

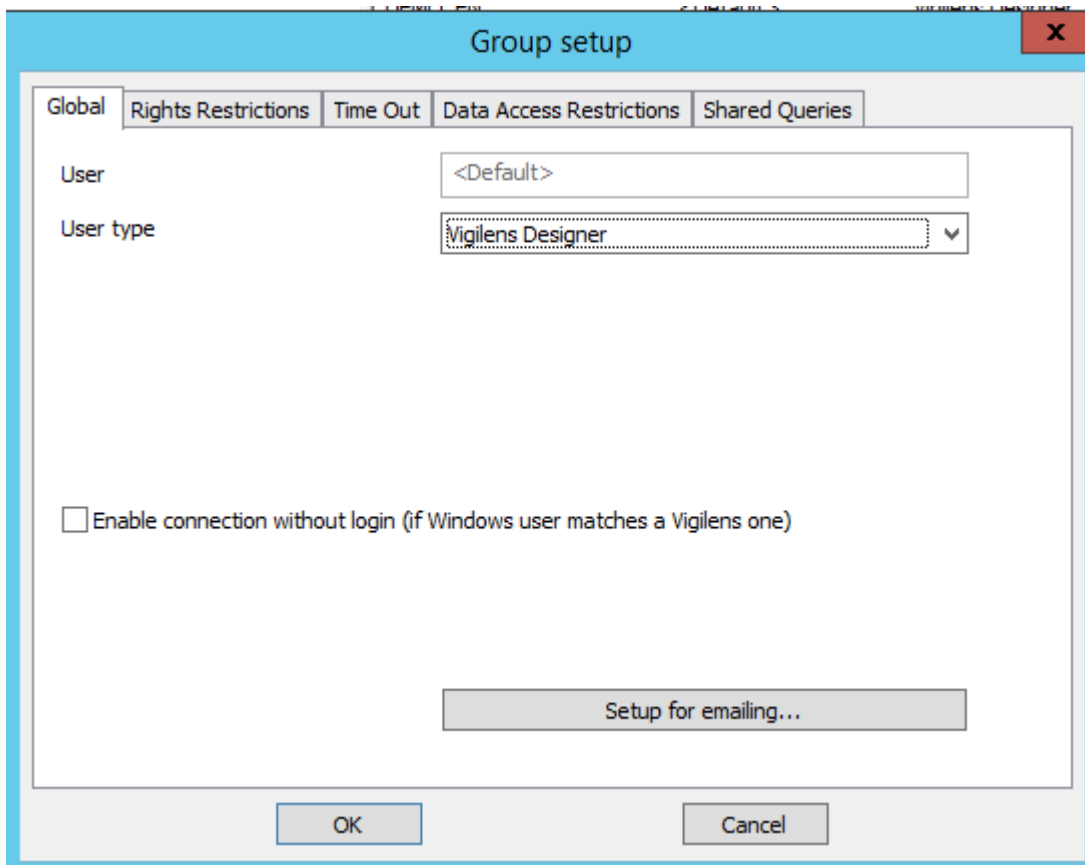
Managent menu > Group

This menu is used in conjunction with the **Group Management** window. See [Admintool](#). If some of the buttons are grayed out, it means that you need to select a group in the Group Management window.

Groups Properties

When we create or modify a group, we have access to all its properties:

Global



Name

Name of the group, knowing that the default group cannot be renamed.

User type

there are 2 possible types of users.

- Vigilens Viewer / Web: only consultation of existing queries
- Vigilens Designer: possibility to create new queries.



The available types depend on the license.

Windows connexion

Allows to launch Vigilens without the login window being displayed, if the Windows user name corresponds to the Vigilens user name.

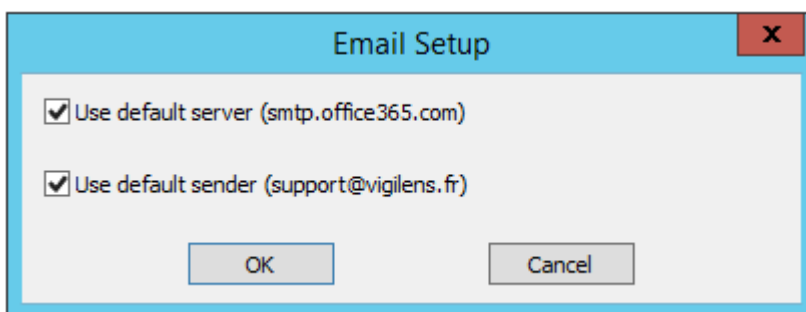
Setup for emailing

You can also assign a different mail server and/or a different sender name for this group than the default server.

The mail server can be set at the user level, in which case it takes precedence over what is set at the group level.



Specifying mail settings at the user level allows you to have a personalized return address.



Unchecking one or both checkboxes opens the entry to the parameters specific to this group.

Email Setup [X]

Use default server (smtp.office365.com)

SMTP

SMTP Server for outgoing mail

SMTP Server requires authentication

User Name

Password

SMTP Server Port

Default encryption

Encryption

None TLS SSL

Use default sender (support@vigilens.fr)

OK Cancel

Email Setup [X]

Use default server (smtp.office365.com)

Use default sender (support@vigilens.fr)

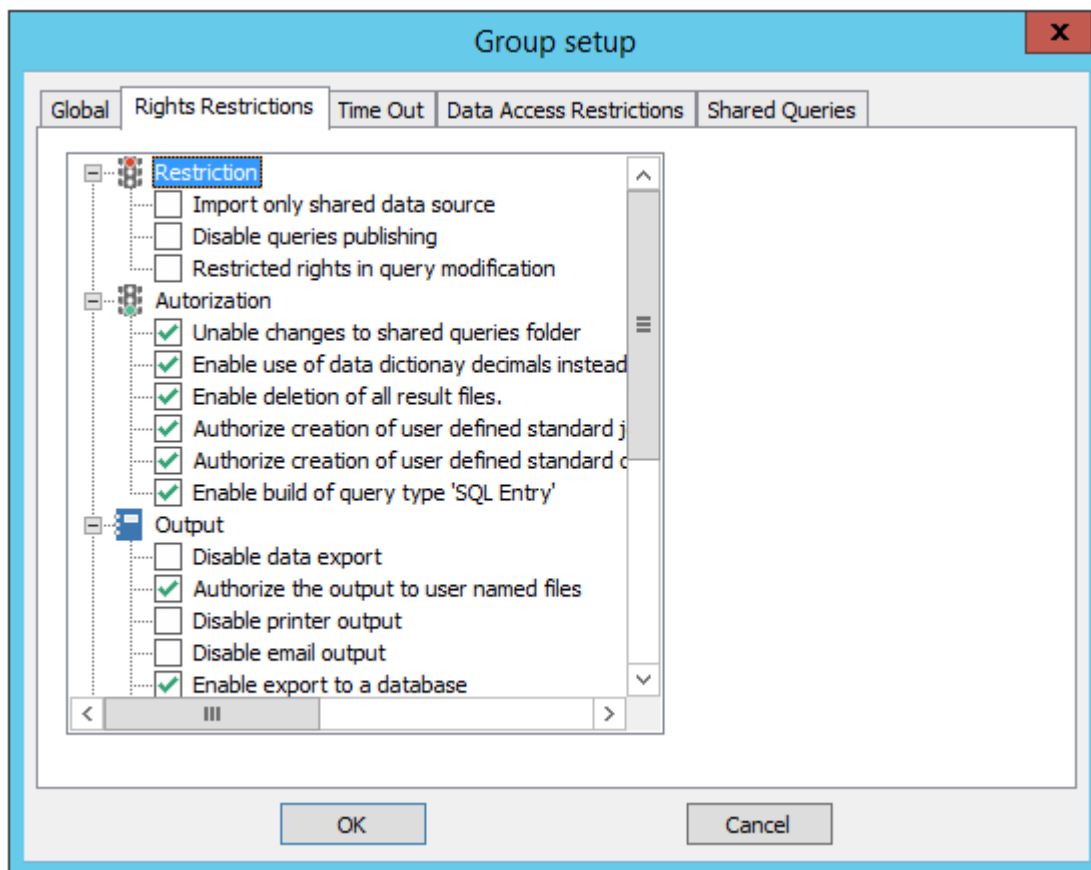
Sender

Sender address

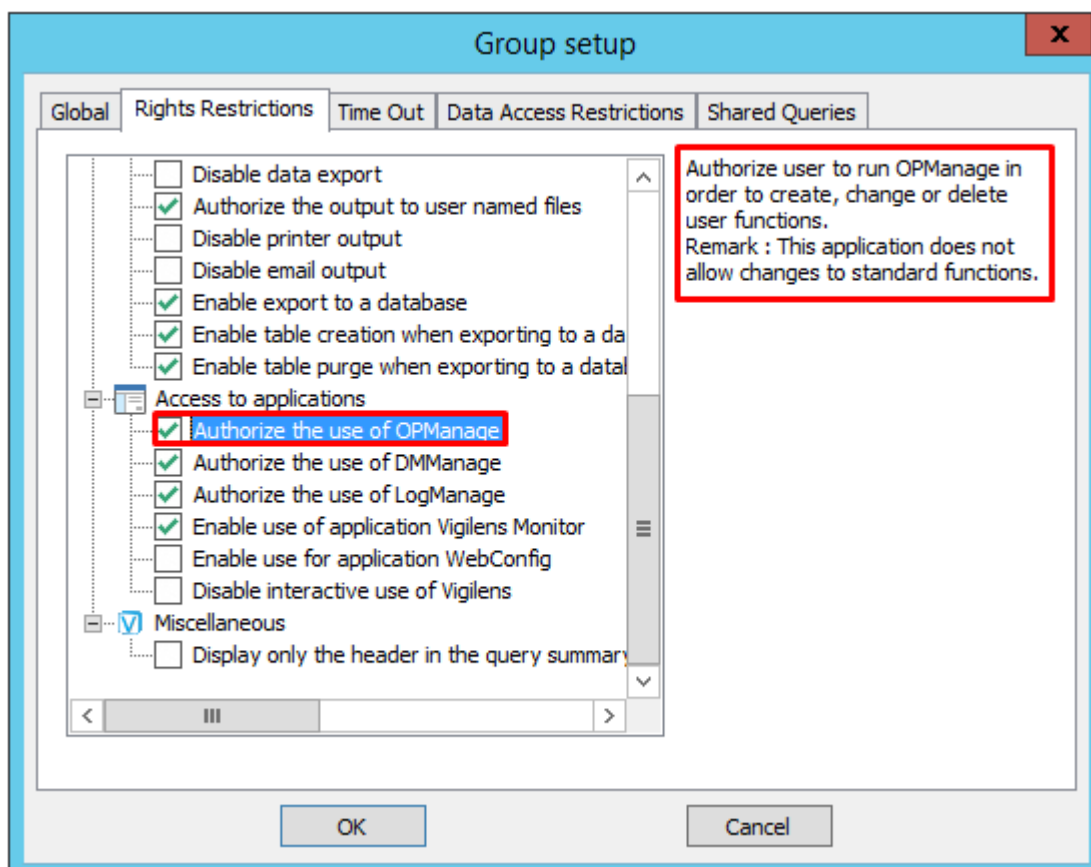
Copy for sender

OK Cancel

Rights restrictions



This is where you define which Vigilens applications a group can access. You can see that for each right, there is a contextual help in the top right corner.





If one of these boxes is checked at the group level, it will also be checked at the group user level and will not be uncheckable.

Restriction

Authorization

Output

Access to applications

Time Out

The screenshot shows a 'Group setup' dialog box with a blue title bar and a red close button. It has five tabs: 'Global', 'Rights Restrictions', 'Time Out', 'Data Access Restrictions', and 'Shared Queries'. The 'Time Out' tab is active. It contains two sections:

- SQL run time out:** A checked checkbox 'Enable time out' followed by a time picker set to 0 h, 3', 0\".
- Total time out (SQL run + Data download and display):** A checked checkbox 'Enable time out' followed by a time picker set to 0 h, 4', 0\".

At the bottom, there are 'OK' and 'Cancel' buttons.

There are 2 times out:

- the first one is purely relative to the database: it is the maximum time between the submission by Vigilens of the request to the SQL server and the end of the execution. This time out is managed by the database itself.
- the second one is managed by Vigilens: compared to the first one, it also takes into account the data extraction time.

These notions of time-out can be defined at different levels:



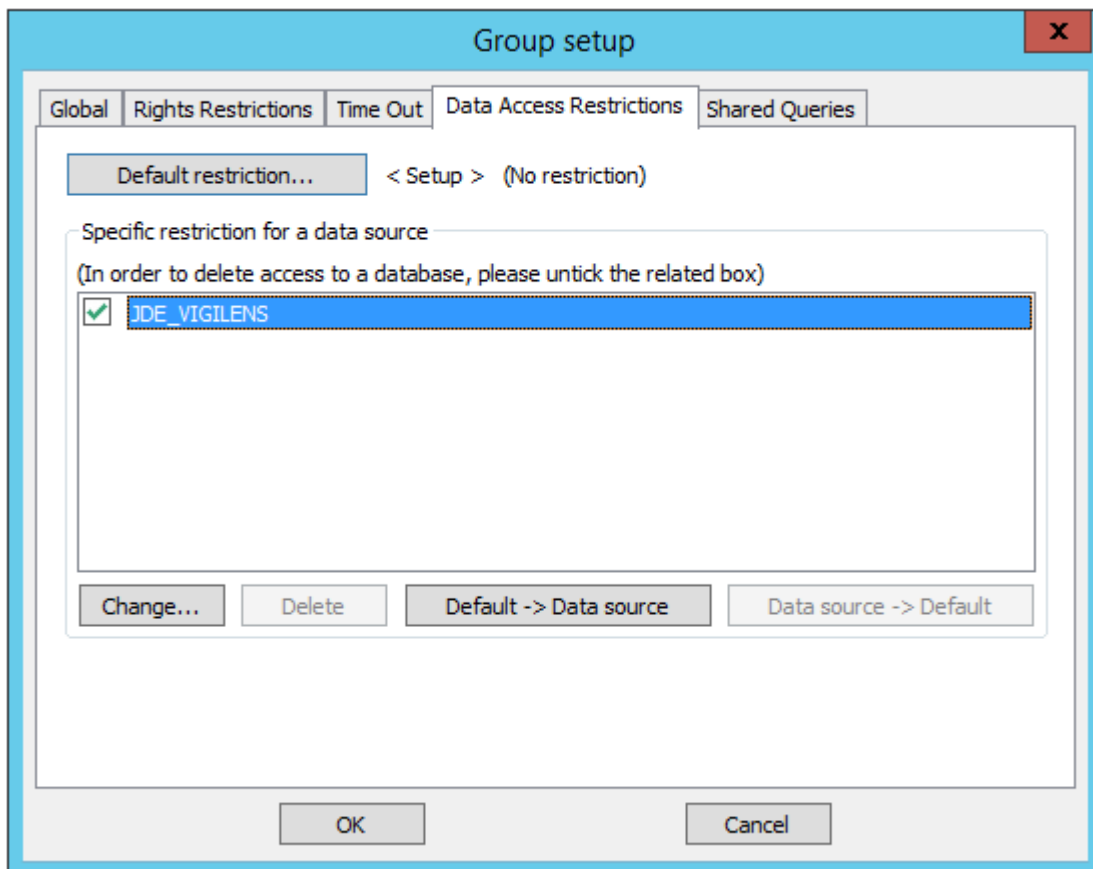
- group
- user
- query

These times must necessarily be smaller and smaller when switching from group to user and then user to query.



Because SQL time out is managed at the database system level, it is not available on all platforms.

Data access restriction



It may be useful to block certain groups from accessing certain sensitive company information. It is possible to prohibit the use of a data source by unchecking it in the list. For each datasource, Vigilens can impose restrictions on :

- Environments

- Tables (for JDE/World type sources)
- Aliases (for JDE/World sources)
- Fields
- Values



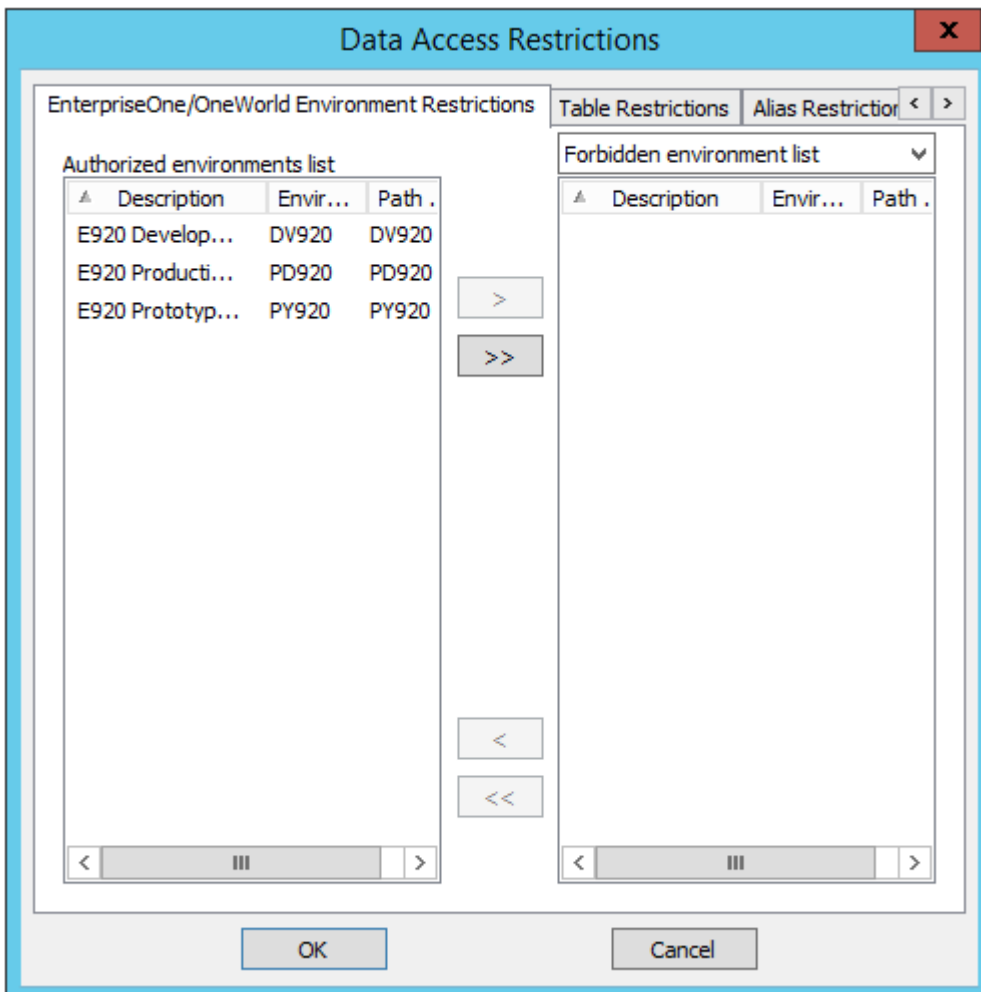
The button `Default restrictions...` gives you access to settings that are valid for all data sources that do not have specific settings. The sequence of the screens is similar in every way to the settings for a particular data source.



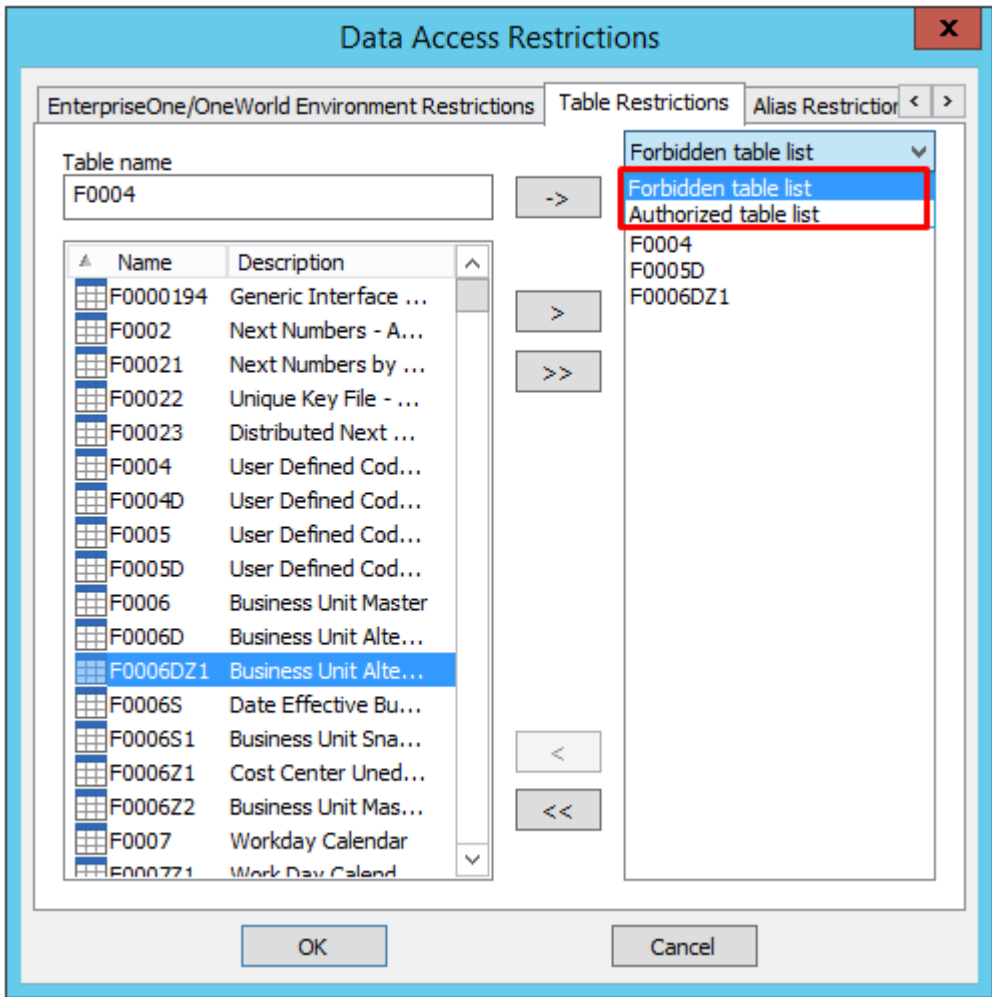
Generally speaking, all of the following restrictions work on either as black list or white list system: either you make explicit which items are prohibited and everything else is allowed, or you make explicit which items are allowed and everything else is prohibited. Black list/White list operation is defined at group level and cannot be changed at user level.

you can:

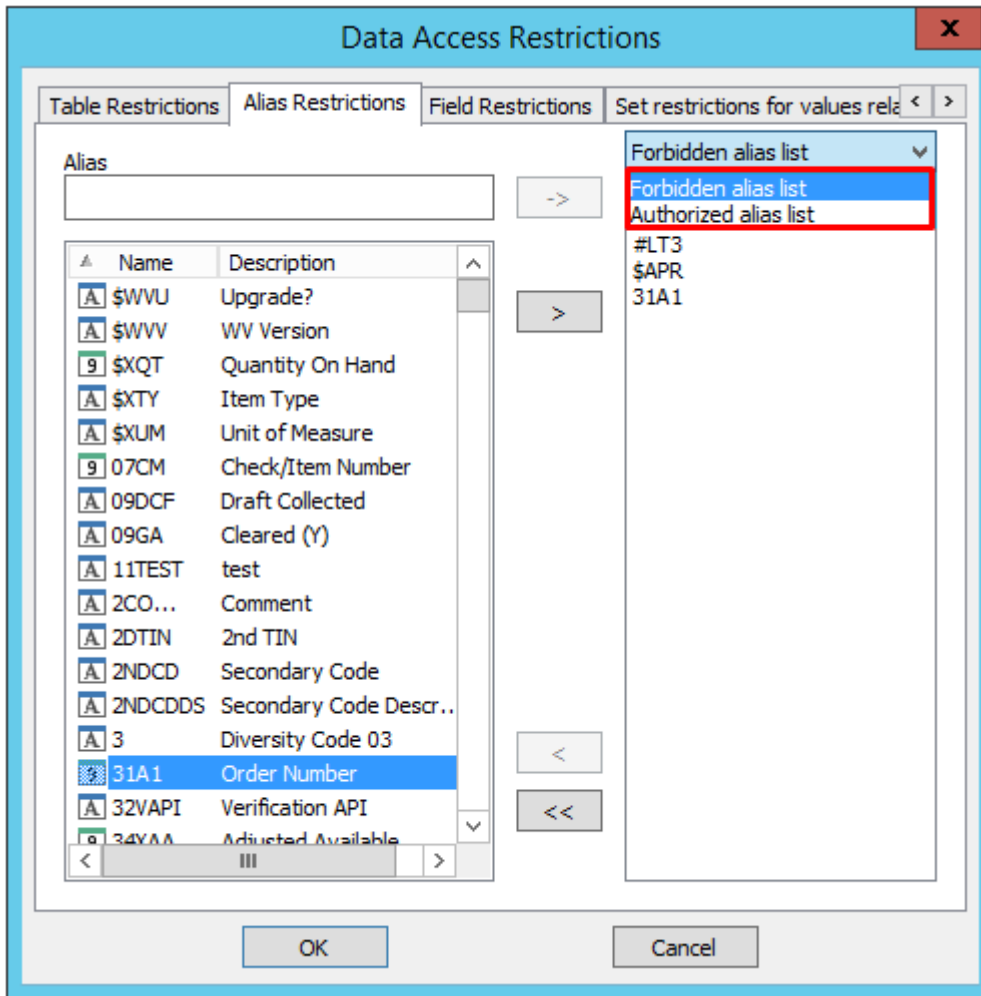
- prevent/allow access to environments, for JDE/World data sources



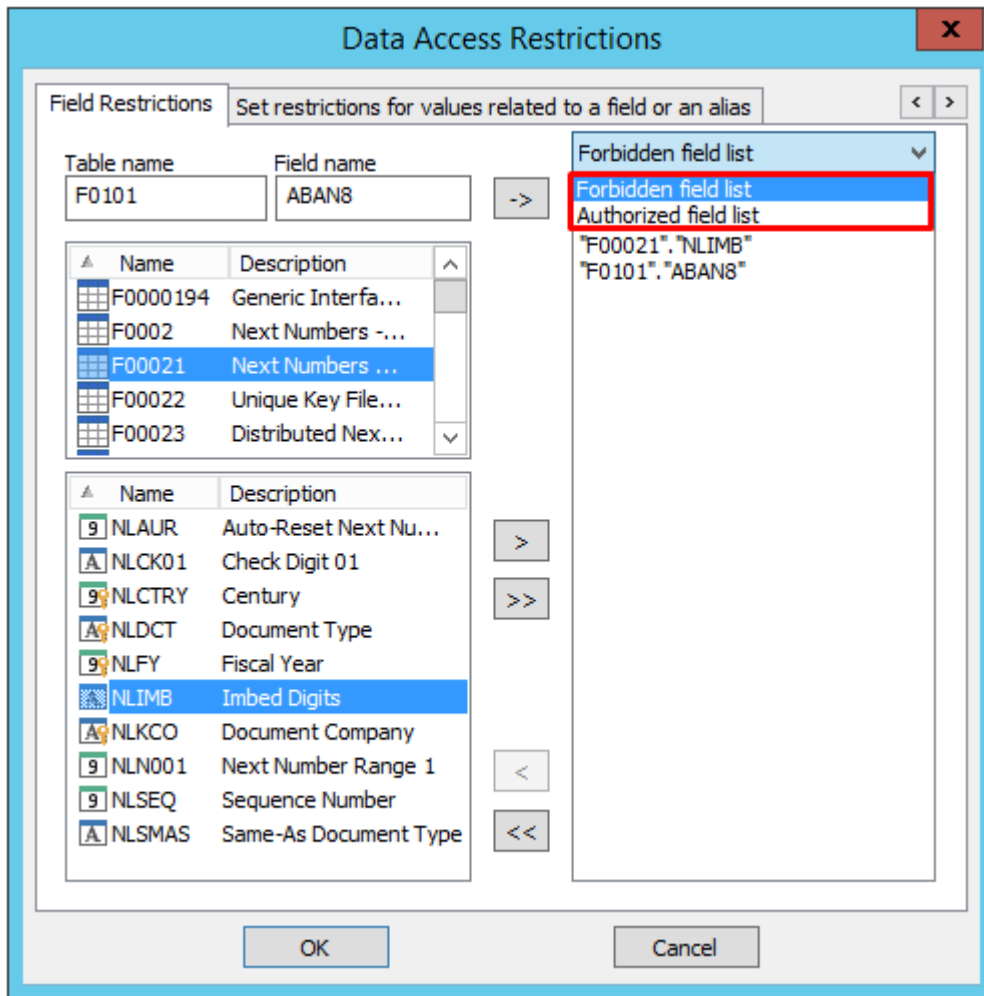
- prevent/allow consultation of a particular table



- prevent/allow access to an alias (JDE/World)




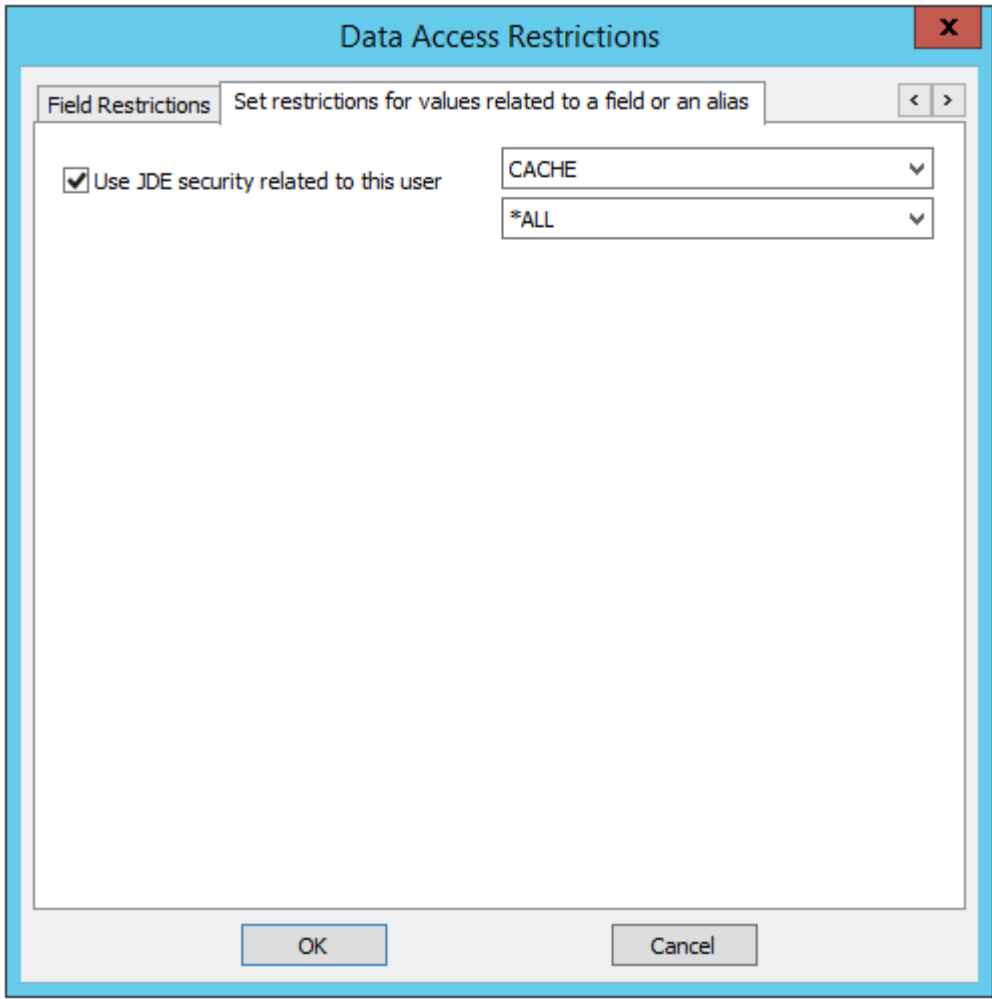
- prevent/allow access to define table column



- prevent/allow the display of certain table rows according to criteria on a table column. The criterion can be a single value, a range of values, or a list of values.

The screenshot shows the 'Data Access Restrictions' dialog box. The 'Field Restrictions' tab is active, with the 'Condition for forbidden data display' dropdown highlighted in red. A '+' button is also highlighted in red. Below it, the 'Set a condition for a value related to a field or an alias' dialog is open. It has three radio buttons: 'Enter an alias', 'Enter a field' (selected), and 'Enter a field without wizard'. Under 'Enter a field without wizard', 'Table name' is 'F0101' and 'Field name' is 'ABAN8'. Under 'Enter a field with wizard', there are two tables. The first table lists various field names and descriptions, with 'F0002' selected. The second table lists check digits from 'NNCK01' to 'NNCK08'. At the bottom, the 'Value for forbidden display' dropdown is set to 'Value equal to the following string :', and the selected value is '[F0002].[NNCK01] ='. A red arrow points from this dropdown to the '[F0002].[NNCK01]' dialog, which is also open. This dialog has three tabs: 'Single value', 'Range of values', and 'List of values'. The 'Single value' tab is active, showing input fields with '0' and '3'.

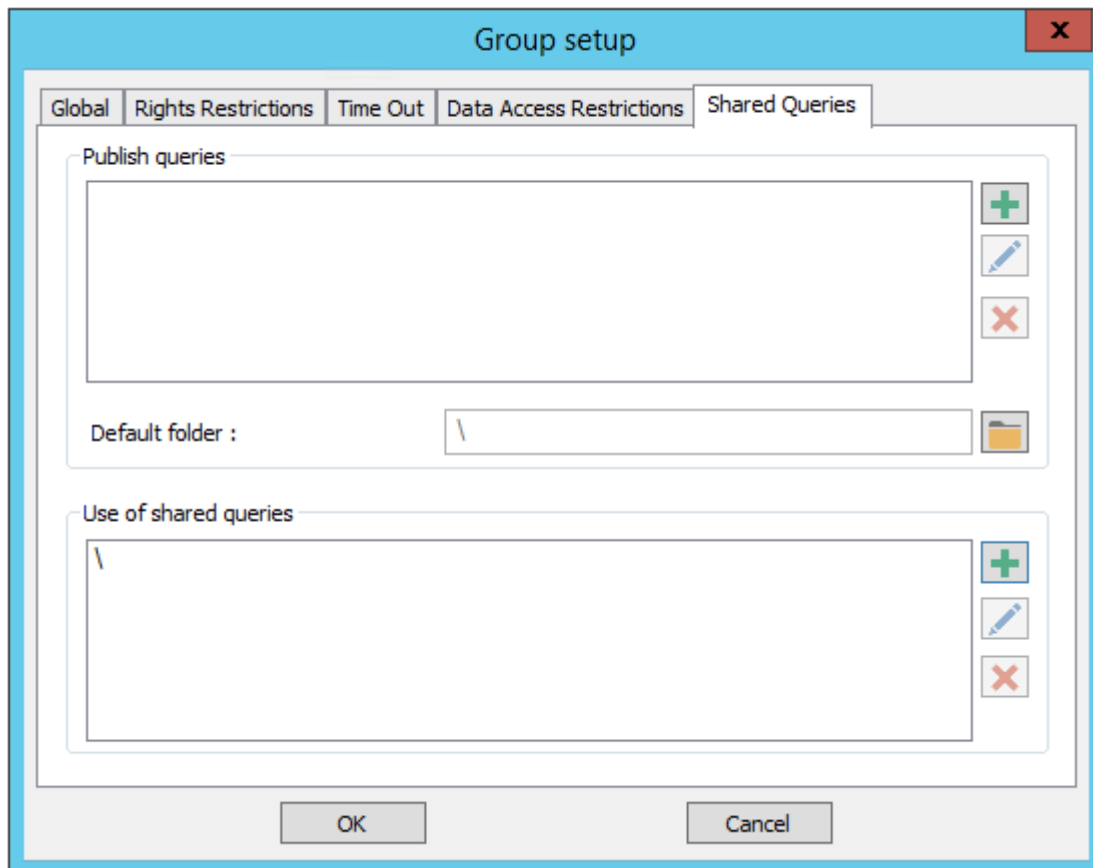
 If the data source is JDE/World, we have in addition the choice to use the JDE security associated with a user and one of his roles (or all roles with the value “*ALL”).



Shared Queries

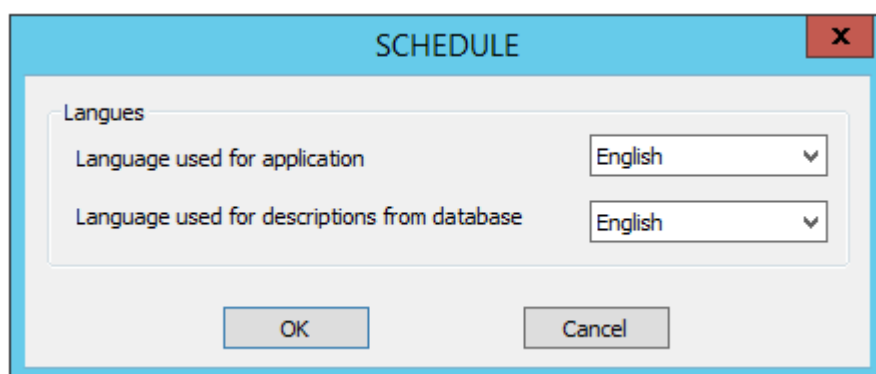
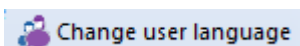
This setting allows you to :

- Define the place(s) where the user can deposit the queries he wants to share. The user has access to the entire tree structure of the specified directories.
- Define the shared queries it can use

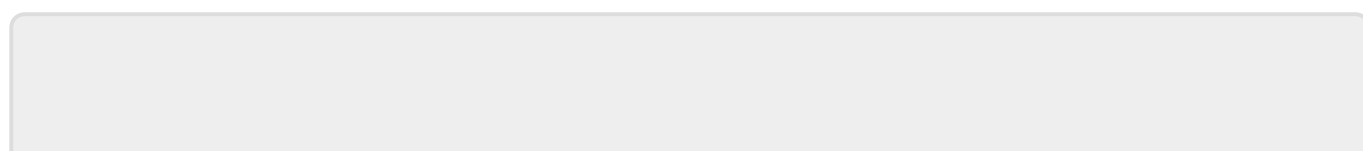


- Publish queries: list of shared folders accessible when publishing queries
 - Default folder: proposed by default when publishing queries
- Use of shared queries: list of shared folders accessible via the web interface

Change Language



Allows you to change the languages (of the interface and of the descriptions coming from the database) of all the users present in the group.



From: <https://vigilens.wiki/dokuwiki/> - **Vigilens Reporting Knowledge Garden**

Permanent link: https://vigilens.wiki/dokuwiki/doku.php?id=en:v8_0_0:admintool:menus:gestion:groupe:start&rev=1601027611

Last update: **2020/09/25 11:53**

