



W4Key

User Manual



Contents

1. About this manual.....	5
1.1. Purpose and scope.....	5
1.2. Intended audience.....	5
1.3. Models covered.....	5
1.4. Firmware and application compatibility.....	6
1.5. Symbols and warning levels.....	6
1.6. Conventions used.....	6
2. Safety.....	8
2.1. General information.....	8
2.2. User responsibilities.....	8
2.3. Electrical safety.....	8
2.4. Unexpected activation.....	9
2.5. Intended use and limitations.....	9
2.6. Profiles, credentials and communication.....	9
2.7. Abnormal operation and emergencies.....	10
2.8. Residual risks and support.....	10
3. Product description and variants.....	12
3.1. Product overview.....	12
3.2. Main functions.....	12
3.3. Device identification.....	12
3.4. Functional elements.....	13
3.5. User profiles.....	13
3.6. Communication methods.....	13
3.7. Data storage.....	13
4. Indicators and service controls.....	14
4.1. LED.....	14
4.2. Device button.....	14
4.3. Indicator summary.....	14
5. Installing the application.....	15
5.1. Purpose.....	15
5.2. Mobile device requirements.....	15
5.3. Compatible operating systems and platforms.....	15
5.4. Installing the application.....	16
5.5. Required permissions.....	16
5.6. Preparing Bluetooth.....	17
5.7. Updating the application.....	17
5.8. General configuration rules.....	18
6. Operating concepts.....	19
6.1. Inputs, outputs, operations and commands.....	19
6.2. Types of activation.....	19
6.3. Duration, delay and sequences.....	20
6.4. Interlocking and input priority.....	20
6.5. Restricted operations and schedules.....	20
6.6. Profiles, hierarchy and dependent profiles.....	21
6.7. Profile restrictions.....	21
6.8. Counting accesses.....	22
6.9. Traceability, credentials and sessions.....	22
6.10. Communication methods.....	23
6.11. History and records.....	23

7. Associating a user profile.....	25
7.1. Signing in and associating the profile.....	25
7.2. Checking the association.....	28
7.3. Association not completed.....	29
8. Managing the profile.....	30
8.1. Profile settings.....	30
9. Device information and account security.....	32
9.1. Device status.....	32
9.2. Information and identification.....	32
9.3. Passwords and sessions.....	33
9.4. Removing the profile.....	33
10. Managing dependent profiles.....	35
10.1. Accessing dependent profiles.....	35
10.2. Creating a dependent profile.....	35
10.3. Dependent profile settings.....	35
10.4. Access limit.....	36
10.5. Time restrictions.....	36
10.6. Saving and sharing the profile.....	37
10.7. Editing or deleting a dependent profile.....	38
11. Executing and configuring commands.....	39
11.1. Executing commands.....	39
11.2. Configuring commands.....	41
11.3. Using Android Auto and Apple CarPlay.....	45
12. One-Time Access.....	47
12.1. Signing in through One-Time Access.....	47
12.2. Using operations.....	47
12.3. Ending access.....	48
13. Offline mode.....	49
13.1. How it works.....	49
13.2. Generating an offline file.....	49
13.3. Available actions.....	50
13.4. Sending the file.....	51
13.5. Executing the file on the device.....	52
13.6. Execution result.....	52
13.7. Limitations and security.....	53
14. History.....	54
14.1. Viewing history.....	54
14.2. Activation history.....	54
14.3. Dependent profile history.....	55
14.4. Records visible to the Installer.....	55
14.5. Creation and deletion of profiles.....	55
14.6. History limitations.....	56
15. Troubleshooting.....	57
15.1. Troubleshooting table.....	57
15.2. General checking procedure.....	60
15.3. Restarting the device.....	61
15.4. When to contact the Installer for a device reset.....	61
15.5. When to stop using the device.....	62
15.6. Contacting technical support.....	62
16. Regulatory compliance.....	64
16.1. CE marking.....	64
16.2. EU Declaration of Conformity.....	64

16.3. Restriction of hazardous substances.....	64
16.4. Changes to the equipment.....	64
17. Disposal and end of life.....	66
17.1. Disposal of the equipment.....	66
17.2. Private users.....	66
17.3. Professional users.....	66
17.4. Internal battery.....	66
17.5. Erasing data.....	67
18. Warranty, responsibility and support.....	68
18.1. User and Installer responsibilities.....	68
18.2. Improper use.....	68
18.3. Limitations of communication, status and records.....	68
18.4. Warranty.....	69
18.5. Technical support.....	69

1. About this manual

1.1. Purpose and scope

This manual provides the information needed to associate a profile, use the W4A Key, execute commands and manage the functions available under the assigned permissions.

Read these instructions before associating a profile and using the device.

Following this manual helps to:

- ensure that the equipment operates correctly;
- protect users' 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 owner and to authorised Administrators, Users and Guests.

1.2. Intended audience

This manual is intended for:

Administrator

A person authorised to use the device and create or manage dependent profiles, in accordance with the assigned permissions.

User

A person authorised to execute available operations and, where permitted, to manage dependent profiles.

Guest

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

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 can be found in the device information area.

The application version can be found in its settings or in the operating system's official app store.

Screens, parameters and procedures may vary between versions.

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

Do not interrupt the application or communication during data transfers. Technical updates to the device must be performed by the Installer.

1.5. Symbols and warning levels

This manual uses the following signal words:

DANGER

Indicates an imminent hazard which, if not avoided, will result in death or serious injury.

WARNING

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

CAUTION

Indicates a situation that may cause minor injury or damage to the equipment, installation or controlled load.

NOTE

Indicates additional information relevant to associating a profile, authorised configuration or use of the device.

1.6. Conventions used

In this manual:

- the names of application menus, buttons and options 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 authorised to access the device;
- “dependent profile” refers to a profile created by another profile;
- “operation” refers to a function configured on the device;
- “command” refers to the application control 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 refer to 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

Improper use of the W4A Key may cause unexpected activation, equipment damage, loss of access control or use by unauthorised persons.

Before using the device:

- read this manual;
- make sure you have selected the correct device and command;
- use only functions you are authorised to use;
- ensure that activation does not endanger people, animals or property;
- follow the instructions of the Installer and the person responsible for the installation.

2.2. User responsibilities

The user must:

- protect their credentials and mobile phone;
- use only the commands available to their profile;
- check that the area is safe before executing an operation;
- report any abnormal operation;
- remove access that is no longer needed, when authorised to do so.

The user must not:

- open the equipment;
- modify the wiring;
- touch the terminals;
- repair the device;
- change settings reserved for the Installer;
- bypass protective devices;
- share credentials with unauthorised persons.

Electrical work, maintenance and repairs must be carried out only by qualified personnel.

2.3. Electrical safety

DANGER — Hazardous electrical voltage

Do not open the enclosure, touch the terminals or alter the connections.

An unlit indicator does not confirm that the equipment is disconnected from the power supply.

If there is damage, water ingress, abnormal heating, a burning smell or unusual electrical noise:

1. stop using the device;
2. move away from the hazardous area;
3. disconnect the power supply if it is safe to do so;
4. contact the Installer or technical support.

2.4. Unexpected activation

WARNING — Unexpected movement or activation

The equipment may be activated through the application, via Bluetooth, Wi-Fi, the Internet, inputs, sensors or sequences, or by another authorised user.

Before executing an operation:

- confirm the device and command;
- check that the area is clear;
- make sure no people, animals or objects are at risk;
- do not activate the equipment remotely unless you can confirm that the area is safe.

Loss of communication does not guarantee that the operation has stopped.

2.5. Intended use and limitations

The W4A Key is intended for access control and execution of previously configured operations, such as controlling doors, gates, barriers, shutters, lighting and auxiliary equipment.

The W4A Key does not replace:

- safety sensors;
- anti-crush devices;
- emergency controls;
- evacuation routes;
- disconnecting or isolating devices;
- systems that protect people.

Do not use the application as the only means of handling an emergency.

2.6. Profiles, credentials and communication

Each profile has its own permissions and restrictions.

When creating or managing dependent profiles:

- assign only the permissions needed;
- limit dates, times and the number of accesses;
- delete profiles that are no longer needed;
- share access details only with authorised people.

Protect passwords, association files, text and QR codes.

Bluetooth, Wi-Fi and Internet communication may fail because of distance, obstacles, interference or network unavailability.

Do not repeat a command until you have checked the actual state of the controlled equipment.

2.7. Abnormal operation and emergencies

Stop using the device if any of the following occurs:

- unexpected activation;
- loss of control;
- persistent error;
- visible damage;
- water ingress;
- abnormal heating;
- smoke, flames or a burning smell.

In the event of danger:

1. use the available physical emergency devices;
2. move people away from the hazardous area;
3. disconnect the power supply if it is safe to do so;
4. contact the Installer, technical support or emergency services.

Do not use the system again until the cause has been identified and corrected.

2.8. Residual risks and support

Even when the device is used correctly, risks may remain in connection with:

- movement of the controlled equipment;
- failure of sensors or external devices;
- delayed or lost communication;
- display of outdated status information;
- misuse of credentials;

- hazards inherent in the installation.

Contact the Installer if:

- you cannot associate your profile;
- the permissions differ from those expected;
- unexpected activation occurs;
- an error persists;
- a technical update is needed;
- a factory reset is needed;
- you have questions about installation safety.

3. Product description and variants

3.1. Product overview

The W4A Key is an access control and automation device that controls 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.

Access to the device is provided through authenticated profiles, which may have 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;
- manage profiles and their restrictions;
- create dependent profiles;
- view statuses and records;
- use compatible peripherals.

3.3. Device identification

The model designation and main specifications 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. Do not remove, alter 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:** allow operations to be executed through the application.
- **Profiles:** identify and authorise users.
- **Communication methods:** provide local or remote access to the device.
- **History:** records events relating to access, activation and changes.

These elements are explained in detail in Chapter 6 Operating concepts.

3.5. User profiles

The W4A Key uses four profile types:

- **Installer:** configures the device and creates Administrator profiles;
- **Administrator:** uses the device and manages User and Guest profiles;
- **User:** executes operations and may manage Guest profiles, when authorised;
- **Guest:** has limited or temporary access.

There is only one Installer profile per device.

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, for executing certain actions using files prepared in advance.

The availability of each method 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 by an external service.

4. Indicators and service controls

4.1. LED

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

How to interpret the indicator depends on the current operating mode.

Active connection to the application

The LED stays on while a user is connected to the device through the application.

Factory reset mode

The LED flashes slowly when the device enters factory reset mode.

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

If the device repeatedly enters this mode, contact the Installer or technical support.

Error mode

The device is in error mode when the LED flashes rapidly.

Normal operation of the equipment may be unavailable in this state.

Follow the checks described in Chapter 15 Troubleshooting.

If normal procedures cannot correct the error, a factory reset may be needed.

4.2. Device button

The device button is intended for technical procedures. Do not press it unless instructed to do so by the Installer or technical support.

4.3. Indicator summary

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

5. Installing the application

5.1. 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.

5.2. Mobile device requirements

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

Requirements may include:

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

Requirements may change in future versions of the application.

Check the current information provided by W4A or the official app store.

5.3. 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 supports Android Auto and Apple CarPlay, allowing selected functions to be accessed through a compatible vehicle's infotainment system.

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

The commands shown in the vehicle are those in the application's **In Car** list. They may be added manually by the profile or made available automatically through the operation settings. See Section 11.3 Using Android Auto and Apple CarPlay.

Screen appearance and the location of some options may vary with:

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

5.4. 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. check that the developer shown is W4A or an officially authorised entity;
4. select Install;
5. wait for installation to finish.

iOS

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

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

5.5. Required permissions

During installation or first use, the application may request permissions needed for operation.

Depending on the operating system and application version, permissions may be requested for:

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

Grant only the permissions requested by the official application that are needed for operation.

Refusing certain permissions may prevent:

- discovery of the W4A Key;
- association via Bluetooth;
- access over the local network.

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

5.6. Preparing Bluetooth

Before associating the W4A Key:

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

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

Start the association process in the application.

5.7. Updating the application

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

Updates may include:

- bug fixes;
- security improvements;
- support for new firmware versions;
- interface changes;
- new functions;
- changes to minimum requirements.

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

After updating, check:

- the device list;

- permissions;
- access to the functions you use.

5.8. 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. establish communication with the device;
4. open the indicated tab;
5. make your changes;
6. press Submit, Save or the equivalent option;
7. maintain the connection until confirmation appears.

Changes should be considered complete only after the application confirms that they have been saved.

During data transfer:

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

The options shown may vary according to the profile, permissions, firmware and application version.

6. Operating concepts

6.1. 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 type of activation;
- the duration;
- the delay;
- any applicable restrictions;
- the possible execution of another operation.

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

Inputs, outputs and operations are configured by the Installer.

6.2. Types of activation

An operation may use the following types of activation:

Bistable

Each execution changes the output state.

If the output is OFF, it changes to ON. If it is ON, it changes to OFF.

ON pulse in seconds

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

ON pulse in milliseconds

Similar to a pulse in seconds, but intended for short activations.

Press and hold

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

Stop

Stops an ongoing activation or sequence, where applicable.

The Installer selects the type of activation according to the equipment being controlled.

6.3. Duration, delay and sequences

Duration defines how long the output stays active for timed activation types.

Delay defines the interval between executing the operation and the start of activation.

An operation may execute another operation:

- at the same time;
- after it has finished;
- in accordance with the configured sequence.

Sequences make combined behaviours possible but must be tested by the Installer before use.

An incorrect sequence may cause unexpected or incompatible activations.

6.4. Interlocking and input priority

Interlocking may prevent both outputs from being active at the same time.

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

Interlocking configured in the W4A Key does not replace independent electrical or mechanical protection where this is required.

Inputs may take priority over commands executed through the application.

For example, an input may:

- activate an operation;
- prevent an activation;
- deactivate an output;
- stop an ongoing operation.

Input behaviour is defined by the Installer.

6.5. Restricted operations and schedules

An operation may be designated as restricted.

Only profiles authorised to use restricted operations can execute it.

An operating schedule may also be set for an operation.

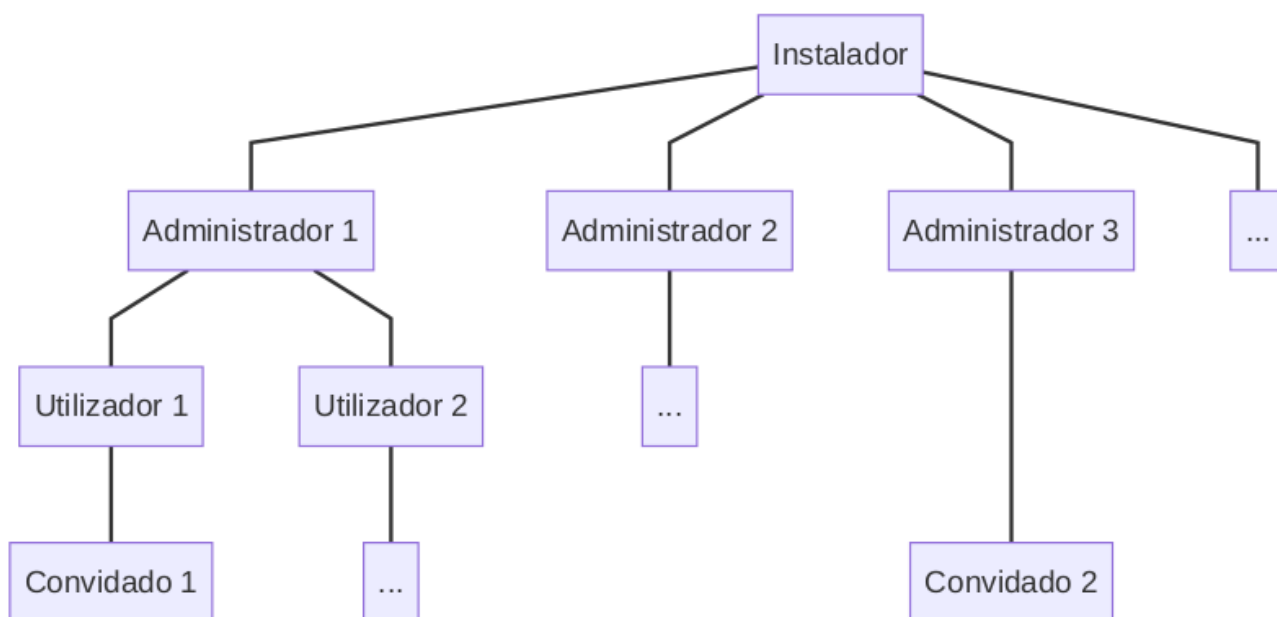
Outside that schedule, the operation is unavailable even if the profile has access to the device.

Operation restrictions are independent of restrictions assigned to the profile.

6.6. Profiles, hierarchy and dependent profiles

The W4A Key uses a hierarchy of profiles:

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



The Installer creates Administrator profiles.

Administrators can create User and Guest profiles.

Users can create Guest profiles when authorised.

A profile created by another profile is called a dependent profile.

The creating profile can manage its dependent profiles within its assigned permissions.

A profile cannot grant its dependent profiles permissions beyond its own.

6.7. Profile restrictions

A profile may be subject to:

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

- permission or no permission to use restricted operations;
- a limit on dependent profiles;
- a minimum traceability level.

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

Restrictions on dependent profiles are set by the creating profile and limited by that profile's permissions.

6.8. 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 Count accesses option is enabled.

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

Only one access is counted per connection to the device. Thus, if the user executes one or more access-counting operations several times without ending the connection, only one access is deducted.

Another access is counted after the connection ends and the profile reconnects to the device to execute an access-counting operation.

Example:

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

In this case, only one access is counted and four remain available.

Once the limit has been reached, the profile can no longer execute operations subject to access counting.

6.9. Traceability, credentials and sessions

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

Depending on the configured type, records may:

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

Credentials authenticate a profile and may include:

- a name or ID;

- a password;
- association text;
- a file;
- a QR code.

A session temporarily retains the profile's authentication 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.

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

6.10. 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 the device to be accessed over the Internet when the service is active and authorised.

Offline mode

Allows certain actions to be prepared in a file for later execution near the device.

The availability of each method depends on configuration, permissions and associated services.

6.11. History and records

The device can store records relating to:

- activations;
- creation of profiles;
- deletion of profiles;
- other management events.

The information available depends on:

- the profile type;
- the hierarchy;

- the configured traceability level;
- the records stored on the device.

The Installer can view the complete activation history without identifying the profiles that performed the activations.

History is intended for viewing and managing the system and does not replace certified surveillance, attendance or access control systems.

7. Associating a user profile

This procedure applies to the following profiles:

- Administrator;
- User;
- Guest.

Before starting, check:

- that you have received the access details;
- that the application is installed;
- that Bluetooth is enabled;
- that the mobile phone is near the device when association is performed locally.

7.1. Signing in and associating the profile

Signing in associates a profile previously created on the W4A Key with the application.

Association can be performed using:

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

To begin:

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 matching the details you received.

Access credentials

Use this method when you are given:

- the profile name or its identifier;
- the password.

To associate the profile:

Associating a user profile

1. select Sign in;
2. wait for the search for nearby devices;
3. select the intended W4A Key;
4. enter the profile name or identifier;
5. enter the password;
6. confirm sign-in.

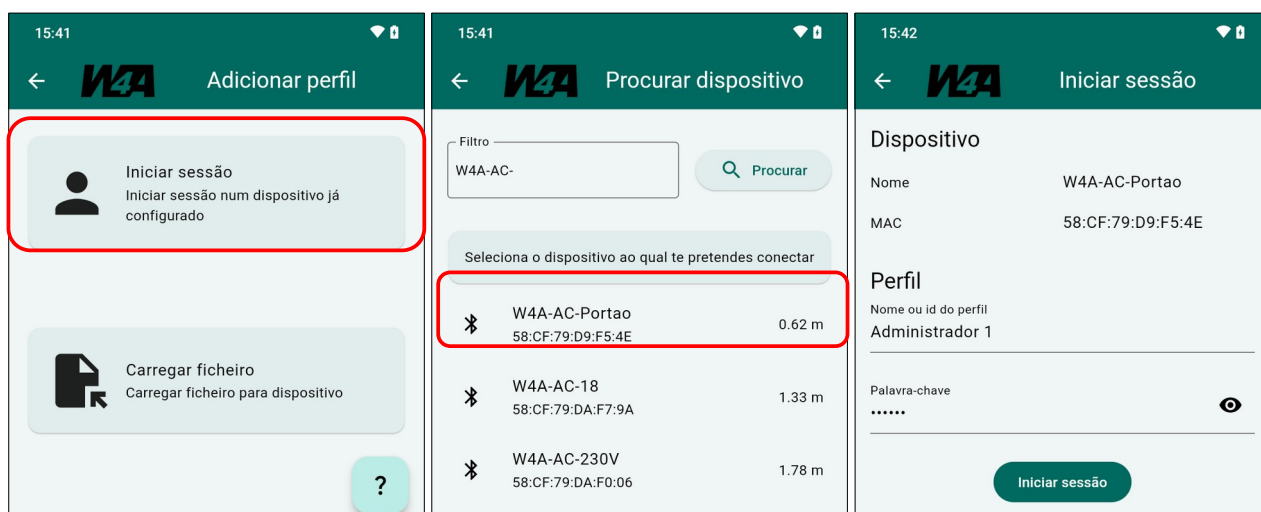
Identification may use:

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

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

The person who created the profile can view its ID in the list of dependent profiles.

If several devices are nearby, make sure you have selected the correct W4A Key before entering your credentials.



Text

Use this method when your association details are supplied in a text message.

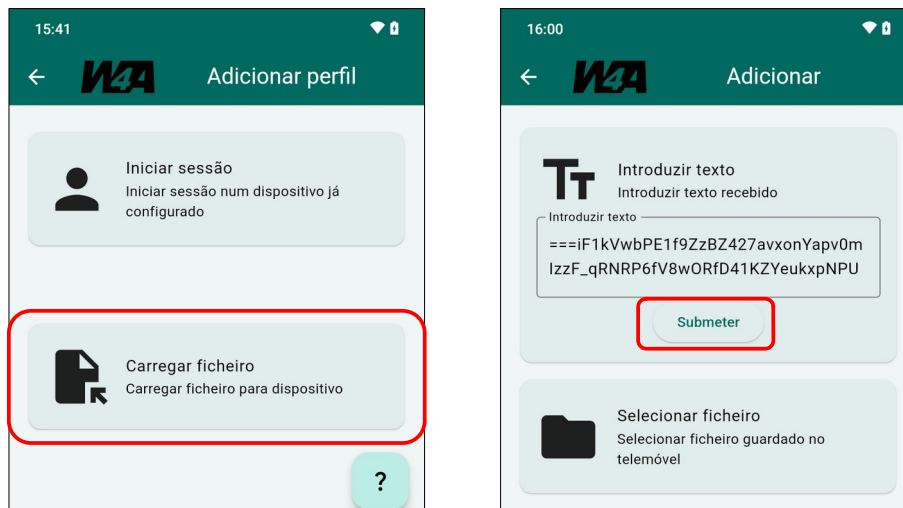
To associate the profile:

1. copy the entire 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 text you received;

6. confirm submission.

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

Incomplete or modified text may prevent association.



File

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

You can start association in either of the following ways:

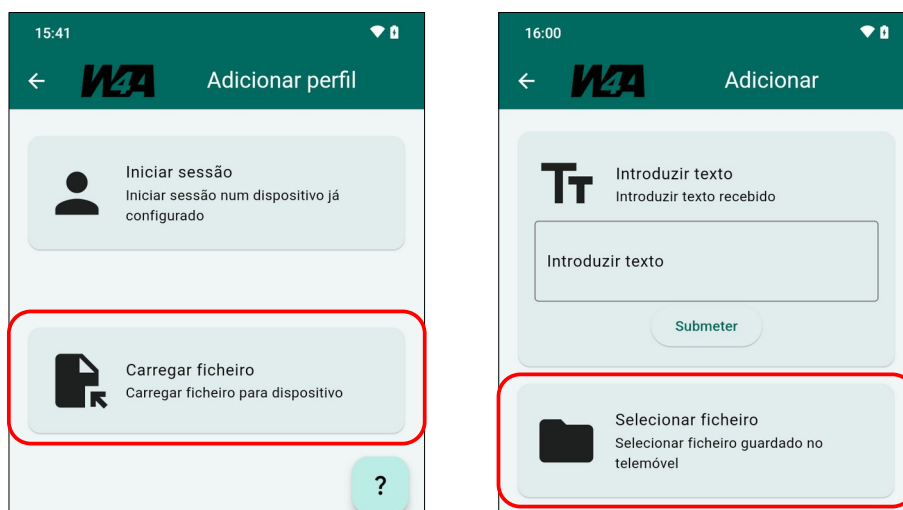
- open the file directly in the mobile phone's file manager and select the W4A Key application;
- open the W4A Key application, select Load file and choose the file you received.

To use the second method:

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

Do not change the file name, extension or contents.

After association, delete the file or store it in a protected location, in accordance with the applicable security rules.



QR code

Use this method when a QR code containing the association details is shown to you.

To associate the profile:

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

If the scanning application 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 contents;
5. confirm submission.

Do not photograph, publish or share the QR code with unauthorised people.

The code may contain information that allows the profile to be associated with the device.

7.2. Checking the association

After association, check:

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

- that communication can be established;
- that the available operations match the assigned permissions;
- that no error messages appear.

When prompted, replace the initial password with a secure personal password.

Do not share your password with anyone else.

7.3. Association not completed

If association cannot be completed, check:

- the details you received;
- the password;
- the profile type;
- your distance from the device;
- the Bluetooth status;
- the application permissions;
- whether the profile is valid.

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

- whether the profile is still active;
- whether the shared details are correct;
- whether there are date or time restrictions;
- whether the profile has been suspended or deleted.

After association, the profile is available for use through the application.

8. Managing the profile

The Information tab lets you view and change the details of the profile currently associated with the application.

8.1. Profile settings

The profile settings area may show the following parameters:

Name

Allows you to 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 7.1 Signing in and associating the profile.

This value is provided for information only and cannot be changed.

Type

Shows the profile type.

The profile type is set when the profile 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 profile above it in the hierarchy and may be available for viewing only.

Maximum session time

Allows you to set the maximum session inactivity period.

After the configured period has elapsed, the password must be entered again to communicate with the device.

Traceability permission

Allows you to select the profile's traceability type from the options authorised by its creator.

See Section 6.9 Traceability, credentials and sessions for an explanation of each option.

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

Password can be reset by creator

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

When this option is 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 this option only if you accept this possibility.

Press Submit to save your changes.

9. Device information and account security

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

The available options depend on the profile type and its permissions.

9.1. Device status

The displayed status is based on information received during the most recent communication with the device.

Clock status

If the clock reports an error, functions that depend on the date or time may become unavailable, including:

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

If a clock error is shown, follow the procedure in **Chapter 15** Troubleshooting.



Input and output states

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

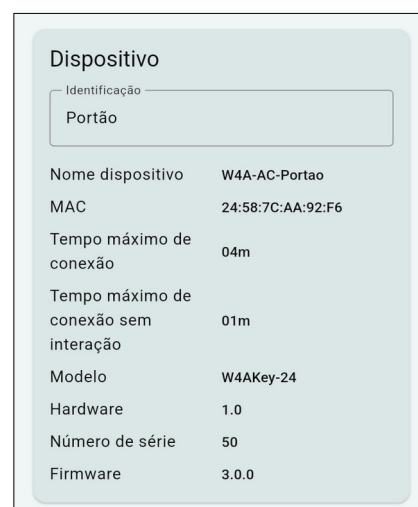
The information shown in the application does not replace direct inspection of the installation when this is necessary for safety.

9.2. 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 this information when diagnosing a fault.



Identification in the application

The identification setting lets you change the name under which the device appears on this mobile phone.

This change only helps organise the local application and does not necessarily change the name stored on the device or shown on other mobile phones.

Use a name that makes the equipment easy to distinguish from other associated devices.

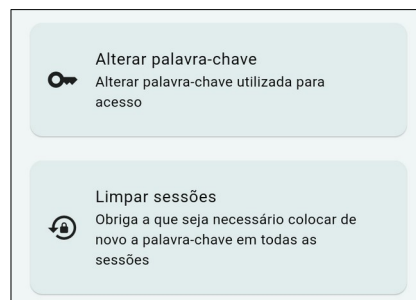
9.3. Passwords and sessions

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.

After the change, you may need to authenticate the profile again.



Clearing sessions

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

After this operation, you must enter the password again to communicate with the device.

You can use this option when:

- a mobile phone has been lost or replaced;
- you suspect unauthorised access;
- you want to end existing authenticated sessions.

9.4. Removing the profile

The application lets you choose between two types of removal.

Remove locally

Removes the profile only from the current mobile phone.

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

Remove from device

Removes the profile from the mobile 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 have to be created to grant access again.

If the profile has dependent profiles, these are also deleted and will lose access to the device.

10. Managing dependent profiles

10.1. Accessing dependent profiles

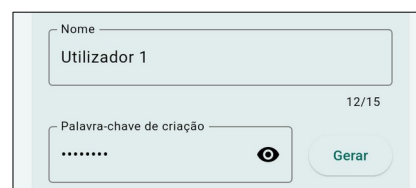
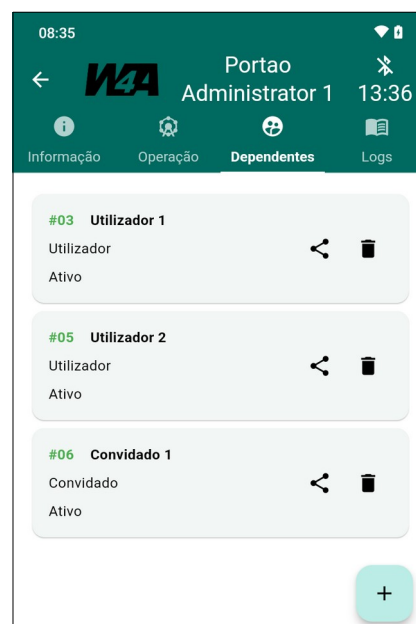
In the relevant profile, open the Dependents tab to view, create or manage profiles below it in the hierarchy.

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

10.2. Creating a dependent profile

To create a dependent profile:

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



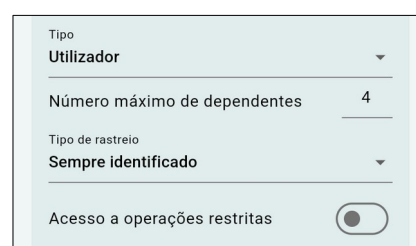
10.3. Dependent profile settings

Type

Selects the dependent profile type.

The available options depend on the profile creating it.

See Section 6.6 Profiles, hierarchy and dependent profiles for the functions and limitations of each profile type.



Maximum number of dependent profiles

Sets the maximum number of profiles that this dependent profile can create.

When this value is 0, the profile cannot add new dependent profiles to the device.

The maximum available number may be limited by the permissions assigned to the profile creating it.

Traceability type

Sets the minimum traceability level for the dependent profile.

The configured value also limits the options that this profile can assign to its own dependent profiles.
See Section 6.9 Traceability, credentials and sessions for the available options.

Access to restricted operations

Authorises the dependent profile to execute operations configured as restricted.

When this option is disabled, the profile cannot activate those operations.

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

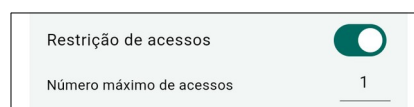
10.4. Access limit

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

Only operations configured to count accesses reduce the available number.

See Section 6.8 Counting accesses for how accesses are counted.

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



10.5. Time restrictions

Time restrictions limit a dependent profile's access according to dates and times.

Restrictions may include:

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

Configured restrictions apply cumulatively. A profile can access the device only when all active conditions are met.

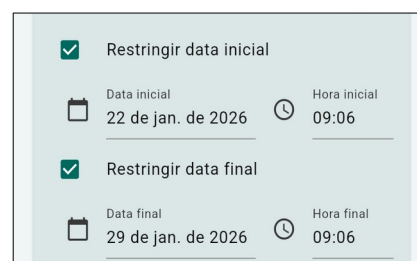
Start date

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

After enabling the option, set:

- the start date;
- the start time.

The profile can access the device only from the configured time onwards.



End date

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

After enabling the option, set:

- the end date;
- the end time.

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

Time schedule restriction

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

The settings include:

Available schedules

Allows you to create or define the time periods available for the restriction.

Each schedule must have:

- a start time;
- an end time.

Selected schedules

Allows you to assign the periods during which the dependent profile may access the device to each day of the week.

A day may:

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

The profile cannot access the device outside the selected periods.

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

10.6. Saving and sharing the profile

After configuring the dependent profile:

1. review its settings;
2. check its restrictions;
3. press Submit;
4. wait for confirmation;
5. check that the profile appears in the list of dependent profiles.

After creation, access details may be shared through the methods available in the application, including:

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

Share these details only with the authorised person.

The recipient should follow the procedure in Chapter 7 Associating a user profile.

10.7. Editing or deleting a dependent profile

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 profile has allowed its creator to reset its password, a new password can also be set here.

To delete a profile:

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

Before deleting, check:

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

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

11. Executing and configuring commands

11.1. Executing commands

Available commands are shown in the Home menu.

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

To execute a command:

1. open the Home menu;
2. find the command you want;
3. check that it matches the equipment you intend to control;
4. press the command;
5. monitor execution using the corresponding indicators.

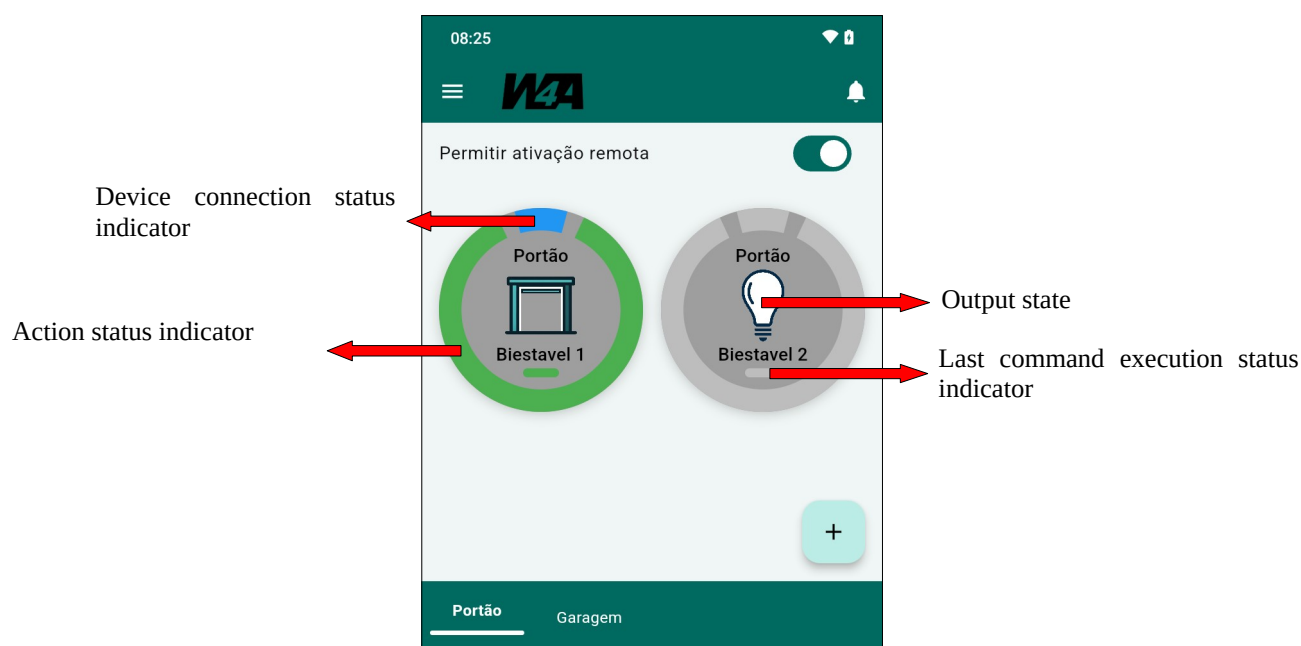
To cancel an ongoing activation, press and hold the command until the application indicates cancellation.

Cancellation depends on execution status and operation type. An operation already sent to the device may not be stopped in every situation.

WARNING — Local or remote activation

Before executing a command:

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



Connection status indicator

This indicator shows the search for and connection to the device while a command is being executed.

Colour	Display	Status
Grey	Solid	Command not executed
Blue	Flashing	The application is searching for the device and attempting to connect
Blue	Solid	Connection established with the device

Establishing a connection does not, by itself, mean that every action in the command has been executed.

Action status indicator

A command may contain one or more actions.

The application displays a section for each action so you can monitor its status individually.

Colour	Status
Grey	The action has not started
Blue	The action is running
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

When 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 behaviour.

Last command status indicator

This indicator shows the result of the most recent command execution.

Colour	Status
Grey	The status of the last execution is unknown
Green	The command was executed successfully
Yellow	The command was not completed because of a connection failure
Red	An error occurred during execution

The indicator shows the last known execution and does not prove the current state of the load.

Remote activation

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

Remote activation is available only when:

- the device has an active remote communication service;
- the device has Internet access;
- the mobile phone has Internet access;
- the profile is authorised to execute the operations;
- the command is authorised for remote activation.

When this option is disabled, the command's actions can be executed only through local communication.

11.2. Configuring commands

Commands are configured in the Commands menu.

This menu shows:

- the existing groups;
- the commands in each group;
- the display order of commands.

Groups correspond to pages in the Home menu.

To change a command's position within its 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 command, press + or the equivalent option.

Command configuration is divided into:

- identification;
- behaviour;
- 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 command names;
- unambiguous.

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

Group

Sets the group to which the command belongs.

The group determines the Home menu page where the command appears.

Icons

Allows you to select icons to:

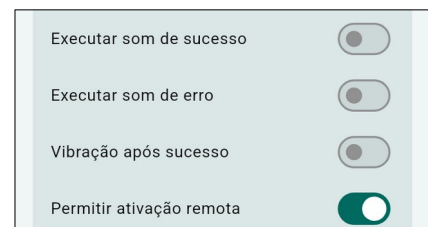
- identify the command;
- represent its inactive state;
- represent its active state, where applicable.

Icons help with visual identification and do not replace checking the actual equipment status.

Command behaviour

Play success sound

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



Play error sound

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

Vibrate after success

When enabled, the mobile phone vibrates after the command is executed successfully.

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

Allow remote activation

Allows the command's actions to be executed through remote communication.

When this option is disabled, actions are executed only over a local connection to the device.

This option does not enable the remote service on the W4A Key. 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 particular device.

A command may contain several actions, allowing a sequence involving:

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

For each action, configure the following settings:

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

Device

Select the device on which to execute the operation.

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

Operation

Select the operation to be executed on the chosen device.

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

Connection attempt timeout

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

If communication is not established within that time:

- the action is cancelled;
- the 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 may increase the wait before an error is shown.

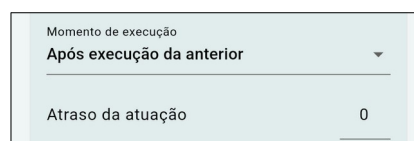
Connection time

Sets how long the application maintains the connection to the device.

This value must be long enough to complete the operation and receive confirmation.

Action sequence

When a command has more than one action, the start time of each subsequent action must be set.



The screenshot shows a configuration window with a light blue header and a white body. The header contains the text 'Momento de execução' and a dropdown menu with the selected option 'Após execução da anterior'. Below this, there is a label 'Atraso da atuação' followed by a text input field containing the number '0'.

At the same time as the previous action

The action starts at the same time as the previous action, or with the smallest difference allowed by the application and communication methods.

After the previous action is executed

The next action starts only when the previous action has been executed successfully.

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

After the previous action is executed or fails

The next action starts after the previous attempt ends, whether it succeeded or produced an error.

Use this option only if the next action can be executed safely even when the previous one has failed.

Activation delay

Sets the wait before the action starts.

The delay is counted from the execution time set for that action.

Before configuring a sequence:

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

Saving the command

After completing the configuration:

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

After saving, the command appears in the selected group in the Home menu.

Test the command before normal use, especially if it contains several actions or devices.

11.3. 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 on the application's In Car list appear in the vehicle. Users can add them manually, or they can be added automatically when the Installer has enabled Automatically make command available in 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 you want them to appear.

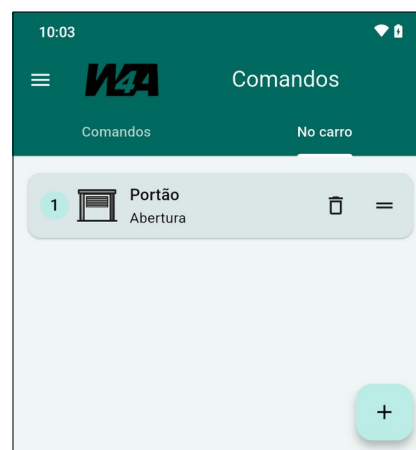
After configuration, the command will be available for display in the car, subject to platform and system compatibility.

Reordering or removing commands

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

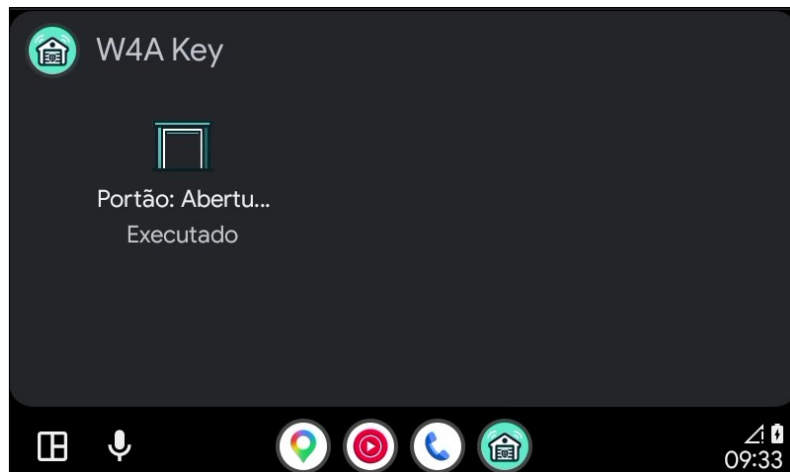
Removing a command from this list prevents it from appearing in the vehicle but does not delete it from the application's main command list.

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



Important notes

- The presentation, arrangement and number of visible commands may depend on platform or infotainment system limits.
- Some functions available in the mobile application may be unavailable in Android Auto or Apple CarPlay.



12. One-Time Access

One-Time Access provides temporary access to a device's authorised operations without permanently associating a profile with the application.

Use this function for a one-off activation on a particular device when you do not want the profile to remain available in the application for future use.

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

12.1. Signing in through One-Time Access

The sign-in process is similar to normal profile association.

The main difference is that you must start it 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 matching the details you received;
4. enter or load the access details;
5. select the intended device when prompted;
6. enter the password where applicable;
7. wait for profile validation and communication with the device.

Access details can be supplied through the same methods used for normal sign-in, including:

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

See Section 7.1 Signing in and associating the profile for information on these methods.

12.2. Using operations

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

To execute an operation:

1. check that the displayed device is correct;
2. select the desired operation;
3. make sure the activation can be performed safely;
4. press the corresponding command;

5. wait for the result.

WARNING — One-off activation

Before executing an operation, ensure that no people, animals or objects are in the movement or activation area of the controlled equipment.

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

12.3. Ending access

One-Time Access does not permanently associate 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 need to sign in again for another use;
- the details remain subject to the restrictions configured on the device.

If you intend to use the same profile regularly, follow the normal association procedure in Chapter 7 Associating a user profile.

13. Offline mode

Offline mode lets an authorised 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 subsequently executes it through the application when near the W4A Key.

This allows changes to be prepared and executed by different people at different times.

Offline mode can be used, for example, to:

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

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

13.1. How it works

The process has three stages:

1. an authorised profile prepares the actions in the application;
2. the application generates an offline file;
3. a person near 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 actions that are valid and authorised.

Each file has a unique identifier, which the device uses to distinguish between generated files.

13.2. Generating an offline file

To generate a file:

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

7. check the order of the actions;
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, check:

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

Generate a new file whenever you need to change an action or its settings.

13.3. Available actions

Available actions depend on profile type and permissions.

They may include:

Create a user

Prepares the creation of a new dependent profile.

Its settings may include the same parameters used for normal dependent profile creation.

This method can be used when the creator is not near the device.

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

Edit a user

Changes the settings of an existing profile.

Before generating the file, check the ID of the profile you want to edit.

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

Delete a user

Prepares the 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 it still needs access;
- whether it has dependent profiles;
- the impact of deletion.

Change or reset a password

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

Send the new password only to the authorised person.

Clear sessions

Invalidates a profile's existing sessions.

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

Invalidate a previous file

Prevents a previously generated offline file from being executed.

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

This action may be useful when:

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

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

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

13.4. Sending the file

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

Share it only with the person responsible for executing it.

Before sending it, check:

- the recipient's identity;
- the target device;
- the actions included;
- 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 unauthorised people.

13.5. Executing the file on the device

Execution must be performed by a person able to communicate with the W4A Key through a supported method.

To execute it:

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

or:

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

Then:

1. confirm the target device;
2. review the displayed actions, when available;
3. establish communication with 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.

13.6. Execution result

After execution, check:

- whether the file was accepted;
- whether all actions were completed;
- whether any action was rejected;
- whether a communication failure occurred;
- whether the procedure needs to be repeated or corrected.

A file may be rejected when:

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

Do not consider changes complete without confirmation from the application.

13.7. Limitations and security

Offline mode does not mean that actions are executed without communicating with the W4A Key.

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

The creator of the file is responsible for:

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

The person executing the file must:

- confirm the target device;
- not alter the file;
- 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.

14. History

14.1. Viewing history

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

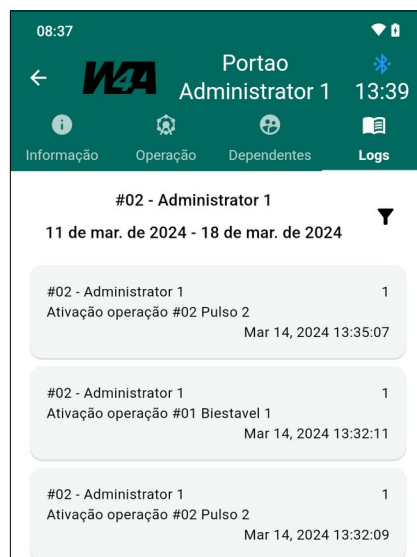
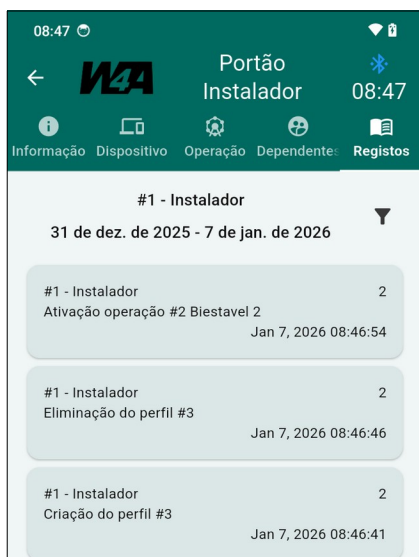
- operation activations;
- profile creation;
- profile deletion.

To view history:

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

The information shown depends on:

- the profile type;
- its hierarchical relationship to the profiles involved;
- the selected traceability type;
- the records still available on the device.



14.2. Activation history

Activation records may show:

- the date and time;

- the operation executed;
- the profile identity, where permitted by the traceability type.

User identification depends on the traceability setting of the profile concerned.

If traceability does not permit identification, the activation may still be recorded without being associated with the user's name.

14.3. Dependent profile history

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

Available information may include:

- activations performed;
- creation of dependent profiles;
- deletion of dependent profiles;
- the identity of the responsible profile, where permitted.

When the traceability type does not authorise identification, events may be shown without association with a particular profile.

A profile can view information only about its dependent profiles and only in accordance with its permissions.

14.4. Records visible to the Installer

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

Activations are shown without identifying the profiles that performed them.

The Installer can view:

- the activation date and time;
- the operation executed;
- the result;
- other technical information provided in the record.

This access helps verify the device's general operation without revealing users' identities.

14.5. Creation and deletion of profiles

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, if identifiable.

14.6. 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 reset.

A factory reset erases records stored on the device.

History is intended for viewing and managing the system and does not replace certified attendance, surveillance or proof-of-presence systems.

15. Troubleshooting

This section describes problems that may occur when installing, configuring or using the W4A Key, together with possible causes and recommended actions.

Before contacting technical support:

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

WARNING — Electrical hazard

Before performing any electrical check, changing wiring, tightening terminals or opening the enclosure:

- disconnect the power supply;
- isolate all energy sources;
- prevent accidental reconnection;
- confirm the absence of voltage;
- follow the applicable safety procedures.

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

Work on the electrical installation must be carried out by qualified personnel.

15.1. Troubleshooting table

Problem	Possible cause	Recommended action
The device does not turn on	No power supply	Check that the supply voltage is present at the designated terminals and check the external protective devices.
	Incorrect supply voltage	Check that the applied voltage is compatible with the installed model.
	Loose conductor, incorrectly connected terminal or tripped protective device	Disconnect 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 that the power supply is stable.
	Poor power connection	Disconnect and isolate the installation, then check the conductors and terminals.
	Electrical interference or	Check the separation between power and signal circuits and the

Troubleshooting

Problem	Possible cause	Recommended action
	disturbance	suppression devices used with loads.
The device operates intermittently	Unstable power supply	Check the supply voltage and protective devices.
	Poor connection	Check the terminals and wiring after disconnecting and isolating the power supply.
	Interference affecting inputs or communication	Check cable routing and move the device away from sources of interference.
Bluetooth communication cannot be established	Device out of range	Move the mobile phone closer to the W4A Key and reduce obstacles between them.
	Bluetooth disabled	Enable Bluetooth on the mobile phone.
	Application lacks permissions	Check Bluetooth, nearby devices and location permissions where required by the operating system.
	Another user connected	Wait for the existing connection to end, then try again.
	Outdated application	Update the application to a compatible 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, check that the mobile 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 status of the remote service.
	Device has no Internet access	Check the Wi-Fi connection and Internet access.
	Mobile phone has no Internet access	Check the mobile phone's 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 the authorised period or schedule	Check the restrictions assigned to the profile.
	Incomplete or modified association details	Request the access details again.
Cannot associate a profile	Wrong device selected	Check the W4A Key identification.
	Invalid access details	Check the text, file, QR code or credentials you received.
	Communication failure	Move the mobile phone closer and repeat the procedure.
An input does not change state	Incorrect connection	Check the contact connection to the common terminal and corresponding input.

Troubleshooting

Problem	Possible cause	Recommended action
	Faulty external contact	Check the connected button, switch, relay or sensor.
	Input disabled or configured incorrectly	Review the input settings.
An input changes state erratically	Poor connection	Check terminal tightness and wiring condition.
	Electrical interference	Keep input cables away from power cables and sources of interference.
	Faulty external contact	Check or replace the external contact.
An output does not activate	Operation configured for another output	Review the operation settings.
	Operation inactive	Enable the operation and submit the configuration again.
	Input preventing activation	Check the input status and settings.
	Interlocking active	Check the status of the other outputs.
	Profile or schedule restriction	Check the applicable permissions and restrictions.
	Device error	Check the LED and restart only when safe.
The application indicates that the output was activated, but the load does not work	Fault in the external circuit	Disconnect and isolate the power supply, then check the wiring, protective devices and controlled equipment.
	External load power supply missing	Check the controlled circuit's power supply.
	Auxiliary relay or contactor fault	Have qualified personnel inspect it.
The load activates unexpectedly	Active input, operation or sequence	Check the status and settings of inputs and operation sequences.
	Command executed by another user	Review the available history.
	Fault in the external circuit	Disconnect and isolate the installation immediately and request help from qualified personnel.
An operation is not executed	Incorrect configuration or configuration not submitted	Review the settings and confirm that the application reported a successful save.
	Restricted operation	Check that the profile is authorised to use restricted operations.
	Profile outside the authorised period	Check the configured dates and times.
	No accesses remaining	Check the number of available accesses.
	Another incompatible operation is running	Wait for completion or execute the stop operation, where applicable.
A command shows a connection failure	Communication could not be established within the configured time	Move the mobile phone closer, check communication and review the connection attempt timeout.
A command shows an activation error	Operation rejected or failed during execution	Check the status of each action and the applicable restrictions.
An action sequence does not complete	The previous action ended with an error	Check when the next action is configured to run.

Problem	Possible cause	Recommended action
	Wrong device or operation	Review the command's actions.
	Timeout or connection time too short	Adjust the configured times.
The date or time is incorrect	Incorrect region or time zone	Correct the region and time zone.
	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 times	Check the configured values.
History does not identify the user	Traceability type does not allow identification	Check the traceability type assigned to the profile.
	History viewed by the Installer	The Installer views activations without user identification.
An offline file is not accepted	File intended for another device	Check the target device.
	File modified or damaged	Request a new file.
	File invalidated	Contact the file creator.
	Profile or authorisation no longer valid	Check the profiles involved 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.
The LED flashes rapidly	Device in error mode	Put the installation in a safe state, restart the device and check whether the error remains.

15.2. General checking procedure

If the cause is not immediately clear:

1. identify the status shown in the application;
2. check the LED;
3. read the error messages;
4. review the history around the time of the event;
5. check the date and time;
6. confirm which profile was used;
7. check permissions and restrictions;
8. check the input and output states;
9. confirm that the configuration was submitted;
10. check the communication method;

11. perform only permitted electrical checks and do so safely.

Do not change several settings at the same time while diagnosing a problem.

Make one change at a time and check the result.

15.3. Restarting the device

A restart may help when there is a temporary communication or operating fault.

Before restarting:

- make sure the load can safely stop or remain in its current state;
- make sure any behaviour after restart will not create a hazard;
- record any existing error messages;
- check whether a configuration transfer is in progress.

To restart by switching off the power:

1. disconnect the power supply using the appropriate disconnecting device;
2. confirm the absence of voltage;
3. wait a few seconds;
4. restore the power supply;
5. wait for start-up to finish;
6. check the date and time;
7. check the states and settings;
8. test only the functions needed.

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

15.4. When to contact the Installer for a device reset

A factory reset may be considered when:

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

A reset should not be the first measure used to correct:

- power supply failures;
- incorrect wiring;
- faulty loads;

- failures of external relays or contactors;
- poor Bluetooth or Wi-Fi coverage;
- incorrectly entered credentials;
- profile or operation restrictions.

Before considering a reset, identify and correct any electrical, mechanical or communication problems.

Contact the Installer to perform the factory reset.

15.5. When to stop using the device

Stop using the device immediately if there is:

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

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

Do not use the equipment again until the cause has been identified and corrected by qualified personnel.

15.6. 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 under which it occurs;
- the LED status;
- messages shown by the application;
- relevant configuration details;
- photographs of the installation and wiring;
- the electrical diagram used;
- a screenshot or description of the history, if available.

Do not send passwords, QR codes, association files, offline files or other credentials unless technical support expressly requests them.

16. Regulatory compliance

16.1. 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 entity responsible for issuing the declaration.

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

16.2. EU Declaration of Conformity

The complete EU Declaration of Conformity is available at:

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

Consult the declaration for the relevant product model and version.

16.3. Restriction of hazardous substances

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

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

16.4. Changes to the equipment

Any unauthorised change 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;

Regulatory compliance

- make the equipment unsuitable for use.

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

17. Disposal and end of life

17.1. Disposal 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 adverse environmental effects;
- reduce risks to human health;
- enable materials recovery;
- promote sustainable use of resources.

17.2. Private users

Private users should contact:

- the retailer where they purchased the product;
- municipal services;
- an authorised collector of waste electrical and electronic equipment;
- another competent body in their country.

These organisations can provide information about collection locations and procedures.

17.3. Professional users

Professional users should contact the supplier or an authorised organisation to confirm the applicable collection and treatment arrangements.

Do not dispose of the product with unsorted commercial waste.

17.4. Internal battery

The internal battery must be removed and sent for appropriate treatment by authorised personnel in accordance with applicable legislation.

Do not dispose of the battery:

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

- with the equipment without checking local requirements.

Handle a damaged, deformed or leaking battery with care and deliver it to an authorised organisation.

17.5. Erasing data

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

1. record any data you wish to keep;
2. contact the Installer to perform a factory reset;
3. remove profiles from the application where applicable;
4. delete association or offline files that are no longer needed.

The Installer must perform the factory reset in accordance with the Installation and Configuration Manual.

18. Warranty, responsibility and support

18.1. User and Installer responsibilities

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 practice.

The Installer is responsible for checking that the product is suitable for the installation, connecting and configuring it correctly, and performing tests before commissioning.

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

18.2. Improper use

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

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

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

18.3. Limitations of communication, status and records

Communication may be affected by distance, obstacles, interference, network failures or temporary service unavailability.

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

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

- physical safety devices;
- certified systems;
- checks performed by qualified personnel.

18.4. Warranty

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

The warranty may not cover damage caused by:

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

The warranty terms must be interpreted in accordance with applicable legislation.

18.5. Technical support

Before contacting technical support, consult Chapter 15 Troubleshooting.

If the problem persists, contact W4A and, where possible, provide the information listed in Section 15.6 Contacting technical support.

Do not send passwords, QR codes, association files or other credentials unless technical support expressly requests them.