Creating and working with service IDs

A service ID identifies a service or application similar to how a user ID identifies a user. A service ID that you create can be used to enable an application outside of IBM Cloud access to your IBM Cloud services. You can assign specific access policies to the service ID that restrict permissions for using specific services, or even combine permissions for accessing different services. Since service IDs are not tied to a specific user, if a user happens to leave an organization and is deleted from the account, the service ID remains ensuring that your application or service stays up and running.

When you create a service ID, you create a unique name and description that is easy for you to identify and work with in the UI. After you create your service ID, you can [create API keys](https://cloud.ibm.com/docs/account?topic=account-serviceidapikeys#create_service_key) specific to each service ID that your application can use to authenticate with your IBM Cloud services. The API key can be set for one-time use or unlimited use. To ensure that your application has the appropriate access for authenticating with your IBM Cloud services, you use access policies that are assigned to each service ID that you create.

The access policies that are associated with a service ID enable specific actions that can be taken when that service ID is used to access a specific service. A single service ID can have multiple policies assigned that define the level of access that is allowed when accessing multiple Identity and access-enabled services, and even different instances of a single service. For example, you have two services with two service instances each. For example, you might assign the Viewer role for all available instances of one service and assign the Editor role for only one instance of a second service. This way you can customize access to multiple services, but use a single API key for authentication to all.

All users have access to create a service ID in an account to which they are a member. However, to allow a user in an account access to view or manage a service ID that they did not personally create, they are required to have access with a role on the IAM identity service account management service. For more information, see [IAM identity service](https://cloud.ibm.com/docs/account?topic=account-account-services#identity-service-account-management).

If the Restrict service ID creation IAM account setting is enabled, then everyone in the account, including account owners, is blocked from creating service IDs unless they are assigned explicit access. For more information, see [Restricting users from creating service IDs](https://cloud.ibm.com/docs/account?topic=account-restrict-service-id-create).

**Creating a service ID**

To create a service ID, complete the following steps:

1. In the IBM Cloud console, go to **Manage** > **Access (IAM)**, and select **Service IDs**.
2. Click **Create**.
3. Follow the process to create a name and description for your service ID.
4. Click **Create**.

Then, hover on the row of a service ID to use the **Actions**  menu to manage your service ID. You can start by assigning a policy and creating API keys. For more information about working with API keys, see [Managing service ID API keys](https://cloud.ibm.com/docs/account?topic=account-serviceidapikeys).

**Updating a service ID**

You can update a service ID by changing the name and description at any time. You can also delete and create new API keys as needed or update the assigned access policies. Hover on the row of a service ID to use the **Actions**  menu to manage your service ID.

Any changes that you make to an existing service ID, such as changing the assigned policies or deleting an API key that is used, might cause service interruptions to applications that use that service ID.

**Locking a service ID**

To avoid a situation where your service ID is deleted causing an outage or disruption for the users of your service, you have the option to lock your service ID by using the UI or CLI. Locking a service ID also prevents any policies from being changed, deleted, or assigned. In addition to the ability to lock a service ID, you can [lock individual API keys](https://cloud.ibm.com/docs/account?topic=account-serviceidapikeys#lockkey) that are associated with each service ID that you create in your account.

While locked service IDs cannot be deleted from the account and the access policies can't be updated, locked service IDs can still be removed from any access group that they are added to. This means that any access that is assigned to the ID by its membership in an access group is removed when the service ID is removed from the access group.

Providing user access for locking service IDs

In order for a user to have access to lock and unlock service IDs and API keys that are associated with service IDs, they must be assigned a specific access policy. Two types of access policies can grant the proper access: access to all service IDs in the account or access to a specific service ID in the account

To assign access to all service IDs in the account, set an access policy for account management services with the following details:

* Editor or Administrator role
* IAM Identity Service

To assign access to a specific service ID in the account, set an access policy for account management services with the following details:

* Editor or Administrator role
* IAM Identity Service
* Specify "serviceid" in the Resource type field
* Specify the service ID identifier in the Resource ID field

To get the identifier of a specific service ID, go to **Manage** > **Access (IAM)**, and select **Service IDs**. Select the service ID that you want to view details for, and copy the ID value.

Locking a service ID from the UI

A locked service ID is indicated by the  icon.

1. In the console, click **Manage** > **Access (IAM)** and then select **Service IDs**.
2. Identify the row of the service ID that you want to lock, and select **Lock service ID** from the **Actions**  menu.

To unlock a service ID, select the service ID from the table that you want to unlock and select **Unlock service ID** from the **Actions**  menu. You must have the appropriate level of access to unlock a service ID.

Locking and unlocking a service ID by using the CLI

To lock a service ID, use the following command:

ibmcloud iam service-id-lock (NAME|UUID) [-f, --force]

Command Options:

**NAME (required)**

Name of the service, exclusive with UUID

**UUID (required)**

UUID of the service, exclusive with NAME

**-f, --force**

Lock without confirmation

**Examples**:

Lock service ID sample-test without confirmation

ibmcloud iam service-id-lock sample-test -f

Lock service ID ServiceId-cb258cb9-8de3-4ac0-9aec-b2b2d27ac976

ibmcloud iam service-id-lock ServiceId-cb258cb9-8de3-4ac0-9aec-b2b2d27ac976

To unlock a service ID, use the following command:

ibmcloud iam service-id-unlock (NAME|UUID) [-f, --force]

Command Options:

**NAME (required)**

Name of the service, exclusive with UUID

**UUID (required)**

UUID of the service, exclusive with NAME

**-f, --force**

Unlock without confirmation

**Examples**:

Unlock service ID sample-test without confirmation

ibmcloud iam service-id-unlock sample-test -f

Unlock service ID ServiceId-cb258cb9-8de3-4ac0-9aec-b2b2d27ac976

ibmcloud iam service-id-unlock ServiceId-cb258cb9-8de3-4ac0-9aec-b2b2d27ac976

**Examples of how to use a service ID**

The following are examples of how a Service ID is used with the Object Storage and Cloud SQL Query services.

* Object Storage - [Use the IBM Cloud CLI](https://cloud.ibm.com/docs/cloud-object-storage?topic=cloud-object-storage-uhc-hmac-credentials-main).
* Cloud SQL Query - [How to use the SQL Query REST API](https://www.youtube.com/watch?v=jDZKF0CnUvU).