



W4AKey

Configuration guide

Practical cases for user management



Contents

1. About this guide.....	3
2. Managing access in a family home.....	6
3. Managing access in a residential building.....	9
4. Managing access in holiday accommodation or rented premises.....	12
5. Managing access in a company, office or shop.....	15
6. Managing access for a cleaning team.....	18
7. Managing access for a maintenance technician.....	20
8. Managing access for a supplier or one-off provider.....	22
9. Removing a profile and protecting an account.....	24
10. Replacing the Administrator in charge.....	26

1. About this guide

This guide presents practical examples of managing users and access on W4A Key.

The cases are organized around real situations, such as:

- a family home;
- a residential building;
- holiday accommodation or rented premises;
- a company, office or shop;
- cleaning;
- maintenance;
- suppliers and service providers.

Each case sets out, where applicable:

- the profiles involved;
- who should create each profile;
- recommended permissions;
- access restrictions;
- access to restricted operations;
- the expected outcome.

This guide does not replace the **W4A Key Instruction Manual**.

1.1. Profile hierarchy

W4A Key uses the following profile types:

- **Installer:** configures the device and creates Administrator profiles;
- **Administrator:** uses the device and creates or manages User and Guest profiles;
- **User:** performs the operations available on the device and may create Guest profiles when authorized.
- **Guest:** has limited, temporary or occasional access.

The Installer does not directly create User or Guest profiles.

A profile cannot grant its dependents permissions greater than its own.

1.2. General rules for creating profiles

An individual profile should be created for each person.

Do not reuse the same profile for different users.

When creating a profile, check:

- the profile type;
- the name;
- the maximum number of dependents;
- the tracking type;
- access to restricted operations;
- the dates and times, where applicable;
- the maximum number of accesses, where applicable.

1.3. Normal and restricted operations

Operations are configured on the device and made available to users according to their respective type and status.

An operation can be defined as:

- **unrestricted**, when profiles with normal access to the device can perform it;
- **restricted**, when only profiles authorized to access restricted operations can perform it.

The profile's **Access to restricted operations** setting determines whether that user can perform operations marked as restricted.

This option can be used, for example, to limit:

- the full opening of a gate;
- access to a technical area;
- control of equipment;
- operations reserved for persons in charge;
- actions that should not be available to all users.

Defining an operation as restricted applies to all profiles. The difference between users depends on the authorization granted to each profile.

1.4. Counting accesses

The maximum number of accesses applies only to operations with **Access counting** enabled.

One access is counted per connection to the device, even if the operation is performed several times during that connection.

This option should be used for operations that actually represent an entry or access.

Operations such as lighting, stopping or auxiliary controls should not normally reduce the number of available accesses.

1.5. Sharing and linking

After creating the profile:

1. check the configured permissions and restrictions;
2. generate the linking method provided by the app;
3. send it only to the authorized person;
4. confirm that the profile has been linked correctly;
5. delete any sharing messages, files or codes that are no longer needed.

1.6. Changing and removing profiles

Profile permissions should be updated whenever the conditions of use change.

The profile should be removed when:

- the person no longer needs access;
- a contract or service ends;
- a booking ends;
- misuse is suspected.

After removing it, confirm that the user can no longer access the device.

2. Managing access in a family home

2.1. Purpose

This case shows how to organize access to a family home, with one person responsible for managing the device and individual profiles for the other family members.

2.2. Profiles used

The recommended configuration is:

- an **Administrator** profile for the homeowner or person responsible for the home;
- a **User** profile for each adult or permanent resident;
- a **Guest** profile for family members, visitors or service providers with temporary access.

The Installer profile creates the Administrator.

The Administrator creates the required User and Guest profiles.

2.3. Homeowner or responsible person's profile

Parameter	Homeowner
Profile type	Administrator
Name	Name of the homeowner or person responsible
Maximum number of dependents	Based on the number of users to be managed
Tracking type	According to the established policy
Access to restricted operations	As needed

The homeowner can use the device and manage the profiles of the other family members.

2.4. Profiles for permanent residents

Create an individual User profile for each resident.

Parameter	Permanent resident
Profile type	User
Name	Resident's name
Maximum number of dependents	0, unless allowed to create Guests
Tracking type	According to the established policy
Access to restricted operations	As needed
Time restriction: Start date	Disabled or specified date
Time restriction: End date	Disabled or specified date

If the resident is not authorized to create Guests, set the maximum number of dependents to **0**.

Access to restricted operations should be enabled only for residents who need to perform those operations.

2.5. Profiles for family members or temporary visitors

Create an individual Guest profile for each person with temporary access.

Parameter	Family member or visitor
Profile type	Guest
Name	Person's name
Tracking type	According to the established policy
Access to restricted operations	Normally no
Access restriction: Maximum number of accesses	Disabled or specified value
Time restriction: Start date	Start of the authorized period
Time restriction: End date	End of the authorized period
Time restriction: Restrict daily	As needed

Use the maximum number of accesses when you want to limit the permitted number of entries.

Use the daily restriction when access should only be available at certain times of day.

This profile can be used for visiting relatives, caregivers, service providers or others who do not need permanent access.

2.6. Restricted operations

Common household operations can remain unrestricted when all users may perform them.

Operations such as the following can be defined as restricted:

- opening a garage;
- accessing a technical area;
- controlling equipment;
- operations reserved for the homeowner.

The **Access to restricted operations** permission should be enabled only for profiles that need this capability.

2.7. Verification

1. link each profile to the respective user;
2. confirm that residents can use the device during the configured period;
3. check that only authorized profiles can perform restricted operations;

4. test the dates, times and number of accesses for Guest profiles;
5. confirm that each person uses their own profile.

2.8. Expected outcome

The homeowner or person responsible manages access to the home through an Administrator profile.

Each permanent resident has an individual User profile.

Family members, visitors and service providers receive Guest profiles limited by date, time or number of accesses, as needed.

3. Managing access in a residential building

3.1. Purpose

This case shows how to organize access in a residential building, distinguishing between:

- the person responsible for management;
- apartment owners or residents;
- permanent staff;
- temporary service providers.

3.2. Profiles used

The recommended configuration is:

- an **Administrator** profile for the building manager or designated person in charge;
- a **User** profile for each apartment owner, resident or permanent staff member;
- a **Guest** profile for cleaning or maintenance companies, suppliers or other temporary providers.

The Installer profile creates the Administrator.

The Administrator creates the required User and Guest profiles.

3.3. Building manager's profile

Parameter	Building manager
Profile type	Administrator
Name	Name of the manager or person responsible
Maximum number of dependents	Based on the number of users to be managed
Tracking type	According to the established policy
Access to restricted operations	As needed

The Administrator is responsible for creating, changing and removing the other profiles.

3.4. Profiles for apartment owners or residents

Create an individual User profile for each apartment owner or resident.

Parameter	Apartment owner or resident
Profile type	User
Name	Person's name or apartment identifier
Maximum number of dependents	0 or specified value

Managing access in a residential building

Tracking type	According to the established policy
Access to restricted operations	Normally no
Time restriction	Disabled

Set a maximum number of dependents greater than 0 only if the apartment owner is authorized to create Guest profiles.

3.5. Profiles for permanent staff

A User profile can be created for people who need regular access, such as:

- a doorman;
- a caretaker;
- a maintenance employee;
- a permanent building staff member.

Parameter	Permanent staff member
Profile type	User
Name	Staff member's name
Maximum number of dependents	Normally 0
Tracking type	According to the established policy
Access to restricted operations	According to the role
Time restriction: Start date	Start of employment
Time restriction: End date	No limit or expected end date

3.6. Profiles for service providers

Create a Guest profile for companies or people with temporary access.

Parameter	Service provider
Profile type	Guest
Name	Name of the person or company
Tracking type	According to the established policy
Access to restricted operations	Normally no
Access restriction: Maximum number of accesses	Disabled or specified value
Time restriction: Start date	Start of the authorized period
Time restriction: End date	End of the authorized period
Time restriction: Restrict daily	According to the service days and hours

This profile can be used for:

- cleaning;

- maintenance;
- gardening;
- inspections;
- deliveries;
- other temporary services.

3.7. Restricted operations

Operations for shared use can remain unrestricted.

Operations such as the following can be defined as restricted:

- opening technical areas;
- accessing restricted areas;
- controlling shared equipment;
- operations reserved for the manager or authorized staff.

The **Access to restricted operations** permission should be enabled only for profiles that need this capability.

3.8. Verification

1. confirm that each apartment owner or resident has an individual profile;
2. check that only authorized profiles can create dependents;
3. test providers' access during the authorized period;
4. confirm that restricted operations are unavailable to unauthorized profiles;
5. remove providers' profiles when the service ends.

3.9. Expected outcome

The building manager manages access profiles through an Administrator profile.

Apartment owners, residents and permanent staff use individual User profiles.

Service providers use Guest profiles limited by date, time or number of accesses.

4. Managing access in holiday accommodation or rented premises

4.1. Purpose

This case shows how to manage access for guests or tenants for a defined period without granting permanent permissions.

4.2. Profiles used

The recommended configuration is:

- an **Administrator** profile for the owner or property manager;
- a **User** profile for permanent staff, where necessary;
- an individual **Guest** profile for each guest or tenant.

The Administrator creates the Guest profiles needed for each booking or contract.

4.3. Owner or manager's profile

Parameter	Owner or manager
Profile type	Administrator
Name	Name of the owner or manager
Maximum number of dependents	Based on the number of profiles to be managed
Tracking type	According to the established policy
Access to restricted operations	As needed

The owner or manager retains permanent control of the device and temporary access.

4.4. Guest or tenant's profile

Create an individual Guest profile for each booking or user.

Parameter	Guest or tenant
Profile type	Guest
Name	Person's name or booking reference
Tracking type	According to the established policy
Access to restricted operations	Normally no
Access restriction: Maximum number of accesses	Disabled or specified value
Time restriction: Start date	Check-in date and time
Time restriction: End date	Check-out date and time

Managing access in holiday accommodation or rented premises

Time restriction: Restrict daily	Normally disabled
----------------------------------	-------------------

The start and end dates should match the actual booking or contract period.

The maximum number of accesses can remain disabled when the guest needs to enter several times during the stay.

4.5. Permanent staff

If staff members need regular access, such as receptionists or property managers, create an individual User profile.

Parameter	Permanent staff member
Profile type	User
Name	Staff member's name
Maximum number of dependents	0 or specified value
Tracking type	According to the established policy
Access to restricted operations	According to the role
Time restriction: Start date	Start date of the role
Time restriction: End date	No limit or specified date

Set a maximum number of dependents greater than 0 only if the staff member is authorized to create Guest profiles.

4.6. Cleaning or maintenance team

Create a Guest profile when access is temporary or limited by time of day.

Parameter	Cleaning or maintenance
Profile type	Guest
Name	Name of the person or company
Tracking type	According to the established policy
Access to restricted operations	Normally no
Access restriction: Maximum number of accesses	Disabled or specified value
Time restriction: Start date	Start of the authorized period
Time restriction: End date	End of the authorized period
Time restriction: Restrict daily	According to the service schedule

4.7. Verification

1. confirm that the profile dates match the booking or contract;

2. test access during the authorized period;
3. confirm that access stops working after the end date;
4. check daily restrictions, where used;
5. remove profiles that are no longer needed.

4.8. Expected outcome

The owner or manager retains permanent access through an Administrator profile.

Each guest or tenant uses a Guest profile valid only for the authorized period.

Access for cleaners, maintenance personnel and other providers is limited by the configured dates, times or number of accesses.

5. Managing access in a company, office or shop

5.1. Purpose

This case shows how to organize access for staff, managers and service providers in a business premises.

5.2. Profiles used

The recommended configuration is:

- an **Administrator** profile for the person in charge of the premises;
- a **User** profile for each staff member with regular access;
- a **Guest** profile for service providers, suppliers or temporary visitors.

The Installer creates the first Administrator.

The Administrator creates the required User and Guest profiles.

5.3. Person in charge's profile

Parameter	Person in charge
Profile type	Administrator
Name	Name of the person in charge
Maximum number of dependents	Based on the number of users to be managed
Tracking type	According to the established policy
Access to restricted operations	According to the role

The person in charge manages access for staff and service providers.

5.4. Staff profiles

Create an individual User profile for each staff member with regular access.

Parameter	Staff member
Profile type	User
Name	Staff member's name
Maximum number of dependents	Normally 0
Tracking type	According to the established policy
Access to restricted operations	According to the role
Time restriction: Start date	Start date of the role
Time restriction: End date	No limit or expected end date

Set a maximum number of dependents greater than 0 only if the staff member is authorized to create Guest profiles.

Access to restricted operations should be granted only to managers, supervisors or staff members who need those operations.

5.5. Profiles for service providers and visitors

Create a Guest profile for people with temporary access.

Parameter	Provider or visitor
Profile type	Guest
Name	Name of the person or company
Tracking type	According to the established policy
Access to restricted operations	Normally no
Access restriction: Maximum number of accesses	Disabled or specified value
Time restriction: Start date	Start of the authorized period
Time restriction: End date	End of the authorized period
Time restriction: Restrict daily	According to the authorized schedule

This profile can be used for:

- cleaning;
- maintenance;
- suppliers;
- deliveries;
- consultants;
- visitors;
- temporary workers.

5.6. Restricted operations

Operations such as the following can be defined as restricted:

- accessing warehouses;
- opening technical areas;
- controlling equipment;
- operations reserved for managers.

The **Access to restricted operations** permission should be enabled only for profiles that need those operations.

5.7. Verification

1. confirm that each staff member has an individual profile;
2. check contract dates or temporary roles;
3. test providers' access during the authorized period;
4. confirm that only authorized profiles perform restricted operations;
5. remove the profile when the employment relationship or service ends.

5.8. Expected outcome

The person in charge manages access through an Administrator profile.

Each staff member has an individual User profile.

Service providers and visitors use Guest profiles limited by date, time or number of accesses.

6. Managing access for a cleaning team

6.1. Purpose

This case shows how to create access for a cleaner or cleaning team that needs to use the device only during certain periods.

It can be applied in homes, residential buildings, holiday accommodation, offices, shops or other premises.

6.2. Profile used

Use a **Guest** profile when access is limited by dates, times or number of accesses.

The profile must be created by the Administrator or by a User authorized to create Guests.

An individual profile should be created for each person who needs access.

6.3. Profile configuration

Parameter	Cleaning team
Profile type	Guest
Name	Person's name
Tracking type	According to the established policy
Access to restricted operations	Normally no
Access restriction: Maximum number of accesses	Disabled or specified value
Time restriction: Start date	Start of the service period
Time restriction: End date	End of the service period
Time restriction: Restrict daily	Enabled, according to the cleaning schedule

For recurring services, the start and end dates can cover the entire contract period.

The daily restriction should match the periods during which cleaners are authorized to enter.

The maximum number of accesses can remain disabled if multiple entries are needed during each service visit.

6.4. Restricted operations

Access to restricted operations should remain disabled unless the team needs to perform a specific operation marked as restricted.

Where possible, the operations needed for the team's entry should remain unrestricted.

6.5. Verification

1. check the start and end dates;
2. test access during the authorized hours;
3. confirm that access does not work outside those hours;
4. check the maximum number of accesses, where used;
5. remove the profile when the service ends.

6.6. Expected outcome

Each cleaning team member has an individual Guest profile.

Access is available only during the defined period and hours and does not allow restricted operations unless specifically authorized.

7. Managing access for a maintenance technician

7.1. Purpose

This case shows how to create temporary access for a technician who needs to enter the premises for maintenance, repair or inspection work.

It can be applied in homes, residential buildings, holiday accommodation, companies, shops or technical facilities.

7.2. Profile used

Use a **Guest** profile.

The profile must be created by the Administrator or by a User authorized to create Guests.

An individual profile should be created for each technician.

7.3. Profile configuration

Parameter	Maintenance technician
Profile type	Guest
Name	Technician's name or work reference
Tracking type	According to the established policy
Access to restricted operations	According to the work required
Access restriction: Maximum number of accesses	Specified value or disabled
Time restriction: Start date	Expected start of the work
Time restriction: End date	Expected end of the work
Time restriction: Restrict daily	According to the authorized schedule

Use a maximum number of accesses when the work requires only a limited number of entries.

If the technician needs to enter several times during the authorized period, the limit can remain disabled.

7.4. Restricted operations

Enable **Access to restricted operations** only if the technician needs to perform an operation marked as restricted.

This may be needed, for example, to:

- access a technical area;
- open a service gate;
- control equipment;

- enter a restricted area.

If it is not needed, leave the option disabled.

7.5. Verification

1. confirm the technician's identity;
2. check the start and end dates;
3. test access during the authorized period;
4. confirm that restricted operations can be performed only when authorized;
5. remove the profile when the work is complete.

7.6. Expected outcome

The technician has a Guest profile valid only for the duration of the work.

Access is limited by the configured dates, times and number of accesses and may include restricted operations only when necessary.

8. Managing access for a supplier or one-off provider

8.1. Purpose

This case shows how to create temporary access for someone who needs to enter once or a few times for a delivery, collection, supply visit or other one-off service.

It can be applied in residential buildings, companies, shops, warehouses, accommodation or rented premises.

8.2. Profile used

Use a **Guest** profile.

The profile must be created by the Administrator or by a User authorized to create Guests.

An individual profile should be created for each person who needs access.

8.3. Profile configuration

Parameter	Supplier or one-off provider
Profile type	Guest
Name	Name of the person, company or service reference
Tracking type	According to the established policy
Access to restricted operations	Normally no
Access restriction: Maximum number of accesses	Low value, according to the service
Time restriction: Start date	Start of the authorized period
Time restriction: End date	End of the authorized period
Time restriction: Restrict daily	According to the planned schedule

The maximum number of accesses should match the number of entries expected for the service.

If access is needed only once, set the limit to one access.

8.4. Restricted operations

Keep **Access to restricted operations** disabled unless the service requires a specific operation marked as restricted.

8.5. Verification

1. confirm the identity of the authorized person;
2. check the date, time and maximum number of accesses;
3. test the profile during the authorized period;

4. confirm that access stops working when the limit is reached;
5. remove the profile when the service ends.

8.6. Expected outcome

The supplier or provider has a Guest profile valid only during the defined period.

Access is limited by the configured schedule and maximum number of accesses.

9. Removing a profile and protecting an account

9.1. Purpose

This case shows how to remove access that is no longer needed or protect an account when a mobile phone is lost.

It can be applied, for example, when there is:

- the end of a contract;
- the departure of a staff member;
- the completion of a service;
- the cancellation of a booking;
- misuse;
- the loss of a mobile phone.

9.2. Removing the profile

Remove the profile when the person permanently stops needing access.

Before removing it, check:

- the user's identity;
- which profile should be removed;
- whether the profile has dependents.

When a profile is deleted, all dependent profiles created by it are deleted as well.

Before confirming deletion, check whether those dependents still need access. If necessary, new profiles should be created by another Administrator or authorized User.

9.3. Replacing a mobile phone

Replacing a mobile phone does not require a new profile, provided the user knows their account credentials.

The user should:

1. install the app on the new mobile phone;
2. sign in with their existing credentials;
3. confirm that the devices and profiles are still available;
4. test communication with the device.

The profile and its permissions remain linked to the account.

9.4. Losing a mobile phone

If a mobile phone is lost:

1. install the app on another mobile phone;
2. sign in with the account credentials;
3. use the option to clear existing sessions;
4. confirm that the previous sessions have ended;
5. test access to the device again.

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

This procedure prevents a session previously opened on the lost phone from being used without fresh authentication.

9.5. Verification

After removing a profile

1. confirm that the profile no longer appears in user management;
2. confirm that its dependents have also been deleted;
3. check whether new profiles must be created for those people;
4. confirm that the previous access no longer works.

After losing a mobile phone

1. confirm that the sessions have been cleared;
2. check that the password is requested again;
3. test communication on the new mobile phone;
4. confirm that the profiles and devices remain linked to the account.

9.6. Expected outcome

When a profile is deleted, its access and all its dependents are removed.

When a mobile phone is replaced under normal circumstances, the user keeps the same profile by signing in with their credentials.

If a mobile phone is lost, clearing sessions requires fresh authentication before communicating with the device.

10. Replacing the Administrator in charge

10.1. Purpose

This case shows how to replace the person responsible for managing the device's users.

This may be necessary, for example, following:

- a change of owner;
- a change in the manager of accommodation;
- a change in the management of a residential building;
- a change in the person in charge of a company;
- the end of the current Administrator's duties;
- the need to transfer management to someone else.

10.2. Creating the new Administrator

The **Installer** profile must create a new **Administrator** profile for the person taking over management.

Configure the profile with the following parameters:

Parameter	New person in charge
Profile type	Administrator
Name	Name of the new person in charge
Maximum number of dependents	As needed
Tracking type	According to the established policy
Access to restricted operations	According to the role

The new Administrator should link the profile to their account and confirm that they can communicate with the device.

10.3. Checking existing dependents

Before deleting the previous Administrator, identify all dependent profiles that must remain active.

These may include, for example:

- User profiles for residents or staff;
- Guest profiles for guests;
- cleaning access;
- maintenance access;

- temporary access that is still valid.

Deleting an Administrator always deletes all their dependent profiles.

Profiles are not automatically transferred to the new Administrator.

10.4. Recreating the required profiles

The new Administrator must recreate all profiles that need to remain active.

When recreating each profile, check:

- the name;
- the profile type;
- the maximum number of dependents, where applicable;
- the tracking type;
- access to restricted operations;
- the start and end dates;
- the maximum number of accesses, where applicable;
- the daily restriction, where applicable.

The respective users should link the new profiles before the previous Administrator is deleted.

10.5. Deleting the previous Administrator

Delete the previous Administrator only after:

1. creating and linking the new Administrator;
2. recreating the profiles that must remain active;
3. confirming that the new profiles have been linked;
4. testing users' access;
5. checking that every required dependent has been recreated.

Deleting the previous Administrator also deletes all their dependents.

10.6. Verification

1. confirm that the new Administrator can communicate with the device;
2. check that they can create and manage dependents;
3. test the new User and Guest profiles;
4. confirm access to restricted operations, where authorized;
5. delete the previous Administrator;

6. confirm that the old profiles and their dependents have been removed;
7. check that only the new profiles remain active.

10.7. Expected outcome

The new person in charge has an active Administrator profile and takes over management of the device's users.

Profiles that need to remain active are recreated and linked before the previous Administrator is deleted.

After deletion, the previous Administrator and all their dependents no longer have access to the device.