Fortanix®

Integration Guide

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

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

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.

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`**
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**.
    f. Now copy the UUID of the newly created application.

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.

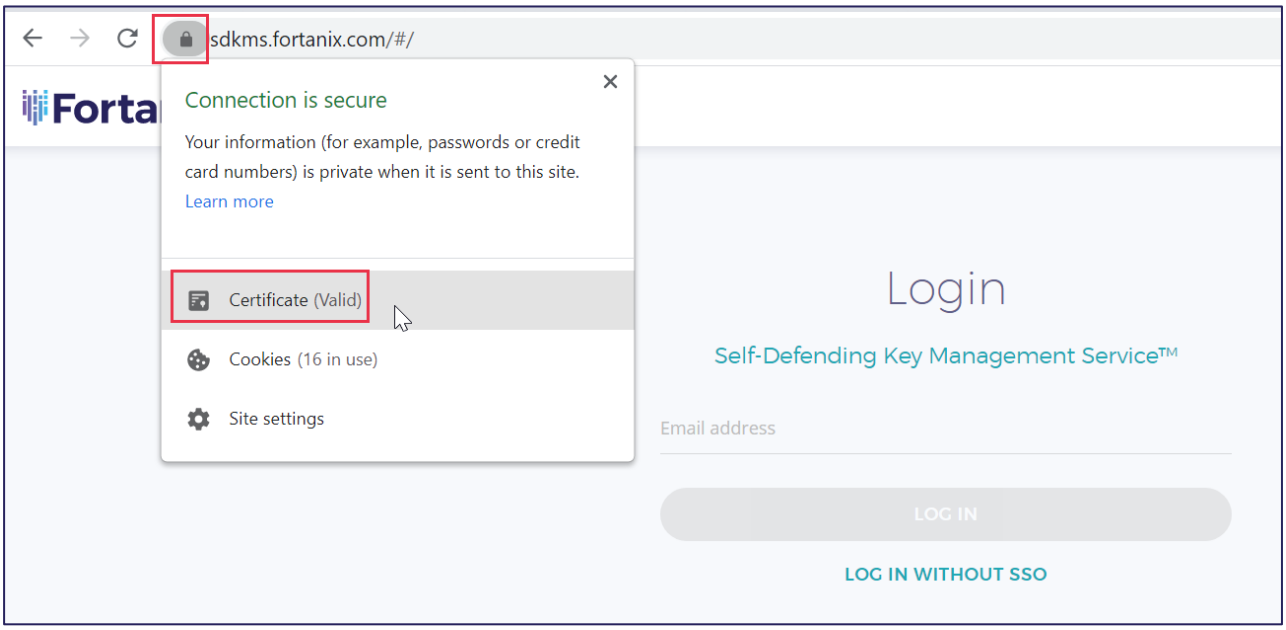

FIGURE 1: SELECT CERTIFICATE

3. Select the certification path and then highlight the root – "**DST Root CA X3**".
4. Select view certificate.

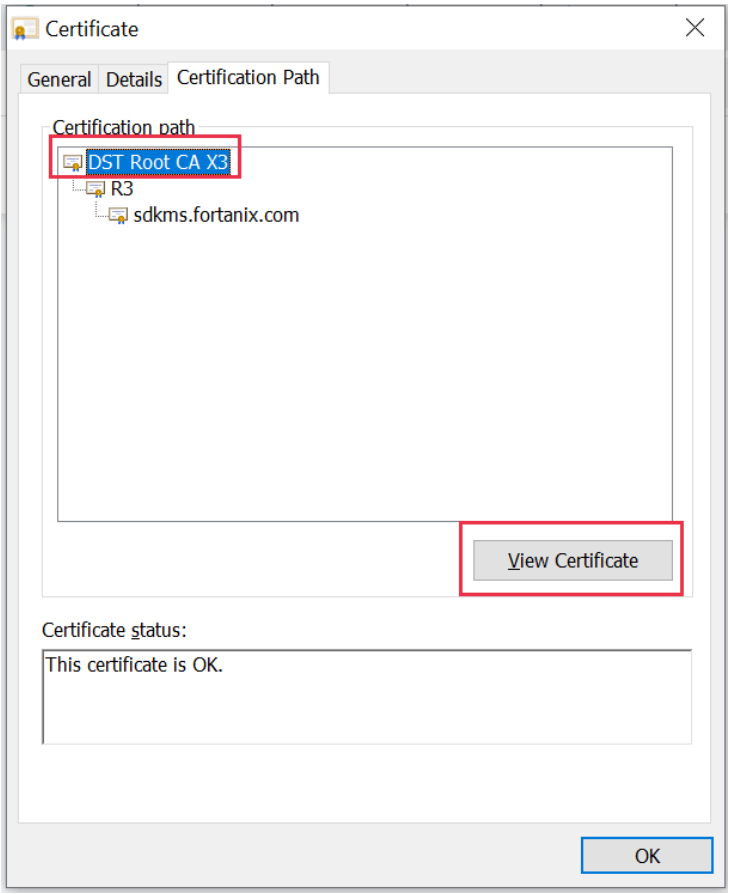

FIGURE 2: VIEW CERTIFICATE

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

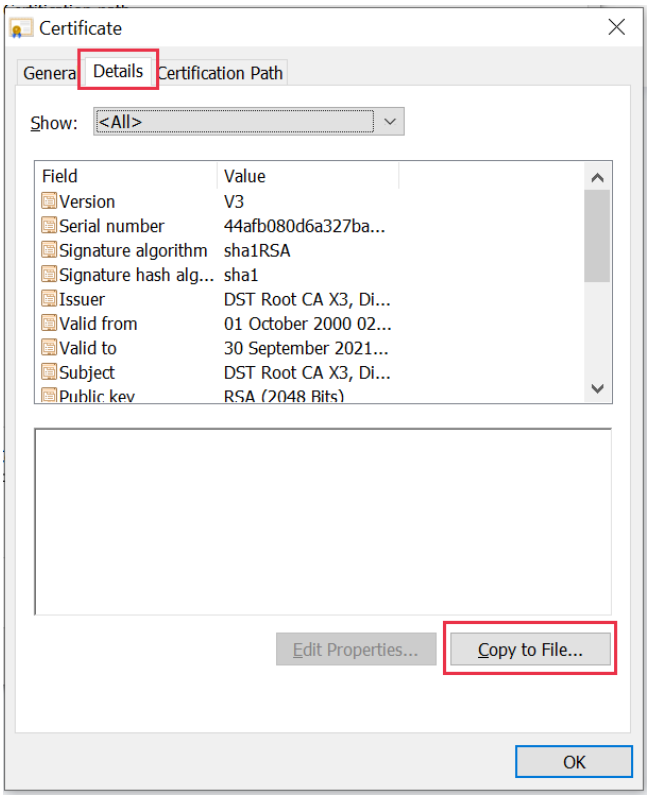

FIGURE 3: COPY TO FILE

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`).

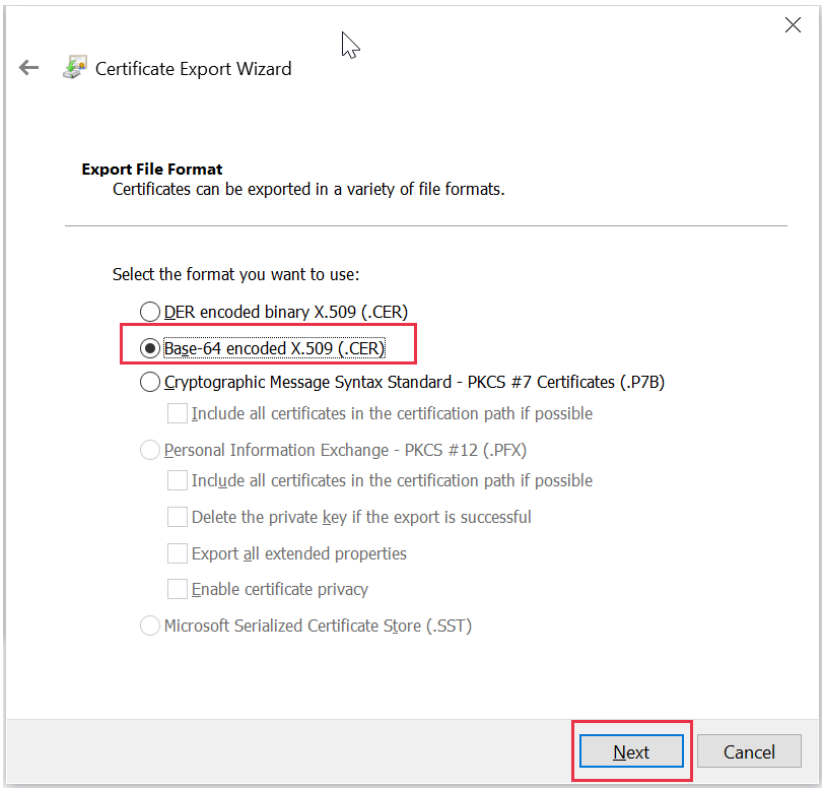

FIGURE 4: BASE64 ENCODED

4.0 GENERATE A CERTIFICATE

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

In the Fortanix DSM interface:

1. Click the **Apps** tab.
2. Select the application (**`Scality S3C Bucket Encryption)`** you created in Section 2.0.
3. In the detailed view of the app, in the **INFO** tab click the **Change authentication method** drop down under the **API Key** section.
4. Select **Certificate** and click **SAVE**.
5. This will open a dialog for entering the certificate. Copy and paste the contents of the `cert.pem` file into the provided text area and click **UPDATE**.

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.

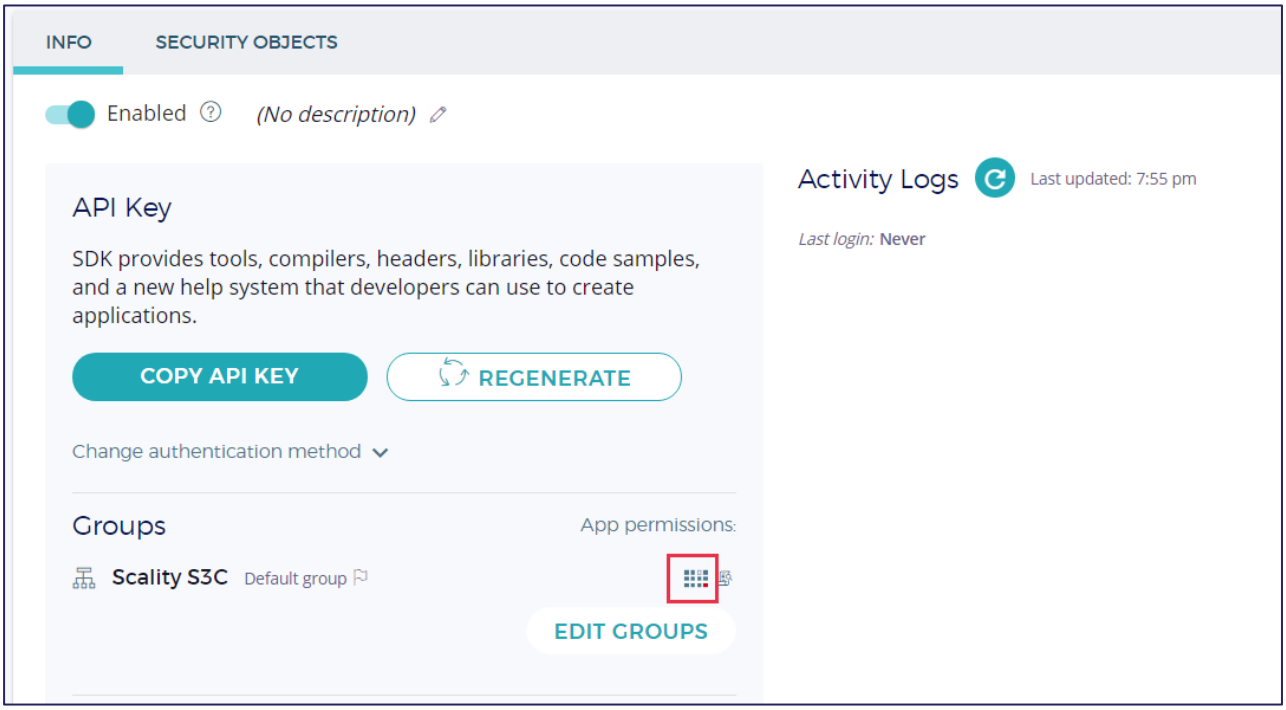

FIGURE 5: APP PERMISSIONS

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

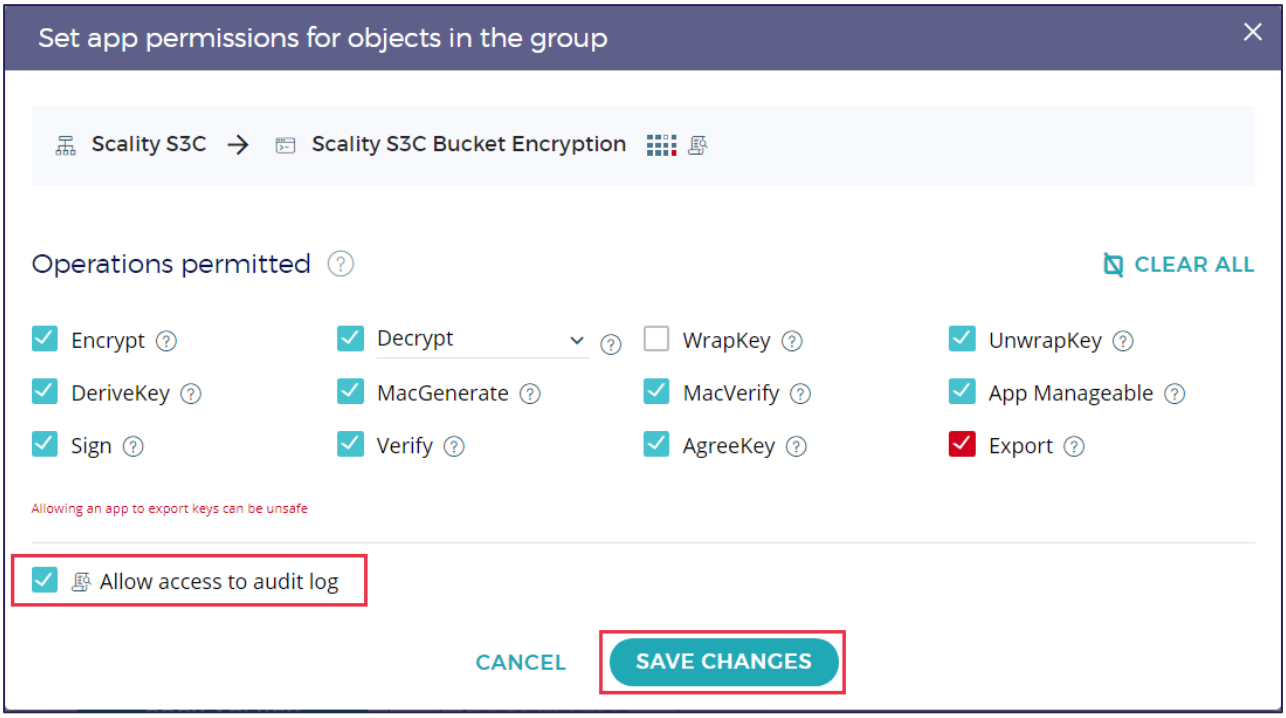

FIGURE 6: ENABLE AUDIT LOGGING

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