

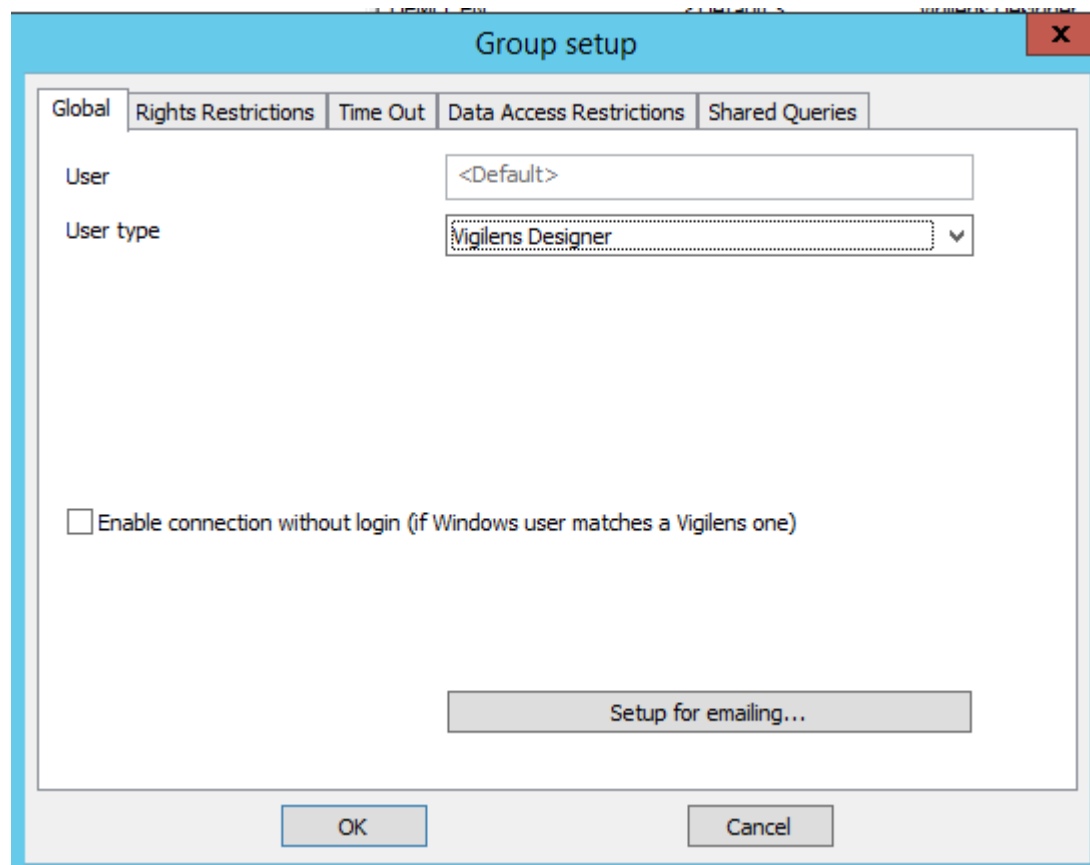
Managent menu > Group

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



The screenshot shows the 'Group setup' dialog box with the 'Global' tab selected. The dialog has a title bar with a close button (X). Inside, there are five tabs: 'Global', 'Rights Restrictions', 'Time Out', 'Data Access Restrictions', and 'Shared Queries'. The 'Global' tab contains the following elements:

- 'User' field: A text box containing '<Default>'.
- 'User type' field: A dropdown menu with 'Vigilens Designer' selected.
- 'Enable connection without login (if Windows user matches a Vigilens one)': An unchecked checkbox.
- 'Setup for emailing...': A button.
- 'OK' and 'Cancel' buttons at the bottom.

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.

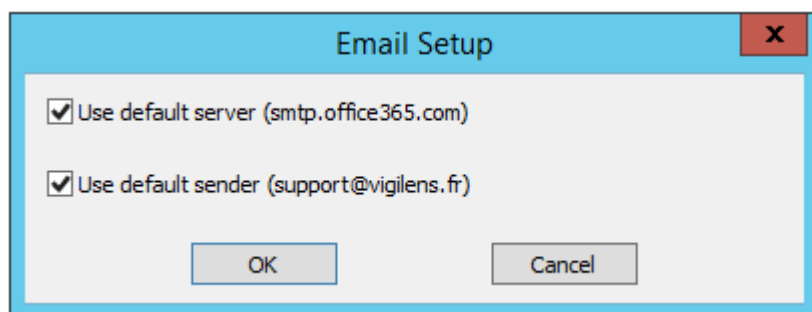
Setup for emailing

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

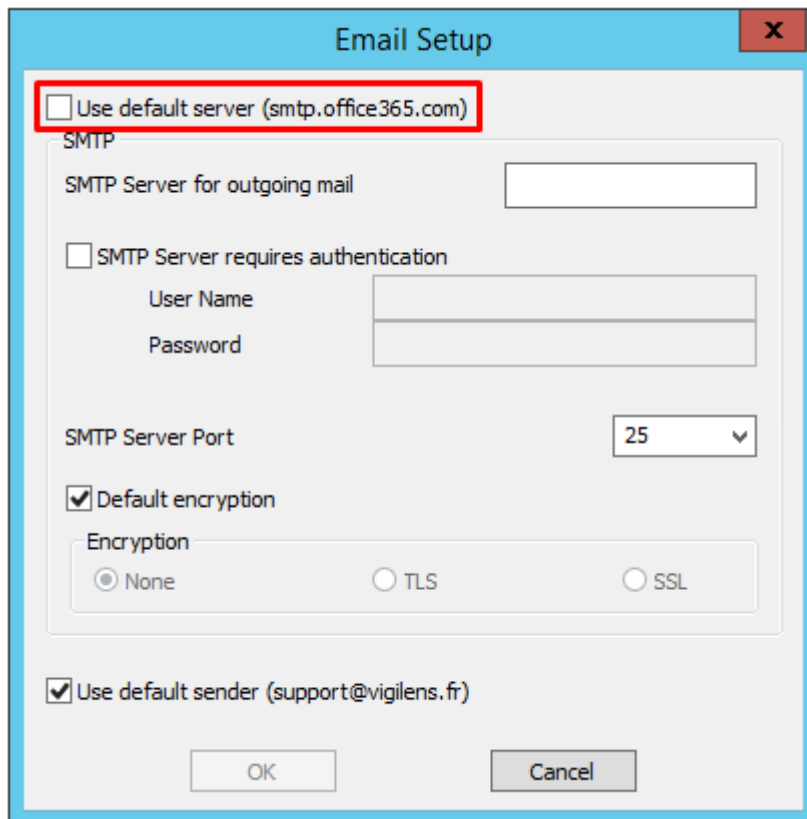
The mail server can be set at the user level, in which case it takes precedence over what is set at the group level.



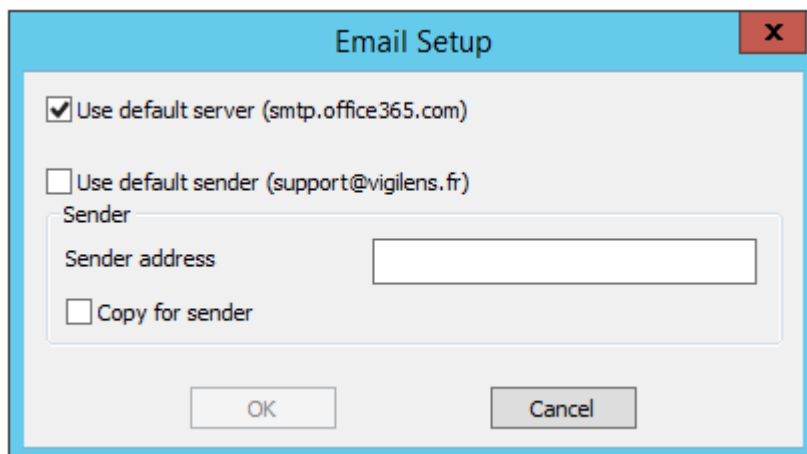
Specifying mail settings at the user level allows you to have a personalized return address.



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

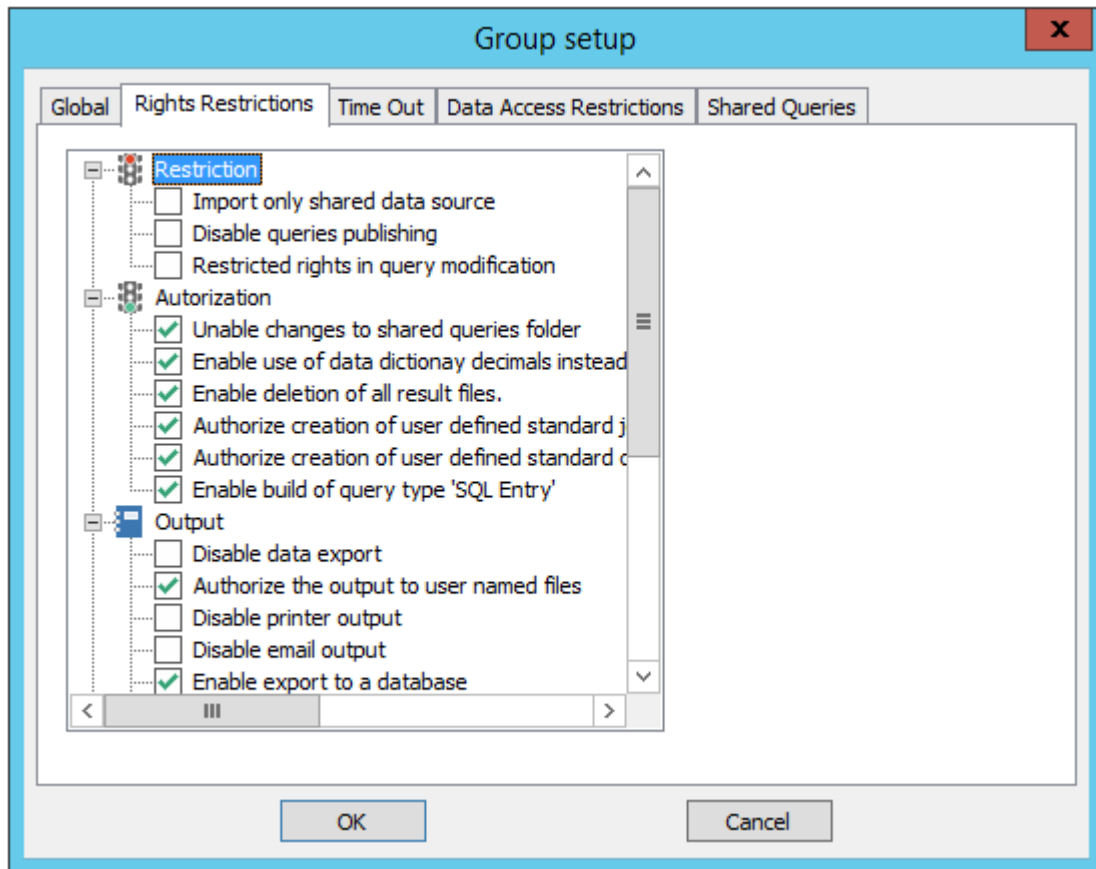


The 'Email Setup' dialog box has a blue title bar with a close button. The main content area is light gray. At the top, there is a checkbox labeled 'Use default server (smtp.office365.com)' which is currently unchecked and highlighted with a red rectangle. Below this, the 'SMTP' section is enclosed in a rounded rectangle. It contains a text field for 'SMTP Server for outgoing mail', an unchecked checkbox for 'SMTP Server requires authentication' with associated 'User Name' and 'Password' text fields, and a 'SMTP Server Port' dropdown menu set to '25'. Below the SMTP section is a checked checkbox for 'Default encryption' and an 'Encryption' group box containing three radio buttons: 'None' (selected), 'TLS', and 'SSL'. At the bottom of the dialog, there is a checked checkbox for 'Use default sender (support@vigilens.fr)' and two buttons: 'OK' and 'Cancel'.

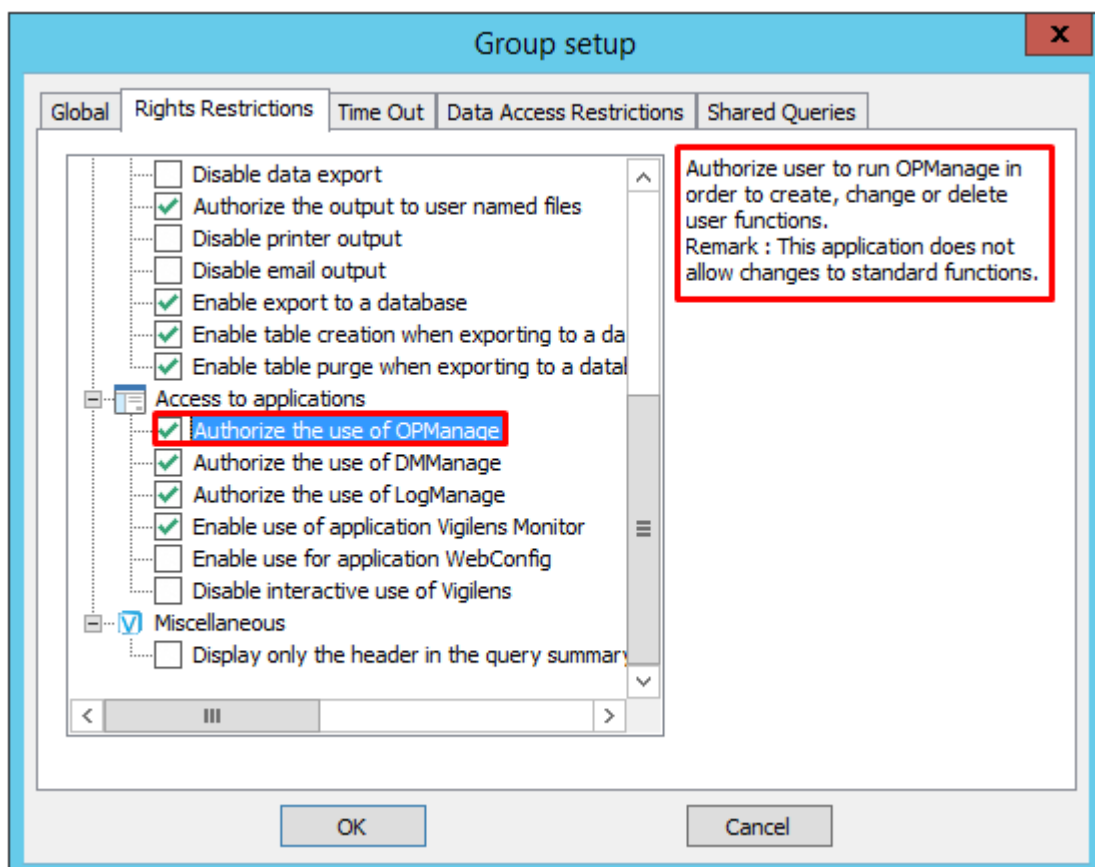


The 'Email Setup' dialog box is shown in a second state. The 'Use default server (smtp.office365.com)' checkbox is now checked. The 'SMTP' section is no longer visible. Instead, the 'Use default sender (support@vigilens.fr)' checkbox is unchecked, and a 'Sender' section is visible below it. This section contains a 'Sender address' text field and an unchecked 'Copy for sender' checkbox. The 'OK' and 'Cancel' buttons remain at the bottom.

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

Group setup

Global Rights Restrictions Time Out Data Access Restrictions Shared Queries

SQL run time out

☒ Enable time out 0 h 3' 0"

Total time out (SQL run + Data download and display)

☒ Enable time out 0 h 4' 0"

OK Cancel

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:



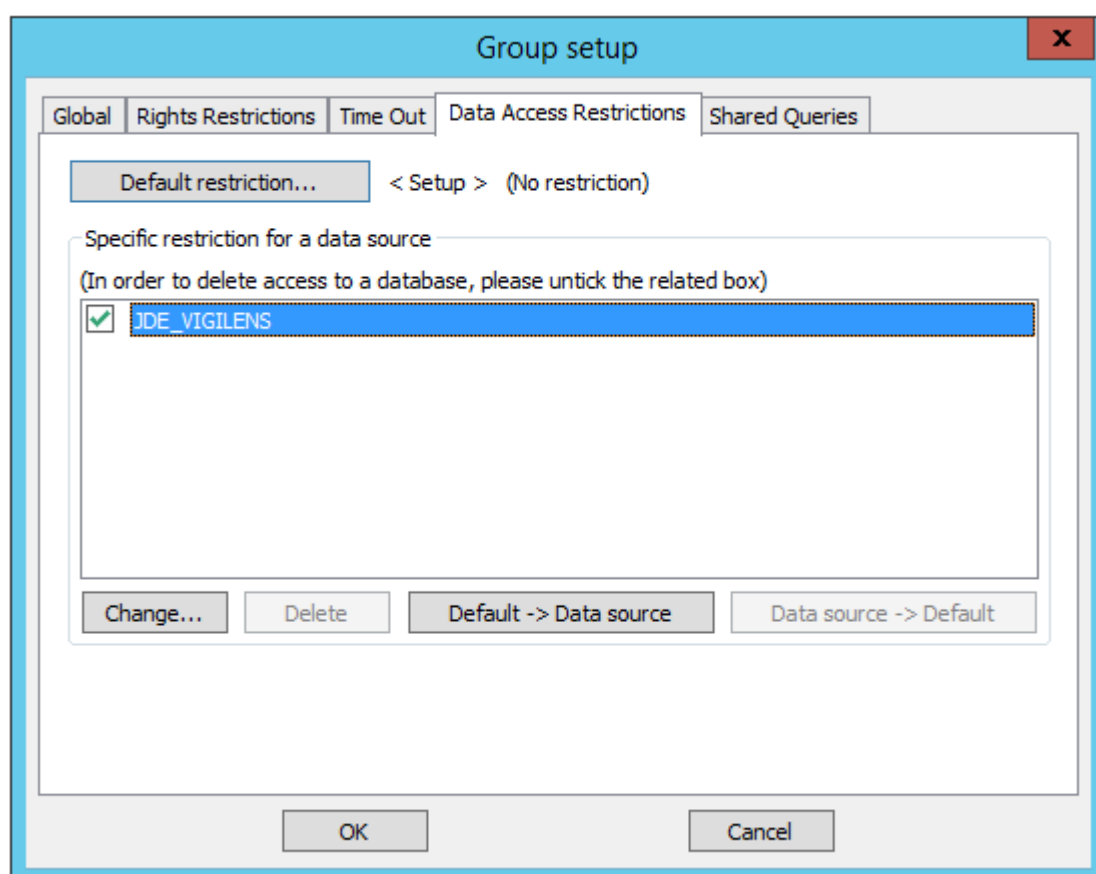
- group
- user
- query

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



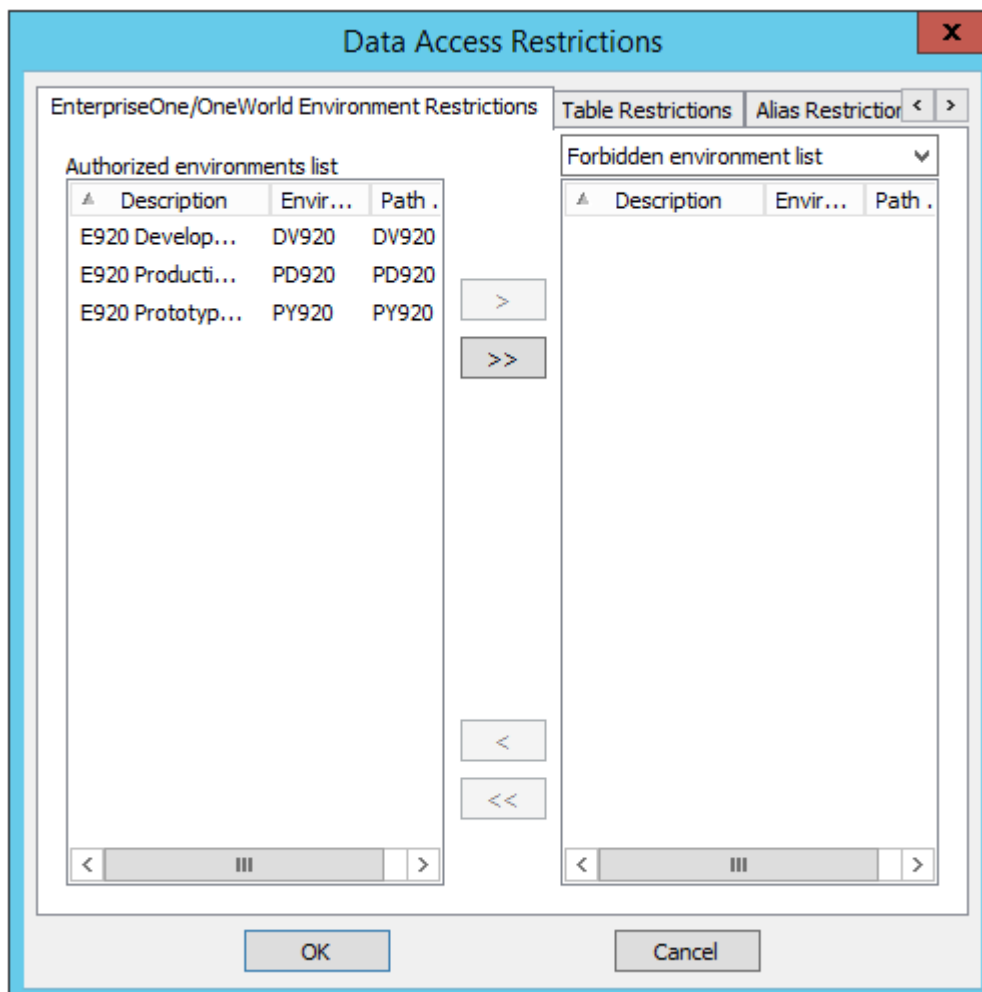
The button `Default restrictions...` gives you access to settings that are valid for all data sources that do not have specific settings. The sequence of the screens is similar in every way to the settings for a particular data source.



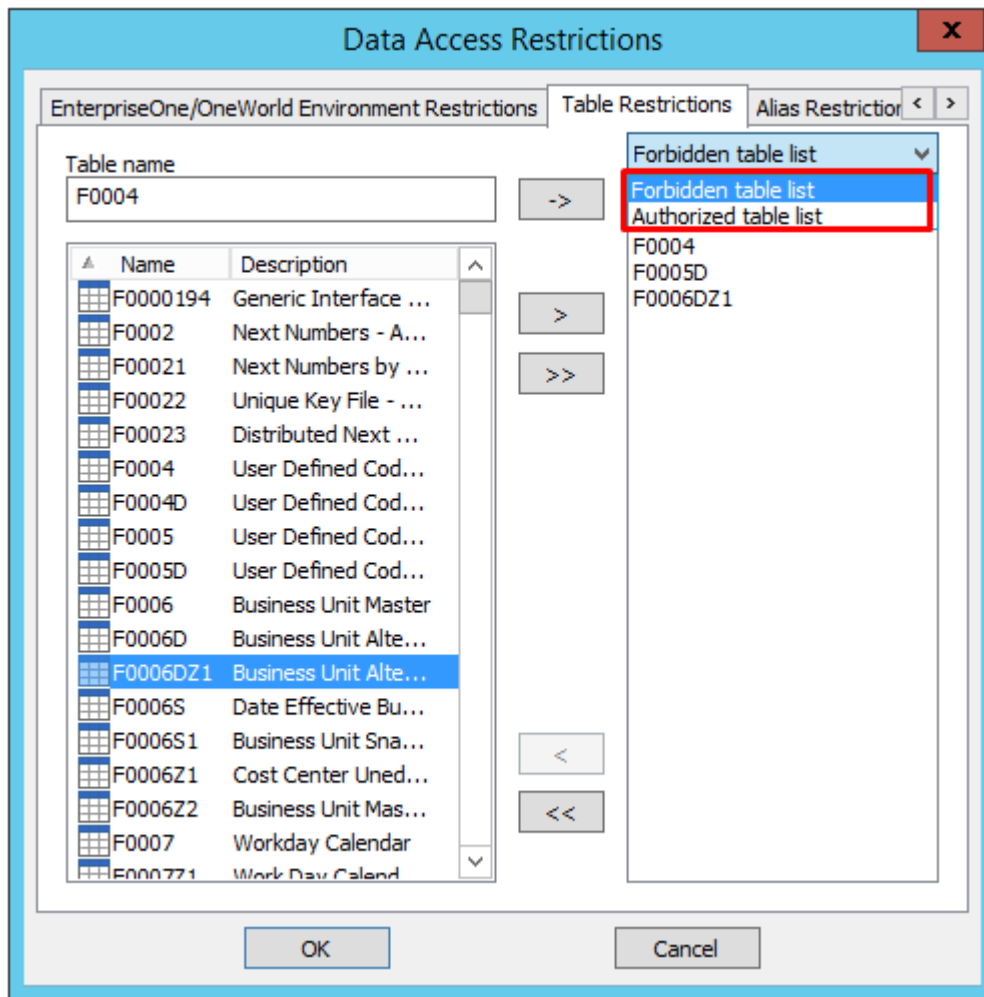
Generally speaking, all of the following restrictions work on either as black list or white list system: either you make explicit which items are prohibited and everything else is allowed, or you make explicit which items are allowed and everything else is prohibited. Black list/White list operation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

you can:

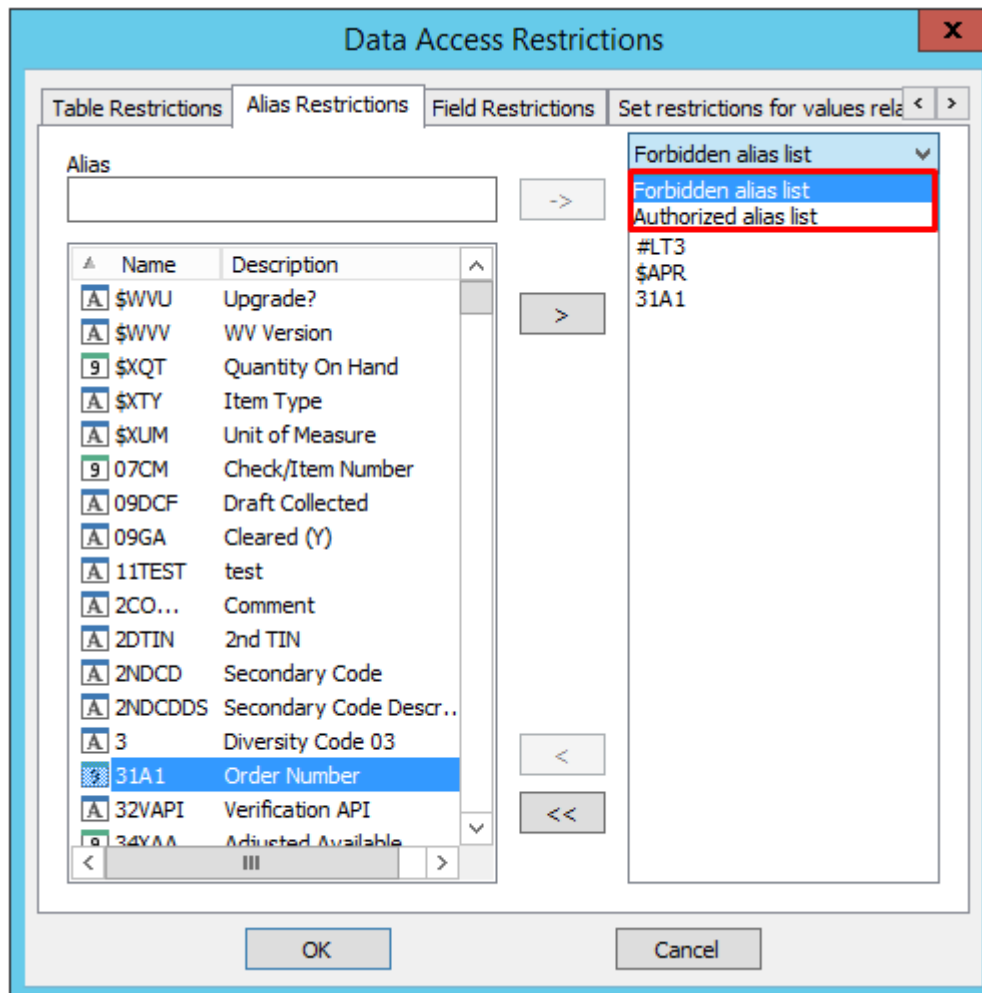
- prevent/allow access to environments, for JDE/World data sources



- prevent/allow consultation of a particular table



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



- prevent/allow access to define table column

Data Access Restrictions

Field Restrictions Set restrictions for values related to a field or an alias

Table name: F0101 Field name: ABAN8

Name	Description
F0000194	Generic Interfa...
F0002	Next Numbers -...
F00021	Next Numbers ...
F00022	Unique Key File...
F00023	Distributed Nex...

Forbidden field list

Forbidden field list

Authorized field list

"F00021", "NLIMB"

"F0101", "ABAN8"

OK Cancel

- 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 with the 'Field Restrictions' tab selected. The 'Condition for forbidden data display' dropdown is highlighted with a red box. Below it, the 'Set a condition for a value related to a field or an alias' dialog box is open, showing the 'Enter a field with wizard' option selected. The 'Table name' is 'F0101' and the 'Field name' is 'ABAN8'. The 'Value for forbidden display' is set to 'Value equal to the following string :'. The 'Single value' tab is selected in the 'Set a condition' dialog, showing the value '0'. A red arrow points from the '...' button in the 'Value for forbidden display' section to the 'Single value' tab in the 'Set a condition' dialog.

Data Access Restrictions

Field Restrictions Set restrictions for values related to a field or an alias

☐ Use JDE security related to this user

Condition for forbidden data display

Set a condition for a value related to a field or an alias

☐ Enter an alias ☒ Enter a field

Field to check

☐ Enter a field without wizard

Table name: F0101 Field name: ABAN8

☒ Enter a field with wizard

Name	Description
F0000194	Generic Interface Table ...
F0002	Next Numbers - Automatic
F00021	Next Numbers by Comp...
F00022	Unique Key File - Next A...
F00023	Distributed Next Number...
F0004	User Defined Code Types
F0004D	User Defined Codes - Alt...
F0005	User Defined Code Values
F0005D	User Defined Codes - Alt...

Name	Description
NNCK01	Check Digit 01
NNCK02	Check Digit 02
NNCK03	Check Digit 03
NNCK04	Check Digit 04
NNCK05	Check Digit 05
NNCK06	Check Digit 06
NNCK07	Check Digit 07
NNCK08	Check Digit 08

Value for forbidden display

☐ Value equal to the following string : ... [F0002].[NNCK01] =

[F0002].[NNCK01]

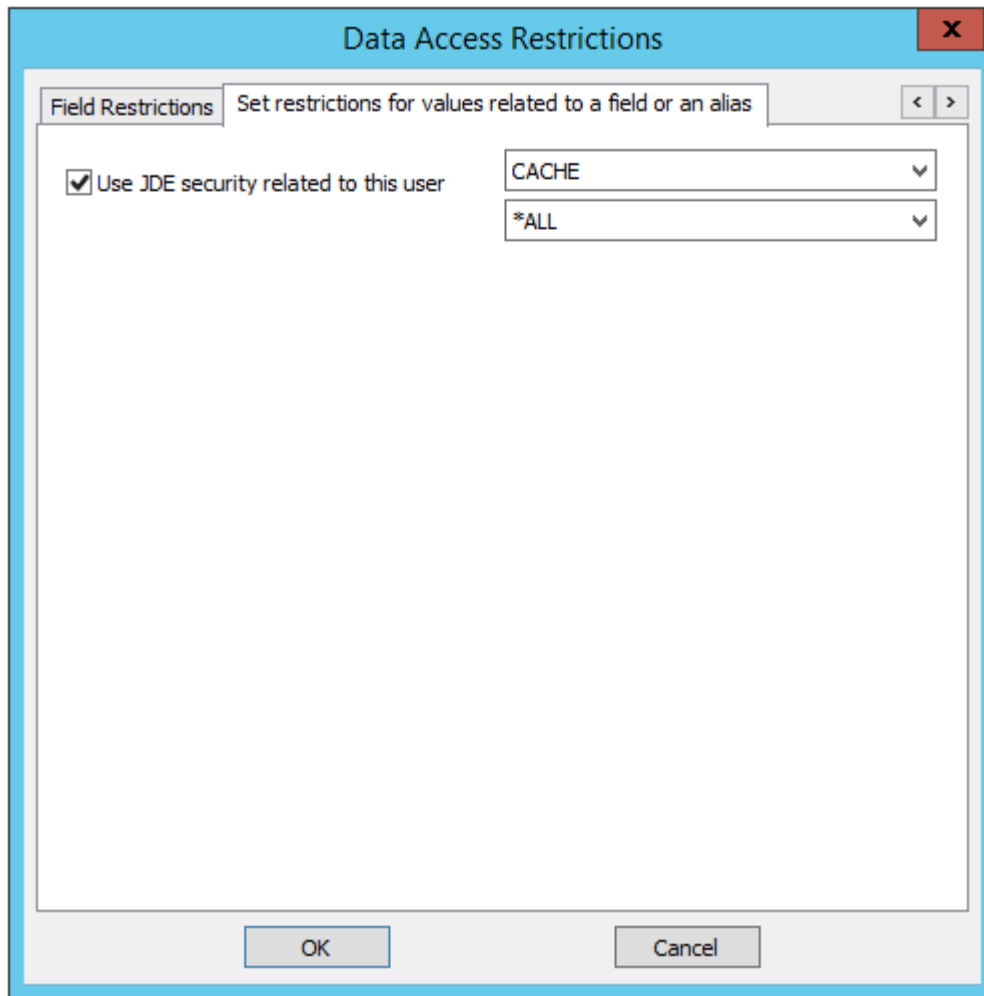
Single value Range of values List of values

0

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**").

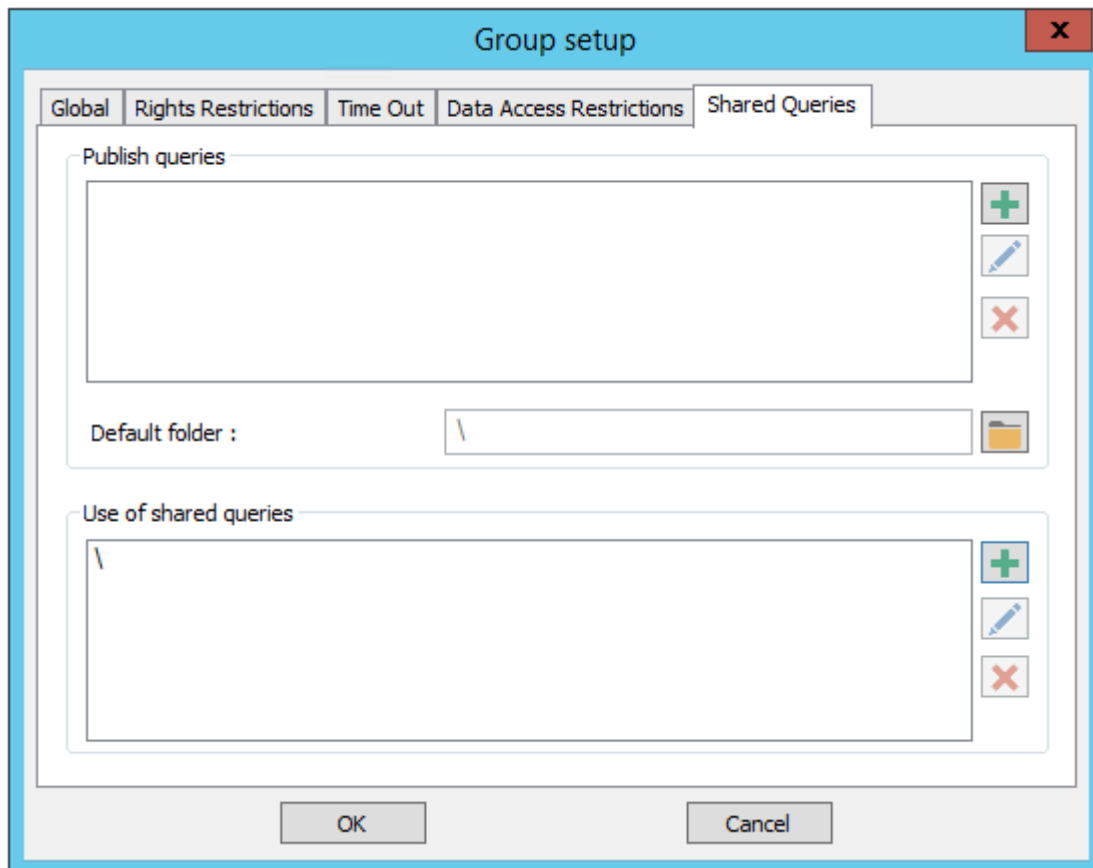


The image shows a dialog box titled "Data Access Restrictions" with a blue header bar and a red close button (X) in the top right corner. Inside the dialog, there is a tabbed interface. The first tab, "Field Restrictions", is selected and contains the text "Set restrictions for values related to a field or an alias". To the right of this tab are navigation arrows "<" and ">". Below the tab, there is a checkbox labeled "Use JDE security related to this user" which is checked. To the right of the checkbox are two dropdown menus. The first dropdown menu is currently set to "CACHE" and the second is set to "*ALL". At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

Shared Queries

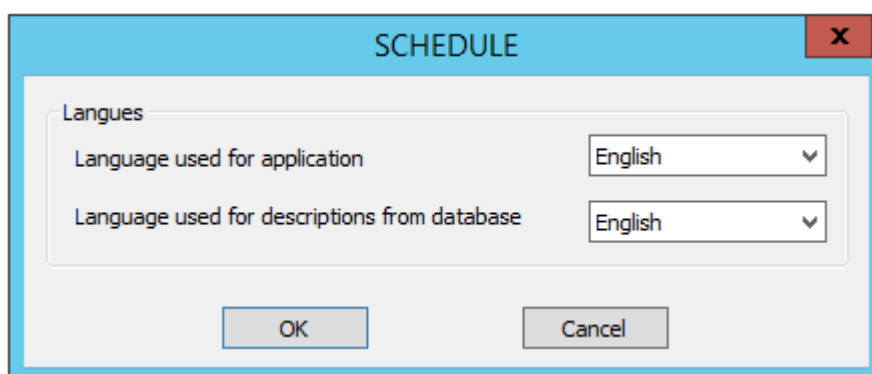
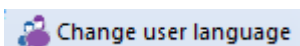
This setting allows you to :

- 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**

