



GCP

- [GCP Overview, on page 1](#)
- [Connect a GCP Project to the Multicloud Defense Controller from the Multicloud Defense Dashboard, on page 3](#)

GCP Overview

GCP Project and GCP Folders

Multicloud Defense currently supports both GCP projects and GCP folders although these components are supported separately. Note the following limitations and exceptions for both of these options.

A GCP project has the potential to contain GCP resources like virtual machines, storage buckets, databases, and more. It can be used to create, enable, and use all Google Cloud services.

- Projects can be onboarded with Terraform, manual onboarding, and scripted onboarding.
- Projects are ideal for environments requiring orchestration, including discovery and investigation.
- You can interact with each project individually through the Multicloud Defense dashboard.

As of Version 23.10, you can connect a GCP folder with Terraform. A GCP folder contains projects, other folders, or a combination of both. Organization resources can use folders to group projects under the organization resource node in a hierarchy.

- Consider folders without the `roles/compute.admin` permission enabled as empty, and do not use them.
- Projects associated with onboarded folders are used for asset and traffic discovery only.
- Projects associated with onboarded folders do not accommodate orchestrating service VPC or gateway creation.
- Permissions made to folders from the GCP console must be made at the folder level. Therefore, perform, Multicloud Defense actions at the folder level.
- When creating a new gateway, do not use 172.16.0.0/16 subnet.

If you want to onboard a GCP folder, see refer to the [Terraform repository](#).

Overview Procedure

The following is an overview of how to connect your GCP project. An shell **script** is provided by Multicloud Defense and facilitates an easy connective process as part of a wizard. The script automates the following steps so you don't have to:

1. Create two service accounts.
2. Enable the following APIs (Compute Engine, Secret Manager).
3. Create the two following VPCs (management, datapath).
4. Create firewall rules to allow traffic to the Multicloud Defense Gateway (app traffic) in the datapath VPC.
5. Create firewall rules to allow management traffic from Multicloud Defense Gateway to the Multicloud Defense Controller in the management VPC.

If you find that the script does not work, or if you need to manually change your settings, these actions can be executed using the GCP cloud console web UI, or using the gcloud CLI. See the alternative method of connecting your project [here](#).

Overview of Creating a GCP Controller Service Account

The Multicloud Defense Controller uses the controller service account to access and manage resources in your GCP project. You must create the account and generate a key. The key is added to the controller as part of Account onboarding to the controller.

Procedure

-
- Step 1** In your GCP dashboard, open IAM in your GCP project.
 - Step 2** Click **Service Accounts**.
 - Step 3** Create **Service Account**.
 - Step 4** Provide a name and ID, such as `multicloud-firewall`, and click **Create**.
 - Step 5** Add **Compute Admin** and **Service Account User** roles.
 - Step 6** Click **Continue**.
 - Step 7** Click **Done**.
 - Step 8** Click on the newly created account, scroll down to Keys and in the dropdown for Add Key and select **Create New Key**.
 - Step 9** Choose JSON (default option) and click **Create**.
 - Step 10** A file is downloaded to your computer. Save this file to your local drive.
-

Create a GCP Firewall Service Account

The firewall service account is used by the Multicloud Defense Gateway instances running inside your GCP project. The gateways may need to access the private keys stored in the SecretManager for TLS decryption and access storage to store PCAP files etc. (if configured by the user). Also, the gateways many need log

writer permissions to send logs from Multicloud Defense Gateway to the GCP logging instance (if configured by the user).

Follow these steps to create a controller service account:

Procedure

- Step 1** In your GCP dashboard, open IAM in your GCP project.
 - Step 2** Click **Service Accounts**.
 - Step 3** Create **Service Account**.
 - Step 4** Provide a name and ID, such as `multicloud-firewall`, and click **Create**.
 - Step 5** Add **Secret Manager Secret Accessor** and **Logs Writer** roles.
 - Step 6** Click **Continue**.
 - Step 7** Click **Done**.
-

Connect a GCP Project to the Multicloud Defense Controller from the Multicloud Defense Dashboard

Once you prepared the GCP project as described in the previous sections, you can link it to the Multicloud Defense Controller.

Before you begin

You must already have a Google Cloud Platform (GCP) project created and have permissions to create VPCs, subnets, and a service account.

Procedure

- Step 1** In the left pane of Security Cloud Control, click Multicloud Defense.
- Step 2** Click the Multicloud Defense Controller button.
- Step 3** In the **Cloud Accounts** pane, click **Add Account**.
- Step 4** On the **General Information** page, select **GCP** from the Account Type list box.
- Step 5** Login to the Multicloud Defense Dashboard.
- Step 6** Click **Manage** and then **Accounts**.
- Step 7** Click **Add Account**.
- Step 8** In step 1, click the link to open an Google Cloud Platform Cloud Shell.
- Step 9** In step 2, click the **Copy** button.
- Step 10** Run the bash script in the Google Cloud Platform Cloud Shell.
- Step 11** Type a name for this GCP account. You can choose to name this the same as your GCP project name. This name is visible on the Multicloud Defense Controller only.

- Step 12** (Optional) Enter a description.
- Step 13** Enter the **Project ID** for the GCP project.
- Step 14** Enter the **Client Email** for the service account created for Multicloud Defense Controller.
- Step 15** Enter the **Private key** of the service account.
- Step 16** Click **Save & Continue**.
-

What to do next

Enable traffic visibility.

Roles Created by Multicloud Defense

When you onboard a cloud service account to Multicloud Defense Controller with the provided script, user roles are created within the parameters of the cloud service provider to ensure that communication between the services are protected. Depending on the cloud service provider, different roles and permissions are created.

The following roles are created when you onboard an account.

GCP IAM Roles

This document explains the details of the service accounts created by the CloudFormation template used in the previous section.

The CloudFormation template creates the following accounts:

- **ciscomcd-controller service account** - This account is used by the Multicloud Defense Controller to access your GCP project to create resources (Multicloud Defense Gateway), load balancers for gateways, and read information about the VPCs, subnets, security group tags, and more. See [Overview of Creating a GCP Controller Service Account, on page 2](#) for more information.
- **ciscomcd-firewall service account** - This account is assigned to the Multicloud Defense Gateway (compute VM instances). The account provides access to the secret manager (private keys for TLS decryption) and storage. Also, the gateways may need permissions to send logs from Multicloud Defense Gateway to the GCP logging instance (if configured by the user). See [Create a GCP Firewall Service Account, on page 2](#) for more information.