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

This page describes how you can control Cloud SQL project access and permissions using Identity and Access Management (IAM).

Project access control is different than the access control provided by the database engine. For information about base access control, see PostgreSQL Users (/sql/docs/postgres/users).

Google Cloud offers Identity and Access Management (IAM), which lets you give more granular access to specific Google Cloud resources and prevents unwanted access to other resources. This page describes the Cloud SQL IAM roles and permissions. For a detailed description of Google Cloud IAM, see the IAM documentation (/iam/docs/).

Cloud SQL provides a set of predefined roles (#roles) designed to help you easily control access to your Cloud SQL resources. You can also create your own custom roles (#custom-roles), if the predefined roles do not provide the sets of permissions you need. In addition, the legacy primitive roles (Editor, Viewer, and Owner) are also still available to you, although they do not provide the same fine-grained control as the Cloud SQL roles. In particular, the primitive roles provide access to resources across Google Cloud, rather than just for Cloud SQL. For more information about primitive roles, see Primitive roles (/iam/docs/understanding-roles#primitive_roles).

This section summarizes the permissions and roles Cloud SQL supports.

Cloud SQL provides some predefined roles you can use to provide finer-grained permissions to project members. The role you grant to a project member controls what actions the member can take. Project members can be individuals, groups, or service accounts.

You can grant multiple roles to the same project member, and you can change the roles granted to a project member at any time, provided you have the permissions to do so.

The broader roles include the more narrowly defined roles. For example, the Cloud SQL Editor role includes all of the permissions of the Cloud SQL Viewer role, along with the addition permissions of the Cloud SQL Editor role. Likewise, the Cloud SQL Admin role includes all of the permissions of the Cloud SQL Editor role, along with its additional permissions.

The primitive roles (Owner, Editor, Viewer) provide permissions across Google Cloud. The roles specific to Cloud SQL provide only Cloud SQL permissions, except for the following Google Cloud permissions, which are needed for general Google Cloud usage:

- `resourcemanager.projects.get`
- `resourcemanager.projects.list`
- `serviceusage.quotas.get`
- `serviceusage.services.get`

The following table lists the predefined roles available for Cloud SQL, along with their Cloud SQL permissions:

Role	Name	Cloud SQL permissions	Description
`roles/owner`	Owner	`cloudsql.*`	Full access and control for all Google Cloud resources; manage user access
`roles/writer`	Editor	All `cloudsql` permissions except for `cloudsql.*.getIamPolicy` & `cloudsql.*.setIamPolicy`	Read-write access to all Google Cloud and Cloud SQL resources (full control except for the ability to modify permissions)

`roles/reader`	Viewer	`cloudsql.*.export`
		`cloudsql.*.get`
		`cloudsql.*.list`
			Read-only access to all Google Cloud resources, including Cloud SQL resources

`roles/cloudsql.admin`	Cloud SQL Admin	`cloudsql.*`	Full control for all Cloud SQL resources.

Role	Name	Cloud SQL permissions	Description

`roles/cloudsql.editor`	Cloud SQL Editor	`cloudsql.instances.addServerCa`
		`cloudsql.instances.connect`
		`cloudsql.instances.export`
		`cloudsql.instances.failover`
		`cloudsql.instances.get`
		`cloudsql.instances.list`
		`cloudsql.instances.listServerCas`
		`cloudsql.instances.restart`
		`cloudsql.instances.rotateServerCa`
		`cloudsql.instances.truncateLog`
		`cloudsql.instances.update`
		`cloudsql.databases.create`
		`cloudsql.databases.get`
		`cloudsql.databases.list`
		`cloudsql.databases.update`
		`cloudsql.backupRuns.create`
		`cloudsql.backupRuns.get`
		`cloudsql.backupRuns.list`
		`cloudsql.sslCerts.get`
		`cloudsql.sslCerts.list`
		`cloudsql.users.list`
			Manage Cloud SQL resources. No ability to see or modify permissions, nor modify users or sslCerts. No ability to import data or restore from a backup, nor clone, delete, or promote instances. No ability to start or stop replicas. No ability to delete databases, replicas, or backups.

`roles/cloudsql.viewer`	Cloud SQL Viewer	`cloudsql.*.export`
		`cloudsql.*.get`
		`cloudsql.*.list`
		`cloudsql.instances.listServerCa`
			Read-only access to all Cloud SQL resources.

`roles/cloudsql.client`	Cloud SQL Client	`cloudsql.instances.connect` `cloudsql.instances.get`	Connectivity access to Cloud SQL instances from App Engine and the Cloud SQL Proxy. Not required for accessing an instance using IP addresses.

The following table lists each permission that Cloud SQL supports, the Cloud SQL roles that include it, and its legacy (primitive) role.

Permission	Cloud SQL roles	Legacy role

Permission	Cloud SQL roles	Legacy role
`cloudsql.backupRuns.create`	Cloud SQL Admin Cloud SQL Editor	Editor
`cloudsql.backupRuns.delete`	Cloud SQL Admin	Editor
`cloudsql.backupRuns.get`	Cloud SQL Admin Cloud SQL Editor Cloud SQL Viewer	Viewer
`cloudsql.backupRuns.list`	Cloud SQL Admin Cloud SQL Editor Cloud SQL Viewer	Viewer
`cloudsql.databases.create`	Cloud SQL Admin Cloud SQL Editor	Editor
`cloudsql.databases.delete`	Cloud SQL Admin Cloud SQL Editor	Editor
`cloudsql.databases.get`	Cloud SQL Admin Cloud SQL Editor Cloud SQL Viewer	Viewer
`cloudsql.databases.getIamPolicy` **`cloudsql.databases.getIamPolicy`** is currently unused, and unsupported for IAM custom roles.	Cloud SQL Admin	Owner
`cloudsql.databases.list`	Cloud SQL Admin Cloud SQL Editor Cloud SQL Viewer	Viewer
`cloudsql.databases.setIamPolicy` **`cloudsql.databases.setIamPolicy`** is currently unused, and unsupported for IAM custom roles.	Cloud SQL Admin	Owner
`cloudsql.databases.update`	Cloud SQL Admin Cloud SQL Editor	Editor

Permission	Cloud SQL roles	Legacy role
`cloudsql.instance.addServerCa` **`cloudsql.instances.addServerCa`** is not yet supported for IAM custom roles.	Cloud SQL Admin Cloud SQL Editor	Editor
`cloudsql.instances.clone`	Cloud SQL Admin	Editor
`cloudsql.instances.connect`	Cloud SQL Admin Cloud SQL Client Cloud SQL Editor	Editor
`cloudsql.instances.create`	Cloud SQL Admin Cloud SQL Editor	Editor
`cloudsql.instances.delete`	Cloud SQL Admin	Editor
`cloudsql.instances.demoteMaster`	Cloud SQL Admin	Editor
`cloudsql.instances.export`	Cloud SQL Admin Cloud SQL Editor Cloud SQL Viewer	Viewer
`cloudsql.instances.failover`	Cloud SQL Admin Cloud SQL Editor	Editor
`cloudsql.instances.get`	Cloud SQL Admin Cloud SQL Client Cloud SQL Editor Cloud SQL Viewer	Viewer
`cloudsql.instances.getIamPolicy` **`cloudsql.instances.getIamPolicy`** is currently unused, and unsupported for IAM custom roles.	Cloud SQL Admin	Owner
`cloudsql.instances.import`	Cloud SQL Admin	Editor
`cloudsql.instances.list`	Cloud SQL Admin Cloud SQL Editor Cloud SQL Viewer	Viewer

Permission	Cloud SQL roles	Legacy role
`cloudsql.instance.listServerCa` **`cloudsql.instances.listServerCa`** is not yet supported for IAM custom roles.	Cloud SQL Viewer	Viewer
`cloudsql.instances.promoteReplica`	Cloud SQL Admin	Editor
`cloudsql.instances.resetSslConfig`	Cloud SQL Admin	Editor
`cloudsql.instances.restart`	Cloud SQL Admin Cloud SQL Editor	Editor
`cloudsql.instances.restoreBackup`	Cloud SQL Admin	Editor
`cloudsql.instance.rotateServerCa` **`cloudsql.instances.rotateServerCa`** is not yet supported for IAM custom roles.	Cloud SQL Admin Cloud SQL Editor	Editor
`cloudsql.instances.setIamPolicy` **`cloudsql.instances.setIamPolicy`** is currently unused, and unsupported for IAM custom roles.	Cloud SQL Admin	Owner
`cloudsql.instances.startReplica`	Cloud SQL Admin	Editor
`cloudsql.instances.stopReplica`	Cloud SQL Admin	Editor
`cloudsql.instances.truncateLog`	Cloud SQL Admin Cloud SQL Editor	Editor
`cloudsql.instances.update`	Cloud SQL Admin Cloud SQL Editor	Editor
`cloudsql.sslCerts.create`	Cloud SQL Admin	Editor
`cloudsql.sslCerts.delete`	Cloud SQL Admin Cloud SQL Editor	Editor
`cloudsql.sslCerts.get`	Cloud SQL Admin Cloud SQL Editor Cloud SQL Viewer	Viewer

Permission	Cloud SQL roles	Legacy role
`cloudsql.sslCerts.list`	Cloud SQL Admin Cloud SQL Editor Cloud SQL Viewer	Viewer
`cloudsql.users.create`	Cloud SQL Admin Cloud SQL Editor	Editor
`cloudsql.users.delete`	Cloud SQL Admin Cloud SQL Editor	Editor
`cloudsql.users.list`	Cloud SQL Admin Cloud SQL Editor Cloud SQL Viewer	Viewer
`cloudsql.users.update`	Cloud SQL Admin	Editor

If the predefined roles do not address your unique business requirements, you can define your own custom roles with permissions that you specify. To support this, IAM offers custom roles (/iam/docs/understanding-custom-roles).

When you create custom roles for Cloud SQL, make sure that if you include either `cloudsql.instances.list` or `cloudsql.instances.get`, that you include them both. Otherwise, the Cloud Console will not function correctly for Cloud SQL.

Task	Required additional permissions
Displaying the instance listing page	`cloudsql.instances.list` `resourcemanager.projects.get`

Creating an instance	`cloudsql.instances.create`
	`cloudsql.instances.get`
	`cloudsql.instances.list`
	`resourcemanager.projects.get`

Connecting to an instance from the Cloud Shell	`cloudsql.instances.get`
	`cloudsql.instances.list`
	`cloudsql.instances.update`
	`resourcemanager.projects.get`

Task	Required additional permissions

Creating a user	`cloudsql.instances.get`
	`cloudsql.instances.list`
	`cloudsql.users.create`
	`cloudsql.users.list`
	`resourcemanager.projects.get`

Viewing instance information	`cloudsql.instances.get`
	`cloudsql.instances.list`
	`cloudsql.users.list`
	`monitoring.timeSeries.list`
	`resourcemanager.projects.get`

Command	Required permissions
`gcloud sql backups create`	`cloudsql.backupRuns.create`
`gcloud sql backups delete`	`cloudsql.backupRuns.delete`
`gcloud sql backups describe`	`cloudsql.backupRuns.get`
`gcloud sql backups list`	`cloudsql.backupRuns.list`
`gcloud sql backups restore`	`cloudsql.backupRuns.get` `cloudsql.instances.restoreBackup`
`gcloud sql connect`	`cloudsql.instances.get` `cloudsql.instances.update`
`gcloud sql databases create`	`cloudsql.databases.create`
`gcloud sql databases delete`	`cloudsql.databases.delete`
`gcloud sql databases describe`	`cloudsql.databases.get`
`gcloud sql databases list`	`cloudsql.databases.list`
`gcloud sql databases patch`	`cloudsql.databases.get` `cloudsql.databases.update`
`gcloud sql export`	`cloudsql.instances.export` `cloudsql.instances.get`
`gcloud sql flags list`	None

Command	Required permissions
`gcloud sql import`	`cloudsql.instances.import`
`gcloud sql instances clone`	`cloudsql.instances.clone`
`gcloud sql instances create`	`cloudsql.instances.create`
`gcloud sql instances delete`	`cloudsql.instances.delete`
`gcloud sql instances describe`	`cloudsql.instances.get`
`gcloud sql instances export`	`cloudsql.instances.export`
`gcloud sql instances failover`	`cloudsql.instances.failover`
`gcloud sql instances import`	`cloudsql.instances.import`
`gcloud sql instances list`	`cloudsql.instances.list`
`gcloud sql instances patch`	`cloudsql.instances.get` `cloudsql.instances.update`
`gcloud sql instances promote-replica`	`cloudsql.instances.promoteReplica`
`gcloud sql instances reset-ssl-config`	`cloudsql.instances.resetSslConfig`
`gcloud sql instances restart`	`cloudsql.instances.restart`
`gcloud sql instances restore-backup`	`cloudsql.backupRuns.get` `cloudsql.instances.restoreBackup`
`gcloud sql operations describe`	`cloudsql.instances.get`
`gcloud sql operations list`	`cloudsql.instances.get`
`gcloud sql operations wait`	`cloudsql.instances.get`
`gcloud sql ssl client-certs create`	`cloudsql.sslCerts.create`
`gcloud sql ssl client-certs delete`	`cloudsql.sslCerts.delete`
`gcloud sql ssl client-certs describe`	`cloudsql.sslCerts.list`
`gcloud sql ssl client-certs list`	`cloudsql.sslCerts.list`
`gcloud sql tiers list`	None
`gcloud sql users create`	`cloudsql.users.create`
`gcloud sql users delete`	`cloudsql.users.delete`

Command	Required permissions
`gcloud sql users list`	`cloudsql.users.list`
`gcloud sql users set-password`	`cloudsql.users.update`

The following table lists the permissions that the caller must have to call each method in the Cloud SQL API, or to perform tasks using Google Cloud tools that use the API (such as the Google Cloud Console or the `gcloud` command line tool).

To call a method, you must also have the required scopes as described in the method's reference page, in addition to t
ssions below. For more information, see Authorizing requests with OAuth 2.0
docs/postgres/admin-api/#OAuth2Authorizing).

All permissions are applied to the project. You cannot apply different permissions based on the instance or other lower-level object.

Method	Required permissions
`backupRuns.delete` (/sql/docs/postgres/admin-api/rest/v1beta4/backupRuns/delete)	`cloudsql.backupRuns.delete`
`backupRuns.get` (/sql/docs/postgres/admin-api/rest/v1beta4/backupRuns/get)	`cloudsql.backupRuns.get`
`backupRuns.insert` (/sql/docs/postgres/admin-api/rest/v1beta4/backupRuns/insert)	`cloudsql.backupRuns.create`
`backupRuns.list` (/sql/docs/postgres/admin-api/rest/v1beta4/backupRuns/list)	`cloudsql.backupRuns.list`
`databases.delete` (/sql/docs/postgres/admin-api/rest/v1beta4/databases/delete)	`cloudsql.databases.delete`
`databases.get` (/sql/docs/postgres/admin-api/rest/v1beta4/databases/get)	`cloudsql.databases.get`
`databases.insert` (/sql/docs/postgres/admin-api/rest/v1beta4/databases/insert)	`cloudsql.databases.create`

Method	Required permissions
databases.list (/sql/docs/postgres/admin-api/rest/v1beta4/databases/list)	cloudsql.databases.list
databases.patch (/sql/docs/postgres/admin-api/rest/v1beta4/databases/patch)	cloudsql.databases.update, cloudsql.databases.get
databases.update (/sql/docs/postgres/admin-api/rest/v1beta4/databases/update)	cloudsql.databases.update
flags.list (/sql/docs/postgres/admin-api/rest/v1beta4/flags/list)	None
instances.clone (/sql/docs/postgres/admin-api/rest/v1beta4/instances/clone)	cloudsql.instances.clone
instances.delete (/sql/docs/postgres/admin-api/rest/v1beta4/instances/delete)	cloudsql.instances.delete
instances.export (/sql/docs/postgres/admin-api/rest/v1beta4/instances/export)	cloudsql.instances.export
instances.failover (/sql/docs/postgres/admin-api/rest/v1beta4/instances/failover)	cloudsql.instances.failover
instances.get (/sql/docs/postgres/admin-api/rest/v1beta4/instances/get)	cloudsql.instances.get
instances.import (/sql/docs/postgres/admin-api/rest/v1beta4/instances/import)	cloudsql.instances.import
instances.insert (/sql/docs/postgres/admin-api/rest/v1beta4/instances/insert)	cloudsql.instances.create
instances.list (/sql/docs/postgres/admin-api/rest/v1beta4/instances/list)	cloudsql.instances.list
instances.patch (/sql/docs/postgres/admin-api/rest/v1beta4/instances/patch)	cloudsql.instances.get, cloudsql.instances.update
instances.promoteReplica (/sql/docs/postgres/admin-api/rest/v1beta4/instances/promoteReplica)	cloudsql.instances.promoteReplica
instances.resetSslConfig (/sql/docs/postgres/admin-api/rest/v1beta4/instances/resetSslConfig)	cloudsql.instances.resetSslConfig

Method	Required permissions
instances.restart (/sql/docs/postgres/admin-api/rest/v1beta4/instances/restart)	cloudsql.instances.restart
instances.restoreBackup (/sql/docs/postgres/admin-api/rest/v1beta4/instances/restoreBackup)	cloudsql.instances.restoreBackup, cloudsql.backupRuns.get
instances.startReplica (/sql/docs/postgres/admin-api/rest/v1beta4/instances/startReplica)	cloudsql.instances.startReplica
instances.stopReplica (/sql/docs/postgres/admin-api/rest/v1beta4/instances/stopReplica)	cloudsql.instances.stopReplica
instances.truncateLog (/sql/docs/postgres/admin-api/rest/v1beta4/instances/truncateLog)	cloudsql.instances.truncateLog
instances.update (/sql/docs/postgres/admin-api/rest/v1beta4/instances/update)	cloudsql.instances.update
operations.get (/sql/docs/postgres/admin-api/rest/v1beta4/operations/get)	cloudsql.instances.get
operations.list (/sql/docs/postgres/admin-api/rest/v1beta4/operations/list)	cloudsql.instances.get
sslCerts.delete (/sql/docs/postgres/admin-api/rest/v1beta4/sslCerts/delete)	cloudsql.sslCerts.delete
sslCerts.get (/sql/docs/postgres/admin-api/rest/v1beta4/sslCerts/get)	cloudsql.sslCerts.get
sslCerts.insert (/sql/docs/postgres/admin-api/rest/v1beta4/sslCerts/insert)	cloudsql.sslCerts.create
sslCerts.list (/sql/docs/postgres/admin-api/rest/v1beta4/sslCerts/list)	cloudsql.sslCerts.list
users.delete (/sql/docs/postgres/admin-api/rest/v1beta4/users/delete)	cloudsql.users.delete
users.insert (/sql/docs/postgres/admin-api/rest/v1beta4/users/insert)	cloudsql.users.create

Method	Required permissions
`users.list` (/sql/docs/postgres/admin-api/rest/v1beta4/users/list)	`cloudsql.users.list`
`users.update` (/sql/docs/postgres/admin-api/rest/v1beta4/users/update)	`cloudsql.users.update`

You can get and set IAM policies and roles using the Google Cloud Console, the IAM methods of the API, or the Cloud SDK. For more information, see Granting, Changing, and Revoking Access to Project Members (/iam/docs/granting-changing-revoking-access).

- Learn how to grant and revoke access to project members (/iam/docs/granting-changing-revoking-access).
- Learn more about IAM (/iam/docs/).
- Learn more about primitive roles (/iam/docs/understanding-roles#primitive_roles).
- Learn about instance access control (/sql/docs/postgres/instance-access-control).
- Learn about database access control (/sql/docs/postgres/users).
- Learn more about custom roles (/iam/docs/understanding-custom-roles).