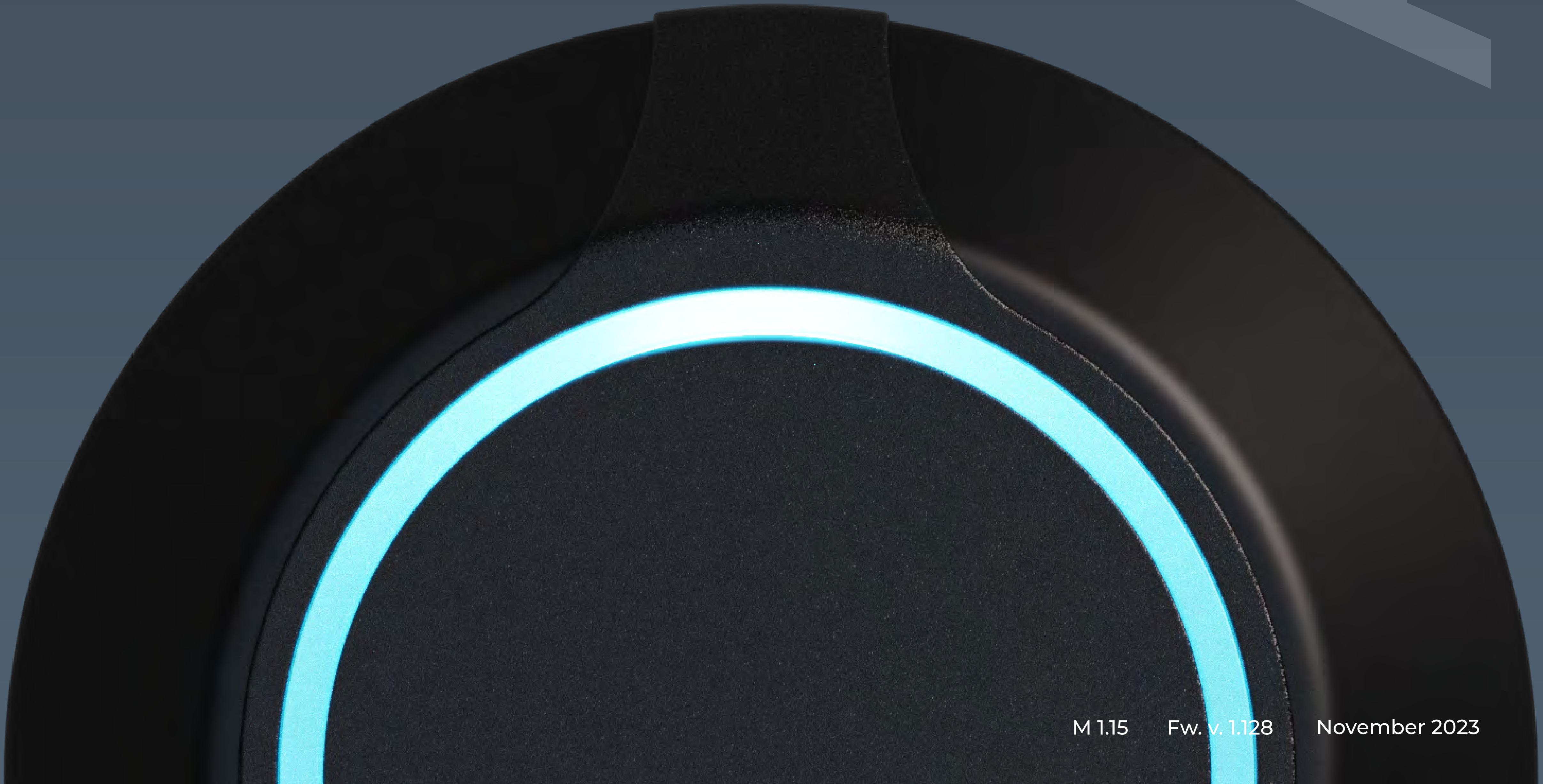
Device version by Pometkov

InVid Tech

Innovative Video Technology

AIIR-R

MANUAL



M 1.15 Fw. v. 1.128 November 2023

CONTENTS

Introduction

This document provides detailed information on the AIR-R Pro reader 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-R Pro_(serial number)
• Access Point (AP) Wi-Fi IP address of the device	192.168.4.1
• 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-R Pro
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
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 (voltage direct current)	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

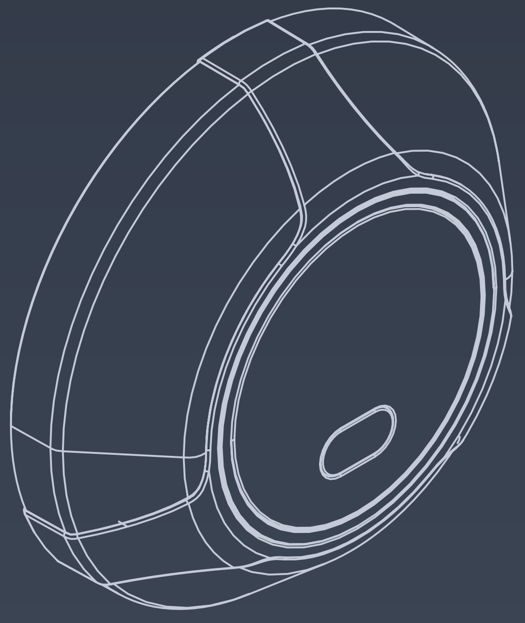
Operating temperature	-22°F ~ 158°F (-30°C ~ 70°C)
Ingress Protection rating	IP65

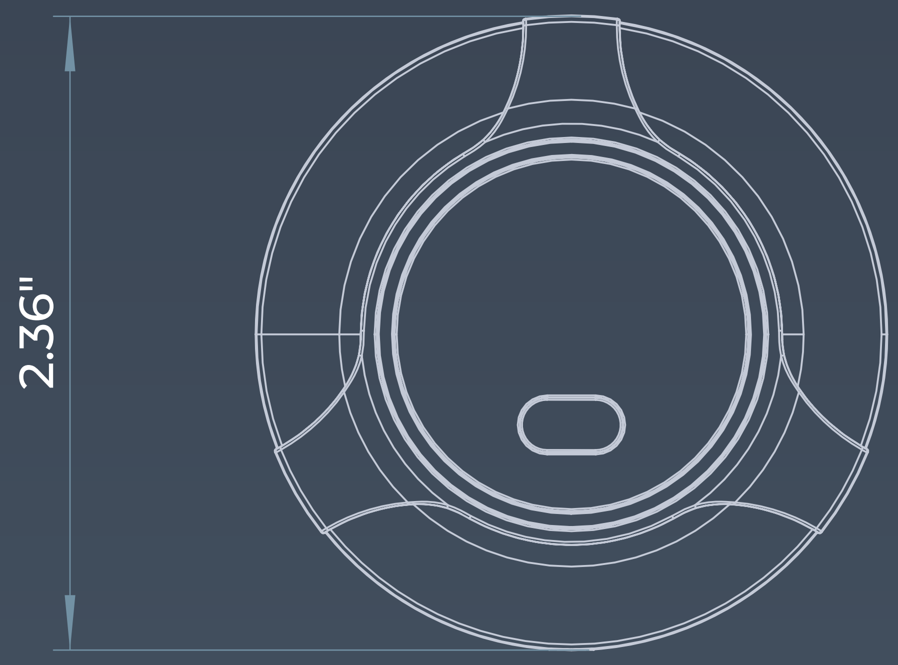
Physical characteristics

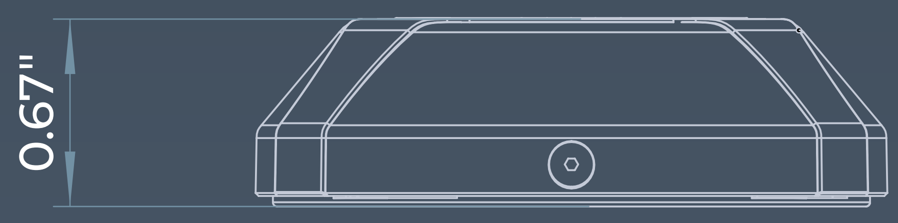
Housing material	ABS plastic UL94 V-0
Mounting method	Wall mount
Dimensions (diameter, height)	2.36" x 0.67" (60 x 17 mm) (mounting ring) 2.36" x 0.86" (60 x 22 mm)
Weight	1.59 oz (45 g)

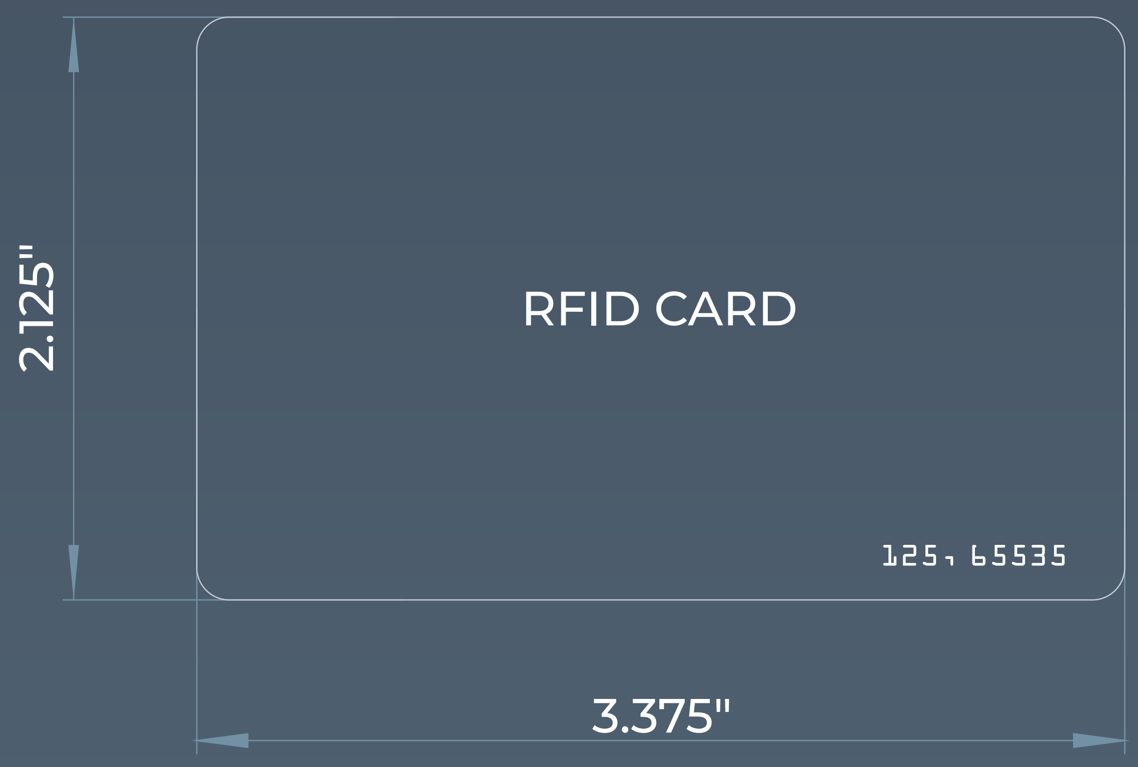
* When using OSDP.
** See general specifications for RS-485 interface.

Device Dimensions

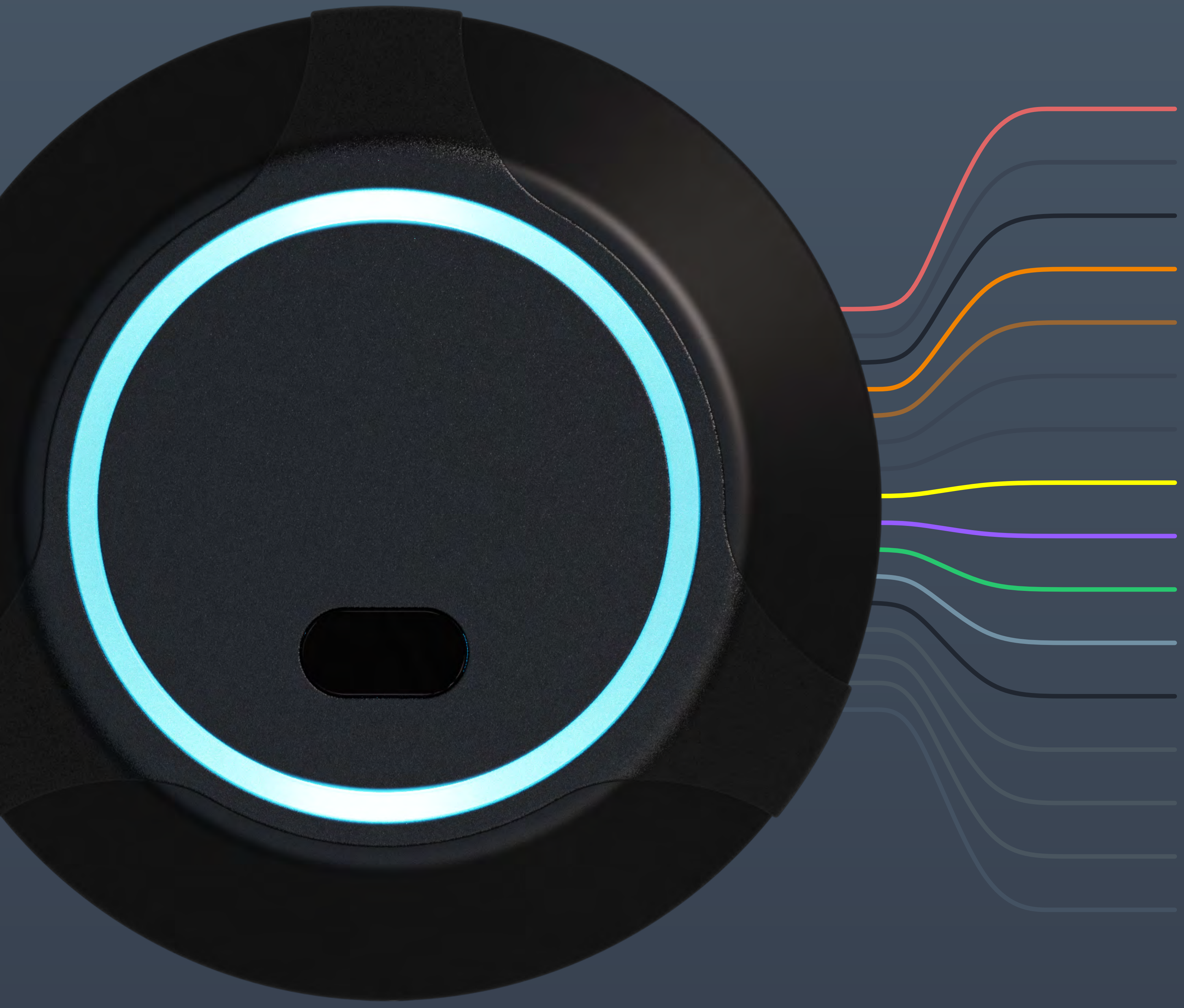








Wire Designation



Red	1	+VDC
Gray	2	GND Lock
Black	3	GND
Orange	4	Green LED
Brown	5	Red LED
Pink	6	DPS
Blue	7	Exit Button
Yellow	8	RS-485 A+
Purple	9	RS-485 B-
Green	10	Data 0
White	11	Data 1
Black	12	GND
Blue	13	TX-
Gray	14	TX+
Orange	15	RX-
White	16	RX+

The current hardware version of the AIR-R Pro reader has more wires than is needed for installation and use. This is necessary for future improvements and extensions of the device.
The wires required to connect the AIR-R Pro reader are highlighted in color.
The type of device determines the order and purpose of the wires.
The numbering starts with the red wire (number 1) and reads from left to right.
Wires that are not used should be ignored.

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.

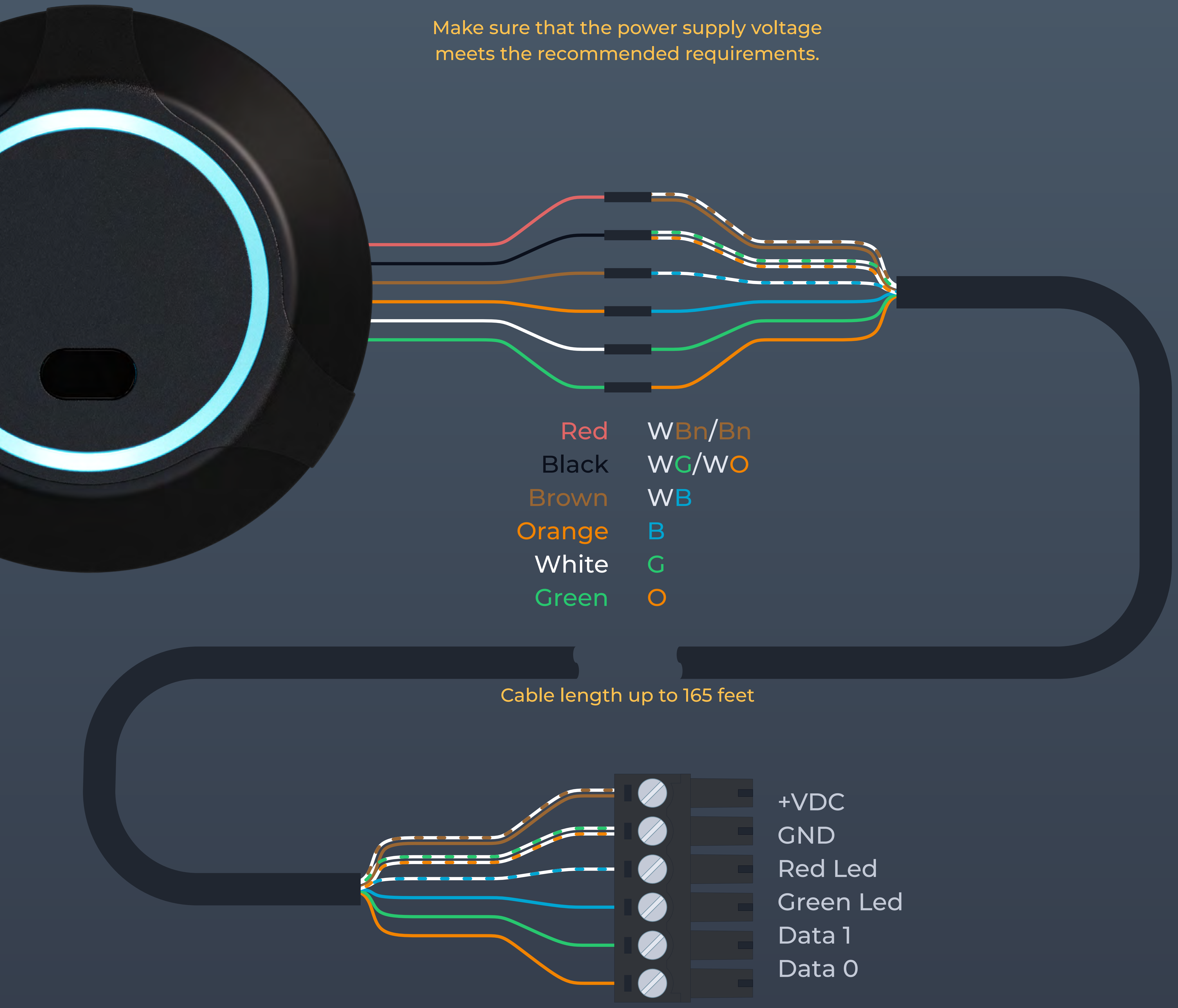
After cabling, ensure that the power supply voltage to the reader is at least 12 VDC with the locks switched on.

Wiegand Interface

Connection Diagram

Warning

Make sure that the power supply voltage meets the recommended requirements.



Red	WBn/Bn
Black	WG/WO
Brown	WB
Orange	B
White	G
Green	O

Cable length up to 165 feet

Example of connection to the terminal blocks of ICON and ICON-Pro controllers.

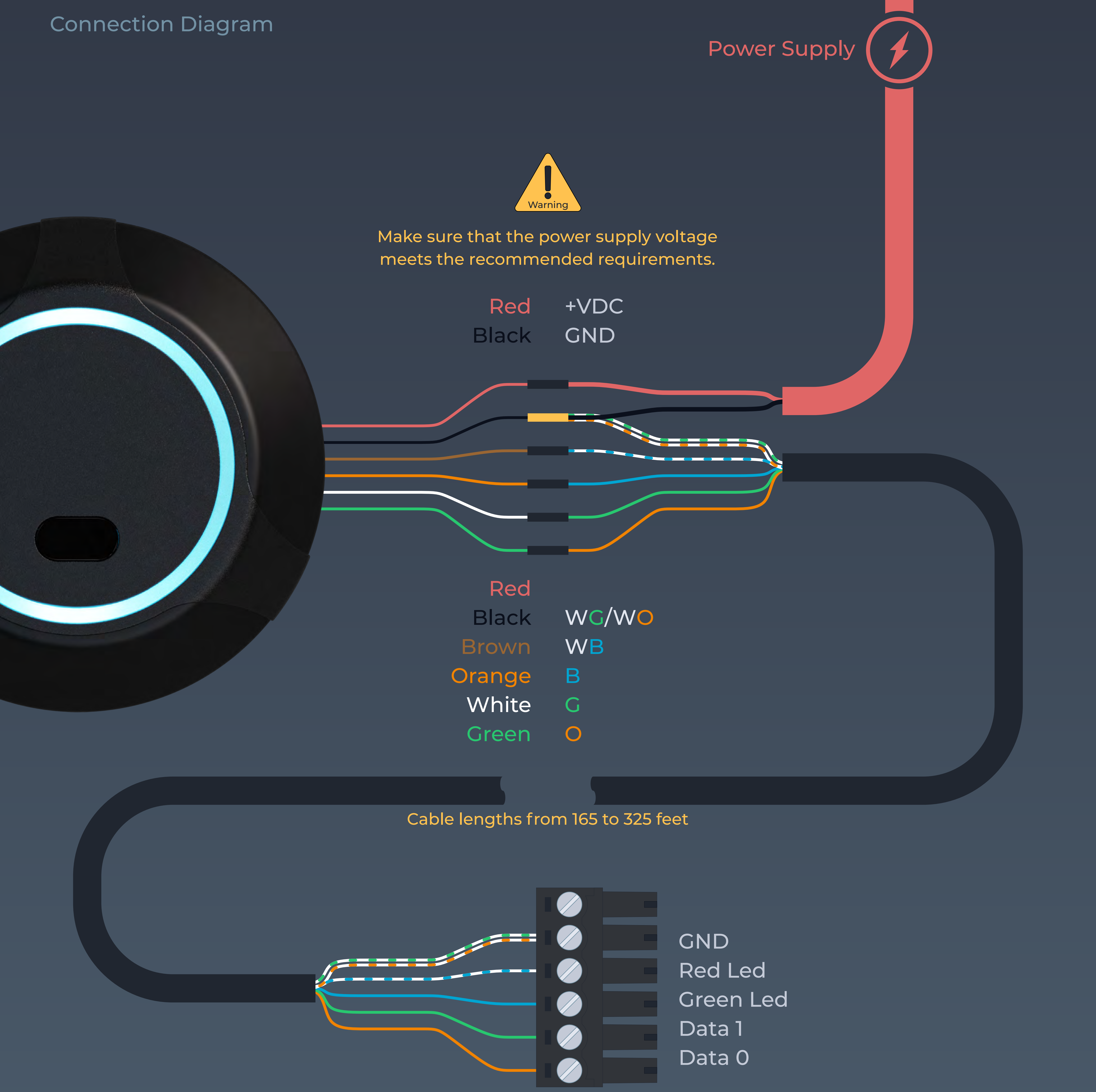
To connect the reader to third-party controllers, please refer to the manufacturer's instructions.

Warning

The voltage level at the power supply and at the reader may differ depending on the cable length and the resistance of the conductor.
The recommended voltage should be at least +10 VDC.
Use a multimeter in the VDC measurement mode to verify that the power supply voltage meets the recommended requirements.

Wiegand Interface with Additional Power Supply

Connection Diagram



Make sure that the power supply voltage meets the recommended requirements.

Red	+VDC
Black	GND

Red	
Black	WG/WO
Brown	WB
Orange	B
White	G
Green	O

Cable lengths from 165 to 325 feet

Example of connection to the terminal blocks of ICON and ICON-Pro controllers.

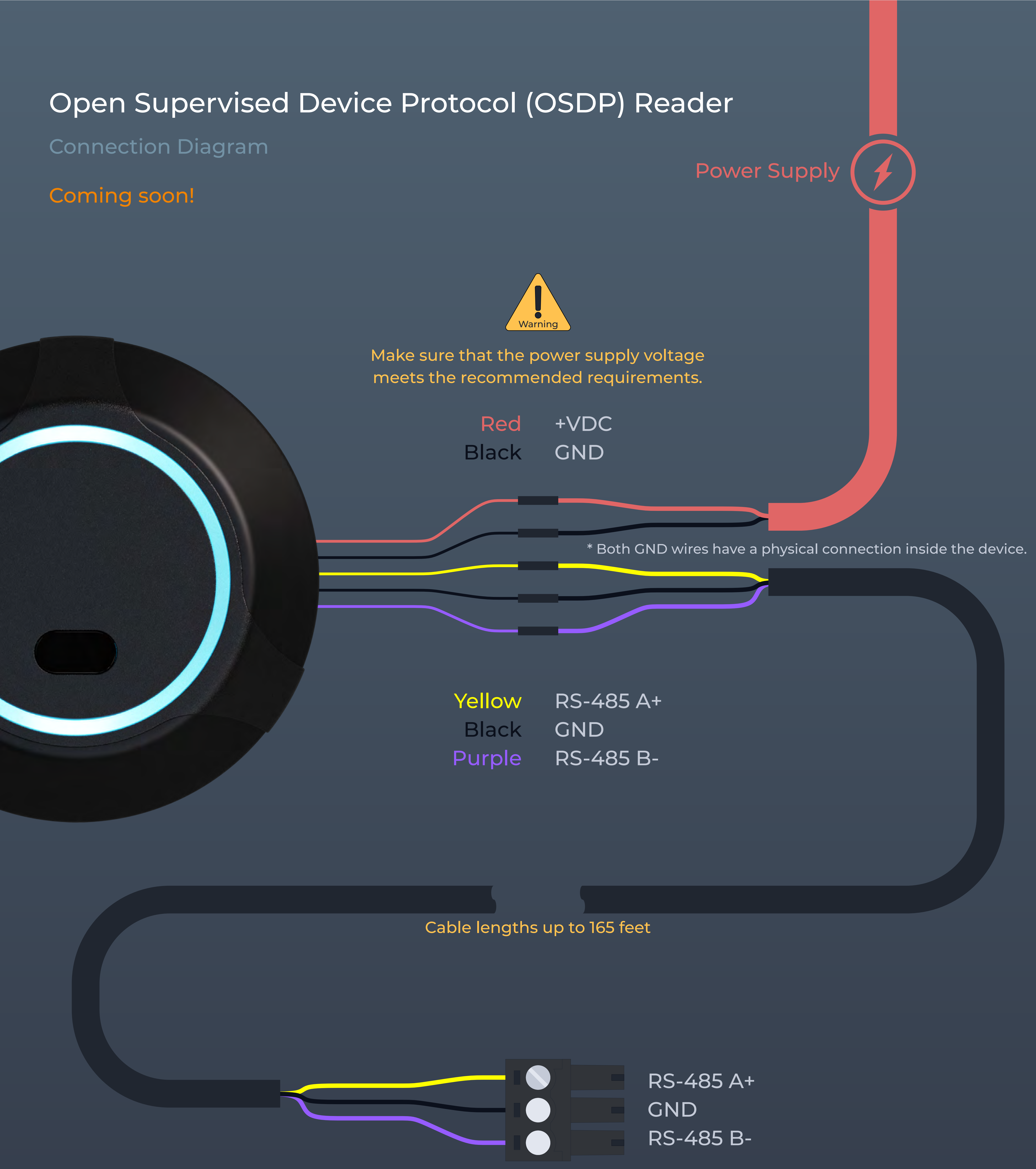
To connect the reader to third-party controllers, please refer to the manufacturer's instructions.

The voltage level at the power supply and at the reader 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

Connection Diagram

Coming soon!



Power Supply

Make sure that the power supply voltage meets the recommended requirements.

Red	+VDC
Black	GND

* Both GND wires have a physical connection inside the device.

Yellow	RS-485 A+
Black	GND
Purple	RS-485 B-

Cable lengths up to 165 feet

RS-485 A+
GND
RS-485 B-

Example of connection to ICON controller terminal blocks.

To connect the reader to third-party controllers, please refer to the manufacturer's instructions.

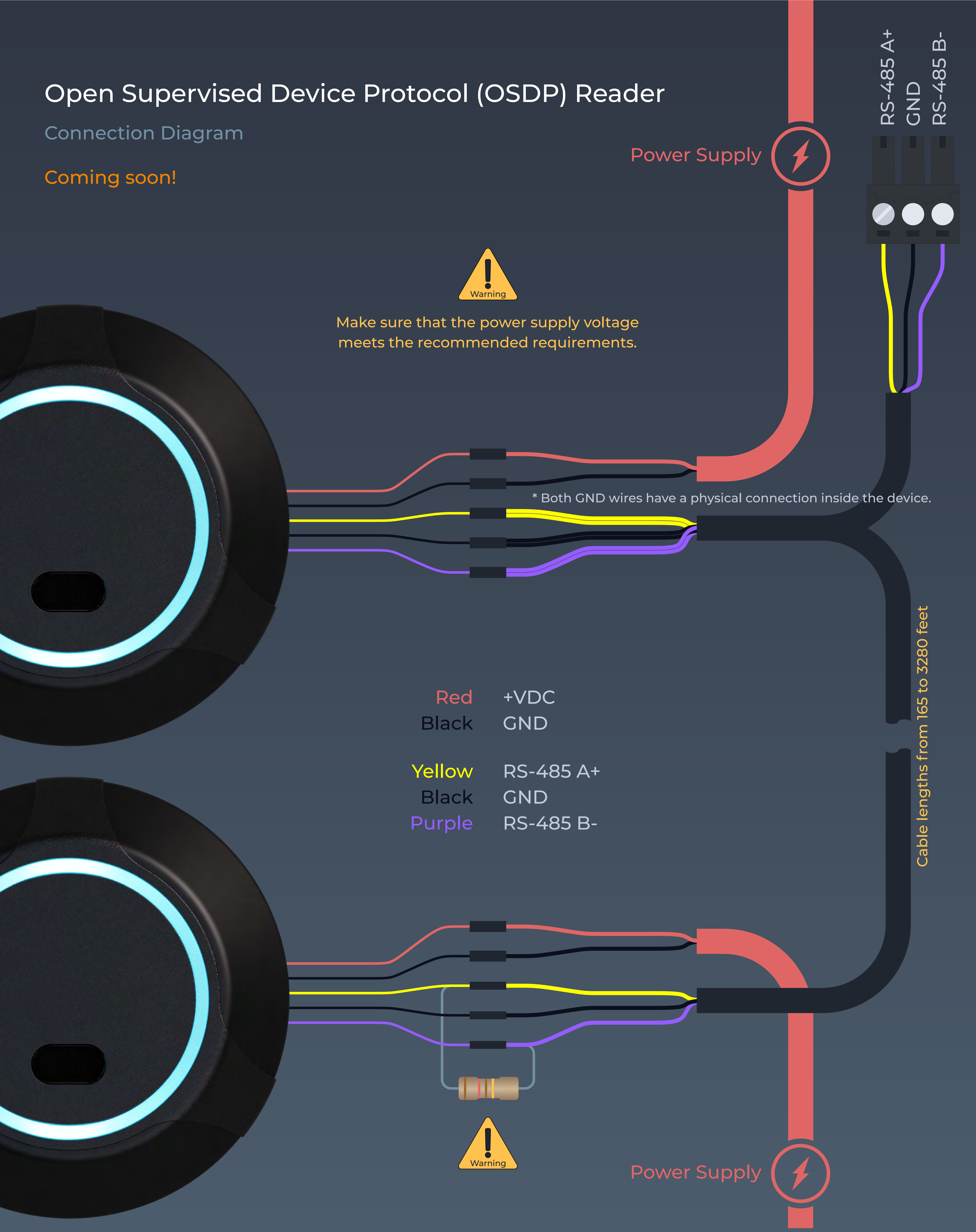
Warning

The voltage level at the power supply and at the reader 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

Connection Diagram

Coming soon!



Make sure that the power supply voltage meets the recommended requirements.

* Both GND wires have a physical connection inside the device.

Red	+VDC
Black	GND
Yellow	RS-485 A+
Black	GND
Purple	RS-485 B-

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!

Terminal resistors ensure that the "open" end of the cable is matched to the rest of the line, eliminating signal reflection.
The nominal resistance of the resistors corresponds to the wave impedance of the cable, and for twisted-pair cables is typically 100 to 120 ohms.
Install a 120 ohm terminating resistor on the outermost reader if the cable runs more than 150 feet.
See RS-485 interface specifications for more information.

Bluetooth Keys Coming soon!

Announcement of an alternative smartphone app to replace ViKey Wallet.

CRYPTOKEY

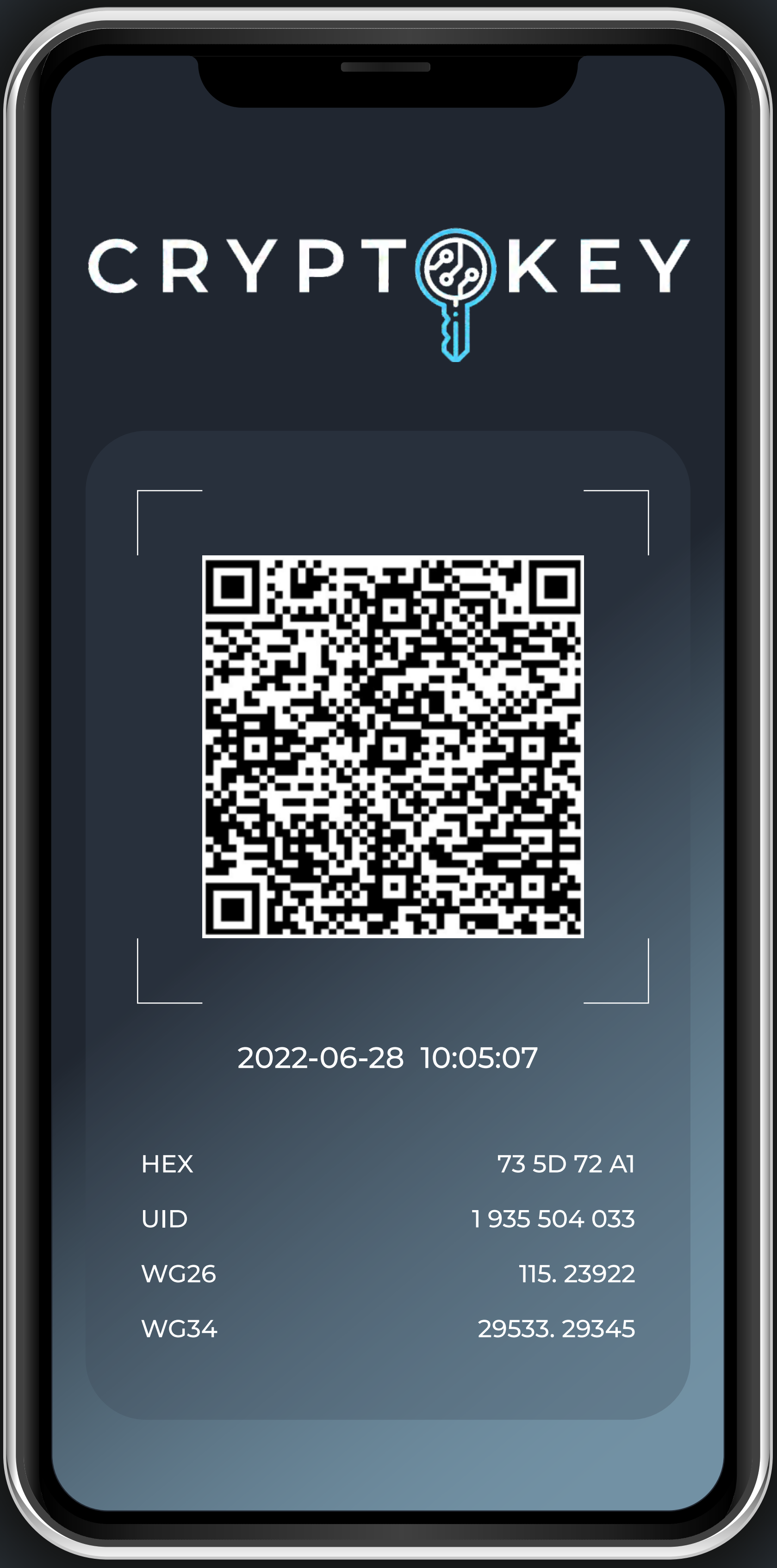
1. Sign up for the cryptokeys.com Cloud Service.

2. Purchase as many AIR Keys as you like.

You can order AIR Keys directly from the Cloud Service or ask your supplier.

3. Transfer the AIR Key to your phone.

The Key is transferred as a digital card with a QR code and key data. The Key can be sent to the user's email directly from a cloud account.



CRYPTOKEY

2022-06-28 10:05:07

HEX	73 5D 72 A1
UID	1 935 504 033
WG26	115. 23922
WG34	29533. 29345

4. Assign the AIR Key to the reader.

Press the bind key and select the Bluetooth reader from the list of detected readers. Confirm the addition of the AIR Key by waving your hand in front of the reader after the yellow light appears.

Access Control System

5. Add the AIR key code to the access control system you are using as a normal card.

Connecting to the Built-in Wi-Fi Access Point

You can use a smartphone, tablet, or other Wi-Fi-capable device to connect to the AIR-R Pro.

To connect to a device, follow these steps:

Step 1: Connect the device to a power source using the wiring diagram provided in the technical documentation.

Step 2: Search for Wi-Fi networks.

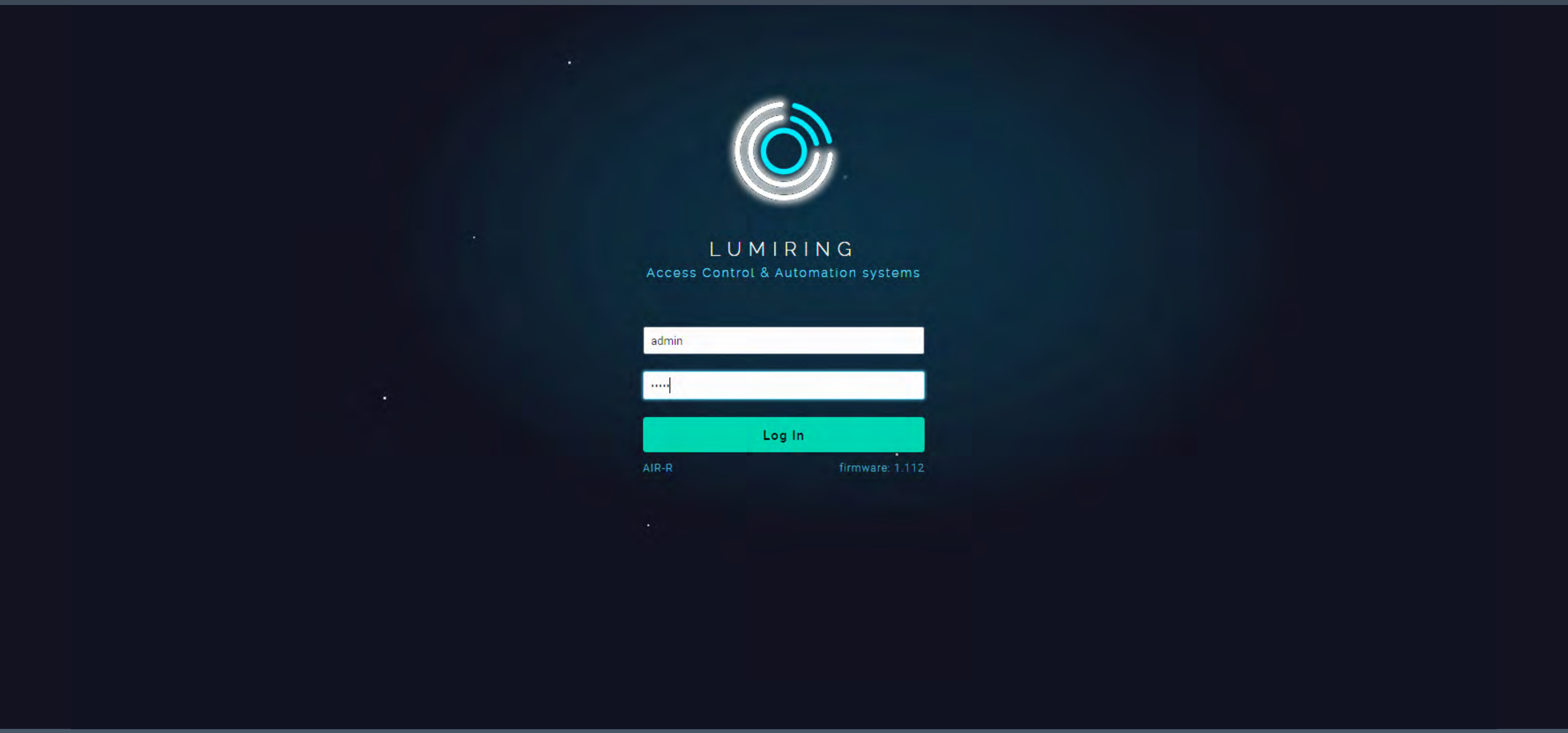
Step 3: Connect to the Wi-Fi network named AIR-R Pro_xxxxxxxxxxxx, where xxxxxxxxxxxxx is the serial number found on the sticker on your device.

Step 4: In the address bar of the browser, enter the network address 192.168.4.1 and click "Go."

Step 5: On the login page (see screenshot below), enter the default login and password: Login - admin / Password - admin.

The browser will automatically redirect you to the System page.

Login



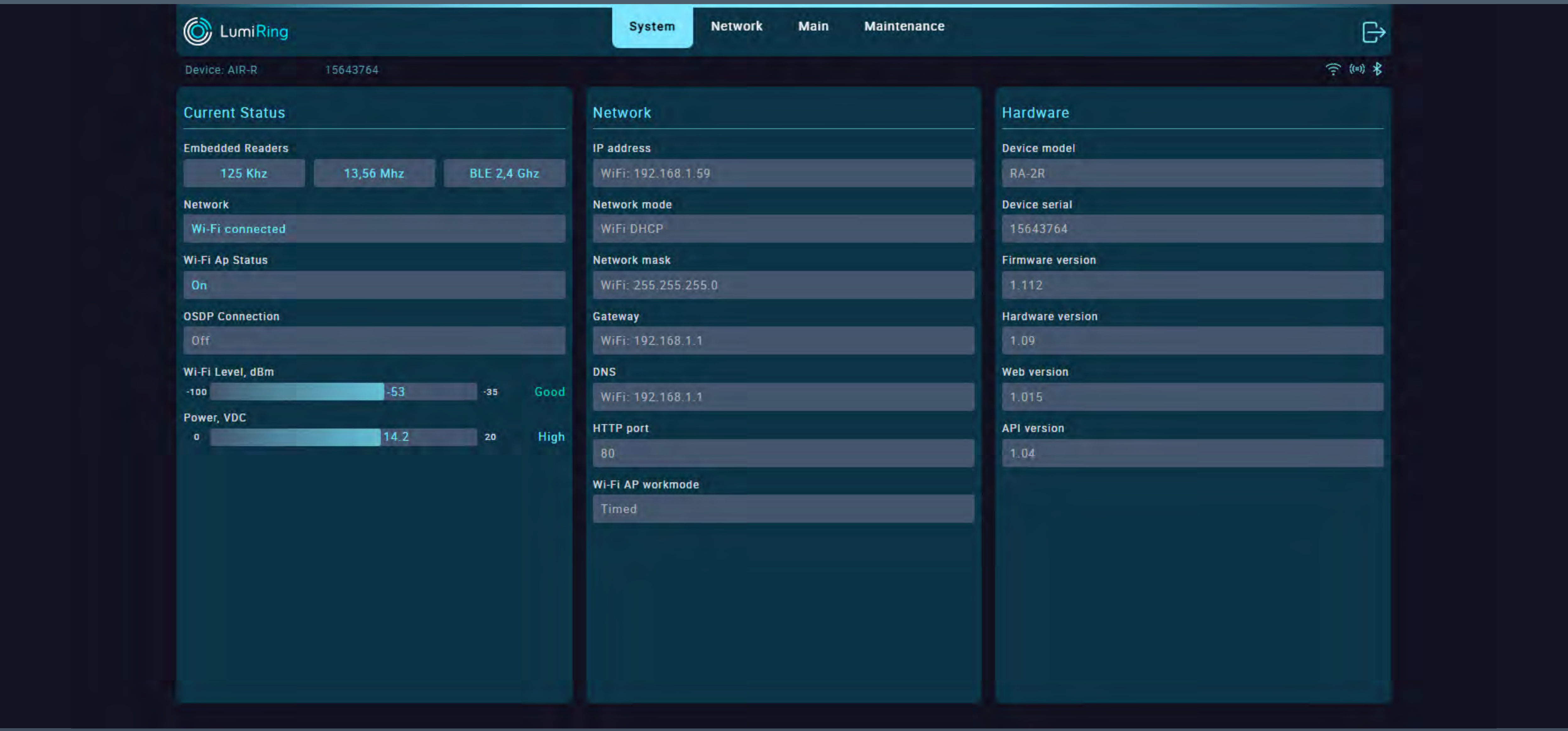
admin

•••••

Note: If you are logging in for the first time or after a factory reset, please use admin/admin.

Important!
The device interface does not provide a password reminder or reset. If you need to change the configuration of the device and you do not remember the password, you will have to perform a hard reset. Remember the password you use or keep it in a safe place.

System



Device: AIR-R 15643764

Current Status

Embedded Readers: 125 Khz | 13,56 Mhz | BLE 2,4 Ghz

Network: Wi-Fi connected

Wi-Fi Ap Status: On

OSDP Connection: Off

Wi-Fi Level, dBm: -100 … -53 … -35 Good

Power, VDC: 0 … 14.2 … 20 High

Network

IP address: WiFi: 192.168.1.59

Network mode: WiFi DHCP

Network mask: WiFi: 255.255.255.0

Gateway: WiFi: 192.168.1.1

DNS: WiFi: 192.168.1.1

HTTP port: 80

Wi-Fi AP workmode: Timed

Hardware

Device model: RA-2R

Device serial: 15643764

Firmware version: 1.112

Hardware version: 1.09

Web version: 1.015

API version: 1.04

This section displays information about the current settings and status of the device.

The Current Status subsection displays the:

- Status of embedded readers 125kHz, 13.56 MHz, and BLE 2.4 GHz.
- The status and type of connection of the device's to the router in use.
- Status of the built-in Wi-Fi access point.
- Level and quality of the device's connection to the Wi-Fi router.
- Power supply voltage value.

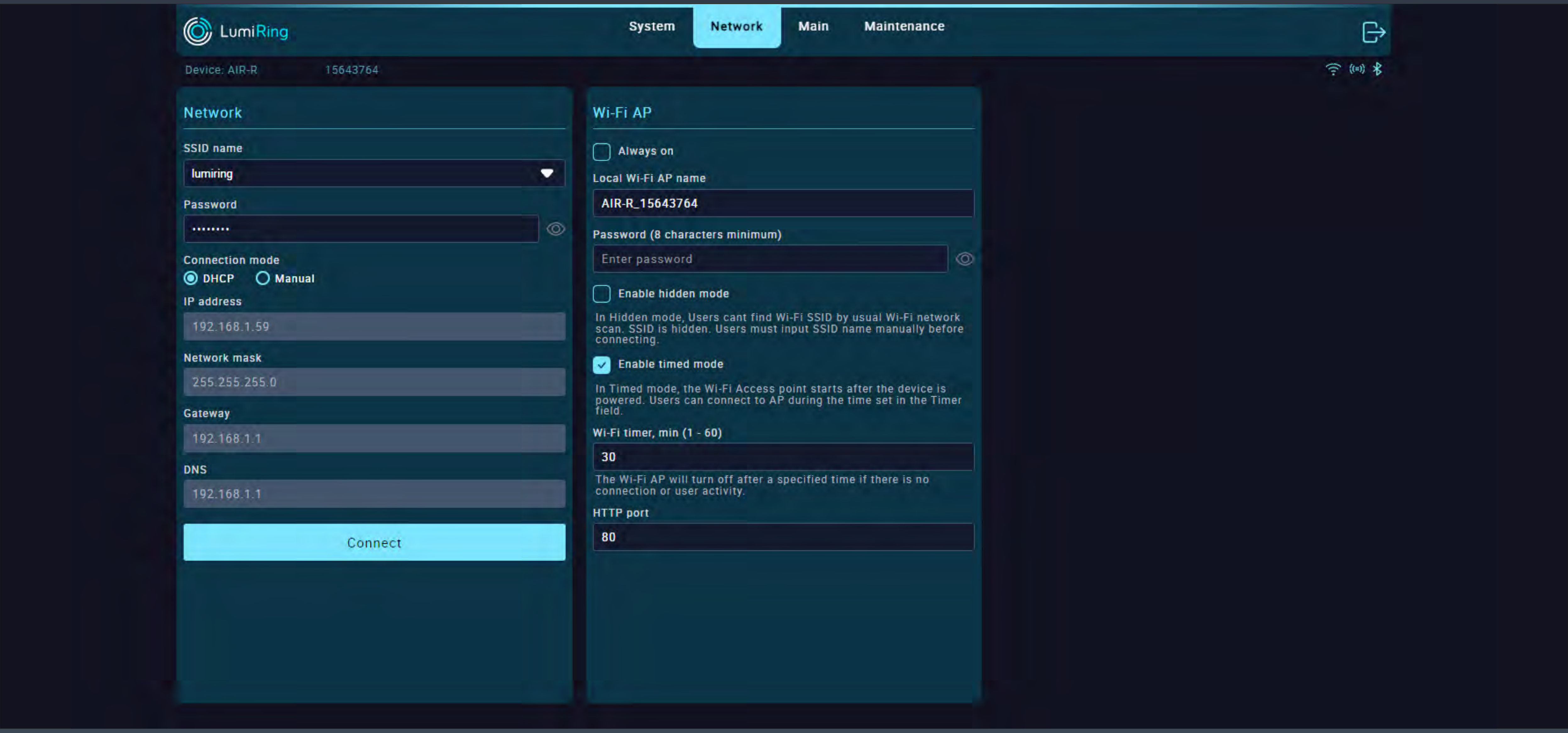
The Network Information subsection displays the:

- Device's current network settings.
- Device's IP address.
- Network mode - Manual or Dynamic Host Configuration Protocol (DHCP).
- Network mask.
- Domain Name Service (DNS).
- Network port of the device.
- Built-in Wi-Fi AP operation mode
- ("Always on" or use a "Timed").

In the Hardware Information 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.
- The application programming interface (API) version used by the device.

Network



Device: AIR-R 15643764

Network

SSID name: lumiring

Password: ••••••••

Connection mode: ● DHCP ○ Manual

IP address: 192.168.1.59

Network mask: 255.255.255.0

Gateway: 192.168.1.1

DNS: 192.168.1.1

Connect

Wi-Fi AP

□ Always on

Local Wi-Fi AP name: AIR-R_15643764

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.

☑ Enable timed mode

In Timed mode, the Wi-Fi Access point starts after the device is powered. Users can connect to AP during the time set in the Timer field.

Wi-Fi timer, min (1 - 60): 30

The Wi-Fi AP will turn off after a specified time if there is no connection or user activity.

HTTP port: 80

In the Network section, you can set up an Internet connection via Wi-Fi, you can change the connection settings for the built-in Wi-Fi AP, and you can set its activity time.

The Network subsection provides the following functions:

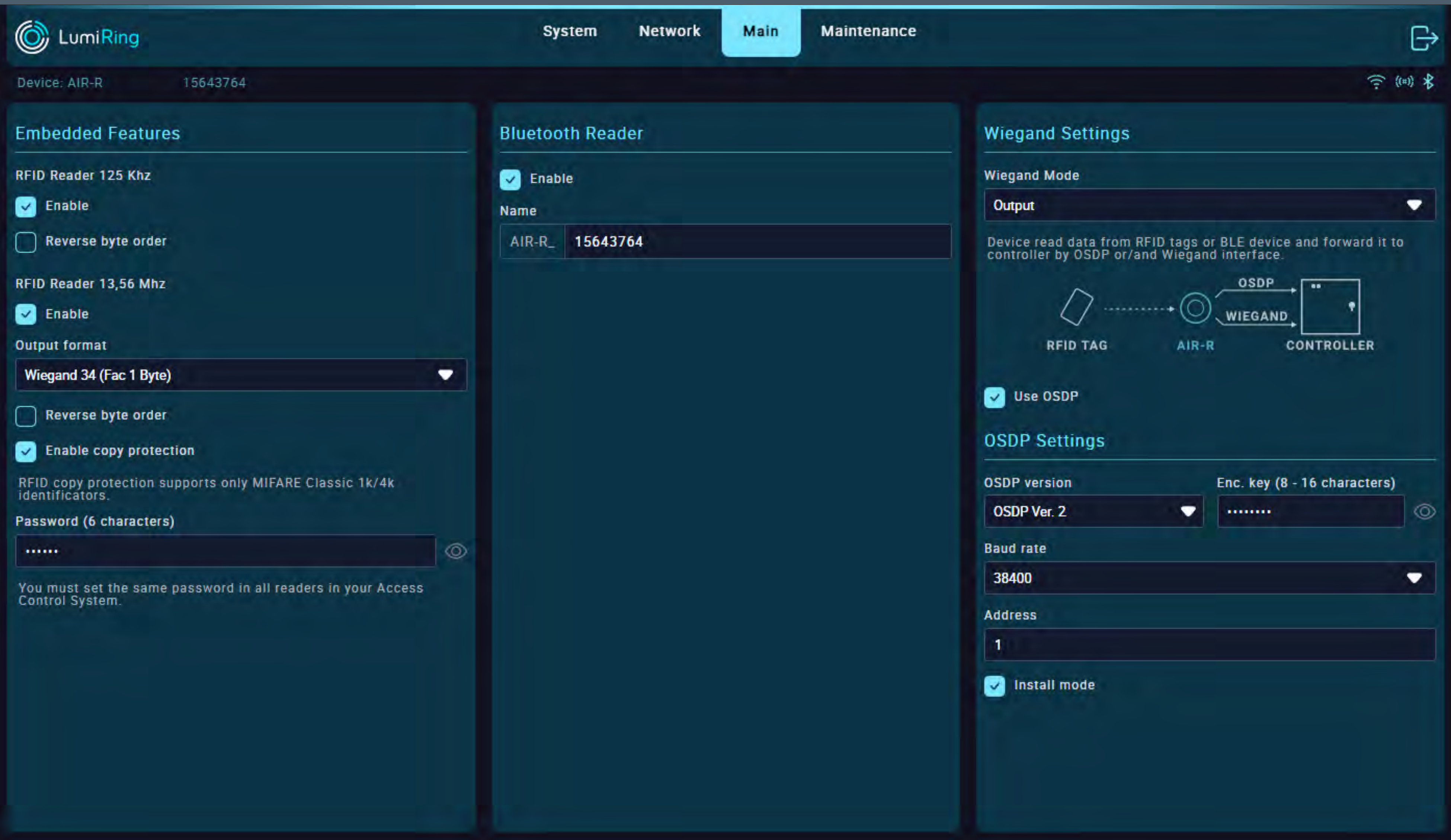
- Click on the “SSID name” field to search for available Wi-Fi networks and enter the password to connect.
- Select “DHCP” for automatic network settings or “Manual” to enter all network settings manually in the available fields below, then click “Connect”.

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.

Main

OSDP is coming soon!



Device: AIR-R 15643764

Embedded Features

RFID Reader 125 Khz

☑ Enable

□ Reverse byte order

RFID Reader 13,56 Mhz

☑ Enable

Output format: Wiegand 34 (Fac 1 Byte)

□ Reverse byte order

☑ Enable copy protection

RFID copy protection supports only MIFARE Classic 1k/4k identificators.

Password (6 characters): ••••••

You must set the same password in all readers in your Access Control System.

Bluetooth Reader

☑ Enable

Name: AIR-R_ 15643764

Wiegand Settings

Wiegand Mode: Output

Device read data from RFID tags or BLE device and forward it to controller by OSDP or/and Wiegand interface.

☑ Use OSDP

OSDP Settings

OSDP version: OSDP Ver. 2

Enc. key (8 - 16 characters): •••••••••

Baud rate: 38400

Address: 1

☑ Install mode

- Selecting RFID Readers makes the 125 kHz and 13.56 MHz built-in reader antenna modules active and configurable.
- 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.
- Uncheck the “Enable” checkbox in the RFID Reader 13.56 MHz settings section to disable the ability to read identifiers of this format.
- Select the desired Output Format from the list of supported Wiegand formats.

Note: The choice of Output Format is determined according to the format used in the access control system and based on the type of identifiers. 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 “Reverse byte order” checkbox to change the code reading order for 13.56 MHz identifiers.
- Check the “Enable copy protection” checkbox to use the 13.56 MHz format ID verification mode for authenticity.
- Enter the ID encryption password.

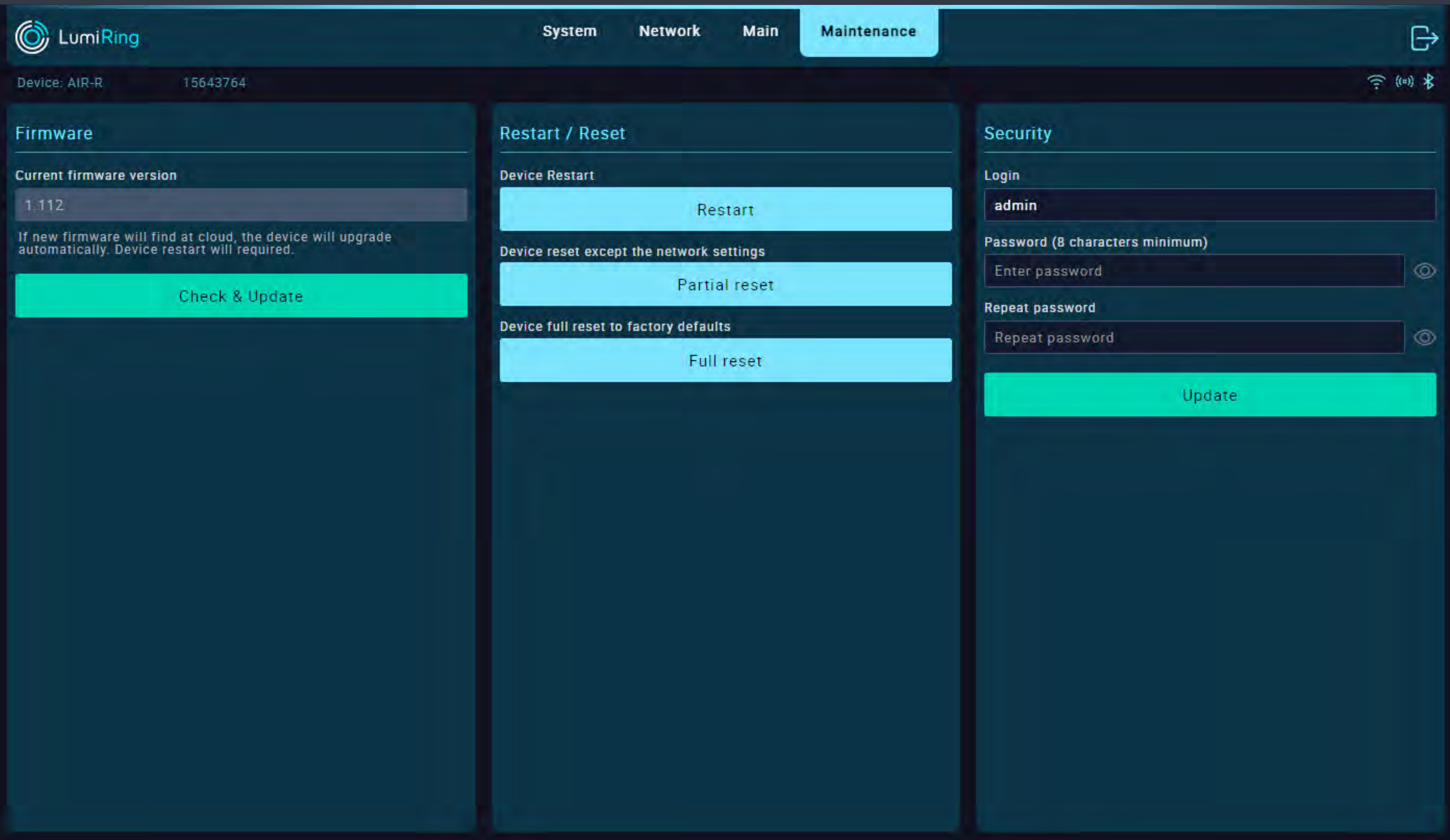
Note: The Copy Protection feature uses a unique password encryption method to encrypt private identifier memory areas. If the encryption password of the identifier and the reader match, then the reader will recognize the identifier. If there is no password or it is different, the identifier is ignored. Thus, all identifiers other than encrypted ones will be ignored. Copying an encrypted identifier means that only part of its code from open areas can be copied. At the same time, closed areas are difficult or impossible to copy.

- 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.

The Wiegand Settings section and OSDP functionality are under development and will be available soon. Keep an eye on the updates.

Maintenance



Device: AIR-R 15643764

Current firmware version: 1.112

If new firmware will find at cloud, the device will upgrade automatically. Device restart will required.

Device Restart

Device reset except the network settings

Device full reset to factory defaults

Login: admin

Password (8 characters minimum): Enter password

Repeat password: Repeat password

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.
- 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:

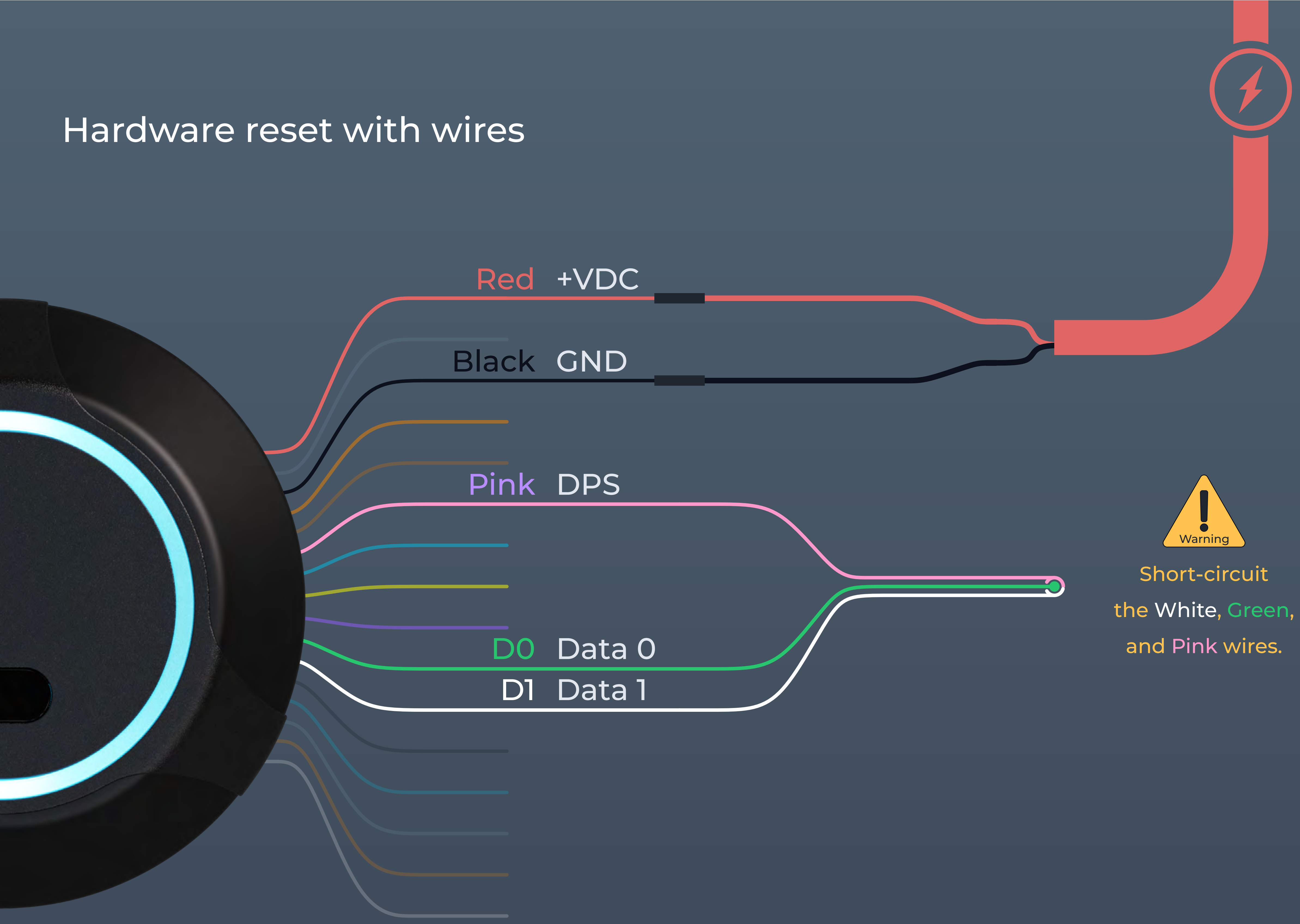
- Restart - restarts the device.
- Partial reset - resets all device settings except for network connection settings.
- Full reset - resets all settings of the device to factory defaults.

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



Short-circuit the White, Green, and Pink 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.

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.

Glossary

- +VDC - Positive Voltage Direct Current.
- API - application programming interface.
- BLE - Bluetooth Low Energy.
- Bluetooth - A short-range wireless communication technology that enables wireless data exchange between digital devices.
- 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. A distributed system that translates domain names into IP addresses to help identify computers on a network.
- 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.
- Encryption password - Key for data protection.
- Exit/Entry/Open button - Logic input which, when activated, activates the corresponding output. Causes an event depending on the attribute used.
- 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.
- Magnetic Lock - A locking mechanism that uses electromagnetic force to secure doors, gates, or access points.
- 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.

Glossary

- OTA update - Over-the-air update. The process of remotely and wirelessly updating software or firmware on a device.
- Power supply - A device or system that provides electrical energy to other devices, enabling them to operate and function.
- 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.
- 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.
- 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.

For Notes