

ACL (Access Control List)
(Etienne Pallier – 24/06/2016)

I – Cycle de vie du statut du matériel

Créer un matériel ==> passe alors en statut **CREATED** ==> *peut alors être éventuellement supprimé (mais ne pourra plus être supprimé ensuite)*

Valider un matériel **CREATED** ==> passe alors en statut **VALIDATED** (resp et admin only)

Demander l'Archivage d'un matériel **VALIDATED** ==> passe alors en statut **TOBEARCHIVED** (resp et admin only)

Sortir de l'inventaire (Valider une demande d'archivage d'un matériel **TOBEARCHIVED**) ==> statut **ARCHIVED** (admin only)

Désarchiver un matériel ==> repasse de **TOBEARCHIVED** ou **ARCHIVED** à **VALIDATED** (admin only)

En résumé :

CREATED ==> **VALIDATED** ==> **TOBEARCHIVED** ==> **ARCHIVED**
 I \wedge **I** **I**
 V **I**-----**I**-----**I** (adminplus only)
DELETED

II - Droits des utilisateurs selon leur profil

A – Globalement (principes généraux)

Un utilisateur non logué ne doit RIEN pouvoir faire. Seulement se loguer, c'est tout. Il n'a accès qu'à la page d'accueil (de login).

Une fois logué, un utilisateur a des droits différents selon son profil, globalement :

- un **USER** ne peut que créer un matériel, un suivi, ou un emprunt, consulter, et modifier (uniquement ce qu'il a créé lui-même)
- un **RESPONSABLE** a tous les droits sauf accès à certains champs et certaines vues réservées à l'administration (**ADMIN**). Il ne peut pas non plus archiver un matériel, mais seulement demander l'archivage (comme un **USER**)(uniquement ce lié à son groupe métier ou thématiques)
- un **ADMIN**(istratif) a tous les droits (y-compris champs réservés à l'administration)
- un **ADMINPLUS** (administratif Plus) a tous les droits de **ADMIN** et en plus il peut modifier un matériel quelque soit son statut (y-compris **TOBEARCHIVED** et **ARCHIVED**), notamment il peut modifier le statut du matériel (pour le rétrograder)
- un **SUPERADMIN** a tous les droits : ceux d'**ADMINPLUS** et certains droits supplémentaires pour lui permettre des corrections d'erreur et la configuration de l'application (notamment l'administration des utilisateurs...)

Concernant les informations internes permettant de savoir **qui a fait quoi** (mises en place en février 2014), elles ne sont bien sûr pas modifiables puisque gérées automatiquement par le système, mais sont visibles par tous excepté le profil **USER**.

B - sur la table MATERIEL

	ALL (TOUS) (droits par défaut)	Utilisateur (quelconque)	Responsable	Administration	Administration Plus	Super-Administrateur
Read (un seul ou une liste) (view ou index)	Y <i>champs caches: donnees admin</i>	idem ALL	idem ALL	(idem Responsable + donnees admin) <i>En mode edit (update), si VALIDATED, on ajoute aux donnees readonly les donnees admin</i>	idem Admin	idem Adminplus
Create (1) (add)	Y <i>champs caches: donnees admin + statut + etiquette</i>	Idem ALL <i>champs readonly : nom_responsable</i>	idem ALL (+ etiquette)		idem Admin (tous les statuts) (+ champ statut) TOBEARCHIVED ou ARCHIVED: seulement le statut	
Update (1) (edit)	Y ssi CREATED (tous les champs) ou VALIDATED (quelques champs visibles sont readonly) (1) <i>champs caches: donnees admin + statut + etiquette</i>	idem ALL ssi createur				
Delete (delete)	Y ssi CREATED		idem ALL	idem Responsable	idem Admin	
Valider (statusValidated)	N (resp+)	idem ALL	Y ssi CREATED			
Demander archivage (statusToBeArchived)	N (resp+)		Y ssi VALIDATED			
Sortir de l'inventaire (statusArchived)	N (admin+)		idem ALL	Y ssi TOBEARCHIVED		
Desarchiver (2)	N (adminplus+)			idem Responsable	Y ssi ARCHIVED ou TOBEARCHIVED	
Exporter (csv)	N (resp+)		Y		idem Admin	
Montee de statut groupée	N (admin+)		idem ALL	Y		

Edition (4) DOCUMENTS	N (admin+)			Y - admission : ssi VALIDATED - sortie : ssi TOBEARCHIVED ou ARCHIVED		
Fiche Matériel	Y (sans partie admin)	Y (sans partie admin)	Y (sans partie admin)	Y	Y	Y (sans partie admin)

Par défaut, le superadmin a TOUS les droits

Conventions d'écriture :

- resp+ = possible pour un **Responsable et plus** (responsable, admin, adminplus, et superadmin)
- admin+ = possible pour un **Admin et plus** (admin, adminplus, et superadmin)
- ...

Notes :

(1) **Droits en modification (edit) :**

- Un simple « user » ne doit pas pouvoir modifier le responsable, ni le statut, ni l'étiquette, ni les données admin d'un matériel (en mode Création comme Modification)
- Un « responsable » ne doit pas pouvoir modifier le statut, ni les données admin d'un matériel (en mode Création comme Modification)
- Les données admin ne sont accessibles qu'aux profils admin+
- Le champ "status" n'est modifiable que par les profils adminplus+
- Tout le monde peut modifier un matériel **VALIDATED** (user ne peut modifier que ses matériels, resp ne peut modifier que les matériels de son groupe thématique ou métier), **MAIS PAS certains champs** qui sont **readonly** (sur_categorie_id', 'categorie_id', 'materiel_administratif', 'materiel_technique', 'date_acquisition', 'nom_responsable', 'fournisseur', 'organisme', 'prix_ht')
- Les seuls champs qu'on peut éditer sont donc : (designation, sous_categorie, materiel_administratif, materiel_technique, description, etiquette, lieu_stockage, lieu_detail, numero_serie, groupes_thematique, groupes_metier),
- Seuls les profils **adminplus+** peuvent modifier un matériel **TOBEARCHIVED, ou ARCHIVED** mais **UNIQUEMENT le champ "status"** (pour pouvoir rétrograder à CREATED ou VALIDATED)
- Le seul moyen de modifier **COMPLÈTEMENT** un matériel **VALIDATED, TOBEARCHIVED, ou ARCHIVED**, c'est de **changer son statut**, en le rétrogradant à **CREATED** (seuls les profils adminplus+ peuvent le faire)

(2) **Désarchiver** : consiste à rétrograder un matériel **ARCHIVED** ou **TOBEARCHIVED** dans le statut **VALIDATED** ou **CREATED** (adminplus+ only) ; utile en cas d'erreur

(3) **Montée de statut groupée** : seul **ADMIN** peut (exporter tout ou partie de la liste des matériels, et) **augmenter (+1) le statut d'un groupe de matériels**, depuis la vue « index » (vue spéciale pour ADMIN, avec des cases à cocher et boutons pour exporter ou faire évoluer le statut)

(4) **Edition des documents :**

- Admission : quand on "VALIDE" un matériel "CREATED", le statut passe en **VALIDATED** et le document d'admission est automatiquement édité
- Sortie : quand on "ARCHIVE" un document "TOBEARCHIVED", le statut passe en **ARCHIVED** et le document de sortie est automatiquement édité
- De plus :
 - Bouton "Doc admission" affiché à partir du statut "VALIDATED"
 - Bouton "Doc Sortie" affiché à partir du statut **TOBEARCHIVED** (et donc aussi pour **ARCHIVED**)
- Enfin, Le doc de sortie doit être couplée avec la liste des matériels a archiver (**TOBEARCHIVED**) quand il y a une demande de sortie.

C - sur les différentes VUES liées au matériel

Page accueil :

Administration & Administration Plus voit un menu avec 2 options :

- « Voir les matériels à valider »
- « Voir les matériels à sortir de l'inventaire »

Responsable voit un menu avec 3 options :

- « Voir les matériels de mon groupe métier »
- « Voir les matériels de mon groupe métier à valider »
- « Voir les suivis des matériels donc je suis responsable »

Page Outils :

User n'a pas accès à cette page

Les autres ont quelques options

superadmin a ces options en plus :

- Configuration générale de l'application
- Gérer les utilisateurs privilégiés
- Passer en mode debug
- Passer en mode install

Vue materiel/index (liste) : limiter aux **matériels actifs** (non archivés)

- Admin+ voit des boutons pour filtrer par « tous », « à valider », « validés », « à sortir », « archivés »

Vue materiel/find : limiter aux **matériels actifs** (non archivés)

Seul les profils Admin+ voit TOUS les matériels (y-compris archivés)

Vue materiel/view :

boutons « Imprimer Etiquettes » : resp+

Vue materiel/edit :

- Etiquette O/N (admin+)
- Statut (superadmin+)
- Informations administratives (admin+)

D - sur un SUIVI et un EMPRUNT

- Dans tous les cas, on ne doit pas pouvoir emprunter ou suivre un materiel non validé (CREATED)
- User a les droits C, R, U (si créateur), D (si créateur)
- Resp+ a les droits C, R, U, D

Un USER peut modifier/supprimer un emprunt dont il est soit le créateur soit l'emprunteur.

Un USER qui créé un emprunt ne doit pas pouvoir changer le nom de l'emprunteur (par défaut, c'est lui). Ainsi, il pourra modifier/supprimer cette fiche au besoin plus tard. Par défaut donc, pour un user, emprunt.emprunteur=creator, materiel.responsable=creator

Tout le monde peut rechercher un suivi,

E - sur les UTILISATEURS

Par défaut, superadmin a tous les droits, et les autres profils n'ont que le droit de lecture (**view** et **index**)

F - sur tous les autres objets métiers

Voici la liste des autres objets métiers :

- Catégories (et domaines et sous-catégories)
- Groupes thématiques
- Groupes métiers

Par défaut, pour tous ces objets, superadmin a tous les droits, adminplus a tous les droits sauf « delete », et les autres profils n'ont que le droit de lecture (**view** et **index**)