Access Commander

Configuration Manual

Version: 1.7

www.2n.cz

The 2N TELEKOMUNIKACE a.s. is a Czech manufacturer and supplier of telecommunications equipment.

The product family developed by 2N TELEKOMUNIKACE a.s. includes GSM gateways, private branch exchanges (PBX), and door and lift communicators. 2N TELEKOMUNIKACE a.s. has been ranked among the Czech top companies for years and represented a symbol of stability and prosperity on the telecommunications market for almost two decades. At present, we export our products into over 120 countries worldwide and have exclusive distributors on all continents.

2N TELEKOMUNIKACE a.s. administers the FAQ database to help you quickly find information and to answer your questions about 2N products and services. On www.faq.2n.cz you can find information regarding products adjustment and instructions for optimum use and procedures „What to do if...".

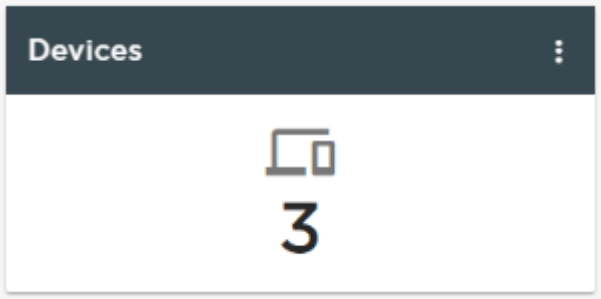
2N TELEKOMUNIKACE a.s. hereby declares that the 2N® product complies with all basic requirements and other relevant provisions of the 1999/5/EC directive. For the full wording of the Declaration of Conformity see the CD-ROM (if enclosed) or our website at www.2n.cz.

The 2N TELEKOMUNIKACE a.s. is the holder of the ISO 9001:2009 certificate. All development, production and distribution processes of the company are managed by this standard and guarantee a high quality, technical level and professional aspect of all our products.

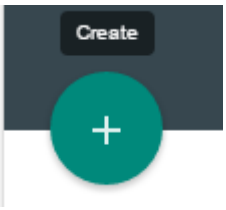
Content:

How to Add Device?

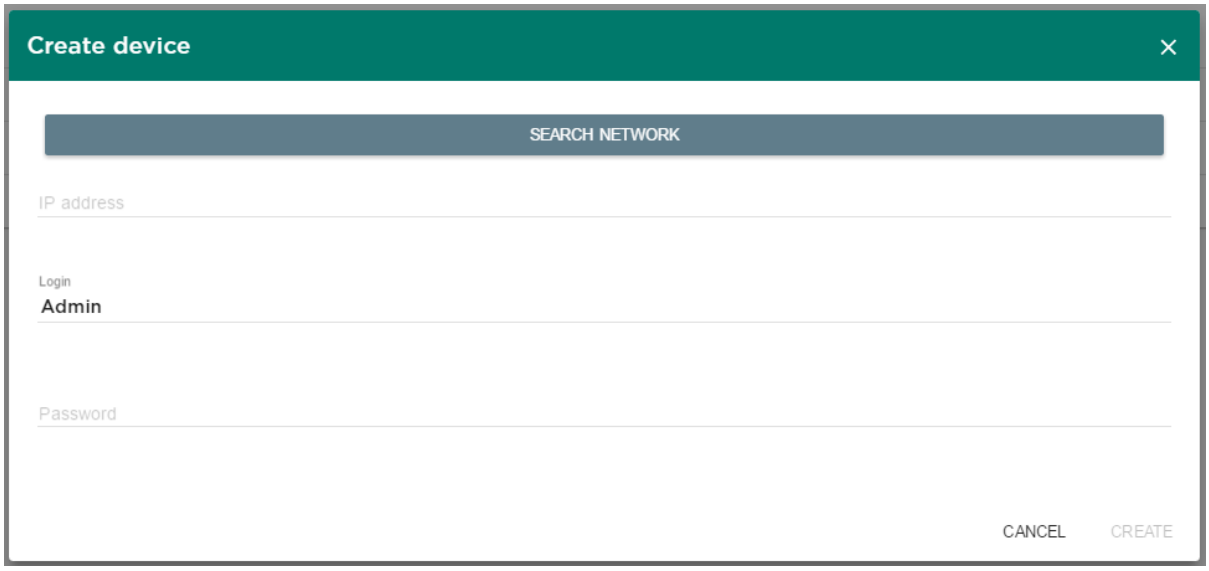
1. Select the **Device** card.



2. Select the **Device – Create** option.

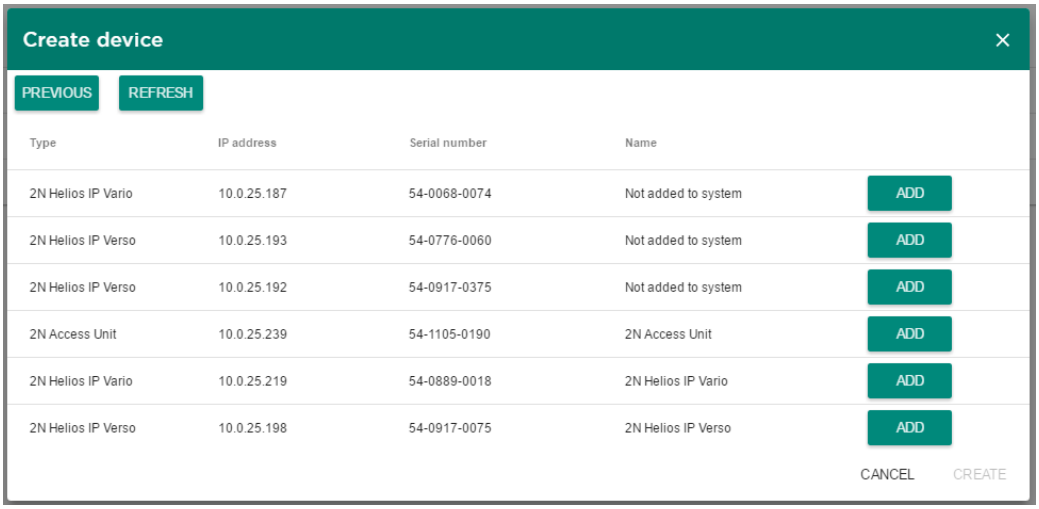


3. Enter **IP address + port** (if the port is other than 443, because the device is behind the NAT, e.g.) and access data



Or try to find the device in the network

And select



Device is behind the router

- 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”.

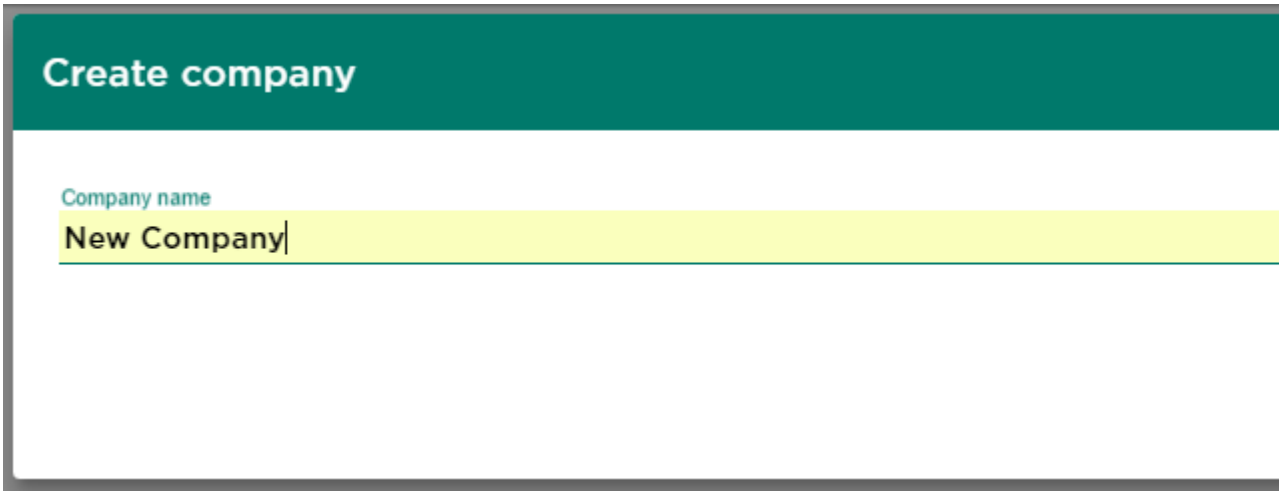
Companies

What Is a Company Used For?

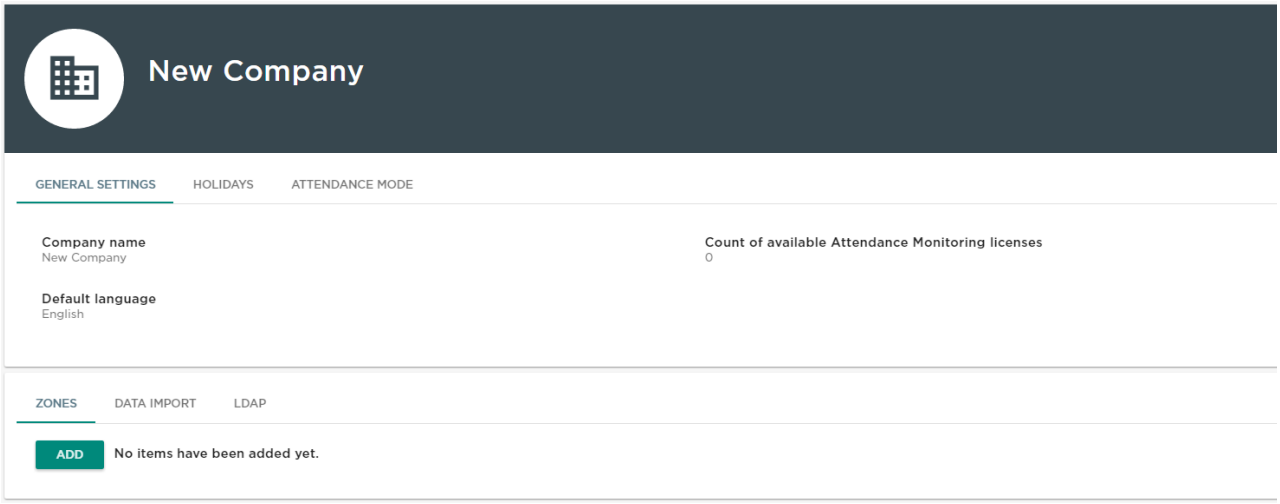
Within one installation, divide the **2N® Access Commander** settings into companies to prevent the managers of one company from seeing the users of the other company. This method also enables common building facilities to be shared by multiple companies (entrances, lifts, restaurants, meeting/conference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

Company Creation

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



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.
- **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. 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

- **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.

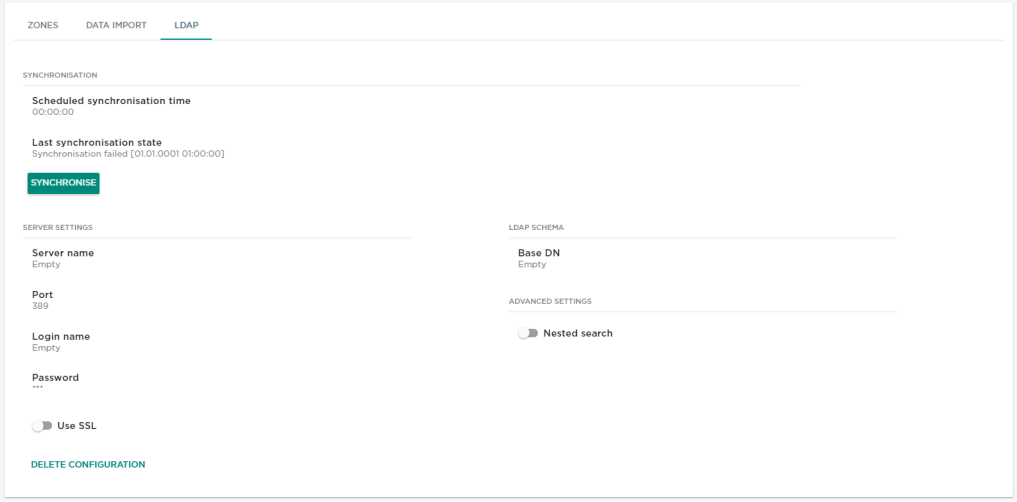
Zones

- **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 CSV file** – import users and groups from a CSV file.
- **Download sample CSV file** – download a sample CSV file for user import.

LDAP



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

User Card Adding

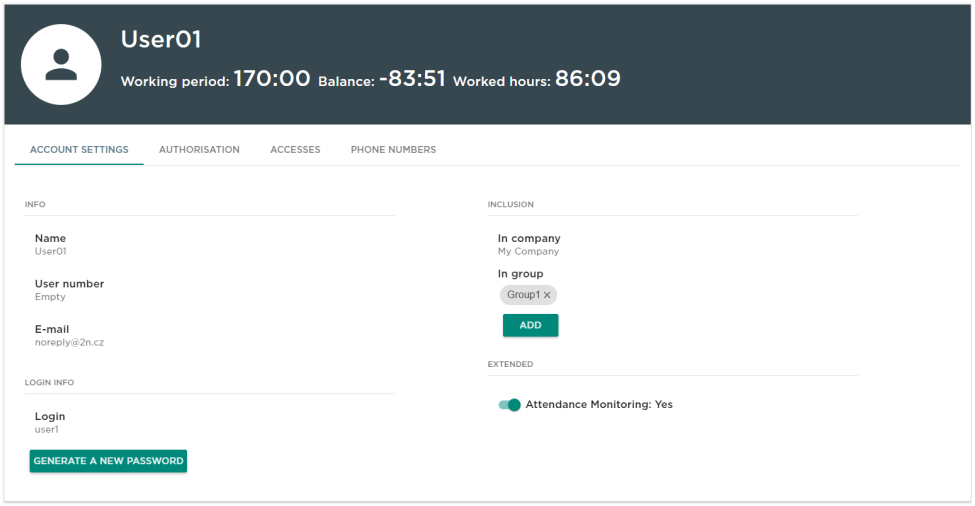
Refer to Subs. **Who is assigned what rights? User Types.**

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

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.



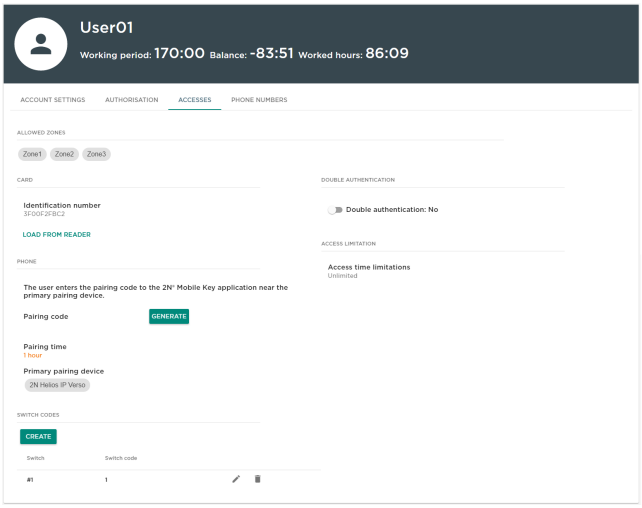
1. Account setting

- 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.

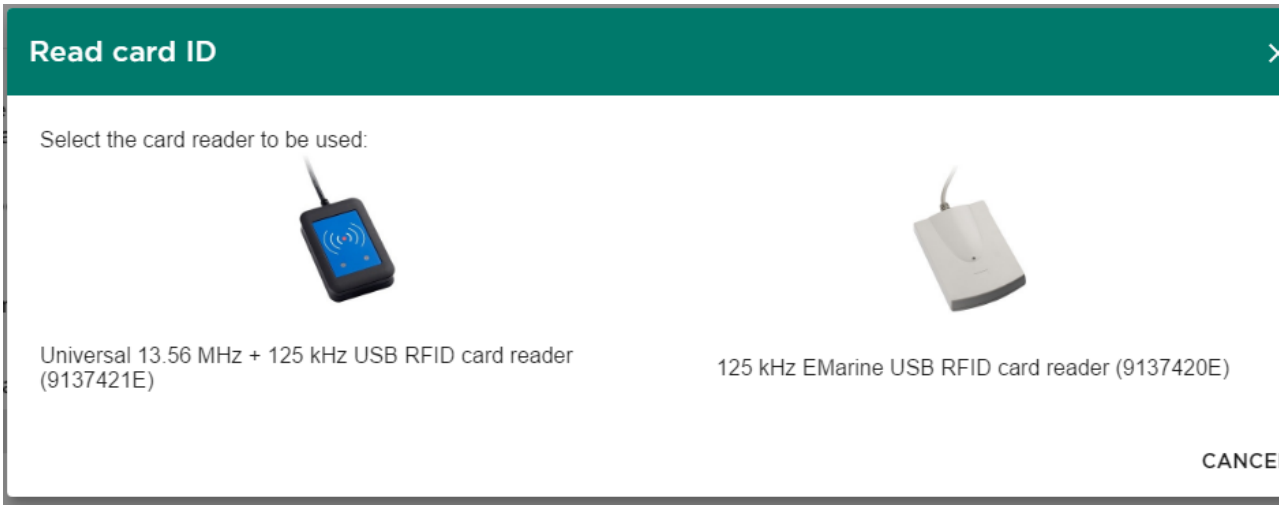
2. Authorisation

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

3. Accesses



- 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.



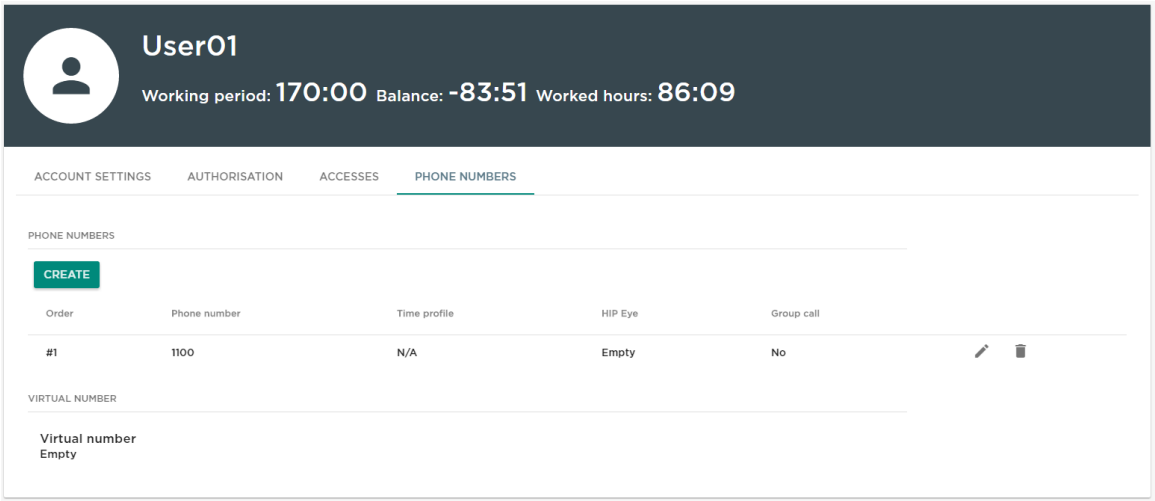
1. 13.56 MHz + 125 kHz (9137421E) USB RFID reader – install a card reader driver.

   Download from **2N® Access Commander** or **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.

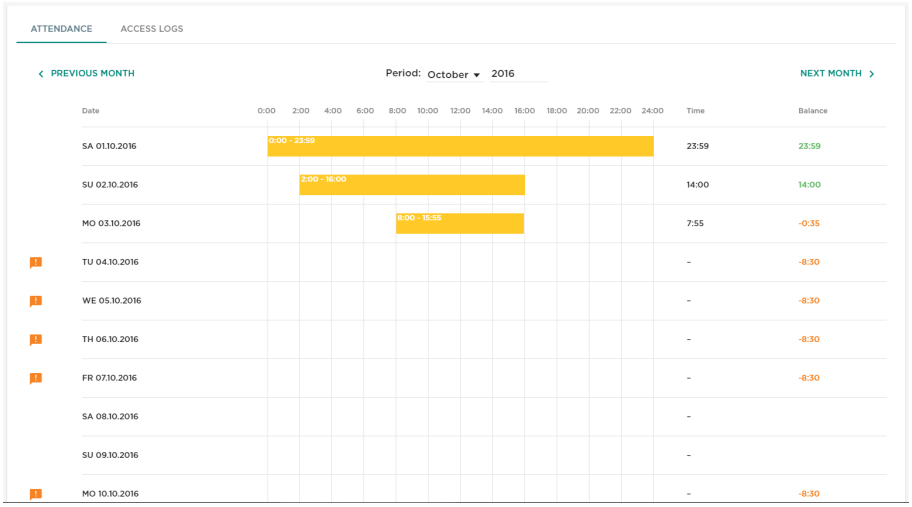
4. Phone numbers



Create phone number via the following parameters.

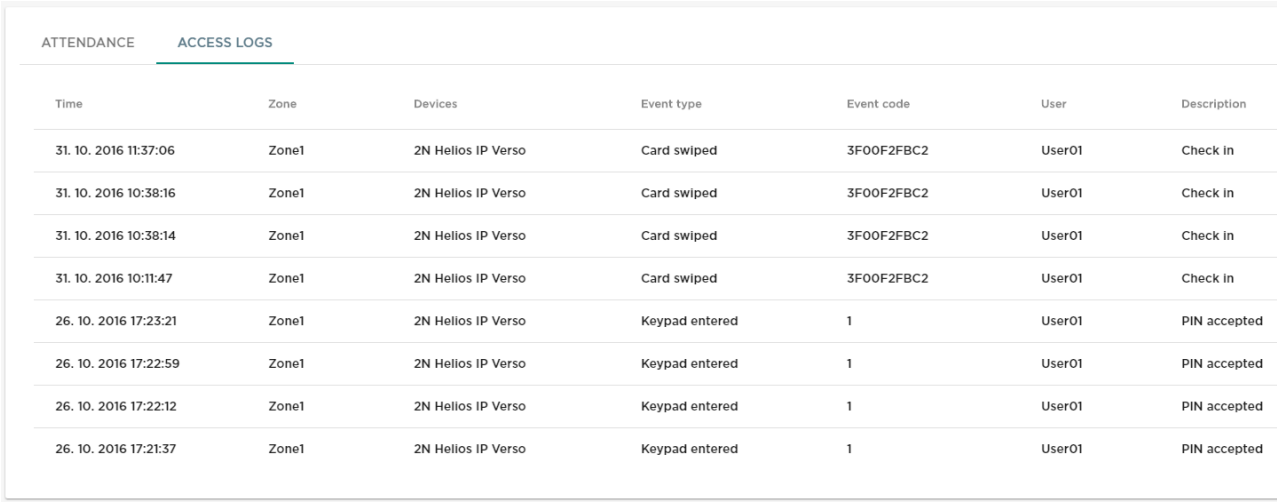
- Phone number sequence – define which number shall be called first. If the first number is unavailable, the second and then the third number shall be dialled.
- Phone number of the station to be called.
- Time profile for phone number time limitations.
- HIP Eye address to be used by 2N® Helios IP Eye 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:

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.

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.

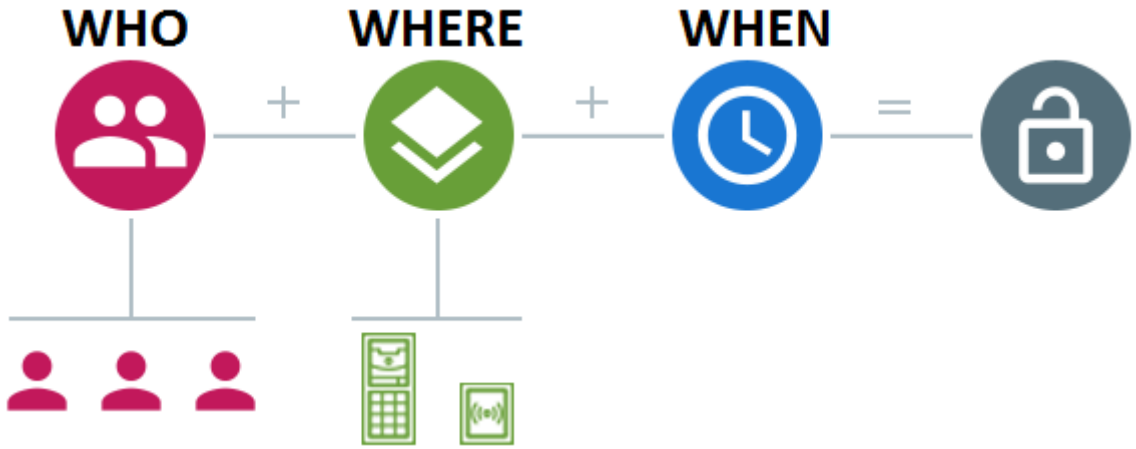
How Do Access Rules Work?

Group	Zone	Time profile
Group1	Zone1	N/A

The access rules define WHERE, to WHOM 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:

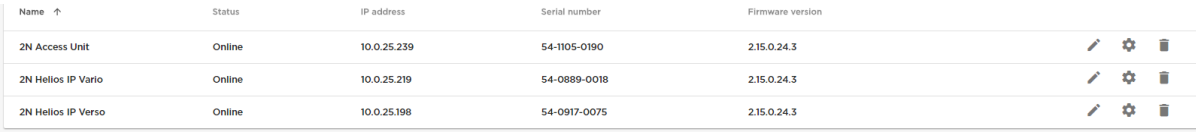


Info

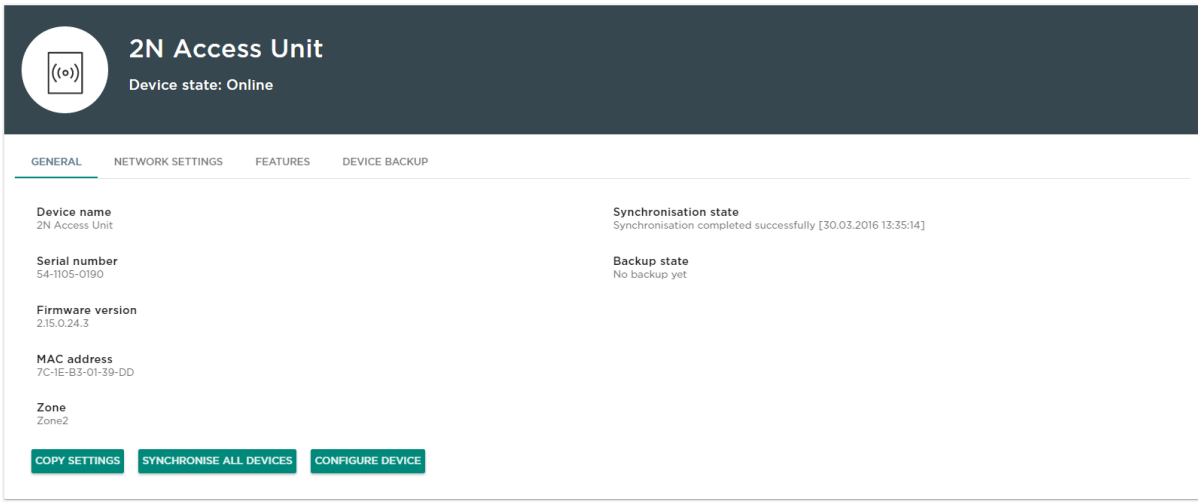
- One group can be assigned to multiple zones as well as one zone can be assigned to multiple groups.
- A selected zone-group pair can be added repeatedly with different time profiles.

Device Configuration via AC

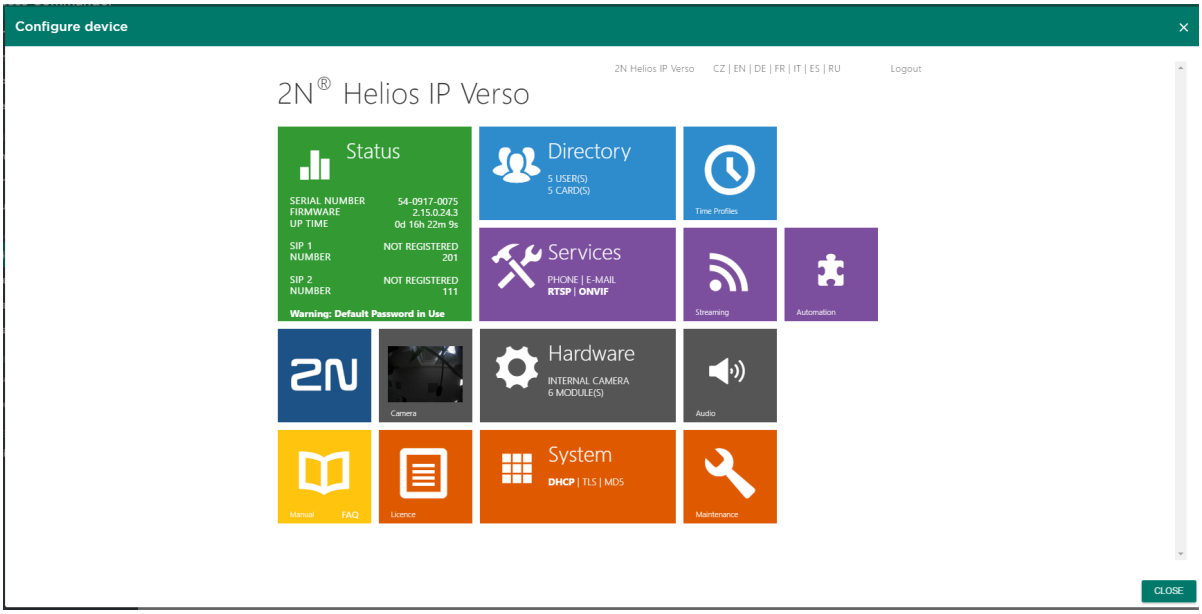
1. Select the **Device** card.
2. Select the **active** device to be configured from the list of added devices and choose the **Modify** device option (click anywhere in the selected device row).



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

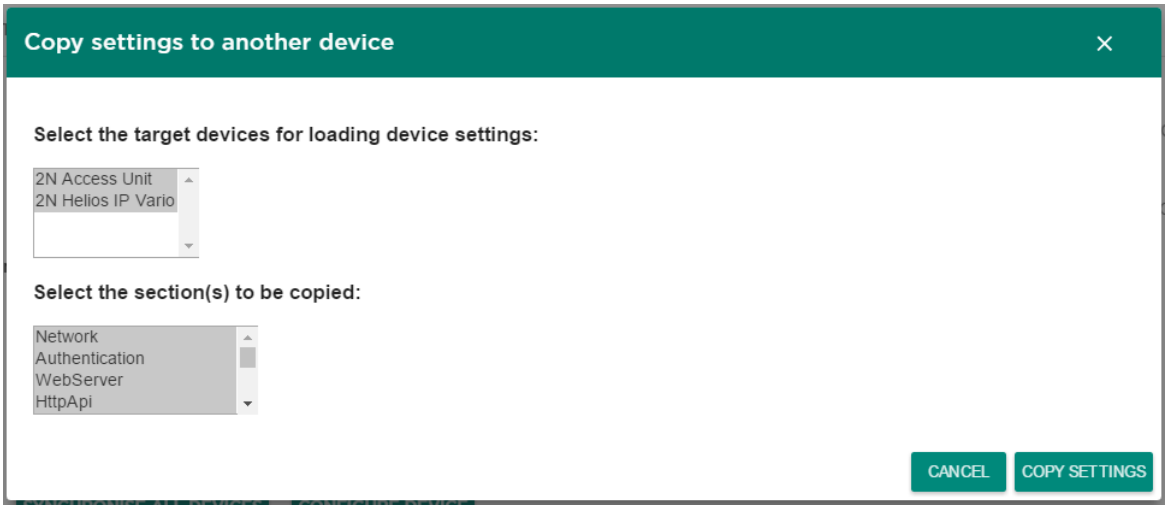


4. A new window opens up for you to configure the selected device (for parameter details refer to the Configuration Manual at **https://manuals.2n.cz/is/en**). Click the right-hand upper corner to close the window any time and return to the environment of the **2N® Access Commander.**


Configure device
2N Helios IP Verso
CZ | EN | DE | FR | IT | ES | RU
Logout
2N® Helios IP Verso
Status
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
Warning: Default Password in Use
Directory
5 USER(S)
5 CARD(S)
Time Profiles
Services
PHONE | E-MAIL
RTSP | ONVIF
Streaming
Automation
Camera
Hardware
INTERNAL CAMERA
6 MODULE(S)
Audio
Manual
FAQ
Licence
System
DHCP | TLS | MD5
Maintenance
CLOSE

Copying of Settings between Devices

1. Go to the **Device**
2. Select the **active** device whose configuration is to be copied and select the **Modify device** option.
3. In the section **Management** select the **Copy setting** item. If the device is not in the **active state**, the option cannot be used. The parameter icon is inactive in this case.
4. Select the device in the open window to which you want to copy the configuration. You can select more devices at once by holding **Ctrl** and selecting more list items with your mouse. Having selected the items, click on the diskette to save the selection.
5. Moreover, you can specify the setting parts to be copied in this window. Again, you can choose more sections using the **Ctrl** key.



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) 

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
2.18.0.27.5	✓	✓	✓	✓	✓	✓
2.17.0.26.5	✓	✓	✓	✓	✓	✗
2.16.1.25.7	✓	✓	✓	✗	✗	✗
2.16.0.25.4	✓	✓	✓	✗	✗	✗
2.15.2.24.7	✓	✓	✓	✗	✗	✗
2.15.1.24.5	✓	✓	✓	✗	✗	✗
2.15.0.24.3	✓	✓	✓	✗	✗	✗

Bluetooth

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

Licence v 1.5.0

There is a change in licensing in version 1.5.0. From now on, one connected device has to be selected as a licensed one.

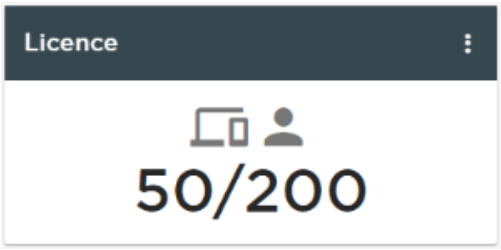
Refer to the **Licence** tile on the administrator's **Dashboard** for the current count of licensed devices and Attendance users. Upon the initial installation of the **2N® Access Commander**, a Trial licence (see below for details) will be available for you to configure one device and monitor Attendance 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:

91379040	2N® Access Commander – licence for +5 devices (5-device licence package)*
91379041	2N® Access Commander – licence for +25 users (25-user licence package)** – for employees' Attendance monitoring only

Info

* 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).

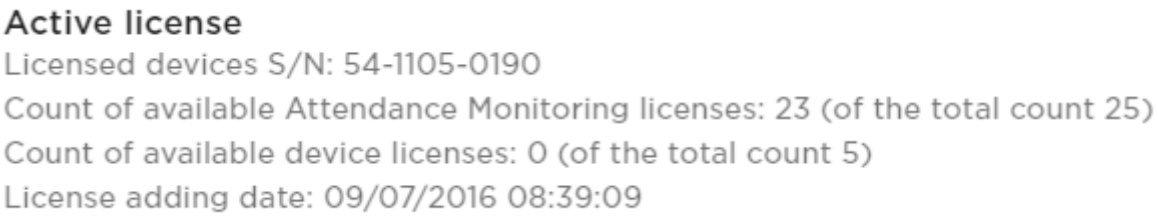
** If you need a licence for 69 users, e.g., then order 3 licences No. 91379041 (to monitor arrivals/departures of up to 75 users in total).



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.

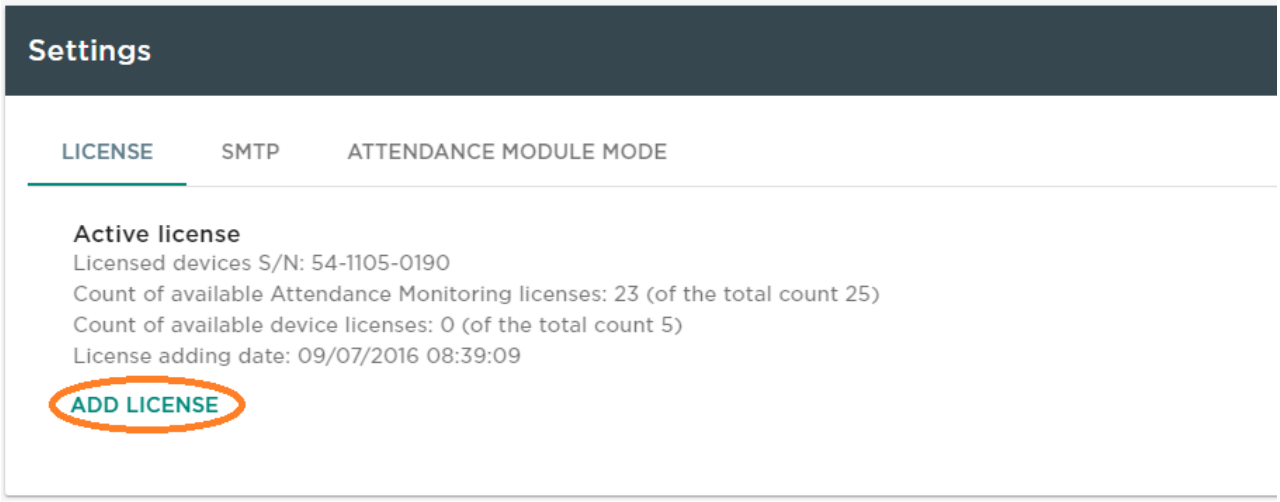


Licence Device S/N for Licence Generation

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.



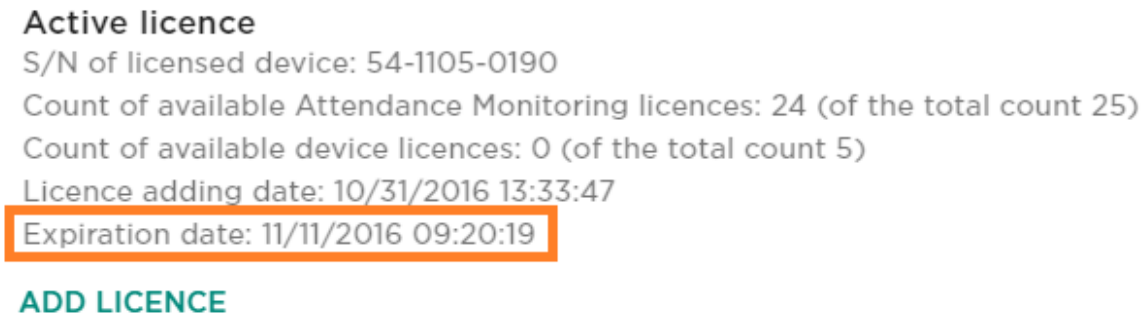
Trial Licence

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.



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

VT-X

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

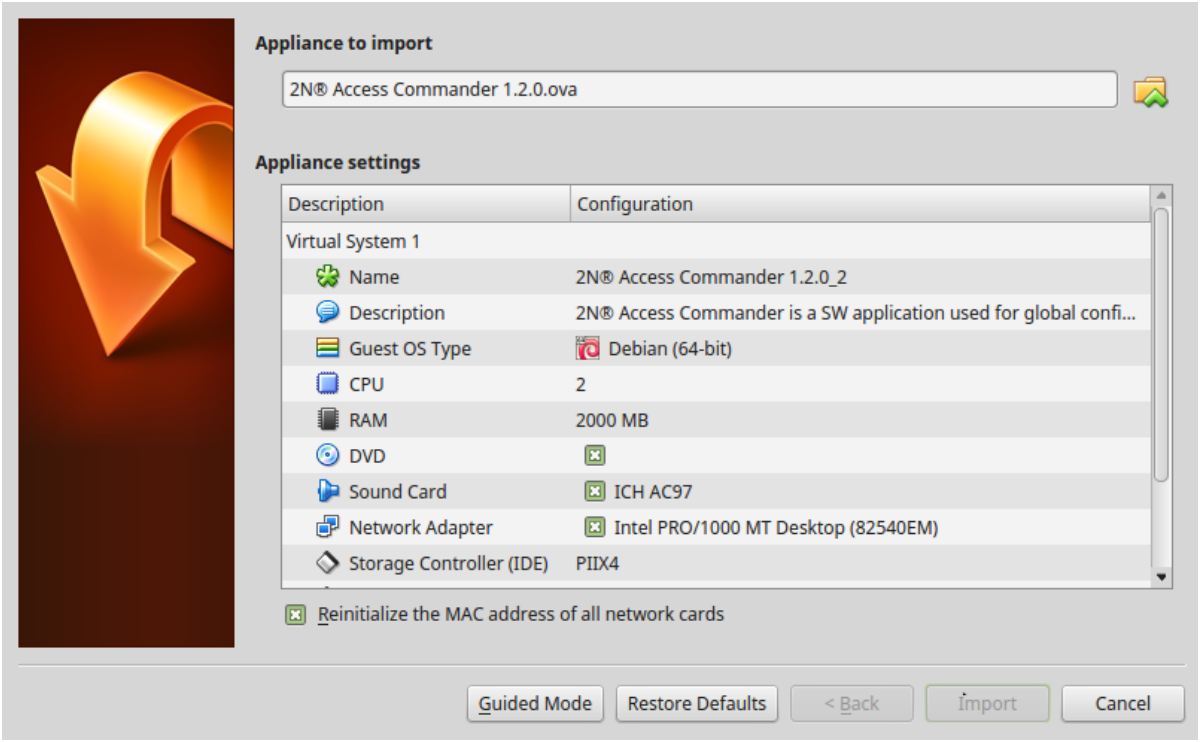
VirtualBox

licence

- *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).

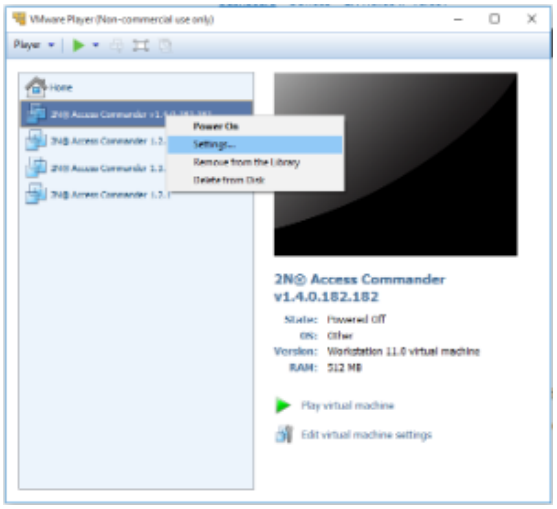
c. Check the RAM setting (2048 MB at least).

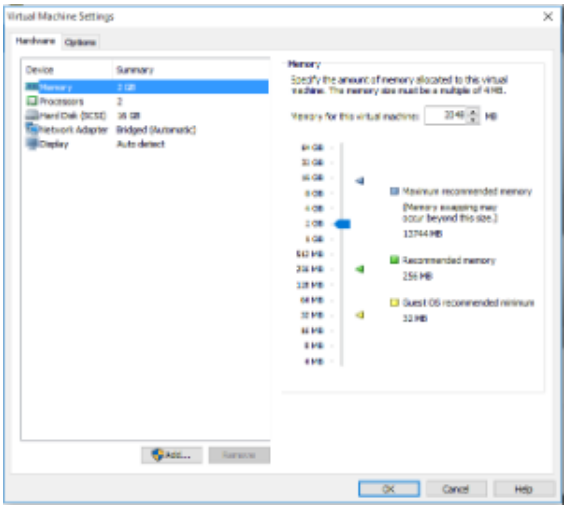
d. Check whether the correct network adapter is selected.

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".



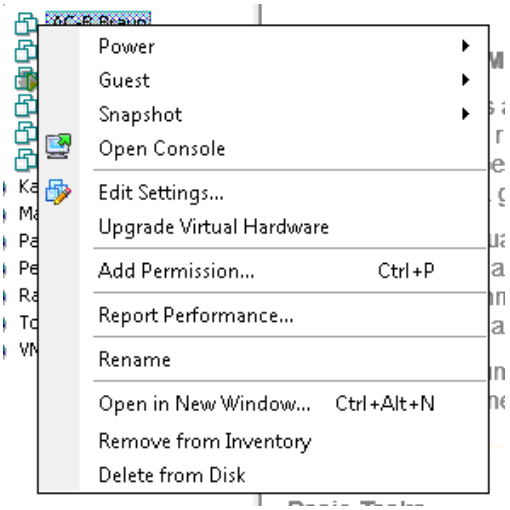


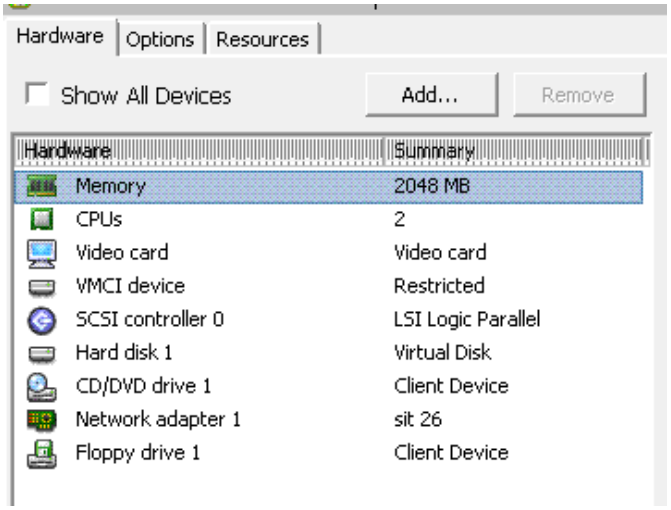
5. Check the settings
    a. Check the CPU setting (2 at least).
    b. Check the RAM setting (2048 MB at least).
    c. Check whether the correct network adapter is selected.

VMware vSphere

- Created in VMware vShere – 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 vShere 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.

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.

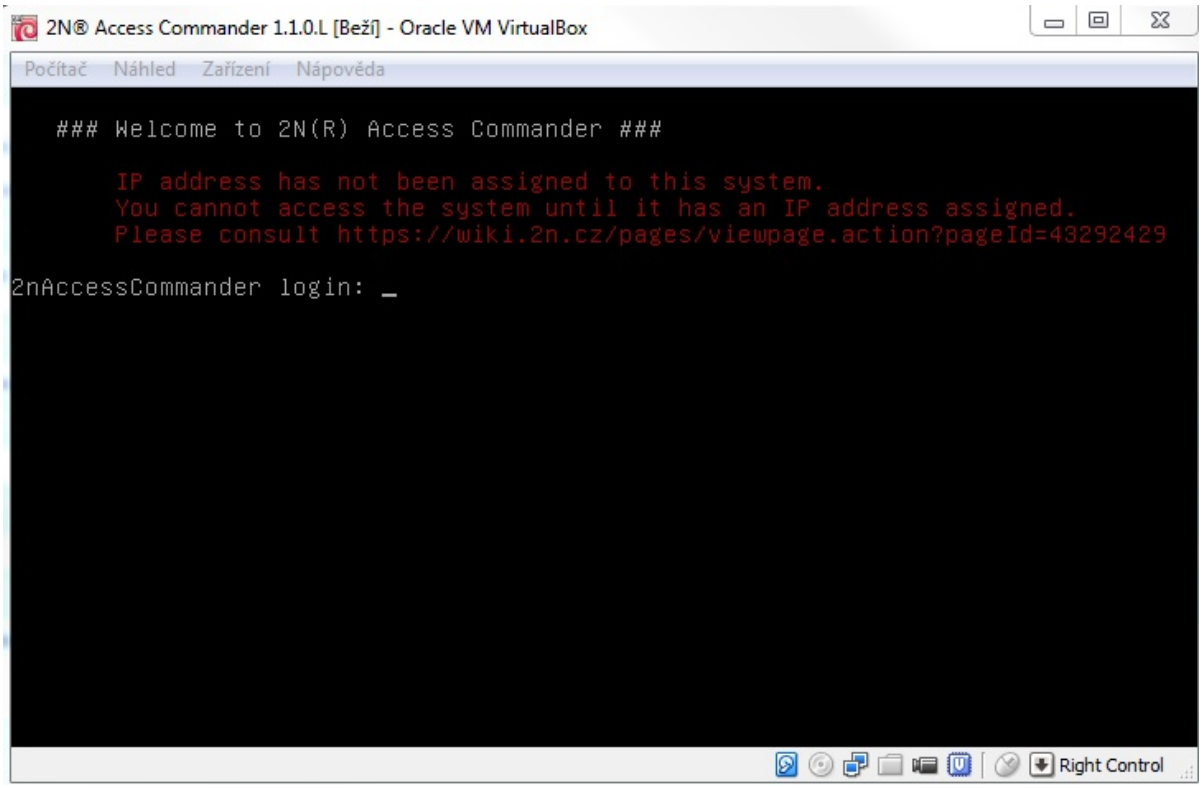
As a rule, the users are added to the device including their card IDs and switch codes. In addition to the card ID and switch code, the time profile assigned to the access rule is added too. If a user is assigned to multiple groups with different access rules and different time conditions, its card ID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

Phone numbers are added instead of card IDs for the users mentioned in rules 2, 3 and 4.

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.

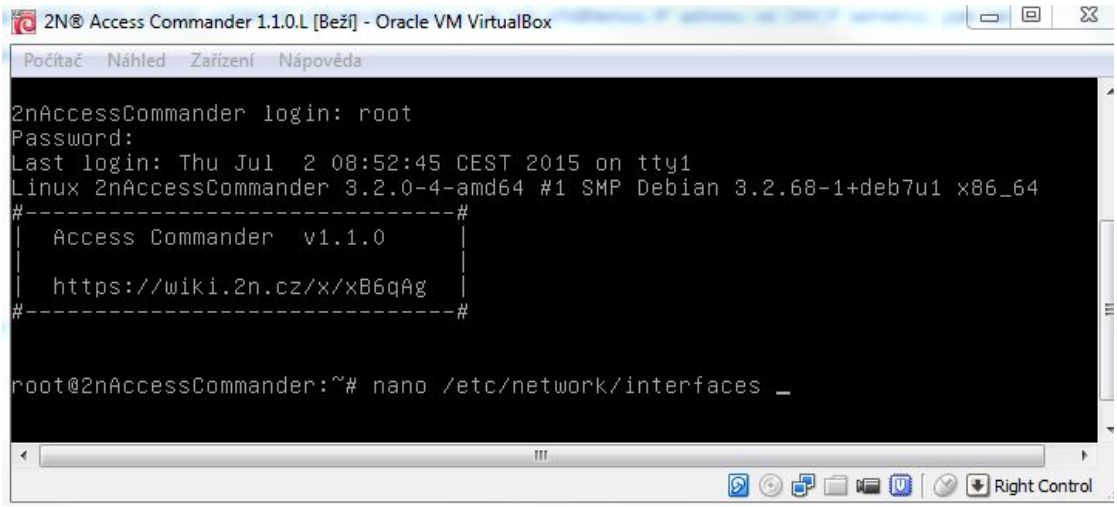
1. Run the virtual server with 2N® Access Commander and open the console. You should see the following message:



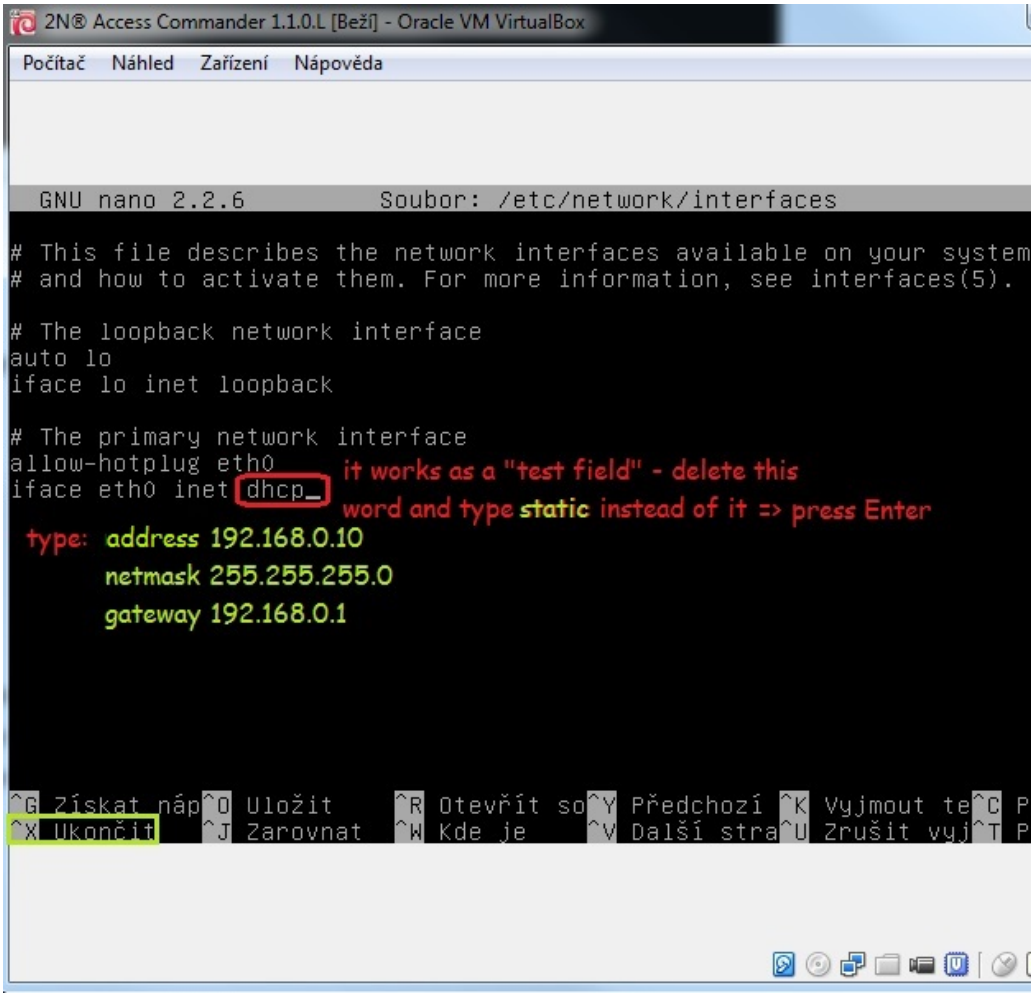
Note

- 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



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



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

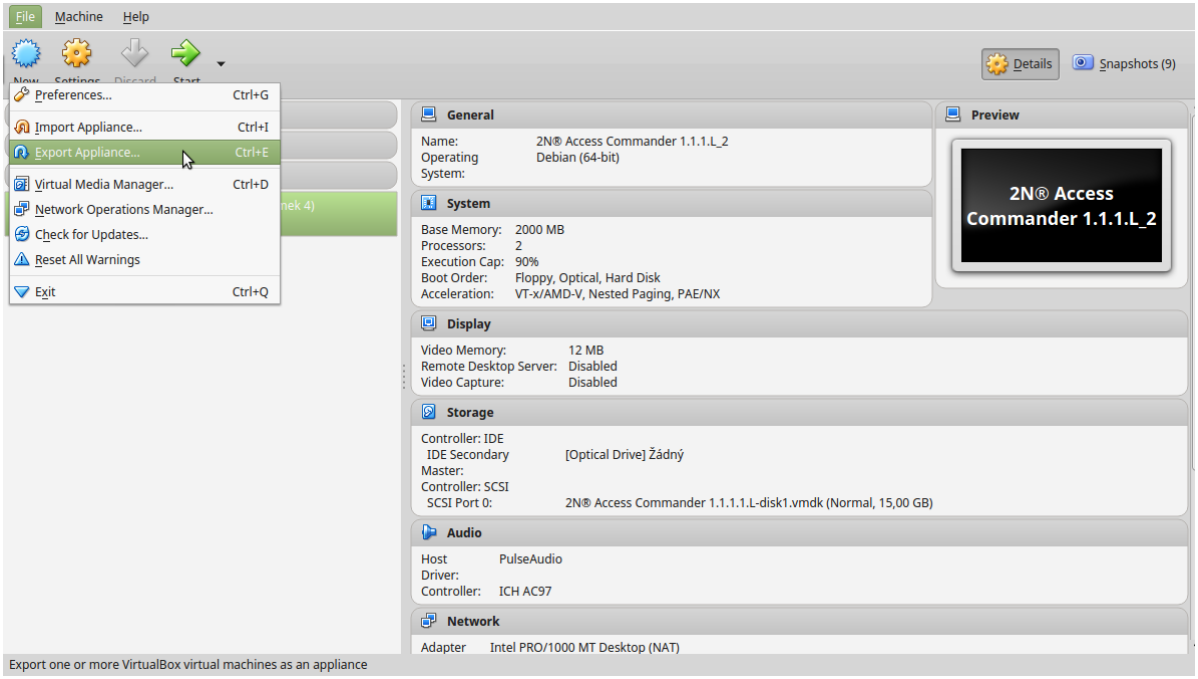
Note

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

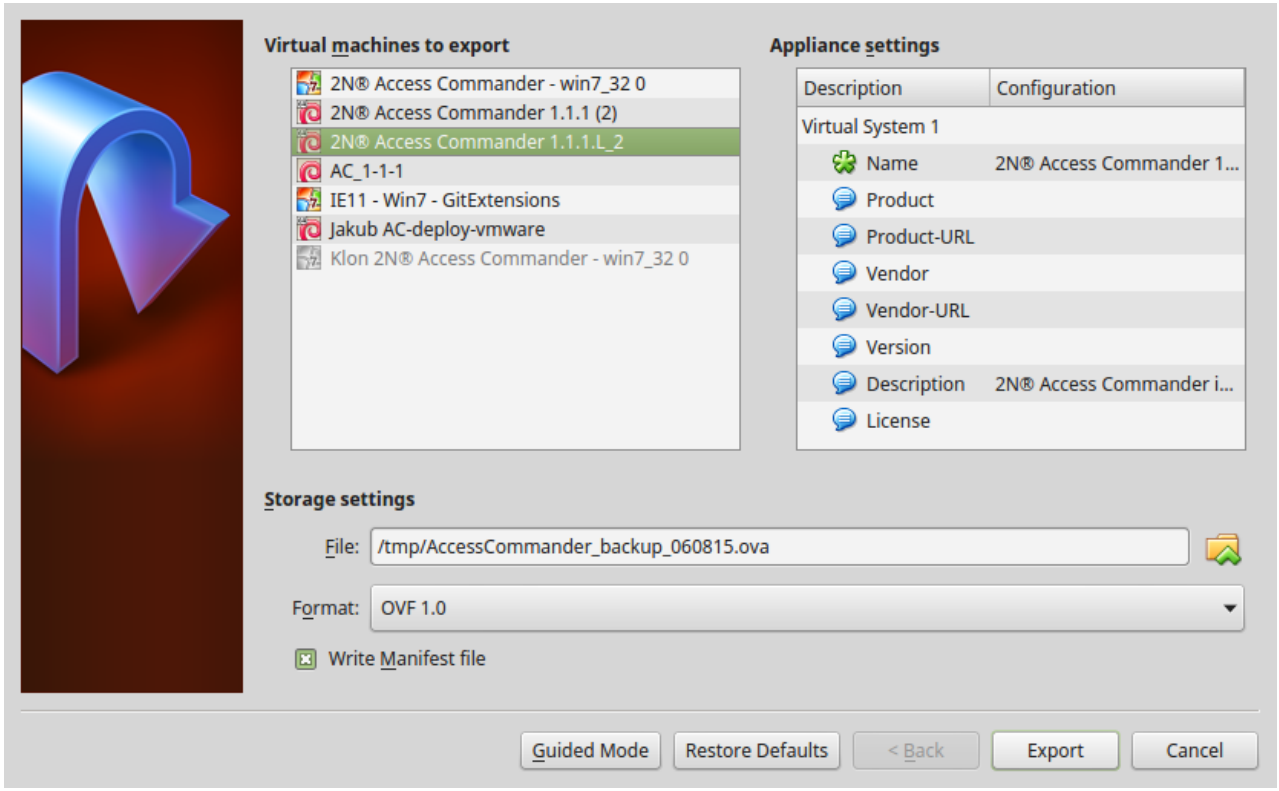
Now that all the steps above have been taken, your **2N® Access Commander** is configured successfully to use the static IP address.

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

- With the virtual machine off.
- Go to File Export appliance...



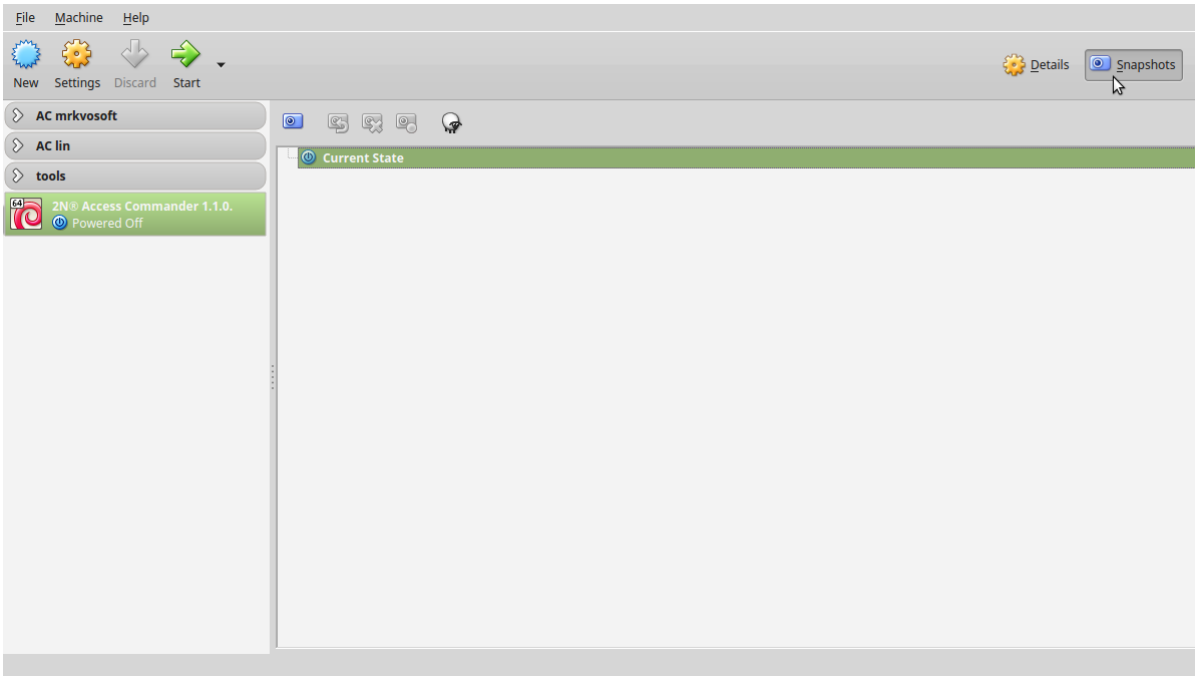
- Select the virtual machine, set the export path and select the Manifest Export storage.



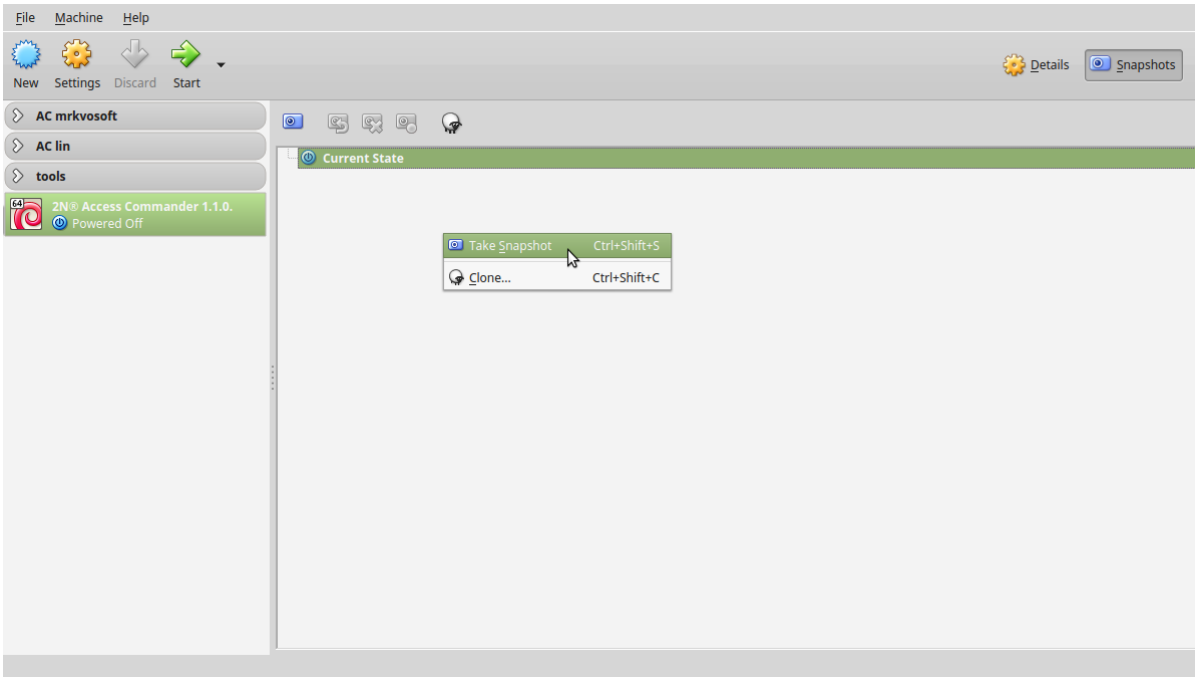
The exported file can be easily transferred and imported (refer to the AC setup) via any machine *(see the minimum virtual machine requirements) to the VirtualBox application (or another virtualisation tool if the file is converted for the given application).

Application / Virtual Machine Snapshot (within VirtualBox only)

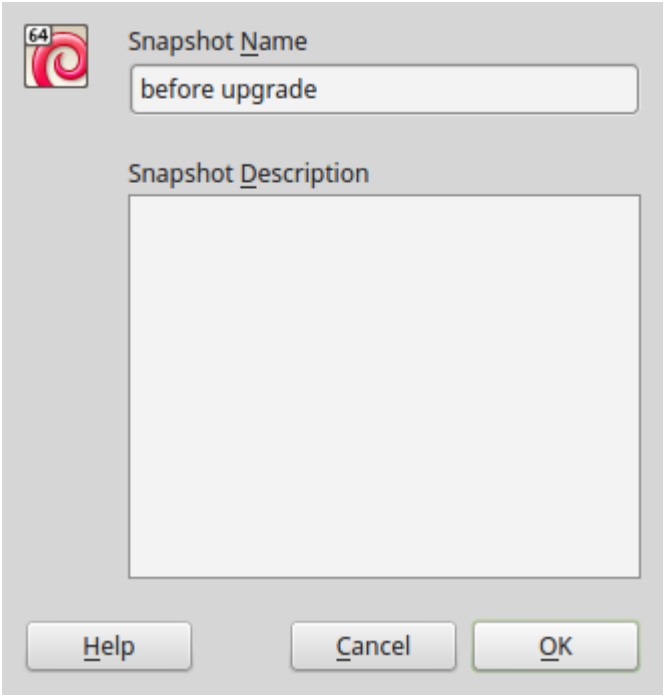
- With the virtual machine on/off.
- Switch to the Snapshots tab.



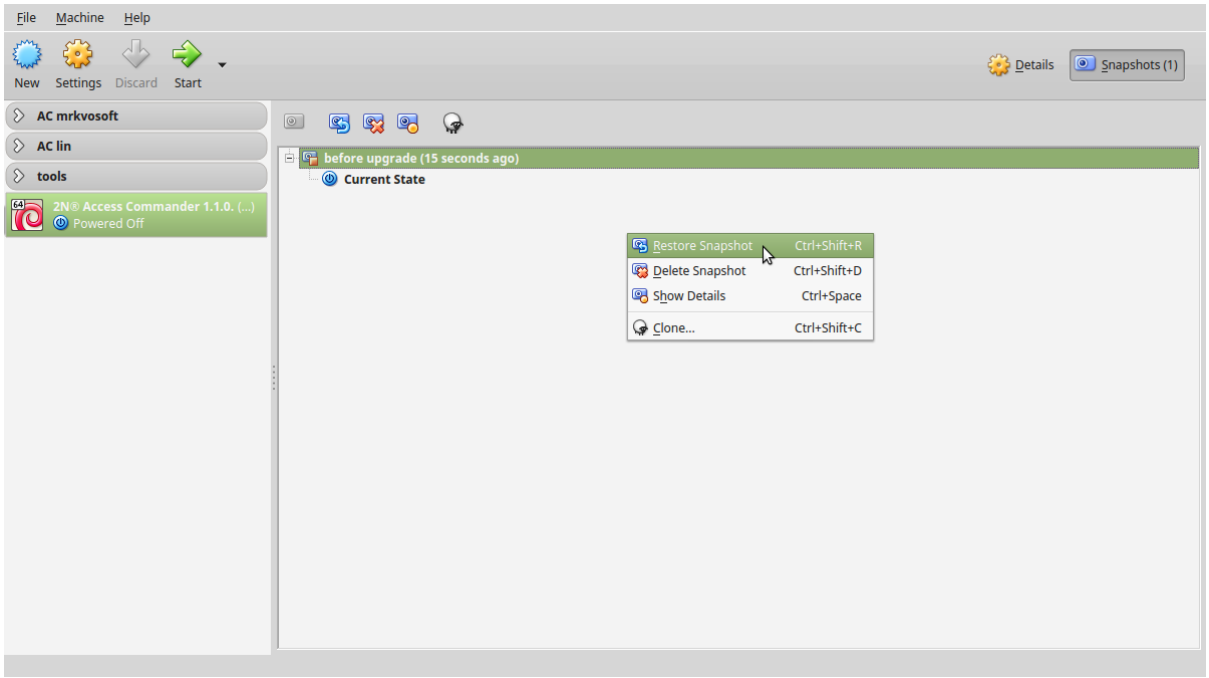
- Perform the Scan snapshot action.

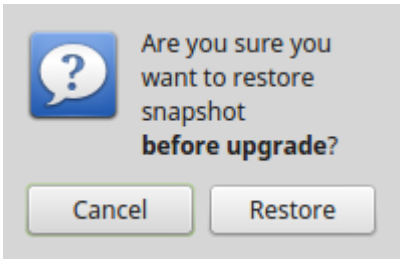


- Edit the name (plus reason for creation).



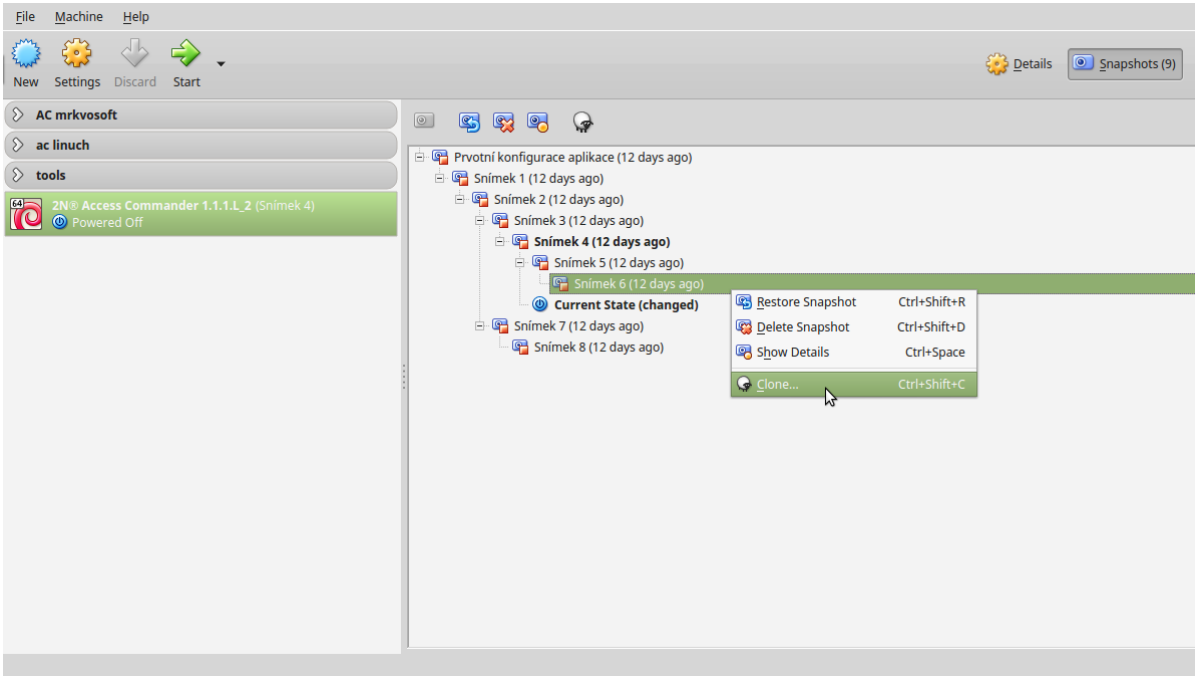
Thus, a renewal point is created that can be easily renewed.



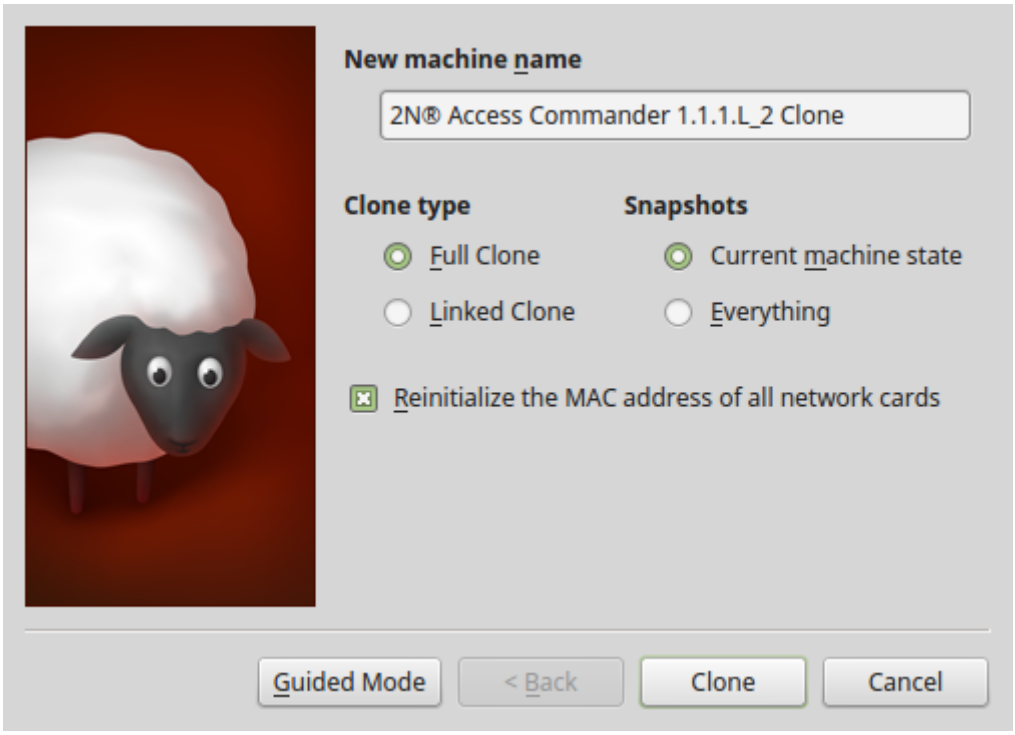


Application / Virtual Machine Cloning (within VirtualBox only)

- 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
2N® Access Commander 1.1.1.L_2 Clone
Clone type
Full Clone
Linked Clone
Snapshots
Current machine state
Everything
Reinitialize the MAC address of all network cards
Guided Mode
< Back
Clone
Cancel

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

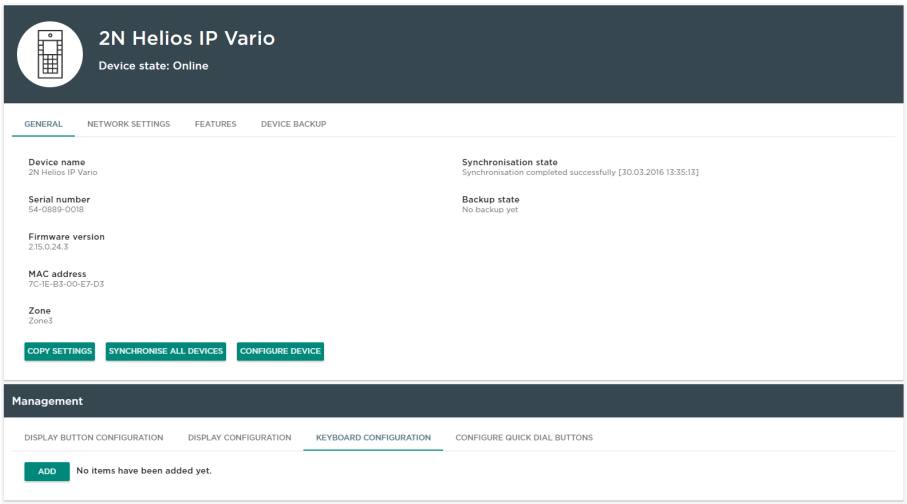
Automatic synchronisation helps you update terminal equipment settings in the whole access system. It is started upon every change that is to be reflected in the terminal equipment configuration, i.e. that is related to user access rights, phone numbers, time rules or button settings. The synchronisation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

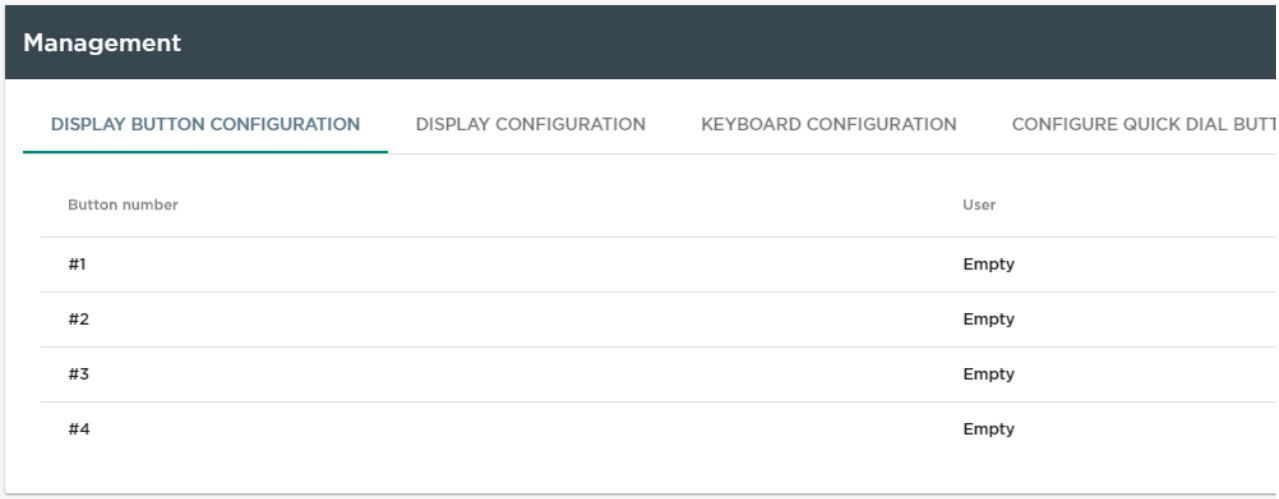
- The automatic synchronisation time (updating of all terminal equipment) depends on the count of devices to be synchronised and the amount of data to be loaded.

Display Configuration

Go to the detail of the device to configure the device display. Select Display button configuration or Display configuration in the Administration section.

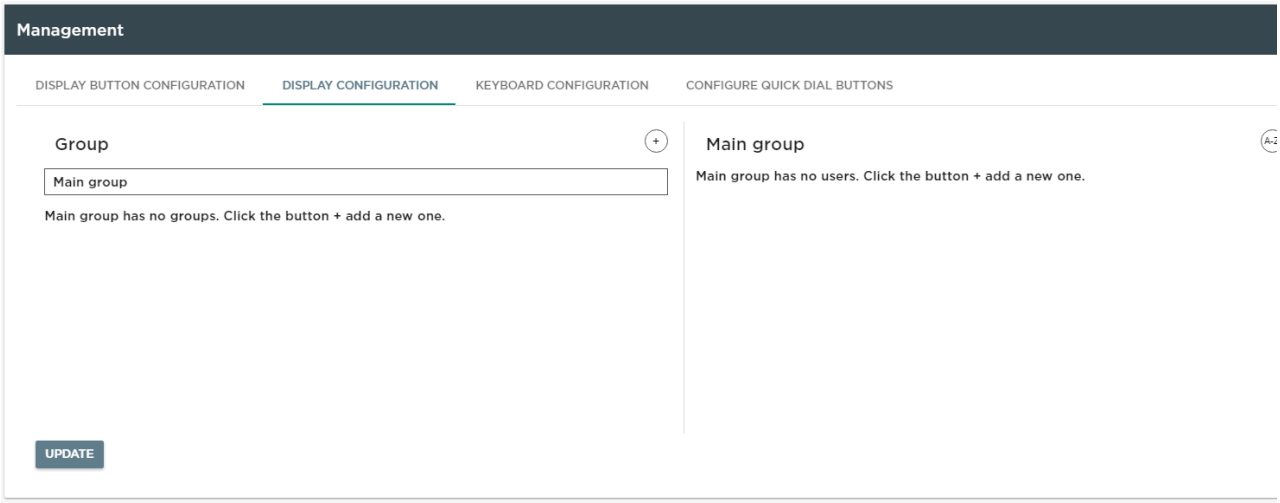


Name Tag Configuration



Name tags are used for quick dialling of users using a single button. Click on "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



This window helps you create the list to be loaded to the device. Click + to create a group. Use Drag&Drop to move groups in the structure. Having created the required structure, assign users to groups. Select a group and click + next to the group name to the right to add a user. Having configured the display, click OK and start synchronisation.

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.

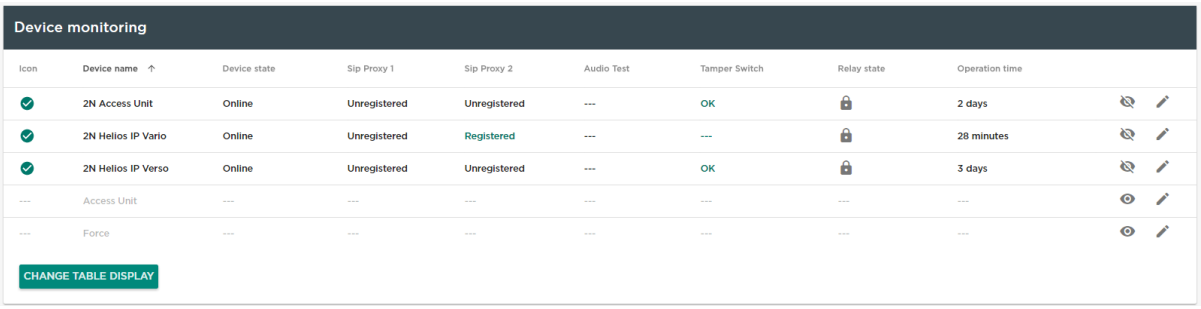


Table items:

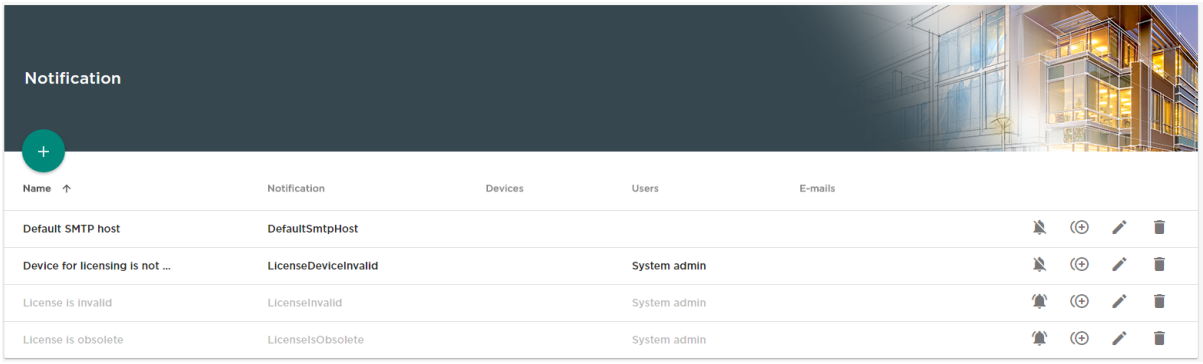
- Icon – display the device state (OK or not).
- Device name
- Device state
- SIP Proxy – display the SIP Proxy state on a device. If there is an error, mouse click the description to get a detail.
- Audio test – display the last audio test result.
- Tamper switch – if there is an error, mouse click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

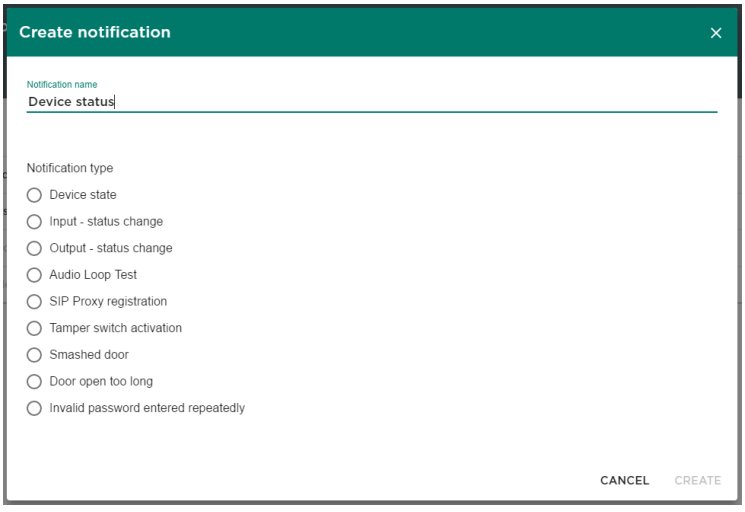
Notification

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



Create a new notification:

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

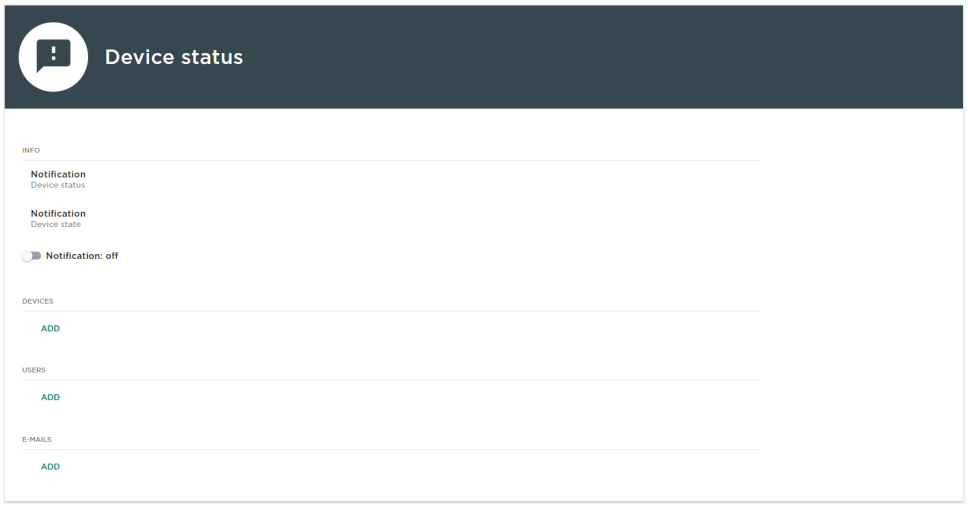


4. A new page will be created for:
   a. notification activation,

b. device adding for monitoring,

c. user adding for e-mail sending,

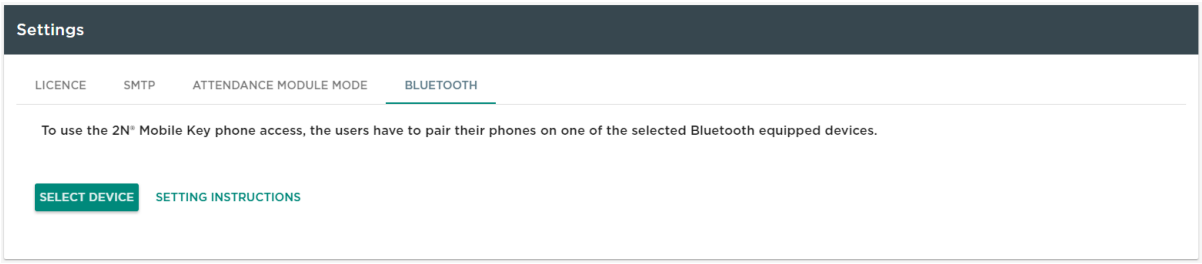
d. e-mail adding if non-existent in the system.



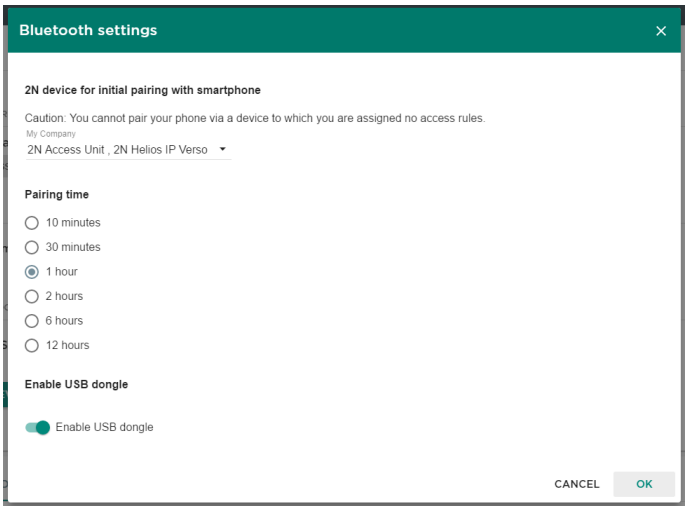
SMTP

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

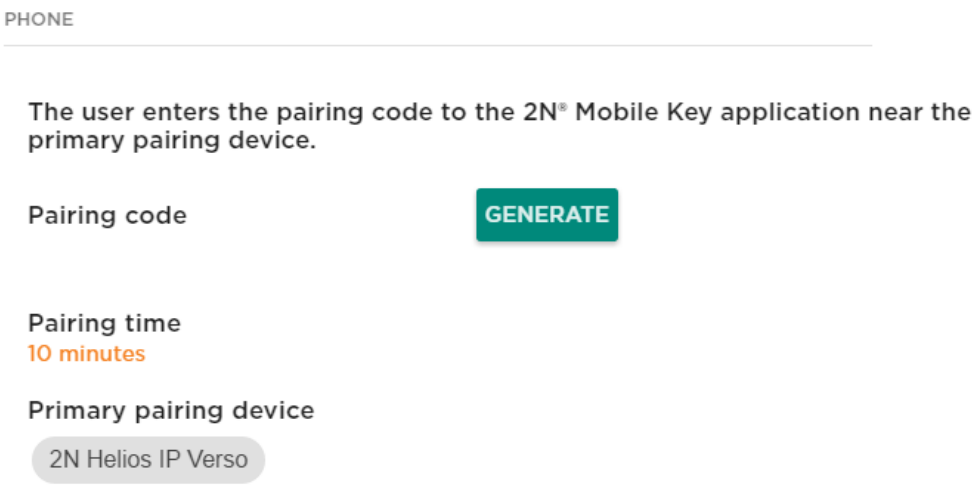
Bluetooth Configuration



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.



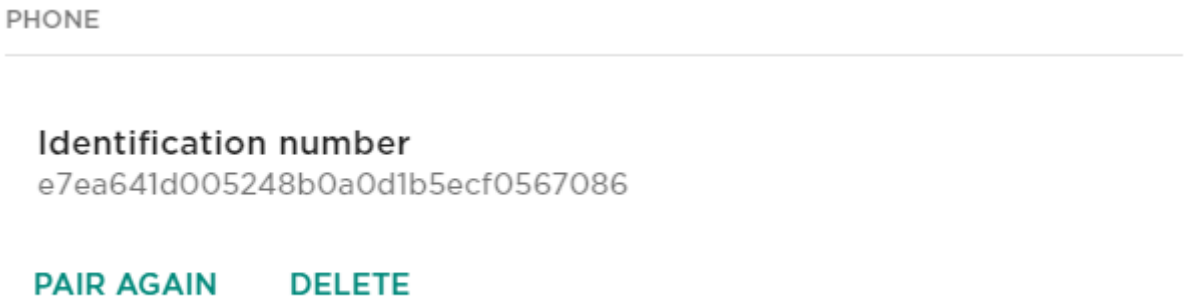
Make sure that the device is configured for each company. If a device is assigned to a zone shared by multiple companies, you can select one device for more companies than one. The pairing time setting is valid from the moment when you click Generate on the user and the PIN gets displayed. Having configured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



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** 1.0.7 is installed for the dongle option. Having selected dongle, just click Start pairing and enter the pairing PIN to your **2N® Mobile Key** equipped smartphone.

> **Generovat**
>
> 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.

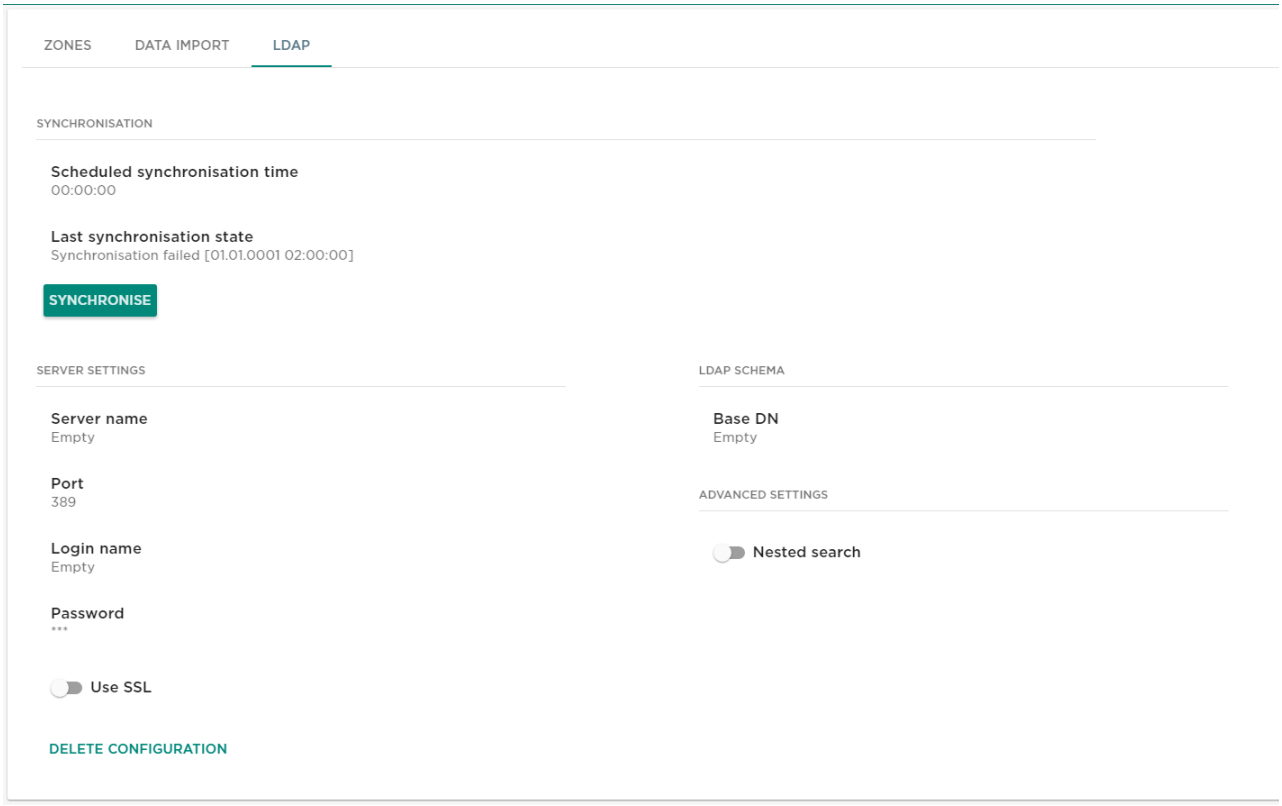
When you click Generate, the PIN for primary pairing will get displayed. A time is set for the user to get to the device and enter its PIN. If the user fails to do so within the timeout, the administrator shall generate a new code. Refer to the user phone ID detail to see if pairing was successful.



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

LDAP

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



- Synchronisation
  1. Periodical synchronisation time
  1.
     - Set the time when the 2N® Access Commander shall make a query to the LDAP server concerning user changes.
  2. 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.
  3. Synchronisation button

- Click the button to start synchronisation immediately. Thus, the administrator does not have to wait for periodical synchronisation.

- Server settings
  1. 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.
  2. 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.
  3. 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**“.
  4. Password
     - The password of the specific user on the LDAP server.
  5. 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.
  6. Delete configuration button
     - Click the Delete configuration button to delete the parameter settings without deleting the previously uploaded users.
- LDAP schema
  1. 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
  1. Nested search
     - If nested search is used, the whole tree is searched instead of a root.

LDAP licence

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

LDAP

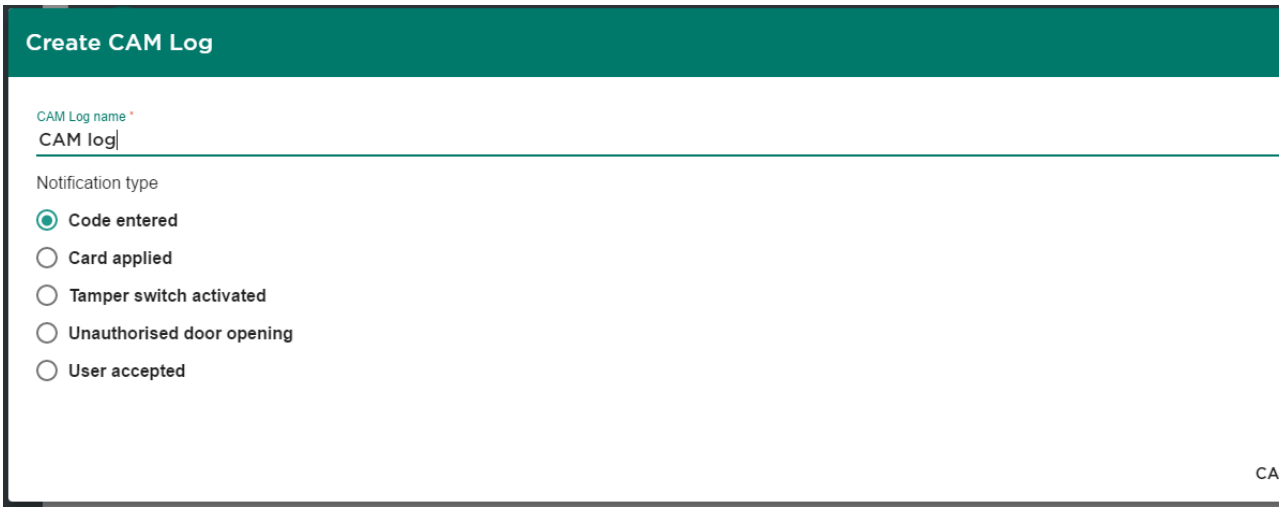
Refer to **www.ldap.com** for LDAP details.

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.

Make sure that firmware 2.1.8.0 or higher is installed in the intercoms to make the CAM logs work properly.

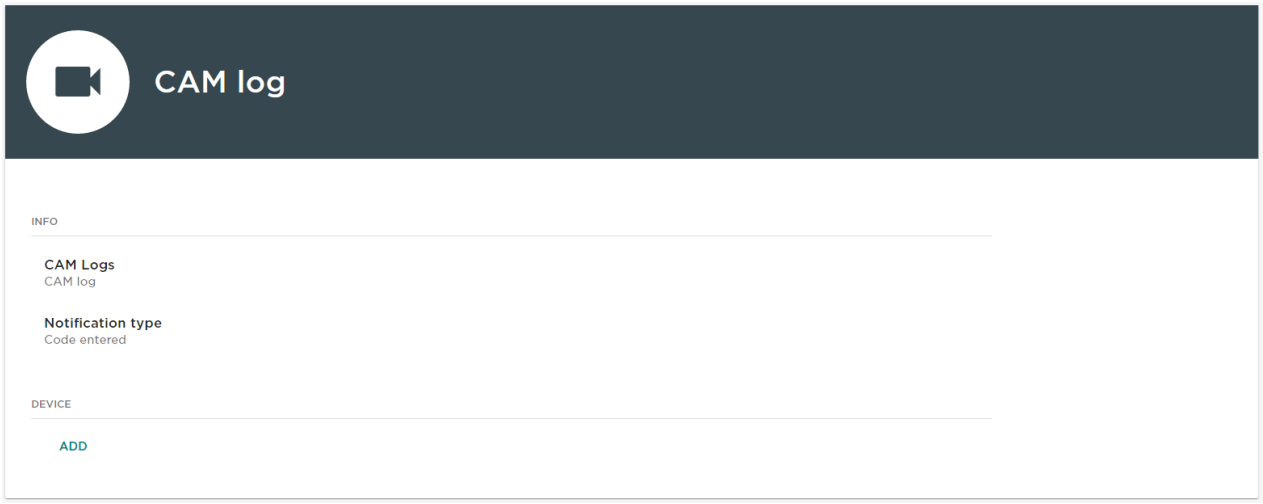
CAM Log Creation



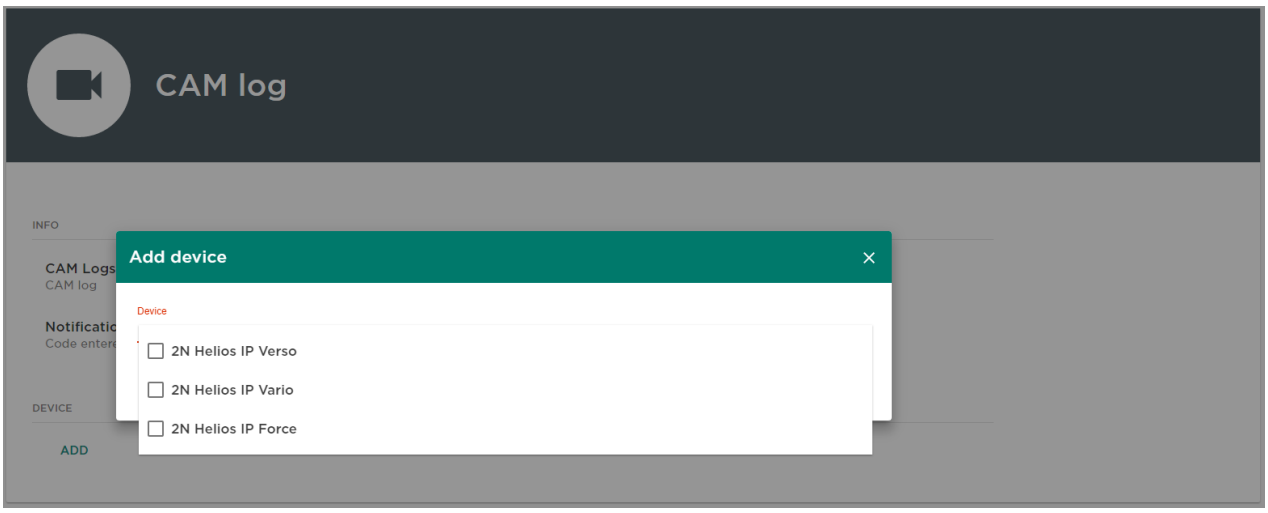
To create a CAM log, enter the CAM log name and select a notification.

- 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.

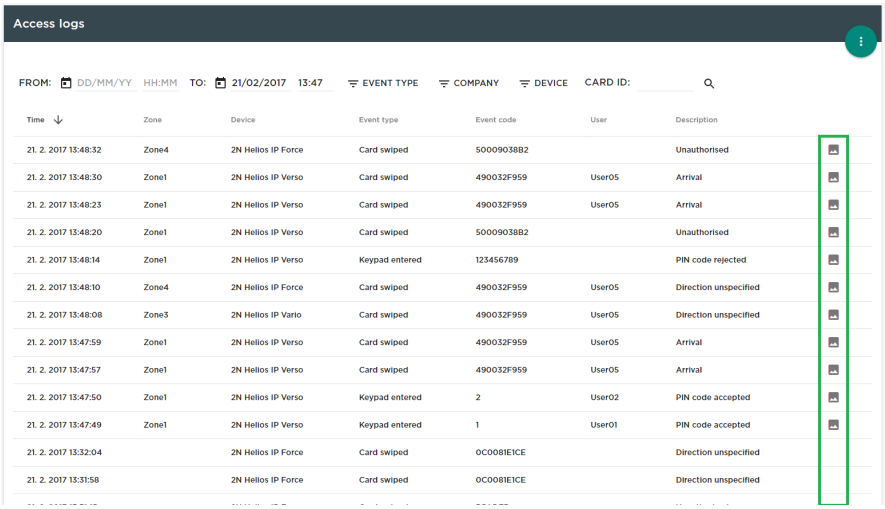


Here select the devices from which CAM logs shall be downloaded.

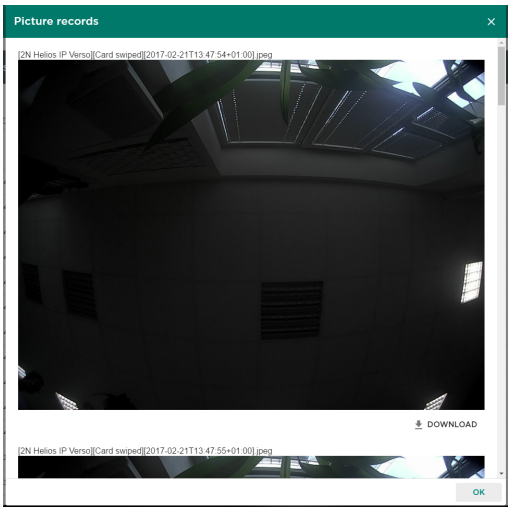


In addition to passage data, the CAM logs display an intercom snapshot display icon. No CAM logs are displayed for the intercoms that are not equipped with a camera.

CAM Log Viewing



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.

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

Make sure that correct time values are set both in the intercom and 2N® Access Commander server to make the CAM logs work properly.

2N TELEKOMUNIKACE a.s.

Modřanská 621, 143 01 Prague 4, Czech Republic

Phone: +420 261 301 500, Fax: +420 261 301 599

E-mail: sales@2n.cz

Web: www.2n.cz

v1.7