Create symmetric and asymmetric keys

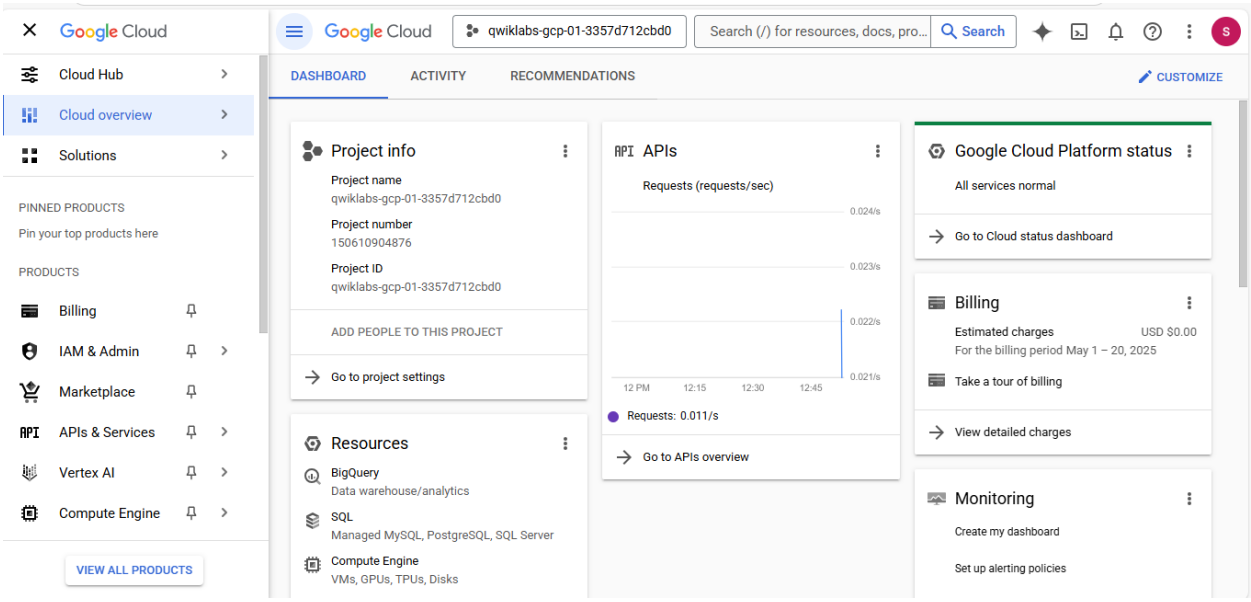
Task 1. Create a symmetric key

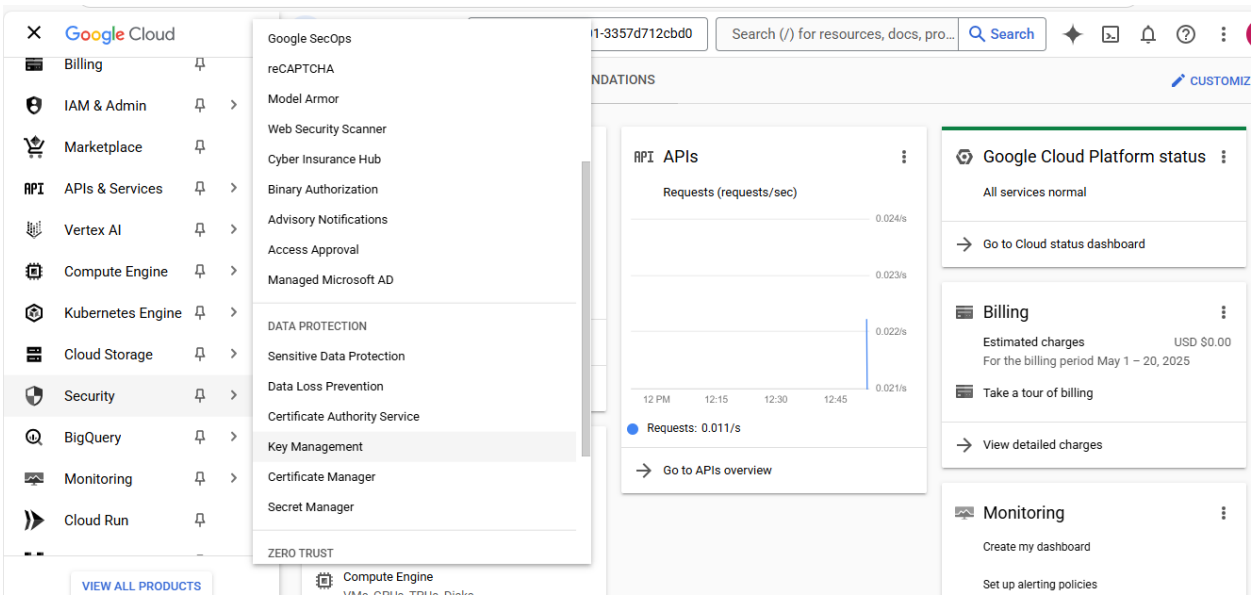
In this task, you'll delve into the intricate process of crafting a symmetric key, complete with considerations for its designated region and the crucial aspect of its protection level. You'll begin by generating a symmetric key with carefully tailored parameters.

1. In the Google Cloud console, click the **Navigation menu** ().
2. Select **Security > Key Management**.
3. On the **Key Rings** tabbed page, click **+ Create Key Ring**.

Now, specify the key details.

4. For **Key ring name**, enter **demo-key-ring**.
5. For the **Location type** category, select **Region**.
6. Expand the **Region** drop-down menu, and select **REGION**.



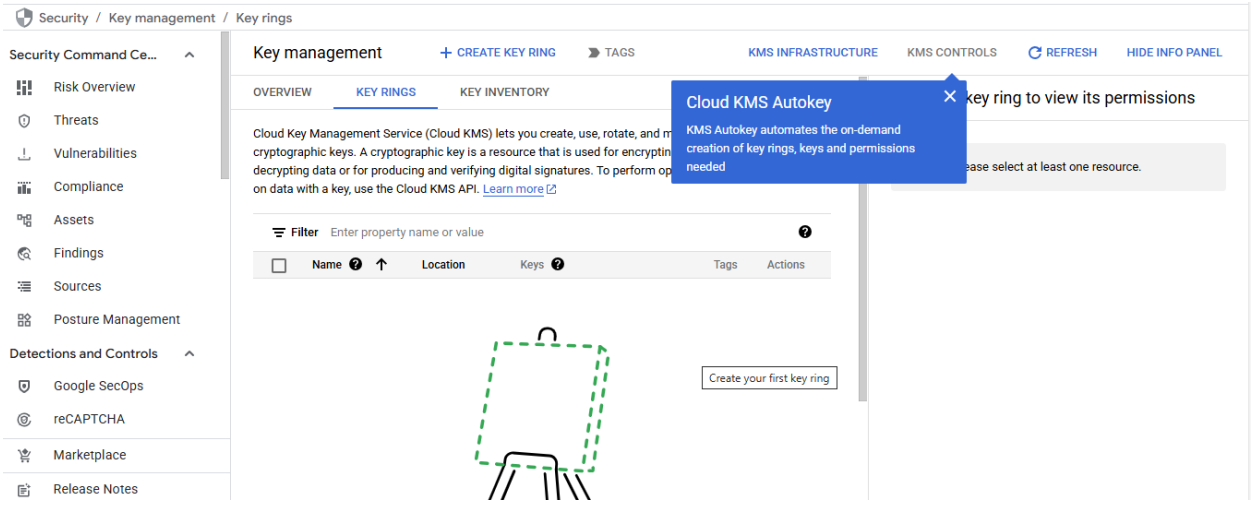


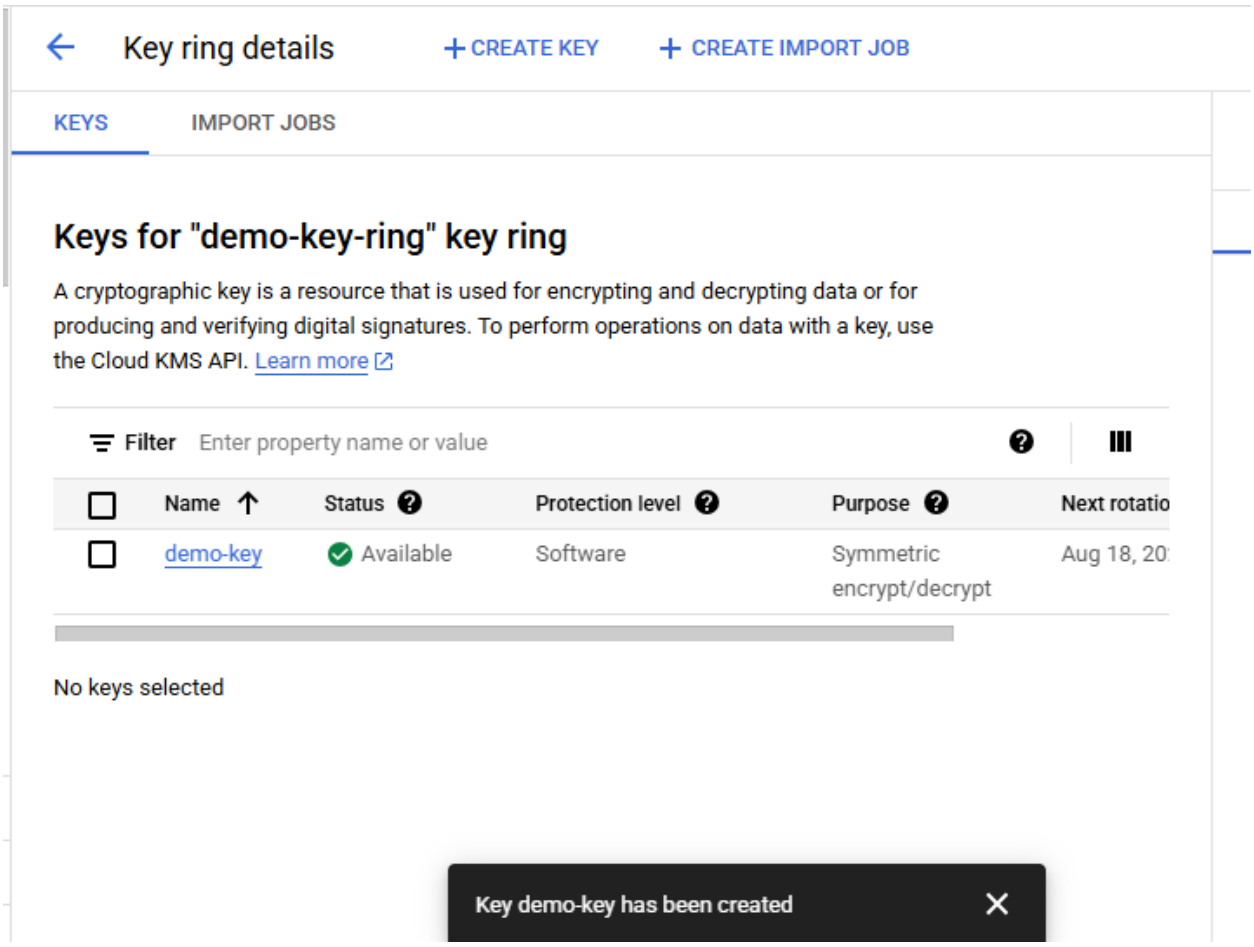
7. Click **Create**.
8. In the **Name and protection level** category, in the **Key name** field, enter **demo-key**.

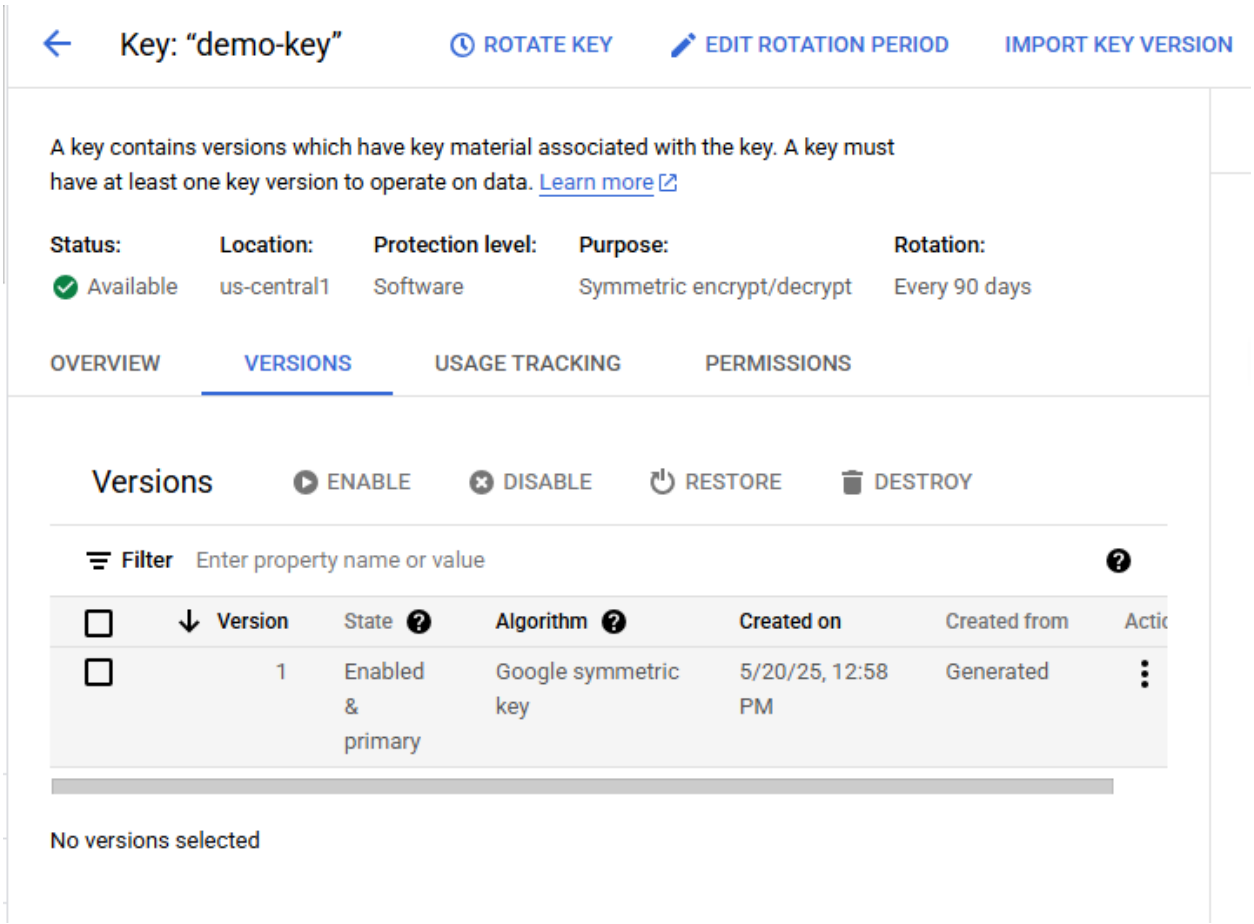
   The **Protection level** should be set to **Software** by default, if not, select it now.
9. Click **Continue**. The Key material category expands.
10. For **Key material**, select **Generated key**.
11. Click **Continue**. The Purpose and algorithm category expands.
12. For **Purpose**, select **Symmetric encrypt/decrypt**.
13. Click **Continue**. The Versions category expands.
14. For **Key rotation period**, select **90 days**.
15. For **Starting on**, leave as the default value.
16. Click **Continue**. No additional settings are needed.
17. Click **Create**.

    Once the key is created, it can be used for a variety of implementations such as data encryption and decryption.

    Symmetric keys are commonly used to encrypt sensitive data before storage or transmission. When data needs to be accessed or shared, the same symmetric key is used to decrypt the encrypted content, ensuring that only authorized parties can access the original information.


Security / Key management / Key rings
Security Command Ce...
Risk Overview
Threats
Vulnerabilities
Compliance
Assets
Findings
Sources
Posture Management
Detections and Controls
Google SecOps
reCAPTCHA
Marketplace
Release Notes
Key management
+ CREATE KEY RING
TAGS
KMS INFRASTRUCTURE
KMS CONTROLS
REFRESH
HIDE INFO PANEL
OVERVIEW
KEY RINGS
KEY INVENTORY
Cloud KMS Autokey
KMS Autokey automates the on-demand creation of key rings, keys and permissions needed
Filter
Enter property name or value
Name
Location
Keys
Tags
Actions
Create your first key ring


Key ring details
+ CREATE KEY
+ CREATE IMPORT JOB
KEYS
IMPORT JOBS
Keys for "demo-key-ring" key ring
A cryptographic key is a resource that is used for encrypting and decrypting data or for producing and verifying digital signatures. To perform operations on data with a key, use the Cloud KMS API. Learn more
Filter
Enter property name or value
Name
Status
Protection level
Purpose
Next rotatio
demo-key
Available
Software
Symmetric encrypt/decrypt
Aug 18, 20
No keys selected
Key demo-key has been created



Task 2. Create an asymmetric key

In this task, you'll create an asymmetric key with specific settings, including that of its algorithm and protection level.

1. In the Google Cloud console, click the **Navigation menu** ( ).
2. Select **Security > Key Management**. The Key Rings tabbed page opens, listing the newly-created key.
3. Under **Name**, click the link for the key you created in the previous task: **demo-key-ring**. The Key ring details page opens.
4. In the **Keys** tabbed page, click **+ Create Key**.

Now, specify the key details.

5. For **Key name**, enter **demo-asymmetric-key**.
6. For **Protection Level**, select **Software**.

7. Click **Continue**. The Key material category expands.
8. For **Key Material**, select **Generated key**.
9. Click **Continue**. The Purpose and algorithm category expands.
10. For **Purpose**, select **Asymmetric decrypt**.
11. For **Algorithm**, leave as the default value.
12. Click **Continue**.
13. For **Versions**, no settings are required.
14. Click **Continue**. No additional settings are needed.
15. Click **Create**.

The asymmetric key for decryption should now be created.

Asymmetric keys can also be used for digital signatures. Digital signatures help verify the authenticity and integrity of messages, files, or software, ensuring that they have not been tampered with during transmission. Digital signatures use two keys, one for signing which involves the user's private key, and one for verifying signatures which involves the user's public key. The output of the signature process is called the digital signature.

Create key

A cryptographic key is a resource that is used for encrypting and decrypting data or for producing and verifying digital signatures. A key can have multiple versions.
Learn more

Name and protection level

Key name *
demo-asymmetric-key

Protection Level

- (●) **Software**
  Cryptographic operations are performed on software
- ( ) **HSM**
  Cryptographic operations are performed on a Hardware Security Module (HSM)
- ( ) **External**
  Cryptographic operations are performed using a key stored in an external key manager. Learn more

CONTINUE

Key ring details

+ CREATE KEY + CREATE IMPORT JOB

KEYS IMPORT JOBS

Keys for "demo-key-ring" key ring

A cryptographic key is a resource that is used for encrypting and decrypting data or for producing and verifying digital signatures. To perform operations on data with a key, use the Cloud KMS API. Learn more

Filter Enter property name or value

Name	Status	Protection level	Purpose	Next rota
demo-asymmetric-key	Not applicable	Software	Asymmetric decrypt	Not appl
demo-key	Available	Software	Symmetric encrypt/decrypt	Aug 18, 2

No keys selected

Key demo-asymmetric-key has been created