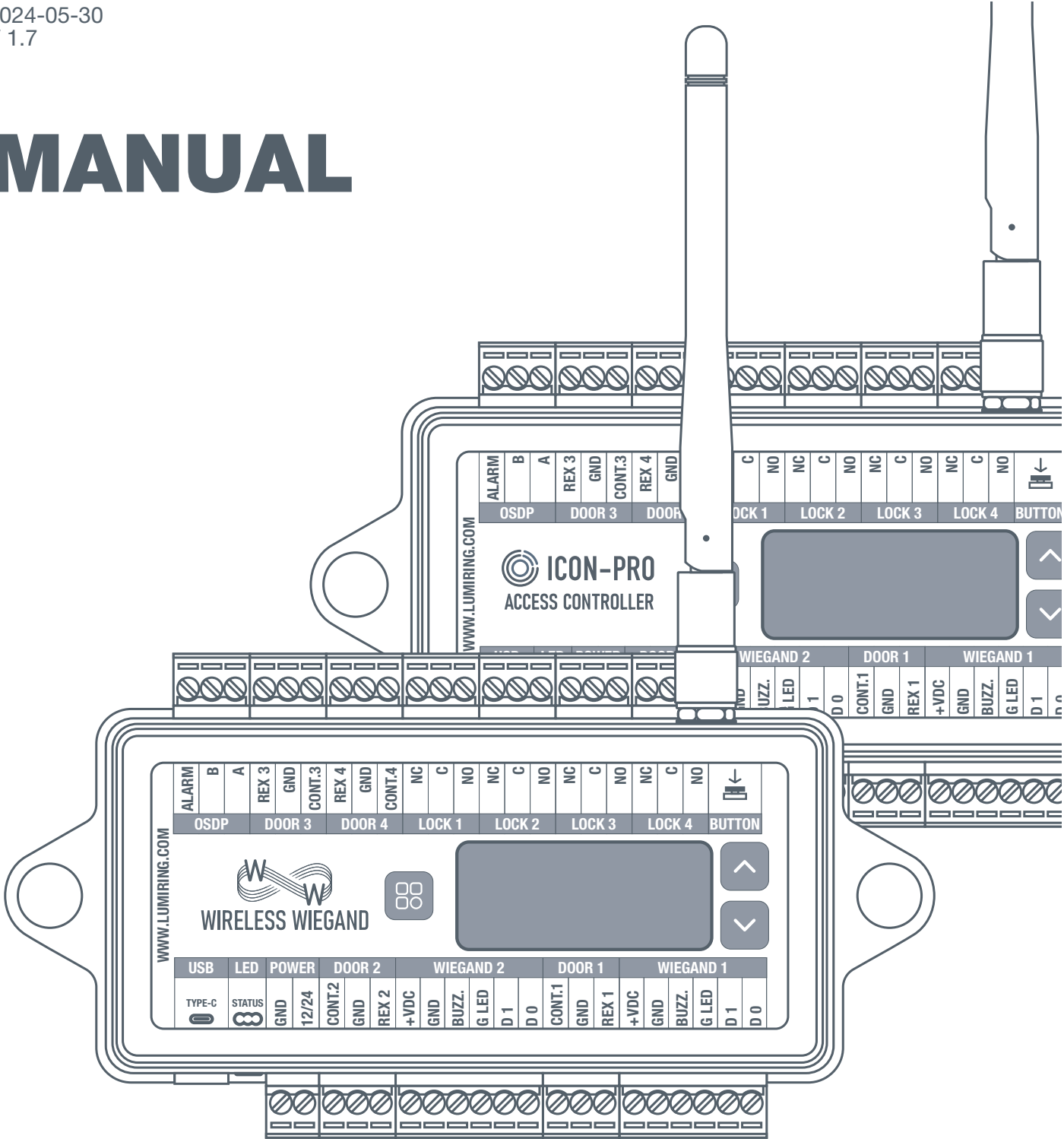


# MANUAL



# ICON-PRO

## ACCESS CONTROLLER WITH WIRELESS GATEWAY

# CONTENTS

|                                                                     |    |
|---------------------------------------------------------------------|----|
| • Introduction                                                      | 3  |
| • Default Device Settings                                           | 3  |
| • Device Specifications                                             | 4  |
| • Radio Transceiver Specifications                                  | 4  |
| • Device Dimensions                                                 | 5  |
| • Controller & Gate Slave mode Connection Terminals                 | 6  |
| • Gate Master mode Connection Terminals                             | 7  |
| • Display                                                           |    |
| ◦ Unit Designation                                                  | 8  |
| ◦ Interactions with Buttons                                         | 8  |
| ◦ Screens                                                           | 8  |
| ◦ Understanding the information displayed                           | 9  |
| • Installation Recommendations:                                     |    |
| ◦ Connecting the OEM Antenna                                        | 9  |
| ◦ Connecting the Antenna Extension Cord (optional accessory)        | 10 |
| ◦ Placement and Wiring                                              | 10 |
| ◦ Connecting Power to the Device                                    | 10 |
| ◦ Wiegand Connection                                                | 10 |
| ◦ Connecting OSDP                                                   | 10 |
| ◦ Connecting Electric Locks                                         | 10 |
| ◦ Protection Against High Current Surges                            | 10 |
| ◦ Recommendations for Connection                                    | 11 |
| ◦ Pairing                                                           | 11 |
| ◦ Automatic Recovery in Case of Connection Loss                     | 11 |
| ◦ Pairing Features                                                  | 11 |
| • Controller & Gate Slave modes (Connection Diagram):               |    |
| ◦ Wiegand Readers                                                   | 12 |
| ◦ Door Sensor & Exit Button                                         | 14 |
| ◦ AIR-Button V 2.0                                                  | 15 |
| ◦ AIR-Button V3.0                                                   | 16 |
| ◦ Request to Exit PIR Motion Sensor                                 | 17 |
| ◦ Electric Lock                                                     | 19 |
| • Gate Master mode (Connection Diagram to the ICON-Pro Controller): |    |
| ◦ Wiegand Outputs                                                   | 20 |
| ◦ REX Outputs, CONTACT Outputs                                      | 21 |
| ◦ Relay Inputs                                                      | 22 |
| ◦ OSDP Inputs (Coming Soon!)                                        | 23 |
| • Web Interface:                                                    |    |
| ◦ Login                                                             | 24 |
| ◦ System                                                            | 25 |
| ◦ Network                                                           | 26 |
| ◦ Maintenance                                                       | 27 |
| ◦ Firmware Update via Cloud Server                                  | 28 |
| • Hardware Reset                                                    | 29 |
| • Glossary                                                          | 31 |
| • Supported Readers models                                          | 32 |
| • For Notes                                                         | 33 |

## Introduction

This document provides detailed information on the structure of the ICON-PRO - Access controller with wireless gateway and instructions for installation and connection.

It also includes instructions that identify potential risks and methods for troubleshooting 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 this 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.

## Default Device Settings

### Wi-Fi device name when searching:

- WW\_M/SD\_(serial\_number)

### AP Wi-Fi IP address of the device:

- 192.168.4.1

### Wi-Fi password:

- None (factory default)

### Web page login:

- admin

### Web page password:

- admin123

### AP Wi-Fi timer:

- 30 minutes

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

## Device Specifications

### Voltage:

- 12 or 24 VDC operation
- The voltage at the outputs is determined by the power supply.
- 0.2A @12 VDC, 0.1A @ 24 VDC current consumption

### Slave device:

- **Outputs:**
  - Four (4) dry form "C" 1.5A rated relay outputs
- **Inputs:**
  - Eight (8) inputs (dry contact) from 0 to 5 VDC
  - One (1) input (dry contact) 0 to 5 VDC for local emergency relay opening

### Master device:

- **Outputs:**
  - Eight (8) outputs (dry contact) from 0 to 5 VDC
- **Inputs:**
  - Four (4) relay control inputs (dry contact) from 0 to 5 VDC

### Communication interfaces:

- Wi-Fi 802.11 b/g/n 2.4 GHz

- Two (2) Wiegand ports from 4 to 80 bits
- RS-485 (OSDP)
- USB port (Type-C) for firmware update

### Range:

- 3,280 ft (1 000 m)

### Encryption:

- AES128

### Dimensions (L x W x H):

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

### Mounting method:

- Wall mount/Din rail mount (option)

### Weight:

- 5.36 oz (152 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

### Ingress protection rating:

- IP 20

## Radio Transceiver Specifications

### Transmit power:

- 1 Watt (30dBm)

### Frequency band:

- 868 MHZ (EU)
- 915 MHz (NA)

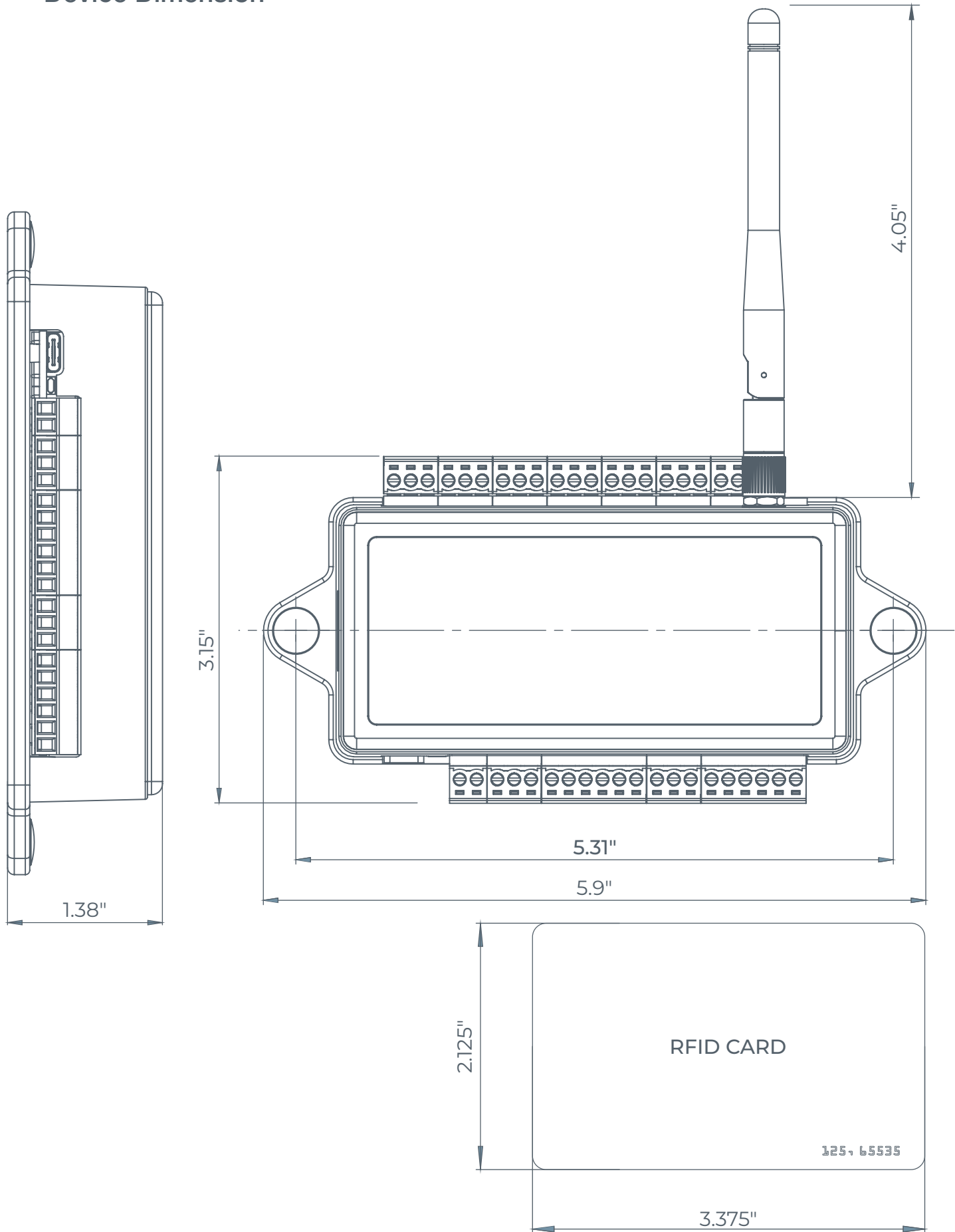
### Channels:

- 140 (FHSS)

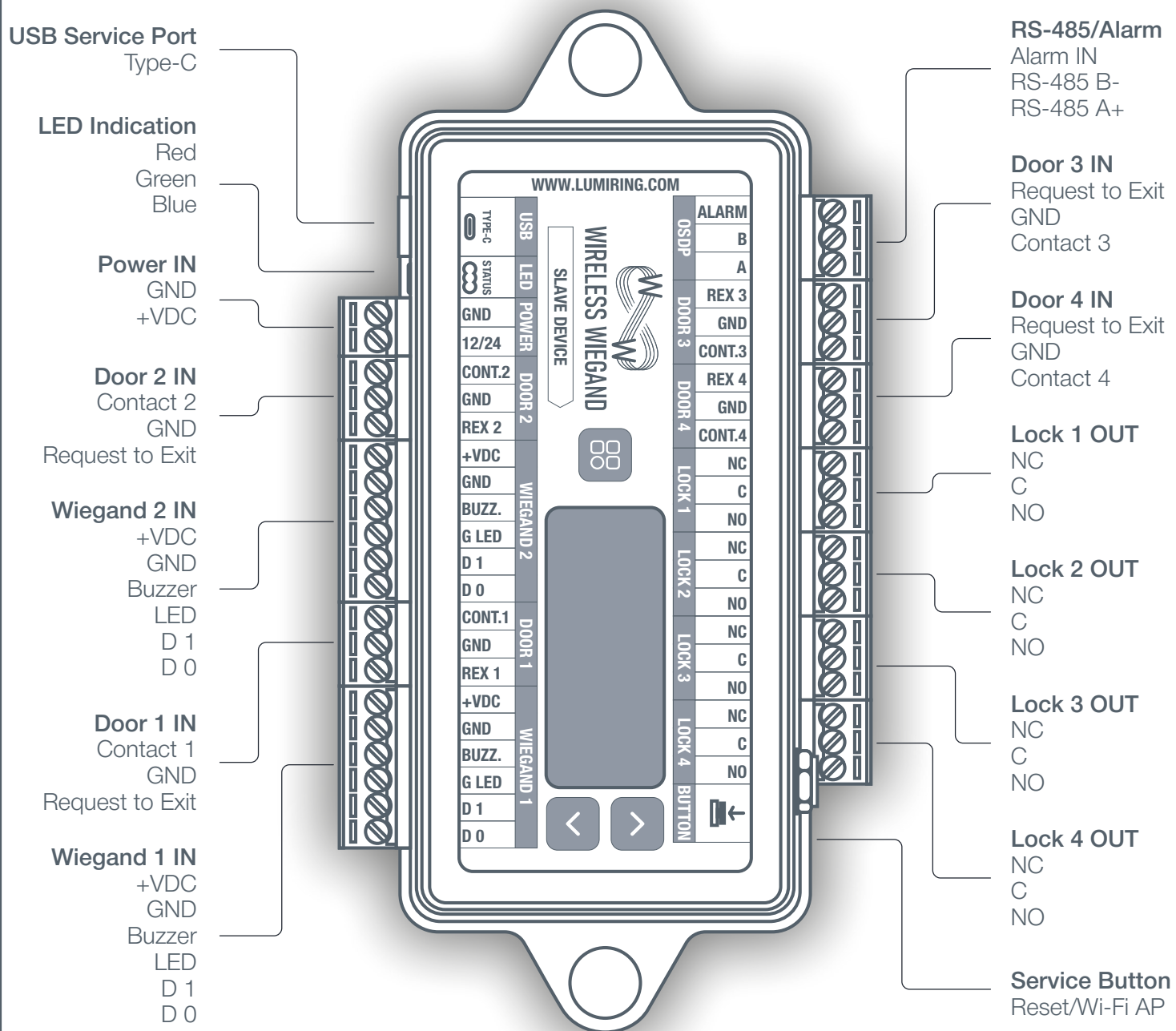
### Receiver sensitivity:

- -117dBm

## Device Dimension



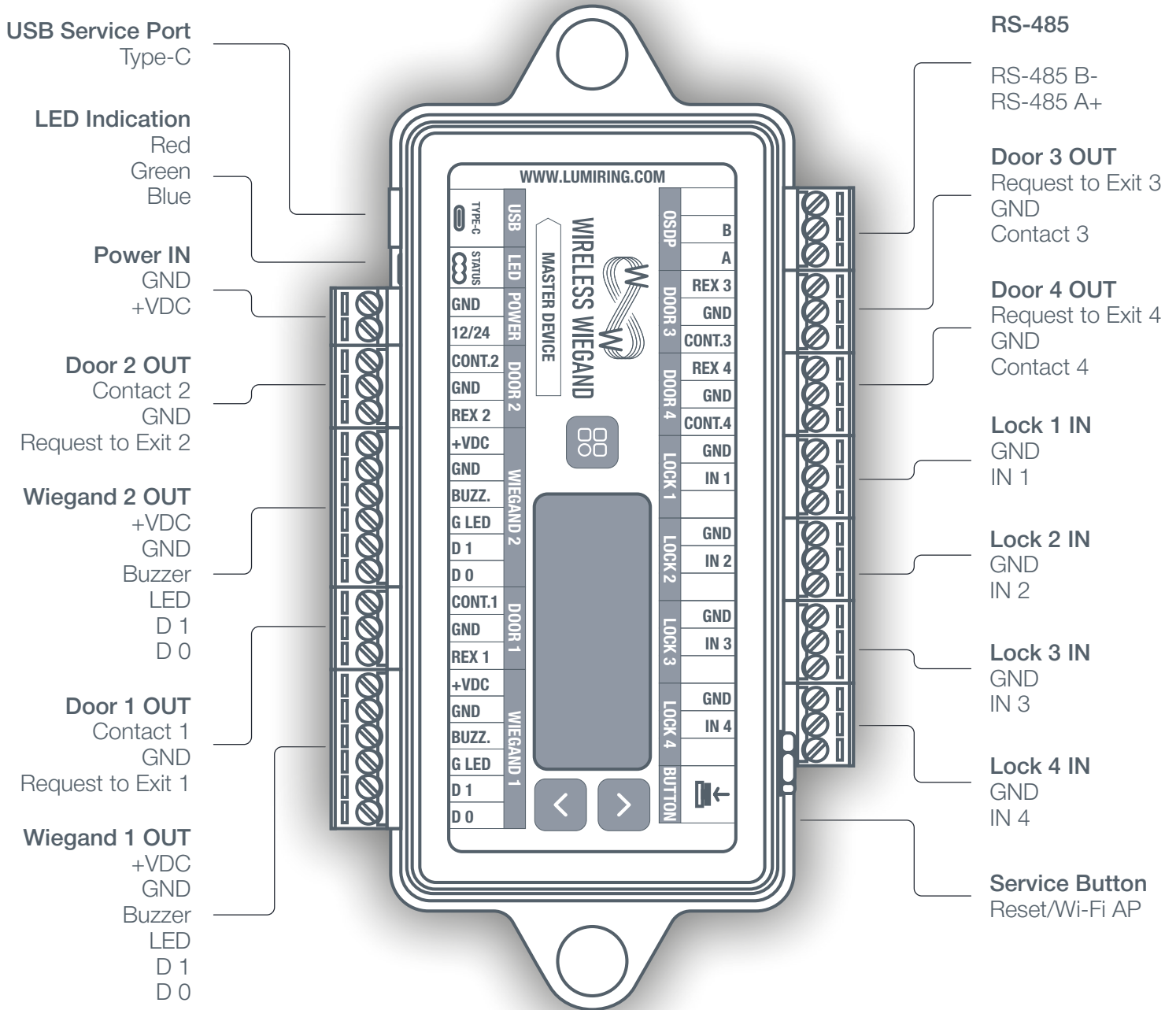
## Controller & Gate Slave Mode Connection Terminals



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.

## Gate Master Mode Connection Terminals



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.

## Display

The information display is designed for the following functions:

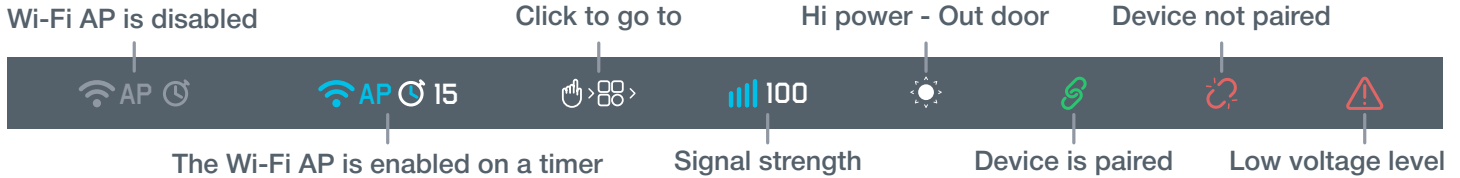
1. Displaying the current status of the device.
2. Providing information about the communication quality.
3. Displaying the operation history of the unit.
4. Control of inputs and outputs.

5. Displaying card codes read from connected readers.

This display provides operational data for:

- Optimization of device placement.
- Analysing the quality of communication in the urban radio environment.

### Unit Designation



### Interaction with Buttons

To enable/disable the Wi-Fi access point (AP):

- Hold down and then release the **Service Button** located near the antenna connector.

For action:

- Hold and then release the **[⏏]** button for 1 second.

To navigate:

- Hold and then release the **[↑/↓]** up/down button for 1 second to move to the next screen.

### Screens



Main screen:

- Wi-Fi AP status and time to disconnect.
- Signal strength in percent.
- Low battery warning.
- Device installation recommendation.
- Pairing status with the responding device.



Device information:

- Name, type, and serial number.
- Firmware version.
- Current power supply voltage.
- Type and serial number of paired device.

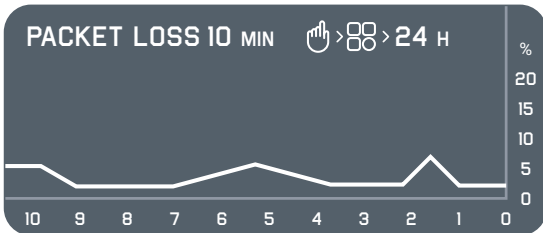
Actions on the device information screen:

- To locate the paired device, hold down the **[⏏]** button for 1 second.
- The device on the opposite side will beep rhythmically to indicate its location.
- The signal strength indicator will also blink while locating.
- To abort the operation, hold down the **[⏏]** button again for 1 second.



## Display

|                  |      |
|------------------|------|
| SIGNAL STRENGTH  | 100% |
| PACKET LOSS 60 S | 3%   |
| PACKET LOSS 10 M | 1%   |
| PACKET LOSS 24 H | 0%   |



### I/O MONITORING

|      |                                                                                   |                                                                                   |                                                                                   |                                                                                   |                                                                                   |                                                                                   |     |
|------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|-----|
|      | 1                                                                                 | 2                                                                                 | 3                                                                                 | 4                                                                                 | 1                                                                                 | 2                                                                                 |     |
| REX  |  |  |  |  |  |  | LED |
| CONT |  |  |  |  |  |  | BUZ |
| LOCK |  |  |  |  |                                                                                   |                                                                                   |     |

|     |                   |
|-----|-------------------|
| HEX | W1_34 5E:A2:D2:AA |
| UID | 1 587 729 066     |
| HEX | W2_26 4D:C5:DC    |
| UID | 5 096 924         |

### Device information

- Indicates the strength of the signal as a percentage ratio.
- Percentage of packet loss in the last 60 seconds.
- Percentage of packet loss in the last 10 minutes.
- Percentage of packet loss in the last 24 hours.

### Packet Loss graph:

- Displays a packet loss graph for the last 60 seconds, 10 minutes, or 24 hours.
- Press  to change the time interval.

**Note:** Statistics are reset when the unit is switched off.

### Input and output monitor

- REX activation status 1 to 4.
- CONT. activation status 1 to 4.
- LOCK activation status 1 to 4.
- LED 1, 2 and BUZ 1, 2 activation status.

### Display of the transmitted code

- HEX in hexadecimal.
- UID (Unique identifier) serial number or pin code.
- Data source: W1, W2, or OSDP address.
- Data bit format: 4 to 80 bits.

### Understanding the information displayed

- All incoming data is displayed sequentially on the screen. The new code is displayed at the bottom.
- The values in front of the data in HEX indicate the Wiegand port number and the number of data bits. This display is the same for all ports with incoming data, including OSDP readers.

**For example: W2\_26 AE:25:CD indicates that the data came from the Wiegand 2 port in 26 bits. The hexadecimal code follows.**

- Unique identifier (UID) data values should be understood as an interpretation of decimal data.

## Installation Recommendations

**Warning! Do not turn on devices without antennas installed! Doing so may damage the radio module and cause premature failure of the device!**

### Connecting the OEM antenna

- The antennas are screwed to the devices before powering up.
- The antenna connector should be tightened by hand, without the use of improvised tools or excessive force.
- Tighten the connector completely and make sure that it does not unscrew when the antenna is rotated.

## Installation Recommendations

### Connecting the Antenna Extension Cord (optional accessory)

|                                     |                                             |
|-------------------------------------|---------------------------------------------|
| <b>Antenna cable:</b>               | The wave impedance of the cable is 50 ohms. |
| <b>Length:</b>                      | 33 ft (10 m) MAX.                           |
| <b>Input connector:</b>             | RPSMA-Female (jack).                        |
| <b>Output connector:</b>            | RPSMA-Male (plug).                          |
| <b>Antenna RPSMA-Female (jack):</b> | Operating frequency 868-915MHz.             |

### Placement and Wiring

- The maximum range increases when devices are placed over obstacles or in direct line of sight of each other.
- Try to choose the best location for installation, away from sources of strong radiation such as cellular repeaters, overhead power lines, electric motors, etc.
- The minimum distance between active radio transmitters is determined by their performance in the radio environment.
- Test results show optimal operation of three active radio transmitters at a distance of one meter from each other. When the number of active radio transmitters increases, delays in radio exchange are observed due to the creation of intensive radio interference.
- Avoid placing the device on metal surfaces, as this may reduce the quality of the radio connection.
- The device is attached to the installation site so that the antenna to be folded is pointing perpendicularly upwards.

### Connecting Power to the Device

- 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 device and the actuators.

### Wiegand Connection

- Use the same Wiegand format and byte order 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 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 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.

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

## Installation Recommendations

### Recommendations for Connection

- Make all connections only when the power is off.
- The wires are only connected to the removable terminal blocks.
- Be sure to check the correct connection before switching on the unit.

### Pairing

1. Connect the master device to a power source. Ensure the LED indicator flashes blue, indicating the pair search mode.
2. Connect the slave device to a power source. Also, ensure the LED indicator blinks blue to indicate the pair search mode.
3. When first powered out of the box or after a hardware reset, the units automatically go through the pairing procedure, which takes approximately 10 seconds.
4. Once this procedure is complete, the teams are ready for use.

### Automatic Recovery in Case of Connection Loss

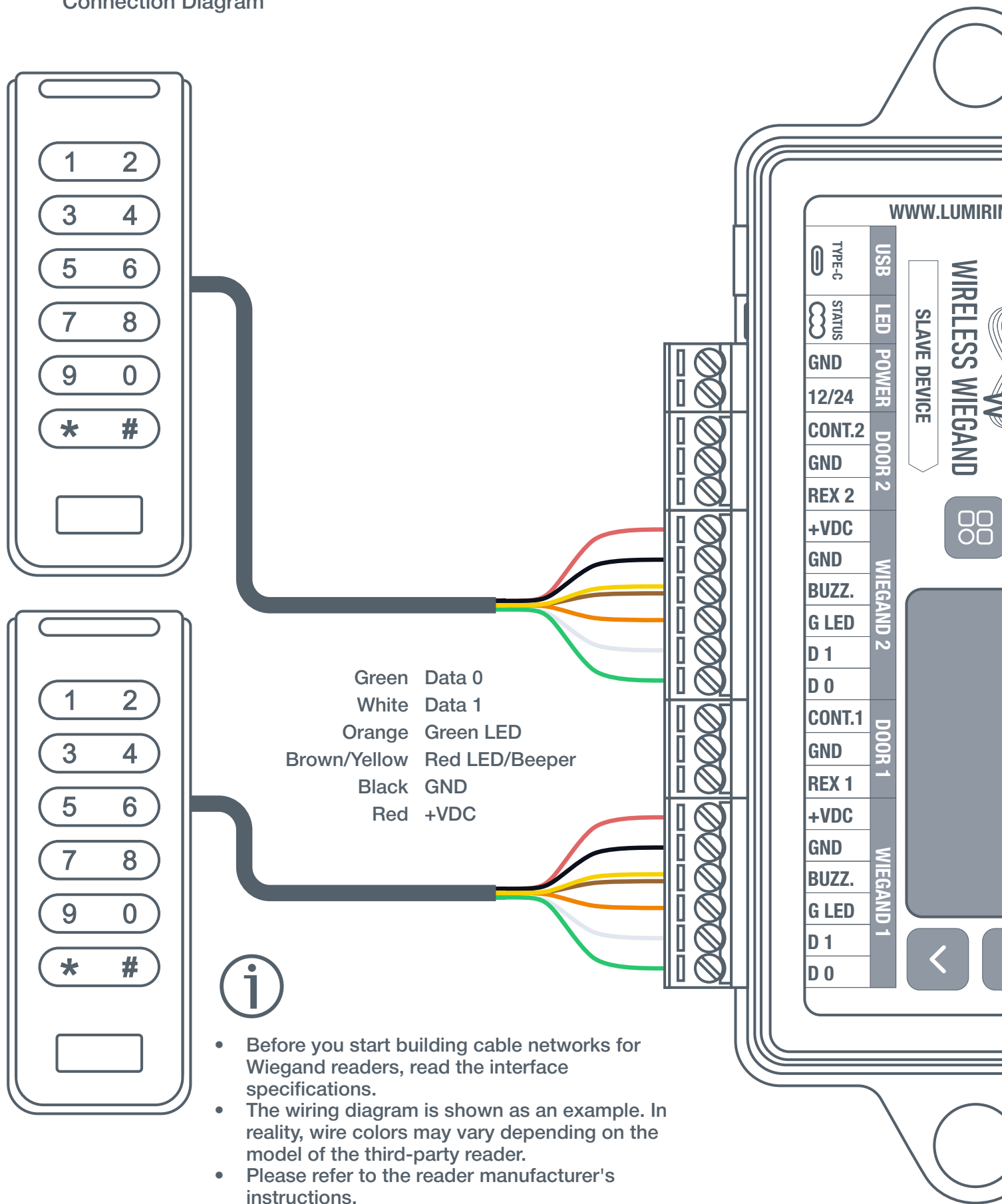
- Over time and during operation, the surrounding radio environment can change, leading to communication failures and reduced operating distance.
- In the event of a dropped connection or power failure, the device will make several attempts to resume communication, including resetting the radio module and a complete restart.
- If the device receives no response, it will enter standby mode.
- Once communication is restored, the unit will automatically resume operation. In some cases, it may take up to one minute from the time the kit is started to re-establish the connection.

### Pairing Features

- When performing device pairing, master-slave device sets should be turned on one at a time.
- If multiple unpaired sets are powered up at the same time, a collision may occur, resulting in erroneous data exchange on the first power-up, and therefore full operation will not be possible.
- If this occurs, simply perform a full reset of the device set and pair again with one set enabled for pairing.

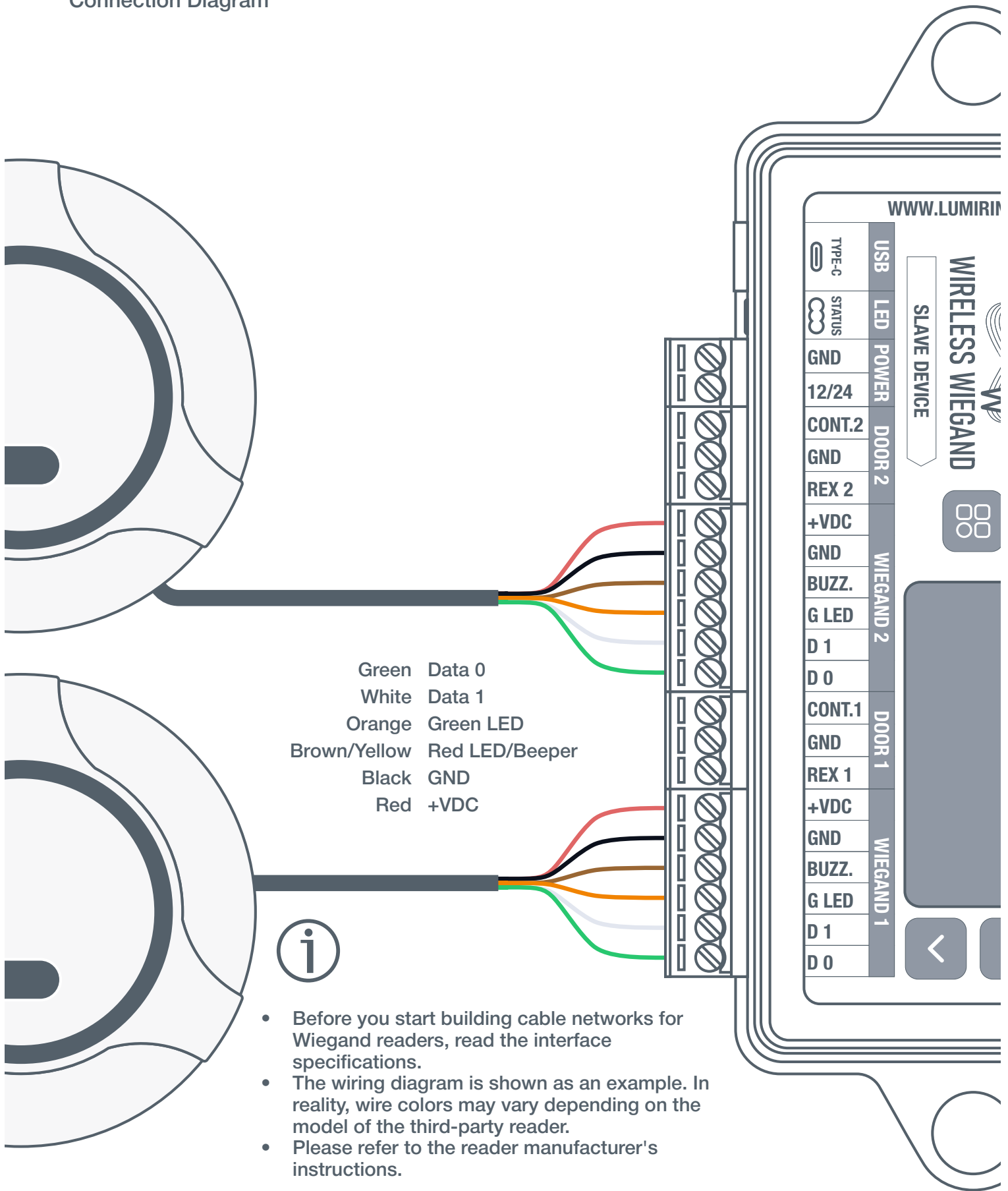
# Controller & Gate Slave modes: Wiegand Readers

## Connection Diagram



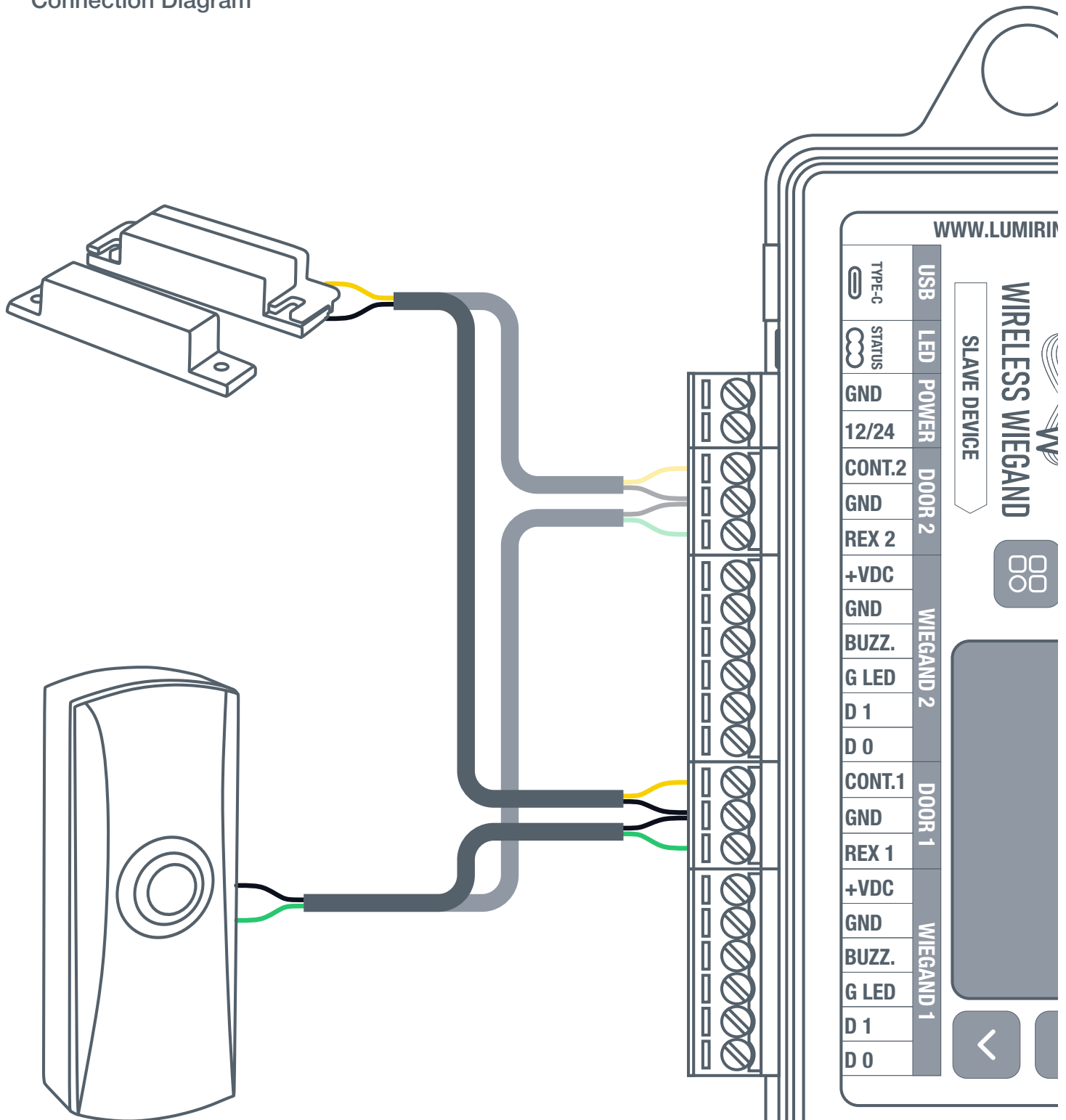
# Controller & Gate Slave modes: Wiegand Readers

## Connection Diagram



- 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



- 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.

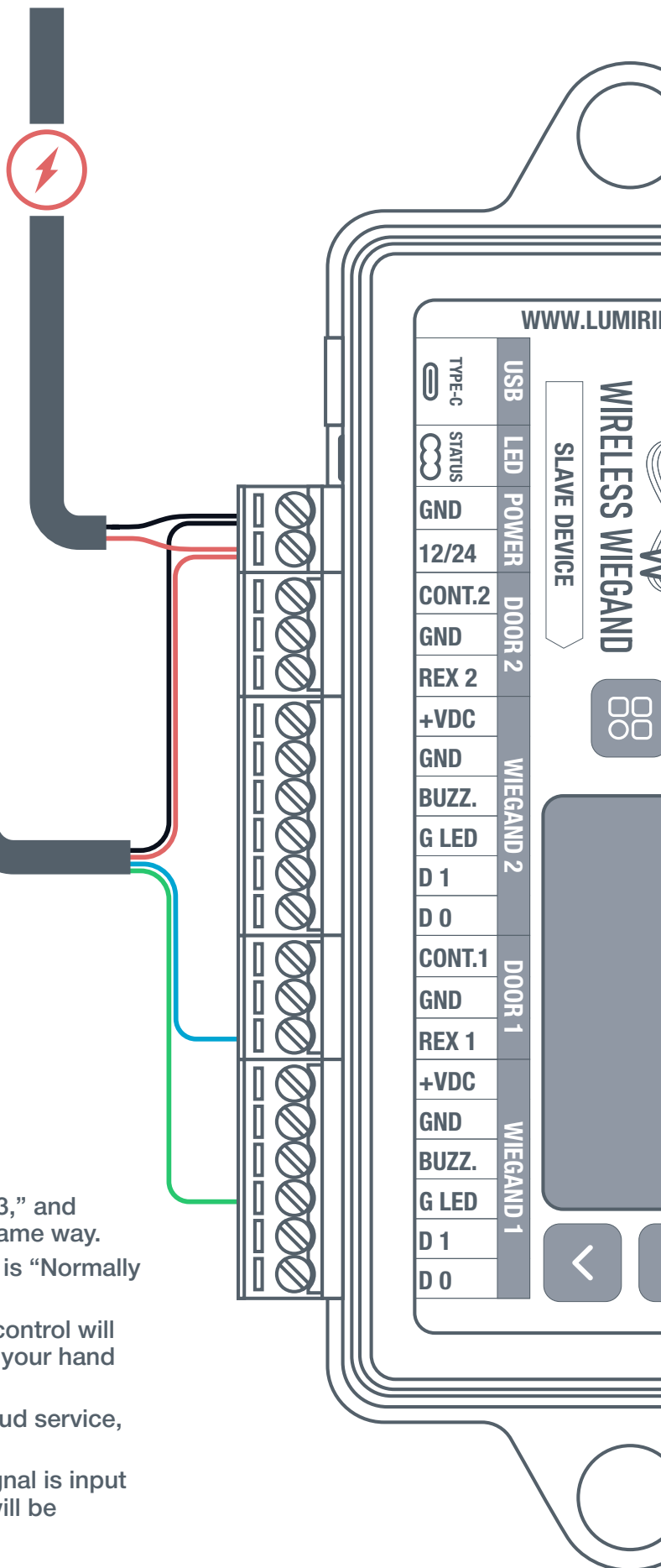
## Connection Diagram

Diagram illustrating the cable connection for the VE OPEN sensor. The sensor is connected to a terminal block via four wires:

- Red: +VDC
- Black: GND
- Blue: REX
- Green: Green LED



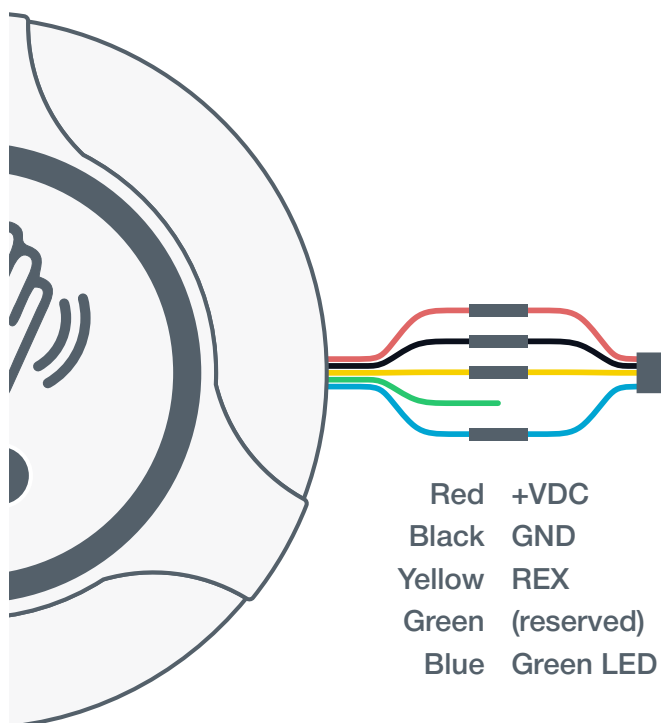
- Connecting to the “DOOR 2,” “DOOR 3,” and “DOOR 4” connectors is done in the same way.
- The buttons is default factory settings is “Normally Open.”
- This means that a low level signal for control will appear on the blue wire when you put your hand to the optical sensor.
- When setting the exit button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



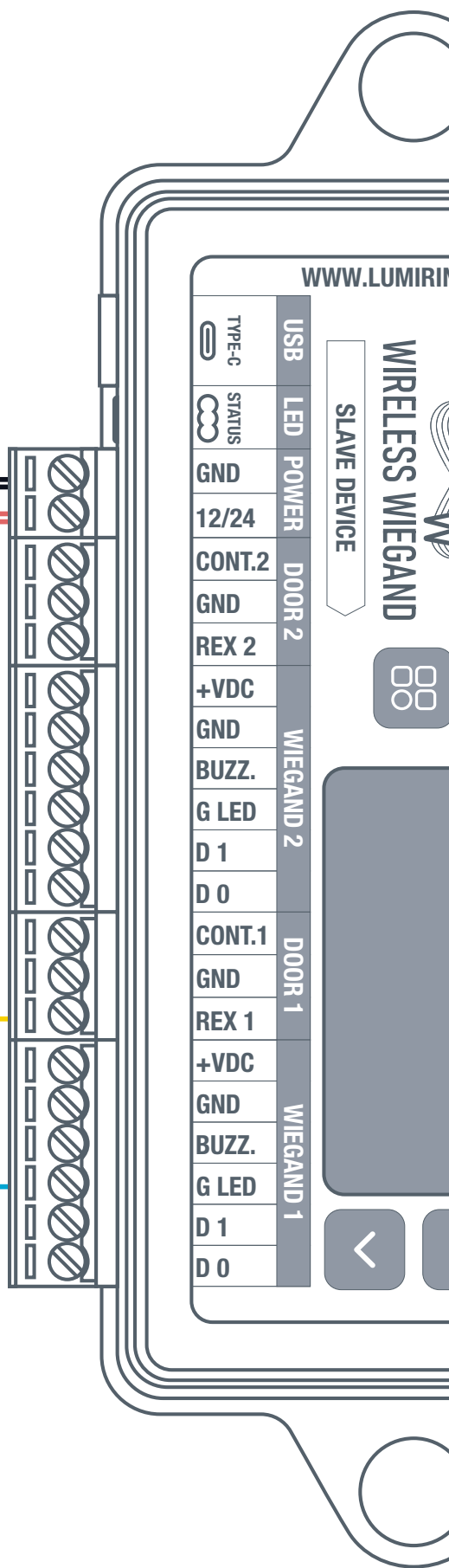
## Controller & Gate Slave modes: AIR-Button V 3.0

### Connection Diagram

# AIR-B (V 3.0 Five-Wire)



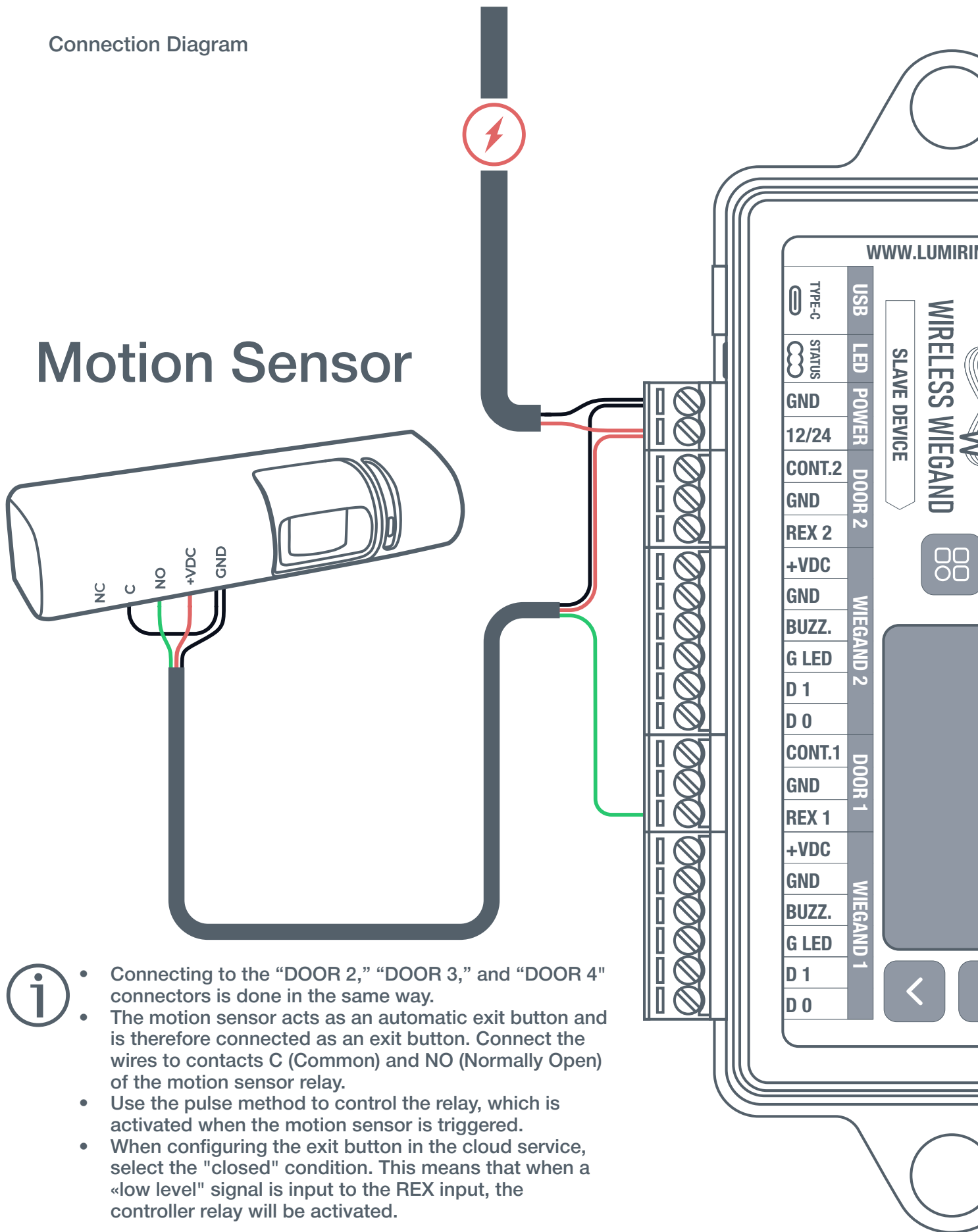
- Connecting to the "DOOR 2," "DOOR 3," and "DOOR 4" connectors is done in the same way.
- The buttons is default factory settings is "Normally Open."
- This means that a low level signal for control will appear on the blue wire when you put your hand to the optical sensor.
- When setting the exit button 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.





## Controller & Gate Slave modes: Request to Exit PIR Motion Sensor

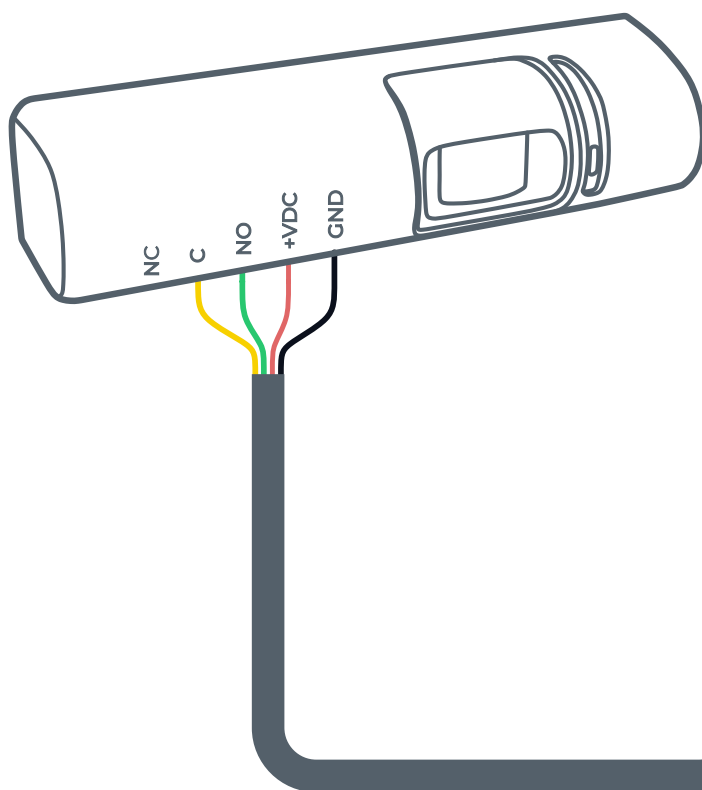
### Connection Diagram



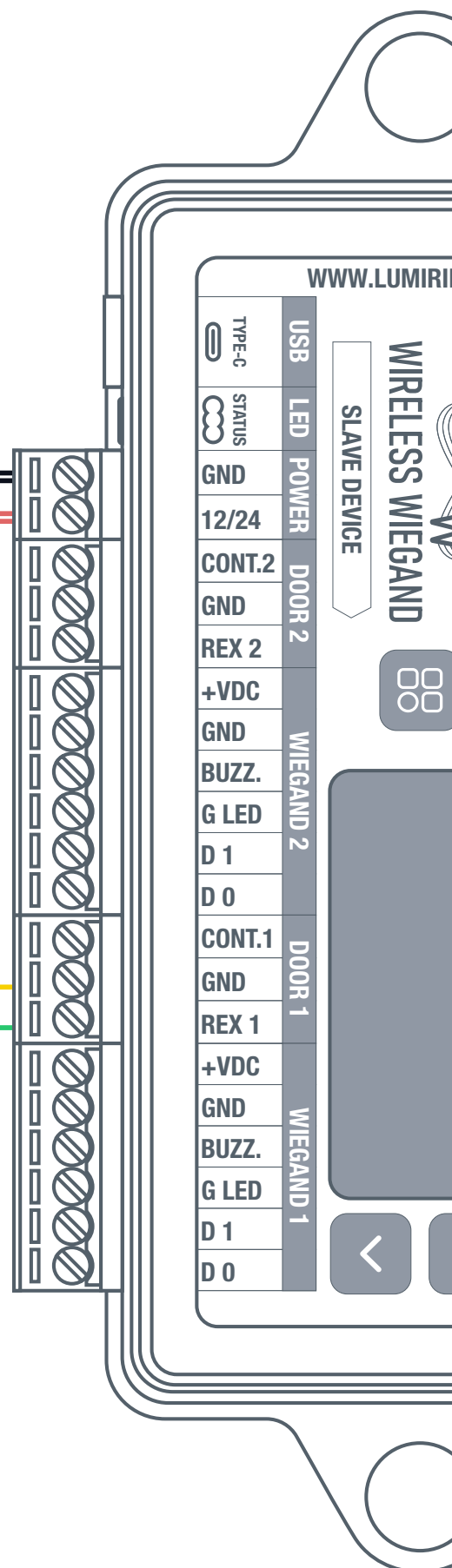
## Controller & Gate Slave modes: Request to Exit PIR Motion Sensor

### Connection Diagram

# 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.

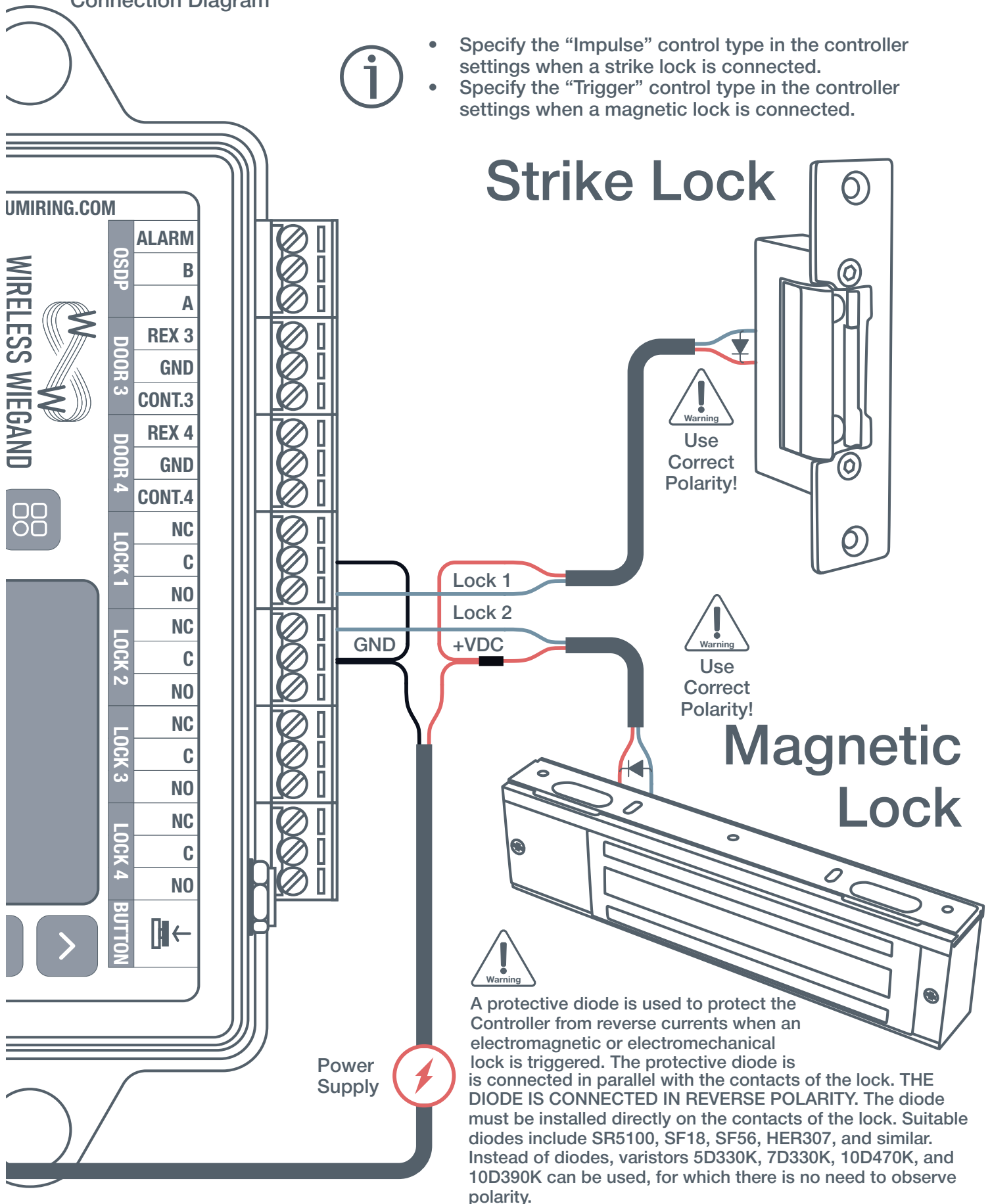


## Controller & Gate Slave modes: Electric Locks

### Connection Diagram



- 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.

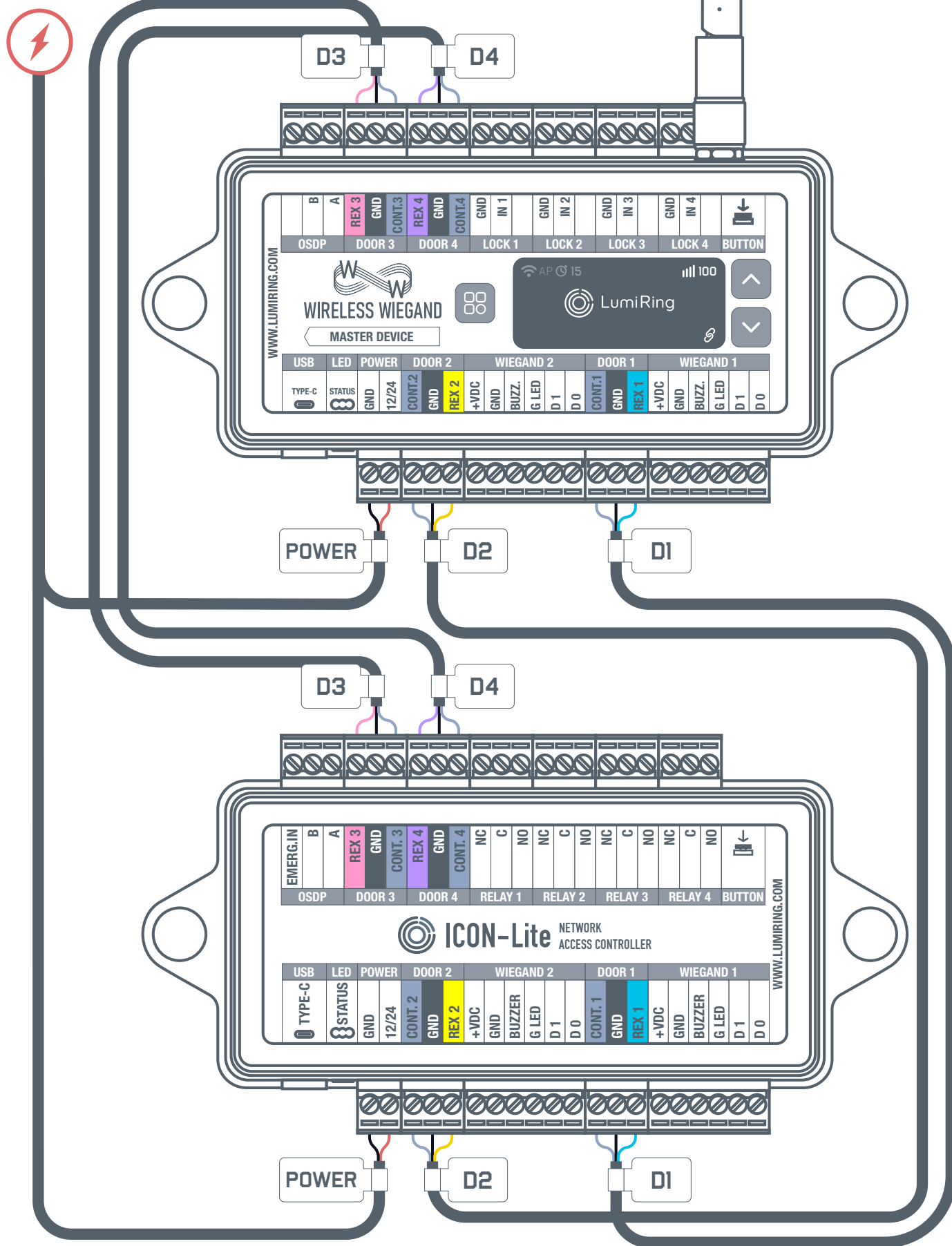


## Connection Diagram to the ICON-Lite Controller



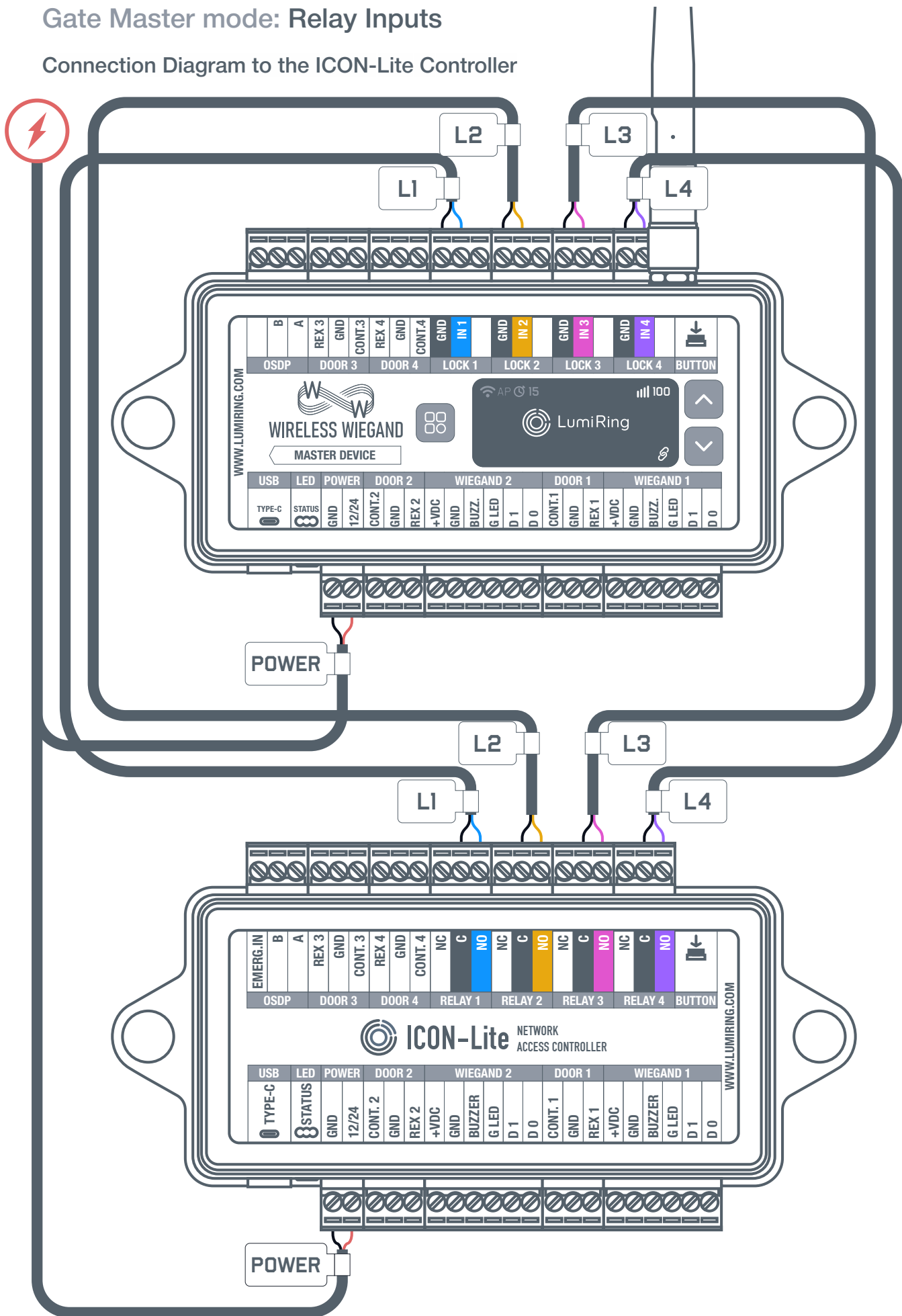
# Gate Master mode: REX Outputs, Contact Outputs

## Connection Diagram to the ICON-Lite Controller



## Gate Master mode: Relay Inputs

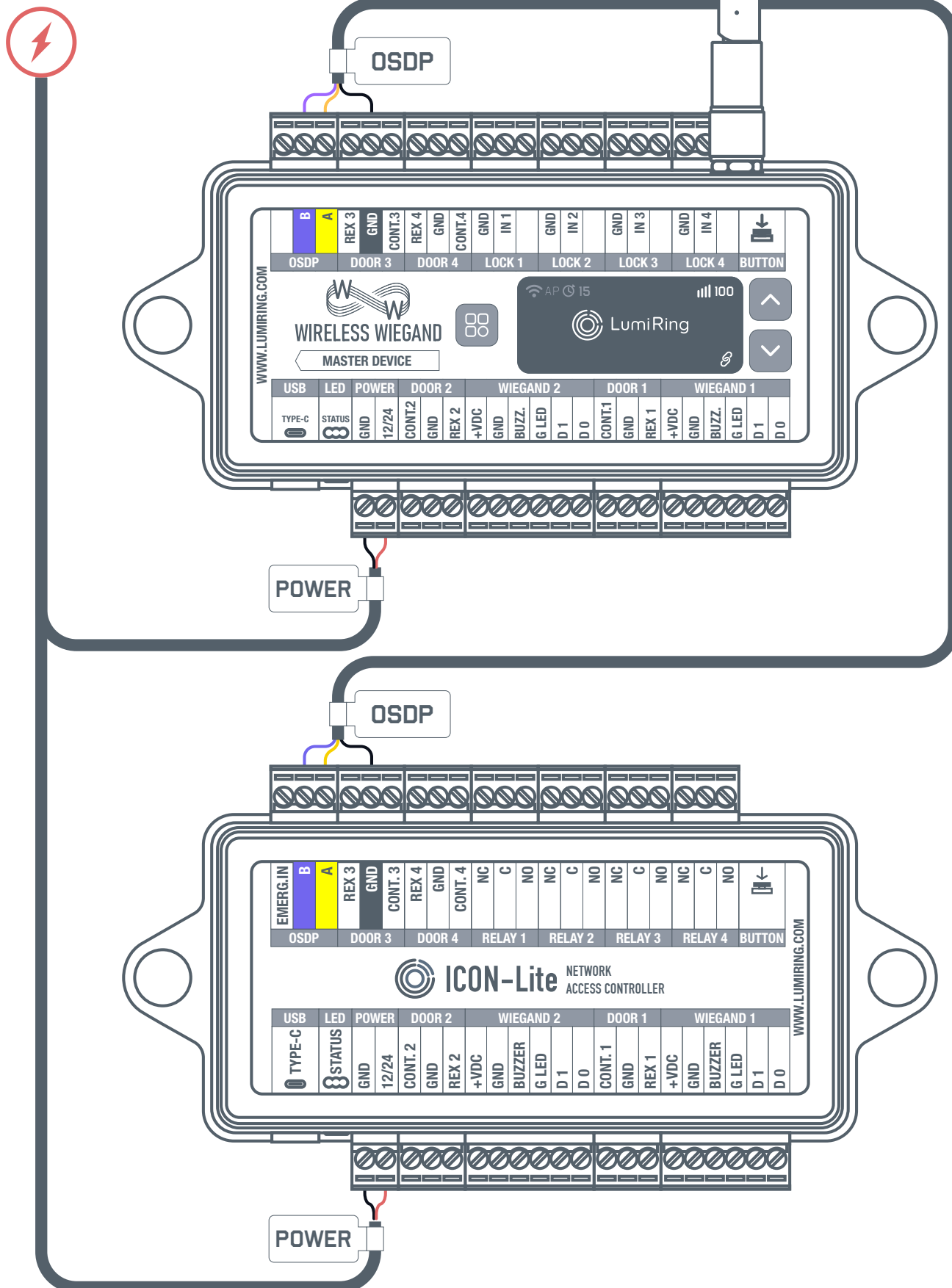
### Connection Diagram to the ICON-Lite Controller



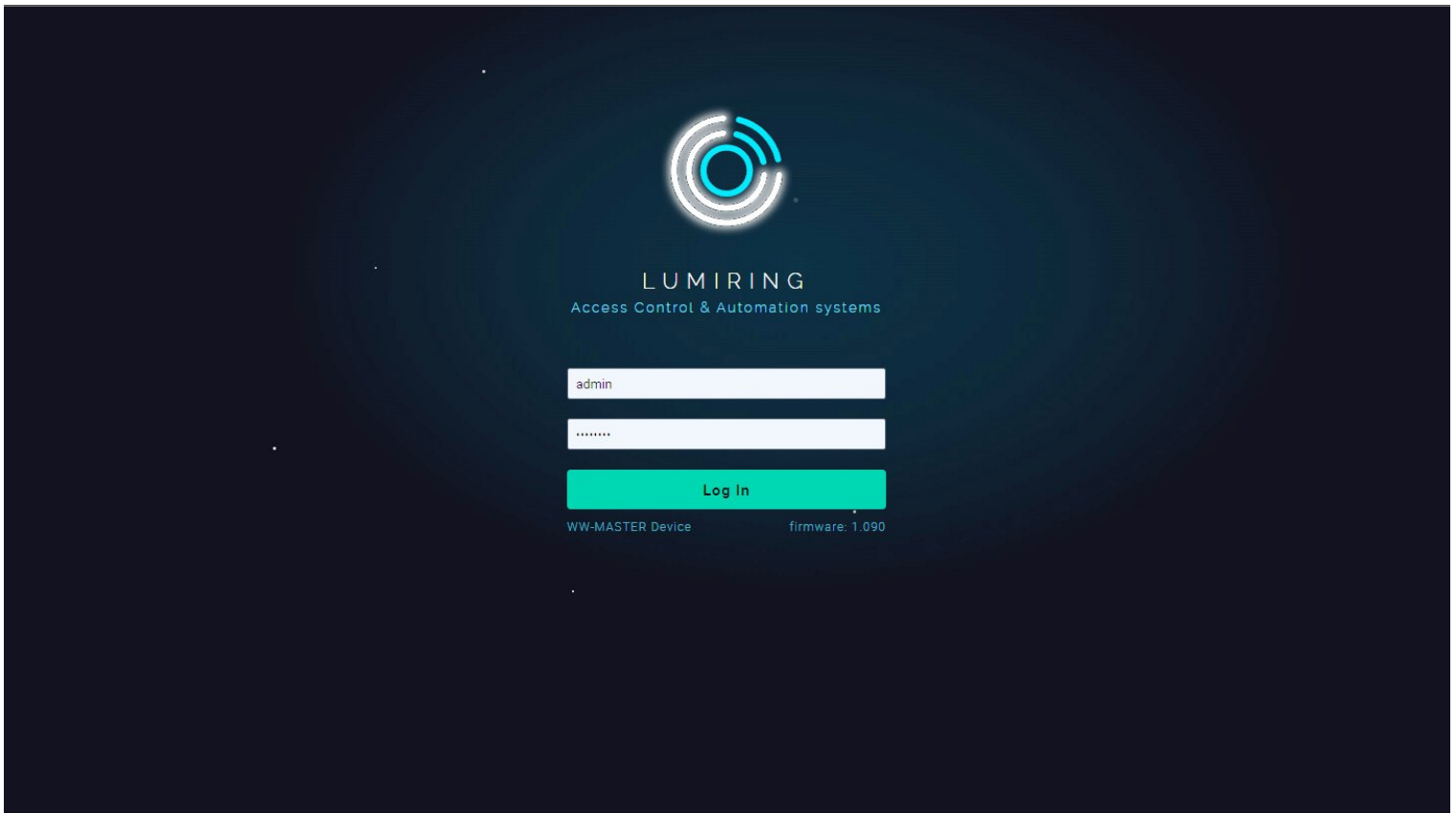
Coming Soon!

## Gate Master mode: OSDP Output

Connection Diagram to the ICON-Lite Controller



## Login



### Connecting to a Wi-Fi Access Point

#### Connecting to the built-in web server

**Step 1.** Connect the device to the +12 VDC power supply. Wait for the device to start up.

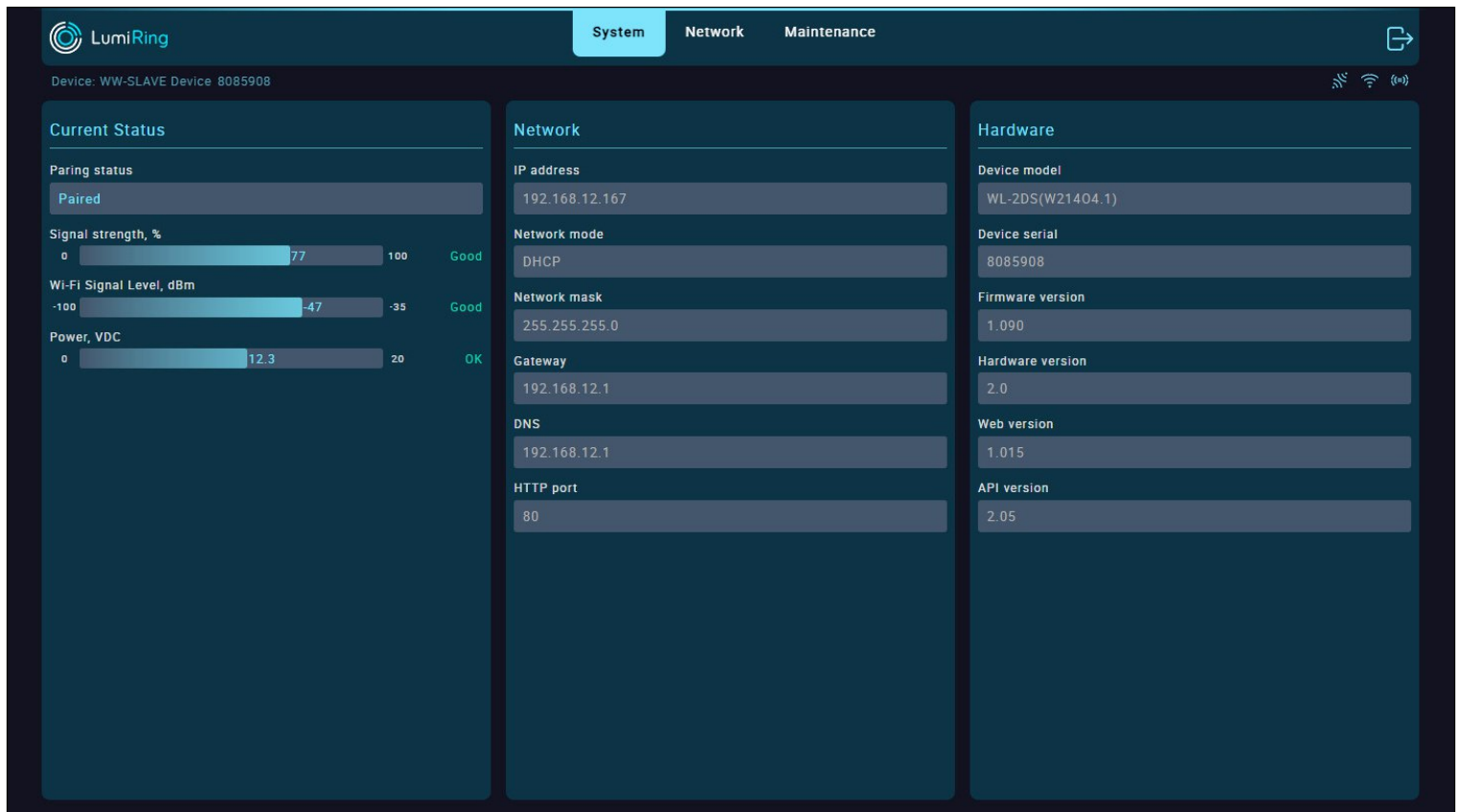
**Step 2.** Quickly press the button near the antenna and then release it to turn on the Wi-Fi hotspot.

**Step 3.** From your PC or cell phone, search for Wi-Fi networks. Select the device named WW\_MD\_xxxxxxxx or WW\_SD\_xxxxxxxx and click Connect.

**Step 4.** 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 5.** 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."





The System section displays the current status of the device, advanced network connection information, and device version information.

### The Current Status column contains the:

- Status of the connection with the pairing device.
- Radio signal strength.
- Connection level when connected to the Wi-Fi router.
- Power supply voltage level.

### The Network column contains the:

- IP address used by the device.
- Network mode - Manual or Dynamic Host Configuration Protocol (DHCP).
- Network mask.

- Gateway.
- Domain Name System (DNS).
- Hypertext Transfer Protocol (HTTP) port used by the device.

### The Hardware column contains the:

- Device model.
- Device serial number.
- Firmware version.
- Hardware version.
- Web version.
- Application programming interface (API) version.

Device: WW-SLAVE Device 8085908

### Network

SSID name  
Lumining

Password  
.....

Connection mode  
☒ DHCP ☐ Manual

IP address  
192.168.12.167

Network mask  
255.255.255.0

Gateway  
192.168.12.1

DNS  
192.168.12.1

Connect

### Wi-Fi AP

Local Wi-Fi AP name  
WW\_SD\_8085908

Password (8 characters minimum)  
Enter password

☐ 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.

Wi-Fi timer, min (1 - 60, off time)  
15

The timer is designed to disable the built-in Wi-Fi AP after a specific time after activation to enhance network security.

HTTP port  
80

### Radio Settings

Relay blocking prevention  
This feature prevents the relay from getting blocked. If the communication with the master is lost, the chosen relays will revert to their previous state after the specified time in the Timer field.

Timer, s (1 - 30)  
2

☐ Relay 1 ☐ Relay 2 ☐ Relay 3 ☐ Relay 4

The Network section provides the ability to configure the built-in Wi-Fi hotspot, including connecting to the Internet, changing the Wi-Fi network name, and setting a password.

## Network

- Click in the SSID Name field to search for available Wi-Fi networks and enter the password to connect.
- If the network to connect to is hidden, wait for the search results and enter the network name manually.
- Select DHCP to get automatic network settings or Manual to enter network settings manually, then click "Connect."

## Wi-Fi Access Point (AP)

- In the "Local Wi-Fi AP Name" field, enter the network name of the device.
- In the "Password" field, enter the connection password (not set by default).

## Hidden Mode

- The "Enable Hidden Mode" checkbox hides the network name of the device's access point when searching.

- To connect to the device when it is in hidden mode, you need to know its name and enter it manually when connecting.

## Wi-Fi timer

- In the "Wi-Fi timer, min" field, enter a value from 1 to 60 minutes. If you enter 0, the AP will be always on when the service button is pressed.

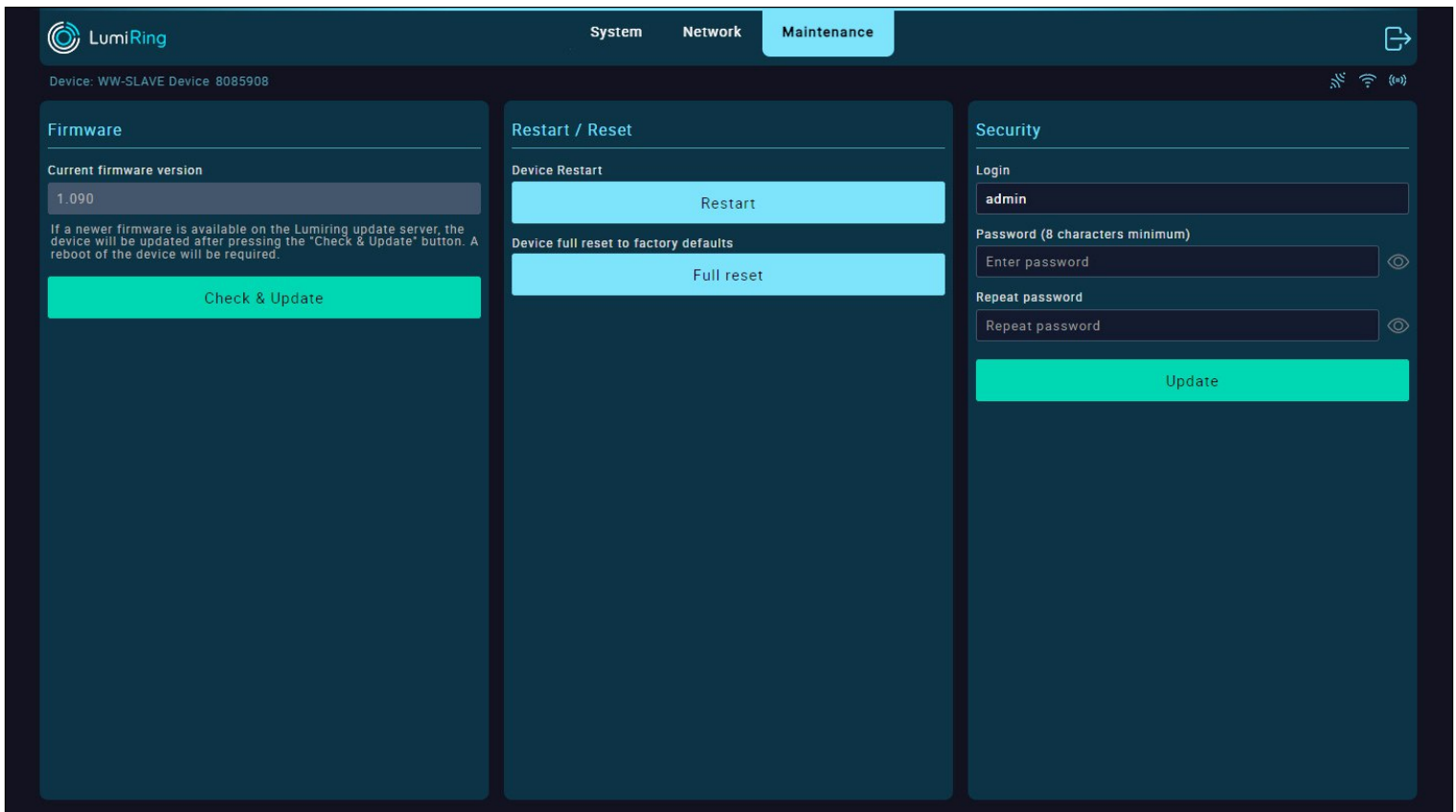
## HTTP port

- Used to access the Web interface of the device.
- By default, the device uses port 80.

## Relay blocking prevention

**Note: The function is only configurable on the slave device.**

- This feature prevents the relay from getting blocking.
- If the communication with the master device is lost, the chosen relays will revert to their previous state after the specified time in the Timer field.



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.

## Firmware Update via Cloud Server

### Device features:

- The Wi-Fi receiving module supports connection to networks operating on 2.4 GHz only.
- You can manually enter the SSID name of the Wi-Fi network to connect to hidden networks. To do so, after the end of the search, start typing the network name in the current field.
- Changing the Wi-Fi router connection parameters from the current one to a new one happens only after the device power reset.
- The built-in Wi-Fi AP is disabled every time the device is rebooted or when the built-in timer expires.
- The device requires a high amount of bandwidth to download the firmware version from the update server. Ensure a quality connection and connection level.
- The device update may be interrupted if radio communication with the responder is in progress.
- If the connection is lost or rebooted during the download, the update operation will be canceled in order to save the current firmware version.
- The device may malfunction if the power is turned off during the update installation.

### Preliminary preparation:

*BE SURE TO COMPLETE ALL PREREQUISITE STEPS BEFORE YOU START UPDATING YOUR DEVICE!*

*FAILURE TO FOLLOW THE PRECAUTIONARY MEASURES FOR THE UPDATE MAY RESULT IN THE DEVICE NOT SWITCHING ON, SWITCHING ON WITH LIMITED FUNCTIONALITY, OR MALFUNCTIONING.*

*IN CASE OF INCORRECT UPDATE INSTALLATION DUE TO POWER FAILURE, THE DEVICE MAY NOT BE ABLE TO BE USED UNTIL THE DEVICE IS REPROGRAMMED VIA USB CABLE.*

- Disconnect all input, output, and reader connectors except the power supply. The device must not receive/transmit data and must not process I/O status during the upgrade.
- Turn off the power to the kit's responder. The responder may continue transmitting data to the device being upgraded, which may interrupt the upgrade process and should therefore be turned off.
- Place the device in direct line of sight from a Wi-Fi router with Internet access at a distance of no more than 3.3 to 6.5 feet (1-2 meters). You can use a smartphone with an activated access point (AP) as a Wi-Fi router.
- Before starting the update, reset the power and wait for the device screen to load.

### Actions with the device:

- Turn on the Wi-Fi AP by pressing the service button on the side of the device.

- Search for Wi-Fi networks on your mobile device and connect to the device's AP. While connecting, check the box to connect automatically.
- Open a Web browser and type 192.168.4.1 in the address bar. Press Enter and wait for the login page to load.
- Enter your login and password.
- Click the Network tab and search for an available Wi-Fi network with Internet access.
- Select your preferred network, enter the password to connect, and click Connect.
- Click the System tab to make sure that the signal strength of the Wi-Fi connection is at least -40 dBm. A reading of -35 dBm is the best connection quality, and -100 dBm is the worst or none.
- Go to the Maintenance tab and click the "Check & Update" button. Wait for the update download to complete.

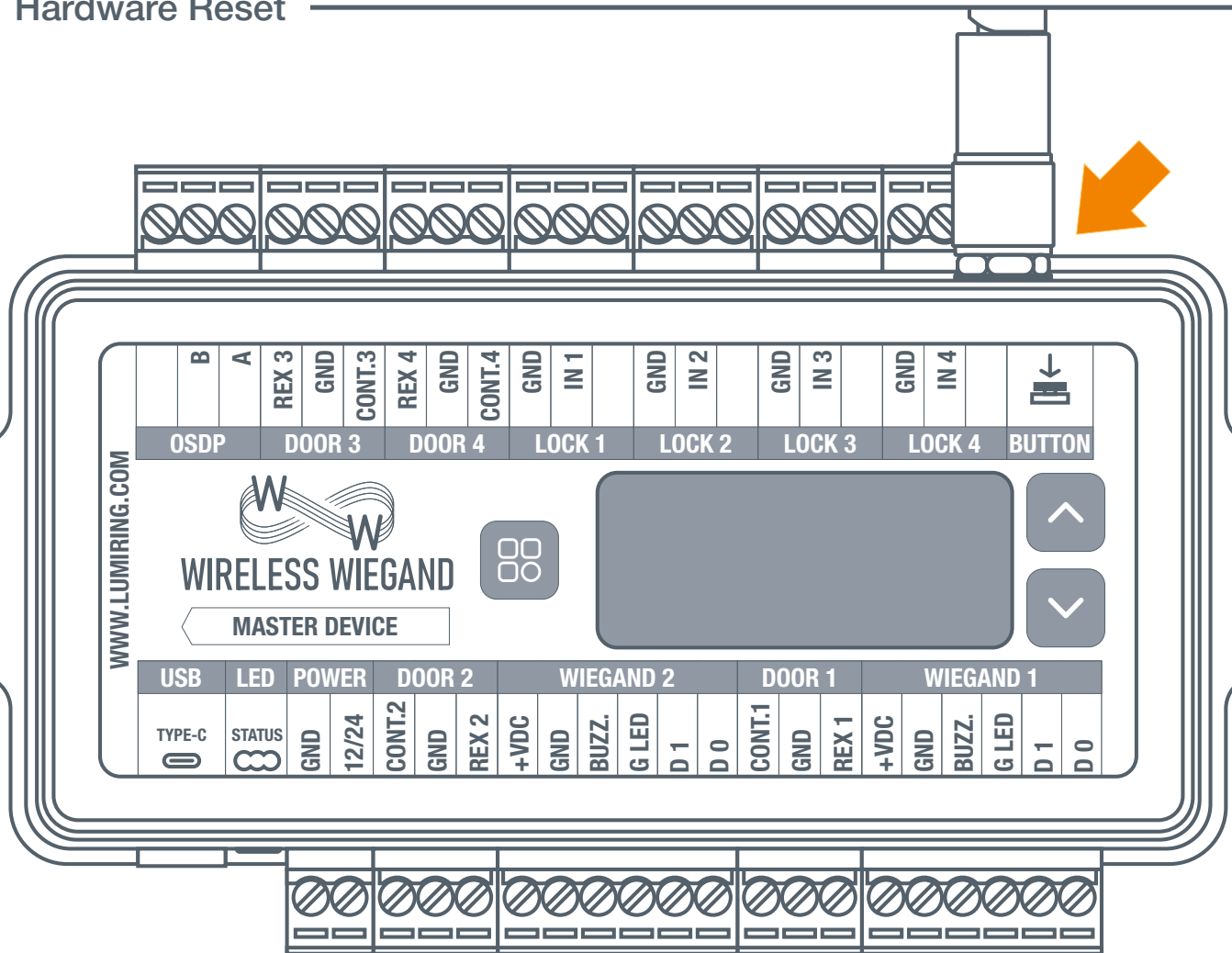
*DO NOT DISCONNECT THE DEVICE FROM THE POWER SOURCE WHILE DOWNLOADING THE UPDATE.*

- When the update is complete, a notification will appear prompting you to reboot. Click "Ok" and wait for the device to restart with an audible beep.
- Power cycle the device and wait for the screen to load. Press the Down button to make sure that the firmware version has changed to the current one.

### Troubleshooting:

- The message "An error occurred during the update" may be displayed in the even of a momentary loss of communication with the device, the response time being exceeded, or an unstable connection to the server. In these situations, the update progress will be stopped at the current value. If after the error occurs, the device remains connected and the "Check & Update" button is clickable, try to update again.
- If the error occurs at 95% or more of the load, wait 30 seconds and reset the device power supply. After starting the device, check the version displayed on the display screen. The firmware may have been downloaded and installed, but the device has not responded after application.
- If interface interaction is no longer available after the error occurs, check the connection status of the built-in Wi-Fi AP. Make sure that the device's Wi-Fi AP is active and you can connect to it. If you are unable to connect to the device, reset the power of the device, activate the Wi-Fi AP, and try to connect again.

## Hardware Reset



### Hardware Reset

1. Hold the button down for 10 seconds.
2. Wait for yellow-blue flashing and a long beep.
3. Release the button.
4. Three consecutive beeps and one separate beep will sound.
5. The LED will first turn red and then change to flashing blue.
6. The hardware reset procedure is complete and the unit is ready for operation.

## 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.

## Supported Reader Models

| Manufacturer                                                                        | Model Name                        | Device Type     |
|-------------------------------------------------------------------------------------|-----------------------------------|-----------------|
| <b>HID</b>                                                                          | Signo 40K 40NKS-00-00027F         | Reader & Keypad |
|                                                                                     | Signo 40 40NKS-01-00001H          | Reader          |
|                                                                                     | iCLASS RPK40 6136AKN000D00-G3.0   | Reader & Keypad |
|                                                                                     | iCLASS RPK40 6130BKN040D00-G3.0   | Reader & Keypad |
|                                                                                     | iCLASS SE R10 900NTNNEK00000-L001 | Reader          |
|                                                                                     | iCLASS SE R10 900NNNTEK2037P      | Reader          |
|                                                                                     | iCLASS SE R40 920PTNNEK00000      | Reader          |
|                                                                                     | multiCLASS RP40 6125CKN0007-G3.0  | Reader          |
|                                                                                     | multiCLASS SE RP15 910PTNNEK00000 | Reader          |
|                                                                                     | multiCLASS SE RP40 920PMNNEKMA01Y | Reader          |
|                                                                                     | multiCLASS SE RP40 920PTNNEK00000 | Reader          |
|                                                                                     | Prox Pro II 5455BKN00             | Reader          |
|                                                                                     | ThinLine II 5395CG100             | Reader          |
| <b>PDK</b>                                                                          | PP-08-RDR-G                       | Reader          |
| <b>BRIVO</b>                                                                        | B-BSPSF                           | Reader          |
|  | B-BSPKF                           | Reader & Keypad |
| <b>LUMIRING</b>                                                                     | AIR-R RA-2                        | Reader          |
| <b>ETE</b>                                                                          | CTI 1200                          | Reader & Keypad |
| <b>U-PROX</b>                                                                       | SE keypad                         | Reader          |
|                                                                                     | SE mini                           | Reader          |
| <b>PAXTON*</b>                                                                      | 345-220-US                        | Reader          |
| <b>OPENPATH**</b>                                                                   | OP-RHF-STD                        | Reader          |

\*, \*\* - Developments are currently underway to support this model



### FCC Statement

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

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

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.

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.