

This page describes how to grant your Compute Engine [virtual machine instance \(/compute/docs/instances/\)](#) permission to access a Cloud Spanner database.

Your instance can access the Cloud Spanner API from Compute Engine by using a service account to act on your behalf. The service account provides [application default credentials](https://developers.google.com/identity/protocols/application-default-credentials) (<https://developers.google.com/identity/protocols/application-default-credentials>) for your applications so that you do not need to configure each Compute Engine instance to use your personal user credentials.

Configure the service account on your instance with one of the following options:

- For easy development and testing, configure your instance to [use the default service account with full access to all Cloud APIs \(#default-full-access\)](#).
- For production environments, [create a service account with read and write access to your Cloud Spanner databases \(#service-account\)](#) and apply it to your instance.

To quickly allow your instance to access the Cloud Spanner API, create a new instance to use the default service account and a scope with full access to all Cloud APIs.

1. Go to the Compute Engine VM instances page.

[Go to the VM instances page](https://console.cloud.google.com/compute/instances) (<https://console.cloud.google.com/compute/instances>)

2. Select your project and click **Continue**.
3. Click **Create Instance** to start creating a new instance.
4. In the **Identity and API access** section, click **Allow full access to all Cloud APIs**.
5. Configure other instance settings as needed, then click **Create**.

Now that the service account on your Compute Engine instance has access to the Cloud Spanner API, [use a client library \(/spanner/docs/tutorials\)](#) to read and write data in your Cloud

Spanner database. The instance uses the credentials from the default service account to authenticate with the Cloud Spanner API.

To restrict instance access to specific APIs and roles, create a service account with permission only to access your Cloud Spanner databases. Then, apply the service account to your instance.

1. Select a service account that will act on your behalf to access Cloud Spanner. Use one of the following options:

- [Create a new service account](#)  
(/iam/docs/creating-managing-service-accounts#creating\_a\_service\_account).
- [Identify an existing service account](#)  
(/iam/docs/creating-managing-service-accounts#listing\_service\_accounts) that you can use for your instance.

2. [Grant a role to the service account](#)

(/iam/docs/granting-roles-to-service-accounts#granting\_access\_to\_a\_service\_account\_for\_a\_resource)

so that it has the necessary permissions to access Cloud Spanner. For a list of roles that apply to Cloud Spanner, see [Access Control for Cloud Spanner](#) (/spanner/docs/iam#roles).

3. Go to the Compute Engine VM instances page.

[Go to the VM instances page](https://console.cloud.google.com/compute/instances) (https://console.cloud.google.com/compute/instances)

4. Select your project and click **Continue**.

5. Click **Create Instance** to start creating a new instance.

6. In the **Identity and API access** section, select the service account from the list under **Service account**.

7. Configure other instance settings as needed, then click **Create**.

Now that the service account on your Compute Engine instance has access to the Cloud Spanner API, [use a client library](#) (/spanner/docs/tutorials) to read and write data in your Cloud

Spanner database. The instance uses the service account credentials to authenticate with the Cloud Spanner API.

- [Connect to your instance](/compute/docs/instances/connecting-to-instance) (/compute/docs/instances/connecting-to-instance) and follow a [client library tutorial](/spanner/docs/tutorials) (/spanner/docs/tutorials) to learn how to read and write data to Cloud Spanner from your instance.
- Learn more about [service accounts on Compute Engine](/compute/docs/access/service-accounts) (/compute/docs/access/service-accounts) and how you can use them to grant IAM roles and API access scopes to the applications that run on your instances.
- Learn how to [change service accounts on existing instances](/compute/docs/access/create-enable-service-accounts-for-instances#changeserviceaccountandscopes) (/compute/docs/access/create-enable-service-accounts-for-instances#changeserviceaccountandscopes)
- Learn more about [creating and starting an Compute Engine instances](/compute/docs/instances/create-start-instance) (/compute/docs/instances/create-start-instance).