Instance access control

MySQL | PostgreSQL (https://cloud.google.com/sql/docs/postgres/instance-access-control) | SQL Server (https://cloud.google.com/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.

Levels of access control

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 the MySQL Access Privilege System (https://dev.mysql.com/doc/refman/5.7/en/access-control.html) to control which MySQL users have access to the data in your instance.

Note: For information about controlling who can *manage* your instance, see Project Access Control (https://cloud.google.com/sql/docs/project-access-control).

Instance-level access

How you configure instance-level access depends on where you are connecting from, and whether you are connecting to a First Generation or Second Generation instance:

Note: Second Generation is replacing First Generation; support for First Generation instances ends January 30, 2020. To upgrade a First Generation instance to Second Generation, see Upgrading a First Generation Instance to Second Generation (https://cloud.google.com/sql/docs/mysql/upgrade-2nd-gen).

Connection source	First Generation instance	Second Generation instance	More information
Compute Engine	Authorize static IP address	• Cloud SQL Proxy • Authorize static IP address	• Connecting from Compute Engine (https://cloud.google.com/sql/docs/mysql/connect-compute-engine)
App Engine standard environment	Authorize Application ID	• Same project: preconfigured • Between projects: configure IAM	• Connecting from App Engine (https://cloud.google.com/sql/docs/mysql/connect-app-engine)
App Engine flexible environment	Not supported	• Same project: preconfigured • Between projects: configure IAM	• Connecting from App Engine (https://cloud.google.com/sql/docs/mysql/connect-app-engine)
`mysql` client	Authorize client IP address	• Cloud SQL Proxy • Authorize client IP address	• Connecting the mysql Client Using the Proxy (https://cloud.google.com/sql/docs/mysql/connect-admin-proxy) • Connecting the mysql Client Using IP Addresses (https://cloud.google.com/sql/docs/mysql/connect-admin-ip)
External applications	Authorize client IP address	• Cloud SQL Proxy • Authorize client IP address	• Connecting to Cloud SQL from External Applications (https://cloud.google.com/sql/docs/mysql/connect-external-app)
Cloud Functions	• A Cloud SQL instance set up with a public IP. • Between projects: also	• A Cloud SQL instance set up with a public IP. • Between projects: also configure IAM	• Connecting Using Cloud Functions (https://cloud.google.com/sql/docs/mysql/connect-functions)

	configure IAM		
Cloud Run	• A Cloud SQL instance set up with a public IP. • Between projects: also configure IAM	• A Cloud SQL instance set up with a public IP. • Between projects: also configure IAM	• Connecting Using Cloud Run (https://cloud.google.com/sql/docs/mysql/connect-run)
Google Kubernetes Engine	• Private IP or Cloud SQL Proxy • If Public IP, Cloud SQL Proxy is required	• Private IP or Cloud SQL Proxy • If Public IP, Cloud SQL Proxy is required	• Connecting Using Google Kubernetes Engine (https://cloud.google.com/sql/docs/mysql/connect-kubernetes-engine)

Database access

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.

You must set up the default user (root) when you create an instance, but you can also create more users to give you finer-grained control over access to your Cloud SQL instance. For more information, see MySQL Users (https://cloud.google.com/sql/docs/mysql/users) and Configuring the default user account (https://cloud.google.com/sql/docs/mysql/create-manage-users/#user-root).

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

What's next

- Learn more about how Cloud SQL works with MySQL users (https://cloud.google.com/sql/docs/mysql/users).

- Learn more about the MySQL Access Privilege System (https://dev.mysql.com/doc/refman/5.7/en/privilege-system.html).
- Learn more about your options for connecting from an external application (https://cloud.google.com/sql/docs/mysql/external-connection-methods).
- Learn about controlling who can manage your Google Cloud Platform project (https://cloud.google.com/sql/docs/project-access-control).
