Gestion des profils de sécurité : droits d'accès et d'actions

Console d'administration

Table des matières

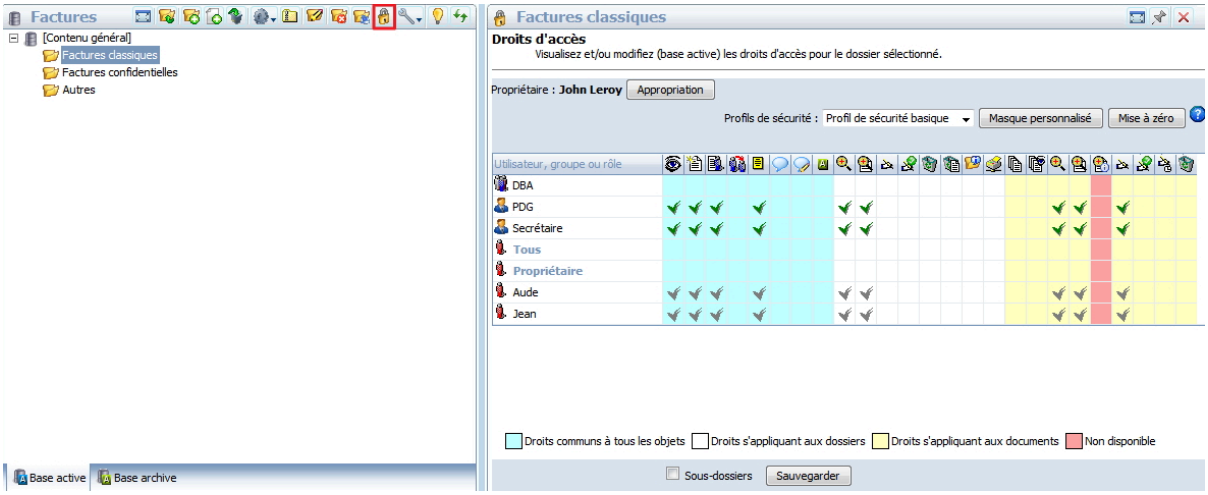
Généralités - Droits d'accès aux ressources documentaires Gargantua

Comment les droits d'accès aux ressources documentaires sont-ils gérés dans Gargantua ?

Avec Gargantua, il est possible de définir très finement quelles opérations chaque utilisateur, groupe ou rôle est autorisé à effectuer sur chaque ressource documentaire (c'est-à-dire sur chaque dossier, document, agrafe, instance de processus...). Par exemple, un utilisateur peut être autorisé ou non à créer, à archiver ou à supprimer un dossier ou un document, à modifier ses attributs, à changer son formulaire, à l'annoter, etc...

L'attribution des droits d'accès sur les ressources documentaires s'effectue par le biais du Client web, en cliquant sur l'icône (**Droits d'accès**) dans la barre d'outils.

On accède à un écran permettant d'affecter des profils de sécurité à l'objet sélectionné (voir procédures détaillées ci-dessous) :

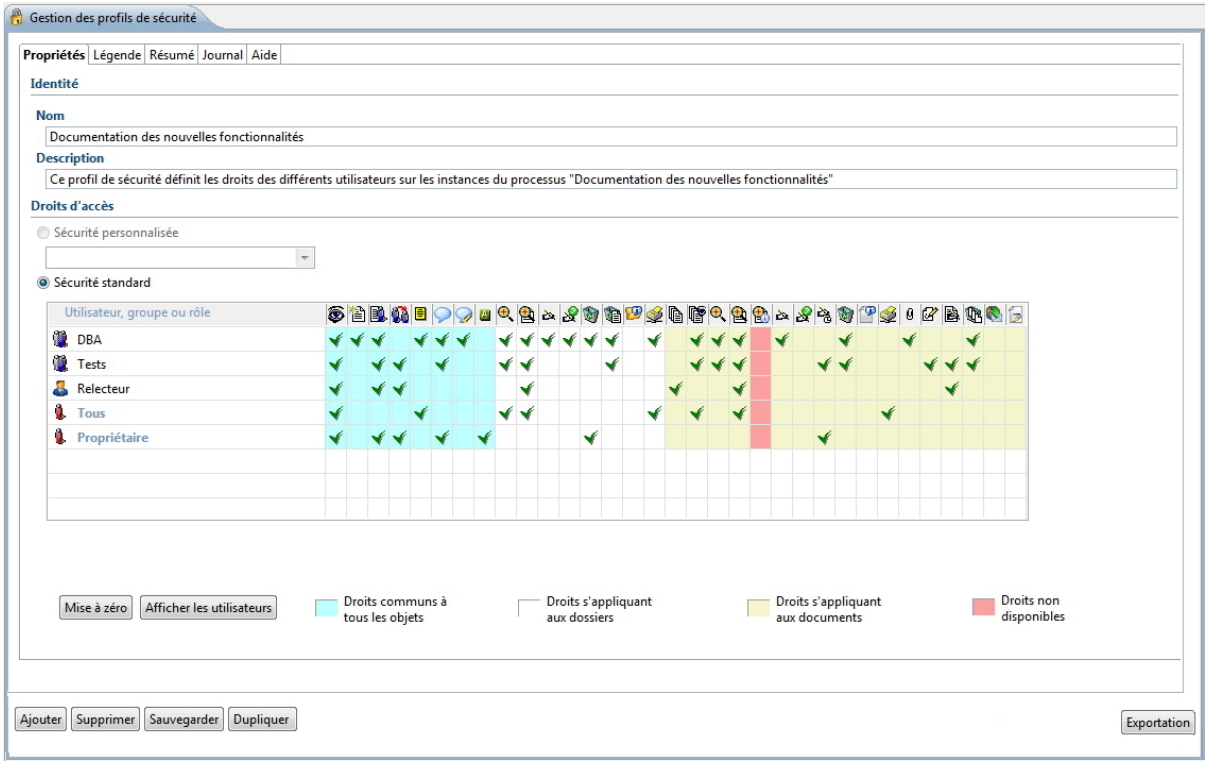


> ***Pour utiliser l'outil « Droits d'accès » , il faut ou bien faire partie du groupe DBA, ou bien posséder le droit « Modifier les droits d'accès » sur l'objet courant.***
>
> ***Les membres du groupe DBA peuvent toujours modifier les droits d'accès, même lorsque la case correspondante est décochée.***

Qu'est-ce qu'un profil de sécurité ?

Un profil de sécurité est un **ensemble prédéfini de droits d'accès**, qu'un administrateur crée au niveau de

l'Outil d'administration, afin de pouvoir ensuite l'affecter aux ressources documentaires de la base GARGANTUA concernée :



Il est intéressant de définir des profils de sécurité dès lors que l'on souhaite mettre en place une politique d'accès cohérente pour des séries de ressources documentaires similaires. En effet, les profils de sécurité :

- Évitent d'avoir à cocher à nouveau toutes les cases à chaque fois qu'on souhaite attribuer les mêmes droits d'accès à une nouvelle ressource documentaire;
- Permettent de modifier les droits d'accès sur une série de ressources documentaires en un seul clic, sans avoir à changer les permissions ressource par ressource : les changements effectués sur un profil de sécurité dans l'Outil d'administration sont en effet répercutés automatiquement sur toutes les ressources auxquelles ce profil est affecté.

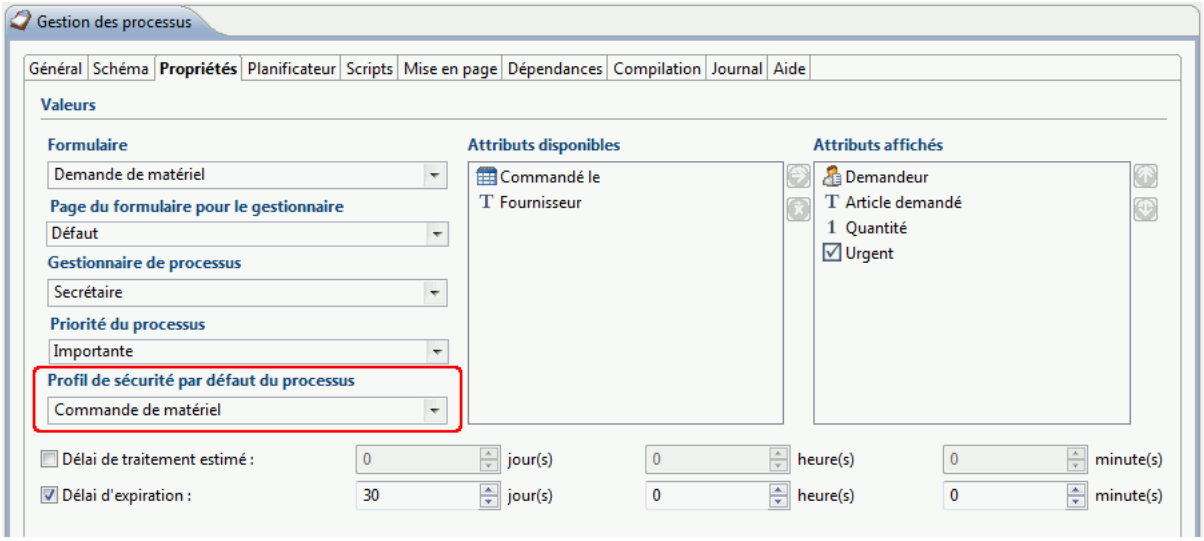
HÉRITAGE EN CASCADE DES DROITS D'ACCÈS

Le principe de l'héritage en cascade s'applique pour les droits d'accès et profils de sécurité, dans le cas des ressources documentaires qui viennent d'être créées et/ou des ressources documentaires qui ne peuvent pas posséder de droits d'accès propres (voir Droits d'accès et niveaux de sécurité des bases).

Cela signifie que :

- Les dossiers héritent par défaut des droits d'accès de la base.
- Les sous-dossiers héritent par défaut des droits d'accès du dossier parent.
- Les documents héritent par défaut des droits d'accès du dossier ou de l'instance de processus parents.

- Les instances de processus héritent des droits d'accès de la base, à moins qu'un profil de sécurité par défaut n'ait été attribué au processus.



Si vous copiez-collez un document à l'intérieur d'une base à l'aide de l'outil , la copie héritera par défaut des droits d'accès de son nouveau parent.

À quoi sert l'attribut système « Profil de sécurité » ?

Un attribut système **Profil de sécurité** peut être ajouté aux formulaires GARGANTUA depuis l'onglet **Contenu** de leur écran de gestion.

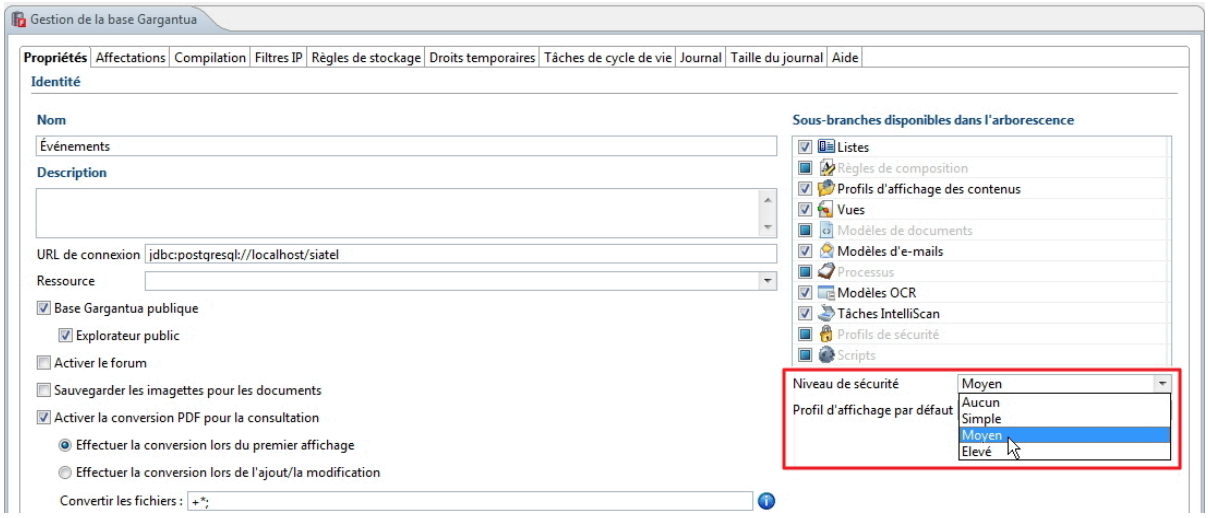
Cet attribut apparaît ensuite en lecture seule lorsque l'on affiche le formulaire d'une ressource documentaire. Il permet alors de savoir si un profil de sécurité a été appliqué et, si oui, lequel, même si l'on ne bénéficie pas de la permission **Modifier les droits d'accès** .

Droits d'accès et niveaux de sécurité des bases

La granularité des droits d'accès dépend du niveau de sécurité choisi pour la base GARGANTUA concernée :

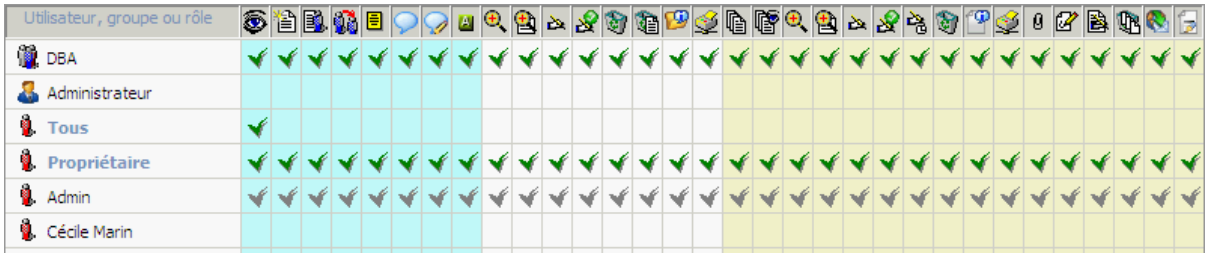
- Si la base est sans sécurité (niveau de sécurité **Aucun**), l'outil **Droits d'accès** n'apparaît pas dans le Client web : tous les utilisateurs ayant accès au contenu de la base peuvent effectuer toutes les opérations sur toutes les ressources documentaires (dans la limite des privilèges dont ils disposent).
- Si la base a un niveau de sécurité **Simple**, il est possible de définir des droits d'accès au niveau de la base : ces permissions s'appliquent à toutes les ressources documentaires contenues dans la base.
- Si la base a un niveau de sécurité **Moyen**, il est possible de définir des droits d'accès au niveau des dossiers et des processus : ces permissions s'appliquent automatiquement aux documents contenus dans ces derniers.

- Si la base a un niveau de sécurité **Élevé**, il est possible de définir des droits d'accès spécifiques pour chaque ressource documentaire, y compris pour les documents.



Lorsqu'un niveau de sécurité **Simple**, **Moyen** ou **Élevé** est appliqué à une base (soit à sa création, soit plus tard), celle-ci reçoit par défaut les droits d'accès suivants :

- Les membres du groupe DBA et le propriétaire de l'objet possèdent tous les droits.
- Les autres utilisateurs reçoivent uniquement le droit de voir que les objets existent ; ils ne peuvent effectuer aucune opération.



Définir un nouveau profil de sécurité

Pour créer un nouveau profil de sécurité, procédez comme suit :

1. Dans l'onglet « Navigation » du bandeau gauche de l'Outil d'administration, cliquez sur le serveur hébergeant votre base documentaire.
2. Utilisez le bouton « Connexion » pour saisir votre compte administrateur dans la popup prévue à cet effet. L'arborescence des rubriques que vous êtes autorisé à administrer s'ouvre.
3. Repérez la rubrique « Bases GARGANTUA » et cliquez sur la flèche **>** pour déployer la liste des bases documentaires installées.
4. Repérez la base documentaire sur laquelle vous souhaitez gérer les profils de sécurité et cliquez sur la flèche **>** pour déployer la liste des différentes rubriques d'administration de cette base.
5. Cliquez sur la rubrique **Profils de sécurité**.

   La liste des profils de sécurité de la base s'affiche dans le volet droit.

6. En bas à gauche du volet droit, cliquez sur le bouton **Ajouter**.

   Le volet « Gestion des profils de sécurité » s'ouvre par défaut sur l'onglet « Propriétés » pour vous permettre de définir le nouveau profil de sécurité.

7. Sous la rubrique **Identité**, renseignez les champs **Nom** et **Description** du profil.
8. Attribuez les droits appropriés aux utilisateurs, groupes et/ou rôles en cliquant dans les cases correspondantes du tableau **Droits d'accès**.

   Vous pouvez cocher toutes les cases d'une ligne en une seule manipulation en double-cliquant sur la case contenant le nom de l'utilisateur, groupe ou rôle. (Double-cliquez à nouveau pour décocher toutes les cases.)

   Si vous ne cochez aucune case, l'ensemble des utilisateurs recevra tous les droits.

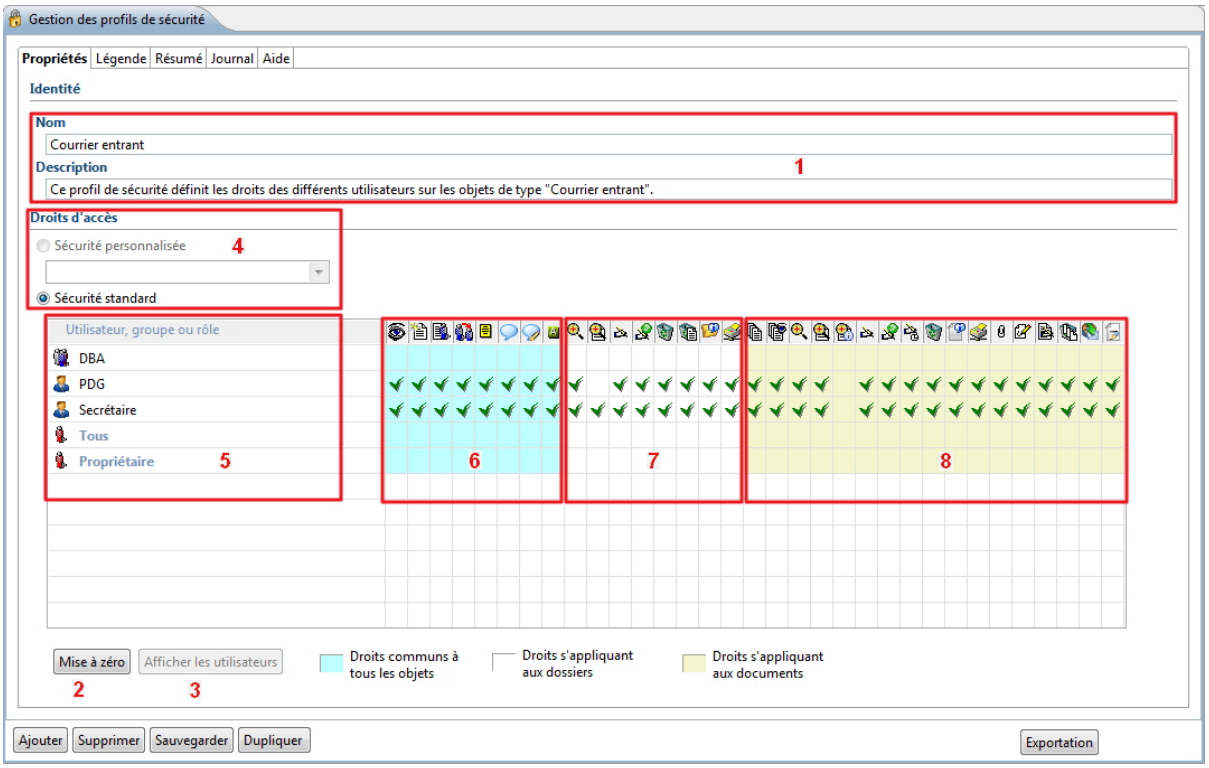
9. Lorsque vous avez terminé, cliquez sur le bouton **Sauvegarder**.

   Le nouveau profil de sécurité a bien été sauvegardé : il peut maintenant être affecté à des ressources documentaires par le biais du Client web.

Volet de gestion d'un profil de sécurité

Structure globale

Le volet de gestion des profils de sécurité se présente de la façon suivante :



1. Champs contenant les informations de base du profil de sécurité courant (nom et description) ;
2. Bouton **Mise à zéro** permettant d'effacer toutes les coches du profil en un clic, de manière à repartir d'un tableau entièrement vide ;
3. Bouton **Afficher les utilisateurs** permettant de lister les utilisateurs individuels (en plus des groupes, rôles...) dans le tableau de définition des droits d'accès, afin de leur attribuer des permissions spécifiques ;
4. Boutons radio permettant de choisir entre un profil de sécurité standard et un profil de sécurité personnalisé (uniquement disponible si des développements personnalisés pour les profils de sécurité ont été fournis par SIATEL) ;
5. Colonne contenant les noms des groupes, des rôles et - si vous avez cliqué sur le bouton **Afficher les utilisateurs** - des utilisateurs affectés à la base ; la ligne **Tous** permet d'affecter un ensemble de droits d'accès à tous les utilisateurs sans distinction, tandis que la ligne **Propriétaire** correspond au créateur de la ressource documentaire (à moins que la propriété de la ressource documentaire n'ait été transférée à un autre utilisateur) ;
6. Colonnes correspondant aux droits d'accès valables pour toutes les ressources documentaires, que le

profil de sécurité soit appliqué à un dossier, à un processus, à un document, etc.

7. Colonnes correspondant aux droits d'accès valables si le profil de sécurité est appliqué à un dossier ou à un processus ;
8. Colonnes correspondant aux droits d'accès valables si le profil de sécurité est appliqué à un document ou à une agrafe.

DROITS D'ACCÈS S'APPLIQUANT À TOUTES LES RESSOURCES DOCUMENTAIRES

Les droits d'accès s'appliquant à tous les types de ressources documentaires sont les suivants :

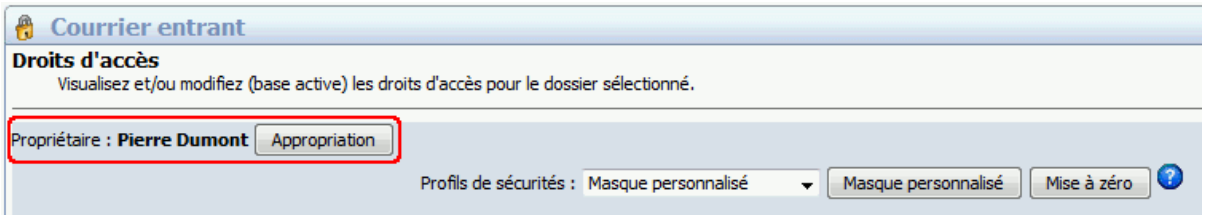
- **Voir que l'objet existe** : Les utilisateurs détenteurs de ce droit peuvent voir le nom et l'emplacement de la ressource documentaire concernée dans le plan de classement, dans la liste des documents ou dans les résultats de recherche, mais ils ne peuvent effectuer aucune autre opération.

  > ***Les membres du groupe DBA peuvent toujours voir qu'un objet existe, même si la case correspondante est décochée.***

- **Créer des objets** : Les utilisateurs détenteurs de ce droit peuvent créer des dossiers ou des documents à l'intérieur de l'objet courant.
- **Modifier les droits d'accès** : Les utilisateurs détenteurs de ce droit sont autorisés à modifier les permissions d'accès à l'objet courant à l'aide de l'outil (**Droits d'accès**).

  > ***Les membres du groupe DBA peuvent toujours modifier les droits d'accès à un objet, même si la case correspondante est décochée.***

- **S'approprier l'objet** : Les utilisateurs détenteurs de ce droit peuvent s'approprier l'objet courant, s'il a été créé par un autre utilisateur. Cette opération s'effectue en cliquant sur le bouton **Appropriation** situé en haut à gauche du cadre de modification des droits d'accès :



  > ***Les utilisateurs autorisés à s'approprier un objet ne peuvent exercer ce droit que s'ils reçoivent également la permission « Modifier les droits d'accès ».***

- **Ajouter une note** : Les utilisateurs détenteurs de ce droit peuvent utiliser l'outil pour ajouter des

notes ou une fiche commentaire au document ou au dossier courant. Ils peuvent également visualiser l'ensemble des notes attachées au document concerné.

> ***Pour visualiser la fiche commentaire existante d'un dossier (en cliquant à nouveau sur l'outil), les utilisateurs doivent également disposer du droit « Voir les attributs du dossier » . Pour modifier la fiche, ils doivent aussi disposer du droit « Modifier les attributs du dossier » .***
>
> ***Pour modifier une note attachée au document courant, les utilisateurs doivent également disposer des droits « Voir les attributs du document » et « Modifier les attributs du document » .***

- **Accéder au forum** : Les utilisateurs détenteurs de ce droit peuvent lire les discussions du forum à propos de l'objet courant.
- **Poster sur le forum** : Les utilisateurs détenteurs de ce droit peuvent poster des messages sur le forum à propos de l'objet courant.
- **Archiver** : Les utilisateurs détenteurs de ce droit peuvent utiliser l'outil **Déplacer vers la base archive** pour transférer l'objet courant de la base active vers la base archive.

> ***Si un utilisateur est autorisé à archiver un dossier ou une agrafe, il pourra également archiver le contenu de ces derniers, quels que soient les droits définis pour chacun des objets enfants.***

Droits d'accès s'appliquant uniquement aux dossiers et processus

Les droits d'accès s'appliquant uniquement aux dossiers et processus sont les suivants :

- **Voir les attributs du dossier** : Les utilisateurs détenteurs de ce droit peuvent afficher le formulaire du dossier ou du processus courant et en visualiser les attributs en lecture seule.
- **Visualiser le contenu des fichiers** : Les utilisateurs détenteurs de ce droit peuvent voir le contenu des fichiers contenus dans le dossier ou dans le processus courant, à condition, dans le cas d'une base à niveau de sécurité **Élevé**, de détenir également le droit **Visualiser le contenu du fichier** pour chacun des documents.
- **Modifier les attributs du dossier** : Les utilisateurs détenteurs de ce droit peuvent modifier les attributs de formulaire du dossier ou du processus courant (à condition de posséder également le droit **Voir les attributs du dossier**).
- **Changer le formulaire du dossier** : Les utilisateurs détenteurs de ce droit peuvent changer le type du dossier courant en sélectionnant un nouveau formulaire à l'aide de la liste déroulante **Sélectionner un formulaire**.

> ***Attention, cette opération entraîne la perte des données associées aux attributs qui ne figurent plus dans le nouveau formulaire. En outre, les utilisateurs ne peuvent l'effectuer que s'ils possèdent également les droits « Voir les attributs du dossier » et « Modifier les attributs du dossier ».***

- **Supprimer le dossier** : Les utilisateurs détenteurs de ce droit peuvent supprimer le dossier courant à l'aide de l'outil (**Supprimer le dossier sélectionné**). Attention, ce droit permet de supprimer non seulement le dossier, mais aussi son contenu, quels que soient les droits qui s'appliquent à chacun des objets-fils.
- **Supprimer le contenu du dossier** : Les utilisateurs détenteurs de ce droit peuvent supprimer les documents contenus dans le dossier courant, à condition, dans le cas d'une base à niveau de sécurité **Élevé**, de posséder également le droit **Supprimer le document** pour chacun des documents.
- **Voir le journal du dossier** : Les utilisateurs détenteurs de ce droit peuvent voir le journal du dossier ou du processus courant en cliquant sur l'outil **Afficher le journal du dossier sélectionné** (dans l'Explorateur), ou sur l'outil **Afficher le journal de l'objet sélectionné** (dans les recherches).
- **Imprimer le contenu du dossier** : Les utilisateurs détenteurs de ce droit peuvent imprimer les documents contenus dans le dossier courant, à condition de posséder également le droit **Visualiser le contenu des fichiers** et, dans le cas d'une base à niveau de sécurité **Élevé**, les droits **Imprimer le document** et **Visualiser le contenu du fichier** pour chacun des documents.

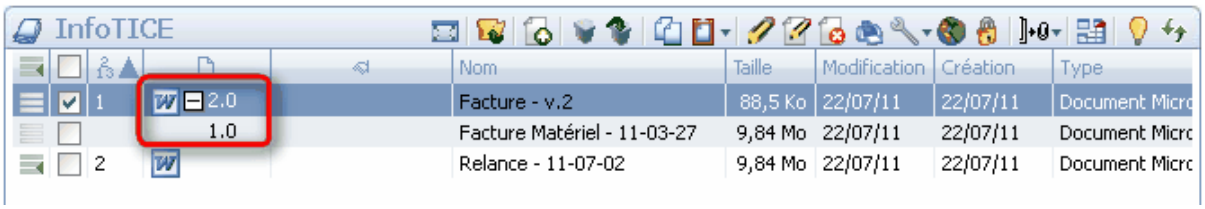
Droits d'accès s'appliquant uniquement aux documents

Les droits d'accès s'appliquant uniquement aux documents sont les suivants :

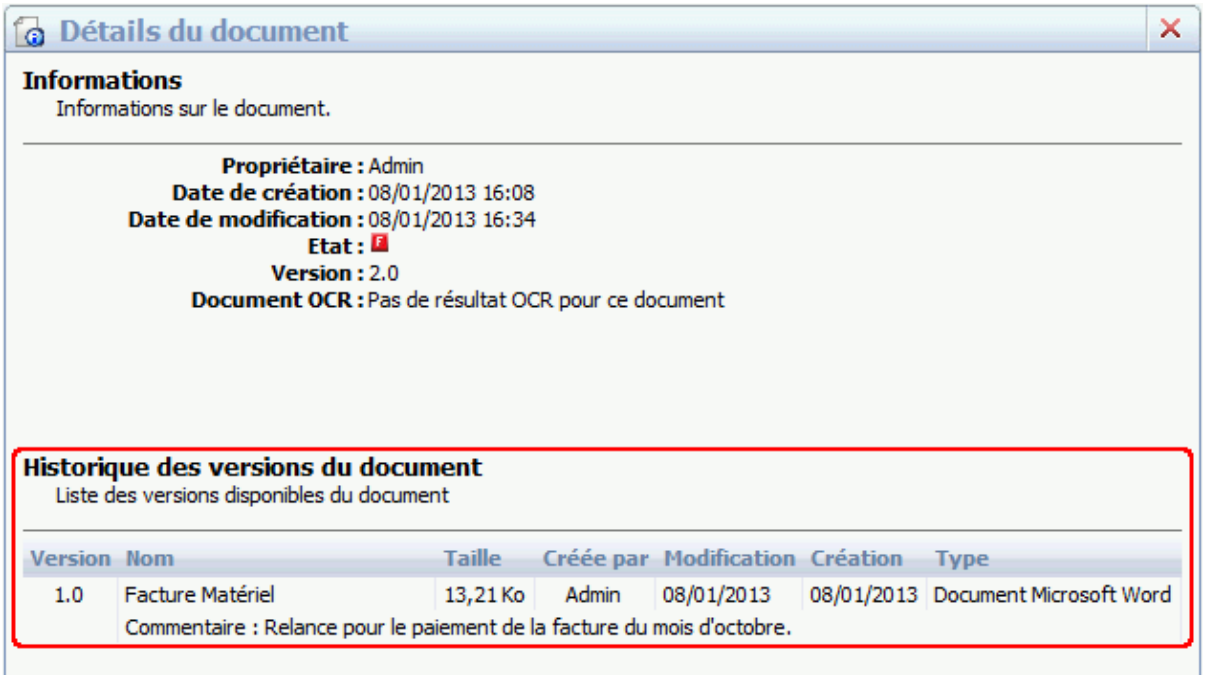
- **Créer une nouvelle version du document** : Les utilisateurs détenteurs de ce droit peuvent télécharger un nouveau fichier et décider s'ils souhaitent remplacer le document courant ou bien en créer une nouvelle version, majeure ou mineure. En l'absence d'autres permissions complémentaires, ils ne peuvent ni télécharger le fichier actuel, ni verrouiller le document, ni voir ses versions antérieures.

> ***Les utilisateurs autorisés à créer une nouvelle version du document ne peuvent exercer ce droit que s'ils reçoivent également les droits « Visualiser le contenu du fichier » et « Modifier le document », ainsi que « Visualiser le contenu des fichiers » au niveau du dossier parent.***

- **Voir les versions du document** : Les utilisateurs détenteurs de ce droit peuvent voir les versions antérieures du document courant dans la liste des documents :



Ils peuvent également accéder à l'historique des versions du document à l'aide de l'outil (**Afficher les infos sur le document sélectionné**) du Client web :



- **Voir les attributs du document** : Les utilisateurs détenteurs de ce droit peuvent afficher le formulaire du document courant et en visualiser les attributs en lecture seule.
- **Visualiser le contenu du fichier** : Les utilisateurs détenteurs de ce droit peuvent voir le contenu du fichier associé au document courant, à condition de posséder également le droit **Visualiser le contenu des fichiers** au niveau du dossier parent.
- **Afficher le fichier source** :
  - Si la conversion PDF pour la consultation est activée sur la base GARGANTUA, le droit **Afficher le fichier source** est modifiable. Les utilisateurs détenteurs de ce droit peuvent consulter la version source d'un document, en mode plugin ActiveX (en plus des versions HTML et PDF), à condition de posséder également le droit **Visualiser le contenu des fichiers** sur le document et sur le dossier parent.
  - Si la conversion PDF pour la consultation est désactivée sur la base GARGANTUA, le droit **Afficher le fichier source** n'est pas modifiable : la colonne correspondante s'affiche en rouge. La version PDF des documents étant indisponible, les utilisateurs disposent toujours de l'accès à la version source, en mode plugin ActiveX.

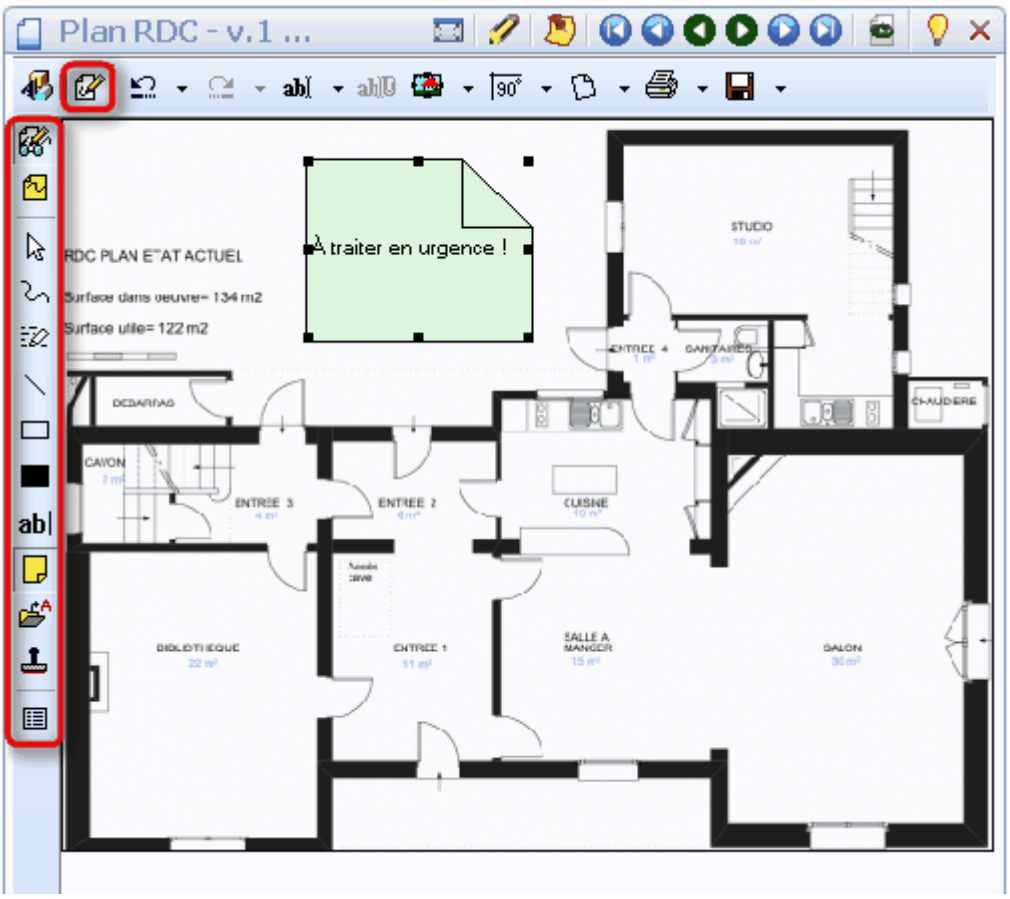
- **Modifier les attributs du document** : Les utilisateurs détenteurs de ce droit peuvent modifier les attributs de formulaire du document courant (à condition de posséder également le droit **Voir les attributs du document**).
- **Changer le formulaire du document** : Les utilisateurs détenteurs de ce droit peuvent changer le type du document courant en sélectionnant un nouveau formulaire.

> ***Attention, cette opération entraîne la perte des données associées aux attributs qui ne figurent plus dans le nouveau formulaire.***
>
> ***En outre, les utilisateurs ne peuvent l'effectuer que s'ils possèdent également les droits « Voir les attributs du document » et « Modifier les attributs du document ».***

- **Bénéficier des droits temporaires** : Les utilisateurs détenteurs de ce droit peuvent apporter des modifications pendant un délai fixé à compter de la création de l'objet.
- **Supprimer le document** : Les utilisateurs détenteurs de ce droit peuvent supprimer le document courant, à condition de posséder également le droit **Supprimer le contenu du dossier** au niveau du dossier parent.
- **Voir le journal du document** : Les utilisateurs détenteurs de ce droit peuvent voir le journal du document courant en cliquant sur l'outil (**Afficher le journal du document** / **de l'objet sélectionné**).
- **Imprimer le document** : Les utilisateurs détenteurs de ce droit peuvent imprimer le document courant, à condition de posséder également le droit **Visualiser le contenu du fichier** et les droits **Imprimer le contenu du dossier** et **Visualiser le contenu des fichiers** au niveau du dossier parent.
- **Agrafer** : Les utilisateurs détenteurs de ce droit peuvent créer et supprimer des agrafes contenant les documents concernés. Ils doivent posséder ce droit pour tous les documents de l'agrafe.

> ***Les utilisateurs autorisés à agrafer des documents ne peuvent exercer ce droit que s'ils reçoivent également le droit « Créer des objets » au niveau du dossier parent.***

- **Annoter** : Les utilisateurs détenteurs de ce droit peuvent utiliser la barre d'outils **Annotations** du plugin ActiveX pour éditer le fichier .tif associé au document courant :



> ***Les utilisateurs autorisés à annoter le document ne peuvent exercer ce droit que si : ils peuvent également utiliser le plugin ActiveX ; ils détiennent les droits « Visualiser le contenu du fichier » et « Modifier le document », ainsi que le droit « Visualiser le contenu des fichiers » au niveau du dossier parent.***

- **Modifier le document** : Les utilisateurs détenteurs de ce droit peuvent télécharger un nouveau fichier afin de remplacer le document courant ; ils peuvent également utiliser les outils d'édition d'images du plugin ActiveX. En l'absence d'autres permissions complémentaires, ils ne peuvent ni télécharger le fichier actuel, ni verrouiller le document, ni en créer une nouvelle version.

> ***Les utilisateurs autorisés à modifier le document ne peuvent exercer ce droit que s'ils reçoivent également la permission de « Visualiser le contenu du fichier », ainsi que le droit « Visualiser le contenu des fichiers » au niveau du dossier parent.***

- **Supprimer une version du document** : Les utilisateurs détenteurs de ce droit peuvent supprimer des versions antérieures du document concerné à l'aide de l'outil du Client web.

> ***Les utilisateurs autorisés à supprimer des versions antérieures du document ne peuvent exercer ce droit que s'ils reçoivent également les droits « Voir les versions de document »***  ***et « Supprimer le document »***  ***, ainsi que le droit « Supprimer le contenu du dossier »***  ***au niveau du dossier parent.***

-  **Télécharger et envoyer par e-mail** : Les utilisateurs détenteurs de ce droit peuvent télécharger le document courant et/ou l'envoyer par la messagerie sous forme de pièce jointe, à condition de posséder également les droits **Visualiser le contenu du fichier**  et **Visualiser le contenu des fichiers**  au niveau du dossier parent.
-  **Apposer une signature électronique** : Les utilisateurs détenteurs de ce droit peuvent signer le document courant à l'aide d'un certificat électronique ; s'ils disposent du privilège **Signature physique**  , ils peuvent également y apposer une signature au format image.

> ***Les utilisateurs autorisés à apposer une signature électronique au document ne peuvent exercer ce droit que s'ils reçoivent également les droits « Visualiser le contenu du fichier »***  ***et « Modifier le document », ainsi que le droit « Visualiser le contenu des fichiers »***  ***au niveau du dossier parent.***

-  **Démarrer un cycle de validation** : Les utilisateurs détenteurs de ce droit peuvent démarrer un cycle de validation et/ou afficher son avancement, à l'aide de l'outil  du Client Web.

Gestion des profils de sécurité

Dupliquer un profil de sécurité

1. Dans le volet gauche de l'Outil d'administration, déployez la rubrique correspondant à la base GARGANTUA de votre choix.
2. Cliquez sur la sous-rubrique **Profils de sécurité**.

   La liste des profils de sécurité de la base s'affiche dans le volet droit.

3. Dans la liste, cliquez sur la ligne correspondant au profil de sécurité que vous souhaitez dupliquer.
4. En bas à gauche du volet droit, cliquez sur le bouton **Dupliquer**.

   Un nouveau profil de sécurité, portant le nom du profil dupliqué suffixé par **(1)**, apparaît en bas de la liste.

5. Cliquez sur le nom du nouveau profil.

   L'écran de définition du profil s'affiche.

6. Après avoir effectué les modifications nécessaires, cliquez sur le bouton **Sauvegarder** en bas du volet droit.

   Un nouveau profil fondé sur un profil existant a bien été créé.

Exporter un profil de sécurité

Pour exporter un profil de sécurité, procédez comme suit :

1. Dans le volet gauche de l'Outil d'administration, déployez la rubrique correspondant à la base GARGANTUA de votre choix.
2. Cliquez sur la sous-rubrique **Profils de sécurité**.

   La liste des profils de sécurité de la base s'affiche dans le volet droit.

3. Dans la liste, cliquez sur la ligne correspondant au profil de sécurité que vous souhaitez exporter.
4. En bas à droite du volet droit, cliquez sur le bouton **Exportation**.

   La boîte de dialogue **Objets à exporter** s'affiche.

5. Cochez la case correspondant au profil de sécurité à exporter, puis cliquez sur **OK**.

   L'explorateur de fichiers s'affiche.

6. Naviguez vers l'emplacement où vous souhaitez enregistrer l'export au format .sxa du profil, puis cliquez sur **Enregistrer**.

Un message de confirmation s'affiche.

7. Cliquez sur **OK**.

   L'export du profil de sécurité sélectionné a bien été réalisé. Vous pouvez maintenant le réimporter dans toute autre base de votre choix.

Importer un profil de sécurité

Pour importer un profil de sécurité, procédez comme suit :

1. Dans le volet gauche de l'Outil d'administration, déployez la rubrique correspondant à la base GARGANTUA de votre choix.
2. Cliquez sur la sous-rubrique **Profils de sécurité**.

   La liste des profils de sécurité de la base s'affiche dans le volet droit.

3. En bas à droite du volet droit, cliquez sur le bouton **Importation**.

   L'explorateur de fichiers s'affiche.

4. Naviguez vers l'emplacement où l'export du profil au format .sxa est stocké, sélectionnez-le, puis cliquez sur **Ouvrir**.

   La boîte de dialogue **Objets à importer** s'affiche.

5. Cochez la case correspondant au profil de sécurité à importer.

   > ***Contrairement aux autres objets, les profils de sécurité que vous importez ne peuvent pas remplacer des profils déjà présents dans la base qui auraient le même nom, même si vous cochez la case « Remplacer les éléments portant le même nom ».***

6. Lorsque vous avez terminé, cliquez sur **OK**.

   Un message de confirmation s'affiche.

7. Cliquez sur **OK**.

   Le profil de sécurité a bien été importé : il se trouve en bas de la liste des profils de sécurité de la base.

Supprimer un profil de sécurité

Pour supprimer un profil de sécurité, procédez comme suit :

1. Dans le volet gauche de l'Outil d'administration, déployez la rubrique correspondant à la base GARGANTUA de votre choix.
2. Cliquez sur la sous-rubrique **Profils de sécurité**.

La liste des profils de sécurité de la base s'affiche dans le volet droit.

3. Dans la liste, cliquez sur la ligne correspondant au profil de sécurité que vous souhaitez supprimer.
4. En bas à gauche du volet droit, cliquez sur le bouton **Supprimer**.

   Un message de confirmation s'affiche.

5. Cliquez sur **Oui**.

   Le profil de sécurité a bien été supprimé : il n'apparaît plus dans la liste des profils de sécurité de la base.

Il est impossible de supprimer un profil de sécurité si celui-ci est actuellement affecté à des ressources documentaires.

Affecter un profil de sécurité à une ressource documentaire depuis l'interface utilisateur Gargantua

L'affectation d'un profil de sécurité à une ressource documentaire depuis l'interface utilisateur Gargantua nécessite l'existence, au préalable, de ce profil de sécurité. Si ce profil de sécurité n'existe pas, il convient de procéder à la création de ce profil de sécurité dans l'Outil d'administration.

Pour affecter un profil de sécurité à un dossier, un processus, un document, ou encore à l'ensemble des objets d'une base, procédez comme suit :

1. Dans l'interface utilisateur Gargantua, positionnez-vous sur la ressource documentaire à laquelle vous souhaitez affecter le profil de sécurité.
2. Dans la barre de commandes, repérez l'icône « Outils ». Les différents outils proposés s'affichent, dont l'outil « Droits d'accès ». Cliquez sur l'icône  (**Droits d'accès**).

   La popup de modification des droits d'accès s'ouvre.

3. Dans la liste du champ **Profils de sécurité**, cliquez sur le profil de sécurité de votre choix, pour l'appliquer à la ressource documentaire sélectionnée.
4. Si la ressource courante contient déjà d'autres ressources et que vous souhaitez leur appliquer le même profil de sécurité, cochez les cases **Sous-dossiers** et/ou **Documents** en bas de la popup de modification des droits d'accès.
5. Cliquez sur **Sauvegarder**.

   Un message de confirmation apparaît. Le profil de sécurité a bien été appliqué à la ressource documentaire courante et, le cas échéant, à ses enfants.

Affecter un masque personnalisé à une ressource documentaire

Plutôt que d'affecter un profil de sécurité à une ressource documentaire, vous pouvez lui affecter un **masque personnalisé**.

Cette fonctionnalité est pratique dans les cas suivants :

- Si vous n'avez pas défini de profil de sécurité dans l'Outil d'administration ;
- Pour un sous-dossier ou un document : si un dossier a déjà un profil de sécurité mais que vous ne souhaitez pas l'appliquer à tous ses sous-dossiers ou documents.

> ***Attention cependant : affecter trop de masques personnalisés peut facilement entraîner des confusions. En effet, il devient difficile de savoir quels éléments sont affectés à un masque personnalisé ou à un profil de sécurité. C'est pourquoi nous recommandons de privilégier autant que possible l'utilisation des profils de sécurité.***

Pour affecter un masque personnalisé à une ressource documentaire, procédez comme suit :

1. Dans l'interface utilisateur GARGANTUA, positionnez-vous sur la ressource documentaire à laquelle vous souhaitez affecter le profil de sécurité.
2. Dans la barre de commandes, repérez l'icône « Outils » puis cliquez sur l'icône  (**Droits d'accès**).

   La popup de modification des droits d'accès s'ouvre.

3. Dans la liste du champ **Profils de sécurité**, sélectionnez **Masque personnalisé**.
4. Cochez les cases du tableau des droits d'accès, en fonction des droits que vous souhaitez affecter aux différents utilisateurs, groupes ou rôles sur cet objet.
5. Si l'objet courant contient déjà d'autres objets et que vous souhaitez leur appliquer le même masque de sécurité, cochez les cases **Sous-dossiers** et/ou **Documents** à côté du bouton **Sauvegarder** en bas du volet droit.
6. Cliquez sur **Sauvegarder**.

   Un message de confirmation s'affiche. Le masque personnalisé a bien été appliqué à l'objet courant et, le cas échéant, à ses enfants.

Affecter un masque personnalisé à une ressource documentaire à partir d'un profil de sécurité existant

Si vous souhaitez affecter un masque personnalisé à une ressource documentaire en particulier à partir d'un profil de sécurité existant, procédez comme suit :

1. Dans l'interface utilisateur GARGANTUA, positionnez-vous sur la ressource à laquelle vous souhaitez affecter le profil de sécurité.
2. Dans la barre de commandes, repérez l'icône "Outils" cliquez sur l'icône  (**Droits d'accès**).

   La popup de modification des droits d'accès s'ouvre.

3. Dans la liste du champ **Profils de sécurité**, cliquez sur le profil de sécurité de votre choix.

   Le tableau des droits d'accès se remplit en fonction du profil de sécurité choisi.

4. Cliquez sur le bouton **Masque personnalisé** : vous pouvez alors définir pour la ressource documentaire courante un profil de sécurité personnalisé fondé sur le profil sélectionné, en cochant ou décochant certains droits.

   Le message **Le modèle de sécurité sélectionné a été modifié** apparaît au-dessus du tableau.

   Attention toutefois, le profil personnalisé ne sera plus mis à jour automatiquement si le profil source est modifié via la console d'administration : les masques personnalisés peuvent être sources de complications !

   Le bouton Mise à zéro permet de repartir d'un tableau entièrement vide pour définir un nouveau profil personnalisé.

5. Si la ressource courante contient déjà d'autres ressources documentaires et que vous souhaitez leur appliquer le même masque de sécurité, cochez les cases **Sous-dossiers** et/ou **Documents** à côté du bouton **Sauvegarder** en bas du volet droit.
6. Cliquez sur **Sauvegarder**.

   Un message de confirmation s'affiche. Le masque personnalisé a bien été appliqué à la ressource courante et, le cas échéant, à ses enfants, à partir d'un profil de sécurité.