Fortanix®

User Guide

FORTANIX DATA SECURITY MANAGER – AWS KMS BRING YOUR OWN KEY (BYOK)

VERSION 3.0

Fortanix Inc. | 3910 Freedom Circle | Suit 104 | Santa Clara, CA 95054 | 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) and Amazon Web Services (AWS) Bring Your Own Key (BYOK) User Guide. This document describes how to perform BYOK lifecycle management in AWS KMS using Fortanix DSM.

The Fortanix solution for AWS Key Management Service (KMS) offers complete Bring Your Own Key (BYOK), as explained in this guide, as well as Cloud Native Key Management (CNKMS) and Bring your own KMS (BYOKMS), with complete lifecycle management for automation.

2.0 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.

2.1 SUPPORT RESOURCES

For more information see support .

3.0 GETTING STARTED WITH FORTANIX CLOUD DATA CONTROL

To understand which solution between CNKMS, BYOK, BYOKMS (AWS XKS), or BYOE is right for you, please see *Fortanix Data Security Manager Cloud Data Control Getting Started Guide*.

4.0 FORTANIX AWS BYOK WORKFLOWS OVERVIEW

- **Generate key**: Navigate to a source key in Fortanix DSM and copy the key into an AWS CDC group to create a linked key and a BYOK key in AWS KMS.
- **Rotate source key:** Rotate the source key that was originally generated in "Fortanix DSM" and click "rotate linked/copied keys".
- **Disable/Enable**: Navigate to the detailed view of the key in the AWS CDC group and disable or enable it from Fortanix DSM.
- **Schedule key deletion**: AWS will not allow you to natively delete a key directly unless you explicitly schedule it for deletion and the mandatory waiting period expires (at least 7 days). Navigate to the detailed view of the key in the AWS CDC group, and in the **AWS KEY DETAILS** tab, schedule the key for deletion.
- **Delete Key Material:** This is only available for BYOK and allows you to ignore the mandatory wait time of Schedule key deletion but keeps the key ARN in place, so when you restore the Key Material, no updates need to be made to services.

5.0 FORTANIX DATA SECURITY MANAGER AWS KMS SECURITY OBJECTS

After the AWS CDC group successfully connects to the AWS KMS using the connection details, the keys from the AWS KMS are stored in the Fortanix DSM AWS CDC group as virtual keys. A virtual key is a key whose key material is not present in the AWS CDC 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 CDC GROUP

You can copy or import a key into a configured AWS CDC group.

5.1.1 BRING YOUR OWN KEY – COPY KEY TO AWS TO CREATE A LINKED KEY

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 CDC group. This feature has the following advantages:

- Maintains a single source key while copying/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 ability to name, and rotate keys everywhere all at once, as well as audit and tracking purposes. Key Rotation at the Source key even handles updating the AWS Alias.
- The Linked Keys approach tends to be a bit easier to manage than AWS native Multi-Region Keys and Multi-Account Keys by handling AWS Alias updates, and showing the keys in AWS KMS where Fortanix can still disable, enable and delete keys and key material
- In AWS, the BYOK keys also further improve your security posture by allowing you to remotely delete key material from a key instantly in AWS. AWS limits your ability to delete a key by creating a 7-day “Key Undo” wait time, this is because AWS wants to protect against accidental deletion. However, with BYOK keys, AWS knows you have another copy of the key and will let you delete key material instantaneously, a great additional security measure not available with native KMS.
- Zero Trust Quorum - Key functions like disabling keys or scheduling the deletion of keys can be done from Fortanix and protected by Quorum. Most customers choose to limit their IAM to only allow Fortanix and perhaps 1 “Break Glass Account” to Create, Disable/Enable, Scheduled Delete, and Delete key material.

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 CDC 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 CDC 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.

5.1.2 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 CDC group. This means that the virtual key in the Fortanix AWS CDC 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. 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 CDC group into which the keys will be imported. The keys will be imported into the region that was selected in the AWS CDC group.
6. Select **IMPORT** to initiate the import 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 Import Key button is only AES 256 keys.

9. 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**.

10. 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 into Fortanix DSM.
11. Click **UPLOAD A FILE** to upload the key file in **Raw**, **Base64**, or **Hex** format.
12. Select the permitted key operations under **Key operations permitted** section.
13. Add a tag in the **AWS Tags** sections. Use the **ADD TAG** button if you are adding more than one tag. *For more details, refer to Section 5.4.*
14. Enable the toggle for **Multi-region primary key** to create an AWS multi-region Primary Key. *For more details, refer to Section 5.2*.
15. Click **IMPORT** to import the key.
16. The key is successfully imported.

5.2 MULTI-REGION KEYS

Fortanix DSM supports marking an AWS virtual key as a multi-region primary key in an AWS KMS 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 significant network latency.
- The AWS CDC 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. A tag is an optional metadata label that you can assign to an AWS resource. You can add new tags using the **NEW TAG** button and add custom attributes by using the **ADD CUSTOM ATTRIBUTE** button. These are user-defined security object attributes that can be added to the security object's metadata.

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 KMS, 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 CDC 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 KMS 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 CDC 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 CDC 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 CDC 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 CDC GROUP

The following section explains the Key Rotation in AWS CDC 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 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 CDC 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.

6.2 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/11532677984404-Fortanix-DSM-AWS-KMS-Bring-Your-Own-Key-BYOK-

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