Fortanix®

User Guide

FORTANIX DATA SECURITY MANAGER – GCP CLOUD KEY MANAGEMENT

VERSION 2.0

Fortanix Inc. | 3910 Freedom Circle | Suite 104 | Santa Clara, CA 950542 | United States of America | +1 (650) 943-2484 |
info@fortanix.com | www.fortanix.com

TABLE OF CONTENTS

1.0 INTRODUCTION

Welcome to the Fortanix Data Security Manager (DSM) Google Cloud Platform (GCP) Key Management User Guide. This document describes how to add a new GCP Cloud Key Management Service (KMS) to Fortanix DSM. It contains the information related to:

- Creating a GCP Cloud KMS group in Fortanix DSM
- Configuring the GCP Cloud KMS Connection in Fortanix DSM
- Testing the GCP Cloud KMS Connection
- Syncing the GCP Cloud KMS keys in Fortanix DSM

1.1 OVERVIEW

The Fortanix solution for GCP Cloud KMS offers complete Bring Your Own Key (BYOK) and lifecycle management for management and automation of native GCP Cloud keys (CMEK – Customer Master Encryption Key) and allows users to manage all keys centrally and securely.

2.0 DEFINITIONS

- **Fortanix Data Security Manager** -

  Fortanix DSM is the cloud solution secured with Intel® SGX. With Fortanix DSM, you can securely generate, store, and use cryptographic keys and certificates, as well as secrets, such as passwords, API keys, tokens, or any blob of data.

- **Accounts** -

  A Fortanix DSM account is the top-level container for security objects managed by the Fortanix DSM. An account is generally associated with an organization, rather than an individual. Security objects, groups, and applications belong to exactly one account. Different accounts are fully isolated from each other. *See support for more information.*

- **Users** -

  Users are associated with an email address. A user can be a member of one or more accounts. Depending on permissions, users can:

  - Perform management operations like adding or modifying users or groups
  - Create security objects
  - Change properties of security objects
  - Review logs of Fortanix DSM activity

  Users cannot perform cryptographic operations. Only applications can perform cryptographic operations.

- **Groups** -

  A group is a collection of security objects created by and accessible by users and applications which belong to the group. The user who creates a group automatically gets assigned the role of the group administrator. The group administrator can add more users to the group in the role of administrators or auditors. They can also add applications to the group to enable the

applications to create and use security objects in that group. *See support for more information.*

Access policies are set at the group level, so all security objects in a group share the same access policy. Any number of users and/or applications can be assigned to a group. *Some examples of usage of groups are given in the Authorization section*.

Quorum policies can also be set at group level. A Quorum policy mandates that all security sensitive operations in that group would require a quorum approval. Such operations include using a key for cryptographic operations or deleting or updating a group. *See Quorum Policy for more information.*

- **Applications** -

  An application can use Fortanix DSM to generate, store, and use security objects, such as cryptographic keys, certificates, or an arbitrary secret. Applications can authenticate to Fortanix DSM using an API key (a secret token) or a TLS client certificate. An application can interact with Fortanix DSM using the RfEST APIs or using the PKCS#11, JCE, or CNG providers. *See support for more information.*

- **Fortanix Data Security Manager Security Objects** –

  A security object is any datum stored in Fortanix DSM (for example a key, a certificate, a password, or other security objects). Each security object is assigned to exactly one group. users and applications assigned to the group have permission to see the security object and to perform operations on it. *See support for more information.*

3.0 GETTING STARTED WITH FORTANIX CLOUD DATA CONTROL

To understand which solution between CNKMS, BYOK, BYOKMS (AWS XKS), or BYOE is right for you, please see < “FORTANIX DATA SECURITY MANAGER CLOUD DATA CONTROL Getting Started Guide”>

For BYOKMS using AWS XKS see <Link guide for BYOKMS>)

4.0 FORTANIX DATA SECURITY MANAGER GCP CLOUD KMS GROUP SETUP

The following section describes the workflow to configure Fortanix DSM to interact with the GCP Cloud KMS. A GCP CDC group is created in the Fortanix DSM account, and this group is configured to interact with the GCP Cloud KMS.

4.1 CREATE A GCP CDC GROUP

1. In the Fortanix DSM **Groups**  page, click the  button to create a new GCP KMS group.
2. In the **Add new group** form,
   a. Enter a name and description for your group.
   b. Next, click the **LINK HSM/EXTERNAL KMS** button to select the GCP KMS type, so that Fortanix DSM can connect to it.
   c. Select the type of HSM/external KMS as **GCP Key Management Service** from the drop down menu.
   d. Enter the GCP KMS Service Account Credentials
      - **GCP Project ID**: This is the unique identifier for the Google Cloud project used to differentiate your project from all others in Google Cloud. For example: **`Fortanix`**
      - Select the geographical region/location where the Google Cloud KMS resource is stored or can be accessed within a Google Cloud project. For example: **`South Carolina (us-east1)`**.
      - **Authentication**: The following Cloud KMS and Cloud Platform APIs must be enabled for using KMS and Cloud platform related GCP services.:

        `https://www.googleapis.com/auth/cloudkms`

        `https://www.googleapis.com/auth/cloud-platform`

        Fortanix DSM uses Google Service Account to authenticate with Google Cloud KMS. Enter the service account email in the format

        `SERVICEACCOUNT@PROJECT.iam.gserviceaccount.com`

        NOTE: The Google service account must have the role of Cloud KMS Admin.
      - **Upload a Private Key**: Upload the JSON/p12 file containing the private key of the service account to authenticate with Google Cloud KMS.

3. Click **TEST CONNECTION** to test your GCP KMS connection. If Fortanix DSM is able to connect to your GCP KMS using your connection details, then it shows the status as "Connected" with a green tick . Otherwise, it shows the status as "**Not Connected**" with a yellow warning sign .
4. After the connection is successful, you will get the list of keyrings from which you have to select the key ring that you want to configure for the GCP KMS group. A key ring organizes keys in a specific Google Cloud location and allows you to manage access control on groups of keys.

NOTE: when you click **TEST CONNECTION** for the first time, Fortanix DSM tests the credentials provided and fetches the key rings. After you select the key ring, if you click **TEST CONNECTION** again, then Fortanix DSM checks the credentials and also checks the accessibility of the selected key ring.

4.2 SAVE GCP KMS GROUP DETAILS

Though testing the connection in the previous section is an optional step, you can save your group details even if the connection information might be incorrect or incomplete, you can edit these details later. Now, save your group details by clicking the **SAVE** button.

After you save your group details, your group is created, and you will see a detailed view of your group.

You can now see that there is an addition of the **HSM/KMS** tab in the group details, this tab shows the details about your KMS.

4.3 THE HSM/KMS TAB

The **HSM/KMS** tab shows the details of the KMS that was added such as the service account email and key ring name of the GCP KMS. You can also edit the GCP connection details such as the **Service account email** and the **Private key** here.

After you edit the connection details and save it, click **TEST CONNECTION** to test the connection.

Click **SYNC KEYS** to create virtual copies of all the keys present in the key ring of the location and project provided in the GCP KMS group.

4.4 NOT CONNECTED SCENARIO

On clicking **TEST CONNECTION**, it is possible that Fortanix DSM is not able to connect to the GCP KMS, in that case, it displays a "**Not Connected**" status with a warning symbol . You can save the details of the new connection details provided and edit them later.

4.5 GROUPS TABLE VIEW

After saving the group details, you can see the list of all groups and notice the special symbol next to the newly created group, this symbol differentiates it from the other groups, as it shows that it is a GCP KMS group.

4.6 USER VIEW

Click the **Users** tab in the Fortanix DSM UI and click the user that says "**You**" to go to the user's detailed view, as shown below.

The detailed view shows all the groups of which the user is a part of, additionally Fortanix DSM displays which groups are mapped to GCP KMS and whether they are "Connected" or "Not Connected".

5.0 FORTANIX DATA SECURITY MANAGER GCP KMS SECURITY OBJECTS

After the GCP KMS group successfully connects to the GCP KMS using the connection details, the keys from the GCP KMS are stored in the Fortanix DSM GCP KMS group as virtual keys. A virtual key is a key whose key material is not present in the GCP KMS group. The key material is stored securely in the key ring of the location and project provided in the GCP KMS group. The virtual key is only a pointer with the key information and key attributes, but it does not hold the key material.

5.1 CREATE A KEY IN GCP KMS GROUP - GENERATE

In this section, you will learn how to generate a key in the configured GCP KMS region.

5.1.1 GENERATE A KEY

This action will generate the configured key type in the configured GCP KMS regions directly, and it will be represented as a virtual key in the corresponding GCP KMS group. This means that the virtual key in the GCP KMS group will point to the actual key in GCP KMS that stores the key material of this new key. The virtual key only stores the key information and key attributes, but it does not have the key material.

In your Fortanix DSM console, follow the process below to create a new key:

1. Click the **Security Objects**  tab.
2. Click  to create a new Security Object.
3. In the **Add New Security Object** form enter a name for the Security Object (Key).
4. Select the **This is an HSM/external KMS object** check box. This will show the GCP KMS configured groups in the **Select group** list.
5. In the GCP KMS group list, select the GCP KMS group into which the keys will be generated. The keys will be generated into the region that was selected in the GCP KMS group.
6. Select **GENERATE IN GCP** to initiate the generate key in the GCP KMS workflow.
7. Enter the **GCP key name** The GCP key name is the key name that will be stored in the GCP Key Ring. The GCP key name will be used to correlate between different versions of a key. All the key versions will have the same GCP key name.
8. Select the key type for the new GCP KMS key.

NOTE: For Fortanix DSM 4.4, the allowed key type for a GCP KMS key generated using the Generate Key flow in Fortanix DSM is AES 256.

These key types can further be restricted by setting a Cryptographic policy for the account or group or a Key Metadata Policy for the group. For more details about the Cryptographic policy, *please refer to the article:* https://support.fortanix.com/hc/en-us/articles/360042064051-User-s-Guide-Crypto-Policy.

For more details about the Key metadata policy, *please refer to the article:* https://support.fortanix.com/hc/en-us/articles/4420883272596-User-s-Guide-Key-Metadata-Policy.

9. Enter the **Key size** and select the permitted key operations under **Key operations permitted** section.
10. Add custom attributes by clicking the **ADD ATTRIBUTE** button.

    NOTE: The custom attributes also depend on the Key metadata policy for the group. If the GCP KMS group has a Key metadata policy configured with restrictions for custom attributes, then these rules will be applied while creating the security object.
11. To store audit logs for the object in the group, enable the toggle for **Keep detailed log for the object**. The initial state of the toggle is based on the parent Crypto policy if any.
12. Click the **GENERATE** button to generate the key in GCP KMS.
13. The new GCP KMS Key is created and represented with a special symbol to denote it is of type HSM/External KMS. In the detailed view of the GCP key you will notice the following things:
    - The group to which it belongs (in the **Group** field). It also shows if the group is mapped to a GCP KMS or not using the special icon .
    - How the key was created (in the **Created by** field). If it is a GCP KMS key, this field shows the group that created this key. It also shows minor details such as if the group is “Connected” or “Not Connected”.
14. The new GCP KMS key is in an **Enabled** state by default which means that all the Encrypt and Decrypt operations can be performed on the actual key in the GCP KMS

according to the key permissions. Click the toggle for **Enabled** to disable it. This will disable the GCP KMS key temporarily.

15. The new key will be added to the Security Objects table.

Tip:

- You can also access the new key from the Group detailed view from the **SECURITY OBJECTS** tab.
- You can also add a new key from the Group detailed view from the **SECURITY OBJECTS** tab, click **ADD SECURITY OBJECT** button, and follow ***steps 3-10*** above.

5.1.2 BRING YOU OWN KEY – IMPORT KEY

This action will import the configured key type in the key ring in one of the configured GCP KMS regions directly, and it will be represented as a virtual key in the corresponding GCP KMS group. This means that the virtual key in the GCP KMS group will point to the actual key in GCP KMS that stores the key material of this new key. The virtual key only stores the key information and key attributes, but it does not have the key material. The import action will not store a copy of the key material in Fortanix DSM.

1. Follow Steps 1-5 from *Section 4.1.1*
2. Select **IMPORT** to initiate the import key in the GCP KMS workflow.
3. Enter the **GCP key name** The GCP key name is the key name that will be stored in GCP Key Ring. The GCP key name will be used to correlate between different versions of a key. All the key versions will have the same GCP key name.
4. Select the key type for the new GCP KMS key.

NOTE: For Fortanix DSM 4.4, the allowed key type for a GCP KMS key generated using the import Key button in Fortanix DSM is AES 256.

These key types can further be restricted by setting a Cryptographic policy for the account or group or a Key Metadata Policy for the group. For more details about the Cryptographic policy, *please refer to the article:* https://support.fortanix.com/hc/en-us/articles/360042064051-User-s-Guide-Crypto-Policy.

For more details about the Key metadata policy, *please refer to the article:* https://support.fortanix.com/hc/en-us/articles/4420883272596-User-s-Guide-Key-Metadata-Policy.

5. Sometimes keys of type AES that need to be imported from a file were previously wrapped (encrypted) by a key from Fortanix DSM. This is done so that the key should not go over the TLS in plain text format. In such scenarios select the check box **The key has been encrypted**.
6. Next, enter or select a Key ID or SO name in the **Select Key Encryption Key** section which will be used to unwrap (decrypt) the encrypted key in the file which will later be stored securely in Fortanix DSM. This key should have already been created or imported in Fortanix DSM.
7. Select the mode of operation.
8. Enter the **Key Check Value (KCV)**.
9. Click **UPLOAD A FILE** to upload the key file in **Raw**, **Base64**, or **Hex** format.
10. Select the permitted key operations.
11. Add custom attributes by clicking the **ADD ATTRIBUTE** button.

 **NOTE**: The custom attributes also depend on the Key metadata policy for the group. If the GCP KMS group has a Key metadata policy configured with restrictions for custom attributes, then these rules will be applied while creating the security object.

12. To store audit logs for the object in the group, enable the toggle for **Keep detailed log for the object**. The initial state of the toggle is based on the parent Crypto policy if any.
13. Click **IMPORT** to import the key in GCP KMS. The key is now successfully imported.

5.1.3 BRING YOUR OWN KEY – COPY KEY TO GCP KMS

Use this option when you want to generate a key in Fortanix DSM and then import the key into the configured GCP KMS. The copy key to GCP feature will copy a security object from one regular Fortanix DSM group to another regular/GCP KMS Fortanix DSM group. This feature has the following advantages:

- Maintains a single source of key material while using/importing that key into various Fortanix DSM groups where applications may need to use a single key to meet business objectives.
- Maintains a link of various copies of the same key material to the source key for audit and tracking purposes.

The following actions will happen as part of the copy key operation:

- A new key will be created in the target group: The new key will have the same key material as the original.
- The source key links to the copied keys: There will be a link maintained from all copied keys to the source key.
- The Source key will also have basic metadata-based information about the linked keys such as:
    - Copied by <user-name/app id>
    - Date of Copy <time stamp>
    - Target copy group name

NOTE: The name of the copied key is suggested automatically to the user `as [original key name]_[copy1,2,...]`, but can be replaced with an alternative unique name.

To copy a key from a regular Fortanix DSM group to a GCP KMS group:

1. Go to the detailed view to a key and click the **NEW OBJECT** icon on the far right of the screen.

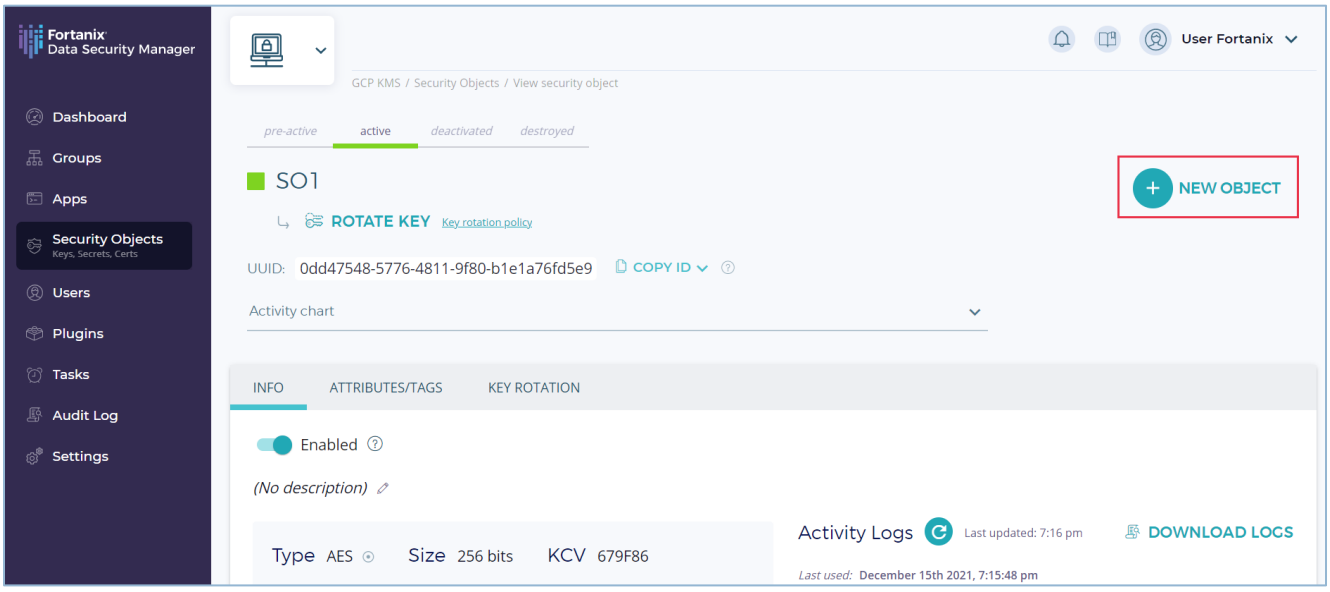

FIGURE 1: INITIATE COPY KEY

2. In the menu that appears, click the **COPY KEY** button.

NOTE:

- To copy a key from a regular Fortanix DSM group to a GCP KMS group, the key must be AES 256. In Fortanix DSM 4.4, GCP KMS only supports only AES 256 keys during copy or import operations.
- The AES 256 key to be copied must have the "Export" permission enabled or the copy key operation will fail.
- The **COPY KEY** button will be disabled for all the GCP KMS virtual keys.

3. In the **COPY KEY** window, update the name of the key if required.
4. Click the **Import key to HSM/External KMS** check box to filter the groups to show only GCP KMS groups. Select the GCP KMS group for the new key into which the copied key should be imported.
5. Enter the **GCP key name**.
6. Update **KEY PERMISSIONS** if you want to modify the permissions of the key.
7. Click **CREATE COPY** to create a copy of the key as shown in the figure above.
8. The source key will now appear as a key link in the **KEY LINKS** tab in the detailed view of the copied key.

NOTE: If a user wants to maintain a copy of the key material in Fortanix DSM, then the user can import a regular AES 256 key into Fortanix DSM using the "import key" workflow and then copy this key into GCP KMS using the "copy key" workflow.

5.2 SYNC KEYS

When you edit the GCP KMS connection details in the GCP KMS group detailed view under **HSM/KMS** tab, click **SYNC KEYS** to import new keys. On clicking **SYNC KEYS**, Fortanix DSM connects to GCP KMS and gets all the keys available. Fortanix DSM then stores them as virtual keys.

NOTE:

- When keys are synced with GCP KMS, the metadata of the existing keys for the configured service account and region are downloaded and represented as virtual keys in Fortanix DSM. The actual key material for those keys is always stored in GCP KMS.
- Clicking **SYNC KEYS** only returns the keys from GCP KMS that are not present in Fortanix DSM. That is, every click will append only new keys to Fortanix DSM.
- The time taken to sync keys from GCP KMS to Fortanix DSM is a function of the number of keys in the GCP KMS and the network latency between the GCP location and Fortanix DSM. It can take several minutes if there are hundreds of keys and there is significant network latency.

5.3 ATTRIBUTES/TAGS TAB

This tab will have all the tags of the GCP key.

5.4 GCP KEY DETAILS

This tab displays details of the **GCP key name** and **GCP protection level**. *For more details about GCP protection level, refer to the Google documentation*.

5.5 SECURITY OBJECTS TABLE VIEW

After you add new GCP keys, go to the **Security Objects** page to view all the security objects from all the groups (GCP and non-GCP).

In the security object table, you will notice that every key belongs to a group and some keys which are virtual keys added from a GCP KMS, belongs to a group with a special symbol  . The security objects table view will continue to show all the keys irrespective of if they belong to a GCP KMS group or not.

6.0 ROTATE A KEY IN GCP CDC GROUP

The following section explains the Key Rotation in the GCP CDC Group. A Key is rotated when you want to retire an encryption key and replace that old key by generating a new cryptographic key.

6.1 ROTATING GCP NATIVE KEY* WITH ANOTHER NATIVE KEY

*Native key is one where the key material was generated by GCP KMS.

When you rotate a virtual key in an GCP CDC group, the action will rotate the key inside the GCP KMS by generating another version of the key within the configured GCP KMS.

To rotate a key in GCP:

1. Select the GCP virtual key to rotate.
2. In the detailed view of the GCP virtual key, click the **ROTATE KEY** button.
3. In the Key Rotation window, click the **ROTATE KEY** button to rotate the virtual key.

   A new rotated key is now generated.

 **NOTE**: The following features will be supported in the upcoming Fortanix DSM releases:

- Rotate GCP native key to Fortanix DSM-owned key (**Rotate to DSM key**).
- Rotate keys in Fortanix DSM source group (**Rotate linked keys**).
- Key rotation policy for scheduling key rotation for GCP BYOK keys.

7.0 DOCUMENT INFORMATION

7.1 DOCUMENT LOCATION

The latest published version of this document is located at the URL:

https://support.fortanix.com/hc/en-us/articles/4423384427796-User-s-Guide-Google-Cloud-KMS

7.2 DOCUMENT UPDATES

This document will typically be updated on a periodic review and update cycle.

For any urgent document updates, please send an email to: support@fortanix.com