Creating custom roles

Each service maps specific actions that you can perform within the context of the service to platform or service roles. From the Roles page, you can view all of the available roles in the account and all roles for a specific service, including the actions that are mapped to each. You can pick and choose actions from all of the roles for a specific service to combine into a custom role of your choice.

Many services map different sets of actions to different platform or service roles. However, you might want to combine some of the actions that are currently spread across multiple roles for a service to make assigning meet your custom use case. With a custom role, you can pick and choose actions mapped to different roles so that next time you assign access to the service, you don't have to select three different roles, for example.

**Required access**

Anyone can view the available roles in the account on Roles page, but to create, edit, or delete a custom role, you must be assigned specific access for the Role management account management service.

| **Role** | **Actions** |
| --- | --- |
| Editor | Can edit and update the role display name, description, and the actions mapped to it. |
| Administrator | Create, edit, update, and delete custom roles and assign other users in the account access to the Role management service |
| Table 1. Actions for Role management service | |

**Creating custom roles**

You can create new roles that are scoped to single services. This means that you can't combine actions for two different services in a custom role, but you can combine as many actions that you want into a new role for a single service. After you create a custom role with a name of your choosing, anyone in the account who can assign access to a particular service can use that role when assigning access.

Custom roles can be created only for individual IAM-enabled services. A custom role can't be created for the options of all account management services or all IAM-enabled services.

1. In the IBM Cloud® console, go to **Manage** > **Access (IAM)**, and select **Roles**.
2. Click **Create**.
3. Enter a name for your role. This name must be unique within the account. Users see this role name in the console when they assign access to the service.
4. Enter an ID for the role. This ID is used in the CRN, which is used when assigning access by using the API. The role ID must begin with a capital letter and use alphanumeric characters only.
5. Optional: Enter a succinct and helpful description that helps the users who are assigning access know what level of access this role assignment gives a user. This description also shows in the console when a user assigns access to the service.
6. Select a service that you want to create the role for.
7. Review the available actions, and select **Add** for all actions that you want in your new role.

You must add at least one service-defined action to successfully create the new role. If you aren't sure which actions are defined by the service, look in the Type column.

1. Click **Create** when you're done adding actions.

If a service removes an action that you use in a custom role, the custom role is not updated, and might not be valid anymore if the role contained only the removed actions.

If you plan to delete a custom role because it is no longer needed, you must be assigned the Administrator role on the Role management service. Deleting a custom role automatically updates access for any users, access groups, or service IDs assigned access by using that role to remove it from any existing policies.