Authorizations

After you have added all required authorization objects, you have to apply them to the dedicated data models.

To do so, open the authorizations tab in your data model.

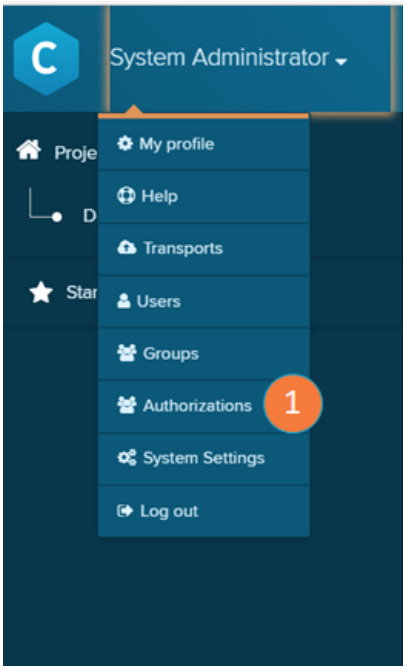
You should see all added Authorization Objects in the bottom left box.

To deploy an authorization object to the data model, simply hover over it and click on the emerging *add* button.

Authorization objects are a handy way to manage access to data within an analysis project.

Authorization objects are typically used to restrict access for users/groups to the data necessary for their field of work. This can be for example regional (by market, country, and continent), division (company code) or client based. Therefore, to use Authorization Objects you must first create them and then assign them to a user and to a data model.

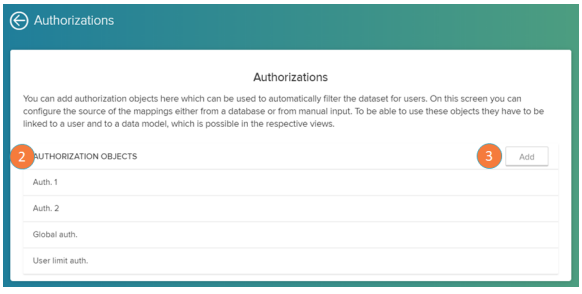
Add Authorization Objects



To enable authorizations, you first have to add authorization objects to Celonis 4.

Therefore, navigate to the Homescreen and choose Authorizations (item 1) from the main menu.

1. Authorizations: click here to open the authorizations screen.
2. Authorization objects: list of already created authorization objects. Click on them to view their properties.
3. Add authorizations: click to create new authorization objects.
4. Name: name of the authorization object.
5. Value mapping: here you can decide whether the values for your mapping should be queried from a database or entered manually.



A. Values queried from a database

Pre-configure your connection and queries in a configuration file on the application server.

6. Database source: select the database that contain the authorization queries.

7. Global: select this ticker if you want your authorization to be active for all users or groups.

8. Automatic sync: select this ticker if you want your authorization to be automatically queried and define the time interval between syncs.

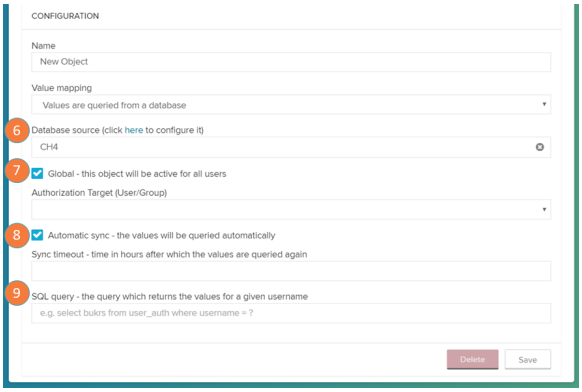
9. SQL query: define the query that returns values according to a given username.

If the 'Add' button (item 3) is clicked:

B. Values entered manually

Choose this option if you want to add the allowed values manually. However, please be aware that the values have to be adapted every time they change, as they are not queried from any external data source.

A. Values queried from a database

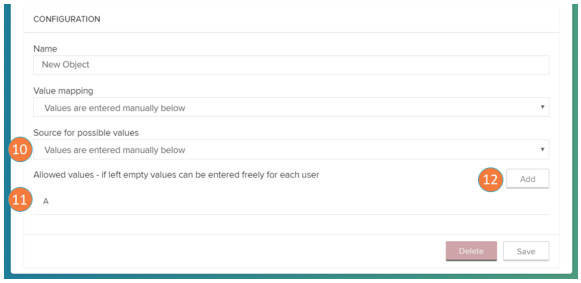


10. Source for possible values: define a source which contains possible values that may be filtered.

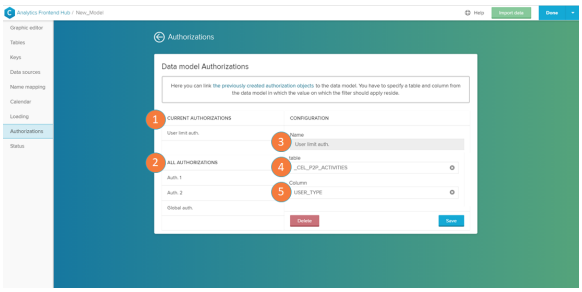
11. Allowed values: list of allowed values.

12. Add: add a new allowed value.

B. Values entered manually



Application to data models



After you have added all required authorization objects, you have to apply them to the dedicated data models.

To do so, open the authorizations tab in your Data Model.

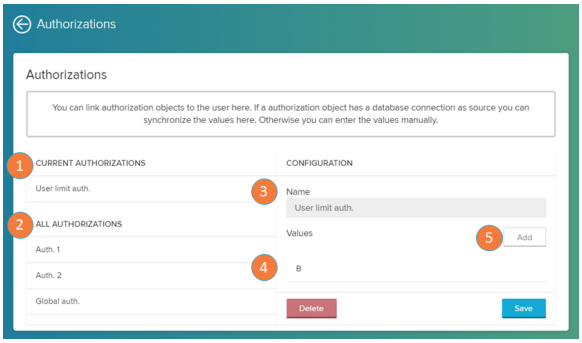
1. Current authorizations: authorizations that were already applied in this data model. Click on one to view its properties.
2. All authorizations: authorizations that have still not been applied in this data model. To deploy an authorization object to the data model, simply hover over it and click on the emerging add button.
3. Name: name of the selected authorization.
4. Table: table in which the authorization filter will be applied.
5. Column: column of the selected table above in which which the authorization filter will be applied.

Once the authorization is created or edited, confirm your operation with the 'Save' button.

Application to user

In this step, you have to apply the authorizations to the respective users /groups.

To do so, click on 'Manage authorizations' on the desired User Profile (see item 5 of the 'User Profile' section in the 'User Profile' page).



1. Current authorizations: authorizations that were already applied to this user. Click on one to view its properties.
2. All authorizations: authorizations that have still not been applied to this user. To deploy an authorization object to the data model, simply hover over it and click on the emerging add button.
3. Name: name of the selected authorization.
4. Values: list of values which the user is allowed to see.
5. Add: add new values to this authorization.

Once the authorization is created or edited, confirm your operation with the 'Save' button. After this is done, the user can only view the part of the data you have authorized him/her to see.