Fortanix®

Integration Guide

USING FORTANIX DATA SECURITY MANAGER WITH SCALITY S3C FOR TRANSPARENT BUCKET ENCRYPTION

VERSION 2.0

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

1.0 INTRODUCTION 2

2.0 FORTANIX DATA SECURITY MANAGER SETUP 2

2.1 Using Fortanix DSM On-Premises Deployments 2

2.2 Using Fortanix DSM SaaS Deployment 4

2.2.1 SCALITY WIZARD INSTANCE DETAILED VIEW 5

3.0 GET THE FORTANIX CERTIFICATE AUTHORITY (CA) 5

4.0 GENERATE A CERTIFICATE AND APPLY 8

5.0 APPLY THE NEW CERT TO THE FORTANIX DATA SECURITY MANAGER APPLICATION OBJECT 8

6.0 ENABLE AUDIT LOGGING IN FORTANIX DATA SECURITY MANAGER 8

7.0 CONFIGURE SCALITY S3C 10

8.0 CREATE AN ENCRYPTED BUCKET 10

9.0 DOCUMENT INFORMATION 11

9.1 Document Location 11

9.2 Document Updates 11

1.0 INTRODUCTION

This article describes how to integrate **Fortanix Data Security Manager (DSM)** with **Scality SC3** for **Transparent Bucket Encryption** using **generic Key Management Interoperability Protocol (KMIP)**. It also contains the information that a user requires to:

- Set up Fortanix DSM
- Grab the Fortanix CA and generate a certificate
- Apply the certificate to the Fortanix DSM Application Object
- Enable audit logging in Fortanix DSM
- Configure S3C and
- Create an encrypted bucket

2.0 FORTANIX DATA SECURITY MANAGER SETUP

The key management cloud service needs to be set up using https://sdkms.fortanix.com/ before configuring Scality for bucket encryption. This document assumes that access to the Fortanix DSM UI and licensing has been established.

There are 2 ways to create an app in Fortanix DSM:

2.1 USING FORTANIX DSM ON-PREMISES DEPLOYMENTS

1. Log in to https://sdkms.fortanix.com.
2. In the Fortanix DSM UI, create a group:
   a. Click the **Groups** tab in the Fortanix DSM left menu.
   b. Click the add new group icon  to add a new group.
   c. In the **Add new group** form, enter a name for the group.

      For example: **`Scality S3C`**

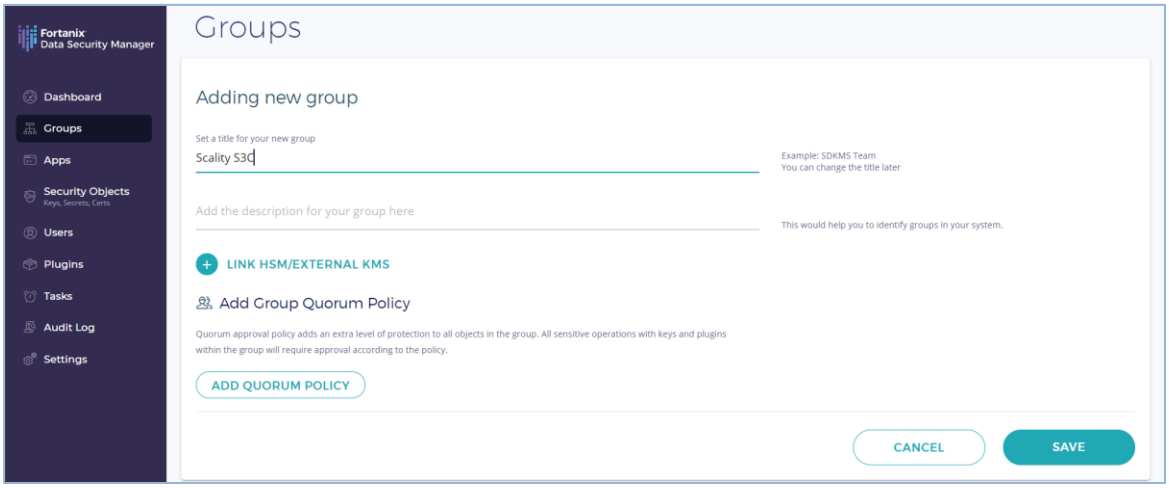

FIGURE 1: ADD GROUP

3. Create an application:
    a. Click the **Apps** tab in the Fortanix DSM left menu.
    b. Click the add new application icon  to add a new application.
    c. In the **Adding new app** form, enter a name for the application.
    For example: **`Scality S3C Bucket Encryption`**
    d. Assign the app to the group you created in Step 2.
    e. Click **Save**.

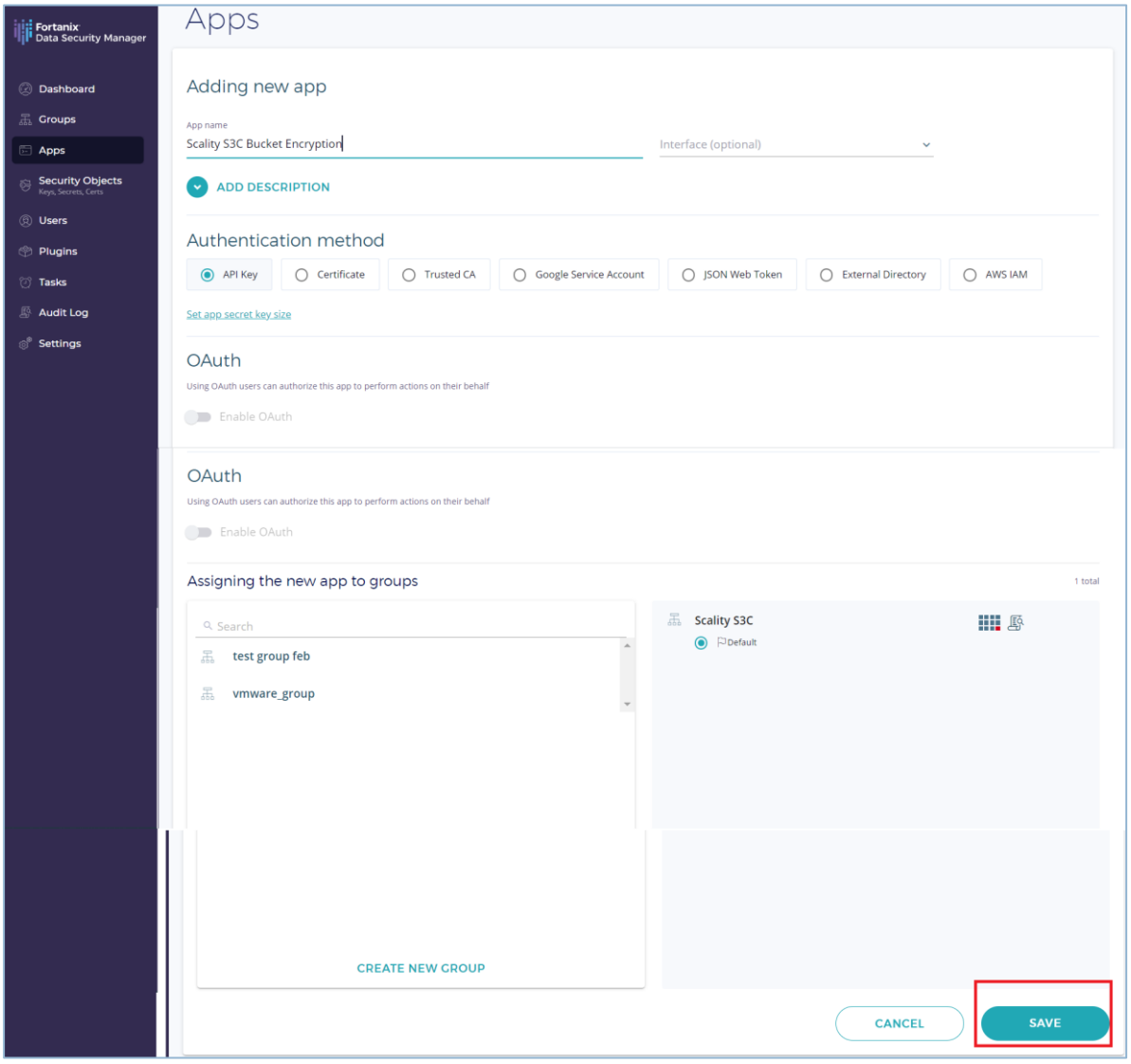

FIGURE 2: ADD APP

4. Now copy the UUID of the newly created application.

5. Change the authentication method of the Fortanix DSM App created to **'Certificate'** and click **SAVE**.
6. Continue to *Section 3.0*, *Section 4.0*, and *Section 5.0* for authentication using client certificate.
7. Click **UPDATE** to update the authentication method.

2.2 USING FORTANIX DSM SAAS DEPLOYMENT

To configure Scality wizard in Fortanix DSM SaaS:

1. Sign up at https://smartkey.io/.
2. Log in to the Fortanix DSM UI.
3. Click the **Integrations** tab in the left panel.
4. On the Integrations page, click **ADD INSTANCE** on the Scality wizard.
5. Enter the details as shown in the screenshot below:
   a. **Add Instance**: This is the name to identify the instance created.
   b. **Authentication method**: Select the desired authentication method. There are two options to choose from:
      i. **API key**: This method is used to authenticate the application with the API Gateway.
      ii. **Client Certificate:** This method is used to authenticate the application with Fortanix DSM using a Client Certificate. To upload the client certificate, click **UPLOAD CERTIFICATE**. Alternatively, the client certificate can be pasted in the field provided.

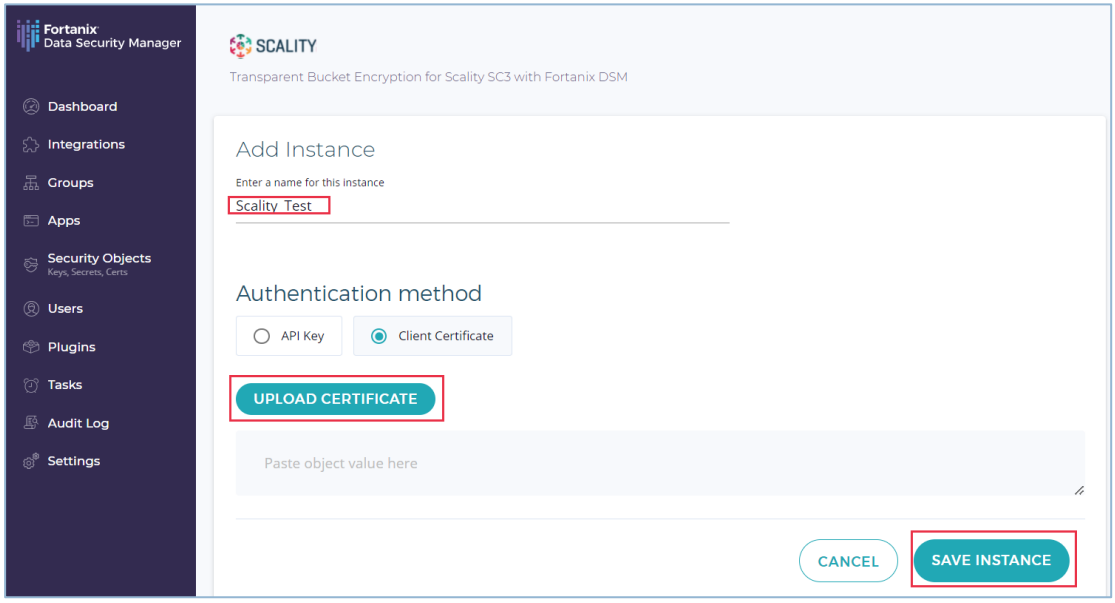

FIGURE 3: ADD INSTANCE

6. Continue to *Section 3.0, Section 4.0, and Section 5.0* for authentication using client certificate.
7. Click **SAVE INSTANCE.** With saving an instance a new Group, an App, and Keys are created within Fortanix DSM.

2.2.1 SCALITY WIZARD INSTANCE DETAILED VIEW

In the instance detailed view page, the created instances are listed as shown below:

In the instance details you will notice the following

- **Credentials**: This is the App authentication method used.
  - Click **CERTIFICATE** to download the Client Certificate. This is applicable only if the App authentication method used is a Client Certificate.
  - Click **COPY API KEY** to copy the API key. This is applicable only if the App authentication method used is API Key.
- **MANAGE**: Click **MANAGE** to manage the keys created.
- **Instance status**: To disable the instance created, click the toggle **Disabled**.

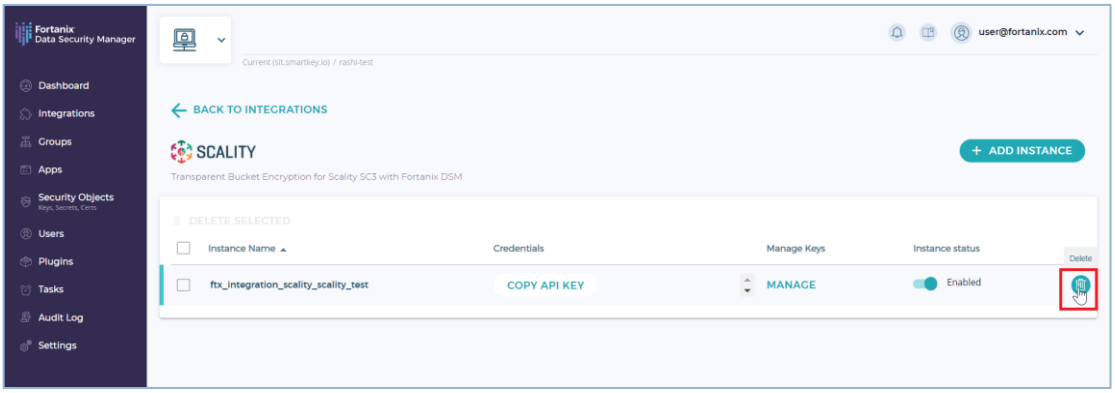

FIGURE 4:DETAILED INSTANCE

1. To delete the instance created click the  button. Note that deleting an instance will delete the App, Group, and all security objects belonging to the instance and all key material will become inaccessible.

3.0 GET THE FORTANIX CERTIFICATE AUTHORITY (CA)

1. Open Google Chrome and browse to https://sdkms.fortanix.com.
2. In the URL address bar select the padlock icon and then certificate.

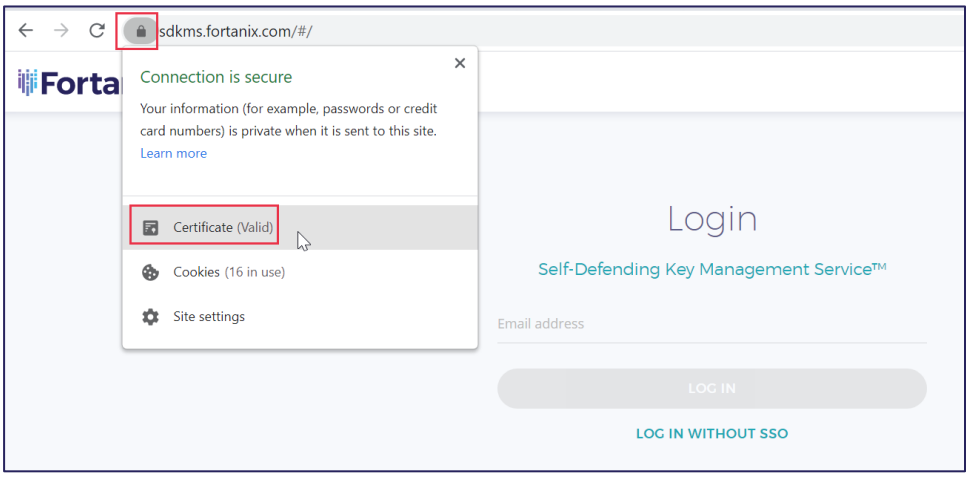

FIGURE 5: SELECT CERTIFICATE

3. Select the certification path and then highlight the root – "**DST Root CA X3**".
4. Click **View Certificate**.

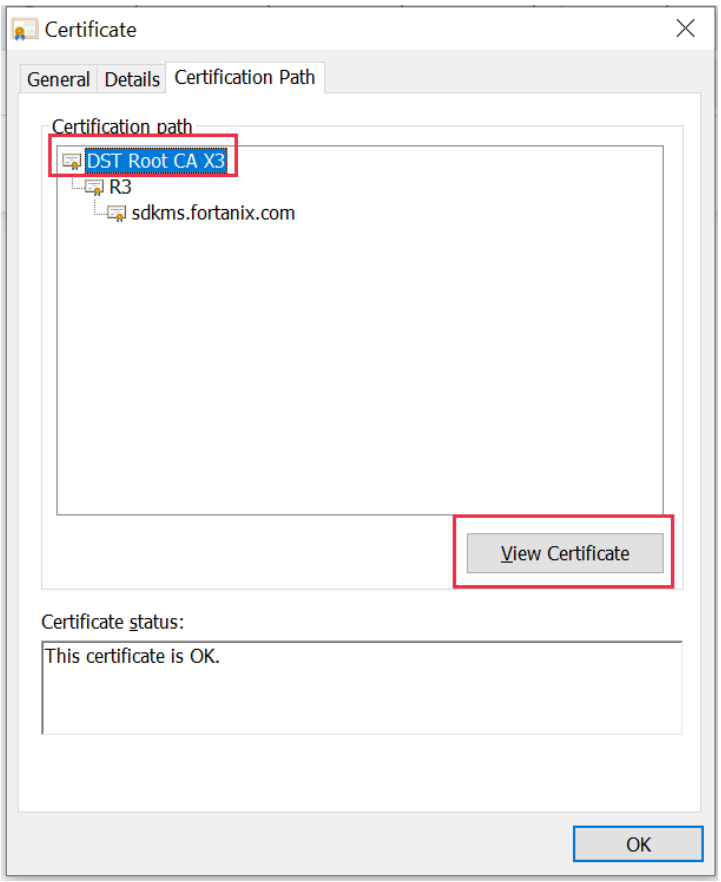

FIGURE 6: VIEW CERTIFICATE

5. Select the **Details** tab and then click the **Copy to File** button.

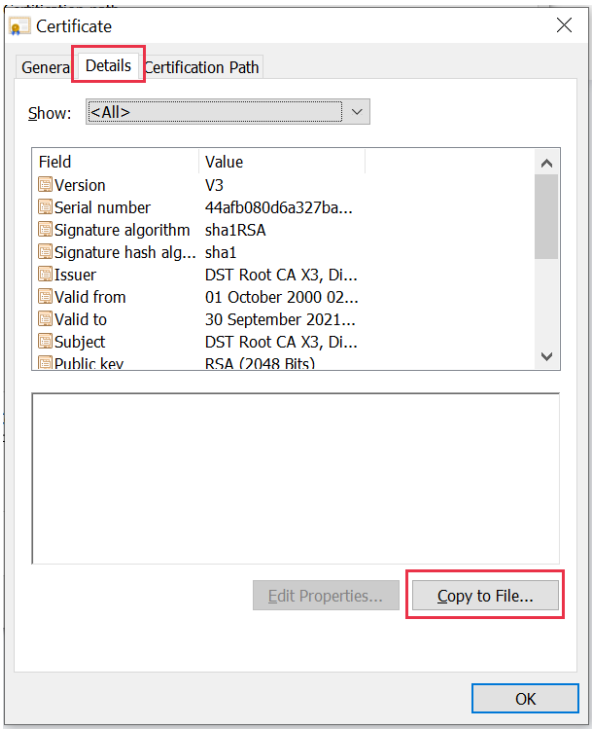

FIGURE 7: COPY TO FILE

6. Click **Next** and then select the radio button for Base-64 encoded X.509 (.CER) before saving it and choosing a filename (Example: `fortanix_ca.cer`).

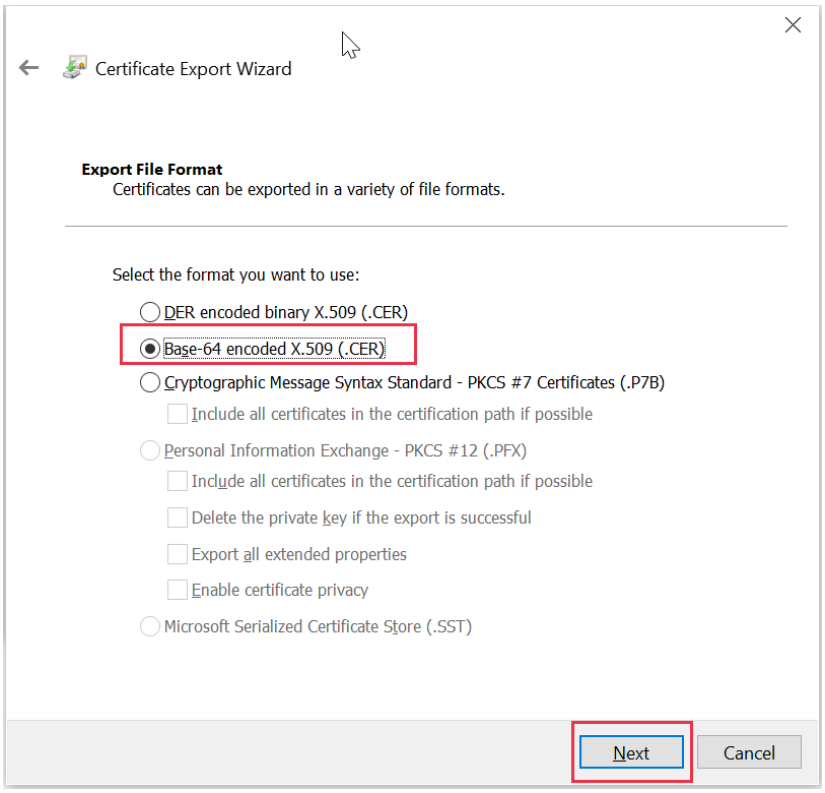

FIGURE 8: BASE64 ENCODED

4.0 GENERATE A CERTIFICATE AND APPLY

On a host with OpenSSL create the certificates that you need to authenticate to the KMIP service you just created.

```
# openssl req -x509 -newkey rsa:2048 -nodes -keyout key.pem \

-out cert.pem -days 365 \

-subj "/CN=<UUID you copied from the app>"
```

For example:

```
openssl req -x509 -newkey rsa:2048 -nodes -keyout key.pem -out cert.pem -days

365 -subj "/CN=c6ad2ad7-4948-4b60-8cd6-f33c00a01428"
```

You should now have the following:

- The Fortanix CA certificate (`fortanix_ca_cer`).
- A private key (`key.pem`).
- A certificate (`cert.pem`).

5.0 APPLY THE NEW CERT TO THE FORTANIX DATA SECURITY MANAGER APPLICATION OBJECT

1. Copy and paste the contents of the `cert.pem` file generated in in the **Upload certificate** text box in the Fortanix DSM app for client certificate authentication and save the details.
2. The application object is configured to use the generated asymmetric key/cert pair you created for authentication.

6.0 ENABLE AUDIT LOGGING IN FORTANIX DATA SECURITY MANAGER

Audit logging is required to confirm that things are working (or why they are not).

In the Fortanix DSM UI:

1. Click the **Apps** tab from the left menu.
2. In the Apps table, click the application you created in Section 2.0.
3. In the detailed view of the app, in the **INFO** tab, under the **Groups** section click the grid for **App permissions** to edit the app permissions.

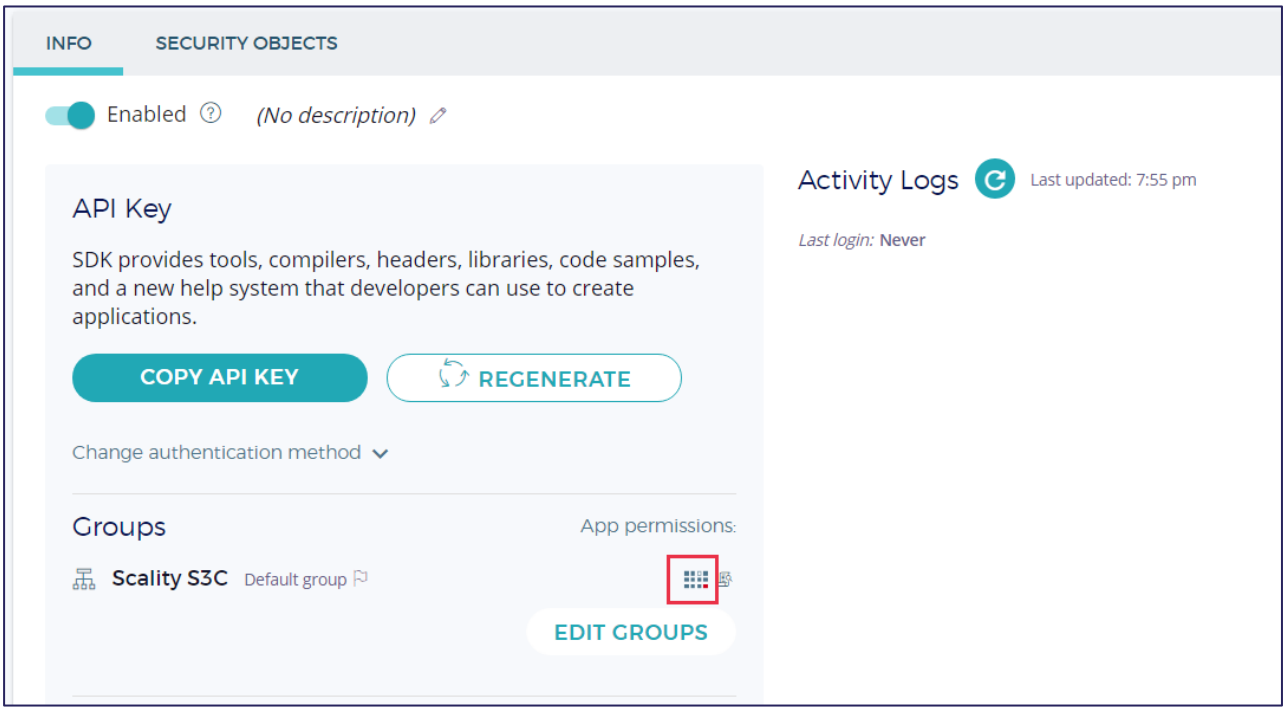

FIGURE 9: APP PERMISSIONS

4. In the **Set app permissions for objects in the group** dialog, select the **Allow access to audit log** option.

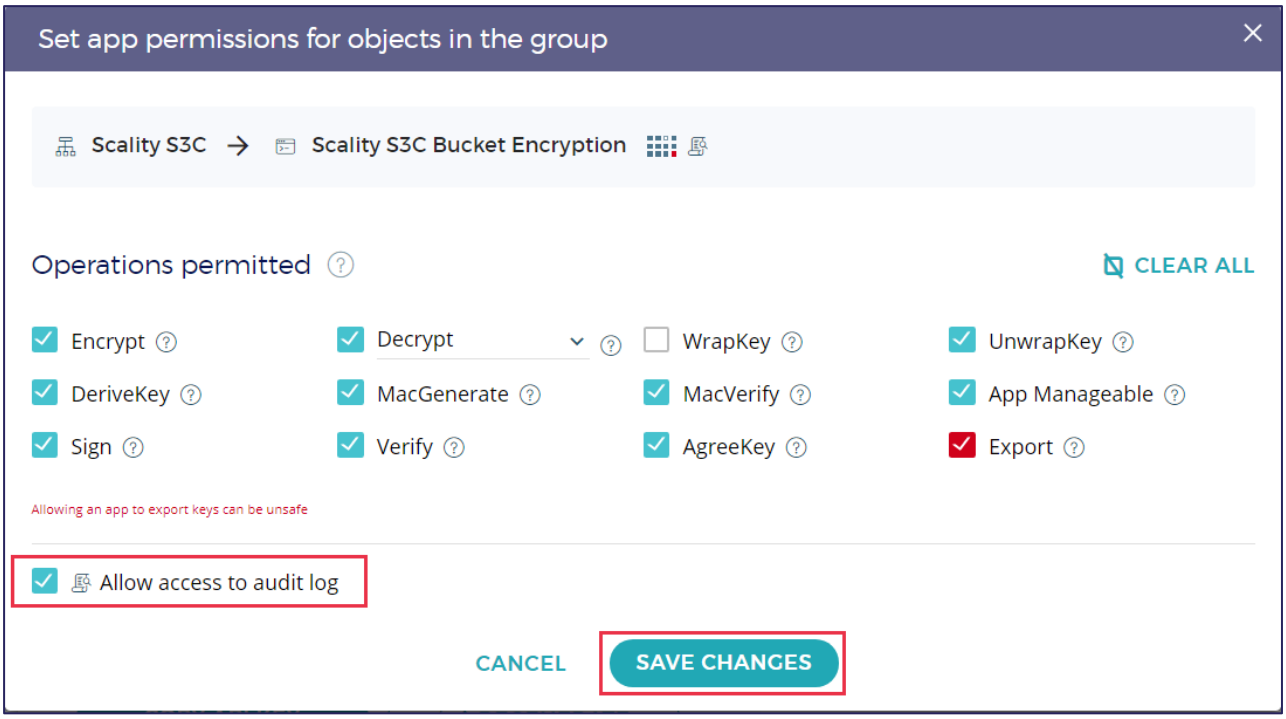

FIGURE 10: ENABLE AUDIT LOGGING

7.0 CONFIGURE SCALITY S3C

Refer to the S3 Connector Install Guide for current information on configuring a KMS. Navigate to https://documentation.scality.com/, select your RING version under RING, then scroll down to the S3 documentation.

In summary: the relevant section in your `group_vars/all` file will look like this:

```
env_s3:
 kmip:
  port: 5696
  host: sdkms.fortanix.com
  compoundCreate: false
  bucketAttributeName: x-zenko-bucket
  pipelineDepth: 8
  key: kmip_key.pem
  cert: kmip_cert.pem
  ca:
   - fortanix_CA.cer
```

All certs go in the kmip directory under your environment (`s3/federation/env/<your env>/kmip`). Also note that, at the time of this writing, there is no boiler-plate in the `group_vars/all` file for the above "`kmip`" section, nor is there a pre-created "`kmip`" directory for the certs. So please create them.

8.0 CREATE AN ENCRYPTED BUCKET

Encrypted buckets with S3C cannot be created with the Amazon API call. It has to be done with a special header on bucket creation. There is a script for doing this in any cloudserver (s3) container. Follow the documentation (see *Using Bucket Encryption* in the *S3 Connector Operation* doc.)

If there is an issue (you get a 50x when trying to create the bucket) errors will show up in the S3 log on the host you are using (For example: `/var/log/s3/scality-s3-1/logs/s3-0.log`). If you did not get an error, congratulations! You have an encrypted bucket.

You will see a new security object in the Fortanix interface confirming communication.

9.0 DOCUMENT INFORMATION

9.1 DOCUMENT LOCATION

The latest published version of this document is located at the URL:
https://support.fortanix.com/hc/en-us/articles/360059489492-Using-Fortanix-Data-Security-Manager-with-Scality-S3C

9.2 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