Fortanix

User Guide

FORTANIX DATA SECURITY MANAGER – EXPORT KEY

VERSION 2.3

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) User Guide. This document describes the Fortanix DSM Export Key feature. It also contains the information related to:

- Export key as Encrypted key material
- Export key as components

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 EXPORT KEY

This section describes "Export Key as Encrypted Key Material" feature of Fortanix DSM. A group administrator can use this option to select a wrapping key that will be used to encrypt the key before it is exported. The following example assumes that:

- A key with "**Export**" key permissions exists in the group.
- The group has the following quorum policy: the members **Approver1** and **Approver2** form a quorum group, and 1 out the 2 member's approvals are required to approve an operation in the group.

In this example:

- A group administrator **User1** creates an "Export Key as Encrypted Key Material" request.
- The goal is to export the AES key named "**Key 1**" so that **User1** can download the key.

1. First, the group administrator **User1** creates an "Export Key as Encrypted Key Material" request by navigating to the detailed view of the key "**Key 1"** to be exported and should click **EXPORT KEY**.

   WARNING: The **EXPORT KEY** button will be disabled:

   - If the key type is not AES, DES, SECRET, HMAC, RSA, EC, or DES3.
   - If the Key does not have the "Export" permission selected.
   - If Quorum policy is not set in the group.
   - The Wrapping Key must have the" WRAP" permission.

   NOTE: If you select the key type as Secret, RSA, or EC and when you click the **EXPORT KEY** button, then the EXPORT KEY window will only have the wrapped key export option since this format does not support the component export. When you submit, a Quorum

approval request is sent for exporting the key. After the request is approved, you can download the key from the **Tasks** tab or from the dashboard.

2. In the "EXPORT KEY" window, the administrator (**User1**) selects the **AS ENCRYPTED KEY MATERIAL** radio button and provides the following details:
    - **Select Wrapping Key**: Select the key with "WRAP" permission that will be listed to wrap the key "Key1" before being exported.

      NOTE: The wrapping key can be AES keys only.
    - **Cipher Mode:** Select the cipher mode of encryption that should be applied to the key material. There are three types of encryption cipher modes to choose from:
        - **ECB:** In this method, plain text is divided into blocks of size 64 bits each. Each such block is encrypted independently of other blocks. For all blocks, same key is used for encryption.
        - **KW:** This method uses symmetric encryption to encapsulate key material.
        - **KWP:** In this method, additional padding of bits or bytes is appended to the encapsulated key material.

      NOTE: A cipher mode of operation may not be available for selection based on the source and selected wrapping key combination.
3. Click **SUBMIT EXPORT REQUEST** to submit the export request.
4. After the "Export as Encrypted Key Material" request Is created, a quorum approval request will be sent to the quorum members that form the group quorum policy. In this example, **Approver1** and **Approver2** will receive a notification that the requester User1 has created an "Export by Encrypted Key Material" request for the key "Key 1".

The following figure shows **Approver1**'s account page, where the "Export by Encrypted Key Material" request is shown. At this point, **Approver1** can approve or decline the request.

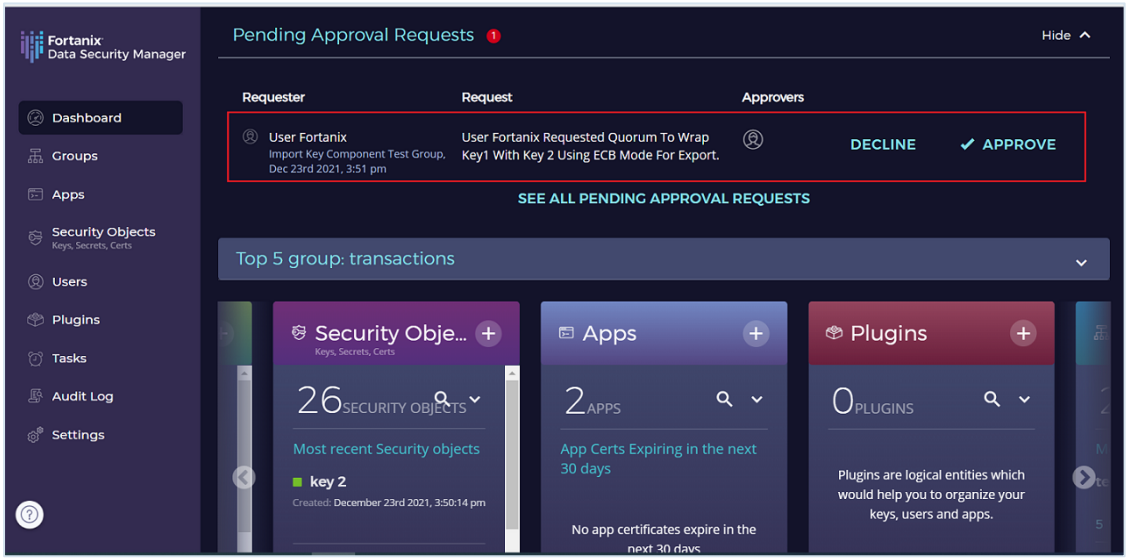

FIGURE 1: EXPORT REQUEST TO APPROVE

The Approvers can also review the export key request from **TASKS** tab -> **PENDING** tab -> **Import/Export** tab in the Fortanix DSM UI.

5. The **Approver1** can review the export request by clicking the **APPROVE** button. This step must also be performed by **Approver2** so that quorum is achieved. Once the quorum approves the "Key Export" request, the following dialog box opens on the screen:
   Any Approver can cancel the export operation by clicking the **DECLINE** button. At this point, the "Export by Encrypted Key Material" request is declined, and the users will not receive the key components. This state is final; once a request is declined by a quorum

member, it cannot be approved. Even if other quorum members have approved the request.

6. The Exported Key will now be available for **User1** to download under the **TASKS** tab -> **COMPLETED** tab -> **Import/Export** tab in the Fortanix DSM UI or in the Dashboard view.
7. By clicking the **DOWNLOAD THE KEY** link, the user will be displayed with the export key details showing the Wrapping key, Key KCV, and the format to download the key. Click **DOWNLOAD THE KEY** to successfully download the key.
8. After the key is download, you will see a tick against the key in the **Download** column.

3.1 EXPORT KEY AS COMPONENTS

The Export Key as Components feature allows a user to export a key as components to other users such that each user has a component of the key. To export a key as component:

- A Key Custodian policy should be set at the group level.
- A Quorum Policy should exist for the group.
- In the absence of the above policies, the **Export Key** button will be disabled.

For the complete end-to-end workflow of the "Export key by component" feature, refer to the article https://support.fortanix.com/hc/en-us/articles/360043559332-User-s-Guide-Key-Components#KeyExport.

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/360049737471-User-s-Guide-Export-Key

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