Fortanix®

User Guide

FORTANIX DATA SECURITY MANAGER – KEY UNDO POLICY

VERSION 1.0

Fortanix Inc. | 3910 Freedom Circle | Suit 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) Key Undo Policy User Guide. This document describes the features of the Fortanix DSM Key Undo Policy. It also contains the information related to:

- Configuring Key undo policy for a group
- Destroy and delete security objects with reversible period configuration
- Remove private key with Key undo policy
- Deactivate and compromise key with Key undo policy
- Remove key operations with Key undo policy
- Multiple key reversible changes with Key undo policy

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 secret, 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 KEY UNDO POLICY FOR A GROUP

To stop accidental sensitive operations on keys, Fortanix DSM allows a user to add a "Key undo policy". When the policy is added, the keys will go through a 2-step process in which the sensitive operations can be undone until a waiting period set by the user before the changes become permanent. The maximum period until which the changes can be undone is 180 days. As a best practice, a minimum period of 7 days is recommended. The following sensitive operations can be undone:

- Change group
- Delete and destroy key
- Deactivate and activate a key
- Mark a key as compromised
- Remove private key
- Remove sensitive key operations encrypt, decrypt, sign, verify, and so on.

NOTE: Quorum approval is not required to create a "Key undo policy".

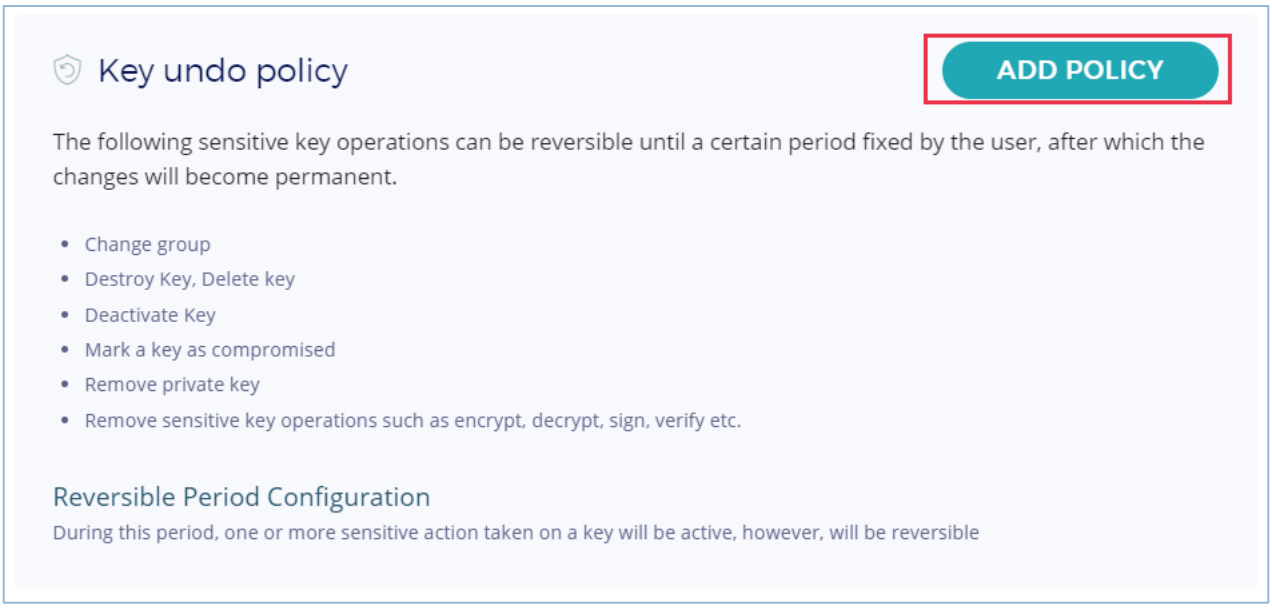

FIGURE 1: KEY UNDO POLICY

To add the "Key undo policy":

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

2. Set the waiting period until which the sensitive operations are reversible under the **Reversible Period Configuration** section.

   NOTE: By default, the Key reversible period is set to **7** days for all the sensitive operations listed above. The minimum waiting period during which a sensitive key operation is reversible is **7** days and the maximum period is **180** days. For Key Destroy operation once the key is destroyed the key metadata can be configured to be automatically or manually deleted.

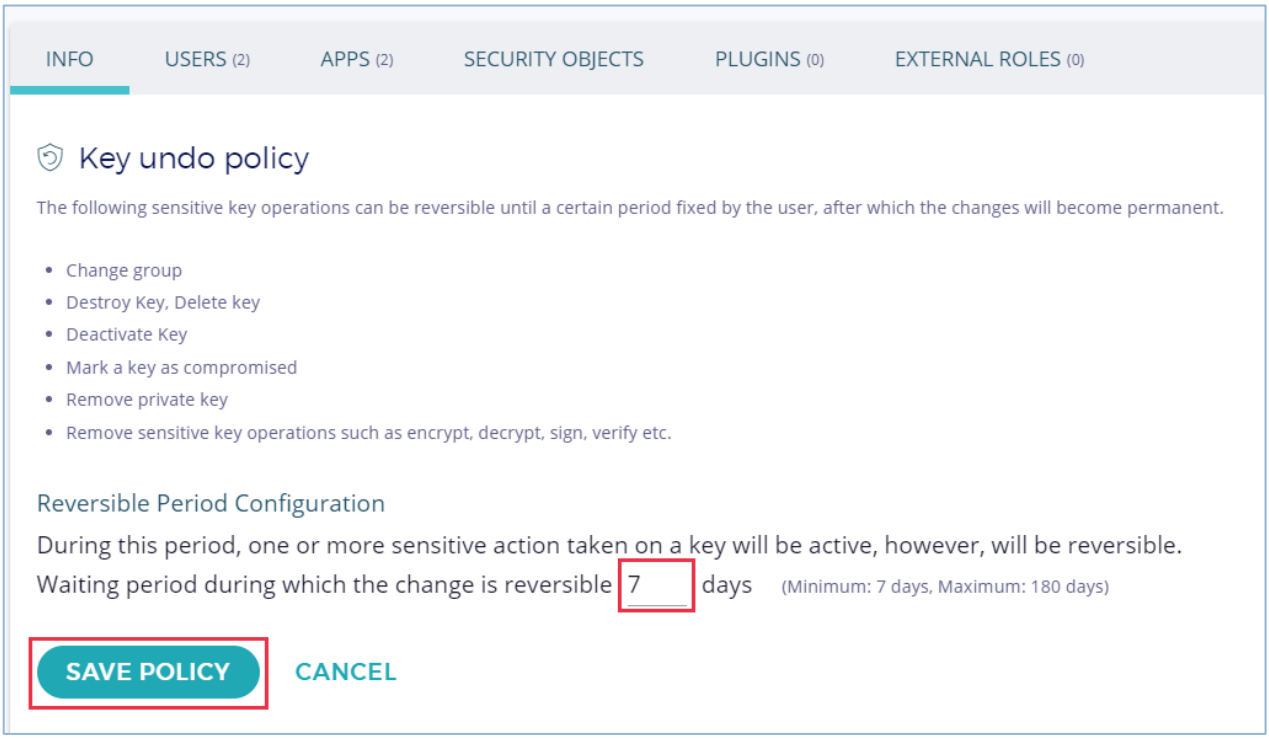

FIGURE 2: CONFIGURE KEY UNDO POLICY

3. The policy is saved successfully.

NOTE: If the reversible period in the policy is updated with a new value, then this will not update the reversible period of the sensitive operations that are already performed with a previous reversible value.

3.1 KEY UNDO POLICY STATE FOR DESTROY AND DELETE KEY

- **Destroyed state**: The key is considered as destroyed in this state. The user has the option to cancel the destroy operation. This will be allowed until the time period specified in the "Key

undo policy" after which the key will be permanently destroyed. When a key is in a destroyed state, the key material will be deleted, and it will retain only the key metadata. The key metadata has the following details:

- Key name
- Key type
- Key description
- The group that it belongs to
- The enabled key operations
- Created by user
- Expiration date if available
- All its activity logs

If the "key destroy" operation is canceled, then the key material will be retained.

- **Deleted state**: In the "Deleted" state the key which was in the "Destroyed" state will be permanently deleted manually or automatically along with the key metadata. At this time, there will not be any trace left of that key in Fortanix DSM, however, all such actions will be audited as part of audit logs. A key can also be directly deleted without entering the destroyed state.

3.2 DESTROY SECURITY OBJECTS WITH REVERSIBLE PERIOD CONFIGURATION

To destroy a Fortanix DSM key with reversible period configuration:

1. Go to the detailed view of the security object and click the **DESTROY KEY** button.

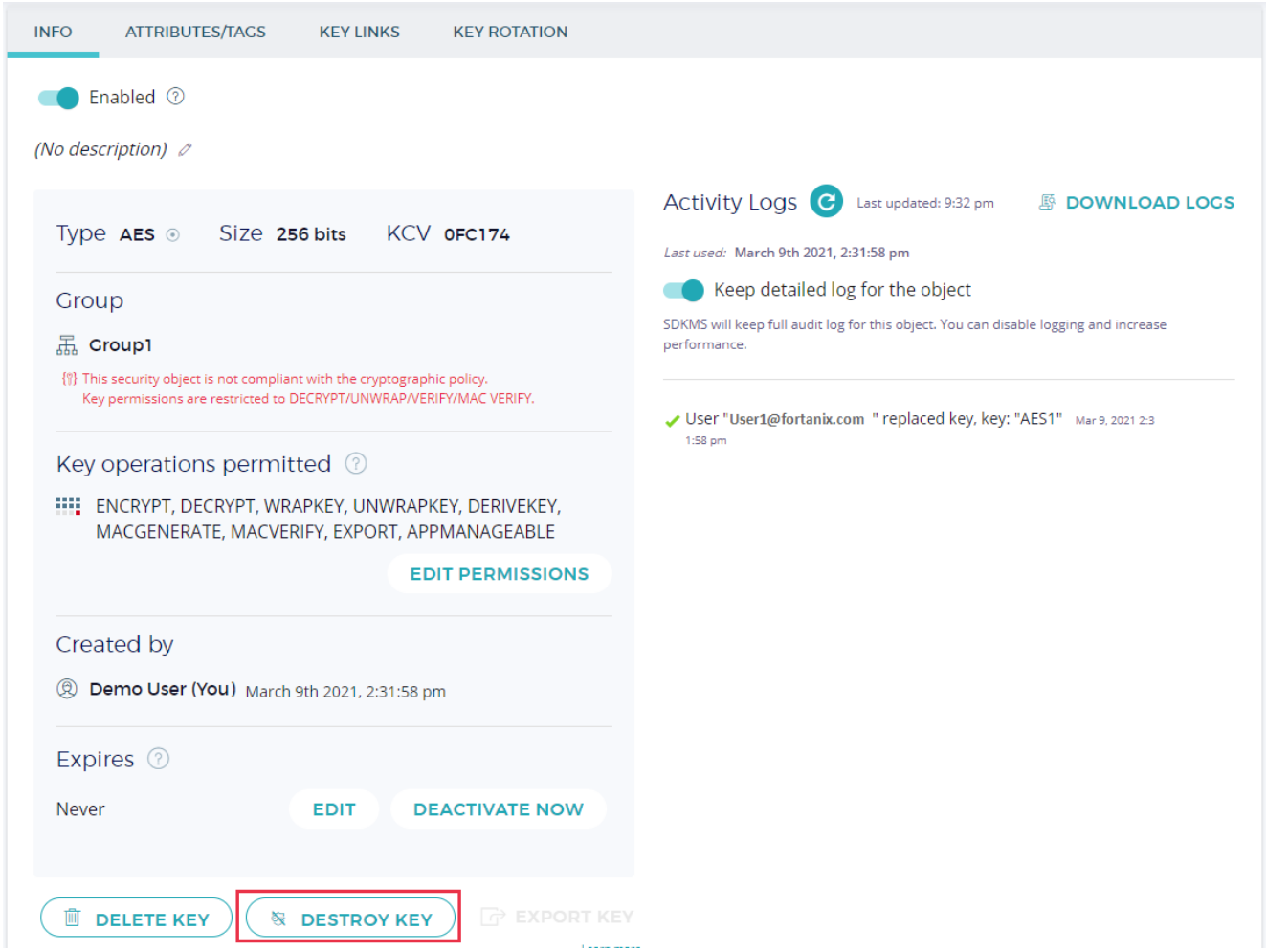

FIGURE 3: DESTROY SECURITY OBJECT

2. In the DESTROY KEY confirmation window, click the check box(es) which is a warning that a user should read and select before destroying the security object. Once this check box(es) are selected, it will enable the **DESTROY** button. You can see the time period until which the key destroy operation will be reversible.

NOTE: If the Security Object had a quorum approval set, then an Approval Request will be initiated once you click the **DESTROY** button in the window below.

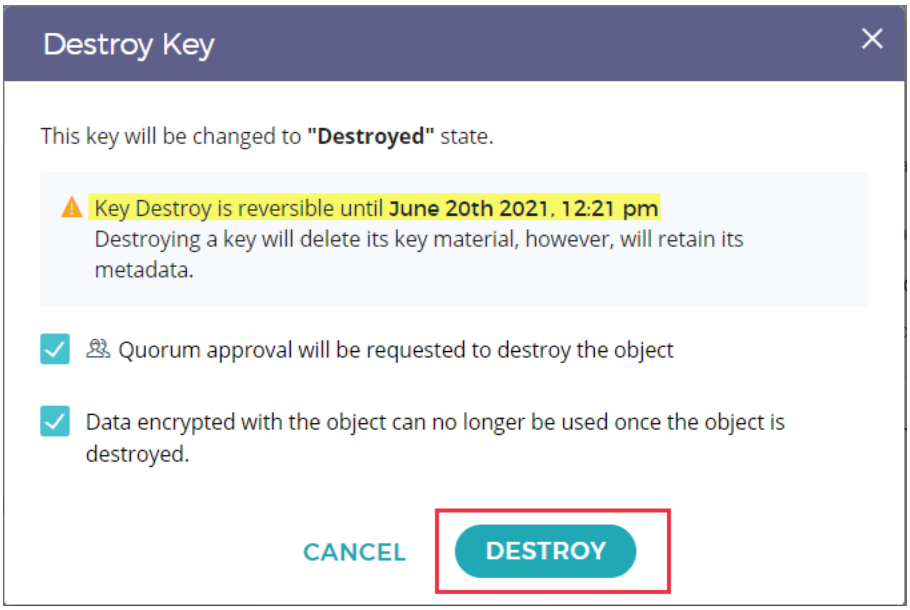

FIGURE 4: DESTROY SECURITY OBJECT

3. Click **DESTROY** to enter the "destroyed" state. The user also has an option to "Cancel" the Key Destroy operation using the **CANCEL** button.
4. You could also start the key destroy process for a key from the SO table view. Select the security object and click the **DESTROY SELECTED** button.

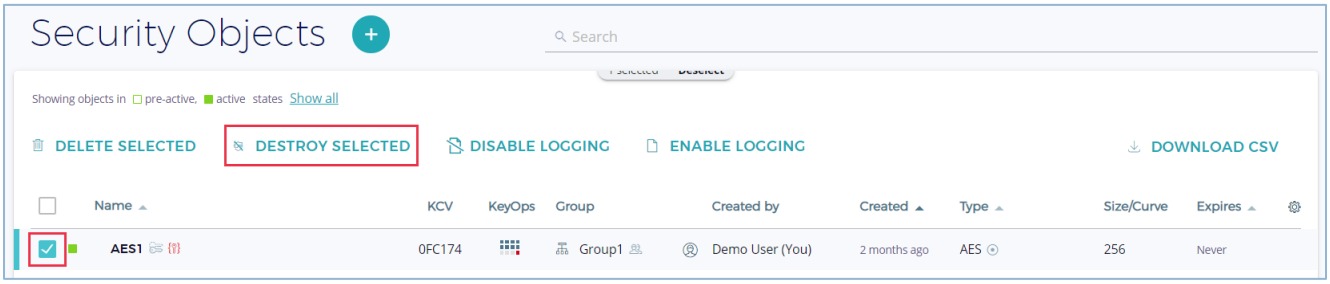

FIGURE 5: DESTROY SO FROM TABLE VIEW

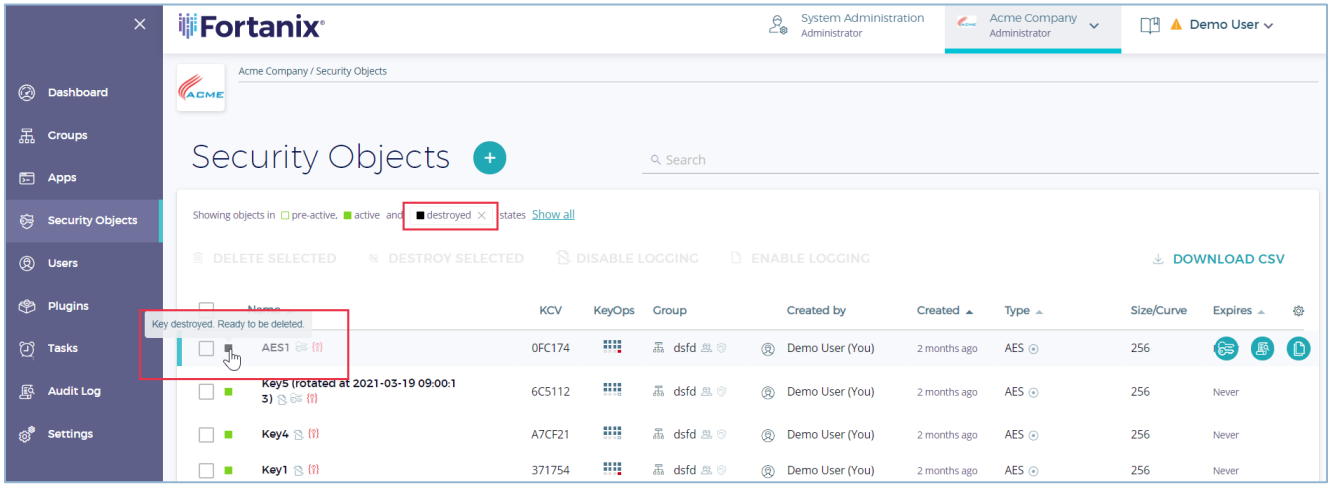

FIGURE 6: KEY IN DESTROYED STATE IN SO TABLE VIEW

Hover on the key to see that the key is in the "Destroyed" state. Notice that the color of the destroyed key icon is black ■ to indicate that the key is destroyed but the action is reversible until a certain period.

5. You will now see an indicator on top of the Security Object detailed view page which shows that the key is destroyed and the time period until which the "Key Destroy" operation can be reversed. You can cancel the "Key Destroy" operation using the **CANCEL CHANGE** button.

   NOTE: If the group that the security object belongs to has a Quorum Policy set, then the "Cancel Change" action will initiate a quorum approval request to confirm the "Key destroy cancel" operation.

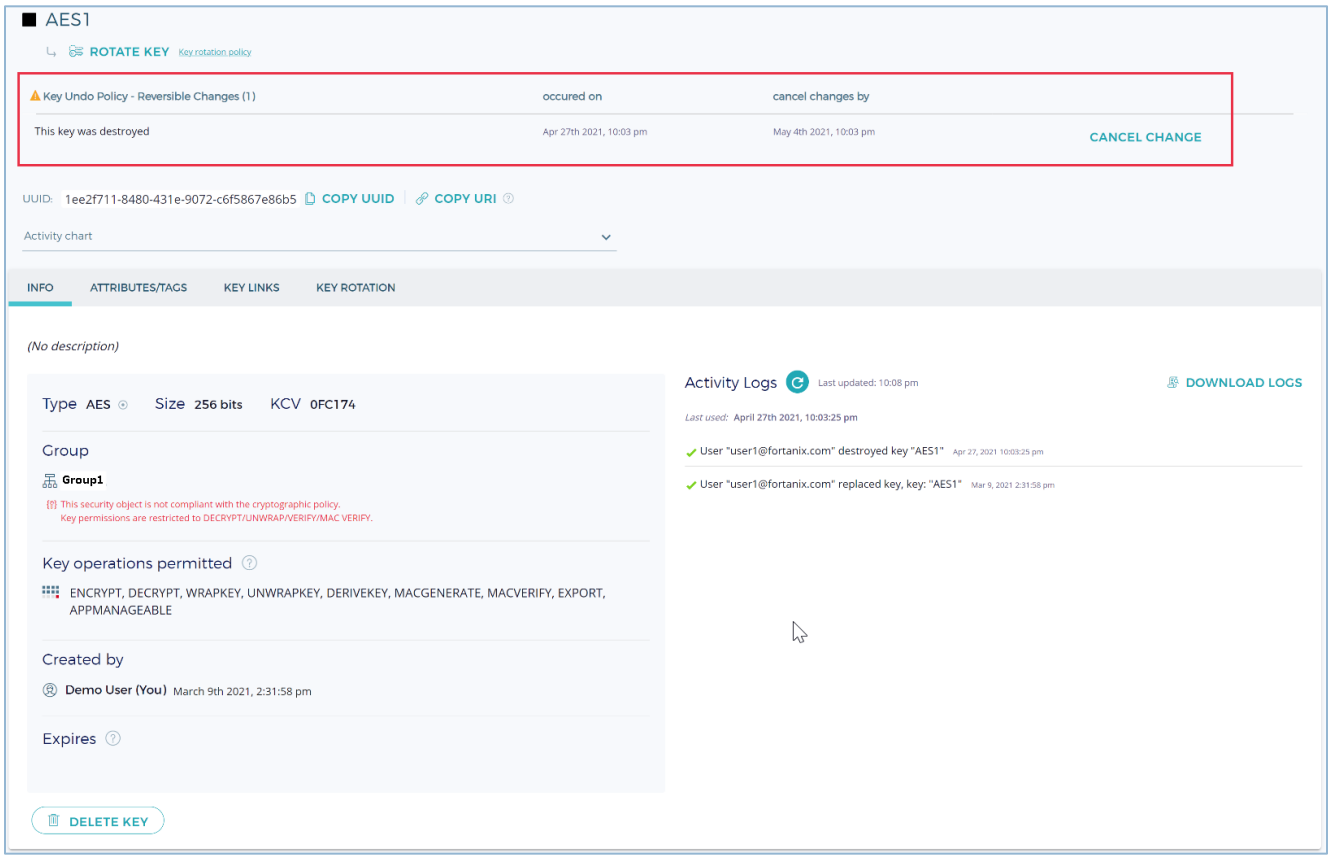

FIGURE 7: REVERSIBLE KEY DESTROYED STATE

6. After the time period to reverse the "Destroyed" state of the key completes, the action cannot be undone.

   NOTE: When a security object is in a "destroyed" state with reversible period configuration, the user can still choose to delete it using the **DELETE KEY** button (Figure 8). The delete operation will now enter a reversible period until which the delete operation can be canceled.

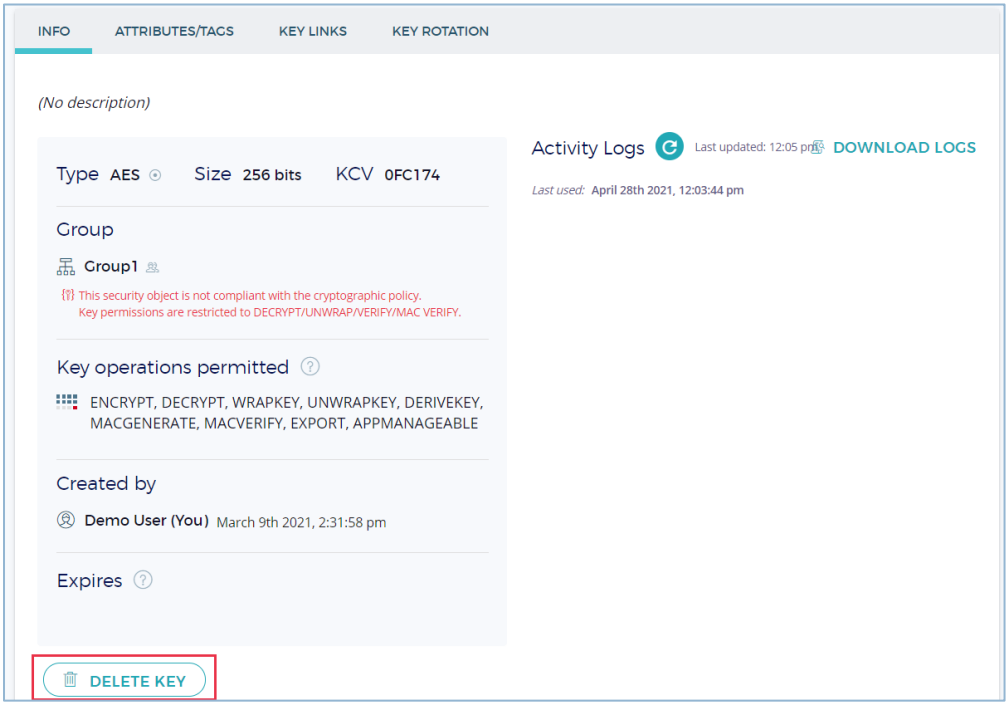

FIGURE 8: ENTERING DELETE SECURITY OBJECT STATE

7. To delete the key metadata permanently, click the **DELETE KEY** button. Since the "Key undo policy" is active, the key delete operation is reversible until the specified time period.

NOTE: If the group that the security object belongs to has a Quorum Policy set, then the "Cancel Change" action will initiate a quorum approval request to confirm the "Key delete cancel" operation.

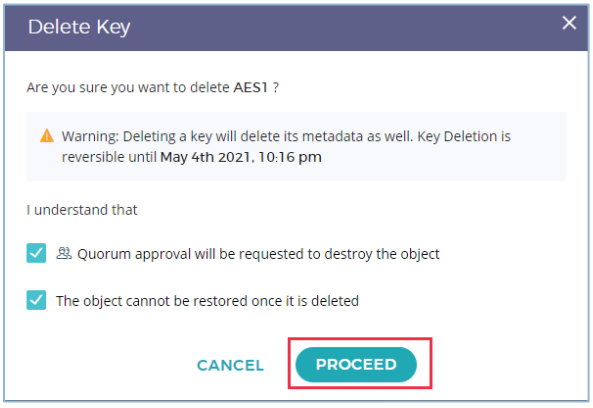

FIGURE 9: PURGE KEY METADATA CONFIRMATION

8. In the DELETE SECURITY OBJECT window, select the check boxes to confirm that you do not need the key metadata anymore and want to delete the key permanently. Once the check boxes are selected it will enable the **PROCEED** button.
9. Click the **PROCEED** button. You will now see an indicator on top of the Security Object detailed view page that shows that the key is deleted and the time period until which the "Key Delete" operation can be reversed. You can cancel the "Key Delete" operation using the **CANCEL CHANGE** button.

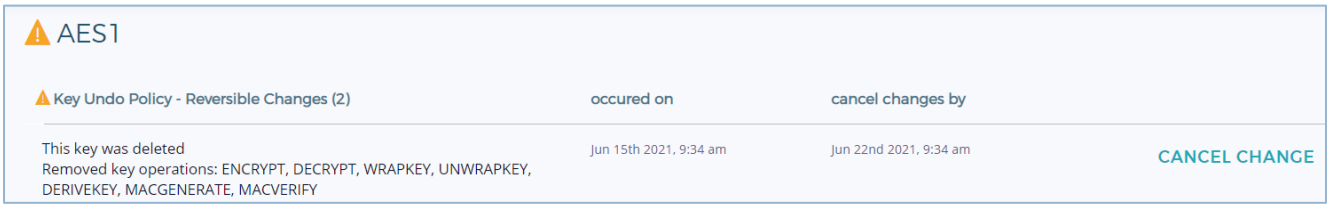

FIGURE 10: CANCEL KEY DELETE

10. The key deletion now enters the "pending deletion" state.

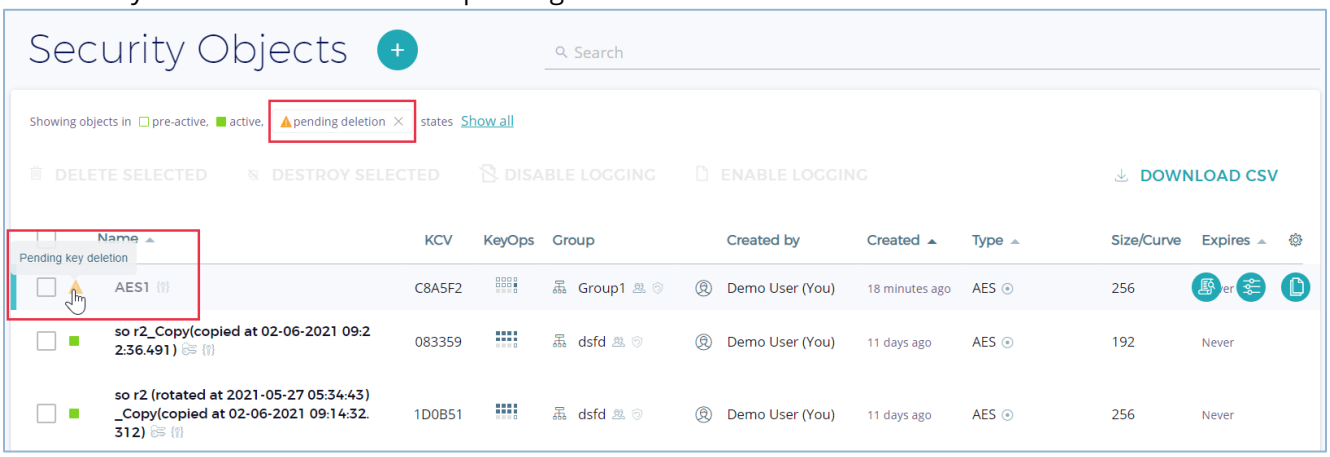

FIGURE 11: KEY DELETED

Now, the key will be automatically deleted once the time period to reverse the "Deleted" state of the key elapses.

3.3 REMOVE PRIVATE KEY WITH KEY UNDO POLICY

If the "Key undo policy" is set at the group level, when you click the **REMOVE PRIVATE KEY** button from the detailed view of a key, the Private Key is removed, and the removal operation becomes reversible until the time period set in the policy.

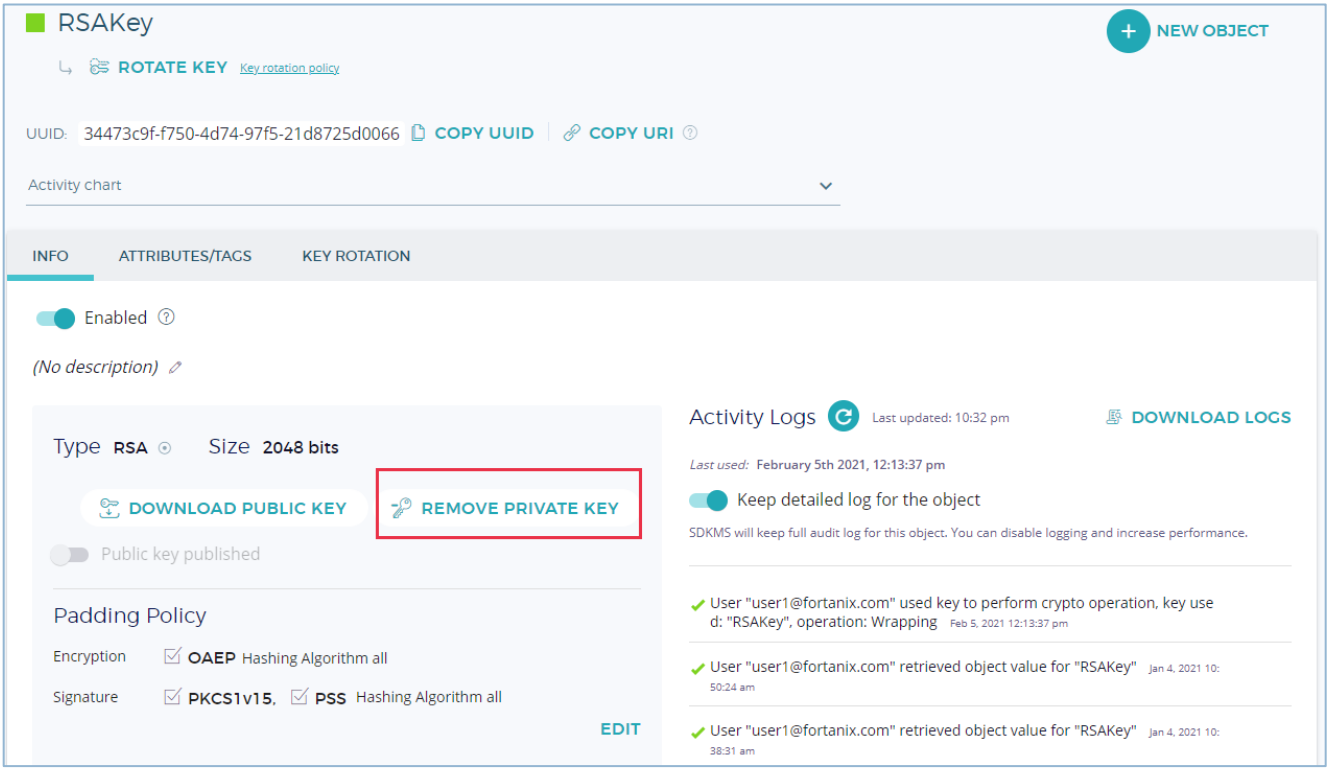

FIGURE 12: REMOVE PRIVATE KEY

1. Click **YES, REMOVE** to confirm the private key removal operation.

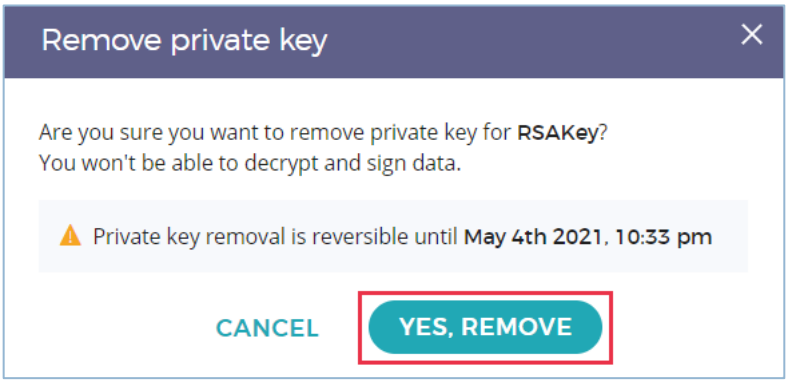

FIGURE 13: CONFIRM PRIVATE KEY REMOVAL

2. A key whose private key is removed is represented as . Notice on the top of the screen that you have an option to reverse the private key removal operation using the **CANCEL CHANGE** button.

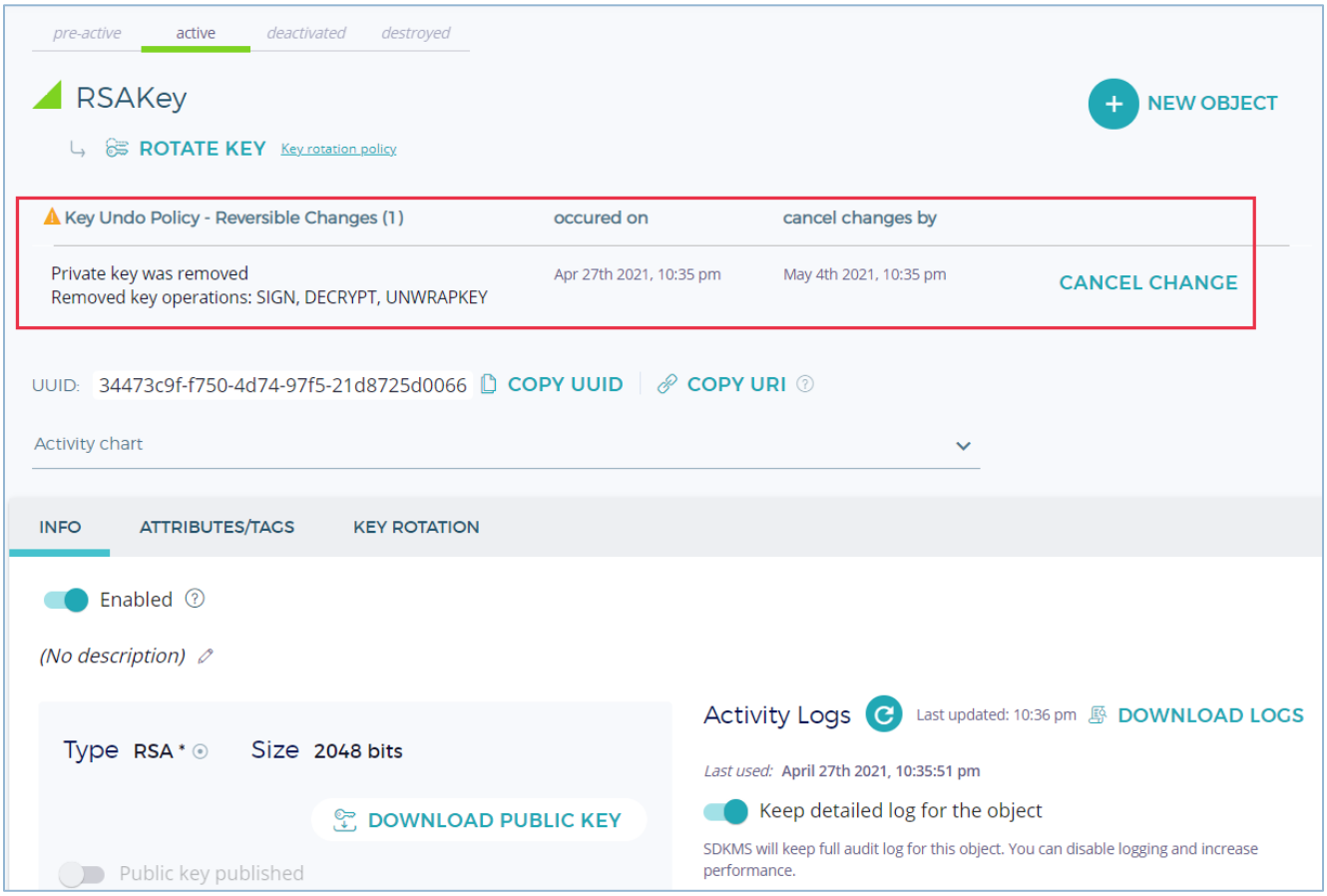

FIGURE 14: CANCEL PRIVATE KEY REMOVAL

3. Once the time elapses to revert the Private Key removal operation, the Private Key will be permanently removed.

3.4 DEACTIVATE AND COMPROMISE KEY WITH KEY UNDO POLICY

If the "Key undo policy" is set at the group level, when you click the **DEACTIVATE NOW** button from the detailed view of a key, the deactivate key/compromise operation becomes reversible until the time period set in the policy.

If the key is compromised, then select the check box **The key has been compromised**.

1. Click **DEACTIVATE** button to confirm the key deactivation/compromise.

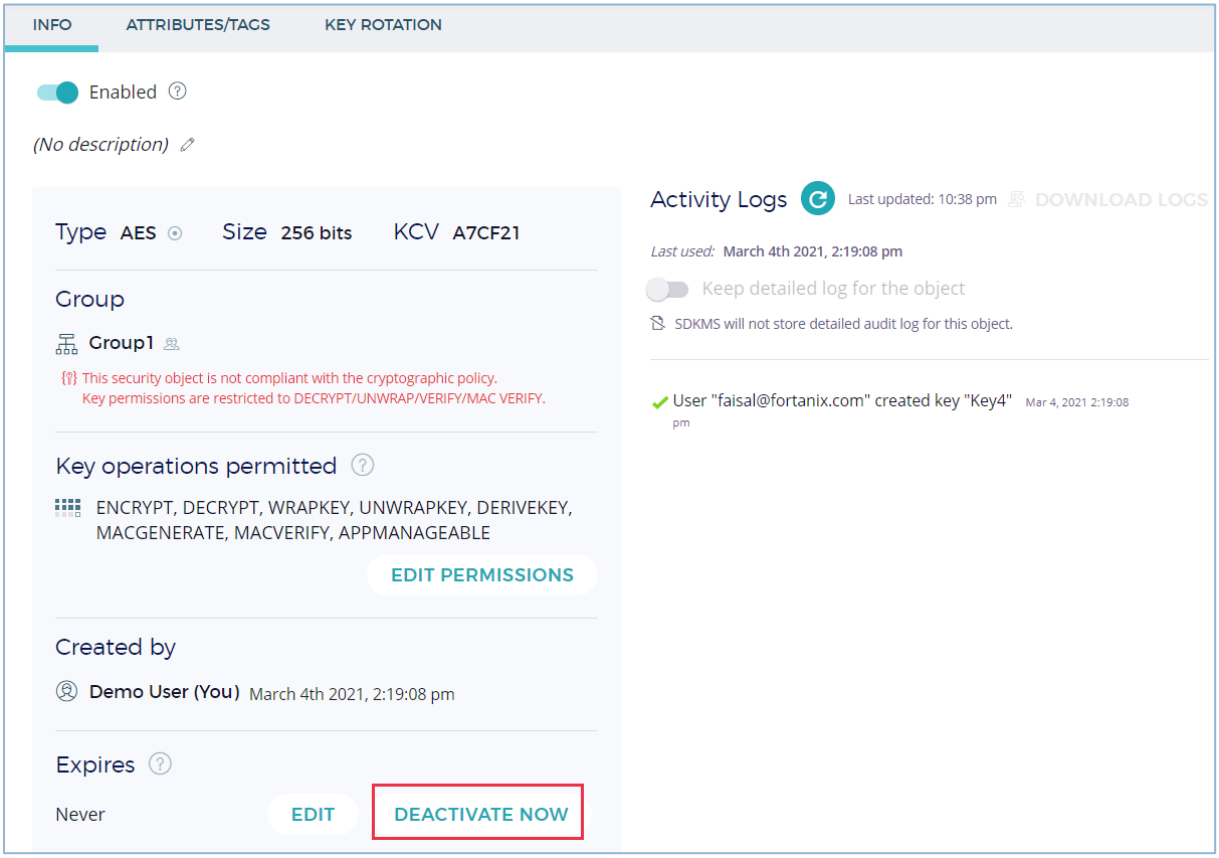

FIGURE 15: DEACTIVATE KEY

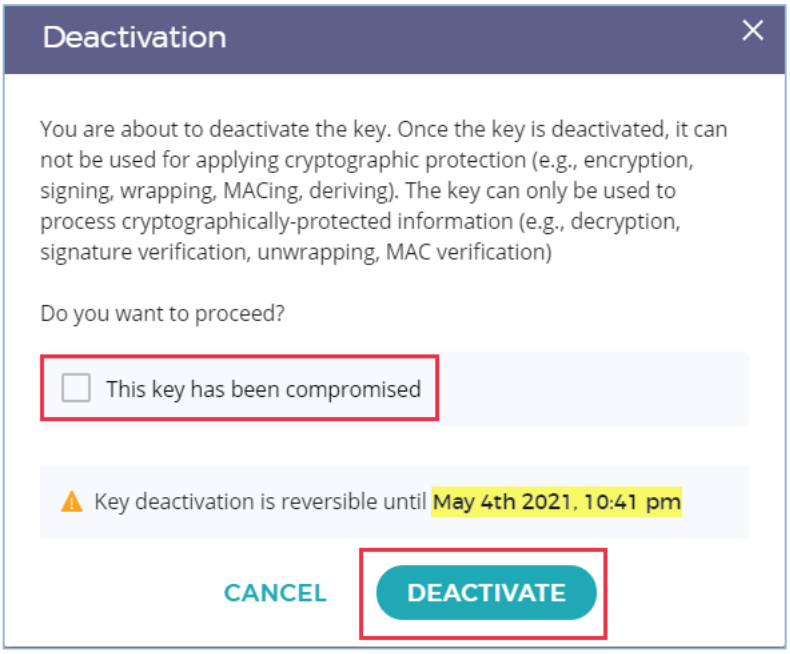

FIGURE 16: CONFIRM KEY DEACTIVATION/COMPROMISE

2. A deactivated key is represented in grey colour and a compromised key is represented in red colour .

   Notice on the top of the screen that you have an option to reverse the key deactivation/compromise operation using the **CANCEL CHANGE** button.

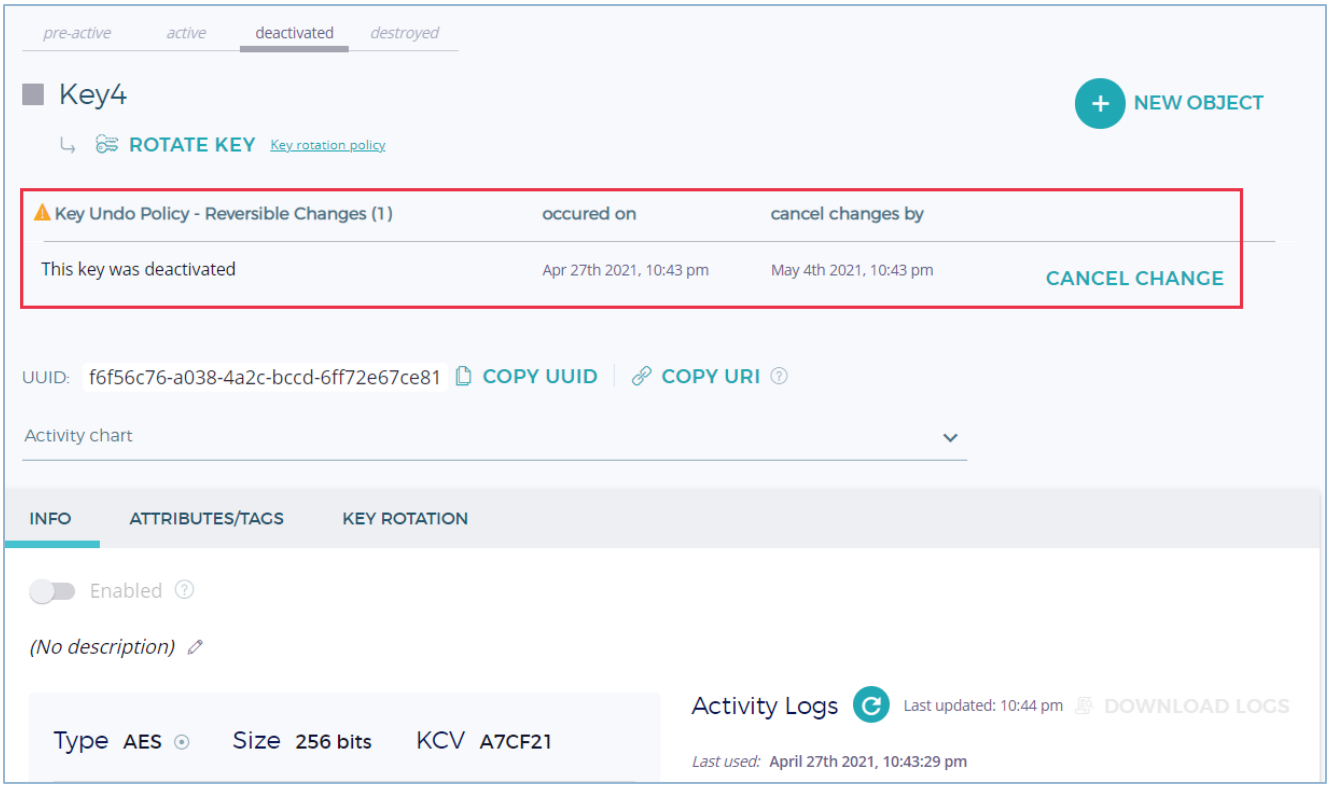

FIGURE 17: CANCEL KEY DEACTIVATION/COMPROMISE

3. Once the time elapses to revert the Key deactivation/compromise operation, the key will be permanently deactivated/compromised and cannot be used for applying cryptographic protection such as encrypt, signing, wrapping, MACing, and deriving. It can only be used to process cryptographically-protected information such as decrypt, signature verify, unwrap, and MAC verify. The key will also be permanently compromised if the "This key has been compromised" option was selected.

3.5 REMOVE KEY OPERATIONS WITH KEY UNDO POLICY

In the "Key undo policy" set at the group level, when you click the **EDIT PERMISSIONS** button from the detailed view of a key and remove some of the key operations, then the key operations removal becomes reversible until the time period set in the policy.

1. Remove the required permissions and click the **SAVE** button to confirm the key operations removal.

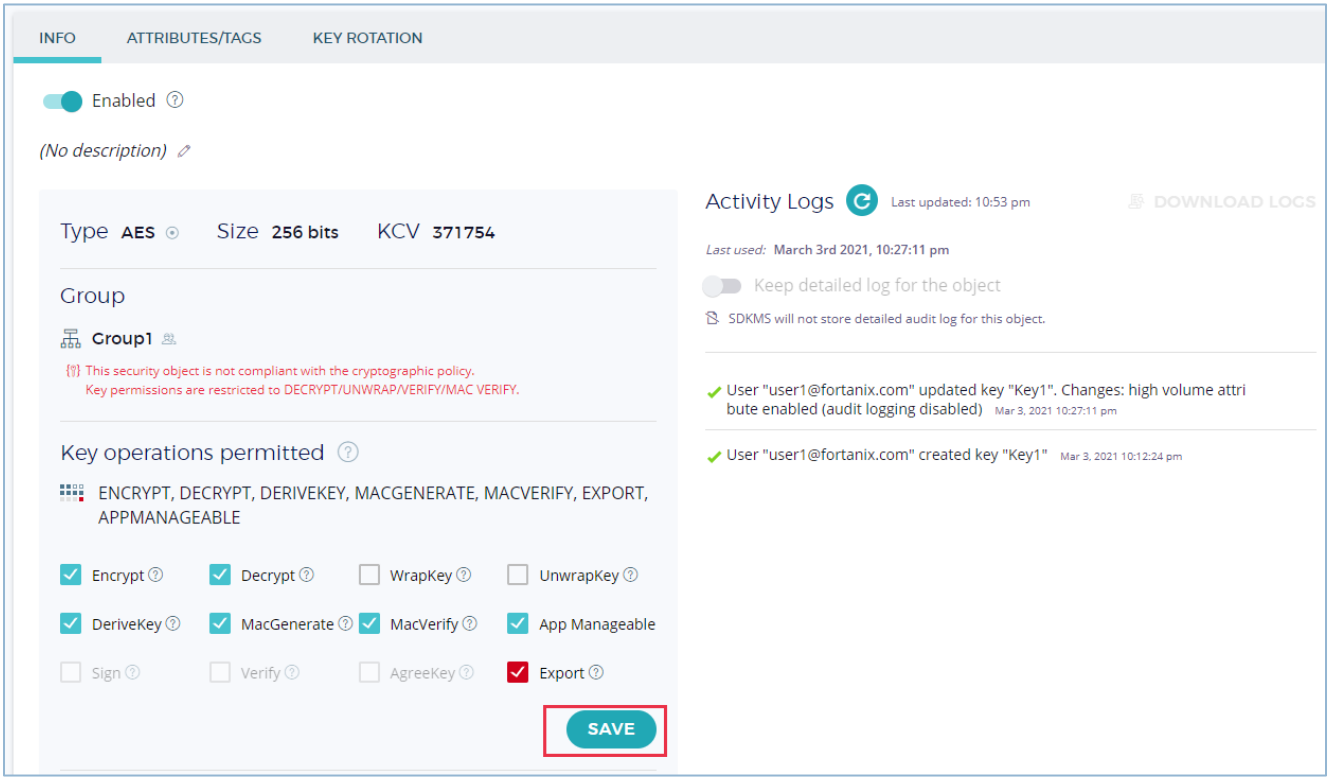

FIGURE 18: REMOVE KEY OPERATIONS

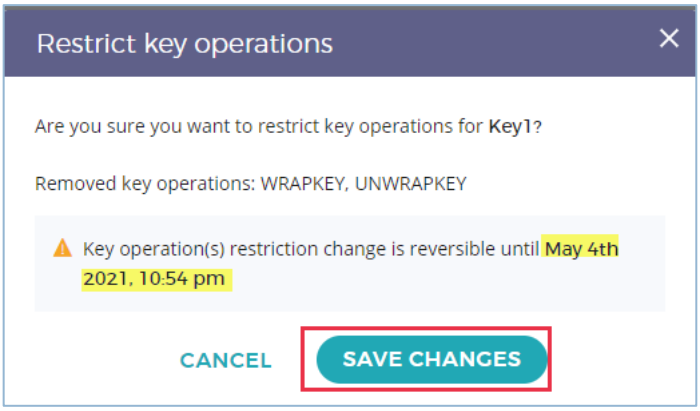

FIGURE 19: CONFIRM KEY OPERATIONS REMOVAL

2. Notice on the top of the screen that you have an option to reverse the key operations removal using the **CANCEL CHANGE** button.

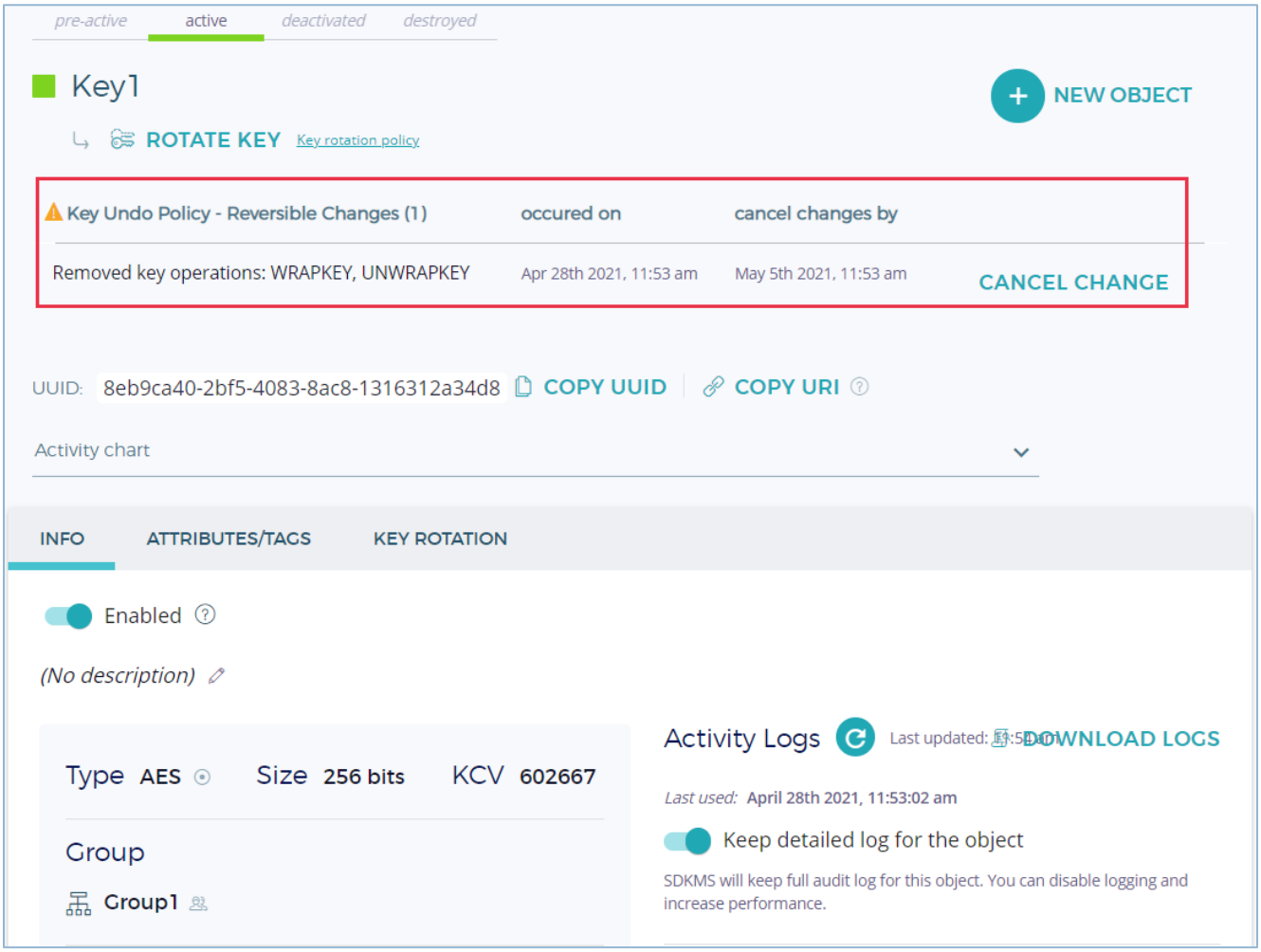

FIGURE 20: CANCEL KEY OPERATIONS REMOVAL

3. When the time elapses to revert the Key operation removal, the Key Operations will be permanently removed and cannot be reverted.

3.6 MULTIPLE KEY REVERSIBLE CHANGES WITH KEY UNDO POLICY

If there are multiple reversible changes made on a key that has a "Key undo policy" configured, then the following rule applies when you click **CANCEL CHANGES** to cancel the reversible changes for a key:

- All reversible change requests performed on and after the time period of the current "Cancel Change" selection will be canceled.

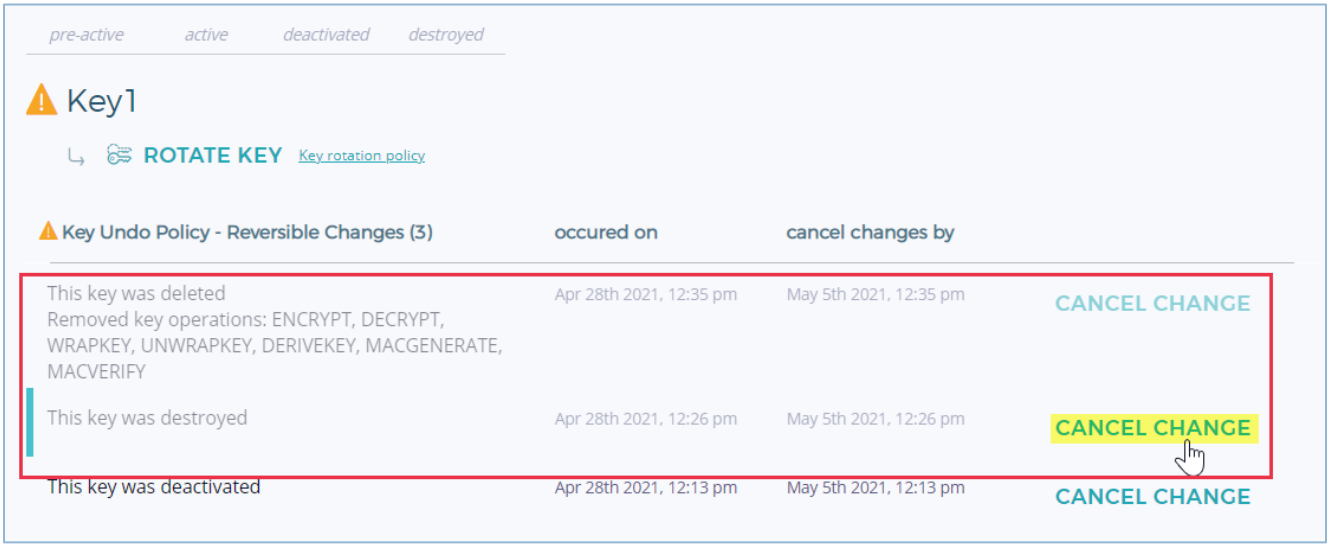

FIGURE 21: CANCEL REVERSIBLE CHANGES

In the example above: All reversible change requests on and after "April 28th 2021, 12:26 pm" will be cancelled.

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/4402562226580-User-s-Guide-Key-Undo-Policy

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