



Technical Documentation: 2N License

Link'nX

X

2N



Contents

- 1 License 2N** **3**
- 1.1 Add a license to the Link'nX gateway 3
- 1.2 Pre-configuring the 2N device 3
 - 1.2.1 Configuring the HTTP API Service 4
 - 1.2.2 Configuring the HTTP API account 4
- 1.3 2N device declaration 5
- 1.4 2N action creation 7
- 1.5 2N trigger creation 8

- 2 Appendix** **9**
- 2.1 2N action list 9
- 2.2 2N trigger list 10

1 License 2N

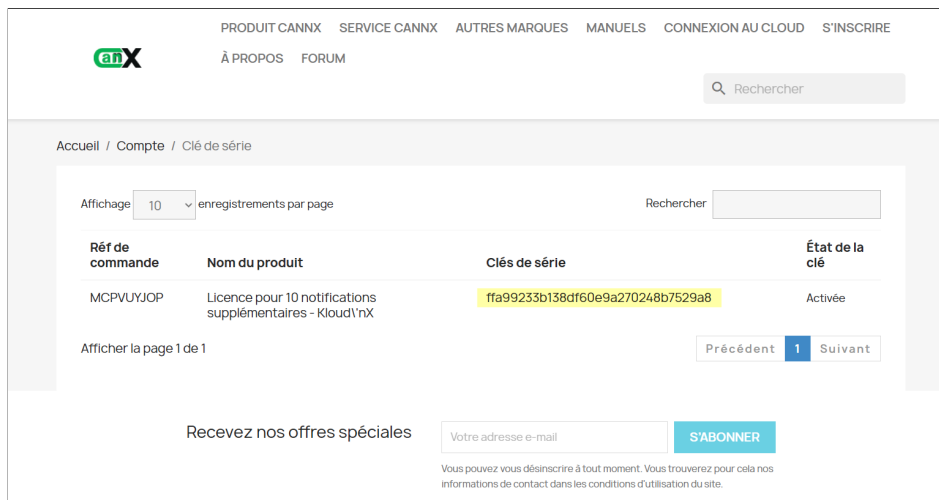
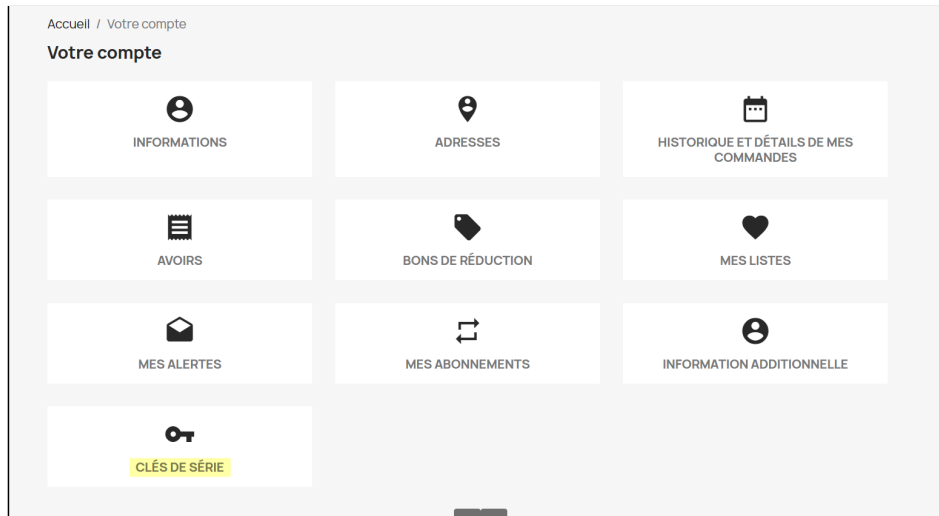
Link'nX can interact with 2N equipment. By registering a 2N device in advance, it is possible to send and receive commands such as opening a door or locking a gate. This section will talk in detail about what you can do/create by interacting with a 2N device.

1.1 Add a license to the Link'nX gateway

Licences can be added to your project to enhance the functionality of your Link'nX gateways.

To add a licence, go to [Can'nX](#), then click on the **"Add an extension"** button in the options of the project containing the Link'nX. Then enter the key in the field and confirm.

To retrieve your key after a purchase, you need to go to the www.can-nx.shop site, to your account. A "Serial key" button allows you to display the list of keys you have purchased.



1.2 Pre-configuring the 2N device

To enable Link'nX to communicate with the 2N device, it is important to set up the 2N device correctly. To do this, access the interface by entering the IP address of the 2N device in your browser's

URL.

Once you have logged in, go to the "Services" page.

1.2.1 Configuring the HTTP API Service

Link'nX and the 2N device communicate using the HTTP API system provided by 2N. These services must therefore be enabled (checked box):

1. Switch API. Allows Link'nX to send commands to the 2N device in order to control the switches.
2. Logging API. Enables Link'nX to retrieve events occurring on the 2N device (code entry, call, door opening, etc.).

Each service can choose an authentication protocol (None, Basic, Digest) and this information will be useful for Link'nX. Link'nX will not be able to communicate with the 2N device if their identification protocol is different.

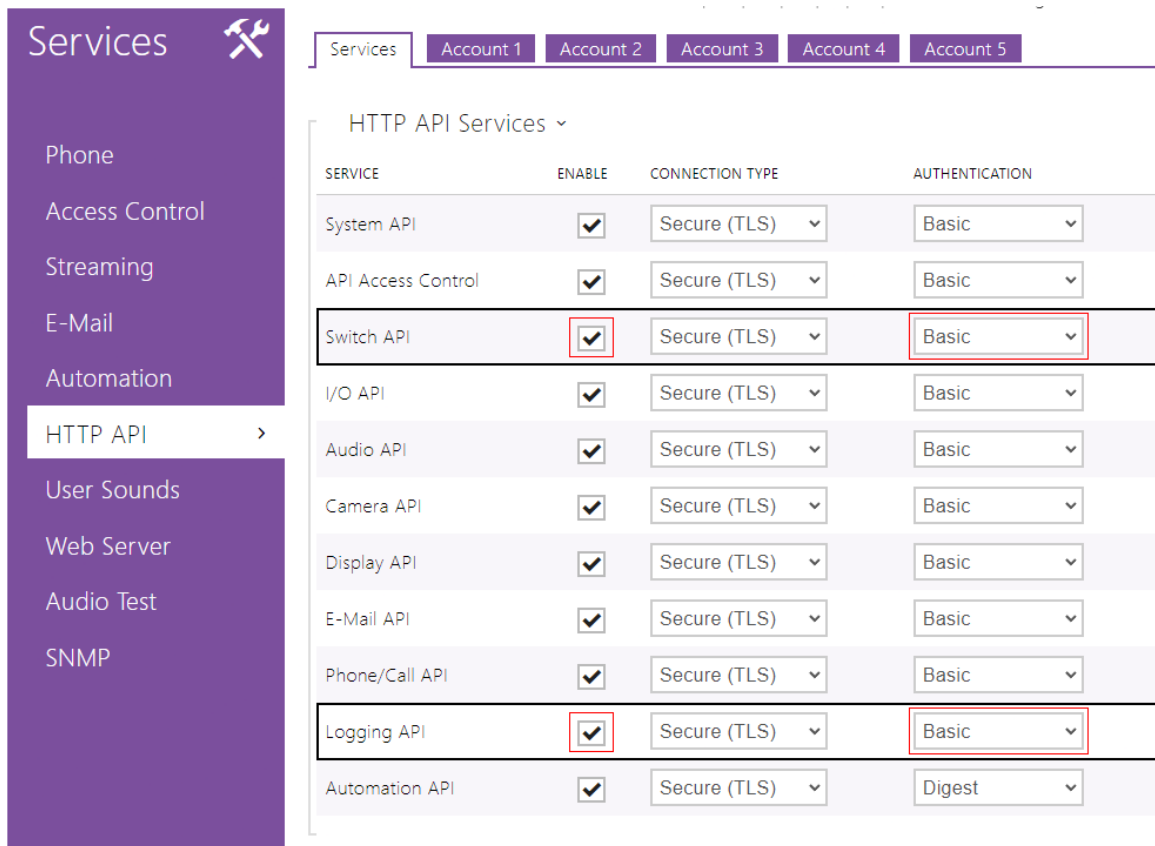
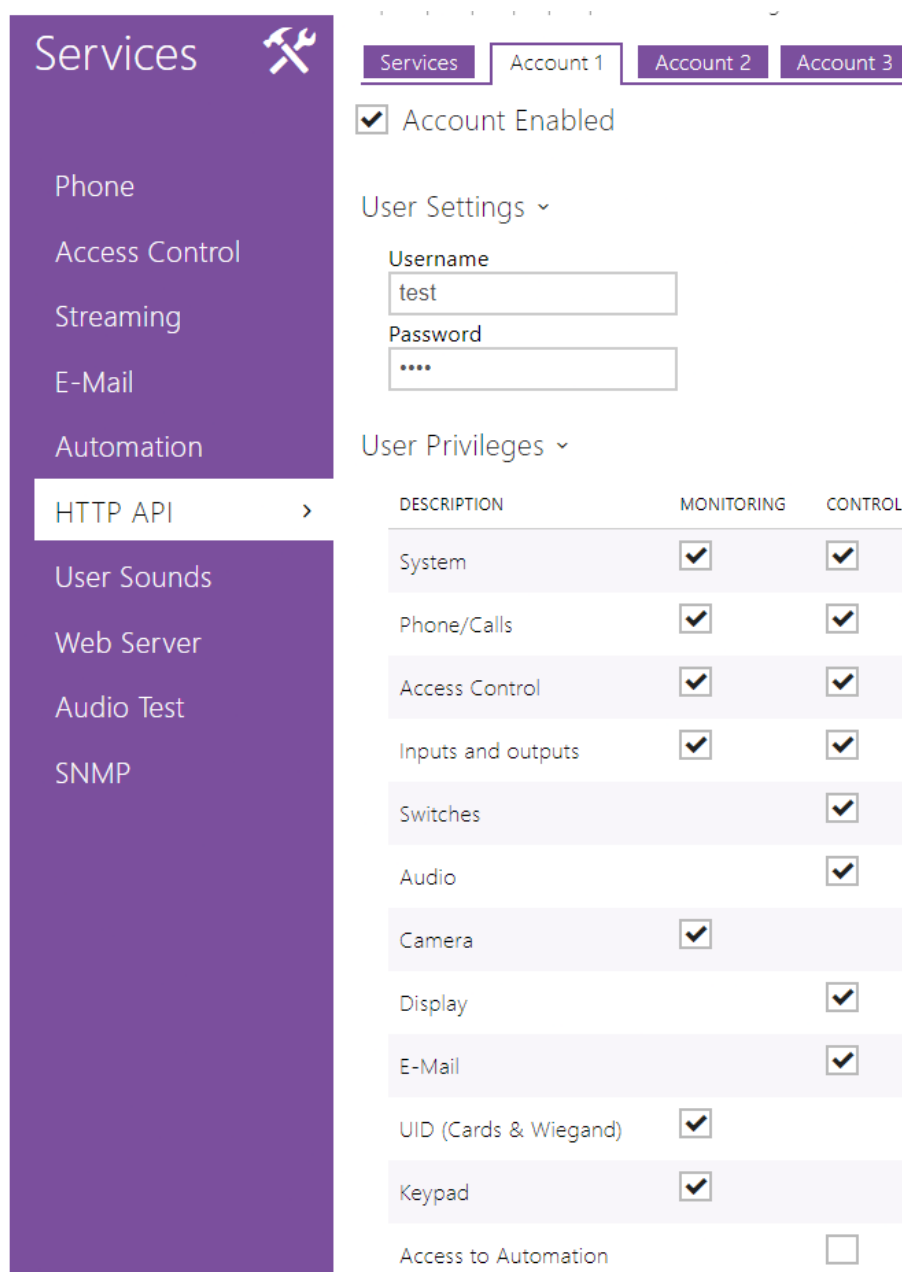



Figure 1: Services API HTTP configuration 2N interface

1.2.2 Configuring the HTTP API account

An account must be set up and activated, and must also have the relevant user privileges activated.



Services 

Phone

Access Control

Streaming

E-Mail

Automation

HTTP API >

User Sounds

Web Server

Audio Test

SNMP

Services Account 1 Account 2 Account 3

Account Enabled

User Settings ▾

Username
test

Password

User Privileges ▾

DESCRIPTION	MONITORING	CONTROL
System	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Phone/Calls	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Access Control	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Inputs and outputs	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Switches		<input checked="" type="checkbox"/>
Audio		<input checked="" type="checkbox"/>
Camera	<input checked="" type="checkbox"/>	
Display		<input checked="" type="checkbox"/>
E-Mail		<input checked="" type="checkbox"/>
UID (Cards & Wiegand)	<input checked="" type="checkbox"/>	
Keypad	<input checked="" type="checkbox"/>	
Access to Automation		<input type="checkbox"/>

Figure 2: Account API HTTP configuration 2N interface

1.3 2N device declaration

The declaration of a 2N device is made on the page dedicated to 2N. To access this page, the user must open the navigation menu and click on the "2N" option, which is slightly detached from the main Link'nX group.

< 2N Declaration

- 1 Name *
2N Office ×
*Required 9/64
- 2 IP address *
192.168.1.1 ×
*Required
- 3 Username *
username ×
*Required
- 4 Password *
..... 🔒
*Required
- 5 Switch authentication method *
Basic ▼
- 6 Log authentication method *
Basic ▼
- 7 Import configuration
- 8 🔒

Figure 3: 2N device declaration form

1. 2N device name
2. 2N device IP address
3. API http account username. (see [1.2.2](#))
4. Password for http API account. (see [1.2.2](#))
5. Authentication method for "Switch API" HTTP API services. In the 2N device configuration interface, the service must be enabled. (see [1.2.1](#))
6. Authentication method for HTTP API "Registration API" services. In the 2N device configuration interface, the service must be enabled. (see [1.2.1](#))
7. Import of the 2N XML configuration file. Downloadable from the 2N interface System – Maintenance – Back Up configuration.
By importing a configuration file, the Name (1) and IP Address (2) fields will be filled in automatically. The list of user names (3) will be retrieved and auto-completion will be proposed.

The list of users is also extracted to propose an auto-completion when a 2N trigger is created. The same applies to authentication methods (5) and (6).

8. Save - Register the 2N device.

Once the device has been registered, it will appear in the list of 2Ns. Each device will have its name, IP address, the username of the account used, and information about whether a configuration file has been imported.







Name	IP address	Username	Configuration file	
2N Bureau 3eme	192.168.10.2	test		 
2N Office	192.168.1.1	username		 

Figure 4: List of registered 2N devices

1.4 2N action creation

< Action creation

- 1 Select an action type
2N
- 2 Name *
Name of the 2N action
*Required 21 / 64
- 3 2N Device *
2N Office
*Required
- 4 Device/Element number (door, gate, ...) *
1
*Required
- 5 Action *
Open
*Required


6 

Figure 5: 2N action form

1. Action type. Select "2N" to create a 2N action.
2. Name of the 2N action.
3. Selected device(s) to be controlled by the action. Several devices can be selected. The action command (4) will be executed for each device.

4. Switch number that needs to be controlled by that action.
5. Order to be carried out on the selected device(s).
6. Save - Register the 2N action.

1.5 2N trigger creation

< Trigger creation

- 1 Select a trigger type
2N
- 2 Name *
Name of 2N trigger
*Required 18 / 64
- 3 2N Device *
2N Office
*Required
- 4 Event *
Code entered

Event conditions

- 5 Code entered
1234
- Code validity
- User ID
Stephan

- 6

Figure 6: 2N trigger form

1. Trigger type (Select 2N for a 2N trigger).
2. Trigger name.
3. 2N device on which the user wishes to interact (retrieve events).



4. 2N event to be monitored by Link'nX. If the selected event occurs at 2N level (e.g. Code entered), the trigger will be activated. The list of available events is detailed in the [Appendix](#).
5. Optional parameter(s) for the selected event (4). These parameters act as conditions to be met before the trigger is activated.
 If no parameter is specified, the trigger will be activated each time the selected event (4) is received.
 If one or more parameters are specified, the event will have to validate all of them for the trigger to be effective (e.g. a code is entered and must be exactly "1234", or the code corresponds to user "X").
 The list of available events and their parameters is detailed in the [Appendix](#).
6. Save - Register the 2N trigger.
 A description of each item is displayed by hovering over the options (4) (5).

2 Appendix

2.1 2N action list

Open

Activates / opens the selected switch

Parameter name	Expected value	Description
-	-	-

Close

Deactivates / closes the selected switch

Parameter name	Expected value	Description
-	-	-

Lock

Locks the switch. A locked switch will remain deactivated/closed and will only react to the "Unlock" action.

Parameter name	Expected value	Description
-	-	-

Unlock

Unlocks the switch. Allows normal operation after a lockout.

Parameter name	Expected value	Description
-	-	-

Hold-open the door

Places the switch in a 'held' state where it will remain on/open. A 'held' switch will only respond to the 'Lock' and 'Release hold-open' actions.

If the switch is both locked and held, it will be considered locked (priority state). When unlocked, the switch will always be in a "held" state.

⚠ When using it to hold a door strike open, check that it is capable of withstanding this condition over time. The equipment could be damaged if this is not the case.

Parameter name	Expected value	Description
-	-	-

Release / cancel hold-open

Releases the switch from its 'held' state. Allows normal operation after a 'held' state.

Parameter name	Expected value	Description
-	-	-

2.2 2N trigger list

Device state

Signals changes in device status. Generated once after device start-up (always the first event).

Parameter name	Expected value	Description
-	-	-

Motion detected

Signals the detection of movement by a camera. The event is only available for models equipped with a camera. The event can only be used if the function is enabled in the intercom camera configuration.

Parameter name	Expected value	Description
Motion detector state	[Start of event] [End of event]	Choose between the start of the event (the moment when motion was detected) and the end of the event (no more motion is detected).

Noise detected

Signals an increase in noise level detected by a built-in or external microphone. The event can only be used if this function is enabled in the intercom configuration.

Parameter name	Expected value	Description
Noise detector state	[Start of event] [End of event]	Choose between the start of the event (the moment when noise was detected) and the end of the event (no more noise is detected).

Code entered

Signals the entry of a code using the numeric keypad. The event can only be used on devices equipped with a numeric keypad.

Parameter name	Expected value	Description
Code entered	Whole number	Code that must match the code entered.
Code validity	[Valid] [Invalid]	Used to specify whether the code entered should be valid or invalid.
User ID	Select a user from a drop-down list.	If the code entered is linked to a user, the "Code entered" event returns information about the identified user. A list of users will only be available if a configuration file has been imported for the 2N device.

Card entered

Signals that an RFID card has been tapped/placed on the card reader. The event can only be used with devices fitted with an RFID card reader.

Parameter name	Expected value	Description
Code validity	[Valid] [Invalid]	Used to specify whether the card entered should be valid or invalid.
User ID	Select a user from a drop-down list.	If the card entered is linked to a user, the "Card entered" event returns information about the identified user. A list of users will only be available if a configuration file has been imported for the 2N device.

Logic input changed AND Logic output changed

Signals a change of state of the logic input.

Enter the url:

<IP_Address.2N>/api/io/caps and enter an HTTP API account to obtain a list of available entries.
(E.g: 192.168.8.2/api/io/caps)

Parameter name	Expected value	Description
I/O port logic state	[Valid] [Invalid]	Define whether the port entered should be active or inactive.
I/O port logic state	String of characters.	I/O port name (e.g. led_secured).

Switch state changed

Indicates a change in switch status (active/inactive).

See intercom configuration in Hardware — Switches.

Parameter name	Expected value	Description
Switch number	[1] [2] [3] [4]	Select the switch concerned by this event.
Switch state	[Inactive] [Active]	Define whether the switch should be active or inactive.

Call state changed

Indicates the establishment/change/end of the status of the active call (Connection, Call, Connected, Finished).

Parameter name	Expected value	Description
Call direction	[Incoming] [Outgoing]	Choose whether the call should be incoming or outgoing.
Call state	[Connecting] [Ringing] [Connected] [Terminated]	Select the state of the call you need to be in to activate the trigger. - Connecting: establishment of the current call (outgoing calls only). - Ringing: Ringing. - Connected: call connected. - Terminated: Call terminated.

Tamper switch activated

Signals activation of the self-protection switch / opening of the device cover. A self-protection switch detects any unauthorised opening of the intercom.

Make sure that the auto-protection function is configured in the Hardware → Digital inputs → Security menu.

Parameter name	Expected value	Description
Switch state	[Start of event] [End of event]	Select between the start of the event (when unauthorized opening of the intercom) and the end of the event (when the device cover is closed)

Unauthorized door open

Signals unauthorised door opening.

Ensure that a door open switch is connected to one of the logic inputs and that the function is configured in the Hardware → Digital inputs → Door menu.

Parameter name	Expected value	Description
Unauthorized door opening state	[Start of event] [End of event]	Choose between the start of the event (when the door has been opened without authorisation) and the end of the event (when the door returns to a normal state).

Door open too long

Indicates that the door has been open too long or has not closed within the set time.

Ensure that a door release switch is connected to one of the logic inputs and that the function is configured in the Digital inputs → Door menu.

Parameter name	Expected value	Description
Door state	[Start of event] [End of event]	Choose between the start of the event (the moment when the door is considered to be "open too long") and the end of the event (when the door returns to a normal state).

User authenticated

Signals user authentication and door opening.

The user can be identified by name.

Parameter name	Expected value	Description
User name	String of characters	Name of the user who has been identified. Must correspond exactly to the name stored in the 2N configuration. Auto-completion will be proposed if a 2N configuration file has been imported.
User ID	Select a user from a drop-down list.	If the code entered is linked to a user, the "Code entered" event will return information about the identified user. A user list will only be available if a configuration file has been imported for the 2N device.

Card held (4 seconds)

Indicates that an RFID card has been tapped/pressed and held on the reader for more than 4 seconds.

Parameter name	Expected value	Description
ID du lecteur	String of characters	Name of the reader who read the card. (E.g: ext2)
Validity result	[Invalid] [Valid]	Choose whether the result of the card held should be valid or not.

Silent alarm

Indicates the activation of a silent alarm.

A silent alarm is a burglar alarm that makes no noise that can be heard by the intruder. The alarm emits an audible or visual signal elsewhere and alerts the police. A silent alarm can also be a panic button alarm.

Parameter name	Expected value	Description
-	-	-

REX button activated

Indicates activation of the REX (Request to EXit) button.

Parameter name	Expected value	Description
-	-	-

Access limited

Indicates that the user has been rejected.

Parameter name	Expected value	Description
-	-	-

Finger entered (Biometric digital identification)

Indicates that a finger has been placed on the biometric reader.

Parameter name	Expected value	Description
Fingerprint validity	[Invalid] [Valid]	Select whether the result of the fingerprint reading should be valid or invalid.
User ID	Select a user from a drop-down list.	If the code entered is linked to a user, the event will return information about the identified user. A user list will only be available if a configuration file has been imported for the 2N device.

Mobile key entered (bluetooth)

Signals authentication of a user on the Bluetooth reader.

Parameter name	Expected value	Description
Mobile key validity	[Invalid] [Valid]	Choose whether the Bluetooth scan result should be valid or invalid.
User ID	Select a user from a drop-down list.	If the code entered is linked to a user, the event will return information about the identified user. A user list will only be available if a configuration file has been imported for the 2N device.

DTMF (Dual-Tone Multi-Frequency) code entered

Signals a DTMF (Dual-Tone Multi-Frequency) code during the call.

Parameter name	Expected value	Description
Code validity	[Invalid] [Valid]	Choose whether the DTMF code should be valid or invalid.

Door state changed

Indicates a change in door status (open/closed).

Parameter name	Expected value	Description
Door state	[Opened] [Closed]	Define whether the door should be open or closed.

User rejected

Signals the rejection of user authentication.

Parameter name	Expected value	Description
Rejection reason	[Access point blocked] [Invalid time] [Invalid profile] [Invalid sequence] [Invalid credential] [Authentication inter- rupted] [Timeout] [Switch disabled]	Select the reason for rejection.
User ID	Select a user from a drop-down list.	If the code entered is linked to a user, the "User rejected" event will return information about the user in question. A user list will only be available if a configuration file has been imported for the 2N device