Setting up access groups

An access group can be created to organize a set of users and service IDs into a single entity that makes it easy for you to assign access. You can assign a single policy to the group instead of assigning the same access multiple times per individual user or service ID.

To manage or create new access groups, you must have the following type of access:

* Account owner
* Administrator or editor on the IAM Access Groups account management service in the account
* Administrator or editor for the all Account Management Services

Additionally, an administrator or editor can be assigned access to manage an individual group by creating an access policy where the resource is the Access group ID. For more information about access policies and roles for the IAM Access Groups service, see [IAM access](https://cloud.ibm.com/docs/account?topic=account-userroles#userroles).

To make assigning and managing access even easier, you can set up resource groups to organize a set of resources that you want a group of users to have access to. When your resource group is set up, you can assign a policy that gives access to all resources within that group instead of creating access policies for individual service instances within your account.

**Creating an access group**

To create an access group, complete the following steps:

1. In the IBM Cloud console, click **Manage** > **Access (IAM)**, and select **Access Groups**.
2. Click **Create**.
3. Enter a name and optional description for your group, and click **Create**.

Next, continue to set up your group by adding users or service IDs. Or, you can start assigning the group access, and decide who you want to add to the access group later.

You can delete a group by selecting the **Remove group** option. When you remove a group from the account, you are removing all users and service IDs from the group and all access that is assigned to the group.

To create an access group by using the CLI, you can use the [ibmcloud iam access-group-create](https://cloud.ibm.com/docs/cli?topic=cli-ibmcloud_commands_iam" \l "ibmcloud_iam_access_group_policy_create) command.

ibmcloud iam access-group-create GROUP\_NAME [-d, --description DESCRIPTION]

**Assigning access to a group**

After you set up your group with users and service IDs, you can assign a common access policy to the group. Remember, any policy that you set for the group applies to all entities within the group.

1. In the console, click **Manage** > **Access (IAM)**, and select **Access Groups**.
2. From the row for the group that you want to assign access, select the **Actions**  menu, and click **Assign access**.
3. Add one or more of the access options that you manage. You must assign at least one access option. For any access options that you don't add and configure, the default value of **No access** is assigned. Depending on the options that you are authorized to manage, you can assign the following types of access:
   * Select **IAM services**, and then select the option for all services or just a specific service. Next, you can scope the access to the entire account, all resource groups, or just one resource group. Then, select all roles that apply. To view what actions are mapped to each role, click the **Actions for role** option to view a list of all actions that are mapped to a specific role.  
       
     Some services support the use of advanced operators to grant access to resources that satisfy specific naming conventions. See [Assigning access by using wildcard policies](https://cloud.ibm.com/docs/account?topic=account-wildcard) for more information.

If you select the **Account** scope for the access policy, the user must already have the Viewer role or higher on the resource group or groups that contain the resources you want the user to have access to. Without a role on a resource group, the user can't work with the resource from the Resource list page in the console.

* + Select **Account management**, and then choose from the all account management services option or select a specific service. Then, select all roles that apply.

1. Click **Add** > **Assign**.

To create an access group policy by using the CLI, you can use the [ibmcloud iam access-group-policy-create](https://cloud.ibm.com/docs/cli?topic=cli-ibmcloud_commands_iam" \l "ibmcloud_iam_access_group_policy_create) command.

ibmcloud iam access-group-policy-create GROUP\_NAME {-f, --file @JSON\_FILE | --roles ROLE\_NAME1,ROLE\_NAME2... [--service-name SERVICE\_NAME] [--service-instance SERVICE\_INSTANCE] [--region REGION] [--resource-type RESOURCE\_TYPE] [--resource RESOURCE] [--resource-group-name RESOURCE\_GROUP\_NAME] [--resource-group-id RESOURCE\_GROUP\_ID]}