Fortanix®

User Guide

FORTANIX DATA SECURITY MANAGER (DSM) – STORE KEYS EXTERNALLY IN DSM – SETUP GUIDE

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

TABLE OF CONTENTS

1.0 INTRODUCTION 2

1.1 Intended audience 2

2.0 EXTENDED VIRTUAL KEYS CONCEPTS 2

3.0 TERMINOLOGY REFERENCES 2

4.0 OBTAINING ACCESS TO FORTANIX DATA SECURITY MANAGER 3

5.0 STORE KEYS EXTERNALLY - GROUP SETUP 3

5.1 Prepare the Source Fortanix DSM Cluster 3

5.2 Configure the Primary DSM Cluster on the Secondary DSM Cluster 4

5.3 Add Certificate (Optional) 5

5.4 The HSM/KMS Tab 6

6.0 DOCUMENT INFORMATION 7

6.1 Document Location 7

6.2 Document Updates 7

1.0 INTRODUCTION

Welcome to the Fortanix Data Security Manager (DSM) Store Keys Externally using a DSM-backed group guide. This document describes how to connect a group in a Fortanix DSM account (secondary group) with a group in another Fortanix DSM account (primary group) in the same/different cluster such that the new keys are physically generated and stored in the primary group. The document also describes the following:

- Creating and configuring a Fortanix DSM-linked primary group (on-premises/cloud/SaaS DSM) in the Fortanix DSM secondary group (on-premises/cloud/SaaS DSM).
- Testing the connection between the primary and secondary groups.
- Syncing the keys from the DSM primary group into the DSM secondary group as virtual keys.
- Optionally caching key material from the DSM primary group in the DSM secondary group for Extended Virtual Keys.
- Enabling auto scan on the source group.

1.1 INTENDED AUDIENCE

This document is intended to be used by technical stakeholders of Fortanix DSM who will be responsible for planning, performing, or maintaining the installation or Deployment of DSM and Extended Virtual Keys, such as the Architects, Systems Administrator, Chief Information Officer (CIO), Analysts, or Developers.

2.0 EXTENDED VIRTUAL KEYS CONCEPTS

Refer to the DSM Extended Virtual Keys – Concepts guide.

3.0 TERMINOLOGY REFERENCES

- **DSM –** Data Security Manager
- **Fortanix DSM secondary group** – This is the Fortanix DSM-backed group.
- **Fortanix DSM primary group –** This is the External DSM group that is going to be configured in the Fortanix DSM secondary group.
- **Fortanix DSM primary key –** This is the actual key present in the Fortanix DSM primary group containing the key material.

- **Fortanix DSM secondary key –** This is the virtual representation of the Fortanix DSM primary key.

4.0 OBTAINING ACCESS TO FORTANIX DATA SECURITY MANAGER

Create an account in Fortanix DSM if you do not have one already. *See the Fortanix DSM Getting Started guide for more information.*

5.0 STORE KEYS EXTERNALLY - GROUP SETUP

This section describes the steps to configure a Fortanix DSM secondary group to interact with the Fortanix DSM primary group. A Fortanix DSM secondary group is created in the secondary Fortanix DSM cluster, and this group is configured to interact with the primary Fortanix DSM cluster that contains the actual keys.

5.1 PREPARE THE SOURCE FORTANIX DSM CLUSTER

This step must be done on the Fortanix DSM primary cluster.

1. Create an account in the DSM primary cluster, then set up account administrators.
2. Create a group in the DSM primary cluster.
3. Create an application (app) in the DSM primary cluster. Make a note of the API Key of this application as it will be required when configuring the group in the Fortanix DSM secondary Cluster.

NOTE:

- For the Extended Virtual Keys use case, the app must have “Export” permission
- The app must belong to the group from where the keys are to be replicated.
- To further secure the use of this app from the cloud, you may add an IP whitelisting policy on this app and mention the IP address(es) or CIDR of your Fortanix DSM secondary cluster. This will ensure the API key cannot be used from anywhere else.

5.2 CONFIGURE THE PRIMARY DSM CLUSTER ON THE SECONDARY DSM CLUSTER

1. On the Fortanix DSM **Groups**  page, click the  button to create a new Fortanix DSM primary group.
2. In the **Add new group** form:
   - Enter a name and description for your group.
   - Next, in the **Configure as HSM/External KMS Group** section, click **LINK HSM/EXTERNAL KMS**.
   - In the drop down menu, select **Fortanix DSM** as the type of HSM/External KMS group.
   - Select the **Store keys externally** option to generate, manage, and use keys in an external DSM primary cluster (on-premises/cloud/SaaS) and store the virtual keys locally in the DSM secondary cluster (on-premises/cloud/SaaS).
   - In the **Authentication** section, enter the following values:
     - DNS name of the **DSM** endpoint. For example:

       `amer.smartkey.io`

       NOTE: Do not add "`https`" before the DNS name.
     - The API key of the application that was created in the DSM primary cluster. *Refer to Section 5.1: Prepare the Source DSM Cluster*.
3. Add a certificate. *For more details refer to Section 5.3*.
4. Click **TEST CONNECTION** to test your primary group connection. If the Fortanix DSM secondary group can connect to your primary group using your connection details, then it shows the status as "Connected" with a green tick  . Otherwise, it shows the status as "**Not Connected**" with a yellow warning sign  .
5. For enabling Extended Virtual Keys, select **Fetch key material** to cache the key material of the keys from the Fortanix DSM primary group in the Fortanix DSM secondary group during a key sync operation. The keys in the Fortanix DSM primary group must be exportable in order to be cached in the Fortanix DSM secondary group. However, if they are not exportable, then you can select one of the following options:

- **Ignore non-exportable keys** – Select this option to ignore all the non-exportable primary keys during key sync so that the virtual keys will not be created in the secondary group for these non-exportable keys.

  NOTE: LMS keys are considered to be non-exportable for Extended Virtual Keys.
- **Create uncached keys** – Select this option if you want to keep all the non-exportable primary keys during key sync so that the virtual keys will be created in the secondary group without the cached key material.

WARNING: Clearing the **Fetch Key Material** check box will cause the key material of existing Extended Virtual Keys in the destination group to be removed on the next key scan operation.

6. Click **Enable auto scan** and set a duration in hours to automatically scan the primary group for new keys and changes in existing keys. The default scan duration is set to 1 hour.
7. Click **Show warnings** to display API warnings that occur during the Fortanix DSM primary group scan.
8. Click **SAVE** to save the group.

5.3 ADD CERTIFICATE (OPTIONAL)

1. Click **+ ADD CONFIGURATION** to add a certificate for authenticating your DSM primary cluster.
   a. There are two certificate options to choose from:
      - **Global Root CA** - Use this certificate if you are using a certificate that is signed by a well-known public CA. By default, every DSM-backed group is configured with a Global Root CA Certificate.
      - **Custom CA Certificate** – Use this certificate if you as an enterprise want to self-sign the certificate using your own internal CA. You can override the default Global CA Certificate with a Custom CA Certificate for the DSM primary group. You can either upload the certificate file or copy the contents of the certificate in the textbox provided.
   b. Select the **Validate Host** check box to check if the certificate that the primary DSM provided has the same `subjectAltName` or `Common Name (CN)` as the hostname that the server certificate is coming from.

2. **+ ADD CLIENT CERTIFICATE** (optional): The Custom CA Certificate also has a Client Certificate section where you can configure a client certificate and a private key (Fortanix DSM Certificate and Key). This allows the Fortanix DSM secondary cluster to authenticate itself to the Fortanix DSM primary cluster and vice versa.

5.4 THE HSM/KMS TAB

The **HSM/KMS** tab shows the connection details of the Fortanix DSM primary cluster. You can also edit the connection details here.
After you edit the connection details and save it, click **TEST CONNECTION** to test the connection.

Click **SYNC KEYS** to sync keys from the configured Fortanix DSM primary group to the Fortanix DSM secondary group.

For Extended Virtual Keys, you can also **Fetch key material**, **Enable auto scan**, and **Show warnings** as explained in *Step 5 in Section 5.2: Configure the Primary DSM Cluster on the Secondary DSM Cluster*.

Click **Save Changes** to save the new settings.

6.0 DOCUMENT INFORMATION

6.1 DOCUMENT LOCATION

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

https://support.fortanix.com/hc/en-us/articles/11593113168148-User-s-Guide-Store-Keys-Externally-Setup

6.2 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