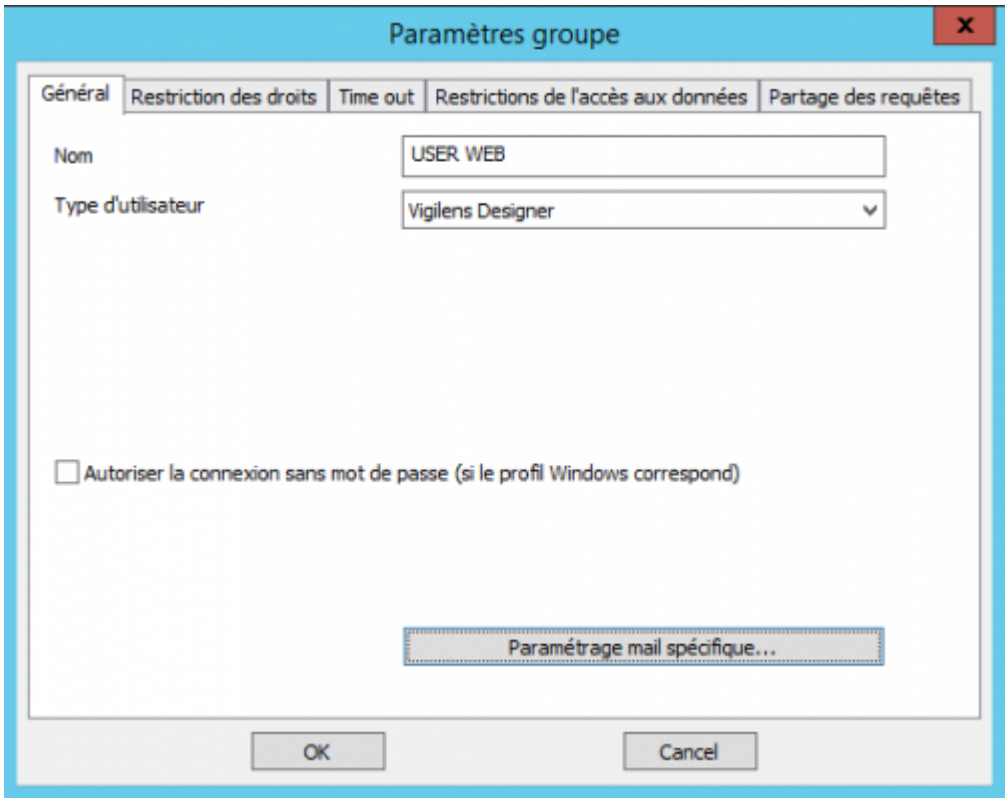
Menu Gestion > Groupe

Ce menu est utilisé en conjonction avec la fenêtre **Gestion des Groupes**. Voir Admintool. Si certains boutons sont grisés, c'est qu'il faut sélectionner un groupe dans la fenêtre Gestion des Groupes.

Propriétés des Groupes

Lorsque nous créons ou modifions un groupe, nous avons accès à l'ensemble de ses propriétés :

Général



Nom

Nom du groupe, sachant que le groupe par défaut ne peut pas être renommé.

Utilisateur

il y a 2 types possibles d'utilisateur.

- Vigilens Viewer / Web : que de la consultation de requêtes existantes
- Vigilens Designer : possibilité de créer de nouvelles requêtes.

Les types disponibles dépendent de la licence.

Connexion Windows

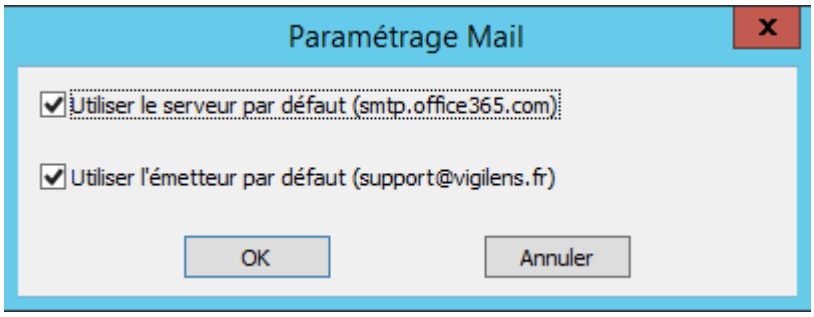
Permet de lancer Vigilens sans que la fenêtre de connexion s'affiche, si le nom de l'utilisateur Windows correspond au nom de l'utilisateur Vigilens

Paramétrage mail spécifique

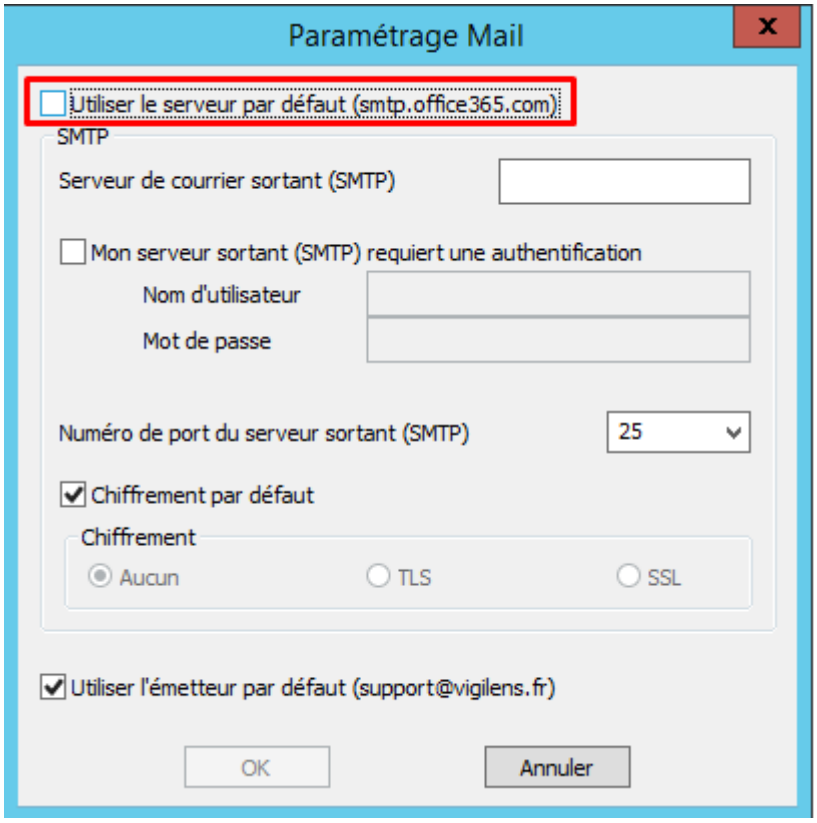
On peut également affecter un serveur mail différent et/ou un nom d'expéditeur différent pour ce groupe par rapport au serveur par défaut.

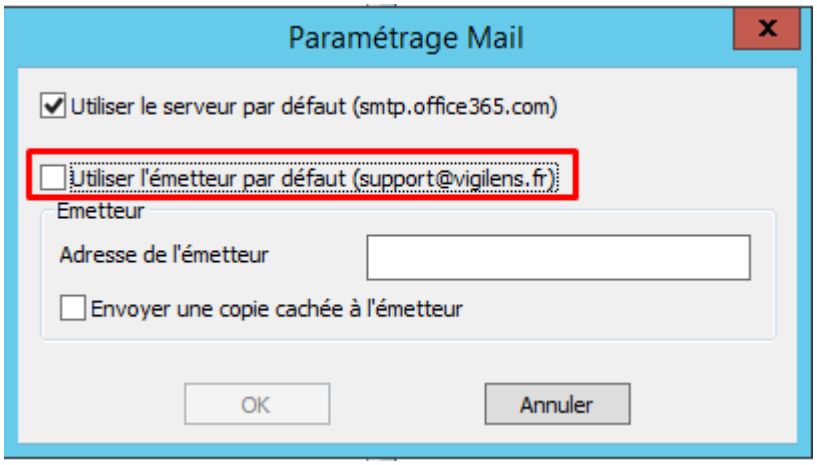
On peut paramétrer le serveur mail au niveau de l'utilisateur, et **dans ce cas il prime sur ce qui est défini au niveau groupe.**

Le fait de spécifier les paramétrages mail au niveau de l'utilisateur permet d'avoir une adresse de retour personnalisée.

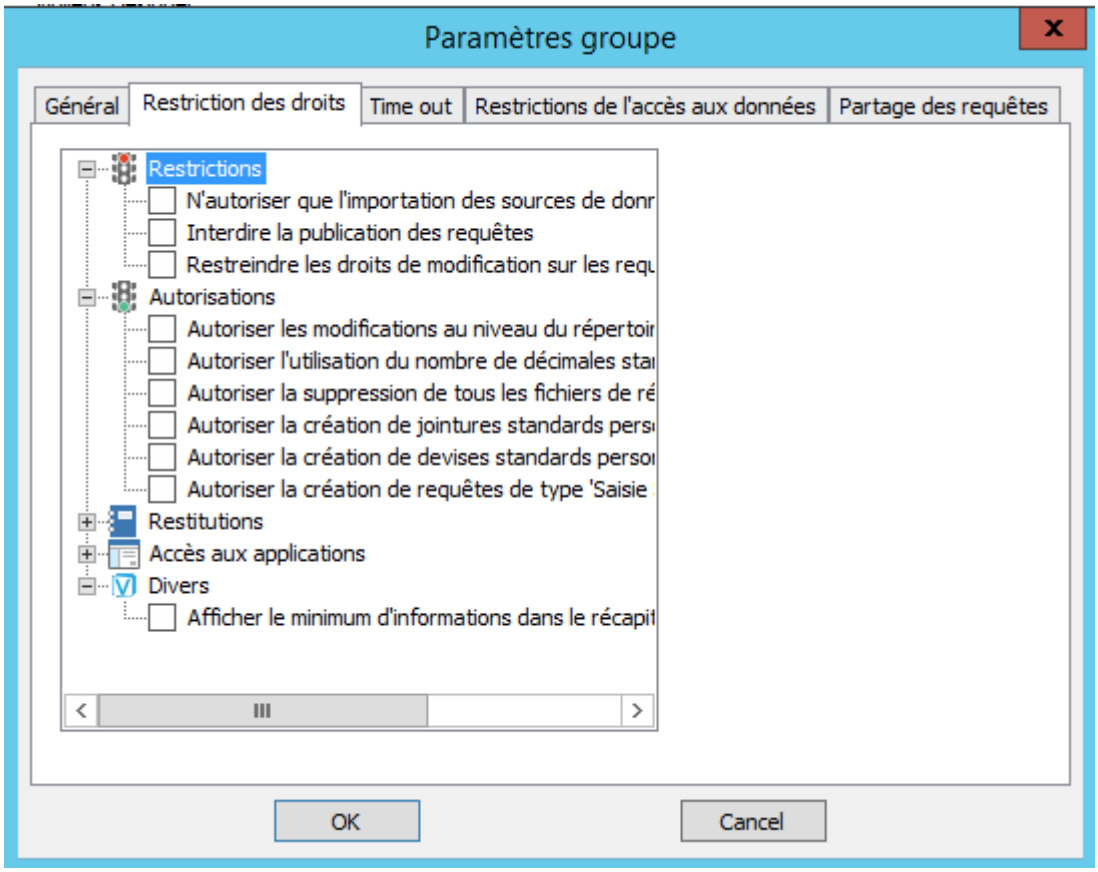


Décocher l'une ou les deux case ouvre la saisie aux paramètres spécifiques à ce groupe.

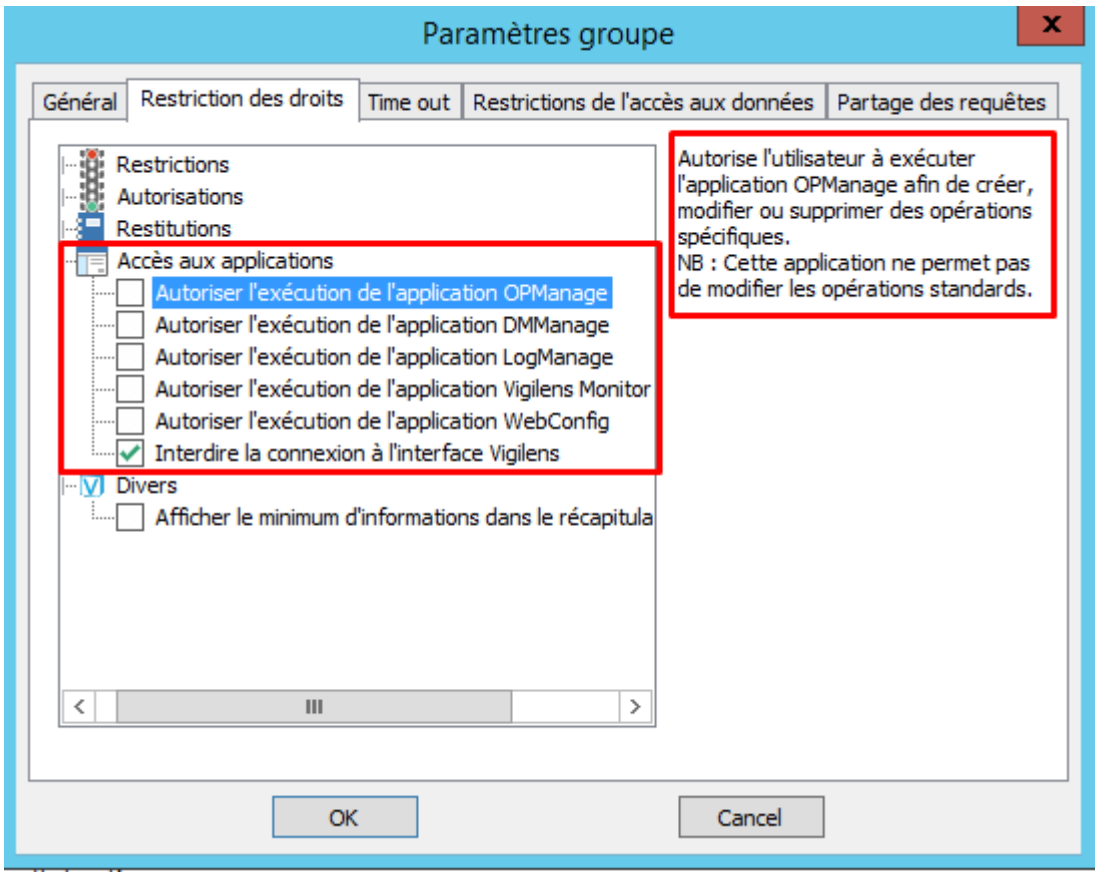




Restriction des droits



C'est notamment ici que l'on définit à quelles applications Vigilens un groupe peut accéder. On remarque que pour chaque droit on a, en haut à droite, une aide contextuelle.



Si une de ces cases est cochée au niveau groupe, elle le sera aussi au niveau des utilisateurs du groupe et ne sera pas décochable

Restrictions

- N'autoriser que l'importation des sources de données partagées
  - Restreint l'utilisation des sources de données aux seules sources partagées par l'administateur, en ne permettant pas à l'utilisateur de créer ou de modifier des sources de données.
- Interdire la publication des requêtes
  - Interdit à l'utilisateur de publier les requêtes qu'il a créés.
- Restreindre les droits de modification sur les requêtes
- Interdit à l'utilisateur de modifier tous ce qui se rapporte à la source de données, aux tables et aux jointures des requêtes existantes.L'utilisateur ne peut pas créer de nouvelles requêtes. Il ne peut que modifier certaines caractéristiques (conditions, champs à restituer...) des requêtes existantes.

Autorisations

- Autoriser les modifications au niveau du répertoire des requêtes partagées
  - Autorise l'utilisateur à effectuer des modifications au niveau du répertoire des requêtes partagées : ajout, modification, suppression de sous-répertoires ou de requêtes.
- Autoriser l'utilisation du nombre de décimales standard pour les montants en devises
  - Autorise l'utilisateur à ne pas renseigner les informations liées au champs correspondant à des montants en devise (le nombre de décimales utilisé pour ces montant étant alors celui spécifié au niveau du dictionnaire de données).
- Autoriser la suppression de tous les fichiers de résultats
  - Autorise l'utilisateur à supprimer tous les fichiers de résultats, y compris ceux qui ont été créés par un autre utilisateur.
- Autoriser la création de jointures standards personnelles
  - Autorise l'utilisateur à créer ses propres jointures standards qui pourront être utilisées par les autres utilisateurs.
- Autoriser la création de devises standards personnelles
  - Autorise l'utilisateur à créer ses propres devises standards qui pourront être utilisées par les autres utilisateurs.
- Autoriser la création de requêtes de type 'Saisie SQL'
  - Autorise l'utilisateur à créer des requêtes de type 'Saisie SQL'.

Restitutions

- Interdire la génération de fichier
  - Interdit à l'utilisateur de procéder à des restitutions sous forme de fichier.
- Autoriser la restitution vers des fichiers particuliers
  - Autorise l'utilisateur à spécifier un chemin ainsi qu'un nom de fichier particulier qui sera utilisé pour la restitution des résultats.

- Interdire les impressions
  - Interdit à l'utilisateur de procéder à des restitutions sous forme d'impression.
- Interdire les envois de mail
  - Interdit à l'utilisateur de procéder à des restitutions sous forme d'envoi de mail.
- Autoriser l'export vers une base de données
  - Autorise l'utilisateur à se servir du type de restitution : _ckgedit_QUOTckgedit>Export vers une base de données_ckgedit_QUOTckgedit>, qui lui permet d'insérer les lignes de résultat de sa requête dans une table d'une base de données.
- Autoriser la création de table lors de l'export vers une base de données
  - Autorise l'utilisateur, lors de l'export vers une base de données, à spécifier une table cible n'existant pas dans la base.
- Autoriser la purge de la table cible lors l'export vers une base de données
  - Autorise l'utilisateur, lors de l'export vers une base de données, à demander la suppression des enregistrements éventuellement présents dans la table cible avant l'export.

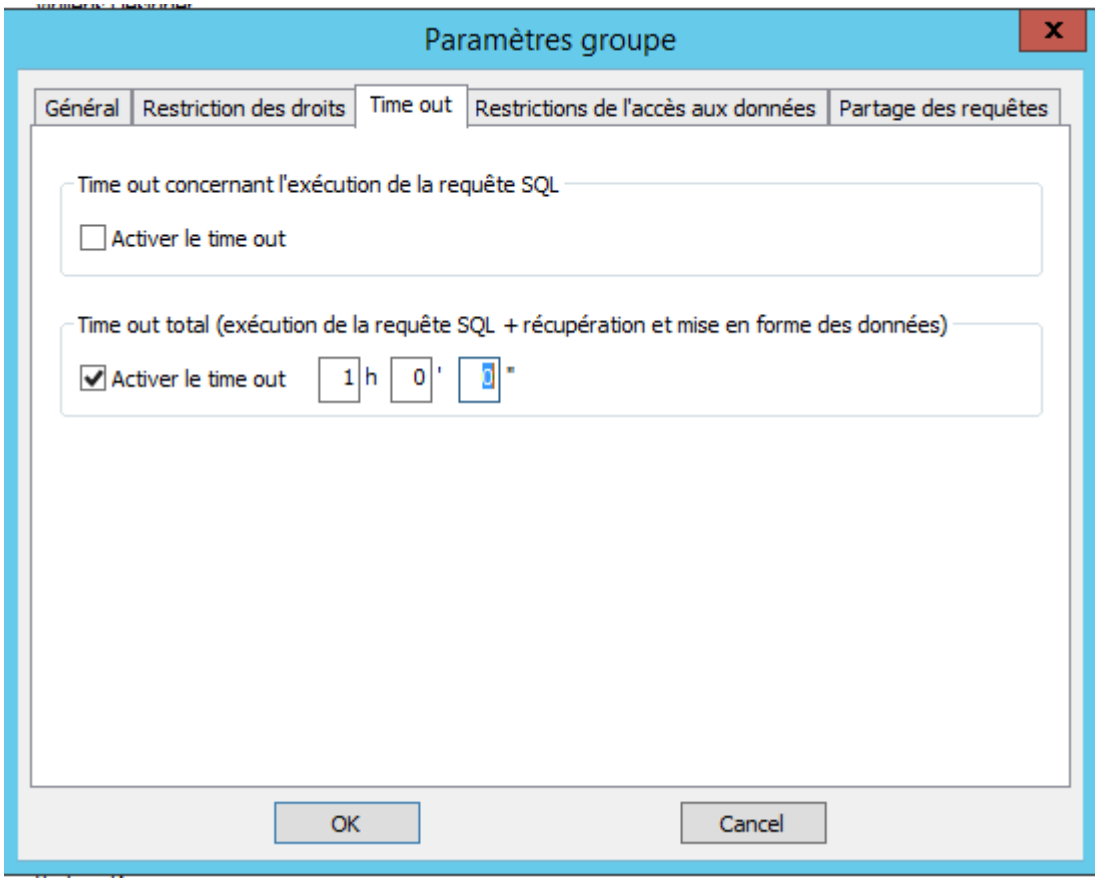
Accès aux Applications

- Autoriser l'exécution de l'application OPManage
  - Autorise l'utilisateur à exécuter l'application OPManage afin de créer, modifier ou supprimer des opérations spécifiques. NB : Cette application ne permet pas de modifier les opérations standards.
- Autoriser l'exécution de l'application DMManage
  - Autorise l'utilisateur à exécuter l'application DMManage afin de renommer et attribuer une description aux tables et aux champs.
- Autoriser l'exécution de l'application LogManage
  - Autorise l'utilisateur à exécuter l'application LogManage afin de gérer les connexions des utilisateurs.
- Autoriser l'exécution de l'application Vigilens Monitor
  - Autorise l'utilisateur à exécuter l'application Vigilens Monitor permettant la création de pages Web incorporant des requêtes Vigilens exécutées automatiquement à une fréquence donnée.
- Autoriser l'exécution de l'application WebConfig
  - Autorise l'utilisateur à exécuter l'application WebConfig afin de gérer les paramètres liés à Vigilens Web.
- Interdire la connexion à l'interface Vigilens
  - Interdit à l'utilisateur de se connecter à l'interface Vigilens. Cet utilisateur ne peut être utilisé que pour ce connecter via une ligne de commande ou une URL.

Divers

- Afficher le minimum d'informations dans le récapitulatif des requêtes
  - Permet de n'afficher qu'un minimum d'informations au niveau du récapitulatif des requêtes (source de données et descriptif de la requête).

Time Out



Il y a 2 time out :

- le premier est purement relatif à la base de donnée : c'est le temps maximum entre la soumission par Vigilens de la requête au serveur SQL et la fin de l'exécution. Ce time out est géré par la base de données elle-même.
- le deuxième est géré par Vigilens : par rapport au premier, il prend également en compte le temps de récupération des données.

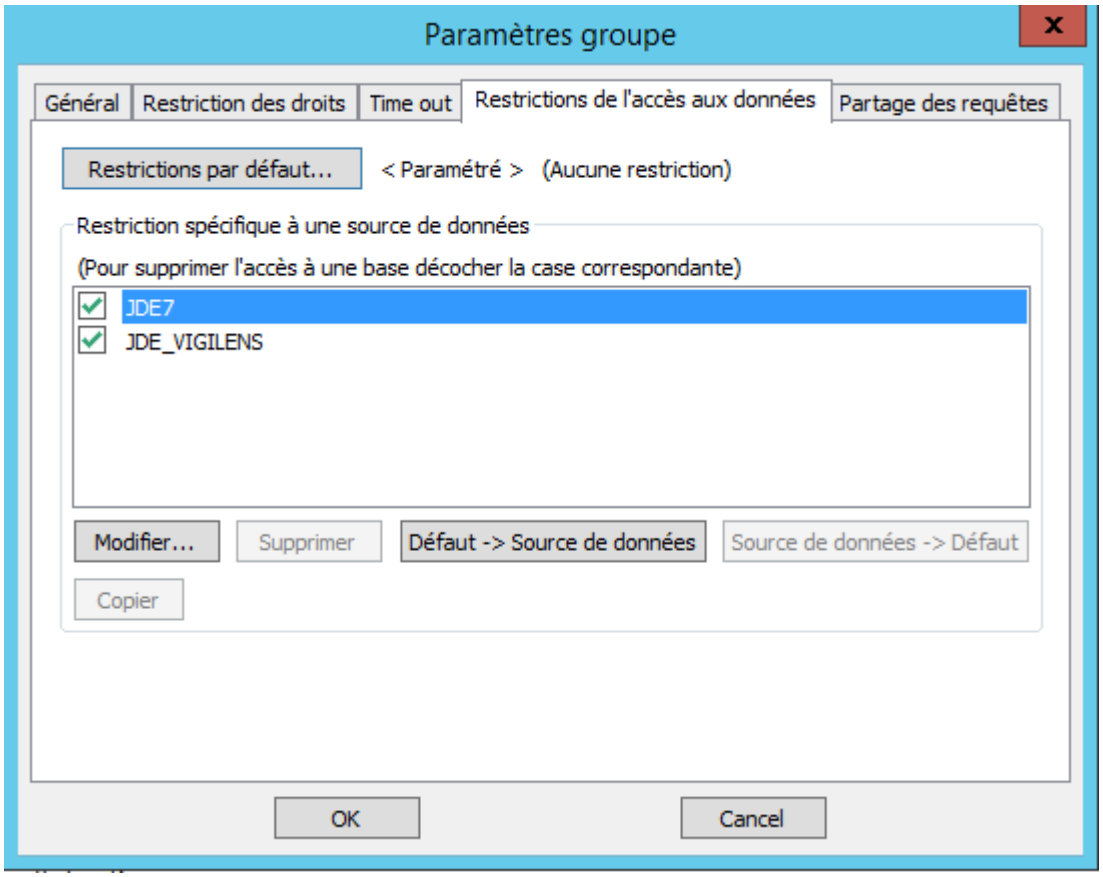
Ces notions de time-out peuvent être définies au niveau :

1. du groupe
2. de l'utilisateur
3. de la requête

Les temps doivent forcément être de plus en plus petits quand on passe de groupe à utilisateur puis utilisateur à requête.

Le time out SQL étant géré au niveau du système de base de données, il n’est pas disponible sur toutes les plates-formes.

Restriction de l'accès aux données



Il peut être utile de bloquer certains groupes pour les empêcher de consulter certaines informations sensibles de l'entreprise.
Il est possible d'interdire l'utilisation d'une source de données en la décochant dans la liste.
Pour chaque source de données, Vigilens permet d'imposer des restrictions au niveau des :

- Environnements (pour les sources de type JDE/World)
- Tables
- Alias (pour les sources de type JDE/World)
- Champs
- Valeurs

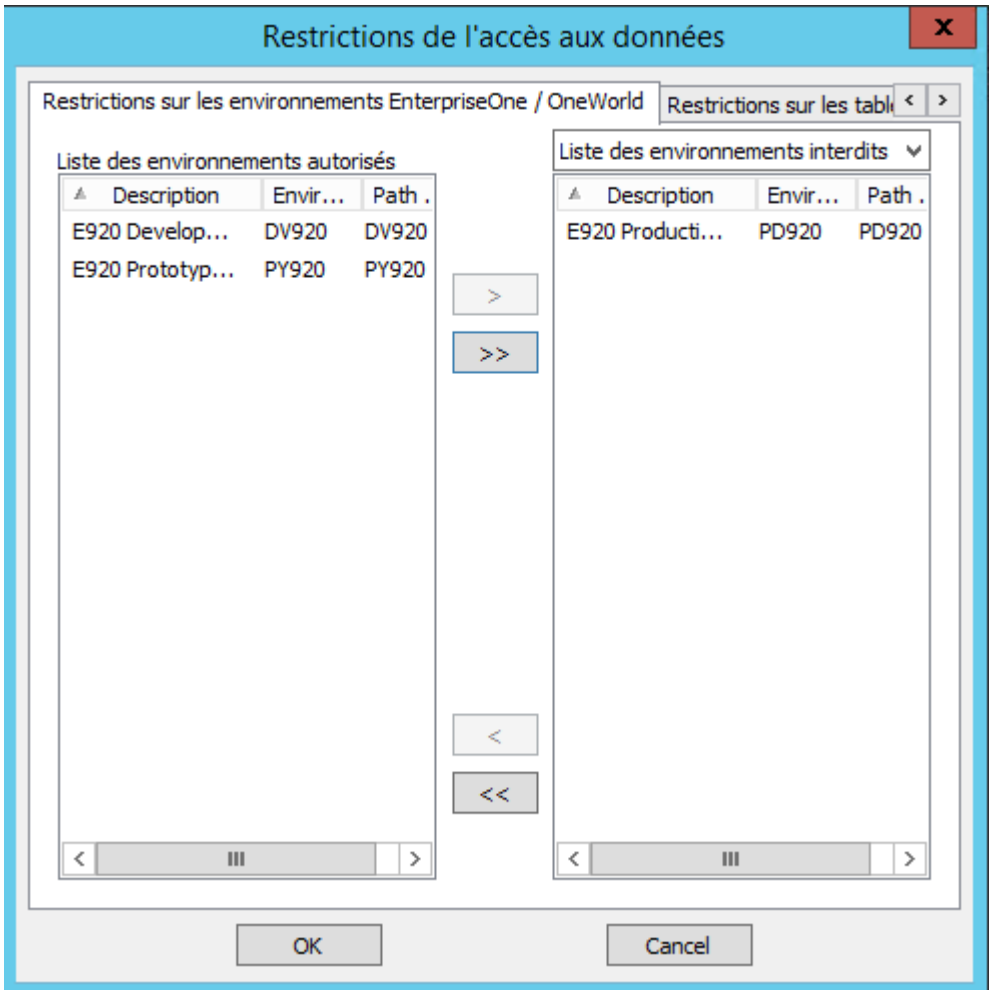
Le bouton `Restrictions par défaut…` donne accès au paramétrage valable pour toutes les sources de données ne possédant pas de paramétrage spécifique.
L'enchaînement des écrans est en tout point similaire au paramétrage d'une source de donnée en particulier.

De manière générale, toutes les restrictions suivantes fonctionnent sur un système soit BlackList soit WhiteList : soit on explicite les éléments à interdire et tout le reste est autorisé, soit on explicite les éléments à autoriser et tout le reste est interdit. Le fonctionnement BlackList/WhiteList est défini au niveau du groupe et ne peux pas être

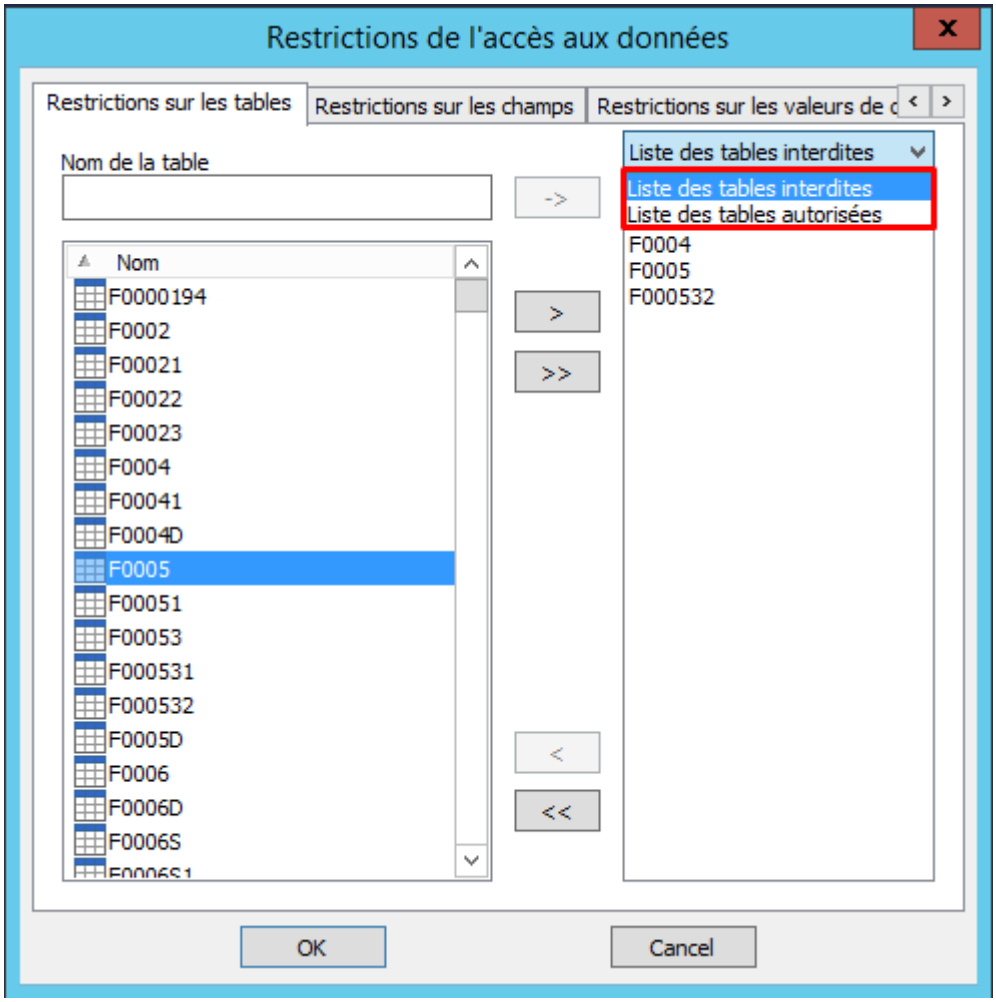
changé au niveau utilisateur

On peut ainsi :

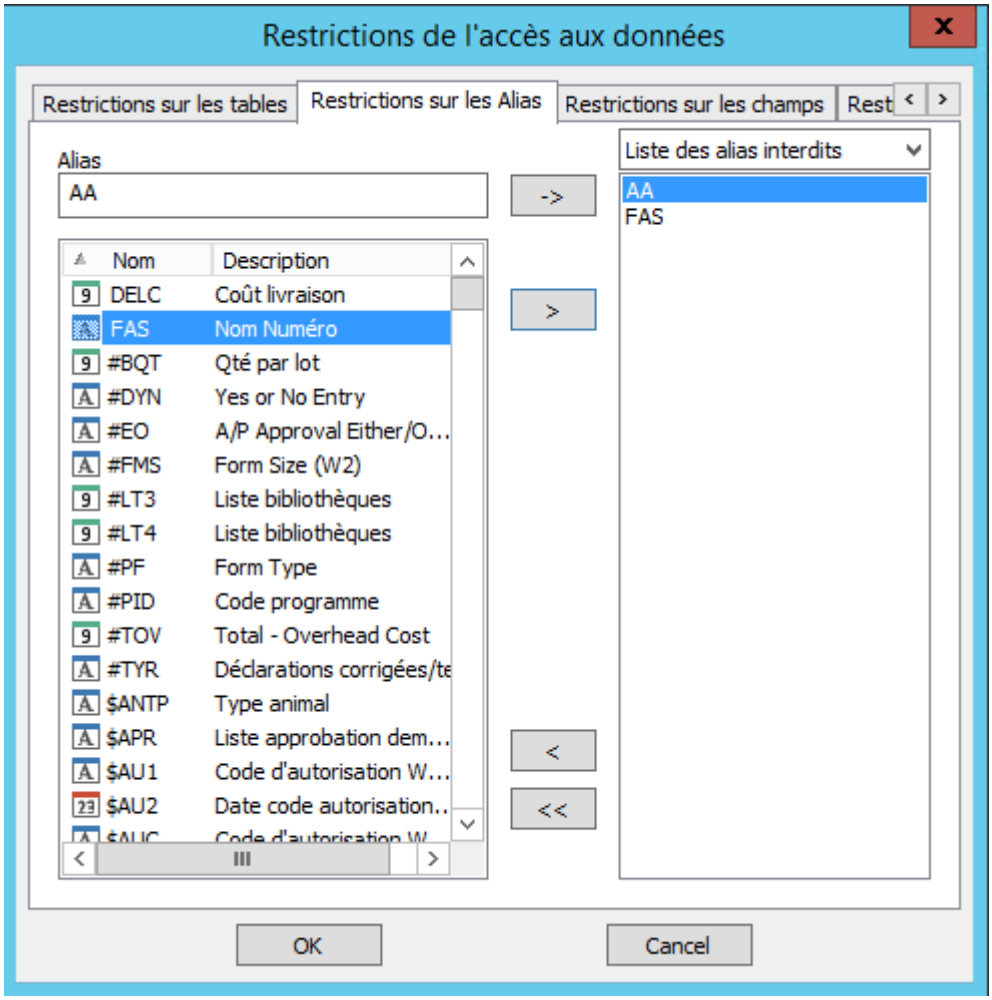
- empêcher/autoriser l'accès à des environnement, pour les sources de données JDE/World



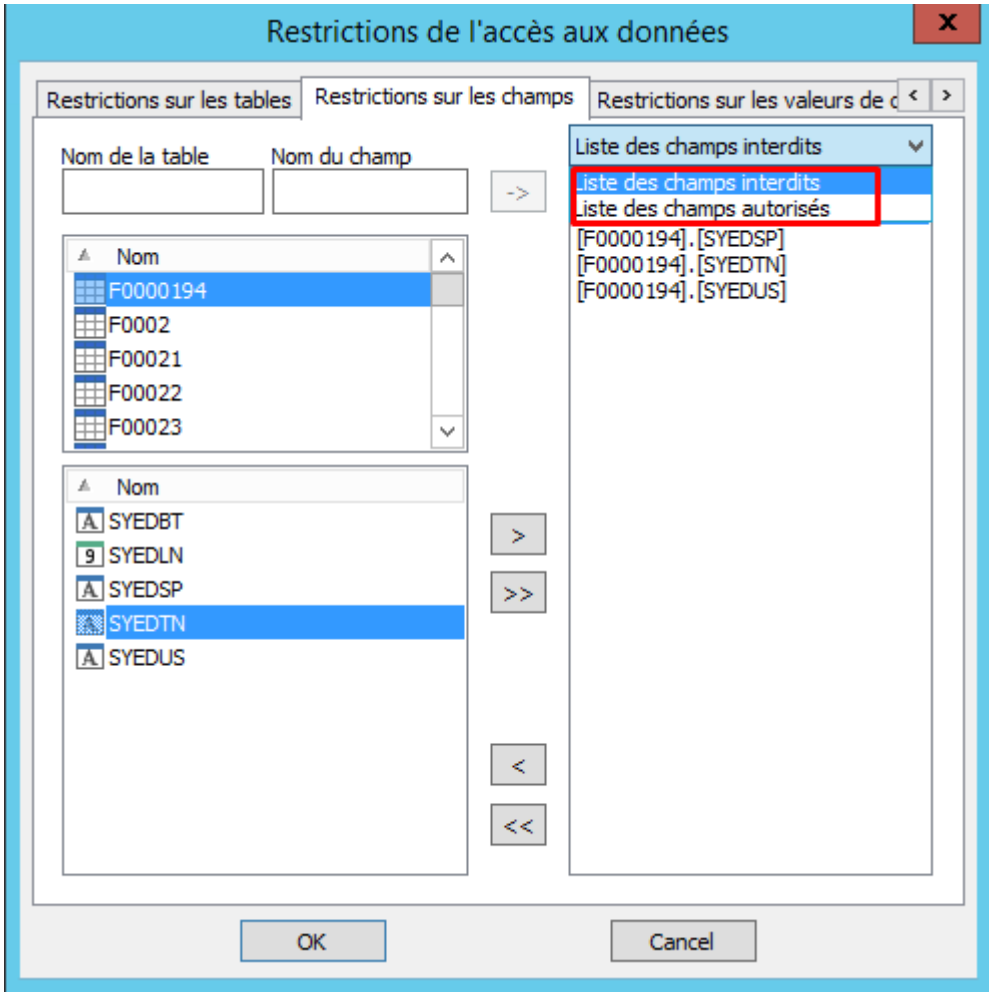
- empêcher/autoriser la consultation d'une table en particulier



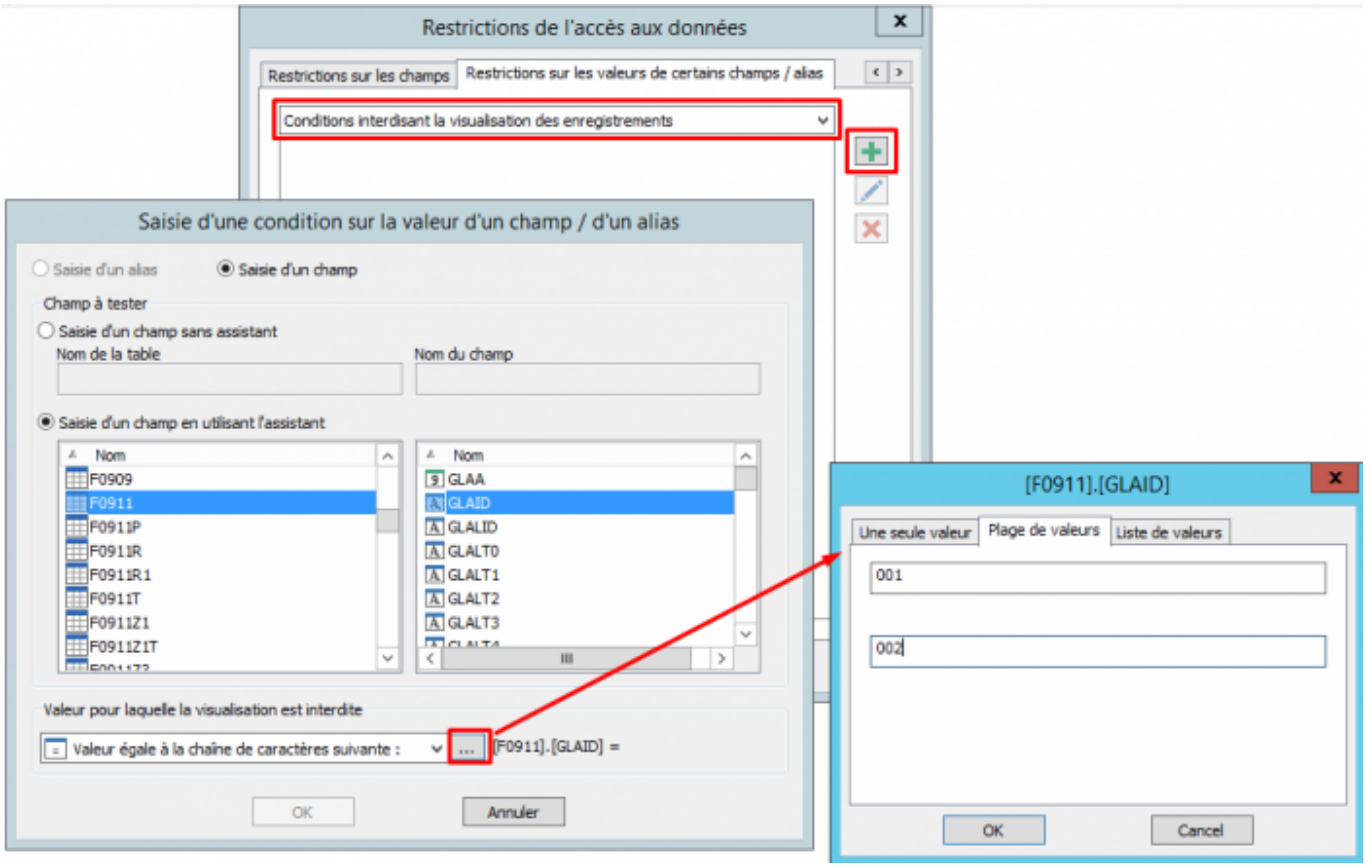
- empêcher/autoriser l'accès à un alias (JDE/World)



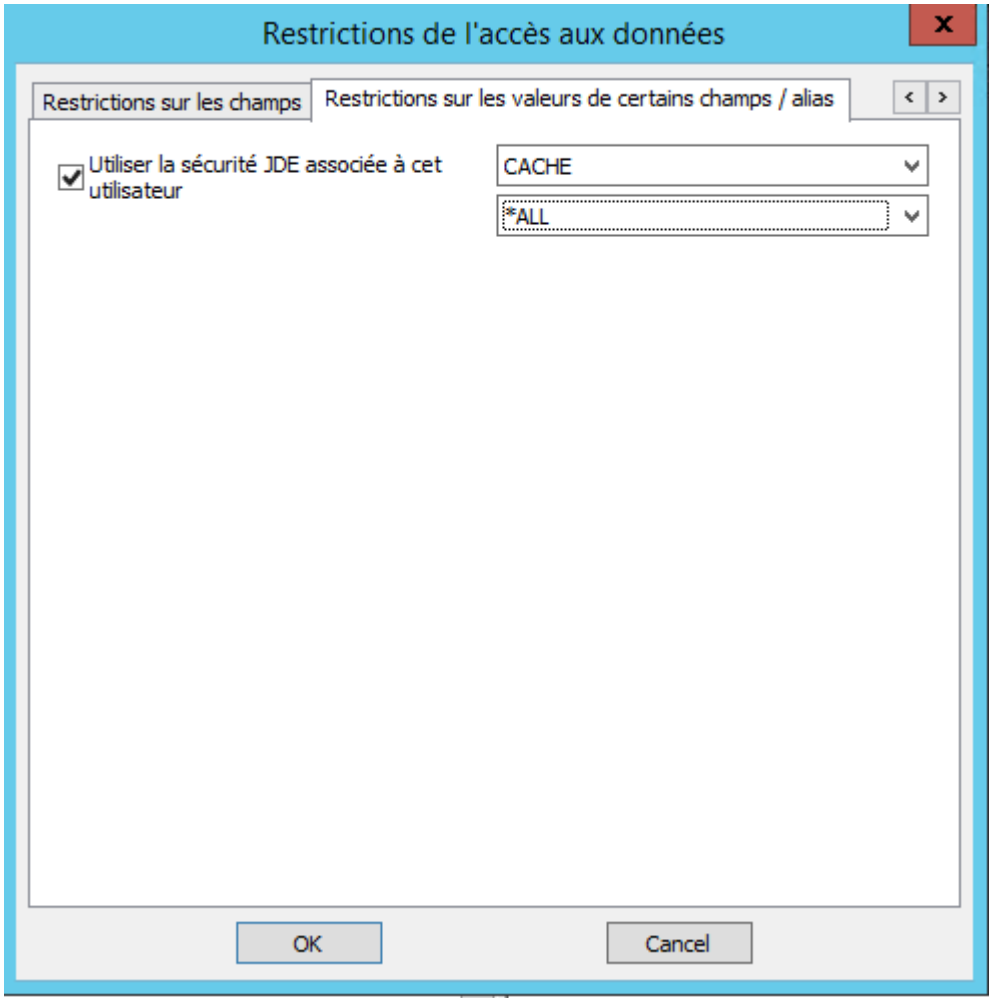
- empêcher/autoriser la consultation de certaines colonnes d'une table



- empêcher/autoriser la consultation de certaines lignes d'une table selon des critères sur une colonne de la table. Le critère peut être une unique valeur, une plage de valeur, ou une liste de valeurs.



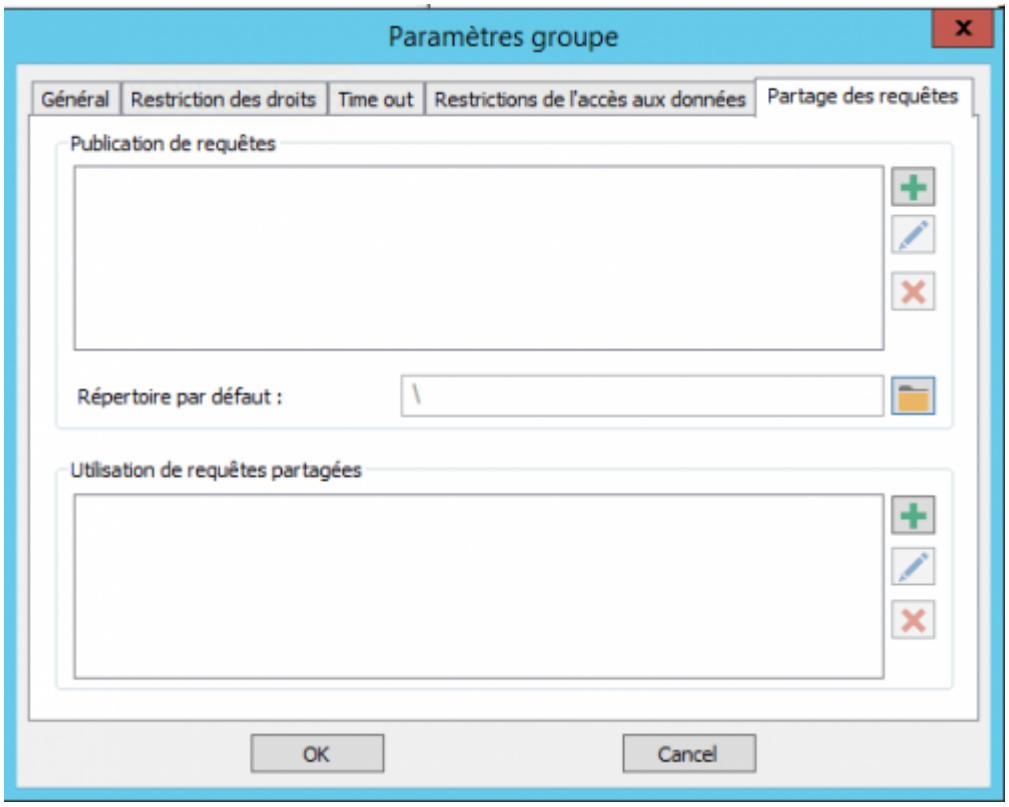
Si la source de données est de type JDE/World, on a en plus le choix d'utiliser la sécurité JDE associée à un utilisateur et l'un des ses rôles (ou bien prendre en considération **tous** ses rôles avec la valeur “*ALL”



Partage des requêtes

Ce paramétrage permet de :

- Définir l'endroit où l'utilisateur peut déposer les requêtes qu'il désire partager
- Spécifier les requêtes partagées qu'il peut utiliser (l'utilisateur a accès à la totalité de l'arborescence des répertoires spécifiés)



- Publication des requêtes : liste des dossiers partagés accessibles lors de la publication des requêtes
    - Répertoire par défaut : proposé par défaut lors de la publication des requêtes
- Utilisation des requêtes partagées : liste des dossiers partagés accessibles via l'interface web (ou Vigilens Designer)

Changer la Langue