[Access Context Manager](https://cloud.google.com/access-context-manager/docs/) (https://cloud.google.com/access-context-manager/docs/)

[Documentation](https://cloud.google.com/access-context-manager/docs/) (https://cloud.google.com/access-context-manager/docs/) [Guides](#)

Creating an access policy

This page describes how to create an access policy for your organization.

> **Note:** Organizations can only have one access policy. If you attempt to create an access policy while one already exists for your organization, you will receive an error.

Before you begin

- Ensure you have the [correct permissions](https://cloud.google.com/access-context-manager/docs/access-control) (https://cloud.google.com/access-context-manager/docs/access-control) to use Access Context Manager.

Create an access policy

CONSOLE	GCLOUD	API

When you [create an access level](https://cloud.google.com/access-context-manager/docs/create-access-level) (https://cloud.google.com/access-context-manager/docs/create-access-level) or VPC Service Controls [service perimeter](https://cloud.google.com/vpc-service-controls/docs/create-service-perimeters) (https://cloud.google.com/vpc-service-controls/docs/create-service-perimeters), a default access policy is created automatically. No additional manual steps are required.

(https://www.apache.org/licenses/LICENSE-2.0). *For details, see our Site Policies*
(https://developers.google.com/terms/site-policies). *Java is a registered trademark of Oracle and/or its affiliates.*

Last updated March 19, 2019.