Workspace Admin Permissions

Contents:

The workspace admin user is super-user for the entire workspace.

> **NOTE:** In Trifacta Self-Managed Enterprise Edition, any user who is granted the admin role is also granted the workspace admin role, which enables owner-level access to some object types in the workspace. Details are below.

Configuration

The workspace admin can enable and disable features and capabilities in the workspace. For more information, see *Workspace Settings Page*.

User Management

A workspace admin can administer all of the other users of the workspace, including disabling or deleting the user.

> **NOTE:** In Trifacta Self-Managed Enterprise Edition, the workspace admin can also edit the platform roles assigned to individual users. For more information, see *Manage Users*.

Object Access

A workspace admin has owner-level access to objects in the workspace.

> **NOTE:** A workspace admin can access these objects like their owners, even if the objects have not been shared.

This access applies, but is not limited, to the following types of objects:

- Flows
- Connections (see below)
- Output objects
- Job profiles and results

- Plans and tasks

A workspace admin has collaborator-level access to the following objects:

- Imported datasets
- Macros
- Schedules

A workspace admin does not have any changed permissions for access to the following object types:

- Deployments and releases

Data Access

The workspace admin can access the data of individual users under the following conditions.

> **NOTE:** Workspace admin privileges do not affect access permissions on outside storage systems. Those systems can prevent data access by the workspace admin user.

Connections with credentials:

If the data is accessed through a connection that requires a specific set of credentials, then the workspace admin can access all data available through the connection when the credentials are shared.

> **If connection credential sharing is disabled after a connection has already been shared with credentials, then the connection remains accessible to the workspace admin and to all users who were previously shared the connection. Workspace admins created in the future also inherit this access. The sharing of a connection's credentials cannot be revoked, except by deleting the connection.**

A workspace admin cannot:

1. Modify or remove the shared credentials.
2. Change the credential sharing on another user's connection.

If a connection with shared credentials remains after credential sharing has been disabled, you can do one of the following for the connection:

- Edit the connection to use credentials that are safe to share with all affected users.
- Create a duplicate connection with private credentials. Delete the old shared connection.

For more information on credential sharing, see *Configure Sharing*.**File-based backend storage:**

Source datasets and job results that are stored on file-based backend storage systems for individual users can be accessed by the workspace admin except in the following situations:

- If users have user-specific access controls to the storage, such as secure impersonation, the workspace admin can only access a user's data if the admin's own permissions enable it.
- Directory permissions on user directories may prevent the workspace admin from accessing a user's data. For example, the workspace admin user can see the link to a user's job results that were written on the backend storage. However, when the workspace admin attempts to download those results, a permissions error is displayed, since the workspace admin user does not have permissions on the directory.

Relational connections:

Data is accessible under the connections with credentials limitations described above.