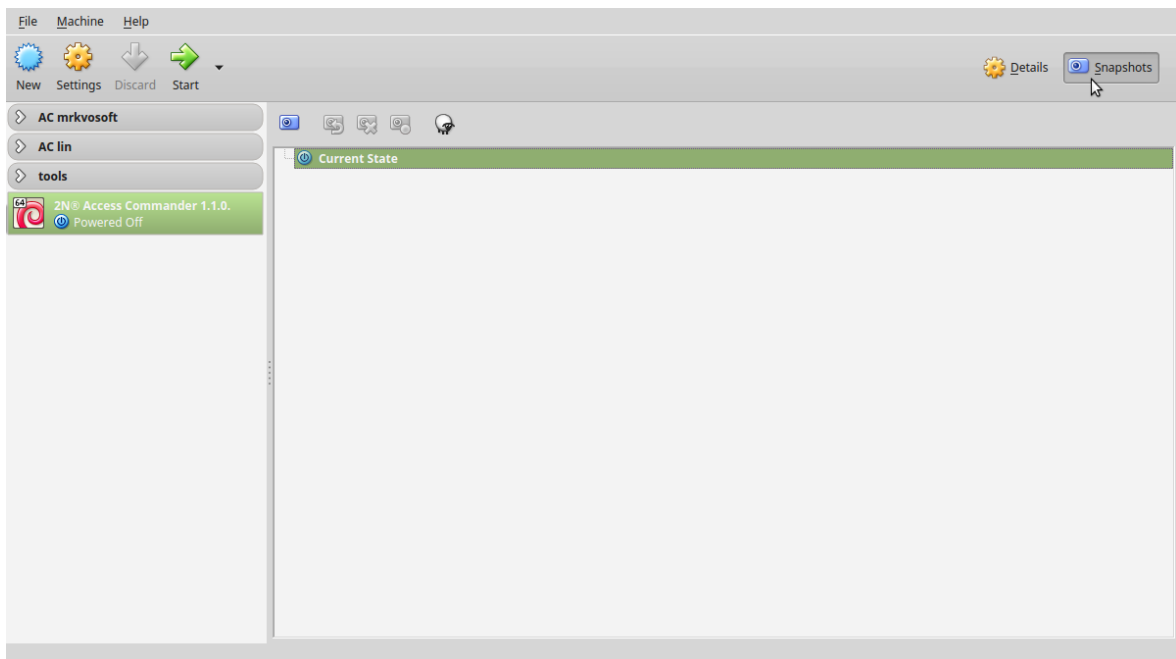
- Select the virtual machine, set the export path and select the Manifest → Export storage.



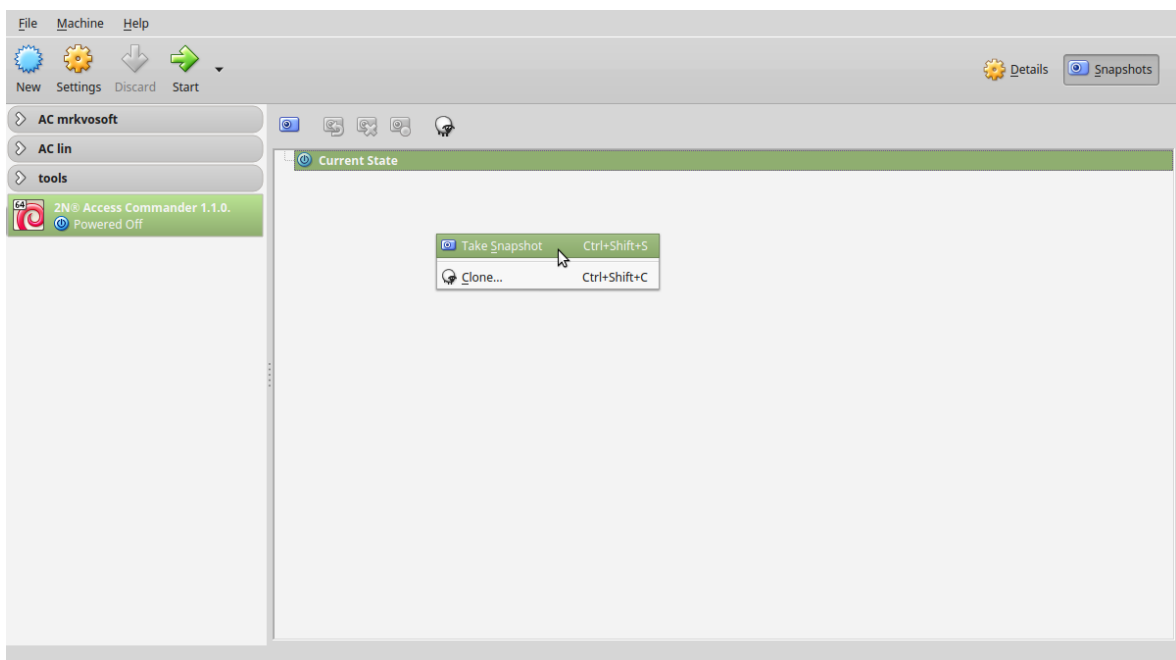
The exported file can be easily transferred and imported (refer to the AC setup) via any machine \*(see the minimum virtual machine requirements) to the VirtualBox application (or another virtualisation tool if the file is converted for the given application).

### **Application / Virtual Machine Snapshot (within VirtualBox only)**

- With the virtual machine on/off.
- Switch to the Snapshots tab.

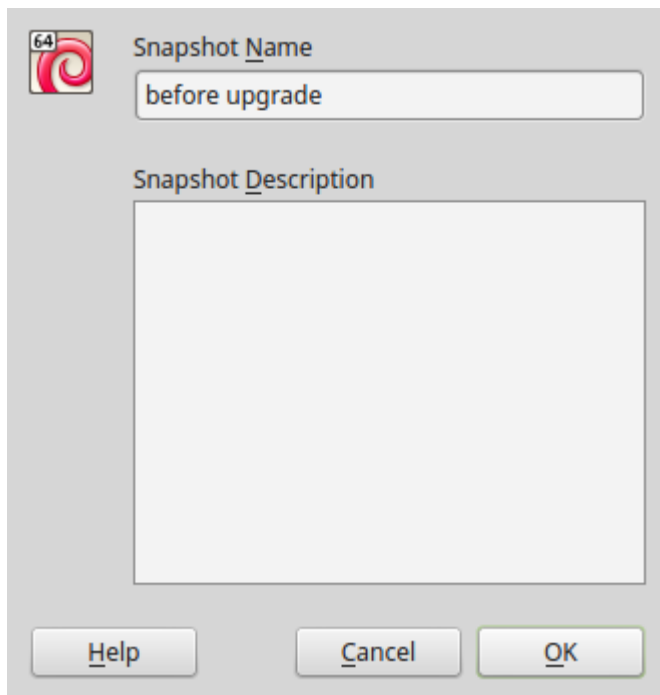


- Perform the Scan snapshot action.

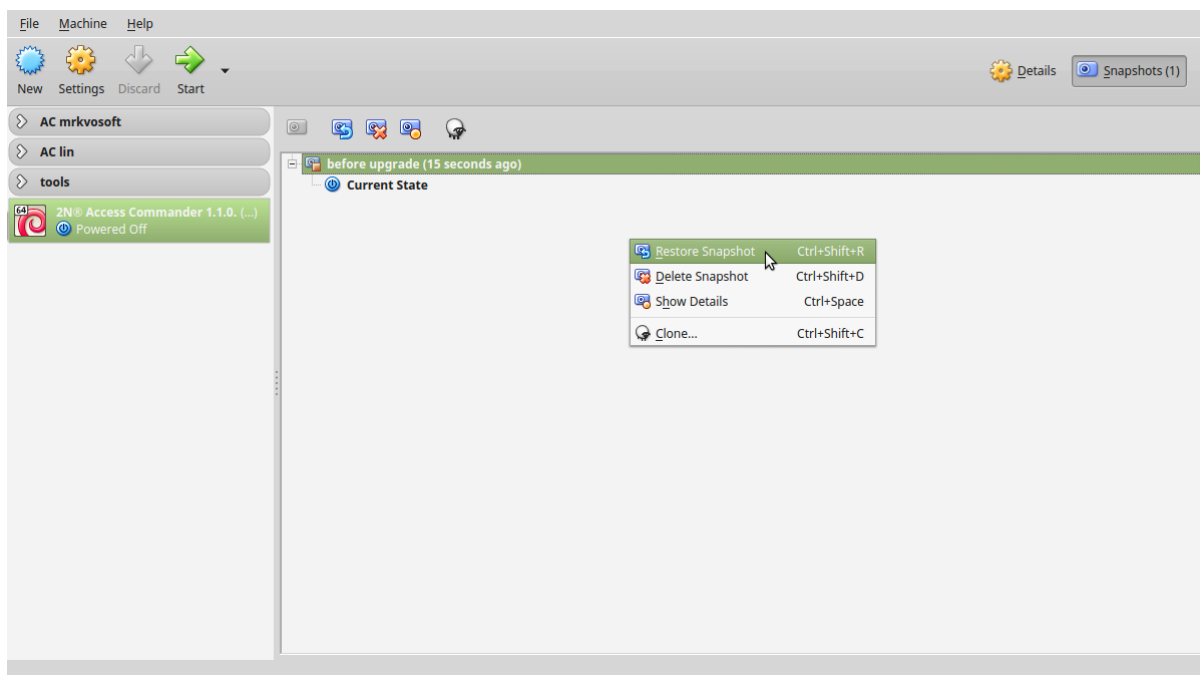


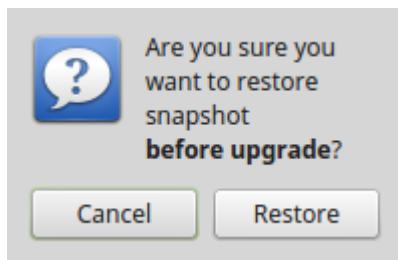
- Edit the name (plus reason for creation).





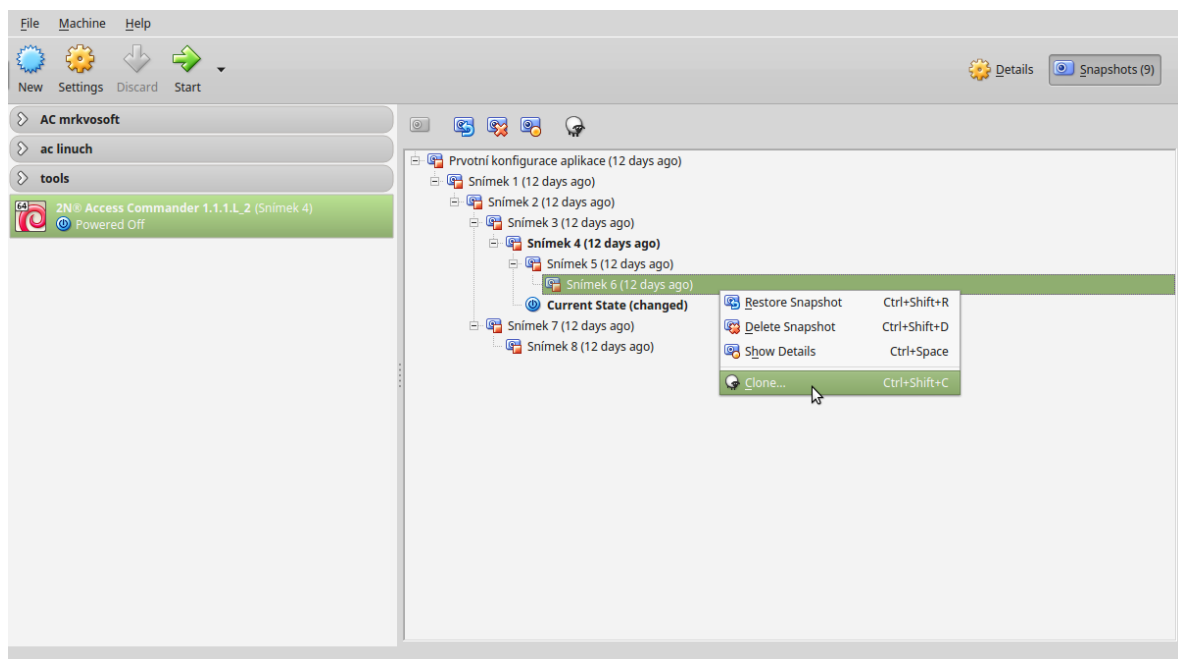
Thus, a renewal point is created that can be easily renewed.






### Application / Virtual Machine Cloning (within VirtualBox only)

- Execute the Cloning action on the created snapshot via the Snapshots tab.



- Choose the Full clone type and Current PC status in Snapshots → edit a new name and select Reinitialise MAC... (to make DHCP assign another IP address).



**New machine name**

**Clone type**

Full Clone

Linked Clone

**Snapshots**

Current machine state

Everything

Reinitialize the MAC address of all network cards

## Presence Module

The **Presence** module is an extending Attendance module used for displaying the list of employees currently present in a building. To make the module work, follow the attendance monitoring start steps specified in [How to Start Monitoring Staff Attendance?](#)

All the users to be monitored are subsequently displayed in the Presence module. Presence is detected from the downloaded card swipes through the end terminals (Helios IP, Access Units).

1. If the **last** user event of the day **is arrival** (IN event), the user is considered **present**.
2. When the user passes through a card reader with an unspecified direction, the current user zone will be changed. The same happens when the user passes through an **IN** card reader.
3. If the **last** event is **departure** (OUT event), the user is considered **absent**.
4. After midnight, the presence records are deleted in case any of the users forgot to mark its departure.

### Info

- The Presence module does not work properly if card readers without IN/OUT specification are used for Attendance monitoring within the company. Readers with IN/OUT specification can only be used.

## Automatic Synchronisation

Automatic synchronisation helps you update terminal equipment settings in the whole access system. It is started upon every change that is to be reflected in the terminal equipment configuration, i.e. that is related to user access rights, phone numbers, time rules or button settings. The synchronisation data check is executed every minute.

Synchronisation is only performed for the devices that are to be updated according to the access rule settings. Only those requests are queued that are initiated by the changes that affect terminal equipment. For example, a change of the user that is not assigned to any group does not start automatic synchronisation.

 **Note**

- The automatic synchronisation time (updating of all terminal equipment) depends on the count of devices to be synchronised and the amount of data to be loaded.

## Display Configuration

Go to the device detail to configure the device display. Select Display button configuration or Display configuration in the General menu.

**2N Helios IP Vario**  
Device state: Online

GENERAL NETWORK SETTINGS FEATURES DEVICE BACKUP

**Device name**  
2N Helios IP Vario

**Serial number**  
54-0889-0008

**Firmware version**  
2.15.0.24.3

**MAC address**  
7C-1E-B3-00-E7-D3

**Zone**  
Zone3

**Synchronisation state**  
Synchronisation completed successfully [30.03.2016 13:35:13]

**Backup state**  
No backup yet

[COPY SETTINGS](#) [SYNCHRONISE ALL DEVICES](#) [CONFIGURE DEVICE](#)

**Management**

[DISPLAY BUTTON CONFIGURATION](#) [DISPLAY CONFIGURATION](#) [KEYBOARD CONFIGURATION](#) [CONFIGURE QUICK DIAL BUTTONS](#)

[ADD](#) No items have been added yet.

## Name Tag Configuration

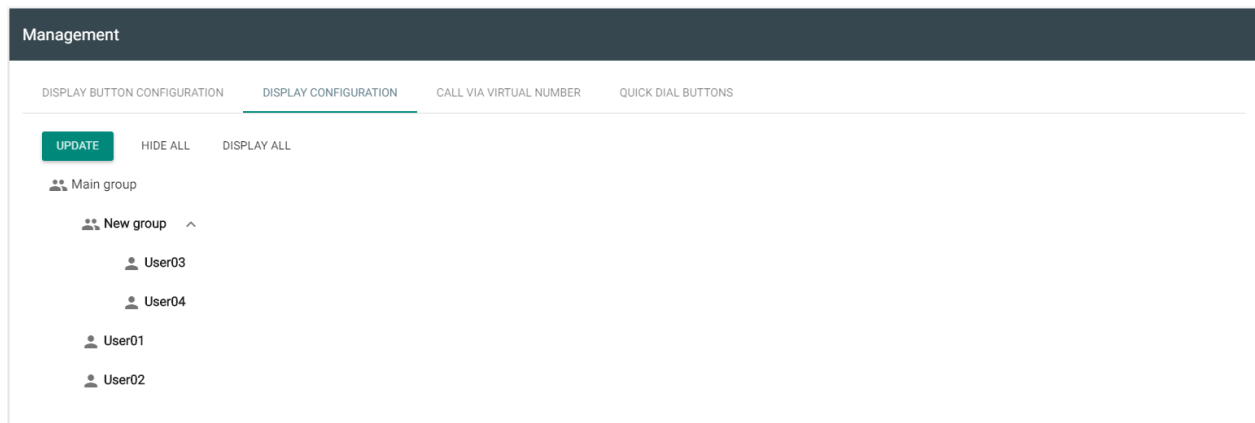
**Management**

[DISPLAY BUTTON CONFIGURATION](#) [DISPLAY CONFIGURATION](#) [KEYBOARD CONFIGURATION](#) [CONFIGURE QUICK DIAL BUTTONS](#)

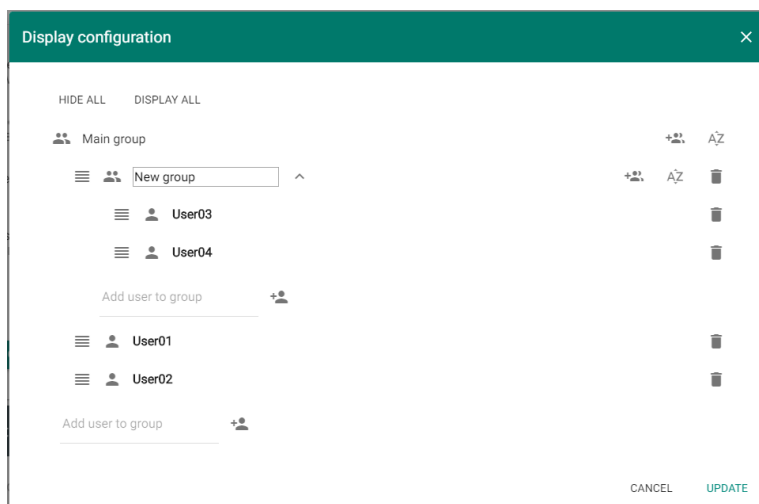
Button number	User	
#1	Empty	
#2	Empty	
#3	Empty	
#4	Empty	

Name tags are used for quick user dialling using a single button. Click Empty next to the button number and enter the user name to be added. Having added the users, click OK and start synchronisation.

## List Configuration



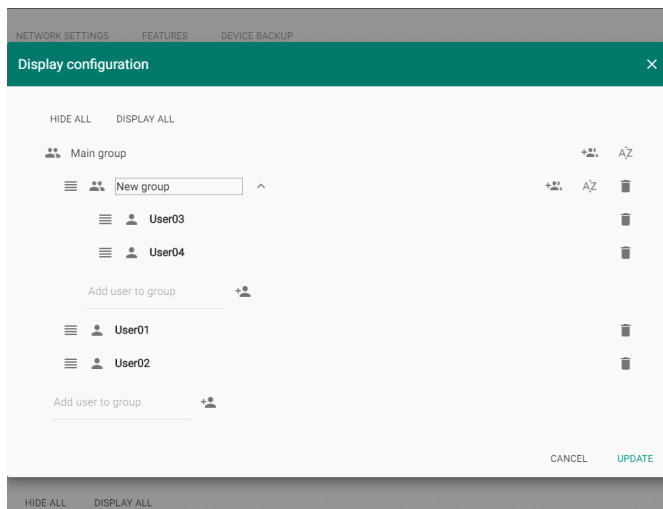
The list structure to be displayed is shown in this window. Click Update to configure the display.



The display structure is created using groups to which users are assigned:

- Click to add a group as a subgroup of a superior group.
- Add a user to a group via the input at the end of the group. You can choose multiple users at once. Remember to click for confirmation.
- All the elements are marked and can be moved via Drag&Drop to any list levels.
- Click to arrange the users alphabetically.
- Click to remove users/groups.

Adding users to the list:





## 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 state	Sip Proxy 1	Sip Proxy 2	Audio Test	Tamper Switch	Relay state	Operation time	
✓	2N Access Unit	Online	Unregistered	Unregistered	---	OK	🔒	2 days	👁️ ✎
✓	2N Helios IP Vario	Online	Unregistered	Registered	---	---	🔒	28 minutes	👁️ ✎
✓	2N Helios IP Verso	Online	Unregistered	Unregistered	---	OK	🔒	3 days	👁️ ✎
---	Access Unit	---	---	---	---	---	---	---	👁️ ✎
---	Force	---	---	---	---	---	---	---	👁️ ✎

CHANGE TABLE DISPLAY

Table items:

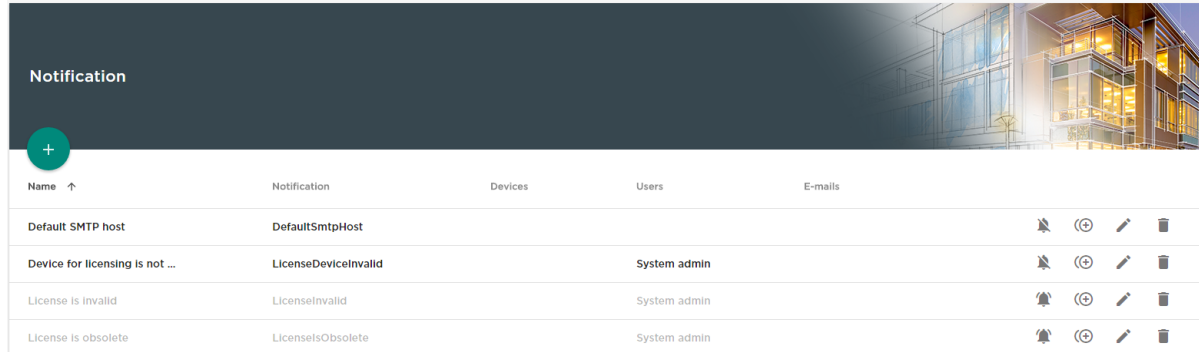
- Icon – display the device state (OK or not).
- Device name
- Device state
- SIP Proxy – display the SIP Proxy state on a device. If there is an error, mouse click the description to get a detail.
- Audio test – display the last audio test result.
- Tamper switch – if there is an error, mouse click 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
- Input state
- Operation 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.

## Notification

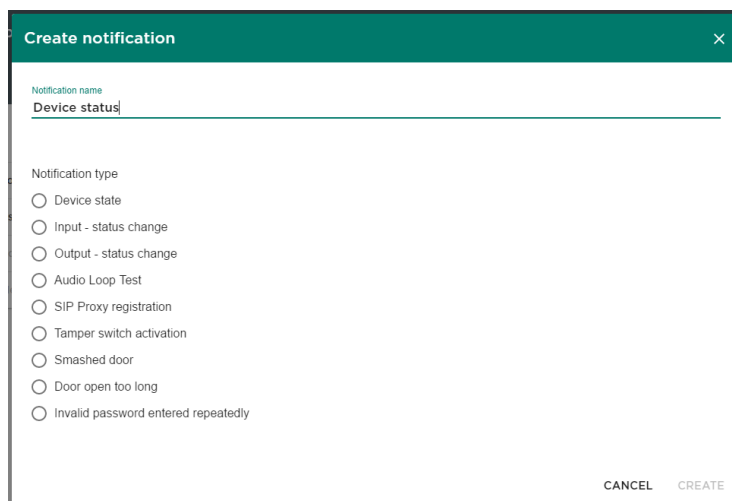
The notification module helps you monitor selected device properties via e-mails.



Name ↑	Notification	Devices	Users	E-mails
Default SMTP host	DefaultSmtphost			
Device for licensing is not ...	LicenseDeviceInvalid		System admin	
License is invalid	LicenseInvalid		System admin	
License is obsolete	LicensesObsolete		System admin	

Create a new notification:

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



Create notification
×

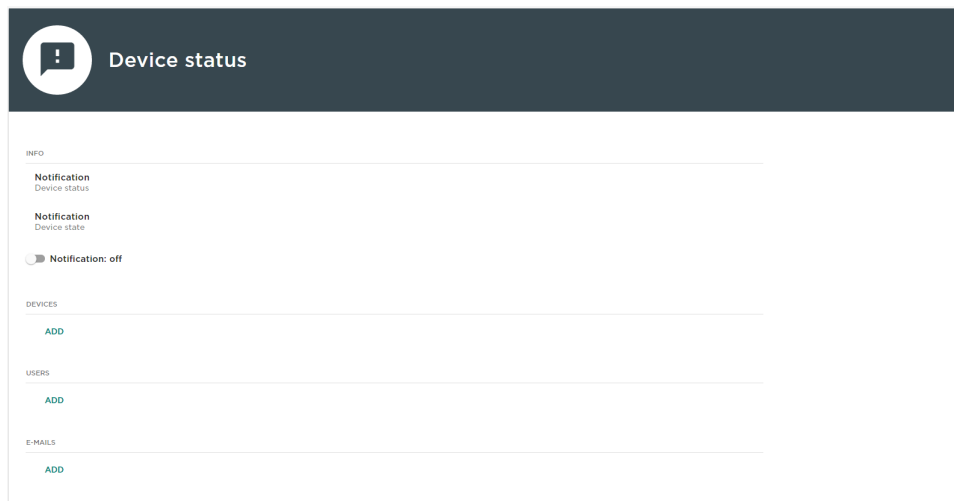
Notification name

Notification type

- Device state
- Input - status change
- Output - status change
- Audio Loop Test
- SIP Proxy registration
- Tamper switch activation
- Smashed door
- Door open too long
- Invalid password entered repeatedly

CANCEL CREATE

4. A new page will be created for:
  - a. notification activation,
  - b. device adding for monitoring,
  - c. user adding for e-mail sending,
  - d. e-mail adding if non-existent in the system.



**Note**

Make sure that SMTP is set correctly to make notifications work properly.

SMTP setting:

By default, SMTP is set to [smtp.2nac.cz](mailto:smtp.2nac.cz). We recommend you to use your own SMTP server for common use. Find the SMTP settings in the system settings.

LICENCE   SMTP   ATTENDANCE MODULE MODE   BLUETOOTH   SYNCHRONISATION

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

SMTP on

Server address \*       User name \*

Port \*       Password \*

SSL off

Default sender address \*

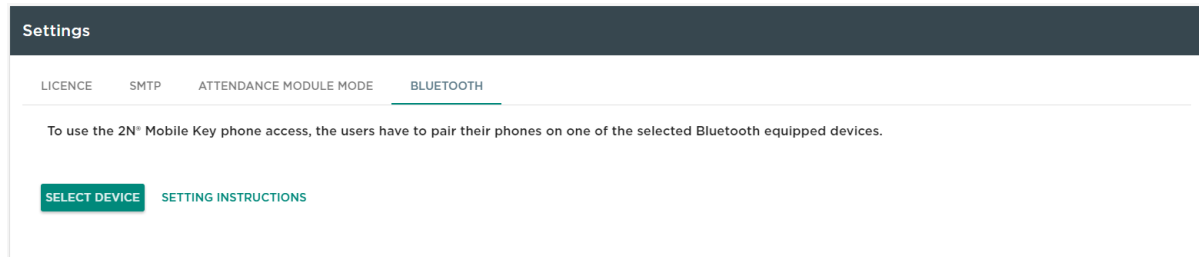
Test e-mail \*

  [SET DEFAULT VALUE](#)

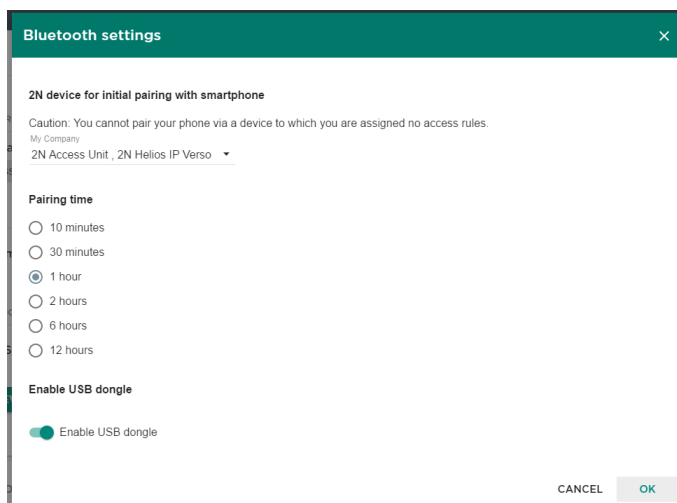
- SMTP switch – enable/disable SMTP
- SMTP server address – enter your SMTP server address.

- Port – port on which SMTP is active.
- SSL switch – change the port number after SSL activation.
- Default sender – add the e-mail sender's address.
- User name – enter the SMTP server login name.
- Password – enter the SMTP server login password.
- Test e-mail – add the destination address for the test e-mail.
- Send test e-mail – send the test e-mail to the address set above.
- Set default value – set the SMTP default values.

## Bluetooth Configuration



Make sure that one device at least equipped with a Bluetooth module is added to the **2N® Access Commander** before configuring Bluetooth. And also make sure that the device is added to the zone that is assigned to the user's company. Click Configure Bluetooth to display the pairing device and time setting window to the administrator.



Make sure that the device is configured for each company. If a device is assigned to a zone shared by multiple companies, you can select one device for more companies than one. The pairing time setting is valid from the moment when you click Generate on the user and the PIN gets displayed. Having configured the device and pairing time, click Change to move to the User list for user selection. Having selected a user, go to the Accesses tab.

PHONE

---

The user enters the pairing code to the 2N® Mobile Key application near the primary pairing device.

Pairing code

**GENERATE**

Pairing time

10 minutes

Primary pairing device

2N Helios IP Verso

Select one of the pairing options in the user detail: dongle or device. Make sure that dongle is connected and **2N® Helios IP USB driver** 1.2.2 is installed for the dongle option ([download](#)). Having selected dongle, just click Start pairing and enter the pairing PIN to your **2N® Mobile Key** equipped smartphone.

**Note**

To generate the pairing PIN successfully, make sure that the user is in the group that is added to the access rule with the zone that the device is assigned to.

When you click Generate, the PIN for primary pairing will get displayed. A time is set for the user to get to the device and enter its PIN. If the user fails to do so within the timeout, the administrator shall generate a new code. Refer to the user phone ID detail to see if pairing was successful.

PHONE

---

**Identification number**

e7ea641d005248b0a0d1b5ecf0567086

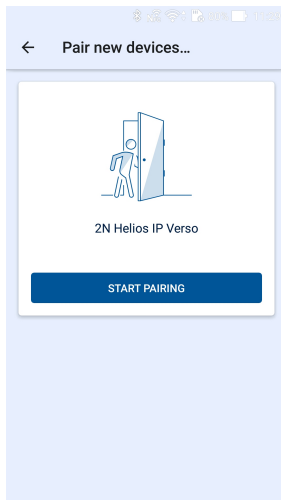
**PAIR AGAIN****DELETE**

After pairing, user pairing can be restarted or the Id can be deleted to remove the user phone access.

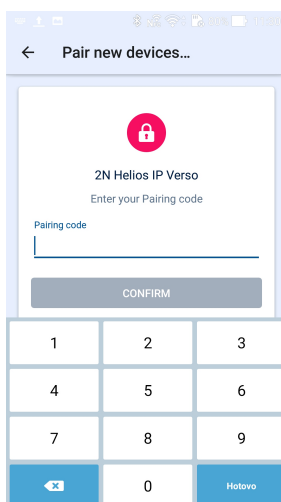
## Pairing via Mobile Application

Having started pairing via **2N® Access Commander**, enter the generated PIN in the mobile application.

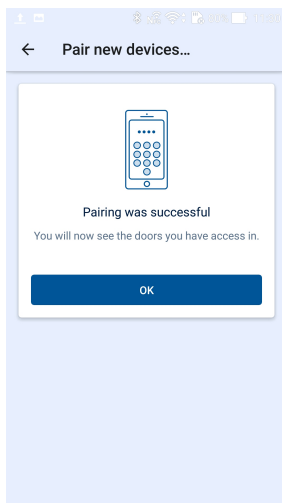
1. The devices to be paired are displayed in the application.



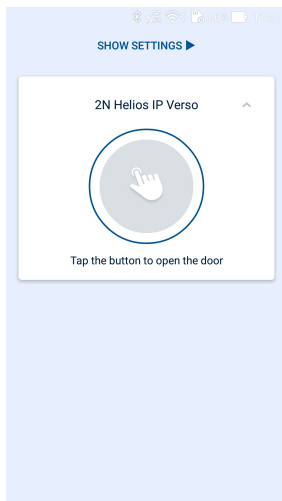
2. Having clicked START PAIRING you are invited to enter the PIN generated in **2N® Access Commander**.



3. If you enter the PIN successfully, information on the pairing result is displayed.



4. You can open a door using the device now.



Store links:





## LDAP

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

The screenshot shows the LDAP configuration page with the following details:

- Navigation:** ZONES, DATA IMPORT, LDAP (selected)
- SYNCHRONISATION:**
  - Scheduled synchronisation time: 00:00:00
  - Last synchronisation state: Synchronisation failed [01.01.0001 02:00:00]
  - SYNCHRONISE button
- SERVER SETTINGS:**
  - Server name: Empty
  - Port: 389
  - Login name: Empty
  - Password: \*\*\*
  - Use SSL:
- LDAP SCHEMA:**
  - Base DN: Empty
- ADVANCED SETTINGS:**
  - Nested search:
- DELETE CONFIGURATION** link

- Synchronisation
  - a. Periodical synchronisation time
    - Set the time when the **2N® Access Commander** shall make a query to the LDAP server concerning user changes.
  - b. Last synchronisation status
    - Information on the last synchronisation: whether it ended up with an error message or whether it ran successfully including the time when the event occurred.
  - c. Synchronisation button
    - Click the button to start synchronisation immediately. Thus, the administrator does not have to wait for periodical synchronisation.
- Server settings
  - a. Server name
    - In case DNS is set correctly, enter the server name („**WIN-9ABEB4AUOHD**“).
    - If DNS is not set, enter the IP address of the server where the LDAP service is running into the server name.
  - b. Port
    - By default, the LDAP port is 389 (without SSL). If you want to use an encrypted connection in your company, enter port 636. Make sure that the SSL support is on the LDAP server side too.

- If the administrator sets a different port number, make sure that it is changed in the **2N® Access Commander** too.
- c. Login name
  - Login name of the user who has the appropriate rights for the root or the whole tree. The login name must be entered in the following format: **"administrator@domain.com"**.
- d. Password
  - The password of the specific user on the LDAP server.
- e. Use SSL
  - If SSL is disabled, it is unnecessary to rewrite the port number.
  - If SSL is enabled, it is necessary to change the port number to 636.
- f. Delete configuration button
  - Click the Delete configuration button to delete the parameter settings without deleting the previously uploaded users.
- LDAP schema
  - a. Base DN
    - Base DN is the root point from which the directory search begins. It can be a suffix or directory root, for example: **"CN=administrator,CN=users,DC=domain,DC=com"**
- Advanced settings
  - a. Nested search
    - If nested search is used, the whole tree is searched instead of a root.

**ⓘ Note**

Remember to purchase and upload a licence to access the LDAP tab on the company.

 **Warning**

Users are only imported via LDAP. Deleting a user in LDAP does not delete the same in **2N® Access Commander**.

 **Tip**

Refer to [www.ldap.com](http://www.ldap.com) for LDAP details.

## CAM Log

The CAM logs record snapshots of the preceding and following events. Suppose you set card tapping records. Then, whenever a card is applied, 5 snapshots before and 5 snapshots after the card is tapped are recorded in the CAM logs. The images are recorded in 1-second intervals and saved into a dedicated 1GB storage. When the storage is full, the oldest records will be deleted. The CAM logs are not deleted.

 **Note**

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



## CAM Log Creation

**Create CAM Log** [X]

CAM Log name \*

CAM log

Notification type

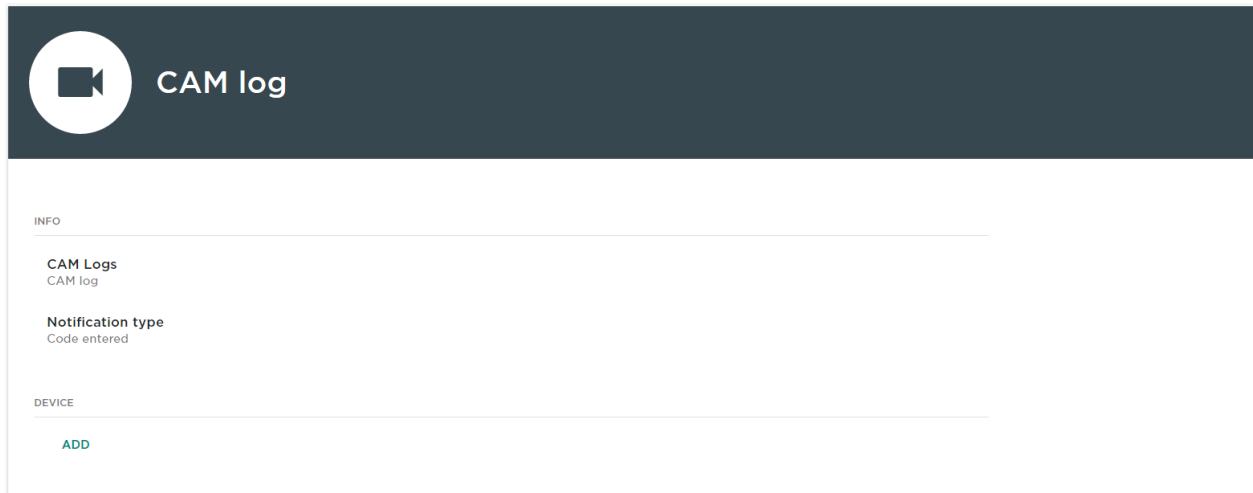
- Code entered
- Card applied
- Tamper switch activated
- Unauthorised door opening
- User accepted

CANCEL CREATE

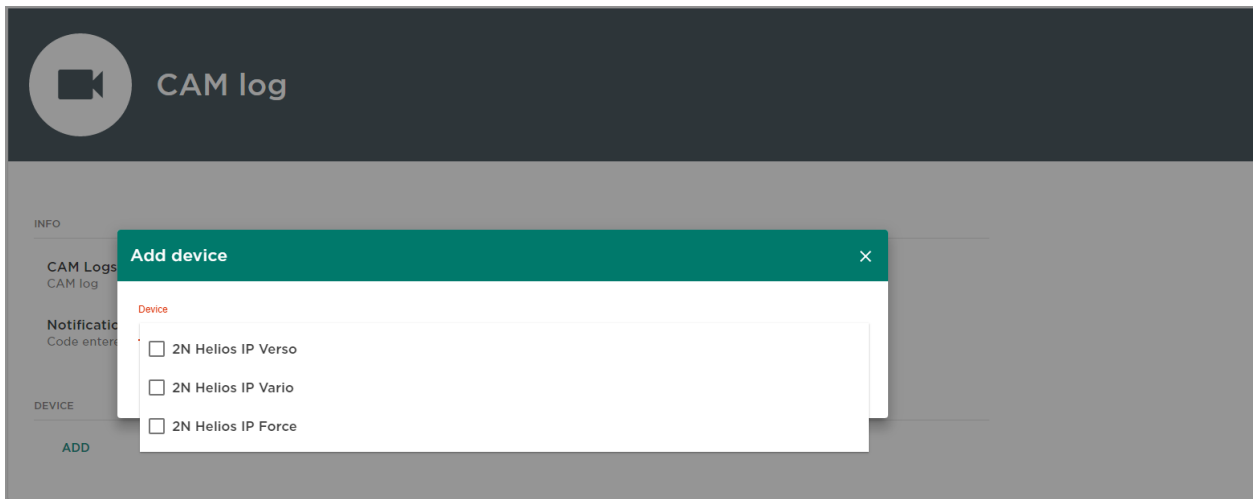
To create a CAM log, enter the CAM log name and select a notification.

- Code entered
  - A snapshot is taken whenever a code is entered via the keypad.
- Card tapped
  - A snapshot is taken whenever a card is applied even if the user is not authorised.
- Tamper switch activated
  - A snapshot is taken whenever the tamper switch is activated. Make sure that this is set in the 2N Helios IP configuration too. Refer to [Intercom Configuration](#).
- Unauthorised door opening
  - A snapshot is taken whenever an unauthorised door opening is detected. Make sure that this is set in the 2N Helios IP configuration too. Refer to [Intercom Configuration](#).
- User accepted
  - A snapshot is taken whenever the user authorises itself via Bluetooth.

Having entered the CAM log name and selected an event, click Create to get to the CAM log detail.



Here select the devices from which CAM logs shall be downloaded.



In addition to passage data, the CAM logs display an intercom snapshot display icon. No CAM logs are displayed for the intercoms that are not equipped with a camera.

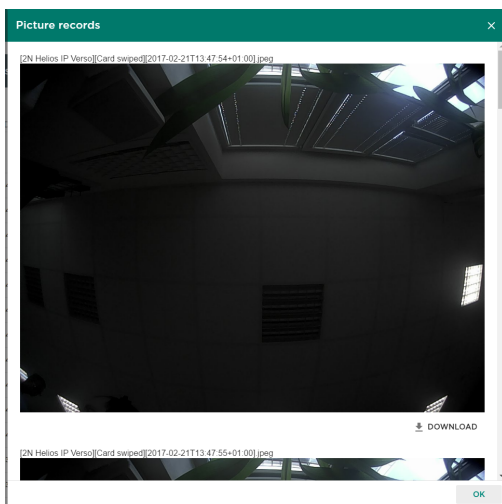
## CAM Log Viewing

Access logs

FROM: DD/MM/YY HH:MM TO: 21/02/2017 13:47 EVENT TYPE COMPANY DEVICE CARD ID: Q

Time ↓	Zone	Device	Event type	Event code	User	Description
21.2.2017 13:48:32	Zone4	2N Helios IP Force	Card swiped	50009038B2		Unauthorised
21.2.2017 13:48:30	Zone1	2N Helios IP Verso	Card swiped	490032F959	User05	Arrival
21.2.2017 13:48:23	Zone1	2N Helios IP Verso	Card swiped	490032F959	User05	Arrival
21.2.2017 13:48:20	Zone1	2N Helios IP Verso	Card swiped	50009038B2		Unauthorised
21.2.2017 13:48:14	Zone1	2N Helios IP Verso	Keypad entered	123456789		PIN code rejected
21.2.2017 13:48:10	Zone4	2N Helios IP Force	Card swiped	490032F959	User05	Direction unspecified
21.2.2017 13:48:08	Zone3	2N Helios IP Varlo	Card swiped	490032F959	User05	Direction unspecified
21.2.2017 13:47:59	Zone1	2N Helios IP Verso	Card swiped	490032F959	User05	Arrival
21.2.2017 13:47:57	Zone1	2N Helios IP Verso	Card swiped	490032F959	User05	Arrival
21.2.2017 13:47:50	Zone1	2N Helios IP Verso	Keypad entered	2	User02	PIN code accepted
21.2.2017 13:47:49	Zone1	2N Helios IP Verso	Keypad entered	1	User01	PIN code accepted
21.2.2017 13:32:04		2N Helios IP Force	Card swiped	0C008IEICE		Direction unspecified
21.2.2017 13:31:58		2N Helios IP Force	Card swiped	0C008IEICE		Direction unspecified

Click the icon to display a new window with intercom images.



Every image header includes [device][event] and [time] information. The images are arranged from the oldest to the latest one. You can download each snapshot separately.

**Note**

The size of a downloaded image 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 values are set both in the intercom and **2N® Access Commander** server to make the CAM logs work properly.

## Visitor Cards

Visitor cards can be created in **2N® Access Commander**. The administrator adds some cards to the system and sets the necessary rights. The duly authorised user assigns the cards to visitors.

### The visitor card allows you to:

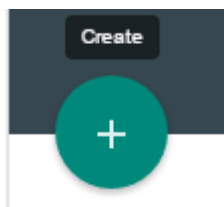
- grant visitors access to selected zones for a limited period of time
- assign access rights easily
- monitor visitors' access logs

### The visitor card does not allow you to:

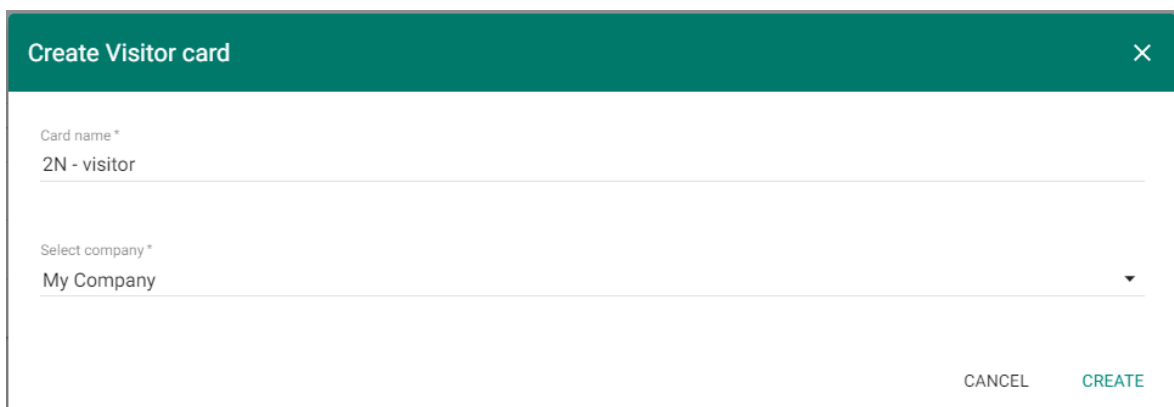
- monitor user attendance
- use BT or PIN for access
- support phone numbers

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

1. Click Create to add a card in Visitor cards.



2. Complete the visitor card name: 2N – visitor, e.g., and the company name.



Create Visitor card

Card name \*  
2N - visitor

Select company \*  
My Company

CANCEL CREATE

3. Complete the card ID (enter it manually or read it from the card reader) and assign the card to a group.

- Once added, the visitor card can be edited by clicking the field to be changed. The administrator can assign a user to the card on the Visitor tab. Users with the Access management right can also assign users as described below. Use the trash bin icon in the visitor card list to delete a visitor card.

#### Access management user settings (assign, edit and delete visitor cards):

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

Name ↑	Company	Visitor name	Purpose of visit	Validity
2N - Visitor	My Company			
2N - Visitor card #7	My Company			
Visitor 3rd floor	My Company			

- Click one of the table fields and set the visitor data: Name, Purpose of visit and From-To validity.

**Visitor settings** ✕

Name \*  
John Malack

---

Purpose of visit  
Sales Representative

---

**From:** **To:**

8/9/2017

Time \*  
13:28

8/9/2017

Time \*  
17:29

CANCEL
UPDATE

4. Save the settings to assign the visitor card to the set user. This user thus gets access to the zones assigned by the administrator for the period of time specified above.
5. Click the user field to display and edit the visitor access data. Click Delete visitor to delete the visitor data and assign the card to another visitor if necessary.

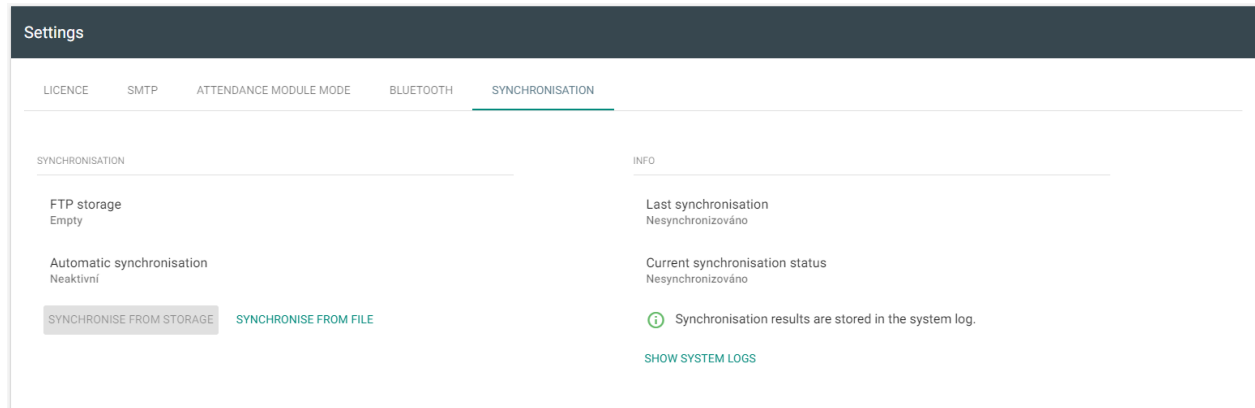
## Visitor History

Use the Access logs to display the history of visitor cards. The log includes the card name and visitor name as completed in the card detail.

Access logs							
FROM:  DD/MM/YY		HH:MM		TO:  DD/MM/YY		13:32	
<span>EVENT TYPE</span> <span>COMPANY</span> <span>DEVICE</span> <span>CARD ID:</span> <input style="width: 50px;" type="text"/>							
Time ↓	Zone	Device	Event type	Event code	User	Description	🗑️
09.08.2017 13:32:40	Zone1	2N Helios IP Verso Ondra Stül	Card swiped	5009015A7	John Malack (2N - Visitor)	Arrival	🗑️
09.08.2017 13:32:40	Zone1	2N Helios IP Verso Ondra Stül	Card swiped	5009015A7	John Malack (2N - Visitor)	Arrival	🗑️
09.08.2017 13:32:28	Zone1	2N Helios IP Verso Ondra Stül	Card swiped	5009015A7	John Malack (2N - Visitor)	Arrival	🗑️
09.08.2017 13:32:28	Zone1	2N Helios IP Verso Ondra Stül	Card swiped	5009015A7	John Malack (2N - Visitor)	Arrival	🗑️
09.08.2017 13:32:18	Zone1	2N Helios IP Verso Ondra Stül	Card swiped	5009015A7	John Malack (2N - Visitor)	Arrival	🗑️
09.08.2017 13:32:18	Zone1	2N Helios IP Verso Ondra Stül	Card swiped	5009015A7	John Malack (2N - Visitor)	Arrival	🗑️
09.08.2017 13:32:07	Zone1	2N Helios IP Verso Ondra Stül	Card swiped	5009015A7	John Malack (2N - Visitor)	Arrival	🗑️
09.08.2017 13:32:01	Zone1	2N Helios IP Verso Ondra Stül	Card swiped	5009015A7	John Malack (2N - Visitor)	Arrival	🗑️
09.08.2017 13:31:57	Zone1	2N Helios IP Verso Ondra Stül	Card swiped	5009015A7	John Malack (2N - Visitor)	Arrival	🗑️
09.08.2017 13:31:49	Zone1	2N Helios IP Verso Ondra Stül	Card swiped	5009015A7	John Malack (2N - Visitor)	Arrival	🗑️
09.08.2017 13:31:49	Zone1	2N Helios IP Verso Ondra Stül	Card swiped	5009015A7	John Malack (2N - Visitor)	Arrival	🗑️
09.08.2017 13:31:20	Zone1	2N Helios IP Verso Ondra Stül	Card swiped	5009015A7	John Malack (2N - Visitor)	Arrival	🗑️
09.08.2017 13:30:48	Zone1	2N Helios IP Verso Ondra Stül	Card swiped	5009015A7		Unauthorised	🗑️
09.08.2017 13:30:48	Zone1	2N Helios IP Verso Ondra Stül	Card swiped	5009015A7		Unauthorised	🗑️

## CSV Synchronisation

Synchronisation using a CSV file.



There are two CSV synchronisation options:

### 1. Synchronise from file:



- a. Create a CSV file as described below.
  - b. Select a file for synchronisation and click Synchronise.
- ### 2. Synchronise via storage:
- a. FTP storage connection setting

**FTP storage settings** X

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

User Name  
admin

Password  
.....

CANCEL UPDATE

- i. FTP server address – set the FTP server address: IP address or domain name. Set the address including the prefix ftp:// and synchronisation file name.
  - ii. User name – set the FTP server user name for access to the requested file.
  - iii. Password – enter the user password.
- b. Automatic synchronisation setting

**Automatic synchronisation settings** X

Allow automatic synchronisation

**From:**

8/9/2017

Time \*  
13:54

Synchronisation interval \*  
Once per day

CANCEL UPDATE

- i. Allow automatic synchronisation.
  - ii. From – set the synchronisation starting date and time.
  - iii. Synchronisation interval – set how often **2N® Access Commander** shall synchronise with the FTP storage: once an hour, once a day or once a week.
3. Information:
- a. Last synchronisation – display the last synchronisation date and time.
  - b. Current synchronisation state – display the last synchronisation result.

Sample CSV:

Be sure to keep the required CSV file structure: all the values are separated with a comma except for the group list, which is separated with a semi-colon. 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 – complete this unique user ID at all times.
- User Name – user name created in **2N® Access Commander**.
- Company – company name created in **2N® Access Commander** for which the user is created.
- User Mail – user email.
- Card Number – user card number.
- Switch Code – switch code, switch 1 code is always created.
- Phone Number 1 – position 1 phone number.
- Group Call – group call to the following phone number: True – group call activated, False – group call disabled.
- Phone Number 2 – position 2 phone number.
- Group Call – group call to the following phone number: True – group call activated, False – group call disabled.
- Phone Number 3 – position 3 phone number.
- Virtual Number – virtual user number.
- Groups – list of groups to which the user is to be added. All the groups are created in **2N® Access Commander**. The group list items are separated with a semi-colon.
- Is Deleted – the user is/is not deleted: True means that the user is created and its data is only updated upon synchronisation, False means that the user is deleted in the next synchronisation. When True is selected, the user is re-created.

Sample CSV file for download:



Synchronisation logs:

Details on each synchronisation are stored in system logs. The log includes basic information on synchronisation success/fail. Use the icon at the row end to download the file.

System logs		REFRESH			
FROM:	DD/MM/YY HH:MM	TO: 09/08/2017 13:56	EVENT TYPE	DEVICE	WARNING LEVEL
Selected CSV Synchronisation X Cancel all filters X					
Time	Description				
09.08.2017 13:56:50	Synchronization result: Created: 7, Deleted: 0, Skipped: 0, Successes: 14, Errors: 0				
09.08.2017 13:56:47	Synchronization result: Created: 7, Deleted: 0, Skipped: 0, Successes: 14, Errors: 0				
09.08.2017 13:56:43	Synchronization result: Created: 7, Deleted: 0, Skipped: 0, Successes: 14, Errors: 0				
09.08.2017 13:56:39	Synchronization result: Created: 7, Deleted: 0, Skipped: 0, Successes: 14, Errors: 0				
09.08.2017 13:56:21	Synchronization result: Created: 7, Deleted: 0, Skipped: 0, Successes: 14, Errors: 0				
09.08.2017 13:56:17	Synchronization result: Created: 7, Deleted: 0, Skipped: 0, Successes: 14, Errors: 0				
09.08.2017 13:56:14	Synchronization result: Created: 7, Deleted: 0, Skipped: 0, Successes: 14, Errors: 0				
09.08.2017 13:56:09	Synchronization result: Created: 7, Deleted: 0, Skipped: 0, Successes: 14, Errors: 0				
21.07.2017 10:24:42	Synchronization failed. Exception Message: Invalid URI: The format of the URI could not be determined.				
21.07.2017 10:24:40	Synchronization failed. Exception Message: Invalid URI: The format of the URI could not be determined.				
21.07.2017 10:24:39	Synchronization failed. Exception Message: Invalid URI: The format of the URI could not be determined.				
21.07.2017 10:24:28	Synchronization failed. Exception Message: Invalid URI: The format of the URI could not be determined.				

**Note**

CSV synchronisation is a licensed function. The tab remains hidden until licence No. **91379042, 2N® Access Commander – Integration Licence** is added.



## HTTP API

<https://wiki.2n.cz/acc/1.8/en/http-api>

(Open API documentation is only available to view online)

