Managing roles and permissions

Admin users are assigned roles that reflect their abilities at the workspace level. Granular permissions are assigned to each role.

Coro has three predefined roles, which can't be edited or deleted:

- **Viewer**: Can view content.
- **Administrator**: Can view and edit content.
- **Super admin**: Can view and edit content. Additionally, only super admins can reassign roles to admin users.

> **Note**
>
> You can't remove the last super admin of a workspace.

Permissions are categorized into the following options:

- **No Access**: The admin user cannot see or interact with the section.
- **Can View**: The admin user can see the section but cannot make changes.
- **Can Edit**: The admin user can view and make changes to the section.

Channel admins can create child workspaces and are automatically added as admin users with super admin permissions. Their roles can be changed within the child workspace. This role is managed at the workspace level, and permissions in one child workspace do not affect roles in other child workspaces. If the channel admin is deleted as an admin user from a child workspace, they still have access with super admin permissions.

To access **Roles**:

1. **Sign into the Coro console**.
2. Navigate to **Control Panel > Access Control**: