



# ICON-PRO



## MANUAL

# CONTENTS

Introduction	3
Default Device Settings	3
Device Specifications	4
Device Dimensions	5
Device Connection Terminals	6
Installation Recommendations	7
Wiegand Reader (Connection Diagram)	9
Open Supervised Device Protocol Reader (Connection Diagram) <i>Coming soon!</i>	11
Exit Button & Door Position Sensor (Connection Diagram)	13
Electric Lock [Power Supply +12 VDC] (Connection Diagram)	14
Electric Lock [Power Over Ethernet] (Connection Diagram)	15
Third-Party Device [Relay +12 VDC] (Connection Diagram)	16
Connecting to Device	17
Login	17
Quick Start	18
System	19
Network	20
Open Supervised Device Protocol (OSDP) <i>OSDP is coming soon!</i>	22
Maintenance	23
Hardware reset with the button	24
Glossary	25
For Notes	28

## Introduction

This document provides detailed information on the ICON-Pro 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                              | ICON_(serial number)         |
| • Device access point (AP) Wi-Fi Internet protocol (IP) address | 192.168.4.1<br>192.168.1.100 |
| • Default Ethernet IP address of the device                     | None                         |
| • Wi-Fi password  | admin                        |
| • Login   | admin                        |
| • Password  | 30 minutes                   |
| • AP Wi-Fi timer  |                              |

# Device Specifications

## Device info

• Model	ICON-Pro
• Processor	ESP32-S3
• Over-the air (OTA) update	Yes
• Built-in web server	Yes
• Message Queuing Telemetry Transport (MQTT) application programming interface (API) provided	Yes
• Users	100 000
• Events	250 000

## Communications

• Wi-Fi	802.11 b/g/n 2.4 GHz
• Ethernet	RJ-45 (10/100 Mbit)
• Wiegand Readers ports	2
• Open Supervised Device Protocol (OSDP) via RS-485 port	1
• USB ports (Type-C)	Yes

## Physical connections

• Inputs	8
• Outputs	4 Relay
• Emergency In	1
• Tamper G-sensor	Built-in

## Electrical characteristics

• Input voltage	12-24 VDC +/- 10 %
	PoE IEEE802.3/802.3af: 2 A (24 W)
• Operation current (MAX) 12 VDC	0.5 A (6 W)
• Operation current (AVG) 12 VDC	0.21 A (2.52 W)
• Relay contact rating 30 VDC	1.5 A (45 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)
• Ethernet RJ-45 (10/100 Mbit)	328 ft (100 m)

## Environmental requirements

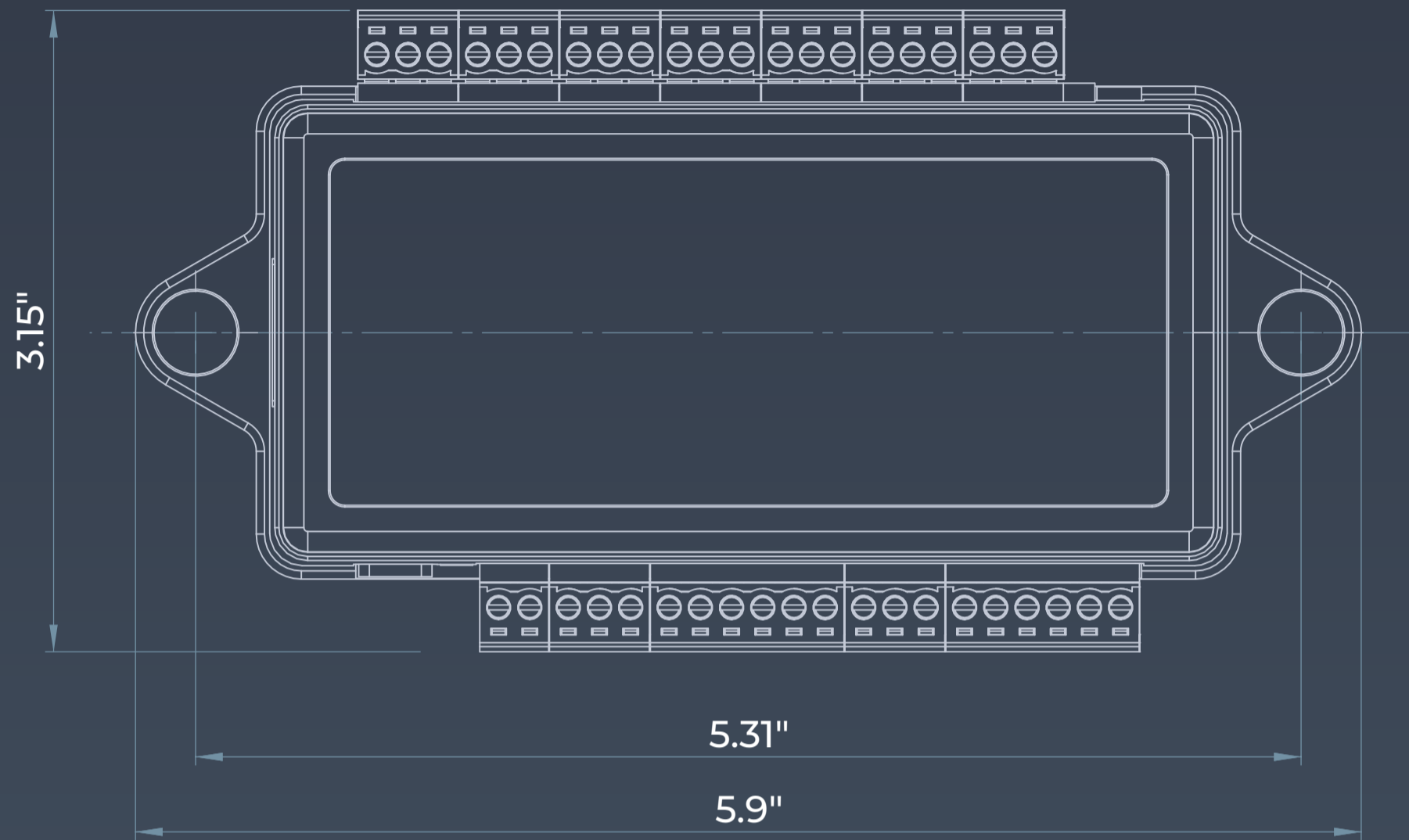
• Operating temperature	-22°F ~ 158°F (-30°C ~ 70°C)
• Ingress Protection rating	IP50

## Physical characteristics

• Housing material	ABS plastic UL94 V-0
• Mounting method	Wall mount/Din rail mount (option)
• Dimensions (length, width, height)	5.9" x 3.15" x 1.38" (150 x 80 x 35 mm)
• Weight	6.75 oz (191 g)

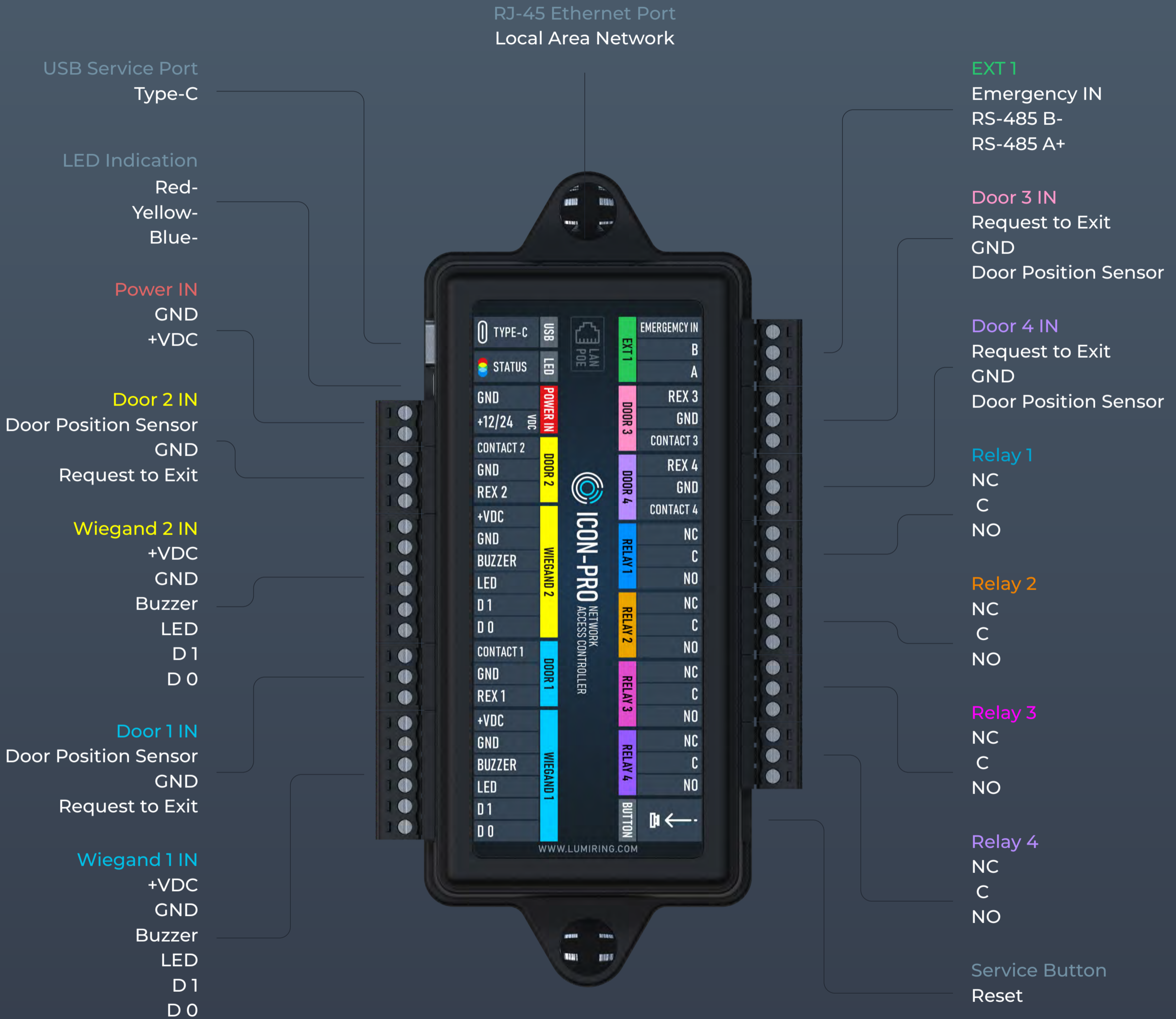
\* See general specifications for RS4-85 interface.

# Device Dimensions





# Device Connection Terminals



The manufacturer reserves the right to modify the external pin assignments and their placement, as well as the appearance of the device without prior notice. These changes may be made to improve functionality or ergonomics, or to comply with technical requirements and standards. Users are advised to consult the latest versions of technical documentation and instructions before using the device.

## Installation Recommendations

### Placement and Wiring

Place controllers as close as possible to Wi-Fi APs to minimize latency. Check the Wi-Fi signal strength after installation, and make sure the minimum allowable signal level is -75 dB. If the signal strength is lower, move the AP closer to the device, or use a stronger antenna on the AP or device. Avoid placing the device on metal surfaces, as this may reduce the quality of the Wi-Fi connections.

### Connecting Power to the Device

Make all connections only when the power is off.

Use a power cable with a suitable cross-section to supply the current consumption of the connected devices. Make sure to use two separate power supplies for the controller and the actuators.

### Wiegand Connection

Use the same Wiegand format and byte order to connect the readers to avoid differences in card code reading and subsequent confusion in the system.

The Wiegand communication line length should not exceed 328 ft (100 m). If the communication line is longer than 16.4 ft (5 m), use a UTP Cat 5E cable. The line should be less than 1.64 ft (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, make sure that the power supply voltage to the reader is at least 12 V when the locks are on.

### 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 one-twisted pair, shielded cable, 120 $\Omega$  impedance, 24 AWG should be used as the OSDP communication line (if possible, ground the shield at one end).

## Installation Recommendations

### Connecting Electric Locks

Connect devices via relays if galvanic isolation from the device to be controlled 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 is used to protect the controller from reverse currents when an electromagnetic or electromechanical lock is triggered. A protective diode or varistor is installed near the lock in parallel with the contacts. THE DIODE IS CONNECTED IN REVERSE POLARITY.

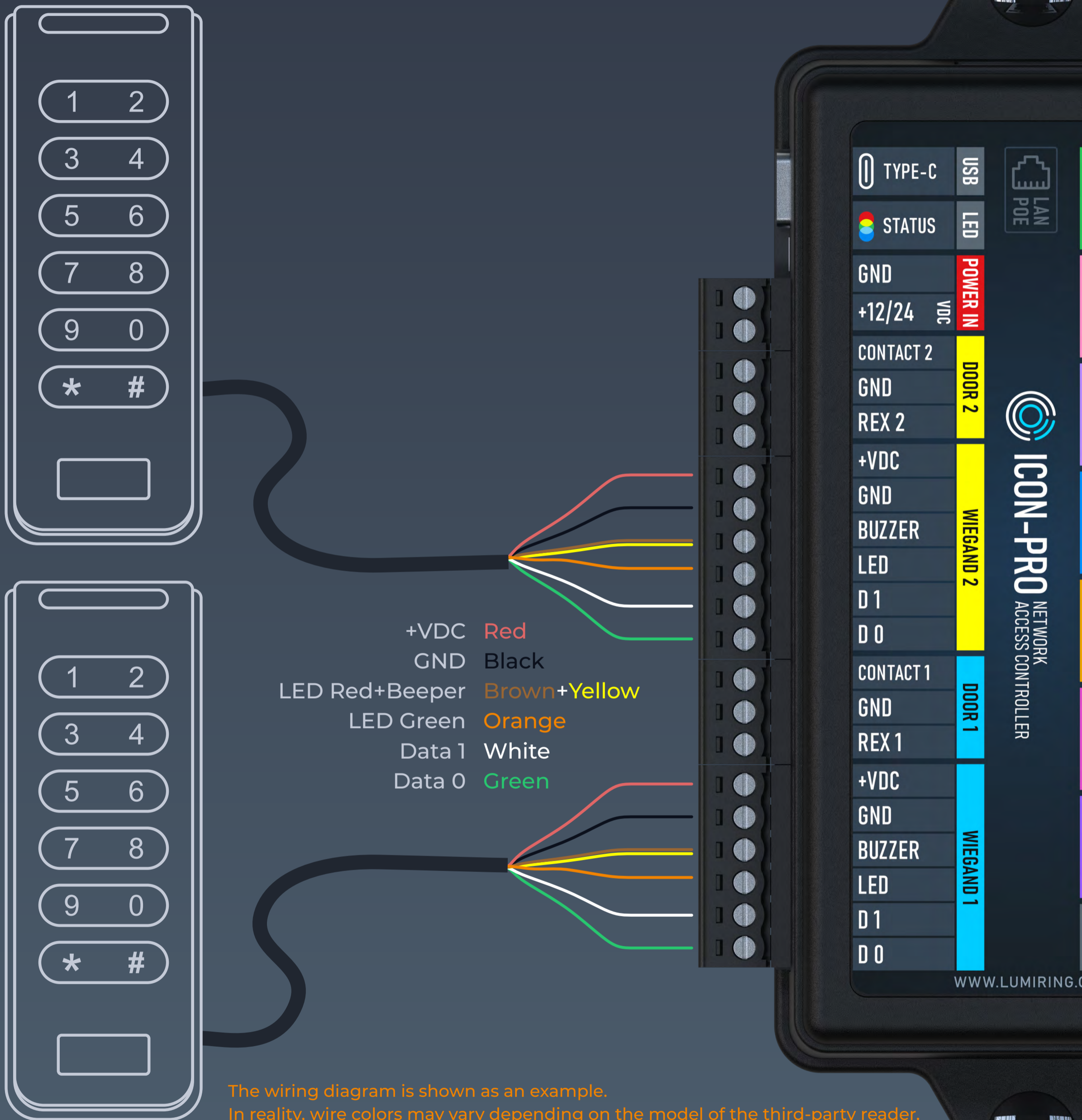
Suitable diodes include SR5100, SF18, SF56, HER307, and similar. Instead of diodes, varistors 5D330K, 7D330K, 10D470K, and 10D390K can be used, for which there is no need to observe polarity.



# Wiegand Reader

## Connection Diagram

HID Signo Keypad Reader 20K



The wiring diagram is shown as an example. In reality, wire colors may vary depending on the model of the third-party reader. Please refer to the reader manufacturer's instructions.



Before you start building cable networks for Wiegand readers, read the interface specifications.



# Wiegand Reader

## Connection Diagram

### Lumiring AIR-R Reader

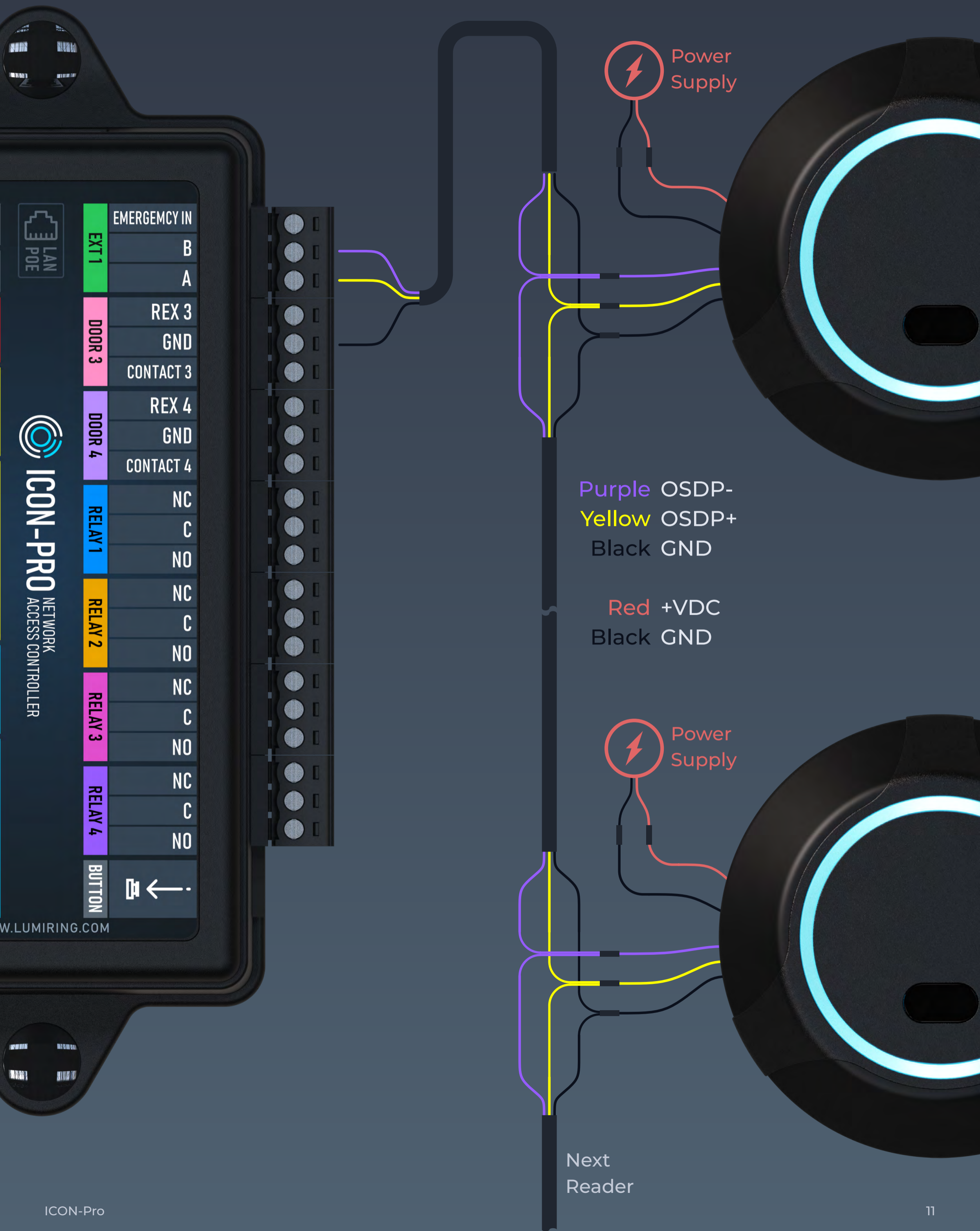


Before you start building cable networks for Wiegand readers, read the interface specifications.



# Open Supervised Device Protocol Reader Coming soon!

## Connection Diagram





# Open Supervised Device Protocol Reader Coming soon!

## 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!

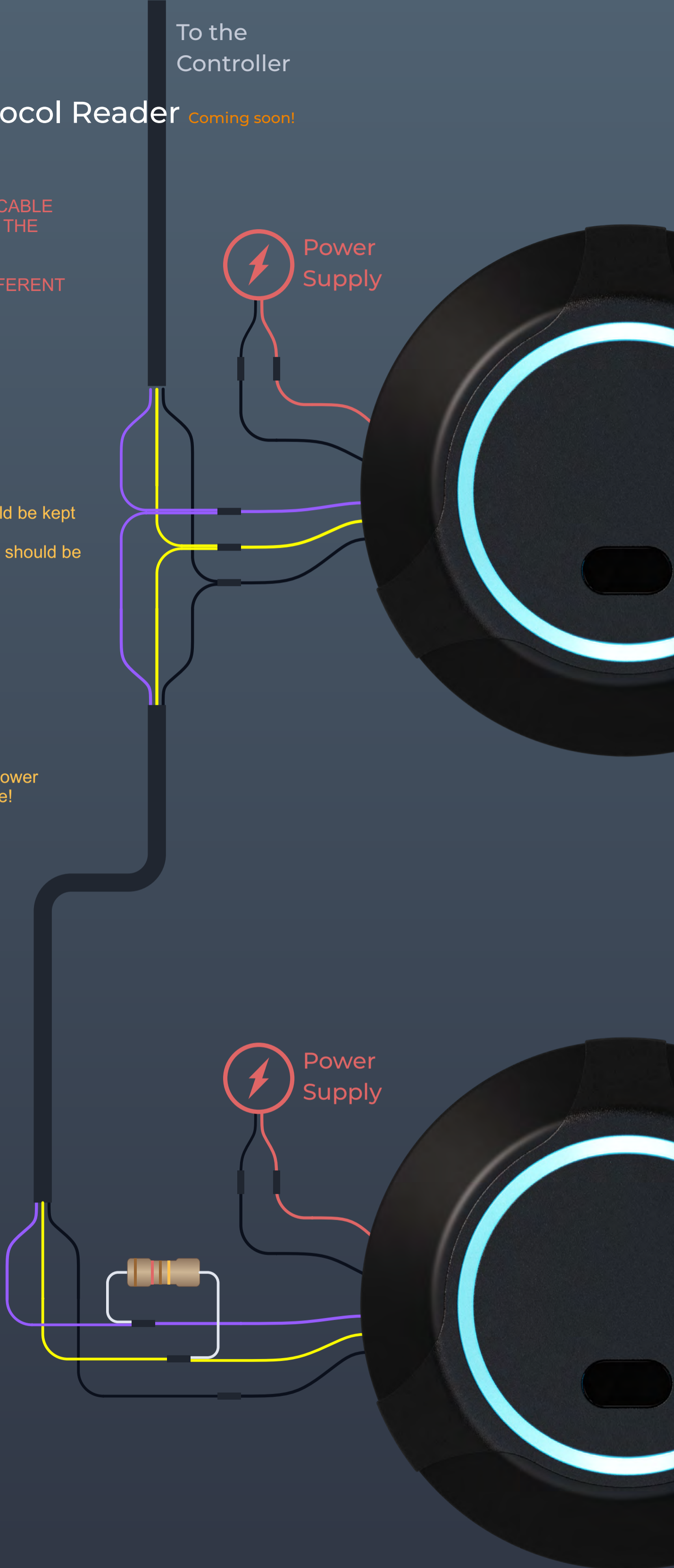


Terminal resistors ensure that the "open" end of the cable is matched to the rest of the line, eliminating signal reflection.

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.

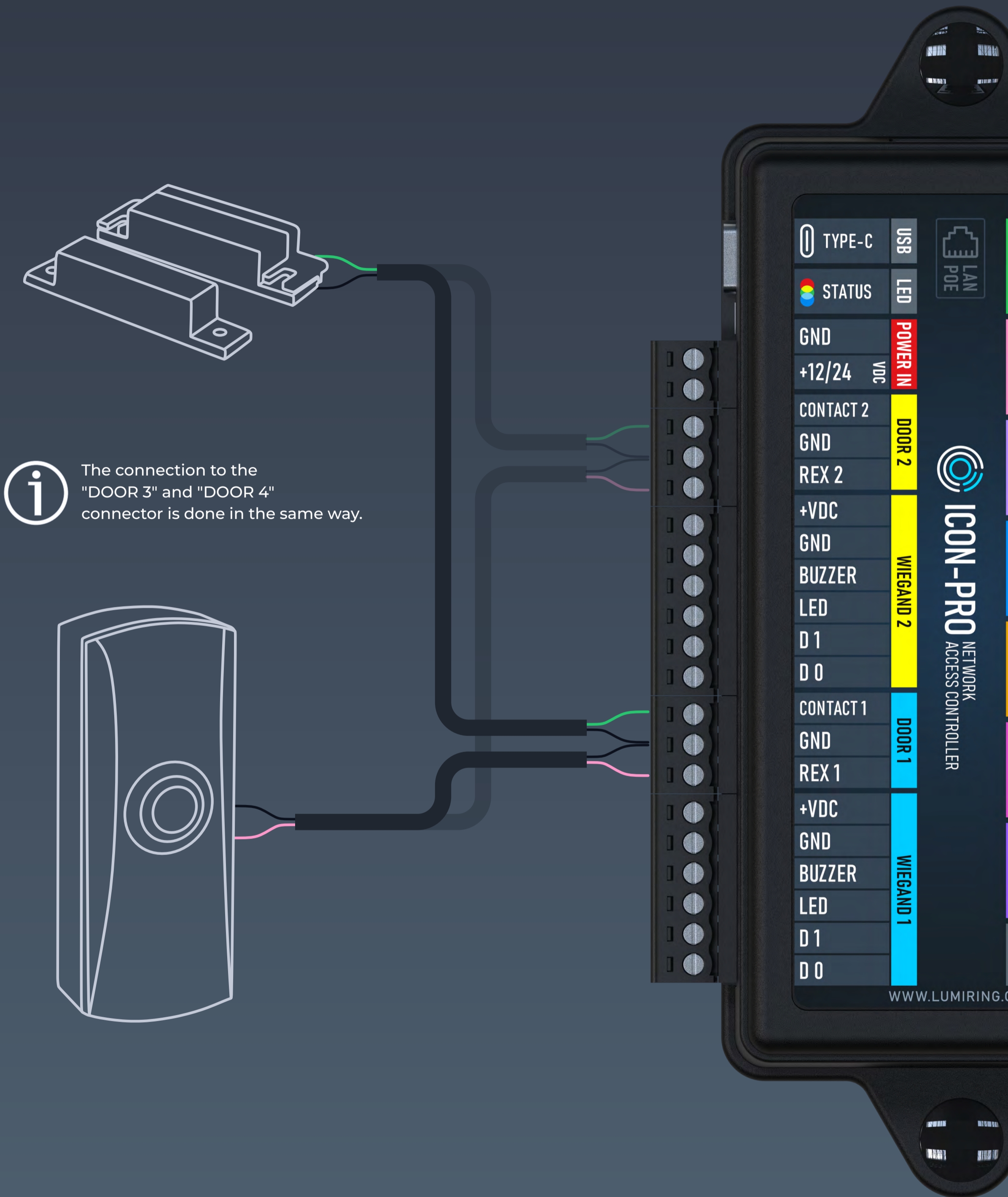
See RS-485 interface specifications for more information.





# Exit Button & Door Position Sensor

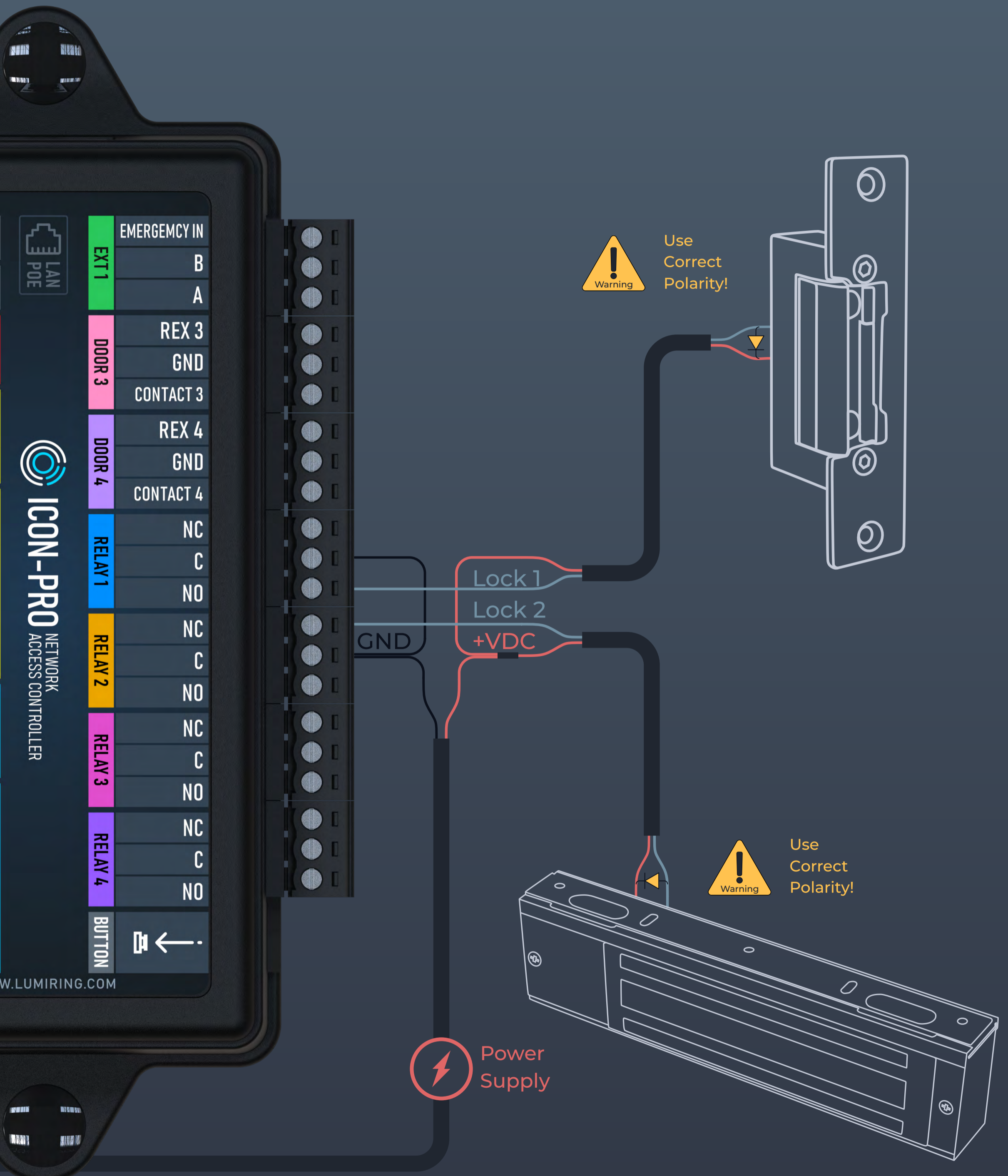
## Connection Diagram





# Electric Lock [Power Supply +12 VDC]

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

# Electric Lock [Power Over Ethernet]

## Connection Diagram

**Warning**  
Use  
Correct  
Polarity!

**Warning**

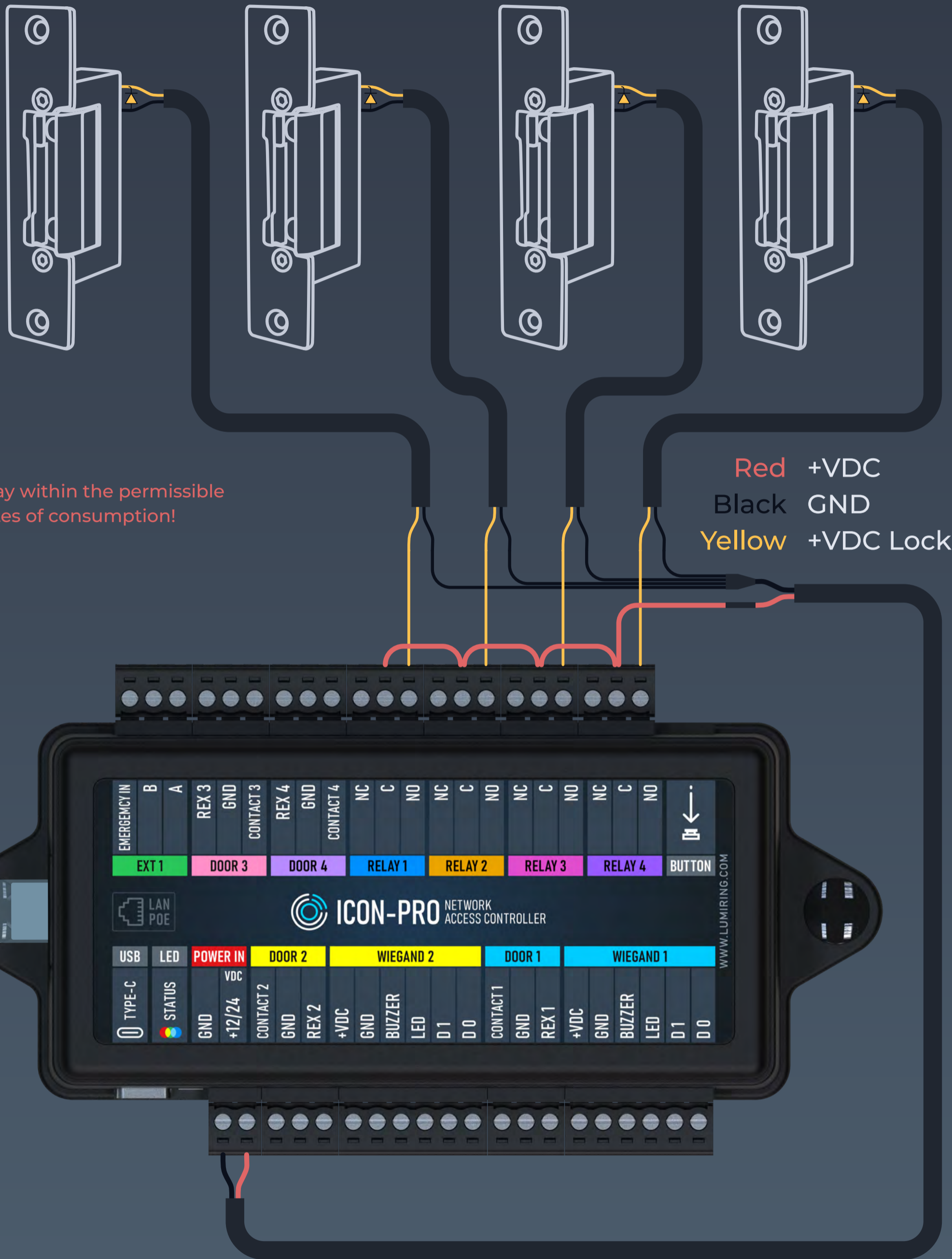
Stay within the permissible  
rates of consumption!

Red +VDC  
Black GND  
Yellow +VDC Lock

**PoE**  
Power  
Over  
Ethernet

**Warning**

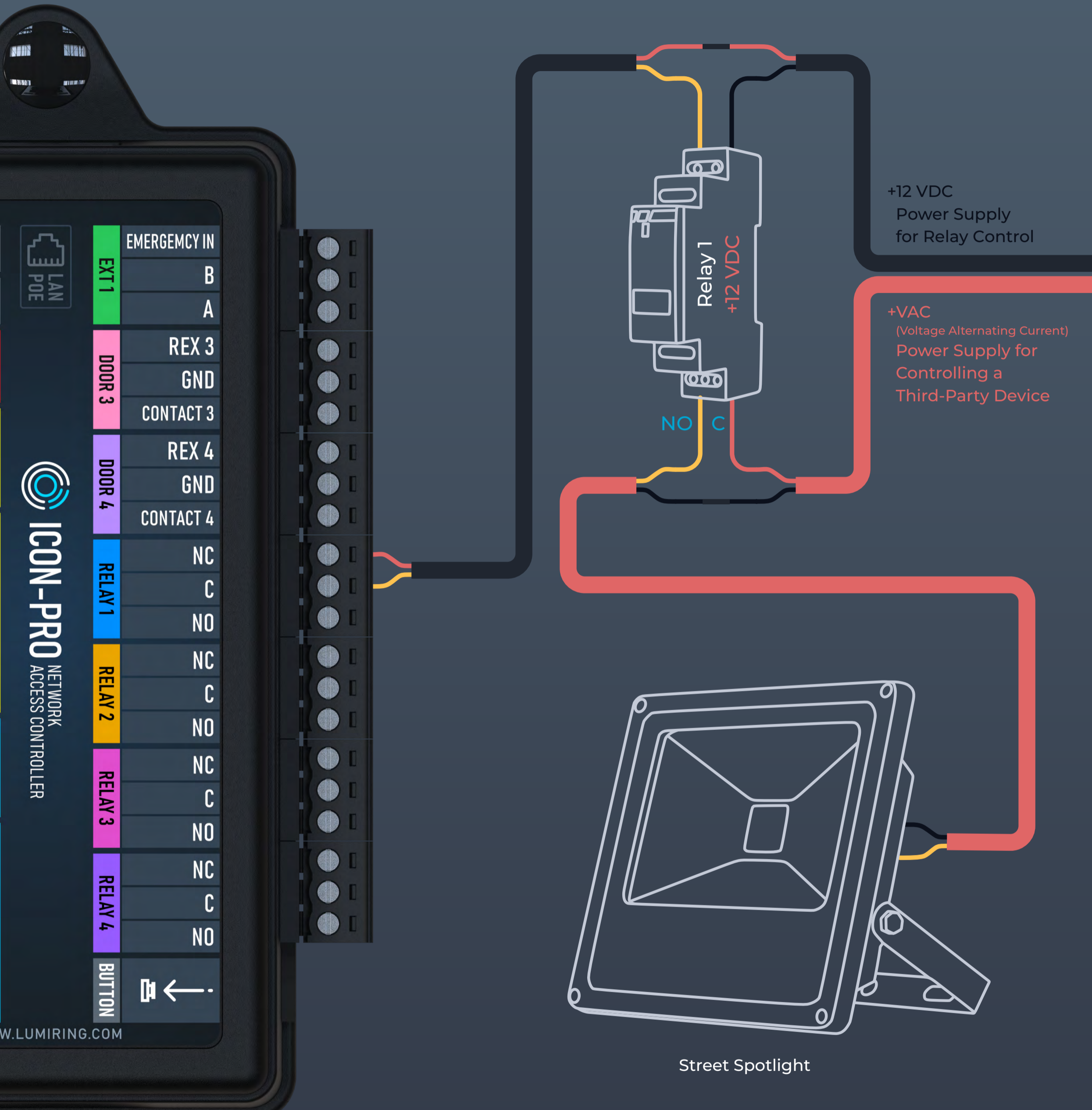
When using PoE to power the controller, the total load of all connected devices must not exceed 1.5A.  
Use the pulse type of electric lock control.  
Do not connect electromagnetic locks to the controller when using PoE!  
High power consumption can lead to overheating of the device and its failure!





# Third-Party Device [Relay +12 VDC]

## Connection Diagram



+12 VDC  
Power Supply  
for Relay Control

+VAC  
(Voltage Alternating Current)  
Power Supply for  
Controlling a  
Third-Party Device

Street Spotlight



When using high-power electric deadbolts, use an auxiliary relay and a separate power supply. Use an auxiliary relay to control circuits using a supply voltage other than the controller supply voltage.



## Connecting to Device

### Connecting to the built-in Wi-Fi AP

Step 1. Connect the device to a power source.

Step 2. Search for Wi-Fi and connect to the ICON-Pro\_(serial number) 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.

*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.*

### Connecting via Ethernet

Step 1. Connect the Ethernet cable to the device.

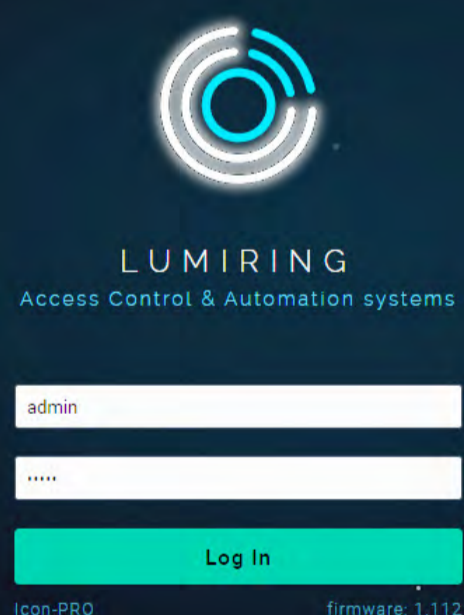
Step 2. Connect the device to a power source.

Step 3. In the address bar of your browser, enter the device's 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



The image shows a login interface for LUMIRING. At the top center is a logo consisting of three concentric circles with a glowing effect. Below the logo, the text "LUMIRING" is displayed in a bold, sans-serif font, followed by "Access Control & Automation systems" in a smaller font. There are two input fields: the first contains the text "admin" and the second contains six dots, indicating a password field. Below these fields is a red button with the text "Log In". At the bottom left, it says "Icon-PRO" and at the bottom right, it says "firmware: 1.112".

# Quick Start

The screenshot shows the LumiRing Quick Start interface. At the top, there is a header with the LumiRing logo and a settings icon. Below the header is a diagram showing an 'ICON' device connected to a router, which is connected to a 'CLOUD' service. The interface is divided into three main sections:

- Network:** This section prompts the user to select a network connection type. The 'Network type' dropdown is set to 'Wi-Fi network'. The 'SSID name' dropdown is set to 'lumiring'. A password field is visible with masked characters. A 'Submit' button is at the bottom.
- Cloud:** This section prompts the user to enter cloud account information. The 'Account Id' field contains '147'. A note below the field states: 'You can find the Account ID information at your UNIMACS cloud account. Please check the account settings. If you have not registered at the UNIMACS cloud - please REGISTER first.' The 'Device note' field contains 'For Office 207'. A 'Submit' button is at the bottom.
- Security:** This section prompts the user to change the password for device network access and Wi-Fi AP. A checkbox 'Use the same password for two purposes' is checked. Under 'Wi-Fi AP', the 'Local Wi-Fi AP name (8 characters minimum)' field contains 'Icon-PRO\_8100416'. There are two password fields: 'Password (8 characters minimum)' and 'Repeat password', both with masked characters. A 'Submit' button is 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.

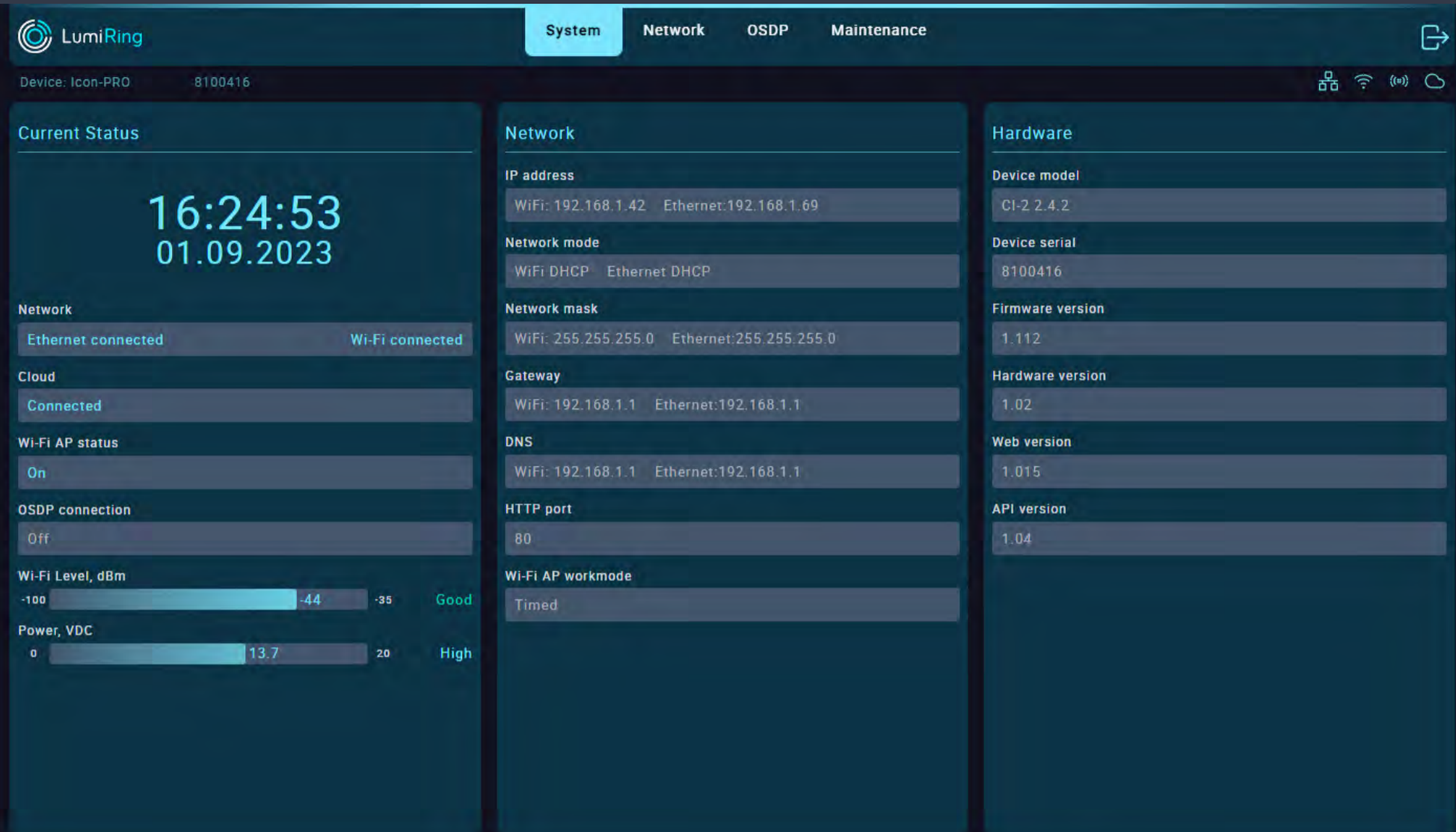
## Cloud:

- 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.

# System



This 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).
- 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.
- Level and quality of the device's connection to the Wi-Fi router.
- Power supply voltage value.

In the Hardware Information subsection, you can see the:

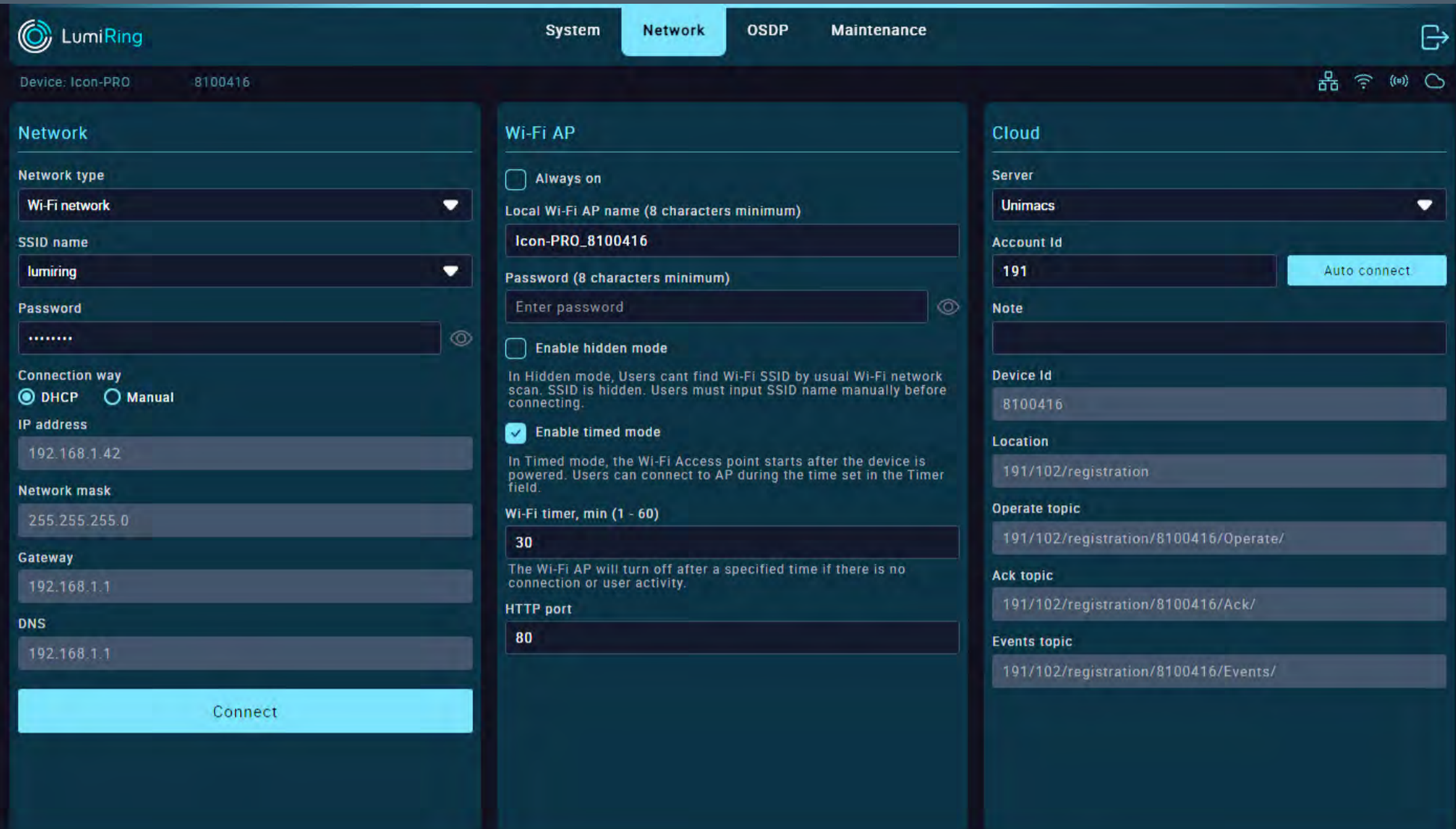
- Device model name.
- Device type.
- Device serial number.
- Current firmware version.
- Current hardware version of the device.
- Web version used by the device.
- Application programming interface (API) version used by the device.

The Network Information 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.



# 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 displays the LumiRing Network configuration page for a device named 'Icon-PRO' with ID '8100416'. The page is organized into three columns:

- Network:** Shows 'Wired Ethernet Network' as the selected network type. The connection method is set to 'DHCP'. The IP address is 192.168.1.69, the network mask is 255.255.255.0, the gateway is 192.168.1.1, and the DNS is 192.168.1.1.
- Wi-Fi AP:** The 'Always on' option is disabled. The local Wi-Fi AP name is 'Icon-PRO\_8100416'. The password field is currently empty. 'Enable hidden mode' is disabled, and 'Enable timed mode' is checked. The Wi-Fi timer is set to 30 minutes.
- Cloud:** The server is set to 'Unimacs'. The account ID is '191'. There is an 'Auto connect' button. The device ID is '8100416'. The location is '191/102/registration'. The MQTT topics are: Operate topic: '191/102/registration/8100416/Operate/', Ack topic: '191/102/registration/8100416/Ack/', and Events topic: '191/102/registration/8100416/Events/'.

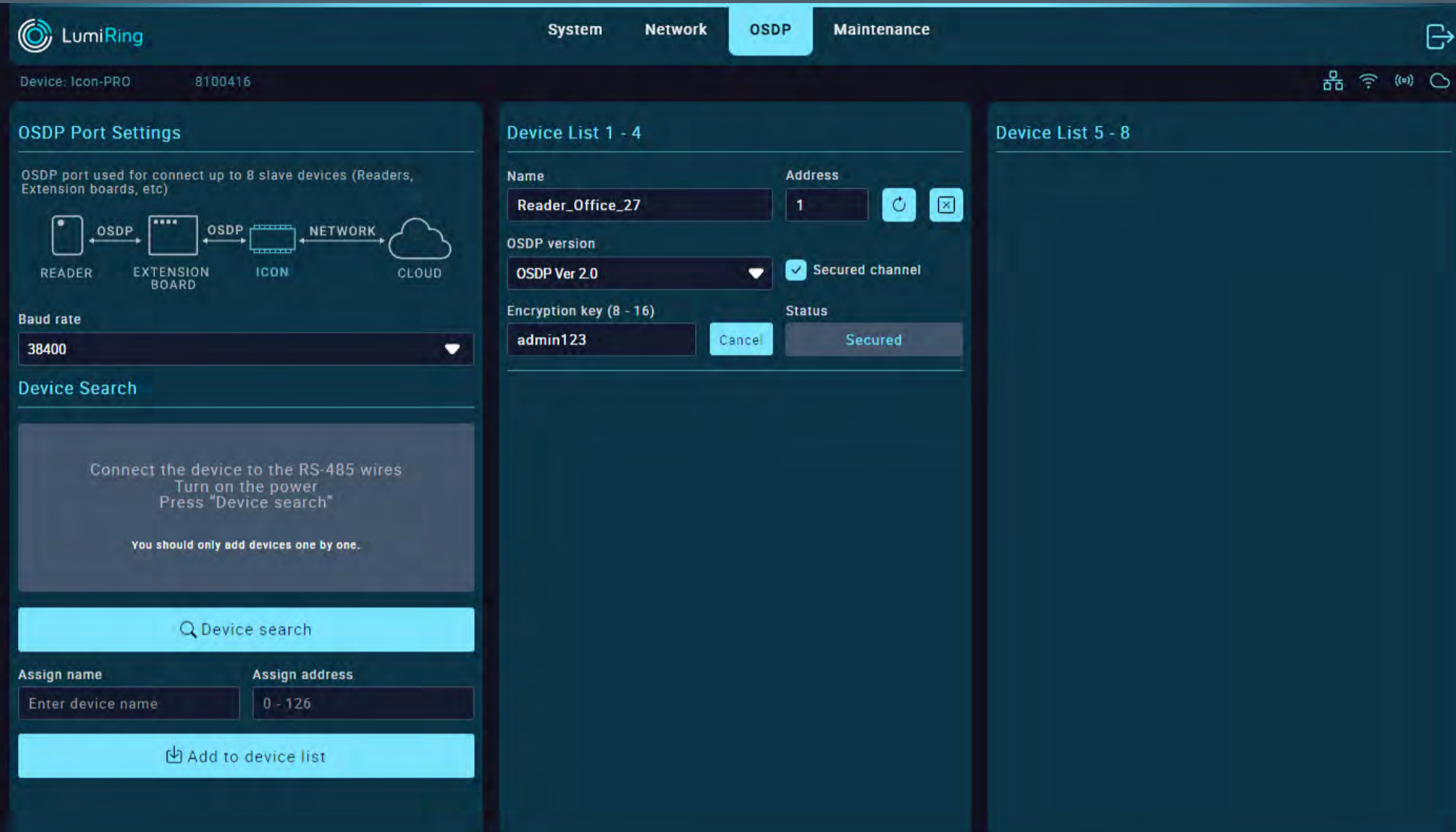
The Cloud settings subsection allows you to connect the controller to a cloud server for later use.

- 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.

# 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.

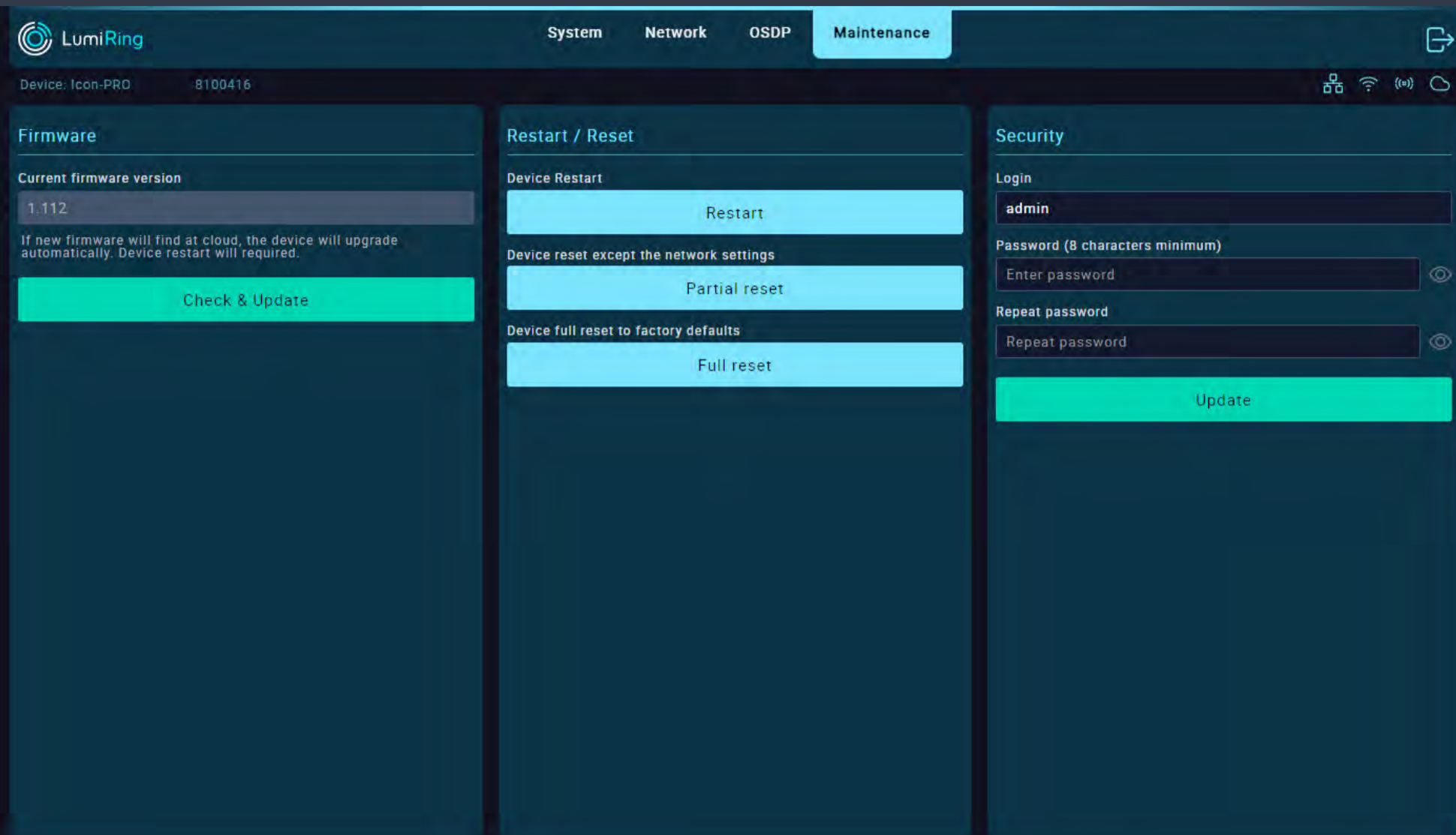
In the Device List 1-4 subsection, you can make additional settings for each device individually.

- 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 - Secure or Not Secure.

*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.*



# 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.
- 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 the button



### Hardware reset

1. Keep the button pressed.
2. Wait for four quick beeps.
3. Release the button.
4. The device will blink red and emit five quick beeps, then change to blue.
5. The hardware reset procedure is complete, and the device is ready for use.



## 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

