Fortanix®

User Guide

FORTANIX DATA SECURITY MANAGER – CREATE TOKENIZATION SECRET

Fortanix Inc. | 800 West El Camino Real | Suite 180 | Mountain View, CA 94040 | 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 steps to create a tokenization secret in Fortanix DSM.

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 STEPS TO CREATE A TOKENIZATION SECRET

1. Click the Fortanix DSM **Groups** tab, and create a new group called **`Tokenization`** (if the group does not exist).

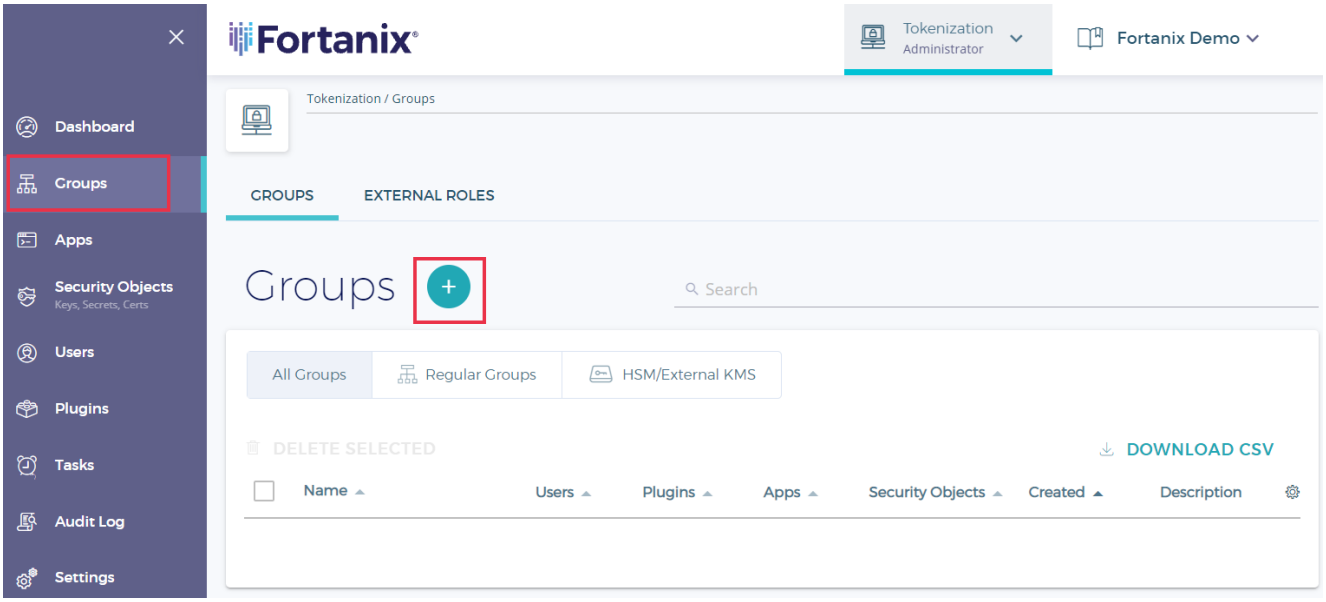

FIGURE 1: CREATE NEW GROUP FOR TOKENIZATION APP

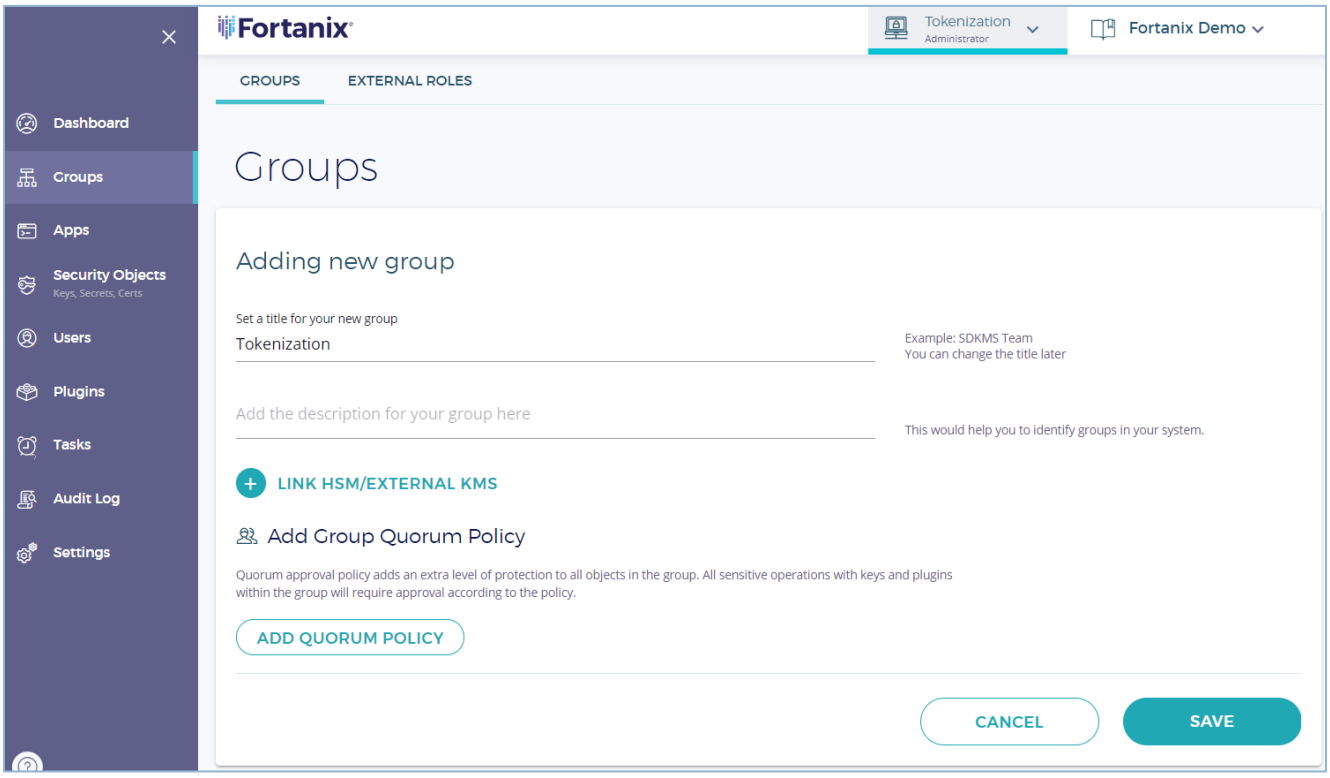

FIGURE 2: CREATE A GROUP

2. Once the group is created, configure any of the policies for the group that are required by your organization, such as the Quorum approval policy, Key undo policy (for sensitive key operations), Cryptographic policy, and Key custodian policy.

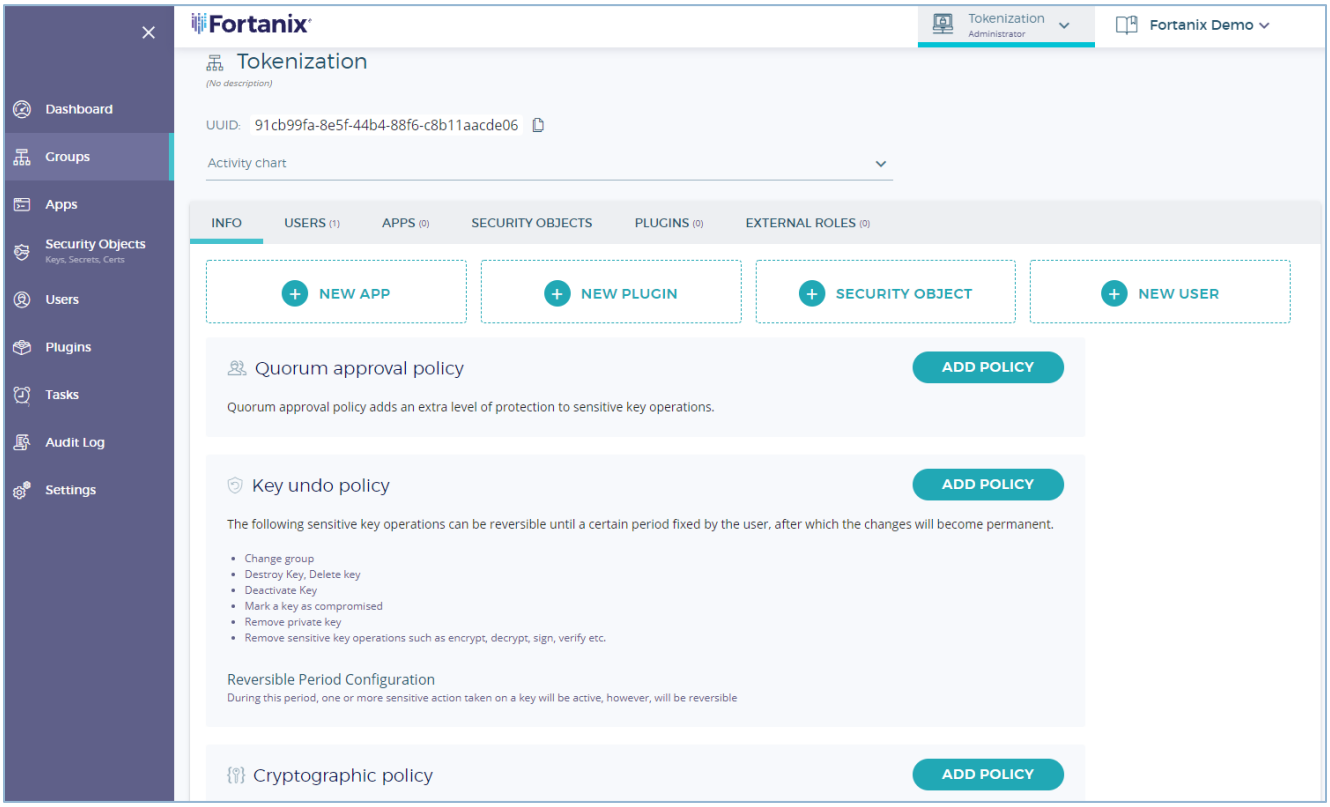

FIGURE 3: CONFIGURE DSM POLICY

3. Add a new "Tokenization App" to the Group.
    a. Give it a name and select the API Interface (in the following example, the Rest API is used).
    b. Select the Authentication Mechanism to be used by the application (in the example below the API Key is used).

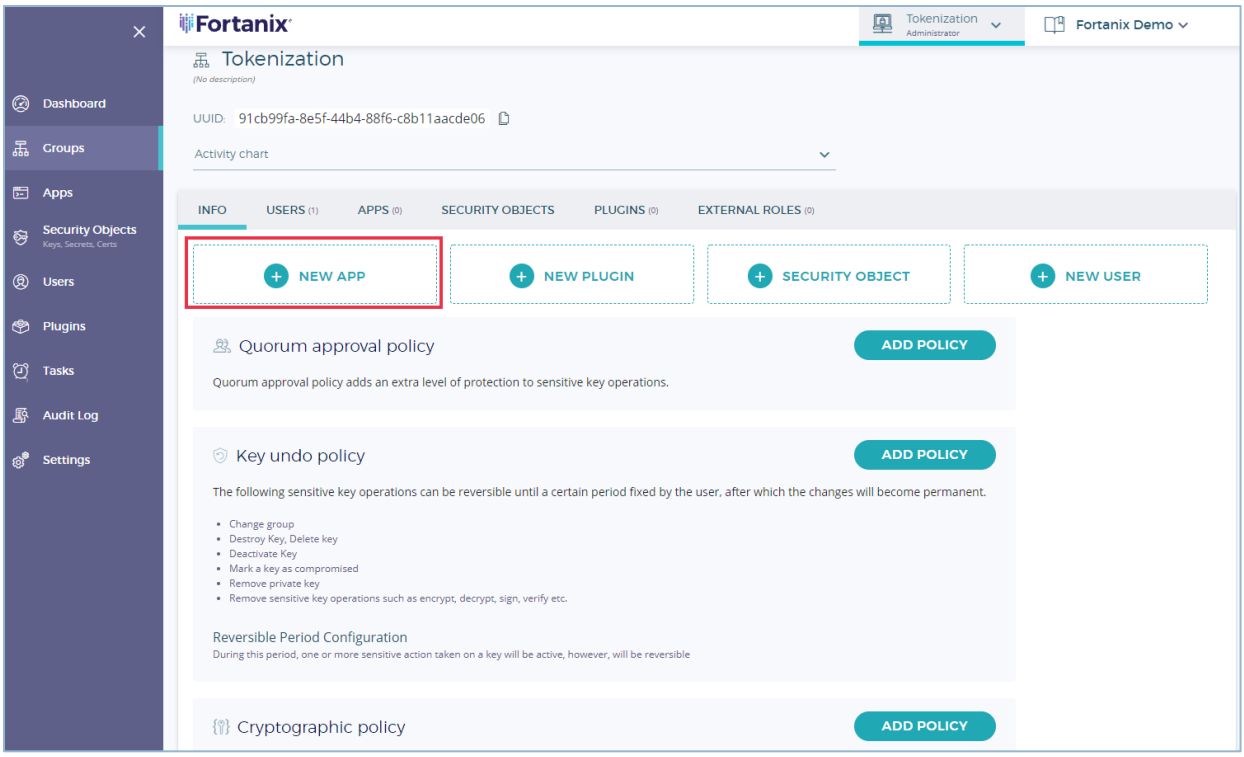

FIGURE 4: CREATE A TOKENIZATION APP

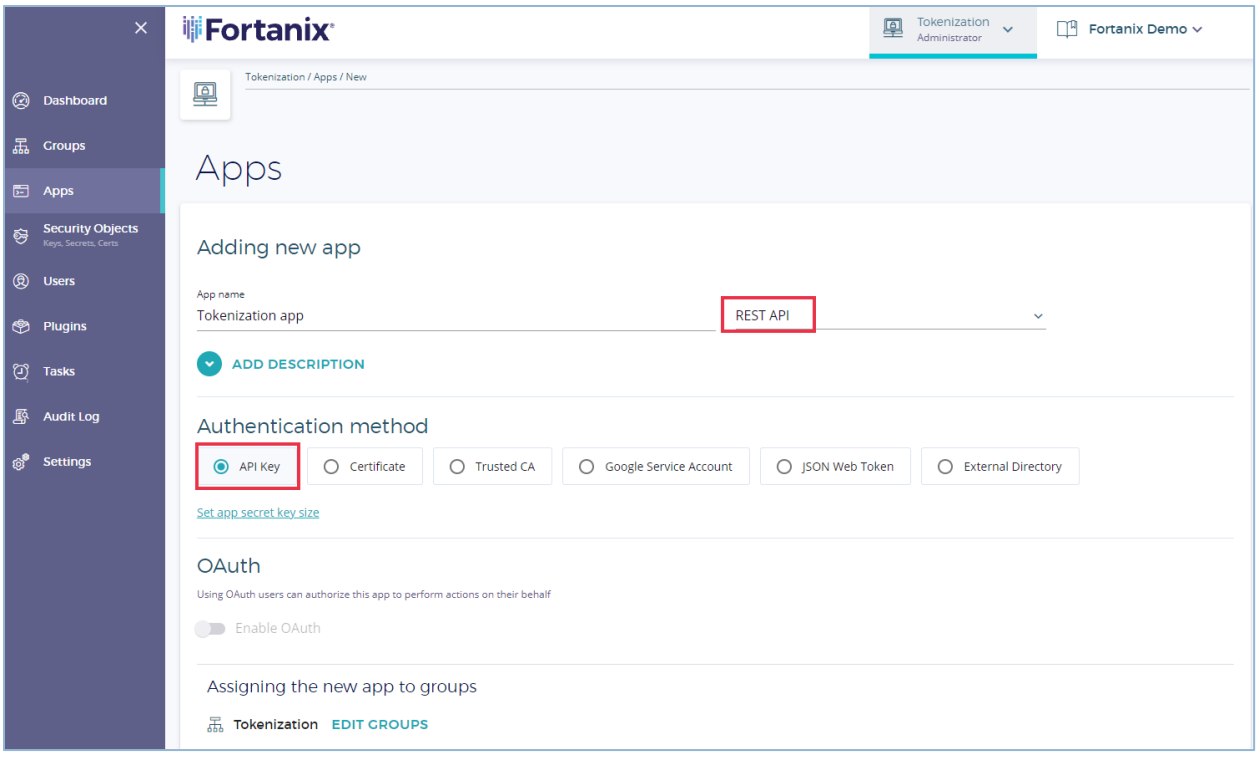

FIGURE 5: SELECT API INTERFACE AND AUTHENTICATION MECHANISM

4. Create a Tokenization Secret in the same group created in *Step 1*.

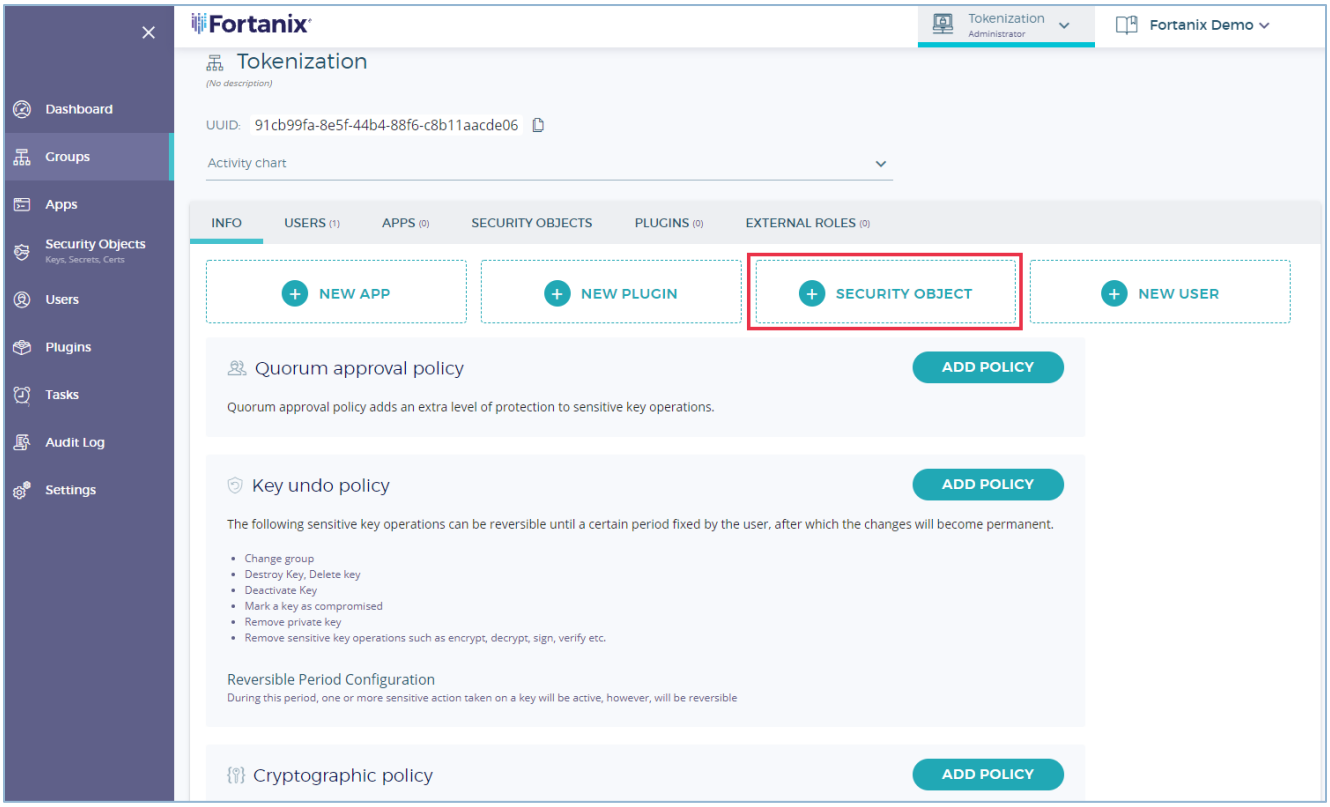

FIGURE 6: CREATE TOKENIZATION SECRET IN THE SAME GROUP

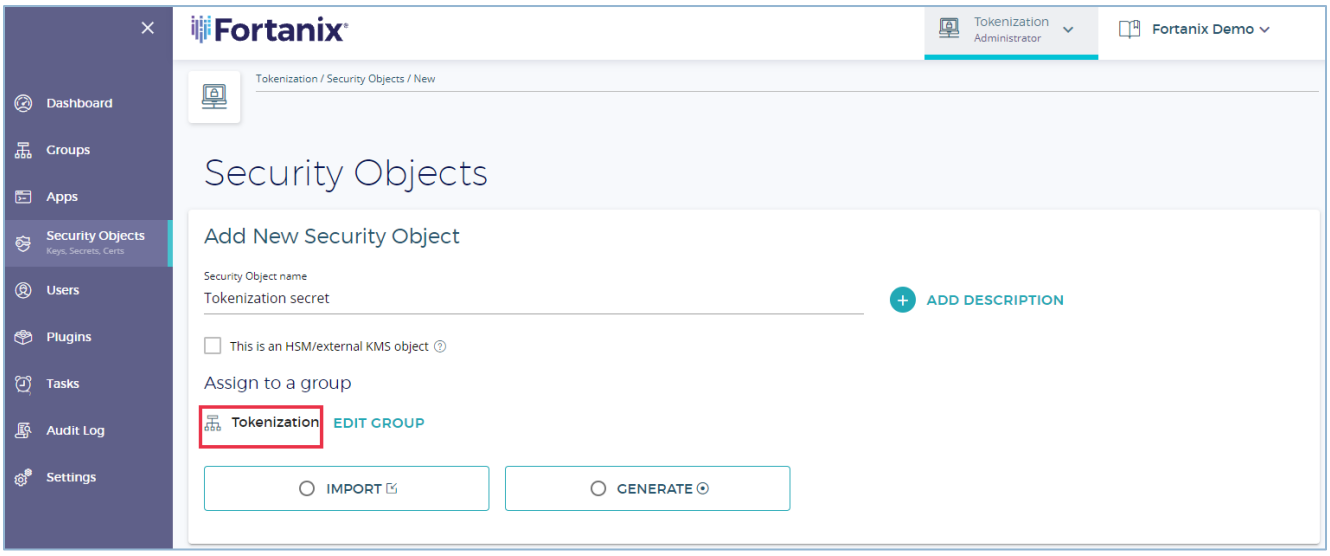

FIGURE 7: CREATE A TOKENIZATION SECRET

In the Add New Security Object form

a. Select **GENERATE** to generate a tokenization secret.

b. In the **Choose a type** section, select the key type as "**Tokenization**".

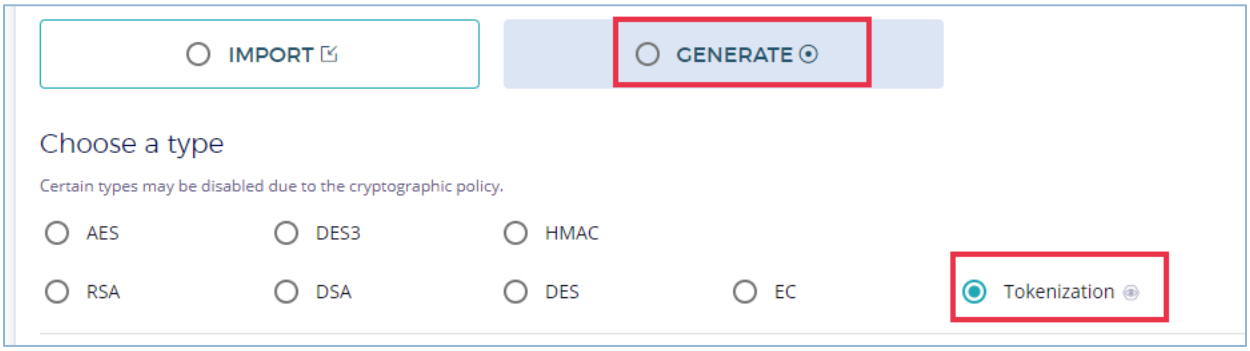

FIGURE 8: GENERATE A TOKENIZATION OBJECT

c. Select the **Data type** to be tokenized.

- **Email Address**

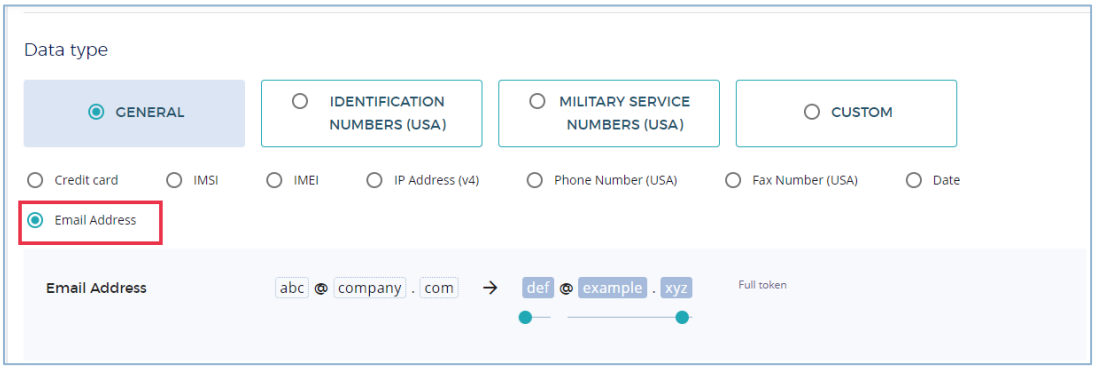

FIGURE 9: TOKENIZE EMAIL ADDRESS

- **Numbers**

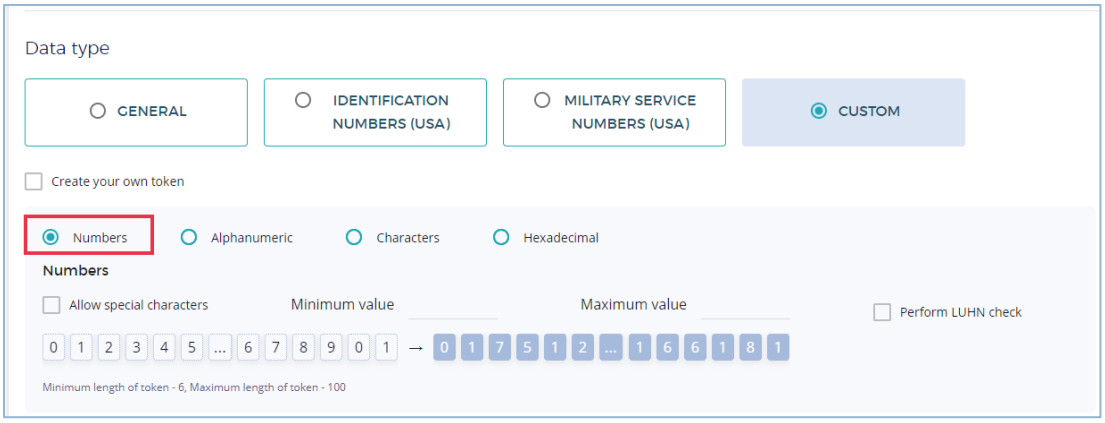

FIGURE 10: TOKENIZE CUSTOM NUMBERS

- **Alphanumeric**

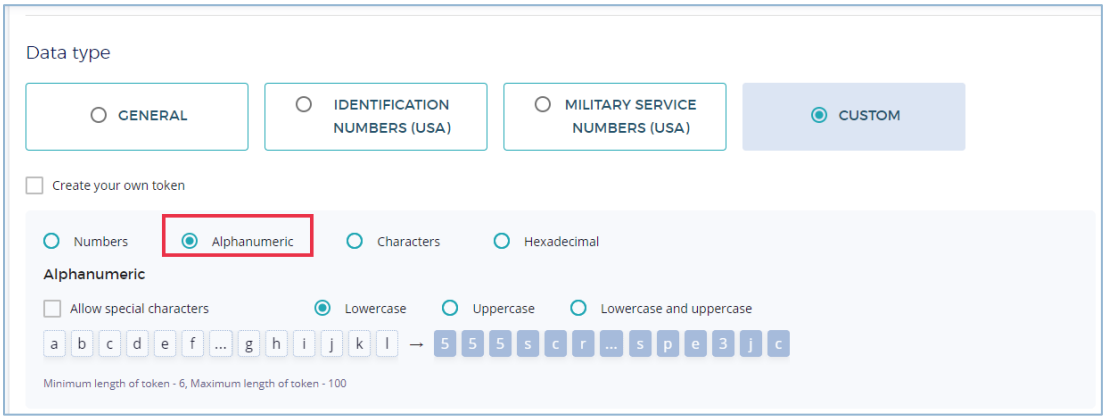

FIGURE 11: TOKENIZE ALPHANUMERIC CHARACTERS

d. Enter the key size and select the key operations.

e. Click **GENERATE** to generate the key.

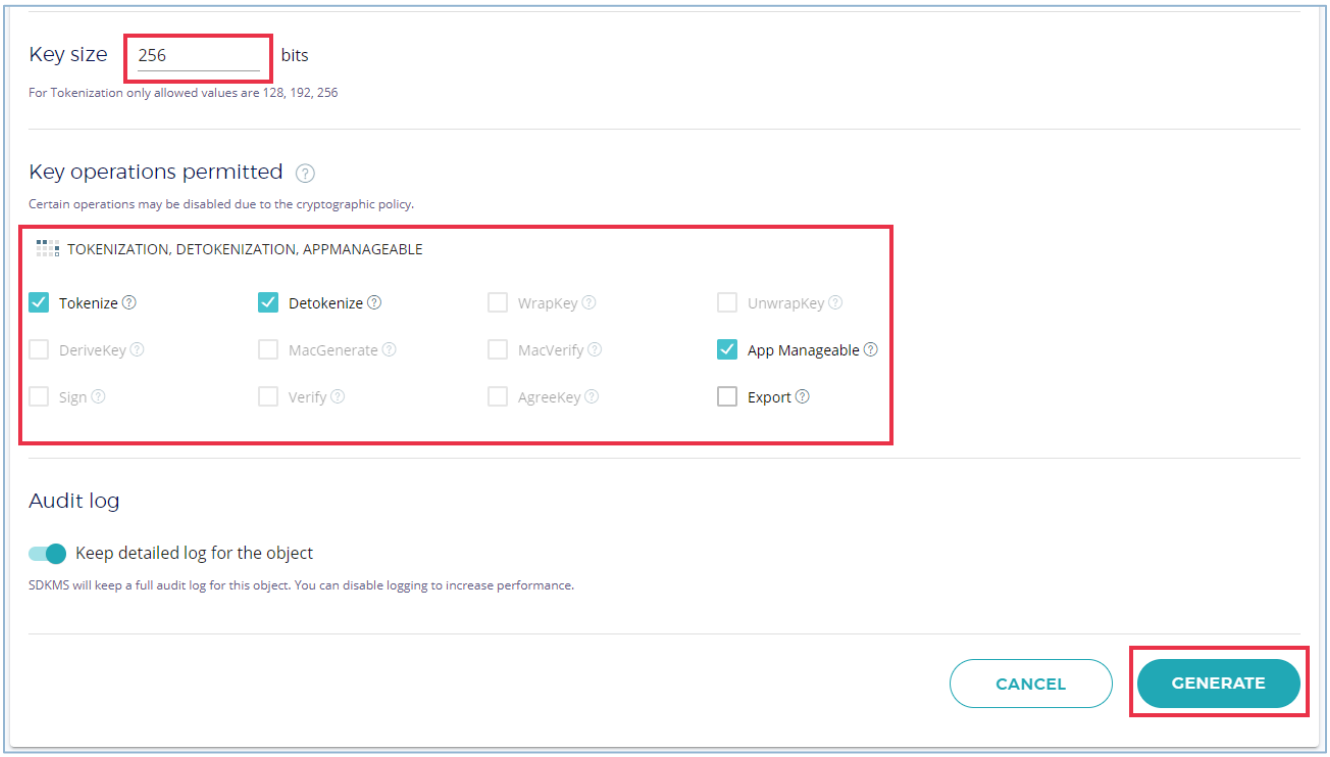

FIGURE 12: KEY SIZE AND KEY OPERATIONS

f. You now have the Unique Identifier (UUID) of the Secret to be used by the Application to reference the Tokenization Secret and perform the tokenization operations.

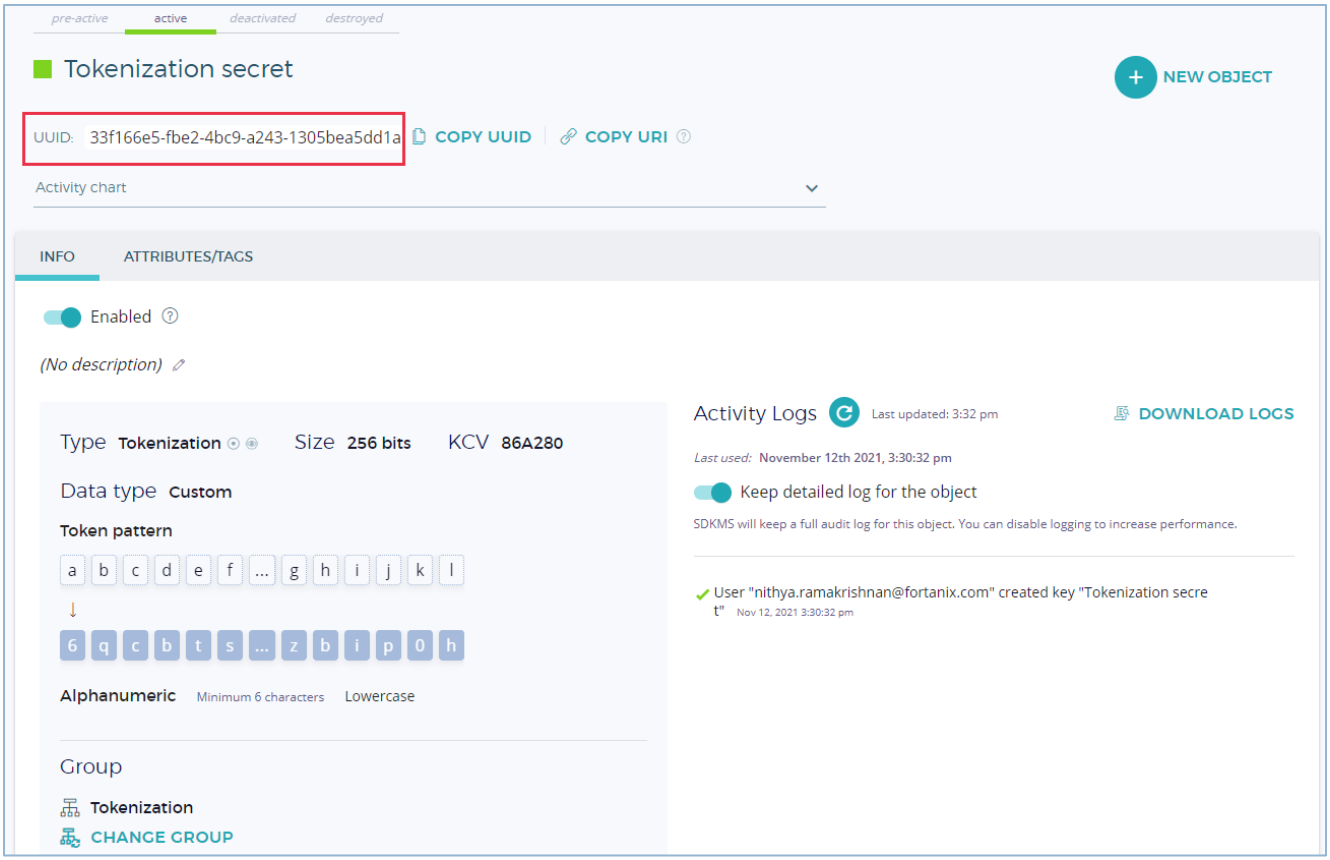

FIGURE 13: KEY UUID TO PERFORM TOKENIZATION OPERATIONS

4.0 REFERENCES

Finally, to utilize the tokenization secrets using the RestAPI, please refer to the following webpage:

Tokenization as an API: A Walkthrough with Fortanix DSM SaaS.

5.0 DOCUMENT INFORMATION

5.1 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