Managing public access to resources

By default, all users and service IDs in an account are members of the Public Access group in your account. Assigning an access policy to the access group opens access to that resource to anyone whether they're a member of your account or not because authentication is no longer required. However, in some cases you might want to ensure that there is never public access that is allowed to your account resources, which you control by disabling public access at the account level.

To manage public access, you must be an administrator of the [IAM Access Groups service](https://cloud.ibm.com/docs/account?topic=account-account-services#access-groups-account-management) in the account.

**Assigning public access to resources**

When public access is enabled in the account, you can create a policy to define the resources that all members of the Public Access group can access. To create a policy, you must have administrator access on the resource.

IBM® Cloud Object Storage is used as the example as it is the only supported resource type for public access at this time. As an example, the following section describes how to assign public access to an Object Storage bucket that is named mybucket123.

Assigning access in the console

1. In the IBM Cloud console, click **Manage** > **Access (IAM)**, and select **Access groups**.
2. Click the name of the public access group > **Assign access**.
3. Select **Object Storage** from the **Services** list.
4. Select the specific instance from the **Service instance** list.
5. Enter bucket for the resource type.
6. Enter mybucket123 for the resource ID.
7. Select the service access role, and click **Assign**.
8. Confirm that you want to assign the public access policy to the resource, and click **Assign**.

Assigning access by using the CLI

To assign access for the Public Access group, run the **ibmcloud iam access-group-policy-create** command. In the command example, the policy details are specified in a JSON file. See [Assigning access by using the API](https://cloud.ibm.com/docs/account?topic=account-public#public-access-api) for an example of what to include in the JSON file.

ibmcloud iam access-group-policy Public Access -f @policy.json

For more information about the command options, see [ibmcloud iam access-group-policy-create](https://cloud.ibm.com/docs/cli?topic=cli-ibmcloud_commands_iam#ibmcloud_iam_access_group_policy_create).

Assigning access by using the API

The following request example creates a policy for the Public Access group.

curl -X POST 'https://iam.cloud.ibm.com/v1/policies' -H 'Authorization: $TOKEN' -H 'Content-Type: application/json' -d '{

"type": "access",

"subjects": [

{

"attributes": [

{

"name": "access\_group\_id",

"value": "AccessGroupId-PublicAccess"

}

]

}

],

"roles":[

{

"role\_id": "crn:v1:bluemix:public:iam::::role:Administrator"

}

],

"resources":[

{

"attributes": [

{

"name": "accountId",

"value": "$ACCOUNT\_ID"

},

{

"name": "serviceName",

"value": "$SERVICE\_NAME"

},

]

}

]

}'

For more information, see [Create a policy](https://cloud.ibm.com/apidocs/iam-policy-management#create-a-policy).

**Disabling public access to resources**

When you disable public access, all existing policies for the Public Access group are deleted, which revokes the previously allowed access. You also can't create or modify any policies for the Public Access group.

Disabling access in the console

To disable public access for the account, go to **Manage** > **Access (IAM)** > **Settings** in the console, and set the Public access setting to **Disable public access**.

Disabling access by using the API

The following request example disables public access for the account.

curl -X PATCH \

'https://iam.cloud.ibm.com/v2/groups/settings?account\_id=<account\_id>' \

-H 'Authorization: $TOKEN' \

-H 'Content-Type: application/json' \

-d '{

"public\_access\_enabled": false

}'

F