Fortanix®

User Guide

FORTANIX DATA SECURITY MANAGER –KEY MOVE

Fortanix Inc. | 800 West El Camino Real | Suite 180 | Mountain View, CA 94040 | 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 steps to move a key from one Fortanix DSM group to another there by modifying the group that the key belongs to.

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 MOVE KEY

The Key Move feature of Fortanix DSM will allow the users to move a security object from a standard Fortanix DSM group to another standard Fortanix DSM group.

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

- The key will be moved from the source group to the target group: The new key will have the same key material as the original key.
- The key links will remain with the source group and will not be moved to the target group when the key material is moved. Key links must be updated to use the new group that the key material resides in.
- The Key Rotation Policy also moves to the target group along with the key.

 **NOTE**:

- The key move operation is applicable for keys in Fortanix DSM groups only.
- The key move operation is applicable for all the key types.
- You can move keys only between two Fortanix DSM groups.
- The key has to satisfy the target group's cryptographic policy in order for the move to be successful.
- You must have "write" access to both groups to perform the key move operation.
- The key can be moved in any state except the `DELETED` state.
- If there is a quorum policy associated with the source group, then it applies. Otherwise, group change is immediate.
- If the key is moved to a group with a different Key Undo Policy, then the Key Undo Policy of the target group applies to the key.
- If the key is moved to a group without a Key Undo Policy, then the existing Key Undo Policy of the source group stays in the source group.
- The users, apps, and plugins of the source group will no longer have access to the key once the group is changed.

To move a key:

1. Go to the detailed view to a key. In the **INFO** tab, under the **Group** section, click **CHANGE GROUP** to initiate the key move operation.

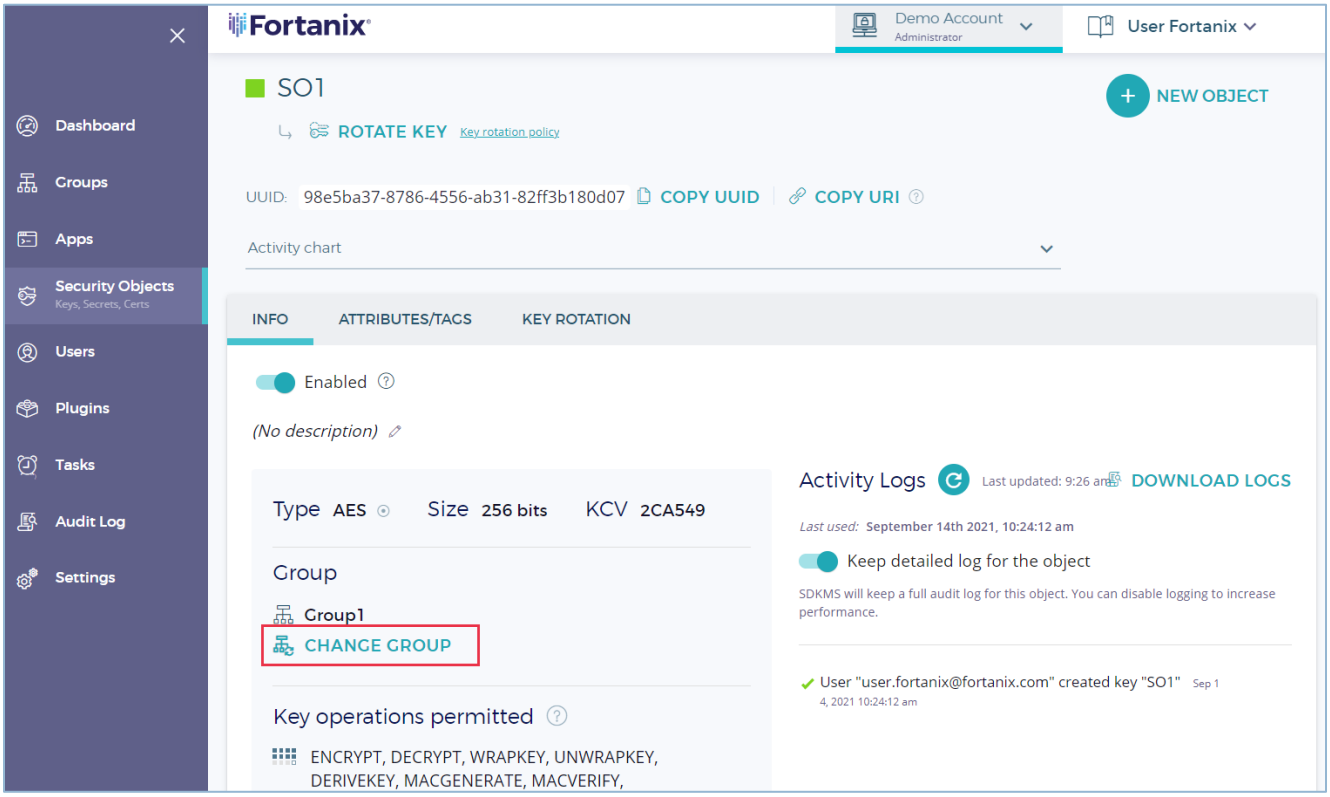

FIGURE 1: INITIATE KEY MOVE

2. In the CHANGE GROUP dialog:
    a. Select the destination group to move the key to.
    b. Select the check box to confirm that:
        i. The users, apps, and plugins will no longer have access to the key once the group is changed and key links will be lost.
    c. Click **SAVE** to move the key to the new group.

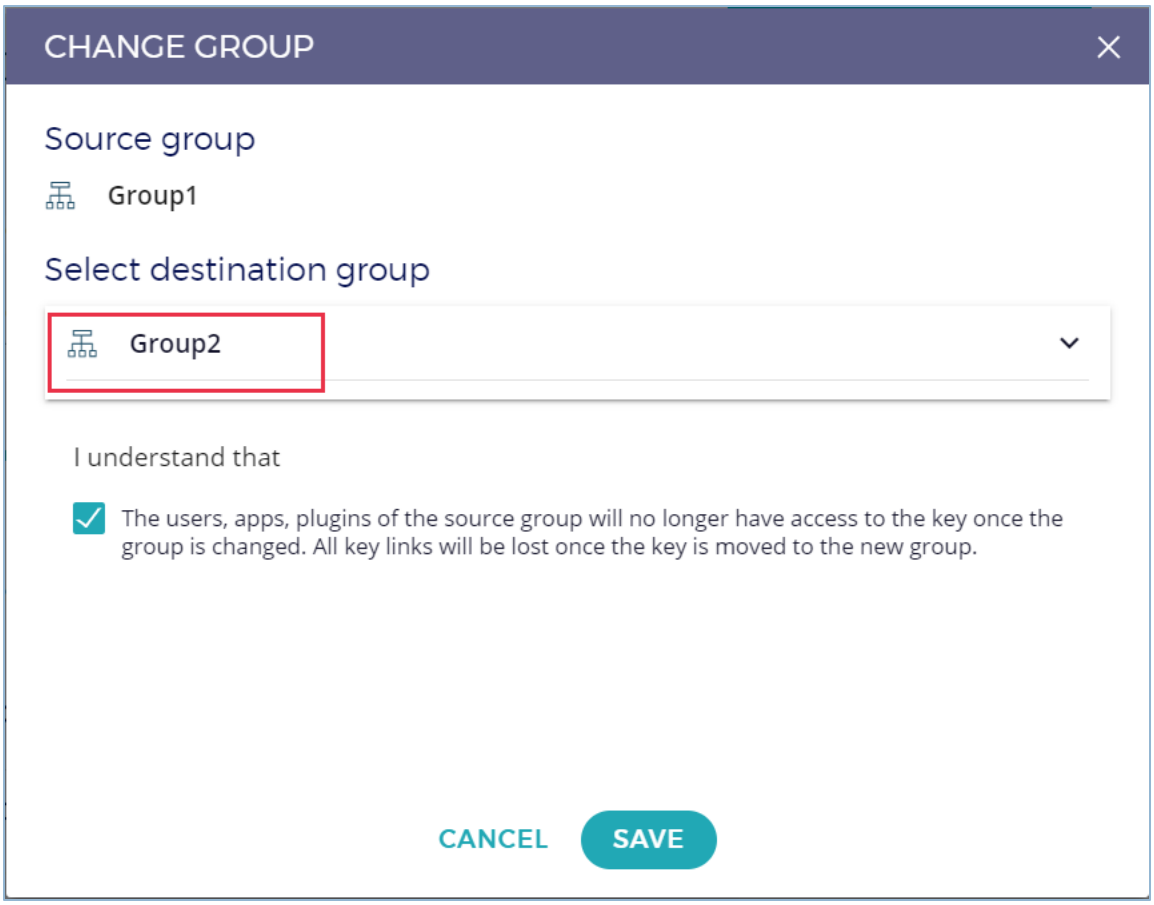

FIGURE 2: CHANGE GROUP

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/4407467898260-User-s-Guide-Key-Move

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