Fortanix®

User Guide

FORTANIX DATA SECURITY MANAGER – KEY OPERATIONS – COPY KEY

VERSION 2.2

Fortanix Inc. | 3910 Freedom Circle | Suite 104 | Santa Clara, CA 95052 | 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) User Guide. This document describes the Fortanix DSM Copy Key operation that can be performed on a Security Object.

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. You can add more users to the group in the role of administrators or auditors. You 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 REST 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 COPY KEY

The Copy Key feature of Fortanix DSM will allow the users to copy a security object from a standard Fortanix DSM group to another standard group. This feature has the following advantages:

- It maintains a single source of key material by using/importing that key with other Fortanix DSM groups. This allows applications in respective groups to use a single key to meet some business objectives.
- It maintains a link to copies of the original key material 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 key.
- The Source key links to the copied keys: A link will be maintained between all copied keys and 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.

Perform the following steps to copy a key:

1. Go to the detailed view of a key and click the **Copy Key** 

button on the right of the screen.
2. In the **COPY KEY** window, you may update the name of the key by clicking on the pencil icon. Copy the new key to a group(s) from the **GROUP** section. To filter only HSM/External KMS groups, select **Import key to HSM/External KMS** option.

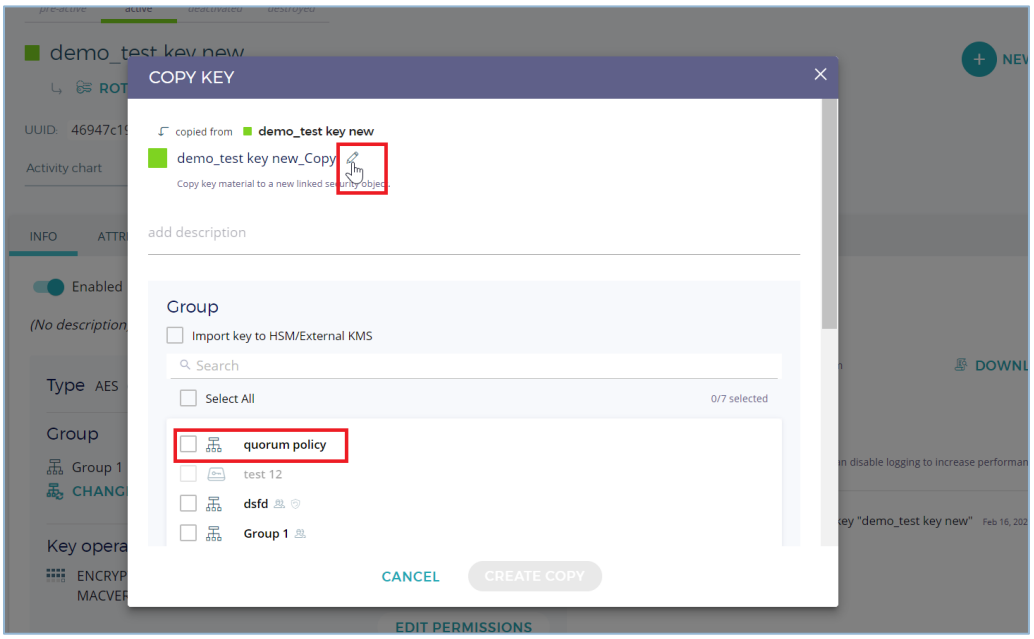

FIGURE 1: EDIT KEY NAME AND ASSIGN TO GROUP

3. Click **EDIT PERMISSIONS** if you want to modify the permissions of the key.

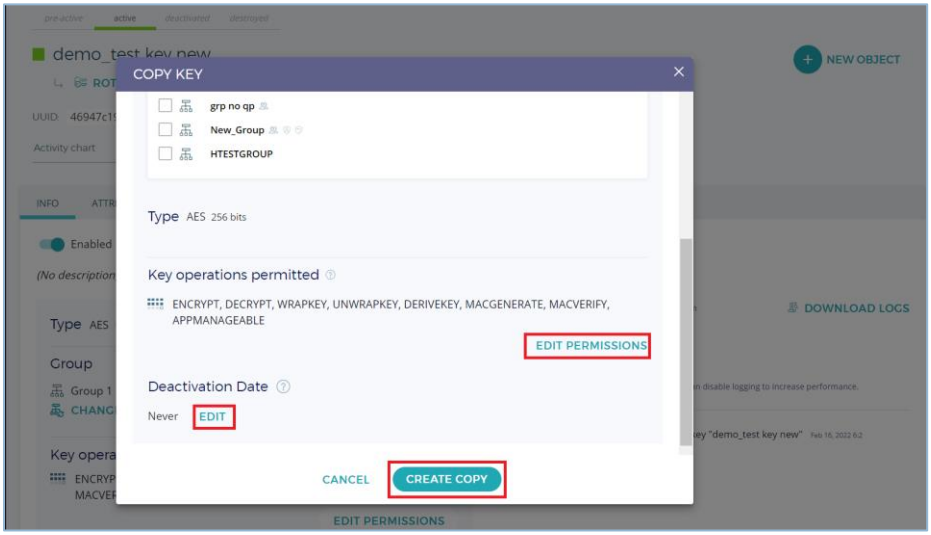

FIGURE 2: SET DEACTIVATION DATE

4. Add **Deactivation Date**: The deactivation date of the security object can be set to 'Never' or to a specified time in the future. To specify the deactivation date, click **EDIT.**
5. Click **CREATE COPY** to create a copy of the key.

6. If there is Quorum policy configured in the source group that contains the original key, then a quorum approval request is created. Only after the request is approved the copy key operation will be successful.
7. The source key will now appear as a key link in the **KEY LINKS** tab in the detailed view of the copied key.

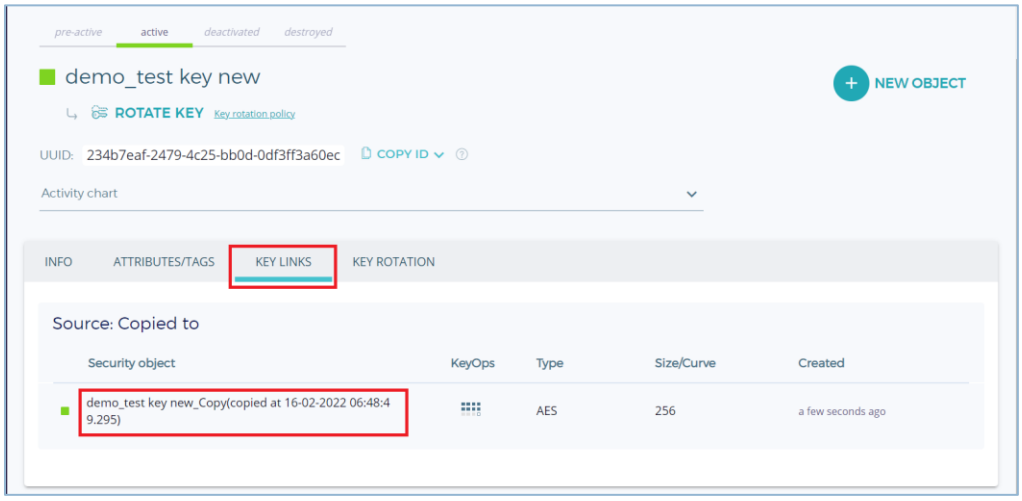

FIGURE 3: KEY LINK CREATED

4.0 CREATE NEW AES KEY

Fortanix DSM allows you to create a new AES key with the similar settings as the currently available key.

Perform the following steps:

1. Go to the detailed view of a key and click the 

button on the right of the screen.
2. On the **Add New Security Object** window, enter the name of the security object in **New Security Object** field.
3. You can make update the existing values in the sections as required.
4. After you have updated the values, click the **Generate** button at the bottom of the screen.

The new AES key is generated in Fortanix DSM.

5.0 DOCUMENT INFORMATION

5.1 DOCUMENT LOCATION

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

https://support.fortanix.com/hc/en-us/articles/360049737111-User-s-Guide-Copy-Key

5.2 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