


## Create & Modify Roles

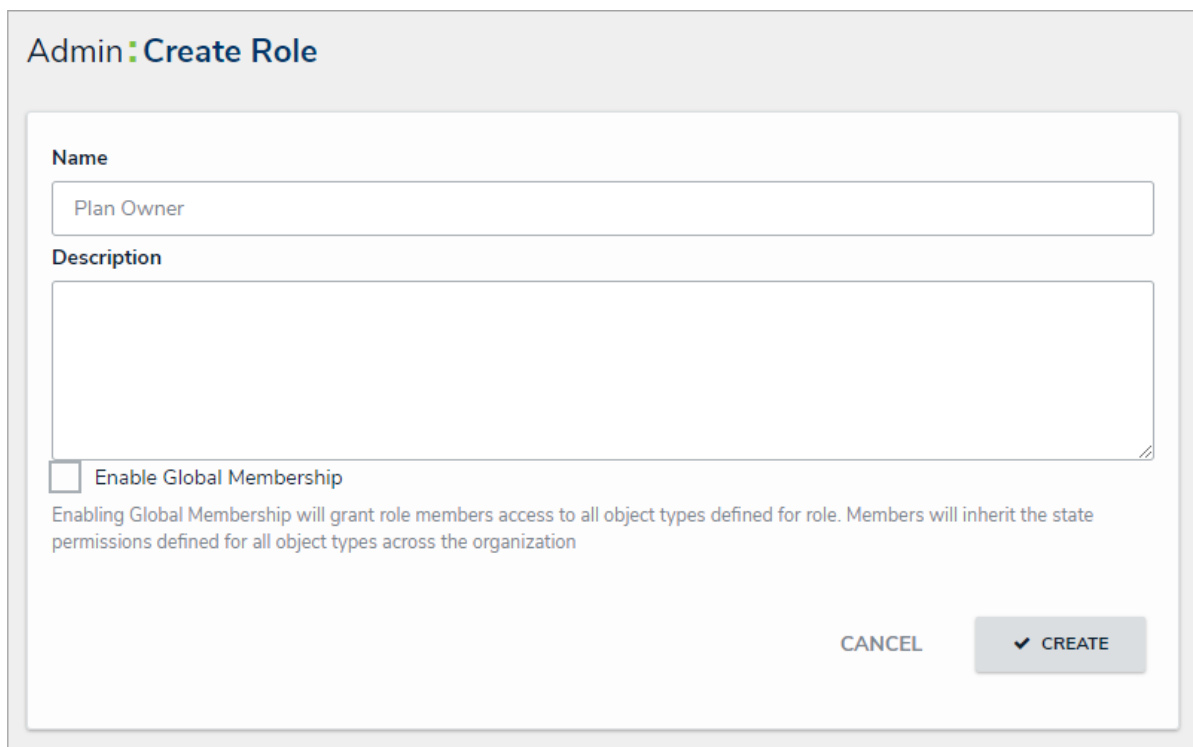
The enabled triggers and permissions in the following steps are recommended; however, you can adjust these triggers and permissions as needed.

To avoid creating duplicate data, it's recommended that admins perform a search to confirm the following roles don't already exist in their organization. For more detailed information on roles and permissions, see the [Roles](#) section and [Workflow Permissions](#) article in the **Resolver Core Administrator's Guide**.

## Create a New Role

### To create a new role:

1. Click the  icon in the top bar > **Roles** in the **People** section.
2. Click **Create Role** to display the **Create Role** page.
3. Enter **Plan Owner** in the **Name** field.
4. Ensure the **Enable Global Membership** checkbox is **not** selected.



Admin: Create Role

**Name**

Plan Owner

**Description**


Enable Global Membership

Enabling Global Membership will grant role members access to all object types defined for role. Members will inherit the state permissions defined for all object types across the organization


CANCEL

5. *The Create Role page.*
6. Click **Create** to display the **Edit Role** page.
7. In the **Object Types** section, begin typing, then select **Risk Response Plan**.

Admin: **Edit Role**

Plan Owner 

Object Types

Risk Response Plan  [EDIT PERMISSIONS](#)

Users

*The Edit Role page.*

8. Click **Edit Permissions**.
9. On the **Active** state:
  - a. Enable **Read** permissions.
  - b. Select the **Risk Response Plan - Plan Owner** form.
10. On the **Pending Update** state:
  - a. Enable **Read**, **Edit**, and **Assign** permissions.
  - b. Enable the **Complete** update trigger.
  - c. Select the **Risk Response Plan - Plan Owner** form.

The screenshot displays three sections for workflow permissions, each corresponding to a different state:


- Active:** Features a blue circle icon. Action buttons include READ, EDIT, DELETE, and MANAGE. A 'Triggers' section contains ARCHIVE and ASSIGN buttons. A dropdown menu is set to 'Risk Response Plan - Plan Owner'.
- Archived:** Features a black circle icon. Action buttons include READ, EDIT, DELETE, and MANAGE. A 'Triggers' section contains an ASSIGN button. A dropdown menu is set to 'Default'.
- Pending Update:** Features a yellow circle icon. Action buttons include READ, EDIT, DELETE, and MANAGE. A 'Triggers' section contains COMPLETE UPDATE and ASSIGN buttons. A dropdown menu is set to 'Risk Response Plan - Plan Owner'.

*Workflow permission.*

11. Click **Done** to return to the previous page.
12. Add the appropriate users and/or user groups to the role through the **Users** and **Groups** sections on the **Edit Role** page. See the [Users](#) and [User Groups](#) sections in the **Resolver Core Administrator's Guide** for more information.

## Modify Existing Roles

### To modify the permissions on existing roles:

1. Click the  icon in the top bar > **Roles** in the **People** section.
2. Select the **Risk Team** role.
3. Select the **Risk Response Plan** object type in the **Object Types** section, then click **Edit Permissions**.
4. Enable the **All Triggers**, **Create**, **Read**, **Edit**, and **Manage** permissions at the top of the page for all workflow states.
5. Select the **Risk Response Plan - Risk Team** form for all workflow states.
6. Repeat steps 1-3 for the **Risk Owner** role.
7. Enable the **All Triggers**, **Create**, **Read**, **Edit**, and **Manage** permissions.
8. Select the **Risk Response Plan - Risk Team** form for all workflow states.

