Permissions On Cubes For Individual Users

Design-time permissions on cubes let users read, update, and delete cubes. Runtime permissions on cubes let users query cubes and create Hive tables from SELECT statements on cubes. You can choose whether to grant these permissions to all users, or to individual users.

Before You Begin

- Ensure that you are logged into AtScale as either a super user or an administrator for the organization for the project or cube that you want to grant permissions on.
- If you are using local authentication for your users, ensure that the users that you want to grant permissions to have been added to AtScale.

  

  Use AtScale's local directory service for testing only. Do not use it in production environments. This directory service is not meant to support the types of workloads that are common to production environments. Before using AtScale in production, configure your AtScale organization to use an external directory service, such as Microsoft Active Directory, another LDAP service, or Google G Suite Directory.

- When using external authentication for your users, ensure the following:
  - Groups in your directory service are mapped to AtScale roles
  - The user accounts that you want to grant permissions to are synchronized to AtScale.
- Note that project and cube creators cannot have the permissions disabled on the projects they have created.

Default Permissions For New Cubes

By default, AtScale grants cube permissions to all users in the external directory service you are using. If you want only the creator of a new cube (and also administrators) to have all permissions:

1. Go to **Settings > Organization Settings > Options**.
2. Locate the **Default Project/Cube Security** option.
3. Choose the **Override & Enable** button for this option.

Procedure

Access the cube permissions dialog as described in Grant Design-Time Permissions.

To grant runtime permissions:

1. Select **Security > Runtime Permissions**. The Cube Runtime Permissions dialog box opens.
2. Enable the **Restrict Access** toggle.
3. Optionally, enable the **Enforce Restricted Access to Simple & Calculated Measures** toggle.
4. In the **Users** list, expand the users you want to set permissions for, and enable/disable the following permissions as needed.

Runtime Permission	Description
Create Table as Select (CTAS)	Users can issue `SELECT` statements against the cube and write the results back to the data warehouse as a new table. If you are using Google BigQuery, the tables are created directly in BigQuery. If you are using a Hadoop cluster, the tables are created in the Hive metastore.
Query	Users can issue `SELECT` statements against the cube.
Access All Measures	Only available when **Enforce Restricted Access to Simple & Calculated Measures** is enabled. When selected, users can access all measures in the cube. Alternatively, you can configure access to specific measures by selecting the checkboxes next to the folders and individual measures in the list. You can also use the text box to filter for specific measures, then click the **Check All Displayed** button to enable access to just the matching measures. **Note:** This functionality is not availale for secondary metrical attributes.

5. Save your changes.

You must publish the cube for any changes to its runtime permissions to take effect.

To grant design-time permissions:

1. Choose **Security > Design Permissions**.
2. Enable **Restrict Access** to grant permissions to a subset of the users.

3. Choose which permissions to give to each user:

    - Read: Can see the cube connection information. Can duplicate a cube (if you also have project update permission)
    - Update: Can open the cube design canvas and edit the cube model and settings.
    - Delete: Can delete the specific cube from the project.

4. Save your changes.