2N

Integration Manual

Device Category

✔ ACS	IAS	FPS	CCTV	DVR	Perimetry	Building	External	✔ Other

Supported Functionality

Import From File	Combined Credentials
✔ Lift	Encrypted Communication
Device Auto Import	Time Synchronization
Time Zone Support	Live Video Streaming
Recorded Video Streaming	Video Records Downloading
Voice Transmitting	Audio Streaming
PTZ	Presets
Motion Detection	Live Stream Snapshot
Recorded Stream Snapshot	Multiple Stream Types
Fire Panel Networking Mode	✔ Card Learning
Dynamic Upload	✔ Access Time Restriction
✔ Holidays Support	✔ Pin Management
✔ Card Management	✔ Fingerprint Management
Reserved Memory Zones	Antipassback Forgiveness
Handicapped Flag	Alarm Suppression
Fire Alarm Counter	Device Audit Log Retrieval
Remote Device Control	Dynamic Command State
Wiegand Biometric Support	

Legend:

- ✔ – Fully supported functionality.
- ◑ – Partially supported functionality, see results of integrations tests for more details.

Licensed Unit

- 2N

Default Credentials

Key	Value
Login	admin
Password	2n

How to Connect Device to C4

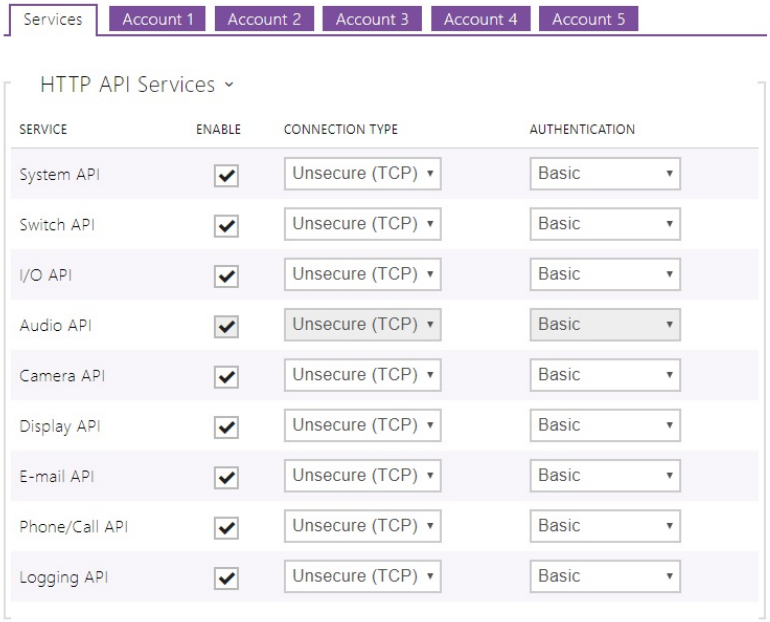
The 2N device is connected to the Local Area Network. The intercom is supplied via PoE or an external power supply.

Refer to product support web sites for more 2N configuration details.

The minimal version of the device FW is 2.33

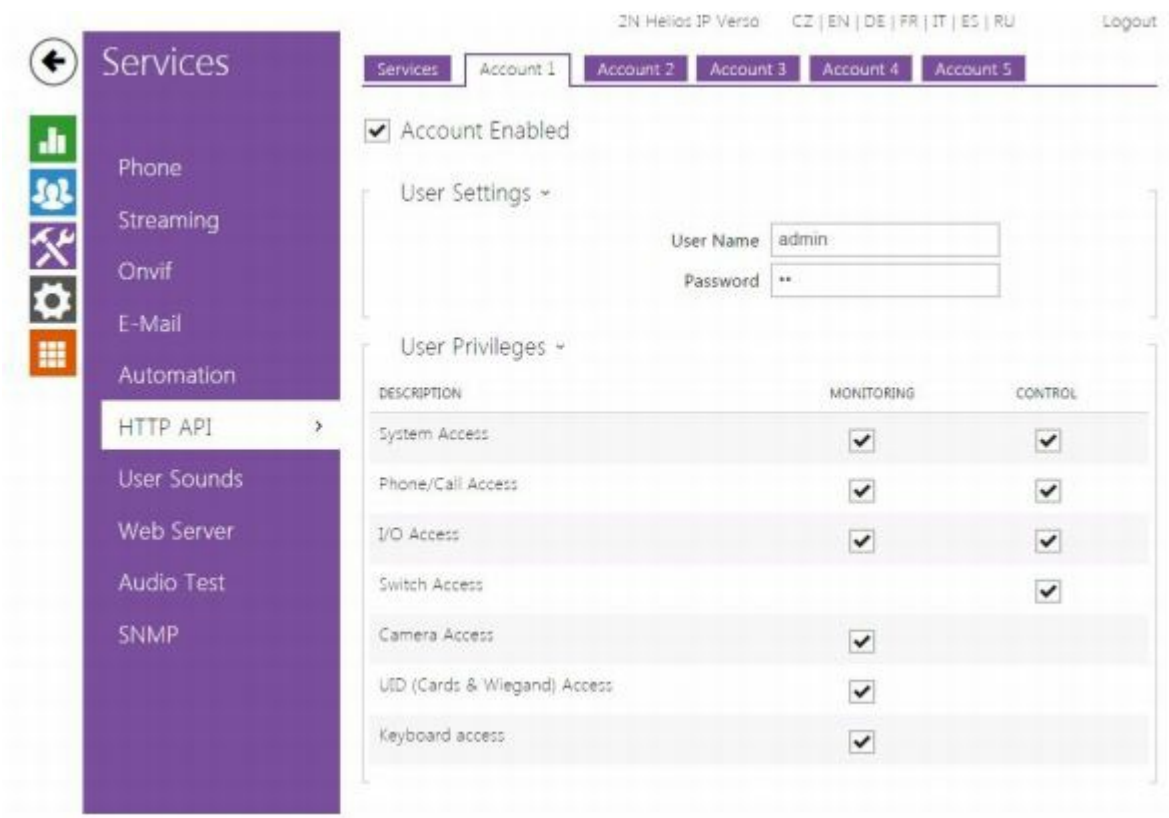
API Access

Make basic configuration after connecting the device to the LAN.Default access values are (Login: admin, Password: 2n). The C4 - 2N communication runs via the intercom HTTP API. Set the API login data and enable the API functions to access this function. Go to the Services menu and select the HTTP API submenu via the 2N web interface. Enable the functions, select the TCP connection type and set the authentication type to None or Basic as shown in the figure below. The HTTPS protocol is not supported.



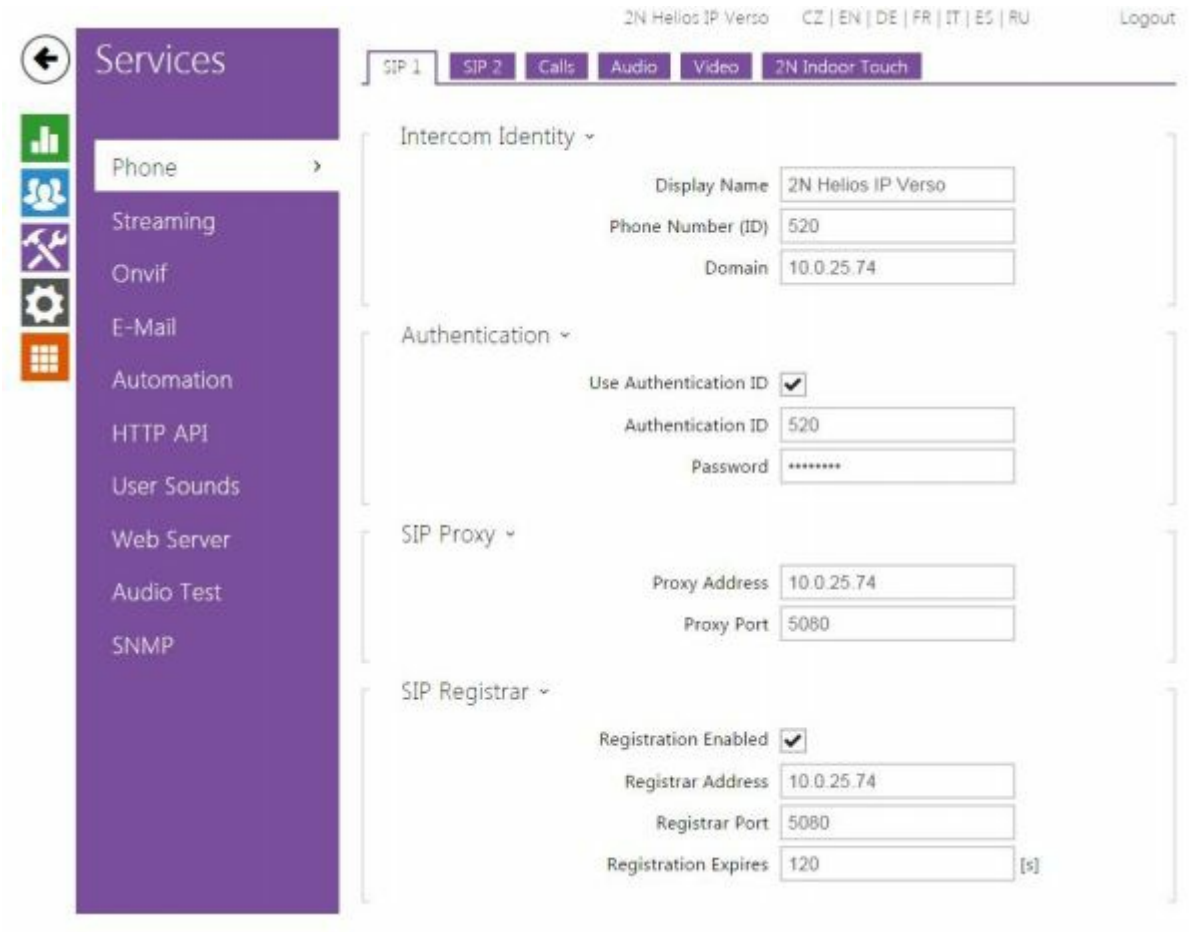
Now switch the tab to Account 1 and enable the account. The HTTP API login data settings are optional and need not be completed. Select User rights in the User Settings as shown in the figure below and save the changes. You can set Authentication as a None or Basic (User and password protected). If some parts of HTTP API is inaccesible, than it will be displayed in Device tree in black color. Example of unsupported Switch API is on following picture.

Settings of User Privileges for Account is also important. If you have only monitoring enabled, then you can see statuses only and sending commands will end with error.



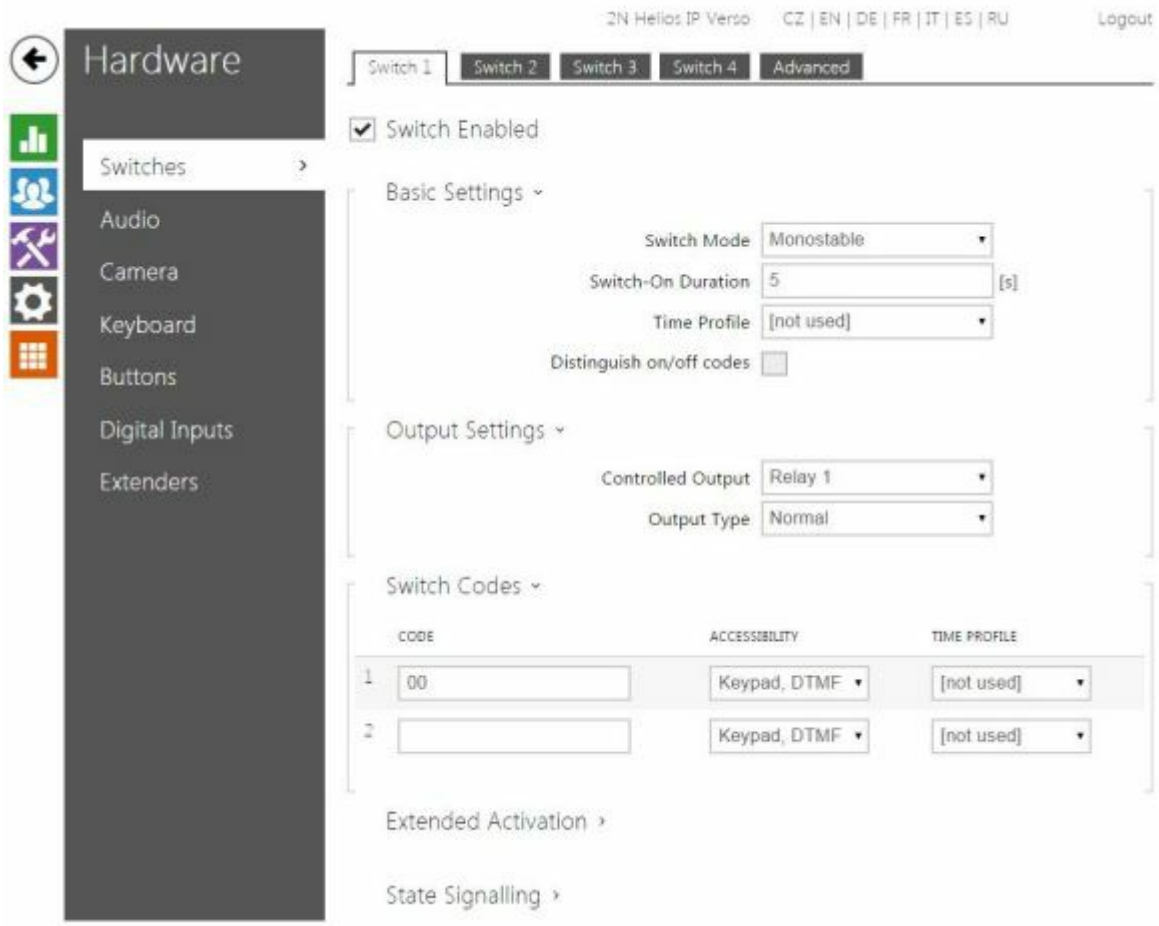
SIP Account Setting

Set the SIP account in the intercom to enable outgoing calls to a defined phone number. Select Telephone in the Services menu. Refer to the figure below for an example of functional setting.



Switch Settings

Set the 2N switch controlling parameters as shown in the figure below.



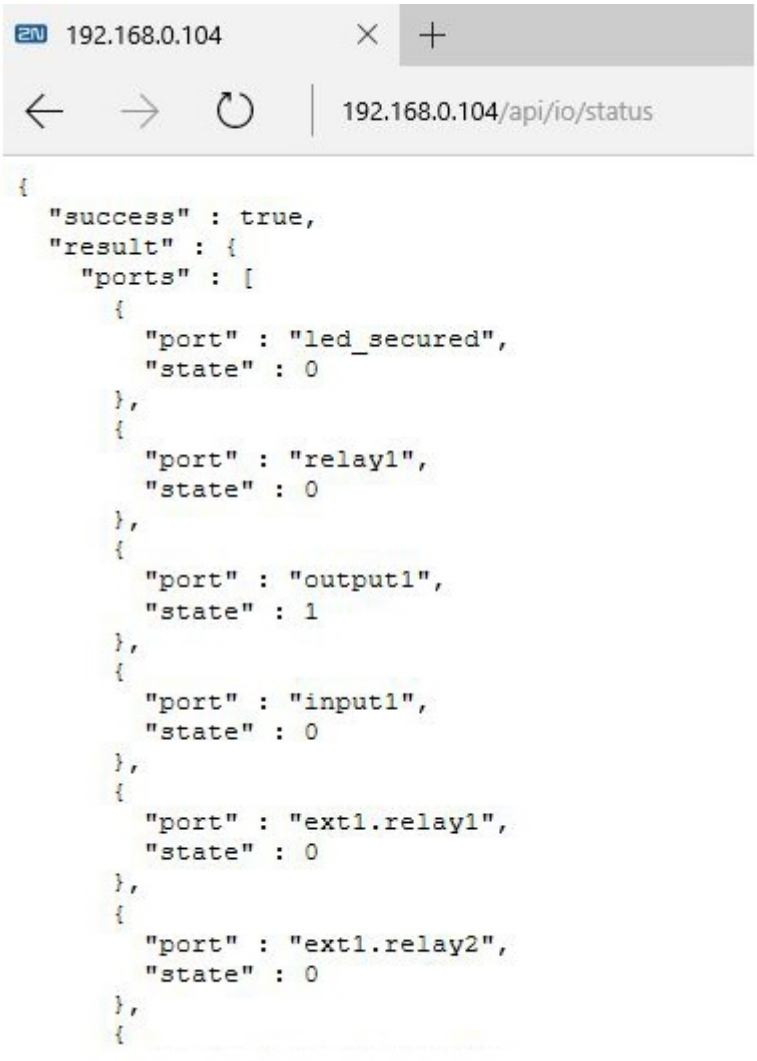
How to find PortName for Input and Output

PortName configuration parameters determine physical port on HW. Unfortunately there is no way how to find exact value in classical web interface on 2N device. Use API call /api/io/status in your browser to find value. You can find PortName values right from “port”.

Note: Webbrowser can ask for API login credentials to perform api command. API login credentials are stored in device web (Service -> HTTP API ->Account 1 - Account 5)

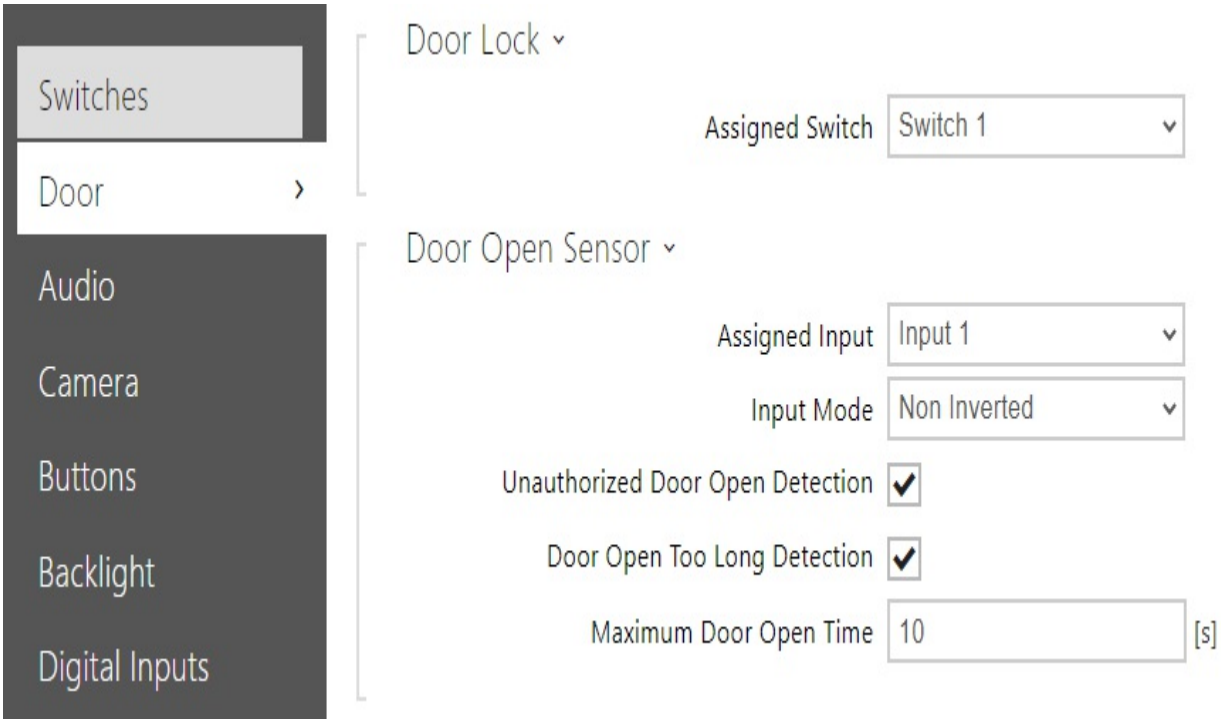
Switch function on 2N device must be enabled. Refer to product documentation to proper device configuration.

Example in MS Edge browser:



Door Settings

In order for the door node in C4 to correctly reflect the status of the actual door, it is necessary to set up the 2N device in the following way:



Namely it is necessary to set the "Door Open Sensor" -> "Assigned Input" to the actual connected input in the 2N device. In this example it is "Input 1". Then the C4 will reflect the door state based on the state of the selected digital input.

Credentials support

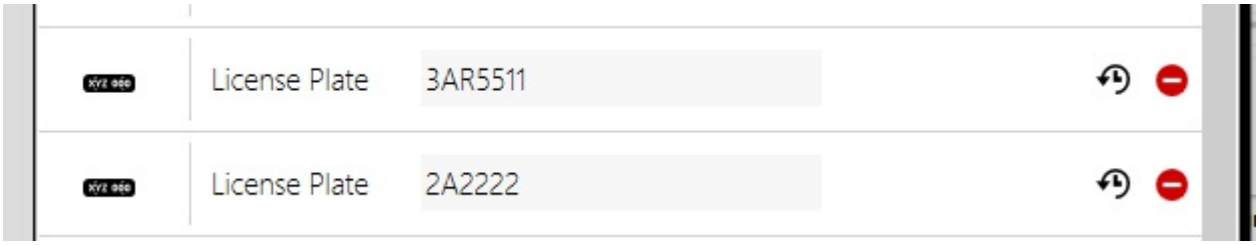
- Only two cards for one user are enabled. The device supports credentials with 6 to 32 hexadecimal characters. The card number is always padded by the driver with zeroes to always accomodate at least 6 digits.
- Only one PIN for one user is enabled (Pin is stored to User Switch Codes - Switch 1)
- Only two fingerprints are allowed for each user. In case there are more fingerprints enrolled, the driver will upload only two leftmost ones. A warning is generated in the Event log

License Plates support

Since firmware version 2.33, the 2N devices support new type of credential - license plates.

Credential management

The LPRs from C4 will be uploaded to 2N device as credentials during full/incremental uploads. The license plates are entered as individual entries to C4:



The license plates can be reviewed in the 2N's address book in the following section:

In the 2N's address book the license plates are merged into one common text field.

License plates recognition

The 2N device itself is not able to recognize license plates from a video source. A third-party device/software needs to be utilized.

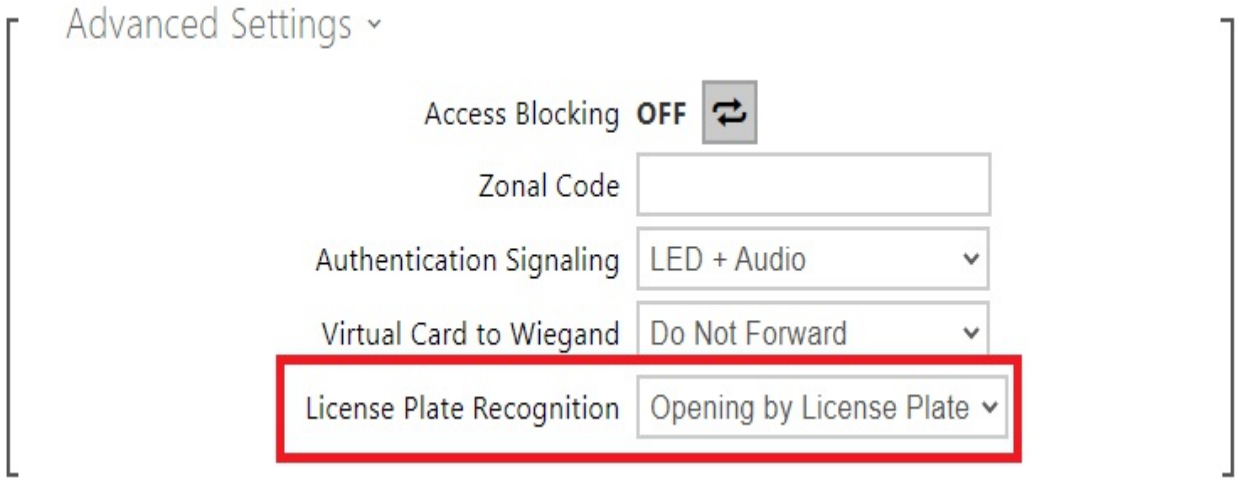
The recommended hardware and software equipment is the following:

- AXIS camera capable of running external applications (e.g. P3245-LVE-3, P1445-LE-3, etc.), firmware >= 8.4.0
- AXIS License Plate Verifier application, version >= 2.1-0

The application in the camera needs to be set in the following manner in order to successfully send recognized LPRs to the 2N device:

The image on the left shows an example setting of the applicatic
In your environment, the IP address, user and password need to
The user provided needs to have the right "License Plate R
Services -> HTTP API menu of the 2N device.

In order for the license plates to work as a credential, one must enable the License Plate Recognition in the Door -> Entry Rules/Exit Rules menu:

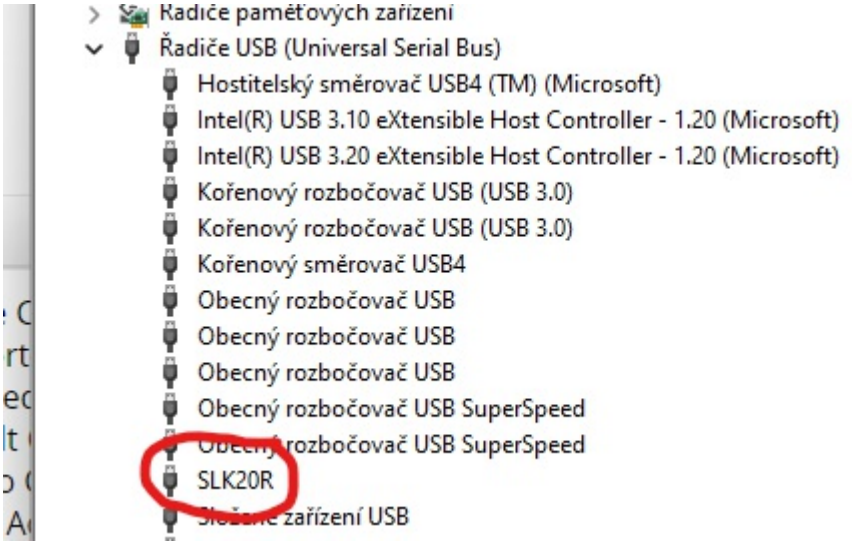


After these settings, the AXIS camera alongside with the installed application will send recognized license plates to the 2N devices. In the 2N device, the license plates will be then evaluated against the uploaded credentials.

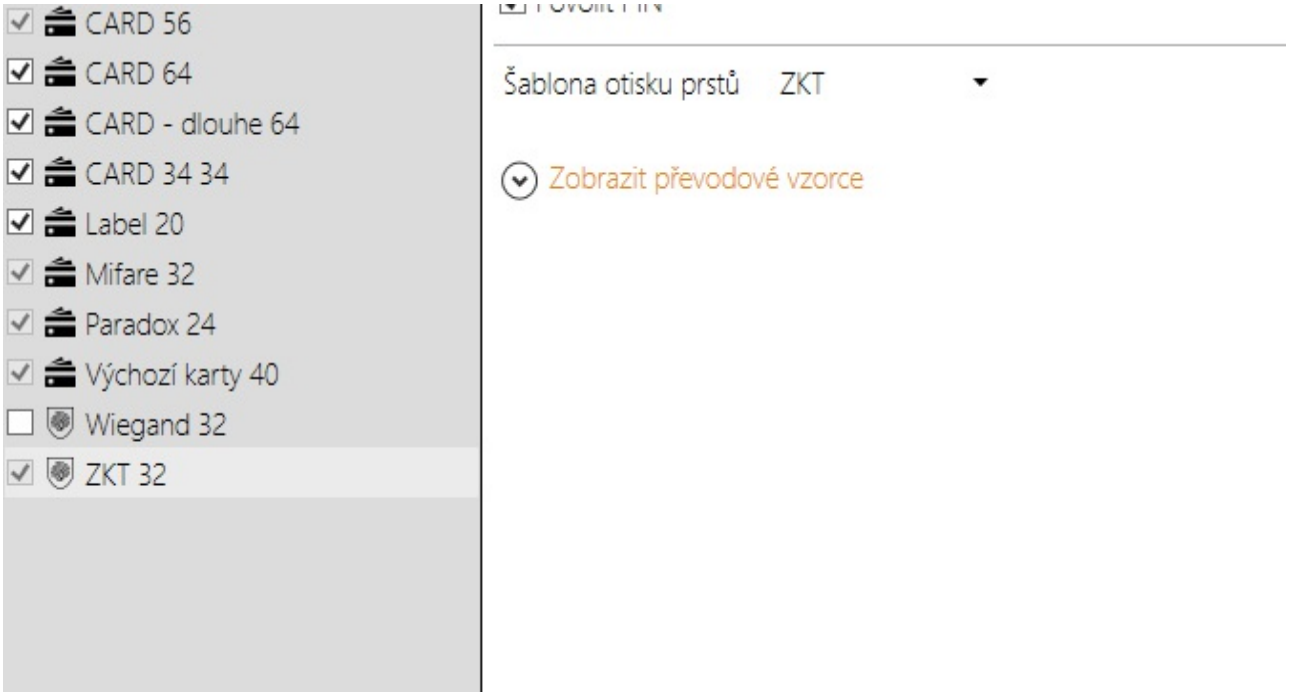
Fingerprint support

In case the device supports fingerprint access (AccessUnit 2.0 or another device equipped with fingerprint reader module), the fingerprints templates may be uploaded from C4.

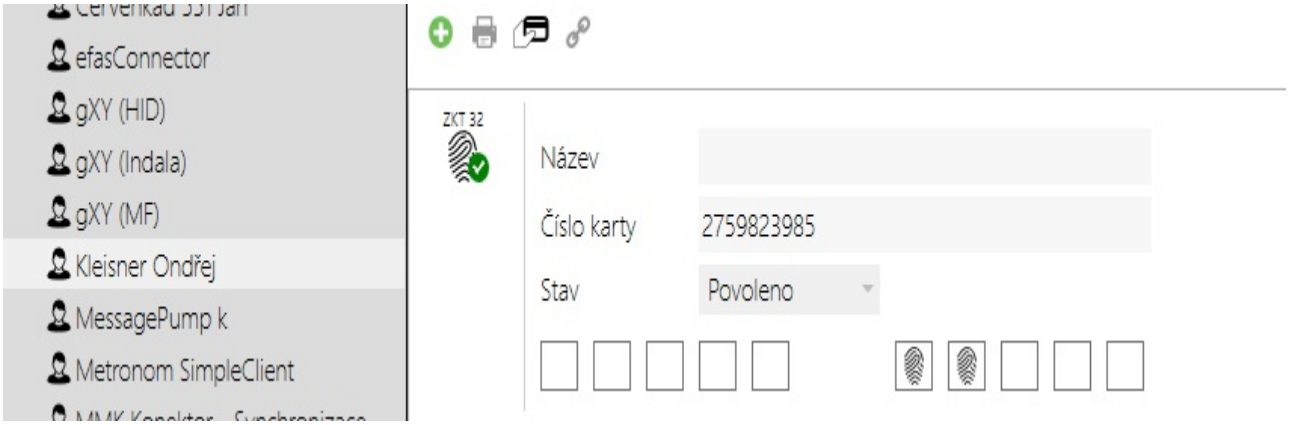
The recommended USB reader to input fingerprints into C4 is **ZKTeco SLK20R** (by using another device, the functionality cannot be guaranteed). Once plugged into the computer, a driver from 2N webpage should be downloaded (https://www.2n.com/en_GB/products/external-fingerprint-reader-usb-interface) and installed. Correctly attached device looks in the Windows Device Manager like this:



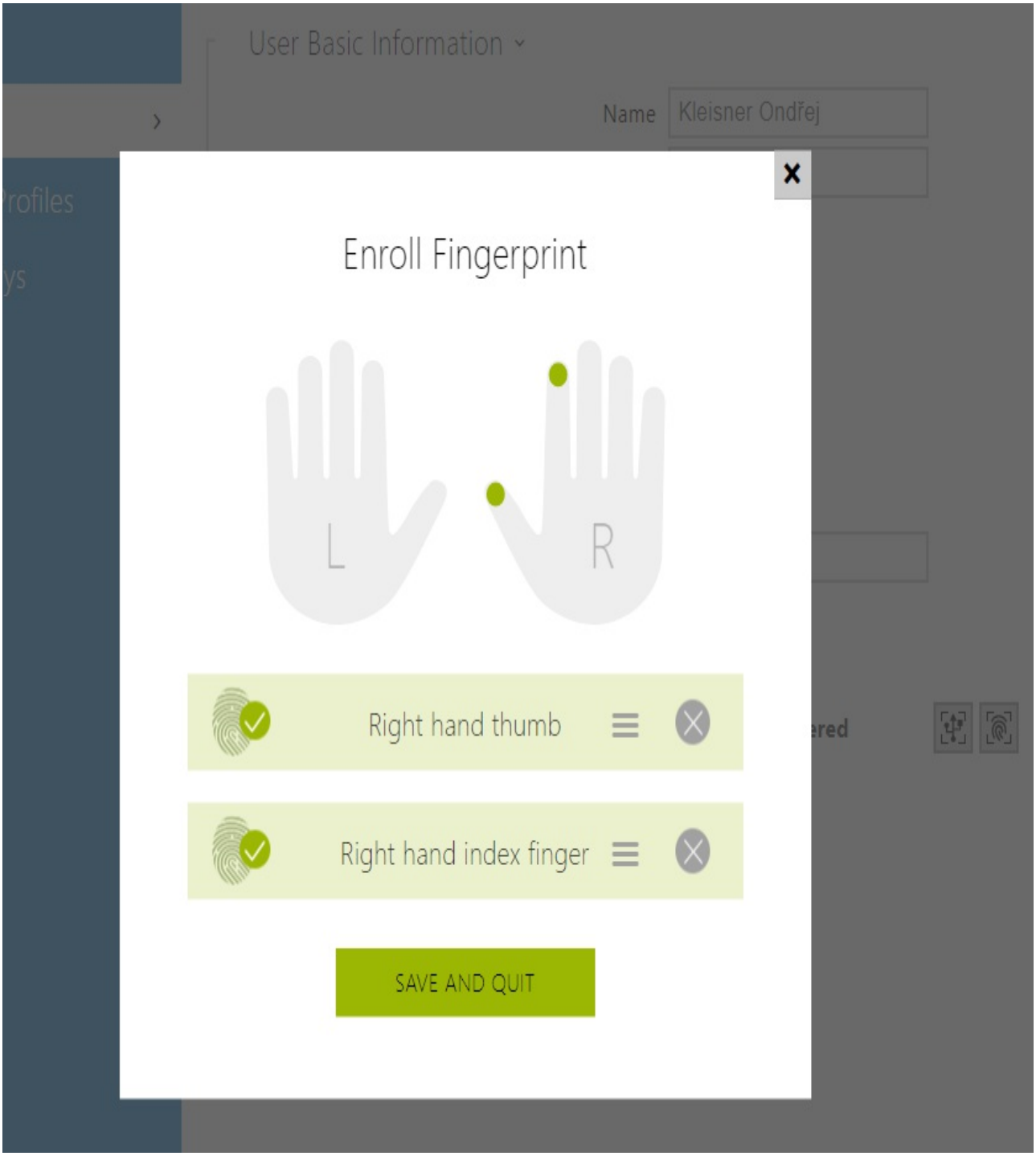
Next, follow the manual for installing ZKTeco driver into C4. Following this step, create a new Credential Type and select ZKT as template:



Then, a new set of fingerprints may be enrolled to a person in C4 using the aforementioned USB reader. The generated card number is irrelevant as it is not sent to the 2N device.



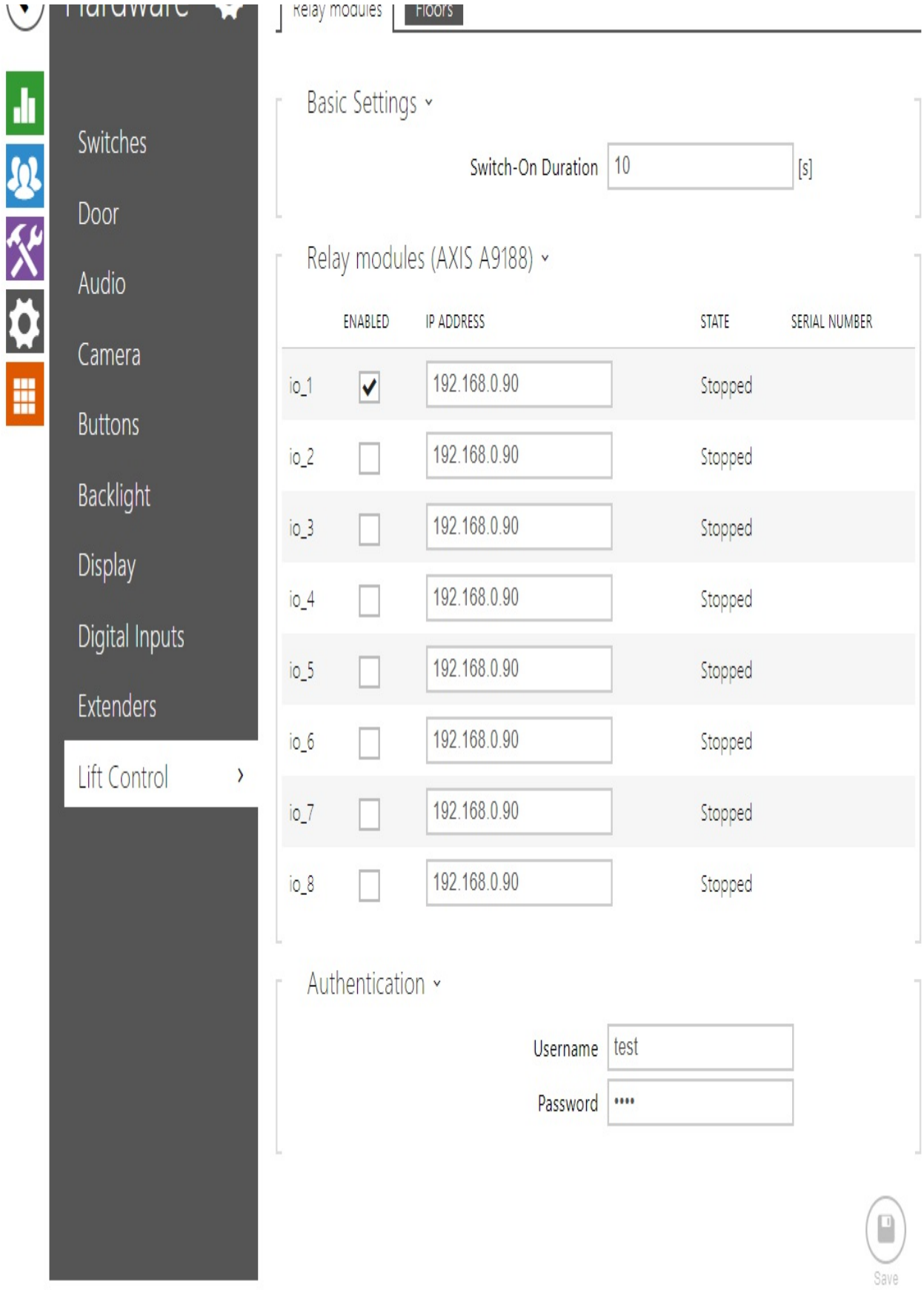
When a credential upload is performed into the device, one can see that the user record has been updated and the fingerprints are present:



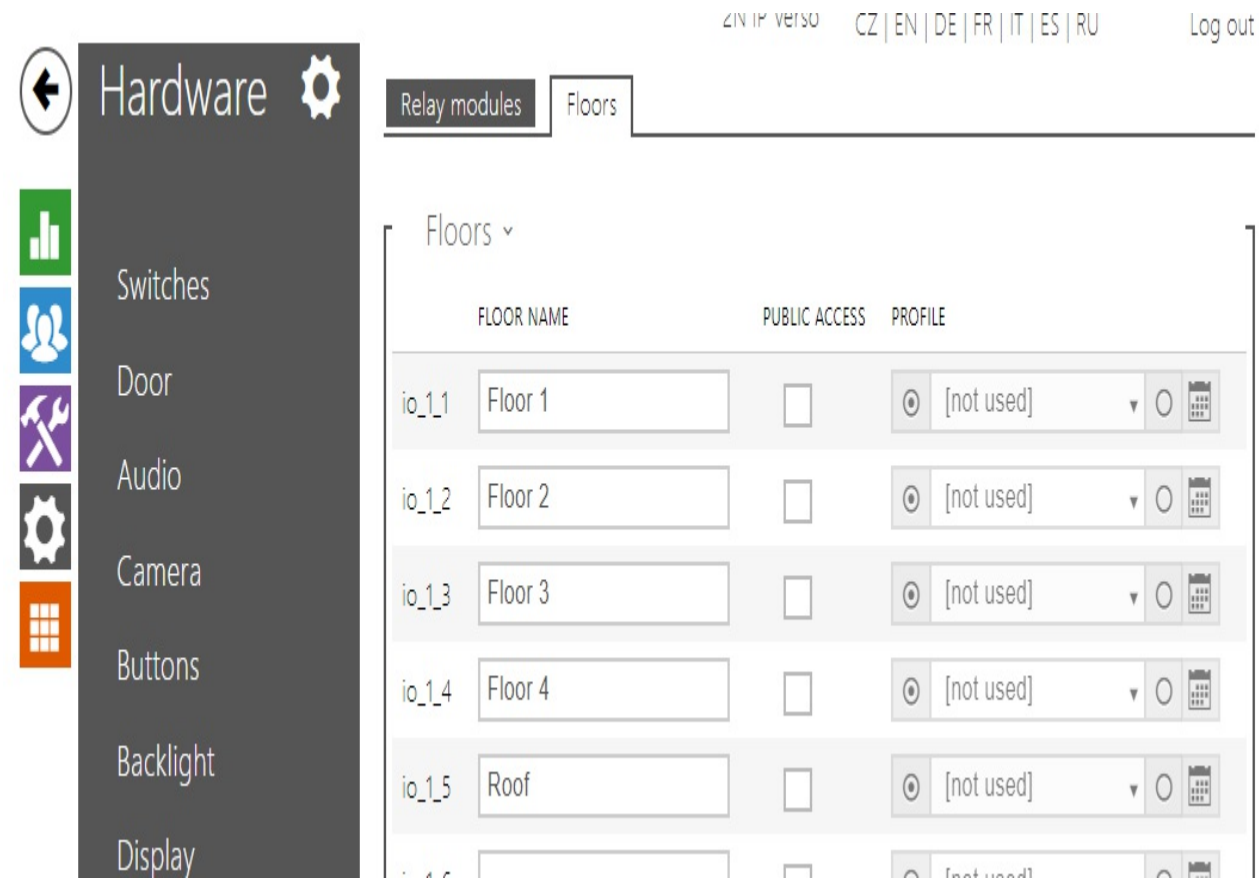
Lift Control support

The driver supports definition of lift and floors. The device tree in C4 must correspond to the lift setting in the 2N device.

In the Hardware -> Lift Control menu of the 2N device, the administrator defines connected AXIS relay module(s) that is responsible for powering relays, thus enabling lift floor controls.



On the next menu - Floors - the administrator defines the actual floors that can be accessed.



Note the hardware addresses of the floors (i. e. io_1_1), this is the address inputted into C4.

Access for individual people is then set on the individual floors. The state of the floors is always active, this is because the 2N device does not posses any information whether the attached relay modules are online.

In case of access granted event, this event is recorded to all allowed floors as well as to the implicit doors. This is due to the fact that the device possesses only one reader.

WaveKey Bluetooth

The driver supports uploading of 2N WaveKey Auth ID into 2N devices. For this to work a credential type with 64bit facility code and 64bit card code needs to be present in C4 and allowed for the device.

Upon uploading the driver recognizes this card type and uploads the Auth ID into a different section of 2N than a

standard access card.

For the WaveKey to be funcional across multiple devices, it is essential that all the devices have the same "Location ID" and they share the same Encryption Keys for Location.

Configuration

2N

- This is *root device*.

PROPERTY	RANGE	DEFAULT
Persons Management		Enabled
Disable/Enable persons management		
Timeout For Response From The Device	0 - 4,294,967,295	10000
General timeout of communication in ms		
IP Address	IPv4 address format xxx.xxx.xxx.xxx	
IP address of device		
Account		
2N HTTP API access user name		
Password		
2N HTTP API access password		
Enabled	True/False	True
Driver enable/disable		
CreateEventsForInvalidLicensePlates	True/False	False
This property controlls what recognized license plates raise C4 event. If unchecked, only recognized license plates followed by an access granted event are stored. If checked, all recognized license plates are stored.		
MaxDateTimeDifferenceBetweenC4AndDeviceMs		5000
Upon starting the driver, it is checked, whether the difference between time in the device and time on the C4 server is not greater than this parameter in milliseconds. In case it is, a device event is raised.		

Door

- This device can be added under device *2N*.

PROPERTY	RANGE	DEFAULT

Phone

- This device can be added under device *2N*.

PROPERTY	RANGE	DEFAULT

Phone number

- This device can be added under device *Phone*.

PROPERTY	RANGE	DEFAULT
PhoneNumberForSendCallDial	PhoneNumberSelector	PhoneNumber
Selection of default phone number for the given SIP account		
PhoneNumber		
Phone number for destination call. (1005, sip:200@192.168.1.1)		
PhoneNumberParallelCallIndicator	true/false	
Indicator whether to include this phone number in the group calling		
PhoneNumber2		
Phone number for destination call. (1005, sip:200@192.168.1.1)		
PhoneNumber2ParallerCallIndicator	true/false	
Indicator whether to include this phone number in the group calling		
PhoneNumber3		
Phone number for destination call. (1005, sip:200@192.168.1.1)		
PhoneNumber3ParallelCallIndicator	true/false	
Indicator whether to include this phone number in the group calling		
DeputyName		
Name of the SIP account to which the call will be routed in case of inaccessibility		
ButtonPosition		1
Indicates to what hardware button of the device this SIP account should be assigned		
TimeProfileNumberIn2N_1	1-20	
Number representing Time Profile in 2N device which should be assigned to this phone number. The number is 1-based. When empty or equal to zero, the property will not be used and there will be no time profile set for this phone number.		
TimeProfileNumberIn2N_2	1-20	
Number representing Time Profile in 2N device which should be assigned to this phone number. The number is 1-based. When empty or equal to zero, the property will not be used and there will be no time profile set for this phone number.		
TimeProfileNumberIn2N_3	1-20	
Number representing Time Profile in 2N device which should be assigned to this phone number. The number is 1-based. When empty or equal to zero, the property will not be used and there will be no time profile set for this phone number.		
DisplayPosition		/
If the device has a Display extender, this property represents positions of an entry in the directory on the display. According to the 2N API manual, the entries can be as following: 1) The default position is in the root folder. This position is achieved by simply entering only one slash. EXAMPLE: / shows the entry in a root folder 2) An entry may be positioned on a display several times - the positions are separated with a semi-colon (;). EXAMPLE: /Folder1/;/Folder2/ shows the entry both in Folder1 and Folder2		

Card Reader

- This device can be added under device *Door*.

PROPERTY	RANGE	DEFAULT

Input

- This device can be added under device *Door*.

PROPERTY	RANGE	DEFAULT
PortName		
Identification of input on 2N device		

Output

- This device can be added under device *Door*.

PROPERTY	RANGE	DEFAULT
PortName		
Identification of output on 2N device		

Switch Output

- This device can be added under device *Door*.

PROPERTY	RANGE	DEFAULT
SwitchNumber	SwitchNumbers	None
Identification of Switch in 2N device		

Group of lift floors

- This device can be added under device *2N*.

PROPERTY	RANGE	DEFAULT

Lift door

- This device can be added under device *Group of lift floors*.

PROPERTY	RANGE	DEFAULT
Address		
The address of the floor as defined in the 2N device in the menu Hardware -> Lift Control -> Floors		

Defined Enumerations

PhoneNumberSelector

- Used by Phone number > PhoneNumberForSendCallDial.

Value	Description
PhoneNumber	
PhoneNumber2	
PhoneNumber3	

SwitchNumbers

- Used by Switch Output > SwitchNumber.

Value	Description
None	
Switch1	Identification of Switch1
Switch2	Identification of Switch2
Switch3	Identification of Switch3
Switch4	Identification of Switch4

Difference between Switch and output

Main purpose of Switch is providing simple control of door lock via time limited impulse. This impulse can be defined in device settings (web device interface: Hardware - Switches).
Main purpose of Output is direct control of relay in device by commands Open and Close.

Limitations of Person Management Systems in this driver

- Only two cards for one user are enabled
- Only one PIN for one user is enabled (Pin is stored to User Switch Codes - Switch 1)

Integration Tests

Test	Name	Result
Supported Functionality > Card Learning		
T09UVU	Personal Management - Card Learning	✔ Passed
Supported Functionality > Access Time Restriction		
T09LQY	Personal Management - Access Time Restriction	✔ Passed
Supported Functionality > Holidays Support		
T09XRR	Personal Management - Holiday Support	✔ Passed
Supported Functionality > Pin Management		
T09VMN	Personal Management - Pin Management	✔ Passed
Supported Functionality > Card Management		
T09IND	Personal Management - Card Management	✔ Passed
Supported Functionality > Fingerprint Management		
T09EZJ	Personal Management - Biometric - Fingerprint Comment: fingerprint reader required	✔ Passed
Supported Functionality > Remote Device Control		
T04XSI	Output Inhibit and Uninhibit Remotely From C4 Comment: not supported by the device	⊘ Not supported
T08ARF	Door Lock and Unlock Comment: not supported by the device	⊘ Not supported
T08LON	Door Remote Open Comment: Open Commmand is not for door, but for output and switch output	⊘ Not supported
Device Category > ACS		
T08FDN	Door Open Permanently Comment: Command doesn´t exist for Open. For this use case is output	⊘ Not supported
T08ICK	Door Forced Open	✔ Passed
T08JRH	Door Open Too Long	✔ Passed
T08OCH	Request to Exit Button Comment: not supported by the device	⊘ Not supported
T09CRN	Personal Management - Handling Access Granted Event	✔ Passed
T09UPY	Personal Management - Antipassback Forgiveness Comment: not supported by the device	⊘ Not supported
T0BBCP	Duress Alarm Comment: not supported by the device	⊘ Not supported
T0BHSL	Tamper Comment: not supported by the device	⊘ Not supported
T0FAFL	Unified Time Management - Time Synchronization When Changed on Device Comment: not supported by the protocol, the API does not support time synchronization	⊘ Not supported
T0FCVB	Contact Monitoring from Device Comment: This is not supported by driver	⊘ Not supported
T0FLFU	Activating Test Mode on Detector from Device Comment: not supported by the device	⊘ Not supported
T0FQCA	Mains Failure Comment: not supported by the device	⊘ Not supported
T0FVUH	Activating Test Mode on Detector Remotely from C4 Comment: not supported by the device	⊘ Not supported
T0FWIK	Unified Time Management - Time Synchronization on Driver Startup	⊘ Not supported

	Comment: not supported by the protocol, the API does not support time synchronization	
T0FYDS	Unified Time Management - Periodical Synchronization Comment: not supported by the protocol, the API does not support time synchronization	⊘ Not supported
T0FYGI	Battery Failure Comment: not supported by the device	⊘ Not supported
T2FESO	Device Audit Log Retrieval Comment: not supported by the device	⊘ Not supported
T3FIGI	Output Activation and Deactivation	✔ Passed
T7FHSW	Missing HW Item Comment: The test is not supported due to communication protocol limitations.	⊘ Not supported
T7FKUJ	Device Auto import Comment: not supported by the protocol	⊘ Not supported
Device Category > Other		
T7FHSW	Missing HW Item Comment: The test is not supported due to communication protocol limitations.	⊘ Not supported
T7FKUJ	Device Auto import Comment: not supported by the protocol	⊘ Not supported

Appendix A

Integration Tests

T08ICK - Door Forced Open

This test verifies behavior of the driver implementation for remote controlling of doors

This test focuses on handling events and statuses during the unauthorized opening of the door in a protected system.

Test Steps

Activate door contact

Expected Results

1.Door status is set to Forcibly open

Following events are stored in audit log:

```
Door 'DEVICE' forced open.
```

Where

DEVICE represents the door name

T08JRH - Door Open Too Long

This test verifies behavior of the driver implementation for remote controlling of doors.

This test focuses on handling events and states during the held open alarm on the door.

Test Steps

Use the credential to access the access point
Activate door contact
Keep the contact activated longer than the predefined time

Expected Results

After successful credential authorization, the door status is set to Unblocked.
Door status is set to Open when the door contact is activated.
After predefined open time expiration, the door status is set to OpenTooLong.

Following events are stored in audit log:

```
'DEVICE' opened by 'PERSON'.
Door 'DEVICE' open too long.
```

Where

DEVICE represents the door name
PERSON represents the name of person who used authorized credential

T09CRN - Personal Management - Handling Access Granted Event

This test verifies behavior of the driver when receiving the access granted event from the device.

Test Steps

Create new person
Assign the person a valid credential
Grant the person access to the access point
Send credentials to the device
Use the credential to access the access point

Expected Results

Person got access to specific access point
Access point status is set to Unblock

Following events are stored in audit log:

```
Access granted to 'PERSON' at 'DEVICE'
```

Where

PERSON represents the name of person who get access to device
DEVICE represents the door name

T09EZJ - Personal Management - Biometric - Fingerprint

This test verifies behavior of the driver implementation for transferring the fingerprint template credentials into the device memory, allowing to define access permissions based on them.

Test Steps

Create new person
Grant the person access to the access point
Assign valid Fingerprint to this person
Send credentials to the device
Check, whether the definitions were transferred correctly by using finger on fingerprint reader.

Expected Results

Person has correctly defined permissions in a device

Following events are stored in audit log:

```
'PERSON' cleared access data on 'DEVICE'
Access granted to 'PERSON1' at 'DEVICE1'.
```

Where

PERSON represents a name of person who executed the command
PERSON1 represents a name of person who used credentials on access point
DEVICE represents the device where the credentials are sent into
DEVICE1 represents a name of access point

T09IND - Personal Management - Card Management

This test verifies behavior of the driver implementation for transferring the card credentials into the device memory, allowing to define access permissions based on them.

Test Steps

Create new person
Grant the person access to the access point
Assign valid Card to this person
Send credentials to the device
Use the credential to access the access point

Expected Results

Person has correctly defined permissions in a device

Following events are stored in audit log:

```
'PERSON' cleared access data on 'DEVICE'
Access granted to 'PERSON1' at 'DEVICE1'.
```

Where

PERSON represents a name of person who executed the command
PERSON1 represents a name of person who used credentials on access point
DEVICE represents the device where the credentials are sent into
DEVICE1 represents a name of access point

T09LQY - Personal Management - Access Time Restriction

This test verifies behavior of the driver implementation for time limited access scenarios, allowing to update the device configuration in that a way, that the access can be limited to some specific hours and/or days of the week.

Test Steps

Create new person
Assign the person a valid credential
Grant the person access to the access point
Restrict the access permission with time restriction
Send credentials to the device
Check whether the restriction is applied correctly

Expected Results

The assigned time restriction is correctly applied
When person has no limitation in access it gets access granted event. When person has limited access by time restriction it gets access denied event.

Following events are stored in audit log:

```
'PERSON' cleared access data on 'DEVICE'
Access granted to 'PERSON1' at 'DEVICE1'.
Access denied to 'PERSON1' at 'DEVICE1'. Reason: Active time restriction
```

Where

PERSON represents a name of person who executed the command
PERSON1 represents a name of person who used credentials on access point
DEVICE represents the device where the credentials are sent into
DEVICE1 represents a name of access point

Notes:

Some devices might impose limits on the complexity and/or amount of available time restrictions.These limits must be enumerated in test notes and validated during this test.

T09UVU - Personal Management - Card Learning

This test verifies behavior of the driver when device provides enough information about the unknown card, that card information can be constructed from these data and new card can be created in a system.

Test Steps

Create new person
Execute Learn Card feature on this person
Choose correct device for card learning
Slide the card on this device

Expected Results

A card of device supported type is created and assigned to the person

Following events are stored in audit log:

```
'PERSON' created Card 'CARDNAME' into 'DECK'.
'PERSON' activated 'CARDNAME' to 'PERSON1'.
```

Where:
PERSON represents a name of person who is executing the command
PERSON1 represents a name of person who got card assigned to
CARDNAME represents a name of card with it's card number
DECK represents a name of card deck

Notes:

Some devices might have some limitations in providing information abut the unknown card
Valid only on devices providing enough information about the unknown card, that the card information can be constructed from these data and new card can be created in a system

T09VMN - Personal Management - Pin Management

This test verifies behavior of the driver implementation for transferring the PIN credentials into the device memory, allowing to define access permissions based on them.

Test Steps

Create new person.
Grant the person access to the access point
Assign valid PIN to this person
Send credentials to the device
Check, whether the definitions were transferred correctly – either by reading the device memory directly or by proving operation on the device

Expected Results

Person has correctly defined permissions in a device.

Following events are stored in audit log:

```
'PERSON' cleared access data on 'DEVICE'
'AREA' was armed by 'PERSON1'.
```

Where

PERSON represents a name of person who executed the command
PERSON1 represents a name of person who used credentials on access point
DEVICE represents the device where the credentials are uploaded into
AREA represents the name of area

Notes:

Some devices might have some limitations in PIN length or some rules to define valid PIN.

T09XRR - Personal Management - Holiday Support

This test verifies behavior of the driver implementation for manipulation with a list of holidays in the device, allowing to define the different rules for holidays than for normal working days or weekends.

Test Steps

Create new person
Assign the person a valid credential
Create holiday set, containing the todays date
Send credentials to the device
Check whether the restriction is applied correctly
Modify holiday set that it doesn't contain todays date
Send credentials to the device
Check whether the restriction is applied correctly

Expected Results

1.The assigned time restriction is correctly applied

Following events are stored in audit log:

```
'PERSON' cleared access data on 'DEVICE'.
```

Where

PERSON represents a name of person who executed the command
DEVICE represents the device where the credentials are uploaded into

Notes:

Some devices might impose limits on the complexity and/or amount of available time restrictions.These limits must be enumerated in test notes and validated during this test.

T3FIGI - Output Activation and Deactivation

This test verifies behavior of the driver implementation for output contact monitoring and controlling support.

Test Steps

Execute command “On” on output.
After the output is opened, execute command “Off” on it.

Expected Results

When output is activated, its status is Open.
When output is deactivated, its status is Normal.

Following events are stored in audit log:

```
'PERSON' sent command 'On' to 'DEVICE'.
'DEVICE' opened.
PERSON' sent command 'Off' to 'DEVICE'.
'DEVICE' closed.
```

Where

PERSON represents the name of person who executed the commands
DEVICE represents the output name