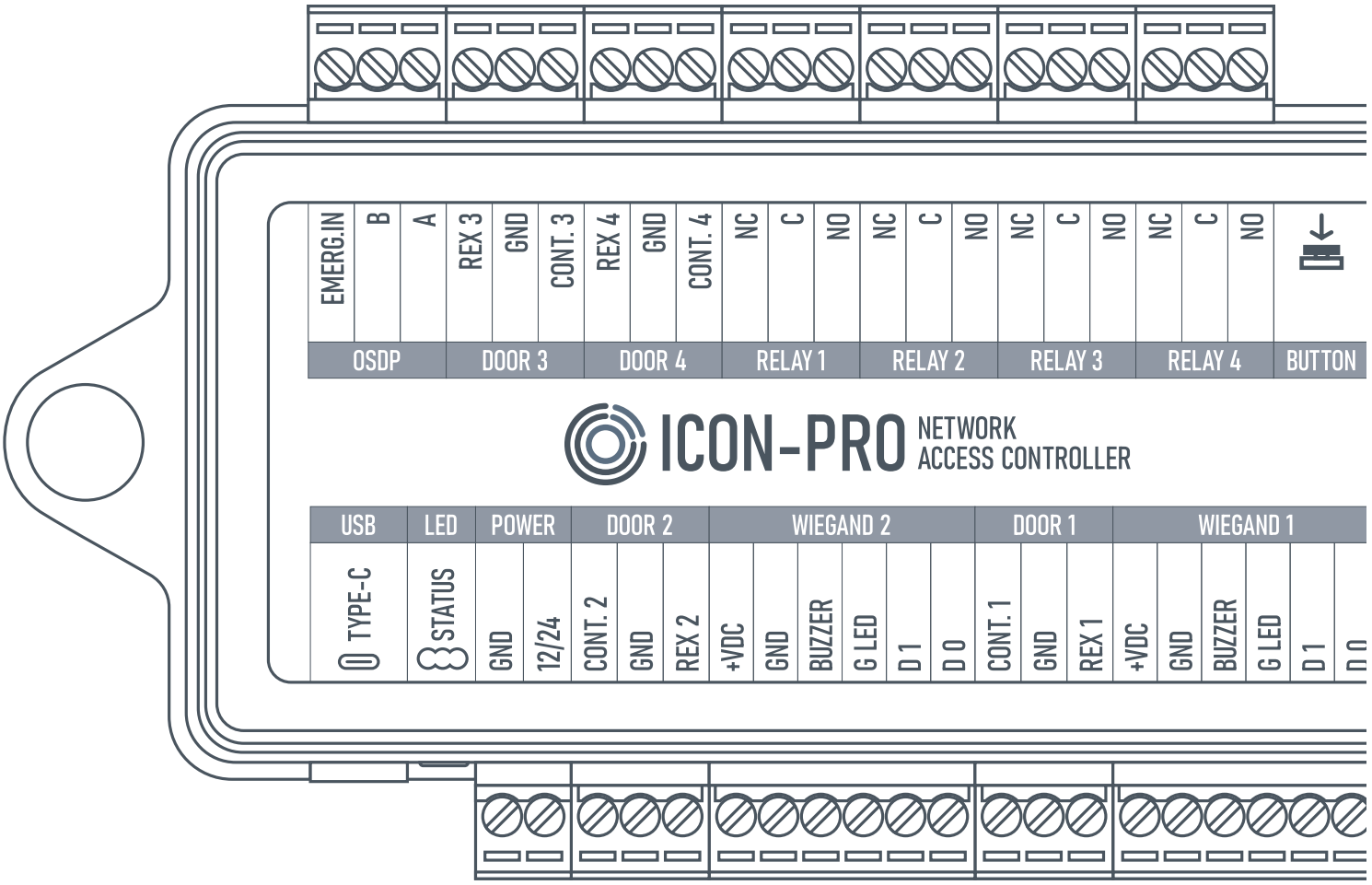
Federal Communications Commissions

MANUAL



ICON-Pro

CONTENTS

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.

Video manuals

We've created these video manuals to make device usage simple and seamless for you. Our goal is to provide clear, step-by-step guidance that addresses common challenges and ensures you can maximize the potential of our device with minimal effort. Whether you're setting up the device, troubleshooting issues, or exploring advanced features, these tutorials are designed to enhance your experience and save you time.

Quick Start Guide
5:00 min.

Device Wizard
1:30 min.

Access Point Wizard
1:40 min.

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: -40°F ~ 149°F (-40°C ~ 65°C)
- Storage: -40°F ~ 158°F (-40°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

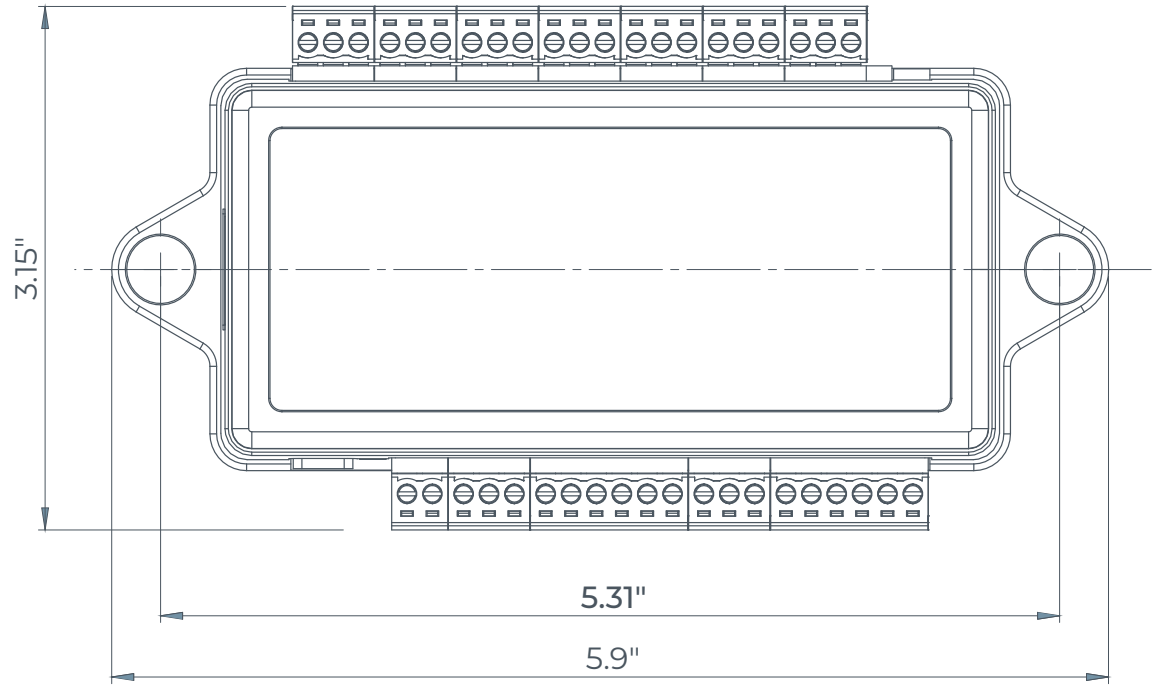
Web page password:

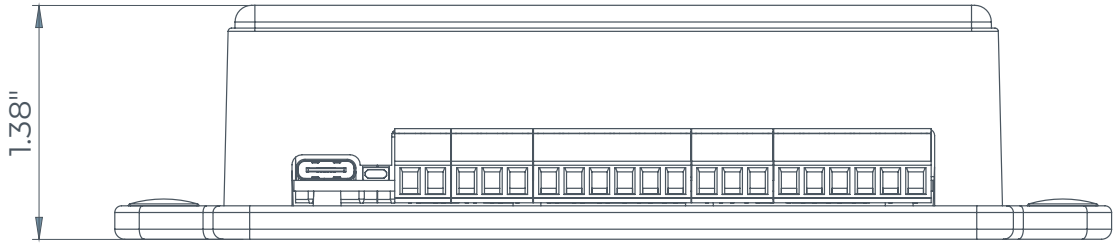
- admin123

AP Wi-Fi timer:

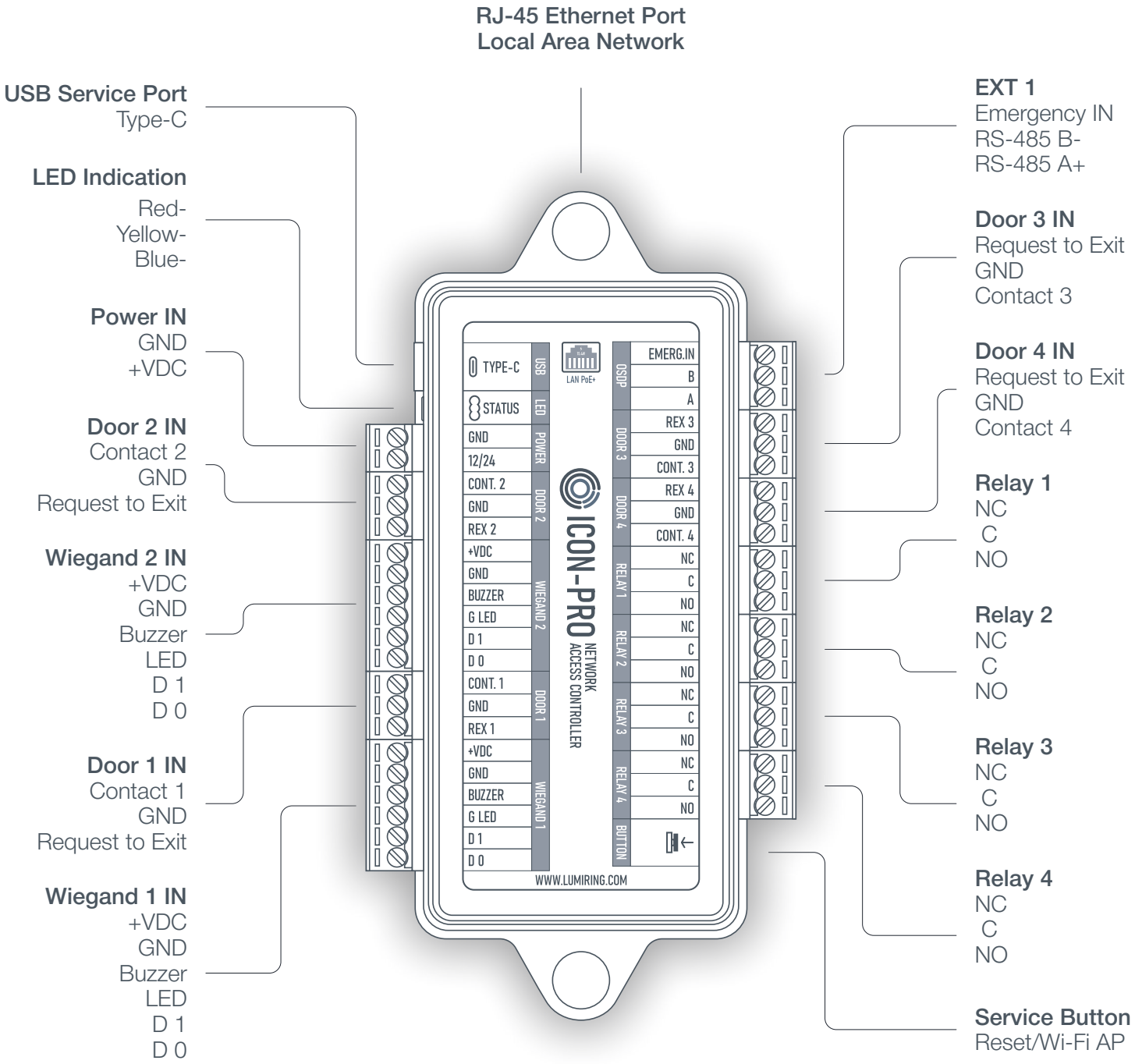
- 30 minutes

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 high-voltage 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.

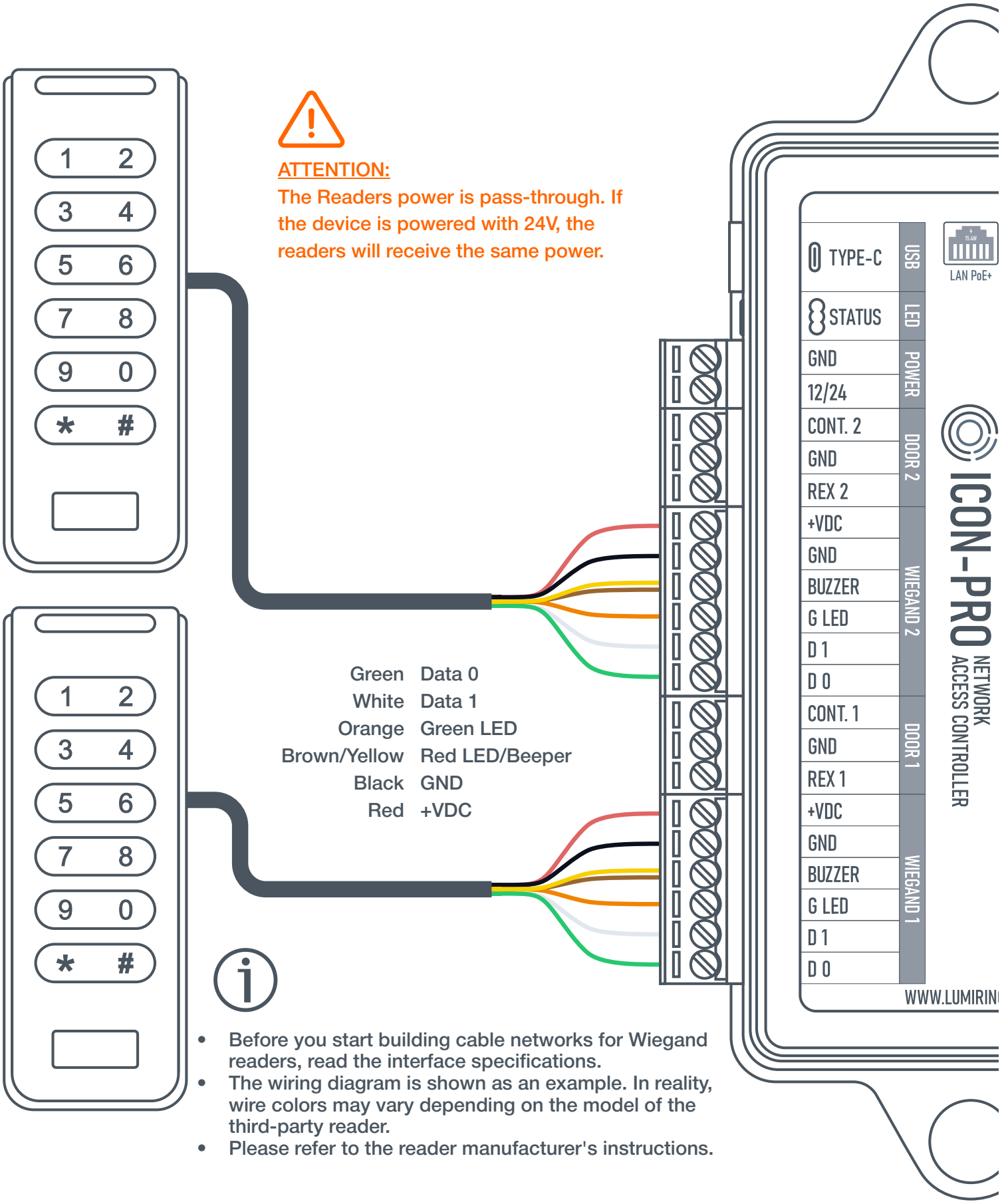
Protection Against High Current Surges

- 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

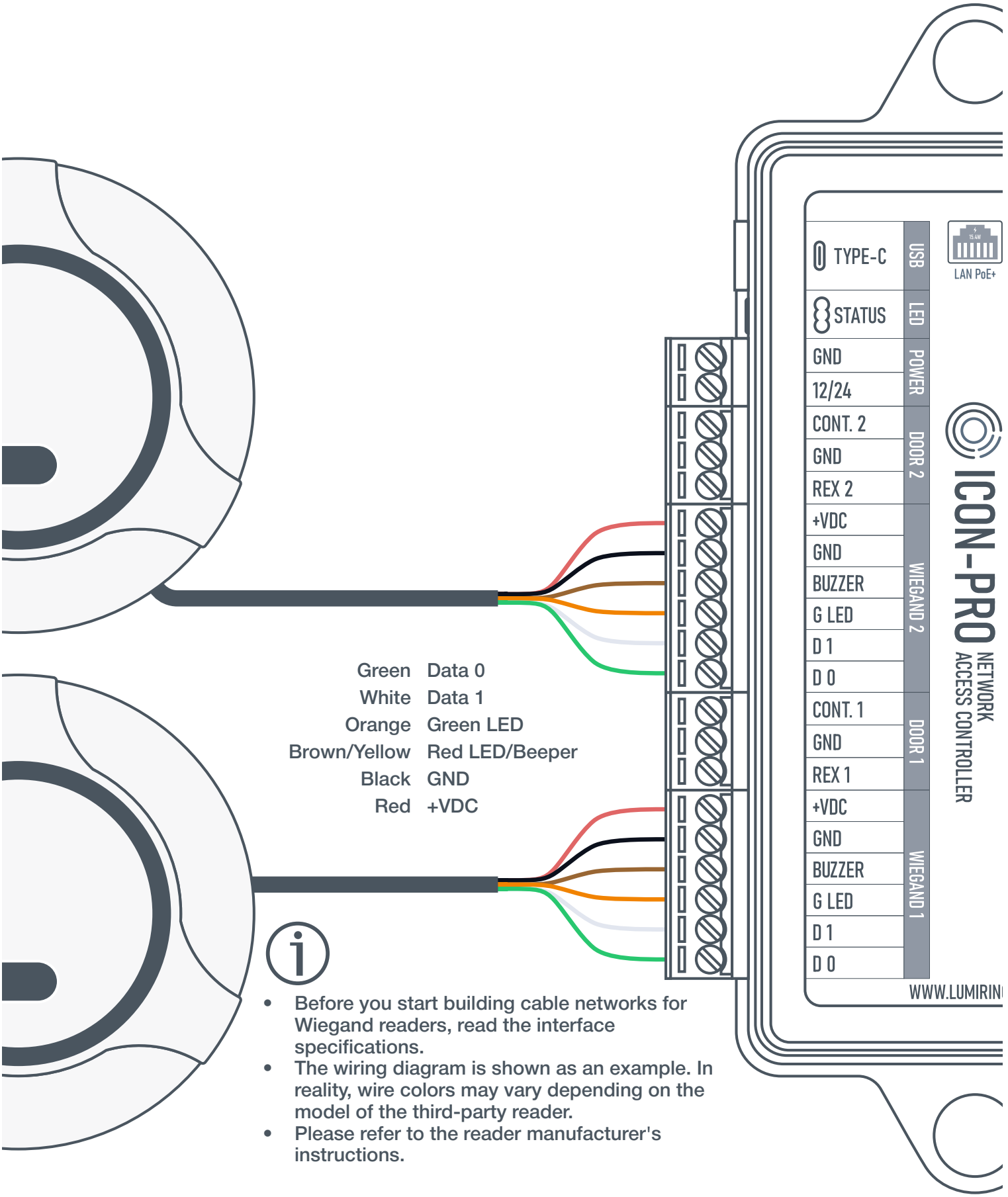
Wiegand Readers



- 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.

Connection Diagram

Wiegand Readers

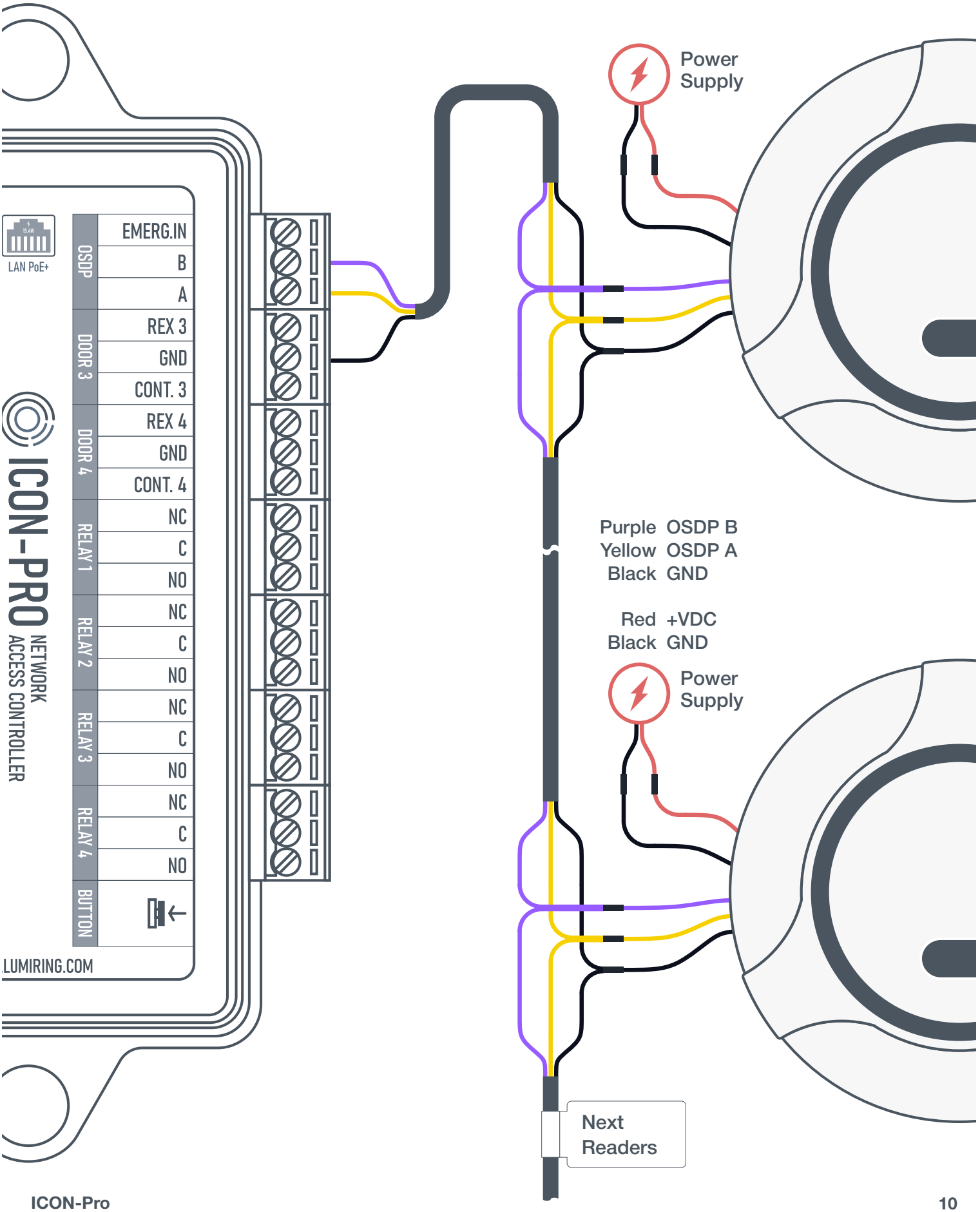


Green	Data 0
White	Data 1
Orange	Green LED
Brown/Yellow	Red LED/Beeper
Black	GND
Red	+VDC

- 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.

Connection Diagram

OSDP Readers



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.

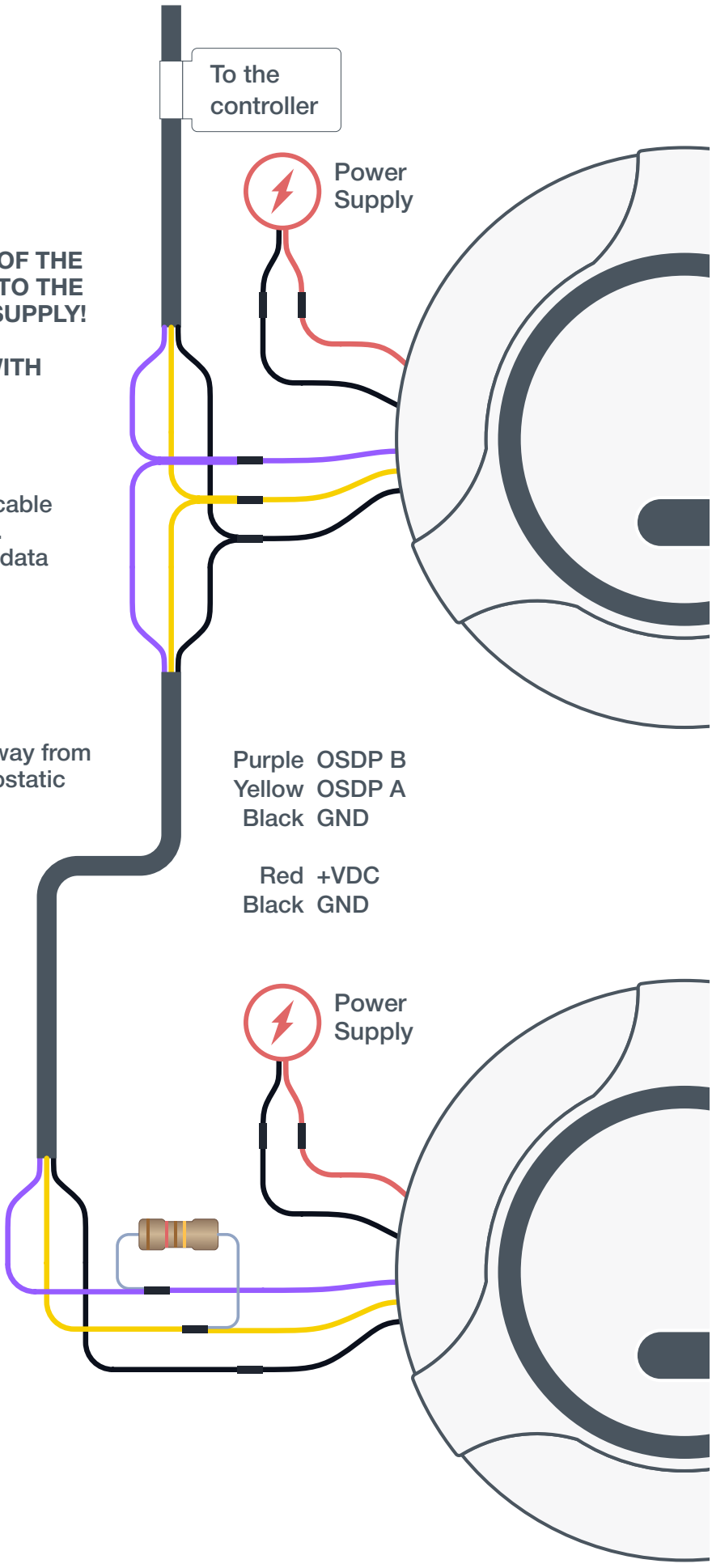
Always route the main data cable away from power cables and sources of electrostatic interference.

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.

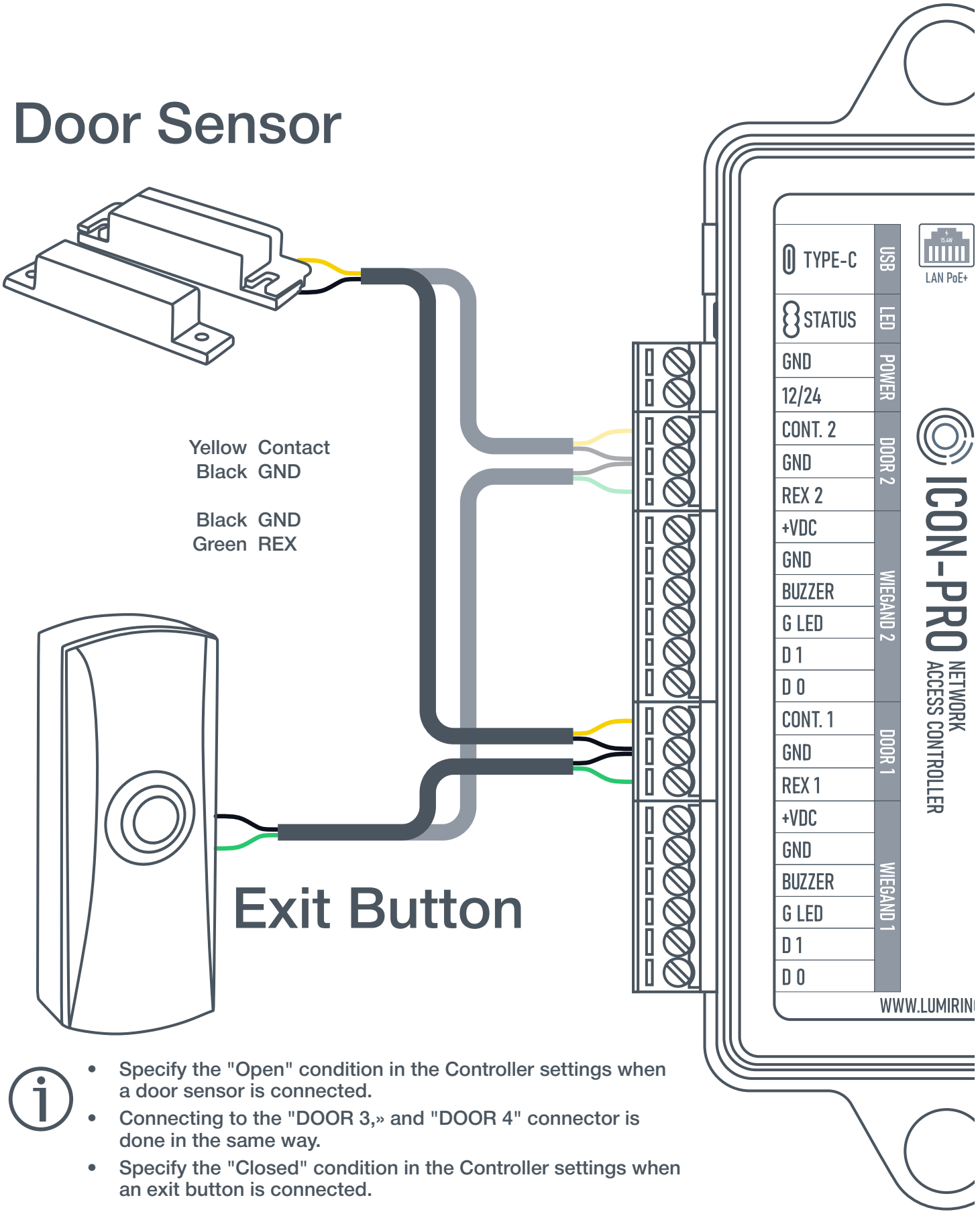
Install a 120 ohm terminating resistor on the outermost reader if the cable runs more than 150 feet.

See RS-485 interface specifications for more information.



Connection Diagram

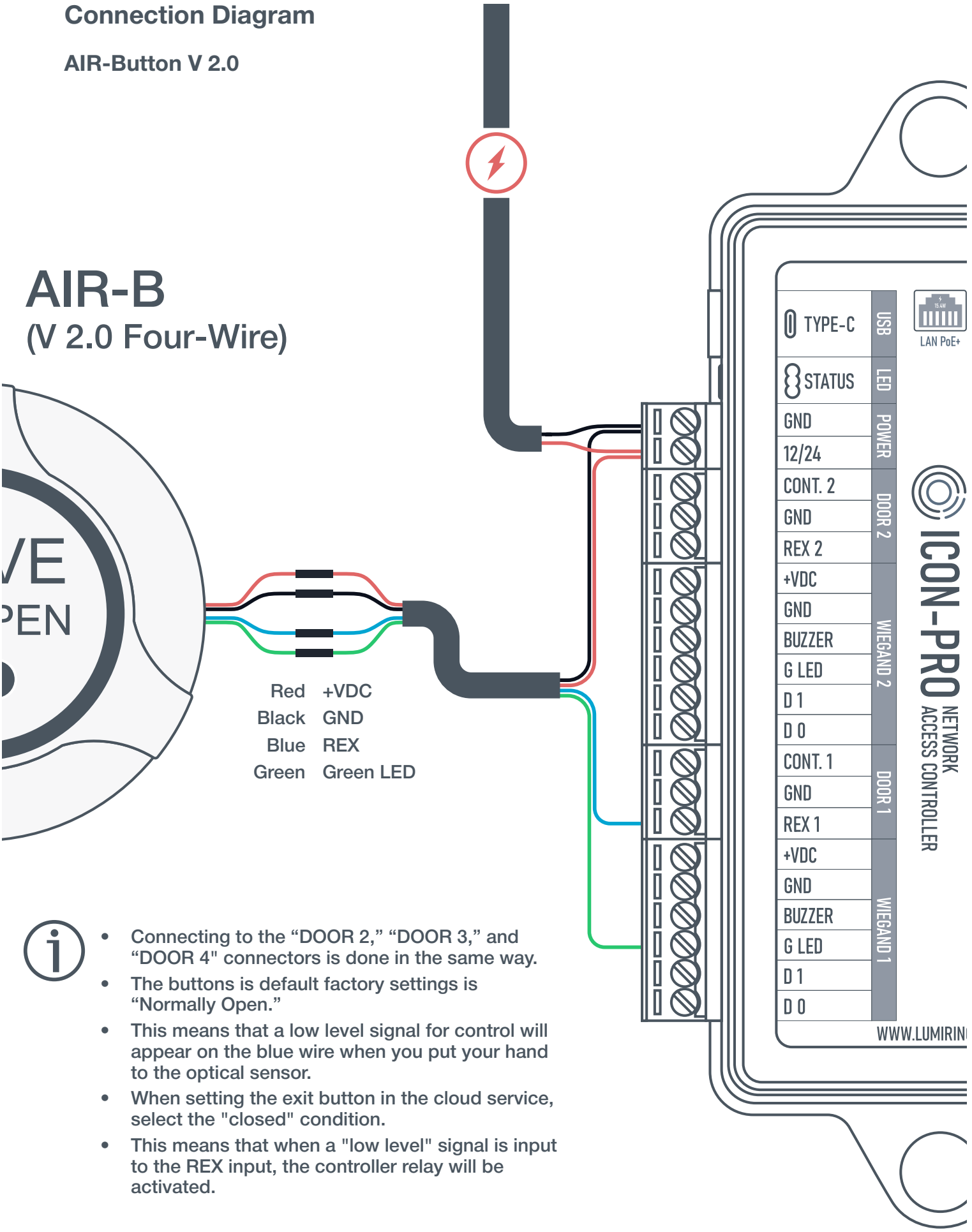
Door Sensor and Exit Button



- 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

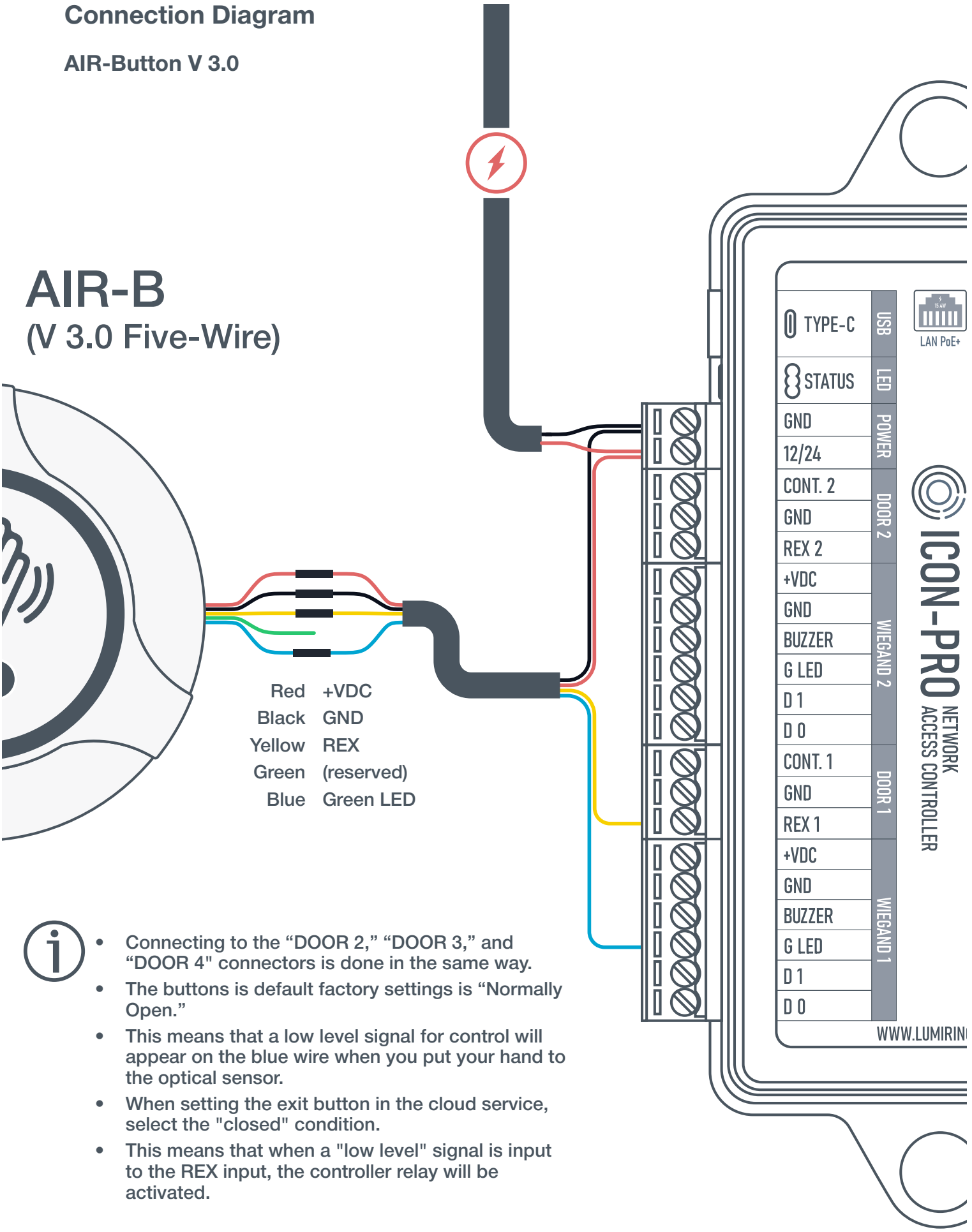
AIR-Button V 2.0



- Connecting to the “DOOR 2,” “DOOR 3,” and “DOOR 4" connectors is done in the same way.
- The 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

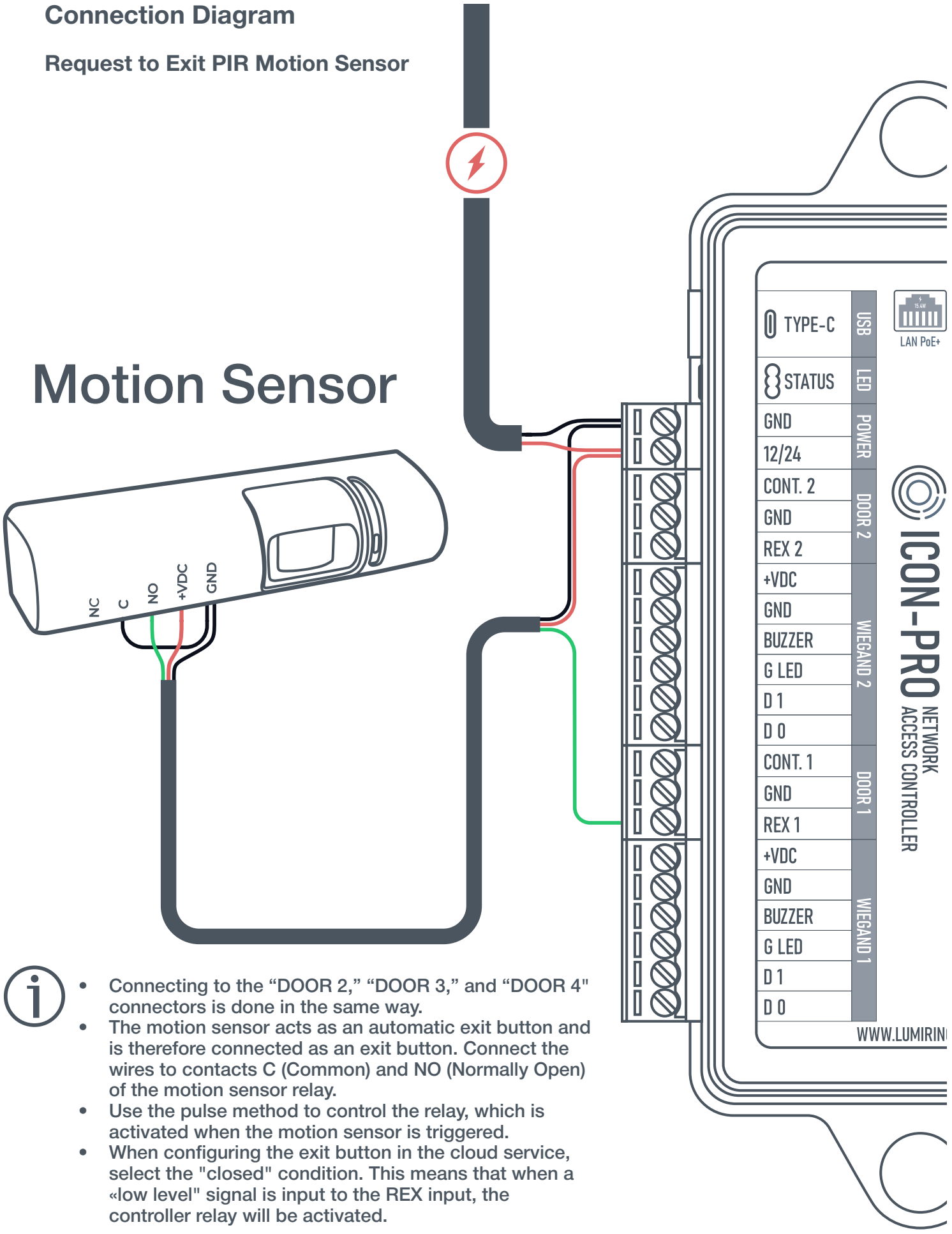
AIR-Button V 3.0



- 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

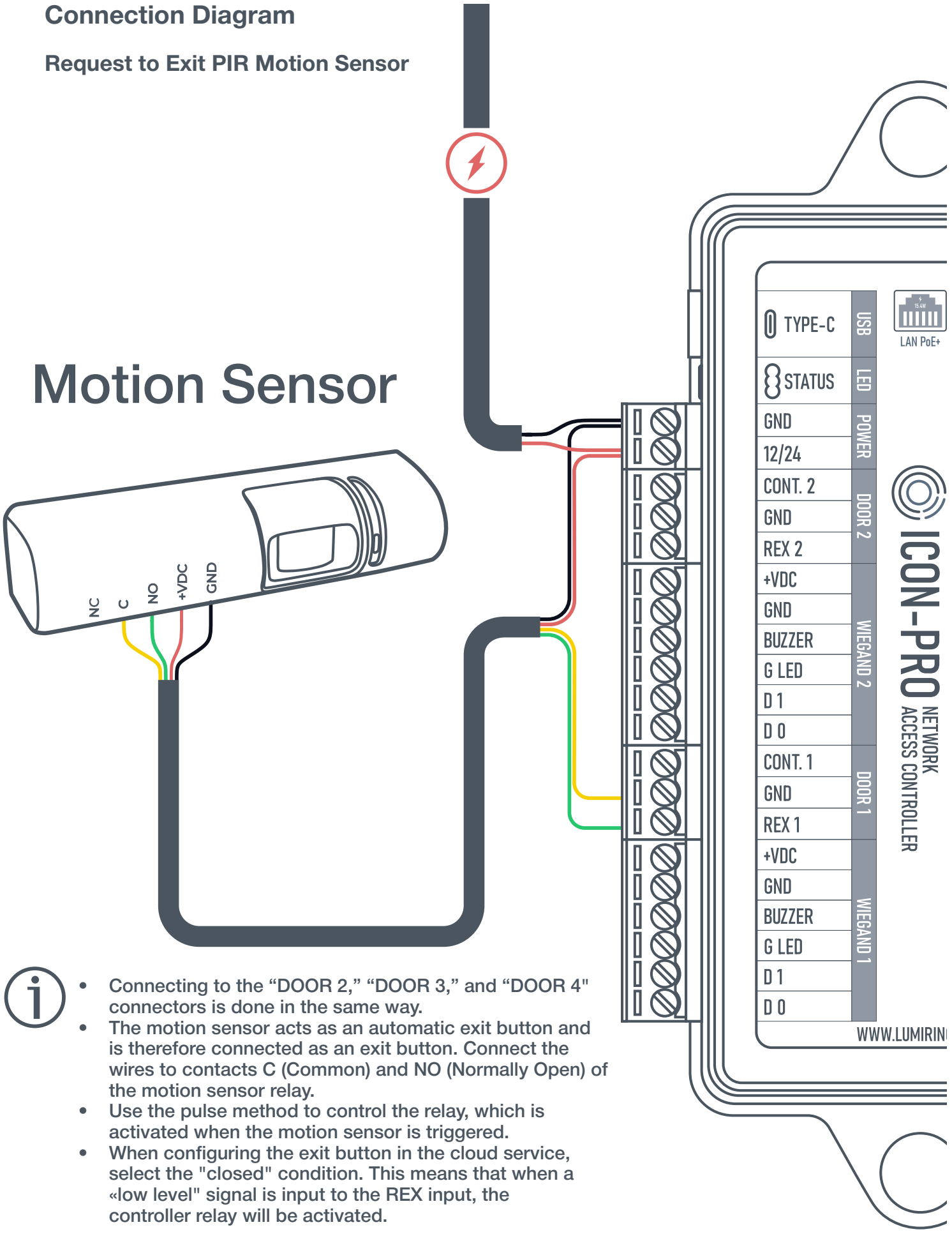
Request to Exit PIR Motion Sensor



- 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.

Connection Diagram

Request to Exit PIR Motion Sensor

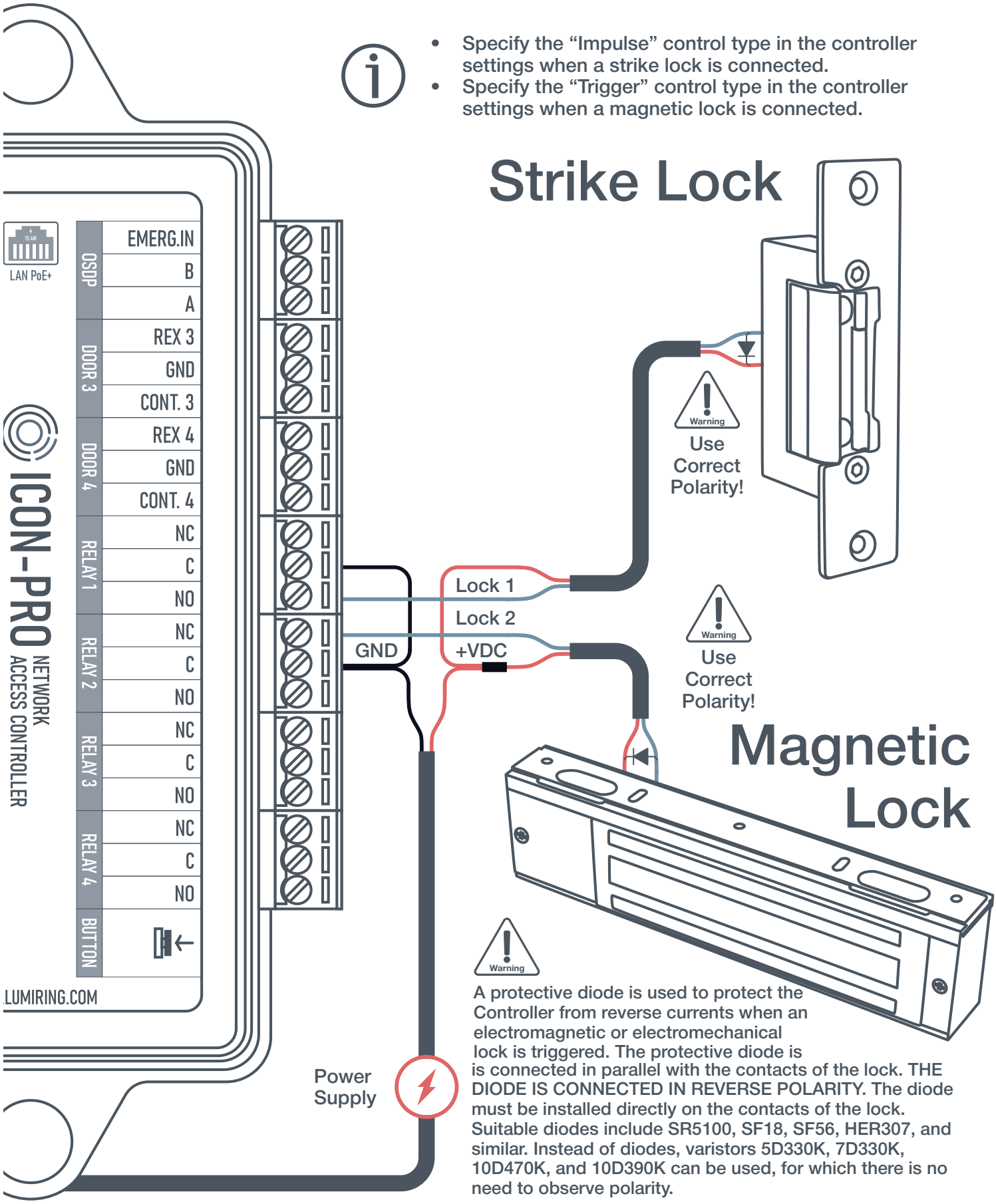


- Connecting to the “DOOR 2,” “DOOR 3,” and “DOOR 4" connectors is done in the same way.
- The motion sensor acts as an automatic exit button and is therefore connected as an exit button. Connect the wires to contacts C (Common) and NO (Normally Open) of the motion sensor relay.
- Use the pulse method 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.

Connection Diagram

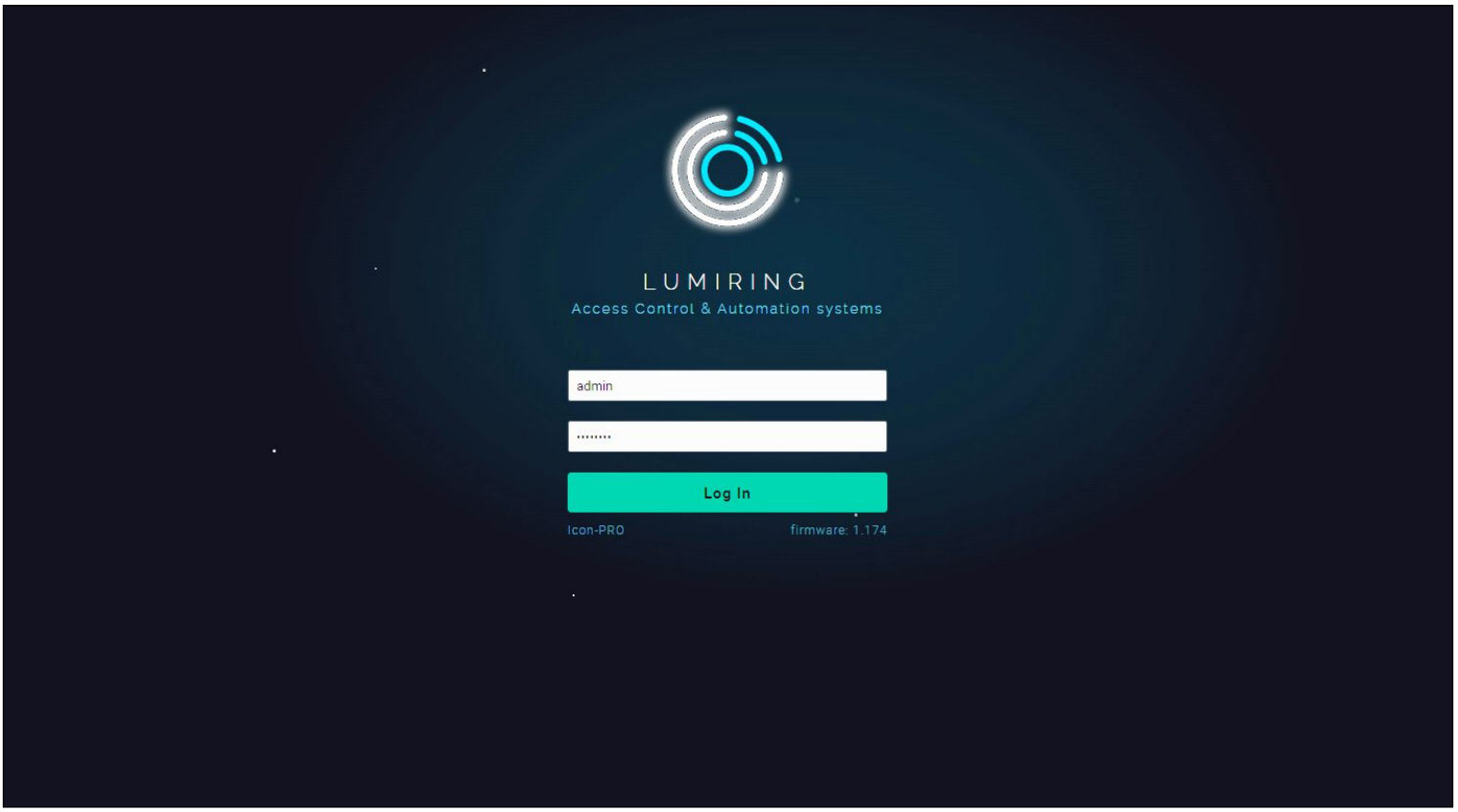
Electric Locks

- Specify the “Impulse” control type in the controller settings when a strike lock is connected.
- Specify the “Trigger” control type in the controller settings when a magnetic lock is connected.



A protective diode is used to protect the Controller from reverse currents when an electromagnetic or electromechanical lock is triggered. The protective diode is is connected in parallel with the contacts of the lock. THE DIODE IS CONNECTED IN REVERSE POLARITY. The diode must be installed directly on the contacts of the lock. Suitable diodes include SR5100, SF18, SF56, HER307, and similar. Instead of diodes, varistors 5D330K, 7D330K, 10D470K, and 10D390K can be used, for which there is no need to observe polarity.

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_xxxxxxxxx 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.

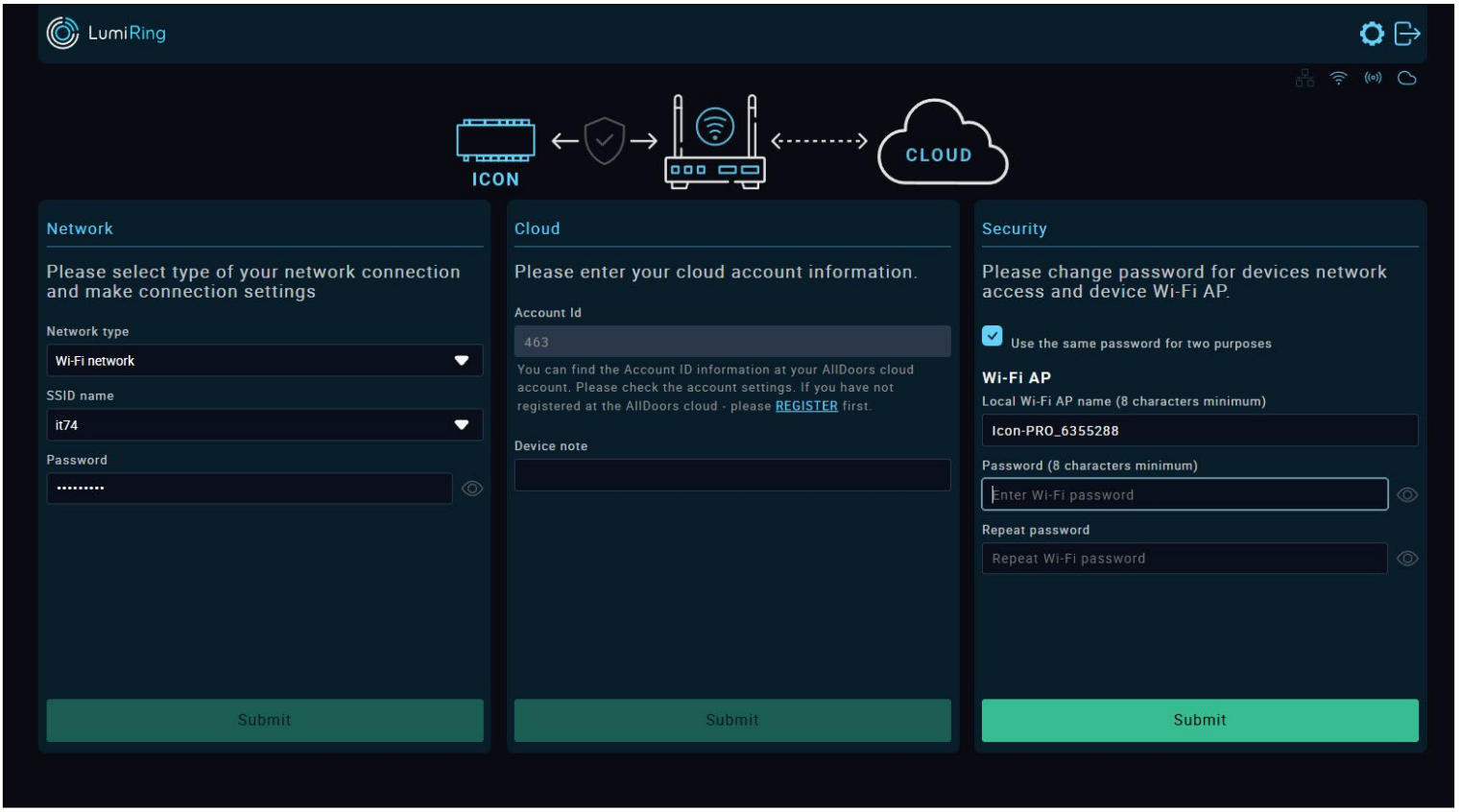
Step 1. Connect the Ethernet cable to the device using an adapter or by connecting the wires, as shown in the diagram below.

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 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:

To connect to the cloud, the controller only requires an active internet connection. The device will automatically establish the connection.

To add the device to your account, follow these steps:

- Create the AllDoors cloud account (alldoors.online)
- Go to the Devices section and use the Setup Wizard .
- Click the Add New button.
- Follow the instructions provided by the wizard.

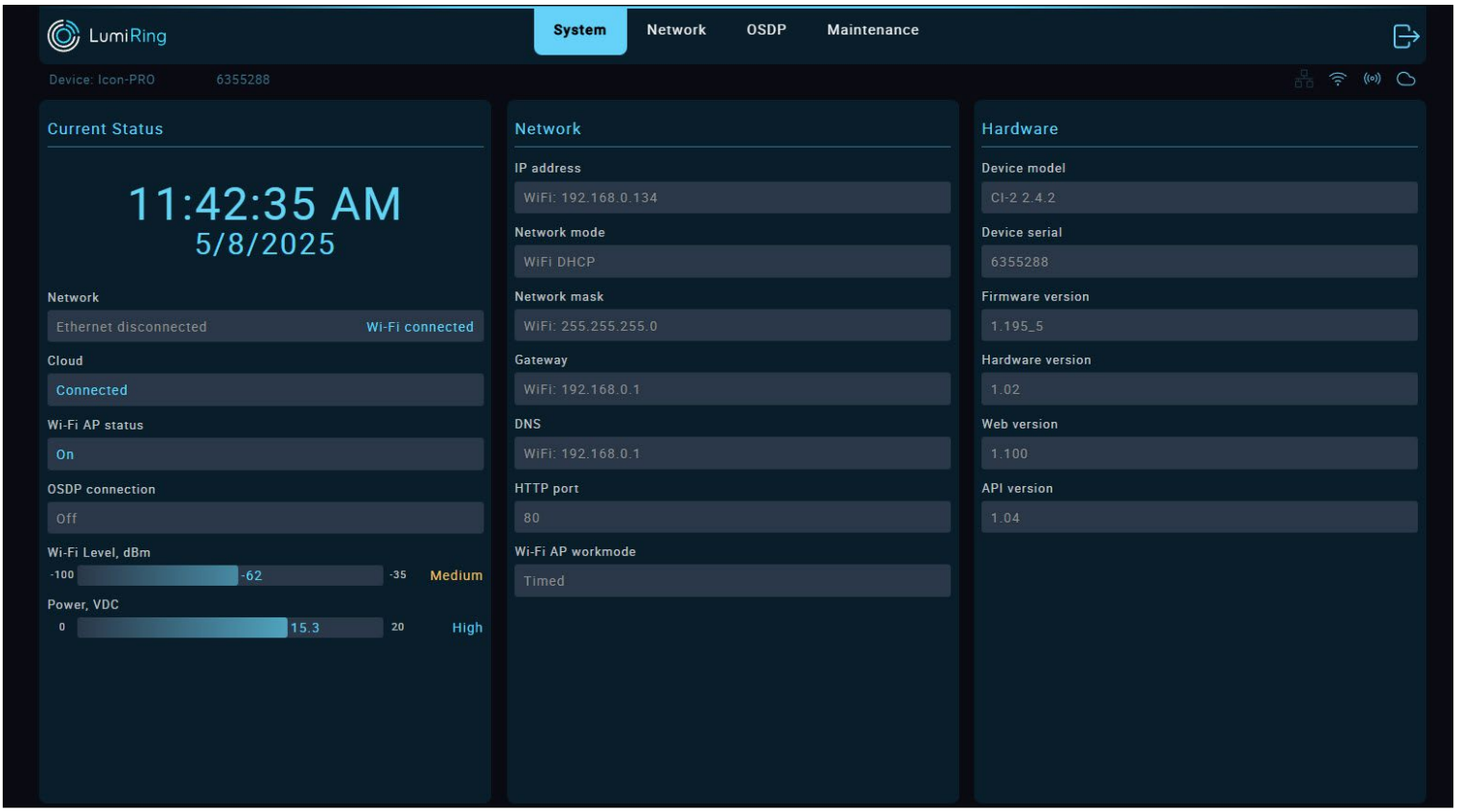
If you want to add controller directly to your account you must to enter your Cloud Account ID and click “Submit.”

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:

- 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.

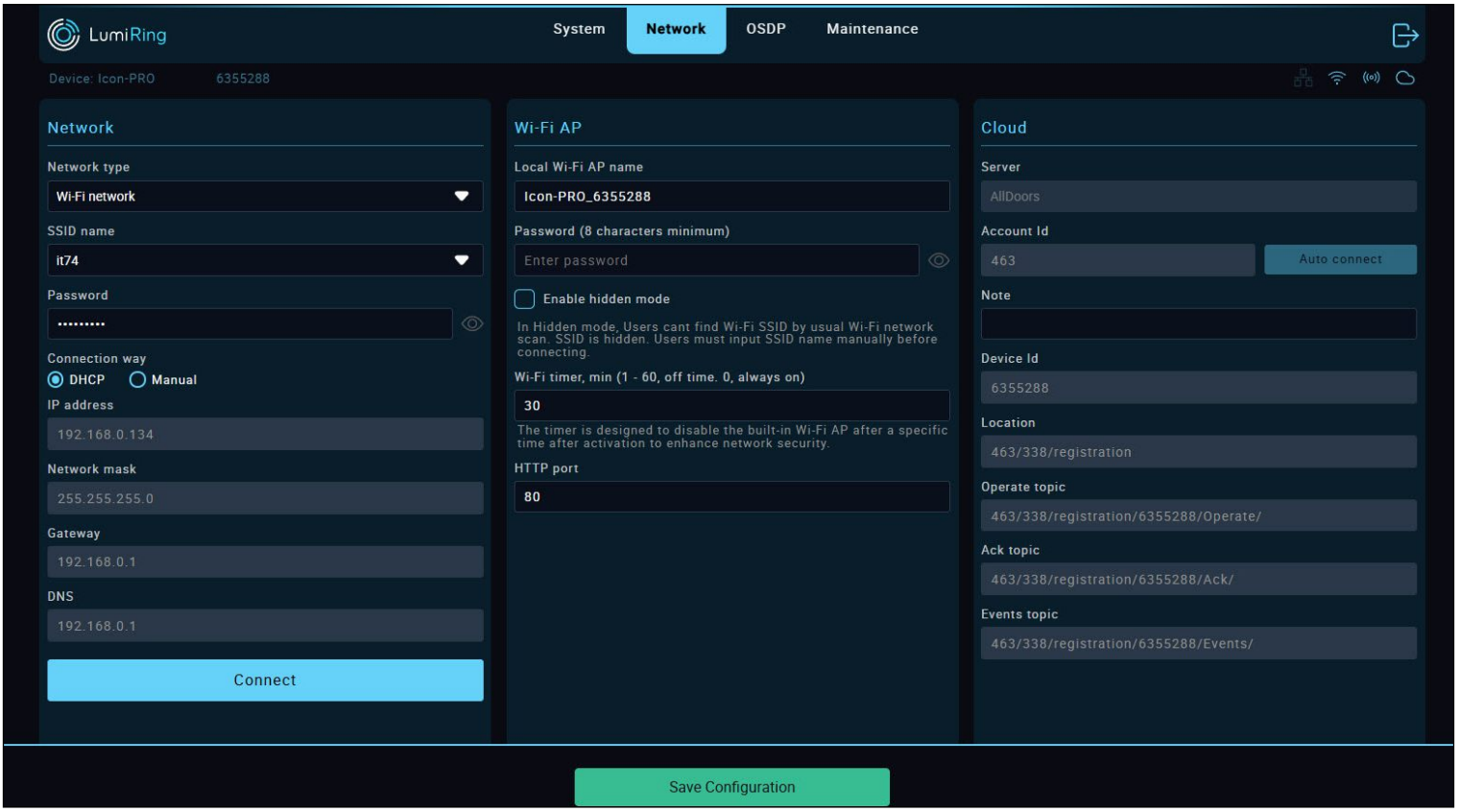
The Network Information subsection displays the:

- 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.

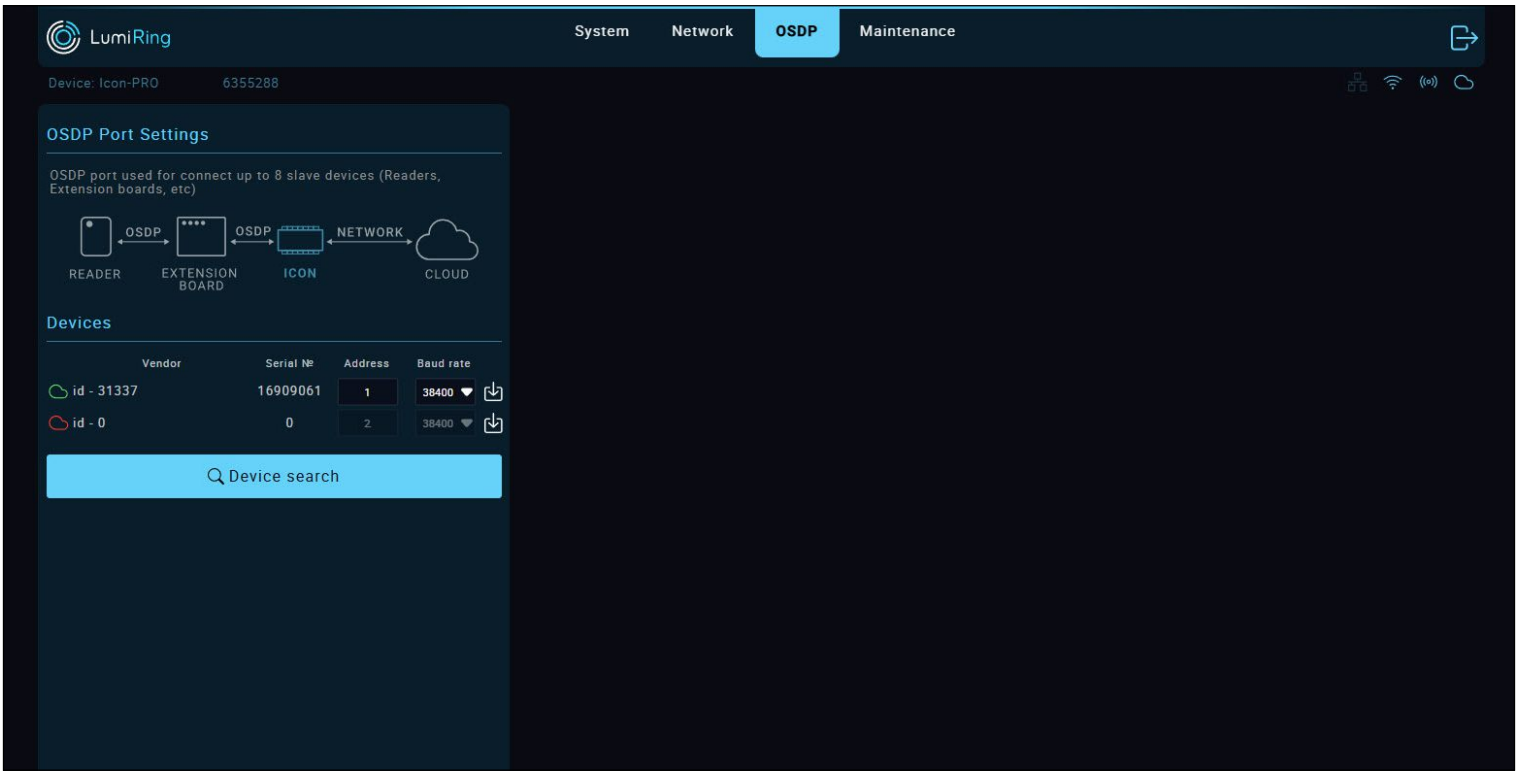
The Cloud settings subsection allows you to connect the Controller to a cloud server for later use.

- 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 AllDoors 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.

Important notes:

- "Address" of all OSDP devices must be unique, and the "Baud rate" must be the same.
- Only one OSDP device can be connected to the Controller during the search; otherwise, the device may not be detected.

Connection and Search

- Connect the OSDP device to the controller according to the wiring diagram on page 10. (example AIR-R reader connection)
- Press **“Search”** button. You will see the search results as a list of found devices on the OSDP bus. Using the controls you can change the device port speed and address.
  The functionality of changing these parameters can be blocked for in the settings of readers of different manufacturers.

  If the functionality is available, you can set the parameters you need and save them by pressing the button “ ”

Connecting multiple devices

If you are not sure about the settings of your OSDP devices and there is a need to connect more than one device, we recommend using the sequential method - connect each device in turn. Disconnect the previous device, which is already configured.

Example for three devices

- Connect the first device. Configure the port and address. Disconnect.
- Connect the Second device. Configure the port and address. Disconnect.
- Connect the Third device. Configure the port and address.
- Connect the First and Second devices
- Verify the connection by pressing **“Search”**

Cloud status indication

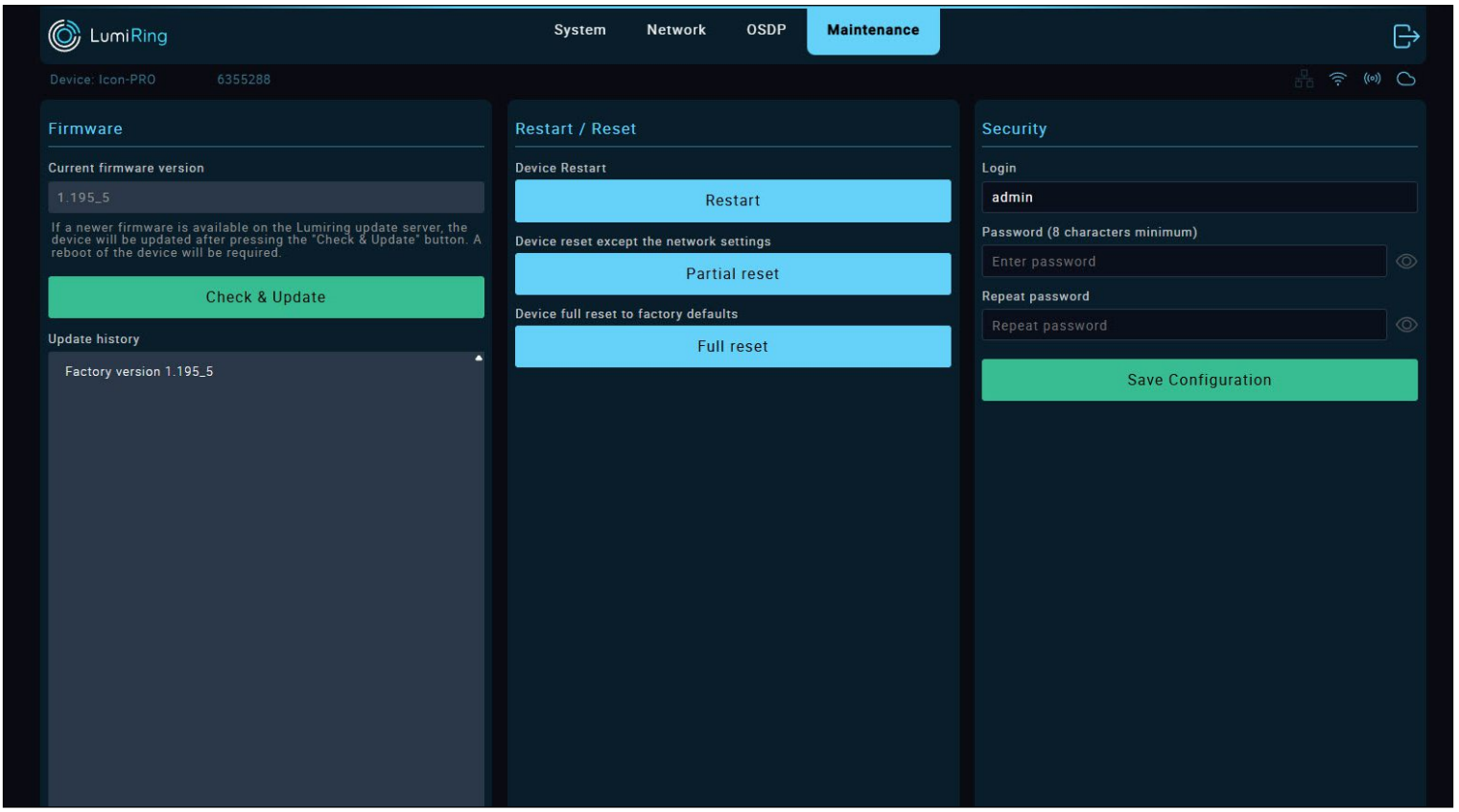
This functionality displays the status of OSDP settings in AllDoors cloud.

No icon - the OSDP device not configured in AllDoors

Red Cloud icon - the OSDP device configured in AllDoors but not connected to the controller

Green Cloud icon - the OSDP device is configured in AllDoors and connected to the conttroller

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.

Note: 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:

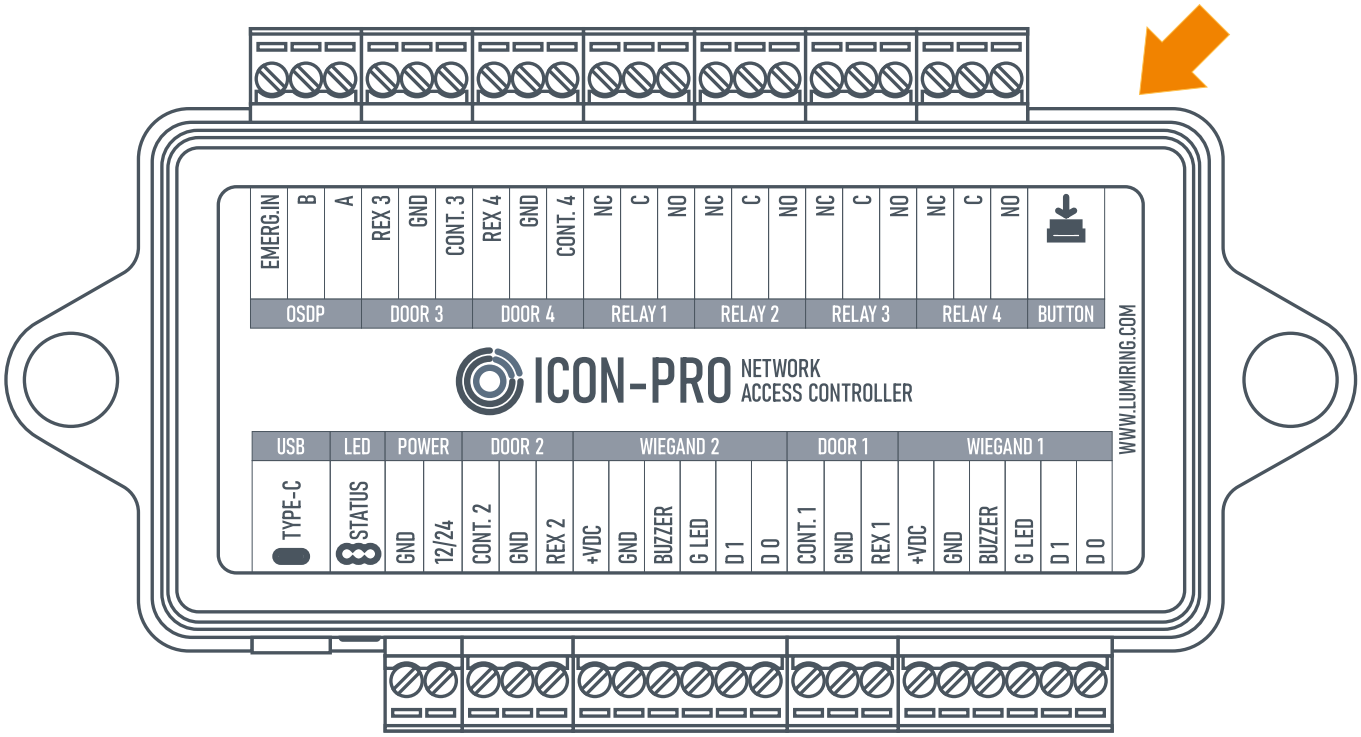
- Restart - restarts the device.
- Full reset - resets all settings of the device to factory defaults.

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.

Glossary

- **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.

FCC Caution

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

  RF warning for Mobile device: This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

For Notes

PROFESSIONAL / COMMERCIAL USE ONLY

This product is intended, marketed, and sold only for professional installation and commercial, industrial, institutional, or business access-control use. It is not intended, marketed, or sold as a consumer product. Any purchase or use confirms buyer is acting for commercial, professional, industrial, institutional, or business purposes.

SAFETY AND APPLICATION LIMITATIONS

This product is an access-control component. It is not a complete access-control system, life-safety device, fire alarm, emergency egress device, or UL 294-listed system unit.

Installation, system design, equipment selection, fail-safe/fail-secure configuration, code compliance, AHJ approval, and testing are the sole responsibility of installer/integrator/system designer.

This product must not be connected to critical entry, exit, barrier, elevator, gate, or emergency egress control as the sole release mechanism without alternate exit means and code approval.

WIRELESS PERFORMANCE

Wireless communication may be affected by RF interference, jamming, distance, obstacles, and site conditions. Range and performance are site-dependent and not guaranteed. Do not use as sole communication path for life-safety or emergency-egress functions.

CYBERSECURITY

Default credentials are for initial setup only and must be changed before deployment. Installer/operator is responsible for device security and credential management.

FIRMWARE UPDATES

Firmware updates may change device behavior. Complete system must be tested before return to service. Do not interrupt updates.

EXPORT CONTROL

This product may be subject to U.S. export control and sanctions laws. Export, re-export, transfer, or use contrary to applicable law is prohibited.

WARRANTY EXCLUSIONS

Warranty does not cover damage, malfunction, or performance issues caused by surge, lightning, water intrusion, incorrect voltage, reverse polarity, improper wiring, improper grounding, unauthorized modifications, abuse, misuse, failure to follow documentation, or use outside rated conditions.

This product is sold subject to New York law.

1. DOCUMENT PRECEDENCE

In any conflict between marketing materials and technical documentation, the current technical documentation prevails.

2. PRODUCT AUDIENCE AND BUYER RESPONSIBILITY

Lumiring products are professional access control devices for system integrators and technically proficient users. Buyer is responsible for verifying product suitability, functionality, compatibility, and compliance with requirements before purchase and deployment.

3. THIRD-PARTY INTEGRATION AND COMPONENTS

Integration with third-party platforms (Home Assistant, Node-RED, custom servers, etc.) requires buyer-side configuration via documented APIs. Compatibility with third-party readers, locks, controllers, and software depends on third-party manufacturer implementation and is buyer responsibility to verify. Lumiring is not responsible for third-party product compatibility, changes, or functionality.

4. RETURNS AND RMA PROCESS

Returns require prior RMA authorization from Lumiring and must be initiated within the period stated on the invoice or applicable warranty terms. Lumiring may require reasonable troubleshooting before issuing an RMA.

An RMA or accepted return does not mean warranty coverage, refund, or replacement approval. Buyer pays return shipping, duties, fees, taxes, and insurance unless Lumiring agrees otherwise in writing. Products must be returned in reasonable condition with applicable accessories unless Lumiring authorizes otherwise.

5. INTERNATIONAL SALES

For sales outside the United States, buyer is responsible for all customs duties, import taxes, VAT, brokerage fees, and compliance with local import/export regulations. Lumiring does not reimburse duties, taxes, shipping or fees paid by buyer.

6. WARRANTY AND LIMITATION OF LIABILITY

Complete warranty terms, return process, exclusions, and liability limitations are subject to Lumiring Inc Terms And Conditions, Limited Warranty, Limited Liability, and Limited License.

To the maximum extent permitted by law, Lumiring is not liable for loss of use, business interruption, lost revenue, lockout, security breach, loss of data, labor, removal/reinstallation costs, or consequential, incidental, indirect, special, or punitive damages. Maximum liability is limited to amount paid for the affected product.

7. GOVERNING TERMS

This product is sold subject to Lumiring Inc Terms and Conditions, Limited Warranty, Limited Liability, and Limited License, and governed by New York law.