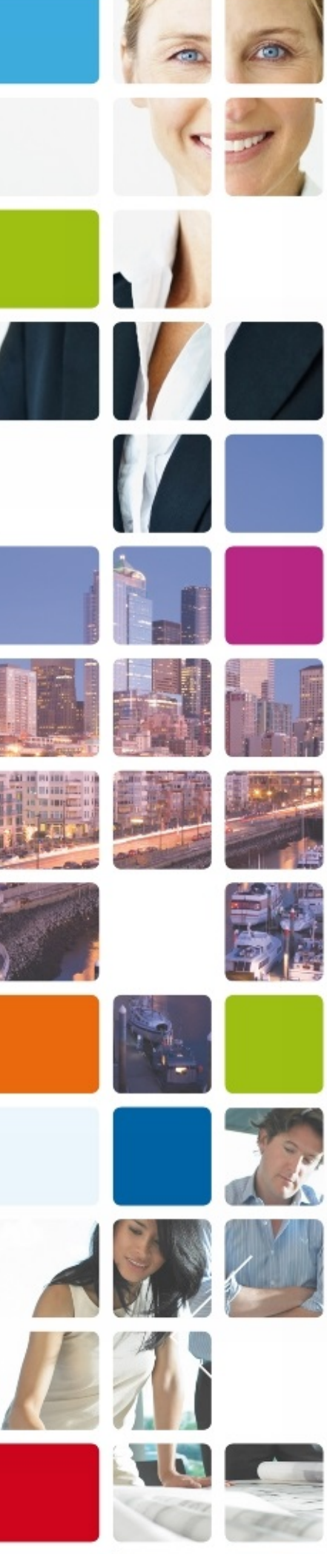


Planon Software Suite

Version: L80

Autorisation

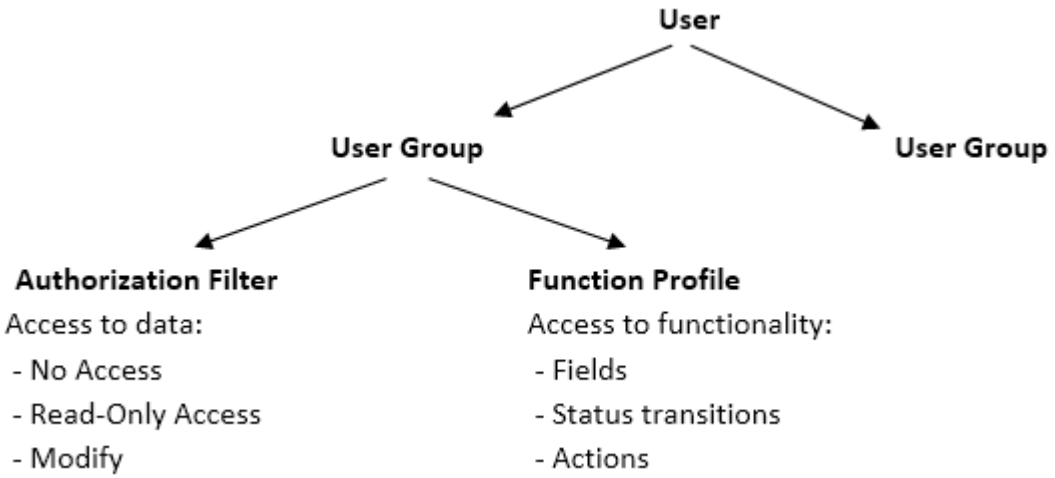
Table of Contents

A propos d’autorisation dans Planon Software Suite

L'autorisation dans Planon Software Suite est basée sur le principe de la séparation de données et de fonctionnalité. Un administrateur peut créer à cette fin :

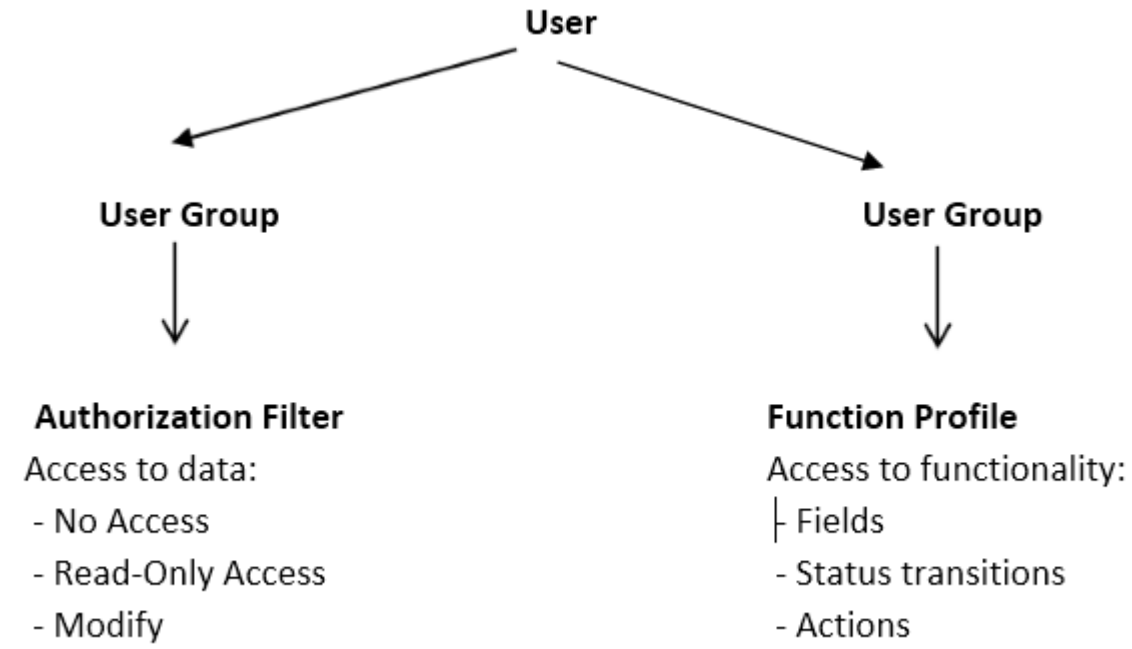
- Des groupes d’utilisateurs qui peuvent être utilisés de deux façons :
  - Pour combiner des données et l’accès fonctionnel
  - Pour séparer des données et l’accès fonctionnel
- Des profils de fonction afin de spécifier les fonctionnalités (comme des champs de données, actions et transitions d'état) qui doivent être rendues disponibles pour certains groupes d'utilisateurs.
- Des filtres d'autorisation afin de limiter l'accès de certains groupes d'utilisateurs à des données spécifiques.

  En associant un profil de fonction et des filtres d'autorisation à un groupe d'utilisateurs, vous pouvez spécifier les droits des utilisateurs appartenant à ce groupe d'utilisateurs.



Lorsque vous utilisez ce type de profil la combinaison de groupes d’utilisateurs accorde l’accès à des données spécifiques. En associant des utilisateurs à plusieurs groupes d’utilisateurs, l’accès aux données est étendu.

Ou vous pouvez également séparer l’accès fonctionnel et l’accès aux données en appliquant Division des rôles et données :



Lorsque vous utilisez ce profil la combinaison de groupes d'utilisaeurs accorde l'accès spécifique aux données. Lorsque vous utilisez des liens d'autorisation ce type de combinaison de profils restreint les possibilités comme expliqué dans Séparer l'accès aux données et l'accès fonctionnel.

Pour de plus amples informations sur les concepts utilisés dans Autorisation, reportez-vous à Autorisation - concepts.

Interaction avec d'autres groupes de navigation

Le tableau suivant montre l'interaction entre l'autorisation et d'autres parties de Planon Software Suite.

TSI	*Function*	*These settings apply to...*
Launch Center Manager	Determine which launch tasks (TSIs) the user can start from his/her launch center	- Individual user groups - Individual TSIs
TSI Manager	Per business object: determine access to fields, actions and status transitions	- Individual user groups, reports, TSIs and pop-ups
Authorization	Per business object: **Functional authorization** > determine access to fields, actions, status transitions trough function profiles **Data authorization** > determine access to data through authorization filters	- Individual user groups - For all reports, TSIs and pop-ups in a user group
FieldDefiner	Per business object: determine access to fields, actions, statuses and status transitions	- For the whole company - For all reports, TSIs and pop-ups

Planon Software Suite est fourni avec un groupe d'utilisateurs Standard. Ce groupe d'utilisateurs comprend un utilisateur ayant des droits de superviseur. Pour configurer Planon Software Suite vous devez toutefois créer et utiliser un nouveau superviseur.

Comme Planon Software Suite est un système extrêmement configurable, tout exemple, scénario, cas décrit dans cette documentation peut différer légèrement des vôtres, bien que les fonctionnalités y décrites soient les mêmes.

Pour de plus amples détails, reportez-vous à *Launch Center Manager*, *TSI Manager* et *FieldDefiner*.

Concepts d'autorisation

Pour bien comprendre le concept de l'autorisation dans Planon Software Suite, il est important de comprendre d'abord les différents concepts impliqués. Cette section décrit ces différents concepts et explique leurs interactions.

Clé d'accès

Une clé d'accès est l'URL chiffrée d'un compte qui peut être utilisé pour accorder l'accès aux fonctionnalités Planon. Les clés d'accès ont pour but de permettre à plusieurs connexions authentifiées sur le même compte d'accéder à des fonctionnalités limitées.

Filtre d'autorisation

Un filtre d'autorisation est utilisé afin de spécifier les données qu'un groupe d'utilisateurs peut consulter et sur lesquelles il peut exécuter des actions. Le même filtre d'autorisation peut être utilisé dans plusieurs groupes d'utilisateurs.

Si par exemple les groupes d'utilisateurs Sécurité, Restauration et Service Desk de la Zone nord d'un bâtiment doivent avoir accès aux mêmes données, il faut seulement associer le même filtre d'autorisation à ces différents groupes d'utilisateurs.

Business object

Un business object est un ensemble logique de fonctionnalités qui représente en général un concept du facility management (p.ex. un ordre de travail, un type de budget, etc.).

Les business objects ne sont pas autorisés par défaut. Ceci veut dire que tous les utilisateurs ont accès à tous les champs de données, toutes les actions et transitions d'état associées à un business object.

Vous pouvez autoriser un business object. Dès que vous autorisez un business object, tous les utilisateurs n'ont qu'accès en lecture seule par défaut au business object en question. Les droits d'accès aux champs de données, actions et transitions d'état peuvent alors être restreints ou étendus pour chaque groupe d'utilisateurs.

Profil de fonction

Un profil de fonction est utilisé afin de définir une certaine fonction qu'un groupe d'utilisateurs peut exercer, par exemple agent de sécurité. Il spécifie à cette fin les droits à utiliser une fonctionnalité et jamais les droits d'accès aux données!

Les profils de fonction peuvent être réutilisés : le même profil de fonction peut être utilisé à plusieurs endroits, par exemple dans différentes régions. Les droits d'accès à la fonctionnalité sont les mêmes, mais les droits d'accès aux données peuvent varier par endroit.

Un profil de fonction Sécurité, par exemple, peut être utilisé pour des agents de sécurité travaillant dans la zone nord et sud d'un complexe de bâtiments. La fonctionnalité disponible pour chaque groupe d'utilisateurs (Nord et Sud) est identique, mais les droits d'accès aux données seront différents (différentes données pour la zone nord et la zone sud).

Vous pouvez spécifier pour chaque business object quels champs, actions et transitions d'état doivent être accessibles. Planon Software Suite connaît trois niveaux d'autorisation :

- Pas d'accès au business object
- Accès en lecture seule au business object
- Le business object peut être modifié

L'accès à un business object est par défaut lecture seule. Les champs peuvent individuellement être mis sur modifiable.

Paire de clés

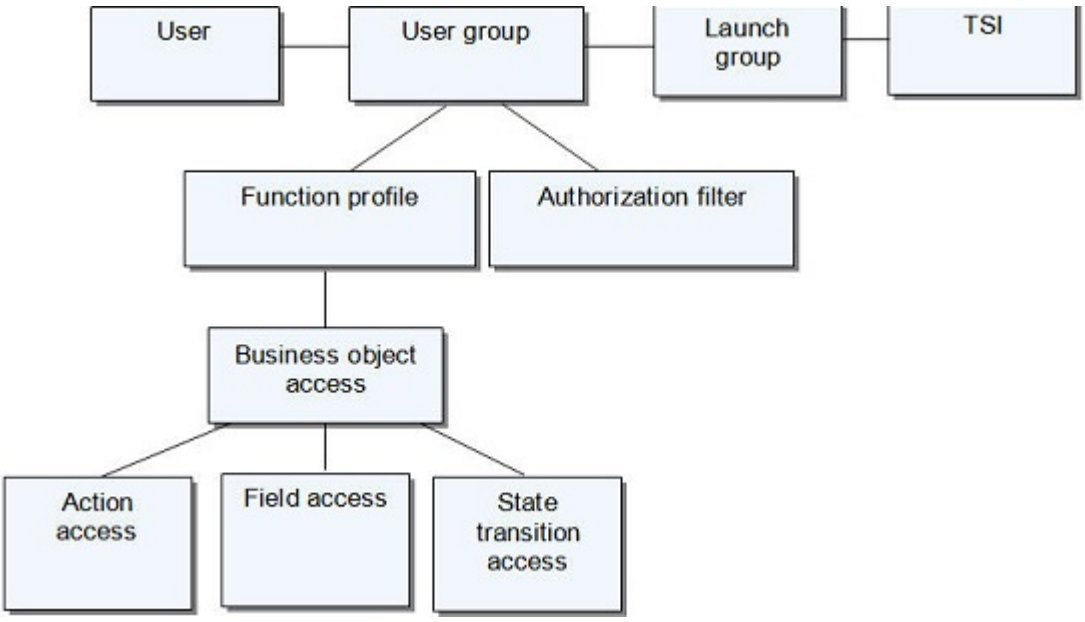
Une paire de clés est composée d'une clé privée et d'une clé publique. Ces clés sont utilisées pour chiffrer/déchiffrer la clé d'accès.

Launch groups

Les launch groups dans le Launch center sont utilisés afin de rendre les TSI disponibles par groupe d'utilisateurs, en d'autres mots : les launch groups sont indispensables pour rendre des TSI disponibles pour les utilisateurs. Un lauch group peut être associé à plusieurs groupes d'utilisateurs.

Pour de plus amples informations sur les launch groups, reportez-vous à *Launch Center Manager*.

Le diagramme suivant montre le lien entre les concepts décrits dans cette section.



Gestionnaire

Un gestionnaire est un ensemble de données comprenant des objets spécifiques (bâtiments). En fonction des autorisations de leur groupe d'utilisateurs, les utilisateurs peuvent consulter différents gestionnaires ou travailler dans différents gestionnaires. Des gestionnaires sont des business objects " autorisables " ce qui veut dire que vous pouvez donner l'autorisation à plusieurs groupes d'utilisateurs à accéder à un ou plusieurs gestionnaires et à y travailler.

TSI

Des TSI (Task Specific Interface) contiennent plusieurs business objects (prédéfinis). Les utilisateurs ont besoin de TSI afin de lire, créer et/ou modifier des business objects.

Pour de plus amples informations sur des TSI, reportez-vous à *TSI Manager*.

Utilisateur

Un utilisateur du *Planon ProCenter* fait partie d'un groupe d'utilisateurs et est lié à une personne. Les utilisateurs sont enregistrés au point **Détails groupes d'utilisateurs**. Un utilisateur peut être lié à un ou plusieurs groupes, de sorte que plusieurs droits puissent être attribués à cet utilisateur.

Des utilisateurs appartenant à plusieurs groupes d'utilisateurs peuvent accéder à tous les launch groups et profils de fonction associés à ces groupes d'utilisateurs.

Au point **Utilisateurs**, vous pouvez :

- ajouter un utilisateur
- associer un utilisateur à une personne
- associer un utilisateur à un groupe d'utilisateurs
- réinitialiser le mot de passe d'un utilisateur
- afficher groupes d'utilisateurs associés

La TSI **Configurations d'utilisateur** dans le launch group **Général** permet aux utilisateurs finaux de maintenir leurs propres configurations d'utilisateur. Les mêmes champs de données d'utilisateur sont disponibles par défaut comme dans la TSI **Groupes d'utilisateurs**. Il y a quand même une différence : la TSI **Général** > **Configurations d'utilisateur** vous permet (l'administrateur) de configurer quelles configurations d'utilisateur peuvent être maintenues par l'utilisateur.

Un compte d'utilisateur sera visible en fonction de la date de référence appliquée sur les dates de début et de fin du compte.

Groupe d'utilisateurs

Un groupe d'utilisateurs dont les droits d'accès sont déterminés par un profil de fonction. Dans Planon Software Suite les utilisateurs doivent appartenir à au moins un groupe d'utilisateurs.

Le profil de fonction lié à un groupe d'utilisateur spécifie les fonctionnalités disponibles pour ce groupe d'utilisateurs. Habituellement, ces fonctionnalités sont basées sur les tâches nécessaires pour une fonction particulière.

Chaque groupe d'utilisateurs doit être lié à un profil de fonction.

Pour chaque groupe d'utilisateurs, vous pouvez configurer les produits qui peuvent être utilisés.

Configuration de l'autorisation

Cette section décrit comment vous pouvez configurer l'autorisation pour les différents groupes d'utilisateurs au sein de votre organisation. La section Autorisation de base décrit la procédure de configuration standard. Dans la partie Autorisation avancée l'emploi de filtres d'autorisation (en option) est expliqué. Cette section explique également comment autoriser des listes de sélection et l'emploi d'ordres standard.

Nous vous recommandons de lire la section Scénarios avant de commencer à configurer l'autorisation dans Planon Software Suite, puisque cette section fournit de l'information utile sur les conséquences de plusieurs configurations de l'autorisation.

L'exportation/importation de groupes d'utilisateurs et de profils de fonction, de filtres d'autorisation et de liens d'autorisation est traitée par **Transfert de configuration**. Pour de plus amples informations, reportez-vous à *Transfert de configuration*.

Autorisation de base

L'autorisation de base comprend :

- Activer l'autorisation
- Autoriser des business objects
- Créer des profils de fonction
- Spécifier la permission de modifier des champs
- Créer des groupes d'utilisateurs et associer des profils de fonction
- Rendre des launch items disponibles dans le Launch center

  Les procédures individuelles pour mettre en œuvre les étapes mentionnées ci-dessus sont décrites en détail ci-après.

Activer l'autorisation

L'autorisation n'est pas active par défaut et il faut par conséquent l'activer avant de commencer à la configurer. Il ne faut activer l'autorisation qu'une seule fois.

Procédure

1. Allez à **Autorisation** > **Filtres d'Autorisation**.
2. Dans le coin supérieur droit, déplacez le curseur  pour activer ou désactiver l'autorisation.

L'activation/désactivation de l'autorisation est soumise à la journalisation sécurité. Pour de plus amples informations sur ce sujet, reportez-vous à *Administrator's Guide* > *Security logging*.

Autoriser des business objects

L'autorisation pour les business objects est désactivée par défaut. Ceci veut dire que tous les utilisateurs peuvent lire tous les champs de données d'un business object et qu'ils peuvent exécuter toutes les actions. Si l'autorisation est activée pour un business object, tous les utilisateurs y auront accès en lecture seule. Il est possible de limiter ou étendre les droits d'accès par groupe d'utilisateurs aux champs de données, actions, transitions d'état et actions supplémentaires.

Pour de plus amples détails sur la création de droits aux champs, actions, transitions d'état et actions supplémentaires, reportez-vous à Créer des profils de fonction.

Activer l'autorisationpour des business objects

Procédure

1. Allez à **FieldDefiner** > **Business objects**.
2. Sélectionnez le business object pour lequel vous voulez activer l'autorisation.

L'autorisation doit être activée pour des sous-types définis par l'utilisateur du business object **Ordres**. Pour les types d'ordre système, l'autorisation ne peut pas être activée! Regardons cela de plus près dans les exemples suivants :

- Work orders
  - External work order
  - Internal work order
  - Purchase order

System type
User-defined sub-type

Pour de plus amples détails sur la création de business objects définis par l'utilisateur, reportez-vous à *FieldDefiner*.

3. Cliquez dans le menu d'actions sur **En construction**.
4. Mettez dans la section des données l'option **Est autorisé** sur **Oui** et cliquez sur **Sauvegarder**.
5. Cliquez dans le menu d'actions sur **Conclu**.

   L'autorisation pour le business object sélectionné est désormais activée.

Tenez en compte que :

- Si le champ **Est autorisé** d'un business object autorisé est mis sur Non, les droits d'accès à ce business object seront par conséquent enlevés de tous les profils de fonction existants.
- Si un business object autorisé et défini par l'utilisateur est mis sur En construction dans FieldDefiner, ce business object est enlevé de la liste de business objects dans Profils de fonction dès que la liste est renouvelée. Aussi longtemps que Renouveler liste n'est pas activé, le business object ne sera pas enlevé de la liste. Cliquer sur un business object et puis essayer d'y ajouter des champs de données peut causer une erreur.

Créer des profils de fonction

Lorsque vous voulez créer des profils de fonction il faut d'abord activer l'autorisation pour les buisness objects en question.

Pour de plus amples informations à ce sujet, reportez-vous à Autoriser des business objects.

Par profil de fonction, vous pouvez spécifier un niveau d'autorisation par défaut pour un business object :

- Invisible
- Lecture seule
- Toutes fonctionnalités

Procédure

1. Allez à **Autorisation** > **Profils de Fonction**.
2. Cliquez dans le menu d'actions sur **Ajouter**.

   Ou si vous voulez réutiliser un profil de fonction existant sélectionnez **Copier**.
3. Saisissez les champs dans la section des données. Pour une description de ces champs, reportez-vous à Profils de fonction - Champs.
4. Cliquez sur **Sauvegarder**. Vous pouvez maintenant spécifier des autorisations de business objects pour ce profil de fonction.

   Les opérations suivantes sont soumises à la journalisation de sécurité :
   - Mettre à jour des profils de fonction liés à un groupe d'utilisateurs
   - Modifier le champ **Type d'autorisation par défaut**

Pour de plus amples informations sur ce sujet, reportez-vous à *Administrator's Guide* > *Security logging*.

Spécifier des autorisations de business objects

Après avoir créé des profils de fonction, vous pouvez spécifier les autorisations que vous souhaitez définir pour chaque business object et pour un profil de fonction particulier.

Spécifier des autorisations

Procédure

1. Sélectionnez au niveau de sélection **Profils de fonction** le profil de fonction pour lequel vous voulez spécifier des autorisations et allez à **Droits BO**.
2. Par business object, saisissez les champs dans la section des données. Pour une description de ces champs, reportez-vous à Droits BO - Champs.
3. Cliquez sur **Sauvegarder**.

   Si vous avez sélectionné **Invisible**, **Lecture seule**, ou **Toutes les fonctionnalités**, vous avez maintenant terminé de spécifier les autorisations pour le profil de fonction sélectionné.

Si vous avez sélectionné **Spécifique** pour un ou plusieurs business objects, vous devez poursuivre la configuration des autorisations du profil de fonction en :

- Associer des champs
- Associer des actions
- Associer des transitions d'état
- Associer des actions supplémentaires
- Spécifier des autorisations

Les rapports de système disponibles dans **Autorisation** fournissent une vue d'ensemble des autorisations par business object/groupe d'utilisateurs. Pour de plus amples informations, reportez-vous à Rapports de système - Autorisation.

Associer des champs

Pour chaque business object, vous pouvez définir quels champs doivent être disponibles pour un profil de fonction spécifique.

Procédure

1. Au niveau de **Droits BO**, sélectionnez l'objet de la liste d'éléments pour lequel vous souhaitez spécifier les champs qui doivent être disponibles.
2. Cliquez dans le menu d'actions sur **Champs**. La boîte de dialogue Champs s'affiche. Vous pouvez ici sélectionner les champs que vous voulez rendre disponible au business object.
3. Utilisez les boutons fléchés pour déplacer les éléments de la liste **Disponible** vers la liste **En usage**, ou vice versa.

   La section **Disponible** affiche les champs de données qui sont disponibles pour le business object sélectionné. La section **En usage** affiche les champs de données qui doivent être inclus dans le profil de fonction et ces champs de données seront ensuite disponibles pour le groupe d'utilisateurs associé au profil de fonction. Utilisez les boutons fléchés pour ajouter ou enlever des champs.

   Lorsque vous ajoutez ou enlevez des champs de données, vous devez toujours tenir compte du suivant :

- Lorsque vous ajoutez un champ de données de référence, comme par exemple Personne, il est également conseillé de définir au moins des autorisations de lecture pour les champs principaux comme **Code** et **Nom** des business objects de référence également.
- Lorsque vous n'ajoutez pas ces champs au profil de fonction, il se peut que des champs et des colonnes manquent dans l'outil de recherche de la boîte de dialogue en question et il est également possible que l'arbre de recherche dans la boîte de dialogue soit affiché irrégulièrement à cause de cela.
- Certains champs de données ne peuvent pas être enlevés du profil de fonction. Il s'agit ici des champs qui indiquent une hiérarchie, comme le champ **ParentOrderGroupRef** dans le business object **Groupe d'ordres**. Si le champ **ParentOrderGroupRef** n'est pas inclus dans le profil de fonction, l'arbre affichera les objets sans aucune hiérarchie.

4. Cliquez sur **OK**. Les champs sélectionnés sont désormais associés au profil de fonction.

L'association de champs à des business objects est soumise à la journalisation de sécurité. Pour de plus amples informations sur ce sujet, reportez-vous à *Administrator's Guide* > *Security logging*.

Associer des actions

Pour chaque business object, vous pouvez définir quelles actions devraient être disponibles pour un profil de fonction spécifique.

Procédure

1. Au niveau de **Droits BO**, sélectionnez le business object de la liste d'éléments pour lequel vous souhaitez définir les actions qui doivent être disponibles.
2. Cliquez dans le menu d'actions sur **Actions**.

   La boîte de dialogue Actions s'affiche. Vous pouvez ici sélectionner les actions que vous voulez rendre disponible au business object.

Si vous souhaitez accorder des droits de désarchivage à un utilisateur, vous devez également accorder des droits d'enregistrement.

3. Utilisez les flèches pour déplacer les éléments depuis la liste **Disponible** vers la liste **En cours d'utilisation**, ou vice-versa.
4. Cliquez sur **OK**.

   Les actions sélectionnées sont désormais associées au profil de fonction.

L'association d'actions à des business objects est soumise à la journalisation de sécurité. Pour de plus amples informations sur ce sujet, reportez-vous à *Administrator's Guide* > *Security logging*.

Associer des transitions d'état

Pour chaque business object, vous pouvez définir quelles transitions d'état doivent être disponibles pour un profil de fonction spécifique.

Procédure

1. Au niveau de **Droits BO**, sélectionnez l'objet de la liste d'éléments pour lequel vous souhaitez spécifier les transitions d'état qui doivent être disponibles.
2. Cliquez dans le menu d'actions sur **Transitions d'état**.

   Vous pouvez ici sélectionner les transitions d'état que vous voulez rendre disponible au business object.
3. Utilisez les boutons fléchés pour déplacer les éléments de la liste **Disponible** vers la liste **En usage**, ou vice versa. Aucune transition d'état n'est disponible par défaut.
4. Cliquez sur **OK**.

   Les transitions d'état sélectionnées sont désormais associées au business object.

L'association de transitions d'état à des business objects est soumise à la journalisation de sécurité. Pour de plus amples informations sur ce sujet, reportez-vous à *Administrator's Guide* > *Security logging*.

Associer des actions supplémentaires

Pour chaque business object, vous pouvez définir quelles actions supplémentaires doivent être disponibles pour un profil de fonction spécifique.

Procédure

1. Au niveau de **Droits BO**, sélectionnez l'objet de la liste d'éléments pour lequel vous souhaitez spécifier les actions supplémentaires qui doivent être disponibles.
2. Cliquez dans le menu d'actions sur **Actions supplémentaires**.

   La boîte de dialogue **Actions supplémentaires** s'affiche. Vous pouvez ici sélectionner les actions supplémentaires que vous voulez attribuer au business object.
3. Utilisez les boutons fléchés pour déplacer les éléments de la liste **Disponible** vers la liste **En usage**, ou vice versa.
4. Cliquez sur **OK**.

   Les actions supplémentaires sont associées au business object.

L'association d'actions supplémentaires à des business objects est soumise à la journalisation de sécurité. Pour de plus amples informations sur ce sujet, reportez-vous à *Administrator's Guide* > *Security logging*.

Spécifier des autorisations

Après avoir associé des actions/champs/actions supplémentaires/transitions d'état, vous pouvez continuer à spécifier des autorisations pour ces éléments.

Cette opération est uniquement nécessaire pour les business objects dont le type d'autorisation est **Spécifique**.

Procédure

1. Sélectionnez au niveau de sélection **Business objects** le business object pour lequel vous voulez spécifier des permissions et allez à Détails.
2. Le niveau de sélection **Détails** comprend plusieurs étapes : Sélectionnez l'étape appropriée : Pour une description des champs disponibles à ce niveau, reportez-vous à Détails - champs.
3. Cliquez sur **Sauvegarder**.

   Vous avez maintenant terminé de spécifier les autorisations pour le profil de fonction sélectionné.

Transférer des autorisations

Très souvent plusieurs profils de fonction disposent des mêmes droits pour un ensemble fixe de business objects.

De la même façon plusieurs business objects appartenant à un seul profil de fonction disposent des mêmes droits pour les actions (supplémentaires). Si vous attribuez ces droits à d'autres business objects et profils de fonction, vous auriez beaucoup de travail manuel répétitif. Pour éviter ce travail répétitif vous pouvez d'abord définir les détails du profil de fonction (champs, actions (supplémentaires) et transitions d'état pour un seul business object et les transférer ensuite à un ou plusieurs business objects dans un ou plusieurs profils de fonction simultanément en faisant appel à l'action Transférer détails profil de fonction. Bien que vous puissiez ajouter et supprimer les détails d'un profil de fonction d'un business object individuel, vous devez transférer les détails ajoutés et supprimés séparément aux autres business objects et/ou profils de fonction.

Procédure

1. Au niveau **Droits BO**, sélectionnez le business object dont vous voulez transférer les détails.

Seuls les business objects dont la case à cocher **Est autorisé** dans **FieldDefiner** est activée sont affichés dans la liste des business objects. Des champs de système ne sont jamais affichés comme ils ne peuvent pas être autorisés.

2. Cliquez dans le menu d'actions sur **Transférer détails**.

   Le wizard **Transférer détails autorisation** apparaît. Suivez les étapes présentées dans le wizard. Les étapes affichées dépendent du type d'autorisation du BO sélectionné.

   Pour les types d'autorisation suivants, passez à Étape 9:

- Invisible
- Lecture seule
- Toutes fonctionnalités

Pour le type d'autorisation *Spécifique*, l'étape **Définir l'action de transfert** est sélectionnée.

3. Indiquez si vous souhaitez changer le type d'autorisation de la cible pour *Spécifique*.
4. Sélectionnez l'option **Ajouter** si vous voulez transférer des détails ajoutés et sélectionnez **Supprimer** si vous voulez transférer des détails supprimés des business objects et profils de fonction sélectionnés.

Si vous devez transférer des détails ajoutés et supprimés, le transfert doit être exécuté deux fois.

5. Cliquez sur **Suivant**.

   L'étape **Sélectionner le(s) champ(s)** apparaît. Sélectionnez le(s) champ(s) que vous voulez ajouter aux business objects et aux profils de fonction.

   Utilisez les touches Shift+CTRL pour sélectionner plusieurs champs à la fois.

   Une barre de recherche est disponible pour effectuer des recherches dans la liste **Disponible**. S'il n'y a pas de champs à ajouter, sautez cette étape et cliquez sur **Suivant**.

   L'étape **Sélectionner l'action/les actions** apparaît.

6. Sélectionnez l'action/les actions que vous voulez ajouter aux business objects et aux profils de fonction. S'il n'y a pas d'action/actions à ajouter, sautez cette étape et cliquez sur **Suivant**.

   L'étape **Sélectionner la/les transition(s) d'état** apparaît.

7. Sélectionnez la/les transition(s) d'état que vous voulez ajouter aux business objects et aux profils de fonction. S'il n'y a pas de transitions d'état à ajouter, sautez cette étape et cliquez sur **Suivant**.

   L'étape **Sélectionner la/les action(s) supplémentaire(s)** apparaît.

8. Sélectionnez l'action supplémentaire/les actions supplémentaires que vous voulez ajouter aux business objects et aux profils de fonction. S'il n'y a pas d'action(s) supplémentaire(s) à ajouter, sautez cette étape et cliquez sur **Suivant**.

   L'étape **Sélectionner le(s) business object(s)** apparaît.

9. Sélectionnez le/les business object(s) au(x)quel(s) vous voulez ajouter les détails mentionnés ci-dessus.
   - Sélectionnez **Afficher tous les business objects** afin d'afficher tous les business objects autorisés.
   - Sélectionnez **Afficher les business objects afférents** afin d'afficher toues les business objects (autorisés) afférents. Des business objects afférents sont tous les business objects ayant le même business object de base que le business object sélectionné à l'étape 1.
10. Sélectionnez le profil de fonction auquel vous voulez ajouter les détails mentionnés ci-dessus. Cliquez sur **Suivant**.

    L'étape **Confirmer** apparaît.

11. Cet écran affiche un aperçu des détails sélectionnés.
    - Cliquez sur **Conclure**.

- Cliquez dans le wizard sur **Précédent** si vous voulez apporter des modifications à l'une des étapes précédentes

Les détails sélectionnés sont transférés aux business objects et aux profils de fonction sélectionnés.

Les modifications suivantes ont lieu lorsque les détails sont transférés.

- Si un champ ajouté est transféré, toutes ses autorisations sont également transférées. Si un champ existe déjà dans le business object de destination, ses autorisations sont modifiées.

  Si le champ sélectionné n'est pas un champ de système dans le business object original, mais si c'est un champ de système dans le business object de destination, il ne sera pas transféré.

- Si un champ, une action, une modification d'état ayant exactement le même nom se trouve dans le business object de destination ou si une action supplémentaire ayant exactement le même class name *Planon Software Suite* se trouve déjà dans le business object de destination, ils seront mis sous *En usage* (s'ils ne l'étaient pas encore).

  Si tel n'est pas le cas, le transfert du détail/des détails de ce business object est/sont sauté(s) et le transfert continue avec le détail/business object suivant.

Si l'option **Supprimer** est sélectionnée, tous les détails des profils de fonction qui ne se trouvent PAS sous En usage pour le business object sélectionné sont maintenant affichés dans la colonne **Disponible**.

Si l'action Supprimer est sélectionnée, les modifications suivantes ont lieu lorsque les détails sont transférés :

- Si un champ, une action, une modification d'état ayant exactement le même nom se trouve dans le business object de destination ou si une action supplémentaire ayant exactement le même class name *Planon Software Suite* se trouve déjà dans le business object de destination, ils seront mis sous **Non en usage** (si c'était auparavant **En usage**).

  Si tel n'est pas le cas, le transfert du détail/des détails de ce business object est/sont sauté(s) et le transfert continue avec le détail/business object suivant.

Créer des groupes d'utilisateurs et associer des profils de fonction

Des utilisateurs doivent toujours appartenir à un groupe d'utilisateurs. Les droits d'utilisateur dans un groupe d'utilisateurs sont déterminés par le profil de fonction et le filtre d'autorisation associés à ce groupe d'utilisateurs. Cette section décrit la procédure générale pour créer un groupe d'utilisateurs et pour y associer un profil de fonction.

Procédure

1. Allez à **Autorisation** > **Groupes d'utilisateurs**.

   Au premier niveau de sélection, **Groupes d'utilisateurs**, il est possible d'ajouter et supprimer des groupes d'utilisateurs.

2. Pour ajouter un groupe d'utilisateurs sélectionnez dans le menu d'actions **Groupes d'utilisateurs** l'option **Ajouter**.

3. Saisissez un nom et une description pour le nouveau groupe d'utilisateurs. Utilisez le champ **Commentaires** pour enregistrer des remarques explicatives.
4. Dans la section **Utilisateurs** les utilisateurs appartenant au groupe d'utilisateurs sélectionné sont affichés. Lorsque vous venez d'ajouter un nouveau groupe d'utilisateurs il n'y a pas d'utilisateurs y associé.
5. Sélectionnez dans le champ **Liens** l'option **Utilisateurs**.

   Une boîte de dialogue avec les utilisateurs disponibles s'affiche. Vous y pouvez sélectionner les utilisateurs que vous voulez inclure dans le groupe d'utilisateurs. Pour de plus amples informations sur l'ajout de nouveaux utilisateurs, reportez-vous à Ajouter de nouveaux utilisateurs.
   Les utilisateurs disponibles sont affichés dans la section **Disponible**. Les utilisateurs appartenant au groupe d'utilisateurs sélectionné sont affichés dans la section **En usage**. Utilisez les boutons fléchés pour ajouter ou enlever des utilisateurs.

De l'information détaillée sur les utilisateurs individuels du groupe d'utilisateurs sélectionné est affichée au niveau de sélection **Détails groupe d'utilisateurs**.
Le bouton **Afficher les comptes d'utilisateurs non-liés** de la liste des éléments vous permet d'afficher les utilisateurs qui ne sont pas liés à un groupe d'utilisateurs (rappelez-vous que le filtrage et la navigation limitent les résultats de la liste des éléments).

6. Associez un profil de fonction au groupe d'utilisateurs en utilisant le champ **Profils de fonction**. Sélectionnez le profil de fonction approprié et cliquez sur **OK**.

   Le profil de fonction est désormais associé au groupe d'utilisateurs.
7. Cliquez dans le champ **Système de contrôle supplémentaire** sur **Oui** si vous voulez journaliser les sessions de connexion et déconnexion des utilisateurs (dans le groupe d'utilisateurs sélectionné). Ces données seront stockées dans le fichier de journalisation de sécurité. Ces données seront stockées dans le fichier de journalisation de sécurité. Pour de plus amples informations, reportez-vous à Security logging.

Il est également possible de copier des groupes d'utilisateurs en utilisant l'option **Copier** dans le menu d'actions **Groupe d'utilisateurs**. Si le groupe d'utilisateurs copié comprend beaucoup d'utilisateurs du groupe d'utilisateurs original, vous pouvez épargner pas mal de temps. Tous les utilisateurs et les filtres d'action associés au groupe d'utilisateurs original sont copiés dans le nouveau groupe d'utilisateurs.
Vous ne pouvez associer qu'un seul profil de fonction à un groupe d'utilisateurs. Il est cependant possible d'associer un ou plusieurs filtres d'autorisation à un groupe d'utilisateurs. Il est nécessaire de créer un groupe d'utilisateurs séparé pour chaque combinaison d'un profil de fonction et de filtres d'autorisation (par exemple Sécurité Zone nord, Sécurité Zone sud).

Pour de plus amples informations sur la création de profils de fonction, reportez-vous à Créer des profils de fonction. Pour de plus amples informations sur la création de filtres d'autorisation et leur association à un groupe d'utilisateurs, reportez-vous à Créer des filtres d'autorisation.

L'ajout, la modification et la suppression de groupes d'utilisateurs et l'association et la dissociation d'utilisateurs avec des groupes d'utilisateurs ainsi que la mise à jour des profils de fonction lorsqu'ils sont liés au groupe d'utilisateurs, sont soumis à la journalisation de sécurité.

Pour de plus amples informations sur ce sujet, reportez-vous à *Administrator's Guide* > *Security logging*.

Les rapports de système disponibles dans **Autorisation** fournissent une vue d'ensemble des autorisations par business object/groupe d'utilisateurs. Pour de plus amples informations, reportez-vous à Rapports de système - Autorisation.

Créer des filtres d'autorisation

Un filtre d'autorisation permet à un administrateur de Planon de spécifier quelles sont les données qu'un utilisateur peut consulter, modifier et sur quelles données il peut exécuter des actions. Par exemple, si une organisation possède deux objets dans deux régions différentes, Nord et Sud. Le personnel travaillant dans la région nord ne peuvent avoir accès qu'aux données qui appartiennent à l'objet nord et de même, le personnel travaillant dans la région sud ne peuvent avoir accès qu'aux données appartenant à l'objet sud. On peut créer deux filtres d'autorisation afin de réaliser le filtrage approprié.

Un bouton **Autorisation** est disponible sur la TSI pour activer ou désactiver la totalité de la fonction d'autorisation.

L'utilisation de filtres d'autorisation est optionnelle.

Lorsque vous créez des filtres d'autorisation, vous ne pouvez pas inclure des champs dont la taille est supérieure à 2000 caractères.

Procédure

1. Allez à **Filtres d'autorisation** > **Filtres**.

   Les **Groupes d'utilisateurs** sont affichés au premier niveau de sélection. Vous pouvez attribure un groupe d'utilisateurs au filtre d'action autorisation.
2. Allez à **Filtres d'autorisation**.
3. Cliquez dans le menu d'actions sur **Ajouter**.
4. Cliquez sur le business object pour lequel vous voulez créer le filtre, par exemple **Visiteur** et cliquez ensuite sur **OK**.
5. Dans le champ **Filtre**, définissez les critères de filtre en sélectionnant les champs à filtrer. Dans chaque champ de données, sélectionnez un opérateur, puis ajoutez un paramètre de filtre correspondant.
6. Cliquez sur **Sauvegarder**.

   Le filtre d'autorisation est prêt à l'emploi.

Si un filtre d'autorisation est appliqué à un sous-type de business object, le filtre n'est d'application qu'à ce sous-type particulier. Les autres types (c.-à-d. l'objet principal et les autres sous-types) seront tous visibles et ne seront pas filtrés. Lorsqu'un filtre d'autorisation est appliqué à un business object, il n'est d'application qu'à ce type principal et tous les sous-types seront visibles et ne seront pas filtrés.

La mise à jour des filtres d'autorisation (lorsqu'ils sont liés à un groupe d'utilisateurs) est soumise à la journalisation de sécurité. Pour de plus amples informations sur ce sujet, reportez-vous à *Administrator's Guide* > *Security logging*.

Pour de plus amples informations sur la définition de paramètres, reportez-vous à *Connaissances de base*. Pour de plus amples détails sur la création de business objects définis par l'utilisateur, reportez-vous à *FieldDefiner*.

Créer des filtres d'action d'autorisation

Le filtre d'action d'autorisation permet aux administrateurs Planon de spécifier les actions auxquelles le groupe d'utilisateurs sélectionné a accès sur la base des critères du filtre d'autorisation. Par exemple, si une organisation a plusieurs propriétés, un filtre d'autorisation est créé pour les utilisateurs de la propriété du Royaume-Uni. Tous les utilisateurs basés dans des propriétés du Royaume-Uni sont autorisés à ajouter, annuler et modifier les actions, mais seuls quelques utilisateurs sont autorisés à en supprimer. Ainsi, deux filtres d'action peuvent être créés sur le même filtre d'autorisation et le même groupe d'utilisateurs, mais pour différentes actions.

Procédure

1. Allez à **Filtres d'autorisation** > **Filtres**.

   Les **Groupes d'utilisateurs** sont affichés au premier niveau de sélection. Vous pouvez créer un filtre d'action d'autorisation pour un groupe d'utilisateurs en l'ouvrant en cascade, ou vous pouvez créer un filtre d'action d'autorisation et lui assigner un groupe d'utilisateurs.
2. Allez à **Filtres d'action**.
3. Cliquez dans le menu d'actions sur **Ajouter**.
4. Cliquez sur le filtre d'autorisation pour lequel vous voulez créer le filtre d'action et cliquez ensuite sur **OK**.

   Vous pouvez également ajouter le filtre d'autorisation directement dans la fenêtre pop-up **Filtre d'autorisation**.
5. Cliquez sur **OK**.
6. Sélectionnez l'action autorisée pour le filtre d'autorisation et le groupe d'utilisateurs, cliquez sur **OK**.

Vous pouvez créer plusieurs filtres pour différentes actions sur le même filtre d'autorisation et le même groupe d'utilisateurs.

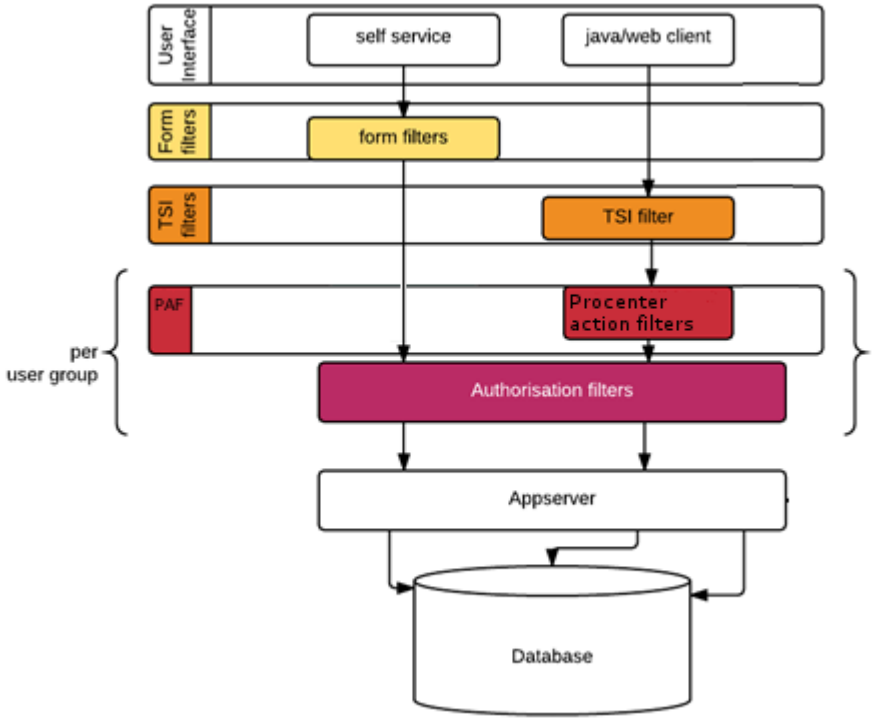
7. Dans le champ **Groupe d'utilisateurs**, sélectionnez le groupe d'utilisateurs auquel vous souhaitez appliquer le filtre, cliquez sur **OK**.
8. Cliquez sur **Sauvegarder**.

Le filtre d'action d'autorisation est prêt à l'emploi.

Filtres ProCenter pour autorisation

Les filtres ProCenter sont similaires aux filtres d'autorisation, sauf qu'ils sont limités aux TSI du **Client Web**. D'autres produits tels que **Kiosk**, **Apps** et **Self-service** ne seront pas affectés par les filtres d'action ProCenter. Après avoir créé un filtre ProCenter, vous pourrez ensuite créer des filtres d'action avec celui-ci. Un bouton **Filtre d'action ProCenter** est disponible sur la TSI pour activer ou désactiver tous les filtres d'actions ProCenter. Il est également possible d'activer ou de désactiver individuellement des filtres d'actions ProCenter.

Le filtre d'action ProCenter filtres et d'autres filtres sont représentés dans l'image ci-dessous :



Si **Autorisation** ou **Dissocier rôle et données** est désactivé, les filtres d'actions ProCenter sont également automatiquement désactivés et ne peuvent pas être activés jusqu'à ce que ces deux paramètres soient activés.

Associer des filtres d'autorisation à des groupes d'utilisateurs

Il est possible d'associer des filtres d'autorisation à des groupes d'utilisateurs afin de spécifier les données auxquelles le groupe d'utilisateurs peut avoir accès. La procédure pour associer un filtre d'autorisation à un groupe d'utilisateurs est la suivante.

Procédure

1. Allez à **Filtres d'autorisation** > **Filtres**.

   Ici vous pouvez ajouter, supprimer or copier des filtres d'autorisation. Des filtres d'actions sont associés à un groupe d'ordres afin de spécifier les actions (p.ex. **Lire**, **Sauvegarder**, **Supprimer**, etc.) que vous pouvez exécuter sur les données filtrées du filtre d'autorisation.

> L'ajout, la suppression et la mise à jour de filtres d'action sont soumis à la journalisation de sécurité. Pour de plus amples informations sur ce sujet, reportez-vous à *Administrator's Guide* > *Security logging*.

2. Cliquez dans le menu d'actions sur **Ajouter**.
3. Sélectionnez dans le champ **Filtre d'autorisation** le filtre d'autorisation souhaité.
4. Sélectionnez l'action souhaitée dans le champ **Actions**.
5. Sélectionnez le **Groupe d'utilisateurs** auquel vous souhaitez associer un filtre d'action.

   L'action sélectionnée détermine ce que les utilisateurs peuvent faire avec les données (consulter, modifier, copier, etc.).

   Un filtre **Lecture seule** (action=Annuler) est appliqué au business object objet (objet=Nord). Ce filtre est associé au groupe d'utilisateurs Sécurité nord. Ceci veut dire que les utilisateurs du groupe d'utilisateurs Sécurité nord peuvent consulter, mais ne pas modifier les informations de l'objet Nord. Les utilisateurs appartenant à Sécurité nord ne peuvent pas consulter les objets d'autres régions.

> Il est impossible d'inclure l'action **Ajouter** dans un filtre d'action, comme cette action est automatiquement incluse dans l'action **Sauvegarder** (l'action **Ajouter** est utilisée automatiquement lorsque l'utilisateur clique sur le bouton **Sauvegarder**.) Il suffit donc d'inclure l'action **Sauvegarder**.

> Si aucun filtre d'autorisation n'est associé à un groupe d'utilisateurs, les utilisateurs appartenant à ce groupe d'utilisateurs auront accès à toutes les données des business objects du profil de fonction associé. Les droits d'accès à ces données seront au moins lecture seule.

> Après avoir dissocié un filtre d'autorisation d'un groupe d'utilisateurs, vous devez renouveler le cache du serveur d'application pour désactiver le filtre.

Combiner des filtres d'autorisation

Il est possible de combiner des filtres d'autorisation comme expliqué ci-dessous :

- Plusieurs filtres d'autorisation peuvent être associés à un seul groupe d'utilisateurs. Il est seulement possible d'associer deux filtres d'autorisation au même groupe d'utilisateurs lorsque chaqu'un est

associé à des actions différentes. Le résultat est la somme des deux filtres: l'utilisateur obtient moins de droits. Par exemple : si les filtres Zone nord et Ordres de moins de 5.000 € sont associés à un groupe d'utilisateurs, les utilisateurs de ce groupe d'utilisateurs ne verront que les ordres de la zone nord ayant une valeur de moins de 5.000 €.

- Si un utilisateur est membre de deux groupes d'utilisateurs, les filtres d'autorisation des deux groupes d'utilisateurs sont combinés et l'utilisateur obtient plus de droits. Par exemple, un utilisateur qui fait partie des groupes d'utilisateurs Service Desk Nord et Service Desk Sud pourra voir les données des deux zones, c.-à-d. les zones nord et sud.

Autoriser l'emploi d'ordres standard

Il existe de nombreuses raisons pour lesquelles on peut appliquer une autorisation à des commandes standard. L'exemple suivant sert uniquement d'exemple pour cette fonctionnalité.

L'administrateur Planon de la société X a ajouté des utilisateurs à un groupe d'utilisateurs « Front Desk », qui auront uniquement l'autorisation d'ajouter des demandes. Ils ne disposent pas du droit d'ajouter des ordres de travail. Afin d'empêcher que le groupe d'utilisateurs ajoute des ordres de travail, l'administrateur Planon n'a pas inclus l'action **Ajouter** dans le profil de fonction 'Front Desk' pour le business object **Ordres de travail**. Cependant, cette action ne suffit pas à elle seule. Les utilisateurs du groupe d'utilisateurs « Front Desk » pourront encore contourner l'autorisation en utilisant des ordres standard dans la TSI **Service Manager**. En sélectionnant l'option **Ajout standard** dans le menu d'action, ils peuvent ouvrir la boîte de dialogue **Ordre standard** et sélectionner n'importe quel type d'ordre standard, en incluant les ordres de travail standard.

Pour de plus amples informations sur l'ajout d'ordres basés sur un ordre standard, reportez-vous à *Service Manager*.

Voilà pourquoi on a besoin d'autorisation supplémentaire afin d'empêcher que des utilisateurs du groupe d'utilisateurs ' Front Desk ' ajoutent un ordre de travail basé sur un ordre standard.

Vous devez prendre les mesures suivantes :

1. Veillez à ce que dans **FieldDefiner** l'option **Est autorisé** soit mis sur **Oui** pour le business object **Ordres de travail standard**.
2. Dans **Autorisation** > **Profils de fonction**, sélectionnez le profil de fonction en question et enlevez l'action **Lire** du profil de fonction. Vous pouvez ce faire en déplaçant l'action **Lire** de la section **En usage** à la section **Disponible** dans la boîte de dialogue **Actions**.

   Pour de plus amples informations sur la configuration de l'autorisation, reportez-vous à Configuration de l'autorisation.

   Après avoir effectué les configurations mentionnées ci-dessus, les utilisateurs du groupe d'utilisateurs ' Front Desk ' ne pourront plus consulter, ni sélectionner des ordres standard dans la boîte de dialogue **Ordres standard**. La boîte de dialogue **Ordres standard** n'affichera que les appels standard.

Autoriser la configuration et l’emploi de listes de sélection

L'autorisation de listes de sélection a lieu à deux niveaux puisque la configuration et l'emploi de listes de sélection peuvent être soumis à l'autorisation.

Il y deux types de listes de sélection dont la configuration et l'emploi pevuent être autorisés :

- Liste de sélection – descriptive :
- Liste de sélection – code, descriptive :

Afin de faciliter les deux types d'autorisation pour les deux types de listes de sélection, il y a plusieurs business objects relatifs aux listes de sélection disponibles. En fonction de vos exigences d'autorisation vous devez activer l'autorisation pour un ou plusieurs business objects relatifs aux listes de sélection dans **FieldDefiner**.

Pour de plus amples informations sur l'activation de l'autorisation des business objects qui jouent un rôle dans la configuration de listes de sélection, reportez-vous à . Pour de plus amples informations sur l'activation de l'autorisation des business objects qui jouent un rôle dans l'emploi de listes de sélection, reportez-vous à .

L'activation de l'autorisation pour un business object constitue l'étape 2 du procédé de l'autorisation de base. Pour de l'information générale sur le processus complet de l'autorisation, reportez-vous à Autorisation de base.

Ajouter un nouvel utilisateur

Procédure

1. A **Détails groupe d'utilisateurs**, sélectionnez le groupe d'utilisateurs approprié.
2. Cliquez dans le menu d’actions sur **Ajouter**.
3. Saisissez les champs dans la section des données. Pour une description de ces champs, reportez-vous à Utilisateur - Champs.
4. Cliquez sur **Sauvegarder**.

Cet utilisateur sera affiché temporairement dans la liste des éléments. Si vous renouvelez d’abord la liste des éléments, l’utilisateur nouvellement ajouté disparaîtra de la liste parce que l’utilisateur doit d’abord être associé au groupe d’utilisateurs.

Créer un nouveau mot de passe

Il est possible de créer un nouveau mot de passe pour de nouveaux comptes. Lorsque vous sauvegardez le nouveau compte, le nouveau mot de passe est encrypté et stocké dans la base de données.

Si le champ **Mot de passe n’expire jamais** est mis sur **Non**, la date d’expiration est la date actuelle plus le nombre de jours comme défini dans la date d’expiration du mot de passe.

Modifier un mot de passe

Les utilisateurs eux-mêmes peuvent modifier leur mot de passe.

Seul un utilisateur peut modifier son mot de passe ; il ne peut pas être modifié par une tierce personne afin de prévenir des abus.

Procédure

1. Allez à **Groupes d'utilisateurs** > **Détails groupe d'utilisateurs** > **Utilisateurs**.
2. Sélectionnez votre compte d'utilisateur.
3. Cliquez dans le menu d'actions sur **Modifier mot de passe**.

   La boîte de dialogue **Saisir les valeurs** apparaît.
4. Saisissez dans le champ **Ancien mot de passe** votre ancien mot de passe.
5. Saisissez dans le champ **Nouveau mot de passe** votre nouveau mot de passe.
6. Retapez dans le champ **Confirmer mot de passe** votre mot de passe afin de le confirmer.
7. Cliquez sur **OK**.

   Un message d'erreur est affiché vous disant que votre mot de passe est modifié et que vous pouvez essayer de vous connecter de nouveau en utilisant votre nouveau mot de passe.
8. Cliquez sur **Continuer**. Votre mot de passe est modifié.

   Lorsque vous modifiez un mot de passe les validations de mot de passe sont exécutées.

Pour de plus amples informations sur les validations de mot de passe, reportez-vous à *Configurations de système*.

Réinitialiser un mot de passe

En tant qu'administrateur vous pouvez réinitialiser le mot de passe d'un utilisateur si l'utilisateur a oublié le mot de passe ou qu'il est expiré ou pour une quelconque autre raison.

Vous devez utiliser l'autorisation pour empêcher qu'un utilisateur puisse réinitialiser le mot de passe d'un autre utilisateur.

Procédure

1. Allez à **Détails groupe d'utilisateurs** > **Utilisateurs**.
2. Sélectionnez le compte d'utilisateur pour lequel vous voulez réinitialiser le mot de passe.
3. Cliquez dans le menu d'actions sur **Modifier mot de passe**. La boîte de dialogue **Saisir les valeurs** apparaît.
4. Le champ **Mot de passe** comprend déjà un nouveau mot de passe généré par le système.

Notez que vous pouvez également remplacer le mot de passe généré par défaut.

Forcer modification mot de passe lors de la connexion

5. Dans le champ **Forcer modification mot de passe lors de la connexion** l'option **Oui** est sélectionnée pas défaut.

   Si le champ **Forcer modification mot de passe lors de la connexion** est mis sur Non, l'utilisateur peut continuer à utiliser le mot de passe généré par le système ou fourni par l'administrateur.

Pour les comptes d'utilisateur dont le mot de passe n'expire jamais, la fonctionnalité **Forcer modification mot de passe** n'est pas disponible.

Le nouveau mot de passe doit être communiqué à l'utilisateur concerné, comme le mot de passe est encrypté et ne peut plus être retrouvé après avoir cliqué sur le bouton **OK**.

Associer un utilisateur à une personne

Quelqu'un qui est enregistré comme étant un utilisateur dans **Groupes d'utilisateurs** n'est pas associé automatiquement à une personne correspondante dans **Gestion des Personnes**. Il faut l'associer manuellement après quoi tous les champs des TSI dans lesquels vous pouvez saisir une personne de **Gestion des Personnes** et pour lesquels une valeur standard est spécifiée au moyen de la macro **&Person** recevront automatiquement le nom de l'utilisateur connecté.

Il est possible d'associer plusieurs utilisateurs à une seule personne **Gestion des Personnes**. Vous pouvez utiliser un compte utilisateur unique pour plusieurs gestionnaires. Chaque gestionnaire contient ses propres personnes, de sorte que vous pouvez associer une personne au compte d'utilisateur de chacun de ces gestionnaires.

Pour de plus amples informations sur la configuration de macros comme valeur standard, reportez-vous à *FieldDefiner*. Pour de l'information générale sur les macros, reportez-vous à *Connaissances de Base*.

Procédure

1. Allez à **Détails groupe d'utilisateurs Utilisateurs**.
2. Sélectionnez l'utilisateur auquel vous souhaitez associer une personne du **Gestion des personnes**.
3. Cliquez dans le menu d'actions sur **Personnes**.
4. Sélectionnez dans la section **Disponible** la personne que vous voulez associer à l'utilisateur sélectionné et déplacez-la vers la section **En usage**.

Vous ne pouvez associer qu'une seule personne à un utilisateur simultanément dans un gestionnaire. Si vous voulez associer une autre personne à l'utilisateur actuel, vous devez d'abord déplacer la personne sélectionnée de la section **En usage** à la section **Disponible** et essayer par la suite de l'associer une autre personne.

5. Cliquez sur **OK**. Vous venez d'associer une personne de **Personnes** à l'utilisateur sélectionné.

Rendre des launch items disponibles dans le Launch center

Après avoir créé de nouveaux groupes d'utilisateurs et après y avoir associé des profils de fonction, il faut les rendre disponibles dans le Launch center du groupe d'utilisateur. Le launch item **Launch Center Manager** vous permet de configurer le Launch center pour chaque groupe d'utilisateurs.

Pour de plus amples informations sur comment rendre des launch items disponibles dans le Launch center, reportez-vous à *Launch Center Manager*.

Donner accès aux produits Planon

Chaque utilisateur (compte) est associé à un groupe d'utilisateurs. En utilisant des groupes d'utilisateurs il y a deux façons de donner accès aux utilisateurs aux produits de Planon.

- Associer des produits à des groupes d'utilisateurs
- Associer des groupes d'utilisateurs à des produits

- La gestion des accès aux produits Planon (ajouts ou suppressions) est soumise à la journalisation de sécurité. Pour en savoir plus sur ce sujet, voir *Guide administratif > Journalisation de sécurité*.
- L'ajout de produits à des groupes d'utilisateurs ou vice-versa peut être restreint pour les produits sous licence. Pour de plus amples informations, reportez-vous à *Système de licences*.

Associer des produits à des groupes d'utilisateurs

Vous pouvez associer plusieurs produits de Planon Software Suite à un groupe d'utilisateurs ce qui vous permet de spécifier quels produits seront accessibles par groupe d'utilisateurs.

Aucune définition de produit n'est attribuée par défaut à un groupe d'utilisateurs ce que veut dire que tous les utilisateurs ont accès à tous les produits disponibles. Pour de plus amples informations à ce sujet, reportez-vous à Exemples d'accès à des produits.

Pour démarrer le client Web, il est obligatoire d'ajouter la définition du produit PSS2 ainsi que la définition du produit PPWeb au groupe d'utilisateurs choisi.

Procédure

1. Sélectionnez au niveau de sélection **Groupes d'utilisateurs** le groupe d'utilisateurs auquel vous voulez associer des produits.
2. Cliquez dans le menu d'actions sur **Définitions de produits**.

   La boîte de dialogue **Définitions de produits** s'affiche.
3. Sélectionnez dans la section **Disponible** un ou plusieurs produits et déplacez-les vers la section **En usage**.

   Sélectionnez par exemple PSS2 dans la liste dans la section **Disponible** et cliquez sur la flèche droite pour le déplacer vers la section **En usage**.
4. Cliquez sur **OK**.

   Le groupe d'utilisateurs est associé au(x) produit(s) sélectionné(s). Les utilisateurs de ce groupe d'utilisateurs n'ont accès qu'au(x) produit(s) associé(s) et non pas aux autres produits.

Associer des groupes d'utilisateurs à des produits

Vous pouvez associer des groupes d'utilisateurs à des produits. Ceci vous permet de spécifier quels groupes d'utilisateurs ont accès à un produit spécifique.

Aucun groupe d'utilisateurs n'est attribué par défaut à une définition de produit ce que veut dire que tous les groupes d'utilisateurs ont accès à tous les produits disponibles. Si un seul produit est associé à un groupe d'utilisateurs (ou vice versa) le groupe d'utilisateurs n'aura pas accès aux autres produits de Planon. Pour de plus amples informations à ce sujet, reportez-vous à Exemples d'accès à des produits.

Veillez à ne pas vous exclure vous-même de l'application ! Veillez à ce que les superviseurs de Planon aient accès à tous les produits.

Procédure

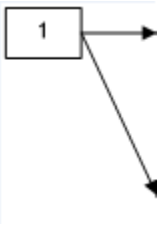
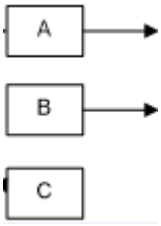
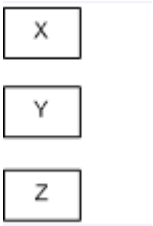
1. Sélectionnez dans **Détails groupe d'utilisateurs** > étape de sélection **Définitions de produit** le produit auquel vous voulez associer un groupe d'utilisateurs.
2. Cliquez dans le menu d'actions sur **Groupes d'utilisateurs**.

   La boîte de dialogue **Groupes d'utilisateurs** s'affiche.
3. Sélectionnez dans la section **Disponible** un groupe d'utilisateurs et déplacez-le vers la section **En usage**.
4. Cliquez sur **OK**.

Le groupe d'utilisateurs est associé à la définition de produit.

Exemples d'accès à des produits

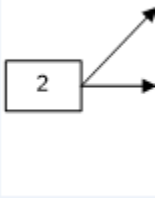
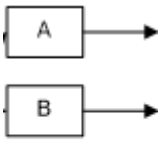
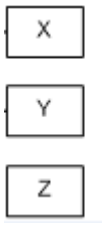
Les tableaux suivants montrent l'effet de l'association de groupes d'utilisateurs à des définitions de produit.

Utilisateur	Groupe d'utilisateurs	Définition de produit	Résultat
			

Utilisateur 1 est associé aux groupes A et C.

Groupe d'utilisateurs C n'est associé à aucune définition de produit ; les utilisateurs exclusivement associés au groupe d'utilisateurs C ont accès à tous les produits.

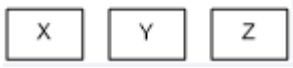
Parce que l'utilisateur 1 est également associé au groupe d'utilisateurs A n'associé qu'à la définition de produit X, il n'a accès qu'au produit X.

Utilisateur	Groupe d'utilisateurs	Définition de produit	Résultat
			

Utilisateur 2 est associé aux groupes d'utilisateurs A et B.

Groupe d'utilisateurs A est associé à définition de produit X et groupe d'utilisateurs B est associé à définition de produit Y.

Utilisateur 2 a accès aux produits X et Y.

Utilisateur	Groupe d'utilisateurs	Définition de produit	Résultat
			

Utilisateur 3 est associé au groupe d'utilisateurs C qui n'est associé à aucune définition de produit.

Par conséquent utilisateur 3 a accès à tous les produits disponibles.

Dissocier la définition de produit du planificateur

Lorsque la définition de produit du planificateur est retirée d'un groupe d'utilisateurs, ce changement n'est pris en compte qu'après le redémarrage du serveur de l'application (qui inclut un redémarrage du planificateur).

Définitions de produit disponibles

Le tableau suivant présente les définitions de produit disponibles et les produits auxquels elles donnent accès.

Pour que les utilisateurs soient en mesure d'utiliser les produits listés, assurez-vous que le groupe d'utilisateurs est lié à la définition de produit correspondante.

Produit	Définition de produit	Nom
PMFS	PMFS	Planon Mobile Field Services
Web Client	PPWeb	Planon ProCenter Web Client
	PSS2	Planon ProCenter Self-Service
Connect for AutoCAD	EnterpriseServiceAPI	Planon ProCenter Enterprise Service API
	JsonServices	Planon JSON services
Connect for Outlook	Exchange	Planon ProCenter Connect for Outlook
AWM	AWMDataEngine	Planon AWM Data Engine
Resource Planner	EnterpriseServiceAPI	Planon ProCenter Enterprise Service API
Apps	Apps	Planon Apps
PSS1	PSS1	Planon Self-Service
Java Client	PPJC	Planon ProCenter Java Client
PSS2	PSS2	Planon ProCenter Self-Service
Scheduler/Alerts	Scheduler	Planon ProCenter Planned Services Scheduler
Web Services	PPWS	Planon ProCenter Web Services

Autorisation avancée

L'autorisation avancée comprend :

- Créer des filtres d'autorisation
- Décision : utiliser des TSI avec ou sans autorisation

  Les paragraphes suivants décrivent les options d'autorisation avancée.

Utiliser autorisation TSI

Lors de la configuration de Planon Software Suite il n'est pas toujours nécessaire d'utiliser l'autorisation. Regardons cela de plus près dans l'exemple suivant :

Une organisation a défini l'usage que font les fonctions suivantes des données des visiteurs :

- Agents de sécurité - peuvent ajouter des visiteurs et modifier les données des visiteurs ;
- Collaborateurs du service desk - peuvent consulter les données des visiteurs, mais ne peuvent pas les modifier ;
- Collaborateurs de la restauration - ne peuvent pas avoir accès aux données des visiteurs du tout.

Deux configurations possibles peuvent être utilisées afin d'implémenter cette structure :

- Une TSI sans autorisation ;
- Une TSI en combinaison avec une autorisation.

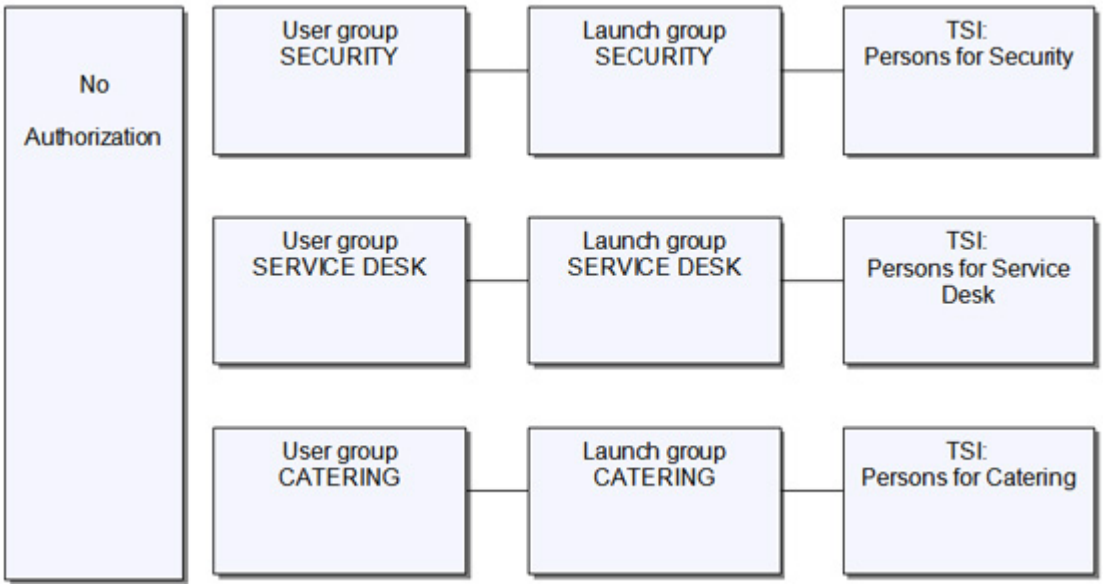
Si les données en question contiennent des informations confidentielles qui ne devraient jamais être accessibles aux utilisateurs finaux, une TSI doit être utilisée en combinaison avec une autorisation. Si de l'autre côté les données ne sont pas confidentielles, il ne faut pas utiliser l'autorisation et la solution est d'utiliser plusieurs TSI.

L'emploi de TSI sans autorisation permet aux utilisateurs d'accéder à des champs de données qu'ils ne peuvent pas accéder en utilisant des boîtes de dialogue ou des rapports. Nous vous recommandons fortement, afin d'être tout à fait sûr, d'utiliser une TSI en combinaison avec une autorisation.

Ces configurations sont le suivantes :

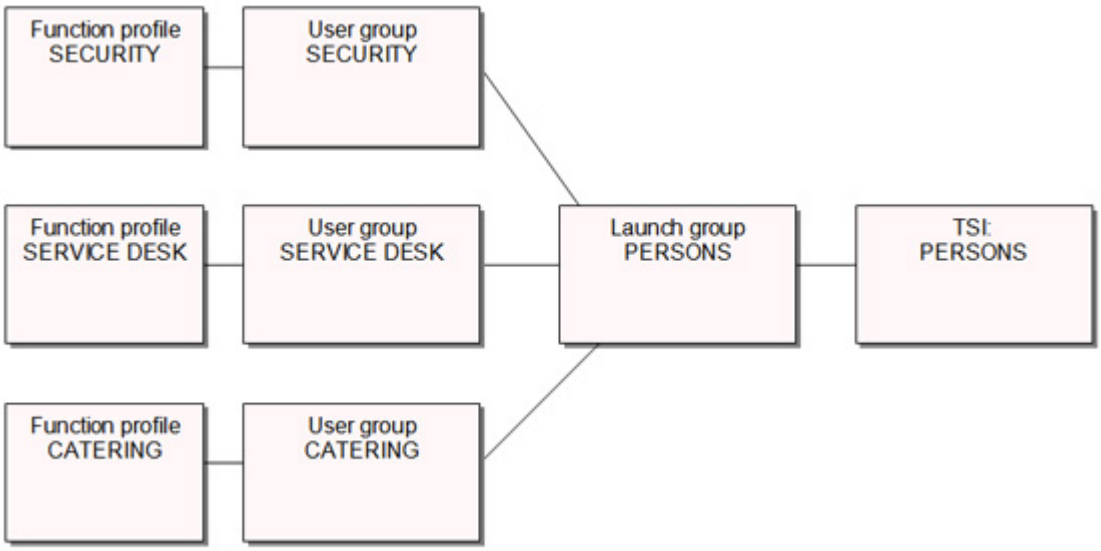
TSI

Ceci implique la création de trois TSI basées sur la TSI standard **Gestion des Personnes**.



TSI et autorisation

Ceci implique la création d'une TSI basée sur la TSI standard **Gestion des Personnes** et trois profils de fonction différents.



- Pour de plus amples informations sur les TSI, reportez-vous à *TSI Manager*.
- Pour de plus amples informations sur les launch groups, reportez-vous à *Launch Center Manager*.

Autorisation sur la date de connexion

Chaque fois qu'un utilisateur se connecte, le système vérifie le nom de l'utilisateur et son mot de passe. Le système vérifie également si l'utilisateur peut se connecter à ce moment particulier en contrôlant la date de début et de fin de l'utilisateur en question. Ces données sont comparées avec la date de système du serveur.

Si la date de début d'un utilisateur est postérieure à la date de système à laquelle il ou elle essaie de se connecter, le processus de connexion s'arrête. Il se passe la même chose lorsque la date de fin de l'utilisateur est antérieure à la date de système à laquelle il ou elle essaie de se connecter.

Configurer la date de début et de fin de l'utilisateur

Pour configurer la date de début et de fin d'un utilisateur, procédez comme suit :

Procédure

1. Sélectionnez au niveau de sélection **Groupes d'utilisateurs** > **Groupes d'utilisateurs** un groupe d'utilisateurs.
2. Sélectionnez le niveau de sélection **Utilisateurs**.
3. Sélectionnez dans la liste des éléments l'utilisateur dont vous voulez configurer la date de début et de fin.
4. Saisissez le champ **Date de début** et éventuellement le champ **Date de fin** dans la section des données.
5. Cliquez sur **Sauvegarder**.

   Vous venez de configurer la date de début (et éventuellement de fin) de l'utilisateur sélectionné.

Utiliser une date de référence

Vous pouvez configurer une date de référence au niveau de sélection **Utilisateurs**. Lorsque vous configurez une date de référence, votre liste d'éléments sera filtrée en fonction de cette date et seuls les utilisateurs qui sont valables à la date de référence, i.e. les utilisateurs dont la date de début est antérieure ou égale à la date de référence et dont la date de fin est postérieure ou égale à la date de référence seront affichés.

La date de système est par défaut la date de référence.

En cliquant sur le bouton **Date de référence** vous pouvez sélectionner une autre date aussi bien dans le futur que dans le passé. Pour distinguer une date de référence sélectionnée de la date actuelle, le nom du bouton **Date de référence** porte une couleur différente.

La date de référence est activée par défaut. Vous pouvez désactiver la date de référence en cliquant dans la barre d'outils sur **Désactiver la date de référence**.

Configurations d’écran d’utilisateur

A votre écran vous pouvez effectuer certaines actions, comme

- redimensionner des boîtes de dialogue,
- sélectionner des options dans des boîtes de dialogue,
- ouvrir une TSI
- et cetera.

  Les résultats de ces actions sont stockés dans la base de données comme des configurations d’écran d’utilisateur et sont spécifiques à chaque utilisateur. Lorsque vous vous connectez, les dernières configurations d’écran d’utilisateur seront chargées dans l’application. Vous pouvez ainsi consulter les données de la façon que vous vous convient.

Généraliser des configurations d’écran

Effectuer des configurations d’écran standard pour tous les utilisateurs dans une société qui ne se sont jamais connectés avant. Ainsi tous les nouveaux utilisateurs travailleront avec la même interface.

Procédure

1. Démarrez **Autorisation**> **Groupes d’utilisateurs** et descendez à **Utilisateurs**.
2. Cliquez au niveau de sélection **Utilisateurs** sur le bouton de la barre d’outils **Généraliser les configurations d’écran**.

   Un message apparaît.
3. Cliquez sur **OK** pour mettre les configurations d'écran pour tous les nouveaux utilisateurs ou cliquez sur **Annuler** pour annuler l'action.

Configurer des configurations d’écran d’utilisateur

Procédure

1. Démarrez **Autorisation** > **Groupes d’utilisateurs** et descendez à **Utilisateurs**.
2. Sélectionnez l’utilisateur pour lequel vous voulez configurer les configurations d'écran.
3. Descendez à **Configurations**.

   Saisissez les champs dans la section des données, reportez-vous à Configurations d’utilisateur - Champs.
4. Cliquez sur **Sauvegarder**.
5. Cliquez sur **Tout renouveler** ou sur **F9**. Déconnectez-vous et connectez-vous au Web Client.

   Vous venez de configurer les configurations d’écran d’utilisateur.

Supprimer des configurations d’écran d’utilisateur

Les configurations d'utilisateurs peuvent occasionnellement être corrompues et l'application peut se comporter de façon inhabituelle. Ceci peut être résolu en utilisant l'action **Effacer configurations d'écran d'utilisateur**.

Procédure

1. Démarrez **Autorisation** > **Groupes d'utilisateurs** et descendez à **Utilisateurs**.
2. Sélectionnez l'utilisateur dont vous voulez effacer les configurations d'écran stockées.
3. Cliquez dans le menu d'actions **Configurations d'utilisateur** sur **Effacer configurations d'écran d'utilisateur**.

   Les configurations stockées de l'utilisateur sélectionné sont maintenant effacées. La prochaine fois que l'utilisateur se connecte, il verra les configurations d'écran standard.

Liens d'autorisation

Un lien d'autorisation vous permet d'associer deux business objects vous permettant ainsi de ne voir que ces enregistrements du business object pour lequel le lien d'autorisation est créé. Ceci se passe lorsqu'un utilisateur crée un lien d'autorisation sur un business object. Dans ce cas le filtre d'autorisation du business object associé (le business object postérieur du lien) influence l'enregistrement du business object sur lequel le lien d'autorisation est créé.

Un filtre d'autorisation détermine si un utilisateur peut voir, modifier ou exécuter des actions pour un certain business object basé sur ses caractéristiques. Un lien d'autorisation est toutefois toujours créé sur l'action **Lecture** du business object.

Pour de plus amples informations sur la création de filtres d'autorisation, reportez-vous à Créer des filtres d'autorisation.

Lorsque deux business objects sont associés, le deuxième business object apparaît en tant que champ de référence du premier. En utilisant par exemple des liens d'autorisation, l'utilisateur peut voir les personnes associées seulement à ces objets/bâtiments que l'utilisateur peut voir.

Dans Planon ProCenter vous pouvez créer des liens d'autorisation seulement pour des business objects de base configurables. Des liens d'autorisation peuvent en plus être utilisés pour de champs de référence libres entiers, mais ils ne peuvent pas être utilisés pour des champs chaîne libres.

Des liens d'autorisation peuvent être définis seulement pour des business objects de base pour lesquels un filtre d'autorisation est mis sur l'action **Lecture**.

- Un lien d'autorisation créé sur le business object de base est également implicitement appliqué à ses sous-éléments.
- L'ajout, la suppression, la mise à jour des liens d'autorisation sont soumis à la journalisation de sécurité. Pour de plus amples informations sur cette configuration, reportez-vous à *Administrator's Guide* > *Security logging*.

Créer un lien d'autorisation

Procédure

1. Allez à **Autorisation** > **Liens d'autorisation**.
   Le niveau de sélection **Business objects** affiche tous les business objects sans les sous-types.
2. Sélectionnez le business object pour lequel vous voulez créer le lien d'autorisation. Per exemple : **Personnes**.

Les liens d'autorisation peuvent également être appliqués sur les business objects pour lesquels **Est autorisé** est mis sur **Non**.

3. Descendez à **Liens d'autorisation**.
4. Cliquez dans le menu d'actions sur **Ajouter**.

   Remplissez dans la section **Général** les champs. Pour une description de ces champs, reportez-vous à Liens d'autorisation.
5. Cliquez sur **Sauvegarder**. Le champ **Lien** affiche le lien d'autorisation créé entre les deux business objects ; c.-à-d. le lien entre le business object source et le business object cible.

Dans **Liens d'autorisation** la fonction **Recherche rapide** vous permet de mettre un filtre sur les champs **Définition de champ Business object, Actif?** et **Nom de système** pour filtrer les business objects.

Vous ne pouvez pas créer des références circulaires entre des business objects utilisant des liens d'autorisation. Si vous avez créé un lien d'autorisation entre les business objects **Personnes** et **Objets**, vous ne pouvez pas créer un autre lien entre **Objets** et **Personnes**. Il n'est pas possible non plus de créer des liens d'autorisation autoréférencés. Par un exemple un lien d'autorisation du business object **Objets** à **Objets** n'est pas possible.

Liens d'autorisation : à faire et à ne pas faire

A cause des liens d'autorisation il se peut que l'interrogation de la base de données soit très intensive lorsque vous voulez prélever des données. Nous vous donnons par la suite quelques instructions pour éviter des problèmes de performance lorsque vous utilisez des liens d'autorisation :

Mettre un filtre sur un champ non indexé

Des liens d'autorisation créés entre des business objects avec des champs non indexés faisant partie d'un query peuvent avoir une pénalité de performance. Dans Planon Software Suite la majeure partie des champs dans des relations (tableau) commençant par FK_ sont indexés. Le champ de code est aussi obligatoirement indexé. Par exemple, le champ **Unité de longueur** dans le business object **Espaces**, avec le nom de table FK_PLC_MEASUREMENT_SYSTEM.

Activer un filtre sur un BO qui est défini sur une vue

Tous les variables de relation (tableau) qui commencent par PLN_VW_ sont des vues dans le planning d'une base de données. Un lien d'autorisation interrogeant une vue créée pour des relations ayant une relation complexe peut avoir une pénalité de performance. Par exemple, créer un lien d'autorisation sur BaseMaintainenceActivityDefinition à BaseAssetRef. Ce lien interroge PLN_VW_ ASSET.

Rendre un utilisateur disponible dans plusieurs groupes d'utilisateurs

Un lien d'autorisation peut causer un query complexe si un utilisateur fait partie de plusieurs groupes d'utilisateurs. Ceci peut causer une pénalité de performance.

Faire un long lien d’autorisation

Si un lien d'autorisation est créé sur un business object qui fait à son tour partie d'un lien d'autorisation d'un autre business object et de même, ceci peut causer une pénalité de performance.

Journalisation de sécurité

Pour pouvoir surveiller et protéger l'intégrité des données de votre application, Planon a activé la journalisation de sécurité. Cela permettra de s'assurer que :

- Les enregistrements de sécurité informatique sont stockés de façon suffisamment détaillée.
- Les violations de la politique peuvent être surveillées et que des mesures appropriées peuvent être prises.

La journalisation des événements se fait dans un fichier ; son nom et son emplacement sont configurables. La journalisation peut être activée/désactivée selon les besoins.

Les événements suivants sont consignés :

- Modification de l'authentification
- Actions (échouées) des utilisateurs
  - Les échecs de connexion des utilisateurs sont consignés
  - Les échecs de connexion des utilisateurs (verrouillés) sont consignés
  - À la première connexion d'un utilisateur
  - Échec de la connexion d'un utilisateur (avant/après la date de début/fin)
  - Le compte d'utilisateur va être verrouillé (plusieurs entrées d'identifiants incorrects, date de fin ou mot de passe expirés)
- Les paramètres de sécurité de mot de passe
- Connexion/déconnexion d'administrateurs Planon
- Les modifications d'autorisations

Pour en savoir plus sur la configuration de la journalisation de sécurité, voir *Guide de l'administrateur* > *Journalisation de sécurité*.

Scénarios

Cette section décrit plusieurs scénarios qui expliquent les conséquences de l'emploi de différentes configurations d'autorisation.

Dans Autorisation vous avez configuré :

Situation 1: Un utilisateur a le droit de modifier le champ **Espace**, mais il ne peut pas voir le champ **Objet**.

Situation 2: Un utilisateur a le droit de modifier le champ **Espace**, et il est autorisé à voir, mais pas à modifier le champ **Objet**.

Si l'utilisateur modifie le champ Espace, il se passera ce qui suit :

Pour la situation 1 : Planon sautera le champ **Objet** et ne le modifiera pas. Planon n'affiche aucun message d'erreur. Lorsque l'utilisateur tente d'enregistrer, un message d'erreur peut s'afficher.

Pour la situation 2 : Planon modifiera le champ **Objet**, bien que l'utilisateur ne soit pas autorisé à modifier ce champ manuellement.

Dans Autorisation vous avez configuré qu'un utilisateur n'est pas autorisé à voir les ordres de travail :

Considérez les situations suivantes :

Une demande standard ensemble avec des sous-ordres standard est définie. Si l'utilisateur qui n'est pas autorisé à voir les ordres de tarvail standard, essaye d'utiliser cette demande standard, il se passe ceci : tous les champs qui font partie de la demande sont saisis automatiquement, mais les sous-ordres ne sont pas créées (même si l'utilisateur a indiqué qu'il voulait créer des sous-ordres).

Dans Autorisation vous avez configuré qu'un utilisateur n'est pas autorisé à voir certains champs d'un ordre de travail :

Considérez les situations suivantes :

Si l'utilisateur essaye d'utiliser un ordre de travail standard ou une demande standard, il se passe ceci : Planon essaye de saisir des champs qui ne peuvent pas être saisis parce que l'utilisateur n'est pas autorisé à les voir. Dans ce cas Planon saisit tous les champs pour lesquels l'utilisateur est autorisé et saute les champs que l'utilisateur ne peut pas voir. Planon n'affiche aucun message d'erreur. Remarque : Note : si un utilisateur a des droits de lecture seule pour un certain champ, Planon peut le saisir.

Dans Autorisation vous avez configuré :

Situation 1 : Un utilisateur a accès en lecture seule au champ **Département** du business object **Personnes**.

Situation 2: Un utilisateur n'a pas d'accès au champ **Département** du business object **Personnes**.

Si l'utilisateur sélectionne une personne du département « FM » et qu'il clique sur **Copier**, il se passe ceci :

Pour la situation 1 : La valeur « FM> se met automatiquement dans le champ **Département** du nouvel objet (personne), bien que l'utilisateur ne soit pas autorisé à modifier la valeur de ce champ manuellement.

Pour la situation 2 : Le champ **Département** du nouvel objet (personne) reste vierge (mais l'utilisateur ne voit pas le champ!).

Combiner des groupes d'utilisateurs

Cette section explique les conséquences au niveau de l'autorisation suite à l'association de personnes à différents groupes d'utilisateurs.

- Si l'action **Lecture** est disponible pour le Groupe d'utilisateurs 1, mais pas disponible pour le Groupe d'utilisateurs 2, l'action **Lecture** sera aussi disponible pour un utilisateur appartenant aux deux groupes d'utilisateurs.
- Si le champ **Objet** du business object Ordres de travail n'est pas disponible pour le Groupe d'utilisateurs 1, mais s'il peut être modifié par le Groupe d'utilisateurs 2, il peut également être modifié par un utilisateur appartenant aux deux groupes d'utilisateurs.
- Si le Groupe d'utilisateurs 1 n'a pas de filtre d'action sur l'action **Lecture** pour l'Objet (i.e. des utilisateurs de ce groupe peuvent voir tous les objets) et le Groupe d'utilisateurs 2 a un filtre d'action sur l'action **Lecture** qui ne permet que de voir les objets à Amsterdam, un utilisateur appartenant aux deux groupes d'utilisateurs pourra voir tous les objets.
- Si le Groupe d'utilisateurs 1 a un filtre qui ne permet que de voir les objets à Londres et que le Groupe d'utilisateurs 2 a un filtre sur l'action **Lire** qui ne permet que de voir les objets à Amsterdam, un utilisateur appartenant aux deux groupes d'utilisateurs pourra voir aussi bien les objets à Londres qu'à Amsterdam.
- Le Groupe d'utilisateurs 1 n'a pas de filtre d'action sur l'action **Lecture** pour Objet (c.-à-d. les utilisateurs de ce groupe peuvent voir tous les objets) et un filtre sur l'action **Sauvegarder** qui permet la modification d'objets seulement à Londres. Le Groupe d'utilisateurs 2 a un filtre qui permet de consulter des objets aux Pays-Bas, mais de ne modifier que des objets à Amsterdam. Un utilisateur appartenant aux deux groupes d'utilisateurs pourra voir tous les objets et pourra modifier les objets aussi bien à Amsterdam qu'à Londres.
- Le Groupe d'utilisateurs 1 a un filtre qui permet de consulter des objets aux Pays-Bas, mais de ne modifier que des objets à Amsterdam. Le Groupe d'utilisateurs 2 a un filtre qui permet de voir des objets à Amsterdam et de modifier des objets seulement à Amsterdam. Un utilisateur appartenant aux deux groupes d'utilisateurs pourra voir des objets à Amsterdam et dans le reste des Pays-Bas, mais il ne pourra modifier que les objets à Amsterdam seulement.

Séparer l’accès aux données et l’accès fonctionnel

Lorsque vous organisez l’autorisation sur la base d’une combinaison de groupes d’utilisateurs et de l’association de profils de fonction vous risquez de devoir maintenir un nombre considérable de groupes, profils et filtres.

Il est possible de diminuer cette charge de maintenance potentielle en séparant l’accès aux données et l’accès fonctionnel. En supprimant le lien entre un groupe d’utilisateurs et un profil de fonction il est désormais possible d’établir une séparation pareille comme il sera expliqué dans les sections suivantes.

Il est possible de réutiliser des données ou des groupes d'utilisateurs fonctionnels pour différents utilisateurs.

Séparer l’accès aux données et l’accès fonctionnel

Procédure

1. Go to **Configurations de système** > **Autorisation**.
2. En supposant que l’Autorisation est déjà mise sur **Oui**, mettez également **Diviser rôle et données** sur **Oui**.
3. Créer des groupes d'utilisateurs de données et des groupes d'utilisateurs fonctionnels.
4. Associer des utilisateurs aux groupes d'utilisateurs de données et aux groupes d'utilisateurs fonctionnels.

Ainsi dans **Autorisation** > **Groupes d’utilisateurs** le champ **Profil de fonction** n’est plus un champ obligatoire. Il est par conséquent possible d’avoir des groupes d’utilisateurs sans y associer un profil de fonction.

Ainsi en associant un filtre d’autorisation à un groupe d’utilisateurs sans profil de fonction, vous pouvez garantir accès aux données à un ensemble de données spécifique (accès aux données).

Utiliser l’autorisation de cette façon entraîne des conséquences comme il sera expliqué plus tard.

Après avoir mis **Diviser rôle et données** sur **Oui**, il sera difficile pour ne pas dire pas impossible de défaire cette modification.

Différences méthodes d’autorisation

Les utilisateurs peuvent appartenir à plusieurs groupes d’utilisateurs. Si un utilisateur est associé à deux groupes d’utilisateurs, un avec des filtres et un sans filtres, l’accès aux données/l’accès fonctionnel est différent.

En combinant des données et accès fonctionnel	En séparant l'accès aux données et accès fonctionnel
les utilisateurs reçoivent plus de droits d'accès, ils ont accès complet, peuvent exécuter toutes les actions.	les utilisateurs ont moins de droits d'accès, l'accès/les actions disponibles sont limités.

Lorsque des liens d'autorisation sont utilisés et qu'un utilisateur est associé à deux groupes d'utilisateurs, un avec des liens et un sans liens, l'accès aux données/l'accès fonctionnel sont différents :

En combinant des données et accès fonctionnel	En séparant l'accès aux données et accès fonctionnel
Le lien n'est utilisé que pour l'ensemble de données du groupe d'utilisateurs associé.	Le lien est utilisé pour l'ensemble de données des deux groupes d'utilisateurs.

Exemples

Les scenarios suivants aideront à comprendre les différences entre les méthodes d'autorisation.

Supposons qu'il y a trios utilisateurs ayant accès à toutes les données suivantes ou à une partie d'elles.

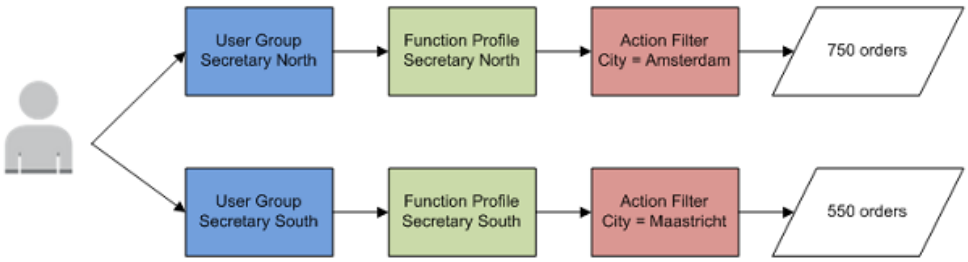
Ensemble de données Amsterdam

Nombre d'ordres	Ordres > €1000	Ordres < €1000
750	250	500

Ensemble de données Maastricht

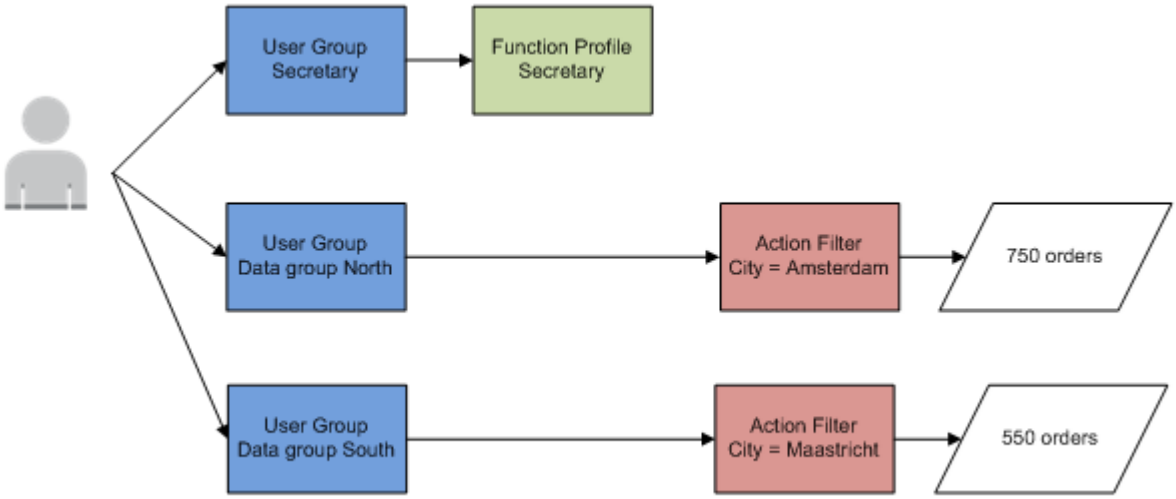
Nombre d'ordres	Ordres > €1000	Ordres < €1000
550	300	250

Combinant accès aux données et accès fonctionnel



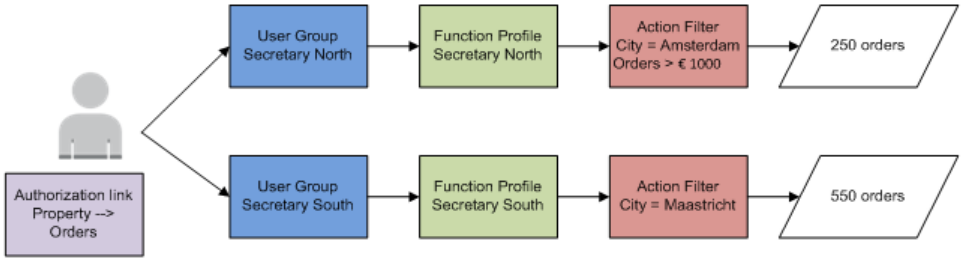
Chaque groupe d'utilisateurs a son propre profil de fonction et filtre d'action.

Séparant l'accès aux données et l'accès fonctionnel



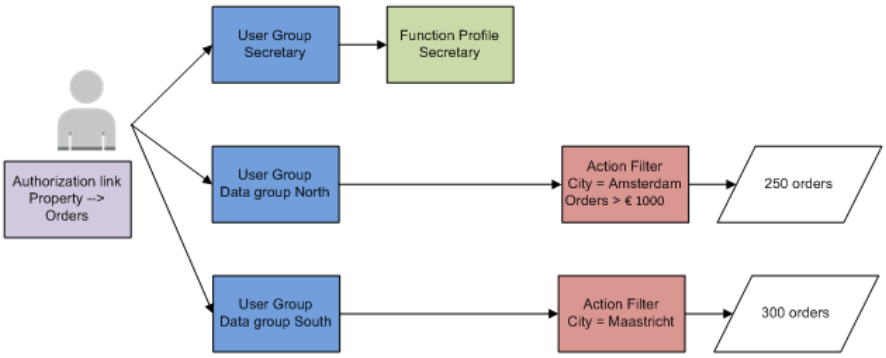
Seulement un seul profil de fonction est nécessaire, division de rôles (champs, actions, etc.) et accès aux données.

Combinant accès aux données et accès fonctionnel (et utilisant des liens d'autorisation)



Le filtre n'est utilisé que pour un ensemble de données, ne limitant l'accès aux données que pour cet ensemble de données.

Séparant l'accès aux données et l'accès fonctionnel (et utilisant des liens d'autorisation)



Le filtre est utilisé pour les deux ensembles de données, limitant l'accès aux données.

Les rapports de système disponibles dans **Autorisation** fournissent une vue d'ensemble des autorisations par business object/groupe d'utilisateurs. Pour de plus amples informations, reportez-vous à Rapports de système - Autorisation.

Utiliser des clés d'accès

En générant une paire de clés, l'administrateur Planon peut activer l'usage de Clés d'accès. Une paire de clés est composée d'une clé privée et d'une clé publique qui, ensemble, remplissent deux fonctions : l'authentification et le cryptage. La clé privée (utilisée pour générer la clé d'accès) et la clé publique (utilisée pour déchiffrer la clé d'accès) sont stockées dans la base de données.

Lorsqu'une paire de clés est générée, l'administrateur Planon peut créer des clés d'accès et les donner aux personnes souhaitées afin de leur accorder un accès (limité) à Planon (voir Instructions d'utilisation).

Configuration

Avant de pouvoir utiliser des clés d'accès, une certaine configuration est nécessaire :

- Vous devez générer des paires de clés.
- Vous devez ajouter l'étape **Clés d'accès** à **Groupes d'utilisateurs**.

Il suffit d'effectuer cette opération une fois.

- Vous devez créer les clés d'accès et les distribuer.

Générer une paire de clés

1. Allez à **Paramètres système** > **Sécurité**
2. Cliquez sur l'onglet **Paires de clés** et cliquez sur **Générer une paire de clés**.

   Planon va générer une paire de clés et remplira automatiquement les champs de l'onglet **Paires de clés**. Pour en savoir plus sur ces champs, voir Champs des paires de clés.

Configurer des groupes d'utilisateurs

1. Allez à **TSI** > **Groupes d'utilisateurs** et mettez-les en construction.
2. Allez à **TSI** et développez **Groupes d'utilisateurs** et sélectionnez le niveau **Configuration**.
3. Ajoutez l'étape de sélection **Clés d'accès** (AccountAccessKey).
4. Mettez l'état de la TSI sur **Conclu**.
5. Déconnectez-vous puis reconnectez-vous pour actualiser votre navigateur.

Vous êtes maintenant prêt à générer les clés d'accès.

Générer des clés d'accès

1. Allez à **Autorisation** > **Groupes d'utilisateurs** > **Clés d'accès**.
2. Cliquez sur **Ajouter** pour ajouter une clé d'accès et remplir les champs nécessaires.

   Pour en savoir plus sur ces champs, voir Champs des clés d'accès.
3. Cliquez sur **Enregistrer**, la clé d'accès apparaît dans le champ **Clé d'accès**. Placez votre curseur dans le champ et copiez son contenu (CTRL+A et CTRL+C).
   - La clé d'accès est une chaîne alphanumérique qui apparaît sur une seule ligne.
   - Vous pouvez générer plusieurs clés d'accès.
4. Collez le contenu dans un éditeur de texte pour l'enregistrer pour une utilisation ultérieure.
5. Accédez au formulaire que vous souhaitez partager et copiez son URL.
6. Collez l'URL dans une nouvelle ligne de l'éditeur de texte qui précède la clé d'accès.
7. Ajoutez la chaîne ***?accesskey=*** à l'URL.

   Voici comment cela apparaîtra dans les différents clients :
   - **PSS** : https://<planon-instance>.pdit.cloud/case/BP/ PUB003/?accesskey=
   - **Kiosk** : https://<planon-instance>.pdit.cloud/kiosk/?accesskey=
   - **SDK** : https://<planon-instance>.pdit.cloud/sdk/?accesskey=
8. Fusionnez l'URL et la clé d'accès sur une seule ligne.

   Vous pouvez maintenant tester l'URL obtenue. Pour ce faire, ouvrez un autre navigateur, collez la nouvelle URL dans la barre d'adresse et appuyez sur ENTRÉE.

   Le formulaire auquel vous accordez un accès direct s'affiche.

- Si vous trouvez que l'URL obtenue (combinaison URL + clé d'accès) est trop longue, vous pouvez générer une URL plus courte en utilisant un raccourcisseur d'URL sur Internet.
- Si vous distribuez la clé d'accès, toutes les personnes qui l'utilisent utiliseront le même compte pour accéder à Planon.
- Cette fonctionnalité a pour objectif de fournir un accès (en lecture seule) aux informations contenues dans Planon ou à une application tierce nécessitant un accès aux données de Planon, tels que : des sondages, des tableaux, etc.
- Cette fonctionnalité fonctionne uniquement pour les clients Self-Service, SDK et Kiosk.
- Une connexion à Planon via la clé d'accès est moins sécurisée qu'une connexion utilisant un nom d'utilisateur et un mot de passe. Veuillez lire attentivement les Instructions d'utilisation.

Instructions d'utilisation

Avant d'utiliser la fonctionnalité des clés d'accès, veuillez lire attentivement les instructions ci-dessous.

Configuration matérielle requise

- Assurez-vous que votre application a suffisamment de mémoire pour gérer ces connexions.

Sécurité

Parce que les utilisateurs peuvent parfois penser que cela ne peut pas faire de mal, ils sont beaucoup plus enclins à partager un lien qu'un nom d'utilisateur et un mot de passe. Planon recommande donc de n'utiliser cette fonctionnalité que dans un cadre très strict :

- Utilisez uniquement ce type d'accès si vous n'avez vraiment pas la possibilité d'utiliser un nom d'utilisateur et un mot de passe.
- Limitez la possibilité de générer des paires de clés pour un compte dédié.
- Définissez une date d'expiration pour la paire de clés d'accès.
- Limitez les privilèges (d'accès) du compte pour lequel cette fonctionnalité est configurée.

(Il est préférable de supprimer l'accès au client Web pour ce compte.)

- Limitez les droits du compte en lien avec que ce que vous voulez accomplir.
- Activez uniquement les définitions de produits nécessaires.
- Créez un formulaire Planon Self-Service uniquement pour le compte pour lequel vous générez des clés d'accès, ne l'utilisez pas à d'autres fins.
- S'il est utilisé pour le SDK, alors vous autoriserez uniquement l'accès au SDK. S'il est utilisé pour Kiosk, alors vous autoriserez uniquement l'accès à Kiosk, etc.

Licence

Lorsque des clés d'accès sont utilisées, les licences Planon seront consommées de manière habituelle. Le type de licence applicable détermine l'usage des licences, le nombre d'utilisateurs autorisés à obtenir un accès simultané, etc. :

- Utilisateur identifié : Si le compte est connecté à une licence d'utilisateur identifié, un nombre illimité de personnes peut s'identifier car ils utilisent tous le même compte.
- Comptage de hits : chaque connexion et utilisation consommera des hits et augmentera le comptage.
- Licence simultanée : le nombre de connexions simultanées est limité au nombre de licences simultanées possédées.
- Attention à la configuration : assurez-vous que les utilisateurs standard de Planon bénéficient toujours d'une licence. Faites une estimation du nombre de connexions simultanées dont vous aurez besoin.

Concepts

Clé d'accès

Une clé d'accès est l'URL chiffrée d'un compte qui peut être utilisé pour accorder l'accès aux fonctionnalités Planon. Les clés d'accès ont pour but de permettre à plusieurs connexions authentifiées sur le même compte d'accéder à des fonctionnalités limitées.

Paire de clés

Une paire de clés est composée d'une clé privée et d'une clé publique. Ces clés sont utilisées pour chiffrer/déchiffrer la clé d'accès.

Descriptions des champs

Champs des paires de clés

Champ	Description
Généré?	Indique si une paire de clés a été générée ou non.
Généré le	Affiche la date et l'heure de la génération de la paire de clés.

Champs des clés d'accès

Champ	Description
Utilisateur	Entrez l'identifiant de l'utilisateur auquel votre compte est lié.
Date-heure de fin	Entrez une date-heure d'expiration pour la clé d'accès. Après cette date, plus personne ne pourra se connecter avec cette clé.
Clé d'accès	Ce champ contiendra la clé d'accès générée après un clic sur **Enregistrer**. Vous pouvez copier et coller cette clé.
Description	Ici, vous pouvez entrer des informations complémentaires, telles que la raison pour laquelle la clé d'accès a été générée, l'utilisateur avec lequel vous avez partagé la clé d'accès, etc.
Nom	Entrez un nom éloquent qui permette d'identifier cette clé d'accès.

Rapports de système - Autorisation

Les sections suivantes décrivent les rapports de système disponibles dans **Autorisation**.

Au niveau de **Groupes d'utilisateurs**, un rapport de système liste les différentes propriétés d'un groupe d'utilisateurs et son profil de fonction. Pour de plus amples informations, reportez-vous à Rapport Groupes d'utilisateurs.

Au niveau de **Profils de fonction** > **Droits BO**, un rapport de système fournit, pour chaque business object et pour chaque profil de fonction, une vue d'ensemble claire :

- Type d'autorisation
- Actions disponibles
- Transitions d'état possibles
- Actions étendues disponibles
- Champs disponibles (optionnel)

  Pour de plus amples informations, reportez-vous à Rapport Droits BO.

Rapport Groupes d'utilisateurs

La section suivante décrit le rapport de système disponible dans **Autorisation** > **Groupes d'utilisateurs**. En cliquant sur **Modifier les paramètres de rapport** dans le menu actions, vous pouvez définir les informations à afficher.

Paramètres	Description
Titre	Saisissez un texte qui remplacera le titre de rapport par défaut.
Sous-titre	Saisissez un texte qui sera placé sous le titre.
Afficher actions	Cochez cette case pour inclure les actions auxquelles le groupe d'utilisateurs a accès dans le rapport.
Afficher liens d'autorisation	Cochez cette case pour inclure les liens d'autorisation auxquels le groupe d'utilisateurs a accès dans le rapport.
Afficher états	Cochez cette case pour inclure les états auxquels le groupe d'utilisateurs a accès dans le rapport.
Afficher les types d'autorisation	Cochez cette case pour inclure les types d'autorisation auxquels le groupe d'utilisateurs a accès dans le rapport.
Afficher filtres d'action	Cochez cette case pour inclure les filtres d'action auxquels le groupe d'utilisateurs a accès dans le rapport.

Rapport Droits BO

La section suivante décrit le rapport de système disponible dans **Autorisation** > **Profils de fonction** > **Droits BO**. En cliquant sur **Modifier les paramètres de rapport** dans le menu actions, vous pouvez définir les informations à afficher.

Paramètres	Description
Titre	Saisissez un texte qui remplacera le titre de rapport par défaut.
Sous-titre	Saisissez un texte qui sera placé sous le titre.
Champs	Cochez cette case pour inclure les champs disponibles pour le profil de fonction dans le rapport.

Autorisation - Descriptions des champs

Utilisateur - Champs

Champs	Etape de sélection Utilisateurs
Nom d'utilisateur	Spécifiez un nom d'utilisateur.
Description	Saisissez une description de l'utilisateur.
Date de début	Spécifiez la date à partir de laquelle l'utilisateur peut se connecter. Si des utilisateurs finaux essaient de se connecter au système avant la date de début saisie, ils recevront un message leur communiquant que leur compte n'est pas encore actif.
Date de fin	Spécifiez la date à laquelle l'utilisateur n'est plus autorisé à se connecter.
	Les utilisateurs ne sont plus autorisés à se connecter à partir de la date de fin.
	Pour s'assurer que vous ne vous excluez pas accidentellement, les utilisateurs ne peuvent pas mettre de date de fin pour eux-mêmes.
Date-heure connexion précédente	Affiche la date-heure de la connexion précédente.
Mot de passe	Spécifiez un mot de passe pour l'utilisateur. Vous pouvez modifier le mot de passe à l'aide de l'option **Modifier mot de passe** dans le menu d'action.
Date d'expiration mot de passe	Spécifiez une date d'expiration mot de passe. A cette date, le mot de passe utilisateur expirera.
Mot de passe n'expire jamais	Si vous sélectionnez **Oui**, le champ **Date d'expiration mot de passe** devient inactif et le mot de passe de l'utilisateur n'expire jamais.
	Si le champ **Mot de passe n'expire jamais** est mis sur **Non**, la date d'expiration est la date actuelle plus le nombre de jours comme défini dans la date d'expiration du mot de passe.
	Pour de plus amples informations sur les configurations du calendrier, reportez-vous à *Configurations de système*.
Département	Sélectionnez le département auquel l'utilisateur est associé.

Champs	Etape de sélection Utilisateurs
Téléphone	Saisissiez le numéro de téléphone de l'utilisateur.
Photo	Vous permet d'afficher une photo de l'utilisateur.
Adresse	Sélectionnez l'adresse de l'utilisateur dans la liste de sélection.
Gestionnaire	Ceci est un champ obligatoire. Sélectionnez un gestionnaire standard dans lequel l'utilisateur sélectionné peut travailler. Un groupe d'utilisateurs dispose par défaut de tous les droits pour tous les gestionnaires. Vous pouvez au moyen d'un filtre d'autorisation sur le business object **Gestionnaire** limiter le nombre de gestionnaires et droits correspondants d'un groupe d'utilisateurs.
Fuseau horaire	Ce champ n'est pas visible par défaut. Si l'utilisation de plusieurs fuseaux horaires est activée dans votre système, ce champ est obligatoire. Vous pouvez utiliser ce champ pour associer un fuseau horaire à un utilisateur.
Détails de personne	Affiche les détails des personnes associées via le lien **Personnes**. Il affiche les détails, comme Code, Prénom, Nom complet, Code département, Numéro de téléphone et E-mail.
Détails groupe d'utilisateurs	Affiche les détails des personnes associées via le lien **Personnes**. Il affiche des détails tels que le nom de système et la description.

Configurations d'utilisateur - Champs

Champs	Description
Utilisateur	Affiche le nom de l'utilisateur sélectionné.
Traducteur	Sélectionnez **Oui** pour indiquer que l'utilisateur est un traducteur. En tant que traducteur, l'utilisateur a l'autorisation de réécrire des traductions personnalisées (définies par l'utilisateur). Les traductions définies par l'utilisateur obtiennent le statut « 2 » dans l'application. En général, lorsqu'un nouveau fichier de langue est importé, les traductions définies par l'utilisateur ne sont pas affectées. Cependant, lorsqu'un fichier de langue est importé par un « traducteur », les champs définis par l'utilisateur sont écrasés par les traductions dans le fichier de langue.
Langue Planon ProCenter	Sélectionner une langue Par exemple, sélectionnez **Anglais** pour le définir comme la langue de l'interface utilisateur.

Champs	Description
ID appareil	Entrez l'ID de l'appareil mobile utilisé par cet utilisateur dans l'application PMFS supportée par Movilizer. L'ID peut être une adresse e-mail valide ou un numéro de téléphone mobile.
Utilisateur PMFS Cloud ?	Ce champ est utilisé pour identifier les utilisateurs qui travaillent avec l'application PMFS supportée par Movilizer. Ce champ est automatiquement paramétré sur **Oui** si les paramètres utilisateur suivants sont présents : • l'**ID appareil** de l'utilisateur est rempli • l'utilisateur est lié à la définition de produits PMFS • la **Langue du Planon ProCenter** de l'utilisateur est remplie Modifier un ou plusieurs paramètres ci-dessus peut faire passer ce champ sur **Non**. Un avertissement s'affichera, vous informant que des données PMFS vont être retirées de l'appareil de l'utilisateur. Ne continuez que si telle est votre intention.
Utiliser format de 24 heures	Sélectionnez **Oui** pour configurer le format de 24 heures dans l'application de l'utilisateur.
Unité de longueur affichée	Sélectionnez une unité de longueur. Les options disponibles sont : *mètre* et *pied*.
Adresse e-mail de retour	Sélectionnez une adresse e-mail. Ce champ vous permet de mettre plusieurs adresses e-mail.
Adresse e-mail de l'émetteur	Sélectionnez une adresse e-mail dans la liste pour l'ajouter comme adresse e-mail de l'émetteur.
Adresse e-mail Exchange	Sélectionnez une adresse e-mail dans la liste pour l'ajouter comme adresse e-mail Exchange. Ce champ est utilisé par la fonction Connect d'Outlook afin de lier l'utilisateur Outlook à un compte Planon.
Cci adresse e-mail	Sélectionnez une adresse e-mail pour l'ajouter comme adresse e-mail Cci.
Thème de couleurs	Vous permet de configurer un thème de couleur.
Longueur nom de champ (en pixels)	Spécifiez la longueur de nom de champ. La longueur de nom de champ spécifiée par défaut est de 200 pixels.
Afficher nom des boutons dans la barre d'outils	Sélectionnez **Oui** pour afficher les noms des boutons dans la barre d'outils.
Sélectionner automatiquement premier élément de la liste	Sélectionnez **Oui** pour mettre en surbrillance et sélectionner automatiquement le premier élément de la liste des éléments.

Liens d'autorisation - Champs

Champ	Description
Nom de système	Spécifiez un nom de système.
Définition de champ Business object	Sélectionnez un business object référencé pour lequel un filtre d'autorisation est créé ayant un lien à l'action **Lecture**. Le pop-up de sélection affiche tous les champs de référence du business object que vous avez sélectionnés au premier niveau. Sélectionnez par exemple le business object **Objets** qui a un filtre d'autorisation ayant un lien à l'action **Lecture** dans **Filtres d'autorisation** > **Filtres** > **Filtres d'action**. Seuls les champs de référence du type *entier* sont supportés dans les liens d'autorisation. Les champs de référence du type *chaîne* ou *chaîne libre* ne sont pas supportés.
Actif?	Cliquez sur **Oui** pour activer le lien.

Profils de fonction - Champs

Champ	Description
Nom de système	Saisissez un nom pour le profil de fonction.
Description	Saisissez une description pour le profil de fonction
Types d'autorisation standard	Sélectionnez le type d'autorisation qui sera utilisé pour tous les business objects lorsqu'un nouveau profil de fonction est créé ou lorsqu'un business object est paramétré sur **Autorisé**. • **Invisible** • **Lecture seule** • **Toutes fonctionnalités** Ce paramètre affecte uniquement les business objects nouvellement autorisés. Si vous paramétrez un objet sur **Autorisé** dans **FieldDefiner** ou si vous ajoutez un champ à un business object, le type d'autorisation spécifié ici sera automatiquement appliqué.  Exemple : Le profil de fonction d'un administrateur Planon doit être paramétré sur Toutes fonctionnalités, pour que chaque business object autorisé soit automatiquement ajouté au profil de fonction d'administrateur avec un accès à l'ensemble des fonctionnalités. Pour un profil de fonction nécessitant des propriétés en lecture seule, la valeur par défaut doit être paramétrée sur **Lecture seule**.

Champ	Description
	Vous pourrez toujours affiner les autorisations spécifiques de chaque business object plus tard. (Voir Spécifier des autorisations de business objects).

Droits BO - Champs

Champ	Description
Nom	Affiche le nom du business object sélectionné.
Profil de fonction	Affiche le nom du profil de fonction pour lequel vous spécifiez des autorisations.
Définition de Business object	Affiche le nom du système du business object défini par l'utilisateur pour lequel vous spécifiez des autorisations.
Type d'autorisation	Affiche le type d'autorisation par défaut attribué au profil de fonction. Vous pouvez modifier la valeur de chaque business object autorisé pour l'une des options suivantes : • **Invisible** Sélectionnez cette option si vous ne voulez pas rendre le business object disponible pour le profil de fonction sélectionné. • **Lecture seule** Sélectionnez cette option si vous voulez que le business object soit uniquement disponible en mode lecture seule pour le profil de fonction sélectionné. • **Spécifique** Sélectionnez cette option si vous souhaitez effectuer des réglages spécifiques pour : • Champs • Actions • Transitions d'état • Actions supplémentaires Si vous sélectionnez **Spécifiques**, un message s'affiche et vous invite à indiquer si l'autorisation initiale doit être en **Lecture seule**. Si vous cliquez sur **Oui**, les autorisations relatives aux champs, actions, transitions d'état et actions supplémentaires seront, dans un premier temps, en lecture seule. Vous pouvez modifier ces réglages selon vos besoins au niveau de **Détails**. (Voir Spécifier des autorisations). Si vous cliquez sur **Non**, les détails ne seront pas accessibles.

Champ	Description
	La modification du type d'autorisation d'un business object est soumise à la journalisation de sécurité. Pour de plus amples informations sur ce sujet, reportez-vous à *Administrator's Guide* > *Security logging*.

Détails - champs

Champs

Champ	Description
Droit	Affiche le business object pour lequel vous spécifiez des autorisations.
Champ	Affiche le nom du champ sélectionné.
Autorisations	Sélectionnez le type d'autorisation spécifique que vous souhaitez appliquer au champ sélectionné. Les options disponibles sont : • **Modification non-autorisée** (valeur par défaut) Passe le champ en lecture seule. • **Modification autorisée** Rend le champ modifiable. • **Modification et transfert autorisés** Rend le champ modifiable. Vous pouvez enregistrer une fois le business object en assignant à ce champ une valeur non-comprise dans votre filtre d'autorisations, ce qui vous permet de modifier la valeur une fois. Par exemple, pour changer le propriétaire d'un problème. L'ajout, la suppression et la mise à jour des autorisations de champs sont soumis à la journalisation de sécurité. Pour de plus amples informations sur ce sujet, reportez-vous à *Administrator's Guide* > *Security logging*.

Actions

Champ	Description
Droit	Affiche le business object pour lequel vous spécifiez des autorisations.
Action	Affiche l'action sélectionné. Dans Associer des actions, vous avez précédemment défini les actions disponibles dans la liste des éléments.

Transitions d'état

Champ	Description
Droit	Affiche le business object pour lequel vous spécifiez des autorisations.
Action	Affiche l'action sélectionné. Dans Associer des transitions d'état, vous avez précédemment défini les actions disponibles dans la liste des éléments.

Actions supplémentaires

Champ	Description
Droit	Affiche le business object pour lequel vous spécifiez des autorisations.
Extension utilisateur - Client	Affiche l'action sélectionné. Dans Associer des actions supplémentaires, vous avez précédemment défini les actions supplémentaires disponibles dans la liste des éléments.

Champs des clés d'accès

Champ	Description
Utilisateur	Entrez l'identifiant de l'utilisateur auquel votre compte est lié.
Date-heure de fin	Entrez une date-heure d'expiration pour la clé d'accès. Après cette date, plus personne ne pourra se connecter avec cette clé.
Clé d'accès	Ce champ contiendra la clé d'accès générée après un clic sur **Enregistrer**. Vous pouvez copier et coller cette clé.
Description	Ici, vous pouvez entrer des informations complémentaires, telles que la raison pour laquelle la clé d'accès a été générée, l'utilisateur avec lequel vous avez partagé la clé d'accès, etc.
Nom	Entrez un nom éloquent qui permette d'identifier cette clé d'accès.

Champs des paires de clés

Champ	Description
Généré?	Indique si une paire de clés a été générée ou non.

Champ	Description
Généré le	Affiche la date et l'heure de la génération de la paire de clés.

Index

R

S

T

U