FORTANIX TECHNICAL DOCUMENTATION

Fortanix®

User Guide

FORTANIX DATA SECURITY MANAGER – KEY COMPONENTS

TABLE OF CONTENTS

1.0 INTRODUCTION

Welcome to the Fortanix Data Security Manager (DSM) Key Components User Guide. This document describes the key import and export functionality using the Key Components feature of the Fortanix DSM GUI. It also contains the information related to:

- Set up Key Custodian policy
- Import key by Clear Components
- Import encrypted key by Components
- Export key Clear Components
- Export encrypted key 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** -

  An 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 SETUP KEY CUSTODIAN POLICY

A Key Custodian is a role assigned to Account Members or Account Administrators in Fortanix DSM who can only perform the following activities:

1. Provision clear (unencrypted) components for an import component operation or receive clear components from an export component operation.
2. Provision encrypted components for an import component operation or receive encrypted components from an export component operation.

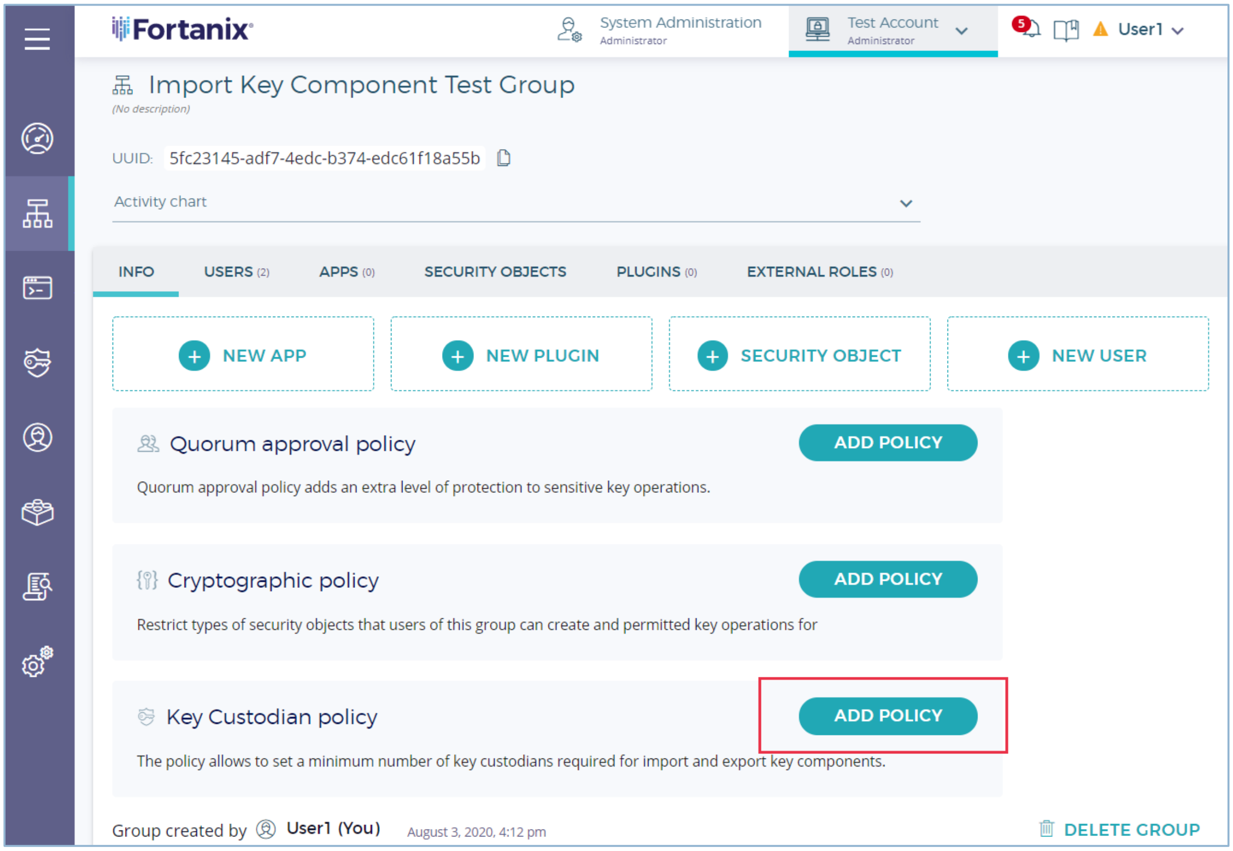
A Key Custodian has the following restrictions:

1. Should exist on a group level in the Fortanix DSM.
2. Should only be assigned to handle activities related to import/export key on clear components in a particular group.
3. Can only be Account Members or Account Administrators.

3.1 SET UP KEY CUSTODIAN POLICY

A Key Custodian policy allows an Account Member or Account Administrator to participate as a Key Custodian for a group. The Key-custodian policy must be set up with at least **2** or **3** custodians (**2** is the default). Key Custodians may be account members or administrators and are required for all the key import/export component flow initiated from this group. To set up the policy:

1. Go to the detailed view of a group, and in the **INFO** tab click the **ADD POLICY** button for the **Key Custodian policy** section.



Import Key Component Test Group

(No description)

UUID: 5fc23145-adf7-4edc-b374-edc61f18a55b

Activity chart

Quorum approval policy

Quorum approval policy adds an extra level of protection to sensitive key operations.

Cryptographic policy

Restrict types of security objects that users of this group can create and permitted key operations for

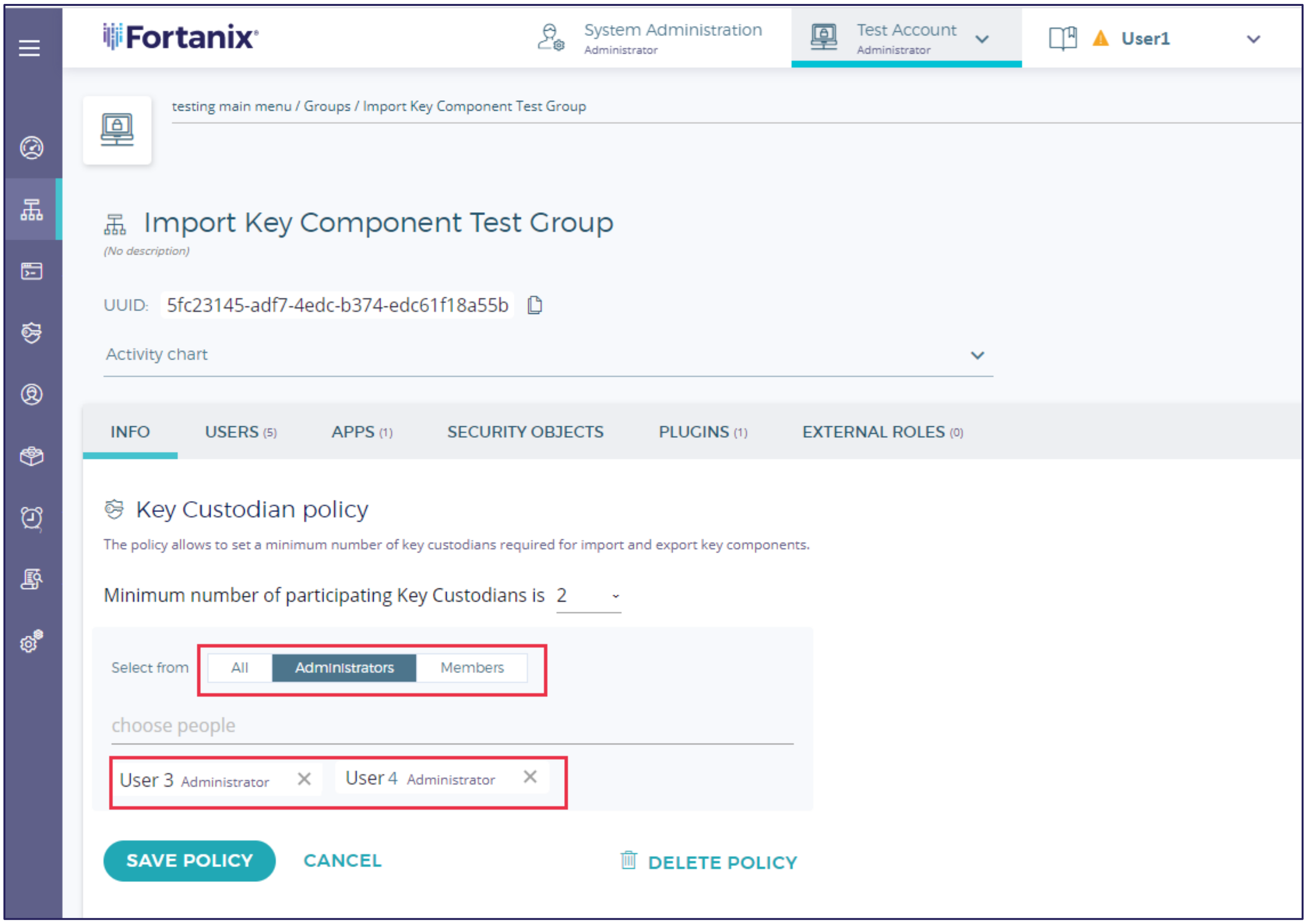
Key Custodian policy

The policy allows to set a minimum number of key custodians required for import and export key components.

Group created by User1 (You) August 3, 2020, 4:12 pm

FIGURE 1: ADD KEY CUSTODIAN POLICY

2. Next add the participating Key Custodians that are required for the import, export component operation.



testing main menu / Groups / Import Key Component Test Group

Import Key Component Test Group

(No description)

UUID: 5fc23145-adf7-4edc-b374-edc61f18a55b

Key Custodian policy

The policy allows to set a minimum number of key custodians required for import and export key components.

Minimum number of participating Key Custodians is 2

Select from: Administrators

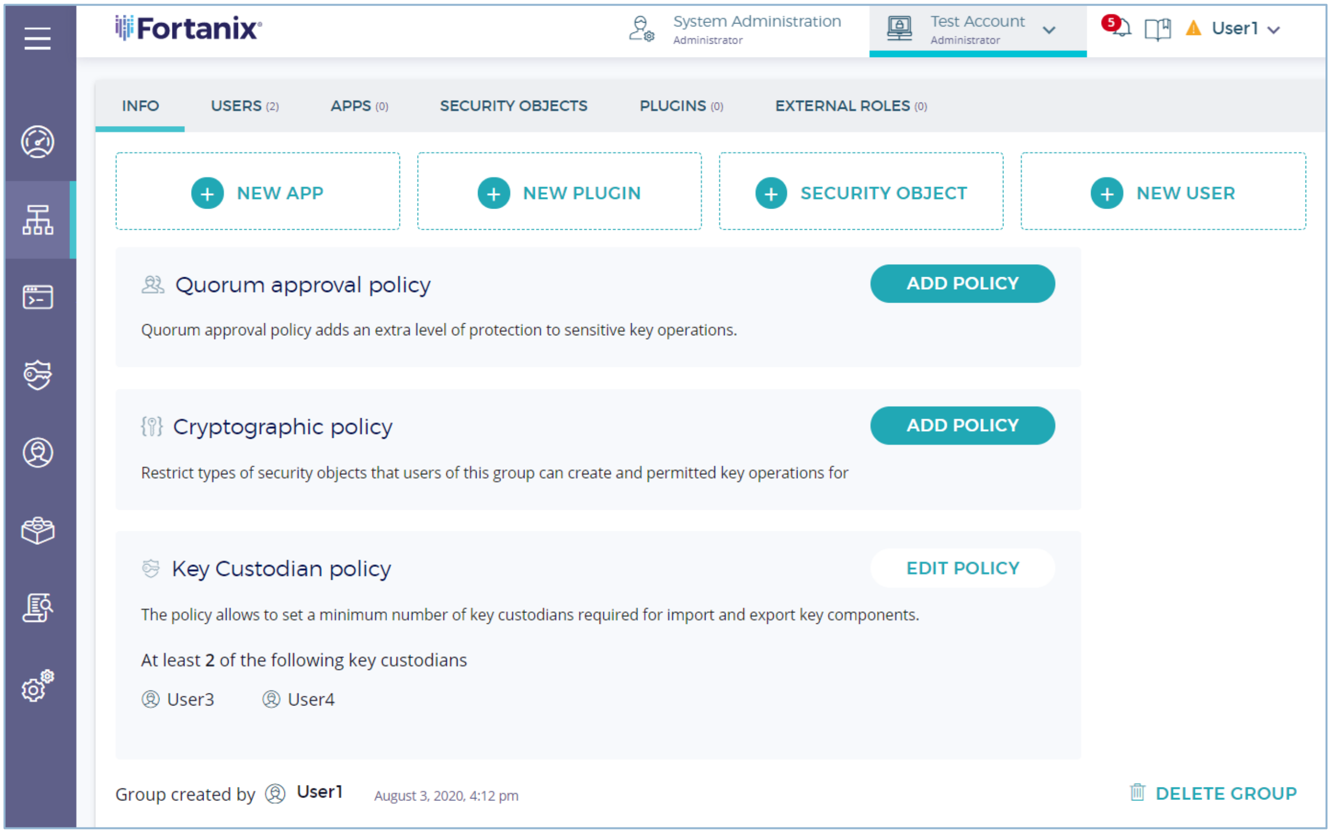
User 3 Administrator ×   User 4 Administrator ×

FIGURE 2: ADD KEY CUSTODIANS

The drop down shows **account members**, **administrators**, or a combination of **account members and administrators**.

- When you select **account members**, the list displays users with Account Member roles.
- When you select **administrators**, the list displays users with Administrator roles.
- When you choose **account members and administrators** , the list displays uses with Account Member and Account Administrator roles.

3. Choose the people who will participate as Key Custodians and then click **SAVE POLICY** to save the policy.



Quorum approval policy

Quorum approval policy adds an extra level of protection to sensitive key operations.

Cryptographic policy

Restrict types of security objects that users of this group can create and permitted key operations for

Key Custodian policy

The policy allows to set a minimum number of key custodians required for import and export key components.

At least 2 of the following key custodians

User3 User4

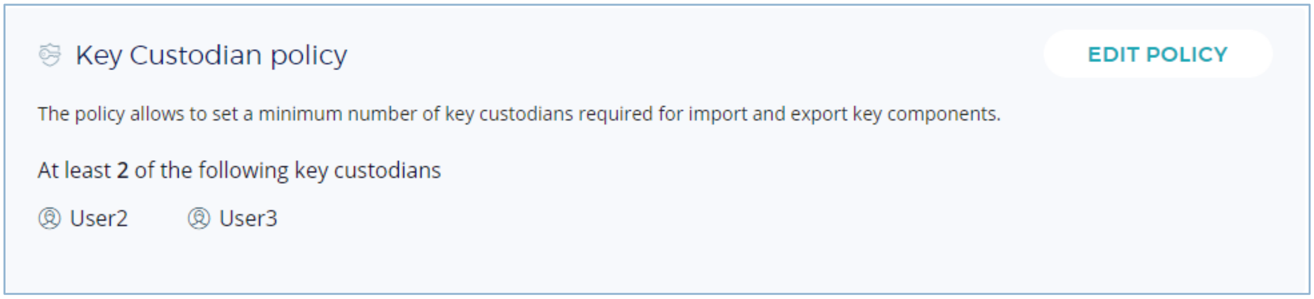
Group created by User1 August 3, 2020, 4:12 pm

FIGURE 3: SAVE POLICY

3.2 EDIT/ DELETE KEY CUSTODIAN POLICY

To delete a Key Custodian policy,

1. Go to the detailed view of the group and then in the **INFO** tab, under the **Key Custodian policy** section, click the **EDIT POLICY** button.



Key Custodian policy

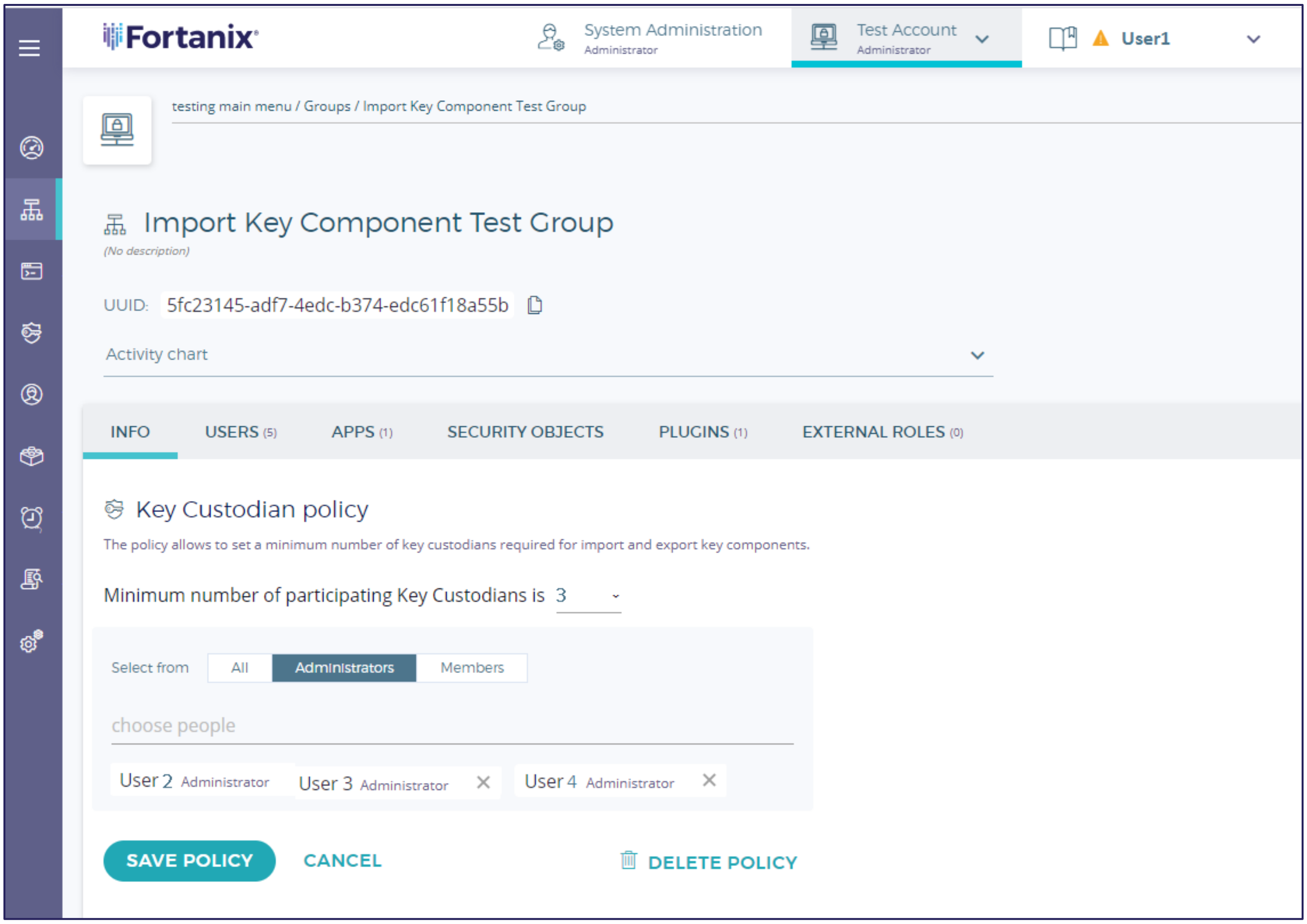
The policy allows to set a minimum number of key custodians required for import and export key components.

At least 2 of the following key custodians

User2 User3

FIGURE 4: EDIT POLICY

2. To edit the policy, In the detailed view of the Key Custodian policy make some changes to the policy and click **SAVE POLICY** button. To delete the policy, click the **DELETE POLICY** button.



testing main menu / Groups / Import Key Component Test Group

Import Key Component Test Group

(No description)

UUID: 5fc23145-adf7-4edc-b374-edc61f18a55b

Key Custodian policy

The policy allows to set a minimum number of key custodians required for import and export key components.

Minimum number of participating Key Custodians is 3

User 2 Administrator

User 3 Administrator ✕

User 4 Administrator ✕

FIGURE 5: EDIT OR DELETE A POLICY

4.0 KEY IMPORT

4.1 IMPORT KEY BY CLEAR COMPONENTS USER FLOW

This section describes the “Import Key by Clear Components” feature. The import key by clear component feature is explained using the following example which assumes that:

- A group called “**Import Key Component Test Group**” exists and has **User1**, and **User2** as group administrators.
- **User3** and **User4** are Key Custodians who were added in the Key Custodian policy.

In this example:

- **User1** creates an “**Import Key by Clear Components**” request.
- **User3** and **User4** are the key custodians of a symmetric key and possess clear components.
- The goal is to import the symmetric by clear components into Fortanix DSM.

Steps

1. To add a new Security Object to the **Import Key Component Test Group**, the **User1** clicks the **ADD SECURITY OBJECT** button in the group detailed view.

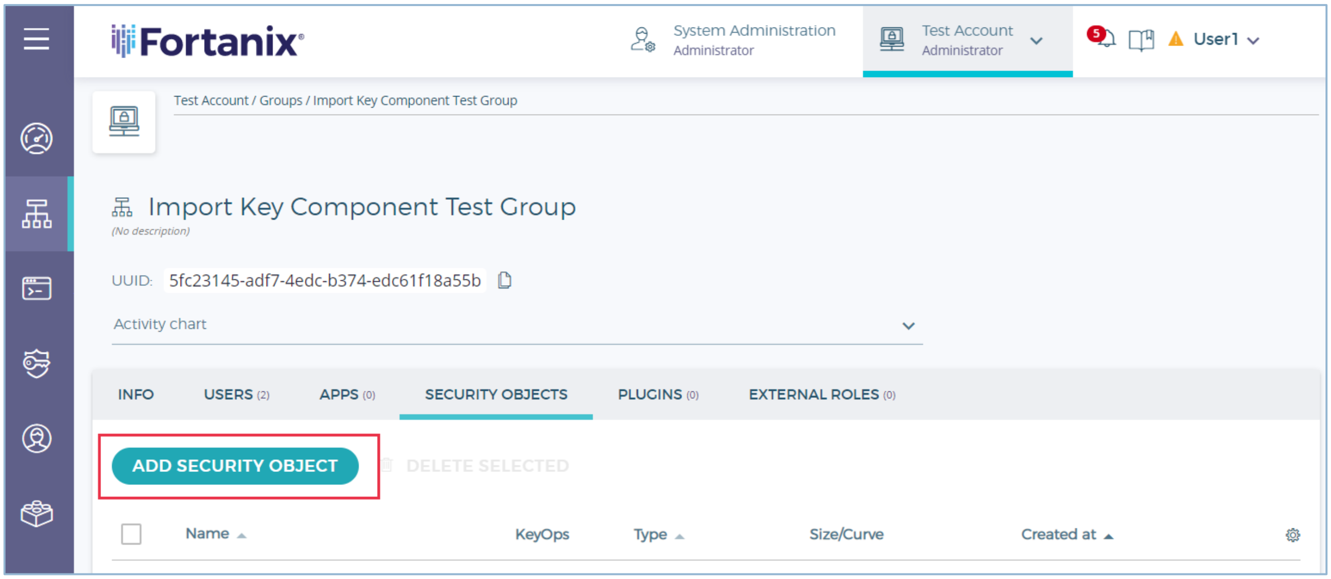
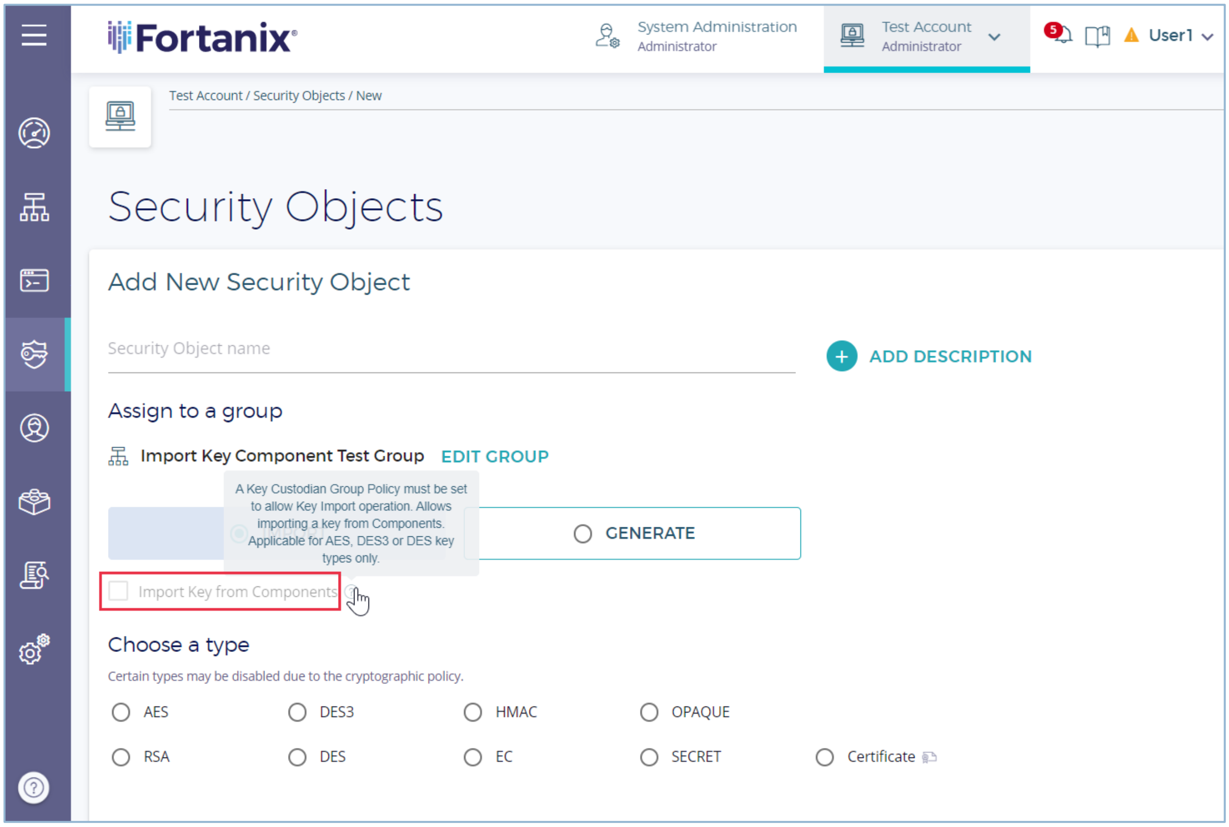


FIGURE 6: ADD SECURITY OBJECT

2. In the Add New Security Objects form, fill the following details:
    - **Security Object (SO) Name:** This is the name that the key will have once all components are received by Fortanix DSM (in this example "**Key 1**").
    - Select the **IMPORT** option for the key create operation.
    - Select the **Import Key from Components** check box to start the process for importing key by components.

NOTE: The **Import Key from Components** check box will be disabled if the **Key Custodian policy** is not set at the group level.



A Key Custodian Group Policy must be set to allow Key Import operation. Allows importing a key from Components. Applicable for AES, DES3 or DES key types only.

Certain types may be disabled due to the cryptographic policy.

FIGURE 7: IMPORT KEY FROM COMPONENTS CHECK BOX DISABLED

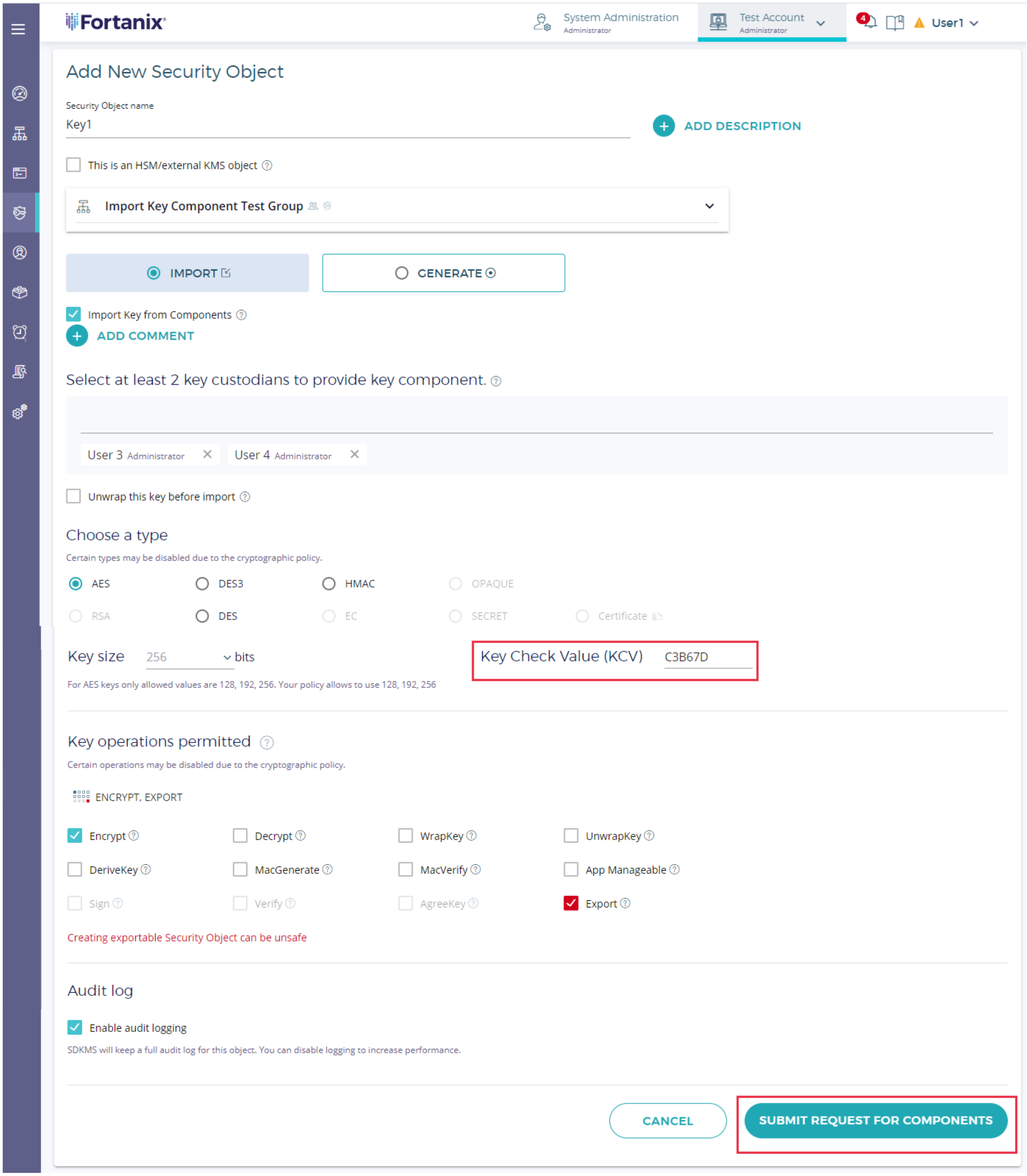
- **Key Custodians:** In this example, **User3**, and **User4** are being selected as the users that will upload their components to Fortanix DSM. The minimum number of participating Key Custodians is set in the Key Custodian Group policy. For example: When the minimum number of Key Custodians is set as 2 in the group policy, the user must select two users from the list of users at the group policy level to participate in the upload component operation.

- **Choose a type** (SO)**:** The type of key that is being imported.

📌 **NOTE**: The allowed key types for importing keys by components are AES, DES3, DES, or HMAC. (in this example: AES).

- **Key size**: The size of the key in bits (in this example 256 bits):
  - For AES, the key size can be 128, 192, or 256 bits.
  - For DES3, the key size can be 112 or 168 bits.
  - For DES, the key size can be 56 bits.
  - For HMAC, choose key size from 112 to 8192 bits.
- **Key Check Value** (**KCV**): The KCV of the imported key which is optionally added by the admin while creating the import request.
- **Key operations permitted**: The operations that the key will be able to execute once it is imported. In this example, the key is given “Encrypt”, “Decrypt” and “Export” key operations.

3. Once all the parameters are selected, the group administrator (**User1**) clicks the **SUBMIT REQUEST FOR COMPONENTS** button.



Add New Security Object

Security Object name
Key1

□ This is an HSM/external KMS object

Import Key Component Test Group

● IMPORT ○ GENERATE

☑ Import Key from Components

Select at least 2 key custodians to provide key component.

User 3 Administrator ✕ User 4 Administrator ✕

□ Unwrap this key before import

Choose a type

Certain types may be disabled due to the cryptographic policy.

● AES ○ DES3 ○ HMAC ○ OPAQUE
○ RSA ○ DES ○ EC ○ SECRET ○ Certificate

Key size 256 bits

Key Check Value (KCV) C3B67D

For AES keys only allowed values are 128, 192, 256. Your policy allows to use 128, 192, 256

Key operations permitted

Certain operations may be disabled due to the cryptographic policy.

ENCRYPT, EXPORT

☑ Encrypt	□ Decrypt	□ WrapKey	□ UnwrapKey
□ DeriveKey	□ MacGenerate	□ MacVerify	□ App Manageable
□ Sign	□ Verify	□ AgreeKey	☑ Export

Creating exportable Security Object can be unsafe

Audit log

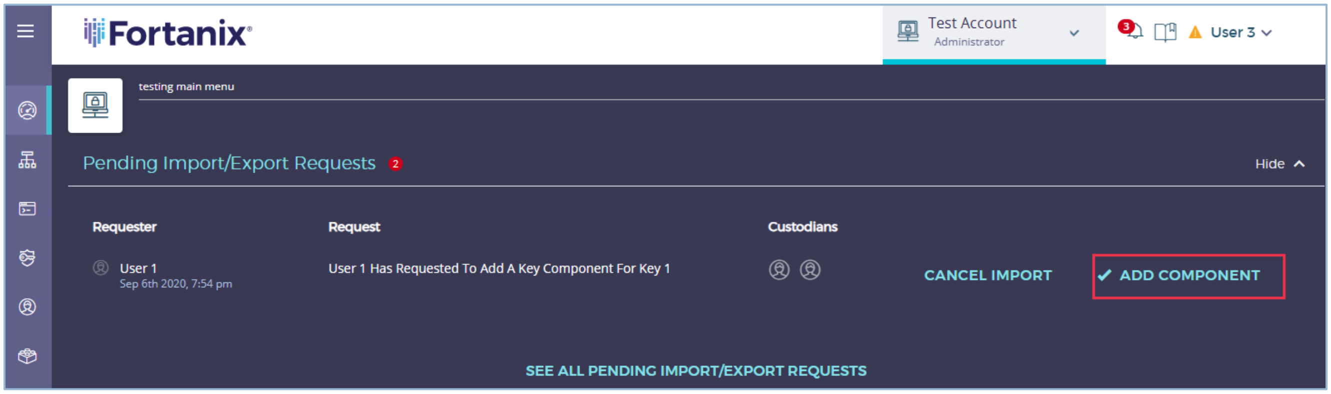
☑ Enable audit logging

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

FIGURE 8: CREATE AN IMPORT KEY COMPONENT REQUEST

Once the “Import Key by Clear Components” request is submitted, **User3** and **User4** will be notified that the request has been created and that they can submit their key components.

4. Now when **User3** opens the Account page in Fortanix DSM, under **Key Components** section, the request created by **User1** to import a key with the name “**Key 1”** will appear (**Figure 9**). **User3** has the option of either **ADD COMPONENT** or **CANCEL IMPORT**.

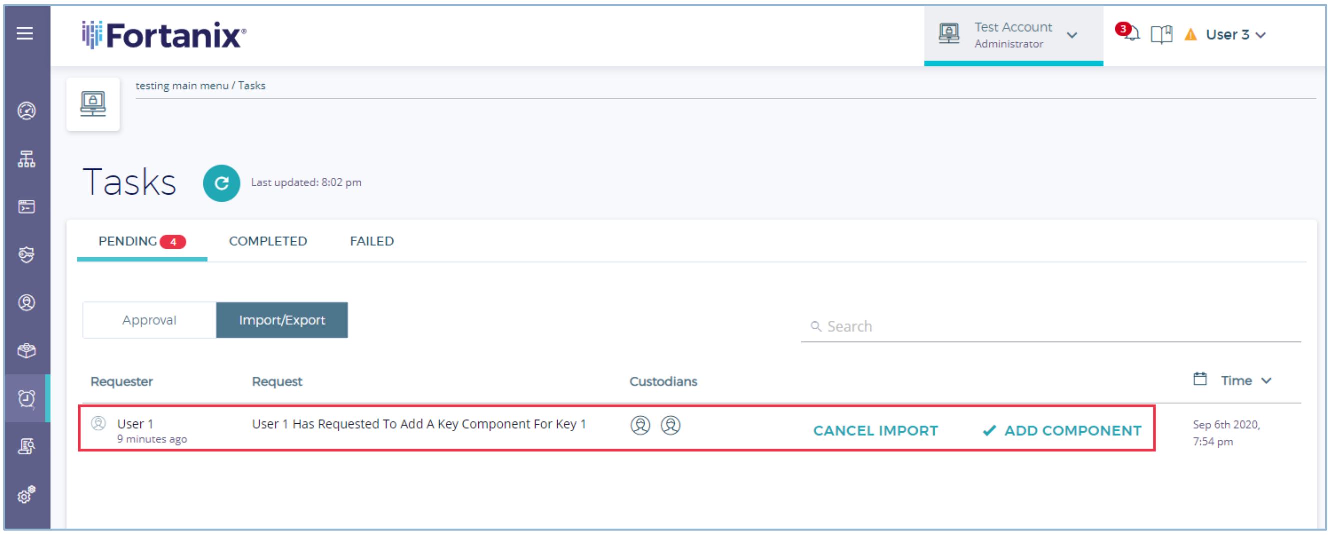


Pending Import/Export Requests 2

Requester	Request	Custodians		
User 1 Sep 6th 2020, 7:54 pm	User 1 Has Requested To Add A Key Component For Key 1		CANCEL IMPORT	✓ ADD COMPONENT

FIGURE 9: ADD KEY COMPONENT REQUEST

The **User3** can also add a key component from the **TASKS** tab -> **PENDING** tab -> **Import/Export** tab in the Fortanix DSM UI.



Tasks

Last updated: 8:02 pm

Requester	Request	Custodians			Time
User 1 9 minutes ago	User 1 Has Requested To Add A Key Component For Key 1		CANCEL IMPORT	✓ ADD COMPONENT	Sep 6th 2020, 7:54 pm

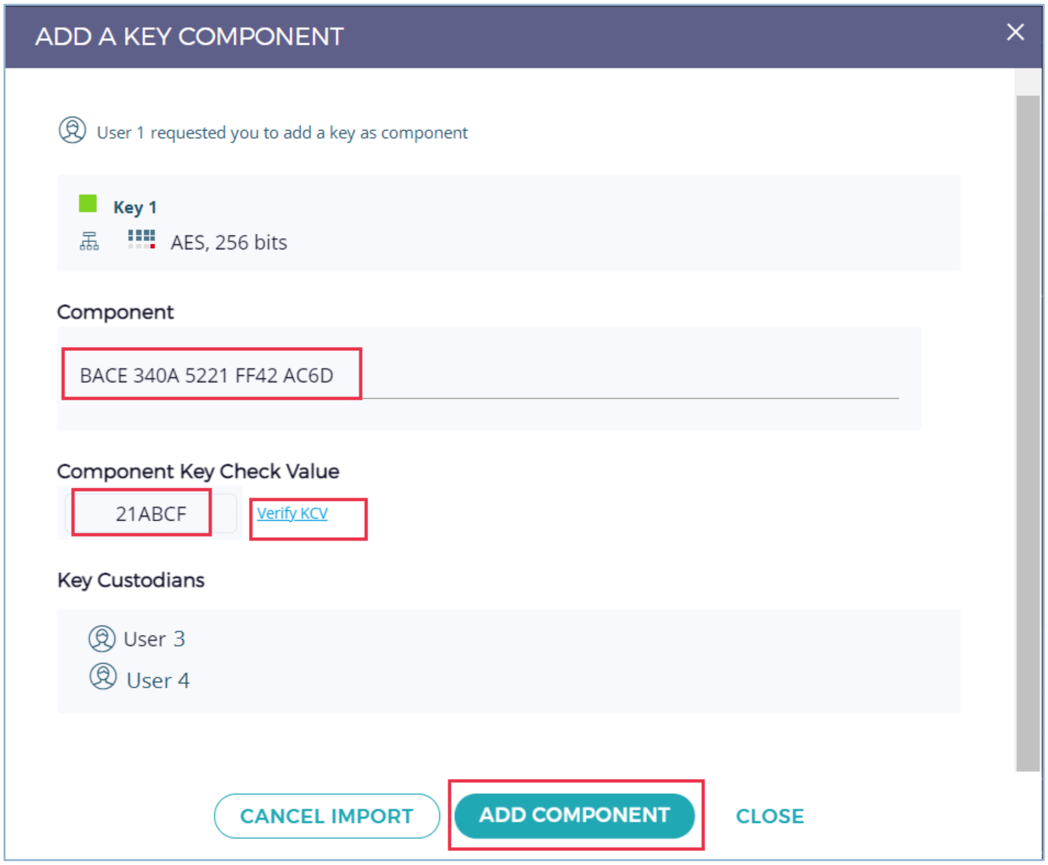
FIGURE 10: ADD KEY COMPONENT REQUEST

5. When **User3** clicks the **ADD COMPONENT** button, the following dialog box is displayed with the information below for **User3** to review.

- The user that has created the "Import Key by Clear Components" request.
- The name of the imported key, that is "**Key 1**".
- The type and size of the key.
- The key KCV value.

The **User3** should provide the following details:

- The key Clear Component value (**Component**).
- The **Component Key Check Value**.



ADD A KEY COMPONENT

User 1 requested you to add a key as component

Key 1
AES, 256 bits

Component: BACE 340A 5221 FF42 AC6D

Component Key Check Value: 21ABCF

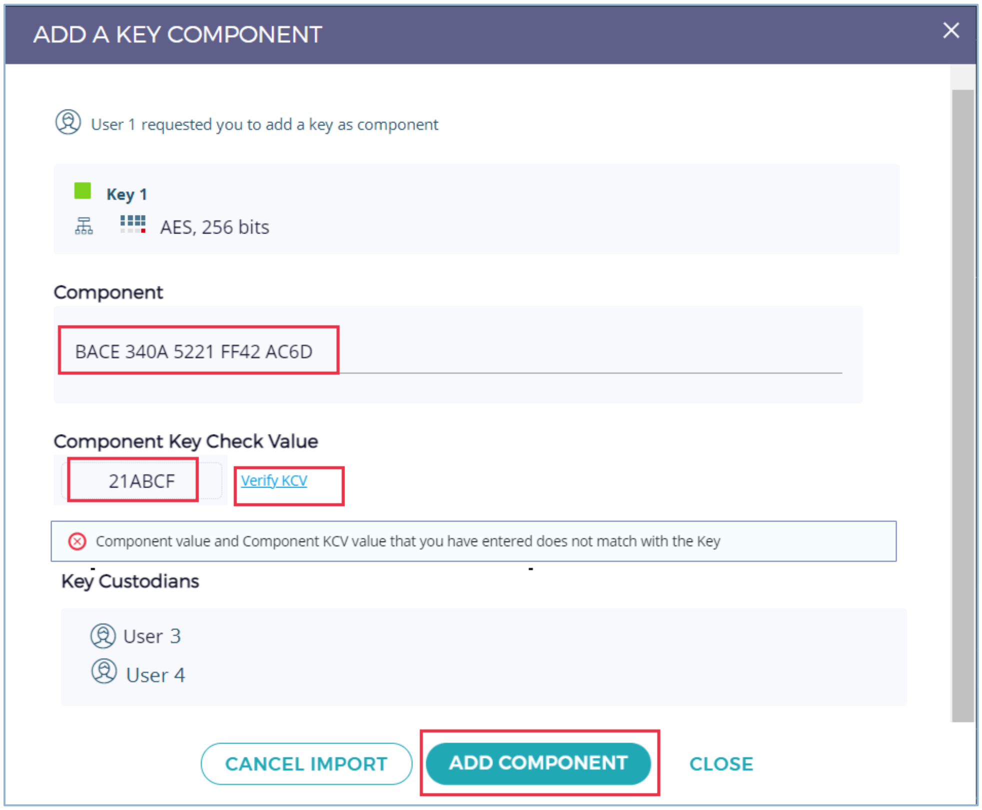
Key Custodians
User 3
User 4

FIGURE 11: ADD KEY COMPONENT VALUES

Similarly, **User4** should also perform ***Step 5*** to add a key component.

6. Once the **Component** and **Component Key Check Value** have been entered, the user can verify if the Component value and Component KCV match using the **Verify KCV** link. If they do

not match, an error message will be displayed indicating the mismatch. At this point, the key custodian will retype the key clear component and KCV and verify them again.



ADD A KEY COMPONENT

User 1 requested you to add a key as component

Key 1

AES, 256 bits

Component

BACE 340A 5221 FF42 AC6D

Component Key Check Value

21ABCF

Verify KCV

Component value and Component KCV value that you have entered does not match with the Key

Key Custodians

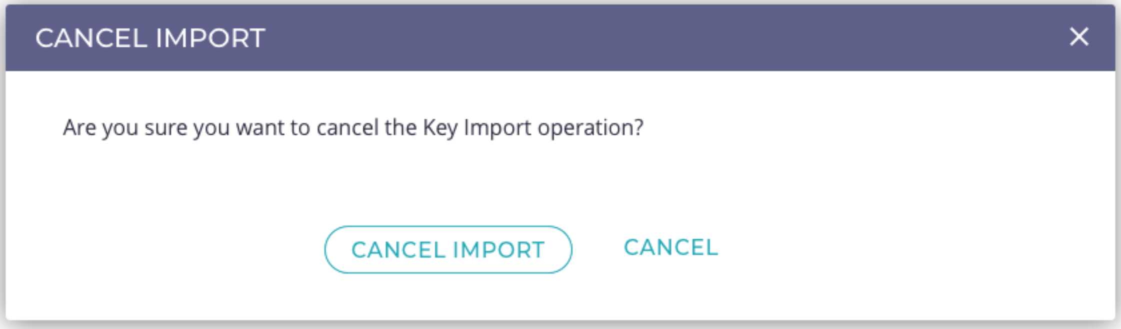
User 3

User 4

FIGURE 12: KEY KCV MISMATCH

7. Once the key clear component and KCV matches, **User3** and **User4** have to click the **ADD COMPONENT** button, and the component value is sent over TLS and stored securely by Fortanix DSM.

   The users can also choose to cancel the "Import Request" by clicking the **CANCEL IMPORT** button. If the user decides to cancel the import operation the following confirmation window is displayed:



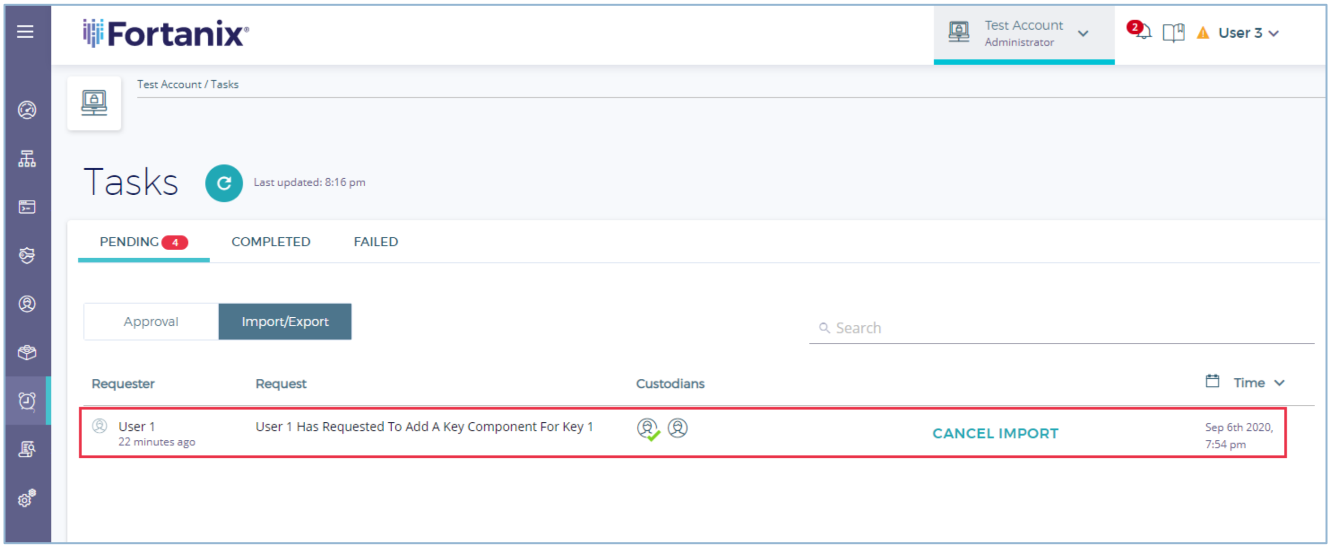
CANCEL IMPORT ✕

Are you sure you want to cancel the Key Import operation?

FIGURE 13: CANCEL IMPORT

NOTE: When an "Import Request" is cancelled by one key custodian, other custodians will not be able to enter key components: the key will not be imported, and all the previously imported components will be destroyed. If the group administrator wants to import the key by clear components, a new "Import Key by Clear Components" request must be created as shown in ***section 4.1***.

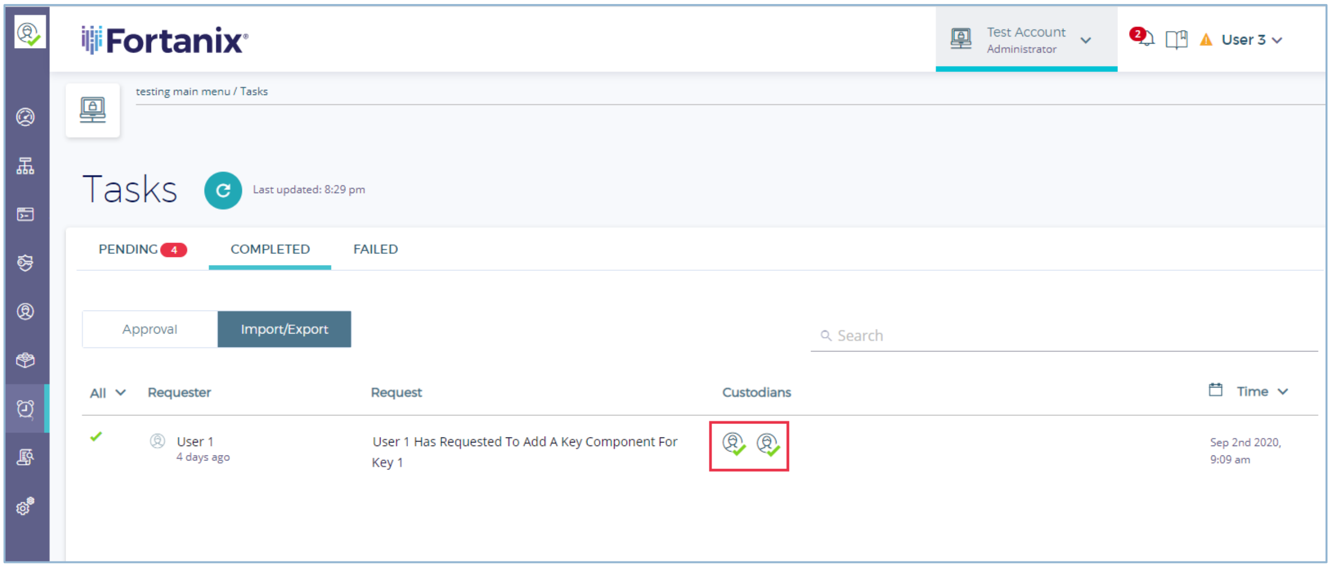
8. Once **User3** has performed ***Steps 4-6*** above to add a key component, the "Import Key by Clear Components" request now moves under the **TASKS** ⏰ tab -> **PENDING** -> **Import/Export** tab in the Fortanix DSM UI.



Requester	Request	Custodians		Time
User 1 22 minutes ago	User 1 Has Requested To Add A Key Component For Key 1		CANCEL IMPORT	Sep 6th 2020, 7:54 pm

FIGURE 14: IMPORT COMPONENT ADDED BY USER3

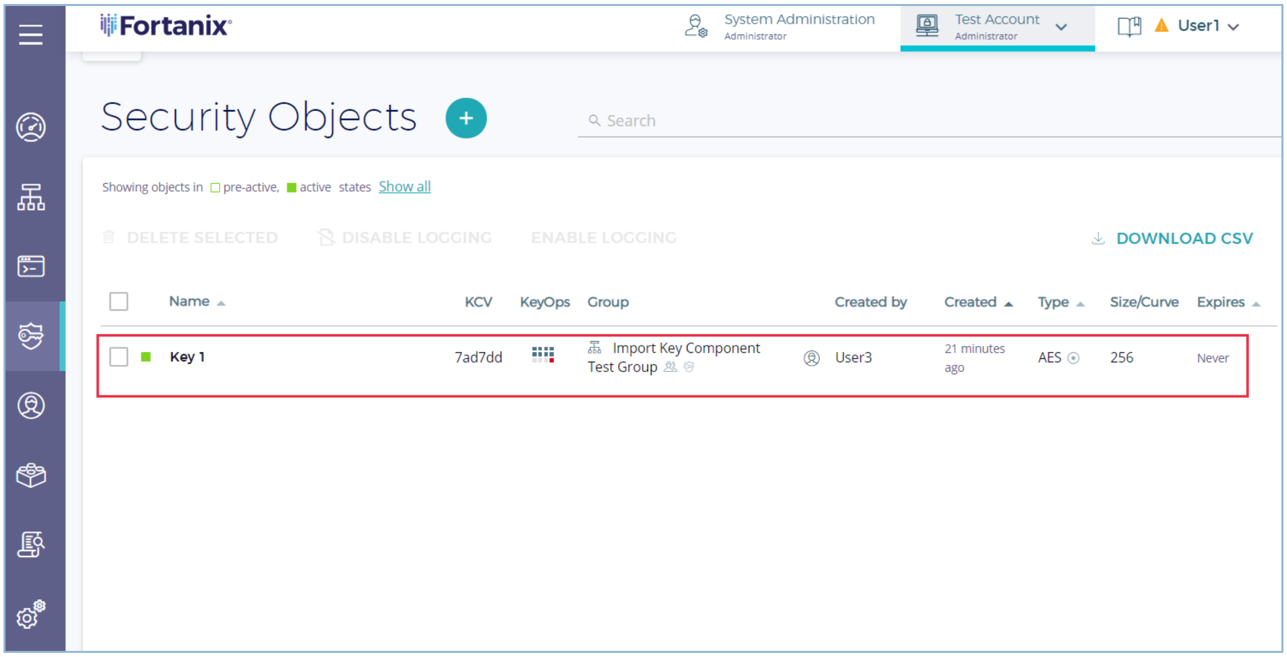
9. After all key custodians have performed ***Steps 4-6*** and the key components are added, Fortanix DSM will recombine all clear components to produce a key with the parameters provided in ***Step 2***. The components are stored in Fortanix DSM for as long as they are needed to recombine the key. Once the key is imported, its components are destroyed.



All	Requester	Request	Custodians	Time
✓	User 1 4 days ago	User 1 Has Requested To Add A Key Component For Key 1		Sep 2nd 2020, 9:09 am

FIGURE 15: IMPORT COMPONENT COMPLETED BY ALL CUSTODIANS

10. When a user navigates to the Security Objects (SO) list page, the newly imported key will be shown in the list of SOs. In the following figure, the key "**Key 1**" is displayed in the list of objects.



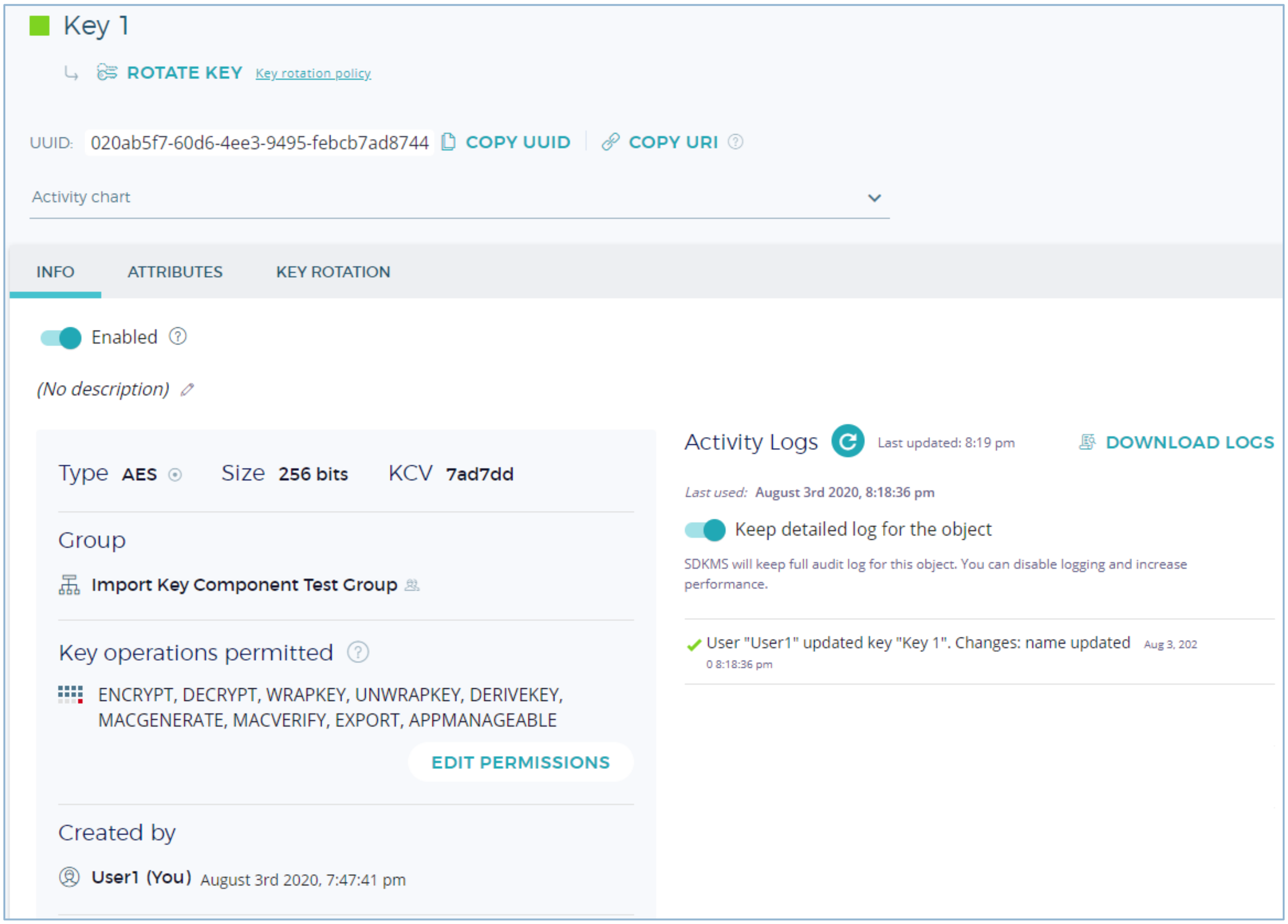
Security Objects

Showing objects in □ pre-active, 🟩 active states Show all

☐	Name	KCV	KeyOps	Group	Created by	Created	Type	Size/Curve	Expires
☐	🟩 Key 1	7ad7dd		Import Key Component Test Group	User3	21 minutes ago	AES	256	Never

FIGURE 16: KEY SUCCESSFULLY CREATED FROM COMPONENTS

The detailed view of “**Key 1**" displays the key properties:



Key 1

UUID: 020ab5f7-60d6-4ee3-9495-febcb7ad8744

Enabled

(No description)

Type AES Size 256 bits KCV 7ad7dd

Group

Import Key Component Test Group

Key operations permitted

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

Created by

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

Activity Logs Last updated: 8:19 pm

Last used: August 3rd 2020, 8:18:36 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" updated key "Key 1". Changes: name updated Aug 3, 2020 8:18:36 pm

FIGURE 17: "KEY 1" DETAILED VIEW

4.2 KEY KCV MATCH

If the admin who created the import request optionally added the KCV, then once all the clear components are submitted and the key is recombined, Fortanix DSM checks that the resulting KCV of the recombined key matches the key KCV provided in ***step 2*** in ***Section 4.1***. If these two KCVs do not match, the key will not be imported, and all the submitted components will be destroyed. The result of the "Key Import" request will display an error message. If the group administrator still wants to import the key by clear components, a new "Import Key by Clear Components" request would need to be created (***Step 1*** in ***Section 4.1***).

4.3 IMPORT ENCRYPTED KEY BY COMPONENTS USER FLOW

Fortanix DSM provides the option to specify a Key-Encryption-Key (KEK) which will unwrap (decrypt) the recombined key components. The Fortanix DSM process for this is:

a. Fortanix DSM waits until quorum approval is completed to import and unwrap the encrypted key material with wrapping key.
b. Once a quorum is reached, Fortanix DSM allows to unwrap the key to be imported with the KEK selected during the Export key as Components operation.
c. Fortanix DSM waits until all custodians provide their components.
d. Once all components are provided, Fortanix DSM recombines all components.
e. Fortanix DSM unwraps (decrypts) the recombined material from ***Step d*** using the specified KEK.
f. The resulting material from ***Step e*** is the final SO that is imported.

NOTE: Recombining Components:

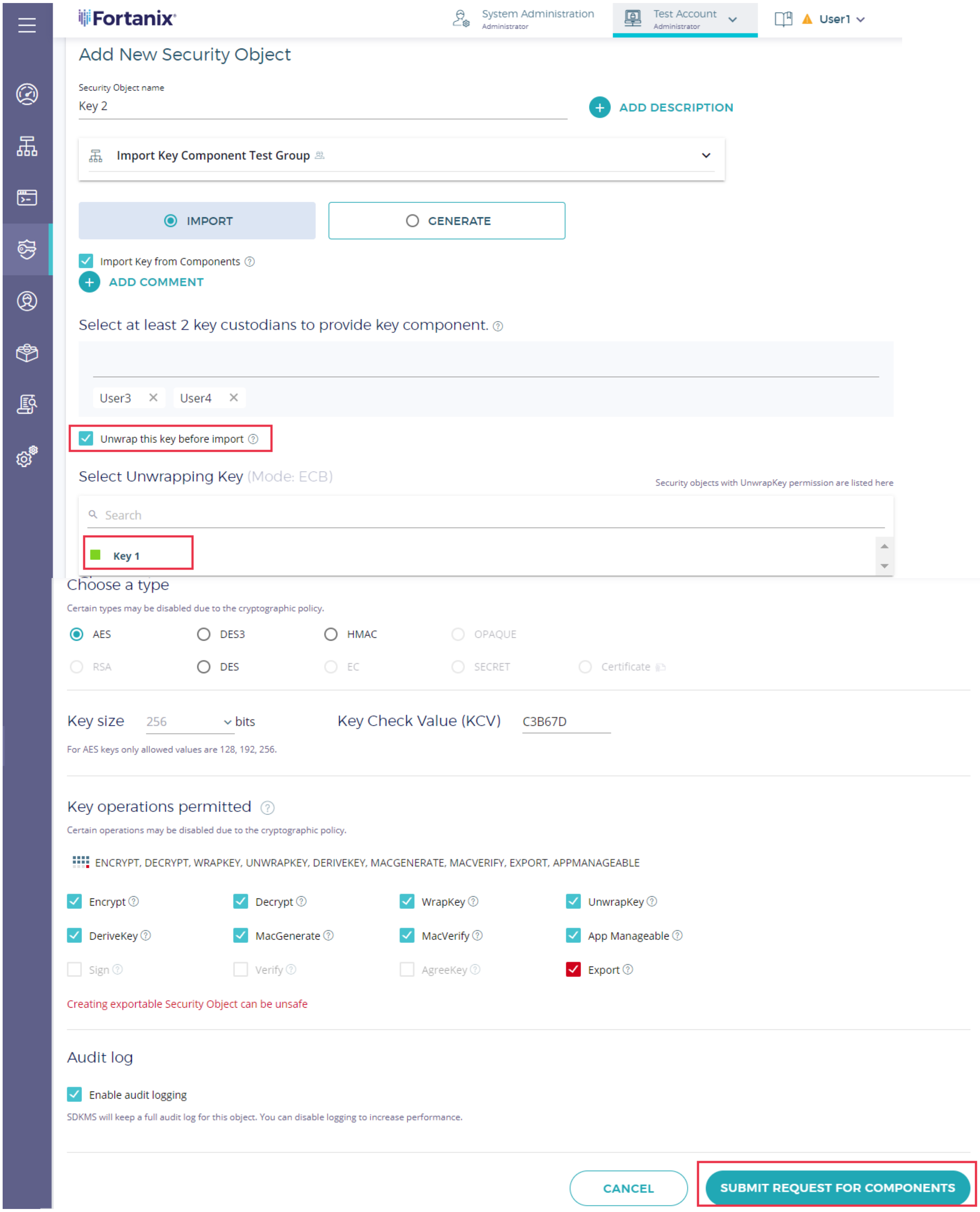
- In case of a key that is not wrapped by a KEK, recombining components results in the original key.
- In case of a key that is wrapped with a KEK, there is the extra step of unwrapping the recombined components to get the original key back.

The user flow for importing an encrypted key by components is similar to the steps described in ***Section 4.1*** with the following two differences:

- In ***Step 3***, the administrator needs to select "**Unwrap this key before import**" check box and select the KEK (unwrapping key).
- The KEK must exist in Fortanix DSM when the "Import Encrypted Key by Components" request is created. The KEK must have "**UNWRAPKEY**" permissions.

The following figure shows creating an "Import Key by Components" request with the "**Unwrap this key before import**" checkbox selected.

NOTE: The administrator is given the option to select the KEK.



Add New Security Object

Security Object name
Key 2

⊕ ADD DESCRIPTION

Import Key Component Test Group

● IMPORT ○ GENERATE

☑ Import Key from Components

⊕ ADD COMMENT

Select at least 2 key custodians to provide key component.

User3 ✕ User4 ✕

☑ Unwrap this key before import

Select Unwrapping Key (Mode: ECB)

Security objects with UnwrapKey permission are listed here

Search

🟩 Key 1

Choose a type

Certain types may be disabled due to the cryptographic policy.

● AES ○ DES3 ○ HMAC ○ OPAQUE

○ RSA ○ DES ○ EC ○ SECRET ○ Certificate

Key size 256 bits Key Check Value (KCV) C3B67D

For AES keys only allowed values are 128, 192, 256.

Key operations permitted

Certain operations may be disabled due to the cryptographic policy.

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

☑ Encrypt ☑ Decrypt ☑ WrapKey ☑ UnwrapKey

☑ DeriveKey ☑ MacGenerate ☑ MacVerify ☑ App Manageable

□ Sign □ Verify □ AgreeKey ☑ Export

Creating exportable Security Object can be unsafe

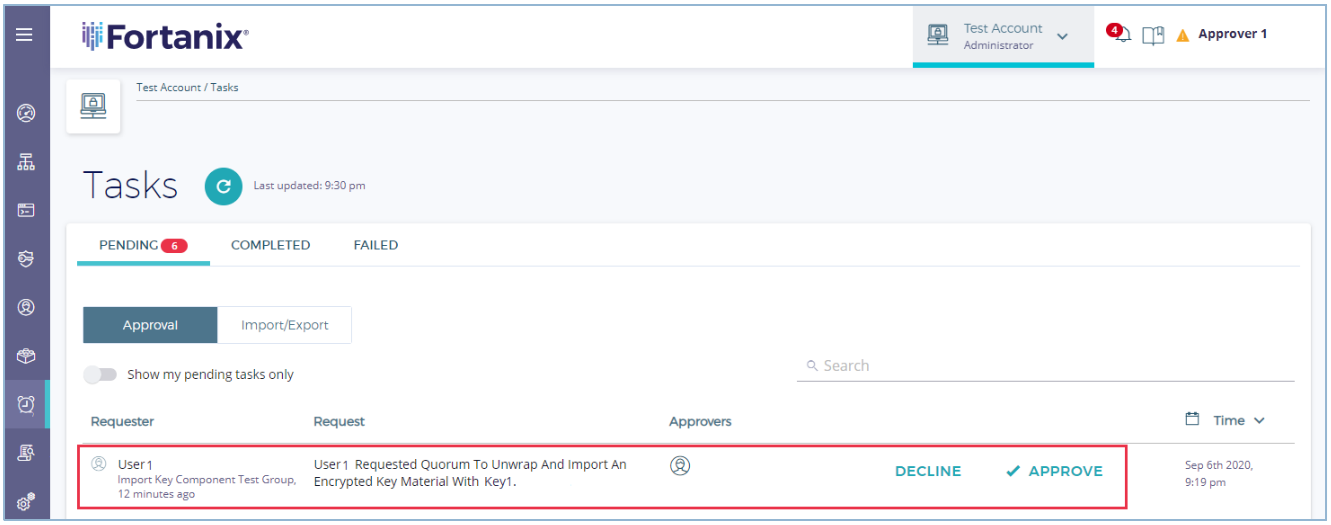
Audit log

☑ Enable audit logging

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

CANCEL SUBMIT REQUEST FOR COMPONENTS

FIGURE 18: REQUEST KEY COMPONENT WITH UNWRAPPING KEY

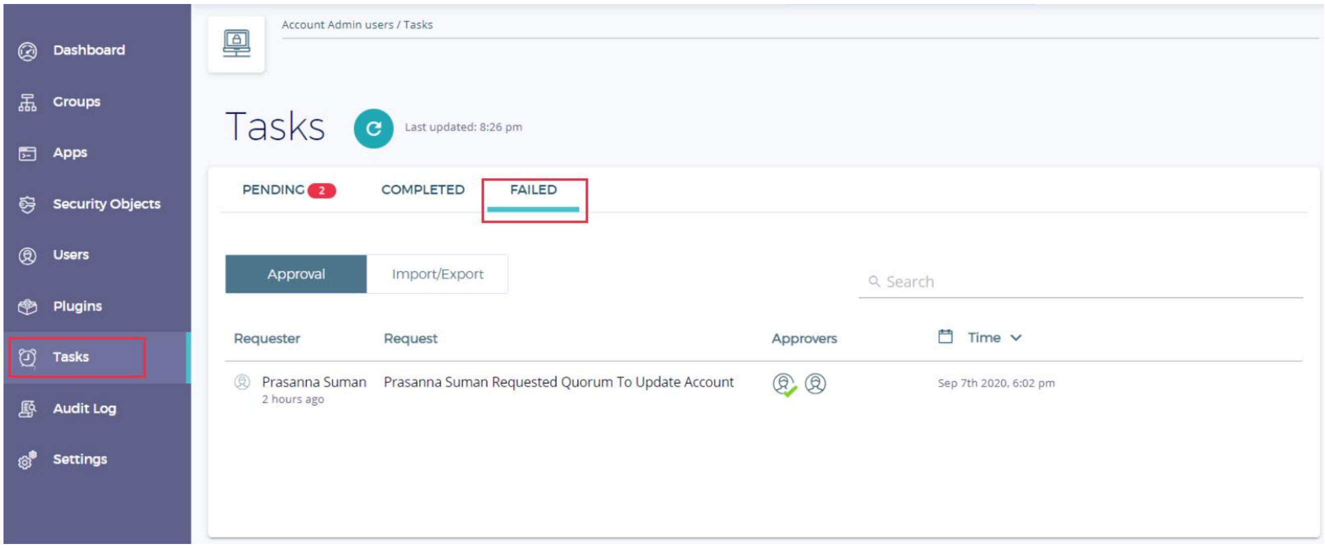


Requester	Request	Approvers		Time
User 1 Import Key Component Test Group, 12 minutes ago	User 1 Requested Quorum To Unwrap And Import An Encrypted Key Material With Key1.		DECLINE ✓ APPROVE	Sep 6th 2020, 9:19 pm

FIGURE 19: QUORUM APPROVAL FOR IMPORT AND UNWRAP ENCRYPTED KEY

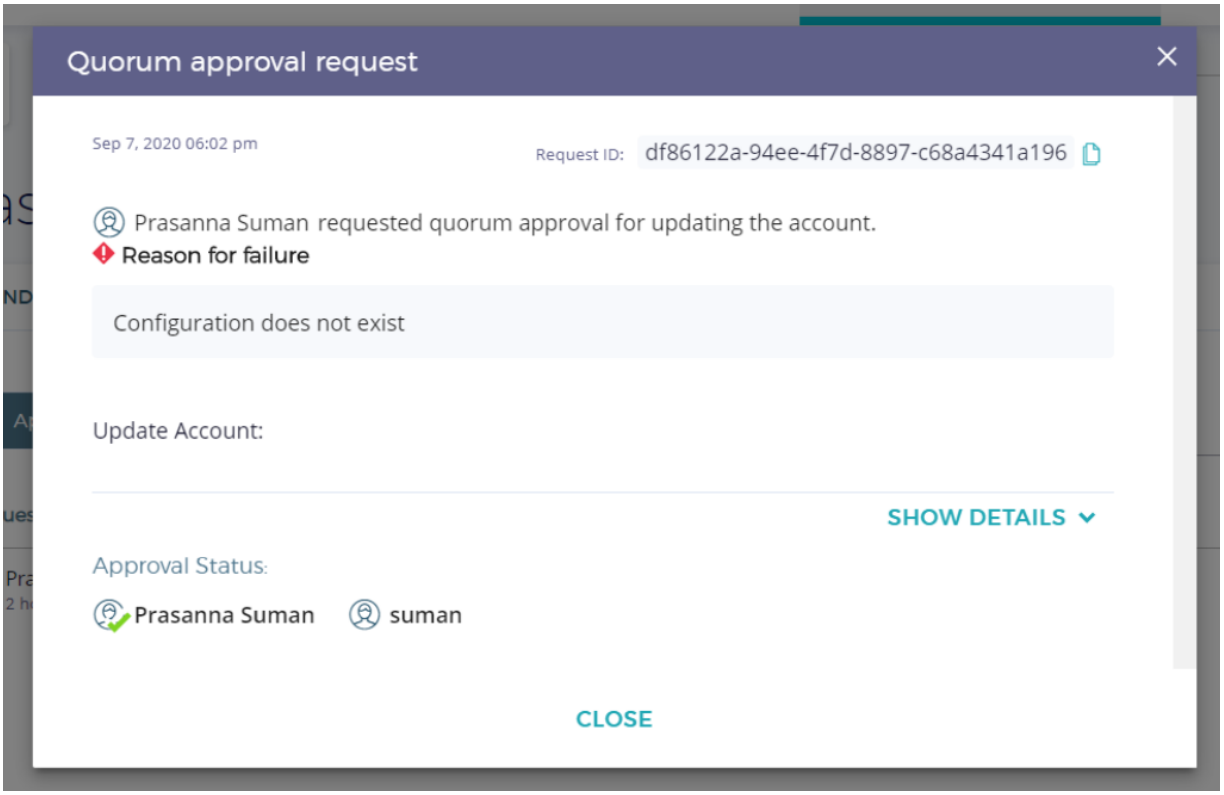
5.0 ERROR SCENARIOS

When a request fails (import request failure or the wrapping key does not have the “unwrap” permission) during the import/export operation, these “failed” scenarios are captured in the **Failed** tab on the **Tasks** page. The user will be notified about the failed task from the alert 🔔 icon on top of the page.



Requester	Request	Approvers	Time
Prasanna Suman 2 hours ago	Prasanna Suman Requested Quorum To Update Account		Sep 7th 2020, 6:02 pm

FIGURE 20: IMPORT TASK FAILED



Quorum approval request

Sep 7, 2020 06:02 pm

Request ID: df86122a-94ee-4f7d-8897-c68a4341a196

Prasanna Suman requested quorum approval for updating the account.

Reason for failure

Configuration does not exist

Update Account:

Approval Status:

Prasanna Suman suman

FIGURE 21: ERROR DETAILED VIEW

6.0 KEY EXPORT

6.1 EXPORT KEY CLEAR COMPONENTS USER FLOW

This section describes “Export Key by Components” feature of Fortanix DSM. The example assumes that:

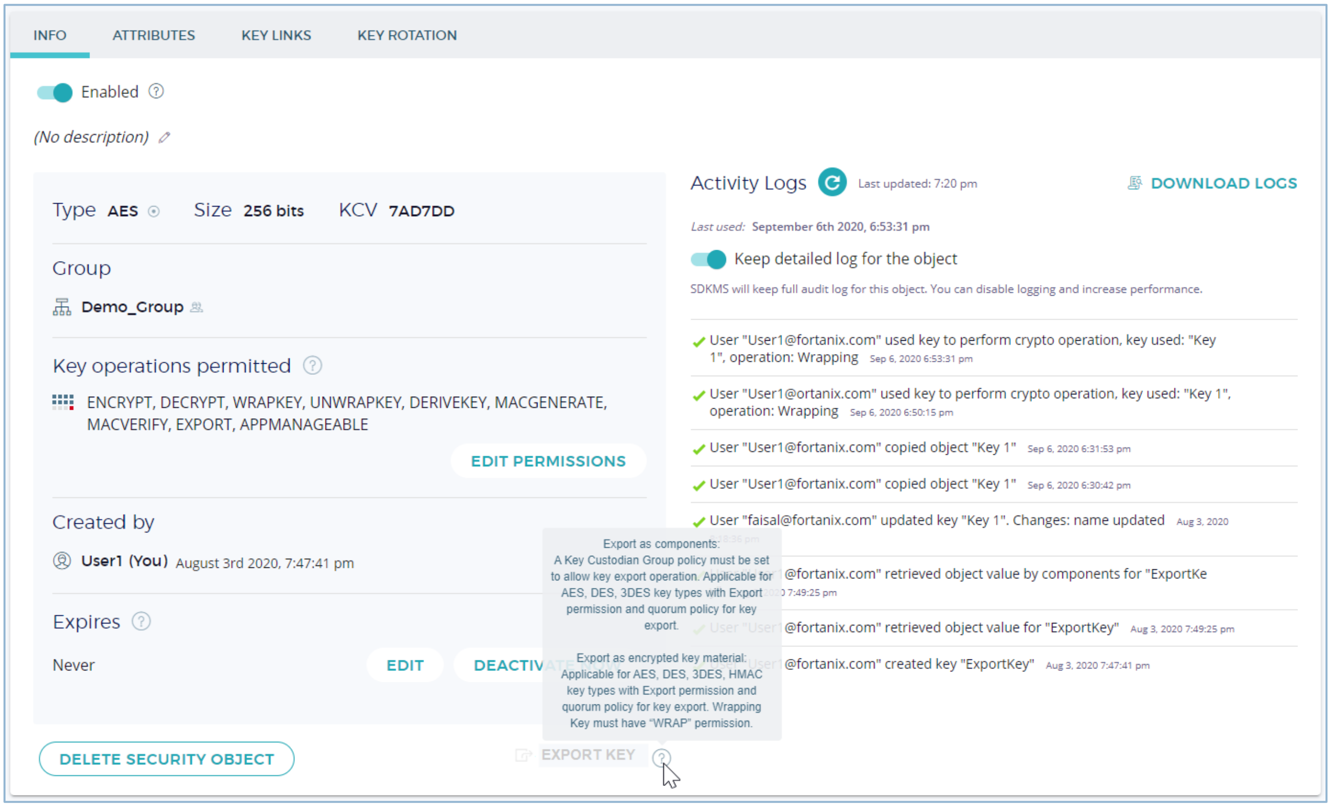
- A key with “**Export**” key permissions exists in the group.
- The group has the following quorum policy: the group members **Approver 1**, **Approver 2**, and **Approver 3** form a quorum group, and 2 out of the 3 member’s approvals are required to approve an operation in the group.

In this example:

- A group administrator **User1** creates an “Export Key by Components” request.
- Account members/administrators **User3** and **User 4** are selected to be the key custodians who are assigned as one of the Key Custodians in the **Key Custodian policy** for the group.
- The goal is to export the AES key named “**Key 1**” by components so that **User3** and **User4** each have a component of the key.

1. First, the group administrator **User1** creates an “Export Key Components” request by navigating to the detailed view of the key “**Key 1”** to be exported and should click **EXPORT KEY**. The **Figure 22** shows a detailed view of the SO “**Key 1”**.

NOTE: The **Export Key** check box will be disabled if the **Key Custodian policy** is not set at the group level.



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

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
- ✓ User "User1@fortanix.com" retrieved object value by components for "ExportKe 2020 7:49:25 pm
- ✓ User "User1@fortanix.com" retrieved object value for "ExportKey" Aug 3, 2020 7:49:25 pm
- ✓ User "User1@fortanix.com" created key "ExportKey" Aug 3, 2020 7:47:41 pm

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.

FIGURE 22: KEY CUSTODIAN POLICY NOT SET

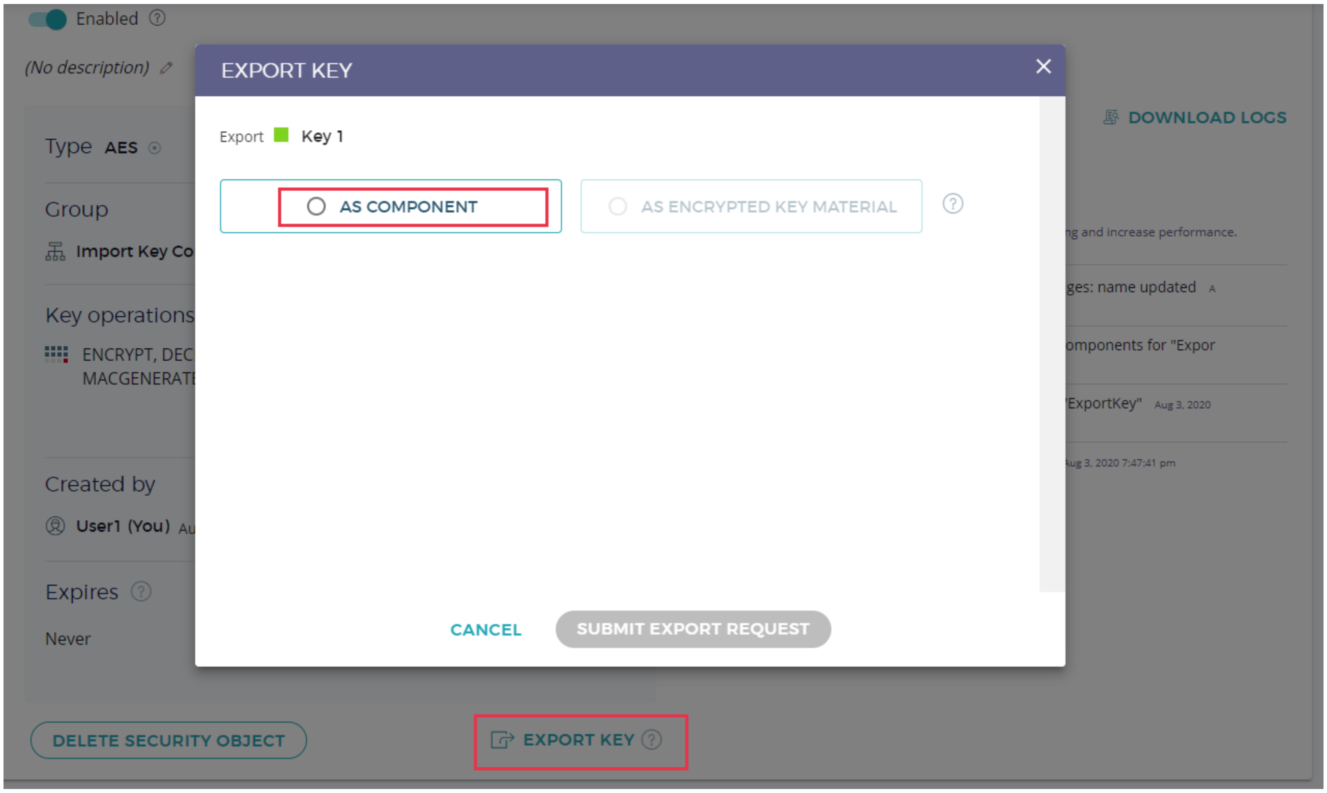
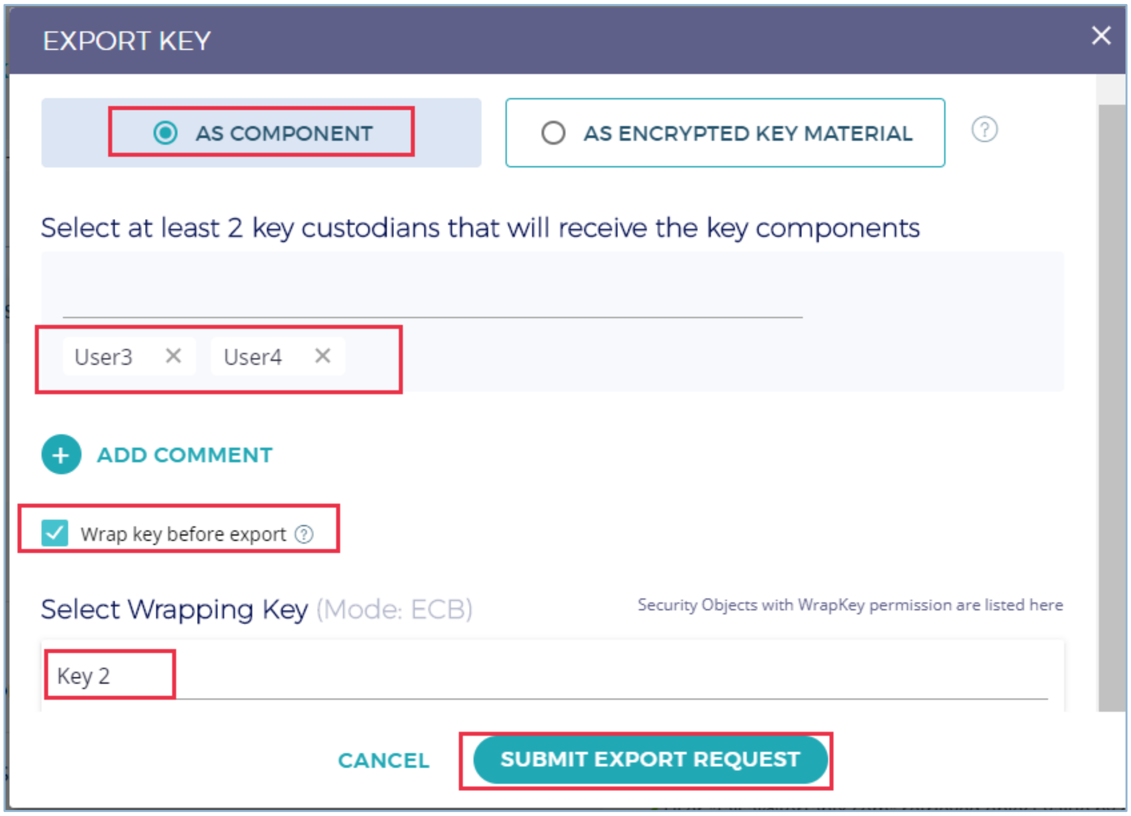


FIGURE 23: SELECT EXPORT

2. In the “EXPORT KEY” form, the administrator (**User1**) selects the **AS COMPONENT** radio button and provides the following details:

   - **Key custodians**: They need to be members of the Key Custodian group policy set at the group level. The administrator creating the request can assign themselves to be one of the key custodians in the group policy. The minimum number of participating Key Custodians is set at the Key Custodian Group policy. For example: When the minimum number of Key Custodians is set as 2 in the group policy, the user can select any two users from the group policy level to receive the key component.
   - **ADD COMMENT** (optional): The administrator can provide a short message describing the context or justification for this request.
   - **Wrap key before export**: Select if the key should be wrapped before being exported (***See Section 6.2***).



EXPORT KEY

● AS COMPONENT ○ AS ENCRYPTED KEY MATERIAL

Select at least 2 key custodians that will receive the key components

User3 ✕ User4 ✕

☑ Wrap key before export

Select Wrapping Key (Mode: ECB)

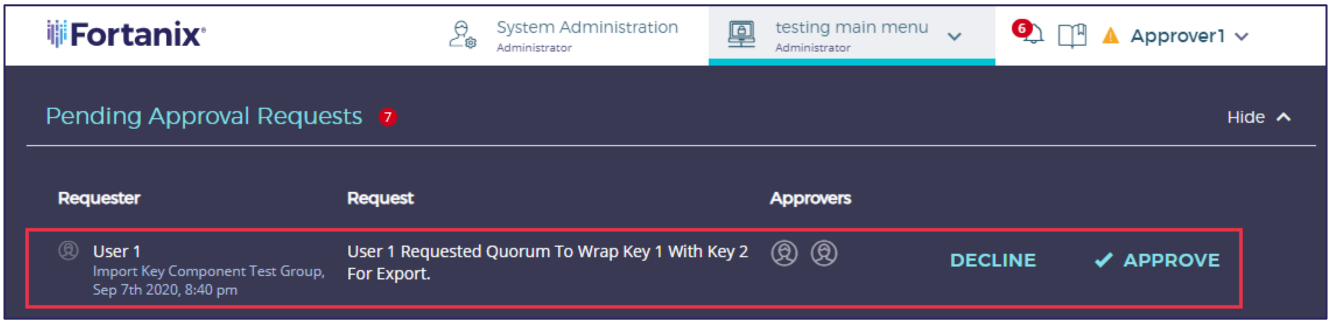
Security Objects with WrapKey permission are listed here

Key 2

FIGURE 24: SUBMIT EXPORT REQUEST

3. Once the key custodians are selected, the administrator clicks the **SUBMIT EXPORT REQUEST** to submit the export request.
4. Once the “Export by Components” request Is created, a quorum approval request will be sent to those group members that form part of the group quorum policy. In this example, **Approver 1**, **Approver 2**, and **Approver 3** will receive a notification (**Figure 25**) that the requester **User1** has created an “Export by Components” request of “**Key 1**”.

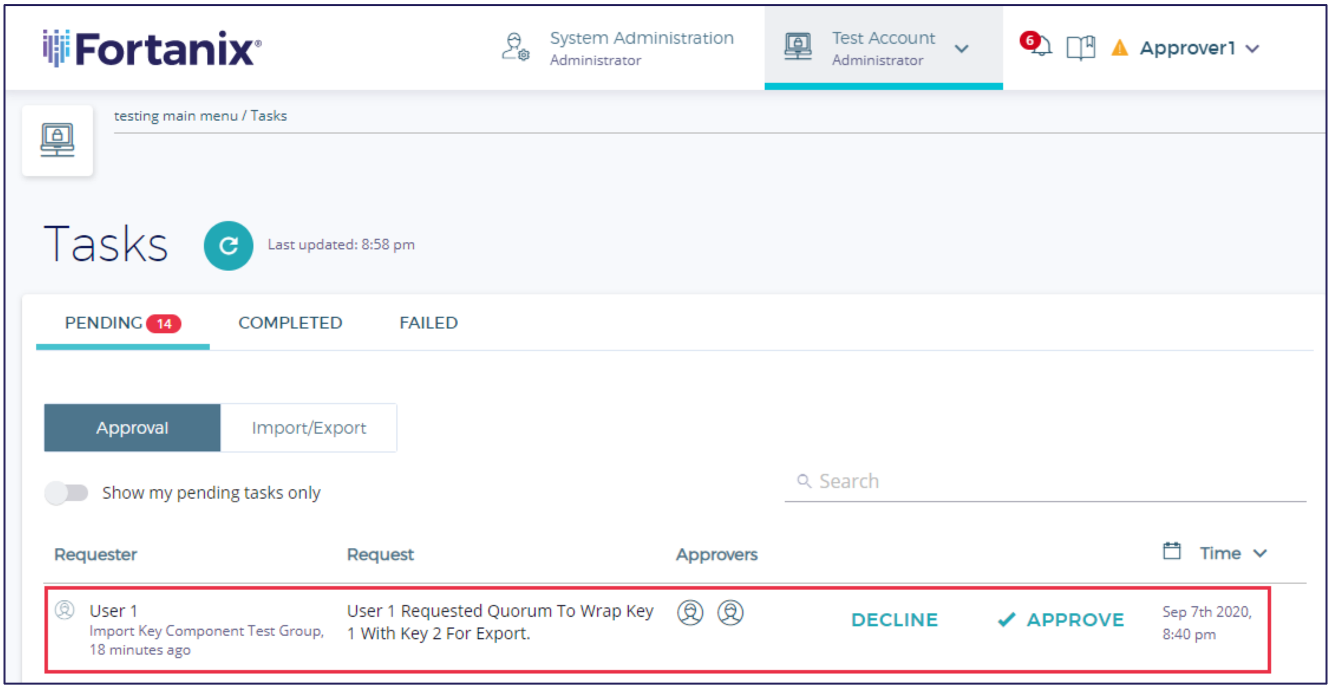
   NOTE: The members of the quorum policy may or may not overlap with the users that have been selected as key custodians.
5. The following figure shows **Approver 1’s** account page, where the “Export Key by Components” request is shown. At this point, **Approver 1** can approve or decline the request.



Requester	Request	Approvers		
User 1 Import Key Component Test Group, Sep 7th 2020, 8:40 pm	User 1 Requested Quorum To Wrap Key 1 With Key 2 For Export.		DECLINE	✓ APPROVE

FIGURE 25: KEY1 EXPORT REQUEST TO APPROVE

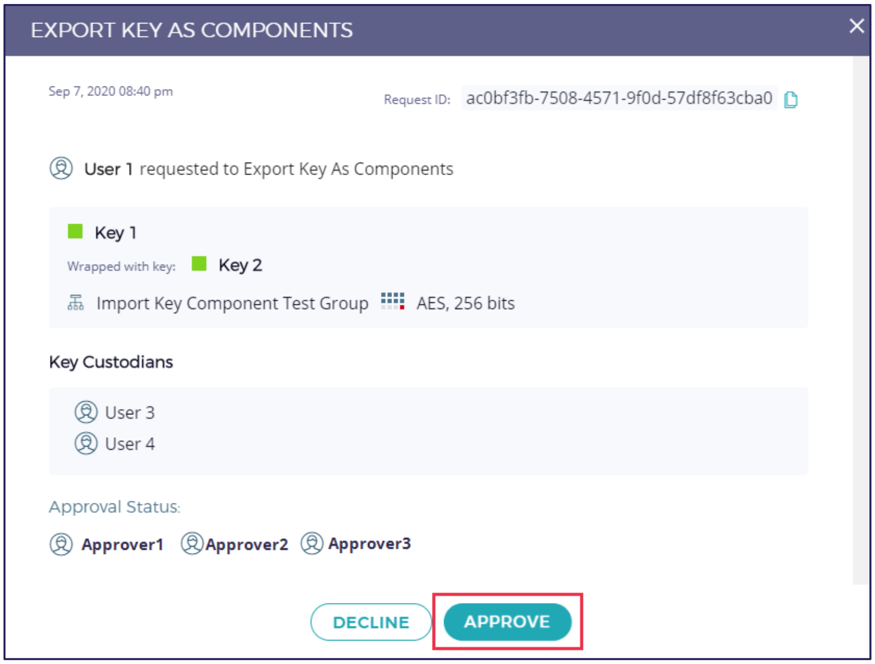
The **Approver** can also review the export key request from **TASKS** tab -> **PENDING** tab -> **Approval** tab in the Fortanix DSM UI.



Requester	Request	Approvers			Time
User 1 Import Key Component Test Group, 18 minutes ago	User 1 Requested Quorum To Wrap Key 1 With Key 2 For Export.		DECLINE	✓ APPROVE	Sep 7th 2020, 8:40 pm

FIGURE 26: REVIEW EXPORT KEY TASK

6. The **Approver1** can review the export request by clicking the **APPROVE** button.



EXPORT KEY AS COMPONENTS

Sep 7, 2020 08:40 pm

Request ID: ac0bf3fb-7508-4571-9f0d-57df8f63cba0

User 1 requested to Export Key As Components

🟩 Key 1

Wrapped with key: 🟩 Key 2

Import Key Component Test Group AES, 256 bits

Key Custodians

User 3

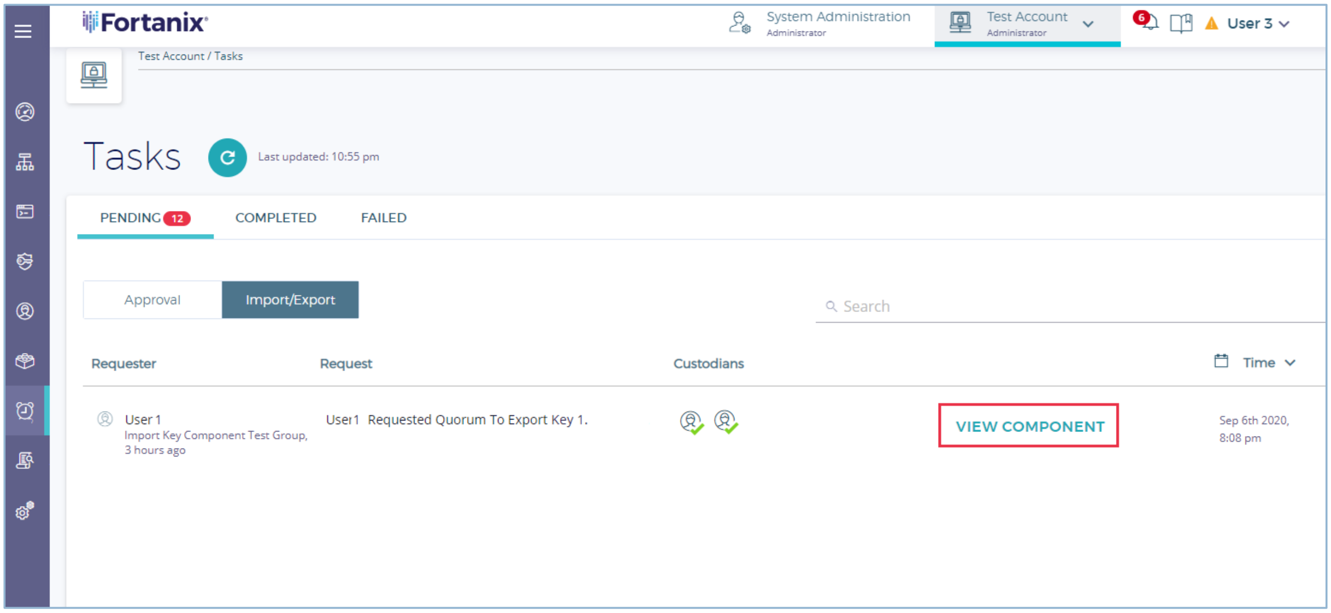
User 4

Approval Status:

Approver1 Approver2 Approver3

FIGURE 27: APPROVE EXPORT REQUEST

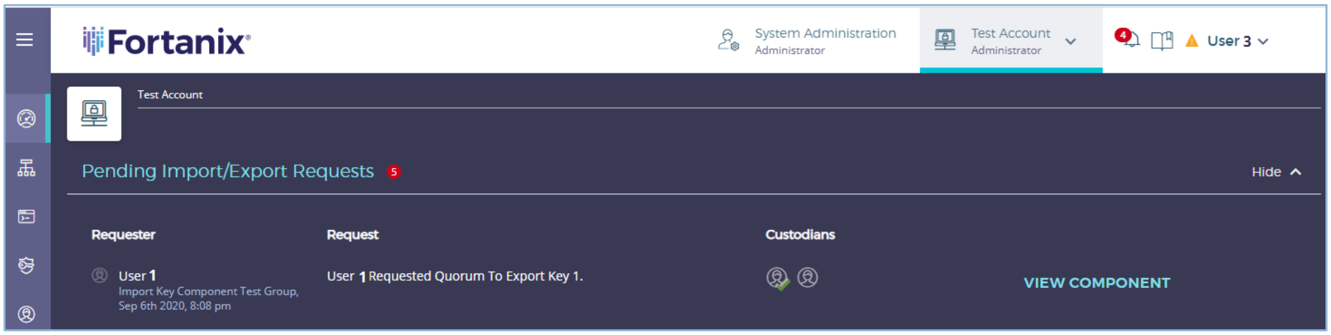
7. This step must also be performed by **Approver2** or **Approve 3** so that quorum is achieved.
8. Once the quorum is achieved, the key custodians will receive a notification that a key component was granted to them. In this example, when the export request is approved, and when one of the key custodians (example: **User3**), navigates to the Account page, a notification is displayed.
9. Once the quorum Approvers approve the “Key Export” request, the Exported component will now be available for **User3** and **User4** under **TASKS** tab -> **PENDING** tab -> **Import/Export** tab in the Fortanix DSM UI.



Requester	Request	Custodians		Time
User 1 Import Key Component Test Group, 3 hours ago	User1 Requested Quorum To Export Key 1.		VIEW COMPONENT	Sep 6th 2020, 8:08 pm

FIGURE 28: VIEW KEY COMPONENT

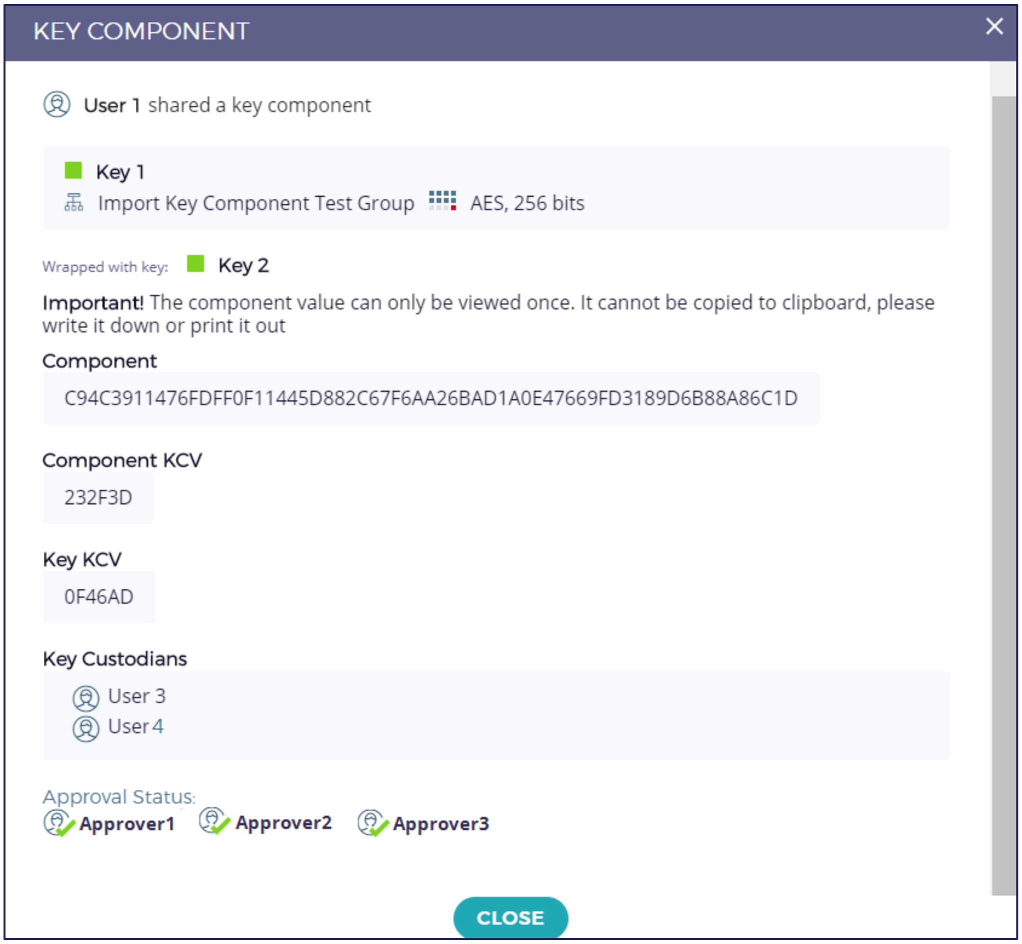
The component is also visible from the Fortanix DSM dashboard.



Requester	Request	Custodians	
User 1 Import Key Component Test Group, Sep 6th 2020, 8:08 pm	User 1 Requested Quorum To Export Key 1.		VIEW COMPONENT

FIGURE 29: VIEW COMPONENT

10. Any Approver can cancel the export operation by clicking the **DECLINE** button. At this point, the “Export by Components” request is declined, and key custodians will not receive the key components. This state is final; once a request is declined by a reviewer, it cannot be approved even if other approvers approve the request.
11. By clicking the **VIEW COMPONENT** link, the user will be displayed with the export request details and the key component data they own:



KEY COMPONENT

User 1 shared a key component

🟩 Key 1
Import Key Component Test Group AES, 256 bits

Wrapped with key: 🟩 Key 2

Important! The component value can only be viewed once. It cannot be copied to clipboard, please write it down or print it out

Component
C94C3911476FDFF0F11445D882C67F6AA26BAD1A0E47669FD3189D6B88A86C1D

Component KCV
232F3D

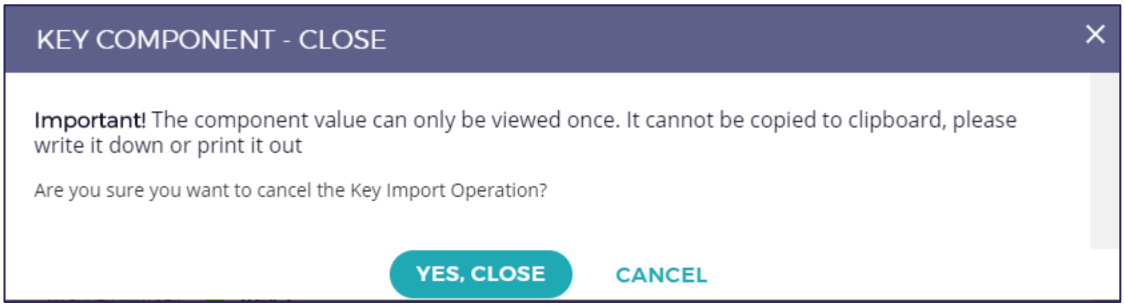
Key KCV
0F46AD

Key Custodians
User 3
User 4

Approval Status:
Approver1 Approver2 Approver3

FIGURE 30: REVIEW KEY 1 EXPORT COMPONENT DETAILS

NOTE: The key component value is displayed ONLY once when a key is exported as a component. It is recommended that the user note the component value by writing it or printing it.



KEY COMPONENT - CLOSE

Important! The component value can only be viewed once. It cannot be copied to clipboard, please write it down or print it out

Are you sure you want to cancel the Key Import Operation?

FIGURE 31: WARNING

6.2 EXPORT ENCRYPTED KEY COMPONENT USER FLOW

Fortanix DSM provides the option to specify a KEK that wraps the exported key and then split the key into components parts. The process on Fortanix DSM is:

a. Wait until quorum approval is reached.

b. Once a quorum is reached, Fortanix DSM wraps the key to be exported with the KEK selected during the Export key as Components operation.

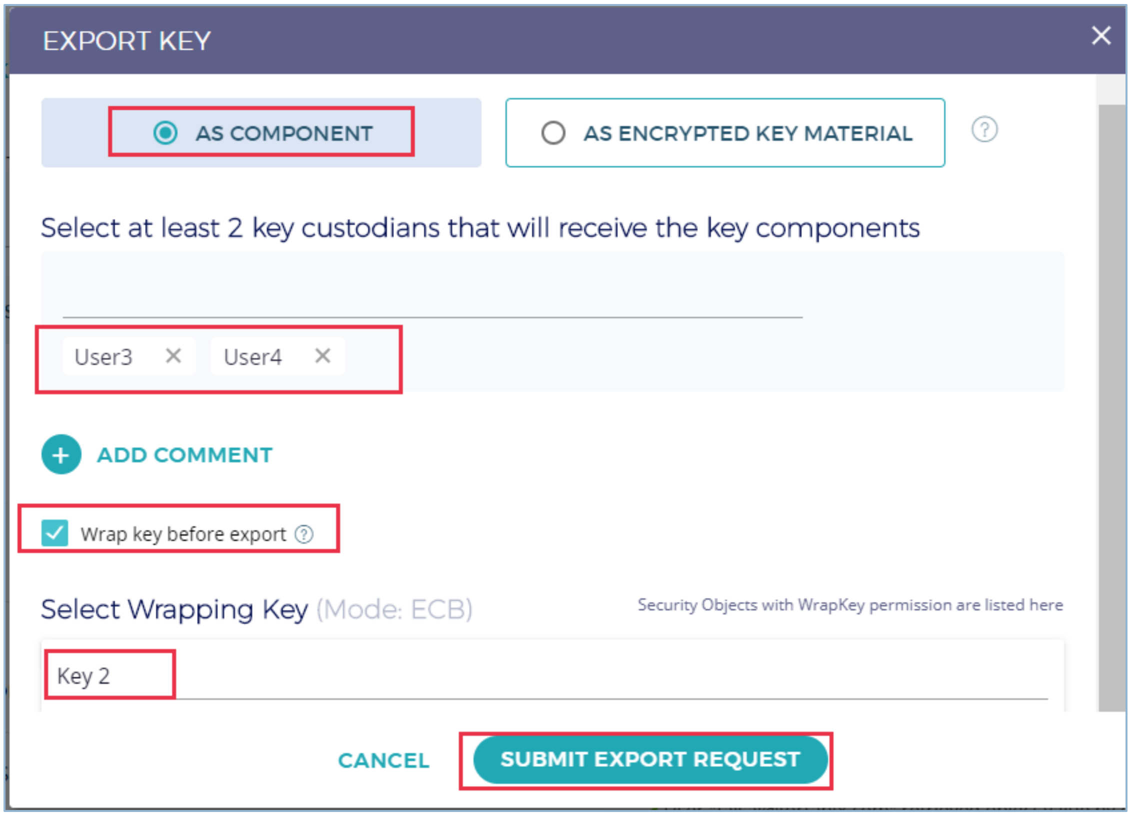
c. Fortanix DSM splits the wrapped material from ***Step b*** into components.

d. The generated components from ***Step c*** are made available to the corresponding custodians.

Exporting Encrypted Key in components user flow is similar to the flow described in the previous ***section 6.1***, with the following two differences:

- In ***Step 1*** of ***Section 6.1***, the administrator (**User1**) needs to select "**Wrap key before export**" check box and select the KEK.
- The KEK must exist in Fortanix DSM when the "Export Key by Components" request is created. The KEK must belong to the same group as the key that is to be exported and have the "**WRAPKEY**" permissions.

The following figure shows creating an "Export Key by Components" request with the "**Wrap key before export**" check box selected. Note that the administrator is given the option to select the KEK.



EXPORT KEY

● AS COMPONENT ○ AS ENCRYPTED KEY MATERIAL

Select at least 2 key custodians that will receive the key components

User3 ✕ User4 ✕

☑ Wrap key before export

Select Wrapping Key (Mode: ECB)

Security Objects with WrapKey permission are listed here

Key 2

FIGURE 32: WRAP KEY BEFORE EXPORT

7.0 DOCUMENT INFORMATION

7.1 DOCUMENT LOCATION

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

https://support.fortanix.com/hc/en-us/articles/360043559332-User-s-Guide-Key-Components

7.2 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.