

Roles and permissions

Create roles, assign permissions, understand inheritance, invite employees, enforce two-factor authentication, legal representatives and the shift restriction. Including the typical mistakes.

unitlify.de/docs/rollen-rechte · 2026-10-22

How permissions work in Unitlify

Every person has one or more **roles**. Every role carries a list of **permissions**, for example "View bookings" or "Create shifts". What a person is allowed to do is the sum of the permissions of their roles. Permissions apply to the whole business.

Unitlify creates two roles when the business is set up:

- **Administrator**: has all permissions, including all future ones. The permissions cannot be changed and the role cannot be deleted. The first person of the business is an administrator and a legal representative (see below).
- **Employee**: the base role. Every invited person receives it automatically. It is **empty** at the start, you decide yourself what everyone in the business is allowed to do.

Menu **Administration** → **Roles**. You need the permission "View roles" to look at roles and "Create roles/Edit roles" to change them.

Setting up the base role "Employee"

This is the most important step after getting started. Everything that every person in the business should see belongs in the base role, for example:

- View own shifts and apply for open shifts
- Request leave, submit sick notes, view own absences
- Clock in and out and view own time account
- Chat, newsfeed, phone book

Without these permissions, invited employees see almost nothing after logging in. Even the page "My shifts" only appears with a matching permission.

The reverse also applies: whatever the base role has, **all** roles above it have automatically. Permissions that only managers should have therefore do not belong in the base role.

Positions such as "Shift lead" or "Trainer" are created as separate roles. They carry only the permissions that go beyond the base role.

Creating roles

New role: code (unique per business), name, optionally a description and an hourly wage. Then tick the permissions, grouped by area: Dashboard, Communication, Booking system, Ticketing & vouchers, Finance, HR, Training, Contracts & forms, Administration.

A new role is placed directly above the base role in the ranking.

If you tick **all** permissions, the role becomes a full-access role like the administrator, including all permissions added later. Use this deliberately.

Template "Tax advisor (read only)"

Via **Template** you create a ready-made read-only role for your tax advisor: read invoices, bookings, finance, Unitlify invoices and expenses only. It inherits nothing and sits directly below the administrator. Please note: every invited person also receives the base role and counts in packages with a price per employee.

Inheritance and ranking

The roles are arranged in a ranking (rank 1 at the very top). **A role inherits all permissions of the roles below it.** Inherited permissions are marked in blue and can be deselected individually per role if a higher role explicitly should not have a certain permission.

Sort by drag and drop. Example: base role "Employee" at the bottom, above it "Trainer", above that "Shift lead", above that "Operations manager". The operations manager thus has everything the three roles below have, plus their own permissions.

Two things are never inherited: the full-access marker ("all permissions") and the shift restriction (below).

Permission changes, role assignments, reordering and deleting roles take effect immediately, without a new login.

Shift restriction

Three permissions exist in the variant "only during own shift": bookings, form submissions and Service Center. A person with this variant sees the data only while they are on duty according to the shift plan (Berlin time, no buffer). Outside of that, "Outside your shift you have no access to this data" is shown.

Important: the restriction applies to the **whole person** as soon as one of their roles carries it, unless another role has full access. So do not give the restriction to a role that managers also carry in addition. And: anyone who has no shift in the plan has no access.

Locations

Under **Administration** → **Locations** you create locations with units and sub-units and assign employees to them. The assignment controls what a person sees in the phone book, in chat channels, in to-dos and in storage, and serves as a filter in staff lists. Permissions themselves apply to the whole business regardless of location.

Inviting employees

Menu **HR** → **Employees** → **Invite employee**. Name, email and at least one role are required; the base role is always included. Optional: locations. Up to 50 people at once.

- The invitation is sent by email, the link is valid for **7 days**. If the email does not arrive, copy the link from the list.
- The invited person must register with **exactly this** email address, password at least 8 characters.
- **Resend** creates a new link for 7 days, the old one becomes invalid.
- If there is already an active account or an open invitation for the address, the invitation is rejected.
- A previously deleted account with the same address is reactivated, with new roles and without the old two-factor setup.
- If you require the employee data form, the person is prompted to fill it in after accepting.

Legal representatives

Legal representatives are the people who legally represent the business. Only they can accept or object to the terms and the DPA, cancel the Unitlify account, and they receive the confirmation when modules are cancelled. The tab **Settings** → **Legal** is only visible to them.

- Only a legal representative can grant this right, and only to administrators.
- The last legal representative can neither lose the right nor be deleted.

Two-factor authentication

Every person can set up a second factor under **My profile**: authenticator app (with backup codes) or passkey. Setup is only possible on the web, the app asks for the code afterwards.

Under **Settings** → **Operations** → **Security** you can **enforce** the second factor for all employees or for individual roles. Anyone who has not set it up yet then only sees the setup screen on the web and cannot log in to the app. So announce the requirement and give the team time before you flip the switch. As long as the requirement applies, nobody can remove their last factor.

Sessions and passwords

- If a person changes their password or email, all other devices are logged out.
- If an employee is deactivated or deleted, their sessions end immediately.
- After 10 failed login attempts, the account is locked for 30 minutes.
- When logging in from a new device, the person receives a notification email.
- Forgotten password: 6-digit code by email, valid for 15 minutes.

Phone book

Every active person appears in the phone book, with name, roles and locations. Whether email, phone, bio and picture are visible is set by each person under **My profile** ("Profile visible within the organization" and the switches per field). External contacts have their own tab with its own permission.

Troubleshooting checklist

- **New employee sees nothing after logging in:** the base role "Employee" has no permissions. Add permissions for shifts, leave, sick notes and clocking there.
- **Everyone suddenly sees finance:** a permission was given to the base role or a low role and inherited upwards.
- **Shift lead cannot see bookings:** one of their roles carries the shift restriction and they currently have no shift in the plan.
- **Invitation cannot be accepted:** link older than 7 days, different email address, or an account already exists.
- **App login fails after enabling the two-factor requirement:** the person must first set up the second factor on the web under "My profile".
- **"Legal" is missing in the settings:** the person is not a legal representative.