Configuring Permissions On Deployed Models

You can configure runtime permissions on deployed models and perspectives to control which users can access them from BI tools. These permissions can be set at the user or group level.

> **Note:** By default, deployed catalogs and models are available to all users in the **Everyone** user group. You can change this behavior using the `catalog.deployment.restriction.enabled` engine setting. For more information, see Catalog Settings and Changing Engine Settings.

To set runtime permissions on a deployed model or perspective:

1. In Design Center, click **Deployed Catalogs** in the main navigation bar. The **Deployed Catalogs** panel opens.
2. Select the deployed catalog in the list, then click the **Permissions** tab.
3. Edit the permissions for the deployed models and perspectives as needed. You can do any of the following:

   - Click **+ Permissions** to add a new group of permissions.
   - Click the pencil icon next to a permission group name to edit it.
   - In the **Scope** section, select the specific permissions you want to set:

     - **Create Table as Select (CTAS)**: Users can issue `SELECT` statements against the model 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.
     - **Query**: Users can issue `SELECT` statements against the model.
     - **Discovery**

   - In the **Users and Groups** section, select the individual users and groups you want to set these permissions for.

4. Click **Save**.