

User Guide

FORTANIX DATA SECURITY MANAGER - GROUP KEY ENCRYPTION KEY (KEK)

VERSION 1.0

TABLE OF CONTENTS

1.0	INTRODUCTION.....	2
2.0	DEFINITIONS.....	2
3.0	CREATE A KEK AND CONFIGURE A GROUP WITH KEK.....	4
3.1	Creating a Group with a New KEK.....	4
3.2	Configuring a Group with a KEK.....	5
4.0	USER KEY OPERATIONS ON A KEK.....	6
4.1	Setting the Key Rotation Policy for a KEK.....	6
4.2	Rotating a KEK.....	6
4.3	Replacing the KEK of a Group.....	6
4.4	Removing the KEK from a Group.....	7
4.5	Deactivating, Disabling/Enabling, Deleting, or Destroying a KEK.....	7
5.0	QUORUM APPROVAL SCENARIOS.....	8
5.1	Assumptions.....	8
5.2	Creating a Group with KEK.....	8
5.3	Removing KEK from a Group.....	8
5.4	Replacing KEK of a Group.....	9
6.0	DOCUMENT INFORMATION.....	10
6.1	Document Location.....	10
6.2	Document Updates.....	10

1.0 INTRODUCTION

Welcome to the Fortanix Data Security Manager (DSM) User Guide. This document describes the Fortanix DSM group “key encryption key” (KEK) feature. This feature allows users to establish a group-level root-of-trust and ensures that all keys generated inside a group always stay encrypted by a symmetric master key (KEK) that the user configured at the group level. If the group KEK is rotated, then new keys in the group will be encrypted with the new version of KEK while older keys in the group stay encrypted with the older KEK. If the group KEK is disabled/deleted/destroyed/revoked, then all the keys in the group will be rendered unusable. The user also cannot generate new keys in the group.

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.*



- **Key Encryption Key (KEK)** –

A key encryption key (KEK) is a cryptographic key that is used for encrypting other cryptographic keys.

3.0 CREATE A KEK AND CONFIGURE A GROUP WITH KEK

3.1 CREATING A GROUP WITH A NEW KEK

To create a group with KEK, follow the steps below:


1. In the Fortanix DSM UI, click the **Groups** tab, and then click  to create a new group.
2. Enter a name for the group. For example, **KEKGroupA**.
3. Enter a description to help you identify that this is a group with KEK. (Optional)
4. Click **CREATE GROUP** to create the group.
5. Click the **Security Objects** tab, and then click  to create a new key.
6. Enter a name for the key. For example, **KEK-A**.
7. Ensure that the KEK group that you have created is selected under the **Select group for the object** section.
8. To configure the key, you can do one of the following:
 - a. Select **IMPORT** to start the key import workflow.
 - i. Select **AES** as the key type.
 - ii. Select **Raw** as the value format.
 - iii. Click **UPLOAD A FILE** and select the key file that you want to import.
 - iv. Disable the **Audit log** option for the key.
 - v. Click **IMPORT** to import the key.
 - b. Select **GENERATE** to start the key generation workflow.
 - i. Select **AES** as the key type.
 - ii. For **Key size**, leave it as the default **256** bits.
 - iii. Disable the **Audit log** option for the key.
 - iv. Click **GENERATE** to create the key.

**NOTE:**

- It is mandatory to disable the **Audit log** option while creating the group KEK key (AES key). Otherwise, the KEK key will not appear for selection in the **Configure a KEK from an existing group** wizard.
- Disabling the Audit log for the group KEK key will also avoid a large volume of logs from being generated since a KEK can wrap a large number of keys.

3.2 CONFIGURING A GROUP WITH A KEK

To configure a group with an existing KEK, follow the steps below:

1. In the Fortanix DSM UI, click the **Groups** tab, and then click  to create a new group.
2. Enter a name for the group. For example, **NormalGroup**.
3. Enter a description to help you identify that this is a group with KEK. (Optional)
4. In the Configure a KEK from an existing group section, click **CONFIGURE A KEK**.
5. Select the group that contains the KEK you want to use for this group.
6. From the KEK list that appears for that group, select a KEK.
7. Click **SAVE** to create the group.



NOTE: If the group that is configured with a KEK has some existing keys already, these keys will not be encrypted with the configured KEK. Only new keys that are created after configuring the group with KEK will be encrypted with the KEK.

Go to the group detailed view to check the following:

- The key ID and key name of the KEK associated with the group.
- If the KEK has been rotated, then this page will also show the key IDs and names of the older keys.
- If the KEK is disabled, this page will display the message: "This Group's KEK is disabled. All the key operations in this Group are no longer available."

4.0 USER KEY OPERATIONS ON A KEK

4.1 SETTING THE KEY ROTATION POLICY FOR A KEK

To set the key rotation policy for a KEK:

1. Click the **Groups** tab, and then click the group name from the table to go to the group detailed view page.
2. Click the **KEY ROTATION** tab.
3. In the **Key rotation policy** section, click **ADD POLICY**.
4. Enter the policy details. For example: Rotate all keys in this group every **7** days starting **10/15/2022 12:00 pm**.
5. If you select **Deactivate original key after rotation** check box, all the existing keys encrypted/wrapped by this KEK will be rendered unusable upon rotation.
6. Click **SAVE POLICY** to save the policy.

4.2 ROTATING A KEK

To rotate a KEK:

1. Click the **Security Objects** tab, and then click the KEK name to go to the KEK detailed view page.
2. Click **ROTATE KEY**, and on the “Key Rotation” modal window click **ROTATE KEY** again.



NOTE: This page has a check box that states **Deactivate the key after rotation**. If you select this check box, all the existing keys encrypted/wrapped by this key will be rendered unusable upon rotation.

4.3 REPLACING THE KEK OF A GROUP

To replace a group’s KEK:

1. Click the **Groups** tab, and then click the group name that is configured with a KEK to go to the group detailed view page.
 2. Under the group name, click **EDIT** next to the label “This group is encrypted by Key Encryption Key”.
 3. On the “Edit KEK” modal window, select the option **Replace with another KEK**.
 4. Select the group that contains the KEK you want to use.
-

5. From the list of KEK in this group, select the KEK you want to use.
6. Click **SAVE** to set the new key as the KEK for the group.



NOTE: The old KEK can still be used to encrypt and decrypt the existing keys in the group while the new KEK will be used to encrypt and decrypt the new keys in the group.

If A KEK key is compromised, you can do one of the following:

- Either rotate the KEK and disable/deactivate the older version of the KEK. In this method, the existing keys configured with the older KEK will all be rendered unusable. **This is the preferred method.**
- Delete KEK from this group and generate a new KEK. To do this, all keys that were encrypted with this key have to be deleted first, thereby breaking the association between the KEK and groups.


4.4 REMOVING THE KEK FROM A GROUP

To remove the KEK from a group:

1. Click the group name containing the KEK to go to the group detailed view page.
2. Under the group name, click **EDIT** next to the label “This group is encrypted by Key Encryption Key”.
3. Select **Remove KEK associated with the group.**
4. Click **SAVE** to remove the KEK from the group.

4.5 DEACTIVATING, DISABLING/ENABLING, DELETING, OR DESTROYING A KEK

To deactivate, disable/enable, delete, or destroy the KEK from a group:

1. Click the **Security Objects** tab, and then click the KEK name to go to the KEK detailed view page.
2. Click  (Enable/Disable toggle bar) to enable or disable the KEK.
3. To deactivate the KEK:
 - a. In the **Expires** section, click **DEACTIVATE NOW.**
 - b. In the modal window, select the check box next to “I understand that deactivation is irreversible, and the object cannot be activated back.”
 - c. Click **DEACTIVATE** to deactivate the KEK.

- To delete or destroy a key click **DELETE KEY** or **DESTROY KEY** respectively at the bottom of the KEK detailed view page.



NOTE: Fortanix DSM does not allow users to destroy a key that is also associated with other groups.

5.0 QUORUM APPROVAL SCENARIOS

5.1 ASSUMPTIONS

For the purpose of this section, we are using the following naming conventions:

- **KEKGroupA** - This is a group that contains an AES 256 key and has a Quorum approval policy configured.
- **KEKGroupB** - This is another group that contains an AES 256 key and has a Quorum approval policy configured.
- **KEK-A** - This is an AES 256 key that is added to the **KEKGroupA** group.
- **KEK-B** - This is an AES 256 key that is added to the **KEKGroupB** group.
- **NormalGroupA** - This is a normal group that will configure a KEK key and also has a Quorum approval policy configured.

5.2 CREATING A GROUP WITH KEK

- If a group "**KEKGroupA**", has a key "**KEK-A**" in it. If another group "**NormalGroup**" is configured with "**KEK-A**" as its KEK key, then this action triggers a Quorum approval request to the approvers of the group "**KEKGroupA**" and "**NormalGroup**".

5.3 REMOVING KEK FROM A GROUP

- If a group "**KEKGroupA**", has a key "**KEK-A**" in it. If another group "**NormalGroup**" is configured with "**KEK-A**" as its KEK key (generates a Quorum approval request to the approvers of both the groups). Now, if "**KEK-A**" is removed as the KEK of "**NormalGroup**", then:
 - A Quorum approval request is generated to the approvers of "**KEKGroupA**" because "**KEK-A**" is being removed.
 - A Quorum approval request is generated to the approvers of "**NormalGroup**" because the "**NormalGroup**" is being updated.

5.4 REPLACING KEK OF A GROUP

- If a group **"KEKGroupA"**, has a key **"KEK-A"** in it. If another group **"KEKGroupB"**, has a key **"KEK-B"** in it. If the third group **"NormalGroup"** is configured with **"KEK-A"** as its KEK key (generates a Quorum approval request to the approvers of **"KEKGroupA"** and **"NormalGroup"** groups). Now, if the KEK key **"KEK-A"** of the **"NormalGroup"** is replaced with the KEK key **"KEK-B"** then:
 - A Quorum approval request is generated to the approvers of **"KEKGroupA"** because **"KEK-A"** is being removed.
 - A Quorum approval request is generated to the approvers of **"KEKGroupB"** because **"KEK-B"** is being added as a KEK.
 - A Quorum approval request is generated to the approvers of **"NormalGroup"** because the **"NormalGroup"** is being updated.

6.0 DOCUMENT INFORMATION

6.1 DOCUMENT LOCATION

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

<https://support.fortanix.com/hc/en-us/articles/8144952406932-User-s-Guide-Group-Key-Encryption-Key>

6.2 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

© 2016 – 2022 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 immediately.