Groupes d'accès — guide de prise en main

> Destiné aux administrateurs et aux testeurs. Aucune connaissance technique requise.
> Emplacement dans l'application : **Administration › Groupes d'accès**.

---

1. À quoi ça sert

Par défaut, chaque salarié voit toutes les données de l'application que ses permissions de rôle l'autorisent à voir. C'est suffisant pour une structure unique, mais pas pour une organisation répartie en agences, en services ou en antennes.

Les groupes d'accès répondent à ce besoin : **cloisonner qui voit quoi**, sans avoir à retoucher les rôles et les permissions de chacun.

Deux exemples réels :

- Une entreprise avec deux agences (Lyon et Gravelines). Chaque agence ne doit voir que ses propres affaires, devis et factures. La direction continue de tout voir.
- Une association avec des services et des responsables. Le responsable d'un service doit accéder aux données de toute son équipe — mais les responsables ne doivent pas se voir entre eux.

---

2. La règle d'or

> **Un groupe d'accès restreint. Il n'accorde jamais de droit.**

C'est le principe le plus important à retenir, et la source de la plupart des malentendus.

Mettre quelqu'un dans un groupe ne lui donne **jamais** accès à quelque chose qu'il ne pouvait pas voir avant. Ça ne fait que **retirer** de la visibilité. Les permissions du rôle continuent de s'appliquer par-dessus, et c'est toujours la règle la plus restrictive qui gagne.

Trois conséquences directes :

Situation	Ce que voit le salarié
Dans **aucun** groupe	Tout, exactement comme avant. Rien ne change pour lui.
Dans un groupe **désactivé**	Tout. Un groupe inactif ne restreint plus personne.
Case **« Voir tout »** cochée sur sa fiche	Tout, même s'il reste membre d'un groupe.

Les administrateurs et le support voient toujours l'intégralité des données, quoi qu'il arrive.

---

3. Les trois niveaux

Un groupe contient trois types de personnes, organisés en **niveaux de visibilité** volontairement asymétriques.

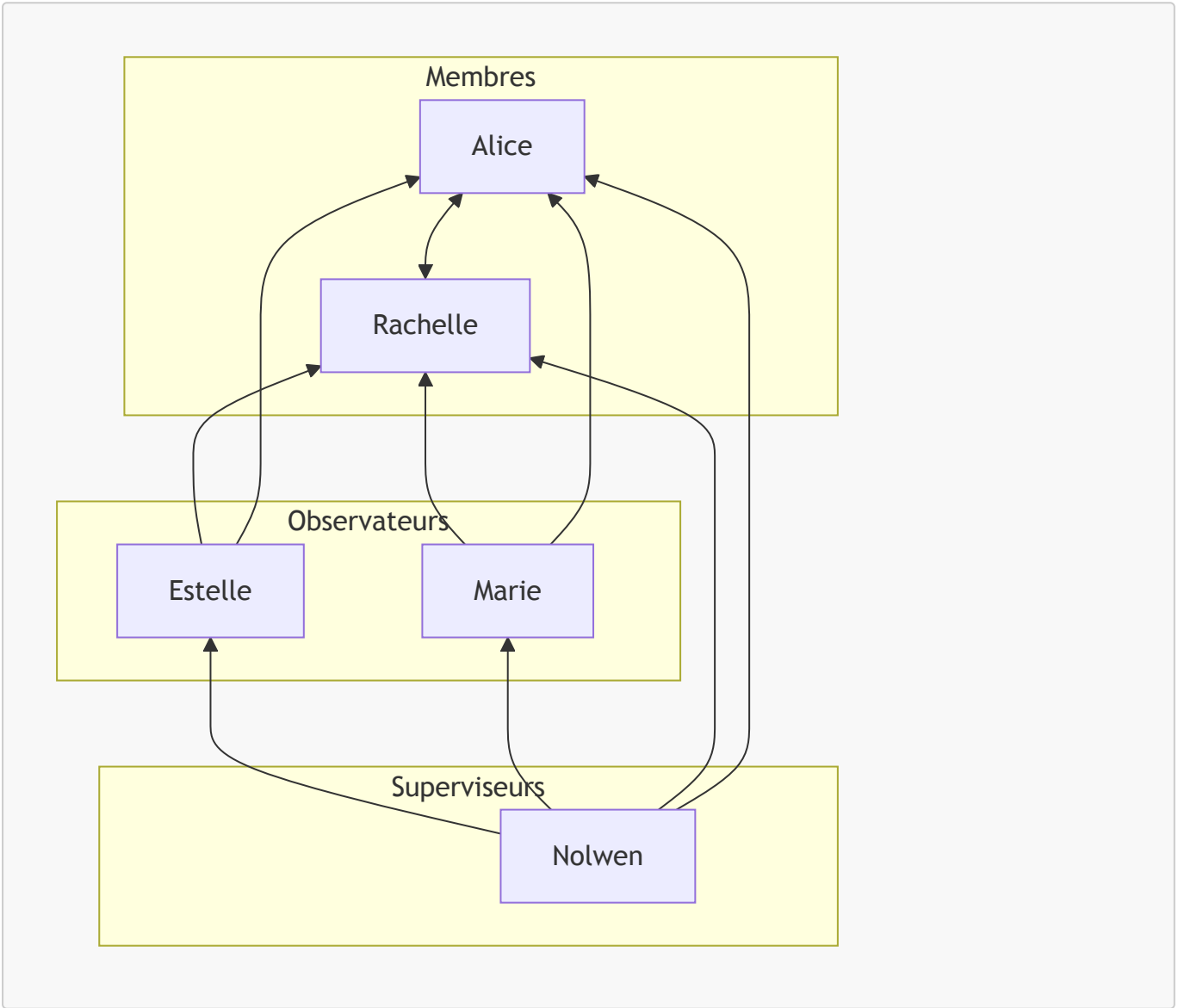
Les membres mettent leurs données en commun. Chaque membre voit les données des autres membres, et les siennes sont visibles par eux. C'est une relation réciproque.

Les observateurs accèdent aux données de tous les membres, **sans partager les leurs** — ni avec les membres, ni avec les autres observateurs. C'est une relation à sens unique.

Les superviseurs accèdent aux données des membres **et des observateurs**, toujours sans partager les leurs et sans voir les autres superviseurs.

Une seule règle produit ces trois comportements :

> **On voit les niveaux situés en dessous du sien, jamais le sien ni au-dessus.** Les membres font exception entre eux : ils forment le socle commun et se voient mutuellement.



Une flèche signifie « voit les données de ». Nolwen voit tout le monde. Estelle et Marie voient Rachelle et Alice, mais pas l'une l'autre, et pas Nolwen. Rachelle et Alice se voient mutuellement.

Qui voit qui, précisément

	Voit Rachelle (membre)	Voit Estelle (obs.)	Voit Marie (obs.)	Voit Nolwen (sup.)
Rachelle (membre)	ses données	non	non	non
Estelle (observatrice)	oui	ses données	non	non
Marie (observatrice)	oui	non	ses données	non
Nolwen (superviseur)	oui	oui	oui	ses données

Chacun garde **toujours** l'accès à ses propres données. Appartenir à un groupe ne retire jamais à quelqu'un ce qui lui appartient.

Quand utiliser lequel

- **Membres** : des collègues d'un même service qui travaillent ensemble et doivent voir les dossiers les uns des autres.
- **Observateurs** : un responsable, un contrôleur de gestion, un auditeur — quelqu'un qui doit consulter sans que ses propres dossiers deviennent visibles par l'équipe.
- **Superviseurs** : le niveau au-dessus, pour qui doit voir à la fois l'équipe **et ses responsables** — un directeur de pôle, un référent RH. Sans ce niveau, il faudrait créer un groupe par responsable à observer.

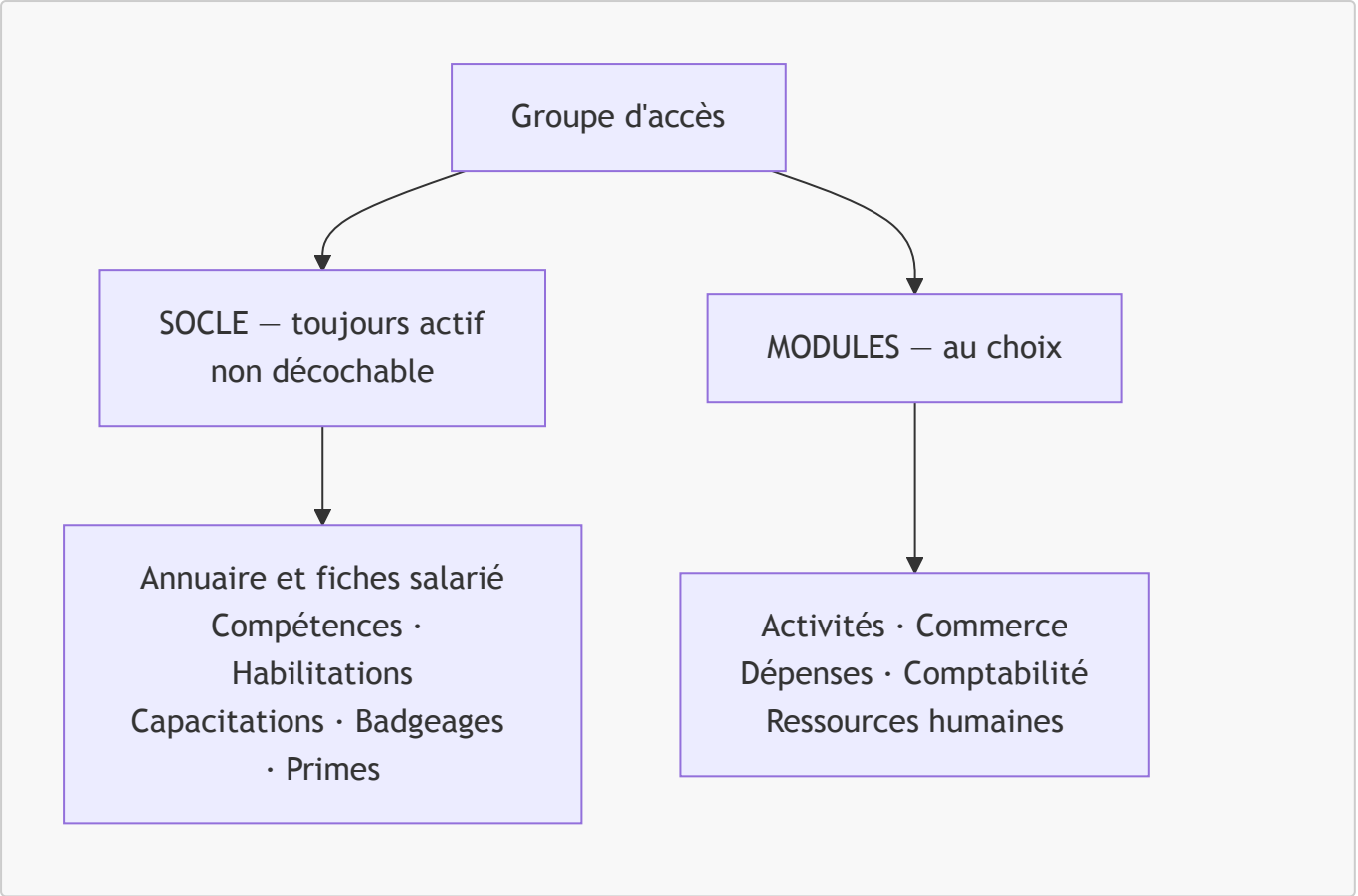
> Deux personnes de même niveau ne se voient jamais — deux observateurs comme deux superviseurs. Si elles doivent se voir, créez un groupe séparé où elles sont **membres**.

> ⚠️ Ni « observateur » ni « superviseur » ne veulent dire « lecture seule », et « superviseur » n'accorde aucun pouvoir de gestion. Un observateur peut **modifier** les données des membres si ses permissions de rôle le lui permettent. Ces mots décrivent ce que la personne voit, pas ce qu'elle a le droit de faire.

---

4. Le périmètre : socle et modules

Un groupe ne cloisonne pas forcément toute l'application. Vous choisissez les **modules** concernés.



Le socle : toujours cloisonné

Dès qu'un salarié appartient à un groupe actif, **la visibilité des salariés est restreinte**, quels que soient les modules cochés. Il ne verra dans l'annuaire, les fiches salarié, les compétences, les habilitations, les capacitations, les badgeages et les primes que les personnes de son périmètre.

Ce socle n'est pas décochable : c'est la raison d'être d'un groupe d'accès.

Les modules : à la carte

Le reste s'active module par module. Ils sont regroupés par domaine pour faciliter la configuration — cocher un domaine coche tous ses modules d'un coup.

Domaine	Modules
Activités	Affaires · Livraisons · Mouvements
Commerce	Devis · Commandes · Factures · Avoirs · Études · Récurrences
Dépenses	Factures fournisseur · Avoirs fournisseur · Dépenses · Notes de frais
Comptabilité	Ordres de paiement · Paiements et journal des règlements
Ressources humaines	Missions · Entretiens · Absences · Pointages

Un groupe **sans aucun module coché** reste valide : il ne cloisonne alors que le socle, c'est-à-dire la visibilité des salariés entre eux.

> Les modules **CRM, GMAO, Stock et Qualité/Sécurité** ne sont pas concernés par les groupes d'accès. Y voir des données hors de son périmètre est normal, ce n'est pas une anomalie.

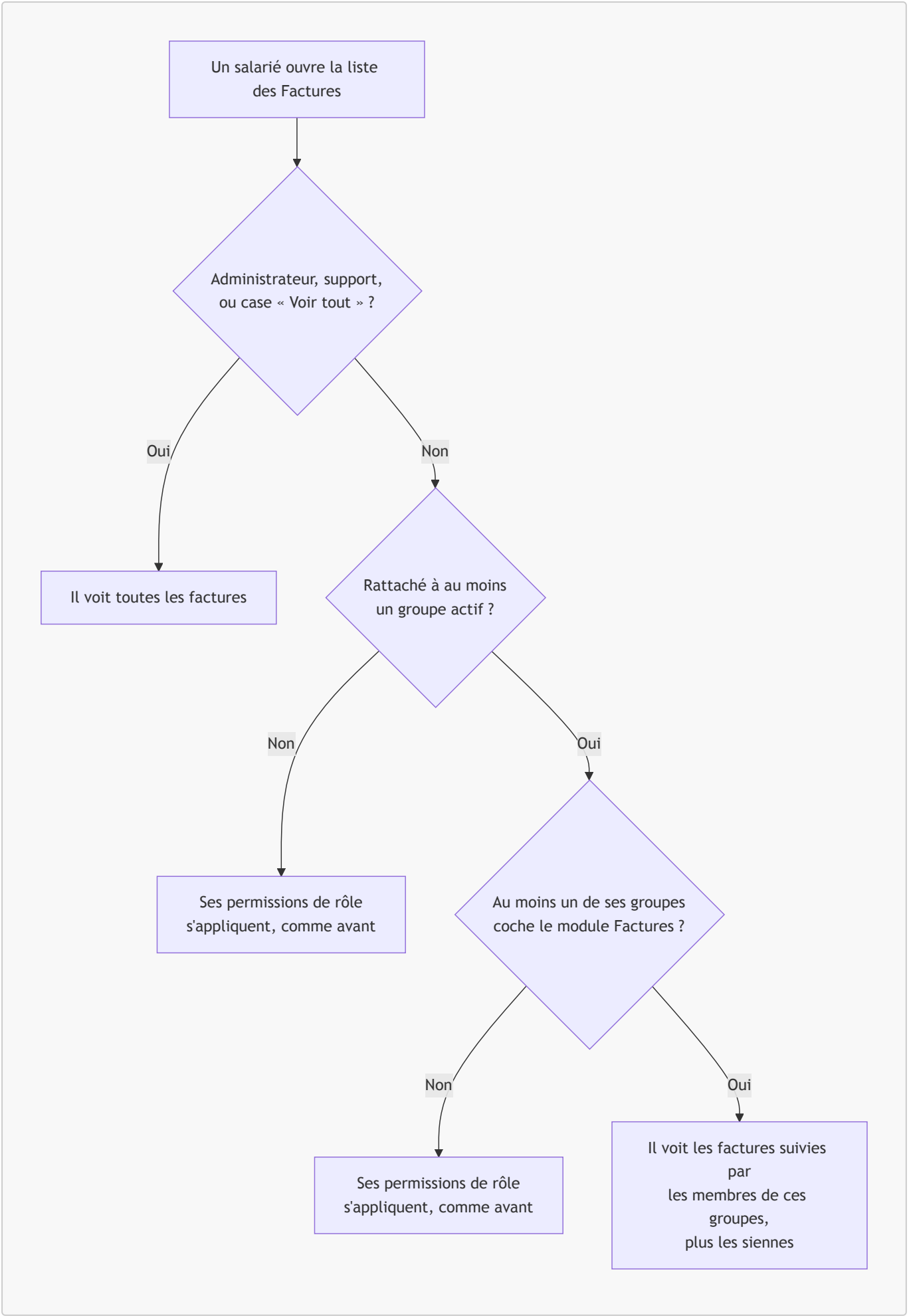
---

5. Décocher un module ≠ tout voir

C'est le point qui surprend le plus souvent.

Décocher un module ne veut **pas** dire « les membres du groupe voient tout sur ce module ». Ça veut dire « le groupe ne s'occupe plus de ce module » — et on retombe alors sur les permissions habituelles du rôle du salarié.

Or ces permissions ont souvent elles-mêmes deux niveaux : *voir mes propres documents* ou *voir tous les documents*. Si le salarié n'a que le premier niveau, décocher le module le ramènera à ses seuls documents — et il verra donc **moins** de choses que ce que vous imaginiez.

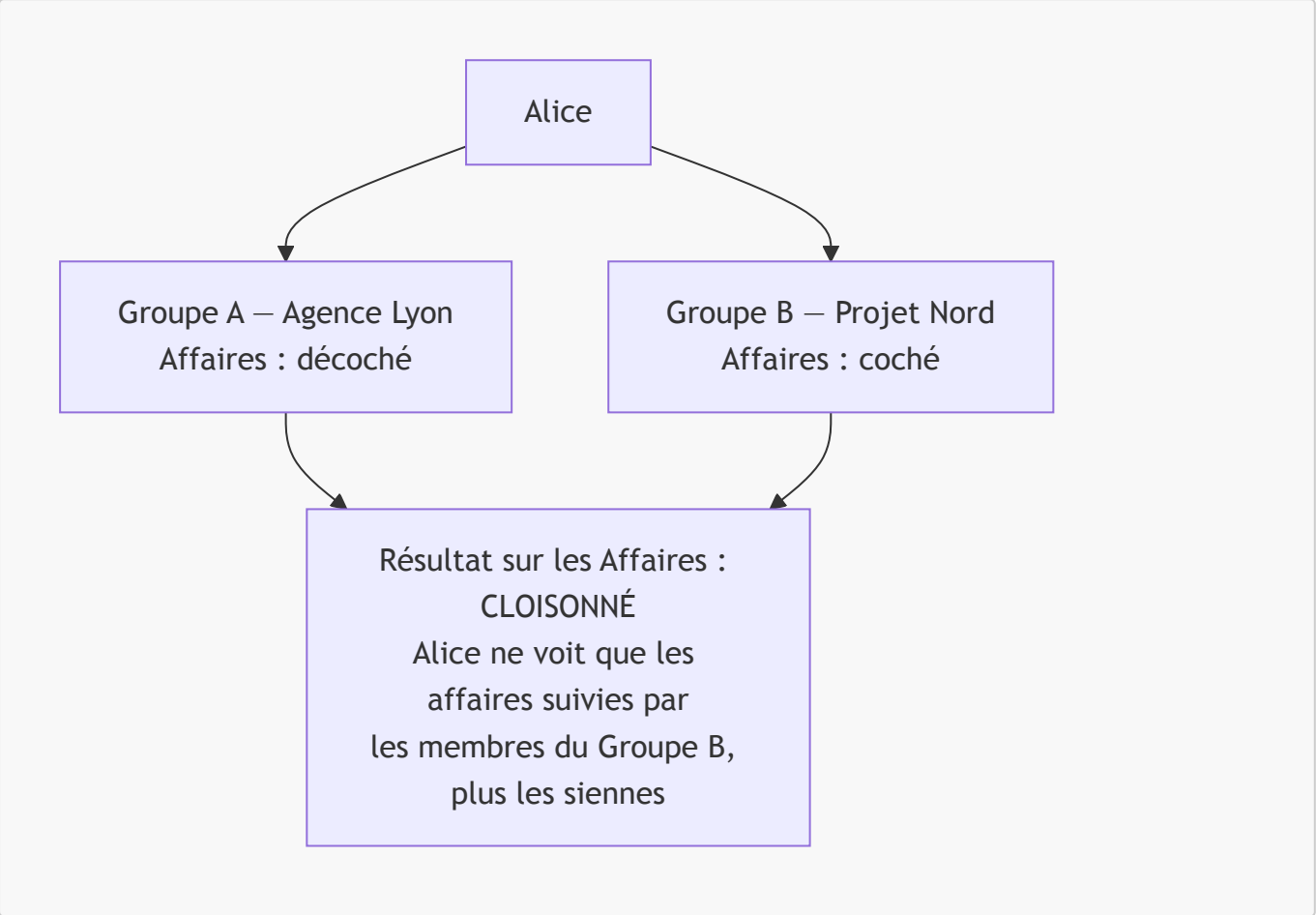

Un salarié ouvre la liste des Factures
Administrateur, support, ou case « Voir tout » ?
Oui
Non
Il voit toutes les factures
Rattaché à au moins un groupe actif ?
Non
Oui
Ses permissions de rôle s'appliquent, comme avant
Au moins un de ses groupes coche le module Factures ?
Non
Oui
Ses permissions de rôle s'appliquent, comme avant
Il voit les factures suivies par les membres de ces groupes, plus les siennes

6. Quand un salarié est dans plusieurs groupes

Un salarié peut appartenir à plusieurs groupes, et y avoir des rôles différents : membre de l'un, observateur de l'autre. C'est légitime, mais c'est là qu'on peut se perdre.

La règle : un module reste cloisonné dès qu'au moins un de ses groupes le coche.

Décocher un module sur un seul groupe ne suffit donc pas à le « libérer » si un autre groupe le coche encore.



C'est volontaire, et c'est le sens le plus sûr : un administrateur qui coche « Affaires » sur un groupe doit pouvoir compter sur le fait que ça cloisonne réellement, sans qu'un autre groupe vienne annuler sa décision en silence.

L'indicateur « Périmètre effectif »

Comme ce cumul est difficile à deviner à l'œil, la fiche salarié affiche, dans la section **Accès & groupes**, un récapitulatif : pour chaque module, il indique s'il est cloisonné et **par quel(s) groupe(s)**.

C'est le premier endroit à regarder quand un salarié ne voit pas ce que vous attendiez. L'indicateur reflète la configuration **enregistrée** : il se met à jour après avoir enregistré la fiche, pas pendant la saisie.

---

7. Mettre en place un groupe, pas à pas

1. **Créer le groupe** — *Administration › Groupes d'accès › Nouveau*. Donner un nom parlant (« Agence Lyon », « Service Animation ») et le laisser **actif**.

2. **Choisir les modules** — dans la section *Périmètre de la restriction*, cocher les domaines ou les modules concernés. En cas de doute, commencer large : vous pourrez restreindre ensuite.
3. **Ajouter les membres** — les salariés qui mettent leurs données en commun et se voient entre eux.
4. **Ajouter les observateurs** *(optionnel)* — les responsables ou contrôleurs qui doivent voir l'équipe sans être vus.

   Puis les **superviseurs** *(optionnel)* — ceux qui doivent voir l'équipe **et** ses observateurs.
5. **Vérifier** — ouvrir la fiche d'un des salariés concernés et lire son **Périmètre effectif**.
6. **Tester avec un vrai compte** — se connecter avec le compte d'un membre. Ne testez jamais avec un compte administrateur : il voit tout par construction, et vous ne verriez rien du cloisonnement.

Un salarié peut aussi être rattaché à des groupes depuis sa propre fiche (*Fiche salarié › Accès & groupes*), ce qui est plus pratique à l'embauche.

---

8. Pièges fréquents

« J'ai créé un groupe mais rien n'a changé. » Vérifiez que le groupe est actif, que le salarié y est bien rattaché, que sa case « Voir tout » est décochée, et qu'il n'est ni administrateur ni support. Vérifiez aussi que vous testez avec son compte et non le vôtre.

« Un salarié ne voit plus rien du tout. » Regardez son *Périmètre effectif*. Il est probablement seul membre de son groupe — ou membre d'un groupe dont les autres membres ne suivent aucun document. Le cloisonnement fonctionne, mais le périmètre est vide.

« J'ai décoché un module et il voit moins de choses qu'avant. » C'est le cas expliqué en section 5 : il est retombé sur ses permissions de rôle, qui sont plus restrictives que le périmètre du groupe.

« Un observateur ne voit pas les données d'un autre observateur. » C'est le comportement attendu, et c'est toute la raison d'être du niveau.

« Le responsable voit les autres responsables. » Il a probablement été ajouté comme *membre* au lieu d'*observateur*. Un salarié saisi dans plusieurs listes est traité au niveau le plus élevé.

« Mon superviseur ne voit pas un autre superviseur. » Normal : deux personnes de même niveau ne se voient jamais. Créez un groupe où elles sont membres, ou ajoutez un niveau au-dessus.

« Je ne peux pas rattacher un salarié à un groupe. » Voir la section 9 : hors administrateur, on ne peut affecter que les groupes dont on est observateur ou superviseur, et à un niveau strictement inférieur au sien.

« Les tableaux de bord affichent des chiffres hors de mon périmètre. » Normal. Les statistiques agrégées (totaux, taux, moyennes) ne sont pas cloisonnées, car elles ne nomment personne. Seuls les écrans nominatifs le sont.

---

9. Rattacher un salarié depuis sa fiche

Faire transiter chaque embauche par un administrateur n'est pas tenable au-delà de quelques dizaines de salariés. Le bloc **Accès & groupes** de la fiche salarié est donc ouvert au-delà des administrateurs, selon la même règle de niveaux que la visibilité :

> **On affecte aux niveaux situés en dessous du sien.**

Vous êtes	Vous pouvez rattacher	À quels groupes
Administrateur	membre, observateur ou superviseur	tous
Dans **aucun** groupe	membre, observateur ou superviseur	tous
Superviseur d'un groupe	membre ou observateur	ce groupe
Observateur d'un groupe	membre	ce groupe
Membre d'un groupe	rien	—

Trois précisions importantes :

- **Vous ne voyez que les groupes que vous pouvez affecter.** Les autres rattachements du salarié restent affichés, mais verrouillés : ils comptent dans le périmètre effectif et seul un administrateur peut les changer.
- **On ne modifie jamais ses propres groupes**, sauf administrateur. Sans quoi n'importe qui pourrait se retirer de son groupe pour retrouver un accès total.
- **La case « Voir tout » reste réservée aux administrateurs.** Elle annule tout le cloisonnement d'un seul clic.

Retirer un salarié de son dernier groupe

C'est autorisé, mais l'effet est double et contre-intuitif, donc un rappel s'affiche sous les champs de groupes :

- **le salarié** n'est plus restreint du tout : il retrouve toute la visibilité que son rôle autorise ;
- **vous** ne le voyez plus dans votre périmètre, et ne pourrez donc plus rouvrir sa fiche.

L'opération est tracée dans le journal, avec l'avant et l'après. C'est la première chose à consulter le jour où l'on se demande depuis quand un salarié voit l'ensemble des données.

---

10. Ce qu'il faut vérifier avant une mise en production

La priorité absolue n'est pas que le cloisonnement fonctionne — c'est que **rien ne change pour les salariés qui ne sont dans aucun groupe**, c'est-à-dire l'immense majorité des utilisateurs.

Deux familles d'anomalies à signaler immédiatement :

- **Fuite** — une donnée visible ou modifiable alors qu'elle est hors du périmètre du groupe.
- **Régression** — une donnée devenue invisible pour quelqu'un qui n'appartient à aucun groupe.

Le cloisonnement s'applique de la même façon sur les **quatre surfaces** d'un module : la liste, la fiche détaillée, l'écran de modification et l'export Excel. Une anomalie sur une seule d'entre elles vaut la peine d'être remontée.