Fortanix®

API Guide

FORTANIX DATA SECURITY MANAGER – OPAQUE AND SECRET OBJECTS

VERSION 1.0

LAST REVISION DATE: 14-APR-2021

Fortanix Inc. | 3910 Freedom Circle | Suit 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) API Guide for Opaque and Secret Objects. This document describes how to create Opaque and Secret objects in Fortanix DSM. It also provides the following details:

- Difference between Opaque and Secret Objects
- How to import Opaque and Secret Objects using API

2.0 HOW TO USE OPAQUE AND SECRET OBJECTS USING API

2.1 FORTANIX DATA SECURITY MANAGER OPAQUE VS SECRET OBJECTS

Opaque Objects: In addition to keys for the algorithms such as AES, ECDSA, ECDH, RSA, DES and so on described in algorithms support, Fortanix DSM has the ability to store "opaque" objects. An opaque object can be used to store arbitrary data, which may or may not be sensitive. Fortanix DSM does not perform cryptographic operations using opaque objects, but clients can fetch the value of the opaque object from Fortanix DSM.

Possible uses of opaque objects include:

- Storing passwords or other non-cryptographic secrets
- Storing keys for algorithms not natively supported by Fortanix DSM

Secret Objects: A Secret type of security object is used to store secret value that is not a key or certificate. For example, passphrase, password and so on.

The following table highlights the differences and similarities between an Opaque and Secret Object.

SECRET OBJECTS	OPAQUE OBJECTS
1. Secret type of security object used to store secret value that is not a key or certificate. For ex: passphrase, password and so on. 2. Accessing the values of Secret objects is audit logged. 3. Maximum size supported by an Opaque object is 512 kilobytes. 4. Can be imported using web interface. 5. Crypto operation is not supported for a Secret security object. 6. By default, import operation stores the object as exportable security object.	1. Opaque type of security object used to store arbitrary data, may or may not be sensitive. 2. There are no audit logs for accessing Opaque objects. 3. Maximum size supported by an Opaque object is 512 kilobytes. 4. Can be imported using web interface. 5. Crypto operation is not supported for a Opaque security object. 6. By default, import operation stores the object as exportable security object.

3.0 OPAQUE OBJECTS USING API

3.1 LOG IN TO FORTANIX DATA SECURITY MANAGER

Log in to Fortanix DSM using the following command

```
curl -X POST "https:// <fortanix_dsm_url>/sys/v1/session/auth" \
-u <user.name@company.com>:PASS
```

The command above will generate the following response:

```
{
```

```
"token_type":"Bearer","expires_in":3600,"access_token":"wO9gVTTESKyCp
dF-CnoOA-WLqEzaCDzQiCMNxOidtM-7MNmp0PhZU5xZSPgWj2yBzfxhsT-
N4tpoep8HAH_Ejg","entity_id":"b4ff897f-97be-4cac-b7d3-878ea5d5a652"
}
```

3.2 SELECT ACCOUNT

Select the account using the following command:

```
curl -X POST
"https://<fortanix_dsm_url>/sys/v1/session/select_account" \
  -H "Authorization: Bearer i7iy-
bt9dXXHmQ0DDDTfeKJomNwu7XTN9edpOUhJpP7dQvIpcZt2wfvWjXn93XfHsZ2yavaope
tVxDIAdb9H3Q" \
  -d "{\"acct_id\": \"c86838af-70cb-48d7-81b5-b7c38c152412\"}"
```

The command above will generate the following response:

```
{
  "cookie":"sdkms_admin_auth=; Domain=<fortanix_dsm_url>; Expires=Thu
, 01 Jan 1970 00:00:00 GMT; Secure"
 }
```

3.3 IMPORT AN OPAQUE OBJECT

To create an opaque security object, use the API:

```
curl -X PUT "https:// <fortanix_dsm_url>/crypto/v1/keys" \
-H "Authorization: Bearer i7iy-bt9dXXHmQ0DDDTfeKJomNwu7XTN9edpOUhJpP7
dQvIpcZt2wfvWjXn93XfHsZ2yavaopetVxDIAdb9H3Q" \
-d "{\"name\" : \"opq1\", \"obj_type\" : \"OPAQUE\", \"value\":
\"<base64 encoded phrase>\", \"group_id\": \"5b623820-f980-46c6-9512-
5058b61840f8\"}"
```

In the specification above,

<base64 encoded phrase> is a base64 encoded string for your passphrase/secrets. For example: `01`

name: Name of the security object to create or import. Security object names must be unique within an account.

object_type: Type of security object. The default value is "*OPAQUE*".

Value: When importing a security object, this field contains the binary contents to import. When creating a security object, this field is unused. The value of an OPAQUE or CERTIFICATE object is always returned. For other objects, the value is returned only with `/crypto/v1/keys/export` API (if the object is exportable).

The code snippet above returns the following response containing the `key_id (kid)`.


```
 {
"acct_id": "c86838af-70cb-48d7-81b5-b7c38c152412",
"activation_date": "20191127T063211Z",
"created_at": "20191127T063211Z",
"creator": {
    "user": "b4ff897f-97be-4cac-b7d3-878ea5d5a652"
 },
"enabled": true,
"key_ops": [
    "EXPORT",
    "APPMANAGEABLE"
],
"key_size": 8,
"kid": "14f7b611-f886-4328-9e93-2aff20daff33",
"lastused_at": "19700101T000000Z",
"name": " opq1",
"never_exportable": false,
"obj_type": "OPAQUE",
"origin": "External",
```

```
"public_only": false,
"state": "Active",
"group_id": "5b623820-f980-46c6-9512-5058b61840f8"
}
```

3.4 EXPORT THE VALUE OF OPAQUE OBJECT

To export the value of opaque object, use the API:

```
curl -X GET "https:// <fortanix_dsm_url>/crypto/v1/keys/ffa75177-019f-4602-9038-f0971c2eea45" -H "Authorization: Bearer 8k3EfJrEYD0IkmP08llvM83x93RTtSOvdHmB99h9Zsu80WKcVLgtQYvUDwfEqcimZMEee1_2SzUaKlPFJ6cjsw"
```

The command above will return the following response:

```
{
    "acct_id": "c86838af-70cb-48d7-81b5-b7c38c152412",
    "activation_date": "20191113T122032Z",
    "created_at": "20191113T122032Z",
    "creator": {
        "user": "b4ff897f-97be-4cac-b7d3-878ea5d5a652"
    },
    "enabled": true,
    "key_ops": [
        "EXPORT",
        "APPMANAGEABLE"
    ],
    "key_size": 8,
    "kid": "ffa75177-019f-4602-9038-f0971c2eea45",
    "lastused_at": "19700101T000000Z",
    "name": "opq1",
    "never_exportable": false,
    "obj_type": "OPAQUE",
    "origin": "External",
    "public_only": false,
    "state": "Active",
```

```
    "value": "0w==",
    "group_id": "5b623820-f980-46c6-9512-5058b61840f8"
}
```

The command above returns the value of the opaque object.

4.0 SECRET OBJECTS USING API

4.1 LOG IN TO FORTANIX DATA SECURITY MANAGER

Log in to Fortanix DSM using the following command:

```
curl -X POST "https:// <fortanix_dsm_url>/sys/v1/session/auth" \
-u <user.name@company.com>:PASS
```

The command above will generate the following response:

```
  {
"token_type":"Bearer","expires_in":3600,"access_token":"wO9gVTTESKyCp
dF-CnoOA-WLqEzaCDzQiCMNxOidtM-7MNmp0PhZU5xZSPgWj2yBzfxhsT-
N4tpoep8HAH_Ejg","entity_id":"b4ff897f-97be-4cac-b7d3-878ea5d5a652"
}
```

4.2 SELECT ACCOUNT

Select the account using the following command:

```
curl -X POST
"https://<fortanix_dsm_url>//sys/v1/session/select_account" \
  -H "Authorization: Bearer i7iy-
bt9dXXHmQ0DDDTfeKJomNwu7XTN9edpOUhJpP7dQvIpcZt2wfvWjXn93XfHsZ2yavaope
tVxDIAdb9H3Q" \
```

```
-d "{\"acct_id\": \"c86838af-70cb-48d7-81b5-b7c38c152412\"}"
```

The command above will generate the following response:

```
{
  "cookie":"sdkms_admin_auth=; Domain=<fortanix_dsm_url>; Expires=Thu
, 01 Jan 1970 00:00:00 GMT; Secure"
}
```

4.3 IMPORT A SECRET OBJECT

To create an Secret security object, use the API:

```
curl -X PUT "https://<fortanix_dsm_url>/crypto/v1/keys" \
-H "Authorization: Bearer i7iy-bt9dXXHmQ0DDDTfeKJomNwu7XTN9edpOUhJpP7
dQvIpcZt2wfvWjXn93XfHsZ2yavaopetVxDIAdb9H3Q" \
-d "{\"name\" : \"opq1\", \"obj_type\" : \"SECRET\", \"value\":
\"<base64 encoded phrase>\", \"group_id\": \"5b623820-f980-46c6-9512-
5058b61840f8\"}"
```

In the specification above,

<base64 encoded phrase> is a base64 encoded string for your passphrase/secrets. For example: `01`

name: Name of the security object to create or import. Security object names must be unique within an account.

object_type: Type of security object. The default value is "*SECRET*".

Value: When importing a security object, this field contains the binary contents to import. When creating a security object, this field is unused. The value of an SECRET or CERTIFICATE object is

always returned. For other objects, the value is returned only with `/crypto/v1/keys/export` API (if the object is exportable).

The code snippet above returns the following response containing the `key_id (kid)`.

```
 {
"acct_id": "c86838af-70cb-48d7-81b5-b7c38c152412",
"activation_date": "20191127T063211Z",
"created_at": "20191127T063211Z",
"creator": {
    "user": "b4ff897f-97be-4cac-b7d3-878ea5d5a652"
 },
"enabled": true,
"key_ops": [
    "EXPORT",
    "APPMANAGEABLE"
],
"key_size": 8,
"kid": "14f7b611-f886-4328-9e93-2aff20daff33",
"lastused_at": "19700101T000000Z",
"name": " secret_obj",
"never_exportable": false,
"obj_type": "SECRET",
"origin": "External",
"public_only": false,
"state": "Active",
"group_id": "5b623820-f980-46c6-9512-5058b61840f8"
 }
```

4.4 EXPORT THE VALUE OF SECRET OBJECT

To export the value of secret object, use the API:

```
curl -X POST "https://<fortanix_dsm_url>/crypto/v1/keys/export" \
```

```
  -H "Authorization: Bearer i7iy-
bt9dXXHmQ0DDDTfeKJomNwu7XTN9edpOUhJpP7dQvIpcZt2wfvWjXn93XfHsZ2yavaopet
VxDIAdb9H3Q" \
  -d "{\"name\": \"secret_obj\"}"
```

The command above will return the following response:


```
{
    "acct_id": "c86838af-70cb-48d7-81b5-b7c38c152412",
    "activation_date": "20191113T122032Z",
    "created_at": "20191113T122032Z",
    "creator": {
        "user": "b4ff897f-97be-4cac-b7d3-878ea5d5a652"
    },
    "enabled": true,
    "key_ops": [
        "EXPORT",
        "APPMANAGEABLE"
    ],
    "key_size": 8,
    "kid": "14f7b611-f886-4328-9e93-2aff20daff33",
    "lastused_at": "19700101T000000Z",
    "name": "secret_obj",
    "never_exportable": false,
    "obj_type": "SECRET",
    "origin": "External",
    "public_only": false,
    "state": "Active",
    "value": "0w==",
    "group_id": "5b623820-f980-46c6-9512-5058b61840f8"
}
```

The command above returns the value of the secret object.

5.0 OPAQUE OBJECTS USING FORTANIX DATA SECURITY MANAGER-CLI

5.1 LOG IN TO FORTANIX DATA SECURITY MANAGER

Log in to Fortanix DSM using the following command:

```
sdkms-cli user-login --username <dsm-username> --account-name <dsm-account-name>
```

5.2 IMPORT AN OPAQUE OBJECT

To create an opaque object, use the following command:

```
sdkms-cli import-secret --in <opaque-object-path> --name <name> --obj-type OPAQUE --group-id <group-id>
```

5.3 EXPORT AN OPAQUE OBJECT

To export an opaque object, use the following command:

```
sdkms-cli export-object --kid <security-object-uuid>
```

6.0 SECRET OBJECTS USING FORTANIX DATA SECURITY MANAGER-CLI

6.1 LOG IN TO FORTANIX DATA SECURITY MANAGER

Log in to Fortanix DSM using the following command:

```
sdkms-cli user-login --username <dsm-username> --account-name <dsm-account-name>
```

6.2 IMPORT A SECRET OBJECT

To create a secret object, use the following command:

```
sdkms-cli import-secret --in <secret-object-path> --name <name> --obj-type SECRET --group-id <group-id>
```

6.3 EXPORT A SECRET OBJECT

To export a secret object, use the following command:

```
sdkms-cli export-object --kid <security-object-uuid>
```

7.0 DOCUMENT INFORMATION

7.1 DOCUMENT LOCATION

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

https://support.fortanix.com/hc/en-us/articles/360015941332-Using-Opaque-and-Secret-objects

7.2 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