Fortanix®

User Guide

FORTANIX DATA SECURITY MANAGER – AWS EXTERNAL KMS

VERSION 2.6

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

Welcome to the Fortanix Data Security Manager (DSM) Amazon Web Services (AWS) Key Management User Guide. This document describes how to add a new AWS / External KMS to Fortanix DSM. It contains the information related to:

- Creating an AWS KMS group in Fortanix DSM
- Configuring the AWS KMS Connection in Fortanix DSM
- Testing the AWS KMS Connection
- Syncing the AWS KMS Keys in Fortanix DSM

The Fortanix solution for AWS Key Management Service (KMS) offers complete Bring Your Own Key (BYOK) and lifecycle management for management and automation of native AWS KMS keys (CMK – Customer Managed Key) and allows users to manage all keys centrally and securely.

2.0 CONCEPTS

2.1 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

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. You 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 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.

- **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, or other security objects). 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 see support .

3.0 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.*

4.0 FORTANIX DATA SECURITY MANAGER AWS KMS GROUP WORKFLOW

The following section describes the workflow to configure Fortanix DSM to interact with the AWS Key Management System (KMS). An AWS KMS group is created in the Fortanix DSM account, and this group is configured to interact with the AWS KMS.

4.1 CREATE AN AWS KMS GROUP

1. On the Fortanix DSM **Groups**  page, click the  button to create a new AWS KMS group.
2. In the **Add new group** form:
   a. Enter a title and description for your group.
   b. Next, click the **LINK HSM/EXTERNAL KMS** button to select the AWS KMS type, so that Fortanix DSM can connect to it.

4.2 CONFIGURE THE AWS KMS

4.2.1 PREREQUISITES

To configure the AWS group, the following are the **AWS KMS permissions** that the AWS Identity and Access Management (IAM) users must have to authenticate the Fortanix DSM group with AWS Key Management Services:

LIST Permissions:

- ListKeys
- ListKeyPolicies
- ListRetirableGrants

- ListAliases
- ListGrants
- ListResourceTags
- ListResourceTagsd

READ Permissions:

- DescribeKey
- GetPublicKey
- GetKeyRotationStatus
- GetKeyPolicy
- GetParametersForImport

WRITE Permissions:

- CreateKey
- ImportKeyMaterial
- DeleteImportedKeyMaterial
- EnableKey
- DisableKey
- ScheduleKeyDeletion
- CancelKeyDeletion
- EnableKeyRotation
- DisableKeyRotation
- CreateAlias
- DeleteAlias
- UpdateAlias
- PutKeyPolicy
- GenerateDataKey
- TagResource
- UntagResource
- CreateGrant
- RetireGrant
- RevokeGrant

4.2.2 CREATE AWS KMS GROUP

1. Select the type of HSM/external KMS as **AWS Key Management Service** from the drop down menu.
2. In the **Choose Region** field, select the AWS region from which the keys should be imported.
3. Enter the AWS KMS Service Account Credentials:
   a. **URL**: The URL of the AWS region gets auto-populated based on the region selected. This is an editable field, so a user can also add a custom URL of the AWS region. In the case of a custom URL, the **URL** label will change to **URL (Custom)**.
   b. **AWS_ACCESS_KEY_ID** and **AWS_SECRET_ACCESS_KEY**: Access key and Secret Access Key are used for accessing the AWS services. Each AWS account has its unique login credentials; Fortanix Data Security Manager should allow its users to log in and securely save AWS credentials to do native cloud key management and offline automation such as automatic key rotation based on a set schedule and so on. *For more information on obtaining AWS credentials, refer to AWS documentation*.

4.3 TEST CONNECTION

Click **TEST CONNECTION** to test your AWS KMS connection. If Fortanix DSM can connect to your AWS 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  .

4.4 ADD CERTIFICATE

1. Click **+ ADD CONFIGURATION** to add a certificate for authenticating your AWS KMS. Fortanix's external KMS solution requires that the customer applications use one of the Fortanix DSM interfaces (REST, PKCS#11, KMIP, JCE, or CNG) to interact with Fortanix DSM for key management and cryptographic operations. These applications should be configured to authenticate to Fortanix DSM using Certificate or Trusted Certificate Authority (CA) instead of directly communicating to AWS KMS.

   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 AWS KMS 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 an AWS KMS group. You can either upload the certificate file or copy the contents of the certificate in the textbox provided.
- Client Certificate (optional): A 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 Fortanix DSM to authenticate itself to the AWS KMS and vice versa.

2. Select the **Validate Host** check box to check if the certificate that the AWS KMS provided has the same `subjectAltName` or `Common Name (CN)` as the hostname that the server certificate is coming from.

4.5 SAVE AWS KMS GROUP DETAILS

Though testing the connection in the previous section is an optional step, you can save your group details even if the connection information might be incorrect or incomplete, you can edit these details later. Now, save your group details by clicking the **SAVE** button.

Once you save your group details, your group is created, and you will see a detailed view of your group.

Now you can see that there is an addition of the **HSM/KMS** tab in the group details, this tab shows the details about your KMS.

4.6 THE HSM/KMS TAB

The **HSM/KMS** tab shows the details of the AWS Service Type and the connection details of that Service Type such as the URL, access key, and secret. You can also edit the AWS connection details here.

Once you edit the connection details and save it, click **TEST CONNECTION** to test the connection.

Click **SYNC KEYS** to sync keys from the configured AWS KMS to the AWS group.

4.7 NOT CONNECTED SCENARIO

On clicking **TEST CONNECTION**, it is possible that Fortanix DSM is not able to connect to the AWS node, in that case, it displays a "**Not Connected**" status with a warning symbol . You can save the details of the new connection details provided and edit them later.

4.8 GROUPS TABLE VIEW

After saving the group details, you can see the list of all groups and notice the special symbol next to the newly created group, this symbol differentiates it from the other groups, as it shows that it is an AWS KMS group.

4.9 USER VIEW

Click the **Users** tab in the Fortanix DSM UI and click the user that says "**You**" to go to the user's detailed view, as shown below:

The detailed view shows all the groups of which the user is a part of, additionally Fortanix DSM displays which groups are mapped to AWS KMS and whether they are "Connected" or "Not Connected".

5.0 FORTANIX DATA SECURITY MANAGER AWS KMS SECURITY OBJECTS

After the AWS group successfully connects to the AWS KMS using the connection details, the keys from the AWS KMS are stored in the Fortanix DSM AWS group as virtual keys. A virtual key is a key whose key material is not present in the AWS group. The key material is stored securely in the AWS KMS. The virtual key is only a pointer with the key information and key attributes, but it does not hold the key material.

5.1 CREATE A KEY IN AWS KMS GROUP - GENERATE

You can generate a key in a configured AWS KMS group.

5.1.1 GENERATE A KEY

This action will generate the configured key type in the configured AWS KMS regions directly, and it will be represented as a virtual key in the corresponding AWS KMS group. This means that the virtual key in the AWS KMS group will point to the actual key in AWS

KMS that stores the key material of this new key. The virtual key only stores the key information and key attributes, but it does not have the key material.

In your Fortanix DSM console, follow the process below to create a new key:

1. Click the **Security Objects** tab.
2. Click to create a new Security Object.
3. In the **Add New Security Object** form enter a name for the Security Object (Key).
4. Select the **This is an HSM/external KMS object** check box. This will show the AWS KMS configured groups in the **Select group** list.
5. In the AWS group list, select the AWS group into which the keys will be generated. The keys will be generated into the region that was selected in the AWS group.
6. Select **GENERATE IN AWS** to initiate the generate key in the AWS workflow.
7. Add an alias in the **AWS Aliases** section. Use the **ADD ALIAS** button if you are adding more than two aliases.
8. Select the key type for the new AWS KMS key.

NOTE: The allowed key type for an AWS key generated using the Generate Key button is AES 256.

These key types can further be restricted by setting a crypto policy for the account or group. For more details about the crypto policy, *please refer to the article:* *https://support.fortanix.com/hc/en-us/articles/360042064051-User-s-Guide-Crypto-Policy*.

NOTE: Currently Fortanix DSM supports key type of AES 256. Support for generating RSA and EC keys is coming soon.

9. Enter the **Key size** and select the permitted key operations under **Key operations permitted** section.
10. Add a tag in the **AWS Tags** sections. Use the **NEW TAG** button if you are adding more than one tag. *For more details, refer to Section 5.4.*
11. Enable the toggle for **Multi-region primary key** to create an AWS multi-region Primary Key. *For more details, refer to Section 5.2.*
12. Click the **GENERATE** button to generate the key in AWS.

13. The new AWS Key is created and represented with a special symbol  to denote it is of type AWS/KMS. In the detailed view of the AWS key, you will notice the following things:
    - An icon next to the key name indicating if it a multi-Region primary key.
    - The group and region to which it belongs (in the **Group** field). It also shows if the group is mapped to an AWS or not using the special icon  .
    - How the key was created (in the **Created by** field). If it is an AWS KMS key, this field shows the group that created this key. It also shows minor details such as if the group is "Connected" or "Not Connected".
14. The new key will be added to the Security Objects table.

 Tip:

- You can also access the new key from the Group detailed view from the **SECURITY OBJECTS** tab.
- You can also add a new key from the Group detailed view from the **SECURITY OBJECTS** tab, click **ADD SECURITY OBJECT** button, and follow ***steps 3-10*** above.

5.1.2 BRING YOU OWN KEY – IMPORT KEY

This action will import the configured key type in one of the configured AWS KMS regions directly, and it will be represented as a virtual key in the corresponding AWS KMS group. This means that the virtual key in the AWS KMS group will point to the actual key in AWS KMS that stores the key material of this new key. The virtual key only stores the key information and key attributes, but it does not have the key material. The import action will not store a copy of the key material in Fortanix DSM.

1. Follow Steps 1-5 from *Section 5.1.1*
2. Select **IMPORT** to initiate the import key in the AWS workflow.
3. Add an alias in the **AWS Aliases** section. Use the **ADD ALIAS** button if you are adding more than two aliases.
4. Select the key type for the new AWS KMS key.

 **NOTE:** The allowed key type for an AWS key generated using the Import Key button is only AES 256 keys.

5. Sometimes keys of type AES that need to be imported from a file were previously wrapped (encrypted) by a key from Fortanix DSM. This is done so that the key should not go over the TLS in plain text format. In such scenarios select the check box **The key has been encrypted**.
6. Next enter or select a Key ID or SO name in the **Select Key Encryption Key** section which will be used to unwrap (decrypt) the encrypted key in the file which will later be stored securely in Fortanix DSM. This key should have already been created or imported in Fortanix DSM.
7. Click **UPLOAD A FILE** to upload the key file in **Raw**, **Base64**, or **Hex** format.
8. Select the permitted key operations under **Key operations permitted** section.
9. Add a tag in the **AWS Tags** sections. Use the **NEW TAG** button if you are adding more than one tag. *For more details, refer to Section 5.4.*
10. Enable the toggle for **Multi-region primary key** to create replicas of the key in other regions of AWS KMS. *For more details, refer to Section 5.2.*
11. Click **IMPORT** to import the key.
12. The key is successfully imported.

5.1.3 BRING YOUR OWN KEY – COPY KEY TO AWS

Use this option when you want to generate a key in Fortanix DSM and then import the key into the configured AWS KMS. The copy key to AWS feature will copy a security object from one regular Fortanix DSM group to another regular/AWS KMS Fortanix DSM group. This feature has the following advantages:

- Maintains a single source of key material while using/importing that key into various Fortanix DSM groups where applications may need to use a single key to meet business objectives.
- Maintains a link of various copies of the same key material to the source key for audit and tracking purposes.

The following actions will happen as part of the copy key operation:

- A new key will be created in the target group: The new key will have the same key material as the original.
- The source key links to the copied keys: There will be a link maintained from all copied keys to the source key.

- The source key will also have basic metadata-based information about the linked keys such as:
  - Copied by <user-name/app id>
  - Date of Copy <time stamp>
  - Target copy group name

NOTE: The name of the copied key is suggested automatically to the user as `[original key name]_[copy1,2,...]`, but can be replaced with an alternative unique name.

To copy a key from a regular Fortanix DSM group to an AWS group:

1. Go to the detailed view of a key and click the **NEW OBJECT** icon on the far right of the screen.
2. In the menu that appears, click the **COPY KEY** button.

NOTE:

- To copy a key from a regular Fortanix DSM group to an AWS KMS group, the key must be AES 256. AWS KMS only supports only AES 256 keys during copy or import operations.
- The AES 256 key to be copied must have the "Export" permission enabled or the copy key operation will fail.
- The COPY KEY button will be disabled for all the AWS KMS virtual keys.

3. In the **COPY KEY** window, update the name of the key if required.
4. Click the **Import key to HSM/External KMS** check box to filter the groups to show only AWS KMS groups. Select the AWS group for the new key into which the copied key should be imported.
5. Add aliases in the **AWS Aliases** section.
6. Update **KEY PERMISSIONS** if you want to modify the permissions of the key.
7. Click **CREATE COPY** to create a copy of the key.
8. The source key will now appear as a key link in the **KEY LINKS** tab in the detailed view of the copied key.

NOTE: If a user wants to maintain a copy of the key material in Fortanix DSM, then the user can import a regular AES 256 key into Fortanix DSM using the "import key" workflow and then copy this key into AWS using the "copy key" workflow.

5.2 MULTI-REGION KEYS

Fortanix DSM supports marking an AWS virtual key as a multi-region primary key in an AWS region so that replicas of this key can be created in other regions of AWS KMS making the primary key a multi-Region key.

NOTE: Replicas of a multi-region key cannot be created from Fortanix DSM.

The multi-Region keys are AWS KMS keys in different AWS Regions that can be used interchangeably – as though you had the same key in multiple Regions. Each set of related multi-Region keys has the same **key material** and **key ID** in AWS KMS, so you can encrypt data in one AWS Region and decrypt it in a different AWS Region without re-encrypting or making a cross-Region call to AWS KMS. You can use multi-Region keys in all cryptographic operations that you can do with single-Region keys.

5.3 SYNC KEYS

When you edit the AWS connection details in the AWS group detailed view under **HSM/KMS** tab, click **SYNC KEYS** to import new keys. On clicking **SYNC KEYS**, Fortanix DSM connects to AWS and gets all the keys available. Fortanix DSM then stores them as virtual keys.

NOTE:

- When keys are synced with AWS KMS, the metadata of the existing keys for the configured service account and region are downloaded and represented as virtual keys. The actual key material for those keys is always stored in AWS KMS.
- Clicking **SYNC KEYS** only returns the keys from AWS that are not present in Fortanix DSM. That is, every click will append only new keys to Fortanix DSM.
- If some keys were marked as multi-Region primary keys or multi-Region replica keys in AWS KMS before the scan, then clicking **SYNC KEYS** will identify these keys and mark them as multi-Region primary keys or multi-Region replica keys respectively.

- The time taken to sync keys from AWS KMS to Fortanix DSM is a function of the number of keys in the AWS KMS and the network latency between the AWS location and Fortanix DSM. It can take several minutes if there are hundreds of keys and there is significant network latency.
- The AWS KMS groups have a scan limitation. When the AWS KMS region has more than 100 keys, only 100 virtual keys are created during the group scan.

5.4 ATTRIBUTES/TAGS TAB

This tab will have all the attributes and tags of the AWS key. You can add new tags using the **NEW TAG** button.

5.5 AWS KEY DETAILS

This tab displays details of the AWS Key Aliases, Key ARN for Key ID, and the AWS key policy.

If the AWS virtual key is a multi-Region primary key, then the Key ARN section will also display the key ARNs of the replica keys.

If the AWS virtual key is a multi-Region replica key, then the Key ARN section will also display the key ARN of the primary key.

The **AWS KEY DETAILS** tab also contains **SCHEDULE KEY DELETION** and **DELETE KEY MATERIAL** options which are explained in *Section 5.7* and *Section 5.9,* respectively.

5.6 SECURITY OBJECTS TABLE VIEW

After you add new AWS keys, go to the **Security Objects** page to view all the security objects from all the groups (AWS and non-AWS).

In the security object table, you will notice that every key belongs to a group and some keys which are virtual keys added from an AWS, belongs to a group with a special symbol  . The security objects table view will continue to show all the keys irrespective of if they belong to an AWS group or not.

5.7 SCHEDULE TO DELETE A KEY IN AWS KMS

When you delete a key from an AWS KMS, the action will delete the actual key in the configured AWS and will appear as disabled in the security objects table.

To delete a key from an AWS KMS:

1. Go to the detailed view of an AWS virtual key and select the **AWS KEY DETAILS** tab.
2. Click the link **SCHEDULE KEY DELETION**.
3. In the Schedule Key Deletion in the AWS KMS window, enter a waiting period (in days) to verify whether you still need the AWS key.

   NOTE: Data encrypted with the key can no longer be used once the key is deleted.
4. Click **SCHEDULE KEY DELETE** button to mark the key for deletion.
5. You can cancel the key deletion any time before the waiting period ends using the **CANCEL KEY DELETION IN AWS** link on the top of the screen in the detailed view of the virtual key.

After the key is permanently deleted from AWS KMS, the **Delete Key** button is enabled in the detailed view of the virtual key in Fortanix DSM.

5.8 DELETE A KEY IN AWS GROUP

NOTE: The **DELETE KEY** option is enabled only when the key is permanently deleted from AWS KMS.

When you delete a key from an AWS group, the action will only delete the virtual key in Fortanix DSM and will not delete the actual key in the configured AWS.

To delete a virtual key:

1. Select the AWS key to delete.
2. In the security object detailed view, scroll down and click the **DELETE KEY** button.

5.9 DELETE KEY MATERIAL IN AWS KMS

When an AES 256 key is copied into AWS KMS from Fortanix DSM, the key material is stored in two places, the source key in the regular Fortanix DSM group and in the configured AWS KMS for a specific account and region. This key is represented as a virtual key in the AWS KMS group. A virtual key is only a virtual representation of the actual AWS KMS key that contains the key information and key attributes; however, this virtual key does not contain the key material. Users may want to delete the key material from the configured AWS KMS to maintain a single copy of key material stored securely in the source key in the regular Fortanix DSM group.

NOTE:

- The Delete Key material feature is enabled only for keys of type AES 256 that have been externally imported into AWS KMS.
- The Delete key material feature is visible only for BYOK keys, that is, for keys that were copied from Fortanix DSM.

To delete the key material:

1. Go to the detailed view of a virtual key in the AWS group and select the **AWS KEY DETAILS** tab.
2. Click the **DELETE KEY MATERIAL** link to delete the key material in AWS KMS.
3. In the **Delete Key Material in AWS KMS** window, click the **DELETE KEY MATERIAL** button. The status of the key in the AWS KMS changes to **"Pending import"**.
4. Once the key material is deleted from AWS KMS, it can be reimported back into AWS KMS to reverse the key material deletion. To reimport the key material:
   a. Go to the detailed view of the virtual key and click the **REIMPORT KEY MATERIAL** link on top of the screen.
   b. The key material is reimported successfully.

6.0 ROTATE A KEY IN AWS GROUP

The following section explains the Key Rotation in AWS Group. A Key is rotated when you want to retire an encryption key and replace that old key by generating a new cryptographic key.

6.1 ROTATING AWS NATIVE KEY* WITH ANOTHER NATIVE KEY

**Native key is one where the key material was generated by AWS KMS.*

When you rotate a virtual key in an AWS group, the action will rotate the key inside the AWS KMS by generating another key within the configured AWS KMS by moving the key alias from the old key to the new key.

To rotate a key in AWS:

1. Select the AWS virtual key to rotate.
2. In the detailed view of the AWS virtual key, click the **ROTATE KEY** button.
3. In the Key Rotation window, click the **ROTATE KEY** button to rotate the virtual key.

A new rotated key is now generated.

6.2 ROTATING KEYS IN FORTANIX DATA SECURITY MANAGER SOURCE GROUP

When a key is rotated that belongs to a Fortanix DSM source group and has linked keys that are copies of the Fortanix DSM source key with the same key material as the source key, then the user is given the option to select the linked keys for key rotation. If these linked keys belong to an AWS group, then rotating the linked keys results in rotating the keys in AWS KMS as well by generating new keys within the configured AWS KMS and by moving the aliases from old to new keys.

1. Click **ROTATE KEY** in the detailed view of a Fortanix DSM Source Key.
2. In the KEY ROTATION window, select the **Rotate linked keys** check box.
3. Select the AWS Virtual Keys that needs to be rotated along with the Fortanix DSM source key and click the **ROTATE KEY** button.

   NOTE: In the KEY ROTATION window, if the user edits the default key size of the source key from AES 256 to a new value, then selecting the "**Rotate linked keys**" option disables the AWS virtual keys. AWS KMS only supports AES 256 keys. Linked keys that are not AWS KMS keys will still be available for rotation with the new key size value.
4. After the keys are rotated, click the **OK** button.

You can also schedule a key rotation policy for the Fortanix DSM source key such that the linked AWS KMS keys that are copies of the source keys are also periodically rotated automatically.
To schedule a key rotation policy for the source key:

1. Go to the detailed view of the source key in the Fortanix DSM UI.
2. In the detailed view, click the **KEY ROTATION** tab and click the **ADD POLICY** button.
3. Enter the key rotation schedule by specifying the rotation frequency, start date, and time.
4. To deactivate the old key after key rotation, select the **Deactivate original key after the rotation** check box.
5. To rotate the linked copied keys, select the **Rotate all copied keys** check box.
6. Click **SAVE POLICY** to save the policy.

For more information on the key rotation policy, refer to the User's Guide: Key Lifecycle Management.

6.3 ROTATE AWS NATIVE KEY TO FORTANIX DATA SECURITY MANAGER OWNED KEY

When an AWS virtual key whose key material is owned by AWS KMS is rotated, the user is given an option to rotate the virtual key with a Fortanix DSM backed key. When the user selects this option and performs the rotation, a new virtual key is created, with corresponding key in AWS KMS, which has the key material of the Fortanix DSM backed key. As a result, the AWS virtual key is backed by a Fortanix DSM source key.

To rotate a virtual key with Fortanix DSM backed key:

1. Click **ROTATE KEY** in the detailed view of an AWS virtual key.
2. In the Key Rotation window, select the **Rotate to S-D KMS key** check box.
3. Select the Fortanix DSM group that contains the source key.
4. Select the source key and click the **ROTATE KEY** button.

The Virtual key is successfully rotated and backed by the source key. To confirm, go to the detailed view of the newly rotated AWS virtual key and click the **AWS KEY DETAILS** tab. The **SOURCE** field now points to “FortanixHSM” instead of “External”.

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/360055605471-User-s-Guide-AWS-External-KMS

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