In order to access Google Cloud Platform (GCP), you will usually have to authorize Google Cloud SDK tools. This page will demonstrate available authorization options and show you how to manage the accounts you use for authorization. If you are using a Google Compute Engine instance or Google Cloud Shell, you are not required to authorize Cloud SDK tools.

To grant authorization to Cloud SDK tools to access GCP, you can use either a user account (/docs/authentication/#user_accounts) or a service account (/docs/authentication/#service_accounts).

A **user account** is a Google account that allows end users to authenticate directly to your application. For most common use cases, especially interactively using Cloud SDK tools from the command line, using a user account is best practice.

A **service account** is a Google account associated with your GCP project and not a specific user. A service account can be used by providing a service account key to your application. Alternatively, you can use the built-in service account available when using Google Cloud Functions, Google App Engine, Google Compute Engine, or Google Kubernetes Engine. A service account is recommended to script Cloud SDK tools for use on multiple machines.

You must authorize the gcloud CLI and other tools in Cloud SDK before you can use them to manage platform resources. Cloud SDK and Cloud Platform use OAuth2 for authentication and authorization.

Choose one of the following authorization types:

Type	Description
User account	Recommended if you are using Cloud SDK tools from the command line or you are scripting Cloud SDK tools for use on a single machine.

Type	Description
Service account	Recommended if you are installing and setting up Cloud SDK as part of a machine deployment process in production, or for use on Google Compute Engine virtual machine instances where all users have access to `root`.

Read the Cloud Platform Auth Guide (/docs/authentication) to learn more about authorization and the Cloud Platform.

You can use the following gcloud CLI commands to authorize access with a user account:

Command	Description
`gcloud init` (/sdk/gcloud/reference/init)	Authorizes access and performs other common Cloud SDK setup steps.
`gcloud auth login` (/sdk/gcloud/reference/auth/login)	Authorizes access only.

During authorization, these commands obtain account credentials from the Cloud Platform and store them on the local system. The specified account then becomes the active account in your Cloud SDK configuration (/sdk/docs/configurations). The gcloud CLI and other Cloud SDK tools use the stored credentials to access the Cloud Platform. You can have any number of accounts with stored credentials for a single Cloud SDK installation, but only one account is active at any time.

`gcloud init` authorizes access and performs other common Cloud SDK setup steps (/sdk/docs/initializing). It uses a web-based authorization flow to authenticate the user account and grant access permissions.

To authorize access and perform other common Cloud SDK setup steps:

1. Run `gcloud init`:

Or, to prevent the command from automatically opening a web browser:

Using the `--console-only` flag is useful if you are running the command on a remote system using `ssh` and do not have access to a browser on that system. You must then manually open the provided URL in a browser on your local system to complete the authorization process.

2. Follow the browser-based authorization flow to authenticate the account and grant access permissions.

Read Initializing Cloud SDK (/sdk/docs/initializing) to learn more about this command and Cloud SDK initialization.

`gcloud auth login` authorizes the user account only.

To authorize access without performing other setup steps:

1. Run `gcloud auth login`:

   Or:

   You can use the `--no-launch-browser` flag to prevent the command from automatically opening a web browser. You must then manually open the provided URL in a browser on your local system to complete the authorization process.

2. Follow the browser-based authorization flow to authenticate the account and grant access permissions.

`gcloud auth activate-service-account` (/sdk/gcloud/reference/auth/activate-service-account) authorizes access using a service account. As with `gcloud init` and `gcloud auth login`, this command saves the service account credentials to the local system on successful completion and sets the specified account as the active account in your Cloud SDK configuration.

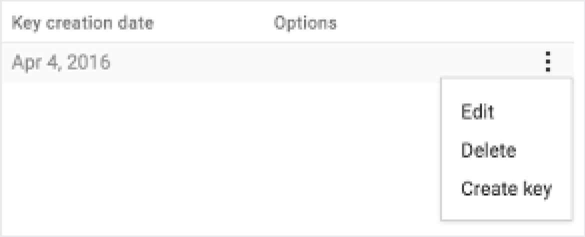
To authorize using a service account:

1. Go to the Service Accounts page in the Google Cloud Console.

   Go to the Service Accounts page (https://console.cloud.google.com/iam-admin/serviceaccounts)

2. Click **Create service account** or choose an existing account.

3. Click the **More** button
   ⋮
   in the **Options** column of the service accounts table and then select **Create key** to create and download a JSON-formatted key file.

Key creation date	Options
Apr 4, 2016	⋮

4. If required, move the key file to a location on the same system where you are authorizing Cloud SDK tools.

   Alternatively, instead of Steps 1-4, you could procure a key for an an existing service account via `gcloud iam service-accounts keys create`.

5. Run `gcloud auth activate-service-account`:

6. Delete the key file from the system. Note that the gcloud CLI stores keys and the gcloud CLI copy of the key will still remain.

To list the accounts whose credentials are stored on the local system, run **`gcloud auth list`** (/sdk/gcloud/reference/auth/list):

The gcloud CLI lists the accounts and shows which account is currently active:

To switch the active account, run **`gcloud config set`** (/sdk/gcloud/reference/config/set):

where [ACCOUNT] is the full e-mail address of the account.

You can also switch accounts by creating a separate configuration that specifies the different account and switching between configurations:

If you want to switch the account used by the gcloud CLI on a per-invocation basis, override the active account using the `--account` (/sdk/gcloud/reference/) flag.

You can revoke credentials when you want to disallow access by the gcloud CLI and other Cloud SDK tools by a particular account. You don't need to revoke credentials to switch between accounts.

To revoke credentials, run: `gcloud auth revoke` (/sdk/gcloud/reference/auth/revoke):

To revoke all access for Cloud SDK for **all** machines, remove Cloud SDK from the list of apps that have access to your account (https://security.google.com/settings/security/permissions).

To find the location of your credential files, run `gcloud info` (/sdk/gcloud/reference/info):

The gcloud CLI prints information about your Cloud SDK installation. Credential files are stored in the user configuration directory:

- Read Google Cloud Platform Auth Guide (/docs/authentication) to learn more about authorization and the Cloud Platform.
- Read Cloud SDK Configurations (/sdk/docs/configurations) to learn more about configurations.
- Read Cloud SDK Properties (/sdk/docs/properties) to learn more about properties.