Overview of Authorization

Contents:

Authorization governs how workspace members can access platform features and user-defined objects in the workspace.

> **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.

Account Roles

In a workspace, a member can have one of the following roles:

Member role

The Member role enables the user to access all product functionality that is enabled within the workspace for the product edition.

Admin role

The Admin role enables all capabilities of the Member role, plus:

- access to all workspace objects, unless specifically limited. See Resource Roles and Privileges below.
- administration functions and settings for the workspace.

> **NOTE:** The workspace Admin role is a super-user. It should be granted on a limited basis.

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

Resource Roles and Privileges

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

- A **role** is a set of zero or more privileges.
- A **privilege** is an access level for a type of object in the workspace.

- A user may have one or more roles in it.

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

- All accounts are created with the `default` role.

Standard roles

default role

All new users are automatically assigned the `default` role. By default, the `default` role enables full access to all workspace 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 workspace 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 workspace 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

The Workspace admin role is a super-user.

> **NOTE:** This role enables for the user owner-level access to all objects in the 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 the `Workspace admin` 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 workspace 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 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 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 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).