Suivre la double authentification des utilisateurs (administrateurs)

Pour les ADMIN et SUPERADMIN.

Dans la liste des utilisateurs

Une cellule indique, pour chaque compte, les seconds facteurs de la personne : **e-mail** ou **e-mail + application**.

- **Vert** : au moins ce qu'exigent ce royaume et ceux du dessus pour ce compte.
- **Rouge** : en dessous. Un « e-mail » rouge signifie qu'une application est exigée et pas encore configurée : la personne devra la configurer à sa prochaine connexion.

La cellule ne montre jamais les navigateurs de confiance, le nombre de codes de récupération ni la dernière méthode utilisée.

Dans la fiche de l'utilisateur

Le bloc **Double authentification** de la fiche reprend cet état et, seulement quand c'est le cas :

- **Exempté jusqu'au …** — voir Exemption temporaire ;
- **Second facteur bloqué** — voir Réinitialisation du second facteur.

Un ADMIN voit ce bloc en lecture seule. Un SUPERADMIN y trouve en plus les boutons des gestes qu'il a le droit de faire ; un bouton grisé explique pourquoi (par exemple « comptes hors de vos royaumes : seul le Support Improvize peut réinitialiser »).

Le journal de sécurité

Voir le journal liste les événements de sécurité de la personne : connexions refusées, application ajoutée ou retirée, navigateurs de confiance, gestes des administrateurs, connexions des applications bureau. Il n'est visible que d'un SUPERADMIN qui pourrait réinitialiser cette personne (et de la personne elle-même), car il peut concerner d'autres royaumes. Les entrées sont gardées 12 mois.

Revision #3
Created 2026-11-08 11:11:38 UTC by Claude-Aida
Updated 2026-11-09 13:28:32 UTC by Claude-Aida