WHISPLI

WHISPLI CASE MANAGEMENT · USER GUIDE

Case Manager Guide

Handle a report from receipt to archiving, in complete confidentiality.

AUDIENCE

Case managers (Member role)

CASE MANAGER GUIDE

Contents

How to use this guide 3

01 Your role and your obligations 4

02 Getting to know your workspace 7

03 Anatomy of a report 10

04 Communicating with the informant 13

05 Collaborating internally 15

06 Investigating the case 18

07 Closing, archiving, retaining 21

08 Checklist: good habits 23

09 Glossary and help 24

How to use this guide

This guide is for **case managers** — the people in charge of receiving, investigating and closing reports in the **Whispli Case Management** platform. It follows the life cycle of a report: from your first sign-in through to archiving.

Each chapter can be read on its own. Numbered steps indicate an order to follow; the boxes highlight what deserves particular attention.

GOOD TO KNOW
A detail or tip that saves time.

DEPENDING ON YOUR CONFIGURATION
A behaviour that depends on your organisation's settings.

CAUTION
A point where a mistake can expose information.

SECURITY
A rule that protects the confidentiality of people and data.

COMPLIANCE
A reminder of the legal obligations that frame case handling.

Interface labels

Menu, tab and button names are given **as they appear in the English interface**, for example `Submit`. The glossary, in chapter 9, maps the platform terms. The screenshots come from a demonstration environment: their content is fictitious.

This guide and your configuration

Whispli is configured organisation by organisation: statuses, workflows, automations, roles and optional features (Tasks, Participants, automatic translation…). This guide describes the **standard behaviour**. When a behaviour depends on your settings, a **Depending on your configuration** box says so. If in doubt, ask your Whispli Administrator or your Customer Success Manager.

CHAPTER 01

Your role and your obligations

Handling a report means guaranteeing three things at once: meeting deadlines, absolute confidentiality and full traceability. Whispli is designed to help you do this.

The case manager in Whispli

In Whispli, the case manager accesses the reports assigned to them, conducts the investigation and communicates with the informant through secure messaging. Case managers usually have the **Member** role: they see the reports of which they are the **owner** or a member, whether they were added manually or by an automation, as well as — depending on your organisation's configuration — reports that do not have an owner yet, which they can take ownership of.

On a report they have access to, a Member can, among other things, view the content, communicate with the informant, fill in workflows, write notes, add files, tags, tasks and participants, change the status and add other members.

Role (name in the interface)	What it allows, in short
Member	Handles the reports they are linked to. The usual role of a case manager.
Administrator (restricted)	Administration rights, but access limited to the reports they are a member or owner of and to reports without an owner; can lock a report.
Administrator	Access to all reports and all settings; can lock a report.
Guest	Temporary access to a single report, limited to the sections shared with them.

DEPENDING ON YOUR CONFIGURATION

Your organisation can create custom roles (for example without access to the Tasks tab, or with read-only access to it). The rights described here are those of the standard roles.

The legal deadlines to keep in mind

Regulations set deadlines for responding to the informant. They set the pace of your case handling.

7 DAYS — Acknowledge receipt

The person who made the report is informed of its receipt within seven days. In France: in writing, seven working days from receipt.

→

3 MONTHS — Provide feedback

The person is informed of the measures envisaged or taken, no later than three months after the acknowledgement of receipt — or three months and seven days after the report, if no acknowledgement was sent. In France: in writing; the seven days are working days.

Directive (EU) 2019/1937, art. 9 · France: Decree No. 2022-1284 of 3 October 2022, art. 4

> **COMPLIANCE**
>
> The applicable deadlines depend on the law of the country concerned and on your organisation's internal procedure. Check with your compliance officer which deadlines apply to you and how the acknowledgement of receipt is sent in your organisation.

Confidentiality: what the informant sees of you

The informant sees **neither your name nor your photo**: instead, they see your organisation's logo and name. Nor do they see the notes, the tags, the owner and members of the report, or its internal name. Chapter 3 details what is visible to them.

Securing your access

Recognising a genuine Whispli notification

Whispli email notifications are sent by **noreply@whispli.com** and their subject begins with "*You have a new notification on Whispli for...*".

- They **contain no link** to the platform: the address is displayed as an image. This is a security measure against phishing.
- They **contain no content** from the report: no message, no case details. They only invite you to sign in. Notifications set up by your Administrators in automations, however, may contain custom text.

> **SECURITY**
>
> An email that presents itself as a Whispli notification **and contains a link** to access the platform should make you suspicious: do not click, and bookmark your platform's address in your browser instead. The only exception: the invitation sent to a **guest** contains a direct access link (chapter 5).

Enabling two-factor authentication (2FA)

Every user can enable two-factor authentication on their account, except users who sign in with SSO (whose authentication is managed by their organisation).

1. Open `Settings` › `Profile`, then the `Two-factor Auth` tab.
2. Turn on the **Enable Two-factor authentication** toggle, then enter your password.
3. On your phone, open an authenticator app (for example Google Authenticator), add an account with **+** and scan the QR code shown on screen.
4. Keep the **secret code** provided: it will let you recover your access if you lose your phone.
5. Enter the six-digit code shown by the app. It changes every 30 seconds: if it is rejected, wait for the next one.

Once 2FA is enabled, each sign-in asks for your email, your password, then the code from the app.

CHAPTER 02

Getting to know your workspace

Home page, reports list, notifications and reminders: the essentials to know so that no case is left unanswered.

The home page

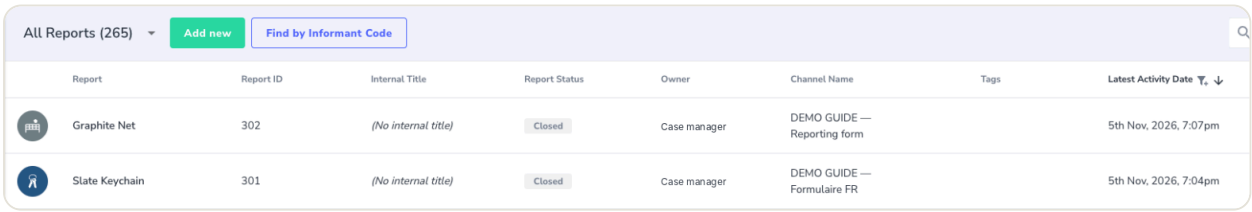
The Home page brings together the key information on the reports assigned to you. The left menu gives access to the different sections of the platform: Reports, Participants, Projects, Analytics and Settings.

- **Click a value or a chart** to display the list of the corresponding reports, then refine it with the filters.
- **Click the name or ID** of a report to open it.

> **DEPENDING ON YOUR CONFIGURATION**
>
> Each home page can be customised: yours may differ from a colleague's. Customisation is done from the **Analytics** section. As a Member, your charts only reflect the reports you have access to.

The reports list

The Reports section lists the reports you have access to: as a Member, only those of which you are the owner or a member. The columns give the essentials of each case: name, ID, internal name, status, owner, channel, tags, date of latest activity.



The Reports list, here with two demonstration reports. The menu next to "All Reports" gives access to deleted reports (chapter 7).

- **Filter** on a column, for example the ID to find the latest report received.
- **Search** with the magnifying glass icon, by report name or ID.

Notifications

Your notifications are under the **bell icon**, at the top right. A red badge shows the number of unread notifications.

1. Click the bell to see the latest notifications, each with a link to the report concerned.
2. Click `See all` to display the full list in full screen.
3. Filter by type of action, by the user who triggered the notification or by period. Unread notifications appear in blue, read ones in white.

When are you notified?

You receive a notification, in particular, when:

- you are assigned to a report or a project (as owner, member or through a user group), or removed from a report;
- the informant sends a new message or a file;
- you or your group are mentioned in a note;
- a new file is added to a report;
- a task is assigned to you;
- a report you are linked to is locked or unlocked;
- an automation sends a message to owners, members or designated users;
- the Snooze on a report reaches its due time.

You choose which email notifications you receive in `Settings` › `Notifications`, using the toggles. By default, they are all enabled.

> **DEPENDING ON YOUR CONFIGURATION**
>
> Custom notifications created by your Administrators (for example an alert if a report stays in the "New" status beyond a set time) cannot be disabled.

Snooze: scheduling a reminder

The `Snooze` button does not mute the report: it schedules a **personal reminder**. During the chosen period, you keep receiving all the report's notifications (messages, status changes, mentions).

1. Open the report and click `Snooze`, at the top right.
2. Choose when: for example Tomorrow, This Weekend, Next Week or a custom date and time.
3. When it is due, you receive a notification in Whispli and, depending on your notification preferences, an email.

Snooze is specific to each user: each team member sets their own reminders, and the same menu lets you cancel it. It is useful for following up a case awaiting information, for regular reviews or for reviewing an archived report **before its retention period expires**.

Projects

A **project** lets you group several related reports (same incident, same site, same topic) in a shared workspace. As with reports, you only see the projects of which you are the owner or a member; a Member can create a project and link reports to it.

CHAPTER 03

Anatomy of a report

A report is a complete case file: the initial account, the exchanges, the investigation, the people involved and the history of every action. Each tab has a specific purpose — and a specific visibility.

The tabs of a report

The tabs of a report, in the order of the interface. The badge shows those the informant also sees.

01 **Overview**

Status, details, internal name, members, tags, workflows and projects.

02 **Report**

The initial report, as submitted. Translation settings.

VISIBLE TO THE INFORMANT

03 **Chat**

The secure, anonymous dialogue with the informant.

VISIBLE TO THE INFORMANT

04 **Notes**

Internal exchanges between members, with mentions and threads.

05 **Workflows**

The steps of the investigation and their progress.

06 **Participants** OPTIONAL

The people involved: implicated persons, witnesses, victims...

07 **Members**

Who has access to the report: members, groups, guests.

08 **Tasks** OPTIONAL

Assigned investigation actions, with due date and priority.

09 **Files**

All documents, by section of origin and in folders.

10 **Activity**

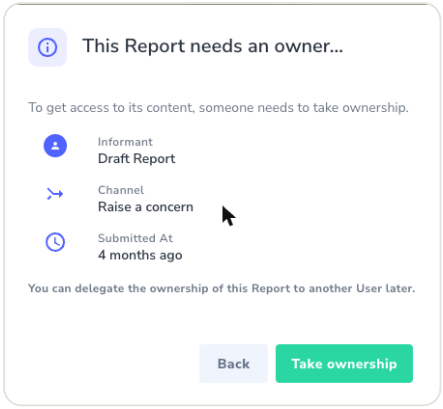
The report's activity and audit history.

Opening a new report

A report that has just arrived does not always have an owner. In that case, opening it displays a dialog: **this report needs an owner**, and someone must take ownership to access its content. The dialog shows the informant's pseudonym, the channel used and the time of submission.

1. Click **Take ownership** to take charge of the case.
2. Or click **Back** if the case should go back to a colleague.

You can delegate the report to another user later (chapter 5).



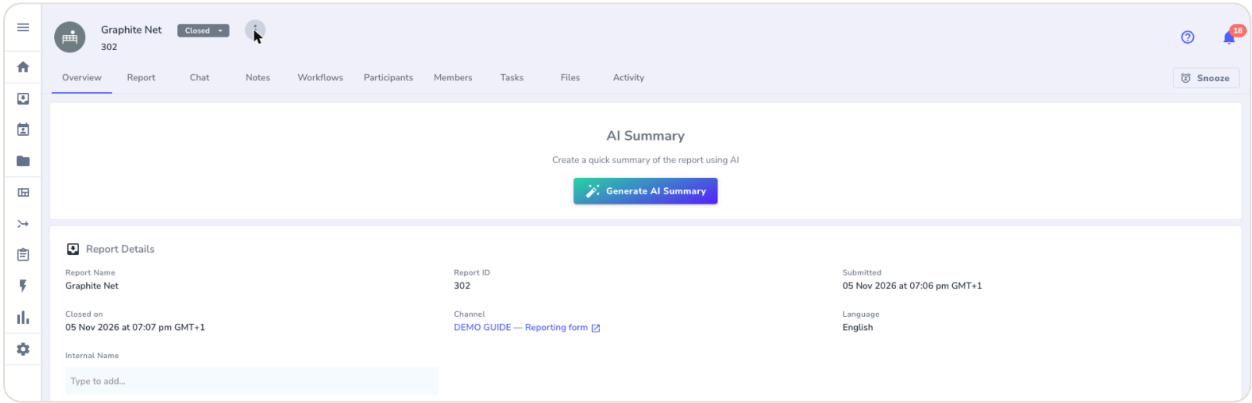
The "This Report needs an owner..." dialog: you must take ownership to open the report.

> **DEPENDING ON YOUR CONFIGURATION**
>
> Often, an automation assigns the owner as soon as the report is received: the report then opens directly.

The Overview tab

This is the first view when you open a report. It contains:

- at the top, the report's **status** and the ··· menu of actions on the report;
- the **report details**: name, ID, date received, communication channel, language;
- an **internal name**, which you can add if needed — the informant does not see it;
- the **members**, **tags**, applied **workflows**, **linked reports** and **projects**, each with an **Add** button.

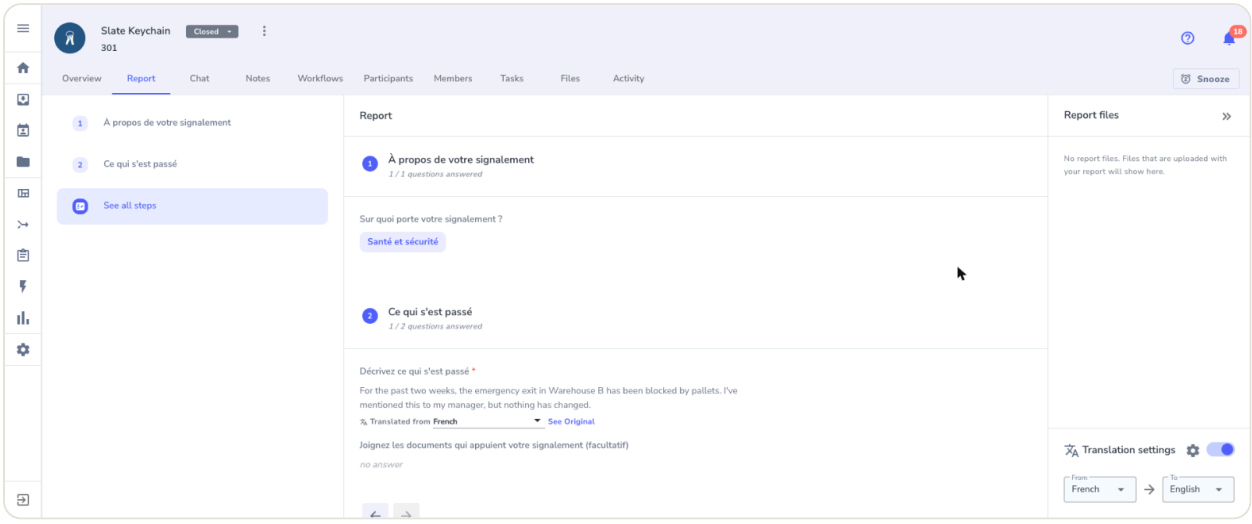


The Overview tab of a demonstration report.

> **DEPENDING ON YOUR CONFIGURATION**
>
> If the feature is enabled, a **Generate AI Summary** button offers a quick summary of the report at the top of the tab.

The Report tab and translation

The **Report** tab contains everything the informant initially submitted, step by step. When the report is written in another language, open the **Translation settings** panel, at the bottom right, and choose the target language. Each translated answer is marked "Translated from…", with a See Original link.



The Report tab: a report written in French, translated into English ("Translated from French · See Original").

Who sees what?

This is the question to ask yourself **before every piece of writing and every file you post**. The informant only sees two sections: their initial report and the Chat. To keep a document in the case file without passing it on to them, post it in the **Notes**, a **workflow** or a **custom folder** in the Files tab — never in the Chat.

	Informant	Owner and members	Guest
Initial report (Report)	● Yes	● Yes	◐ Yes (by default)
Chat: messages and files	● Yes	● Yes	◐ If shared, read-only
Notes	○ No	● Yes	◐ If shared; can contribute if allowed
Workflows and their files	○ No	● Yes	◐ If shared
Participants	○ No	● Yes	◐ If shared, read-only (if the feature is enabled)
Tasks	○ No	● Yes	○ No
Custom folders (Files)	○ No	● Yes	◐ If shared

A guest can never communicate with the informant. The informant sees neither the tags, nor the owner and members, nor the internal name.

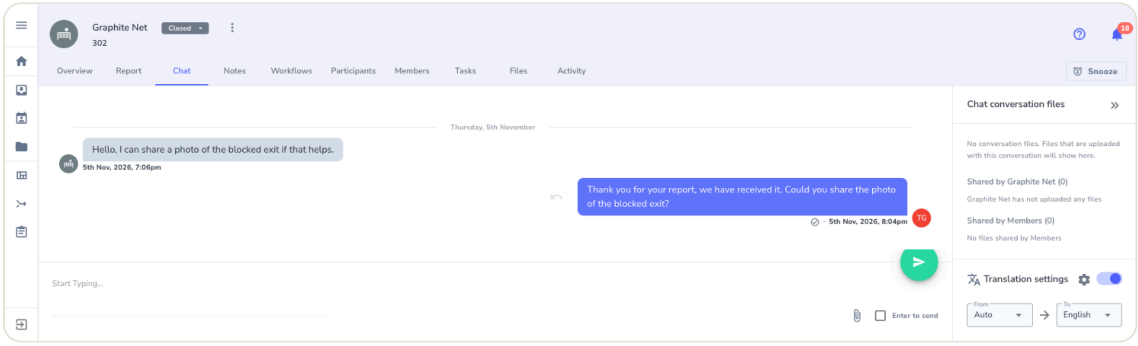
CHAPTER 04

Communicating with the informant

The Chat is the space for dialogue with the informant in Whispli. It protects your identity, lets the informant remain anonymous if they wish, and keeps a record of every exchange.

Sending a message or a file

1. Open the report's **Chat** tab. A banner reminds you that the messages sent here are addressed to the person who submitted the report.
2. Write your message, then click the **green button** to send it. Tick **Enter to send** if you prefer to send with the Enter key.
3. To attach a document, click the **paperclip icon**. You can send as many files as needed.



The Chat: the informant's message on the left, the case manager's reply on the right, the "Chat conversation files" panel on the right.

The informant receives the message in their secure Whispli inbox. If they have linked an email address to it or use the mobile app, they are notified. They can also send you messages and files.

> **GOOD TO KNOW**
>
> Your initials appear next to your messages, but **only for you and your colleagues**. The informant sees your organisation's name and logo, never your identity.

Knowing whether your message has been read

An icon appears under each message sent. Hover over it to see the delivery date. When it is **green**, the informant has signed in and viewed the message: the date and time it was read appear on hover.

Retracting a message sent by mistake

A message can be retracted at any time, even if the informant has already read it.

1. Click the **arrow** next to the message.
2. Enter the **reason for retracting it**, which the system requires for traceability.

The message then appears struck through for you and for all members. The informant only sees a notice stating that the sender removed the message. A file sent by mistake can also be retracted.

Translating the conversation

The **Translation settings** panel, at the bottom right, lets you turn on translation and choose the languages (**From** → **To**). The informant's messages are then displayed translated into the chosen language. Translation is an option enabled by your organisation: if the panel does not appear, contact your Whispli Administrator.

Finding the files exchanged

All the files shared in the Chat are grouped in the **Chat conversation files** panel, on the right, under two headings: those shared by the informant and those shared by members. They also appear in the **Files** tab, Chat section.

> ! **CAUTION**
>
> Everything posted in the Chat is **visible to the informant**. Internal documents go in the Notes, a workflow or a custom folder in the Files tab.

After closure and archiving

In progress

CHAT OPEN

Two-way exchanges. The informant is notified if they have linked an email address or use the app.

Closed

CHAT OPEN

The informant is notified of the closure. Exchanges remain possible.

Archived

CHAT CLOSED

Communication cut off. The informant can reread their report and download it as a PDF.

Deleted

CHAT CLOSED

The report disappears from the informant's inbox.

CHAPTER 05

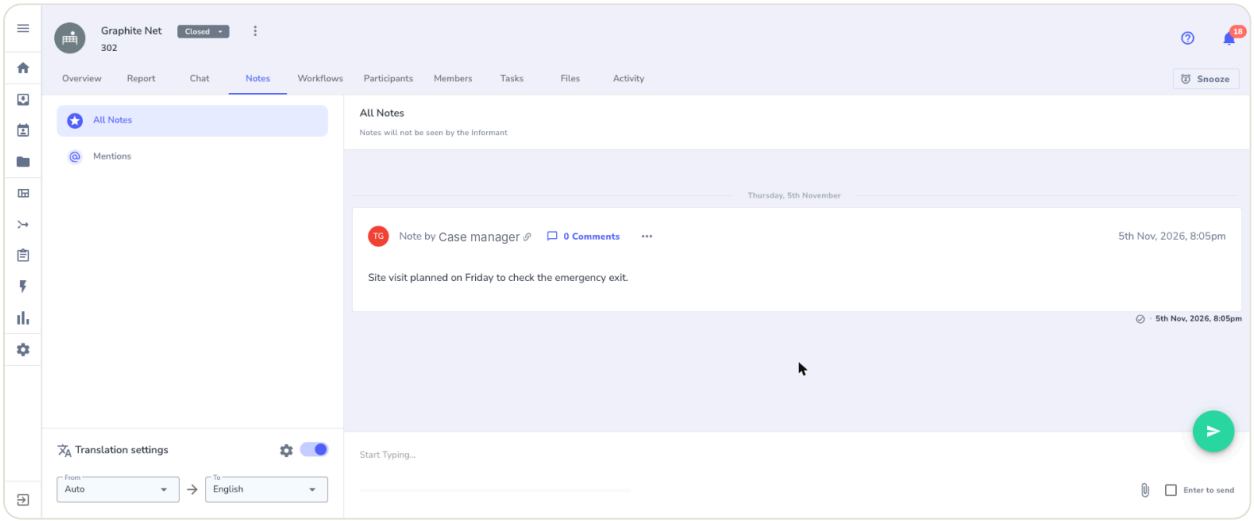
Collaborating internally

Notes, members, guests and tasks: everything that lets you work as a team on a case, without information ever leaving the platform.

Notes: the team's discussion space

The **Notes** tab is an open discussion area between the report's members: messages, files, threads. **Notes are never visible to the informant.** All members of the report see them, even when a note is addressed to a specific person.

1. Write your note, then click the **green button** to send it.
2. Type **@** to mention a member or a user group of the report. The **Mentions** view, on the left, groups the notes that mention you.
3. To open a thread, click the **number of comments** under a note: a panel opens on the right.



The Notes tab: an internal note, its comment count and its read icon.

The read icon. Under each note, an icon stays grey as long as no other user has seen the note, then turns green. On hover, it shows the date of posting and the date it was first read.

Retracting a note. A note is not deleted but retracted — and only its author can do so, through the ⋯ menu. A reason is required for the audit trail. For the author, the note appears struck through and greyed out; for others, it is replaced by a retraction notice. Replies in the thread remain visible, unless their authors retract them.

> **WITHOUT A MENTION, NO ONE IS ALERTED**
>
> A new note only shows a red badge on the Notes tab. For your colleagues to receive a notification (by email and in the application), **mention them with @**. The email does not include the content of the note.

The report's members

The **Members** tab lists everyone who has access to the report, how they were added and their role. The **User groups** and **Guests** views show the groups and guests with access. Click `Add members` to add individual members or entire groups.

Changing the owner

- **You are the owner**: in the Members tab, click ⋯ at the end of your row to change the owner. Choose the new owner and decide whether you remain a member or leave the report.
- **You are an Administrator or Administrator (restricted)**: click ⋯ next to the status, at the top of the report, then `Change owner`. You can also assign yourself; the previous owner then remains a member.

Sharing a report with a guest

When someone outside the platform needs to view a case (lawyer, expert...), **choose guest access over sending it by email**. Guest access is temporary, limited to a single report and fully logged in the audit trail.

1. In the **Members** tab, click `Add members`, then `Invite a guest`.
2. Search for an existing guest, or enter the name and email of a new guest. Enter the **reason for the invitation**, then click `Next`.
3. Set an **expiry date**. You can also make access expire automatically when the report's status changes.
4. Tick the **sections** the guest will be able to view and, if needed, allow them to reply and post files in the Notes.
5. Send the invitation.

The guest receives an email containing a direct link. This link **only works on the first device** that uses it: if forwarded or intercepted, it does not work. In the Members tab, the guest appears greyed out, pending, until they have opened the link, then **Active**. The ⋯ menu lets you change their rights, resend the invitation or revoke access at any time.

> **SECURITY**
>
> A guest can **never** communicate with the informant. They do not see tasks. Exporting a report as a PDF (`Export as PDF`) exists for specific needs (legal proceedings, for example), but by default it is reserved for Administrators.

Tasks

The **Tasks** tab is used to allocate and track investigation actions (interviews, requests for analysis...) and corrective measures.

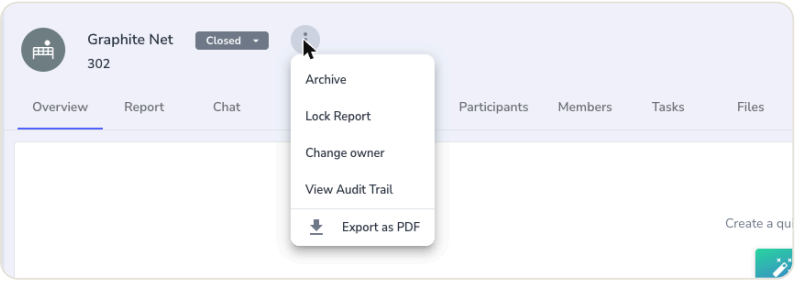
1. Click `Create Task`.
2. Fill in the title (required), the status, the person responsible for the task (you, by default), the priority, the due date, the type and the description. You can attach as many files as needed.
3. Click `Create Task`: the assignee is notified automatically.

- **Who can be assigned?** The interface offers a member of the report, a user group or yourself. The Help Center specifies that it must be a licensed user with active access to the report: guests cannot be assigned.
- **Task types.** These are tags: if the type you want does not exist, type it to create it.
- **Tracking.** An overdue task is flagged and its date is shown in red. A quick filter shows only the tasks assigned to you; each column can be sorted and filtered.
- **Editing.** Click a task's title to open and edit it; its history is available through ···. Any member of the report can delete a task, after a warning message.
- **Visibility.** Tasks are visible to all licensed members of the report — not to guests, the informant or participants. Their attachments also appear in the Files tab, **Tasks** section.

> **DEPENDING ON YOUR CONFIGURATION**
>
> Tasks are an optional feature. If the tab does not appear, contact your Customer Success Manager or support@whispli.com. Assignment and overdue reminders can be turned off by each user in their notification settings.

Sensitive cases: locking

For a conflict of interest or a highly sensitive case, an **Administrator** or an **Administrator (restricted)** can lock the report (··· menu next to the status, then `Lock Report`). No one else can access it any more, not even its owner or members: the report appears with a padlock and opening it displays an error message.



The report's ··· menu, here on a closed report: Archive appears because the report is at an end status (chapter 7).

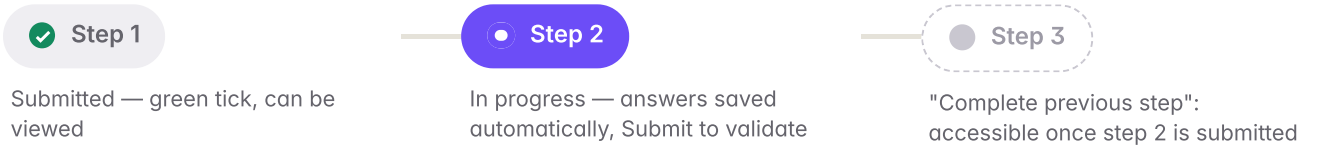
CHAPTER 06

Investigating the case

The workflow structures the investigation, participants document the people involved, files gather the evidence and the Activity tab keeps track of everything.

Workflows: the backbone of the investigation

Workflows reflect the investigation procedure defined by your organisation. The **Workflows** tab shows those applied to the report (**Current** section) and those that are finished (**Previous** section). Each workflow is divided into successive **steps**, with a progress counter (for example 1/2).

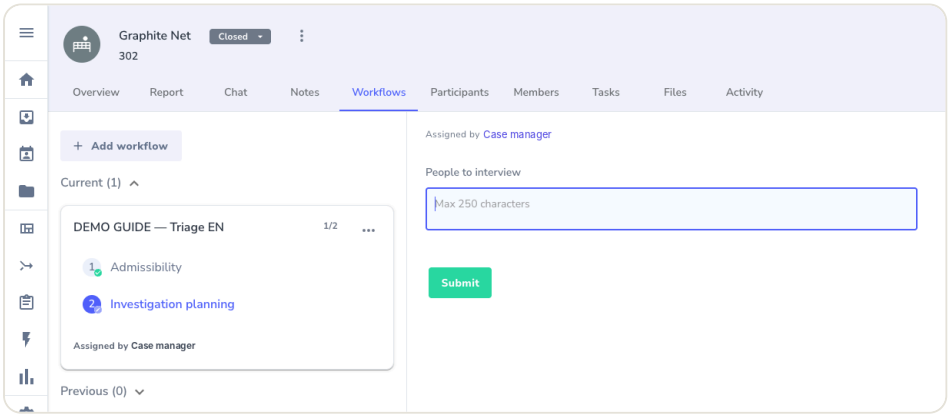


Submitted — green tick, can be viewed

In progress — answers saved automatically, Submit to validate

"Complete previous step": accessible once step 2 is submitted

1. Open the **Workflows** tab, then click the current step.
2. Answer the questions. Your answers are **saved automatically** as you type.
3. Click Submit to validate the step. An unanswered required question prevents you from submitting it.
4. The submitted step is marked with a **green tick**. You can reopen it to reread your answers and, if needed, correct them and submit the step again.



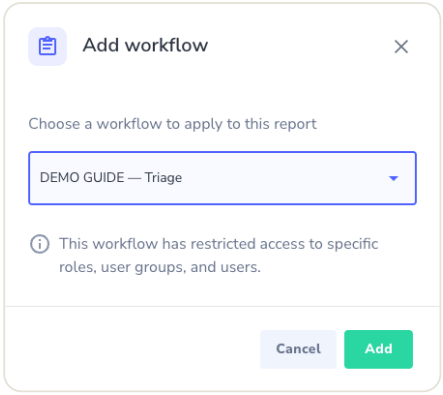
A workflow in progress: step 1 (Admissibility) is submitted, step 2 (Investigation planning) is open.

A step only becomes accessible once the previous one has been submitted: otherwise, the interface displays "Complete previous step". Finished workflows remain viewable and time-stamped: the history of the investigation is kept.

Adding a workflow

Workflows are usually added **automatically** by automations. You can also add one with Add workflow, then choose the one to apply — for example if the nature of the report turns out to differ from what was declared.

A **restricted** workflow is reserved for certain roles, user groups and users; it is tagged "Restricted". People without access see it locked, without its content. Its files are only visible to authorised people — and, as with any workflow, **never to the informant**.



The Add workflow dialog: this workflow has restricted access.

DEPENDING ON YOUR CONFIGURATION

Depending on the settings, adding a workflow or your answers can trigger automations: status updated, next workflow added, members notified. Using several different workflows in parallel on the same report is usually enabled by the Whispli team.

Participants: documenting the people involved

The **Participants** tab lists all the people linked to the report: the person implicated, the person who made the report, witnesses, victims or any other party relevant to the case.

A participant **is not a user**: they have no access to the platform and receive no notifications. The feature serves as a directory, to easily spot the same person mentioned in several reports.

1. Click Add Participant.
2. Type at least **three characters** to search for a person already recorded (first name, last name or email); their details are filled in automatically. Otherwise, create a new participant by entering their details.
3. Enter their **role in the report** (for example "Witness") and, later, the **outcome** concerning them. Choose an existing value, or type a new one to create it.
4. Confirm to add them to the case.

Each row shows the name and email address, the role in the report, the organisation, the job title, the location and the outcome. The **arrow** on the right of a row opens two spaces shared with all members: free-form **notes** (interview schedule, background...) and **files** (interview reports, contracts, emails...). The ··· menu lets you edit the participant, update their record in the directory or remove them from the report.

CONFIDENTIALITY

The informant **never** sees the Participants tab: not the names, the roles or the outcomes. Participant fields can be adapted to your organisation, and an HR directory (HRIS) connected to Whispli can prefill employees' details.

Files: the evidence file

The **Files** tab centralises all the report's documents, organised by section of origin: Report, Chat, Notes, Participants, Workflows or Tasks.

1. Click `Create Folder` to structure the evidence, with names of your choice (by type, by source, by date...).
2. Add your documents to it with `Upload files`.

Each file posted in a folder is encrypted and only accessible to the people authorised on the report. Custom folders are **not visible** to the informant, and both folder creation and file uploads are logged in the audit trail.

GOOD TO KNOW

Use the same folder names from one report to the next (for example "Legal review"): this makes collaboration and audits easier.

The Activity tab: the audit trail

The **Activity** tab presents the report's activity and gives access to its **Audit Trail**: every action performed, and by whom. The same log opens from the ··· menu, option `View Audit Trail`. It is the proof of rigorous handling in the event of an inspection or audit.

CHAPTER 07

Closing, archiving, retaining

The end of an investigation also follows rules: informing the informant, applying the right retention period, then letting deletion take place in a traceable way.

From end status to deletion

1 — 2 — 3 — 4

End status
e.g. Closed
The informant is notified. The Chat stays open.

Archiving
Retention policy
The informant is notified. The Chat is cut off.

Retention
Period set by the policy
Snooze is useful to review the case before the deadline.

Deletion
Permanent and irreversible
Personal data deleted; audit trail kept.

Closing the report

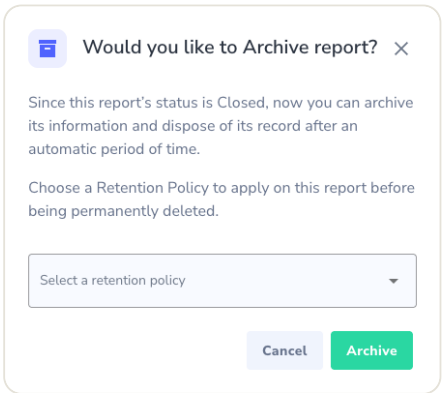
When the status changes to an **end** status (usually **Closed**), the informant receives a notification telling them that their report has been closed; in their inbox, the report shows as closed, with a message stating that your organisation has closed it. They are not notified of any other status change; if there are several end statuses, they do not see which one was applied.

The Chat stays open after closure: you can still exchange messages and files with the informant, and they with you.

Archiving with a retention policy

The Archive option only appears in the report's ··· menu once the report has moved to an end status.

1. Click the ··· menu, then Archive.
2. Choose the appropriate **retention policy**.
3. Click Archive to confirm.
4. Check how the policy applies to the report and the **date on which it will be deleted**.



Archiving a closed report: selecting the retention policy.

As soon as the report is archived, the informant is notified. They can still view their report and messages and download it as a PDF, but **can no longer send messages or files**: communication is cut off. Remember to Snooze the report so you are reminded to review it **before** its retention period expires.

DEPENDING ON YOUR CONFIGURATION

Statuses, retention policies and the automations that apply them are defined by your Administrators. A notification can, for example, warn the people concerned a week or a month before the deletion date.

What remains after deletion

When the retention period expires, all data likely to contain **personal data** is permanently and irreversibly deleted. The report then disappears from the informant's inbox.

Permanently deleted

- Free-text fields of the report and workflows
- All messages exchanged with the informant
- All notes between case managers
- All files, whatever their section
- All tasks

Kept (without personal data)

- Technical fields and dates (submission date, channel...)
- Multiple-choice answers and custom dates from channels and workflows
- Tags and internal name
- Projects the report was linked to

Deleted reports can still be viewed in the list, but are hidden by default: in Reports, open the menu next to "All Reports" and choose Deleted Reports. Each record shows a minimal summary and its audit trail, which indicates who applied the retention policy that led to the deletion.

GOOD TO KNOW

Multiple-choice answers and custom dates are not displayed on the record, but remain available, consolidated, in **Analytics**: tick the corresponding option in the chart configuration to include deleted reports.

CHAPTER 08

Checklist: good habits

A page to keep at hand. Each habit refers to the chapter that covers it in detail.

1. **Acknowledge receipt on time** — Seven working days in France, according to your internal procedure. — Ch. 1
2. **Read the whole report** — Account, attachments, answers to questions; translate if needed. — Ch. 3
3. **Ask yourself "who will see this?"** — Everything posted in the Chat is visible to the informant. — Ch. 3
4. **Move the workflow forward step by step** — Answers saved automatically; Submit to validate the step. — Ch. 6
5. **Mention with @** — Without a mention, your colleagues are not notified of a new note. — Ch. 5
6. **Share through guest access** — Rather than by email: guest access is limited, time-bound and traced. — Ch. 5
7. **Schedule a Snooze** — On pending cases, so that none is forgotten. — Ch. 2
8. **Provide feedback within three months** — Inform the informant of the measures envisaged or taken. — Ch. 1
9. **Close, then archive** — With the retention policy suited to your procedure. — Ch. 7

COMPLIANCE

These habits complement your internal whistleblowing procedure: if they differ, your procedure prevails.

CHAPTER 09

Glossary and help

The platform's terms, as they appear in the English interface — and where to find help.

Glossary

Term	In the interface	Definition
Report	Report	Central case file that brings together all the information related to a concern raised on the platform.
Case manager	—	User in charge of handling reports rigorously, confidentially and in compliance with the rules.
Informant	Informant	Person who made the report. They communicate with you from their secure Whispli inbox.
Owner	Owner	Case manager responsible for the report.
Member	Member	User with access to the report. Member is also the usual role of case managers.
Guest	Guest	External person with temporary access, limited to the shared sections of a single report.
Participant	Participant	Person involved in the report (implicated person, witness...). They have no access to the platform.
Overview	Overview	First tab of the report: status, details, members, tags, workflows.
Chat	Chat	Secure, anonymous messaging with the informant.
Notes	Notes	Internal discussion space between members, never visible to the informant.
Workflow	Workflows	Investigation procedure divided into successive steps, to be submitted one by one.
Project	Projects	Space that groups several related reports.
Audit trail	Activity, Audit Trail	Time-stamped history of all actions performed on a report.

Term	In the interface	Definition
Reminder	Snooze	Personal reminder scheduled on a report; notifications continue in the meantime.
Locking	Lock Report	Restriction of a sensitive report to Administrators and Administrators (restricted) only.
Retention policy	Retention Policies	Period at the end of which an archived report is deleted.

Need help?

- **Whispli Help Center** — help.whispli.com/case-management: up-to-date articles on each feature.
- **Whispli Support** — support@whispli.com.
- **Your Customer Success Manager** — for any question about your platform's configuration (statuses, workflows, automations, optional features).
- **Your Whispli Administrator** — for your access rights and your account.

WHISPLI

Case Manager Guide

help.whispli.com/case-management · support@whispli.com