Global Anti-passback Controller U-PROX IC A

Installation and Operation Manual

Rights and Their Protection

Trademarks

About This Document

This Operating Manual describes the procedure for installing, connecting, and operating the U-PROX IC A access control system command controller (hereinafter referred to as "the controller"). Before mounting the controller, read this manual carefully.

The controller's specifications and parameters are described in the **Specifications** section. The **Terms** section explains the terminology used throughout this document.

The appearance of the controller, as well as a description of its contacts and operating modes, is provided in the **Description and Operation** section. The installation and configuration procedure is described in the **Operating Procedure with the Device** section.

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

Training and Technical Support

Training courses covering installation and use of the U-PROX IC A controller are conducted by Limited Liability Company Integrated Technical Vision. For more information, contact the company at:

Phone: +38 (091) 481-01-69

E-mail: support@u-prox.systems

Technical support for all U-PROX products is provided during business hours. Note that this support is intended for trained professionals; end users should contact their dealers or installers before reaching out directly.

Technical information is available at: www.u-prox.systems

Certification

Limited Liability Company Integrated Technical Vision declares that the U-PROX IC A controller complies with the Electromagnetic Compatibility Directive 2014/30/EU and the RoHS Directive 2011/65/EU. The original Declaration of Conformity is available on the website under the Certificates section.

Contents

Controller Description

The U-PROX IC A controller is a device designed for organizing global anti-passback and controlling access to residential and industrial premises. It also performs the function of emergency door unlocking. The U-PROX IP400 controllers, which serve as the access control devices, work in conjunction with this controller.

U-PROX IC A receives information from the U-PROX IP400 controllers via an Ethernet (wired computer network) interface.

The controller includes a function for programming network settings and updating its firmware via a standard USB port (micro USB B).

It is equipped with advanced hardware and intelligent functions that support operation with up to 255 devices and up to 64 anti-passback zones.

Purpose of the Device

The U-PROX IC A controller is intended for use in access control and management systems (ACS) of various scales—from small office systems to the entry systems of large enterprises. In an ACS, controllers are networked together via a computer network.

Specifications

Power Supply: External 12V source
Current Consumption: Not more than 150 mA at 12V
DC Ripple: Not more than 500 mV
Communication with U-PROX IP400 Controllers: Via Ethernet with galvanic isolation
USB Port: One micro USB B port for network configuration and firmware updates
Configuration: Full configuration is performed via ACS software over the computer network; auto-configuration is available in a peer-to-peer network
Real-time Clock
Non-volatile Memory: Supports 32,000 identifiers and 47,000 events
Device Capacity: Up to 255 devices and 64 anti-passback zones

Terms

Identifiers: In access control systems, each user has an identifier with a unique code.

Identifiers may take the form of plastic cards, key fobs, etc.

Reader: Devices designed to read identifier codes, which are connected to the ACS controllers.

PIN Code: For readers with an integrated keypad, the PIN code may serve as an identifier or as an adjunct to a card or key fob. After presenting the card, the reader "waits" for the PIN code to be entered.

Door: The access point where control is directly performed (e.g., door, turnstile, or portal equipped with necessary control devices).

Access Point: See Door.

Loading: After the controller parameters are programmed, the configuration must be loaded (transferred from the computer to the controller).

Anti-passback: A function to prevent a situation where a user passes through a controlled door and then transfers their identifier to another person. When enabled, the controller tracks the location of the identifier (inside/outside) and denies access if a repeat passage is attempted in the same direction.

Global Anti-passback: The tracking of an identifier's movement across all controlled access points. In a global anti-passback system, the object is divided into access zones; entering a new zone is considered an exit from the previous one. If a repeat passage is attempted, the system denies access and issues a "Global Anti-passback: Access Denied" message.

Description and Operation

Controller Construction

(Images and figures omitted for brevity)

Function of Contacts, Jumpers, and Buttons

Name	Function
+12V	Connection for external power supply
GND	Ground
USB Port (micro B)	Used for initial network configuration and firmware updates
Jumper BAT	Enables the backup battery for clock and memory support
FUNC Button	Service button for resetting to factory settings

Audio-visual Indication of the Controller

The controller's indicator LEDs (displayed from left to right) are as follows:

- **Link LED:** Lit when the Ethernet cable is functioning.
- **Act LED:** Blinks rapidly when data exchange is in progress.
- **LED (bi-color):**
    - **Normal mode:** Red – two short pulses per second indicate no connection to the ACS server; Green – one short pulse per second indicates normal connection.
    - **Loading mode:** Rapid red blinking indicates the device is booting up.

Controller Operation

Controllers are shipped in an un-loaded (factory default) state. In this state, the bi-color LED blinks red twice per second. To operate the controller in an ACS, network settings must be loaded using the "Configurator" software or by using the auto-configuration mode.

After loading, the controller enters "Normal" mode.

The controller can be reset to an un-loaded state either via a command from a computer or by following the procedure described in the **Service and Maintenance** section.

Communicator Operation

The U-PROX IC A controller operates in automatic mode. After loading its configuration from the server, it processes data from authorized U-PROX IP400 controllers participating in global anti-passback, handles access event notifications for presented identifiers, and sends these notifications to the ACS server.

The communicator works in notification mode – whenever an event (such as an access or zone violation) occurs, data is transmitted to the ACS server.

The U-PROX IC A controller can be connected to a computer network via a wired Ethernet connection, supporting both local network operation and Internet connectivity.

Global Anti-passback

The basis of global anti-passback is zone-based anti-passback. The object is divided into rooms – access zones. In such a configuration, entering a new zone is considered exiting the previous one, and access to a zone may be possible via different doors.

The anti-passback controller tracks employee movements from zone to zone by receiving data

from access controllers. Initially, an employee's status is set to "Undefined" until the first presentation of an identifier to a reader, at which point the location is recorded. The "Undefined" status is assigned during new employee registration or after a "General Location Reset" command.

Using global anti-passback prevents repeated passages, duplication of cards, unauthorized entry, or sharing of identifiers. (See Figure 4 for an illustration of access zone distribution.)

In cases of lost connection with the ACS controller, forced door entry, or if a door switches to free passage mode, the anti-passback system merges the zones, assuming personnel may be present in both. Once the door or connection is restored, the zones separate again, with the actual location determined by subsequent identifier presentations (see Figure 5).

If communication with the U-PROX IC A controller is lost, U-PROX IP400 access controllers can be configured to either block all access or grant access according to locally stored personnel location data (local anti-passback).

Requirements for Configuring the U-PROX IC A Controller: The controller must have a static (fixed) IP address.

Requirements for Configuring U-PROX IP400 Controllers:

- Only controllers with double-sided doors (entry and exit by identifier presentation) participate in global anti-passback.
- The first ACS server address in the device's communication settings must be the IP address of the computer running the U-PROX IP server software.
- The second ACS server address must be that of the U-PROX IC A controller.
- The U-PROX IP software must have the "General" anti-passback mode enabled for doors.
- The access controller must be configured with the master anti-passback controller and the corresponding reaction for connection loss.

U-PROX IP400 controllers send access event notifications to two addresses simultaneously. The first address is the ACS server (for display and storage in the database), and the second is the U-PROX IC A controller, which sends a command to either deny or grant access.

After presenting an identifier, the delay in granting or denying access may be up to 1 second, depending on network topology and bandwidth.

System Deployment

Using the existing network infrastructure and standard protocols (e.g., DHCP) allows the "plug-and-play" principle to be implemented. The auto-configuration mode for the ACS server

address in devices greatly simplifies ACS deployment.

System Deployment Procedure: (See Figure 7)

The auto-configuration algorithm for U-PROX IC A is as follows:

1. Upon power-up, the controller checks whether DHCP is enabled (device IP is 0.0.0.0) or if it has obtained a static IP address.
2. If DHCP is enabled, the dynamic IP address assignment procedure is initiated.
3. If the ACS server address (IP or DNS name) is not set, the controller enters auto-configuration mode:
    - The device broadcasts data packets announcing itself as a new device on the local network.
    - Although this broadcast is limited to the peer-to-peer local network and active networking equipment, in networks with complex topology the ACS server IP must be set manually.
    - Upon receiving a packet from a new device, the system operator is alerted and must add the device to the database.
    - Once added, the device receives a response from the ACS server. The server address is stored in the controller's settings and the broadcast stops.
    - If the server address changes, the device will auto-configure again; however, communication will only be possible with the ACS to which it is bound.
4. To unbind the controller from the ACS, reset it to factory settings.

Operating Procedure with the Device

The controller is supplied in a plastic housing. The overall dimensions are shown in Figure 8.

Connection Procedure:

- Run the Ethernet cable.
- Connect the power supply cable (if necessary).
- Route the mounting cables within the wall.
- Mount and secure the controller housing.
- Register the controller in the ACS using the provided instructions.
- Load the full configuration via the ACS software.

After these steps, the device is ready for operation.

Installation Recommendations

The controller should be installed in an accessible location for maintenance.

To install the controller on a wall (see Figure 9):

1. Open the housing cover, remove the board, align the housing to the intended mounting location, and mark the drill holes.
2. Run cables through the holes in the housing wall.
3. Secure the controller housing to the wall.
4. Connect all necessary cables.

Communication

For communication with the ACS server, the U-PROX IC A controller can use a wired computer network. The device can be configured either via auto-configuration or manually from a PC using the "Configurator" software.

When properly configured, the following is ensured:

- Assignment of a static or dynamic (DHCP) IP address to the device;
- Operation with the ACS server using an IP or DNS address;
- Internet connectivity with support for redundant routes via a secondary router.

The communicator operates in notification mode – upon occurrence of an event (access or zone violation), data is transmitted to the ACS server.

Additionally, the controller protects against unauthorized access through robust encryption (crypto-resistance and imitation resistance) and periodic test signals for channel monitoring.

Wired Computer Network (Ethernet)

The Ethernet interface is used to network system components and, when using PoE technology, to supply power. Ethernet cables without additional equipment can be run up to 100 meters, with data speeds up to 100 Mbps.

Figure 10. Ethernet Cable Connection Examples

The following examples show direct crimping for connection to a switch or router, and crossover wiring for connection to a computer:

Direct Crimping:

1. White-yellow – white-yellow
2. Yellow – yellow
3. White-green – white-green
4. Blue – blue
5. White-blue – white-blue

6. Green – green
7. White-brown – white-brown
8. Brown – brown

Crossover Wiring:

1. White-yellow – white-green
2. Yellow – green
3. White-green – white-yellow
4. Blue – blue
5. White-blue – white-blue
6. Green – yellow
7. White-brown – white-brown
8. Brown – brown

During Ethernet configuration, set the following parameters:

- Device IP address (if not using DHCP)
- Subnet mask
- Gateway IP address
- DNS server IP addresses (if domain name resolution is used)
- Communication parameters with the ACS server (IP or DNS address, read/write ports, test signal frequency)

Controller Programming Procedure

Software: Use the "Configurator" software via the USB port to program the device.

Procedure:

1. Determine the configuration mode: auto-configuration or manual.
2. If manual configuration is chosen, enter the initial network parameters:
    - ACS server settings (IP or DNS name, read and write ports)
    - If using DHCP, some steps may be skipped.
    - Device settings (IP address, subnet mask, DNS, gateway, etc.)
3. Connect and register the device in the ACS software as per its manual.
4. After loading the configuration, the device is ready for operation.

Service and Maintenance

Factory Reset

To reset the controller to factory settings, perform the following steps:

1. Disconnect the power supply.
2. Press and hold the FUNC button.
3. Reconnect the power supply.
4. Wait 10 seconds until the LED lights red, then release the FUNC button.
5. The LED will flash red 6 times to indicate that the reset process is complete.

Switching to Programming Mode

To enter programming mode, simply connect the controller to a computer using the USB cable. Then configure the device using the "Configurator" software.

Firmware Update

1. Connect the USB cable first to the computer, then to the controller.
2. Using the designated firmware update software, perform the update.
3. After the firmware is loaded into the controller, wait 25–30 seconds before disconnecting; then the controller is ready for operation.

Factory Settings

Default factory settings include:

- DHCP enabled (no static IP set for the controller)
- No ACS server address specified (auto-configuration is enabled)

Maintenance and Repair

Warranty and post-warranty service for U-PROX IC A controllers is provided only by persons or organizations authorized by the manufacturer.

Warranty Obligations

The manufacturer guarantees that the U-PROX IC A controller meets the parameters described in this manual, provided that the storage and operating conditions are as specified.

Storage Warranty: 6 months from the date of manufacture.

Operational Warranty: 12 months from the date the device is put into service.

Device supply, staff training, installation, commissioning, and warranty service for the U-PROX IC A controller are performed by the manufacturer or by organizations authorized by the manufacturer.

If a defect attributable to the manufacturer is detected, authorized organizations will remedy the issue within 10 days of notification.

If commissioning is carried out by an organization not authorized by the manufacturer, the consumer forfeits warranty service.

Warranty repairs will not be performed if the device fails due to improper connection, non-compliance with this manual, mechanical damage, or force majeure.

The manufacturer reserves the right to make design changes that do not affect the main technical characteristics or reliability of the product.