



W4AKey

Instruction Manual



W4A[®]

Contents

1. About this manual.....	6
1.1. Purpose and scope.....	6
1.2. Intended audience.....	6
1.3. Models covered.....	7
1.4. Firmware and application compatibility.....	7
1.5. Symbols and warning levels.....	7
1.6. Conventions used.....	8
2. Safety.....	9
2.1. General information.....	9
2.2. Qualifications and responsibilities.....	9
2.3. Electrical safety and protective devices.....	10
2.4. Conductors, terminals, inputs, and outputs.....	10
2.5. Unexpected or remote operation.....	11
2.6. Intended use and limitations.....	12
2.7. Prohibited uses.....	13
2.8. Interlocking, sequences, and inputs.....	13
2.9. Environment, mounting, and maintenance.....	14
2.10. Communications, credentials, and updates.....	15
2.11. Abnormal operation and emergencies.....	15
2.12. Residual risks.....	16
3. Product description and variants.....	17
3.1. Product overview.....	17
3.2. Main functions.....	17
3.3. Device identification.....	17
3.4. Functional elements.....	18
3.5. User profiles.....	18
3.6. Communication methods.....	18
3.7. Data storage.....	19
4. Technical specifications.....	20
4.1. Scope of the specifications.....	20
4.2. General characteristics.....	20
4.3. Power supply and consumption.....	20
4.4. Output circuits.....	20
4.5. Input circuits.....	21
4.6. Radio communications.....	21
4.7. Dimensions and weight.....	21
4.8. Application limits.....	22
5. Planning and electrical installation.....	23
5.1. Scope.....	23
5.2. Checks before installation.....	23
5.3. Selecting the installation location.....	23
5.4. Mounting the enclosure.....	24
5.5. Identifying the components.....	25
5.6. Preparing and routing the cables.....	25
5.7. Connecting the power supply.....	26
5.8. Connecting the inputs.....	27
5.9. Connecting the outputs.....	28
5.10. Connecting to an automation input.....	28
5.11. Connecting through an auxiliary relay or contactor.....	29

5.12. Closing the enclosure.....	29
5.13. Final connection checks.....	30
5.14. First power-up.....	30
6. Indicators and service controls.....	32
6.1. LED.....	32
6.2. Device button.....	32
6.3. Indicator summary.....	33
7. Installing the application.....	34
7.1. Purpose.....	34
7.2. Mobile device requirements.....	34
7.3. Compatible operating systems and platforms.....	34
7.4. Installing the application.....	35
7.5. Required permissions.....	35
7.6. Preparing Bluetooth.....	36
7.7. Updating the application.....	36
7.8. General configuration rules.....	37
8. Operating concepts.....	38
8.1. Inputs, outputs, operations, and commands.....	38
8.2. Actuation types.....	38
8.3. Duration, delay, and sequences.....	39
8.4. Interlocking and input priority.....	39
8.5. Restricted operations and schedules.....	39
8.6. Profiles, hierarchy, and dependents.....	40
8.7. Profile restrictions.....	40
8.8. Counting accesses.....	41
8.9. Traceability, credentials, and sessions.....	41
8.10. Communication methods.....	42
8.11. History and records.....	42
9. Initial pairing and setup.....	44
9.1. Purpose and prerequisites.....	44
9.2. Starting installation in the application.....	45
9.3. Selecting the device.....	45
9.4. Creating the Installer profile.....	45
9.5. Completing and verifying pairing.....	46
9.6. Troubleshooting pairing.....	46
10. Configuring the device.....	48
10.1. Identification and general settings.....	48
10.2. Sessions and connections.....	49
10.3. Configuring Wi-Fi communication.....	50
10.4. Remote communication.....	52
10.5. General output settings.....	53
10.6. General input settings.....	54
11. Configuring operations.....	56
11.1. Accessing operation settings.....	56
11.2. Creating an operation.....	56
11.3. Operation parameters.....	56
11.4. Editing, disabling, or deleting an operation.....	60
11.5. Testing an operation.....	61
12. Testing and commissioning.....	62
12.1. Preparation.....	62
12.2. Testing inputs and outputs.....	62
12.3. Testing operations and access.....	63

12.4. Completing commissioning.....	63
13. Managing Administrators.....	64
13.1. Creating an Administrator.....	64
13.2. Administrator parameters.....	64
13.3. Sharing the profile.....	65
13.4. Editing or deleting an Administrator.....	65
13.5. Verification.....	66
14. Pairing a user profile.....	67
14.1. Signing in and pairing the profile.....	67
14.2. Verifying pairing.....	70
14.3. Pairing not completed.....	71
15. Managing the profile.....	72
15.1. Profile settings.....	72
16. Device information and management.....	74
16.1. Device status.....	74
16.2. Information and identification.....	74
16.3. Password and sessions.....	75
16.4. Removing the profile.....	75
16.5. Updating the device.....	76
16.6. Factory data reset.....	76
17. Managing dependents.....	77
17.1. Accessing dependents.....	77
17.2. Creating a dependent.....	77
17.3. Configuring the dependent.....	77
17.4. Access limit.....	78
17.5. Time restrictions.....	78
17.6. Saving and sharing the profile.....	79
17.7. Editing or deleting a dependent.....	80
18. Executing and configuring commands.....	81
18.1. Executing commands.....	81
18.2. Configuring commands.....	83
18.3. Using Android Auto and Apple CarPlay.....	87
19. One-Time Access.....	89
19.1. Signing in with One-Time Access.....	89
19.2. Using operations.....	89
19.3. Ending access.....	90
20. Offline mode.....	91
20.1. How it works.....	91
20.2. Generating an offline file.....	91
20.3. Available actions.....	92
20.4. Sending the file.....	93
20.5. Executing the file on the device.....	94
20.6. Execution result.....	94
20.7. Limitations and security.....	95
21. History.....	96
21.1. Viewing history.....	96
21.2. Actuation history.....	96
21.3. Dependent history.....	97
21.4. Installer history.....	97
21.5. Profile creation and deletion.....	97
21.6. History limitations.....	98
22. Troubleshooting.....	99

22.1. Troubleshooting table.....	99
22.2. General checking procedure.....	102
22.3. Restarting the device.....	103
22.4. When to consider a factory data reset.....	103
22.5. When to stop using the equipment.....	104
22.6. Contacting technical support.....	104
23. Factory data reset.....	106
23.1. Purpose and consequences.....	106
23.2. Option 1 — Reset by the Installer.....	106
23.3. Option 2 — Reset using the button.....	107
23.4. Option 3 — Full reset.....	108
23.5. Checks after reset.....	108
24. Regulatory compliance.....	109
24.1. CE marking.....	109
24.2. EU Declaration of Conformity.....	109
24.3. Restriction of hazardous substances.....	109
24.4. Changes to the equipment.....	109
25. Disposal and end of life.....	111
25.1. Disposing of the equipment.....	111
25.2. Private users.....	111
25.3. Professional users.....	111
25.4. Internal battery.....	111
25.5. Deleting data.....	112
26. Warranty, liability, and support.....	113
26.1. Responsibilities of the user and Installer.....	113
26.2. Improper use.....	113
26.3. Limitations of communications, states, and records.....	113
26.4. Warranty.....	114
26.5. Technical support.....	114

1. About this manual

1.1. Purpose and scope

This manual contains the information needed to install, configure, use, maintain, and troubleshoot the W4A Key.

Read the instructions before installing, wiring, configuring, or using the device.

Following this manual helps to:

- ensure that the equipment operates correctly;
- prevent incorrect wiring and configuration;
- reduce electrical hazards and unexpected operation;
- protect user credentials and data;
- ensure proper use of the available communication methods.

Keep this manual with the equipment throughout its service life and make it accessible to the Installer, owner, users, and maintenance personnel.

1.2. Intended audience

This manual is intended for:

Installer

A person qualified and authorized to:

- select and install the equipment;
- make the electrical connections;
- configure inputs, outputs, and operations;
- create the Installer profile;
- test and commission the device.

Only qualified personnel may work on the electrical installation.

Administrator

A person authorized to use the device and create or manage dependent profiles, according to the permissions assigned.

User

A person authorized to perform the available operations and, where permitted, manage dependent profiles.

Guest

A person with limited or temporary access, subject to restrictions set by the profile that created the Guest profile.

Maintenance and technical support personnel

A person qualified and authorized to diagnose, maintain, update, recover, or replace the equipment.

1.3. Models covered

This manual applies to the following models:

Product	Model
W4A Key	W4A Key-24
W4A Key	W4A Key-230

Check the identification label, packaging, or application to confirm the exact model designation.

Some functions may depend on:

- the model;
- the hardware version;
- the firmware version;
- the application version;
- the configuration;
- the profile permissions;
- the available services.

1.4. Firmware and application compatibility

The firmware version is shown in the device information section.

The application version is shown in its settings or in the operating system's official app store.

The availability of Android Auto, Apple CarPlay, and other external service integrations may depend on the application version, operating system, and services provided by third parties.

Screens, parameters, and procedures may vary between versions.

Whenever possible, use firmware and application versions provided or recommended by W4A.

Do not interrupt the power supply or communication during an update unless the application expressly instructs you to do so.

1.5. Symbols and warning levels

This manual uses the following signal words:

DANGER

Indicates an imminent hazardous situation that, if not avoided, will result in death or serious injury.

WARNING

Indicates a potentially hazardous situation that could result in death or serious injury.

CAUTION

Indicates a situation that could result in minor injury or damage to the equipment, installation, or controlled load.

NOTE

Indicates additional information relevant to installation, configuration, use, or maintenance.

1.6. Conventions used

In this manual:

- menu, button, and option names in the application appear in bold;
- numbered instructions must be followed in the order shown;
- “device” or “equipment” refers to the W4A Key;
- “application” refers to the compatible official application;
- “profile” refers to an identity authorized to access the device;
- “dependent” refers to a profile created by another profile;
- “operation” refers to a function configured on the device;
- “command” refers to the element in the application used to execute an operation;
- “input” refers to a terminal intended to receive an external contact;
- “output” refers to a relay contact used to control an external circuit;
- ON and OFF correspond to the active and inactive states, respectively.

References to remote communication assume that the required services and Internet connection are available.

2. Safety

2.1. General information

Incorrect installation, configuration, or use of the W4A Key can cause:

- electric shock;
- fire;
- damage to the equipment or controlled load;
- unexpected operation of doors, gates, barriers, shutters, or other mechanisms;
- loss of control over access;
- use by unauthorized persons.

Before installing, configuring, or using the device:

- read this manual;
- confirm that the model is suitable for the installation;
- check the characteristics of the power supply and load;
- use the equipment only for its intended purpose;
- make sure local and remote operation cannot create a hazardous situation.

Compliance with this manual does not replace compliance with applicable legislation, electrical regulations, and safety rules.

2.2. Qualifications and responsibilities

Installation, electrical connection, changes to wiring, technical configuration, testing, and commissioning must be carried out by qualified personnel.

The Installer must have the knowledge needed to:

- interpret electrical diagrams;
- select conductors and protective devices;
- assess the compatibility of the power supply and load;
- identify installation hazards;
- configure inputs, outputs, and operations;
- verify the safety of the complete system.

The end user must not:

- open the equipment;
- modify electrical connections;

- repair the device;
- change settings reserved for the Installer;
- disable protective devices.

2.3. Electrical safety and protective devices

DANGER — Hazardous electrical voltage

Before installing, connecting, removing, or working on the equipment:

1. switch off all power sources;
2. isolate the circuits;
3. prevent accidental reconnection;
4. verify the absence of voltage with a suitable instrument.

Do not touch terminals, conductors, or internal components while the equipment is energized.

The absence of indicator lights does not prove that voltage is absent.

The W4A Key does not replace the protective, switching, or isolation devices required for the installation and the controlled load.

Where applicable, the installation must include:

- short-circuit and overcurrent protection;
- protection against electric shock;
- residual current protection;
- surge protection;
- a switching and isolation device;
- protection appropriate to the load;
- independent means of emergency stopping, opening, or release.

Protective devices must be rated for the required voltage, current, and breaking capacity.

The designer and Installer are responsible for selecting the protective devices.

2.4. Conductors, terminals, inputs, and outputs

Before making any connection, confirm:

- the device model;
- the supply voltage;
- the voltage and current of the external circuit;
- the type of load;

- the electrical diagram;
- the conductor cross-section and insulation.

Conductors must:

- have characteristics appropriate to the installation;
- be correctly inserted into the terminals;
- have no exposed copper;
- have no loose strands;
- be protected against pulling and mechanical damage.

Loose terminals or unsuitable conductors can cause overheating, electric arcing, malfunction, or fire.

The inputs are intended only for dry contacts. Do not apply an external voltage to the inputs.

The outputs are potential-free relay contacts. They do not supply power to the load.

Do not exceed the maximum values stated in the technical specifications.

Inductive loads or loads with high inrush current may require:

- an auxiliary relay;
- a contactor;
- a flyback diode;
- an RC snubber;
- a varistor;
- another suitable protective device.

2.5. Unexpected or remote operation

WARNING — Unexpected movement or operation

The outputs can be activated:

- through the application;
- via Bluetooth;
- via Wi-Fi;
- remotely over the Internet;
- by the inputs;
- by compatible peripherals;
- by sequential operations;
- by another authorized user.

Before executing an operation:

- confirm that you selected the correct operation;
- check that the area around the load is clear;
- make sure no people, animals, or objects are at risk;
- do not operate remotely if you cannot confirm that the area is safe.

Loss of communication does not guarantee that the load is switched off or isolated.

Before inspecting, cleaning, releasing, or repairing the load:

1. put the system in a safe state;
2. switch off and isolate the load's power supply;
3. prevent accidental reconnection;
4. verify the absence of voltage;
5. eliminate the possibility of automatic operation.

2.6. Intended use and limitations

The W4A Key is intended for access control and for operating external circuits through relay outputs.

Depending on the installation, it can be used to control:

- electric locks;
- automatic doors and gates;
- barriers;
- lighting;
- shutters;
- contactors;
- auxiliary circuits;
- other compatible equipment.

The device must be used:

- within its electrical and environmental limits;
- with compatible loads;
- with the required protective devices;
- according to the configuration set by the Installer.

The W4A Key must not be used as the sole device for:

- protecting people;

- emergency stopping;
- emergency evacuation;
- fire safety;
- electrical isolation;
- locking out hazardous machinery;
- preventing crushing or entrapment;
- controlling critical processes.

Where necessary, independent means of emergency opening, stopping, evacuation, or intervention must be provided.

2.7. Prohibited uses

The following are prohibited:

- using the equipment outside its specifications;
- applying an incompatible power supply;
- exceeding the input or output ratings;
- directly connecting incompatible loads;
- using the device as an isolator;
- using the application as the sole means of emergency control;
- operating remotely without ensuring safety;
- removing or bypassing protective devices;
- using incompatible sensors, contacts, or peripherals;
- installing the equipment in explosive atmospheres;
- using equipment with a damaged enclosure, terminals, or cables;
- modifying the hardware or firmware without authorization;
- carrying out unauthorized repairs;
- sharing credentials with unauthorized persons;
- using another person's credentials.

2.8. Interlocking, sequences, and inputs

The inputs may take priority over commands from the application, depending on the configuration.

Interlocking can prevent the outputs from activating simultaneously or deactivate one output when the other is activated.

This function does not replace independent electrical or mechanical interlocking when required for safety.

Operations can be executed sequentially or simultaneously.

Incorrect configuration can cause:

- activation of the wrong output;
- overlapping commands;
- unexpected movement;
- excessive operating times;
- conflicts with inputs or external commands.

The Installer must test all inputs, operations, sequences, and interlocks before making the system available to users.

2.9. Environment, mounting, and maintenance

Install and use the equipment only within the specified environmental limits.

Do not install the device in locations with:

- condensation;
- water or excessive humidity;
- conductive dust;
- flammable or corrosive gases;
- excessive vibration;
- temperatures outside the permitted range;
- direct sunlight;
- intense heat sources;
- potentially explosive atmospheres.

Avoid installing it near:

- large metal surfaces;
- motors;
- transformers;
- contactors;
- power cables;
- sources of electromagnetic interference.

The enclosure must be properly closed and the seals must remain in good condition.

Only qualified personnel or authorized technical support may perform maintenance and repairs.

Do not use the equipment if it shows:

- visible damage;
- deformation;
- moisture;
- signs of overheating;
- a burning smell;
- damaged terminals.

2.10. Communications, credentials, and updates

Bluetooth, Wi-Fi, and Internet communications can be affected by distance, obstacles, interference, network failures, or service outages.

Do not use wireless communication as the sole means of controlling safety-critical functions.

Treat credentials as confidential information.

Users must:

- use strong passwords;
- protect their phone;
- share access data only with authorized persons;
- use secure means to send files, QR codes, or credentials;
- remove profiles that are no longer needed;
- change the password if unauthorized access is suspected.

Use only applications, firmware, and updates provided or authorized by W4A.

Do not disconnect the power supply or interrupt communication during an update unless the application expressly instructs you to do so.

2.11. Abnormal operation and emergencies

Immediately switch off and isolate the power supply, if safe to do so, in the event of:

- smoke, flames, or a burning smell;
- sparks or electric arcing;
- unusual electrical noise;
- excessive heat;
- water ingress;

- damage to the enclosure, terminals, or cables;
- loss of control over the load;
- unexpected operation;
- repeated tripping of protective devices;
- signs of a short circuit;
- any situation that endangers people, animals, or property.

Do not touch the equipment if live parts, fire, water, or another immediate hazard are present.

Use the upstream isolation device.

Do not switch the equipment back on until qualified personnel have identified and corrected the cause.

Failures of Bluetooth, Wi-Fi, the Internet, the application, the clock, or status updates do not necessarily indicate an electrical fault, but must be investigated if they affect safe use.

2.12. Residual risks

Even when the equipment is installed and used correctly, risks may remain due to:

- the presence of voltage;
- unexpected operation of the load;
- movement of doors, gates, barriers, or shutters;
- failure of relays, sensors, or external equipment;
- loss or delay of communications;
- display of outdated status information;
- misuse of credentials;
- incorrect configuration;
- loss of date, time, or data;
- hazards inherent to the controlled load.

The W4A Key does not replace a risk assessment of the complete installation.

The designer, Installer, and person responsible for the installation must implement independent protective measures whenever required.

3. Product description and variants

3.1. Product overview

The W4A Key is an access control and automation device that lets you control external circuits through a mobile application.

Depending on the installation, it can control:

- doors and electric locks;
- gates and barriers;
- shutters;
- lighting;
- contactors;
- auxiliary circuits;
- other compatible equipment.

Device access is managed through authenticated profiles with different permissions and restrictions.

3.2. Main functions

Depending on the model, configuration, firmware, and available services, the W4A Key can:

- read inputs;
- activate outputs;
- create custom operations;
- communicate via Bluetooth and Wi-Fi;
- execute commands remotely over the Internet;
- use selected commands through Android Auto and Apple CarPlay;
- manage profiles and their restrictions;
- create dependent profiles;
- view status information and records;
- update firmware through the application;
- use compatible peripherals.

3.3. Device identification

The model designation and main characteristics are shown on the device identification label.

Additional information, such as the serial number and hardware and firmware versions, can be viewed in the application.

Before installation, confirm that the model is suitable for the power supply, load, and site conditions.

Do not remove, change, or make the identification label illegible.

3.4. Functional elements

The W4A Key operates using the following elements:

- **Inputs:** receive signals from compatible contacts, buttons, switches, or sensors.
- **Outputs:** use relay contacts to control external circuits.
- **Operations:** define how the outputs behave.
- **Commands:** let users execute operations through the application.
- **Profiles:** identify and authorize users.
- **Communications:** provide local or remote access to the device.
- **History:** records events relating to access, operation, and changes.

These elements are explained in detail in Chapter 8 Operating concepts.

3.5. User profiles

The W4A Key uses four types of profile:

- **Installer:** configures the device and creates Administrators;
- **Administrator:** uses the device and manages Users and Guests;
- **User:** performs operations and may manage Guests, if authorized;
- **Guest:** has limited or temporary access.

Each device has only one Installer profile.

The permissions and restrictions for each profile are described in the chapters on profile management.

3.6. Communication methods

The device can communicate via:

- Bluetooth, for local access;
- Wi-Fi, for access over the local network;
- the Internet, when remote communication is enabled;
- Offline mode, to perform certain actions using files prepared in advance.

Each method's availability depends on the configuration and associated services.

3.7. Data storage

Settings, profiles, and records are stored locally on the W4A Key.

Normal operation does not require this data to be stored in an external service.

4. Technical specifications

4.1. Scope of the specifications

The characteristics in this chapter vary by W4A Key model.

Before installation, check the exact model designation on the device identification label.

4.2. General characteristics

Characteristic	Specification
Local communication	Bluetooth Low Energy
Wi-Fi	2.4 GHz, IEEE 802.11 b/g/n
Remote control	Available according to the subscription and associated services
Enclosure protection rating	IP65
Operating temperature	−5 °C to 50 °C
Operating relative humidity	20% to 60%, non-condensing
Clock backup battery	3 V DC — CR2032

The specified protection rating applies when the equipment is correctly installed, the cover is closed, the seals are in good condition, and the cable gland is correctly fitted with compatible cables.

4.3. Power supply and consumption

Model	AC power supply	DC power supply	Maximum power consumption
W4A Key-24	24 V AC, 50/60 Hz	9 to 26 V DC	1.4 W
W4A Key-230	90 to 230 V AC, 50/60 Hz	22 to 48 V DC	1.4 W

AC and DC power supplies are alternatives. Do not apply both at the same time.

4.4. Output circuits

Model	Number of channels	Contact type	Maximum current/voltage (AC)	Maximum current/voltage (DC)
W4A Key-24	2	Normally open	5 A at 250 V AC	5 A at 30 V DC
W4A Key-230	2	Normally open	5 A at 250 V AC	5 A at 30 V DC

The relay contacts are potential-free and do not supply power to the load.

The voltage required by the controlled circuit must be provided by a suitable external source.

Technical specifications

These values are maximum contact ratings; they do not mean that every load drawing less than 5 A can be connected directly.

Actual switching capacity depends, among other things, on:

- the type of load;
- inrush current;
- power factor;
- switching frequency;
- operating temperature;
- the presence of inductive components;
- surge protection.

Inductive loads or loads with high inrush current may require an auxiliary relay, contactor, or suitable protection circuit.

4.5. Input circuits

Model	Number of channels	Input type
W4A Key-24	2	Dry contact, connected to terminal C
W4A Key-230	2	Dry contact, connected to terminal C

Do not apply an external voltage to the input terminals.

4.6. Radio communications

Technology	Characteristics
Bluetooth	Bluetooth Low Energy 5, compatible with Bluetooth Low Energy 4.2 devices or later.
Wi-Fi	2.4 GHz, IEEE 802.11 b/g/n
Bluetooth frequency band	2402 MHz to 2480 MHz
Maximum Bluetooth power	+9 dBm
Wi-Fi frequency band	2412 MHz to 2472 MHz
Maximum Wi-Fi power	18 dBm
Bluetooth range	Up to 150 m in open space under ideal conditions

Actual range depends on obstacles, interference, the mobile device, and network conditions.

4.7. Dimensions and weight

Model	Dimensions	Approximate weight
W4A Key-24	50 × 70 × 38 mm	86 g

W4A Key-230	50 × 70 × 38 mm	86 g
-------------	-----------------	------

4.8. Application limits

The values in this chapter are maximum limits or nominal conditions and must not be taken as recommended values for every installation.

The following are prohibited:

- applying an incompatible supply voltage;
- exceeding the relay contact ratings;
- applying an external voltage to the inputs;
- operating outside the specified temperature range;
- operating outside the specified humidity range;
- using the device in condensing conditions;
- assuming the maximum range applies to every installation;
- treating the enclosure IP rating as a guarantee of protection for the complete installation.

When load, power supply, or environmental characteristics are close to the maximum limits, the Installer must allow a suitable safety margin.

If you are unsure whether the device is suitable for an application, contact W4A or technical support before installation.

5. Planning and electrical installation

5.1. Scope

This chapter describes the planning, mounting, and electrical connection of the W4A Key.

Installation, changes to connections, and commissioning must be carried out only by qualified personnel.

5.2. Checks before installation

Before installing the W4A Key, confirm:

- the exact model designation;
- compatibility with the available power supply;
- compatibility of the circuits to be connected to the outputs;
- compatibility of the contacts to be connected to the inputs;
- the presence of the necessary electrical protective devices;
- the presence of a switching and isolation device;
- the site's environmental conditions;
- the space available for installation and maintenance;
- the cable route and type;
- Bluetooth and Wi-Fi coverage, where applicable;
- the presence of the safety devices required for the controlled load.

Determine the function of each input and output in advance.

5.3. Selecting the installation location

Install the W4A Key on a firm, stable surface suitable for mounting the equipment.

The location must allow:

- access to the enclosure for installation and maintenance;
- proper cable routing and retention;
- opening and closing of the cover;
- visibility of the LED;
- access to the components needed for technical procedures;
- adequate propagation of Bluetooth and Wi-Fi signals.

Where possible, install the equipment:

- away from large metal surfaces;
- away from motors, transformers, and contactors;
- separate from power cables;
- within the coverage area of the Wi-Fi network;
- close to the usual Bluetooth operating area;
- protected against impacts;
- protected against unauthorized tampering.

Avoid installing it:

- inside fully metal enclosures;
- near strong sources of electromagnetic interference;
- in direct sunlight;
- near heat sources;
- in places subject to excessive vibration;
- where water or condensation may accumulate;
- outside the specified environmental limits.

If installation inside a metal enclosure is unavoidable, check communication quality after configuring the device.

5.4. Mounting the enclosure

The enclosure has mounting holes and a cable gland for cable entry.

Before mounting:

1. confirm that the surface is suitable;
2. select fasteners suitable for the surface;
3. check for hidden cables, pipes, or other elements in the drilling area;
4. plan the cable route;
5. allow enough room to open and close the enclosure.

Secure the enclosure using the mounting holes provided.

The mounting must prevent:

- movement of the equipment;
- vibration of the enclosure;
- deformation of the base or cover;
- mechanical stress on the terminals;

- pulling of the cables;
- water entering through the cable gland.

Do not drill additional holes or modify the enclosure without W4A's authorization.

Feed the cables through the existing cable gland.

The diameter and arrangement of the cables must allow:

- proper tightening of the gland;
- mechanical retention;
- sealing of the entry point;
- proper closure of the enclosure.

If the wiring cannot be sealed adequately, use an installation solution compatible with the required protection rating.

5.5. Identifying the components

The arrangement, number, and function of the terminals may vary by model. Before making any connection, confirm that the diagram shown matches the variant stated on the device identification label.



1	Battery	
2	Power supply	AC_IN
3	Button	
4	2 inputs	C IN1 IN2 
	2 outputs	NO1 C1 NO2 C2
6	LED	

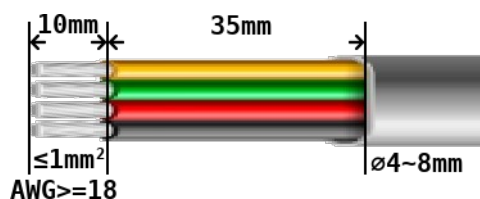
5.6. Preparing and routing the cables

Use cables suitable for:

- the circuit voltage;
- the expected current;
- the installation environment;
- the operating temperature;
- the cable gland;
- the device terminals.

The following cables with the stated dimensions are recommended for the connections:

- O.C. 100 8G0.50;
- O.C. 100 6G0.75;
- 1896/9C;
- or cables with equivalent characteristics suitable for the installation.



The Installer is responsible for the final cable selection.

Prepare the conductors so that:

- no copper is exposed outside the terminals;
- there are no loose strands;
- the insulation does not enter the contact area;
- the conductors are fully inserted;
- the cables do not put stress on the terminals.

Where possible, separate:

- power supply conductors;
- output circuit conductors;
- input conductors;
- other signal cables.

Avoid running signal cables in parallel over long distances with:

- power supply cables;
- motor cables;
- contactor cables;
- high-current cables.

All cables must pass through the gland and be mechanically secured before the enclosure is closed.

5.7. Connecting the power supply

DANGER — Hazardous electrical voltage

Before making the connection:

1. switch off the power supply;

2. isolate the circuit;
3. prevent accidental reconnection;
4. verify the absence of voltage;
5. confirm the W4A Key model;
6. confirm that the available voltage is compatible.

Connect the power supply to the AC_IN terminals. The supply may be AC or DC, within the limits of the model. Polarity is not relevant.

Procedure:

1. identify the power supply conductors;
2. prepare their ends;
3. insert the conductors into the corresponding terminals;
4. tighten the terminals correctly;
5. check for loose strands;
6. pull gently to confirm that the conductors are secure;
7. leave the power supply disconnected until all connections are complete.

Do not connect more than one power source to the device at the same time.

The power supply must have protection and isolation suitable for the installation.

5.8. Connecting the inputs

The inputs are intended for dry contacts.

Examples include:

- buttons;
- switches;
- relay contacts;
- sensor contacts;
- contacts provided by other equipment.

Each input is ON when its terminal is connected to the common terminal.

When the contact is open, the input is OFF.

General procedure:

1. identify the common terminal and input terminal in the diagram;
2. confirm that the external device provides a dry contact;
3. connect the contact between the common terminal and the chosen input;

4. identify the conductors;
5. check that there is no external voltage in the circuit.

CAUTION

Do not apply an external voltage to the input terminals.

Before connecting a contact from another device, confirm that it is a dry, potential-free contact.

If the external device provides a voltage output, use a suitable interface relay.

5.9. Connecting the outputs

The outputs use normally open, potential-free, electrically independent relay contacts.

When an output is OFF, its contact is open.

When an output is ON, its contact is closed.

The contacts do not supply power to the controlled equipment.

The load or control circuit must be powered by a suitable external source.

General procedure:

1. identify the common terminal and normally open output contact in the diagram;
2. check the voltage and current of the external circuit;
3. check that the load type is compatible;
4. connect the external circuit to the appropriate terminals;
5. identify the conductors;
6. confirm that the output limits will not be exceeded.

The common terminals of different outputs are not necessarily connected internally.

Any common connection between circuits must be made externally, and only after electrical compatibility has been confirmed.

5.10. Connecting to an automation input

When the W4A Key controls a gate, barrier, automatic door, or other automation equipment, preferably use a dry-contact control input provided by that equipment.

Before connecting:

1. consult the automation equipment manual;
2. identify the control input;
3. confirm that the input accepts a dry contact;
4. identify the equipment's common terminal;

5. check the recommended command type and duration.

Connect one W4A Key output contact to the automation equipment's control input terminals.

Do not apply an external voltage to an input intended exclusively for a dry contact.

The operation type and duration will be configured later in the application.

5.11. Connecting through an auxiliary relay or contactor

Use an auxiliary relay or contactor when:

- the load is unsuitable for direct connection to the output contact;
- the inrush current is high;
- the load is inductive;
- additional contacts are needed;
- a different contact type is needed;
- the load's utilization category requires it.

In this case, the W4A Key output must control only the coil of the auxiliary relay or contactor.

Select the auxiliary device according to:

- coil voltage;
- coil current;
- load voltage;
- load current;
- load type;
- expected switching frequency.

Where necessary, fit surge protection close to the coil.

5.12. Closing the enclosure

Before closing the enclosure:

- confirm that all connections match the diagram;
- confirm that the terminals are tight;
- check for loose conductors;
- check that no copper is exposed;
- arrange the cables inside;
- confirm that cables do not press on components;
- confirm that every cable passes through the gland;

- tighten the gland correctly;
- check the condition of the seal;
- confirm that no cable is caught between the cover and the base.

Close the cover evenly.

An incorrectly closed enclosure or improperly tightened gland can compromise the equipment's protection rating.

5.13. Final connection checks

Before powering the device, confirm:

- the correct model;
- a compatible supply voltage;
- the power supply is connected to the correct terminals;
- no external voltage is applied to the inputs;
- dry contacts are connected correctly;
- output circuits are connected correctly;
- loads are within the permitted limits;
- auxiliary relays or contactors are fitted where needed;
- electrical protective devices are installed;
- the terminals are tight;
- there are no loose strands;
- there are no short circuits;
- the gland secures the cables correctly;
- the enclosure is properly closed;
- the controlled load is in a safe state.

Do not switch on the power supply if there is any doubt about the connections.

5.14. First power-up

The first power-up is intended only to check that the device starts correctly and is available for pairing through the application.

Do not test the operation of inputs, outputs, or controlled loads at this stage.

Before switching on the power supply:

1. put the controlled equipment in a safe state;

2. prevent unexpected movement;
3. keep people, animals, and objects away from hazardous areas;
4. confirm that the connections have been checked;
5. make sure the power supply can be switched off quickly.

Switch on the power supply and check:

- that the device starts;
- that protective devices do not trip;
- that there is no abnormal heating;
- that there is no burning smell;
- that there is no unusual electrical noise;
- that no load is activated unexpectedly;
- that the device is available for pairing in the application.

Switch off the power supply immediately if any abnormal operation is detected.

6. Indicators and service controls

6.1. LED

The W4A Key has a blue LED that provides information about device status.

Interpretation of the indicator depends on the current operating mode.

Active connection to the application

When a user is connected to the device through the application, the LED remains on.

Factory data reset mode

When the device enters factory data reset mode, the LED flashes slowly.

In this mode, pressing the button can confirm the reset and delete the data and settings stored on the device.

See Chapter 23 Factory data reset before carrying out this procedure.

Error mode

When the LED flashes rapidly, the device is in error mode.

Normal operation may be unavailable in this state.

Perform the checks described in Chapter 22 Troubleshooting.

If the error cannot be resolved through normal procedures, a factory data reset may be necessary.

6.2. Device button

The button on the W4A Key is intended for technical and service procedures.

Depending on the device's status, it can be used to:

- confirm a factory data reset;
- start or finish recovery procedures;
- cancel certain technical procedures, where provided;
- perform other functions expressly described in this manual.

The button is not intended for normal output control or everyday use.

CAUTION

Before pressing the button, confirm:

- the LED status;
- the procedure in progress;

- the consequences of the operation;
- whether a copy or record of the required settings exists.

6.3. Indicator summary

Indicator status	Meaning
Off	The LED does not indicate an active connection, or the device may have no power
Steady blue	A user is connected to the device through the application
Slowly flashing blue	Factory data reset mode
Rapidly flashing blue	Error mode or technical procedure in progress, depending on the context

7. Installing the application

7.1. Purpose

The application lets you configure, monitor, and manage the W4A Key, according to the functions available for the model, firmware version, and user account.

The application does not replace physical controls, protective devices, electrical isolation, or the installation's safety procedures.

7.2. Mobile device requirements

Before installation, check that the mobile device meets the minimum requirements set by W4A.

Requirements may include:

- a compatible operating system;
- a minimum operating system version;
- Bluetooth Low Energy;
- available storage space;
- Bluetooth permissions;
- a valid account in the app store;
- a compatible screen and resolution.

Requirements may change in future versions of the application.

Consult the latest information provided by W4A or the official app store.

7.3. Compatible operating systems and platforms

The W4A Key application is available for the following operating systems:

Operating system	Minimum compatible version
Android	8.0
iOS	15

The W4A Key application is compatible with Android Auto and Apple CarPlay, providing access to selected functions through compatible vehicle infotainment systems.

Availability depends on the application version, the mobile device operating system, the availability of Android Auto or Apple CarPlay, and the compatibility of the vehicle or infotainment system.

Commands shown in the vehicle are those in the application's In Car list. They can be added manually by the profile or made available automatically through the operation settings. See 11.3 Operation parameters and 18.3 Using Android Auto and Apple CarPlay.

Screen appearance and the location of some options may vary according to:

- the operating system;
- the application version;
- the mobile device manufacturer;
- the screen size;
- the selected language.

7.4. Installing the application

Install the application only through the official channels indicated by W4A.

Android

1. open Google Play;
2. search for W4A Key;
3. confirm that the listed developer is W4A or an officially authorized entity;
4. select Install;
5. wait for installation to finish.

iOS

1. open the App Store;
2. search for W4A Key;
3. confirm that the listed developer is W4A or an officially authorized entity;
4. select Get;
5. wait for installation to finish.

Do not install versions obtained from unauthorized websites, files, or stores.

7.5. Required permissions

During installation or first use, the application may request permissions needed to operate.

Depending on the operating system and application version, it may request permission for:

- Bluetooth;
- nearby devices;
- location;
- local network access;
- storage, where applicable.

Grant only the permissions required and requested by the official application.

Refusing certain permissions may prevent:

- detection of the W4A Key;
- pairing via Bluetooth;
- access to the local network.

Certain Android versions may require location permission to detect Bluetooth devices, even if the application does not use location to track the user.

7.6. Preparing Bluetooth

Before pairing the W4A Key:

- enable Bluetooth on the mobile device;
- keep the mobile device near the W4A Key;
- confirm that the application has permission to use Bluetooth;
- confirm that the W4A Key has power;
- avoid metal obstacles between the mobile device and the equipment;
- close other applications that may be using Bluetooth heavily if problems occur.

Do not pair directly from the operating system's Bluetooth settings unless W4A expressly instructs you to do so.

Start pairing from the application.

7.7. Updating the application

Keep the application up to date through the official app store.

Updates may include:

- bug fixes;
- security improvements;
- compatibility with new firmware versions;
- interface changes;
- new features;
- changes to minimum requirements.

Before updating, confirm that you have the credentials needed to sign in again.

After updating, check:

- the device list;

- permissions;
- access to the functions you use.

7.8. General configuration rules

Unless otherwise stated, to view or change W4A Key data:

1. open the menu for the relevant profile type;
2. select the desired profile or device;
3. connect to the device;
4. open the indicated tab;
5. make the changes;
6. press Submit, Save, or the equivalent option;
7. keep the connection active until confirmation appears.

Do not consider changes complete until the application confirms that they have been saved.

During data transfer:

- do not switch off the power supply;
- do not close the application;
- do not interrupt communication;
- do not start another procedure.

The available options may vary by profile, permissions, firmware, and application version.

8. Operating concepts

8.1. Inputs, outputs, operations, and commands

The W4A Key works through the relationship between inputs, outputs, operations, and commands.

Inputs receive signals from external contacts, such as compatible buttons, switches, relays, or sensors.

Outputs are relay contacts used to control external circuits.

An operation defines the action performed by the device, including:

- the output used;
- the actuation type;
- the duration;
- the delay;
- applicable restrictions;
- the possible execution of another operation.

A command is an element shown in the application that lets the user execute an operation.

The Installer configures the inputs, outputs, and operations.

8.2. Actuation types

An operation can use the following actuation types:

Bistable

Each execution changes the output state.

If the output is OFF, it switches ON. If it is ON, it switches OFF.

ON pulse in seconds

The output switches ON for the configured time and automatically returns to OFF.

ON pulse in milliseconds

Similar to a pulse in seconds, but intended for short-duration actions.

Press and hold

The output remains active while the command is pressed and is deactivated when it is released or communication ends.

Stop

Stops an ongoing actuation or sequence, where applicable.

The actuation type must suit the equipment being controlled.

8.3. Duration, delay, and sequences

Duration determines how long the output remains active for timed actuation types.

Delay determines the interval between executing an operation and the start of actuation.

An operation can execute another operation:

- at the same time;
- after it finishes;
- according to the configured sequence.

Sequences allow combined behaviors, but the Installer must test them before use.

An incorrect sequence can cause unexpected or incompatible actuation.

8.4. Interlocking and input priority

Interlocking can prevent both outputs from being active simultaneously.

Depending on the configuration, activating one output may deactivate the other.

Interlocking configured in the W4A Key does not replace independent electrical or mechanical protective measures where these are needed.

Inputs can take priority over commands executed through the application.

An input can, for example:

- activate an operation;
- prevent actuation;
- deactivate an output;
- interrupt an ongoing operation.

The Installer defines input behavior.

8.5. Restricted operations and schedules

An operation can be marked as restricted.

Only profiles authorized to use restricted operations can execute it.

An operating schedule can also be defined for an operation.

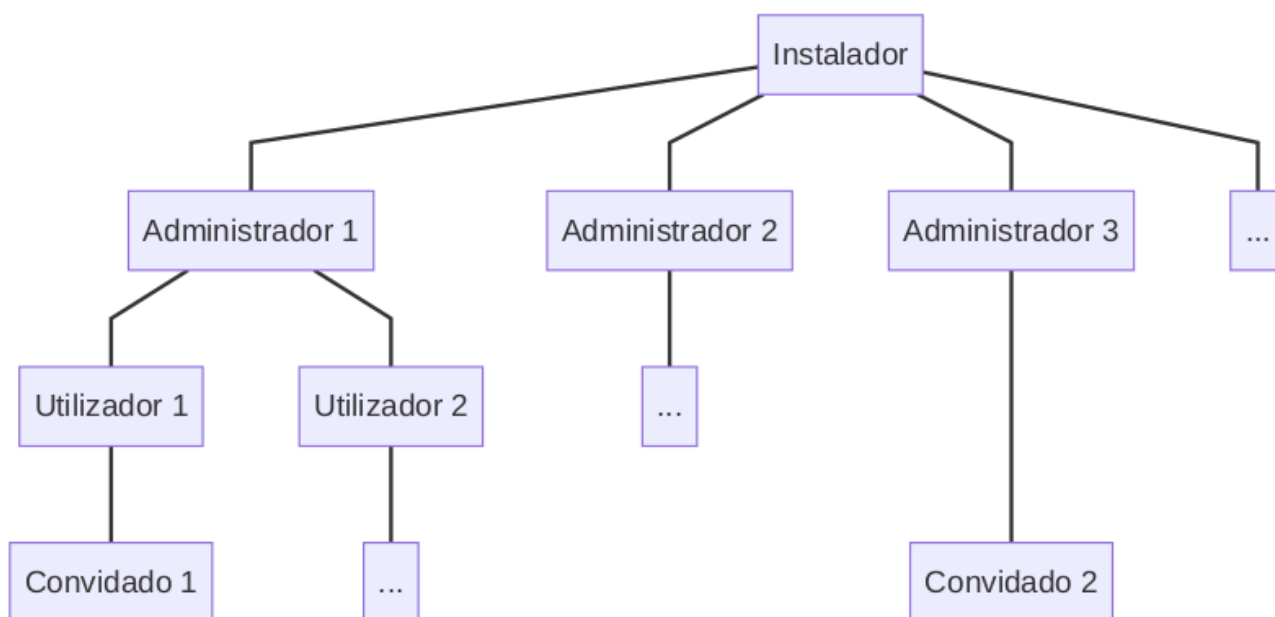
Outside that schedule, the operation is unavailable even if the profile has access to the device.

Operation restrictions are independent of the restrictions assigned to a profile.

8.6. Profiles, hierarchy, and dependents

The W4A Key uses a hierarchy of profiles:

- Installer;
- Administrator;
- User;
- Guest.



The Installer creates Administrators.

Administrators can create Users and Guests.

Users can create Guests when authorized.

A profile created by another profile is called a dependent.

The creating profile can manage its dependents within its assigned permissions.

A profile cannot grant dependents permissions greater than its own.

8.7. Profile restrictions

A profile can be subject to:

- a start date;
- an end date;
- daily schedules;
- a maximum number of accesses;

- permission to use restricted operations;
- a limit on dependent profiles;
- a minimum traceability type.

When the maximum number of accesses is reached, the profile can no longer execute the affected operations.

The creating profile sets restrictions for dependents, subject to its own permissions.

8.8. Counting accesses

A Guest profile can be configured with a maximum number of accesses.

An access is counted only when the profile executes an operation for which the Access counting option is enabled.

Operations without this option do not reduce the number of remaining accesses.

Only one access is counted per connection to the device. Thus, if the user repeatedly performs one or more access-counted operations without ending the connection, only one access is deducted.

A new access is counted after the connection ends and the profile reconnects to execute an access-counted operation.

Example:

1. the profile has five accesses available;
2. it connects to the W4A Key;
3. it executes an access-counted operation three times;
4. it ends the connection.

In this case, only one access is counted, leaving four accesses available.

When the limit is reached, the profile can no longer execute operations subject to access counting.

Operations that actually represent a passage or entry, such as opening a door, gate, barrier, or turnstile, should be configured to count accesses.

Operations such as lighting, stopping, maintenance, or auxiliary commands should not normally count accesses.

8.9. Traceability, credentials, and sessions

Traceability determines the level of identification associated with a profile's actions.

Depending on the type configured, records may:

- identify the profile;
- show only that an actuation occurred;
- limit information available to higher-level profiles.

Credentials authenticate a profile and may include:

- a name or ID;
- a password;
- pairing text;
- a file;
- a QR code.

The session temporarily keeps the profile authenticated in the application.

After the maximum inactivity period, the password may need to be entered again.

A session is different from an active connection to the device.

The connection exists only while the application is actually communicating via Bluetooth, Wi-Fi, or the Internet.

8.10. Communication methods

The W4A Key can communicate via:

Bluetooth

Used for local communication and initial configuration.

Local Wi-Fi

Allows communication over the configured local network.

Remote communication

Allows access to the device over the Internet when the service is active and authorized.

Offline mode

Allows certain actions to be prepared in a file and executed later near the device.

Each method's availability depends on configuration, permissions, and associated services.

8.11. History and records

The device can store records relating to:

- actuations;
- profile creation;
- profile deletion;
- other management events.

Available information depends on:

- the profile type;
- the hierarchy;
- the configured traceability;
- the records stored on the device.

The Installer can view the complete actuation history, but without identifying the profiles that performed the actions.

History is intended for system review and management and does not replace certified surveillance, time-and-attendance, or access control systems.

9. Initial pairing and setup

9.1. Purpose and prerequisites

This chapter describes initial pairing of the W4A Key with the application and creation of the Installer profile.

Initial pairing lets you:

- identify the device in the application;
- create Installer credentials;
- give the equipment a name;
- establish the first connection;
- access the configuration area.

Complete this procedure after:

- finishing the electrical installation;
- checking the connections;
- powering up for the first time;
- installing the application;
- granting the required permissions.

Before starting, confirm:

- the W4A Key has power;
- there is no indication of abnormal operation;
- the device has not yet been configured;
- the phone's Bluetooth is enabled;
- the application is installed and up to date;
- the phone is near the device.

During pairing:

- keep the phone near the W4A Key;
- do not switch off the power supply;
- do not close the application;
- do not interrupt communication;
- do not press the device button unless expressly instructed to do so.

9.2. Starting installation in the application

To start pairing:

1. open the W4A Key application;
2. open the Installer menu;
3. select the option to add a new Installer;
4. choose Install new device;
5. wait while the application searches for nearby devices.

When the application is opened for the first time, the Install new device option may appear immediately.



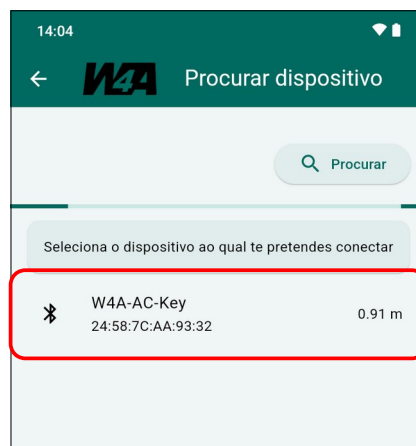
9.3. Selecting the device

The application shows devices within Bluetooth range that have not yet been configured.

If more than one device appears:

- stay near the desired equipment;
- compare the identifiers shown;
- confirm that the identifier matches the installed device;
- select only the equipment you intend to configure.

Do not proceed if you are unsure which device it is.



9.4. Creating the Installer profile

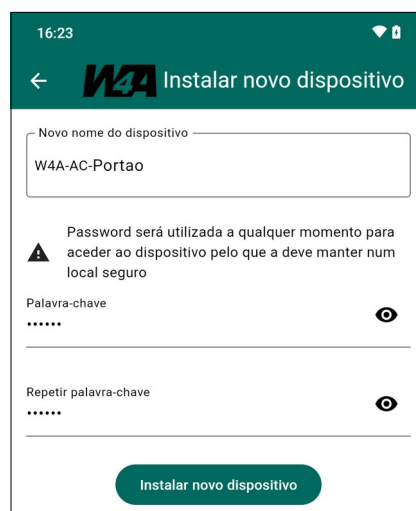
During setup, the application requests:

- a name for the device;
- an Installer password;
- confirmation of the password.

Choose a clear name related to the location or function of the equipment.

Examples:

- Main gate;
- Warehouse entrance;
- Garage door;
- North barrier.



The password must:

- be difficult to guess;
- meet the stated minimum length;
- not be reused for other services;
- not be shared with ordinary users;
- be kept in a secure place.

CAUTION

Losing the Installer password may require a factory data reset.

9.5. Completing and verifying pairing

After entering the details:

1. confirm the device name;
2. confirm the password;
3. select Install new device or the equivalent option;
4. keep the phone near the equipment;
5. wait for the initial settings to be transferred;
6. do not switch off the power supply;
7. do not close the application.

When pairing succeeds, the device appears in the Installer menu.

After completion, confirm:

- the displayed name is correct;
- the device appears in the Installer list;
- its section can be opened;
- the profile shown is of the Installer type;
- communication is established;
- no error messages appear;
- basic device information can be viewed.

Protect Installer credentials and make them available only to authorized persons.

9.6. Troubleshooting pairing

Pairing may fail because of:

- Bluetooth being disabled;

- permissions not being granted;
- excessive distance;
- interference;
- the device already being configured;
- an active connection on another phone;
- a power interruption;
- the application being closed;
- a communication error;
- incompatibility between the application and firmware.

If pairing does not finish:

1. leave the device powered;
2. move the phone closer;
3. check Bluetooth;
4. check permissions;
5. close and reopen the search;
6. repeat the procedure;
7. check whether the device still appears as unconfigured.

Do not perform a factory data reset as a first step.

Consider a reset only when:

- the device was only partially configured;
- pairing cannot be resumed;
- sign-in is impossible;
- the procedure is recommended in Chapter 23 Factory data reset.

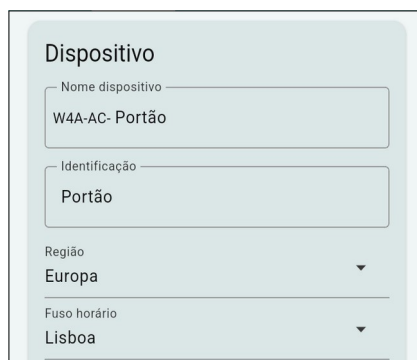
After completing pairing, proceed to Chapter 10 Configuring the device.

10. Configuring the device

In the Installer menu, select the device and open the Device tab.

10.1. Identification and general settings

The general settings area contains options for identifying the W4A Key and adapting its operation to the installation.



The screenshot shows a configuration window titled 'Dispositivo'. It contains four input fields: 'Nome dispositivo' with the text 'W4A-AC- Portão', 'Identificação' with the text 'Portão', 'Região' with a dropdown menu showing 'Europa', and 'Fuso horário' with a dropdown menu showing 'Lisboa'.

Device name

The device name is used during communications and distinguishes the W4A Key from nearby equipment.

Choose a name that is:

- short;
- clear;
- related to its location or function;
- different from the names of other devices.

Identification in the application

Identification lets you customize the name shown in the application.

It can add information such as:

- building;
- floor;
- area;
- function;
- internal reference.

The name used in the application does not replace the technical identification on the product label.

Region and time zone

The region and time zone are used by functions that depend on the date and time.

These settings affect:

- profile validity periods;
- time restrictions;
- operation schedules;
- records;
- chronological display of history.

Select the region and time zone corresponding to the installation location.

After changing these settings, check the date and time shown in the information area.

Incorrect settings may prevent time-restricted operations or profiles from working.

10.2. Sessions and connections

The W4A Key lets you set time limits related to profile authentication and communication.

Tempo máximo de sessão	03d
Tempo máximo de conexão	04m
Tempo máximo de conexão sem interação	30s

Maximum session duration

The maximum session duration determines how long a profile remains authenticated without requiring the password to be entered again.

When the session expires:

- the profile still exists;
- settings are not deleted;
- the password may need to be entered again at the next connection.

A longer period makes everyday use easier but extends the time during which the session remains valid on the phone.

A shorter period requires more frequent authentication.

The Installer must choose a value appropriate to the installation's required security level.

Maximum connection duration

The maximum connection duration limits how long a profile can remain continuously connected to the device.

When the limit is reached, the W4A Key ends the connection so that other communications can take place.

Ending a connection does not necessarily end the session.

Maximum idle connection duration

This setting determines how long a connection can remain active without communication or interaction.

When the period expires, the device ends the connection.

This reduces the time during which an idle connection can prevent or delay another user's access.

When setting these limits, consider:

- the expected number of users;
- the communication method;
- the usual duration of operations;
- the need for frequent access;
- the desired security level.

10.3. Configuring Wi-Fi communication

By default, the device can be used via Bluetooth.

Enable Wi-Fi communication if you want to:

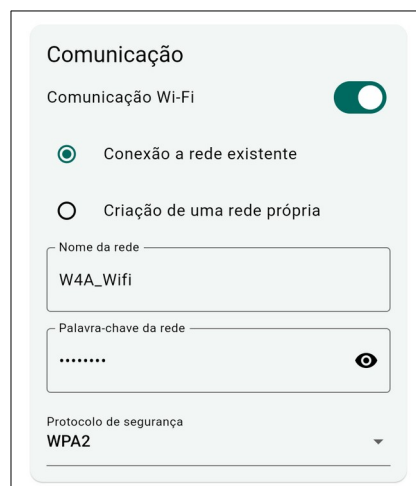
- use the W4A Key over the local network;
- allow simultaneous access by several users, when supported;
- use remote communication over the Internet;
- reduce reliance on Bluetooth proximity.

Connecting to an existing network

This is the recommended mode when a Wi-Fi network is available on site.

To configure it:

1. enable Wi-Fi communication;
2. choose to connect to an existing network;
3. enter or select the network name;
4. enter the password;
5. select the security protocol if prompted;
6. confirm the details;



The screenshot shows a 'Comunicação' (Communication) settings screen. At the top, there is a toggle switch for 'Comunicação Wi-Fi' which is turned on. Below this, there are two radio button options: 'Conexão a rede existente' (selected) and 'Criação de uma rede própria' (not selected). Under the selected option, there are two input fields: 'Nome da rede' (Network name) with the text 'W4A_Wifi' and 'Palavra-chave da rede' (Network password) with a masked password '.....'. At the bottom, there is a dropdown menu for 'Protocolo de segurança' (Security protocol) with 'WPA2' selected.

7. submit the settings to the device.

Enter the network name and password exactly as set on the router.

Passwords may be case-sensitive.

After saving, wait while the device attempts to connect.

Creating a network with the device

If no Wi-Fi network is available, the W4A Key can create its own network.

Use this mode only when needed.

When configuring a device-hosted network:

- choose an identifiable name;
- use a strong password;
- avoid credentials that are easy to guess;
- limit the distribution of network details;
- check the range at the place of use.

Creating its own network does not guarantee Internet access or remote communication.

Checking the Wi-Fi connection

After submitting the settings, confirm:

- the device indicates that it is connected to the network;
- the selected network is correct;
- there is no error message;
- you can communicate with the device again;
- the connection remains stable.

If the connection fails, check:

- the network name;
- the password;
- signal strength;
- the security protocol;
- router availability;
- network filters or restrictions.

10.4. Remote communication

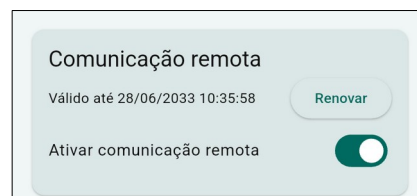
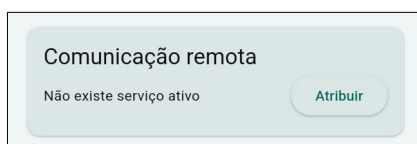
Remote communication lets you access the W4A Key over the Internet without the phone being near the device or connected to the same local network.

This function may depend on:

- a subscription;
- an activation key;
- the W4A Key's Internet connection;
- the phone's Internet connection;
- service availability;
- the firmware and application versions.

To enable remote communication:

1. confirm that Wi-Fi communication is enabled;
2. confirm that the device has Internet access;
3. enter or assign the service key, where applicable;
4. wait for validation;
5. enable Remote communication;
6. submit the settings;
7. check the service status.



Remote communication can be temporarily disabled without deleting the other settings.

WARNING — Operation without direct observation

Before executing an operation remotely, confirm that the area around the controlled load is safe.

Do not use remote communication if you cannot ensure that the operation will not endanger people, animals, or property.

Unavailability of remote communication does not mean that:

- the device is switched off;
- local operations are disabled;
- the inputs have stopped working;
- the load is electrically isolated.

10.5. General output settings

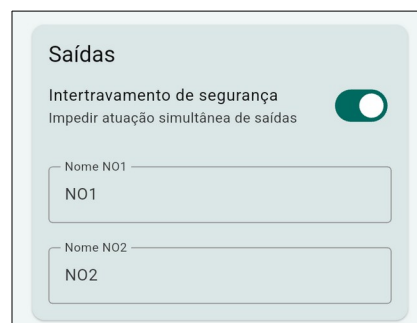
In the output area, the Installer can set common properties used by operations.

Output name

Assign a name that clearly identifies the function of the connected circuit.

Examples:

- Open gate;
- Lock;
- Lighting;
- Raise shutter;
- Lower shutter;
- Auxiliary relay.



Saídas

Intertravamento de segurança ☒

Impedir atuação simultânea de saídas

Nome N01
N01

Nome N02
N02

The output name helps prevent the wrong output being selected when creating operations.

Interlocking

When available, interlocking prevents incompatible outputs from remaining active at the same time.

If one output is active and another is triggered, the device may deactivate the first before activating the second.

This function may be suitable for:

- raising and lowering;
- opening and closing;
- commands for opposite directions;
- circuits that must not operate simultaneously.

Before enabling interlocking:

- confirm the intended behavior;
- check the electrical installation;
- check whether external interlocks are present;
- consider whether a pause is needed;
- test all combinations during commissioning.

Interlocking configured in the W4A Key does not replace mandatory electrical or mechanical protective measures.

The output selection and actuation type are set later for each operation.

10.6. General input settings

Each input can be assigned a name and function.

Choose a name related to the connected external contact.

Examples:

- Inside button;
- Door sensor;
- Limit switch;
- External lockout;
- Authorization;
- Local control.

Operating modes may include:

Disabled

The input takes no action when its state changes.

Use this mode when:

- the input is not connected;
- its function has not yet been configured;
- you want to suspend its use temporarily.

Execute an operation

A change in the input state executes a selected operation.

This mode can be used with:

- buttons;
- switches;
- relay contacts;
- commands from other equipment.

The operation must exist before it can be assigned to the input.

If it has not yet been created, complete operation configuration first.

Prevent actuation when ON

When the input is ON, the selected or affected operations are blocked.

This mode can be used, for example, when a contact indicates that a lockout condition is present.

Prevent actuation when OFF

When the input is OFF, the selected or affected operations are blocked.

This mode can be used when an external authorization must remain active to permit operation.

Input priority

Actuations initiated by inputs may take priority over commands executed from the application.

Behavior depends on:

- the assigned operation;
- the actuation type;
- interlocking;
- the current output states;
- other ongoing operations.

After configuring the inputs, the Installer must test each state individually and all relevant interactions.

11. Configuring operations

Operations define what the W4A Key does when it receives a command from the application, an input, a peripheral, or another operation.

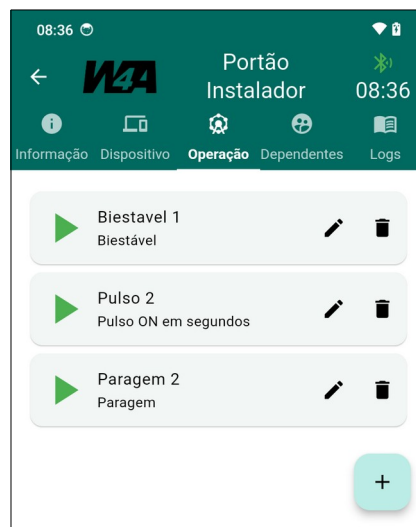
Only the Installer profile may configure operations.

In the Installer menu, select the device and open the Operations tab.

11.1. Accessing operation settings

To open the operations area:

1. open the Installer menu;
2. select the device;
3. connect to it;
4. open the Operations tab;
5. view the list of existing operations.



11.2. Creating an operation

To create a new operation:

1. open the Operations tab;
2. select the option to add an operation;
3. complete the displayed settings;
4. set the applicable permissions and restrictions;
5. review the settings;
6. save or submit the operation.

Available settings depend on the selected actuation type and application version.

11.3. Operation parameters

Operation settings may include the following parameters:

Name

Enter a short, clear name identifying the function performed.

Examples:

- Open gate;
- Close gate;

- Open door;
- Turn on lighting;
- Raise shutter;
- Lower shutter;
- Stop shutter.

Avoid ambiguous names, especially when several operations are similar.

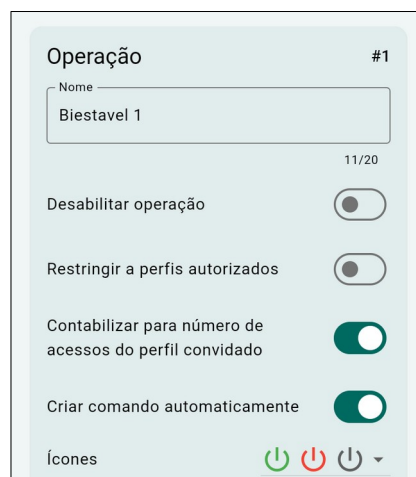
Operation status

An operation can be active or inactive.

When inactive, it:

- remains stored;
- can be edited by the Installer;
- cannot be executed by users.

This option temporarily suspends a function without deleting its settings.



Restricted operation

When enabled, only profiles authorized to use restricted operations can execute the operation.

Use this setting for functions that must not be available to every user, such as:

- access to technical areas;
- permanent release;
- maintenance operations;
- reserved commands;
- functions with a significant effect on the installation.

Permission to use restricted operations is assigned in each profile's settings, as described in Chapter 13 Managing Administrators.

Access counting

When enabled, executing the operation can count toward the access limit of a profile subject to that restriction.

Enable this option only for operations that should count as an access for the configured limit.

It is not recommended for functions such as:

- lighting;
- stopping;

- auxiliary commands;
- maintenance operations.

Access counting is described in Section 8.8 Counting accesses.

Automatic command creation

When enabled, the application automatically creates a command linked to the operation.

This command can be made available to authorized profiles and shown on the control screen.

Automatic creation may include selecting:

- an icon for the OFF state;
- an icon for the ON state.

The automatically created command can later be:

- edited;
- renamed;
- rearranged;
- moved to another group;
- deleted from the application.

Deleting the command does not necessarily delete the operation stored on the device.

Automatically making a command available in the car

When Automatic command creation is enabled, you can also make the command available in the car automatically.

When enabled, the command automatically created in the application for authorized profiles is also added to their In Car list, making it available for display in the vehicle.

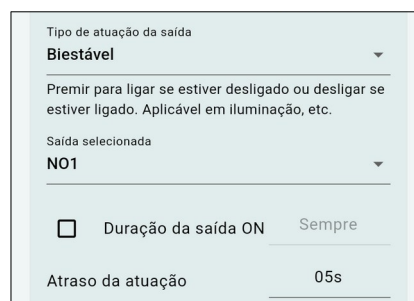
A profile can later remove the command from the In Car list if it should not be available in the vehicle. Removing it from the list does not delete it from the application.

Output

Select the output connected to the circuit to be controlled.

Before proceeding, confirm:

- the output corresponds to the intended equipment;
- the electrical installation is correct;
- the load is compatible;
- there is no risk of unintended operation.



The screenshot shows a configuration screen for an output. At the top, there is a dropdown menu labeled 'Tipo de atuação da saída' with the selected option 'Biestável'. Below this is a text instruction: 'Premir para ligar se estiver desligado ou desligar se estiver ligado. Aplicável em iluminação, etc.'. Underneath is another dropdown menu labeled 'Saída selecionada' with the selected option 'NO1'. Further down, there is a checkbox labeled 'Duração da saída ON' which is currently unchecked, with the value 'Sempre' displayed to its right. At the bottom, there is a field labeled 'Atraso da atuação' with the value '05s'.

Actuation type

Select the desired output behavior.

Available types may include:

- bistable;
- ON pulse in seconds;
- ON pulse in milliseconds;
- press and hold;
- stop.

See Section 8.2 Actuation types for the behavior of each option.

An incorrect selection can result in:

- the output remaining ON unintentionally;
- a pulse that is too short;
- a pulse that is too long;
- behavior other than expected;
- actuation incompatible with the load.

Duration

Where applicable, enter the period for which the output must remain active.

Duration may represent:

- the length of a pulse;
- the maximum time in the ON state;
- the period before automatically returning to OFF.

Do not use durations longer than those recommended by the manufacturer of the controlled equipment.

Delay

Delay is the time between accepting the operation and starting the actuation.

It can be used to:

- create a timed sequence;
- allow another action to finish;
- wait before activation.

Inform users when an operation has a delay to prevent them from unnecessarily repeating the command.

Next operation

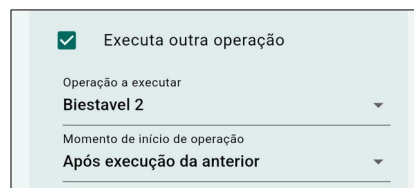
Where available, an operation can start another operation:

- at the same time;
- after it has finished.

Before creating a sequence:

- confirm the intended order;
- check its interaction with interlocking;
- avoid circular sequences;
- test the complete behavior.

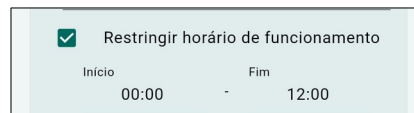
Do not configure an operation to start itself, directly or indirectly.



Operating schedule

Where applicable, define when the operation can be executed.

Outside the permitted schedule, the operation is refused.



11.4. Editing, disabling, or deleting an operation

To change an existing operation:

1. select it in the list;
2. open the edit option;
3. change the required settings;
4. review the effects;
5. submit the settings again.

Before changing an operation already used by profiles, inputs, peripherals, or sequences, check all dependencies.

A change can affect:

- existing commands;
- peripherals;
- sequences;
- behavior familiar to users.

Disable an operation when you want to suspend its use temporarily.

Delete it only when it is no longer needed.

Before deleting it, check that it is not linked to:

- commands;
- inputs;
- peripherals;
- other operations;
- profiles;
- safety procedures.

11.5. Testing an operation

Test only after configuration is complete and the installation is in a safe state.

Before testing:

- move people, animals, and objects away from the moving area;
- confirm that the load can be operated safely;
- confirm that safety devices are active;
- verify that the operation corresponds to the intended load.

Test each of the following separately:

- state change;
- duration;
- return to OFF;
- interlocking;
- sequence with other operations;
- blocking by inputs.

If behavior differs from what was expected:

1. stop using it;
2. put the installation in a safe state;
3. review the operation;
4. check the general settings;
5. repeat the test.

Make the operation available to users only after it has been validated during commissioning.

12. Testing and commissioning

12.1. Preparation

Carry out tests after completing:

- the electrical installation;
- device configuration;
- input and output configuration;
- creation of operations.

Before starting:

1. put the installation in a safe state;
2. keep people, animals, and objects away from moving areas;
3. confirm that the power supply can be switched off quickly;
4. check that there are no error messages;
5. confirm that you are connected to the correct device.

12.2. Testing inputs and outputs

Test every configured input individually.

Confirm that:

- the state shown in the application matches the external contact state;
- the input executes or blocks the configured function;
- there are no unexpected changes of state.

Then test each output using an appropriate operation.

Confirm that:

- the correct output is activated;
- the load responds as expected;
- the output returns to the expected state;
- the duration and delay are correct;
- interlocking works where configured.

Stop the test if you observe unexpected behavior.

12.3. Testing operations and access

Test all configured operations and confirm:

- the actuation type;
- the duration;
- the delay;
- sequences between operations;
- restricted operations;
- schedule restrictions;
- access counting.

If different profile types exist, confirm that each profile can use only the operations for which it is authorized.

12.4. Completing commissioning

The installation can be put into service when:

- all inputs work correctly;
- all outputs control the intended load;
- all operations behave as configured;
- permissions and restrictions are enforced;
- the required communication methods are working;
- there are no error messages;
- the installation is in a safe state.

Before handing over the system, the Installer must:

- create a suitable profile for the person responsible;
- explain the available commands;
- explain how operations behave;
- explain the existing restrictions;
- provide the manual.

Do not use Installer profile credentials for everyday operation of the device.

13. Managing Administrators

The Installer profile can create Administrator profiles to allow use of the device and management of other profiles.

Depending on the assigned permissions, an Administrator can:

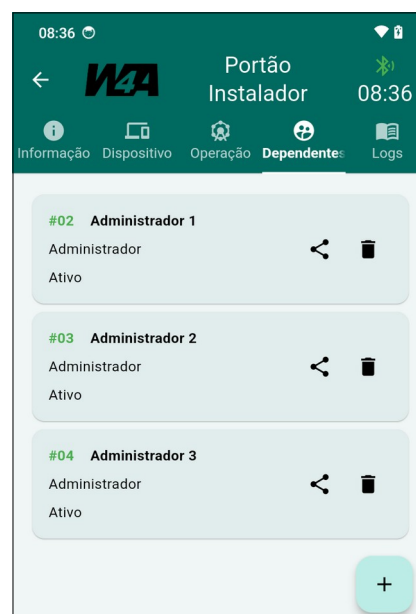
- execute operations;
- create User and Guest profiles;
- assign restrictions to dependents;
- view available records;
- manage their own access details.

Do not use Installer profile credentials for everyday operation of the device.

13.1. Creating an Administrator

To create an Administrator:

1. open the Installer menu;
2. select the device;
3. connect to it;
4. open the Dependents tab;
5. select the option to add a profile;
6. complete the displayed settings;
7. save or submit the settings.



13.2. Administrator parameters

The settings may include:

Name

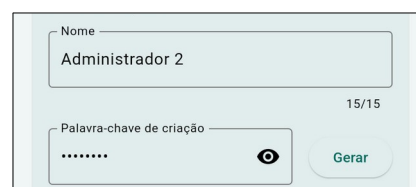
Enter a name that identifies the Administrator.

Password

Set an initial password for pairing the profile with the application.

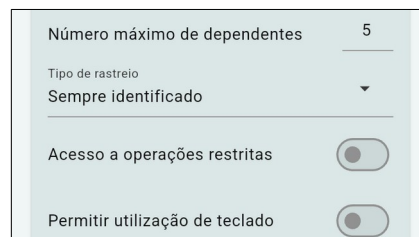
Share the password only with the authorized person, using a secure method.

The Administrator can change it later when that function is available.



Maximum number of dependents

Sets the maximum number of profiles the Administrator can create.



Número máximo de dependentes	5
Tipo de rastreio	Sempre identificado
Acesso a operações restritas	☒
Permitir utilização de teclado	☒

Minimum traceability

Sets the minimum level of identification required for the Administrator and their dependents.

See Section 8.9 Traceability, credentials, and sessions.

Restricted operations

When enabled, the Administrator can execute operations classified as restricted.

Grant this permission only when needed.

Use of peripherals

Where applicable, determines whether the Administrator can use peripherals associated with the device.

13.3. Sharing the profile

After creating the Administrator, the application may allow pairing details to be shared as:

- text;
- a QR code;
- a file;
- another method available in the application.

Share the details only with the authorized person.

Do not publish access details, send them to groups, or store them where third parties can access them.

13.4. Editing or deleting an Administrator

To change an Administrator:

1. open the Dependents tab;
2. select the profile;
3. change its settings;
4. save or submit the changes.

Changes can affect:

- available operations;

- creation of new dependents;
- access to restricted operations;
- use of peripherals;
- access to records.

Delete an Administrator profile when that person no longer needs access.

Before deleting it, confirm that you selected the right person.

Deleting the profile may also affect dependent profiles created by that Administrator.

13.5. Verification

After creating or changing an Administrator, confirm:

- the profile appears in the dependent list;
- the name is correct;
- the assigned permissions are appropriate;
- the pairing details were given to the right person;
- the profile can sign in;
- only authorized functions are available.

The Administrator must pair the profile with their application using the procedure described in the next chapter.

14. Pairing a user profile

This procedure applies to:

- Administrator;
- User;
- Guest profiles.

Before starting, confirm:

- you have received the access details;
- the application is installed;
- Bluetooth is enabled;
- the phone is near the device if pairing locally.

14.1. Signing in and pairing the profile

Signing in links a profile already created on the W4A Key to the application.

The profile can be paired using:

- access credentials;
- text;
- a file;
- a QR code.

To start:

1. open the application;
2. open the Add menu;

or:

1. open the Profile menu;
2. select the + button;
3. open Add profile.

Select the method corresponding to the information you received.

Access credentials

Use this method if you are given:

- the profile name or identifier;
- the password.

To pair the profile:

Pairing a user profile

1. select Sign in;
2. wait while nearby devices are searched;
3. select the desired W4A Key;
4. enter the profile name or identifier;
5. enter the password;
6. confirm sign-in.

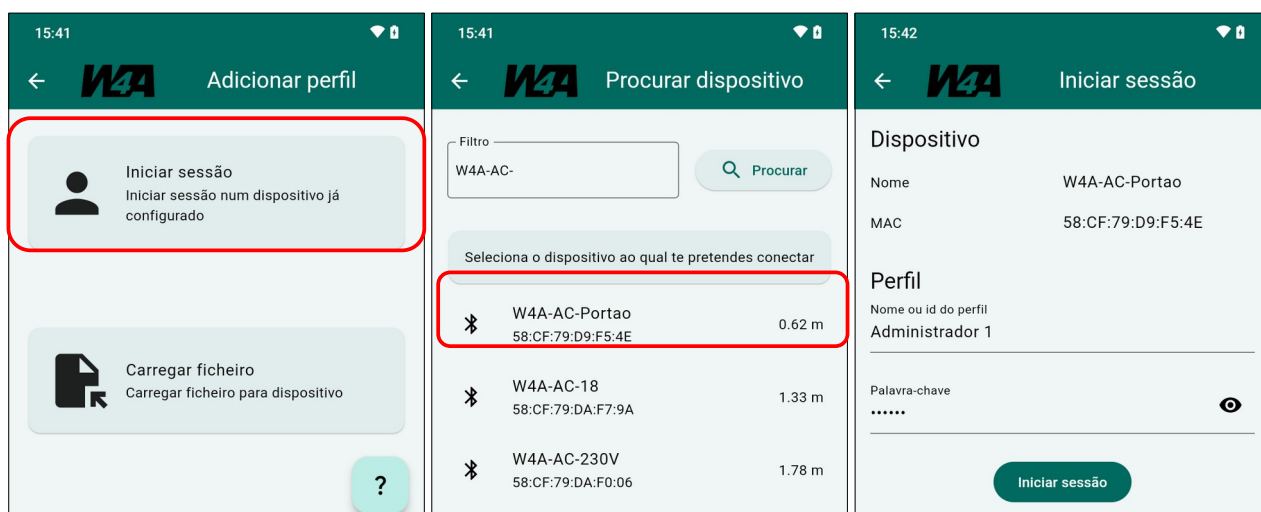
Identification can use:

- **Profile name;**
- **Profile ID.**

The device assigns the ID automatically when the profile is created.

The person who created the profile can find its ID in the dependents list.

If several devices are nearby, confirm that you selected the correct W4A Key before entering credentials.



Text

Use this method when pairing details are provided in a text message.

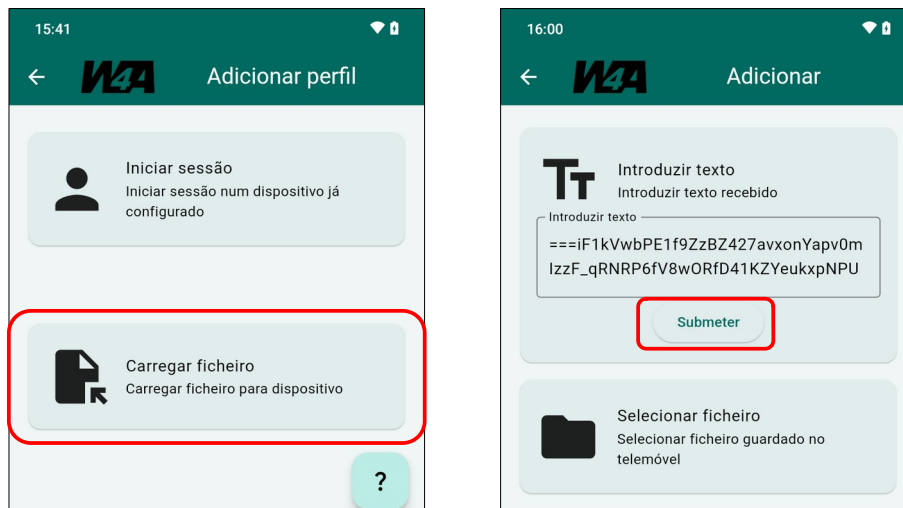
To pair the profile:

1. copy all the text you received;
2. open the Add profile menu;
3. select Load file or the equivalent option;
4. choose the text entry option;
5. paste the received content;

6. confirm submission.

Do not edit, format, or remove any part of the received text.

Incomplete or modified text may prevent pairing.



File

Use this method when you receive a file containing the profile details.

Pairing can be started in either of these ways:

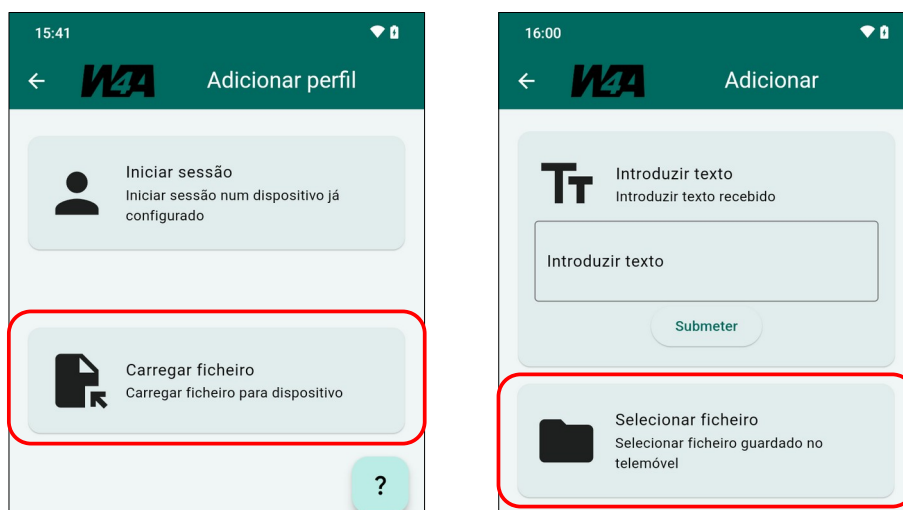
- open the file directly from your phone's file manager and select the W4A Key application;
- open the W4A Key application, select Load file, and choose the received file.

For the second option:

1. open the Add profile menu;
2. select Load file;
3. find the file on your phone;
4. select it;
5. confirm the import.

Do not change the file name, extension, or contents.

After pairing, delete the file or keep it in a protected location, according to the applicable security rules.



QR code

Use this method when you receive a QR code with pairing details.

To pair the profile:

1. open an application that can scan QR codes;
2. point the camera at the code;
3. wait for it to be read;
4. allow the W4A Key application to open if prompted;
5. confirm pairing.

If the scanner does not automatically open the W4A Key application:

1. copy the text obtained from the QR code;
2. open the Add profile menu;
3. select the text entry option;
4. paste the content;
5. confirm submission.

Do not photograph, publish, or share the QR code with unauthorized persons.

The code may contain data that allows the profile to be linked to the device.

14.2. Verifying pairing

After pairing, confirm:

- the profile appears in the application;
- the name and device are correct;

- you can connect to the device;
- available operations match the assigned permissions;
- there are no error messages.

When prompted, change the initial password to a secure personal password.

Do not share your password with third parties.

14.3. Pairing not completed

If pairing cannot be completed, check:

- the details you received;
- the password;
- the profile type;
- proximity to the device;
- Bluetooth status;
- application permissions;
- profile validity.

If the problem persists, contact the person who created the profile to confirm:

- the profile is still active;
- the shared details are correct;
- there are no date or time restrictions;
- the profile has not been suspended or deleted.

After pairing, the profile is ready for use through the application.

15. Managing the profile

The Information tab lets you view and change the details of the profile currently linked to the application.

15.1. Profile settings

The profile settings area may show the following parameters:

Name

Lets you change the name used to identify the profile.

ID

Shows the identifier automatically assigned to the profile by the device.

The ID can be used to sign in, as described in Section 14.1 Signing in and pairing the profile.

This value is for information only and cannot be changed.

Type

Shows the profile type.

The profile type is set when it is created and cannot be changed here.

Access type

Shows the access restrictions assigned to the profile, where applicable.

These restrictions are set by the higher-level profile and may be read-only.

Maximum session duration

Lets you set the maximum period of session inactivity.

After the configured period, you must enter the password again to communicate with the device.

Tracking permission

Lets you choose the traceability type associated with the profile, within the options authorized by its creator.

See Section 8.9 Traceability, credentials, and sessions for the meaning of each option.

The creator can reset the password

Indicates whether the profile that created this access is authorized to reset its password.

Perfil	
Nome	Administrador 1
Id	#02
Tipo	Administrador
Estado	Ativo
Número de dependentes	0/5
Tipo de acesso	Sem restrições
Tempo máximo de sessão	03d00h00m
Permissão de rastreamento	Sempre identificado
Palavra-chave pode ser reposta pelo criador	☐

Submeter

Managing the profile

When enabled, the creator can set a new password if the user loses their credentials.

This permission also allows the creator to gain access to the profile by resetting the password.

Enable it only if you accept this possibility.

Press Submit to save the changes.

16. Device information and management

The Information tab lets you view device status and details and perform management functions.

Available options depend on the profile type and its permissions.

16.1. Device status

The displayed status reflects information received during the most recent communication with the device.

Clock status

When the clock indicates an error, functions that depend on the date or time may be unavailable, including:

- validity periods;
- time restrictions;
- operation schedules;
- chronological records.

If a clock error appears, follow the procedure in Chapter 22 Troubleshooting.



Input and output states

The displayed states let you check the current condition of the configured circuits.

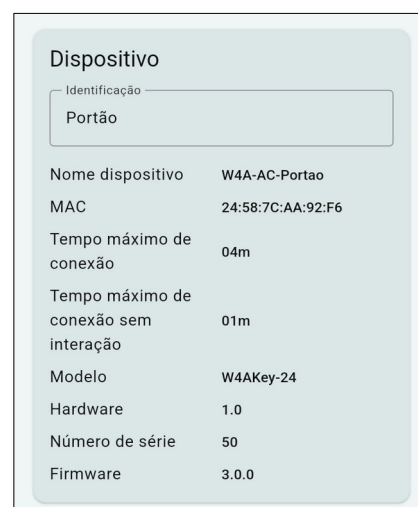
The information shown in the application does not replace direct inspection of the installation when required for safety.

16.2. Information and identification

This area may show technical details such as:

- model;
- serial number;
- hardware version;
- firmware version;
- other information provided by the device.

Technical support may request these details when diagnosing a fault.



Identification in the application

Identification lets you change the name shown for the device on this phone.

This change is only for organizing the local application and does not necessarily change the name stored on the device or shown on other phones.

Choose a name that clearly distinguishes the equipment from other paired devices.

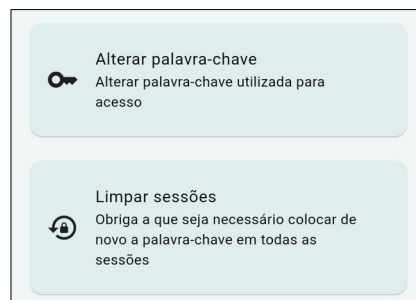
16.3. Password and sessions

Changing the password

To change the profile password:

1. open the password management option;
2. enter the new password;
3. confirm the new password;
4. submit the change.

You may need to authenticate the profile again after the change.



Clearing sessions

The Clear sessions option invalidates the profile's existing sessions.

After using it, you must enter the password again to communicate with the device.

You can use this option if:

- a phone has been lost or replaced;
- unauthorized access is suspected;
- you want to end existing authentications.

16.4. Removing the profile

The application offers two removal methods.

Remove locally

Removes the profile only from the current phone.

The profile remains stored on the W4A Key and can be paired again with its access details.

Remove from device

Removes the profile from the phone and also deletes it from the W4A Key.

After this operation:

- the credentials are no longer valid;
- the profile can no longer communicate with the device;
- a new profile may be required to grant access again.

If the profile has dependents, they are deleted too and will lose access to the device.

16.5. Updating the device

Available only to the Installer profile.

Lets you check for and install new firmware provided by W4A.

Before starting:

- put the installation in a safe state;
- ensure a stable power supply;
- keep the phone nearby;
- do not execute other operations.

During the update:

- do not switch off the power supply;
- do not close the application;
- do not interrupt communication;
- do not press the button unless instructed by the application.

After the update, confirm the installed version and test the configured functions.

16.6. Factory data reset

Available only to the Installer profile.

This option deletes all settings, profiles, and records stored on the device.

If data has been configured, it may be necessary to press the device button to confirm the reset.

See Chapter 23 Factory data reset before performing this operation.

17. Managing dependents

17.1. Accessing dependents

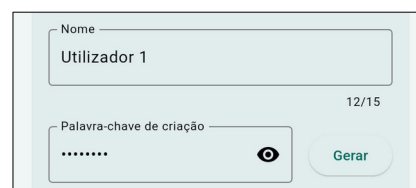
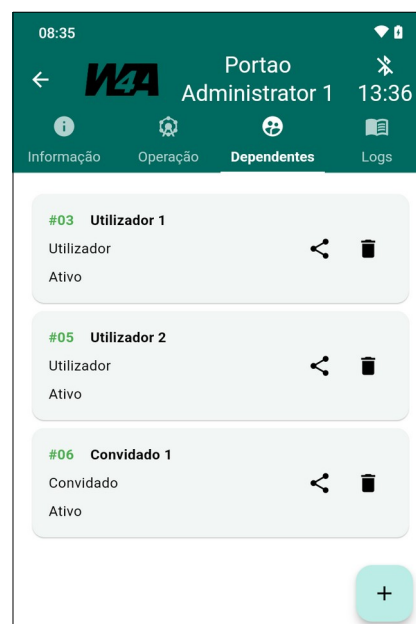
In the desired profile, open the Dependents tab to view, create, or manage profiles lower in the hierarchy.

The number and types of profiles that can be created depend on the permissions assigned to the current profile.

17.2. Creating a dependent

To create a dependent:

1. open the Dependents tab;
2. press the + button;
3. enter the profile name;
4. set the initial password;
5. configure the dependent's settings;
6. set the applicable restrictions;
7. press Submit;
8. wait for confirmation from the device.



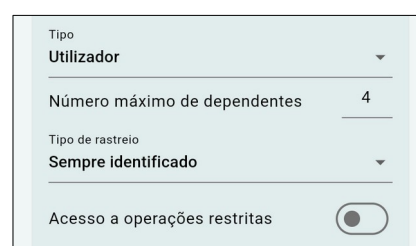
17.3. Configuring the dependent

Type

Lets you select the dependent's profile type.

Available options depend on the profile creating it.

See Section 8.6 Profiles, hierarchy, and dependents for the functions and limitations of each profile type.



Maximum number of dependents

Sets the maximum number of profiles the dependent can create.

If set to 0, the profile cannot add new dependents to the device.

The maximum available value may be limited by the permissions of the creating profile.

Traceability type

Sets the minimum traceability level for the dependent.

This setting also limits the options the profile can assign to its own dependents.

See Section 8.9 Traceability, credentials, and sessions for the available options.

Access to restricted operations

Lets you authorize the dependent to execute operations configured as restricted.

When disabled, the profile cannot execute these operations.

Grant this permission only when the user actually needs access to restricted functions.

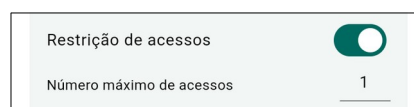
17.4. Access limit

An access limit restricts the number of accesses available to a Guest profile.

Only operations configured to count accesses reduce the remaining number.

See Section 8.8 Counting accesses for how accesses are counted.

When the limit is reached, the profile can no longer execute operations subject to this restriction.



17.5. Time restrictions

Time restrictions limit a dependent's access by date and schedule.

Restrictions may include:

- a start date;
- an end date;
- different schedules for each day of the week.

Configured restrictions apply cumulatively. The profile can access the device only when every active condition is met.

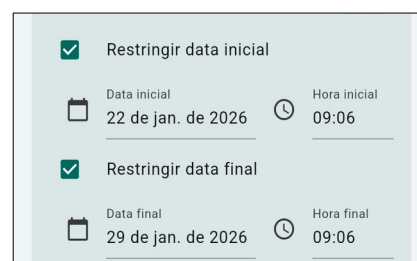
Start date

Enable Restrict start date to prevent access before a specified date and time.

After enabling it, set:

- the start date;
- the start time.

The profile can access the device only from the configured moment onward.



End date

Enable Restrict end date to limit access to a specified date and time.

After enabling it, set:

- the end date;
- the end time.

After that time, the profile can no longer access the device.

Schedule restriction

Enable Restrict daily to set different access schedules for each day of the week.

Settings include:

Available schedules

Lets you create or define time periods for the restriction.

Each schedule must have:

- a start time;
- an end time.

Selected schedules

Lets you assign the times at which the dependent can access the device for each day of the week.

A day can:

- use one or more schedules;
- have no authorized time period;
- use different schedules from other days.

Outside the selected periods, the profile cannot access the device.

Before using time restrictions, check that the W4A Key's date, time, and time zone are correct.

The screenshot displays the 'Restringir diariamente' (Restrict daily) settings. At the top, there is a checkbox labeled 'Restringir diariamente' which is checked. Below this, there are two sections: 'Horários disponíveis' (Available schedules) and 'Horários selecionados' (Selected schedules).

Horários disponíveis:

	Start Time	End Time	Duration
1	09:00	18:00	
2	08:00	12:00	
3	22:00	06:00	+1d
4	00:00	00:00	+1d

Horários selecionados:

Day	Selected Schedules
dom.	
seg.	09:00 - 18:00
ter.	00:00 - 00:00+1d
qua.	22:00 - 06:00+1d
qui.	09:00 - 18:00 22:00 - 06:00+1d
sex.	
sáb.	

17.6. Saving and sharing the profile

After configuring the dependent:

1. review the settings;
2. confirm the restrictions;
3. press Submit;
4. wait for confirmation;
5. check that the profile appears in the dependents list.

After creation, access details can be shared using methods offered by the application, including:

- credentials;
- text;
- a file;
- a QR code.

Share the details only with the authorized person.

The recipient should follow the procedure in Chapter 14 Pairing a user profile.

17.7. Editing or deleting a dependent

To change an existing profile:

1. open the Dependents tab;
2. select the profile;
3. change the desired settings;
4. press Submit;
5. wait for confirmation.

If the dependent has authorized its creator to reset the password, a new password can also be set here.

To delete a profile:

1. select the dependent;
2. choose Delete;
3. confirm the operation;
4. wait for the device to update.

Before deleting, confirm:

- you selected the correct profile;
- access is no longer needed;
- whether the profile has dependents;
- whether deletion will affect other users.

After deletion, the profile's access details are no longer valid.

18. Executing and configuring commands

18.1. Executing commands

Available commands are shown in the Home menu.

Each command can execute one or more operations configured on paired devices.

To execute a command:

1. open the Home menu;
2. find the desired command;
3. confirm that it corresponds to the equipment you want to control;
4. press the command;
5. monitor execution through the status indicators.

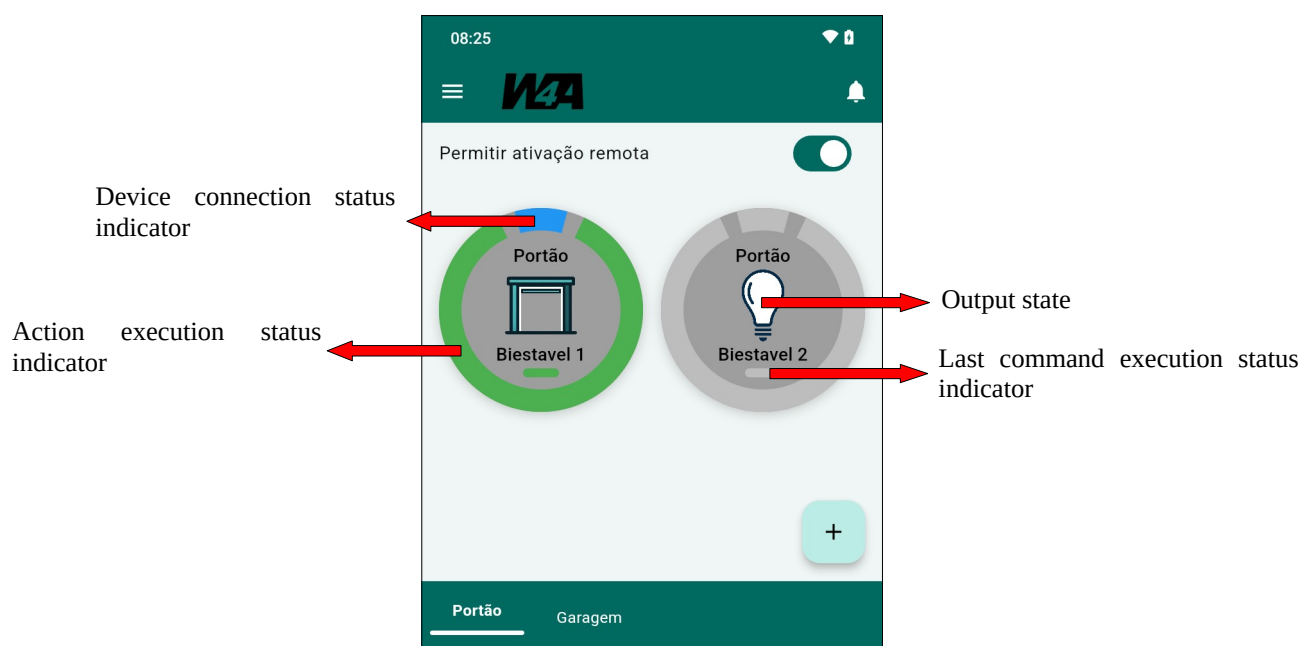
To cancel an ongoing actuation, press and hold the command until the application shows a cancellation message.

Whether cancellation succeeds depends on the execution state and operation type. An operation already sent to the device cannot always be interrupted.

WARNING — Local or remote operation

Before executing a command:

- confirm that the controlled area is safe;
- confirm that you selected the correct device and command;
- do not operate remotely if you cannot assess the safety of the area.



Connection status indicator

This indicator shows device discovery and connection progress during command execution.

Color	Display	Status
Gray	Solid	Command not executed
Blue	Flashing	The application is searching for the device and trying to connect
Blue	Solid	Connection to the device established

Establishing a connection does not, by itself, mean that all command actions have been executed.

Action status indicator

A command can contain one or more actions.

The application shows a section for each action so you can monitor its status separately.

Color	Status
Gray	The action has not yet started
Blue	The action is in progress
Green	The action was executed successfully
Yellow	The connection to the device could not be established or maintained
Red	An error occurred while executing the action

If a command contains several actions, they may have different statuses.

Failure of one action may or may not prevent subsequent actions, depending on the command's configured behavior.

Last command status indicator

This indicator shows the result of the last command execution.

Color	Status
Gray	The result of the last execution is unknown
Green	The command was executed successfully
Yellow	The command did not finish because the connection failed
Red	An error occurred during execution

The indicator represents the last known execution; it does not prove the load's current state.

Remote operation

To allow a command to be executed through remote communication, enable Allow remote activation in the command settings.

Remote operation is available only when:

- the device's remote communication service is active;
- the device has Internet access;
- the phone has Internet access;
- the profile is authorized to execute the operations;
- the command is authorized for remote operation.

If this option is disabled, command actions can be executed only through local communication.

18.2. Configuring commands

Configure commands in the Commands menu.

This menu shows:

- existing groups;
- commands in each group;
- the order in which commands are shown.

Groups correspond to pages in the Home menu.

To move a command within a group, press and hold it, then drag it to the desired position.

To edit an existing command, press its button in the Commands menu.

To create a new command, press + or the equivalent option.

Command settings are divided into:

- identification;
- behavior;
- actions.



Command identification

Name

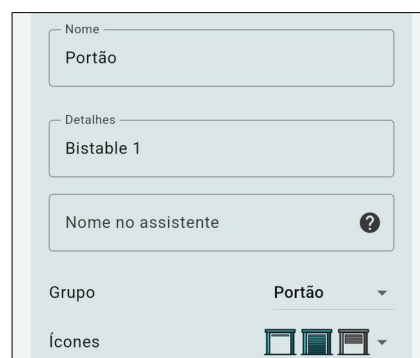
Sets the text shown at the top of the command.

Use a short name that makes the function easy to identify.

Details

Sets the additional text shown at the bottom of the command.

It can indicate:



- the location;
- the equipment;
- the purpose;
- other useful information.

Assistant name

Sets the name used by a compatible assistant, such as Siri or Google Assistant, to identify the command.

Choose a name that is:

- simple;
- easy to pronounce;
- different from other commands;
- unambiguous.

Availability depends on the operating system, application version, and installed services.

Group

Sets the group to which the command belongs.

The group determines on which Home menu page the command appears.

Icons

Lets you choose the icons used to:

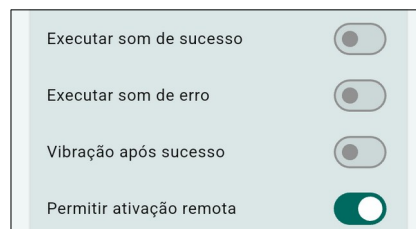
- identify the command;
- represent the inactive state;
- represent the active state, where applicable.

Icons make identification easier but do not replace confirmation of equipment status.

Command behavior

Play success sound

When enabled, the application plays a sound after the command executes successfully.



Play error sound

When enabled, the application plays a sound when the command cannot be completed.

Vibrate on success

When enabled, the phone vibrates after the command executes successfully.

Vibration availability depends on the phone's capabilities and settings.

Allow remote activation

Lets the command's actions run through remote communication.

When disabled, actions run only through a local connection to the device.

This option does not activate the W4A Key's remote service. The service must already be configured on the device.

Command actions

A command must contain at least one action.

Each action identifies an operation to be executed on a specific device.

A command can contain several actions, creating a sequence involving:

- different operations;
- different devices;
- simultaneous actions;
- sequential actions;
- delays between actions.

Configure the following for each action:

Dispositivo	
Portao	▼
Operação	
Biestavel 1	▼
Timeout de tentativa de conexão	05s
Tempo de conexão	30s

Device

Select the device on which the operation will be executed.

Check that you selected the correct equipment, especially if several devices have similar names.

Operation

Select the operation to execute on the chosen device.

The list shows only operations available to the profile being used.

Connection attempt timeout

Sets how long the application tries to connect to the device after the command is pressed.

If communication is not established within that time:

- the action is canceled;
- its status is shown as a connection failure;
- the corresponding indicator turns yellow.

A timeout that is too short may cause failures on slow networks or in environments with slow communication.

A timeout that is too long can delay the error message.

Connection duration

Sets how long the application keeps the connection to the device open.

The value must be long enough to finish the operation and receive confirmation.

Action sequence

If a command contains more than one action, determine when each subsequent action starts.

Momento de execução	
Após execução da anterior	▼
Atraso da atuação	0

At the same time as the previous action

The action starts at the same time as the previous action, or as close to it as the application and communication methods permit.

After successful execution of the previous action

The next action starts only after the previous one has succeeded.

If the previous action fails, the sequence does not proceed to this action.

After execution or failure of the previous action

The next action starts after the previous action's attempt ends, whether it succeeded or failed.

Use this option only if the next action can be performed safely even when the previous one fails.

Actuation delay

Sets the waiting time before the action starts.

The delay is measured from the action's configured execution point.

Before configuring a sequence:

- confirm the action order;
- confirm the selected devices and operations;
- assess the effect of a connection failure;
- check whether the next action can run if the previous action fails;
- avoid sequences that could cause incompatible movements or actuations.

Saving the command

After configuring it:

1. review its identification;
2. confirm the group;
3. confirm sound, vibration, and remote operation options;
4. review all actions;
5. confirm the order and delays;
6. press Save or the equivalent option.

After saving, the command is available in the selected group in the Home menu.

Test the command before routine use, especially if it includes several actions or devices.

18.3. Using Android Auto and Apple CarPlay

The W4A Key application can make selected commands available through Android Auto and Apple CarPlay when the mobile device and vehicle or infotainment system are compatible.

Only commands in the application's In Car list appear in the vehicle. Users can add commands to this list manually, or they can be added automatically if the Installer enabled Automatically making a command available in the car in the operation settings.

Adding commands to In Car

To make a command available in the vehicle:

1. open the Commands menu in the application;
2. select the In Car tab;
3. tap + to add a command to the list;
4. select the desired command;
5. arrange the commands in the order in which you want them to appear.

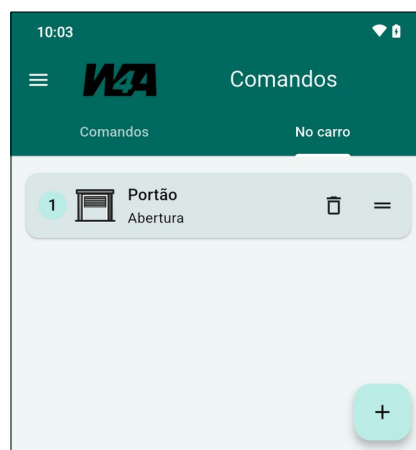
After configuration, the command will be available for display in the car, subject to the compatibility of the platform and system used.

Reordering or removing commands

Commands in the In Car list can be reordered or removed in the same tab.

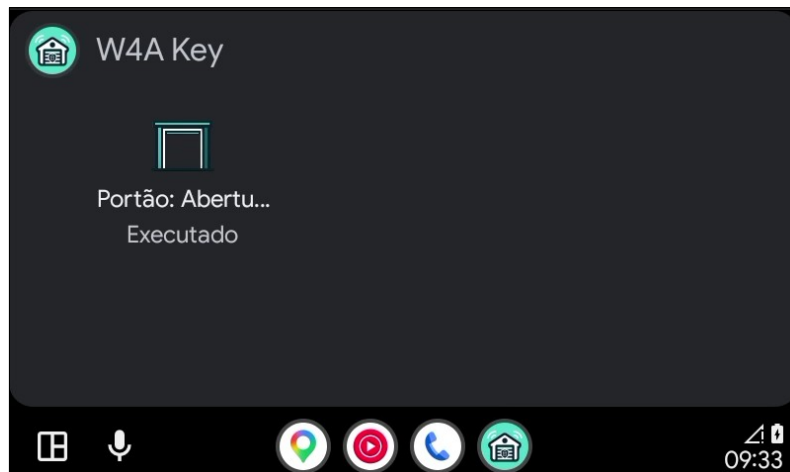
Removing a command from this list prevents it from appearing in the vehicle but does not delete it from the application's main command list.

If the command is deleted from the application, it will also be unavailable in Android Auto and Apple CarPlay.



Important notes

- The display, organization, and number of visible commands may depend on the platform or infotainment system's limitations.
- Some functions available in the mobile application may not be available in Android Auto or Apple CarPlay.



19. One-Time Access

One-Time Access provides temporary access to a device's authorized operations without permanently linking a profile to the application.

Use this function when you need to operate a particular device once without keeping its profile available in the application for future use.

Access ends after use or when the session closes, according to the conditions set for the profile.

19.1. Signing in with One-Time Access

Sign-in is similar to normal profile pairing.

The main difference is that you start from the One-Time Access menu.

To use this function:

1. open the application;
2. open the One-Time Access menu;
3. select the method corresponding to the details received;
4. enter or load the access details;
5. select the desired device if prompted;
6. enter the password where applicable;
7. wait for profile validation and communication with the device.

Access details may be provided through the same methods as normal sign-in, including:

- credentials;
- text;
- a file;
- a QR code.

See Section 14.1 Signing in and pairing the profile for details of these methods.

19.2. Using operations

After sign-in, the application shows operations available to the profile.

To execute an operation:

1. confirm that the displayed device is correct;
2. select the desired operation;
3. verify that it can be performed safely;
4. press the corresponding command;

5. wait for the result.

WARNING — Temporary operation

Before executing an operation, make sure there are no people, animals, or objects in the controlled equipment's moving or operating area.

Do not use One-Time Access to operate equipment remotely if you cannot confirm that the area is safe.

19.3. Ending access

One-Time Access does not permanently pair the profile with the application.

After use:

- the profile does not remain available in the Profile menu;
- no permanent access is created in the application;
- you may have to sign in again for the next use;
- the details remain subject to the restrictions set on the device.

If you intend to use the same profile regularly, complete the normal pairing procedure described in Chapter 14 Pairing a user profile.

20. Offline mode

Offline mode lets an authorized profile prepare a file containing management actions for a W4A Key without being in direct contact with the device.

The file can be sent to another person, who later executes it through the application when they are in contact with the W4A Key.

Thus, changes can be prepared and carried out by different people at different times.

Offline mode can be used, for example, to:

- create a dependent remotely;
- change a profile's details;
- delete a profile;
- change or reset a user's password;
- clear a user's sessions;
- invalidate an offline file generated earlier.

Actions take effect only after the file has been submitted to and accepted by the device.

20.1. How it works

The process has three stages:

1. an authorized profile prepares the actions in the application;
2. the application generates an offline file;
3. a person in contact with the device loads and executes the file.

The person executing the file does not need to configure its actions manually.

The device validates the file and executes only valid, authorized actions.

Each file has a unique identifier that the device uses to distinguish it from other generated files.

20.2. Generating an offline file

To generate a file:

1. open the application;
2. open the Offline mode area;
3. open the profile authorized to perform the desired actions;
4. create a new file;
5. add the management actions;
6. configure their parameters;

7. confirm the action order;
8. generate the file;
9. save or share it through a secure channel.

The application may allow several actions in one file.

Before generating the file, confirm:

- the target device;
- the profile authorizing the actions;
- the users affected;
- the data entered;
- the consequences of each action;
- the execution order.

Generate a new file whenever you need to change the actions or their parameters.

20.3. Available actions

Available actions depend on the profile type and permissions.

They may include:

Create a user

Prepares creation of a new dependent profile.

Settings may include the same parameters used when creating dependents normally.

Use this method when the creator is not near the device.

The file can be sent directly to the intended user. When that person is near the W4A Key, they can execute the file to create the profile, then use its access details normally.

Edit a user

Changes the settings of an existing profile.

Before generating the file, confirm the ID of the profile you intend to edit.

Changes take effect only when the file is executed on the device.

Delete a user

Prepares deletion of an existing profile.

After execution, that profile's access details are no longer valid.

Before including this action, check:

- the selected profile;

- whether access is still needed;
- whether it has dependents;
- the impact of deletion.

Change or reset a password

Sets a new password for a profile, provided the profile generating the file is authorized to do so.

Share the new password only with the authorized person.

Clear sessions

Invalidates a profile's existing sessions.

After execution, the password must be entered again to communicate with the device.

Invalidate an earlier file

Prevents execution of an offline file generated earlier.

To use this function, provide the unique identifier of the file to be invalidated.

This action may be useful if:

- an error was found in the file;
- incorrect details were included;
- the file was sent to the wrong person;
- the actions are no longer needed;
- unauthorized disclosure is suspected.

Invalidation takes effect only after the new file has been executed on the device.

If the original file was already executed before invalidation, its actions are not automatically reversed.

20.4. Sending the file

The offline file can be transferred using the sharing methods available on the phone.

Share it only with the person responsible for execution.

Before sending, confirm:

- the recipient's identity;
- the target device;
- the included actions;
- whether the file contains access details;
- whether a password needs to be sent through a separate channel.

Treat the file as confidential information.

Do not:

- publish it;
- send it to groups;
- store it in public locations;
- modify it;
- rename it in a way that prevents identification;
- share it with unauthorized persons.

20.5. Executing the file on the device

The file must be executed by someone in contact with the W4A Key using a supported communication method.

To execute it:

1. open the file on the phone and select the W4A Key application;

or:

1. open the Add profile menu;
2. select Load file;
3. find the file on the phone;
4. select it;
5. confirm the import.

Then:

1. confirm the target device;
2. review the listed actions where available;
3. connect to the W4A Key;
4. confirm execution;
5. keep the application open;
6. wait for completion.

Do not interrupt communication during execution.

The application should show the result of the submitted actions.

20.6. Execution result

After execution, confirm:

- whether the file was accepted;
- whether all actions finished;
- whether an action was refused;
- whether communication failed;
- whether the procedure needs to be repeated or corrected.

A file may be refused if:

- it is not intended for the selected device;
- it has been modified or damaged;
- the permissions are no longer valid;
- one of the affected profiles no longer exists;
- the file has already been invalidated;
- the file has already been used and cannot be run again;
- it is incompatible with the device's current configuration.

Do not consider changes complete until the application confirms them.

20.7. Limitations and security

Offline mode does not mean that actions run without contact with the W4A Key.

The file can be prepared remotely, but execution requires communication with the device.

The file's creator is responsible for:

- selecting the correct actions;
- using appropriate profiles;
- checking the data;
- protecting the file;
- informing the person executing it about the procedure.

The person executing the file must:

- confirm the target device;
- leave the file unchanged;
- not execute files from unknown sources;
- check the result;
- delete or protect the file after use.

If an error is found in a file that has already been sent, generate and execute an invalidation file as soon as possible.

21. History

21.1. Viewing history

History lets you view events recorded by the W4A Key, including:

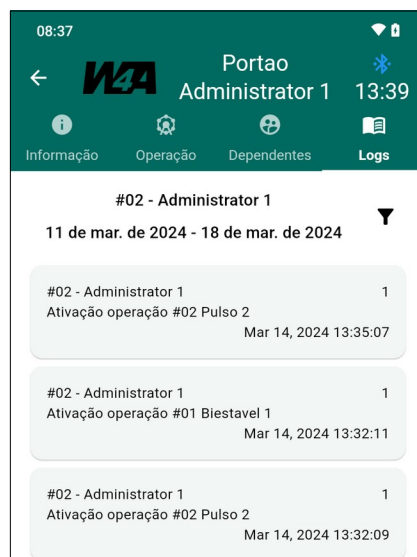
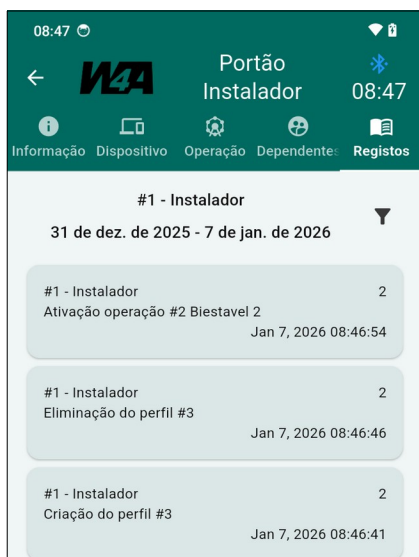
- execution of operations;
- creation of profiles;
- deletion of profiles.

To view history:

1. open the desired profile;
2. open the Records tab;
3. connect to the device if needed;
4. wait for the records to load.

The information shown depends on:

- the profile type;
- the hierarchical relationship with the affected profiles;
- the selected traceability type;
- the records still available on the device.



21.2. Actuation history

Actuation records may show:

- the date and time;

- the operation executed;
- the profile identifier, when permitted by the traceability type.

User identification depends on the profile's traceability settings.

If traceability does not permit identification, an actuation may still be recorded without being linked to the user's name.

21.3. Dependent history

Depending on the selected traceability type, a profile may view actions performed by its dependents.

Available information may include:

- actuations;
- creation of dependent profiles;
- deletion of dependent profiles;
- identification of the responsible profile, when permitted.

If the traceability type does not allow identification, events may be shown without a link to a specific profile.

A profile can view only information about its dependents, subject to the defined permissions.

21.4. Installer history

The Installer profile can access the complete history of actuations recorded on the device.

Actuations are shown without identifying the profiles that executed them.

The Installer can view:

- the date and time of actuation;
- the operation executed;
- the result;
- other technical information provided by the record.

This access lets the Installer check the device's general operation without revealing user identities.

21.5. Profile creation and deletion

History may show events relating to:

- creation of a profile;
- deletion of a profile.

Depending on the traceability type and hierarchical relationship, a record may show:

- the date and time;

- the event type;
- the profile created or deleted;
- the profile responsible for the action, when identifiable.

21.6. History limitations

Available information may be limited by:

- the device's storage capacity;
- the traceability type;
- the hierarchical relationship between profiles;
- deletion of data;
- a factory data reset.

A factory data reset deletes records stored on the device.

History is intended for system review and management; it does not replace certified attendance, surveillance, or proof-of-presence systems.

22. Troubleshooting

This section describes problems that may arise during installation, configuration, or use of the W4A Key, along with possible causes and recommended actions.

Before contacting technical support:

1. check the current status in the application;
2. check the device LED;
3. read the messages shown by the application;
4. view the history for the period when the problem occurred;
5. perform only checks that can be carried out safely.

WARNING — Electrical hazard

Before checking electrical circuits, changing wiring, tightening terminals, or opening the enclosure:

- switch off the power supply;
- isolate all power sources;
- prevent accidental reconnection;
- verify the absence of voltage;
- follow applicable safety procedures.

Disabling an output or operation through the application does not guarantee electrical isolation.

Only qualified personnel may work on the electrical installation.

22.1. Troubleshooting table

Problem	Possible cause	Recommended action
The device does not power on	No power supply	Confirm that the specified terminals receive the supply voltage and check the external protective devices.
	Incorrect supply voltage	Confirm that the applied voltage is compatible with the installed model.
	Loose conductor, incorrect terminal connection, or tripped protective device	Switch off and isolate the power supply. Check the wiring, terminal tightness, and external protective devices.
	Internal fault	Disconnect the equipment and contact technical support. Do not attempt to repair the device.
The device restarts unexpectedly	Power supply failure or voltage drop	Check the stability of the power supply.
	Poor power supply connection	Switch off and isolate the installation, then check conductors and terminals.
	Electrical interference or disturbance	Check the separation of power and signal circuits and the suppression devices used on loads.

Troubleshooting

The device operates intermittently	Unstable power supply	Check the supply voltage and protective devices.
	Poor connection	Check terminals and wiring after switching off and isolating the power supply.
	Interference affecting inputs or communications	Check cable routing and move the device away from interference sources.
Bluetooth communication cannot be established	Device out of range	Move the phone closer to the W4A Key and reduce obstacles between them.
	Bluetooth disabled	Enable Bluetooth on the phone.
	Application lacks permissions	Check Bluetooth, nearby device, and location permissions where required by the operating system.
	Another user connected	Wait for the existing connection to end and try again.
	Outdated application	Update to a compatible application version provided by W4A.
Wi-Fi communication cannot be established	Wrong network or invalid credentials	Check the configured network name, password, and security method.
	Insufficient coverage	Check signal strength at the installation location.
	Mobile device connected to another network	For local access, confirm that the phone and W4A Key can access the appropriate network.
	Router or network unavailable	Check the router and local network.
Remote communication is unavailable	Remote service inactive or expired	Check the remote service status.
	Device has no Internet access	Check the Wi-Fi connection and Internet access.
	Phone has no Internet access	Check the phone's mobile data or Wi-Fi connection.
	Remote activation disabled for the command	Enable Allow remote activation in the command settings.
Cannot sign in	Incorrect name, ID, or password	Check the details entered.
	Profile deleted	Contact the profile creator.
	Profile outside its authorized period or schedule	Check the restrictions assigned to the profile.
	Incomplete or changed pairing details	Request the access details again.
Cannot pair a profile	Wrong device selected	Check the W4A Key identifier.
	Invalid access details	Check the text, file, QR code, or credentials received.
	Communication failure	Move the phone closer and repeat the procedure.
An input does not change state	Incorrect connection	Check the connection between the contact, common terminal, and corresponding input.
	Faulty external contact	Check the connected button, switch, relay, or sensor.
	Input disabled or incorrectly configured	Review the input settings.
An input changes state erratically	Poor contact	Check terminal tightness and the wiring condition.
	Electrical interference	Route input cables away from power cables and interference

Troubleshooting

		sources.
	Faulty external contact	Check or replace the external contact.
An output does not activate	Operation assigned to another output	Review the operation settings.
	Inactive operation	Enable the operation and submit the settings again.
	Input blocking actuation	Check input states and settings.
	Interlocking active	Check the states of other outputs.
	Profile or schedule restriction	Check the applicable permissions and restrictions.
	Device error	Check the LED and restart only when safe to do so.
The application says the output is active, but the load does not work	External circuit fault	Switch off and isolate the power supply, then check the wiring, protective devices, and controlled equipment.
	No external power supply to the load	Check the controlled circuit's power source.
	Faulty auxiliary relay or contactor	Have it checked by qualified personnel.
The load operates unexpectedly	Active input, operation, or sequence	Check states, input settings, and operation sequences.
	Command executed by another user	Check the available history.
	External circuit fault	Switch off and isolate the installation immediately and request help from qualified personnel.
An operation does not execute	Incorrect settings or settings not submitted	Review the settings and confirm that the application reported a successful save.
	Restricted operation	Confirm that the profile is authorized to use restricted operations.
	Profile outside its authorized period	Check the configured dates and times.
	Access limit reached	Check the number of remaining accesses.
	Another incompatible operation is running	Wait for it to finish or run the Stop operation where applicable.
A command shows a connection failure	Communication was not established within the configured time	Move the phone closer, check communications, and review the connection attempt timeout.
A command shows an actuation error	Operation refused or failure during execution	Check each action's status and applicable restrictions.
An action sequence does not finish	Previous action ended with an error	Check when the next action is configured to run.
	Wrong device or operation	Review the command actions.
	Connection attempt timeout or connection duration too short	Adjust the configured times.
The date or time is wrong	Incorrect region or time zone	Correct the region and time zone.

Troubleshooting

	Internal clock error	Restart the device and check again. If the error persists, contact technical support.
Time restrictions do not work	Invalid date or time	Check the clock status.
	Restriction not submitted	Review the settings and press Submit.
	Incorrect dates or schedules	Check the configured values.
History does not identify the user	Traceability type does not allow identification	Check the traceability type assigned to the profile.
	Viewed by the Installer	The Installer views actuations without identifying users.
An offline file is not accepted	File intended for another device	Check the target device.
	File modified or damaged	Request a newly generated file.
	File invalidated	Contact the file creator.
	Profile or permission no longer valid	Check the affected profiles and their permissions.
	File already used	Generate a new file if needed.
The LED flashes slowly	Device in reset mode	Do not press the button unless you intend to confirm the reset. See the relevant chapter.
The LED flashes rapidly	Device in error mode	Put the installation in a safe state, restart the device, and check whether the error persists.

22.2. General checking procedure

If the cause is not immediately clear:

1. identify the status shown in the application;
2. check the LED;
3. read error messages;
4. check the history around the time of the problem;
5. confirm the date and time;
6. confirm the profile used;
7. check permissions and restrictions;
8. check input and output states;
9. confirm the settings were submitted;
10. check the communication method;
11. carry out only permitted electrical checks, safely.

Do not change several settings at once while diagnosing the problem.

Change one setting at a time and check the result.

22.3. Restarting the device

A restart may help with a temporary communication or operating failure.

Before restarting:

- confirm that the load can stop or remain in its current state safely;
- confirm that possible behavior after restart will not create a hazard;
- record existing error messages;
- check whether a configuration transfer is in progress.

To restart by switching the power supply:

1. switch off the supply using the appropriate isolation device;
2. verify the absence of voltage;
3. wait a few seconds;
4. restore the power supply;
5. wait for startup to finish;
6. check the date and time;
7. check states and settings;
8. test only the necessary functions.

Do not repeatedly interrupt the power supply as a routine troubleshooting method.

22.4. When to consider a factory data reset

Consider a factory data reset if:

- access to the device cannot be recovered;
- configuration cannot be completed or resumed;
- the device remains in error mode;
- valid settings cannot be restored through normal procedures.

Do not use a reset as a first step to correct:

- power supply failures;
- incorrect wiring;
- faulty loads;
- external relay or contactor faults;
- Bluetooth or Wi-Fi coverage problems;
- incorrectly entered credentials;

- profile or operation restrictions.

Before resetting, identify and correct any electrical, mechanical, or communication problems.

See Chapter 23 Factory data reset for the procedure and its consequences.

22.5. When to stop using the equipment

Stop using the equipment immediately if there is:

- smoke;
- a burning smell;
- abnormal heating;
- electrical noise;
- water ingress;
- damage to the enclosure, cables, or terminals;
- unexpected operation;
- loss of control over the load;
- repeated tripping of protective devices;
- behavior not described in this manual.

Switch off and isolate the power supply if it is safe to do so.

Do not use the equipment again until qualified personnel have identified and corrected the cause.

22.6. Contacting technical support

If the preceding procedures do not resolve the problem, contact W4A technical support.

Where possible, provide:

- the equipment model;
- the serial number;
- the hardware version;
- the firmware version;
- the application version;
- a detailed description of the problem;
- the date and time it occurred;
- how often it occurs;
- the conditions in which it occurs;
- the LED status;

- messages shown by the application;
- relevant settings;
- photos of the installation and wiring;
- the electrical diagram used;
- a screenshot or description of the history, if available.

Do not send passwords, QR codes, pairing files, offline files, or other credentials unless technical support expressly instructs you to do so.

23. Factory data reset

23.1. Purpose and consequences

A factory data reset can restore access to the W4A Key when:

- the device is in error mode;
- the Installer profile password has been lost;
- valid settings cannot be recovered through normal procedures.

The reset is irreversible and deletes all data and settings stored on the device, including:

- profiles;
- passwords;
- sessions;
- settings;
- operations;
- restrictions;
- history.

After the reset, the device returns to its initial state and must be paired, configured, and tested again before use.

WARNING — Electrical hazard

Only qualified personnel may perform options requiring the equipment to be opened or the battery to be removed.

Before opening the device:

1. switch off the power supply;
2. isolate all power sources;
3. prevent accidental reconnection;
4. verify the absence of voltage.

Do not touch terminals or internal components while the equipment is energized, except where the procedure expressly requires pressing the button and the necessary safety conditions are in place.

23.2. Option 1 — Reset by the Installer

Use this option if the Installer profile can still communicate with the device.

To reset:

1. open the Installer menu;

2. select the device;
3. connect to it;
4. open the Information tab;
5. select Factory data reset;
6. read and confirm the warning;
7. follow the application's instructions.

If the device already contains configured data, you may need to confirm the procedure physically using its button.

When the LED flashes slowly:

1. confirm that you want to delete all data;
2. press the device button;
3. wait for the reset to finish.

Do not switch off the power supply during the procedure.

23.3. Option 2 — Reset using the button

Use this option if the Installer profile cannot access the device.

Procedure:

1. switch off the device's power supply;
2. open the enclosure safely;
3. remove the battery;
4. switch the power supply back on;
5. confirm that the LED flashes slowly;
6. press the button for approximately 5 seconds;
7. keep it pressed until the LED starts flashing faster;
8. release the button;
9. wait until the LED stops flashing;
10. switch off the power supply again;
11. reinstall the battery;
12. close the enclosure correctly;
13. restore the power supply.

The reset is complete when the LED stops flashing.

23.4. Option 3 — Full reset

Use this option only if the preceding options cannot reset the device.

Procedure:

1. switch off the device's power supply;
2. open the enclosure safely;
3. remove the battery;
4. press and hold the button;
5. while holding the button, switch the power supply back on;
6. confirm that the LED starts flashing slowly;
7. keep the button pressed for approximately 5 seconds;
8. when the LED starts flashing faster, release the button to begin the reset;
9. wait while the LED flashes;
10. when the LED stops flashing, switch off the power supply again;
11. reinstall the battery;
12. close the enclosure correctly;
13. restore the power supply.

Canceling a full reset

To cancel, keep the button pressed after the LED starts flashing faster. Hold it for approximately 10 seconds, until the LED stops flashing. The reset is canceled only if you have not released the button to confirm it.

23.5. Checks after reset

After completing any of these options:

1. confirm that the device starts without remaining in error mode;
2. check that it appears as an unconfigured device;
3. remove any previous pairings from the application that are no longer valid;
4. create the Installer profile again;
5. configure the device and operations;
6. carry out commissioning tests.

If the device remains in error mode or cannot be configured again, switch it off and contact technical support.

24. Regulatory compliance

24.1. CE marking

The W4A Key bears the CE marking and has undergone the applicable conformity assessment procedure.

The equipment was designed to meet the requirements of European Union legislation applicable to electrical, electronic, and radio equipment.

The EU Declaration of Conformity identifies:

- the manufacturer;
- the product and models covered;
- the applicable legislation;
- the standards or technical specifications used;
- the organization responsible for issuing the declaration.

CE marking does not remove the need to follow the installation, operating, and safety instructions in this manual.

24.2. EU Declaration of Conformity

The complete EU Declaration of Conformity is available at:

www.w4a.pt/products/w4akey/legal/ce

Consult the declaration corresponding to the product model and version.

24.3. Restriction of hazardous substances

The W4A Key was designed with regard to applicable requirements restricting the use of certain hazardous substances in electrical and electronic equipment.

Applicable legislation and any amendments are identified in the EU Declaration of Conformity or the product's regulatory documentation.

24.4. Changes to the equipment

Unauthorized changes to the equipment, including changes to its hardware, firmware, enclosure, internal connections, or components, may:

- compromise safety;
- change performance;
- invalidate the conformity assessment;
- affect the warranty;

- make the equipment unsuitable for use.

Use only accessories, components, and firmware versions authorized by W4A.

25. Disposal and end of life

25.1. Disposing of the equipment

The W4A Key and its electrical and electronic components must not be disposed of with household waste or unsorted commercial waste.

At the end of its service life, take the equipment to an appropriate collection or treatment system for waste electrical and electronic equipment.

Separate collection helps to:

- prevent negative environmental impacts;
- reduce risks to human health;
- allow materials to be recovered;
- promote sustainable use of resources.

25.2. Private users

Private users should contact:

- the retailer from whom they purchased the product;
- municipal services;
- an authorized electrical and electronic waste collection organization;
- another competent body in their country.

These organizations can provide information on drop-off locations and procedures.

25.3. Professional users

Professional users should contact the supplier or an authorized organization to confirm the applicable arrangements for collection and treatment.

Do not dispose of the product with unsorted commercial waste.

25.4. Internal battery

Authorized personnel must remove the internal battery and send it for appropriate treatment in accordance with applicable legislation.

Do not dispose of the battery:

- in household waste;
- in fire;
- by incineration;

- with the equipment without checking local requirements.

Handle a damaged, deformed, or leaking battery carefully and take it to an authorized organization.

25.5. Deleting data

Before transferring, returning, recycling, or disposing of the equipment:

1. record any data you want to keep;
2. perform a factory data reset;
3. remove the device and its profiles from the application where applicable;
4. delete pairing files and offline files that are no longer needed.

The factory data reset is described in Chapter 23 Factory data reset.

26. Warranty, liability, and support

26.1. Responsibilities of the user and Installer

The W4A Key must be installed, configured, used, and maintained in accordance with:

- this manual;
- the model's technical specifications;
- the instructions for connected equipment;
- applicable legislation;
- good technical and safety practices.

The Installer is responsible for checking that the product is suitable for the installation, making the connections and settings correctly, and testing before commissioning.

The user is responsible for using only authorized functions and following the warnings and limits in this manual.

26.2. Improper use

W4A cannot guarantee correct or safe operation if the equipment is subject to:

- incorrect installation or use;
- use outside its specifications;
- absence of the necessary external protective devices;
- incompatible connections or components;
- unauthorized changes to hardware or firmware;
- repairs by unauthorized personnel;
- failure to follow this manual;
- damage caused by external conditions.

This provision does not limit rights or responsibilities that cannot be excluded under applicable law.

26.3. Limitations of communications, states, and records

Communications may be affected by distance, obstacles, interference, network failures, or temporary service outages.

States shown in the application reflect information received during the most recent communication with the device.

Records and history support use and management of the system and do not replace:

- physical safety devices;

- certified systems;
- checks by qualified personnel.

26.4. Warranty

Applicable warranty terms are provided with the product or made available by W4A.

The warranty may not cover damage resulting from:

- incorrect installation or use;
- normal wear;
- unauthorized changes;
- environmental conditions outside the limits;
- surges or external disturbances;
- inadequate maintenance;
- work by unauthorized personnel.

Warranty terms must be interpreted in accordance with applicable law.

26.5. Technical support

Before contacting technical support, see Chapter 22 Troubleshooting.

If the problem persists, contact W4A and, where possible, provide the information listed in Section 22.6 Contacting technical support.

Do not send passwords, QR codes, pairing files, or other credentials unless technical support expressly instructs you to do so.