WHISPLI

WHISPLI CASE MANAGEMENT · ADMINISTRATION GUIDE

Roles and access rights

Who sees what, who can do what: standard roles, custom roles and report-level controls.

AUDIENCE

Administrators, Configurators and compliance leads

Contents

How to use this guide 3

01 How Whispli decides who sees what 4

02 The standard roles 6

03 The permission matrix 8

04 Creating and managing custom roles 10

05 Assigning roles to users 15

06 Protecting one specific report 17

07 Best practices and access review 20

08 Glossary and help 22

How to use this guide

This guide explains **who sees what and who can do what** in Whispli Case Management: the standard roles, how they combine, custom roles and the settings that protect one specific report. It replaces the document “Understanding Access Roles in Whispli Case Management” and includes the custom roles setup guide (*Advanced Roles and Permissions*).

It is written for the Administrators and Configurators who grant access, and for the compliance leads who must be able to show that only authorised people access reports.

GOOD TO KNOW
A detail or a tip that saves time.

DEPENDING ON YOUR CONFIGURATION
A behaviour that depends on the modules or options enabled for your organisation.

CAUTION
A setting where a mistake exposes data or locks users out.

SECURITY
A rule that protects the confidentiality of informants and the people concerned.

Interface labels

Menus and buttons are quoted **as they appear in the English interface**, for example `Create custom role`. The names and descriptions of the standard roles and the names of the permissions are in English in every interface language. The glossary in chapter 8 gives the French equivalents.

This guide and your configuration

The standard roles are the same for every organisation; they cannot be edited, only duplicated. **Custom roles** are part of the *Advanced Roles & Permissions* module: your Customer Success Manager can confirm whether your organisation has it. Some organisation options, enabled by Whispli, also change how roles behave: for example Members' access to unowned reports (chapter 1) or role management through SSO (chapter 5). Screenshots come from a demo environment; their content is fictitious.

CHAPTER 01

How Whispli decides who sees what

A user can access a report when three conditions are met: their role allows it, the report is within their scope, and nothing restricts that report.

Four layers

1 The role
What can they do?
A standard role, a combination of standard roles or a custom role. It sets an access level for each feature: none, view only, full.

2 The scope
Which reports do they see?
The Reports section level: all reports, the reports they are a member of (with or without unowned reports) or none.

3 Membership
Which reports are they a member of?
They own the report, were added manually, belong to a user group added to the report or an automation assigned them.

4 Report restrictions
Does anything restrict this report?
A locked report, a restricted workflow, or, for a guest, only the sections shared with them.

The four layers apply together: a restriction set on a report or a workflow never grants more rights than the role.

The scope: the *Reports section*

The **Reports section** level decides which reports appear in a user's `Reports` list. There are four levels:

Level (interface)	The user sees...
Full access	every report in the organisation, whether or not they are a member.
Assigned as member and unowned	the reports they own or are a member of, **and** the reports that do not have an owner yet.
Assigned as member	only the reports they own or are a member of.
No access	no reports: the `Reports` menu is of no use to them.

The standard roles use only two of these levels: *Full access* for the Administrator, *Assigned as member and unowned* for the Administrator (restricted) and the Member (subject to the option described below for the Member). The *Assigned as member* level is only available in a custom role.

SECURITY

By default, an unowned report is visible to **every** user whose role includes unowned reports, which means every Member; to open its content, someone must take ownership. This behaviour depends on an option Whispli enables for your organisation: with the *Restrict access to unowned reports* option, Members no longer see or open unowned reports. Your Customer Success Manager can tell you whether it is enabled. Other solutions: assign each report on receipt with an automation, or use a custom role set to *Assigned as member*.

What the role allows inside a report

For each tab of a report (Report, Chat, Notes, Workflows, Participants, Members, Tasks, Files, Activity), the role sets a level: no access, view only or full access. Actions (change status, archive, lock, export as PDF...) are either allowed or not. Chapter 3 details these settings for each standard role.

Whispli's documentation sums up this logic as three levels of access to a report:

- **No access** — the default: until the user is linked to the report (by an automation, a user group or a manual assignment), the report is invisible to them.
- **View only** — they read the report, attachments and history, without changing anything or writing to the informant.
- **Full access** — they handle the case end to end: chat with the informant, notes, change of owner, closing.

GOOD TO KNOW

A restriction set on a workflow or a report **narrows** access and never widens it: a user whose role is view-only on workflows stays read-only, even if they are listed with “Can edit” on a restricted workflow.

CHAPTER 02

The standard roles

Five roles come with the platform. Three of them can be combined; the two Administrator roles and custom roles are assigned on their own.

The five roles and the guest

Administrator

CANNOT BE COMBINED

Owner of the speak-up programme: access to everything. Keep it to very few people.

- ✓ All reports, participants and projects, with full access to every tab.
- ✓ Every action, including locking a report and exporting it as PDF.
- ✓ All configuration, roles, users and user groups.
- ✓ Analytics computed on all reports.
- ✓ Audit trail, export of all reports and all workflows.

Administrator (restricted)

CANNOT BE COMBINED

Functional administrator who should only see the cases that concern them.

- ✓ Reports they own or are a member of, plus unowned reports.
- ✓ The same tabs and actions as an Administrator, including locking and exporting as PDF.
- ✓ All configuration, roles, users and user groups.
- — No audit trail, no organisation-wide data export.
- — Analytics limited to the reports they can access.

Member

CAN BE COMBINED

Case manager: investigates the reports entrusted to them.

- ✓ Reports they own or are a member of and, unless the Restrict access to unowned reports option is on, unowned reports; full access to the tabs.
- ✓ Status, tags, closing, archiving, redaction, guests, change of owner.
- ✓ Analytics menu and dashboard sharing.
- — No locking, no PDF export, no change of project owner.
- — No configuration, no organisation settings.

Configurator

CAN BE COMBINED

IT team or technical lead: configures without seeing reports.

- ✓ Pages, channels, workflows, automations, overview, statuses, tags, retention policies.
- ✓ Roles and permissions, users, user groups.
- ✓ Dashboards: create, share, assign.
- — No access to reports, participants or projects.
- — No audit trail, no exports; analytics without access to the data of all reports.

Analytics manager

CAN BE COMBINED

Reporting lead: consolidated figures without opening cases.

- ✓ Analytics computed on the data of all reports, which may include sensitive information.
- ✓ Create, share and assign dashboards.
- — No access to reports, configuration or settings.

Guest

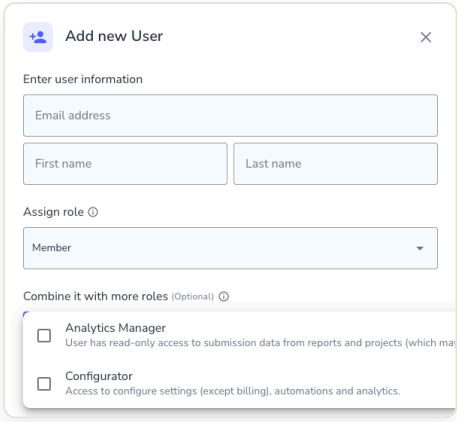
Lawyer, external expert, ethics committee: not a role assigned in Users, but an invitation on one report.

- ✓ Read-only access to the sections of one report shared with them; can be allowed to contribute to Notes.
- ✓ Time-limited access through an email link that works on the first device only; no licence.

Combining roles

In a user's dialog, the **Combine it with more roles** field adds one or more roles to the main role. The possible combinations:

Main role	Can be combined with
Administrator	no role
Administrator (restricted)	no role
Member	Analytics manager, Configurator
Configurator	Member, Analytics manager
Analytics manager	Member, Configurator
Custom role	no role



Add new User: Member chosen as main role, Analytics Manager and Configurator offered as combinations

The interface help explains that the Administrator role cannot be combined because it already has every system right, and that custom roles cannot be combined because they already include every permission needed. A combination is used to **extend** a user's rights.

Two combinations meet frequent needs:

- **Member + Configurator** — a case manager who also adapts the configuration (pages, channels, workflows, automations) while only seeing the reports they are a member of.
- **Member + Analytics manager** — a manager who tracks the figures for all reports but only opens the cases they are a member of.

> **CAUTION**
>
> A user who needs a mix of permissions that combinations do not allow (for example read-only reports plus the audit trail) must receive **one single custom role** that brings together everything they need: you can neither stack two custom roles nor add a standard role to a custom role.

CHAPTER 03

The permission matrix

Every permission for every standard role, as displayed by the platform. These settings are also the starting point of any custom role created from an existing role.

Reports, participants and projects

Permission (interface label)	Administrator	Administrator (restricted)	Member	Configurator	Analytics manager
Case management — reports, participants and projects					
Reports section Which reports the user sees in the Reports list	Full	Member + unowned	Member + unowned	—	—
Report (tab), Chat, Notes, Workflows, Participants, Members, Tasks, Files the informant's answers · chat with the informant · internal notes	Full	Full	Full	—	—
Activity The report's activity log	View only	View only	View only	—	—
REPORT OVERVIEW ACTIONS					
Create report (internal form), Take ownership of unowned reports, Reassign report ownership, Change status, Update internal name, Add and delete tags from report, Add versions, Close report, Linked reports Internal form	✓	✓	✓	—	—
REPORT PRIVACY ACTIONS					
Invite guests	✓	✓	✓	—	—
Lock/Unlock	✓	✓	—	—	—
Archive, Unarchive, Redact report, Manage redactions Archive a report · Unarchive a report	✓	✓	✓	—	—
Export as PDF	✓	✓	—	—	—
PARTICIPANTS AND PROJECTS					
Participants section Participants menu	Full	From assigned reports	From assigned reports	—	—
Projects section Projects menu	Full	From assigned reports	From assigned reports	—	—
Create, Archive, Link/Unlink to a report Create a project · Archive a project · Link a project to a report	✓	✓	✓	—	—
Reassign project ownership	✓	✓	—	—	—

Configuration, analytics and administration

Permission (interface label)	Administrator	Administrator (restricted)	Member	Configurator	Analytics manager
Platform configuration					
Pages section, Channels section, Workflows section, Automations section, Organization overview, Statuses, Tags, Retention policies Workflow builder	Full	Full	—	Full	—
Data and insights					
Access all data from analytics Analytics computed on all reports	✓	—	—	—	✓
View analytics, Share dashboards	✓	✓	✓	✓	✓
Assign dashboard to another user	✓	✓	—	✓	✓
Admin and governance					
View audit trail Settings › Audit Trail	✓	—	—	—	—
Roles and permissions, Manage users Settings › Roles & permissions · Settings › Users	Full	Full	—	Full	—
Manage user groups Settings › User Groups	✓	✓	—	✓	—
Export all reports, Export all workflows	✓	—	—	—	—

Default role settings; the Restrict access to unowned reports organisation option removes unowned reports from Members (ch. 1). ✓ allowed · — denied or no access · Full = Full access · Member + unowned = Assigned as member and unowned · From assigned reports = Participants / Projects from assigned reports.

Key points

- **Member and Administrator (restricted) have the same default scope**: the reports they own or are a member of, plus unowned reports — except for Members if the *Restrict access to unowned reports* option is enabled for your organisation. The difference lies in actions (lock, export as PDF, change project owner) and configuration.
- **Lock and export as PDF** are reserved for the two Administrator roles among the standard roles. A custom role can, however, be given both permissions.
- **The audit trail and organisation-wide exports** (all reports, all workflows) are reserved for the Administrator. The Administrator (restricted) cannot access them.
- **Analytics**: only the Administrator and the Analytics manager see analytics computed on all reports; for other roles, figures are limited to the reports they can access.

SECURITY

The **Configurator** has full access to Roles & permissions and Users. Even without seeing any report, they can therefore change other users' access: assign this role with the same care as an Administrator role, and check regularly who holds it.

CHAPTER 04

Creating and managing custom roles

A custom role sets, permission by permission, what a group of people can see and do. It is how you apply the need-to-know principle.

DEPENDING ON YOUR CONFIGURATION

Custom roles are part of the *Advanced Roles & Permissions* module. There is no limit to their number; each user has at most one.

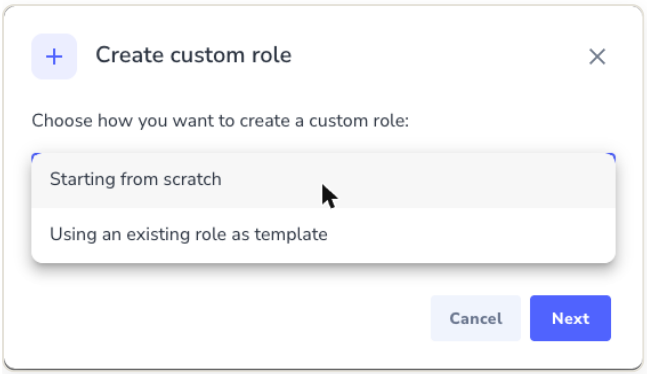
When to create a custom role

Whispli's documentation lists these typical needs:

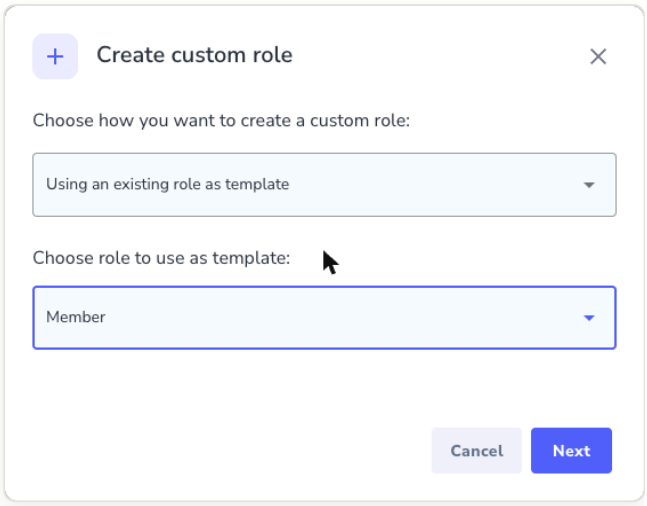
- **A viewer** — a lawyer or external auditor who reads reports without being able to write to the informant or change anything.
- **An investigator without chat** — they document the investigation but do not communicate with the informant.
- **A role limited to certain actions** — they chat with the informant but do not change the status or export anything; or, conversely, a group allowed to export as PDF for litigation.
- **A tailored configurator** — they manage users and view the audit trail, but do not change automations.
- **A reporting role** — they view consolidated figures without accessing cases.

Create the role

1. Open `Settings` › `Roles & permissions`, then click `Create custom role`.
2. Choose `Starting from scratch` or `Using an existing role as template`. With a template, choose the starting role (a standard role or an existing custom role): its settings are copied and you only adjust the differences.
3. Click `Next`, then enter a name in `Add name` and a description (255 characters at most).



Choosing the creation method



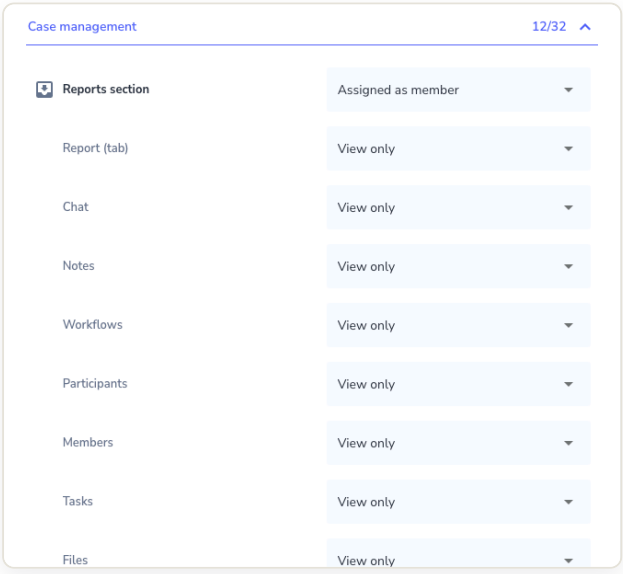
Choosing the role to use as template

GOOD TO KNOW

Start from the standard role closest to the need: the Member role for a viewer; the Administrator (restricted) for someone who administers the platform without the audit trail. You will only have a few permissions to change.

Set the permissions

The **Permissions** section shows the four panels of the matrix: *Case management*, *Platform configuration*, *Data and insights*, *Admin and governance*. Each header shows the number of permissions granted (for example 12/32), and the **Search permissions** field finds a permission by name. Access to tabs and menus is set in a drop-down list; actions are set with a toggle.



Editor: scope and report tabs set to view only

The levels offered differ from one permission to another:

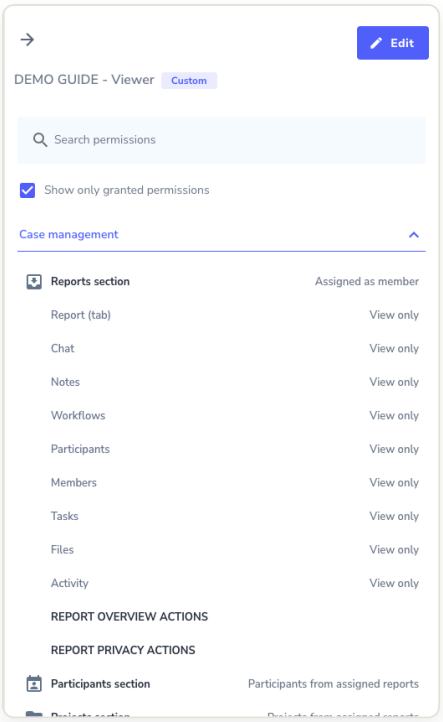
Permission	Levels offered in the editor
Reports section Scope of reports	No access · Assigned as member · Assigned as member and unowned · Full access
Report (tab), Chat, Notes, Members	No access · View only · Full access
Workflows, Participants, Tasks, Files	No access · View only · View and update · Full access
Activity	No access · View only
Participants section, Projects section	No access · ... from assigned reports · Full access
Pages, Channels, Workflows, Automations; Organization overview, Statuses, Tags, Retention policies Platform configuration	No access · View only · Full access
Roles and permissions, Manage users	No access · View only · View and update · Full access
Actions (report, privacy, projects), Data and insights, other Admin and governance permissions	On · Off

The **View and update** level is only documented for workflows: the user opens and fills in a workflow, but does not add or deactivate workflows; full access also allows adding and deactivating workflows. For the other permissions that offer it (Participants, Tasks, Files, Roles and permissions, Manage users), test its effect with a test account before using it.

> **CAUTION**
>
> The **Full access** level of the *Reports section* gives access to **every** report in the organisation. For an investigation role, choose *Assigned as member* or *Assigned as member and unowned*.

Save and check

Click **Create custom role** at the bottom of the editor. A confirmation message appears, and the **See permissions** panel opens with the *Custom* badge. By default it only lists the permissions granted; untick **Show only granted permissions** to see them all.



The See permissions panel of the new role



Menu of a custom role: Edit, Duplicate role, Delete

Example: a read-only role

The demo role *DEMO GUIDE - Viewer*, created for this guide from the Member role, illustrates the “viewer” need:

Permission	Setting
Reports section	Assigned as member — neither the full list nor unowned reports
Report (tab), Chat, Notes, Workflows, Participants, Members, Tasks, Files, Activity	View only
Participants section, Projects section	… from assigned reports (copied from the template)
Report overview actions, report privacy actions, project actions	all off
Data and insights	View analytics and Share dashboards (copied from the template)
Platform configuration, Admin and governance	no access

Edit, duplicate, delete

The ⋯ menu of a custom role offers `Edit`, `Duplicate role` and `Delete`. The menu of a standard role only offers `See permissions` and `Duplicate role`: standard roles cannot be edited, only duplicated. Editing reopens the editor; save your changes at the bottom of the page.

Before deleting a role, assign another role to the users who have it, and check that no restricted workflow lists it in its access list.

CHAPTER 05

Assigning roles to users

The role is chosen when the user is invited and can be changed at any time from the user list, unless your organisation manages access through SSO.

Invite a user

Users whose role includes *Manage users* (Administrator, Administrator (restricted), Configurator or a custom role that grants it) manage the list in **Settings** › **Users**.

1. Click **Add user**.
2. Enter the email address, first name and last name.
3. In **Assign role**, choose the main role. The list shows custom roles first, then default roles, each with its description.
4. If the role allows it, add one or more roles in **Combine it with more roles** (optional). For a role that cannot be combined, the field reads “This role cannot be combined with others”.
5. Click **Next** and complete the invitation.

Invitations are temporary: if the user has not activated their account in time, send them a new invitation. The page header shows how many paid seats are in use.

Change a user's role

In the list, click ··· at the end of the user's row, then **Edit user**. The dialog lets you change the role and its combination, and make the user inactive: inactive users cannot access their Whispli account. Confirm with **Update user**.

> **GOOD TO KNOW**
>
> When a user leaves the organisation, first change the owner of their reports, then make them inactive: they can no longer sign in.

User groups

A user group (for example *HR France* or *Internal Audit*) gives all its members access to the reports the group is added to, manually or by an automation. Adding someone to a group opens these reports to them immediately; removing them closes the reports at once, unless they were also added individually. The group gives access to the report; what each person can do there depends on their role.

SSO: roles come from your directory

If your organisation manages users through SSO, the company directory is the source of truth. At **every sign-in**, Whispli resets from the SSO information:

- the role (including a custom role);
- user groups;
- the name.

Depending on how SSO is set up, manual editing of these fields can be blocked for Administrators and Configurators. A change made by hand in Whispli is overwritten at the next sign-in anyway: make the change in the directory.

For IT teams, setup follows three steps:

1. **Map the attribute** — in the identity provider (Okta, Microsoft Entra ID, Google Workspace...), map the user's role to the SAML attribute Whispli expects. Each role created in Whispli automatically generates a matching role attribute.
2. **Match the values** — the values sent must exactly match the identifiers of the roles created in Whispli.
3. **Just-in-time provisioning** — when the user signs in, Whispli reads the attribute and assigns or updates their role.

> **DEPENDING ON YOUR CONFIGURATION**
>
> Role management through SSO is an option Whispli enables for your organisation (*SSO Managed Role*). Whispli Support (support@whispli.com) gives you the exact name of the SAML attribute and the role identifiers when you configure SSO. Test with one account before opening access to everyone.

Two-factor authentication

Each user turns on two-factor authentication in Settings › Profile, with an authenticator app (except SSO users). If a user loses their device, an Administrator can turn off two-factor authentication for that user so they can set it up again. The *2FA* column of the user list shows who has turned it on.

CHAPTER 06

Protecting one specific report

The role sets access in general. Three settings go further for a given case: locking, restricted workflows and guest access.

Lock a report

For a conflict of interest or a highly sensitive case, a report can be locked: ··· menu next to the status, then `Lock Report`.

- No one can access it any more, **not even its owner or members**, except Administrators and Administrators (restricted). Others see it in their list with a padlock, and opening it shows an error message.
- On a locked report, Administrators can still communicate with the informant, write notes, manage participants, view files, change the status and archive. They can no longer edit the workflow, add tags, upload files in the Files tab or add anyone (member, group or guest).
- Unlocking is done from the same menu.

Among the standard roles, only the two Administrator roles have the *Lock/Unlock* permission. The custom role editor also offers this permission.

Restrict a workflow

When several teams work on the same report without seeing each other's work (an HR investigation and a compliance investigation in parallel, for example), a workflow can be reserved for certain roles, groups or users: in the workflow builder, gear menu, `Edit workflow access`, then `Restricted`. For each entry on the list, choose `Can view` or `Can edit`.

Two settings then decide what a user can do with that workflow:

1. **Their role**, which sets their level on the Workflows tab of every report (table rows).
2. **The workflow restriction**, which says whether they are on its list, and with which right (table columns).

The more restrictive of the two always applies.

Role on the Workflows tab	Open workflow (default)	Restricted — on the list, *Can view*	Restricted — on the list, *Can edit*	Restricted — not on the list
No access	tab hidden	tab hidden	tab hidden	tab hidden
View only	reads	reads	reads (the role blocks editing)	locked
View and update	reads and fills in	reads	reads and fills in	locked
Full access	reads, fills in, adds and deactivates workflows	reads	reads and fills in	locked

EXAMPLE

Sophie has the Member role: she has full access to the Workflows tab. On a report, two workflows are added: *Triage*, open, and *HR investigation*, restricted to the HR group with *Can edit*. Sophie is not in the HR group: she fills in *Triage* as usual, and sees *HR investigation* in the list, but locked, without any of its content. Her colleague Karim, also a Member and part of the HR group, fills in both. If Sophie joins the HR group, she gets access to *HR investigation* at once.

Good to know:

- **Administrators always keep access.** The Administrator and Administrator (restricted) roles are on the list by default, with a padlock: they cannot be removed. An entry whose role is view-only cannot be raised to *Can edit*.
- **What a user who is not on the list sees**: the workflow stays in the report's workflow list, locked. Selecting it shows the message “Workflow has restricted access”, which says only specific members have access and who to contact. Nothing of its content is revealed.
- **Full access does not bypass the restriction.** A user with *Full access* to workflows, or to the builder, still sees a workflow locked if they are not on its list: add them, their role or one of their groups.
- **Removal from a group takes effect at once.** Access through a group is re-checked on every request: removing someone from a group on the list removes their access immediately. This is the usual cause of “I lost access although nobody edited the workflow”.
- **Duplicating a restricted workflow gives a restricted copy with nobody on the list**, so only Administrators can see it. After duplicating, fill in the list before using the copy.
- **The audit trail** records every change to the list: who made it, which entry, which workflow.
- Restricting a workflow does not change who can see the report itself.

Share a report with a guest

Rather than downloading a report to send it by email, invite the external person: **Members** tab, `Add members`, then `Invite a guest`. The invitation asks for a reason (255 characters at most); you then set an expiry date (or end of access on a status change), the sections to share and whether the guest can write in Notes.

- The guest has no Whispli account and no licence. They receive a secure link that only works on the **first device** where it is opened: a forwarded email or a hacked inbox does not give access to the report.
- They only see the shared tabs, read-only, except Notes if you allow it.
- Until they open the link, they appear with the *Pending* status in the Members tab; you can edit their permissions, resend the invitation or revoke access at any time.

> **SECURITY**
>
> The *Invite guests* permission is granted to Members as well as Administrators. If your policy reserves external sharing for certain people, turn it off in a custom role for the other case managers.

CHAPTER 07

Best practices and access review

Access to a speak-up platform must be justified: the EU Directive and the French Sapin II law require the identity of the reporting person and of the persons concerned to remain confidential. Use this list at setup and for periodic reviews.

Checklist

1. **As few Administrators as possible**
   The role gives access to every report and to the audit trail. Plan at least two people for continuity, no more than needed. — Ch. 2
2. **The Member scope decided**
   By default a Member also sees unowned reports. If that is not wanted: the Restrict access to unowned reports option (ask Whispli) or a custom role set to Assigned as member. — Ch. 3
3. **Configuration and investigation kept apart**
   Configurator for the IT team, Member for case managers; combine them only for someone who really does both. — Ch. 2
4. **Roles that manage users identified**
   Administrator, Administrator (restricted) and Configurator manage roles and users: assign them with the same care. — Ch. 3
5. **User groups rather than individuals**
   Automations assign reports to groups, so work continues when someone is away. — Ch. 5
6. **Every custom role tested**
   With a test account: report list, visible tabs, possible actions, before assigning it in production. — Ch. 4
7. **Explicit names and descriptions**
   The name says who the role is for, the description (255 characters) what it allows and what it does not. — Ch. 4
8. **Sensitive cases protected**
   Lock for a conflict of interest, restricted workflow for a parallel investigation, guests with an expiry date. — Ch. 6

9 **SSO aligned**
If roles come from your directory, make changes in the directory: changes made in Whispli are overwritten at the next sign-in. Ch. 5

10 **A periodic review**
Inactive users deactivated, roles and groups checked, audit trail reviewed. Ch. 7

Keep configuration and investigation apart

Organise access around two distinct jobs:

- **Those who configure** — the IT team or technical lead gets the Configurator role: they build channels, workflows and automations without ever seeing a report's content. It is also the role under which a Whispli Customer Success Manager works on your production platform, when you ask them to.
- **Those who investigate** — case managers get the Member role, or a more restricted custom role. They only access the reports entrusted to them.

Review access regularly

At least once a year, and at every reorganisation:

1. In Users, check roles and make unused accounts inactive.
2. In User Groups, check the members of each group used by automations.
3. In Roles & permissions, open See permissions for each custom role and confirm it still matches its purpose.
4. In the Audit Trail (Administrator), check changes to roles and to workflow access.

COMPLIANCE

Document your roles: who gets which role and why. This record lets you show, in an audit or a dispute, that access to reports is limited to the people authorised to handle them.

CHAPTER 08

Glossary and help

Role and permission terms, as they appear in the English and French interfaces.

Glossary

Term	EN interface	FR interface	Definition
Role	Role	Rôle	Set of permissions assigned to a user.
Standard role	Default roles	Rôles par défaut	The five roles provided: Administrator, Administrator (restricted), Member, Configurator, Analytics manager. They cannot be edited.
Custom role	Custom roles (*Custom* badge)	Rôles personnalisés	Role created by the organisation, permission by permission. One per user.
Combination	Combine it with more roles	Le combiner avec d'autres rôles	One or more combinable standard roles added to the main role.
Permission	Permissions	Autorisations	Single right (tab, menu, action), set by level or by toggle. Names stay in English in both languages.
Scope	Reports section	Reports section	Level that decides which reports the user sees in the Reports list.
Unowned	Unowned	—	Report that nobody has taken ownership of yet.
Owner	Owner	Responsable	Person responsible for handling a report.
Member	Member	Membre	Person added to a report; also the name of the case managers' role.
User group	User Groups	Groupes d'utilisateurs	Set of users added to a report at once, often by an automation.
Guest	Guest	Invité	External person without an account, invited read-only on one report.
Lock	Lock Report	Verrouiller le rapport	Reserves a report for Administrator roles, even against its owner.

Term	EN interface	FR interface	Definition
Restricted workflow	Workflow access: Restricted	Accès à la procédure : Restreint	Workflow reserved for a list of roles, groups or users.
Audit trail	Audit Trail	Historique d'audit	Log of the organisation's actions, reserved for the Administrator among standard roles.
SSO	SSO	—	Sign-in through the company directory; role and groups are then managed there.

Need help?

- **Whispli Help Center** — help.whispli.com/case-management: up-to-date articles on roles, groups, guests and restricted workflows.
- **Whispli Support** — support@whispli.com: SSO configuration, questions about your plan.
- **Your Customer Success Manager** — designing custom roles, access review before going live.

WHISPLI

Roles and access rights

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