

[Security & Identity Products](https://cloud.google.com/products/security/) (<https://cloud.google.com/products/security/>)

[Cloud Key Management Service](https://cloud.google.com/kms/) (<https://cloud.google.com/kms/>)

[Documentation](https://cloud.google.com/kms/docs/) (<https://cloud.google.com/kms/docs/>) [Guides](#)

Importing a pre-wrapped key into Cloud KMS

This topic shows you how to manually wrap your key that was created from a source other than Cloud Key Management Service and then import it to Cloud KMS.

If you want to have Cloud KMS automatically wrap your key instead of you manually wrapping your key, see [Importing a key](https://cloud.google.com/kms/docs/importing-a-key) (<https://cloud.google.com/kms/docs/importing-a-key>).

Note: You can import only into keys with [protection level](https://cloud.google.com/kms/docs/algorithms#protection_levels) (https://cloud.google.com/kms/docs/algorithms#protection_levels) **HSM**.

Introduction

Cloud KMS allows you to import user-provided cryptographic keys. As an example, you might have existing keys that you use on-premises, with a key store other than Cloud KMS, and/or in a multi-cloud environment. You can import those keys if you want to use the existing key material with Cloud KMS.

To import your keys, first create an *import job*, which is a temporary resource used only for importing keys. When you create an import job, Cloud KMS generates a "wrapping key", which is a public/private key pair. You use the public key portion of the wrapping key to encrypt (also known as wrap) your pre-existing key material to protect it during the import process. Once your key material is wrapped, you can import it into a new key or key version. The private key portion of the wrapping key is available only within Cloud HSM. Restricting the private key portion to Cloud HSM prevents Google from unwrapping your key material outside of Cloud HSM.

You can repeatedly use the same import job to wrap multiple keys that you want to import. Note that an import job expires 3 days after it is created. Once expired, Cloud KMS will no longer be able to import or unwrap any key material that was wrapped with the import job's public key.

Before you begin

1. This topic assumes you are already using Cloud KMS. If you are not already using Cloud KMS, follow the steps in the [Cloud KMS QuickStart](https://cloud.google.com/kms/docs/quickstart) (<https://cloud.google.com/kms/docs/quickstart>).
2. Create a key ring in a region that supports Cloud HSM as described in [Creating key rings](https://cloud.google.com/kms/docs/hsm#create_a_key_ring) (https://cloud.google.com/kms/docs/hsm#create_a_key_ring).
3. Create a key with protection level HSM as described in [Creating keys](https://cloud.google.com/kms/docs/hsm#create_a_key) (https://cloud.google.com/kms/docs/hsm#create_a_key).
4. Set up [Cloud Identity and Access Management permissions](https://cloud.google.com/kms/docs/iam) (<https://cloud.google.com/kms/docs/iam>) for the key ring and key.
5. Ensure that the key you want to import is in the [correct format](https://cloud.google.com/kms/docs/formatting-keys-for-import) (<https://cloud.google.com/kms/docs/formatting-keys-for-import>).

Key import flow

To import a key, follow these steps.

1. [Create an import job](#) (#create_importjob).
2. [Retrieve the wrapping key](#) (#retrieve_wrapping_key) from the import job.
3. [Wrap the key](#) (#wrap_key) that you want to import.
4. [Make an import request](#) (#request_import).

Create an import job

Import jobs are [ImportJob](#)

(<https://cloud.google.com/kms/docs/reference/rest/v1/projects.locations.keyRings.importJobs>) resources. When you create an import job, you need to specify the [protection level](https://cloud.google.com/kms/docs/algorithms#protection_levels) (https://cloud.google.com/kms/docs/algorithms#protection_levels) and [import method](https://cloud.google.com/kms/docs/key-wrapping#import_methods) (https://cloud.google.com/kms/docs/key-wrapping#import_methods) that you want to use to wrap your key.

To create an import job:

CONSOLE

GCLOUD

API

1. Open the **Cryptographic Keys** page in the Cloud Console.
2. Click the name of the key ring for which you will create an import job.
3. Click **Create import job**.
4. In the **Name** field, enter the name for your import job.
5. From the **Import method** dropdown, select an import method.
6. Click **Create**.

Check the state of the import job

The initial state for an import job is **PENDING_GENERATION**. When the state is **ACTIVE**, the import job is ready to use.

To check the state:

CONSOLE

GCLOUD

API

1. Open the **Cryptographic Keys** page in the Cloud Console.
2. Click the name of the key ring that contains your import job.
3. Click the **Import Jobs** tab at the top of the page.
4. The state will be visible under **Status** next to your import job's name.

Retrieve the wrapping key

To retrieve the wrapping key:

CONSOLE

GCLOUD

API

1. Open the **Cryptographic Keys** page in the Cloud Console.
2. Click the name of the key ring that contains your import job.

3. Click the **Import Jobs** tab at the top of the page.
4. Click the **More** icon (3 vertical dots) next to your import job.
5. Click **Download wrapping key** in the pop-up menu.

For more information about the PEM-encoded format, see the [RFC 7468](https://tools.ietf.org/html/rfc7468) (https://tools.ietf.org/html/rfc7468) sections for [General Considerations](https://tools.ietf.org/html/rfc7468#section-2) (https://tools.ietf.org/html/rfc7468#section-2) and [Textual Encoding of Subject Public Key Info](https://tools.ietf.org/html/rfc7468#section-13) (https://tools.ietf.org/html/rfc7468#section-13).

Wrap the key material

Wrap your pre-existing key material using the import job's public key, which is the PEM value that you retrieved in the previous step. The documentation for the [import method](https://cloud.google.com/kms/docs/key-wrapping#import_methods) (https://cloud.google.com/kms/docs/key-wrapping#import_methods) associated with your import job contains more specific instructions for how your key should be wrapped.

Make a request to import your key

When you include wrapped key material in a request to create a new key or a new key version, Cloud KMS unwraps your key material and stores it in the resulting key version.

To make an import request that includes your wrapped key:

CONSOLE

G CLOUD

API

Create a key to import your key material into.

1. Open the **Cryptographic Keys** page in the Cloud Console.
2. Click the name of the key ring that contains your import job.
3. Click **Create key**.
4. In the **Key name** field, enter the name for your key.
5. In the **Protection level** dropdown, select **HSM**.
6. Select the **Purpose** corresponding to your key from the dropdown. If you selected an asymmetric purpose, select the appropriate **Algorithm** from the dropdown.
7. Under **Key material**, select **Import key material**. Your **Create key** page should look similar to:

Key name *
MyKey

Protection level
HSM

Purpose
Symmetric encrypt/decrypt

Algorithm
Google symmetric key

Key material

Generate a key for me (default)

Import key material

Rotation period
Never (manual rotation)

Labels

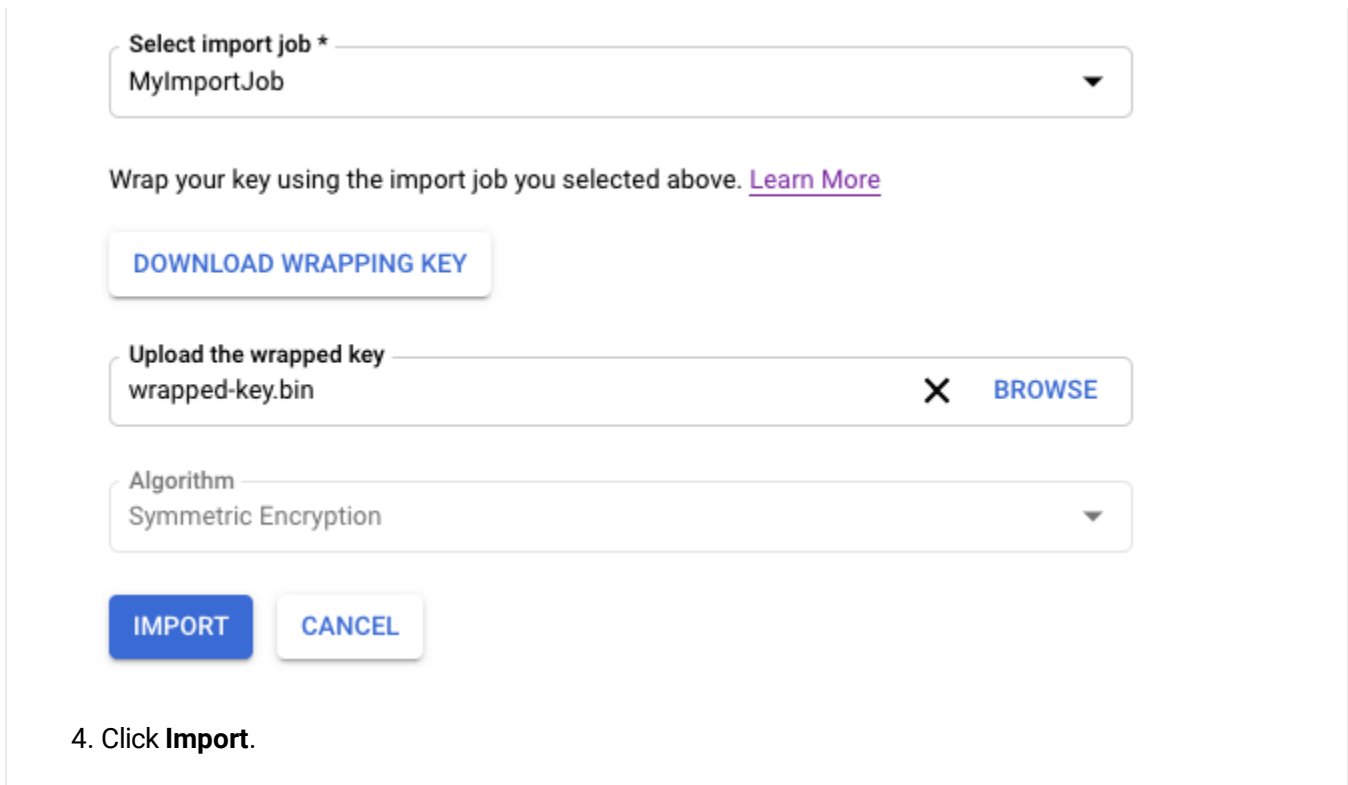
+ ADD LABEL

CREATE CANCEL

8. Click **Create**.

You will be redirected to the **Import key version** page.

1. Select your import job from the **Select import job** dropdown.
2. In the **Upload the wrapped key** selector, selector the key material that you wrapped in the [Wrap the key material](#) (#wrap_key) step.
3. If you are importing an asymmetric key, select the algorithm from the **Algorithm** dropdown. Your **Import key version** page should look similar to:



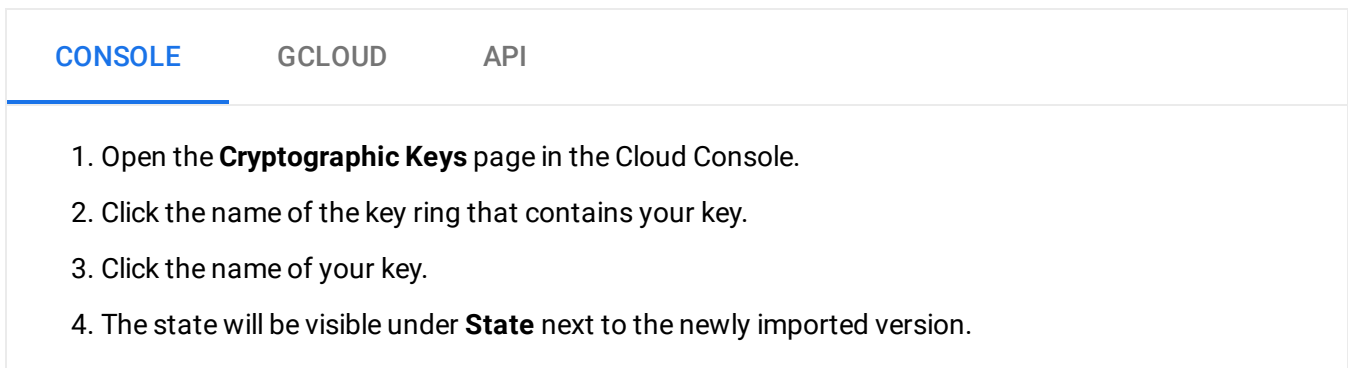
The screenshot shows a web interface for importing a key. At the top, there is a dropdown menu labeled "Select import job *" with "MyImportJob" selected. Below this is a text instruction: "Wrap your key using the import job you selected above. [Learn More](#)". Underneath is a button labeled "DOWNLOAD WRAPPING KEY". The next section is an upload area labeled "Upload the wrapped key" with the filename "wrapped-key.bin" and a "BROWSE" button. Below that is another dropdown menu labeled "Algorithm" with "Symmetric Encryption" selected. At the bottom of the form are two buttons: "IMPORT" and "CANCEL".

4. Click **Import**.

Check the state of the imported key

The initial state for an imported key is `PENDING_IMPORT`. When the state is `ENABLED`, the imported key is ready to use.

To check the state:



The screenshot shows the Cloud Console interface with three tabs: "CONSOLE", "GCLOUD", and "API". The "CONSOLE" tab is selected. Below the tabs is a list of four steps:

1. Open the **Cryptographic Keys** page in the Cloud Console.
2. Click the name of the key ring that contains your key.
3. Click the name of your key.
4. The state will be visible under **State** next to the newly imported version.

When a key is successfully imported, its state is `ENABLED` and you can use it via Cloud KMS. However, it is not configured as the primary version.

Note: By default, the imported key will not have [automatic rotation](https://cloud.google.com/kms/docs/key-rotation#automatic_rotation) (https://cloud.google.com/kms/docs/key-rotation#automatic_rotation) enabled. Additionally, you may turn on automatic rotation or manually rotate the imported key within Cloud KMS, but any rotation within Cloud KMS means the rotated key will no longer be synchronized with your original imported key.

To verify that the key contains your key material and is HSM-protected, see [Verify your imported key](https://cloud.google.com/kms/docs/importing-a-key#verify_key) (https://cloud.google.com/kms/docs/importing-a-key#verify_key).

After verifying the imported key, you can optionally [configure it to be the primary version](https://cloud.google.com/sdk/gcloud/reference/kms/keys/set-primary-version) (<https://cloud.google.com/sdk/gcloud/reference/kms/keys/set-primary-version>). Only symmetric keys can have a primary version.

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 22, 2020.