

LumiRing ICON-Pro Access Control Devices Instruction Manual

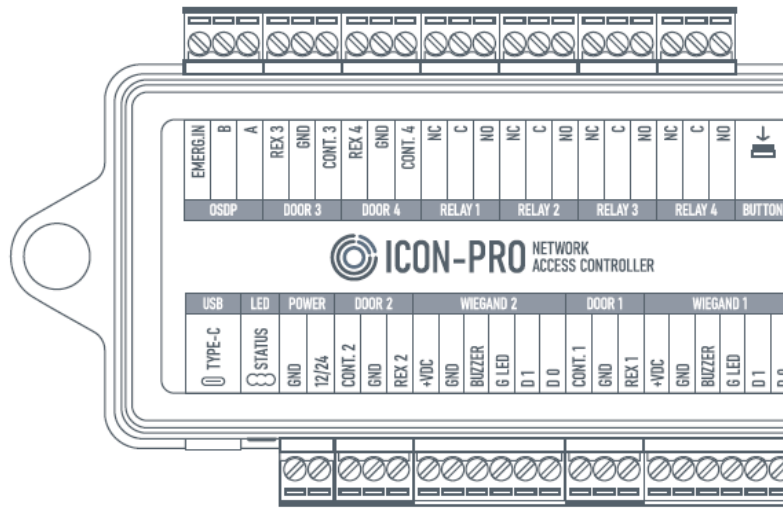
[Home](#) » [LUMIRING](#) » LumiRing ICON-Pro Access Control Devices Instruction Manual 

Contents

- 1 LumiRing ICON-Pro Access Control Devices
- 2 Product Information
- 3 Device Specifications
- 4 Default Device Settings
- 5 Device Dimension
- 6 Device Connection Terminals
- 7 Installation Recommendations
- 8 Connection Diagram
- 9 Login
- 10 Quick Start
- 11 System
- 12 Network
- 13 Open Supervised Device Protocol (OSDP)
- 14 Maintenance
- 15 Hardware Reset
- 16 Glossary
- 17 Documents / Resources
 - 17.1 References
- 18 Related Posts



LumiRing ICON-Pro Access Control Devices



Device Specifications

- Default Device Settings: ICON-Pro
- Device Dimensions: 3.15" x 5.31" x 5.9"
- Device Connection Terminals: USB Service Port Type-C, LED Indication, Door IN Contact, Request to Exit, Wiegand IN, Buzzer LED, RJ-45 Ethernet Port, Emergency IN, RS-485, Relay NC/C/NO

Product Information

The ICON-Pro Controller is a versatile device designed for access control systems. It offers various connection terminals and features to enhance security and convenience in commercial or residential settings.

Installation Recommendations

When installing the ICON-Pro Controller, ensure to use diodes like SR5100 or varistors such as 5D330K for protection against electrical surges. Follow the connection diagram provided in the manual for proper installation.

Connection Instructions

Placement and Wiring

Find a suitable location to mount the controller where it can be easily accessed for wiring purposes. Ensure all wiring connections are secure and follow the specified wiring diagram for proper functionality.

Connecting Power to the Device

Connect the power source to the designated power input terminals on the controller. Make sure to observe polarity and voltage requirements to prevent damage to the device.

Wiegand Connection

For Wiegand connections, follow the provided connection diagram to connect readers to the controller. Ensure correct wiring of data lines and power supply to enable communication between devices.

Connecting Open Supervised Device Protocol (OSDP)

For OSDP connections, refer to the appropriate diagram provided in the manual. Follow the warnings and instructions to ensure proper grounding and voltage levels for reliable operation.

Connecting Electric Locks

If using electric locks with the controller, connect them to the designated terminals following the recommended

wiring configuration. Test the functionality of the locks after installation.

Protection Against High Current Surges

Install diodes and varistors as recommended in the manual to protect the controller from high current surges that may occur in the system.

Frequently Asked Questions (FAQ)

- **Where can I find additional documentation for the ICON-Pro Controller?**

You can find the latest version of the manual and additional documentation on our website or by contacting customer support.

- **How do I troubleshoot common problems with the ICON-Pro Controller?**

Refer to the troubleshooting section of the manual for guidance on resolving common issues. If you need further assistance, you can reach out to our support team via email.

- **What should I do if I encounter an error while using the product?**

If you encounter any errors or have questions regarding the product, please contact us via email at <https://support.lumiring.com> for assistance.

Did you find an error or have a question? Please email us at <https://support.lumiring.com>.

Introduction

This document provides detailed information on the ICON-Pro Controller device structure and steps for installing and connecting it. It also includes instructions for preventing or troubleshooting many common problems. This guide is for informational purposes only, and the actual product takes precedence in case of any discrepancies. All instructions, software, and functionality are subject to change without prior notice. The latest version of the manual and additional documentation can be found on our website or by contacting customer support. The user or installer is responsible for complying with local laws and privacy regulations when collecting personal data while using the product.

Device Specifications

Voltage:

- 12 or 24 VDC operation
- The power supply determines the voltage at the outputs.
- 0.15A @12 VDC, 0.075A @ 24 VDC current consumption
- POE 802.3af (15.4W)
- Total output current when powered by POE 0.6 A @ 11.5 VDC

ATTENTION:

The Readers power is pass-through. If the device is powered with 24V, the readers will receive the same power.

Outputs:

- Four (4) dry form "C" 1.5A rated relay outputs. Inputs:
- Nine (9) inputs (dry contact type) from 0 to 5 volts

Communication interfaces:

- Wi-Fi 802.11 b/g/n 2.4 GHz
- Power over Ethernet (10/100 Mbit) IEEE802.3/802.3af
- Wiegand 4, 8, 26, 32, 33, 34, 35, 36, 37, 40, 42, 48, 56 bit
- OSDP via RS-485
- USB ports (Type-C) for firmware update

Memory storage:

- 100,000 cards
- 250,000 events

Dimensions (L x W x H):

- 5.9" x 3.15" x 1.38" (150 x 80 x 35 mm)

Mounting method:

- Wall mount/Din rail mount (option)

Weight:

- 6.75 oz (191 g)

Temperature:

- Operation: 32°F ~ 120°F (0°C ~ 49°C)
- Storage: -22°F ~ 158°F (-30°C ~ 70°C)

Relative humidity

- 5-85 % RH without condensation

Default Device Settings**Wi-Fi device name when searching:**

- ICON-Pro_(serial_number)

Access point (AP) Wi-Fi IP address of the device:

- 192.168.4.1

Ethernet IP address of the device:

- DHCP

Wi-Fi password:

- None (factory default)

Web page login:

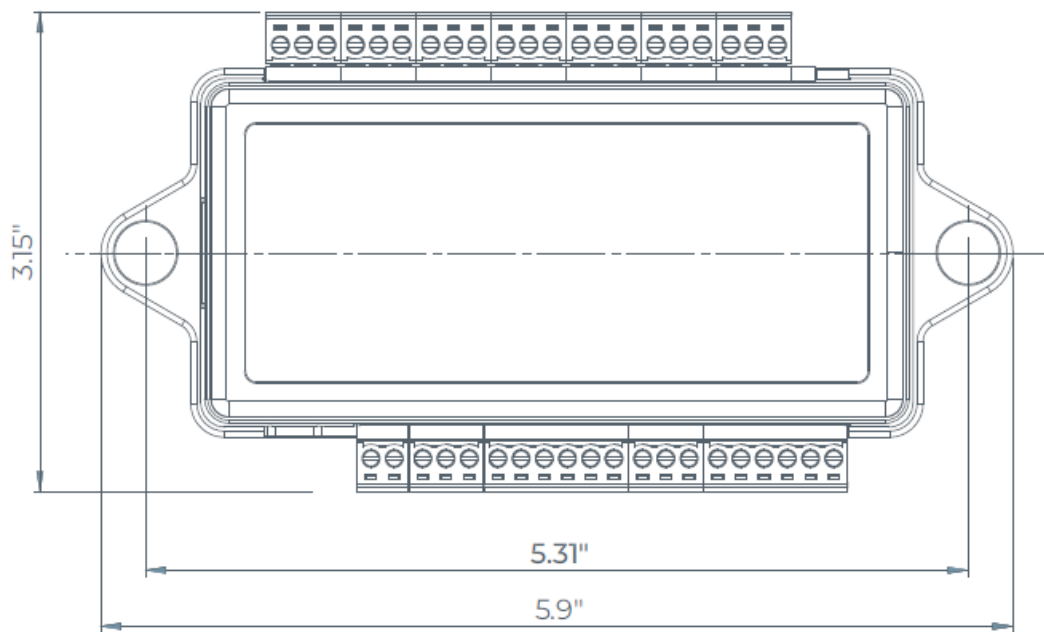
- admin

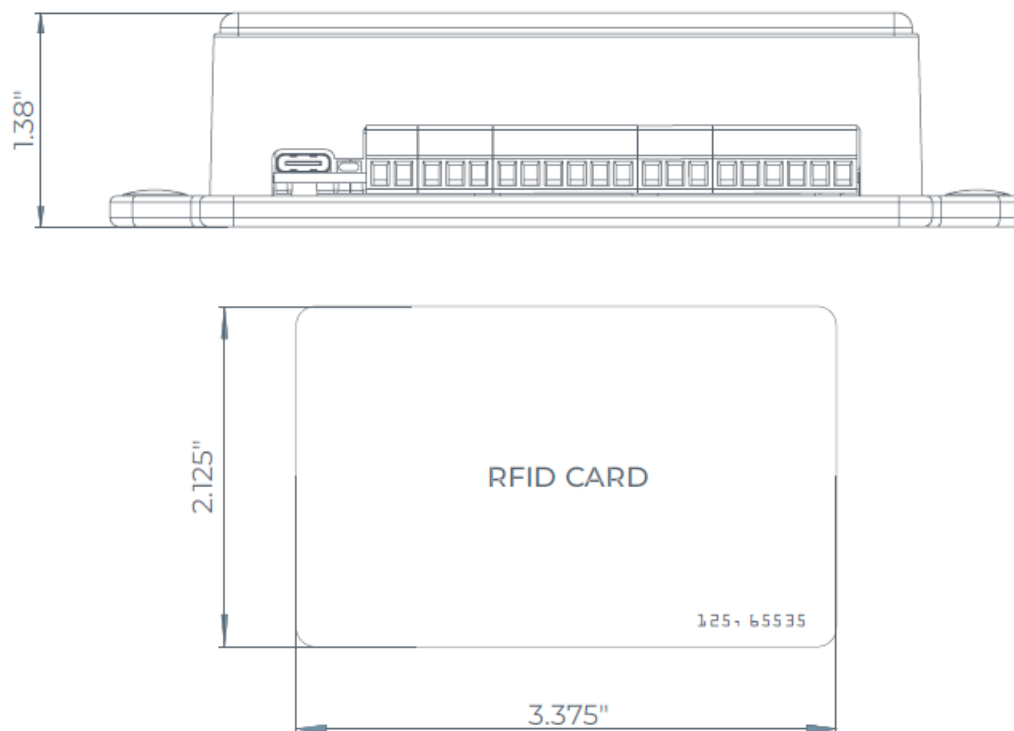
Web page password:

- admin123

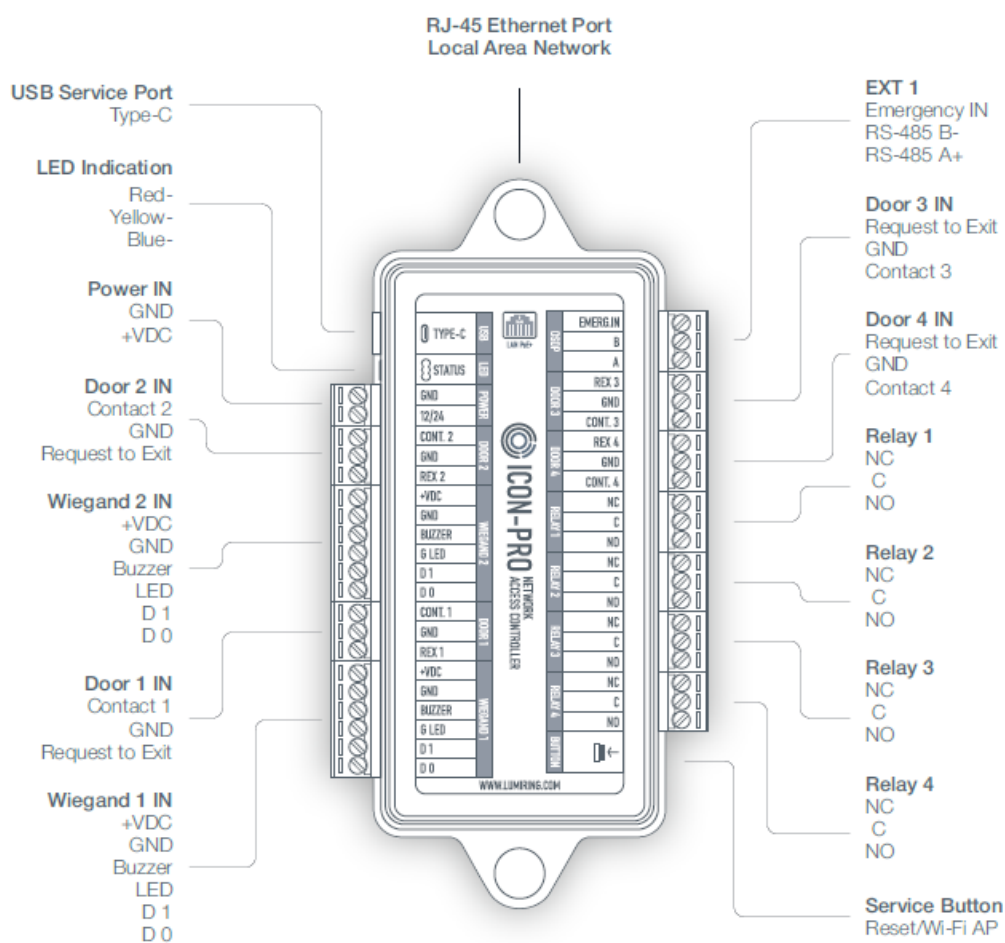
AP Wi-Fi timer:

- 30 minutes

Device Dimension



Device Connection Terminals



Installation Recommendations

Placement and Wiring

- Connecting the Controller via Wi-Fi should be considered an alternative without an Ethernet connection, but not

as the primary method.

- It is recommended that an Ethernet connection be used as the primary method. If a Wi-Fi connection is chosen, the controllers should be placed as close as possible to the access points to minimize communication delays.
 - After installation, it's crucial to check the Wi-Fi signal strength. Ensure the minimum allowable signal level is – 55 dB.
 - If the signal strength is lower, consider moving the AP closer to the device or using a more robust antenna on the AP or device.
 - Remember, avoiding metal surfaces is vital as they can reduce the quality of the Wi-Fi connections.
- Connecting Power to the Device**
- A power cable with a suitable cross-section is used to supply the current consumption of the connected devices. Make sure to use two separate power supplies for the device and the actuators.

Wiegand Connection

- Connect the readers using the same Wiegand format and byte order to avoid differences in card code reading and subsequent confusion in the system.
- The Wiegand communication line length should be at most 328 ft (100 m). If the communication line is longer than 16.4 ft (5 m), use a UTP Cat5e cable. The line must be at least 1.64 feet (0.5 m) away from power cables.
- Keep the reader power line wires as short as possible to avoid a significant voltage drop across them. After laying the cables, ensure the power supply voltage to the reader is at least 12 VDC when the locks are on.

Connecting Open Supervised Device Protocol (OSDP)

- The OSDP uses an RS-485 interface that is designed for long-distance communications. It operates at up to 3,280 ft (1,000 m) with good resistance to noise interference.
- The OSDP communication line should be far from power cables and electric lights. A one-twisted pair, shielded cable, 120 impedance, 24 AWG should be used as the OSDP communication line (if possible, ground the shield at one end).

Connecting Electric Locks

- Connect devices via relays if galvanic isolation from the device is needed or if you need to control highvoltage devices or devices with significant current consumption.
- To ensure reliable system operations, it is best to use one power source for the controllers and a separate one for the actuators.

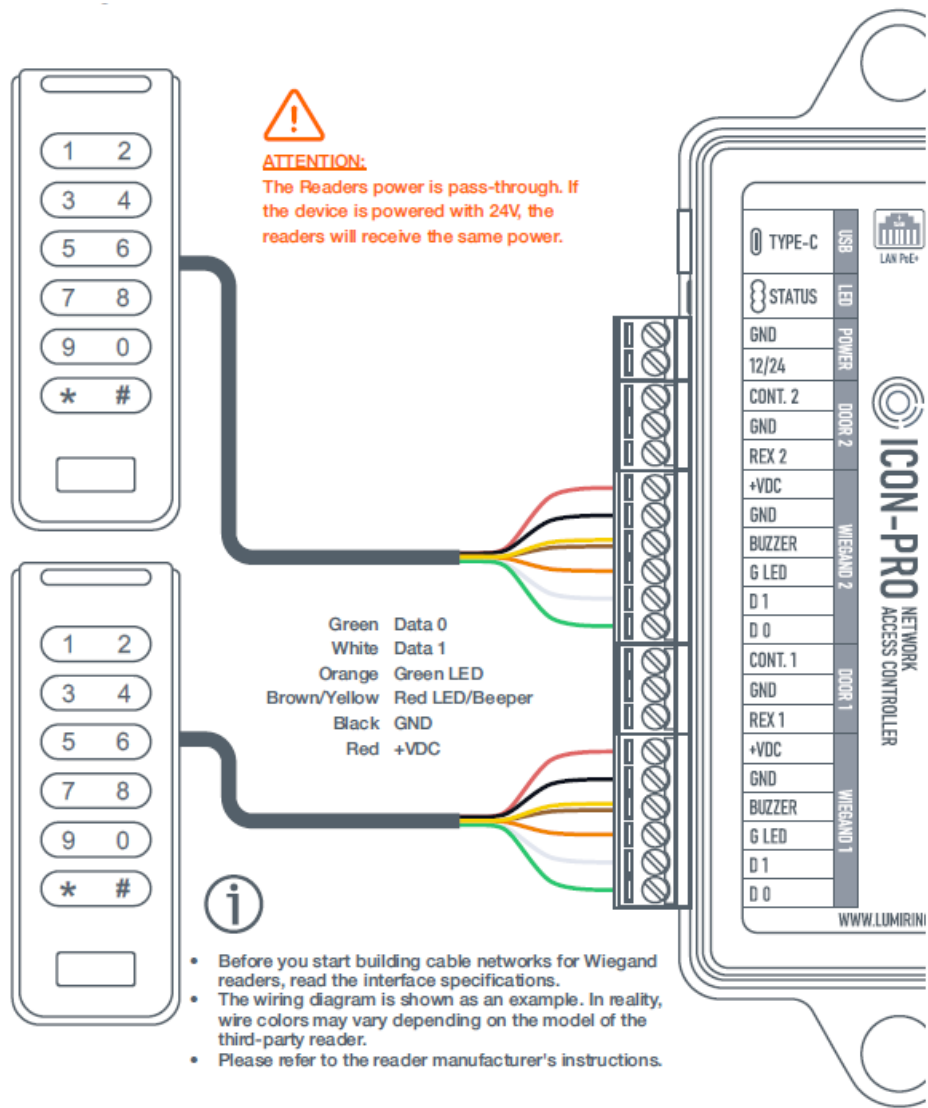
Protection Against High Current Surges

- A protective diode protects the devices from reverse currents when triggering an electromagnetic or electromechanical lock. A protective diode or varistor is installed near the lock parallel to the contacts.
- THE DIODE IS CONNECTED IN REVERSE POLARITY.

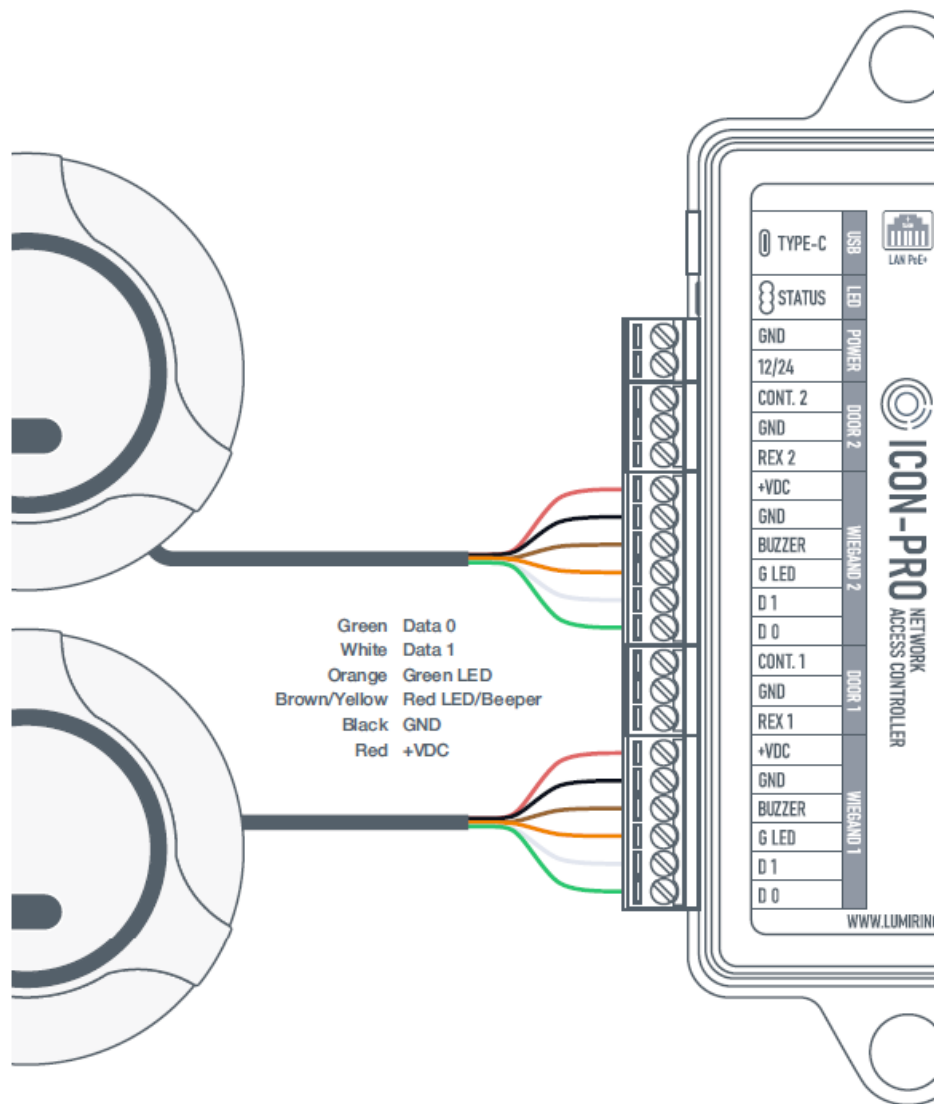
Diodes: (Connect in reverse polarity)	SR5100, SF18, SF56, HER307, and similar.
Varistors: (No polarity required)	5D330K, 7D330K, 10D470K, 10D390K, and similar.

Connection Diagram

Wiegand Readers



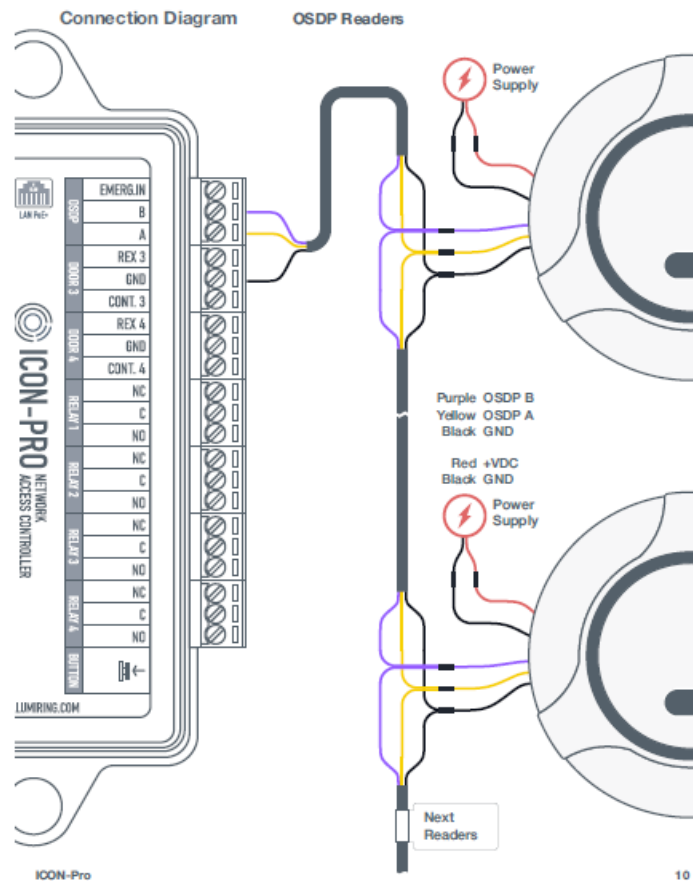
Wiegand Readers



- Before you start building cable networks for Wiegand readers, read the interface specifications.
- The wiring diagram is shown as an example. In reality, wire colors may vary depending on the model of the third-party reader.
- Please refer to the reader manufacturer's instructions.

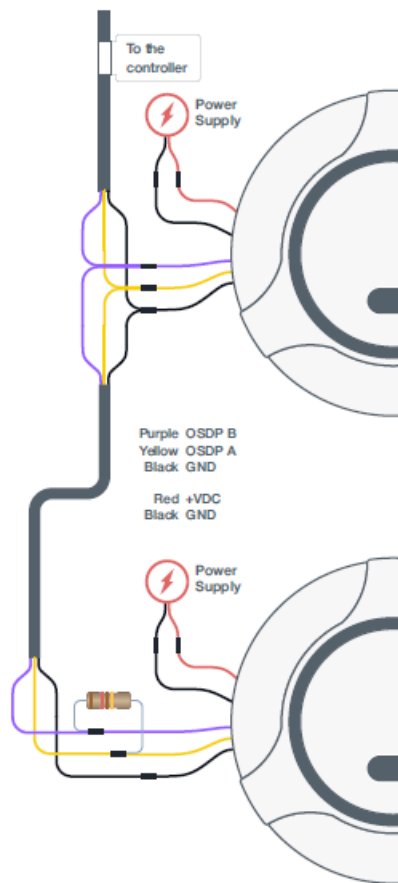
Coming Soon!

Connection Diagram

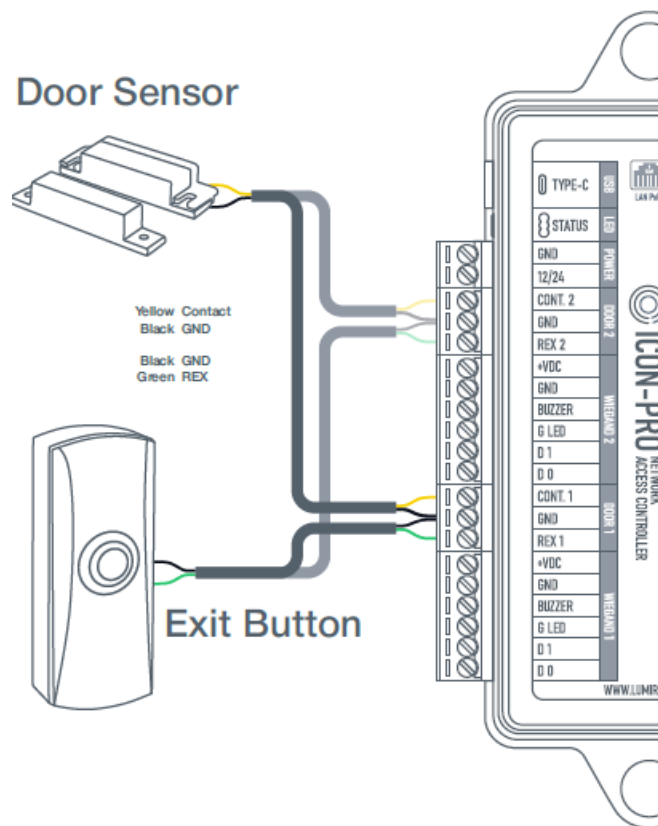


OSDP Readers

- BE SURE TO CONNECT THE GND OF THE CABLE FROM THE CONTROLLER TO THE GND OF THE AUXILIARY POWER SUPPLY!
- DO NOT USE POWER SUPPLIES WITH DIFFERENT VOLTAGE LEVELS!
- All branches from the primary data cable should be kept as short as possible.
- The length of taps from the primary data cable should be at most 8 inches.
- Always route the main data cable away from power cables and sources of electrostatic interference.
- Terminal resistors ensure that the “open” end of the cable is matched to the rest of the line, eliminating signal reflection.
- The nominal resistance of the resistors corresponds to the wave impedance of the cable, and for twisted pair cables is typically 100 to 120 ohms.
- Install a 120 ohm terminating resistor on the outermost reader if the cable runs more than 150 feet. See RS-485 interface specifications for more information.



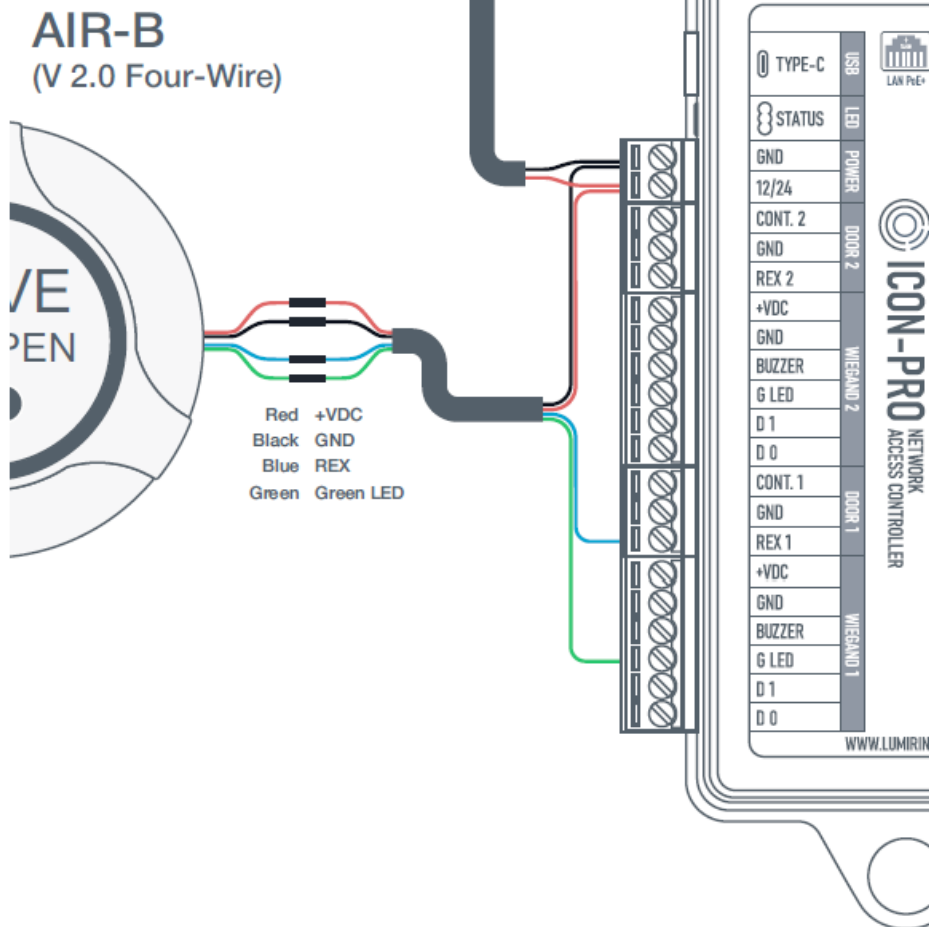
Door Sensor and Exit Button



- Specify the “Open” condition in the Controller settings when a door sensor is connected.
- Connecting to the “DOOR 3,» and “DOOR 4” connector is done in the same way.
- Specify the “Closed” condition in the Controller settings when an exit button is connected.

Connection Diagram

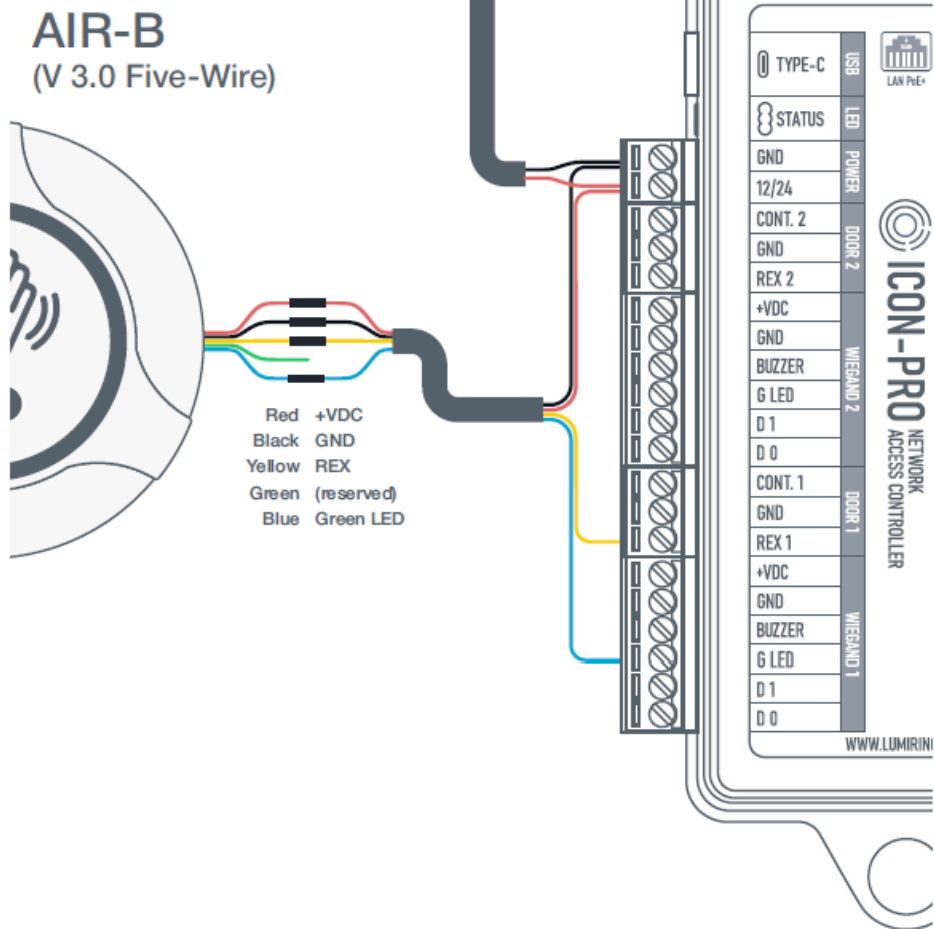
AIR-Button V 2.0



- Connecting to the “DOOR 2,” “DOOR 3,” and “DOOR 4” connectors is done in the same way.
- The button's default factory settings is “Normally Open.”
- This means that a low level signal for control will appear on the blue wire when you put your hand to the optical sensor.
- When setting the exit button in the cloud service, select the “closed” condition.
- This means that when a “low level” signal is input to the REX input, the controller relay will be activated.

Connection Diagram

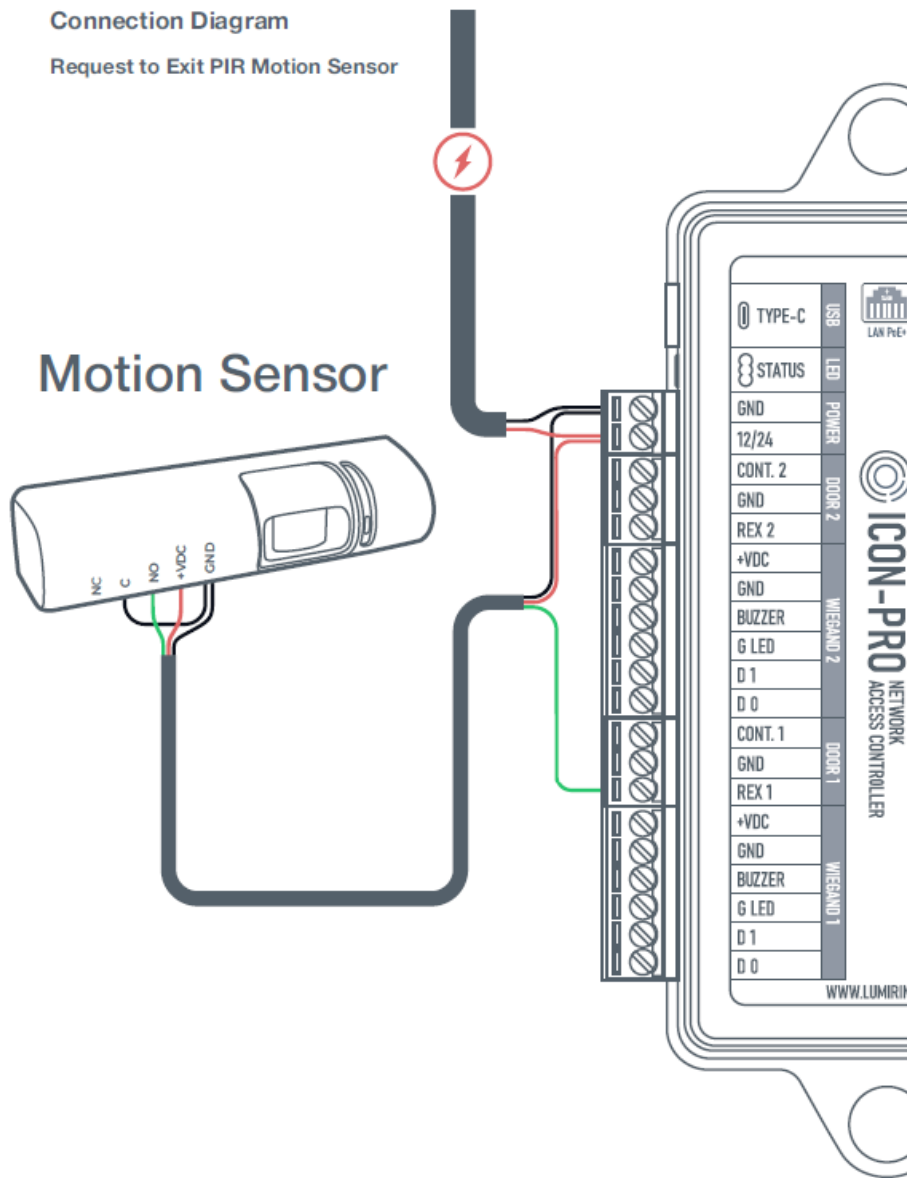
AIR-Button V 3.0



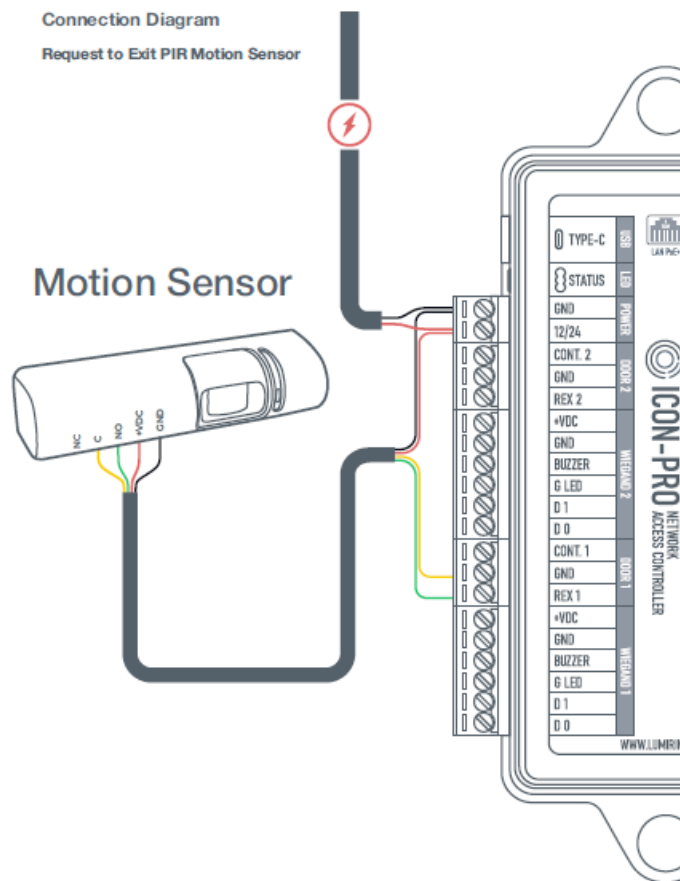
- Connecting to the “DOOR 2,” “DOOR 3,” and “DOOR 4” connectors is done in the same way.
- The buttons is default factory settings is “Normally Open.”
- This means that a low level signal for control will appear on the blue wire when you put your hand to the optical sensor.
- When setting the exit button in the cloud service, select the “closed” condition.
- This means that when a “low level” signal is input to the REX input, the controller relay will be activated.

Connection Diagram

Request to Exit PIR Motion Sensor



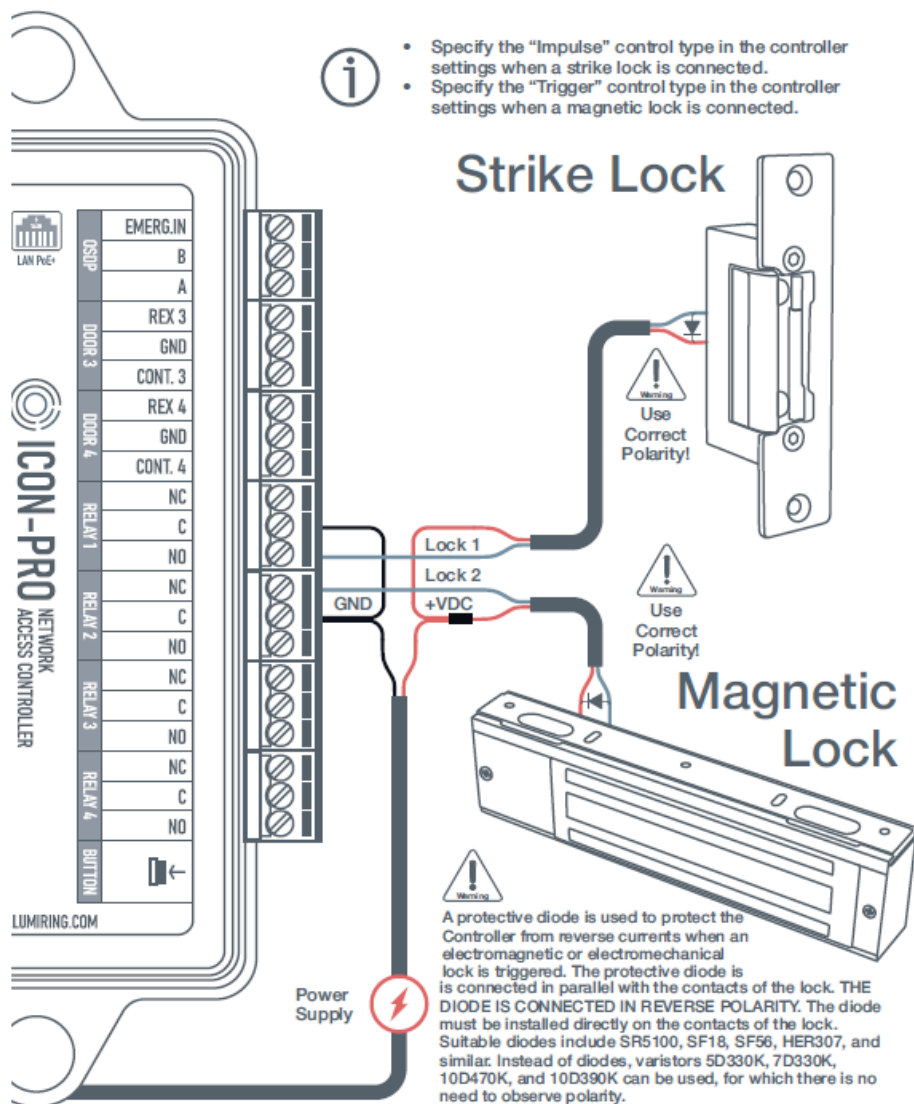
- Connecting to the “DOOR 2,” “DOOR 3,” and “DOOR 4” connectors is done in the same way.
- The motion sensor acts as an automatic exit button and is therefore connected as an exit button. Connect the wires to contacts C (Common) and NO (Normally Open) of the motion sensor relay.
- Use the pulse method to control the relay, which is activated when the motion sensor is triggered.
- When configuring the exit button in the cloud service, select the “closed” condition. This means that when a «low level” signal is input to the REX input, the controller relay will be activated.



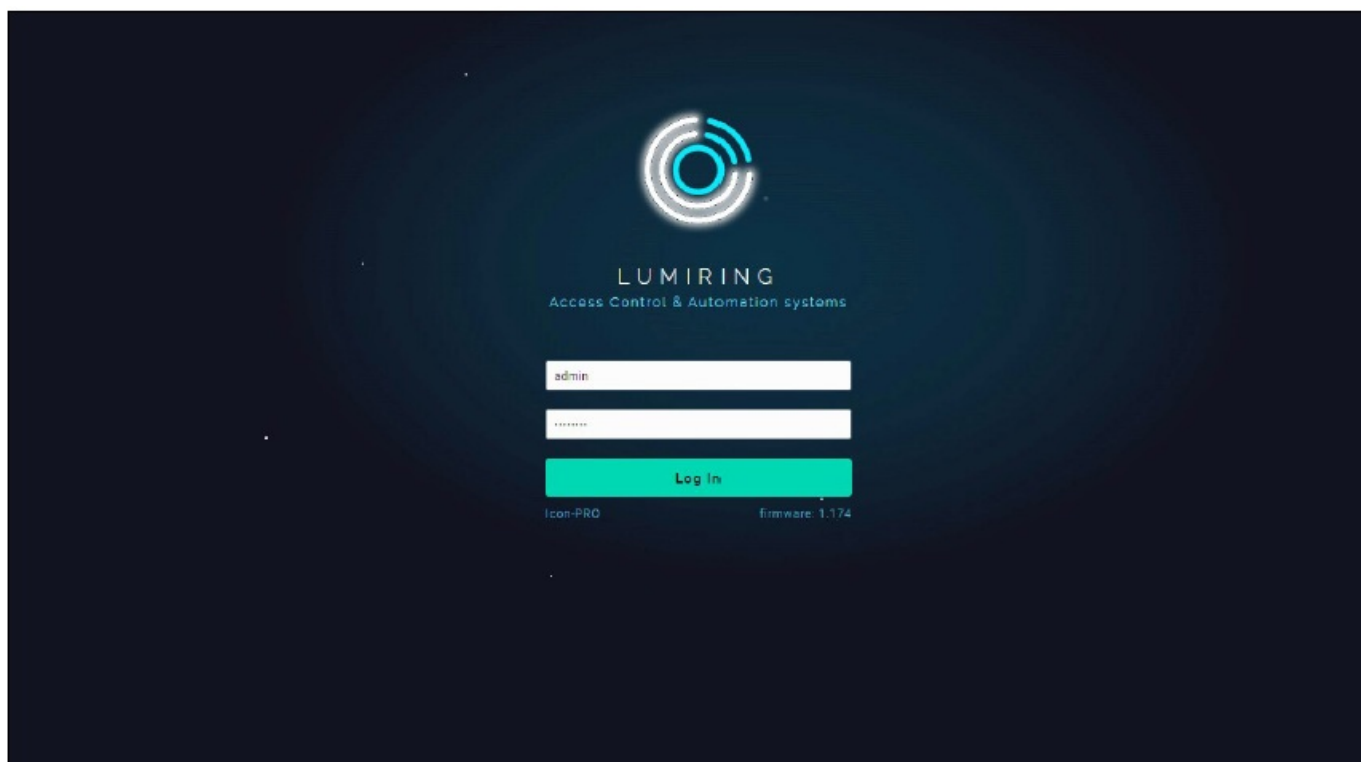
- Connecting to the “DOOR 2,” “DOOR 3,” and “DOOR 4” connectors is done in the same way.
- The motion sensor acts as an automatic exit button and is therefore connected as an exit button. Connect the wires to contacts C (Common) and NO (Normally Open) of the motion sensor relay.
- Use the pulse method to control the relay, which is activated when the motion sensor is triggered.
- When configuring the exit button in the cloud service, select the “closed” condition. This means that when a «low level» signal is input to the REX input, the controller relay will be activated.

Connection Diagram

Electric Locks



Login



Connecting to Device

Connecting to the built-in Wi-Fi access point (AP).

- Step 1. Connect the device to a power source.
- Step 2. Search for Wi-Fi and connect to the ICON-Pro_xxxxxxxx network.
- Step 3. In the address bar of your browser, enter the factory IP address (192.168.4.1) and press “Enter.” Wait for the start page to load.
- Step 4. Enter the user name and password (if they have already been set) and press “Enter.” If the device is new or has been previously reset, enter login: admin, pass: admin123 and press “Enter.”

Connecting via Ethernet

Reminder: You must first change the network settings of the Controller if they are different from those of the network you are connecting to. The Controller and the mobile device from which you are configuring must be on the same network.

- Step 1. Connect the Ethernet cable to the device using an adapter or by connecting the wires, as shown in the diagram below.
- Step 2. Connect the device to a power source.
- Step 3. In the address bar of your browser, enter the device IP address and press enter.
- Step 4. Enter the user name and password (if they have already been set) and press “Enter.” If the device is new or has been previously reset, enter login: admin, pass: admin123 and press “Enter.”

Quick Start

The screenshot displays the LumiRing Quick Start interface, which is divided into three main sections: Network, Cloud, and Security. At the top, there is a diagram showing the device (ICON) connected to a Wi-Fi router, which is then connected to a cloud service (CLOUD). The Network section prompts the user to select a network type, with 'Wired Ethernet Network' selected. The Cloud section prompts the user to enter their cloud account information, including an Account ID (235) and a Device note (Lumiring). The Security section prompts the user to change the password for device network access and device Wi-Fi AP, with a checkbox for 'Use the same password for two purposes' checked. The Wi-Fi AP section shows the Local Wi-Fi AP name (Icon-PRO_6350800) and fields for Password and Repeat password. Each section has a 'Submit' button at the bottom.

Network

Please select type of your network connection and make connection settings

Network type

Wired Ethernet Network

Cloud

Please enter your cloud account information

Account ID

235

You can find the Account ID information at your AllDoors cloud account. Please check the account settings. If you have not registered at the AllDoors cloud - please [REGISTER](#) first.

Device note

Lumiring

Security

Please change password for devices network access and device Wi-Fi AP.

☒ Use the same password for two purposes

Wi-Fi AP

Local Wi-Fi AP name (8 characters minimum)

Icon-PRO_6350800

Password (8 characters minimum)

Repeat password

The device's interface allows you to use the Quick Start feature to quickly set up your device to connect to the Internet and add it to a cloud service.

Network:

Select the connection method: Wi-Fi or Ethernet.

- A. Wi-Fi:
 - Click on the empty Service Set Identifier (SSID) field to scan and choose a network.
 - Enter the network password and click “Submit” to establish the connection.
- B. Ethernet:
 - Submit the entered information to confirm the settings.

Cloud:

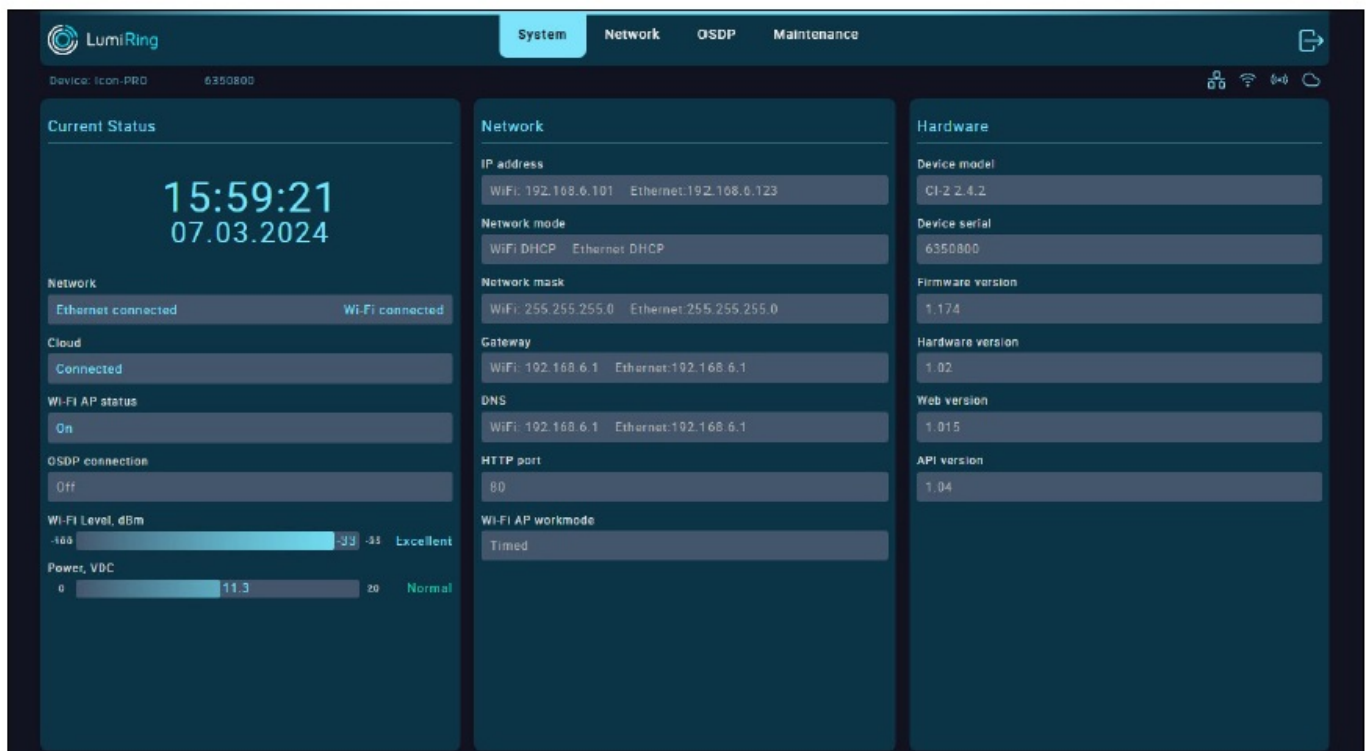
- Enter your account ID and click “Submit.”

Security:

- Checkbox: Use the same password for two purposes.
- The entered SSID will be displayed during Wi-Fi scanning.
- Choose a strong and unique password, and keep it secured at all times.

Note: After changing the factory default password to connect to the built-in Wi-Fi AP or the login password, a reboot may be required, increasing the time until the device appears in the cloud service.

System



This section displays information about the current settings and status of the device.

The Current Status subsection displays the:

The Current Status subsection displays the:

- Current time and date (when the device is connected to the Internet).
- Status and type of connection of the device to the router in use.
- Status of the device's connection to the cloud server.
- Status of the built-in Wi-Fi AP.
- OSDP connection status.
- Level and quality of the device's connection to the Wi-Fi router.
- Power supply voltage value.

The Network Information subsection displays the:

- Device's current network settings.
- Device's network address.
- Network mode – Manual or Dynamic Host Configuration Protocol (DHCP).
- Network mask.
- Domain Name Service (DNS).
- Network port of the device.

In the Hardware Information subsection, you can see the:

- Device model name.
- Device serial number.
- Current firmware version.
- Current hardware version of the device.
- Web version used by the device.
- API version used by the device.

Network

In the Network section, you can set up an Internet connection via Wi-Fi or Ethernet, you can change the connection settings for the built-in Wi-Fi AP, and you can set its activity time. This section is also intended for configuration when connecting to a cloud server.

The Network subsection provides the following functions:

- Select your preferred Wi-Fi or Ethernet network type. When using Wi-Fi, click on the SSID name field to search for available Wi-Fi networks and enter the password to connect.
- Select DHCP for automatic network settings or Manual to enter all network settings manually in the available fields below, then click “Connect.”
- When using Ethernet, select DHCP for automatic network settings or Manual to enter all network settings manually in the available fields below and then click “Update.”

The Wi-Fi AP subsection provides the following functions:

- In the Local Wi-Fi AP name field, enter the device’s network name.
- In the Password field, enter the connection password.
- “Enable hidden mode” checkbox: hides the AP’s built-in network name when searching. To connect to the device, you must know its name and enter it manually when connecting.
- In the “Wi-Fi Timer, min” field, enter a value from 1 to 60 minutes. If you enter 0, the access point will be on all the time.
- HTTP port: By default, the device uses port 80.

The Cloud settings subsection allows you to connect the Controller to a cloud server for later use.

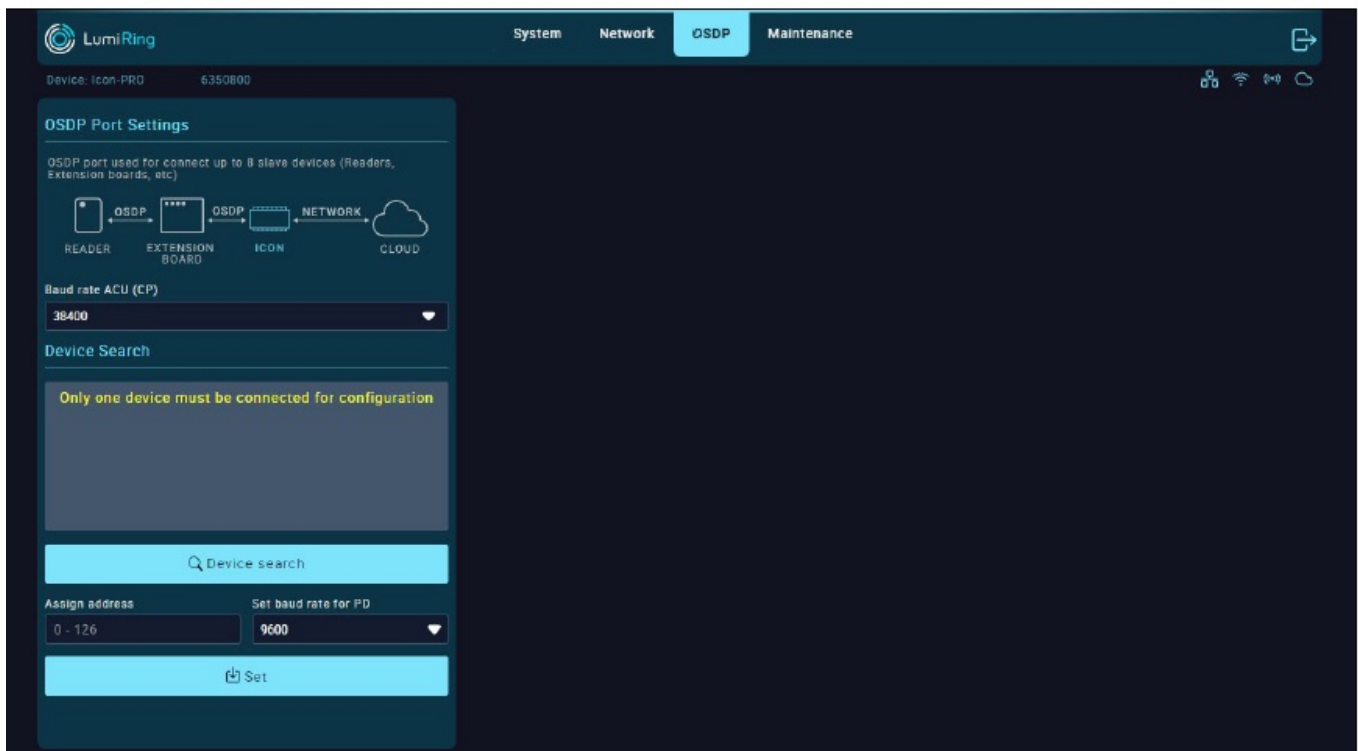
- In the Server form, you can select one of the available servers to connect to, or select a custom connection option if a private server is used.
- The Account ID form is used for adding to the All Doors cloud system, as you only need to specify the ID to

connect.

When using a private server, you must fill in the parameters required for connection. The parameters are determined by the properties of the server and its security level.

- Enter the address of the MQTT server, login ID and password for logging in. Then specify the location of the device to create the topic

Open Supervised Device Protocol (OSDP)



The “Open Supervised Device Protocol (OSDP)” section can be used to search for devices connected via the RS-485 interface. This tool allows you to assign the address and baud rate.

You must first set the addressing and baud rate of the OSDP devices you want to use with the Controller.

It is important to note that the “Address” of all OSDP devices must be unique, and the “Baud rate” must be the same.

- Connect the first OSDP device to the controller according to the wiring diagram.

Note: Only one OSDP device can be connected to the Controller during the search; otherwise, the device may not be detected.

- Select the ACU baud rate to match the OSDP device and click the “Device search” button.

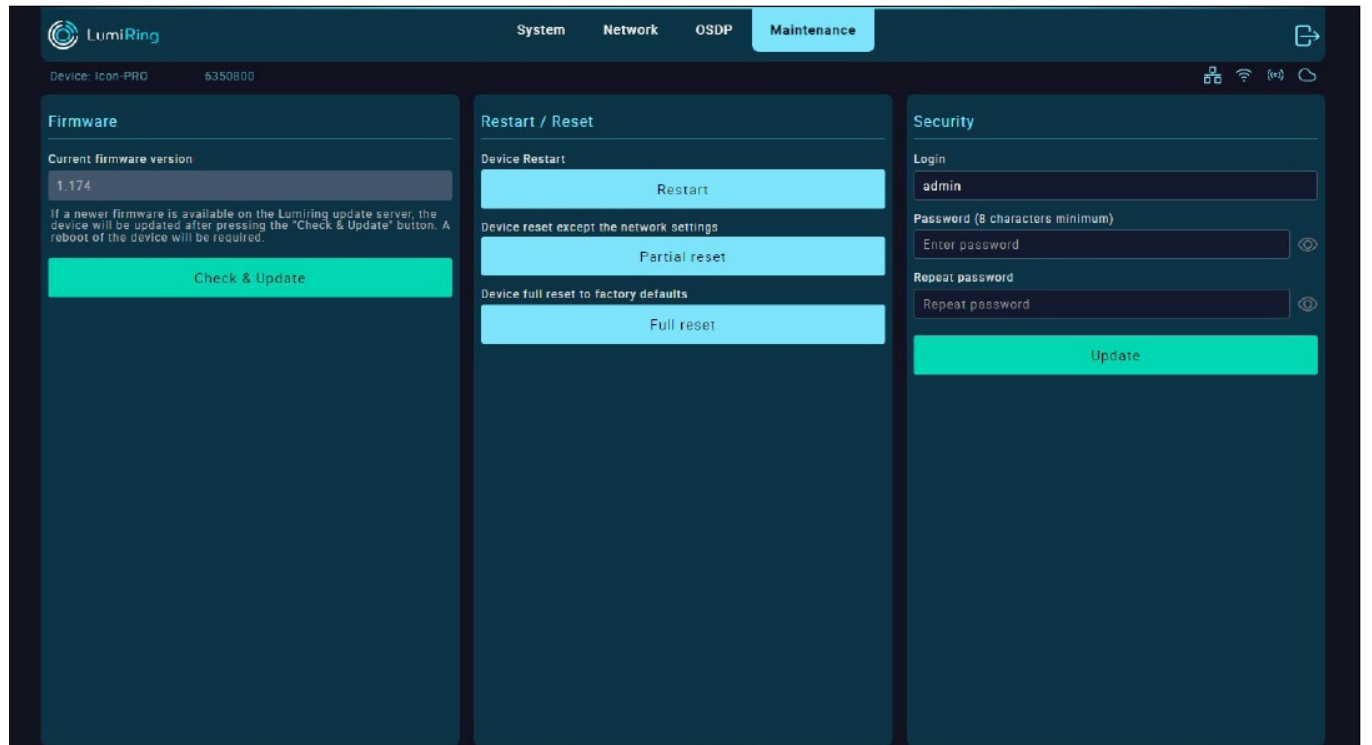
If the search results do not find an OSDP device, change the ACU baud rate and click the “Device search” button again.

- When a device is found, assign it an “Address, ” select the desired “Baud rate,” and click the “Set” button. Disconnect the first OSDP device and connect the next one.
- Repeat the operation with all OSDP devices.

- Once you individually set different addresses and the same baud rate for all OSDP devices, they can be connected to the Controller.

Further configuration and communication with the devices are done via the cloud service. The OSDP section is under development and will be available soon. Watch for updates.

Maintenance



The Firmware section displays the current version of the unit's firmware.

Note: It is recommended to upgrade the device to the latest firmware version before use.

- The device must be connected to the Internet and close to a Wi-Fi router during the update.
- To download a new firmware version, connect to a network with Internet access in the Network section.
- Click the “Check & Update” button and wait until the update process completes.
- A modal window will prompt you to reboot the device.
- After restarting, verify that the device version has changed.

Note: The update duration depends on the Internet connection quality and firmware version but usually takes a maximum of 5 minutes.

If the update takes more than 5 minutes, forcibly reboot the device by switching off the power and trying the update again.

A power failure or network connection interruption during the update may cause a firmware update application error. If this happens, disconnect power from the device for 10 seconds and reconnect.

Leave the unit switched on for 5 minutes without attempting to connect or log into the web interface.

The unit will automatically download the latest previously used firmware version and resume operation.

The Restart/Reset subsection performs the following actions:

- Restart – restarts the device.

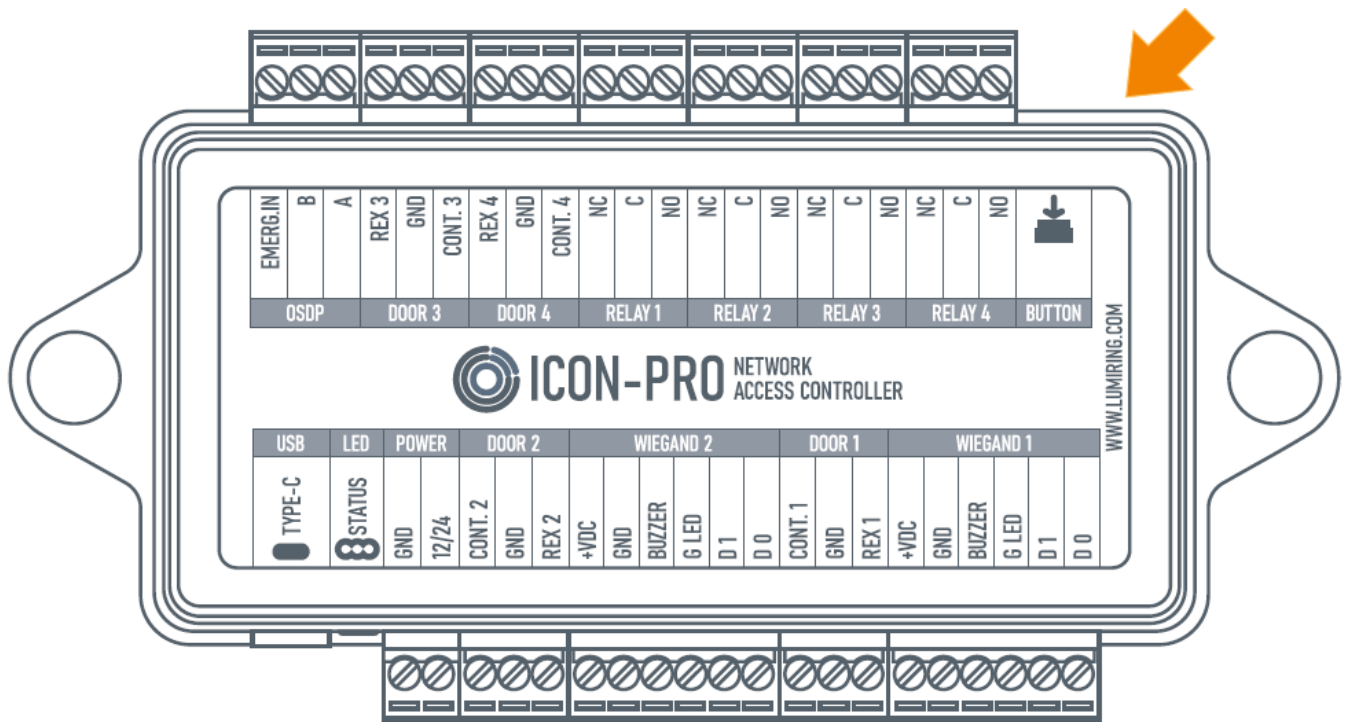
- Full reset – resets all settings of the device to factory defaults.

The Security subsection is used to change the password for logging into the interface of the device:

- Enter the new login password and confirm it.
- Apply the changes by clicking “Update.”

The new password can be used the next time you log into the device interface.

Hardware Reset



Hardware Reset

1. Hold the button down until a long beep sounds.
2. Release the button.
3. The device will start flashing red, emitting three short beeps, and then switch to flashing blue.
4. Wait for the blue LED to stop flashing, disconnect power to the device for 5 seconds, and reconnect it.
5. The device will be ready for operation when the blue LED starts to glow continuously.

LED Indication

LED color/behavior	Device status	Description
Blue (flashing)	The device is booting up	The device performs booting and initialization.
Blue (solid)	Ready to work	The device is in default mode and ready for setup.
Green (slow flashing)	Online. Main connection.	Connected to the cloud via primary connection
Yellow (slow flashing)	Online. Backup connection.	Connected to the cloud via backup connection
Purple (slow flashing)	No cloud connection	The device cannot connect to the cloud.
Red (solid)	Full reset	The device is performing a full system reset.

Glossary

- +VDC – Positive voltage direct current.
- Account ID – A unique identifier associated with an individual or entity's account, used for authentication and access to services.
- ACU – Access control unit. The device and its software that establishes the access mode and provides reception and processing of information from readers, control of executive devices, display and logging of information.
- API – application programming interface.
- BLE – Bluetooth Low Energy.
- Block in – Function for the input activating "block out" with the event "blocked by operator." It is used for turnstile control.
- Block out – Output activated when "block In" is triggered.
- Bluetooth – A short-range wireless communication technology that enables wireless data exchange between digital devices.
- BUZZ – Output for connecting the reader wire responsible for sound or light indication.
- Cloud – A cloud-based platform or service provided to manage and monitor an access control system over the Internet. Allows administrators to manage access rights, monitor events, and update system settings using a web-based interface, providing the convenience and flexibility to manage the access control system from anywhere there is an Internet connection.
- Copy protection – A method used to prevent unauthorized copying or duplication of smart cards to secure the access control system and prevent possible security breaches.
- D0 – "Data 0." A bit line with the logical value "0."
- D1 – "Data 1." A bit line with the logical value "1."
- DHCP – Dynamic Host Configuration Protocol. A network protocol that allows network devices to automatically obtain an IP address and other parameters necessary for operation in a Transmission
- Control Protocol/Internet Protocol TCP/IP network. This protocol works on a "client-server" model.
- DNS – Domain Name System is a computer-based distributed system for obtaining domain information. It is most often used to obtain an IP address by host name (computer or device), to obtain routing information, and to obtain serving nodes for protocols in a domain.
- DPS – Door position sensor. A device that is used to monitor and determine the current status of a door, such as whether the door is open or closed.
- Electric latch – An electronically controlled door locking mechanism.
- Emergency in – Input for emergency situations.
- Encryption password – Key for data protection.
- Ethernet network – A wired computer network technology that uses cables to connect devices for data transmission and communication.
- Exit/Entry/Open button – Logic input which, when activated, activates the corresponding output. Causes an event depending on the attribute used.
- Exit/Entry/Open out – Logical output that is activated when the corresponding input is triggered. Causes an event depending on the attribute used.
- External relay – Relay with potential- free dry contact for remote control of the power supply. The relay is equipped with a dry contact, which is galvanically unconnected to the power supply circuit of the device.
- GND – Electrical ground reference point.


- HTTP – Hypertext Transfer Protocol. A fundamental protocol for transferring data, documents, and resources over the Internet.
- RFID Identifier 125 kHz – Radio-frequency identification at 125 kHz; short-range, low-frequency technology with a typical range of 7 cm to 1 m.
- RFID Identifier 13.56 MHz – Radio-frequency identification at 13.56 MHz; high-frequency technology with short to moderate range, around 10 cm.
- Keypad – A physical input device with a set of buttons or keys, often used for manual data entry or access control.
- LED – Light emitting diode.
- Loop sensor – A device that detects the presence or passage of traffic in a certain area by means of a closed electrical loop. Used in barriers or gates.
- Magnetic Lock – A locking mechanism that uses electromagnetic force to secure doors, gates, or access points.
- MQTT – Message Queuing Telemetry Transport. A server system that coordinates messages between different clients. The broker is responsible, among other things, for receiving and filtering messages, identifying the clients subscribed to each message, and sending messages to them.
- NC – Normally closed. Configuration of a changeover contact that is closed in the default state and open when activated.
- NO – Normally open. A switch contact configuration that is open in its default state and closes when activated.
- No-touch button – A button or switch that can be activated without physical contact, often using proximity or motion-sensing technology.
- Open collector – A transistor switch configuration in which the collector is left unconnected or open, typically used for signal grounding.
- OSDP – Open Supervised Device Protocol. A secure communication protocol used in access control systems for device-to-device data exchange.
- Pass control – The process of regulating, monitoring, or granting permission for individuals to enter or exit a secure area.
- Power supply – A device or system that provides electrical energy to other devices, enabling them to operate and function.
- Radio 868/915 MHz – A wireless communication system operating on the 868 MHz or 915 MHz frequency bands.
- Reader – A device that scans and interprets data from RFID or smart cards, often used for access control or identification.
- Revers byte order – A process of reordering the sequence of bytes in a data stream, often for compatibility or data conversion.
- REX – Request to exit. An access control device or button used to request to exit from a secured area.
- RFID – Radio-frequency identification. A technology for wireless data transmission and identification using electromagnetic tags and readers.
- RS-485 – A standard for serial communication used in industrial and commercial applications, supporting multiple devices over a shared network.
- Strike lock – An electronic locking mechanism that releases a door's latch or bolt when electrically activated, often used in access control systems.
- Terminal block – A modular connector used for connecting and securing wires or cables in electrical and

electronic systems.

- Topic – In the context of MQTT, a label or identifier for published messages, enabling subscribers to filter and receive specific information.
- Unblock in – An input or signal used to release a lock, barrier, or security device, allowing access to a previously secured area.
- Unblock out – An output or signal used to release a lock, barrier, or security device to allow exit or opening.
- Wiegand format – A data format used in access control systems, typically for transmitting data from card readers to controllers.
- Wiegand interface – A standard interface used in access control systems to communicate data between card readers and access control panels.
- Wi-Fi AP – Wireless access point. A device that allows wireless devices to connect to a network.
- Wireless access control gateway – A device that manages and connects wireless access control devices to a central system or network.

For Notes

Documents / Resources

	<p>LumiRing ICON-Pro Access Control Devices [pdf] Instruction Manual ICON-Pro Access Control Devices, ICON-Pro, Access Control Devices, Control Devices</p>
--	---

References

- support.lumiring.com
- [User Manual](#)

Manuals+, Privacy Policy

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.