Fiche mémo

Gestion des permissions et des droits utilisateurs

Principe général

Chaque objet d'eLabFTW (Expérience, Ressource, Modèle…) possède deux types de permissions distincts et indépendants : **Lecture (Read / « Can view ») — qui peut voir l'entrée** — et **Écriture (Write / « Can edit ») — qui peut la modifier**.

Avoir le droit d'écriture donne aussi le droit de modifier les permissions de l'entrée elle-même. Les permissions sont additives : on part d'une permission de base, que l'on peut ensuite étendre à des équipes, groupes ou utilisateurs supplémentaires.

1. Les niveaux de « permission de base »

Niveau	Signification
Uniquement le propriétaire (Only me / Only owner)	Seul le créateur de l'entrée y a accès
Propriétaire + Admins (Only me + Admins)	Le créateur et les Admins de l'équipe
Équipe (Team)	Tous les membres de l'équipe dans laquelle l'entrée a été créée
Groupes d'utilisateurs (Team groups / User groups)	Membres d'un groupe défini par un Admin (peut inclure des utilisateurs d'autres équipes)
Tout le monde avec un compte (Everyone with an account)	Tous les comptes de l'instance, toutes équipes confondues
Tout le monde y compris anonyme (Everyone including anonymous)	Accès public, y compris sans compte (cette options est désactivée par le Sysadmin, un compte est obligatoire pour accéder au CLE)

⚠️ Le Sysadmin peut désactiver certains niveaux au niveau serveur (ex. interdire « Uniquement moi » pour garantir l'accès des Admins, ou bloquer les niveaux « Tout le monde… » pour éviter les fuites accidentelles entre équipes).

2. Extension additive des permissions

Depuis la fenêtre « Permissions » (icône +) d'une expérience ou d'une ressource, on peut ajouter, en plus de la base :

- une équipe entière
- un groupe d'utilisateurs (Team group / User group, créé par un Admin)
- un utilisateur individuel (y compris d'une autre équipe)

Ces ajouts se cumulent à la permission de base sans la remplacer.

3. Réglages par défaut

Objet	Lecture par défaut	Écriture par défaut
Expérience	Équipe (tous les membres de l'équipe de création)	Propriétaire + Admins uniquement
Ressource	Équipe	Toute l'équipe peut modifier (plus permissif), configurable

Ces valeurs par défaut peuvent être personnalisées par chaque utilisateur dans ses préférences personnelles, ou imposées par un Admin au niveau de toute l'équipe. Il est recommandé de mettre en valeur par défaut « Uniquement le propriétaire » puis d''étendre les persmissions si nécessaire.

4. Cas particuliers par type d'objet

Modèles (Templates)

Depuis la version 5.0, deux jeux de permissions distincts existent pour un modèle : celui du modèle lui-même (qui peut le voir/modifier), et celui des entrées créées à partir de ce modèle (permissions héritées par défaut, mais modifiables).

Un modèle peut aussi contenir des étapes verrouillées : lorsqu'une expérience/ressource est créée à partir du modèle, ces étapes apparaissent en lecture seule et ne peuvent être ni modifiées ni supprimées.

Ressources réservables

Quand une Ressource est rendue « réservable », une permission supplémentaire apparaît : « Peut réserver ». Par défaut elle correspond à la permission de lecture, mais peut être ajustée indépendamment.

Catégories de ressources

Définies par l'Admin, communes à l'équipe. Elles ne portent pas (à ce jour) de permission fine de type « qui peut créer une entrée dans cette catégorie » — une demande d'évolution existe sur ce point auprès du projet.

Groupes d'utilisateurs

Créés par un Admin depuis le « Panneau d'administration ». Un membre du groupe peut restreindre la visibilité/l'édition d'une entrée à ce seul groupe. Un groupe peut inclure des utilisateurs d'autres équipes.

Partage par lien (accès anonyme ponctuel)

Indépendamment de la permission de base, chaque entrée peut générer un lien avec clé d'accès unique, partageable pour donner un accès en lecture seule, même à quelqu'un sans compte — révocable à tout moment en désactivant l'option.

5. Rôle des Admins et du Sysadmin

- Un Admin peut, depuis le Panneau d'administration, imposer des permissions de lecture/écriture par défaut à toute son équipe : les utilisateurs ne peuvent plus s'en écarter tant que ce mode reste actif.
- Le Sysadmin peut, au niveau serveur, désactiver certains niveaux de permission de base pour toute l'instance (ex. interdire l'accès public anonyme).
- Le Sysadmin peut aussi effectuer des corrections en masse des permissions existantes via des requêtes SQL directes (utile en cas de changement de politique après coup).

Tableau de synthèse

Élément	Portée	Qui peut le configurer
Permission de base d'une entrée	Cette entrée uniquement	Créateur / tout utilisateur ayant le droit d'écriture
Extension à équipe/groupe/utilisateur	Cette entrée uniquement	Idem
Permissions par défaut personnelles	Toutes les futures entrées de l'utilisateur	L'utilisateur lui-même (préférences)
Permissions imposées (enforced)	Toute l'équipe	Admin
Désactivation de niveaux de permission	Toute l'instance	Sysadmin
Permissions du modèle vs. entrée créée	Modèle et objets dérivés	Créateur/éditeur du modèle
« Can book »	Ressource réservable	Créateur/éditeur de la ressource

Points clés à retenir

- Lecture et écriture sont toujours séparées et se configurent indépendamment.
- Le système est additif : base + extensions, jamais une liste figée unique.
- Les Ressources sont plus ouvertes en écriture par défaut que les Expériences (toute l'équipe vs. propriétaire + Admins seulement).
- Un modèle a désormais ses propres permissions, distinctes de celles des entrées qu'il génère.
- Le partage par lien à clé d'accès contourne temporairement la permission de base, sans la modifier.
- Les Admins et le Sysadmin disposent de leviers pour encadrer (imposer ou restreindre) les choix laissés aux utilisateurs.