



lumiring AIR-R Multifunctional Access Control Reader Owner's Manual

[Home](#) » [LUMIRING](#) » lumiring AIR-R Multifunctional Access Control Reader Owner's Manual 

lumiring AIR-R Multifunctional Access Control Reader Owner's Manual



Contents

- [1 Introduction](#)
- [2 FCC Statement](#)
- [3 Device Specifications](#)
- [4 Default Device Settings](#)
- [5 Device Dimensions](#)
- [6 Wire Designation](#)
- [7 Installation Recommendations](#)
- [8 Wiegand Interface](#)
 - [8.1 Connection Diagram](#)
 - [8.2 Coming Soon!](#)
 - [8.3 OSDP Interface Connection Diagram](#)
 - [8.4 Login](#)
 - [8.5 Connecting to Device](#)
 - [8.6 System](#)
 - [8.7 Network](#)
 - [8.8 Main](#)
 - [8.9 Embedded features](#)
 - [8.10 Maintenance](#)
 - [8.11 Hardware Reset](#)
 - [8.12 Indication](#)
 - [8.13 Glossary](#)
- [9 Documents / Resources](#)
 - [9.1 References](#)
- [10 Related Posts](#)

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.

FCC Statement

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

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

- Consult the dealer or an experienced radio/TV technician for help

This device complies with part 15 of the FCC rules. Operation is subject to the following two conditions (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.

This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Device Specifications

Voltage:

- 12 or 24 VDC operation
- 0.13A @12 VDC, 0.065A @ 24 VDC current consumption

Outputs*:

- One output (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
- Bluetooth® 5 (LE)
- Wiegand 26, 34, 48, 56 bit
- OSDP via RS-485

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

Dimensions (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-R_(serial_number)

Access point (AP) Wi-Fi IP address of the device:

- 192.168.4.1

Wi-Fi password:

- None (factory default)

Web page login:

- admin

Web page password:

- admin123

RFID 125 kHz:

- Enabled

RFID 13.56 MHz:

- Enabled

Copy protection:

- Disabled

Bluetooth:

- Enabled

AP Wi-Fi timer:

- 30 minutes

Wiegand format 125 kHz:

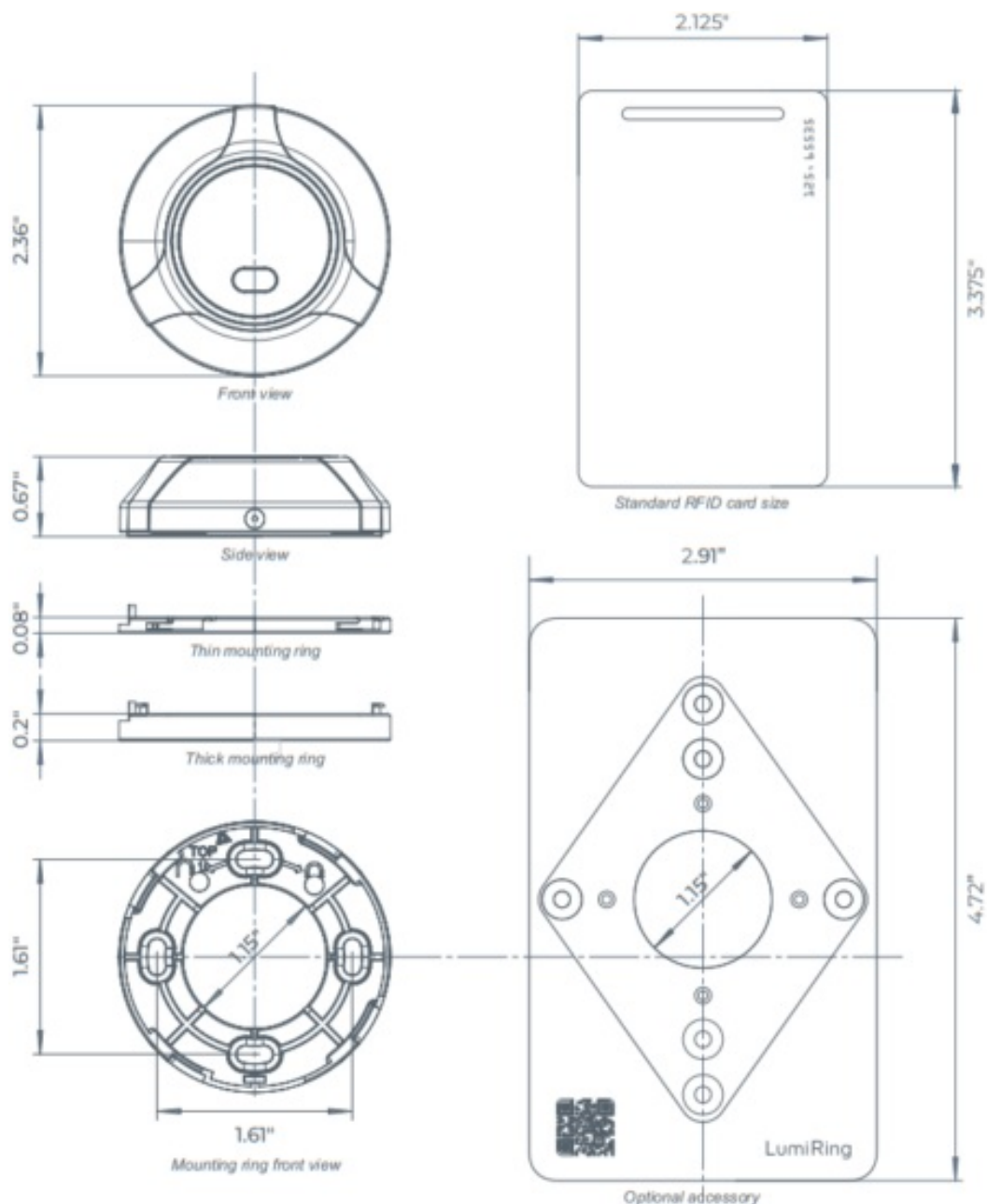
- 26 bit

Wiegand format 13.56 MHz:

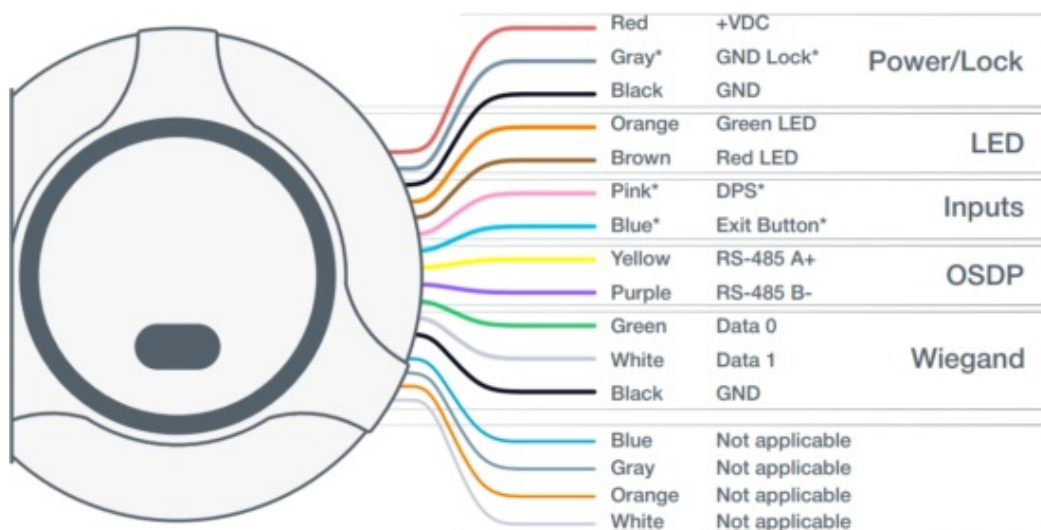
- 34 bit

* When using OSDP with ICON and ICON-Pro Controllers. **Coming soon!**

Device Dimensions



Wire Designation



- * Available when using OSDP when connected to the Controller as an expansion device.

Installation Recommendations

Placement and Wiring

- The reader is designed for outdoor and indoor installation.
- When placing the reader, it is necessary to avoid installation on metal surfaces, as it can reduce the distance of access card reading, as well as the operation of the built-in Bluetooth and Wi-Fi module.

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 Cat5e cable. The line must be at least 1.64 feet (0.5 m) away from power cables.
- Keep the reader power line wires as short as possible to avoid a significant voltage drop across them. After laying the cables, ensure the power supply voltage to the reader is at least 12 VDC when the locks are on.

Connecting 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.

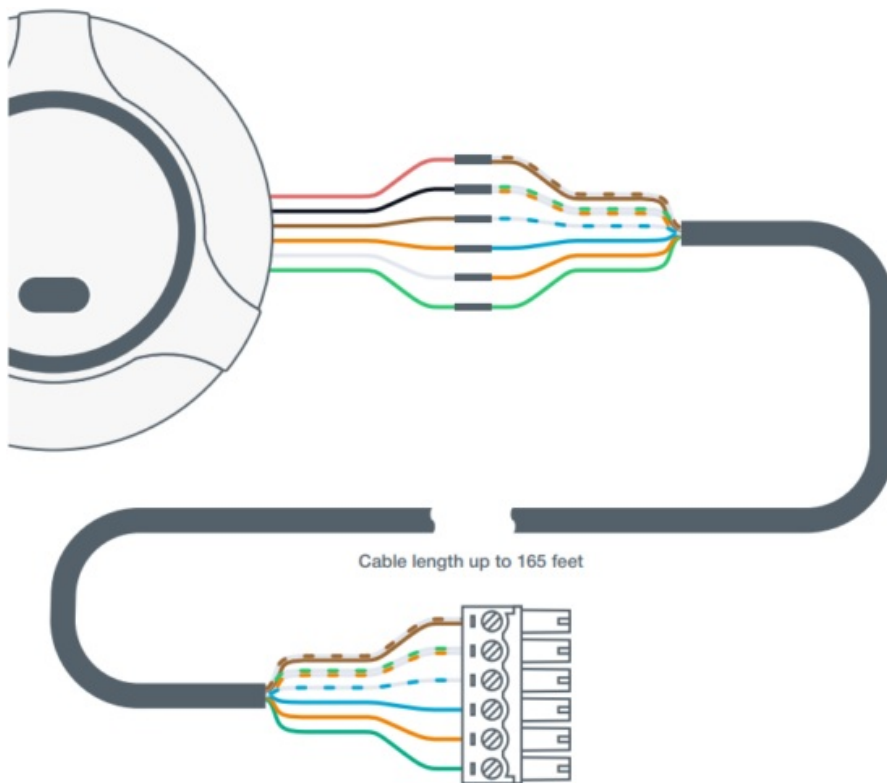
Protection Against High Current Surges

- A protective diode protects the devices from reverse currents when triggering an electromagnetic or electromagnetically 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.

Wiegand Interface

Connection Diagram



Red: White Brown/Brown
Black: White-green/White-orange
Brown: White-Blue
Orange: Blue
White: Green
Green: Orange
White Brown/Brown: +VDC
White-green/White-orange: GND
White-Blue: Red Led
Blue: Green Led
Green: Data 1
Orange: Data 0

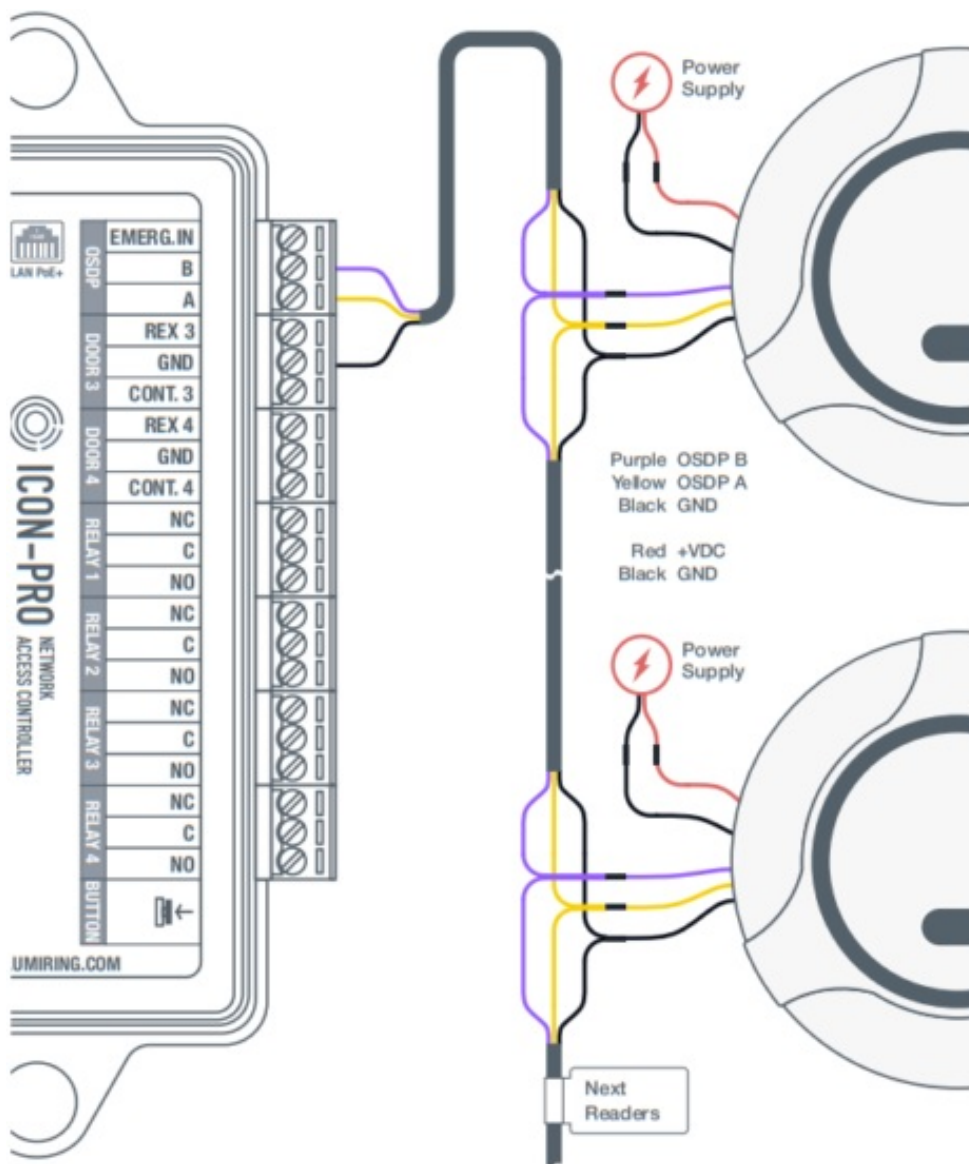
Example of connection to the terminal blocks of ICON and ICON-Pro Ccontrollers.

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.
- The recommended voltage should be at least +10 VDC.
- Use a multi meter in the VDC measurement mode to verify that the power supply voltage meets the recommended requirements.

Coming Soon!

OSDP Interface Connection Diagram



OSDP Interface Connection Diagram



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!



All branches from the primary data cable should be kept as short as possible.
The length of taps from the primary data cable should be at most 8 inches.



Always route the main data cable away from power cables and sources of electrostatic interference.

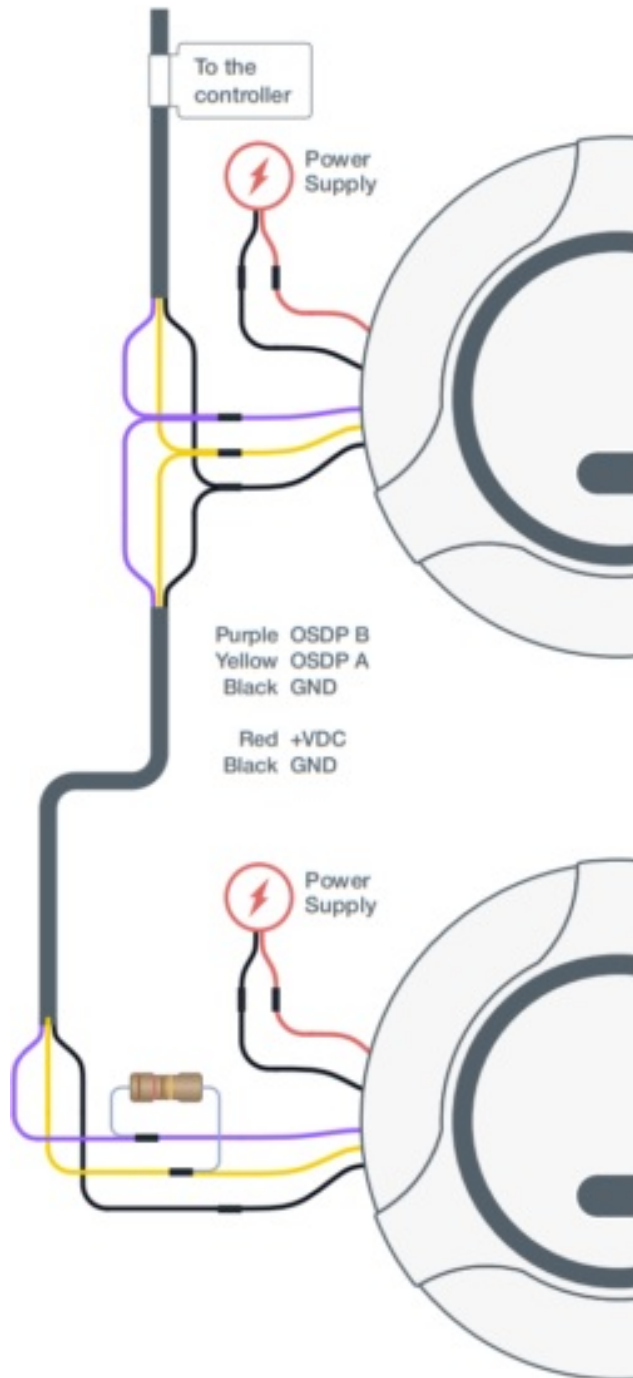


Terminal resistors ensure that the “open” end of the cable is matched to the rest of the line, eliminating signal reflection.

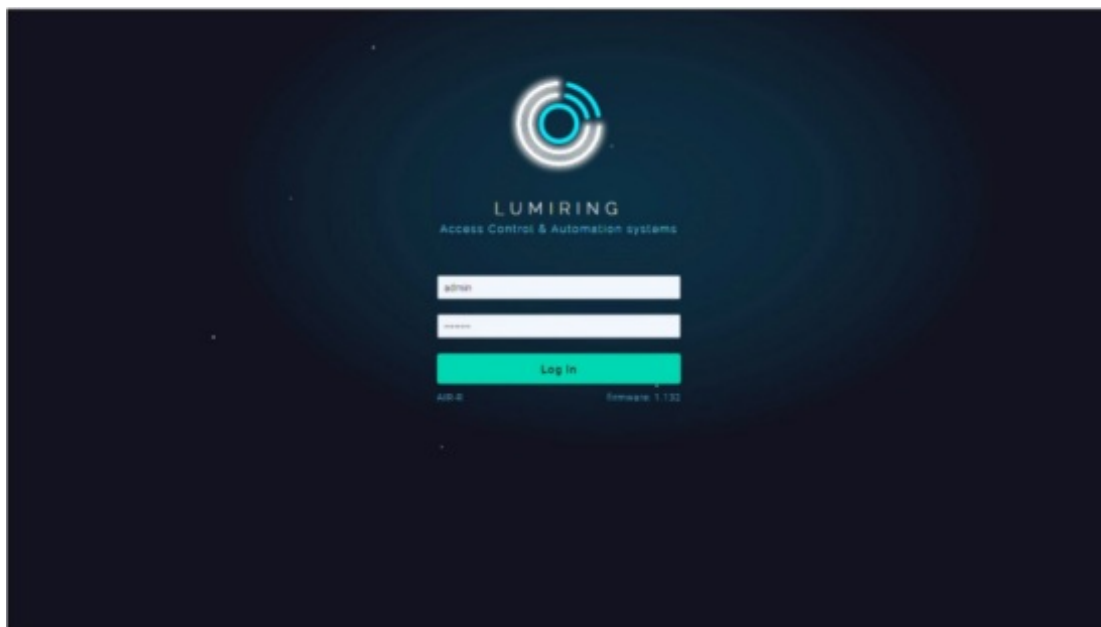
The nominal resistance of the resistors corresponds to the wave impedance of the cable, and for twisted pair cables is typically 100 to 120 ohms.

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.



Login



Connecting to Device

Connecting to the built-in Wi-Fi access point (AP).

Step 1. Connect the device to a power source.

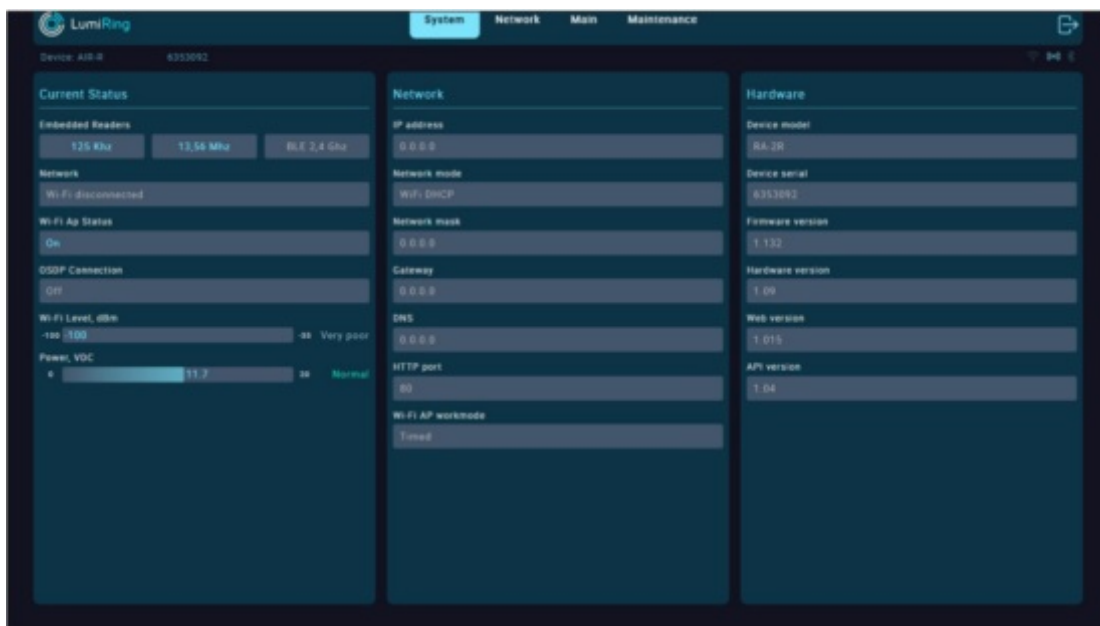
Step 2. Search for Wi-Fi and connect to the AIR-R_xxxxxxxx network.

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.”

The browser will automatically redirect you to the System page.

System



This System 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.

- Status of the device connection to the router in use.
- Status of the built-in Wi-Fi access point.
- OSDP connection status.
- Level and quality of the device's connection to the Wi-Fi router.
- Power supply voltage value.

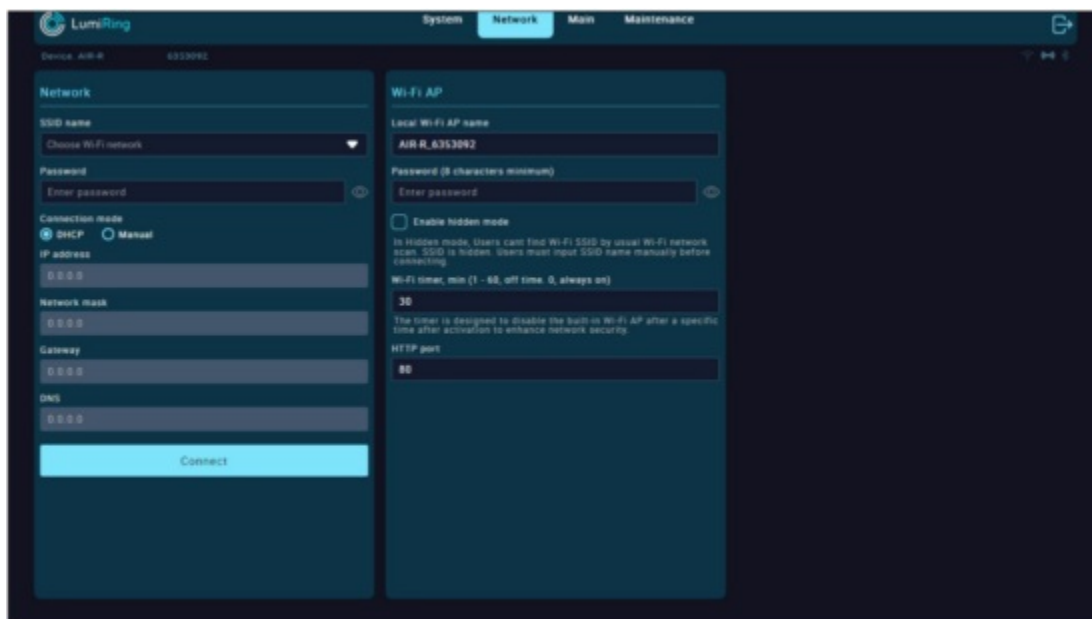
The Network Information subsection displays the:

- Device's IP address.
- Network mode – Manual or Dynamic Host Configuration Protocol (DHCP)
- Network mask.
- Gateway
- Domain Name Service (DNS).
- Network port of the device.
- Built-in Wi-Fi AP operation mode (“Always on” or “Timed”).

In the Hardware Information subsection, you can see the:

- Device model name.
- Device serial number.
- Current firmware version.
- Current hardware version of the device.
- Web version used by the device.
- The 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.

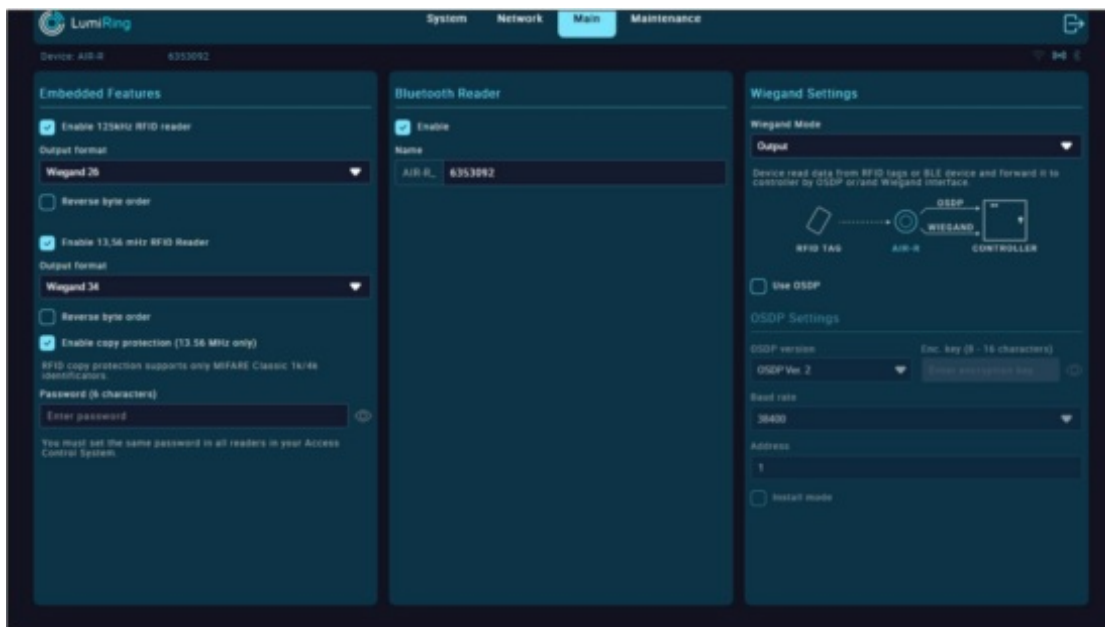
The Network subsection provides the following functions:

- 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:

- 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.

Main



Embedded features

- Selecting RFID Readers makes the 125 kHz and 13.56 MHz built-in reader antenna modules active and configurable.
- Unchecked 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.
- Unchecked 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.

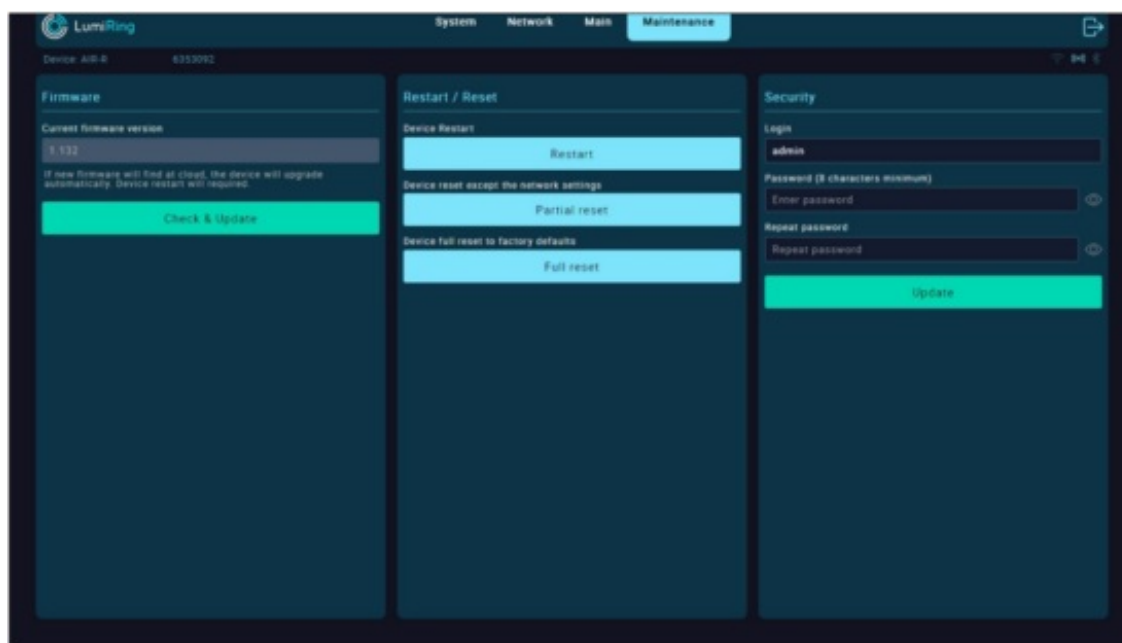
Note: The Copy Protection feature uses a unique password encryption method to encrypt private identifier memory areas. If the encryption password of the identifier and the reader match, then the reader will recognise the identifier. If there is no password or it is different, the identifier is ignored. 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.

Bluetooth reader

- Check the “Enable” checkbox in the Bluetooth Reader section 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.

The Wiegand Settings subsection and OSDP functionality are under development and will be available soon. Keep an eye out 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 into the web interface. The unit will automatically download the latest previously used firmware version and resume operation.

The Restart/Reset subsection performs the following actions:

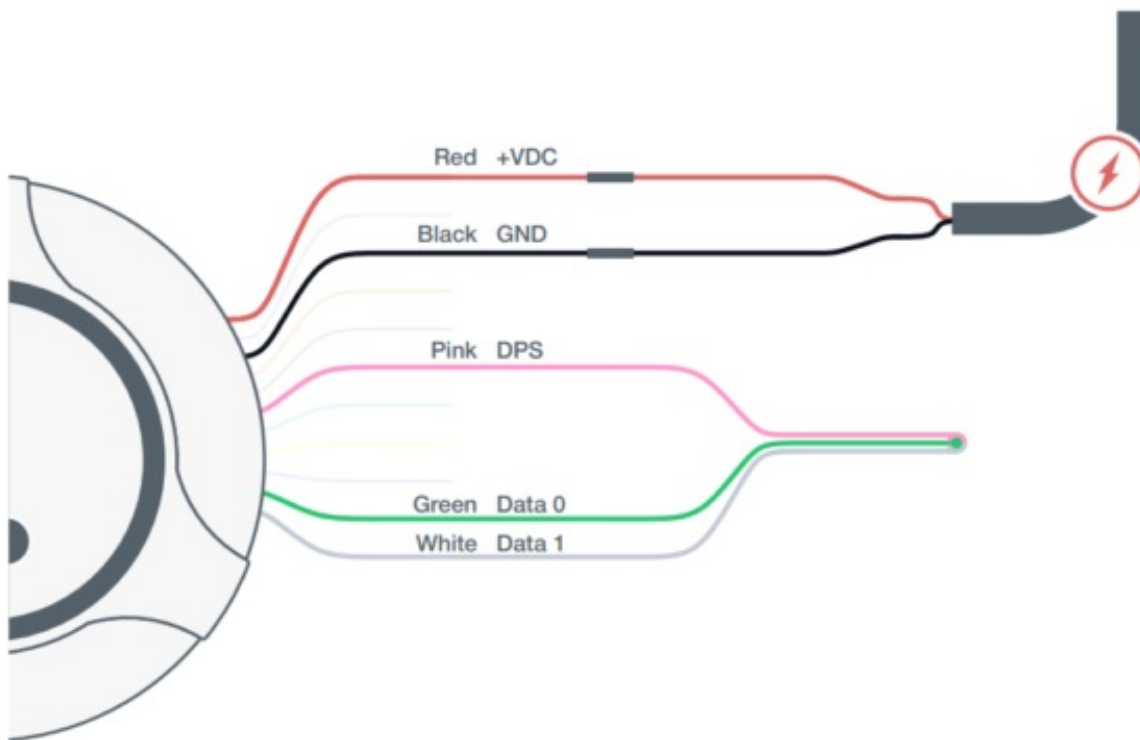
- Restart – restarts the device.
- Full reset – resets all settings of the device to factory defaults.

The Security subsection is used to change the password for logging into the interface of the device:

- Enter the new login password and confirm it.
- Apply the changes by clicking “Update.”

The new password can be used the next time you log into the device interface.

Hardware Reset




Short-circuit the white, green, and pink wires.

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.

-  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 readers, control of executive devices, display and logging of information.
- **API** – application programming interface.
- **BLE** – Bluetooth Low Energy.
- **Block in** – Function for the input activating "block out" with the event "blocked by operator." It is used for turnstile control.
- **Block out** – Output activated when "block In" is triggered.
- **Bluetooth** – A short-range wireless communication technology that enables wireless data exchange between digital devices.
- **BUZZ** – Output for connecting the reader wire responsible for sound or light indication.
- **Cloud** – A cloud-based platform or service provided to manage and monitor an access control system over the Internet. Allows administrators to manage access rights, monitor events, and update system settings using a web-based interface, providing the convenience and flexibility to manage the access control system from anywhere there is an Internet connection.
- **Copy protection** – A method used to prevent unauthorized copying or duplication of smart cards to secure the access control system and prevent possible security breaches.
- **D0** – "Data 0." A bit line with the logical value "0."
- **D1** – "Data 1." A bit line with the logical value "1."


- **DHCP** – Dynamic Host Configuration Protocol. A network protocol that allows network devices to automatically obtain an IP address and other parameters necessary for operation in a Transmission
- Control Protocol/Internet Protocol TCP/IP network. This protocol works on a “client-server” model.
- **DNS** – Domain Name System is a computer-based distributed system for obtaining domain information. It is most often used to obtain an IP address by host name (computer or device), to obtain routing information, and to obtain serving nodes for protocols in a domain.
- **DPS** – Door position sensor. A device that is used to monitor and determine the current status of a door, such as whether the door is open or closed.
- **Electric latch** – An electronically controlled door locking mechanism.
- **Emergency in** – Input for emergency situations.
- **Encryption password** – Key for data protection.
- **Ethernet network** – A wired computer network technology that uses cables to connect devices for data transmission and communication.
- **Exit/Entry/Open button** – Logic input which, when activated, activates the corresponding output. Causes an event depending on the attribute used.
- **Exit/Entry/Open out** – Logical output that is activated when the corresponding input is triggered. Causes an event depending on the attribute used.
- **External relay** – Relay with potential-free dry contact for remote control of the power supply. The relay is equipped with a dry contact, which is galvanic ally 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.
- **LED** – Light emitting diode.
- **Loop sensor** – A device that detects the presence or passage of traffic in a certain area by means of a closed electrical loop. Used in barriers or gates.
- **Magnetic Lock** – A locking mechanism that uses electromagnetic force to secure doors, gates, or access points.
- **MQTT** – Message Queuing Telemetry Transport. A server system that coordinates messages between different clients. The broker is responsible, among other things, for receiving and filtering messages, identifying the clients subscribed to each message, and sending messages to them.
- **NC** – Normally closed. Configuration of a changeover contact that is closed in the default state and open when activated.
- **NO** – Normally open. A switch contact configuration that is open in its default state and closes when activated.
- **No-touch button** – A button or switch that can be activated without physical contact, often using proximity or motion-sensing technology.
- **Open collector** – A transistor switch configuration in which the collector is left unconnected or open, typically used for signal grounding.

- **OSDP** – Open Supervised Device Protocol. A secure communication protocol used in access control systems for device-to-device data exchange.
- **Pass control** – The process of regulating, monitoring, or granting permission for individuals to enter or exit a secure area.
- **Power supply** – A device or system that provides electrical energy to other devices, enabling them to operate and function.
- **Radio 868/915 MHZ** – A wireless communication system operating on the 868 MHz or 915 MHz frequency bands.
- **Reader** – A device that scans and interprets data from RFID or smart cards, often used for access control or identification.
- **Revers byte order** – A process of reordering the sequence of bytes in a data stream, often for compatibility or data conversion.
- **REX** – Request to exit. An access control device or button used to request to exit from a secured area.
- **RFID** – Radio-frequency identification. A technology for wireless data transmission and identification using electromagnetic tags and readers.
- **RS-485** – A standard for serial communication used in industrial and commercial applications, supporting multiple devices over a shared network.
- **Strike lock** – An electronic locking mechanism that releases a door's latch or bolt when electrically activated, often used in access control systems.
- **Terminal block** – A modular connector used for connecting and securing wires or cables in electrical and electronic systems.
- **Topic** – In the context of MQTT, a label or identifier for published messages, enabling subscribers to filter and receive specific information.
- **Unblock in** – An input or signal used to release a lock, barrier, or security device, allowing access to a previously secured area.
- **Unblock out** – An output or signal used to release a lock, barrier, or security device to allow exit or opening.
- **Wiegand format** – A data format used in access control systems, typically for transmitting data from card readers to controllers.
- **Wiegand interface** – A standard interface used in access control systems to communicate data between card readers and access control panels.
- **Wi-Fi AP** – Wireless access point. A device that allows wireless devices to connect to a network.
- **Wireless access control gateway** – A device that manages and connects wireless access control devices to a central system or network.

For Notes



Documents / Resources

	<p>lumiring AIR-R Multifunctional Access Control Reader [pdf] Owner's Manual V 3.5, AIR-R Multifunctional Access Control Reader, AIR-R, Multifunctional Access Control Reader, Access Control Reader, Control Reader, Reader</p>
--	--

References

- [🌐 EMERG.IN](#)
- [User Manual](#)

[Manuals+](#), [Privacy Policy](#)

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.