MySQL (/sql/docs/mysql/connect-admin-proxy) | **PostgreSQL** | SQL Server (/sql/docs/sqlserver/connect-admin-proxy)

This page describes how to connect a psql client (https://www.postgresql.org/docs/9.6/static/app-psql.html) to your Cloud SQL instance using the Cloud SQL Proxy, rather than over IP.

For information about connecting a psql client to a Cloud SQL instance using IP, see Connecting psql Client Using IP Addresses (/sql/docs/postgres/connect-admin-ip).

For more information about how the proxy works, see About the Cloud SQL Proxy (/sql/docs/postgres/sql-proxy).

Before you can connect a psql to a Cloud SQL instance, you must have:

- Created a Cloud SQL instance, including configuring the default user.
  For more information about creating instances, see Creating Instances (/sql/docs/postgres/create-instance).

  For more information about configuring the default user, see Configuring the default user account (/sql/docs/postgres/create-manage-users#user-root).
- Determined how you will connect to your instance.
  For information about the available connection options and how to choose between them, see Connection Options for External Applications (/sql/docs/postgres/external-connection-methods).

Connecting a psql to your Cloud SQL instance with the proxy involves the following steps:

1. Enable the Cloud SQL API (#enable-api)
2. Install the proxy (#install)
3. Create a service account (#service-account)
4. Start the proxy (#start-proxy)
5. Start the psql session (#start-mysql)

Enable the Cloud SQL Admin API.

Enable the API (https://console.cloud.google.com/flows/enableapi?apiid=sqladmin&redirect=https://console.cloud.google.com)

If your operating system isn't included here, you can also compile the proxy from source (http://github.com/GoogleCloudPlatform/cloudsql-proxy).

When you connect using the proxy, the proxy needs to authenticate with Google Cloud Platform. You can either use your Cloud SDK credentials, or you can provide the proxy with a path to a local key file from a service account you create (recommended for production instances). If you are using your Cloud SDK credentials, you can skip this step.

For more information about service accounts, see the Google Cloud Platform Auth Guide (/docs/authentication#service_accounts).

To create a service account with the required permissions, you must have **`resourcemanager.projects.setIamPolicy`** permiss
ermission is included in the Project Owner, Project IAM Admin, and Organization Administrator roles.
ust also have enabled the Cloud SQL Admin API.

When you use a service account to provide the credentials for the proxy, you must create it with sufficient permissions. If you are using the finer-grained Identity Access and Management (IAM) roles to manage your Cloud SQL permissions, you must give the service account a role that includes the cloudsql.instances.connect permission. The predefined Cloud SQL roles that include this permission are:

- Cloud SQL Client
- Cloud SQL Editor
- Cloud SQL Admin

If you are using the legacy project roles (Viewer, Editor, Owner), the service account must have at least the Editor role.

1. Go to the **Service accounts** page of the Google Cloud Console.

   Go to the Service accounts page (https://console.cloud.google.com/iam-admin/serviceaccounts/)

2. Select the project that contains your Cloud SQL instance.
3. Click **Create service account**.
4. In the **Create service account** dialog, provide a descriptive name for the service account.
5. For **Role**, select one of the following roles:

   - **Cloud SQL > Cloud SQL Client**
   - **Cloud SQL > Cloud SQL Editor**
   - **Cloud SQL > Cloud SQL Admin**

   Alternatively, you can use the primitive Editor role by selecting **Project > Editor**, but the Editor role includes permissions across Google Cloud.

   If you do not see these roles, your Google Cloud user might not have the `resourcemanager.projects.setIamPolicy` permission. You can check your permissions by going to the IAM page (https://console.cloud.google.com/iam-admin) in the Google Cloud Console and searching for your user id.

6. Change the **Service account ID** to a unique, easily recognizable value.
7. Click **Furnish a new private key** and confirm that the key type is `JSON`.
8. Click **Create**.

   The private key file is downloaded to your machine. You can move it to another location. Keep the key file secure.

Depending on your language and environment, you can start the proxy using either TCP sockets or Unix sockets.

Now that you have installed and started the proxy, you can start a psql session using the proxy. This command can be used whenever you want to connect to your Cloud SQL instance with a psql client.

The connection string you use depends on whether you started the proxy using a TCP socket or a UNIX socket.

Need help? For help troubleshooting the proxy, see Troubleshooting Cloud SQL Proxy connections (/sql/docs/postgres/sql-proxy#troubleshooting). Or, see our Cloud SQL Support page (/sql/docs/postgres/support).

- Learn more about the proxy (/sql/docs/postgres/sql-proxy).
- Get help troubleshooting connection issues (/sql/docs/postgres/sql-proxy#troubleshooting) for the Cloud SQL Proxy.
- Learn about the two levels of access control (/sql/docs/postgres/instance-access-control) for Cloud SQL instances.
- Create users (/sql/docs/postgres/create-manage-users) and databases (/sql/docs/postgres/create-manage-databases).
- Learn about connecting to your instance from your application (/sql/docs/postgres/instance-access-control).
- Learn about the psql Client (https://www.postgresql.org/docs/9.6/static/app-psql.html).
- Learn about options for support (/sql/docs/support).