Fortanix®

User Guide

FORTANIX DATA SECURITY MANAGER - STORE KEYS EXTERNALLY – KEY MANAGEMENT GUIDE

VERSION 1.0

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) Store Keys Externally guide using a DSM-backed group guide. This document describes the key management operations performed on a Fortanix DSM-backed group. The document also describes the following:

- Generating/importing/copying a key in the Fortanix DSM primary group.
- Deleting a key in the Fortanix DSM primary group.
- Rotating a key in the Fortanix DSM primary group.

1.1 INTENDED AUDIENCE

This document is intended to be used by technical stakeholders of Fortanix DSM who will be responsible for planning, performing, or maintaining the installation or Deployment of DSM and Extended Virtual keys, such as the Architects, Systems Administrator, Chief Information Officer (CIO), Analysts, or Developers.

2.0 EXTENDED VIRTUAL KEYS CONCEPTS

Refer to the DSM Extended Virtual Keys – Concepts guide.

3.0 TERMINOLOGY REFERENCES

- **DSM –** Data Security Manager
- **EKV – Extended Virtual Keys**
- **Fortanix DSM secondary group** – This is the Fortanix DSM-backed group.
- **Fortanix DSM primary group –** This is the External DSM group that is going to be configured in the Fortanix DSM secondary group.
- **Fortanix DSM primary key –** This is the actual key present in the Fortanix DSM primary group containing the key material.
- **Fortanix DSM secondary key –** This is the virtual representation of the Fortanix DSM primary key.

4.0 FORTANIX DSM SOURCE GROUP SECURITY OBJECTS

Following a successful connection between the Fortanix DSM secondary cluster and the Fortanix DSM primary cluster using the connection details described in the "Fortanix DSM - Store Keys Externally -- Setup Guide," the keys from the DSM primary group are stored in the DSM secondary

group as "virtual keys" following a key scan operation on the DSM primary group. A virtual key in this scenario is a key that may or may not have the key material, depending on the Extended Virtual Key's **Fetch Key Material** configuration that caches the key material, as explained in the <Fortanix DSM - Store Keys Externally – Setup Guide>. If the key material of the keys is cached in the DSM secondary group, cryptographic operations with these keys are not proxied to the linked primary group.

NOTE: In DSM 4.13:

- The allowed key types for a primary key generated using the Generate/Import Key button are AES, DES, DES3, EC, and RSA.
- The allowed key types for a primary key generated using the DSM Generate REST APIs are AES, DES, DES3, EC, RSA, HMAC, Tokenization, ARIA, SEED, and LMS.
- All key types are allowed for a primary key imported using the DSM Import REST APIs.
- If you create an LMS key in the Fortanix DSM primary group, then the key is considered to be non-exportable for Extended Virtual Keys. Hence, when you perform a key scan in the Fortanix DSM secondary group, the LMS virtual key can never cache the key material.

These key types can further be restricted by setting a crypto policy for the account or group. For more details about the crypto policy, *please refer to the article:* *https://support.fortanix.com/hc/en-us/articles/360042064051-User-s-Guide-Crypto-Policy*.

4.1 GENERATE A KEY IN FORTANIX DSM PRIMARY GROUP

You can generate a key in a configured Fortanix DSM primary group.

This action will generate the configured key type in the Fortanix DSM primary group directly, and it will be represented as a virtual key in the corresponding Fortanix DSM secondary group. The virtual key only stores the key information and key attributes, and it may or may not have the key material depending on the **Fetch Key Material** configuration.

In your Fortanix DSM console, follow the process below to create a new key:

1. Click the **Security Objects** tab.
2. Click to create a new Security Object.
3. In the **Add New Security Object** form enter a name for the Security Object (Key).

4. Select the **This is an HSM/external KMS object** check box. This will show the HSM/External KMS configured groups in the **Select group** list.
5. From the list of groups, select the Fortanix DSM primary group into which the keys will be generated.
6. Select **GENERATE** to initiate key generation in the DSM primary group workflow.
7. Select the key type for the new DSM source key.
8. Enter the **Key size** and select the permitted key operations under **Key operations permitted** section.

   NOTE: When you create a key in the Fortanix DSM secondary group without the **Export** permission, the **Export** permission is automatically added to the actual key in the Fortanix DSM primary group.
9. Click the **GENERATE** button to generate the key in the Fortanix DSM primary group.
10. To create Extended Virtual Keys by caching the key material of the primary key in the secondary group:
    a. Go to the detailed view of the secondary group.
    b. Click the **HSM/KMS** tab.
    c. Select the check box **Fetch Key Material**.
    d. Click **SYNC KEYS** to cache the key material in the secondary group.
11. The new primary key is created and represented with a special symbol in the secondary group that indicates it is a virtual representation of the primary key. In the detailed view of the virtual key, you will notice the following things:
    - The group to which it belongs (in the **Group** field). It also shows if the group is mapped to a DSM group using the special icon .
    - How the key was created (in the **Created by** field). This field shows the group that created this key. It also shows minor details such as if the group is "Connected" or "Not Connected".
12. The new key will be added to the Security Objects table.

Tip:

- You can also access the new key from the Group detailed view from the **SECURITY OBJECTS** tab.

4.2 IMPORT KEY IN FORTANIX DSM SOURCE GROUP

This action will import the configured key type in the Fortanix DSM primary group directly, and it will be represented as a virtual key in the corresponding Fortanix DSM secondary group. The virtual key only stores the key information and key attributes, and it may or may not have the key material depending on the **Fetch Key Material** configuration.

1. Click the **Security Objects**  tab.
2. Click  to create a new Security Object.
3. In the **Add New Security Object** form enter a name for the Security Object (Key).
4. Select the **This is an HSM/external KMS object** check box. This will show the HSM/External KMS configured groups in the **Select group** list.
5. From the list of groups, select the Fortanix DSM primary group into which the keys will be imported.
6. Select **IMPORT** to initiate the import key in the DSM primary group workflow.
7. Select the key type for the new DSM primary key.
8. Sometimes keys that need to be imported from a file were previously wrapped (encrypted) by a key from Fortanix DSM. This is done so that the key should not go over the TLS in plain text format. In such scenarios select the check box **The key has been encrypted**.
9. Next enter or select a Key ID or SO name in the **Select Key Encryption Key** section which will be used to unwrap (decrypt) the encrypted key in the file which will later be stored securely in Fortanix DSM. This key should have already been created or imported into Fortanix DSM.
10. Click **UPLOAD A FILE** to upload the key file in **Raw**, **Base64**, or **Hex** format.
11. Select the permitted key operations under **Key operations permitted** section.

 **NOTE**: When you import a key in the Fortanix DSM secondary group without the **Export** permission, the **Export** permission is automatically added to the actual key in the Fortanix DSM primary group.

12. Click **IMPORT** to import the key.
13. To create Extended Virtual Keys by caching the key material of the primary key in the secondary group:
    a. Go to the detailed view of the secondary group.

b. Click the **HSM/KMS** tab.

c. Select the check box **Fetch Key Material**.

d. Click **SYNC KEYS** to cache the key material in the secondary group.

4.3 COPY KEY TO FORTANIX DSM PRIMARY GROUP

Use this option when you want to generate a key in Fortanix DSM and then import the key into the configured Fortanix DSM primary group. The copy key to the DSM primary group feature will copy a security object from one regular Fortanix DSM group to another regular Fortanix DSM group.

This feature has the following advantages:

- Maintains a single primary key (from regular DSM group) while copying/importing that key into various Fortanix DSM groups where applications may need to use a single key to meet business objectives.
- Maintains a link of various copies of the same key material to the primary key (from regular DSM group) for the ability to name, and rotate keys everywhere all at once, as well as 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 (Fortanix DSM primary group): The new key will have the same key material as the original key.
- The source key (from the regular DSM group) links to the copied keys: There will be a link maintained from all copied keys to the source key (from the regular DSM group).
- The source key (from the regular DSM group) 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 from a regular Fortanix DSM group to an Fortanix DSM primary group:

1. Go to the detailed view of a key and click the **NEW OBJECT** icon on the far right of the screen.
2. In the menu that appears, click the **COPY KEY** button.

NOTE:

- The key to be copied must have the "Export" permission enabled, or the copy key operation will fail.

3. In the **COPY KEY** window, update the name of the key if required.
4. Click the **Import key to HSM/External KMS** check box to filter the groups to show only HSM/External groups. Select the secondary group for the new key into which the copied key should be imported.
5. Update **KEY PERMISSIONS** if you want to modify the permissions of the key.
6. Click **CREATE COPY** to create a copy of the key.
7. The source key (from the regular DSM group) will now appear as a key link in the **KEY LINKS** tab in the detailed view of the copied key.
8. To create Extended Virtual Keys by caching the key material of the source key (from the regular DSM group) in the Fortanix DSM secondary group:
   a. Go to the detailed view of the Fortanix DSM secondary group.
   b. Click the **HSM/KMS** tab.
   c. Select the check box **Fetch Key Material**.
   d. Click **SYNC KEYS** to cache the key material of the copied key in the Fortanix DSM secondary group.

4.4 DELETE A KEY IN THE FORTANIX DSM DESTINATION GROUP

When you delete a key from a DSM secondary group, the action will only delete the virtual key in Fortanix DSM and will not delete the actual key in the configured DSM primary group.

To delete a virtual key:

1. Select the virtual secondary key to delete.
2. Click the **DELETE SELECTED** button on top of the security objects table.

   Or

   Go to the detailed view of the key, scroll to the bottom, and click the **DELETE KEY** button to delete the key.

NOTE: If you delete a key from the DSM primary group, and you perform a key scan operation in the DSM secondary group, the key material in the secondary virtual key if present will

be deleted and it will become a virtual key without a key material. You can then manually delete the virtual key if required.

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/11593753674900-User-s-Guide-Store-Keys-Externally-Key-Management

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