2026-05-19
V 3.3

Fw.v. 1.106

Hw.v. RA-2R / REV.1.09

Federal Communications Commissions

DATASHEET

DESKTOP READER/ENCODER

AIR-D

Description

The AIR-D desktop RFID personalizer is an essential element for an access control system with a large number of users. It provides a convenient way to add identifiers to the system, and it protects identifiers from unauthorized copying by securely encrypting the available memory areas. The device is also capable of restoring previously protected identifiers to the factory state.

The advantages of AIR-D are ease of use, simple connection, and no need for additional software. You can start using the device right out of the package. In addition, we have a user-friendly, built-in web interface that allows you to quickly and responsively change the configuration to meet your system requirements.

The AIR-D desktop RFID personalizer finds its application in companies, residential complexes, hotels, and many other institutions with a constantly changing number of users in the system.

Specification

Device info

Model	AIR-D
Processor	ESP32-S3
Over-the-air (OTA) update	Yes
Built-in web server	Yes
Support for 125 kHz identifiers	EM Marine
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)
USB 2.0	Yes

Electrical characteristics

Input voltage	5 VDC +/- 10%
Operation current (AVG) 12 VDC	0.13 A (1.56 W)

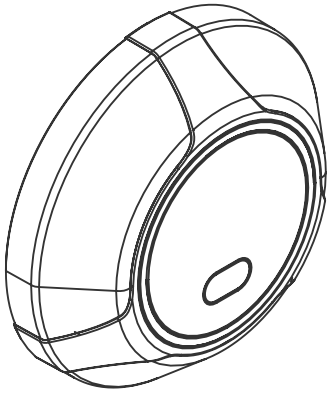
Environmental requirements

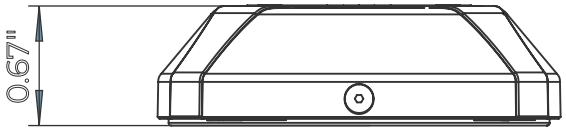
Operating temperature	-22°F ~ 158°F (-30°C ~ 70°C)
Ingress Protection rating	IP54

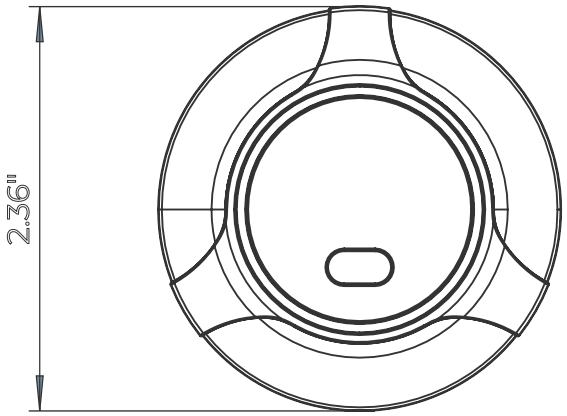
Physical characteristics

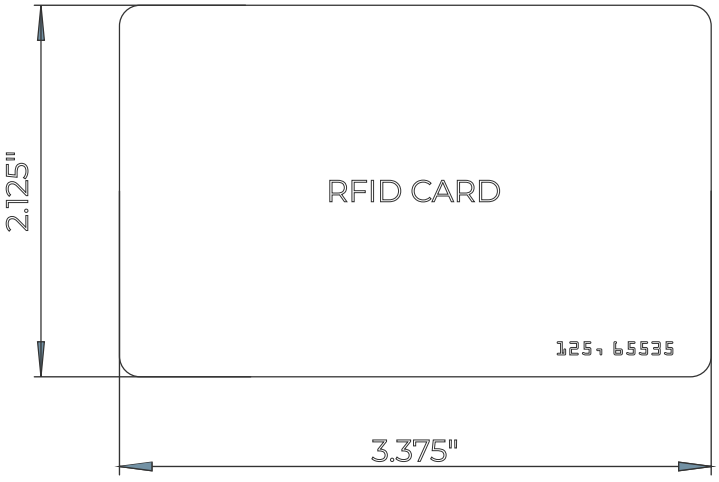
Housing material	ABS plastic UL94 V-0
Dimensions (diameter, height)	2.36" x 0.86" (60 x 22 mm)
USB cable length	40" (100 cm)
Weight	1.59 oz (45 g)

Device Dimensions

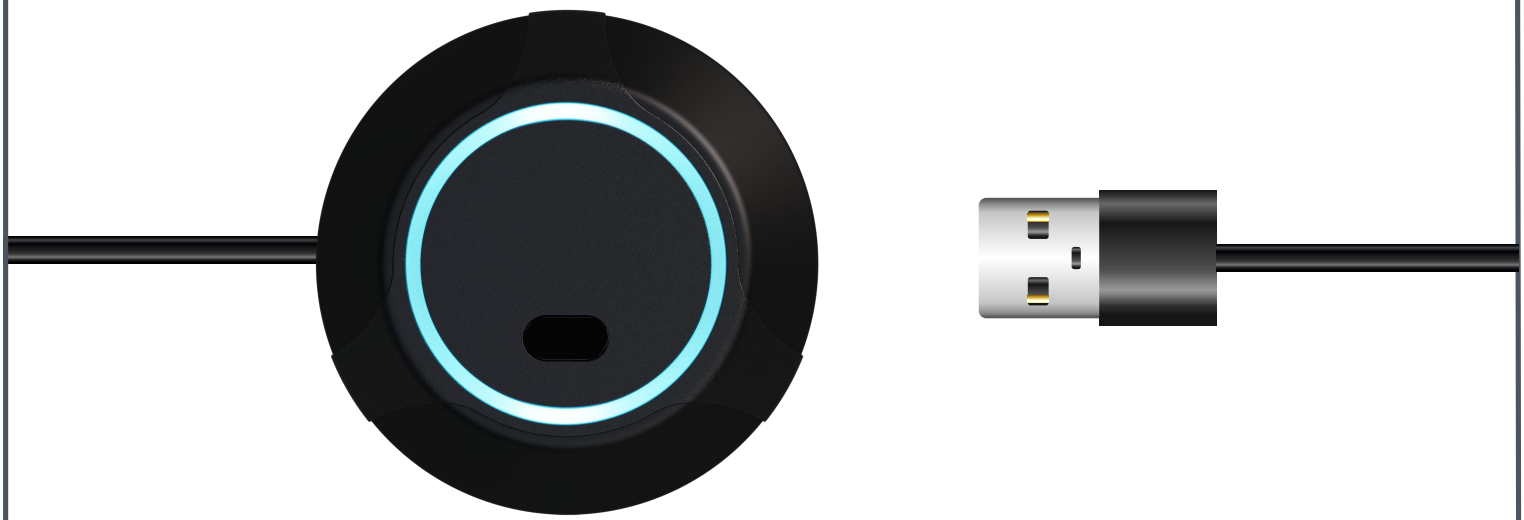




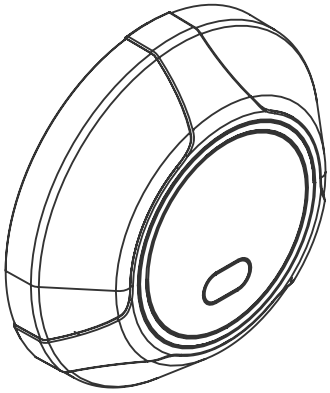


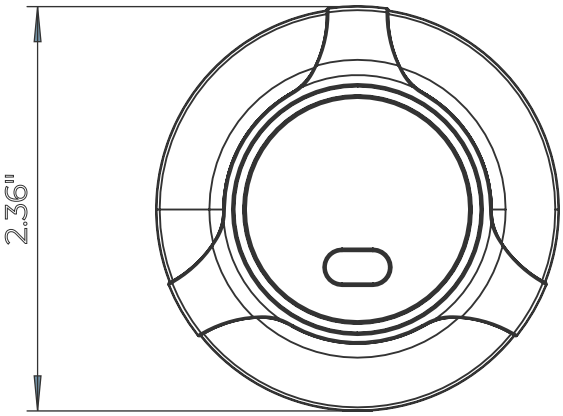


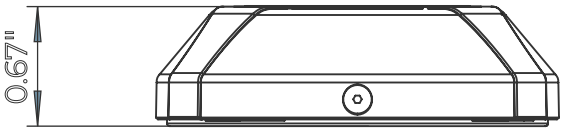
Device Appearance

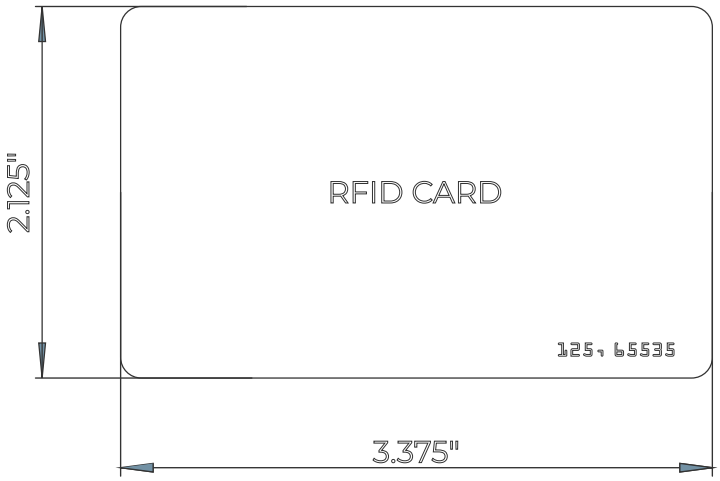


Device Dimensions

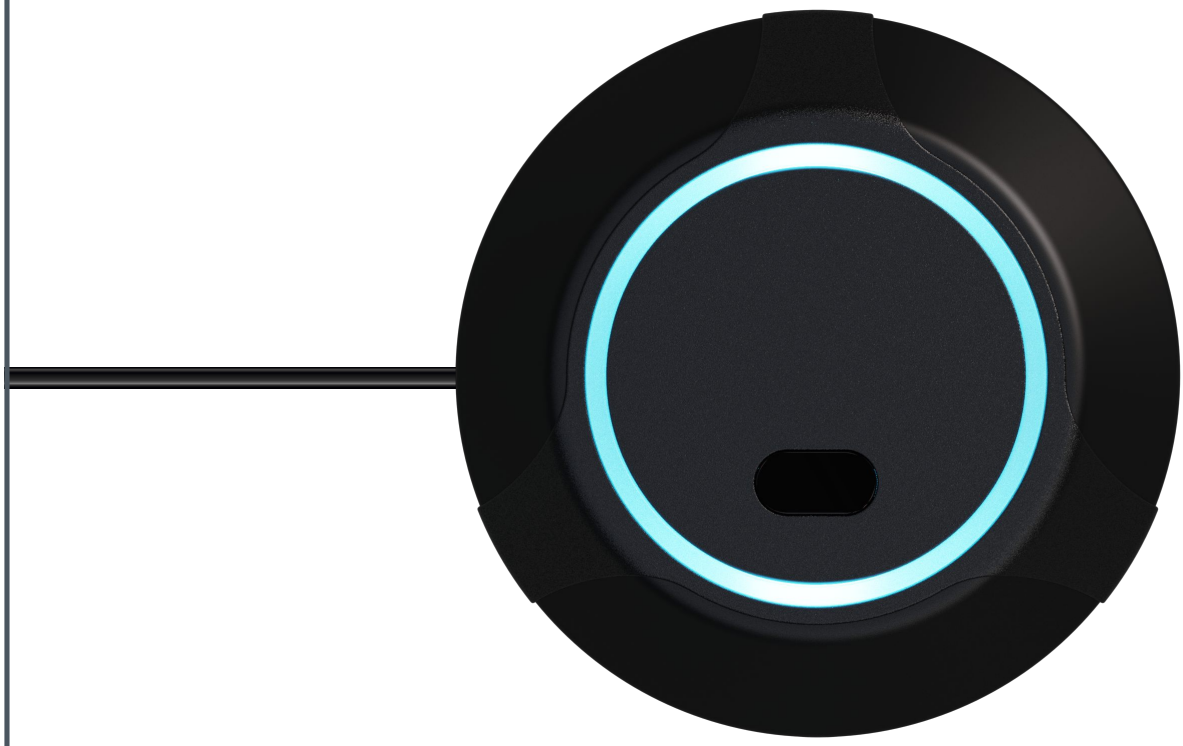






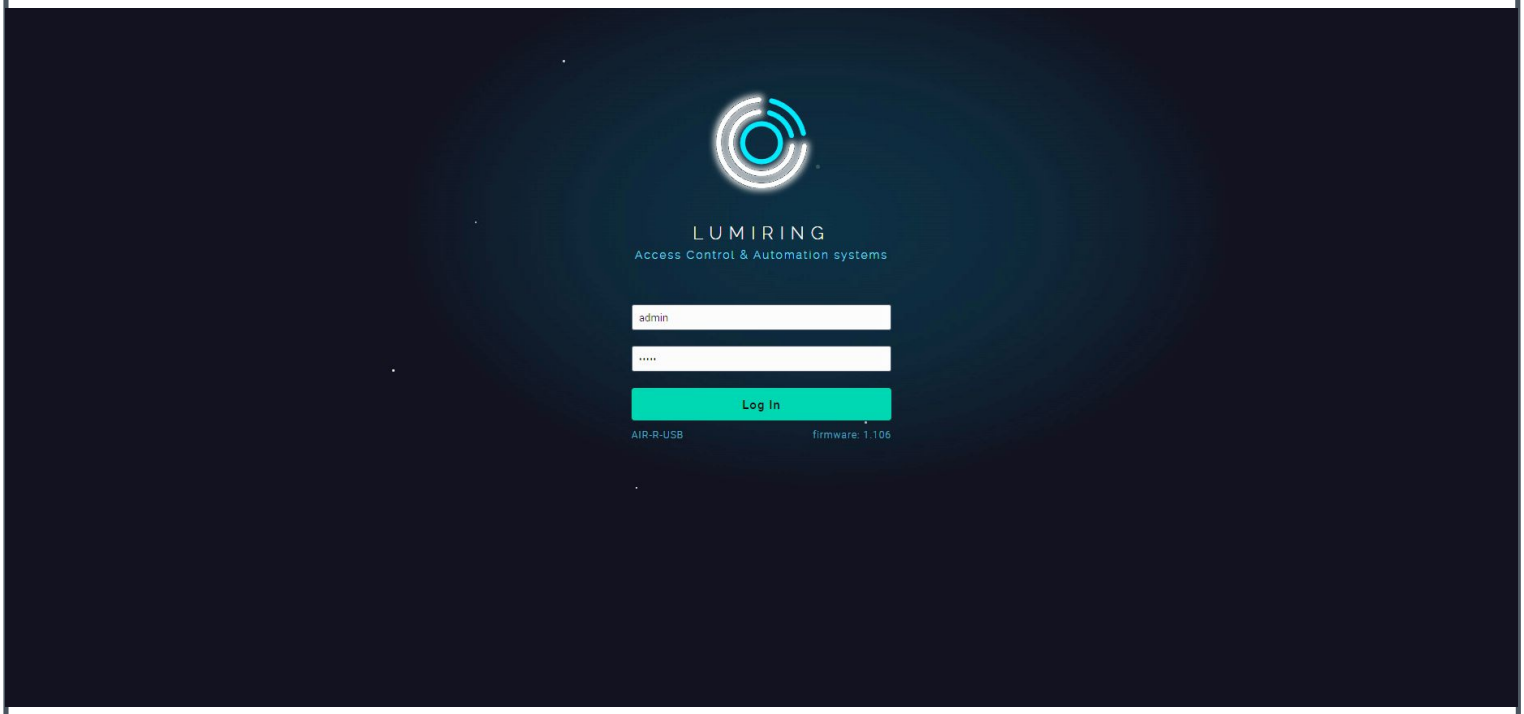


Device Appearance



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.

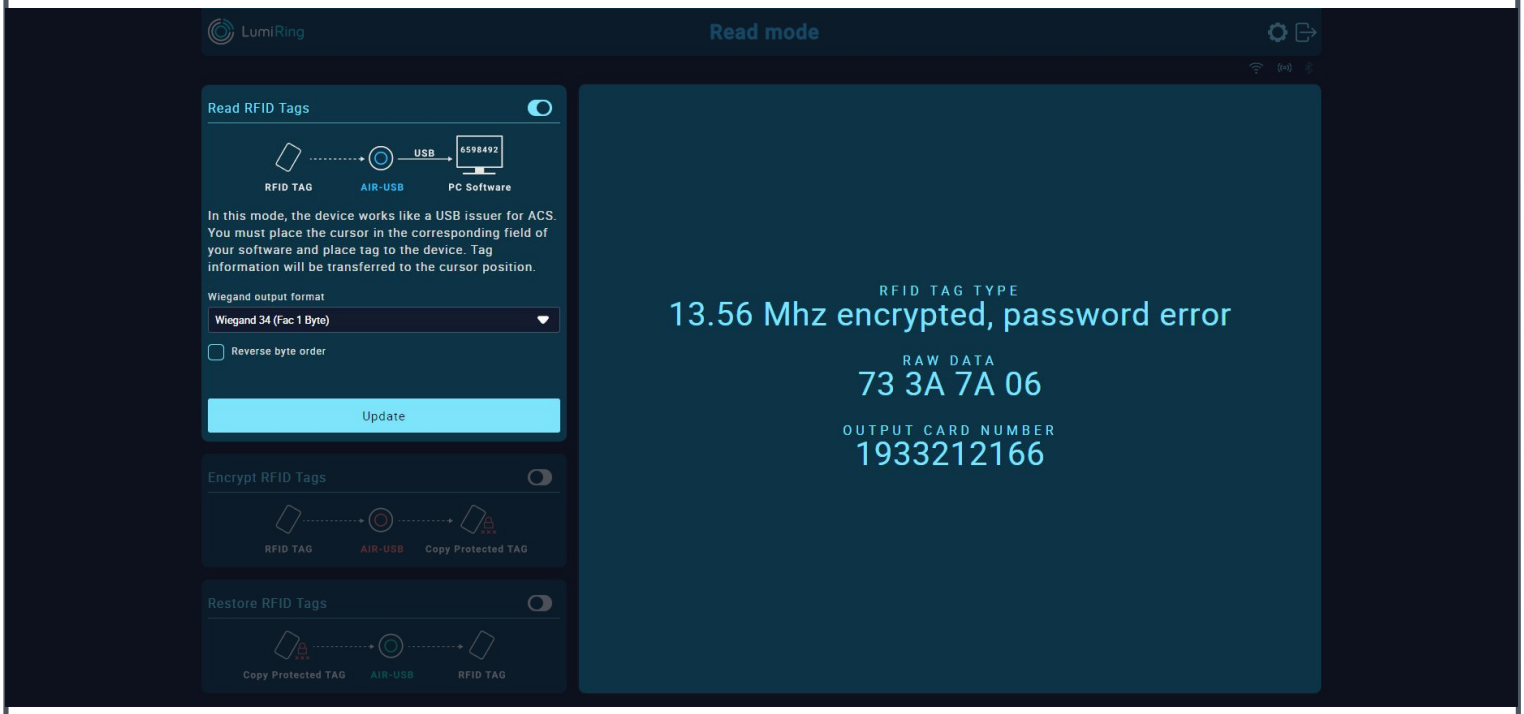
Connection to Device



Connecting to the built-in Wi-Fi AP

Step 1. Connect the device to a USB port.
Step 2. Search for Wi-Fi and connect to the AIR-R-USB_(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 Identifications Read Mode page.

Read Mode



Work mode includes various functions such as Read mode, Encryption mode, and Restore mode for RFID operation. To change modes, use the radio buttons in the mode name headers.

Read mode is designed to read information from IDs and display it on the screen. Merely touch the ID to the device, and its data will be displayed on the right side of the interface screen.

The read ID will automatically be placed in the active field where the mouse pointer is located. This simplifies transferring information to applications or forms, as there will be no need to enter data manually.

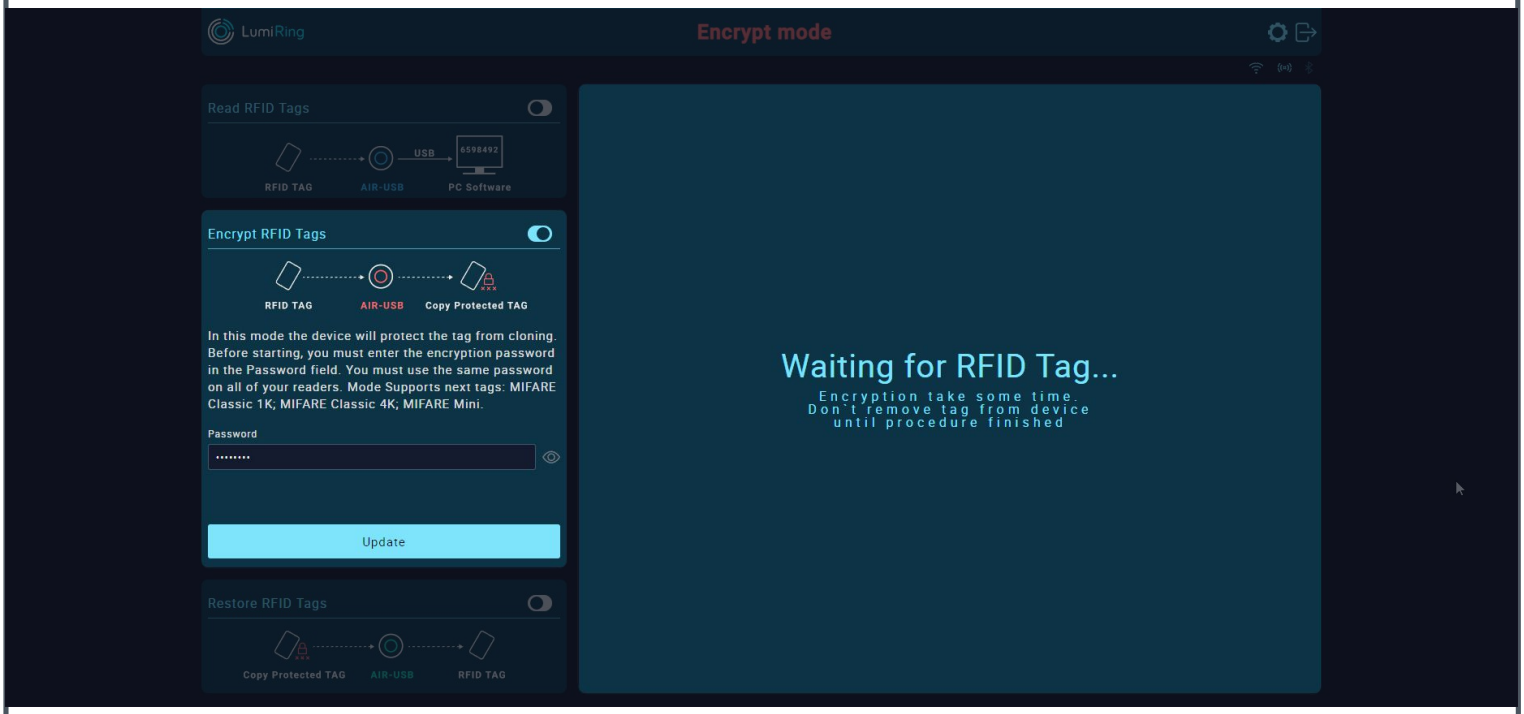
Select the desired output format of the ID codes using the Output Format drop-down list. This allows the ID code output to be tailored to the requirements of a particular system or program.

The user can also select the order in which the ID bytes are read using the appropriate option. This can be useful when the identifier data is read from different devices and where specific formatting is required.

Click the Update button to apply all settings.

Note: The distance from which the ID can be read depends on the type and size of the built-in antenna. It is recommended to keep the IDs at a sufficient distance from the device to avoid reading errors.

Encrypt Mode



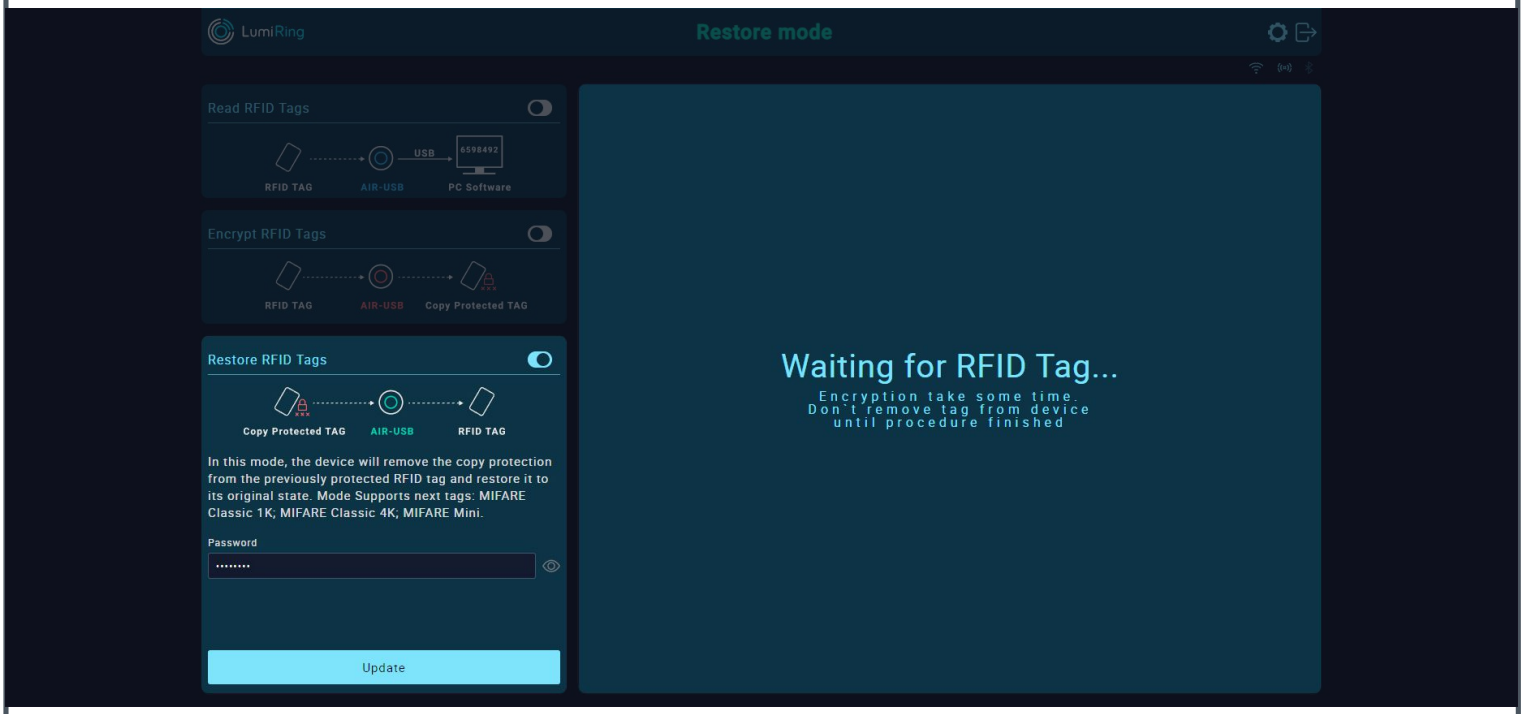
Encrypt mode is designed to protect MIFARE Classic mini/1K/4K RFID identifiers.

To encrypt the identifier, it is necessary to specify a six-character password. After that, to apply the settings, press the Update button.

For the encryption process, attach the identifier to the device and wait for the encryption procedure to finish. After completion, the result of the encryption process will be displayed on the right side of the interface screen: "Success" and the device indication will turn green, or "Failure" and the device indication will turn red.

Note: The encryption process may take longer than an average reading. Wait to remove the attached ID until the encryption process is complete to avoid data transmission errors and prevent data damage.

Restore Mode



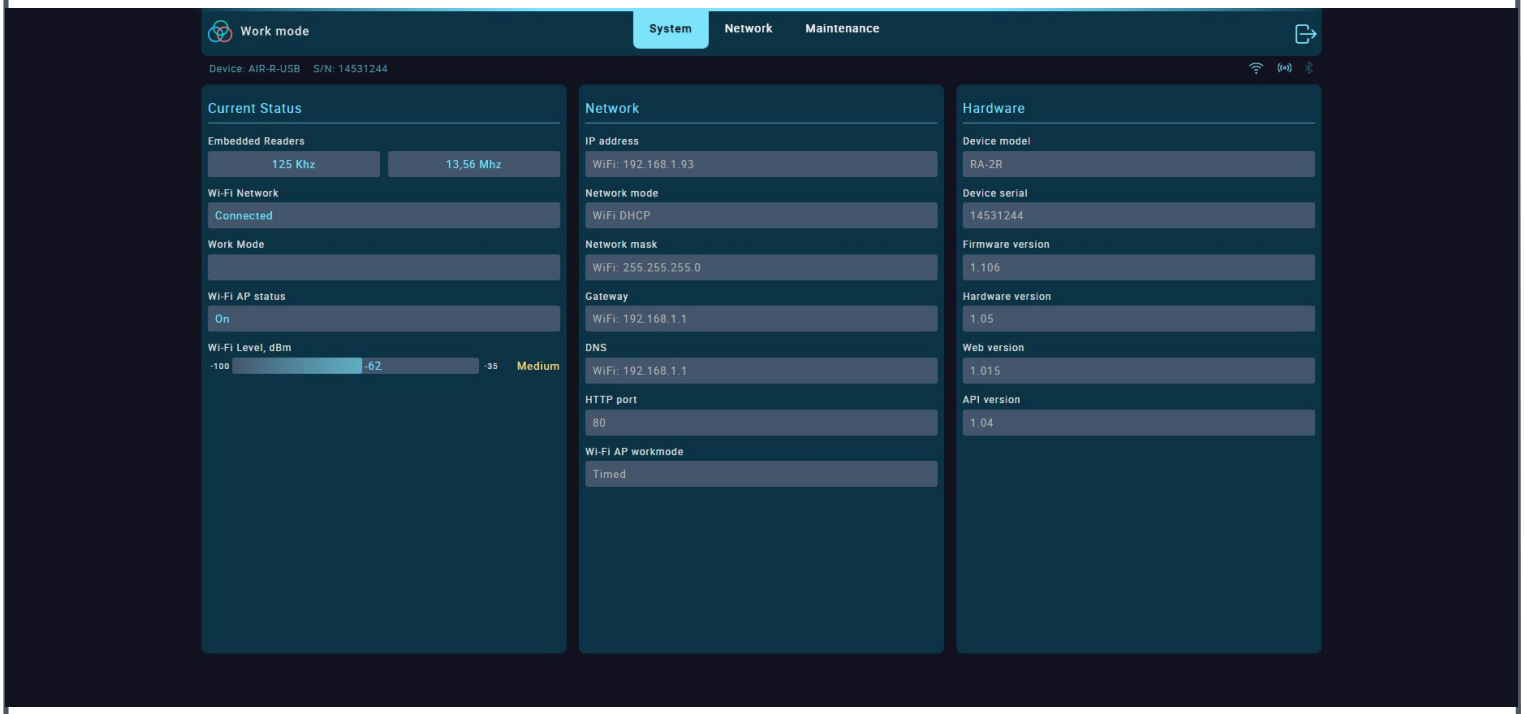
Restore mode is used to unprotect MIFARE Classic mini/1K/4K RFID IDs.

To unprotect, enter the previously used encryption password and press the Update button to apply the setting.

For the recovery process, attach the ID to the device and wait for the recovery procedure to complete. Upon completion, the recovery result will be displayed on the right side of the interface screen: "Success" and the device indication will turn green, or "Failure" and the device indication will turn red.

Note: The ID recovery process may take longer than an average reading. When attaching the ID to the device, do not remove it until the recovery procedure is complete to avoid corrupting the transmitted data and prevent the ID from malfunctioning.

System



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

The Current Status subsection displays the:

- Status of Embedded Readers 125 kHz and 13.56 MHZ. If highlighted, the readers are active. If not highlighted, they are inactive.
- Status of the device's connection to the Wi-Fi router.
- Work Mode status: Read mode, Encrypt mode, or Resore mode.
- Status of the built-in Wi-Fi AP: On or Off.
- Level and quality of the device's connection to the Wi-Fi router.

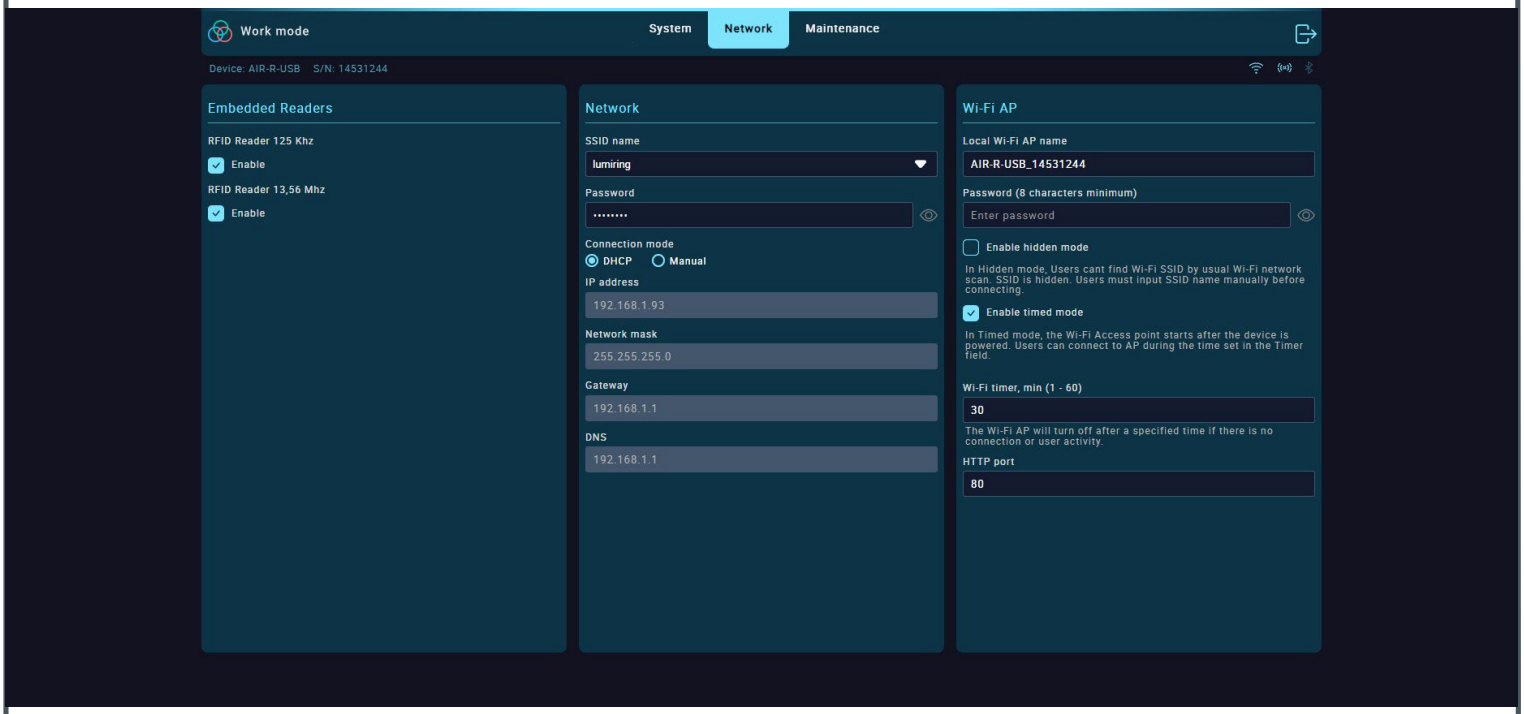
The Network subsection displays the:

- Device’s current network settings.
- Device’s network address.
- Network mode - Manual or Dynamic Host Configuration Protocol (DHCP).
- Network mask.
- Gateway.
- Domain Name Service (DNS).
- Network port of the device.
- Wi-Fi AP Workmode: Timed or Always On.

In the Hardware subsection, you can see the:

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

Network



In the Network section, you can turn the ability to read 125 kHz and 13.56 MHz IDs on or off and set up a connection to the Wi-Fi router for remote administration or firmware updates. You can also change the connection settings for the built-in Wi-Fi AP and set the activity time.

Embedded Readers

- To disable or enable reading of 125 kHz or 13.56 MHz identifiers, select the corresponding Enable checkboxes.
- Click the Update button to apply the settings.

Network

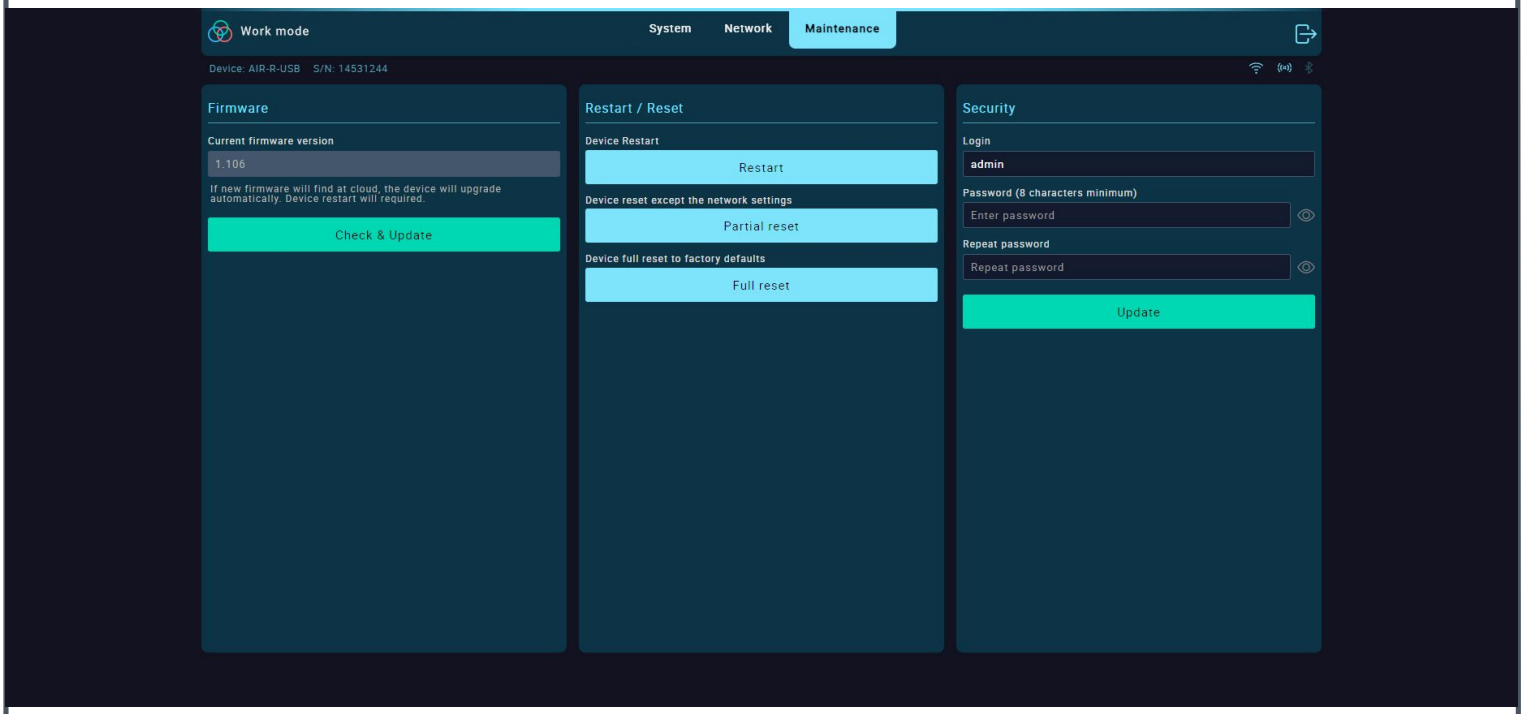
- Click on the SSID Name field to start scanning for available Wi-Fi networks.
- Select the desired network and enter the connection password.
- You can choose the DHCP connection path, in which the device will receive all settings automatically, or Manual, where you will have to enter all network settings yourself.
- Click the Update button to apply the settings.

Wi-Fi AP

- 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.

Note: A reboot may be required to apply the network settings.

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 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.
- 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 pressing Update.

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

FCC Caution

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

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

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

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

  RF warning for Mobile device: This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

For Notes

PROFESSIONAL / COMMERCIAL USE ONLY

This product is intended, marketed, and sold only for professional installation and commercial, industrial, institutional, or business access-control use. It is not intended, marketed, or sold as a consumer product. Any purchase or use confirms buyer is acting for commercial, professional, industrial, institutional, or business purposes.

SAFETY AND APPLICATION LIMITATIONS

This product is an access-control component. It is not a complete access-control system, life-safety device, fire alarm, emergency egress device, or UL 294-listed system unit.

Installation, system design, equipment selection, fail-safe/fail-secure configuration, code compliance, AHJ approval, and testing are the sole responsibility of installer/integrator/system designer.

This product must not be connected to critical entry, exit, barrier, elevator, gate, or emergency egress control as the sole release mechanism without alternate exit means and code approval.

WIRELESS PERFORMANCE

Wireless communication may be affected by RF interference, jamming, distance, obstacles, and site conditions. Range and performance are site-dependent and not guaranteed. Do not use as sole communication path for life-safety or emergency-egress functions.

CYBERSECURITY

Default credentials are for initial setup only and must be changed before deployment. Installer/operator is responsible for device security and credential management.

FIRMWARE UPDATES

Firmware updates may change device behavior. Complete system must be tested before return to service. Do not interrupt updates.

EXPORT CONTROL

This product may be subject to U.S. export control and sanctions laws. Export, re-export, transfer, or use contrary to applicable law is prohibited.

WARRANTY EXCLUSIONS

Warranty does not cover damage, malfunction, or performance issues caused by surge, lightning, water intrusion, incorrect voltage, reverse polarity, improper wiring, improper grounding, unauthorized modifications, abuse, misuse, failure to follow documentation, or use outside rated conditions.

This product is sold subject to New York law.

1. DOCUMENT PRECEDENCE

In any conflict between marketing materials and technical documentation, the current technical documentation prevails.

2. PRODUCT AUDIENCE AND BUYER RESPONSIBILITY

Lumiring products are professional access control devices for system integrators and technically proficient users. Buyer is responsible for verifying product suitability, functionality, compatibility, and compliance with requirements before purchase and deployment.

3. THIRD-PARTY INTEGRATION AND COMPONENTS

Integration with third-party platforms (Home Assistant, Node-RED, custom servers, etc.) requires buyer-side configuration via documented APIs. Compatibility with third-party readers, locks, controllers, and software depends on third-party manufacturer implementation and is buyer responsibility to verify. Lumiring is not responsible for third-party product compatibility, changes, or functionality.

4. RETURNS AND RMA PROCESS

Returns require prior RMA authorization from Lumiring and must be initiated within the period stated on the invoice or applicable warranty terms. Lumiring may require reasonable troubleshooting before issuing an RMA.

An RMA or accepted return does not mean warranty coverage, refund, or replacement approval. Buyer pays return shipping, duties, fees, taxes, and insurance unless Lumiring agrees otherwise in writing. Products must be returned in reasonable condition with applicable accessories unless Lumiring authorizes otherwise.

5. INTERNATIONAL SALES

For sales outside the United States, buyer is responsible for all customs duties, import taxes, VAT, brokerage fees, and compliance with local import/export regulations. Lumiring does not reimburse duties, taxes, shipping or fees paid by buyer.

6. WARRANTY AND LIMITATION OF LIABILITY

Complete warranty terms, return process, exclusions, and liability limitations are subject to Lumiring Inc Terms And Conditions, Limited Warranty, Limited Liability, and Limited License.

To the maximum extent permitted by law, Lumiring is not liable for loss of use, business interruption, lost revenue, lockout, security breach, loss of data, labor, removal/reinstallation costs, or consequential, incidental, indirect, special, or punitive damages. Maximum liability is limited to amount paid for the affected product.

7. GOVERNING TERMS

This product is sold subject to Lumiring Inc Terms and Conditions, Limited Warranty, Limited Liability, and Limited License, and governed by New York law.