## Fortanix<sup>®</sup>

# User Guide

# FORTANIX DATA SECURITY MANAGER – KEY OPERATIONS – COPY KEY

**VERSION 2.2** 



#### TABLE OF CONTENTS

1.0 INTRODUCTION	2
2.0 DEFINITIONS	2
3.0 COPY KEY	
4.0 CREATE NEW AES KEY	6
5.0 DOCUMENT INFORMATION	7
	_
5.1 Document Location	7
5.2 Document Updates	7
•	
5.3 Revision History	Error! Bookmark not defined.



#### **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 <u>support</u> 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:

- o 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 <u>support</u> 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 <u>Authorization</u> 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 <u>Quorum Policy</u> 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 <u>support</u> 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.
- 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.



	× + NEV
UUID.       46947c1!       Copied from demo_test key new         Activity chart       demo_test key new_Copy Copy key material to a new linked se why object.         INFO       ATTR:       add description	
Croup No description Import key to HSM/External KMS Search	Down
Type AES     Select All     0/7 selected       Croup	in disable logging to increase performan
Image: Second state state     Image: Second state state       Image: Second state state     Image: Second state state       Image: Second state state     Image: Second state state       Image: Second state state     Image: Second state       Image: Second state     Image: Se	tey "demo_test key new" Feb 16, 202

FIGURE 1: EDIT KEY NAME AND ASSIGN TO GROUP

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

	t kev new COPY KEY		+ NEW OBJECT
JUID: 46947c1! Activity chart	표     grp no qp 표       표     New Group 표 0 0       표     HTESTGROUP	1	
INFO ATTR	Type AES 256 bits	ł	
(No description	Key operations permitted 💿	- 88	
Type AES	ROCRYPT, DECRYPT, WRAPKEY, UNWRAPKEY, DERIVEKEY, MACGENERATE, MACVERIFY, APPMANAGEABLE     EDIT PERMISSIONS	l	# DOWNLOAD LOCS
品 Group 1 高 CHANG	Deactivation Date ⑦ Never EDIT	in dis	able logging to increase performance.
Key opera ENCRYP	CANCEL CREATE COPY	dey c	zemo_test key new 196016,2022.02

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.

pre-active active deactivated destroyed				
demo_test key new				+ NEW OBJECT
UUID: 234b7eaf-2479-4c25-bb0d-0df3ff3a60ec	ID 🗸 🕜			
Activity chart			~	
INFO ATTRIBUTES/TAGS KEY LINKS KEY ROTATI	ION			
Source: Copied to				
Security object	KeyOps	Туре	Size/Curve	Created
demo_test key new_Copy(copied at 16-02-2022 06:48:4 9.295)		AES	256	a few seconds ago

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:

- Go to the detailed view of a key and click the Create a new key with similar settings button on the right of the screen.
- 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.

### 🐺 Fortanix<sup>®</sup>

#### **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: <a href="mailto:support@fortanix.com">support@fortanix.com</a>

© 2016 – 2023 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 <u>info@fortanix.com</u> immediately.