Managing access to resources

To manage access for users or service IDs by using IAM policies, you must be the account owner or have the correct access assigned. To assign user's access to resources you must be an administrator on all services in the account, or the assigned administrator for the particular service or service instance. To assign acces to a service ID, you must be administrator on the identity service or the specific service ID.

**Assigning access**

You can assign access to resources by using two types of policies:

* Access to resources within a resource group, including the option for just one resource or all
* Access to resources in the account, including the option for just one type or all types

If you delete or edit an existing policy for a service ID currently being used, it might cause service interruption.

If you want to enable a user full administrator access to complete [account management tasks](https://cloud.ibm.com/docs/account?topic=account-account-services#account-services), such as inviting and removing users, viewing billing and usage, managing service IDs, managing access groups, managing user access, and access to all account resources, you must assign a user the following access:

* A policy for **All Identity and Access enabled services** within the **Account** with the Administrator and Manager roles.
* A policy with Administrator role on **All Account Management Services**.

Access to resources within a resource group

To assign access to all resources in a resource group or to just one service within a resource group, complete the following steps:

1. In the console, click **Manage** > **Access (IAM)**, and select **Users** or **Manage** > **Access (IAM)**, and select **Service IDs**, depending on which identity you want to assign access.
2. From the row for the user or service ID that you want to assign access, select the **Actions**  menu, and click **Assign access**.
3. Add the user or service ID to an access group. Click **Add** for the access group that you want the user or service ID to belong to.
4. (Optional) Manually assign additional access.
   1. Expand the Assign additional access section, and click **IAM services**.
   2. Select the option for all services or just a specific service, and then specify if the access is in the **Account**, which means the user or service ID doesn't get access to the resource group that contains the resource, or select a specific resource group. By selecting a resource group, you can select roles for access to manage the resource group as well.
   3. Select any combination of roles to assign, and click **Add** > **Assign**.

Access to resources

To assign access to an individual resource in the account or access to all resources in the account, complete the following steps:

1. In the console, click **Manage** > **Access (IAM)**, and select **Users** or **Manage** > **Access (IAM)**, and select **Service IDs**, depending on which identity you want to assign access.
2. From the row for the user or service ID that you want to assign access, select the **Actions**  menu > **Assign access**.
3. Add the user or service ID to an access group. Click **Add** for the access group that you want the user or service ID to belong to.
4. (Optional) Manually assign users access.
   1. Expand the Assign additional access section, and click **IAM services**.
   2. Select the option for all services or just a specific service.
   3. Select any combination of roles to assign the user or service ID, and click **Add** > **Assign**.

If a user doesn't have a role on the resource group that contains the resources, they can see the resources, but can't access the resources by going to the Resource list page in the account to start working with them. Assign the Viewer role or higher on the resource group itself to ensure a user can access the resource.

**Removing access**

Removing access for a user or service ID can take up to 10 minutes to take effect.

1. In the console, click **Manage** > **Access (IAM)**, and select **Users** or **Manage** > **Access (IAM)**, and select **Service IDs**, depending on which identity you want to assign access.
2. Select the user's name or service ID that you want to remove access for.
3. From the **Access policies** tab, select the **Actions**  menu on the row for the policy you want to remove, and click **Remove**.
4. Review the policy details that you're about to remove, and confirm by clicking **Remove**.

You can also remove users and service IDs from access groups by selecting the check box for the user or service ID that you want to remove, and click **Remove**. Then, click **Remove** again to approve the process.

Removing access by using the CLI

To remove a user policy by using the CLI, you can use the **[ibmcloud iam user-policy-delete](https://cloud.ibm.com/docs/cli?topic=cli-ibmcloud_commands_iam" \l "ibmcloud_iam_user_policy_delete)** command.

ibmcloud iam user-policy-delete USER\_ID POLICY\_ID [-f, --force]

To remove a service ID policy by using the CLI, you can use the **[ibmcloud iam service-policy-delete](https://cloud.ibm.com/docs/cli?topic=cli-ibmcloud_commands_iam" \l "ibmcloud_iam_service_policy_delete)** command.

ibmcloud iam service-policy-delete SERVICE\_ID POLICY\_ID [-f, --force]

**Reviewing assigned access**

If you need to review your assigned access in an account that you've been added to, complete the following steps:

1. In the console, click **Manage** > **Access (IAM)**, and select **Users** or **Manage** > **Access (IAM)**, and select **Service IDs**, depending on which identity you want to review.
2. Select your name or the service ID.
3. Review the assigned access in the **Access policies** section.

If you need more access, you must contact the account owner to update your access or contact the administrator for the service or service instance to update the access policy.