Fortanix®

User Guide

DATA SECURITY MANAGER – KEY METADATA POLICY

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) Key Metadata Policy User Guide. This document describes how a user can set key metadata policies for Fortanix DSM groups.

1.1 FORTANIX DATA SECURITY MANAGER KEY METADATA POLICY DEFINITION

Fortanix DSM supports key metadata policies that can be set on groups that allow users to configure certain restrictions on "metadata" associated with security objects. Here "metadata" refers to elements of security objects that are not covered by cryptographic policies, for example, custom metadata, description, expiry, and so on. The policy should be able to specify that certain metadata "must be present", "must not be present", or "must be present and have certain value".

2.0 FORTANIX DSM CONCEPTS

2.1 OVERVIEW AND DEFINITIONS

- **Fortanix Data Security Manager** -

  Fortanix Data Security Manager (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.

- **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.

  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 the 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.

- **Fortanix Data Security Manager Security Objects** –

  A security object is any datum stored in 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.

2.2 SUPPORT RESOURCES

For more information, visit *support*.

3.0 CREATE / EDIT A KEY METADATA POLICY

3.1 CREATE A GROUP LEVEL KEY METADATA POLICY

A group-level Key metadata policy allows you to configure certain restrictions on the "metadata" associated with security objects such as key description, activation and deactivation dates, custom attributes, and so on.

To add a key metadata policy at the group level:

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

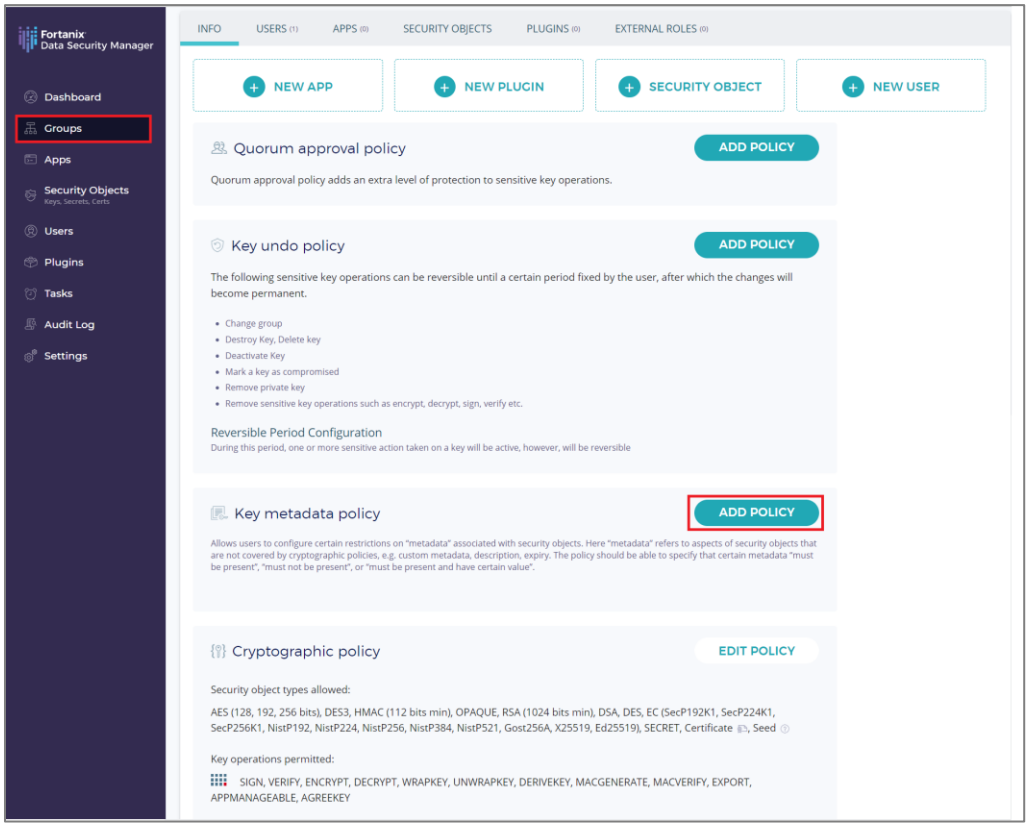

FIGURE 1: ADD KEY METADATA POLICY FOR GROUP

2. Select the following metadata that you want to allow for this group:
   a. **Key description:** Set the **Key description** rule as either optional or required by selecting the **Optional** or **Required** radio button.
   b. **Activation date:** Set the **Activation date** rule as either optional or required by selecting the **Optional** or **Required** radio button.
      - If you select the **Required** radio button, you can set the activation date to a time between 'x' (seconds/minutes/hours/days) and 'y' (seconds/minutes/hours/days) within the creation of the security object by selecting the optional check box **User must specify an activation date within '0' (seconds/minutes/hours/days) and '0' (seconds/minutes/hours/days) of security object's creation time**.

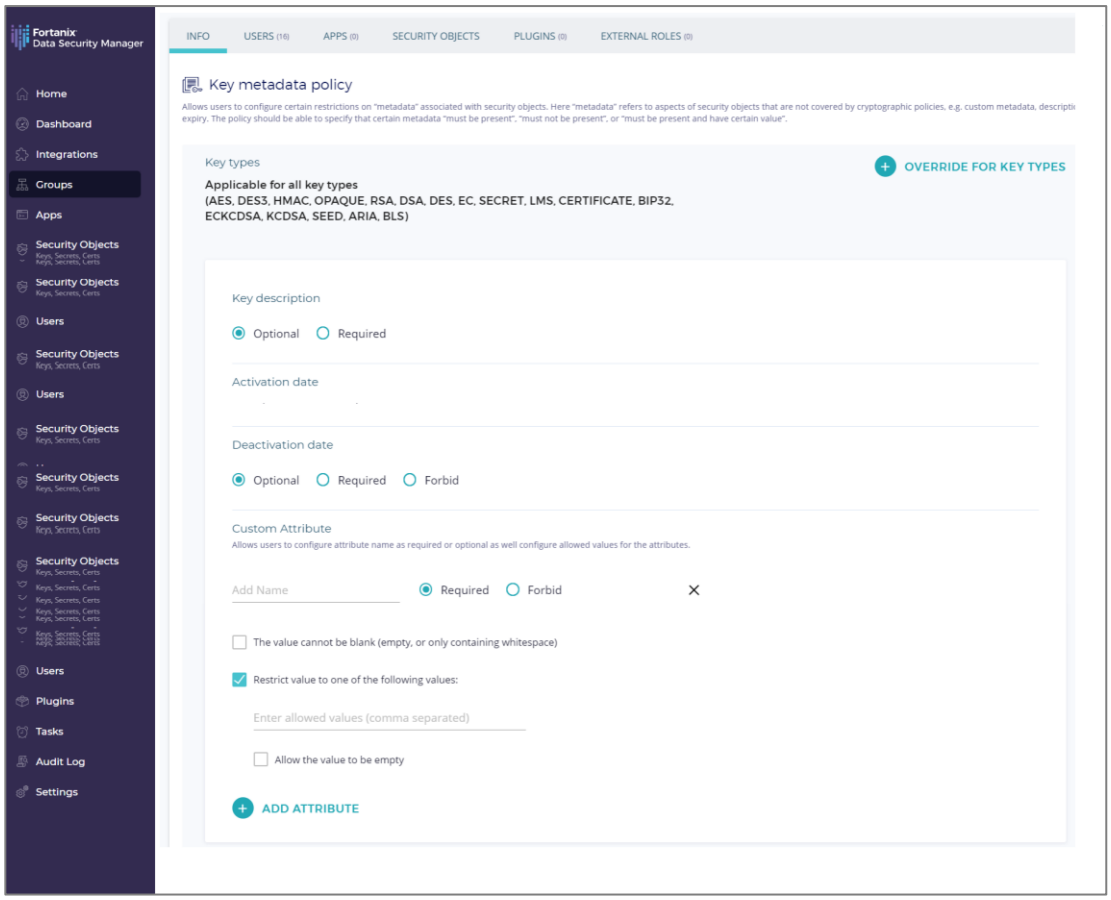

FIGURE 2: SETTING KEY METADATA POLICY

NOTE: "x" is the minimum time and "y" is the maximum time within which the security object will be activated. The value of "x" should always be less than 'y'.

For example, the user can specify an activation date between 20 minutes and 10 hours of a security object's creation time.

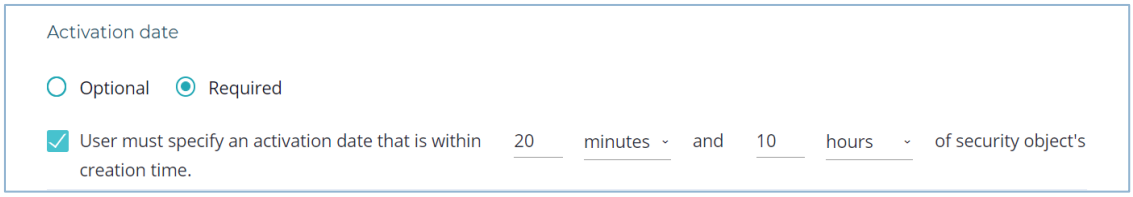

FIGURE 3: ACTIVATION DATE

c. **Deactivation date:** Set the **Deactivation date** rule to optional, required, or forbid by selecting the **Optional**, **Required,** or **Forbid** radio button.

- If you select the **Required** radio button, you can set the deactivation date to a time between 'x' (seconds/minutes/hours/days) and 'y' (seconds/minutes/hours/days) within the creation of the security object by selecting the optional check box **User must specify a deactivation date within '0' (seconds/minutes/hours/days) and '0' (seconds/minutes/hours/days) of security object's creation time.**

NOTE: "x" is the minimum time and "y" is the maximum time within which the security object will be deactivated. The value of "x" should always be less than "y'.

For example, the user can specify a deactivation date between 10 hours and 1 day of a security object's creation time.

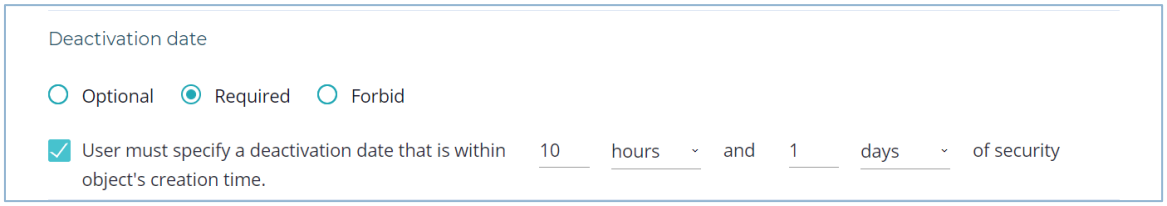

FIGURE 4: DEACTIVATION DATE

- If you select the **Forbid** radio button, you are forbidden from deactivating the key.

d. **Custom Attribute:** These are user-defined security object attributes that can be added to the security object's metadata. The attributes can be configured to be required or you can forbid the user from adding them.

i. Add the attribute name and configure it either as **Required** or **Forbid.** For example, consider the attribute name: Country.

- If you selected the **Required** radio button, you can optionally select the following options:
    - **The value cannot be blank (empty, or only containing whitespace):** If this option is selected, the user must enter attribute values that are not just whitespaces.
    - **Restrict value to one of the following values**: Selecting this option will restrict the allowed attributes values of the security objects to the ones specified in the textbox.

      Enter comma separated values. For example: India, Australia, China, US, and so on.
        - If you want to leave the value blank, then select the **Allow empty values** option. This will allow you enter an empty string as a custom attribute while creating a security object".

          NOTE: Selecting the "**The value cannot be blank**" option will override selection of "**Allow empty values**" option.

ii. Click **ADD ATTRIBUTE** to configure multiple custom attributes.

3. Click **SAVE POLICY** in the **KEY METADATA POLICY** window, to save the Key metadata policy.

3.2 OVERRIDING KEY METADATA POLICY FOR SELECTED KEY TYPES

By default, all types of keys are selected for Key metadata policy: AES, DES3, HMAC, OPAQUE, RSA, DSA, DES, EC, SECRET, CERTIFICATE, and SEED. To override default Key metadata policy for selected key types:

1. Click the **OVERRIDE FOR KEY TYPES** button.

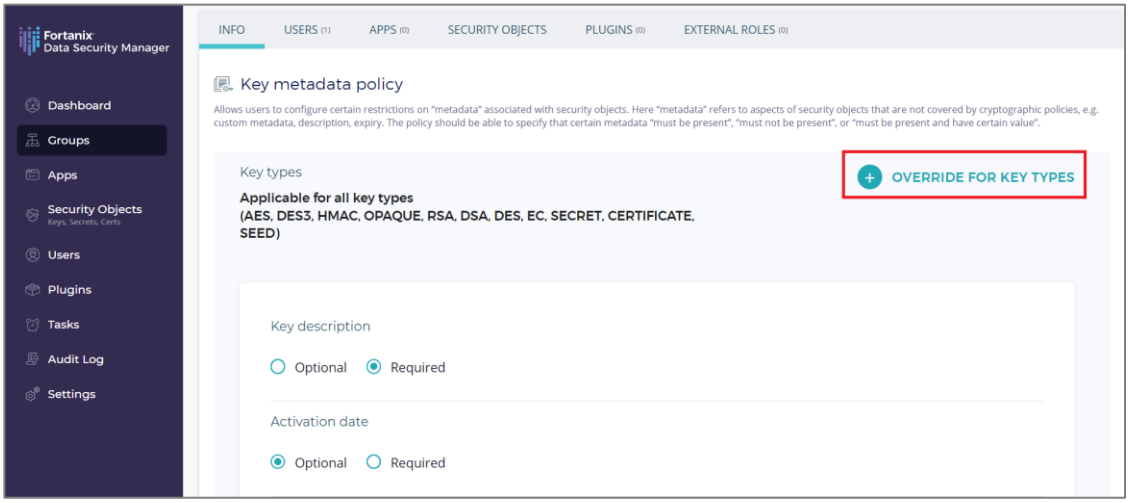

FIGURE 5: OVERRIDE FOR KEY TYPES

2. Select the key types from the drop down menu that should be overridden by the default Key metadata policy.

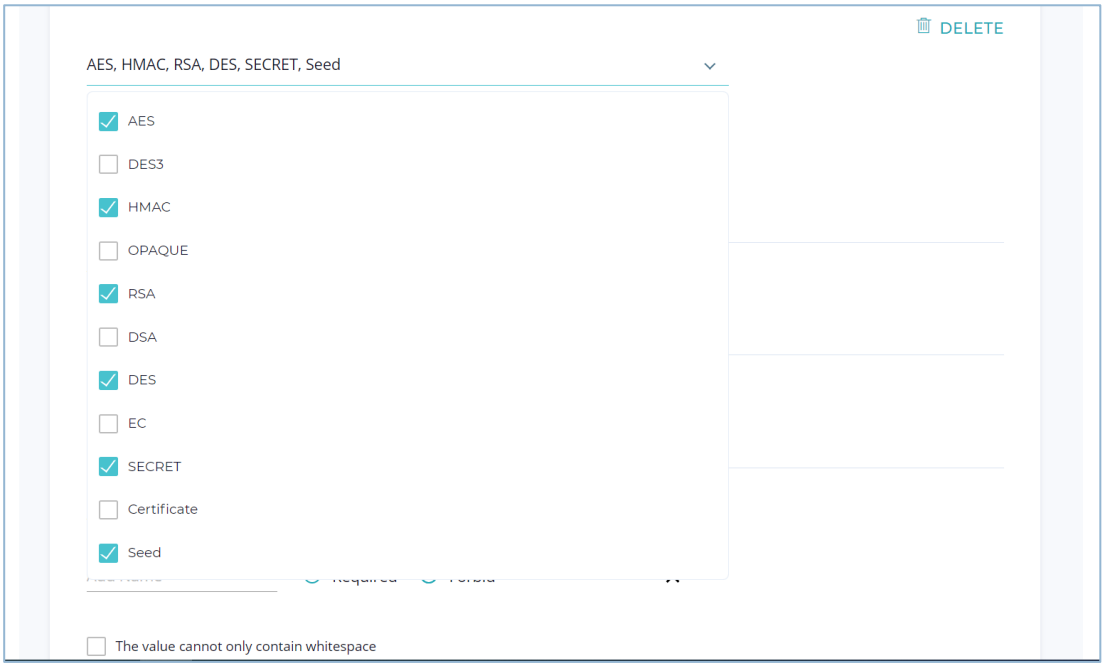

FIGURE 6: SELECT KEY TYPES

3. To configure the metadata of security objects such as key description, activation date, deactivation date, and custom attribute applicable to the selected key types, *refer to Section 3.1*.

3.3 HANDLING EXISTING NON-COMPLIANT KEYS

- All new keys will be allowed/denied based on the Key metadata policy rules.
- Any existing keys that are not compliant with the policy will still exist in the group. However, these keys will be marked separately as policy-violating keys. For more information on the conditions applicable to policy-violating keys refer to *policy enforcement* .

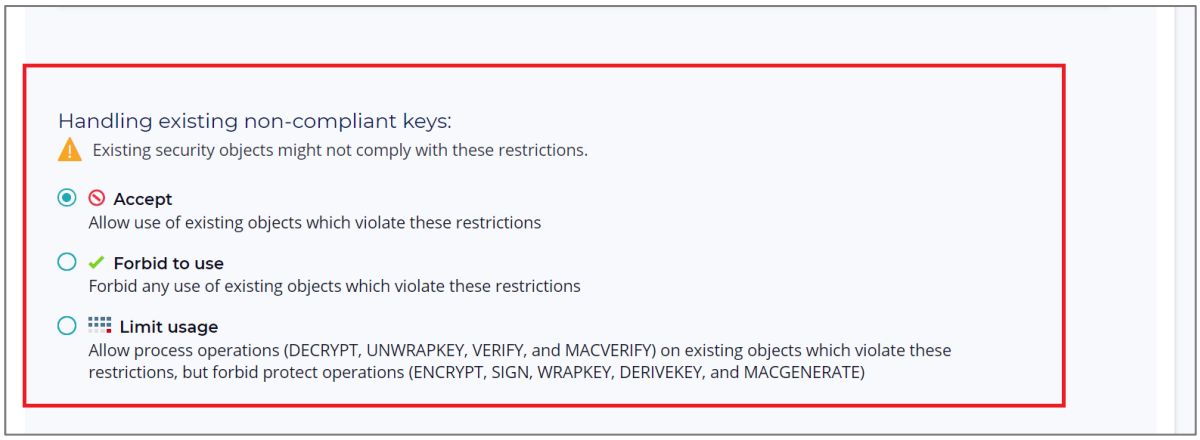

FIGURE 7: HANDLING EXISTING NON-COMPLIANT KEYS

When a key metadata policy is created at a group level, there are 3 options provided to handle non-compliant keys. These options are detailed in the following section:

a. **Accept**: Accept non-compliant objects even though they violate the current policy. If this option is selected, you may continue to use existing non-compliant keys, but you may not generate or import new non-compliant objects.

b. **Forbid to use:** Forbid any use of non-compliant objects. If this option is selected, you are forbidden from using the non-compliant keys for any operation.

c. **Limit usage:** Restrict non-compliant objects so that they may only be used for "process operations" (DECRYPT, UNWRAPKEY, VERIFY, and MACVERIFY) on existing objects which violate these restrictions, but forbid "protect operations" (ENCRYPT, SIGN, WRAPKEY, DERIVEKEY, and MACGENERATE).

4.0 DELETE A GROUP LEVEL KEY METADATA POLICY

To edit or delete a group level key metadata policy:

1. Go to the detailed view of a group.
2. In the **INFO** tab, under the **Key metadata policy** section, click the **EDIT POLICY** button.

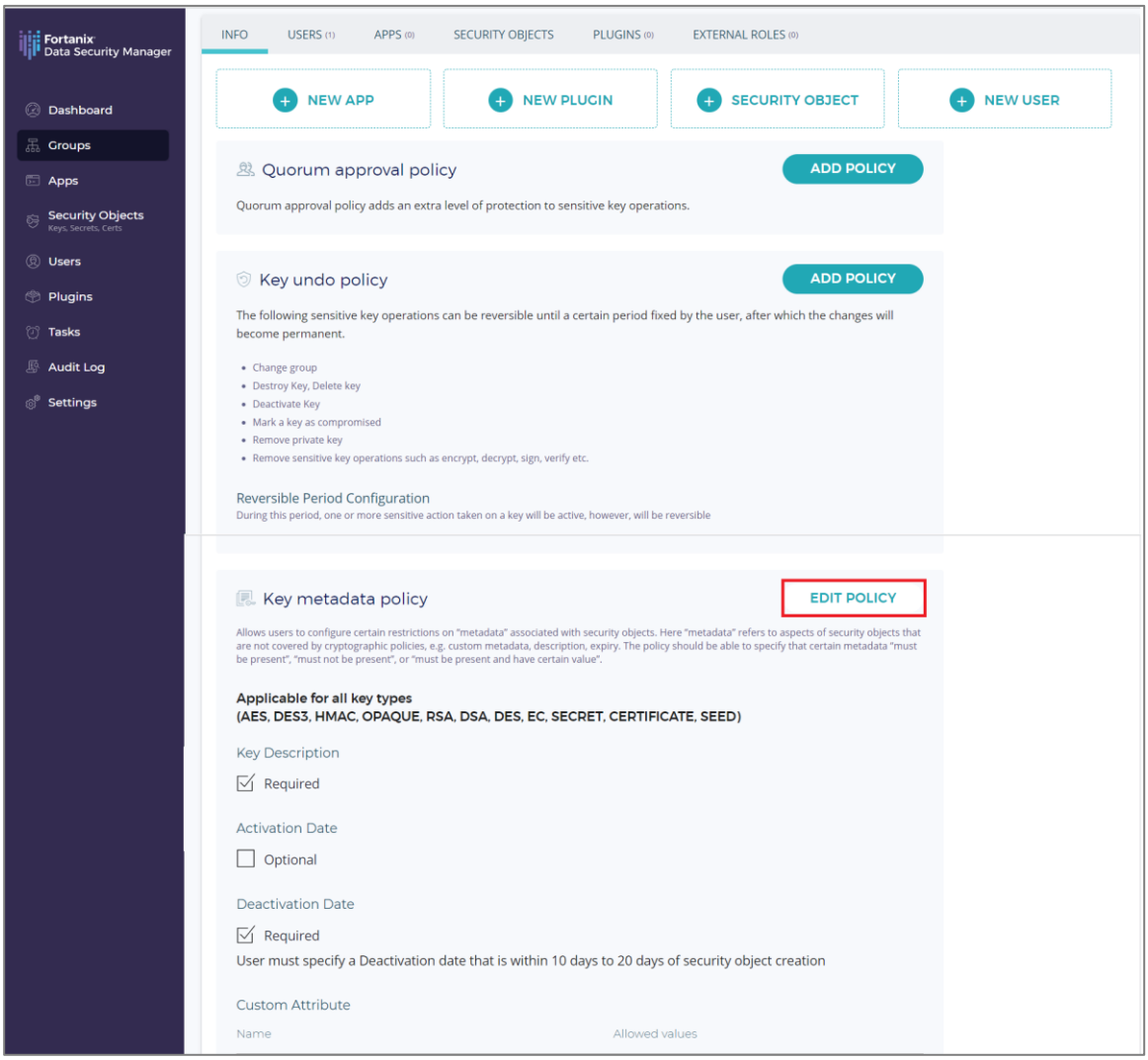

FIGURE 8: EDIT GROUP KEY METADATA POLICY

3. Click the **DELETE POLICY** button, to delete the Key metadata policy.

5.0 DOCUMENT INFORMATION

5.1 DOCUMENT LOCATION

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

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