



**ENTRUST**

# Bring Your Own Key for Google Cloud Key Management and Entrust KeyControl

Integration Guide

11 Jul 2023

# Contents

1. Introduction	3
1.1. Documents to read first	3
1.2. Product configurations	3
1.3. Features tested	3
1.4. Requirements	4
2. Install and configure Entrust KeyControl	5
2.1. Deploy an Entrust KeyControl cluster	5
2.2. Create an Entrust KeyControl Management Vault	5
3. Configure Google Cloud Platform	7
3.1. Required GCP permissions	7
3.2. Create a service account in GCP	8
3.3. Create a key for the service account	10
3.4. Create a GCP key ring	11
4. Configure Entrust KeyControl as GCP KMS	14
4.1. Create an Entrust KeyControl CSP account for the GCP service account	14
4.2. Verify the connection between Entrust KeyControl and GCP	16
5. Test integration	18
5.1. Create a key set in Entrust KeyControl	18
5.2. Create a cloud key in Entrust KeyControl	20
5.3. Import a GCP cloud key into Entrust KeyControl	23
5.4. Rotate a cloud key in Entrust KeyControl	25
5.5. Remove a cloud key in Entrust KeyControl	26
5.6. Upload a removed Entrust KeyControl key back to GCP	28
5.7. Delete a cloud key in Entrust KeyControl	29
5.8. Cancel a cloud key deletion in Entrust KeyControl	30

# 1. Introduction

This document describes the integration of Google Cloud Platform (GCP) Bring Your Own Key (BYOK), referred to as GCP BYOK in this guide, with the Entrust KeyControl Key Management Solution (KMS).

## 1.1. Documents to read first

This guide describes how to configure Entrust KeyControl server as a KMS in GCP.



Entrust KeyControl v10.1 supports BYOK as an add-on. You can request a free trial of Entrust KeyControl BYOK here: <https://go.entrust.com/keycontrol-byok-30-day-free-trial>.

To install and configure the Entrust KeyControl server see [KeyControl Installation and Upgrade Guide](#).

Also refer to the documentation and set-up process for GCP BYOK in the [Google Cloud Key Management Service documentation](#).

## 1.2. Product configurations

Entrust has successfully tested the integration of KeyControl with GCP BYOK in the following configurations:

System	Version
Entrust KeyControl	10.1

## 1.3. Features tested

Entrust has successfully tested the following features:

Feature	Tested
Create cloud key	✓
Import cloud key	✓
Rotate cloud key	✓
Remove cloud key	✓

Feature	Tested
Upload removed cloud key	✓
Delete cloud key	✓
Cancel cloud key deletion	✓

## 1.4. Requirements



Entrust recommends that you allow only unprivileged connections unless you are performing administrative tasks.

## 2. Install and configure Entrust KeyControl

- [Deploy an Entrust KeyControl cluster](#)
- [Create an Entrust KeyControl Management Vault](#)

### 2.1. Deploy an Entrust KeyControl cluster

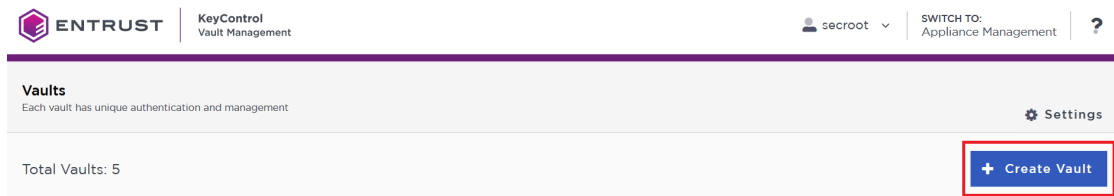
For this integration, Entrust KeyControl was deployed as a two-node cluster on premises. The installation software was downloaded in the form of an OVA file, deployed in VMware ESXi.

Follow the installation and set-up instructions in [KeyControl Installation and Upgrade Guide](#). If using an HSM, the integration guide with the Entrust nShield HSM is available at <https://www.entrust.com/documentation>. Search for the key phrase **KeyControl nShield HSM**.

### 2.2. Create an Entrust KeyControl Management Vault

To create an Entrust KeyControl Management Vault:

1. Sign in to the Entrust KeyControl Appliance Manager.
2. In the home page, select **Create Vault**.



3. Select **Create Vault**.

The **Create Vault** dialog appears.

4. In the **Type** drop-down box, select **Cloud Key Management**. Enter the required information.
5. Select **Create Vault**.

For example:

**Type**  
Choose the type of vault to create

Cloud Key Management

**Name\***

GCP-BYOK-KeyControl

**Description**

Google Cloud Platform BYOK KeyControl CSP account

Max. 300 characters

**Administration**  
Invite an individual to have complete access and control over this vault. They will be responsible for inviting additional members.

**Admin Name\***

Administrator

**Admin Email\***

[Redacted]

Create Vault Cancel

- When you receive an email with a URL and sign-in credentials to the Entrust KeyControl vault, bookmark the URL and save the credentials.

For example:



**Administrator, you have been invited to become an administrator of the Cloud Key Management vault, GCP-BYOK-KeyControl.**

To sign in, use the following:

URL: [https://\[Redacted\]/cloudkeys/\[Redacted\]/GCP-BYOK-KeyControl/](https://[Redacted]/cloudkeys/[Redacted]/GCP-BYOK-KeyControl/)

User Name: [Redacted]

Password: [Redacted]

- Sign in to the URL provided in the email. Change the initial password when prompted.

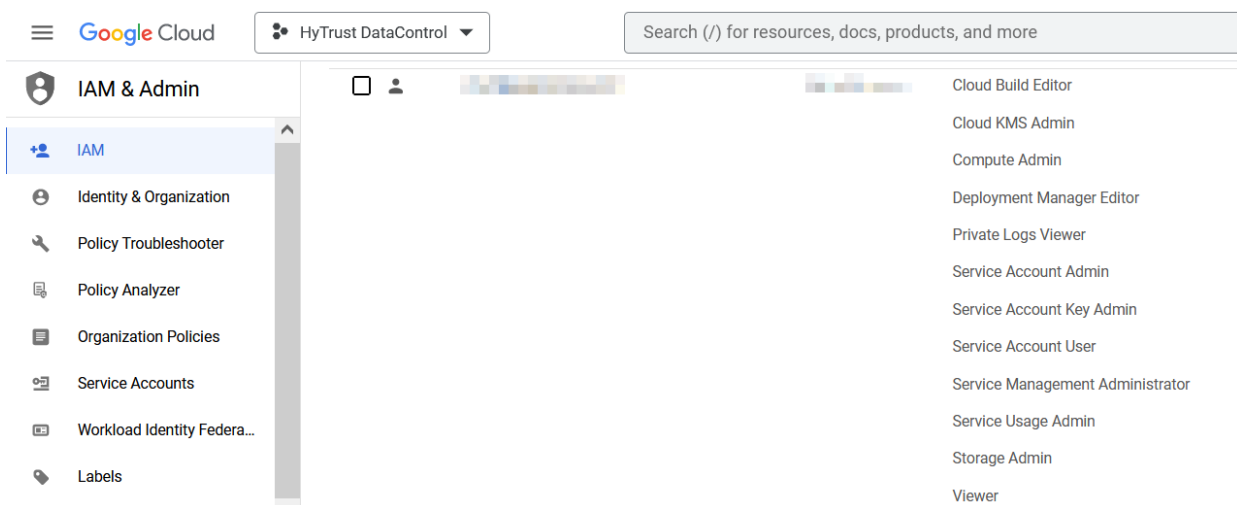
# 3. Configure Google Cloud Platform

- [Required GCP permissions](#)
- [Create a service account in GCP](#)
- [Create a key for the service account](#)
- [Create a GCP key ring](#)

## 3.1. Required GCP permissions

The GCP account performing this integration had the following permissions. These were granted by the project admin. Not all these permissions are required to perform this integration.

- Cloud Build Editor
- Cloud KMS Admin
- Compute Admin
- Deployment Manager Editor
- Private Logs Viewer
- Service Account Admin
- Service Account Key Admin
- Service Account User
- Service Management Administrator
- Service Usage Admin
- Storage Admin
- Viewer



## 3.2. Create a service account in GCP

A service account needs to be created in a GCP IAM. This service account will be used by Entrust KeyControl to access the GCP key rings. Once created, this service account needs permissions that have to be granted by the project admin.

1. Open a browser and sign in to the GCP portal <https://console.cloud.google.com>.
2. Select **IAM & Admin** on the Welcome screen, or navigate to **Cloud overview > Dashboard**.
3. Select **Service Accounts** in the left-hand pane, or enter **IAM & Admin** in the **Search** box and then select **IAM & Admin** from the pull-down menu that appears.
4. Select **CREATE SERVICE ACCOUNT** in the right-hand pane.
5. Enter the **Service account details** and then select **DONE**.

For example:

The screenshot shows the Google Cloud IAM & Admin console. The left-hand navigation pane is open to 'Service Accounts'. The main content area displays the 'Create service account' wizard. Step 1, 'Service account details', is active. It includes the following fields and options:

- Service account name:** gcp-byok-entrust-kc (Display name for this service account)
- Service account ID \*:** gcp-byok-entrust-kc (with clear and refresh icons)
- Email address:** gcp-byok-entrust-kc@htdc-project.iam.gserviceaccount.com (with copy icon)
- Service account description:** Entrust KeyControl KMIP for GCP KeyRings (with a blue border around the text)

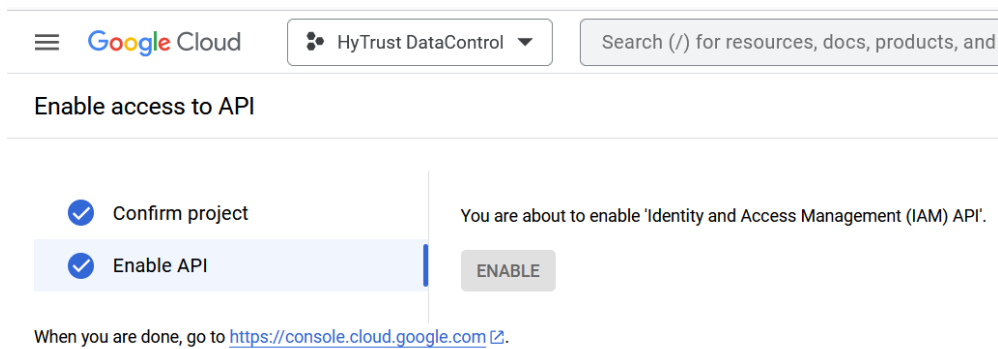
Below the description field is a 'CREATE AND CONTINUE' button. Step 2, 'Grant this service account access to project (optional)', and Step 3, 'Grant users access to this service account (optional)', are visible but not active. At the bottom, there are 'DONE' and 'CANCEL' buttons.



Youself or the project administrator may need to enable access to APIs. Once enabled, the screen appears as follows.

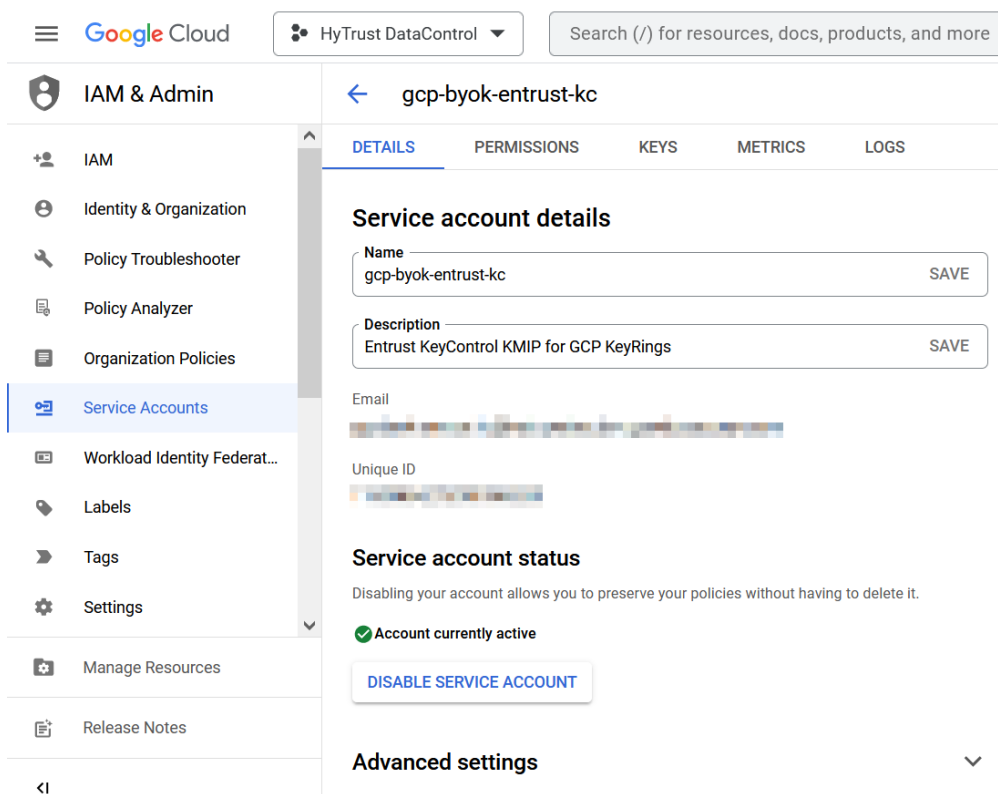
For example:





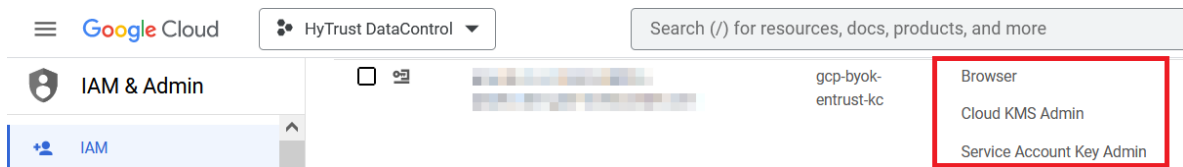
6. Select **Service Accounts** > **Service accounts** and then select the service account you just created.
7. Select the **DETAILS** tab. Take note of the **Unique ID**.

For example:



8. The following permissions were given to this service account by the system admin after it was created:
  - Browser
  - Cloud KMS Admin
  - Service Account Key Admin

For example:



### 3.3. Create a key for the service account

A key needs to be created for the service account created in [Create a service account in GCP](#). This key will be used by Entrust KeyControl to access the GCP service account.

1. Open a browser and sign in to the GCP portal: <https://console.cloud.google.com>.
2. Select **IAM & Admin** on the Welcome screen, or navigate to **Cloud overview > Dashboard**.
3. Select **Service Accounts** in the left-hand pane, or type **IAM & Admin** in the **Search** box and then select **IAM & Admin** from the pull-down menu that appears.
4. Select the service account created in [Create a service account in GCP](#) from the list in the right-hand pane.
5. Select the **KEYS** tab.
6. Select **ADD KEY** and then select **Create new key**.
7. Select **JSON** from the available **Key type** options.

For example:

#### Create private key for "gcp-byok-entrust-kc"

Downloads a file that contains the private key. Store the file securely because this key can't be recovered if lost.

##### Key type

JSON  
Recommended

P12  
For backward compatibility with code using the P12 format

**CANCEL** **CREATE**

8. Select **CREATE**. A pop-up message appears indicating that the key created was downloaded to your computer.

For example:

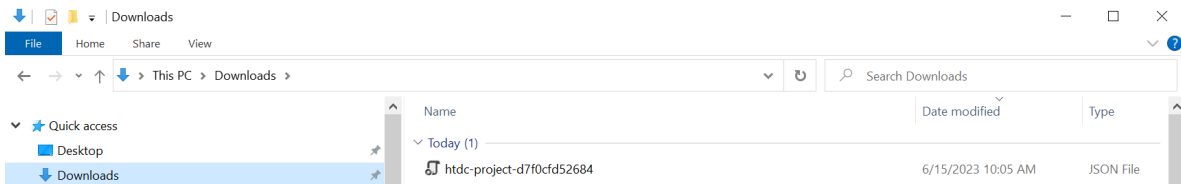
## Private key saved to your computer

htdc-project-d7f0cfd52684.json allows access to your cloud resources, so store it securely. [Learn more best practices](#)

CLOSE

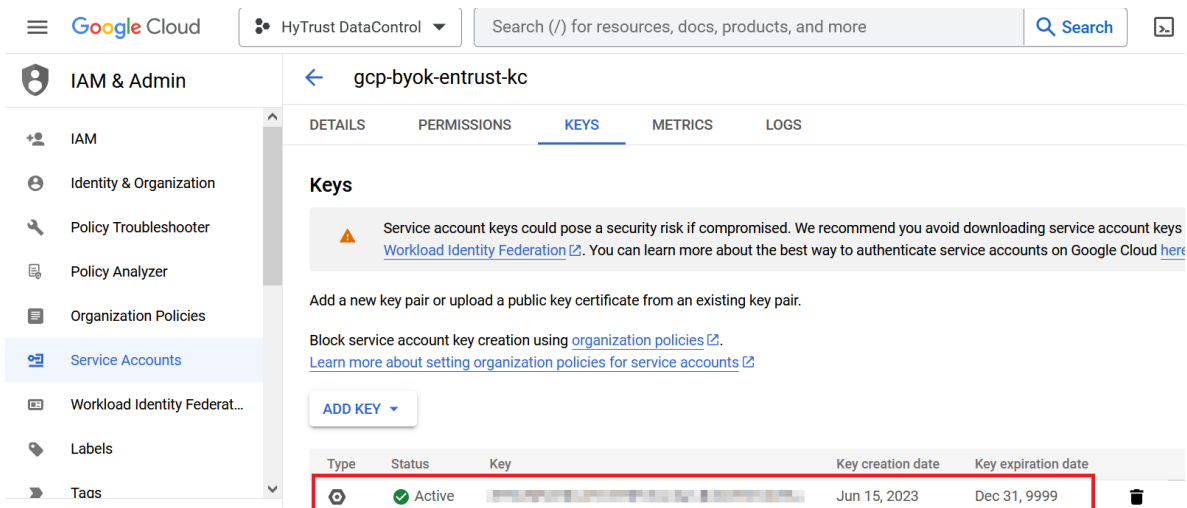
9. Verify by checking your **Downloads** folder.

For example:



10. Take note of the new key in the GCP console.

For example:



## 3.4. Create a GCP key ring

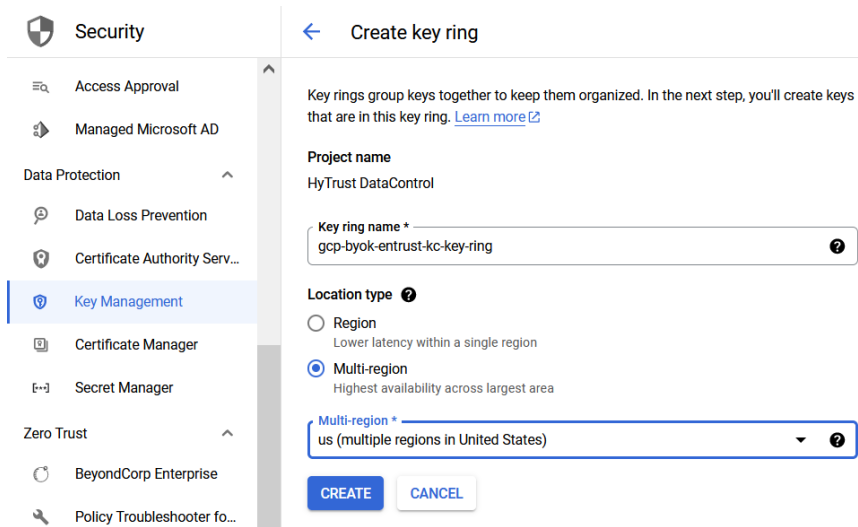
This key ring will be used to store keys managed by Entrust KeyControl. A new GCP key ring was created for this integration to show the entire process. You can use an existing key ring instead.

If using an existing GCP key ring, proceed to section [Create an Entrust KeyControl CSP account for the GCP service account](#) directly, skipping this section entirely.

1. Open a browser and sign in to the GCP portal: <https://console.cloud.google.com>.
2. In the navigation menu select **Security > Key Management**.

3. In the **KEY RINGS** tab in the left-hand pane, select **+ CREATE KEY RING**.
4. Enter the **Key ring name** and select the **Location type**.

For example:



5. Select **CREATE** to create the key ring
6. Select **CANCEL** in the **Create key** pane.
7. Verify your key ring has the following inherited permissions. Navigate to **Security** > **Key Management**. Select the newly created key ring. The permissions are in the right-hand pane.

For example:

## gcp-byok-entrust-kc-key-ring







Edit or delete permissions below, or select "Add Principal" to grant new access.

 + ADD PRINCIPAL

Show inherited permissions

 Filter Enter property name or value



Role / Principal 	Inheritance
 Cloud KMS Admin (17)	
 Cloud KMS Crypto Operator (1)	
 Editor (7)	
 Owner (1)	
 Viewer (14)	

## 4. Configure Entrust KeyControl as GCP KMS

- [Create an Entrust KeyControl CSP account for the GCP service account](#)
- [Verify the connection between Entrust KeyControl and GCP](#)

### 4.1. Create an Entrust KeyControl CSP account for the GCP service account

The following steps establish the connection between Entrust KeyControl and GCP, making Entrust KeyControl the CSP of the GCP service account.

1. Sign in to the Entrust KeyControl Vault URL bookmark from [Create an Entrust KeyControl Management Vault](#).
2. Select the **CLOUDKEYS** icon on the toolbar.
3. Select the **CSP Accounts** tab.
4. Select the **Action** icon and then **Add CSP Account** from the drop-down menu that appears.

The **Add CSP Account** dialog appears.

5. In the **Details** tab, enter the **Name** and **Description**.
6. From the **Admin Group** drop-down menu box, select **Cloud Admin Group**.
7. From the **Type** drop-down menu box, select **GCP**.
8. In the **Service Account Key File (.json)** field, select the file download to your computer in [Create a key for the service account](#).

For example:

Add CSP Account ✕

[Details](#) [Schedule](#)

Name \*

GCP-BYOK-CSP-Account

Description

Google Cloud Platform (GCP) Bring Your Own (BYOK) Key CSP account.

Admin Group \*

Cloud Admin Group

Type \*

GCP

Service Account Key File(.json) \*

htdc-project-d7f0cfd52684.json Clear Preview

Cancel Continue

9. Select **Continue**.
10. In the **Schedule** tab, select **Never**.

For example:

Add CSP Account ✕

[Details](#) [Schedule](#)

Define a schedule for which service account keys are rotated.

Rotation Schedule \*

Never  Define Schedule

Cancel Apply

11. Select **Apply**.

The new CSP account is created.

The screenshot shows the Entrust KeyControl interface. At the top, there is a navigation bar with the Entrust logo and 'KeyControl Vault for Cloud Key Management'. Below this, there are tabs for 'Key Sets', 'CloudKeys', and 'CSP Accounts'. A table lists the CSP Accounts with columns for Name, Description, Admin Group, and Key Set. A green success message box is overlaid on the table, stating 'Success CSP Account created successfully'.

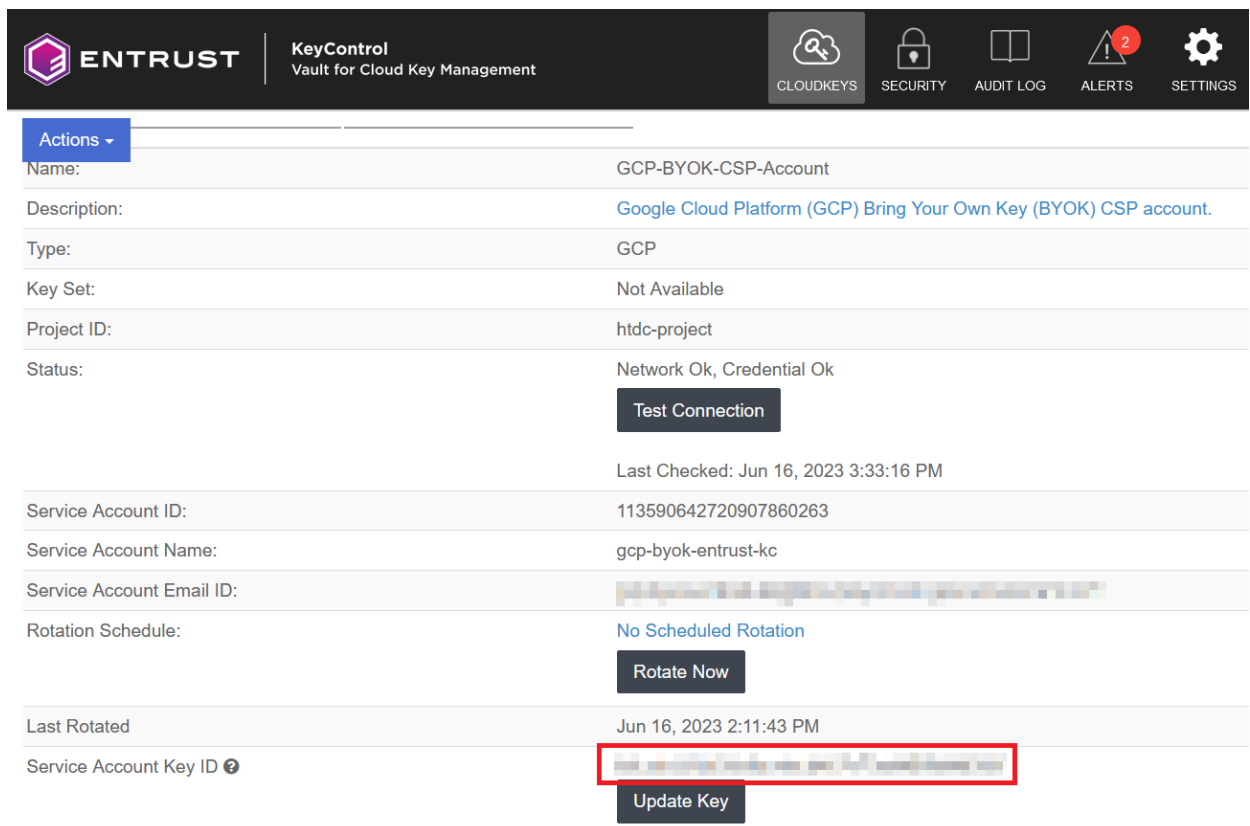
CSP Account Name	Description	Admin Group	Key Set
GCP-BYOK-CSP-Account	Google Cloud Platform (GCP) Brin...	Cloud Admin Group	GCP

## 4.2. Verify the connection between Entrust KeyControl and GCP

The key created in [Create a key for the service account](#) was rotated automatically after the CSP account was created. The key in the downloaded file is no longer valid. Verify the new key as follows.

1. Select the newly created CSP account in [Create an Entrust KeyControl CSP account for the GCP service account](#).
2. Scroll down until you see **Service Account Key ID**. Note the value.

For example:



The screenshot shows the Entrust KeyControl interface for a GCP-BYOK-CSP-Account. The account details are as follows:

Name:	GCP-BYOK-CSP-Account
Description:	Google Cloud Platform (GCP) Bring Your Own Key (BYOK) CSP account.
Type:	GCP
Key Set:	Not Available
Project ID:	htdc-project
Status:	Network Ok, Credential Ok <a href="#">Test Connection</a>
	Last Checked: Jun 16, 2023 3:33:16 PM
Service Account ID:	113590642720907860263
Service Account Name:	gcp-byok-entrust-kc
Service Account Email ID:	[Redacted]
Rotation Schedule:	No Scheduled Rotation <a href="#">Rotate Now</a>
Last Rotated	Jun 16, 2023 2:11:43 PM
Service Account Key ID	[Redacted] <a href="#">Update Key</a>

3. Open a browser and sign in to the GCP portal <https://console.cloud.google.com>.
4. Select **IAM & Admin** on the Welcome screen.
5. Select **Service Accounts** in the left-hand pane.
6. Select your service account and then select the **KEYS** tab.
7. Check that the key is the same as the **Service Account Key ID** in Entrust KeyControl.

For example:



IAM & Admin

gcp-byok-entrust-kc

- IAM
- Identity & Organization
- Policy Troubleshooter
- Policy Analyzer
- Organization Policies
- Service Accounts**
- Workload Identity Federa...
- Labels
- Tags

DETAILS PERMISSIONS **KEYS** METRICS LOGS

Keys

Service account keys could pose a security risk if compromised. We recommend you avoid downloading service account keys about the best way to authenticate service accounts on Google Cloud [here](#).

Add a new key pair or upload a public key certificate from an existing key pair.

Block service account key creation using [organization policies](#).  
[Learn more about setting organization policies for service accounts](#)

ADD KEY

Type	Status	Key	Key creation date	Key expiration date	
	Active		Jun 16, 2023	Dec 31, 9999	

## 5. Test integration

- [Create a key set in Entrust KeyControl](#)
- [Create a cloud key in Entrust KeyControl](#)
- [Import a GCP cloud key into Entrust KeyControl](#)
- [Rotate a cloud key in Entrust KeyControl](#)
- [Remove a cloud key in Entrust KeyControl](#)
- [Upload a removed Entrust KeyControl key back to GCP](#)
- [Delete a cloud key in Entrust KeyControl](#)
- [Cancel a cloud key deletion in Entrust KeyControl](#)

### 5.1. Create a key set in Entrust KeyControl

This key set will be used to create a cloud key in Entrust KeyControl.

1. Sign in to the Entrust KeyControl Vault URL bookmark in [Create an Entrust KeyControl Management Vault](#).
2. Select the **CLOUDKEYS** icon on the toolbar.
3. Select the **Key Sets** tab.
4. Select **Actions > Create Key Set**.

The **Choose the type of keys...** dialog appears.

5. Choose **GCP Key**.

The **Create Key Set** dialog appears.

6. In the **Details** tab, enter a **Name** and **Description**.
7. From the **Admin Group** menu, select **Cloud Admin Group**.

For example:

Create Key Set ✕

Details CSP Account HSM Schedule

Name \*

Description

Admin Group \*

8. Select **Continue**.
9. In the **CSP Account** tab, select the CSP account created in [Create an Entrust KeyControl CSP account for the GCP service account](#).

For example:

Create Key Set ✕

Details CSP Account HSM Schedule

CSP Account \*  
 Choose an existing CSP Account or add a new one to use with this Key Set.

[+ Add CSP Account](#)

10. Select **Continue**.
11. In the **HSM** tab, select **Enable HSM** if using one. The HSM must be configured prior to this step.

For example:

Create Key Set ✕

Details CSP Account HSM Schedule

**Enable HSM**  
 If checked, the HSM linked to KeyControl will be used for generating cryptographic material for Cloudkeys in this Key Set.

12. Select **Continue**.
13. In the **Schedule** tab, select a **Rotation Schedule**.

For example:

**Create Key Set** X

Details   CSP Account   HSM   Schedule

Default CloudKey rotation schedule presented during CloudKey creation.

Rotation Schedule \*

Other v

Every  days (max limit is 1096 days)

14. Select **Apply**.

The key set is added.

For example:

Key Set Name	Description	Admin Group	Type	Keys
GCP-BYOK-Key-Set	Google Cloud Platform (GCP) Bring Yo...	Cloud Admin Group	GCP	0

15. Verify the GCP key ring created in [Create a GCP key ring](#) is listed in the **Key Rings** tab. Select **Sync Now** on the right of the display to update the **Key Ring** list.

For example:

Name	Location	Key Ring ID	Tags
gcp-byok-entrust-kc-key-ring	us	us-gcp-byok-entrust-kc-key-ring	

For additional information, see [Creating a Key Set](#).

## 5.2. Create a cloud key in Entrust KeyControl

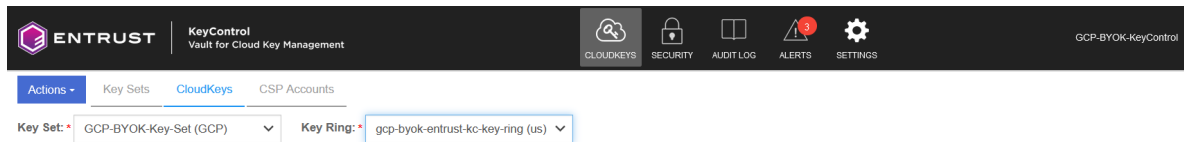
The following steps create a cloud key in Entrust KeyControl and verify it is available in GCP key ring:

1. Sign in to the Entrust KeyControl Vault URL bookmark from [Create an Entrust](#)

## KeyControl Management Vault.

2. Select the **CLOUDKEYS** icon on the toolbar.
3. Select the **CloudKeys** tab.
4. In the **Key Set** menu, select the **Key Set** created in [Create a key set in Entrust KeyControl](#).
5. In the **Key Ring** menu, select the key ring created in [Create a GCP key ring](#).

For example:

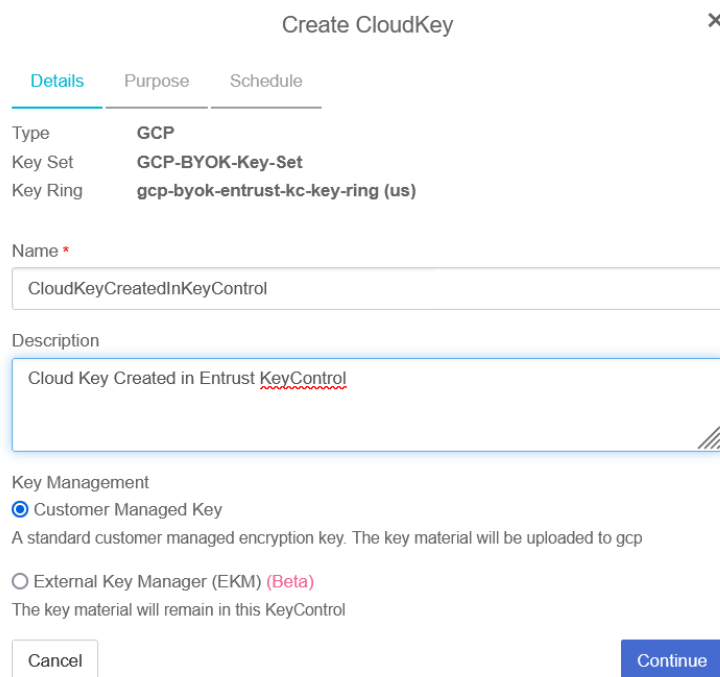


6. Select **Actions > Create CloudKey**.

The **Create CloudKey** dialog appears.

7. In the **Details** tab, enter a **Name** and **Description**.
8. Select **Customer Managed Key** from the list of **Key Management** options.

For example:

A screenshot of the 'Create CloudKey' dialog box. The dialog has a title bar 'Create CloudKey' and a close button 'X'. There are three tabs: 'Details', 'Purpose', and 'Schedule'. The 'Details' tab is active. Below the tabs, there are three rows of information: 'Type' with value 'GCP', 'Key Set' with value 'GCP-BYOK-Key-Set', and 'Key Ring' with value 'gcp-byok-entrust-kc-key-ring (us)'. Below this is a 'Name \*' field with the text 'CloudKeyCreatedInKeyControl'. Underneath is a 'Description' field with the text 'Cloud Key Created in Entrust KeyControl'. Below the description field is the 'Key Management' section with two radio button options: 'Customer Managed Key' (which is selected) and 'External Key Manager (EKM) (Beta)'. Below the radio buttons are two buttons: 'Cancel' and 'Continue'.

9. Select **Continue**.
10. If you are using the hardware protection method, in the **Purpose** tab, select **HSM** from the **Protection Level** options.
11. From the **Purpose** and **Algorithm** pull down menus, select the appropriate options for your application.

For example:

Create CloudKey

Details Purpose Schedule

Protection Level \*

Software

HSM

Choosing a purpose will determine the key type and algorithm selection

Purpose \*

Symmetric encrypt/decrypt

Algorithm \*

Google symmetric key

Cancel Continue

12. In the **Schedule** tab, select the **Rotation Schedule** and **Expiration**.

For example:

Create CloudKey

Details Purpose Schedule

Rotation Schedule \*

Define a schedule for which the CloudKey will be rotated.

Inherit from keyset (Once 180 days)

Expiration \*

Define when the CloudKey should be expired.

Never  Choose a date

Cancel Apply

13. Select **Apply**.

The cloud key is created.

CloudKey Name	Description	Expires	Cloud Status
CloudKeyCreatedInKeyControl	Cloud Key Created in Entrust KeyControl	Never	AVAILABLE

14. Verify the cloud key created in Entrust KeyControl is **Available** in the GCP key ring.

Google Cloud HyTrust DataControl Search (/) for resources, docs, products, and more

Security Key ring details + CREATE KEY + CREATE IMPORT JOB

Security Command Center

KEYS IMPORT JOBS

### Keys for "gcp-byok-entrust-kc-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

<input type="checkbox"/>	Name ↑	Status ?	Protection level ?
<input type="checkbox"/>	<a href="#">CloudKeyCreatedInKeyControl</a>	✓ Available	Software

For additional information, see [Creating a CloudKey](#).

## 5.3. Import a GCP cloud key into Entrust KeyControl

The following steps document how to import an existing cloud key from GCP to Entrust KeyControl.



It is recommended that all cloud keys be created in Entrust KeyControl, and never directly in GCP.

1. Open a browser and sign in to the GCP portal <https://console.cloud.google.com>.
2. In the navigation menu select **Security > Key Management**.
3. In the **KEY RINGS** tap in the left-hand pane, select the key ring created in [Create a GCP key ring](#).
4. The existing cloud key in GCP to be imported into Entrust KeyControl is enclosed in the red box.

For example:

Google Cloud HyTrust DataControl Search (/) for resources, docs, products, and more Search

Security Key ring details + CREATE KEY + CREATE IMPORT JOB REFRESH SHOW INFO PANEL

Security Command Center

KEYS IMPORT JOBS

### Keys for "gcp-byok-entrust-kc-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

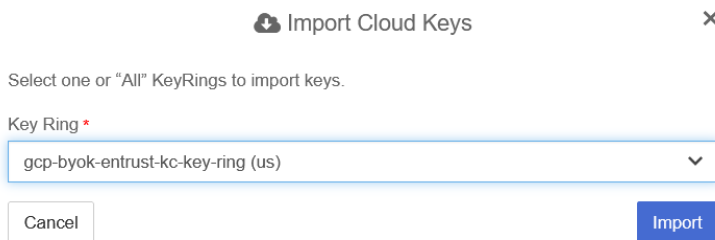
<input type="checkbox"/>	Name ↑	Status ?	Protection level ?	Purpose ?	Next rotation ?	Actions
<input type="checkbox"/>	<a href="#">CloudKeyCreatedInGCP</a>	✓ Available	Software	Symmetric encrypt/decrypt	Sep 19, 2023	⋮
<input type="checkbox"/>	<a href="#">CloudKeyCreatedInKeyControl</a>	✓ Available	Software	Symmetric encrypt/decrypt	Not applicable	⋮

5. Sign in to the Entrust KeyControl Vault URL bookmark from [Create an Entrust KeyControl Management Vault](#).
6. Select the **CLOUDKEYS** icon on the toolbar.
7. Select the **Key Sets** tab.
8. Select the key set created in [Create a key set in Entrust KeyControl](#).
9. Select **Actions > Import CloudKey**.

The **Import Cloud Keys** dialog appears.

10. From the **Key Ring** pull-down menu, select the GCP key ring created in [Create a GCP key ring](#).

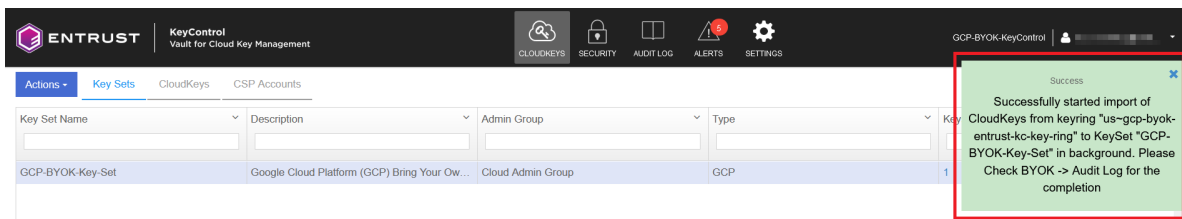
For example:



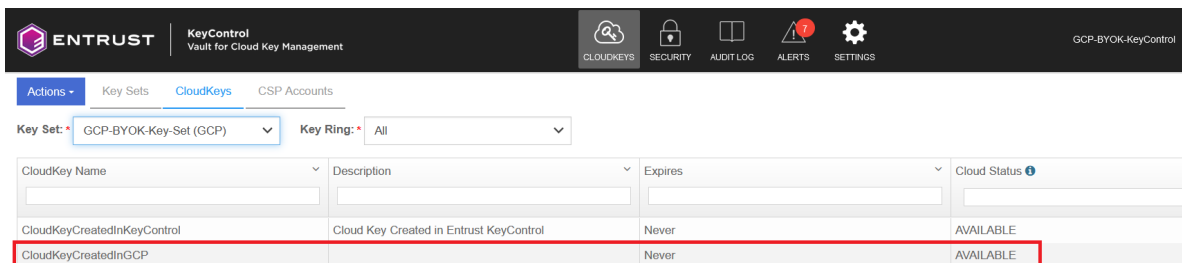
11. Select **Import**.

The key is imported.

For example:



12. Verify that the GCP cloud key is **AVAILABLE** in Entrust KeyControl.



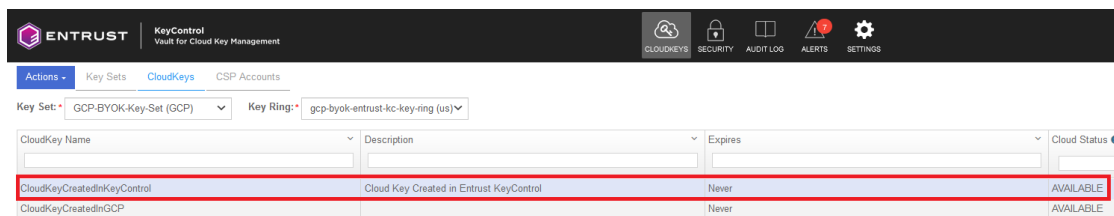


## 5.4. Rotate a cloud key in Entrust KeyControl

To rotate a cloud key in Entrust KeyControl:

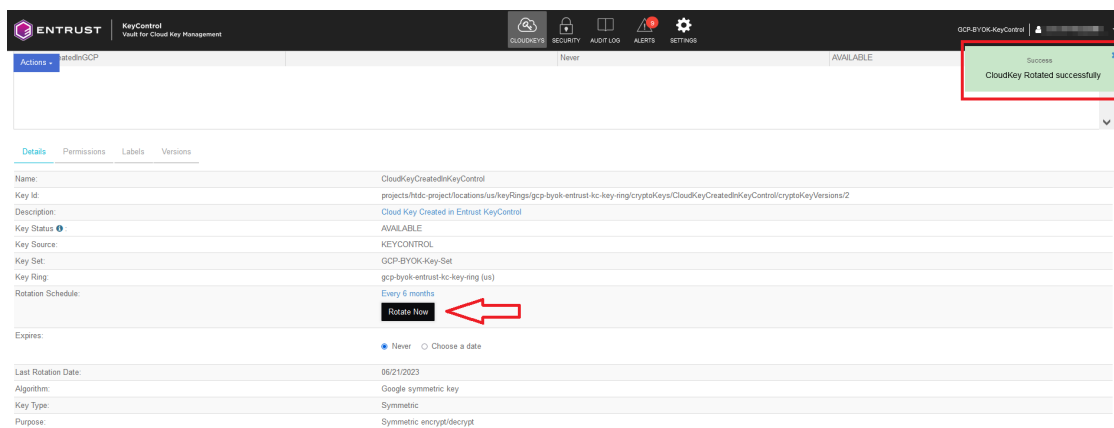
1. Sign in to the Entrust KeyControl Vault URL bookmark from [Create an Entrust KeyControl Management Vault](#).
2. Select the **CLOUDKEYS** icon on the toolbar.
3. Select the **CloudKeys** tab.
4. From the **Key Set** menu, select the **Key Set** created in [Create a key set in Entrust KeyControl](#).
5. From the **Key Ring** menu, select the key ring created in [Create a GCP key ring](#).
6. Select the key to rotate.

For example:



7. Select **Rotate Now**. You might need to scroll down the page to view this button.

For example:



8. In GCP, navigate to **Security > Key Management**.
9. In the **KEY RINGS** tab in the left-hand pane, select the key ring created in [Create a GCP key ring](#).
10. Select the key you just rotated in Entrust KeyControl.
11. Verify that the key has been rotated in GCP in synchronization with Entrust KeyControl.

For example:

Google Cloud | HyTrust DataControl | Search (/) for resources, docs, products, and more

Security | Key: "CloudKe..." | ROTATE KEY | EDIT ROTATION PERIOD | IMPORT KEY VERSION

A key contains versions which have key material associated with the key. A key must have at least one key version to operate on data. [Learn more](#)

Status: ✔ Available | Location: us | Protection level: Software | Purpose: Symmetric encrypt/decrypt

OVERVIEW | **VERSIONS** | USAGE TRACKING | PERMISSIONS

Versions | ENABLE | DISABLE | RESTORE | DESTROY

Filter Enter property name or value

<input type="checkbox"/>	Version	State	Algorithm	Created on	Created from	Actions
<input type="checkbox"/>	2	Enabled & primary	Google symmetric key	6/21/23, 4:50 PM	Import job	⋮
<input type="checkbox"/>	1	Enabled	Google symmetric key	6/21/23, 2:01 PM	Import job	⋮

## 5.5. Remove a cloud key in Entrust KeyControl

A removed cloud key in Entrust KeyControl will no longer be available for use in GCP. However, Entrust KeyControl will keep a copy of the removed cloud key, which can be reloaded back to GCP for use.

1. Sign in to the Entrust KeyControl Vault URL bookmark from [Create an Entrust KeyControl Management Vault](#).
2. Select the **CLOUDKEYS** icon on the toolbar.
3. Select the **CloudKeys** tab.
4. In the **Key Set** menu, select the **Key Set** created in [Create a key set in Entrust KeyControl](#).
5. In the **Key Ring** menu, select the key ring created in [Create a GCP key ring](#).
6. Select the key to the removed.
7. Select **Actions > Remove from Cloud**.

The **Remove from Cloud** dialog appears.

8. Type the name of the cloud key in **Type CloudKey Name**.

For example:

Remove from Cloud ✕

**⚠** Removing the key from the cloud will remove the key material from the KMS. An application will no longer be able to use this key from the cloud.

Appliance Management will keep a copy of the key. This copy can always be uploaded back to the cloud.

Are you sure you want to remove the following CloudKey from the cloud?

CloudKey **CloudKeyCreatedInKeyControl**

KeyId **projects/htdc-project/locations/us/keyRings/gcp-byok-entrust-kc-key-ring/cryptoKeys/CloudKeyCreatedInKeyControl/cryptoKeyVersions/2**

Type CloudKey Name \*

9. Select **Remove**.
10. Verify the status change in Entrust KeyControl.

For example:

The screenshot shows the Entrust KeyControl interface. A green notification box in the top right corner states: "Success CloudKey removed from cloud Successfully". Below this, a table lists CloudKeys. The row for "CloudKeyCreatedInKeyControl" is highlighted with a red box, and its "Cloud Status" is "NOT AVAILABLE". The row for "CloudKeyCreatedInGCP" is also visible with a status of "AVAILABLE".

CloudKey Name	Description	Expires	Cloud Status
CloudKeyCreatedInKeyControl	Cloud Key Created in Entrust KeyControl	Never	NOT AVAILABLE
CloudKeyCreatedInGCP		Never	AVAILABLE

11. Verify the key is now **Not available** in GCP.

For example:

The screenshot shows the Google Cloud console interface for the "gcp-byok-entrust-kc-key-ring" key ring. A table lists the keys within this ring. The row for "CloudKeyCreatedInKeyControl" is highlighted with a red box, and its "Status" is "Not available". The row for "CloudKeyCreatedInGCP" is also visible with a status of "Available".

Name	Status	Protection level	Purpose	Next rotation	Actions
CloudKeyCreatedInGCP	Available	Software	Symmetric encrypt/decrypt	Sep 19, 2023	⋮
CloudKeyCreatedInKeyControl	Not available	Software	Symmetric encrypt/decrypt	Not applicable	⋮

For additional information, see [Removing a CloudKey from the Cloud](#).

## 5.6. Upload a removed Entrust KeyControl key back to GCP

Follow these steps to upload back to GCP the Entrust KeyControl key removed in [Remove a cloud key in Entrust KeyControl](#).

1. Sign in to the Entrust KeyControl Vault URL bookmark from [Create an Entrust KeyControl Management Vault](#).
2. Select the **CLOUDKEYS** icon on the toolbar.
3. Select the **CloudKeys** tab.
4. From the **Key Set** menu, select the **Key Set** created in [Create a key set in Entrust KeyControl](#).
5. From the **Key Ring** menu, select the key ring created in [Create a GCP key ring](#).
6. Select the key to be uploaded.
7. Select **Actions > Upload to Cloud**.

The **Upload to CloudKey** dialog appears.

For example:

Upload to CloudKey ✕

Once the key is Uploaded to the cloud it will be available for applications to use.

CloudKey	<b>CloudKeyCreatedInKeyControl</b>
KeyId	<b>projects/htdc-project/locations/us/keyRings/gcp-byok-entrust-kc-key-ring/cryptoKeys/CloudKeyCreatedInKeyControl/cryptoKeyVersions/2</b>
Keyring	<b>gcp-byok-entrust-kc-key-ring(us)</b>

CancelUpload

8. Select **Upload**.
9. Verify the status change in Entrust KeyControl.

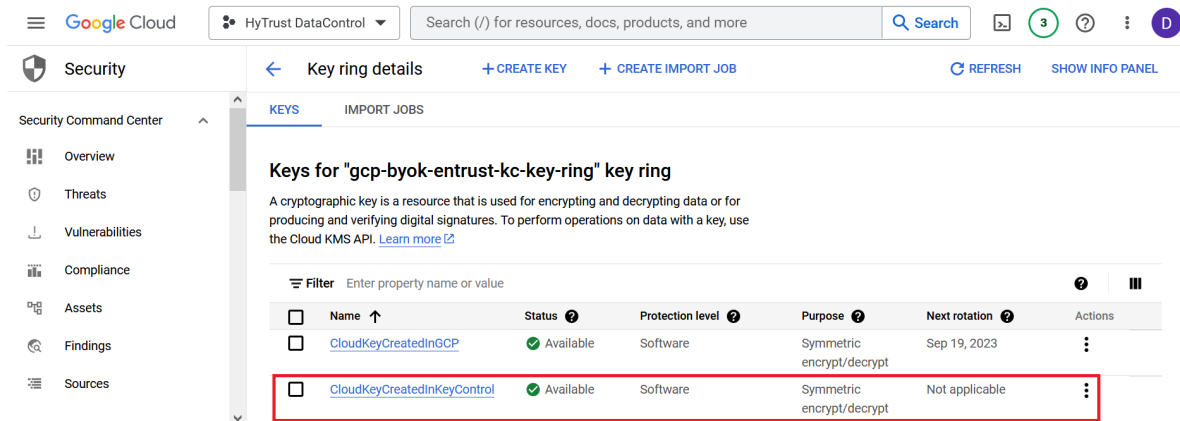
For example:

The screenshot shows the Entrust KeyControl interface. A green notification box in the top right corner displays "Success" and "CloudKey Uploaded Successfully". Below the notification, a table lists cloud keys. The first row is highlighted with a red border, showing the key name "CloudKeyCreatedInKeyControl", description "Cloud Key Created in Entrust KeyControl", expiration "Never", and status "AVAILABLE".

CloudKey Name	Description	Expires	Cloud Status
CloudKeyCreatedInKeyControl	Cloud Key Created in Entrust KeyControl	Never	AVAILABLE
CloudKeyCreatedInGCP		Never	AVAILABLE

10. Verify the key is now **Available** in GCP.

For example:



## 5.7. Delete a cloud key in Entrust KeyControl

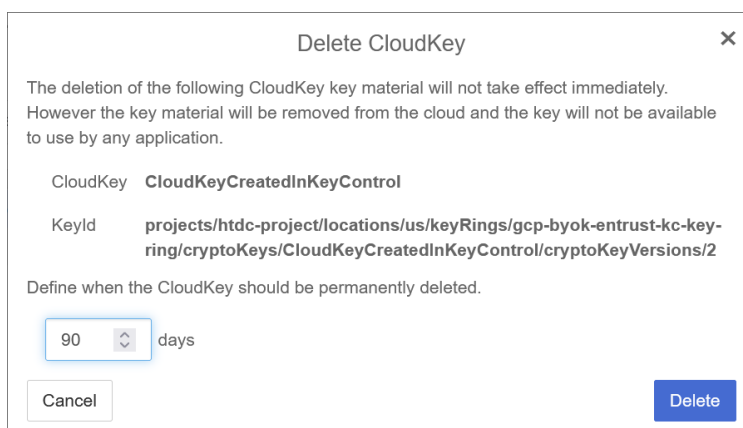
The deletion of a cloud key does not take effect immediately. However, after a user-defined interval, the key will be permanently removed.

1. Sign in to the Entrust KeyControl Vault URL bookmark from [Create an Entrust KeyControl Management Vault](#).
2. Select the **CLOUDKEYS** icon on the toolbar.
3. Select the **CloudKeys** tab.
4. From the **Key Set** menu, select the **Key Set** created in [Create a key set in Entrust KeyControl](#).
5. From the **Key Ring** menu, select the key ring created in [Create a GCP key ring](#).
6. Select the key to delete.
7. Select **Actions > Delete CloudKey**.

The **Delete CloudKey** dialog appears.

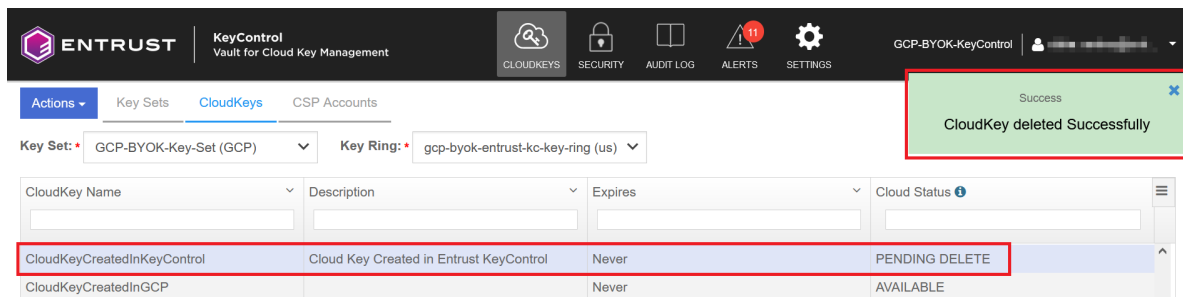
8. Select a time in **Define when the CloudKey should be permanently deleted**.

For example:



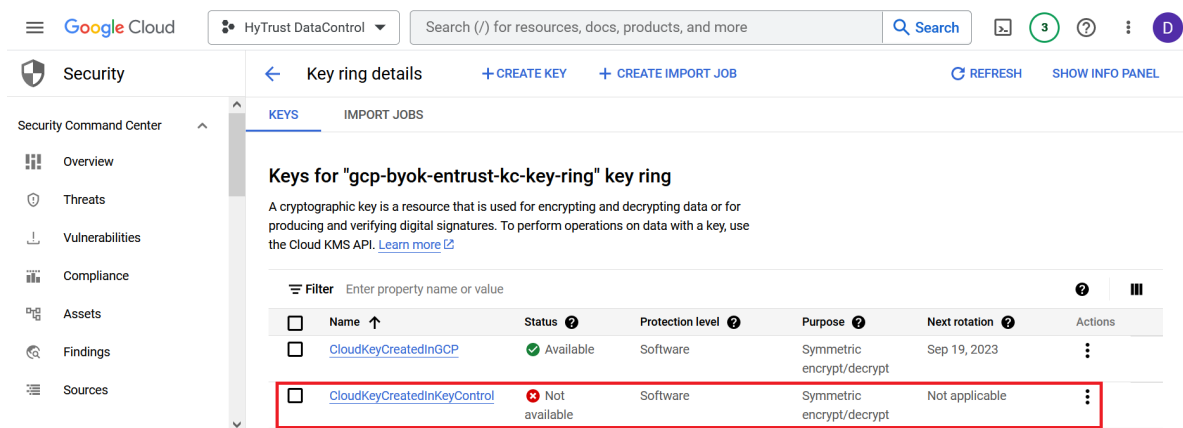
9. Select **Delete**.
10. Verify the status change in Entrust KeyControl.

For example:



11. Verify the key is now **Not available** in GCP.

For example:



A permanently removed key continues to appear in both GCP and Entrust KeyControl. Its status is set to *"Destroyed"* by GCP. Neither the key nor its name can ever be used again.

For additional information, see [Deleting a CloudKey](#).

## 5.8. Cancel a cloud key deletion in Entrust KeyControl

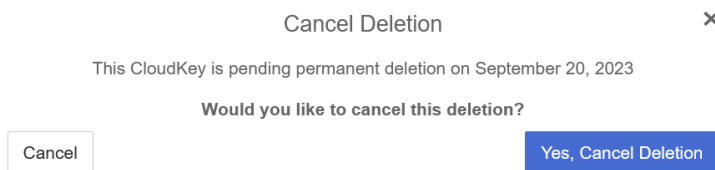
The deletion of a key can be canceled while the time in the **Define when the CloudKey should be permanently deleted** setting has not expired. Follow these steps to upload back to GCP the Entrust KeyControl key deleted in [Delete a cloud key in Entrust KeyControl](#).

1. Sign in to the Entrust KeyControl Vault URL bookmark from [Create an Entrust KeyControl Management Vault](#).
2. Select the **CLOUDKEYS** icon on the toolbar.

3. Select the **CloudKeys** tab.
4. In the **Key Set** menu, select the **Key Set** created in [Create a key set in Entrust KeyControl](#).
5. In the **Key Ring** menu, select the key ring created in [Create a GCP key ring](#).
6. Select the key deletion to be canceled.
7. Select **Actions > Cancel Deletion**.

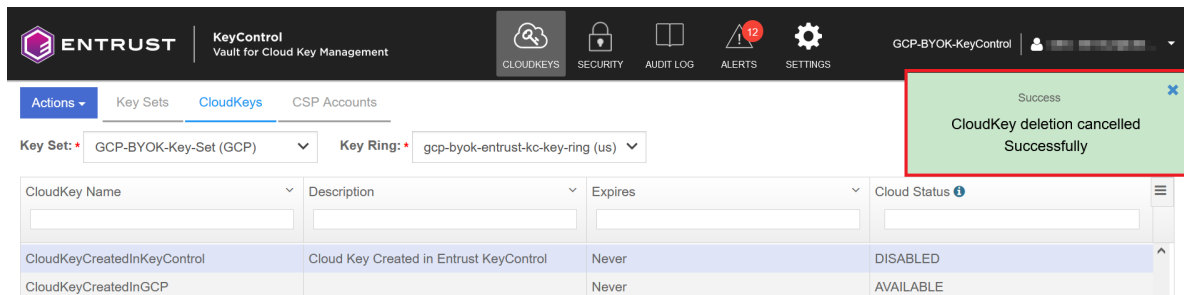
The **Cancel Deletion** dialog box appears.

For example:



8. Select **Yes, Cancel Deletion**.
9. Verify the status change in Entrust KeyControl.

For example:



10. Select **Actions > Enable CloudKey**.

The **Enable CloudKey** dialog box appears.

For example:



11. Select **Enable**.
12. Verify the status change in Entrust KeyControl.

For example:

The screenshot shows the Entrust KeyControl interface. At the top, there is a navigation bar with 'ENTRUST KeyControl Vault for Cloud Key Management' and various icons for CloudKeys, Security, Audit Log, Alerts, and Settings. Below this, there are tabs for 'Actions', 'Key Sets', 'CloudKeys', and 'CSP Accounts'. The 'CloudKeys' tab is active. A notification box in the top right corner says 'Success CloudKey Enabled Successfully'. Below the notification, there are dropdown menus for 'Key Set' (GCP-BYOK-Key-Set (GCP)) and 'Key Ring' (gcp-byok-entrust-kc-key-ring (us)). A table below shows the status of keys:

CloudKey Name	Description	Expires	Cloud Status
CloudKeyCreatedInKeyControl	Cloud Key Created in Entrust KeyControl	Never	AVAILABLE
CloudKeyCreatedInGCP		Never	AVAILABLE

13. Verify the key is now **Available** in GCP.

For example:

The screenshot shows the Google Cloud Security Command Center interface. The 'Security' section is active, and the 'Key ring details' page is displayed. The page title is 'Key ring details' and it includes buttons for '+ CREATE KEY' and '+ CREATE IMPORT JOB'. Below the title, there are tabs for 'KEYS' and 'IMPORT JOBS'. The main content area shows 'Keys for "gcp-byok-entrust-kc-key-ring" key ring'. A description explains that a cryptographic key is used for encrypting and decrypting data. Below the description, there is a table of keys:

Name	Status	Protection level	Purpose	Next rotation	Actions
CloudKeyCreatedInGCP	Available	Software	Symmetric encrypt/decrypt	Sep 19, 2023	
CloudKeyCreatedInKeyControl	Available	Software	Symmetric encrypt/decrypt	Not applicable	

For additional information, see [Canceling a CloudKey Deletion](#).