MySQL (/sql/docs/mysql/instance-access-control) | **PostgreSQL** | SQL Server (/sql/docs/sqlserver/instance-access-control)

This page discusses the two levels of access control for Cloud SQL instances. You must configure both levels of access control before you can manage your instance.

Configuring access control for an instance is about controlling who or what can access the instance. Access control occurs on two levels:

Instance-level access

Instance-level access authorizes access to your Cloud SQL instance from an application or client (running on App Engine or externally) or another Google Cloud service, such as Compute Engine.

Database access

Database access uses PostgreSQL roles (https://www.postgresql.org/docs/9.6/static/user-manag.html) to control which PostgreSQL users have access to the data in your instance.

For information about controlling who can *manage* your instance, see Project Access Control docs/project-access-control).

How you configure instance-level access depends on where you are connecting from:

Connection source	Access configuration options	More information
Compute Engine	• Cloud SQL Proxy • Authorize static IP address	• Connecting from Compute Engine (/sql/docs/postgres/connect-compute-engine)
GKE	• Cloud SQL Proxy Docker image	• Connecting from GKE (/sql/docs/postgres/connect-kubernetes-engine)

App Engine standard environment	• Same project: configure IAM • Between projects: configure IAM	• Connecting from App Engine (/sql/docs/postgres/connect-app-engine)
App Engine flexible environment	• Same project: preconfigured • Between projects: configure IAM	• Connecting from App Engine (/sql/docs/postgres/connect-app-engine)
`psql` client	• Cloud SQL Proxy • Authorize client IP address	• Connecting the psql Client Using the Proxy (/sql/docs/postgres/connect-admin-proxy) • Connecting the psql Client Using IP Addresses (/sql/docs/postgres/connect-admin-ip)
External applications	• Cloud SQL Proxy • Authorize client IP address	• Connecting to Cloud SQL from External Applications (/sql/docs/postgres/connect-external-app)
Cloud Functions	• A Cloud SQL instance set up with a public IP. • Between projects: also configure IAM	• Connecting Using Cloud Functions (/sql/docs/postgres/connect-functions)
Cloud Run	• A Cloud SQL instance set up with a public IP. • Between projects: also configure IAM	• Connecting Using Cloud Run (/sql/docs/postgres/connect-run)
Google Kubernetes Engine	• Private IP or Cloud SQL Proxy • If Public IP, Cloud SQL Proxy is required	• Connecting Using Google Kubernetes Engine (/sql/docs/postgres/connect-kubernetes-engine)

After a connection to an instance has been negotiated, the user or application must log in to the database instance with a user account. You create and manage user accounts as part of managing your Cloud SQL instance.

For more information, see PostgreSQL Users (/sql/docs/postgres/users) and Creating and Managing PostgreSQL Users (/sql/docs/postgres/create-manage-users).

If you are authorizing access via IP addresses, you should use SSL and set a strong password for the default user ar you create.

- Learn more about how Cloud SQL works with PostgreSQL users (/sql/docs/postgres/users).
- Learn more about PostgreSQL roles (https://www.postgresql.org/docs/9.6/static/user-manag.html).
- Learn more about your options for connecting from an external application (/sql/docs/postgres/external-connection-methods).
- Learn about controlling who can manage your Google Cloud Platform project (/sql/docs/project-access-control).