

MANUAL



ICON CONTROLLER

CONTENTS

• Introduction	3
• Default Device Settings	3
• Device Specifications	4
• Device Dimensions	5
• ICON Device Connection Terminals	6
• Installation Recommendations	7
• Wiegand Reader (Connection Diagram)	9
• Open Supervised Device Protocol Reader (Connection Diagram) Coming soon!	11
• Exit Button and Door Sensor (Connection Diagram)	13
• AIR-B v 2.1 Four Wire (Connection Diagram)	14
• AIR-B v 3.1 Five Wire (Connection Diagram)	15
• Request to Exit PIR Motion Sensor (Connection Diagram)	16
• Electric Locks [Power +12 VDC] (Connection Diagrams)	18
• Electric Locks [Power over Ethernet] [Wet Mode] (Connection Diagrams)	21
• Electric Locks [Power over Ethernet] [Dry Mode] (Connection Diagrams)	24
• Connecting to Device	26
• Login	26
• Quick Start	27
• System	28
• Network	29
• Open Supervised Device Protocol (OSDP) OSDP is coming soon!	31
• Maintenance	32
• Hardware Reset With a Jumper	33
• Glossary	34
• For Notes	36
• Safety and Legal Notice	37
• Appendix: Important Notices	38

INTRODUCTION

This document provides detailed information on the ICON 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 in the event of any discrepancies, the actual product takes precedence.

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.

SPECIFICATIONS

Voltage:

- 12 or 24 VDC operation
- The voltage at the outputs is determined by the power supply.
- 0.15A @12 VDC, 0.075A @ 24 VDC current consumption
- POE 802.3af (15.4W)
- Total output current when powered by POE 1A @ 11.5 VDC

Outputs:

- One (1) Form "C" relay output for 1.5A (dry mode) or 0.5A @ 12VDC (wet mode)
- One (1) outputs (open collector) 0.5A @ 12 VDC

Inputs:

- Four (4) 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

Memory storage:

- 100,000 cards

- 250,000 events

Demensions (L x W x H):

- 4.39" x 2.95 x 1.38" (111.5 x 75 x 35 mm) excluding antenna

Mounting method:

- Wall mount/Din rail mount (option)

Weight:

- 4.84 oz (137 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

Ingress protection rating:

- IP 20

DEFAULT SETTINGS

Wi-Fi device name when searching:

- ICON_(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

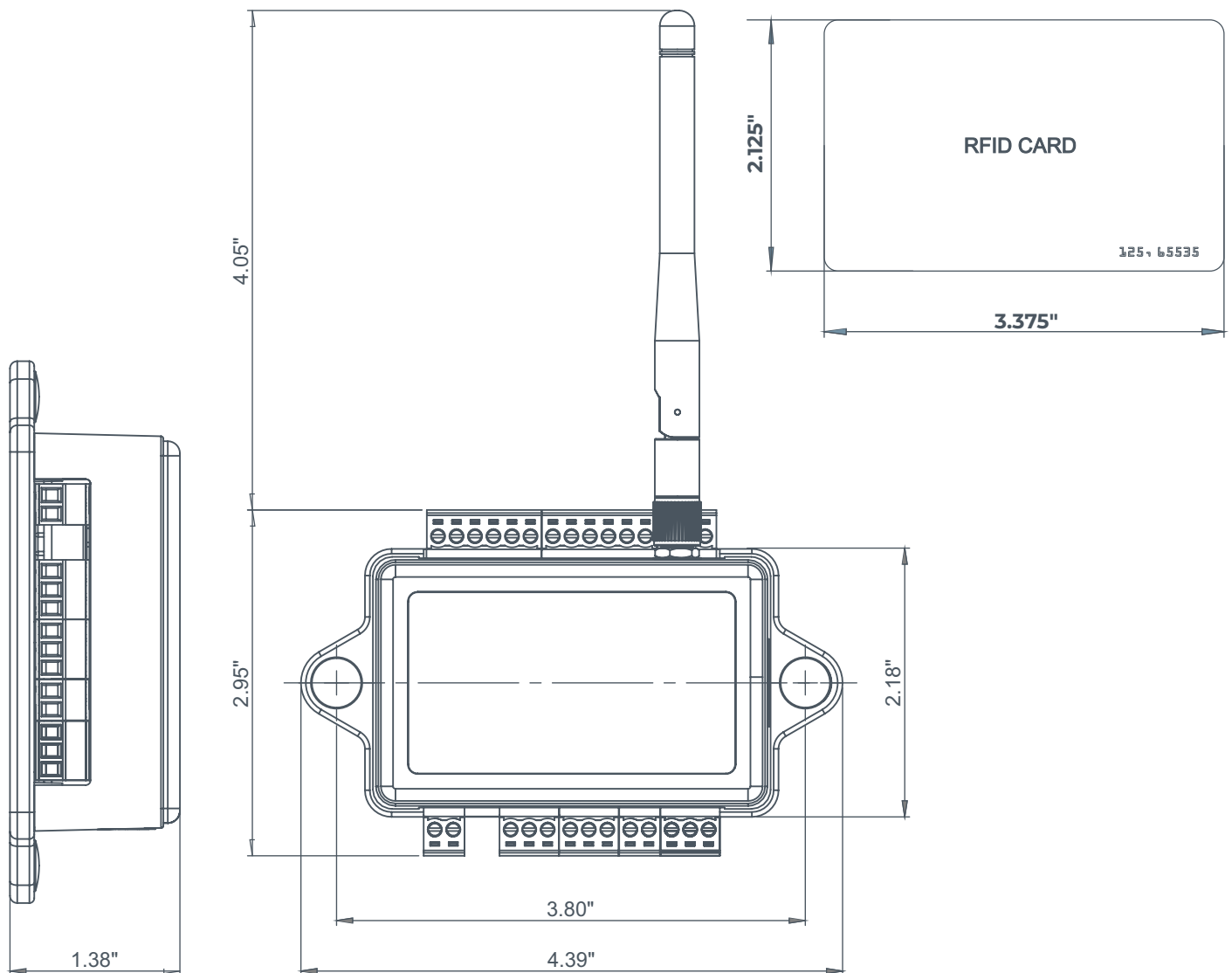
Web page password:

- admin123

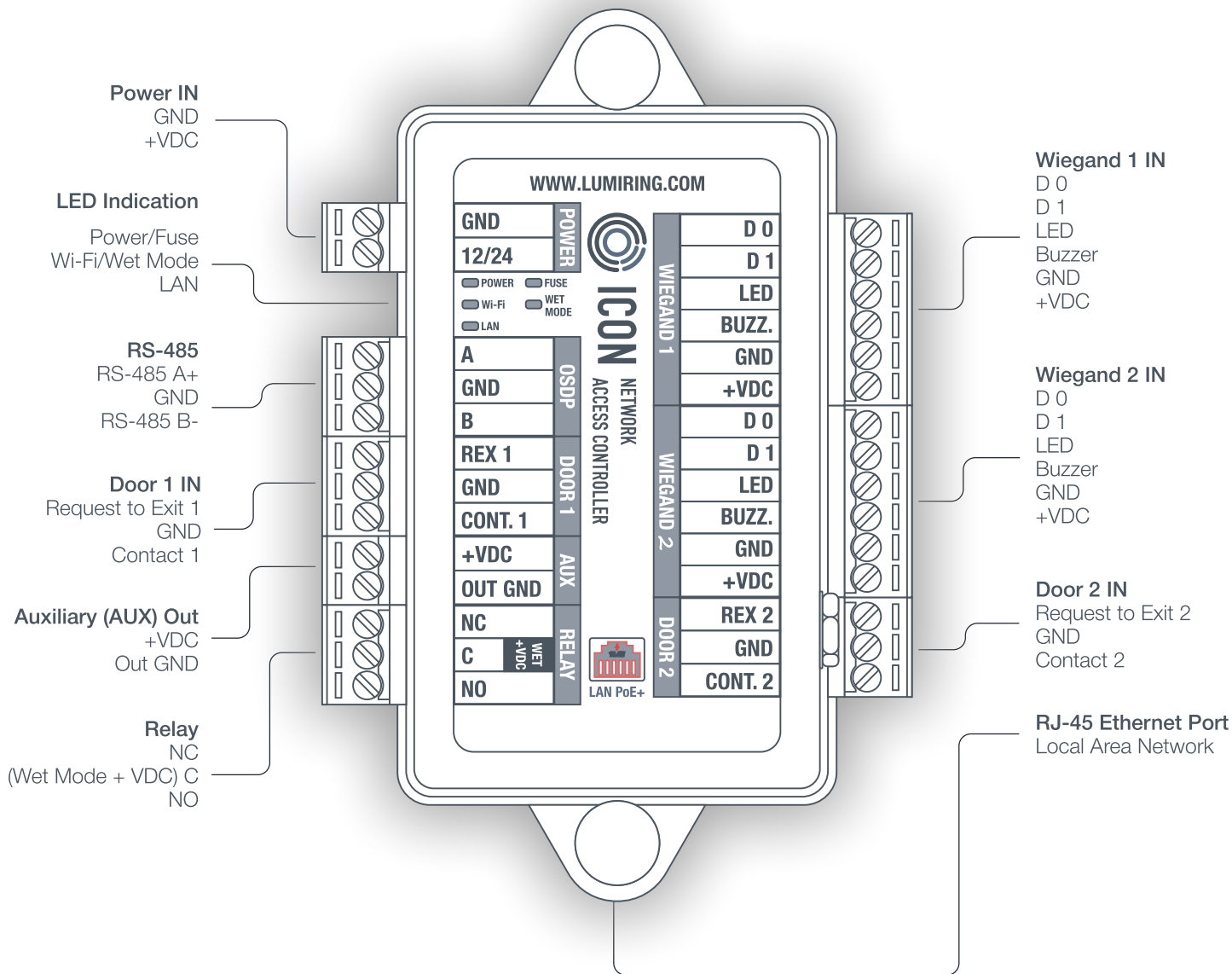
AP Wi-Fi timer:

- 30 minutes

DIMENSIONS



CONNECTIONS



The manufacturer reserves the right to modify the external pin assignments and their placement, as well as the appearance of the device without prior notice.

These changes may be made to improve functionality or ergonomics, or to comply with technical requirements and standards.

Users are advised to consult the latest versions of technical documentation and instructions before using the device.

RECOMMENDATION

Placement and Wiring

Place controllers as close as possible to Wi-Fi APs to minimize latency.

Check the Wi-Fi signal strength after installation, and make sure the minimum allowable signal level is -75 dB. If the signal strength is lower, move the AP closer to the device, or use a stronger antenna on the AP or device. Avoid placing the device on metal surfaces, as this may reduce the quality of the Wi-Fi connections.

Connecting Power to the Device

Make all connections only when the power is off. Use a power cable with a suitable cross-section to supply the current consumption of the connected devices. Make sure to use two separate power supplies for the controller and the actuators.

Wiegand Connection

Use the same interface to connect the readers to avoid differences in card code reading and subsequent confusion in the system.

The Wiegand communication line length should not exceed 328 ft (100 m).

If the communication line is longer than 16.4 ft (5 m), use a UTP Cat 5E cable. The line should be less than 1.64 ft (0.5 m) away from power cables.

Connecting OSDP

The OSDP uses an RS-485 interface that is designed for long-distance communications. It operates at ranges up to 3,280 ft (1,000 m) with good resistance to noise interference.

The OSDP communication line should be laid as far away as possible from power cables and electric lights. A UTP Cat 5E or FTP Cat 5E twisted pair cable should be used as the OSDP communication line (if possible, ground the shield at one end). To ensure reliable system operations, it is best to use one power source for the controllers and a separate one for the actuators.

The power supply line wires for the reader should be kept as short as possible to avoid a significant voltage drop across them. After cabling, ensure that the power supply voltage to the reader is at least 12 VDC with the locks switched on.

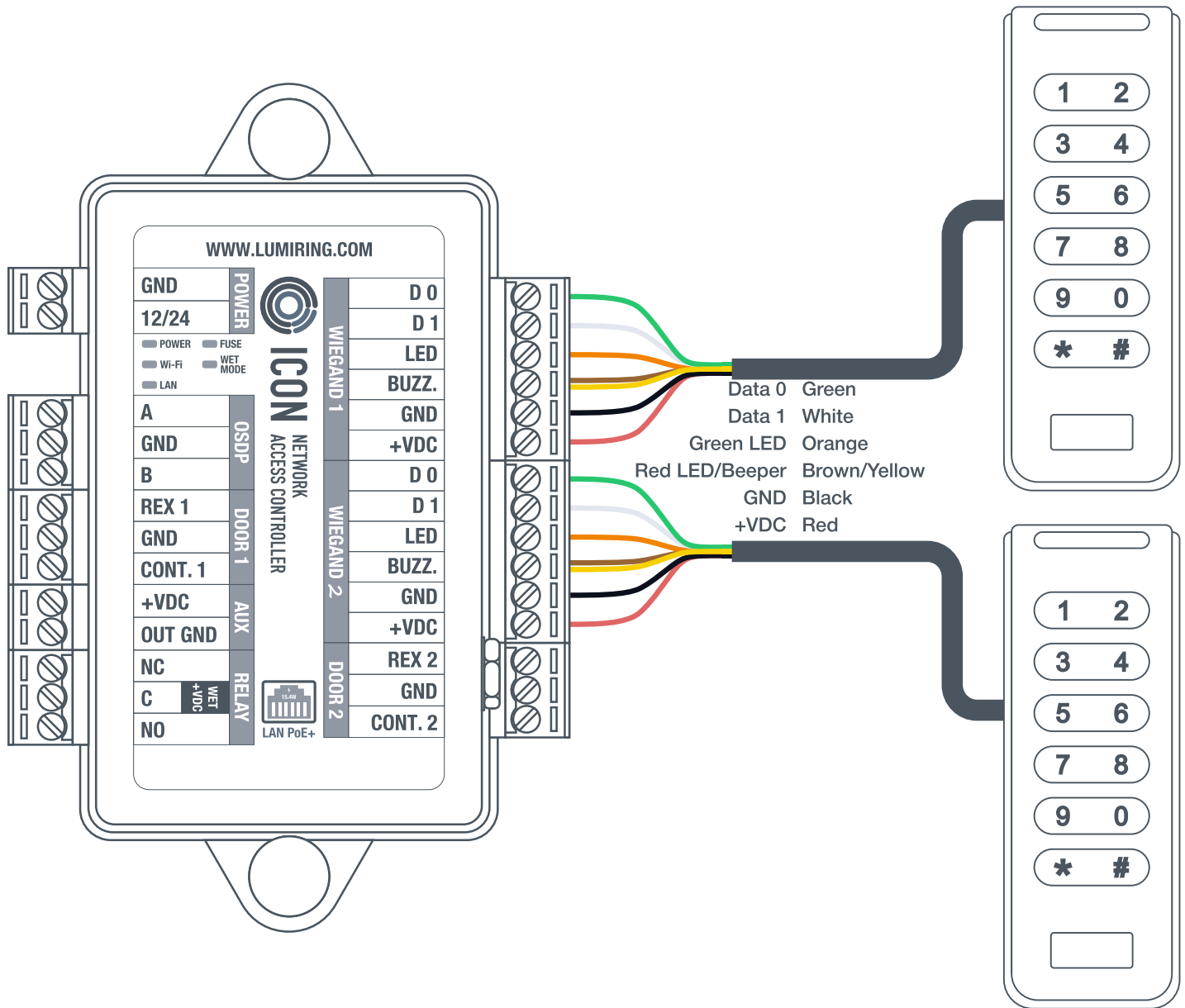
Connecting Electric Locks

Connect devices via relays if galvanic isolation from the device to be controlled is needed, or if you need to control high-voltage devices or devices with significant current consumption. Use a protection diode or varistor when using electromagnetic or electromechanical locks.

CONNECTION DIAGRAM

WIEGAND READER

HID Signo Keypad Reader 20K



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.

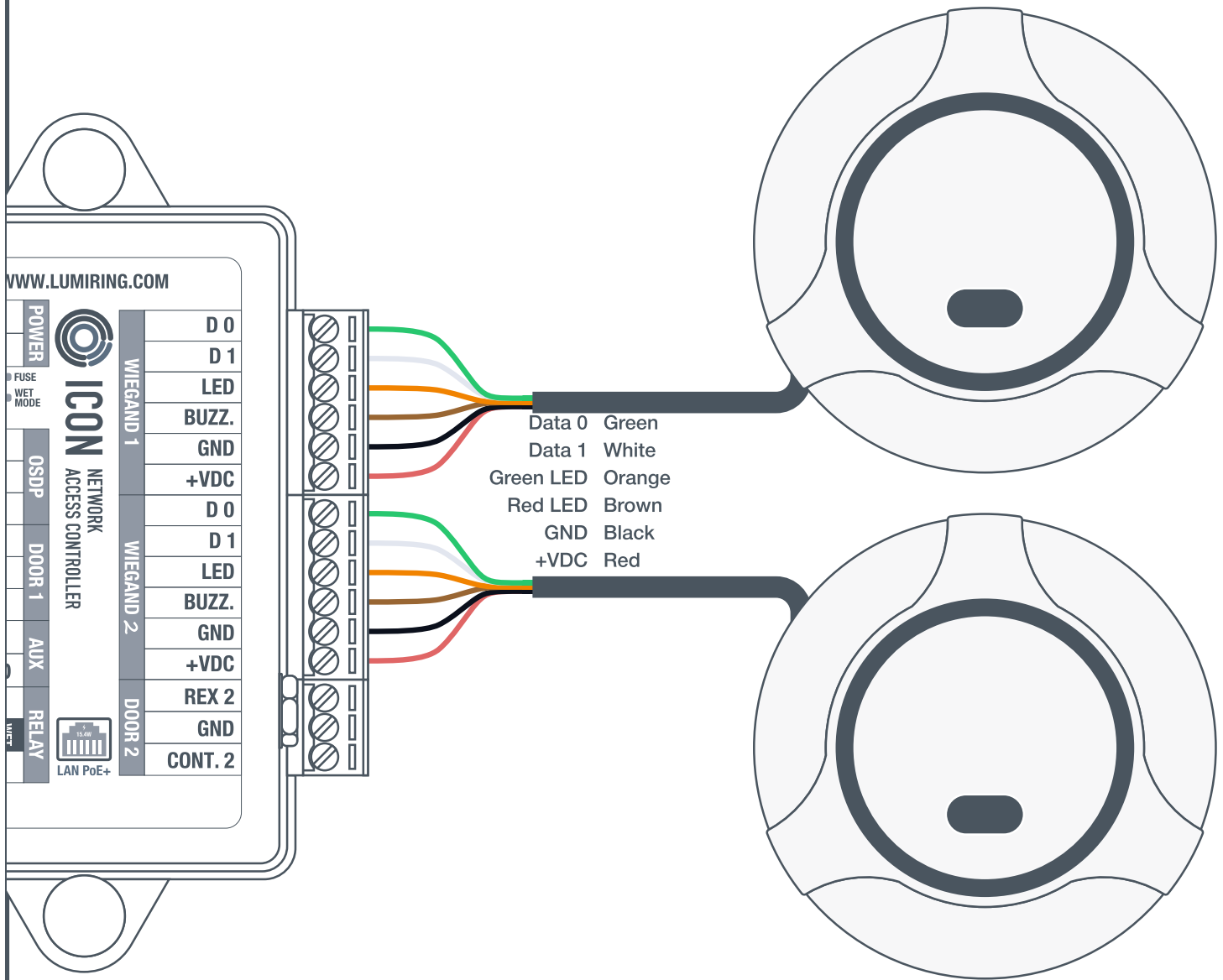


Before you start building cable networks for Wiegand readers, read the interface specifications.

CONNECTION DIAGRAM

WIEGAND READER

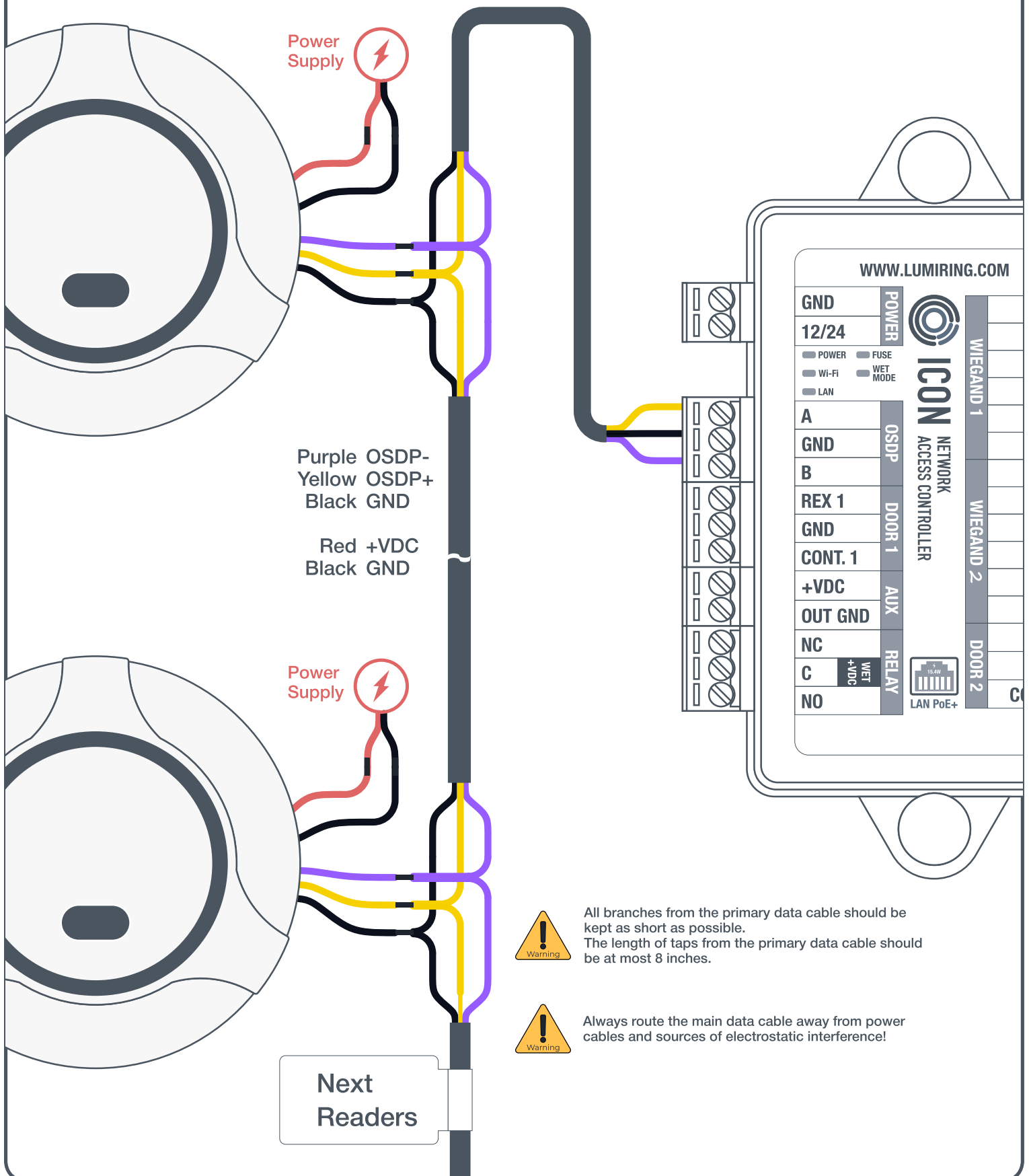
Lumiring AIR-R Reader



Before you start building cable networks for Wiegand readers, read the interface specifications.

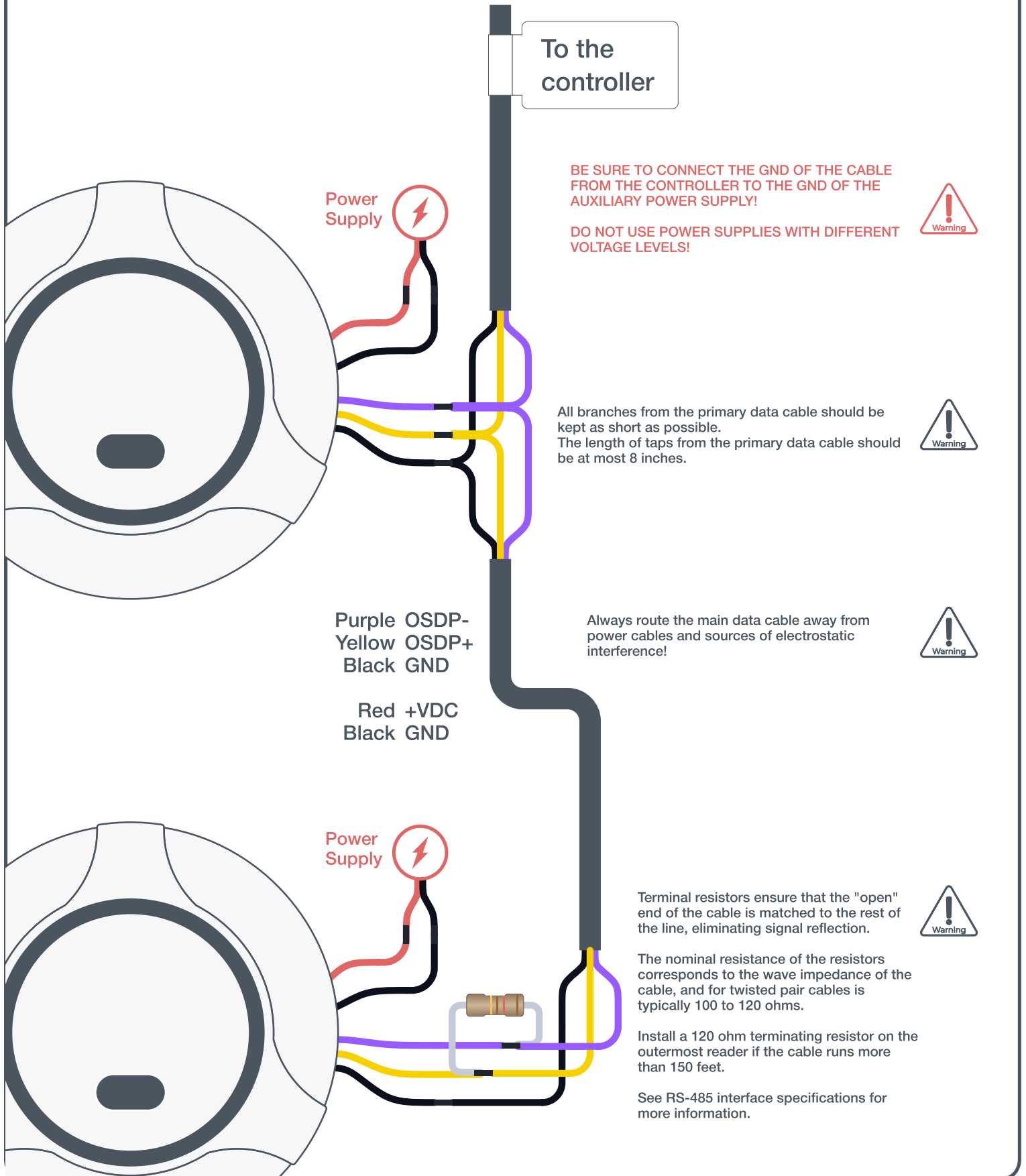
CONNECTION DIAGRAM

OSDP Reader



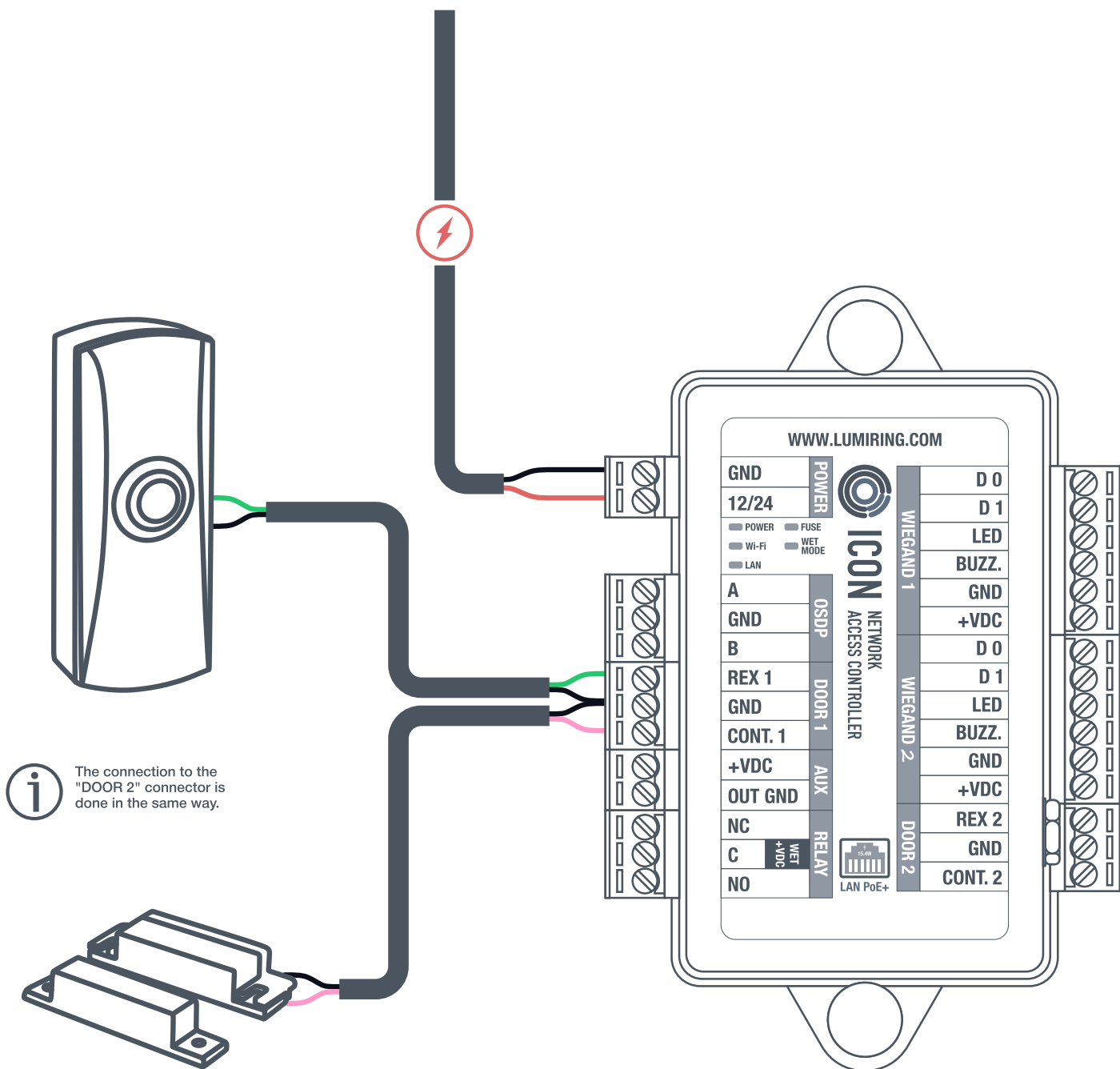
CONNECTION DIAGRAM

OSDP Reader



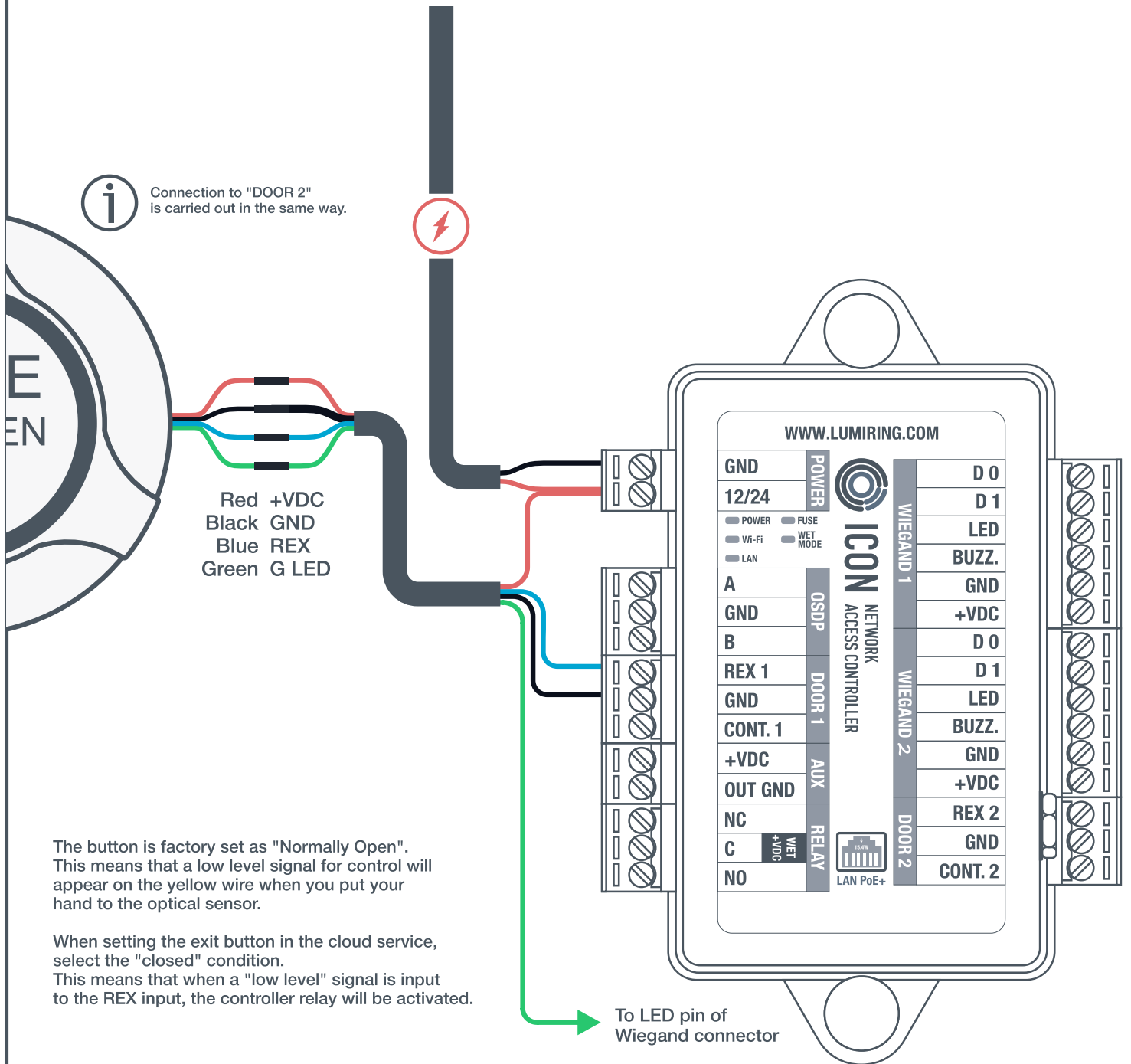
CONNECTION DIAGRAM

Exit Button and Door sensor



CONNECTION DIAGRAM

AIR-B v 2.1 Four Wire

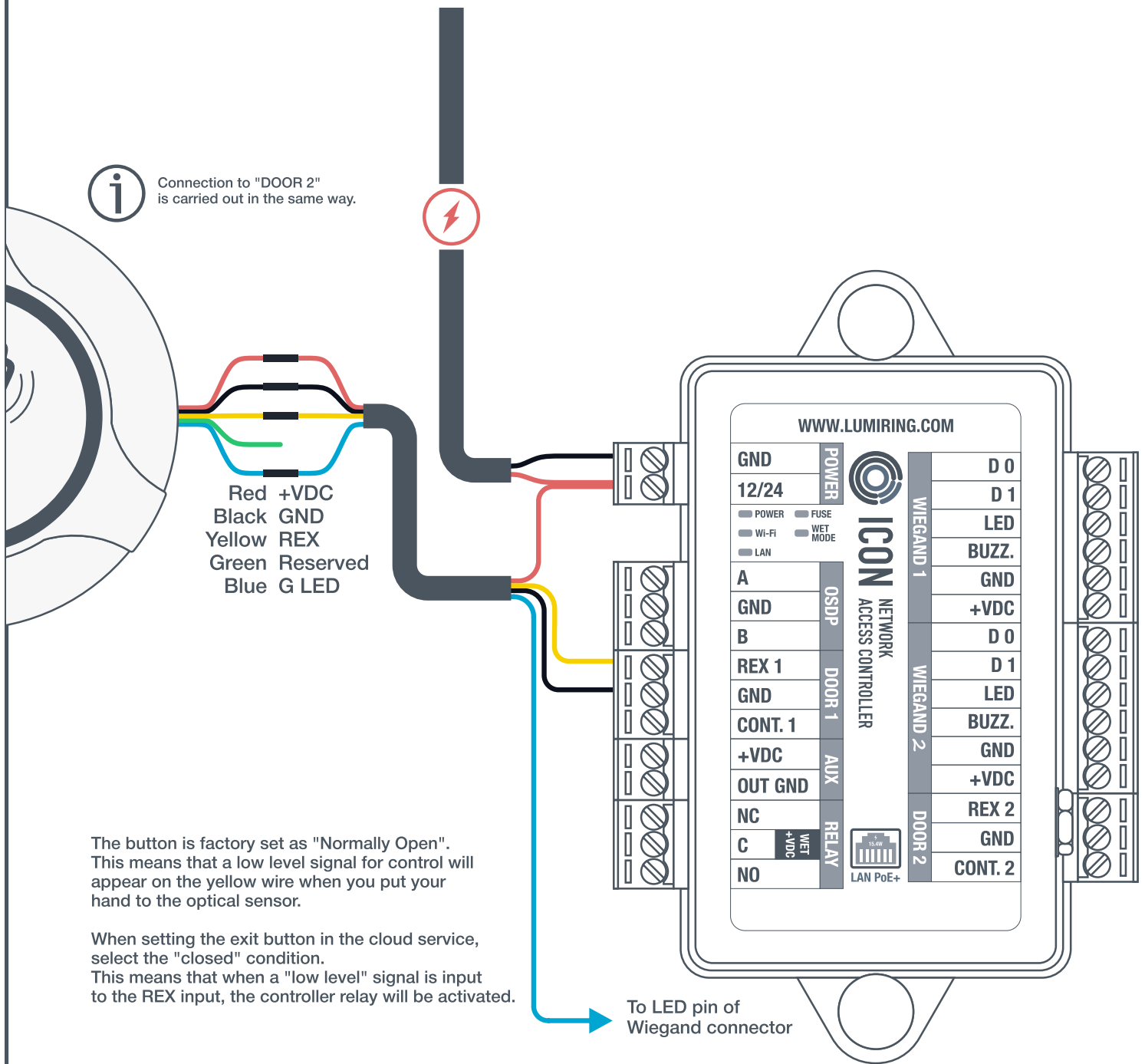


CONNECTION DIAGRAM

AIR-B v 3.1 Five Wire

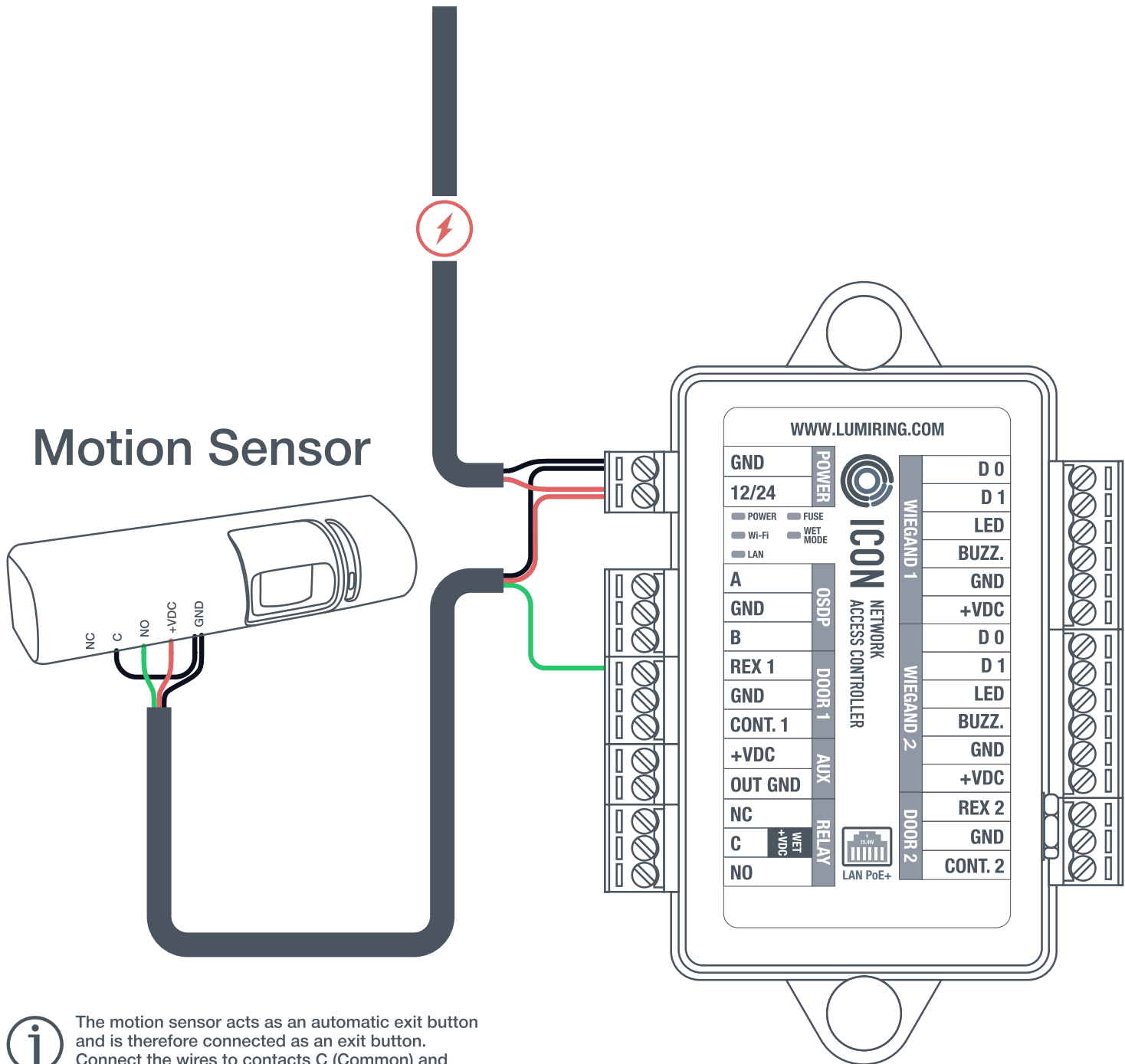


Connection to "DOOR 2" is carried out in the same way.



CONNECTION DIAGRAM

Request to Exit PIR Motion Sensor

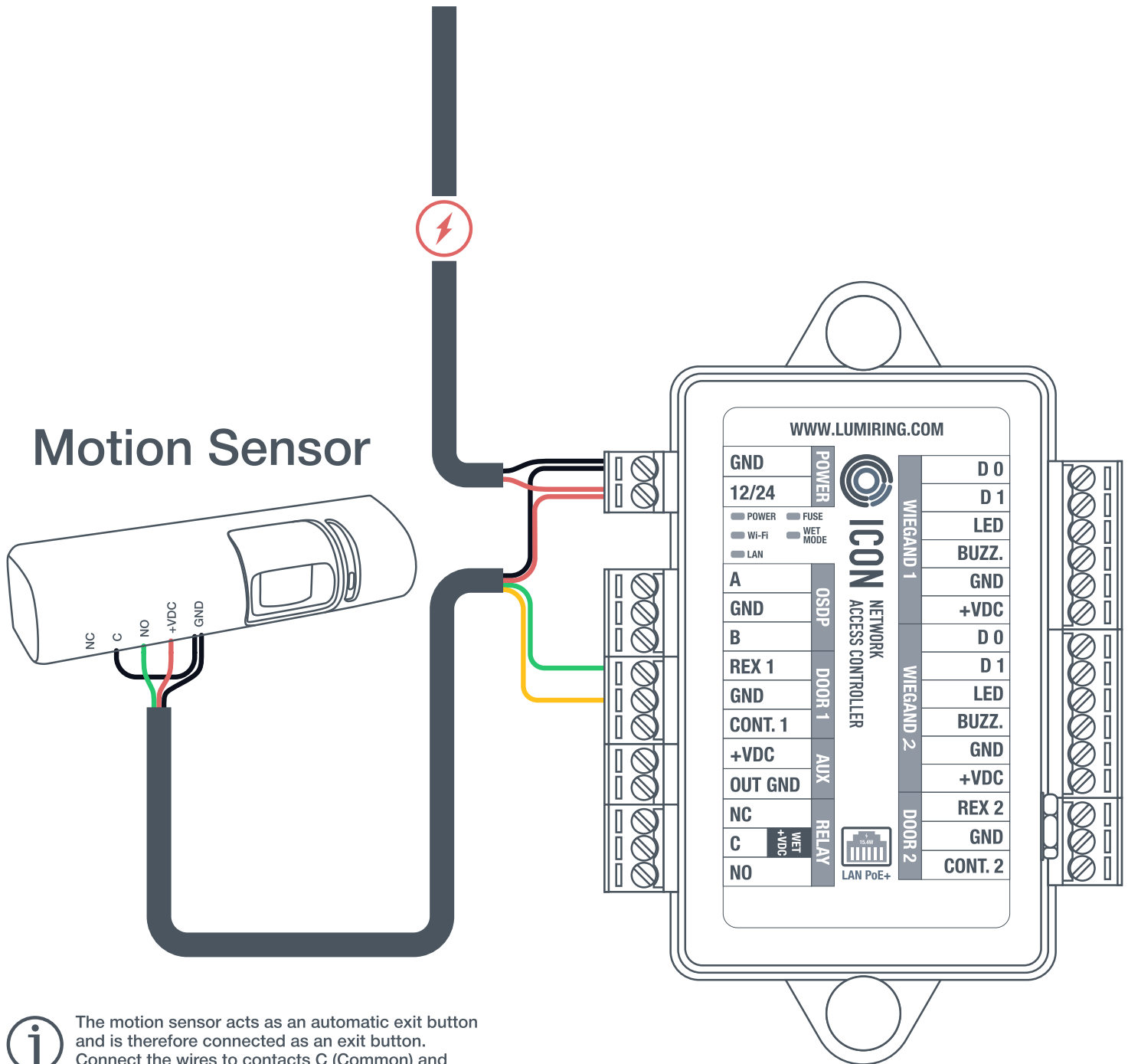


The motion sensor acts as an automatic exit button and is therefore connected as an exit button. Connect the wires to contacts C (Common) and NO (Normally Open) of the motion sensor relay. Use the pulse method to control the relay, which is activated when the motion sensor is triggered.

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



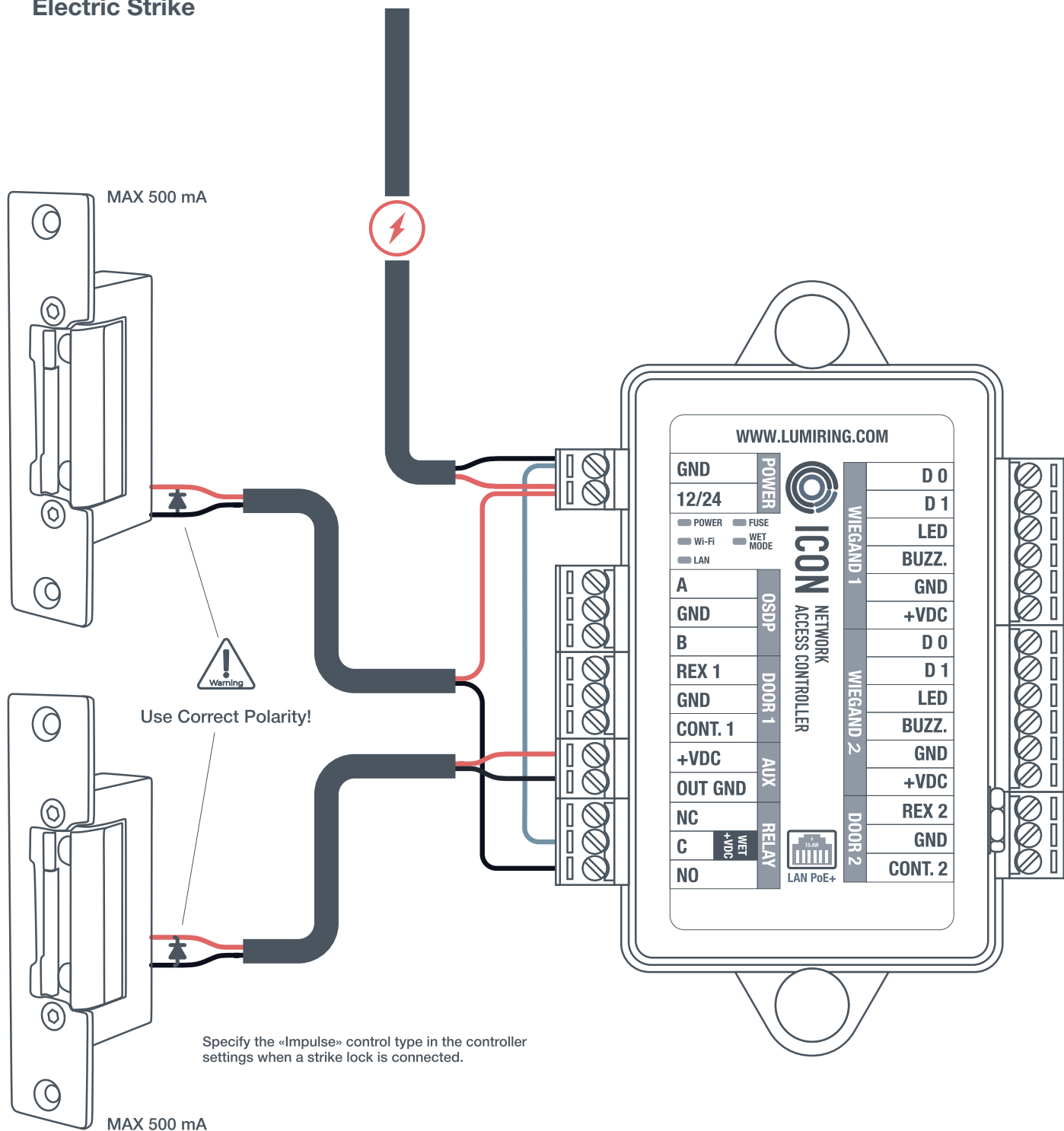
The motion sensor acts as an automatic exit button and is therefore connected as an exit button. Connect the wires to contacts C (Common) and NO (Normally Open) of the motion sensor relay. Use the pulse method to control the relay, which is activated when the motion sensor is triggered.

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 [Power +12 VDC]

Electric Strike

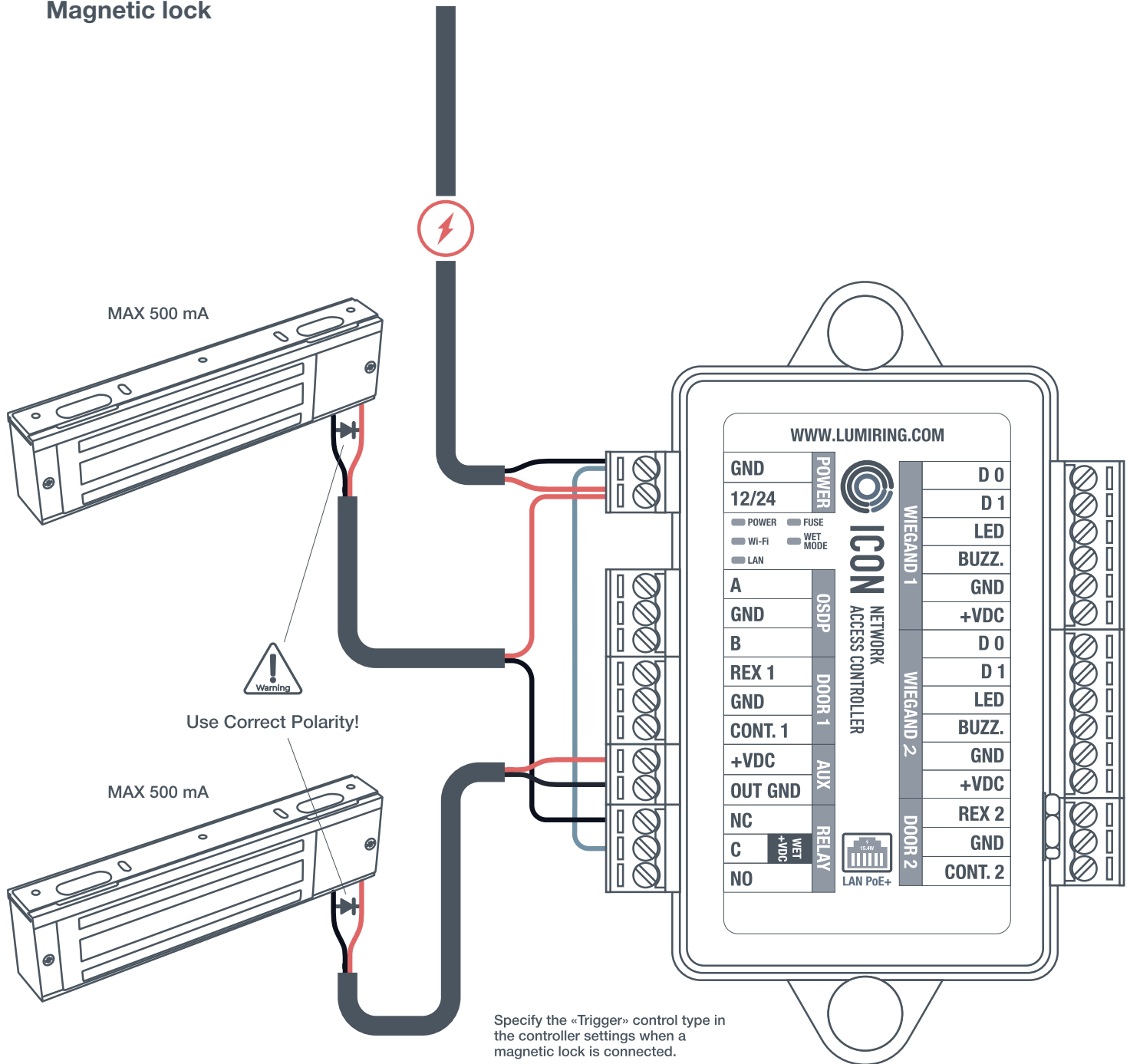


A protective diode is used to protect the controller from reverse currents when an electromagnetic or electromechanical lock is triggered. The protective diode is connected in parallel with the contacts of the lock. **THE DIODE IS CONNECTED IN REVERSE POLARITY.** The diode must be installed directly 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.

CONNECTION DIAGRAM

Electric Locks [Power +12 VDC]

Magnetic lock

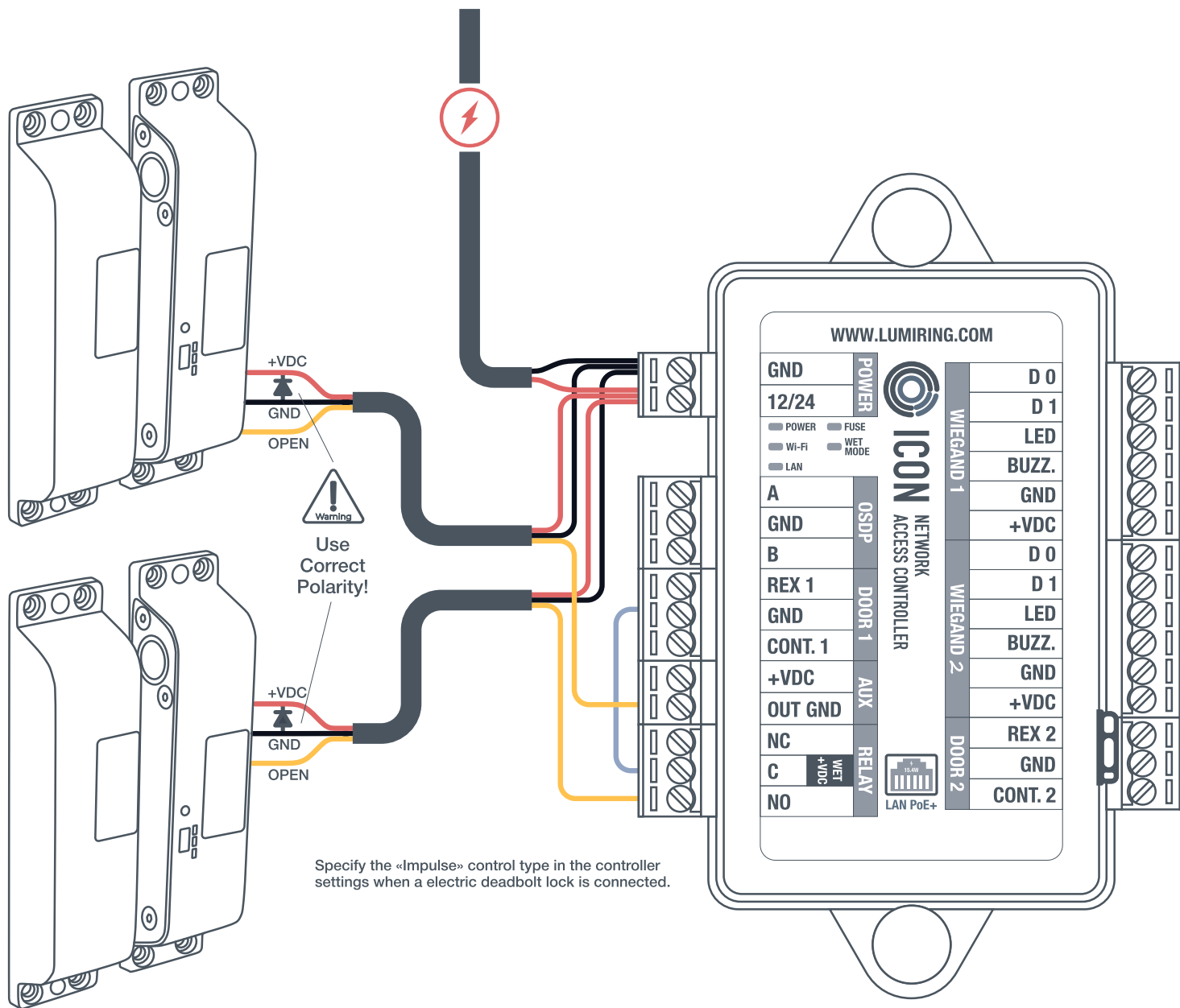


A protective diode is used to protect the controller from reverse currents when an electromagnetic or electromechanical lock is triggered. The protective diode is connected in parallel with the contacts of the lock. **THE DIODE IS CONNECTED IN REVERSE POLARITY.** The diode must be installed directly 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.

CONNECTION DIAGRAM

Electric Locks [Power +12 VDC]

Electric Deadbolt Lock with External Control



A protective diode is used to protect the controller from reverse currents when an electromagnetic or electromechanical lock is triggered. The protective diode 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.

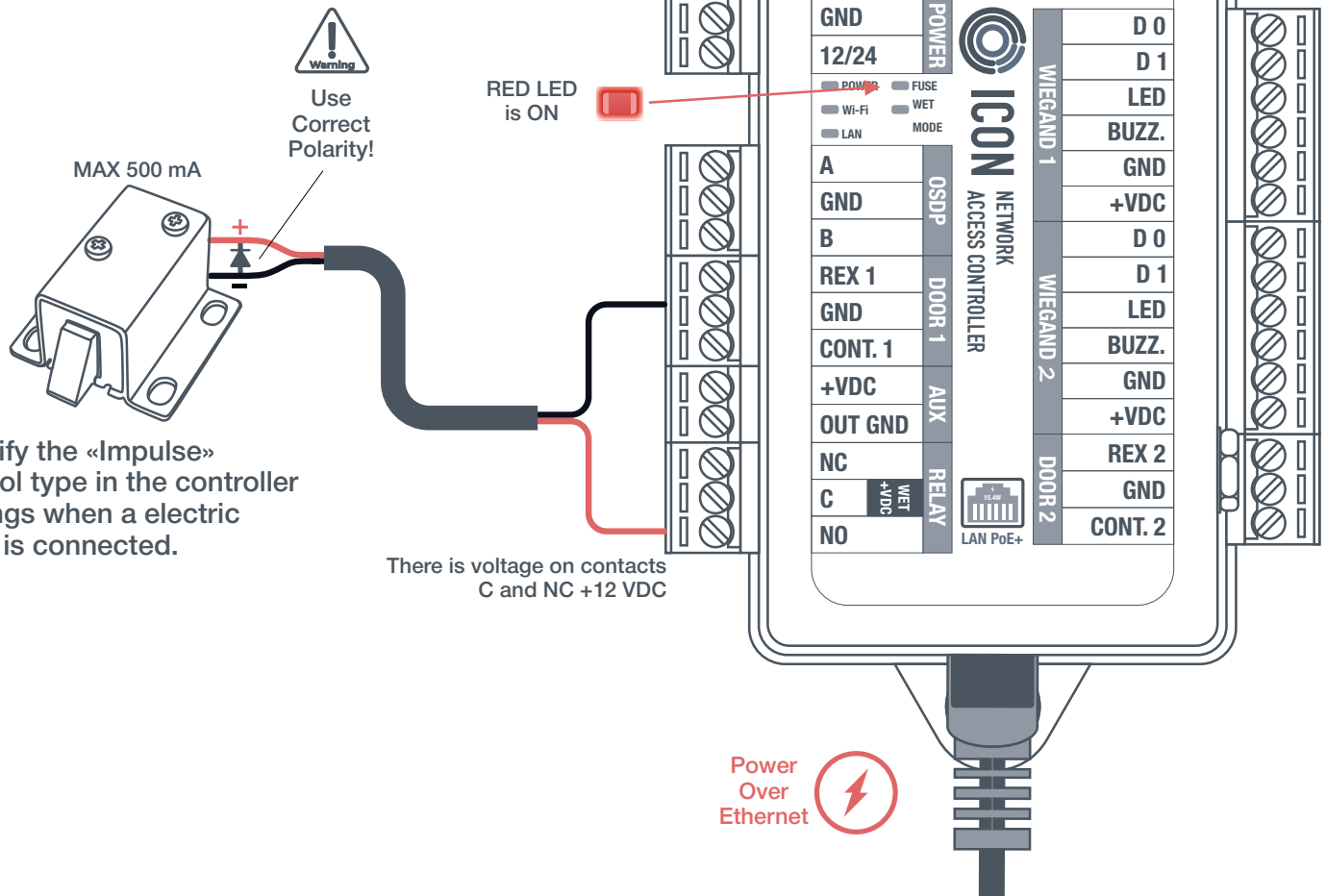
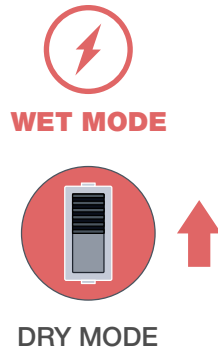
CONNECTION DIAGRAM

Electric Locks [Power over Ethernet] [WET MODE]

Electric Latch

? How to enable wet mode?

⚡ Power off the device, unscrew the four screws, and carefully open the housing cover. Slide the switch to turn on wet mode. Assemble the device in reverse order.



A protective diode is used to protect the controller from reverse currents when an electromagnetic or electromechanical lock is triggered. The protective diode 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.

CONNECTION DIAGRAM

Electric Locks [Power over Ethernet] [WET MODE]

Electric Strike Lock



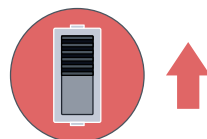
How to enable wet mode?



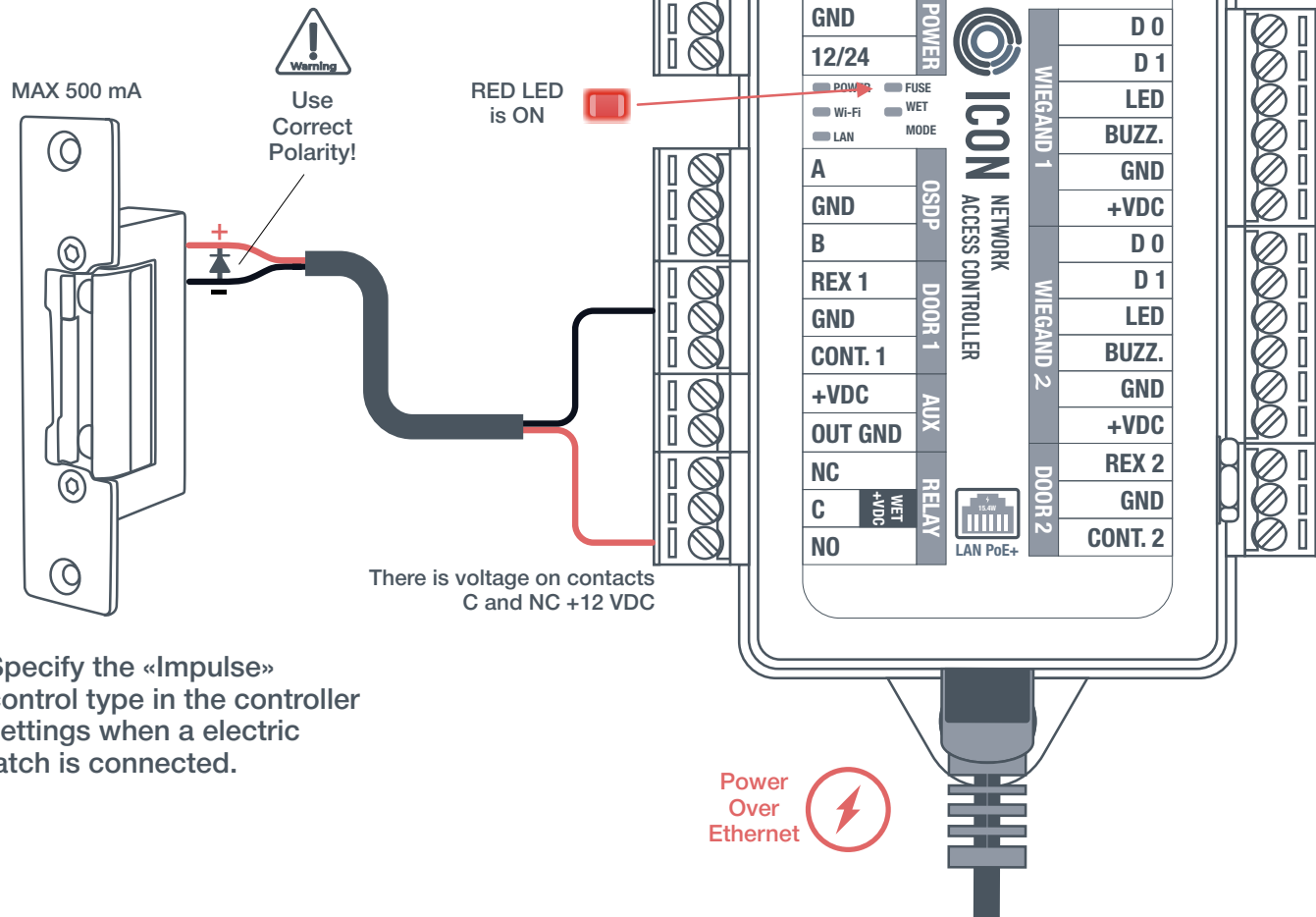
WET MODE



Power off the device, unscrew the four screws, and carefully open the housing cover. Slide the switch to turn on wet mode. Assemble the device in reverse order.



DRY MODE



A protective diode is used to protect the controller from reverse currents when an electromagnetic or electromechanical lock is triggered. The protective diode 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.

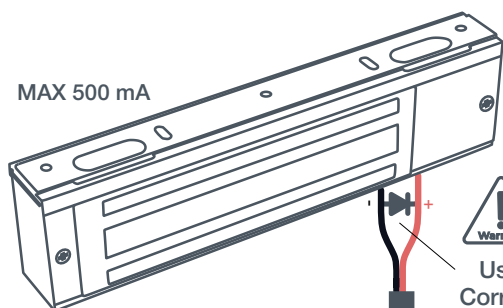
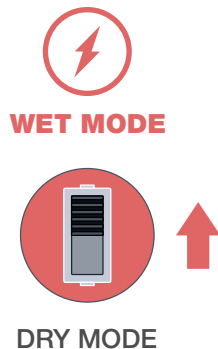
CONNECTION DIAGRAM

Electric Locks [Power over Ethernet] [WET MODE]

Magnetic Lock

? How to enable wet mode?

⚡ Power off the device, unscrew the four screws, and carefully open the housing cover. Slide the switch to turn on wet mode. Assemble the device in reverse order.



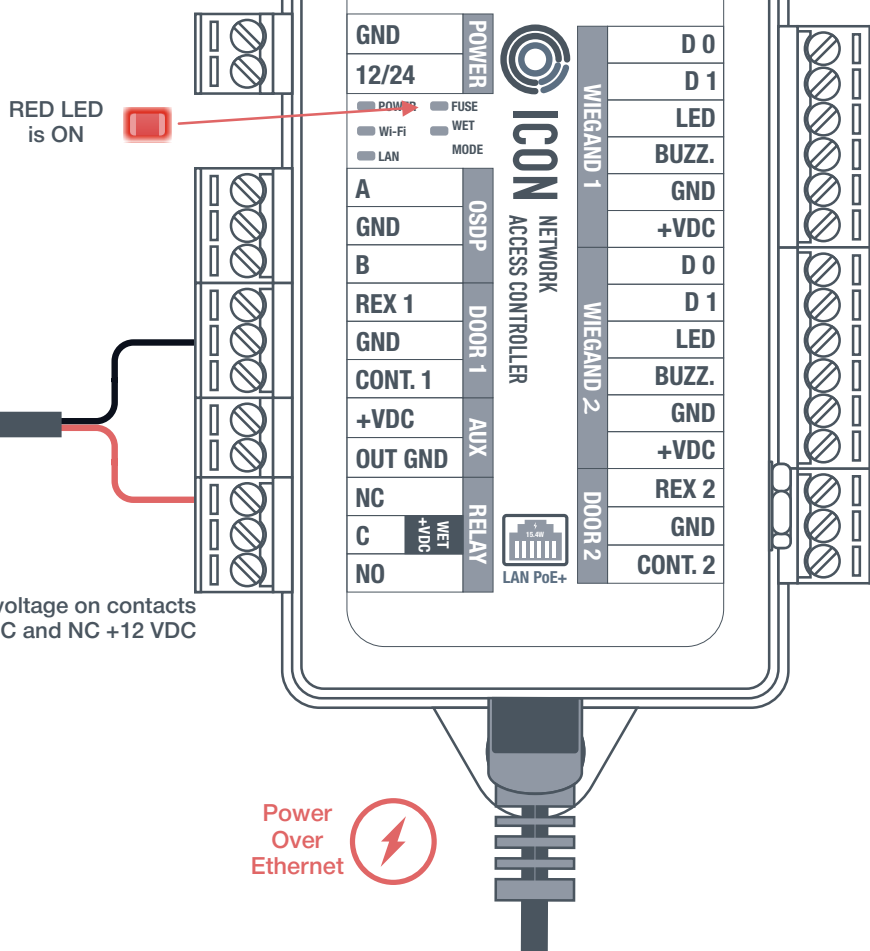
MAX 500 mA

There is voltage on contacts C and NC +12 VDC

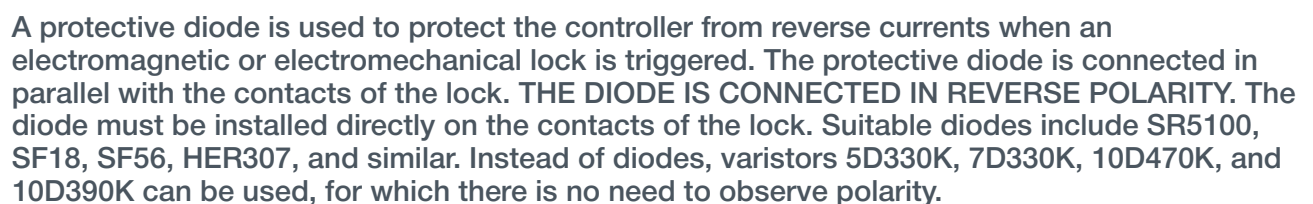
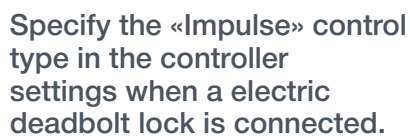
Specify the «Trigger» control type in the controller settings when a magnetic lock is connected.



A protective diode is used to protect the controller from reverse currents when an electromagnetic or electromechanical lock is triggered. The protective diode is 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.



Electric Deadbolt Lock with External Control



CONNECTION DIAGRAM

Electric Locks [Power over Ethernet]

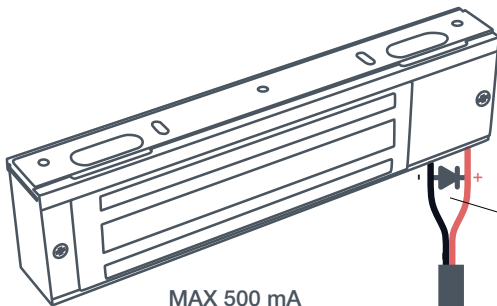
Magnetic Lock



WET MODE



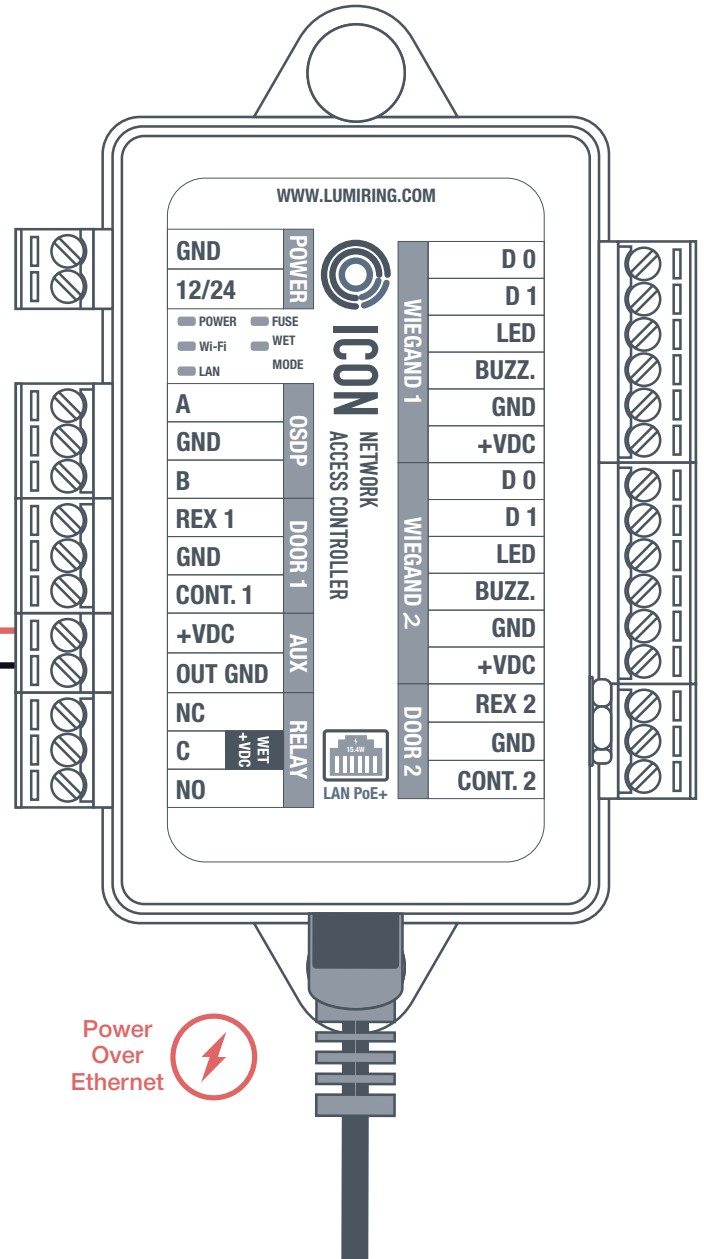
DRY MODE



MAX 500 mA



Use
Correct
Polarity!



Specify the «Trigger» control type
in the controller settings when a
magnetic lock is connected.

Power
Over
Ethernet



A protective diode is used to protect the controller from reverse currents when an electromagnetic or electromechanical lock is triggered. The protective diode 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.

CONNECTION TO THE 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_xxxxxxxx network.

Step 3. Enter the AP Wi-Fi IP address of the device (192.168.4.1) in the address bar of your browser and press Enter.

Step 4. After the page loads, enter your login and password.

After login, the browser will redirect you to the Quick Start page.

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.

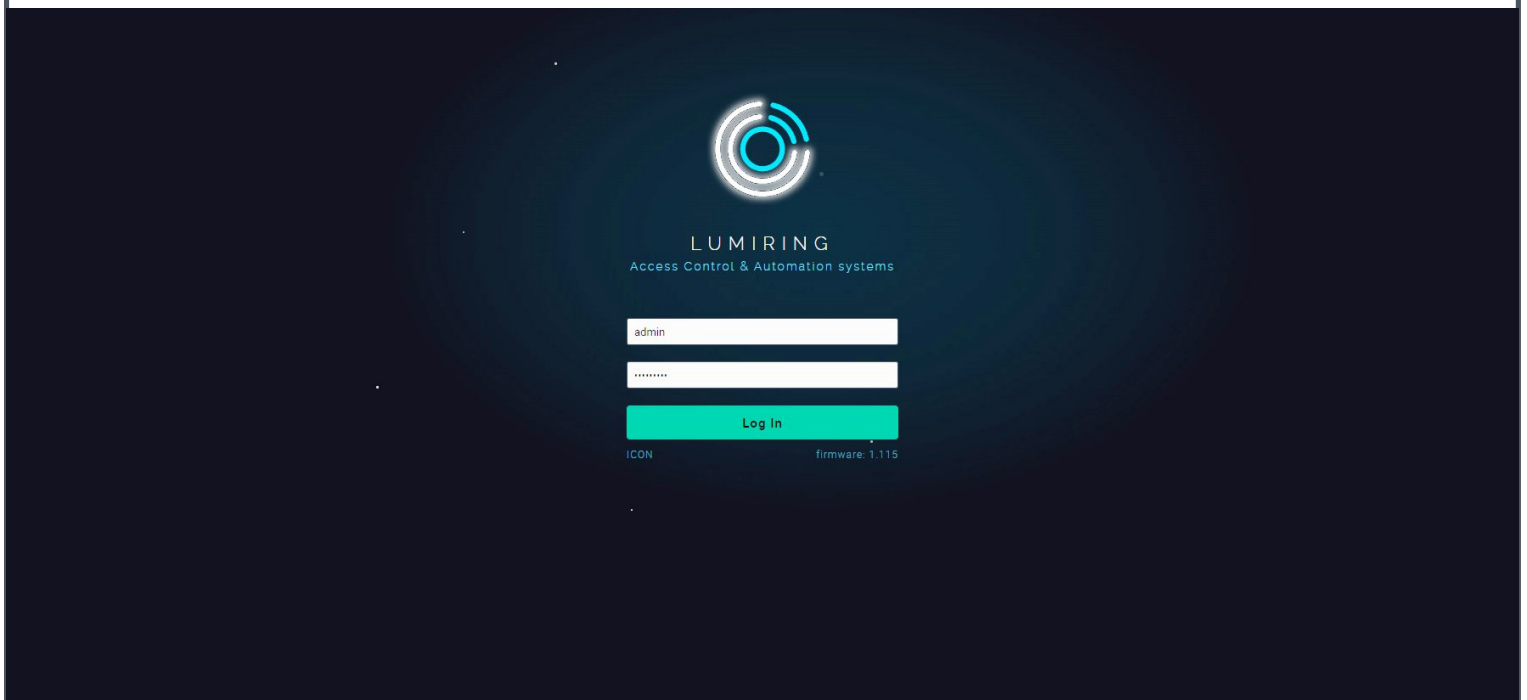
Step 2. Connect the device to a power source.

Step 3. In the address bar of your browser, enter the device IP address and press enter.

Step 4. After the page loads, enter your login and password.

After login, the browser will redirect you to the Quick Start page.

Login



The login page displays the model name of the device and the current firmware version.

- Enter your username, password and click "Log In."

The screenshot shows the LumiRing Quick Start interface. At the top, there's a header with the LumiRing logo and a settings icon. Below the header is a diagram showing the device (ICON) connected to a router, which is connected to the cloud. The interface is divided into three main sections:

- Network:** "Please select type of your network connection and make connection settings". It includes a dropdown for "Network type" (set to "Wi-Fi network"), a dropdown for "SSID name" (set to "lumiRing"), and a password field. A "Submit" button is at the bottom.
- Cloud:** "Please enter your cloud account information." It includes an "Account ID" field (set to "147") and a "Device note" field (set to "My Device"). A "Submit" button is at the bottom.
- Security:** "Please change password for devices network access and device Wi-Fi AP." It includes a checkbox "Use the same password for two purposes" (checked), a "Wi-Fi AP" section with an "SSID name" field (set to "ICON_6234172"), a "Password (8 characters minimum)" field, and a "Repeat password" field. A "Submit" button is at the bottom.

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.

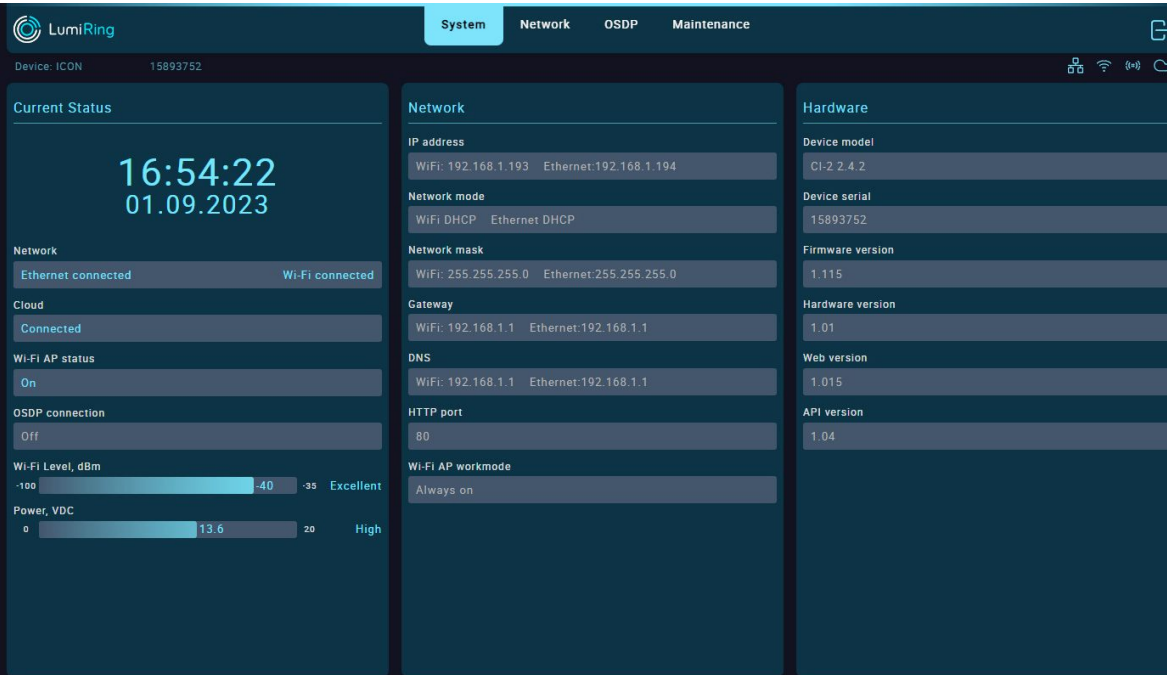
Cloud:

- 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.



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.

The screenshot shows the LumiRing configuration interface with the following details:

- Network Section:**
 - Network type: Wi-Fi network
 - SSID name: lumiring
 - Password: [Redacted]
 - Connection way: DHCP (selected), Manual
 - IP address: 192.168.1.193
 - Network mask: 255.255.255.0
 - Gateway: 192.168.1.1
 - DNS: 192.168.1.1
 - Connect button
- Wi-Fi AP Section:**
 - Always on: [Unchecked]
 - Local Wi-Fi AP name (8 characters minimum): ICON_15893752
 - Password (8 characters minimum): [Redacted]
 - Enable hidden mode: [Unchecked]
 - Enable timed mode: [Checked]
 - Wi-Fi timer, min (1 - 60): 30
 - HTTP port: 80
- Cloud Section:**
 - Server: Unimacs
 - Account Id: 191
 - Auto connect button
 - Device Id: 15893752
 - Location: 191/102/registration
 - Operate topic: 191/102/registration/15893752/Operate/
 - Ack topic: 191/102/registration/15893752/Ack/
 - Events topic: 191/102/registration/15893752/Events/

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 screenshot displays the LumiRing configuration interface with the 'Network' tab selected. The interface is divided into three main sections: Network, Wi-Fi AP, and Cloud.

Network Section:

- Device: ICON, 15893752
- Network type: Wired Ethernet Network (dropdown)
- Connection way: ☒ DHCP, ☐ Manual
- IP address: 192.168.1.194
- Network mask: 255.255.255.0
- Gateway: 192.168.1.1
- DNS: 192.168.1.1

Wi-Fi AP Section:

- ☐ Always on
- Local Wi-Fi AP name (8 characters minimum): ICON_15893752
- Password (8 characters minimum): [masked]
- ☐ Enable hidden mode
 - In Hidden mode, Users cant find Wi-Fi SSID by usual Wi-Fi network scan. SSID is hidden. Users must input SSID name manually before connecting.
- ☒ Enable timed mode
 - In Timed mode, the Wi-Fi Access point starts after the device is powered. Users can connect to AP during the time set in the Timer field.
- Wi-Fi timer, min (1 - 60): 30
 - The Wi-Fi AP will turn off after a specified time if there is no connection or user activity.
- HTTP port: 80

Cloud Section:

- Server: Unimacs (dropdown)
- Account Id: 191 [Auto connect button]
- Note: [empty text area]
- Device Id: 15893752
- Location: 191/102/registration
- Operate topic: 191/102/registration/15893752/Operate/
- Ack topic: 191/102/registration/15893752/Ack/
- Events topic: 191/102/registration/15893752/Events/

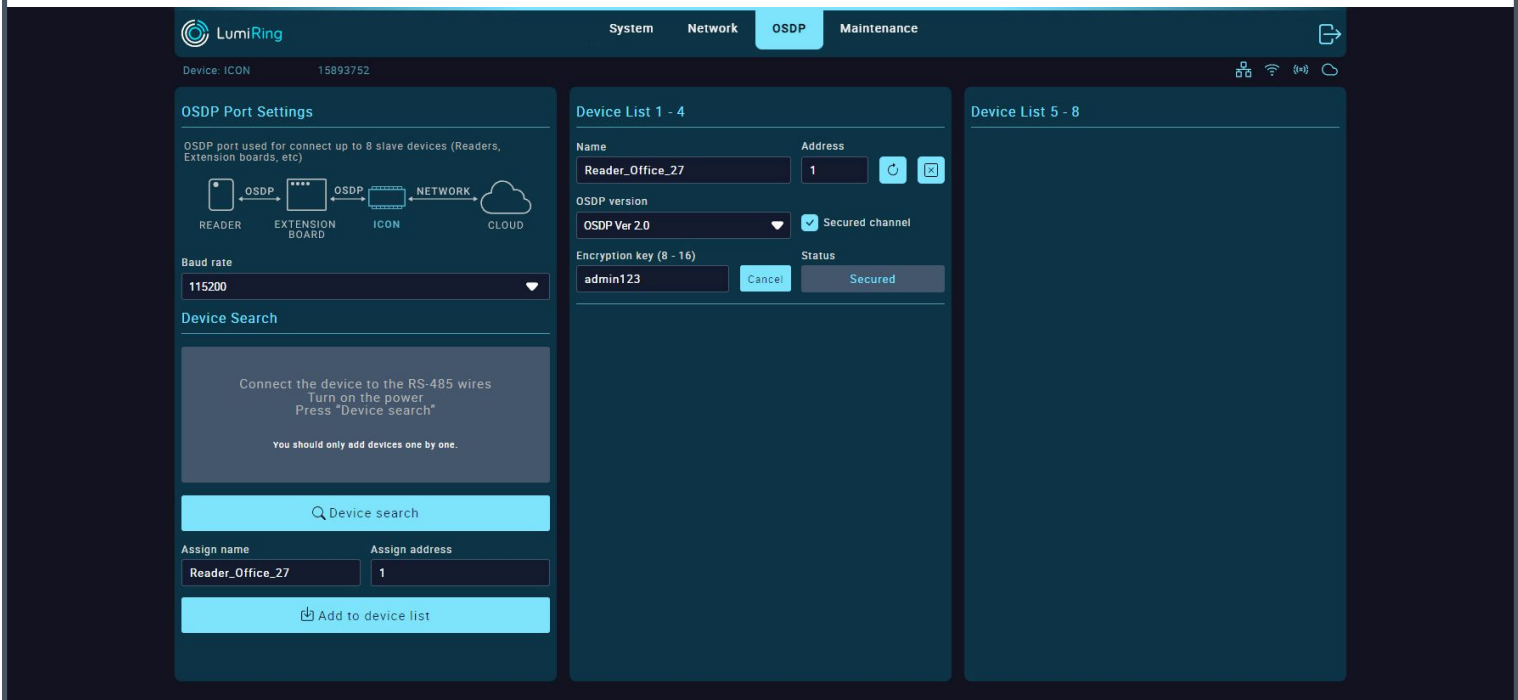
The Cloud settings subsection allows you to connect the Controller to a cloud server for later use.

- 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) [Coming soon!]



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.

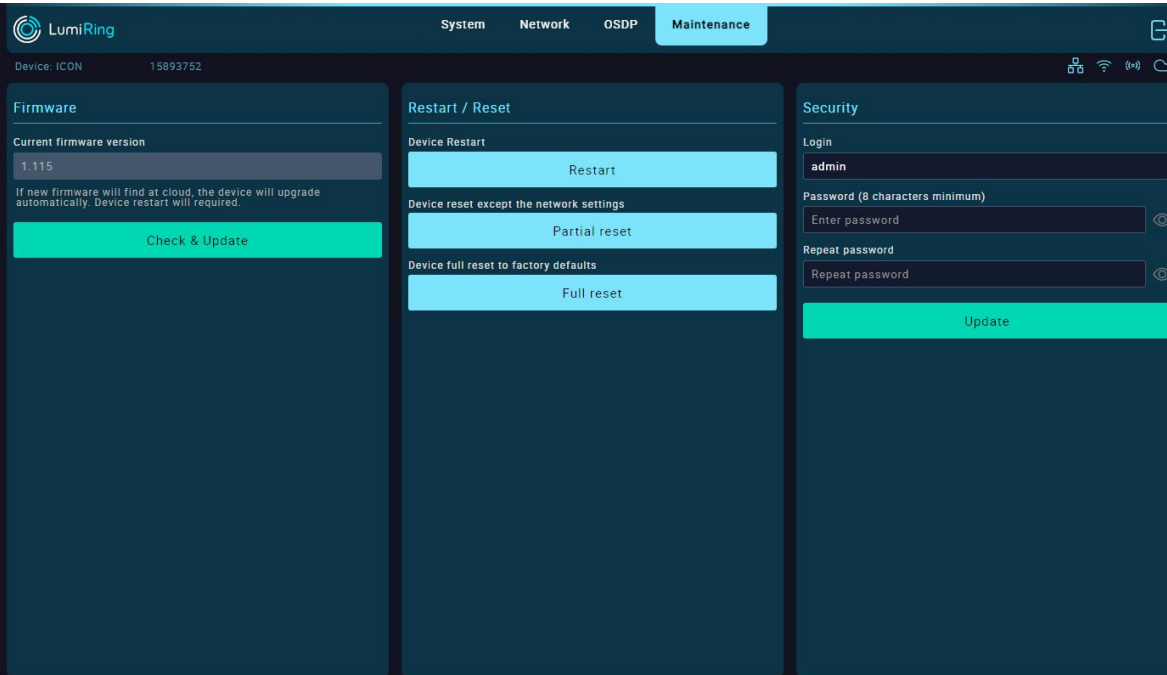
If the search results do not find an OSDP device, change the ACU baud rate and click the "Device search" button again.

- 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 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 via Ethernet 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 message 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.

A power failure or network connection interruption during the update may cause a firmware update application error.

If an error occurs during the update process, unplug the power to the unit for 10 seconds and reconnect it. Leave the unit switched on for 5 minutes without attempting to connect or log in to 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:

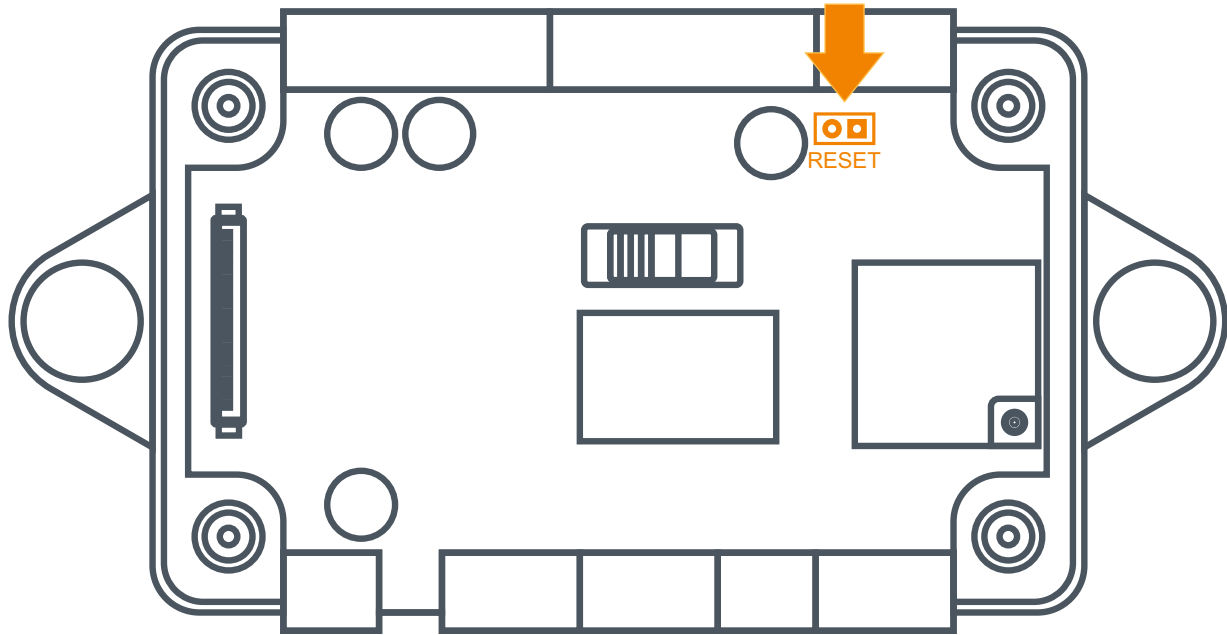
- Restart - restarts the device.
- Partial reset - resets all device settings except for network connection settings.
- Full reset - resets all settings of the device to factory defaults.

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 in to the device interface.

HARDWARE RESET



Hardware reset

1. Turn off the power to the device.
2. Remove the four screws and remove the front of the case.
3. Place a jumper on both pins to short them to each other.
4. Connect the power supply.
5. The blue LED will blink rapidly for 10 seconds and then become solid.
6. Remove the jumper.
7. Disconnect power to the unit.
8. Replace the front of the case and tighten the four screws.
9. Wait 10 seconds until the blue LED starts flashing.
10. The hardware reset procedure is complete, and the device is ready for use.

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 identification devices, 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 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.

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.