Before you can access or interact with hosted repositories from your system, you must set up local authentication in your environment.

After you set up local authentication, you can access hosted repositories for which you have the appropriate roles and permissions (/source-repositories/docs/configure-access-control). You can also perform standard Git operations such as `git clone`, `git pull`, and `git push`. Local authentication isn't required to perform operations in the Google Cloud Console, for example, to browse the contents of a repository.

Cloud Source Repositories supports the following types of authentication:

- SSH (#ssh)
- Cloud SDK (#authenticate-using-the-cloud-sdk)
- Manually generated credentials (#manually-generated-credentials)

Cloud Source Repositories lets you use SSH public key authentication to access hosted repositories. In this scenario, you first generate a key pair on the local system from which you want to access the repository. Then you register the public key with Google Cloud. If you already have an SSH key pair on your system, you can re-use those keys for authentication. You can register up to 20 public keys per Google Account.

You cannot configure authentication for service accounts by using SSH keys.

Cloud Source Repositories supports three SSH key types:

- RSA (only for keys with more than 2048 bits)
- ECDSA
- ED25519

The SSH key pair consists of a private key that resides on your local system and a public key that you register with Google Cloud.

You can also use an existing key pair for SSH authentication.

1. In the GCP Console, open the **Manage SSH Keys** page.

   Open Cloud Source Repositories (https://source.cloud.google.com/user/ssh_keys)

2. Click **Register SSH key**.

   The **Register SSH Key** dialog opens.

3. In the **Key name** field, type a unique name for the key.

4. In the **Key** field, copy the key string from your public key file.

5. Click **Register**.

After you set up SSH authentication, you can clone any repository (/source-repositories/docs/cloning-repositories#ssh) for which you have the required roles and permissions, or push the contents (/source-repositories/docs/pushing-code-from-a-repository) of a local repository to an empty hosted repository.

Cloud Source Repositories lets you authenticate by using the Cloud SDK. In this scenario, you run the `gcloud init` (/sdk/gcloud/reference/init) command on your system to set up local authentication.

1. Ensure that the Cloud SDK (/sdk/install) is installed on your local system.

2. At a command prompt, run `gcloud init`:

3. Follow the instructions.

After you set up authentication by using the Cloud SDK, you can use standard Git commands to interact with the hosted repository on Cloud Source Repositories.

You can also use manually generated credentials for authentication. Cloud Source Repositories provides a set of scripts you can use to manually generate the credentials you need to access hosted repositories.

1. Go to the **Configure Git** page to generate your credentials.

Go to the Configure Git page (https://source.developers.google.com/auth/start?scopes=https://www.googleapis.com/auth/cloud-platform)

2. Open a terminal window.
3. Type the following command:

   Where:

   - ***PROJECT_ID*** is the name of your project
   - ***REPOSITORY_NAME*** is the name of your repository

After you set up authentication with manually generated credentials, you can interact with the hosted repository on Cloud Source Repositories by using the standard Git commands.