# U-Prox

# **Access control panel**

# **U-Prox IP400**

# Installation and programming manual

**About this document**

This manual covers installation, adjustment and use of U-Prox IP400 (hereinafter panel) access control panel. Read this manual carefully prior to installing the system.

Characteristics, Intended use and parameters of the panel are described in the section "Summary". Section "Terms" provides an explanation of terms found in this document.

The look of the panel, the pins and the mode of work are described in the "Description section". Order of installation, adjustment of external devices and panel configuration are described in "Working with the device" section.

---

**Attention!** Read this manual carefully prior to installing the system.
Installation, adjustment and utilization of panel is allowed only to persons or organizations with the appropriate authority from the manufacturer

---

**Technical support**

To get warranty and technical support you can apply to authorized service centers, situated on the territory of countries, enlisted in the warranty card.

Warranty and technical support are performed on the territory of the country, where the customer applied for warranty or free service.

Technical information is available on the system website

***www.u-prox.com***

# Contents

**U-Prox**

## Brief description of the panel

U-Prox IP400 panel - a device designed to control access to residential and business premises, including time of passage of and events.

Panel operates with two readers, which are connected to the access control panel via Wiegand interface.

U-Prox IP400 processes the information received from the reader (readers), and controls actuator (e.g. a lock) with the built-in four relays.

Panel has eight End-of-line supervised inputs.

The panel can work offline or as part of the network. To add it to Access Control network Ethernet (wired computer network) are used.

The network settings of the control panel are programmed via a standard USB port (mini USB B).

U-Prox IP400 has advanced hardware capabilities and intellectual functions to control two access points (AP) with a single reader and Request to Passage button (RTE) (two single-sided AP), or one access point with two readers (double-sided AP). Having a large amount of non-volatile memory U-Prox IP400 is an access control system that provides for access control in variable establishments in small offices as well as on large enterprises with number of employees up to 31768 and up to 1,000 visitors.

Thoroughly elaborated technical and design solutions, the ability to connect two readers, communication over a computer network, non-volatile memory and the clock, protecting the communication ports and reader ports from short circuit, over-voltage and reverse polarity - all allows to use the panel to build a variety of Access Control Systems (ACS) - from the system for a small office to the entrance of a large enterprise.

## Intended use

Panel U-Prox IP400 is designed for operation in access control systems (ACS) of diverse scale in small offices as well as on large enterprises. Panels are connected in ACS via computer network Ethernet.

The panel provides access to one room with the ability to control entry and exit as well as an alarm system of rooms connected with this access point. In the case of simultaneous control of entry and exit from the rooms function " Antipassback" is provided (prohibition of re-runs).

## Characteristics

- Power supply, 12V:
  - Current consumption max 160 mA @ 12V
  - Maximum voltage ripple 500 ma peak to peak
- Wiegand interface for 2 RF ID readers connection
- Eight end-of-line resistor supervised inputs (EOL = 2kOhm)
- Two relays (contacts NO, NC, COM) 5 A @ 24 V
- Two relays (contacts NO, COM) 1 A @ 24 V
- One USB port for  network settings configuring (for connection to ACS server)
- Ethernet port, 10BASE-T/100BASE-TX
- Adjusted with U-Prox IP software
- Real-time clock
- Antipassback
- Non-volatile memory:

| IDs | 31768 |
|---|---|
| Events | 35000 |
| Time zones | 250 |
| Weekly schedules | 250 |
| Holidays | 250 |
| Temporary IDs | 1000 |

- Overall dimensions of device enclosure - 300x291x77,5 mm
- Access control panel weight - 1.0 kg
- Temperature range: 0 -55 $^0$C at 80.% relative humidity.
- Maximum relative humidity 80% without condensation

# Terms

### Identifiers

In access control systems each user has a unique RF ID. Identifiers can take the form of a plastic card, key FOB etc.

### Reader

The information on the identifiers is read with READERS, connected to the ACS control panel. There are several types of RF IDs and readers for them. It is essential that reader and control panel use the same interface. U-Prox IP400 use Wiegand interface.

### PIN (Personal Identification Number)

Some readers have built-in keypad. Keypads may be used for PIN entering. It can be both self-dependent or used as an additional code to user RF ID. When PIN is programmed as additional code, reader waits for PIN entering after RF ID is read-out.

### Access point (AP)

Access point is a logical concept of the access control system implying control of passing through a door in one direction. It consists of reader, access control panel (or its part), door supervision devices (like door contact, RTE button etc.) and door locking device. For instance, the turnstile with two-way passes has two Access points – one for entrance and the other one for exit, door of this type is called double-sided door. A door with a reader on one side has only one Access point – Entry point, and it is called single-sided door.

### Direction of passage

Passageway - is a logical unit of ACS, controlling passage through the access point in one direction. It includes reader, access control panel (or part of access control panel), actuator. So, tourniquet with double-sided control has two passageways, and the door, having single-sided reader - only one passageway. Access point, which consists of two passageways, is called double-sided, and the point of access, which consists of one direction of passage - single- sided.

### RTE (request to exit)

To exit from the premises with a single-sided door, a button wired to control panel is used. This button is called RTE (request to exit) button. If someone opens a door otherwise than pressing RTE button – by re-energizing locking device, opening lock with a key etc., "Door Forced Open" event arises. RTE button may be used for remote door opening as well.

### Door contact

Properly designed ACS is used to supervise door status (opened or closed), such as magnetic door sensor, sensor of the turnstile rotor position, inductive sensor of the road barrier, etc.

This ensured that the system prevents situations when several users access the door with one RF ID or door left open after user's access and so on. For these purposes the magnetic sensor of door closing, position sensor of the turnstile rotor and the position sensor of boom barrier are connected to the input of access control panel. The input used to connect these sensors, is called the input of sensor of passage (or Door Contact)

**Antipassback**

Antipassback function is implemented in access control panels to prevent the situation when user gives his RF ID to another person after passing into the premises. If this function is on, control panel tracks an RF ID position – inside or outside the premises. On any attempt to pass in the same direction twice the panel denies access and stores "Access Denied, Antipassback" event into the Log.

Antipassback function can be set On only in case of the double-sided door control.

**Global antipassback**

Prevents user door pass from the areas where he must not appear. The facility spitted into the closed areas connected with double-sided access points, in which system supervises the personnel appearance for this purpose. System detects the global antipassback violation when somebody tries to re-enter such area without exit or tries to enter somewhere from the area he have not enter. System generates message "GLOBAL ANTIPASSBACK: Access Denied" in case of global antipassback violation.

**Door time**

If door sensor is open, corresponding access point goes into "Alarm" mode (refer to "Alarm» mode below). Alarm is not invoked, if contact is opened during Door Time interval. This interval starts when access is granted and lasts for the programmed time or terminates on opening and subsequent closing of door contact.

**Code matching attempt**

Control panels can activate alarm on attempt of a code (or RF ID) matching. Code matching is considered when invalid code (or RF ID) is entered several times successively. Valid code entering clears the counter. This function switching On and number of code entrances are subjects of programming.

**Schedules**

Date and time of valid access are indicated when setting user access rights.

Depending on modification, control panel stores up to 250 time zones. 250 week schedules can be combined from these time zones. Moreover, control panel can store up to 250 holidays, which happen once a year.

**Time zones**

Time zones are a part of schedule. This is a way to organize a range of days and times and associate it with access levels.

Time zones are utilized by the application to validate, authorize, or perform various functions based on schedules.
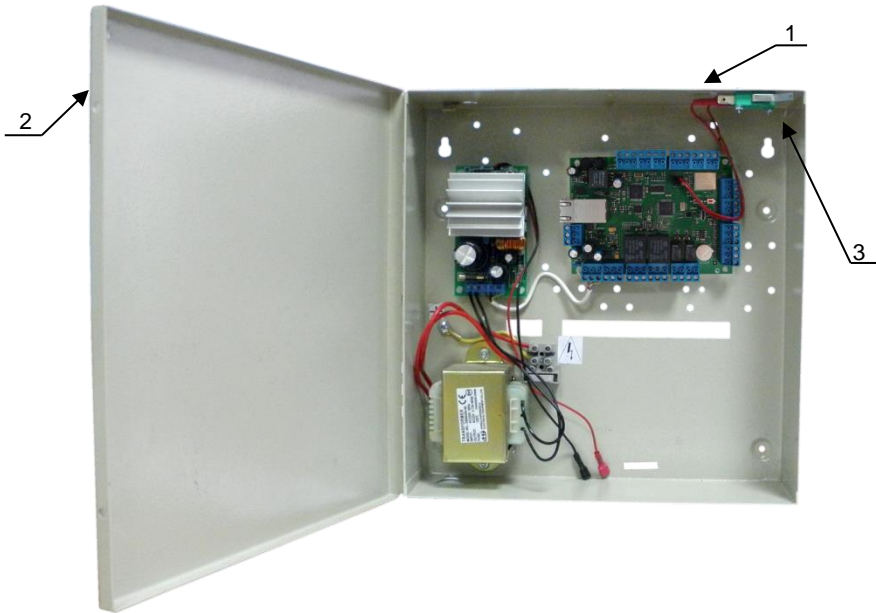
**Downloading**

Control panel is to be downloaded after all parameters are set – modes of inputs, outputs, access rights and others. During downloading parameters are rewritten into access control panel.

# Description and operation

**Panel**

The look of the access control panel is shown in Fig. 1



1. The Enclosure
2. The top cover of the Enclosure
3. Tamper

**Fig.** 1. U-Prox IP400 panel

Location of jumpers and removable pads with connectors on access control panel board and their function is shown in Fig. 2
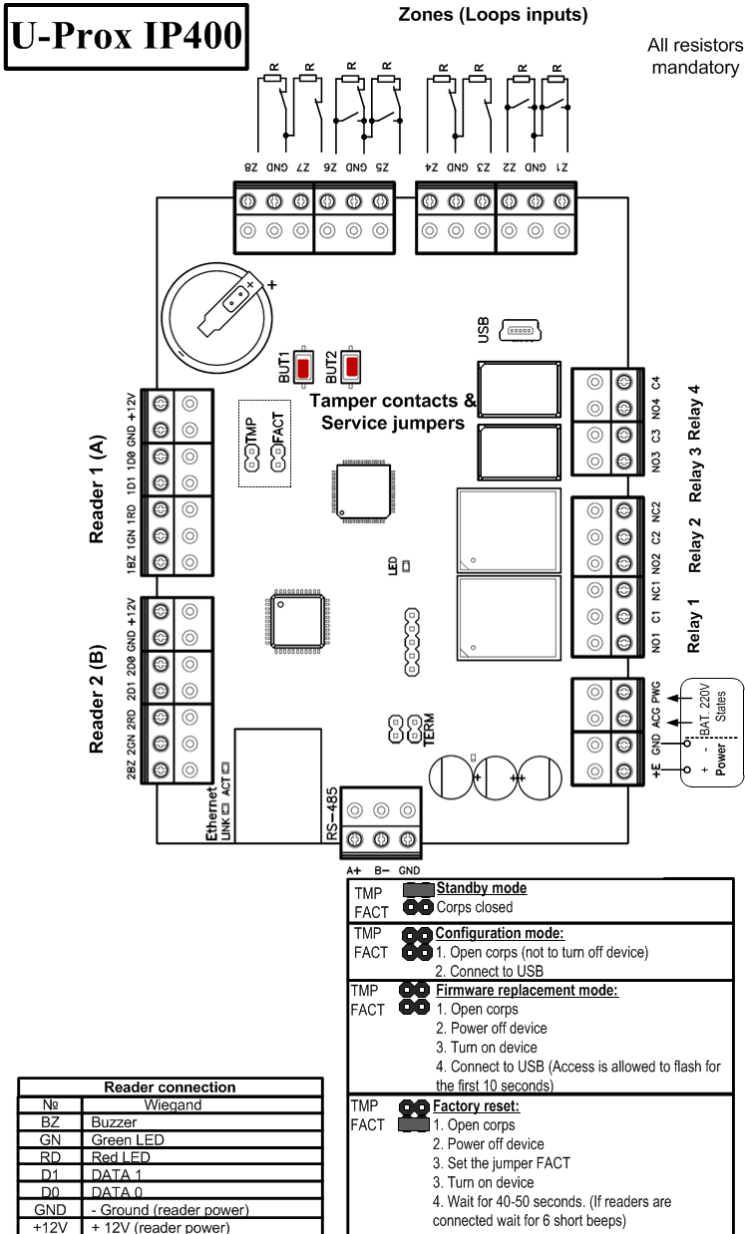


**Fig. 2.** U-Prox IP400 components

**Assignment of the access control panel**

| Contact | Name | Purpose |
|---------|------|---------|
| Z1 | Z1 | Terminals for Loop |
| Z2 | Z2 | |
| Z3 | Z3 | |
| Z4 | Z4 | |
| Z5 | Z5 | |
| Z6 | Z6 | |
| Z7 | Z7 | |
| Z8 | Z8 | |
| GND | GND | |
| NC1 | normally closed | Relay contacts 1 |
| NO2 | normally disclosed | |
| C1 | General | |
| NC2 | normally closed | Relay contacts 2 |
| NO2 | normally disclosed | |
| C2 | General | |
| NO3 | normally disclosed | Relay contacts 3 |
| C3 | Total | |
| NO4 | normally disclosed | Relay contacts 4 |
| C4 | General | |
| 1BZ | Buzzer | Connection of an reader 1 ('A' access point of the door) |
| 1GN | green LED | |
| 1RD | red LED | |
| 1D1 | Data 1 | |
| 1D0 | Data 0 | |
| +12 V | Power | |
| GND | GND | |
| 2BZ | Buzzer | Connection of an reader 2 ('B' access point of the door) |
| 2GN | green LED | |

| 2RD | red LED | |
|---|---|---|
| 2D1 | Data 1 | |
| 2D0 | Data 0 | |
| +12 V | Power | |
| GND | GND | |
| A+ | RS-485 A+ | Port RS485, for future use with extension modules |
| B- | RS-485 B- | |
| GND | RS-485 GND | |
| E+ | | External power supply |
| GND | | |
| ACG | Battery OK | Status of power supply |
| PWG | Mains 220V OK | |
| TMP | Tamper | Tamper switch |
| USB connector | | |
| USB Mini B | USB connector | For initial configuration of the network settings |

**Jumpers**
**Service**

- TMP – tamper contact
- FACT - Factory reset

**Buttons**

- But1 – access point A RTE button
- But2 – access point B RTE button

**Sound and light panel**
   **Yellow LED:**

- Standby mode (periodic blinking):
  - 1 short pulse once per second - communication - working in notification mode, connection normal;
  - 2 short pulse once per second - communication - working in notification mode, no connection
- frequent blinking - downloading data from the server
- uploading mode:
  - LED is on for 5 seconds - detection of TMP jumper removing, uploading mode start

- o frequent blinking - waiting in uploading mode (jumper TMP off), this indication means that the attempt to upgrade the firmware failed
  - o 6 short blinks - successful **upgrade of firmware**
  - o 2 short blinks - uploading mode exit
- 6 short beeps (enclosure opened and shorted jumper FACT) - Factory reset (reset to factory settings was done)

LED **Link**:

- On - Ethernet cable is OK

LED **Akt.**:

- Frequent blinking - Data Exchange.

## Panel operation

The panels supplied unloaded with factory settings below in document. In this state, the indicators of readers and the yellow LED on the panel flashes once per second. To make the panel work in access control system (ACS) you have to upload a network setting using the "Configurator" software and USB port.

If no inputs are triggered panel goes to mode "Normal" after uploading the configuration. Panel can supervise two independent access directions. There are four different modes of access point: "Normal", "Alarm", "Blocking" and "Free pass". Mode "Free pass" has the highest priority, as this mode is activated in the event of a fire, followed by modes of "Blocking", "Alarm" and "Normal." in decreasing order of priority.

### "Normal" mode

This is the main mode of panel. In this mode the panel grants or denies access to RF ID owners. In "Normal" mode the readers blink red.

### *Passing after entering RF ID*

To pass through user enters contactless RF ID to the reader. If RF ID is registered and the passage is granted, access point opens (the panel activates the actuator). The reader LED becomes green.

### *Passing after entering RF ID and PIN code*

On entering enrolled RF ID, panel tests whether PIN code is required, and, if required, waits for entering PIN code. After entering the correct PIN code, AP opens (the actuator is activated).

The reader LED becomes green.

### *Passing upon Request to Exit (remote opening of doors)*

Exit from premises with single-sided door or passing of users is granted upon pressing Request to Exit (RTE). Pressing and releasing of RTE AP opens the door (actuator is activated). The reader LED becomes green.

### *Access denial upon entering RF ID*

Access may be denied to RF ID owner due to the following reasons (the reader LED is red)::

- Cards (RF IDs) and schedules are not loaded in the panel (light off)
- access control panel is in unloaded state
- card is not enrolled in the panel
- card term expired (for 1 second buzzer is on and LED is red )
- RF ID passed out of schedule (for 1 second buzzer is on and LED is red)
- attempt to re-pass when "Antipassback" is on (for 1 second buzzer is on and LED is red)
- entered RF ID is marked as lost or blocked (for 1 second buzzer is on and LED is red)
- the panel is in "Alarm" mode (LED is constantly on and red)
- the panel is in "Blocked" mode (LED flashes red and yellow)
- Pass count is exhausted for the temporary card (visitor).

**"Alarm" Mode**

In "Alarm" mode the reader indicator is constantly red. Depending on the programmed functions Access point goes into mode **"Alarm"** in case of unauthorized passage (Door Forced Open), opening of panel cover, entering RF ID recorded as lost, if AP is open too long (open time AP is exceeded), and in case of RF ID matching attempt.

In "Alarm" mode panel activates outputs, programmed as ALARM and SIREN.

"Alarm" output remains activated till "Alarm" mode is turned off. For output "SIREN", siren time is programmable.

If Access point is in "Alarm mode", passage is prohibited. Access point may be opened by pressing RTE.

To exit from the "Alarm" mode pass the ID with "Disalarm" attribute or by command from the computer.

**"Free Pass" Mode**

There are circumstances when you need to open access points for Free pass of people, such as in the case of fire, earthquake or in other emergency. For this case, the panel has "Free Pass" mode.

In "Free Pass" Mode LED of reader flashes green and yellow.

The access point goes into "Free Pass" Mode after the command of operator from the computer or after the loop violation (break or shortage) programmed as FREE PASS. The access point is in "Free Pass" Mode for as long as the loop FREE PASS is broken or until the command from the computer comes (while the loop is broken, command from the computer will not work).

The panel allows to configure the function of loop "Free Pass" for access points A, B,

> or for both access points (A + B).

As long as access point is in "Free Pass" mode, the lock is held in open position, the panel stores a log event "Access granted" on presentation of RF ID code regardless of the antipassback state of, schedules, etc. It is used to control the presence of personnel on the premises in case of an emergency.

To ensure "Free Pass" mode when using locking devices with mechanical re-platoon you must control access point state. Locking devices with mechanical re-platoon can be unlocked with current pulse and remain unlocked until access point is not opened. While closing door, locking device goes into a closed state. Panel in "Free Pass" mode tests the door contact. Each closing of door again gives unlocking signal to the door.

**"Blocking" mode**

If it is necessary to deny access to AP to all users of the system, the panel switches into "Blocking" mode. If AP is in "Blocking" mode, the passage is granted only to owners of RF IDs with the sign "Security Service". AP cannot be opened by pressing RTE.

> In Mode "Blocking" LED is alternately flash red and yellow

Access point goes into "Blocking" mode after the operator command from the computer or after loop violation designated as BLOCKING. Access point is in "Blocking" mode for as long as the loop is violated or until the command from the computer (while the loop is broken, command from the computer will not work).

> Panel allows to configure loop function "Blocking" for access point A, B, or for both access points (A + B).

**RF ID properties (cards)**

*Code (RF ID card code)*

Each card has a unique code which is set at the time of its manufacture. It consists of 10 hexadecimal digits.

*PIN-code*

Additional code is assigned to the card. It consists of no more than six decimal digits. It can be used together with readers that have a built-in keyboard.

Enter PIN code with the reader's keypad and press '#' key. Always enter PIN code AFTER the card pass. If PIN-code is correct, panel unlocks access point and grants access. Otherwise, panel generates a warning signal, and records "Invalid PIN-code" event into the log. Door remains closed.

*Validity (of Card)*

Card Validity expiration date

**Alarm Cancel**

Passing the card to door reader, when the door is in "Alarm" state, panel registers event "Alarm cancelled" and puts the door to Normal mode. If the card that has no right to cancel the "Alarm" is passed, the door will remain in the same state. "Access denied. Alarm Status" event recorded into the log.

*Security Service*

Security Service mark gives the right of access to a blocked door.

When the ordinary card is passed if door is in "Blocking" Mode, "Access denied. Blocked state" event recoded. Card with attribute "Security Service" pass. If the card is valid and has access right at the moment, the panel gives access and event "Access granted. Blocked state» is registered.

*VIP*

Access right to pass always everywhere, except through blocked door.

VIP card may be assigned any schedule, Antipassback and validity period is NOT applied to it. The card may have PIN code

If the door is in "Blocked state", access is denied for RF ID with this attribute checked.

*Antipassback is off*

Access right without considering Antipassback Mode.

Access is granted regardless of the direction of the previous access, but due to the schedule and other attributes designated to the Card.

**Variants of Use and modes of output**

All panel outputs can be programmed in any order for several functions: Blocking, Siren, Alarm, Programmable output. In addition, there is programmable operation mode for each output: start-stop (output remains active until the corresponding command is present, for example, during the time until the panel is in "Alarm" Mode), impulse (the output is activated for the programmed time), trigger mode (on the first event the output is activated, on the following is off, etc.), continuous.

**The communicator**

U-Prox IP400 panel operates automatically - after downloading data from the server, it processes the card passed according to its access rights, grants or denies access and sends event rehire to the ACS server.

Panel communicator operates in the **notification** mode. If there is event (passage, violation of input) event report message is send ACS server.

U-Prox IP400 panel can be connected to a computer network via wired connection (Ethernet). This ensures work within local network (see Figure 3) or via the Internet (see Fig. 4), that allows to build distributed access control systems of any size.
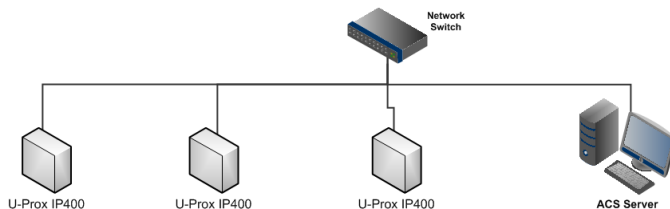


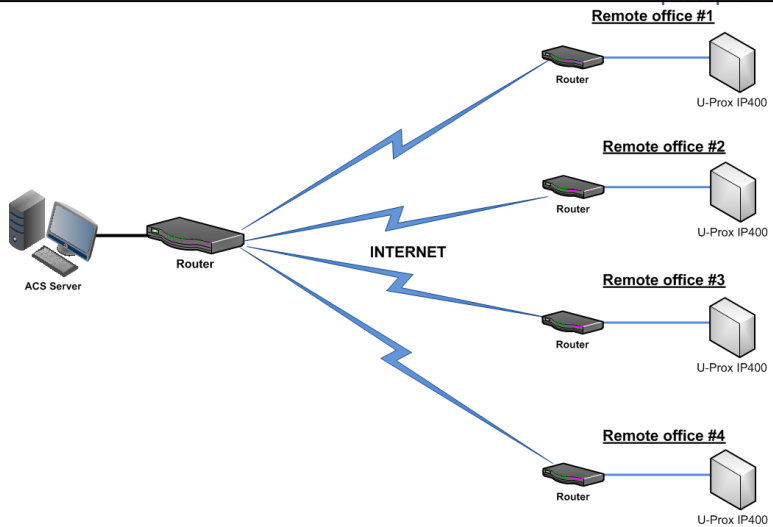**Fig. 3.** An example of a local network

**Fig. 4.** An example of a distributed network

*Algorithm of working in LAN*

1. If DHCP on (IP is 0.0.0.0) - obtaining IP address with the start of the access control panel

2. Update of IP status of address (announcement and extension of reserved IP, if DHCP)

3. Determine accessibility of ACS server and U-Prox IC A control panel (IP or DNS name)

4. Periodic sending of test signals

5. If there is, sending of events. Waiting for server commands.

*Algorithm of working on the Internet (local wire net)*

1. If DHCP on (IP is 0.0.0.0) - obtaining of IP address within local network affiliate at panel launch

2. Update of status of IP addresses (announcement and extension of reserved IP, if DHCP)

3. Determine possibility of access to the Internet (accessibility of given IP address of router)

4. Determine accessibility of ACS server and U-Prox IC A control panel (IP or DNS name)

5. Periodic sending of test signals

6. If there is, send the events. Waiting for server commands.

7. Failure - transition to the second specified IP address of router.

### *Server addresses automatic configuration for control panel*

The use of the existing computer network infrastructure, standard network protocols (DHCP for instance) allowed to provide the "plug-and-play" principle. The mode of the automatic server address configuration in the panels eases the access system deployment significantly.
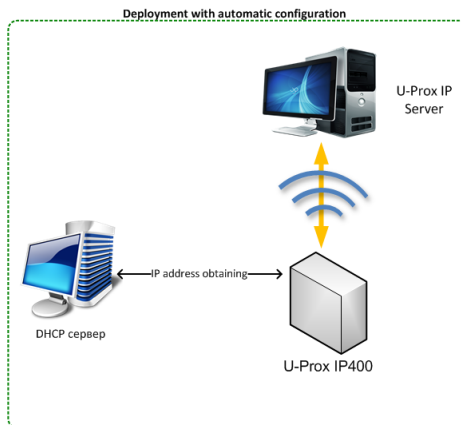


**Fig. 5**. System deployment

The algorithms for operation on each step described below

1. Panel checks for DHCP mode ON (panel address 0.0.0.0) or static IP
2. If DHCP mode is ON, the dynamic IP address obtain routine will start
3. The panel automatic configuration mode starts if the access control system IP address (IP or DNS name) is not set:

    a. Panel sends data packages announcing access control system server about itself as a new device in the local network

    > Despite it is broadcast announcement, it is limited with single range local network and active network equipment. That's why the IP addresses of the access control system server are to be set manually for networks with sophisticated topology.

    b. The system will warn operator after the receiving of the data package from the new panel. Operator must add panel to the system database (DB).

    c. After the panel added to the DB it receives the answer from the access control system server. The address of the access control system server recorded into the control panel and it stops to broadcast.

    d. Operator has to upload panel after its adjustment recorded into the DB. Panel becomes associated to the certain access control system server, eliminating panel control capture with another system.

17

> Return panel to the factory settings to eliminate the panel association to the system

e. In the case of access control system server IP address change panel will initiate the automatic configuration routine, but the data exchange will be possible with previously connected system only.

**Global antipassback**

U-Prox IP400 control panel can operate in a system of global antipassback. The main controller U-Prox IC A tracks the location of a person on the fact of its passage through the access point. U-Prox IC A receives data about the passages from control panels NDC F18 IP, U-Prox IP100, U-Prox IP300, U-Prox IP400.

The basis of the global antipassback is the zoned antipassback. The facility is divided into rooms - zones of access or areas. With this division the entrance to another area is exit from the previous one, and the passage in the area is possible through various access points.

Antipassback control panel receives data from the access control panels and tracks the movement of personnel from area to area . Also can be tracked the location of the person who has multiple IDs (See Figure 6).
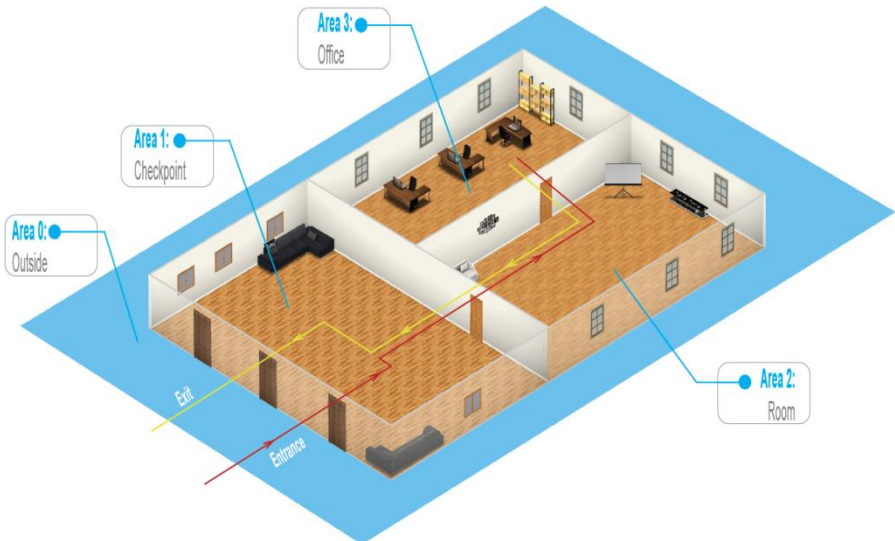


**Fig. 6. Allocation of access areas**

Initially an employee has the location "unspecified". After the first presentation ID to a reader's location

The location "unspecified" is assigned when registering a new employee, or after the system operator command "location reset" of person is fixed by U-Prox IC A.

With the use of global antipassback it is possible to suppress passback, using duplicate card for infiltration (sudden appearance inside), transferring the ID to another person, etc (See Figure 7).
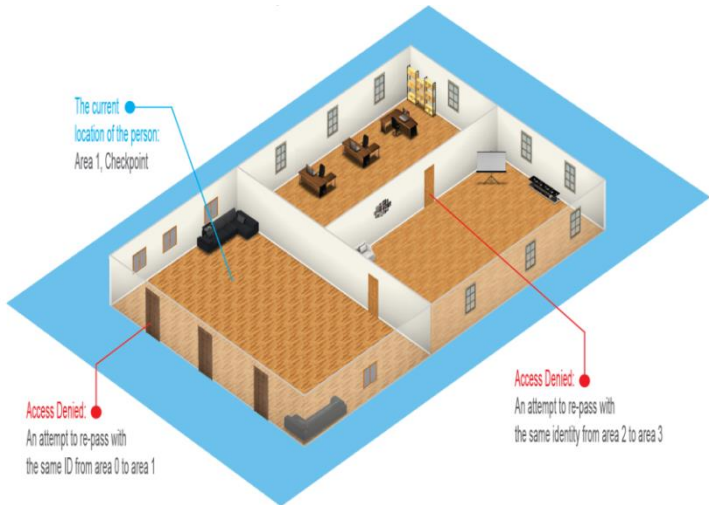


**Fig. 7.** Tracking the violations

In case of lost communication with the access control panels, forced entry, free pass, etc. U-Prox IC A merges access areas together , considering that the personnel may be both there and there.

After restoring the normal state of access point or communication with the control panels, areas will be unmerged (See Figure 8).
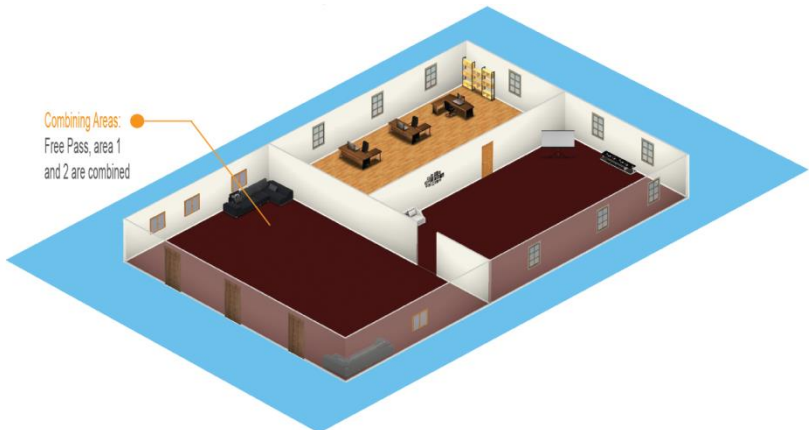


**Fig. 8.** Merging access zones

U-Prox IP100, U-Prox IP300, U-Prox IP400, NDC F18 IP access control dialog boxes can be configured to two variants of behavior in case communication lost with U-Prox IC A:

- Not just anyone has permission to pass;
- Pass all, according to the rules of the local antipassback

*The requirements for U-Prox IC A adjusting:*

- The control panel must have a static address (IP or DNS)

*The requirements for U-Prox IP100, U-Prox IP300, U-Prox IP400, NDC F18 IP adjusting:*

- Only control panels with double-sided doors (entrance and way out on presentation of ID) can be involved in global antipassback.
- In configuring server address # 1 has to be the ACS server address.
- In configuring server address #2 has to be the address of the U-Prox IC A
- In the U-Prox IP software must be enabled antipassback mode "General" for the door
- For each access control dialog box must be specified master antipassback control panel and reaction to the deprivation of communication with him.

U-Prox IP100, U-Prox IP300, U-Prox IP400, NDC F18 IP control panels deliver events to two destinations at the same time. First one is ACS server's address, to display and store events in a database program. The second one is address of U-Prox IC A. The Antippassback control panel sends an answer with command to deny or grant access.

After ID presentation the delay in granting or denial of access may be up to 1 minutes, depending on the topology and bandwidth of the computer net

# How to work with the device

Before installation do initial setup of access control panel (that specifies settings of network parameters) with utility "Configurator" via USB Port. Overall dimensions are shown in Fig. 9
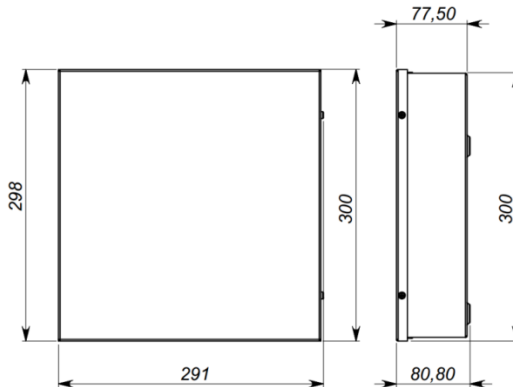


**Fig. 9**. Overall dimensions

**Connection procedure**

1. Before installation, do initial setup of panel (that specifies settings of network parameters) with utility "Configurator" via USB port

When the panel is in stand-alone mode, paragraphs 11 and 12 should be performed before paragraph 2.

2. In the place of installation of the panel do preparing - mark and drill the holes (see Installing panel)
3. Run the cable lead from the power supply
4. Run the cable lead from the actuator (lock)
5. Install external readers and run their cables (if necessary)
6. Run loops from sensors / buttons
7. Run cable lead-Ethernet (if necessary)
8. Placing of installation cables in the wall
9. Fit and fix access control panel enclosure
10. Run the wire commutation of power supply, lock, reader, inputs of the panel with the loops in accordance with the sections below
11. Perform installation of the Ethernet cable into the connector terminal blocks
12. Place the top cover and fix it with screw
13. Connect the panel to ACS (in accordance with the instructions ACS)
14. By means of ACS, perform full panel adjustment (set of inputs, outputs, schedules, RF IDs, etc.).
15. Ready for operating

**Installation recommendations**

Access control panel should be placed in a place accessible for maintenance.

To install the access control panel on the wall (see Fig. 10), do the following:

- open the cover, attach the enclosure to proposed site of attachment and make layout of holes;

- pass the wires through the holes in the wall of enclosure;

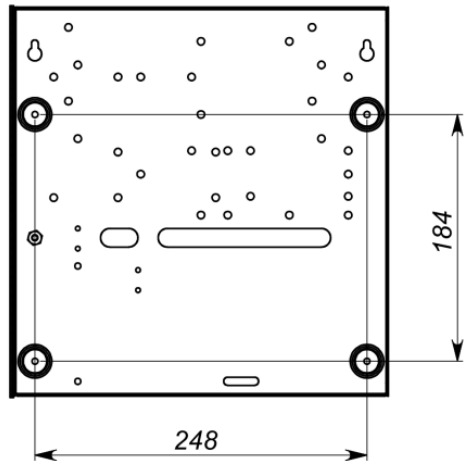- attach the access control panel;

- connect the wires



**Fig. 10. Marking fixing holes**

**Connecting external readers**

The panel has two Wiegand format ports for external readers. Together with access control panel a variety of readers can run.

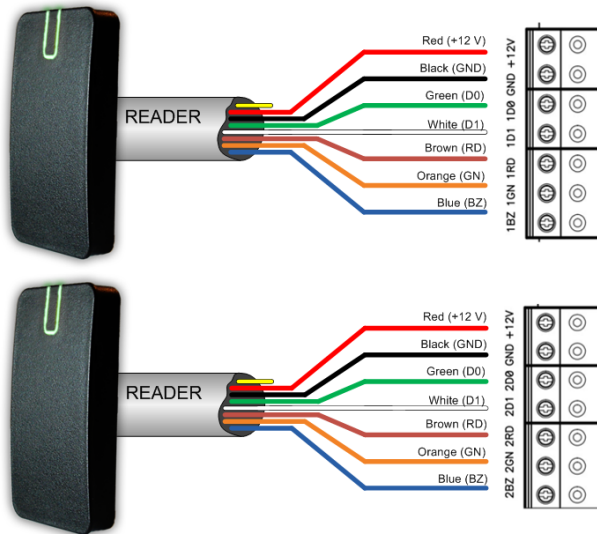In Fig. 11 connection of readers is shown.



**Fig. 11.** Connecting external readers

Color matching circuits:

- White - data 1

- Green - data 0

- Blue - inclusion of buzzer signal

- Brown - inclusion of red indicator

- Orange - inclusion of green indicator

- Black – GND

- Red - +12 V

When using readers of different manufacturers, colors of wires may vary. Color matching wires; see the operating instructions for the reader.

Current consumption of each external reader connected to terminals "12 V" should not exceed 100 mA. When connecting to panel a reader of long range with current consumption more than 100 mA, supply the voltage to it from the separate source.

## Connecting LoopControl

Panel has eight inputs for connecting the loops supervised with end of line resistors. Each input functionality programmable. Inputs' functions are:

- Door Contact
- RTE
- Door Contact + RTE
- Free pass (A, B, A+ B)
- Blocking (A, B, A +B)
- Sensors monitoring

The following describes how to connect various types of inputs. After factory reset all loops have no purpose and are not supervised. All loops work both for closing and opening.

> Normal state of the loop - from 1.4 kOm to 3kOm, Line shortage - less than 1.4 kOm, the broken line - more than 3 kOm.
> It is recommended to use supplied resistors.

### Request to Exit button (RTE)

RTE is used for exit through single-sided door. In this case, access point opens when you press and release RTE. Use this input type for remote door opening button connection also. For example, to open the door manually, by the secretary or security guard.

The example of normally open contact RTE buttons connection to Z1 and Z2 terminals is on the Fig. 12.
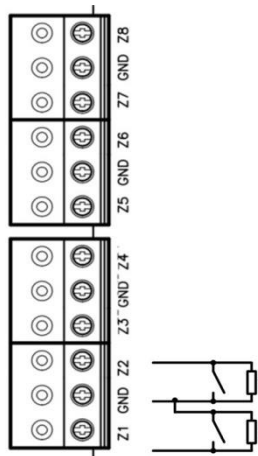


**Fig. 12**. Connection of RTE button

Z1 and Z2 inputs function assigned as follows:

- Z1 – Request to Exit button (RTE) of access direction A

- Z2 - RTE of access direction B

The use of button of the electric lock to open access point or "allow access" button on the turnstile evokes the "DOOR FORCED OPEN" event

*For proper operation, it is necessary to assign the connected loops as RTE when programming.*

**Door Contact**

Control panel supervises the door state or position of the turnstile rotor wit the door contact. Panel cannot detect unauthorized access or door is open too long (multiple entrance with one ID for instance) without the Door Contact.

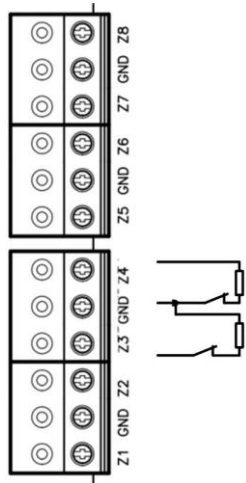The example of normally closed door contacts connection to Z3 and Z4 terminals is on the Fig. 13.



**Fig. 13**. Connecting door contacts

Z3 and Z4 inputs function assigned as follows:

- Z3 - door contact of access direction A

- Z4 - door contact of access direction B

Access point, controlled by ACS, must have the door closer.

*Program input as 'Door Contact' for proper operation of the door contact.*

The control panel can operate without the door contact. In this case, after the passing RF ID for identify and granting access, an event "Access granted" is generated, the control panel send unlocking impulse, and returns to normal mode after door time expire.

**Combined Loop- RTE and Door Contact**

Panel inputs can be configured for simultaneous use of RTE button and Door Contact on single loop. In this case the loop breaking means breaking of Door Contact and (short-circuit) shorted - pressing of RTE button.

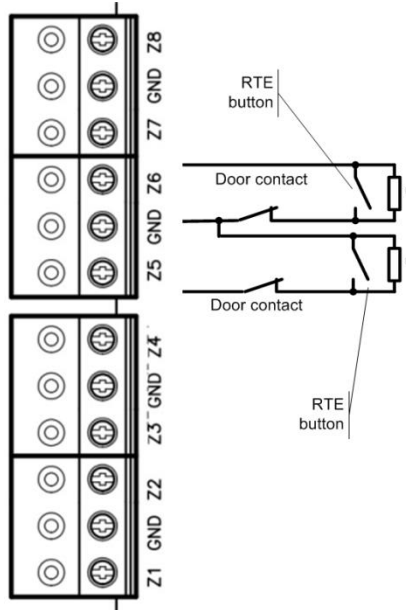The example of combined loops connection to Z5 and Z6 terminals is on the Fig. 14.



**Fig. 14.** Connecting combined loops

Z5 and Z6 inputs function assigned as follows:

- Z5 - Combined door contact and RTE button of access direction A

- Z6 - Combined door contact and RTE button of access direction B

*Any of 8 inputs can be assigned as a combined for service of door contact and RTE button*

**Integration with the fire alarm system**

It is necessary to program the input as "Free Pass" for work with fire alarm system. Connect fire output of the fire control panel to "Free Pass" input. All access points controlled by the panel will release on "Free Pass" input violation. The Fire output of fire control panel can be directly connected to this input. When fire alarm is on, loop of access control panel, designated as "Free pass", is broken. All access points, supervised by access control panel, are automatically released and the staff can freely leave the zone of fire (see Figure 15).
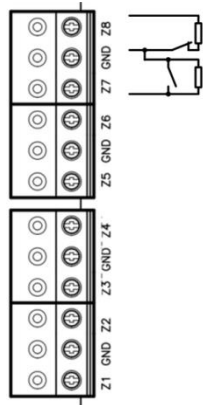
**Fig. 15.** Connecting Blocking and Free Pass loops

Z7 and Z8 inputs function assigned as follows:

- Z7 – Blocking A+B

- Z8 – Free Pass A+B

*"Blocking" can be assigned to the direction of passage A, B and A + B*

*"Free Pass" can be assigned to the direction of passage A, B and A + B*

*"Blocking" and "Free Pass" input can work for short and break circuit.*

It is necessary to program the input as "Blocking" for work with security alarm system. Connect fire output of the alarm control panel to " Blocking " input. All access points controlled by the panel will release on " Blocking " input violation. The Alarm output of security control panel can be directly connected to this input. When security alarm is on, loop of access control panel, designated as " Blocking ", is broken. All access points, supervised by an access control panel, are automatically blocked and only security service staff can entrance.

## Actuators

Panel have four relay to supervise actuators. Panel controls electric lock or latch, barrier operation, turnstile, or turns on and off any optional hardware with this outputs.

Relays 1 and 2 have normally closed and normally open contacts. Relays contacts rating is 1A @ 24V. Relays 3 and 4 have only normally open contacts. Relays contacts rating is 0,5A @ 12V.

---

Voltage ripple at actuator operation must not cause the panel malfunction. In case of such malfunction power up actuators from alternate power supply.

---

**Electric locks**

Normally closed and normally open relay contacts, are programmable for a wide range (0 ... 255 sec) of lock operation time. Thus panel may control a wide range of electric locks and latches of almost any type.

When the lock time is equal to 0 pulse duration of 200 ms will sent to relay.

The example of actuator connection is on the Fig. 16. The first is powering the lock and second by depowering.
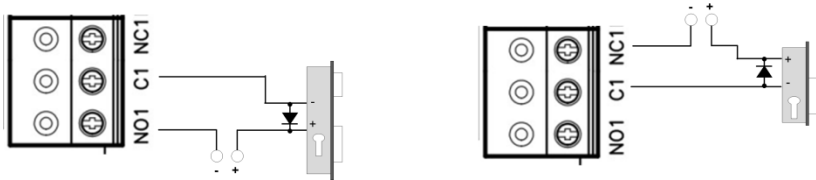


**Fig. 16**. Connecting locks

When using relay to turn on / off current via inductive load, for example, to run electromagnetic lock, there are electric pulses of high amplitude. To prevent damage of relay contacts shunt inductive load by diode, set in opposite direction to voltage of coil supply

Remember, that low-cost solenoid latch do not allow long power supply. For these latches program the lock time as short as possible to prevent coil overheating.

Do not use diodes for connecting actuators to AC power supply.

*Assign relay outputs as outputs of locks at panel programming for proper operation.*

**Sirens and Bells**

Electric bell (see Fig. 17) are inductive load for voltage source. When connecting a bell to DC source it is necessary to use a protective diode (see warning about the inductive load).
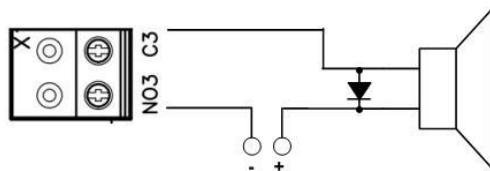


**Fig. 17**. Connecting bells

Read the instructions when connecting sirens. Current consumption of sirens should not be more than 1 A

When using custom actuators (magnetic starters, turnstiles, etc.), refer for advice to your hardware vendor.

For proper operation of the siren assign the relay output as a siren output (alarm, etc.) when programming.

### Connection

Wired computer network used for U-Prox IP400 communication to the ACS server. Device setup is possible with using autoconfiguration or manually with a PC using the software "Configurator":

Appropriate configuration provides:

- Assigning of static or dynamic (DHCP) IP address to a device;

- Working with two (primary and backup) IP or DNS (Domain Name Service) of ACS server addresses;

- Working on the Internet (service of remote branches) with the ability of reserving paths to the Internet via the second router;

Panel works automatically after data upload from the ACS server. It processes access rights for IDs passed grants or denies access and sent event reports to the server.

Panel communicator operates in notification mode. If there is event (passage, input violation) data transmission to ACS server is initiated.
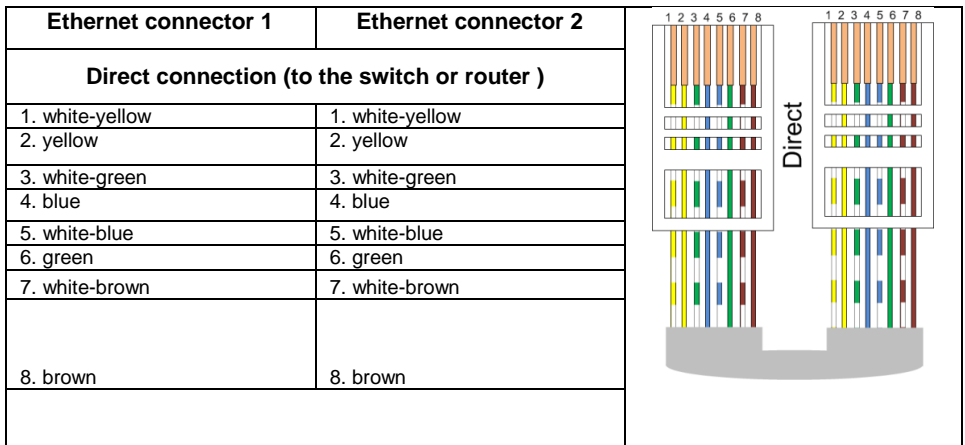
Panel provides protection against arbitrary interference due to the encryption of data with 256-bit key and against panel substitution supervising the unique serial number of the device at its work in the network. It also provides supervision of the communication channel by means of periodic test signals from the device.

### Wired computer network (Ethernet)

Ethernet interface is used to connect components of the system (PC and access control panels) in the network. Ethernet cable length without additional equipment can be up to 100 meters

Use standard Ethernet cable, and RJ45 connector. Transfer rate is up to 100Mb / s.

In **Fig.** 18 examples of connection cable Ethernet are shown.

| Ethernet connector 1 | Ethernet connector 2 | |
|---|---|---|
| **Direct connection (to the switch or router )** | | |
| 1. white-yellow | 1. white-yellow |  |
| 2. yellow | 2. yellow | |
| 3. white-green | 3. white-green | |
| 4. blue | 4. blue | |
| 5. white-blue | 5. white-blue | |
| 6. green | 6. green | |
| 7. white-brown | 7. white-brown | |
| 8. brown | 8. brown | |

**U-Prox**

| Crossover (directly to the computer network card) | |
|---|---|
| 1. white-yellow | 1. white-green |
| 2. yellow | 2. green |
| 3. white-green | 3. white-yellow |
| 4. blue | 4. blue |
| 5. white-blue | 5. white-blue |
| 6. green | 6. yellow |
| 7. white-brown | 7. white-brown |
| 8. brown | 8. brown |
| | |

**Fig.18.** Connecting cable Ethernet

To configure the Ethernet device of access control panel:

- Enable Ethernet communication
- Set network parameters of panel (do not set if you use DHCP):
  - IP address
  - Subnet Mask
  - IP address of the gateway (router) Internet 1 (not necessarily in the local area network)
  - IP address of the gateway (router) to the Internet 2 (optional)
  - IP address of the DNS Server 1 (if data transfer of the domain name is used)
  - IP address of the DNS Server 2 (optional, if data transfer of the domain name is used)
- Setting communication with server:
  - IP or DNS address server 1
  - IP or DNS address server 2 (address of U-Prox IC A panel, optional)
  - Access Ports (port to read and port to write)
  - Period of the link channel checking (test signal)

**Panel programming**

| Software | Operation |
|---|---|
| | 1. Determination of access control panel mode: standalone or as part of ACS |
| The"Configurator" Software- connect via USB port | 2. Setting initial parameters: network settings of access control panel:<br>a. Server settings: IP address or DNS name of the server, access ports (port to read, port to write)<br><br>Don't proceed paragraph d. if DHCP used in the network.<br><br>b. Device Settings: IP address of the device in computer network, subnet mask, IP DNS server, gateway to the Internet |
| ACS software | 3. Registration and activation device in access control software (refer to ACS)<br>4. Set up device with ACS software<br>a. Configuring access points: one-way or two-way access point, Antipassback mode, time of entering PIN code (or off)<br>b. Setting access direction: № of reader, time of doors opening, signs of "Alarm Prohibited. Door forced open", "Alarm Prohibited. Door opened too long"<br>c. Setting of readers: reader type of 26 or 42 bit<br>d. Setting access control panel input: type of reaction and pass point (e.g. door sensor, pass point A and B, or free pass, pass B)<br>e. Setting access control panel output: type of use (block, siren, etc.), operating mode, pulse duration (if available in this mode), pass point that controls this output.<br>5. By means of access control, the list is created with a set of user RF IDs and their additional parameters, schedules, rules of passage through certain access points (refer ACS)<br>6. After forming and loading the configuration from ACS software the device is ready for use |

# Maintenance

## Factory reset

To return access control panel to the factory settings, perform the following steps:

1. Open enclosure
2. Disconnect access control panel
3. Set jumper FACT
4. Power up
5. Wait for six beeps, signaling the successful panel reset
6. Disconnect panel
7. Remove jumper FACT, close enclosure

## Switching to programming mode

To put access control panel in programming mode do the following:

1. Do not turn off the power.
2. Open enclosure
3. Connect cable to the USB and configure the device using the software "Configurator"

## Replacing the device firmware

1. De-power the panel
2. Remove the top cover of panel
3. Connect the notebook with USB cable to the panel
4. Using special software, do the replacement of panel firmware
5. After downloading the software to the access control panel WAIT for or 40-50 seconds. (If readers are connected wait for 6 short beeps)

> Attention! Downloading hardware will only be allowed within the first 10 seconds after access control panel launch.

## Factory settings
### Communicatior

Ethernet mode enabled, DHCP enabled (no device IP set), no ACS server set

### Inputs

Z1 – Z8 are disabled

### Outputs

Relays 1-4 are disabled

### Readers

Wiegand 42bits

---