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

Integration Guide

2026-04-15

© Entrust Corporation. All rights reserved.

Table of Contents

1. Introduction . . . 1
    1.1. Documents to read first . . . 1
    1.2. Product configurations . . . 2
    1.3. Features tested . . . 2
    1.4. Requirements . . . 2
2. Install and configure Entrust KeyControl . . . 3
    2.1. Deploy an Entrust KeyControl cluster . . . 3
    2.2. Create an Entrust KeyControl Management Vault . . . 3
3. Configure Google Cloud Platform . . . 5
    3.1. Required GCP permissions . . . 5
    3.2. Create a service account in GCP . . . 6
    3.3. Create a key for the service account . . . 8
    3.4. Create a GCP key ring . . . 9
4. Configure Entrust KeyControl as GCP KMS . . . 12
    4.1. Create an Entrust KeyControl CSP account for the GCP service account . . . 12
    4.2. Verify the connection between Entrust KeyControl and GCP . . . 13
5. Test integration . . . 16
    5.1. Create a key set in Entrust KeyControl . . . 16
    5.2. Create a cloud key in Entrust KeyControl . . . 18
    5.3. Import a GCP cloud key into Entrust KeyControl . . . 21
    5.4. Rotate a cloud key in Entrust KeyControl . . . 22
    5.5. Remove a cloud key in Entrust KeyControl . . . 24
    5.6. Upload a removed Entrust KeyControl key back to GCP . . . 25
    5.7. Delete a cloud key in Entrust KeyControl . . . 27
    5.8. Cancel a cloud key deletion in Entrust KeyControl . . . 28
6. Additional resources and related products . . . 31
    6.1. nShield HSMs . . . 31
    6.2. nShield as a Service . . . 31
    6.3. KeyControl BYOK . . . 31
    6.4. Entrust products . . . 31
    6.5. nShield product documentation . . . 31

Chapter 1. Introduction

Entrust KeyControl has been rebranded as the Entrust Cryptographic Security Platform (CSP) Key Manager.

The Entrust CSP Key Manager continues to provide a comprehensive solution for discovering and managing the lifecycles of cryptographic keys, secrets, certificates, tokens, libraries, protocols, and configurations:

- The KeyControl Compliance Manager is now the Entrust CSP Compliance Manager. It still integrates with Entrust nShield Hardware Security Modules (HSMs) to protect the master keys for the CSP.
- KeyControl Vault is now the Entrust Cryptographic Security Platform Vault. The Cryptographic Security Platform Vaults also still integrate with Entrust nShield HSMs to provide an optional HSM root of trust.

Because the Entrust integrations are tested against specific product versions, this guide is still branded as a "KeyControl" integration. It was tested against a pre-CSP version of KeyControl.

Exercise caution when using an Entrust Integration Guide with a product version that does not match the tested version, because your version might not function in exactly the same way.

Entrust cannot guarantee the success of integrations in configurations other than those indicated in the guide. This guide remains on the website for customers using pre-CSP versions of KeyControl.

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	✓
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.

Chapter 2. Install and configure Entrust KeyControl

- Deploy an Entrust KeyControl cluster
- Create an Entrust KeyControl Management Vault

2.1. Deploy an Entrust KeyControl cluster

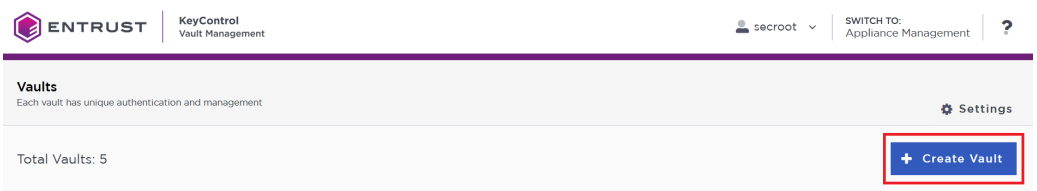
For this integration, Entrust KeyControl was deployed as a two-node cluster on premises. The installation software was downloaded in the form of an OVA file, deployed in VMware ESXi.

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**.

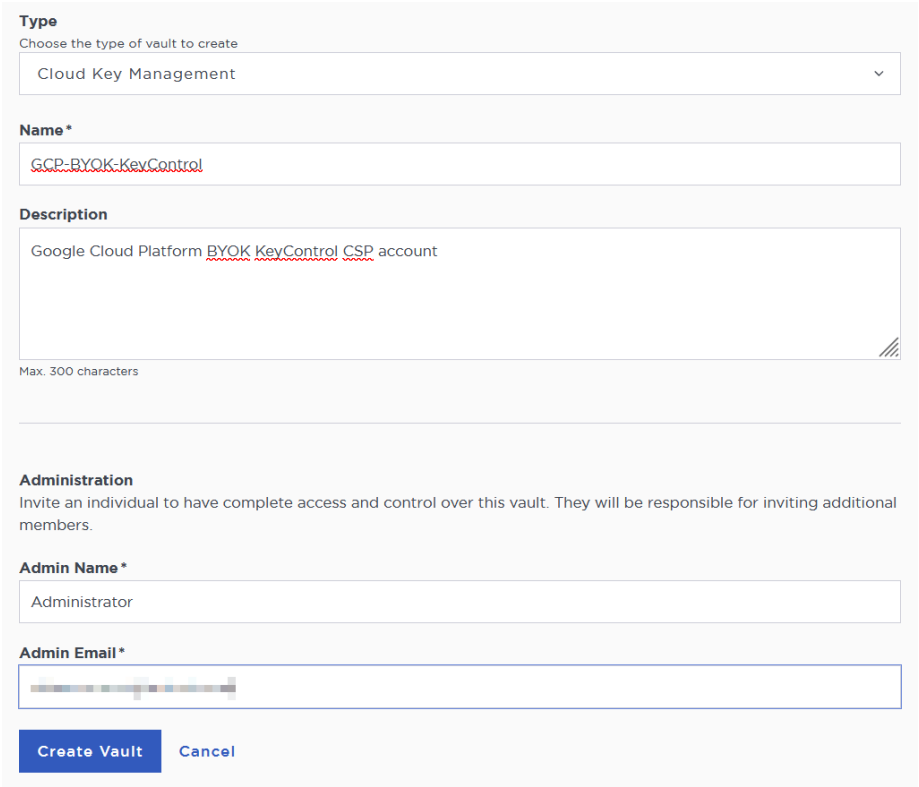


3. Select **Create Vault**.

   The **Create Vault** dialog appears.

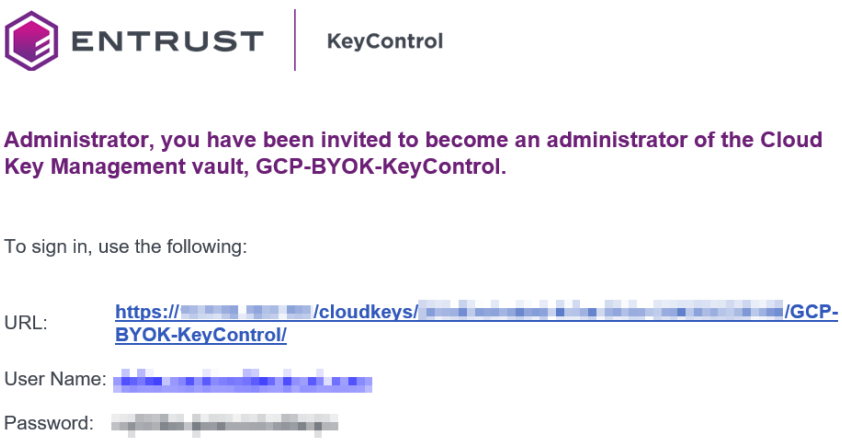
4. In the **Type** drop-down box, select **Cloud Key Management**. Enter the required information.
5. Select **Create Vault**.

   For example:



6. 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:



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

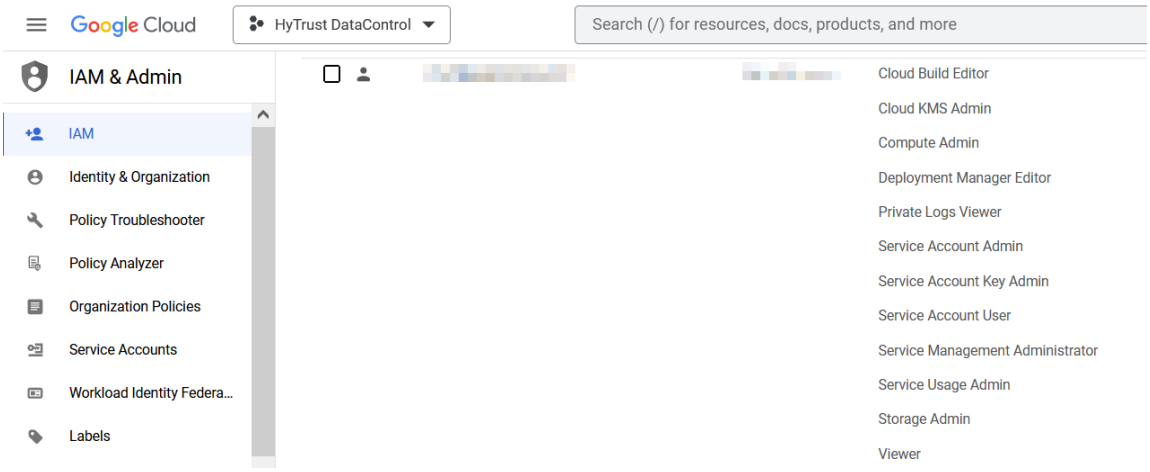
Chapter 3. Configure Google Cloud Platform

- 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

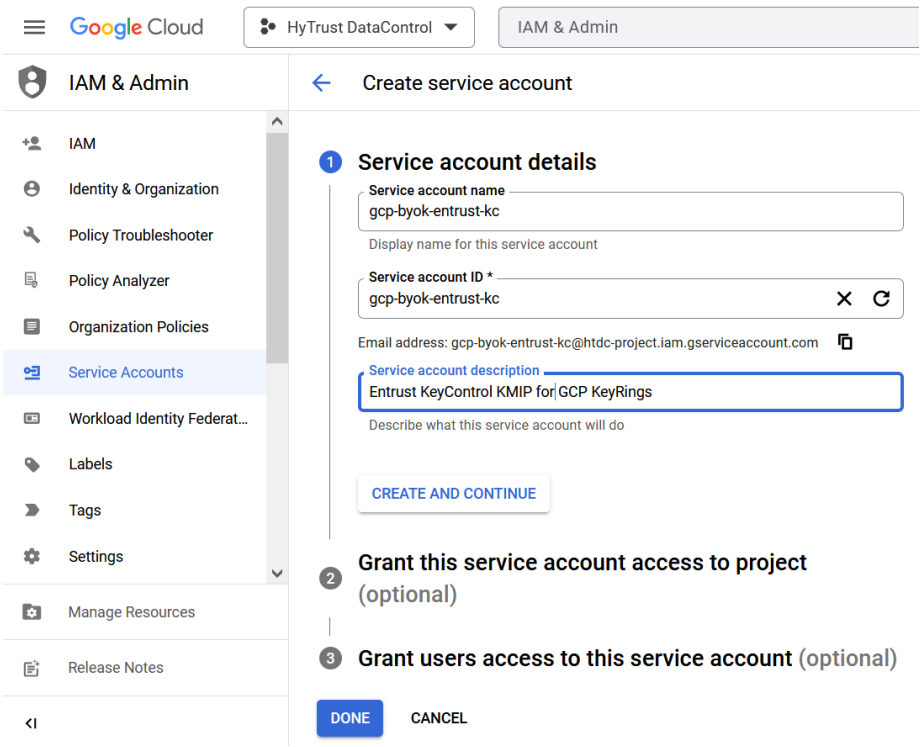


3.2. Create a service account in GCP

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.

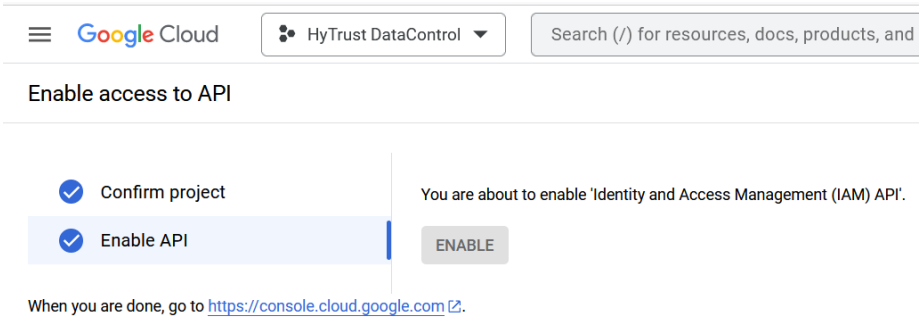
1. Open a browser and sign in to the GCP portal https://console.cloud.google.com.
2. Select **IAM & Admin** on the Welcome screen, or navigate to **Cloud overview** > **Dashboard**.
3. Select **Service Accounts** in the left-hand pane, or enter `IAM & Admin` in the **Search** box and then select **IAM & 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:



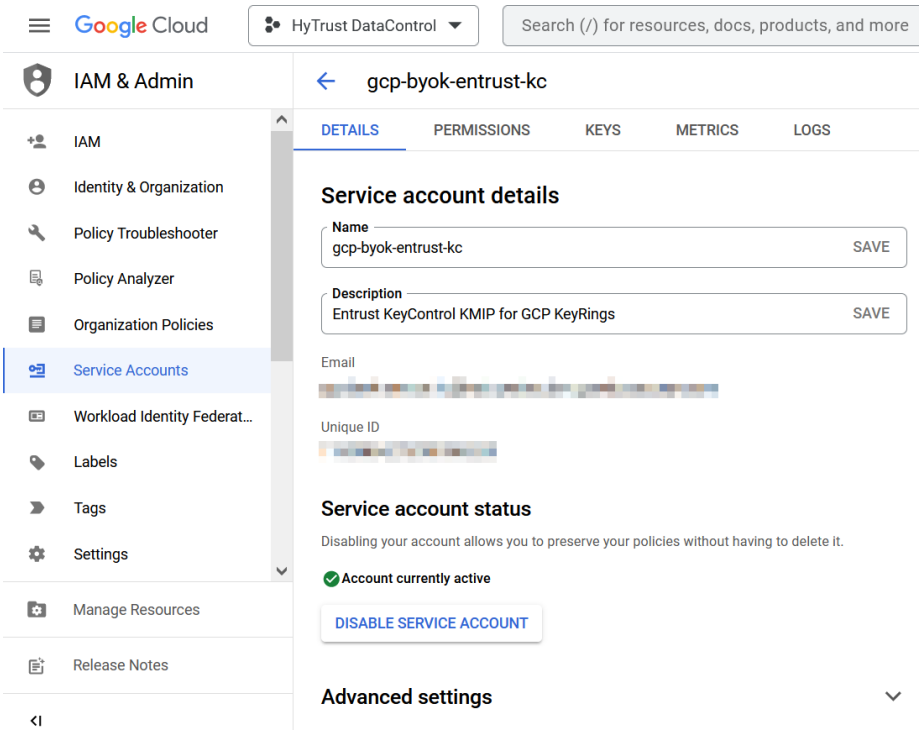
Yourself or the project administrator may need to enable access to APIs. Once enabled, the screen appears as follows.

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**.

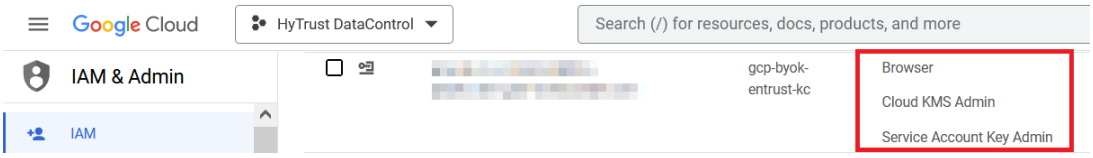
   For example:



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:

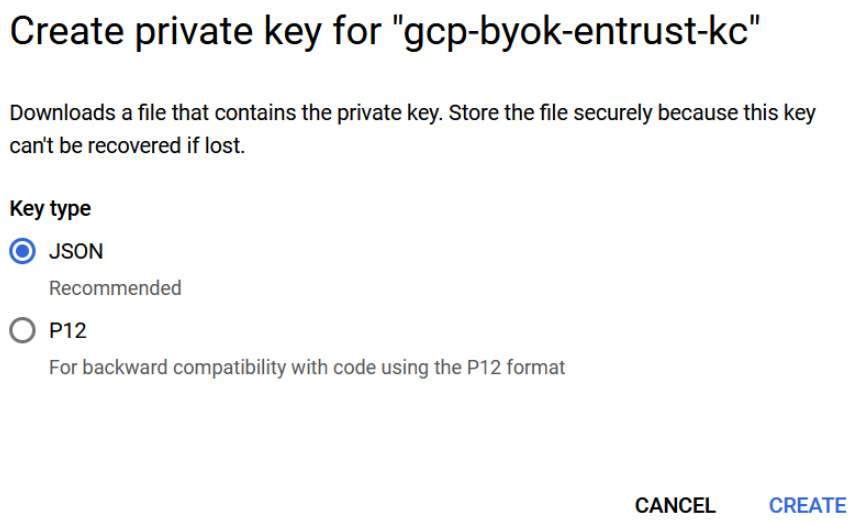


3.3. Create a key for the service account

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.

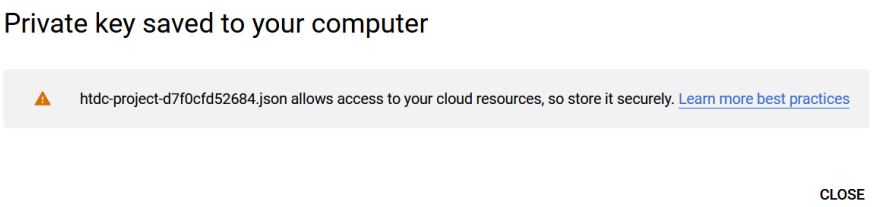
1. Open a browser and sign in to the GCP portal: https://console.cloud.google.com.
2. Select **IAM & Admin** on the Welcome screen, or navigate to **Cloud overview** > **Dashboard**.
3. Select **Service Accounts** in the left-hand pane, or type `IAM & Admin` in the **Search** box and then select **IAM & 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:



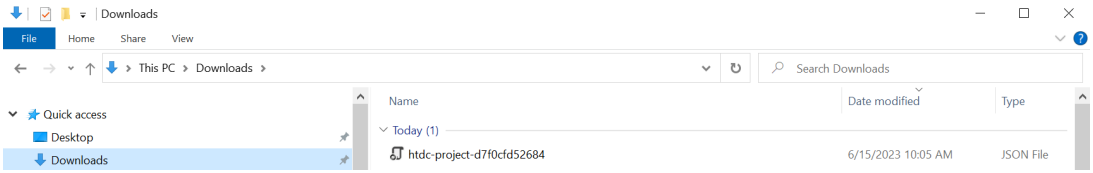
8. Select **CREATE**. A pop-up message appears indicating that the key created was downloaded to your computer.

   For example:



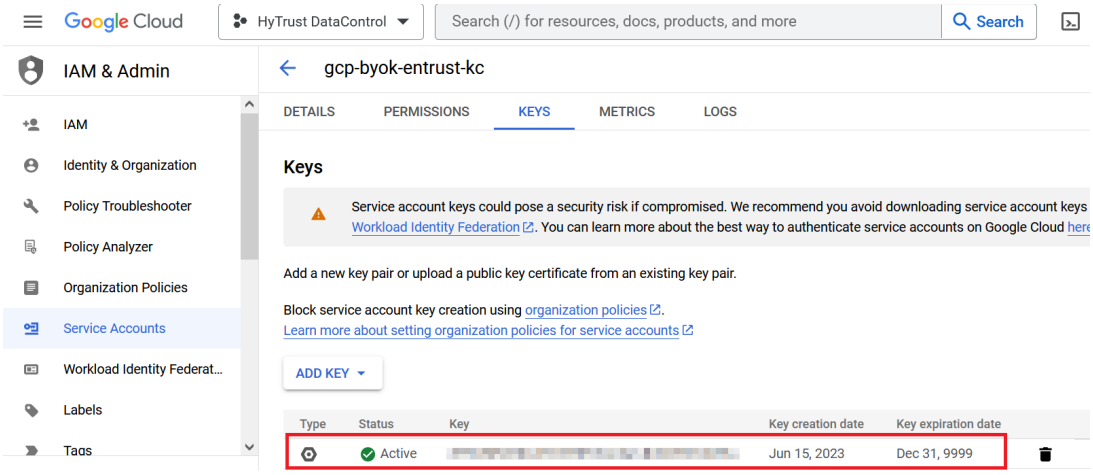
9. Verify by checking your `Downloads` folder.

   For example:



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

    For example:



3.4. Create a GCP key ring

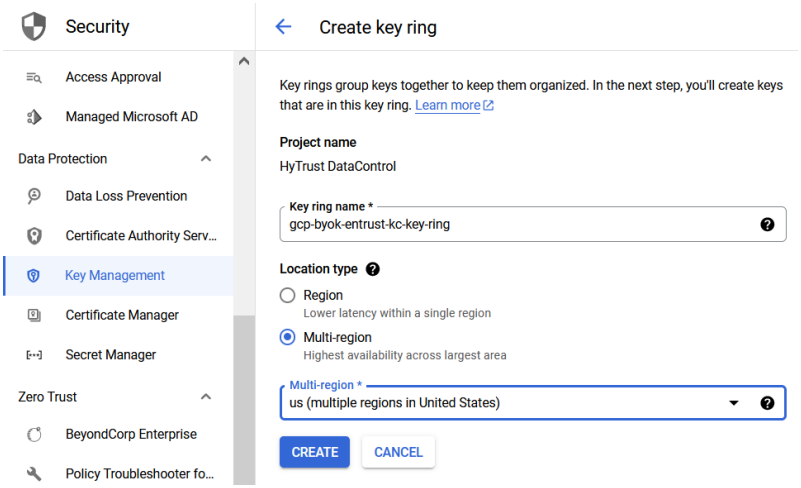
This key ring will be used to store keys managed by Entrust KeyControl. A new GCP key ring was created for this integration to show the entire process. You can use an existing key ring instead.

If using an existing GCP key ring, proceed to section [configure-gcp:::create-keycontrol-csp-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**.

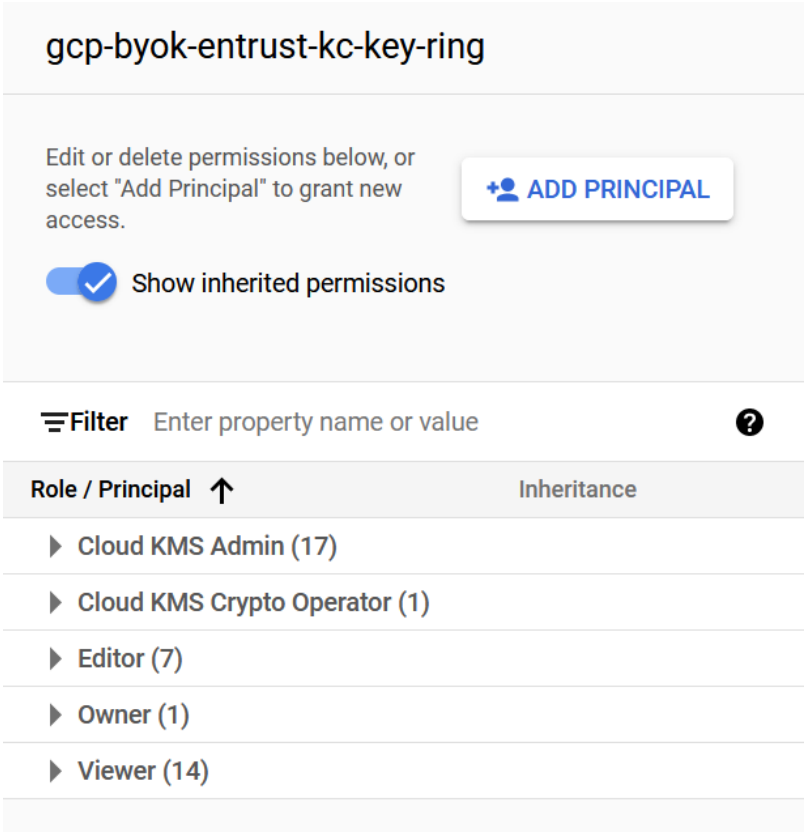
3. In the **KEY RINGS** tab in the left-hand pane, select **+ CREATE KEY RING**.
4. Enter the **Key ring name** and select the **Location type**.

   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)

Chapter 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

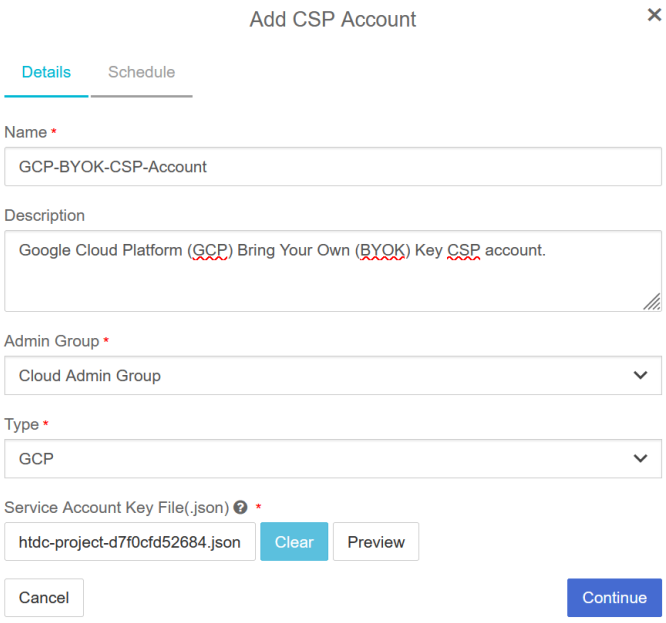
The following steps establish the connection between Entrust KeyControl and GCP, making Entrust KeyControl the CSP of the GCP service account.

1. Sign in to the Entrust KeyControl Vault URL bookmark from [configure-kc-as-gcp-csp:::create-keycontrol-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.

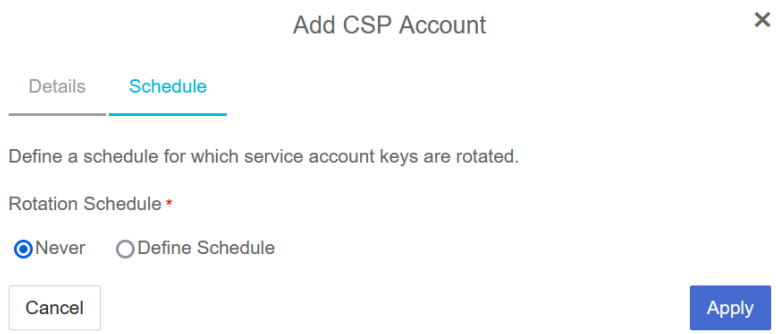
5. In the **Details** tab, enter the **Name** and **Description**.
6. From the **Admin Group** drop-down menu box, select **Cloud Admin Group**.
7. From the **Type** drop-down menu box, select **GCP**.
8. In the **Service Account Key File (.json)** field, select the file download to your computer in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

   For example:



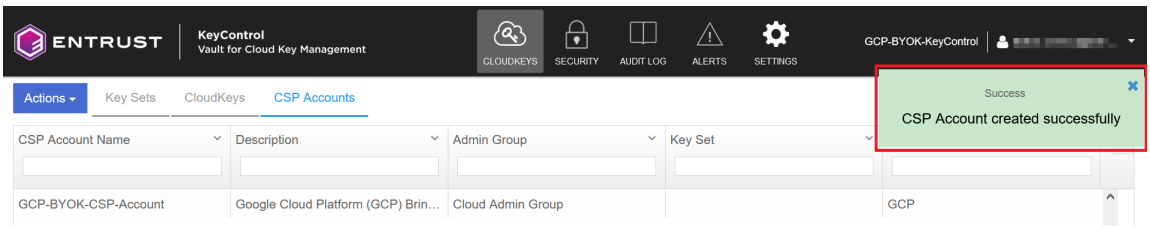
9. Select **Continue**.
10. In the **Schedule** tab, select **Never**.

    For example:



11. Select **Apply**.

    The new CSP account is created.

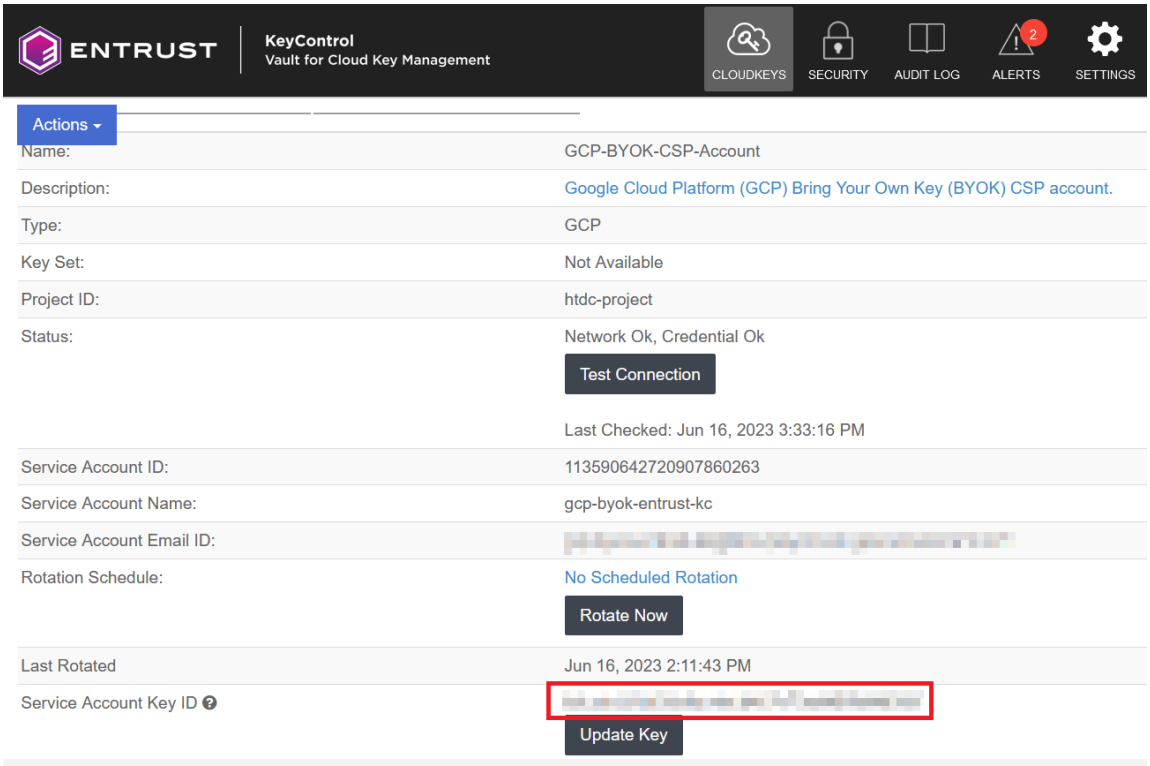


4.2. Verify the connection between Entrust KeyControl and GCP

The key created in [configure-kc-as-gcp-csp:::create-key-for-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.

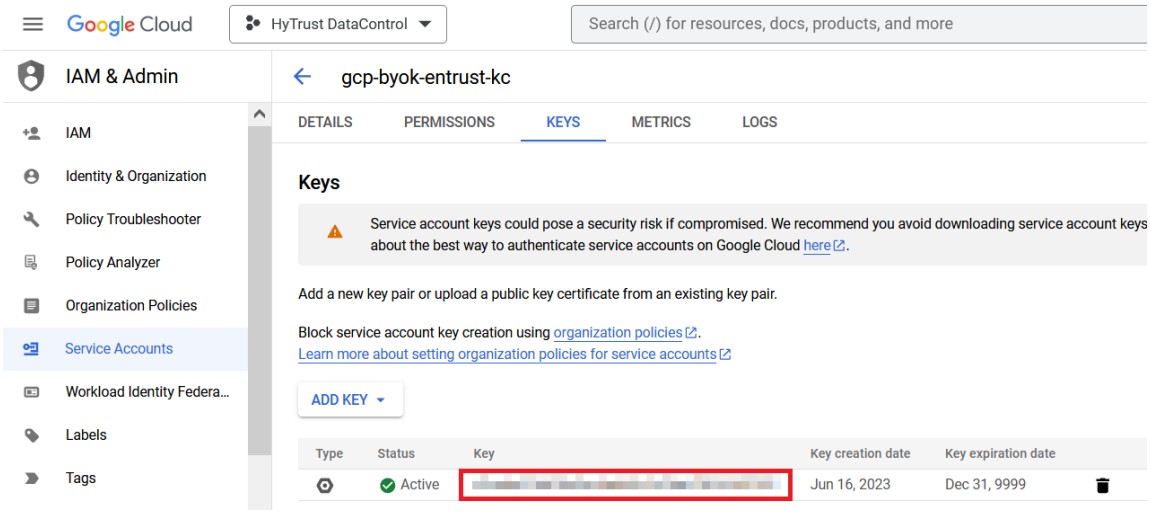
1. Select the newly created CSP account in Create an Entrust KeyControl CSP account for the GCP service account.
2. Scroll down until you see **Service Account Key ID**. Note the value.

   For example:



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:


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

Chapter 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 [test-integration:::create-keycontrol-vault].
2. Select the **CLOUDKEYS** icon on the toolbar.
3. Select the **Key Sets** tab.
4. Select **Actions** > **Create Key Set**.

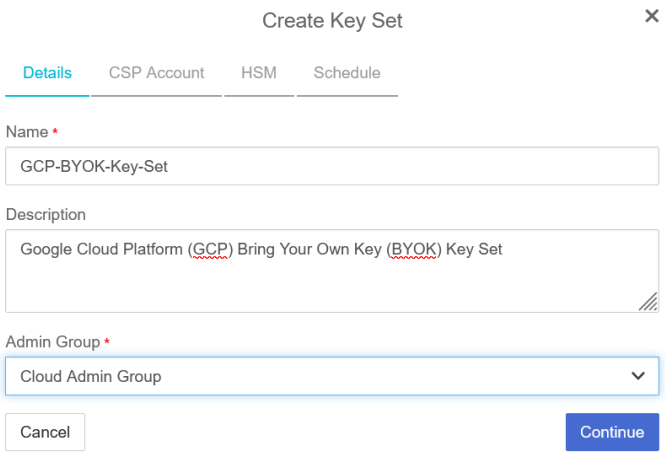
   The **Choose the type of keys...** dialog appears.

5. Choose **GCP Key**.

   The **Create Key Set** dialog appears.

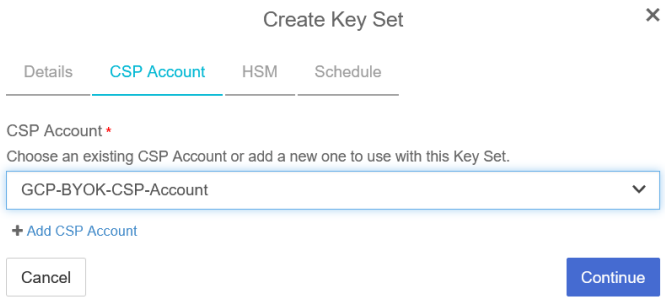
6. In the **Details** tab, enter a **Name** and **Description**.
7. From the **Admin Group** menu, select **Cloud Admin Group**.

   For example:



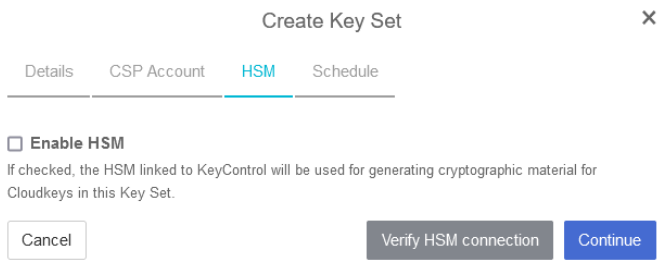
8. Select **Continue**.
9. In the **CSP Account** tab, select the CSP account created in [test-integration:::create-keycontrol-csp-account].

   For example:



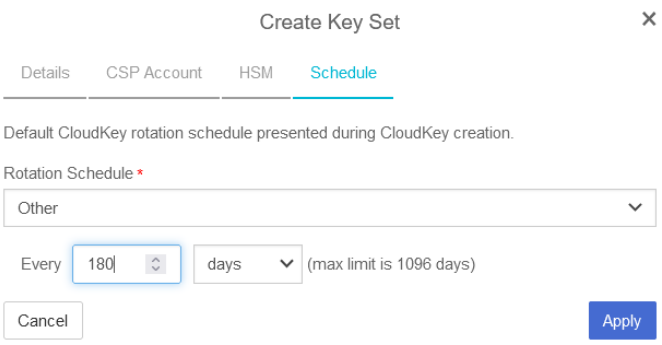
10. Select **Continue**.
11. In the **HSM** tab, select **Enable HSM** if using one. The HSM must be configured prior to this step.

    For example:



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

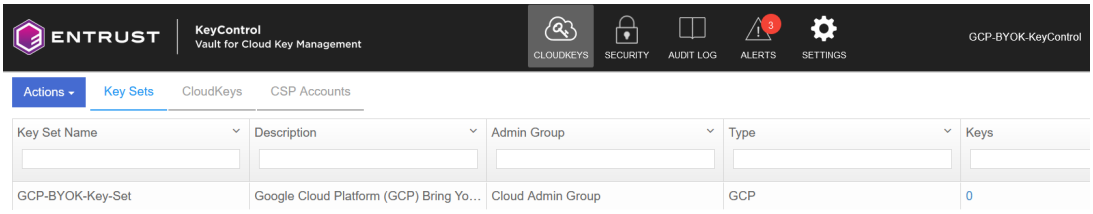
    For example:



14. Select **Apply**.

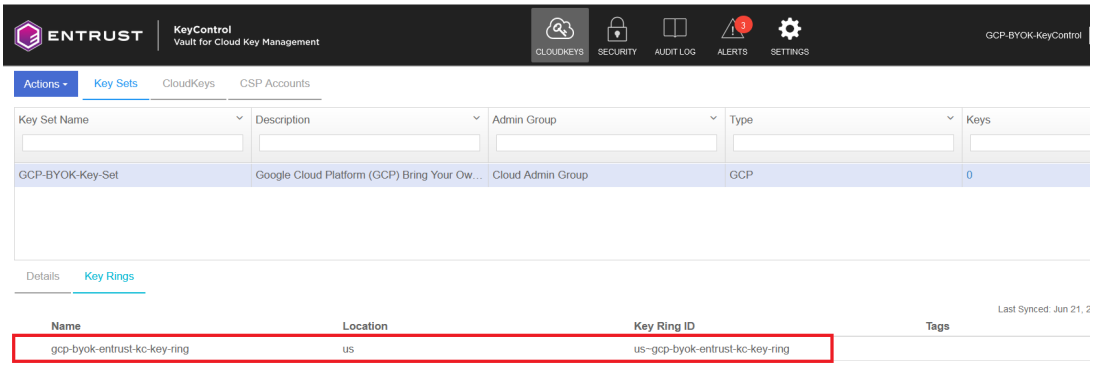
    The key set is added.

    For example:



15. Verify the GCP key ring created in [test-integration:::create-gcp-keyring] is listed in the **Key Rings** tab. Select **Sync Now** on the right of the display to update the **Key Ring** list.

    For example:



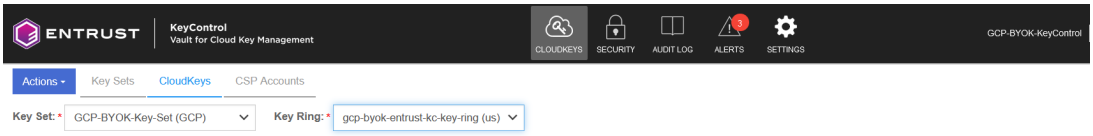
For additional information, see Creating a Key Set.

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 [test-integration:::create-keycontrol-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 [test-integration:::create-gcp-keyring].

   For example:

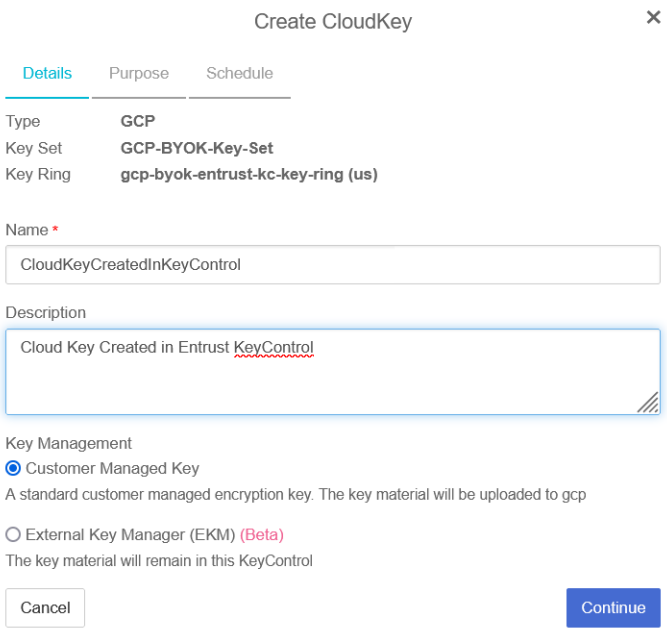


6. Select **Actions** > **Create CloudKey**.

   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.

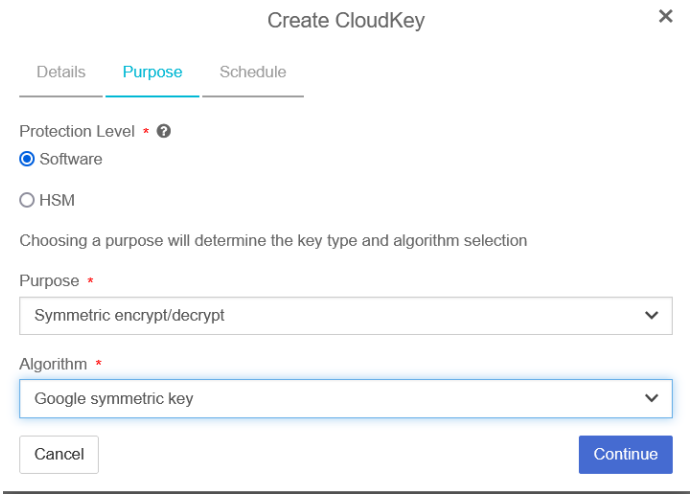
   For example:



9. Select **Continue**.
10. If you are using the hardware protection method, in the **Purpose** tab, select **HSM** from the **Protection Level** options.

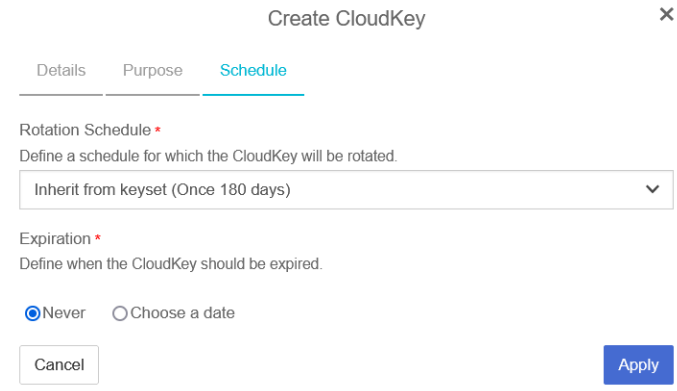
11. From the **Purpose** and **Algorithm** pull down menus, select the appropriate options for your application.

    For example:



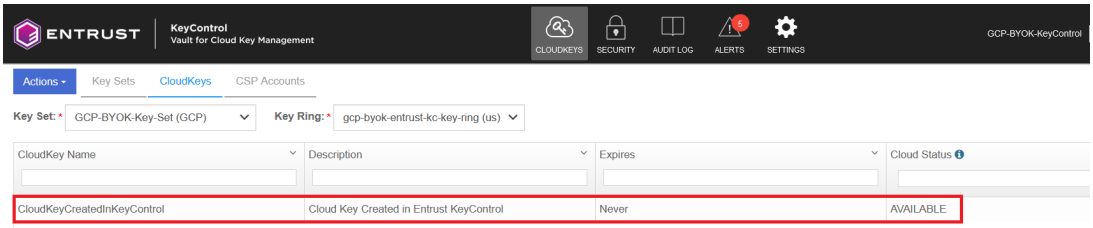
12. In the **Schedule** tab, select the **Rotation Schedule** and **Expiration**.

    For example:

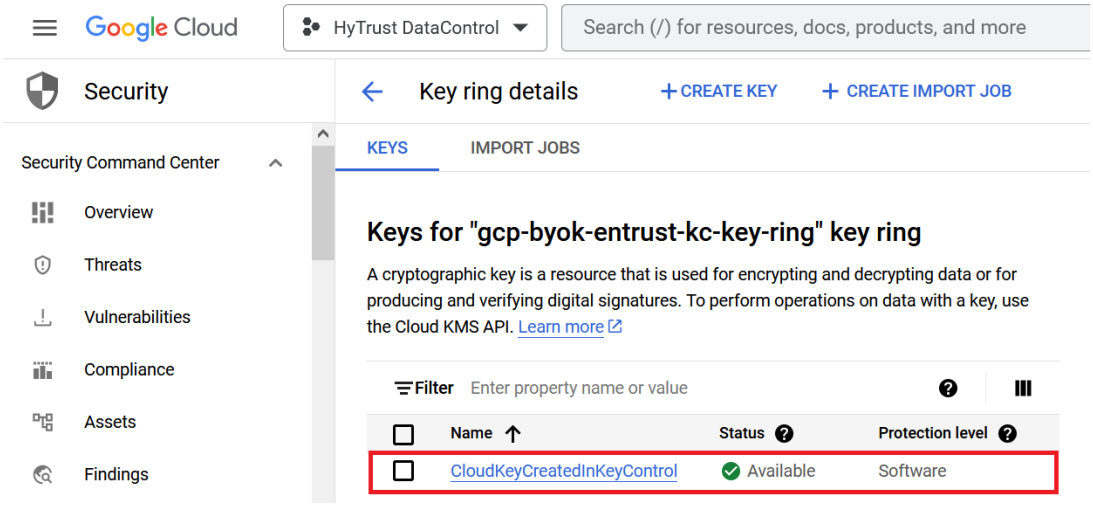


13. Select **Apply**.

    The cloud key is created.



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



For additional information, see Creating a CloudKey.

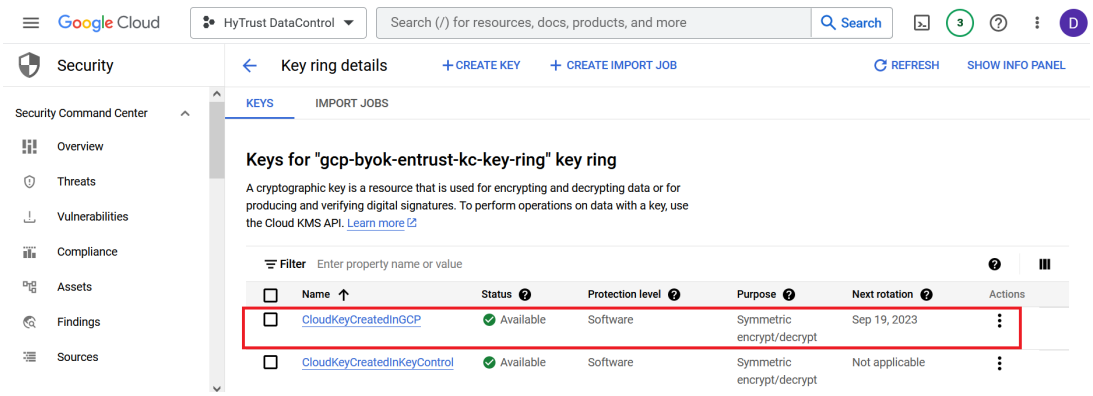
5.3. Import a GCP cloud key into Entrust KeyControl

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 [test-integration:::create-gcp-keyring].
4. The existing cloud key in GCP to be imported into Entrust KeyControl is enclosed in the red box.

   For example:

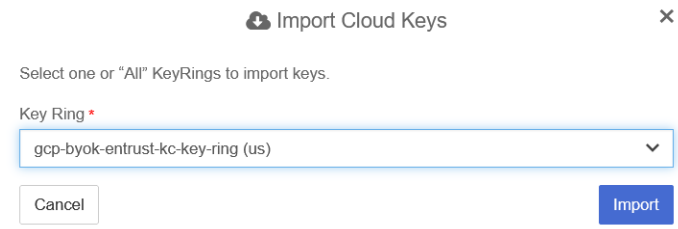


5. Sign in to the Entrust KeyControl Vault URL bookmark from [test-integration:::create-keycontrol-vault].
6. Select the **CLOUDKEYS** icon on the toolbar.
7. Select the **Key Sets** tab.
8. Select the key set created in Create a key set in Entrust KeyControl.
9. Select **Actions** > **Import CloudKey**.

   The **Import Cloud Keys** dialog appears.

10. From the **Key Ring** pull-down menu, select the GCP key ring created in [test-integration:::create-gcp-keyring].

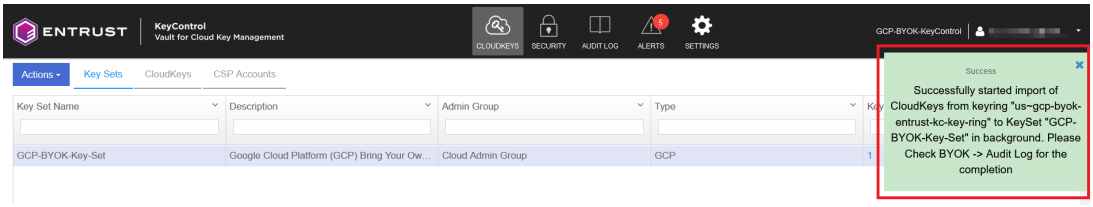
    For example:



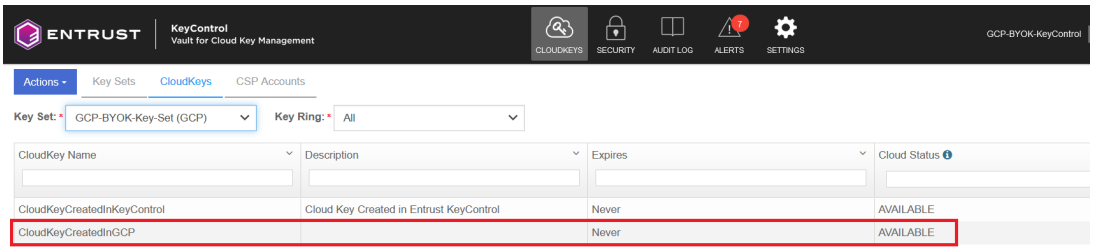
11. Select **Import**.

    The key is imported.

    For example:



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

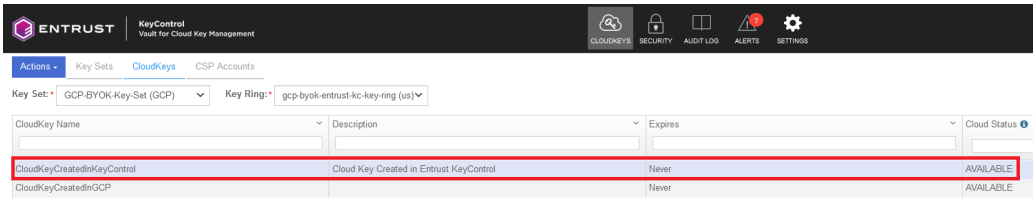


5.4. Rotate a cloud key in Entrust KeyControl

To rotate a cloud key in Entrust KeyControl:

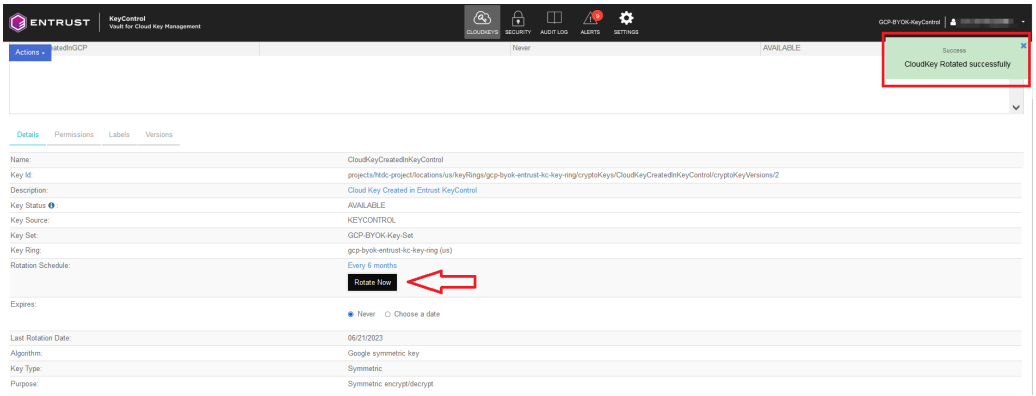
1. Sign in to the Entrust KeyControl Vault URL bookmark from [test-integration:::create-keycontrol-vault].
2. Select the **CLOUDKEYS** icon on the toolbar.
3. Select the **CloudKeys** tab.
4. From the **Key Set** menu, select the **Key Set** created in Create a key set in Entrust KeyControl.
5. From the **Key Ring** menu, select the key ring created in [test-integration:::create-gcp-keyring].
6. Select the key to rotate.

   For example:



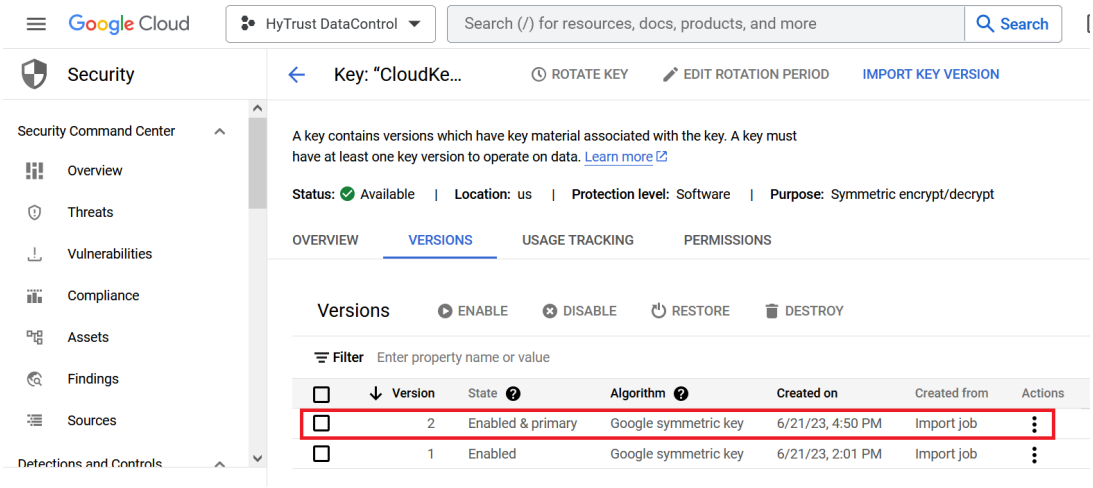
7. Select **Rotate Now**. You might need to scroll down the page to view this button.

   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 [test-integration:::create-gcp-keyring].
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:



5.5. Remove a cloud key in Entrust KeyControl

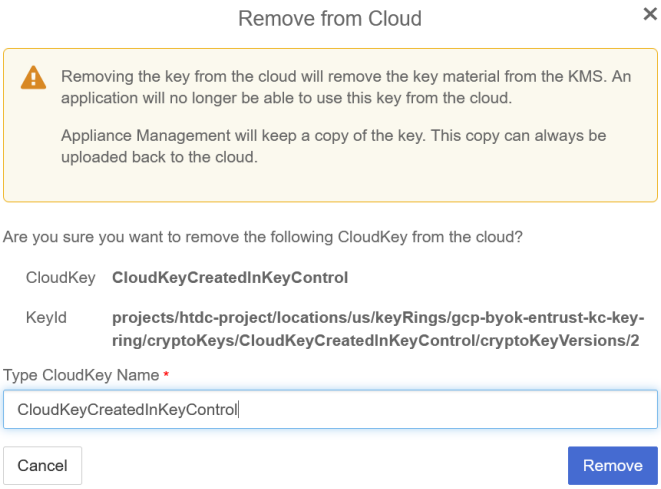
A removed cloud key in Entrust KeyControl will no longer be available for use in GCP. However, Entrust KeyControl will keep a copy of the removed cloud key, which can be reloaded back to GCP for use.

1. Sign in to the Entrust KeyControl Vault URL bookmark from [test-integration:::create-keycontrol-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 [test-integration:::create-gcp-keyring].
6. Select the key to the removed.
7. Select **Actions** > **Remove from Cloud**.

   The **Remove from Cloud** dialog appears.

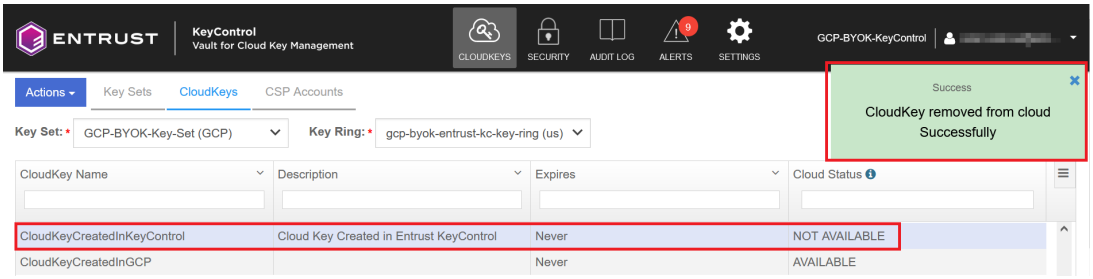
8. Type the name of the cloud key in **Type CloudKey Name**.

   For example:



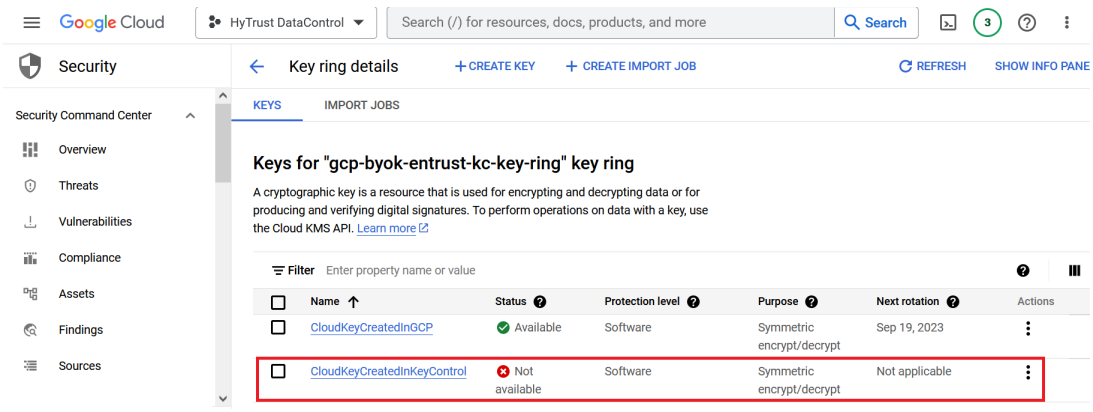
9. Select **Remove**.
10. Verify the status change in Entrust KeyControl.

    For example:



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

    For example:



For additional information, see Removing a CloudKey from the Cloud.

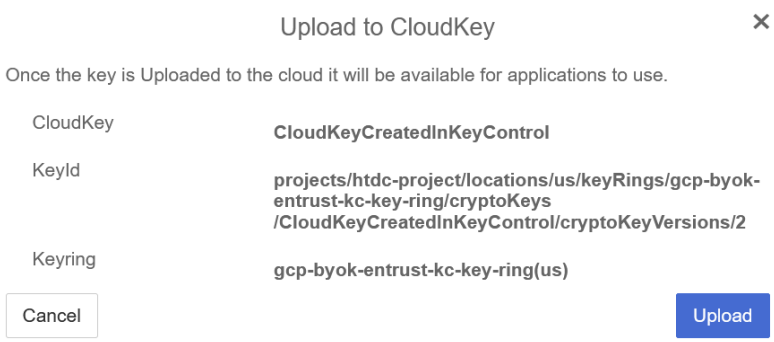
5.6. Upload a removed Entrust KeyControl key back to GCP

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 [test-integration:::create-keycontrol-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 [test-integration:::create-gcp-keyring].
6. Select the key to be uploaded.
7. Select **Actions** > **Upload to Cloud**.

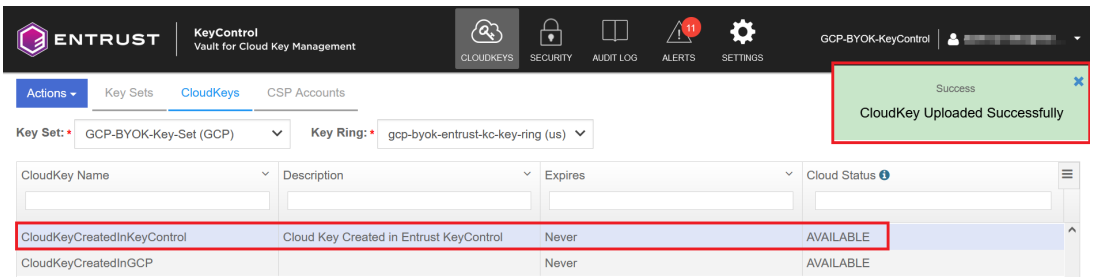
   The **Upload to CloudKey** dialog appears.

   For example:



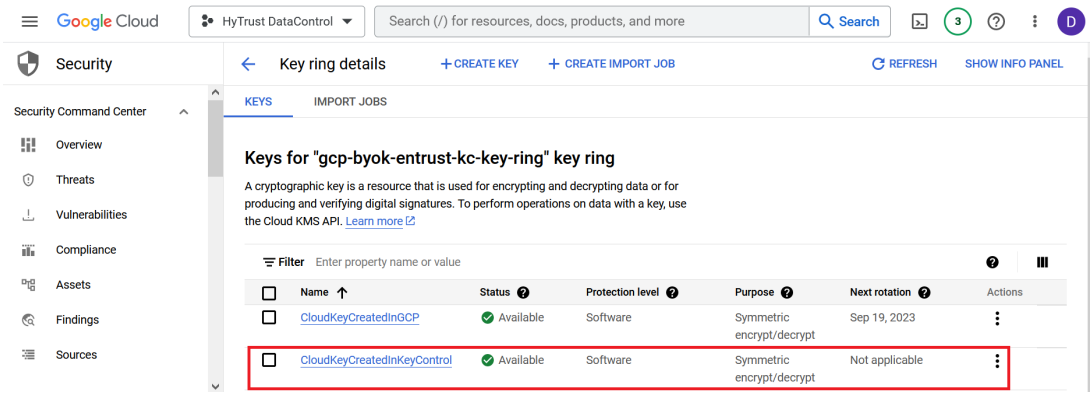
8. Select **Upload**.
9. Verify the status change in Entrust KeyControl.

   For example:



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

    For example:



5.7. Delete a cloud key in Entrust KeyControl

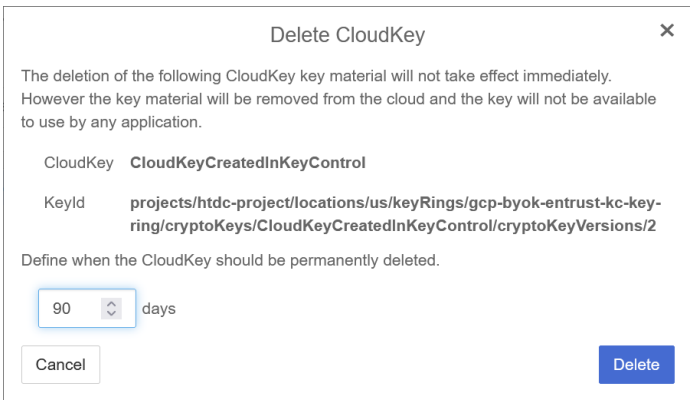
The deletion of a cloud key does not take effect immediately. However, after a user-defined interval, the key will be permanently removed.

1. Sign in to the Entrust KeyControl Vault URL bookmark from [test-integration:::create-keycontrol-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 [test-integration:::create-gcp-keyring].
6. Select the key to delete.
7. Select **Actions** > **Delete CloudKey**.

   The **Delete CloudKey** dialog appears.

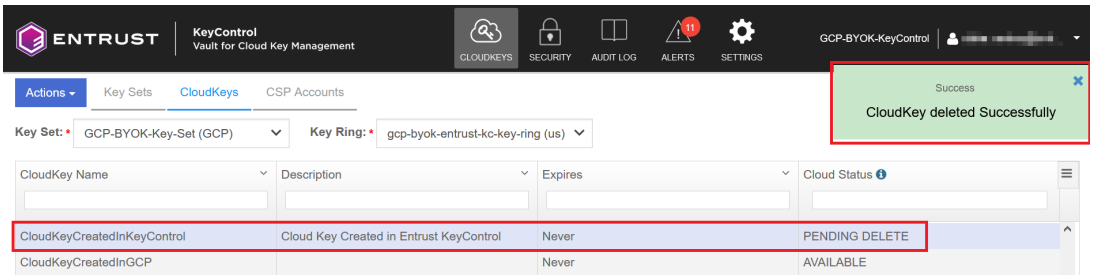
8. Select a time in **Define when the CloudKey should be permanently deleted**.

   For example:



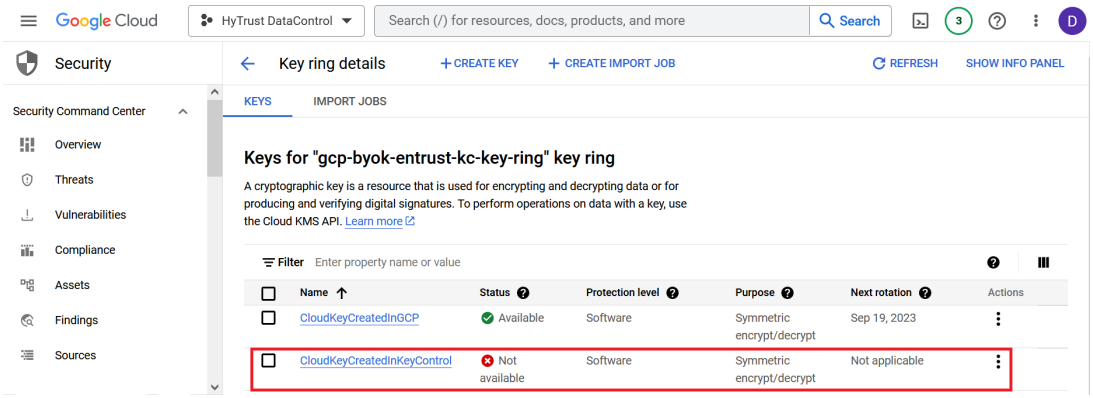
9. Select **Delete**.
10. Verify the status change in Entrust KeyControl.

    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

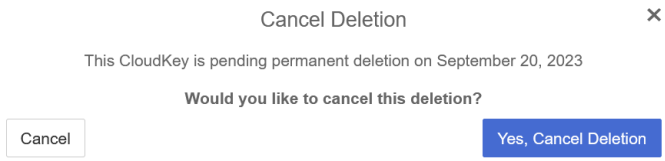
The deletion of a key can be canceled while the time in the **Define when the CloudKey should be permanently deleted** setting has not expired. Follow these steps to upload back to GCP the Entrust KeyControl key deleted in Delete a cloud key in Entrust KeyControl.

1. Sign in to the Entrust KeyControl Vault URL bookmark from [test-integration:::create-keycontrol-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 [test-integration:::create-gcp-keyring].
6. Select the key deletion to be canceled.
7. Select **Actions** > **Cancel Deletion**.

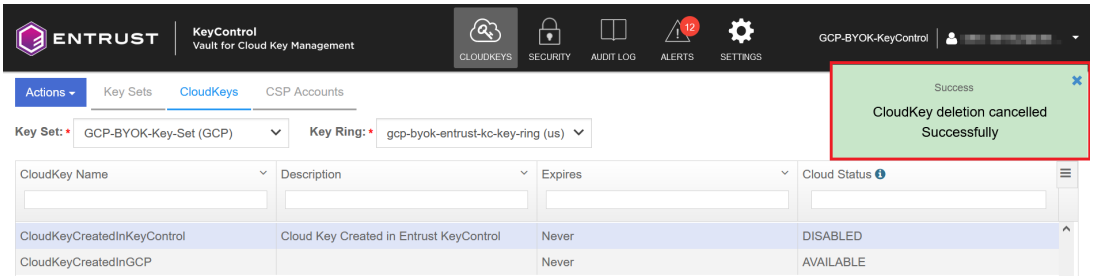
   The **Cancel Deletion** dialog box appears.

   For example:



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

   For example:



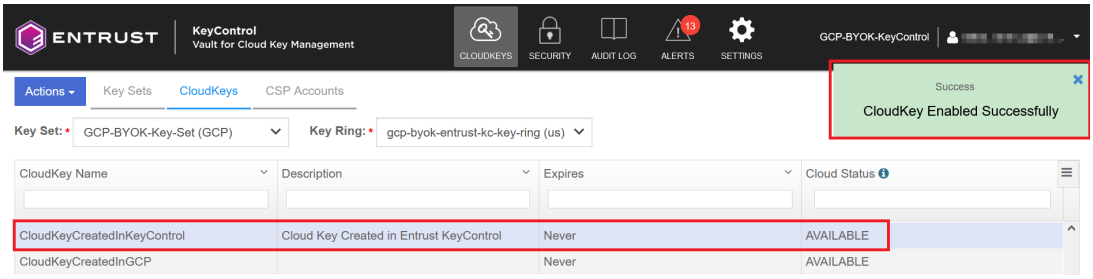
10. Select **Actions** > **Enable CloudKey**.

    The **Enable CloudKey** dialog box appears.

    For example:

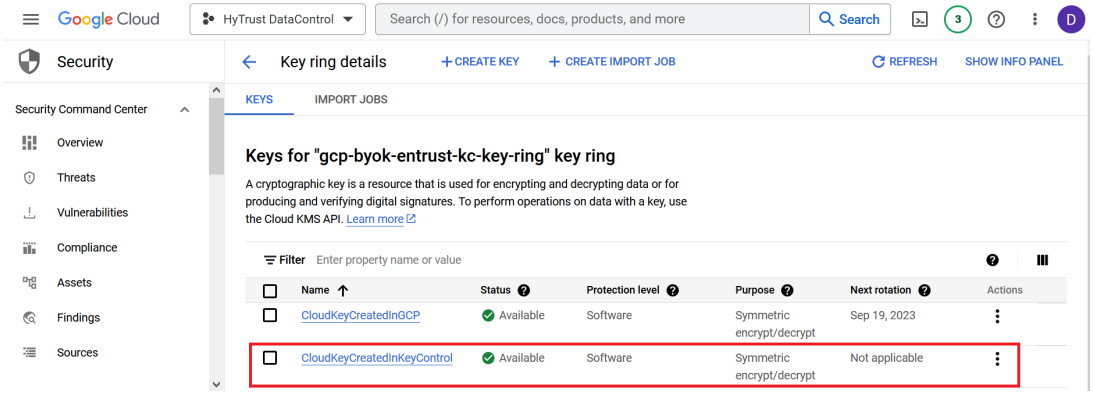
11. Select **Enable**.
12. Verify the status change in Entrust KeyControl.

For example:



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

For example:



For additional information, see Canceling a CloudKey Deletion.

Chapter 6. Additional resources and related products

6.1. nShield HSMs

6.2. nShield as a Service

6.3. KeyControl BYOK

6.4. Entrust products

6.5. nShield product documentation