Stackdriver Profiler controls access to profiling activities in Google Cloud Platform projects by using Cloud Identity and Access Management (/iam/docs/overview) (Cloud IAM) roles and permissions.

To use Stackdriver Profiler, you must have the appropriate Cloud IAM permissions granted on the GCP project for the feature in question.

Permissions are not granted directly to users; permissions are instead granted indirectly through roles, which group multiple permissions to make managing them easier. For more information on these concepts, see the Cloud IAM documentation on roles, permissions, and related concepts (/iam/docs/overview#concepts_related_to_access_management).

Features of Stackdriver Profiler require permission to the underlying API methods used to perform the tasks of those feature. This section summarizes the permissions and roles that apply to Profiler.

The following table lists the permissions required for profiling activities:

Activity	Required permissions
Create new profiles	`cloudprofiler.profiles.create`
List profiles	`cloudprofiler.profiles.list`
Modify profiles	`cloudprofiler.profiles.update`

IAM roles include permissions and can be assigned to users, groups, and service accounts. The following roles include the listed permissions for Profiler:

Role ID Role name	Includes permissions	Description
`roles/cloudprofiler.agent` Stackdriver Profiler Agent	`cloudprofiler.profiles.create` `cloudprofiler.profiles.update`	Ability to register and provide profiling data

`roles/cloudprofiler.user`
Stackdriver Profiler User
	`cloudprofiler.profiles.list`
	`resourcemanager.projects.get`
	`resourcemanager.projects.list`
	`servicemanagement.projectSettings.get`
		Ability to view and query profiling data

To learn how to assign IAM roles to a user or service account, see Managing Policies (/iam/docs/managing-policies).