Access control in Google Cloud is controlled using Cloud Identity and Access Management (/iam) (Cloud IAM). Cloud IAM allows you to set permissions specifying **who** has **what** kind of access to **which** resources in your project.

Cloud Source Repositories uses Cloud IAM for access control. You can use Cloud IAM to add team members to your project and to grant them permissions to create, view, and update repositories.

This page describes the Cloud IAM permissions and roles that apply to Cloud Source Repositories.

With Cloud IAM, every action on a repository in Cloud Source Repositories requires that the account initiating the action has the appropriate permissions. You don't grant specific permissions to an account. Instead, you grant a role that contains the appropriate set of permissions.

The following table describes the permissions available in Cloud Source Repositories.

Permission	Description
`source.repos.list`	List repositories within a project.
`source.repos.create`	Create a repository within a project.
`source.repos.get`	Clone, fetch, and browse repositories.
`source.repos.update`	Push changes to a repository.
`source.repos.updateRepoConfig`	Change a repository configuration.
`source.repos.delete`	Delete a repository.
`source.repos.getIamPolicy`	Read/view the Cloud IAM policy of a repository.
`source.repos.setIamPolicy`	Change the Cloud IAM policy of a repository.
`source.repos.getProjectConfig`	Read/view the Cloud project configuration.
`source.repos.updateProjectConfig`	Change the Cloud project configuration.

You assign permissions to accounts through the use of roles. The following table lists the roles available for Cloud Source Repositories.

Role	Role Title
`roles/source.reader`	Source Repository Reader
`roles/source.writer`	Source Repository Writer
`roles/source.admin`	Source Repository Administrator

Use the table below to select the appropriate role for an account based on the types of actions you want that account to perform.

Capability	reader (#source.reader)	writer (#source.writer)	admin (#bigq)
List repositories	✓	✓	✓
Clone, fetch, and browse repositories	✓	✓	✓
Update repositories	🚫	✓	✓
Create repositories	🚫	🚫	✓
Update repository configurations	🚫	🚫	✓
Delete repositories	🚫	🚫	✓
View Cloud IAM policies	🚫	🚫	✓
Set Cloud IAM policies	🚫	🚫	✓
View Cloud project configurations	🚫	🚫	✓
Update Cloud project configurations	🚫	🚫	✓

In addition to the predefined roles, Cloud Source Repositories also supports custom roles. For more information, see Creating and managing custom roles (/iam/docs/creating-custom-roles) in the Cloud

IAM documentation.

The `source.repos.update` permission cannot be granted to a custom role.

In Cloud IAM, you grant access to **members**. There are multiple types of members. For a complete list, see Concepts related to identity (/iam/docs/overview#concepts_related_identity).

For specific steps on granting member access, see Granting, changing, and revoking access to resources (/iam/docs/granting-changing-revoking-access).

You can't make a Google Cloud repository public. As a result, Cloud Source Repositories doesn't support the following member types:

- allAuthenticatedUsers
- allUsers