Fortanix®

User Guide

FORTANIX DATA SECURITY MANAGER – USAGE METRICS

VERSION 1.0

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

This document goes through the structure of a Fortanix Data Security Manager (DSM) dashboard. Fortanix DSM collects metrics that track the usage of resources associated with an account. Real-time and historical data of these metrics can be viewed in the Fortanix DSM account dashboard. Usage metrics in Fortanix DSM allow you to proactively manage usage by visualizing metrics in the Fortanix DSM Dashboard, detecting changes in activity, and configuring notifications that alert you when usage approaches a threshold.

2.0 FORTANIX DSM CONCEPTS

2.1 OVERVIEW AND 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.

- **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
  - Create and invoke plugin

⚠ **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. A group administrator 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 Fortanix DSM (for example a key, a certificate, a password, API keys, tokens, or any blob of data). 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 ACCOUNT ADMINISTRATOR DASHBOARD VIEW

The following metrics are represented on the Account Administrator dashboard.

- Overview of the key metrics that indicate the actual activity of the account under the **current calendar month**. This section displays the data related to the following metrics:
  - **Total Active Apps:** It is the total number of cloud accounts configured in Fortanix DSM plus the total number of Fortanix DSM Generic Apps in the account.
    - Total Number of Cloud Accounts (configured in Fortanix DSM) :
      - Total AWS Accounts
      - Total Azure Accounts
    - Total Number of Fortanix DSM Generic Apps: Generic apps are applications that use both Secrets Management (Encrypt, Decrypt, WrapKey, UnwrapKey, Sign, Verify, MacGenerate, and others) and Tokenization (Tokenize and detokenize operations, that is, Encrypt or Decrypt in format-preserving encryption (FPE) mode.)
  - **Total Operations**

    Operations Metered on Cryptographic Key:
    - Key Generation, Import, Export
    - Digest Key, Re-key, Derive Key, Agree Key
    - Persist Transient Key
    - Encrypt, Decrypt
    - Wrap, Unwrap
    - Multi-part Encrypt (Init, Update, Final)
    - Multi-part Decrypt (Init, Update, Final)
    - Signature Generation, Signature Verification
    - Mac Generation, Mac Verification

    Operations Metered on Secrets:
    - Import a Secret Object
    - Rotate a Secret Object with a new Secret Object
    - Export a Secret Object

Operations Metered on Opaque Objects:

- Import an Opaque Object

- Number of **Tokenization Operations**: The key operations that are permitted for a tokenization key are Tokenize (encrypt), Detokenize (decrypt), App Manageable, and Export.
- Number of **Tokenization Apps:** Tokenization Apps are applications that are assigned to perform tokenization operations in a specific calendar month.
- Total Security Objects
- Total Plugins
- HSM Gateways (if enabled)

NOTE: Total Operations count will include the tokenization Operations count as well. For example, if the user has performed 10000 tokenization operations. The tokenization operation will display the count as 10000 and the Total operations will display the count 10000/10000. The individual operations count will remain 0.

- Historical Usage data of the following key metrics that summarise activities for the past **six months**.
  - Total Operations
  - Total Tokenization Operations
  - Total Plugin Invocations

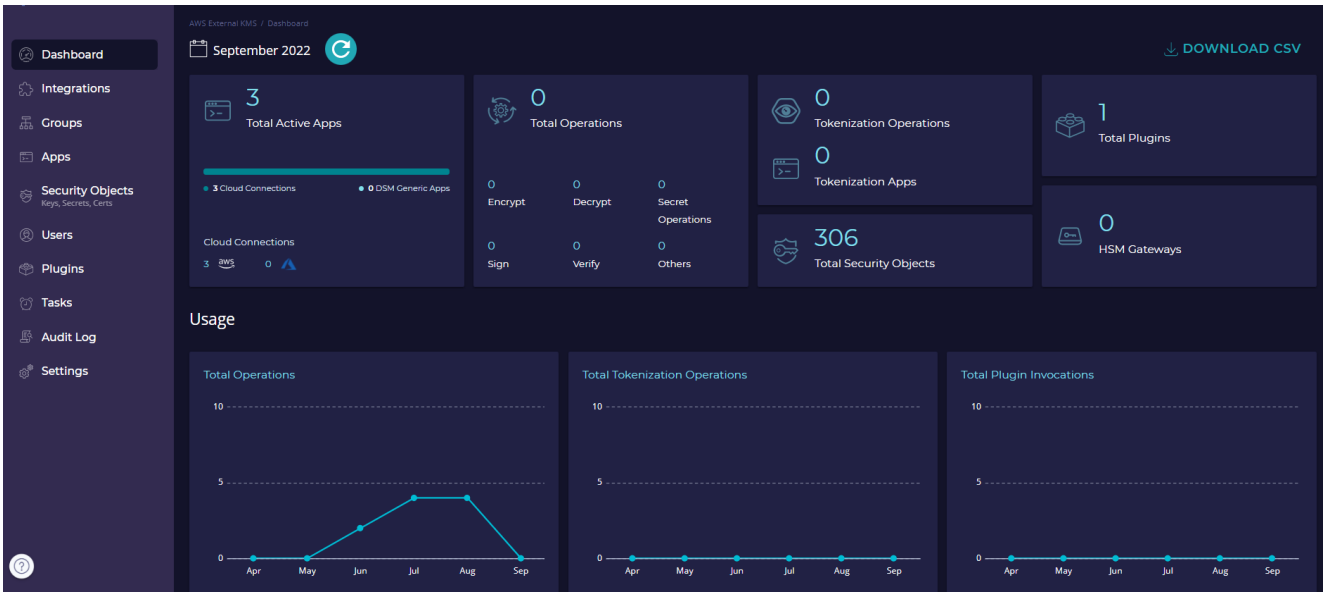

FIGURE 1: ACCOUNT ADMINISTRATOR DASHBOARD VIEW

1. The above data can be exported to a CSV file for the last 'x' number of months (up to **12 months**) that can be used for billing. To download the CSV file, click **DOWNLOAD CSV.**

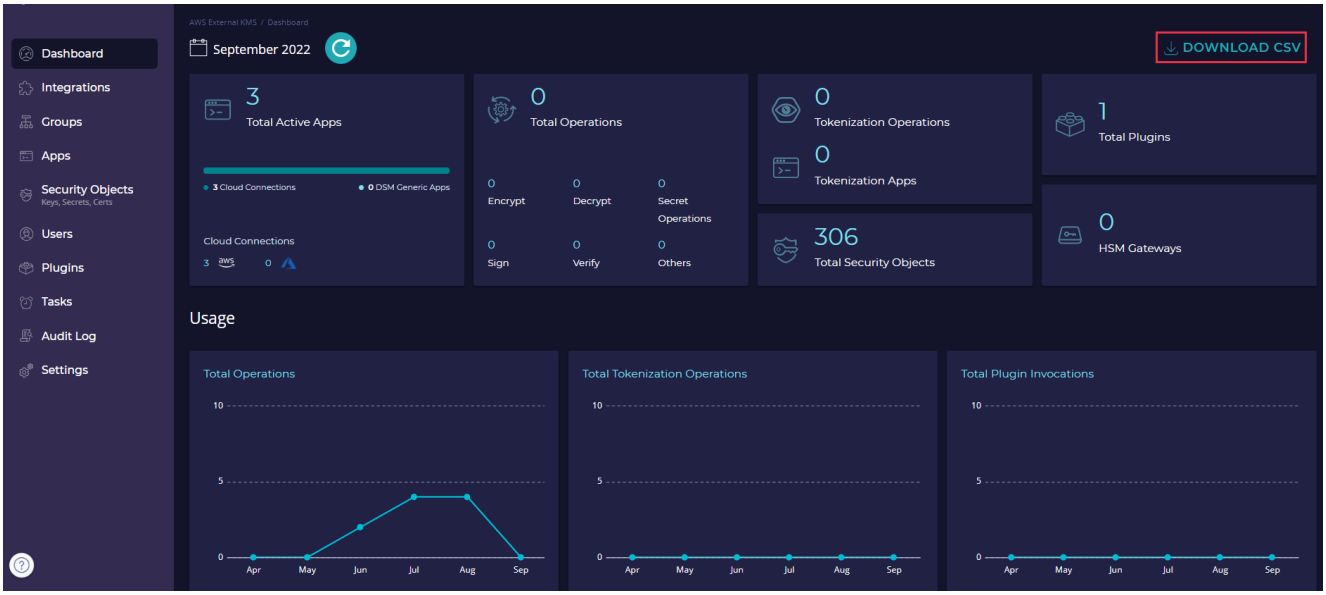

FIGURE 2: DOWNLOAD CSV FILE

2. Select the number of months up to which the data should be exported and click **DOWNLOAD**.

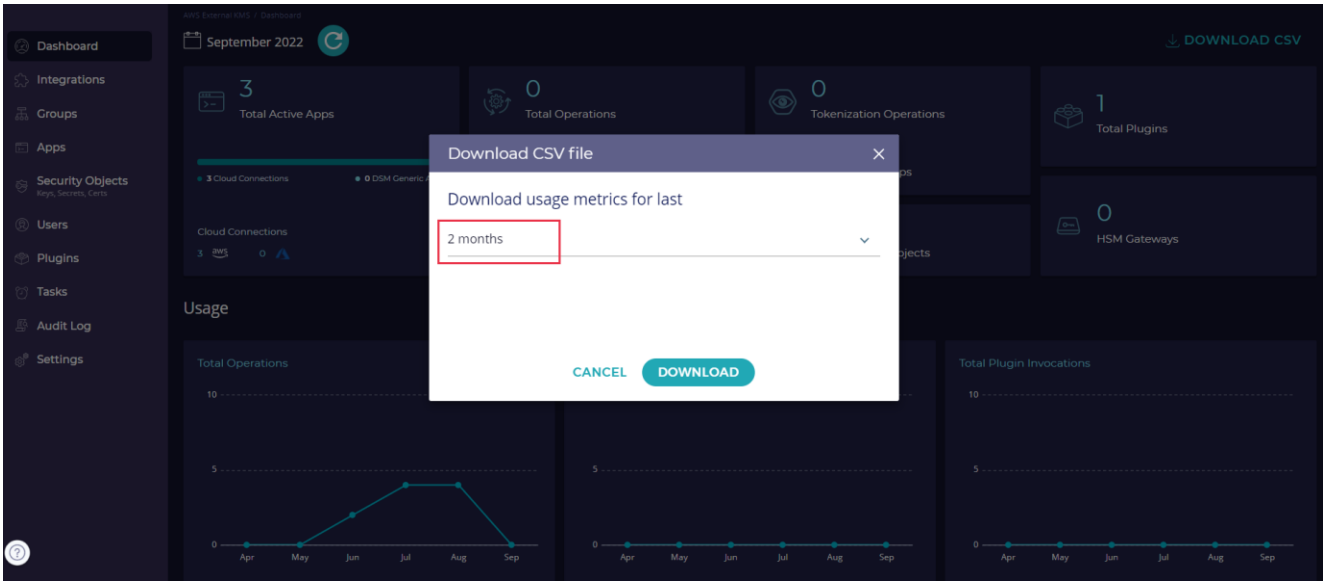

FIGURE 3: SELECT NUMBER OF MONTHS

3.1 NOTIFICATION

In the event of exceeding limits on any billable key metrics such as Total Operations, Total Apps (including cloud accounts), Total Plugins, Total HSM Gateways, the Account Administrator will receive a notification on the dashboard.

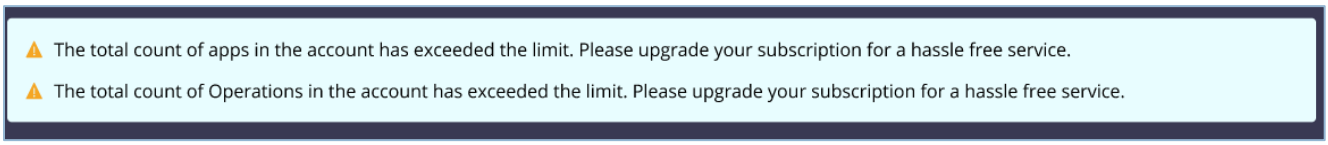

FIGURE 4: NOTIFICATIONS

4.0 SYSTEM ADMINISTRATOR DASHBOARD VIEW

Fortanix Data Security Manager System Administrator can view the metrics and activities associated with all accounts. To view the usage of key metrics of any individual account:

1. Go to the **Accounts** Page.
2. Select the account from the list of accounts to view the key metrics associated with it.

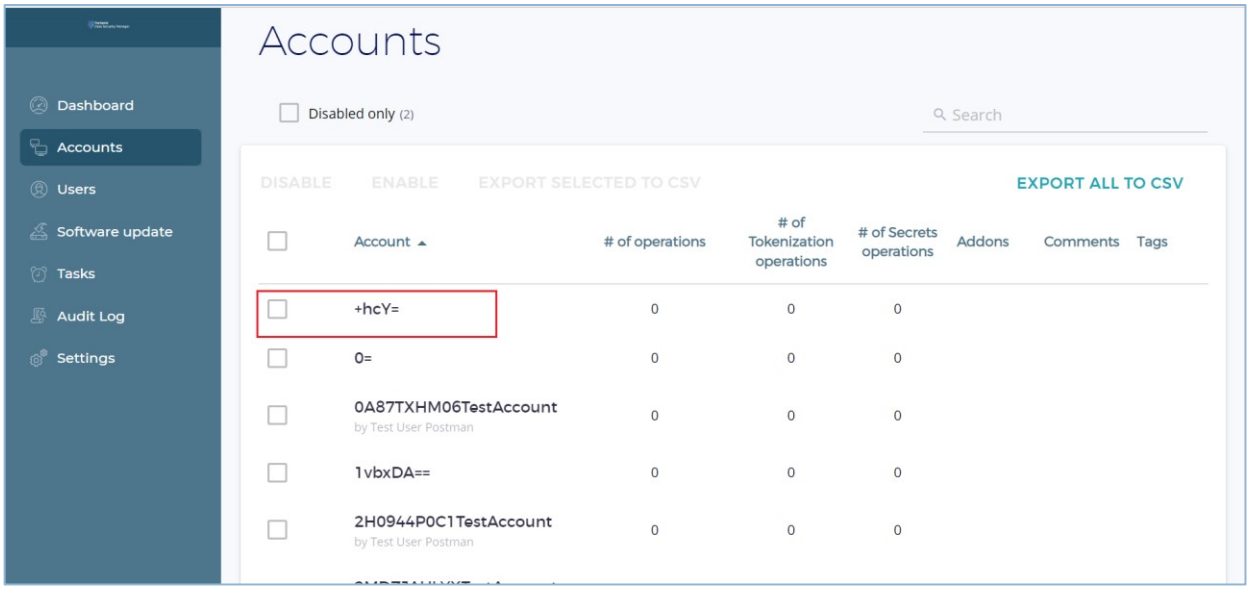

FIGURE 5: SELECT ACCOUNT

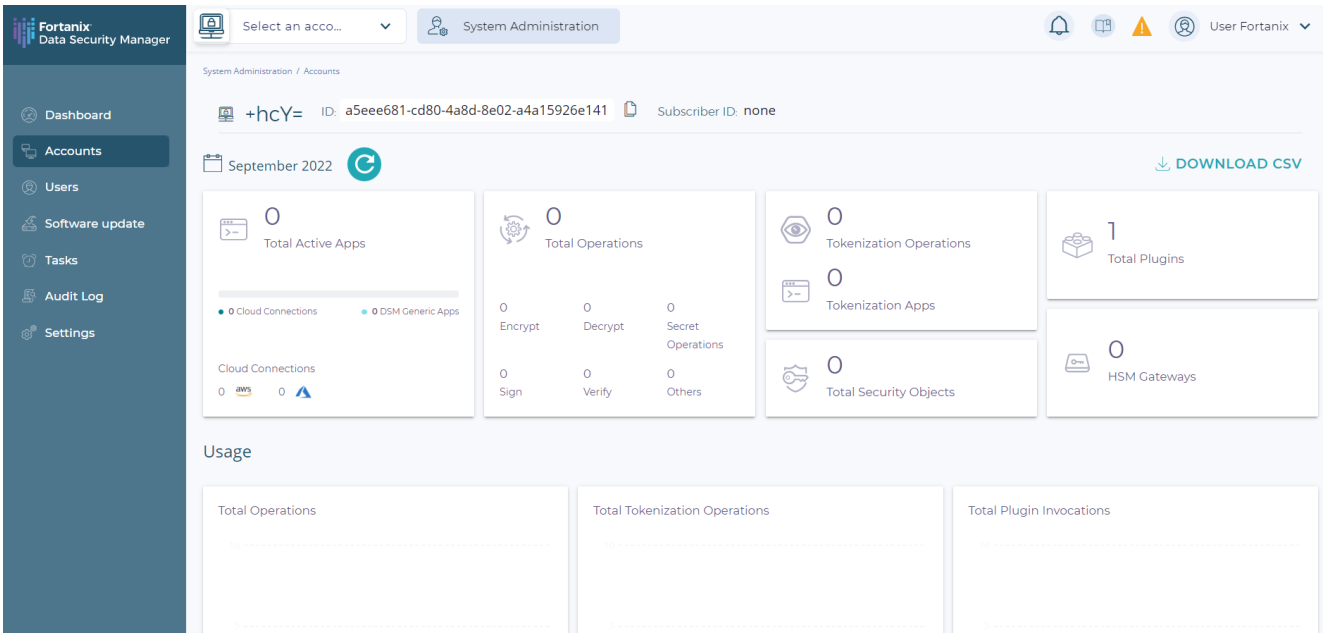

FIGURE 6: SYSTEM ADMINISTRATOR DASHBOARD VIEW

3. In the event of any anomaly, the System Administrator can notify the Account Administrator by clicking **MESSAGE.**

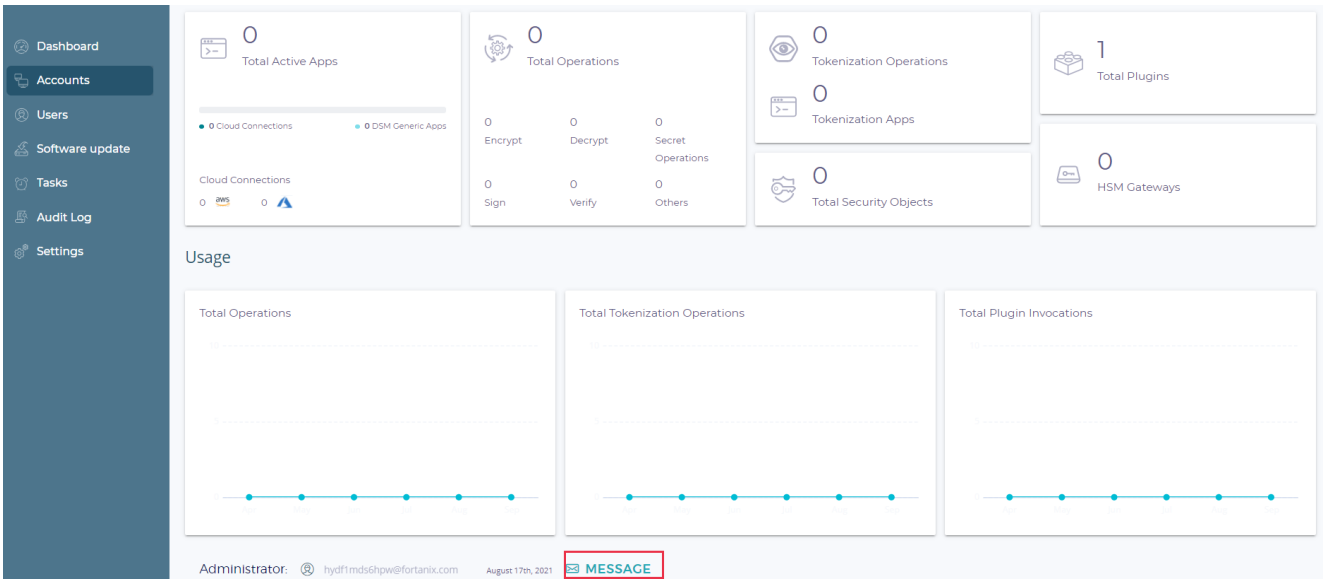

FIGURE 7:MESSAGE THE ACCOUNT ADMINISTRATOR

4. Click the toggle **Disabled** to disable the account.

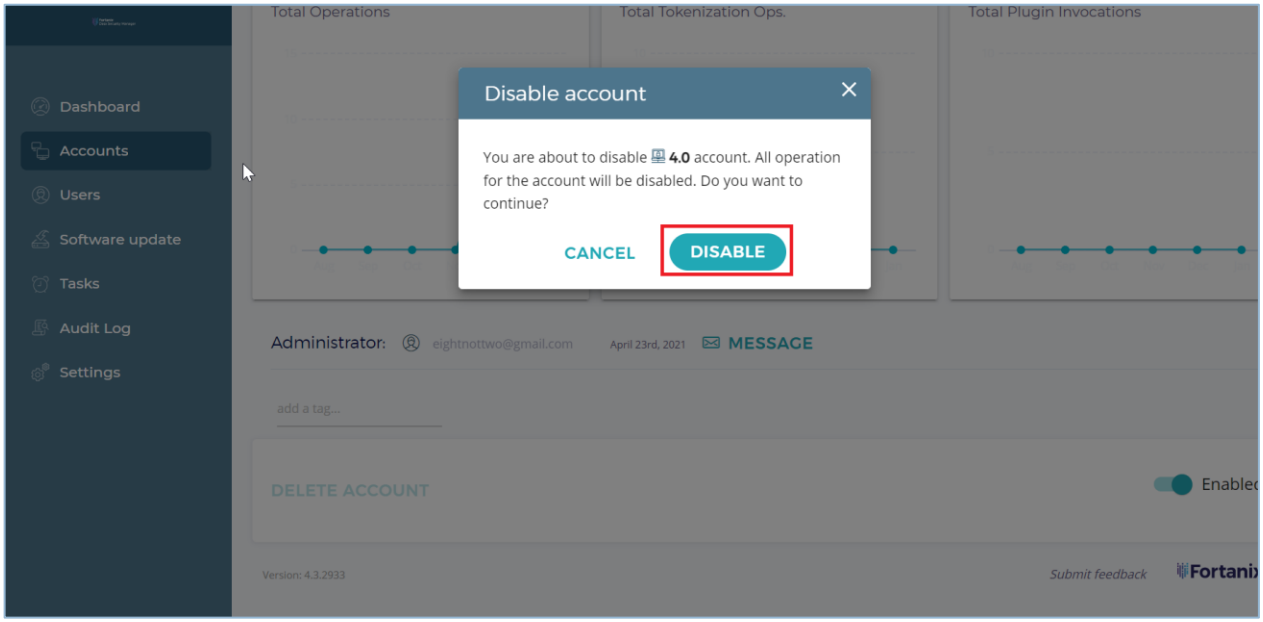

FIGURE 8: DISABLE ACCOUNT

NOTE: A System Administrator can disable an account, but not delete it. An Account Administrator can delete an account after deleting all objects (apps, security objects, plugins, groups, users) from within the account.

5.0 DOCUMENT INFORMATION

5.1 DOCUMENT LOCATION

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

https://support.fortanix.com/hc/en-us/articles/4420783611540-User-s-Guide-Usage-Metrics

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