Inviting users

Get up and running quickly with IBM Cloud Identity and Access Management (IAM) by setting up access groups for quick access assignments, inviting users to your account, and managing their access.

This tutorial is for IAM-enabled resources. For services that don't support creating IAM policies for managing access, you can use [Cloud Foundry access](https://cloud.ibm.com/docs/account?topic=account-cfaccess) or [classic infrastructure permissions](https://cloud.ibm.com/docs/account?topic=account-infrapermission).

**Before you begin**

If you are new to using IAM, check out the following documentation to learn more about the features, concepts, and components of the access management system:

* [IBM Cloud Identity and Access Management](https://cloud.ibm.com/docs/account?topic=account-iamoverview) provides a quick overview of what IAM is in IBM Cloud, the available features, and links to available CLI and API docs.
* [IAM access](https://cloud.ibm.com/docs/account?topic=account-userroles) gives a more in-depth review of how access management works by using access policies.

**Step 1: Create access groups**

To streamline the process of assigning access to users in your account, you can create an access group. Access groups are a way to organize users and service IDs so that you can easily assign access by adding one or more policies for the entire group. Then, you can add or remove users and service IDs as needed instead of assigning individual access to each user.

Set up your groups

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.
4. Click **Create**.

Next, continue to set up your group by adding users or service IDs:

1. Select the name of the group that you want to update.
2. Click **Add users**.
3. Select the users that you want to add from the list, and click **Add to group**.
4. To add service IDs to the group, click **Service IDs**.
5. Select the IDs that you want to add from the list, and click **Add to group**.

Assign access to your groups

After you create your access groups, you can assign access to all members of the group with one or more policies. By assigning a group of users access to a group of resources with a single policy, you reduce the overall number of policies that you need to manage.

1. From the **Access policies** tab, click **Assign access**.
2. Select **IAM services** or **Account management**.
3. Select the type of access that you want to assign.

If you're assigning access to IAM-enabled services, 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.

1. Click **Add**. Repeat as needed to add more access.
2. Click **Assign** to assign all added access to your access group.

**Step 2: Invite users**

You can invite one or multiple users in a single invite. If you invite multiple users in one invitation, the same access is assigned to each user. However, you can invite users to your account with no access, and assign them access later.

1. In the console, go to **Manage** > **Access (IAM)**, and select **Users**.
2. Click **Invite users**. Specify the email addresses of the users. If you are inviting more than one user with a single invitation, they are all assigned the same 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:
   * Add users to access groups. Click **Add** for each access group that you want the users to belong to.
   * Manually assign users access. Expand this section to assign individual IAM access policies, Cloud Foundry roles, or classic infrastructure permissions.
     + Select **Cloud Foundry** > an organization > a region to select a specific space, and assign a space role. An organization and space role are both required to add the access assignment to the invite.
     + Select **Classic infrastructure**, and then select from the three permission sets.
     + 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 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. Select **Add** to save the access assignment to the invitation.
2. After you add all the necessary access assignments, click **Invite**.

For more information, see [Inviting users to an account](https://cloud.ibm.com/docs/account?topic=account-iamuserinv).

**Step 3: Manage access for existing users**

After you invite users, you might want to assign more access or edit the existing access to ensure that all members of your account have the correct level of access.

Assigning new access

To assign a new access policy, complete the following steps:

1. In the console, click **Manage** > **Access (IAM)**, and select **Users**.
2. From the row for the user that you want to assign access, select the **Actions**  menu, and click **Assign access**.
3. Click **Add** for each access group that you want the users to belong to.
4. (Optional) If you want to assign additional access to Cloud Foundry roles, classic infrastructure permissions, individual IAM services, or account management services, expand the Assign users additional access section.
5. Select any combination of roles or permissions to define the scope of access, and click **Add**. For more information, see [Cloud IAM roles](https://cloud.ibm.com/docs/account?topic=account-userroles#iamusermanrol).
6. Click **Assign** to assign all added access to the selected user.

Assign the viewer role or higher to the resource group that contains the resource to ensure that the user can access the resource from their list of resources.

Editing existing access

You can update existing access by editing the assigned roles for a user.

1. In the console, click **Manage** > **Access (IAM)**, and select **Users**.
2. Select the name of the user that you want to edit access for.
3. Click **Access policies**.
4. Click **Edit** from the **Actions**  menu on the row for the policy that you want to edit.
5. Edit the policy by updating the assigned roles.
6. Click **Save**.

**Next steps**

Learn what else you can do with IBM Cloud IAM by checking out the [features list](https://cloud.ibm.com/docs/account?topic=account-iamoverview#features).

Language:

English