

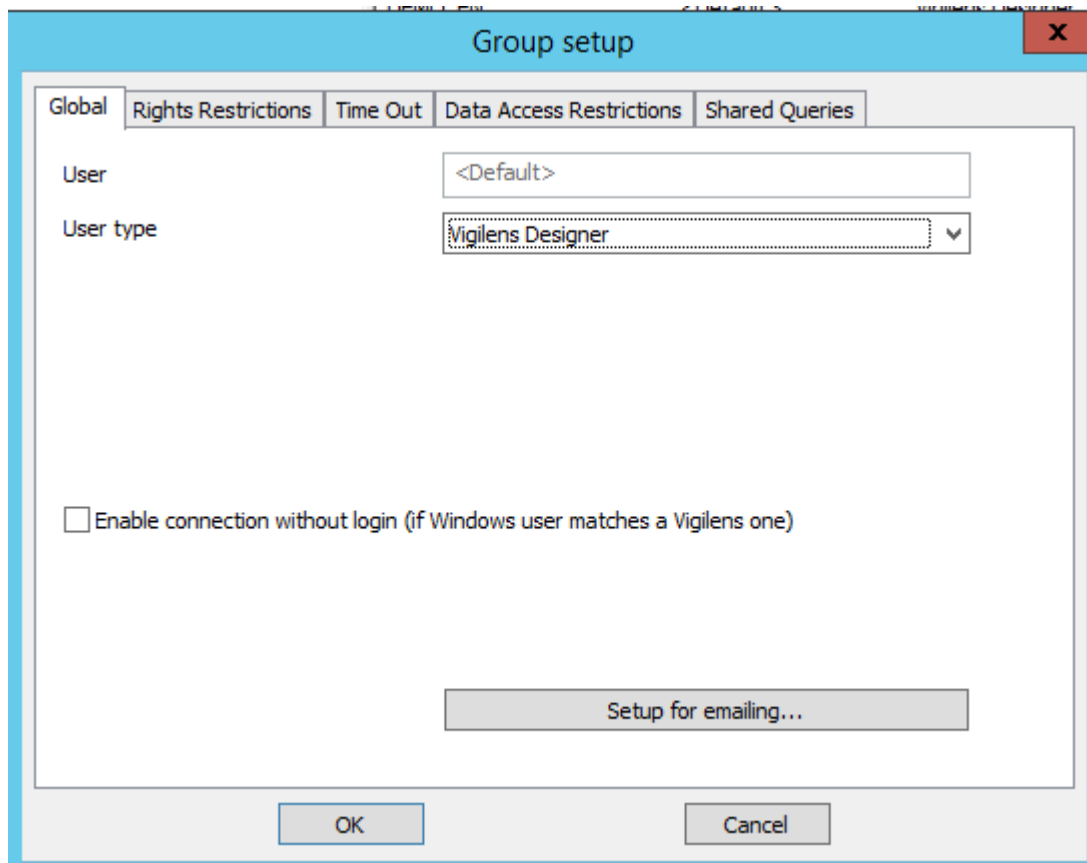
Managent menu > Group

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 fields and controls:

- User:** A text field with the value '<Default>'.
- User type:** 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.

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

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.

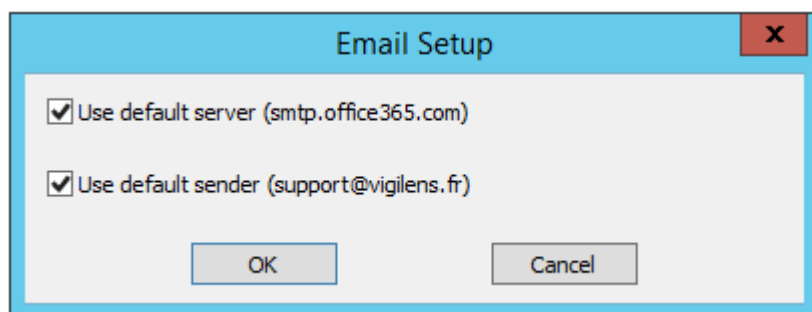
Setup for emailing

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

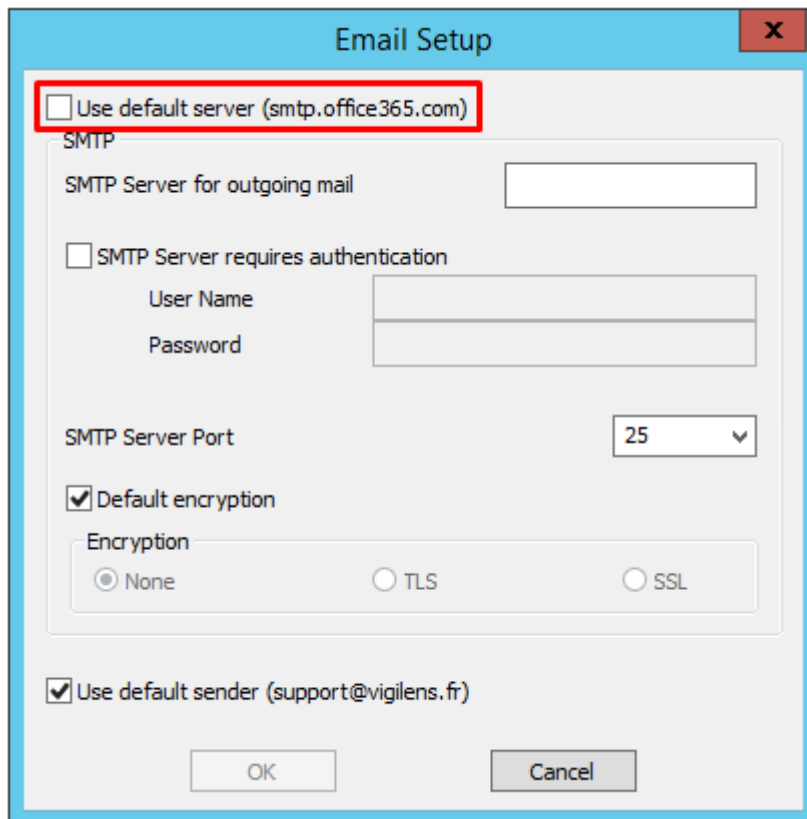
The mail server can be set at the user level, in which case it takes precedence over what is set at the group level.



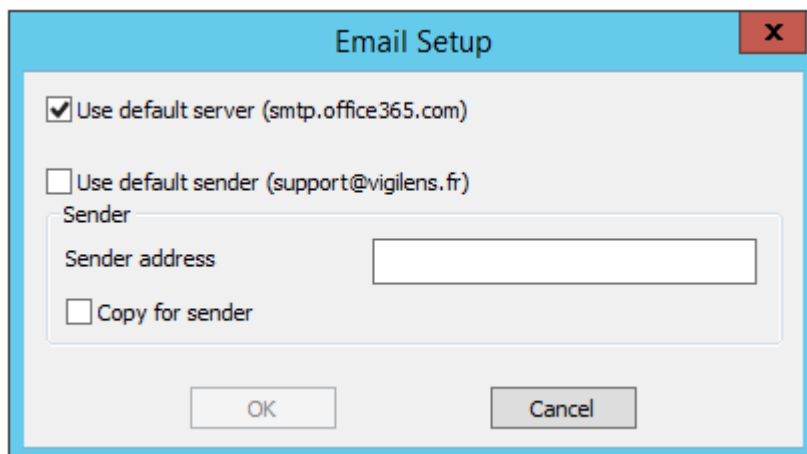
Specifying mail settings at the user level allows you to have a personalized return address.



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

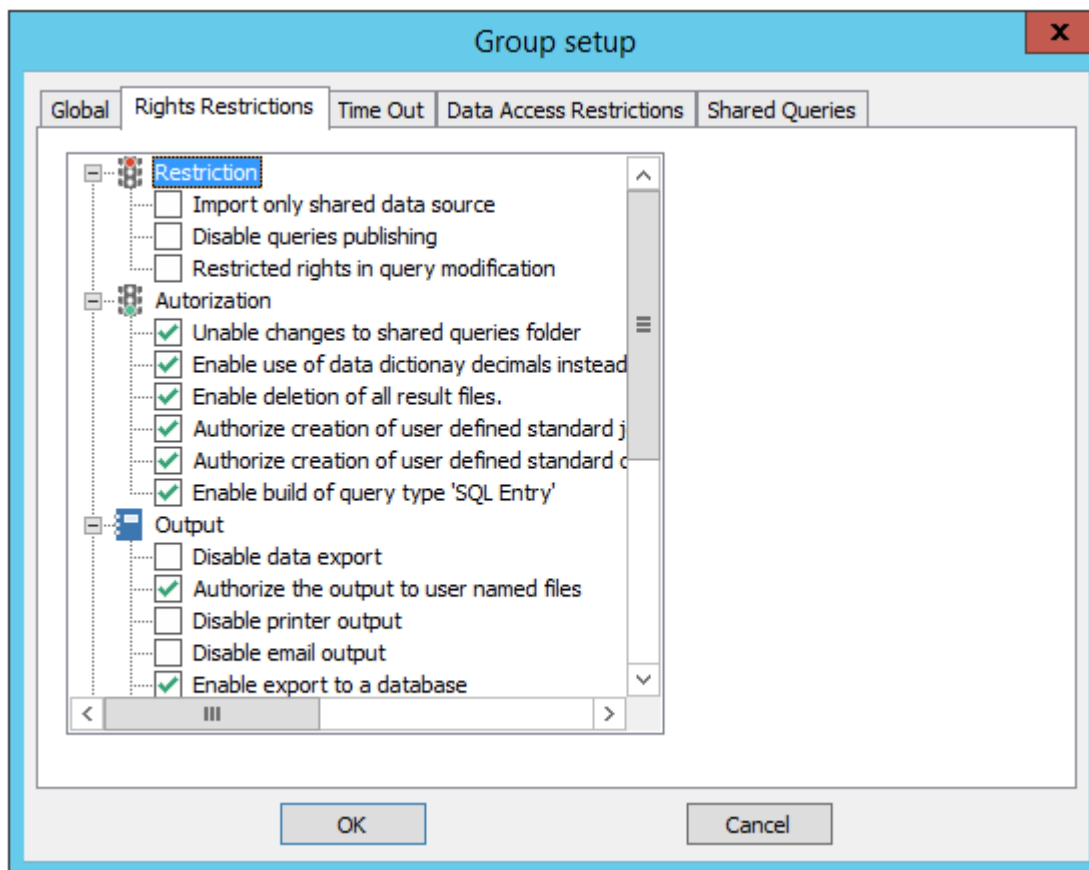


The 'Email Setup' dialog box has a blue title bar with a close button (X). The main content area is light gray. At the top, there is a checkbox labeled 'Use default server (smtp.office365.com)' which is currently unchecked and highlighted with a red rectangular border. Below this, the 'SMTP' section 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', and two text fields for 'User Name' and 'Password'. Below these is a dropdown menu for 'SMTP Server Port' set to '25'. There is a checked checkbox for 'Default encryption' and a sub-section titled 'Encryption' with 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'.

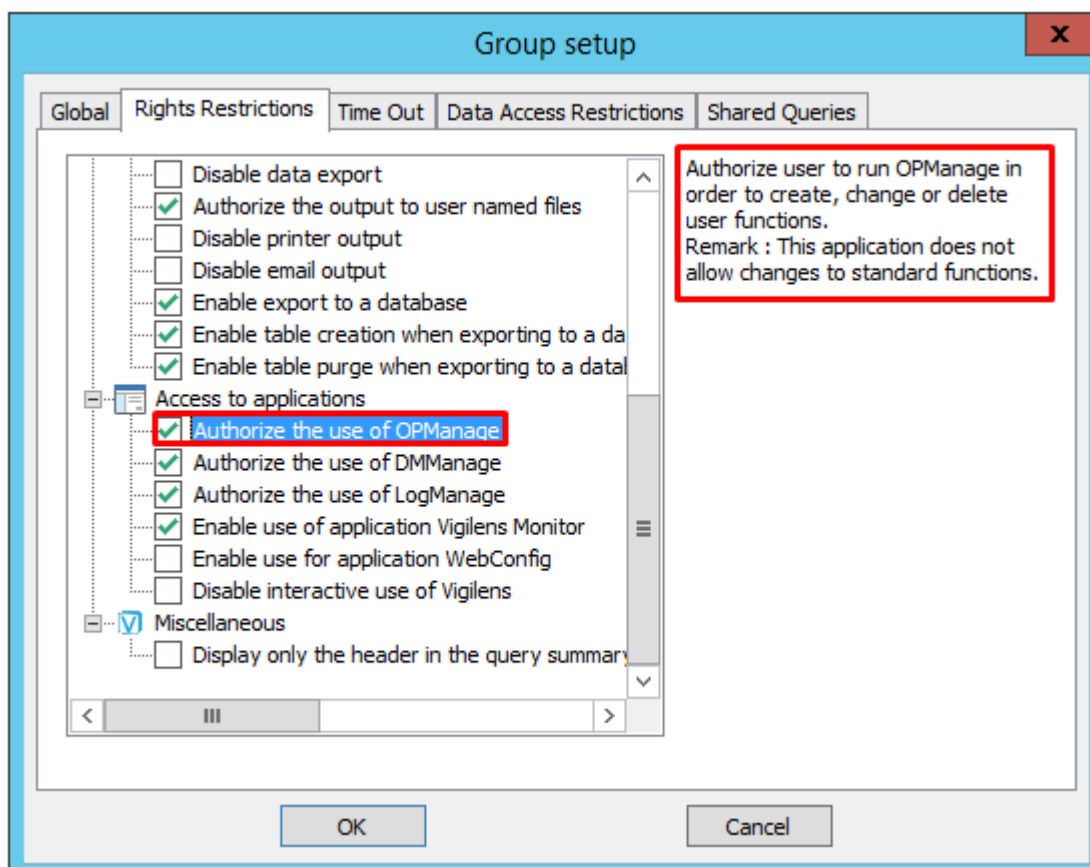


The 'Email Setup' dialog box has a blue title bar with a close button (X). The main content area is light gray. At the top, there is a checked checkbox labeled 'Use default server (smtp.office365.com)'. Below this is an unchecked checkbox labeled 'Use default sender (support@vigilens.fr)'. Under the 'Sender' section, there is a text field for 'Sender address' and an unchecked checkbox for 'Copy for sender'. At the bottom of the dialog, there are two buttons: 'OK' and '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.

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:



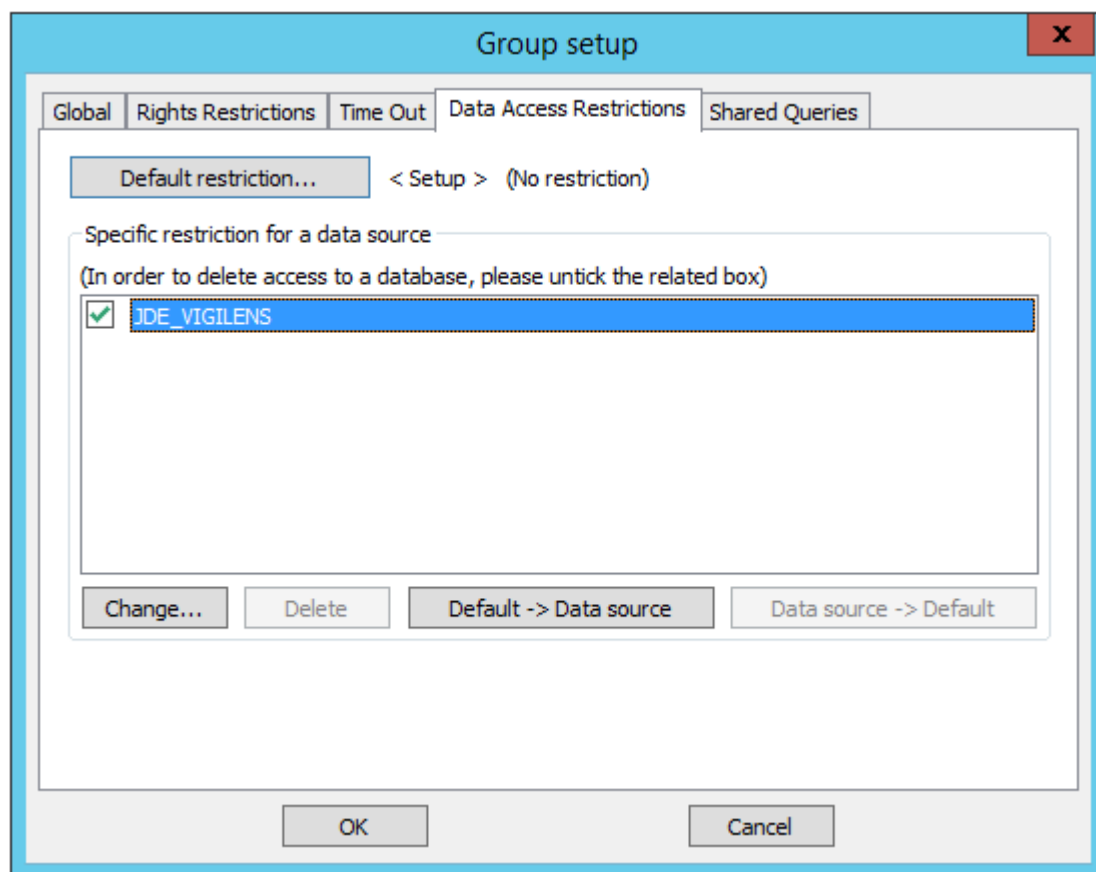
- group
- user
- query

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



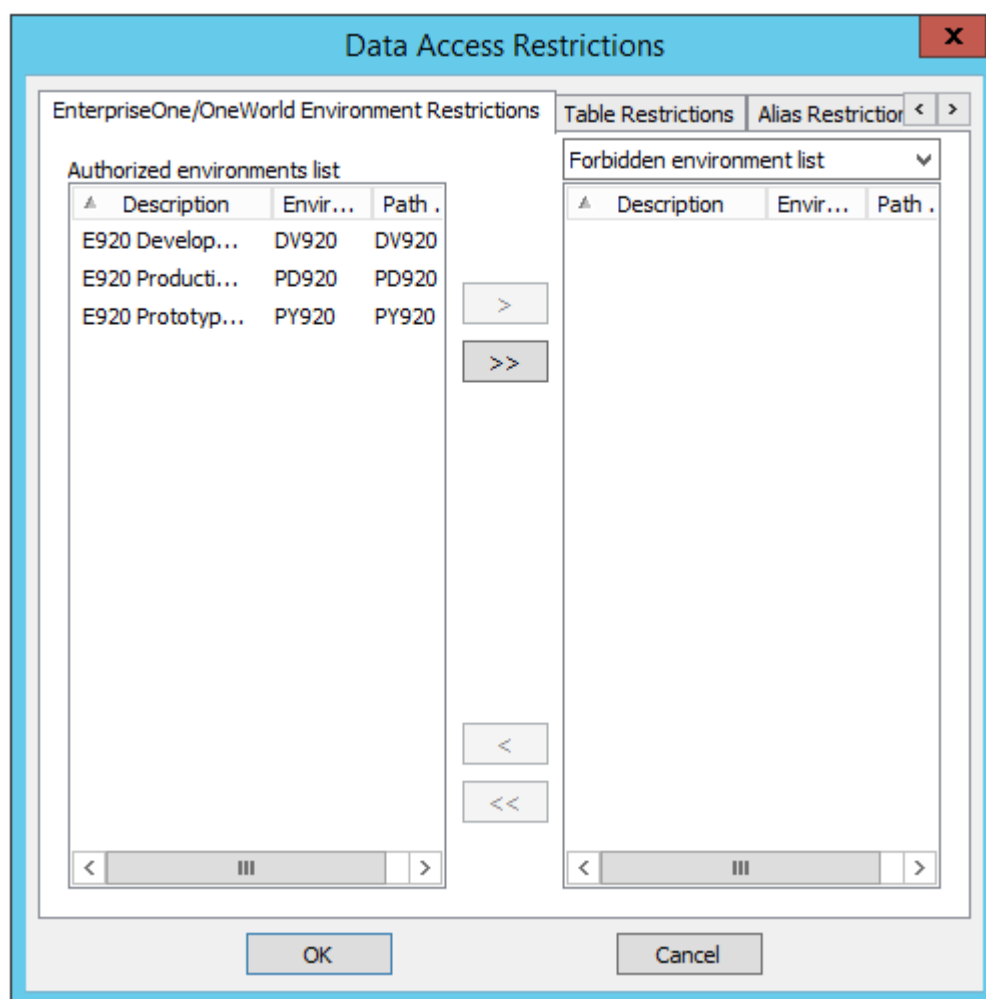
The button **Default restrictions...** gives you access to settings that are valid for all data sources that do not have specific settings. The sequence of the screens is similar in every way to the settings for a particular data source.



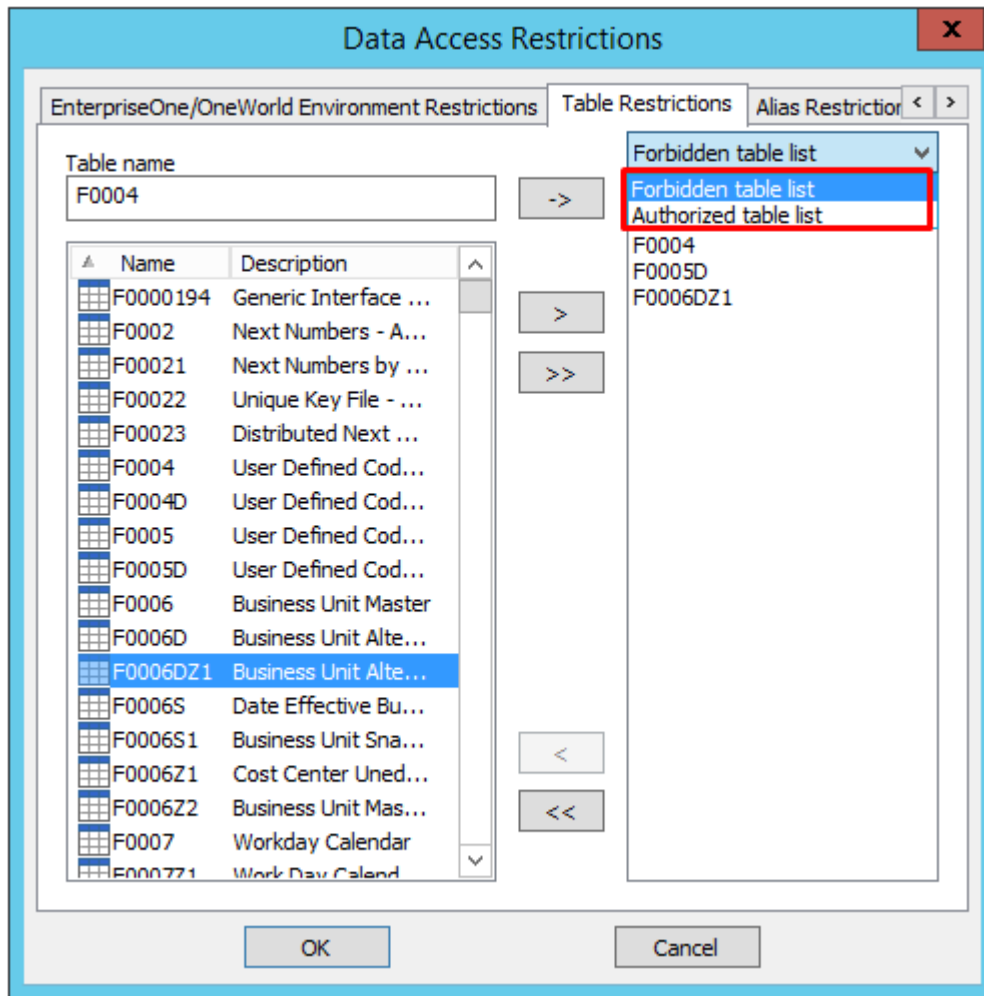
Generally speaking, all of the following restrictions work on either as black list or white list system: either you make explicit which items are prohibited and everything else is allowed, or you make explicit which items are allowed and everything else is prohibited. Black list/White list operation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

you can:

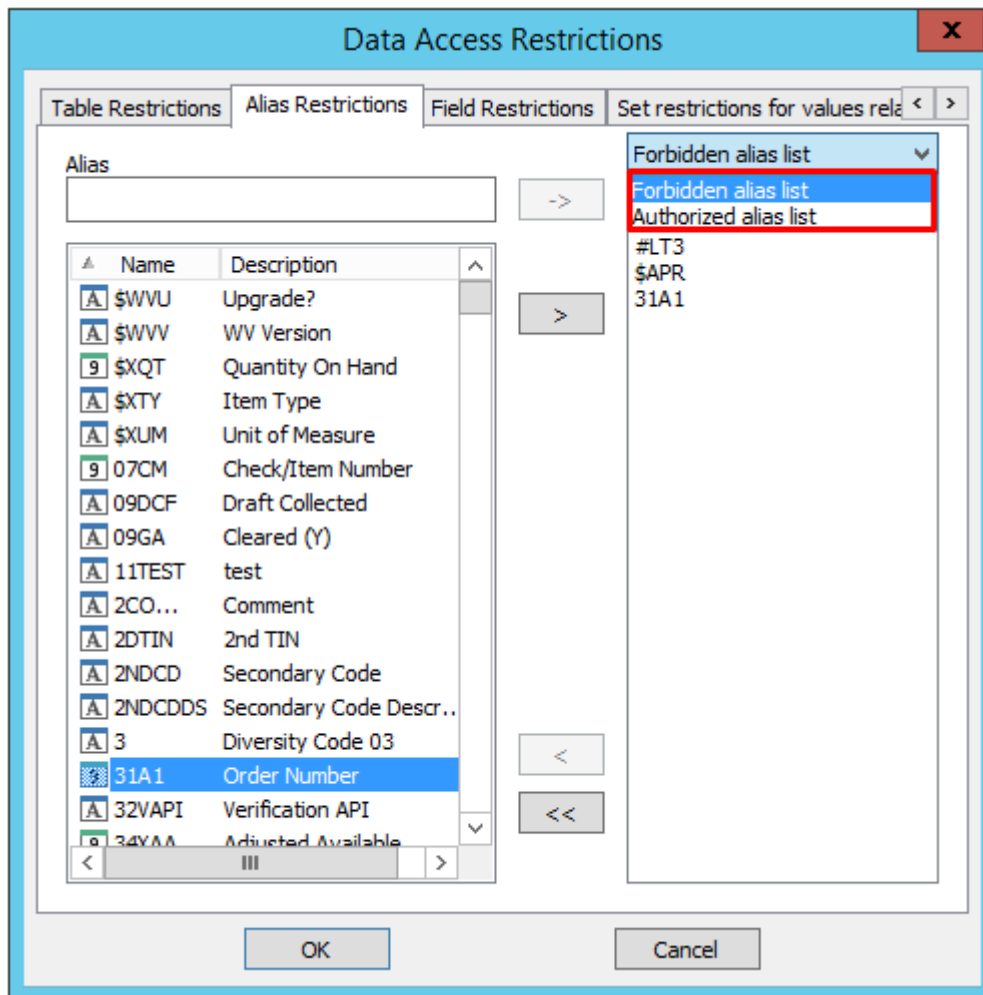
- prevent/allow access to environments, for JDE/World data sources



- 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

Forbidden field list

Forbidden field list

Authorized field list

"F00021", "NLIMB"

"F0101", "ABAN8"

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

Name	Description
NLAUR	Auto-Reset Next Nu...
NLCK01	Check Digit 01
NLCTRY	Century
NLDCT	Document Type
NLFY	Fiscal Year
NLIMB	Imbed Digits
NLKCO	Document Company
NLN001	Next Number Range 1
NLSEQ	Sequence Number
NLSMAS	Same-As Document Type

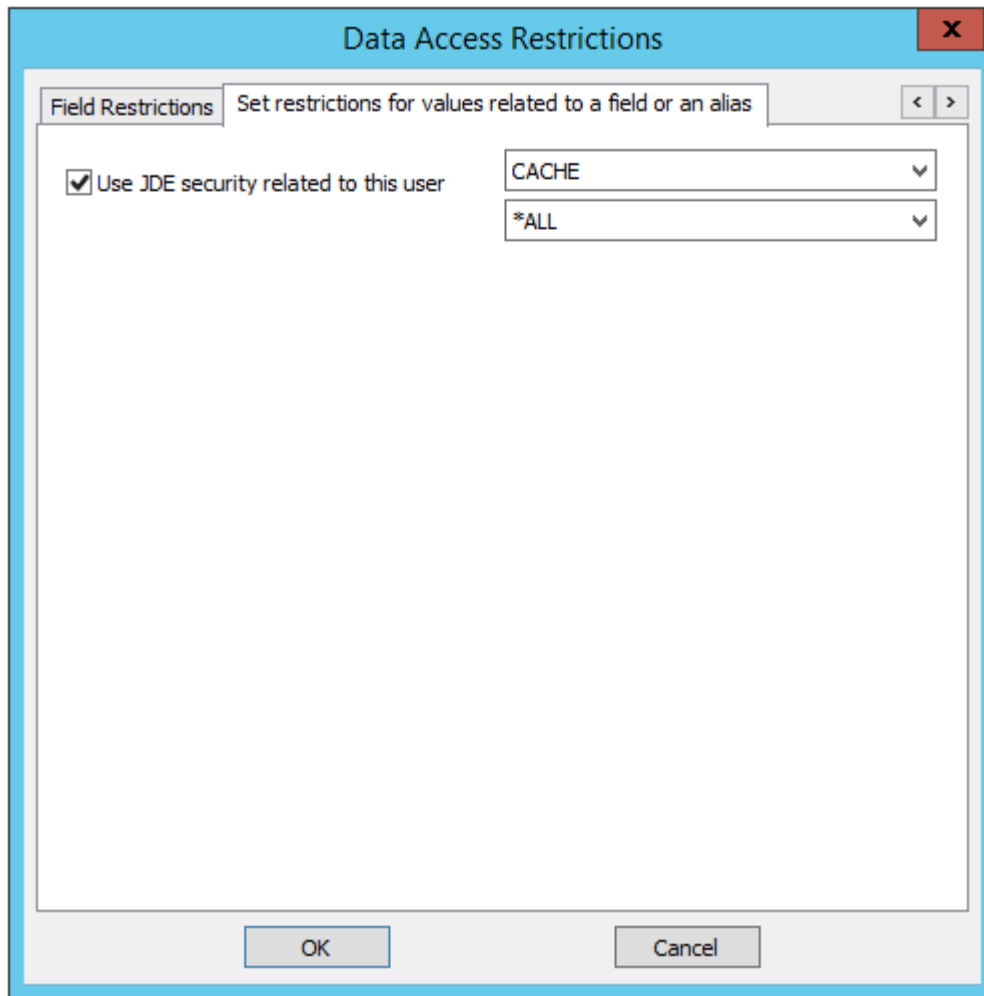
OK Cancel

- 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 in SAP. The 'Field Restrictions' tab is selected. The 'Condition for forbidden data display' dropdown is highlighted with a red box. A red arrow points from this dropdown to the 'Value for forbidden display' field in the 'Enter a field with wizard' section, which contains the expression '[F0002].[NNCK01] ='. A secondary dialog box titled '[F0002].[NNCK01]' is open, showing the 'Range of values' tab with input fields for '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”).

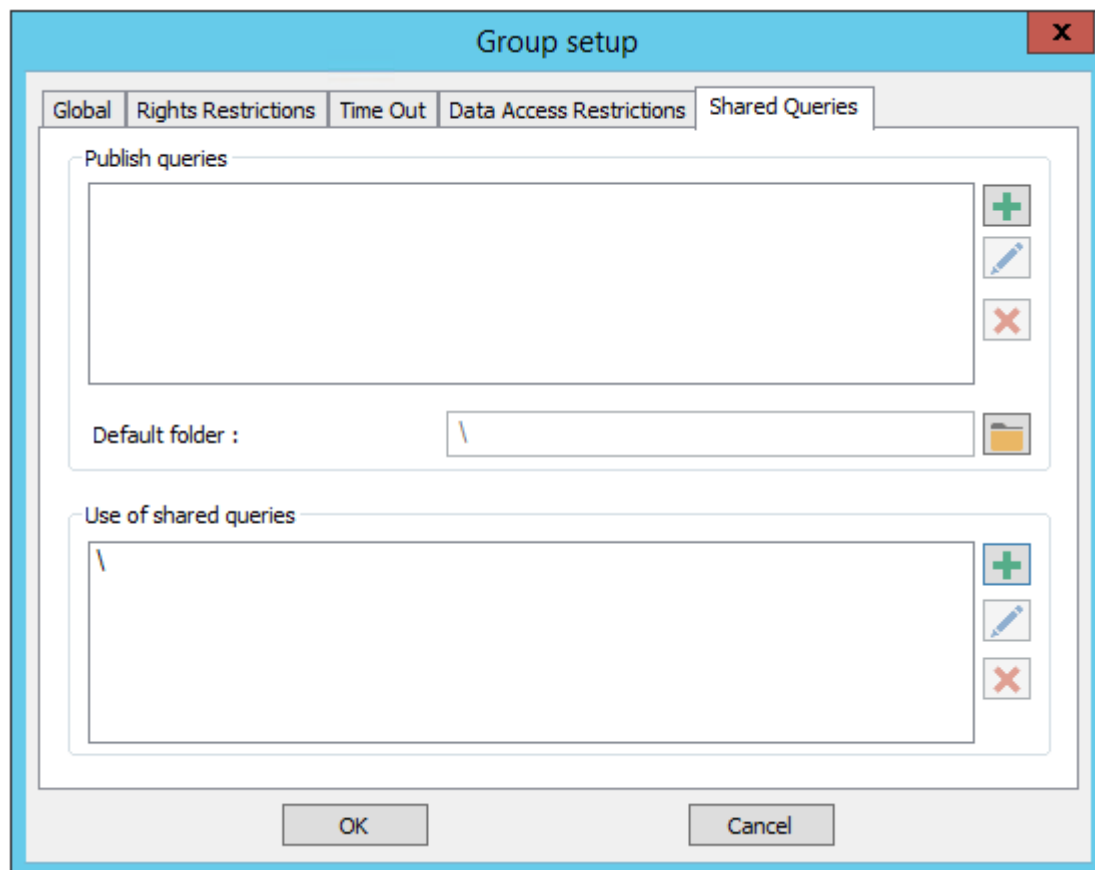


The image shows a dialog box titled "Data Access Restrictions" with a blue header bar and a red close button (X) in the top right corner. Inside the dialog, there is a tabbed interface. The first tab, "Field Restrictions", is selected and contains the text "Set restrictions for values related to a field 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 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

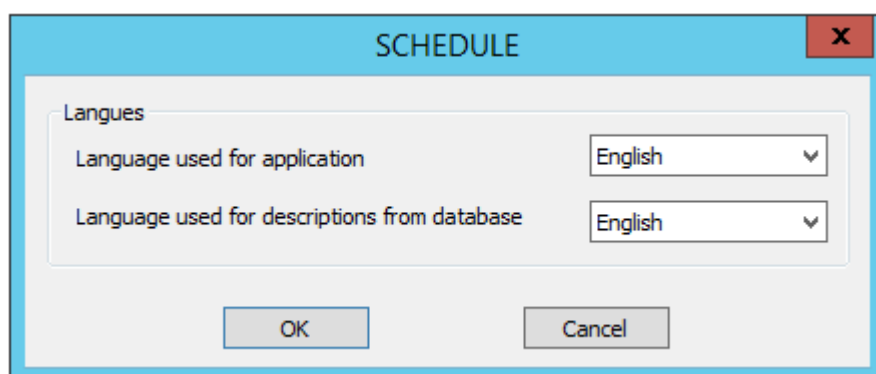
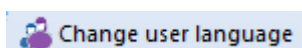
This setting allows you to :

- 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=1600091604

Last update: **2020/09/14 15:53**

