

# User Guide

## FORTANIX DATA SECURITY MANAGER – KEY OPERATIONS – COPY KEY

---

## TABLE OF CONTENTS

<b>1.0</b>	<b>INTRODUCTION .....</b>	<b>2</b>
<b>2.0</b>	<b>DEFINITIONS.....</b>	<b>2</b>
<b>3.0</b>	<b>COPY KEY .....</b>	<b>4</b>
<b>4.0</b>	<b>DOCUMENT INFORMATION .....</b>	<b>10</b>
<b>4.1</b>	<b>Document Location .....</b>	<b>10</b>
<b>4.2</b>	<b>Document Updates.....</b>	<b>10</b>
<b>4.3</b>	<b>Revision History.....</b>	<b>Error! Bookmark not defined.</b>



---

## 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.

To copy a key:

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

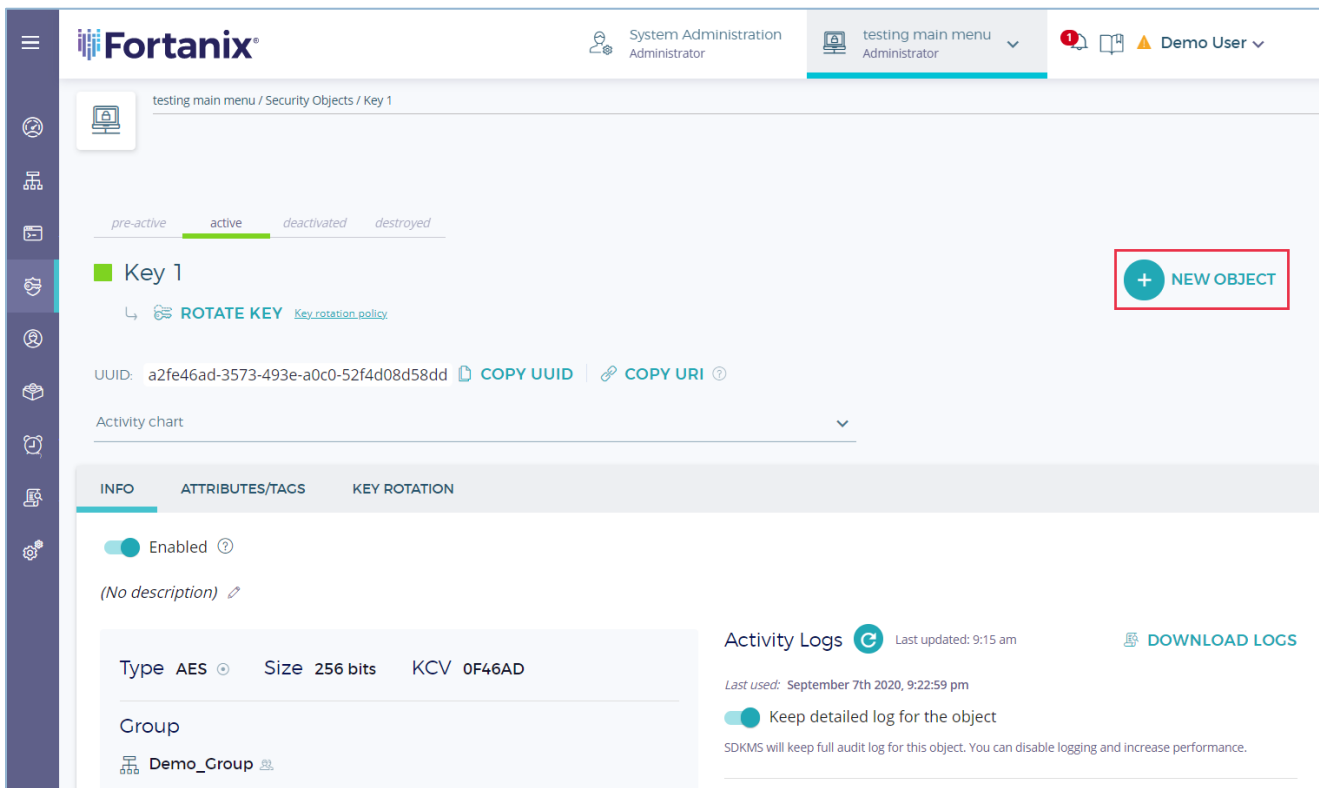



FIGURE 1: INITIATE COPY KEY

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



The screenshot shows the Fortanix Data Security Manager interface. At the top, there is a navigation bar with the Fortanix logo, user roles (System Administration Administrator and testing main menu Administrator), and a user profile (Demo User). The main content area is titled 'testing main menu / Security Objects / Key 1'. Below the title, there are tabs for 'pre-active', 'active', 'deactivated', and 'destroyed', with 'active' selected. A 'NEW OBJECT' button is visible in the top right. A 'COPY KEY' button is highlighted with a red box. Below this, there is a 'CREATE NEW AES KEY' button. The main content area also displays the key name 'Key 1', a 'ROTATE KEY' button, and the key's UUID. Below the UUID, there are 'COPY UUID' and 'COPY URI' buttons. An 'Activity chart' is also present. The bottom section of the interface shows the 'INFO' tab, which includes a toggle for 'Enabled', a description '(No description)', and key details: 'Type AES', 'Size 256 bits', and 'KCV 0F46AD'. There is also an 'Activity Logs' section with a 'DOWNLOAD LOGS' button and a toggle for 'Keep detailed log for the object'.

FIGURE 2: CLICK COPY KEY

3. 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/groups from the **GROUP** section. To filter only HSM/External KMS groups, select **Import key to HSM/External KMS** option.

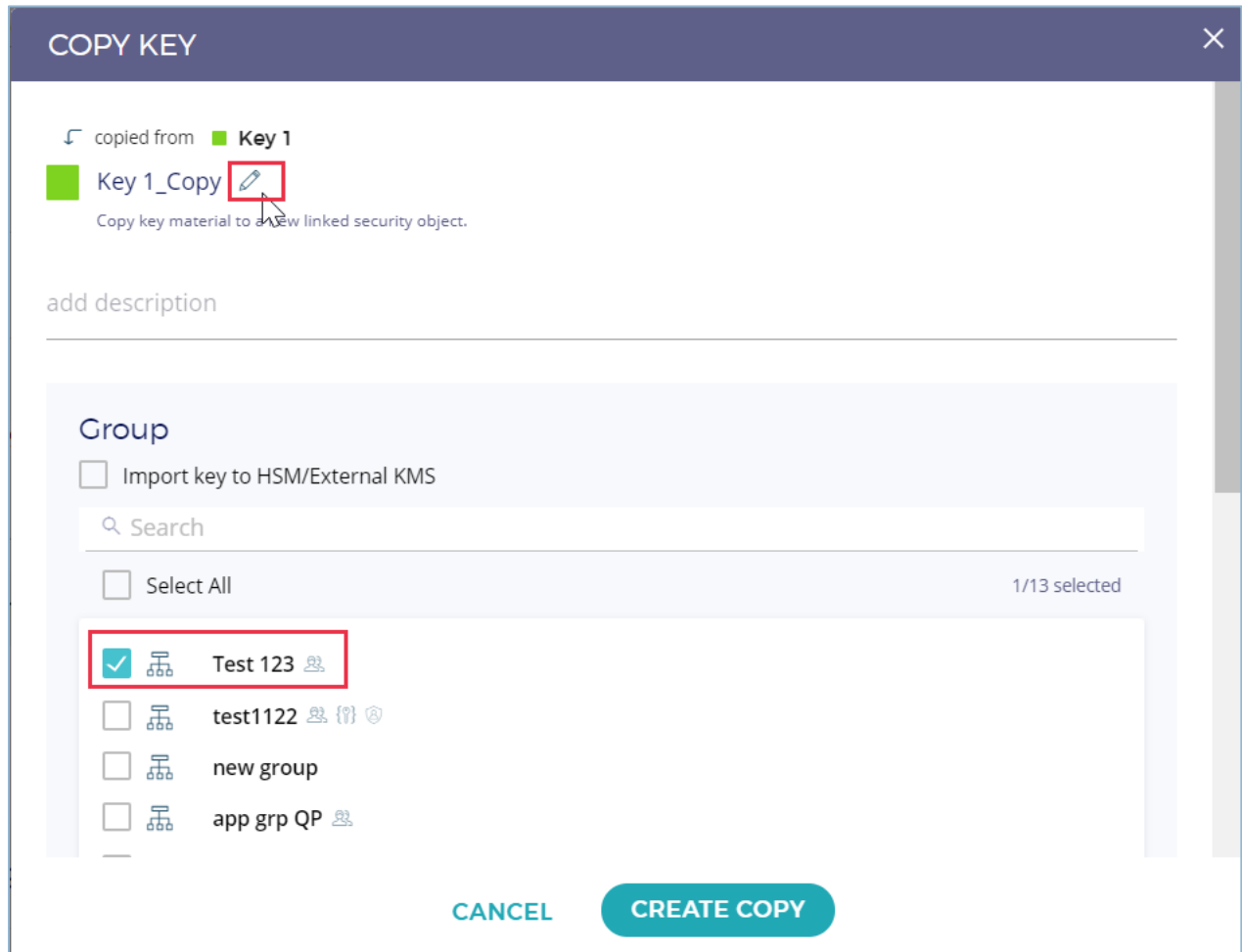


FIGURE 3: EDIT KEY NAME AND ASSIGN TO GROUP

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



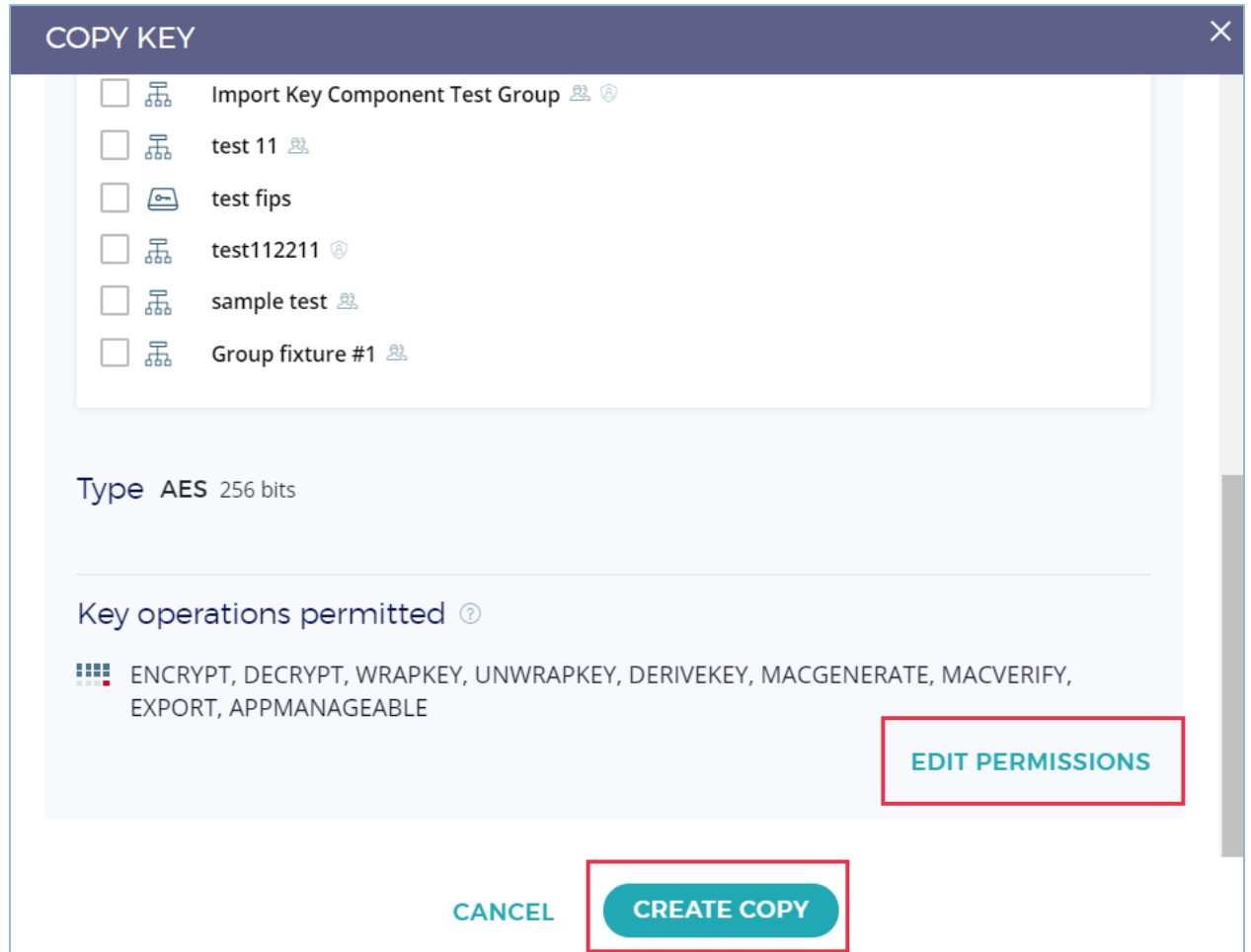


FIGURE 4: ASSIGN NEW KEY TO A GROUP

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.

The screenshot shows the Fortanix Data Security Manager interface. At the top, there is a navigation bar with the Fortanix logo, user roles (System Administration Administrator and testing main menu Administrator), and a demo user profile. The main content area displays the details for a security object named 'Key 1\_Copy'. The object is currently in an 'active' state. Below the name, there is a 'ROTATE KEY' button and a link to the 'Key rotation policy'. The UUID is 'bc409d96-b3c2-462d-8b1d-b90c45530656', with links for 'COPY UUID' and 'COPY URI'. An activity chart is visible below this information. The 'KEY LINKS' tab is selected and highlighted with a red box. It shows a table with one entry: 'Key 1' is the source of the copy. The table has columns for 'Security object', 'KeyOps', 'Type', 'Size/Curve', and 'Created'. The 'Key 1' entry is also highlighted with a red box.

testing main menu / Security Objects / Key 1\_Copy

pre-active active deactivated

Key 1

Key 1\_Copy

ROTATE KEY Key rotation policy

UUID: bc409d96-b3c2-462d-8b1d-b90c45530656 COPY UUID COPY URI

Activity chart

INFO ATTRIBUTES **KEY LINKS** KEY ROTATION

Source: Copied from

Security object	KeyOps	Type	Size/Curve	Created
Key 1		AES	256	a month ago

FIGURE 5: KEY LINK CREATED



---

## 4.0 DOCUMENT INFORMATION

---

### 4.1 DOCUMENT LOCATION

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

<https://support.fortanix.com/hc/en-us/articles/360049737111>

---

### 4.2 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](mailto:support@fortanix.com)

© 2016 – 2021 Fortanix, Inc. All Rights Reserved.

Fortanix® and the Fortanix logo are registered trademarks or trade names of Fortanix, Inc.

All other trademarks are the property of their respective owners.

**NOTICE:** This document was produced by Fortanix, Inc. (Fortanix) and contains information which is proprietary and confidential to Fortanix. The document contains information that may be protected by patents, copyrights, and/or other IP laws. If you are not the intended recipient of this material, please destroy this document and inform [info@fortanix.com](mailto:info@fortanix.com) immediately.