Cloud Access Control Controller

U-PROX IP401

Installation and Operation Manual

Rights and Their Protection

Trademarks

About This Document

This manual describes the procedure for installing, connecting, and operating the access control system controller U-PROX IP401 (hereinafter "the controller"). Please study these instructions carefully before installing the controller.

The characteristics and parameters of the controller are described in the **Characteristics** section. The **Terminology** section explains the terms used in this document.

The external appearance of the controller, along with the description of its contacts and operating modes, is presented in the **Description and Operation** section. The installation, connection of external devices, and configuration of the controller are described in the **Controller Operation** section.

Attention!

Before installing and connecting the controller, you must carefully study this manual. Installation and connection are permitted only by persons or organizations authorized by the manufacturer.

Training and Technical Support

Training courses covering the installation and use of the U-PROX IP401 controller are conducted by Limited Liability Company Integrated Technical Vision. For additional information, please contact the personnel of Limited Liability Company Integrated Technical Vision at the phone numbers provided below.

Technical Support:
+38 (091) 481 01 69
support@u-prox.systems
https://t.me/u_prox_support_bot

This support is intended for trained specialists. End users should contact their dealers or installers before reaching out to Limited Liability Company Integrated Technical Vision.

Technical information is available on the website: www.u-prox.systems

Certification

Limited Liability Company Integrated Technical Vision certifies that U-PROX IP401 complies with the Electromagnetic Compatibility Directive 2014/30/EU and the Directive 2011/65/EU (RoHS). The original Declaration of Conformity is available on the website www.u-prox.systems under the "Certificates" section.

Contents

Controller Description

The U-PROX IP401 controller is a device designed for controlling access to residential and industrial premises, as well as for recording passage times and events.

The controller is supplied in a case with a built-in touch button for exit requests and without a power module.

The controller works with readers that connect via the RS232 interface (only U-PROX readers) or via the RS485 interface using the OSDP protocol (U-PROX SE series or other OSDP2.2-compatible readers).

U-PROX IP401 processes the information received from the reader and, using two outputs, switches output devices (e.g., locks, sirens, etc.).

The controller has two fixed-function inputs – a door sensor and an exit request button.

The controller can operate autonomously or as part of a network. To integrate controllers in an access control system, the Wi-Fi interface (a wireless computer network) is used.

The controller supports network configuration via Bluetooth Low Energy (BLE) using the U-PROX Config mobile app.

Firmware updates are performed from a central server via Wi-Fi.

The controller is powered by a 12V source.

U-PROX IP401 controls doors with one reader and an exit request button. Its large non-volatile memory allows the system to manage up to 10,000 identifiers.

Carefully engineered technical and design solutions, communication via Wi-Fi, non-volatile memory and a real-time clock, and protection of reader ports from short circuits, overvoltage, and reverse polarity enable this controller to be used in various access control and management systems.

Purpose of the Device

The Cloud Controller U-PROX IP401 is intended for use as part of access control and management systems of various scales – from small office systems to large enterprises. Controllers are interconnected via a computer network.

Characteristics

Power Supply: External 12V source; current consumption (with loads disconnected) not more than 100 mA; ripple voltage not more than 500 mV.

Reader Connection:

- RS232 – up to 10 m (for U-PROX contactless identifiers)
- RS485 (OSDP2.2) – up to 1000 m

Inputs: 8 inputs for connecting loops with current monitoring (end resistor – 2.2 kΩ).

Built-in Touch Button: for exit requests.

External Signal Inputs: door sensor (DC) and input for the exit request button (RTE).

Tamper Contact: for detecting case opening.

Outputs: one relay (NO/NC, COM) rated at 3 A @ 12V; a transistor open-collector alarm output – 12V, 160 mA.

Wireless Interface: Wi-Fi 2.4 GHz, 802.11b/g/n, supports Open/WPA/WPA2/WEP.

Cloud AC System: U-PROX ACS Cloud.

Local AC System: U-PROX WEB.

Configuration: Full configuration is performed via the access control system using a computer network.

Real-Time Clock.

Non-Volatile Memory:

- Identifiers – 10,000
- Events – 47,000
- Time zones – 250
- Weekly schedules – 250
- Holidays – 250
- Temporary identifiers – 1000

Terminology

Identifiers: In access control systems, each user has a unique code. Identifiers may be in the form of a plastic card, key fob, etc.

Reader: Devices that read identifier codes and connect to the access controller. The Wiegand interface is used.

PIN Code: A code entered via the reader's keypad; it can be a standalone identifier or supplement a card or key fob.

Doors: The access control point (e.g., doors, turnstiles). The access point is the logical unit of the system.

Access Point: See "Doors".

Passage Point: A logical unit in an access control system that manages passage through a door in one direction, including the reader, controller (or part of it), and the output mechanism. Doors with a single passage point are one-sided; with two, they are two-sided.

Exit Request Button: Used for exiting the premises; alternative methods (e.g., an electric lock button or key) trigger a "DOOR BREACH" event.

Door Sensor: An input for connecting sensors (magnetic, rotor, etc.) to monitor door status.

"Door Open Time" Interval: The period during which, after a user passes, the door is not monitored even if the sensor signal is disrupted.

Identifier Pickup Attempt: If an unregistered identifier is presented several times consecutively, the controller enters lockout mode.

Schedules: Time intervals and schedules that define access rights. The controller can store up to 250 time intervals, 250 weekly schedules, and 250 holidays.

Time Zones: Time intervals used for organizing access schedules.

Loading: The transfer of settings from a computer to the controller after programming.

Description and Operation

Controller Construction

The external appearance of the device is shown in Figure 1.

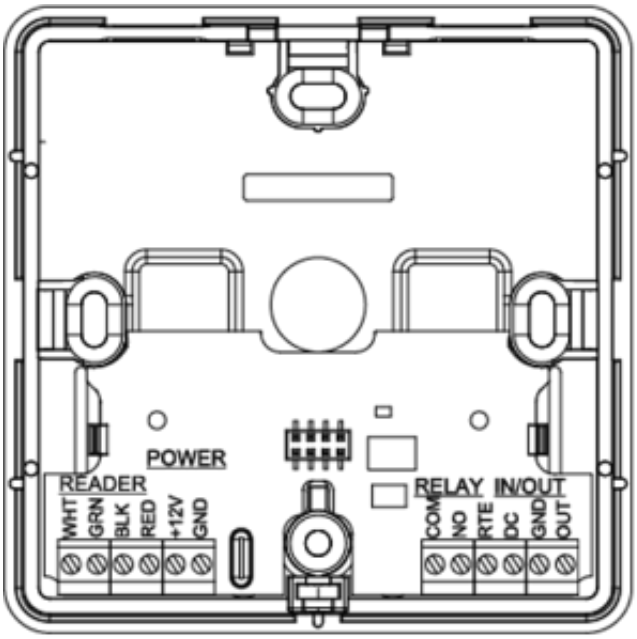
The controller consists of the following components:

- The top part of the device casing
- The touch exit request button
- The bottom part of the device casing
- A mounting screw
- The circuit board with terminal blocks

Figure 1. External appearance of U-PROX IP401

Terminal Block Layout

The layout of the connectors on the bottom board is shown in Figure 2.



Purpose of Controller Contacts

Contact	Name	Purpose
GND	–	Connection of the external power source
+12V	–	–
NO/NC	Relay Contact	Relay contacts
COM	Common	–
RED	+12V, Power	Reader connection
BLK	GND	–
GRN	Data 0	–
WHT	Data 1	–
GND	–	Loop connection
DC	Door Contact	–
RTE	Exit Request Button	–
OUT	Alarm Output	–

Audio-Visual Indication

The access modes are indicated via the reader connected to the controller. The default indications are as follows:

- **Standby Mode:** no sound, red blinking once per second
- **Night Mode or Lockout:** no sound, red-yellow blinking once per second
- **Alarm:** no sound, continuous red
- **Card Registration:** no sound, green blinking once per second
- **Initialization:** no sound, no light indication
- **Data Reading/Loading, Firmware Update:** no sound, continuous red
- **Access Granted:** a short beep, continuously green; 5 seconds before door time expires – a short beep once per second
- **Access Denied:** continuous beep, continuously red

The LED on the touch button indicates only its press.

Controller Operation

Controllers are shipped in the factory default state, in which the red LED blinks once per second.

To operate the controller, it must be configured using the configuration software on a mobile device. Once the settings are loaded, and if the inputs are intact, the controller enters "Standby" mode.

The controller manages a single passage point that can operate in four modes: "Standby", "Alarm", "Lockout", and "Free Passage". The "Free Passage" mode has the highest priority (for example, during a fire), followed by "Lockout", "Alarm", and "Standby".

Standby Mode

The standby mode is the default operating mode of the controller. In this mode, the controller grants or denies access to registered identifiers.

Passage with Identifier Presentation

To pass through a door, the user presents a contactless identifier to the reader. If the identifier is registered and access is currently allowed, the door is opened (the controller activates the output mechanism).

Passage with Identifier and PIN Code

After presenting a registered identifier, the controller checks if a PIN code is required. If

needed, it waits for PIN code entry. Once the correct PIN code is entered, the passage point opens (the output mechanism is activated).

Passage via Exit Request Button (Remote Door Opening)

Exiting through a door with a single-sided passage point or allowing visitor passage is achieved using the exit request button. Pressing and releasing the button opens the passage point (activating the output mechanism).

Access Denied upon Identifier Presentation

Access may be denied for the following reasons:

- The controller is in its factory default (unloaded) state
- The card is not registered in the controller
- The card's validity period has expired
- Access is currently prohibited due to time and/or day of the week
- An identifier registered as lost or blocked is presented
- The controller is in "Alarm" mode
- The controller is in "Lockout" mode
- The temporary card's validity period has not yet begun
- The passage counter for a temporary card (visitor card) has been exhausted

Alarm Mode

The passage point enters "Alarm" mode when unauthorized access occurs (e.g., door breach), when the controller case is opened, when an identifier registered as lost is presented, or when the door remains open too long (exceeding the door open time) and if the identifier pickup function is enabled.

In "Alarm" mode, the controller activates outputs designated for ALARM or SIREN. The alarm output remains active until the alarm is cleared, and the siren output is timed.

If the passage point is in "Alarm" mode, passage is blocked. Doors can be opened by pressing the exit request button.

The "Alarm" mode can be disabled by presenting an identifier with the "Alarm Clear" attribute or by issuing a command from a computer.

Free Passage Mode

In some situations, such as during a fire, earthquake, or other emergency, it may be necessary to open the door for free passage. In such cases, the controller supports "Free Passage" mode.

The passage point enters "Free Passage" mode by a command from an operator on a computer.

While in "Free Passage" mode, the lock remains open, and the controller logs all presented identifiers and code entries as "Access Granted" regardless of the schedule. This mode is used to monitor the presence of personnel during emergencies.

To ensure proper operation in "Free Passage" mode when using mechanically actuated locking devices, it is essential to monitor the door sensor. Mechanical locks are released with a current pulse and remain open until the door is closed. When the door is closed, the lock re-engages. The controller in "Free Passage" mode checks the door contact and sends an unlock pulse after each door closure.

If the controller is used without a door contact (e.g., a microswitch), using an "impulse" output type for unlocking is not recommended. In such cases, "Free Passage" mode will not function correctly – the door cannot be opened without presenting an identifier.

Lockout Mode

The controller enters "Lockout" mode when a situation arises that requires all users to be denied access. In this mode, passage is allowed only for identifiers with the "Security Service" attribute. Doors cannot be opened by pressing the exit request button.

The passage point enters "Lockout" mode by a command from a computer operator.

Properties of Identifiers (Cards)

Code (Electronic Card Code)

Each card has its unique code assigned during manufacturing.

PIN Code

A supplementary code for the card. It must consist solely of six decimal digits. It may be used with readers that have an integrated keypad.

After the card is presented to the reader, the integrated keypad is used to enter the PIN code by pressing the “#” button. If the correct PIN code is entered, the controller unlocks the door and grants access. Otherwise, a warning signal is issued, an "Incorrect PIN Code" event is logged, and the door remains locked.

Validity

The expiration date of the card’s validity.

Alarm Clear

When a card with the alarm clear attribute is presented to the reader of a door in alarm state, the controller logs an event "Alarm Cleared" and resets the door to standby mode. If a card without the right to clear the alarm is presented, the door remains in its current state and an event "Access Denied. Alarm State" is logged.

Security Service

This attribute grants the right to pass through locked doors. If a door is in "Lockout" mode, presenting a regular card will result in an "Access Denied. Lockout State" event. However, when a card with the "Security Service" attribute is presented, the controller grants access and logs an "Access Granted. Lockout State" event.

VIP

This attribute allows unconditional access (except when the door is in lockout mode). A VIP card may have any schedule assigned; anti-duplication and validity limitations do not apply. It may also have a PIN code.

If a door is in "Lockout" mode, an identifier with the VIP attribute will not be granted access.

Anti-Duplication Disabled

This means that access is granted regardless of previous passage direction, but still subject to the assigned schedule and other card attributes.

Usage Options and Operating Modes of Outputs

The relay output of the controller can be programmed as a **lock** (with an optional inversion setting). The OUT output can be programmed as a **siren or alarm**. In addition, each output is assigned an operating mode: **start-stop** (the output remains active while the condition persists, e.g., while in "Alarm" mode), **impulse** (the output is active for a set duration), **trigger** (the output toggles on the first event and off on the next, etc.), or **continuous** (the output is activated or deactivated by individual commands).

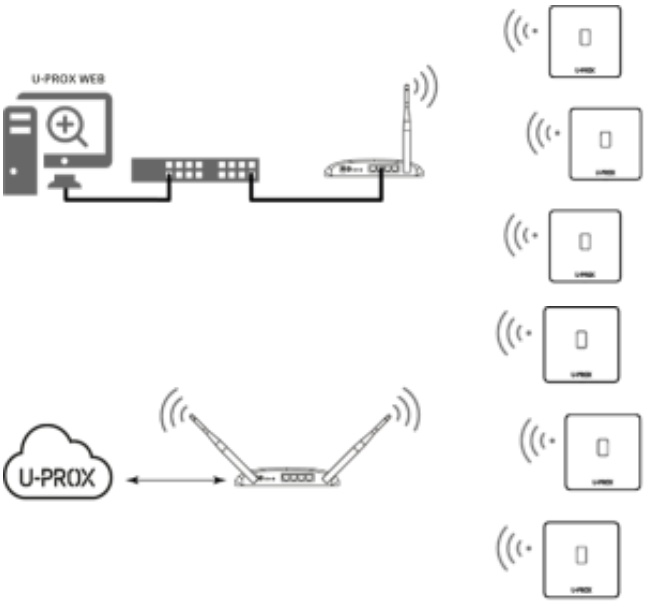
Communicator Operation

The U-PROX IP401 controller operates automatically. Once data is loaded from the server, the controller processes the access rules for presented cards and sends event notifications to the access control system server.

The controller's communicator operates in notification mode, meaning that when an event (e.g., passage, zone breach) occurs, data is transmitted to the AC server.

When connected to a computer network, the controller ensures protection against unauthorized access by encrypting data packets with a 256-bit key and verifying the device's unique serial number, as well as monitoring the communication channel through periodic test signals.

The U-PROX IP401 can be connected to a computer network via a wireless connection (Wi-Fi). It supports operation within a local network (see Figure 3) as well as over the Internet (see Figure 4), allowing for the construction of distributed access control systems of any scale.



Local Network Operation Algorithm

1. After the controller is powered on, it connects to the pre-configured Wi-Fi and obtains an IP address dynamically;
2. It periodically updates the IP address status (maintaining the reserved IP address);
3. It checks the availability of the AC server (by IP or DNS name);
4. It sends periodic test signals;
5. It transmits event notifications;
6. It waits for commands.

Internet (Wired Local Network) Operation Algorithm

1. After the controller is powered on, it connects to the pre-configured Wi-Fi and obtains an IP address dynamically;
2. It periodically updates the IP address status (maintaining the reserved IP address);
3. It checks for Internet connectivity (availability of the router's IP address);
4. It checks the availability of the AC server (by IP or DNS name);
5. It sends periodic test signals;

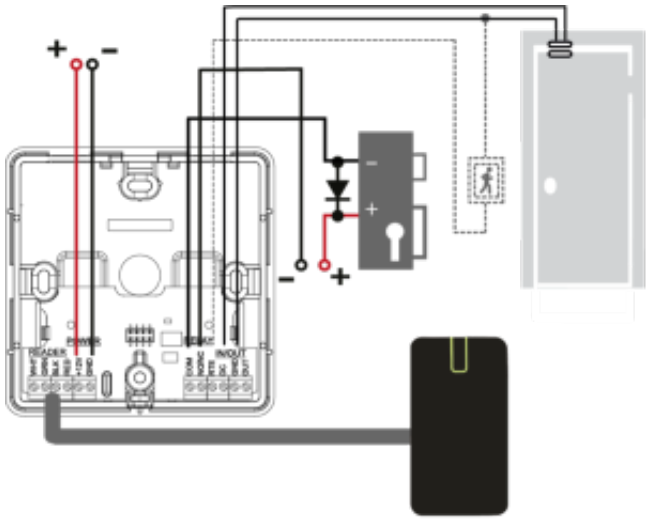
6. It transmits event notifications;
7. It waits for commands.

Device Operation Procedure

The controller is housed in a small plastic case with a glass surface.

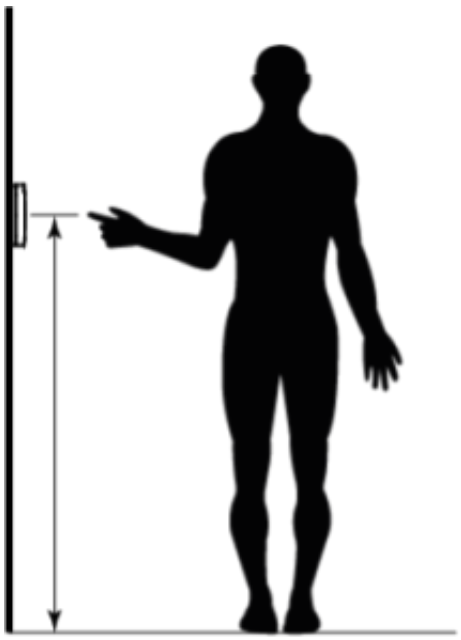
Connection Procedure

1. At the installation site, mark and drill the necessary holes:
    1. Screw in the mounting screw on the bottom of the controller;
    2. Remove the top cover;
    3. Using the back plate of the controller as a template, mark and drill two holes with a 5 mm diameter and a depth of 30 mm.
2. Run the cable from the power supply unit;
3. Run the cable from the output device (e.g., lock);
4. Install the reader and run its cable;
5. Run the cables from the sensors/buttons;
6. Connect the wires from the power supply, lock, reader, and controller inputs according to the sections below (using a junction box is recommended);
7. Lay the installation cables in the wall;
8. Install and secure the back plate of the controller, connect the communication cable connector, attach the top cover, and fasten with a screw;
9. Using the mobile app, configure the network parameters of the controller;
10. The device is ready for operation.



Installation Recommendations

It is recommended to mount the controller on the wall near the door so that all users can easily press the exit request button.



Power and other cables should not run closer than 0.1 m from the device's casing.

Reader Connection

The controller works with a reader that connects via the RS232 interface (only U-PROX readers) or via the RS485 interface using the OSDP protocol (U-PROX SE series or other OSDP2.2-compatible readers).

The reader connection type is configured via the U-PROX Config mobile app.

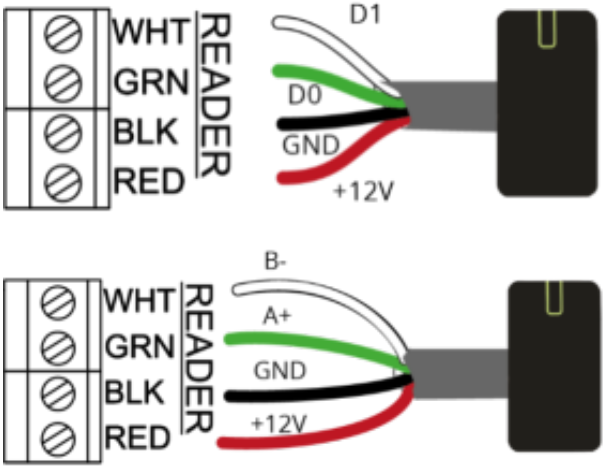
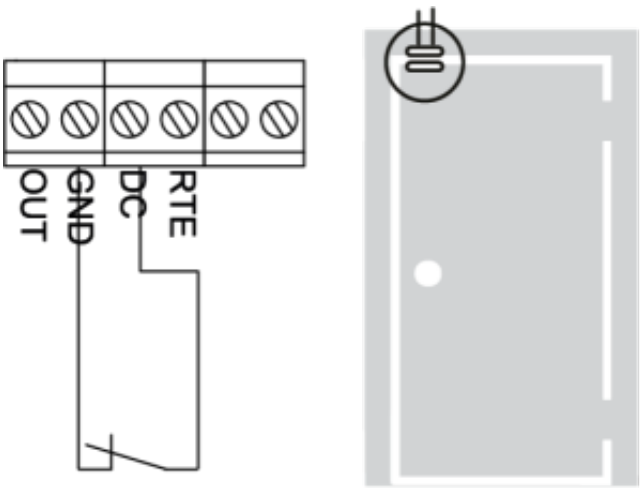


Figure 7. Connection of a U-PROX SE series reader via OSDP

The current consumption of each external reader connected to the "+12V" terminals should not exceed 100 mA. For long-distance readers with consumption above 100 mA, the power should be supplied from a separate source.

Door Sensor

The controller uses a door contact to determine whether the door is open or closed. If the door contact is absent, the controller cannot detect unauthorized access or situations where the door remains open too long (e.g., when several people pass through the same entry point).

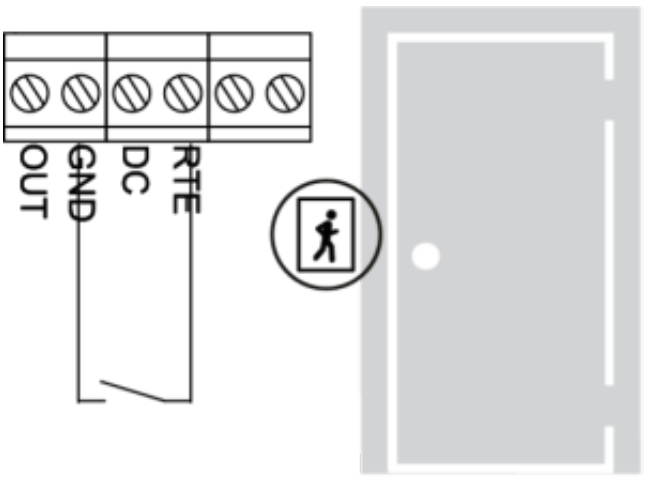


Doors in an access control system are recommended to be equipped with a door closer.

Exit Request Button

Doors are opened by pressing and releasing the exit request button.

Additionally, the exit request button can be used for remote door opening (e.g., by a receptionist or security guard).



Using the button on an electric lock for door opening will trigger a DOOR BREACH event.

Output Devices (Relays)

The controller features one solid-state relay to control output devices such as an electric lock or latch.

The relay has normally closed (NC) and normally open (NO) contacts and can handle devices consuming up to 1 A at 30 V.

Voltage drops or surges when all outputs are switched on or off simultaneously should not cause the controller to malfunction. Otherwise, a separate power source should be used for the outputs.

Electric Locks

The ability to program both standard and inverse operating modes, as well as to set the activation time for the lock over a wide range (from 1 to 255 seconds), allows the controller to operate nearly any type of electric lock or latch.

A special case is when the time is set to 0. In this case, a 200 ms pulse is sent to the relay.

Figure 10 shows an example of connecting output devices: the first is activated by applying voltage (NO), and the second by cutting the circuit (NC).

When using relay contacts to control an inductive load (for example, an electromagnetic lock), high-amplitude voltage pulses may occur. To prevent damage to the relay contacts, a flyback diode should be installed across the inductive load in reverse polarity.

Note that inexpensive electromagnetic locks do not tolerate prolonged voltage application. For these devices, the relay activation time should be programmed to prevent coil overheating.

Alarm Output

The controller’s alarm output is a transistor open-collector output. When activated, the OUT contact is connected to GND.

The alarm output can be used to connect to an external alarm system or output device with a current consumption not exceeding 60 mA.

If a door contact (normally closed) is connected, the alarm output will activate when the door contact is interrupted, except during the designated "door open" interval. The alarm output is activated for a programmed duration, from 0 to 254 seconds.

<p style="font-weight: