User Guide

FORTANIX DATA SECURITY MANAGER – EXPORT KEY

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

3.1 ENCRYPT KEY BEFORE EXPORT

This section describes “Export Key as Encrypted Key Material” feature of Fortanix DSM. 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.

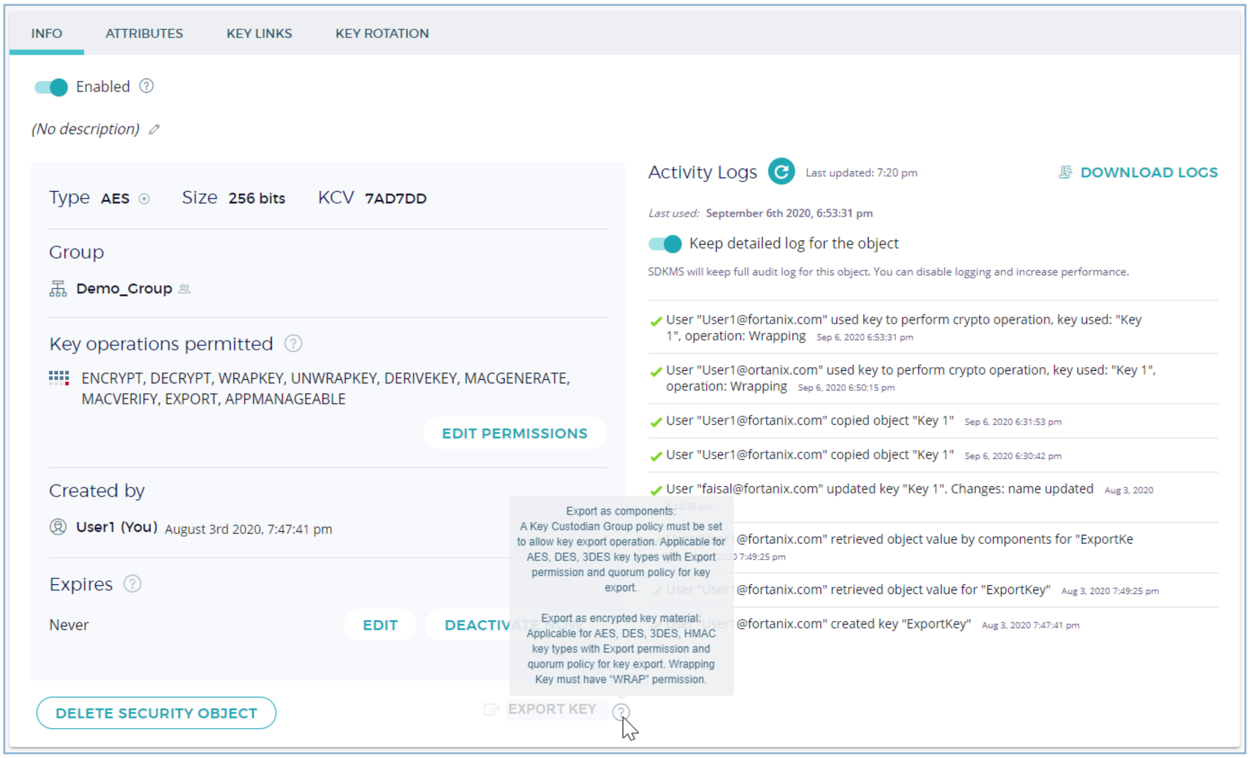
In this example:

- 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**. The following figure shows a detailed view of the SO "**Key 1**".

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

- If the Key type is not AES, DES, SECRET, HMAC, RSA, or DES3.
- If the Key does not have the “Export” permission selected.
- If Quorum Policy is not set in the group for keys of type AES, DES, HMAC, or DES3. For SECRET and RSA key the button will be enabled even without a Quorum policy.
- The Wrapping Key must have the ”WRAP” permission.



Enabled

(No description)

Type AES Size 256 bits KCV 7AD7DD

Group

Demo_Group

Key operations permitted

ENCRYPT, DECRYPT, WRAPKEY, UNWRAPKEY, DERIVEKEY, MACGENERATE, MACVERIFY, EXPORT, APPMANAGEABLE

Created by

User1 (You) August 3rd 2020, 7:47:41 pm

Expires

Never

Export as components:
A Key Custodian Group policy must be set to allow key export operation. Applicable for AES, DES, 3DES key types with Export permission and quorum policy for key export.

Export as encrypted key material:
Applicable for AES, DES, 3DES, HMAC key types with Export permission and quorum policy for key export. Wrapping Key must have “WRAP” permission.

Activity Logs Last updated: 7:20 pm

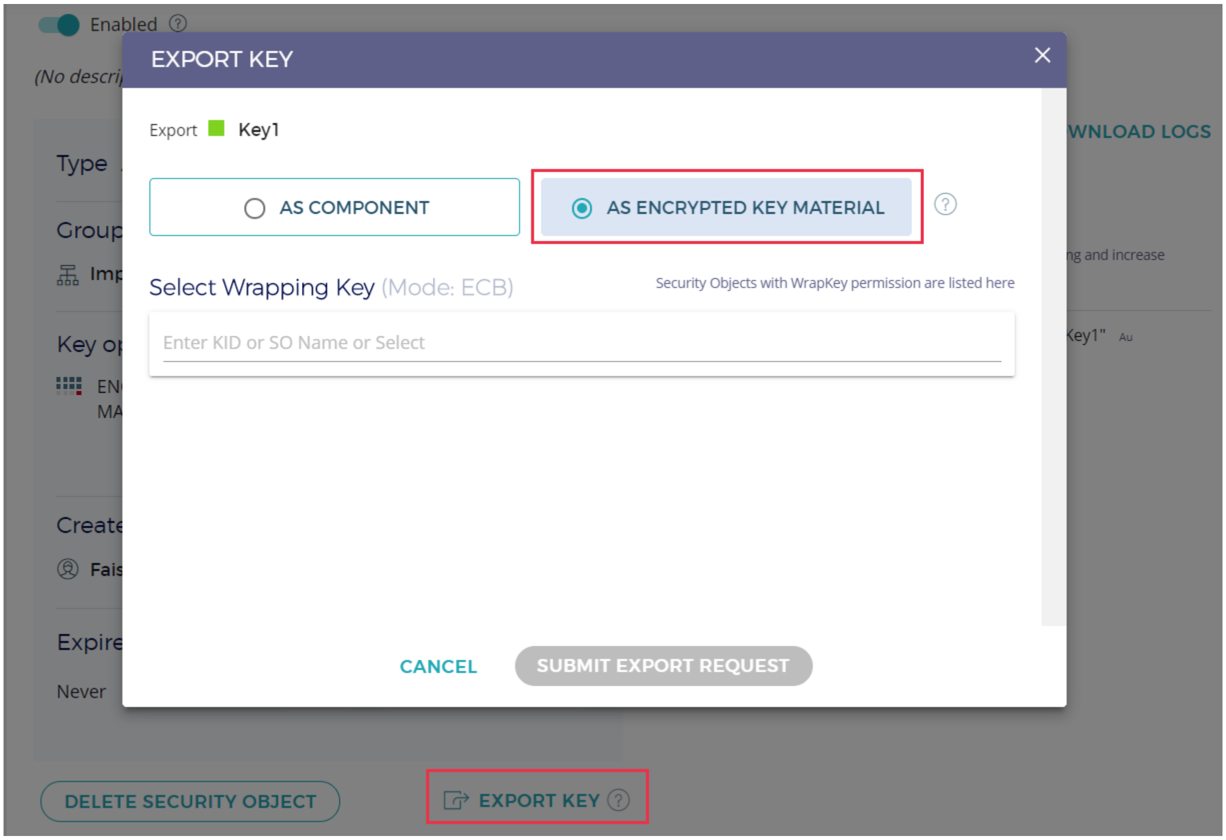
Last used: September 6th 2020, 6:53:31 pm

Keep detailed log for the object

SDKMS will keep full audit log for this object. You can disable logging and increase performance.

- ✓ User "User1@fortanix.com" used key to perform crypto operation, key used: "Key 1", operation: Wrapping Sep 6, 2020 6:53:31 pm
- ✓ User "User1@ortanix.com" used key to perform crypto operation, key used: "Key 1", operation: Wrapping Sep 6, 2020 6:50:15 pm
- ✓ User "User1@fortanix.com" copied object "Key 1" Sep 6, 2020 6:31:53 pm
- ✓ User "User1@fortanix.com" copied object "Key 1" Sep 6, 2020 6:30:42 pm
- ✓ User "faisal@fortanix.com" updated key "Key 1". Changes: name updated Aug 3, 2020 8:18:36 pm
- @fortanix.com" retrieved object value by components for "ExportKe 7:49:25 pm
- ✓ User "User1@fortanix.com" retrieved object value for "ExportKey" Aug 3, 2020 7:49:25 pm
- User1@fortanix.com" created key "ExportKey" Aug 3, 2020 7:47:41 pm

FIGURE 1: EXPORT KEY DISABLED



EXPORT KEY

Export 🟩 Key1

○ AS COMPONENT ● AS ENCRYPTED KEY MATERIAL

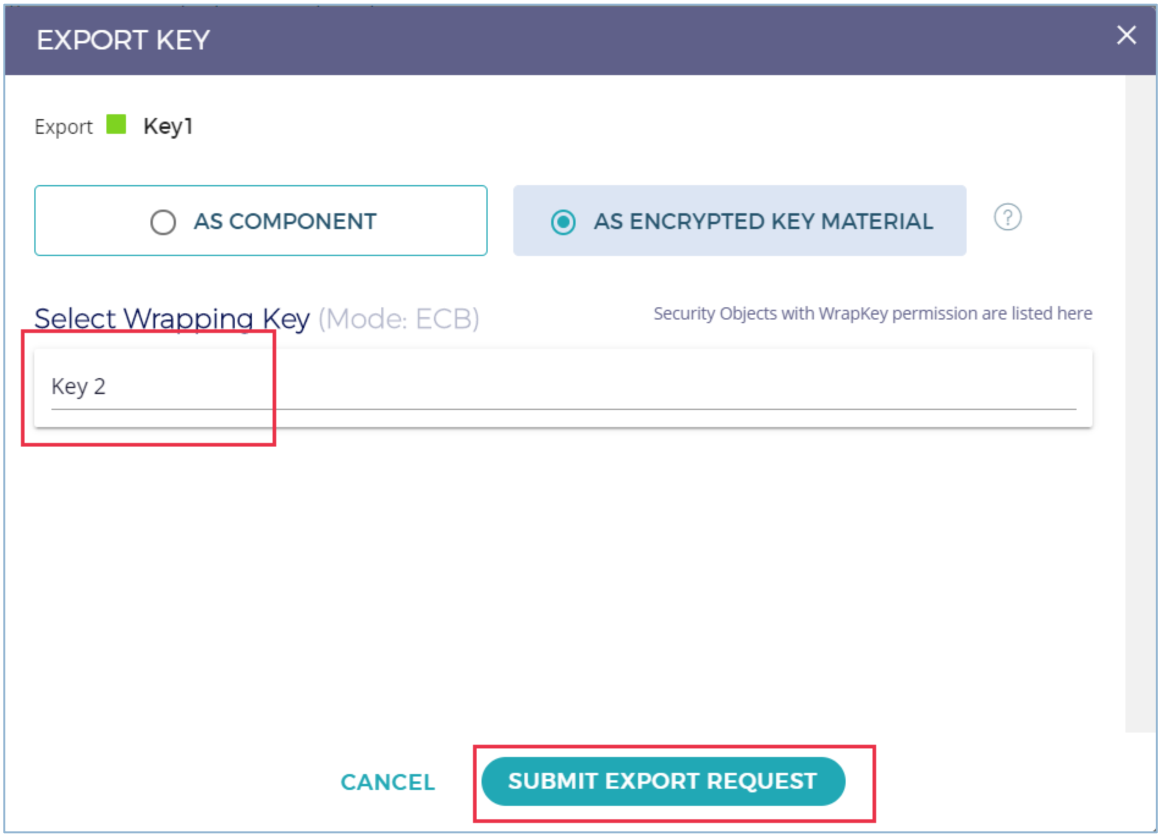
Select Wrapping Key (Mode: ECB) Security Objects with WrapKey permission are listed here

Enter KID or SO Name or Select

FIGURE 2: EXPORT AS ENCRYPTED KEY MATERIAL

NOTE: If you select the security type as 'Secret' or 'RSA' and when you click the **EXPORT KEY** button, then instead of showing the **EXPORT KEY** window, Fortanix DSM directly generates the export request as both these formats do not support the component export and wrapped key export. If a quorum policy is set for the group, an approval request is sent for exporting the key. Once 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.
3. Click **SUBMIT EXPORT REQUEST** to submit the export request.



EXPORT KEY

Export 🟩 Key1

○ AS COMPONENT ● AS ENCRYPTED KEY MATERIAL

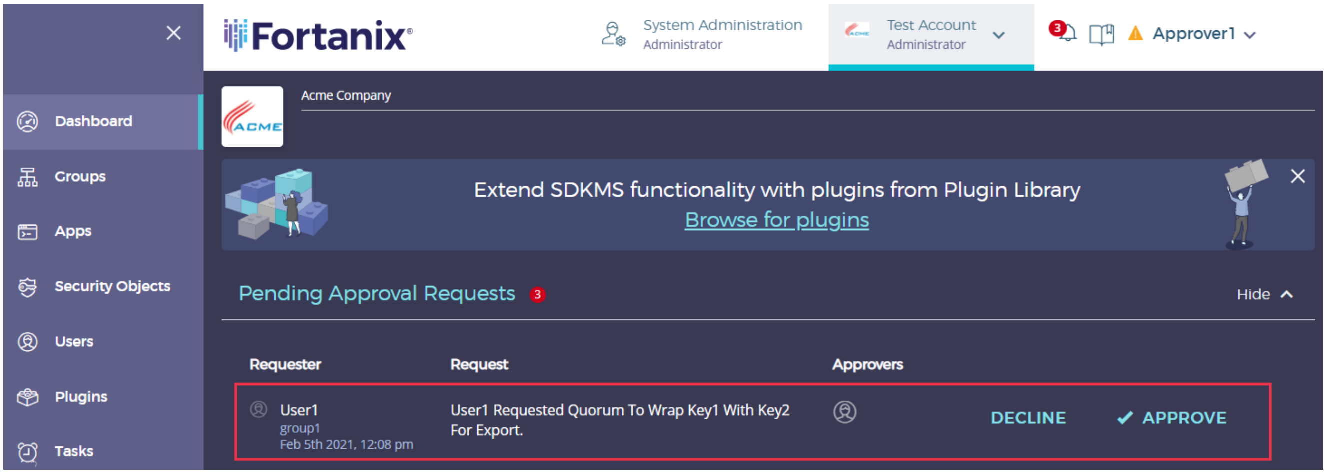
Select Wrapping Key (Mode: ECB)

Security Objects with WrapKey permission are listed here

Key 2

FIGURE 3: SUBMIT EXPORT REQUEST

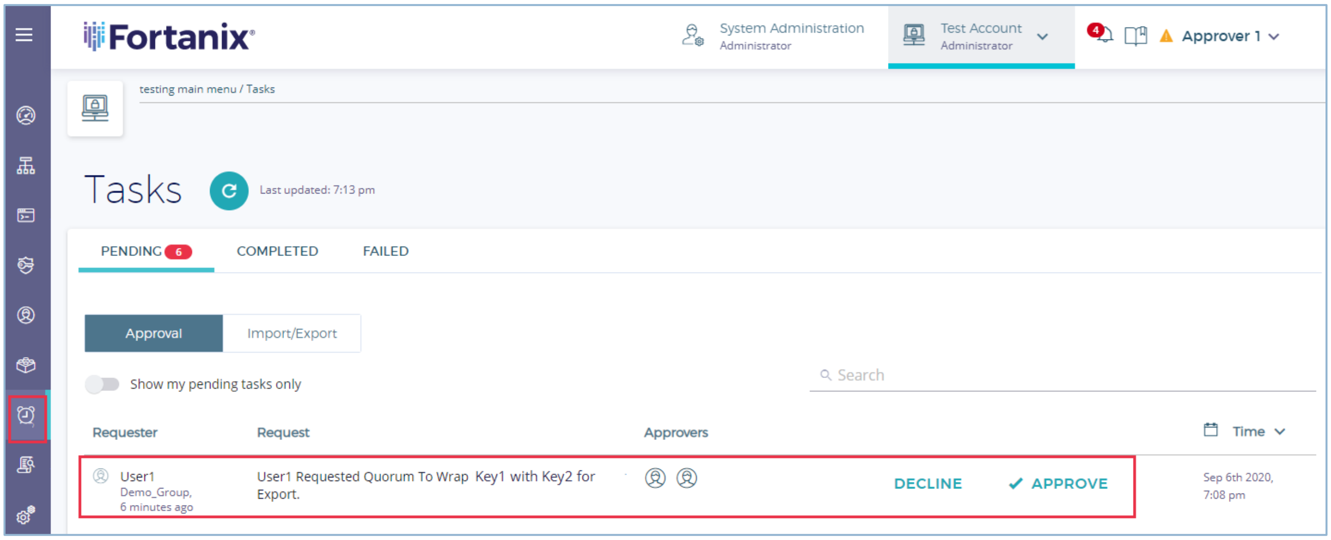
4. Once the “Export as Encrypted Key Material” request Is created, a quorum approval request will be sent to the quorum members that form the group quorum policy. In this example, **Approver1** and **Approver2** will receive a notification (**Figure 4**) that the requester User1 has created an “Export by Encrypted Key Material” request for the key “Key 1”.
5. 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.



Requester	Request	Approvers
User1 group1 Feb 5th 2021, 12:08 pm	User1 Requested Quorum To Wrap Key1 With Key2 For Export.	

FIGURE 4: EXPORT REQUEST TO APPROVE

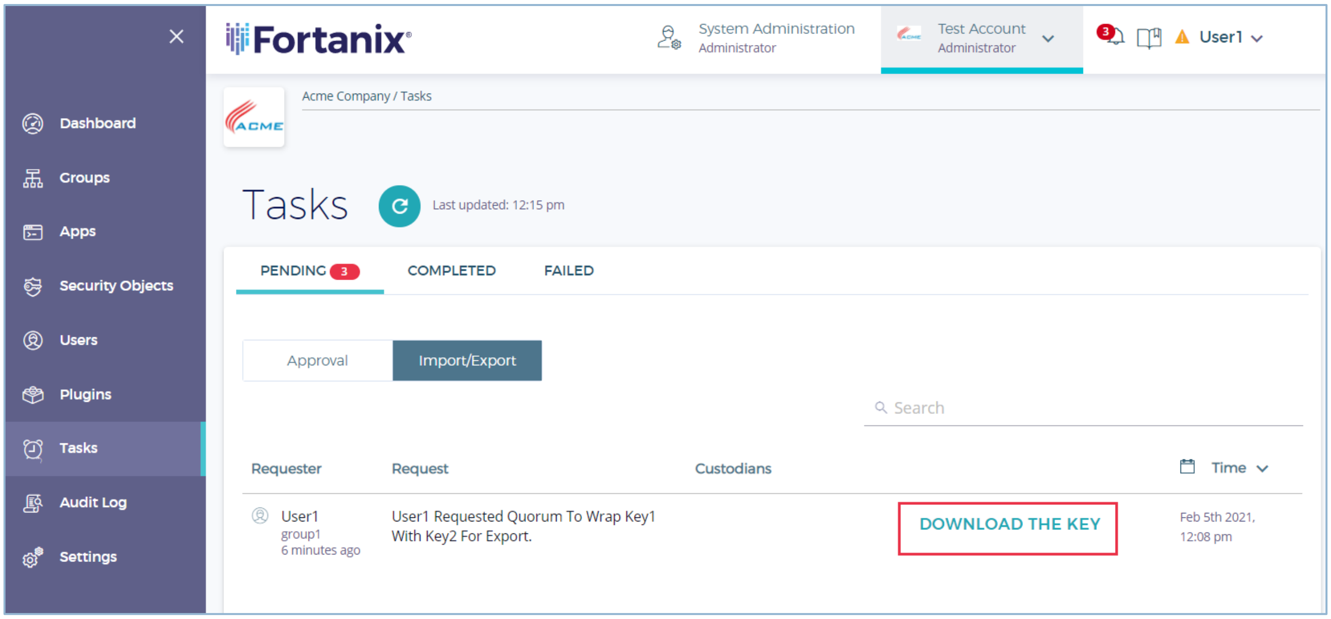
The **Approvers** can also review the export key request from **TASKS** tab -> **PENDING** tab -> **Approval** tab in the Fortanix DSM UI.



Requester	Request	Approvers	Time
User1 Demo_Group, 6 minutes ago	User1 Requested Quorum To Wrap Key1 with Key2 for Export.		Sep 6th 2020, 7:08 pm

FIGURE 5: REVIEW EXPORT KEY TASK

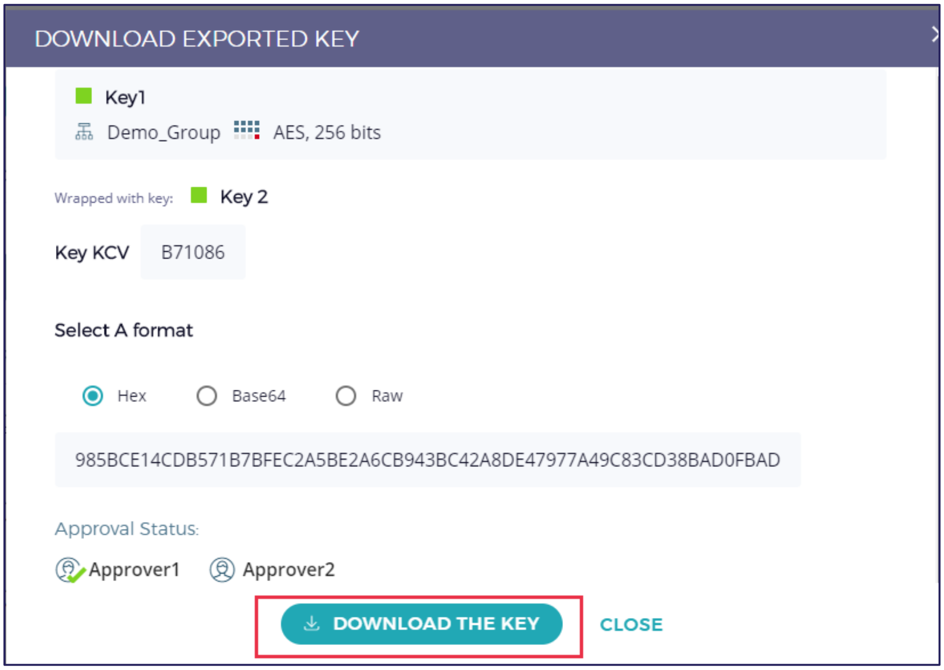
6. The **Approver1** can review the export request by clicking the **APPROVE** button. This step must also be performed by **Approver2** so that quorum is achieved. Once the quorum approves the “Key Export” request, the Exported Key will now be available for **User1** to download under the **TASKS** ⏰ tab -> **PENDING** tab -> **Import/Export** tab in the Fortanix DSM UI or in the Dashboard view.



Requester	Request	Custodians	Time
User1 group1 6 minutes ago	User1 Requested Quorum To Wrap Key1 With Key2 For Export.		Feb 5th 2021, 12:08 pm

FIGURE 6: DOWNLOAD THE KEY

7. 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.
8. By clicking the **DOWNLOAD THE KEY** link, the user will be displayed with the export key details showing the Wrapped key, Key KCV, and the format to download the key. Click **DOWNLOAD THE KEY** to successfully download the key.



DOWNLOAD EXPORTED KEY

🟩 Key1

Demo_Group AES, 256 bits

Wrapped with key: 🟩 Key 2

Key KCV B71086

Select A format

● Hex ○ Base64 ○ Raw

985BCE14CDB571B7BFEC2A5BE2A6CB943BC42A8DE47977A49C83CD38BAD0FBAD

Approval Status:

Approver1 Approver2

FIGURE 7: REVIEW AND DOWNLOAD THE KEY – KEY 1 WRAPPED WITH KEY 2

3.2 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

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.