

[Cloud SQL](https://cloud.google.com/sql/) (<https://cloud.google.com/sql/>)

[Documentation](https://cloud.google.com/sql/docs/) (<https://cloud.google.com/sql/docs/>)

[MySQL](https://cloud.google.com/sql/docs/mysql/) (<https://cloud.google.com/sql/docs/mysql/>) [Guides](#)

Using customer-managed encryption keys (CMEK)

MySQL | [PostgreSQL](https://cloud.google.com/sql/docs/postgres/configure-cmek) (<https://cloud.google.com/sql/docs/postgres/configure-cmek>) | [SQL Server](https://cloud.google.com/sql/docs/sqlserver/configure-cmek) (<https://cloud.google.com/sql/docs/sqlserver/configure-cmek>)

This page describes how to set up a service account and keys for customer-managed encryption keys, and how to create an instance that uses a customer-managed encryption key. To learn more about using customer-managed encryption keys with Cloud SQL, see [Overview of customer-managed encryption keys](https://cloud.google.com/sql/docs/mysql/cmek) (<https://cloud.google.com/sql/docs/mysql/cmek>).

Before you begin

1. [Sign in](https://accounts.google.com/Login) (<https://accounts.google.com/Login>) to your Google Account.

If you don't already have one, [sign up for a new account](https://accounts.google.com/SignUp) (<https://accounts.google.com/SignUp>).

2. In the Cloud Console, on the project selector page, select or create a Google Cloud project.

★ **Note:** If you don't plan to keep the resources that you create in this procedure, create a project instead of selecting an existing project. After you finish these steps, you can delete the project, removing all resources associated with the project.

[GO TO THE PROJECT SELECTOR PAGE](https://console.cloud.google.com/projectselector) ([HTTPS://CONSOLE.CLOUD.GOOGLE.COM/PROJECTSELECT](https://console.cloud.google.com/projectselector))

3. Make sure that billing is enabled for your Google Cloud project. [Learn how to confirm billing is enabled for your project](https://cloud.google.com/billing/docs/how-to/modify-project) (<https://cloud.google.com/billing/docs/how-to/modify-project>).
4. [Install and initialize the Cloud SDK](https://cloud.google.com/sdk/docs/) (<https://cloud.google.com/sdk/docs/>).
5. Make sure you have the Cloud SQL Admin role on your user account.

[GO TO THE CLOUD IAM PAGE](https://console.cloud.google.com/iam-admin/iam) ([HTTPS://CONSOLE.CLOUD.GOOGLE.COM/IAM-ADMIN/IAM](https://console.cloud.google.com/iam-admin/iam))

6. Enable the Cloud Key Management Service API.

ENABLE THE API ([HTTPS://CONSOLE.CLOUD.GOOGLE.COM/FLOWS/ENABLEAPI?APIID=CLOUDKMS](https://console.cloud.google.com/flows/enableapi?apiid=cloudkms))

Workflow for creating a Cloud SQL instance with CMEK

1. Create a service account (#service-account) for each project that requires customer-managed encryption keys.
2. Create a keyring and key (#key), and set the location for each key.
3. Grant the key access (#grantkey) to the service account.
4. Note the key ID (KMS_RESOURCE_ID) and location. You need this information to create instances enabled with CMEK.
5. Go to a project and create a Cloud SQL instance (#createcmekinstance) with the following options:
 - a. The same location as the customer-managed encryption key
 - b. The customer-managed key configuration
 - c. The customer-managed encryption key ID

Your Cloud SQL instance is now enabled with CMEK.

Creating a service account

Note: To create a service account with the required permissions, you must have `resourcemanager.projects.setIamPolicy` permission. This permission is included in the Project Owner, Project IAM Admin, and Organization Administrator roles.

You must also enable the Cloud SQL Admin API.

You need to create a service account for each project that requires customer-managed encryption keys. Currently, you can only use `gcloud` command-line tool commands to create the type of service account you need for customer-managed encryption keys.

To create a service account with `gcloud` command-line tool, run the following command:

```
gcloud alpha services identity create --service=sqladmin.googleapis.com \  
--project=[USER_PROJECT]
```



The previous command returns a service account name, using the following format:

```
service-[PROJECT_NUMBER]@gcp-sa-cloud-sql.iam.gserviceaccount.com
```



For example:

```
service-534582264470@gcp-sa-cloud-sql.iam.gserviceaccount.com
```



You use this service account name during the procedure in [Granting the key access to the service account](#) (#grantkey).

Creating a key

You can create the key in the same GCP project as the Cloud SQL instance or in a separate user project. The Cloud KMS key ring location must match the region where you want to create Cloud SQL instance. A multi-region or global region key **will not** work. The Cloud SQL instance create request fails if the regions don't match.

To create a Cloud KMS key:

CONSOLE

G CLOUD

1. Go to the **Cryptographic keys** page.

[GO TO THE CRYPTOGRAPHIC KEYS PAGE \(HTTPS://CONSOLE.CLOUD.GOOGLE.COM/SECURITY/KM](https://console.cloud.google.com/security/kms)

2. Click **CREATE KEY RING**.
3. Add a **Key ring name**.
4. Add a **Key ring location**.
5. Click **CREATE**. The **Create key** page opens.
6. Add a **Key name**.
7. Select a **Purpose** (symmetric or asymmetric).
8. Select a **Rotation period** and **Starting on date**.
9. Click **CREATE**.

10. On the **Keys** table, click the three dots in the last column, and select **Copy Resource ID**. This is the `KMS_RESOURCE_ID`. You need the `KMS_RESOURCE_ID` when creating the Cloud SQL instance.


Granting the key access to the service account

To grant access to the service account:

CONSOLE GCLOUD

1. Go to the **Cryptographic keys** page.

GO TO THE CLOUD KMS PAGE ([HTTPS://CONSOLE.CLOUD.GOOGLE.COM/SECURITY/KMS](https://console.cloud.google.com/security/kms))

2. Select the keys you created for customer-managed encryption keys.
3. Select **SHOW INFO PANEL**.
4. Click **ADD MEMBER**.  add member button
5. Add the service account name you created in **New members**.
6. In **Select a role**, select **Cloud KMS > Cloud KMS CryptoKey Encrypter/Decrypter**.
7. Click **SAVE**.
8. Return to the **Cryptographic keys** (<https://console.cloud.google.com/security/kms>) page and select the key again.
9. Select the **SHOW INFO PANEL**. You should see roles on the ****Role/Member**** column.

Creating a Cloud SQL instance with CMEK

Note: Currently, you can only use `gcloud` command-line tool commands and `cURL` to create Cloud SQL instances with CMEK.

To create an instance with customer-managed encryption keys:

GCLOUD CURL

```
gcloud sql instances create [INSTANCE_NAME] --project [PROJECT_ID] \  
--disk-encryption-key [KMS_RESOURCE_ID]
```



This cURL command uses [Instances:Insert](#)

(<https://cloud.google.com/sql/docs/mysql/admin-api/v1beta4/instances/insert>).

Creating a backup for a CMEK-enabled instance

When you create a backup of a Cloud SQL instance, the backup is encrypted with the same customer-managed encryption key as the primary instance.

See [Creating and managing on-demand and automatic backups](#)

(<https://cloud.google.com/sql/docs/mysql/backup-recovery/backing-up>). The only change is that you see a warning on the **Create a backup** page that says: "Your backup will be encrypted with this instance's customer-managed encryption key. If anyone destroys this key, all data encrypted with the key will be permanently lost."

Creating a replica for a CMEK-enabled instance

When you create a read replica of a Cloud SQL instance, it inherits the same customer-managed encryption key as the parent instance.

See [Creating read replicas](#) (<https://cloud.google.com/sql/docs/mysql/replication/create-replica>). The only change is that you see a warning on the **Create read replica** page that says: "Your replica will be encrypted with the master instance's customer-managed key. If anyone destroys this key, all data encrypted with it will be permanently lost."

Creating a clone of a CMEK-enabled instance

When you create a clone of Cloud SQL instance, it inherits the same customer-managed encryption key as the one used to encrypt the source instance.

See [Cloning instances](#) (<https://cloud.google.com/sql/docs/mysql/clone-instance>). The only change is that you see a warning on the **Create clone** page: "Your clone will be encrypted with the source

instance's customer-managed key. If anyone destroys this key, all data encrypted with it will be permanently lost."

Disabling and re-enabling key versions

See the following topics:

- [Disable an enabled key version](https://cloud.google.com/kms/docs/enable-disable#disable_an_enabled_key_version)
(https://cloud.google.com/kms/docs/enable-disable#disable_an_enabled_key_version)
- [Enable a disabled key version](https://cloud.google.com/kms/docs/enable-disable#enable_a_disabled_key_version)
(https://cloud.google.com/kms/docs/enable-disable#enable_a_disabled_key_version)

Troubleshooting

This section describes things to try when you get an error message while setting up or using CMEK-enabled instances.

Cloud SQL administrator operations, such as create, clone, or update, might fail due to Cloud KMS errors, and missing roles or permissions. Common reasons for failure include a missing Cloud KMS key version, a disabled or destroyed Cloud KMS key version, insufficient IAM permissions to access the Cloud KMS key version, or the Cloud KMS key version is in a different region than the Cloud SQL instance. Use the following troubleshooting table to diagnose and resolve common problems.

Customer-managed encryption keys troubleshooting table

For this error...	The issue might be...	Try this...
Per-product, per-project service account not found	The service account name is incorrect.	Make sure you created a service account for the correct user pr GO TO THE SERVICE ACCOUNTS PAGE (HTTPS://CONSOLE.CI
Cannot	The user account does not have	Add the Organization Administrator role on your user or servic

grant permission to grant access to this access to key version. the service account	GO TO THE IAM ACCOUNTS PAGE (HTTPS://CONSOLE.CLOUD.GOOGL
Cloud KMSThe key version is destroyed. key version is destroyed	If the key version is destroyed, you cannot use it to encrypt or d
Cloud KMSThe key version is disabled. key version is disabled	Re-enable the Cloud KMS key version. GO TO THE CRYPTO KEYS PAGE (HTTPS://CONSOLE.CLOUD.GOOGL
InsufficientThe <code>cloudkms . cryptoKeyEncrypterDecrypter</code> permission to use the role is missing on the user or Cloud KMSservice account you are using to key run operations on Cloud SQL instances, or the Cloud KMS key version doesn't exist.	Add the <code>cloudkms . cryptoKeyEncrypterDecrypter</code> role on GO TO THE IAM ACCOUNTS PAGE (HTTPS://CONSOLE.CLOUD.GOOGL If the role is already on your account, see Creating a key (https://cloud.google.com/sql/docs/mysql/configure-cmek#k
Cloud KMSThe key version does not exist. key is not found	Create a new key version. See Creating a key (https://cloud.google.com/sql/docs/mysql/configure-cmek#k note).
Cloud SQL The Cloud KMS key version and instance Cloud SQL instance must be in the and Cloud same region. It does not work if KMS key the Cloud KMS key version is in a version areglobal region or multi-region. in different regions	Create a key version in the same region where you want to crea (https://cloud.google.com/sql/docs/mysql/configure-cmek#k

Note: If the instance is in a failed state during the `create` operation, you must delete it, add the role to the account you are using, and create a new instance with a active Cloud KMS key version.

What's next

- [Configure access to the instance](https://cloud.google.com/sql/docs/mysql/instance-access-control) (<https://cloud.google.com/sql/docs/mysql/instance-access-control>).

- [Connect to the instance with a client](https://cloud.google.com/sql/docs/mysql/connect-admin-ip)
(<https://cloud.google.com/sql/docs/mysql/connect-admin-ip>).
- [Create a database on the instance](https://cloud.google.com/sql/docs/mysql/create-manage-databases)
(<https://cloud.google.com/sql/docs/mysql/create-manage-databases>).
- [Import data into the instance](https://cloud.google.com/sql/docs/mysql/import-export/importing)
(<https://cloud.google.com/sql/docs/mysql/import-export/importing>).
- [Create users on the instance](https://cloud.google.com/sql/docs/mysql/create-manage-users) (<https://cloud.google.com/sql/docs/mysql/create-manage-users>).
- [Learn more about instance settings](https://cloud.google.com/sql/docs/mysql/instance-settings)
(<https://cloud.google.com/sql/docs/mysql/instance-settings>).

Except as otherwise noted, the content of this page is licensed under the [Creative Commons Attribution 4.0 License](https://creativecommons.org/licenses/by/4.0/) (<https://creativecommons.org/licenses/by/4.0/>), and code samples are licensed under the [Apache 2.0 License](https://www.apache.org/licenses/LICENSE-2.0) (<https://www.apache.org/licenses/LICENSE-2.0>). For details, see our [Site Policies](https://developers.google.com/terms/site-policies) (<https://developers.google.com/terms/site-policies>). Java is a registered trademark of Oracle and/or its affiliates.

Last updated January 15, 2020.