WHISPLI

WHISPLI CASE MANAGEMENT · CONFIGURATION GUIDE

Configurator Guide

Set up pages, channels, workflows, automations and user access, step by step.

AUDIENCE

Administrators and Configurators

CONFIGURATOR GUIDE

Contents

About this guide 3

01 The Configurator's role 4

02 Pages 6

03 Channels 9

04 Workflows 13

05 Statuses and tags 16

06 Users, groups and roles 18

07 Retention policies 21

08 Automations 22

09 Dashboards 24

10 Go-live checklist 25

Glossary and help 26

About this guide

This guide is for the people who **set up and maintain** a Whispli platform: Administrators, Administrators (restricted) and Configurators. It follows the order in which a platform is usually built, from the page that whistleblowers see to the rules that route reports to the right people.

Each chapter can be read on its own. Numbered steps are meant to be followed in order; boxes highlight what deserves particular attention.

GOOD TO KNOW
A detail or shortcut that saves time.

DEPENDING ON YOUR SUBSCRIPTION
A feature that is only available if your organisation has it.

CAUTION
A point where a mistake is hard to undo or affects people already using the platform.

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

COMPLIANCE
A reminder of the legal obligations that frame the configuration.

Interface labels

Buttons, menus and tabs are given **in English**, as they appear in the Whispli interface and Help Center, for example `Add new`. The interface is available in several languages: each user chooses theirs, for the device they use, in `Settings` › **Me** › `Languages`.

This guide and your platform

Whispli is configured organisation by organisation, and some features are optional. This guide describes the **standard behaviour**. When a feature depends on what your organisation has subscribed to, a **Depending on your subscription** box says so. If in doubt, ask your Whispli Customer Success Manager.

CHAPTER 01

The Configurator's role

Configurators build and adapt the platform without ever seeing the content of reports. This chapter explains what they can do, and in which order a platform is usually set up.

What a Configurator can and cannot do

Configurators can configure Whispli but **cannot access any report or project**. Organisations typically give this role to their IT team when setting up Whispli, and later to adapt the configuration.

A Configurator can	A Configurator cannot
View and edit all Pages, Channels, Workflows and Automations	Open reports or projects: these tabs do not appear in their menu
Manage organisation settings: overview, user groups, retention policies, statuses and tags, as well as users depending on your user-management settings	Access the Audit Trail or perform organisation-wide data exports (Administrators only)
Create and share charts and dashboards	See data in those charts: they remain empty for Configurators

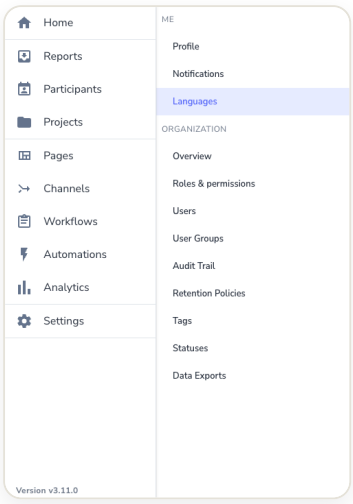
Administrators and Administrators (restricted) have the same configuration rights, plus access to reports (all reports for an Administrator; reports they are a member of and unowned reports for an Administrator (restricted)). Only Administrators can view the audit trail and export data. A user can also combine the **Member** and **Configurator** roles: they then access the configuration tabs and only the reports and projects they are invited to, plus unowned reports depending on the organisation's configuration.

SECURITY

When your organisation asks for help, Whispli Customer Success Managers may access the production platform **as Configurators**, so they can adapt settings without any access to report data.

Where to find everything

The left-hand menu gives access to each configuration area: Pages, Channels, Workflows, Automations, Analytics and Settings. Under Settings, the **Organization** section groups Overview, Roles & permissions, Users, User Groups, Audit Trail, Retention Policies, Tags, Statuses and Data Exports, as an Administrator sees it; Audit Trail and Data Exports are not available to Configurators. The version of the platform is shown at the bottom of the menu.



Left-hand menu and Settings sections

How the building blocks fit together

A **Page** is the entry point for whistleblowers. It displays up to three buttons, each opening a **Channel** (a reporting form). Every submission through a channel creates a **Report**. On each report, case managers complete one or more **Workflows** (investigation procedures), while **Automations** route the report, apply tags and statuses, and send messages and notifications.

1. **Page** — Presents the programme and shows up to 3 buttons.
2. **Channel** — The reporting form behind each button.
3. **Report** — Created by each submission.
4. **Workflows** — Investigation procedures completed by case managers.
5. **Automations** — Route reports, apply tags and statuses, notify.

Recommended order of configuration: pages and channels, then workflows, then statuses, tags, users and groups; finally, automations, which reference all of them.

GOOD TO KNOW

Validate the page and forms in your **main language first**, then translate them. Translating content that is still changing multiplies the rework. A page button can only point to a **live** channel: put the channels live before finishing the page.

CHAPTER 02

Pages

A Page presents your whistleblowing programme and gives access to your reporting forms. It is the first thing a whistleblower sees.

You can create an **unlimited number of pages**: one for the whole organisation, or one per brand, business unit or audience (employees, third parties, customers). Pages can be edited at any time, without help from Whispli. Administrators, Administrators (restricted) and Configurators can create and edit them from `Pages` in the main menu.

Create a page

1. In `Pages`, click `Add new`.
2. Give the page a name (it is **not visible** to whistleblowers and can be changed at any time) and choose its **default language**.
3. Click `Create`, then fill in the elements below.

> **GOOD TO KNOW**
>
> Pages automatically adapt to the language of the visitor's browser. If no version exists in that language, the page is shown in its **default language**: choose one that is widely understood by your audience.

The elements of a page

Element	What to know
Logo	At least 200 × 100 px, PNG (ideally transparent, horizontal) or JPEG. Without a logo, the page shows the one defined in Settings › Overview.
Headline	Up to 300 characters, displayed in bold, no formatting.
Description	Up to 800 characters, displayed in grey and centred, no formatting.
Tabs	The *How it works* tab is managed by Whispli and cannot be modified. You can add **up to 3 custom tabs**, each with a short name and up to 30,000 characters of content (policy, message from management, protection of whistleblowers, FAQ, useful links).
Buttons	**Up to 3 buttons**, each linked to a channel that must be **live**. You choose the label of each button, in each language.
Banner (optional)	Landscape image, PNG or JPEG, 1024 × 576 px recommended. It is the same in every language, so avoid text in the image.

The character limits keep the buttons visible at first glance on every device, including mobiles. For more detail, use the tabs or link to external documents.

> ! **CAUTION**
>
> Some elements are shared by all Whispli pages and cannot be changed: the *Follow up* button at the top right, the *How it works* tab, the layout and size of the buttons. Legal notices or a data protection notice therefore go in a custom tab.

Add a language

1. Open the page editor and click Translations in the left-hand menu.
2. Select the language from the drop-down list on the right.
3. Fill in the translations of your own content: headline, description, button labels and tabs. The original text is shown as a reference.
4. Once every section is filled in, switch on the toggle to put the language live.

Whispli already translates its own components, such as the *How it works* tab. Pages can be made available in more than 75 languages, with no limit and no additional fee. The content does not have to be identical in every language: you can adapt it to local legislation.

Publish, change the URL, get the QR code

- **Publish**: use the toggle at the top of the editor to switch the page between *Live* and *Paused*.
- **Change the URL**: only the last part of the URL can be customised. The page must be **paused** first; then click the pencil icon next to the URL and confirm.
- **QR code**: available from `Get QR Code` once the page is live. Pausing and re-publishing a page does not change its QR code, but the QR code does not work while the page is not live.

GOOD TO KNOW

The QR code can be printed on posters, onboarding material or pay slips, which every employee keeps at home.

CAUTION

Changing the URL of a page that has already been shared makes its **QR code stop working**. Update every link and reprint every QR code where they were published.

CHAPTER 03

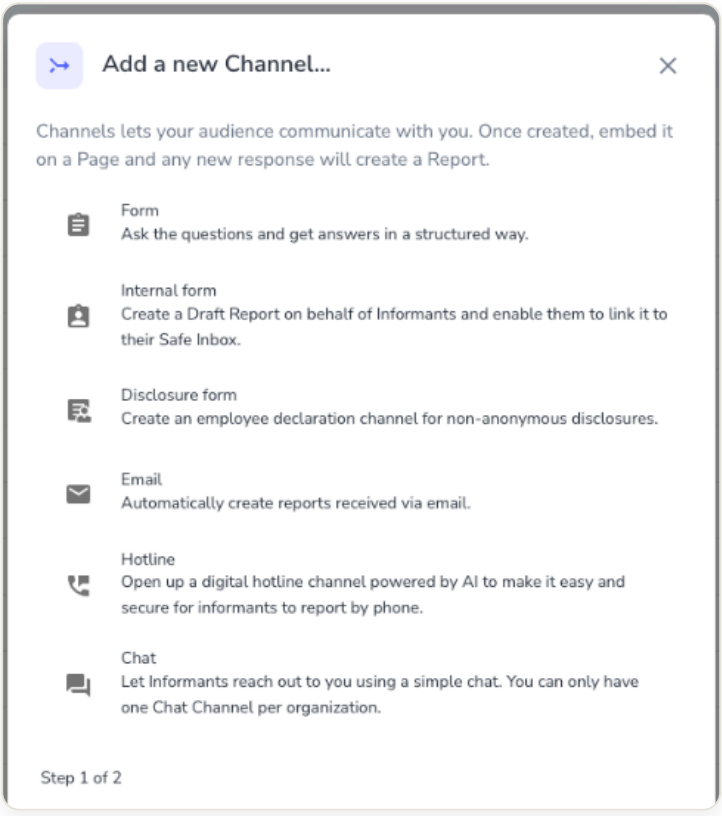
Channels

A channel is a reporting form. It can be used by whistleblowers, by people who report under their own name, or by case managers who record a report on someone's behalf.

Administrators, Administrators (restricted), Configurators and custom roles with access to Channels can create channels. In each channel you define the steps and the questions, so the form fits your reporting programme. Every new submission through a channel creates a report.

Types of channels

Click Add new in Channels to choose the type of channel.



The six types of channels offered when you create a channel

Type	Used by	What to know
Form	Whistleblowers, on the web	The standard form, usable anonymously. It is linked to a page through a button.
Internal form	Case managers, inside the case management platform	Lets a licensed user record a report on behalf of an informant, who can then link it to their secure inbox.
Disclosure form	Identified employees, on the web	For non-anonymous declarations: the person gives their identity through SSO or their email address.
Email	Anyone who writes to a dedicated address	Once the channel is live, each email received creates a report.
Hotline	Whistleblowers, by phone	Usually set up by the Whispli team, as it requires a phone number; fed by a recording and transcription, or by AI, depending on your plan.
Chat	Whistleblowers, on the web	A one-field form that opens a chat directly. Only **one** Chat channel per organisation.

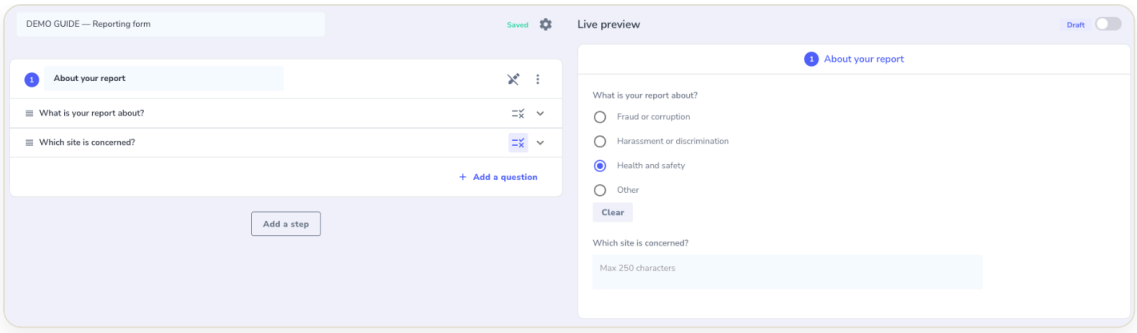
DEPENDING ON YOUR SUBSCRIPTION

Not every organisation has all these types. The email channel, for example, is an add-on, and internal forms are only available on accounts that purchased them. If a type is missing, contact your Customer Success Manager.

Build the form

A channel is made of **steps**, each containing **questions**. The builder shows the form next to a **live preview**. Twelve question types are available:

- **Short Answer** (up to 250 characters) and **Long Answer** (free text);
- **Multiple Choice Answer**: one or several options (*Enable Multiple Options to be selected*), as a list or as a drop-down (*Display as a Dropdown*);
- **Statement**: text to read, with no answer expected (instructions, legal reminder);
- **Media** (file upload), **Date** and **Number**;
- **User List**, **Country List** and **Dynamic List**;
- **Voice message**, offered in channels only;
- **Repeater**: a block of up to 20 sub-questions that the person can fill in up to 20 times (for example one block per person involved).

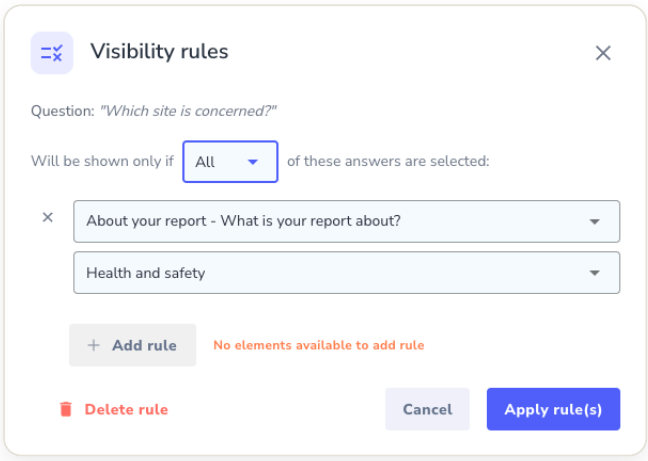


A draft channel in the builder: the second question only appears when "Health and safety" is chosen

Files can be uploaded in the common document, image, audio and video formats (Word, Excel, PowerPoint, PDF, emails, JPEG, PNG, MP3, MP4 and more), as well as PGP-encrypted files.

Display logic

The logic icon of a question opens its **Visibility rules**: the question *"will be shown only if"* **all** or **any** of the chosen answers are selected. Each option of a question can be shown or hidden in the same way. This keeps forms short: informants only see the questions that apply to their situation.



Visibility rules of a question

In a channel, logic applies to questions and options, not to whole steps. A repeater's display logic applies to the repeater as a whole, not to its sub-questions, and a repeater cannot contain another repeater.

> **GOOD TO KNOW**
>
> Display logic works on multiple-choice questions. For a country question, use a **drop-down list containing your own list of countries** rather than the *Country list* type: you can then base display logic and automatic routing on the country chosen.

Edit a live channel

To protect the consistency of reports already received, a live channel cannot be edited directly.

1. **Pause** the channel: it stops accepting submissions while you work.
2. To **add or remove an option** in a multiple-choice question, edit it directly. An existing option cannot be renamed: add a new option and archive the old one.
3. For **any other change**, duplicate the question, edit the copy, drag it to the place of the original, then archive the original.
4. If the channel is translated, open the translations (gear icon at the top of the builder) and add the new wording in each language.
5. Put the channel **live** again.

> **CAUTION**
>
> The builder offers to **archive** questions, channels and workflows rather than delete them. Plan your structure before publishing, and give drafts a clear name so they are easy to tell apart from live versions.

The email channel

Once the channel is live, each email sent to its address becomes a submitted report holding the sender, recipients, subject, message and attachments. Whispli sends an automatic acknowledgement, in the language you choose, to the sender only.

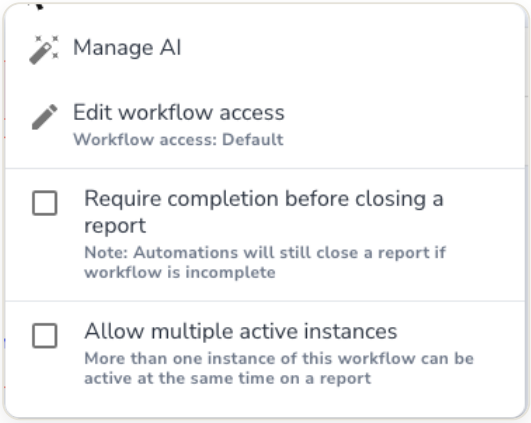
- Email reports are **not anonymous**: the sender's address is stored with the report.
- The address **cannot be changed** once the channel has received its first email.
- To prevent abuse, Whispli refuses automated mail and spam and limits each sender to 10 reports per hour and each channel to 500 messages per hour. Refused emails are listed on the channel page with the reason.

CHAPTER 04

Workflows

A workflow is the procedure that case managers follow on a report, step by step: triage, investigation, outcome, closure. It structures the work and the data collected.

Workflows are organised in steps and use the same question types as channels, except *Voice message*. Case managers complete them inside each report; their answers are recorded and can be used by automations and dashboards.



Workflow settings, from the gear icon of the builder

Design your workflows

- **One workflow per stage.** Keep the closing workflow separate from the investigation workflow: each can then be added at the right time, manually or by an automation.
- **No limit on the number of workflows.** Use clear naming conventions (for example a country or team prefix) so everyone finds the right one.
- **Parallel workflows.** Several workflows can run on the same report, for example an HR investigation and a Compliance investigation. The same workflow can also be active more than once on a report, if you tick *Allow multiple active instances* (see below).

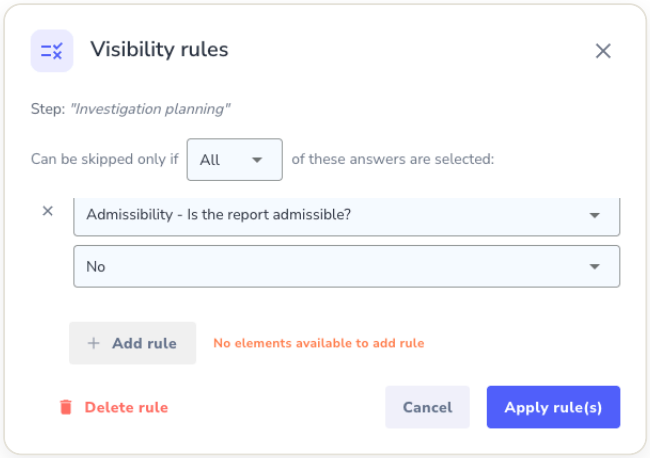
GOOD TO KNOW

Running different workflows in parallel is usually switched on by the Whispli technical team. Contact your Customer Success Manager.

Logic in workflows

Workflows support the same question and option logic as channels, and also **step logic**:

- question and option logic **shows** an element when the condition is met; a condition can use an answer from any earlier step;
- step logic works the other way round: the builder reads *"Can be skipped only if"*. Without a rule, a step can't be skipped; with a rule, it **can be skipped** when the condition is met. Base a branch step's rule on the options that make it unnecessary.

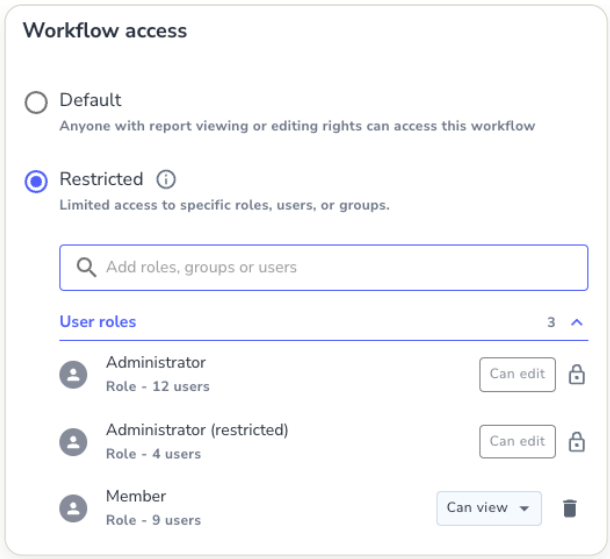


Step logic: the investigation step can be skipped when the report is not admissible

Restrict access to a workflow

By default, anyone who can view or edit a report can access its workflows. You can restrict a workflow to chosen roles, user groups and users, for example when an HR and a Compliance team work on the same report.

1. Open the workflow in the builder, click the gear icon and select `Edit workflow access`.
2. Select **Restricted**.
3. Add the roles, user groups or users who need access, and give each **Can view** or **Can edit**. Only roles and users who already have at least view access to Workflows can be added.
4. Click `Save changes`: the restriction applies immediately and is recorded in the audit trail.



Restricted access: the two Administrator roles are always included, locked on "Can edit"

SECURITY

A restriction can only **narrow** access, never widen it: someone whose role is view-only stays read-only. The Administrator and Administrator (restricted) roles always keep access. The access setting is defined for a **whole workflow**: to reserve some data for a few people, put it in a separate, restricted workflow.

People without access still see the restricted workflow in the report, locked, with the message *Workflow has restricted access*; nothing of its content is shown.

Workflow settings to know

- **Require completion before closing a report**: prevents a case manager from closing a report while the workflow is incomplete. An automation can still close it.
- **Allow multiple active instances**: lets the same workflow be active more than once at the same time on a report.
- **Statements are frozen once the workflow is live.** To change one, pause the workflow, create a new statement with the right text, put it in place of the old one, archive the old one, then put the workflow live again.
- **Workflows are not translated by the platform.** For multilingual teams, write labels in both languages in the same workflow (for example "Admissible / Recevable").

CHAPTER 05

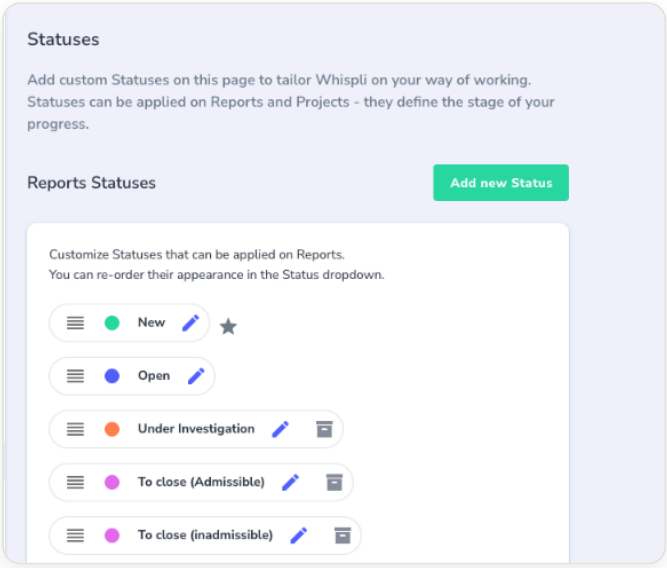
Statuses and tags

Statuses show where each report stands; tags label reports so they can be filtered, analysed and routed.

Administrators, Administrators (restricted) and Configurators manage both in Settings.

Statuses

In Settings › Statuses, statuses are defined separately for **reports** and for **projects**.



Report statuses: re-order, colour, edit, archive; the star marks the default status

- **Add** a status with Add new Status, **rename** it with Edit status and give it a **colour**.
- **Re-order** statuses by drag and drop: the order is the one shown in the status drop-down list.
- Choose the **default status** applied to every new report or project (marked with a star).
- Statuses marked with the →| icon are **end statuses**: they mark the report as closed.
- **Archive** a status you no longer use; it can be unarchived later. Some built-in statuses cannot be archived.

GOOD TO KNOW

Keep the list short and meaningful: statuses are used in filters, dashboards and automations (for example "change the status when the triage step is submitted").

Tags

In `Settings` › `Tags`, click `Add a Tag` and type its name; Whispli warns you if it already exists. For each tag, the list shows how many reports, projects and automations use it.

Common uses: issue type, country, entity or region, priority or criticality. A tag such as **"Exclude from stats"** is useful to keep tests, errors and duplicates out of your dashboards.

> **CAUTION**
>
> A tag can be deleted only as long as no report, project or automation uses it. After that, it can only be **archived**, so it is no longer offered.

Tags can be applied by case managers or automatically: see *Automations*, chapter 8.

CHAPTER 06

Users, groups and roles

Access to reports is the most sensitive part of the configuration. Roles decide what each user can do; user groups decide, together with automations, which reports they see.

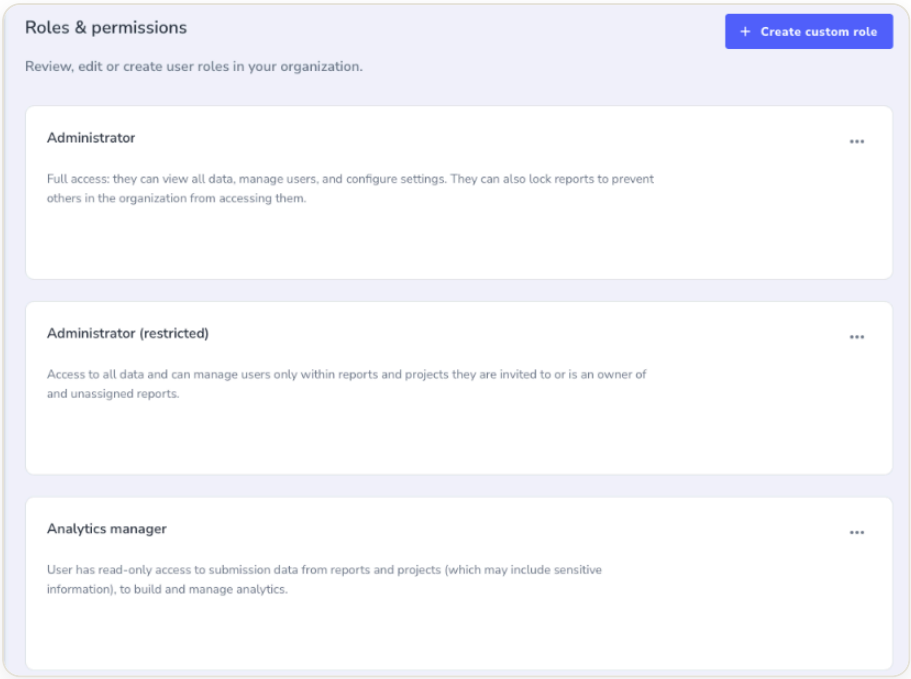
Standard roles

Role	Typical user	Access
Administrator		All reports and projects, all settings, audit trail and data exports. Can lock a report so that no one else in the organisation can access it.
Administrator (restricted)		Same configuration rights as a Configurator; reports and projects they are a member of, and unowned reports. No audit trail, no data exports.
Member	Case manager	The reports and projects they are invited to, manually or by an automation, and, unless Whispli has enabled the *Restrict access to unowned reports* option, unowned reports, which they can take ownership of.
Configurator	IT team	All configuration areas and settings except the audit trail and data exports. No access to reports or projects.
Analytics manager	Manager in charge of reporting	Read-only access to submission data from all reports and projects, to build analytics; cannot open individual reports.
Guest	External counsel, ethics committee	Read-only access to a single report, for a limited time, to the sections shared with them (they can be allowed to contribute to Notes).

GOOD TO KNOW

The Member, Configurator and Analytics manager roles can be combined with one another (for example Member + Configurator). Custom roles, described below, cannot be combined with any other role.

Custom roles



Roles & permissions: built-in roles and the Create custom role button

In Settings › Roles & permissions, Create custom role lets you define your own roles: an external auditor who reads reports without writing anything, a regional compliance officer, a reporting role without access to individual cases. You can start from an existing role and only change the permissions you need. For each feature, a permission can be full access, view only or no access; some features, such as Workflows, also have a *view and update* level.

> **GOOD TO KNOW**
>
> Custom roles are part of the Advanced Roles & Permissions module. There is no limit to the number of custom roles, but each user has **one** custom role, which must therefore hold all the permissions that user needs.

Users

Users are managed in Settings › Users: you choose each user's role when you invite them. Invitations are temporary; if a user has not activated their account in time, you can send a new invitation. A user's details show all the groups they belong to.

> **CAUTION**
>
> If your organisation manages users through **SSO**, each user's role, groups and name are reset from your company directory every time they sign in. Changes made by hand in Whispli are then overwritten, and editing may be locked: make the change in your directory instead.

User groups

A user group (for example *HR Brazil* or *Internal Audit*) gives all its members access to every report assigned to the group. Assigning reports to groups rather than to individuals ensures continuity: when someone is away, colleagues in the group can still handle their reports.

1. In `Settings` › `User Groups`, create the group and give it a functional name.
2. Add members from the list of existing users.
3. Use the group in automations or when assigning reports manually.

Adding a user to a group gives them access to all the group's reports **immediately**; removing them withdraws that access at once, unless they were also added to a report individually.

Guests and two-factor authentication

- **Guests** have no Whispli account: they receive a secure link by email, which only works on the first device where it is opened. They do not need a licence. Case managers can let a guest contribute to the Notes of a report.
- **Two-factor authentication** is activated by each user in `Settings` › `Profile` (except SSO users), with an authentication app. If a user loses their device, an Administrator can deactivate it for that user from the list of users, so they can set it up again.

CHAPTER 07

Retention policies

A retention policy sets how long an archived report or project is kept before it is permanently deleted. It helps your organisation comply with data protection rules such as the GDPR.

Administrators, Administrators (restricted) and Configurators create retention policies in Settings › Retention Policies. By default, only the *Unlimited* policy exists.

1. Click Add a Policy.
2. Give the policy a name and a duration in months or years.
3. Save: the policy is offered to every user who can archive reports and projects.

For each policy, the list shows how many reports and projects it has been applied to, and how many of them have already been deleted.

How a policy applies

- A policy is applied **when a report or project is archived**, manually from a drop-down list or automatically by an automation.
- The report is then locked, and a message at the top of the report shows the planned deletion date.
- **Unarchiving** a report cancels its policy; if a policy is applied again, the full period starts over.
- After permanent deletion, some information remains available for the audit trail and analytics.

Create one policy per legal requirement you need to cover (for example by type of case or by country), and apply it automatically with a time-based automation after closure, so that no report is forgotten.

> **COMPLIANCE**
>
> Align each retention period with your legal and data protection teams before creating it: durations differ by country and by type of case.

CHAPTER 08

Automations

Automations perform actions for you as soon as conditions are met: routing reports to the right people, sending messages, applying statuses, tags and retention policies.

Every automation follows the same chain: a **trigger** (the event that starts it), **conditions** (the cases where it applies) and **actions** (what the platform does). Automations are managed in `Automations`, in three tabs.

Family	When it runs	Typical uses
Triggered by an event	As soon as an event occurs: a report is submitted, a workflow step is submitted, a status changes, a tag is added...	Acknowledgement message, assignment, status change, adding the next workflow
Triggered by time	A set time after an event, for example a week after a report is submitted	Reminders, escalation of reports still untouched, applying a retention policy after closure
Advanced	Like an event automation, but with a different action for each combination of conditions	Assignment by country or business unit, a tag per issue type, a closing status per outcome

Combine conditions

With several conditions, event and time automations let you choose **any** (one condition is enough) or **all** (every condition must be true). Advanced automations always combine their conditions with **all**.

Rules to know before you start

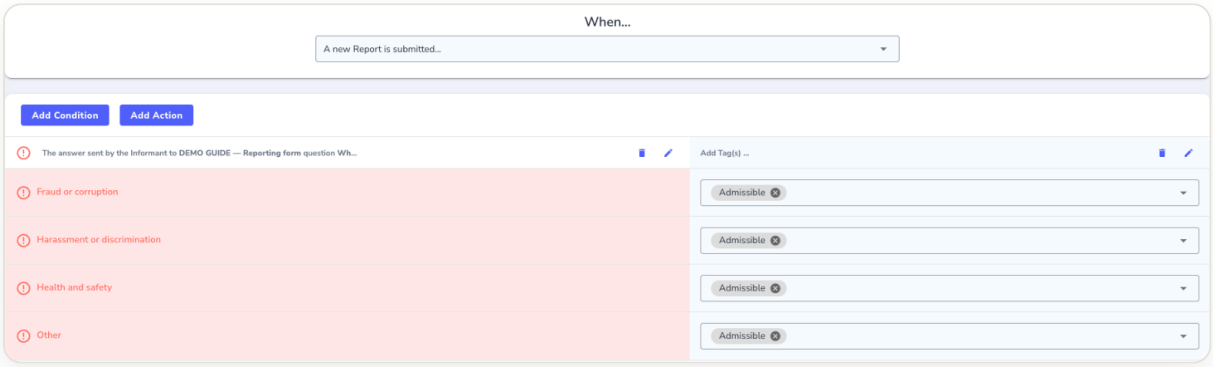
- **Everything starts from the trigger.** Each trigger offers only the conditions and actions that make sense for it, and changing the trigger of an existing automation **resets** its conditions and actions.
- **One trigger per automation.** An advanced automation takes **up to 4 conditions** and **up to 5 actions for each combination** of conditions.
- In an advanced automation, a condition on a form or workflow answer refers to **one channel or one workflow**: create one advanced automation per channel.
- An advanced automation can be put live only when **every cell** of its table is filled in and has no error. For example, a condition on a channel that is not live is flagged in red until the channel goes live.
- A condition can only use answers from the workflow whose step submission triggers the automation.

When each answer to the same question calls for a different action (an owner per country, a closing status per outcome), a single **advanced** automation handles the whole table, instead of one automation per answer.

> **CAUTION**
>
> A user group's members are notified as soon as the group is added to a report: an extra notification action would send a duplicate.

Example: tags from a form answer

1. In **Automations** › **Advanced Automations**, create an automation with a clear name, for example *Issue type tags*.
2. Trigger: *A new Report is submitted*.
3. Condition: *The answer sent by the Informant to a Form question*, then choose the channel, the question and its options.
4. Action: *Add Tag(s)*, then choose the tag for each option in the table.
5. Once every cell is filled in, switch the automation live.



An advanced automation in progress: one row per answer, one tag per row. The red marks show that the demo channel is not live yet.

To tag from a workflow answer, use the trigger *A Workflow step on a Report is first submitted* and the condition *The answer(s) to a Workflow question*.

> **COMPLIANCE**
>
> Time-based automations help you meet the legal deadlines for acknowledging and following up on reports, by reminding case managers or escalating reports that are still untouched.

CHAPTER 09

Dashboards

Dashboards bring together the key figures of your programme. Configurators can build and share them, but never see the data themselves.

Charts are created in Analytics: counts of reports, column charts, pie charts and tables; tables can be downloaded as CSV or Excel files. Charts are then grouped into dashboards and shared.

- A dashboard holds **up to eight charts**, of any type; each user can have as many dashboards as needed.
- A chart can be renamed at any time; the new name appears in every dashboard that contains it, including shared ones.
- A shared dashboard **adapts its data** to the reports each user is allowed to see.
- Configurators and Administrators can add **custom attributes**: data from channel or workflow questions that become dimensions available in charts.

The Help Center shows each type of chart in a short video: counts, column charts, pie charts, tables, dashboards and sharing.

SECURITY

Charts stay **empty** for Configurators. A Member sees figures only for the reports they have access to; an Analytics manager cannot open individual reports, but has read-only access to submission data from all reports, which may include sensitive information.

CHAPTER 10

Go-live checklist

Before announcing the platform, check each building block. Each item refers to the chapter that explains it.

1. **Page validated in the main language, then translated** — Ch. 2
   Headline, description, tabs and buttons; checked on computer and mobile.
2. **Final URL set before printing the QR code** — Ch. 2
   Changing the URL later breaks the QR codes already printed.
3. **Channels tested and live** — Ch. 3
   Each button of the page leads to a live channel; translations complete.
4. **Workflows tested end to end** — Ch. 4
   Step logic, restricted workflows, closing workflow.
5. **Statuses and tags defined** — Ch. 5
   Default status, end statuses, an 'exclude from stats' tag for tests.
6. **Users invited, groups populated** — Ch. 6
   Roles checked; access tested with a member account.
7. **Retention policies agreed with legal** — Ch. 7
   One policy per case to cover, applied automatically if possible.
8. **Automations live and tested** — Ch. 8
   On dummy reports: routing, messages, notifications, statuses.
9. **Dashboards shared** — Ch. 9
   With the case managers and managers who need them.

GOOD TO KNOW

Test on dummy reports, on a computer and on a mobile phone, before inviting case managers: it is the surest way to check routing, messages and notifications end to end.

Glossary and help

Glossary

Term	Definition
Page	Public web page presenting the programme, with up to three buttons to channels.
Channel	Reporting form: form, internal form, disclosure form, email, hotline or chat.
Report	File created by each submission, handled by case managers.
Workflow	Procedure in steps that case managers complete on a report.
Automation	Rule that performs actions when a trigger and conditions are met.
Status	Stage of a report or project; end statuses mark it as closed.
Tag	Label applied to reports, manually or automatically.
User group	Set of users who receive access to the same reports.
Custom role	Role whose permissions you define feature by feature.
Retention policy	Period after which an archived report is permanently deleted.
Informant	The person who submits a report (whistleblower).

Getting help

- **Your Customer Success Manager**: configuration advice, training, best practices, new features, additional options.
- **Whispli Support**, available 24/5: by chat from the question-mark icon at the top right of the case management platform, or at support@whispli.com.
- **Help Centers**: help.whispli.com/case-management for case managers and Administrators; help.whispli.com/en/articles for whistleblowers.

WHISPLI

Configurator Guide

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