



# **NODER EE12/EWE4**

**IP controller of Access Control and Intruder Alarm Systems**

**Start-up and configuration instruction**

# TABLE OF CONTENTS

<b>TABLE OF CONTENTS .....</b>	<b>2</b>
<b>1. Before starting work .....</b>	<b>3</b>
<b>2. Device description .....</b>	<b>3</b>
<b>3. Noder module configuration .....</b>	<b>3</b>
3.1 System installation .....	3
3.2 Noder Server .....	4
3.3 Noder object .....	6
3.4 Noder controller object .....	7
3.4.1 Action tab .....	8
3.4.2 Communication tab .....	10
3.4.3 Settings tab .....	12
3.4.4 Cards format tab .....	14
3.4.5 OSDP tab .....	15
3.4.6 Others tab .....	16
3.4.7 NRS tab .....	17
3.5 Readers .....	18
3.5.1 Basic settings tab .....	20
3.5.2 Alarm and logs tab .....	22
3.5.3 Others tab .....	26
3.5.4 Online mode and AntiPassBack tab .....	27
3.6 Inputs .....	29
3.6.1 Inputs configuration .....	30
3.6.2 Inputs connection diagrams for Access Control System .....	33
3.6.3 Inputs connection diagrams for Intruder Alarm System .....	35
3.7 Outputs .....	38
3.8 IO16 modules .....	40
3.8.1 IO16 module configuration .....	40
3.8.2 Virtual reader configuration .....	41
3.9 Noder IAS Zone .....	43
<b>4. User management .....</b>	<b>45</b>

## 1. Before starting work

Before starting implementation works, the EE12/EWE4 Network Controller must be correctly installed, connected and running in accordance with TD.

## 2. Device description

The IP Controller of the Access Control System and Intruder Alarm System is an advanced microprocessor I/O device for automated user identification. It can be used in building security systems, access control, time and attendance, hotel and recreational facilities. Leading and managing system is Axxon PSIM platform. Details about starting up, configuring network settings and connecting devices to controller can be found in the technical documentation of controllers.

## 3. Noder module configuration

This chapter will present the start-up and configuration of the Noder module.

### 3.1 System installation

The Noder Access Control and Intruder Alarm Systems operates under the Axxon PSIM platform. The dedicated *NoderEe12.run* module is responsible for communication with the controllers. For proper operation with ACS Noder, the following components must be installed on the server:

**Axxon PSIM-Base version** (version 1.0.0.14 or higher)

**Access Control and Fire Alarm Module** (version 1.0.0.14 or higher) with modules:

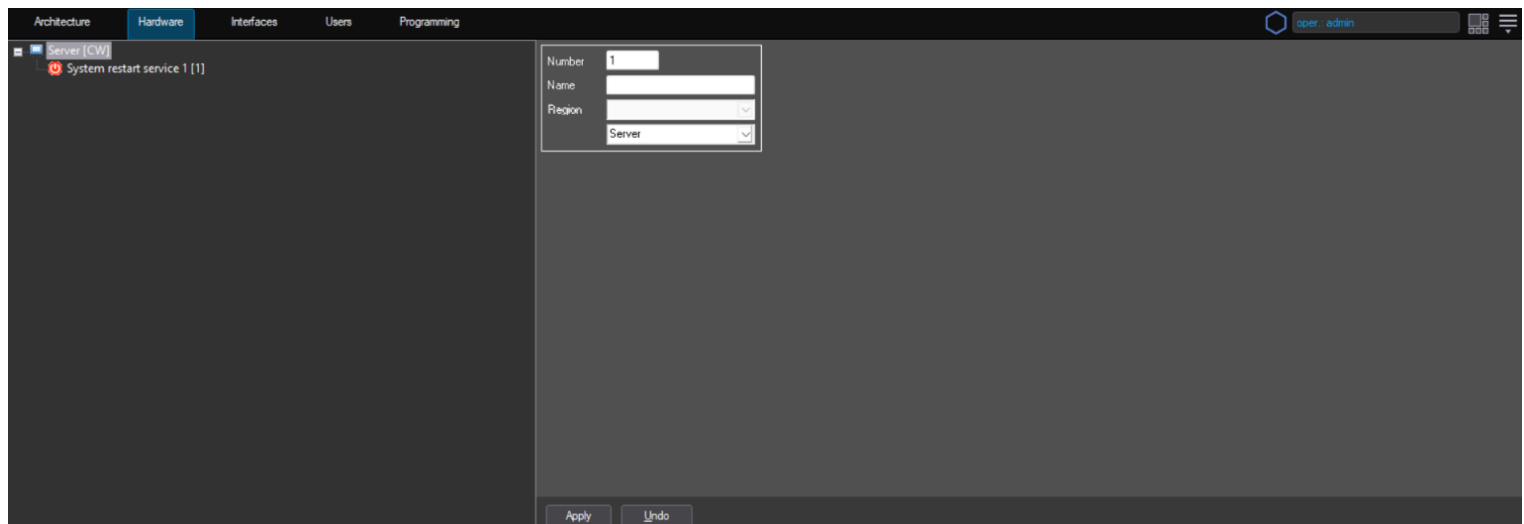
- **Noder EE12/EWE4** from Access Control Systems
- **Access Manager** from Application software

***Intruder Alarm System feature is available only for controllers with motherboards revision at least 1.06 for EWE4 and 1.08 for EE12. Module version at least 2.1.1.204, firmware version at least RC38 2021-06-02 (core update 517).***

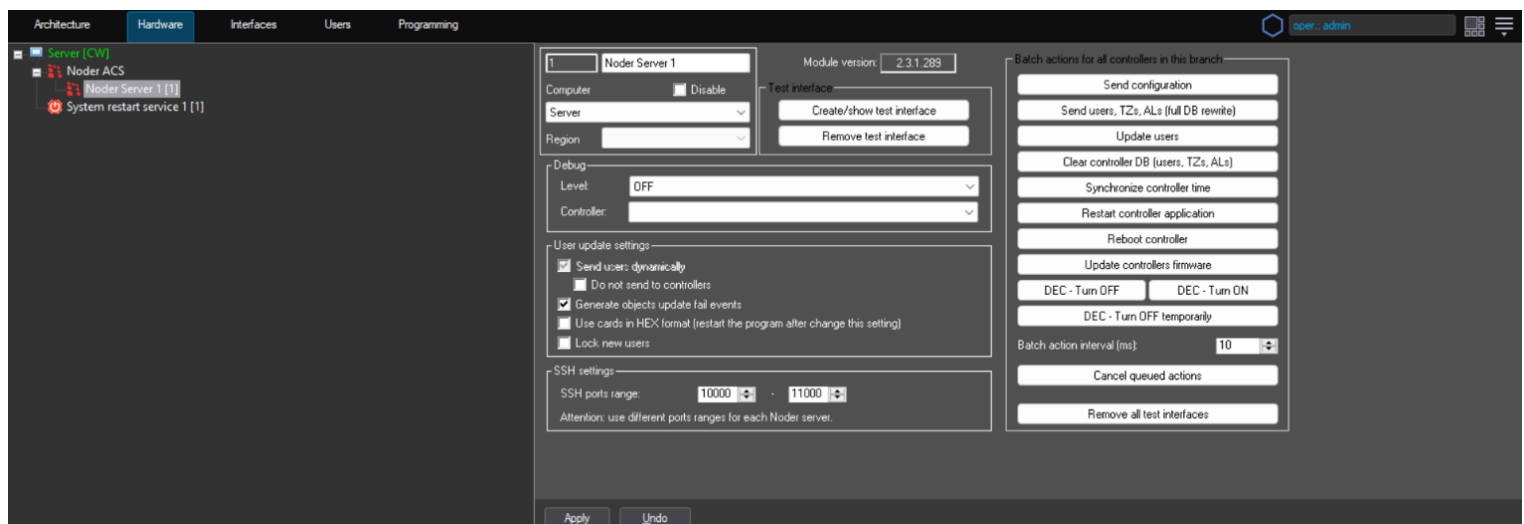
***The manual is compatible with EWE4 controllers with boards from version 1.06 and EE12 controllers with boards from version 1.08. Module version 2.3.1.289 or higher, Controller update ID 1135 or higher.***

## 3.2 Noder Server

Configuration of the Noder system elements takes place from the Axxon PSIM server administration panel. In **Hardware** tab on server where module is to work, we add a new object named **Noder Server** via **Create object** (Right click on **Server object** -> **Create object** -> **Noder Server**). A new object will be created in folder named **ACS Noder**.



**Noder Server** is a module responsible for communication with controllers. **Noder Server** including objects **Noder Object**.



**Debug** – option for programmers allowing to specify certain settings of files containing logs from communication with controller. Option allows to choose:

**Level** – the option allows you to select logs that will be saved in the file.

**Controller** – the option allows to select the controllers from which logs will be saved to the file.

### User update settings:

**Send users dynamically** – this function allows to send automated users and access levels to controllers with each change in Access Manager.

**Do not send to controllers** – this function allows to make changes in users permissions and their access levels, but without automatically applying these changes to the controllers. If this option is selected, user permissions and access levels and schedules will have to be sent manually.

**Generate objects update fail events** – this function allows to generate an additional event after objects update fail.

**Use cards in HEX format** – this function allows to change the notation of card numbers from decimal to hexadecimal.

**Lock new users** – after selecting the option, when creating a new user, the **User blocked** parameter is marked as YES.

### SSH settings:

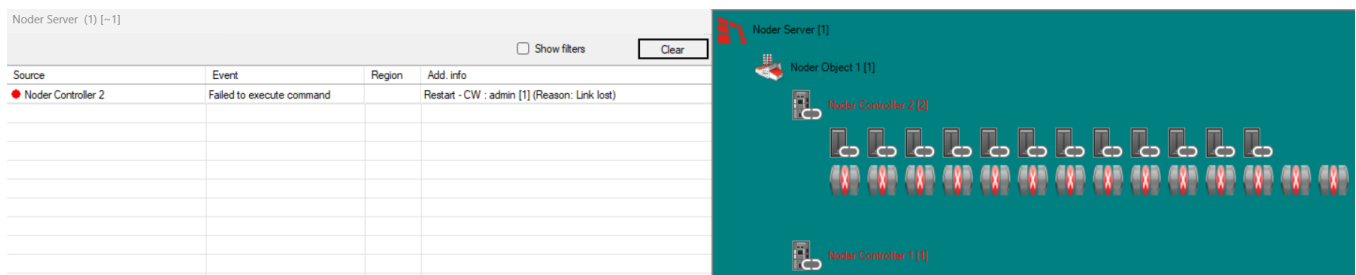
**SSH ports range** – range of ports used for SSH tunnelling.

**Module version** – the field shows the version of the Noder module.

### Testing interface:

**Create/show testing interface** – creates an interface containing a map and events for the object and devices located in its tree. Below is a screenshot of an example test interface.

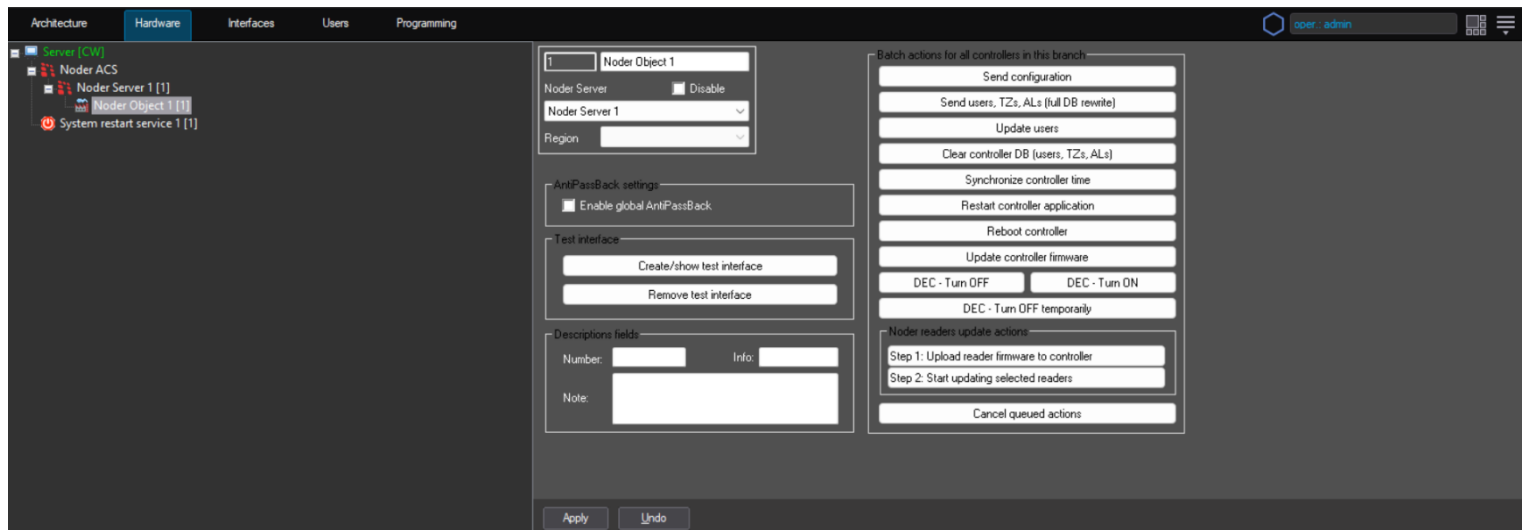
**Remove testing interface** – removes test interface.



**Batch actions for all controllers in this branch** – section allows to perform the selected action on all controllers in the tree with a set time delay. When there are more than 50 controllers in the system, the commands to the next controllers will be sent sequentially. Actions for all controllers in this server described in *Action tab*.

### 3.3 Noder object

**Noder object** is a logical element that allows to divide the system into logical parts (floors, buildings, departments) and manage them.



**Enable global AntiPassBack** - option enables AntiPassBack on the object.

#### Testing interface:

**Create/show testing interface** – creates an interface containing a map and events for the object and devices located in its tree. Below is a screenshot of an example test interface.

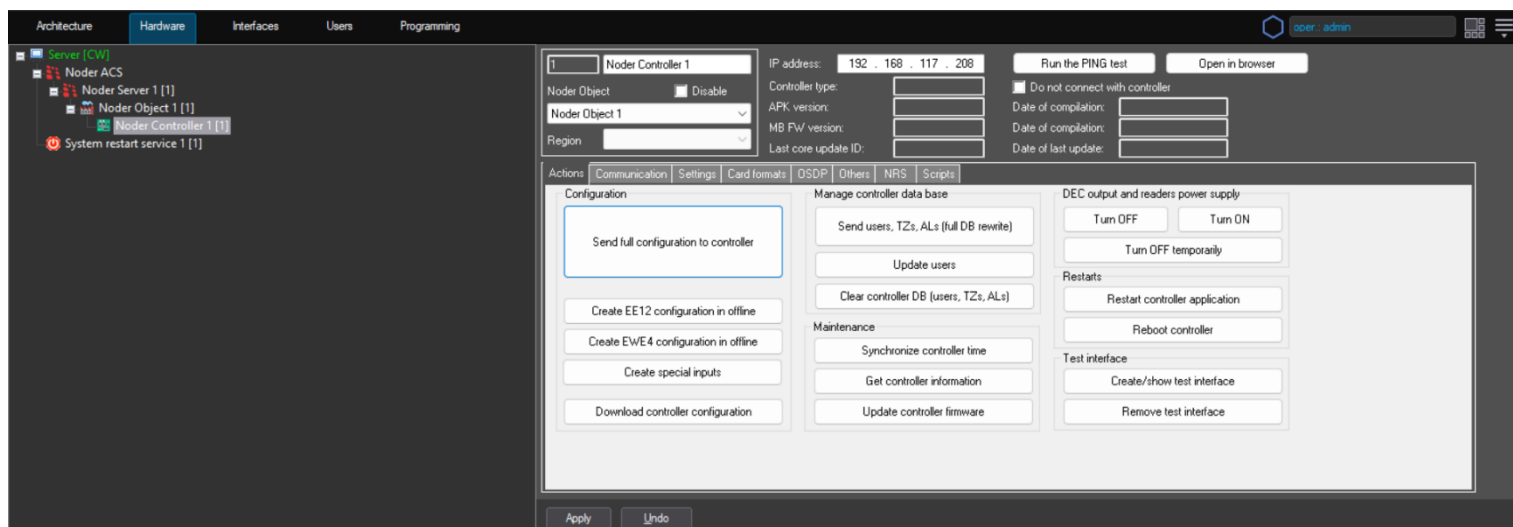
**Remove testing interface** – removes test interface.

**Description fields** - information about object can be stored. Function **does not affect the logic of the controller**.

**Batch actions for all controllers in this branch** – section allows to perform the selected action on all controllers in object. Actions for all controllers in this object described in Action tab.

## 3.4 Noder controller object

The object enables connection with the controller and its configuration.

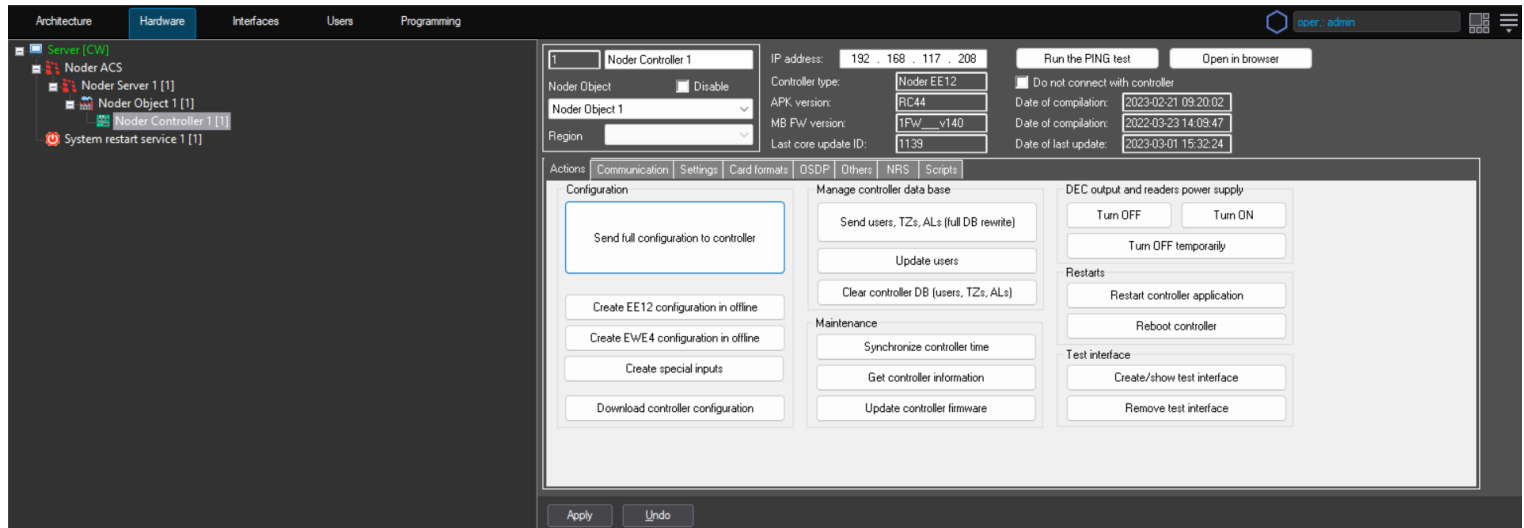


After adding the **Controller object**, configuration interface is displayed. In the **IP address field** enter previously set controller IP address and click **Apply** to send changes. **Run the PING test** runs cmd.exe and monitors the device with the ICMP protocol. **Open in browser** will launch the default web browser in the system and automatically log on to the controller's website.

After the correct connection, fields **APK version**, **uC FW version** with **dates of compilation** and **Last core update ID** with **date of last update**. will be automatically completed by information downloaded from the controller.

### 3.4.1 Action tab

Action tab enable creating, checking and sending controller configuration, and sending users. Tab provide remote controller, devices restart and creation of a test interface.



#### Configuration:

**Send configuration** – sends the current settings contained in the ACS Noder module. The configuration is sent dynamically, that means that all changes that are configured on an ongoing basis are sent to the controller.

**Create EE12 configuration in offline, Create EWE4 configuration in offline** – function of creating a configuration (readers and inputs) in a situation where we do not have a connection to the controller, and we want to configure the system in offline mode in advance.

**Create special inputs** – function of creating objects for special inputs (21-BAT, 22-AC, 23-TMP, 24-DR) and setting default values for purpose described in chapter 3.5.5.

**Download controller configuration** – gets controller's settings. New controller always has a startup configuration, it must be downloaded at the first start. As the work continues, this configuration will change.

#### Manage controller data base:

**Send users, TZs, ALs (clear DB first)** – deletes all users, access levels and schedules in controller, and then saves the entire database again.

**Update users** – sends all changes on users buffered in the ACS Noder module.

**Clear controller DB (users, TZs, ALs)** – deletes all users, access levels and schedules in controller.



## Maintenance:

**Synchronize controller time** – synchronizes the time and date of controller with the management server. This function works automatically when connected to controller and is then called every 4 hours in background.

**Get controller information** – allows downloading from controller information about controller and readers firmware version.

**Update controller firmware** – allows to upload software from indicated folder.

## DEC output and readers power supply:

**Turn OFF** – option used to disable devices powered on controller ports and DEC output.

**Turn ON** – option used to enable devices powered on controller ports and DEC output.

**Turn OFF temporarily** – option used to temporarily disable devices powered on controller ports and DEC output. Time is configurable in Setting tab. This function can be used e.g. for restarting readers.

## Restarts:

**Restart controller application** – restarts the application (APK) responsible for the controller's logic.

**Reboot controller** – full controller reboot.

## Testing interface:

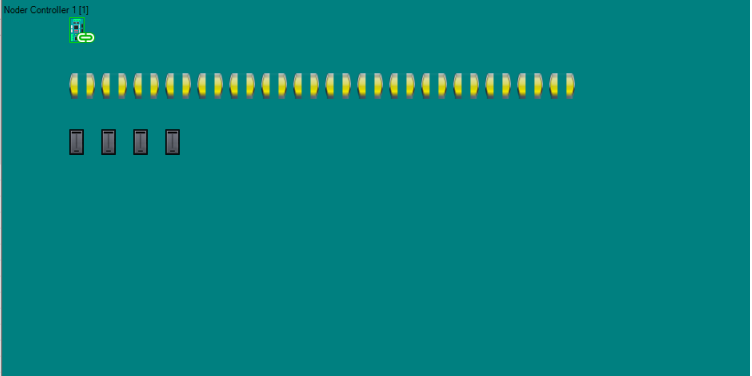
**Create/show testing interface** – creates a controller interface consisting of viewing events related to a given controller and a map with icons of all readers and inputs of a given controller. If such a test interface has been created earlier, the recall of this function will refresh the map according to the current configuration and display interface.

**Remove testing interface** – removes test interface.

An example test interface is shown below:

**Noder Controller 1 (1) [~8]**
☐ Show filters
 Clear

Source	Event	Region	Add. info	Card	Date and time
Noder Control...	Running the command		Send configuration to controller		28.04.2021 15:11:08
Noder Control...	Command executed successfully		Send configuration to controller (Took 2s 667ms)		28.04.2021 15:11:11
Noder Control...	Running the command		Download controller configuration		28.04.2021 15:11:15
Noder Control...	Command executed successfully		Download controller configuration (Took 19ms)		28.04.2021 15:11:15
Noder Reader 1	Command executed successfully		Saving settings in controller		28.04.2021 15:11:16
Noder Reader...	Command executed successfully		Saving settings in controller		28.04.2021 15:11:17
Noder Reader...	Command executed successfully		Saving settings in controller		28.04.2021 15:11:18
Noder Control...	Command executed successfully		Restart		28.04.2021 15:11:23

**Noder Controller 1 [1]**


## 3.4.2 Communication tab

Tab is used to configure connection, firewall and secure SSH tunneling.



### TCP/IP connection settings:

**TCP port** – port 7000 used for TCP connection with controller.

**Connection timeout [s]** – maximum time of waiting controller's response during connection. Decrease this time for fast reconnection.

**Response timeout [ms]** – maximum time of waiting controller's response during communication. Decrease this time for fast reconnection.

**Package timeout [ms]** – maximum time of reading answer from controller. Decrease this time for fast reconnection.

**Frequency of inquiries [ms]** – time between previous and next check of events and states.

### MySQL connection settings:

**MySQL port** – port 3306 for direct connection to controller's database. This connection is mainly used for fast user update (up to 1000 per second).

**Connection timeout [s]** – maximum time of waiting controller's database response during connection.

**Query timeout [s]** – maximum time of waiting for SQL query execution.

**Enable Firewall** – option activates the controller's firewall. Remember to disable it when changing the server's IP address.

**Open access after reboot [s]** – when the firewall is on, devices with not allowed addresses are not able to connect to the controller. Thanks to this option, the user can connect to the controller for the set time from controller APK start, even when it is outside the allowed IP addresses.

**Additional IP Addresses** – administrator has the option to add an additional IP addresses that will belong to the allowed IP addresses. Use comma as a separator. E.g. 10.10.1.50,192.168.1.10,192.168.1.22

**All allowed IP addresses** – summary with list of allowed IP addresses. Apart from custom ones, there will be all IPs of the computer where Noder server belong.

**Network settings** – mask and gateway of controller configured in browser.

**Use secured SSH tunnel** – It's a feature to establish encrypted channel between server and controller, than redirect whole communication through this channel.

**Generate new RSA keys** – button to generate pairs of RSA keys (public and private) for SSH connection and SSH commands.

SSH connection is on 22 port. When SSH tunnel is in use also firewall is enabled by default and ports 3306 and 80 are also closed. TCP port 7000 is used only to get controller version, then SSH tunnel is established.

The connection from the user card to the server is encrypted. The following technologies protect the system:

- Securing the server-client connection → TLS 1.2 encryption
- Server-controller protection → SSH tunnel, firewall in the controller (access to the controller only from specific IP addresses)
- Controller-reader protection → AES-256 encryption
- Mifare DESFire 13.56 MHz reader-card protection → AES-128 encryption

#### **Advanced actions:**

**Restart connection** – button to disconnect with controller and connect again.

**Reboot controller (SSH cmd)** – Secured command on 22 port to reboot controller (works even if controller is disconnected with Axxon PSIM).

**Watchdog test (SSH cmd)** – command will stop heartbeat message from controller operating system to motherboard microcontroller, what should be detected by watchdog up to 2 minutes. It will cause controller reboot by short brake of power. *Do not run this command if you have old motherboard without external watchdog installed. After command connection will be lost in ca. 2 minutes. This is secured command on 22 port working even if controller is disconnected with Axxon PSIM.*

### 3.4.3 Settings tab

Settings tab allows to configure the DEC output. Additionally, tab allows to configure the outputs in case of connection loss and violation



#### DEC (voltage) output control:

**Time of temporarily off impulse [s]** – option enables setting temporarily turn off time of DEC output.

#### Rights update settings:

**Generate user update events** – after selecting, each update of a single user will generate an additional event in the system.

**Disable synchronization of users after reconnect** – after selecting, disables synchronization of users after connection with the Axxon PSIM software.

**Disable synchronization of AL and TZ after reconnect** – after selecting, disables synchronization Access Levels and Time Zones after connection with the Axxon PSIM software.

#### Activate output if the special input is violated:

**Duration of alarm output activation [s]** – time for which the output is to be activated after violation of the special input (21-24). When the value is 0, the output is active until the violation exist.

**Output** – controller relay output

#### Activate output if communication with server is lost:

**Delay of alarm output activation [s]** – after a set time from the loss of connection with server output is to be activated. When the value is 0, function is inactive.

**Output** – controller relay output

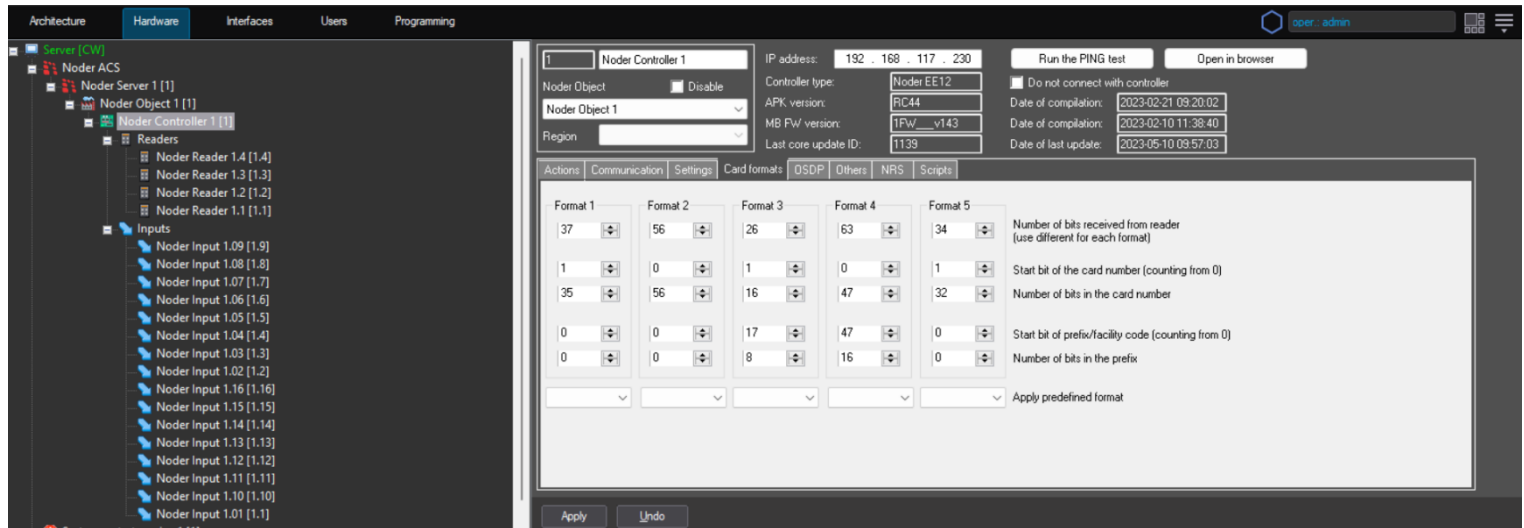
**Duress alarm settings** – generates an additional log in the system "Silent alarm !!! Duress code applied !!!" after entering a PIN code with more characters

**Expected PIN code length** – number of digits in the PIN assigned to users in the system

**Number of duress digits** – number of additional digits to be entered, which will generate a duress log (e.g. 4-Expected PIN code length, Number of duress digits -2. To generate an alarm, enter 6 digits and confirm # on the reader's keypad)

### 3.4.4 Cards format tab

The setting of various card formats gives the possibility of connecting readers with different parameters of read cards to one controller.



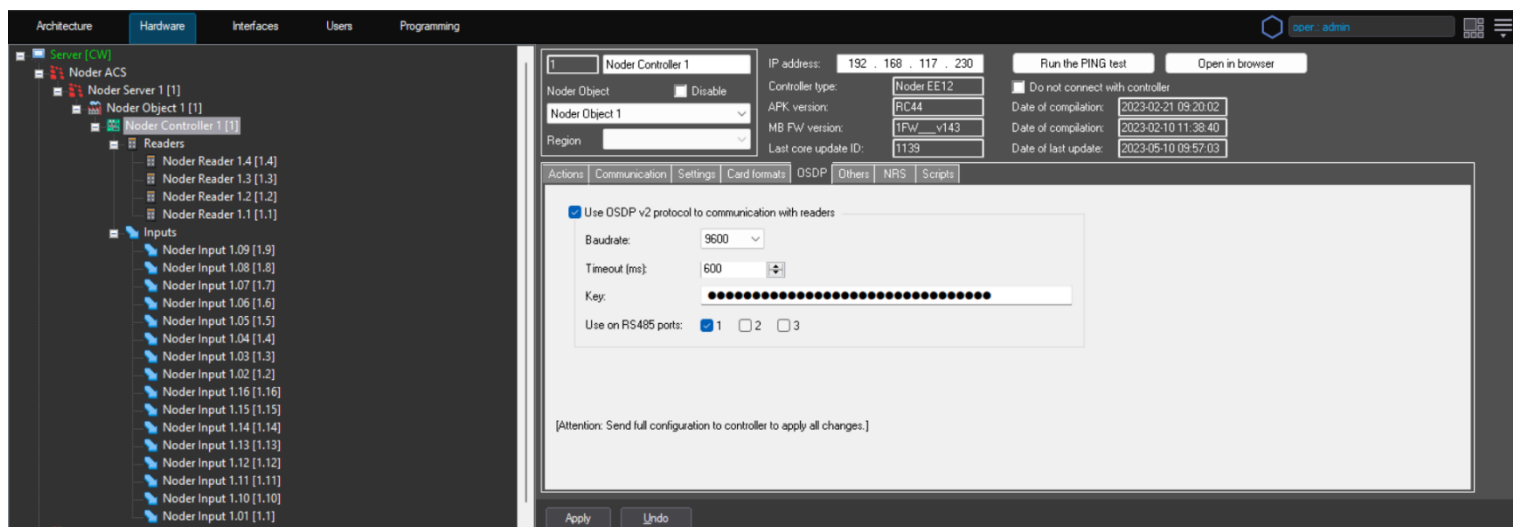
The controller can handle 5 card formats based on number of received bits. Axxon PSIM gives you the choice of predefined card formats or their manual configuration.

Using of a card with an undefined number of bits in card formats will generate in the system an event “Invalid number of bits” with information on how many bits have been read.

Source	Event	Region	Add. info
Noder Reader 1	Invalid number of bits read		37

### 3.4.5 OSDP tab

The controllers enable communication with the reader via the OSDP v2 protocol.



**Use OSDP v2 protocol to communication with readers** – selecting this function allows to use OSDPv2. Otherwise, communication with the factors will follow the **RS485** protocol. OSDP v2 options:

**Baudrate** – available in the drop-down list are following baud rates: 9600, 19200, 38400, 57600, 115200.

**Timeout (ms)** – reader response timeout in communication with controller.

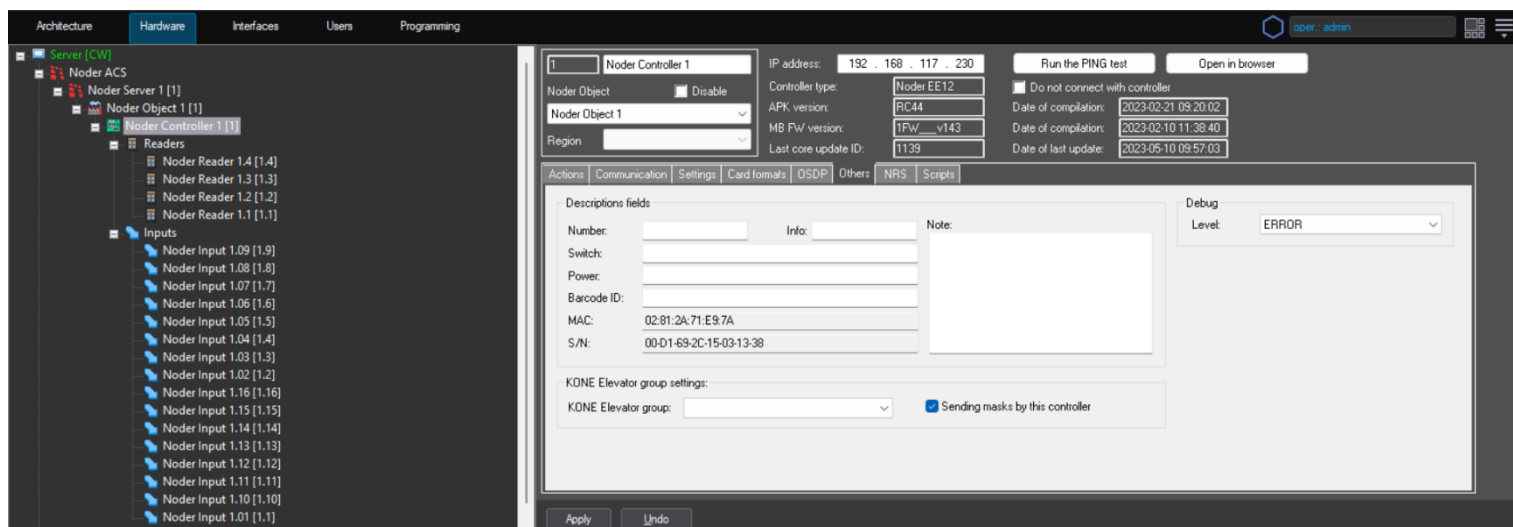
**Key** – 128 bit key introduced in hexadecimal form (32 characters) e.g default key for HID readers in Install Mode: 303132333435363738393A3B3C3D3E3F.

**Use on RS485 ports** – selecting RS485 ports to use OSDP v2. Controller EE12 allows simultaneous use of protocol OSDP v2 and native protocol (e.g 1 port – OSDP v2, 2 port – native, 3 port – native).

OSDPv2 implemented in controller is compatible with supported OSDP protocol implemented in HID, Elatec and ISBC ESMART readers. Readers should set the address in the range from 1 to 4. Reader has to set the **Compliance** option to 0x02 (controller **does not support OSDPv1**).

### 3.4.6 Others tab

Tab is used to configure additional controller settings.



**Descriptions fields** – information about the network and electrical infrastructure can be stored. You can record the switch and socket number, electrical switchboard and fuse, MAC controller address, and more. The information stored **does not affect the logic of the controller**.

**KONE Elevator group settings** (only if integration with KONE is in use):

**KONE Elevator group** – Select one Kone Elevator group to manage from this controller.

**Sending masks by this controller** – If checked controller is sending masks specified in KONE Elevator group.

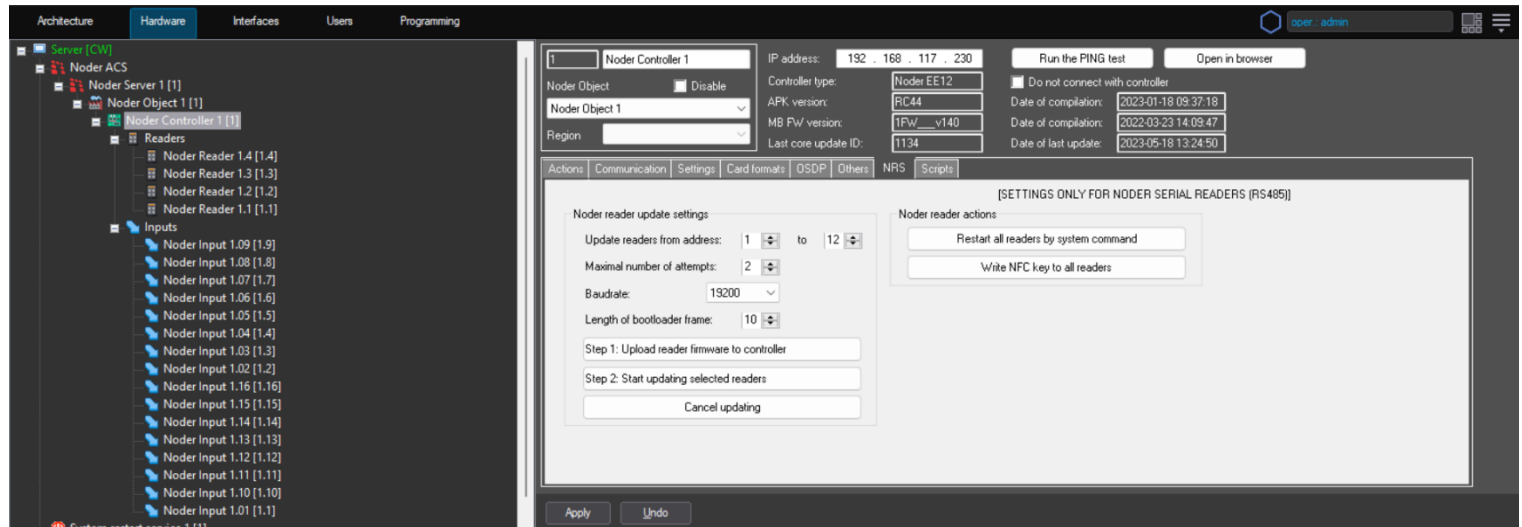
**Debug** – option for programmers allowing to specify certain settings of files containing logs from communication with controller. Option allows to choose:

**Level** – the option allows you to select logs that will be saved in the file.



### 3.4.7 NRS tab

Tab allows to upload files and update Noder readers to support NFC technology.



#### Noder reader update settings:

**Update readers from address** - option enables update readers on selected addresses connected to the controller.

**Minimal number of attempts** - option enables to indicate the number of attempts to update readers.

**Baudrate** - option allows to select the baud rate when updating the reader. The default value is 19200.

**Length of bootloader frame** - option allows to set the size of data packets sent to the reader. The default value is 10.

**Step 1: Upload reader firmware to controller** - after clicking the button, a window will open in which a folder with the reader's update files should be indicated. Uploading files is necessary to run NFC in readers.

**Step 2: Start updating selected readers** - after setting the update parameters and uploading the files from the reader firmware, you can start the update by clicking this button.

**Cancel updating** - the option allows you to interrupt the update

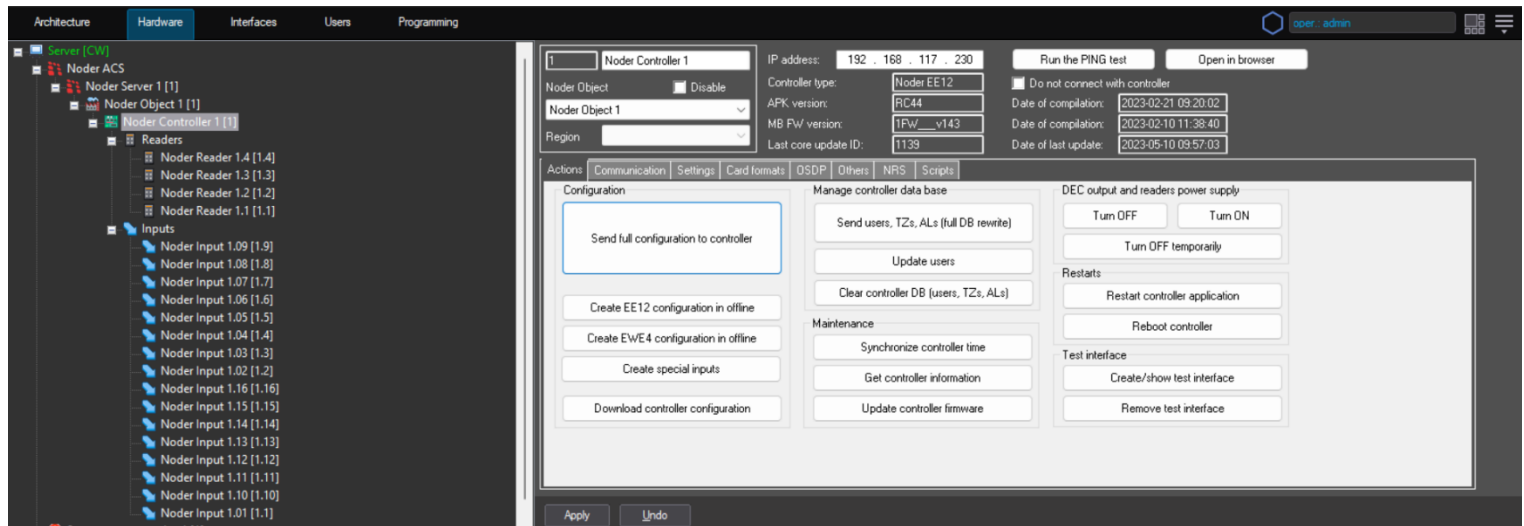
#### Noder reader actions:

**Restart all readers by system command** - option allows to restart all readers connected to the controller by system command (restart via the DEC output).

**Write NFC key to all readers** - the option allows you to send NFC keys to readers. Remember to set them for each reader in advance

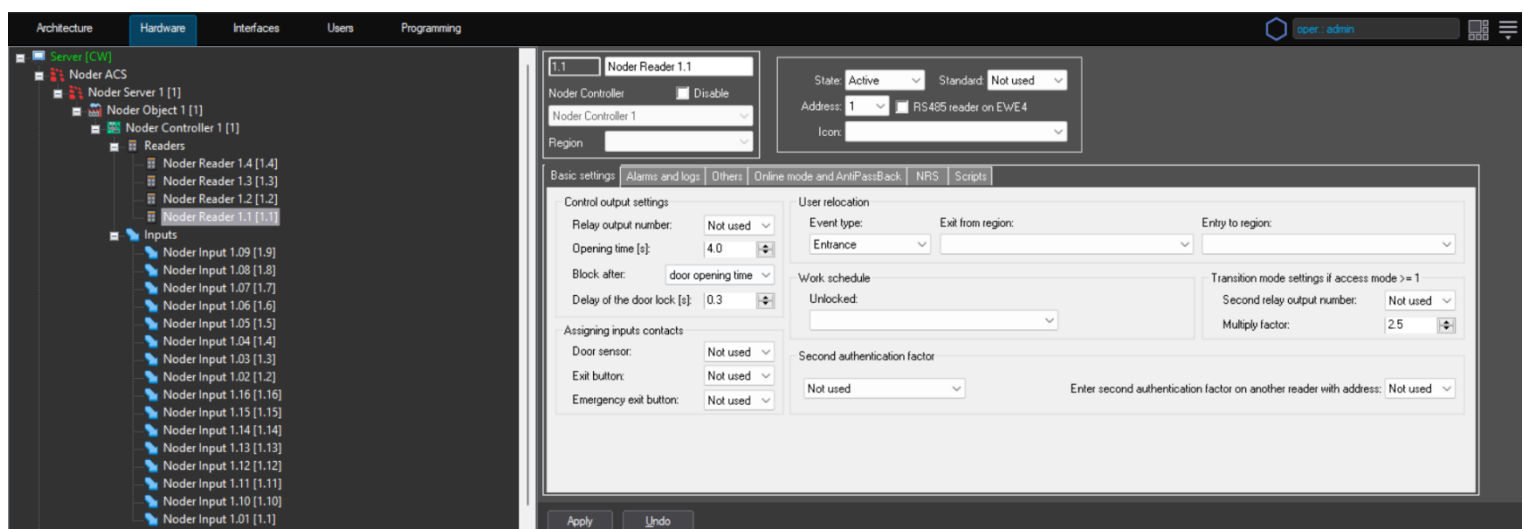
## 3.5 Readers

First time you start controller, you need to download its startup configuration by clicking **Download controller configuration**.



After downloading the configuration from controller will be created **Inputs** and **Readers**. 12 readers and 20 inputs will be created for EE12 and 4 readers and 16 inputs will be created for EWE4. It is necessary to configure readers and zones according to the needs of the system. **Unused ones to be removed and then send the configuration to controller** (button "Send full configuration to controller").

To connect to the reader, its status, address and type must be configured:



**State:**

**Inactive** – this is state set when the device is to be turned off for the system.

**Active** – this is state set for normal system operation.

**Locked** – it is state set to block the operation of reader.

**Address** – in the dropdown list, free addresses in the 1-12 range are available. Readers are addressed by programming cards giving them addresses from the range 1-4. The addresses for EE12 controller are converted as follows:

<i>Reader address</i>	<i>Port</i>	<i>Logical address in controller</i>
1	1	1
2	1	2
3	1	3
4	1	4
1	2	5
2	2	6
3	2	7
4	2	8
1	3	9
2	3	10
3	3	11
4	3	12

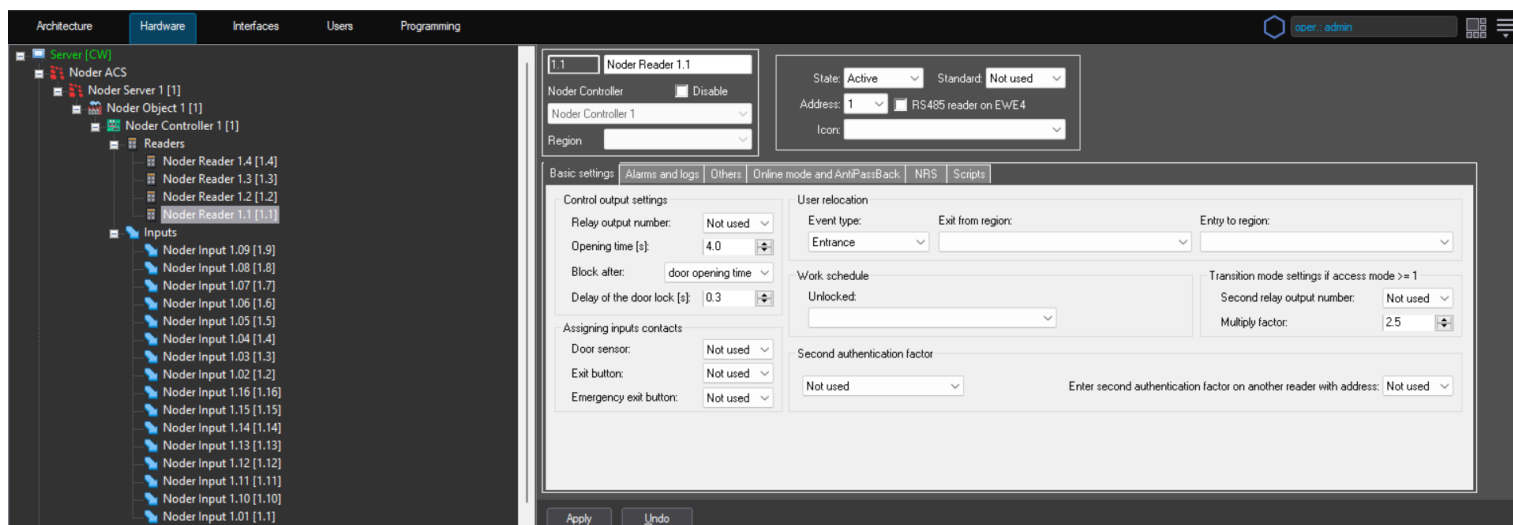
In the case of EWE4 controller, it is possible to connect up to four readers (both Wiegand and RS-485 in any configuration: e.g. 1 Wiegand reader and 3 RS-485 readers). Noder readers should be addressed by programming cards (MD-R/MDK-R using 1-4 programming cards to addressed reader and upload keys, MD-W using 1 address programming card to upload keys).

**Icon** – it is a kind of icon that will represent reader on the visualization map.

**RS reader on EWE4** – this option should be selected when RS-485 reader (Noder MD-R/MDK-R) is configuring on EWE4 controller.

### 3.5.1 Basic settings tab

Tab is used to configure the transition. Allows to assign inputs and outputs to the reader.



#### Control output settings:

**Relay output number** – number of the relay that is assigned to the reader. For EWE4 select relay 1- 6, for EE12 select relay 1-16.

**Opening time [s]** – the time for which controller will release control output corresponding to the given reader after granting access.

**Block after** – transition can be blocked after **door opening time**, **door opening** or **door closing**. For parameters **door opening** and **door closing**, blocking the door takes place after **door opening time**, when no action occurs on it.

**Delay of the door lock [s]** – enables setting an additional time delay for parameters door opening and door closing. Maximum value is 2s.

#### Assigning inputs contacts:

**Door sensor** – number of the input to which the door sensor is connected.

**Exit button** – number of the input to which the exit button is connected.

**Emergency exit button** – number of the input to which the emergency exit button is connected.

### **User relocation:**

**Event type** – following options are possible: **Entrance, Exit, Business entrance/exit, Private entrance/exit, Arrival, Departure, Patrol**. These are events that the system will record when card will be reading from reader and passage through the door .

**Exit from region/Entry to region** – these are regions used by the AntiPassBack system to logically map the system and control the presence of the user in a given region and the possibility of its passage only to neighboring regions. Without setting these regions, it is not possible to use the global AntiPassBack.

### **Work schedule:**

**Unlocked** – the option enables assigning a schedule created in Access manager. During it, the passage will be unblocked. Note that changing the status of the reader to inactive (e.g. when disconnecting it from the system) does not disable the schedule. This schedule must be set to "empty" before changing the status of the reader. Otherwise, the relay will be activated after time schedule start.

### **Second authentication factor:**

**Not used** – second authentication factor inactive.

**Require PIN code** – after selecting this, system will wait for input PIN on reader after card.

**Require card number** – after selecting this, system will wait for input the same card number but on another reader selected in parameter "Enter second factor on another reader". If second reader is not selected, second authentication factor is inactive.

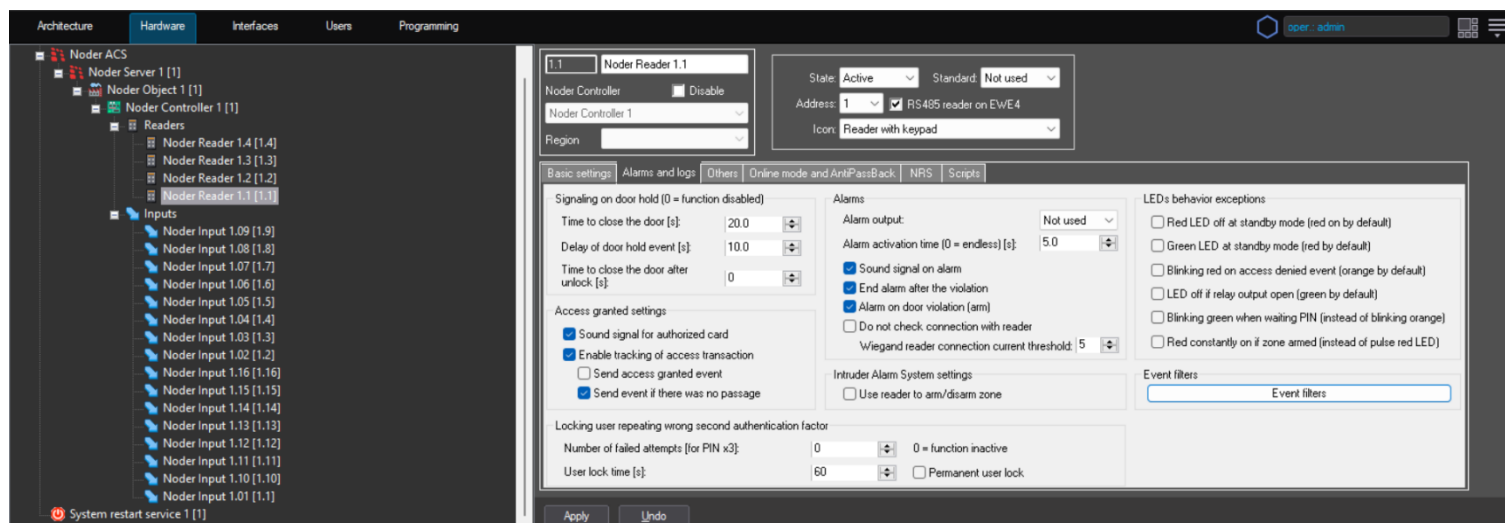
**Access code instead of card** – after selecting the option, user authorization can be done using the access code assigned to the user in the "Access code" field in Access Manager.

#### **Enter second factor on another reader:**

- **Not used** – option results in that the system expects entering PIN code on the same reader where the card has been registered.
- **1-12** – address of another reader connected to controller.
- **13** – results in indicating to the system that it should expect confirmation from a special RS port on EE12 used for connection with special devices (e.g. face or fingerprint biometric readers connected by Wiegand to RS485 converter).

## 3.5.2 Alarm and logs tab

Tab is used to set alarming after violation or too long opening of the door.



### Signaling on door hold:

**Time to close the door [s]** – this is time after which the system will generate an user warning alarm (event not generate in system yet) about holding the door opened. User should close the door or approach his card again in time “Delay of door hold event” to prevent generating alarm event. For the value 0, function is inactive.

**Delay of door hold event [s]** – this is delay time after which an event in the system and alarm on reader will be generated if door was opened to long. For the value 0 alarm is generated immediately after "Time to close the door". But if this value is different, alarm will be delayed by this time.

**Time to close the door after unlocked [s]** – this is time after which the system will start to generate an alarm for operator after opening door with the function permanently unlock. For the value 0, function is inactive.

### **Access granted settings:**

**Sound signal for authorized card** – deselecting this option will result in application of a valid card to reader only by changing the LED's color to green. The sound signaling will only be in the case of an unauthorized card or alarm.

**Enable tracking of access transaction** – when this option is deselected, immediately after the card is applied, event “Access in” is generated. When option is selected, “Access in” event is generated only after the door has been physically opened. Also, when this function is enabled, two other settings are possible:

- **Send access granted event** – if this option is selected, an event is generated for the user after the card has been applied „Access granted”.
- **Send event if there was no passage** – if this option is selected, after approved card's applied, if the door is not opened, after **door opening time [s]**, „No passage after access was granted” event will be generated.

### **Alarms:**

**Alarm output** – the number of the relay that will work in correlation with the alarm event (forcing the passage or if the door is opened for too long).

**Alarm activation time [s]** – the parameter determines time during which the reader signals an alarm situation (flashing of the diode and sound signaling) – forcing or door open too long. If the cause of the alarm does not stop, the acoustic signaling will be repeated every 24 hours. The visual indication is kept until the cause of the alarm is removed. Signaling is as follows:

- **In case of violation the door** – continuous tone, the LED flashes orange at approximately 2/3 Hz;
- **In case hold the door** – time counted from the moment the user opens the passage, after which the sound signaling on reader starts (intermittent signal with a frequency of 0.5Hz) and the diode blinking in orange at the same frequency. Its purpose is to warn the user to close the door before the alarm is generated.

**Sound signal on alarm** – if this option is unchecked, the alarm on reader is only indicated by the LED blinking in orange..

**End alarm after the violation** – when the option is selected, in the event of an alarm (forcing or a long-open passage) the acoustic and visual signaling is deleted immediately after the cause of the alarm has been eliminated (closing the passage). Otherwise, the audible alarm is signaled by the **Alarm activation time [s]**. If this option is not selected, the LED on the reader will continue to flash orange after the alarm time, until the authorized card is applied to reader.

- **Option selected in case of violation the door** – continuous beep, LED flashes orange at approximately 2/3 Hz. After cessation of the violation, the sound and light signaling stops;
- **Option selected in case hold the door** – audio signal is interrupted at a frequency of about 2.5 Hz and the LED is flashing in orange at the same frequency. After closing passage, the sound and light signaling stops.
- **Option deselected in case of violation the door** – continuous beep, LED flashes orange at approximately 2/3 Hz. After the violation ceases, sound and light signaling is continued according to Alarm activation time. After this time, sound signaling stops, but LED on reader still flashes orange at a frequency of about 2 / 3Hz, until the moment when the valid card is applied to reader, the exit button is used or the operator opens the door.

- **Option deselected in case hold the door** – audio signal is interrupted at a frequency of about 2.5 Hz and the LED is flashing in orange at the same frequency. After violation ceases, sound and light signaling is continued according to Alarm activation time. After this time, sound signaling stops, but LED on reader still flashes orange at a frequency of about 2.5 Hz, until reader applies an authorized card to the reader, use the exit button or open the door by operator.

**Alarm on door violation (arm)** – this option enables turning off the alarm generation in the event of unauthorized opening of the passage. Signaling function for a too long transition will continue.

**Do not check connection with reader** – option for devices connected via Wiegand. If the device is powered from a source other than the configured port, controller will not have confirmation of communication with device. Selecting this option allows to permanently set the normal state for device on the map.

**Wiegand reader connection current threshold** – option allows to set the current level for which the Wiegand reader is detected on the EWE4 controller. Detection is based on the current consumption on the port, therefore the low power readers may not be detected when the option is not set appropriately. It should be

#### **Locking user repeating wrong second authentication factor**

**Number of failed attempts [for PIN x3]** option is used in Intruder Alarm Systems. Allows to arm the zone which the reader is assigned. To

**User lock time [s]** - parameter in which the time of blocking the user after the number of failed attempts [for PIN x3] is determined. If the option **Permanent user lock** is selected, user will be permanently blocked after a certain number of incorrectly entered PIN codes (In order for the user to be able to use the system again, the operator will have to change the **User locked** parameter to **No**)

#### **Intruder Alarm System settings:**

**Use reader to arm/disarm zone** – option is used in Intruder Alarm Systems. Allows to arm the zone which the reader is assigned. To arm zone you must use an authorized card on the reader twice within 2,5 second. To disarm zone you must use an authorized card once on reader. Activation of arming the zone is signalled by the reader beeping twice and orange LED flashing every 2 seconds.

#### **LEDs behaviour exceptions:**

**Red LED off at standby mode** – enables switching off the red diode when the reader is in normal state.  
**Green LED at standby mode** – enables to turn on the green LED when the reader is in normal state.  
**Blinking red on access denied event** – enables to blink red instead of orange when access is denied.  
**LED off in relay output open** – enables to turn off the LED after getting access, permanently opening the door, etc.

**Blinking green when waiting PIN** – enable to blinking green diode instead of the orange after the start of the waiting time for entering the PIN code.

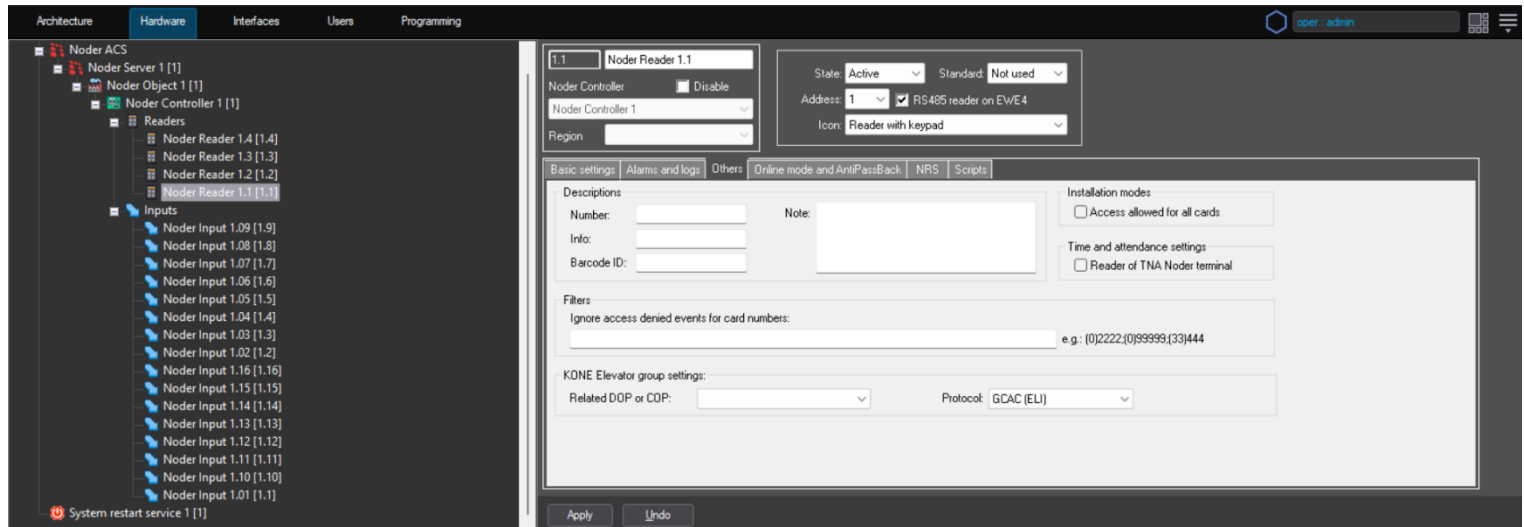
**Red constantly on if zone armed** – enable to turn on the red LED when the zone is armed.



**Event filters** – the option enables disabling some events from generating and saving in database.

### 3.5.3 Others tab

Tab is used to configure additional reader settings.



**Descriptions** – these are fields that allow assigning certain descriptions to the readers, e.g. inventory number, location and others.

#### Filters:

**Ignore access denied events for card numbers** - The function enables entering card numbers (separated by a semicolon), for which the system will not register an event of reading an unauthorized card.

**Kone Elevator group settings** (only if integration with KONE is in use):

**Related DOP or COP** – assign reader to specific Destination Operation Panel or Car Operation Panel

**Protocol** – select protocol of communication:

- **GCAC (ELI)** – protocol to manage access from DOP or COP.
- **RCGIF (Home floor)** – protocol to call home floor from turnstile.

#### Installation modes:

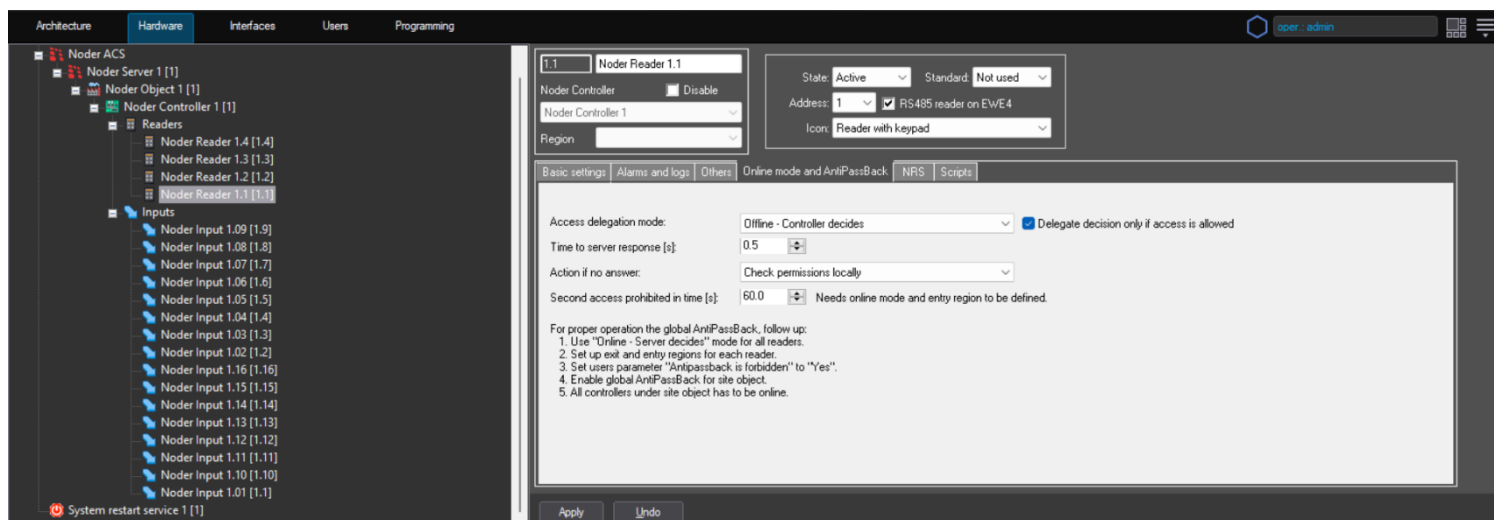
**Access allowed for all cards** - using any card read by the reader will unblock the door.

#### Time and attendance settings:

**Reader on TNA Noder terminal** - the option should be selected when the **Noder RCP-1** reader is assigned to a given address in the controller. If the option is not selected, you will not be able to connect to the terminal

### 3.5.4 Online mode and AntiPassBack tab

The tab is used to set the mode in which the reader is to work.



#### Mode of access delegation:

**Offline - Controller decides** – access queries will be directed to the internal database of controller. Enabling these function will disable the operation of the global AntiPassBack on this reader (the function must also be enabled for the user).

**Offline - Script decides** – granting access is based on script logic.

**Online - Server decides** – option switches reader to the online mode of work. Granting access after applying the card will be decided by the server automatically. Enabling these function will enable the operation of the global AntiPassBack on this reader (the function must also be enabled for the user).

**Online - Operator decides** – option switches reader to the online mode of work. Granting access after applying the card will be decided by displaying the previously prepared interface for the operator. Enabling these function will enable the operation of the global AntiPassBack on this reader (the function must also be enabled for the user).

**Online - Server decides then script** – the option switches the reader to online mode. Granting access after using the card is done automatically by the server. Enabling this feature will enable global AntiPassBack on the reader. If there is no response from the server, the mode is changed to **Script decides**.

**Online - Operator decides then script** – the option switches the reader to online mode. Granting access after applying the card is performed by the operator on a previously prepared interface. Enabling this feature will enable global AntiPassBack on the reader. If there is no response from the server, the mode is changed to **Script decides**.

**Delegate decision only if access is allowed** – option is used in the Online mode - operator decides. After selecting , requests of users with access will be confirmed by the operator. Unauthorized users will be immediately denied access on the reader.

***Time to server response [s]*** – time that controller has to wait for the server's response.

***Action if no answer*** – in the absence of a server response controller will perform one of the following options:

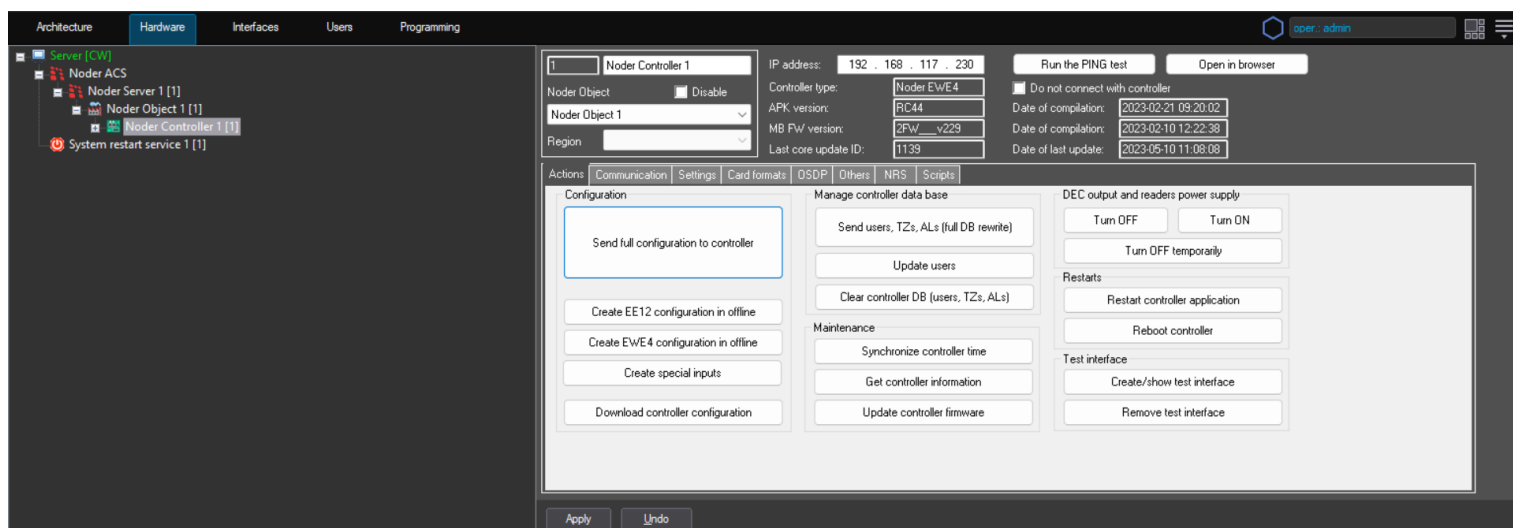
- ***Deny access*** – after losing connection with the server and using the card, the user will not automatically receive access even if his card is authorized.
- ***Check permission locally*** – after losing connection with the server and using card, access will be granted after checking the user's permissions in the controller's internal database.

***Second access prohibited in time*** – time after which user can re-access the zone. For the function to work, the option “Allow multiply access” in user permissions must be marked as “No” and the controller must be in online mode.

## 3.6 Inputs

Downloading configuration from controller will automatically create 16 inputs for EWE4 and 20 inputs for EE12 in off state. To create special inputs select option **Create special inputs** in **Action tab** of controller.

In addition to assigning the entry number to the reader in order to indicate its function in the system (e.g. reed switch or exit button), it should also be configured accordingly. First of all, define whether the input should work in NO or NC logic.



Special inputs can't be freely configured and used, for example, as exit button. The types allowed for these inputs are **Off**, **Special - NC** and **Special - NO**. Purpose of special inputs:

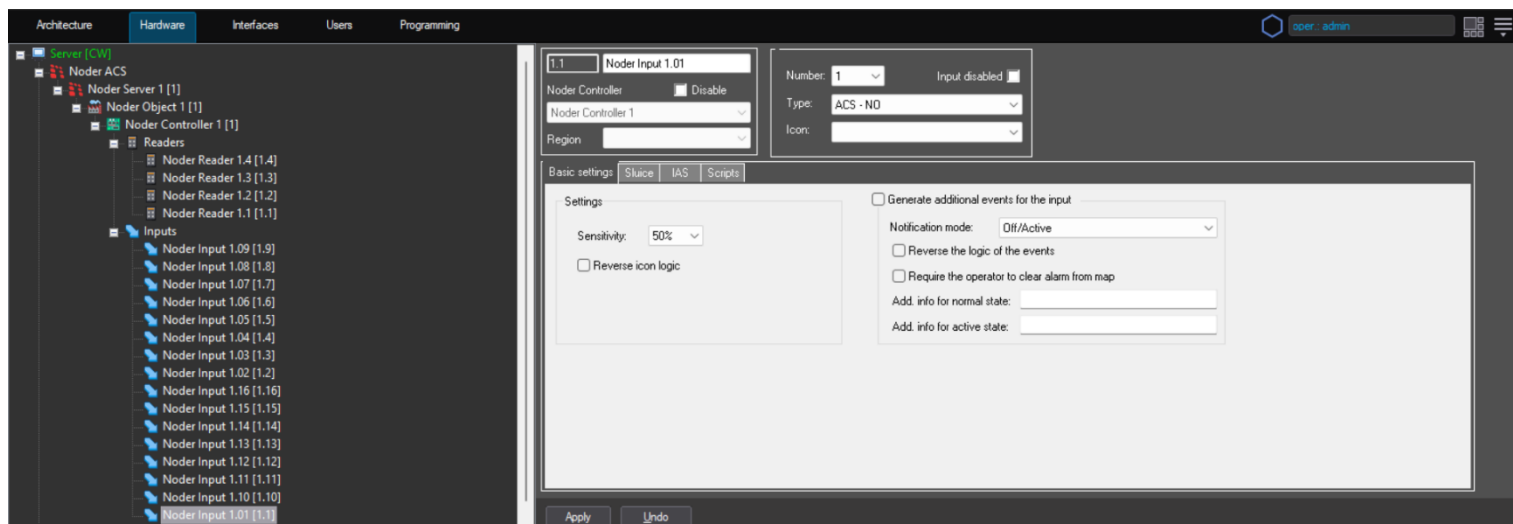
**BAT** – signal of discharged batteries.

**AC** – no 230 V power supply.

**TMP** – 12V DC power supply damage,

**DR** – serial connection of all tamper cabinet doors and wall mounting.

### 3.6.1 Inputs configuration



**Input disabled** – input activation is not recorded in the system.

#### Settings:

**Number** - controller input number.

**Sensitivity** - the option allows setting the time from input activation to registering it in the system using the levels 10-100%.

**Type**- type of input. from available dropdown list. When input is used only by Access Control System, select input type „ACS”. When input is used only by Intruder Alarm System, select input type „IAS”. When input is used by Access Control System and Intruder Alarm System, select input type „ACS + IAS”. Input types:

- **Off**
- **ACS - NO**
- **ACS - NC**
- **ACS - EOL/NO**
- **IAS - NO**
- **IAS - NC**
- **IAS - EOL/NO**
- **ACS - EOL/NO**
- **IAS - 2EOL/NO**
- **IAS - 2EOL/NC**
- **ACS + IAS - NO**
- **ACS + IAS - NC**
- **ACS + IAS - EOL/NO**
- **ACS + IAS - EOL/NC**
- **ACS + IAS - 2EOL/NO**
- **ACS + IAS - 2EOL/NC**
- **Special - NO**

- **Special - NC**

**Icon** – icon that will represent the input on the visualization from the available dropdown list.

**Reverse logic** - selecting this option will cause the icon on the visualization to show the opposite of the actual signal.

**Generate additional events for input** – selecting this option will generate an additional event in the system

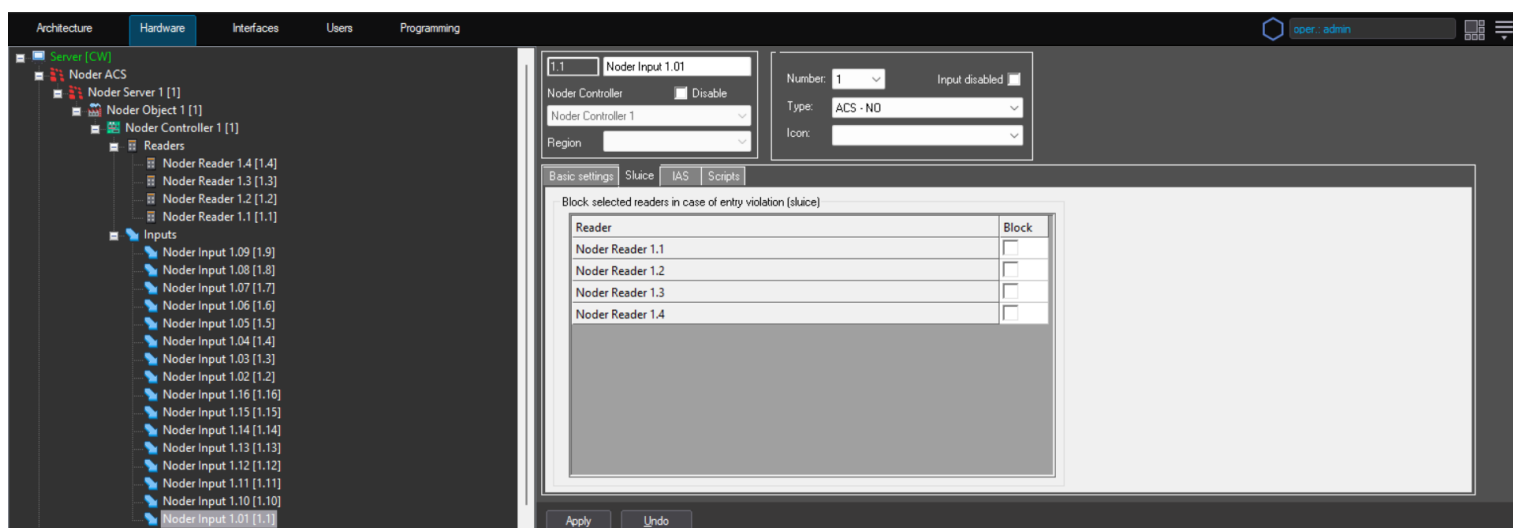
**Notification mode:**

- **Off/Active**
- **Normal/Alarm**
- **Normal/Failure**

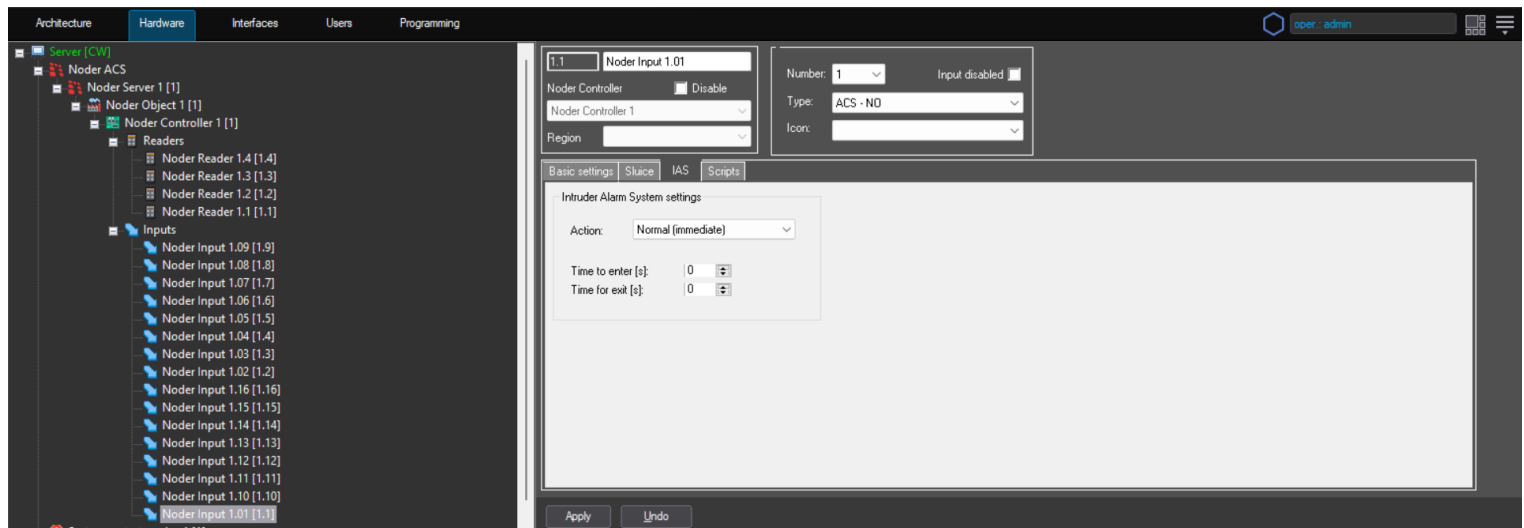
**Reverse logic**– selecting this option will reverse the logic of events generated by the system in relation to the actual input state.

**Require the operator to clear alarm from map** – selecting this option will cause keeping the alarm status by icon on the map until it is deleted by the operator, even if physical input returns to the normal state

**Add. Info for normal/active state** – these are text fields that allows to attach a permanent comment to the event. They are displayed in event viewer in **Add. info** column.



**Block selected readers in case of entry violation (sluice)** –readers marked here will be blocked for time of input activation.



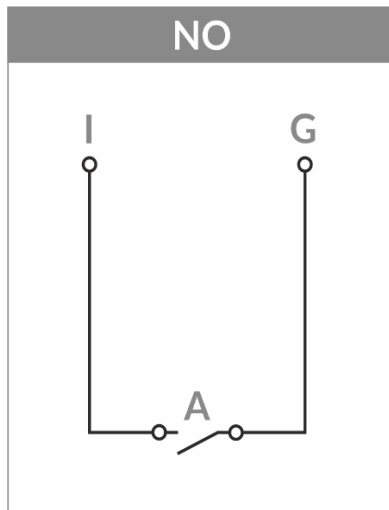
**Intruder Alarm System settings** – function will be valid if the input type is configured as „IAS” or „ACS+IAS”.

**Action** – from available dropdown list you can select when alarm will be triggered:

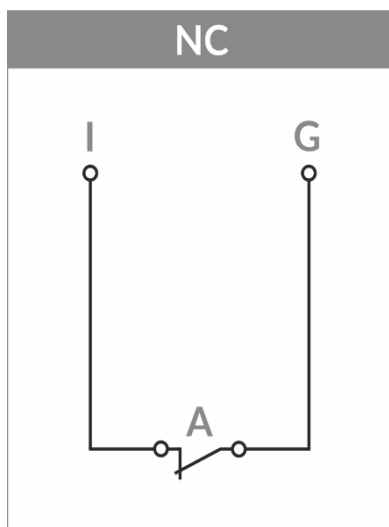
- **Normal (immediate)** – after arming the zone and activating input
- **Entry/Exit** – when zone is armed after activating input user have **Time to enter (sec.)** (time to disarm)/**Time to exit (sec.)** this zone. After this time alarm is activated. The feature is useful in places where zones are disarmed and armed.
- **24h** – each input activation (even if zone is disarmed).
- **24h silent alarm** – each input activation generate a silent alarm (even if zone is disarmed). Readers and outputs will not change their state.
- **Panic** – each input activation generate panic alarm (even if zone is disarmed).
- **Silent panic** – each input activation generate a silent panic alarm (even if zone is disarmed). Readers and outputs will not change their state.
- **Technical – AC power failure** – each input activation generate a silent AC power failure alarm (even if zone is disarmed). Readers and outputs will not change their state.
- **Technical – Battery failure** – each input activation generate a silent Battery failure alarm (even if zone is disarmed). Readers and outputs will not change their state.
- **Arming** – activating the input arming the zone.
- **Disarming** – activating the input disarming the zone.
- **Monostable arming/disarming** – change to the opposite state after each leading edge (input disabled → input enabled).
- **Bistable arming/disarming** – the status change to armed/disarmed takes place each time the input status changes.
- **Resetting alarm** – activation of the input resets the alarm



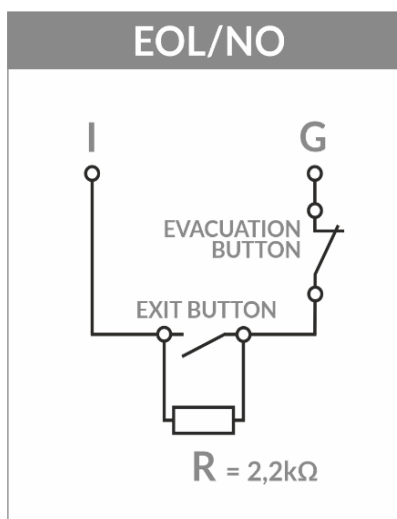
### 3.6.2 Inputs connection diagrams for Access Control System



Input configured as NO is used for the exit button. After pressing it, the relay is activated and the event „Opening by exit button” is received.



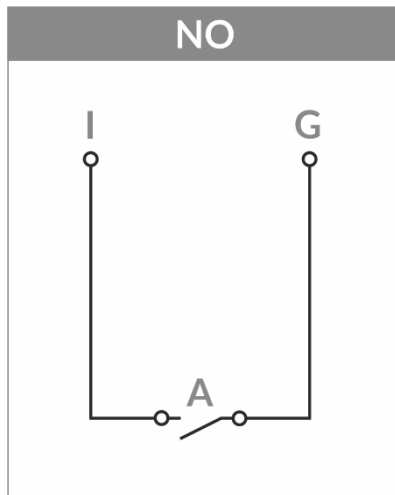
Input configured as NC is used for the door sensor or emergency exit button. Door sensor informs about the current status of the door. After pressing emergency exit button event “Emergency exit button pressed” is received



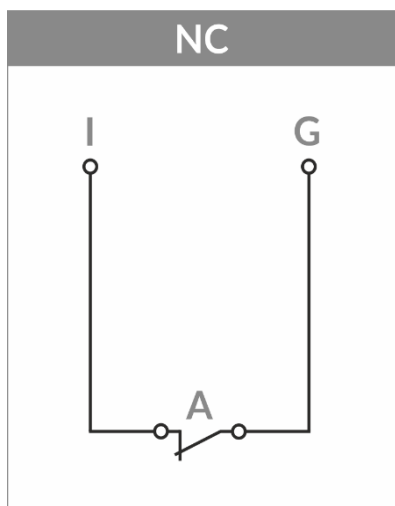
Input in configuration NO with end of line resistor (2,2kOhm). After pressing exit button, the relay is activated and the event „Opening by exit button” is received. After pressing evacuation button, the event „Emergency button is pressed” is received.



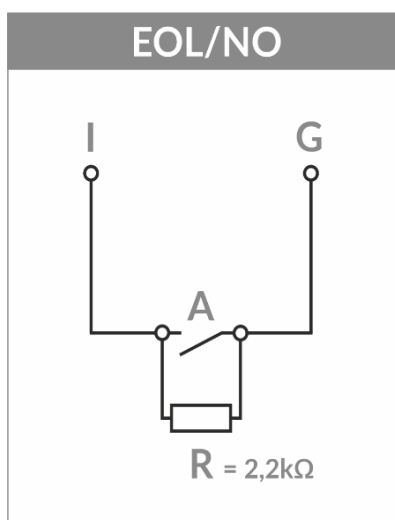
### 3.6.3 Inputs connection diagrams for Intruder Alarm System



Detector with normally open output. Closing the circuit triggers an alarm. We do not receive information about sabotage („Alarm” event is not generated) or fault („Alarm” event is not generated).

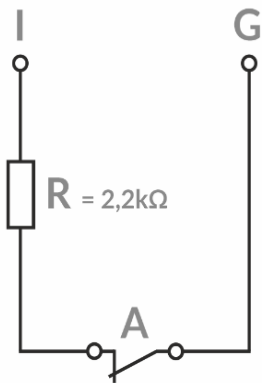


Detector with normally closed output. Opening the circuit triggers an alarm. We do not receive information about sabotage („Alarm” event is generated) or fault („Alarm” event is not generated).



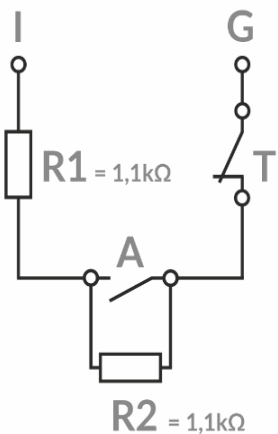
Detector in configuration with end of line resistor (2,2kOhm). Closing the circuit triggers an alarm. We receive information about sabotage („Tamper” event is generated) and do not receive about fault („Alarm” event is generated).

## EOL/NC



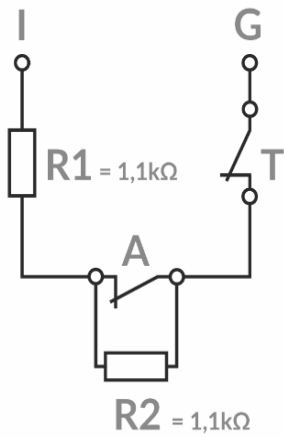
Detector in configuration with end of line resistor (2,2kOhm). Opening the circuit triggers an alarm. We do not receive information about sabotage („Alarm” event is generated) and receive about fault („Fault” event is generated).

## 2EOL/NO



Detector in configuration with 2 end of line resistors (2x1,1kOhm). Closing the circuit triggers an alarm. We receive information about sabotage („Tamper” event is generated) and („Fault” event is generated).

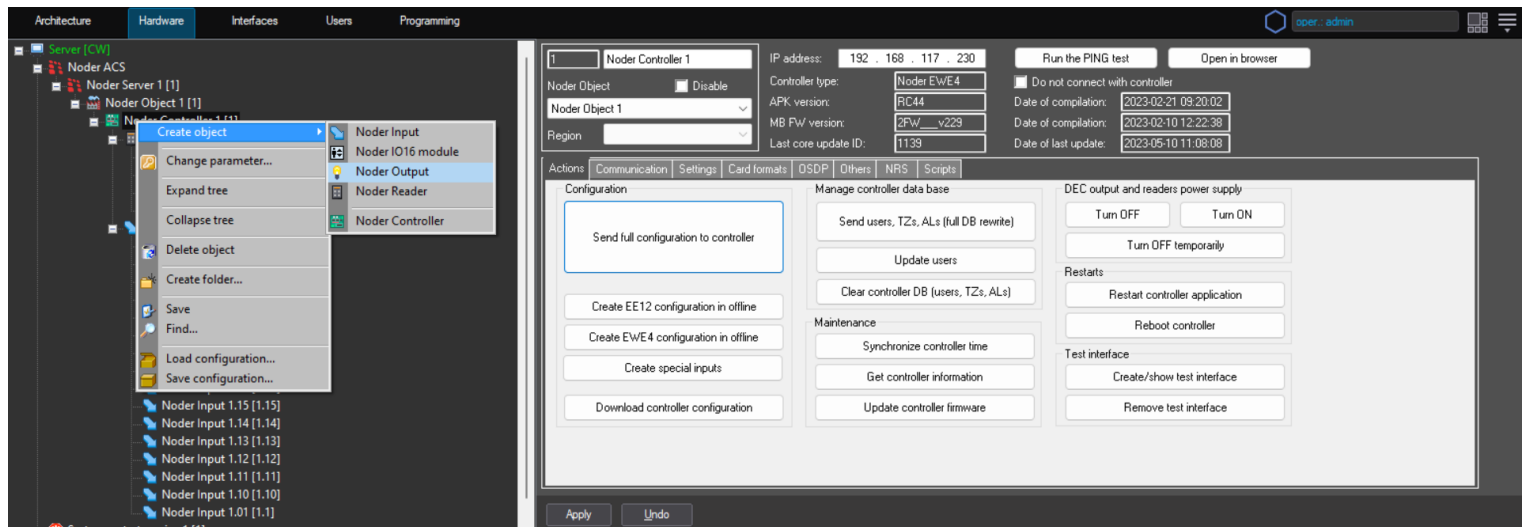
## 2EOL/NC



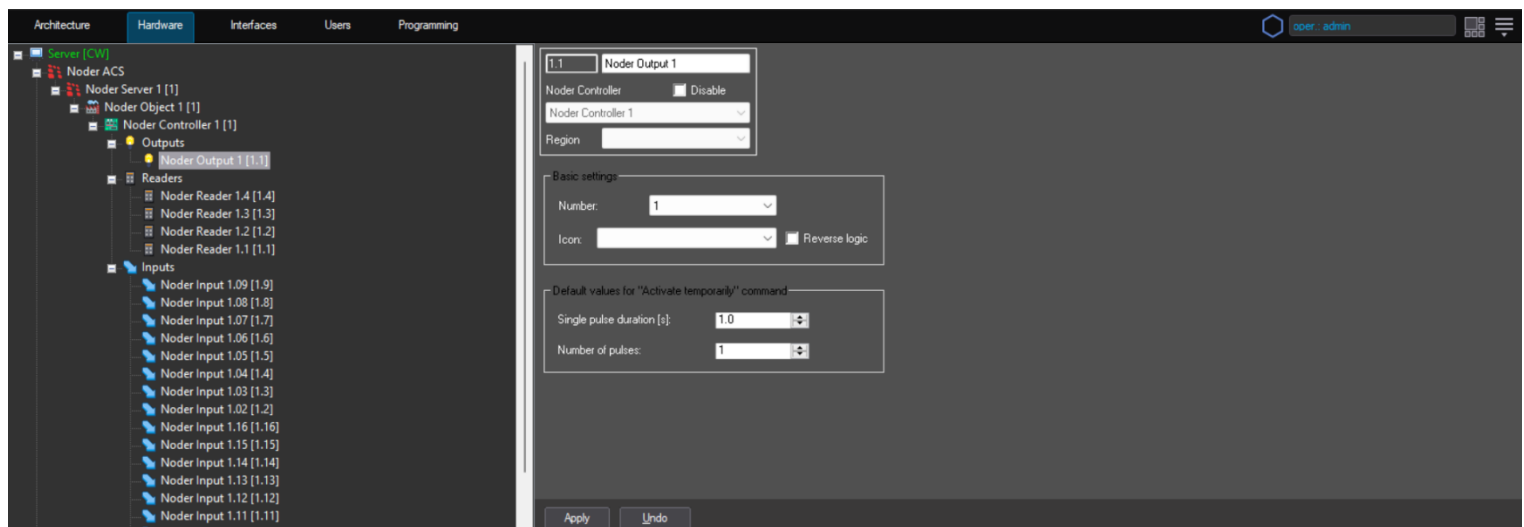
Detector in configuration with 2 end of line resistors (2x1,1kOhm). Opening the circuit triggers an alarm. We receive information about sabotage („Tamper” event is generated) and („Fault” event is generated).

## 3.7 Outputs

To create an output, right-click on the controller and select **Noder Output**. After giving the name and number of output, settings window will open.



Object can be used in an Intruder Alarm System (after created, it will be visible in IAS Zone settings) to be activated on alarm or just to control relay from map, macro or script.



### Basic settings:

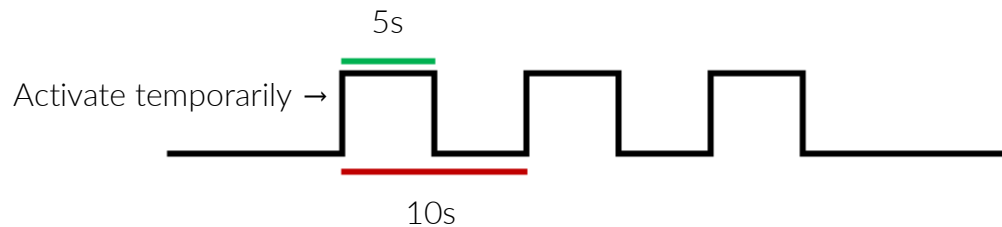
**Number** - controller relay number.

**Icon** - icon that will represent the output on the visualization from the available dropdown list.

### Default values for “Activate temporarily” command:

**Single pulse duration [s]** – time of single pulse duration (in example below **Single pulse duration [s]** = 5).

**Number of pulses** – number of pulses after “Activate temporarily” command (in example below **Number of pulses** = 3).



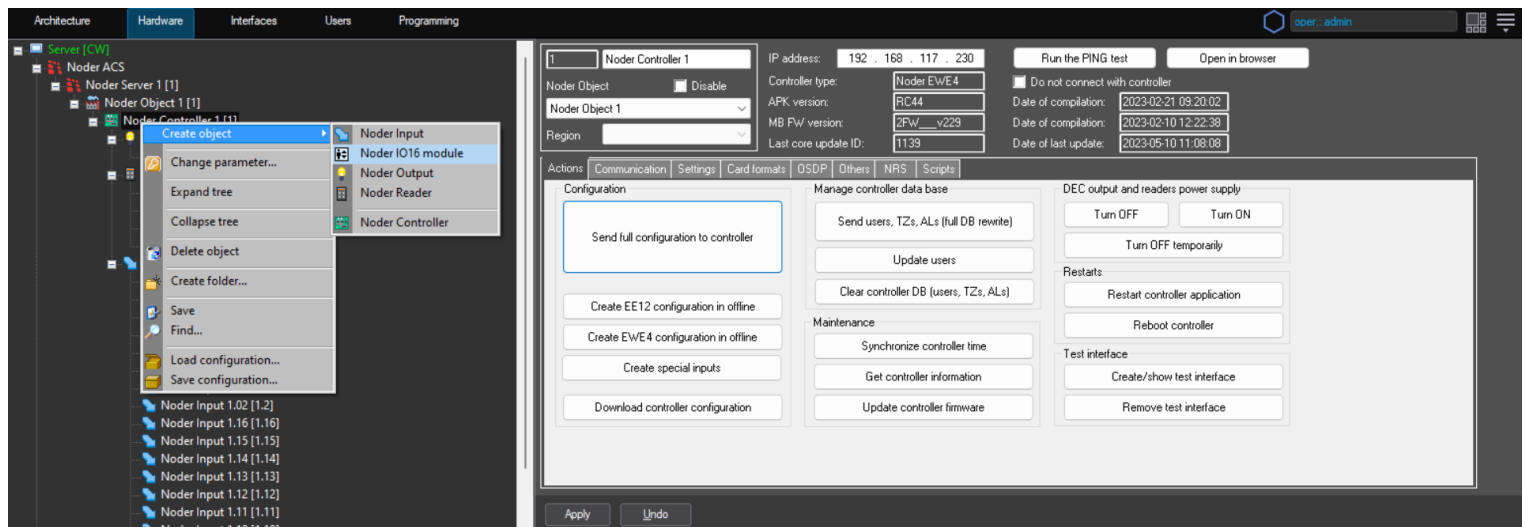
**Reverse logic** – selecting this option will reverse the logic of icon on the map in relation to the actual output state.

## 3.8 IO16 modules

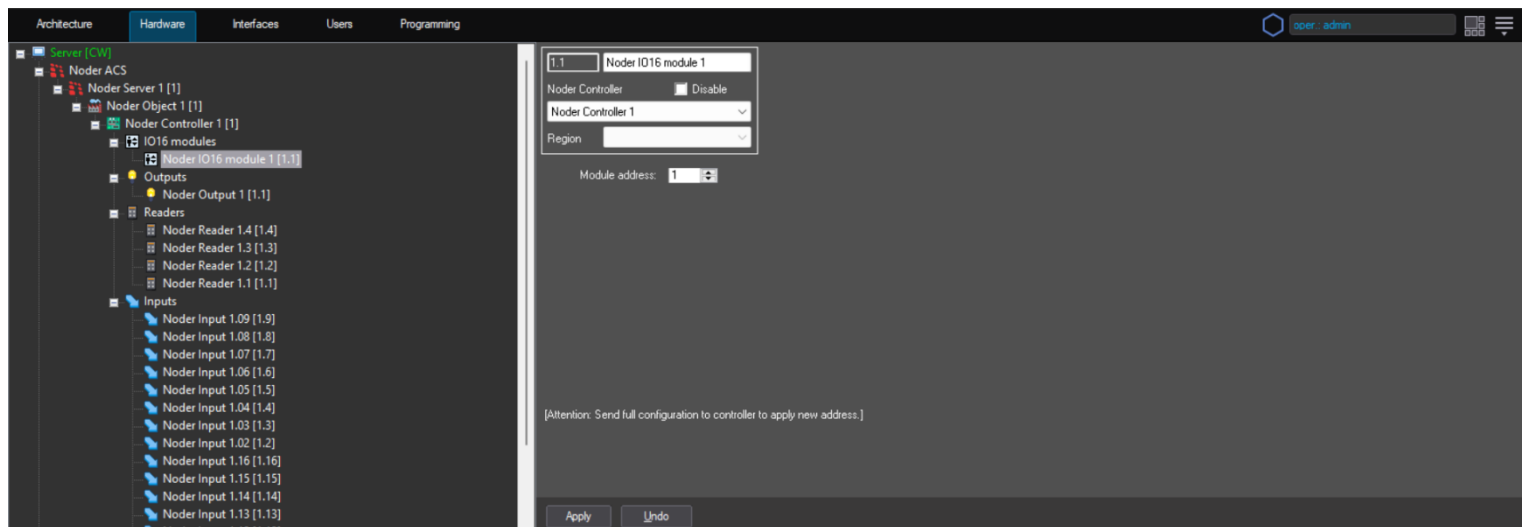
After the controller is connected and configured, the administrator can add IO16RS module.

### 3.8.1 IO16 module configuration

To create object, right-click on the controller to which the device is to be connected and then create the **Noder IO16 module** object.



After choose the object, a window will open in which you should assign a number and name the device. Click Apply, a window of module options will appear.



The object address must be the same as that set on the module's DIP switch (addressing described in Noder TD-IO16RS). 4 modules can be connected to one EE12 and EWE4 controller. In the case of the EE12 controller, connect the module to the expansion bus (port 4), and for EWE4 - to the RS485 bus. One type of devices can operate on the RS485 bus, therefore EWE4 only supports readers on the Wiegand bus.

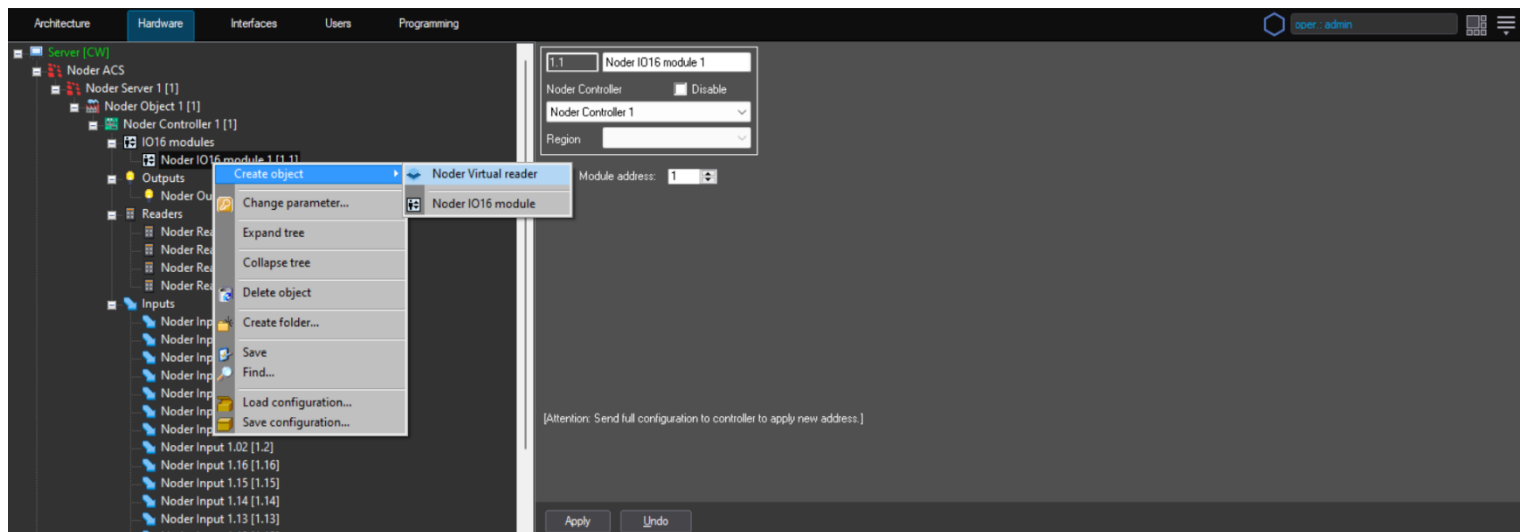


After assigning the address, click Apply and click Send configuration to controller in controller settings. At this point, the device should establish a connection. RX and TX communication LEDs on the controller and module should start blinking regularly with high frequency.

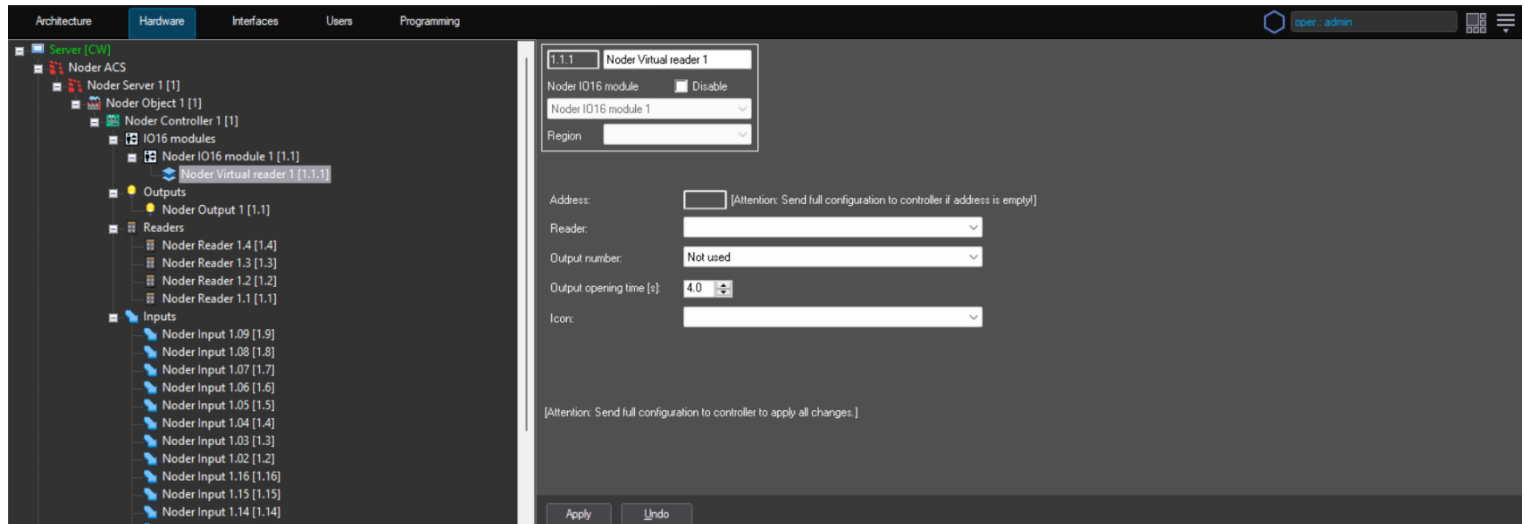
You can create a test interface to check the connection. If the connection is correct, the Event viewer will display the "Connected" event and the module icon will be green.

### 3.8.2 Virtual reader configuration

IO16RS has 16 relays that should be assigned specific objects (e.g. building floors, cabinets). To create a Virtual reader object, right-click on the **Noder IO16 module** and select **Noder Virtual reader** object. You should assign a number and name of object.



After clicking Apply button, a window of floor options will appear.



**Reader** – a physical reader in the elevator, to which the module relays are activated when an authorized card is put to device. The reader should be assigned to all floors it serves. After applying the authorized card, the relays are activated according to the access level assigned to the user.

**Output number** – module relay assigned to the floor.

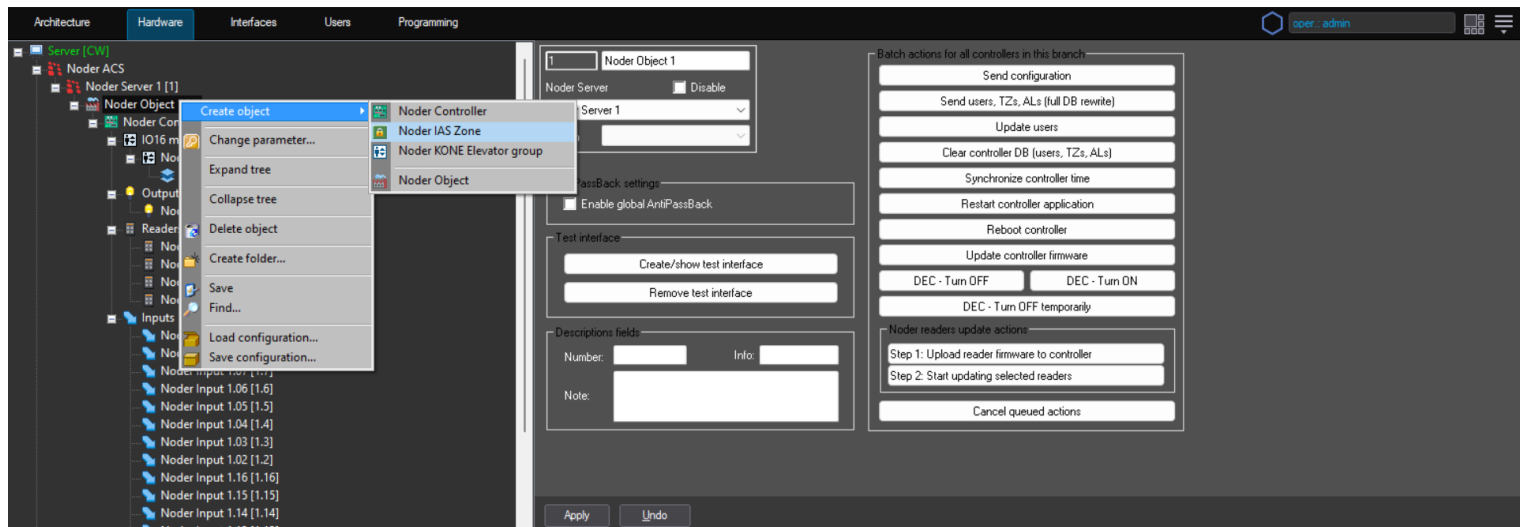
**Output opening time** – the time the module relay is actuated after the card is applied or the operator issues the "Open temporarily" command.

**Icon** – icon displayed on the map.

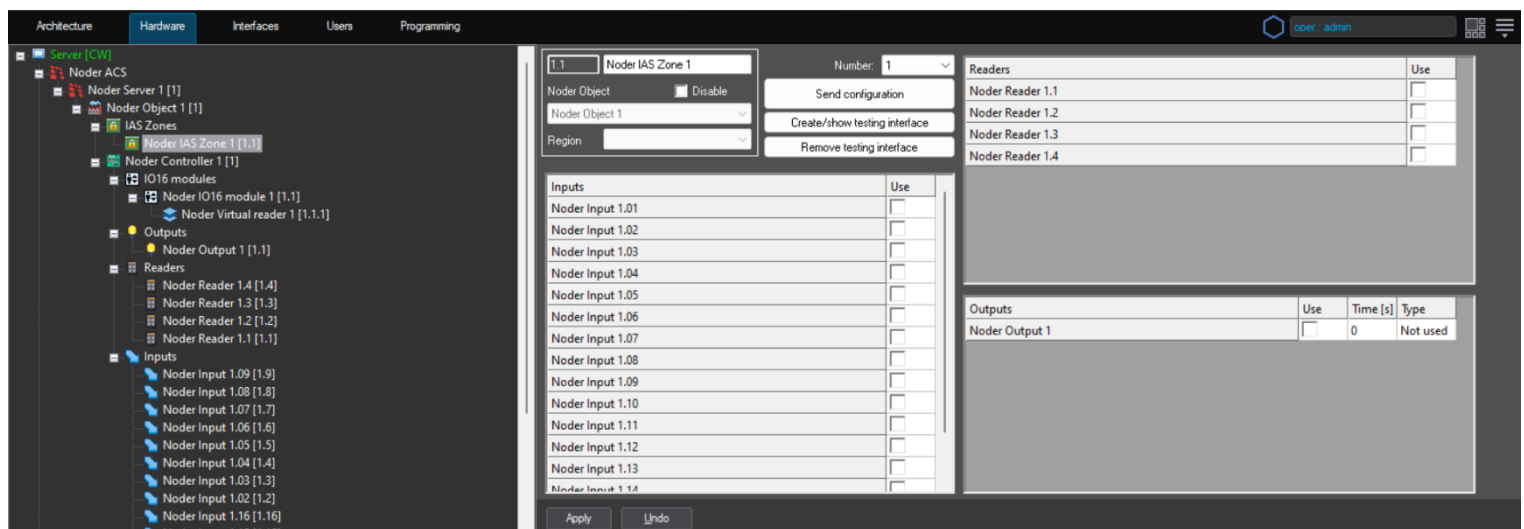
After each change of the configuration, it should be confirmed with the **Apply** button and the configuration sent to the controller by clicking **Send configuration to controller** in its settings.

### 3.9 Noder IAS Zone

To create object, right-click on **Noder Object** to which the zone will belong and choose **Noder IAS Zone**. . You should assign a number and name of object.

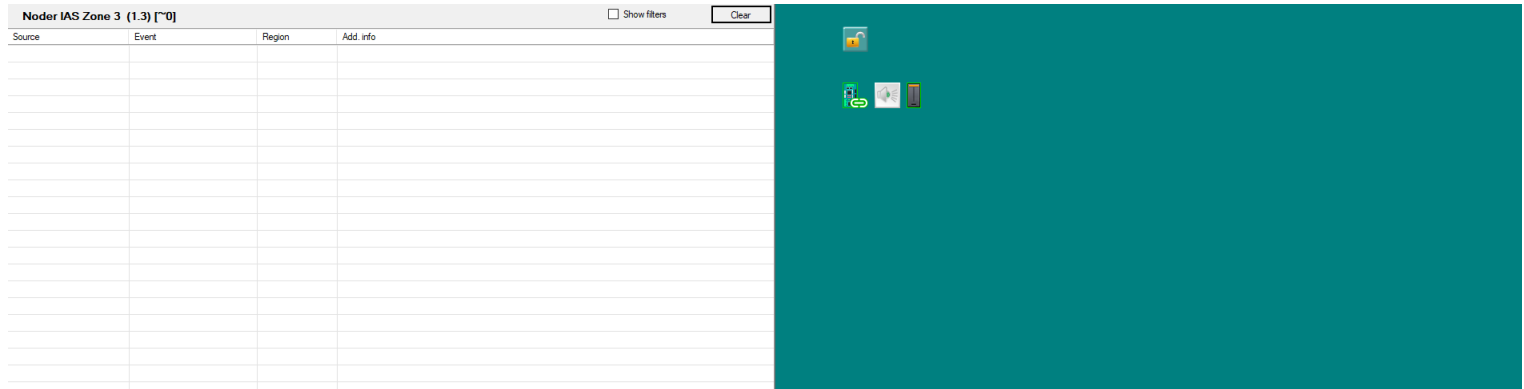


After adding the Noder IAS Zone object, configuration interface is displayed.



**Send configuration** – sends the current settings of the zone to all related controllers.

**Create/show testing interface** – creates a controller interface consisting of viewing events related to a given zone and a map with icons of zone, all controllers, readers, inputs and outputs of a given zone. If such a test interface has been created earlier, the recall of this function will refresh the map according to the current configuration and display interface.



**Remove testing interface** – removes test interface.

**Inputs** – after selecting inputs and sending configuration, they will be used in the zone. Configuration is described in chapter **Inputs**.

**Readers** – after selecting readers and sending configuration, they will be used in the zone in case of alarm (does not apply to silent alarm) or sabotage readers will start alarming. Reader assigned to zone can be also used to arm or disarm it (option **Use reader to arm/disarm zone** must be checked). Reader behaviour:

**Zone disarmed** – red LED on the reader.

**Zone armed** – red LED blinking with a frequency of 0.5 Hz.

**Zone arming** – 3xbeeper with a frequency of 2.5 Hz. When you try to arm a zone and it is **Not ready to arm** reader behaviour is orange LED for 1 second and beeper for 1 second.

**Zone disarming** – 2xbeeper with a frequency of 1 Hz.

**Alarm** – beeper for **Alarm activation time** (reader settings) with frequency of 2.5 Hz and red LED with frequency of 2.5 Hz to reset alarm.

**Reset alarm** – beeper for **Alarm activation time** (reader settings) with frequency of 2.5 Hz and red LED with frequency of 2.5 Hz to reset alarm → red LED on the reader.

**Outputs** – after selecting outputs and sending configuration, they will be used in the zone. In case of alarm (does not apply to silent alarm), sabotage (tamper or fault) controller will trigger indicated relay for a limited time. Configuration of relay number and icon is described in chapter **Outputs**.

## 4. User management

Managing users and access levels is possible using the Access Manager. Is an element of the Interface. A special user with appropriate privileges should be created to manage access control users.

Details for user service and access levels can be found in the document:

[Noder access control system operator's instruction](#)