2026-05-19 Fw.v. 1.143 Hw.v. RA-2R / REV.1.09
V 3.3

Federal Communications Commissions

MANUAL

AIR-CR

CONTENTS

Introduction

This document provides detailed information on the structure of the device as well as the steps to install and connect it.

It also includes instructions for preventing or troubleshooting many common problems. This guide is for informational purposes only, and the actual product takes precedence in case of any discrepancies.

All instructions, software, and functionality are subject to change without prior notice. The latest version of the manual and additional documentation can be found on our website or by contacting customer support.

The user or installer is responsible for complying with local laws and privacy regulations when collecting personal data while using the product.

Device Specifications

Voltage:

- 12 or 24 VDC operation
- 0.15A @12 VDC, 0.075A @ 24 VDC current consumption

Outputs:

- One outputs (open collector) 0.5A @ 12 VDC

Inputs:

- Two inputs (dry contact type) from 0 to 5 volts

Communication interfaces:

- Wi-Fi 802.11 b/g/n 2.4 GHz
- Ethernet with the RJ-45 adapter (10/100 Mbit)
- Bluetooth® 5 (LE)
- Wiegand 4, 8, 26, 32, 33, 34, 35, 36, 37, 40, 42, 48, 56 bit
- OSDP via RS-485

Memory storage:

- 30,000 cards
- 450,000 events

RFID 125 kHz support:

- EM Marine

RFID 13.56 MHZ support:

- MIFARE DESFire; MIFARE Plus; MIFARE Ultra Light; MIFARE Classic mini/1K/4K; MIFARE Classic EV1 1K/4K; NFC Tag

Support copy protection:

- MIFARE Classic mini/1K/4K

Demensions (D x H):

- 2.36" x 0.67" (60 x 17 mm)
- 2.36" x 0.86" (60 x 22 mm) mounting ring

Mounting method:

- Wall mount

Weight:

- 1.59 oz (45 g)

Operation temperature:

- -22°F ~ 158°F (-30°C ~ 70°C)

Ingress protection rating:

- IP 65

Default Device Settings

Wi-Fi device name when searching:

- AIR-CR_(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

RFID 125 kHz:

- Enabled

RFID 13.56 MHz:

- Enabled

Copy protection:

- Disabled

Bluetooth:

- Enabled

AP Wi-Fi timer:

- 30 minutes

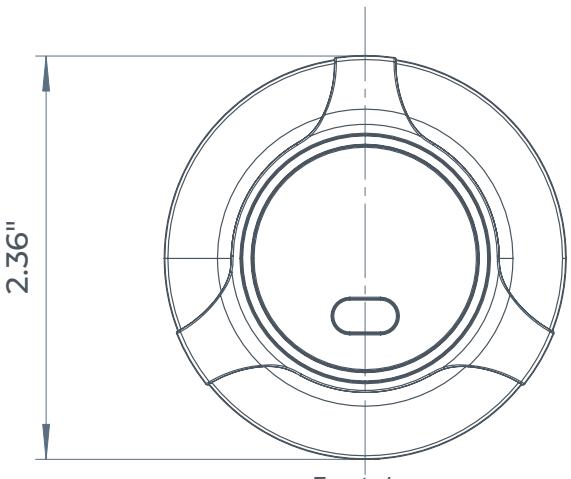
Wiegand format 125 kHz:

- 26 bit

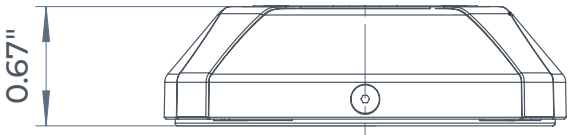
Wiegand format 13.56 MHZ:

- 34 bit

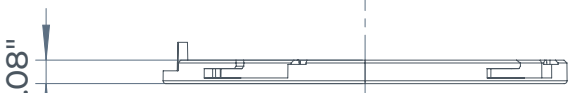
Device Dimension



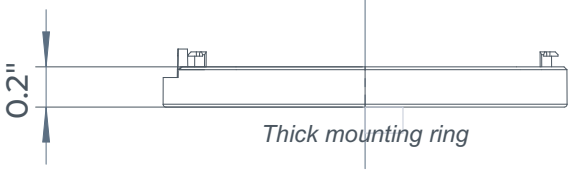
Front view



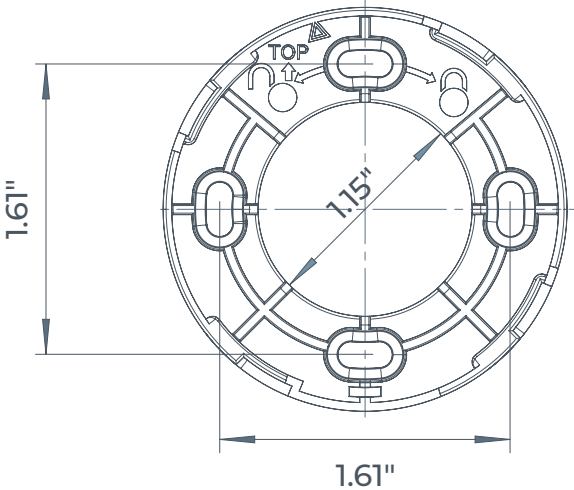
Side view



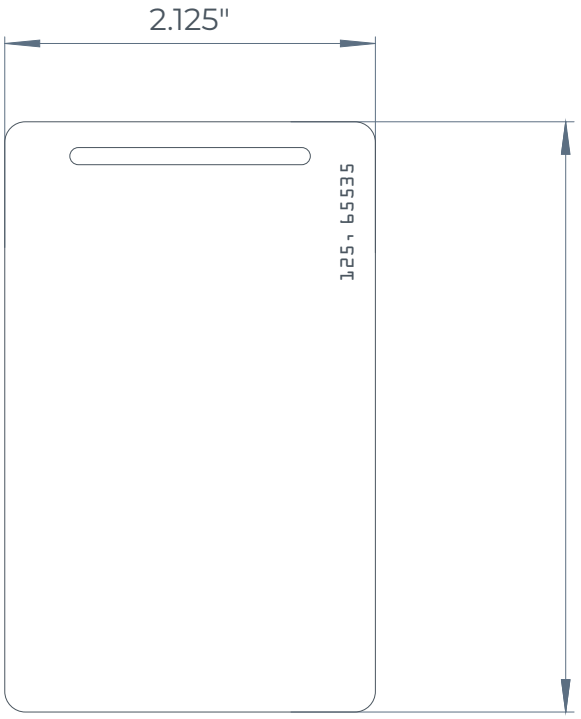
Thin mounting ring



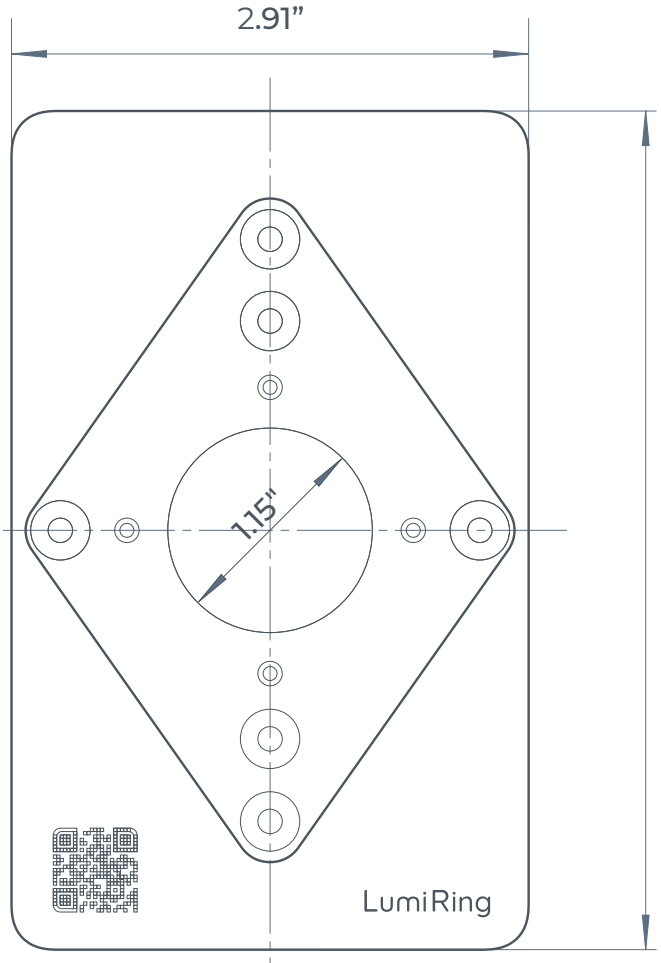
Thick mounting ring



Mounting ring front view

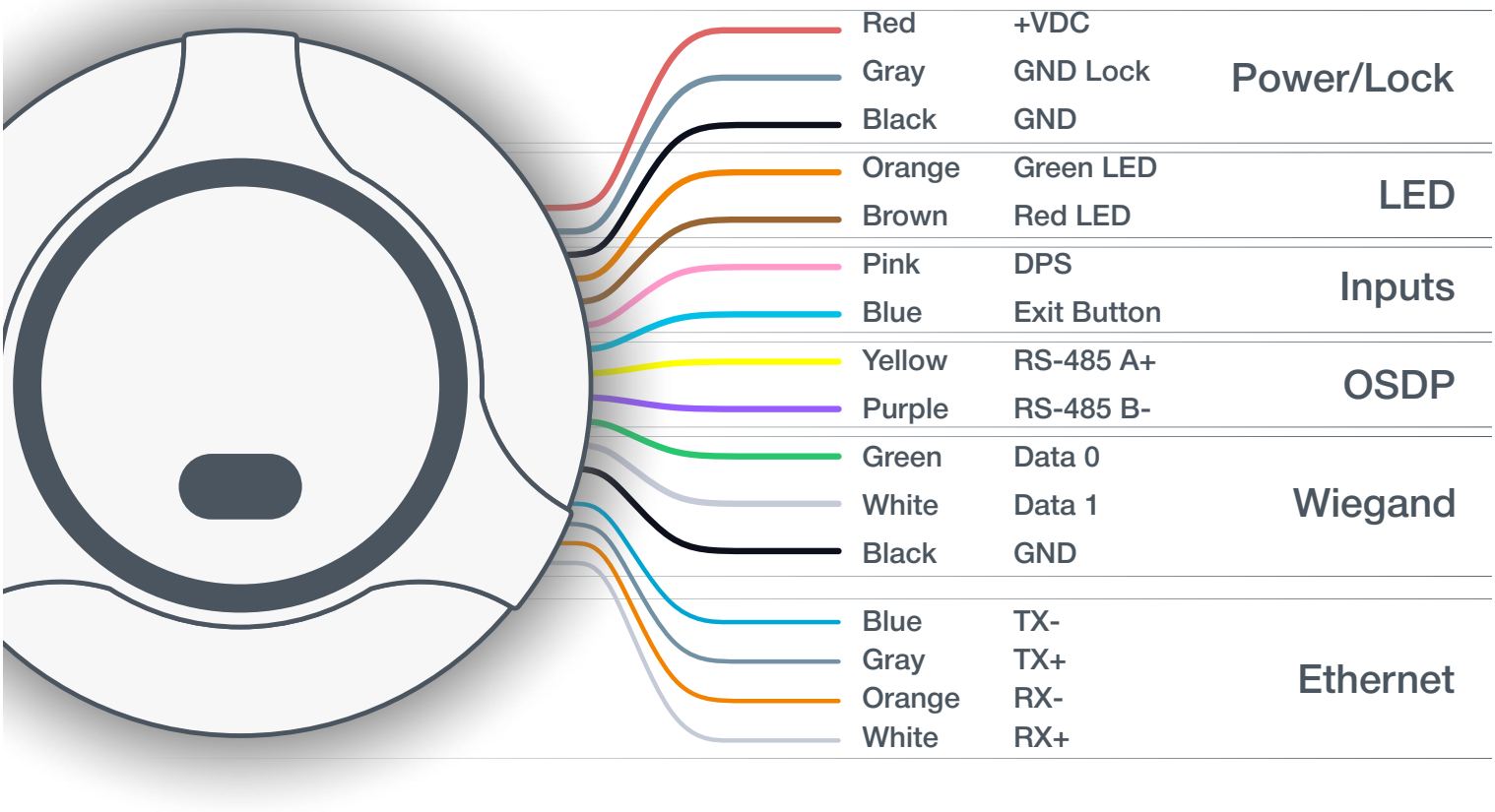


Standard RFID card size



Optional accessory

Wire Designation



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 Cat 5e 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.

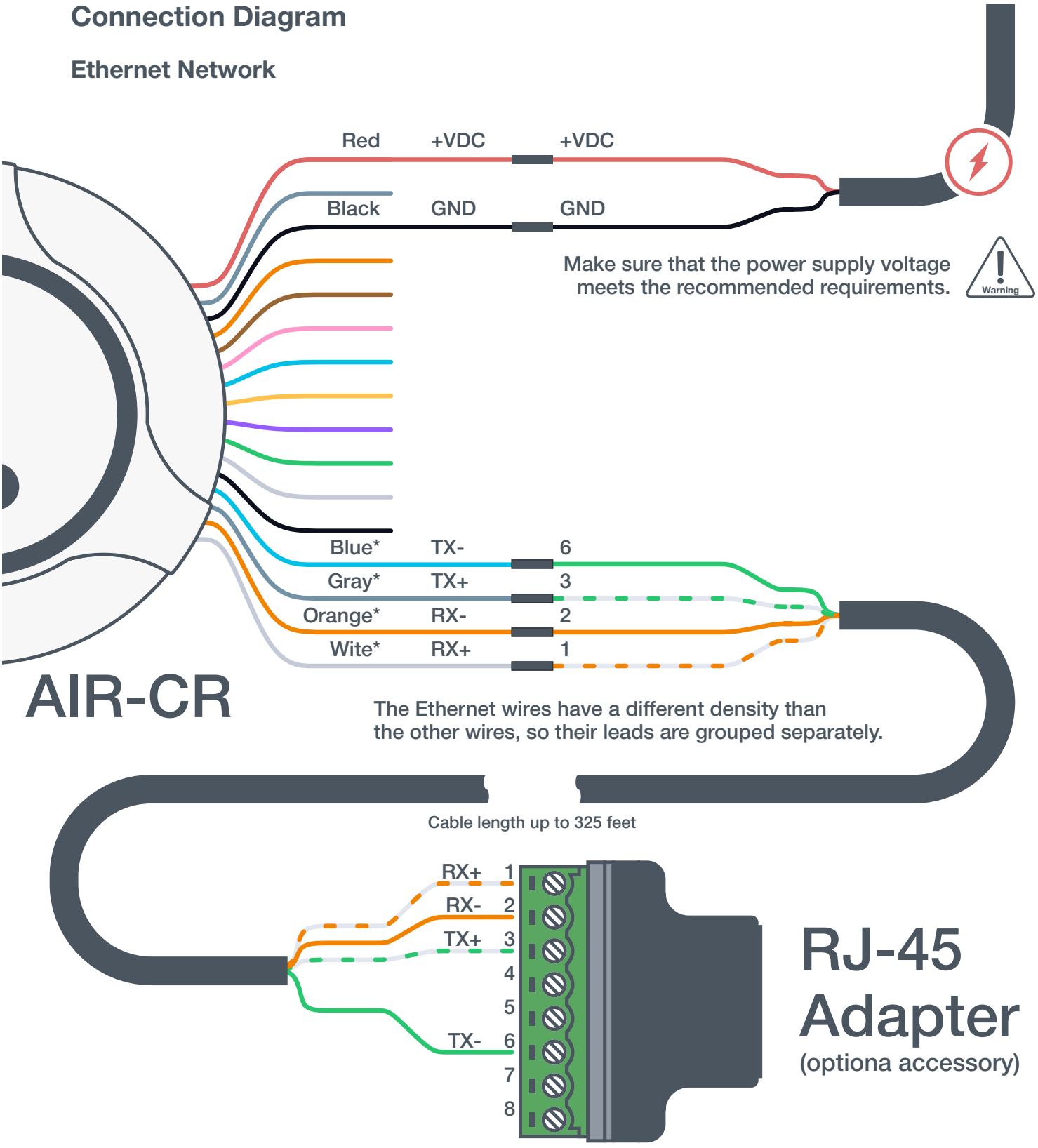
Protection Against High Current Surges

- 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

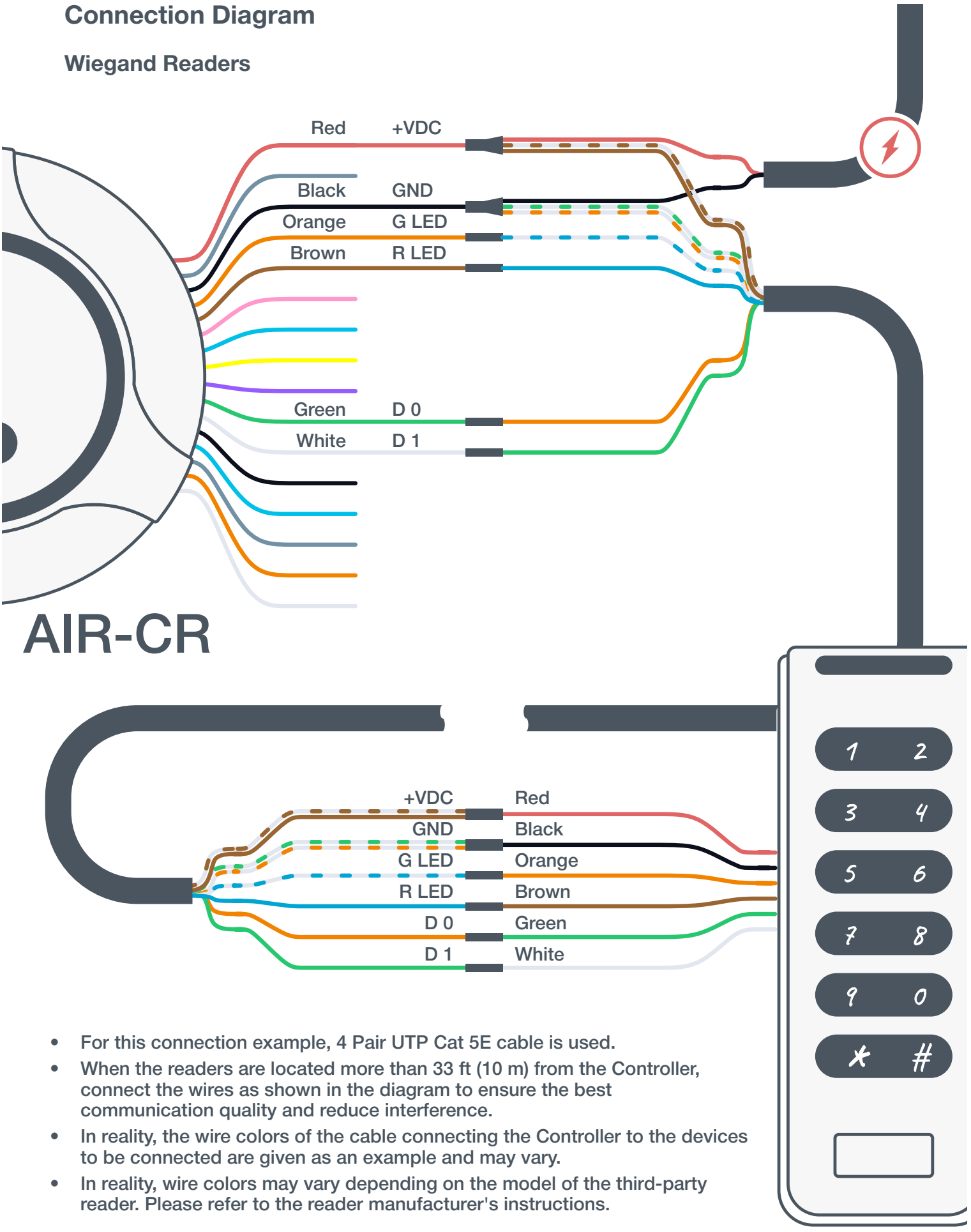
Ethernet Network



- The voltage levels of the power supply and the Controller may differ depending on the cable length and the resistance of the conductor.
- Use a separate power supply to connect the reader if the cable is longer than 165 feet or the voltage at the end of the line is less than 10 volts.
- 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!
- Use a multimeter in the VDC measurement mode to verify that the power supply voltage meets the recommended requirements.

Connection Diagram

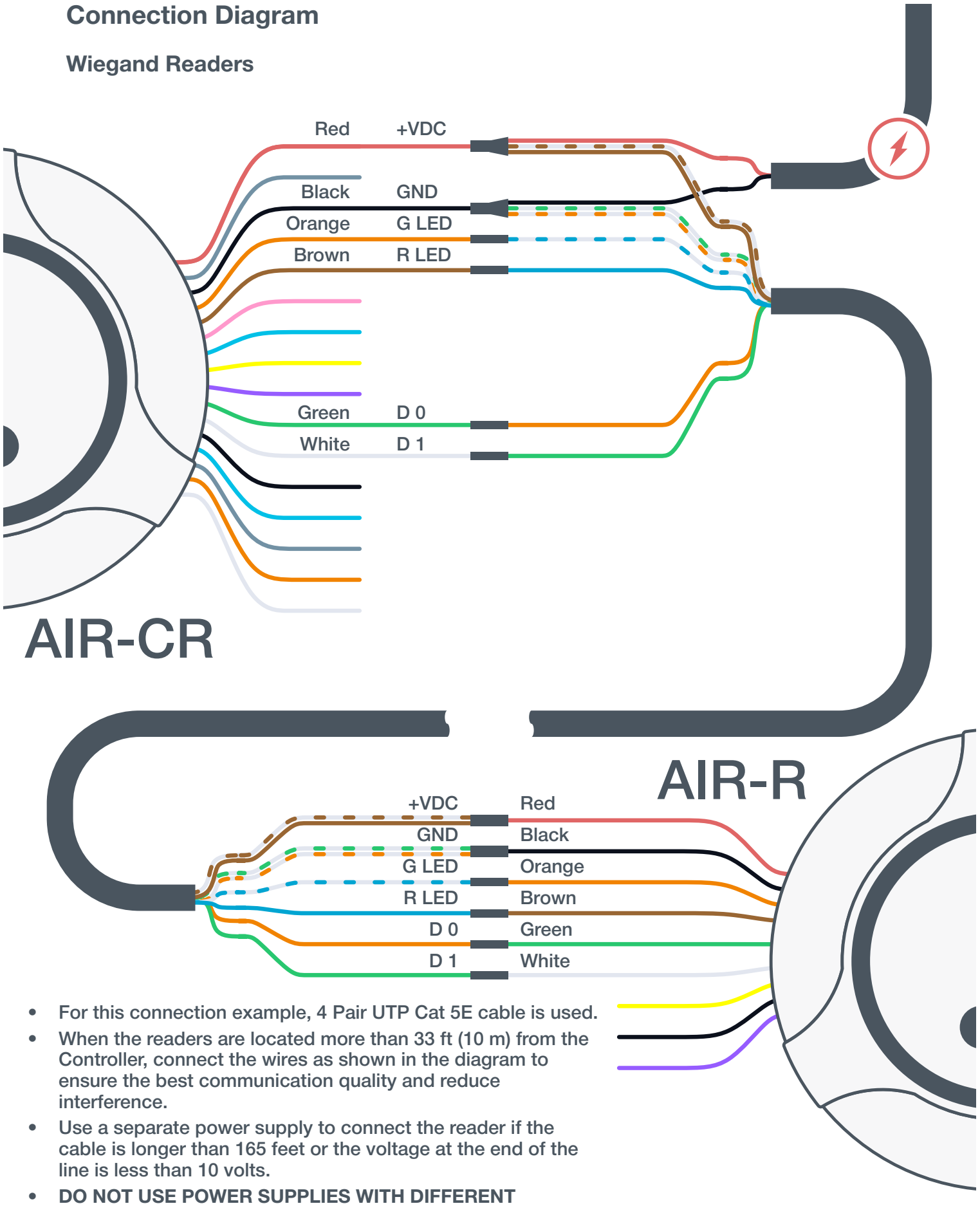
Wiegand Readers



- For this connection example, 4 Pair UTP Cat 5E cable is used.
- When the readers are located more than 33 ft (10 m) from the Controller, connect the wires as shown in the diagram to ensure the best communication quality and reduce interference.
- In reality, the wire colors of the cable connecting the Controller to the devices to be connected are given as an example and may vary.
- 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

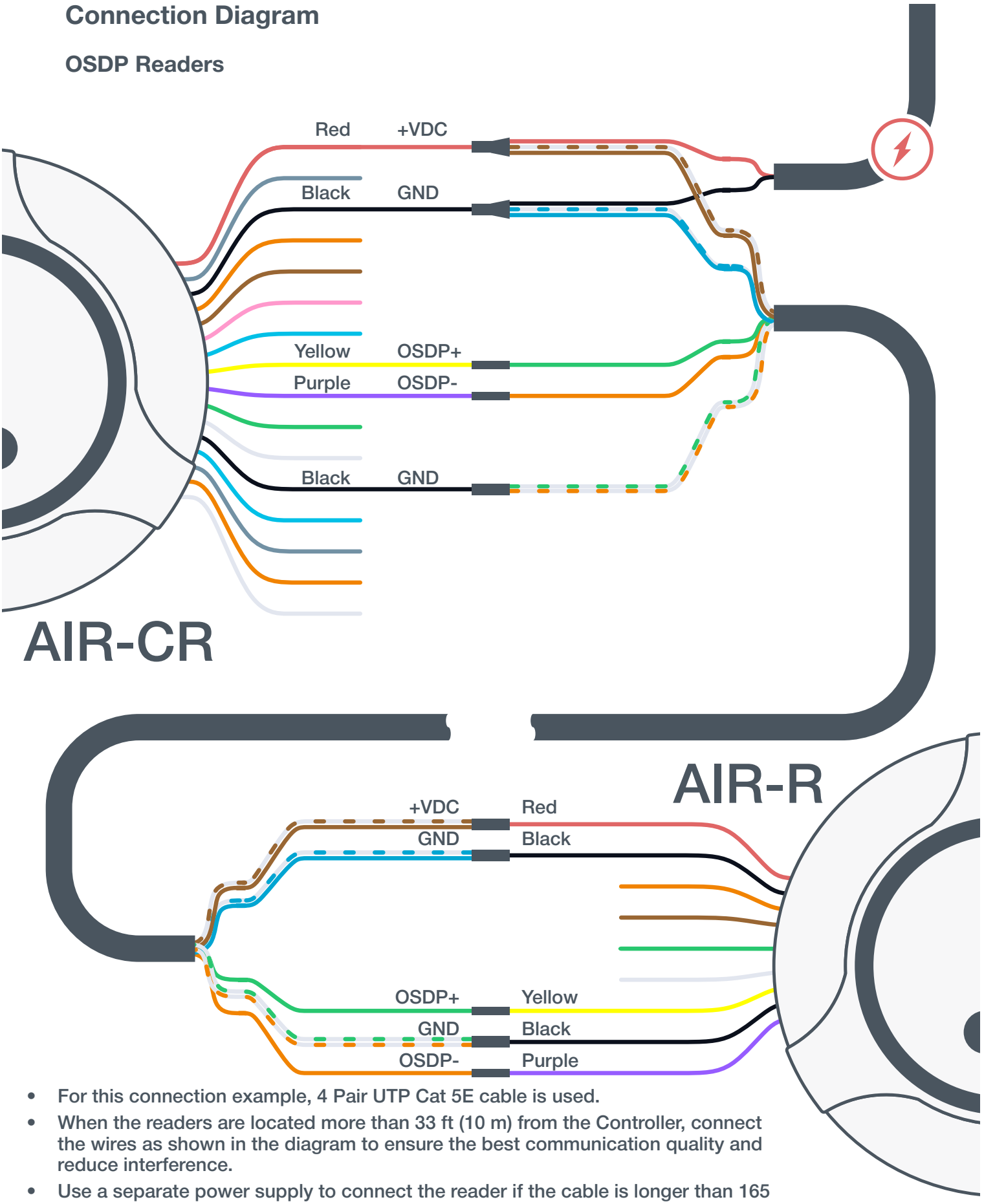
Wiegand Readers



- For this connection example, 4 Pair UTP Cat 5E cable is used.
- When the readers are located more than 33 ft (10 m) from the Controller, connect the wires as shown in the diagram to ensure the best communication quality and reduce interference.
- Use a separate power supply to connect the reader if the cable is longer than 165 feet or the voltage at the end of the line is less than 10 volts.
- **DO NOT USE POWER SUPPLIES WITH DIFFERENT VOLTAGE LEVELS!**

Connection Diagram

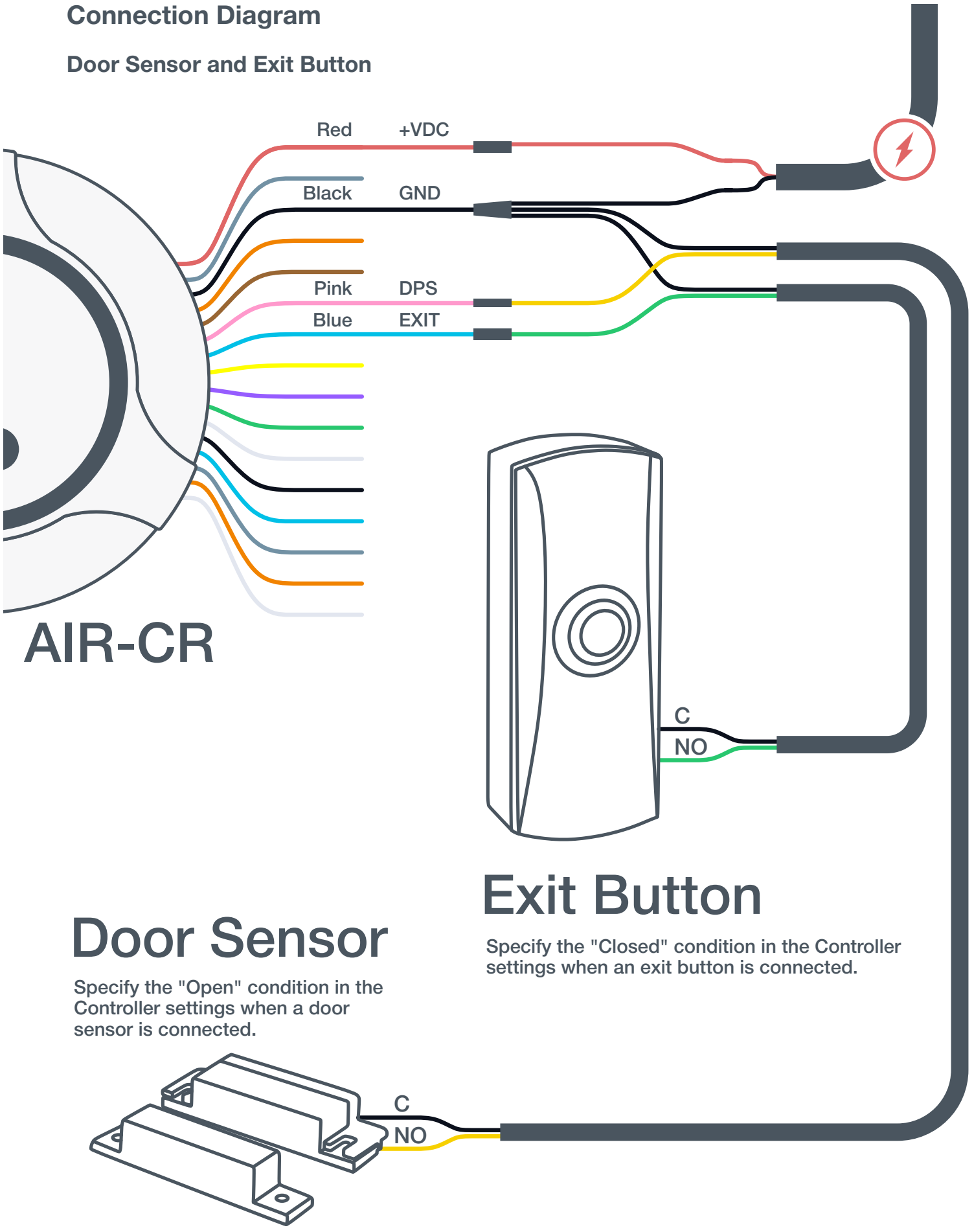
OSDP Readers



- For this connection example, 4 Pair UTP Cat 5E cable is used.
- When the readers are located more than 33 ft (10 m) from the Controller, connect the wires as shown in the diagram to ensure the best communication quality and reduce interference.
- Use a separate power supply to connect the reader if the cable is longer than 165 feet or the voltage at the end of the line is less than 10 volts.
- **DO NOT USE POWER SUPPLIES WITH DIFFERENT VOLTAGE LEVELS!**

Connection Diagram

Door Sensor and Exit Button



Exit Button

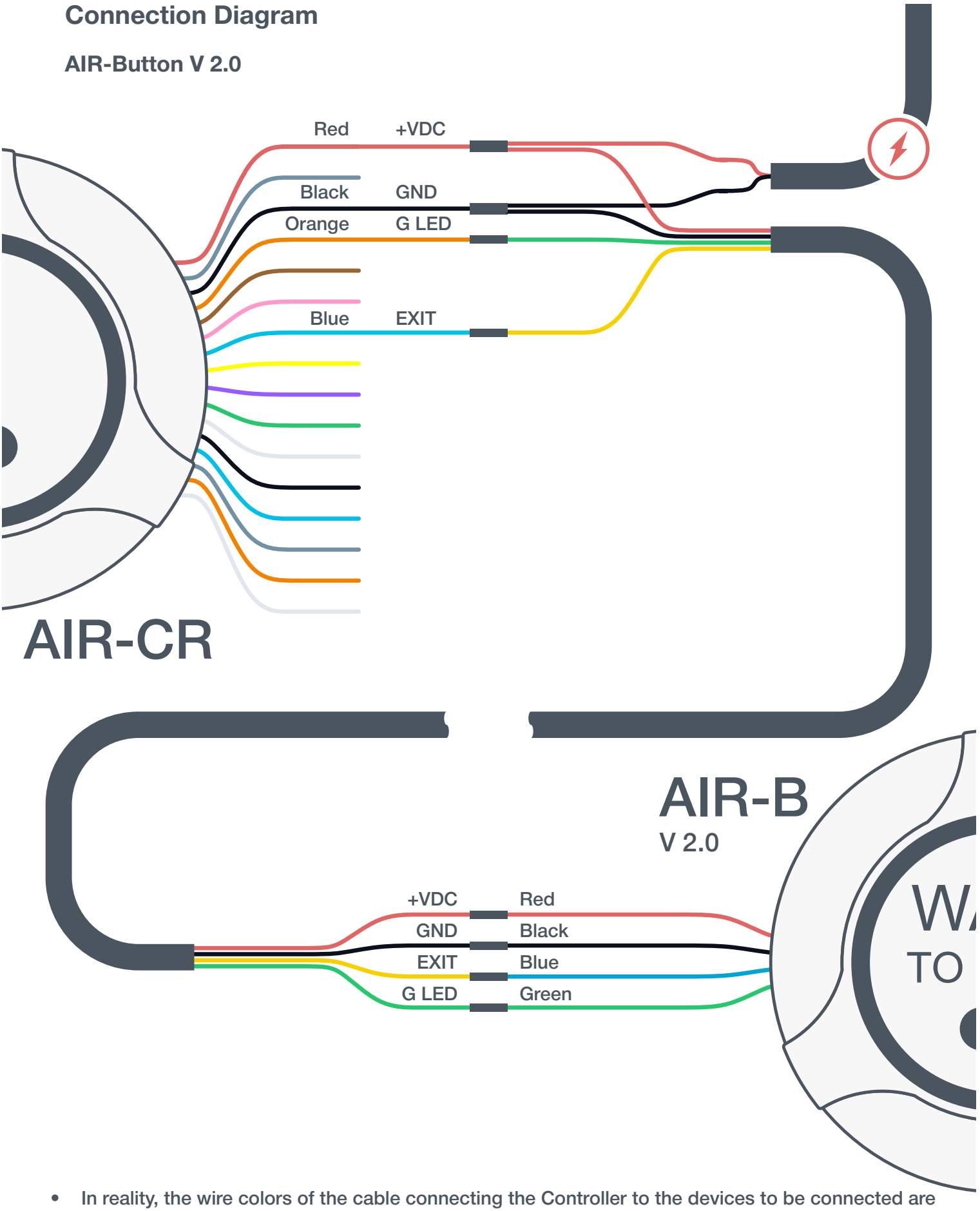
Specify the "Closed" condition in the Controller settings when an exit button is connected.

Door Sensor

Specify the "Open" condition in the Controller settings when a door sensor is connected.

Connection Diagram

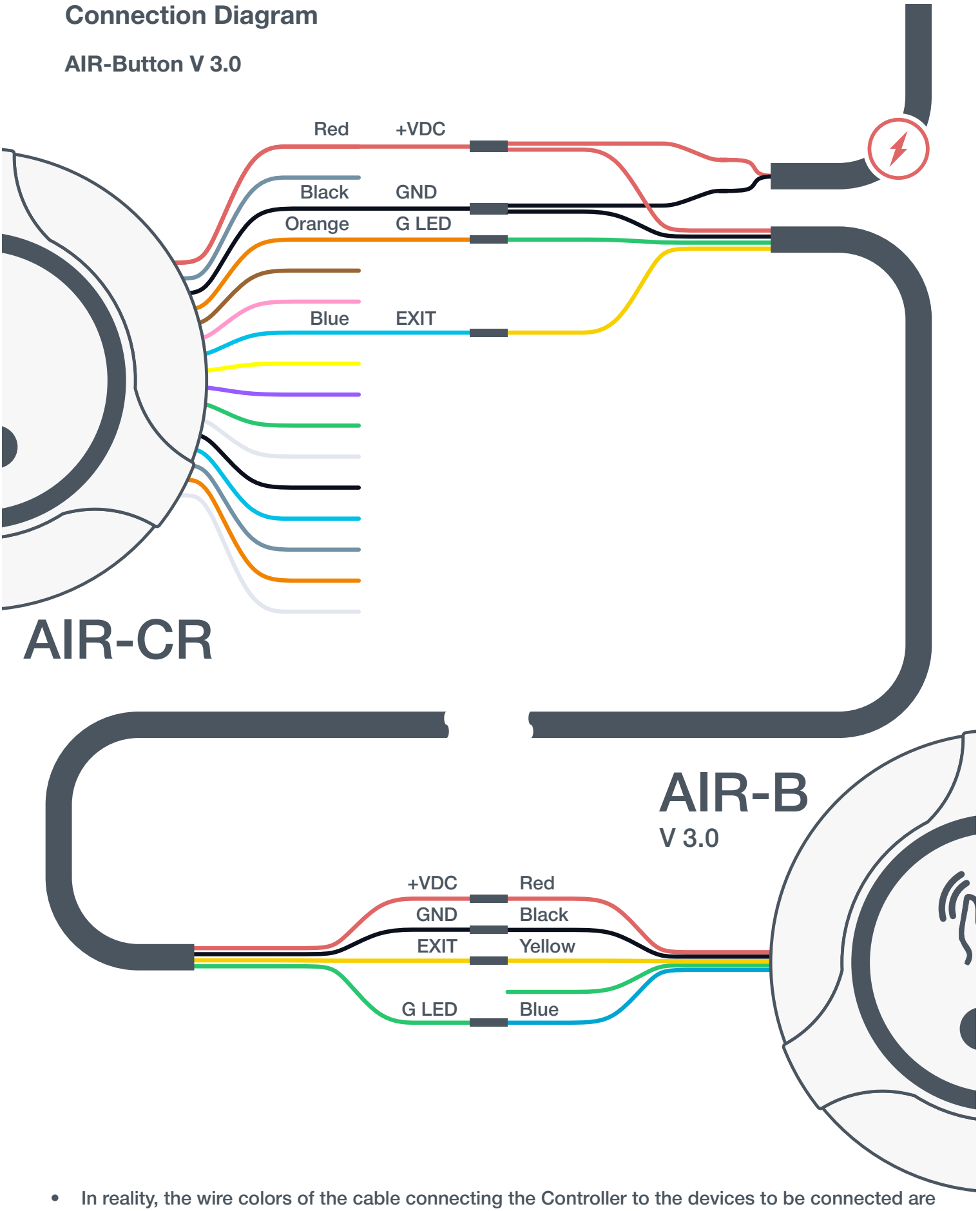
AIR-Button V 2.0



- In reality, the wire colors of the cable connecting the Controller to the devices to be connected are given as an example and may vary.

Connection Diagram

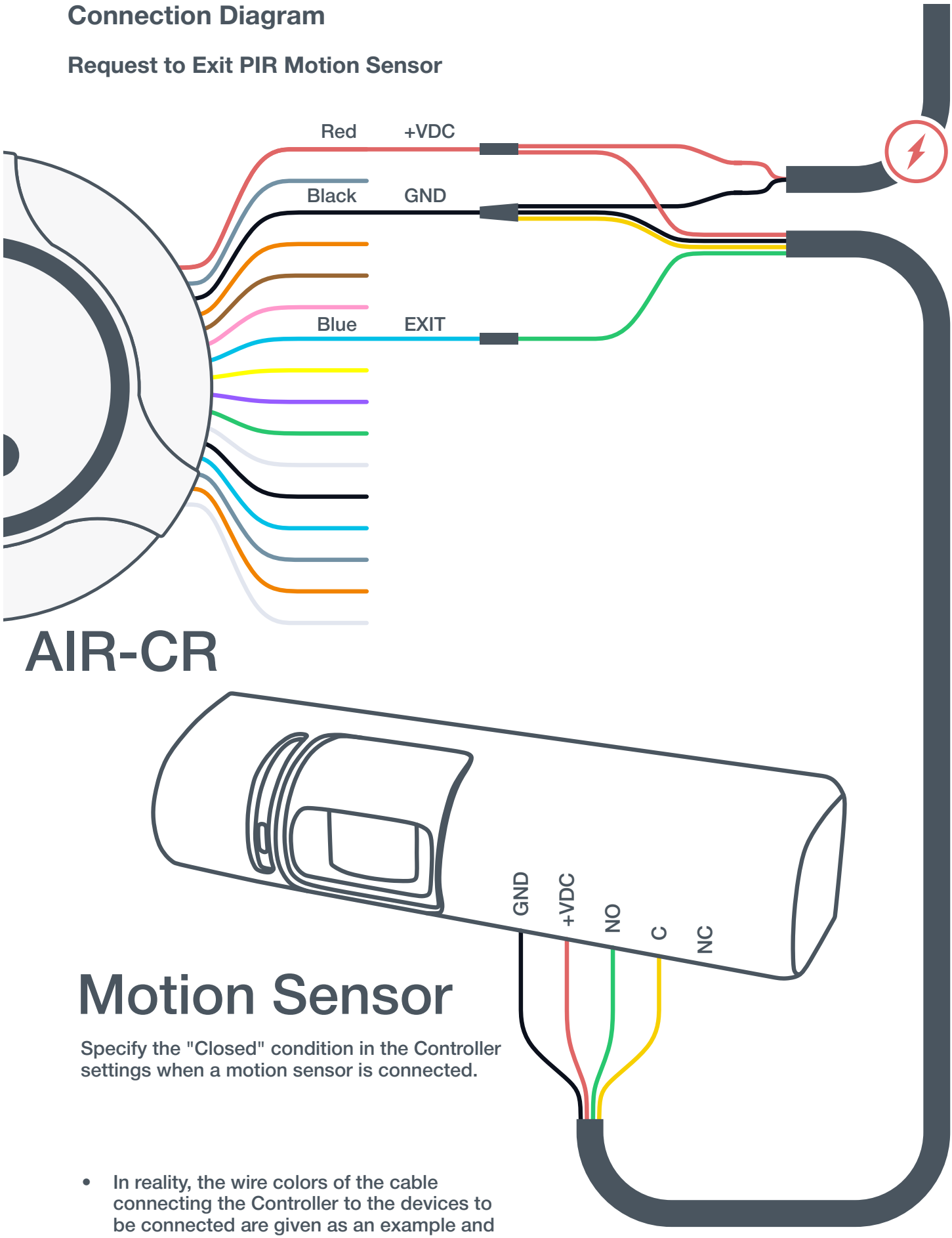
AIR-Button V 3.0



- In reality, the wire colors of the cable connecting the Controller to the devices to be connected are given as an example and may vary.

Connection Diagram

Request to Exit PIR Motion Sensor

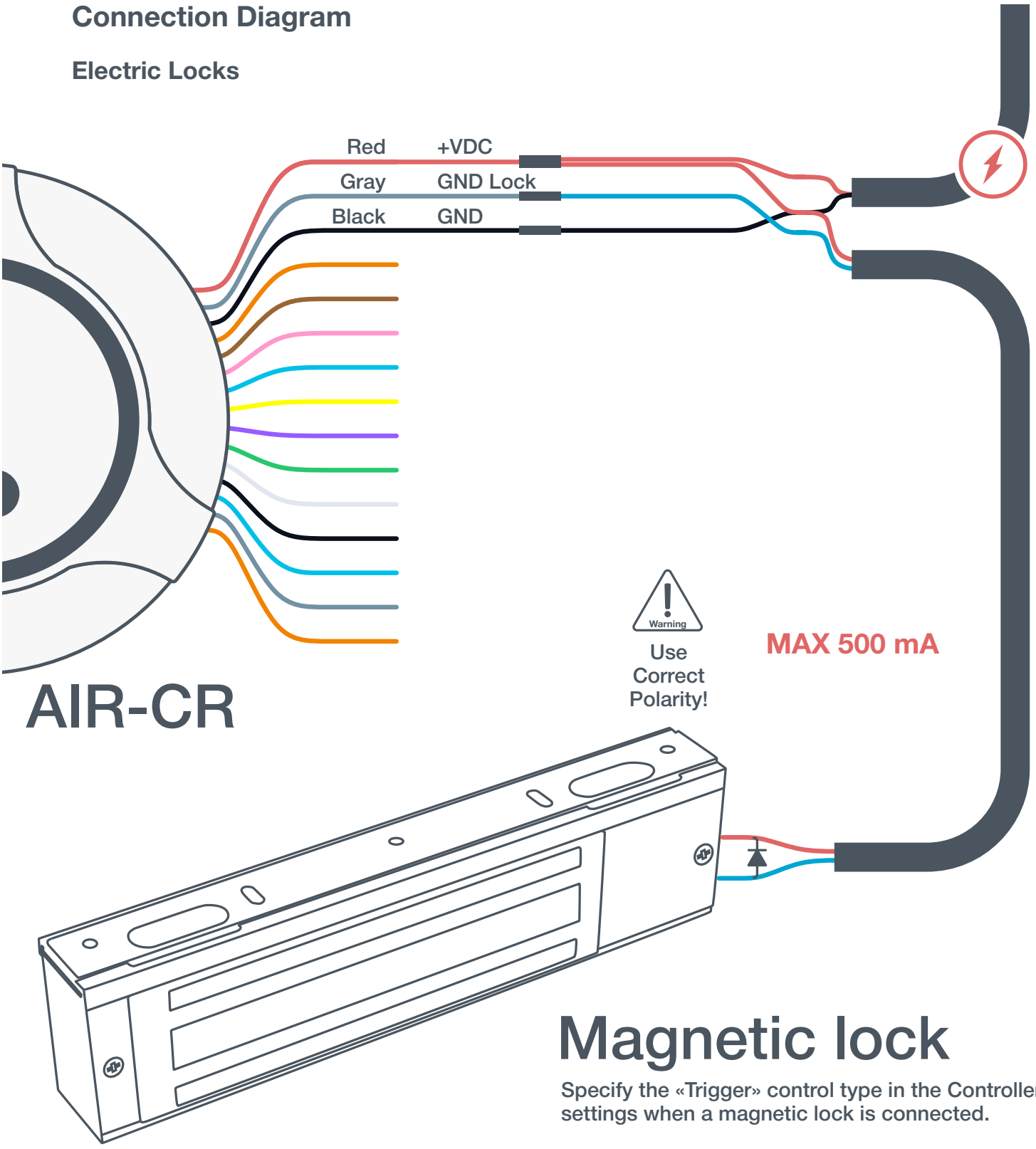


Specify the "Closed" condition in the Controller settings when a motion sensor is connected.

- In reality, the wire colors of the cable connecting the Controller to the devices to be connected are given as an example and may vary.

Connection Diagram

Electric Locks



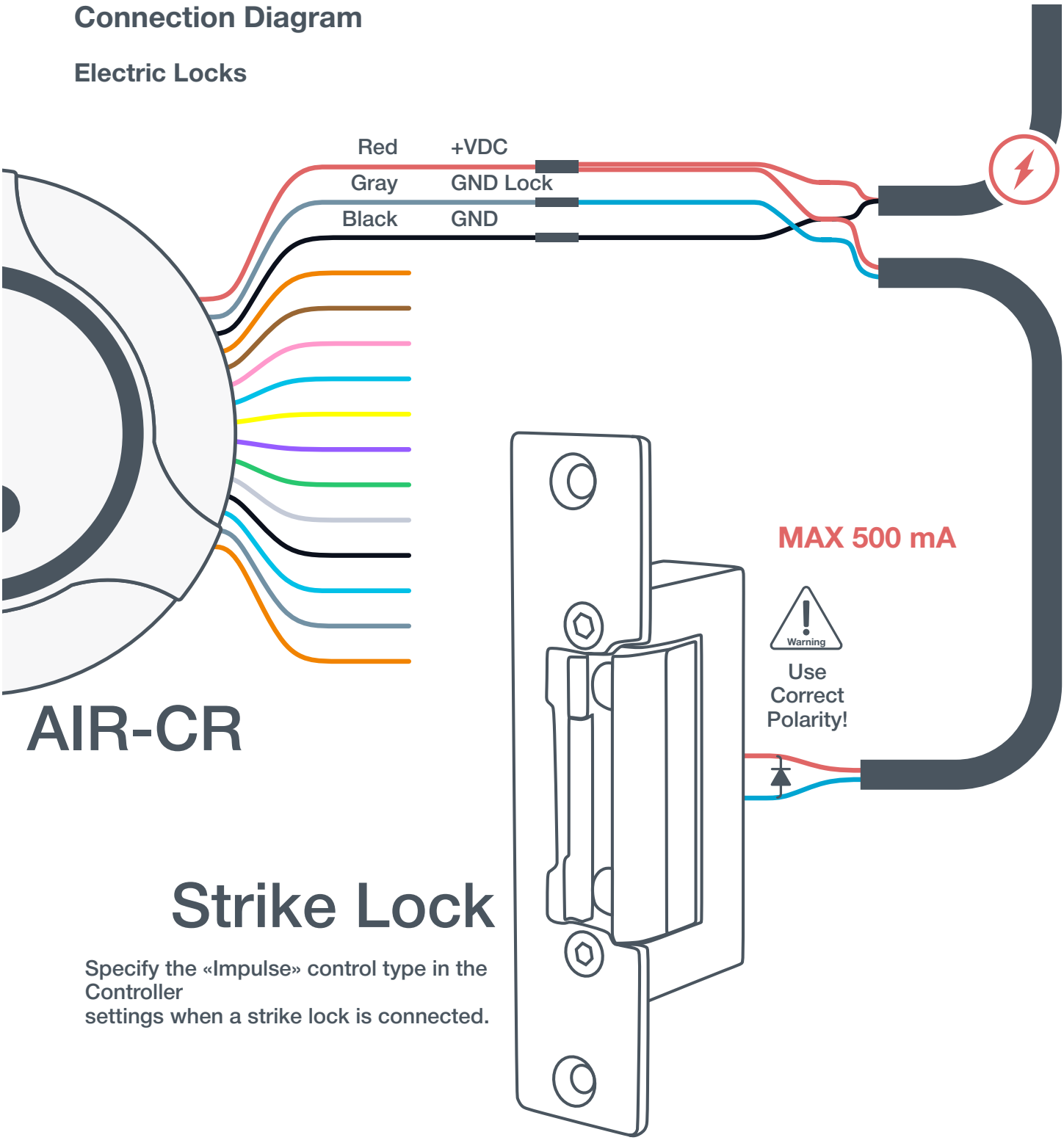
Magnetic lock

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, or 10D390K can be used, for which there is no need to observe polarity.

Connection Diagram

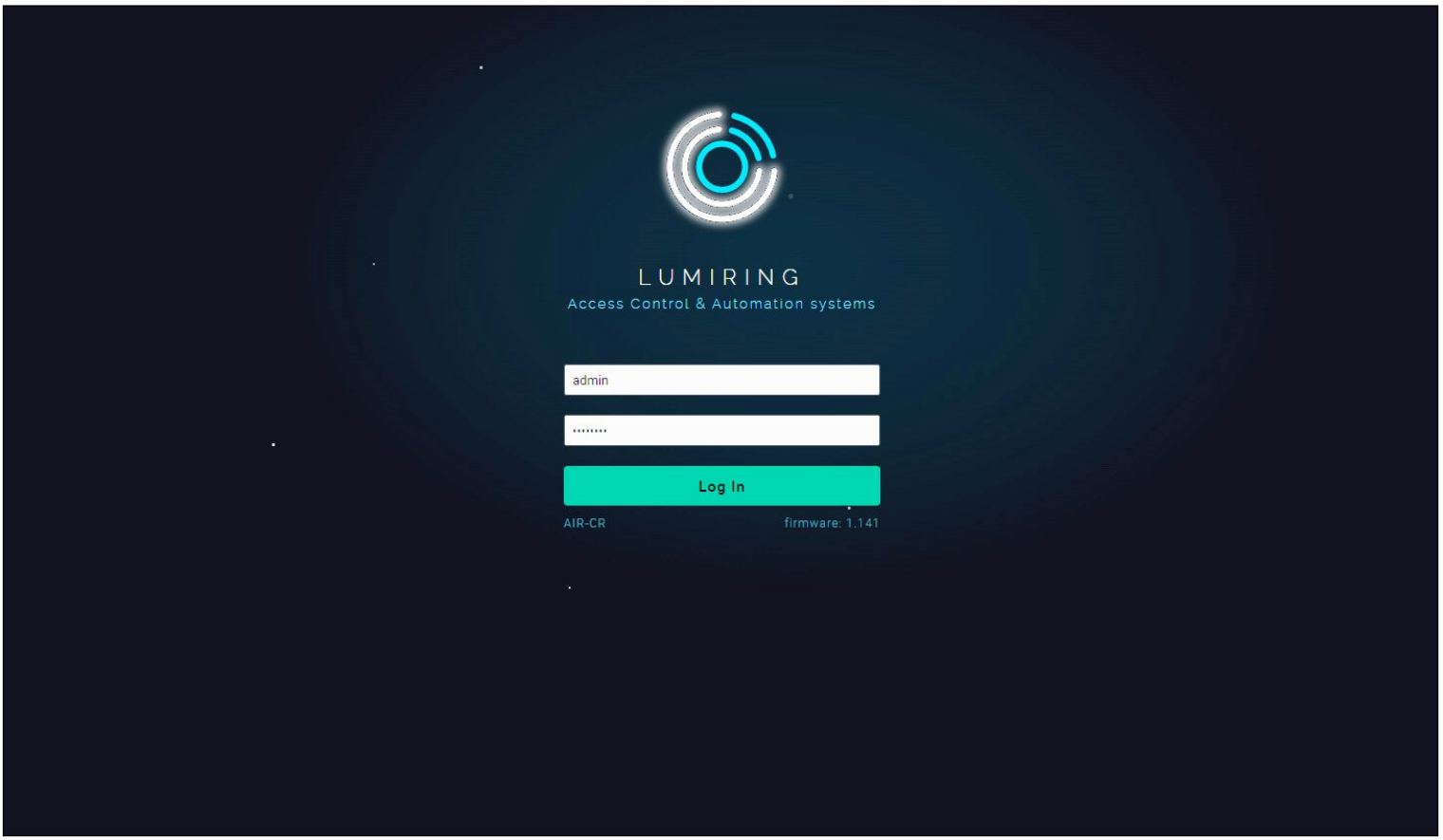
Electric Locks



Specify the «Impulse» control type in the Controller
settings when a strike 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, or 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 AIR-CR_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.

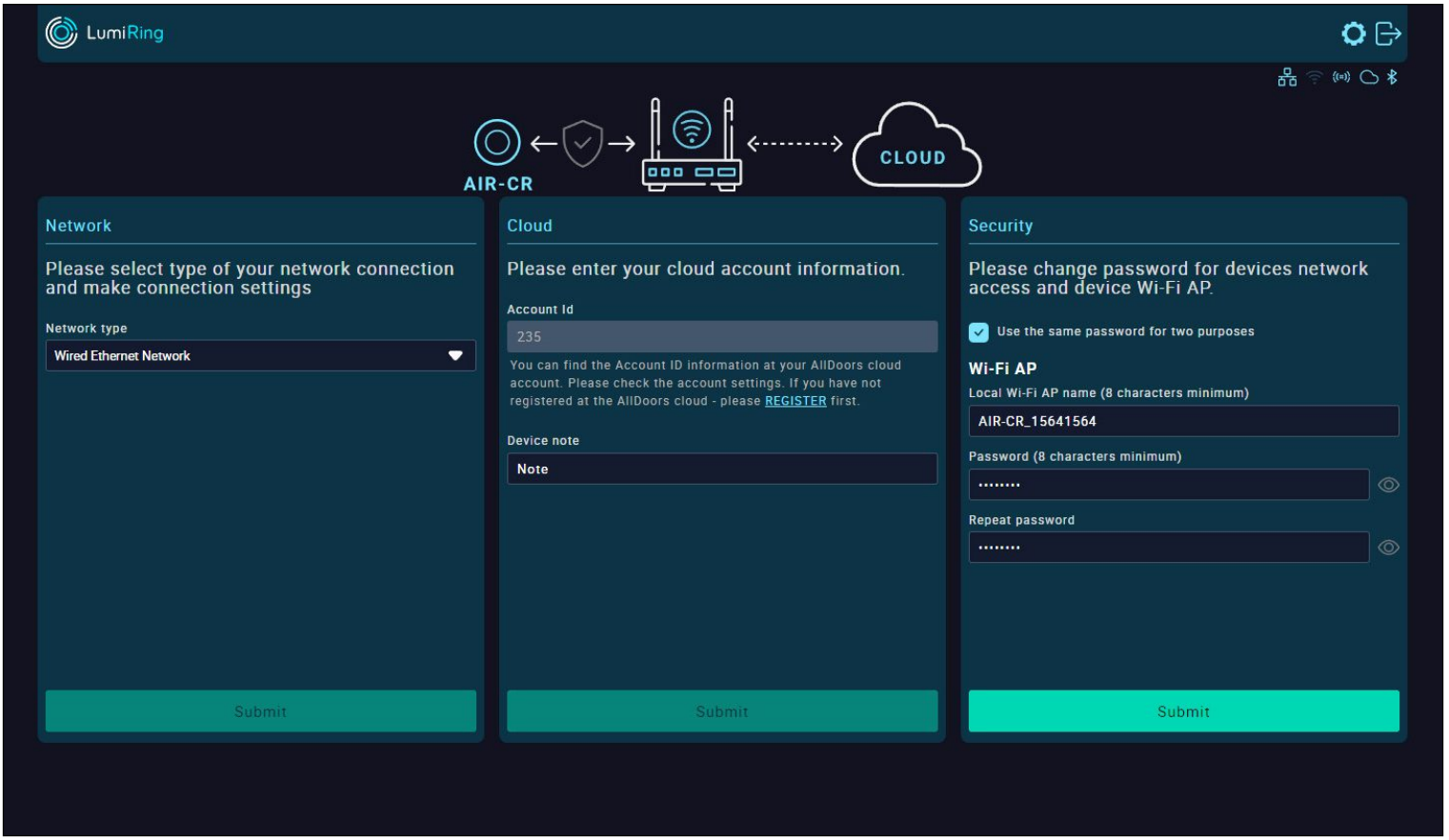
Step 1. Connect the Ethernet cable to the device using an adapter or by connecting the wires, as shown in the diagram below.

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:

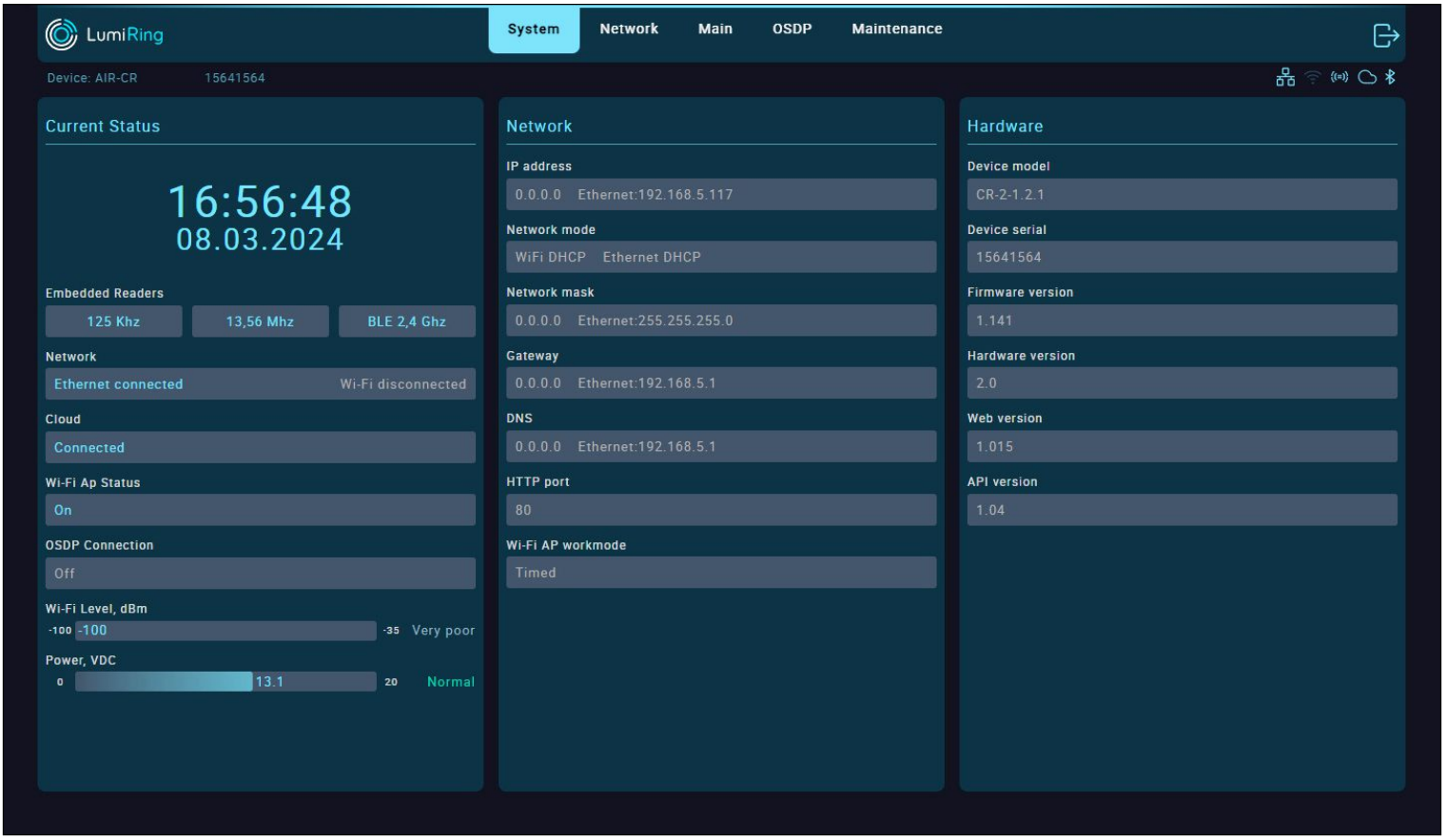
- Enter your account ID and click “Submit.”

Security:

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

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

System



The Current Status subsection displays the:

- Current time and date (when the device is connected to the Internet).
- Status of embedded readers 125 kHz, 13.56 MHz, and BLE 2.4 GHz.
- The 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 access point (AP).
- Level and quality of the device's connection to the Wi-Fi router.
- Power supply voltage value.

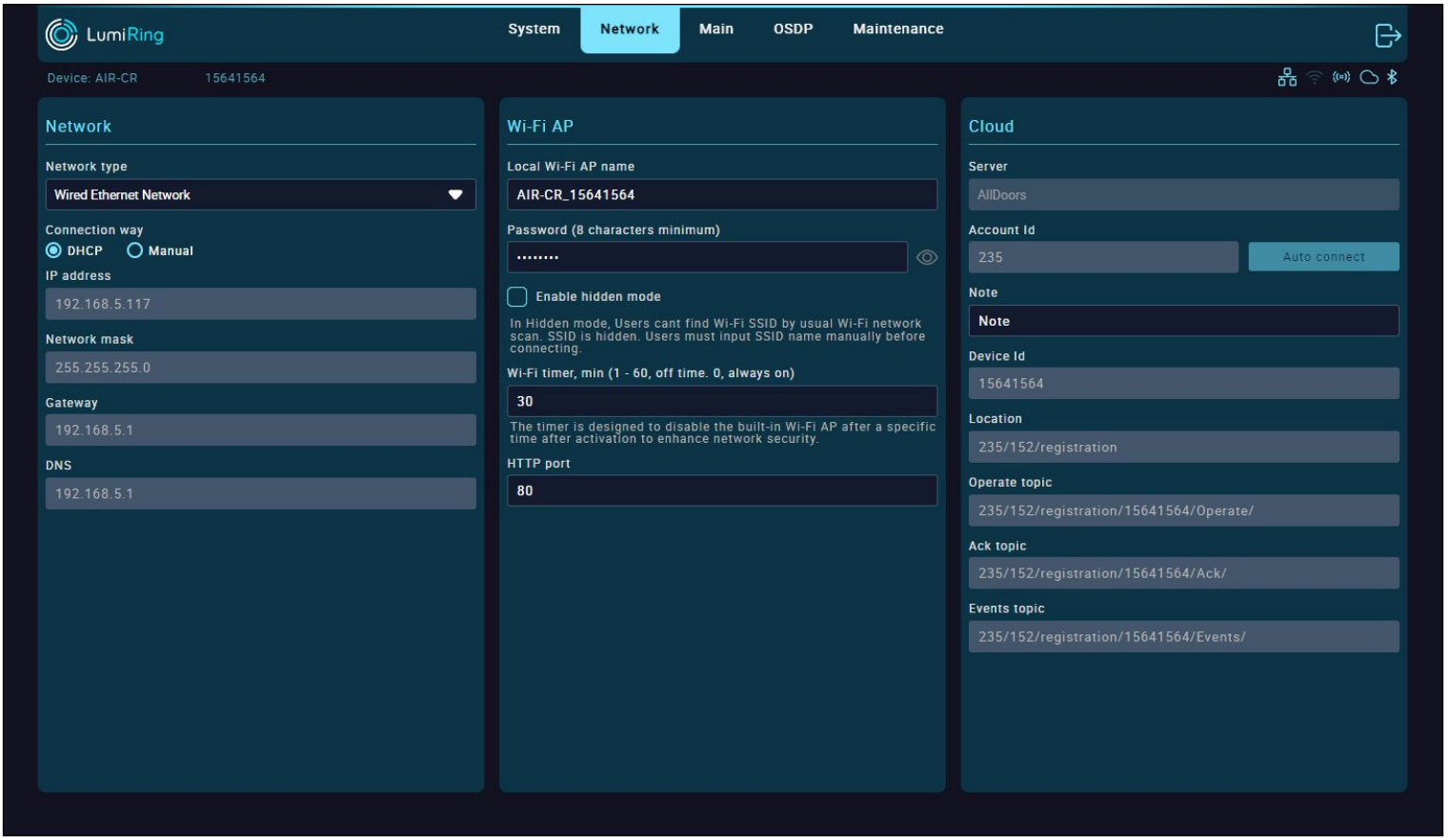
The Network subsection displays the:

- 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 subsection, you can see the:

- Device model name.
- Device type.
- Device serial number.
- Current firmware version.
- Current hardware version of the device.
- Web version used by the device.
- Application programming interface (API) version used by the device.c

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.

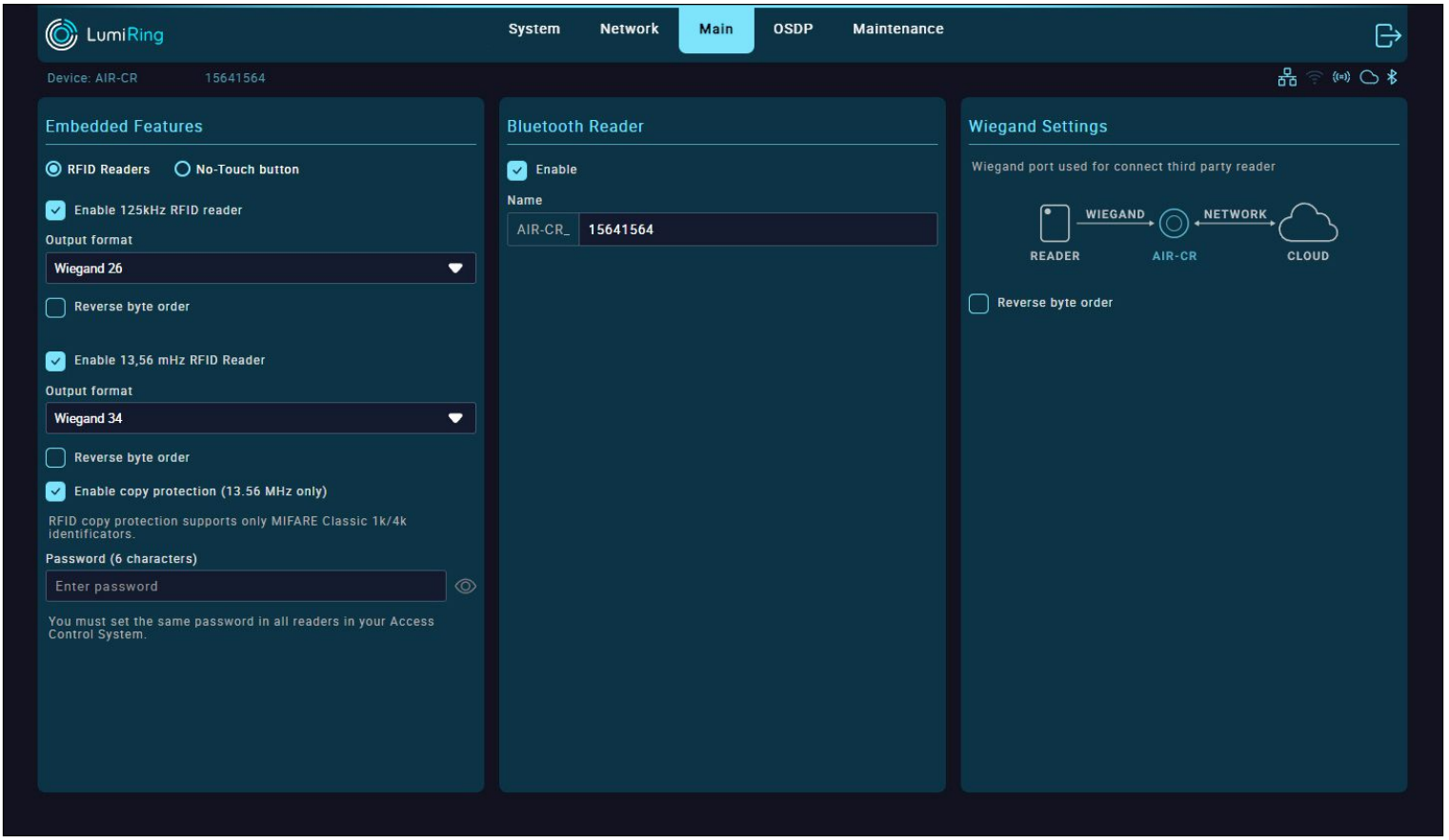
The Cloud settings subsection allows you to connect the Controller to a cloud server for later use.

- 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.

Main



The Main section allows you to configure the functionality of the device and determine the modes of operation.

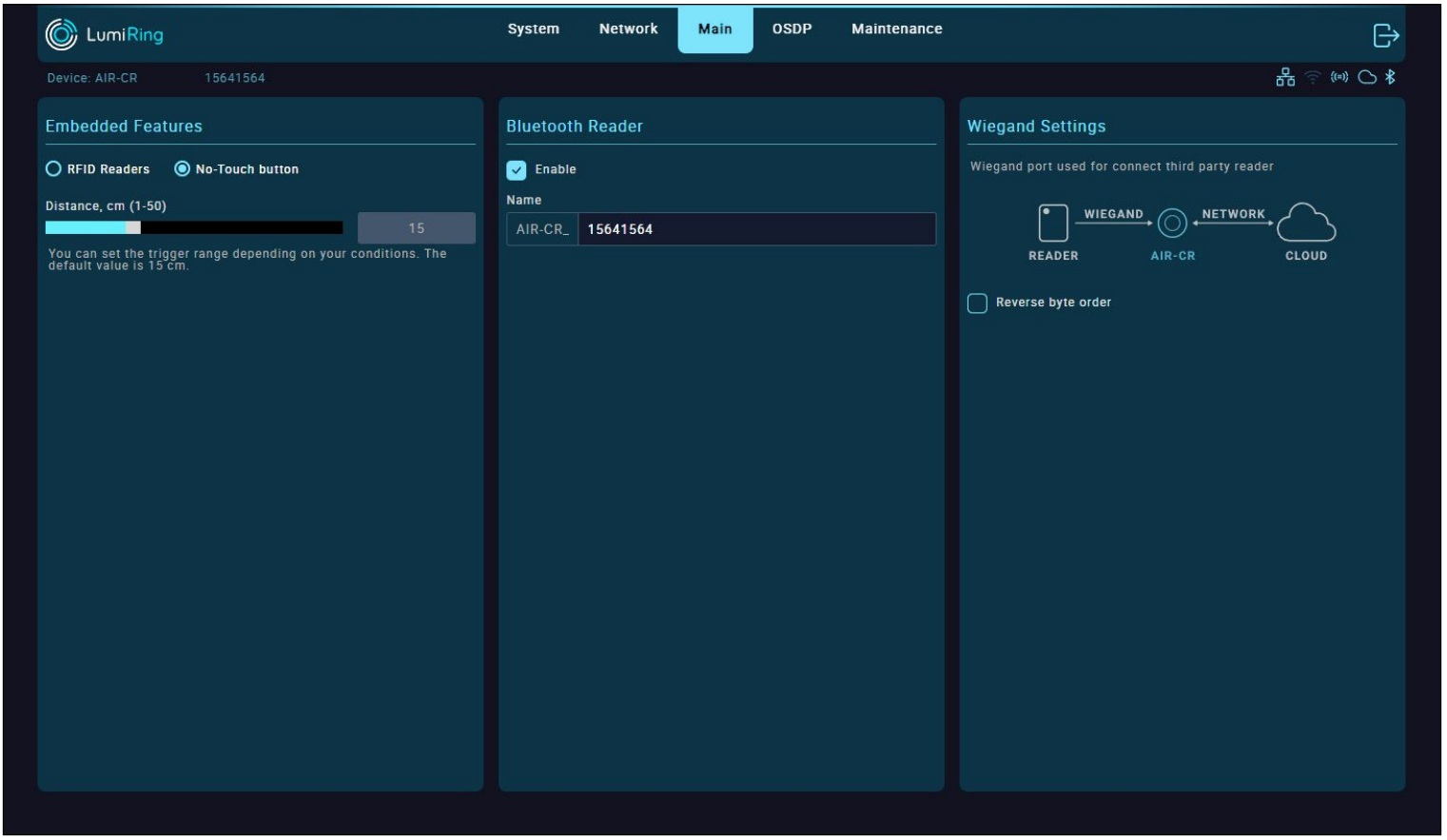
- The “RFID Readers“ button turns on the Controller's built-in antennas, and the button “No-Touch button“ turns off the antennas and turns on the proximity sensor, turning the Controller into an exit button.
- Uncheck the “Enable“ checkbox in the RFID Reader 125 kHz settings section to disable the ability to read identifiers of this format.
- Check the “Reverse byte order“ checkbox to change the code reading order for 125 kHz identifiers.
- Select the desired “Output format” from the list of supported Wiegand formats.
- Uncheck the “Enable“ checkbox in the RFID Reader 13.56 MHz settings section to disable the ability to read identifiers of this format.
- Check the “Reverse byte order“ checkbox to change the code reading order for 13.56 MHz identifiers.
- Select the desired “Output format” from the list of supported Wiegand formats.

Note: It is recommended to use the same format on all readers within an access control system. The default format for 13.56 MHz identifiers is Wiegand 34 bit.

- Check the “Enable copy protection (13.56 MHZ only)” checkbox to use the 13.56 MHz format ID verification mode for authenticity.
- Enter the ID encryption password.

Note: The Copy Protection feature uses a unique password encryption method to encrypt private identifier memory areas. If the encryption password of the identifier and the reader match, then the reader will recognize the identifier. If there is no password or it is different, the identifier is ignored. Thus, all identifiers other than encrypted ones will be ignored.

Main

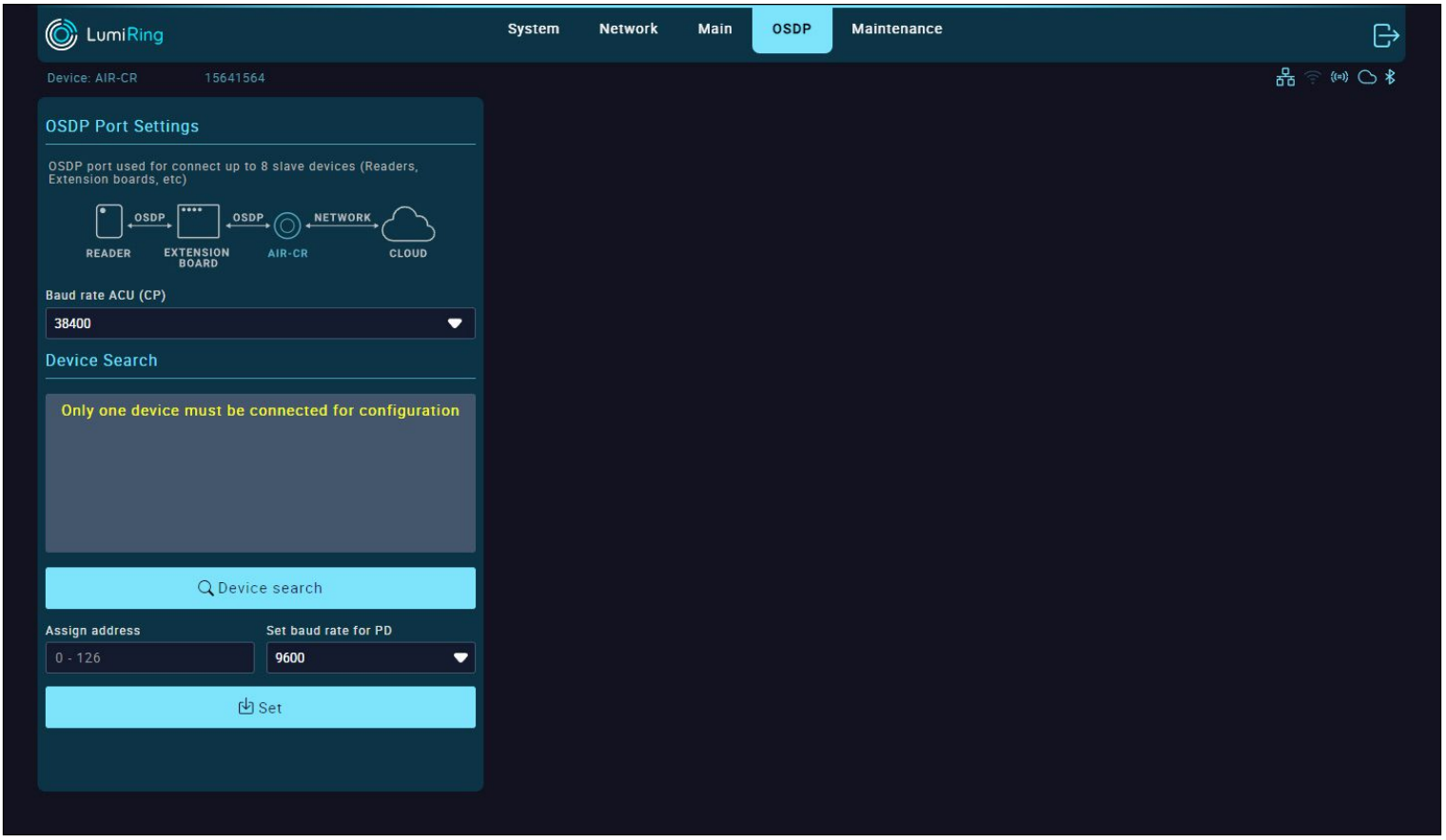


The Main section allows you to configure the functionality of the device and determine the modes of operation.

- Selecting the “No-Touch button” activates the built-in proximity sensor, which acts as an exit button.
- Using the Distance slider, you can select the required distance at which the configured output will be activated.
- Check the “Enable” checkbox to enable the built-in Bluetooth Low Energy (BLE) module. In the Name field, you can give the device a name that will be visible when scanning available Bluetooth connections.
- Check the “Reverse byte order” checkbox to change the order in which the identifier code is read from the reader connected to the Controller.

Note: The byte order will be reversed for all identifier types.

OSDP



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

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

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

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

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

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

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

- When a device is found, assign it an "Address, " select the desired "Baud rate," and click the "Set" button.

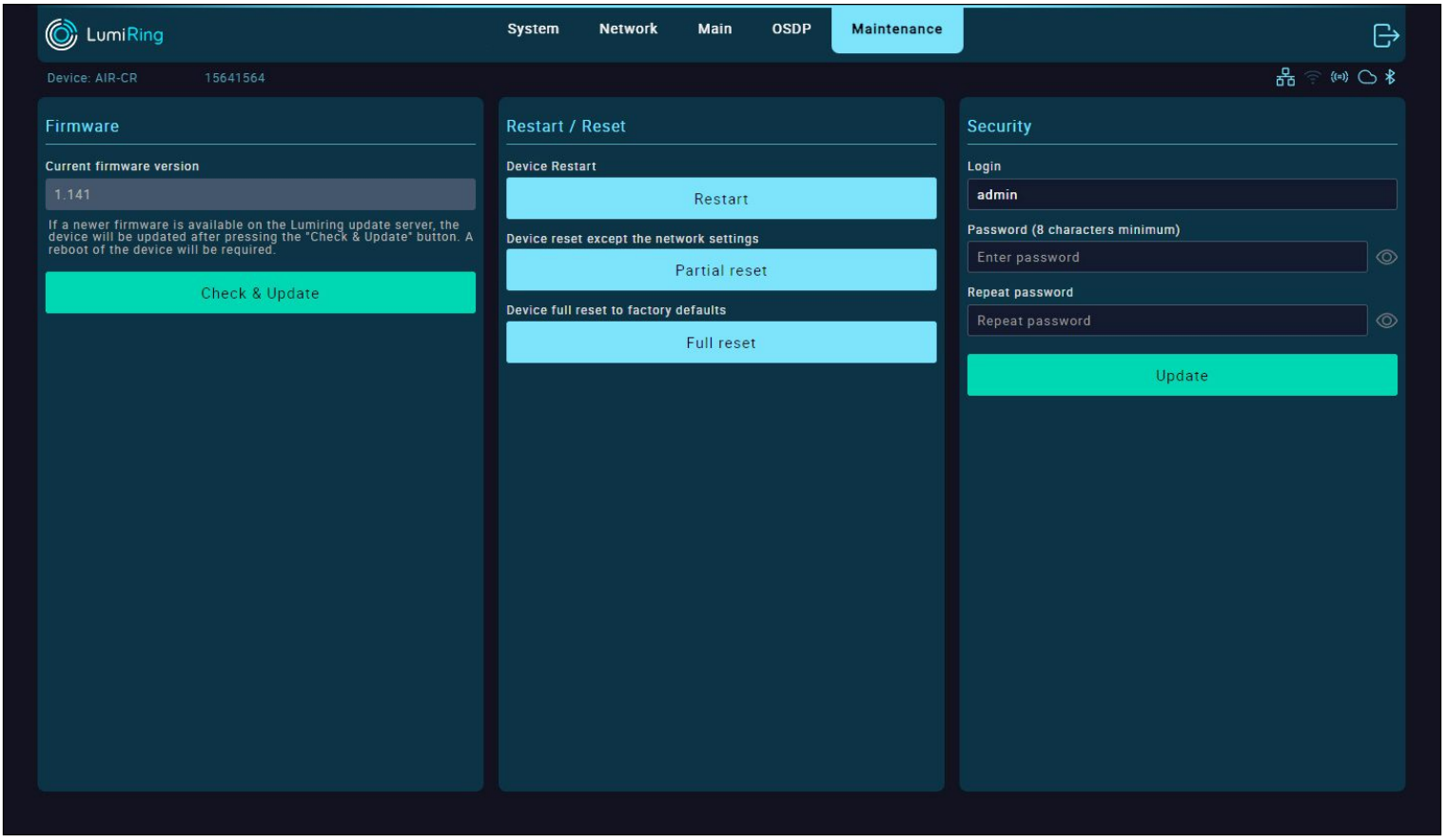
Disconnect the first OSDP device and connect the next one.

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

Further configuration and communication with the devices are done via the cloud service.

The OSDP section is under development and will be available soon. Watch for updates.

Maintenance



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

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

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 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:

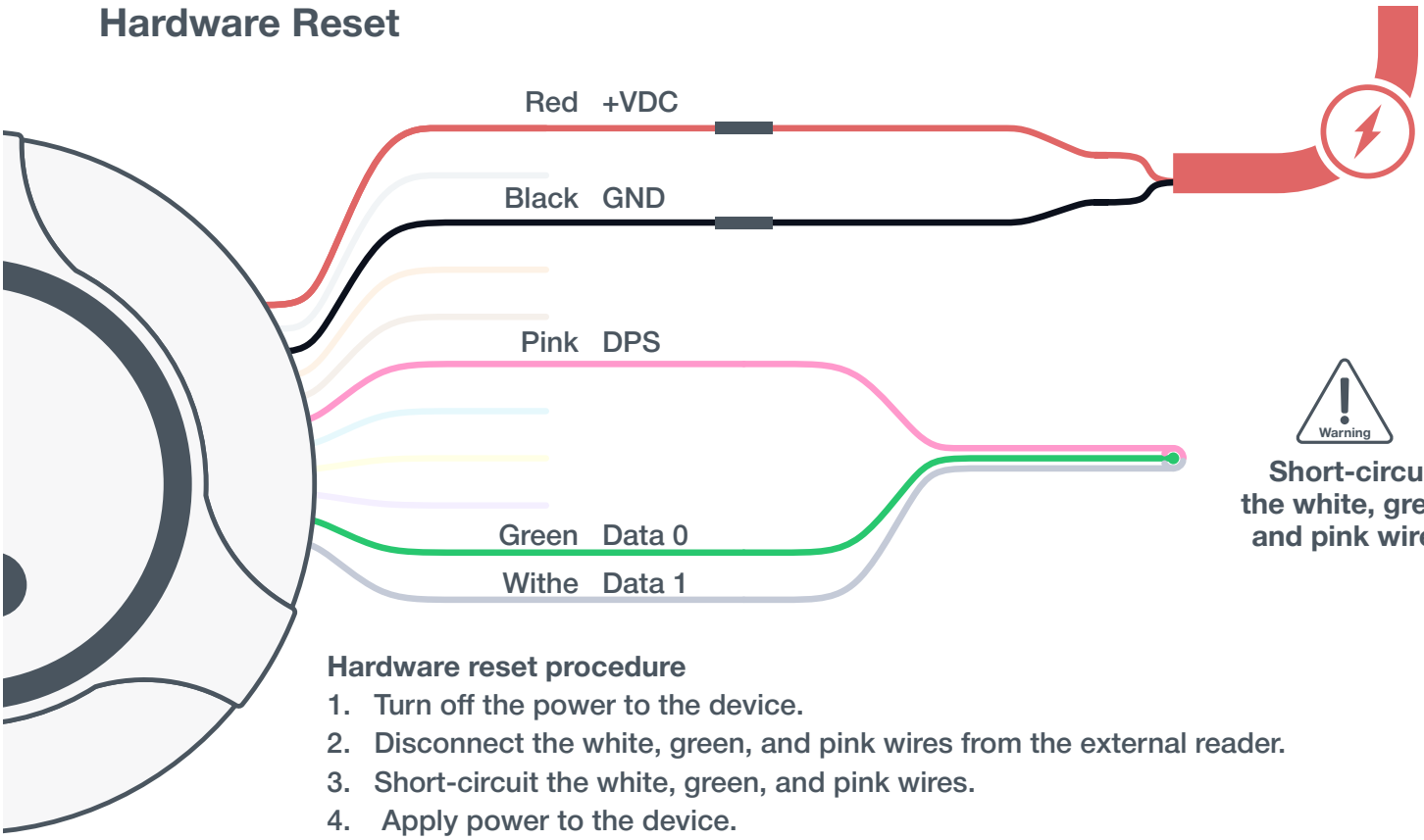
- Restart - restarts the device.
- Full reset - resets all settings of the device to factory defaults.

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 procedure

1. Turn off the power to the device.
2. Disconnect the white, green, and pink wires from the external reader.
3. Short-circuit the white, green, and pink wires.
4. Apply power to the device.
5. The device will flash yellow and emit seven short beeps, then turn green and emit three short beeps.
6. Disconnect the white, green, and pink wires from each other.
7. The device will light up yellow, beep three times, and then go into standby mode.
8. The hardware reset procedure is complete, and the device is ready for use.

Warning

- When performing a hardware reset, all data stored in the device memory and all related settings will be deleted.
- This procedure cannot be undone.

Indication

LED color/behavior	Device status	Description
Blue (solid)	Standby mode	Waiting state of the identifier
Green (solid)	Access granted	Indication color when a low voltage level appears on the orange wire.
Red (solid)	Access denied	Indication color when a low voltage level appears on the brown wire.
Yellow (solid)	Waiting for confirmation	The device's Wi-Fi Access Point (AP) is activated.
Yellow (flashing)	Configuration via the Web interface is in progress	Connected to the Web interface via the built-in Wi-Fi AP
Red/Buzzer	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 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 elctromagnetic 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.