



# Gestion des droits

Documentation fonctionnelle

<b>Introduction</b>	<b>5</b>
<b>Comment se servir de cette documentation ?</b>	<b>5</b>
<b>Une documentation à entretenir</b>	<b>6</b>

## CHAPITRE 1 : Comprendre les 3 grands modes de gestion

<b>Faire le choix adapté</b>	<b>7</b>
Gestion par “classification” : piloter via les dossiers	7
Gestion par “cycle de vie” : utiliser les statuts	8
Gestion par contenu : la diffusion sélective de l’information	9
<b>Droits sur le plan de classement</b>	<b>10</b>
Autoriser un dossier à un groupe	10
Niveaux de droits sur un dossier	11
Héritage du dossier parent	12
Structuration du plan de classement	12
Elévation de droits impossible	12
<b>Droits par les statuts</b>	<b>14</b>
3 familles de statuts	14
Créer, modifier ou supprimer un statut	14
Les dossiers en lecture n’affichent que les éléments publiés	16
Appliquer des restrictions selon les statuts à un groupe utilisateur	16
Publication et champs obligatoires	18
Qu’est-ce qu’un statut “public” ?	18
Automatiser les changements de statut	19
<b>Diffusion sélective de l’information (ABAC)</b>	<b>20</b>
Principe	20
Paramétrer la diffusion sélective	20
Précautions d’usage	22

## CHAPITRE 2 : Connaître les principes fondamentaux

<b>Groupes, licences et fonctionnalités autorisées</b>	<b>23</b>
4 différents niveaux de groupe	23
Fonctionnalités sur les assets	24
Fonctionnalités de diffusion	25
Fonctionnalités de recherche	25
Fonctionnalités collaboratives	26
Fonctionnalités d’administration	26
Fonctionnalités du portail utilisateur	27
Paramétrage des fonctionnalités autorisées au groupe	27
<b>Formats d’exports et niveaux de téléchargement</b>	<b>29</b>

Notion de haute et basse définition	29
Définir les formats d'export autorisés d'un groupe	30
Modes de téléchargement	31
Le niveau de téléchargement occasionne d'autres impacts	32
<b>Autres notions de paramétrage de droits</b>	<b>33</b>
Planches-contacts	33
Fiches autorisées à la création	33
Champs visibles / modifiables par les non administrateurs	35
Filtrage IP	37
<b>Droits dans les espaces collaboratifs</b>	<b>40</b>
Paniers et workflow : le droit du propriétaire prévaut	40
Tableau : chaque membre est responsable de ce qu'il partage	40
Classement dans un dossier	41
Cas particulier pour la diffusion sélective de l'information (ABAC)	42
Accès administrateur à tous les espaces collaboratifs	42

## CHAPITRE 3 : Gestion avancée pour les projets d'envergure

<b>Multigroupe</b>	<b>44</b>
Du multigroupe pour gérer du multi-marques	44
Module d'inscription	44
Quels droits prévalent entre 2 groupes ?	45
Un groupe additionnel pour un droit transverse à plusieurs groupes	45
Groupes gestionnaires et sous-groupes	46
Précautions d'usage	46
<b>Administration déléguée aux gestionnaires</b>	<b>47</b>
Paramétrage des fonctionnalités autorisées à la gestion	47
Gestion d'utilisateurs	49
Gestion documentaire	50
Gestion des contenus	50
Autres	51
<b>Accès aux applications</b>	<b>54</b>
Portée des droits du Backoffice	54
Autoriser une autre application à un groupe	54
Portail et Keepicker : cloisonnement par filtrage permanent	55
Cloisonnement des paniers	56

## CHAPITRE 4 : Informations complémentaires

<b>F.A.Q : foire aux questions</b>	<b>58</b>
Peut-on masquer un sous-dossier à un groupe ?	58
Un asset est présent dans 2 dossiers sur lesquels un groupe à des droits différents, que se passera-t-il ?	58

Un utilisateur est attribué à 2 groupes qui ont des droits différents sur un même dossier, que se passera-t-il ?	58
Les visiteurs ne voient pas certains médias alors que je n'utilise pas la restriction par statut, pourquoi ?	59
Pourquoi les utilisateurs voient dans leur filtres des noms de fiche ou de champs qui ne leur sont pas autorisés ?	59
Lorsqu'un contributeur crée un média, ce média disparaît immédiatement après sa création ! Pourquoi ?	59
En tant qu'administrateur, comment accéder aux contenus des murs d'import?	59
<b>Annexes</b>	<b>60</b>
Annexe 1 : pyramide des droits	60
Annexe 2 : complexité du modèle de droits sur dossiers	62
Annexe 3 : réflexions sur la simplification du module de droits	63
Annexe 4 : refonte complète du module ?	69

# Introduction

Une solution de Digital Asset Management se doit d'offrir une capacité de contrôle d'accès aux contenus qui sache s'adapter au contexte de toute entreprise. Keepeek a construit au fil des années de nombreuses fonctionnalités de gestion de droits, qui offrent une palette très versatile de paramétrages.

Leur nombre implique aussi de la complexité, cette documentation va vous permettre d'y voir plus clair sur les bonnes pratiques et les logiques de mise en place.

## Comment se servir de cette documentation ?

Il y a beaucoup de choses dans cette documentation. On peut facilement s'y perdre. Selon ce que vous cherchez, voici comment aborder cette documentation.

La partie 1 "[Faire le choix adapté](#)" est destinée à comprendre les 3 différentes approches de gestion des droits proposées dans Keepeek. Cette question doit être étudiée et maîtrisée avant le démarrage d'un projet.

S'en suivent une explication détaillée de chacun de ces 3 modes. Selon votre mode de gestion ou votre problématique, vous trouverez probablement les informations dans ces rubriques.

- [Droits sur le plan de classement](#)
- [Droits par les statuts](#)
- [Diffusion sélective de l'information \(ABAC\)](#)

Vous allez ensuite retrouver différents principes de bases des droits qu'il est important de maîtriser.

- [Groupes, licences et fonctionnalités autorisées](#)
- [Formats d'exports et niveaux de téléchargement](#)
- [Autres notions de paramétrage de droits](#)
- [Droits dans les espaces collaboratifs](#)

Trois autres sections un peu plus spécifiques s'adressent seulement aux projets de grosse envergure (multi-marques, plusieurs applications, etc). Toutefois, de plus petits projets peuvent aussi y trouver une utilité selon le contexte.

- [Multigroupe](#)
- [Administration déléguée aux gestionnaires](#)
- [Accès aux applications](#)

Enfin, vous trouverez une [F.A.Q](#) qui ne demande qu'à s'étoffer avec le temps ainsi que des documents en [annexe](#) pour les plus grands passionnés de droits.

## Une documentation à entretenir

Cette documentation ne demande qu'à être enrichie, à la fois en termes de précision et d'exhaustivité d'informations, mais aussi pour apporter des regards complémentaires, des retours d'expériences, des exemples pratiques, des astuces, etc.

N'hésitez pas à y apporter votre contribution.

# CHAPITRE 1

Comprendre les 3 grands modes de gestion

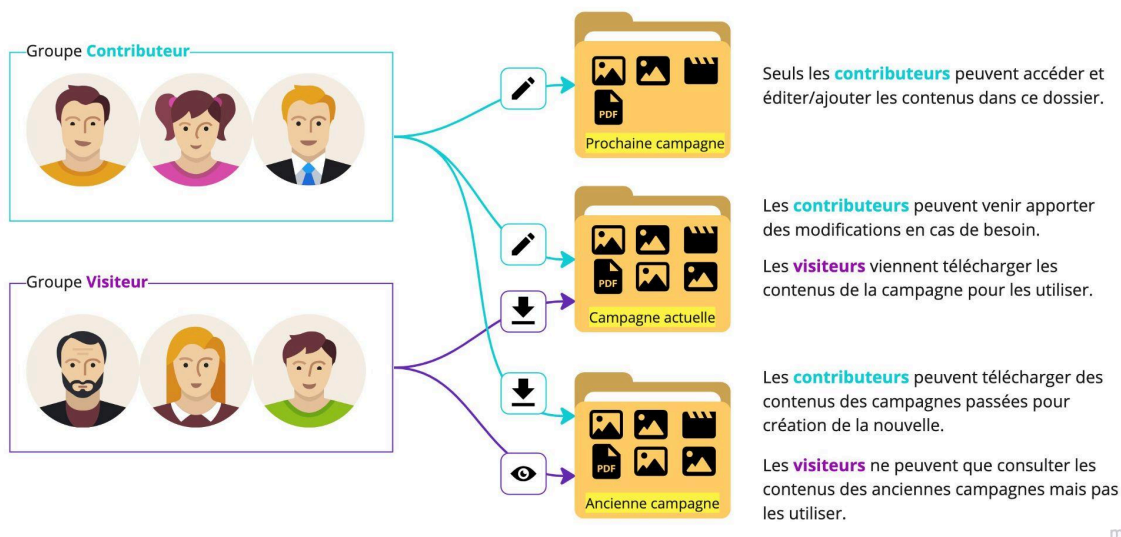
## Faire le choix adapté

Dans Keepeek, la gestion des droits peut paraître compliquée. Elle l'est assurément, mais parce qu'il est possible d'adapter l'outil à l'organisation interne de chaque entreprise. Beaucoup de possibilités sont en effet offertes dans l'écran d'administration. Mais il faut savoir les utiliser à bon escient, et surtout faire un choix d'orientation clair, qui va régir votre approche. Il est périlleux de vouloir utiliser toutes les mécaniques conjointement, car c'est le meilleur moyen de s'y perdre et de ne pas comprendre pourquoi les contenus sont accessibles ou pourquoi ils ne le sont pas.

## Gestion par "classification" : piloter via les dossiers

Cette approche est la plus ancienne qui existe dans Keepeek. Elle est d'ailleurs incontournable car quel que soit votre mode de gestion principal, il faudra un minimum de droit sur dossier pour la faire fonctionner (on y reviendra).

Gérer le droit sur le plan de classement indique que **vos éléments vont être visibles, ou éditables, en fonction du dossier dans lequel ils se trouvent** dans le plan de classement.



Pour un groupe visiteur, vous allez pouvoir définir quels dossiers ces visiteurs pourront consulter et s'ils sont autorisés à y télécharger des contenus.

Pour un groupe contributeur, vous pourrez déterminer qu'un dossier leur permet de travailler son contenu (ajouter des médias, les compléter, les modifier...), qu'un autre ne leur sera accessible qu'en lecture seule (qu'ils ne pourront rien y modifier) ou que même d'autres dossiers leurs soient totalement inaccessibles.

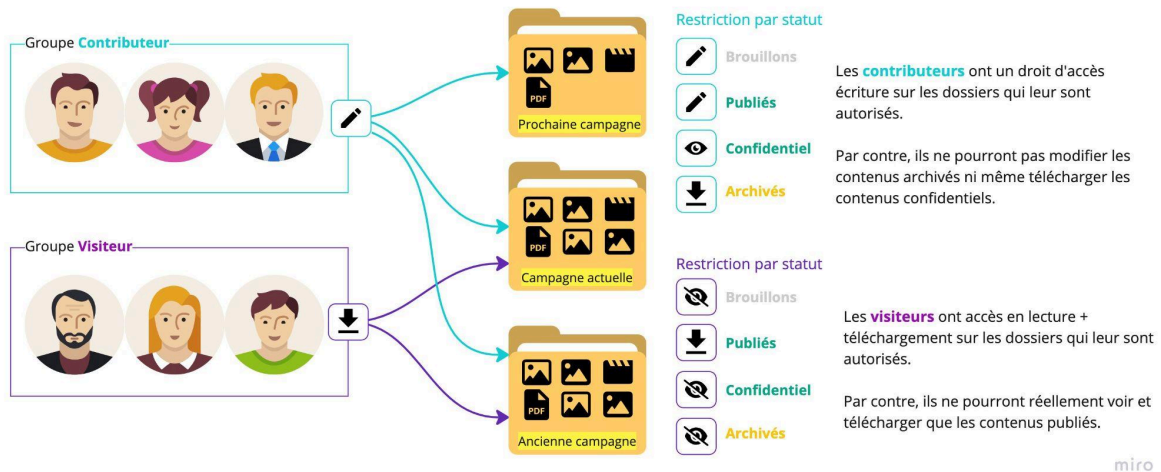
## Gestion par "cycle de vie" : utiliser les statuts

Dans cette orientation, finalement, peu importe où les éléments se trouvent, ce qui va primer, c'est le statut dans lequel l'élément se trouve à l'instant T.

A un média correspond un cycle de vie, il passe par une étape de production, avant d'être finalisé et rendu disponible (publié, diffusé). Puis vient le temps où son usage devient obsolète et se voit archivé.

Dans cette perspective, 3 grandes familles de statuts ont été établies dans Keepeek :

- Les statuts **brouillons**
- Les statuts **publiés**
- Les statuts **archivés**



Bien entendu, d'une organisation à une autre, se limiter à ces 3 statuts peut s'avérer limité et contraignant. D'où la liberté de créer autant de statuts que nécessaire (comme dans le schéma ci-dessus avec le statut "confidentiel"). Vous pourrez ainsi matérialiser votre cycle de vie et piloter l'accès aux assets en fonction de leur statut.

## Gestion par contenu : la diffusion sélective de l'information

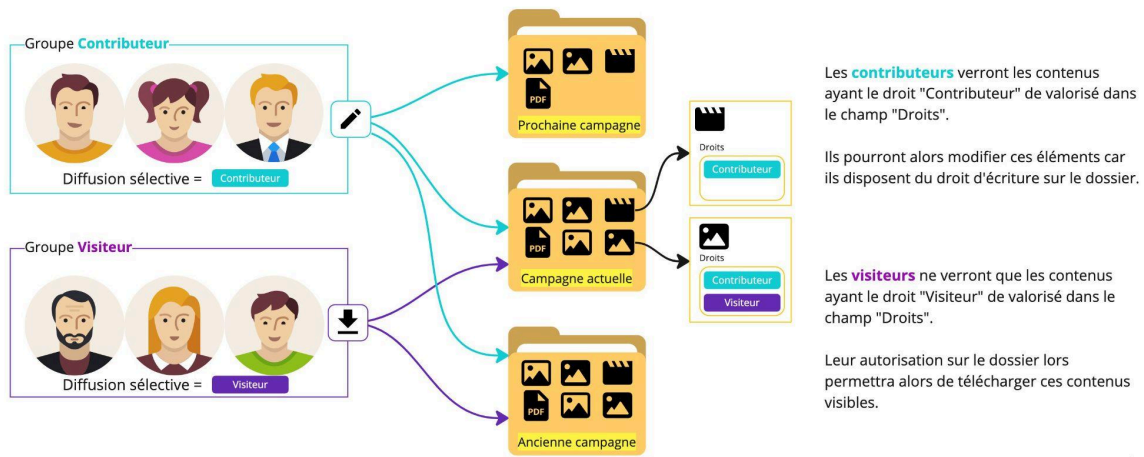
Cette troisième approche est plus technique et difficile à bien appréhender. Elle n'est d'ailleurs pas disponible par défaut. L'idée, c'est de conditionner l'accès à un élément en fonction d'informations qui lui sont attribuées.

Sur la base d'un champ de type thésaurus, vous pourrez ainsi définir à qui les médias seront accessibles selon les valeurs attribuées.

Prenons l'exemple d'un thésaurus "Accès" avec les valeurs suivantes :

- Administrateur
- Contributeur
- Visiteur

Pour le groupe visiteur, vous allez définir que la diffusion sélective ne remontera que les éléments dont le champ "Accès" a pour valeur "Visiteur". Une fois établi, cela veut dire que l'accès aux éléments ne se pilote plus dans l'administration, mais bel et bien dans la fiche de l'élément.



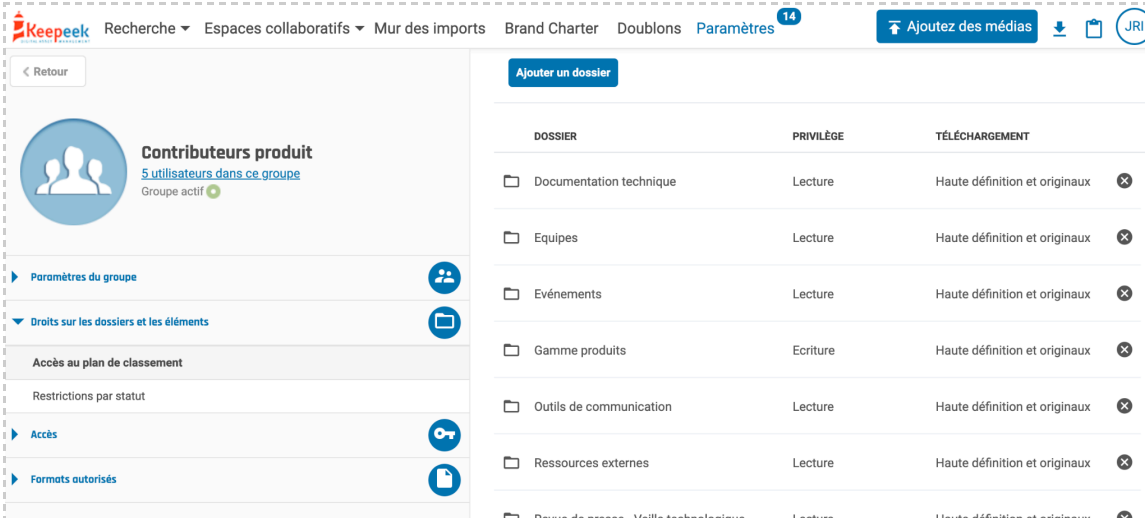
miro

Ce mode comporte certaines contraintes, il est important de bien analyser le besoin avant de décider d'aller dans cette voie.

# Droits sur le plan de classement

Historiquement, Keepeek a construit sa gestion des droits autour de son plan de classement. C'est la manière qui s'avérait la plus naturelle, notamment lorsque l'on est déjà familiarisé avec ce concept d'accès aux dossiers, que l'on connaît avec les Systèmes d'exploitation tels que Windows, MacOS, etc.

## Autoriser un dossier à un groupe



The screenshot shows the Keepeek interface for the 'Contributeurs produit' group. The 'Droits sur les dossiers et les éléments' section is expanded to 'Accès au plan de classement', displaying a table of permissions for various folders.

DOSSIER	PRIVILÈGE	TÉLÉCHARGEMENT
Documentation technique	Lecture	Haute définition et originaux
Equipes	Lecture	Haute définition et originaux
Événements	Lecture	Haute définition et originaux
Gamme produits	Ecriture	Haute définition et originaux
Outils de communication	Lecture	Haute définition et originaux
Ressources externes	Lecture	Haute définition et originaux
Revue de presse - Veille technologique	Lecture	Haute définition et originaux

Les accès aux dossiers d'un groupe sont à définir dans la section "Droit sur les dossiers et les éléments > Accès au plan de classement".

Le bouton "Ajouter un dossier" va vous permettre de sélectionner un dossier de l'arborescence et définir quel niveau de droit le groupe aura sur ce dossier.

Notez qu'un groupe visiteur ne pourra pas avoir autre chose qu'un accès en lecture. Vous pourrez simplement définir s'il aura le droit de télécharger les contenus du dossier ou non.

### Ajoutez un nouveau dossier ✕

Sélection du dossier

▼ Événements	77
Inauguration	5
Réunion	8
Présentations	28
Séminaires	28
Formations	8
▶ Outils de communication	344
▶ Recette	2
▼ Ressources externes	586
Abstrait	74
▶ Flore	100
Icône & Picto	31
Ponts	10
▶ Risques naturels	128
▶ Espace naturel	130
▶ Faune	116
▶ Revue de presse - Veille technologique	25
▼ Gamme produits	299
▶ Géothermie	44
▶ Hydroélectricité	34
▶ Divers	40

**Dossier sélectionné**

Ressources externes

**Privilège sur les dossiers \***

Lecture ▼

Choisissez les droits accordés au groupe sur ce dossier ainsi que ses sous-dossiers. Accorder un droit entraîne automatiquement l'accès aux niveaux inférieurs.

Les éléments avec statuts non publiés ne seront pas visibles sur ce dossier en mode lecture seule

**Niveau de téléchargement \***

Haute définition et originaux ▼

Choisissez le niveau de téléchargement accordé sur le dossier (et ses sous-dossiers). Accorder un niveau de téléchargement entraîne automatiquement l'accès aux niveaux inférieurs.

Annuler
Sauvegarder
Sauvegarder et fermer

Inutile d'ajouter tous les sous-dossiers, dès que vous autorisez un dossier, les sous-dossiers (et leurs sous-sous-dossiers, etc) qu'il contient seront également automatiquement autorisés avec le même niveau de droit. Référez vous plus bas à la rubrique "Héritage du indexation dossier parent".

Le bouton "Sauvegarder" va vous permettre de réaliser plusieurs autorisations successives, sans devoir fermer et rouvrir cette fenêtre.

Le bouton "Sauvegarder et fermer" appliquera l'autorisation et fermera la fenêtre.

Vous pourrez alors vérifier les autorisations dans la liste.

## Niveaux de droits sur un dossier

Pour chaque dossier autorisé, vous devrez définir le niveau de droit associé :

- **Lecture** : donne le droit d'accéder au média et à sa fiche d'information
  - **+ Téléchargement basse définition** : autorise l'utilisateur à télécharger l'élément dans des formats basse définition
  - **+ Téléchargement haute définition** : octroie les formats haute définition, et l'accès au fichier original (tous les niveaux supérieurs induisent le droit haute définition)

12

- **Ecriture** : donne le droit de modifier les éléments contenus dans le dossier (modifier la fiche d'information ou modifier le fichier original)
- **Publication** : donne le droit de basculer un élément au statut publié afin qu'il soit diffusé (sur le portail par exemple)
- **Suppression** : autorise l'utilisateur à supprimer les éléments contenus dans le dossier
- **Gestion des dossiers** : autorise l'utilisateur modifier ou supprimer le dossier, mais surtout à y créer des sous-dossiers

## Héritage du dossier parent

Il n'est pas nécessaire de devoir re-préciser le droit sur chaque dossier du plan de classement. En l'absence de droit sur le dossier, ce sont les droits du dossier parent qui s'appliqueront (et si pour celui-ci, aucun droit n'a été spécifié, alors ce sont les droits du dossier supérieur qui s'appliqueront, de façon récursive, jusqu'à remonter à un dossier de premier niveau).

Note : par contre, vous ne pouvez pas rendre invisible un sous-dossier à un groupe utilisateur si celui-ci possède un droit sur un dossier parent. Si ce devait être une contrainte forte, il vous faudra probablement revoir la structure de votre plan de classement.

## Structuration du plan de classement

Pour une bonne organisation des assets et de leurs accès, il est important d'avoir un plan de classement bien structuré. Il est recommandé de faire appel aux services de nos documentalistes Keepeek pour effectuer des choix éclairés.

Une mauvaise structuration peut conduire à complexifier les droits inutilement.

## Élévation de droits impossible

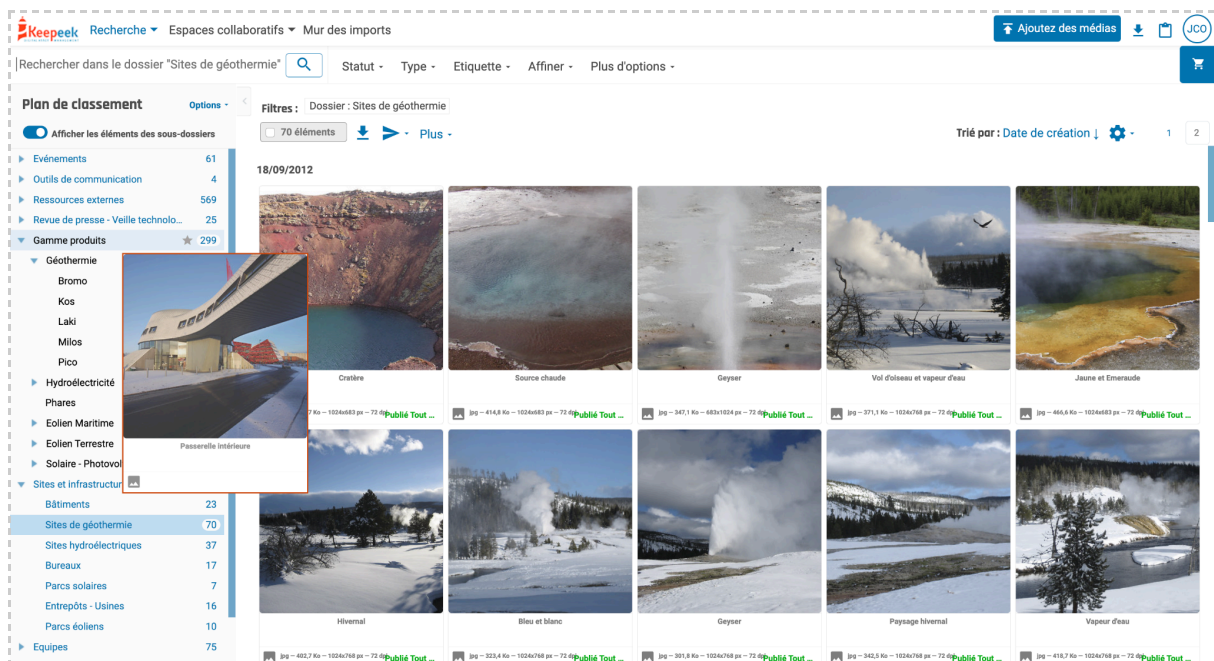
Dans Keepeek, un asset peut être placé dans plusieurs dossiers à la fois sans toutefois être dupliqué. Si sa présence dans différentes catégories est pertinente, il est appréciable qu'elle ne génère pas inutilement de doublons (potentiellement désynchronisés) et ne consomme pas d'espace disque inutile.

Un contributeur peut placer un média d'un dossier vers un autre, mais à une condition ! Qu'il ne possède pas de droits supérieurs sur le dossier de destination qu'il n'en a sur le dossier source.

Pourquoi ? Parce que cela constituerait une faille de sécurité.

Si je pouvais déplacer un média sur lequel je n'ai que le droit de téléchargement vers un dossier offrant le droit d'édition, je me serais alors octroyé tout seul des droits qu'on ne m'a pas transmis.

Cette contrainte est donc incontournable.



Ci-dessus, on constate que le déplacement par Drag & Drop d'un asset en lecture n'est pas autorisé (encadré rouge) vers un dossier sur lequel on possède le droit d'écriture.

# Droits par les statuts

## 3 familles de statuts

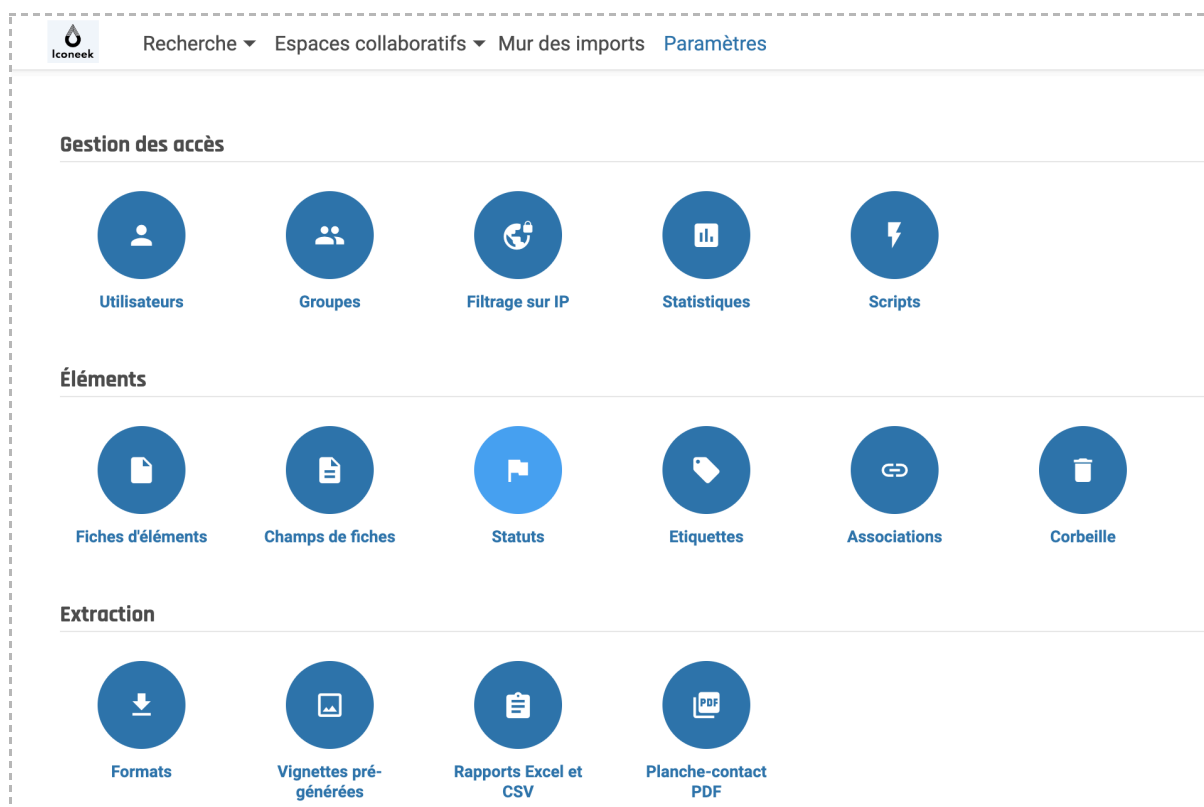
Il existe trois types de statuts dans Keepeek, définissant l'étape du cycle de vie dans lequel se trouve un élément :

- **Brouillon** : l'élément est encore en cours de construction, d'indexation ou attend une validation
- **Publié** : l'élément est prêt, disponible au plus grand nombre
- **Archivé** : l'élément est désormais obsolète, il ne doit plus être utilisé

Un élément Keepeek est toujours dans un seul et unique statut à la fois.

## Créer, modifier ou supprimer un statut

La gestion des statuts de l'application possède un menu d'administration dédié.



Vous y retrouvez l'ensemble des statuts paramétrés, classés selon les 3 familles :

NOM	DESCRIPTION	PUBLIC
<i>Brouillon</i>	Un élément non publié ne peut être vu par les utilisateurs en lecture seule.	non
<i>Brouillon</i>	Un média non publié ne peut être vu par les utilisateurs en lecture seule.	oui
<i>Publié</i>	Un élément publié est accessible à tous les utilisateurs pouvant consulter son	non
<i>Soumis à autoris...</i>		oui
<i>Publié</i>	Un média publié est accessible à tous les utilisateurs pouvant consulter son dr	oui
<i>Archivé</i>	Un élément archivé ne peut plus être vu par les utilisateurs en lecture seule.	non
<i>Archivé</i>	Un média archivé ne peut plus être vu par les utilisateurs en lecture seule.	non

En bout de ligne, une icône crayon permet d'éditer chacun de ces statuts. En haut de l'écran, un bouton vous permet de créer un nouveau statut.

Les caractéristiques d'un statut sont les suivantes :

- Nom
- Famille (brouillon, publié, archive)
- Description (visible par les contributeurs lors d'un changement de statut)
- Affichage public (voir ci-après)
- Couleurs de texte et de fond

Il est en effet possible d'appliquer une coloration distincte à un statut pour le rendre identifiable visuellement. Mais ce rendu visuel n'a aucun effet sur les caractéristiques de la famille.

**Statut** ▾ Type

- Brouillon*
- Soumis à autorisation**
- Publié**
- Archivé**

**Choisissez le statut pour ces 7 éléments** ×

Cette opération s'appliquera aux 7 résultats de votre recherche. Si le changement de statut que vous demandez ne peut pas s'appliquer à certains éléments, vous en serez informés à la fin de l'opération.

- Brouillon**  
Un média non publié ne peut être vu par les utilisateurs en lecture seule.
- Soumis à autorisation**  
Statut restreint à pour des contenus confidentiels.
- Publié**  
Un média publié est accessible à tous les utilisateurs pouvant consulter son dossier.
- Archivé**

Annuler

Note : A la création du statut, la mention "**Autoriser ce statut à tous les groupes**" vous permet d'initialiser la restriction d'accès à ce statut (voir plus bas) pour l'ensemble des groupes.

### Créez un nouveau statut ×

**Nom \***

**Statut \***

Brouillon ▼  
Brouillon  
Publié  
Archivé

**Texte**

**Fond**

**Affichage public**  
Si cette case est cochée, les éléments ayant ce statut seront affichés dans les différents partages publics.

**Autoriser ce statut à tous les groupes**  
Tous les groupes gestionnaires et contributeurs pourront accéder aux éléments dans ce statut. Vous pourrez appliquer des restrictions sur ce statut unitairement dans le paramétrage de chaque groupe.

Par défaut, il n'y a pas de restriction particulière sur un statut, il faut aller explicitement décocher ce statut groupe par groupe, pour le restreindre. **Décocher l'option à la création permet de restreindre à "invisible" le statut.** Utile si vous créez un statut confidentiel qui ne sera visible que par peu de personnes. Il vous suffit de lever la restriction pour ce ou ces quelques groupes.

Pour supprimer un statut, cliquez sur l'icône de suppression en bout de ligne.  
Note : vous ne pouvez supprimer que les statuts additionnels qui ont été créés.

Ceux de base (un par famille) sont modifiables mais non supprimables.

## Les dossiers en lecture n'affichent que les éléments publiés

**Une règle implicite** qu'il est important de connaître, c'est qu'un dossier **autorisé en lecture** n'exposera pas les contenus de types **Brouillon** et **Archivé**. C'est l'une des seules spécificités liées aux familles de statut.

De cette manière, vous vous assurez que les visiteurs n'accèdent qu'à des contenus finalisés et viables: les statuts de type **Publié**. Et ce, sans être obligé de placer dans d'autres dossiers les contenus en cours de construction ou en fin de vie. Pas de risque d'erreur.

## Appliquer des restrictions selon les statuts à un groupe utilisateur

Sur un groupe utilisateur, on peut restreindre ses droits sur les assets en fonction du statut dans lequel ils se trouvent. Cette mécanique permet de coller au plus proche du cycle de vie de vos assets, quel que soit le dossier dans lequel il se trouve.

Recherche ▾ Espaces collaboratifs ▾ Mur des imports Paramètres

Ajoutez des médias ↓ 📁 JRI

< Retour

**Contributeurs produit**  
9 utilisateurs dans ce groupe  
Groupe actif

Paramètres du groupe

Droits sur les dossiers et les éléments

Accès au plan de classement

Restrictions par statut

Accès

Formats autorisés

Activer les restrictions par statut

Les restrictions par statut définies actuellement limitent les droits sur les éléments dans le(s) dossier(s) : Image de marque, Nos Campagnes Marketing, Produits Iconeek  
- permettant seulement la lecture pour ceux avec statut(s) : Soumis à autorisation, Archivé

STATUT	LECTURE	TÉLÉCHARGEMENT BD	TÉLÉCHARGEMENT HD	ECRITURE ET +
Brouillon	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Soumis à autorisation	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Publié	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Archivé	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pour chacun de vos statuts, vous aurez en effet la possibilité de réduire le droit maximum du groupe. Il faut d'abord explicitement "activer" la restriction par statut sur le groupe avec le switch en haut de l'écran.

Les restrictions possibles sont :

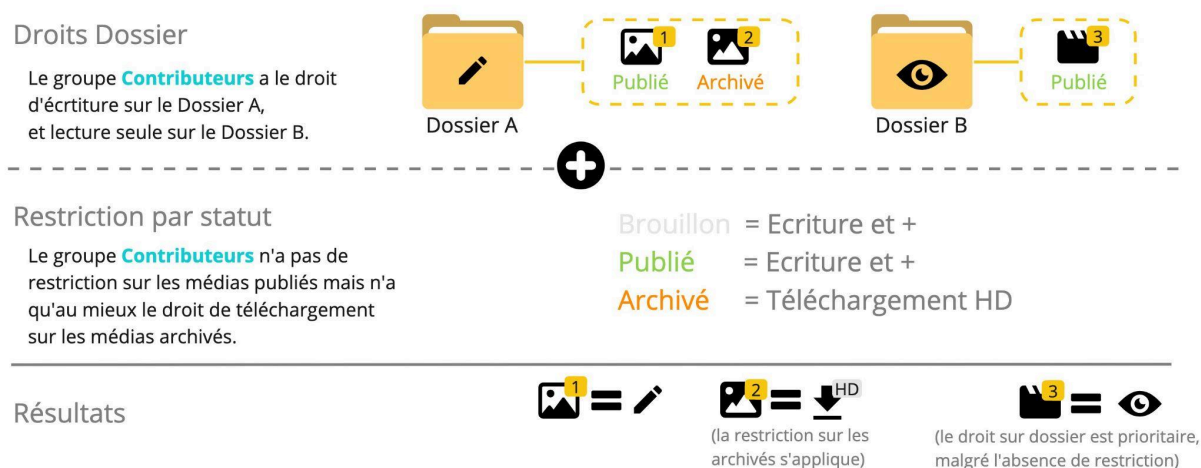
- Ecriture et + (pas de restriction)
- Téléchargement Haute définition

- Téléchargement Basse définition
- Lecture seule
- Invisible (si tout est décoché)

Un message **orange** vous rappelle les dossiers avec un droit supérieur pour lesquels les restrictions définies s'appliqueront.

Important : il faut bien interpréter cette mécanique comme une réduction des droits autorisés via les dossiers.

Exemple :



## Publication et champs obligatoires

Comme vu précédemment, le droit de publication est un niveau de droit à part entière à donner sur un dossier à un groupe utilisateur.

Mais pour pouvoir publier - c'est-à-dire passer un élément dans un statut publié - il ne suffit pas d'avoir ce droit sur l'élément.

Il faut en plus que **tous les champs obligatoires soient remplis**. Sans quoi, les statuts de type **Publié** ne sont pas proposés.

### Des règles ajustables en cas de plateforme multilingue

Les champs obligatoires ne sont peut-être à renseigner que dans une langue précise, et pas obligatoire dans les autres.

Exemple : prenons une plateforme proposant le FR (français), l'EN (anglais) et l'IT (italien) en langues de données. Vous pouvez définir que seules le FR et l'EN soient à remplir avant publication. L'italien sera alors optionnel et n'empêchera pas la publication.

Une autre possibilité, plus rare, consiste à imposer à un contributeur de saisir les champs obligatoires dans sa langue de donnée principale. S'il a l'EN en langue de données, il devra renseigner les champs obligatoires en EN mais pas dans les autres langues, et réciproquement pour un contributeur en FR. Utile lorsque des entités travaillent dans des langues différentes, ou que des contenus à destinations de différentes zones géographiques.

**TECH**, utilisez la propriété technique `LOCALE_LIST_FOR_MANDATORY_FIELDS` pour ajuster ce paramètre.

## Qu'est-ce qu'un statut "public" ?

**ATTENTION**, à ne pas confondre avec publié, la notion de statut public intervient dans la diffusion de vos assets dans les partages publics.

Vous et vos utilisateurs pouvez en effet diffuser du contenu publiquement, c'est-à-dire les rendre accessibles à des populations ne disposant pas d'un compte utilisateur dans Keepeek.

Définir qu'un statut est public ou ne l'est pas permet de garantir la période de diffusion du média, selon le cycle de vie de l'élément. Si un média a été partagé publiquement, le jour où il sera archivé (et que le statut Archivé correspondant n'est pas public), alors le partage cessera automatiquement de fonctionner.

### Editez le statut ×

**Nom (FR) \***

**Nom (EN) \***

**Description (FR)**

**Description (EN)**

**Texte**

**Fond**

**Affichage public**

Si cette case est cochée, les éléments ayant ce statut seront affichés dans les différents partages publics.

## Automatiser les changements de statut

Matérialiser le cycle de vie de ses assets par des statuts, c'est bien. Mais s'il faut soit même changer à la main les statuts des médias, ça peut s'avérer vite laborieux et source d'erreur.

Il existe une mécanique d'expiration de médias qui, sur la base d'un rôle d'un champ de type date, permet d'assurer qu'un média sera automatiquement archivé lorsque la date sera atteinte (date de fin de droit, par exemple).

Pour aller encore plus loin, il est possible de définir des règles métiers via la recherche avancée, permettant de basculer quotidiennement les médias d'un statut à un autre sous certaines conditions. Pour en savoir plus, consultez la [documentation sur les tâches planifiées de la recherche avancée](#).

## Diffusion sélective de l'information (ABAC)

Attention, cette mécanique de droit est d'un niveau plus expert et s'active uniquement sur demande avec un accompagnement de Keepeek dans sa mise en œuvre. TECH, paramétrer la propriété technique ABAC\_ACTIVATED.

### Principe

En plus des droits sur dossier et la restriction sur statut, il existe un 3ème mode permettant de piloter les droits d'accès aux éléments.

Il s'agit cette fois de conditionner la visibilité d'un accès en fonction d'une valeur de la fiche du média.

Prenons l'exemple d'un thésaurus "Accès" avec les valeurs suivantes :

- Administrateur
- Contributeur
- Visiteur

Pour le groupe visiteur, vous allez définir que la diffusion sélective ne remontera que les éléments dont le champ "Accès" a pour valeur "Visiteur". Une fois établi, cela veut dire que l'accès aux éléments ne se pilote plus dans l'administration, mais bel et bien dans la fiche de l'élément.

Note : il reste nécessaire d'attribuer les droits sur les dossiers adéquats. Quel que soit le mode, les autorisations sur dossier restent incontournables.

### Paramétrer la diffusion sélective

Au préalable, il vous faut créer le champ thésaurus qui servira d'attribution de droits, avec les valeurs distinctes qui vous intéressent.

Keeppeek Recherche ▾ Espaces collaboratifs ▾ Mur des imports Brand Charter Doublons Paramètres <sup>14</sup>

< Retour

**Droit d'accès**  
 Identifiant du champ : 87  
 Nom interne : access  
 Type de champ : Thésaurus

**Description**  
 Accéder à la description du champ de fiche, le renommer ou changer son rôle.

**Termes du thésaurus**  
 Construire le contenu du thésaurus.

Rechercher un terme

▾ **Droit d'accès** 0

Administrateur	0
Contributeur	0
Designer	0
Intranet	0
Materiel marketing	0
Visiteur	0

Astuce : vous pouvez le paramétrer pour qu'il ne soit [pas visible/modifiable par les profils non administrateur](#).

Ensuite, sur un groupe donné, attribuer la ou les valeurs adéquates du thésaurus.

Keeppeek Recherche ▾ Espaces collaboratifs ▾ Mur des imports Brand Charter Doublons Paramètres <sup>14</sup>

< Retour

**Visiteur**  
 13 utilisateurs dans ce groupe  
 Groupe actif

Paramètres du groupe

Droits sur les dossiers et les éléments

Accès au plan de classement

Restrictions par statut

Diffusion sélective de l'information

Accès

Formats autorisés

Ajouter un critère ▾

**Droit d'accès**

Visiteur

Seuls les éléments dont le champ "Droit d'accès" comporte au moins l'un des termes ci-dessus seront visibles par les utilisateurs du groupe.

Sur l'exemple ci-dessus, je définis que le groupe "Visiteur" ne verra que des éléments qui ont pour valeur "Visiteur" dans le champ "Droit d'accès".

## Précautions d'usage

L'ABAC fonctionne bien pour les utilisateurs en lecture. Cela demande un bon processus rigoureux ou automatisé pour assurer que les droits soient correctement attribués aux fiches.

Par ailleurs, appliquer cette mécanique au profils contributeurs peut occasionner quelques difficultés. Notamment, si le contributeur importe un contenu, et qu'à son import, la bonne valeur n'est pas attribuée (par lui-même ou par automatisme), alors il ne verra pas le média qu'il vient d'importer, sans comprendre pourquoi. Il est donc préconisé de réserver la diffusion sélective aux profils visiteurs.

# CHAPITRE 2

## Connaître les principes fondamentaux

### Groupes, licences et fonctionnalités autorisées

Keeppeek propose un grand nombre de fonctionnalités. Elles ne s'adressent pas toutes à l'ensemble des utilisateurs. En fonction des métiers, rôles, expertises et responsabilités, vous allez pouvoir construire vos groupes pour qu'ils reflètent la structure de votre organisation.

#### 4 différents niveaux de groupe

Il existe 4 niveaux de groupes :

- Visiteur
  - Fonctionnalités de téléchargement et diffusion
  - Accès en lecture uniquement
- Contributeur
  - Fonctionnalités d'édition
  - Accès en écriture et capacité de publication
- Gestionnaire
  - Fonctionnalités d'édition
  - Certaines fonctionnalités de paramétrage déléguées
- Administrateur
  - La totalité des contenus, des fonctionnalités activées et des paramétrages
  - Accès aux espaces collaboratifs de tous les utilisateurs

Sur ces niveaux de droits repose d'ailleurs le décompte des licences Keeppeek. 3 niveaux de licence utilisateur sont proposés, en sachant que les gestionnaires et administrateurs sont regroupés dans le même niveau. Les gestionnaires sont en effet des administrateurs à qui on souhaite proposer un niveau d'accès bien délimité (souvent dans des contextes multi-marques).

En réalité, il en existe 2 supplémentaires un peu particuliers :

- Le "Guest" qui est un utilisateur "invité" à collaborer dans un espace collaboratif. Un guest n'a pas d'accès au reste du backoffice et des autres applications Keeppeek, il ne peut se rendre que dans un espace collaboratif dans lequel il a été ajouté en tant que membre.

Note : il est possible de convertir un compte guest en utilisateur.

- L'administrateur technique est un profil particulier, réservé aux collaborateurs Keepeek, qui ont un accès à certains paramètres techniques pour adapter la plateforme aux besoins du client.

Ces 2 types d'utilisateurs ne rentrent pas dans le décompte des licences.

Ci-dessous, vous trouverez l'ensemble des fonctionnalités disponibles pour chaque niveau de groupe.

En vert = fonctionnalité disponible à partir de ce niveau de groupe

En gris = fonctionnalité déjà disponible pour le niveau de groupe inférieur

Attention, cette liste de fonctionnalités comprend des modules auxquels vous n'avez pas forcément souscrit, et qui n'apparaîtront pas dans l'application quel que soit le profil utilisateur.

## Fonctionnalités sur les assets

Visiteur	Contributeur	Gestionnaire	Administrateur
Visualiser un élément image, document, vidéo ou son	Visualiser un élément image, document, vidéo ou son	Visualiser un élément image, document, vidéo ou son	Visualiser un élément image, document, vidéo ou son
Télécharger un élément	Télécharger un élément	Télécharger un élément	Télécharger un élément
Export excel/csv	Export excel/csv	Export excel/csv	Export excel/csv
Planches-contact PDF	Planches-contact PDF	Planches-contact PDF	Planches-contact PDF
Demande de téléchargement	Demande de téléchargement	Demande de téléchargement	Demande de téléchargement
Téléchargement de pièces jointes *	Téléchargement de pièces jointes *	Téléchargement de pièces jointes *	Téléchargement de pièces jointes *
Désarchivage de pièces jointes *	Désarchivage de pièces jointes *	Désarchivage de pièces jointes *	Désarchivage de pièces jointes *
Exporter vers Google Drive	Exporter vers Google Drive	Exporter vers Google Drive	Exporter vers Google Drive
	Upload, modification, suppression de pièces jointes *	Upload, modification, suppression de pièces jointes *	Upload, modification, suppression de pièces jointes *
	Détection manuelle de mots-clés via l'IA *	Détection manuelle de mots-clés via l'IA *	Détection manuelle de mots-clés via l'IA *
	Demande de classement	Demande de classement	Demande de classement
	Edition de la fiche	Edition de la fiche	Edition de la fiche
	Changer de statut	Changer de statut	Changer de statut
	Géolocaliser un élément	Géolocaliser un élément	Géolocaliser un élément
	Traitement par lot	Traitement par lot	Traitement par lot
	Associer des éléments	Associer des éléments	Associer des éléments

	Attribution d'étiquette Remplacer un fichier Supprimer une version Supprimer un élément Extraire une image/séquence d'une vidéo Indexation via fichier excel Créer, modifier, supprimer un dossier Dupliquer une arborescence Importer des éléments riches (liens RMM) Importer depuis Google Drive Publier une vidéo sur YouTube * Accéder aux statistiques d'un élément	Attribution d'étiquette Remplacer un fichier Supprimer une version Supprimer un élément Extraire une image/séquence d'une vidéo Indexation via fichier excel Créer, modifier, supprimer un dossier Dupliquer une arborescence <b>avec les médias contenus</b> Importer des éléments riches (liens RMM) Importer depuis Google Drive Publier une vidéo sur YouTube * Accéder aux statistiques d'un élément	Attribution d'étiquette Remplacer un fichier Supprimer une version Supprimer un élément Extraire une image/séquence d'une vidéo Indexation via fichier excel Créer, modifier, supprimer un dossier Dupliquer une arborescence <b>avec les médias contenus</b> <b>Créer un dossier de 1er niveau</b> Importer des éléments riches (liens RMM) Importer depuis Google Drive Publier une vidéo sur YouTube * Accéder aux statistiques d'un élément
--	--	--	---

## Fonctionnalités de diffusion

Visiteur	Contributeur	Gestionnaire	Administrateur
Partage public unitaire Liens vers les vignettes Création de vignette personnalisée Envoi par email Envoi par FTP Notification sur sélection Crop sur point d'intérêt * Partage grand public *	Partage public unitaire Liens vers les vignettes Création de vignette personnalisée Envoi par email Envoi par FTP Notification sur sélection Crop sur point d'intérêt * Partage grand public *	Partage public unitaire Liens vers les vignettes Création de vignette personnalisée Envoi par email Envoi par FTP Notification sur sélection Crop sur point d'intérêt * Partage grand public *	Partage public unitaire Liens vers les vignettes Création de vignette personnalisée Envoi par email Envoi par FTP Notification sur sélection Crop sur point d'intérêt * Partage grand public *

## Fonctionnalités de recherche

Visiteur	Contributeur	Gestionnaire	Administrateur
Recherche texte	Recherche texte	Recherche texte	Recherche texte

Plan de classement Recherche avancée Navigation personnalisée Personnes * Geolocalisation *	Plan de classement Recherche avancée Navigation personnalisée Personnes * Geolocalisation *	Plan de classement Recherche avancée Navigation personnalisée Personnes * Geolocalisation *	Plan de classement Recherche avancée Navigation personnalisée Personnes * Geolocalisation *
---	---	---	---

## Fonctionnalités collaboratives

Visiteur	Contributeur	Gestionnaire	Administrateur
Créer un panier Contribuer en tant qu'invité dans un panier, workflow ou tableau Commentaires, annotations sur image, sur document, étiquettes collaboratives Notifications par email	Créer un panier, workflow ou tableau Contribuer en tant qu'invité dans un panier, workflow ou tableau Commentaires, annotations sur image, sur document, étiquettes collaboratives Notifications par email Inviter des collaborateurs dans un panier, workflow ou tableau	Créer un panier, workflow ou tableau Contribuer en tant qu'invité dans un panier, workflow ou tableau Commentaires, annotations sur image, sur document, étiquettes collaboratives Notifications par email Inviter des collaborateurs dans un panier, workflow ou tableau Inviter des collaborateurs dans un panier, workflow ou tableau	Créer un panier, workflow ou tableau Contribuer en tant qu'invité dans un panier, workflow ou tableau Commentaires, annotations sur image, sur document, étiquettes collaboratives Notifications par email Inviter des collaborateurs dans un panier, workflow ou tableau Inviter des collaborateurs dans un panier, workflow ou tableau Accéder à tous les paniers Accéder à tous les workflows Accéder à tous les tableaux

## Fonctionnalités d'administration

Visiteur	Contributeur	Gestionnaire	Administrateur
		Administration Statistiques Création de fiche	Administration Statistiques Création de fiche

		Création de champs Création de sous-groupe Création d'utilisateur Formats de planches-contact Faceting et paramètres de recherche Formats de téléchargement Paramétrer les autorisations d'un sous-groupe (dans la limite de ses propres droits)	Création de champs Création de sous-groupe Création d'utilisateur Formats de planches-contact Faceting et paramètres de recherche Formats de téléchargement Paramétrer les autorisations d'un groupe Étiquettes Statuts Types d'associations Détection automatique de mots-clés *
--	--	---	---

## Fonctionnalités du portail utilisateur

Visiteur	Contributeur	Gestionnaire	Administrateur
Recherche Téléchargement Téléchargement de pièces jointes * Partage public unitaire Partage public de panier Planches-contact Formulaire de contribution	Recherche Téléchargement Téléchargement de pièces jointes * Partage public unitaire Partage public de panier Planches-contact Formulaire de contribution Module d'import *	Recherche Téléchargement Téléchargement de pièces jointes * Partage public unitaire Partage public de panier Planches-contact Formulaire de contribution Module d'import * Paramétrage de l'ancien portail	Recherche Téléchargement Téléchargement de pièces jointes * Partage public unitaire Partage public de panier Planches-contact Formulaire de contribution Module d'import * Paramétrage de l'ancien portail Paramétrage du nouveau portail (Front Edit)


## Paramétrage des fonctionnalités autorisées au groupe

Ces tableaux ci-dessus vous ont listé les différentes fonctionnalités possibles par niveau de groupe. Elles ne sont cependant pas toutes systématiquement disponibles aux utilisateurs.

Une partie d'entre elles doivent être autorisées explicitement à vos groupes utilisateurs. Cela vous permet d'ajuster plus finement les fonctionnalités disponibles à vos utilisateurs.

Keeppeek Recherche ▾ Espaces collaboratifs ▾ Mur des imports Brand Charter Doublons Paramètres <sup>14</sup> [Ajoutez des médias](#)

[Retour](#)







**BrouillonLecture - ABAC v1 - filtrage par statut**

[0 utilisateurs dans ce groupe](#)

Groupe actif ●

Créé par Anonyme Anonyme le 27/11/2017

- [Paramètres du groupe](#) 
- [Droits sur les dossiers et les éléments](#) 
- [Accès](#) 
- Applications
- Fonctionnalités**
- Chaînes YouTube
- [Formats autorisés](#) 

**Fonctionnalités d'import et d'édition**

Imports de fichiers par le navigateur  
Ce module permet aux utilisateurs d'importer de nouveaux fichiers à travers leur navigateur web.

Autoriser les opérations sur de gros volumes  
Les utilisateurs de ce groupe pourront réaliser des opérations de changement de statut ou de traitement par lot sur plusieurs milliers d'éléments à la fois.

Indexation par fichier Excel  
Cette fonctionnalité permet d'indexer les éléments d'un panier avec les données provenant d'un fichier Excel

Détection automatique de mots-clés par intelligence artificielle  
Cette fonctionnalité permet de définir automatiquement des mots-clés sur des éléments grâce à de l'intelligence artificielle

**Fonctionnalités collaboratives**

Commentaires depuis le plan de classement  
Donner l'accès à l'onglet "Commentaires" dans le détail de l'élément pour que les utilisateurs de ce groupe puissent commenter depuis le plan de classement.

Partage collaboratif  
Cette fonctionnalité permet de partager une sélection d'éléments avec d'autres utilisateurs via les paniers.

Partage public  
Cette fonctionnalité permet de partager un élément depuis son détail ou une sélection d'éléments depuis un panier avec toute personne externe.

Création de workflows

[Sauvegarder](#)

Dans la section "Accès > Fonctionnalités", en fonction du niveau de groupe (visiteur, contributeur, gestionnaire), certains droits peuvent être ajustés.

Vous pourrez par exemple définir si le groupe utilisateur permet l'activation du partage collaboratif ou public d'un panier, s'il permet de créer des workflows, importer des fichiers dans la plateforme, etc.

## Formats d'exports et niveaux de téléchargement

Les formats d'exports sont évidemment un élément central d'une solution de Digital Asset Management. Ils offrent la capacité aux utilisateurs à télécharger les contenus de leur choix dans la déclinaison adaptée à leur besoin.

Qu'il s'agisse de format, de dimensions, de définition, les formats offrent une palette de paramétrage très poussée, notamment pour les images.

### Notion de haute et basse définition

En conséquence, d'un format à l'autre, le niveau de définition peut varier.

Bien que moins utilisée de nos jours, il est parfois souhaité de ne pas exposer les fichiers originaux à des utilisateurs mais tout en leur laissant un accès à un format de faible qualité.

Comme présenté dans le paramétrage des [droits sur le plan de classement](#), lorsque vous donnez à un utilisateur l'accès en lecture, vous pouvez finement définir les capacités de téléchargement :

- Pas de téléchargement
- Basse définition
- Haute définition

Et côté paramétrage des formats d'export, il est possible de déclarer si le format est un format basse ou haute définition.

The screenshot shows the 'Son original' format configuration page in Keepeek. The interface is divided into two main sections: a left sidebar with descriptive information and a main right area for editing details.

**Left Sidebar:**

- Header:** 'Son original' with 'Identifiant du format : 10' and 'Fichiers sons'.
- Description:** 'Changer les informations générales du format.'
- Titre du fichier de sortie:** 'Changer le titre du fichier généré.'
- Format:** 'Format de sortie du son. Fichier original ou version pré-générée.'
- Gestion des métadonnées:** 'Changer les métadonnées qui seront écrites dans le fichier de sortie.'

**Main Editing Area:**

- Nom du format (FR) \*:** Input field containing 'Son original'.
- Nom du format (EN) \*:** Input field containing 'Original sound'.
- Description du format (FR):** Empty text area.
- Description du format (EN):** Empty text area.
- Niveau de téléchargement autorisé \*:** A dropdown menu with three options:
  - Haute définition et originaux (selected)
  - Basse définition
  - Haute définition et originaux
 A note below the dropdown states: 'quels utilisateurs auront accès au format en fonction des droits'

La conséquence, c'est que lorsqu'on télécharge un média, les formats personnalisés proposés vont varier selon que l'on possède le droit haute définition ou basse définition sur le média.

En ayant le droit basse définition, je n'aurais qu'une liste limitée aux formats basse définition, alors qu'en haute définition, il me sera proposé l'exhaustivité des formats autorisés.

Le principe existe aussi pour les vignettes pré-générées qu'il est possible de proposer en téléchargement express. Dans le menu "Vignettes pré-générées", si vous éditer un format de vignette, vous pourrez en effet préciser s'il sera proposé en téléchargement express pour les différents type de fichiers (image, vidéo...) et à partir de quel niveau de téléchargement.



Notez que vous pouvez identifier à quel type de fichier chaque format est destiné (image, vidéo, etc).

Vous pouvez ainsi décocher les formats à ne pas proposer à un groupe.

Comme expliqué précédemment, si vous ne donnez qu'un droit en "basse définition" sur l'ensemble des dossiers du groupe, il aura beau avoir ici des formats haute définition de cochés, ils ne lui seront pas proposés.

## Modes de téléchargement

Dans le backoffice, mais aussi dans d'autres produits Keepeek, vous retrouverez 3 modes de téléchargement :

- **Le téléchargement express** : présente les fichiers originaux et pré-générés qui sont accessibles en téléchargement direct
- **Les formats personnalisés** : présentent les formats d'exports présentés précédemment, qui vont opérer une transformation sur le fichier
- **La demande de téléchargement** : en cas d'absence de droit de téléchargement total ou partiel (droit BD uniquement), l'utilisateur peut formuler une demande de téléchargement pour qu'un responsable valide et transmettre les contenus au bon format

En fonction des droits dont dispose un utilisateur sur sa sélection de médias, il lui sera proposé différentes options.

	Droit HD	Droit BD	Pas de téléchargement
Téléchargement express	✓	✓	✗
Formats personnalisés	✓	✓	✗
Demande de téléchargement	✗	✓	✓

Notez que sur une sélection hétérogène d'éléments, c'est le droit le plus bas qui prévaudra.

Si sur ses 12 médias, un utilisateur a un droit HD sur 11 d'entre eux, et un droit BD sur le 12ème, c'est le droit Basse Définition qui sera retenu.

## Le niveau de téléchargement occasionne d'autres impacts

Avoir le droit Haute Définition ou pas, sur un élément n'a pas que des conséquences sur les fonctionnalités de téléchargement.

Il en a aussi sur les fonctionnalités de diffusion. Qu'il s'agisse du partage public ou des liens vers les vignettes, les fichiers originaux ne seront proposés qu'en cas de droit HD.

Il en va de même pour le module Dynameek, le générateur de vignettes de Keepeek, qui utilise une image source haute résolution pour générer ses liens.

# Autres notions de paramétrage de droits

## Planches-contacts

Un peu à la manière des formats d'export, mais en beaucoup plus simple, vous pouvez autoriser des planches-contacts à chacune de vos populations. Particulièrement utile en multimarque, cela vous permet de ne proposer que les structures de planches-contacts adaptées (chartées et avec les informations pertinentes) aux différents contextes de vos utilisateurs.

Dans le paramétrage de chaque groupe, vous pouvez accéder à la section "Formats autorisés > Planches-contacts PDF" et cocher/décocher les planches-contacts autorisées au groupe.

The screenshot shows the Keeppeek interface for the 'Contributeurs produit' group. The group has 6 users and is active. The 'Formats autorisés' section is expanded to show 'Planches-contacts PDF'. The settings for 'Planches-contacts PDF autorisées' are as follows:

Planches-contacts PDF autorisées	
Tout sélectionner / Tout désélectionner	
NOM	
<input checked="" type="checkbox"/>	Planche-contact standard (image + titre) Planche-contact par défaut
<input checked="" type="checkbox"/>	Shooting photo
<input type="checkbox"/>	Infos produits

Si aucune planche-contact n'est cochée, alors la fonctionnalité ne sera pas proposée à ce groupe (que ce soit dans le backoffice ou le portail utilisateur).

## Fiches autorisées à la création

Pour vos contributeurs, vous avez la possibilité de limiter les fiches d'éléments qu'ils peuvent utiliser pour les médias qu'ils importent. Une nouvelle fois, cette capacité s'adresse principalement aux contextes multi-marques qui peuvent accumuler un grand nombre de fiches différentes et qui souhaitent éviter les erreurs d'import.

Keeppeak Recherche ▾ Espaces collaboratifs ▾ Mur des imports Brand Charter Doublons Paramètres

< Retour

**Contributeurs produit**  
6 utilisateurs dans ce groupe  
Groupe actif

- Paramètres du groupe
- Droits sur les dossiers et les éléments
- Accès
- Formats autorisés
  - Formats d'export
  - Fiches autorisées à la création**
  - Planches-contacts PDF

Tout sélectionner / Tout désélectionner

**Images**

Nom	
<input type="checkbox"/>	Exemple 1
<input checked="" type="checkbox"/>	Images
<input checked="" type="checkbox"/>	Photos produit
<input type="checkbox"/>	Tous les types de champ de fiches
<input type="checkbox"/>	Vega - photos d'implantation
<input type="checkbox"/>	Zephyr - photos

**Documents**

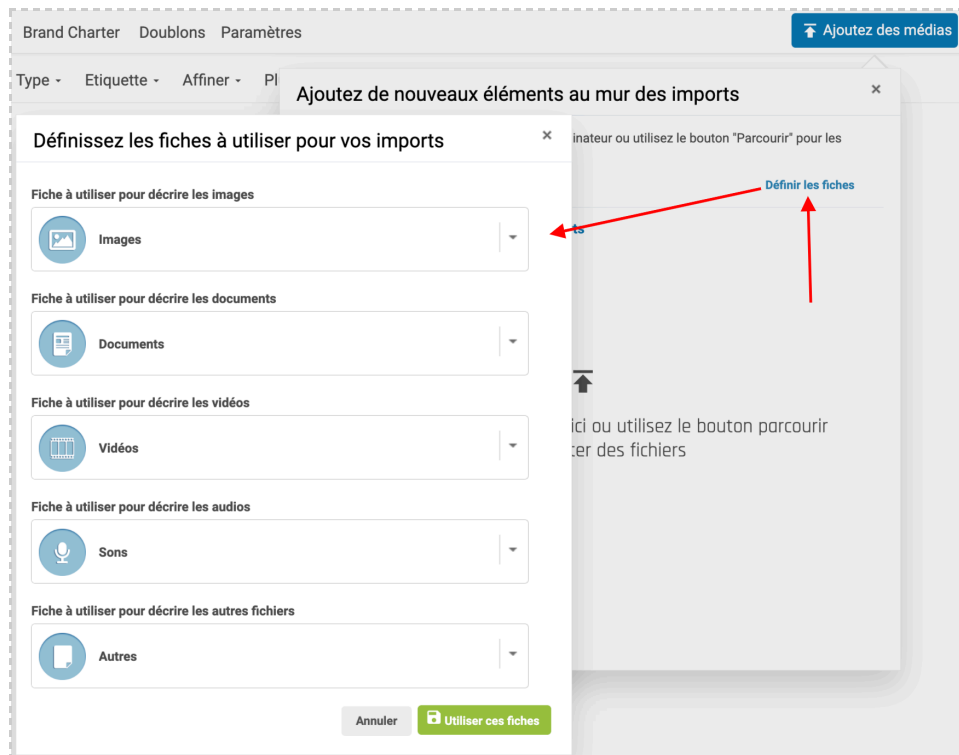
Nom	
<input checked="" type="checkbox"/>	Contrat photographe

Dans la section "Formats autorisés > Fiches autorisées à la création", vous pourrez décocher les fiches que ce groupe utilisateur ne pourra pas utiliser pour créer de nouveaux contenus.

Pour chaque type d'élément, vous pouvez donc limiter les fiches cibles. Cependant, vous êtes obligé de laisser au moins une fiche par type pour que le groupe utilisateur puisse importer tout type de fichier sans encombre.

Dès lors, dans la popup d'import, un utilisateur ne pourra définir des fiches cibles que parmi celles qui lui sont autorisées.

Note : en multi-groupe, un utilisateur accumule toutes les fiches autorisées à ses groupes.



Note : cette liste restreinte de fiches s'applique également dans les fonctionnalités suivantes

- Création d'élément vide
- Extraction de séquence vidéo
- Extraction d'image depuis une vidéo
- Changement de fiche

Important : les fiches autorisées n'affectent que la création d'éléments et non l'accès. Par exemple, ce n'est pas parce qu'un groupe ne peut pas créer d'images "Photo produit" qu'il ne peut pas en consulter, télécharger ou même éditer les informations. Keepeek ne propose pas de pilotage de droit par fiche.

## Champs visibles / modifiables par les non administrateurs

Pour chaque champ de fiche, il est possible de définir si celui-ci sera visible et éditable pour les utilisateurs qui ne sont pas administrateurs.

Recherche ▾ Espaces collaboratifs ▾ Mur des imports Brand Charter Doublons Paramètres <sup>14</sup>

**Ce champ est utilisé dans les fiches suivantes : Photos produit (Droits), Vidéos (Droits), Sons (Droits)**

rights

**Rôle du champ**  
Mentionner dans les conditions d'utilisations ▾

**Description du champ (FR)**

**Description du champ (EN)**

**Activer les optimisations du moteur de recherche**  
Ce paramètre vous permet d'augmenter les résultats des recherches de vos utilisateurs en prenant en compte les termes approchant qu'ils pourraient saisir.  
Par exemple : singulier/pluriel, masculin/féminin, infinitif/conjugué, majuscule/minuscule, avec/sans accents...

**Champ visible pour les non administrateurs**  
Si décoché alors seuls les administrateurs pourront voir le contenu de ce champ.

**Champ modifiable par les non administrateurs**  
Si décoché alors seuls les administrateurs pourront modifier le contenu de ce champ.

Supprimer le champ

Cette mécanique permet de :

- masquer des champs qui ne sont pas pertinents pour vos utilisateurs
  - champs techniques ou temporaire
  - champ utilisé pour la migration
  - zone d'annotation réservée aux admins
- empêcher les contributeurs de modifier la valeur dans l'onglet édition et le traitement par lot
  - par exemple si le champ est consolidé par un autre outil, un script de synchro...
  - ou si la référence est unique et ne doit pas être modifiée après coup

Dès lors les champs seront visibles et éditables pour les profils administrateurs comme n'importe quel autre champ de fiche. Mais ils seront grisés, voire totalement masqués à vos autres utilisateurs.

Attention, nous insistons sur le fait que ce paramétrage n'est pas un "droit" à proprement parler, mais simplement une protection dans l'interface du Backoffice. Ils n'empêchent pas l'accès et l'édition de ces champs via l'API, par exemple.

Note : dans le même esprit, il est également possible de réduire les champs qui sont exposés en partage public et dans les portails utilisateurs. Ce sont des propriétés des champs dans le paramétrage des fiches.

### Editez le champ Date de fin des droits

**Type de champ :** Date

**Nom interne :** end\_date

**Résumé**  
Ce paramètre conditionne l'affichage du champ dans le résumé de l'élément qui s'affiche à sa sélection.

**Affichage public**  
Si cette case est cochée, le champ sera consultable par les visiteurs et intégré dans le fichier information.txt du fichier ZIP créé lors des téléchargements par les utilisateurs. L'affichage dans le détail de l'élément dans le portail utilisateur est géré par un paramètre dédié (cf ci-dessous).

**Affichage sur le portail utilisateur**  
Si la case est cochée, le champ sera affiché dans le détail de l'élément (à côté de la vignette).

**Obligatoire**  
Ce paramètre conditionne le statut de l'élément en "indexé" dans la zone d'import de la médiathèque.

**Indexable**  
Si cette case est cochée, l'indexation des éléments tiendra compte des informations stockées dans ce champ. Les résultats des recherches des utilisateurs intégreront donc ces données.

**Indexable sur le portail utilisateur**  
Ce paramètre est identique au "indexable" mais il ne concerne que les recherches effectuées dans le portail utilisateur.

**Poids du champ**  
Important

## Filtrage IP

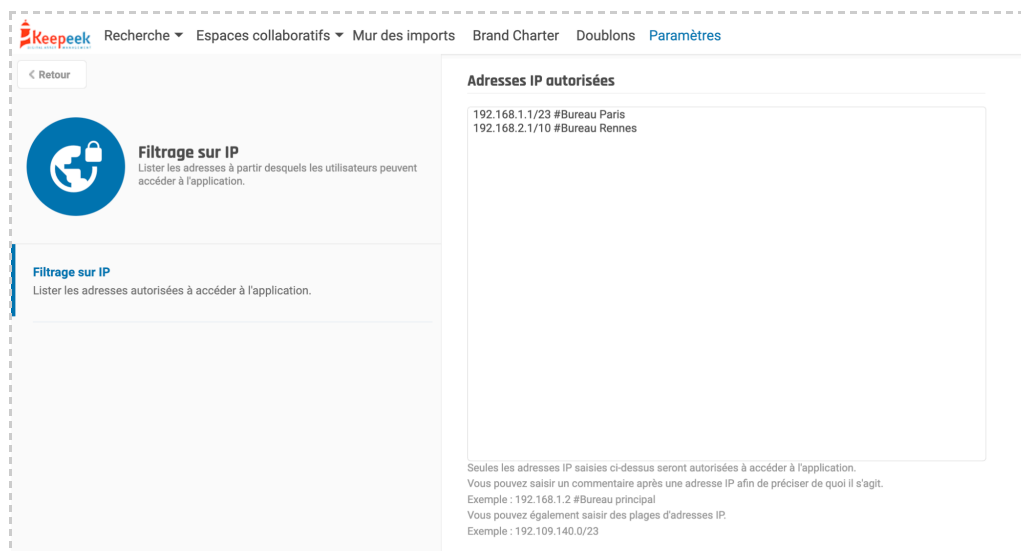
Vos contenus sont confidentiels et vous voulez réduire au maximum les risques de fuite ? Vous pouvez envisager d'utiliser le filtrage par adresse IP.

Le principe consiste à n'autoriser l'accès qu'à une liste restreinte de plages d'adresses IP. De cette manière, vos utilisateurs devront soit être connectés dans les locaux de l'entreprise ou bien à distance via un accès VPN.

Pour paramétrer le filtrage IP, il faut tout d'abord faire une demande à Keepeek pour activer le module de paramétrage. Il est désactivé par défaut car par de mauvaises manipulations, il peut bloquer l'accès à votre plateforme.

**TECH**, activer la propriété technique `IP_FILTERING_ADMIN_ENABLED`.

Dès lors, vous disposerez de l'écran de paramétrage ci-dessous.



Dans le champ texte, vous allez pouvoir déclarer les adresses IP ou plages d'IPs qui seront les seules autorisées à accéder à la plateforme.

Vous pouvez saisir un commentaire après une adresse IP afin de préciser de quoi il s'agit.

Exemple : 192.168.1.2 #Bureau principal

Vous pouvez également saisir des plages d'adresses IP.

Exemple : 192.109.140.0/23

Prenez garde, lorsque vous enregistrez, le changement est immédiatement effectif. Et si vous avez fait une erreur d'adressage ip ou que vous avez oublié d'y mettre votre adresse, vous ne pourrez plus accéder au backoffice.

### **Exception pour les partages publics et collaboratifs ?**

Par défaut, plus aucune interface du backoffice n'est alors accessible si on ne se connecte pas via une adresse IP autorisée.

Cela peut toutefois s'avérer contraignant, si vous avez besoin d'utiliser le partage public ou inviter des agences externes dans des espaces collaboratifs.

Pour cela, il vous est possible de demander un paramétrage spécifique, permettant d'autoriser les accès aux partages publics et/ou aux partages collaboratifs

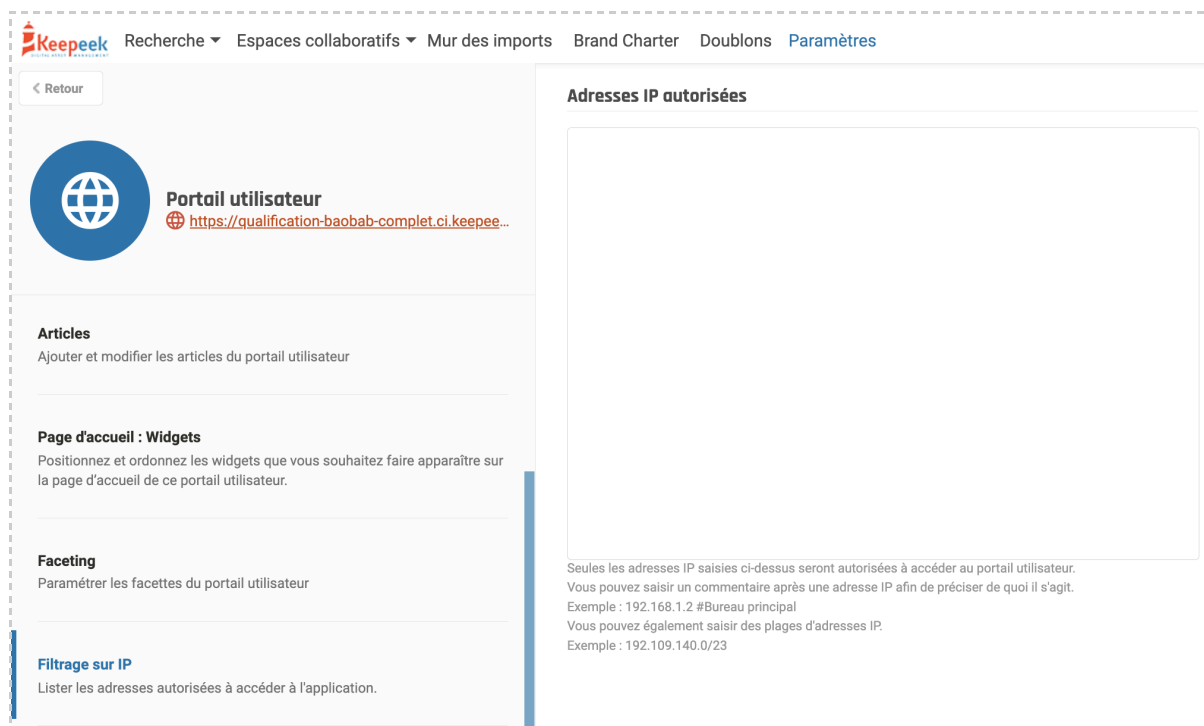
**TECH, utiliser les tech pro suivantes :**

- **FILTER\_IP\_PUBLIC\_SHARE** pour autoriser les accès sans contraintes IP aux partages publics
- **BY\_PASS\_IP\_FILTER\_ACCESSING\_COLLABORATIVE\_SPACE\_AS\_GUEST** pour les accès aux partages collaboratifs

## Filtrage IP pour les portails utilisateurs

Pour le portail utilisateur, il est également possible d'appliquer un filtrage IP. Celui-ci peut d'ailleurs être différent du backoffice si les IP à autoriser ne sont pas les mêmes.

Pour l'ancien portail, un écran similaire à celui du backoffice existe dans le paramétrage du portail depuis l'administration backoffice :



The screenshot shows the 'Adresses IP autorisées' (Authorized IP addresses) configuration page in the Keepeek administration interface. The page is divided into two main sections: a left sidebar with navigation options and a main content area for IP management.

**Navigation (top):** Recherche, Espaces collaboratifs, Mur des imports, Brand Charter, Doublons, Paramètres.

**Left Sidebar:**

- Retour** (button)
- Portail utilisateur** (header) with a globe icon and URL: <https://qualification-baobab-complet.ci.keepee...>
- Articles**: Ajouter et modifier les articles du portail utilisateur.
- Page d'accueil : Widgets**: Positionnez et ordonnez les widgets que vous souhaitez faire apparaître sur la page d'accueil de ce portail utilisateur.
- Faceting**: Paramétrer les facettes du portail utilisateur.
- Filtrage sur IP**: Lister les adresses autorisées à accéder à l'application.

**Main Content Area:**

- Adresses IP autorisées** (header)
- A large empty text area for entering IP addresses.
- Instructions:**
  - Seules les adresses IP saisies ci-dessus seront autorisées à accéder au portail utilisateur.
  - Vous pouvez saisir un commentaire après une adresse IP afin de préciser de quoi il s'agit.
  - Exemple : 192.168.1.2 #Bureau principal
  - Vous pouvez également saisir des plages d'adresses IP.
  - Exemple : 192.109.140.0/23

Pour les nouveaux portails, le paramétrage se paramètre différemment car l'infrastructure technique est différente. Il faut solliciter Keepeek pour adapter le paramétrage.

TECH, se référer à [cette documentation](#) pour en savoir plus sur le filtrage ip du nouveau portail.

## Droits dans les espaces collaboratifs

Les espaces collaboratifs (paniers, workflows et tableaux) permettent de constituer des équipes de travail pour manipuler des contenus du DAM. Des règles spécifiques de droits s'appliquent.

Pour plus d'informations sur l'utilisation de ces espaces collaboratifs, veuillez consulter la [documentation dédiée](#).

### Paniers et workflow : le droit du propriétaire prévaut

Les paniers et workflows permettent aux propriétaires (créateurs) d'inviter des collaborateurs à accéder et contribuer à leur contenu. L'objectif de ces espaces collaboratifs est de permettre le partage de droits et de rendre disponible des contenus à des utilisateurs qui ne disposent pas des droits.

La logique qui a été choisie est celle de considérer que **c'est le propriétaire qui est responsable des contenus de son espace**, et qu'il y délègue les droits aux membres qu'il invite.

Cela implique une contrainte importante : les membres contributeurs ne pourront déposer dans le paniers que des éléments autonomes ou classés dans un dossier sur lequel le propriétaire possède les droits adéquats.



Le propriétaire du panier ne possède pas les droits suffisants sur cet élément. Le droit du propriétaire doit être au moins équivalent au niveau de téléchargement qu'il a autorisé en partageant ce panier.

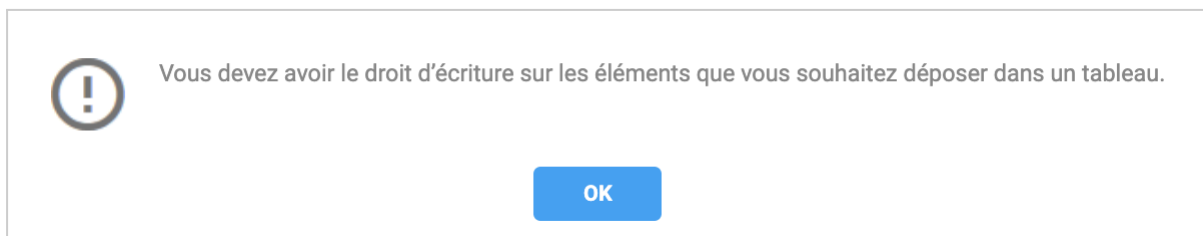
OK

Notez que dans les paniers, un membre peut être invité en lecture seule ou contribution. En cas de "lecture seule", il pourra consulter les médias, les télécharger, et pourra interagir dans le fil de discussion avec les autres membres. Il ne pourra par contre pas modifier les éléments ni importer de nouveaux éléments autonomes.

### Tableau : chaque membre est responsable de ce qu'il partage

Les tableaux adoptent une stratégie différente. Cette fonctionnalité a été développée plus récemment et nous avons souhaité mettre en place une autre approche.

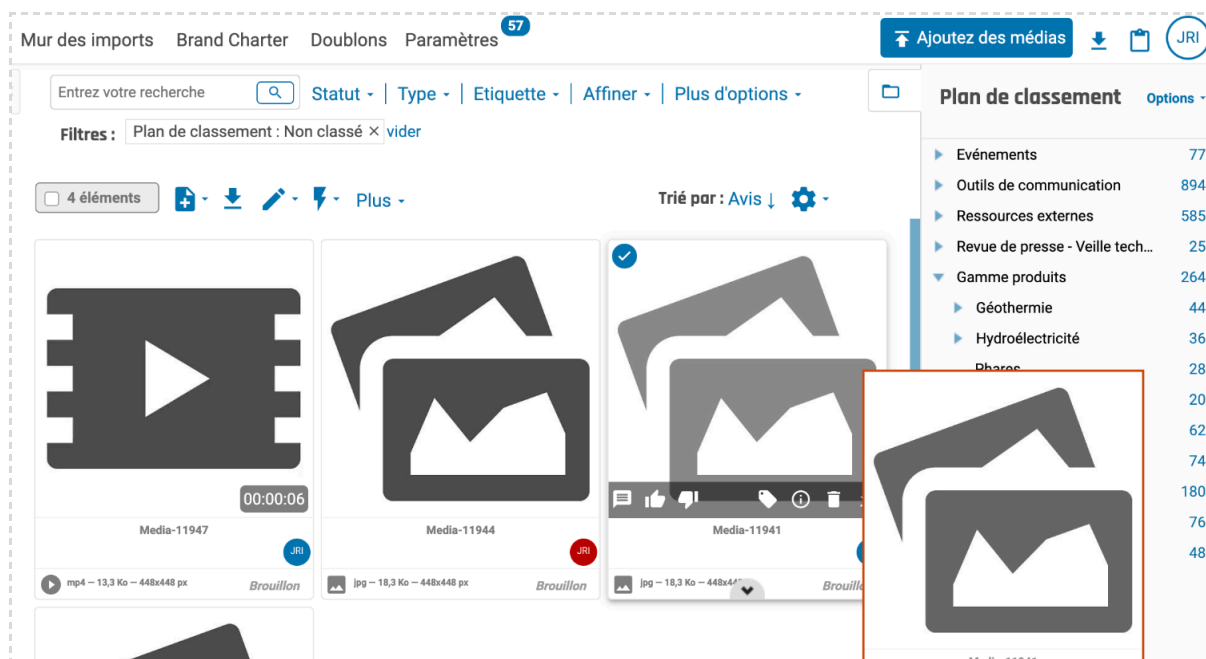
Il n'y a plus de notion de propriétaire. **Les contributeurs sont tous responsables des contenus qu'ils y déposent.** Il est requis de disposer du droit d'écriture sur les médias que l'on souhaite y déposer



## Classement dans un dossier

Depuis un espace collaboratif, il est possible de déposer des contenus dans le plan de classement, via le volet de droite.

Les dossiers autorisés sont ceux sur lesquels l'utilisateur possède au moins le droit d'écriture.



Attention, si les contenus déposés sont déjà classés ailleurs, la règle limitant l'élévation de droit s'applique ! On ne peut pas placer un média dans un autre dossier si on a moins de droit sur le dossier d'origine que sur le dossier de destination.

## Cas particulier pour la diffusion sélective de l'information (ABAC)

Par défaut, les règles de "partage de droit" présentées ci-dessus s'appliquent.

Dans le cas de la diffusion sélective de l'information (ABAC), il est cependant possible d'activer une sécurité qui permet de faire appliquer les limitations sur la valeur du champ thésaurus. Cela assure qu'un contenu inadapté ne sera pas visible d'un membre du partage.

**TECH**, la propriété technique `ABAC_BASKET_ACTIVATED` permet d'ajuster le comportement dans l'ensemble des espaces collaboratifs.

## Accès administrateur à tous les espaces collaboratifs

Afin d'offrir un contrôle total aux administrateurs, chaque espace collaboratif (paniers, workflows, tableaux) propose un filtre réservé aux admins, permettant d'afficher l'exhaustivité des contenus.



Accéder de cette manière à un espace collaboratif offre l'équivalent des droits du propriétaire (ou gestionnaire pour les tableaux). Cela veut dire qu'en tant qu'admin, vous pouvez agir sur les membres du partage (inviter, retirer, modifier le niveau de droit), ainsi que les contenus.

Vous pouvez par ailleurs supprimer n'importe quel espace pour faire du ménage.

Pour les paniers, vous avez la possibilité de réattribuer un panier à un autre propriétaire. Pratique lorsqu'un collaborateur quitte l'entreprise et que ses paniers en cours sont à reprendre.

Pour ce faire, vous pouvez le modifier unitairement dans le paramétrage du panier :

**Les éléments du panier**

---

**Paramètres du panier**  
Modifiez les informations, le statut ou l'ordre d'affichage des éléments

---

**Partage collaboratif**  
Partager le panier avec des membres ou des invités identifiés

---

**Partage public et emailing**  
Activer le partage public et envoyez un lien pour donner un accès à votre sélection.

**Tags**

---

**Statut \***

Activé ▼

---

**Ordre d'affichage des éléments**

Choisissez un critère de tri ou optez pour le tri manuel des éléments \*

Date d'ajout ▼

Croissant  
 Décroissant

---

**Propriétaire de panier**

Panier créé le 11/11/2023 à 23:41  
Propriétaire: UJ Visiteur [Changer](#)

Vous pouvez aussi effectuer cette modification par lot depuis la liste des paniers avec le bouton édition.

### Édition du panier

✕

Les actions que vous choisirez d'effectuer en cochant les cases ci-dessous s'effectueront sur tous les paniers sélectionnés

Modifier les tags

Ajouter les tags

Supprimer les tags

Tags...

Modifier le propriétaire

Julien Richard ✕

Modifier le statut

Statut... ▼

Annuler
Modifier les paniers

Pour rappel, ce sont les droits du propriétaire qui prévalent. Changer de propriétaire implique donc que les nouveaux contenus ajoutés seront désormais soumis aux droits de ce nouvel utilisateur. Par contre, il n'est pas vérifié que l'utilisateur possède les droits adéquats sur les contenus déjà présents dans le panier. En règle générale, on substitue un propriétaire par un utilisateur occupant un rôle équivalent, ce qui ne pose donc aucun problème.

Note : le changement de propriétaire de workflow n'est pas proposé, mais vous pouvez modifier les responsables des étapes. Pour les tableaux, la notion de propriétaire n'existant

pas, vous pouvez attribuer un nouveau membre en gestionnaire du tableau (on peut d'ailleurs cumuler plusieurs gestionnaire pour un même tableau).

# CHAPITRE 3

## Gestion avancée pour les projets d'envergure

### Multigroupe

Le multigroupe offre la possibilité de placer un utilisateur dans plusieurs groupes. Cette mécanique a été instaurée afin de répondre aux besoins de gestions de droits plus complexes des entreprises souhaitant accueillir les contenus de plusieurs entités dans une seule instance Keepeek.

Cela implique de gérer différentes populations d'utilisateurs, leur attribuer les droits adéquats, mais permettre d'avoir des accès transverses à certains contenus des autres entités.

### Du multigroupe pour gérer du multi-marques

Il est fréquent que lorsqu'on souhaite cumuler plusieurs marques dans une même instance Keepeek, on doive s'appuyer sur le multi-groupe. Cela permet en effet de pouvoir attribuer un niveau de rôle par marque à un utilisateur. De cette manière, un utilisateur peut être un contributeur de la marque A, mais accéder en visiteur (lecture) aux contenus de la marque B.

ATTENTION, le multi-marques en mono-instance comporte certaines limitations qu'il est important de connaître.

Ce [document](#) expose ces différentes limitations qui permettront de décider s'il est sage de cumuler l'ensemble des contenus dans une seule instance ou préférable de créer une instance par marque.

### Module d'inscription

Sur les portails, il peut être proposé un formulaire d'inscription pour que vos utilisateurs externes puissent se créer un compte. En fonction de ce que l'utilisateur remplit comme informations, il pourra être attribué à un groupe, avec accès immédiat ou nécessitant validation préalable d'un administrateur.

Le multigroupe permet dans ce contexte d'offrir un accès temporaire partiel à celui qui s'inscrit. Lors de son inscription, il peut en effet être ajouté dans un groupe actif, qui lui donne accès à un contenu limité, tout en étant ajouté dans un groupe avec plus de droits, mais en attente d'activation.

Le module d'inscription et le multigroupe servent aussi à la cohabitation de plusieurs portails. Un utilisateur déjà inscrit sur un portail peut s'inscrire sur un autre, et être alors ajouté à un groupe additionnel pour lui octroyer les droits adéquats sur le nouveau portail sans pour autant perdre ses accès sur l'autre.

## Quels droits prévalent entre 2 groupes ?

Si un utilisateur est placé dans 2 groupes différents, et que ces 2 groupes offrent un accès à un même dossier du plan de classement, c'est le droit le plus élevé qui prévaudra.

Par exemple, reprenons nos marques Primo et Secondo :

- Le groupe "Contributeur Primo" propose des droits en écriture sur les dossiers de la marque Primo, mais offre aussi un accès en lecture aux contenus publiés de la marque Secondo.
- Même chose côté Secondo. Le groupe "Contributeur Secondo" donne le droit en écriture sur les dossiers de la marque Secondo mais offre aussi un accès aux contenus de la marque Primo.
- Alors, un utilisateur qui serait positionné dans les 2 groupes contributeurs des marques obtiendrait, par union des droits, l'accès en écriture sur les dossiers des 2 marques

Note : il est cependant conseillé de rester "simple" et donc de ne pas cumuler des droits sur un même dossier. Cela vous facilitera la lecture des accès octroyés à un utilisateur et lever les ambiguïtés.

## Un groupe additionnel pour un droit transverse à plusieurs groupes

Une autre façon d'exploiter le multigroupe consiste à créer un groupe dédié à un droit précis.

Prenons l'exemple d'un groupe avec de nombreux utilisateurs. Pour une partie d'entre eux, vous souhaitez activer le module "Tableaux". Plutôt que de devoir les séparer dans des groupes distincts pour y attribuer les bons droits, vous avez une autre alternative.

Créez un nouveau groupe "Accès tableau", dans lequel vous vous contentez d'autoriser l'accès à la fonctionnalité "Tableaux". Il vous suffit alors d'ajouter ce groupe aux utilisateurs concernés, sans les changer de groupe d'origine. Ils bénéficieront alors des mêmes accès que précédemment, mais avec en plus la possibilité d'utiliser les tableaux.

## Groupes gestionnaires et sous-groupes

Pour la gestion d'une population, il est souvent nécessaire de déléguer la responsabilité à des responsables de l'entité. Mais il n'est souvent pas souhaitable que ces personnes disposent d'un droit d'administrateur complet sur toute l'instance.

C'est pourquoi il existe le niveau de groupe "gestionnaire", qui permet de se substituer à un administrateur sur un sous-ensemble de contenus et fonctionnalités.

Veuillez consulter la rubrique "[Administration déléguée aux gestionnaires](#)" de cette documentation.

## Précautions d'usage

Utiliser le multi-groupe peut occasionner des incohérences et élévations de droits si on ne connaît pas bien son mécanisme.

Si on n'y prend pas garde, la combinaison des droits du groupe A avec ceux du groupe B peut engendrer des droits que ni l'un ni l'autre des groupes ne proposent à la base.

Pour plus d'informations, consultez [l'Annexe 1 : pyramide des droits](#).

# Administration déléguée aux gestionnaires

Un groupe gestionnaire permet d'octroyer certaines activités d'administration à des utilisateurs, mais restreintes à une sous-partie de Keepeek.

Voyons ce qu'il est possible de déléguer :

- Gestion d'utilisateurs :
  - Création de groupes visiteur et contributeur
  - Création d'utilisateurs
  - Ajout d'utilisateurs dans les sous-groupe du gestionnaire
- Gestion documentaire
  - Création de fiche d'élément
  - Création de champ de fiche
- Gestion des contenus
  - Accès à la corbeille globale
  - Accès aux doublons
  - Accès au paramétrage des formats de téléchargement
  - Accès au paramétrage des planches-contacts
  - Accès aux statistiques d'usage
  - Accès au paramétrage de la recherche
- Autres
  - Gestion de chaîne YouTube ([nécessite le module YouTube](#))
  - Edition/modification des personnes ([nécessite le module de détection de visages](#))
  - Paramétrage des anciens portails utilisateurs

Important à savoir : dans Keepeek, on peut créer plusieurs groupes "gestionnaires". Cependant, un même utilisateur ne peut être attribué qu'à un seul groupe gestionnaire maximum. Au-delà, il faut envisager le niveau "Administrateur".

## Paramétrage des fonctionnalités autorisées à la gestion

Même principe que pour les fonctionnalités autorisées à un groupe. On retrouve dans la section "Accès > Modules de paramétrage" les différentes sections à déléguer au groupe gestionnaire.

Keeppeek Recherche ▾ Espaces collaboratifs ▾ Mur des imports Brand Charter Doublons Paramètres <sup>14</sup> [Ajoutez des médias](#)

[Retour](#)

**Diffusion Interne - Eolienne**  
[1 utilisateurs dans ce groupe](#)  
 Groupe actif ●  
 Créé par Alban Bolzon le 29/05/2018

- Paramètres du groupe
- Droits sur les dossiers et les éléments
- Accès
- Applications
- Fonctionnalités
- Chaînes YouTube
- Modules de paramétrage
  - Formats autorisés
  - Gestion documentaire

**Accès au paramétrage des formats**  
 Ce module permet de créer ou de modifier les formats de téléchargement. Il permet également de gérer les permaliens ou les formats de galeries

**Accès au paramétrage de recherche**  
 Ce module permet de paramétrer le moteur de recherche et la liste des facettes affichées. Il permet également la gestion des formulaires de recherche.

**Accès au paramétrage des portails utilisateurs**  
 Ce module permet de paramétrer les éléments de la page d'accueil, de la recherche ainsi que le filtrage des adresses IP pour chacun des portails utilisateurs sélectionnés ci-dessous.

	Nom	Adresse
<input type="checkbox"/>	baobab-standard	https://qualification-baobab-standard.ci.keepe...
<input checked="" type="checkbox"/>	baobab-complet	https://qualification-baobab-complet.ci.keepe...

**Accès aux statistiques**  
 Ce module permet d'observer l'utilisation de la photothèque. Des termes recherchés aux éléments téléchargés en passant par les connexions des utilisateurs, il permet de constater l'activité de la photothèque et d'en déduire des actions à mener pour la rendre encore plus exploitable.

**Accès à l'édition des personnes**  
 Ce module permet l'édition et la suppression des personnes identifiées pour la reconnaissance de visages

**Accès au paramétrage des blanches-contacts PDF**

[Sauvegarder](#)

Pour déléguer la gestion des fiches et des champs de fiche, une autre section est dédiée : "Gestion documentaire".

Keeppeek Recherche ▾ Espaces collaboratifs ▾ Mur des imports Brand Charter Doublons Paramètres <sup>14</sup> [Ajoutez des médias](#)

[Retour](#)

**Diffusion Interne - Eolienne**  
[1 utilisateurs dans ce groupe](#)  
 Groupe actif ●  
 Créé par Alban Bolzon le 29/05/2018

- Paramètres du groupe
- Droits sur les dossiers et les éléments
- Accès
- Formats autorisés
- Gestion documentaire
- Fiches d'éléments
- Champs de fiches

**Autoriser la gestion des fiches d'éléments**  
 Donne accès au menu d'administration des fiches d'éléments.

Sélectionnez les fiches d'éléments autorisées :  
[Tout sélectionner](#) / [Tout désélectionner](#)

**Images**

	Nom
<input type="checkbox"/>	Zephyr - photos
<input type="checkbox"/>	Exemple 1
<input type="checkbox"/>	Images
<input type="checkbox"/>	Photos produit
<input type="checkbox"/>	Vega - photos d'implantation
<input type="checkbox"/>	Tous les types de champ de fiches

**Documents**

Pour chaque rubrique, il faut d'abord activer le switch en haut de l'écran.

Autoriser la gestion des fiches permettra au groupe gestionnaire de créer de nouvelles fiches.

Mais en plus de ça, l'écran expose la liste des fiches existantes pour autoriser le gestionnaire à modifier des fiches communes, etc.

Il en va de même pour la section "champ de fiche", pour d'une part autoriser la création de nouveaux champs, mais aussi l'édition de champs existants.

## Gestion d'utilisateurs

### La création de groupe

Fonctionne de la même manière que pour les administrateurs.

Le groupe créé ne peut être que de type "Visiteur" ou "Contributeur" (un groupe gestionnaire ne peut pas être sous la gestion d'un autre groupe gestionnaire).

Le nouveau groupe créé se trouve associé au groupe gestionnaire en tant que groupe parent.

En termes de droits, le gestionnaire sera cependant limité à octroyer des accès et fonctionnalités que dont son groupe gestionnaire dispose. C'est une contrainte de sécurité.

### La création d'utilisateurs

Fonctionne de la même manière que pour les administrateurs.

L'utilisateur créé ne pourra bien sûr qu'être ajouté à l'un des sous-groupes du gestionnaire.

Le gestionnaire peut modifier/supprimer un utilisateur seulement s'il n'est dans aucun autre groupe dont il n'a pas la gestion.

### L'ajout d'utilisateurs

Un gestionnaire **peut accéder à l'ensemble des utilisateurs de la plateforme** !

Cependant, il n'aura pas possibilité de modifier un utilisateur qui est associé à un autre groupe dont il n'a pas la gestion.

Il ne peut qu'ajouter des groupes dont il a la gestion pour leur fournir des droits d'accès sur l'entité qu'il gère. Dans un contexte multi-marque, cela permet à un gestionnaire de marque de définir les droits d'accès aux contenus de sa marque, à n'importe quel utilisateur de l'entreprise.

Paramétrage expert pour multi-marque :

Pour information, il existe une mécanique de "groupe de dépôt" ou "groupe de synchro". Utilisée dans certains contextes multi-marques où un groupe sert à stocker l'ensemble des utilisateurs issus d'un annuaire externe, et où les gestionnaires de marque vont venir

rechercher dans ce groupe de dépôt pour attribuer le bon niveau de droit à sa marque. Afin de ne pas être limité en modification de l'utilisateur (comme le groupe synchro n'est pas un sous-groupe de marque), la subtilité du groupe de dépôt est qu'il sera retiré de l'utilisateur dès qu'il sera associé à un autre groupe. L'utilisateur devient ainsi pleinement sous le contrôle du gestionnaire qui l'a récupéré.

## Gestion documentaire

Là aussi, cette délégation de droit est le plus souvent mise en place pour du multi-marque. Chaque gestionnaire de marque va vouloir être autonome sur la création de ses fiches et de ses champs de fiches, sans risquer d'affecter le paramétrage des autres marques.

Fonctionne comme pour les administrateurs.

Limite simplement la liste aux fiches et champs de fiches qui ont été autorisés ou créés par le gestionnaire.

## Gestion des contenus

### Accès à la corbeille globale

Chaque utilisateur dispose de sa propre corbeille pour y retrouver les contenus qu'il a supprimé. Mais il existe la corbeille dite "globale" permettant de retrouver l'ensemble des contenus qui ont été supprimés par les utilisateurs afin d'apporter une surveillance avant leur suppression définitive

Déléguer l'accès à la corbeille aux gestionnaires va permettre de les laisser superviser les contenus supprimés qui les concernent.

Ne remonteront en effet que les éléments supprimés qui étaient placés dans un dossier sur lequel le groupe gestionnaire possède un accès en "gestion des dossiers".

### Accès aux doublons

Le module de doublons permet de remonter les doublons exacts présents dans la base. Déléguer aux gestionnaires est souvent nécessaire car ce sont eux qui sauront choisir ce qui est à nettoyer.

Les droits dont ils disposent sur le plan de classement assurent qu'ils ne pourront supprimer que les contenus sur lesquels ils disposent du droit de suppression.

### Accès au paramétrage des formats de téléchargement



Avec cette option, vous pourrez offrir à vos gestionnaires la liberté de créer de nouveaux formats de téléchargement et les proposer aux sous-groupes d'utilisateurs dont ils ont la gestion.

### **Accès au paramétrage des planches-contacts**

Il en va de même pour les planches-contacts que vos gestionnaires pourront ainsi structurer, charter et partager à leurs utilisateurs.

### **Accès au statistiques d'usages**

Si vos gestionnaires sont responsables d'une partie du plan de classement, leur donner accès aux outils de statistiques leur permettra de contrôler l'usage qui est fait de leur fonds documentaire.

Leur permettre de suivre les connexions de leurs utilisateurs, les consultations, téléchargements et imports, pourra leur servir à optimiser leur gestion.

### **Accès au paramétrage de la recherche**

Ajouter des champs aux facettes (filtre "Affiner") ou construire des formulaires de recherche peut être délégué à des gestionnaires.

Attention cependant, ces paramétrages sont totalement partagés à tous les utilisateurs. Il n'y a pas de mécanique de cloisonnement par entité/marqué pour ce module de paramétrage donc déléguez prudemment.

## Autres

### **Gestion de chaîne YouTube** (nécessite le module YouTube)

Le module YouTube permet de gérer la publication de vidéos uploadées dans Keepeek vers une chaîne YouTube.

Déléguez à vos responsables de marques le paramétrage de leurs chaînes respectives.

### **Edition/modification des personnes** (nécessite le module de détection de visages)

Le module de détection de visages permet de détecter les visages de vos images et de nommer les personnes correspondantes.

Ce module propose alors un nouvel écran de recherche proposant l'ensemble des images où une personne apparaît.

Il nécessite toutefois un contrôle à avoir sur les personnes à référencer, et cette gestion peut donc être déléguée aux groupes gestionnaires.

## Paramétrage des anciens portails utilisateurs

Pour les anciens portails, le paramétrage se faisait depuis l'interface d'administration du backoffice.

Il peut être nécessaire d'y autoriser l'accès à un groupe gestionnaire, afin que celui-ci se charge d'adapter, d'éditorialiser et d'animer son contenu.

Cochez les portails dont vous voulez déléguer le paramétrage :

	Nom	Adresse
<input checked="" type="checkbox"/>	Portail utilisateur #1	https://qualification-baobab-standard.ci.keepee...
<input type="checkbox"/>	Portail utilisateur #2	https://qualification-baobab-complet.ci.keepee...

Dès lors, ils pourront accéder à l'ensemble des menus de paramétrage du portail pour y modifier les widgets de la page d'accueil, les dossiers proposés en mosaïques, etc.

**Widgets de la page d'accueil**  
Définissez les mosaïques, les articles et autres widgets à faire apparaître sur la page d'accueil du portail utilisateur.

Ajouter un widget à gauche +    Ajouter un widget à droite +

- Outils de communication**  
Mosaïque (taille intermédiaire)
- Bienvenue !**  
Article
- Mes dernières recherches**  
Widget
- Dossiers favoris**  
Widget
- Notre société**  
Dernières vidéos
- Notre société**  
Derniers contenus

Pour les nouveaux portails, le paramétrage s'effectue directement depuis le portail, mais n'est pour le moment réservé qu'aux profils administrateurs. Il ne peut être délégué à un gestionnaire.

## Accès aux applications

Le Backoffice est un outil très complet mais parfois complexe pour les populations novices. Keepeek propose une gamme de produits variés pour s'adapter à votre écosystème et vos différentes populations.

Par exemple, le portail utilisateur proposera une interface plus épurée et personnalisée à la charte graphique de l'entreprise, à destination des visiteurs qui viennent simplement rechercher et télécharger des contenus.

Voici les différents types d'applications disponibles :

- Le Backoffice
- Les portails ancienne génération
- Les portails nouvelle génération
- L'application Mobile (Android / iPhone)
- Les plugins (Photoshop, Keepicker, etc...)
- Autre application tierce (utilisant l'API Keepeek)

### Portée des droits du Backoffice

Les droits d'un utilisateur dans Keepeek, qu'il accède à des contenus via le Backoffice, un portail, un plugin ou même l'API, dépendent exclusivement de ce qui a été autorisé à ses groupes via le Backoffice.

C'est la source de vérité. Si vous vous demandez pourquoi un utilisateur peut accéder à un contenu, c'est que les droits du backoffice le lui permettent.

### Autoriser une autre application à un groupe

Les droits d'accès d'un utilisateur sont toujours définis par le groupe auquel il appartient. Les applications qui lui sont autorisées suivent la même logique :

The screenshot shows the 'Accès aux applications' (Application Access) settings for the 'Visiteur' group. The interface includes a navigation menu on the left with options like 'Paramètres du groupe', 'Droits sur les dossiers et les éléments', 'Accès', 'Applications', 'Fonctionnalités', 'Chaînes YouTube', and 'Formats autorisés'. The main content area displays a table of applications with checkboxes to enable or disable access.

	Nom	Adresse
<input type="checkbox"/>	Backoffice	https://qualification.ci.keepeek-dev.com
<input type="checkbox"/>	Mobile Keeppeek	
<input checked="" type="checkbox"/>	Portail utilisateur #1	https://qualification-baobab-complet.ci.keepeek-dc
<input checked="" type="checkbox"/>	Portail utilisateur #2	https://rc-qualification-refront.keepeek.com
<input type="checkbox"/>	Plugins Keeppeek	

Ainsi, pour chaque groupe utilisateur, vous pourrez définir à quelles applications il donnera le droit d'accès.

## Portail et Keeppicker : cloisonnement par filtrage permanent

Comme dit précédemment, le droit défini dans le Backoffice prévaut. Les contenus auxquels un utilisateur accèdera au travers d'un portail ne sont que le reflet de ce que le groupe dispose comme droits sur le plan de classement du backoffice.

Cependant, il est parfois utile de restreindre les contenus qu'un portail (ou toute autre application peut remonter) selon le contexte.

Prenons l'exemple d'un portail destiné aux téléchargements des contenus publiés. Les contributeurs ont le droit d'y accéder. Mais le backoffice les autorise en plus à accéder aux contenus en cours de création/validation (brouillons). Mécaniquement, ces contenus pourraient leur être remontés dans le portail. Mais pour éviter toute ambiguïté et un mauvais usage des contenus du portail, il est préférable d'assurer qu'aucun contenu non publié n'apparaisse dans le portail, et ce, même si les utilisateurs disposent de droits supérieurs.

Autre cas de figure très fréquent : le multi-marque.

Un même backoffice sert souvent à stocker les assets de toutes les marques du groupe. Mais pour les exposer au téléchargement, il est généralement mis en place un portail utilisateur PAR marque. Un utilisateur peut être autorisé à accéder au contenu de plusieurs

marques, mais il serait mal venu qu'il trouve du contenu de la marque A via le portail de la marque B.

Pour résoudre ces cas de figures, plusieurs de nos applications (ancien et nouveau portail, ainsi que le Keepicker) proposent une mécanique de filtrage permanent.

Ce sont des filtres additionnels qui s'appliqueront à toute recherche, pour s'assurer que des contenus inadaptés ne puissent remonter.

Cette mise en œuvre ne peut être réalisée que par l'intermédiaire des intervenants Keepeek (généralement établi dès le build projet). Côté nouveau portail, il est possible d'affiner la portée du filtrage permanent pour le faire s'appliquer aux éléments associés ou pas dans la page détail.

**Note :** Nous insistons sur le fait que le filtrage permanent n'est pas véritablement une notion de droit, mais une simple capacité de filtre. C'est une notion important à garder en tête pour les aspects sécurité. La source de vérité reste le paramétrage Backoffice. Le détournement des appels API (et des critères de filtre) peut exposer l'ensemble des contenus qu'un utilisateur, sans que le filtrage permanent de l'application ne s'applique.

TECH, pour en savoir plus sur le paramétrage du filtrage permanent sur un nouveau portail, consultez [cette documentation](#).

### **Le filtrage permanent comme mécanique de navigation ?**

Certains portails se sont appuyés sur le filtrage permanent pour proposer une expérience de navigation par grappe. Le principe consiste à avoir des médias associés entre eux (exemple, des déclinaisons d'un même logo), et que sur l'un d'eux soit apposé une valeur "média représentatif". Dans le filtrage permanent, on définit qu'on ne souhaite remonter que les médias représentatifs. Si bien que de la grappe de déclinaison de logos, un seul résultat ne remonte dans la recherche.

Mais, les autres médias associés sont quant à eux accessibles via l'affichage des associations, dans le détail de l'élément représentatif, si bien que l'accès aux déclinaisons du logo fonctionne, sans pour autant polluer le résultat de recherche par trop de médias correspondants.

## Cloisonnement des paniers

Dans la continuité du filtrage permanent, une autre mécanique est à l'œuvre pour éviter de se retrouver avec des contenus d'un panier du portail A, accessible via le portail B.

On parle de "cloisonnement des paniers".

Dans le backoffice, il est possible de remonter tous ses paniers, quelque soit l'application où il a été construit. Un filtre est à disposition pour cibler l'application souhaitée.

Sur les anciens portails, seuls les paniers créés dans le portail sont accessibles.

Sur les nouveaux portails, il existe un paramétrage permettant de choisir si le cloisonnement doit s'appliquer (comme dans les anciens portails) ou pas.

L'application mobile (android et iPhone) crée et remonte des paniers attribués au "backoffice".

# CHAPITRE 4

## Informations complémentaires

### F.A.Q : foire aux questions

#### Peut-on masquer un sous-dossier à un groupe ?

Non, lorsqu'un dossier a été autorisé à un groupe, tous les sous-dossiers seront accessibles. Il est possible d'abaisser le niveau de droit d'un sous-dossier, mais pas au point de le masquer totalement.

Cependant, dans le portail utilisateur, un dossier n'apparaît que si au moins 1 asset est accessible à l'utilisateur. Les dossiers vides ou n'ayant que du contenu masqué (par restriction de statut par exemple) n'apparaissent pas.

#### Un asset est présent dans 2 dossiers sur lesquels un groupe à des droits différents, que se passera-t-il ?

En effet, un média Keepeek peut être placé dans plusieurs dossiers.

On résout les droits en prenant le droit maximum de l'utilisateur. Si j'ai le droit "lecture" sur le dossier A et le droit "écriture" sur le dossier B, un média présent dans les deux dossiers me sera autorisé en "écriture".

#### Un utilisateur est attribué à 2 groupes qui ont des droits différents sur un même dossier, que se passera-t-il ?

En effet, un utilisateur Keepeek peut être placé dans plusieurs groupes.

On résout les droits en prenant le droit maximum de l'utilisateur. Si j'ai le droit "lecture" sur le dossier X grâce au groupe A et le droit "écriture" sur ce même dossier X via le groupe B,, un média présent dans ce dossier me sera autorisé en "écriture".

## Les visiteurs ne voient pas certains médias alors que je n'utilise pas la restriction par statut, pourquoi ?

Même sans restriction par statut, le droit en lecture sur un dossier ne fera apparaître que les éléments qui sont dans un statut "publié". Les éléments brouillons ou archivés ne sont jamais visibles pour les utilisateurs ne disposant que du droit "lecture" d'un dossier.

## Pourquoi les utilisateurs voient dans leur filtres des noms de fiche ou de champs qui ne leur sont pas autorisés ?

Dans Keepeek, il n'y a pas de notion de droit sur les fiches. Les accès sont régis par les 3 grands modes de droits exposés dans cette documentation. Si bien que dans la recherche avancée, les ordre de tris, il est présenté l'exhaustivité des fiches et des champs qui existent dans la base, indépendamment des droits paramétrés, par souci de performance.

## Lorsqu'un contributeur crée un média, ce média disparaît immédiatement après sa création ! Pourquoi ?

La diffusion sélective de l'information (ABAC) implique qu'un contenu ne sera visible que s'il possède la valeur adéquate dans sa fiche. Si un contributeur crée un contenu alors qu'il est soumis à une diffusion sélective, s'il ne positionne pas la bonne valeur, il ne sera pas autorisé à voir son propre contenu.

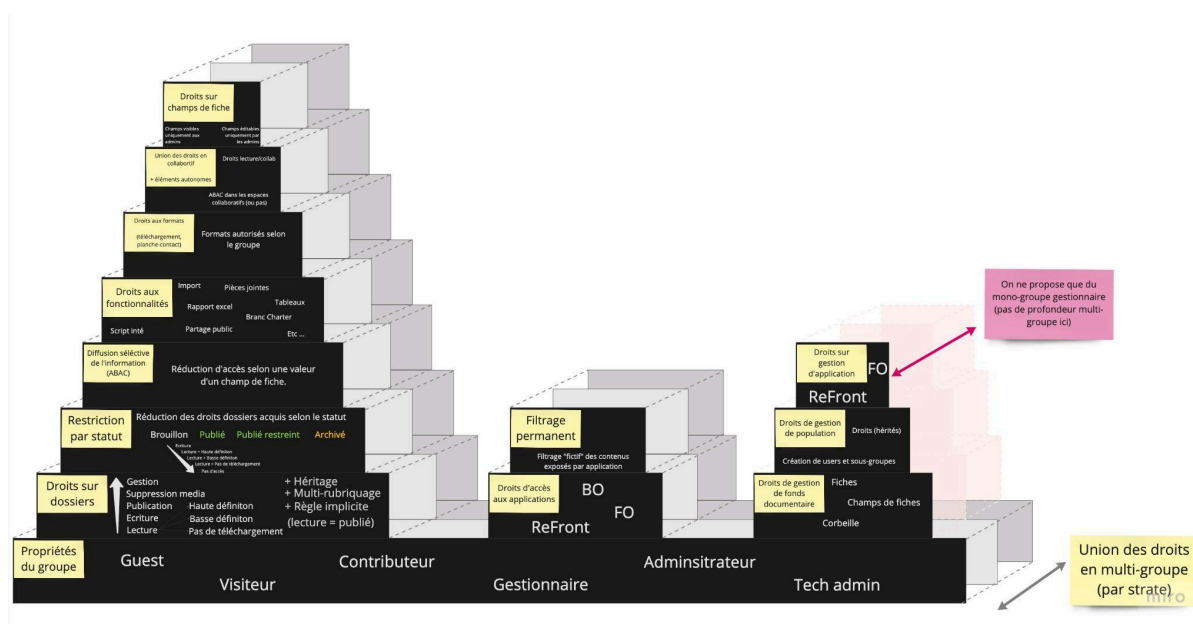
La diffusion sélective de l'information ne se prête pas bien aux profils contributeurs, il est conseillé de le réserver aux profils visiteurs.

## En tant qu'administrateur, comment accéder aux contenus des murs d'import?

Cette fonctionnalité n'est pas disponible actuellement. Nous envisageons aujourd'hui de supprimer la fonctionnalité de mur des imports et rediriger les utilisateurs vers la fonctionnalité "Panier" pour effectuer leurs imports.

# Annexes

## Annexe 1 : pyramide des droits



Il s'agit d'une représentation de l'ensemble de notre module de droit.

Il décrit notamment comment cette mécanique fonctionne. La résolution des droits fonctionne en effet par couches successives.

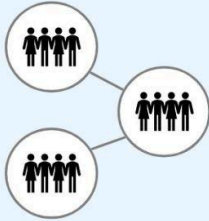
Et la profondeur (gris clair et foncé) exprime que les droits en multi-groupe sont résolus PAR couche de droit.

On résout indépendamment l'ensemble des dossiers, l'ensemble des restrictions par statut, l'ensemble des fonctionnalités autorisées, etc.

Si bien que le multi-groupe peut occasionner quelques phénomènes étranges.

La combinaison de 2 groupes peut offrir des droits que ni l'un ni l'autre des groupes ne possède à la base.

Quelques exemples décrits par l'infographie ci-dessous :



Le multi-groupe a vu le jour avant tout pour répondre à des contextes multi-marque et multi-fonds. Dans ces contextes, des personnes peuvent se retrouver à accéder à différents fonds du DAM, et avec des niveaux de droits différents.



Le multi-groupe déclenche l'union des droits pour chaque étage de la pyramide.



### Prenez par exemple ces 2 groupes :



A chaque étage, on prend le "meilleur" des 2 mondes (le moins contraint) Si bien qu'en ajoutant l'accès visiteur Stanhome à un contributeur Yves-Rocher, celui-ci se retrouve à obtenir le droit de téléchargement haute def sur les éléments en **Brouillon** et **Archivé** du répertoire **Yves Rocher**.

Dans cette logique, donner accès à un utilisateur à un Groupe A et un Groupe B peut octroyer des droits que ni le groupe A, ni le groupe B n'offrent en temps normal. Et donc générer des failles de sécurités.

Note : dans l'exemple, cela se compense par aller paramétrer la même configuration de restriction par statut sur le groupe

### Un autre exemple :

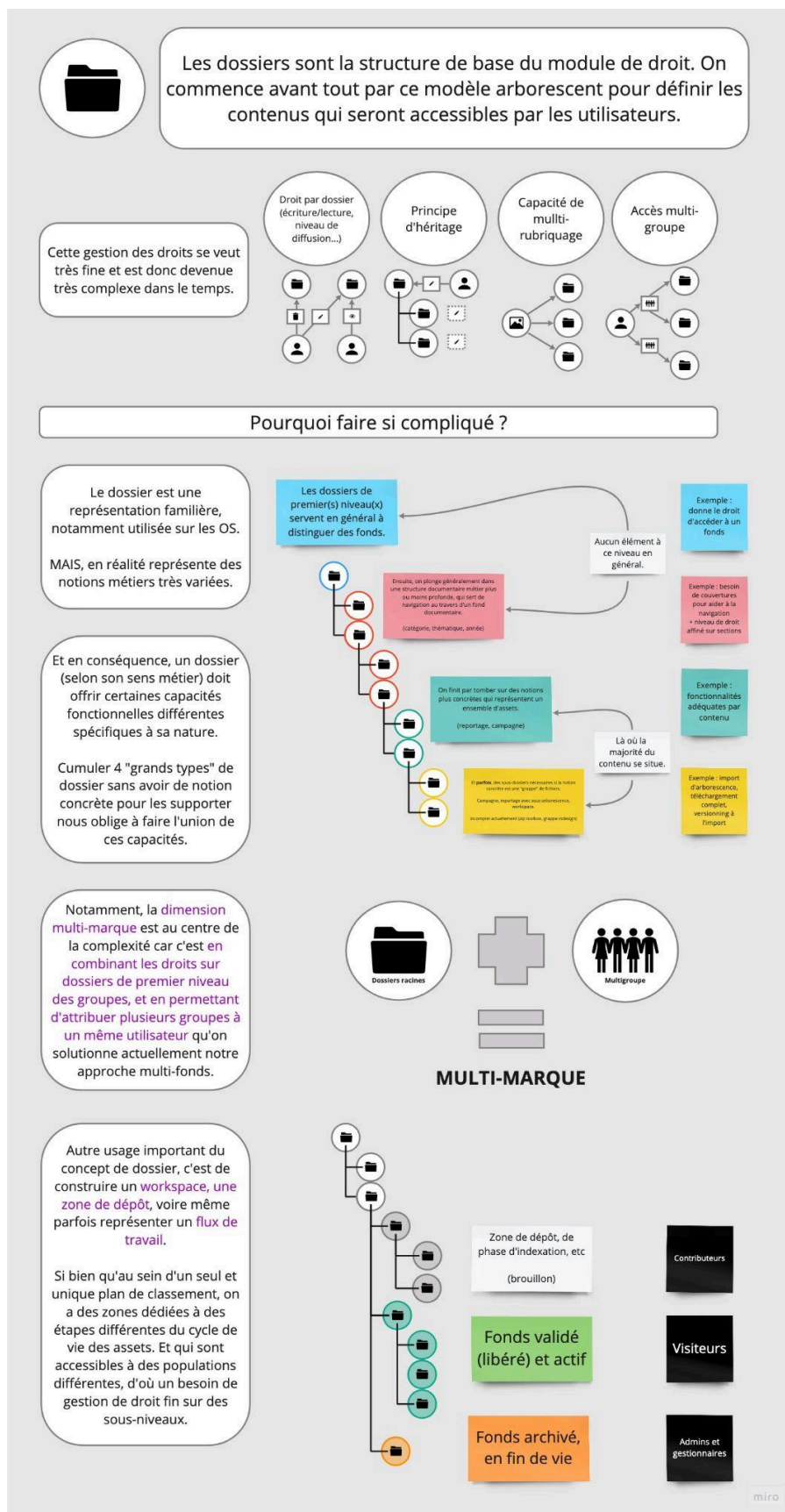


Les formats ne sont pas cloisonnés et associés aux dossiers attribués à chacun des groupes. Si bien que la **planche Yves-Rocher** m'est proposée pour extraire les **contenus Stanhome** (et vis-versa).

Moins "grave" en terme de sécurité MAIS finalement plus visible et perturbant en terme d'expérience utilisateur, on obtient l'ensemble des formats et des fonctionnalités sur l'ensemble des contenus cumulés.

miro

## Annexe 2 : complexité du modèle de droits sur dossiers



## Annexe 3 : réflexions sur la simplification du module de droits

Quand on parle de simplification du module de droits, on poursuit en même temps 2 objectifs.

Le 1er objectif est de réduire la complexité technique et fonctionnelle pour envisager plus sereinement de nouvelles évolutions. Durant une période où Keepeek a connu ses premiers gros clients, notamment multi-marques, le Backoffice a connu une période de boulimie des droits où de nombreux concepts se sont additionnés pour résoudre des besoins différents d'un client à l'autre. Le multi-groupe, l'ABAC, la restriction par statut sont autant de concepts qui sont venus alourdir la mécanique de droits initiale.

Au point où désormais, après avoir connu une douloureuse période de stabilisation, nous refusons quasiment systématiquement les évolutions fonctionnelles du module de droit, même si elles peuvent paraître légitimes. Le risque de régression est trop élevé.

Le 2ème objectif, c'est de clarifier l'administration pour nos clients. Cette complexité induite par notre pyramide des droits se répercute inévitablement sur l'interface et laisser un client seul organiser les droits de sa plateforme, sans formation préalable est dangereux voire impossible.

Différentes pistes ont pu être identifiées pour avancer vers ces objectifs. Cependant, le constat est qu'il n'y a pas de quick win.

### **Retirer l'ABAC**

L'ABAC n'est activé que sur demande et ce modèle des droits est peu utilisé et n'est pas pleinement abouti.

Le principe est intéressant, mais cumulé au reste de nos principes de droits, il engendre une complexité supplémentaire et ne pourra pas atteindre tout son potentiel.

### **Pourquoi le faire ?**

- Nettoyage de code et tech pro pour réduire la complexité du module de droits
- Clarification de la posture de déconseiller l'ABAC dans Keepeek
- On retire un étage de la pyramide, donc meilleure capacité à envisager d'autres évolutions sur le module de droits

### Pourquoi ne pas le faire ?

- Certains clients ont bâti leur gestion des droits dessus ?
  - A vérifier avec une analyse de données
- Le code est stabilisé, et modifier quelque chose sans gain fonctionnel est une prise de risque pour n'en obtenir aucun gain immédiat

Note : Bynder utilise principalement une mécanique similaire à l'ABAC. La gestion des droits est media-centrique, là où Keepeek est avant tout dossier-centrique.

### Retirer le niveau intermédiaire "basse définition"

L'opposition "Haute vs Basse définition" existe depuis la V3 dans Keepeek.

Elle provient du fait que des utilisateurs doivent pouvoir accéder à des formats standardisés mais pas aux originaux.

Cependant, dans les faits, il y a rarement de combinatoire poussée entre des dossiers "basse def" et d'autres "haute def" pour un même groupe. De plus, plusieurs fonctionnalités récentes dans Keepeek requiert un droit HD pour être utilisée (car vont potentiellement exposé l'original) : c'est le cas pour Dynameek, les pièces jointes, etc.

Le pilotage au niveau des formats autorisés serait plus pertinent. Et pour compenser cette perte de dissociation haute/basse définition, il serait possible de déporter le droit au téléchargement express des originaux au niveau des formats du groupe.

### Pourquoi le faire ?

- Nettoyage de code et tech pro pour réduire la complexité du module de droits
- Possibilité d'y aller progressivement
- Simplification de l'administration, des interfaces et des concepts à appréhender

### Pourquoi ne pas le faire ?

- Certains clients ont bâti leur gestion des droits dessus ?
  - A vérifier avec une analyse de données
  - "Migration" automatique probablement impossible, songer à un accompagnement
- Impacte la logique de demande de téléchargement : pouvoir la proposer même en droit HD
- Pas mal d'évolutions dans différents écrans

- "Perte" fonctionnelle
- Le code est stabilisé, et modifier quelque chose sans gain fonctionnel est une prise de risque pour n'en obtenir aucun gain immédiat

### **Contraindre/encadrer le multigroupe**

Comme vu en Annexe 1, le multigroupe peut occasionner des combinaisons inattendues.

Pour autant, se passer totalement du multigroupe dans Keepeek, c'est retirer un potentiel apprécié et confortable pour les grosses structures. Pour notre module d'inscription, et les contextes multi-portails, il n'est pas envisageable de s'en passer.

Toutefois, de nombreuses combinaisons possibles mais irréalistes sont autant de complexité de code à résoudre et de confusion fonctionnelle dans l'administration.

Concrètement, ça se matérialise comment ?

- Favoriser/faciliter le geste mono-groupe
  - Disposer d'un mode "mono-groupe" et n'activer que la capacité multi-groupe pour les projets avancés
- Interdire l'accumulation de droits groupes d'un utilisateur sur une même arborescence

### **Pourquoi le faire ?**

- Améliore l'expérience utilisateur de l'administration et simplifie la compréhension
- Evite les combinaisons fumeuses
- Réduit la complexité du code

### **Pourquoi ne pas le faire ?**

- Certains clients ont des structures de groupes complexes en multi-marque, et des mapping d'inscription/synchro sophistiqués
- Perte fonctionnelle
- Le code est stabilisé, et modifier quelque chose sans gain fonctionnel est une prise de risque pour n'en obtenir aucun gain immédiat

### **Droit "espace collaboratif" simplifié**

Actuellement, dans le code, il y a 2 stratégies distinctes de résolution des droits.

Il y a celle qui va calculer les droits qu'un utilisateur possède sur un média via le plan de classement. Celle-ci est utilisée dans le plan de classement ainsi que dans les différents modules de recherche.

Mais il y a également la méthode qui va en plus vérifier si des droits supplémentaires sont octroyés via un espace collaboratif. Car nous avons fait le choix que dans les espaces collaboratifs, on bénéficie de l'union des droits.

Exemple : si j'ai le droit de lecture dans un panier, mais que sur l'un des médias présents, j'ai le droit d'écriture via le plan de classement, alors j'aurais la possibilité de l'éditer, même depuis le panier, car on résout le droit par l'autorisation maximum.

#### Pourquoi le faire ?

- Perf et simplification du code
- Cohérence fonctionnelle => Je suis dans un espace collaboratif avec des droits bien définis sur son contenu, il n'y a pas de raisons majeures de bénéficier d'un autre droit dans ce contexte.

#### Pourquoi ne pas le faire ?

- Incompatibilité potentielle avec l'ABAC\_IN\_BASKET ?
  - A vérifier
- Impact sur l'ouverture détail hors contexte ?
- Le code est stabilisé, et modifier quelque chose sans gain fonctionnel est une prise de risque pour n'en obtenir aucun gain immédiat

#### **Droit dossier sur le 1er niveau uniquement**

Dans l'esprit des droits selon le cycle de vie où il est vivement conseillé de rester sur une autorisation simpliste du plan de classement, il pourrait s'avérer intéressant de limiter l'attribution des droits sur le 1er niveau de l'arborescence, impliquant l'impossibilité de redéfinir un niveau de droits plus bas dans la sous-arborescence.

C'est par ailleurs faire un pas vers la possibilité de ne plus avoir de plan de classement.

#### Pourquoi le faire ?

- Abaisser le côté "dossier-centrique" de la gestion des droits dans Keepeek (capacité à envisager l'absence de plan de classement comme certains outils concurrents)

#### Pourquoi ne pas le faire ?

- Le droit sur dossier est la brique de base de la pyramide et la logique fondamentale de Keepeek
- La limitation fonctionnelle est importante et nécessiterait probablement des compensations à faire développer à d'autres niveaux du module de droit
- Le code est stabilisé, et modifier quelque chose sans gain fonctionnel est une prise de risque pour n'en obtenir aucun gain immédiat

### **Droit "d'accès" sur dossier**

Dans l'approche "cycle de vie", le niveau de droit dossier donné n'a pas tant d'importance étant donné qu'il sera restreint ensuite par la restriction par statut.

Pour accentuer la compréhension et cette logique, on pourrait retirer la notion de droits sur dossier et ne considérer que tout ce qu'on donne sur un dossier du plan de classement, c'est un droit d'accès, sans autre subtilité. J'ai accès à un dossier, ou je n'y ai pas accès.

Les droits que j'aurais sur les médias d'un dossier sur lequel j'aurais accès dépendent simplement du statut dans lequel ils se trouvent (et du niveau de droit qu'on m'a octroyé pour ce statut). Cela impliquerait d'avancer dans l'approche "Cycle de vie" qui devrait permettre le même niveau de droits que celui proposé : Lecture/Ecriture/Publication/Suppression

#### **Privège sur les dossiers \***

The image shows a dropdown menu with the following options: 'Ecriture' (highlighted in green), 'Lecture', 'Ecriture', 'Publication', 'Suppression', and 'Gestion des dossiers'.

#### **Pourquoi le faire ?**

- Simplification de l'approche "cycle de vie" et des
- Vers une généralisation de l'approche "cycle de vie"

#### **Pourquoi ne pas le faire ?**

- A moins de pousser tout le monde vers la gestion en cycle de vie, cette approche resterait optionnelle

### **Dissocier les droits sur "la gestion de dossier" des droits sur "les éléments du dossier"**

Ici, il ne s'agit pas tant d'une simplification. L'évolution n'est pas sans risque, mais elle permettrait de débloquer une contrainte.

Actuellement, la hiérarchie des droits sur dossier implique que pour pouvoir créer une arborescence, il faut bénéficier du droit maximum.

Je ne peux pas créer une arborescence pour y inclure des éléments sur lesquels j'ai un droit inférieur à la suppression.

Dans différents cas d'usage, c'est une contrainte forte comme par exemple la duplication d'arborescence => implique de posséder le droits de suppression sur les éléments dupliqués (car les placer dans un dossier en gestion m'oblige à avoir le droit maximum)

Le client est alors amené à donner des droits élevés sur des données sources, ce qui l'expose à des risques d'erreur (voir des médias d'origine supprimés par erreur, etc).

#### Pourquoi le faire ?

- Débloquer certaines contraintes rencontrées chez nos clients et limiter les risques d'erreur
- Meilleure cohésion fonctionnelle
- Pas de problématique complexe de migration

#### Pourquoi ne pas le faire ?

- On toucherait à la brique de base de la pyramide des droits, ce n'est pas sans risque
- Mal pensé/présenté, ça peut se révéler comme une nouvelle complexification des droits
- Pas assez d'enjeux identifiés pour y aller ?

## Annexe 4 : refonte complète du module ?

Si nous avons la liberté de tout reconstruire, nous ferions sans doute des choix différents, grâce à tout ce que nous avons appris des concepts établis.

Une ébauche de réflexion pour la postérité :

