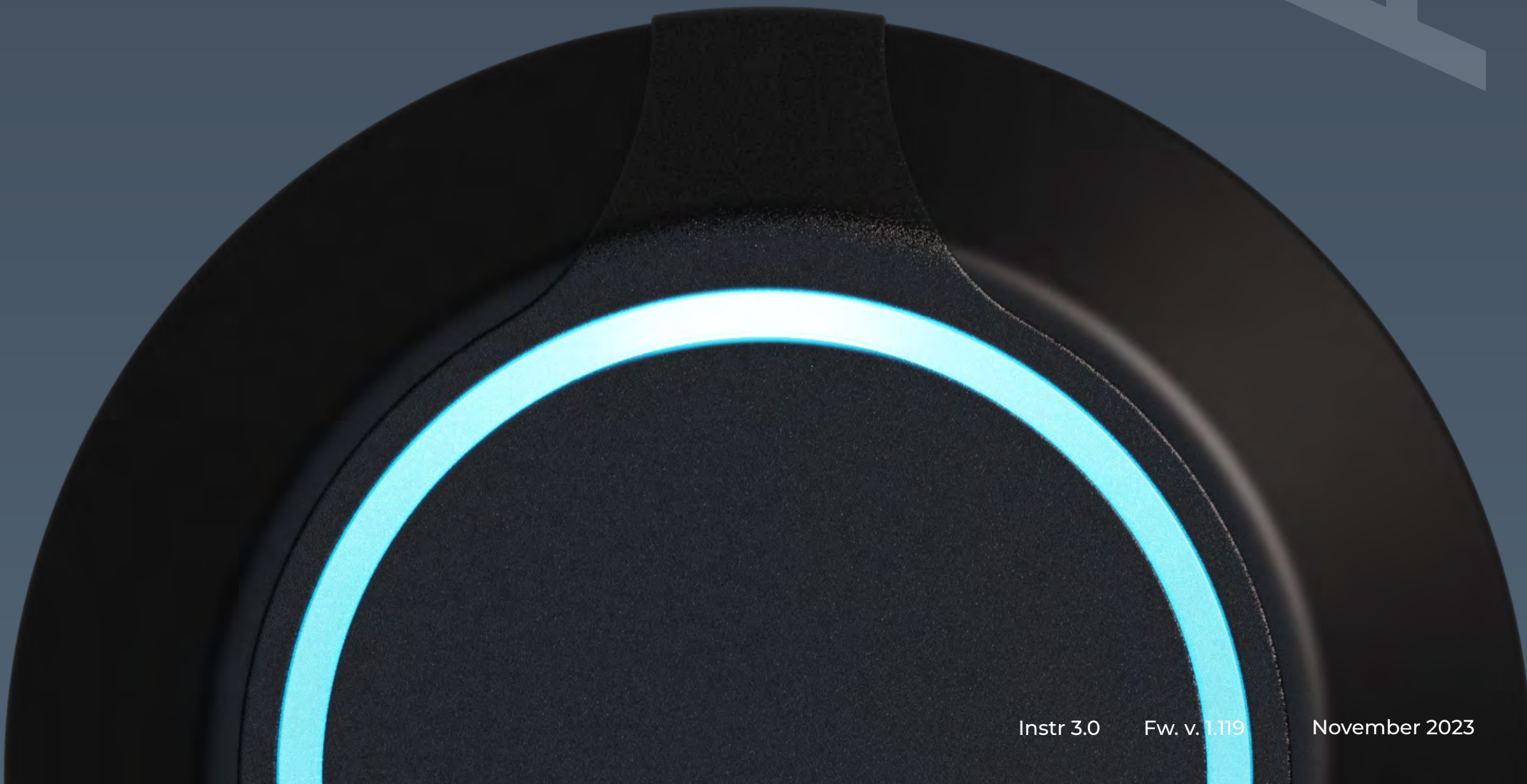




MANUAL

RECORDER



CONTENTS

Introduction	3
Default Device Settings	3
Device Specifications	4
Device Dimensions	5
Wire Designation	6
Installation Recommendations	7
Ethernet Network (Connection Diagram)	8
Wiegand Reader (Connection Diagram)	9
Open Supervised Device Protocol (OSDP) Reader (Connection Diagram) <i>Coming soon!</i>	10
Exit Button (Connection Diagram)	11
Door Sensor & Magnetic Lock (Connection Diagram)	12
Connecting to Device	13
Login	13
Quick Start	14
System	15
Network	16
Main	18
Open Supervised Device Protocol (OSDP) <i>OSDP is coming soon!</i>	20
Maintenance	21
Hardware Reset With Wires	22
Glossary	23
For Notes	26

Introduction

This document provides detailed information on the AIR-CR 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 during the use of the product.

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	192.168.1.100
• Wi-Fi password	none
• Login	admin
• Password	admin
• RFID 125 kHz	Enabled
• RFID 13.56 MHz	Enabled
• Copy protection	Disabled
• Bluetooth	Disabled
• AP Wi-Fi timer	30 minutes
• Wiegand or Open Supervised Device Protocol (OSDP) sending method	Wiegand
• Wiegand format 125 kHz	26 bit
• Wiegand format 13.56 MHz	34 bit

Device Specifications

Device info

- Model AIR-CR
- Processor ESP32-S3
- Over-the-air (OTA) update Yes
- Built-in web server Yes
- Support for 125 kHz identifiers EM Marin
- Support for 13.56 MHz identifiers MIFARE DESFire; MIFARE Plus; MIFARE Ultra Light; MIFARE Classic mini/1K/4K; MIFARE Classic EV1 1K/4K; NFC Tag
- Support for copy protection for MIFARE Classic mini/1K/4K identifiers Yes

Communications

- Wi-Fi 802.11 b/g/n 2.4 GHz
- Ethernet With the RJ-45 adapter (10/100 Mbit)
- Bluetooth Bluetooth® 5 (LE)
- Wired interfaces Wiegand/OSDP via RS-485

Physical connections

- Inputs 2
- Outputs (open collector) 0.5 A 1

Electrical characteristics

- Input voltage 12-24 VDC +/- 10 %
- Operation current (MAX) 12 VDC 0.5 A (6 W)
- Operation current (AVG) 12 VDC 0.13 A (1.56 W)
- Switchable output current (MAX) 12 VDC 0.5 A (6 W)
- Output short-circuit protection Yes
- Power supply reverse polarity protection Yes

Work distance

- RS-485 * 3280 ft (1000 m)
- Wiegand 328 ft (100 m)
- Wi-Fi 2.4 GHz (open space) 33 ft (10 m)
- Bluetooth (open space) 33 ft (10 m)

Environmental requirements

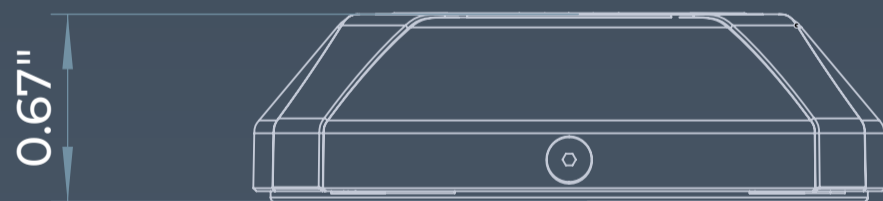
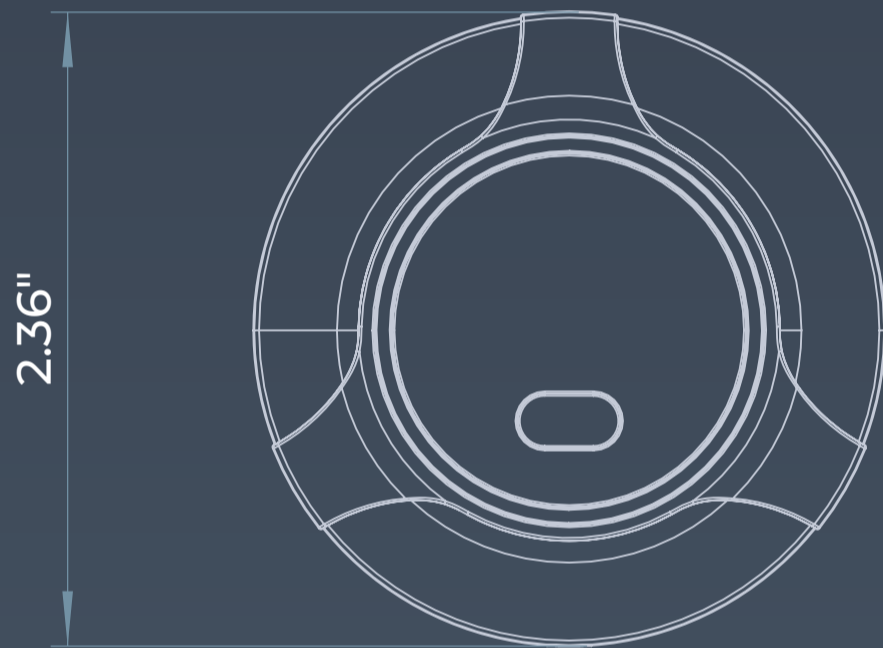
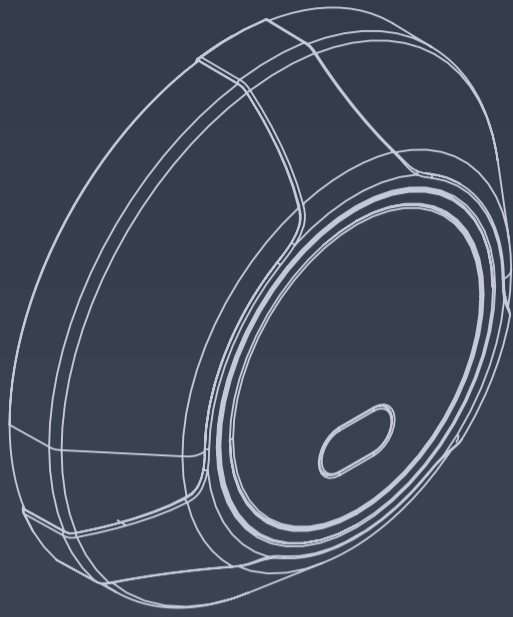
- Operating temperature -22°F ~ 158°F (-30°C ~ 70°C)
- Ingress Protection rating IP65

Physical characteristics

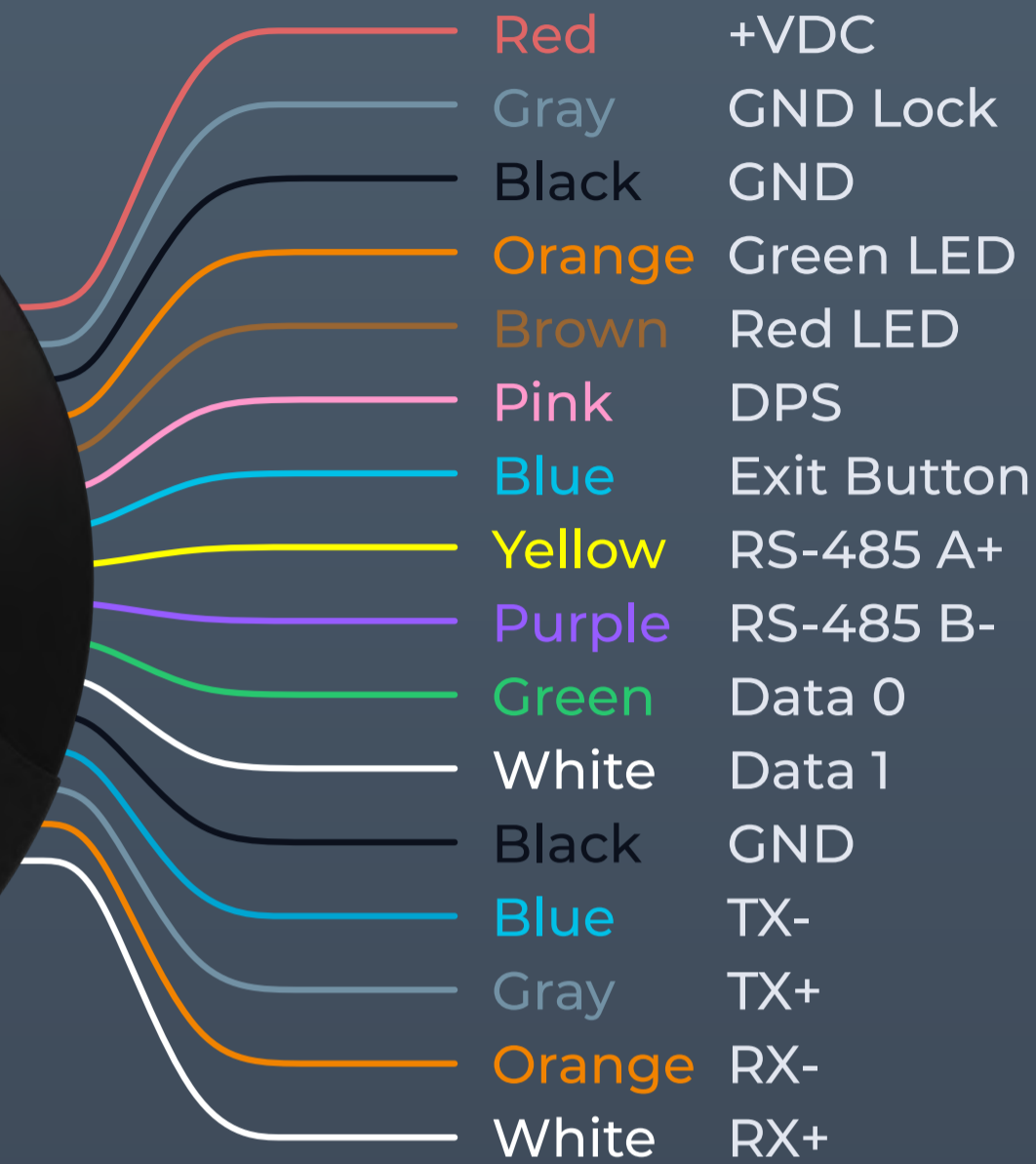
- Housing material ABS plastic UL94 V-0
- Mounting method Wall mount
- Dimensions (diameter, height) 2.36" x 0.67" (60 x 17 mm)
(mounting ring) 2.36" x 0.86" (60 x 22 mm)
- Weight 1.59 oz (45 g)

* See general specifications for RS-485 interface.

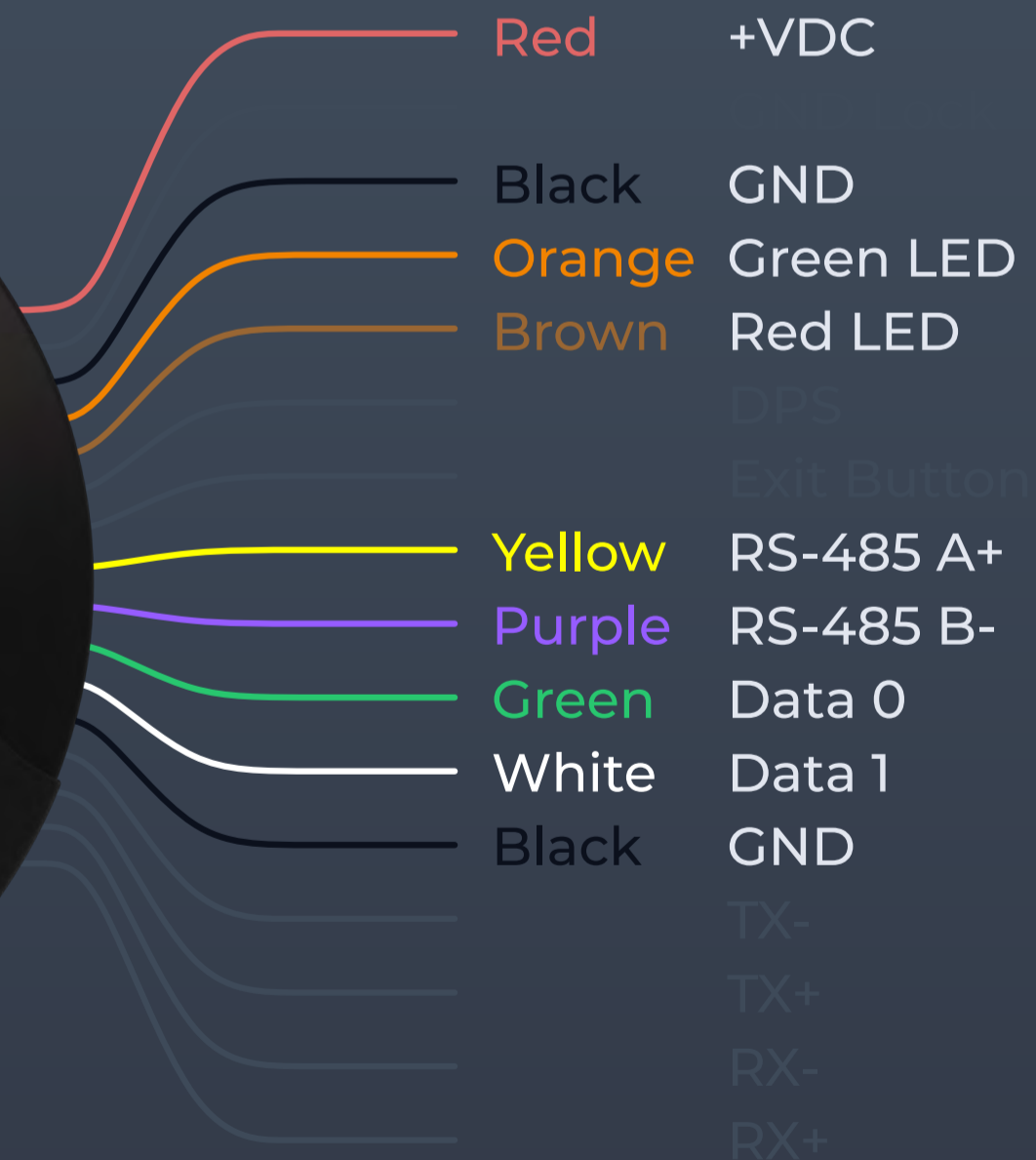
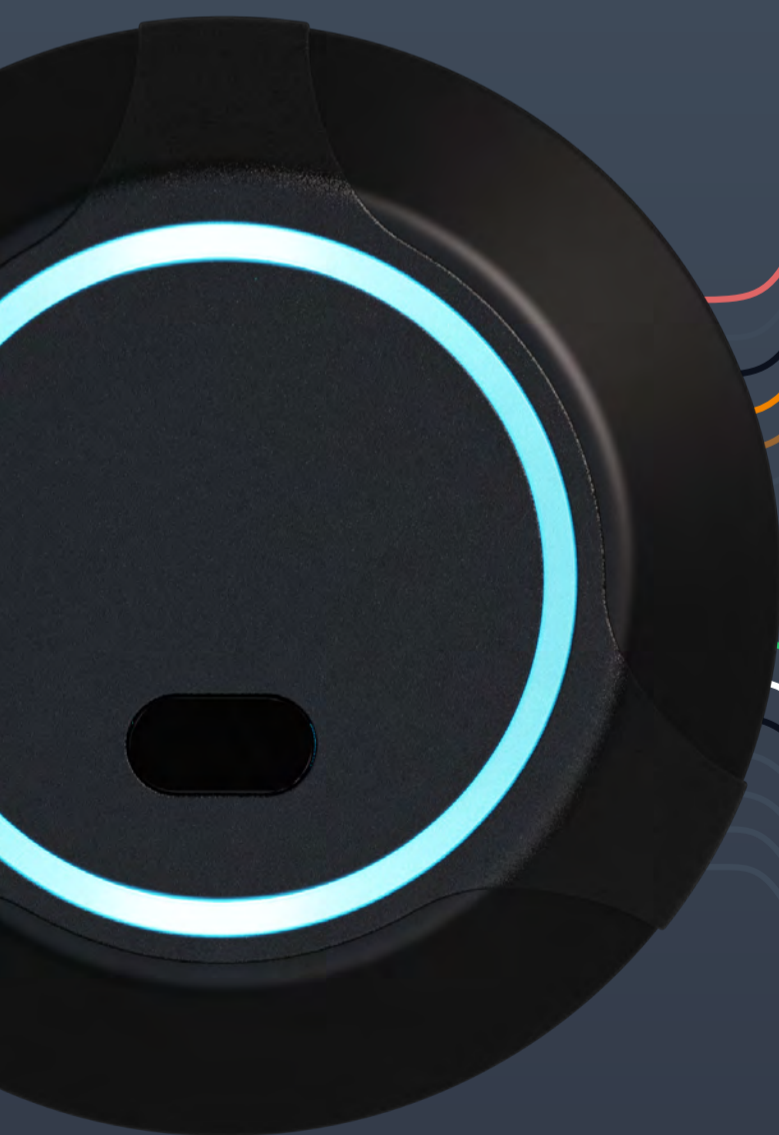
Device Dimensions



Wire Designation



AIR-CR



AIR-R



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.

Installation Recommendations

Installation

It is best to avoid installing the device on metal surfaces, as this may reduce the card reading distance, WI-Fi connection quality, and Bluetooth connectivity.

If installing on a metal surface is necessary, use the reinforced plastic mounting base that is supplied with the device.

Wiegand connection

The length of the communication line through the Wiegand interface must not exceed 328 ft (100 m).

This interface is susceptible to external sources of interference. We do not recommend running it directly parallel to power cables or near electric lights.

It is recommended that the Wiegand communication line be routed at least than 1.64 ft (0.5 m) away from any power cables.

If the communication line is longer than 16.4 ft (5 m), a UTP 5E cable is recommended.

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.

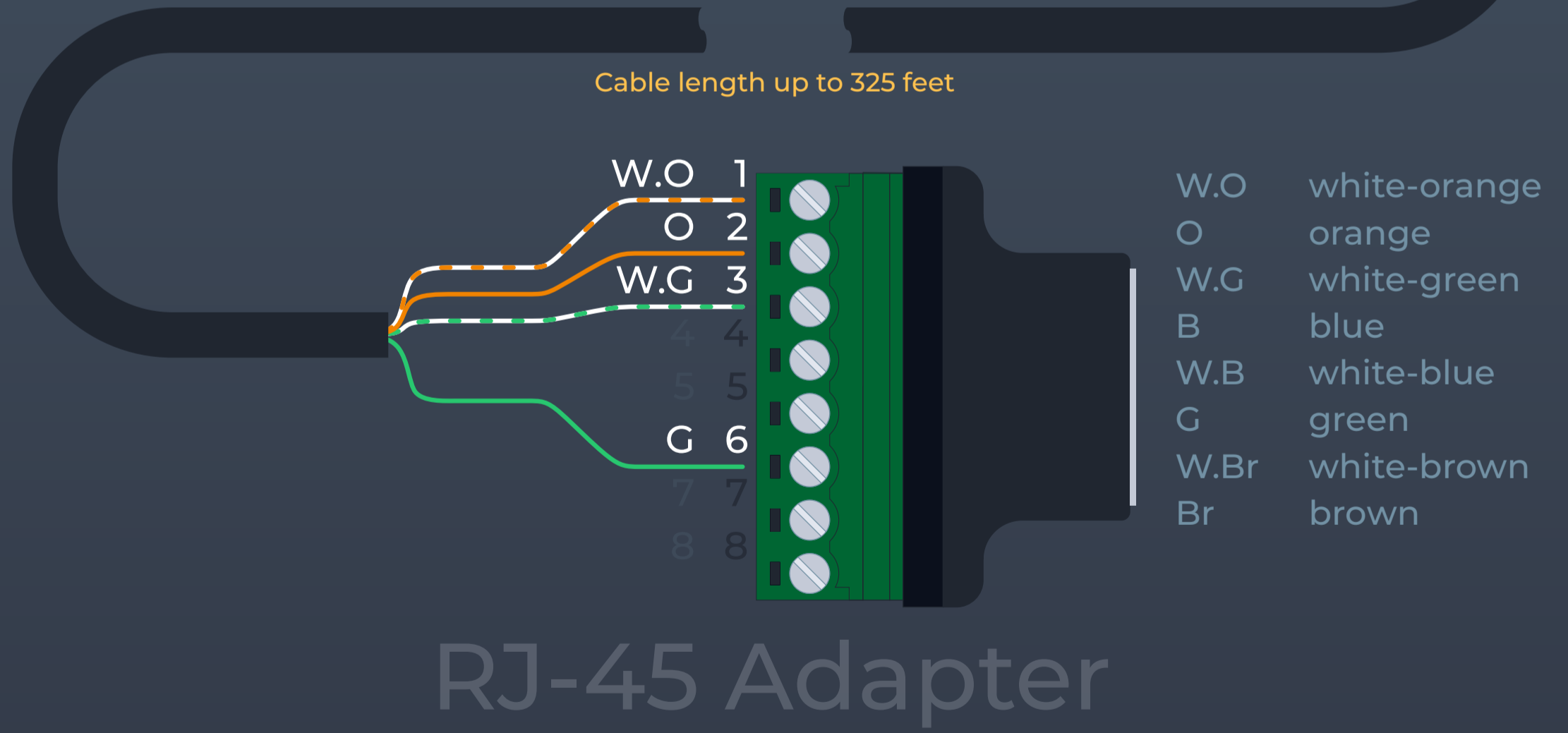
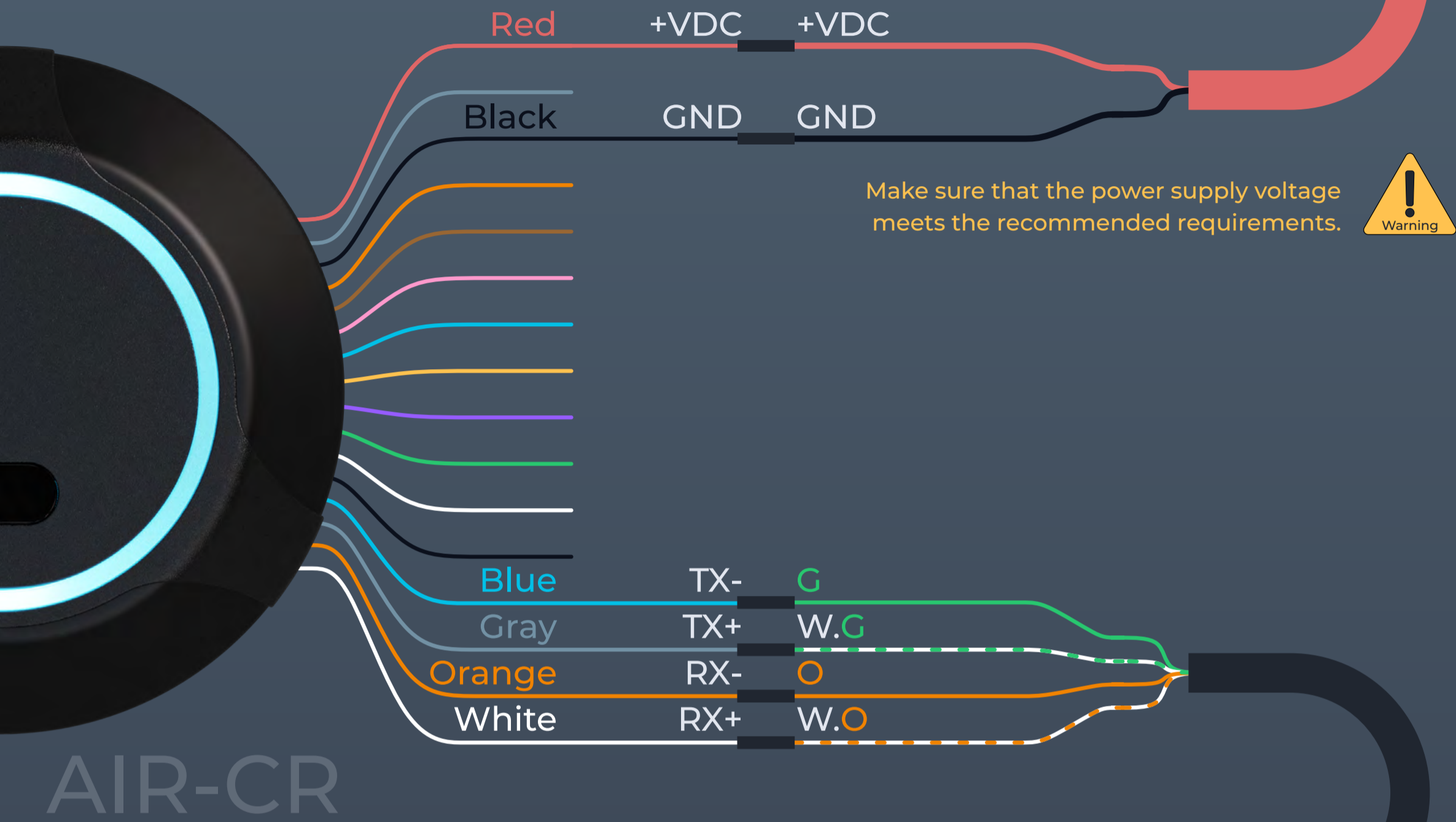
The OSDP communication line should be laid as far away as possible from power cables and electric lights. A UTP 5E or FTP 5 twisted pair cable should be used as the OSDP communication line (if possible, ground the shield at one end). To ensure reliable system operations, it is best to use one power source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

Ethernet Network

Connection Diagram



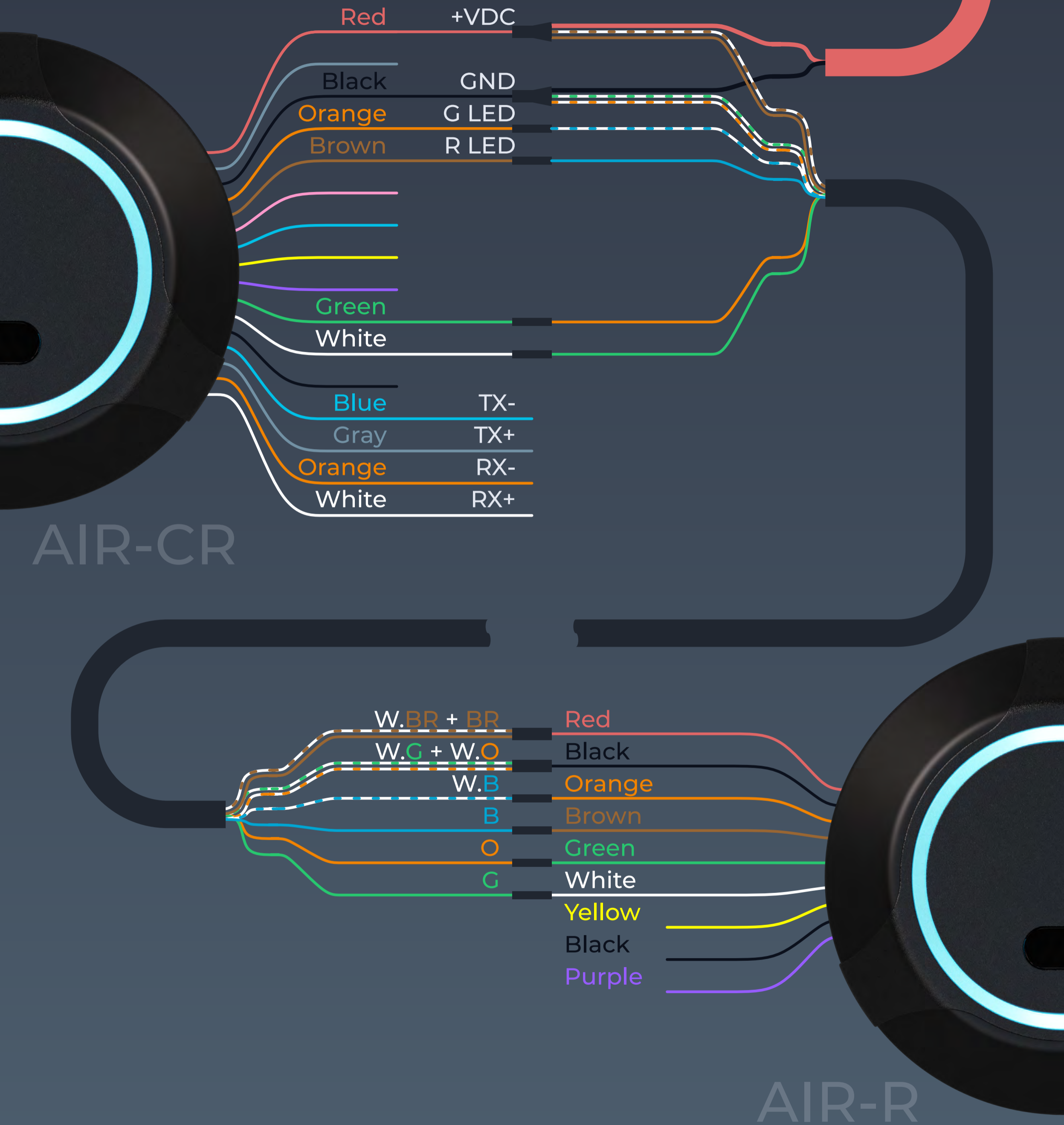
The voltage levels of the power supply and the Controller may differ depending on the cable length and the resistance of the conductor. Use a separate power supply to connect the reader if the cable is longer than 165 feet or the voltage at the end of the line is less than 10 volts.

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.

Wiegand Reader

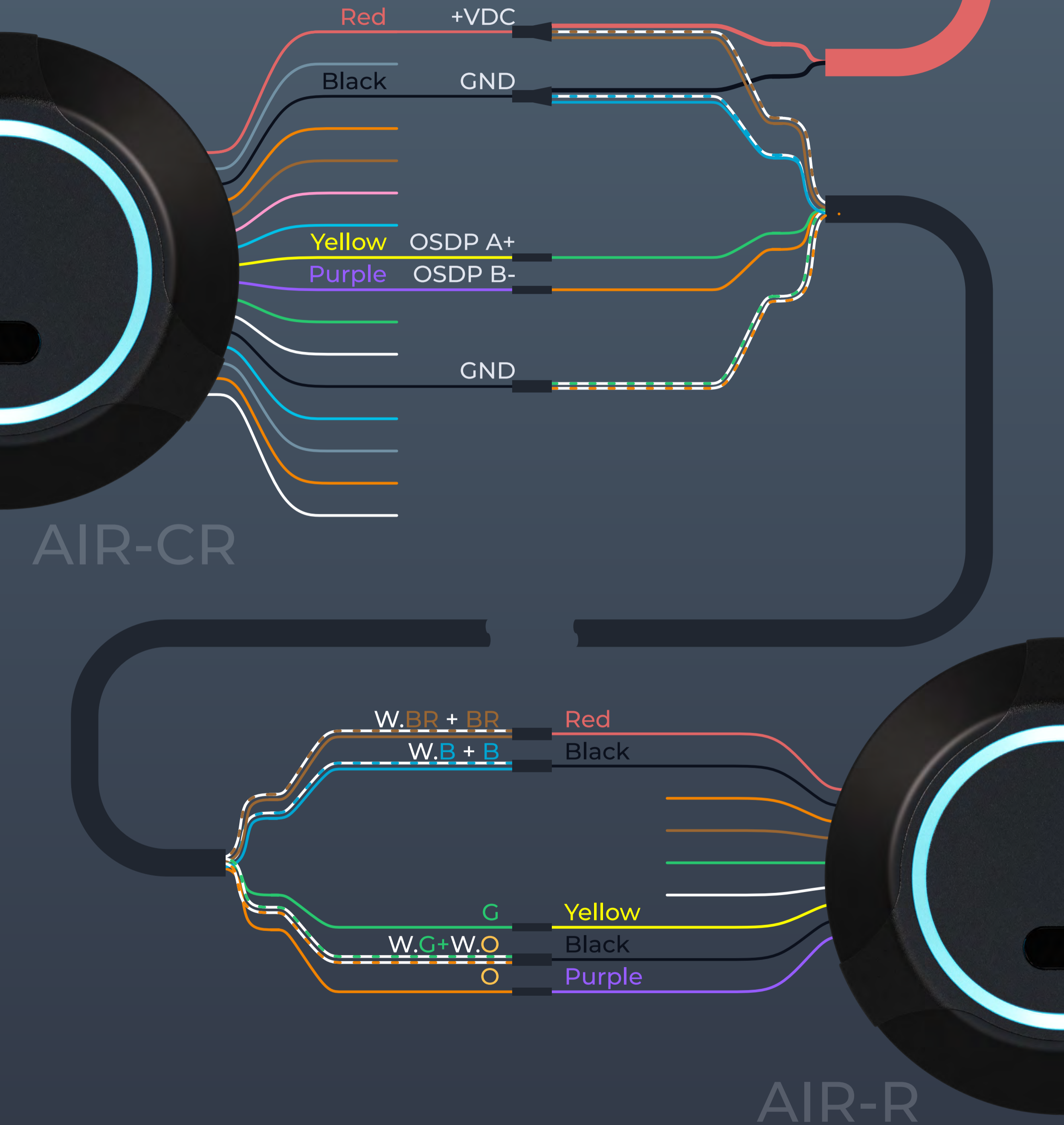
Connection Diagram



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.

Open Supervised Device Protocol (OSDP) Reader Comming soon!

Connection Diagram



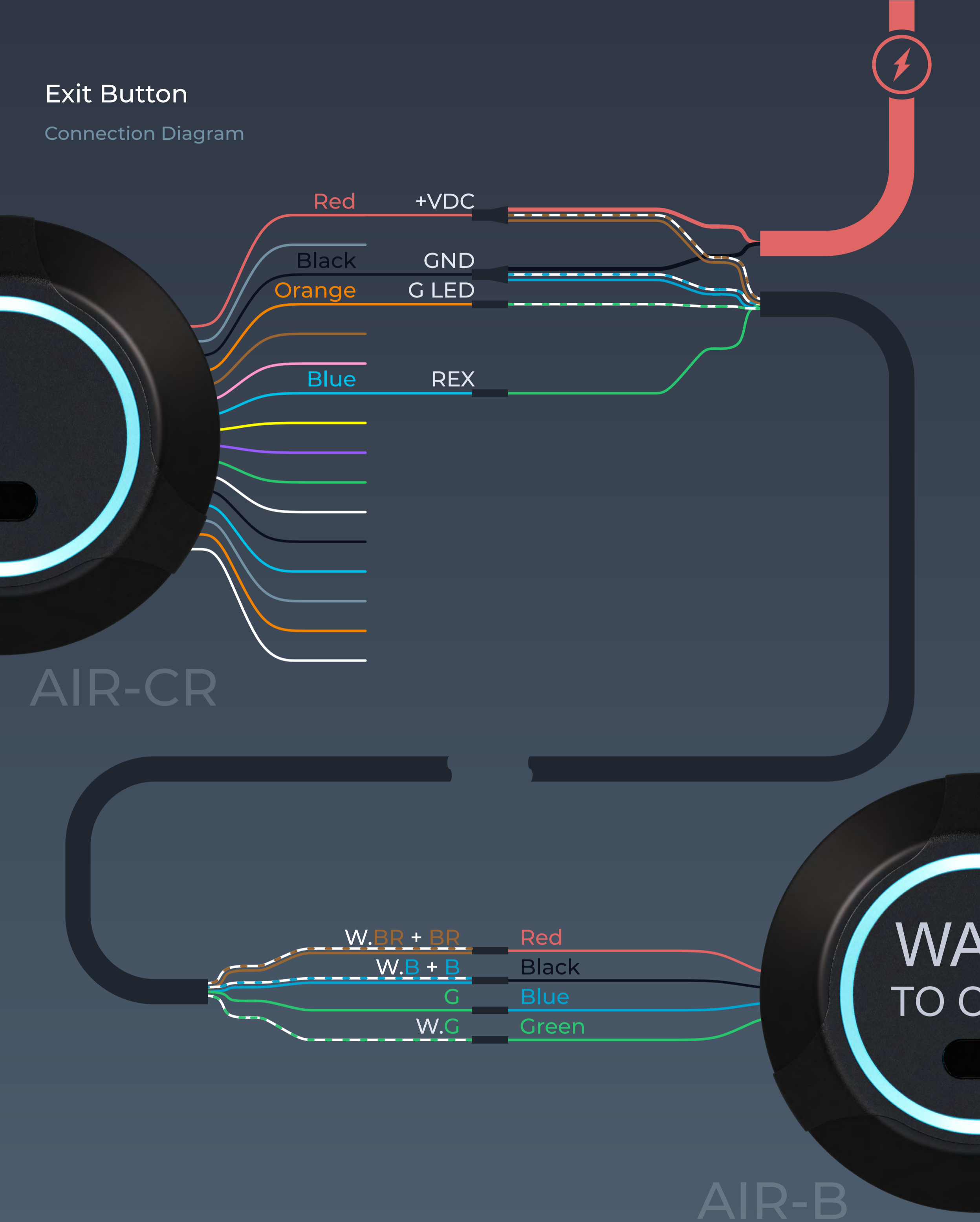
The voltage levels of the power supply and the Controller may differ depending on the cable length and the resistance of the conductor. Use a separate power supply to connect the reader if the cable is longer than 165 feet or the voltage at the end of the line is less than 10 volts.

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.

Exit Button

Connection Diagram



AIR-CR

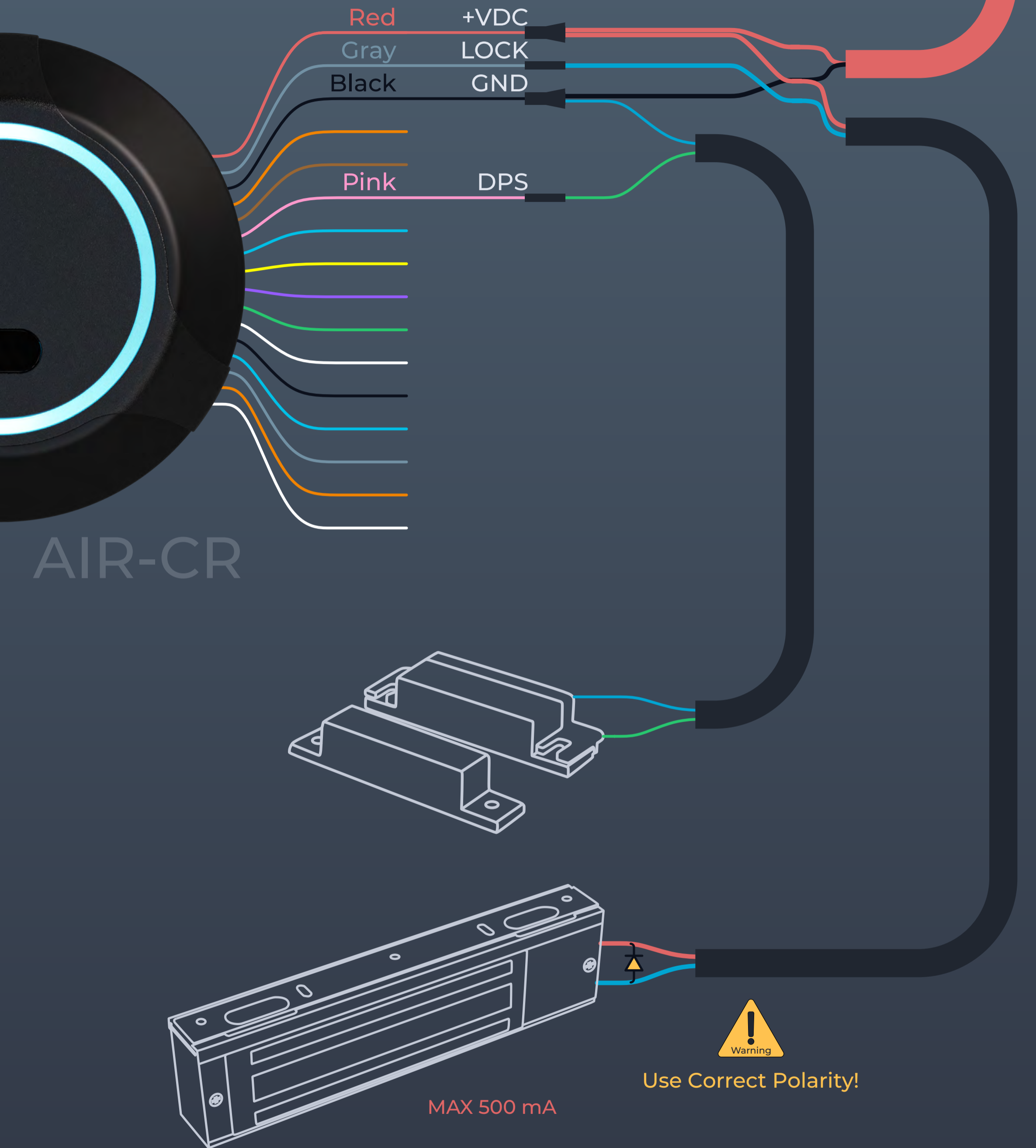
AIR-B



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.

Door Sensor & Magnetic Lock

Connection Diagram



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.

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_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.

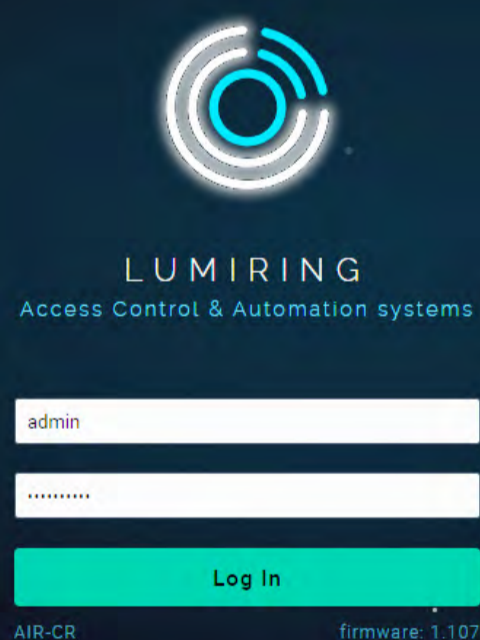
Step 1. Connect the Ethernet cable to the device using an adapter or by connecting the wires, as shown in the diagram below.

Step 2. Connect the device to a power source.

Step 3. In the address bar of your browser, enter the device IP address 192.168.1.100 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



LUMIRING
Access Control & Automation systems

admin

.....

Log In

AIR-CR firmware: 1.107

Quick Start

The screenshot displays the Lumiring Quick Start interface, which is divided into three main sections: Network, Cloud, and Security. At the top, there is a diagram showing the device (AIR-CR) connected to a cloud service. The Network section prompts the user to select a connection type (Wi-Fi network) and enter the SSID name (lumiring) and password (26022015). The Cloud section prompts the user to enter their Account ID (145) and a Device note (Hi). The Security section prompts the user to change the password for device network access and device Wi-Fi AP, with a checkbox for 'Use the same password for two purposes' and fields for the Local Wi-Fi AP name (AIR-CR_14531312), Password (8 characters minimum), and Repeat password. Each section has a 'Submit' button 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:

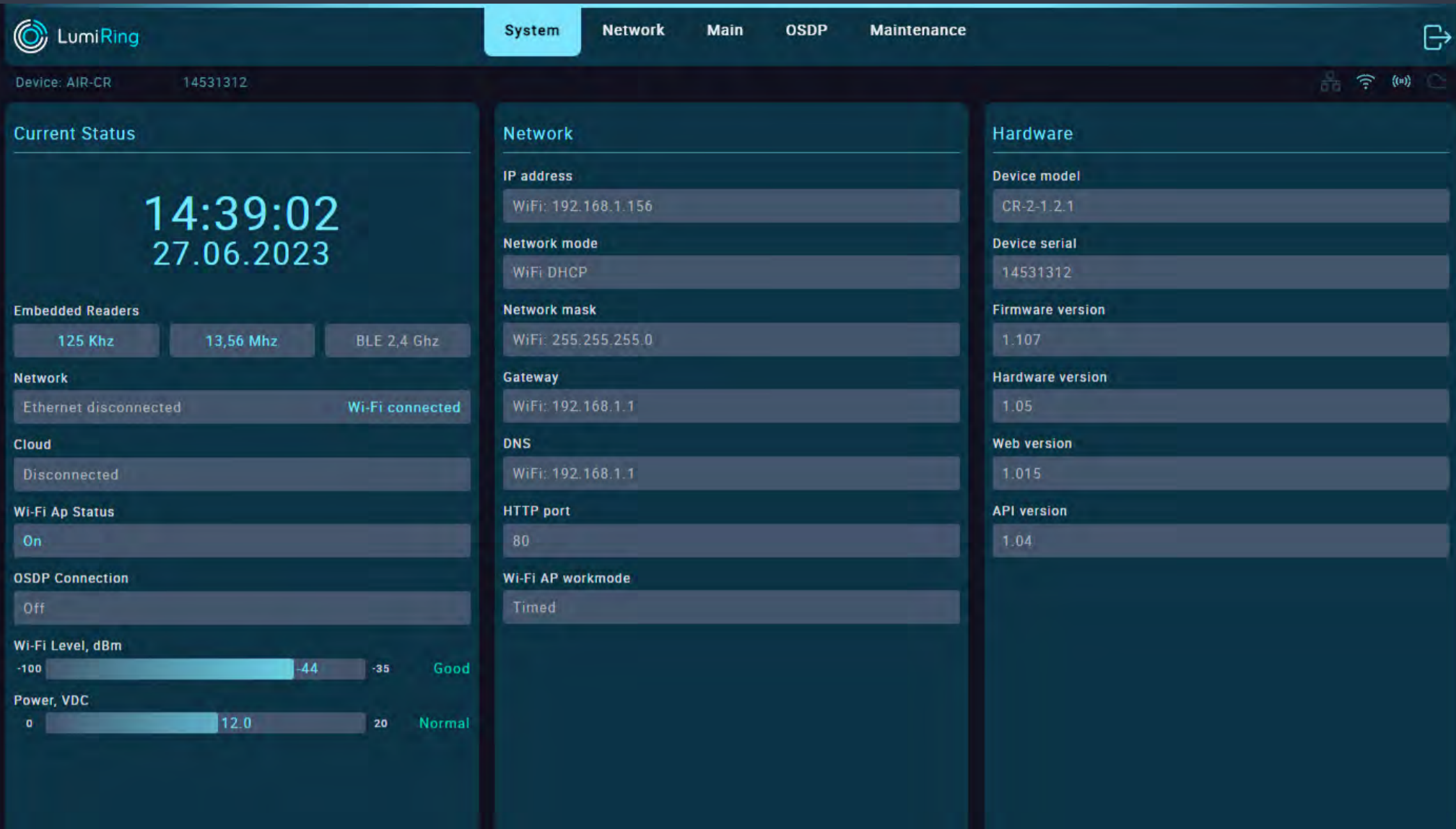
- Enter your account ID and click "Submit."

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.

System



The System 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 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.

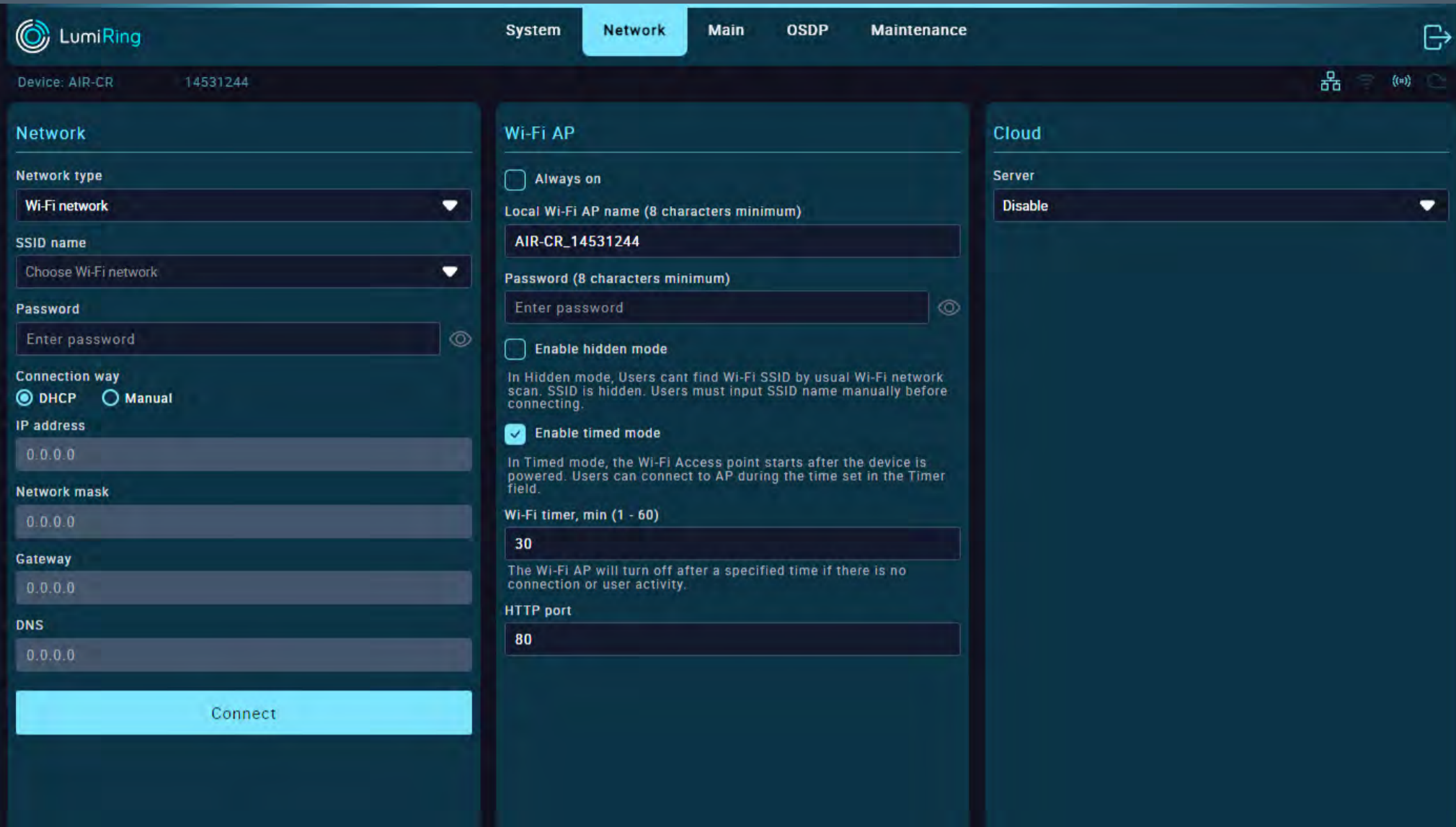
The Network subsection displays the:

- 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.

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:

- Select your preferred option for the built-in Wi-Fi AP:

- “Always on”: if checked, makes the device hotspot searchable all the time. If unchecked, makes the device's hotspot available for 30 minutes after an active connection.
- 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.
- “Enable timed mode” checkbox: allows the user to specify when the built-in Wi-Fi AP is available.
- “Wi-Fi timer” field: sets the built-in Wi-Fi AP availability time from 1 to 60 minutes.
- HTTP port: By default, the device uses port 80.

Network

The screenshot shows the LumiRing Network configuration page. At the top, there are navigation tabs: System, Network (selected), Main, OSDP, and Maintenance. The device information is AIR-CR 14531244. The Network section is configured with 'Wired Ethernet Network' type, 'Manual' connection, IP 192.168.1.100, mask 255.255.255.0, gateway 192.168.1.1, and DNS 8.8.8.8. The Wi-Fi AP section has 'Always on' unchecked, local name 'AIR-CR_14531244', and 'Enable timed mode' checked. The Cloud section is configured with 'Unimacs' server, 'Auto connect' button, and various MQTT topics.

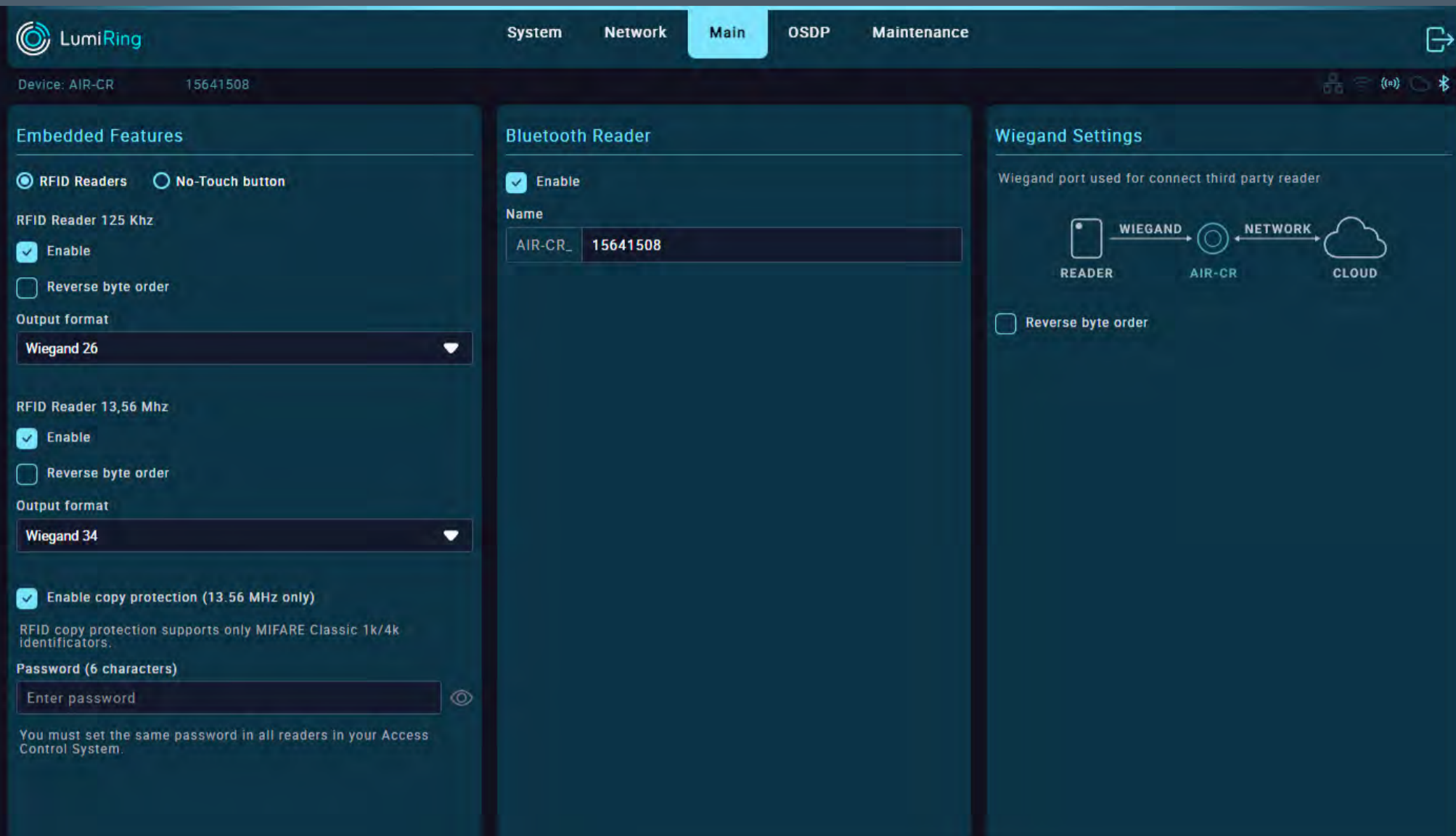
The Cloud settings subsection allows you to connect the controller to a cloud server for later use.

- 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.
- Next you need to select the connection method. If you have connected the device to the Internet via Ethernet cable, then specify the connection method as Ethernet. If you connected the device to the Internet using a Wi-Fi connection, specify the connection method as Wi-Fi.
- The Account ID form is used for adding to the UNIMACS cloud system, as you only need to specify the ID to connect.

When connecting to other cloud systems, you may need to enter server address, login password, and invite key.

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

Main



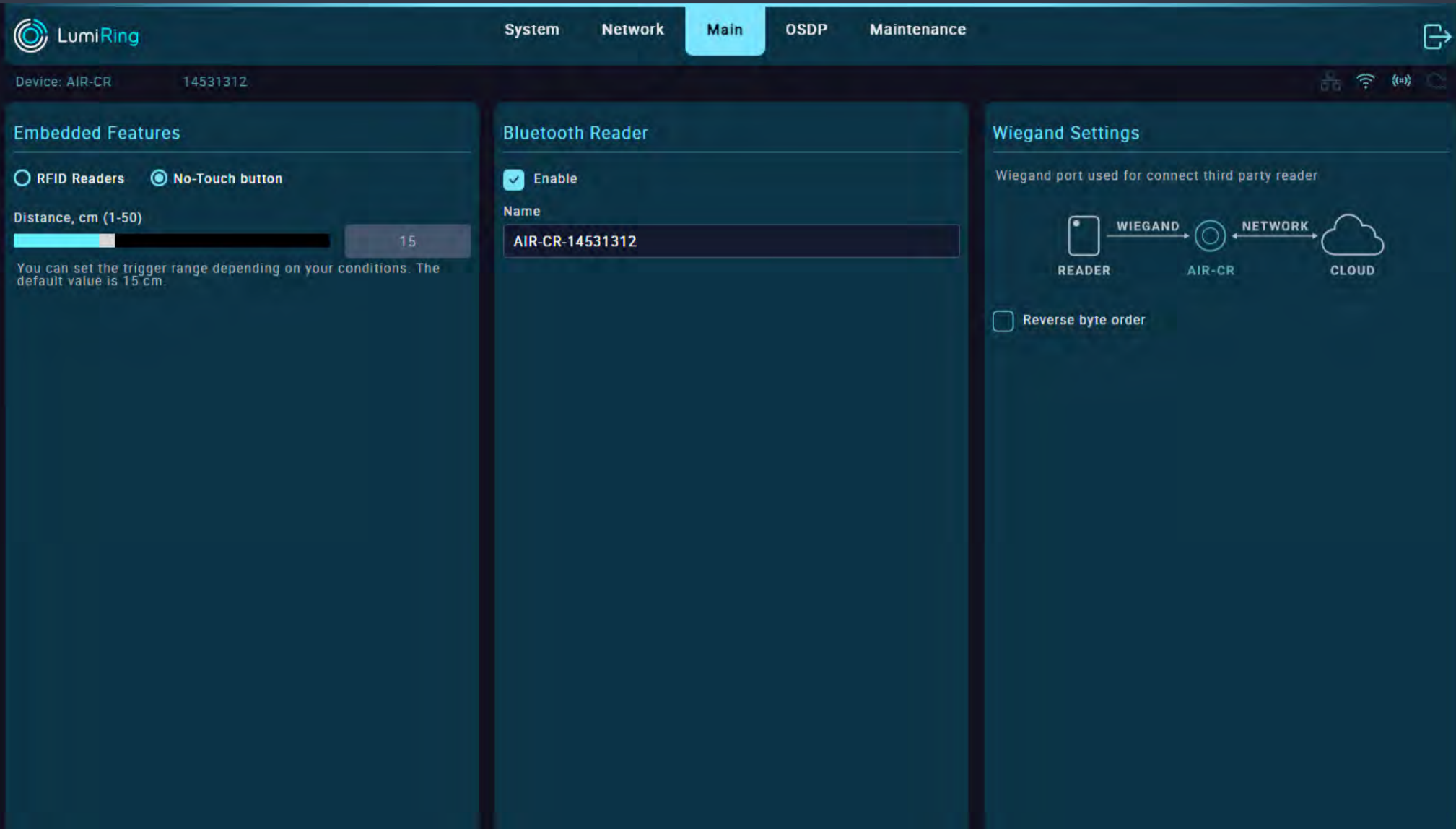
The Main section allows you to configure the functionality of the device and determine the modes of operation.

- The “RFID” 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.
- Enter the ID encryption password.

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.

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

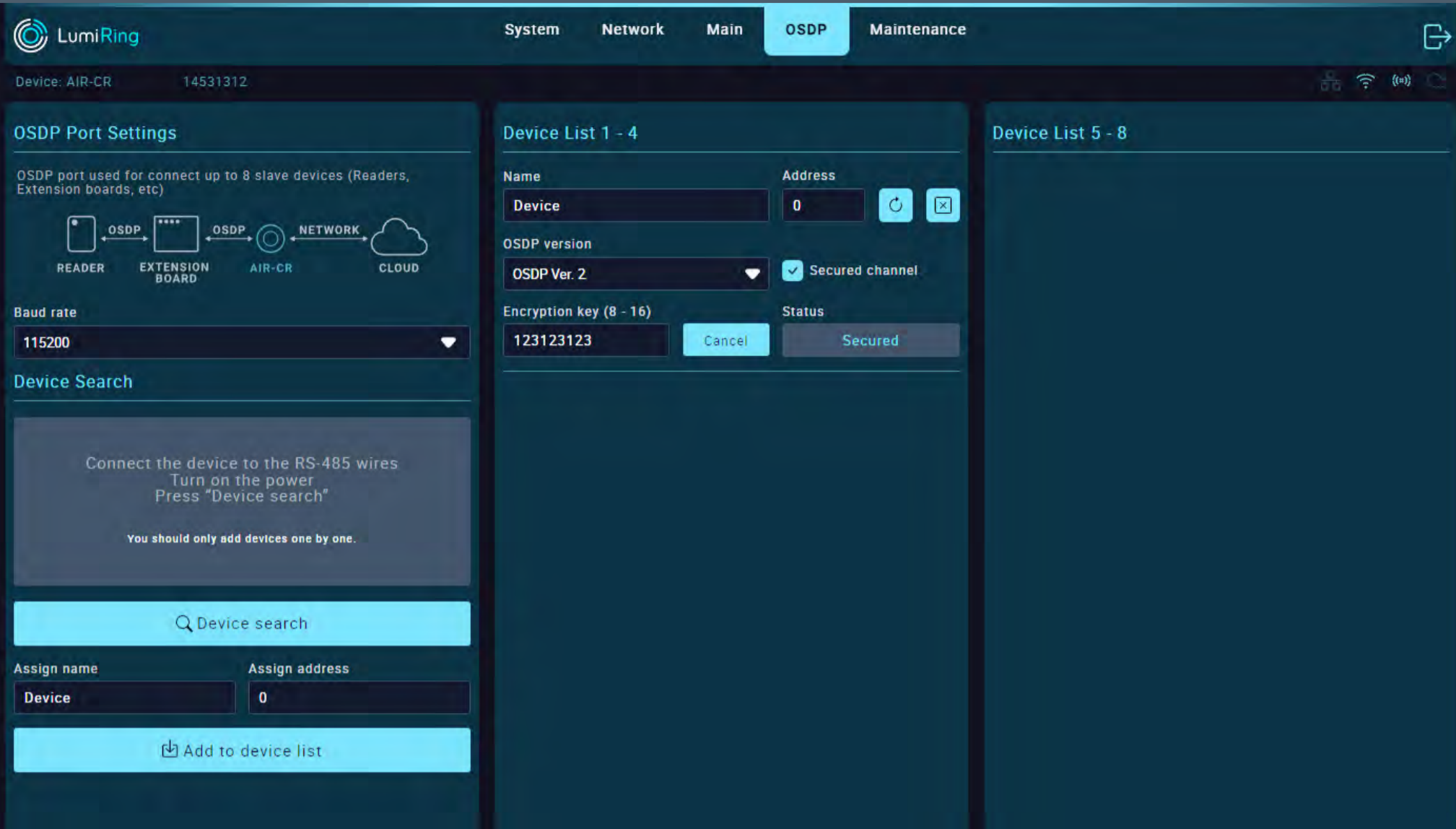


The Main section allows you to configure the functionality of the device and determine the modes of operation.

- 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.

Open Supervised Device Protocol (OSDP) OSDP is coming soon!



The Open Supervised Device Protocol (OSDP) Port Settings subsection allows you to configure the connection of external devices and shows the interaction method on the diagram.

- Select the required baud rate for all connected devices in the baud rate form.

The Device Search subsection allows you to detect the presence of a connected device automatically. Automatic detection is performed if the device can publish data about itself.

- It is necessary to perform a search and subsequent addition by connecting devices individually. This means there can be up to one unknown device on the line.
- After a device is detected by auto-search, information about it is displayed in the information field, and you can assign a name and physical address to the found device.
- Clicking the “Add to the device list” button will add the device to the list on the left.

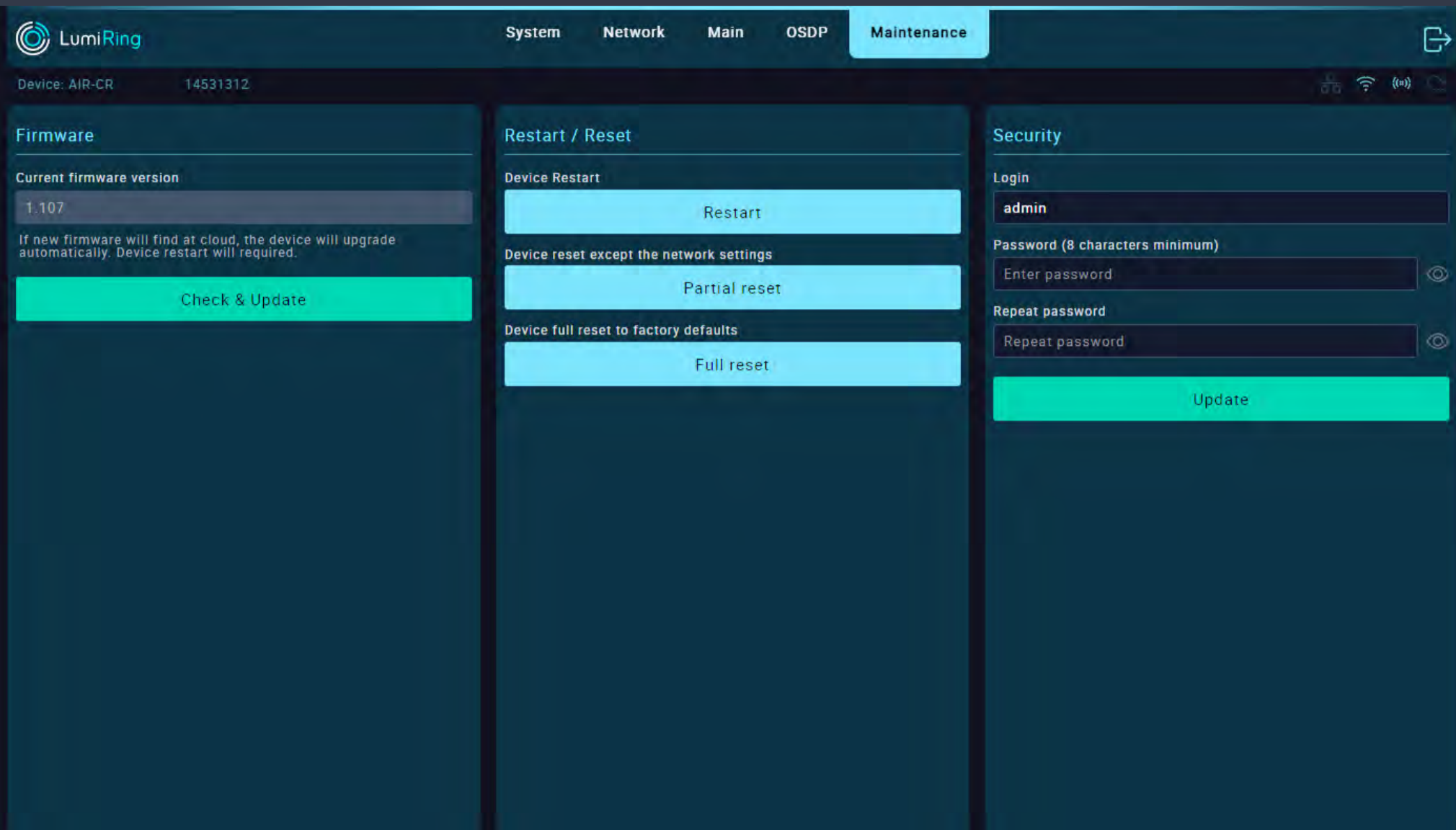
In the Device List 1-4 subsection, you can make additional settings for each device individually.

- You can edit each device’s name and address, remove it from the list, and use the OSDP version.
- Selecting version 2 of the OSDP allows the use of a secure channel.
- Check the appropriate box and enter the connected device's encryption key. After clicking the "Link" button, the result of establishing a secure connection is displayed - Secured or Not Secured.

Note: To determine the device to be added by OSDP, the "Installation Mode" function must be enabled. If this condition is not met, the device being added may not be detected or configured. After finishing adding and configuring, turn off "Installation Mode" on the device being added.

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

Maintenance



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

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

- To download a new firmware version, connect to a network with Internet access in the Network section.

Note: Connect to a network with Internet access in the Network section (see page 17)

- 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:

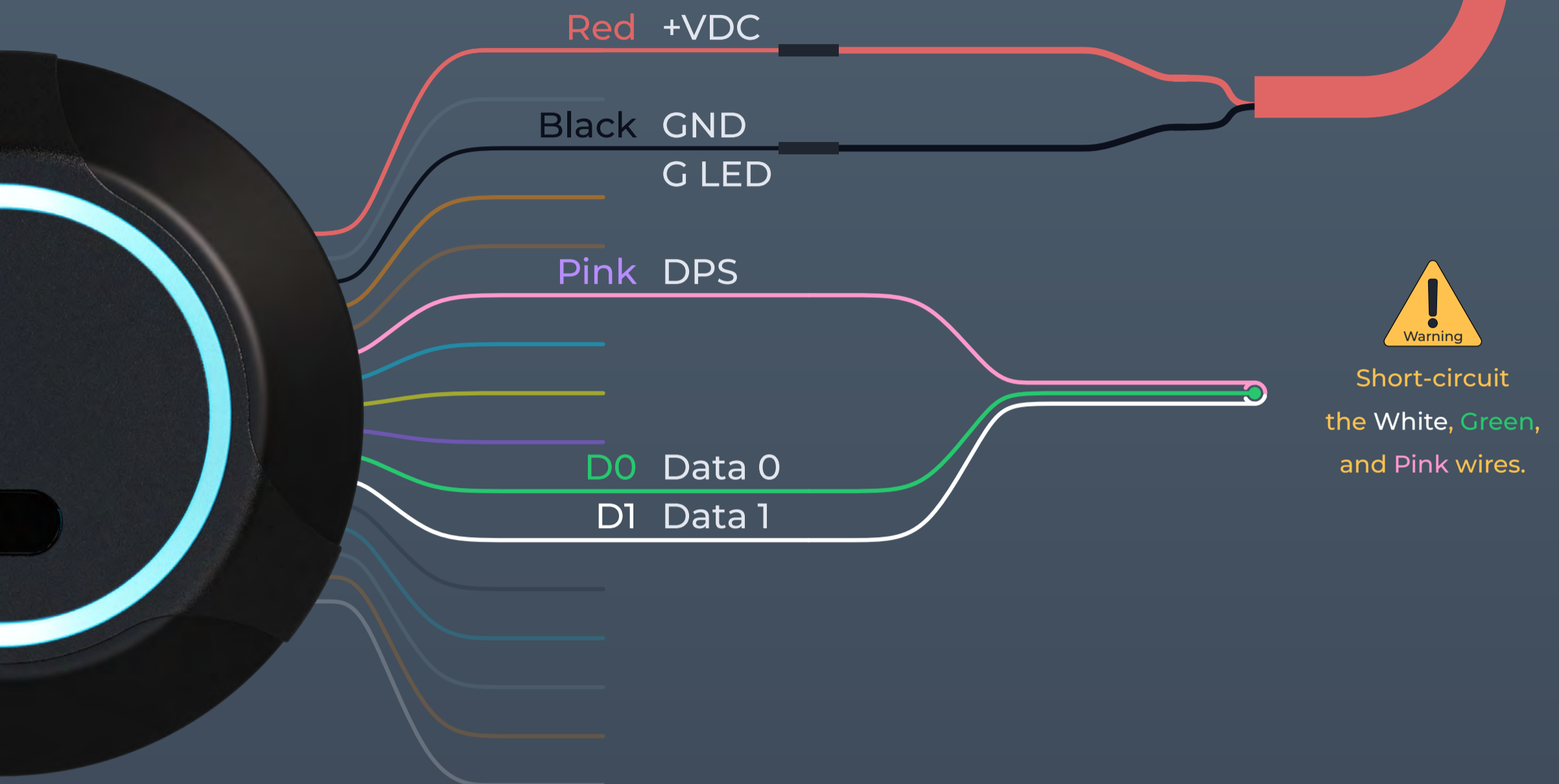
- Restart - restarts the device.
- Partial reset - resets all device settings except for network connection settings.
- Full reset - resets all settings of the device to factory defaults.

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 With Wires



Hardware reset

1. Turn off the power to the device.
2. Disconnect the white, green, and pink wires to 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.



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

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.
- 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.
- 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.

Glossary

- **GND** - Electrical ground reference point.
- **HTTP** - Hypertext Transfer Protocol. A fundamental protocol for transferring data, documents, and resources over the Internet.
- **RFID Identifier 125 kHz** - Radio-frequency identification at 125 kHz; short-range, low-frequency technology with a typical range of 7 cm to 1 m.
- **RFID Identifier 13.56 MHz** - Radio-frequency identification at 13.56 MHz; high-frequency technology with short to moderate range, around 10 cm.
- **Keypad** - A physical input device with a set of buttons or keys, often used for manual data entry or access control.
- **LED** - Light emitting diode.
- **Loop sensor** - A device that detects the presence or passage of traffic in a certain area by means of a closed electrical loop. Used in barriers or gates.
- **Magnetic Lock** - A locking mechanism that uses electromagnetic force to secure doors, gates, or access points.
- **MQTT** - Message Queuing Telemetry Transport. A server system that coordinates messages between different clients. The broker is responsible, among other things, for receiving and filtering messages, identifying the clients subscribed to each message, and sending messages to them.
- **NC** - Normally closed. Configuration of a changeover contact that is closed in the default state and open when activated.
- **Network access controller** - The fundamental element of an ACS (access control and management system). This device serves as a control center for all links (locks, turnstiles, drives, barriers), receiving a signal from the reader and giving a command to admit or deny a visitor to the object.
- **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.
- **OTA update** - Over-the-air update. The process of remotely and wirelessly updating software or firmware on a device.
- **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.

Glossary

- **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.
- **Secured channel** - A protected and encrypted communication path that ensures data confidentiality and integrity between two or more parties.
- **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

