

# Rôles et permissions

Créer des rôles, attribuer des permissions, comprendre l'héritage, inviter des collaborateurs, imposer l'authentification à deux facteurs, représentants légaux et restriction au service. Avec les erreurs typiques.

[unitlify.de/docs/rollen-rechte](https://unitlify.de/docs/rollen-rechte) · 2026-10-22

## Comment fonctionnent les permissions dans Unitlify

---

Chaque personne possède un ou plusieurs **rôles**. Chaque rôle porte une liste de **permissions**, par exemple « Voir les réservations » ou « Créer des services ». Ce qu'une personne a le droit de faire est la somme des permissions de ses rôles. Les permissions s'appliquent à toute l'entreprise.

Unitlify crée deux rôles à la création de l'entreprise :

- **Administrateur** : possède toutes les permissions, y compris toutes celles à venir. Les permissions ne peuvent pas être modifiées et le rôle ne peut pas être supprimé. La première personne de l'entreprise est administrateur et représentant légal (voir plus bas).
- **Collaborateur** : le rôle de base. Chaque personne invitée le reçoit automatiquement. Il est **vide** au départ, vous définissez vous-même ce que chacun a le droit de faire dans l'entreprise.

Menu **Administration** → **Rôles**. Vous avez besoin de la permission « Voir les rôles » pour les consulter et « Créer des rôles/Modifier les rôles » pour les changer.

## Configurer le rôle de base « Collaborateur »

---

C'est l'étape la plus importante après le démarrage. Tout ce que chaque personne de l'entreprise doit voir appartient au rôle de base, par exemple :

- Voir ses propres services et postuler aux services ouverts
- Demander des congés, déposer un arrêt maladie, voir ses propres absences
- Pointer et consulter son propre compte de temps
- Chat, fil d'actualités, annuaire

Sans ces permissions, les collaborateurs invités ne voient presque rien après la connexion. Même la page « Mes services » n'apparaît qu'avec une permission correspondante.

À l'inverse : ce que possède le rôle de base, **tous** les rôles au-dessus le possèdent automatiquement. Les permissions réservées aux responsables n'ont donc pas leur place dans le rôle de base.

Les postes comme « Chef d'équipe » ou « Formateur » se créent comme rôles distincts. Ils ne portent que les permissions qui vont au-delà du rôle de base.

## Créer des rôles

---

**Nouveau rôle** : code (unique par entreprise), nom, éventuellement une description et un taux horaire. Vous cochez ensuite les permissions, regroupées par domaine : Dashboard, Communication, Système de réservation, Billetterie & bons cadeaux, Finances, Personnel, Formations, Contrats & formulaires, Administration.

Un nouveau rôle se place directement au-dessus du rôle de base dans le classement.

Si vous cochez **toutes** les permissions, le rôle devient un rôle à droits complets comme l'administrateur, y compris toutes les permissions ajoutées par la suite. Utilisez cela en connaissance de cause.

### Modèle « Cabinet comptable (lecture seule) »

Via **Modèle**, vous créez un rôle de lecture prêt à l'emploi pour l'expert-comptable : lecture seule des factures, réservations, finances, factures Unitlify et notes de frais. Il n'hérite de rien et se place directement sous l'administrateur. Attention : chaque personne invitée reçoit en plus le rôle de base et compte dans les forfaits avec un prix par collaborateur.

## Héritage et classement

---

Les rôles sont ordonnés dans un classement (rang 1 tout en haut). **Un rôle hérite de toutes les permissions des rôles situés en dessous de lui.** Les permissions héritées sont marquées en bleu et peuvent être décochées individuellement par rôle si un rôle supérieur ne doit expressément pas avoir une certaine permission.

Triez par glisser-déposer. Exemple : rôle de base « Collaborateur » en bas, au-dessus « Formateur », au-dessus « Chef d'équipe », au-dessus « Direction d'exploitation ». La direction d'exploitation a ainsi tout ce que possèdent les trois rôles en dessous, plus ses propres permissions.

Deux choses ne sont jamais héritées : le marquage droits complets (« toutes les permissions ») et la restriction au service (ci-dessous).

Les modifications de permissions, les attributions de rôles, le réordonnement et la suppression de rôles prennent effet immédiatement, sans nouvelle connexion.

## Restriction au service

---

Trois permissions existent dans la variante « uniquement pendant son propre service » : réservations, envois de formulaires et Service Center. Une personne avec cette variante ne voit les données que tant qu'elle est en service selon le planning (heure de Berlin, sans marge). En dehors, le message « En dehors de votre service, vous n'avez pas accès à ces données » s'affiche.

Important : la restriction s'applique à la **personne entière** dès que l'un de ses rôles la porte, sauf si un autre rôle a des droits complets. N'attribuez donc pas la restriction à un rôle que les

responsables portent également en complément. Et : qui n'a pas de service dans le planning n'a pas d'accès.

## Sites

---

Sous **Administration** → **Sites**, vous créez des sites avec des secteurs et sous-secteurs et y affectez des collaborateurs. L'affectation détermine ce qu'une personne voit dans l'annuaire, les canaux de chat, les tâches et le stockage, et sert de filtre dans les listes du personnel. Les permissions elles-mêmes s'appliquent à toute l'entreprise, indépendamment du site.

## Inviter des collaborateurs

---

Menu **Personnel** → **Collaborateurs** → **Inviter un collaborateur**. Obligatoires : nom, e-mail et au moins un rôle ; le rôle de base est toujours inclus. Optionnel : sites. Jusqu'à 50 personnes à la fois.

- L'invitation part par e-mail, le lien est valable **7 jours**. Si l'e-mail n'arrive pas, copiez le lien depuis la liste.
- La personne invitée doit s'inscrire avec **exactement cette** adresse e-mail, mot de passe d'au moins 8 caractères.
- **Renvoyer** génère un nouveau lien valable 7 jours, l'ancien devient invalide.
- S'il existe déjà un compte actif ou une invitation en cours pour l'adresse, l'invitation est refusée.
- Un compte supprimé auparavant avec la même adresse est réactivé, avec de nouveaux rôles et sans l'ancienne configuration à deux facteurs.
- Si vous exigez le questionnaire du personnel, la personne reçoit l'invitation à le remplir après avoir accepté.

## Représentants légaux

---

Les représentants légaux sont les personnes qui représentent juridiquement l'entreprise. Eux seuls peuvent accepter ou refuser les CGV et le contrat de sous-traitance, résilier le compte Unitlify, et ils reçoivent la confirmation lors des résiliations de modules. L'onglet **Paramètres** → **Mentions légales** n'est visible que pour eux.

- Seul un représentant légal peut attribuer ce droit, et uniquement à des administrateurs.
- Le dernier représentant légal ne peut ni perdre ce droit ni être supprimé.

## Authentification à deux facteurs

---

Chaque personne peut configurer un second facteur sous **Mon profil** : application d'authentification (avec codes de secours) ou passkey. La configuration n'est possible que sur le web, l'application demande ensuite le code.

Sous **Paramètres** → **Exploitation** → **Sécurité**, vous pouvez **imposer** le second facteur à tous les collaborateurs ou à certains rôles. Qui ne l'a pas encore configuré ne voit alors plus que l'écran de configuration sur le web et ne peut pas se connecter dans l'application. Annoncez donc l'obligation et laissez du temps à l'équipe avant d'activer l'interrupteur. Tant que l'obligation s'applique, personne ne peut supprimer son dernier facteur.

## Sessions et mots de passe

---

- Si une personne change son mot de passe ou son e-mail, tous les autres appareils sont déconnectés.
- Si un collaborateur est désactivé ou supprimé, ses sessions prennent fin immédiatement.
- Après 10 tentatives de connexion échouées, le compte est bloqué pendant 30 minutes.
- Lors d'une connexion depuis un nouvel appareil, la personne reçoit un e-mail d'avertissement.
- Mot de passe oublié : code à 6 chiffres par e-mail, valable 15 minutes.

## Annuaire

---

Chaque personne active apparaît dans l'annuaire, avec nom, rôles et sites. Chaque personne règle elle-même sous **Mon profil** si l'e-mail, le téléphone, la bio et la photo sont visibles (« Profil visible au sein de l'organisation » et les interrupteurs par champ). Les contacts externes ont leur propre onglet avec une permission dédiée.

## Liste de contrôle en cas de problème

---

- **Un nouveau collaborateur ne voit rien après la connexion** : le rôle de base « Collaborateur » n'a pas de permissions. Y inscrire les permissions pour les services, congés, arrêts maladie et pointage.
- **Tout le monde voit soudain les finances** : une permission a été attribuée au rôle de base ou à un rôle inférieur et héritée vers le haut.
- **Le chef d'équipe ne voit pas les réservations** : l'un de ses rôles porte la restriction au service et il n'a actuellement pas de service dans le planning.
- **L'invitation ne peut pas être acceptée** : lien de plus de 7 jours, autre adresse e-mail, ou un compte existe déjà.
- **La connexion dans l'application échoue après activation de l'obligation à deux facteurs** : la personne doit d'abord configurer le second facteur sur le web sous « Mon profil ».
- **« Mentions légales » manque dans les paramètres** : la personne n'est pas représentant légal.