This page shows you how to create, disable and delete Hash-based Message Authentication Code (HMAC) keys associated with service accounts in your project. For general information, see HMAC keys (/storage/docs/authentication/hmackeys).

Before using this feature in Cloud Storage, you should:

1. Have sufficient permission to work with HMAC keys in the desired project:
    - If you own the project, you most likely have the necessary permissions.
    - You should have the IAM permissions that are prefixed with `storage.hmacKeys` for the project. See Using IAM Permissions (/storage/docs/access-control/using-iam-permissions) for instructions on how to get a role, such as `roles/storage.hmacKeyAdmin`, that has these permissions.
2. Have a service account in your project that you intend to create HMAC keys for. See Creating a service account (/iam/docs/creating-managing-service-accounts#creating_a_service_account) if you don't currently have one.

ant: When you create an HMAC key, you are given the *secret* for that key, which you must store securely. If you lose t you are no longer able to use the HMAC key to authorize requests.

To create an HMAC key for a service account:

To list the HMAC keys for a project, and get information about the keys:

To switch an HMAC key between being active and inactive:

n: HMAC keys cannot be recovered once you delete them. If you want to keep an HMAC key but prevent it from being
set its state (#update) to **`INACTIVE`**.

An HMAC key must be in an inactive state in order to delete it. To delete an inactive HMAC key:

- Follow the guidelines for migrating (/storage/docs/authentication/hmackeys#migration) from user account HMAC keys to service account HMAC keys.
- Use an HMAC key in an authenticated request (/storage/docs/migrating#authentication).