Overview of Authorization

Contents:

Authorization governs how Designer Cloud Powered by Trifacta® Enterprise Edition users can access platform features and user-defined objects in the Designer Cloud application .

> **NOTE:** Authorization manages access to object types. It does not cover access to individual objects of a specified type. For example, access to a specific flow is governed by ownership of the flow (owner) and sharing of the flow by the owner (to a collaborator). If a flow is shared with a user who is not permitted to access flows, then the user cannot access the flow.

Resource Roles and Privileges

Access to Trifacta objects is governed by roles in the user account.

- A **role** is a set of zero or more privileges. A user may have one or more assigned roles.

  > **NOTE:** Roles are additive. If a user has multiple roles, the user has access at the highest level of privileges from each role.

- A **privilege** is an access level for a type of object. A role may have one or more privileges assigned to it.
- All accounts are created with the `default` role, which provides a set of basic privileges.

Standard roles

default role

All new users are automatically assigned the `default` role. By default, the `default` role enables full access to all types of Trifacta objects.

- If you have upgraded from a version of the product that did not support authorization, the `default` role represents no change in behavior. All existing users can access Trifacta objects as normal.

Since roles in a user account are additive, you may choose to reduce the privileges on the `default` role and then add privileges selectively by creating other roles and assigning them to users. See the example below.

> **NOTE:** You can modify the `default` role. You can also remove it from a user account. You cannot delete the role.

> **NOTE:** In future releases of the software, additional objects may be made available. A level of access may be defined in the `default` role. No other roles will be modified.

Workspace admin role

This admin role is a super-user. The admin role enables all capabilities of the `default` role, plus:

- access to all Designer Cloud application objects, unless specifically limited. See Resource Roles and Privileges below.
- administration functions and settings within the Designer Cloud application .

> **NOTE:** This role enables for the user owner-level access to all objects in the project or workspace and access to all admin-level settings and configuration pages in the admin console. This role should not be assigned to many users. At least one user should always have this role.

> **NOTE:** A platform administrator is automatically granted the admin role.

Custom role(s)

As needed, administrators can create custom roles for users of the project or workspace. For more information, see *Create Role*.

Privileges

For a complete list of privileges for each type of object, see *Privileges and Roles Reference*.

Example model

In the following model, three separate roles have been created. Each role enables the highest level of access to a specific type of object.

The `default` object has been modified:

- Since all users are automatically granted the `default` role, the scope of its permissions has been reduced here to view-only.
- There is no `viewer` privilege for Plans (`none`, `author`).

> **NOTE:** Depending on your product edition, some of these privileges may not be applicable.

Privilege/Role	default	Role A	Role B	Role C	Notes
Flows	viewer	author	none	none	
Connections	viewer	none	author	none	Paid product editions only
Plans	none	none	none	author	Premium product editions only
User defined functions	viewer	none	none	author	Dataprep by Trifacta product editions only

User 1:

Roles: `default`

- User can see flows in Flows page. User cannot schedule, modify, or create new ones.
- User can see connections in the Connections page. User cannot schedule, modify, or create new ones.
- User cannot access the Plans page.
- User can invoke UDFs but cannot create, modify or delete them.

User 2:

Roles: `default`, `Role A`

- User can create, schedule, modify, run jobs, and delete flows (full privileges).
- User can see connections in the Connections page. User cannot schedule, modify, or create new ones.
- User cannot access the Plans page.
- User can invoke UDFs but cannot create, modify or delete them.

User 3:

Roles: `Role A`, `Role B`, `Role C`

- User can create, schedule, modify, run jobs, and delete flows (full privileges).
- User can create, modify, and delete connections (full privileges).
- User can create, schedule, modify, run jobs, and delete plans (full privileges).
- User can create, modify, and delete UDFs.